Scientific Journal of Passive Defence
Vol. 15, No. 2, Summer 2024, Serial No. 58
ISSN: 2980-8030 , E-ISSN: 2008-6849

Presenting a Conceptual Model of Leveling Types of Threats in Security and Cyber Defense of Knowledge-Based Organizations in the Country

Alireza Alizadeh Soodmand, Kiamarth Fathi Hafeshjani *, Ashraf Shah Mansouri , Abouzar Arabsorkhi
* Assistant Professor, Department of Information Technology Management, Faculty of Management, Islamic Azad University, South Tehran Branch, Tehran, Iran
(Received: 23/01/2024, Revised: 12/05/2024, Accepted: 08/07/2024, Published: 15/08/2024)
DOR: 20.1001.1.20086849.1403.15.2.6.5

ABSTRACT

In recent years, the rapid development of knowledge-based organizations and companies and the need to pay attention to all kinds of threats, attacks are considered as the most important factor in their development. Therefore, the survival of these organizations depends on the principle of leveling all types of threats and presenting a comprehensive conceptual model in these organizations. The main purpose of the research is to present a conceptual model of the leveling of various threats in the security and cyber defense of knowledge-based organizations in the country. The methodology of the above research is based on the type of research to provide a conceptual model, it has a practical aspect, according to the purpose, it is of a developmental-applicative type, considering the dimensions of the research that It deals with theoretical, functional and operational areas. This research is divided in terms of purpose (type of research in the category of applied-developmental research and in terms of research approach in the category of mixed quantitative and qualitative research). In the qualitative section, by referring to articles, books and research reports, upstream documents using the metacomposition method, dimensions, components and indicators of the conceptual model of leveling various types of cyber threats in cyber security and defense in knowledge-based organizations, the extraction and qualitative control of findings was carried out, based on the findings of the model An initial concept was formed and after evaluation with scientific methods and based on structural equation modeling, the proposed validation framework and the final conceptual model were presented. To identify the dimensions and components of the model by studying previous researches, theoretical literature as well as interviews with specialists and experts in this field, the dimensions and components were extracted, then to validate the dimensions and components from the survey method (a field from the statistical population of experts, experts) with tools The questionnaire was asked. After performing valid tests (factor analysis test), the dimensions and components of the model were confirmed. The results of the research findings showed that all the considered factors for each of the components have a factor load greater than 0.4; Therefore, they load well on the relevant dimensions, or in other words, the components of the subset of dimensions are related and form part of the model structures; Therefore, the components are interdependent with the dimensions and have a meaningful relationship. The presented conceptual model explained well the relationship between dimensions, components, and variables in order to stratify the types of threats in security and cyber defense of knowledge-based organizations. The calculation and analysis of the fit indices with the software Smart-PLS$_{(4)}$ also confirmed the conformity of the conceptual framework and the experimental background with the reality.

Keywords: Conceptual Model, Threat Leveling, Cyber Security and Defense, Knowledge-Based Organizations

This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

Publisher: Imam Hussein University © Authors

* Corresponding Author Email: fathikiamars@yahoo.com

نشریه علمی پدافند غیرعامل

سال پانزدهم، شماره ۲، تابستان ۱۴۰۳، (پیاپی ۵۸): صص ۱۰۰-۷۵

شاپای چاپی: ۲۰۰۸-۶۹۴۹ | **شاپای الکترونیکی:** ۲۹۸۰-۸۰۳۰

علمی – پژوهشی

ارائه مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور

علیرضا علیزاده سودمند[۱]، کیامرث فتحی هفشجانی[۲*]، اشرف شاه منصوری[۳]، ابوذر عرب سرخی[۴]

DOR: 20.1001.1.20086849.1403.15.2.6.5

تاریخ دریافت: ۱۴۰۲/۱۱/۰۳ تاریخ پذیرش: ۱۴۰۳/۰۴/۱۸

تاریخ بازنگری: ۱۴۰۳/۰۲/۲۳ تاریخ انتشار: ۱۴۰۳/۰۵/۲۵

چکیده

در سال‌های اخیر توسعه سریع سازمان‌ها، شرکت‌های دانش‌بنیان و لزوم توجه به انواع تهدیدات، حملات به‌عنوان مهمترین عامل درراستای توسعه آنها به‌شمار می‌آید. لذا ادامه حیات این سازمان‌ها، منوط به اصل سطح‌بندی انواع تهدیدات و ارائه مدل مفهومی جامع در این سازمان‌هاست. هدف اصلی پژوهش، ارائه مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور می‌باشد. روش‌شناسی تحقیق فوق براساس نوع تحقیق ارائه مدل مفهومی بوده، جنبه کاربردی دارد، با توجه به هدف از نوع توسعه‌ای- کاربردی است، با توجه ابعاد پژوهش که به حوزه‌های نظری، کارکردی و عملیاتی می‌پردازد. این پژوهش از لحاظ هدف (نوع تحقیق در زمره تحقیقات کاربردی- توسعه‌ای و به لحاظ رویکرد تحقیق در زمره تحقیقات آمیخته کمی و کیفی) تقسیم می‌شود. در بخش کیفی با مراجعه به مقالات، کتاب‌ها و گزارشات پژوهشی، اسناد بالادستی با استفاده از روش فراترکیب، ابعاد، مولفه‌ها و شاخص‌های مدل مفهومی سطح‌بندی انواع تهدیدات سایبری در امنیت و پدافندسایبری در سازمان‌های دانش‌بنیان استخراج و کنترل کیفی یافته‌ها انجام شد، براساس یافته‌ها مدل مفهومی اولیه شکل گرفت و پس از ارزیابی با روش‌های علمی و براساس مدل‌سازی معادلات ساختاری، چارچوب پیشنهادی اعتبارسنجی و مدل مفهومی نهایی ارائه گردید. برای شناسایی ابعاد و مؤلفه‌های مدل با مطالعه بر تحقیقات پیشین، ادبیات نظری و همچنین مصاحبه با متخصصین و خبرگان این حوزه ابعاد و مؤلفه‌ها استخراج شده، سپس برای اعتبار بخشی ابعاد و مؤلفه‌ها از روش پیمایشی (میدانی از جامعه آماری متخصصین، خبرگان) با ابزار پرسشنامه مورد پرسش قرار گرفت. پس از انجام آزمون‌های معتبر (آزمون تحلیل عاملی) ابعاد و مؤلفه‌های مدل مورد تأیید قرار گرفت. نتایج حاصل از یافته‌های تحقیق نشان داد، تمامی عامل های در نظر گرفته شده برای هر یک از مؤلفه‌ها دارای بار عاملی بزرگتر از ۰/۴ هستند؛ بنابراین بر روی ابعاد مربوطه به خوبی بار می‌شوند یا به‌عبارتی مؤلفه‌های زیرمجموعه ابعاد مرتبط بوده و تشکیل بخشی از سازه‌های مدل را می‌دهد؛ بنابراین مؤلفه‌ها با ابعاد، به هم وابسته بوده و دارای ارتباط معنادار می‌باشند. مدل مفهومی ارائه شده، ارتباط میان ابعاد، مولفه‌ها، متغییرها در راستای سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان به خوبی تبیین نمود. محاسبه، تحلیل شاخص‌های برازش با نرم افزار Smart-PLS(4) نیز انطباق چارچوب مفهومی و پیشینه تجربی با واقعیت را تایید نمود.

کلیدواژه‌ها: مدل مفهومی، سطح‌بندی تهدیدات، امنیت و پدافندسایبری، سازمان‌های دانش‌بنیان

[۱] دانشجوی دکتری رشته مدیریت فناوری اطلاعات، دانشگاه آزاد اسلامی، واحد تهران جنوب، تهران، ایران

[۲] استادیار گروه مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه ازاد اسلامی، واحد تهران جنوب، تهران، ایران(fathikiamars@yahoo.com) نویسنده مسئول

[۳] استادیار گروه مدیریت صنعتی، دانشکده مدیریت، دانشگاه ازاد اسلامی، واحد تهران جنوب، تهران، ایران

[۴] استادیار پژوهشی پژوهشکده امنیت، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

* این مقاله یک مقاله با دسترسی آزاد است که تحت شرایط و ضوابط مجوز Creative Commons Attribution (CC BY) توزیع شده است.

© نویسندگان

ناشر: دانشگاه جامع امام حسین (ع)

۱- مقدمه

امروزه شرکت‌ها و سازمان‌ها با مجموعه‌ای از تهدیدات جدید، در حال توسعه و ناشناخته مواجه هستند. این تهدیدات در حال تغییر و تحولات گسترده بوده، لذا نیازمند یک سامانه امنیت و پدافند نوین سایبری هستند، همراستا با این موضوع صنعت امنیت اطلاعات و پدافند سایبری نیز می‌بایست در حال توسعه و تغییر باشد، این امر مهم سبب شده است که؛ شرکت‌ها و سازمان‌ها برای حفاظت از ساختارهای اطلاعاتی، امنیتی، سامانهی و شبکه‌ای همیشه در حالت آماده باش، قرار داشته باشند. با توجه به تغییرات گسترده تهدیدات و حملات سایبری بایستی سامانه‌های اطلاعاتی، امنیتی و حافظتی نیز پیشرفت نموده و ساختاری تکامل یافته و پیچیده‌تری داشته باشند [۱].

مطابق مرکز سایبری اتحادیه اروپا از ابتدای سال ۲۰۲۰ تا پایان سال ۲۰۲۳ بسیاری از شرکت‌ها و سازمان‌ها با انواع تهدیدات و حملات نوین مواجه بوده اند. انواع خطاهای یادگیری ماشینی، اختلال در داده‌های هوش‌مصنوعی، سامانه‌های خبره[1] آسیب دیده، تهدیدات در تولید ارزهای دیجیتال و سایر مواردی هستند که، شرکت‌ها و سازمان‌ها در سال‌های اخیر با آنها مواجه هستند. در اقتصاد دانش بنیان که ارزش شرکت‌ها و سازمان‌ها همواره برگرفته از ارزش محصولات دانش بنیان و فناورانه می‌باشد، تبیین ارزش محصولات و خدمات به‌عنوان یک مسئله راهبردی برای شرکت‌ها و سازمان‌های دانش بنیان مطرح می‌باشد [۲].

دستاوردهای تحقیق و توسعه بطور پیوسته از طریق سرمایه گذاری به محصول، فرایند و سامانه های نوین تبدیل می‌گردد و دسترسی به ظرفیت‌های سرمایه‌گذاری برای کارآفرینان و پژوهشگران عامل مهمی در ایجاد نوآوری و بهره‌برداری از توان فناوری در حوزه اقتصاد دانش بنیان[2] به‌شمار می‌آید. شرکت‌ها و سازمان‌های دانش بنیان زمینه‌هایی دارند که، ارائه محصولات دانش بنیان، فناوری‌های نوین و میانگین امور پژوهشی و توسعه در آن‌ها از دیگر زمینه‌های فناورانه، پژوهشی و صنعتی بیشتر است. بهره‌گیری از زمینه‌های فناورانه و دانش بنیان در شرکت‌ها و سازمان‌های دانش بنیان با تغییرات گسترده، فرایندهای ساختارمند، افزایش پیچیدگی و رقابت در سازمان‌ها همراستا می‌باشد [۳]. یکی از مهمترین مشکلات و چالش‌های سازمان‌های دانش بنیان تغییرات گسترده، فرایندهای غیرساختارمند، افزایش پیچیدگی و رقابت ناهمتراز در این سازمان‌ها می‌باشند. این مسائل، مشکلات و چالش‌ها می‌توانند داده‌ها، اطلاعات، دانش موثر سازمان‌ها را با تهدیدات و آسیب‌های گوناگونی روبرو سازد. عدم سطح‌بندی انواع تهدیدات در شرکت‌ها و سازمان‌های دانش بنیان و فقدان یک مدل مفهومی جامع در این شرکت‌ها و سازمان‌ها کشور را، در حوزه امنیت و پدافند سایبری دچار بحران نموده است. همچنین عدم بهره‌گیری از یک مدل مفهومی جامع مطابق با استانداردهای بین‌المللی سرمایه و دارایی‌های سازمان‌ها، شرکت‌ها، دولت‌ها و افراد را در معرض انواع تهدیدات، آسیب پذیری‌ها و خطرات دائمی قرار داده است. استفاده از یک مدل مفهومی جامع مطابق با استانداردهای و قوانین بین‌المللی[3] فرصت‌های اطلاعاتی و ارتباطی برای دموکراتیزه شدن در فضای سایبر در کشور ایجاد می‌کند [۴].

براساس گزارش مدیر ارشد امنیت شرکت ای بی ام[4]، صنعت امنیت و پدافندسایبری همچنان‌که در معرض انواع تهدیدات، آسیب‌پذیری‌ها و خطرات قرار دارد، از کمبود شدید خبرگان، مهندسان و متخصصان امنیت سایبری رنج می‌برد، کارشناسان امنیت و پدافند سایبری هشدار می‌دهند که، خطرات و تهدیدات مختلف در حوزه فضای سایبری افزایش یافته اند، زیرا همه‌گیری[5] انواع تهدیدات، آسیب‌پذیری‌ها و جرایم سایبری حتی می‌تواند باور عمومی را نسبت به آرمان‌های مختلف در بخش‌های امنیتی مانند امنیت دموکراسی، امنیت سرمایه داری و حریم خصوصی، امنیت شخصی متزلزل کند. همچنین براساس گزارش مرکز عالی امنیت سایبری آی‌بی‌ام[6](CCoE) اشتراک‌گذاری اطلاعات و تخصص در ایجاد موفقیت فردی و سازمانی در شرکت‌های فناورمحور بسیار مهم و راهبردی است. در واقع، نوآوری واقعی بدون همکاری عملا غیرممکن است، نوآوری برای موفقیت یک اصل ضروری است. شرکت آی بی ام برای سطح‌بندی انواع تهدیدات و حملات ساختار مشخصی را تعیین نموده است که، در تشکیل یک مرکز عالی امنیت سایبری[7] در حوزه ستاد کل فناوری این سازمان، با مشارکت سایر بخش‌های امنیتی، مفهوم نوآوری براساس سطح‌بندی انواع تهدیدات و حملات مشترک را به کار می‌گیرد [۵]. در سال‌های اخیر سازمان‌ها و شرکت‌های

[1] Expert systems
[2] Knowledge-based Economy
[3] International standards and laws
[4] IBM Security
[5] Epidemic
[6] IBM Cyber Security Center of Excellence (CCoE)
[7] Cyber Security Center of Excellence

دانش‌بنیان کشور در محیطی مملو از بحران، تحولات قرار گرفته‌اند، لازمه بقاء و ادامه حیات این سازمان‌ها در چنین محیطی همسویی با تغییرات محیطی، پاسخ‌گویی مناسب به انواع تغییرات، تهدیدات، آسیب‌پذیری‌ها و حملات در سطوح مختلف سازمان‌هاست. پاسخگویی صحیح مستلزم تصمیم‌گیری درست در برابر انواع تهدیدات و آسیب‌ها و مقابله با آنها در شرایط محتمل واقعی است. سازمان‌ها و شرکت‌های دانش‌بنیان دریافته‌اند که، برای رویارویی با انواع تهدیدات باید آمادگی کاملی داشته باشند. برخی از سازمان‌ها با نحوه مقابله با انواع تهدیدات آشنا هستند و یا می‌دانند چگونه می‌توان به یک سازمان مقاوم و منعطف در برابر انواع تهدیدات و آسیب‌ها تبدیل شد. افزایش انواع تهدیدات سایبری در سازمان‌های دانش‌بنیان سبب شکل‌گیری ساختارهای امنیتی در این سازمان‌ها شده است. لذا می‌بایست تدابیر جدیدی برای کاهش آسیب پذیری‌ها در این سازمان‌ها اتخاذ نموده و سامانه‌های امنیتی برای مدیریت این تهدیدات در فضای سایبر در نظر گرفته شود [۲،۳].

اهمیت و ضرورت توجه به امنیت فضای سایبری و مقابله با انواع تهدیدات، حملات و آسیب‌ها در سازمان‌ها به‌عنوان مهمترین اصل در حوزه فضای سایبری سازمان‌ها و شرکت‌ها در بخش‌های مختلف دولتی، خصوصی، غیرانتفاعی و.. در کشور مطرح است. این مهم به‌عنوان دغدغه‌های حاکم بر فضای سایبری کشور هم توسط مسئولان ارشد نظام، دولت‌های مختلف و هم طی سال‌های اخیر در بیانات مقام معظم رهبری (۱۴۰۲/۱۰/۲۲) بارها شنیده شده است و ایشان در اظهارات متعددی غفلت از آسیب‌های مرتبط با فضای سایبری را گوشزد کرده‌اند و تعابیری راهبردی بکار گرفته‌اند. ایشان در جایی فرمودند: «اگر من امروز رهبر انقلاب نبودم، حتماً رئیس فضای مجازی کشور می‌شدم» که این بیانات اهمیت فضای مجازی (فضای سایبری) را نشان می‌دهد. در جایی دیگر نیز فرموده رهبر انقلاب اینگونه است: «اهمیت فضای مجازی (فضای سایبری) به اندازه اهمیت انقلاب اسلامی است».
همچنین در بخش دیگری رهبر فرزانه انقلاب فرموده‌اند (۱۳۹۱/۷/۲۰): «رایانه، فضای سایبری که الان در اختیار شماست، اگر بتوانید اینها را یاد بگیرید، می‌توانید یک حرف درست خودتان را به هزاران مستمعی که شما آنها را نمی‌شناسید، برسانید. آسیب‌ها و بحران‌های را بشناسید و به دیگران نیز اطلاع دهید.» اگرچه این اظهارات و تعابیر راهبردی مقام معظم رهبری، تبیین اهمیت فضای مجازی و فضای سایبری را به همراه دارد، یکی از اولویت‌ها و ارجحیت‌های مدیریت اجرایی کشور را به روشنی بیان می‌کند، اما با این وجود، بی توجهی به مدیریت عالمانه و هوشمند مسائل مرتبط با فضای سایبری در کشور، نبود اعمال حاکمیت جمهوری اسلامی بر فضای سایبری و حتی عدم تشکیل منظم جلسات شورای عالی فضای مجازی، بارها مورد مطالبه رهبر انقلاب قرار گرفته است. این موضوع طی یک سال اخیر نیز از سوی کارشناسان و فعالان فضای سایبری با انتقادات و واکنش‌های زیادی همراه شده است. عدم شناخت آسیب‌ها و بحرانهای موجود در این حوزه، عدم تبیین کارکردهای مناسب فضای سایبری، نبود الگوی بومی در حوزه فضای مجازی و فضای سایبری و... از مهمترین مطالبات و دغدغه‌های ایشان درخصوص فضای مجازی و فضای سایبری می‌باشد.

۱-۱- اهداف تحقیق

هدف کلی :

- ارائه مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور

اهداف فرعی :

- شناخت ابعاد، مولفه‌ها، متغییرها انواع تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
- شناخت ابعاد، مولفه‌ها، متغییرها انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
- شناخت ابعاد، مولفه‌ها، متغییرها انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
- شناخت ابعاد، مولفه‌ها، متغییرها انواع تهدیدات شناخته شده (موجود) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
- شناخت ابعاد، مولفه‌ها، متغییرها انواع تهدیدات ناشناخته و هوشمند در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان.

۱-۲- جدید بودن و نوآوری تحقیق

علاوه بر موارد مطرح شده در حوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان و نیز اهمیت ویژه و ضرورت توجه به امنیت فضای سایبری و مقابله با انواع تهدیدات، حملات و آسیب‌ها در سازمان‌ها در این بخش به تبیین جنبه جدید بودن و نوآوری تحقیق پرداخته می‌شود. مهمترین نکته جنبه جدید بودن و نوآوری این تحقیق ارائه مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور می‌باشد. همچنین عامل دیگری که در بخش جنبه جدید

بودن و نوآوری تحقیق به روش تحقیق مورد استفاده در این تحقیق بوده که ترکیب آن برای ارائه مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور خود به‌عنوان نوآوری در این بخش تحقیق مطرح است. در ذیل برخی دیگر از موارد دیگری که در بخش جنبه جدید بودن و نوآوری تحقیق مطرح می‌گردد به شرح ذیل می‌باشد.

- تبیین ابعاد، مولفه‌ها، متغییرها انواع تهدیدات‌سخت در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان
- تبیین ابعاد، مولفه‌ها، متغییرها انواع تهدیدات نیمه‌سخت در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان
- تبیین ابعاد، مولفه‌ها، متغییرها انواع تهدیدات نرم در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان
- تبیین ابعاد، مولفه‌ها، متغییرها انواع تهدیدات شناخته شده (موجود) در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان
- تبیین ابعاد، مولفه‌ها، متغییرها انواع تهدیدات ناشناخته و هوشمند در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان.

۲- مبانی نظری و ادبیات تحقیق

۲-۱-پیشینه تحقیق

ساختار سامانه‌های اطلاعاتی، فناوری‌اطلاعات، امنیت‌اطلاعات، مبتنی بر نفوذ، هک، تهدیدات، سایر آسیب‌ها و تهدیدات در فضای سایبری است. جنگ‌سایبری و پدافندسایبری بخشی از مولفه‌ها و مباحث مرتبط با فناوری‌های نوین ارتباطی و اطلاعاتی است. در حوزه امنیت‌اطلاعات در سامانه‌های اطلاعاتی، نفوذ در شبکه‌های ارتباطی، هک در فناوری‌اطلاعات، تهدیدات سایبری و سایر آسیب‌های امنیتی در حوزه‌اینترنت، فضای سایبری، فضای مجازی پژوهش‌های مختلف و متعددی در سال‌های اخیر صورت گرفته است[۶]. ولیکن درخصوص مدل‌سازی سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان پژوهش خاصی صورت نگرفته و مطالب مرتبط بسیار اندک می‌باشد. در جدول (۱) خلاصه پیشینه تحقیقات در حوزه امنیت و پدافندسایبری بیان شده است :

جدول(۱): خلاصه پیشینه تحقیقات در حوزه امنیت و پدافندسایبری

نظریه پرداز(محقق)	عنوان پیشینه	خلاصه
کلدی و همکاران (۱۳۹۱)	شناخت انواع تهدیدات، آسیب‌های اجتماعی کلان شهر تهران	تجزیه و تحلیل داده‌ها نشان داد، تهدیدات، تهدیدات، آسیب‌های مختلف خصوصا در بخشهای اجتماعی، اقتصادی، جامعه شناختی و حتی شبکه‌های اجتماعی در حال افزایش بوده و چشم‌انداز آتی با تاکید بر تهدیدات ناشناخته باید مورد شناسایی و ارزیابی قرار گرفت [۷].
ظاهری و همکاران (۱۳۹۸)	بررسی تهدیدات امنیتی در محاسبات ابری، ارائه روش امن جهت نگهداری داده‌ها	نتایج نشان داد، ساختار نوینی براساس نوع تهدیدات در فضای سایبری باید ایجاد شود و روشی امن جهت نگهداری داده‌ها ارائه گردید [۸].
تقی‌پور و همکاران (۱۳۹۸)	طراحی مدل مفهومی الگوی پدافندسایبری جمهوری اسلامی ایران	نتایج حاصل از تجزیه‌وتحلیل داده‌ها نشان در طراحی مدل مفهومی میان مولفه‌های مورد بررسی نوعی همخوانی ساختاری با امنیت، یکپارچگی، صحت و دسترس‌پذیری در الگوی پدافندسایبری وجود دارد. همچنین به مولفه‌های دیگر مانند کنترل، ارزیابی، امکانسنجی و کنترل‌دسترسی و.. در طراحی مدل مفهومی الگوی پدافندسایبری توجه نمود [۹].
موسوی و همکاران (۱۳۹۹)	راهبردهای ارتقاء توانمندی‌های جنگ الکترونیک و سایبری (سایبرالکترونیک) نیروهای مسلح در برابر تهدیدات ناهمتراز	نتایج پژوهش نشان داد، اطلاعات برای تمامی سازمان‌ها به عنوان شریان اصلی سازمان می‌باشد لذا باید اهمیت ویژه‌ای جهت حفظ و نگهداری اطلاعات با توجه به شرایط رقابتی قائل شد. ضمنا راهبردهای ارتقاء توانمندی‌های جنگ الکترونیک و سایبری (سایبرالکترونیک) نیروهای مسلح در برابر تهدیدات ناهمتراز مورد بررسی قرار گرفت [۱۰].

جدول(۱): خلاصه پیشینه تحقیقات در حوزه امنیت و پدافندسایبری

میرزایی دیزجی و همکاران (۱۴۰۰)	راهکارهای ارتقاء مدیریت امنیت اطلاعات با استفاده از روش مدلسازی ساختاری تفسیری	با استفاده از شیوه‌های نوین مدیریت امنیت اطلاعات در سازمان توسعه و ارتقاء یافت. همچنین با بهره‌گیری از روش مدلسازی ارتباط میان ابعاد، مولفه‌ها و متغییرهای امنیت اطلاعات در سازمان مشخص شده، میزان ارتباط، تاثیرگذاری مولفه‌ها ومتغییرها بر یکدیگر مشخص گردید [۱۱].
ساده و همکاران (۱۴۰۱)	ارزیابی مدل شاخص‌های مختلف امنیت‌اطلاعات در سازمان‌ها	تجزیه‌وتحلیل داده‌ها نشان داد، ارزیابی مدل‌های شاخص‌های مختلف امنیت‌اطلاعات مبتنی بر الگوریتم ژنتیک بوده و ویژگی‌های عمده مدل‌های مختلف امنیت‌اطلاعات تبیین گردید. این ویژگی‌ها, شامل تضمین امکان انتخاب و اولویت‌بندی شاخص‌های مختلف امنیت‌اطلاعات، امنیت‌سایبری، ...برای توسعه امنیت‌اطلاعات است. [۱۲].
ادوارد روسو و همکاران (۲۰۱۲)	حفاظت از زیرساخت‌های ملی در ظبرابر حملات سایبری	نتایج نشان داد، مباحث امنیتی و حفاظت از زیرساخت‌های ملی در برابر حملات سایبری به عنوان اولویت ساختارهای امنیتی در حوزه‌های سایبری در برابر انواع تهدیدات می‌باشد. ضمنا در تهدیدات فضای سایبری می‌بایست نوع دفاع وسامانه‌های حفاظتی متناسب با نوع حمله، نوع نفوذ باشند [۱۳].
خین تاهان و همکاران (۲۰۲۰)	بررسی چالش‌های امنیت‌اطلاعات در فضای سایبری	در این تحقیق چالش‌های امنیت‌اطلاعات در فضای سایبری مورد ارزیابی قرار گرفت. راه‌کارهای عوامل حیاتی موفقیت در حوزه امنیت‌اطلاعات ارایه گردید [۱۴].
اولریک فرانکه و همکاران (۲۰۲۲)	بررسی مسائل و چالش‌های آگاهی موقعیتی سایبری، امنیت سایبری	تجزیه‌وتحلیل داده‌ها نشان داد، بیشتر شرکت‌ها به طور فزاینده‌ای به فناوری اطلاعات برای انجام عملیات خود متکی هستند. این همچنین مستلزم نیاز روزافزون به آگاهی موقعیت سایبری است. مشخص شد، روش‌های قدیمی در حوزه سایبری دیگر قادر به پاسخگویی مناسب به رویدادهایی مانند حملات یا آسیب‌ها است. نتایج این تحقیق استدلال می‌کند که آگاهی امنیت سایبری مبتنی بر دیدگاه‌های فناورانه و..می‌توانند بسیاری از چالش‌های موجود را برطرف نمایند[۱۵].
دامجان فوجس و همکاران (۲۰۲۳)	بررسی نرم‌افزار متعادل کننده و الزامات آموزشی برای امنیت اطلاعات در فضای‌سایبری	نتایج نشان داد، امنیت سایبری یکی از مهمترین حوزه‌های کلیدی مورد توجه برای اطمینان از امنیت سامانه‌های اطلاعاتی است. همچنین قابلیت اعتماد و اطمینان بر امنیت سامانه‌های اطلاعاتی اثرگذار می‌باشد. نیزدستیابی به سطح مناسبی از امنیت مستلزم در نظر گرفتن همزمان جنبه‌های فنی سامانه‌های اطلاعاتی و جنبه‌های انسانی آن است. این جنبه‌ها را می‌توان در قالب الزامات امنیت و پدافندسایبری توصیف کرد[۱۶].
انستیتوی امنیت سایبری روسیه (۲۰۲۲)	شناسایی انواع حملات در فضای سایبری بر مقوله نفوذ در شبکه، تهدید زیرساخت‌های شبکه، ایجاد بدافزارهای جدید	مطابق گزارش‌های این مرکز بیشتر آسیب‌ها، حملات و خسارات ناشی از حملات سایبری به شرکت‌ها و سازمان‌ها از روش‌های نوین نفوذ در شبکه و حملات ناشناخته توسط مهاجمین صورت پذیرفته است. لذا برای مقابله با انواع تهدیدات و حملات ناشناخته توسط مهاجمین می‌بایست رویکردی فراسامانهی نسبت به انواع تهدیدات و حملات ناشناخته داشت[۲،۳]..
مرکز جرائم رایانه‌ای اتحادیه‌اروپا (۲۰۲۳)	بررسی خسارات ناشی از تهدیدات و حملات‌سایبری به سازمان‌های مختلف	تحقیقات مطالعات انجام شده نشان داد، تهدیدات و حملات‌سایبری به سازمان‌های آنها خسارت‌های جبران‌ناپذیری به بخش‌های مختلف سازمانی، ملی، بین‌المللی وارد نموده است[۱۷].

۲- ادبیات تحقیق

۲-۱- مبانی نظری تحقیق

در سال‌های اخیر، استفاده از فناوری‌اطلاعات و هوشمندسازی فرایندها، به سرعت در حال پیشرفت می‌باشد. هدف‌گذاری کاربرد هوش‌مصنوعی، هوشمندسازی، اتوماسیون، سایر پیشرفت‌ها در فناوری‌اطلاعات بطور خاص زمینه را برای تکامل بیشتر این فناوری فراهم می‌کند. سامانه‌ها، سازمان‌ها، شبکه‌ها و... در حال هوشمندتر شدن هستند. محققان بیان می‌کنند، اگر می‌خواهید حرفه‌تان در فناوری‌اطلاعات نیز پیشرفت کند، باید در صدر نوآوری‌هایی باشید که به بازار می‌آیند [۶]. پیشرفت ساختارها، نرم‌افزارها، انواع استانداردهای بین‌المللی امنیتی و ... در فضای سایبری همراستا با این موضوع می‌باشند. بسیاری از متخصصان فناوری‌اطلاعات پذیرفته‌اند، بدون شناخت انواع تهدیدات، برقراری امنیت ممکن نیست. سوالات بسیاری در ترکیب امنیت در فضای‌سایبری و هوش‌مصنوعی مطرح می‌گردد، که می‌تواند بسیاری از چالش‌ها و مسائل این حوزه را برطرف نماید. اما حقیقت این است که، انواع مختلفی از تهدیدات در حوزه‌های جدید فناوری وجود دارد، نمی‌توان مطمئن بود که آنها ایمن هستند یا نه؟! [۱۶].

۲-۲-"انتقاد صریح رهبر انقلاب از مدیریت فضای مجازی (سایبری) در کشور"؛

در آغاز سال ۱۴۰۰ رهبر معظم انقلاب اسلامی در اولین روز از سال نو در سخنرانی زنده تلویزیونی خطاب به ملت شریف ایران، صراحتاً از مدیریت فضای مجازی و فضای سایبری در کشور انتقاد کردند. (۱۴۰۰/۱/۱).

۱-"عدم ساختارمندی و نظام‌مندی بنیادین در فضای مجازی(سایبری) کشور"

ایشان فرمودند: «دشمنان از فضای مجازی (سایبری) حداکثر استفاده را می‌کنند. متأسفانه در فضای مجازی (سایبری) کشور ما آن رعایت‌های لازم با وجود آنهمه تأکیدی که داشته‌ام، صورت نمی‌گیرد و در یک جهاتی واقعاً «ول» است. باید کسانی که مسئول هستند حواسشان باشد».

۲- فضای مجازی(سایبری) را باید مدیریت کرد.

حضرت آیت الله خامنه‌ای تاکید کردند: «همه دنیا و همه کشورهای دنیا روی فضای مجازی (سایبری) خودشان دارند اعمال مدیریت می‌کنند. اما ما افتخار می‌کنیم به‌اینکه فضای مجازی (سایبری) را «ول» کردیم. این افتخار ندارد. این به هیچ وجه افتخار ندارد؛ فضای مجازی (سایبری) را باید مدیریت کرد.»

۳- نباید فضای سایبری را دراختیار دشمن گذاشت؛

« باید از این امکان مردم (نظارت) استفاده کنند. فضای سایبری بلاشک برای مردم وسیله آزادی است و خیلی هم خوب است. اما نباید این وسیله را در اختیار دشمن گذاشت که بتواند علیه کشور و ملت توطئه کند. دشمنان دارند از این فضا استفاده می‌کنند».(۱۴۰۰)

۴- قوی شدن و اقتدار در استفاده از فناوری اطلاعات و فضای سایبری

« قوی شدن کشور جزو هدف‌های ما است. امروز قوّت در فضای سایبری و فناوری اطلاعات حیاتی است؛ امروز فضای سایبری حاکم بر زندگی انسان ها است در همه‌ی دنیا؛ و یک عدّه‌ای همه کارهایشان را از طریق فناوری اطلاعات و فضای سایبری پیش می‌برند؛ قوّت در این [زمینه] حیاتی است.» (بیانات مقام معظم رهبری در تاریخ ۳ فروردین ۱۳۹۹).

۲-۳-کاربرد امنیت و سطح‌بندی انواع تهدیدات

کاربرد امنیت و سطح‌بندی انواع تهدیدات در فناوری‌های اطلاعاتی، شناسایی تهدیدهای مختلف سایبری، در وضعیت رقابتی فضای سایبری و نیاز راهبردی به توسعه امنیت در حوزه فضای سایبری، از مهمترین عوامل سطح‌بندی انواع تهدیدات در فضای سایبری و توسعه سامانه‌های سازمانی است [۱۸]. به اقدامات پیشگیرانه امنیتی در فضای سایبری در حوزه‌های دانش‌بنیان در شرکت‌ها، سازمان‌ها از الزامات این پژوهش می‌باشد. همچنین ضرورت توجه به فناوری‌های نوین اطلاعاتی، توسعه امنیت در فضای سایبری از مهمترین نیازهای سازمان‌های دانش‌بنیان به‌شمار می‌روند [۱۹].

۲-۴- مدل‌سازی انواع تهدیدات در حوزه امنیت و پدافندسایبری

فرآیند مدل‌سازی انواع تهدیدات در حوزه امنیت و پدافندسایبری در سازمان‌ها براساس مدل ارائه شده توسط شرکت سیسکو[1] به شرح ذیل می‌باشد: [۲۰].

۱-هدف[2]: هدف قبل از نزدیک شدن به مدل‌سازی انواع تهدیدات در حوزه امنیت و پدافندسایبری در سازمان‌های دانش‌بنیان باید در درون سازمان مشخص باشد که، از مدل سازی تهدیدات به چه

[1] Cisco
[2] Aim

چیزی دست خواهد یافت؟!، یعنی برنامه باید از سه‌گانه محرمانگی[1]، یکپارچگی[2]، دسترس‌پذیری[3] پیروی کند[۲۰].

• **محرمانه بودن:** به محافظت از داده ها در برابر دسترسی غیرمجاز کمک می‌کند. بعبارت دیگر اصل محرمانه بودن بیانگر اطلاعات حساس نباید دست افرادی که مجوز دسترسی به آن را ندارد، بیافتد؛ بنابراین اطلاعات تنها باید در دسترس مالک آن اطلاعات و یا سازمان‌های مشروع باشد [۲۰،۲۱].

• **یکپارچگی:** اصل یکپارچی به پایدار بودن اطلاعات، دقیق بودن و عدم تغییرپذیری اشاره دارد. داده‌ها نباید در طول جابجایی و یا اقدامات دیگر تغییر کنند؛ بنابراین اصل یکپارچگی این اطمینان را می‌دهد که داده‌ها دقیق و قابل اعتماد هستند و چه بصورت تصادفی و چه غیرتصادفی تغییری نخواهند کرد [۲۰،۲۱].

• **دسترس‌پذیری:** اصل دسترس‌پذیری می‌گوید اطلاعات باید همیشه و به سادگی در دسترس افراد مشروع باشد. این اصل شامل سخت افزارها و زیرساخت‌ها نیز می‌شود؛ به بیان دیگر این اصل تضمین می‌کند که، زمانی که کاربران به داده‌ها نیاز داشته باشند، سامانه توانایی پاسخگویی به آن‌ها را دارد [۲۰،۲۱].

• **صحت**: اصل صحت به جلوگیری از تغییرات محدود کمک می‌کند [۲۱-۱۸].

• **دردسترس بودن:** اصل دردسترس بودن به انجام وظایف مهم تحت حملات خاص کمک می‌کند [۲۱-۱۹].

۲-تجسم[4]تهدیدات: در این بخش به آنچه که قرار است شکل گیرد، بصورت نماد و الگو اولیه پرداخته می‌شود. لذا باید یک نمای کلی از برنامه وجود داشته باشد که به آسان‌تر کردن فرآیندها کمک می‌کند. نمودارهایی را براساس ابعاد، مولفه‌ها، متغییرها انواع تهدیدات در حوزه امنیت و پدافندسایبری در سازمان‌های دانش‌بنیان ساخته شود که به آسان‌تر کردن فرآیندها کمک می‌کند. این عمل به دو صورت قابل انجام است: [۲۱-۱۹].

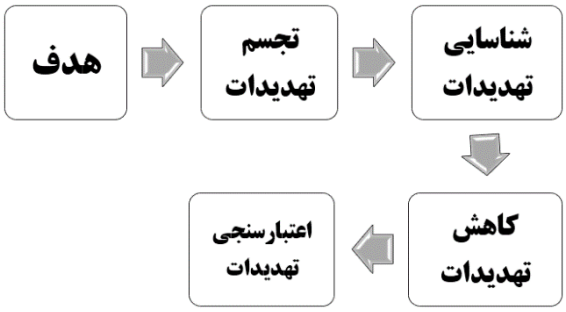
نمودار جریان داده: به نشان دادن چگونگی جریان داده در سامانه کمک می‌کند.

نمودار جریان فرآیند: به یافتن فرآیند سامانه کمک می‌کند که از کجا کاربران در سامانه تعامل دارند و چگونه سامانه در داخل کار می‌کند.

۳- شناسایی[5]تهدیدات : هدف اصلی در این مرحله شناسایی انواع تهدیدات در حوزه امنیت و پدافندسایبری در سازمان‌های دانش‌بنیان است. لذا محقق قصد دارد به این موضوع بپردازد که چگونه می‌توان تهدیدات را شناسایی کند یا چه چیزی ممکن است، در این فرآیند اشتباه پیش برود. با تجزیه وتحلیل تصاویر بخش قبل، متوجه شد که چگونه می‌توان انواع تهدیدات در حوزه امنیت و پدافند سایبری را شناسایی کرده و به‌صورت کامل تشریح گردد. این روش‌ها در روش‌های مدل‌سازی انواع تهدیدات در حوزه امنیت و پدافند سایبری ذکر شده‌اند [۲۲-۲۰].

۴- کاهش[6]تهدیدات: در این مرحله، هدف دستیابی به آنچه که در مورد کاهش و تقلیل انواع تهدیدات در حوزه امنیت و پدافند سایبری انجام خواهد شد، پرداخته می‌شود. لذا در این مرحله، به بررسی لایه‌ها پرداخته شده تا آسیب‌پذیری‌های مورد نیاز را شناسایی گردد و سپس فرایندهای مربوطه صورت پذیرد. کاهش آسیب‌پذیری‌های مستلزم بررسی مداوم هر تهدید، آسیب‌پذیری در بخش‌های مختلف سازمان‌های دانش‌بنیان است تا بتوان مؤثرترین تلاش‌ها را طراحی کرد [۲۲-۲۰].

۵- اعتبارسنجی[7]تهدیدات: این مرحله نهایی در فرآیند مدل‌سازی انواع تهدیدات در حوزه امنیت و پدافندسایبری در سازمان‌های دانش‌بنیان است، در این مرحله به‌این موضوع پرداخته می‌شود که ایا کار خوبی انجام شده یا نه. آیا همه تهدیدات در حوزه امنیت و پدافند سایبری کاهش یافته است یا خیر؟ لذا بایستی تغییرات را مورد بررسی قرار گیرد و از آنجایی که مدل‌سازی انواع تهدیدات در حوزه امنیت و پدافندسایبری یک فعالیت یکباره نیست، باید بطور مرتب این موارد را بررسی، ارزیابی، تجزیه‌وتحلیل قرار گیرد [۲۲-۲۰]. در شکل (۱) فرآیند مدل‌سازی انواع تهدیدات در حوزه امنیت و پدافندسایبری نمایش داده شده است: (سیسکو، ۲۰۲۳).



شکل (۱): فرآیند مدل‌سازی انواع تهدیدات در حوزه امنیت و پدافندسایبری (سیسکو، ۲۰۲۳). [۲۲-۱۹].

[1] Confidentiality
[2] Integrity
[3] Availability
[4] Visualization
[5] Identification threat
[6] Mitigation
[7] Validation

۲-۵- شناخت ابعاد، مولفه‌ها، متغییرها انواع تهدیدات در امنیت و پدافندسایبری در سازمان‌های دانش‌بنیان

شناخت ابعاد، مولفه‌ها، متغییرها انواع تهدیدات در امنیت و پدافندسایبری در سازمان‌های دانش‌بنیان کشور به قرار ذیل می‌باشد: [۲۲-۹،۱۱].

- ابعاد، مولفه‌ها، متغییرها انواع تهدیدات سخت (کاملا پیش‌بینی نشده و ناشناخته، غیرساختار)
- ابعاد، مولفه‌ها، متغییرها انواع تهدیدات نیمه‌سخت (اقدامات اطلاعاتی، امنیتی وسایبری که به صورت پیش بینی نشده و نیمه‌ساختارمند)
- ابعاد، مولفه‌ها، متغییرها انواع تهدیدات نرم (اقدامات فرهنگی، سیاسی، اقتصادی و ساختارمند)
- ابعاد، مولفه‌ها، متغییرها انواع تهدیدات موجود شناخته شده(اقدامات ساختارمند، روانشناختی، رسانه‌ای، اجتماعی، شبکه‌ای، زنجیره‌ای و ...)
- ابعاد، مولفه‌ها، متغییرها انواع سایر تهدیدات ناشناخته و هوشمند (حملات مبتنی بر هوش‌مصنوعی، پیشگیری‌های فازی، مقابله هوشمند، حملات ابری، سامانه‌های امنیتی خبره، انواع حملات روزصفر[1]). در شکل (۲) سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور نمایش داده شده است: [۲۲-۱۹].

شکل (۲): سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور[۲۲-۱۹].

۲-۶- ساختار غیرمتمرکز انواع تهدیدات در امنیت و پدافندسایبری

- هر چند فضای سایبری به علت ساختار غیرمتمرکز در حوزه فناوری‌اطلاعات و تهدیدات در این بخش، امکان استفاده و بهره‌برداری از فناوری‌های نوین را در بخش‌های مختلف سایبری به کشورهای مختلف داده است، اما در برخی از کشورهای جهان به دلایلی چون وجود زیرساخت‌های بهتر، باکیفت‌تر، موقعیت برتر و ویژه‌ای در فضای سایبری به خود اختصاص داده است [۲۳-۲۰].
- موقعیتی راهبردی، استراتژیک سازمان‌های دانش‌بنیان کشور، شکل جدیدی از برتری فناوری‌ها و اقتصاد دانش‌بنیان را به نمایش گذاشته است و کشور از آن در راستای عملیات در بهره‌گیری از فناوری‌های نوین بهره می‌برد [۲۳-۲۰].
- بنابراین مبارزه با انواع تهدیدات در فضای سایبری صرفا به صورت کلاسیک و متقارن امکان پذیر نیست بلکه، باید با رویکرد نبرد نامتقارن در مقابل آن ایستاد. همچنین شناسایی و سطح‌بندی انواع تهدیدات در فضای سایبری سازمان‌های دانش‌بنیان بسیار الزامی است. براساس همین اصل عوامل موثر در سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان مورد بررسی قرار گیرد [۲۴-۲۰].

۲-۷- مقابله با انواع تهدیدات و لزوم توسعه اصطلاح" تبیین جهاد سایبری"

- همان طور که در فضای واقعی وقتی قلمرو، مرزهای کشوری مورد هجوم قرار می‌گیرد، دفاع از سرزمین، مقابله با انواع تهدیدات دیگر وظیفه خاص نیروهای نظامی و مسلح نیست، بلکه به وظیفه و تکلیف عمومی برای تمام افراد جامعه بدل می‌شود، استفاده از این عزم ملی برای مقاومت و مدیریت آن با رویکرد نبرد نامتقارن می‌تواند بزرگترین سرمایه در جهت حفظ استقلال تلقی شود [۲۵-۱۹].
- چنانچه از دیدگاه اسلامی نسبت به مسئله دفاع باید دیدگاهی فراملی داشت، لذا مقاومت و مقابله همه جانبه باید در کشور نهادینه شود، بعبارت بهتر دیدگاهی حقیقی، در مسئله دفاع به مقاومت مردمی، جهاد تبیین تاکید فراوان شده است، در فضای مجازی و فضای سایبری نیز می‌توان با مدیریت مقاومت مردمی، دفاع و مقاومت همه جانبه در برابر انواع تهدیدات با رویکرد نبرد نامتقارن بایستی به رویارویی با تهاجمات سایبری در این حوزه پرداخته شود؛ که‌این موضوع مسئله‌ای بسیار حیاتی برای کشور است. امری که از آن با عنوان جهاد سایبری در کشور یاد می‌شود [۲۴،۲۶].
- ضمنا از نظر مقام معظم رهبری(مدّظله العالی) جهاد تبیین، مهم‌ترین عرصه جهاد (دربرابر انواع تهدیدات) است؛ زیرا اکنون دشمن با هزاران دستگاه رسانه‌ای و خبری، سایبری دست به جنگ روانی زده است تا با وارونه جلوه دادن واقعیت‌ها، رابطه مؤمنانه مؤمنین را قطع کند. از این رو باید با تبیین و روشنگری،

[1] Zero Day Attacks

حقیقت‌ها را برای همگام بیان کرد.

- همچنین ایشان درخصوص جهاد تبیین در حوزه مدیریت فضای مجازی (سایبری) بیان نموده اند، مدیریت فضای مجازی (سایبری) جزو مسائل کلیدی، کوتاه و میان مدت است؛ رهبر انقلاب اسلامی در بیاناتی که با نمایندگان یازدهمین دوره مجلس شورای اسلامی داشتند، بر اهتمام به مسائل کلیدی و اولویت‌دار تاکید کردند و مساله مدیریت بر فضای سایبری را یکی از این مسائل مهم عنوان کردند.
- ایشان فرمودند: «مسئله مدیریت فضای مجازی (سایبری) جزو مسائل مهم ما است. این مسئله، مسئله بلندمدت هم نیست بلکه مسئله کوتاه‌مدت و میان‌مدت و جزو مسائل نزدیک ما است که باید به آن توجه شود. امثال اینها مسائل کلیدی وجود دارد. توجه کنید دچار حاشیه‌ها نشوید، دچار مسائل فرعی و بی اولویت نشوید.(۱۳۹۹/۴/۲۲).

۲-۸- مولفه‌های اثرگذار بر سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان

مولفه‌های اثرگذار برسطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان به شرح ذیل می‌باشد: [۹،۲۰،۲۱،۲۲،۲۴،۲۸].

الف) ابعاد، مولفه‌ها، متغییرها انواع تهدیدات‌سخت در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان :

زیرمولفه‌های اثرگذار تهدیدات سخت در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان شامل، تهدیدات کاملا پیش‌بینی نشده، ناشناخته، غیرساختارمند می‌باشد. برخی از این تهدیدات و آسیب‌ها در جدول (۲)مشخص شده است: [۹،۲۱،۲۴،۲۸،۲۹].

جدول(۲): ابعاد و مولفه‌های اثرگذار تهدیدات‌سخت [۹،۲۱،۲۴،۲۸،۲۹].

شاخص اصلی	مولفه‌های اثرگذار
تهدیدات سخت	میزان اهمیت مراکز و سازمان‌های دانش‌بنیان
	تشکیلات استراتژیک سازمان داده محور
	الویت بندی طرح‌ها و برنامه‌ها
	پیاده سازی پروژه‌های امنیت‌اطلاعات
	خرید سخت افزارهای جدید
	تامین استانداردهای امنیتی
	اصل و گزینش مکان‌یابی سایبری
	تایید اصل امایش سرزمین
	طراحی اماکن و مراکز داده ای
	استقرار سایتها
	نقض داده‌ها در سایتها
	انواع باج افزارها

ب) ابعاد، مولفه‌ها، متغییرها انواع تهدیدات نیمه‌سخت در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان :

زیرمولفه‌های اثرگذار تهدیدات نیمه‌سخت در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان شامل تمامی اقدامات اطلاعاتی، امنیتی و سایبری که به صورت پیش بینی نشده و نیمه‌ساختارمند می‌باشد. برخی از این تهدیدات و آسیب‌ها در جدول (۳) مشخص شده است: [۹،۲۱،۲۳،۲۸،۲۹].

جدول(۳): ابعاد و مولفه‌های اثرگذار تهدیدات نیمه‌سخت [۹،۲۱،۲۳،۲۸،۲۹].

شاخص اصلی	مولفه‌های اثرگذار
تهدیدات نیمه‌سخت	تعیین نقاط امن برای استقرار عملکرد ها
	انتخاب جایگزین بهینه در مکان‌گزینی مناسب
	استقرار طرح ها در سایت
	میزان قابلیت استحکام سایت‌ها در برابر حملات
	ایمن سازی بسترهای ارایه سرویس
	عملکردهای پروژه‌ای سایبری
	اقدامات اطلاعاتی پیش بینی نشده
	مقاوم سازی کدهای تحلیلی در حملات
	قابلیت ایمن‌سازی شبکه‌ها
	انواع گزارشات نامعتبر
	انتقالف دستکاری غیرمجاز داده

ج) ابعاد، مولفه‌ها، متغییرها انواع تهدیدات‌نرم در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان

زیرمولفه‌های اثرگذار نیمه تهدیدات نرم در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان شامل اقدامات فرهنگی، سیاسی، اقتصادی و ساختارمند می‌باشد. برخی از این تهدیدات و آسیب‌ها در جدول (۴) مشخص شده است: [۹،۲۱،۲۸،۲۹].

جدول(۴): ابعاد و مولفه‌های اثرگذار تهدیدات‌نرم [۹،۲۱،۲۸،۲۹].

شاخص اصلی	مولفه‌های اثرگذار
تهدیدات نرم	محصولات و خدمات ارائه شده توسط پیمانکاران
	تجهیزات امنیتی در سایت‌ها و سامانه‌ها
	روابط بین سامانه‌ها در برابر حملات و تهدیدات
	اطمینان از کفایت قدرت پردازشی و حافظهٔ سامانه‌ها
	امن سازی سامانه‌های اطلاعاتی
	حفاظت از دارایی ها در برابر حملات شبکه‌ای
	امن سازی سایتهای ارتباطی و شبکه‌ای
	اصل انطباق در تحلیل تهدیدات نرم
	همراستایی سامانه امنیتی مورد استفاده
	تبیین اصل جهاد فرهنگی
	اصل غفلت از تهدیدات داخلی

د) ابعـاد، مولفـه‌هـا، متغییرهـا انـواع سـایر تهدیـدات شناخته‌شده در امنیـت و پدافندسـایبری سـازمان‌هـای دانش‌بنیان :

زیرمولفه‌های اثرگذار سـایر تهدیـدات شـناخته شـده(موجود) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان شامل تهدیـدات موجود شناخته شده؛ اقدامات ساختارمند، روانشناختی، رسانه‌ای، اجتماعی، شبکه‌ای و... در سازمان می‌باشد برخی از این تهدیدات و آسـیب‌هـا در جـدول (۵) مشـخص شـده اسـت [۹،۲۰،۲۱،۲۸،۲۹،۳۰].

جدول(۵): ابعاد و مولفه‌های اثرگذار تهدیدات شناخته‌شده [۹،۲۰،۲۱،۲۸،۲۹،۳۰].

شاخص‌اصلی	مولفه‌های اثرگذار
سایر تهدیدات	توسعه زیرساخت‌های سامانه‌ها
	تحلیل شبکه‌ای با توجه به نوع استفاده در فضای‌سایبری
	اقدامات ساختارمند (حفاظ‌های الکتریکی و..)
	کاربردهای محوری سامانه‌های امنیتی
	استفاده از انواع ارتینگ[1] و.. درسایت‌ها
	ایمن سازی مجازی در فضای سایبری
	تهدیدات رسانه‌ای در فضای سایبری
	افزایش قابلیت اطمینان در مراکز اطلاعاتی
	استفاده از مشاوران امنیت اطلاعات در فضای سایبری
	تبیین انواع حملات اجتماعی (مهندسی اجتماعی[2])
	شبکه‌های طعمه و نشت اطلاعات

ه) ابعاد، مولفه‌ها، متغییرها انواع سایر تهدیدات ناشـناخته و هوشـمند در امنیـت و پدافندسـایبری سـازمان‌هـای دانش‌بنیان:

زیرمولفه‌های اثرگـذار سـایر تهدیـدات ناشـناخته و هوشـمند در امنیت و پدافند سایبری سازمان‌هـای دانـش‌بنیـان شـامل انـواع تهدیدات ناشناخته و هوشمند همانند پیشگیری‌های فازی، مقابله هوشمند، بهره‌گیری از سامانه‌های امنیتی خبـره، انـواع حمـلات روزصفر می‌باشد برخی از این تهدیدات و آسیب‌ها در جـدول (۶) مشخص شده است: [۹،۲۰،۲۱،۲۸،۲۹،۳۰].

[1]Earthing
[2]Social Engineering

جدول(۶): ابعاد و مولفه‌های اثرگذار تهدیدات ناشناخته(هوشمند) [۹،۲۰،۲۱،۲۸،۲۹،۳۰].

شاخص‌اصلی	مولفه‌های اثرگذار
سایر تهدیدات	شکاف‌های امنیت سایبری(بات نت و..)
	سرقت هوشمند سرمایه یا نابودی دارایی‌های معنوی
	انواع حملات هوشمند مبتنی بر اینترنت اشیا
	بدافزارهای برنامه‌نویسی‌شده
	انواع باج‌افزارها و بدافزارهای هوشمند
	انواع تکنیک‌های علم داده
	الگوریتم‌های یادگیری ماشین
	تشخیص پیشگام تهدیدات روزصفر
	الگوریتم‌های داده‌کاوی
	حملات مبتنی بر وب و برنامه‌های وب‌کاوی
	سرقت هویت (جعل هویت)در فضای سایبری
	فیشینگ[3] و عملیات انواع فیشینگ
	حملات سایبری در محیط ابری

۳- روش‌شناسی تحقیق

دراین تحقیق با توجه به نوع موضوع و متغییرهای موجود در ارائه مدل تجربی و مفهومی برای سطح‌بندی انواع تهدیـدات در حـوزه امنیت و پدافند سایبری سازمان‌های دانش‌بنیان سـاختار تحقیـق به‌صورت عملیاتی مورد بررسی و ارزیابی قرار گرفت.

۳-۱- نوع تحقیق

یکی از روش‌های، کشف مطالعه و مـدیریت تهدیـد، شناسـایی و ارائه مـدل تجربـی و مفهـومی بـرای انـواع تهدیـدات در سـطوح مختلـف سـازمانی اسـت. ارائـه مـدل تجربـی-مفهـومی بـرای سطح‌بندی انـواع تهدیـدات در حـوزه امنیـت و پدافنـد سـایبری سازمان‌های دانش‌بنیـان اجـازه کشـف انـواع تهدیـدات بـالقوه و بالفعل، حملات و آسیب پذیری‌های ممکن را، پیش از حمله انواع نفوذگران و هکرها را می‌دهد. در این خصـوص مـدل‌هـای ارائـه شده توسط متخصصین و مـدیران امنیتـی مختلـف راه‌حـل‌هـای متفاوتی را برای حل مسائل و مدیریت بحران‌ها نشـان مـی‌دهـد. روش‌شناسی تحقیق فوق براساس نوع تحقیق باتوجه به‌اینکـه، در اجرای این تحقیق، ارائـه مـدل مفهـومی بـرای شـناخت منطـق سطح‌بندی انواع تهدیدات سایبری در امنیت و پدافندسـایبری در سـازمان‌هـای دانـش‌بنیـان اسـت و نتـایج عملیـاتی آن قـدرت تصمیم‌سـازی و تصـمیم‌گیـری مـدیران حـوزه امنیـت سـایبری

[3]Phishing

شرکت‌ها و سازمان‌های دانش‌بنیان را افزایش می‌دهد، لذا جنبه کاربردی دارد و با توجه به کاربردی بودن دانش در سطوح مختلف این سازمان‌ها می‌توان بیان نمود، ساختار عملکردی این تحقیق حاضر با توجه به هدف از نوع توسعه‌ای- کاربردی است.

۳-۲-روش تحقیق

روش تحقیق مورد استفاده با رویکرد آمیخته کیفی و کمی است. در بخش کیفی با مراجعه به مقالات، کتاب‌ها و گزارشات پژوهشی، اسناد بلادستی با استفاده از روش فراترکیب، ابعاد، مولفه‌ها و شاخص‌های مدل مفهومی سطح‌بندی انواع تهدیدات سایبری در امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان استخراج و کنترل کیفی یافته‌ها انجام شد، براساس یافته‌ها مدل مفهومی اولیه شکل گرفت و پس از ارزیابی با روش‌های علمی ساختار مدل مفهومی نهایی ارائه گردید.

۳-۳- جامعه و نمونه

جامعه آماری پژوهش حاضر شامل اساتید، محققان، متخصصین، مهندسین و خبرگان) سازمان‌های دانش‌بنیان (مورد مطالعه استان تهران) می باشند.

حجم نمونهٔ آماری پیشنهادی در این بخش حدود ۷۰ نفر از مدیران ارشد فنآوری اطلاعات، متخصصین امنیت و پدافند سایبری و همچنین کارشناسان امنیت سایبری شرکت‌های دانش بنیان بودند. پرسشنامه‌ها میان آنها توزیع شده، فقط ۶۰ پرسشنامه به‌طور کامل تکمیل شده و عودت گردید. نرمال بودن توزیع داده‌های جمع‌آوری شده که با آزمون کولموگروف اسمیرنوف تأیید گردیده و همگونی و همسان‌بودن جامعه آماری از نظر داشتن تجربه در حوزه امنیت وپدافندسایبری و فعالیت در شرکت‌های دانش بنیان را توجیه می‌کند.

۳-۴- روش گردآوری داده‌ها و ابزار تحقیق

داده‌های کیفی با روش فراترکیب جمع آوری شدند. روش فراترکیب، نوعی مطالعه کیفی است که، اطلاعات و یافته‌های استخراج شده از مطالعات کیفی دیگر با موضوع مشابه و مرتبط را بررسی می‌نماید. در نتیجه نمونه مورد نظر براساس مطالعات صورت گرفته تحقیق کیفی ساختارمند، براساس ارتباط آنها با اهداف و سوالات، ارتباط میان ابعاد، مولفه‌ها، متغیرها مورد بررسی قرار می‌گیرد. در این پژوهش از روش فراترکیب به منظور مقایسه، تفسیر تبدیل، ترکیب چارچوب‌ها و مدل‌های مختلف ارائه شده در زمینه تهدیدات سایبری امنیت و پدافندسایبری سازمان‌های دانش‌بنیان استفاده می‌گردد.

در تحقیق حاضر برای گردآوری داده‌ها و اطلاعات مورد نیاز از روش‌های کتابخانه‌ای و میدانی استفاده شده است. اطلاعات مربوط به مبانی نظری، ادبیات و پیشینه نیز به روش کتابخانه‌ای و با مطالعه کتاب‌ها، مقالات منتشره در پایگاه‌های اطلاعات علمی، مجلات علمی و مجموعه مقالات کنفرانس‌های و داخلی گرد آمده‌اند و نیز در بخش تحقیقات میدانی، با بهره‌گیری از خبرگان و متخصصین و ... اطلاعات جمع‌آوری شد.

۳-۵- نوع ساختار پژوهش حاضر

در این بخش تحقیق؛ بر اساس نوع موضوع و ساختار پژوهش و نیز با توجه ابعاد پژوهش که به حوزه‌های نظری، کارکردی و عملیاتی در حوزه سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور می‌پردازد. این پژوهش از لحاظ هدف (نوع تحقیق در زمره تحقیقات کاربردی- توسعه‌ای و به لحاظ رویکرد تحقیق در زمره تحقیقات آمیخته کمی و کیفی) تقسیم می‌شود. نظر به‌اینکه نوع این پژوهش به دلیل ماهیت موضوعی آن، تحلیل و سطح‌بندی انواع تهدیدات فضای سایبری در سازمان‌های دانش‌بنیان جمهوری اسلامی ایران می‌باشد، می‌بایست براساس نظرات خبرگان و امکانسنجی مولفه‌های مورد بررسی و اثرگذار مورد سنجش قرار گیرد. برای شناسایی ابعاد و مؤلفه‌های مدل با مطالعه بر تحقیقات پیشین، ادبیات نظری، همچنین مصاحبه با خبرگان این حوزه ابعاد و مؤلفه‌ها استخراج گردید، سپس برای اعتبار بخشی ابعاد و مؤلفه‌ها از روش پیمایشی (میدانی از جامعه آماری متخصصین، مهندسین و خبرگان) با ابزار پرسشنامه مورد پرسش قرار گرفت. پس از انجام آزمون‌های آماری ابعاد و مؤلفه‌های مدل مورد تأیید قرار گرفت. قلمرو مکانی این تحقیق سازمان‌های دانش‌بنیان کشور (مورد مطالعه استان تهران) است.

همچنین، نیازهای اطلاعاتی برای بررسی و آزمون فرضیات تحقیق و برازش مدل نیز از طریق پیمایش و با استفاده از ابزار پرسشنامه گردآوری شد. با توجه به مدل مفهومی تحقیق، متغیرهای مورد مطالعه شامل عوامل تهدیدات سخت، تهدیدات نیمه‌سخت، تهدیدات نرم، تهدیدات شناخته‌شده و تهدیدات ناشناخته و هوشمند در حوزه امنیت و پدافندسایبری سازمان‌های دانش‌بنیان که در جداول(۶-۲) مولفه‌ها و مولفه‌های اثرگذار آنها مشخص شده است. افزون بر این برای تضمین اعتبار و روایی ابزار گردآوری اطلاعات از طریق روش تحقیق اکتشافی و کیفی و با استفاده از مبانی نظری تحقیق، مولفه‌ها و عوامل مؤثر بر امنیت و

پدافند سایبری سازمان‌های دانش‌بنیان نتایج تحقیقات مشخص و با نظر اساتید، خبرگان تعدیل و اصلاح گردید، همچنین بهره‌گیری از مبانی نظری تحقیق و نیز نظر خبرگان و صاحبنظران ضامن روایی پرسشنامه است.

برای سنجش پایایی یا قابلیت اعتماد ثبات و سازگاری پرسشنامه، از مهمترین شاخص سازگاری درونی یعنی آزمون آلفای‌کرونباخ استفاده شده است. این آزمون که، حاصل آن یک ضریبی به نام آلفای‌کرونباخ است، برای آزمون پایایی پرسشنامه‌ای که به صورت طیف لیکرت طراحی شده به کار رفته، لذا چنانچه ضریب محاسبه شده از رقم ۰/۷ بیشتر باشد، سؤال‌های پرسشنامه از نظر پایایی دارای همبستگی درونی مناسبی بوده و قابل پذیرش است. جدول زیر ضرایب آلفا برای سؤال‌های مربوط به عوامل مؤثر بر امنیت و پدافندسایبری سازمان‌های دانش بنیان نتایج تحقیقات و مجموع سؤال‌های پرسشنامه را نشان می‌دهد.

جدول(۷): ضرایب آلفای‌کرونباخ محاسبه شده برای پایایی متغیرها

نام متغیر	تعداد سؤال‌ها	آلفای‌کرونباخ
تهدیدات سخت	۱۲	۰/۷۸۰
تهدیدات نیمه‌سخت	۱۱	۰/۸۵۰
تهدیدات نرم	۱۱	۰/۸۸۵
تهدیدات شناخته‌شده	۱۱	۰/۷۹۵
تهدیدات ناشناخته (هوشمند)	۱۳	۰/۸۹۸
کل سؤال‌ها	۵۸	۰/۸۹۰

براساس جدول فوق، ضریب آلفای کرونباخ برای کل پرسشنامه برابر با ۰/۸۹ بوده و کاملاً به یک نزدیک است و نشان می‌دهد در مجموع پرسشنامه از انسجام درونی مناسب واعتماد پذیری بالایی برخوردار است. از آنجایی ضریب آلفا برای مقیاس مولفه‌های مختلف بالای ۰/۷ است، این موضوع نشان می‌دهد که، مقیاس فرعی پرسشنامه نیز انسجام درونی مناسب و اعتمادپذیری بالایی دارد.

۴- تجزیه وتحلیل داده‌ها

با توجه به استخراج ابعاد، مولفه‌ها، متغییرها و زیرمتغییرها سطح‌بندی انواع تهدیدات فضای سایبری در سازمان‌های دانش‌بنیان برگرفته از ادبیات، پیشینه تحقیق و نیز اسناد بالادستی اشاره شده در قسمت‌های قبلی، فرمایشات مقام معظم رهبری (مدظله العالی) و سایر منابع مورد بررسی، مدل اولیه استخراج گردید. در گام بعدی با طراحی سوالات و مصاحبه با خبرگان، متخصصین، مهندسین، اساتید، فرهیختگان، ابعاد شناسایی شده و مولفه‌ها و زیرمولفه‌ها مورد بازبینی ارزیابی مجدد قرار گرفتند. در جداول ۱۳-۹ ابعاد شناسایی شده و مولفه‌ها و زیرمولفه‌ها نمایش داده شده است.

- شناخت و بررسی ابعاد، مولفه‌ها، متغییرها انواع تهدیدات‌سخت (کاملا پیش‌بینی نشده، ناشناخته، غیرساختار) در فضای سایبری در سازمان‌های دانش‌بنیان
- شناخت و بررسی ابعاد، مولفه‌ها، متغییرها انواع تهدیدات نیمه‌سخت (اقدامات اطلاعاتی، امنیتی و سایبری که به صورت پیش بینی نشده و نیمه‌ساختارمند) در فضای سایبری در سازمان‌های دانش‌بنیان
- شناخت و بررسی ابعاد، مولفه‌ها، متغییرها انواع تهدیدات‌نرم (اقدامات فرهنگی، سیاسی، اقتصادی و ساختارمند) در فضای سایبری در سازمان‌های دانش‌بنیان
- شناخت و بررسی ابعاد، مولفه‌ها، متغییرها انواع تهدیدات موجود شناخته شده(اقدامات ساختارمند، روانشناختی، رسانه‌ای، اجتماعی، شبکه‌ای، زنجیره‌ای و...) در فضای سایبری در سازمان‌های دانش‌بنیان
- شناخت و بررسی ابعاد، مولفه‌ها، متغییرها انواع سایر تهدیدات ناشناخته و هوشمند (حملات مبتنی بر هوش‌مصنوعی، پیشگیری‌های فازی، مقابله هوشمند، حملات ابری، سامانه‌های امنیتی خبره، انواع حملات روزصفر) در فضای سایبری سازمان‌های دانش‌بنیان

۴-۱-آزمون مدل مفهومی پژوهش

برای آزمون مدل مفهومی، پژوهش از الگوریتم تحلیل مدل‌ها در روش Smart-PLS- SEM به شرح زیر استفاده و تحلیل‌های لازم در سه بخش (۱) برازش مدل‌های اندازه‌گیری، (۲) برازش مدل ساختاری و (۳) برازش کلی مدل اندازه‌گیری و ساختاری انجام گردید. به این ترتیب که ابتدا از صحت روابط موجود در مدل‌های اندازه‌گیری با استفاده از معیارهای پایایی و روایی اطمینان حاصل کرده، سپس به بررسی و تفسیر روابط موجود در بخش ساختاری پرداخته و در مرحله پایانی نیز برازش کلی مدل پژوهش بررسی شده است. لازم به توضیح است، هر چند مهمترین دلیل برتری روش PLS نسبت به سایر روش‌ها، نمونه های کوچک و داده‌های غیرنرمال ذکر شده است، ولی برای بررسی فرض نرمال بودن توزیع داده‌ها از آزمون کولموگروف - اسمیرنوف استفاده شده و

نتایج آن در جدول (۸) آورده شده است.

جدول (۸): نتایج آزمون بررسی نرمال بودن توزیع داده ها

نام متغیر	میانگین	انحراف معیار	P-value
تهدیدات سخت	۴۳/۸۵	۵۸/۶	۰/۱۲۰
تهدیدات نیمه‌سخت	۴۱/۱۳	۵۶/۷	۰/۰۷۵
تهدیدات نرم	۴۴/۳۵	۷۲/۹	۰/۲۵۱
تهدیدات شناخته‌شده	۴۳/۶	۵۷/۹	۰/۱۱۲
تهدیدات ناشناخته (هوشمند)	۴۰/۷۹	۵۵/۴	۰/۰۶۴

با توجه به نتایج آزمون کولموگروف - اسمیرنف برای داده‌های مربوط به سؤال‌ها و گویه‌های مربوط به هر یک از عوامل تهدیدات سخت، تهدیدات نیمه‌سخت، تهدیدات نرم، سایر تهدیدات شناخته‌شده و تهدیدات ناشناخته (هوشمند) و نیز نتایج حاصل از تجزیه و تحلیل داده‌های جمع آوری شده، از آنجا که در سطح اطمینان ۹۵ درصد مقدار آماره و P-value محاسبه شده از ۵ درصد بیشتر است؛ بنابراین، ادعای نرمال بودن توزیع داده‌ها به عنوان یکی از مفروضات و شروط مقدماتی برای استفاده از آزمون‌های پارامتریک برای تحلیل‌های آماری پذیرفته می‌شود.

۴-۲- برازش مدل مفهومی[1] تحقیق

برازش مدل نشان می‌دهد، مدل طراحی شده توسط پژوهشگر چقدر براساس داده‌های واقعی، پشتیبانی می‌شود. به‌عبارت دیگر میزان سازگاری مدل تجربی با مدل نظری را نشان می‌دهد. منظور از مدل نظری (مفهومی) مدلی است که، توسط پژوهشگر براساس ادبیات پژوهش یا تحلیل محتوای کیفی به‌دست آمده است. منظور از مدل تجربی نیز مدلی است که، براساس داده‌های گردآوری شده توسط پژوهشگر اجرا شده است.

۴-۳- برازش مدل‌های اندازه‌گیری

برازش مدل‌های اندازه‌گیری شامل بررسی پایایی و روایی سازه‌های پژوهش است. پایایی آزمون به دقت اندازه‌گیری و ثبات آن مربوط است، فورنل و لارکر برای بررسی پایایی سازه‌ها سه ملاک را پیشنهاد می‌کنند:

الف) پایایی هر یک از گویه‌ها،

ب) پایایی ترکیبی هر یک از سازه‌ها

ج) میانگین واریانس استخراج شده.

بنابراین مطابق الگوریتم تحلیل مدل‌ها در روش PLS-SEM برای بررسی برازش مدل‌های اندازه‌گیری سه معیار پایایی، روایی همگرا و روایی واگرا استفاده و نتایج زیر حاصل شده است:

الف) پایایی:

برای بررسی پایایی مدل‌های اندازه‌گیری معیارهای ضرایب بارهای عاملی آلفای کرونباخ و پایایی ترکیبی به شرح زیر محاسبه شد:

۱)سنجش بارهای عاملی:

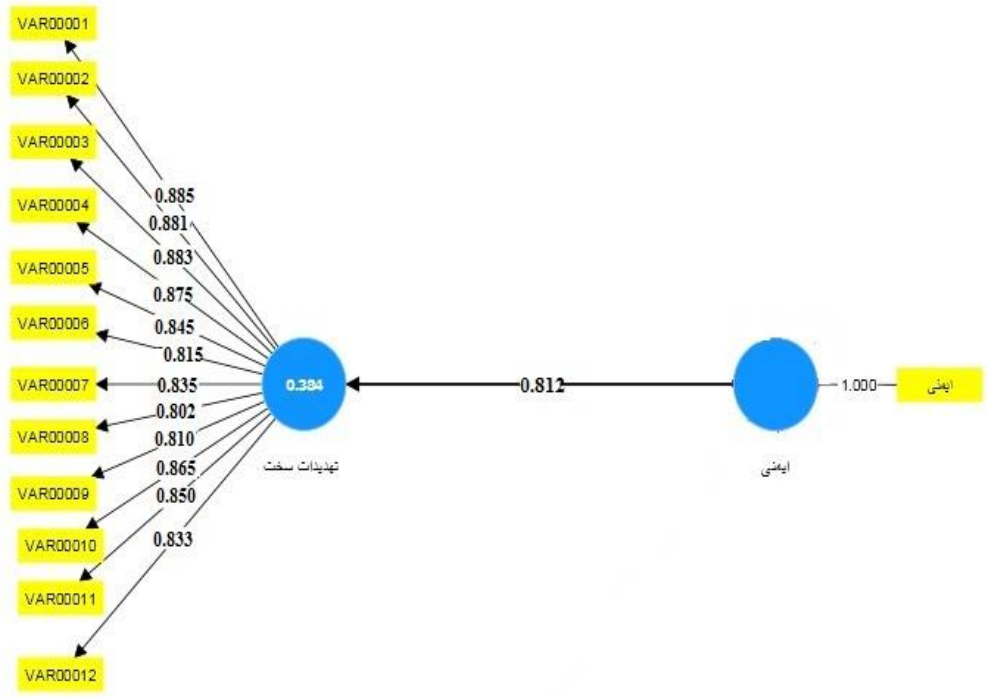
پایایی هر یک از گویه‌ها به مقدار بارهای عاملی هر یک از متغیرهای مشاهده شده اشاره دارد و برای مشخص کردن این که شاخص‌های اندازه‌گیری (متغیرهای مشاهده شده) تا چه اندازه برای سنجش متغیرهای پنهان قابل قبول هستند، مورد استفاده قرار گرفته و حداقل مقدار قابل قبول آن ۰/۳ و بارهای عاملی ۰/۴ سطح معناداری متوسط را نشان می‌دهد. در تحلیل‌های عاملی تأییدی مقادیر بارهای عاملی بالاتر از ۰/۵ نشانگر سطح معناداری قوی و همبستگی زیاد بین متغیرهای مشاهده شده عامل بوده و نیز بیانگر آن است که سازه خوب تعریف شده است البته با افزایش حجم نمونه و تعداد متغیرها، بارهای عاملی کوچک تر از ۰/۲۵ نیز معنادار است. نتایج حاصل از تحلیل عاملی تاییدی و بررسی ضرایب بارهای عاملی و اعداد مندرج در ستون ضرایب بارهای عاملی جداول مربوطه نشان می‌دهد تمام سؤال‌ها با سطح همبستگی بالا به خوبی متغیرهای مشاهده شده را اندازه‌گیری می کند.

برای هر یک از این شاخص‌ها دامنه قابل قبولی در نظر گرفته شده است. در جداول شماره (۱۳-۹) آزمون تحلیل عاملی ابعاد، مولفه‌ها، متغییرهای انواع تهدیدات که در مدل مفهومی اثرگذار می‌باشند، بیان شده است:

[1]Conceptual Model Fit

جدول(۹): آزمون تحلیل عاملی ابعاد، مولفه‌ها، متغییرهای تهدیدات‌سخت در مدل مفهومی

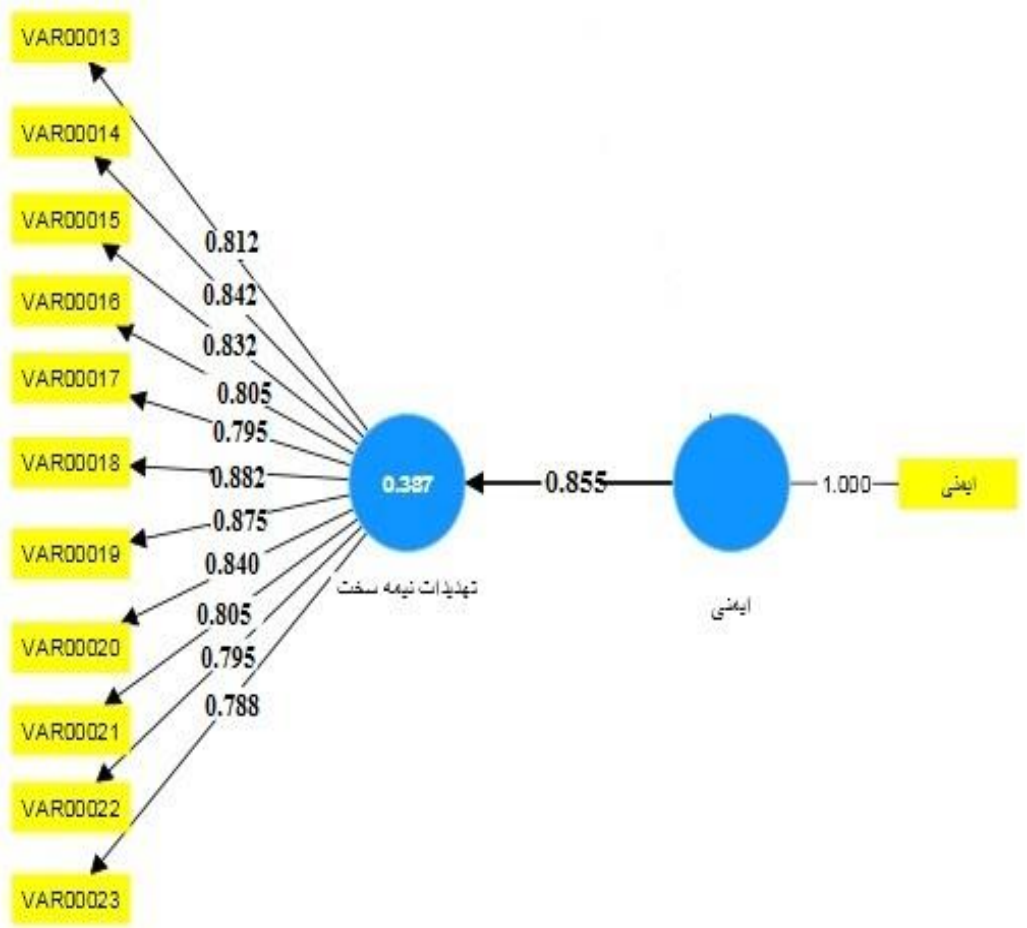
آزمون	ابعاد و مولفه‌ها	متغییرها، ساختارها و اقدامات	بارعاملی	مولفه‌های اثرگذار	بارعاملی
تحلیل عاملی	تهدیدات سخت	زیرمولفه‌ها،متغییرهای کاملا پیش‌بینی‌نشده و ناشناخته، غیرساختار	۰/۸۱۲	میزان اهمیت مراکزو سازمان‌ها	۰/۸۸۵
				تشکیلات استراتژیک سازمان داده‌محور	۰/۸۸۱
				الویت بندی طرح ها و برنامه‌ها	۰/۸۸۳
				پیاده سازی پروژه‌های امنیت‌اطلاعات	۰/۸۷۵
				خرید سخت افزارهای جدید	۰/۸۴۵
				تامین استانداردهای امنیتی	۰/۸۱۵
				اصل و گزینش مکان یابی سایبری	۰/۸۳۵
				تایید اصل امایش سرزمین	۰/۸۰۲
				طراحی اماکن و مراکز داده ای	۰/۸۱۰
				استقرار سایت‌ها پدافندسایبری	۰/۸۶۵
				نقض داده‌ها در سایت‌ها	۰/۸۵۰
				انواع باج افزارها و بدافزارها	۰/۸۳۳



شکل (۳): برآورد مدل مقوله‌های متغیر تهدیدات‌سخت در مدل مفهومی

جدول(۱۰): تحلیل عاملی ابعاد، مولفه‌ها، متغییرهای تهدیدات نیمه‌سخت در مدل مفهومی

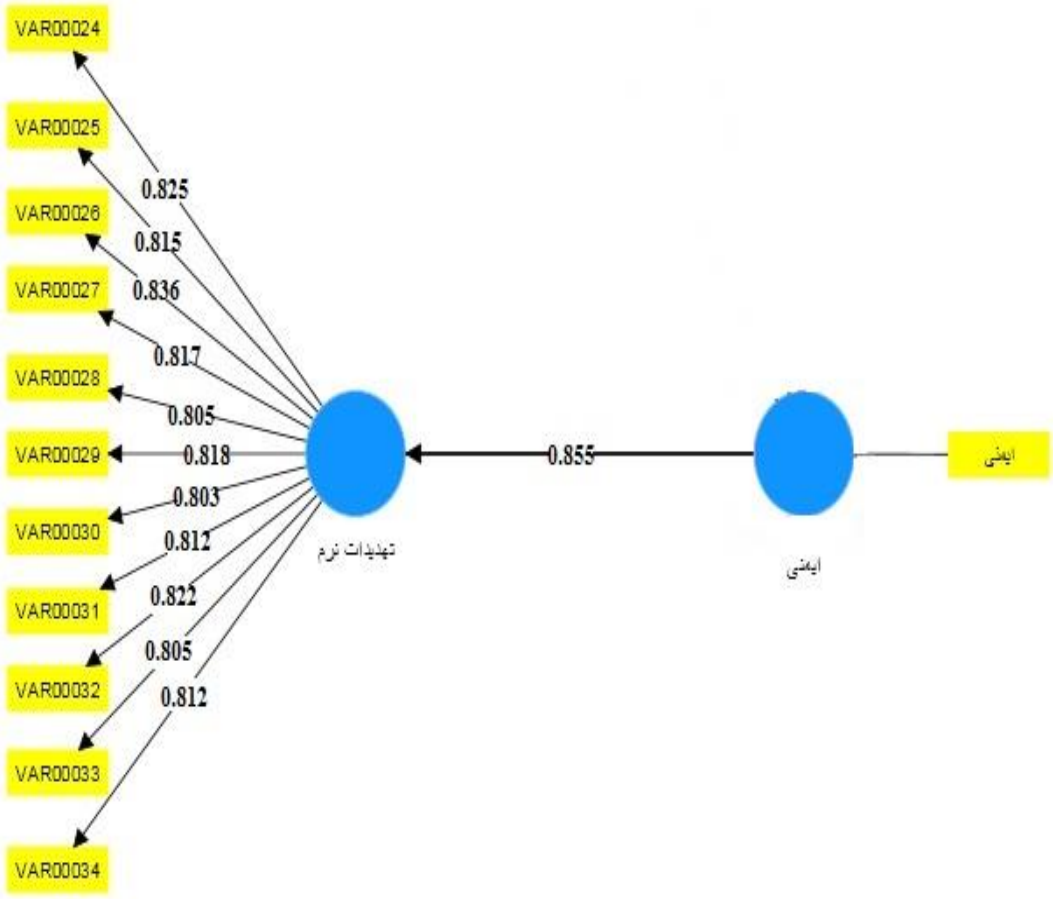
آزمون	ابعاد و مولفه‌ها	متغییرها، ساختارها و اقدامات	بارعاملی	مولفه‌های اثرگذار	بارعاملی
تحلیل عاملی	تهدیدات نیمه‌سخت	مولفه‌ها و متغییرهای اقدامات اطلاعاتی، امنیتی‌وسایبری که بصورت پیش بینی‌نشده و نیمه‌ساختارمند	۰/۸۵۵	تعیین نقاط امن برای استقرار عملکردها	۰/۸۱۲
				انتخاب جایگزین بهینه درمکان‌گزینی	۰/۸۴۲
				استقرار طرح ها در سایت	۰/۸۳۲
				میزان قابلیت استحکام سایت‌ها درحملات	۰/۸۰۵
				ایمن سازی بسترهای ارایه سرویس	۰/۷۹۵
				عملکردهای پروژه‌ای سایبری	۰/۸۸۲
				اقدامات اطلاعاتی پیش بینی نشده	۰/۸۷۵
				مقاوم سازی کدهای تحلیلی در حملات	۰/۸۴۰
				قابلیت ایمن‌سازی شبکه‌ها	۰/۸۰۵
				انواع گزارشات نامعتبر	۰/۷۹۵
				انتقال، دستکاری غیرمجاز داده	۰,۷۸۸



شکل (۴): برآورد مدل مقوله‌های متغیر تهدیدات نیمه‌سخت در مدل مفهومی

جدول(۱۱): آزمون تحلیل عاملی ابعاد، مولفه‌ها، متغییرهای تهدیدات نرم در مدل مفهومی

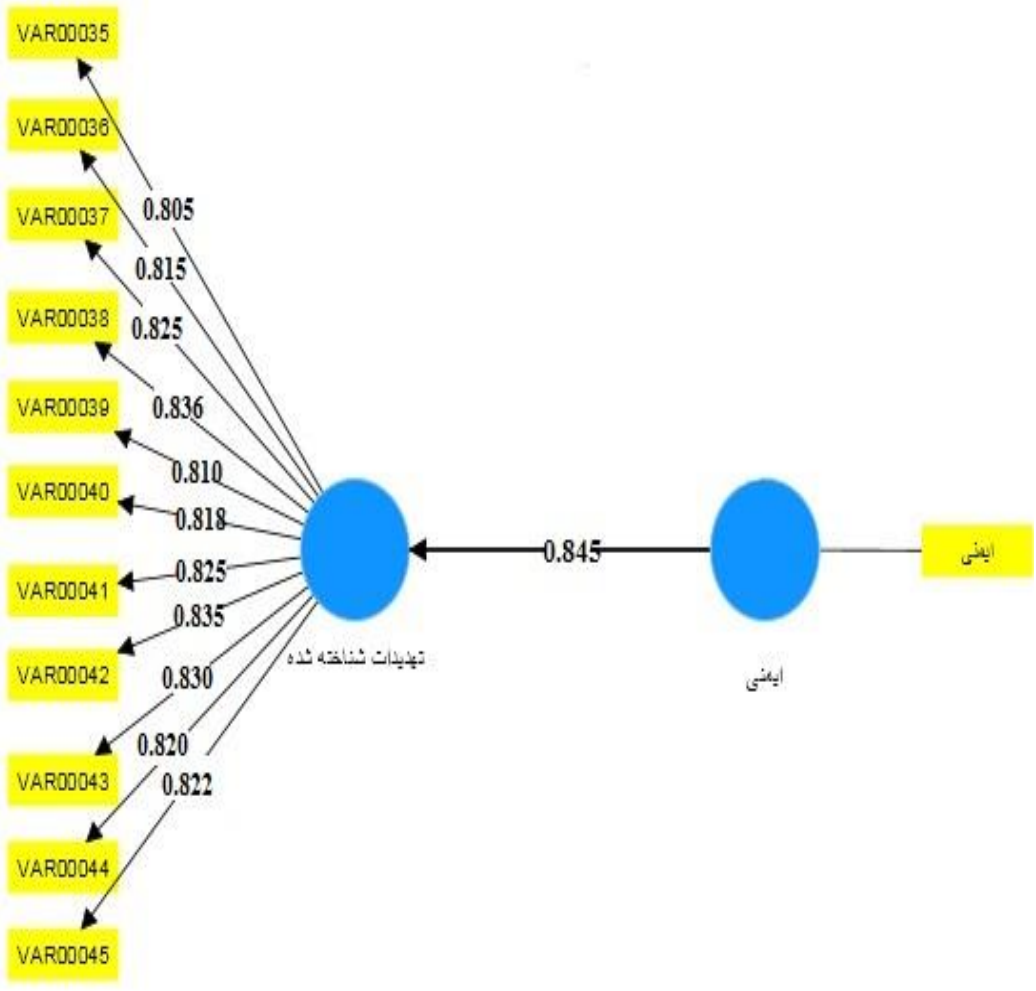
آزمون	ابعاد و مولفه‌ها	متغییرها، ساختارها و اقدامات	بارعاملی	مولفه‌های اثرگذار	بارعاملی
تحلیل عاملی	تهدیدات نرم	مولفه‌ها و متغییرهای اقدامات فرهنگی، سیاسی، اقتصادی و ساختارمند	۰/۸۵۵	محصولات، خدمات ارائه شده توسط پیمانکاران	۰/۸۲۵
				تجهیزات امنیتی در سایت‌ها و سامانه‌ها	۰/۸۱۵
				روابط بین سامانه‌ها دربرابر حملات و تهدیدات	۰/۸۳۶
				اطمینان ازکفایت قدرت پردازشی‌وسامانه‌ها	۰/۸۱۷
				امن سازی سامانه‌های اطلاعاتی	۰/۸۰۵
				حفاظت از دارایی‌ها در برابر حملات شبکه‌ای	۰/۸۱۸
				امن سازی سایت‌های ارتباطی و شبکه‌ای	۰/۸۰۳
				اصل انطباق در تحلیل تهدیدات نرم	۰/۸۱۲
				همراستایی سامانه امنیتی مورد استفاده	۰/۸۲۲
				تبیین اصل جهاد فرهنگی	۰/۸۰۵
				اصل غفلت از تهدیدات داخلی	۰/۸۱۳



شکل (۵): برآورد مدل مقوله‌های متغیر تهدیدات نرم در مدل مفهومی

جدول(۱۲). آزمون تحلیل عاملی ابعاد، مولفه‌ها، متغییرهای تهدیدات موجود(شناخته شده) در مدل مفهومی

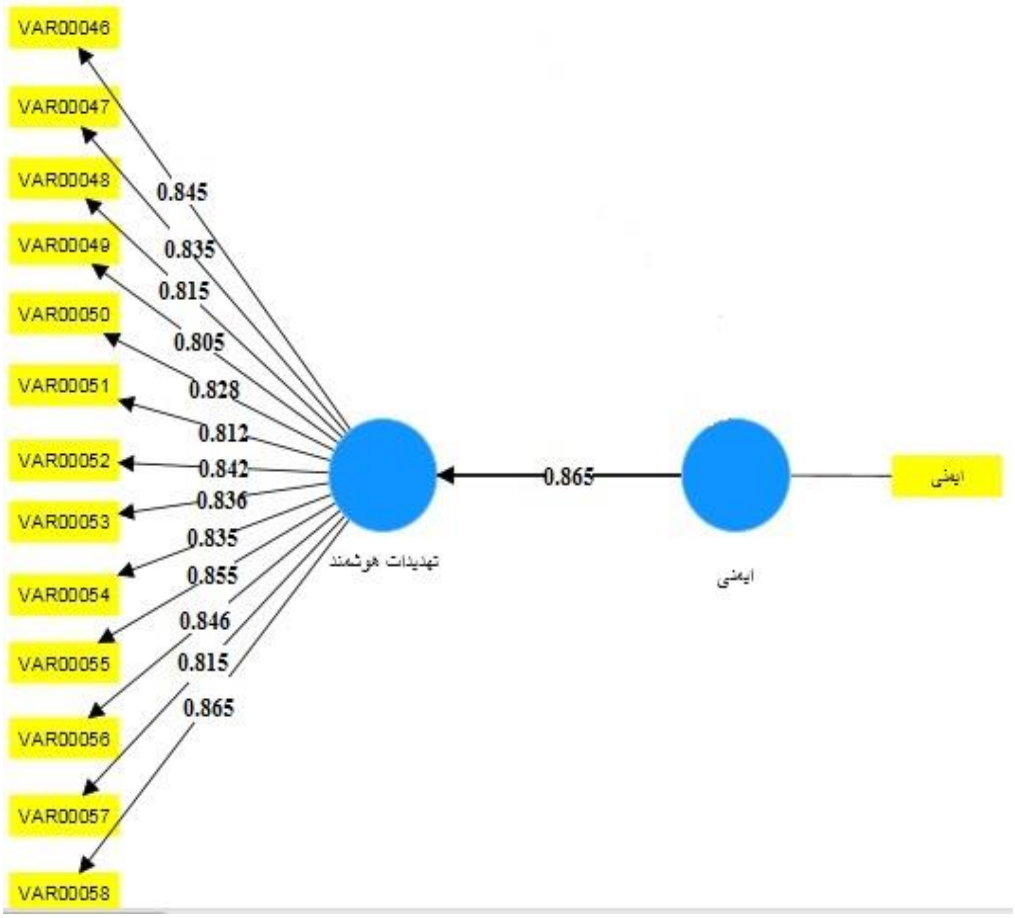
آزمون	ابعاد و مولفه‌ها	متغییرها، ساختارها و اقدامات	بارعاملی	مولفه‌های اثرگذار	بارعاملی
تحلیل عاملی	تهدیدات موجود (شناخته شده)	مولفه‌ها و متغییرهای اقدامات ساختارمند، روانشناختی، رسانه‌ای، اجتماعی، شبکه‌ای و...	۰/۸۴۵	توسعه زیرساخت‌های سامانه‌ها	۰/۸۰۵
				تحلیل شبکه‌ای براساس نوع استفاده در فضای‌سایبری	۰/۸۱۵
				اقدامات ساختارمند مانندحفاظهای الکتریکی	۰/۸۲۵
				کاربردهای محوری از سامانه‌های امنیتی در سایت‌ها	۰/۸۳۶
				ایمن سازی مجازی در فضای سایبری	۰/۸۱۰
				تهدیدات رسانه‌ای در فضای سایبری	۰/۸۱۸
				افزایش قابلیت اطمینان در مراکز اطلاعاتی	۰/۸۲۵
				استفاده از مشاوران امنیت‌اطلاعات در فضای سایبری	۰/۸۳۵
				تبیین انواع حملات اجتماعی (مهندسی اجتماعی)	۰/۸۳۰
				شبکه‌های طعمه و نشت اطلاعات	۰/۸۲۲



شکل (۶): برآورد مدل مقوله‌های متغیر تهدیدات موجود(شناخته شده) در مدل مفهومی

جدول(۱۳): آزمون تحلیل عاملی ابعاد، مولفه‌ها، متغییرهای تهدیدات ناشناخته و هوشمند در مدل مفهومی

آزمون	ابعاد و مولفه‌ها	متغییرها، ساختارها و اقدامات	بارعاملی	مولفه‌های اثرگذار	بارعاملی
تحلیل عاملی	سایرتهدیدات ناشناخته و هوشمند	مولفه‌هاو متغییرهای پیشگیری‌های فازی، حملات مبتنی برهوش‌مصنوعی، مقابله هوشمند،بهره‌گیری از سامانه‌های امنیتی خبره، انواع حملات روزصفر	۰/۸۶۵	شکاف‌های امنیت سایبری	۰/۸۴۵
				سرقت یا نابودی دارایی‌های معنوی	۰/۸۳۵
				انواع حملات پیچیده و هوشمند	۰/۸۱۵
				بدافزارهای برنامه‌نویسی‌شده	۰/۸۰۵
				انواع باج‌افزارها و بدافزارهای هوشمند	۰/۸۲۸
				انواع تکنیک‌های علم داده	۰/۸۱۲
				الگوریتم‌های یادگیری ماشین	۰/۸۴۲
				تشخیص پیشگام تهدیدات روز	۰/۸۳۶
				الگوریتم‌های داده‌کاوی	۰/۸۳۵
				حملات مبتنی بر وب، هک وب‌کاوی	۰/۸۵۵
				سرقت هویت (جعل هویت)در فضای سایبری	۰/۸۴۶
				حملات سایبری در محیط ابری	۰/۸۱۵
				هکتیویسم‌های مبتنی بر هوش‌مصنوعی	۰/۸۶۵



شکل (۷): برآورد مدل مقوله‌های متغیر تهدیدات ناشناخته و هوشمند در مدل مفهومی

جدول (۱۴): میزان خوبی برازش با معیارهای مختلف مقوله‌های بعد ایمنی

متغیرها	میانگین واریانس استخراجی (AVE)	پایایی اشتراکی (CR)>۰	ضریب تعیین (R Square)	آلفای کرونباخ	مقادیر اشتراکی <Communality.	افزونگی (Redundancy)
تهدیدات سخت	۰/۶۰۷	۰/۹۸۹	۰/۹۷۰	۰/۷۹۰	۰/۶۰۷	۰/۵۸۹
تهدیدات نیمه سخت	۰/۵۶۰	۰/۹۸۰	۰/۹۶۰	۰/۷۸۵	۰/۵۶۰	۰/۵۳۷
تهدیدات نرم	۰/۵۶۸	۰/۹۷۹	۰/۹۵۴	۰/۸۵۶	۰/۵۶۸	۰/۵۴۱
تهدیدات شناخته شده	۰/۵۶۲	۰/۹۸۲	۰/۹۶۲	۰/۷۹۱	۰/۵۶۲	۰/۵۳۹
تهدیدات ناشناخته (هوشمند)	۰/۵۰۱	۰/۹۸۸	۰/۹۱۵	۰/۸۷۰	۰/۵۰۱	۰/۴۵۸

جدول (۱۴) معیارهای کلی کیفیت مدل و میزان خوبی برازش با معیارهای مختلف آورده شده است. در ذیل به تمامی موارد مطرح شده درخصوص بررسی و ازیابی مدل مفهومی پرداخته می‌شود:

۲)آلفای کرونباخ

معیار کلاسیک برای سنجش پایایی و شاخص ارزیابی پایداری درونی محسوب می‌شود. پایداری درونی نشانگر میزان همبستگی یک سازه و شاخص‌های مربوط به آن است. در مورد متغیرهای با تعداد سؤال‌های کم مقدار ضریب آلفای ۰/۶ به عنوان سرحد ضریب معرفی و بالاتر از ۰/۷ نشانگر پایایی قابل قبول است. در مدل پژوهش حاضر، مقدار آلفا برای تمامی مولفه ها بالای ۰/۷ می‌باشد.

۳)پایایی ترکیبی(CR)

برای تعیین پایایی هر یک از سازه ها علاوه بر معیار سنتی آلفای کرونباخ از معیار نوینی، پایایی ترکیبی استفاده میکنند. برتری این معیار نسبت به ضریب آلفای کرونباخ این است که پایایی سازه ها نه به صورت مطلق بلکه با توجه به همبستگی سازه هایشان با یکدیگر محاسبه می‌شود برای سنجش بهتر پایایی هر دو معیار به کار برده میشود. مقدار پایایی ترکیبی بالای ۰/۷ برای هر سازه نشان از پایداری درونی مناسب برای مدل‌های اندازه‌گیری داشته و مقدار کمتر از ۰/۶ عدم وجود پایایی را نشان می‌دهد. مقادیر پایایی ترکیبی برای سازه های تحقیق بالاتر از ۰/۸ به دست آمده است

ب) روایی همگرا

پس از بررسی معیار، پایایی دومین معیار برازش مدل‌های اندازه‌گیری روایی همگرا است. معیار میانگین واریانس استخراج شده[1] برای سنجش روایی همگرا، میزان همبستگی هر سازه با سؤال‌های (شاخص‌ها) خود را بررسی می نماید. معیار AVE نشانگر میانگین واریانس به اشتراک گذاشته شده بین هر سازه با شاخص‌های خود است و مقدار ۰/۴به بالای آن کافی محسوب میشود. پس از حصول نتایج مقادیر بارهای عاملی و ضرایب آلفای کرونباخ، پایایی ترکیبی و AVE از طریق تحلیل‌ها و خروجی نرم‌افزار و از آنجا که مقادیر هر یک از معیارهای مذکور برای هر یک از متغیرهای مکنون بیشتر از حد نصاب و آستانه تعریف شده است؛ بنابراین، می‌توان مناسب بودن وضعیت پایایی و روایی همگرای مدل پژوهش را تأیید کرد.

ج) روایی واگرا

سومین معیار سنجش برازش مدل‌های اندازه‌گیری در تحلیل‌های PLS روایی واگرا است که، با روش بارهای عاملی متقابل و روش فورنل لارکر بررسی می‌شود. در روش اول میزان همبستگی بین شاخص‌های یک سازه با آن سازه و میزان همبستگی بین شاخص‌های یک سازه با سازه‌های دیگر مقایسه می‌شود. اگر مشخص شود میزان همبستگی بین یک شاخص با سازه دیگری غیر از سازه خود بیشتر از میزان همبستگی آن شاخص با سازه مربوط به خود است، روایی زیر سؤال می‌رود.

روایی واگرا معیاری است که نشان می‌دهد چقدر سنجه‌های عوامل متفاوت واقعاً باهم تفاوت دارند. در یک پرسشنامه برای سنجش عوامل مختلف سؤالات متعددی مطرح می‌شود، بنابراین لازم است که، مشخص شود این سؤالات از یکدیگر متمایز بوده و باهم همپوشانی ندارند. در پژوهش حاضر، سازه‌های مدل تعامل بیش تری با شاخصهای خود دارند تا با سازه‌های دیگر به‌عبارت دیگر روایی واگرای مدل در حد مناسبی است. برای کیفیت مدل اندازه گیری هر متغیر مکنون از شاخص اشتراکی نیز استفاده می‌کنند.

[1] Average Variance Extracted (AVE)

مقادیر مثبت این شاخص نشانگر کیفیت مدل اندازه‌گیری متغیرهای مکنون است.

۴-۴- برازش مدل ساختاری

مطابق با الگوریتم تحلیل داده‌ها در روش PLS پس از برازش مدل‌های اندازه‌گیری، برازش مدل ساختاری پژوهش بررسی می‌شود. برخلاف مدل‌های اندازه‌گیری که در آن روابط بین متغیر مکنون با متغیرهای آشکار مورد توجه است، در بررسی مدل ساختاری روابط بین متغیرهای مکنون با همدیگر تجزیه و تحلیل شده و معیارهای ضرایب معناداری t-values، معیار Squares یا R، معیار افزونگی برای برازش مدل ساختاری بررسی شد.

الف) مقادیر معناداری t

برای ارزیابی برازش مدل ساختاری پژوهش از چندین معیار استفاده می‌شود که، اولین و اساسی‌ترین آن ضرایب معناداری Z یا همان مقادیر t-values است که با اجرای فرمان بوت استراپیگ مقادیر بر روی خطوط مسیرها نشان داده می‌شوند. در صورتی‌که مقادیر t از ۱/۹۶ بیشتر باشد بیانگر صحت رابطه بین سازه ها و در نتیجه تأیید فرضیه‌های پژوهش در سطح اطمینان ۹۵ درصد است. با توجه به این که تمام اعداد واقع بر مسیرها بالاتر از ۱/۹۶ هستند. این مطلب حاکی از معنادار بودن مسیرها، مناسب بودن مدل ساختاری و تأیید تمام فرضیه های پژوهش است.

ب) معیار R Squares یا R^2

دومین معیار ضروری برای بررسی برازش مدل ساختاری بررسی ضرایب تعیین (R) مربوط به متغیرهای مکنون درونزای (وابسته) مدل است. این معیار برای متصل کردن بخش اندازه‌گیری و بخش ساختاری مدل‌سازی معادلات ساختاری به کار رفته و بیانگر تأثیر یک متغیر برونزا بر یک متغیر درونزا است. لازم به ذکر است مقادیر R در داخل دایره‌های مدل نشان داده شده و تنها برای سازه های درونزا (وابسته) مدل محاسبه می‌شود و در مورد سازه های برونزا مقدار این معیار صفر است. داوری و رضازاده به نقل از چین، سه مقدار ۰/۱۹، ۰/۳۳ و ۰/۶۷ را به‌عنوان ملاکی برای ضعیف، متوسط و قوی R و زیاد بودن مقدار آن را نشان از برازش بهتر مدل معرفی می‌کنند. مقادیر ضریب تعیین در جدول (۱۴) و اشکال (۷-۳) قابل مشاهده است. با توجه به این که مقدار R برای متغیرهای تهدیدات سخت ۰/۹۷۰، تهدیدات نیمه سخت ۰/۹۶۰، تهدیدات نرم ۰/۹۵۴، تهدیدات شناخته شده ۰/۹۶۲و تهدیدات ناشناخته (هوشمند) ۰/۹۱۵ محاسبه شده است، با در نظر گرفتن مقادیر فوق، ملاک مناسب بودن برازش مدل ساختاری تأیید می‌شود.

ج) معیار افزونگی[1]

این معیار از حاصل ضرب مقادیر اشتراکی سازه ها در مقادیر R^2 مربوط به آنها به دست آمده و نشانگر مقدار تغییر پذیری شاخص‌های یک سازه درونزا است که از یک یا چند سازه برونزا تأثیر می‌پذیرد. در مورد مقدار ملاک برای این شاخص عددی بیان نشده و میانگین شاخص افزونگی یک معیار کلی کیفیت مدل ساختاری است که برای همه سازه های درونزا به کار می‌رود و تنها برای استفاده در فرمول محاسبه برازش مدل کلی و شاخص نیکویی برازش محاسبه می‌شود مقادیر معیار افزونگی در جدول (۱۴) بر اساس خروجی تحلیل‌های نرم افزار گزارش شده است.

۴-۵- آزمون فرضیه ها

مطابق با الگوریتم تحلیل داده‌ها در روش PLS پس از بررسی برازش مدل‌های اندازه‌گیری ساختاری، اندازه‌گیری کلی مدل با بررسی ضرایب معناداری (Z مقادیر) هر یک از مسیرها و نیز ضرایب استاندارد شده بارعاملی مربوط به مسیرها فرضیه‌های تحقیق آزموده می‌شوند. در صورتی‌که مقدار ضریب معناداری هر یک از مسیرها بیش از ۱/۹۶ باشد، مسیر مربوطه در سطح اطمینان ۹۵ درصد معنادار و فرضیه مرتبط با آن تأیید می‌شود.

جدول(۱۵): نتایج آزمون مدل ساختاری پژوهش(منبع، محقق)

	مسیر	مقدار تی	ضریب همبستگی	نتیجه فرضیه
تهدیدات سخت	مقوله‌های بعد ایمنی	۴/۶۸	۰/۷۲۸	تایید
تهدیدات نیمه سخت	مقوله‌های بعد ایمنی	۴/۶۵	۰/۷۸۷	تایید
تهدیدات نرم	مقوله‌های بعد ایمنی	۲/۷۹	۰/۷۸۰	تایید
تهدیدات شناخته شده	مقوله‌های بعد ایمنی	۲/۶۰	۰/۷۳۳	تایید
تهدیدات ناشناخته (هوشمند)	مقوله‌های بعد ایمنی	۲/۶۵	۰/۷۸۳	تایید

[1] Redundancy

بر اساس جدول (۱۵) و مدل مفهومی آزمون شده در اشکال (۷-۳) و اعداد واقع بر خطوط، ضریب مسیر و ارتباط بین متغیرهای مکنون را نشان می‌دهد، برای بررسی میزان معنادار بودن ضریب مسیر، لازم است مقدار t هر مسیر نیز مورد توجه قرار گیرد. با توجه به این که مقدار ۱ ضرایب هر یک از مسیرها بالاتر از ۱/۹۶ است؛ بنابراین در سطح اطمینان ۹۵ درصد، مسیرهای پیش بینی شده مقوله‌های بعد ایمنی، متغییرها و عوامل مقوله‌های بعد ایمنی از متغیرهای مکنون و مولفه های موثر بر "تهدیدات سخت، تهدیدات نیمه سخت، تهدیدات نرم و تهدیدات ناشناخته (هوشمند)" ساختاری معنادارند. بنابراین رابطه بین متغیرها با بعد ایمنی تایید می‌شود. به عبارت دیگر بین دو متغییر ارتباط بزرگتر از ۱/۹۶ باشد، ارتباط معناداری میان آن دو متغییر وجود دارد (بین دو متغییر در سطح اطمینان ۹۵ درصد ارتباط معناداری وجود دارد). همچنین، بررسی نهایی نتایج نشان می‌دهد که، بین عوامل مورد بررسی نیز همبستگی مثبت و معنادار وجود دارد. لذا، فرضیه‌های طرح شده در تحقیق حاضر تأیید می‌شوند.

۵-یافته‌های تحقیق

به منظور تایید و برازش مدل مفهومی اولیه تحقیق، روشی برای سنجش میزان سازگاری یک الگوی نظری (تئوریک) با یک الگوی تجربی تحقیق می‌باشد. به منظور تایید و برازش مدل مفهومی‌تحقیق، برای هریک از مولفه‌ها، متغییرها و زیرمتغییرها سوالاتی در قالب پرسشنامه تحقیق تدوین گردید، هم به روش پیمایشی و هم به صورت میدانی جهت اخذ نظرات متخصصین، خبرگان، اساتید پخش گردیده و نظرات و عقاید آنها پس از جمع‌آوری وارد نرم‌افزار گردید. همچنین از آزمون تحلیل عاملی، باربودن مولفه‌ها، متغییرها و زیرمتغییرها ابعاد و ارتباط میان آنها مورد بررسی قرار گرفت. برای این منظور از شاخص‌های متعددی استفاده شد.

۵-۱-آزمون تحلیل عاملی جهت بررسی ارتباط میان ابعاد، مولفه‌ها، متغییرها:

روش‌های تحلیل عاملی در این تحقیق برمبنای اطلاعات به‌دست آمده در مورد وابستگی های متقابل بین متغیرهای مشاهده شده است که، می‌تواند برای تبیین ساختار شاخص‌ها، متغیرها و جهت بررسی ارتباط میان ابعاد، مولفه‌ها، متغییرهای امنیت و پدافندسایبری سازمان‌های دانش‌بنیان استفاده شده است. همچنین تحلیل بار عاملی یکی از متداول‌ترین تکنیک‌های وابستگی متقابل میان ابعاد، مولفه‌ها، متغییرهای تحقیق است و زمانی استفاده می‌شود که مجموعه متغیرهای مربوطه یک وابستگی متقابل سامانهاتیک را نشان می‌دهد و هدف، کشف ارتباط و میزان ارتباط عوامل و متغییرهای تحقیق است که یک اشتراک متقابل را ایجاد می‌کنند.

جهت تحلیل این موضوع ابتدا می‌بایست مشخص شود میان ابعاد، مولفه‌ها، متغییرها ارتباط معنادار وجود دارد یا نه؟! آزمون تحلیل عاملی این موضوع را مشخص می‌کند. به‌عبارت دیگر آزمون تحلیل عاملی جهت بررسی ارتباط معنادار بودن میان ابعاد، مولفه‌ها و همراستایی متغییرها و زیرمتغییرها تحقیق استفاده می‌گردد. در آزمون تحلیل عاملی، اگر بار عاملی محاسبه شده کمتر از ۰/۴ باشد بیانگر آن است که میان ابعاد، مولفه‌ها تحقیق ارتباط معناداری وجود ندارد، اگر مقدار به‌دست آمده بزرگتر از ۰/۴ باشد، ارتباط میان ابعاد، مولفه‌های تحقیق مورد تایید قرار می‌گیرد. با تحلیل عاملی انجام گرفته مشخص گردید، تمامی گویه‌های مورد بررسی مربوط به ابعاد، مولفه‌ها، متغییرهای تحقیق دارای بارعاملی بزرگتر از ۰/۴ می‌باشد. بنابراین تمامی گویه‌ها، مولفه‌ها مورد تایید قرار گرفتند.

مرتبط بودن هر یک از مؤلفه‌ها با ابعاد از طریق آزمون تحلیل عاملی مورد بررسی قرار گرفت، نتایج به‌دست آمده در جداول مربوطه نشان می‌دهد که، تمامی عامل‌های در نظر گرفته شده برای هر یک از مؤلفه‌ها دارای بار عاملی بزرگتر از ۰/۴ هستند؛ بنابراین بر روی ابعاد مربوطه به خوبی بار می‌شوند یا به‌عبارتی مؤلفه‌های زیرمجموعه ابعاد مرتبط بوده، تشکیل بخشی از سازه‌های مدل را می‌دهد؛ بنابراین مؤلفه‌ها با ابعاد به هم وابسته بوده و دارای ارتباط معنادار می‌باشند.

۵-۲- مدل مفهومی[1]

طراحی مدل مفهومی براساس الگوی سامانهی طراحی شده است. برای شناخت مدل مفهومی، سامانه به‌عنوان یک کل نگریسته می‌شود که، اجزای آن با ارتباط و همکاری مشترک هدف خاص یا

[1]Conceptual Model

مورد نظری را دنبال می‌کنند در پاسخ به‌این سؤال که «مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان چگونه است؟»، ضمن شناسایی و بررسی ابعاد مؤلفه‌ها، متغییرها و زیرمتغییرها مدل تحقیق طراحی، تأیید و مورد قبول قرار گرفت.

۵-۳- سایر یافته ها براساس متغیرهای و مولفه ها

➢ به منظور طراحی مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور، اجزاء و مولفه‌های مؤثر بر سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری از ادبیات شناسایی و با تحلیل داده‌های میدانی با روش مربعات جزیی به عنوان یکی از جدیدترین رویکردها در مدل سازی معادلات ساختاری (PLS-SEM) هدف پژوهش محقق شد. به طور کلی عوامل و مولفه های "تهدیدات سخت، تهدیدات نیمه سخت، تهدیدات نرم، سایر تهدیدات شناخته شده و تهدیدات ناشناخته (هوشمند)" نقش اساسی در تبیین سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری را برعهده داشتند.

➢ در بین مولفه‌های عوامل تهدیدات سخت؛ مولفه‌های میزان اهمیت مراکز و سازمان‌ها با ضریب و بارعاملی ۰/۸۸۵ و پیاده‌سازی پروژه‌های امنیت‌اطلاعات ا ضریب و بار عاملی ۰/۸۷۵ به ترتیب بیشترین تأثیر را بر سطح بندی تهدیدات سخت داشته و مولفه‌های تایید اصل امایش سرزمین با ضریب و بارعاملی ۰/۸۰۲ و طراحی اماکن و مراکز داده ای با ضریب و بارعاملی ۰/۸۱۰ کمترین تأثیر را بر سطح‌بندی انواع تهدیدات سخت در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشوردارند.

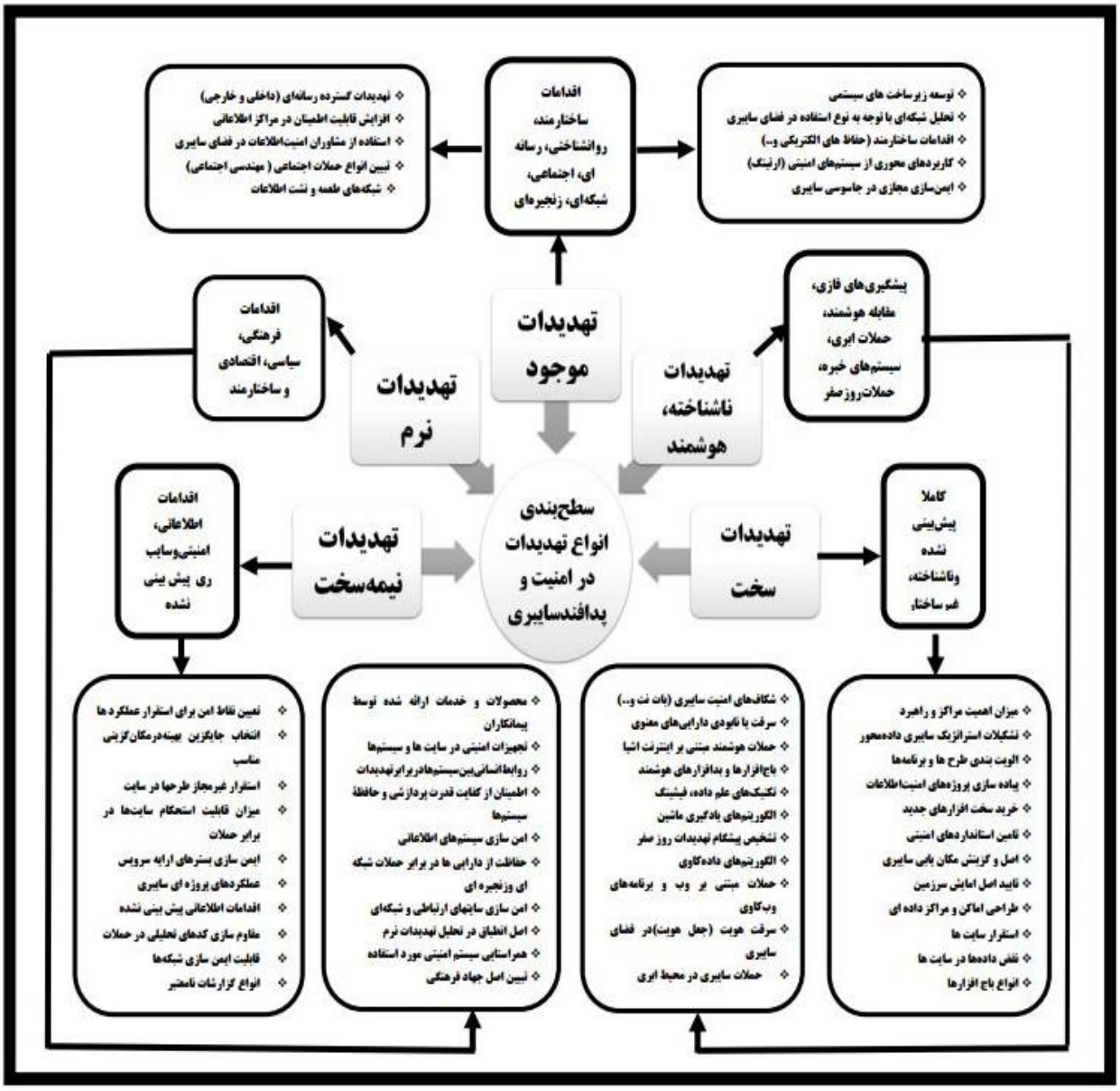
➢ در بین مولفه‌های عوامل تهدیدات نیمه سخت، مولفه‌های عملکردهای پروژه‌ای سایبری با ضریب و بارعاملی ۰/۸۸۲و اقدامات اطلاعاتی پیش بینی نشده ۰/۸۷۵ به ترتیب بیشترین تأثیر را بر سطح بندی تهدیدات نیمه سخت داشته و مولفه‌های تایید انتقال، دستکاری غیرمجاز داده با ضریب و بارعاملی ۰/۷۸۸و انواع گزارشات نامعتبر و ایمن سازی بسترهای ارایه سرویس با ضریب و بارعاملی ۰/۷۹۵ کمترین تأثیر را بر سطح‌بندی انواع تهدیدات نیمه سخت در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشوردارند.

➢ در بین مولفه‌های عوامل تهدیدات نرم مولفه‌های روابط بین سامانه‌ها دربرابر حملات و تهدیدات با ضریب و بارعاملی ۰/۸۳۶، محصولات، خدمات ارائه شده توسط پیمانکاران با ضریب و بار عاملی ۰/۸۲۵ و حفاظت از دارایی‌ها در برابر حملات شبکه‌ای با ضریب و بار عاملی ۰/۸۲۵ به ترتیب بیشترین تأثیر را بر سطح بندی تهدیدات نرم داشته و مولفه‌های امن‌سازی سامانه‌های اطلاعاتی و تبیین اصل جهاد فرهنگی با ضریب و بارعاملی ۰/۸۰۵ کمترین تأثیر را بر سطح‌بندی انواع تهدیدات نرم در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشوردارند.

➢ در بین مولفه‌های عوامل سایر تهدیدات تهدیدات موجود (شناخته شده)؛ مولفه‌هایکاربردهای محوری از سامانه‌های امنیتی در سایت‌ها با ضریب و بارعاملی ۰/۸۳۶ و استفاده از مشاوران امنیت‌اطلاعات در فضای سایبری با ضریب و بار عاملی ۰/۸۳۵ به ترتیب بیشترین تأثیر را بر سطح بندی تهدیدات سخت داشته و مولفه‌های توسعه زیرساخت‌های سامانه‌ها با ضریب و بارعاملی ۰/۸۰۵و ایمن‌سازی مجازی در فضای سایبری با ضریب و بارعاملی ۰/۸۱۰ کمترین تأثیر را بر سطح‌بندی انواع تهدیدات موجود (شناخته شده) در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشوردارند.

➢ در بین مولفه‌های عوامل تهدیدات ناشناخته (هوشمند) مولفه‌های هکتیویسم‌های مبتنی بر هوش‌مصنوعی با ضریب و بارعاملی ۰/۸۶۵، تشخیص پیشگام تهدیدات روز با ضریب و بارعاملی ۰/۸۵۶و حملات مبتنی بر وب، هک وب‌کاوی با ضریب و بار عاملی ۰/۸۵۵ به ترتیب بیشترین تأثیر را بر سطح بندی تهدیدات ناشناخته (هوشمند) داشته و مولفه‌های بدافزارهای برنامه‌نویسی‌شده با ضریب و بارعاملی ۰/۸۰۵ و انواع تکنیک‌های علم داده مخرب با ضریب و بارعاملی ۰/۸۱۲ کمترین تأثیر را بر سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشوردارند.

همچنین؛ می‌توان این‌گونه بیان نمود، هدف اصلی تحقیق دستیابی به «مدل مفهومی دستیابی به یک مدل کاربردی در راستای سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان، تجزیه‌وتحلیل سطوح مختلف تهدیدات در امنیت و پدافندسایبری این سازمان‌ها در سطح کشور می‌باشد. در شکل (۸).مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور نمایش داده شده است:



شکل (۸): مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور

❖ داده‌های جمع آوری شده، تجزیه‌وتحلیل برروی آنها صورت پذیرفت. همچنین آزمون تحلیل عاملی درراستای بررسی ارتباط میان ابعاد، مولفه‌ها، متغییرها انجام پذیرفته و مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان به خوبی تبیین گردید. الگوی حاصل از این پژوهش، روابط بین ابعاد، مؤلفه‌های آن‌که در شکل شماره (۲،۱) نمایش داده شده است، بیانگر واقعیت تعاملات، ارتباطات میان بخش‌های مختلف، ارتباط میان ابعاد، مولفه‌ها، متغییرهای تحقیق درراستای سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری در سازمان‌های دانش‌بنیان را تبیین می‌نماید.

❖ در این خصوص از شاخص‌های برازندگی برای تعیین برازندگی و اعتبار مدل مفهومی طراحی شده، سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان کشور، استفاده گردید. با استفاده از شاخص‌های برازندگی، همپوشانی مدل مفهومی با داده‌های تجربی مقایسه گردیده و شاخص‌های متعددی برای سنجش برازندگی مدل استفاده شد.

❖ این تحقیق دارای ۵ بعد، مولفه متفاوت در تشکیل مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان بود. اولین بعد، مولفه مربوط به تهدیدات سخت که در برگیرنده متغییرها، زیرمتغییرهای کاملا

پیش‌بینی‌نشده، شناخته‌شده، غیرساختار بوده، دومین بعد، مولفه مربوط به تهدیدات نیمه‌سخت که در برگیرنده متغییرها، زیرمتغییرهای اقدامات اطلاعاتی، امنیتی و سایبری که بصورت پیش بینی نشده، نیمه‌ساختارمند است، سومین بعد، مولفه مربوط به تهدیدات نرم که در برگیرنده متغییرها، زیرمتغییرهای اقدامات فرهنگی، سیاسی، اقتصادی و ساختارمند می‌باشد، چهارمین بعد، مولفه مربوط به تهدیدات موجود شناخته‌شده که در برگیرنده متغییرها، زیرمتغییرهای اقدامات ساختارمند، روانشناختی، رسانه‌ای، اجتماعی، شبکه‌ای، زنجیره‌ای و ... است، پنجمین، آخرین بعد، مولفه مربوط به سایرتهدیدات ناشناخته، هوشمند که در برگیرنده متغییرها، زیرمتغییرهای پیشگیری‌های فازی، حملات مبتنی بر هوش‌مصنوعی و مقابله با آسیب‌ها بصورت هوشمند، حملات ابری، سامانه‌های امنیتی خبره، انواع حملات روزصفر می‌باشد.

۴- نتیجه‌گیری و پیشنهادات

مرتبط بودن تجزیه‌وتحلیل داده‌های تحقیق نشان داد، حملات سایبری به زیرساخت‌های سازمانی و حیاتی، مانند شبکه‌های اینترنتی، سامانه‌های توزیع برق، تلفن همراه، سامانه‌های مخابراتی، و زیرساخت‌های سازمان‌ها و ... آسیب جدی وارد می‌نماید، لذا تهدیدی جدی برای امنیت و پایداری سازمان‌ها به حساب می‌آیند. با پیشرفت فناوری‌های مختلف مانند هوش‌مصنوعی، استفاده از آن هم در بخش حمله و هم مقابله با انواع حملات سایبری در سازمان‌ها بسیار موثر می‌باشد.

۴-۱- نتیجه‌گیری

➢ بعد تهدیدات سخت، تحت تاثیر زیرمولفه‌ها، زیرمتغییرهای اهمیت مراکز و راهبرد، تشکیلات استراتژیک سایبری داده محور، الویت‌بندی طرح ها، طبقه‌بندی برنامه‌ها، پیاده‌سازی پروژه‌های امنیت‌اطلاعات، خرید سخت افزارهای جدید، تامین استانداردهای امنیتی، اصل و گزینش مکان‌یابی سایبری، تایید اصل امایش سرزمین، طراحی اماکن و مراکز داده‌ای، استقرار سایت‌ها، نقض داده‌ها در سایت‌ها، انواع باج‌افزارها قرار دارد، که بطور مستقیم برسطح‌بندی تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان تاثیر مثبت می‌گذارد.

➢ همچنین بعد تهدیدات نیمه‌سخت نیز تحت تاثیر زیرمولفه‌های ساختارهای ثانویه، به‌عنوان یک فناوری پیشرفته، نقش بسیار مهمی در حملات سایبری ایفا می‌کند. توانایی‌های دانشی، نرم‌افزاری در تحلیل داده‌ها، شناسایی الگوها، پیش‌بینی رفتارها، آن را به یک ابزار قدرتمند برای حملات سایبری تبدیل کرده است. با استفاده از نرم‌افزارهای، حمله‌کنندگان می‌توانند الگوریتم‌ها، مدل‌های استاندارد بین‌المللی را در حملات سایبری خود بکار بگیرند. این الگوریتم‌ها می‌توانند با تجزیه‌وتحلیل داده‌های بزرگ، شناسایی ضعف‌ها، نقاط ضعف در سامانه‌های امنیتی، حملات را بطور ساختارمند انجام دهند.

➢ همچنین سایر نتایج نشان داد، تهدیدات‌نرم تحت تاثیر زیرمولفه‌های محصولات، خدمات ارائه شده توسط پیمانکاران، تجهیزات امنیتی در سایت‌ها و سامانه‌ها، روابط بین سامانه‌ها در برابر حملات و تهدیدات، اطمینان از کفایت قدرت پردازشی و حافظهٔ سامانه‌ها، امن سازی سامانه‌های اطلاعاتی، حفاظت از دارایی ها در برابر حملات شبکه‌ای و زنجیره‌ای، امن‌سازی سایت‌های ارتباطی و شبکه‌ای، اصل انطباق در تحلیل تهدیدات‌نرم، همراستایی سامانه امنیتی مورد استفاده، تبیین‌اصل جهاد فرهنگی، اصل غفلت از تهدیدات داخلی قرار دهد.

➢ همچنین بررسی نتایج حاصل از تجزیه‌وتحلیل داده‌ها نشان داد، تهدیدات شناخته شده (موجود) تحت تاثیر زیرمولفه‌های توسعه زیرساخت‌های سامانهی، تحلیل شبکه‌ای با توجه به نوع استفاده در فضای سایبری، اقدامات ساختارمند (حفاظهای الکتریکی، ساختارهای امنیتی، اشباع سامانه‌های ماهواره‌ای، کیت‌های جاسوسی، کاربردهای محوری از سامانه‌های امنیتی (ارتینگ و....) در سایت‌ها، ایمن‌سازی مجازی در جاسوسی سایبری،تهدیدات گسترده رسانه‌ای (داخلی و خارجی)، افزایش قابلیت اطمینان در مراکز اطلاعاتی، استفاده از مشاوران امنیت اطلاعات در فضای سایبری، تبیین انواع حملات اجتماعی (مهندسی اجتماعی)، شبکه‌های طعمه و نشت اطلاعات قرار دارد.

➢ همچنین نتایج حاصل از تجزیه‌وتحلیل داده‌ها درخصوص تهدیدات ناشناخته (هوشمند) نشان داد، تهدیدات ناشناخته (هوشمند) تحت تاثیر زیرمولفه‌های شکاف‌های امنیت‌سایبری (بات نت[1] و..)، سرقت یا نابودی دارایی‌های معنوی، حملات هوشمند مبتنی بر اینترنت اشیا، انواع باج‌افزارها، بدافزارهای هوشمند، تکنیک‌های علم داده، عملیات فیشینگ، الگوریتم‌های یادگیری ماشین، تشخیص پیشگام تهدیدات روزصفر، الگوریتم‌های داده‌کاوی، حملات مبتنی بر وب، برنامه‌های هک، وب‌کاوی، سرقت هویت (جعل هویت) در فضای سایبری، حملات سایبری در محیط ابری، هکتیویسم‌های مبتنی بر هوش‌مصنوعی[2] براساس سطح‌بندی تهدیدات در امنیت و

[1] Botnets
[2] Hacktivism based on artificial intelligence

پدافندسایبری سازمان‌های دانش‌بنیان کشور قرار دارد.

➢ این تحقیق ارتباط میان ابعاد گوناگون، مولفه‌ها، متغییرها، زیرمتغییرهای مختلف انواع تهدیدات در امنیت و پدافند سایبری را در تحقیق مشخص نموده و قالب‌های گوناگون سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان مشخص نمود. براساس نتایج حاصل از تجزیه‌وتحلیل آنها مدل مفهومی سطح‌بندی انواع تهدیدات در امنیت و پدافندسایبری سازمان‌های دانش‌بنیان ترسیم گردید. لازم بذکر است تمامی ابعاد، مولفه‌ها، متغییرها این مدل برگرفته از ساختارها، اصول بنیادین امنیت و پدافندسایبری بومی کشور بوده و مطابق با اسناد بالادستی کشور مانند آیین‌نامه‌های امنیت و پدافندسایبری افتا ریاست جمهوری، آیین‌نامه امنیت و پدافندسایبری معاونت علمی‌وفناوری ریاست‌جمهوی، سندراهبردی امنیتی ارائه شده توسط سازمان فناوری اطلاعات‌وارتباطات و سندراهبردی پدافندسایبری کشور می‌باشد.

۴-۲-پیشنهادات تحقیق

➢ حملات سایبری، بویژه حملات مهندسی اجتماعی، همچنان به رشد و تکامل خود ادامه می دهند. با افزایش تقاضای باج و تهاجمات جدید و شدید به سامانه‌عامل‌های ابری[1]، برای صاحبان مشاغل هرگز مهم نیست که، بطور فعال وضعیت امنیت سایبری خود را بررسی کنند. درک نحوه مقابله با حملات سایبری به یک تعهد حیاتی در تضمین آینده مالی و اعتباری مشتریان، از شرکت های بزرگ گرفته تا مشاغل کوچک تبدیل شده است. یک طرح پیشگیری از حملات سایبری به مشتریان و مدیران امنیت سایبری کمک می‌کند، نه تنها از حملات جلوگیری کنند، بلکه آماده باشند تا زمانی که زمان آن فرا می رسد و حمله سایبری رخ می‌دهد، پاسخ دهند. حمله سایبری بهره برداری عمدی از سامانه‌ها یا شبکه است. حملات سایبری از کدهای مخرب برای به خطر انداختن رایانه، منطق یا داده های سازمانی و سرقت، درز یا گروگان نگه داشتن داده‌ها استفاده می‌کنند. پیشگیری از حملات سایبری برای هر کسب‌وکار و خصوصا سازمان‌های دانش‌بنیان ضروری است. لذا پیشنهاد می‌شود:

➢ انواع تهدیدات سایبری مانند سرقت هویت[2]، کلاهبرداری، اخاذی، بدافزار، فیشینگ، هرزنامه، جعل، نرم‌افزارهای جاسوسی، تروجان‌ها[3]، ویروس‌ها با نمونه‌ها و مدل‌های مختلف با سایر کشورها مورد مقایسه قرار گیرد.

➢ مدل ارائه با سایر مدل‌های موجود مورد مقایسه قرار گرفته و با برخی از مدل مورد تطبیق قرار گیرد.

➢ انواع تهدیدات سخت، نیمه سخت، تهدیدات نرم و .. براساس نوع مولفه‌ها، متغییرها در سازمان‌های گوناگون مورد بررسی ومقایسه جداگانه صورت گیرد.

➢ الگوی مفهومی جدیدی براساس انواع تهدیدات برای سازمان‌های مختلف نیز مورد بررسی قرار گرفته، سپس با مدل مفهومی ارائه شده برای سازمان‌های دانش‌بنیان کشور مورد مقایسه قرار گیرد .

[1] Cloud Operating Systems
[2] Identity theft
[3] Trojans

۵- مراجع

[1] A. Taati, "Presenting a native model for the implementation of information security management in a service organization," Master's thesis (Islamic Azad University, Science and Research Unit, Faculty of Management and Economics, Department of Information Technology Management, Information Technology Management, Advanced Information Systems), 2019. (In Persian)

[2] United Nations performance research working group, Offices attached to the United Nations, annual report on the performance of various working groups of the United Nations. United Nations International Unit Publications, 2020. https://www.un.org/annualreport/2020/files/2020/09/Annual-report

[3] B. E. Sarfarazi and M. Mohammadi, "Presenting the model of effective factors on talent management in knowledge-based companies with an emphasis on the longevity of knowledge workers," Journal: Productivity Management » Spring - No. 60 Scientific-Research Rank, ISC (30, page - from 78 to 107, 2023. (In Persian)

[4] M. Khalafkhani, "Information and communication opportunities for democratization in cyber space," Guided by Abdul Ali Qawam; Consulting Ahmed Sae, Mohammad Amjad. Ph.D. (Islamic Azad University. Science and Research Unit, Faculty of Law and Political Science, Department of Political Science), 2013. (In Persian)

[5] IBM Cyber Security Annual Report, IBM Cyber Security and Defense Industry Research and Development Center, IBM Cyber Security Center of Excellence (CCoE) 2023. https://research.ibm.com/haifa/ccoe/motivation.shtml

[6] M. R. Zandi, "Preliminary investigations in cyber crimes," Tehran, Jungle: Javadane, pp. 42-10, 2011. (In Persian)

[7] A. R. Kaldi, "Recognizing the threats and social harms of Tehran and the future perspective with emphasis on Shahran neighborhood (District one of Panj region municipality)," Lutfi Hassan Ali consulting Mehrdad Navabakhsh. Master's Thesis (Islamic Azad University, Department of Science and Research, Faculty of Humanities and Social Sciences, Research Field of Social Sciences), 2013. (In Persian)

[8] Z. Zaheri, "Investigating security threats in cloud computing and providing a secure method for data storage," Guided by Mahmoud Al Borzi; Consulting Alireza Pourebrahimi. Master's degree (Islamic Azad University, Department of Science and Research, Faculty of Management and Economics, Department of Information Technology Management), 2019. (In Persian)

[9] R. Taghipour and A. Esmaili, "Designing a Conceptual Model of the Cyber Defense Model of the Islamic Republic of Iran," Magazine: National Security » Winter, Year 8 - Scientific-Research Number 30/ISC (22 pages - from 181 to 202, 2018. (In Persian)

[10] Mousavi et al., "Strategies to improve the capabilities of electronic and cyber warfare (cyberelectronics) of the armed forces against unequal threats," pp. 22-34, 2020. (In Persian)
[11] E. Mirzai Dizaji, "Strategies for improving information security management using interpretive structural modeling method (case study: Tehran Municipal Organization)," Guided by Ahmed Reza Ghasemi; Advising Ehsan Sadeh. Master's degree (Islamic Azad University, Science and Research Unit, Faculty of Management and Economics, Department of Information Resource Management), 2021. (In Persian)
[12] R. Sadeh, "The issue of evaluating the model of various information security indicators in organizations," master's thesis, pp. 12-56, 2022. (In Persian)
[13] E. D. Rousseau, "Protecting national infrastructures against cyber attacks," Translated by Ahmad Salahi; Communication and Information Technology Research Center (Iran Telecommunication Research Center). Tehran: Arad Kitab, 2016.
[14] Khin Than Win, D. Elena Vlahu-Gjorgievska, "Information Security Governance Challenges and Critical Success Factors: Systematic Review," Computers & Security In press, journal pre-proofAvailable online September 3. 2020.
[15] U. Ulrik Franke, A. Andreasson, and Niklas Vilhelm, "Cyber situational awareness issues and challenges," Cybersecurity and Cognitive Science17, Chapter 10, June 2022.
[16] D. Damjan Fujs, S. Simon Vrhovec, and D. Damjan Vavpotič, "Balancing software and training requirements for information security," Computers & Security2 September 2023.
[17] Cyber Security and Defense Task Force, Cyber Security and Defense Center Report, EU Cybercrime Centre, 2022.
[18] V. R. Zeraat pisheh, "Security pathology of mobile phone use among middle school male students of Sepidan city," Guided by Ahmed Yazdi Yazdanabadi; Consulting Saeed Zarghami. Master's degree (Islamic Azad University, Science and Research Unit, Educational Management), 2018. (In Persian)
[19] Z. Nasirirad, "Comparison of the amount and manner of using Facebook social networks with Viber and WhatsApp mobile phone programs (case study: university students of Research Sciences Unit and students of Stockholm KTH University)," Guided by Shahnaz Hashemi; Advising Afsana Mozafari, Master's degree (Islamic Azad University, Department of Science and Research, Department of Social Communication Sciences), 2015. (In Persian)
[20] The process of modeling various types of threats in the field of cyber security and defense, Cisco, 2023.
[21] A. R. Purebrahimi, "The best in information security," Azad Islamic University, Electronic Department. Publications of Azad Islamic University, 2018. (In Persian)
[22] M. R. Behbodhi, "Evaluation of Information Security Management (ISMS) in Hormozgan University and providing strategies for its improvement," Master's Thesis, Hormozgan University, Faculty of Literature and Humanities, 2018. (In Persian)
[23] A. M. Mahdavi, "Evaluation of information security indicators in Tehran Stock Exchange and Securities Organization," Biglarbagian Parisa. Consultant professor: Mohammad Soltani Delgosha. Zahra Razmi Master's thesis. Al-Zahra University (S). Faculty of Economics and Accounting, 2013. (In Persian)
[24] M. Mari Karjalainen, M. Mikko Siponen, and S. Suprateek Sarker,Toward a stage theory of the development of employees' information security behavior. Computers & Security. June, 2020.
[25] E. Edyta Karolina Szczepaniuk, H. Hubert Szczepaniuk, Tomasz Rokicki, Bogdan Klepacki. , Information security assessment in public administration. Computers & SecurityMarch, 2020.
[26]. A. R. Alizadeh Soodmand, Azimi. Zahra, Explanation of the strategies of empowering commanders and managers in organizations, the first national conference of Islamic command and management, Bahman. Imam Hussain (AS) University, 2020. (In Persian)
[27] V. Sajjadi and D. Azar, "Improving the ability of the Islamic Republic of Iran Army to deal with the cyber operations of the US Army," Magazine: Military Sciences and Techniques » Spring. ISC scientific-research number 51. 22 pages - from 5 to 26, 2019. (In Persian)
[28] S. H. Kazemi, "Investigation and identification of effective factors in information security management in electronic universities of Iran (case study: electronic unit of universities located in Tehran)," Fathnejad cross-border guide; Amir Massoud Rahmani's advice. Master's degree (Islamic Azad University, Science and Research Unit, Faculty of Management and Economics, Department of Information Technology Management), 2017. (In Persian)
[29] A. Ali Kavak and H. Hüseyin Odabaş, "The impact of information security management guide utilization on technological and institutional information security measures in university libraries in Türkiye," The Journal of Academic Librarianship 16 October 2023.
[30] S. Sebastian Hengstler, S. Stephan Kuehnel, and S. Simon Trang, "Should I really do that? Using quantile regression to examine the impact of sanctions on information security policy," compliance behavior, 2023.