Management of Information Resources & Services

Print ISSN: 2383-1049
Online ISSN: 2538-5356

User Information Security Behavior in Virtual Professional Communities Based on Technology Threat Avoidance Approach

Document Type: Research Paper

Faramarz Soheili
***Corresponding author:** Associated Professor, Department of Knowledge and Information Science, Payame Noor University, Tehran, Iran. E-mail: fsohieli@gmail.com

Aliakbar Khasseh
Associated Professor, Department of Knowledge and Information Science, Payame Noor University, Tehran, Iran. E-mail: khasseh@gmail.com

Farhad Shariat
MSc, Department of Knowledge and Information Sciences, payame Noor University, Tehran, Iran. E-mail: f.shariat1394@gmail.com

Abstract

Purpose: The purpose of this study was to determine the information security behavior of users in professional virtual communities based on Islamic Azad University, Kermanshah Branch.

Methodology: The method of the present study was descriptive-correlational. The statistical population of this study was faculty members of Islamic Azad University of Kermanshah, which was selected data. Descriptive statistics, Pearson correlation matrix and structural equation test were used to analyze the data using SPSS and Amos software.

Findings: The results indicated that the variables "Safeguarding Measure Cost", "Perceived Susceptibility", "Perceived Severity", "Information Security Knowledge Sharing" and "Information Security Experience" had a positive and significant relationship with users' "Avoidance Behavior". On the other hand, the variable "Avoidance Motivation" as a mediating dependent variable had a positive and significant relationship with "Avoidance Behavior". Also, the fit of the model showed that the proposed conceptual model was very useful.

Conclusion: The results of the research showed that it is necessary for the planners and trustees of information protection in organizations to provide necessary and continuous training for people to better understand information protection against various threats. Therefore, it is necessary to pay more attention to various factors, including sharing knowledge and experience of people and creating a safe environment for trust between people. On the other hand, awareness and understanding of the types of threats and the nature of each of them will lead to keeping organizations healthy and progressing.

Keywords: Information Behavior, Information Security, Professional Virtual Communities, Technology Threat Avoidance Approach.

Citation: Soheili, F., & Khasseh, A., Shariat, F. (2022). User Information Security Behavior in Virtual Professional Communities Based on Technology Threat Avoidance Approach. *Management of Information Resources & Services*, 9(1), (25-40). (In Persian)

(DOI): 10.30473/MRS.2022.63943.1516
Quarterly Journal of Management of Information Resources & Services
Vol 9, No 1, (Series 33), Spring 2022, (25-40)
Received: (2022/05/07)
Accepted: (2022/09/19)

مدیریت منابع و خدمات اطلاعاتی

شاپا چاپی: ۲۳۸۳-۱۰۴۹
شاپا الکترونیکی: ۲۵۳۸-۵۳۵۶

رفتار امنیت اطلاعاتی کاربران در جوامع مجازی حرفه‌ای براساس رویکرد اجتناب از تهدید فناوری

نوع مقاله: پژوهشی

فرامرز سهیلی
***نویسنده مسئول:** دانشیار، گروه علم اطلاعات و دانش‌شناسی، دانشگاه پیام نور، تهران، ایران. E-mail: fsohieli@gmail.com

علی‌اکبر خاصه
دانشیار، گروه علم اطلاعات و دانش‌شناسی، دانشگاه پیام نور، تهران، ایران. E-mail: khasseh@gmail.com

فرهاد شریعت
کارشناس ارشد، گروه علم اطلاعات و دانش‌شناسی، دانشگاه پیام نور، تهران، ایران. E-mail: f.shariat1394@gmail.com

چکیده

هدف پژوهش: هدف از این پژوهش، تعیین رفتار امنیت اطلاعاتی کاربر در جوامع مجازی حرفه‌ای براساس رویکرد اجتناب از تهدید فناوری در بین اعضای هیئت‌علمی دانشگاه آزاد اسلامی واحد کرمانشاه بود.

روش کار پژوهش : روش پژوهش حاضر از نوع توصیفی- همبستگی است. جامعه آماری این پژوهش اعضای هیئت‌علمی دانشگاه آزاد اسلامی واحد کرمانشاه بود که با استفاده از فرمول کوکران و به روش نمونه‌گیری تصادفی ساده ۱۶۲ نفر انتخاب گردید. ابزار گردآوری داده‌ها پرسشنامه استاندارد بود. جهت تحلیل داده‌ها از شاخص‌های آماری توصیفی، ماتریس همبستگی پیرسون و آزمون معادلات ساختاری با استفاده از نرم‌افزار اس. پی. اس. اس. و آموس استفاده شد.

یافته‌ها: یافته‌های پژوهش نشان داد متغیرهای هزینه‌های امنیتی و حفاظتی در مقابل تجربه امنیت اطلاعات رابطه مثبت و معناداری وجود دارد، همچنین متغیرهای هنجارهای گروه و خودکار کارآمدی رابطه مثبت و معناداری با رفتار اجتنابی دارد. همچنین برازش مدل نشان داد که مدل مفهومی ارائه شده از مطلوبیت خوبی برخوردار بود.

بحث و نتیجه‌گیری: نتایج پژوهش نشان داد که برنامه‌ریزان و متولیان حفاظت اطلاعات در سازمان‌ها، ضروری است که آموزش‌های لازم و مستمر جهت درک بهتر افراد از حفاظت اطلاعات در برابر تهدیدات مختلف سرلوحه کار خود قرار دهند ازاین‌رو ضروری است به عوامل مختلفی اعم به اشتراک گذاری دانش و تجربه افراد و ایجاد محیطی امن جهت اعتماد بین افراد توجه بیشتری شود که این امر می‌تواند به‌عنوان راهکارهای ارزشمندی برای هر سازمان باشد. از طرفی، آگاهی و شناخت نسبت به انواع تهدیدها و ماهیت هرکدام از آن‌ها، منجر به سالم نگه‌داشتن سازمان‌ها و پیشرفت آن‌ها خواهد شد.

واژه‌های کلیدی: رفتار اطلاعاتی امنیت اطلاعات، جوامع مجازی حرفه‌ای، رویکرد اجتناب از تهدید فناوری.

استناد: سهیلی، فرامرز و خاصه، علی اکبر و شریعت، فرهاد (۱۴۰۱). رفتار امنیت اطلاعاتی کاربران در جوامع مجازی حرفه‌ای براساس رویکرد اجتناب از تهدید فناوری. *مدیریت منابع و خدمات اطلاعاتی*، ۹(۱)، (۲۵-۴۰).

(DOI): 10.30473/MRS.2022.63943.1516
فصلنامه مدیریت منابع و خدمات اطلاعاتی
سال نهم، شماره اول، (پیاپی ۳۳)، بهار ۱۴۰۱، (۴۰-۲۵)
تاریخ دریافت: (۱۴۰۱/۰۲/۱۷)
تاریخ پذیرش: (۱۴۰۱/۰۶/۲۸)

مقدمه

جوامع مجازی[1] در سال‌های اخیر به‌عنوان پدیده‌ای فزاینده در میان کاربران اینترنتی، توجه زیادی را به خود جلب کرده‌اند. بسیاری از کاربران اکنون هویت خود را در دنیای دیجیتال شکل می‌دهند و فاش می‌کنند، زیرا اطلاعات را ایجاد، توزیع و تبادل می‌کنند؛ همچنین با افزایش مجازی‌سازی سازمان‌ها، کار از مرزهای فیزیکی فراتر رفته زیرا کارکنان شرکت‌ها نیز می‌توانند از دفاتر مجازی کار کنند. (نور فسین و محدوی،[2] ۲۰۱۵)، یک جامعه مجازی حرفه‌ای به یک نهاد انسان‌محور اشاره دارد که برای به حداکثر رساندن تحقق کارکنان دانشی و بهترین پشتیبان از نوآوری در یک محیط مجازی طراحی شده است (اسلام[3] ۲۰۱۸)، بنابراین جوامع مجازی فضای پیوسته ثابتی هستند که در آن کاربران تعامل حرفه‌ای و اجتماعی در حال پیشرفت را تجربه می‌کنند. در این راستا، ندری و بخشایش تأکید می‌کنند که شناخت پیامدهای امنیتی ناشی از گسترش روزافزون شبکه‌های اجتماعی مجازی، از یک‌سو، مستلزم شناخت سطوح مختلف این آثار و از سوی دیگر آگاهی یافتن از سازوکارهای چگونگی شکل‌گیری فرصت‌ها و تهدیداتی است که در نهایت جامعه را با انواع چالش‌ها روبه‌رو می‌سازد (نادری و بخشایش، ۲۰۲۰)، بنابراین امنیت اطلاعات[4] زمینه‌ای برای افراد حرفه‌ای فراهم می‌کند تا دانش خود و مهارت‌ها را بدون محدودیت‌های جغرافیایی به اشتراک بگذارند (بیفولکو و سنتورو،[5] ۲۰۰۵)، هم‌زمان با گسترش استفاده از رایانه‌های شخصی، گوشی‌های هوشمند و تبلت‌ها و مطرح شدن شبکه‌های رایانه‌ای و به دنبال آن اینترنت، حیات این ابزار الکترونیکی و کاربران آنان دستخوش تغییرات اساسی شده است. استفاده‌کنندگان از رایانه‌ها و وسایل ارتباطی به‌منظور استفاده از دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مؤلفه‌های تأثیرگذار در تداوم ارائه خدمات و امنیت اطلاعات در یک سیستم رایانه‌ای می‌باشند. حال با گسترش این فضا برخی افراد فرصت‌طلب با نفوذ در وب‌سایت‌ها سعی در سرقت اطلاعات شخصی افراد دارند، برخی دیگر با ایجاد صفحات جعلی درگاه‌های پرداخت بانک‌ها در پی سرقت اطلاعات کارت‌های بانکی افراد هستند. از همین رو نیاز است تا یک کاربر به امنیت در فضای مجازی توجه داشته باشد (ویکی‌پدیا،[6] ۲۰۲۱). با توجه به گسترش فناوری‌ها و حضور روزافزون افراد و شرکت‌های دولتی و خصوصی در این بستر الکترونیکی، این امر موجب نگرانی بیشتر و سازمان‌دهی آگاهانه برای امنیت اطلاعات برای توسعه مؤثر و اقتصادی است. امروزه این امکان وجود دارد که جوامع مجازی حرفه‌ای هدف حملات سایبری قرار گیرند. افراد کلاهبردار اغلب از این فضا برای شروع حملات دیجیتالی استفاده می‌کنند. با وجود این، بسیاری از کاربران با شیوه‌های غیرایمن به مشارکت در اجتماعات مجازی ادامه می‌دهند. با توجه به اهمیت مسئله، مایکروسافت نیز چندین مطالعه رفتار امنیت اطلاعات کاربر در برابر تهدیدهای امنیتی را انجام داده است (یودیتیما[7]، ۲۰۱۹)، گرچه مطالعات قبلی بیشتر بر درک استفاده از رایانه‌های خانگی در سازمان‌ها و خطرات امنیتی مرتبط با آن‌ها تمرکز داشته است و کاربرد آن‌ها و انطباق آن در سازمان‌ها و خطرات امنیتی مرتبط با آن مورد بررسی قرار داده است اما در همه آن‌ها به‌طور کلی تهدیدات امنیتی در رسانه‌های اجتماعی تأیید شده است.

عامل مهم در امنیت اطلاعات عامل انسانی می‌باشد که رفتار امنیت اطلاعاتی کاربر در جوامع مجازی را شامل می‌شود؛ و اینکه چه افرادی امکان تغییر در این داده‌ها را دارند؟ کانون توجه نفوذگران، سهل‌انگاری و ساده‌اندیشی کاربران است. بنابراین، کاربران باید با افزایش خودکارآمدی در امنیت اطلاعات و افزایش دانش خود این خلأ را پرکرده و هزینه‌های حفاظتی و افشای اطلاعات را کاهش دهند و با این حساسیتی که در حفاظت اطلاعات از خود نشان می‌دهند مانعی برای تهدیدهای فناوری داشته باشند (جانسن[8] و همکاران، ۲۰۱۴)، با توجه به مطلب فوق، عوامل چندی در کاهش امنیت اطلاعات افراد در فضای مجازی دخیل می‌باشد که یکی از مهم‌ترین آن‌ها عدم دانش و مهارت‌های شخصی کاربر در استفاده از این جوامع است و هرچقدر خودکارآمدی فردی و دانش استفاده از این فضای مجازی در افراد بالاتر باشد تهدیدهای فناوری به نسبت پایین‌تر خواهد آمد و کاربران با اشتراک‌گذاری دانش امنیت اطلاعات در جوامع مجازی دانش استفاده و وارد شدن به جوامع مجازی را به سایر کاربران انتقال می‌دهند (سمتانی و

1. Virtual communities
2. Noor, Fasin &Mahdavi
3. Aslam
4. Information security
5. Bifulco & Santoro
6. Wikipedia
7. yudatama
8. Jansen

همکاران[1]، ۲۱۷). هرچقدر دانش و مهارت کاربران توسعه یابد نکات امنیتی بیشتر رعایت خواهد شد که نتیجه آن کاهش تهدیدهای امنیتی برای کاربران و حتی سازمان‌ها خواهد شد. علاوه‌بر این، با ظهور اینترنت و به دنبال آن فضای مجازی، هنجارهایی جدید پدید آمده‌اند که مخصوص پیام‌رسان‌ها و شبکه‌های اجتماعی است که رعایت این هنجارها می‌تواند از تهدیدهای فناوری اطلاعات جلوگیری نماید و یا از تأثیر آن بکاهد، (فرزمند، مشایخ و همسایی[2]، ۲۰۱۲). در این راستا لازم است که کاربران و حتی سازمان‌ها برای حفاظت از اطلاعات ارزشمند خود، به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی را اجرا نماید. نبود نظام مناسب امنیتی، بعضاً پیامدهای منفی و دور از انتظاری را به دنبال دارد. توفیق در ایمن‌سازی اطلاعات، منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات است؛ بدین منظور از سرویس‌های امنیتی متعددی استفاده می‌گردد. سرویس‌های انتخابی باید پتانسیل لازم در خصوص ایجاد یک سیستم حفاظتی مناسب، تشخیص به‌موقع حملات و واکنش سریع را داشته باشند. بنابراین حفاظت مطمئن، تشخیص به‌موقع و واکنش مناسب، ازجمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت شود، (گرین فلد و همکاران، ۲۰۱۴[3]).

با وجود پژوهش‌های اندکی که در این مورد در ایران صورت گرفته و از طرفی تاکنون پژوهشی در مورد نقش رفتار امنیت اطلاعات کاربر در جامعه اعضای هیئت‌علمی صورت نگرفته است؛ لذا این پژوهش می‌تواند خلأ اطلاعاتی در موضوع را تا حدی کامل کند. نقش رفتار امنیت اطلاعات کاربر (خودکارآمدی، هزینه اقدام حفاظتی، حساسیت درک شده، تهدید فناوری اطلاعات، اشتراک‌گذاری دانش امنیت اطلاعات)، هنجارهای گروه که به گفته آلبرت باندورا[4]، خودکارآمدی را به‌عنوان «باور شخص به موفقیت در یک موقعیت خاص یا انجام یک وظیفه است.» حس خودکارآمدی می‌تواند نقش مهمی در رسیدن به اهداف، انجام وظایف و فائق آمدن بر چالش‌ها داشته باشد. با خودکارآمدی می‌توان برای برنامه‌های و اهداف سازمان برنامه‌ریزی کرد و با کنترل هزینه اقدامات حفاظتی منابع سازمانی را که در اختیار سازمان قرار دارد را مدیریت نماید و در راستای منافع سازمان و توسعه خدمات اقدام نماید و حساسیت‌های سازمان را کاهش دهد. حساسیت درک شده در سازمان این امکان را فراهم می‌کند که نقاط ضعف و قوت را شناسایی و براساس اولویت‌هایی موجود آن‌ها را بررسی و رفع یا توسعه دهد و تهدیدهای مخربی را که فناوری‌های درک شده در سازمان را هدف می‌گیرد شناسایی نماید. تهدیدهای فناوری می‌تواند اطلاعات سازمان را در خطر قرار دهد و برای جلوگیری از به خطر افتادن اطلاعات سازمان باید دانش امنیت اطلاعات را در سازمان به اشتراک بگذارند که کل سازمان بتوانند از آن استفاده نمایند. از طرف دیگر، کارکنان نیز تجربیات خود را درزمینهٔ امنیت اطلاعات اشتراک‌گذاری می‌کنند که در نهایت می‌تواند به‌عنوان هنجارهای گروهی سازمان قرار گیرد. یکی از عواملی که بر رفتارهای امنیت اطلاعاتی نقش داشته باشد موضوع انگیزه‌های اجتناب است. انگیزه اجتناب یا انگیزه حفاظتی متغیری است که ویژگی‌های معمول یک انگیزه را دارد. به عبارتی، فعالیت را برمی‌انگیزد، حفظ و هدایت می‌کند (روگرز[5]، ۱۹۸۵). همچنین در توضیح بیشتر انگیزه اجتناب اظهار می‌کند که انگیزه اجتناب متغیری که باعث تغییر رفتار می‌شود. همچنین جان استون و (وارکنتین[6]، ۲۰۱۰). ادعا کردند که وقتی ارزیابی تهدید و ارزیابی مقابله در سطوح متوسط تا بالا باشد، انگیزه حفاظتی افراد به یک اندازه افزایش می‌یابد، در نتیجه بر رفتار واقعی تأثیر بسزایی می‌گذارد. یا (پوسی[7]، ۲۰۱۵). این ادعا دارد که تأثیر انگیزه اجتنابی/حفاظتی بر رفتار نه‌تنها قابل توجه است بلکه مثبت نیز است سیتد (این جیویتی[8]، ۲۰۱۹)؛ لذا، در این پژوهش تلاش می‌شود تا رفتار امنیت اطلاعاتی کاربر در جوامع مجازی حرفه‌ای براساس رویکرد اجتناب از تهدید فناوری در بین اعضای هیئت‌علمی علمی دانشگاه آزاد اسلامی واحد کرمانشاه مورد کنکاش قرار گیرد. در همین راستا فرضیه‌های زیر در معرض آزمون قرار می‌گیرد:

- حساسیت درک شده رابطه مثبتی با انگیزه اجتناب از تهدید فناوری دارد.
- هزینه اقدام حفاظتی رابطه مثبتی با انگیزه اجتناب از تهدید فناوری دارد.

1. Samtani & et al
2. Farazmand, Mashayekh & Hesami
3. Greenfield & et al
4. Albert Bandura
5. Rogers
6. Johnston & Warkentin
7. Posey
8. Cited in: Giwah

- شدت تهدیدهای مخرب فناوری درک شده رابطه مثبتی با انگیزه اجتناب از تهدید فناوری دارد.
- به اشتراک‌گذاری دانش امنیت اطلاعات رابطه مثبتی با انگیزه اجتناب از تهدید فناوری دارد.
- تجربه امنیت اطلاعات رابطه مثبتی با انگیزه اجتناب از تهدید فناوری دارد.
- هنجارهای گروه رابطه مثبتی با رفتار اجتنابی فناوری اطلاعات دارد.
- خودکار کارآمدی رابطه مثبتی با رفتار اجتنابی فناوری اطلاعات دارد.
- انگیزه اجتناب رابطه مثبتی با رفتار اجتنابی فناوری اطلاعات دارد.

پیشینه پژوهش

تاکنون پژوهش‌های چندی به مبحث امنیت اطلاعات و یا جوامع مجازی پرداخته‌اند. به‌عنوان نمونه (کیخیا[1]، ۲۰۱۸)، عوامل اعتماد بین فردی مؤثر بر رفتار اشتراک دانش در جوامع مجازی را مورد بررسی قرار داد و نشان داد که اعتماد بین فردی به میزان قابل‌توجهی قصد اشتراک دانش را در بین کاربران جوامع مجازی تحت تأثیر قرار می‌دهد و عواملی مانند توانایی، خیرخواهی، صداقت، قابل پیش‌بینی بودن، شایستگی، دیدگاه مشترک، رشد دانش و ایجاد و شرکت در ارتباطات شخصی همگی بر افزایش اعتماد بین فردی اعضای مجازی تأثیر مثبت دارند (یوسفی، حسن‌پور و موسوی، ۲۰۱۵). در پژوهشی به بررسی ارائه مدلی جهت اولویت‌بندی ریسک‌های امنیت اطلاعات سازمانی با استفاده از نرم‌افزار AHP فازی و شبکه بیزین در صنعت بانکداری پرداخت. یافته‌های این پژوهش نشان می‌دهد در سازمان مورد پژوهش، ریسک عدم آگاهی و عدم ارائه آموزش‌های مناسب در حوزه امنیت اطلاعات، بالاترین اولویت و بیشترین نیاز به توجه را دارد. (یوسفی، حسن‌پور و موسوی، ۲۰۱۵). همچنین در پژوهشی به بررسی شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری پرداختند. آن‌ها الگویی براساس استاندارد ایزو و چارچوب کوبیت شناسایی کردند که شامل شش شاخص و زیرشاخص ریسک امنیت اطلاعات سازمانی برای بانک بود.

در خارج از ایران، پژوهش‌های بیشتری بر روی مقولهٔ امنیت اطلاعات و جوامع مجازی انجام شده است. در یکی از این پژوهش‌ها (شامالا و همکاران[2]، ۲۰۱۷). در پژوهشی به بررسی یکپارچه‌سازی ابعاد کیفی اطلاعات در امنیت اطلاعات مدیریت ریسک پرداختند. نتایج پژوهش نشان داد که توجه به روند فعلی انتقال اطلاعات از طریق یک جهان بدون مرز و آسیب‌پذیر، امنیت اطلاعات تبدیل به یک نهاد مهم برای اکثر سازمان‌ها می‌شود. این به سازمان‌دهی نگرانی و آگاهی بیشتر برای استفاده از مدیریت ریسک امنیت اطلاعات برای ایجاد استراتژی‌های کنترل مؤثر و اقتصادی می‌پردازد. در یکی از مرتبط‌ترین پژوهش‌ها (فورستر[3]، ۲۰۱۹). رفتار امنیت اطلاعات کاربر در انجمن‌های مجازی حرفه‌ای را مورد بررسی قرار داد. نتایج پژوهش نشان داد عامل مهم در امنیت اطلاعات عامل انسانی می‌باشد که رفتار امنیت اطلاعاتی کاربر در جوامع مجازی را شامل می‌شود. اطلاعات و دانش کارکنان و استفاده‌کنندگان از فضای مجازی هرچقدر که بیشتر باشد امکان لو رفتن اطلاعات و یا سرقت اطلاعات کمتر می‌گردد. (کارجلالیان، سیپونن و سارکر[4]، ۲۰۲۰)، در پژوهشی با عنوان توسعه رفتارهای امنیتی اطلاعات کارمندان در شرکت‌های چندملیتی پرداختند. نتایج این پژوهش نشان داد نقش اصلی فناوری اطلاعات و فناوری اطلاعات، امنیت اطلاعات را به‌عنوان نگرانی اصلی سازمان‌ها تبدیل کرده است. یکی از مباحث مشخص شده در ادبیات امنیت اطلاعات به‌اصطلاح رفتاری، مربوط به این است که چرا کارمندان از روش‌های امنیتی اطلاعات سازمانی خود (ISP) پیروی می‌کنند یا آن را نقض می‌کنند.

به‌طور کلی و با توجه به نتایج پیشنه‌های پژوهش می‌توان نتیجه گرفت که رفتار اجتناب از تهدیدهای فناوری شاید پرهزینه و وقت‌گیر به نظر آید اما با توجه به اهمیت اطلاعات در بقای سازمان وجود چنین سیستمی بسیار ضروری می‌نماید. اعمال چنین سیستمی برای هر سازمان لازم بوده و بسته به سطح اطلاعات و ارزش اطلاعات سازمان گستردگی متنوعی خواهد داشت اما هرگز محو نخواهد شد. مهم‌ترین مؤلفه هر برنامه امنیتی مؤثر، افرادی هستند که آن را اجرا و مدیریت می‌کنند. نقایص امنیتی بیش از آنکه ناشی از سیستم باشند، به‌وسیله افرادی که مدیریت

1. Keikha

2. Shamala & et al
3. Forrester
4. Karjalainen, Siponen & Sarker

سیستم را بر عهده دارند و کاربران سیستم رخ می‌دهند. بیشتر مطالعات گذشته نشان داده‌اند تهدیدهای داخلی سیستم‌ها الکترونیک اغلب بسیار مهم‌تر از تهدیدهای خارجی بوده‌اند. در بسیاری از موارد مجرمانی که در نفوذ به سیستم بوده‌اند یا دانش قبلی از سیستم داشته‌اند و یا شریک جرمی در داخل شرکت می‌باشند. به‌طور کلی نتایج پیشینه‌ها نشان می‌دهد که عوامل مختلف داخلی و خارجی موجب تهدید امنیت اطلاعات در جوامع مجازی می‌شود که نیازمند بررسی و تحلیل بیشتر آن در جوامع و زمان‌های مختلف و همچنین براساس فناوری‌های اطلاعاتی و ارتباطی جدید است.

روش کار پژوهش

روش کار پژوهش حاضر توصیفی از نوع همبستگی است. در این پژوهش از پرسشنامه (فورستر[1]، ۲۰۱۵). برای گردآوری داده‌ها استفاده گردید. در این پرسشنامه از مؤلفه‌های مختلفی استفاده شده است که هریک پرسشنامه جداگانه‌ای دارند. به بیان دقیق‌تر، برای متغیر خودکارآمدی از پرسشنامه کامپیوتر و هیگنس[2]، (۱۹۹۶) متغیر حفاظت از هزینه از پرسشنامه فرین و همکاران[3]، (۱۹۹۱)، متغیر حساسیت درک شده از پرسشنامه لینگ و ایکسیو[4]، (۲۰۱۰). متغیر درک شدت تهدیدهای مخرب فناوری از پرسشنامه نگ و همکاران[5]، (۲۰۰۹). متغیر اشتراک‌گذاری دانش امنیت اطلاعات از پرسشنامه هسیو و همکاران[6]، (۲۰۰۷). متغیر تجربه امنیت اطلاعات از پرسشنامه کل[7]، (۲۰۱۱). متغیر هنجارهای گروه از پرسشنامه زنگ و همکاران[8]، (۲۰۰۹). متغیر انگیزه اجتناب از پرسشنامه لینگ و ایکسیو[9]، (۲۰۱۰) و برای متغیر رفتار اجتنابی از پرسشنامه لینگ و ایکسیو، (۲۰۱۰). استفاده شده است. به‌منظور تعیین روایی سازه پرسشنامه، از تحلیل عاملی اکتشافی متغیرها استفاده و در چهار مرحله اصلی گزارش داده شد. مرحله اول تحلیل عاملی این است که آیا بر روی داده‌های گردآوری شده امکان تحلیل عاملی وجود دارد یا خیر؟ بدین منظور، ابتدا کفایت نمونه‌گیری براساس آزمون کیسر–مایر – الکین و کرویت و بارتلت[10] به شرح جدول ۲ نشان داده شده است. نتایج این تجزیه و تحلیل در جدول ۱ و جدول ۲ نشان داده شده است.

جدول ۱. آزمون کیسر–مایر – الکین و کرویت بارتلت

کفایت نمونه‌گیری کیسر–مایر – الکین	۰/۷۱
کای اسکوئر (x^2)	۵۶۴۶/۷۹
آزمون کرویت بارتلت ده آزادی	۵۹۵
سطح معناداری	۰/۰۰۰

همان‌طور که در جدول ۱ ملاحظه می‌شود، ملاک کفایت نمونه‌گیری کیسر–مایر الکین ۰/۷۱۹ بود که نشان‌دهنده مناسب بودن حجم داده‌ها برای تحلیل مؤلفه‌های اصلی است. همچنین نتیجه آزمون کرویت بارتلت نیز از نظر آماری معنادار بود (x^2 =۵۶۴۶/۷۹۸ و P<۰/۰۰۰). از آنجایی که مقدار شاخص کفایت نمونه بیشتر از ۰/۵ است، لذا می‌توان تحلیل عاملی به روش مؤلفه‌های اصلی را در مورد این مؤلفه‌ها اجرا کرد. مرحله دوم تحلیل عاملی، شناخت سهم مجموعهٔ عامل‌ها در تبیین واریانس هر گویه است که با عنوان اشتراکات مشخص شده است. جدول ۲ آن را نشان می‌دهد.

می‌توان نتیجه گرفت که کوواریانس موجود بین آیتم‌های طرح شده برای سنجش سازه‌های اصلی پژوهش به‌اندازه کافی برای استخراج حداقل یک عامل کافی است.

1. Forrester
2. Compeau &Higgins
3. Fruin & et al
4. Liang & Xue
5. Ng & et al
6. Hsu & et al
7. Claar
8. Zeng & et al
9. Liang & Xue

10. Kasier-Meyer-Olkin Measure of Sampling (KMO, & Bartlett's Test of Sphericity)

جدول ۲. اشتراکات گویه‌های عوامل

سؤال	شرح سؤال	مقدماتی	استخراج [1]
۹	مراجعه به فضاری مجازی، رایانه من را آلوده می‌کند	۱/۰۰۰	۰/۶۵۳
۶	فعال کردن اقدامات امنیتی سهولت کار در فضای مجازی راکم می‌کند	۱/۰۰۰	۰/۸۸۰
۱۰	هویت من با دسترسی به فضاهای مجازی به سرقت می رود	۱/۰۰۰	۰/۹۰۵
۱۱	مراجعه به فضاهای مجازی عمومی داده های من را به خطر می اندازد.	۱/۰۰۰	۰/۸۶۳
۱۲	اطلاعات شخصی من در فضای مجازی ممکن است مورد سوءاستفاده قرار گیرد	۱/۰۰۰	۰/۶۷۵
۷	استفاده از نرم‌افزارهای امنیتی ممکن است برای سایر برنامه ها مشکل ایجاد کند	۱/۰۰۰	۰/۹۰۵
۲۹	من قصد دارم از نرم‌افزار امنیتی برای جلوگیری از بدافزار استفاده کنم	۱/۰۰۰	۰/۶۸۱
۳۰	قصد دارم از نرم‌افزارهای امنیتی برای جلوگیری از سوءاستفاده از بدافزار استفاده کنم	۱/۰۰۰	۰/۶۳۲
۳۱	برای محافظت از داده های خود ازاقدامات امنیتی مضاعف بهره خواهم گرفت	۱/۰۰۰	۰/۷۰۵
۲۷	اعضای گروه اقداماتی را انجام می دهند که از تهدیدات امنیتی جلوگیری میکند.	۱/۰۰۰	۰/۶۹۵
۲۸	اعضای گروه با فعالیت هایی مخالف هستند که ممکن است به آن‌ها آسیب برساند	۱/۰۰۰	۰/۶۵۸
۱۴	به سرقت رفتن اطلاعات من از طریق شبکه های آنلاین برای من مشکل ایجاد نموده است	۱/۰۰۰	۰/۸۶۱
۲۵	اعضای گروه از اقداماتی که به نفع امنیت است، استقبال می‌کنند	۱/۰۰۰	۰/۷۴۵
۲۶	اعضای گروه درگیر فعالیتهایی هستند که به نفع امنیت فضای مجازی است.	۱/۰۰۰	۰/۶۸۲
۵	من به راحتی می‌توانم اطلاعاتی در مورد چگونگی ایمن کردن صفحات شخصی خود درفضای مجازی بیابم	۱/۰۰۰	۰/۸۹۰
۱۸	اگر راه‌حلی برای تهدیدهای امنیتی باشد، آن‌ها را با اعضای گروه مجازی به اشتراک می‌گذارم	۱/۰۰۰	۰/۸۹۲
۳	من می‌توانم از نرم‌افزارهای امنیتی مختلف برای محافظت از اطلاعات خود استفاده کنم	۱/۰۰۰	۰/۹۴۴
۲۱	من تجربه آسیب دیدن داده های خودتوسط بدافزاررا دارم	۱/۰۰۰	۰/۷۷۹
۲۲	من تجربه بسرقت رفتن هویتم توسط یک حمله سایبری رادارم.	۱/۰۰۰	۰/۸۳۵
۲۳	من تجربه آلوده شدن رایانه‌ام را دارم	۱/۰۰۰	۰/۶۵۹
۲۴	من تجربه سوءاستفاده از اطلاعات شخصی خود از طریق حمله سایبری را دارم	۱/۰۰۰	۰/۷۹۸
۳۲	من نرم‌افزار امنیتی رایانه خود را مرتباً به روز می کنم	۱/۰۰۰	۰/۷۷۲
۳۳	من قبل از ورود به سیستم برای تأیید به دنبال یک نماد امنیتی، علائم اعتماد هستم	۱/۰۰۰	۰/۷۰۳
۳۴	من برای دسترسی تنظیمات امنیتی را در رایانه خود تغییر داده ام	۱/۰۰۰	۰/۶۳۱
۳۵	من نرم‌افزار اضافی را برای کاهش تأثیرات نقض امنیتی اطلاعات اضافه می کنم	۱/۰۰۰	۰/۶۶۶
۱۹	به اشتراک‌گذاری دانش امنیت اطلاعات با اعضا همیشه سودمند هستند	۱/۰۰۰	۰/۷۰۷
۱۷	اگر تهدیدهای امنیتی جدیدی پیدا کنم، اعضای گروه های مجازی را مطلع خواهم کرد	۱/۰۰۰	۰/۹۲۴
۲۰	به اشتراک‌گذاری دانش امنیت اطلاعات با اعضا گروه همواره باارزش هست	۱/۰۰۰	۰/۶۷۹
۸	فعال کردن ویژگی های امنیتی در فضای مجازی می تواند زمانبر باشد	۱/۰۰۰	۰/۸۶۴
۳	من می‌توانم تنظیمات امنیتی مرورگر وب خود را پیکربندی کنم	۱/۰۰۰	۰/۹۲۹
۲	من می‌توانم به درستی نرم‌افزار امنیتی را روی رایانه خود نصب کنم	۱/۰۰۰	۰/۷۷۲
۱۳	آلوده شدن رایانه من از طریق نرم‌افزارها برای من مشکلاتی را ایجاد می‌کند	۱/۰۰۰	۰/۸۶۲
۱	من این توانایی را دارم که به راحتی ویژگی های امنیتی را در فضای مجازی فعال کنم	۱/۰۰۰	۰/۶۷۶
۱۵	از دست دادن داده‌های شخصی به دلیل بدافزار از طریق فضاری مجازی یک مشکل جدی است	۱/۰۰۰	۰/۷۲۵
۱۶	از دست دادن داده های سازمانی از طریق بدافزار برای من یک مشکل جدی است	۱/۰۰۰	۰/۵۶۳

1. Extraction

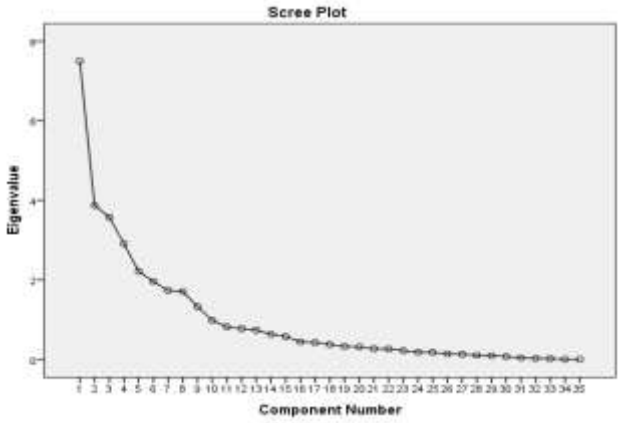
همان‌گونه که در جدول ۲ مشاهده می‌کنید، ستون مقدماتی نشان‌دهندهٔ مقدار کل واریانس هر متغیر است که مجموعهٔ عوامل می‌توانند آن را تبیین کنند. ستون استخراج، نشان‌دهنده‌ی مقداری از واریانس هر متغیر است که مجموعهٔ عوامل موردنظر توانسته‌اند آن را تبیین کنند. مقدار این واریانس از (۰) تا (۱) نوسان دارد. هرچه مقادیر به عدد (۱) نزدیک‌تر باشد، بهتر است. در جدول این عامل‌ها توانسته‌اند ۹۴ درصد (۹۴٪) از واریانس گویه شماره ۳ یعنی (من می‌توانم از نرم‌افزارهای امنیتی مختلف برای محافظت از اطلاعات خود استفاده کنم) و در مقابل ۵۶ درصد (۵۶٪) از واریانس گویه ۱۶ یعنی (از دست دادن داده‌های سازمانی از طریق نرم‌افزار برای من یک مشکل جدی است) را تبیین کنند.

مرحله سوم از تحلیل عاملی بر روی پرسشنامه، مشخص شدن شناخت سهم هر عامل در تبیین مجموع واریانس تمامی گویه‌ها است. نتایج نشان می‌دهد که ۳۵ سؤال موردنظر قابل‌تفکیک به ۹ عامل بوده و می‌توانیم از ترکیب این ۳۵ گویه، ساختار جدیدی براساس عامل‌ها به تحلیل بپردازیم. در جدول ۳ عوامل استخراج شده همراه با مقدار ویژه، درصد واریانس و درصد واریانس تجمعی ارائه شده است.

جدول ۳. واریانس عوامل استخراج شده به روش تحلیل عامل‌های اصلی

عامل‌ها	مقدار ویژه اولیه			مجذورات عوامل استخراج شده پس از چرخش		
	مقدار ویژه	درصد واریانس	درصد واریانس تجمعی	مقدار ویژه	درصد واریانس	درصد واریانس تجمعی
۱	۷/۴۹۹	۲۱/۴۲۶	۲۱/۴۲۶	۴/۲۰۵	۱۲/۰۱۴	۱۲/۰۱۴
۲	۳/۸۷۴	۱۱/۰۶۸	۳۲/۴۹۴	۳/۱۵۷	۹/۰۲۰	۲۱/۰۳۴
۳	۳/۵۷۹	۱۰/۲۲۷	۴۲/۷۲۱	۳/۱۳۲	۸/۹۴۹	۲۹/۹۸۳
۴	۲/۹۰۷	۸/۳۰۷	۵۱/۰۲۸	۳/۰۵۷	۸/۷۳۵	۳۸/۷۱۷
۵	۲/۲۱۶	۶/۳۳۱	۵۷/۳۵۹	۲/۹۱۹	۸/۳۴۱	۴۷/۰۵۸
۶	۱/۹۵۹	۵/۵۹۷	۶۲/۹۵۶	۲/۷۸۶	۷/۹۶۱	۵۵/۰۱۹
۷	۱/۷۳۳	۴/۹۵۲	۶۷/۹۰۸	۲/۷۳۴	۷/۸۱۰	۶۲/۹۲۹
۸	۱/۷۱۱	۴/۸۸۹	۷۲/۷۷۹	۲/۶۸۶	۷/۶۷۴	۷۰/۵۰۳
۹	۱/۳۳۱	۳/۸۰۲	۷۵/۵۹۹	۲/۱۳۴	۶/۰۹۶	۷۶/۵۹۹

بررسی تفکیکی عامل‌های استخراج شده در جدول ۳، سهم هر عامل در تبیین ۳۵ سؤال به صورت نزولی نشان داده شده است. به عبارتی نه عامل دارای ارزش بیشتر از یک است. عامل اول با مقدار ویژه ۷/۴۴۹ به تنهایی توانسته است ۲۱/۴۲۶ درصد از کل واریانس را تبیین کند. عامل دوم که مقدار ویژه آن ۳/۸۷۴ توانسته است با ۱۱/۰۶۸ درصد از کل واریانس تبیین کند، عامل سوم که مقدار ویژه ۳/۷۵۹ بود، ۱۲/۱۰/۲۲۷ درصد از کل واریانس را به خود اختصاص داده است. و در نهایت عامل نهم که مقدار ویژه آن ۱/۳۳۱ بود، ۳/۸۰۲ درصد از واریانس را تبیین کند. نه عامل استخراج شده درمجموع ۷۵/۵۵۹ درصد از کل واریانس پرسشنامه را تبیین می‌کنند که این مقدار مناسب و قابل‌قبولی است. نمودار ۱ نتایج جدول ۳ مبنی بر تعداد مناسب عامل‌ها را به صورت تصویری که همانند معیار کیزر است را نشان می‌دهد.



نمودار ۱. مقدارهای ویژه مربوط به مؤلفه‌های اصلی

مطابق نمودار ۱، نـه عامـل دارای مقـدار ویـژه بـالاتر از یـک هستند، به عبـارتی مجمـوع ۳۵ گویـه مربـوط بـه پرسشـنامه قابل‌تفکیک به نه عامل است. نتایج مشاهده شده در این نمودار تأییدکننده یافته‌های قبلی در جدول ۴، مبنی بر وجود نه مؤلفـه است که راه‌حل مؤلفه‌های اصلی را بهتر تبیین می‌کنند.

مرحله چهارم از تحلیل عاملی، شناخت ماتریس همبستگی بین گویه‌ها و عامل‌ها و دسته‌بندی هر گویـه در هـر عامـل اسـت. بنـابراین بـه‌منظور تفسـیر ایـن وضـعیت از جـدول مـاتریس همبستگی چرخش شده واریماکس استفاده شد. نتایج چـرخش واریماکس در جدول ۴ نشان داده شده است.

جدول ۴. ماتریس همبستگی بین به روش واریماکس

شماره سؤال	۱	۲	۳	۴	۵	۶	۷	۸	۹
۳	۰/۹۳۵								
۴	۰/۹۲۵								
۵	۰/۹۱۸								
۲	۰/۷۴۷								
۱	۰/۵۶۳								
۱۰		۰/۹۳۶							
۱۱		۰/۸۹۶							
۱۲		۰/۷۶۷							
۹		۰/۶۷۶							
۲۴			۰/۸۷۱						
۲۲			۰/۸۲۱						
۲۱			۰/۷۷۵						
۲۳			۰/۷۳۵						
۷				۰/۹۰۵					
۶				۰/۸۹۹					
۸				۰/۸۸۵					
۱۳					۰/۸۲۴				
۱۴					۰/۸۲۰				
۱۵					۰/۷۰۴				
۱۶					۰/۴۷۶				
۲۵						۰/۸۱۱			
۲۶						۰/۷۴۳			
۲۷						۰/۷۱۲			
۲۸						۰/۶۷۵			
۳۲							۰/۸۱۵		
۳۳							۰/۷۵۹		
۳۴							۰/۷۰۳		
۳۵							۰/۶۶۹		
۱۷								۰/۹۳۵	
۱۸								۰/۹۲۷	
۲۰								۰/۶۵۶	
۱۹								۰/۴۱۰	
۲۹									۰/۷۶۷
۳۱									۰/۷۱۸
۳۰									۰/۶۷۹

مطـابق جـدول ۴، مقـادیری کـه در هـر عامـل اعـداد آن را در کادر نوشـته شـده اسـت مـی‌تواننـد بـا همـدیگر تشـکیل عامـل رابطه را بدهنـد. براسـاس جـدول فـوق بـالاترین بـار پـنج سـؤال اول یعنـی سـؤال‌های q۳، q۴، q۵، q۲ و q۱ بـر روی عامـل اول اسـت در دسـته‌بندی سـایر گویـه‌هـا در عامـل‌هـای دوم تـا نهم نیز وجود این همبستگی بـین گویـه‌هـا و عامـل‌هـا ملاحظـه شـد. و مـی‌تـوان براسـاس ایـن همبسـتگی و بزرگ‌تـرین بـار عاملی آن‌هـا را در عامـل‌هـا دسـته‌بنـدی کـرد. همچنـین میـزان آلفای کرونبـاخ کلـی برابـر بـا ۰/۷۴ اسـت. بـرای هـر متغیـر بـه صـورت جداگانـه آلفـای کرونبـاخ در جـدول ۵ نشـان داده شـده اسـت. بعـد تحلیـل عـاملی بـر روی پرسشـنامه، جهـت پایـایی پرسشنامه از آزمون ضریب آلفای کرونباخ استفاده شد.

جدول ۵. ضرایب مربوط به آلفای کرونباخ

سازه‌های موردسنجش	مقدار ضریب آلفای کرونباخ
خودکار کارآمد	۰/۷۳
هزینه اقدام حفاظتی	۰/۷۸
حساسیت درک شده است	۰/۷۲
شدت تهدیدهای مخرب فناوری درک شده	۰/۷۵
به اشتراک‌گذاری دانش امنیت اطلاعات	۰/۷۸
تجربه امنیت اطلاعات	۰/۷۲
هنجارهای گروهی	۰/۷۶
انگیزه اجتنابی	۰/۷۵
رفتار اجتنابی	۰/۷۹

جامعه آماری این پژوهش شامل کلیه اعضای هیئت‌علمی تمام‌وقت در دانشگاه آزاد اسلامی واحد کرمانشاه است (۲۸۲ نفر) که با استفاده از فرمول کوکران و روش نمونه‌گیری تصادفی ساده ۱۶۲ نفر به‌عنوان نمونه انتخاب گردیدند.

به‌منظور بررسی رابطه بین متغیرهای مستقل و وابسته و بررسی فرضیه‌های پژوهش، با استفاده از نرم‌افزار اس. پی. اس. اس. از آزمون ضریب همبستگی استفاده شد. همچنین به‌منظور آزمون مجموعه روابط علت و معلولی بین متغیرها و مؤلفه‌های مورد بررسی با استفاده از نرم‌افزار آموس، معادلات ساختاری روابط بین متغیرها مدل‌سازی گردید.

یافته‌های پژوهش

به‌منظور آزمون فرضیه‌های پژوهش از ماتریس همبستگی پیرسون استفاده شد. نتایج این آزمون در جدول‌های ۶ الی ۸ نمایش داده شده است.

جدول ۶. محاسبه همبستگی بین متغیرهای پژوهش

متغیرها	۱	۲	۳	۴	۵	۶
انگیزه اجتناب	۱	–	–	–	–	–
حفاظت از هزینه	۰/۷۴۶ ۰/۰۰۰	۱	–	–	–	–

ادامه جدول ۶. محاسبه همبستگی بین متغیرهای پژوهش

حساسیت درک شده	۰/۷۱۳ ۰/۰۰۰	۰/۸۹۱ ۰/۰۰۰	۱	–	–	–
شدت تهدید های مخرب	۰/۷۱۵ ۰/۰۰۰	۰/۶۹۵ ۰/۰۰۰	۰/۶۵۴ ۰/۰۰۰	۱	–	–
به اشتراک‌گذاری دانش	۰/۶۳۲ ۰/۰۰۰	۰/۷۸۵ ۰/۰۰۰	۰/۷۲۶ ۰/۰۰۰	۰/۶۸۰ ۰/۰۰۰	۱	–
تجربه امنیت اطلاعات	۰/۷۰۹ ۰/۰۰۰	۰/۸۲۲ ۰/۰۰۰	۰/۶۷۴ ۰/۰۰۰	۰/۷۶۷ ۰/۰۰۰	۰/۶۷۳ ۰/۰۰۰	۱

فرضیه اول: هزینه اقدام حفاظتی رابطه مثبت و معناداری با انگیزه اجتناب از تهدید فناوری دارد.

مطابق جدول ۶ با اطمینان ۰/۹۹ و میزان خطای ۰/۰۱ درصد و با توجه به سطح معناداری به دست آمده (Sig.=۰/۷۴۶) بین دو متغیر حساسیت درک شده و انگیزه اجتناب رابطه معناداری وجود

دارد. از نظر شدت همبستگی بین دو متغیر با توجه مقدار r به دست آمده (r=۰/۷۴۶) در حد خیلی قوی و مثبت بوده است. بنابراین، فرضیه پژوهش تأیید و فرض خلاف رد می‌شود.

فرضیه دوم: حساسیت درک شده رابطه مثبت و معناداری با انگیزه اجتناب از تهدید فناوری دارد.

مطابق جدول ۶ با اطمینان ۰/۹۹ و میزان خطای ۰/۰۱ درصد و با توجه به سطح معناداری به دست آمده (Sig.=۰/۰۰۰) بین دو متغیر حفاظت از هزینه و انگیزه اجتناب رابطه معناداری وجود دارد. از نظر شدت همبستگی بین دو متغیر با توجه مقدار r به دست آمده (r=۰/۷۱۳) در حد خیلی قوی و مثبت بوده است. بنابراین، فرضیه پژوهش تأیید و فرض خلاف رد می‌شود.

فرضیه سوم: شدت تهدیدهای مخرب فناوری درک شدت رابطه مثبت و معناداری با انگیزه اجتناب از تهدید فناوری دارد.

مطابق جدول ۶ با اطمینان ۰/۹۹ و میزان خطای ۰/۰۱ درصد و با توجه به سطح معناداری به دست آمده (Sig.=۰/۰۰۰) بین دو متغیر شدت تهدیدهای مخرب و انگیزه اجتناب رابطه معناداری وجود دارد. از نظر شدت همبستگی بین دو متغیر با توجه مقدار r به دست آمده (r=۰/۷۱۵) در حد خیلی قوی و ثبت بوده است. بنابراین، فرضیه پژوهش تأیید و فرض خلاف رد می‌شود.

فرضیه چهارم: به اشتراک‌گذاری دانش امنیت اطلاعات رابطه مثبت و معناداری با انگیزه اجتناب از تهدید فناوری دارد.

مطابق جدول ۶ با اطمینان ۰/۹۹ و میزان خطای ۰/۰۱ درصد و با توجه به سطح معناداری به دست آمده (Sig.=۰/۰۰۰) بین دو متغیر به اشتراک‌گذاری دانش و انگیزه اجتناب رابطه معناداری وجود دارد. از نظر شدت همبستگی بین دو متغیر با توجه مقدار r به دست آمده (r=۰/۶۳۲) در حد خیلی قوی و مثبت بوده است. بنابراین فرضیه پژوهش تأیید و فرض خلاف رد می‌شود.

فرضیه پنجم: تجربه امنیت اطلاعات رابطه مثبت و معناداری با انگیزه اجتناب از تهدید فناوری دارد.

مطابق جدول ۶ با اطمینان ۰/۹۹ و میزان خطای ۰/۰۱ درصد و با توجه به سطح معناداری به دست آمده (Sig.=۰/۰۰۰) بین دو متغیر شدت تهدیدهای مخرب و انگیزه اجتناب رابطه معناداری وجود دارد. از نظر شدت همبستگی بین دو متغیر با توجه مقدار r به دست آمده (r=۰/۷۰۹) در حد خیلی قوی و مثبت بوده است. بنابراین، فرضیه پژوهش تأیید و فرض خلاف رد می‌شود.

جدول ۷. محاسبه همبستگی بین متغیرهای پژوهش (میانجی و ملاک)

متغیرها	۱	۲	۳
رفتار اجتنابی	۱	–	–
خودکارآمدی	۰/۵۸۷ ۰/۰۰۰	۱	–
هنجارهای گروهی	۰/۵۸۶ ۰/۰۰۰	۰/۶۰۳ ۰/۰۰۰	۱

فرضیه ششم: هنجارهای گروه رابطه مثبت و معناداری با رفتار اجتنابی دارد.

مطابق جدول ۷، با اطمینان ۰/۹۹ و میزان خطای ۰/۰۱ درصد و با توجه به سطح معناداری به دست آمده (Sig.=۰/۰۰۰) بین دو متغیر هنجارهای گروه و رفتار اجتنابی رابطه معناداری وجود دارد. از نظر شدت همبستگی بین دو متغیر با توجه مقدار r به دست آمده (r=۰/۵۸۷) در حد متوسط و مثبت بوده است. بنابراین، فرضیه پژوهش تأیید و فرض خلاف رد می‌شود.

فرضیه هفتم: خودکار کارآمدی رابطه مثبت و معناداری با رفتار اجتنابی دارد.

مطابق جدول ۷، با اطمینان ۰/۹۹ و میزان خطای ۰/۰۱ درصد و با توجه به سطح معناداری به دست آمده (Sig.=۰/۰۰۰) بین دو متغیر خودکارآمدی و رفتار اجتنابی رابطه معناداری وجود دارد. از نظر شدت همبستگی بین دو متغیر با توجه مقدار r به دست آمده (r=۰/۵۸۶) در حد متوسط و مثبت بوده است. بنابراین، فرضیه پژوهش تأیید و فرض خلاف رد می‌شود.

جدول ۸. محاسبه همبستگی بین متغیر میانجی با ملاک

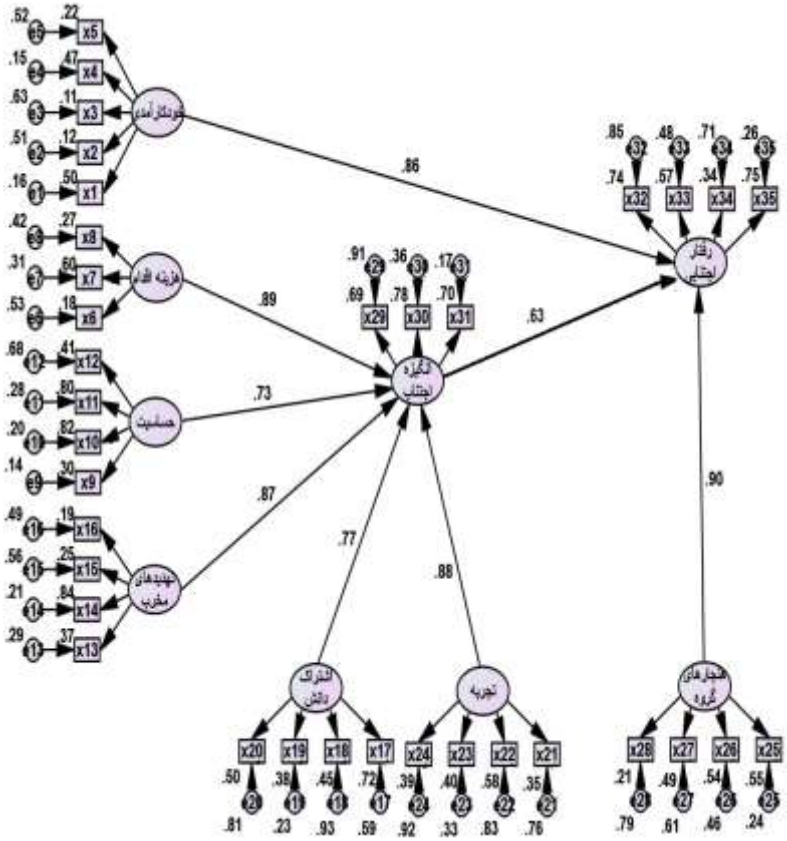
متغیرها	تعداد	آماره پیرسون	سطح معناداری
انگیزه اجتناب و رفتار اجتنابی	۱۶۲	۰/۶۲۲	۰/۰۰۰

فرضیه هشتم: انگیزه اجتناب رابطه مثبت و معناداری با رفتار اجتنابی دارد.

مطابق جدول ۸، با اطمینان ۰/۹۹ و میزان خطای ۰/۰۱ درصد و با توجه به سطح معناداری به دست آمده (Sig.=۰/۰۰۰) بین دو متغیر انگیزه اجتناب و رفتار اجتنابی رابطه معناداری وجود دارد. از نظر شدت همبستگی بین دو متغیر با توجه مقدار r به دست آمده (r=۰/۶۲۲) در حد قوی و مثبت بوده است. بنابراین فرضیه پژوهش تأیید و فرض خلاف رد می‌شود.

مدل‌یابی معادلات ساختاری

از آنجا که هدف پژوهش، دست‌یابی به مدلی از روابط علّی بین متغیرهاست، لازم است تا از شیوه مدل‌یابی علّی استفاده گردد. به‌منظور نمایش بصری روابط بین متغیرهای مستقل، وابسته میانی و وابسته ملاک از معادلات ساختاری استفاده گردید.

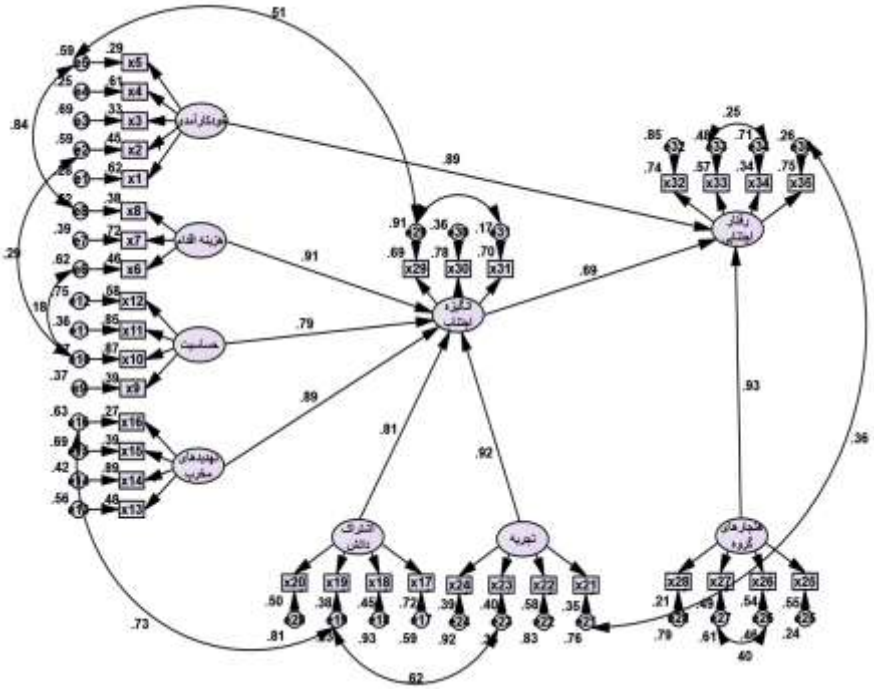


شکل ۱. مدل ساختاری پژوهش با ضرایب استاندار برازش مدل

جدول ۹. شاخص‌های برازش مدل کلی

مدل کل	X2/df	RMSEA	NFI	CFI	IFI	RFI	PRATIO	PNFI	PCFI
میزان قابل‌قبول	<۳	<۰/۰۵	>۰/۹	>۰/۹	>۰/۹	>۰/۹	>۰/۵۰	>۰/۵۰	>۰/۵۰
مقادیر محاسبه شده	۶/۳۱۲	۰/۳۱۷	۰/۷۱۸	۰/۶۵۳	۰/۷۴۷	۰/۶۸۴	۰/۳۱۳	۰/۲۸۰	۰/۳۲۴

نسبت مجذور کای مدل ساختاری به درجه آزادی برابر ۶/۳۱۲ و نامناسب است. شاخص‌های برازش تطبیقی همگی پایین‌تر از ۹۰ درصد و نامناسب هستند. شاخص RMSEA بالاتر از ۵ درصد و نامناسب است. اما شاخص‌های مقتصد (اقتصادی بودن) همه بالاتر از ۵۰ درصد بوده و مناسب هستند. بنابراین نیاز به اصلاحاتی در مدل است.



شکل ۲. مدل اصلاحی پژوهش با ضرایب استاندارد

جدول ۱۰. شاخص‌های برازش مدل کلی اصلاحی

مدل کلی	X2/df	RMSEA	NFI	CFI	IFI	RFI	PRATIO	PNFI	PCFI
میزان قابل‌قبول	<۳	<۰/۰۵	>۰/۹	>۰/۹	>۰/۹	>۰/۹	>۰/۵۰	>۰/۵۰	>۰/۵۰
مقادیر محاسبه شده	۱/۵۴۳	۰/۰۲۱	۰/۹۳۶	۰/۹۴۲	۰/۹۶۶	۰/۹۲۴	۰/۶۷۶	۰/۶۸۲	۰/۶۱۷

شاخص‌های تطبیقی (NFI، RFI، CFI، IFI)

– مقدار NFI یا شاخص برازش هنجار شده بنتلر–بونت به دست آمده مقدار ۰/۹۳۶ است که با توجه به مقدار استاندارد ۰/۹ که حد مطلوب این شاخص می‌باشد، مدل با توجه به این شاخص از برازش مطلوبی برخوردار است.

– مقدار RFI یا شاخص برازش نسبی به دست آمده مقدار ۰/۹۲۴ می‌باشد که این شاخص به برازش مطلوب مدل اشاره دارد.

– مقدار IFI یا شاخص برازش افزایشی به دست آمده مقدار ۰/۹۶۶ می‌باشد که این شاخص به برازش مطلوب مدل اشاره دارد.

– مقدار CFI یا شاخص برازش تطبیقی به دست آمده مقدار ۰/۹۴۲ می‌باشد که این شاخص به برازش مطلوب مدل اشاره دارد.

– مقدار RMSEA یا ریشه دوم میانگین مربعات خطای برآورد به دست آمده مقدار ۰/۰۲۱ می‌باشد که با توجه به مقدار استاندارد کمتر از ۰/۰۵، مطلوب می‌باشد.

شاخص‌های مقتصد (PNFI، PCFI، PRATIO)

– مقدار PNFI یا شاخص هنجار شده مقتصد برابر ۰/۶۸۲ و بالاتر از ۰/۵ و نشان از وضعیت مطلوب مدل دارد.

– مقدار PCFI یا شاخص برازش تطبیقی مقتصد برابر ۰/۶۱۷ و بالاتر از ۰/۵ و نشان از وضعیت مطلوب مدل دارد.

مقدار PRATIO یا نسبت مقتصد بودن برابر ۰/۶۷۶ و بیشتر از ۰/۵ و نشان از وضعیت مطلوب مدل دارد.

لذا در کل با توجه به همه شاخص‌ها می‌توان گفت مدل از برازش مناسبی برخوردار است. در نتیجه اصلاح شاخص‌ها بهبود یافتند.

بحث و نتیجه‌گیری

این مطالعه با هدف شناسایی رفتار امنیت اطلاعاتی کاربر در جوامع مجازی حرفه‌ای براساس رویکرد اجتناب از تهدید فناوری انجام شد. امنیت اطلاعات فرایندی است که براساس آن از اطلاعات در مقابل تجاوزهای مختلف حفاظت خواهد شد؛ به نحوی که از ادامه فعالیت با حداقل خسارت و حداکثر کار

آیی و بهره‌برداری از فرصت‌های عملیاتی، اطمینان حاصل شود. نتایج پژوهش نشان داد که هرچقدر هزینه اقدام حفاظتی برای امنیت اطلاعات بیشتر باشد تهدید برای فناوری اطلاعات کاهش می‌یابد. براساس پژوهش انجام شده دسترسی به اطلاعات حفاظت شده باید محدود باشد به افراد، برنامه‌های رایانه‌ای، فرایندها و سیستم‌هایی که مجاز به دسترسی به اطلاعات هستند. این مستلزم وجود سازوکار برای کنترل دسترسی به اطلاعات حفاظت شده می‌باشد. پیچیدگی سازوکارهای کنترل دسترسی باید مطابق با ارزش اطلاعات مورد حفاظت باشد. اطلاعات حساس‌تر و با ارزش‌تر نیاز به سازوکار کنترل دسترسی قوی‌تری دارند. اساس سازوکارهای کنترل دسترسی بر دو مقوله احراز هویت و تصدیق هویت است؛ و در این راستا هزینه‌های به سازمان تحمیل می‌گردد که نتیجه آن امنیت اطلاعات افزایش خواهد یافت در رابطه با دو متغیر فوق می‌توان گفت که حساسیت درک شده تأثیر مثبتی بر انگیزه اجتناب از تهدید فناوری را دارد به این صورت که هرچقدر حساسیت درک شده بیشتر باشد در طرف مقابل تهدیدهای فناوری اطلاعات کاهش یافته و همچنین انگیزه برای دسترسی به اطلاعات نیز کاهش می‌یابد. نتیجه این فرضیه با نتایج پژوهش (الهی، طاهری و حسین‌زاده، ۲۰۲۱)، همسو می‌باشد. به این صورت که امنیت سیستم‌های اطلاعاتی هم فناوری و هم افراد (عوامل انسانی) را در برمی‌گیرد و حساسیت درک شده اطلاعات را نشان می‌دهد که در سازمان باید برای جلوگیری از تهدیدهای موجود جلوگیری گردد.

با توجه به اینکه درک از تهدیدهای مخرب فناوری باعث انگیزه در اجتناب فناوری می‌شود هرچه این درک کامل‌تر باشد نتیجه بهتری دارد؛ یعنی از تهدیدهای مخرب فناوری جلوگیری می‌کند. با توجه به فعال کردن فناوری‌های جدید و گسترش برنامه‌های امنیتی در سراسر شرکت و تنظیم معیارهای امنیتی می‌توان مؤثر در عملکرد امنیت اطلاعات باشد و تهدیدهای مخرب فناوری را کاهش دهد.

به اشتراک گذاشتن دانش امنیت اطلاعات باعث بهبود وضعیت امنیتی می‌شود یعنی اطلاعات مختلف تجمیع و راهکارهای جدیدی برای حفظ امنیت اطلاعات به دست می‌آید با اشتراک‌گذاری دانش و اطلاعات به صورت یکدست در سازمان توزیع می‌شود و محدود به یک قسمت از سازمان نمی‌گردد و هرچقدر اطلاعات و دانش در سازمان در سطح بالایی قرار داشته باشد باعث می‌شود باعث کاهش تهدیدات فناوری می‌شود این موضوع در پژوهش‌های مختلف ثابت شده است. نتیجه این فرضیه با نتایج پژوهش (خیرگو و شکوهی[1]، ۲۰۱۷)، همسو می‌باشد. با توجه به آن‌که در آن پژوهش نقش متغیرهایی چون «عوامل سازمانی»، «عوامل انسانی» و «عوامل فنی» مورد بررسی قرار گرفته است. این عوامل نقش مهمی در بهبود عملکرد امنیت اطلاعات سازمان دارد.

هرچه در سازمان تجربه بیشتری در بحث امنیت اطلاعات وجود داشته باشد باعث کارایی بهتر و مناسب‌تری در امنیت اطلاعات می‌شود و کاربران و استفاده‌کنندگان تهدید فناوری را کمتر احساس می‌کنند این در حالی است که نبود تجربه باعث تهدیدات بیشتر در این زمینه می‌شود و احساس ناامنی کاربران و تهدیدات فناوری اطلاعات بیشتر می‌شود. نتیجه این فرضیه با نتایج پژوهش (یوسفی، خیرگو و شکوهی، ۲۰۱۵). همسو می‌باشد. در این پژوهش الگویی براساس استاندارد ایزو و چارچوب کوبیت ارائه شده است در این الگو شش شاخص و زیرشاخص ریسک امنیت اطلاعات سازمانی شناسایی شد یکی از این شاخص‌ها تجربه امنیت اطلاعات بود که نقش مهمی در کاهش ریسک امنیت اطلاعات داشت.

هنجارها تقریباً در هر حوزه‌ای از رفتار انسان عمل می‌کنند. خیلی افراد ممکن است تشخیص ندهند که هنجارهای جامعه آن‌ها اساساً قراردادی است، مگر اینکه مشاهده کنند که در فرهنگ متفاوتی هنجارهای متفاوتی در جریان است. بر این اساس هنجارهای گروهی می‌تواند رفتارهای اجتنابی را در برداشته باشد و متأثر از آن باشد. نتیجه این فرضیه با نتایج پژوهش (کیخا[2]، ۲۰۱۵). همسو می‌باشد. به این شکل که در آن پژوهش افزایش اعتماد بین فردی می‌تواند انگیزه افراد مجازی را در جهت اشتراک دانش افزایش دهد. بنابراین، به درک عوامل مؤثر بر اعتماد بین فردی و رفتار اشتراک دانش اعضا نیاز داریم و هنجارهای گروهی را در راستای اهداف سازمان توسعه دهند.

حس خود کارآمدی می‌تواند نقش مهمی در رسیدن به اهداف، انجام وظایف و فائق آمدن بر چالش‌ها داشته باشد افراد با خود کارآمدی بالا می‌توانند در جریان فناوری اطلاعات به صورت مناسب‌تری عمل کنند و همچنین با خود کارآمدی به توسعه فناوری اطلاعات دست یابند و بر رفتارهای اجتنابی تأثیرگذار می‌باشد. با ظهور اینترنت و فضای مجازی هنجارهایی جدید پدید آمده‌اند که مخصوص پیام‌رسان‌های مجازی است که باید رعایت این الگوهای رفتاری را جدی بگیریم.

1. Kheirgoo & Shukuhy
2. Keikha

انگیزه اجتناب در سازمان برای امنیت اطلاعات بر رفتارهای اجتنابی تأثیرگذار می‌باشد به این شکل که انگیزه‌های به وجود آمده در کارکنان و فراهم شدن شرایط مناسب برای آن‌ها انگیزه لازم را به وجود آورده و متأثر از آن رفتارهای اجتنابی شکل می‌گیرد. نتیجه این فرضیه با نتایج پژوهش‌های (شاما و همکاران[1]، ۲۰۱۷) و (فورستر[2]، ۲۰۱۹)، همسو می‌باشد. اطلاعات و دانش کارکنان و استفاده‌کنندگان از فضای مجازی هرچقدر که بیشتر باشد امکان لو رفتن اطلاعات و یا سرقت اطلاعات کمتر می‌گردد یکی از مباحث مشخص شده در ادبیات امنیت اطلاعات به‌اصطلاح رفتاری، مربوط به این است که چرا کارمندان از روش‌های امنیتی اطلاعات سازمانی خود پیروی یا آن را نقض می‌کنند.

نتایج کلی پژوهش نشان داد که از آنجایی که اطلاعات برای هر سازمانی به‌عنوان یک کالای کاملاً ارزشمند و حیاتی محسوب شده و برای حفظ و امنیت اطلاعات در برابر تهدیدهای مختلف، نیاز است دسترسی افراد در سمت‌های مختلف یک سازمان و حتی خارج از سازمان به اطلاعات با سازوکارهای مختلف که بستگی به ارزش هر نوع اطلاعات را دارد، کنترل شود. برنامه‌ریزان و متولیان حفاظت اطلاعات در سازمان‌ها، ضروری است که آموزش‌های لازم و مستمر جهت درک بهتر افراد از حفاظت اطلاعات در برابر تهدیدات مختلف سرلوحه کار خود قرار دهند که این امر موجب می‌شود عوامل مخرب و تهدیدات اطلاعات را شناسایی و برای مقابله با آن برنامه مناسبی را مهیا کنند. همچنین جهت رسیدن به این وضعیت یعنی کاهش تهدیدات، ضروری است به عوامل مختلفی اعم به اشتراک‌گذاری دانش و تجربه افراد و ایجاد محیطی امن جهت اعتماد بین افراد توجه بیشتری شود که این امر می‌تواند به‌عنوان راهکارهای ارزشمندی برای هر سازمان باشد. از طرفی، آگاهی و شناخت نسبت به انواع تهدیدها و ماهیت هرکدام از آن‌ها، منجر به سالم نگه‌داشتن سازمان‌ها و پیشرفت آن‌ها خواهد شد. همچنین به‌منظور تقویت خود کارآمدی افراد، با این اینکه خود کارآمدی تقریباً یک عامل فردی است ولی سازمان‌ها با اتخاذ تدابیر و خط‌مشی مناسب می‌توانند در افزایش خود کارآمدی افراد در سازمان نقش سازنده‌ای داشته باشند. در نهایت ایجاد انگیزه‌های مختلف اعم از پاداش‌های مادی و معنوی می‌تواند نقش مؤثری در شناخت و آگاهی در کاهش تهدیدات را میسر سازد. به‌طور کلی یافته‌های این مطالعه این بحث را روشن ساخت که چگونه کاربران اطلاعاتی در تصمیم‌گیری امنیتی خود در برابر تهدیدات اطلاعاتی رفتار می‌کنند. از دیگر نتایج این پژوهش، برازش مدل ارائه شده بود که نتایج نشان داد مدل ارائه شده از برازش مطلوبی برخوردار است. این مدل می‌تواند در تحقیقات آتی مرتبط با رفتار امنیت اطلاعاتی کاربران در جوامع مجازی بیشتر مورد بررسی قرار گیرد.

راهکارها

براساس فرضیه اول و دوم پژوهش، هزینه برای اقدامات حفاظتی از عواملی است که در سازمان باید مورد توجه قرار گیرد که براساس آن تجهیزات و فناوری‌های به‌روزتری در دسترس سازمان قرار می‌گیرد و همین موضوع باعث می‌گردد که انگیزه‌های که برای تهدید فناوری وجود دارد کاهش پیدا کند چراکه سطح امنیت افزایش پیدا کرده است. بنابراین پیشنهاد می‌شود سطوح دسترسی به اطلاعات برای همه افراد تعریف گردد و هر فردی براساس نوع مسئولیتی که دارد بتواند فقط به اطلاعات تعریف شده مربوط به خود دسترسی داشته باشند.

براساس فرضیه سوم و چهارم، اشتراک‌گذاری دانش بین اعضا می‌تواند با افزایش دانش آن‌ها نسبت به اطلاعات و فناوری‌های جدید همراه باشد و سطح دانش در افراد افزایش پیدا می‌کند که در این صورت اعضا می‌توانند در برابر تهدیدات فناوری‌ها بهتر عمل کنند و تصمیمات مناسب‌تری را بگیرند. پیشنهاد می‌شود به‌منظور اشتراک‌گذاری دانش در خصوص امنیت اطلاعات و درک صحیح از تهدیدهای مخرب فناوری اطلاعات و همچنین داشتن سواد اطلاعاتی امنیت اطلاعات افراد در برابر تهدیدهای ایجاد شده، تشکیل کارگاه‌های آموزشی مستمر می‌تواند این توانایی را در بین افراد تقویت کند.

براساس فرضیه پنجم و ششم، پیشنهاد می‌شود مدیران سازمان‌ها توجه و نظارت بیشتری به موضوع امنیت اطلاعات در سازمان داشته باشند. از طرفی، توجه به امنیت اطلاعات موجب کاهش انواع تهدیدها خواهد بود. بنابراین تدوین و توسعه نظام نظارت و حفاظت امنیتی بر محتوای داده‌های مبادله شده با توجه به قانون امنیتی دانشگاه و حفظ حریم عمومی و خصوصی که نقش اساسی در پیشگیری از گسترش فساد، تهدیدات امنیتی، رسوخ جاسوسی و خراب‌کاری الکترونیک و عملیات روانی خواهد داشت.

1. Shamala & et al
2. Forrester

References

Bifulco, A., & Santoro, R. (2005, September). A conceptual framework for "Professional Virtual Communities". In *Working Conference on Virtual Enterprises* (pp. 417-424). Springer, Boston, MA.

Elahi, S., Taheri, M., & Hassanzadeh, A. (2021). A Framework for the Role of Human Factors In information Systemsâ Security.*Management Research in Iran*, *13*(2), 1-22.

Fathian, M,. & Mahdavi Noor, H. (2015). Information Technology: Fundation and Management, Tehran: *Iran University of Science & Technology*. (In Persian).

Farazmand, H., Mashayekh, M, & Hesami, K. (2012). The Relationship between Information Technology and Manpower Productivity and Capital in Companies Listed in Tehran Stock Exchange. *The Journal of Social Development*, 7(3), 63-78. (In Persian).

Forrester, V. V. (2019). *User Information Security Behavior in Professional Virtual Communities: A Technology Threat Avoidance Approach* (Doctoral dissertation, Nova Southeastern University). Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2019). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory.*Journal of Intellectual Capital*.

Jackson, B. A., Greenfield, V. A., Morral, A. R., & Hollywood, J. S. (2014). Police department investments in information technology systems: challenges assessing their payoff.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS quarterly*, 549-566.

Karjalainen, M., Siponen, M., & Sarker, S. (2020). Toward a stage theory of the development of employees' information security behavior. *Computers & Security*, *93*, 101782.

Keikha, F. (2018). Interpersonal trust factors affecting members' knowledge sharing behavior in virtual communities. *Iran. J. Inf. Process. Manag*, 34, 275-300.

Kheirgoo, M., & Shukuhy, J. (2017). Identification and ranking of key factors influencing the effectiveness of information systems in State-Owned Organizations. *Iranian Journal of Information processing and Management*, *32*(3), 695-712.

Nadri, Gh. & Bakhshayesh, A (2020). Investigating the Impact of Virtual Social Networks on Social Security of Iran with a policy approach. *Protectiv and Society researchs*, 7(25), 125-154. (In Persian)

Nia, M. G., Harandi, M. F., & de Vries, M. J. (2019). Technology development as a normative practice: A meaning-based approach to learning about values in engineering—Damming as a case study. *Science and engineering ethics*, *25*(1), 55-82.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

Samtani, S., Chinn, R., Chen, H., & Nunamaker Jr, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, *34*(4), 1023-1053.

Shamala, P., Ahmad, R., Zolait, A., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications*, *36*, 1-10.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. Computers in Human Behavior, 78, 283-297.

Yousefi Zenouz, R., Hassanpoor, A., & Mousavi, P. (2015). A model to Prioritizing Organizational Information security risks using by Fuzzy AHP and Bayesian

Networks in the banking industry. *Industrial Management Studies*, 13(37), 161-185. (In Persian).

Yudatama, U., Hidayanto, A. N., Nazief, B. A., & Phusavat, K. (2019). Data to model the effect of awareness on the success of IT Governance implementation: A partial least squares structural equation modeling approach (PLS-SEM). *Data in brief*, *25*, 104333.