ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

شماره مجوز مجله:۸۰۴۰۰ زمان چاپ:۱۴۰۲/۱۱/۲۰

بررسی جرائم رایانه ای مربوط به سیستم بانکی در استان کهگیلویه وبویراحمد

سید احمد موسوی[۱]

۱- کارشناسی ارشد حسابداری

amosavi۶۴۷@gmail.com

چکیده

هدف تحقیق حاضر بررسی جرائم رایانه‌ای مربوط به سیستم بانکی در استان کهگیلویه و بویراحمد می‌باشد. تحقیق از نظر کاربردی از نوع تحقیقات مقطعی، توصیفی ـ پیمایشی می‌باشد. جامعه آماری مطالعه شامل کلیه کارکنان بانک‌های استان کهگیلویه و بویراحمد می‌باشد با استفاده از فرمول کوکران ۹۴ نفر از آن‌ها به روش تصادفی ساده به‌عنوان نمونه آماری تحقیق انتخاب گردید. ابزار اصلی گردآوری داده‌های تحقیق، پرسشنامه است در این تحقیق، از دو پرسشنامه استفاده شد : پرسشنامه جرائم اینترنتی بانکداری الکترونیکی شامل ۱۸ گویه و شش مؤلفه، تقلب در کارت اعتباری و انتقال وجه الکترونیکی، جعل پول الکترونیکی، رمزگیری (سرقت هویت و اطلاعات)، کلاه‌برداری اینترنتی، اختلال (یا تخریب) سامانه‌های الکترونیکی،افشای اطلاعات و حریم خصوصی می‌باشد. روایی پرسشنامه‌ها به‌وسیله اساتید و خبرگان به تائید و پایایی آن به‌وسیله ضرایب آلفای کرونباخ تمام گویه بالای ۰/۷۰ مورد تائید قرار گرفت. برای تحلیل داده‌ها از آزمون‌های آماری اسمیرنوف-کولموگروف، تی-تک نمونه در نرم‌افزار spss نسخه ۲۴ استفاده شد. نتایج فرضیه اول نشان داد که تفاوت معناداری بین میانگین کارت اعتباری و انتقال وجه الکترونیکی و میانگین نظری وجود دارد. همچنین نتایج فرضیه دوم نشان داد که تفاوت معناداری بین میانگین جعل پول الکترونیکی و میانگین نظری وجود دارد. بنابراین میزان جعل پول الکترونیکی در بانک‌های موردمطالعه در سطح پایینی است. (عدم تائید فرضیه فرعی دوم). نتایج نشان داد که تفاوت معناداری بین میانگین رمزگیری (سرقت هویت و اطلاعات)و میانگین نظری وجود دارد. بنابراین میزان رمزگیری (سرقت هویت و اطلاعات)در بانک‌های موردمطالعه در سطح بالایی است. (تائید فرضیه فرعی سوم). همچنین بر اساس t به‌دست‌آمده (۷،۵۱۶)در درجه آزادی ۹۳ ، تفاوت معناداری بین میانگین کلاه‌برداری اینترنتی و میانگین نظری وجود دارد. بنابراین میزان کلاه‌برداری اینترنتی در بانک‌های موردمطالعه در سطح بالایی است (تائید فرضیه فرعی چهارم). تفاوت معناداری بین میانگین اختلال (یا تخریب) سامانه‌های الکترونیکی و میانگین نظری وجود دارد. بنابراین میزان اختلال (یا تخریب) سامانه‌های الکترونیکی در بانک‌های موردمطالعه در سطح بالایی است (تائید فرضیه فرعی پنجم). درنهایت تفاوت معناداری بین میانگین افشای اطلاعات و حریم خصوصی و میانگین نظری وجود دارد. بنابراین میزان افشای اطلاعات و حریم خصوصی در بانک‌های موردمطالعه در سطح پایینی است (عدم تائید فرضیه فرعی ششم).

کلمات کلیدی: جرائم رایانه‌ای، سیستم بانکی، کهگیلویه و بویراحمد

۱- مقدمه

پیشرفت در فن‌آوری اطلاع‌رسانی و ارتباطات شبکه‌های اطلاعاتی جهت افزایش سرعت و کیفیت در ارائه خدمات، بانکداری را نیز تحت تأثیر خود قرار داده است (قریشی محمدی،۱۴۰۱). بانکداری الکترونیک می‌تواند کارایی و رقابت‌پذیری یک بانک را

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

افزایش دهد، بنابراین مشتریان موجود بالقوه می‌تواند از درجه تسهیلات بالاتری در تراکنش‌ها و معاملات، بهره‌مند شوند. زمانی که این تسهیلات ارائه توسط بانک، با خدمات جدید ترکیب می‌شوند، می‌توانند مشتریان نهایی بانک را فراتر از بازارهای سنتی، بسط و توسعه دهند(جوینده،۱۳۹۴). سیستم بانکی در حوزه فن‌آوری و ارتباطات، پیشرفت‌هایی از قبیل راه‌اندازی دستگاه‌های خودپرداز، اپلیکشین های بانکداری الکترونیکی، شبکه شتاب و خدمات اینترنتی بانکی اشاره کرد. از سویی باید توجه داشت که پیشرفت‌های نوین بانکی از برخی پیامدهای منفی نیز مبرا نبوده است و پیدایش انواع جرائم نوین در بهره‌برداری از فن‌آوری و اطلاعات، بخش جدیدی از آن به شمار می‌رود .جرائم خدمات نوین بانکی شامل دو گروه است که موجب سوءاستفاده گسترده در سیستم بانکی می‌شوند.(اسنل[۱]،۲۰۱۷). با شیوع استفاده از رایانه در زندگی شخصی و روابط اداری، بزهکاری و تخلف در استفاده از رایانه نیز واقعه اجتناب‌ناپذیر است. آنچه امروز تحت عنوان جرائم رایانه‌ای نام برده می‌شود، مجموعه‌ای از همین تخلفات و بزهکاری‌هاست که از طریق رایانه یا مؤثر بر رایانه اتفاق می‌افتند و مصادیق متعددی از آن نیز در ذهن ما نقش بسته است. چه‌بسا ساده‌ترین مصادیقی که به جهت کثرت اتفاق در ذهن داریم، مواردی مانند هک پایگاه‌های اینترنتی یا انتشار داده‌های محرمانه از طریق وب‌سایت‌هاست که اغلب با تصور تخلف در خالق انون و عدم امکان تعقیب اتفاق افتاده است (هنری[۲]،۲۰۱۸).

.

در این تحقیق جرائم رایانه‌ای را در حوزه بانکی و نظام بانکی مورد بحث قرار می دهیم .مجرمان رایانه‌ای معمولاً به از بین بردن، خراب کردن و دزدی اطلاعات تمایل دارند. کدرهایی از قبیل کلاه‌برداری الکترونیکی، سوءاستفاده از تجهیزات، جازدن خود به جای کس دیگر و همین طور اخلال در سیستم‌ها ازجمله جرائم رایانه‌ای معمول است که تقریب به‌اتفاق آن در سیستم بانکی رخ می‌دهد. یک عمل مجرمانه رایانه‌ای لزوماً واردکردن خسارت فیزیکی به یک تجهیزات یا یک سیستم نیست. بلکه گاه فقط دسترسی به برخی اطلاعات حساس یا محرمانه می‌تواند جرم باشد(سیمونز[۳]،۲۰۱۸).

پیشرفت فن‌آوری رایانه‌ای این امکان را به وجود آورده که جرائم جدیدی پیدا شوند که در مقایسه با روش سنتی جعل، بسیار غنی‌تر می‌باشند. هرچند که اغلب دزدان کامپیوتری برای خودنمایی این کار را انجام می‌دهند، ولی این دزدها که با هدف دسترسی به بانک‌های اطلاعاتی بانک‌ها می‌باشد، مشکل عمده‌ای را به وجود آورده است. مثال بارز آن جلوگیری از دسترسی اینترنتی به‌حساب های بانکی برای مشتریان بوده که دسترسی به برخی از پایگاه‌های اینترنتی معروف را غیرممکن کرده بود (شاهرخی،۱۳۹۲). بانک‌ها از فن‌آوری پیچیده‌ای استفاده می‌کنند تا از دسترسی افراد غیرمجاز به بانک‌های اطلاعاتی مالی خود جلوگیری کنند و با شناسایی خطرات جدید، سیستم‌های خود را به‌طور مداوم ، بهنگام و مد روز می‌نمایند. ولی روشن است که بانک‌ها باید در پی به‌کارگیری روش‌های جدی برای پیشگیری از این جرائم اینترنتی باشند تا بتوانند از زیربنای مالی کشور حفاظت کنند. مبادله دانش فنی برای شناخت جرائم کامپیوتری و یافتن راه مبارز با آن‌ها امری اساسی است. به کمک متخصصان فن‌آوری اطلاعات در حرفه، بانکداری، ارتباطات مستقیمی میان مؤسسات مالی، دولت و مقامات مجری قانون به وجود آمده است تا با این جرائم مبارزه شود (فرانک،۲۰۱۱).

جرائم اینترنتی شبکه بانکی تنوع زیادی دارد، ازجمله زیان‌های ناشی از جعل و سوءاستفاده از کارت‌های اعتباری که امروزه در شبکه بانکی بسیار شاهد آن هستیم و یا بسیاری دیگر از جرائم اینترنتی محسوس در شبکه بانکی. کشور ما به هیچ‌کدام از کنوانسیون‌های بین‌المللی مربوط به جرائم اینترنتی نپیوسته است و با توجه به خلأ موجود در قوانین داخلی، نیروهای انتظامی برای پیشگیری از این جرائم و کشف آن‌ها، در عمل با مشکلاتی مواجه هستند و این در حالی است که امروزه پلیس با بهره

---

[۱] Snell

[۲] Henry

[۳] Simmons

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

گرفتن از فن‌آوری -های نوینی که در عرصه نرم‌افزارهای تخصصی پلیس به وجود آمده است، می‌تواند در پیشگیری از وقوع جرائم مزبور نقش مؤثری داشته باشد(شررام و همکاران،۲۰۱۵).

بنابراین مسئله اساسی در این پژوهش شناسایی انواع جرائم اینترنتی در شبکه بانکی و راه‌های جلوگیری از آن می‌باشد. به‌عبارتی‌دیگر محقق در این پژوهش در پی یافتن پاسخ برای این سؤال است که انواع جرائم اینترنتی مربوط به شبکه بانکی کدام موارد هستند و چگونه می‌توان از آن‌ها جلوگیری نمود .در حوزه پیشگیری از این جرائم، نیز ابزار و متدهای متعددی اندیشیده شده است، در حقوق کیفری، قوانین و مقرراتی بازدارنده در جهت پیشگیری از این جرائم وضع شده است؛ همچنین در حوزه فناوری رایانه‌ای نیز سیستم‌های حسابداری، سیستم‌های بانکداری نوین پیشرفته‌ای طراحی‌شده است تا حدالامکان از رخ داد این جرائم پیشگیری شود. در حوزه پژوهش نیز تحقیقات و مطالعات زیادی به این مسئله توجه داشته است ؛ اما بااین‌وجود هنوز در سیستم‌های بانکی ، جرائم مختلفی صورت می‌گیرد. ازاین‌رو بررسی این موضوع،بررسی جرائم رایانه‌ای در سیستم بانکی استان کهگیلویه و بویراحمدلازم و ضروری است.

۲-پیشینه پژوهش

علیزاده و غلامی (۱۳۹۹) پژوهشی با عنوان پیشگیری از جرائم بانکی از طریق ارتقای مسئولیت اجتماعی انجام دادند. در این مقاله سعی بر آن است به روش توصیفی ـ تحلیلی، با هدف تبیین مسئولیت اجتماعی، به نقش آن در پیشگیری از جرائم بانکی پرداخته شود. علیزاده و همکاران (۱۳۹۸) در پژوهشی یافتند اساساً، حاکمیت شرکتی در بانک، دربرگیرنده کلیه قوانین و مقررات، سازوکارهای مدیریتی و فرآیندهای حسابداری و حسابرسی است که راه را برای رسیدن به چهار هدف اصلی پاسخگویی، شفافیت، عدالت و رعایت حقوق ذینفعان هموار میسازد و ضمن ایجاد یک ساختار شفاف و قابل اعتماد در بانک، احتمال بروز انواع جرائم را در آن به حداقل میرساند. در واقع الگوی مذکور، یک ابزار مؤثر نظارتی است که در حوزه پیشگیری از جرائم بانکی کارساز بوده و اصول کمیته بازل، عناصر مهم فرآیندی آن را تشکیل میدهند.

کریستی (۲۰۲۰) در مقاله ای بیان داشتند چالش های جهانی در زمینه تحول جرایم سایبری در مورد کشورهای در حال ظهور یا در حال توسعه پویا است ، بنابراین توسعه پایدار نقش اساسی را ایفا می کند . عالوه بر این ، اثرات انتشار می تواند خسارات قابل توجهی را در بخش بانکی ایجاد کند . مدیریت کارآمد بانک در زمینه ارائه تکنیک های پیشرفته برای امنیت سایبری ضروری است. اقدامات امنیتی سایبری سنتی برای اطمینان از حفاظت از داده ها و حفظ حریم خصوصی اطالعات آنالین کافی نیست. در نتیجه ، تحقیقات درباره فعالیتهای مجرمانه سایبری باید به عنوان یک اولویت به ویژه در زمینه جهانی شدن تبدیل شود. در مطالعه آکینبووال و همکاران (۲۰۲۰) = یک بررسی ادبیات و کارت امتیازی متوازن BSCبرای تجزیه و تحلیل تأثیر جرایم سایبری بر بخش بانکی استفاده می کند .ادبیات مورد بررسی موج فزاینده ای از جرایم سایبری را تحت تاثیر قرار می دهد که بر حسن نیت و رشد اقتصادی موسسات مالی ، به طور غیرمستقیم از طریق از دست دادن اعتماد به زیرساخت های دیجیتال یا مستقیماً از طریق کلاهبرداری و اخاذی در کشورهای در حال توسعه و توسعه یافته تأثیر منفی گذاشته است.

۳-فرضیه‌های تحقیق

فرضیه اصلی

جرائم رایانه‌ای در سیستم بانکی استان کهگیلویه و بویراحمد به میزان بالایی است.

فرضیه‌های فرعی

۱- تقلب در کارت اعتباری و انتقال وجه الکترونیکی در سیستم بانکی استان کهگیلویه و بویراحمد به میزان بالایی است.

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

۲- جعل پول الکترونیکی در سیستم بانکی استان کهگیلویه و بویراحمد به میزان بالایی است.
۳- رمزگیری (سرقت هویت و اطلاعات) در سیستم بانکی استان کهگیلویه و بویراحمد به میزان بالایی است.
۴- کلاه‌برداری اینترنتی در سیستم بانکی استان کهگیلویه و بویراحمد به میزان بالایی است.
۵- اختلال (یا تخریب) سامانه‌های الکترونیکی در سیستم بانکی کهگیلویه و بویراحمد به میزان بالایی است.
۶- افشای اطلاعات و حریم خصوصی در سیستم بانکی کهگیلویه و بویراحمد به میزان بالایی است.

۴- روش تحقیق

به طور کلی این پژوهش برحسب هدف از نوع تحقیقات کاربردی و ازلحاظ روش‌شناسی از نوع تحقیقات مقطعی، توصیفی ـ پیمایشی است. به این دلیل کاربردی است که با استفاده از نتایج تحقیق می‌توان به تشخیص و پیشگیری جرائم اینترنتی در حوزه بانک بهره برد و به این دلیل توصیفی است که مطالعه وضعیت بودجه‌ریزی عملیاتی در سازمان‌ها مدنظر است. و ازاین‌جهت که در جهت تبیین جرائم اینترنتی در بانک از نوع تحلیلی است جامعه آماری تحقیق کلیه کارکنان بانک‌های موردمطالعه است که این تعداد ۱۲۵ نفر برآورد شده است. نمونه آماری تعداد کارمندان بوده که با جدول مورگان ۹۴ نفر محاسبه گردید.

ابزار جمع‌آوری داده‌های تحقیق، پرسشنامه است. در این تحقیق، از یک پرسشنامه محقق ساخته استفاده‌شده است :

پرسشنامه جرائم اینترنتی بانکداری الکترونیکی این پرسشنامه شامل ۱۸ سؤال باشد

۱. تقلب در کارت اعتباری و انتقال وجه الکترونیکی
۲. جعل پول الکترونیکی
۳. رمزگیری)سرقت هویت و اطلاعات
۴. کلاه‌برداری اینترنتی
۵. اختلال (یا تخریب)سامانه‌های الکترونیکی
۶. افشای اطلاعات و حریم خصوصی

تجزیه و تحلیل داده‌های تحقیق در نرم‌افزار spss نسخه ۲۴ انجام گردید. یافته‌های پژوهش در دو بخش آمار توصیفی و آمار استنباطی انجام گردید. در بخش توصیفی، توزیع فراوانی ویژگی‌های جمعیت شناختی پاسخ‌گویان، شاخص‌های مرکزی)میانگین (و پراکندگی)مینیمم-ماکزیمم- انحراف معیار(به همراه جداول و نمودارها ارائه‌شده است. در بخش استنباطی، ابتدا با استفاده از آزمون کولموگروف -اسمیرنوف، نرمال بودن داده‌های تحقیق مورد سنجش قرار می‌گیرد و در ادامه، با استفاده از آزمون تی -تک نمونه ای، به بررسی فرضیات پژوهش بررسی می‌شود

در تحقیق حاضر آزمون پایایی توسط نرم‌افزار SPSS انجام شد. با توجه به اینکه برای پژوهش‌های علوم انسانی ضریب آلفای بالاتر از ۰/۷ قابل قبول است می توان نتیجه گرفت که پایایی پرسشنامه تحقیق خوب است.

جدول۱- ضریب آلفای کرونباخ متغیرهای تحقیق

نام متغیر	تعداد گویه‌ها	ضریب آلفای کرونباخ

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

تقلب در کارت اعتباری و انتقال وجه	۳	۰/۷۷
جعل پول الکترونیکی	۳	۰/۷۶
رمزگیری	۳	۰/۸۹
کلاه‌برداری اینترنتی	۳	۰/۹۱
اختلال (یا تخریب)	۳	۰/۷۳
افشای اطلاعات و حریم خصوصی	۳	۰/۷۹

۵-یافته‌های تحقیق

۵-۱- یافته های توصیفی

جدول ۲-یافته های توصیفی

		فراوانی	درصد
جنسیت	زن	۱۶	۱۴
	مرد	۷۸	۸۶
	مجموع	۹۴	۱۰۰
میزان تحصیلات	کاردانی	۱۲	۸
	کارشناسی	۳۵	۶۸
	کارشناسی ارشد	۴۵	۲۳
	دکتری	۲	۱
	مجموع	۹۴	۱۰۰
سن	زیر ۳۰	۶	۱۰
	۴۰-۳۱	۳۳	۳۳
	۵۰-۴۱	۳۰	۲۹
	۵۱ به بالا	۲۵	۲۸
	مجموع	۹۴	۱۰۰

۵-۲-یافته‌های استنباطی

آزمون نرمال بودن توزیع متغیرهای تحقیق

در جدول ۳-نتایج آزمون کولموگروف- اسمیرنوف برای نرمال بودن توزیع متغیرهای پژوهش ارائه‌شده است.

جدول ۳-نتایج آزمون کولموگروف- اسمیرنوف

متغیر	k-s-z	Sig
پرسشنامه	۰,۹۵۴	۰,۳۲۳

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

نتایج نشان می‌دهد کلیه سطوح آماره z-s-k کولموگرف-اسمیرنوف متغیرهای پژوهش بزرگ‌تر از خطای ۵ درصد می‌باشد. بنابراین توزیع نمرات متغیرها نرمال می‌باشد لذا امکان استفاده از آزمون‌های پارامتریک مجاز می‌باشد به همین سبب از آزمون‌های پارامتریک استفاده گردیده است.

۵-۳- آزمون فرضیات

در این بخش، با استفاده از آزمون تی-تک نمونه ای به بررسی وضعیت متغیرهای تحقیق پرداخته می‌شود. بدین‌صورت که میانگین نمره متغیرهای تحقیق با میانگین نظری (عدد۳)مقایسه می‌گردد.

جدول ۴- آزمون تی-تک نمونه ای فرضیات

میانگین نظری : ۳				
شاخص	اختلاف میانگین	آماره t	درجه آزادی	سطح معناداری
تقلب در کارت اعتباری و انتقال وجه الکترونیکی؛	۰/۶۹۸۵۸	۱۱/۵۸۴	۹۳	۰/۰۰۰
جعل پول الکترونیکی	-۰/۱۴۵۳۹	-۲/۱۱۱	۹۳	۰/۰۳۷
رمزگیری(سرقت هویت و اطلاعات)	۰/۲۱۹۸۶	۲/۴۹۵	۹۳	۰/۰۱۴
کلاهبرداری اینترنتی	۰/۵۴۲۵۵	۷/۵۱۶	۹۳	۰/۰۰۰
اختلال (یا تخریب) سامانه های الکترونیکی	۰/۱۶۶۶۷	۲/۰۵۵	۹۳	۰/۰۴۳
افشای اطلاعات و حریم خصوصی	-۰/۲۹۰۷۸	-۳/۵۱۵	۹۳	۰/۰۰۱

بر اساس جدول ،اختلاف میانگین تقلب در کارت اعتباری و انتقال وجه الکترونیکی با عدد ۳ مثبت می‌باشد. همچنین بر اساس t به‌دست‌آمده (۱۱,۵۸۴) در درجه آزادی ۹۳ ، تفاوت معناداری بین میانگین کارت اعتباری و انتقال وجه الکترونیکی و میانگین نظری وجود دارد. بنابراین میزان تقلب در کارت اعتباری و انتقال وجه الکترونیکی در بانک‌های موردمطالعه در سطح بالایی است (تائید فرضیه فرعی اول).

.بر اساس جدول ،اختلاف میانگین جعل پول الکترونیکی با عدد ۳ منفی می‌باشد .همچنین بر اساس t به‌دست‌آمده (۲,۱۱۱-) در درجه آزادی ۹۳ ، تفاوت معناداری بین میانگین جعل پول الکترونیکی و میانگین نظری وجود دارد. بنابراین میزان جعل پول الکترونیکی در بانک‌های موردمطالعه در سطح پایینی است (عدم تائید فرضیه فرعی دوم).

بر اساس جدول اختلاف میانگین رمزگیری (سرقت هویت و اطلاعات) با عدد ۳ مثبت می‌باشد. همچنین بر اساس t به‌دست‌آمده (۲,۴۹۵) در درجه آزادی ۹۳ ، تفاوت معناداری بین میانگین رمزگیری (سرقت هویت و اطلاعات) و میانگین نظری

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

وجود دارد. بنابراین میزان رمزگیری (سرقت هویت و اطلاعات) در بانک‌های موردمطالعه در سطح بالایی است (تائید فرضیه فرعی سوم).

بر اساس جدول ،اختلاف میانگین کلاه‌برداری اینترنتی با عدد ۳ مثبت می‌باشد .همچنین بر اساس t به‌دست‌آمده (۷,۵۱۶) در درجه آزادی ۹۳ ، تفاوت معناداری بین میانگین کلاه‌برداری اینترنتی و میانگین نظری وجود دارد. بنابراین میزان کلاه‌برداری اینترنتی در بانک‌های موردمطالعه در سطح بالایی است (تائید فرضیه فرعی چهارم).

.بر اساس جدول اختلاف میانگین اختلال (یا تخریب) سامانه‌های الکترونیکی با عدد ۳ مثبت می‌باشد. همچنین بر اساس t به‌دست‌آمده (۲,۰۵۵) در درجه آزادی ۹۳ ، تفاوت معناداری بین میانگین اختلال (یا تخریب) سامانه‌های الکترونیکی و میانگین نظری وجود دارد. بنابراین میزان اختلال (یا تخریب) سامانه‌های الکترونیکی در بانک‌های موردمطالعه در سطح بالایی است (تائید فرضیه فرعی پنجم).

بر اساس جدول ،اختلاف میانگین افشای اطلاعات و حریم خصوصی با عدد ۳ منفی می‌باشد. همچنین بر اساس t به‌دست‌آمده (۳,۵۱۵-)در درجه آزادی ۹۳، تفاوت معناداری بین میانگین افشای اطلاعات و میانگین نظری وجود دارد. بنابراین میزان افشای اطلاعات و حریم خصوصی در بانک‌های موردمطالعه در سطح پایینی است (عدم تائید فرضیه فرعی ششم).

۵-۴-اولویت‌بندی مؤلفه‌های متغیرهای تحقیق

در این بخش با استفاده از آزمون فریدمن، مؤلفه‌های متغیرهای تحقیق)بودجه‌ریزی عملیاتی(را از نظر اولویت و اهمیت رتبه‌بندی می‌نماییم. نتایج آزمون فریدمن در ادامه تشریح شده است:

جدول ۵- نتایج آزمون فریدمن در خصوص اولویت‌بندی انواع جرائم اینترنتی

مؤلفه	رتبه میانگین	رتبه
تقلب در کارت اعتباری و انتقال وجه	۴,۷۱	۱
جعل پول الکترونیکی	۲,۶۷	۵
رمزگیری	۳,۵۹	۳
کلاه‌برداری اینترنتی	۴,۳۰	۲
اختلال (یا تخریب)	۳,۴۶	۴
افشای اطلاعات و حریم خصوصی	۲,۲۸	۶
آمار خی دو: ۱۲۲,۷۸ (۰,۰۰۱)		

بنابراین در سطح خطای ۵ درصد، تمایز معناداری بین شاخص‌های جرائم اینترنتی بانکداری اینترنتی در بانک وجود دارد. همچنین با توجه به ستون رتبه میانگین‌ها ملاحظه می‌شود که تقلب در کارت اعتباری و انتقال وجه الکترونیکی با رتبه میانگین ۷۱/۴ بیشترین سهم را در جرائم اینترنتی بانکداری الکترونیکی؛ و افشای اطلاعات و حریم خصوصی با رتبه میانگین ۲۸/۲ کمترین سهم را در جرائم اینترنتی بانکداری الکترونیکی دارد.

۶-نتیجه‌گیری

به نظرمی رسد، ادعای عدم امکان صیانت از داده‌های خصوصی در اینترنت، صرفاً برای رفع تکلیف از سازندگان و گردانندگان شبکه‌های ارتباطی ابزار می‌شود . باوجود این طرز تلقی که حفظ حریم خصوصی در فضای مجازی غیرممکن است، قانون جرائم رایانه‌ای در اقدامی که نشان می‌دهد، این قانون درصدد حمایت جدی از داده‌های شخصی می‌باشد؛ برای افشای داده‌های

ماهنامه علمی تخصصی پایا شهر

ISSN ۲۹۸۰-۷۷۸۶

خصوصی در فضای مجازی، مجازات تعیین کرده است. به‌موجب ماده ۱۷ این قانون هر کس به‌وسیله سیستم‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به‌نحوی‌که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد». افشای اطلاعات خصوصی، ممکن است به دلیل نقص سهوی یا عمدی در طراحی مرورگرهایی باشد که برای شبکه جهانی (اینترنت)یا شبکه‌های خصوصی طراحی می‌شوند.

گفته می‌شود، اغلب مرورگرهای امروزی اطلاعاتی از کاربران خود را به سازندگان خود ارسال می‌کنند .فایرفاکس، اکسپلورر، کروم، سافاری و ...ازجمله مرورگرهای معروفی هستند که اطلاعاتی از حریم خصوصی کاربران خود را به دست سازندگان خود می رسانند . این اطلاعات در تبلیغات متناسب با ذائقه ی او استفاده شود . برنامه هایی هم برای خنثی کردن کارکرد جاسوسی مرورگرها ارایه و بازاریابی شده، ۳ که ممکن است خود، ابزار جاسوسی باشند.

درنهایت پیشنهادات زیر ارائه می‌شود:

۱-در راستای فرضیه اول پیشنهاد می‌شود که برای کاهش تقلب در کارت های اعتباری و انتقال وجه الکترونیکی، رمز پویا یک بار مصرف متناظر با روش های پیشرفته ریاضی تولید گردد.

۲-در راستای فرضیه دوم پیشنهاد می‌شود علیرغم اینکه میزان جعل پول کم است اما باید دستگاه‌های الکترونیکی و نرم‌افزاری هوشمند تولید شود و در دسترس عموم قرار گرفته شود.

۳-در راستای فرضیه سوم پیشنهاد می‌شود که برای امنیت بالا در حوزه هویت و سرقت اطلاعات کاربران می بایست نرم‌افزارهایی در حوزه بانکداری الکترونیکی دارای ضریب امنیت بالایی طراحی کرد که کمتر مورد هکر قرار گیرند.

۴-در راستای فرضیه چهارم پیشنهاد می‌شود که درگاه های انتقال وجه دارای شناسه معین و مشخصی باشند و این ویژگی‌ها به عموم کاربران نشان داده شوند و راهنمایی‌ها در این خصوص ارائه داده شود.

۵-در راستای فرضیه پنجم پیشنهاد می‌شود سامانه‌های الکترونیکی و نرم‌افزارهای الکترونیکی بانکی دارای ضریب امنیت بالایی ساخته بشود که کمتر مورد هک قرار گیرند.

در فرآیند انجام فعالیت‌های پژوهشی معمولاً موانع، مشکلات و محدودیت‌هایی وجود دارد. چنانچه محقق بتواند بر این‌گونه محدودیت‌ها فائق آید، آنگاه نتایج تحقیق با دقت و اطمینان بیشتری به دست خواهد آمد. این پژوهش نیز از این قاعده مستثنی نبوده است. لذا این تحقیق به‌طور ناخواسته با محدودیت‌هایی مواجه بوده است.

- با توجه به این قلمرو مکانی تحقیق، بانک‌ها در استان کهگیلویه و بویراحمد بوده است لذا تعمیم نتایج به سایر بانک‌ها باید با جنبه احتیاط باشد.
- با توجه به قلمرو زمانی اجرای و گردآوری داده‌های تحقیق و وضعیت جرائم اینترنتی موجود، نمی توان بدون رعایت جنبه احتیاط نتایج حاصل را به سایر دوره های زمانی تعمیم داد.

مراجع

۱. جوینده، مصطفی،۱۳۹۴،بررسی جرایم اینترنتی در سیستم بانکداری الکترونیک،اولین کنفرانس بین المللی یافته های نوین علوم و تکنولوژی،تهران،https://civilica.com/doc/۴۳۳۰۰۷

۲. شاهرخی فخرآباد ، زینت (۱۳۹۲)" بررسی تاثیر امنیت و حریم خصوصی بر اعتماد و تعهد مشتریان در بانکداری اینترنتی(مورد مطالعه:اینترنت بانک ملت در شهر مشهد)" پایانامه کارشناسی ارشد، دانشگاه فردوسی مشهد .

ISSN ۲۹۸۰-۷۷۸۶

۳. علیزاده, رامین, غلامی, حسین & ,جاهد, محمدعلی. (۱۳۹۸). پیشگیری از جرائم بانکی از طریق اعمال ضوابط حاکمیت شرکتی .*دانشنامه حقوق اقتصادی*۱۶,۷۵۳۵۴/le.v۲۶i۱۶,۷۵۳۵۴ :doi .۱۰۸-۷۷ ,(۱۵)۲۶ ,

۴. قریشی محمدی, فاطمه السادات. (۱۴۰۱). جرایم بانکی در فضای مجازی در حقوق ایران و اسناد بین‌المللی .*فقه جزای تطبیقی*۱۲۳۳,۳۹۰۰۱۳,۲۰۲۳.jccj/۱۰,۲۲۰۳۴ :doi .۵۴-۴۵ ,(۳)۲ ,

۵. Cristi, Oliver., & John. Moore. (۲۰۲۰). “A theory of debt based on the inalienability of human capital”, quarterly journal of economics.

٦. Frank, R (۲۰۱۱). Encyclopedia of Criminology and Deviant Behavior. Vol.II, Brunnner-Routledge /Taylor and Francis Publishers

۷. Henry S. Warren ،Hacker's Delight ،Addison Wesley Publishing،-۲۰۱۸

۸. Shreeram, M.Suban, P.Shanthi, K.Manjula “Anti-phishing detection of phishing attacks using genetic algorithm” in proceedings of Communication control and computing technology(ICCCCT),IEEE international conference, Ramanathapuram , pages ٤٤٧-٤٥٠, ٢٠١٥

۹. Simmons, B, (۲۰۱۸). "Money and the Law: Why empty with the Public International Law of Money?”. Yale Journal of International Law, ۳۲۳-۳۲٦.

۱۰. Snell, S. A & Bohlander, G. W. (۲۰۱۷). Managing Human Resources. Thomson Publishing Company. .