Electronical & Cyber Defence
Vol. 13, No. 1, Spring 2025, Serial No. 49

Explanation of the Stratification Strategy of Various Threats in security and Cyber Defense of Knowledge-Based Organizations in the Country

A.R. Alizadeh Soodmand [1]*, K. Fathi Hafeshjani [2], A. Shah Mansouri [3] , A. Arab Sorkhi

*PhD student, Information Technology Management, Islamic Azad University, South Tehran Branch, Tehran, Iran

Received:2024 /10/30, Revised: 2024/12/24, Accepted: 2025/03/03, Published: 2025/04/21

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.1.8.3

ABSTRACT

In recent years, the rapid development of knowledge-based companies and the need to pay attention to all kinds of threats in these organizations are considered as the most important challenges in their development. The continued life of these organizations depends on the principle of leveling various types of threats in organizations. The main goal of the research is the leveling of various threats in cyber security and defense of knowledge-based organizations. The research method was descriptive-survey based on the applied purpose, descriptive-survey based on the data collection method, and quantitative based on the type of data. The statistical population of this research is the experts and professors of information technology and…, Islamic Azad University, Tehran South branch (200 people), the samples were selected using random sampling, data analysis and research hypotheses were done with SPSS$_{(23)}$ software. In the inferential statistics section, Kolmogorov-Smirnov tests were used to check the normality of the data, and Spearman's correlation coefficient was used to evaluate the impact and significance of the relationships between variables. All the data are normal, and there is a significant relationship between the research factors and components. The results of data analysis showed that of the four existing hypotheses, the first, second, and third hypotheses were confirmed and the fourth hypothesis was not confirmed. Then the research components were ranked, other results showed that the research variables do not have the same priority, there is a significant difference between them. In terms of leveling, there is a significant difference between the variables. It was found that the research variables have different levels in different research levels.

Keywords: : Strategic, Threat leveling, Security, Cyber defense, Knowledge-Based Organizations

❖ Corresponding Author Email: aras.soud@gmail.com

"پدافند الکترونیکی و سایبری"
سال سیزدهم، شماره ۱، بهار ۱۴۰۴، ص۱۱۶-۹۵
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

علمی – پژوهشی

تبیین راهبرد سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور

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

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 واحدتهران جنوب، تهران، ایران ۳- استادیار ، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران

(دریافت: ۱۴۰۳/۰۸/۰۹، بازنگری: ۱۴۰۳/۱۰/۰۴، پذیرش: ۱۴۰۳/۱۲/۱۳، انتشار: ۱۴۰۳/۰۲/۰۱)

DOR: https://dor.isc.ac/dor/20.1001.1.23224347.1404.13.1.8.3

چکیده

در سال‌های اخیر توسعه سریع شرکت‌های دانش‌بنیان و لزوم توجه به انواع تهدیدات در این سازمان‌ها به‌عنوان مهم‌ترین چالش در توسعه آنها به شمار می‌آید. ادامه حیات این سازمان‌ها، منوط به تبیین اصل سطح‌بندی انواع تهدیدات در سازمان‌هاست. هدف اصلی پژوهش، سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان است. روش پژوهش برحسب هدف کاربردی، از نظر روش گردآوری داده‌ها، توصیفی - پیمایشی از نوع همبستگی و از نظر نوع داده کمی بود. جامعه آماری این پژوهش، خبرگان و اساتید فناوری اطلاعات و... شرکت‌های دانش‌بنیان وابسته به دانشگاه آزاد اسلامی واحدهای تهران است (۲۰۰ نفر)، نمونه‌ها با استفاده از نمونه‌گیری تصادفی انتخاب شده، تحلیل داده‌ها و فرضیه‌های تحقیق، با نرم‌افزار $SPSS_{(23)}$ صورت پذیرفت. در بخش آمار استنباطی از آزمون‌های کولموگروف - اسمیرنف، جهت بررسی نرمال بودن داده‌ها، از ضریب همبستگی اسپیرمن جهت ارزیابی تأثیر و معنادار بودن ارتباطات میان متغیرها استفاده شد. داده‌ها نرمال نبوده و میان عوامل و مؤلفه‌های تحقیق ارتباط معناداری وجود دارد. نتایج حاصل از تجزیه‌وتحلیل داده‌ها نشان داد، از پنج فرضیه فرعی از فرضیه اول اصلی، فرضیه اول، دوم، چهارم و پنجم تأیید شده و فرضیه سوم فرعی تأیید نشد. بر اساس فرضیه دوم اصلی، مؤلفه‌های تحقیق رتبه‌بندی شده، نتایج نشان داد، متغیرهای تحقیق از اولویت یکسانی برخوردار نیستند، تفاوت معناداری میان آنها وجود دارد. از لحاظ سطح‌بندی میان متغیرها تفاوت معناداری وجود دارد. مشخص شد، متغیرهای تحقیق، دارای سطح‌بندی متفاوتی در سطوح مختلف تحقیق هستند.

کلیدواژه‌ها: راهبرد، سطح‌بندی تهدیدات، امنیت، پدافند سایبری، سازمان‌های دانش‌بنیان

نویسنده مسئول: * aras.soud@gmail.com

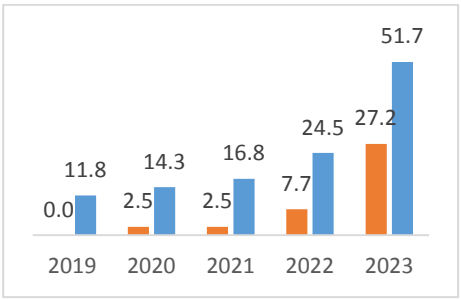
۱. مقدمه

امروزه بسیاری از سازمان‌ها به دنبال ایجاد تغییرات گسترده در شیوه‌های طراحی، توسعه فرایندها و مدیریت سازمانی هستند. هدف اصلی از این تغییرات، کسب برتری ساختارمند و مزیت رقابتی در راستای اهداف عالی سازمان [1] است. عوامل مختلفی همچون؛ مدیریت سازمانی، دانش سازمانی [2]، توسعه انواع محصولات، خدمات سازمانی و بهره‌گیری از فناوری‌های نوین همانند فناوری اطلاعات به‌عنوان اهرم و محور پیشرفت است. رقابت در بازار امروزی و پایداری در این میدان پرتلاطم، نیازمند جهت-گیری‌های مناسب نهادها، شرکت‌ها و سازمان‌هاست.

شرکت‌ها، به‌خصوص شرکت‌های نوآور و سازمان‌های دانش‌بنیان [3] باید بتوانند با دانش و اطلاعاتی که از مشتریان، بازار و رقبا به دست می‌آورند، محصولات متناسب با شرایط محیط و بازار را تولید کنند تا پایداری آنان در میدان رقابت تضمین گردد [1].

۱-۱. بیان مساله

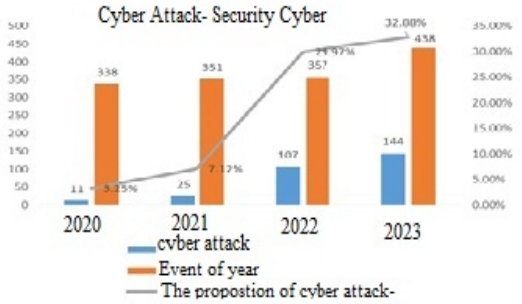
در سال‌های اخیر سازمان‌های اطلاعات‌محور و شرکت‌های دانش‌بنیان دریافته‌اند که برای رویارویی با انواع بحران‌ها، مسائل و تهدیدات باید آمادگی کاملی داشته باشند. برخی از سازمان‌ها با نحوه مقابله با انواع تهدیدات آشنا هستند یا می‌دانند چگونه می‌توان به یک سازمان مقاوم در برابر انواع تهدیدات و آسیب‌ها تبدیل شوند [2]. افزایش انواع تهدیدات و بحران‌ها در فضای سایبر در سازمان‌های دانش‌بنیان، سبب تغییرات گسترده در حاکمیت امنیت در بخش‌های مختلف سازمان‌ها و شرکت‌های دانش‌بنیان شده است. لذا باید ساختار جدیدی برای کاهش تهدیدات در این سازمان‌ها ایجاد شده و راهبردهای امنیتی جدیدی برای کاهش، مدیریت تهدیدات و آسیب‌ها در فضای سایبری اعمال گردد (نمودار۱) [3]. بر اساس گزارش‌های سازمان امنیت و پدافند سایبری چین، در سال ۲۰۲۳ اکثر تهدیدات و حملات در فضای سایبری بر اساس نفوذ در سیستم‌های اطلاعاتی، سیستم‌های شبکه‌ای، تهدیدات هوشمند، حملات ساختاریافته، توسعه باج‌افزارها [4] و بدافزارهای نوین [5] و... می‌باشد [4].



نمودار ۱. گزارش تهدیدات و بحران‌ها در فضای سایبر تا سال ۲۰۲۳

همچنین بر اساس گزارش‌ها متعدد از مراکز امنیتی هند، از سال ۲۰۰۰ در راستای مجهز کردن مراجع قضایی به قوانین مرتبط با جرایم سایبری، اقدامات اجرایی متعددی از سوی دولت هند انجام گرفت. از جمله این اقدامات می‌توان به تأسیس دفتر هماهنگ‌کننده امنیت سایبری، در دبیرخانه شورای‌عالی امنیت ملی آن کشور اشاره کرد که باهدف هماهنگ‌کردن نهادهای مختلف، در امر حفظ و ارتقای امنیت سایبری در سطح ملی فعالیت می‌کنند، راه‌اندازی شد. تأسیس مراکز مختلف امنیت سایبری و سازمان‌های پدافند سایبری جهت کاهش تهدیدات سایبری و جرایم سایبری در دیگر کشورها از الزامات هر کشوری به شمار می‌آید [5]. مراکز مختلف امنیت و پدافند سایبری در کشورهای درحال‌توسعه، می‌بایست بر فرایند امنیت اطلاعات و پدافند سایبری نظارت و کنترل داشته باشند، تا بتوانند در مواقع لزوم با انواع تهدیدات و آسیب مقابله نموده و خطرات ناشی از آنها را کاهش دهند. همچنین وجود چنین مراکزی در حوزه امنیت و پدافند سایبری در کشورهای مختلف، خصوصاً سازمان‌های دانش‌بنیان و فناور به‌عنوان یکی از الزامات اساسی جهت جلوگیری از حملات ناخواسته، کاهش تهدیدات و آسیب‌پذیری‌ها در این سازمان‌ها می‌باشد. مراکز امنیت و پدافند سایبری در شرکت‌های دانش‌بنیان به‌عنوان نهادی که در زمینه اطلاع‌رسانی و مقابله با انواع تهدیدات سایبری فعالیت می‌کنند، مطرح هستند. این مراکز در حوزه‌های اشتراک‌گذاری اطلاعات حساس بین نهادهای امنیتی دخیل در بحث امنیت سایبری نیز مشارکت می‌کند [2,3]. در کنار راه‌اندازی مراکز مختلف امنیت و پدافند سایبری در کشورهای درحال‌توسعه، وجود یک نهاد تحت عنوان مرکز محافظت از زیرساخت‌های اطلاعاتی [6] حیاتی ملی بایستی تأسیس گردید. در سال ۲۰۱۸ نهاد مستقلی در سازمان ملل متحد تحت عنوان، بخش امنیت سایبری و اطلاعاتی بین‌الملل تأسیس شد، اکثر کشورهای جهان در این نهاد بین‌المللی عضو شدند. بر اساس گزارشات ارائه شده توسط نهادهای بین‌المللی از سال ۲۰۲۳-۲۰۲۰حملات سایبری رشد۲۰ درصدی در بخش حملات ناشناخته و هوشمند داشته‌اند. در سال۲۰۲۳ کشورهای عضو برای محافظت از داده‌های مهم و اطلاعات راهبردی در حوزه‌های مختلف فناور محور درخواست تشکیل سازمان مستقلی تحت‌نظر مراجع بین‌المللی ارائه نمودند. وظیفه این سازمان کمک به سازمان‌های مختلف جهت ارتقا سیستم امنیت و پدافند سایبری بوده و همچنین این سازمان می‌تواند در خصوص کاهش تهدیدات و آسیب‌پذیری‌ها به ذی‌نفعان و سایر سازمان‌ها خدمات امنیتی و سایبری ارائه نماید (نمودار۲) [2,4].

[1] Great goals of the organization
[2] Organizational knowledge
[3] Knowledge-based organizations
[4] Ransomware
[5] New malware
[6] Information infrastructure



نمودار ۲.مقایسه حملات و امنیت سایبری در فضای سایبر تا سال ۲۰۲۳

در فضای سایبری نیز طرح محافظت از سازمان‌های فناور محور در برابر جرایم سایبری از سوی دولت‌های مختلف را کلید خورد که یکی از خروجی‌های آن راه‌اندازی آزمایشگاه جرم‌شناسی سایبری که هدف آن ارائه آموزش و افزایش آگاهی تخصصی پیرامون موضوعات امنیت سایبری و جرایم سایبری است. بر اساس مطالعات انجام شده توسط مرکز آسیب‌شناسی جرائم سایبری هند تا پایان سال ۲۰۲۳، بیش از هزار حمله فقط در یک ماه توسط مهاجمین و هکرها در سیستم‌های و شبکه‌ای سیستم‌های اطلاعاتی اتفاق افتاده است. حملات‌سایبری به سازمان‌های فناور محور و دانش بنیان خسارت‌های جبران‌ناپذیری مادی و معنوی به بخش‌های مختلف سازمانی، ملی و حتی در حوزه‌های بین‌المللی به سازمان‌های مربوطه در این کشور وارد نموده است [۲,۵].

۱-۲. نوآوری تحقیق :

انجام این پژوهش از جنبه‌های مختلف دارای نوآوری است. در ذیل به‌اختصار به برخی از این موارد اشاره می‌گردد:

۱) بررسی راهبرد سطح‌بندی انواع تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۲) بررسی راهبرد سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۳) بررسی راهبرد سطح‌بندی انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۴) بررسی راهبرد سطح‌بندی انواع تهدیدات شناخته شده (موجود) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۵) بررسی راهبرد سطح‌بندی انواع تهدیدات ناشناخته و هوشمند در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۶) سطح‌بندی و اولویت درون‌گروهی میان متغیرهای امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۷) سطح‌بندی و اولویت برون‌گروهی میان متغیرهای امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

۱-۳. هدف اصلی تحقیق :

❖ تبیین راهبرد سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور

- اهداف فرعی:

۱) تبیین سطح‌بندی انواع تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۲) تبیین سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۳) تبیین سطح‌بندی انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۴) تبیین سطح‌بندی انواع تهدیدات شناخته شده (موجود) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۵) تبیین سطح‌بندی انواع تهدیدات ناشناخته و هوشمند در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۶) تبیین سطح‌بندی و اولویت درون‌گروهی میان متغیرهای امنیت و پدافند سایبری سازمان‌های دانش‌بنیان
۷) تبیین سطح‌بندی و اولویت برون‌گروهی میان متغیرهای امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

۱-۴. فرضیات تحقیق

الف- فرضیه اول اصلی تحقیق:

- سطح‌بندی انواع تهدیدات بر اساس راهبرد امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور است.

- فرضیه‌های فرعی:

۱) تبیین راهبرد سطح‌بندی انواع تهدیدات سخت در افزایش امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور تأثیر مثبت و معناداری دارد.
۲) تبیین راهبرد سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد.
۳) تبیین راهبرد سطح‌بندی انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور تأثیر مثبت و معناداری دارد.
۴) تبیین راهبرد سطح‌بندی انواع تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد.
۵) تبیین راهبرد سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد.

ب- فرضیه دوم اصلی تحقیق

H_0 *سطح‌بندی و اولویت میان متغیرهای موردبررسی تحقیق یکسان است:*

H_1 *سطح‌بندی و اولویت میان متغیرهای موردبررسی تحقیق یکسان نیست:*

به‌عبارت‌دیگر می‌توان این‌گونه بیان نمود:

فرض صفر: میان متغیرهای موردبررسی تحقیق تبیین سطح‌بندی انواع تهدیدات اختلاف معناداری وجود دارد

فرض مقابل: میان متغیرهای موردبررسی تحقیق تبیین سطح‌بندی انواع تهدیدات اختلاف معناداری وجود دارد.

۲- مبانی نظری تحقیق

توسعه زیرساخت‌های اطلاعاتی و ارتباطی در کشورهای درحال‌توسعه، به دنبال آن افزایش سطح دسترسی مردم به اینترنت و خدمات اینترنتی سبب شده تا در دو دهه گذشته، کشورهای درحال‌توسعه با افزایش چشمگیر جرایم سایبری[1] مواجه شود. در همین راستا، این کشورها با تصویب لوایح قانونی برای برخورد با این‌گونه جرایم اقدام نموده‌اند. همچنین دولت‌های تابعه با تأسیس مراکز و نهادهای اجرایی متعدد برای پیشگیری، اطلاع‌رسانی و افزایش آگاهی، مقابله و مدیریت جرایم سایبری، تلاش کرده‌اند تا روند صعودی این جرایم را کنترل کنند. طبق آمار سال ۲۰۱۶ اتحادیه بین‌المللی مخابرات "آی‌تی یو[2]، متعلق به سازمان ملل، اکثر کشورهای درحال‌توسعه از لحاظ توسعه زیرساخت‌های اطلاعاتی و ارتباطی رشد سریعی داشتند. اکثر این کشورها با داشتن زیرساخت‌های اطلاعاتی و ارتباطی بسیار قوی در برابر حملات متعدد سایبری آسیب‌های اندکی دیدند، ولیکن از سال ۲۰۱۷، با پیشرفت انواع باج‌افزارها، بدافزارها و استفاده از فناوری نوین همانند هوش مصنوعی[3] آسیب‌های زیادی را متحمل شده‌اند [۶].

با تغییر نوع حملات، شیوه حمله، ساختار انواع حملات، نوع تهدیدات نیز تغییر نمود، لذا هم‌راستا با این تغییرات شیوه، روش و ابزار مقابله با انواع حملات و تهدیدات نیز می‌بایست تغییر نماید. دراین‌خصوص لازم است تا انواع تهدیدات در امنیت و پدافند سایبری مشخص شده، سطح‌بندی انواع تهدیدات در بخش امنیت صورت‌گرفته و روش مدونی از انواع تهدیدات در حوزه امنیت و پدافند سایبری سازمان‌ها ارائه گردد. افزایش جمعیت، عدم وجود متخصصین کارآمد و نیز عدم فناوری‌های پیشرفته و... در این کشورها، به‌عنوان دلایلی است که توسعه زیرساخت‌های اطلاعاتی و ارتباطی را در حوزه‌های سایبری دچار مشکل نموده است. مطابق آمار اعلام شده در سال ۲۰۲۳، حدود ۱۵ درصد از خانوارها در این کشورها دارای رایانه شخصی و حدود ۲۲ درصد نیز دسترسی راحت به اینترنت دارند. اما آمارها، افزایش ده برابری نفوذ اینترنت و دسترسی راحت به اینترنت، در کشورهای توسعه‌یافته را در سال‌های اخیر نشان می‌دهند ۲,۷ . توسعه زیرساخت‌های اطلاعاتی و ارتباطی و به‌تبع آن افزایش سطح دسترسی به اینترنت در تمامی بخش‌های این کشورها، جرایم سایبری را نیز گسترش خواهد داد. طبق گزارش مؤسسه تحقیقاتی پرایس واتر هاوس کوپرز[4] *PWC*، جرایم سایبری که در سال ۲۰۱۰ سومین جرم رایج در کشورهای درحال‌توسعه بودند، در سال ۲۰۱۶ به رتبه دوم صعود کرده، در سال ۲۰۲۳ به رتبه اول صعود نموده است [۸].

این شرکت همچنین به این نکته اشاره می‌کند که نحوه دسترسی سایت‌های آمریکایی به مشتریان در حال تغییر است. بیشتر آنها در حال راه‌اندازی سامانه‌ها و سرویس‌های امنیتی[5] فوق‌العاده پیشرفته هستند و تعداد کمتری از سیستم‌ها، سرویس‌ها، استانداردهای امنیتی[6] قدیمی استفاده می‌کنند. در گزارش مدیر امنیت سایبری این شرکت بیان شده است؛ در سال ۲۰۲۳ "باتوجه‌به افزایش تقاضا برای سکوهای[7] ساخت این شرکت، تأمین امنیت سکوهای موجود و نیز ارتقا سرویس‌های امنیتی در حوزه سایبری در این شرکت بر اساس استانداردهای جدید، بهره‌گیری از سرویس‌های نوین امنیتی و قابلیت‌های گسترده هوش مصنوعی است" [۹].

آمارهای دیگر در این حوزه سبب شده تا مسئولین کشورهای درحال‌توسعه بیش‌ازپیش نسبت به برخورد با جرایم سایبری و به‌خصوص جرایم سایبری ساختاریافته و... وارد عمل شوند. در ایران نیز مسئولین فضای سایبری و امنیتی اقدامات مؤثری را تدوین نموده‌اند ولیکن، تاکنون در خصوص تبیین راهبردی سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌ها اقدام مؤثر انجام نداده‌اند؛ لذا در این تحقیق در خصوص راهبردی در راستای سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور تبیین می‌گردد. تغییر در نوع حملات، شیوه حملات و ساختار انواع حملات در سازمان‌های دانش‌بنیان، سبب تغییر در سرویس‌های امنیتی و ساختار امنیت در فناوری اطلاعات سازمانی در کشور شده است. همچنین استفاده و هدف‌گذاری کاربرد هوش مصنوعی، هوشمندسازی، اتوماسیون هوشمند و سایر پیشرفت‌ها در زمینه تأمین امنیت فناوری اطلاعات و نیز امنیت سایبری به طور خاص زمینه را برای تکامل بیشتر این فناوری فراهم می‌کند. سیستم‌ها، سازمان‌ها، شبکه‌های اطلاعاتی[8] و... در سازمان‌های دانش‌بنیان در حال هوشمندتر شدن (هوشمندسازی سازمانی[9]) هستند، لذا براین‌اساس در تبیین راهبردی سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌ها می‌بایست به انواع حملات و تهدیدات هوشمند در فضای سایبری توجه ویژه داشت ۲,۱۰ . مدیر ارشد امنیت سایبری شرکت آمازون اعلام نمود، در دوران پساکرونا این شرکت با بیشترین تهدیدات روبرو بوده و تغییرات گسترده‌ای در نوع حملات و تهدیدات سایبری روی داده است؛ لذا پیشرفت ساختارها، نرم‌افزارها، انواع استانداردهای بین‌المللی امنیتی و... در فضای سایبری هم‌راستا با این موضوع هستند. بسیاری از متخصصان فناوری اطلاعات پذیرفته‌اند، بدون شناخت انواع تهدیدات و آسیب‌ها، برقراری امنیت ممکن نیست. سؤالات بسیاری در ترکیب امنیت در فضای سایبری و هوش مصنوعی 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؟! [۱۰].

۲-۱. تبیین موضوعی تحقیق:

[1] Cvber crimes
[2] International Telecommunication Union (ITU)
[3] Artificial intelligence
[4] PricewaterhouseCoopers
[5] Security services
[6] Security standards
[7] platforms
[8] Information networks
[9] Organization intelligence

رشد روزافزون برنامه‌های سایبری باهدف حذف اطلاعات الکترونیکی یا تغییر آنها، به‌دست‌آوردن اطلاعات الکترونیکی [1] باارزش، سوءاستفاده از سیستم‌ها و سرویس‌ها، کاهش کارآمدی و دسترس‌پذیری، باعث افزایش هزینه‌های حفظ امنیت رایانه‌ها و فضای سایبری شرکت‌ها و سازمان‌های دانش‌بنیان شده است. حفظ گمنامی برای انواع حملات و آسیب‌ها همانند بدافزارها به‌منظور شناسایی‌نشدن توسط انواع برنامه‌های تشخیص انواع حملات و آسیب‌ها از جمله ویژگی‌های بسیار مهم حملات و آسیب‌های پیشرفته است [۱۱]. بدین منظور توسعه‌دهندگان بدافزار برای پایداری محصولاتشان در محیط هدف، ناگزیر به استفاده از روش‌های نوین دورزدن در سیستم‌های امنیتی و پدافند سایبری هستند؛ لذا رقابتی دائمی و همیشگی میان توسعه‌دهندگان انواع بدافزار[2] و شرکت‌ها و سازمان‌های امنیتی مرتبط با ابزارهای شناسایی حملات و آسیب‌ها، وجود دارد [۱۲]. انواع ویروس و بدافزارهای با ایجاد تغییر در فناوری، با مقیم شدن در حافظه به‌جای قرارگرفتن در هارددیسک و اجرا در آن، امکان شناسایی توسط سامانه‌های امنیتی و پدافند سایبری را با مشکل جدی مواجه نموده است [۱۳]؛ لذا برای شناسایی انواع ویروس، کرم‌ها، تروجان‌ها، بدافزارها، باج‌افزارها، انواع حملات، آسیب‌ها شرکت‌ها و سازمان‌های دانش‌بنیان نیازمند، تبیین سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور است [۱۴]. همچنین 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 سیستم‌های سازمانی است [۱۵]. اقدامات پیشگیرانه امنیتی در فضای سایبری در حوزه‌های دانش‌بنیان در شرکت‌ها و سازمان‌های از الزامات این پژوهش است. همچنین ضرورت توجه به فناوری‌های نوین اطلاعاتی[3]، توسعه امنیت در فضای سایبری از مهم‌ترین نیازهای شرکت‌ها و سازمان‌های دانش‌بنیان به شمار می‌روند. [۱۶].

۲-۲. پیشینه تحقیق

ساختار سیستم‌های اطلاعاتی، فناوری اطلاعات، امنیت اطلاعات، مبتنی بر نفوذ، هک، تهدیدات، سایر آسیب‌ها و تهدیدات در فضای سایبری است. جنگ سایبری و پدافند سایبری بخشی از مؤلفه‌ها و مباحث مرتبط با تکنولوژی‌های نوین ارتباطی و اطلاعاتی است [۱۷]. در حوزه امنیت اطلاعات در سیستم‌های اطلاعاتی، نفوذ در شبکه‌های ارتباطی، هک در فناوری اطلاعات[4]، تهدیدات سایبری و سایر آسیب‌های امنیتی در حوزه اینترنت، فضای سایبری، فضای مجازی پژوهش‌های مختلف و متعددی در سال‌های اخیر صورت‌گرفته است [۱۷،۱۸]. ولیکن در خصوص سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان پژوهش خاصی صورت نگرفته و مطالب مرتبط بسیار اندک است [۱۹]. در ذیل خلاصه‌ای از برخی از تحقیقات انجام شده و مشابه بیان می‌گردد:

طی تحقیق دیگری که توسط لطفی و همکارانش در سال ۱۳۹۴ با موضوع شناخت تهدیدات و آسیب‌های اجتماعی[5] تهران و چشم‌انداز آتی با در کلان سازمان تهران انجام پذیرفت. در این تحقیق تهدیدات، آسیب‌های اجتماعی کلان سازمان تهران و چشم‌انداز آتی سازمان[6] با تأکید بر انواع تهدیدات مورد شناسایی و ارزیابی قرار گرفت. همچنین این تحقیق از نوع کاربردی و میدانی بوده، از روش‌های پیمایشی در انجام تحقیق استفاده گردید. در این تحقیق قابلیت تبیین انواع تهدیدات در حوزه‌های مختلف اجتماعی، فضای مجازی و شبکه‌های اجتماعی مشخص شد [۲۰،۲۱].

طی تحقیق دیگری که توسط البرزی و همکارانش در سال ۱۳۹۸ با موضوع بررسی تهدیدات امنیتی در محاسبات ابری و ارائه روش امن جهت نگهداری داده‌ها انجام پذیرفت. در این تهدیدات امنیتی در محاسبات ابری مورد مطالعه قرار گرفت. همچنین بر اساس ساختار تحقیق و نوع تهدیدات در فضای سایبری روشی امن جهت نگهداری داده‌ها ارائه گردید [۲۲].

طی تحقیق دیگری که توسط اسماعیلی و همکارانش در سال ۱۳۹۷ با موضوع طراحی مدل مفهومی الگوی پدافند سایبری جمهوری اسلامی ایران انجام پذیرفت. در این مدل مفهومی برای الگوی پدافند سایبری جمهوری اسلامی ایران ارایه گردید. براساس داده‌های تحقیق، نتایج حاصل از تجزیه‌وتحلیل داده‌ها نشان در طراحی مدل مفهومی میان مولفه‌های مورد بررسی نوعی همخوانی ساختاری با امنیت، یکپارچگی[7]، صحت[8] و دسترس‌پذیری[9] در الگوی پدافند سایبری وجود دارد. همچنین می‌بایست به مولفه‌های دیگر مانند کنترل، ارزیابی، امکانسنجی و کنترل دسترسی و ... در طراحی مدل مفهومی الگوی پدافند سایبری توجه نمود [۲۳].

طی تحقیقی که توسط موسوی و همکارانش در سال ۱۳۹۹ با موضوع راهبردهای ارتقاء توانمندی‌های جنگ الکترونیک و سایبری (سایبرالکترونیک[10]) نیروهای مسلح در برابر تهدیدات ناهمتراز انجام پذیرفت. اطلاعات برای تمامی سازمان‌ها به عنوان شریان اصلی یک سازمان می‌باشد و با توجه به عصر حاضر که عصر اطلاعات و الکترونیک نامگذاری شده است باید اهمیت ویژه‌ای جهت حفظ و نگهداری اطلاعات با توجه به شرایط رقابتی قائل شد. در این تحقیق راهبردهای ارتقاء توانمندی‌های جنگ الکترونیک و سایبری

[1] Electronic information
[2] malware
[3] New information technologies
[4] Hacking in information technology
[5] Social harm
[6] The future vision of the organization
[7] Integrity
[8] Correctness
[9] Accessibility
[10] Cyberelectronics

(سایبرالکترونیک) نیروهای مسلح در برابر تهدیدات ناهمتراز مورد بررسی قرار گرفت [۲۴].

طی تحقیقی که توسط میرزایی و همکارانش در سال ۱۴۰۱ با موضوع ارزیابی مدل شاخص‌های مختلف امنیت‌اطلاعات در سازمان‌ها انجام پذیرفت. ارزیابی مدل‌های شاخص‌های مختلف امنیت اطلاعات مبتنی بر الگوریتم ژنتیک بوده، ویژگی‌های عمده مدل‌های مختلف امنیت اطلاعات تبیین شده است. این ویژگی‌ها،شامل تضمین امکان انتخاب، اولویت‌بندی شاخص‌های مختلف امنیت اطلاعات، امنیت سایبری، بهینه شاخص‌های سنجش کیفیت خدمات، امنیت سیستم‌های اطلاعاتی، فراهم ساختن امکان مشارکت خبرگان و متخصصین در فرایند تعیین شاخص‌های مختلف امنیت اطلاعات و کمک به مدیران جهت اتخاذ تصمیم بهینه یا نزدیک به بهینه درباره سرمایه گذاری برای توسعه امنیت اطلاعات است که با کمک فرایند تحلیل سلسله مراتبی و الگوریتم ژنتیک تحقق یافته اند [۲۵].

طی تحقیقی که توسط علیزاده سودمند و همکارانش در سال ۱۴۰۳ با موضوع تحلیل ساختارمند شاخص ایمنی[1] در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان انجام پذیرفت. پس از مشخص نمودن شاخص‌های فرعی و مؤلفه‌های اصلی اثرگذار با استفاده از روش‌های علمی (روش دلفی)، میزان اهمیت آنها توسط خبرگان مشخص گردید. مؤلفه‌های اثرگذار ترکیبی از مؤلفه‌های امنیت و پدافند سایبری هستند. وجود انواع تهدیدات و شرایط کشور موجب شد، تا سه سازمان دانش‌بنیان" دانشگاه آزاد اسلامی واحد تهران‌جنوب، واحد علوم تحقیقات و دانشگاه تهران موردمطالعه قرار گرفتند. میزان اهمیت مؤلفه‌های اثرگذار با نظرات خبرگان تعیین گردیده، میانگین هندسی به دست آمد و پس از وزن‌دهی مؤلفه‌ها تمامی مقادیر نرمال‌سازی شدند و با استفاده از الگوریتم تکاملی پرومیتی به‌عنوان یکی از روش‌های نوین تصمیم‌گیری، مقایسه درون‌گروهی مؤلفه‌های صورت پذیرفته و سپس اولویت بر اساس جنس مؤلفه‌های میان گروهی امنیت و پدافند سایبری انجام پذیرفت. سازمان‌ها بر اساس اولویت و میزان امتیاز رتبه‌بندی شدند [۲۶].

همچنین میکی کراوزه[2] در کتاب معروف خود با عنوان مدیریت حفاظت و امنیت اطلاعات، به بررسی ساختارهای امنیتی و مدیریت حفاظت و امنیت اطلاعات در برابر انواع حملات سایبری پرداخت. در این کتاب به طور واضح مشخص گردید، قابلیت‌های امنیتی توسط سرویس‌های مختلف امنیتی، نیز نرم‌افزارها و استانداردهای امنیتی می‌تواند اثرات بسیاری از حملات و تهدیدات را کاهش دهد. ولیکن این موارد به‌تنهایی کافی نمی‌باشد، بلکه نیازمند کارکنان خبره که آموزش‌های لازم را در حوزه‌های مختلف امنیتی دیده‌اند در بهبود عملکردهای امنیتی در سازمان‌ها بسیار مؤثر است [۲۷].

طی تحقیقی هم‌راستا که توسط سونگ [3]و همکارانش در سال ۲۰۱۵ با موضوع پویایی دیدگاه تحمل چندسطحی در شبکه‌های فرماندهی و کنترل نظامی انجام پذیرفت. در این تحقیق پویایی دیدگاه تحمل چندسطحی در شبکه‌های فرماندهی و کنترل نظامی مبتنی بر حملات سایبری مورد بررسی قرار گرفت. مطالعات کمی به پویایی نظرات در سازمان‌های فرماندهی و کنترل نظامی (*C2*) در برابر انواع انواع تهدیدات پرداخته‌اند که، اغلب به صورت سلسله مراتبی در یک ساختار درختی رتبه‌بندی می‌شوند. علاوه بر این، ماموران نظامی براساس اصول سایبری و انواع تهدیدات باید در هنگام برقراری ارتباط با عوامل دارای رتبه‌بندی متفاوت، سطوح تحمل متفاوتی داشته باشند، که دلیل برای پیشنهاد یک مدل پویایی نظر با تحمل چند سطحی در این مطالعه بود [۲۸].

طی تحقیقی هم‌راستا که توسط النا ولاهو[4]و همکارانش در سال ۲۰۲۰ با موضوع ارائه بررسی چالش‌های امنیت اطلاعات در فضای سایبری انجام پذیرفت. در این تحقیق چالش‌های امنیت اطلاعات در فضای سایبری مورد ارزیابی قرار گرفت. راهکارهای عوامل حیاتی موفقیت در حوزه امنیت اطلاعات ارائه گردید. همچنین به جنبه‌های مختلف استراتژی، کنترل و تنظیم در حوزه امنیت اطلاعات در فضای سایبری پرداخته شد، در ادامه رویه‌ها و دستورالعمل‌های مختلف را حوزه امنیت اطلاعات در فضای سایبری را مطابقت داده شد. در این تحقیق مشخص شد؛ امنیت اطلاعات یک جنبه حیاتی است و نقش مهمی در حفاظت از کسب‌وکار سازمان ایفا می‌کند. سازمان‌ها موظف‌اند از اطلاعات و دارایی‌های خود برای حفظ ارزش و سازمان خود محافظت کنند [۲۹]

طی تحقیقی دیگری که توسط ماری کارجلاینن[5] و همکارانش در سال ۲۰۲۰ با موضوع بررسی نرم‌افزار مختلف امنیتی و الزامات آموزشی برای امنیت اطلاعات در فضای سایبری انجام پذیرفت. مطابق تجزیه‌وتحلیل صورت‌گرفته در حوزه‌های نرم‌افزاری در بخش امنیت، استفاده از نرم‌افزارهای مختلف امنیتی می‌تواند در ارتقا امنیت و جلوگیری از انواع تهدیدات هوشمند نموده و حملات روز صفر را کاهش دهد. از سویی دیگر آموزشی برای امنیت اطلاعات به‌عنوان یکی از الزامات امنیتی و پدافند سایبری در فضای سایبری به شمار می‌آید [۳۰].

طی تحقیقی دیگری که توسط دامیان فوجس[6] و همکارانش در سال ۲۰۲۳ با موضوع استفاده از نرم‌افزار مختلف امنیتی و الزامات آموزشی برای امنیت اطلاعات در فضای سایبری انجام پذیرفت. دستیابی به سطح مناسبی از امنیت سیستم‌های اطلاعاتی مستلزم درنظرگرفتن هم‌زمان جنبه‌های فنی سیستم‌های اطلاعاتی و جنبه‌های انسانی مربوط به کاربران نهایی سیستم‌های اطلاعاتی است. این جنبه‌ها را می‌توان در قالب الزامات امنیت اطلاعات

[1] Safety index
[2] Mickey Krause,
[3] Elena Vlahu
[4] Elena Vlahu
[5] Mari Karjalainen
[6] Damjan Fujs

توصیف کرد. رویکردی را که محقق پیشنهاد می‌کند، انتخاب، الزامات نرم‌افزارهای امنیت اطلاعات و الزامات آموزشی امنیت اطلاعات باتوجه‌به عملکرد امنیت اطلاعات کاربران نهایی کمک می‌کند. این رویکرد در آزمایشی شامل ۱۲۸ متخصص سیستم‌های اطلاعاتی آزمایش شد. نتایج نشان داد که استفاده از رویکرد پیشنهادی به متخصصان سیستم‌های اطلاعاتی باتجربه محدود در امنیت اطلاعات کمک می‌کند تا تصمیمات بهتری در مورد نرم‌افزارهای امنیت اطلاعات و الزامات آموزشی امنیت اطلاعات بگیرند [۳۱].

جدول (۱): خلاصه پیشینه تحقیق

نظریه‌پرداز (محقق)	عنوان پیشینه	خلاصه
لطفی و همکاران (۱۳۹۴)	شناخت تهدیدات و آسیب‌های اجتماعی تهران و چشم‌انداز آتی با در کلان سازمان تهران	در این تحقیق تهدیدات، آسیب‌های اجتماعی کلان سازمان تهران و چشم‌انداز آتی با تأکید بر انواع تهدیدات مورد شناسایی و ارزیابی قرار گرفت. در این تحقیق قابلیت تبیین انواع تهدیدات در حوزه‌های مختلف اجتماعی، فضای مجازی و شبکه‌های اجتماعی مشخص شد.
اسماعیلی و همکاران (۱۳۹۷)	طراحی مدل مفهومی الگوی پدافند سایبری جمهوری اسلامی ایران	نتایج حاصل از تجزیه‌وتحلیل داده‌های این تحقیق نشان داد، در طراحی مدل مفهومی میان مؤلفه‌های موردبررسی نوعی همخوانی ساختاری با امنیت، یکپارچگی، صحت و دسترس‌پذیری در الگوی پدافند سایبری وجود دارد. همچنین می‌بایست به مؤلفه‌های دیگر مانند کنترل، ارزیابی، امکان‌سنجی و کنترل دسترسی و.. در طراحی مدل مفهومی الگوی پدافند سایبری توجه نمود.
البرزی و همکاران (۱۳۹۸)	بررسی تهدیدات امنیتی در محاسبات ابری و ارائه روش امن جهت نگهداری داده‌ها	نتایج این پژوهش نشان داد، بر اساس ساختار تحقیق و نوع تهدیدات در فضای سایبری روشی امن جهت نگهداری داده‌ها ارائه گردید.
موسوی و همکاران (۱۳۹۹)	راهبردهای‌ارتقاء‌توانمندی‌های جنگ الکترونیک و سایبری (سایبر الکترونیک) نیروهای مسلح در برابر تهدیدات ناهم‌تراز	نتایج حاصل از تحقیق نشان داد، باید اهمیت ویژه‌ای جهت حفظ و نگهداری اطلاعات باتوجه‌به شرایط رقابتی قائل شد. در این تحقیق راهبردهای ارتقاء توانمندی‌های جنگ الکترونیک و سایبری (سایبر الکترونیک) نیروهای مسلح در برابر تهدیدات ناهم‌تراز موردبررسی قرار گرفت.
میرزایی و همکاران (۱۴۰۱)	ارزیابی مدل شاخص‌های مختلف امنیت اطلاعات در سازمان‌ها	الگوریتم نتایج حاصل از تحقیق نشان داد، ارزیابی مدل‌های شاخص‌های مختلف امنیت اطلاعات مبتنی بر بوده و ویژگی‌های عمده مدل‌های مختلف امنیت اطلاعات تبیین شده است. این ویژگی‌ها، شامل تضمین ژنتیک امکان انتخاب و اولویت‌بندی شاخص‌های مختلف امنیت اطلاعات، امنیت سایبری و. کمک به مدیران جهت اتخاذ است. تصمیم بهینه یا نزدیک به بهینه درباره سرمایه‌گذاری برای توسعه امنیت اطلاعات
علیزاده سودمند و همکاران (۱۴۰۳)	تحلیل ساختارمند شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	در این تحقیق به تحلیل ساختارمند شاخص ایمنی در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان پرداخته شد. پس از مشخص نمودن شاخص‌های فرعی و مؤلفه‌های اصلی اثرگذار با استفاده از روش‌های علمی (روش دلفی)، میزان اهمیت آنها توسط خبرگان مشخص گردید. با استفاده از الگوریتم تکاملی پرومیتی مقایسه گروهی مؤلفه‌های صورت پذیرفته، سازمان‌ها بر اساس اولویت و میزان امتیاز رتبه‌بندی شدند.
میکی کراوزه و همکاران (۲۰۰۹)	مدیریت حفاظت و امنیت اطلاعات	در این تحقیق، ساختارهای امنیتی و مدیریت حفاظت و امنیت اطلاعات در برابر انواع حملات سایبری موردبررسی قرار گرفت. مشخص گردید، قابلیت‌های امنیتی توسط سرویس‌های امنیتی، و استانداردهای امنیتی و... می‌توان اثرات بسیاری از حملات و تهدیدات را کاهش دهد. ولیکن به‌تنهایی کافی نمی‌باشد، بلکه نیازمند کارکنان خبره که آموزش‌های لازم را در حوزه‌های امنیتی دیده‌اند.
سونگ و همکاران (۲۰۱۵)	پویایی دیدگاه تحمل چندسطحی در شبکه‌های فرماندهی و کنترل نظامی	در این تحقیق پویایی دیدگاه تحمل چندسطحی در شبکه‌های فرماندهی و کنترل نظامی مبتنی بر حملات سایبری مورد بررسی قرار گرفت. مطالعات کمی به پویایی نظرات در سازمان‌های فرماندهی و کنترل نظامی در برابر انواع تهدیدات پرداخته، به‌صورت سلسله‌مراتبی در یک ساختار درختی رتبه‌بندی شدند.
الناولاهو و همکاران (۲۰۲۰)	بررسی چالش‌های امنیت اطلاعات در فضای سایبری	در این تحقیق راهکارهای عوامل حیاتی موفقیت در حوزه امنیت اطلاعات ارائه گردید. همچنین به جنبه‌های مختلف استراتژی، کنترل و تنظیم در حوزه امنیت اطلاعات در فضای سایبری پرداخته شد. ضمناً رویه‌ها و دستورالعمل‌های مختلف را حوزه امنیت اطلاعات در فضای سایبری را مطابقت داده شد.
ماری کارجلاینن و همکاران (۲۰۲۰)	بررسی نرم‌افزار مختلف امنیتی و الزامات آموزشی برای امنیت اطلاعات در فضای سایبری	مطابق تجزیه‌وتحلیل صورت‌گرفته، در حوزه‌های نرم‌افزاری در بخش امنیت، استفاده از نرم‌افزارهای مختلف امنیتی می‌توان در ارتقا امنیت، جلوگیری از انواع تهدیدات هوشمند مؤثر بوده و حملات روز صفر را کاهش دهد. از سویی دیگر آموزشی برای امنیت اطلاعات به‌عنوان یکی از الزامات امنیتی و پدافند سایبری در فضای سایبری به شمار می‌آید.
دامیان فوجس و همکاران (۲۰۲۳)	استفاده از نرم‌افزار مختلف امنیتی و الزامات آموزشی برای امنیت اطلاعات در فضای سایبری	نتایج این پژوهش نشان داد، دستیابی به سطح مناسبی از امنیت سیستم‌های اطلاعاتی مستلزم درنظرگرفتن هم‌زمان جنبه‌های فنی سیستم‌های اطلاعاتی و جنبه‌های انسانی مربوط به کاربران نهایی سیستم‌های اطلاعاتی است. این جنبه‌ها را می‌توان در قالب الزامات امنیت اطلاعات توصیف کرد.

۲-۳.سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان کشور

متغیرها و مؤلفه‌های سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان به‌قرار ذیل است. سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

کشور در (شکل ۱) قابل‌مشاهده است: ۱۷,۲۰,۲۳,۲۵ .

۱.تهدیدات سخت (کاملاً پیش‌بینی نشده و ناشناخته، غیرساختاری)

۲.تهدیدات نیمه‌سخت (اقدامات اطلاعاتی، امنیتی و سایبری که به‌صورت پیش‌بینی نشده و نیمه‌ساختارمند)

۳.تهدیدات نرم (اقدامات فرهنگی، سیاسی، اقتصادی و ساختارمند)

۴.تهدیدات موجود شناخته‌شده (اقدامات ساختارمند، روان‌شناختی، رسانه‌ای، اجتماعی، شبکه‌ای و...)

۵.سایر تهدیدات ناشناخته و هوشمند (پیشگیری‌های فازی، مقابله و دفاع هوشمند[1]، بهره‌گیری از سیستم‌های امنیتی خبره، انواع حملات روز صفر).

شکل ۱. سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان

۲-۴.شناخت ساختار نوین انواع تهدیدات در امنیت و پدافند سایبری:

با شناخت ساختار نوین انواع تهدیدات در امنیت و پدافند سایبری قرار است استفاده از طریق طیف وسیعی از سامانه‌های دیجیتال[2]، سکوهای الکترونیکی[3] و پلتفرم‌های هوشمند[4] به نفع جامعه در فضای سایبری باشد. برآوردها در این حوزه متفاوت بوده و به‌سرعت درحال‌رشد است. انواع حملات و تهدیدات جدید در فضای سایبری در حد ده‌ها میلیارد است و در حال گسترش بسیار زیادی است. غالباً تمرکز این بررسی بر ساختار نوین انواع تهدیدات به‌صورت نوین حملات و تهدیدات ساختاریافته[5] است. سیستم‌های کنترل امنیتی هوشمند مجهز به:

- اینترنت اشیا[6]
- داده‌کاوی امنیتی[7]
- سیستم‌های نوین امنیتی[8]
- سیستم‌های خبره امنیتی[9]
- سیستم‌های هوشمند امنیتی[10] و... است.

این سرویس‌ها و سیستم‌ها در حال تبدیل‌شدن به بخش قابل‌توجهی از زیرساخت‌های حیاتی فعلی و آینده سازمان‌ها هستند، آنها باهدف جذب بالا در زمینه‌هایی مانند انرژی، حمل‌ونقل، ساخت، محیط‌های امن، ارتباطات و کلیه بخش‌های حیاتی فعالیت نموده، ساختارها و امکانات در بخش تولیدات و ارائه خدمات را فراهم می‌کنند. لازم به ذکر است پیامدهای شکست در این پروژه‌های امنیتی و سایبری می‌توان در این محیط‌ها زیاد باشد؛ بنابراین، درک نحوه ارائه سرویس‌ها و سیستم‌های امنیتی و سایبری لازم و ضروری است [۱۷,۳۲].

زیرساخت‌های قوی در سرویس‌ها و سیستم‌های امنیتی، چالش‌های امنیتی را کاهش می‌دهد و همچنین ممکن است چالش‌های جدیدی را برای خود ایجاد می‌کند؛ لذا شناخت ساختار نوین انواع تهدیدات و اولویت‌بندی اقدامات، شناسایی ریسک‌های نوظهور، مؤلفه‌های کلیدی و شکاف‌های موجود، شناخت توانایی‌های سرویس‌ها و سیستم‌ها از اقدامات ضروری به شمار می‌آید [۳۳].

۲-۵. مولفه‌های اثرگذار بر سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان :

متغیرها یا مؤلفه‌های اثرگذار بر سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان به شرح ذیل است: [۲۴,۲۶,۲۸].

الف) مؤلفه تهدیدات سخت[11] در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان:

لازمه توسعه پایدار در تمامی جهت‌ها، توسعه، حفظ منابع و زیرساخت‌ها در برابر حوادث، حملات خارجی و تهدیدات سخت است. پروژه‌های مختلف سایبری معمولاً به‌صورت ریزشبکه‌ها و شبکه‌های متداخل در نظر گرفته می‌شوند، این موضوع سبب شده تا از زیرساخت شبکه‌ای و شبکه‌های اطلاعاتی مختلف در حفظ پایداری اطلاعاتی استفاده شود، امنیت زیرساخت در سازمان‌ها افزایش یابد [۳۴]. زیرمؤلفه‌های اثرگذار تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان شامل، تهدیدات کاملاً پیش‌بینی نشده، ناشناخته، غیرساختارمند است. برخی از این تهدیدات و آسیب‌ها در ذیل مشخص شده است: ۱۱ ,۲۰,۲۳ .

- میزان اهمیت مراکز و سازمان‌های دانش‌بنیان
- تشکیلات استراتژیک سازمان داده‌محور
- اولویت‌بندی طرح‌ها و برنامه‌ها
- پیاده‌سازی پروژه‌های امنیت اطلاعات[12]
- خرید سخت‌افزارهای امنیتی جدید
- تأمین استانداردهای بین‌المللی امنیتی
- اصل و گزینش مکان‌یابی سایبری

[1] Smart Defense
[2] Digital systems
[3] Electronic platforms
[4] Smart platforms
[5] Structured threats
[6] Internet of Things (IoT)
[7] Security data mining
[8] New security systems
[9] Expert security systems
[10] Intelligent security systems
[11] Threats hard
[12] Implementation of information security projects

- تأیید اصل امایش سرزمین
- طراحی اماکن و مراکز داده‌ای
- استقرار سایت‌ها پدافند سایبری

ب) مؤلفه تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان:

یکی از مهم‌ترین روش‌های امنیت و پدافند سایبری در حوزه‌های مختلف زیرساخت‌ها، حفاظت فیزیکی از تأسیسات حیاتی آن‌ها است. این حفاظت سبب می‌شود، تا احتمال موفقیت‌آمیز بودن حملات فیزیکی و خرابکارانه در برابر حملات و تهدیدات نیمه‌سخت کاهش یابد. در این‌گونه حملات ویژگی‌ها و قابلیت‌های مهاجمین (خرابکاران) در محاسبه احتمال موفقیت‌آمیز بودن حمله به تأسیسات حیاتی در نظر گرفته شده است [۳۴]. شاخص‌ها و زیرمولفه‌های اثرگذار تهدیدات نیمه‌سخت **در** امنیت و پدافند سایبری سازمان‌های دانش‌بنیان شامل تمامی اقدامات اطلاعاتی، امنیتی و سایبری که به صورت پیش‌بینی‌نشده و نیمه‌ساختارمند می‌باشد. برخی از این تهدیدات و آسیب‌ها در ذیل مشخص شده است: [۸،۲۴،۲۸].

- تعیین نقاط امن برای استقرار عملکردها
- انتخاب جایگزین بهینه در مکان‌گزینی مناسب[1]
- استقرار طرح‌ها در سایت‌های ایستا و پویا[2]
- میزان قابلیت استحکام سایت‌ها[3] در برابر حملات
- ایمن‌سازی بسترهای ارائه سرویس
- عملکردهای پروژه‌های سایبری پدافندی
- مقاوم‌سازی کدهای تحلیلی[4] در حملات
- ارتقا محصون‌سازی و قابلیت ایمن‌سازی شبکه‌ها

ج) مؤلفه تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان:

شاخص‌ها و زیرمؤلفه‌های اثرگذار نیمه تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان شامل اقدامات فرهنگی، سیاسی، اقتصادی و ساختارمند است. برخی از این تهدیدات و آسیب‌ها در ذیل مشخص شده است: [۸،۲۶،۲۸].

- محصولات و خدمات ارائه شده توسط پیمانکاران
- تجهیزات امنیتی[5] در سایت‌ها و سیستم‌ها
- روابط بین سیستم‌ها در برابر حملات و تهدیدات
- اطمینان از کفایت قدرت پردازشی[6] و حافظهٔ سیستم‌ها
- اصل پشتیبانی از منابع و سیستم‌های اطلاعاتی
- حفاظت از دارایی‌ها در برابر حملات شبکه‌ای
- اصل انطباق در تحلیل تهدیدات نرم
- هم‌راستایی سیستم امنیتی و محیط سایبری

[1] Appropriate location
[2] Static and dynamic sites
[3] The strength of the sites
[4] Analytical codes
[5] Security equipment
[6] Processing power

- تبیین اصل جهاد فرهنگی

د) مؤلفه سایر تهدیدات شناخته شده (موجود) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان:

شاخص‌ها و زیرمؤلفه‌های اثرگذار سایر تهدیدات شناخته شده (موجود) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان شامل تهدیدات موجود شناخته شده؛ اقدامات ساختارمند، روان‌شناختی، رسانه‌ای، اجتماعی، شبکه‌ای و... در سازمان است. برخی از این تهدیدات و آسیب‌ها در ذیل مشخص شده است [۱۱،۱۲،۲۳،۲۶].

- توسعه زیرساخت‌های سیستمی و تحلیل شبکه‌ای
- اقدامات ساختارمند (حفاظ‌های الکتریکی و..)
- کاربردهای محوری از سیستم‌های امنیتی در (ارتینگ و....)
- تهدیدات رسانه‌ای[7] در فضای سایبری
- افزایش قابلیت اطمینان در مراکز اطلاعاتی
- استفاده از مشاوران امنیت اطلاعات در فضای سایبری
- تبیین انواع حملات اجتماعی (مهندسی اجتماعی[8]) و...

ه) مؤلفه سایر تهدیدات ناشناخته و هوشمند[9] در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان:

یکی از مهم‌ترین تهدیدات در سال‌های اخیر در جهان تهدیدات ناشناخته و هوشمند است. اهداف اصلی، این مدل جدید از تهدیدات بسیار گسترده و ناشناخته است. ایجاد، توسعه و گسترش انواع تهدیدات ناشناخته و هوشمند در راستای آسیب‌های نامتقارن و ناهمگون در فضای سایبری و نیز کسب حداکثر سود برای مهاجمین است؛ لذا تشخیص این حملات و تهدیدات نیز بسیار پیچیده و مبهم است، این موضوع مهم، نیازمند سازوکارهای فراتشخیصی هوشمندی است که برای مدت طولانی ماندگاری داشته باشند. برای این منظور، نیاز به یک تغییر رویکرد با قابلیت مقابله هوشمند[10] و دفاع ساختارمند[11] در مواجهه با این گونه تهدیدات ناشناخته و هوشمند در سطح بین‌الملل است [۲۶]. شاخص‌ها و زیرمولفه‌های اثرگذار سایر تهدیدات ناشناخته و هوشمند در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان شامل، انواع تهدیدات ناشناخته و هوشمند همانند؛ پیشگیری‌های فازی، مقابله هوشمند، بهره‌گیری از سیستم‌های امنیتی خبره، انواع حملات روزصفر[12] می‌باشد. برخی از این تهدیدات و آسیب‌ها در ذیل مشخص شده است: [۱۲،۱۷،۲۶،۲۸].

- سرقت یا نابودی دارایی‌های معنوی[13]
- انواع آسیب‌های فراتشخیصی هوشمند[14]
- انواع بدافزارهای و باج‌افزارهای محیطی

[7] Media threats
[8] Social engineering
[9] Unknown and intelligent threats
[10] Smart Coping
[11] Structured Defense
[12] Zero Day Attacks
[13] Intellectual property
[14] Smart Hyperdiagnostic Injuries

- کدهای مخرب برنامه‌نویسی شده مخفی[1]
- انواع تکنیک‌های مخرب علم داده[2]
- الگوریتم‌های یادگیری ماشین[3]
- تشخیص پیش‌گام تهدیدات روز صفر
- الگوریتم‌های داده‌کاوی[4] مبهم و نامعین و..

۳- روش تحقیق

در این تحقیق باتوجه‌به نوع موضوع و متغیرهای موجود در سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور ساختار تحقیق به‌صورت عملیاتی موردبررسی و ارزیابی قرار گرفت.

۳-۱.نوع پژوهش حاضر(جامعهٔ آماری، روش نمونه‌گیری)

با توجه ماهیت موضوع و روش انجام آن اطلاعات مربوط به مباحث نظری و فعالیت‌های کتابخانه‌ای به همراه فعالیت‌های تحقیقاتی معتبر اینترنتی، مجلات و مقالات به همراه روش‌ها، متدولوژی اندازه‌گیری و ارزیابی مورداستفاده قرار خواهد گرفت. ضمناً از ابزار پرسش‌نامه، مصاحبه، غیره جهت تکمیل تحقیق، تجزیه‌وتحلیل با استفاده از روش میدانی میسر خواهد شد [۳۵]. این روش پژوهش از نوع مطالعات کمی بوده که می‌تواند، قابلیت آزمون‌پذیری، تعمیم‌پذیری داشته باشد، در بعد خرد قرار دارد؛ لذا در این تحقیق هم از روش‌های کمی و هم کیفی استفاده گردید. به عبارت دیگر روش پژوهش در این تحقیق برحسب هدف کاربردی، ازنظر روش گردآوری داده‌ها توصیفی-پیمایشی از نوع همبستگی و همین‌طور از نظر نوع داده کمی بود. در این تحقیق با راهنمایی اساتید و خبرگان متناسب با موضوع، نوع تحقیق، متغیرها و فرضیات تحقیق به روش نمونه گیری تصادفی[5] بر روی جامعه آماری انجام پذیرفت. جامعه آماری این پژوهش، مدیران، خبرگان، اساتید مهندسی کامپیوتر، فناوری‌اطلاعات و ... دانشگاه آزاد اسلامی واحدهای تهران می‌باشند که در حوزه امنیت و پدافند سایبری شرکت‌های دانش بنیان زیرمجموعه این دانشگاه‌ها فعالیت نموده‌اند، که با استفاده از نمونه‌گیری تصادفی، نمونه‌های مربوطه انتخاب گردید.

۳-۲. حجم نمونه: منظور از حجم نمونه در واقع میزان افراد مورد مطالعه در هر تحقیق می‌باشد که براساس موضوع و نوع تحقیق مورد بررسی قرار می‌گیرد. در این تحقیق با استفاده از یک نمونه تصادفی تحقیقات بر روی افراد جامعه مورد نظر صورت پذیرفته است. با توجه به این که تعداد جامعه آماری مورد مطالعه مشخص بود.(حدود ۲۰۰ نفر). پس از فرمول کوکران برای جوامع متناهی برای مشخص کردن حجم نمونه به شرح رابطه ۱. استفاده شده است (کوکران، *1977*): (رابطه۱)

$$n=\frac{Nz^{2}{}_{\alpha/2}pq}{(N-1)\varepsilon^{2}+z^{2}{}_{\alpha/2}pq}$$

N=حجم جامعه آماری،

n= حجم نمونه لازم،

P= احتمال موفقیت = ۰,۵ ،

$q=(1-p)$= احتمال شکست

ε=۰,۵ نماینده دقت برآورد یا همان حداکثر خطاست

$Z_{\alpha/2}$= ۰,۰۵ مقدار متغیر متناظر با سطح اطمینان مورد نظر برای فاصله اطمینان۹۵٪ که برابر با ۱,۹۶ می‌باشد.

حجم نمونه به‌دست‌آمده جهت مطالعه یا جامعه آماری مورد مطالعه ۱۳۲ نفر می‌باشد. در انجام تحقیق چون احتمال این مورد وجود داشت که تمامی پرسشنامه‌ها تکمیل نگردند. لذا ۲۰۰ پرسشنامه در بین جامعه آماری مورد مطالعه پخش گردید و در پایان دقیقا تعداد ۱۳۲ پرسشنامه مورد تایید قرار گرفته و جمع آوری گردید. در ضمن در خصوص سؤالات تحقیق از آزمون‌های مورد تایید و معتبر همچون آزمون آلفای‌کرونباخ[6] برای پایایی سوالات پرسشنامه استفاده شده است که میزان پایایی سوالات پرسشنامه را تایید می‌نماید. ضریب آلفای‌کرونباخ زمانی که بیش از ۰,۷ باشد می‌توان گفت پرسشنامه از اعتبار بالایی برخوردار است، چون ضریب آلفای‌کرونباخ در این تحقیق با استفاده از نرم افزار *Spss* برابر با جداول ذیل به دست آمده پس می‌توان این گونه بیان نمود پرسشنامه تحقیق فوق از اعتبار قابل قبولی برخوردار است. در جداول (۷-۲) شاخص‌ها و زیرمولفه‌های اثرگذار انواع تهدیدات در امنیت سایبری سازمان‌ها به همراه ضریب آلفای‌کرونباخ نمایش داده شده است.

جدول ۲.زیرمولفه‌های اثرگذار تهدیدات سخت در امنیت و پدافند سایبری

متغیر اصلی	زیرمؤلفه‌های اثرگذار (شاخص‌ها)	ضریب آلفای کرونباخ
تهدیدات سخت	میزان اهمیت مراکز و سازمان‌های دانش‌بنیان	۰,۷۵
	تشکیلات استراتژیک داده‌محور	۰,۷۴
	الویت بندی طرح‌ها و برنامه‌ها	۰,۷۶
	پیاده‌سازی پروژه‌های امنیت اطلاعات	۰,۷۳
	خرید سخت‌افزارهای امنیتی جدید	۰,۷۹
	تأمین استانداردهای بین‌المللی	۰,۷۸
	اصل و گزینش مکان‌یابی سایبری	۰,۷۹
	تأیید اصل امایش سرزمین	۰,۷۶
	طراحی اماکن و مراکز داده‌ای	۰,۷۷
	استقرار سایت‌ها پدافند سایبری	۰,۷۸

جدول ۳.زیرمولفه‌های اثرگذار تهدیدات نیمه‌سخت در پدافند سایبری

شاخص اصلی	زیرمؤلفه‌های اثرگذار (شاخص‌ها)	ضریب آلفای کرونباخ
تهدیدات	تعیین نقاط امن برای استقرار عملکردها	۰,۷۵

[1] Secretly programmed malicious codes
[2] Destructive techniques of data science
[3] Machine learning algorithms
[4] Data mining algorithms
[5] Simple random sampling
[6] Cronbach's alpha

نیمه‌سخت	انتخاب جایگزین بهینه در مکان‌گزینی مناسب	۰,۷۹
	استقرار طرح‌ها در سایت‌های ایستا و پویا	۰,۷۸
	میزان قابلیت استحکام سایت‌ها در برابر حملات	۰,۷۷
	ایمن‌سازی بسترهای ارائه سرویس	۰,۷۶
	عملکردهای پروژه‌های سایبری پدافندی	۰,۷۹
	اقدامات اطلاعاتی پیش‌بینی‌نشده	۰,۷۶
	مقاوم‌سازی کدهای تحلیلی در حملات	۰,۷۹
	ارتقا محصون‌سازی و قابلیت ایمن‌سازی شبکه‌ها	۰,۷۸

جدول ۴. زیرمولفه‌های اثرگذار تهدیدات نرم در امنیت و پدافند سایبری

متغیر اصلی	زیرمؤلفه‌های اثرگذار (شاخص‌ها)	ضریب آلفای کرونباخ
تهدیدات نرم	محصولات و خدمات ارائه شده توسط پیمانکاران	۰,۷۹
	تجهیزات امنیتی در سایت‌ها و سیستم‌ها	۰,۸۲
	روابط بین سیستم‌ها در برابر حملات و تهدیدات	۰,۸۱
	اطمینان از کفایت قدرت پردازشی و حافظهٔ سیستم‌ها	۰,۷۵
	اصل مقاوم‌سازی منابع و سیستم‌های اطلاعاتی	۰,۷۹
	حفاظت از دارایی‌ها در برابر حملات شبکه‌ای	۰,۷۸
	اصل امن‌سازی سایت‌های ارتباطی و سیستمی	۰,۷۶
	اصل انطباق در تحلیل تهدیدات نرم	۰,۷۷
	هم‌راستایی سیستم امنیتی و محیط سایبری	۰,۷۵
	تبیین اصل جهاد فرهنگی	۰,۷۴

جدول ۵. زیرمولفه‌های اثرگذار تهدیدات شناخته شده در پدافند سایبری

متغیر اصلی	زیرمؤلفه‌های اثرگذار (شاخص‌ها)	ضریب آلفای کرونباخ
سایر تهدیدات	توسعه زیرساخت‌های سیستمی	۰,۷۹
	تحلیل شبکه‌ای با توجه نوع استفاده در فضای سایبری	۰,۷۹
	اقدامات ساختارمند (حفاظ‌های الکتریکی و..)	۰,۷۸
	کاربردهای محوری از سیستم‌های امنیتی (ارتینگ و..)	۰,۷۶
	ایمن‌سازی مجازی در فضای سایبری	۰,۷۷
	تهدیدات رسانه‌ای در فضای سایبری	۰,۷۶
	افزایش قابلیت اطمینان در مراکز اطلاعاتی	۰,۷۹
	استفاده از مشاوران امنیت اطلاعات	۰,۷۶
	تبیین انواع حملات اجتماعی (مهندسی اجتماعی)	۰,۸۱

جدول ۶. زیرمولفه‌های اثرگذار تهدیدات ناشناخته در پدافند سایبری

متغیر اصلی	زیرمؤلفه‌های اثرگذار (شاخص ها)	ضریب آلفای کرونباخ
سایر	شکاف‌های امنیت سایبری	۰,۷۹
تهدیدات	سرقت یا نابودی دارایی‌های معنوی	۰,۷۶
	انواع حملات پیچیده و مبهم	۰,۷۳
	انواع آسیب‌های فراتشخیصی هوشمند	۰,۷۹
	انواع باج‌افزارها محیطی	۰,۷۸
	کدهای مخرب برنامه‌نویسی شده مخفی	۰,۷۷
	انواع بدافزارهای سیستمی	۰,۷۶
	انواع تکنیک‌های مخرب علم داده	۰,۷۹
	الگوریتم‌های یادگیری ماشین	۰,۸۱
	تشخیص پیش‌گام تهدیدات روز صفر	۰,۷۹
	الگوریتم‌های داده‌کاوی مبهم و نامعین	۰,۷۸

جدول ۷. جدول نهایی متغیرها و ضریب آلفای کرونباخ پرسشنامه‌ها

نوع پرسش‌نامه	ضریب آلفای کرونباخ
پرسش‌نامه مؤلفه تهدیدات سخت	۰,۷۴
پرسش‌نامه مؤلفه تهدیدات نیمه‌سخت	۰,۷۱
پرسش‌نامه مؤلفه تهدیدات نرم	۰,۷۲
پرسش‌نامه مؤلفه سایر تهدیدات شناخته شده	۰,۷۳
پرسش‌نامه مؤلفه سایر تهدیدات ناشناخته	۰,۷۵
پرسش‌نامه مؤلفه فرایند پدافند سایبری	۰,۷۶

۴. یافته‌های تحقیق " تجزیه وتحلیل داده‌ها"

در ابتدا با استفاده از داده‌های جمع‌آوری شده که از پرسش‌نامه توزیع شده میان جامعه آماری استخراج گردیده فرضیه‌های تحقیق موردبررسی قرار گرفت و با استفاده از نرم‌افزارهای مانند،*Spss* *Excel* به تجزیه‌وتحلیل داده‌ها پرداخته شد. در بخش آمار توصیفی به‌منظور کسب اطلاعات بیشتر درباره جامعه آماری و متغیرهای موردمطالعه، از جداول فراوانی مطلق، فراوانی نسبی، فراوانی نسبی تجمعی، نمودار میله‌ای برای تجزیه‌وتحلیل داده‌ها استفاده گردید. در بخش آمار استنباطی نیز ابتدا جهت محاسبه نرمال بودن متغیرهای تحقیق از آزمون آماری کولوموگروف– اسمیرنوف استفاده شد. سپس باتوجه‌به خروجی داده‌ها، از آزمون ضریب همبستگی اسپیرمن جهت بررسی فرضیه‌ها، نحوه ارتباط میان مؤلفه‌ها و تأثیر متغیرها و مؤلفه‌ها بر یکدیگر استفاده گردید. همچنین در بخش پایانی تحقیق میان مؤلفه‌های مورد بررسی، سطح‌بندی، اولویت‌بندی صورت پذیرفت [۳۶].

۴-۱. آمار توصیفی داده‌ها :

در این بخش می‌بایست سؤالاتی که این فرضیه‌ها را شامل می‌شوند مشخص گردید، سپس بر اساس داده‌های موجود فراوانی مطلق، فراوانی نسبی، فراوانی نسبی تجمعی را به دست آورد و نمودارهای مربوط به هر جدول ترسیم گردید.

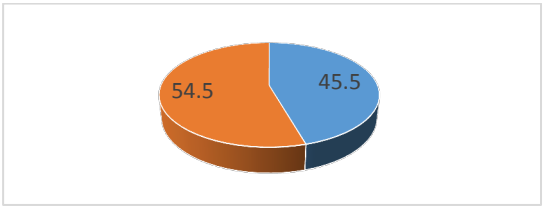
۴-۱-۱. آمار توصیفی جنسیت افراد مورد مطالعه :

بر اساس اطلاعات به‌دست‌آمده از پرسش‌نامه جنسیت افراد موردمطالعه در این تحقیق مطابق جدول ۸. و نمودار ۳. ذیل می‌باشد:

جدول ۸. توزیع فراوانی مربوط به جنسیت پاسخ دهندگان

جنسیت	فراوانی	فراوانی نسبی	فراوانی نسبی تجمعی
زن	۶۰	۴۵,۵	۴۵,۵
مرد	۷۲	۵۴,۵	۱۰۰
جمع	۱۳۲	۱۰۰	

جنسیت بیشتر پاسخ‌دهندگان مرد بوده ۷۲ نفر و ۶۰ نفر نیز زن می‌باشد.



نمودار ۳. توزیع فراوانی مربوط به جنسیت پاسخ دهندگان

۴-۱-۲. آمار توصیفی گروه سنی افراد مورد مطالعه :

بر اساس اطلاعات به‌دست‌آمده از پرسش‌نامه سن پاسخ‌دهندگان در این تحقیق مطابق جدول ۹ می‌باشد :

جدول ۹. توزیع فراوانی مربوط به سن پاسخ دهندگان

سن	فراوانی	فراوانی نسبی	فراوانی نسبی تجمعی
۲۰-۳۰ سال	۲۲	۱۶,۶	۱۶,۶
۳۰-۴۰ سال	۴۳	۳۲,۵	۴۹,۱
۴۰-۵۰ سال	۳۵	۲۶,۵	۷۵,۶
۵۰-۶۰ سال	۲۷	۲۰,۵	۹۶,۱
بالاتر از ۶۰ سال	۵	۳,۹	۱۰۰
جمع	۱۳۲	۱۰۰	

گروه سنی بیشترین پاسخ‌دهندگان حدود ۴۰-۳۰ سال یعنی ۴۳ نفر حدود ۳۲,۵ درصد می‌باشد، گروه سنی کمترین پاسخ دهندگان بالاتر از ۶۰ سال یعنی ۵ نفر حدود ۳,۹ درصد می‌باشد.

۴-۲. آمار استنباطی داده‌ها :

در این بخش آمار استنباطی داده‌ها ارائه می‌شود که شامل بررسی نرمال بودن داده‌ها و اثر آنها به‌صورت مستقیم بر سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان است. لازم به ذکر است، بررسی نرمال بودن داده‌ها این امکان را برای محقق ایجاد می‌نماید تا بتواند و بداند از چه نوع همبستگی می‌بایست در تحقیق استفاده نماید. حال باتوجه‌به مطالب فوق مشخص گردید:

H_0 *داده‌ها نرمال هستند.*

H_1 *داده‌ها نرمال نیستند.*

به عبارت ساده می‌توان این‌گونه بیان نمود:

پذیرش H_0 *یعنی داده‌ها نرمال هستند.* $(sig > 0.05)$

رد H_0 *یعنی داده‌ها نرمال نمی‌باشند.* $(0.05 > sig)$

۴-۲-۱. ارزیابی و نرمال بودن داده‌ها :

فرض نرمال بودن داده‌ها در واقع شامل ۵ متغیر و مولفه اثرگذار در فرضیه‌های تحقیق می‌باشد که به طور جداگانه، نرمال بودن نمرات این مولفه‌ها مورد سنجش قرار گرفته است :

جدول ۱۰. آمار استنباطی نرمال بودن داده‌ها

متغیر	تعداد	p - مقدار
تبیین میزان اثرگذاری مؤلفه تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۱۳۲	**۰,۰۰۲**
تبیین میزان اثرگذاری مؤلفه تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۱۳۲	**۰,۰۰۳**
تبیین میزان اثرگذاری مؤلفه تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۱۳۲	**۰,۰۰۱**
تبیین میزان اثرگذاری مؤلفه تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۱۳۲	**۰,۰۰۱**
تبیین میزان اثرگذاری مؤلفه تهدیدات ناشناخته و هوشمند در پدافند سایبری سازمان‌های دانش‌بنیان	۱۳۲	**۰,۰۰۲**

مطابق جدول ۱۰چون P-مقدار به دست آمده برای تمامی مولفه‌های مورد بررسی کمتر از ۰/۰۵ است. بنابراین فرض صفر مبنی بر نرمال بودن داده‌ها در این مولفه‌ها برقرار نیست $(0.05>sig)$.

یعنی P- مقدار به‌دست‌آمده برای تبیین میزان اثرگذاری مؤلفه تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان برابر با ۰,۰۰۲، تبیین میزان اثرگذاری مؤلفه تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان برابر با ۰,۰۰۳، تبیین میزان اثرگذاری مؤلفه تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان برابر با ۰,۰۰۱، تبیین میزان اثرگذاری مؤلفه تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان برابر با ۰,۰۰۱، تبیین میزان اثرگذاری مؤلفه تهدیدات ناشناخته و هوشمند در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان برابر با ۰,۰۰۲ است؛ بنابراین ازآنجا که همه P قدارهای به دست آمده از ۰,۰۵ کوچکتر می‌باشد فرض H_0 مورد پذیرش قرار نمی‌گیرد به عبارت ساده تر داده‌ها نرمال نمی‌باشند .

۴-۳. بررسی فرضیات تحقیق :

فرضیه اول اصلی:

- "سطح‌بندی انواع تهدیدات بر اساس راهبرد امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور است."

برای تبیین و بررسی این فرضیه می‌بایست تمامی فرضیه فرعی در این حوزه موردبررسی قرار گیرد. در این بخش فرضیات فرعی موردبحث در این بخش تحقیق موردبررسی قرار می‌گیرد:

۴-۳-۱. فرضیه اول فرعی :

" سطح‌بندی انواع تهدیدات سخت در افزایش امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور تأثیر مثبت و معناداری دارد."

در ابتدا قبل از سطح‌بندی انواع تهدیدات سخت در افزایش امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌بایست میزان اثرگذاری و اثرپذیری مؤلفه‌ها مشخص گردد، برای این منظور نوع آزمون و میزان اثرگذاری مؤلفه‌ها توسط آزمون همبستگی استفاده می‌گردد، برای این مهم قبل از انجام تمامی امور، نرمال بودن داده‌ها موردبررسی قرار گیرد؛ بنابراین در این مرحله هدف انجام آزمون فرض زیر است:

سطح‌بندی انواع تهدیدات سخت در افزایش امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور تأثیر مثبت و معناداری ندارد: H_0

سطح‌بندی انواع تهدیدات سخت در افزایش امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور تأثیر مثبت و معناداری دارد: H_1

مطابق مطالب بالا اگر مقدار $0.05>sig$ باشد سطح‌بندی انواع تهدیدات سخت در افزایش امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد و H_1 مورد تأیید است، لذا H_0 رد خواهد شد. در فرضیه اول می‌بایست اثر افزایش مولفه انواع تهدیدات سخت در افزایش پدافند سایبری سازمان‌های دانش‌بنیان مورد بررسی قرار گیرد. نتایج به دست آمده از آزمون فرض فوق در جدول ۱۱ به شرح زیر می‌باشد :

جدول ۱۱. آمار استنباطی بررسی فرضیه اول

متغیرها	بررسی اثر افزایش مؤلفه تهدیدات سخت در فرایند پدافند سایبری در سازمان‌های دانش‌بنیان
تعداد	۱۳۲
p- مقدار	۰,۰۰۱
ضریب همبستگی	۰,۴۶۵

همان‌طور که در جدول بالا بیان شده:

- تعداد برابر با ۱۳۲ می‌باشد و چون p-مقدار برابر با ۰,۰۰۱و کمتر از ۰,۰۵ می‌باشد.
- بنابراین، افزایش مؤلفه سطح‌بندی انواع تهدیدات سخت در افزایش امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور اثر مثبت و معناداری دارد و فرضیه اول تأیید می‌گردد.
- بنابراین، فرض H_0 رد می‌شود؛ بنابراین فرض صفر در سطح ۹۵ درصد مورد تایید قرار نمی‌گیرد و فرض مقابل تایید می‌گردد.
- لازم به ذکر است ازآنجاکه مقدار ضریب همبستگی اسپیرمن مثبت است (r=۰,۴۶۵). با افزایش هر یک از شاخص‌ها بر شاخص دیگر نیز اثر مثبت و مستقیمی می‌گذارد.

۴-۳-۲. فرضیه دوم فرعی :

"سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد."

ازآنجاکه در مرحله قبل فرض نرمال بودن داده‌ها در مورد تمامی متغیر رد شد، اکنون می‌بایست نحوه تأثیر و معنادار بودن بین دو متغیر در فرضیات موردبررسی قرار گیرد. برای بررسی اثرپذیری بین دو متغیر از ضریب همبستگی اسپیرمن استفاده می‌شود.

سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری ندارد: H_0

سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد: H_1

مطابق مطالب بالا اگر مقدار $0.05>sig$ باشد سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد، لذا H_1 موردتأیید است و H_0 رد خواهد شد. در فرضیه دوم می‌بایست اثر افزایش مؤلفه انواع تهدیدات نیمه سخت در پدافند سایبری سازمان‌های دانش‌بنیان مورد بررسی قرار گیرد. نتایج به دست آمده از آزمون فرض فوق در جدول ۱۲. به شرح زیر می‌باشد :

جدول ۱۲. آمار استنباطی بررسی فرضیه دوم

متغیرها	بررسی اثر افزایش مؤلفه تهدیدات نیمه‌سخت در فرایند پدافند سایبری در سازمان‌های دانش‌بنیان
تعداد	۱۳۲
p- مقدار	۰,۰۰۲
ضریب همبستگی	۰,۵۲۱

همان‌طور که در جدول بالا بیان شده:

- تعداد برابر با ۱۳۲ می‌باشد و چون p-مقدار برابر با ۰,۰۰۲ و کمتر از ۰,۰۵ می‌باشد.
- بنابراین، افزایش سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد و فرضیه دوم تأیید می‌گردد.
- بنابراین، فرض H_0 رد می‌شود؛ بنابراین فرض صفر در سطح ۹۵ درصد مورد تایید قرار نمی‌گیرد و فرض مقابل تایید می‌گردد.
- لازم به ذکر است ازآنجاکه مقدار ضریب همبستگی اسپیرمن مثبت است (r=۰,۵۲۱). با افزایش هر یک از شاخص‌ها بر شاخص دیگر نیز اثر مثبت و مستقیمی می‌گذارد.

۴-۳-۳. فرضیه سوم فرعی :

" سطح‌بندی انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور تأثیر مثبت و معناداری دارد."

برای بررسی اثرپذیری بین دو متغیر از ضریب همبستگی اسپیرمن استفاده می‌شود. در این مرحله هدف انجام آزمون فرض زیر است:

سطح‌بندی انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان *تأثیر مثبت و معناداری ندارد:* H_0

سطح‌بندی انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان *تأثیر مثبت و معناداری دارد.* : H_1

مطابق مطالب بالا اگر مقدار $0.05>sig$ باشد افزایش مؤلفه انواع تهدیدات نرم در پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد و H_1 موردتأیید است، لذا H_0 رد خواهد شد. در فرضیه سوم اثر افزایش مولفه انواع تهدیدات نرم در پدافند سایبری

سازمان‌های دانش‌بنیان مورد بررسی قرار گرفت. نتایج به دست آمده از آزمون فرض فوق در جدول ۱۳. به شرح زیر می‌باشد:

جدول ۱۳. آمار استنباطی بررسی فرضیه سوم

متغیرها	بررسی اثر افزایش مؤلفه تهدیدات نرم در فرایند پدافند سایبری در سازمان‌های دانش‌بنیان
تعداد	۱۳۲
p- مقدار	۰,۰۷۰
ضریب همبستگی	۰,۴۳۵

همان‌طور که در جدول بالا بیان شده:

- تعداد برابر با ۱۳۲ می‌باشد و چون p-مقدار برابر با ۰,۰۷۰ و بزرگتر از ۰,۰۵ می‌باشد.
- بنابراین، افزایش مؤلفه انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری ندارد، لذا فرضیه چهارم تأیید نمی‌گردد.
- بنابراین، فرض H_0 تأیید می‌شود؛ بنابراین فرض صفر در سطح ۹۵ درصد مورد تایید قرار می‌گیرد و فرض مقابل تایید نمی‌گردد، بنابراین هیچ گونه ارتباطی میان مولفه‌های این تحقیق با یکدیگر وجود ندارد. یعنی میان افزایش مولفه تهدیدات نرم (درون گروهی و برون گروهی) در فضای سایبری در فرایند پدافند سایبری در سازمان‌های دانش‌بنیان هیچ گونه ارتباطی وجود ندارد.

۴-۳-۴. فرضیه چهارم فرعی :

" سطح‌بندی انواع تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد."

چون در مرحله قبل فرض نرمال بودن داده‌ها در مورد تمامی متغیر رد شد، لذا نحوه تأثیر و معنادار بودن بین دو متغیر در فرضیات بایستی موردبررسی قرار گیرد. در این مرحله هدف انجام آزمون فرض زیر است:

سطح‌بندی انواع تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری ندارد: H_0

سطح‌بندی انواع تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد. : H_1

مطابق مطالب بالا اگر مقدار $0.05>sig$ باشد، افزایش مؤلفه انواع تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد و H_1 موردتأیید است، لذا H_0 رد خواهد شد. در فرضیه چهارم می‌بایست اثر افزایش مؤلفه انواع تهدیدات موجود (شناخته شده) در امنیت سازمان‌های دانش‌بنیان موردبررسی قرار گرفت. نتایج به‌دست‌آمده از آزمون فرض فوق در جدول ۱۴. به شرح زیر می‌باشد:

جدول ۱۴. آمار استنباطی بررسی فرضیه چهارم

متغیرها	بررسی اثر افزایش مؤلفه سایر تهدیدات موجود (شناخته شده) در فرایند پدافند سایبری در سازمان‌های دانش‌بنیان
تعداد	۱۳۲
p- مقدار	۰,۰۰۲
ضریب همبستگی	۰,۳۸۸

همان‌طور که در جدول ۱۴. بیان شده:

- تعداد برابر با ۱۳۲ می‌باشد و چون p-مقدار برابر با ۰,۰۰۲و کمتر از ۰,۰۵ می‌باشد.
- بنابراین، افزایش مولفه انواع تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان اثر مثبت و معناداری دارد و فرضیه چهارم تایید می‌گردد.
- بنابراین، فرض H_0 رد می‌شود؛ بنابراین فرض صفر در سطح ۹۵ درصد مورد تایید قرار نمی‌گیرد و فرض مقابل تایید می‌گردد.
- لازم به ذکر است ازآنجاکه مقدار ضریب همبستگی اسپیرمن مثبت است (r=۰,۳۸۸)؛ لذا ارتباط در جهت مستقیم است. با افزایش هر یک از شاخص‌ها بر شاخص دیگر نیز اثر مثبت و مستقیمی می‌گذارد.

۴-۳-۵. فرضیه پنجم فرعی:

" سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد."

چون در مرحله قبل فرض نرمال بودن داده‌ها در مورد تمامی متغیر رد شد، لذا نحوه تأثیر و معنادار بودن بین دو متغیر در فرضیات بایستی موردبررسی قرار گیرد. هدف انجام آزمون فرض زیر است:

سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان *تأثیر مثبت و معناداری ندارد:* H_0

سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان *تأثیر مثبت و معناداری دارد:* H_1

مطابق مطالب بالا اگر مقدار $0.05>sig$ باشد، افزایش مؤلفه انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان تأثیر مثبت و معناداری دارد و H_1 موردتأیید است، لذا H_0 رد خواهد شد. در فرضیه پنجم می‌بایست اثر افزایش مؤلفه انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان موردبررسی قرار گرفت. نتایج به‌دست‌آمده از آزمون فرض فوق در جدول ۱۵. به شرح زیر می‌باشد:

جدول ۱۵. آمار استنباطی بررسی فرضیه پنجم

متغیرها	بررسی اثر افزایش مؤلفه سایر تهدیدات هوشمند در فرایند پدافند سایبری در سازمان‌های دانش‌بنیان
تعداد	۱۳۲
p- مقدار	۰,۰۰۱
ضریب همبستگی	۰,۴۵۵

همان‌طور که در جدول بالا بیان شده:

- تعداد برابر با ۱۳۲ می‌باشد و چون p-مقدار برابر با ۰,۰۰۱و کمتر از ۰,۰۵ می‌باشد.

❖ بنابراین، افزایش مؤلفه انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان اثر مثبت و معناداری دارد و فرضیه پنجم تأیید می‌گردد.

❖ بنابراین، فرض H_0 رد می‌شود؛ بنابراین فرض صفر در سطح ۹۵ درصد مورد تایید قرار نمی‌گیرد و فرض مقابل تایید می‌گردد.

❖ لازم به ذکر است ازآنجاکه مقدار ضریب همبستگی اسپیرمن مثبت است (r=۰,۴۵۵)؛ لذا ارتباط در جهت مستقیم است. با افزایش هر یک از شاخص‌ها بر شاخص دیگر نیز اثر مثبت و مستقیمی می‌گذارد.

۴-۴. تبیین سطح‌بندی متغیرهای تحقیق :

برای تبیین سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور می‌بایست در ابتدا سطح و اولویت هر یک از متغیرها و مؤلفه‌های مشخص شده و سپس بر اساس میزان امتیاز متغیرها سطح‌بندی و اولویت‌بندی میان مؤلفه‌ها صورت می‌پذیرد. فرضیه مربوط به شرح ذیل است:

H_0 *سطح‌بندی و اولویت میان متغیرهای موردبررسی تحقیق یکسان است:*

H_1 *سطح‌بندی اولویت میان متغیرهای موردبررسی تحقیق یکسان نیست:*

به‌عبارت‌دیگر می‌توان این‌گونه بیان نمود:

فرض صفر: میان متغیر موردبررسی تحقیق در تبیین سطح‌بندی انواع تهدیدات اختلاف معناداری وجود ندارد.

فرض مقابل: میان متغیر موردبررسی تحقیق تبیین سطح‌بندی انواع تهدیدات اختلاف معناداری وجود دارد.

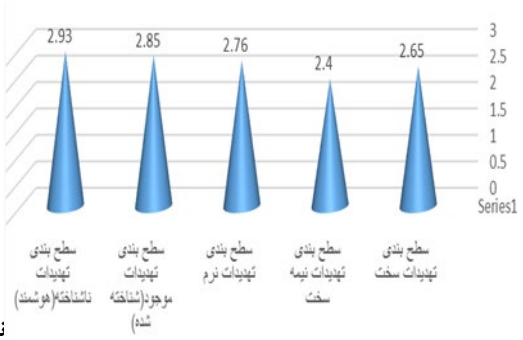
در ادامه پس از بررسی فرضیه‌ها، متغیرهای تحقیق و ارتباط میان آنها و ارزیابی همبستگی میان متغیرها در راستای تبیین سطح‌بندی انواع تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان در این بخش می‌بایست متغیرهای موردبررسی رتبه‌بندی شوند:

جدول ۱۶. آمار سطح‌بندی آزمون فریدمن متغیرهای تحقیق

متغیرهای موردبررسی تحقیق	میانگین رتبه متغیر	*p-value*
تبیین سطح‌بندی انواع تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۲,۶۵	۰,۰۰۲
تبیین سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۲,۴۰	۰,۰۰۳
تبیین سطح‌بندی انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۲,۷۶	۰,۰۰۲
تبیین سطح‌بندی انواع تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۲,۸۵	۰,۰۰۱
تبیین سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان	۲,۹۳	۰,۰۰۲

مطابق جدول ۱۶. آمار توصیفی مربوط به متغیرهای مورد بررسی تحقیق بیان شده است در این جدول میانگین نمرات هر متغیر نشان داده شده است. بر اساس نتایج به دست آمده :

میانگین رتبه متغیر سطح‌بندی انواع تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان (برابر است با ۲,۶۵)، سطح‌بندی انواع تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان (برابر است با ۲,۴۰)، سطح‌بندی انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان (برابر است با ۲,۷۶)، سطح‌بندی انواع تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان (برابر است با ۲,۸۵)، سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان (برابر است با ۲,۹۶)، همچنین باتوجه‌به جدول ۱۳.میانگین رتبه متغیرهای موجود در جدول، این مقادیر به هم بسیار نزدیک است.



نمودار ۴. سطح‌بندی انواع تهدیدات در پدافند سایبری سازمان‌ها

مطابق جدول ۱۷. آمار استباطی مربوط به متغیرهای مورد بررسی تحقیق بیان شده است در این جدول سطح معناداری متغیرها (sig) به علت اینکه کمتر از ۰,۰۵ است فرض H_0 مورد تایید قرار نمی‌گیرد و فرض H_1 مورد قبول واقع می‌شود. به عبارت دیگر تفاوت معناداری میان آنها وجود دارد به عبارت دیگر از لحاظ سطح بندی و رتبه‌بندی میان این متغیرها تفاوتی وجود دارد، فرض صفر مورد تایید قرار نمی‌گیرد. براساس میزان تعریف سطح‌بندی میان متغیرها، نیز تنوع متغیرها، درجه آزادی و سطح معناداری می‌توان این گونه بیان شود که، متغیرهای مورد بررسی دارای سطح‌بندی در سطوح مختلف تحقیق هستند.

جدول ۱۷. مقادیر آزمون فریدمن متغیرهای مورد بررسی تحقیق

اقدامات متغیرهای تحقیق	مقادیر آزمون فریدمن
تعداد داده‌های هر متغیر	۱۳۲
مقدار آماره کای دو.	۰,۱۴۶
درجه آزادی	۴
سطح معناداری متغیرها (sig)	۰,۰۳۵

۵-یافته‌های تحقیق(*تحلیل* و بحث روی نتایج تحقیق)

در این بخش نتایج به‌دست‌آمده از تجزیه‌وتحلیل داده‌ها پرداخته می‌شود:

۵-۱. نتیجه‌گیری فرضیه اول فرعی:

❖ هرچه به بهبود شرایط در حوزه امنیت سیستم‌ها و کاهش آسیب‌پذیری و خطرات در حوزه تهدیدات سخت و زیرمؤلفه‌های موجود توجه شود، قاعدتاً این مهم باعث افزایش

اثرگذاری بیشتر و دقیق‌تر در نحوه مقابله با انواع چالش‌ها و مقابله با انواع تهدیدات سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌گردد. در توضیح ابهامات این نتیجه‌گیری باید بیان شود، گاها تمامی مسائل مربوط به بهبود شرایط در حوزه امنیت سیستم‌ها و کاهش آسیب‌پذیری و خطرات در حوزه تهدیدات سخت نمی‌تواند مثبت واقع گردد، ولیکن با تبیین ساختارهای مثبت در سیستم، نیز تبیین آموزش در بخش‌های مختلف برای کارکنان و ارزش‌گذاری برای مسائل مختلفی در حوزه‌های متعددی مانند؛ میزان اهمیت مراکز و سازمان‌های دانش‌بنیان، تشکیلات استراتژیک سازمان داده‌محور، اولویت‌بندی طرح‌ها و برنامه‌ها، تأیید اصل امایش سرزمین و... در فضای سایبری سازمان‌ها و شرکت‌های دانش‌بنیان می‌تواند در سطح‌بندی انواع تهدیدات سخت در افزایش امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کشور تأثیر مثبت و معناداری داشته باشد.

- ❖ پیشگیری در برابر انواع تهدیدات و سطح‌بندی آن را از مهم‌ترین اولویت‌های امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌توان برشمرد، لذا در اجرای اصل سطح‌بندی تهدیدات سخت به‌منظور حفظ دستاوردهای امنیتی و حفاظتی، ایجاد ساختار منسجم، تشکیل شبکه‌های یکپارچه، ارتقاء سلامت نظام‌مند سیستم‌ها، تغییرات راهبردی استانداردهای امنیتی، در شرایط بحرانی جامعه، اقدامات مختلفی را در دستور کار خود قرارداد.

۵-۲. نتیجه‌گیری فرضیه دوم فرعی:

- ❖ هرچه توجه به بهبود شرایط، افزایش آگاهی و فهم مدیران فناوری اطلاعات و خبرگان نسبت به مؤلفه‌ها و زیرشاخص‌های تهدیدات نیمه‌سخت بیشتر شود، قاعدتاً این مهم باعث افزایش اثرگذاری بیشتر و ساختارمندی بهتر بر نحوه تقابل با زیرشاخص‌های تهدیدات نیمه‌سخت در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌گردد.
- ❖ تقویت مقابله با تهدیدات نیمه‌سخت در امنیت و پدافند سایبری در راستای طبقه‌بندی و کنترل دارایی در شرکت‌ها و سازمان‌های دانش‌بنیان مطابق استانداردهای *ISO*، سبب بهبود، افزایش امنیت و پدافند سایبری در این سازمان‌ها می‌شود.

۵-۳. نتیجه‌گیری فرضیه سوم فرعی:

نکته مهمی در خصوص نتیجه‌گیری از تجزیه‌وتحلیل داده‌های حاصل از این فرضیه می‌توان به دست آورد در قالب موارد ذیل تشریح می‌گردد:

۱.در خصوص این فرضیه این مورد است که در نگاه اول برداشتی که از فرضیه می‌شود این است که این دو متغیر با هم ارتباط معناداری دارند، تجزیه وتحلیل داده های جمع آوری شده بیانگر عدم ارتباط و اثرگذاری این دو متغیر با هم می باشد.

۲.چون نتایج از یک جامعه آماری و به‌صورت واقعی و میدانی جمع‌آوری‌شده است و محقق هیچ‌گونه دخالتی در اطلاعات و نتایج به‌دست‌آمده نداشته است، پس تأیید و عدم تأیید فرضیه دلیل محکمی در رویکرد مثبت نسبت به نتیجه به‌دست‌آمده از این فرضیه است.

۳. همچنین بر اساس نظر خبرگانی همچون طبیبی و همکاران (۱۳۹۸)، تایید یا عدم تایید یک فرضیه هیچ گونه خللی در نتایج برگرفته از تحقیق نیست و صحت و دقت یک تحقیق را دچار چالش نمی‌کند بلکه هدف از بررسی یک فرضیه تایید و یا عدم فرضیه و یا نظریه است نه اثبات آن.

- ❖ افزایش قابلیت امنیت و مقابله با انواع تهدیدات نرم در امنیت و پدافند سایبری می‌تواند با بهره‌گیری از تخصص، خبرگی، مهارت مدیران فناوری اطلاعات، خبرگان فضای سایبری در سازمان‌ها و شرکت‌های دانش‌بنیان بهبود یابد.
- ❖ به‌عبارت‌دیگر هرچه توجه به بهبود فرایندهای امنیتی، کاهش چالش‌ها، زیرمؤلفه‌های تهدیدات نرم در سازمان‌ها و شرکت‌های دانش‌بنیان بیشتر شود، قاعدتاً این مهم باعث افزایش اثرگذاری بیشتر، دقیق‌تر بر روند کاهش آسیب‌پذیری، ارتقا استانداردهای امنیتی و مدیریت تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌گردد.
- ❖ در راستای تهدیدات امنیت سایبری و کاهش اقدامات مخربی که برای سرقت، تخریب یا ازبین‌بردن داده‌های حساس، به خطر انداختن سیستم‌ها یا هویت‌های رایانه‌ای، مختل کردن یا خرابکاری در عملیات تجاری، مقابله با انواع تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان الزامی است.

۵-۴. نتیجه‌گیری فرضیه چهارم فرعی :

- ❖ قانونمندی و ساختارپذیری مؤلفه سایر تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌تواند حاصل مثبتی بر نتیجه حاصل از این تحقیق داشته باشد؛ لذا با افزایش هر یک از شاخص‌ها بر شاخص دیگر نیز اثر مثبت و معناداری دارد و می‌بایست عوامل دیگر نیز موردبررسی قرار گیرد.
- ❖ همچنین ممکن است در انجام تحقیق عوامل مداخله‌گر یا عوامل ثانویه دیگری وجود داشته باشد که بایستی در تحقیقات دیگر و با انجام آزمون‌های دیگر تحقیقاتی یا سایر روش‌های دیگر آماری و تحقیق در عملیاتی موردبررسی قرار گیرد.
- ❖ مکانیسم‌های تهدیدات موجود (شناخته شده) شامل اقدامات ساختارمند، روان‌شناختی، رسانه‌ای، اجتماعی، شبکه‌ای و... در سطح سازمان‌های دانش‌بنیان است.
- ❖ کاربردهای محوری از سیستم‌های امنیتی در (ارتینگ و....) در سایت‌ها، ایمن‌سازی مجازی، تهدیدات رسانه‌ای و.. تکنیک‌های مقابله با انواع تهدیدات موجود (شناخته شده) در سازمان‌های دانش‌بنیان طراحی شده‌اند.

۵-۵. نتیجه‌گیری فرضیه پنجم فرعی:

- قانونمندی و ساختارپذیری مؤلفه سایر تهدیدات ناشناخته در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌تواند حاصل مثبتی بر نتیجه حاصل از این تحقیق داشته باشد؛ لذا با افزایش هر یک از شاخص‌ها بر شاخص دیگر نیز هیچ‌گونه اثری ندارد و می‌بایست عوامل دیگر نیز موردبررسی قرار گیرد.
- همچنین ممکن است در انجام تحقیق عوامل مداخله‌گر و یا عوامل ثانویه دیگری وجود داشته باشد که بایستی در تحقیقات دیگر و با انجام آزمون‌های دیگر تحقیقاتی یا سایر روش‌های دیگر آماری و تحقیق در عملیاتی موردبررسی قرار گیرد.
- مکانیسم‌های مناسبی برای انواع حملات ناشناخته و *zeroday* (روز صفر) در شرکت در نظر گرفته شود، به‌طورکلی ایجاد اختلال در زندگی دیجیتالی بر اساس مقابله با انواع تهدیدات ناشناخته (هوشمند) سازمان‌های دانش‌بنیان طراحی شده‌اند؛ لذا انواع رایج تهدیدات ناشناخته سایبری شامل روز صفر، بدافزار، باج‌افزار، انکار سرویس (*DDOS*) و حملات تزریق *SQL* قابل‌مشاهده است.

۶-۵. نتیجه‌گیری سطح‌بندی متغیرهای تحقیق :

- در خصوص رتبه‌بندی متغیرهای تحقیق، پس از بررسی نتایج و تجزیه‌وتحلیل دقیق متغیرها که در بخش اول تحقیق بیان شد، مشخص گردید، میان متغیرهای موردبررسی تحقیق، میزان قابلیت سطح‌بندی انواع تهدیدات سخت، ساختاربندی و کنترل سطح‌بندی انواع تهدیدات نیمه‌سخت، تبیین سطح‌بندی انواع تهدیدات نرم، تبیین سطح‌بندی تهدیدات موجود (شناخته شده) و تبیین سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان دارای اولویت متفاوتی است، به‌عبارت‌دیگر تفاوت معناداری میان آنها وجود دارد، لذا از لحاظ رتبه‌بندی میان این متغیرها تفاوتی متناسبی وجود دارد و فرض صفر موردتأیید قرار نمی‌گیرد. همچنین متغیرهای تحقیق از اولویت یکسانی برخوردار نیستند.
- همچنین از لحاظ سطح‌بندی موضوع کاملاً متفاوت است که می‌توان بر اساس تجزیه‌وتحلیل نتایج به‌دست‌آمده این‌گونه بیان نمود؛ رتبه سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در جایگاه اول، تهدیدات موجود (شناخته شده) در جایگاه دوم، تهدیدات نرم در جایگاه سوم، تهدیدات سخت در جایگاه چهارم، تهدیدات نیمه‌سخت در جایگاه پنجم امنیت و پدافند سایبری سازمان‌های دانش‌بنیان قرار دارد.

۶- پیشنهادها:

۶-۱. پیشنهادات فرضیه اول فرعی :

بر اساس یافته‌های این فرضیه پیشنهاد می‌شود:

- دانش و نحوه نگرش و شاخص‌های امنیتی در فضای سایبری در حوزه امنیت و پدافند سایبری در سازمان‌های دانش‌بنیان اهمیت فراوان دارد. زیرا این مهم اثر مثبتی بر استفاده بهینه از امکانات مختلف از جمله امنیت و شناخت تهدیدات سخت در حوزه‌های مختلف از جمله زیرساخت‌های فناوری اطلاعات و فضای سایبری در این سازمان‌ها دارد.
- جهت افزایش دانش امنیتی پدافند سایبری در سازمان‌های دانش‌بنیان می‌بایست بر اساس برنامه منسجم و یکپارچه، ساختارمند بر اساس مؤلفه تهدیدات سخت تدوین گردد.
- دوره‌های ویژه امنیتی در حوزه‌های مختلف فناوری اطلاعات، ارتقا هوش مصنوعی در راستا ارتقا امنیت و پدافند سایبری در جهت هم‌افزایی متقابل میان بخش‌های مختلف در سازمان‌های دانش‌بنیان در نظر گرفته شود.

۶-۲. پیشنهادات فرضیه دوم فرعی:

بر اساس یافته‌های این فرضیه پیشنهاد می‌شود:

- ساختارهای امنیتی مبتنی بر توسعه امنیت در فضای سایبری در تهدیدات نیمه‌سخت در سازمان‌های دانش‌بنیان افزایش یابد.
- قابلیت سطوح امنیتی بر اساس کنترل بیشتر بر امنیت و پدافند سایبری، تهدیدات نیمه‌سخت در سازمان‌های دانش‌بنیان بررسی گردد.
- لایه امنیتی مختلف موجود در معماری سیستم‌های اطلاعاتی در سازمان‌های دانش‌بنیان ارزیابی شود.

۶-۳. پیشنهادات فرضیه سوم فرعی :

بر اساس یافته‌های این فرضیه پیشنهاد می‌شود:

- باتوجه‌به افزایش تهدیدات نرم در سازمان‌های دانش‌بنیان می‌بایست از تخصص خبرگان، مهارت مهندسین، کارآمدی متخصصین فناوری اطلاعات، امنیت و پدافند سایبری در این سازمان‌ها بیشتر استفاده گردد.
- جهت مدیریت تهدیدات نرم در سازمان‌های دانش‌بنیان بایستی از امکانات و منابع موجود بهتر استفاده شود.
- اثرگذاری کنترل، مهندسی مجدد سیستم‌های امنیتی می‌تواند پدافند سایبری باعث کاهش تهدیدات نرم در سازمان‌های دانش‌بنیان گردد.
- استفاده از تکنولوژی‌های نوین باعث افزایش امنیت و کاهش آسیب‌پذیری و تهدیدات نرم در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان می‌گردد.

۶-۴. پیشنهادات فرضیه چهارم فرعی:

بر اساس یافته‌های این فرضیه پیشنهاد می‌شود:

- استفاده از قوانین، مقررات مدون و مشخص می‌تواند سایر تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کاهش دهد.

- بهبود فرایندهای سازمانی و ساختار منسجم، یکپارچه اثر مطلوبی بر مدیریت سایر تهدیدات موجود (شناخته شده) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان داشته باشد.
- برنامه‌های اطلاعاتی در پروژه‌های امنیتی، اطلاعات باعث کاهش ریسک‌پذیری در این حوزه می‌شود. همچنین سبب بهبود اقدامات ساختارمند، روان‌شناختی، رسانه‌ای، اجتماعی، شبکه‌ای و... سازمان‌های دانش‌بنیان می‌شود.

۶-۵. پیشنهادات فرضیه پنجم فرعی:

بر اساس یافته‌های این فرضیه پیشنهاد می‌شود:

- استفاده از قوانین، مقررات مدون و مشخص می‌تواند سایر تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان کاهش دهد.
- جهت مدیریت سایر تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان باید بر اساس ساختارها و الگوهای بومی در این حوزه استفاده نمود.
- بهبود فرایندهای سازمانی و ساختار منسجم، یکپارچه اثر مطلوبی بر مدیریت سایر تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان داشته باشد.
- برنامه‌های امنیتی و اطلاعاتی در پروژه‌های امنیتی، اطلاعات باعث پیشگیری‌های فازی، مقابله هوشمند، بهره‌گیری از سیستم‌های امنیتی خبره، انواع حملات روز صفر در این حوزه می‌شود.

۶-۵.پیشنهادات فرضیه سطح‌بندی متغیرهای تحقیق :

بر اساس یافته‌های این فرضیه پیشنهاد می‌شود:

- بر اساس تحلیل صورت‌گرفته، میزان قابلیت سطح‌بندی انواع تهدیدات سخت می‌تواند، تهدیدات و حملات سایبری و فعالیت‌های آسیب‌رسانی که باهدف تخریب، سرقت یا مختل کردن کامل اطلاعات هستند را تا حدود زیادی کاهش دهد.
- همچنین ساختاربندی و کنترل سطح‌بندی انواع تهدیدات نیمه‌سخت، باتوجه‌به نوع حمله، مقیاس حمله، شیوه حمله و محل تهاجم را مشخص نموده و تدابیر امنیتی لازم اعمال گردد.
- تبیین سطح‌بندی انواع تهدیدات نرم، می‌تواند از در شناسایی روابط بین سیستم‌ها در برابر حملات، اطمینان‌بخشی از کفایت قدرت پردازشی، حافظهٔ سیستم‌ها و قدرت نرم تحلیل فرایندهای تهدیدات در سیستم را ارتقا می‌دهد.
- تبیین سطح‌بندی تهدیدات بر ایمن‌سازی سیستم‌های اطلاعاتی و دارایی‌ها معنوی در برابر تهدیدات موجود (شناخته شده) را بهبود می‌بخشد. همچنین سبب بهبود فرایندهای سازمانی و ساختار منسجم، یکپارچه‌سازمانی می شود. سبب ارتقا اقدامات ساختارمند، روانشناختی، رسانه‌ای، اجتماعی، شبکه‌ای و... سازمان‌های دانش‌بنیان می‌شود.
- تبیین سطح‌بندی انواع تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان دارای کمیت و کیفیت متفاوتی در سیستم است، بر اساس آن می‌توان انواع ویروس‌های کامپیوتری، نقض داده، انواع حملات *DDoS*، حملات روز صفر و... تاحد زیادی کاهش داده و مدیریت نمود. این نوع تهدیدات سایبری ناشناخته فراگیرتر شده و درعین‌حال شاهد خطرات نوین سایبری پیشرفته‌تری نیز می‌باشد.

۷-آینده‌پژوهی و سیاست‌گذاری سطح‌بندی تهدیدات در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان:

۷-۱.آینده‌پژوهی و سیاست‌گذاری انواع تهدیدات سخت در پدافند سایبری:

جهت تبیین آینده‌پژوهی و سیاست‌گذاری تهدیدات سخت در پدافند سایبری در سازمان‌های دانش‌بنیان باید به ساختارهای مختلف و شاخص‌های گوناگونی توجه نمود. در ذیل به برخی از آنها اشاره می‌گردد:

- سطح‌بندی (اهمیت مراکز و تشکیلات استراتژیک) در فضای سایبری (پدافند سایبری)
- اولویت‌بندی طرح‌ها و پروژه‌های فناوری اطلاعات خصوصاً پدافند سایبری
- بررسی استانداردهای امنیت در فضای سایبری (پدافند سایبری)
- توسعه سطح ایمنی موردنیاز در فضای سایبری (پدافند سایبری)
- اصل مکان‌یابی در فضای سایبری (پدافند سایبری)
- طراحی اماکن و مراکز داده‌ای و استقرار سایت‌ها در فضای سایبری (پدافند سایبری)
- مجموعه ضوابط و استانداردهای بین‌المللی در فضای سایبری (پدافند سایبری)

۷-۲.آینده‌پژوهی و سیاست‌گذاری انواع تهدیدات نیمه‌سخت در پدافند سایبری:

جهت تبیین آینده‌پژوهی و سیاست‌گذاری تهدیدات نیمه‌سخت در پدافند سایبری در سازمان‌های دانش‌بنیان باید به ساختارهای مختلف و زیر شاخص‌های گوناگونی توجه نمود. در ذیل به برخی از آنها اشاره می‌گردد:

- انتخاب نقاط امن برای استقرار عملکردها در پدافند سایبری
- انتخاب جایگزین بهینه در مکان‌گزینی مناسب در فضای سایبری (پدافند سایبری)
- استقرار طرح‌ها در فضای سایبری
- مقاومت سایت‌ها در برابر حملات و تهدیدات نیمه‌سخت در فضای سایبری (پدافند سایبری)

❖ ایمن‌سازی بسترهای ارائه سرویس در فضای سایبری (پدافند سایبری)
❖ عملکردهای ساختاری در فضای سایبری (پدافند سایبری)
❖ پشتیبانی از کدهای تحلیلی در مقابل تهدیدات نیمه‌سخت در فضای سایبری (پدافند سایبری)
❖ ایمن‌سازی زیر ساخت شبکه‌ای در فضای سایبری (پدافند سایبری)

۷-۳.آینده‌پژوهی و سیاست‌گذاری انواع تهدیدات نرم در پدافند سایبری:

جهت تبیین آینده‌پژوهی و سیاست‌گذاری تهدیدات نرم در پدافند سایبری در سازمان‌های دانش‌بنیان باید به ساختارهای مختلف و زیر شاخص‌های گوناگونی توجه نمود. در ذیل به برخی از آنها اشاره می‌گردد:

❖ محصولات و خدمات ارائه شده توسط پیمانکاران در فضای سایبری (پدافند سایبری)
❖ تجهیزات امنیتی در سایت‌ها و سیستم‌ها در فضای سایبری (پدافند سایبری)
❖ روابط بین سیستم‌ها در برابر حملات و تهدیدات نرم در فضای سایبری (پدافند سایبری)
❖ اطمینان از کفایت قدرت پردازشی و حافظهٔ سیستم‌ها در فضای سایبری (پدافند سایبری)
❖ ایمن‌سازی سیستم‌های اطلاعاتی و دارایی‌ها در برابر تهدیدات نرم در فضای سایبری (پدافند سایبری) در سازمان‌های دانش‌بنیان
❖ امن‌سازی زیرساخت‌های ارتباطی و شبکه‌ای در فضای سایبری (پدافند سایبری)
❖ اصل انطباق و هم‌راستایی سیستم امنیتی مورد استفاده در فضای سایبری (پدافند سایبری)

۷-۴.آینده‌پژوهی و سیاست‌گذاری تهدیدات موجود (شناخته شده) در پدافند سایبری:

جهت تبیین آینده‌پژوهی و سیاست‌گذاری تهدیدات موجود (شناخته شده) در پدافند سایبری سازمان‌های دانش‌بنیان باید به ساختارهای مختلف و زیر شاخص‌های گوناگونی توجه نمود. در ذیل به برخی از آنها اشاره می‌گردد:

❖ توسعه زیرساخت‌های سیستمی در فضای سایبری (پدافند سایبری)
❖ تحلیل شبکه‌ای باتوجه‌به نوع استفاده در فضای سایبری (پدافند سایبری)
❖ استفاده از حفاظ‌های الکتریکی (ارتینگ و...) در فضای سایبری (پدافند سایبری) خصوصاً سایت‌های سازمان‌های دانش‌بنیان
❖ ایمن‌سازی مجازی در فضای سایبری (پدافند سایبری)
❖ تهدیدات رسانه‌ای در فضای سایبری (پدافند سایبری)
❖ افزایش قابلیت اطمینان در مراکز اطلاعاتی در فضای سایبری (پدافند سایبری)
❖ استفاده از مشاوران امنیت اطلاعات در فضای سایبری (پدافند سایبری)

۷-۵.آینده‌پژوهی و سیاست‌گذاری انواع تهدیدات ناشناخته (هوشمند) در پدافند سایبری:

جهت تبیین آینده‌پژوهی و سیاست‌گذاری تهدیدات ناشناخته (هوشمند) در پدافند سایبری سازمان‌های دانش‌بنیان باید به ساختارهای مختلف و زیر شاخص‌های گوناگونی توجه نمود. در ذیل به برخی از آنها اشاره می‌گردد:

❖ تکمیل ساخت‌های سیستمی و هوشمند در فضای سایبری (پدافند سایبری)
❖ آموزش مقابله با تهدیدات فرا شبکه‌ای در فضای سایبری (پدافند سایبری)
❖ قابلیت استفاده از نرم‌افزارهای ترکیبی در وب‌سایت‌ها
❖ ایمن‌سازی هوشمند ابزارها و امکانات در فضای سایبری (پدافند سایبری)

۷-۶.آینده‌پژوهی و سیاست‌گذاری انواع سطح‌بندی متغیرهای تحقیق :

❖ تعیین قابلیت تطبیق‌پذیری سطح‌بندی انواع تهدید در فضای سایبری
❖ تشخیص دامنه انواع در فضای سایبری (شناخت موضوع و بازیگران)
❖ افزایش قابلیت اطمینان در مراکز اطلاعاتی امن
❖ استفاده از قوانین، مقررات مدون و مشخص در برابر انواع تهدیدات نرم
❖ شناسایی ساختارها و الگوهای بومی در تهدیدات شناخته شده
❖ بهبود فرایندهای سازمانی و ساختار منسجم، یکپارچه اثر مطلوبی بر مدیریت سایر تهدیدات ناشناخته (هوشمند) در امنیت و پدافند سایبری سازمان‌های دانش‌بنیان داشته باشد.
❖ برنامه‌ریزی‌های امنیتی و اطلاعاتی در پروژه‌های امنیتی، اطلاعات باعث
❖ پیشگیری‌های فازی و غیرفازی، مقابله هوشمند،
❖ بهره‌گیری از سیستم‌های امنیتی خبره، انواع حملات روز صفر در این حوزه است. همچنین امکان بهره‌برداری از انواع حملات روز صفر در برابر آسیب‌پذیری‌های همگن، ناهمگن و رفع نواقص مربوطه می‌باشد.
❖ ارزیابی سطح‌بندی آسیب‌ها مستلزم به تشخیص زمان، زمان هشدار، زمان اثرگذاری، سرعت دگردیسی و زمان بازیابی (تهدید) است.

۸. مراجع

[1]. Ismailpour M., Bahrainizad, M., Qaidi, H.A. "Investigation of the impact of organizational approach dimensions on the success of new products with the

[16]. Stephan Kuehnel, Sebastian Hengstler, Simon Trang, “Should I really do that? Using quantile regression to examine the impact of sanctions on information security policy”, compliance behavior, Computers & Security29 June 2023, (In Persian).
[17]. Pourabrahimi, A. Safar Nejad. D., Kashif, H.R, “Islamic Republic of Iran's cyber defense strategies against psychological warfare threats”, National Security, 6(22), 119-146. 2016. , (In Persian).
[18]. The first square. P, “Estimating information security risks using intelligent methods”, Supervisor: Mohammad Ali Dostari. Ali Yazdian Master's Thesis of Information Technology, Shahid University. Faculty of Technology and Engineering, 2016, , (In Persian).
[19]. “Transformation document of the cyber defense base, Defense Organization of the Islamic Republic of Iran”, 2022, (In Persian).
[20]. Behbodi, M. R. “Evaluation of Information Security Management (ISMS) in Hormozgan University and presenting strategies for its improvement”, Master's Thesis, Hormozgan University, Faculty of Literature and Humanities, 2019, (In Persian).
[21]. Lutfi H.A. “Recognizing the threats and social harms of Tehran and the future perspective with emphasis on Shahran neighborhood” (district one of Panj region municipality). Student; cold Alireza, MA (Islamic Azad University, Science and Research Unit, Faculty of Humanities and Social Sciences, Social Sciences Research Department). 2015, (In Persian).
[22]. Al-Barzi, M. “Investigating security threats in cloud computing and providing a secure method for data storage”, Islamic Azad university. Science and Research Unit, Faculty of Management and Economics, Department of Information Technology Management. 2020, (In Persian).
[23]. Esmaili, A; Taghipour, R.; “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).
[24]. Mousavi. A. R. Sepehri. M., “Strategies to improve the capabilities of electronic and cyber warfare (cyberelectronics) of the armed forces against asymmetric threats”, Strategic Defense Studies Quarterly, Fall 2020, No. 81, (In Persian).
[25]. Mirzaei, A., “Strategies for improving information security management using interpretive structural modeling method (Case of Study: Organizational Cultural and Artistic Organization of Tehran) ”, Guided by Ahmad Reza Ghasemi; Simple kindness advice. Master's degree (Islamic Azad University, Science and Research Unit, Faculty of Management and Economics, Department of Information Resource Management). 2022. , (In Persian).
[26]. Alizadeh Soodmand, A.R., Fathi Hafeshjani, K., Shah Mansouri, A., Arab Sorkhi, A. “Structured analysis of safety indicators in cyber security and defense of knowledge-based organizations in IRAN”. Passive Defense, scientific-research journal Passive Defense, 15th year, number 1, spring 2024, (57 series): pp. 1-11, print shop: 2008-6949 | Electronic mail: 2980-8030, (In Persian).
[27]. Mickey Krause, K., Harold F. tipton T, “Management of information protection and security”, translated by Mohammad Hossein Abedi. - Tehran: Eizairan Institute, 2018.
[28]. Song, X, Shi, W, Tan, G, Maa. Y , “Multi-Level Tolerance Opinion Dynamics in Military Command and Control Networks”, Physica A: Statistical Mechanics and its applications, 2015, Vol.43, No . 3.
variables of customer knowledge management and market knowledge" (a study on knowledge-based companies in the Persian Gulf Science and Technology Park). Bushehr. New Marketing Research, 2015 , 6(3), 87-108. (In Persian). doi: 10.22108/nmrj.2016.21074
[2]. Researcher . R & D, United Nations performance research and research group”, United Nations affiliated offices, annual performance report of various United Nations working groups. United Nations International Publications, 2023
[3]. Khalafkhani M, “ information and communication opportunities for democratization in cyber (virtual) space”. Guided by Abdul Ali Qavam; Consulting Ahmed Sae, Mohammad Amjad. Ph.D. (Islamic Azad University, Department of Sciences and Research, Faculty of Law and Political Sciences, Department of Political Sciences). 2015, (In Persian).
[4]. Reports of the China Cyber Security Institute, “ China National Cyber Security Coordination Office Center in 2024” (Reports of the China Cyber Security and Defense Organization, 2023).
[5]. Reports of cyber attacks on security and intelligence centers in India”. India Government Reports, Office of the National Cyber Security Coordinator, India, 2024.
[6]. International Telecommunication Union "ITU, belonging to the United Nations”. 2024. https://www.itu.int/en/Pages/default.aspx
[7]. Cyber Security Systems Reports, “United Nations Office of Technology Research in 2023 Various reports on cyber attacks on security and intelligence centers in the world”. United Nations International Publications, 2024
[8]. Price Water. HouseCoopers, “PricewaterhouseCoopers PWC Cybercrime Report”, 2024
https://www.pwc.com/gx/en/research-insights.html
[9]. Edyta Karolina Szczepaniuk, Hubert Szczepaniuk, Tomasz Rokicki, Bogdan Klepacki. “Information security assessment in public administration”, Computers & SecurityMarch. 2020
[10]. Amazon Cyber Security, ” Amazon Cyber Security Center Report”, 2024, https://aws.amazon.com/security
[11]. Javaheri, H. R. Shaghaghi, A. Abbasi. M, “investigation of new threats of cyberspace based on fileless malware. Information Sciences and Technologies, 2022, 1(1), 81-108. (In Persian).
[12]. Agronomist V.R, “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). 2017, (In Persian).
[13]. Nasirirad. G. “Comparison of the amount and manner in which users use 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 Afshana Mozafari.- Master's degree (Islamic Azad University, Department of Sciences and Research, Department of Social Communication Sciences). 2016, (In Persian).
[14]. Ali Kavak, 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, (In Persian).
[15]. Pooribrahimi, A. “Information Security Architecture”, Islamic Azad University, Electronic Department, Islamic Azad University Publications, 2013, (In Persian).

[29] Elena Vlahu, Khin Than Win, Gjorgievska. " Information Security Governance Challenges and Critical Success Factors: Systematic Review". Computers & Security In press, journal pre-proofAvailable online 2021 September.
[30]. Mari Karjalainen, Mikko Siponen, Suprateek Sarker, "Toward a stage theory of the development of employees' information security behavior", Computers & Security. 2020 June.
[31]. Damjan Fujs, Simon Vrhovec, Damjan Vavpotič, "Balancing software and training requirements for information security", Computers & Security2 September 2023
[32]. Sajadi, and; Azar, D; "Improving the ability of the Islamic Republic of Iran's army to deal with the US army's cyber operations", Magazine: Military Sciences and Techniques Spring. ISC scientific-research number 51. 22 pages - from 5 to 26, 2020, (In Persian).
[33]. Lloyd's Register Research Foundation, "Lloyd's Register Foundation Research Center Report", 2023. https://www.lrfoundation.org.uk/en/about-us/
[34]. Ranjbar, M. H, Mardani Shahrbabak. M, Piraysh. A. "presenting a model for evaluating the physical protection of critical facilities for passive defense against physical and sabotage threats", Modern Defense Sciences and Technologies, 8(4), 387-398. 2017, (In Persian).
[35]. Hafez Nia M. R. "An introduction to the research method in humanities", organization for the study and compilation of humanities books of universities (Samt), 2016, (In Persian).
[36]. Khaki. R, "Research method in management", Tehran: Fuzhan, 2019, (In Persian).