Supreme National Defense University Quarterly Journal of National Security
https://ns.sndu.ac.ir E-ISSN: 2980-8251
Vol. 15, No. 4, Issue. 58, Winter 2026 **Received:** 2024/12/03 **Accepted:** 2025/09/02
Research paper

Cognitive Vulnerability Model with Cyber Defense Approach

Mohammad Mahdi Sheikholislam
Master of Computer Engineering, Cyber Researcher, Tehran, Iran
Email: sheikholislam@alumni.kntu.ac.ir
Mohammad Ali Sheikholislam
PhD student in Science and Technology Policy, Iran University of Science and Technology, Tehran, Iran (Corresponding Author)
Email: m_sheikholislam@pgre.iust.ac.ir

Abstract
Macro-security trends indicate that the nature of wars will undergo major changes in the coming years and decades. In 2020, NATO designated five war domains for members of this military alliance, and recently a new domain was added to these domains, called "cognitive warfare." On the other hand, with the advancement of the arms industry and the increasing cost of military confrontation for various countries, countries' interests in using cyberattacks, social influence operations, and cognitive warfare have increased. The present study is of an applied and developmental nature in terms of purpose, descriptive and review in terms of nature, and mixed research (quantitative and qualitative) in terms of data type. Using the content analysis method, a cognitive vulnerability model with a cyber defense approach has been presented. In order to examine the validity of the presented model, in the first step, the analyzed themes were examined, and after necessary amendments, the expert feedback method was used. The results and initial framework were presented to a total of 16 experts and professors in this field. To examine the reliability of the questionnaire, Cronbach's alpha was calculated using SPSS software, and the number 0.842 indicates the appropriate reliability of the questionnaire. Also, considering the use of the Likert scale to answer the questions and converting it into a quantitative score, the result and average score of the experts' responses to the general questions section was 4.14 out of 5, which indicates the appropriate validity of the presented model. The final model presented in the field of cybercognitive vulnerability includes 7 main dimensions and 43 components and is presented in 2 solar and layered forms at the end of the research.

Keywords: Cognitive Warfare, Cyber Defense, Cognitive Vulnerability, Hybrid Warfare

فصلنامه امنیت ملی

سال پانزدهم، شماره چهارم (پیاپی ۵۸)، زمستان ۱۴۰۴، صص. ۱۳۷-۱۸۰
تاریخ دریافت: ۱۴۰۳/۰۹/۱۳ ـ تاریخ پذیرش: ۱۴۰۴/۰۶/۱۱

مقاله پژوهشی

چهارچوب آسیب‌پذیری سایبر شناختی

محمدمهدی شیخ‌الاسلام
دانش‌آموخته کارشناسی ارشد مهندسی کامپیوتر، پژوهشگر حوزه سایبر
Email: sheikholislam@alumni.kntu.ac.ir

محمدعلی شیخ‌الاسلام
دانشجوی دکتری سیاست‌گذاری علم و فناوری، دانشگاه علم و صنعت ایران (نویسنده مسئول)
Email: m_sheikholislam@pgre.iust.ac.ir

چکیده

روندهای امنیتی کلان نشان می‌دهد که ماهیت جنگ‌ها طی سال‌ها و دهه‌های آینده تغییرات عمده‌ای را به خود خواهد دید. ناتو طی سال ۲۰۲۰ پنج حوزهٔ جنگی را برای اعضای این ائتلاف نظامی تعیین نمود و اخیراً حوزه جدیدی نیز به این حوزه‌ها اضافه‌شده که «جنگ شناختی» نام دارد. از طرفی با پیشرفت صنایع تسلیحاتی و پُرهزینه شدن رویارویی نظامی برای کشورهای مختلف، علایق کشورها به استفاده از حملات سایبری و عملیات تأثیرگذاری اجتماعی و جنگ شناختی، افزایش یافت. پژوهش حاضر ازنظر هدف، از نوع کاربردی- توسعه‌ای، ازنظر ماهیت، از نوع توصیفی- مروری و ازنظر نوع داده‌ها، تحقیق آمیخته (کمی- کیفی) است. با استفاده از روش تحلیل مضمون، چهارچوب آسیب‌پذیری سایبر شناختی ارائه گردیده است. به‌منظور بررسی اعتبار چهارچوب ارائه‌شده در قدم اول ابتدا به بررسی مضامین تحلیل‌شده پرداخته و پس از اصلاحات لازم از روش بازخورد خبرگان استفاده شد. نتایج و چهارچوب اولیه درمجموع به ۱۶ نفر از خبرگان و اساتید این حوزه ارائه گردید. جهت بررسی پایایی پرسش‌نامه با استفاده از نرم‌افزار SPSS آلفای کرونباخ محاسبه گردید که عدد ۰/۸۴۲ بیانگر پایایی مناسب پرسش‌نامه مذکور است. همچنین با توجه به استفاده از طیف لیکرت برای پاسخ سؤالات و تبدیل آن به امتیاز کمی، نتیجه و میانگین امتیاز پاسخ خبرگان به بخش سؤالات عمومی عدد ۴/۱۴ از ۵ بوده است که حاکی از اعتبار مناسب چهارچوب ارائه‌شده است. چهارچوب نهایی ارائه‌شده در حوزه آسیب‌پذیری سایبر شناختی شامل ۷ بُعد اصلی و ۴۳ مؤلفه است که به ۲ صورت خورشیدی و لایه‌ای در انتهای پژوهش ارائه گردیده است.

کلیدواژه‌ها: جنگ شناختی، دفاع سایبری، آسیب‌پذیری سایبر شناختی، جنگ ترکیبی (هیبریدی)

https://ns.sndu.ac.ir/ E-ISSN: 2980-8251

مقدمه

روندهای دفاعی امنیتی کلان نشان می‌دهد که ماهیت جنگ‌ها طی سال‌ها و دهه‌های آینده تغییرات عمده‌ای را به خود خواهند دید. ائتلاف ناتو طی سال ۲۰۲۰ پنج عرصه نبرد را برای اعضای این ائتلاف نظامی مشخص نمود که به ترتیب عبارت بودند از زمین، هوا، دریا، فضا و عرصه سایبری، اخیراً عرصه جدیدی نیز به این عرصه‌ها اضافه گردید که عرصه «شناختی» است. از جهتی با پیشرفت صنایع تسلیحاتی و هزینه‌بر بودن رویارویی نظامی برای کشورهای مختلف، علایق کشورها به استفاده از حملات سایبری و عملیات تأثیرگذاری اجتماعی و جنگ شناختی، افزایش‌یافته است. به‌عنوان‌مثال پس از انتخابات ۲۰۱۶ آمریکا و نبرد ترکیبی روسیه علیه آن در عرصه‌های شناختی (تأثیرگذاری مستقیم بر افکار عمومی آمریکا قبل و بعد از انتخابات)، نبرد سایبری (نفوذ و هک زیرساخت‌های انتخاباتی به همراه کمپین نامزدها) و نبرد سیاسی (ارتباط‌گیری مستقیم با سران کمپین انتخاباتی ترامپ)، این مسئله به افواه عمومی و رسانه‌ها درز پیدا کرد و داده‌های موجود از این حمله، توسط سرویس‌های جاسوسی آمریکایی در اختیار رسانه‌ها قرار گرفت.

حوزه امنیت سایبری به همان اندازه که با یکپارچگی شبکه کامپیوتری ارتباط دارد، با حوزه انسانی نیز ارتباط دارد. بااین‌حال، درحالی‌که فناوری شبکه‌های کامپیوتری به‌طور منظم به‌سرعت تغییر می‌نماید، مکانیسم‌های یادگیری و تصمیم‌گیری انسان تغییر نمی‌نماید. در این صورت، تحقیقات متمرکز بر علوم شناختی ممکن است قابلیت‌های موفقیت‌آمیز موردنیاز را برای امنیت طولانی‌مدت شبکه و بازگشت سرمایه بیشتری نسبت به تلاش برای تعقیب جدیدترین آسیب‌پذیری‌های نرم‌افزار فراهم نماید. علوم شناختی و به‌ویژه مدل‌سازی شناختی نوید بزرگی را برای حوزه امنیت سایبری نشان می‌دهد (وکسلر[1] و همکاران، ۲۰۱۸).

از طرفی نبردهای پیشرفته قرن بیست و یکم نه‌تنها در لایه‌ها و ابعاد گوناگون کیفی و کمی نسبت به عرصه‌های سنتی نبرد ارتقاءیافته‌اند، بلکه حیطه‌ها و دامنه‌های جدیدی را نیز به وجود آورده‌اند. به عبارت ساده‌تر نبرد جدید صرفاً در عرصه‌های سنتی گذشته نبرد

1. Veksler

همچون هوا، دریا، زمین و فضا به وقوع نخواهد پیوست، بلکه عرصه‌ها و محیط‌های درگیری و نزاع به حوزه‌های متنوع دیگری ازجمله فضای سایبری با ابعاد اطلاعاتی، شناختی و فیزیکی کشانیده شده‌اند. جدید بودن عرصه‌های مورداشاره، به‌نوبه خود بیانگر ضرورت توجه و ورود هوشمندانه و مدبرانه به این عرصه است (صحنه پنجم نبرد). در نبردهای جدید به سبب دگرگونی در محیط راهبردی جهانی، علاوه بر زیرساخت حداقل در دو محیط جدید نبرد نقشی تعیین‌کننده و سرنوشت‌ساز دارند. نبرد در محیط اطلاعاتی و نبرد در محیط شناختی، هم‌زمان بر حرکت از محیط اطلاعاتی به محیط شناختی بر درجه راهبردی بودن صحنه نبرد افزوده می‌گردد. ضمن آنکه روند تکامل شیوه‌های نبرد در هر یک از این محیط‌ها نیز نشان می‌دهد که نرخ و سرعت تکامل نبردها بر مبنای راهبردی بودن آن‌ها تعریف می‌گردد؛ اما درمجموع شکی نیست که عرصه‌های نبرد سایبری، اطلاعاتی و شناختی به‌واسطه اثرگذاری مستقیم بر کارکردهای انسانی به‌مراتب از عرصه‌های نبرد فیزیکی راهبردی‌تر محسوب می‌گردند. نبرد شناختی عمدتاً به اطلاعات معنایی و بر محیط تعقلی انسان توجه دارد. بنابراین عناصر تشکیل‌دهنده صحنه نبردهای جدید سایبری را عناصری چون داده‌ها، خطوط ارتباطی، فضای تبادل اطلاعات یا داده، منابع اطلاعات و ... تشکیل می‌دهند و صحنه نبرد شناختی از عناصری چون دانش، آگاهی، فهم، درک، باور، تفکر، فرایندهای تصمیم‌گیری و شعور تشکیل گردیده است. باوجود پیشرفت‌های چشمگیر در حوزه امنیت سایبری و توسعه فناوری‌های حفاظتی، همچنان شاهد وقوع حملات سایبری موفقیت‌آمیز هستیم. یکی از دلایل اصلی این امر، نادیده گرفتن نقش عامل انسانی و آسیب‌پذیری‌های سایبر شناختی در فرایندهای امنیتی است. درواقع، بسیاری از حملات سایبری موفق با بهره‌برداری از ضعف‌های شناختی کاربران و تصمیم‌گیرندگان صورت می‌گیرد.

آسیب‌پذیری شناختی در حوزه سایبر (آسیب‌پذیری سایبر شناختی)، به‌عنوان نقاط ضعف در فرایندهای شناختی انسان‌ها تعریف می‌شود که مهاجمان سایبری می‌توانند از آن‌ها برای نفوذ به سیستم‌ها و دستیابی به اهداف خود استفاده کنند. این آسیب‌پذیری‌ها شامل طیف گسترده‌ای از عوامل شناختی، روان‌شناختی و اجتماعی می‌شوند که بر تصمیم‌گیری، قضاوت

و رفتار کاربران تأثیر می‌گذارند. این مسئله ابعاد مختلف و قابل بررسی اعم از تعریف مبهم و چندوجهی، تنوع آسیب‌پذیری‌ها، تأثیر عوامل فردی و اجتماعی، کمبود مدل‌های جامع و پیامدهای جدی دارد.

تعریف مبهم و چندوجهی: آسیب‌پذیری شناختی یک مفهوم پیچیده و چندوجهی است که هنوز تعریف دقیق و جامعی برای آن ارائه نشده است.

تنوع آسیب‌پذیری‌های شناختی: این آسیب‌پذیری‌ها شامل طیف گسترده‌ای از عوامل مانند خطاهای انسانی، سوگیری‌های شناختی، مهندسی اجتماعی، فیشینگ، اعتماد بیش‌ازحد، ترس از دست دادن و بسیاری موارد دیگر می‌شوند.

تأثیر عوامل فردی و اجتماعی: عوامل فردی مانند دانش، تجربه، شخصیت و عوامل اجتماعی مانند فرهنگ سازمانی، فشارهای اجتماعی و روابط بین فردی بر آسیب‌پذیری‌های شناختی تأثیرگذار هستند.

کمبود مدل‌های جامع: مدل‌های موجود برای ارزیابی و مدیریت ریسک‌های سایبری اغلب به اندازه کافی به ابعاد شناختی مسئله نپرداخته‌اند.

پیامدهای جدی: آسیب‌پذیری‌های شناختی می‌توانند به عواقب جدی مانند افشای اطلاعات حساس، اختلال در عملیات، خسارات مالی و از دست رفتن اعتماد مشتریان منجر شوند؛ بنابراین با عنایت به اینکه راهبرد دفاعی جمهوری اسلامی ایران، هوشمندی راهبردی و جلوگیری از غافلگیری است و هنوز در این زمینه چهارچوب مفهومی خاصی وجود ندارد، این پژوهش درصدد است چهارچوب آسیب‌پذیری سایبر شناختی را ارائه نماید. بنا به موارد فوق مسئله اصلی این پژوهش اکتشاف اجزا و عواملی است که ذهن عامل انسانی مسئول و درگیر با سیستم‌های دفاع سایبری را درگیر می‌نماید.

با بررسی ادبیات این حوزه، خلأ چهارچوب مفهومی، احساس می‌گردد که این پژوهش قصد دارد در راستای ارتقای سطح نگرش و شناسایی فراگیر نسبت به آسیب‌پذیری سایبر شناختی بپردازد. همچنین بررسی‌ها، نیازسنجی‌ها و همچنین پیش‌بینی محقق، نشان‌دهنده موارد ذیل در اهمیت انجام این پژوهش است:

- ارتقای سطح نگرش و شناسایی فراگیر نسبت به آسیب‌پذیری سایبر شناختی؛
- توسعه دانش بومی این حوزه به‌منظور ارتقای وضعیت تأمین امنیت سایبر شناختی؛
- شناخت منطقی اقدامات تهدیدآمیز و آسیب‌زای سایبر شناختی جهت مواجهه فعال.

بررسی‌های اولیه نشان می‌دهد پیامدهای عدم انجام این پژوهش به شرح زیر هستند:

- ضعف در پیش‌بینی و شناخت تهدیدات و آسیب‌پذیری سایبر شناختی؛
- کاهش توانمندی در شناسایی و پاسخ‌گویی به تهدیدات و آسیب‌پذیری سایبر شناختی و تحمیل هزینه‌های زیاد؛
- افزایش میزان خسارات اقدامات تهدیدآمیز سایبر شناختی در صورت نبود چهارچوب مفهومی مقبول برای مواجهه فعال.

نظر به اینکه اجرای این تحقیق ارائه چهارچوب مفهومی برای شناخت آسیب‌پذیری سایبر شناختی است و نتایج عملیاتی آن قدرت تصمیم‌سازی تصمیم‌سازان حوزه دفاع سایبری را افزایش می‌دهد، جنبه کاربردی دارد و با توجه به گسترش دانش در این حوزه، توسعه‌ای است؛ بنابراین تحقیق حاضر با توجه به هدف، از نوع توسعه‌ای-کاربردی است.

از نظر داده، این پژوهش ترکیبی (کمی و کیفی) است. اکثر استنتاج‌هایی که در این پژوهش انجام می‌گیرد براساس داده‌های کمی در پرسش‌نامه‌ها است. البته داده‌های کیفی نظیر مطالعات کتابخانه‌ای، مصاحبه‌های انجام‌شده و نظرات خبرگی نیز در احصای الگو نقش بسیار مؤثری خواهد داشت.

جدول ۱: تحقیق از منظرهای مختلف

هدف	ماهیت	داده‌ها	مکان و زمان اجرا	فرایند اجرا
کاربردی و توسعه‌ای	توصیفی	ترکیبی (کمی و کیفی)	کتابخانه‌ای (مروری)	کیفی (تحلیل مضمون- نظرات خبرگی، بازخورد مشارکت‌کنندگان از طریق برگزاری جلسات تخصصی)

۱. مبانی نظری

با افزایش وابستگی به اینترنت و فضای مجازی، تهدیدات سایبری نیز به‌طور فزاینده‌ای پیچیده و خطرناک‌تر می‌شوند. حملات سایبری می‌توانند طیف وسیعی از پیامدهای منفی ازجمله سرقت اطلاعات شخصی، اختلال در عملیات تجاری و حتی خسارات مالی هنگفت را به دنبال داشته باشند. در این راستا، درک عوامل روان‌شناختی که افراد را در برابر این حملات آسیب‌پذیر می‌کنند، برای توسعه راهبردهای مؤثر دفاع سایبری از اهمیت بالایی برخوردار است.

آسیب‌پذیری سایبر شناختی به عوامل روانی و شناختی اشاره دارد که افراد را در برابر حملات سایبری و اختلالات روانی آسیب‌پذیر می‌کند. حملات سایبری مهندسی اجتماعی از ضعف‌ها در عملکردهای شناختی انسان بهره‌برداری می‌کنند و نیاز به درک عمیق‌تری از این آسیب‌پذیری‌ها را ایجاد می‌کنند (مونتانیز رودریگز[1] و همکاران، ۲۰۲۰). مدل‌های آسیب‌پذیری شناختی پیشنهاد می‌کنند که برخی از سوگیری‌های شناختی می‌توانند منجر به ایجاد مشکلات روانی شوند، به‌ویژه زمانی که افراد با رویدادهای استرس‌زا روبه‌رو می‌شوند (ریسکین و آلی[2]، ۲۰۰۶). این آسیب‌پذیری‌ها می‌توانند از طریق طراحی‌های تحقیقی و روش‌های مختلف مورد مطالعه قرار گیرند، ازجمله بررسی سوگیری‌های اسکیما در پردازش اطلاعات و عوامل رشد (ریسکین و آلی، ۲۰۰۶). محققان پیشنهاد داده‌اند که چهارچوب عملکردهای شناختی انسانی را گسترش دهند تا بهتر بتوان با حملات سایبری مهندسی اجتماعی مواجهه کرد و توسعه یک زیررشته جدید به نام روان‌شناسی شناختی امنیت سایبری را الهام بخشند (مونتانیز رودریگز و همکاران، ۲۰۲۰).

آسیب‌پذیری سایبر شناختی به آسیب‌پذیری افراد در برابر تهدیدات سایبری به دلیل سوگیری‌های شناختی و عوامل روان‌شناختی موجود اشاره دارد. این مفهوم به‌طور فزاینده‌ای مهم است؛ زیرا مجرمان سایبری از رفتار انسانی بهره‌برداری می‌کنند و نه‌فقط به نقاط ضعف فنی تکیه می‌کنند. تحقیقات نشان می‌دهد که بیش از ۹۹ درصد از حملات سایبری از

1. Montañez, R
2. Riskind, Alloy

ویژگی‌های انسانی، مانند محدودیت‌های شناختی و تمایلات روان‌شناختی، برای دستیابی به اهداف خود استفاده می‌کنند (گالوا[1]، ۲۰۲۳). درک این آسیب‌پذیری‌ها برای توسعه راهبردهای مؤثر امنیت سایبری که عوامل انسانی را در نظر بگیرد، ضروری است.

حملات سایبر شناختی از نقاط ضعف روانی با القای رفتارها از طریق فریب و دست‌کاری بهره‌برداری می‌کنند، همان‌طور که در درگیری‌های مختلف ازجمله جنگ روسیه و اوکراین دیده می‌شود (کیم[2]، ۲۰۲۳) تعصبات شناختی می‌تواند تیم‌های امنیت سایبری را گمراه کند و باعث شود آن‌ها بر تهدیدات کمتر مرتبط تمرکز کنند و خطرات قابل‌توجهی مانند بدافزارهای مداوم و حملاتی فیشینگ را نادیده بگیرند (دارلی[3]، ۲۰۲۳).

فرایندهای شناختی انسانی جزء جدایی‌ناپذیری از «سیستم‌های فیزیکی انسان و سایبری»[4] هستند و آن‌ها را هدف حملات شناختی قرار می‌دهند که می‌توانند این سیستم‌ها را مختل کنند. تعصبات شناختی می‌تواند راهبردهای امنیت سایبری را از بین ببرد و منجر به تخصیص نادرست منابع و ارزیابی‌های بی‌اثر تهدید شود (دارلی، ۲۰۲۳).

یکی از موضوعات مهم و قابل‌تأمل، نقش سوگیری‌های شناختی در فرایندهای تصمیم‌گیری در حوادث سایبری است. سوگیری‌های شناختی، مانند اعتمادبه‌نفس بیش‌ازحد می‌تواند باعث شود که کاربران خطرات را دست‌کم بگیرند یا توانایی خود در شناسایی تهدیدات را بیش‌ازحد تخمین بزنند (سایر و هانکاک[5]، ۲۰۱۸). به‌عنوان مثال، کاربران ممکن است به سیستم‌های خودکار بیش‌ازحد اعتماد کنند که باعث سستی و تنبلی در شیوه‌های امنیتی می‌شود، یا ممکن است به سیستم‌هایی که می‌توانند امنیت آن‌ها را بهبود بخشند، بی‌اعتماد شوند (سایر و هانکاک، ۲۰۱۸). این ناهم‌ترازی در اعتماد می‌تواند منجر به عملکرد نامطلوب و افزایش آسیب‌پذیری در برابر تهدیدات سایبری شود (نوبلز[6]، ۲۰۲۳).

1. Galvão
2. Kim
3. Darley
4. Human Cyber-Physical System (HCPS)
5. Sawyer, B. D. and Hancock, P. A.
6. Nobles

ادغام هوش مصنوعی در HCPS نیازمند یک پارادایم امنیتی جدید به نام «امنیت شناختی» برای محافظت در برابر حملات شناختی با پرداختن به آسیب‌پذیری‌های شناختی انسان است (هانگ و ژو[1]، ۲۰۲۳).

درک عمومی و تعامل با خطرات سایبری تحت تأثیر آسیب‌پذیری‌های شناختی قرار می‌گیرد و بر پاسخ آن‌ها به حملاتی سایبری تأثیر می‌گذارد (بادا و نرس[2]، ۲۰۲۰) توسعه یک مدل پردازش مبتنی بر روان‌شناسی برای حملاتی‌های شناختی سایبری می‌تواند به درک و کاهش این تهدیدها کمک کند (کیم، ۲۰۲۳). نظریه پردازش دوگانه نشان می‌دهد که رویکردهای تصمیم‌گیری می‌توانند در تشخیص آسیب‌پذیری‌های نرم‌افزاری تأثیر بگذارند و نیاز به راهبردهای عمدی و محاسباتی در کدگذاری امن را برجسته می‌کند (ایووری[3] و همکاران، ۲۰۲۴).

حملات مهندسی اجتماعی نمونه‌ای از چگونگی بهره‌برداری مهاجمان سایبری از آسیب‌پذیری‌های شناختی هستند. این حملات فرایندهای روان‌شناختی را به‌گونه‌ای دست‌کاری می‌کنند که افراد را به افشای اطلاعات حساس یا انجام اقداماتی که امنیت را به خطر می‌اندازد، فریب دهند (مونتانز و همکاران، ۲۰۲۰). تحقیقات نشان داده است که درک جنبه‌های شناختی که باعث می‌شود افراد در برابر چنین حملاتی آسیب‌پذیر شوند، برای توسعه تدابیر دفاعی بسیار مهم است (مونتانز و همکاران، ۲۰۲۰). به‌عنوان مثال، برنامه‌های آموزشی که اصول روان‌شناسی را در نظر می‌گیرند، می‌توانند آگاهی کاربران را از این تاکتیک‌ها افزایش دهند و مقاومت آن‌ها را در برابر دست‌کاری بهبود بخشند (تیلور–جکسون[4] و همکاران، ۲۰۲۰).

علاوه بر این، تعصبات شناختی به‌طور قابل‌توجهی بر تیم‌های امنیت سایبری تأثیر می‌گذارد و باعث می‌شود تا تهدیدات را سوء قضاوت کنند. این قضاوت غلط می‌تواند توجه را از فوری‌ترین خطرات منحرف کند تا بر تهدیدات کمتر مرتبط تمرکز کند. درک تعصبات

1. Huang, L. & Zhu, Q.
2. Bada & Nurse
3. Ivory
4. Taylor-Jackson, J.

شناختی برای متخصصان امنیت سایبری بسیار مهم است. با شناخت این تعصبات، تیم‌ها می‌توانند فرایندهای تصمیم‌گیری خود را بهبود بخشند و راهبردهای خود را بهتر با تهدیدات واقعی هماهنگ کنند. گنجاندن تجزیه‌وتحلیل روان‌شناختی در امنیت سایبری می‌تواند به تیم‌ها کمک کند تا اثرات تعصبات شناختی را شناسایی و کاهش دهند و در نهایت منجر به راهبردهای امنیتی مؤثرتری شود (دارلی، ۲۰۲۳).

تقاطعی که بین روان‌شناسی شناختی و امنیت سایبری وجود دارد، اهمیت توجه به عوامل انسانی در آموزش و تربیت امنیتی را نیز برجسته می‌کند. آموزش‌های سنتی امنیت سایبری معمولاً اجزای روانی تأثیرگذار بر رفتار کاربران را نادیده می‌گیرد (تیلور–جکسون و همکاران، ۲۰۲۰). با ادغام نظریه‌های روان‌شناسی در برنامه‌های آموزشی امنیت سایبری، سازمان‌ها می‌توانند درک جامع‌تری از ابعاد انسانی تهدیدات سایبری ایجاد کنند و بدین ترتیب وضعیت امنیتی کلی را بهبود بخشند (سینگ[1]، ۲۰۲۴). ادغام یادگیری ماشین با راهبردهای دفاعی شناختی می‌تواند به‌طور قابل‌توجهی پیش‌بینی و پیشگیری از تهدیدات سایبری را افزایش دهد و به نرخ دقت بالایی در شناسایی حملاتی بالقوه دست یابد (دودرشینی[2] و همکاران، ۲۰۲۳).

علاوه بر این، روش‌های آموزش شناختی مانند آموزش حافظه کاری نشان داده‌اند که می‌توانند خشونت‌طلبی و رفتارهای ریسک‌پذیری را کاهش دهند که این موارد برای کاهش آسیب‌پذیری‌های سایبری شناختی حیاتی هستند (موستافا[3] و همکاران، ۲۰۲۱). این روش‌ها می‌توانند به افراد کمک کنند تا منابع شناختی خود را بهتر مدیریت کرده و در شرایط استرس‌زا مانند یک حادثه سایبری، تصمیم‌گیری بهتری داشته باشند (موستافا و همکاران، ۲۰۲۱).

از طرفی آسیب‌پذیری‌های نرم‌افزاری را می‌توان به‌عنوان نقاط کور شناختی مشاهده کرد که این نقاط مناطقی هستند که توسعه‌دهندگان به دلیل سبک پردازش ذهنی خود آن‌ها را نادیده می‌گیرند. این مفهوم توسط نظریه پردازش دوگانه که بین تفکر شهودی (سیستم ۱) و

1. Singh
2. Devadarshini
3. Moustafa, A.

تحلیلی (سیستم ۲) تمایز قائل می‌شود، پشتیبانی می‌شود. شواهد تجربی نشان می‌دهد که نقاط کور در کد، شناسایی آسیب‌پذیری‌ها را برای توسعه‌دهندگان سخت‌تر می‌کند و یافته‌های قبلی را تأیید می‌کند که تخصص فنی به‌طور قابل‌توجهی تشخیص آسیب‌پذیری را بهبود نمی‌بخشد (آیوری و همکاران، ۲۰۲۴).

دفاع سایبری جزء حیاتی امنیت سایبری مدرن است و تمرکز بر حفاظت از سیستم‌ها و شبکه‌ها در برابر اقدامات دشمن است. این موضوع شامل طیف وسیعی از راهبردها و فناوری‌ها با هدف اطمینان از تضمین اطلاعات و حفاظت از زیرساخت‌های حیاتی است. ادغام هوش مصنوعی (AI) قابلیت‌های دفاع سایبری را بیشتر افزایش داده و امکان پاسخ‌های فعال‌تر و مؤثرتر به تهدیدات سایبری را فراهم می‌کند. دفاع سایبری به اقدامات حفاظتی انجام‌شده برای مقابله با تهدیدات سایبری، اطمینان از یکپارچگی و در دسترس بودن سیستم‌های اطلاعاتی اطلاعات اشاره دارد (گالینک[1]، ۲۰۲۳)؛ (احمد و همکاران[2]، ۲۰۲۳).

امروزه، سیستم‌های مبتنی بر هوش مصنوعی با تجزیه‌وتحلیل مجموعه داده‌های بزرگ برای شناسایی الگوها و پاسخ به فعالیت‌های مخرب، دفاع سایبری و زمان تشخیص و پاسخ را به‌طور قابل‌توجهی بهبود می‌بخشند (رنگرز[3]، ۲۰۲۴).

چشم‌انداز تهدیدات در حال تحول است و پیچیدگی حملات سایبری در حال افزایش است و نیاز به سازگاری مداوم راهبردهای دفاعی است (سوگومارا [4] و همکاران، ۲۰۲۳)

درحالی‌که راهبردهای دفاع سایبری در حال پیشرفت است، پتانسیل دشمنان برای بهره‌برداری از فناوری‌های مشابه یک چالش قابل‌توجهی ایجاد می‌کند و نیاز به نوآوری مداوم و همکاری در این زمینه را برجسته می‌کند. از طرفی افزایش تهدیدات ترکیبی تلاش‌های دفاع سایبری جمعی را پیچیده می‌کند و سؤالاتی را در مورد کاربرد مقررات کمک متقابل موجود در رساله‌های بین‌المللی مطرح می‌کند (نبیریدز[5]، ۲۰۲۳). در نتیجه، پرداختن

1. Galinec
2. Ahmed
3. Rangrez
4. Sugumaran
5. Nebieridze

به آسیب‌پذیری سایبری شناختی نیازمند یک رویکرد چندوجهی است که بینش‌هایی از روان‌شناسی، علم شناختی و شیوه‌های امنیت سایبری را ترکیب می‌کند. با شناسایی زیرساخت‌های روانی رفتار کاربران، سازمان‌ها می‌توانند راهبردهای مؤثرتری برای کاهش ریسک‌های مربوط به عوامل انسانی در امنیت سایبری توسعه دهند.

هدف اصلی از انجام این تحقیق «ارائه چهارچوب آسیب‌پذیری سایبر شناختی» است. به شکلی که با ارائه آن بتوان روند شناسایی این تهدیدها را در قالبی با قدرت شناسایی بیشتر و خطای کمتر مورد نظر قرارداد. بر این اساس، اهداف فرعی ذیل آن به‌صورت «شناخت ابعاد آسیب‌پذیری سایبر شناختی» و «شناخت مؤلفه‌های آسیب‌پذیری سایبر شناختی» در نظر گرفته شده است.

مهم‌ترین واصلی‌ترین سؤال پژوهش این است که چهارچوب مفهومی آسیب‌پذیری سایبر شناختی چیست؟ همچنین سؤالات فرعی این پژوهش عبارتند از: چهارچوب مفهومی آسیب‌پذیری سایبر شناختی دارای چه ابعاد و چه مؤلفه‌هایی است؟

۲. پیشینهٔ پژوهش

با بررسی‌های صورت گرفته در مجلات، پایگاه‌های اطلاعات علمی و اسنادی داخلی و خارجی، مشخص گردید از میان پژوهش‌های انجام‌شده هیچ‌کدام به‌صورت مستقیم در خصوص ارائه چهارچوب آسیب‌پذیری سایبر شناختی نبوده و پژوهشی‌هایی که تا حدودی مرتبط با موضوع این تحقیق هستند به شرح زیر است:

صادقی و نادری (۱۳۹۵) در تحقیقی با موضوع تحلیل ابعاد امنیت دولت در ایران قرن ۲۱، در فصلنامه دولت‌پژوهی، با اشاره به محورهای اساسی مکتب کپنهاگ (مطرح‌شدن امنیت به‌عنوان مفهومی بینا ذهنی، دولت به‌عنوان مرجع امنیت، موسع بودن امنیت و ابعاد پنج‌گانه آن) امنیت ملی را مرکز ثقل امنیت قلمداد نموده‌اند.

کورکی نژاد قرایی (۱۳۹۴) در پایان‌نامه کارشناسی ارشد خود در دانشگاه تهران با عنوان تروریسم سایبری (دهشت افکنی در فضای سایبر) و راهکارهای افزایش امنیت سایبر در

ایران با تأکید بر عملکرد دولت آمریکا با بررسی تأثیرات تهدیدهای سایبری بر روی فرد و بخش‌های دولتی و خصوصی مؤکداً بر قانون ارتقای آموزش امنیت سایبری در سطوح ملی و انجام انواع مختلف پژوهش‌های حقوقی در این زمینه تأکید و اصرار داشته است.

بچاری لفته و نجفی شوشتری (۱۳۹۷) در مطالعه‌ای با عنوان «بررسی نقش امنیت سایبری در آینده حمل‌ونقل دریایی» به این نتیجه رسیدند که فضای سایبری می‌تواند به‌عنوان دنیای الکترونیکی درک گردد، جایی که اطلاعات نرم‌افزارها و مردم به اشتراک گذاشته می‌شود و به‌صورت یکپارچه در دنیای فیزیکی درهم‌آمیخته شده‌اند. حملات سایبری مربوط به وسایل کامپیوتری در کشتی‌ها، پایانه‌ها، بنادر و تمام تجهیزات کامپیوتری است که از عملیات دریایی پشتیبانی می‌نماید.

زابلی زاده و وهاب‌پور (۱۳۹۷) در مطالعه‌ای با عنوان «قدرت بازدارندگی در فضای سایبر» به این نتیجه رسیدند که راهبرد بازدارندگی بدون اقدامات تلافی‌جویانه، موفق نخواهد بود و در نبود اقدامات تلافی‌جویانه، مهاجمان بالقوه هم انگیزه‌ای برای خودداری از حمله ندارند.

امیرلی و تقی‌پور (۱۳۹۸) در پژوهشی با عنوان «ارائه مدل فرایندی دفاع سایبری بومی» با بهره‌گیری از روش موردی زمینه‌ای و چهارچوب معماری زکمن، فرایندهای کلیدی دفاع سایبری را احصا و با استفاده از روش مدل ساختاری تفسیری و مقایسه‌ای زوجی این فرایندها را سطح‌بندی و مدل نهایی را ارائه نموده‌اند.

«مالوی»[1] و همکاران (۲۰۲۳) در مقاله‌ای با عنوان «آموزش دفاع با حمله (و بالعکس): انتقال یادگیری در بازی‌های امنیت سایبری» یک مدل جدید معرفی می‌کند که سیستم‌های دفاع سایبری را با گنجاندن تعصبات شناختی در تصمیم‌گیری انسانی بهبود می‌بخشد که در نهایت عملکرد را در برابر مهاجمان انسانی بهبود می‌بخشد. این تحقیق اهمیت درک رفتار شبیه انسان در بازی‌های امنیتی را که می‌تواند منجر به مکانیسم‌های دفاعی قوی‌تر در برابر راهبردهای مختلف انسانی شود، برجسته می‌کند.

1. Malloy

«سولمز و نیکرک»[1] (۲۰۱۳) در پژوهشی با عنوان «بررسی امنیت اطلاعاتی و امنیت سایبری» با روش توصیفی و تحلیلی به بررسی تفاوت بین امنیت اطلاعات و امنیت در فضای مجازی پرداخته و بیان نمودند که در آسیب‌های فضای مجازی مستقیم مربوط به جامعه است مانند زورگیری اینترنتی و برخلاف فضای اطلاعات که انسان در نقش فرایند امنیتی است.

«ناردینا»[2] (۲۰۲۰) در پژوهشی با عنوان «ایمنی سازی کودکان در فضای سایبر از تهدیدهای تروریستی» با روش توصیفی و تحلیلی به بررسی تهدیدهای فضای سایبر بر امنیت اجتماعی کودکان از حیث افراط‌گرایی و تروریستی می‌پردازد.

دارلی (۲۰۲۳) در پژوهشی با عنوان «خطرات تسلیم شدن در برابر سوگیری در امنیت سایبری؛ ارزیابی تأثیر سوگیری‌های شناختی بر ارزیابی تهدید و راهبردهای امنیت سایبری» با روش توصیفی و تحلیلی به بررسی چند نمونه زمینه‌ای از چگونگی تأثیر سوء سوگیری‌های شناختی بر تیم‌های امنیت سایبری از پشته امنیتی آن‌ها، بزرگ‌ترین تهدیدات شبکه‌ها و املاک دیجیتال آن‌ها، درک طرز فکر مهاجم و انتخاب متخصصان فنی برای هدایت برنامه‌های آن‌ها می‌پردازد.

«کای‌مینل»[3] و همکاران (۲۰۲۳) در پژوهشی با عنوان «تمرین چندبُعدی دفاع سایبری: تأکید بر جنبه‌های احساسی، اجتماعی و شناختی» با روش توصیفی و تحلیلی یک رویکرد چندبُعدی را برای تمرین‌های دفاع سایبری مورد بحث و پیشنهاد قرار می‌دهد که جنبه‌های شناختی، عاطفی و اجتماعی مهم برای یادگیری میان‌رشته‌ای موفق را متعادل می‌کند.

«حکیمی»[4] و همکاران (۲۰۲۴) در پژوهشی با عنوان «عوامل انسانی در امنیت سایبری؛ تحلیل عمیق مطالعات کاربرمحور» با روش توصیفی و تحلیلی به بررسی تقاطع پیچیده رفتار، شناخت، فناوری و انسان در حوزه امنیت سایبری می‌پردازد که هدف آن افزایش درک ما از چالش‌های انسان‌محور مؤثر بر اثربخشی اقدامات امنیت سایبری است.

1. Von Solms, R., & Van Niekerk, J.
2. Nardina, O. V.
3. Maennel, K.
4. Hakimi

کیم (۲۰۲۳) در پژوهشی با عنوان «مدل پردازش و طبقه‌بندی حملات سایبر شناختی: براساس روان‌شناسی شناختی» نشان می‌دهد که بسیاری از حملات سایبری به‌جای ضعف‌های فنی سیستم، از آسیب‌پذیری‌های شناختی مدیران سیستم بهره‌برداری می‌کنند. این اهمیت درک روان‌شناسی انسان در امنیت سایبری را برجسته می‌کند و تأکید می‌کند که بهبود امنیت سیستم‌های حیاتی ملی نیاز به رویکرد دوگانه دارد: تقویت دفاع فنی و رسیدگی به آسیب‌پذیری‌های شناختی پرسنل.

بر این اساس خلأ چهارچوب جامعی از عوامل انسانی دخیل در سیستم‌های سایبری که با ترکیب مدل‌های شناختی و روان‌شناسی و براساس تجربیات، بتواند یک مدل جامع از عوامل انسانی دخیل در سیستم‌های سایبری ارائه دهد و عوامل مختلفی مانند دانش، مهارت، انگیزه و احساسات را در نظر بگیرد، به‌شدت احساس می‌گردد که این پژوهش درصدد رفع این خلأ است.

۳. روش‌شناسی پژوهش

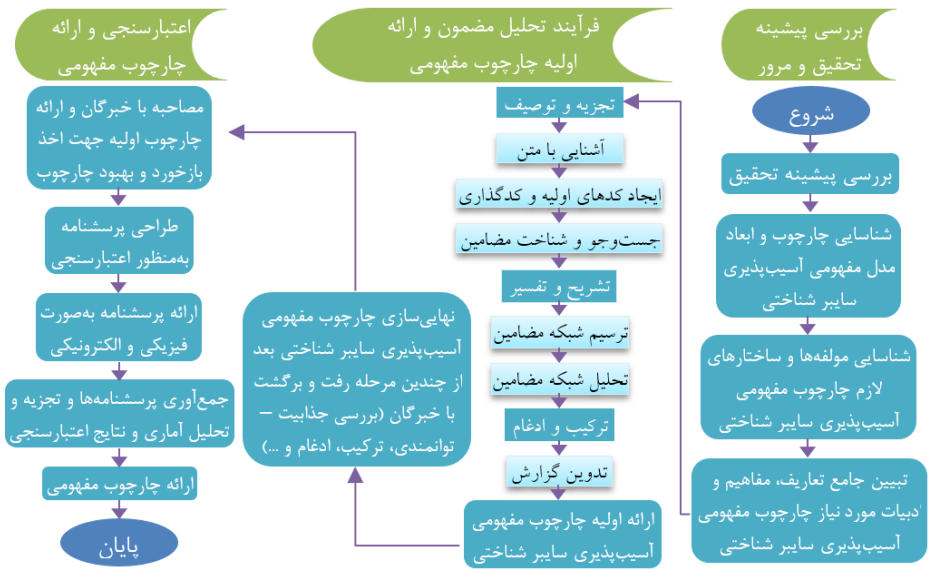
این پژوهش ازنظر هدف کاربردی-توسعه‌ای است و با توجه به ماهیت این تحقیق که طرحی کلان با دامنه گسترده بوده، از روش مطالعات توصیفی-کتابخانه‌ای استفاده می‌گردد. همچنین این پژوهش با استناد به منابع معتبر کتابخانه‌ای به دنبال پاسخ به سؤال اصلی است که عبارت است از: چهارچوب مفهومی آسیب‌پذیری سایبر شناختی چه ابعاد و مؤلفه‌هایی دارد؟

برای پاسخ به این سؤالات، اطلاعات به شیوه کتابخانه‌ای برآورد خواهد شد؛ بدین ترتیب که با مراجعه به منابع معتبر و مرتبط مانند کتب، مقالات، گزارش‌های سازمان‌های ملی و بین‌المللی، طرح‌های پژوهشی و اسناد بالادستی منابع موردنیاز تهیه و متناسب با بخش‌های مختلف پژوهش تکمیل خواهد شد؛ و پس‌ازآن برای استفاده از منابع گردآوری‌شده مرتبط از روش تحلیل مضمون استفاده شده است. بدین‌صورت که پس گردآوری منابع معتبر، تحلیل مضمون بر روی آن‌ها براساس مضامین اصلی و فرعی در راستای پاسخ به سؤالات پژوهش

صورت می‌گیرد. در نهایت با استفاده از پرسش‌نامه و مصاحبه‌های عمیق نیمه ساختاریافته با خبرگان چهارچوب طراحی‌شده و تحلیل ورودی‌ها مورد تأیید قرار می‌گیرد.

۳-۱. جامعهٔ آماری، نمونه آماری و ابزار گردآوری داده‌ها

جامعهٔ آماری مورد استفاده در این پژوهش، مدیران، کارشناسان و خبرگان در حوزه سایبری و شناختی و همچنین اساتید و پژوهشگران دانشگاه‌ها و مراکز تحقیقاتی بوده است؛ همچنین ابزار گردآوری داده‌ها، استفاده از مصاحبه، پرسش‌نامه و بهره‌گیری از نظرات خبرگان است.



شکل ۱: نمای گرافیکی فرایند پژوهش

۴. یافته‌های تحقیق و تجزیه‌وتحلیل آن‌ها

با توجه به فرایند تحقیق تبیین شده، تمامی متون منتخب منابع از قبیل مقالات، کتب و گزارش‌های معتبر جمع‌آوری گردید. سپس در راستای پاسخ به سؤالات پژوهش تحلیل مضمون منابع صورت گرفته و شبکه مضامین ترسیم شده است. در نهایت ضمن تحلیل شبکه مضامین و ارائه جمع‌بندی، چهارچوب احصا شده ارائه گردیده است.

۴-۱. تحلیل مضمون حوزه آسیب‌پذیری سایبر شناختی (اولیه)

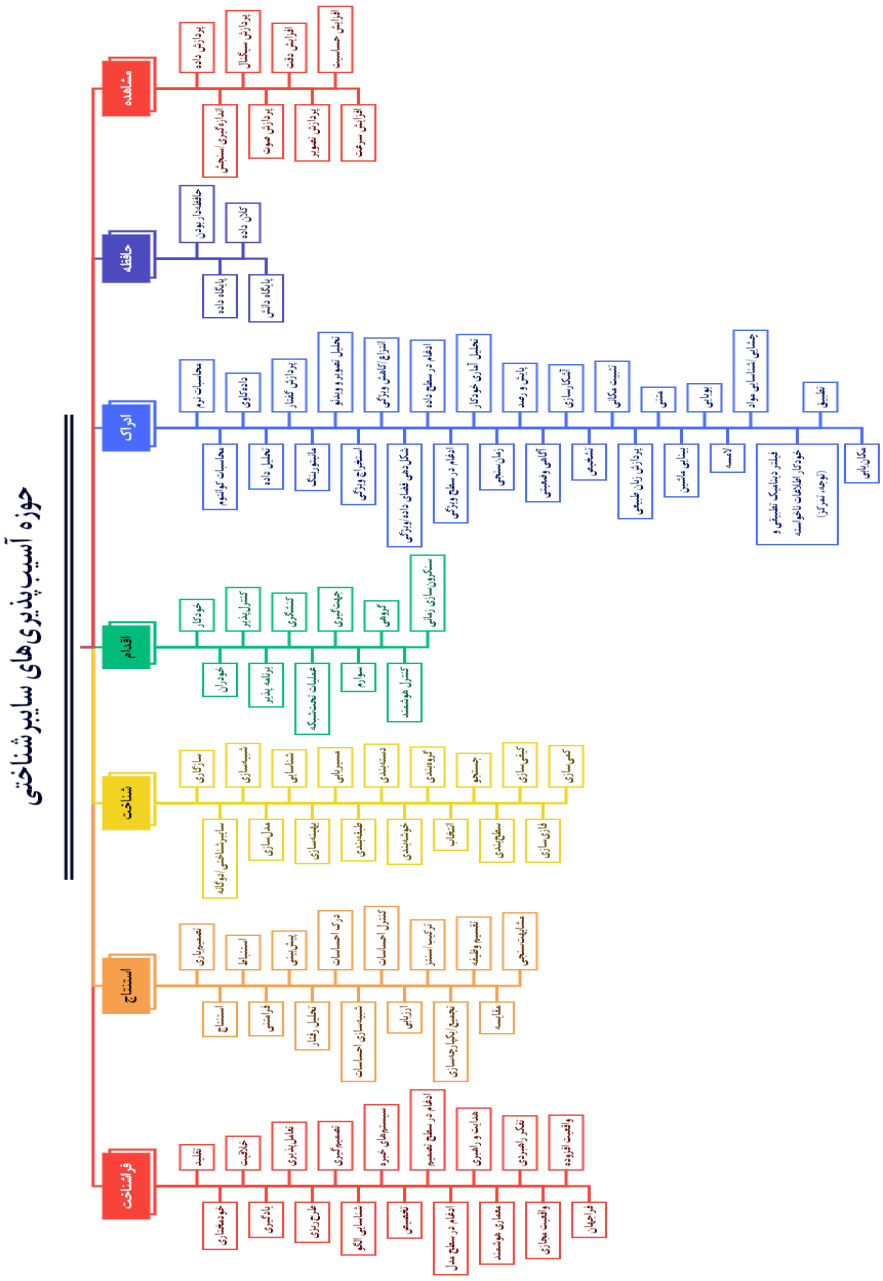
در این بخش ابتدا مصاحبه‌های خبرگانی و متون منتخب منابع از قبیل مقالات، کتب و گزارش‌های معتبر مورد تحلیل و بررسی قرار گرفت و با توجه به فرایند روش تحلیل مضمون در جدول (۲)، مضامین اصلی، فرعی شناسایی و استخراج گردید. لازم به ذکر است در فاز اول سعی شد با توجه به رویکرد پژوهش که دفاع سایبری است، تمامی مؤلفه‌های مهم هر دو حوزه شناختی و سایبر مدنظر باشد، بنابراین برخی از مؤلفه‌ها در مرحله اول جنبه فناوری دارند. در فاز اول، ۷ مضمون اصلی (بُعد) و ۱۰۱ مضمون فرعی (مؤلفه‌ها) شناسایی شد.

جدول ۲: تحلیل مضمون حوزه آسیب‌پذیری سایبر شناختی (اولیه)

ردیف	محور اصلی	مضمون‌های اصلی (بُعد-لایه)	مضمون‌های فرعی (مؤلفه‌ها)			
۱,۲,۳,۴	حوزه آسیب‌پذیری‌های سایبر شناختی	مشاهده	اندازه‌گیری-سنجش	پردازش داده	پردازش سیگنال	پردازش صوت
۵,۶,۷,۸			پردازش تصویر	افزایش دقت	افزایش سرعت	افزایش حساسیت
۹,۱۰,۱۱,۱۲		حافظه	حافظه‌دار بودن	پایگاه داده	پایگاه دانش	کلان داده
۱۳,۱۴,۱۵,۱۶		ادراک	محاسبات نرم	محاسبات کوانتوم	داده‌کاوی	تحلیل داده
۱۷,۱۸,۱۹,۲۰			پردازش گفتار	مانیتورینگ	استخراج ویژگی	زمان‌سنجی
۲۱,۲۲,۲۳,۲۴			آشکارسازی	تشخیص	تثبیت مکانی	پایش و رصد
۲۵,۲۶,۲۷,۲۸			متنی	بینایی ماشین	بویایی	لامسه
۲۹,۳۰,۳۱,۳۲			تطبیق	مکان‌یابی	ادغام در سطح داده	آگاهی وضعیتی
۳۳,۳۴,۳۵			تحلیل تصویر و ویدئو	پردازش زبان طبیعی		انتزاع-کاهش ویژگی
۳۶,۳۷,۳۸			چشایی-شناسایی مواد	ادغام در سطح ویژگی		تحلیل آماری خودکار

ردیف	محور اصلی	مضمون‌های اصلی (بُعد-لایه)	مضمون‌های فرعی (مؤلفه‌ها)			
۳۹,۴۰			شکل‌دِهی فضای داده- ویژگی			فیلتر دینامیک تطبیقی و خودکار اطلاعات ناخواسته (توجه، تمرکز)
۴۱,۴۲,۴۳,۴۴	اقدام	خودکار	خودران		کنترل‌پذیر	برنامه‌پذیر
۴۵,۴۶,۴۷,۴۸		کنشگری	جهت‌گیری		سوارم	گروهی
۴۹,۵۰,۵۱		عملیات تحت شبکه	کنترل هوشمند			سنکرون سازی زمانی
۵۲,۵۳,۵۴	شناخت	سازگاری	مسیریابی			سایبر شناختی- دوگانه
۵۵,۵۶,۵۷,۵۸		شناسایی	بهینه‌سازی		شبیه‌سازی	مدل‌سازی
۵۹,۶۰,۶۱,۶۲,۶۳		خوشه‌بندی	گروه‌بندی	انتخاب	طبقه‌بندی	دسته‌بندی
۶۴,۶۵,۶۶,۶۷,۶۸		سطح‌بندی	کیفی‌سازی	فازی‌سازی	کمی‌سازی	جستجو
۶۹,۷۰,۷۱,۷۲	استنتاج	تصمیم‌یاری	استنتاج		استنباط	فرامتنی
۷۳,۷۴,۸۷۵,۷۶		پیش‌بینی	تحلیل رفتار		ارزیابی	ترکیب- سنتز
۷۷,۷۸,۷۹,۸۰		درک احساسات	کنترل احساسات		تقسیم وظیفه	مقایسه
۸۱,۸۲,۸۳,۸۴		مشابهت‌سنجی	تقلید		خودمختاری	خلاقیت
۸۵,۸۶,۸۷,۸۸		یادگیری	تعامل‌پذیری		تخصیص	هدایت و راهبری
۸۹,۹۰,۹۱,۹۲	فراشناخت	طرح‌ریزی	تصمیم‌گیری		شناسایی الگو	سیستم‌های خبره
۹۳,۹۴,۹۵,۹۶		واقعیت مجازی	واقعیت افزوده		فراجهان	تفکر راهبردی
۹۷,۹۸,۹۹		معماری هوشمند	تجمیع- یکپارچه‌سازی			شبیه‌سازی احساسات
۱۰۰,۱۰۱		ادغام در سطح تصمیم			ادغام در سطح مدل	

۴-۱-۱. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی (اولیه)



شکل ۲: شبکه مضامین اصلی و فرعی حوزه آسیب‌پذیری سایبر شناختی (اولیه)

۴-۱-۲. بررسی نتایج اولیه از منظر جذابیت و توانمندی

در این بخش شبکه مضامین اولیه که شامل ۷ بُعد و مضمون اصلی و ۱۰۱ مؤلفه و مضمون فرعی بود، در اختیار خبرگان قرار گرفت و از آن‌ها خواسته‌شده که نمرات خود را از منظر جذابیت و توانمندی اعلام کنند. نمرات و میانگین مرتبط با مفاهیم «جذابیت» و «توانمندی» در هریک از ابعاد هفت‌گانه براساس یافته‌های حاصل از جلسات خبرگی در جدول ۳: نمرات شبکه مضامین اولیه از منظر جذابیت-توانمندی(۳) به تفکیک مضامین اصلی و فرعی آمده است.

جدول ۳: نمرات شبکه مضامین اولیه از منظر جذابیت-توانمندی

ردیف	محور اصلی	مضمون اصلی	مضمون فرعی (مؤلفه‌ها)	جذابیت		توانمندی	
				نمره مؤلفه	نمره بُعد	نمره مؤلفه	نمره بُعد
۱	حوزه آسیب‌پذیری‌های سایبر شناختی	مشاهده	اندازه‌گیری- سنجش	۷	۷/۲	۵	۵/۵
۲			پردازش داده	۷/۲۳		۶/۵۴	
۳			پردازش سیگنال	۶/۶۹		۶/۱۵	
۴			پردازش صوت	۶/۷۷		۵/۵۴	
۵			پردازش تصویر	۷/۲۳		۶/۲۳	
۶			افزایش دقت	۷/۴۶		۴/۶۹	
۷			افزایش سرعت	۷/۸۵		۵/۴۶	
۸			افزایش حساسیت	۷/۰۸		۴/۶۲	
۹		حافظه	حافظه‌دار بودن	۷/۱۵	۷/۵	۵/۳۸	۵/۶
۱۰			پایگاه داده	۷/۵۴		۶/۰۰	
۱۱			پایگاه دانش	۷/۵۴		۵/۴۶	
۱۲			کلان داده	۷/۹۲		۵/۴۶	
۱۳		ادراک	محاسبات نرم	۶/۶۲	۷/۲	۴/۶۲	۴/۹
۱۴			محاسبات کوانتوم	۵/۹۲		۲/۵۴	
۱۵			داده‌کاوی	۸/۰۰		۵/۶۲	
۱۶			تحلیل داده	۸/۰۸		۵/۵۴	
۱۷			پردازش گفتار	۷/۰۸		۵/۲۳	
۱۸			مانیتورینگ	۷/۰۰		۵/۵۴	
۱۹			تحلیل تصویر و ویدئو	۷/۶۹		۵/۴۶	

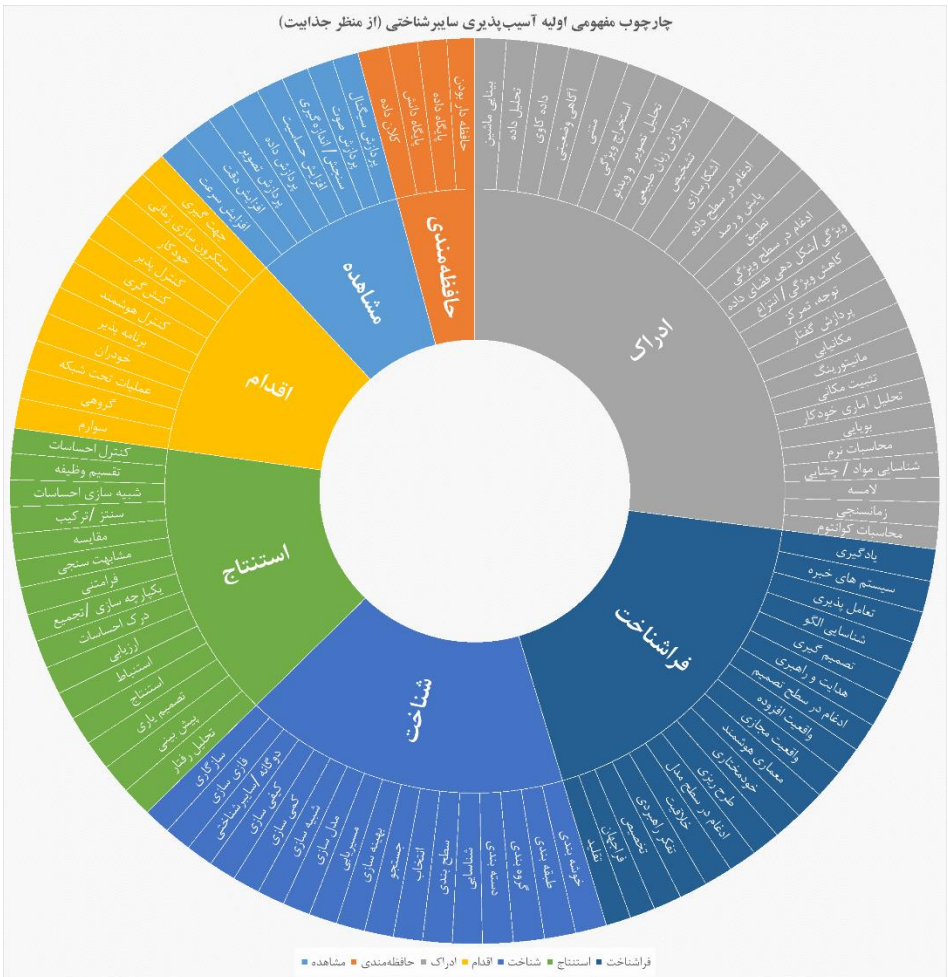
ردیف	محور اصلی	مضمون اصلی	مضمون فرعی (مؤلفه‌ها)	جذابیت		توانمندی	
				نمره مؤلفه	نمره بُعد	نمره مؤلفه	نمره بُعد
۲۰			استخراج ویژگی	۷/۶۹		۴/۷۷	
۲۱			انتزاع-کاهش ویژگی	۷/۱۵		۴/۰۸	
۲۲			شکل‌دهی فضای داده- ویژگی	۷/۱۵		۴/۶۹	
۲۳			ادغام در سطح داده	۷/۳۱		۴/۹۲	
۲۴			ادغام در سطح ویژگی	۷/۱۵		۴/۵۴	
۲۵			تحلیل آماری خودکار	۶/۶۹		۵/۵۴	
۲۶			زمان‌سنجی	۶/۴۶		۴/۸۵	
۲۷			پایش و رصد	۷/۲۳		۵/۳۸	
۲۸			آگاهی وضعیتی	۷/۹۲		۵/۰۸	
۲۹			آشکارسازی	۷/۵۴		۵/۳۱	
۳۰			تشخیص	۷/۵۴		۵/۱۵	
۳۱			تثبیت مکانی	۶/۷۷		۵/۰۸	
۳۲			پردازش زبان طبیعی	۷/۵۴		۵/۳۱	
۳۳			متنی	۷/۷۷		۴/۹۲	
۳۴			بینایی ماشین	۸/۰۸		۵/۶۲	
۳۵			بویایی	۶/۶۲		۳/۴۶	
۳۶			لامسه	۶/۵۴		۳/۳۱	
۳۷			چشایی- شناسایی مواد	۶/۵۴		۳/۹۲	
۳۸			فیلتر دینامیک تطبیقی و خودکار اطلاعات ناخواسته (توجه، تمرکز)	۷/۰۸		۴/۷۷	
۳۹			تطبیق	۷/۱۵		۵/۳۸	
۴۰			مکان‌یابی	۷/۰۰		۵/۴۶	
۴۱		اقدام	خودکار	۷/۱۵	۷/۵	۴/۷۷	۵
۴۲			خودران	۷/۶۲		۵/۱۵	
۴۳			کنترل‌پذیر	۷/۳۸		۵/۴۶	
۴۴			برنامه پذیر	۷/۵۴		۵/۵۴	
۴۵			کنشگری	۷/۴۶		۵/۲۳	
۴۶			عملیات تحت شبکه	۷/۸۵		۵/۱۵	
۴۷			جهت‌گیری	۶/۷۷		۵/۰۸	

ردیف	محور اصلی	مضمون اصلی	مضمون فرعی (مؤلفه‌ها)	جذابیت		توانمندی	
				نمره مؤلفه	نمره بُعد	نمره مؤلفه	نمره بُعد
۴۸			سوارم	۷/۹۲		۴/۱۵	
۴۹			گروهی	۷/۸۵		۴/۶۲	
۵۰			کنترل هوشمند	۷/۴۶		۵/۰۰	
۵۱			سنکرون سازی زمانی	۷/۰۰		۵/۳۸	
۵۲		شناخت	سازگاری	۷/۰۰	۷/۴	۵/۱۵	۵/۵
۵۳			سایبر شناختی- دوگانه	۷/۰۸		۴/۹۲	
۵۴			شبیه‌سازی	۷/۱۵		۶/۰۰	
۵۵			مدل‌سازی	۷/۱۵		۵/۸۵	
۵۶			شناسایی	۷/۶۹		۵/۷۷	
۵۷			بهینه‌سازی	۷/۳۸		۵/۶۲	
۵۸			مسیریابی	۷/۳۱		۵/۷۷	
۵۹			طبقه‌بندی	۸/۰۸		۵/۸۵	
۶۰			دسته‌بندی	۷/۹۲		۵/۸۵	
۶۱			خوشه‌بندی	۸/۰۸		۵/۴۶	
۶۲			گروه‌بندی	۸/۰۰		۵/۵۴	
۶۳			انتخاب	۷/۵۴		۵/۷۷	
۶۴			جستجو	۷/۴۶		۶/۰۷۷	
۶۵			سطح‌بندی	۷/۶۲		۵/۶۱۵	
۶۶			کیفی‌سازی	۷/۰۸		۴/۳۰۸	
۶۷			فازی سازی	۷/۰۰		۴/۸۴۶	
۶۸			کمی سازی	۷/۰۸		۵/۱۵۴	
۶۹		استنتاج	تصمیم یاری	۷/۸۵	۷/۳	۴/۹۲۳	۴/۳
۷۰			استنتاج	۷/۵۴		۴/۳۰۸	
۷۱			استنباط	۷/۴۶		۴/۰۷۷	
۷۲			فرامتنی	۷/۳۱		۴/۲۳۱	
۷۳			پیش‌بینی	۷/۸۵		۴/۱۵۴	
۷۴			تحلیل رفتار	۷/۸۵		۴/۰۷۷	
۷۵			درک احساسات	۷/۳۸		۳/۸۴۶	
۷۶			شبیه‌سازی احساسات	۷/۰۸		۳/۷۶۹	

ردیف	محور اصلی	مضمون اصلی	مضمون فرعی (مؤلفه‌ها)	جذابیت		توانمندی	
				نمره مؤلفه	نمره بُعد	نمره مؤلفه	نمره بُعد
۷۷			کنترل احساسات	۶/۶۲		۳/۳۰۸	
۷۸			ارزیابی	۷/۳۸		۴/۴۶۲	
۷۹			ترکیب- سنتز	۷/۰۸		۴/۵۳۸	
۸۰			تجمیع- یکپارچه‌سازی	۷/۳۱		۴/۹۲۳	
۸۱			تقسیم وظیفه	۷/۰۰		۴/۲۳۱	
۸۲			مقایسه	۷/۰۸		۴/۹۲۳	
۸۳			مشابهت سنجی	۷/۱۵		۴/۶۹۲	
۸۴		فراشناخت	تقلید	۶/۴۶	۷/۶	۴/۴۶۲	۴/۲
۸۵			خودمختاری	۷/۵۴		۴/۰۷۷	
۸۶			خلاقیت	۷/۳۸		۳/۲۳۱	
۸۷			یادگیری	۸/۴۶		۵/۱۵۴	
۸۸			تعامل‌پذیری	۸/۳۱		۴/۶۱۵	
۸۹			طرح‌ریزی	۷/۴۶		۴/۳۰۸	
۹۰			تصمیم‌گیری	۸/۱۵		۴/۳۸۵	
۹۱			شناسایی الگو	۸/۱۵		۴/۸۴۶	
۹۲			سیستم‌های خبره	۸/۳۱		۴/۹۲۳	
۹۳			تخصیص	۷/۳۱		۴/۸۴۶	
۹۴			ادغام در سطح تصمیم	۷/۶۲		۳/۸۴۶	
۹۵			ادغام در سطح مدل	۷/۳۸		۳/۷۶۹	
۹۶			هدایت و راهبری	۷/۶۹		۳/۵۳۸	
۹۷			معماری هوشمند	۷/۵۴		۴/۵۳۸	
۹۸			تفکر راهبردی	۷/۳۱		۳/۲۳۱	
۹۹			واقعیت مجازی	۷/۵۴		۴/۷۶۹	
۱۰۰			واقعیت افزوده	۷/۵۴		۴/۶۱۵	
۱۰۱			فراجهان	۶/۵۴		۲/۶۹۲	
جمع کل				۷/۷		۴/۶۴	

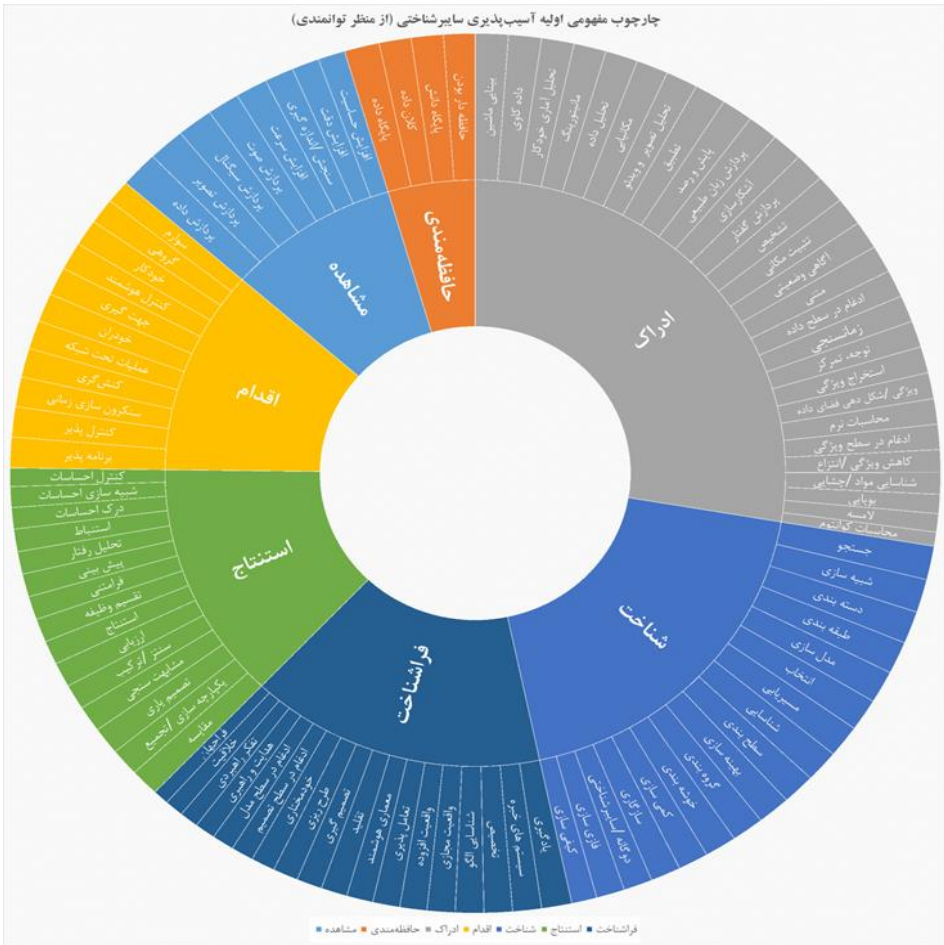
همان‌طور که انتظار می‌رفت بُعد فراشناخت بیشترین امتیاز را از لحاظ جذابیت و بُعد حافظه‌مندی بیشترین امتیاز را از لحاظ توانمندی کسب نموده‌اند.

براساس امتیازات کسب‌شده، چهارچوب مفهومی اولیه از منظر جذابیت به شکل زیر است.



شکل ۳: مدل مفهومی اولیه از منظر جذابیت

همچنین، براساس امتیازات کسب‌شده، مدل مفهومی اولیه از منظر توانمندی به شکل زیر است.



شکل ۴: مدل مفهومی اولیه از منظر توانمندی

۴-۲. تحلیل مضمون حوزه آسیب‌پذیری سایبر شناختی (بازبینی‌شده)

در این بخش، مضامین احصا شده اولیه توسط خبرگان مورد بازنگری قرار گرفت و با تکیه‌بر نظرات خبرگی، نمرات و امتیازات کسب‌شده از منظر جذابیت و توانمندی، متون منتخب

منابع از قبیل مقالات، کتب و گزارش‌های معتبر مضامین دقیق‌تر شدند و سعی گردید فناوری‌های شناسایی‌شده در مرحله قبل با مؤلفه‌های شناختی متناظر خود ادغام شوند. در این مرحله ۷ مضمون اصلی (بُعد-لایه) و ۷۸ مضمون فرعی (مؤلفه‌ها) شناسایی شدند که با توجه به فرایند روش تحلیل مضمون در جدول ۴: تحلیل مضمون حوزه آسیب‌پذیری سایبر شناختی (بازبینی‌شده)(۴) مضامین اصلی و فرعی ذکر شده است.

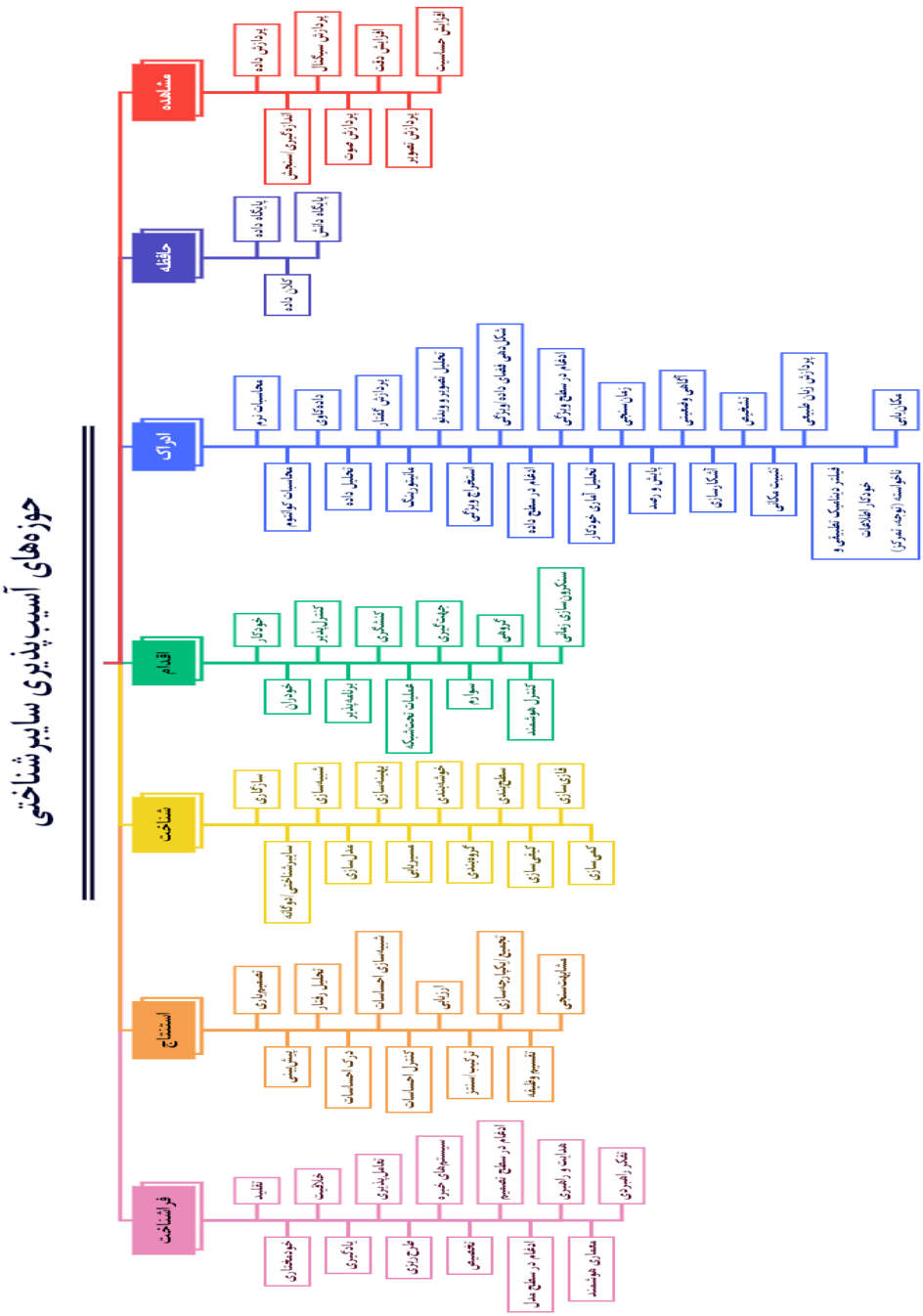
جدول ۴: تحلیل مضمون حوزه آسیب‌پذیری سایبر شناختی (بازبینی‌شده)

ردیف	محور اصلی	مضمون‌های اصلی	مضمون‌های فرعی (مؤلفه‌ها)			
۱,۲,۳,۴	حوزه آسیب‌پذیری‌های سایبر شناختی	مشاهده	افزایش حساسیت	پردازش داده	پردازش سیگنال	افزایش دقت
۵,۶,۷			پردازش صوت	پردازش تصویر	اندازه‌گیری-سنجش	
۸,۹,۱۰		حافظه	پایگاه داده	پایگاه دانش	کلان‌داده	
۱۱,۱۲,۱۳		ادراک	محاسبات نرم	محاسبات کوانتوم	داده‌کاوی	
۱۴,۱۵,۱۶			تحلیل‌داده	پردازش گفتار	مانیتورینگ	
۱۷,۱۸,۱۹			تحلیل تصویر و ویدئو	استخراج ویژگی	تحلیل آماری خودکار	
۲۰,۲۱,۲۲			ادغام در سطح ویژگی	ادغام در سطح داده	زمان‌سنجی	
۲۳,۲۴,۲۵			پایش و رصد	آگاهی وضعیتی	آشکارسازی	
۲۶,۲۷,۲۸			تشخیص	تثبیت مکانی	پردازش زبان طبیعی	
۲۹,۳۰			مکان‌یابی	شکل‌دِهی فضای داده-ویژگی		
۳۱			فیلتر دینامیک تطبیقی و خودکار اطلاعات ناخواسته (توجه، تمرکز)			
۳۲,۳۳,۳۴,۳۵		اقدام	خودکار	خودران	کنترل‌پذیر	برنامه‌پذیر
۳۶,۳۷,۳۸,۳۹			سوارم	کنشگری	گروهی	کنترل هوشمند

ردیف	محور اصلی	مضمون‌های اصلی	مضمون‌های فرعی (مؤلفه‌ها)			
۴۰,۴۱,۴۲			عملیات تحت شبکه	سنکرون‌سازی زمانی		جهت‌گیری
۴۳,۴۴,۴۵		شناخت	سازگاری	سایبر شناختی-دوگانه		شبیه‌سازی
۴۶,۴۷,۴۸			مدل‌سازی	بهینه‌سازی		مسیریابی
۴۹,۵۰,۵۱			خوشه‌بندی	گروه‌بندی		سطح‌بندی
۵۲,۵۳,۵۴			کیفی‌سازی	فازی‌سازی		کمی‌سازی
۵۵,۵۶,۵۷		استنتاج	تصمیم‌یاری	پیش‌بینی		تحلیل رفتار
۵۸,۵۹,۶۰			درک احساسات	شبیه‌سازی احساسات		کنترل احساسات
۶۱,۶۲,۶۳			ارزیابی	ترکیب-سنتز		تجمیع-یکپارچه‌سازی
۶۴,۶۵			تقسیم وظیفه	مشابهت‌سنجی		
۶۶,۶۷,۶۸,۶۹		فراشناخت	تقلید	خودمختاری	خلاقیت	یادگیری
۷۰,۷۱,۷۲			تعامل‌پذیری	طرح‌ریزی		سیستم‌های خبره
۷۳,۷۴,۷۵			تخصیص	ادغام در سطح تصمیم		ادغام در سطح مدل
۷۶,۷۷,۷۸			هدایت و راهبری	معماری هوشمند		تفکر راهبردی

۴-۲-۱. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی (بازبینی‌شده)

در شکل ۵: شبکه مضامین اصلی و فرعی حوزه آسیب‌پذیری سایبر شناختی (بازبینی‌شده) نشان داده‌شده است.



شکل ۵: شبکه مضامین اصلی و فرعی حوزه آسیب‌پذیری سایبر شناختی (بازبینی‌شده)

۴-۲-۱-۱. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی- مشاهده

بُعد مشاهده: مشاهده، کسب فعال اطلاعات از یک منبع اولیه است. در موجودات زنده، مشاهده حواس را به کار می‌گیرد. در علم، مشاهده همچنین می‌تواند شامل درک و ثبت داده‌ها از طریق استفاده از ابزارهای علمی باشد. این اصطلاح همچنین ممکن است به هر داده جمع‌آوری‌شده در طول فعالیت علمی اشاره کند. مشاهدات می‌توانند کیفی باشند، یعنی فقط عدم وجود یا وجود یک خاصیت ذکر می‌گردد، یا اگر مقدار عددی با شمارش یا اندازه‌گیری به پدیده مشاهده‌شده الصاق گردد، کمی باشد.

۴-۲-۱-۲. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی- حافظه

بُعد حافظه: متشکل از حافظه بلندمدت (ضرایب درون گره‌ها، ازجمله اتصال آن‌ها در شبکه‌های عصبی)، حافظه کوتاه‌مدت (وضعیت فعلی یک سیستم در یک شبکه عصبی)، پایگاه داده (پایگاه داده مجموعه‌ای منظم و سازمان‌یافته از داده‌های ذخیره‌شده و الکترونیکی از سیستم رایانه‌ای است؛ درجایی که پایگاه داده‌ها پیچیده‌تر هستند، آن‌ها اغلب با استفاده از تکنیک‌های طراحی رسمی و مدل‌سازی توسعه می‌یابند) و پایگاه دانش (مجموعه‌ای از حقایق در دسترس یک برنامه همان‌طور که پایگاه داده را می‌توان به‌عنوان مجموعه‌ای سازمان‌یافته از داده‌ها در نظر گرفت، پایگاه دانش مجموعه‌ای سازمان‌یافته از «واقعیت‌ها» یا اظهارات روابط بین اشیا است. سازمان‌دِهی خاص دانش توسط روش بازنمایی دانش انتخاب‌شده توسط طراح برنامه دیکته می‌گردد.)

۴-۲-۱-۳. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی- ادراک

بُعد ادراک: این فرایند کسب، تفسیر، انتخاب و سازمان‌دِهی اطلاعات حسی است. در انسان، ادراک توسط اندام‌های حسی به دست می‌آید. در حوزه سایبر شناختی، سازوکار ادراک داده‌های به‌دست‌آمده توسط حسگرها را به شیوه‌ای معنادار کنار هم قرار می‌دهد.

۴-۲-۱-۴. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی- اقدام

بُعد اقدام: متشکل از خودکارسازی (حذف عامل انسانی از انجام یک فرایند)، خودرانی (ایجاد قابلیت هدایت یک موجودیت در یک فضای داده مکانی بدون دخالت انسان)، کنترل‌پذیری (کنترل‌پذیری، یکی از خاصیت‌های مهم هر سیستم است و نقش مهمی در مسئله‌های کنترل ایفا می‌کند، مثل پایدار نمودن سیستم‌های ناپایدار به‌وسیله بازخورد یا کنترل بهینه. کنترل‌پذیر بودن به معنی توانایی سیستم در رفتن از هر حالت اولیه به حالت دلخواه با استفاده از ورودی‌های دلخواه است. معنی دقیق کنترل‌پذیری بستگی به محل کاربرد آن دارد)، برنامه‌پذیری (یک فرایند استنتاجی است که توسط یک دستور کار یا فهرست مشاغل کنترل می‌شود. این فرایند سیستم را به مراحل واضح و مدولار تقسیم می‌کند. هر یک از ورودی‌ها، یا وظایف، در فهرست کار، وظیفه خاصی است که باید در طول یک فرایند حل مسئله انجام شود)، عملکرد (یک تابع رابطه‌ای است که صفر یا چند ویژگی را می‌گیرد و یک آیتم را که ممکن است مرکب باشد، برمی‌گرداند؛ در سیستم‌های مبتنی بر کلاس و فریم، تابعی که یک جمله واحد را می‌گیرد و یک عبارت واحد را برمی‌گرداند، گاهی اوقات اسلات نامیده می‌شود. تابع چند متغیره تابعی است که یکشی مرکب مانند یک لیست یا یک آرایه را برمی‌گرداند که ممکن است به‌عنوان مشخصات یک آیتم چندبُعدی در نظر گرفته شود)، کنشگری (قابلیت نشان دادن عکس‌العمل به رخدادهای محیط عملیات) و ... .

۴-۲-۱-۵. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی- شناخت

بُعد شناخت: متشکل از سیستم انطباقی (یک اصلاح‌کننده کلی که برای توصیف سیستم‌هایی مانند شبکه‌های عصبی یا سایر سیستم‌های کنترل پویا که می‌توانند از داده‌های مورد استفاده یاد بگیرند یا تطبیق دهند، استفاده می‌گردد)، سایبر شناختی (صفت سایبر شناختی برای توصیف ویژگی بین کلیه‌ی فرایندها، پدیده‌ها و اشیایی که هم به حوزه اطلاعات دیجیتال و هم به حوزه شناخت گسترش می‌یابند، استفاده می‌گردد. صفت «شناختی سایبری» به‌عنوان بخشی از اصطلاحات «چهارچوب عصر دیجیتال» ابداع شده است)، شبیه‌سازی (ایجاد بستر

نمایش رفتار یک موجودیت)، مدل‌سازی (نمایشی انتزاعی از اجزا و ارتباطات یک پدیده که روابط این موجودیت‌ها و متغیرهای مختلف آن پدیده را به نمایش درمی‌آورد. ازآنجاکه تجربه نمودن همه واقعیت‌ها و پدیده‌ها به‌صورت عملی ممکن نیست از مدل‌ها برای ترسیم وقایع، حقایق یا وضعیت‌ها استفاده می‌گردد. درواقع مدل‌سازی ایجاد ساختاری جهت نمایش، تحلیل و پیش‌بینی رفتار یک موجودیت است)، بهینه‌سازی (به برگزیدن بهترین عضو از یک مجموعه از اعضای دست‌یافتنی اشاره می‌نماید؛ در ساده‌ترین شکل تلاش می‌گردد که با گزینش نظام‌مند داده‌ها از یک مجموعه قابل دستیابی و محاسبه مقدار یک تابع حقیقی مقدار بیشینه و کمینه آن به دست آید)، مسیریابی (هدایت یک موجودیت در یک فضای داده‌ای مکانی)، کلاس‌بندی (طبقه‌بندی با نظارت)، طبقه‌بندی (نگاشت فضای ویژگی به فضای برچسب‌ها یا کلاس‌ها) و ... .

۴-۲-۱-۶. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی- استنتاج

بُعد استنتاج: متشکل از عقلانیت (عقلانیت با اعمال و نتایج مورد انتظار بسته به آنچه عامل درک نموده است، سروکار دارد. انجام اقدامات با هدف به دست آوردن اطلاعات مفید بخش مهمی از عقلانیت است)، فرا استدلال (توانایی استدلال در مورد قوانین فرایند استدلال)، استدلال (مجموعه فرایندهایی است که ما را قادر می‌سازد مبنایی برای قضاوت، تصمیم‌گیری و پیش‌بینی فراهم کنیم)، استنباط (فرایند استنباط یک اصل کلی از داده‌ها یا مثال‌ها)، تصمیم‌یاری (ایجاد گزینه‌های مختلف بر مبنای توابع هدف برای تصمیم‌گیرنده)، استنتاج (به فرایندهایی اشاره دارد که برای نتیجه‌گیری از حقایق و سایر مقدمات یا نتیجه‌گیری‌ها استفاده می‌گردد)، مدل‌های پیش‌بین (مدل‌هایی که برای پیش‌بینی ارزش یک ویژگی یا مجموعه‌ای از ویژگی‌ها براساس مقادیر دیگر ویژگی‌ها طراحی‌شده‌اند. پیش‌بینی اغلب از طبقه‌بندی متمایز می‌گردد، جایی که هدف طبقه‌بندی یک مشاهده است؛ در این زمینه، پیش‌بینی به معنای تولید مقادیر یا محدوده‌ها برای یک ویژگی یا گروهی از ویژگی‌های مرتبط است. بااین‌حال، در یک مفهوم کلی، طبقه‌بندی فقط یک شکل (احتمالاً محدود) از پیش‌بینی چند متغیره است) و ... .

۴-۲-۱-۷. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی- فراشناخت

بُعد فراشناخت: متشکل از تقلید (روشی برای استدلال یا یادگیری که با مقایسه وضعیت فعلی با موقعیت‌های دیگر که به‌نوعی شبیه به هم هستند، استدلال می‌نماید)، خودمختاری (ایجاد قابلیت کنشگری در شرایط تعریف‌نشده)، خلاقیت (توان ساختن یا خلق نمودن چیزی نو است، خواه راهکاری نو برای حل یک مشکل، یک روش یا یک دستگاه نو و یا یک شیء یا فرم نو هنری. خلاقیت بشر تعریفی از قابلیت‌های اقتصاد، زندگی، فناوری، صنایع نو، ثروت نو و کلیه چیزهایی است که از یک اقتصاد خوب جریان می‌گیرند. خلاقیت چندوجهی و چندبُعدی است؛ خلاقیت مهم‌ترین و اساسی‌ترین قابلیت و توانایی انسان و بنیادی‌ترین عامل ایجاد ارزش است که در همه ابعاد و جوانب زندگی وی نقش کاملاً حیاتی ایفا می‌نماید. خلاقیت و نوآوری از والاترین ویژگی‌های انسان است. همه علوم، تولیدات، فناوری‌ها، صنایع، ابداعات، اختراعات، هنرها، ادبیات، موسیقی، معماری و به‌طور کلی اساس انواع تمدن‌ها از ابتدا تاکنون و کلیه دستاوردهای بشری، جلوه‌های گوناگونِ خلاقیت و نوآوری است. تمدن انسانی و زندگی وی بدون خلاقیت امکان‌پذیر نیست)، حل مسئله (فرایندی است که در آن فرد با در پیش گرفتن مسیری که با موانع شناخته‌شده یا ناشناخته مسدود می‌گردد، از موقعیت فعلی به راه‌حل مطلوبی می‌رسد و می‌کوشد به آن دست یابد. حل مسئله شامل تصمیم‌گیری نیز می‌شود که فرایند انتخاب بهترین جایگزین مناسب از بین چندین گزینه برای رسیدن به هدف مورد نظر است)، یادگیری (عبارت است از فعالیت کسب دانش یا مهارت از طریق مطالعه، تمرین، آموزش یا تجربه چیزی، یادگیری باعث افزایش آگاهی افراد مورد مطالعه می‌گردد) و ... .

۴-۳. تحلیل مضمون حوزه آسیب‌پذیری سایبر شناختی (نهایی)

در این بخش مضامین احصا شده مجدداً توسط خبرگان و کارشناسان این حوزه مورد بازنگری قرار گرفت که با تکیه‌بر نظرات خبرگی در این مرحله ۷ مضمون اصلی (بُعد-لایه) و ۴۳ مضمون فرعی (مؤلفه‌ها) شناسایی شدند که با توجه به فرایند روش تحلیل مضمون در

جدول ۵: تحلیل مضمون حوزه آسیب‌پذیری سایبر شناختی (نهایی)(۵)، مضامین اصلی، فرعی ذکر شده است.

جدول ۵: تحلیل مضمون حوزه آسیب‌پذیری سایبر شناختی (نهایی)

ردیف	محور اصلی	مضمون اصلی (بُعد-لایه)	مضمون فرعی (مؤلفه‌ها)		
۱,۲,۳	حوزه آسیب‌پذیری‌های سایبر شناختی	حِسی (Sensational)	بینایی (Vision)	شنوایی (Audition)	بویایی (Smell)
۴,۵			لامسه (Tactility)	چشایی (Taste)	
۶		حافظه (Memory)	حافظه موقت حسی (Sensory buffer Memory)		
۷			حافظه کوتاه‌مدت (Short-term Memory)		
۸			حافظه بلندمدت (Long-term Memory)		
۹			حافظه موقت کُنشی (Action Buffer Memory)		
۱۰,۱۱		ادراک (Perception)	توجه (Attention)	نگرش (Attitudes)	
۱۲,۱۳			حِس حرکتی (Sense of motion)	حِس فضایی (Sense of spatiality)	
۱۴			انگیزش و تعیین هدف (Motivation and goal-setting)		
۱۵			احساسات- عواطف- هیجانات (Emotions)		
۱۶			خودآگاهی (Self- Consciousness)		
۱۷		اقدام (Action)	مهارت-توانایی خاص (Skills)		
۱۸			رفتارهای غیرمترقبه- اتفاقی (Temporary Behaviors)		
۱۹,۲۰		فراشناخت (Meta-Cognitive)	به‌گزینی (Selection)	مقایسه/ تطبیق (Comparison)	
۲۱,۲۲			انتزاع (Abstraction)	به یاد سپردن (Memorization)	
۲۳,۲۴			جستجو (Search)	مصورسازی/ تخیل (Imagery)	
۲۵			دسته‌بندی-طبقه‌بندی (Categorization)		
۲۶			شناسایی هدف- موضوع (Object Identify)		
۲۷			شناختن-تثبیت مفهوم (Concept Establish)		
۲۸			جرح‌وتعدیل-اصلاح (Qualification)		

ردیف	محور اصلی	مضمون اصلی (بُعد-لایه)	مضمون فرعی (مؤلفه‌ها)	
۲۹			کمی‌سازی- سنجش کمیت (Quantification)	
۳۰			تثبیت مدل (Model establish)	
۳۱,۳۲		فرا استنتاج (Meta-inference)	استنتاج (Deduction)	استقراء (Induction)
۳۳,۳۴			استنتاجِ بهترینِ تبیین (Abduction)	قیاس منطقی (Analogy)
۳۵,۳۶			تجزیه‌وتحلیل (Analysis)	امتزاج-بازآفرینی (Synthesis)
۳۷,۳۸		شناختیِ عالی (Higher cognitive)	فهم- معرفت (Comprehension)	یادگیری/ فراگیری (Learning)
۳۹,۴۰			حل مسئله (Problem Solving)	تصمیم‌گیری (Decision Making)
۴۱			خلق- ابداع-پدیدآوردن چیزی (Creation)	
۴۲			برنامه‌ریزی-طرح‌ریزی (Planning)	
۴۳			بازشناخت-شناسایی الگو (Pattern Recognition)	

۴-۳-۱. شبکه مضامین حوزه آسیب‌پذیری سایبر شناختی (نهایی)

در شکل ۶: شبکه مضامین اصلی و فرعی حوزه آسیب‌پذیری سایبر شناختی (نهایی) نشان داده شده است.

شکل ۶: شبکه مضامین اصلی و فرعی حوزه آسیب‌پذیری سایبر شناختی (نهایی)

۴-۴. تجزیه‌وتحلیل و ارائه نتایج اعتبارسنجی

اعتبارسنجی چهارچوب مفهومی ارائه‌شده، براساس تکنیک طراحی پرسش‌نامه، جمع‌آوری پاسخ‌ها و تحلیل آن‌ها استوار گردید. این پرسش‌نامه‌ها به‌منظور ارزیابی عمومی و ارزیابی اختصاصی چهارچوب مفهومی پیشنهادی است که در پیوست‌ها آورده شده است و در این قسمت صرفاً به ارائه نتایج و تحلیل‌ها می‌پردازیم. در ابتدا با استفاده از نرم‌افزار SPSS آلفای کرونباخ محاسبه‌شده که با توجه به اینکه آلفای کرونباخ عدد ۰/۸۴۲ محاسبه‌شده و ضریب پایایی از ۰/۷ بالاتر است، پرسش‌نامه مذکور از پایایی مناسبی برخوردار است.

لازم به ذکر است طیف پاسخ در نظر گرفته‌شده برای سؤالات طیف لیکرت بوده و برای محاسبه میانگین امتیازات برای پاسخ سؤالات اعداد زیر در نظر گرفته‌شده است که عبارتند از:

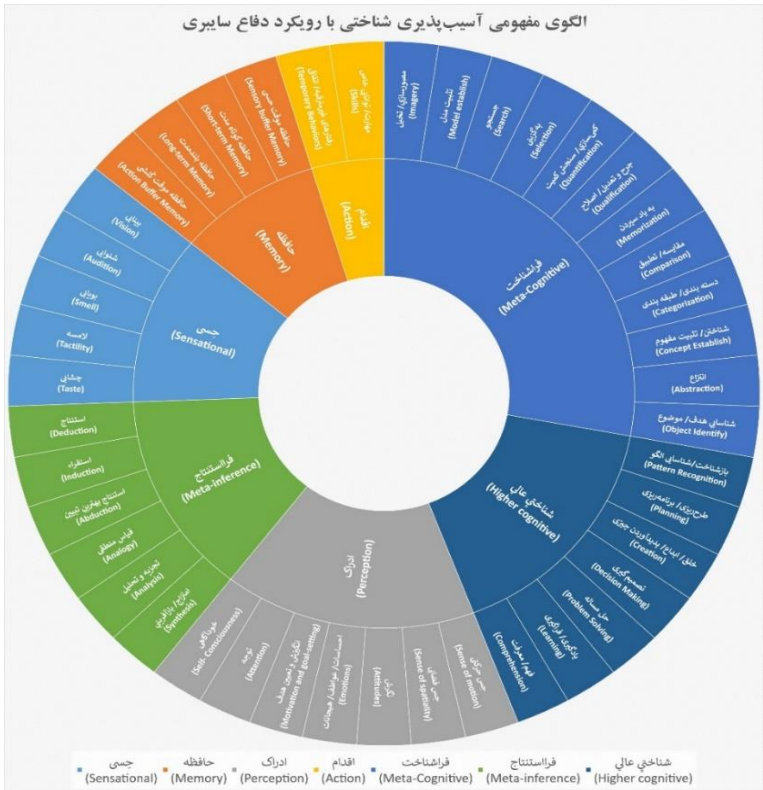
خیلی زیاد=۵، زیاد=۴، متوسط=۳، کم=۲، خیلی کم=۱

در جدول ۶: نتایج ارزیابی عمومی چهارچوب مفهومی (۶)، نتایج ارزیابی سؤالات عمومی به‌صورت میانگین امتیازات همراه با مفهوم کیفی امتیازات ذکر شده است. با توجه به پاسخ سؤالات و میانگین امتیازات کسب‌شده، وضعیت کیفی امتیاز چهارچوب مفهومی ارائه‌شده هم در بخش سؤالات عمومی و هم در بخش سؤالات اختصاصی در سطح بسیار مناسبی ارزیابی شده است.

جدول ۶: نتایج ارزیابی عمومی چهارچوب مفهومی طراحی‌شده

ردیف	محور سؤالات: ارزیابی عمومی چهارچوب مفهومی طراحی‌شده و ورودی‌های تحلیل‌شده	میانگین امتیاز	مفهوم کیفی امتیاز
۱	چه میزان چهارچوب مفهومی طراحی‌شده از جامعیت کافی برخوردار است؟	۴/۴۴	بسیار مناسب
۲	چه میزان چهارچوب مفهومی طراحی‌شده متناسب با اهداف تحقیق است؟	۴/۵۰	بسیار مناسب
۳	چه میزان حجم و کیفیت مستندات ارائه‌شده برای استفاده از چهارچوب مفهومی کافی است؟	۴/۲۷	بسیار مناسب
۴	چه میزان رویکرد چهارچوب مفهومی در استفاده از منابع مرتبط مناسب است؟	۴/۴۰	بسیار مناسب
۵	چه میزان رویکرد چهارچوب مفهومی در تبیین کارکردهای بخش‌های مختلف مناسب است؟	۳/۷۵	مناسب
۶	با توجه به بخش‌های مختلف چهارچوب مفهومی، چقدر الگو انعطاف‌پذیری لازم را دارا است؟	۳/۸۸	مناسب
۷	با توجه به استفاده از روش تحلیل مضمون در طراحی الگو، میزان قابلیت بهبود الگو چه میزان است؟	۴/۱۳	بسیار مناسب
۸	میزان سهولت فهم چهارچوب مفهومی طراحی‌شده چقدر است؟	۴/۱۳	بسیار مناسب

ردیف	محور سؤالات: ارزیابی عمومی چهارچوب مفهومی طراحی‌شده و ورودی‌های تحلیل‌شده	میانگین امتیاز	مفهوم کیفی امتیاز
۹	میزان سادگی مبانی و مفاهیم تدوین‌شده برای استفاده از چهارچوب مفهومی طراحی‌شده چقدر است؟	۴/۱۳	بسیار مناسب
۱۰	میزان وضوح و شفافیت چهارچوب مفهومی طراحی‌شده چه اندازه است؟	۴/۱۳	بسیار مناسب
۱۱	میزان تطبیق‌پذیری چهارچوب مفهومی طراحی‌شده با محیط دفاعی و امنیتی چقدر است؟	۳/۸۱	مناسب
۱۲	میزان قابلیت استفاده و کاربردی بودن چهارچوب مفهومی طراحی‌شده را در چه سطحی ارزیابی می‌کنید؟	۴/۱۳	بسیار مناسب
میانگین امتیازات		۴/۱۴	بسیار مناسب



شکل ۷: چهارچوب مفهومی آسیب‌پذیری سایبر شناختی (مدل خورشیدی)

شکل ۸: چهارچوب مفهومی آسیب‌پذیری سایبر شناختی (مدل لایه‌ای)

نتیجه‌گیری و پیشنهاد

همان‌طور که بیان گردید به‌منظور احصای چهارچوب آسیب‌پذیری سایبر شناختی، در فاز اول سعی شد با توجه به رویکرد پژوهش که دفاع سایبری است، تمامی مؤلفه‌های مهم هر دو حوزه شناختی و سایبر مدنظر باشد؛ لذا برخی از مؤلفه‌ها در مرحله اول جنبه فناوری داشتند. در فاز اول ۷ مضمون اصلی (بُعد) و ۱۰۱ مضمون فرعی (مؤلفه‌ها) شناسایی شد. سپس شبکه مضامین اولیه که شامل ۷ بُعد اصلی و ۱۰۱ مؤلفه فرعی بود، در قالب پرسش‌نامه

در اختیار خبرگان قرار گرفت و از آن‌ها خواسته‌شده که نظرات خود را از منظر «جذابیت» و «توانمندی» اعلام کنند. سپس مجدداً مضامین احصا شده اولیه توسط خبرگان مورد بازنگری قرار گرفت و با تکیه‌بر نظرات خبرگی، نمرات و امتیازات کسب‌شده پرسش‌نامه‌ها، متون منتخب منابع از قبیل مقالات، کتب و گزارش‌های معتبر مضامین دقیق‌تر شدند و سعی گردید فناوری‌های شناسایی‌شده در مرحله قبل با مؤلفه‌های شناختی متناظر خود ادغام شوند. در این مرحله ۷ مضمون اصلی (بُعد–لایه) و ۷۸ مضمون فرعی (مؤلفه‌ها) شناسایی شدند. در نهایت مضامین احصا شده مجدداً توسط خبرگان و کارشناسان این حوزه مورد بازنگری قرار گرفت که با تکیه‌بر نظرات خبرگی در این مرحله ۷ مضمون اصلی (بُعد–لایه) و ۴۳ مضمون فرعی (مؤلفه‌ها) شناسایی شدند. بنابراین سؤال اصلی پژوهش که ارائه چهارچوب مفهومی و سؤالات فرعی که ارائه ابعاد و مؤلفه‌های متناسب با آن بود، پاسخ داده شد.

پیشنهادهای پژوهش

پیشنهادها برای تحقیقات آتی عبارتند از:

- ✓ راهبردهای جلوگیری از آسیب‌پذیری سایبر شناختی با رویکرد دفاع سایبری؛
- ✓ بازطراحی نهادی در راستای جلوگیری از آسیب‌پذیری سایبر شناختی؛
- ✓ بررسی زیست‌بوم تهدیدات نوین در حوزه سایبر شناختی؛
- ✓ ترسیم ابعاد و مؤلفه‌های صحنه نبرد آینده در حوزه سایبر شناختی.

فهرست منابع

- امیرلی، حسین؛ تقی پور، رضا (۱۳۹۹). ***ارائه مدل فرایندی دفاع سایبری بومی***. امنیت ملی، ۱۰(۳۷)، ۳۵۳-۳۸۶.
- بچاری لفته، محمدرضا؛ نجفی شوشتری، سیدمنصور (۱۳۹۷). ***بررسی نقش امنیت سایبری در آینده حمل‌ونقل دریایی***. دومین همایش بین‌المللی مهندسی برق. علوم کامپیوتر و فناوری اطلاعات. همدان.
- زابلی زاده، اردشیر؛ وهاب پور، پیمان (۱۳۹۷). ***قدرت بازدارندگی در فضای سایبر***. مطالعات بین‌رشته‌ای در رسانه و فرهنگ (رسانه و فرهنگ)، ۸(۱ (پیاپی ۱۵))، ۴۷-۷۴.
- صادقی، سیدشمس‌الدّین؛ نادری، مسعود (۱۳۹۵). ***تحلیل ابعاد امنیت دولت در ایران قرن بیست‌ویکم***. دولت پژوهی، ۲(۵)، ۱۶۵-۲۰۲.
- کورکی‌نژاد قرایی، مجید (۱۳۹۴). ***تروریسم سایبری (دهشت افکنی در فضای مجازی) و راهکارهای افزایش امنیت سایبر در ایران با تأکید بر عملکرد دولت ایالات‌متحده آمریکا***. پایان‌نامه کارشناسی ارشد. دانشگاه تهران

References

- Ahmed, M. F., Molla, A. H., Uddin, M. R., & Chowdhury, T. R. (2023). Advancing cyber resilience: Bridging the divide between cyber security and cyber defense. International Journal for Multidisciplinary Research (IJFMR), 5(6).
- Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In Emerging cyber threats and cognitive vulnerabilities (pp. 73-92). Academic press.
- Darley, H. M. (2023). Dangers of succumbing to bias in cyber security: An evaluation of the impact of cognitive biases on threat assessments and cyber security strategies. Cyber Security: A Peer-Reviewed Journal, 6(3), 211-219.
- Devadarshini, P. T., Chandrashekar, B., Pundir, S., Tiwari, M., Madala, R., & Indhuma, E. (2023, September). Cognitive Defense Cyber Attack Prediction and Security Design in Machine Learning Model. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1361-1366). IEEE.
- Galinec, D. (2023). Cyber security and cyber defense: Challenges and building of cyber resilience conceptual model. International Journal of Applied Sciences & Development, 1, 83-88.
- Galvão, A., Chumbo, I., & Anes, E. (2023). Behavioural Psychology Towards Artificial Intelligence in Cybersecurity. In Exploring Cyber Criminals and Data Privacy Measures (pp. 19-39). IGI Global Scientific Publishing.
- Hakimi, M., Quchi, M. M., & Fazil, A. W. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID), 3(01), 20-33.
- Huang, L., Zhu, Q. (2023).Introduction. In: Cognitive Security. SpringerBriefs in Computer Science. Springer, Cham.
- Ivory, M. R., Towse, J. N., Sturdee, M., Levine, M., & Nuseibeh, B. (2024). Software Vulnerabilities as Cognitive Blindspots; assessing the suitability of a dual processing theory of decision making for secure coding.
- Kim, K. B., Lim, E., & Kwon, H. Y. (2023, June). Processing Model and Classification of Cybercognitive Attacks: Based on Cognitive Psychology. In ECCWS 2023 22nd European Conference on Cyber Warfare and Security (No. 1). Academic Conferences and publishing limited.
- Maennel, K., Brilingaitė, A., Bukauskas, L., Juozapavičius, A., Knox, B. J., Lugo, R. G., ... & Sütterlin, S. (2023). A multidimensional cyber defense exercise: Emphasis on emotional, social, and cognitive aspects. SAGE Open, 13(1), 21582440231156367.
- Malloy, T., & Gonzalez, C. (2023, July). Learning to defend by attacking (and vice-versa): Transfer of learning in cybersecurity games. In 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 458-464). IEEE.
- Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. Frontiers in psychology, 11, 1755.
- Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The role of user behaviour in improving cyber security management. Frontiers in Psychology, 12, 561011.

- Nardina, O. V. (2020, March). Keeping Minors Safe in Cyberspace: Extremist and Terrorist Threats. In International Scientific Conference" Far East Con"(ISCFEC 2020) (pp. 1640-1646). Atlantis Press.
- Nebieridze, M. (2023). Collective Cyber Defense: Legalization of Cyberspace. In Cyber Security Policies and Strategies of the World's Leading States (pp. 129-149). IGI Global.
- Nobles, C., & McAndrew, I. (2023). The intersectionality of offensive cybersecurity and human factors: A position paper. Scientific Bulletin-Nicolae Balcescu Land Forces Academy, 28(2), 215-233.
- Rangrez, U. S., Qadri, S. A., Kumar, C. A., & Kumar, C. J. (2024, May). Cyber-attack defense system enhanced by artificial intelligence. In 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS) (pp. 1-5). IEEE.
- Riskind, J. H., & Alloy, L. B. (2006). Cognitive vulnerability to psychological disorders: Overview of theory, design, and methods. Journal of Social and Clinical Psychology, 25(7), 705-725.
- Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. Human factors, 60(5), 597-609.
- Singh, B., & Cheema, S. S. (2024). Psychology in cybersecurity: unveiling the human dimensions of digital resilience. International Journal of Advanced Networking and Applications, 16(1), 6281-6290.
- Sugumaran, D., John, Y. M., Joshi, K., Manikandan, G., & Jakka, G. (2023, April). Cyber defence based on artificial intelligence and neural network model in cybersecurity. In 2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) (pp. 1-8). IEEE.
- Taylor-Jackson, J., McAlaney, J., Foster, J. L., Bello, A., Maurushat, A., & Dale, J. (2020, February). Incorporating psychology into cyber security education: a pedagogical approach. In International Conference on Financial Cryptography and Data Security (pp. 207-217). Cham: Springer International Publishing.
- Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018). Simulations in cyber-security: a review of cognitive modeling of network attackers, defenders, and users. Frontiers in psychology, 9, 691.
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.