Scientific Journal Of Organizational knowledge Management

18

Vol. 3
Autumn 2022

Use of Structural Equation Modeling for Agent-based Modeling and Simulation in the Analysis of Information Security Knowledge Sharing

Mohammad Ali Kiashmeshki [1] | Amir Daneshvar [2]

Research Paper

Received:
01 August 2022
Accepted:
14 August 2022
P.P: 151-199

Print ISSN: 2645-4262
Online ISSN: 2645-5242

Abstract

In this study, the information security knowledge sharing model is presented from the integration of the theories of planned behavior, motivation, triandis and behavior change stages in an organization by combining the statistical method of structural equation modeling and agent-based modeling and simulation; Also, in this study, structural equation modeling has been used to build models as inputs for factor-based modeling and to improve and improve their reliability and validity. in other words; In this study, structural equation modeling has been applied for factor-based modeling. The data collection method is a questionnaire made by the researcher and collected by simple random sampling method. After testing the validity and reliability of the questionnaire, data was collected from 217 participants. Using SmartPLS3.2.6 and Anylogic software, hypothesis testing and simulation based on statistical results are analyzed in order to analyze the change of behavior over time. The findings have shown that the factors of the theory of planned behavior, including attitude, mental norms, perceived behavioral control and motivation theory, which include internal and external motivational factors, and the Triandis model, in order to facilitate the conditions, have positive effects on the stages of behavior change from It includes the stages of pre-reflection, reflection, preparation, action, maintenance and termination. In addition, the change in information security knowledge sharing behavior in the organization increases over time until reaching the end stage. The innovation of this study is factor-based modeling in order to test hypotheses over time along with the statistical method of structural equation modeling. In addition, the behavior change model has also been applied to analyze the behavior change stages of information security knowledge sharing. Knowledge sharing plays an important role in the field of information security; Because it has a positive effect on the awareness of employees' information security.

Keywords: Knowledge Management, Information Security, Agent-Based Modeling, Structural Equation Modeling.

DOR: 20.1001.1.26454262.1401.5.3.5.3

1.Department of Information Technology Management, Science and Research Unit, Islamic Azad University, Tehran, Iran.
2.Corresponding author: Assistant Professor, Department of Information Technology Management, Management Faculty, Electronic Branch, Islamic Azad University, Tehran, Iran. Daneshvar.amir@gmail.com

نشریه علمی مدیریت دانش سازمانی

به کار گیری مدلسازی معادلات ساختاری برای شبیه سازی و مدلسازی مبتنی بر عامل در تجزیه و تحلیل به اشتراک گذاری دانش امنیت اطلاعات

محمدعلی کیاشمشکی [1] | امیر دانشور [2]

۱۸

سال پنجم
پاییز ۱۴۰۱

مقاله پژوهشی

تاریخ دریافت:
۱۴۰۱/۰۵/۱۰
تاریخ پذیرش:
۱۴۰۱/۰۵/۲۳
صص: ۱۹۹-۱۵۱

شاپا چاپی: ۴۲۶۲-۲۶۴۵
الکترونیکی: ۵۲۴۲-۲۶۴۵

چکیده

در این مطالعه، مدل به اشتراک‌گذاری دانش امنیت اطلاعات از تلفیق تئوری‌های رفتار برنامه‌ریزی‌شده، انگیزش، تریاندیس و مراحل تغییر رفتار در یک سازمان با ترکیب روش آماری مدل‌سازی معادلات ساختاری و مدل‌سازی و شبیه‌سازی مبتنی بر عامل ارائه شده است؛ همچنین در این مطالعه از مدل‌سازی معادلات ساختاری استفاده شده است تا مدل‌هایی به‌عنوان ورودی‌های مدل‌سازی مبتنی بر عامل ساخته شود و قابلیت اطمینان و اعتبار آن‌ها را بهبود و ارتقا بخشد. به‌عبارت‌دیگر؛ در این مطالعه مدل‌سازی معادلات ساختاری برای مدل‌سازی مبتنی بر عامل اعمال شده است. روش جمع‌آوری داده‌ها یک پرسشنامه است که توسط محقق ساخته شده و به روش نمونه‌گیری تصادفی ساده جمع‌آوری شده است. بعد از آزمودن قابلیت اعتبار و اطمینان پرسشنامه، داده‌ها از ۲۱۷ شرکت‌کننده جمع‌آوری شده است. با استفاده از SmartPLS3.2.6 و نرم‌افزار Anylogic فرضیه‌ها آزمون و شبیه‌سازی مبتنی بر نتایج آماری به ترتیب تجزیه‌وتحلیل می‌شود تا تغییر رفتار در طی زمان تحلیل شود. یافته‌ها نشان داده است که عوامل تئوری رفتار برنامه‌ریزی شده از جمله نگرش، هنجارهای ذهنی، کنترل رفتاری ادراک شده و تئوری انگیزش که عوامل انگیزشی درونی و بیرونی را در برمی‌گیرند و مدل تریاندیس، به‌منظور تسهیل شرایط، تأثیرات مثبتی روی مراحل تغییر رفتار از جمله مرحله‌های پیش تأمل، تأمل، آماده‌سازی، اقدام، نگهداری و خاتمه می‌گذارد. به‌علاوه، تغییر در رفتار به اشتراک‌گذاری دانش امنیت اطلاعات در سازمان، در طی زمان و تا رسیدن به مرحله پایان، افزایش پیدا می‌کند. نوآوری این مطالعه مدل‌سازی مبتنی بر عامل به‌منظور آزمون فرضیه¬ها در طی زمان در کنار روش آماری مدل‌سازی معادلات ساختاری است. علاوه بر این، مدل تغییر مراحل رفتار نیز برای تجزیه‌وتحلیل مراحل تغییر رفتار به اشتراک‌گذاری دانش امنیت اطلاعات اعمال شده است. به اشتراک‌گذاری دانش، نقش مهمی در زمینه امنیت اطلاعات ایفا می‌کند؛ زیرا تأثیر مثبتی روی آگاهی از امنیت اطلاعات کارکنان می‌گذارد.

کلیدواژه‌ها: مدیریت دانش، امنیت اطلاعات، مدل‌سازی مبتنی بر عامل، مدل‌سازی معادله ساختاری.

DOR: 20.1001.1.26454262.1401.5.3.5.3

۱. گروه مدیریت فناوری اطلاعات، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.
۲. نویسنده مسئول: استادیار، گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، واحد الکترونیکی، دانشگاه آزاد اسلامی، تهران، ایران. Daneshvar.amir@gmail.com

مقدمه

امروزه اینترنت از ضروریات زندگی انسان‌ها به شمار می‌آید و فعالیت‌های سازمانی به‌طور فزاینده‌ای بر فناوری‌های مبتنی بر وب متکی است. علاوه بر آن، کارکنان با به‌کارگیری تلفن‌های همراه خودشان، از موقعیت‌های مکانی متفاوتی می‌توانند به اطلاعات سازمانی دست یابند. تغییرات در شرایط کاری، به‌ویژه در بحران‌هایی مانند بیماری کرونا (کوید-۱۹) به کارکنان این امکان را داد که بتوانند از راه دور و از منزل‌های خود به اطلاعات سازمانی دست پیدا کنند (حضری[1] و همکاران، ۲۰۰۸).

بنابراین، امنیت اطلاعات به موضوعی بحث‌برانگیز برای کاربران و سازمان‌ها تبدیل شده است. اینترنت پلتفرمی است که نقض و افشای اطلاعات در آن امکان‌پذیر است. هکرها از روش‌های هوشمندانه و جدیدی استفاده می‌کنند تا سیستم‌های کامپیوتری را هک کنند (سوفا[2] و سولمس، ۲۰۱۶). این روزها بیش از ۶۰ درصد از تمام معامله‌های تجاری به‌صورت آنلاین انجام می‌شود؛ بنابراین، این حوزه نیاز به امنیت بالایی دارد تا معاملات به بهترین شکل انجام شود. در نتیجه، امنیت سایبری یکی از جدیدترین مسائلی است که باید به آن‌ها پرداخته شود. دامنه امنیت سایبری به ایمن بودن اطلاعات در حوزه‌های مختلفی مانند فضای سایبری گسترش یافته است. حفظ حریم شخصی و امنیت داده‌ها همیشه از مهم‌ترین اقدامات امنیتی هستند که هر سازمانی باید به آن‌ها بپردازد. علاوه بر این، با افزایش جرائم سایبری، اقدامات امنیتی نیز رشد و افزایش داشته است. ۹۸ درصد از منابع امنیت سایبری خودشان را افزایش داده یا حفظ کرده‌اند، و نیمی از آن‌ها منابعی را به حملات آنلاین اختصاص داده‌اند (ردی[3] و ردی، ۲۰۱۴).

از طرفی، انسان‌ها به‌عنوان موجوداتی پیچیده و چندوجهی، برنامه‌ها، توانایی‌ها، اعتقادات و اولویت‌های خاص خودشان را دارند. حتی پیچیده‌ترین سیستم‌ها نیز ممکن است به‌واسطه مهندسی اجتماعی[4] دستکاری روانشناختی افراد در انجام کارهای خاص یا افشای اطلاعات- مورد تهدید و ریسک واقع شوند؛ بنابراین، امنیت سایبری در مورد افراد است. هر کاربر باید درک و شناخت

1. Hazari
2. Safa & Solmes
3. Reddy
4. Social Engineering

اساسی و بنیادین از تهدیدات اینترنتی و نیز چگونگی تشخیص آن‌ها داشته باشد –موضوعاتی که زیر چتر سواد دیجیتال قرار می‌گیرند (ای سی ای[1]، ۲۰۱۶).

امنیت اطلاعات به حفاظت از اطلاعات در برابر دسترسی، افشا، استفاده، دستکاری، اخلال یا تخریب غیرمجاز اطلاق می‌شود. در امنیت اطلاعات، مسائل مهم شامل حفظ محرمانگی، یکپارچگی و قابلیت در دسترس قرار گرفتن می‌باشد. به اشتراک‌گذاری دانش امنیت اطلاعات نقش مهمی در حوزه امنیت اطلاعات بازی می‌کند زیرا تأثیر مثبتی روی آگاهی از امنیت اطلاعات در کاربران دارد. مشخص شده است که آگاهی امنیتی مهم‌ترین عاملی است که خطر نقض امنیت اطلاعات در سازمان‌ها را کاهش می‌دهد. سازمان‌ها در مورد به اشتراک‌گذاری دانش امنیت اطلاعات با کارکنان خود، با مشکلاتی مواجه هستند و راه‌حل‌های متناسب با آن‌ها باید ارائه بشود. عدم توانایی در اتخاذ راه‌حل‌های مناسب برای مشکلاتی که در به اشتراک‌گذاری دانش وجود دارد، منجر به اتلاف وقت بسیار و هزینه‌های اضافی می‌شود (فلورس و همکاران، ۲۰۱۴).

به اشتراک‌گذاری دانش، از هر نوعی که باشد، باعث ارتقای کل سازمان می‌شود و اعتماد بین کارکنان را افزایش می‌دهد (الاحمری و همکاران، ۲۰۱۸). به اشتراک‌گذاری دانش امنیت اطلاعات در این مطالعه از اهمیت ویژه‌ای برخوردار است. مطالعه موردی این تحقیق، سازمانی دولتی در حوزه فناوری اطلاعات می‌باشد که به دلیل اجرای طرح‌های ملی فناوری اطلاعات، مورد حملات مهندسی اجتماعی واقع می‌شود؛ لذا، از جمله مکانیزم‌های دفاعی در مواجهه با این حملات، ارتقای آگاهی‌های امنیتی کارکنان می‌باشد. به دلیل وجود سیاست‌های امنیتی در برابر مهندسی اجتماعی در این سازمان به‌عنوان سطح پایه‌ای مکانیزم دفاعی، در سطح بعد افزایش آگاهی‌های امنیتی کارکنان مدنظر قرار می‌گیرد. هدف اصلی به اشتراک‌گذاری دانش امنیت اطلاعات، در دسترس قرار دادن دانش امنیت اطلاعات برای هر کسی است که به آن نیاز دارد. در نهایت هدف غایی آن، بهبود و ارتقای امنیت اطلاعات در سراسر سازمان است؛ لذا، در این مطالعه بر اشتراک‌گذاری دانش امنیت اطلاعات در این سازمان تمرکز می‌شود.

در این مطالعه، یک چارچوب مفهومی ارائه شده است که نشان می‌دهد، چگونه فاکتورهای تئوری رفتار برنامه‌ریزی شده، مدل تریاندیس و تئوری انگیزه برای به اشتراک‌گذاری دانش امنیت

1. ACE

اطلاعات[1] بر روی مراحل تغییر رفتاری به اشتراک‌گذاری دانش امنیت اطلاعات تأثیر می‌گذارد. انگیزه افراد را تشویق می‌کند که به‌طور ویژه‌ای رفتار کنند. به اشتراک‌گذاری دانش امنیت اطلاعات معمولاً در هر زمانی که به افراد انگیزه داده شود؛ اتفاق می‌افتد. نظریه رفتار برنامه‌ریزی شده نشان می‌دهد که چگونه نگرش‌ها، کنترل رفتاری درک شده و هنجارهای ذهنی بر روی انگیزه‌های فرد در راستای انجام رفتاری ویژه تأثیر می‌گذارند. در همین ارتباط، شرایط تسهیل‌کننده در شکل‌دهی رفتار افراد اهمیت دارد.

هدف اصلی تحقیق عبارت است از: ارائه مدل اشتراک‌گذاری دانش امنیت اطلاعات در سازمان متشکل از تئوری‌های رفتار برنامه‌ریزی شده، تئوری انگیزش، مدل تریاندیس، و مراحل تغییر رفتار با ترکیب روش آماری و روش‌شناسی مدل‌سازی و شبیه‌سازی مبتنی بر عامل[2]

اهداف فرعی تحقیق عبارت‌اند از:

- تعیین مؤلفه‌های مدل اشتراک‌گذاری دانش امنیت اطلاعات در سازمان
- بررسی نقش زمان در مدل اشتراک‌گذاری دانش امنیت اطلاعات در سازمان
- تعیین میزان تأثیر نگرش (عامل تئوری رفتار برنامه‌ریزی شده) بر هر مرحله از تغییر رفتار اشتراک‌گذاری امنیت اطلاعات
- تعیین میزان تأثیر هنجارهای ذهنی (عامل تئوری رفتار برنامه‌ریزی شده) بر هر مرحله از تغییر رفتار اشتراک‌گذاری امنیت اطلاعات
- تعیین میزان تأثیر کنترل رفتاری درک شده (عامل تئوری رفتار برنامه‌ریزی شده) بر هر مرحله از تغییر رفتار اشتراک‌گذاری امنیت اطلاعات
- تعیین میزان تأثیر قصد (عامل تئوری رفتار برنامه‌ریزی شده) بر هر مرحله از تغییر رفتار اشتراک‌گذاری امنیت اطلاعات
- تعیین میزان تأثیر شرایط تسهیل‌کننده (عامل مدل ترایاندیس) بر هر مرحله از تغییر رفتار اشتراک‌گذاری امنیت اطلاعات
- تعیین میزان تأثیر انگیزش درونی (عامل تئوری انگیزش) بر هر مرحله از تغییر رفتار

1. ISKS
2. Agent based Modeling

اشتراک‌گذاری امنیت اطلاعات

- تعیین میزان تأثیر انگیزش بیرونی (عامل تئوری انگیزش) بر هر مرحله از تغییر رفتار اشتراک‌گذاری امنیت اطلاعات
- نوآوری‌های این تحقیق را می‌توان به شرح ذیل در دو بخش نظری و کاربردی مطرح کرد:

الف) نوآوری‌های نظری

- استفاده از مدل‌سازی مبتنی بر عامل[1] برای تجزیه‌وتحلیل نتایج شبیه‌سازی تأثیرات عوامل تعیین‌شده سه نظریه رفتار برنامه‌ریزی شده، تریاندیس و انگیزش بر روی مراحل تغییر رفتاری به اشتراک‌گذاری امنیت اطلاعات
- استفاده از مدل‌سازی معادلات ساختاری[2] به‌منظور ایجاد مدل‌هایی به‌عنوان ورودی‌های مدل‌سازی مبتنی بر عامل تا بدین‌وسیله قابلیت اطمینان و اعتبار مدل‌سازی مبتنی بر عامل ارتقا یابد. مدل‌سازی معادلات ساختاری تأثیر عوامل تعیین‌شده از سه نظریه رفتار برنامه-ریزی شده، تریاندیس و انگیزش را بر مراحل تغییر رفتاری به اشتراک‌گذاری دانش امنیت اطلاعات شناسایی می‌کند.
- در این تحقیق با استفاده مدل‌سازی معادلات ساختاری در کنار مدل‌سازی مبتنی بر عامل، هر فرضیه تثبیت‌شده در مدل معادلات ساختاری خود، در طی زمان توسط مدل‌سازی مبتنی بر عامل آزمون می‌شود که باعث می‌شود، این تحقیق از سایر تحقیقاتی که فقط بر روی آزمون‌های آماری و تثبیت فرضیات متمرکز بوده‌اند، متمایز باشد.
- مدل مراحل تغییر که توسط پروچسکا[3] و دی کلمنته[4] در سال ۱۹۸۳ پیشنهاد شده است، در این تحقیق به‌منظور تجزیه‌وتحلیل تغییر رفتاری به اشتراک‌گذاری دانش امنیت اطلاعات اعمال شده است.

1. Agent based Modeling (ABM)
2. Structural Equation Modeling (SEM)
3. Prochaska
4. DiClemente

ب) نوآوری‌های عملی

جنبه‌های انسانی امنیت اطلاعات در این حوزه بسیار حائز اهمیت است. رویکردهای متفاوتی در مطالعات قبلی موردبحث و بررسی قرار گرفته است. بااین‌وجود؛ تحقیقات اندکی وجود دارد که به اشتراک‌گذاری دانش امنیت اطلاعات را در سازمان‌ها به‌عنوان عامل بازدارنده خطرات امنیتی موردبررسی قرار داده باشد. فرهنگ به اشتراک‌گذاری دانش به‌عنوان یک ارزش برای سازمان در نظر گرفته می‌شود که آگاهی از امنیت اطلاعات در سازمان را افزایش می‌دهد و هم‌زمان هزینه امنیت اطلاعات در شرکت‌ها را کاهش خواهد داد. یافته‌ها نشان می‌دهد که نگرش، هنجارهای ذهنی، کنترل رفتاری درک شده، نیت، انگیزه درونی و بیرونی و شرایط تسهیل‌کننده می‌تواند تأثیرات مثبتی روی مراحل تغییر رفتار داشته باشد، این مراحل عبارت‌اند از پیش تأمل، تأمل، آماده‌سازی، اقدام، نگهداری و خاتمه؛ بنابراین مدیرانی که قصد دارند به اشتراک‌گذاری دانش امنیت اطلاعات را به‌عنوان یک ارزش در سازمان‌های خود ارتقا بدهند باید بر روی بهبود و تقویت این فاکتورها تمرکز کنند.

ادامه مقاله به شرح زیر سازمان‌دهی شده است؛ مطالعات موجود در بخش دوم مرور و بررسی شده است، مدل مفهومی اتخاذشده مبتنی بر مطالعات در بخش سوم آمده است، روش‌شناسی در بخش چهارم و نتایج شبیه‌سازی و آماری مدل پیشنهادی در بخش پنجم ارائه شده است و در انتها، نتیجه‌گیری و ارائه پیشنهادات در بخش ششم آورده شده است.

ادبیات نظری

۱- امنیت اطلاعات

اطلاعات مجموعه‌ای از داده‌هاست که دارای معنی و هدف باشند؛ بنابراین اطلاعات به هر نوع از داده‌های معنی‌دار نظیر اطلاعات چاپی، کاغذی، الکترونیکی، صوتی و تصویری گفته می‌شود و حتی شامل گفتمان‌های شفاهی بین افراد نیز می‌تواند باشد. امنیت اطلاعات، فرایند حفاظت از اطلاعات در مقابل کارهای غیرمجاز شامل دسترسی، استفاده، افشا، اختلال، تغییر، مطالعه، بازرسی، ضبط، یا تخریب می‌باشد. در این تعریف، واژه غیرمجاز اشاره به نامطلوب و مضر بودن

دارد. بر این اساس، اگر افراد مجاز دسترسی به اطلاعات مرتبط نداشته باشند نیز کاری نامطلوب صورت گرفته است و برای تصمیم‌گیری‌های سازمانی مضر است.

امروزه، یکی از اولویت‌های اصلی مدیران افزایش امنیت اطلاعات در سازمان‌ها می‌باشد. سازمان ملل متحد در سال ۲۰۰۵ گزارش داده است که نگرانی‌های مربوط به امنیت اطلاعات، صدها میلیارد دلار آسیب به اقتصاد جهان وارد کرده است. آمار دقیقی از آسیب‌های اقتصادی در ایران وجود ندارد، اما برای مثال، بر اساس اطلاعاتی که توسط سایمنتک[1] منتشر شده است، حدود ۶ درصد از سیستم‌های کامپیوتری که با ویروس استاکس نت درگیر می‌شوند؛ در ایران قرار گرفته‌اند، این وضعیت حاکی از آن است که در سازمان‌های ایران، نیاز مبرمی به امنیت وجود دارد (جعفری و همکاران، ۲۰۱۶).

در طی دهه اخیر، برنامه‌های امنیت اطلاعات به‌آرامی تکامل یافته‌اند تا هر دو جنبه فنی و انسانی حفاظت از تهدیدات امنیتی، شناسایی و کنترل شوند (وانگ[2] و همکاران، ۲۰۱۹). تمرکز بسیاری از برنامه‌های امنیت اطلاعات از یک برنامه صرفاً فنی به یک برنامه اجتماعی - فنی تغییر کرده است. این برنامه‌ها همچنان به ایجاد راه‌حل‌هایی پیرامون زیرساخت‌های فنی یک سازمان ادامه می‌دهند، اما اکنون به پتانسیل کارکنان به‌عنوان اهداف حمله نیز توجه می‌کنند (فلورس[3] و همکاران، ۲۰۱۴).

بسیاری از مطالعاتی که در سال‌های اخیر در حوزه تطابق و پذیرش کارکنان سازمان با سیاست‌های امنیت اطلاعات صورت گرفته است، بر مبنای روان‌شناختی از جمله تئوری‌های رفتار برنامه‌ریزی شده[4]، اقدام مستدل[5]، انگیزش درونی و بیرونی، انگیزش محافظت[6]، شبکه اجتماعی و عوامل تأثیرگذار بر پذیرش سیاست‌ها بوده است (اسفندیارپور و اکبری، ۱۳۹۵). تئوری رفتار برنامه‌ریزی شده بیشترین میزان کاربرد را در بین تئوری‌ها داشته است (لبک[7] و همکاران، ۲۰۱۴).

1. Symantec
2. Wang
3. Rocha Flores
4. Theory of Planned Behavior (TPB)
5. Theory of reasoned action
6. Protection Motivation Theory
7. Lebek

۲- دانش امنیت اطلاعات

دانش امنیت اطلاعات به اطلاعات و دانش در مورد شیوه‌ها و استراتژی‌های سازمانی اشاره دارد که می‌تواند از دارایی‌های اطلاعاتی سازمان مانند داده‌های مشتری، اطلاعات محصول و اطلاعات فروش محافظت کند (فلورس و همکاران، ۲۰۱۴). دلایل متعددی وجود دارد که چرا کارکنان ممکن است دانش امنیت اطلاعات را نداشته باشند. این ممکن است به دلیل مشارکت سطح پایین کارکنان در هنگام توسعه سیاست‌های امنیت اطلاعات یا نحوه ابلاغ قوانین و مقررات به آن‌ها در خصوص مسئولیتشان در قبال حفاظت از دارایی‌های اطلاعاتی باشد (جانستون[1] و همکاران، ۲۰۱۹). تحقیقات اخیر همچنین به تکنیک‌های ناکارآمد برای ایجاد انگیزه، درگیر کردن و آموزش کارکنان برای عمل ایمن هنگام کار با سیستم‌های سازمانی و داده‌های آن‌ها اشاره می‌کند. مسائلی که می‌تواند تلاش‌های انطباق یک سازمان را خنثی کند و فرهنگ امنیت آن‌ها را کاهش دهد یا از بین ببرد (سیلیک و لوری[2]، ۲۰۱۹).

تا زمانی که کارکنان به دانش کافی امنیت اطلاعات مجهز نباشند، سازمان‌ها به مبارزه برای دفاع از خود ادامه خواهند داد. یکی از راه‌هایی که سازمان‌ها با این مشکل برخورد کرده‌اند، به اشتراک‌گذاری دانش امنیت اطلاعات است (حسن دوست و همکاران، ۲۰۲۲). برای اینکه سازمان‌ها دانش امنیت اطلاعات کارکنان خود و توانایی بعدی برای کمک به دفاع از خود را بهبود بخشند، نیاز اساسی به ایجاد روش‌های مؤثر به اشتراک‌گذاری دانش امنیت اطلاعات وجود دارد.

۳- به اشتراک‌گذاری (تسهیم) دانش

به اشتراک‌گذاری دانش را به شکل ارائه و دریافت دانش تعریف می‌کنند. وقتی گفته می‌شود که شخصی دانش خود را به اشتراک می‌گذارد، این بدان معنی است که آن فرد با استفاده از دانش، نگرش و افکار خود، فرد دیگری را راهنمایی می‌کند تا موقعیت آن فرد را ارتقا بدهد (سرلک و اسلامی، ۱۳۹۰). علاوه بر این، فردی که دانش خود را به اشتراک می‌گذارد باید از

1. Johnston
2. Silic and Lowry

هدف دانشی که به اشتراک گذاشته می‌شود و کاربرد آن آگاهی داشته باشد، همچنین باید از نیازهای اطلاعاتی و خلأهای فردی که دانش را دریافت می‌کند، شناخت داشته باشد.

به اشتراک‌گذاری دانش، فعالیتی پیچیده و ارزشمند است که پایه و اساس بسیاری از اقدامات مهم مدیریت دانش را تشکیل می‌دهد. موفقیت در فعالیت‌های مدیریت دانش مستقیماً به موفقیت در به اشتراک‌گذاری دانش مرتبط می‌شود (وانگ و نئو[1]، ۲۰۱۰). دستیابی به یک سیستم کارآمد به اشتراک‌گذاری دانش و محقق کردن مدیریت مؤثر دانش در یک سازمان، رشد و بالندگی سازمان را تضمین می‌کند. داشتن نگرش مثبت به مقوله به اشتراک‌گذاری دانش توسط کارکنان می‌تواند منجر به ایجاد فرصت‌ها و نوآوری‌های جدیدی در سازمان شود. از سوی دیگر، اگر دانش پنهان درون ذهن کارکنان به‌صورت مؤثر و کارآمد به اشتراک گذاشته نشود، در طول زمان درون ذهن کارکنان محو می‌شود و کارآمدی خود را از دست می‌دهد (پور و مرتضوی، ۱۳۹۲).

۴- به اشتراک‌گذاری (تسهیم) دانش امنیت اطلاعات

نتایج مطالعات فلورس و همکاران (۲۰۱۴) نشان می‌دهد که مکانیسم‌های به اشتراک‌گذاری دانش امنیت اطلاعات تأثیر مستقیم و زیادی در به وجود آوردن به اشتراک‌گذاری دانش درون سازمان‌ها دارد. فلدی[2] و همکاران (۲۰۱۳) نشان داده‌اند که مانع اصلی برای به اشتراک‌گذاری دانش، عدم ایجاد انگیزه در کارکنان است. استانتون[3] و همکاران (۲۰۰۵) مدلی را پیشنهاد کرده‌اند که دو بعد تخصص و نیت رفتار امنیتی کاربران را در برمی‌گیرد.

زیبا و بانگیووانی[4] (۲۰۲۲) چارچوبی برای مدیریت ریسک دانش ارائه کرده‌اند. آن‌ها دانش را دارایی در نظر گرفته‌اند که به دلیل حملات و خطرات سایبری در ارتباط با از دست دادن دانش، سازمان باید تلاش‌هایی در پیاده‌سازی مدیریت دانش و فرایندهای آن مانند تسهیم دانش در زمینه سازمانی انجام دهد. حسن دوست و همکاران (۲۰۲۲) بیان کرده‌اند که به اشتراک‌گذاری دانش امنیت اطلاعات بین کارکنان عاملی مهم در ارتقای توانایی سازمانی برای محافظت خود از هرگونه تهدیداتی است.

---

1. Wang & Noe
2. Feledi
3. Stanton
4. Zieba & Bongiovanni

۱-۴- تئوری رفتار برنامه‌ریزی شده

فنگ[1] و همکاران (۲۰۲۱) یک مدل از تئوری رفتار برنامه‌ریزی شده به وجود آورده‌اند که نشان‌دهنده عواملی است که روی تمایل کاربران برای به اشتراک‌گذاری دانش تأثیر می‌گذارد. آن‌ها نشان داده‌اند که این مدل توانایی توصیفی دارد، علاوه بر این ایجاد احساس خودکارآمدی و جوایز مادی می‌تواند بر نگرش در مورد به اشتراک‌گذاری دانش تأثیر مثبت بگذارد. افشار جلیلی و قلعه[2] (۲۰۲۰) به کار گرفتن تئوری رفتار برنامه‌ریزی شده در پیش‌بینی رفتار به اشتراک‌گذاری دانش را توضیح داده‌اند. اوبرنوویچ[3] و همکاران (۲۰۲۰) از تئوری رفتار برنامه‌ریزی شده استفاده کرده‌اند تا رفتار تلویحی به اشتراک‌گذاری دانش را توضیح بدهند. بلو و اویکونل[4] (۲۰۱۴) از تئوری رفتار برنامه‌ریزی شده استفاده کرده و نشان داده‌اند که نگرش، نیت و انگیزه می‌تواند رفتار به اشتراک‌گذاری دانش را تحت تأثیر قرار دهد.

۲-۴- تئوری کنش مستدل

با توسعه تئوری کنش مستدل که در آن سازه کنترل رفتاری درک شده توسط آجزن[5] در سال ۱۹۸۵ به‌عنوان عامل تعیین‌کننده رفتار و مقاصد رفتاری معرفی شده است، تئوری رفتار برنامه‌ریزی شده با این سازه می‌تواند رفتارهای غیرارادی را پیش‌بینی کند (مادن[6] و همکاران، ۱۹۹۲). کنترل رفتاری درک شده، درک محدودیت‌های رفتاری درونی (اطلاعات، مهارت‌ها و توانایی‌های شخصی برای انجام کار) و بیرونی (فرصت‌ها، منابع و امکانات انجام کار) را ارائه می‌کند. هنجارهای ذهنی به آن فشار اجتماعی اطلاق می‌شود که شخص برای انجام دادن یا ندادن کار موردنظر متحمل می‌شود. افراد معمولاً بر اساس درک خودشان از آنچه دیگران، مانند دوستان، خانواده، همکاران و امثالهم فکر می‌کنند که آن‌ها باید انجام بدهند؛ رفتار می‌کنند و نیت آن‌ها برای پذیرش رفتاری که باید انجام بدهند به‌طور بالقوه تحت تأثیر کسانی هستند که روابط نزدیکی با ایشان داشته باشند (ماتیسون[7]، ۱۹۹۱). نگرش یک احساس مثبت یا منفی در مورد رفتار موردنظر

1. Feng
2. Afshar Jalili and Ghaleh
3. Obrenovic
4. Bello and Oyekunle
5. Ajzen
6. Madden
7. Mathieson

می‌باشد (فیش باین و آجزن[1]، ۱۹۷۵). قصد رفتاری به نیت، قصد و اراده شخص برای انجام رفتار موردنظر اطلاق می‌شود (موریس و دیلون[2]، ۱۹۹۷).

۳-۴- مدل تریاندیس

تیم و لی[3] (۲۰۱۲)، مدل تریاندیس را اصلاح کرده و توسعه داده‌اند تا روابط ساختاری بین توانمندسازها، فرآیند و نتایج به اشتراک‌گذاری دانش را توضیح دهند. تریاندیس نقش کلیدی‌ای که عوامل اجتماعی و احساسی در به وجود آوردن هدف ایفا می‌کنند، تشخیص داده و شناسایی نمود. وی همچنین بر اهمیت رفتار گذشته نسبت به حال تأکید نمود. موضوع مهم دیگر آن است که عادت‌ها نیز بر روی رفتار فرد تأثیر می‌گذارد. بر اساس مطالعات تریاندیس، رفتار در هر موقعیتی تابعی از قصد و نیت، بخشی از واکنش‌هایی که ناشی از عادت‌های فرد هستند و بخشی از محدودیت‌ها و شرایط وابسته به موقعیت می‌باشد. تریاندیس نقش عوامل احساسی در قصد و نیت رفتاری را مشخص کردند.

۴-۴- انگیزش درونی و بیرونی

نگوین[4] و همکاران (۲۰۱۹) دریافته‌اند که انگیزه‌های درونی و بیرونی بر تسهیم دانش تأثیر می گذارد. گاگنه[5] (۲۰۰۹) بر اساس تئوری رفتار برنامه‌ریزی شده و نظریه خودمختاری، مدل انگیزه به اشتراک‌گذاری دانش را پیشنهاد نموده‌اند. انگیزه‌های درونی از درون فرد نشئت می‌گیرند درحالی‌که انگیزه‌های بیرونی منشأ در محیط خارج دارند. انگیزه درونی به مواردی گفته می‌شود که در آن فرد پس از انجام یک رفتار خاص انتظار دارد که از یک منبع در درون خود، پاداش و جایزه دریافت کند؛ یعنی فرد کار خاصی را انجام می‌دهد تا به پاداشی درونی دست پیدا کند. انگیزه خارجی به زمانی گفته می‌شود که منبع تقویت آن رفتار خاص یا ارائه پاداش به ازای انجام آن رفتار، یک عامل خارجی باشد؛ یعنی فرد رفتار خاصی را انجام می‌دهد تا یک حالت یا شرایط ویژه بیرونی را به دست آورد.

---

1. Fishbein and Ajzen
2. Morris and Dillon
3. Tim and Lee
4. Nguyen
5. Gagne

۵- مراحل تغییر رفتار

تمرکز مراحل مدل تغییر (پروچاسکا و دیکلمنت، ۱۹۸۳: ۱۹۸۶) بر این موضوع است که چگونه می‌توان آگاهانه تصمیمات را تغییر داد. این مدل تأکید می‌کند که تغییر اصلاً ساده نیست. ممکن است افراد به مدت طولانی در یک مرحله باقی بمانند، برخی ممکن است هرگز نتوانند به هدف خود برسند. این مدل را می‌توان در موقعیت‌های متفاوت برای رفتارهای اعتیادآور انجام داد. در این مدل برای ایجاد تغییر در رفتار، ۶ مرحله معرفی می‌شود که به شرح زیر هستند:

- پیش تأمل: در این مرحله، برنامه‌ای برای ایجاد یک تغییر مثبت در ۶ ماه آینده وجود ندارد. تنها زمانی که فرد مزایای تغییر را درک کرده و تشخیص بدهد، آنگاه می‌تواند به مرحله بعدی برود.
- تأمل: در این مرحله فرد به این موضوع می‌اندیشید که مزایای تغییراتی که منجر به تغییر عادت‌های وی شود ممکن است سودمند باشد؛ اما اغلب به این موضوع فکر می‌کند که انجام این تغییرات چقدر سخت و دشوار است. این مرحله ممکن است زمان زیادی طول بکشد، برای مثال: یک سال یا حتی بیشتر. کلید عبور از این مرحله آن است که یک ایده انتزاعی را به یک باور تبدیل کنید.
- آماده‌سازی: در این مرحله، برنامه‌ریزی انجام شده است. این مرحله کوتاه است و بیشتر از چند هفته طول نمی‌کشد.
- عمل یا اقدام: در این مرحله باید به تصمیم بر اجرای برنامه‌ریزی عمل شود. این مرحله نیز اغلب چندین ماه طول می‌کشد؛ اما حقیقت آن است که فرآیند تغییر مدت‌ها قبل آغاز شده است.
- نگهداری/ حفظ: چند ماه بعد از مرحله عمل، تمرکز بر روی چگونگی حفظ و نگهداری این شرایط است. فرد باید محرک‌های قدیمی خود را بشناسد و آگاهانه عادت‌های جدید خود را حفظ کند. اگر در این مرحله اقدامات ضروری اتخاذ نشود، عادت‌های جدید ادامه پیدا نمی‌کنند. زمانی که عادت‌های جدید برای مدتی طولانی مثلاً یک ماه حفظ شدند، فرد می‌تواند وارد مرحله بعدی شود. حفظ و نگهداری عادت‌ها می‌تواند یک چالش دشوار باشد؛ زیرا یک مجموعه جدید از عادت‌ها نیازمند تثبیت تغییرات است.

- خاتمه: هر کسی نمی‌تواند به این نقطه برسد. در این مرحله، تعهد کامل به عادت جدید به وجود آمده و اطمینان از عدم بازگشت به عادت‌های قبلی نیز وجود دارد. اغلب مردم همیشه در مرحله حفظ و نگهداری باقی می‌مانند؛ زیرا زمان بسیار زیادی طول می‌کشد تا یک عادت جدید برای فرد طبیعی شده و به یک رفتار خودکار تبدیل شود که تا همیشه ادامه پیدا کند. ممکن است چندین سال طول بکشد که افراد بتوانند به مرحله خاتمه برسند.

پیشینه تحقیق

بر اساس نظریه نونهادها[1] و یک بررسی میدانی چندمطالعه‌ای از ۸۳۴ مدیر حرفه‌ای در ایالات متحده، حسن دوست و همکاران (۲۰۲۲)، مدلی را توسعه داده و آزمایش کردند که استقرار شیوه‌های تسهیم دانش امنیت اطلاعات را در یک سازمان به‌عنوان حاصل نیروهای نهادی وابسته به سازمان توضیح می‌دهد. یافته‌های آن‌ها همچنین بر اهمیت ایجاد شیوه‌های تسهیم دانش امنیت اطلاعات برای حصول اطمینان از انطباق کارکنان با سیاست‌های امنیت اطلاعات و فرهنگ مؤثر امنیتی تأکید می‌کند.

دلونا[2] و همکاران (۲۰۱۸) در تحقیقی به بررسی پذیرش پرداخت تلفن همراه با توجه به فناوری اعمال شده پرداخته‌اند. نتایج این تحقیق نشان داده که در هریک از نظام‌های پرداخت موبایلی خدمات پیام کوتاه[3] (SMS)، ارتباط میدان نزدیک[4] (NFC) و پاسخ سریع[5] (QR)، هنجارهای ذهنی تأثیر قابل‌توجهی بر قصد استفاده، سهولت استفاده و سودمندی درک شده دارند. سهولت استفاده، سودمندی دستگاه‌های پرداخت و نگرش مصرف‌کننده را تعیین می‌کند و سودمندی درک شده مصرف‌کنندگان با نگرش آن‌ها و قصد استفاده از روش‌های پرداخت تلفن همراه مرتبط است. همچنین نتایج نشان داده که نگرش مستقیماً قصد استفاده را تعیین می‌کند و امنیت درک شده بر رفتار مصرف‌کننده (قصد استفاده) تأثیر مثبت می‌گذارد.

1. Neo-institutional theory
2. de Luna
3. Short Message Service
4. Near Field Communication
5. Quick Response

اشتراک دانش به دلیل تأثیر مثبت آن بر آگاهی از امنیت اطلاعات کارکنان، نقش مهمی در حوزه امنیت اطلاعات ایفا می‌کند. اذعان می‌شود که آگاهی از امنیت مهم‌ترین عاملی است که خطر نقض امنیت اطلاعات در سازمان‌ها را کاهش می‌دهد. در تحقیق صفا و سولمز (۲۰۱۶)، مدلی ارائه شده است که نشان می‌دهد چگونه اشتراک دانش امنیت اطلاعات شکل می‌گیرد و خطر حوادث امنیت اطلاعات را کاهش می‌دهد. نظریه انگیزه و نظریه رفتار برنامه‌ریزی شده در کنار مدل تریاندیس به‌عنوان ستون فقرات نظری چارچوب مفهومی به کار گرفته شد. نتایج تجزیه‌وتحلیل داده‌ها نشان داد که کسب شهرت و ارتقاء به‌عنوان انگیزه بیرونی و رضایت از کنجکاوی به‌عنوان انگیزه درونی بر نگرش کارکنان نسبت به تسهیم دانش امنیت اطلاعات تأثیر مثبت دارد. بااین‌حال، رضایت از خود ارزشی[1] بر نگرش تسهیم دانش امنیت اطلاعات تأثیر نمی‌گذارد. علاوه بر این، یافته‌ها نشان داد که نگرش، کنترل رفتاری درک شده و هنجارهای ذهنی تأثیر مثبتی بر قصد تسهیم دانش امنیت اطلاعات دارند و قصد تسهیم دانش امنیت اطلاعات بر رفتار تسهیم دانش امنیت اطلاعات تأثیر می‌گذارد. نتایج همچنین نشان داد که حمایت سازمانی بر رفتار تسهیم دانش امنیت اطلاعات بیش از اعتماد تأثیر می‌گذارد.

آزاد (۱۳۹۲) در تحقیقی به بررسی فاکتورهای مؤثر بر پذیرش فناوری‌های جدید اطلاعات در شرکت با استفاده از مدل پذیرش فناوری پرداخته است. نتایج این تحقیق نشان می‌دهد که برداشت ذهنی کارکنان نسبت به مفید بودن، برداشت ذهنی کارکنان نسبت به‌آسانی استفاده فن‌آوری‌های جدید، نگرش به کاربرد فن‌آوری‌های جدید، تصمیم به استفاده و استفاده عملی کارکنان از فناوری بر میزان پذیرش این فناوری‌ها اثر معنی‌دار داشته است.

جدول ۱ مطالعاتی که در خصوص تئوری‌های ذکرشده انجام شده است را فهرست‌وار نشان می‌دهد.

1. self-worth

جدول ۱. مطالعات استفاده شده در تئوری‌ها

مرجع	توضیحات
صفا و سولمز (۲۰۱۶)	به اشتراک‌گذاری دانش امنیت اطلاعات تحت دو تئوری اصلی ارائه شده است: رفتار برنامه‌ریزی شده و انگیزه؛ و مدل تریاندیس با در نظر گرفتن شرایط تسهیل‌کننده در سازمان‌ها به بهبود و ارتقای مدل کمک کرده است.
بولگورجو[1] و همکاران (۲۰۱۰)	تئوری رفتار برنامه‌ریزی شده را به کار گرفته است تا تأثیر باورهای کارکنان را بر روی پیامدهای تطبیق یا عدم تطبیق با سیاست‌های امنیت اطلاعات بررسی کنند.
بولگورجو و همکاران (۲۰۰۹)	تأثیر دو عامل آگاهی از امنیت اطلاعات و شناخت نیازهای سیاست امنیت اطلاعات را با استفاده از تئوری رفتار برنامه‌ریزی شده بررسی شده است.
ایفیندو[2] (۲۰۱۲)	تأثیر اعتمادبه‌نفس، هنجارهای ذهنی، اثربخشی پاسخ، درک آسیب‌پذیری، ذهنیت مربوط به پاداش تطبیق‌دهی و هزینه پاسخ‌دهی را توسط یک مدل یکپارچه با استفاده از تئوری رفتار برنامه‌ریزی شده و تئوری انگیزش بررسی شده است.
سیپونن[3] و همکاران (۲۰۰۶)	تئوری انگیزش با فاکتورهایی مانند شفافیت، هنجارهای ذهنی اتخاذ شده است تا قصد و نیت برای پذیرش و اتخاذ سیاست‌های امنیت اطلاعات بررسی شود.
پهنیلا[4] و همکاران (۲۰۰۷)	یک مدل تئوری با استفاده از تئوری‌های اقدام مستدل و انگیزش که فاکتورهای تأثیرگذار بر سیاست امنیت اطلاعات را نیز شامل می‌شود؛ اتخاذ شده است.
پروچاسکا و دی کلمنت (۱۹۸۳)	مراحل و رویه‌های خود تغییر عادت سیگار کشیدن مدل‌سازی شده است.

به‌طورکلی، بر اساس مروری که بر روی مطالعات حاضر صورت گرفته است، مطالعه صفا و سولمز (۲۰۱۶) تنها تحقیقی است که حاصل از ترکیب سه تئوری رفتار برنامه‌ریزی شده، مدل تریاندیس، تئوری انگیزش درونی و بیرونی است. این در حالی است که مطالعه‌ای وجود ندارد که از ترکیب تئوری رفتار برنامه‌ریزی شده، مدل تریاندیس، تئوری انگیزش درونی و بیرونی و مدل

1 Bulgurcu
2. Ifinedo
3. Siponen
4. Pehnila

تغییر رفتاری، استفاده کرده باشد. به‌طور خاص، این مطالعه بر رفتار به اشتراک‌گذاری دانش امنیت اطلاعات متمرکز شده است

مدل مفهومی

مدل تحقیقاتی که در شکل ۱ نشان داده شده است، ترکیبی از نظریه رفتاری برنامه‌ریزی شده، نظریه انگیزش و مدل تحقیقاتی تریاندیس (صفا و سولمز، ۲۰۱۶) و تئوری تغییر رفتار (پروچاسکا و دی کلمنت، ۱۹۸۳) می‌باشد.

شکل ۱. مدل تحقیقاتی

جداول ۲ و ۳، نشان‌دهنده چارچوب نظری تحقیق بر اساس تحقیقات مرتبط موجود می‌باشد.

جدول ۲. متغیرها و شاخص‌های تئوری‌های رفتار برنامه‌ریزی شده، تئوری انگیزش و تئوری تریاندیس

متغیر	شاخص	مرجع
نگرش	علاقه به تسهیم دانش امنیت اطلاعات	(صفا و سولمز، ۲۰۱۶، اجزن، ۱۹۸۵، متیوسون، ۱۹۹۱، حضری و همکاران، ۲۰۰۸)
	داشتن این طرز فکر که تسهیم دانش امنیت اطلاعات مفید است	
	علاقه به یادگیری دانش امنیت اطلاعات	
	داشتن دانش و تجربیات مرتبط با امنیت اطلاعات	
هنجارهای ذهنی	برقراری ارتباط و مشاوره با همکاران در مورد تسهیم دانش امنیت اطلاعات	
	اعتماد همکاران و سازمان به کارکنانی که دانش امنیت اطلاعات را به اشتراک می‌گذارند	
	سودمندی اطلاعات به‌دست‌آمده در فرایند تسهیم دانش امنیت اطلاعات	
کنترل رفتار درک شده	ایجاد اطمینان از این‌که کارکنان می‌توانند دانش امنیت اطلاعات را بیاموزند و به اشتراک بگذارند	
	ایجاد اطمینان از این‌که کارکنان می‌توانند دانش امنیت اطلاعات را استفاده کنند.	
	ایجاد اطمینان از این‌که کارکنان می‌توانند مشکلات امنیت را شناسایی کنند	
قصد و نیت	داشتن قصد تسهیم دانش امنیت	

متغیر	شاخص	مرجع
	اطلاعات	
	تسهیم دانش امنیت اطلاعات از اولویت بسیار بالایی برخوردار است	
شرایط تسهیل‌کننده	پیاده‌سازی سیستم مدیریت دانش امنیت اطلاعات	(صفا و سولمز، ۲۰۱۶، تریاندیس،۱۹۷۷)
	تعیین و اولویت‌بندی دارایی‌های اطلاعاتی	
	اعتماد بین کارکنان در تسهیم دانش امنیت اطلاعات	
	پشتیبانی مدیریت برای پیاده‌سازی فرایند تسهیم دانش امنیت اطلاعات	
انگیزه‌های درونی	احساس آرامش کارکنان در تسهیم دانش امنیت اطلاعات	(صفا و سولمز، ۲۰۱۶؛ کروز و همکاران، ۲۰۰۹، سان و اسکات، ۲۰۰۵، میفیلد، ۲۰۱۰، چاتزواغلو، ۲۰۰۹، هوآنگ، ۲۰۰۹).
	تلاش کارکنان برای موفقیت در پیاده‌سازی تسهیم دانش امنیت اطلاعات	
	انجام آنچه سازمان از کارکنان انتظار دارد که در تسهیم دانش امنیت اطلاعات انجام بدهند.	
	علاقه‌مندی به تسهیم دانش امنیت اطلاعات	
	ارتباط برقرار کردن و مشاوره دادن به همکاران برای تسهیم دانش امنیت اطلاعات	
	علاقه‌مندی به یادگیری دانش امنیت اطلاعات	
	داشتن این طرز فکر که تسهیم دانش امنیت اطلاعات مفید است.	

متغیر	شاخص	مرجع
انگیزه‌های بیرونی	تخصیص پاداش برای مشارکت در فرایند تسهیم دانش امنیت اطلاعات	
	شناسایی افرادی که در فرایند تسهیم دانش امنیت اطلاعات مشارکت می-کنند.	
	ارتقاء به دلیل مشارکت در فرایند تسهیم دانش امنیت اطلاعات	
	تضمین امنیت شغلی به دلیل مشارکت در فرایند تسهیم دانش امنیت اطلاعات	
	دستیابی به امکانات و شرایط بهتر به دلیل مشارکت در فرایند تسهیم دانش امنیت اطلاعات	
	دستیابی به فرصت‌های آموزشی بهتر به دلیل مشارکت در فرایند تسهیم دانش امنیت اطلاعات	

جدول ۳. متغیرها و شاخص‌های تئوری تغییر رفتار

متغیر	شاخص	مرجع
پیش تأمل	احساس بیهوده بودن در مورد تسهیم دانش امنیت اطلاعات وجود دارد.	(پروچاسکا و دیکلمنته، ۱۹۸۳)
	صرفاً مزایای تسهیم دانش امنیت اطلاعات شناسایی می‌شود.	
تأمل	تأمل بر روی مزایای تسهیم دانش امنیت اطلاعات وجود دارد.	
	تأمل بر روی برنامه تغییر برای تسهیم دانش امنیت اطلاعات وجود دارد.	
آماده‌سازی	حس آمادگی برای تسهیم دانش امنیت اطلاعات سازمانی در شرکت وجود دارد.	
	برنامه‌ریزی برای تسهیم دانش امنیت اطلاعات سازمانی در شرکت انجام می‌شود.	

متغیر	شاخص	مرجع
اقدام	صرفاً تصمیم به اجرای برنامه برای تسهیم دانش امنیت اطلاعات سازمانی در شرکت وجود دارد.	
	الزامات اجرای برنامه برای تسهیم دانش امنیت اطلاعات سازمانی در شرکت فراهم می‌شود.	
نگهداری	برنامه‌ها برای تسهیم دانش امنیت اطلاعات پیاده‌سازی می‌شود.	
	عملکرد برنامه‌های تسهیم دانش امنیت اطلاعات کنترل می‌شود.	
خاتمه	تعهد کامل به پیاده‌سازی برنامه‌های تسهیم دانش امنیت اطلاعات وجود دارد.	
	رفتاری منسجم برای تسهیم دانش امنیت اطلاعات وجود دارد.	

روش‌شناسی

مطالعه حاضر یک بررسی توصیفی از نظر جمع‌آوری داده‌ها می‌باشد و این تحقیق از نوع همبستگی می‌باشد. هدف اصلی تحقیق ارائه مدل به اشتراک‌گذاری دانش امنیت اطلاعات در یک سازمان بر اساس تئوری رفتار برنامه‌ریزی شده، تئوری انگیزش، مدل تریاندیس و مراحل تغییر رفتار با استفاده از مدل معادلات ساختاری همراه با مدل‌سازی مبتنی بر عامل می‌باشد.

موردمطالعه سازمانی دولتی در حوزه فناوری اطلاعات است که مجری طرح‌های ملی فناوری اطلاعات می‌باشد. جمعیت آماری این تحقیق، کارکنان این سازمان هستند که بر اساس آمار به‌دست‌آمده از این سازمان، در سال ۲۰۲۰ تعداد آن‌ها ۵۰۰ نفر بوده است و بر اساس جدول مورگان، تعداد ۲۱۷ نفر نمونه آماری از میان آن‌ها، از طریق نمونه‌برداری تصادفی ساده انتخاب شده است.

جدول ۴. جامعه آماری سازمان موردمطالعه

۵۰ درصد جامعه آماری کارکنان جوان و بین ۳۱ تا ۴۱ سال سن می‌باشند.
۵۰ درصد جامعه آماری، کارکنان دارای مقطع تحصیلی کارشناسی ارشد می‌باشند.
۵۰ درصد جامعه آماری، کارکنان دارای سابقه کاری ۱۶-۲۰ سال می‌باشند.
۵۰ درصد جامعه آماری دارای جایگاه شغلی کارشناسی و کارشناسی ارشد می‌باشند.
تخصص غالب جامعه آماری، کامپیوتر و فناوری اطلاعات می‌باشد.

روش جمع‌آوری اطلاعات و داده‌ها که برای این تحقیق موردنیاز است، به دو شکل زیر انجام می‌شود:

الف) روش کتابخانه‌ای: این روش برای جمع‌آوری موارد و تئوری‌های موردنیاز برای نگارش مطالعات تحقیقی؛ از طریق کتاب‌ها، مقاله‌ها، پایان‌نامه‌ها و اینترنت مورداستفاده قرار گرفته است.

ب) روش میدانی: داده‌های این تحقیق از طریق پرسشنامه جمع‌آوری شده است. بعد از مرور و بررسی مطالعه‌های تئوری، مدل‌های ارائه شده و استفاده از ابعاد و شاخص‌های استخراج‌شده‌ای که چارچوب مفهومی این تحقیق را تشکیل می‌دهند؛ یک پرسشنامه ایجاد شده توسط محقق (جداول ۲ و ۳) به دست می‌آید و پس از اخذ نظرات تخصصی اساتید محترم هیئت‌علمی در حوزه فناوری اطلاعات، پرسشنامه نهایی برای جمع‌آوری داده‌های میدانی اتخاذ می‌شود.

پایایی[1] و روایی[2]

با استفاده از روایی صوری، پرسشنامه به اساتید متخصص ارائه می‌شود تا روایی محتوایی آن تأیید شود و برای مرور جامع‌تر؛ پرسشنامه بین چند تن از کارکنان شرکت توزیع می‌شود. با توجه به روایی ساختاری، میانگین واریانس استخراج شده[3] (AVE) در نرم‌افزار SmartPLS استفاده می‌شود و شرط پذیرش آن است که مقدار متوسط باید بیشتر از ۰/۵ باشد. در یک مطالعه آزمایشی، ۳۰ پرسشنامه بین کارکنان شرکت توزیع شده است. پایایی مرکب[4] (پایایی سازه) و مقادیر ضریب آلفای کرونباخ[5] برای تمام متغیرها محاسبه شده و بیشتر از ۰/۷ هستند. شایان‌ذکر است که پایایی مرکب هر متغیر از مقدار میانگین واریانس استخراج شده آن بیشتر است؛ بنابراین

1. Reliability
2. Validity
3. average variance extracted
4. Composite Reliability (CR)
5. Cronbach`s alpha coefficient

پرسشنامه از روایی همگرا برخوردار است. علاوه بر این، مقدار ضریب آلفای کرونباخ ۰/۹۵ می‌باشد، این نیز نشان‌دهنده پایایی مناسب پرسشنامه می‌باشد. نتایج در جدول ۵ آورده شده است.

جدول ۵. میانگین واریانس استخراج شده و پایایی برای متغیرهای تحقیق

متغیر	میانگین واریانس استخراج شده (AVE)	آلفای کرونباخ	پایایی مرکب (CR)
نگرش	۰/۶۷	۰/۸۳	۰/۸۹
هنجارهای ذهنی	۰/۶۴	۰/۸۱	۰/۸۴
کنترل رفتاری درک شده	۰/۶۴	۰/۸۰	۰/۸۵
قصد	۰/۷۱	۰/۸۱	۰/۸۷
شرط تسهیل‌کننده	۰/۶۹	۰/۸۰	۰/۸۶
انگیزه درونی	۰/۶۳	۰/۸۰	۰/۸۲
انگیزه خارجی	۰/۶۶	۰/۸۱	۰/۸۸
پیش تأمل	۰/۷۱	۰/۷۵	۰/۸۰
تأمل	۰/۶۵	۰/۸۷	۰/۹۲
آماده‌سازی	۰/۶۹	۰/۸۵	۰/۹۰
اقدام	۰/۶۵	۰/۸۳	۰/۸۷
نگهداری	۰/۶۳	۰/۸۱	۰/۸۷
خاتمه	۰/۶۲	۰/۸۰	۰/۸۵
کل		۰/۹۵	

مدل‌سازی معادلات ساختاری برای مدل‌سازی مبتنی بر عامل

۱- مدل‌سازی معادلات ساختاری

مدل‌سازی معادلات ساختاری (SEM) به‌عنوان یک روش آماری چند متغیره به‌منظور برآورد کردن و تخمین زدن و آزمون روابط علّی به کار می‌رود. این روش، تأثیر مشترک یک یا چند متغیر مستقل را بررسی می‌کند که در نمودار مسیر نشان داده می‌شود، بنابراین، گاهی به آن تحلیل مسیر گفته می‌شود. در این مدل‌ها، دو متغیر با نقش‌های مختلف وجود دارد:

(۱) متغیرها یا عوامل پنهان، عناصری نامرئی هستند که آن‌ها را فقط می‌توان از آنچه قابل‌مشاهده باشد، استنباط کرد.

(۲) متغیرهای مشاهده‌شده قابل‌اندازه‌گیری هستند و به مفاهیم پنهان مرتبط می‌شوند.

این مدل از دو بخش تشکیل شده است: (۱) بخش ساختاری مدل که چگونگی ارتباط متغیرهای پنهان را نشان می‌دهد و مدل اندازه‌گیری که نشان می‌دهد، چگونه متغیرهای پنهان با متغیرهای قابل‌مشاهده ارتباط برقرار می‌کنند (هنلین و کاپلان[1]، ۲۰۰۴).

اساساً، SEM یک تجزیه‌وتحلیل چندمتغیری عمومی و قدرتمند از مجموعه تحلیل‌های رگرسیون چند متغیری است که به‌منظور ایجاد یک مدل عمومی خطی استفاده می‌شود تا بتوان با کمک آن مجموعه‌ای از معادلات رگرسیون را به‌صورت هم‌زمان آزمون کرد. این تحلیل برای آنالیز کردن ساختارهای پیچیده داده‌ها و بررسی روابط علّی استفاده می‌شود (ابراهیمی، a 2021).

۲- مدل‌سازی مبتنی بر عامل

مدل‌سازی مبتنی بر عامل (ABM) شبیه‌سازی‌های کامپیوتری هستند که برای مدل‌سازی دینامیک سیستم در سطح عامل‌هایی که عملیات‌های آن را انجام می‌دهند؛ استفاده شده‌اند. این عامل‌ها با یکدیگر و نیز با محیط در ارتباط هستند؛ بنابراین، عملکرد آن‌ها بستگی به ارتباط عامل-ها با یکدیگر و با محیط دارد. نتایج مدل‌سازی مبتنی بر عامل نه‌تنها اطلاعات مفیدی در مورد رفتار سیستم ارائه می‌کند؛ بلکه تعاملات نامرئی به‌ویژه آن‌هایی که منجر به پیامدهای ناخواسته می‌شود را نیز موردبررسی قرار می‌دهد (ابراهیمی، ۲۰۱۹). عامل‌ها در مدل نقش کلیدی ایفا می‌کنند. در مدل‌سازی مبتنی بر عامل هر یک از این عامل‌ها توانایی درک و تحلیل محیط و در نهایت اقدام کردن را دارند (ابراهیمی، 2021b).

۳- به‌کارگیری مدل‌سازی معادلات ساختاری برای شبیه‌سازی و مدل‌سازی مبتنی بر عامل

مدل‌سازی آماری قابل‌اعتماد، یک چالش نوظهور در مدل‌سازی مبتنی بر عامل است. مدل‌سازی معادلات ساختاری به‌عنوان یک مدل آماری قوی برای تجزیه‌وتحلیل رفتار مدل‌سازی

1. Henlein & Kaplan

مبتنی بر عامل معرفی شده است. مدل‌سازی معادلات ساختاری می‌تواند با شرح و توضیح تعاملات بین عامل‌های مختلف، به قابلیت اعتماد و اطمینان مدل‌سازی مبتنی بر عامل قدرت بیشتری ببخشد. مدل‌سازی مبتنی بر عامل با دینامیک پیچیده، روزبه‌روز بیشتر به دنبال نتایج قابل‌اعتماد هستند. اخیراً، سیستم‌های دینامیک یا عامل‌های مرتبط با یکدیگر، تحلیل مدل‌سازی مبتنی بر عامل را پیچیده کرده‌اند. ارائه یک مدل به‌ویژه برای ذینفعان[1] ممکن است برای مدل‌سازی مبتنی بر عامل پیچیده باشد و بنابراین در مورد رفتار مدل شبیه‌سازی، عدم قطعیت وجود دارد. علاوه بر این، تجزیه‌وتحلیل مدل‌سازی مبتنی بر عامل منابع زیادی را مصرف می‌کند.

مدل‌سازی مبتنی بر عامل بر روی پرسش‌های توضیحی در علوم رفتاری و اجتماعی تأکید دارد. بااین‌وجود؛ استفاده از مدل‌های آماری استاندارد می‌تواند برای دستیابی به نتایج قابل‌توجه، ساده‌تر باشد؛ زیرا تأثیرات مربوطه را بر روی سیستم نشان می‌دهد. این تحقیق مدل‌سازی معادلات ساختاری را برای مدل‌سازی مبتنی بر عامل ارائه داده است تا بتوان درک بهتری از رفتار پیچیده مدل شبیه‌سازی به دست آورد. توانایی مدل‌سازی معادلات ساختاری برای تخمین تعاملات و دستیابی به رفتارهای اجتماعی نوظهور پنهان با استفاده از ساختارها و مسیرها به برای مدل‌سازی مبتنی بر عامل و همچنین ارزیابی رفتار مدل شبیه‌سازی‌شده کمک می‌کند. علاوه بر این، نتایج آماری قابل‌اعتماد مبتنی بر مدل‌سازی معادلات ساختاری به توضیح و تفسیر نتایج شبیه‌سازی کمک می‌کند (مرتنز[2] و همکاران، ۲۰۱۷).

ابراهیمی (2021a) مطالعه‌ای را برای بررسی تأثیر مدیریت ارتباط با مشتری[3] (CRM) بر روی دستیابی به خدمات و محصولات نوآورانه با استفاده از مدل‌سازی مبتنی بر عامل ارائه داده است. او تأثیر مؤلفه‌های مدیریت ارتباط با مشتری بر مراحل گسترش و پخش خدمات و محصولات نوآورانه را موردمطالعه قرار داده است. در این تحقیق، وی ابتدا مدل‌سازی مبتنی بر معادلات ساختاری را انجام داده و از نتایج آن در مدل‌سازی مبتنی بر عامل برای شبیه‌سازی استفاده کرده است؛ بنابراین، علاوه بر ارائه مدل شبیه‌سازی، نتایج شبیه‌سازی را نیز می‌توان ارزیابی کرد و توصیفی قابل‌فهم‌تر در اختیار ذی‌نفعان قرار داد.

1. stakeholder
2. Mertens
3. Customer Relationship Management

به‌کارگیری رفتار در مدل‌سازی مبتنی بر عامل در مطالعات گوناگونی شبیه‌سازی شده است (رسول خانی و همکاران، ۲۰۱۷؛ ابراهیمی، ۲۰۲۱ الف، ابراهیمی، ۲۰۲۱ ب). رسول خانی و همکاران (۲۰۱۷) یک چارچوب مدل‌سازی مبتنی بر عامل را به‌منظور شناسایی عوامل گوناگون و رفتارهای پویایی که بر پذیرش فناوری صرفه‌جویی در مصرف آب تأثیر می‌گذارند، اتخاذ نموده‌اند. ابراهیمی (۲۰۲۱ الف) تأثیر مدیریت ارتباط با مشتری بر دستیابی به خدمات و محصولات نوآورانه با استفاده از متدولوژی مدل‌سازی مبتنی بر عامل را بررسی کرده‌اند. مطالعه وی بر پذیرش خدمات و محصولات نوآورانه تمرکز کرده است و تأثیر عوامل مدیریت ارتباط با مشتری در طی زمان بر تغییر رفتار مشتری را نشان داده است. ابراهیمی (۲۰۲۱ ب) تأثیر مدیریت ارتباط با مشتری را بر شرکت‌های دیجیتال بررسی کرده است درحالی‌که با استفاده از مدل‌سازی مبتنی بر عامل در یک فروشگاه دیجیتال، بر فروش دیجیتال متمرکز شده است. در این تحقیق نشان داده‌اند که سیستم مدیریت ارتباط با مشتری منجر به بهبود و تقویت عملکرد شرکت دیجیتال شده است و تمام ابعاد سیستم مدیریت ارتباط با مشتری تأثیر مثبتی بر مراحل فروش دیجیتال دارد.

مطالعه پیش رو، تغییر در رفتار تسهیم دانش امنیت اطلاعات مبتنی بر تأثیرات عوامل مرتبط با تئوری رفتار برنامه‌ریزی شده، تریاندیس و تئوری انگیزه‌های درونی و بیرونی را بررسی کرده است. در این تحقیق، از مدل‌سازی معادلات ساختاری در کنار مدل‌سازی مبتنی بر عامل استفاده شده است که در تعدادی محدود از تحقیقات فعلی این کاربرد دیده می‌شود. از توضیحات این بخش مشخص است که مزیت‌های استفاده از مدل‌سازی معادلات ساختاری در کنار مدل‌سازی مبتنی بر عامل به شرح ذیل می‌باشد:

۱. شناخت تأثیرات عوامل بر تغییر رفتار تسهیم دانش امنیت اطلاعات با کمک مدل‌سازی معادلات ساختاری به‌عنوان ورودی مدل‌سازی و شبیه‌سازی مبتنی بر عامل بر قابلیت اطمینان نتایج می‌افزاید.
۲. استفاده این دو در کنار هم توصیفی قابل‌فهم‌تر در اختیار ذی‌نفعان سازمان موردمطالعه قرار می‌دهد.
۳. تغییر رفتار در طی زمان را ارزیابی می‌شود.
۴. فرضیات در طی زمان قابل تثبیت خواهند بود.

۵. ایجاد سناریو یکی از اهداف این تحقیق نیست؛ بااین‌وجود تقویت و بهبود فاکتورهای تأثیرگذار بر تغییر رفتار را می‌توان به‌عنوان استراتژی‌های بهبود سیستم در نظر گرفت.

۶. بر اساس تحقیق ژیانگ[1] در سال ۲۰۰۵، مقایسه مدل به مدل، تکنیکی است که نتایج مختلف مدل‌سازی را با نتایج مدل‌های دیگر مقایسه می‌کند. در این تحقیق دو مدل شامل معادلات ساختاری و مدل مبتنی بر عامل ارائه شده است که دومی برگرفته از آماری قابل‌اعتماد است با فنون متعدد تائید روایی و پایایی داشته است و این تائیدی بر اعتبار نتایج شبیه‌سازی مبتنی بر عامل است. گنجاندن تکنیک‌های تجزیه‌وتحلیل آماری در فرآیند اعتبار سنجی می‌تواند به‌طور قابل‌توجهی اعتبار مدل را افزایش دهد.

از طرفی، ازآنجایی‌که در زمینه تسهیم دانش امنیت اطلاعات آزمایش‌های تجربی در دنیای واقعی انجام نشده است، نتایج مدل‌سازی مبتنی بر عامل توسط استادان حوزه به اشتراک‌گذاری دانش و امنیت اطلاعات تأیید شده است. همچنین، به‌منظور مقایسه و تحلیل بهتر مدل‌سازی و شبیه‌سازی مبتنی بر عامل با مدل‌سازی معادلات ساختاری، هر فرضیه به‌طور جداگانه در معادلات ساختاری در نظر گرفته شده است.

نتایج

۱- آمار توصیفی

۱-۱- آمار جمعیت شناختی

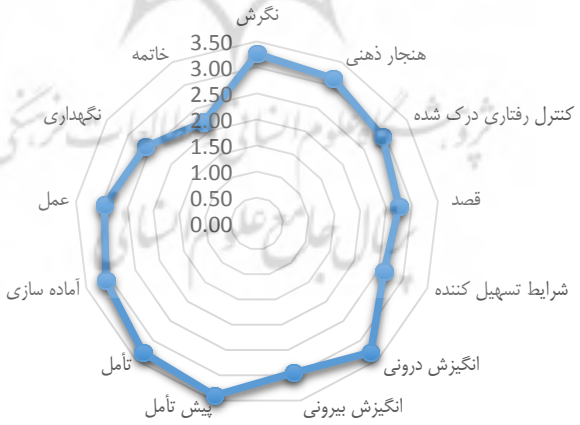
بر اساس مطالعات جمعیت شناختی، کمترین پاسخ‌دهندگان به تعداد ۸۷ نفر با ۰,۴۰ درصد از کل پاسخ‌دهندگان زن هستند و بیشتر پاسخ‌دهندگان به تعداد ۱۳۰ نفر با ۰,۶۰ درصد از کل پاسخ‌دهندگان، مرد هستند. علاوه بر آن، بیشترین مشارکت‌کنندگان به تعداد ۱۰۹ نفر در سنین ۳۱ تا ۴۱ سال یا فراوانی ۰,۵۰ درصد بوده‌اند و سپس سنین ۴۱ تا ۵۱ به تعداد ۱۰۲ نفر با فراوانی ۰,۴۷ درصد و کمترین مشارکت‌کنندگان کمتر از ۳۱ سال به تعداد ۶ نفر با فراوانی ۰,۰۳ بوده‌اند. سنین بالای ۵۱ سال مشارکتی در پاسخ به پرسشنامه نداشتند. در خصوص تحصیلات، بیشترین مشارکت-

1. Xiang

کنندگان دارای تحصیلات کارشناسی ارشد به تعداد ۱۰۲ نفر و فراوانی ۰,۴۷ بوده‌اند و سپس کارشناسی به تعداد ۴۳ نفر و با فراوانی ۰,۲۰ و در نهایت کمترین مشارکت‌کنندگان دارای تحصیلات دکتری و دیپلم، هر کدام به تعداد ۳۶ نفر و با فراوانی ۰,۱۷ بوده‌اند. از منظر سابقه، بیشترین مشارکت‌کنندگان دارای سابقه کاری ۱۶ تا ۲۰ سال به تعداد ۱۱۵ نفر و با فراوانی ۰,۵۳ بوده‌اند و سپس سابقه کاری ۱۱ تا ۱۵ سال به تعداد ۵۰ نفر و با فراوانی ۰,۲۳ و در نهایت کمترین مشارکت‌کنندگان به ترتیب دارای سابقه کاری کمتر از ۱۰ سال به تعداد ۲۹ نفر و با فراوانی ۰,۱۳ و سپس سابقه کاری ۲۱ تا ۲۵ سال به تعداد ۲۳ و با فراوانی ۰,۱۰ بوده‌اند.

۲-۱- میانگین متغیرها

برای تجزیه‌وتحلیل شاخص گرایش به مرکز، یا میانگین مجموعه داده‌های هر متغیر، مشخص شده است که بیشترین میانگین مربوط به انگیزه درونی با مقدار ۳/۳۰ است و سپس نگرش با مقدار ۳/۲۶ قرار گرفته است. علاوه بر این، بیشترین میانگین مراحل تغییر رفتار مربوط به مرحله پیش تأمل با مقدار ۳/۴۰ است، پس‌ازآن مرحله تأمل با ۳/۳۰ قرار دارد. کمترین مقدار میانگین در مورد متغیرهای تأثیرگذار، مرتبط است با شرایط تسهیل‌کننده و برای مراحل تغییر رفتار مربوط به مرحله خاتمه است. میانگین‌های متغیرها در شکل ۲ به نمایش درآمده است.



شکل ۲. میانگین‌های متغیرها

۳-۱-آزمون فرضیه

فرضیه اصلی در این تحقیق آن است که عوامل تئوری رفتار برنامه‌ریزی شده، تئوری انگیزش و مدل تریاندیس مراحل تغییر رفتار در تسهیم دانش امنیت اطلاعات در سازمان را تغییر می‌دهد. به‌منظور آزمون فرضیه اصلی و فرضیه‌های فرعی تحقیق از برازش مدل معادلات ساختاری به روش حداقل مربعات جزئی (PLS) استفاده شده است. در این مدل، روابط بین متغیرهای تحقیق به‌طور هم‌زمان سنجیده شده و میزان سهم هریک از متغیرهای مشاهده شده در تبیین مفاهیم مکنون تحقیق تعیین می‌گردد. در این روش، فرض نرمال بودن توزیع متغیرها ضرورتی ندارد. با توجه به ضرایب تأثیر به‌دست‌آمده از مدل ساختاری تحقیق مشاهده می‌شود که تأثیر هریک از متغیرها (عوامل تئوری‌ها) بر روی متغیرهای وابسته (مراحل تغییر رفتار) در جهت مستقیم برآورد شده است. به‌منظور بررسی معناداری ضرایب به‌دست‌آمده در مدل، قدر مطلق آماره‌های معناداری که دارای توزیع تی-استودنت می‌باشند موردتوجه قرار گرفته‌اند.

جدول ۶. نتایج آزمون فرضیه اصلی

متغیر مستقل	متغیر وابسته	ضریب تأثیر	قدر مطلق آماره t	معناداری	نتیجه
نگرش	پیش تأمل	۰/۲۹	۵/۶۷۸	۰/۰۰۰۱	اثرگذار
نگرش	تأمل	۰/۰۲۲	۷/۱۲۹	۰/۰۰۰۱	اثرگذار
نگرش	آماده‌سازی	۰/۰۴۸	۴/۲۵۰	۰/۰۰۲	اثرگذار
نگرش	اقدام	۰/۱۴۴	۴/۵۹۳	۰/۰۰۰۱	اثرگذار
نگرش	نگهداری	۰/۱۸۰	۳/۶۲۷	۰/۰۰۰۱	اثرگذار
نگرش	خاتمه	۰/۳۴۳	۲/۹۳۴	۰/۰۰۴	اثرگذار
هنجارهای ذهنی	پیش تأمل	۰/۴۵۶	۳/۵۹۱	۰/۰۰۰۱	اثرگذار
هنجارهای ذهنی	تأمل	۰/۳۸۸	۲/۵۴۲	۰/۰۰۰۱	اثرگذار
هنجارهای ذهنی	آماده‌سازی	۰/۳۱۱	۲/۰۶۶	۰/۰۰۰۱	اثرگذار
هنجارهای ذهنی	اقدام	۰/۵۱۵	۲/۸۰	۰/۰۰۰۱	اثرگذار
هنجارهای ذهنی	نگهداری	۰/۵۲۲	۲/۴۵۲	۰/۰۰۰۱	اثرگذار
هنجارهای ذهنی	خاتمه	۰/۲۵۴	۲/۲۱۴	۰/۰۰۰۱	اثرگذار
کنترل رفتار درک شده	پیش تأمل	۰/۵۴۹	۵/۲۰۱	۰/۰۱۶	اثرگذار

متغیر مستقل	متغیر وابسته	ضریب تأثیر	قدر مطلق آماره t	معناداری	نتیجه
کنترل رفتار درک شده	تأمل	۰/۲۵۱	۳/۲۴۷	۰/۰۰۰۱	اثرگذار
کنترل رفتار درک شده	آماده‌سازی	۰/۰۱۲	۳/۲۸۰	۰/۰۰۰۱	اثرگذار
کنترل رفتار درک شده	اقدام	۰/۰۹۰	۲/۳۴۷	۰/۰۰۰۱	اثرگذار
کنترل رفتار درک شده	نگهداری	۰/۵۲۰	۳/۰۹۷	۰/۰۰۰۱	اثرگذار
کنترل رفتار درک شده	خاتمه	۰/۴۵۳	۲/۵۲۳	۰/۰۰۲	اثرگذار
نیت	پیش تأمل	۰/۳۶۷	۳/۲۹۳	۰/۰۰۰۱	اثرگذار
نیت	تأمل	۰/۲۱۶	۳/۲۵۵	۰/۰۰۰۱	اثرگذار
نیت	آماده‌سازی	۰/۲۸۲	۲/۰۵۴	۰/۰۰۰۱	اثرگذار
نیت	اقدام	۰/۱۱۸	۳/۵۴۷	۰/۰۱۶	اثرگذار
نیت	نگهداری	۰/۴۵۹	۳/۰۴۳	۰/۰۰۰۱	اثرگذار
نیت	خاتمه	۰/۳۰۹	۲/۷۱۸	۰/۰۰۰۱	اثرگذار
شرایط تسهیل‌کننده	پیش تأمل	۰/۳۴۲	۲/۸۳۳	۰/۰۰۰۱	اثرگذار
شرایط تسهیل‌کننده	تأمل	۰/۲۸۲	۲/۵۹۲	۰/۰۰۰۱	اثرگذار
شرایط تسهیل‌کننده	آماده‌سازی	۰/۲۷۰	۲/۲۶۳	۰/۰۰۰۱	اثرگذار
شرایط تسهیل‌کننده	اقدام	۰/۳۵۵	۲/۸۰۲	۰/۰۱۶	اثرگذار
شرایط تسهیل‌کننده	نگهداری	۰/۵۳۳	۳/۲۲۲	۰/۰۰۰۱	اثرگذار
شرایط تسهیل‌کننده	خاتمه	۰/۳۲۰	۲/۴۷۲	۰/۰۰۰۱	اثرگذار
انگیزه درونی	پیش تأمل	۰/۲۸۵	۲/۳۹۵	۰/۰۰۰۱	اثرگذار
انگیزه درونی	تأمل	۰/۳۰۱	۲/۹۰۸	۰/۰۱۶	اثرگذار
انگیزه درونی	آماده‌سازی	۰/۳۴۱	۲/۷۸۱	۰/۰۰۰۱	اثرگذار
انگیزه درونی	اقدام	۰/۴۴۶	۲/۹۳۷	۰/۰۰۰۱	اثرگذار
انگیزه درونی	نگهداری	۰/۶۵۳	۴/۱۵۴	۰/۰۰۰۱	اثرگذار
انگیزه درونی	خاتمه	۰/۲۱۰۰	۲/۷۱۶	۰/۰۰۰۱	اثرگذار
انگیزه بیرونی	پیش تأمل	۰/۴۹۷	۳/۶۰	۰/۰۰۰۱	اثرگذار
انگیزه بیرونی	تأمل	۰/۲۷۶	۳/۰۵۰	۰/۰۱۶	اثرگذار
انگیزه بیرونی	آماده‌سازی	۰/۰۸۳	۳/۴۴۸	۰/۰۰۰۱	اثرگذار
انگیزه بیرونی	اقدام	۰/۲۸۵	۳/۹۶۲	۰/۰۰۰۱	اثرگذار
انگیزه بیرونی	نگهداری	۰/۶۵۹	۳/۰۱۴	۰/۰۰۰۱	اثرگذار
انگیزه بیرونی	خاتمه	۰/۸۱۰	۳/۲۰۳	۰/۰۰۰۱	اثرگذار

با توجه به نتایج جدول ۶ مشاهده می‌شود که سطح معناداری اثر هر یک از متغیرها (عوامل تئوری‌ها) بر متغیرهای وابسته (مراحل تغییر رفتار) کمتر از ۰/۰۵ به‌دست‌آمده و نشان از معناداری اثرات مورد برآورد دارد. با توجه به سطوح معناداری و ضرایب تأثیر مثبت مدل خلاصه یافته‌های آزمون اثرات اصلی متغیرها بر روی یکدیگر به این شرح است:

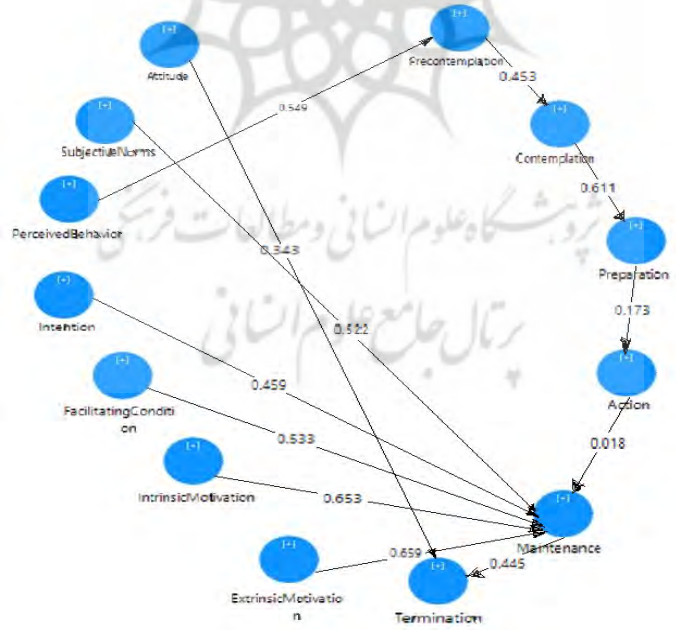
- نگرش (beta = ۰/۲۹)، هنجارهای ذهنی (beta =۰/۴۵۶)، کنترل رفتار درک شده (beta =۰/۵۴۹)، نیت (beta =۰/۳۶۷)، شرایط تسهیل کننده (beta =۰/۳۴۲)، انگیزه درونی (beta =۰/۲۸۵) و انگیزه بیرونی (beta =۰/۴۹۷) بر مرحله پیش تأمل تغییر رفتار تسهیم دانش امنیت اطلاعات تأثیر مستقیم و معناداری دارند.
- نگرش (beta =۰/۰۲۲)، هنجارهای ذهنی (beta =۰/۳۸۸)، کنترل رفتار درک شده (beta =۰/۲۵۱)، نیت (beta =۰/۲۱۶)، شرایط تسهیل کننده (beta =۰/۲۸۲)، انگیزه درونی (beta =۰/۳۰۱) و انگیزه بیرونی (beta =۰/۲۷۶) بر مرحله تأمل تغییر رفتار تسهیم دانش امنیت اطلاعات تأثیر مستقیم و معناداری دارند.
- نگرش (beta =۰/۰۴۸)، هنجارهای ذهنی (beta =۰/۳۱۱)، کنترل رفتار درک شده (beta =۰/۰۱۲)، نیت (beta =۰/۲۸۲)، شرایط تسهیل کننده (beta =۰/۲۷۰)، انگیزه درونی (beta =۰/۳۴۱) و انگیزه بیرونی (beta =۰/۰۸۳) بر مرحله آماده‌سازی تغییر رفتار تسهیم دانش امنیت اطلاعات تأثیر مستقیم و معناداری دارند.
- نگرش (beta =۰/۱۴۴)، هنجارهای ذهنی (beta =۰/۵۱۵)، کنترل رفتار درک شده (beta =۰/۰۹۰)، نیت (beta =۰/۱۱۸)، شرایط تسهیل کننده (beta =۰/۳۵۵)، انگیزه درونی (beta =۰/۴۴۶) و انگیزه بیرونی (beta =۰/۲۸۵) بر مرحله اقدام تغییر رفتار تسهیم دانش امنیت اطلاعات تأثیر مستقیم و معناداری دارند.
- نگرش (beta =۰/۱۴۴)، هنجارهای ذهنی (beta =۰/۵۱۵)، کنترل رفتار درک شده (beta =۰/۰۹۰)، نیت (beta =۰/۱۱۸)، شرایط تسهیل کننده (beta =۰/۳۵۵)، انگیزه درونی (beta =۰/۴۴۶) و انگیزه بیرونی (beta =۰/۲۸۵) بر مرحله اقدام تغییر رفتار تسهیم دانش امنیت اطلاعات تأثیر مستقیم و معناداری دارند.
- نگرش (beta =۰/۱۸۰)، هنجارهای ذهنی (beta =۰/۵۲۲)، کنترل رفتار درک شده

(beta =۰/۵۲۰)، نیت (beta =۰/۴۵۹)، شرایط تسهیل کننده (beta =۰/۵۳۳)، انگیزه درونی (beta =۰/۶۵۳) و انگیزه بیرونی (beta =۰/۶۵۹) بر مرحله نگهداری تغییر رفتار تسهیم دانش امنیت اطلاعات تأثیر مستقیم و معناداری دارند.

- نگرش (beta =۰/۳۴۳)، هنجارهای ذهنی (beta =۰/۲۵۴)، کنترل رفتار درک شده (beta =۰/۴۵۳)، نیت (beta =۰/۳۰۹)، شرایط تسهیل کننده (beta =۰/۳۲۰)، انگیزه درونی (beta =۰/۲۱۰۰) و انگیزه بیرونی (beta =۰/۸۱۰) بر مرحله خاتمه تغییر رفتار تسهیم دانش امنیت اطلاعات تأثیر مستقیم و معناداری دارند.

بنابراین فرضیه‌های فرعی و در نهایت فرضیه اصلی تحقیق در سطح خطای ۰/۰۵ مورد تائید قرار گرفته است.

به دلیل پیچیده بودن روابط مدل همان‌طور که در جدول ۶ توضیح داده شد، شکل ۳ برآورد بیشترین مقادیر ضرایب مدل ساختاری تحقیق را به همراه ضرایب بین مراحل تغییر رفتار تسهیم دانش امنیت اطلاعات (جدول ۷) را نشان می‌دهد.



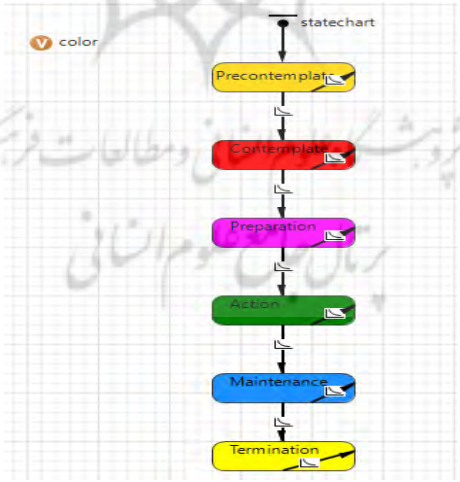
شکل ۳. برآورد بیشترین مقادیر ضرایب مدل ساختاری تحقیق به همراه ضرایب بین مراحل تغییر رفتار تسهیم دانش امنیت اطلاعات

جدول ۷. نتایج بین مراحل تغییر رفتار تسهیم دانش امنیت اطلاعات

متغیر مستقل	متغیر وابسته	ضریب تأثیر	قدر مطلق آماره t	معناداری
پیش تأمل	تأمل	۰/۴۵۳	۳/۱۰۸	۰/۰۰۰۱
تأمل	آماده‌سازی	۰/۶۱۱	۴/۵۵۳	۰/۰۰۰۱
آماده‌سازی	اقدام	۰/۱۷۳	۴/۸۴۶	۰/۰۰۲
اقدام	نگهداری	۰/۰۱۸	۴/۰۶۲	۰/۰۰۰۱
نگهداری	خاتمه	۰/۴۴۵	۲/۰۱۸	۰/۰۰۰۱

۲- نتایج ABM

نرم‌افزار شبیه‌سازی AnyLogic قابلیت‌های گسترده‌ای برای ایجاد و تحلیل مدل‌سازی مبتنی بر عامل را ارائه می‌دهد. همچنین امکان ترسیم رفتار عامل را با استفاده از نمودارهای حالت در نرم‌افزار امکان‌پذیر می‌سازد. در این بخش، نمودار حالت سیستم برای تجزیه‌وتحلیل رفتار عامل‌ها ارائه شده است.



شکل ۴. نمودار حالت سیستم

عامل‌ها کارکنان شرکت هستند. در نمودار حالت[1]، انتقال[2] بین مراحل تغییر رفتار در تسهیم دانش امنیت اطلاعات درون شرکت؛ مشابه با ضرایب استاندارد هستند. علاوه بر این؛ زمان بین هر مرحله در محاسبه نرخ[3] تأثیر دارد. ضرایب استاندارد بر اساس زمان تقسیم شده‌اند و امتیازها برحسب ماه محاسبه شده است. زمان انتقال بین مراحل به شکل زیر است:

- بین پیش تأمل و تأمل، زمان ۶ ماه است.
- بین تأمل و آماده‌سازی، زمان ۱۲ ماه است.
- بین اقدام و نگهداری زمان ۴ ماه است.
- بین نگهداری و خاتمه زمان ۲۴ ماه است.

انتقال‌های به‌کاررفته به‌عنوان امتیاز در هر مرحله نشان‌دهنده تأثیر مؤلفه‌های تئوری رفتار برنامه‌ریزی شده، تئوری انگیزش و مدل تریاندیس بر مراحل تغییر رفتار تسهیم دانش امنیت اطلاعات می‌باشد.

کدهای اصلی نمودار حالت به شکل زیر است:

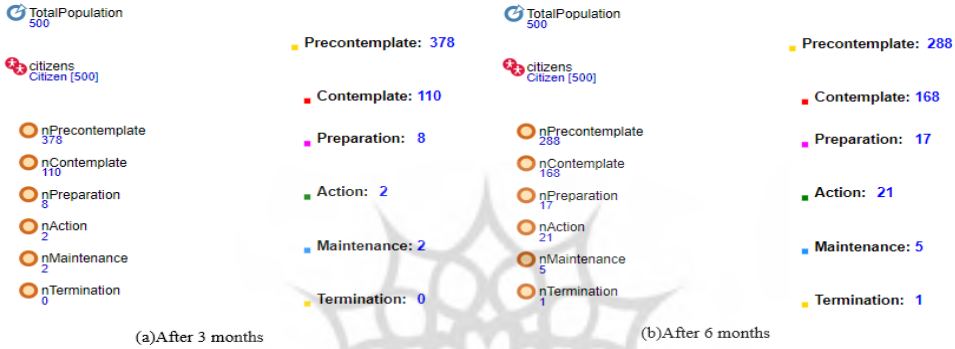
```
Entry action:
get_Main().nPrecontemplate++;
color = GOLD;
Exit action:
get_Main().nPrecontemplate--;

Entry action:
get_Main().nContemplate++;
color = RED;
Exit action:
get_Main().nContemplate--;

Entry action:
get_Main().nPreparation++;
color = MAGENTA;
Exit action:
get_Main().nPreparation--;
```

```
Entry action:
get_Main().nAction++;
color = GREEN;
Exit action:
get_Main().nAction--;

Entry action:
get_Main().nMaintenance++;
color = dodgerBlue;
Exit action:
get_Main().nMaintenance--;

Entry action:
get_Main().nTermination++;
color = yellow;
Exit action:
get_Main().nTermination--;
```

1. State Chart
2. Transition
3. Rate

بر اساس نتایج ضرایب استاندارد مدل‌سازی معادلات ساختاری، مدل‌های فرضیه‌ای، با در نظر گرفتن هر متغیر مربوطه با ۵۰۰ نفر از کارکنان شرکت شبیه‌سازی شده است. نتایج در شکل‌های ۵ تا ۱۱ از نتایج مدل‌سازی مبتنی بر عامل ارائه شده است، به صورتی که زمان تقریباً ۳ ماه و ۶ ماه در نظر گرفته شده است.

▪ شبیه‌سازی فرضیه اول



شکل ۵: نتایج شبیه‌سازی فرضیه اول

شکل a۵ نشان‌دهنده تغییر در رفتار تسهیم دانش امنیت اطلاعات ناشی از نگرش و طرز فکر مربوط به تسهیم دانش امنیت اطلاعات بعد از سه ماه است. واضح است که هیچ‌یک از کارکنان شرکت در مرحله خاتمه قرار نخواهد گرفت. ۲ نفر از کارمندان به مرحله نگهداری رسیده‌اند. ۲ نفر از کارکنان در مرحله اقدام هستند. ۱۱۰ نفر از کارمندان در مرحله تأمل و ۳۷۸ نفر از افراد در مرحله ابتدایی پیش تأمل قرار خواهند گرفت. شکل b۵ نشان‌دهنده تغییرات بعد از ۶ ماه می‌باشد. همان‌طور که شبیه‌سازی نشان می‌دهد، تنها یک نفر از کارکنان شرکت در مرحله خاتمه قرار خواهد گرفت. ۵ نفر در مرحله نگهداری و ۲۱ نفر در مرحله اقدام هستند. ۱۷ نفر از کارکنان نیز در مرحله آماده‌سازی قرار دارند؛ درحالی‌که ۱۶۸ نفر در مرحله تأمل قرار دارند و ۲۸۸ نفر همچنان در مرحله پیش تأمل هستند.

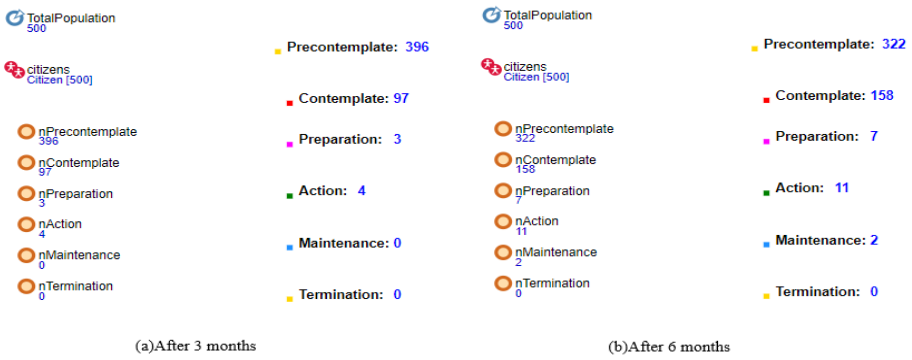
▪ شبیه‌سازی فرضیه دوم

(a)After 3 months (b)After 6 months

شکل ۶. نتایج شبیه‌سازی فرضیه دوم

شکل a۶ نشان‌دهنده تغییر در رفتار تسهیم دانش امنیت اطلاعات است که تحت تأثیر هنجارهای ذهنی تسهیم دانش امنیت اطلاعات بعد از ۳ ماه به وجود آمده است. همان‌طور که نتایج شبیه‌سازی نشان می‌دهد؛ هیچ‌یک از کارکنان شرکت در مرحله خاتمه قرار نگرفته است، همچنین هیچ‌کس به مرحله نگهداری نیز نرسیده است. ۳ نفر در مرحله اقدام هستند، ۶ نفر در مرحله آماده‌سازی، ۸۵ نفر در مرحله تأمل و ۴۰۶ نفر در مرحله پیش تأمل هستند. شکل b۶ نشان‌دهنده تغییرات بعد از ۶ ماه است. همان‌طور که نتایج شبیه‌سازی نشان می‌دهد هیچ‌یک از افراد شرکت بعد از ۶ ماه در مرحله خاتمه قرار نگرفته‌اند و همچنان نیز هیچ‌کس به مرحله نگهداری نرسیده است. ۷ نفر در مرحله اقدام هستند، ۱۳ نفر در مرحله نگهداری، ۱۴۵ نفر در مرحله تأمل و ۳۳۵ نفر در مرحله پیش تأمل قرار دارند.

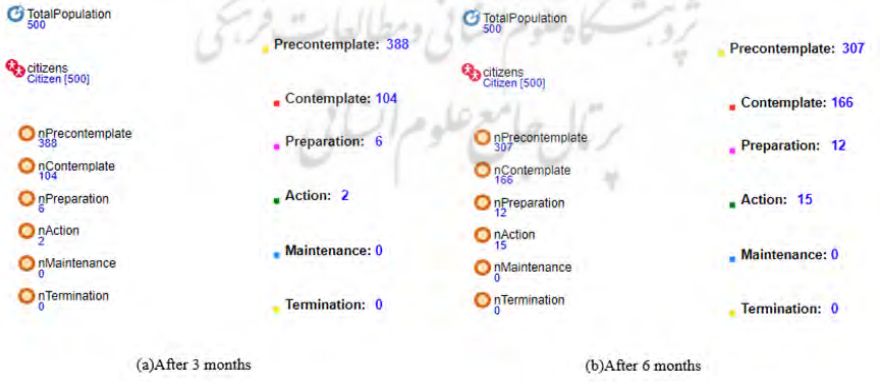
▪ شبیه‌سازی فرضیه سوم



شکل ۷. نتایج شبیه‌سازی فرضیه سوم

شکل a۷ تغییر در رفتار تسهیم دانش امنیت اطلاعات را نشان می‌دهد که تحت تأثیر وجود کنترل رفتار درک شده ISKS بعد از سه ماه ایجاد شده است. همان‌طور که نتایج شبیه‌سازی نشان می‌دهد، هیچ‌یک از کارکنان شرکت بعد از سه ماه نه مرحله خاتمه و نیز در مرحله نگهداری قرار نگرفته‌اند. ۴ نفر در مرحله اقدام هستند و ۳ نفر نیز در مرحله آماده‌سازی قرار دارند. ۹۷ نفر در مرحله تأمل و ۳۹۶ نفر در مرحله پیش تأمل هستند. شکل b۷ تغییر بعد از ۶ ماه را نمایش می‌دهد. تنها ۲ نفر توانسته‌اند که به مرحله نگهداری برسند. ۱۱ نفر در مرحله اقدام قرار دارند، ۷ نفر نیز در مرحله آماده‌سازی می‌باشند. ۱۵۸ نفر در مرحله تأمل و ۳۲۲ نفر در مرحله پیش تأمل هستند.

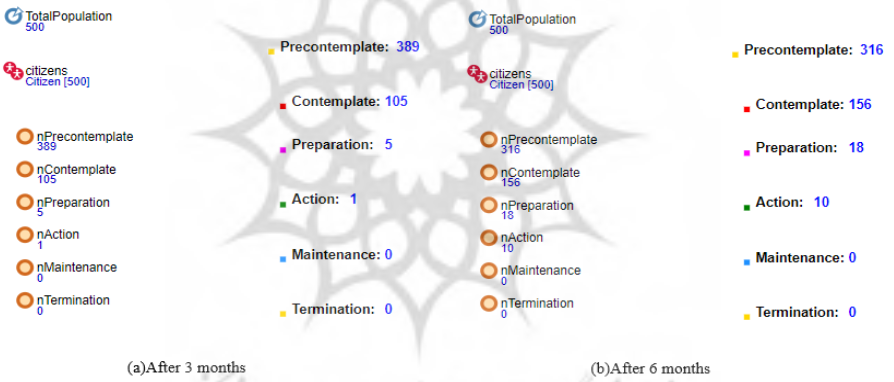
▪ شبیه‌سازی فرضیه چهارم



شکل ۸ نتایج شبیه‌سازی فرضیه چهارم

شکل a۸ تغییرات در رفتار تسهیم دانش امنیت اطلاعات که تحت تأثیر نیت و قصد رفتار تسهیم دانش امنیت اطلاعات بعد از ۳ ماه ایجاد شده است را نمایش می‌دهد. همان‌طور که مشاهده می‌شود، هیچ‌یک از افراد به مرحله خاتمه و یا نگهداری نرسیده‌اند. دو نفر در مرحله اقدام و ۶ نفر در مرحله آماده‌سازی هستند. ۱۰۴ کارمند در مرحله تأمل و ۳۸۸ نفر در مرحله پیش تأمل هستند. شکل b۸ تغییرات بعد از ۶ ماه را نشان می‌دهد. همان‌طور که از روی نتایج شبیه‌سازی مشاهده می‌شود، هیچ‌یک از کارکنان به مرحله خاتمه نرسیده‌اند، به همین ترتیب هیچ‌کدام از آن‌ها نیز در مرحله نگهداری قرار نخواهند گرفت. ۱۵ کارمند در مرحله اقدام و ۱۲ نفر در مرحله آماده‌سازی هستند؛ ۱۶۶ نفر در مرحله تأمل و ۳۰۷ نفر پس از شش ماه در مرحله پیش تأمل قرار گرفته‌اند.

- **شبیه‌سازی فرضیه پنجم**

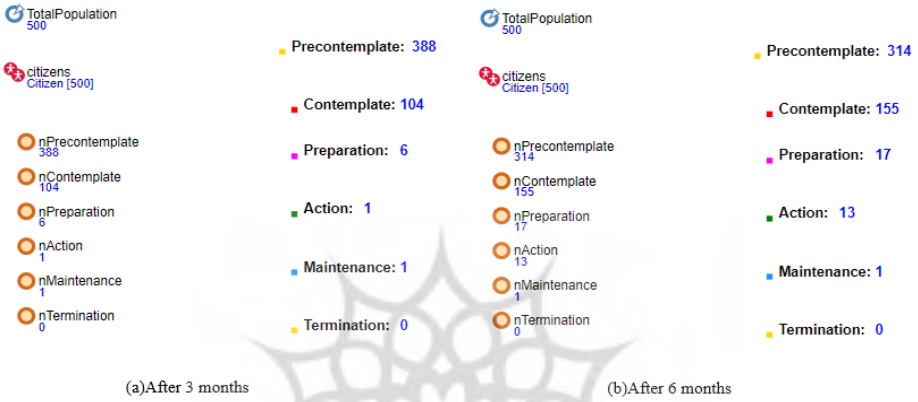


شکل ۹. نتایج شبیه‌سازی فرضیه پنجم

شکل a۹ تغییر در رفتار تسهیم دانش امنیت اطلاعات را نشان می‌دهد که تحت تأثیر شرایط تسهیل‌کننده رفتار تسهیم دانش امنیت اطلاعات بعد از ۳ ماه اتفاق می‌افتد. همان‌طور که نتایج شبیه‌سازی نشان می‌دهد؛ هیچ‌یک از کارکنان شرکت در مرحله خاتمه قرار نگرفته است. همچنین هیچ‌کس نیز در مرحله نگهداری قرار ندارد. ۱ نفر کارمند در مرحله اقدام است. ۵ نفر از کارمندان در مرحله آماده‌سازی قرار دارند، ۱۰۵ نفر در مرحله تأمل و ۳۸۹ نفر در مرحله پیش تأمل قرار گرفته‌اند. شکل b۹ نشان‌دهنده تغییرات بعد از ۶ ماه است. همان‌طور که نتایج شبیه‌سازی نشان می-

دهد؛ هیچ‌کدام از افراد به مرحله خاتمه نرسیده‌اند، همچنین هیچ‌کدام به مرحله نگهداری نیز نرسیده‌اند. ده نفر از کارکنان در مرحله اقدام قرار گرفته‌اند. ۱۸ نفر از کارمندان در مرحله آماده‌سازی، ۱۵۶ کارمند در مرحله تأمل و ۳۱۶ نفر در مرحله پیش تأمل قرار گرفته‌اند.

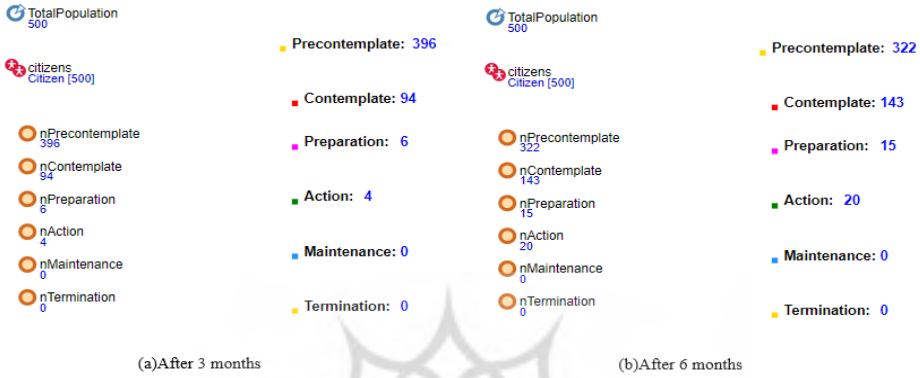
- **نتایج شبیه‌سازی فرضیه ششم**



شکل ۱۰. نتایج شبیه‌سازی فرضیه ششم

شکل a۱۰ تغییر در رفتار تسهیم دانش امنیت اطلاعات را نشان می‌دهد که تحت تأثیر انگیزه‌های درونی برای به اشتراک گذاشتن دانش امنیت اطلاعات بعد از ۳ ماه اتفاق می‌افتد. همان‌طور که نتایج شبیه‌سازی نشان می‌دهد؛ هیچ‌یک از کارکنان شرکت در مرحله خاتمه قرار نگرفته است. تنها یک نفر به مرحله نگهداری رسیده است. ۱ نفر کارمند در مرحله اقدام است. ۶ نفر از کارمندان در مرحله آماده‌سازی قرار دارند، ۱۰۴ نفر در مرحله تأمل و ۳۸۸ نفر در مرحله پیش تأمل قرار گرفته‌اند. شکل b۱۰ نشان‌دهنده تغییرات بعد از ۶ ماه است. همان‌طور که نتایج شبیه‌سازی نشان می‌دهد؛ هیچ‌کدام از افراد به مرحله خاتمه دست نیافته‌اند، تنها یک نفر به مرحله نگهداری رسیده است؛ ۱۳ نفر از کارکنان در مرحله اقدام قرار گرفته‌اند. ۱۷ نفر از کارمندان در مرحله آماده‌سازی، ۱۵۵ کارمند در مرحله تأمل و ۳۱۴ نفر در مرحله پیش تأمل قرار گرفته‌اند.

- **شبیه‌سازی فرضیه هفتم**



شکل ۱۱. نتایج شبیه‌سازی فرضیه هفتم

شکل a۱۱ نشان‌دهنده تغییرات در رفتار تسهیم دانش امنیت اطلاعات است که تحت تأثیر انگیزه‌های بیرون برای به اشتراک گذاری دانش امنیت اطلاعات بعد از سه ماه به وجود آمده است. همان‌طور که نتایج نشان می‌دهد هیچ‌یک از افراد شرکت در مرحله خاتمه قرار نگرفته‌اند. همچنین هیچ‌کدام از افراد به مرحله نگهداری نیز نرسیده‌اند. ۴ نفر در مرحله اقدام هستند. ۶ نفر در مرحله آماده‌سازی، ۹۴ نفر از کارمندان در مرحله تأمل و ۳۹۶ نفر در مرحله پیش تأمل قرار دارند. شکل b۱۱ نشان‌دهنده تغییرات بعد از ۶ ماه است. همان‌طور که نتایج شبیه‌سازی نشان می‌دهد، هیچ‌یک از کارکنان به مرحله خاتمه نرسیده‌اند؛ همچنین هیچ‌کدام از کارمندان در مرحله نگهداری قرار نگرفته‌اند. ۱۵ نفر از کارمندان در مرحله آماده‌سازی، ۱۴۳ نفر در مرحله تأمل و ۳۲۲ نفر در مرحله پیش تأمل قرار دارند.

۳- بحث و بررسی

نتایج این شبیه‌سازی نشان داد که همان‌طور که در تجزیه‌وتحلیل آماری ارائه شده است، متغیرها بر رفتار تسهیم دانش امنیت اطلاعات و تغییر رفتار افراد در طول زمان تأثیر مثبت می‌گذارند.

جدول ۸. تغییر رفتار در طول زمان

	ماه	پیش تأمل	تأمل	آماده‌سازی	اقدام	نگهداری	خاتمه
نگرش	۳	۳۷۸	۱۱۰	۸	۲	۲	۰
	۶	۲۸۸	۱۶۸	۱۷	۲۱	۵	۱
هنجارهای ذهنی	۳	۴۰۶	۸۵	۶	۳	۰	۰
	۶	۳۳۵	۱۴۵	۱۳	۷	۰	۰
کنترل رفتار درک شده	۳	۳۹۶	۹۷	۳	۴	۰	۰
	۶	۳۲۲	۱۵۸	۷	۱۱	۲	۰
نیت	۳	۳۸۸	۱۰۴	۶	۲	۰	۰
	۶	۳۰۷	۱۶۶	۱۲	۱۵	۰	۰
شرایط تسهیل‌کننده	۳	۳۸۹	۱۰۵	۵	۱	۰	۰
	۶	۳۱۶	۱۵۶	۱۸	۱۰	۰	۰
انگیزه درونی	۳	۳۸۸	۱۰۴	۶	۱	۱	۰
	۶	۳۱۴	۱۵۵	۱۷	۱۳	۱	۰
انگیزه بیرونی	۳	۳۹۶	۹۴	۶	۴	۰	۰
	۶	۳۲۲	۱۴۳	۱۵	۲۰	۰	۰

هدف اصلی استفاده از مدل‌سازی مبتنی بر عامل بر اساس یکی از اهداف فرعی تحقیق، بررسی اثرگذاری عوامل تئوری‌های مختلف (رفتار برنامه‌ریزی شده، تریاندیس و انگیزه‌های درونی و بیرونی) بر روی مراحل تغییر رفتار تسهیم دانش امنیت اطلاعات در طی زمان است. در این مطالعه، سناریوسازی را نمی‌توان انجام داد زیرا امتیازها، ضرایب تأثیر هستند. بااین‌وجود، استراتژی‌های زیر با در نظر داشتن به اشتراک‌گذاری دانش امنیت اطلاعات سازمان، توصیه شده است.

- بهبود و تقویت نگرش و طرز فکر کارمندان

- بهبود و تقویت هنجارهای ذهنی کارکنان
- بهبود و تقویت کنترل رفتار درک شده کارکنان
- بهبود و تقویت قصد و نیت رفتاری کارکنان
- بهبود و تقویت شرایط تسهیل‌کننده سازمان
- بهبود و تقویت انگیزه درونی کارمندان
- بهبود و تقویت انگیزه‌های بیرونی کارمندان

در بخش پیشنهادات، برای بهبود و تقویت این عوامل پیشنهادهایی مطرح شده است.

نتیجه‌گیری

در این مطالعه؛ مدل به اشتراک‌گذاری دانش امنیت اطلاعات (ISKS) پیشنهاد شده است که بر اساس تئوری‌های رفتار برنامه‌ریزی شده، تئوری انگیزش و مدل تریاندیس طراحی شده است. برای تجزیه‌وتحلیل این مدل در یک سازمانی که در حوزه فنّاوری اطلاعات کار می‌کند، روش آماری مدل‌سازی معادلات ساختاری (SEM) و مدل‌سازی مبتنی بر عامل (ABM) و متدولوژی شبیه‌سازی اعمال شده است. تئوری رفتار برنامه‌ریزی شده شامل عواملی مانند نگرش، هنجارهای ذهنی، کنترل رفتار درک شده و نیت را شامل می‌شود؛ تئوری انگیزش شامل عوامل انگیزه‌های درونی و بیرونی می‌شود، مدل تریاندیس نیز شرایط تسهیل‌کننده را در برمی‌گیرد، تئوری تغییر رفتار نیز مراحل پیش تأمل، تأمل، آماده‌سازی، اقدام، نگهداری و خاتمه را شامل می‌شود. داده‌ها از طریق پرسشنامه‌ای که توسط محقق طراحی شده، با استفاده از نمونه‌گیری تصادفی ساده از بین ۲۱۷ شرکت‌کننده جمع‌آوری شده است. روایی و پایایی پرسشنامه تست شده است، فرضیه‌ها مدل‌سازی و ارزیابی شده، سپس هر یک از آن‌ها شبیه‌سازی شده است. همان‌طور که تجزیه‌وتحلیل آماری تأیید کرده است؛ شبیه‌سازی نیز نشان می‌دهد که متغیرها بر روی تغییر رفتار ISKS در طول زمان تأثیرگذار هستند.

دلالت‌ها[1] و معانی که از نتیجه این تحقیق آشکار می‌شود را می‌توان به دو مفاهیم نظری و مدیریتی تقسیم کرد که به شرح ذیل می‌باشد:

1. implications

۱. دلالت نظری: صفا و سولمز (۲۰۱۶) اذعان داشته‌اند که نگرش، کنترل رفتار درک شده و هنجارهای ذهنی تأثیر قابل‌توجهی بر روی نیت و قصد تسهیم دانش امنیت اطلاعات می‌گذارند، نیت تغییر تسهیم دانش امنیت اطلاعات نیز بر روی رفتار تسهیم دانش امنیت اطلاعات تأثیر مثبت می‌گذارد؛ علاوه بر این، آن‌ها نشان دادند که عوامل انگیزه‌ای بر روی تسهیم دانش امنیت اطلاعات تأثیر مثبت می‌گذارد. آن‌ها نشان داده‌اند که حمایت و پشتیبانی سازمانی بر روی رفتار تسهیم دانش امنیت اطلاعات تأثیرگذار است. مطالعه آن‌ها تنها تحقیقی بوده است که در آن سه تئوری رفتار برنامه‌ریزی شده، مدل تریاندیس و تئوری انگیزش در آن مورداستفاده قرار گرفته است و نتایجی که آن‌ها به دست آورده‌اند با نتایج به‌دست‌آمده در این تحقیق، همخوانی دارد.

۲. دلالت مدیریتی: ازآنجایی‌که به اشتراک‌گذاری دانش به‌عنوان یک فرآیند مهم مدیریت دانش در نظر گرفته می‌شود و امنیت اطلاعات نقش اصلی در کاهش حوادث امنیتی را ایفا می‌کند، مدیران می‌توانند عواملی که رفتار تسهیم دانش امنیت اطلاعات را مجدد تحت تأثیر قرار می‌دهند، در سازمان خودشان تقویت کنند. شناخت این عوامل، در تغییر تسهیم دانش امنیت اطلاعات نقش کلیدی ایفا می‌کند. نتیجه‌های به‌دست‌آمده تأکید کرده‌اند که نگرش مثبت، هنجارهای ذهنی، کنترل رفتار درک شده، نیت، انگیزه‌های درونی و بیرونی و شرایط تسهیل‌کننده بر روی مراحل تغییر رفتار از جمله پیش تأمل، تأمل، آماده‌سازی، اقدام، نگهداری و خاتمه تأثیر مثبت می‌گذارد.

بر اساس نتایج آماری، (۱) نگرش بیشترین میزان تأثیر را مرحله خاتمه تغییر رفتار تسهیم دانش امنیت اطلاعات داشته است؛ به عبارتی به افزایش دانش و تجربه حوزه امنیت اطلاعات در افراد و افزایش علاقه‌مندی آن‌ها با برگزاری کلاس‌های آموزشی و بهره‌گیری از مکانیزم‌های انگیزشی می‌توان تعهد به پیاده‌سازی برنامه‌های تسهیم دانش امنیت اطلاعات و داشتن رفتاری منسجم برای تسهیم دانش امنیت اطلاعات را افزایش داد. (۲) کنترل رفتار درک شده بیشترین میزان اثر را بر مرحله پیش تأمل دارد؛ به عبارتی هر چه اطمینان سازمان از مشارکت کارکنان در تسهیم دانش امنیت اطلاعات افزایش یابد، مزایای تسهیم دانش امنیت در سازمان برای استقرار آن بررسی و شناخته می‌شود؛ بنابراین سازمان می‌تواند با افزایش اطلاعات، مهارت‌ها و توانایی‌های شخصی کارکنان در حوزه امنیت اطلاعات با برگزاری دوره‌های آموزشی، این اطمینان را افزایش دهد.

(۳) سایر عوامل بر مرحله نگهداری بیشترین میزان تأثیر را دارند. به عبارتی سایر عوامل بیشترین اثر را بر پیاده‌سازی برنامه‌های تسهیم دانش امنیت اطلاعات و کنترل عملکرد آن دارند؛ لذا سازمان با برنامه‌های الف) بهبود نظام منابع انسانی (مانند جذب کارکنان مسلط به امنیت اطلاعات و افرادی که تمایل به تسهیم دانش دارند، ارتقای کارکنانی که در این فرایند مشارکت دارند و مدیریت عملکرد کارکنان با توجه با شاخص مشارکت در تسهیم دانش امنیت اطلاعات)، ب) برنامه‌های آموزشی و سنجش اثربخش آن‌ها و ج) استفاده از مکانیزم‌های انگیزشی درونی و بیرونی مانند ارتقا، شناخت و پاداش پولی می‌تواند بر پیاده‌سازی برنامه‌های تسهیم دانش امنیت اطلاعات و کنترل عملکرد آن اثرگذار باشد.

بر اساس نتایج حاصل از مدل‌سازی و شبیه‌سازی مبتنی بر عامل:

- به‌منظور بهبود و تقویت نگرش، هنجارهای ذهنی، کنترل رفتار درک شده و قصد رفتاری کارکنان، سازمان باید دوره‌های آموزشی‌ای مانند امنیت اطلاعات، مدیریت دانش، شبکه، مهندسی اجتماعی و از این قبیل را در سازمان برنامه‌ریزی و اجرا نماید.
- به‌منظور بهبود و تقویت نگرش، هنجارهای ذهنی، کنترل رفتار درک شده و قصد رفتاری کارکنان، سازمان باید بازنگری در نظام مدیریت منابع انسانی خود داشته باشد که این نظام متشکل از زیرسیستم‌هایی مانند جذب کارکنان، ارتقا و مدیریت عملکرد کارکنان است. به عبارتی سازمان باید کارکنان مسلط به امنیت اطلاعات و افرادی که تمایل به تسهیم دانش دارند را جذب کند، کارکنانی که در این فرایند مشارکت دارند را ارتقا دهد و ارزیابی عملکرد کارکنان را با توجه با شاخص مشارکت در تسهیم دانش امنیت اطلاعات انجام دهد.
- به‌منظور بهبود و تقویت شرایط تسهیل‌کننده سازمان، سازمان برای ساده‌سازی به اشتراک‌گذاری دانش و به‌خصوص تسهیم دانش امنیت اطلاعات می‌تواند راهکارهایی مانند سامانه مدیریت دانش، شیرپوینت و گروه‌های مجازی و حضوری را اتخاذ کند تا بلکه بدین‌وسیله شرایط تسهیم دانش امنیت اطلاعات تسهیل شود.
- در راستای بهبود و تقویت انگیزه درونی و بیرونی کارمندان و به‌منظور بهبود و تقویت شرایط تسهیل‌کننده سازمان، سازمان باید برای به اشتراک‌گذاری دانش امنیت اطلاعات،

مکانیزم‌های انگیزشی درونی و بیرونی را به کار ببندد. به‌عنوان مثال می‌تواند برنامه‌های تقدیر از کارکنانی که در تسهیم دانش امنیت اطلاعات پیشتاز بودند را اجرا کند، پاداش مالی به‌طور ویژه برای کسانی که در تسهیم دانش امنیت اطلاعات در سازمان مشارکت می‌کنند، تخصیص داده شود.

- به‌منظور بهبود و تقویت شرایط تسهیل‌کننده سازمان، یک تیم در سازمان باید مسئولیت امنیت اطلاعات را به عهده بگیرد؛ یک تیم نیز باید به‌منظور مدیریت دانش در سازمان ایجاد شود؛ و اگر امکان دارد بهتر است که برای این منظور ساختاری ایجاد شود.
- به‌منظور بهبود و تقویت شرایط تسهیل‌کننده سازمان، به مدیران توصیه می‌شود که به‌منظور انتقال دانش و استفاده از تجربه کارکنان باتجربه برای دیگر کارکنان در زمینه امنیت اطلاعات، بیشتر سرمایه‌گذاری کنند.
- به‌منظور بهبود و تقویت نگرش، هنجارهای ذهنی، کنترل رفتار درک شده و قصد رفتاری کارکنان، سازمان باید افراد آموزش‌دیده در زمینه امنیت اطلاعات و مدیریت دانش را به کار بگیرد. حتی ممکن است لازم باشد که مدیران در این حوزه نقش مربیان را ایفا کنند.
- تاکنون در تحقیقات تسهیم دانش امنیت اطلاعات، از روش‌شناسی‌های مدل‌سازی و شبیه‌سازی استفاده نشده بود. پس‌ازاین تحقیق، پیشنهادهایی برای تحقیقات آینده در ادامه آورده شده است:
- ABM را می‌توان روی تنها فقط یک تئوری مانند تئوری رفتار برنامه‌ریزی شده پیاده‌سازی کرد.
- یک شبیه‌سازی ترکیبی را می‌توان به کار گرفت.
- به‌جای ABM دیگر روش‌های شبیه‌سازی مانند دینامیک‌های سیستم را می‌توان به کار گرفت.
- در مطالعه پیش رو؛ با استفاده از پرسشنامه سعی بر این بود که با ایجاد انگیزه در پاسخ‌دهنده‌ها و ارائه توضیح کافی در مورد هدف تحقیق، خطاهای احتمالی تحقیق به حداقل رسانده شود. یکی از محدودیت‌های این تحقیق آن است که نتایج تحقیق را نمی‌توان به سازمان‌های دیگر تعمیم داد و به دلیل جمعیت آماری محدود، نتایج این تحقیق

تنها به سازمان تحت مطالعه مربوط می‌شود و برای به کار بردن در سازمان‌های دیگر، مدل باید تطبیق داده شود.

فهرست منابع

آزاد، حسین. (۱۳۹۲). بررسی فاکتورهای مؤثر بر پذیرش فناوری‌های جدید اطلاعات در شرکت با استفاده از مدل پذیرش فناوری(TAM) ؛ (مطالعه موردی: اداره بازرگانی بندرعباس). پایان‌نامه کارشناسی ارشد، دانشکده علوم انسانی، دانشگاه هرمزگان.

اسفندیارپور، زهرا، اکبری، مرتضی. ۱۳۹۵. شناسایی الگوهای ذهنی کارمندان در خصوص سیاست های امنیت اطلاعات. دانشکده مدیریت دانشگاه تهران.دوره ۸، شماره ۲، ۲۱۵ تا ۲۳۰.

پور، سمیرا، و مرتضوی، سعید. ۱۳۹۲. تبیین عوامل مؤثر بر نگرش و رفتار مبتنی بر تسهیم دانش ، مورد مطالعه پرستاران بیمارستان ۱۷ شهریور. فصلنامه مطالعات رفتار سامانی. سال دوم، شماره ۳. ۷۳- ۴۵.

سرلک، محمد علی، و اسلامی، طاهره. ۱۳۹۰. تسهیم دانش در دانشگاه صنعتی شریف با رویکرد سرمایه اجتماعیو نشریه مدیریت دولتیو دوره ۳، شماره ۸، ۱۸- ۱.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M.H. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review, 37 (12), 1049-1092

Wang, Sheng, Raymond A. Noe. 2010. Knowledge sharing: A review and directions for future research. Human Resource Management Review 20: 115–131.

Xiang, X., Kennedy, R., Madey, G. (2005). Verification and validation of agent-based scientific simulation models. Retrieved 18 May 2021 on https://www3.nd.edu/~nom/Papers/ADS019_Xiang.pdf

Afshar Jalili, Y., & Ghaleh, S. (2020). Knowledge sharing and the theory of planned behavior: a meta-analysis review. VINE Journal of Information and Knowledge Management Systems, Vol. 51, No. 2, pp. 2059-5891.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. Kuhl J. and Beckmann J. (Eds.). Action-Control: From Cognition to Behavior (pp. 11-39). Springer, Heidelberg.

Al-Ahmari, S, Renaud, K., & Omoronyia, I. (2018). A systematic review of information security knowledge-sharing research. Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018), 101-110.

Amabile, T. A. (1993). Motivational synergy: Toward new conceptualizations of intrinsic and extrinsic motivation in workplace. Human Resource Management Review, Vol. 3, No. 3, pp.185-201.

Australian Computer Society. (2016). Cybersecurity threats challenges opportunities, Sydney, Australia.

Bello, O. W., Y Oyekunle, R. A. (2014). Attitude, perceptions, motivation towards knowledge sharing: views from universities in kwara state. African Journal of Library, Vol. 24, No. 2, pp. 123-134.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, Vol. 34, No. 3, pp. 523-548.

Bulgurcu, B., Cavusoglu, H. & Benbasat, L. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. Americas Conference on Information Systems, AMCIS2009, San Francisco, California.

Chatzoglou, V. (2009). Knowledge-sharing behavior of bank employees in Greece. Business Process Management Journal, Vol. 15, No. 2, pp. 245-266.

,,,,, ,, 2009). The influence of employee motivation on knowledge transfer. Journal of Knowledge Management, Vol. 13, No. 6, pp. 478-490.

D'Arcy, J., Anat H., & Dennis G. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, Vol. 20, No.1, pp. 79-98.

de Luna I. R., Liébana-Cabanillas F., Sánchez-Fernández J., & Muñoz-Leiva F. (2019). Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied. Technological Forecasting and Social Change, Vol 146, 931-944.

Ebrahimi, M. (2019). An analysis of the impact of business networks on technology development: Using agent-based modeling. Ebrahimi, M. (Eds.). Private Sector Innovations and Technological Growth in the MENA Region (pp. 20-44), IGI Global, USA.

Ebrahimi, M. (2021a). Analysis of the impact of customer relationship management on innovation acquisition using agent-based modeling", Amini, A., Bushell, S., and Mahmood, A. (Eds.). Driving Innovation and Productivity Through Sustainable Automation (1-28), IGI Global, USA.

Ebrahimi, M. (2021b). Analysis of the effect for customer relationship management on digital enterprises: Using agent-based modeling", Sandhu, K. (Eds.). Emerging Challenges, Solutions, and Best Practices for Digital Enterprise Transformation (pp. 138-163), IGI Global, USA.

Feng, X., Wang, L., Yan, Y., Zhang, Q., Sun, L., Chen, J., & Wu, Y. (2021). The sustainability of knowledge-sharing behavior based on the theory of planned behavior in Q&A social network community. Special Issue of Collective Behavior Analysis and Graph Mining in Social Networks, Complexity, Vol. 2021, Article ID 1526199, pp. 1-12.

Fishbein, M., & Ajzen, I. (1975). Belief, attitudes, intention and behavior: An introduction to theory and research. Reading, Addison-Wesley, MA.

Feledi, D., Fenz, S. & Lechner, L. (2013) Toward web-based information security

knowledge sharing. Information Security Technical Report, Vol. 17, No. 4, pp. 199-209.

Flores, W.R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, Vol. 43, pp. 90-110.

Gagne, M. (2009). A model of knowledge-sharing motivation. Human Resource Management, Vol. 48, No. 4, pp. 571-589.

Hassabdoust, F., Subasinghage, M., & Johnston, A.C. (2022). A neo-institutional perspective on the establishment of information security knowledge sharing practices. Information & Management, Vol.59, pp. 1-11.

Hazari, S., Hargrave, W., & Clenney, B. (2008). An empirical investigation of factors influencing information security behavior. Journal of Information Privacy & Security, Vol. 4, No. 4, pp. 3-20.

Hnnlei Kapla,, A. (2004) A beginnrr's guid prr tial letst sqrrr s analysis. Understanding Statistics, Vol. 3, No. 4, pp. 283–297.

Huang, C.C. (2009). Knowledge sharing and group cohesiveness on performance: an empirical study of technology R&D teams in Taiwan. Technovation, Vol. 29, pp. 786-797.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, Vol. 31, No. 1, pp. 83-95.

Johnston, A.C., Warkentin, M., Dennis, A.R., & Siponen, M. (2019). Speak their langaag dnsigning efftct iv m ss g s improv employe s' ioformtt inn security decision making. Decision Sciences, Vol. 50 No. 2, pp. 245-264.

Madden, T.J., Ellen, P.S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. Personality and Social Psychology Bulletin, Vol. 18, No. 3, pp. 3-9.

Mathieson, K. (1991). Predicting user intentions: Comparing the technology acceptance model with the theory of planned behavior. Information Systems Research, Vol. 2, No. 3, pp. 173-191.

Mayfield, M. (2010). Tacit knowledge sharing: techniques for putting a powerful tool in practice. Development and Learning in Organizations, Vol. 24, No. 1, pp. 24-26.

Mertens, K.G., Lorscheid, I., & Meyer, M. (2017). Using structural equation-based modeling for agent-based models. Chan, W. K. V., D'Ambrogio, A., Zacharewicz, G., Mustafee, N., Wainer, G., & Page, E. (Eds.). Proceedings of the 2017 Winter Simulation Conference.

Morris, M.G., & Dillon, A. (1997). How user perceptions influence software use. IEEE Software, Vol. 14, No. 4, pp. 58-65.

Nguyen, T.M., Nham, T.P., Froese, F.J., & Malik, A. (2019). Motivation and knowledge sharing: a meta-analysis of main and moderating effects. Journal of Knowledge Management, Vol. 23, No. 5, ISSN: 1367-327.

Obrenovic, B., Jianguo, D., Tsoy, D., Obrenovic, S., Shafique Khan, M.A., &

Anwar, F. (2014). The enjoyment of knowledge sharing: Impact of altruism on tacit knowledge-sharing behavior. Frontiers in Psychology, Vol. 16, https://doi.org/10.3389/fpsyg.2020.01496

nnhnil S,, Siponnn aa hmood, (2007) Employe s' behrvirr rrrwrr ds IS security policy compliance. Proceedings of the 40th Hawaii International Conference on System Sciences, DOI: 10.1109/HICSS.2007.206.

Prochaska, J. O. & DiClemente, C. (1983). Stages and processes of self-change of smoking: Toward an integrative model of change. Journal of Consulting and Clinical Psychology, Vol. 51, pp. 390–395.

Prochaska J.O., & Diclemente C.C. (1986). Toward a Comprehensive Model of Change. In Miller W.R., Heather N. (eds) Treating Addictive Behaviors. Applied Clinical Psychology, vol 13. Springer, Boston, MA.

Rasoulkhani, K., Logasa, B., Reyes, M.P., & Mostafavi, A. (2017). Agent-based modeling framework for simulation of complex adaptive mechanisms underlying household water conservation technology adoption. Chan, W. K. V., D'Ambrogio, A., Zacharewicz, G., Mustafee, N., Wainer, G., & Page, E. (Eds.). Proceedings of the 2017 Winter Simulation Conference.

Reddy, G. N., & Reddy, G.J.U. (2014). A study of cyber security challenges and its emerging trends on latest technologies. available at: https://arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf (accessed 3 June 2021)

Ransbotham, S., & Sabyasachi M. (2009). Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research, Vol. 20, No. 1, pp. 121-139

Safa, N.S., & Solms, R.V. (2016). An information security knowledge sharing model in organizations. Computer in Human Behavior, Vol. 57, pp. 442-451.

Silic, M., & Lowry, P.B. (2019). Using design-science based gamification to improve organizational security training and compliance. Journal of Management Information Systems, Vol. 37, No. 1, pp. 129-161.

Stanton, J. M. Stam, K. R., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, Vol. 24, No. 2, pp. 124-133.

Siponen, M., Pahnila, S. & Mahmood, M. (2006). Factors influencing protection motivation and IS security policy compliance", Innovations in Information Technology Conference, Dubai.

Sun, P.Y.T. & Scott, J.L. (2005). An investigation of barriers to knowledge transfer. Journal of Knowledge Management, Vol. 9, No. 2, pp. 75-90.

Tim, T.T., & Lee, G. (2012). A modified and extended Triandis model for the enablers–process–outcomes relationship in hotel employees' knowledge sharing. Service Industries Journal, Vol. 32, No. 13, pp. 2059-2090

Triandis, H. C. (1977). Interpersonal behavior. Brooks/Cole, CA.

Wang, S., & Raymond A. N. (2010). Knowledge sharing: A review and directions for future research. Human Resource Management Review, Vol. 20, pp. 115-131.

Wang, J., Shan, Z., Gupta, M., & Rao, H.R. (2019). A longitudinal study of unauthorized access attempts on information systems the role of opportunity contexts. MIS Quarterly, Vol. 43, No. 2, pp. 601-622.

Zieba, M., & Bongiovanni, I. (2022). Knowledge management and knowledge security—Building an integrated framework in the light of COVID-19. Knowledge and Process Management, Vol. 29, No. 2, pp. 1-11.