Shahid Sattari Aeronautical University
of Science and Technology

Journal of Innovation Management in Defensive Organizations
ISSN: 2676-7112
Volume 5, Issue 16
Summer 2022
P.P.127-148

Development an Innovative Model of Cyber Defense With an Integrated Approach to Data Access in Data-Driven Organizations

Mohamed-Ali Mahamed[1], Nadjla Hariri[2], Fahimeh Babolhavaeji[3]

Abstract

Background & Purpose: Due to the ever-increasing growth of technologies, the use of big data, which is the result of the integrated approach to data access, is an undeniable necessity. The use of a cyber defense model in the mentioned field, which is the goal of the present research, can improve the identification, reduce risks and prevent cyber attacks and threats on the organization's data infrastructures and repositories.

Methodology: This research is applied research in terms of purpose and descriptive-exploratory in terms of research method. In the first phase of the research, in order to identify the elements of the model, 15 cyber defense experts and experts working in data-oriented organizations were selected by purposive sampling and participated in the Delphi panel. In the second phase, in order to validate the model, 288 employees of data-oriented organizations were selected by simple random sampling method. The data collection tool is a questionnaire and the Delphi method and structural equation modeling were used to analyze the data.

Findings: The findings of the research indicated the identification of 5 dimensions with 21 components and 70 indicators for the innovative model of cyber defense with the approach of data access integration in data-oriented organizations. The dimensions of the model included identification, protection, discovery, response and recovery, which had the greatest explanatory power among these dimensions of response and protection.

Conclusion: According to the study and the competitive environment in the present era, it is necessary for data-driven organizations to use the model presented in this study to implement the necessary planning for the implementation of cyber defense in the field of data access integration in their organizations.

Keywords: : *Data-Driven Organization, Data Access Integrity, Cyber Defense Pattern, Delphi method, Confirmatory factor analysis.*

Citation: Mohamed, Mohammad-Ali; Hariri, Najla and Babolhavaeji, Fahimeh.(2021). Development an Innovative Model of Cyber Defense With an Integrated Approach to Data Access in Data-Driven Organizations. *Journal of of Innovation Management In Defensive Organization*, 5(16), 127-148.

---

1. Ph.D. Student, Department of communication Science and Knowledge, Science and Research Branch Islamic Azad University, Tehran, Iran. **E-mail: Masterit_ali@yahoo.com**

2. Professor, Department of communication Science and Knowledge, Science and Research Branch Islamic Azad University, Tehran, Iran. **E-mail: Nadjlahariri@gmail.com**

3. Associate Professor, Department of communication Science and Knowledge, Science and Research Branch Islamic Azad University, Tehran, Iran. **E-mail: F.babalhavaeji@gmail.com**

Received: 21/01/2022 **Article Type: Research-based**
Accepted: 30/04/2022 **DOI: 10.22034/qjimdo.2022.325763.1480**
Corresponding Author: Nadjla Hariri

دانشکده مدیریت

فصلنامهٔ مدیریت نوآوری در سازمان‌های دفاعی
شاپای انتشار:۷۱۱۲-۲۶۷۶
دورهٔ۵، شمارهٔ ۱۶
تابستان ۱۴۰۱
صص ۱۲۷-۱۴۸

تدوین الگوی نوآورانه پدافند سایبری با رویکرد یکپارچگی دسترسی به داده‌ها در سازمان‌های داده‌محور

محمد علی محامد[۱]، نجلا حریری[۲]، فهیمه باب الحوائجی[۳]

چکیده

زمینه و هدف: با توجه به رشد روزافزون فن‌آوری‌ها، بهره‌گیری از داده‌های عظیم که منتج از رویکرد یکپارچگی دسترسی به داده‌ها است، ضرورتی انکارناپذیر می‌باشد. استفاده از یک الگوی پدافند سایبری در حوزه مذکور، که هدف پژوهش حاضر است که می‌تواند موجب ارتقای شناسایی، کاهش مخاطرات و ممانعت از حملات و تهدیدات سایبری متصور بر مخازن و زیرساخت‌های داده‌ای سازمان گردد.

روش‌شناسی: این تحقیق از نظر هدف کاربردی بوده و از نظر روش پژوهشی توصیفی–اکتشافی است. در فاز اول تحقیق به منظور شناسایی عناصر الگو، تعداد ۱۵ نفر از خبرگان و صاحب‌نظران پدافند سایبری و شاغل در سازمان‌های داده‌محور به روش نمونه گیری هدفمند انتخاب و در پانل دلفی مشارکت کردند. در فاز دوم به منظور اعتبارسنجی مدل، تعداد ۲۸۸ نفر از کارکنان سازمان های داده‌محور به روش نمونه گیری تصادفی ساده انتخاب شدند. ابزار گرداوری داده ها پرسشنامه بوده و برای تحلیل داده ها از روش دلفی و مدل یابی معادلات ساختاری استفاده شده است.

یافته‌ها: یافته‌های تحقیق حاکی از شناسایی ۵ بُعد با ۲۱ مولفه و ۷۰ شاخص برای الگوی نوآورانه پدافند سایبری با رویکرد یکپارچگی دسترسی به داده‌ها در سازمان‌های داده‌محور بود. ابعاد مدل شامل شناسایی، حفاظت، کشف، پاسخگویی و بازیابی بوده است که در بین این ابعاد پاسخگویی و حفاظت بیشترین قدرت تبیین کنندگی را داشتند.

نتیجه‌گیری: با توجه به مطالعه انجام شده و همچنین وجود فضای رقابتی در عصر حاضر، ضروریست سازمان‌های داده‌محور با بهره‌گیری از الگوی ارائه شده در این پژوهش برنامه‌ریزی لازم را در خصوص اجرای پدافند سایبری در حوزه یکپارچگی دسترسی به داده‌ها در سازمان‌های خود به‌عمل آورند.

کلیدواژه‌ها: *سازمان داده‌محور، یکپارچگی دسترسی به داده، الگوی پدافند سایبری، روش دلفی، تحلیل عاملی تاییدی.*

استناد: محامد، محمدعلی؛ حریری، نجلا و باب الحوائجی، فهیمه. (۱۴۰۱). تدوین الگوی نوآورانه پدافند سایبری با رویکرد یکپارچگی دسترسی به داده‌ها در سازمان‌های داده‌محور. *فصلنامه مدیریت نوآوری در سازمان‌های دفاعی*، ۵(۱۶)، ۱۲۷-۱۴۸.

---

۱. دانشجوی دکترای علم اطلاعات و دانش شناسی گرایش مدیریت دانش، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران.
رایانامه: Masterit_ali@yahoo.com

۲. استاد گروه علوم ارتباطات و دانش‌شناسی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران. **رایانامه:** Nadjlahariri@gmail.com

۳. دانشیار گروه علوم ارتباطات و دانش‌شناسی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران. **رایانامه:** F.babalhavaeji@gmail.com

---

نوع مقاله: پژوهشی
DOI: 10.22034/qjimdo.2022.327013.1481

تاریخ دریافت مقاله: ۱۴۰۰/۱۱/۰۱
تاریخ پذیرش نهایی مقاله: ۱۴۰۱/۰۲/۱۰
نویسنده مسئول مقاله: نجلا حریری

مقدمه

یک سازمان داده‌محور، سازمانی است که تفکر استفاده مستمر از داده جهت تجزیه و تحلیل و تصمیم‌گیری مبتنی بر بینش در تاروپود آن پرورش و نهادینه شده باشد. در این نوع سازمان‌ها، استفاده از داده و تحلیل توسط مدیران و کارکنان به بخشی تفکیک‌ناپذیر از جریان‌های کاری روزمره تبدیل شده است (گاست بلوگار[1]، ۲۰۱۶). استفاده صحیح و به موقع از دارایی‌های داده به منظور تصمیم‌گیری سریعتر بستر مناسب جهت هدایت سازمان به سمت موفقیت را فراهم می‌نماید. سازمان‌های داده‌محور با استفاده حداکثری از داده و تجزیه و تحلیل (استفاده از داده صحیح در زمان مناسب برای تصمیم‌گیری قطعی) قادر به تمایز خود با سایر رقبا می‌باشند (فرابر، ۱۳۹۷).

با افزایش میزان بهره‌برداری و همه‌گیر شدن استفاده از قابلیت‌های فضای سایبری، تهدیدات متصور این فضا و به تبع آن پیچیدگی‌های مربوطه، دفاع و پدافند در این فضا را پیچیده‌تر نموده است. حملات و سوءاستفاده‌های سایبری بر زیرساخت‌های تبادل داده به ویژه اینکه این مهم منجر به خلق پارادایمی چون داده‌های عظیم و سامانه‌های تعامل‌پذیر یکپارچه گردیده است، بسیار تاثیرات جبران‌ناپذیری را به همراه داشته است. اطلاعات در سازمان‌های دولتی، خصوصی و حتی در کاربردهای فردی به عنوان مولد سرمایه فکری و سرمایه سازمانی است. همانطور که مجموعه‌ها برای حفظ دارایی‌های سنتی خود مجدانه تلاش می‌کنند و از تمهیدات لازم فیزیکی بهره می‌گیرند تا میزان آسیب را به حداقل برسد، رصد و پایش مستمر فضای سایبری و بکارگیری سامانه‌های دفاع در عمق در سازمان‌های داده‌محور به منظور حفظ سرمایه‌های اطلاعاتی نیز بسیار حائز اهمیت می‌باشد (عرب سرخی، ۱۳۹۶). یک سازمان داده‌محور، می‌تواند به کلیه اعضای سازمان امکان دسترسی سریع به اطلاعات مورد نیاز را داده باشد، تا بتواند در طی چند ثانیه تصمیمات داده‌محور را اتخاذ نماید (پریگود[2]، ۲۰۱۸). ایجاد و بهره‌برداری از الگوی پدافند سایبری در سازمان‌های داده‌محور باعث دستیابی به موارد زیر می‌گردد که مبین ضرورت و اهمیت تحقیق است:

- حفظ، نگهداری و پدافند سایبری منابع و سرمایه‌های اطلاعاتی سازمان.
- رویکردی جدید در طرح مسئله و مطالعات آتی به منظور ایجاد سامانه‌های هوشمند و خبره در حوزه پدافند سایبری.

---

[1]. Gästbloggare
[2]. Peregud

- توان پاسخگویی و اجرای فرآیندهای پدافند سایبری در حداقل زمان ممکن با رویکرد دفاع در عمق با بهره‌گیری از سامانه‌های نرم‌افزاری، سخت‌افزاری و زیرساخت‌های ارتباطی امن.

عدم دستیابی به چنین الگویی، باعث بروز آسیب‌های محتمل بر دارایی‌های داده‌های سازمان و به تبع آن اختلال در تصمیم‌سازی، تصمیم‌گیری و به تبع آن ممانعت از کسب موقعیت بهتر و یا حتی حفظ وضع موجود در فضای کسب و کار رقابتی شده و ضریب دسترسی‌های غیرمجاز را افزایش می‌دهد. سازمان‌های داده محور با بهره‌گیری از یک الگوی پدافند سایبری که برگرفته از تجربیات خبرگان و افراد متخصص و صاحب نظر حوزه سایبر در ایجاد و به‌کارگیری لایه‌های امنیتی و همچنین سامانه‌های امنیتی می‌باشد، می‌توانند تحولی شگرف در شناسایی، کاهش مخاطرات و ممانعت از حملات و تهدیدات سایبری متصور بر مخازن داده‌ای سازمان به عنوان سرمایه ارزشی و منبع حیاتی سازمان، داشته باشند. لذا این پژوهش در نظر دارد الگویی برای پدافند سایبری در سازمان‌های داده‌محور ارائه نماید.

نتایج حاصل از پژوهش حاضر و بررسی سایر مطالعات انجام شده در خصوص موضوعات پدافند سایبری و سازمان‌های داده‌محور، بیانگر آن است که هیچ‌یک از مطالعات و پژوهش‌های قبلی، به بررسی وضعیت سایبری و نحوه پدافند سایبری در سازمان‌های داده‌محور نپرداخته‌اند، اما موارد احصاء شده از این پژوهش‌ها که عمدتاً با موضوعاتی عام (مواردی کلی و غیرمرتبط به مقوله کاربرد پدافند سایبری در سازمان داده‌محور) مورد مطالعه قرار گرفته و در آنها مواردی همچون بازیابی داده‌ها، مخازن نگهداری، نگهداری سرورها، ساختار و سازمان، نظارت بر یکپارچگی شبکه، محافظت از اطلاعات، هویت سنجی، نظارت مستمر امنیتی، آموزش و یادگیری سازمانی، هوشمندی، سیاست لایه‌ای و دفاع در عمق، ارتقاء پاسخگویی، ارزیابی مخاطرات، شناسایی تهدیدات، جداسازی محیط، آگاهی‌رسانی و اطلاع‌رسانی، مدیریت ریسک، فرهنگ، مشاغل مرتبط با سایبر، تاب‌آوری و قالب‌ها و نوع‌های داده‌ای، مورد جمع‌بندی و توصیه قرار گرفته‌اند، لذا پژوهش حاضر مبتنی بر توصیه‌ها و نتایج حاصل از مراجع مذکور بوده و از دیدگاه مدیریت سایبری در سازمان‌های داده‌محور، پژوهشی نوآورانه می‌باشد.

پیشینهٔ پژوهش

کلان‌داده‌ها؛ کلان‌داده‌ها به مجموعه داده‌هایی اشاره دارد که با استفاده از روش‌های سنتی فناوری اطلاعات و ابزارهای سخت‌افزاری و نرم‌افزاری موجود در آن نمی‌توانند در زمان

معقولی درک، گردآوری، مدیریت و پردازش شوند. کلان‌داده‌ها روش‌ها و فناوری‌های نوینی را جهت جمع‌آوری، ذخیره و آنالیز داده‌های غیرساخت‌یافته به صورت مقیاس‌پذیر معرفی می‌کند. آنچه که کلان‌داده‌ها و به دنبال آن فناوری‌های مرتبط با آن را از مفاهیم قبلی (نظیر انبار داده[۱]، هوش تجاری[۲] و غیره) متمایز می‌سازد، امکان پاسخ‌گویی به چالش‌هایی است که تاکنون یا وجود نداشته‌اند و یا امکان پاسخ‌گویی به آنها وجود نداشته است. این چالش‌ها، که از خصوصیات کلان‌داده‌ها محسوب می‌شوند، شامل حجم داده، سرعت، تنوع، صحت، اعتبار، نوسان، نمایش و ارزش[۳] می‌باشند: (کلکلی و رجایی، ۱۳۹۶).

به‌کارگیری فناوری کلان داده‌ها در سازمان مستلزم استفاده از طیفی از فناوری‌ها در مجموعه‌ای از فرآیندهای سازمان می‌باشد. مهم‌ترین تصمیمی که در تشکیل تیم‌های علم داده گرفته می‌شود، این است که این تیم به صورت متمرکز یا غیرمتمرکز کار کنند. متمرکز شدن تیم این امکان را به اعضای تیم می‌دهد، که تجربیاتشان را با هم به اشتراک بگذارند. این روش مطمئن‌ترین روش برای آغاز به کار یک تیم علم داده است، حتی اگر در درازمدت قصد داشته باشید تیم را به صورت غیرمتمرکز اداره کنید، چون این روش باعث می‌شود که اعضاء تیم یک رویه مشخص را در فرایندها به کار بگیرند(سهرابی و ایرج، ۱۳۹۴).

در روش غیرمتمرکز اعضای تیم علم داده عضوی از تیم کسب و کار نیز هستند. این ساختار سازمانی اعضای تیم علم داده را با سازمان همسو می‌کند ولی درگیر شدن در فعالیت‌های علمیاتی واحدهای کسب و کار تیم علم داده را به سمت تحلیل فعالیت‌های گذشته می‌برد و نقشی که این تیم می‌تواند در پیش‌بینی وضعیت آینده داشته باشد، کم‌رنگ می‌شود. تیم‌های غیرمتمرکز معمولا هماهنگ کار نمی‌کنند و همین امر باعث بوجود آمدن مشکلاتی برای تجمیع این فعالیت‌های واحدها می‌شود(دینس‌مور[۴] و همکاران، ۲۰۱۴).

سازمان‌های داده‌محور[۵]؛ جوامع امروز را جوامع سازمانی می‌نامند، زیرا در دنیای امروز، سازمان، همه جوانب زندگی را فرا گرفته‌اند. سازمان عبارتست از پدیده‌ای اجتماعی یا گروهی متشکل از دو یا چند نفر که در محیطی با ساختار منظم به طور آگاهانه، هماهنگ شده و برای نیل به اهداف گروهی، با یکدیگر همکاری می‌کنند. (اصغری، ۱۳۹۲) به‌کارگیری فناوری کلان داده‌ها در سازمان مستلزم استفاده از طیفی از فناوری‌ها در مجموعه‌ای از

---

[1]. Data Warehouse
[2]. Business Intelligence
[3]. Volume, Velocity, Variety, Veracity, Validity, Volatility, Visualization Value
[4] Dinsmore
[5]. Data Driven Organization

فرآیندهای سازمان می‌باشد. یکی از عواملی که در موفقیت پروژه‌های داده در یک سازمان موثر است، موفقیت در استقرار سیستم‌های اطلاعاتی است که تولیدکننده این داده‌ها هستند. اگر سیستم‌های اطلاعاتی به درستی پیاده‌سازی نشده باشند و مورد پذیرش سازمان قرار نگرفته باشند، طبیعتاً داده‌هایی که در این سیستم‌ها ثبت شده است، با واقعیت تفاوت خواهد داشت و تهیه هیچ گزارشی یا اجرای هیچ الگوریتمی نمی‌تواند ارزشی برای سازمان ایجاد کند. بنابراین پذیرش سیستم‌های اطلاعاتی پیش‌نیاز ایجاد داده‌های درون سازمانی درست و قابل استفاده است(سهرابی و ایرج، ۱۳۹۴).

تفاوت‌های سازمان‌های داده‌محور با سایر سازمان‌ها؛ مکافی و همکاران، تفاوت‌های سازمان‌های داده‌محور با سایر سازمان‌ها را در تدوین فرضیه‌ها و حل مساله می‌دانند. سازمان‌های داده‌محور از نوعی روش علمی در کار با داده‌ها استفاده می‌کنند، که شامل موارد زیر است؛

- شروع به کار با داده‌ها،
- کاوش در داده‌ها و سوال‌هایی که با داده‌ها می‌توان پاسخ داد،
- فرموله کردن سوال،
- بررسی داده‌های فعلی برای یافتن سوال درست برای مطرح کردن،
- ایجاد چارچوبی برای اجرای آزمایش روی داده‌ها،
- تحلیل نتایج برای ایجاد بینش‌های جدید راجع به سوال (برینژوفسون[1] و همکاران، ۲۰۱۴).

پدافند سایبری و چارچوب امنیت سایبری[2]؛ به اقداماتی که برای ایجاد امنیت در فضای سایبر انجام می‌شود، اقدامات پدافند سایبری می‌گویند. (ابوالحسینی، ۱۳۹۲). در تعریف جامع تر پدافند سایبری عبارت است از مجموعه اقدامات سایبری و غیرسایبری است که توانمندی رصد، پایش، تشخیص تهدید، استخراج آسیب‌پذیری، تجزیه و تحلیل میزان خطر، مدیریت و کنترل تهاجم سایبری، بازیابی اطلاعات و تولید قدرت پاسخگویی به تهدید سایبری دشمن را ایجاد کند و موجب مصون‌سازی، کاهش آسیب‌پذیری و حفاظت از سرمایه‌های ملی سایبری و زیست بوم سایبری کشور شود و با تولید بازدارندگی امکان تهاجم سایبری را از کلیه متخاصمین سلب نماید(سند راهبردی پدافند سایبری کشور، ۱۳۹۴).

---

[1]. Brynjolfsson
[2]. NIST Cyber Security Framework

چارچوب امنیت سایبری در سال۲۰۱۴ توسط ان.آی اس.تی[1] و با هدف ارائه یک چارچوب برای ارتقاء امنیت سایبری زیرساخت‌های حیاتی منتشر و در سال ۲۰۱۷ به‌روزرسانی شد. این چارچوب در سراسر جهان مقبولیت زیادی کسب کرده و از زمان انتشار تاکنون یکی از بخش‌های اصلی مذاکرات و صحبت‌های امنیت سایبری زیرساخت‌های حیاتی در آمریکا و دیگر کشورهای جهان بوده است. این چارچوب با تکیه بر استانداردها، دستورالعمل‌ها و شیوه‌ها، یک طبقه‌بندی مشترک را برای سازمان‌ها فراهم می‌کند. چارچوب فوق از سه بخش تشکیل شده است: هسته چارچوب، لایه پیاده‌سازی چارچوب، پروفایل‌های چارچوب. در اینجا تنها بخش هسته چارچوب فوق‌الذکر بررسی می‌گردد (اِن.آی.اِس.تی[2]، ۲۰۱۷). هسته‌ی چارچوب امنیت سایبر ان.آی اس.تی مجموعه‌ای از فعالیت‌ها، خروجی‌های مطلوب و مراجع مرتبط با این فعالیت‌ها است، که در میان زیرساخت‌های حیاتی مقبولیت بیشتری دارند. این بخش(هسته) شامل پنج عملکرد اصلی است: شناسایی، حفاظت، کشف، پاسخ‌گویی، بازیابی[3]؛ این پنج عملکرد اصلی چرخه عمر مخاطرات امنیت سایبری را پوشش داده و مدیریت می‌کنند. ذیل هر کدام از این عملکردهای اصلی، دسته‌ها و زیردسته‌هایی (از فعالیت‌های امنیت سایبری) قرار می‌گیرند و در نهایت برای هر کدام از این دسته‌ها و زیردسته‌ها مراجع اطلاعاتی و استانداردهای مرتبط (نظیر CCS[4]، ANSI/ISA[5]، ISO/IEC و Cobit، به منظور بهره برداری) معرفی می‌گردند. شرح پنج عملکرد اصلی در زیر ارائه شده است:

شناسایی: ایجاد و توسعه درک سازمانی در رابطه با مدیریت مخاطرات امنیت سایبری سیستم، دارایی‌ها، داده و قابلیت‌ها. فعالیت‌های این عملکرد به عنوان مبنا و پایه‌ای برای استفاده موثر از چارچوب قلمداد می‌شوند. درک محیط تجاری (محیط ماموریت‌های سازمانی)، منابعی که خدمات حیاتی را پشتیبانی می‌کنند و مخاطرات امنیت سایبری متوجه آنها سازمان را قادر می‌سازد تا تلاش‌های خود در حوزه امنیت سایبری را مطابق با نیازهای سازمانی و استراتژی‌های مدیریت مخاطره خود متمرکز و اولویت‌دهی نماید.

حفاظت: توسعه و به‌کارگیری حفاظ‌های (کنترل‌های حفاظتی) مناسب به منظور اطمینان از استمرار ارائه خدمات زیرساخت‌های حیاتی. فعالیت‌های ذیل این عملکرد توانایی محدودکردن یا مقابله با تاثیرات رویدادهای بالقوه امنیت سایبری را تامین می‌کنند. مثال‌هایی

---

[1]. NIST: National Institute of Standards and Technology
[2]. NIST
[3]. Identify, Protect, Detect, Respond, Recover
[4]. Retrievable from: http://www.counciloncybersecurity.org
[5]. Retrievable from: https://www.isa.org/templates/one

از فعالیت‌های زیرمجموعه این عملکرد عبارتند از: کنترل دسترسی، آموزش و آگاه‌سازی، امنیت داده.

کشف: توسعه و به‌کارگیری اقدامات مناسب (شامل کنترل‌های امنیتی نظارت و کشف) به منظور شناسایی رویداد امنیت سایبری که ممکن است حادث شود. این عملکرد، قابلیت کشف رویدادهای امنیت سایبری در الگوی زمانی قابل قبول را فراهم می‌کند.

پاسخگویی: توسعه و به‌کارگیری اقدامات مناسب به منظور برخورد و واکنش به رویدادهای امنیت سایبری کشف شده. این عملکرد امکان محدودکردن دامنه تاثیرات رویدادهای سایبری را فراهم می‌کند.

بازیابی: توسعه و به‌کارگیری فعالیت‌ها و اقدامات مناسب به منظور ایجاد ویژگی تاب‌آوری و بازیابی هر قابلیت یا خدمتی که بخاطر رویدادهای امنیت سایبری تضعیف یا مختل شده‌اند (اِن.آی.اِس.تی[1]، ۲۰۱۷).

پیشینه تجربی

به استناد بررسی انجام شده بر روی پیشینه‌ها و مستندات چاپی و اینترنتی در دسترس، پژوهش‌ها و مطالعات متعددی توسط سایر پژوهشگران در خصوص موضوعات سایبر، امنیت داده، داده‌کاوی، کلان‌داده‌ها و غیره به صورت کلی صورت پذیرفته است، که در این بخش به صورت مختصر به چند نمونه از آنها اشاره می‌گردد.

رمضان‌زاده و همکارن (۱۴۰۰) پژوهشی از نوع کاربردی با عنوان "بررسی قدرت پدافند سایبری نیروهای مسلح با روش برنامه‌ریزی مبتنی بر سناریو" انجام داده‌اند، و نتیجه آنکه رویکرد پدافند سایبری دارای مؤلفه‌های چهارگانه شامل: بستر پدافندی، دیپلماسی سایبری، عامل انسانی و افزارها می‌باشد، و مؤلفه عامل انسانی، از اولویت بالاتری نسبت به سایر مؤلفه‌ها برخوردار است. کتابچی و بابک‌پور (۱۴۰۰) پژوهشی با عنوان "چالش‌های امنیتِ سایبری در کشورهای « آسه‌آن»" را با بهره‌گیری از روش پژوهش توصیفی- تحلیلی انجام داده‌اند و نتایج پژوهش حاکی از آن بود که زمینه‌های امنیت سایبری، از جمله دفاع در برابر حملات سایبری نوآورانه، راهبردهایی در برابر تهدیدات سایبری، سیاست‌های دولت و محافظت در برابر حریم خصوصی، محافظت از زیرساخت‌های رایانه‌ای در دولت و مسائل حقوقی و اخلاقی در فضای سایبری می‌بایست توسط اعضاء «آسه آن» مورد توجه قرار گیرد. مردیها (۱۳۹۸) پژوهشی با موضوع " افزایش داده‌ها و پیشرفت علم" را با استفاده از روش

---

[1]. NIST

تحقیق استنادی و کتابخانه‌ای به انجام رسانده است، که با بررسی شاخص‌ها به چرایی واقعه پرداخته و بر این نکته متمرکز می شود که انبوهی داده‌ها مشکل چندانی از رشد علم حل نمی‌کند؛ زیرا رشد علم در گرو فرضیات آزمون‌پذیر است و داده‌های انبوه‌تر و گرفتن متغیرهای بیشتر امکان فرضیه‌پردازی را دشوار می‌کند. مانیان و همکاران (۱۳۹۵) پژوهشی را با موضوع "طراحی الگوی داده‌کاوی پیشنهادی به منظور شناسایی مجرمان" با استفاده از روش پژوهش داده‌بنیان انجام داده است که در آن با بهره‌گیری از روش‌های مختلف ساخت الگو مانند درخت تصمیم و شبکه‌های عصبی، الگوی مربوطه را با تمرکز روی داده و بهره‌گیری از تجمیع داده‌ها در مدیریت دانش ارائه نموده است.

در بین تحقیقات خارجی نیز، میاو[1]و همکاران (۲۰۲۲) پژوهشی را با عنوان "حملات سایبری مبتنی بر یادگیری ماشین با هدف کنترل اطلاعات کنترل شده: یک نظرسنجی" با بهره‌گیری از روش کتابخانه‌ای و استنادی انجام داده اند و در آن بکارگیری راه حل های تجزیه و تحلیل پیشرفته، حملات جدید سرقت از الگوریتم های یادگیری ماشین برای دستیابی به میزان موفقیت بالا و ایجاد خسارت زیاد استفاده پرداخته اند، به طوریکه تشخیص و دفاع در برابر چنین حملاتی چالش برانگیز و فوری شناسایی گردیدند و بنابراین دولت ها، سازمان ها و افراد باید اهمیت زیادی برای حملات سرقت مبتنی بر یادگیری ماشین (حملات هوشمند) که شامل سه دسته از حملات (فعالیت های کنترل شده کاربر، اطلاعات مربوط به مدل یادگیری ماشین کنترل شده و اطلاعات احراز هویت کنترل شده) می باشد، قائل شوند.

ما[2] (۲۰۲۲) پژوهشی را با عنوان "رفتار امنیت اطلاعات متخصصان سیستم اطلاعات در سازمان‌های فناوری اطلاعات چین برای حفاظت از امنیت اطلاعات" با بهره‌گیری از روش پژوهش پیمایشی راه‌های ایجاد انگیزه در متخصصان سیستم‌های اطلاعاتی برای حفاظت از امنیت اطلاعات در برابر خطرات احتمالی، با تکیه بر چارچوب‌های نظری نظریه انگیزش حفاظتی و نظریه رفتار برنامه‌ریزی شده و نیز سوابق سازمانی مرتبط با کار (به عنوان مثال، تعهد سازمانی و رضایت شغلی) را مورد بررسی قرار داد، و نتایج حاصل بیانگر آن بود که نگرش‌های امنیت اطلاعات و هنجارهای ذهنی، رفتارهای حفاظتی امنیت اطلاعات را به‌طور قابل توجهی تحت تأثیر قرار می‌دهند و ارزیابی مقابله (خودکارآمدی و هزینه پاسخ) و ارزیابی تهدید (حساسیت تهدید و شدت تهدید) به‌طور قابل توجهی رفتارهای حفاظتی امنیت اطلاعات را پیش‌بینی می‌کرد، و همچنین تعهد سازمانی بر رفتارهای حفاظتی

---

[1]. Miao
[2]. Ma

امنیت اطلاعات تأثیر مثبت داشت و ارتباط نزدیک بـا زیردسـتان نقـش مهمـی در تضـمین امنیت اطلاعات ایفا می‌کند. سااورا[1] و همکاران (۲۰۲۱) پژوهشی را با عنوان"از داده تولیـدی کاربر به نـوآوری داده‌محـور: تحقیقـی مطـرح شـده بـرای فهـم حـریم خصـوص کـاربر در فروشگاه‌های دیجیتال" با هدف ارائـه درک جـامع از چالش‌هـای اصـلی مربـوط بـه حـریم خصوصی کاربران انجام دادند و در آن با استفاده از روش پژوهش سـه مرحلـه‌ای: (۱) مـرور ادبیات سیستماتیک؛ (۲) مصاحبه‌های عمیق در مورد نگرانی‌های مربوط به حـریم خصوصـی کاربران؛ (۳) مدل سازی موضوع با استفاده از یـک مـدل تخصـیص نهفتـه بـرای اسـتخراج بینش‌های مربوط به موضوع مطالعه، پژوهش انجـام گردیـده اسـت. بِرِسـیانی[2] و همکـاران (۲۰۲۱) پژوهشی را با عنوان " استفاده از داده‌های عظیم برای فرآیندهای نوآوری مشـترک: ترسیم زمینه نوآوری مبتنی بر داده ، پیشنهاد تحولات نظری و ارائه دستور کار تحقیقاتی" به عنوان اولین بررسی ادبی سیستماتیک در مورد ارتباط بین داده‌های عظیم و نوآوری مشـترک انجام دادند. از داده‌های عظیم به عنوان دیدگاه مشترک تجزیه و تحلیل و همچنـین مفهـوم تجمیع جریان‌های مختلف تحقیق (نوآوری باز، ایجاد مشترک و نوآوری مشـارکتی) اسـتفاده می‌گردد. هوساک[3] و همکاران (۲۰۲۱) پژوهشی را با عنوان "روش‌هـای پیش‌بینـی در دفـاع سایبری: تجربیات و چالش‌های تحقیقاتی کنونی" بـه انجـام رسـانده‌انـد و در آن جنبـه‌های مختلف روش‌های پیش‌بینی در دفاع سایبری را مورد بحث قرار دادند. روش اول از داده‌کاوی بـرای اسـتخراج سـناریوهای حملـه مکـرر اسـتفاده می‌کنـد. در روش دوم از نمـره شـهرت موجودیت شبکه پویا برای پیش‌بینی بازیگران مخرب اسـتفاده می‌گـردد و در روش سـوم از تجزیه و تحلیل سری‌های زمانی برای پیش‌بینی میزان حملات در شبکه استفاده می‌نمایند.

لینِن و مِیِر[4] (۲۰۲۱) پژوهشی را با عنوان "هوش مصنوعی و تجزیه و تحلیل داده‌های بزرگ در حمایت از دفاع سایبری" و با هدف مفیـد بـودن تشـخیص الگوهـا، همبسـتگی‌ها، روندها و سایر اطلاعات و اینکـه تحلیلگـران امنیـت سـایبری، بـرای پیش‌بینـی، شناسـایی، توصیف و مقابله با تهدیدات امنیتی به حجم وسیعی از داده‌های رویداد امنیتی متکی هسـتند، انجام داده‌اند. بِرندسون[5] و همکاران (۲۰۲۰) پژوهشی را با عنوان "۱۳ تلاش سازمان‌ها برای تبدیل شدن به داده‌محور" از نوع کتابخانه‌ای و استنادی، ضمن انجام مصاحبه با هدف تبدیل

---

[1]. Jose RamonSaura
[2]. Stefano Bresciani
[3] Stefano Bresciani
[3]. Martin Husák
[4]. Louise Leenen and Thomas Meyer
[5]. Berndtsson

شدن به یک سازمان داده‌محور به عنوان چشم انـدازی بـرای سـازمان‌های مختلـف، انجـام داده‌اند. بارها در ادبیات ذکر شده است که سـازمان‌های مبتنـی بـر داده احتمـالاً موفـق‌تر از سازمان‌هایی هستند که به صورت سنتی تصمیم‌گیری می‌کنند.

روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف کاربردی است و از نظـر ماهیـت و روش انجـام آن توصـیفی – اکتشافی است که با بهره‌گیـری از روش‌هـای دلفـی و پیمایشـی تحلیلـی از ضـمن مطالعـه چارچوب‌ها انجام گرفتـه اسـت. در ایـن تحقیـق بـرای مطالعـه پدافنـد سـایبری، چـارچوب اِن.آی.اِس.تی با توجه به ماهیت (نو بودن، جامعیت و توصیه خبرگان حوزه پدافنـد سـایبری) شناسایی و انتخاب شده است. سپس پرسشنامه‌ای ساخت‌یافتـه مبتنـی بـر ابعـاد، مولفـه‌ها و شاخص‌های پدافند سایبری و حـوزه یکپـارچگی دسترسـی بـه داده سـازمان‌های داده‌محـور طراحی و با بهره‌گیری از روش دلفی و استفاده از نظر خبرگان مورد مطالعه قرار گرفـت و در نهایت به منظور سنجش و ارزیابی از روش پیمایشی تحلیلی و الگوسازی معادلات ساختاری، که به محقق کمک می‌کند تا پژوهش خود را از نظر مطابقت مدل نظری (مـدل تئـوری) بـا داده‌های واقعی (داده‌های تجربی) مورد بررسی قرار دهد، استفاده شده است.

در این تحقیق تعداد ۱۵ نفر از خبرگـان و صـاحب‌نظران پدافنـد سـایبری و شـاغل در سـازمان‌های داده‌محـور بـه منظـور اجـرای روش دلفـی انتخـاب گردیدنـد. در فـاز دوم تحقیق(اعتبارسنجی) نیز با توجه به مطالعات و بررسی‌های انجام شده در مجمـوع تعـداد ۸۶ سازمان شناسایی گردیدند، که از این تعداد، ۴۴ سازمان داده‌محور در سطح کشور (نظیر: ثبت احوال، هواشناسی، پست، گمرکات، اپراتورهای تلفـن همـراه و ...)، ۳۶ مرکـز آپـا در مراکـز دانشگاهی و ۶ مجموعه پشتیبانی‌کننده و متولی در حوزه پدافند سایبری در سـطح کشـور (از جمله سازمان پدافند غیرعامل) مورد استفاده قرار گرفتند. در مجموع ۱۱۴۴ نفـر بـه عنـوان جامعه مورد مطالعه در سازمان‌های داده‌محور و مراکز پشتیبانی‌کننده حوزه پدافند سایبری در سطح کشور با مدرک تحصیلی حداقل کارشناسی و حداقل ۵ سـال سـابقه فعالیـت در حـوزه پدافند سایبری و آگاه نسبت به مفاهیم سـازمان‌های داده‌محـور و داده‌هـای عظـیم در نظـر گرفته شدند، که با استفاده از فرمول کوکران تعداد حجم نمونه ۲۸۸ نفـر، تعیـین و بـه روش تصادفی ساده در تحقیق مشارکت داده شدند.

ابزار گرداوری داده ها در این تحقیق پرسشنامه محقق ساخته بوده اسـت. در پرسشـنامه مرحله دلفی هفتاد شاخص بر اساس مرور مبانی نظری استخراج شدند، در نظر گرفته شد. با استفاده از نرم‌افزار SPSS، ضریب همبستگی (کندال) برای پرسشنامه محاسبه گردیـد و بـه

استناد آن، در حوزه یکپارچگی دسترسی به داده سازمان‌های داده‌محور مورد بررسی و تحلیل قرار گرفت، که به دلیل عدم توافق نظرات خبرگان، تعداد ۱۰ شاخص حذف شدند و پرسشنامه با توجه به حذف موارد احصاء شده از نتیجه ضریب همبستگی کندال، مجدداً بازنگری و پیاده‌سازی شد. در ادامه پرسشنامه‌ای براساس خروجی حاصل از روش دلفی طراحی و به منظور اجرای فاز دوم (ارزیابی و اعتبارسنجی) مدل تنظیم و توزیع گردید. با استفاده از نرم‌افزارهای اِس‌پی‌اِس‌اِس و آموس تحلیل داده ها صورت گرفت.

یافته‌های پژوهش

نتایج حاصل از اجرای پنل دلفی در بین ۱۵ نفر از خبرگان و صاحب نظران حوزه پدافند سایبری مسلط به حوزه سازمان‌های داده‌محور و داده‌های عظیم، نشان داد ۱۰ شاخص با شماره‌های ۱۲، ۱۶، ۳۱، ۳۶، ۵۰، ۵۲، ۵۵، ۵۶، ۶۸ و ۶۹ بخاطر ضریب توافق (ضریب کندال) ضعیف حذف شدند. مقوله بندی شاخص ها براساس چارچوب اِن.آی.اِس.تی طی مراحل دلفی با نظر خبرگان انجام گرفت که ۶۰ شاخص تایید شده در قالب ۲۳ مولفه و ۵ بعد دسته بندی شدند(جدول۱). برای ارزیابی و اعتبارسنجی یافته های حاصل از پنل دلفی از مدل یابی معادلات ساختاری (مدل اندازه گیری/تحلیل عاملی تاییدی) استفاده شد. در هر الگوی تحلیل عاملی ارائه شده معناداری، وزن‌های رگرسیونی در سطح اطمینان ۹۵ درصد، بر روایی این الگو دلالت دارد. ضرایب رگرسیونی در الگو، اندازه‌گیری میزان تأثیر هر یک از شاخص‌ها را بر روی مولفه و تأثیر هریک از مولفه‌ها را بر بعد نشان می‌دهد. به عبارتی هرچه میزان ضریب استاندارد شده رگرسیونی بیشتر باشد، آن شاخص یا مولفه توان بیشتری در تبین متغیر پنهان سطح بالاتر خود دارد.

جدول ۱. نتایج تحلیل دلفی

سازمان داده محور	بعد پدافند سایبری	مؤلفه		دور اول دلفی			دور دوم دلفی		
			شاخص	میانگین	ضریب کندال	تغییرات کیفی	میانگین	ضریب کندال	تغییرات کیفی
یکپارچگی دسترسی به داده‌ها	شناسایی	مدیریت دارایی	۱-شناسایی رایانه‌ها (سیستم‌های موجود)	۳/۴۰	۰/۳۵۰	تایید	۳/۸۹۲	۰/۷۸۶	تایید
			۲-شناسایی سیستم‌های عامل	۳/۷۳	۰/۴۱۵	تایید	۴	۱	تایید
			۳-شناسایی برنامه‌های کاربردی	۴/۱۳	۰/۸۰۰	تایید	۴	۱	تایید
			۴-شناسایی داده‌ها	۴/۶۰	۰/۸۶۷	تایید	۵	۱	تایید
			۵-شناسایی ارتباطات و شبکه تبادل‌داده سازمانی	۴/۰۷	۰/۸۶۷	تایید	۴	۱	تایید
		محیط کسب و کار	۶-شناسایی نقش‌ها و مسئولیت‌های پدافند سایبری ذی‌نفعان	۴/۱۳	۰/۷۳۳	تایید	۴	۱	تایید
			۷-شناسایی زنجیره تأمین	۳/۶۷	۰/۶۰۰	تایید	۴	۱	تایید
			۸-شناسایی زیرساخت	۴/۲۷	۰/۶۲۱	تایید	۴	۱	تایید
			۹-شناسایی مأموریت سازمانی، اهداف و فعالیت‌ها	۳/۶۷	۰/۵۵۶	تایید	۴	۱	تایید
			۱۰- شناسایی ارائه و پشتیبانی ازخدمات	۳/۶۰	۰/۳۶۳	تایید	۴	۱	تایید
		حاکمیت	۱۱-شناسایی سیاست امنیت داده سازمانی	۴/۰۷	۰/۸۰۰	تایید	۴	۱	تایید

			۱۲-شناسایی الزامات قانونی و نظارتی	۳/۴۰	۰/۱۲۸	رد	۳/۱۳	۰/۱۳۳	رد
		ارزیابی مخاطرات	۱۳-شناسایی آسیب‌پذیری دارایی‌ها	۳/۶۷	۰/۲۴۰	تایید	۴	۱	تایید
			۱۴-کسب آگاهی از منابع اشتراکی	۴/۱۳	۰/۷۳۳	تایید	۴	۱	تایید
			۱۵- شناسایی تهدیدات داخلی/ خارجی	۳/۷۳	۰/۳۵۶	تایید	۴	۱	تایید
			۱۶-شناسایی مشاغل مورد نیاز پدافند سایبری	۳/۳۳	۰/۰۲۷	رد	۳/۰۷	۰/۰۶۷	رد
			۱۷-شناسایی و اولویت‌بندی پاسخ‌های مخاطره	۳/۸۰	۰/۳۵۶	تایید	۴	۱	تایید
			۱۸- شناسایی مدیریت ریسک سازمانی	۳/۷۳	۰/۴۲۷	تایید	۴	۱	تایید
		مدیریت	۱۹- شناسایی زنجیره تأمین	۳/۹۳	۰/۴۷۶	تایید	۴	۱	تایید
			۲۰-شناسایی ریسک تأمین‌کنندگان سیستم‌های مهم اطلاعاتی	۴/۰۰	۰/۶۶۷	تایید	۴	۱	تایید
	حفاظت	مدیریت هویت و دسترسی	۲۱- صدور مجوزها و اعتبارنامه‌ها	۳/۸۰	۰/۴۶۷	تایید	۴	۱	تایید
			۲۲- کنترل دسترسی	۴/۰۷	۰/۷۵۱	تایید	۴	۱	تایید
			۲۳- نظارت بر یکپارچگی شبکه	۳/۸۰	۰/۲۵۱	تایید	۴	۱	تایید
		آگاهی و آموزش پدافند سایبری	۲۴- آموزش و آگاه سازی کاربران	۳/۸۷	۰/۶۸۶	تایید	۴	۱	تایید
			۲۵-آموزش ذی‌نفعان	۳/۸۰	۰/۶۰۰	تایید	۴	۱	تایید
			۲۶- حذف، نقل و انتقال و مرتب‌سازی امن داده ها	۴/۰۷	۰/۶۲۱	تایید	۴	۱	تایید
			۲۷- حفظ ظرفیت کافی برای نگهداری داده‌ها	۳/۹۳	۰/۴۹۱	تایید	۴	۱	تایید
			۲۸- کنترل یکپارچگی سخت‌افزار	۳/۶۷	۰/۴۶۷	تایید	۴	۱	تایید
			۲۹-کنترل یکپارچگی نرم‌افزار	۴/۱۳	۰/۹۳۳	تایید	۴	۱	تایید
			۳۰-کنترل یکپارچگی اطلاعات	۴/۴۰	۰/۸۶۷	تایید	۴	۱	تایید
			۳۱- نظارت بر جداسازی محیط(های) توسعه و آزمایش از محیط تولید	۳/۲۷	۰/۰۵	رد	۳/۰۷	۰/۰۶۷	رد
		مراحل و روش‌های محافظت از اطلاعات	۳۲-نظارت بر پیکربندی امن سیستم‌های اطلاعاتی	۳/۹۳	۰/۴۹۱	تایید	۴	۱	تایید
			۳۳-تهیه نسخه پشتیبان	۴/۰۰	۰/۶۸۶	تایید	۴	۱	تایید
			۳۴-نظارت بر اجرای صحیح سیاست‌ها و مقررات	۳/۵۳	۰/۱۷۱	تایید	۴	۱	تایید
			۳۵-بهبود مستمر فرآیندهای محافظت	۴/۴۰	۰/۶۲۱	تایید	۴	۱	تایید
			۳۶-نظارت بر اجرای برنامه‌های بازیابی	۳/۲۰	۰/۰۴۸	رد	۳/۱۳	۰/۱۳۳	رد
			۳۷-بهبود جذب و نگهداشت منابع انسانی با رویکرد پدافند سایبری	۴/۰۰	۰/۳۰۵	تایید	۴	۱	تایید
			۳۸- تهیه و اجرای برنامه مدیریت آسیب‌پذیری	۴/۰۰	۰/۶۲۱	تایید	۴	۱	تایید
		نگهداری	۳۹-تعمیر و نگهداری دارایی‌ها	۳/۷۳	۰/۴۵۱	تایید	۴	۱	تایید
		فن‌آوری حفاظتی	۴۰- مستندسازی سوابق ورود به سیستم	۳/۹۳	۰/۴۹۱	تایید	۴	۱	تایید
			۴۱-محافظت از رسانه‌های جدا شده و نظارت بر نحوه استفاده مجدد از آن	۳/۵۳	۰/۳۵۲	تایید	۴	۱	تایید
			۴۲- محافظت از شبکه‌های ارتباطی	۴/۲۷	۰/۷۳۳	تایید	۴	۱	تایید
			۴۳-دسترس‌پذیری پایدار	۴/۱۳	۰/۶۲۱	تایید	۴	۱	تایید
	کشف	ناهنجاری‌ها و وقایع	۴۴-تجزیه و تحلیل رویدادهای کشف شده از منابع و حسگرها	۳/۸۷	۰/۳۶۰	تایید	۴	۱	تایید
		نظارت مستمر امنیتی	۴۵-نظارت بر شبکه شناسایی رویدادهای محتمل	۴/۱۳	۰/۴۷۶	تایید	۴	۱	تایید
			۴۶-نظارت بر فعالیت‌های سایبری کارکنان	۳/۹۳	۰/۶۰۰	تایید	۴	۱	تایید
			۴۷-شناسایی کد مخرب	۳/۶۰	۰/۳۶۳	تایید	۴	۱	تایید
			۴۸-نظارت بر فعالیت امن سایبری ارائه‌دهندگان خدمات خارجی	۴/۱۳	۰/۳۵۶	تایید	۴	۱	تایید
			۴۹-نظارت بر دسترسی غیرمجاز	۴/۰۰	۰/۵۳۸	تایید	۴	۱	تایید
			۵۰-نظارت بر تجهیزات غیرمجاز	۳/۴۰	۰/۰۸۹	رد	۳/۱۳	۰/۱۳۳	رد
			۵۱-نظارت بر نرم‌افزار غیرمجاز	۳/۶۰	۰/۳۰۰	تایید	۴	۱	تایید

		۵۲-اسکن آسیب‌پذیری	۳/۲۷	۰/۰۵۵	رد	۳/۱۳	۰/۱۳۳	رد
	فرآیندهای تشخیص	۵۳-تعریف بهینه نقش‌ها و مسئولیت‌های تشخیص وقایع غیرطبیعی	۳/۸۷	۰/۳۵۶	تایید	۴	۱	تایید
		۵۴-بهبود مستمر و آزمایش فرآیندهای تشخیص وقایع غیرطبیعی	۳/۹۳	۰/۳۹۸	تایید	۴	۱	تایید
		۵۵-اطلاع‌رسانی وقایع غیرطبیعی کشف شده	۳/۳۳	۰/۱۰۷	رد	۳/۰۷	۰/۰۶۷	رد
	طرح‌ریزی	۵۶- اجرای طرح پاسخگویی به رخداد سایبری	۳/۲۰	۰/۰۰۶	رد	۳/۰۷	۰/۰۶۷	رد
	ارتباطات	۵۷-آگاهی کارکنان از وظایف	۴/۱۳	۰/۳۵۶	تایید	۴	۱	تایید
		۵۸-گزارش رویدادها	۴/۰۰	۰/۲۹۷	تایید	۴	۱	تایید
		۵۹-اشتراک اطلاعات مطابق با طرح‌های پاسخ‌دهی	۳/۷۳	۰/۴۷۱	تایید	۴	۱	تایید
پاسخگویی	تحلیل و بررسی	۶۰-بررسی اعلان سیستم‌های شناسایی	۴/۱۳	۰/۸۶۷	تایید	۴	۱	تایید
		۶۱-درک تأثیر و طبقه بندی حوادث	۴/۰۷	۰/۳۵۶	تایید	۴	۱	تایید
		۶۲-فارنزیک	۳/۴۰	۰/۳۰۵	تایید	۴/۱۳	۰/۹۳۳	تایید
	کاهش	۶۳-انجام اقدامات پیشگیرانه در خصوص کاهش حوادث	۴/۰۷	۰/۳۵۶	تایید	۴	۱	تایید
		۶۴- ثبت و مستند سازی آسیب‌پذیری‌های تازه شناسایی شده	۳/۷۳	۰/۴۳۶	تایید	۴	۱	تایید
	پیشرفت ها	۶۵-تدوین برنامه‌های پاسخ و به روزرسانی با استفاده از یادگیری سازمانی	۳/۶۰	۰/۴۵۱	تایید	۴	۱	تایید
	برنامه‌ریزی بازیابی	۶۶-اجرای برنامه بازیابی در حین یا بعد از رویداد	۴/۲۰	۰/۶۶۷	تایید	۴	۱	تایید
	پیشرفت ها	۶۷-تدوین برنامه‌های بازیابی و به‌روزرسانی با استفاده از یادگیری سازمانی	۳/۶۷	۰/۵۲۸	تایید	۴	۱	تایید
بازیابی	ارتباطات	۶۸- مدیریت روابط عمومی	۳/۰۰	۰/۰۰۷	رد	۳/۰۷	۰/۰۶۷	رد
		۶۹-تصحیح اعتبار بعد از یک رویداد	۳/۰۷	۰/۰۰۶	رد	۳/۰۷	۰/۰۶۷	رد
		۷۰-اطلاع‌رسانی فعالیت‌های بازیابی	۳/۶۷	۰/۳۷۱	تایید	۴	۱	تایید

جدول ۲. شاخص‌های برازش الگوی اندازه‌گیری عوامل

عوامل	CMIN/DF(<5)	NFI(>0.9)	GFI(>0.9)	RMR(<0.09)	RMSEA(<0.08)
شناسایی	۲/۳۶۸	۰/۹۷۴	۰/۹۶۶	۰/۰۶۵	۰/۰۴۷
حفاظت	۳/۵۶۸	۰/۹۸۷	۰/۹۲۵	۰/۰۳۷	۰/۰۲۶
کشف	۲/۰۴۷	۰/۹۶۱	۰/۹۱۳	۰/۰۴۹	۰/۰۳۴
پاسخگویی	۱/۱۴۸	۰/۹۳۵	۰/۹۵۲	۰/۰۷۱	۰/۰۶۲
بازیابی	۲/۵۸۹	۰/۹۴۹	۰/۹۸۶	۰/۰۵۸	۰/۰۴۹

با توجه به جدول (۲)، تمامی شاخص‌های بدست آمده از برازش مدل در محدوده قابل قبول قرار دارند که الگو ارائه شده در هر یک از عوامل را تایید می‌کند.

جدول ۳. نتایج تحلیل عاملی تاییدی برای عوامل

بعد	عامل	مقدار بحرانی	بارهای عاملی استاندارد شده	معنی‌داری	نتیجه
شناسایی	مدیریت دارایی	۳/۲۱۹	۰/۵۷	<۰/۰۰۱	تایید
	محیط کسب و کار	۲/۶۸۵	۰/۸۵	<۰/۰۰۱	تایید
	حاکمیت	۲/۹۶۳	۰/۷۹	<۰/۰۰۱	تایید
	ارزیابی مخاطرات	۳/۰۱۲	۰/۹۳	<۰/۰۰۱	تایید
	مدیریت ریسک زنجیره تامین	۲/۳۵۶	۰/۸۵	<۰/۰۰۱	تایید

حفاظت	مدیریت هویت و دسترسی	۲/۸۷۴	۰/۷۲	<۰/۰۰۱	تایید
	آگاهی و آموزش پدافند سایبری	۲/۵۴۶	۰/۷۱	<۰/۰۰۱	تایید
	روش‌های محافظت از اطلاعات	۷/۶۹۳	۰/۸۶	<۰/۰۰۱	تایید
	نگهداری	۵/۵۹۷	۰/۶۳	<۰/۰۰۱	تایید
	فن آوری حفاظتی	۲/۶۳۷	۰/۵۹	<۰/۰۰۱	تایید
کشف	ناهنجاری‌ها و وقایع	۳/۵۳۲	۰/۷۲	<۰/۰۰۱	تایید
	نظارت مستمر امنیتی	۲/۳۸۷	۰/۸۹	<۰/۰۰۱	تایید
	فرآیندهای تشخیصی	۳/۹۸۷	۰/۷۹	<۰/۰۰۱	تایید
پاسخگویی	ارتباطات	۲/۷۵۰	۰/۶۷	<۰/۰۰۱	تایید
	تحلیل و بررسی	۳/۶۵۳	۰/۸۶	<۰/۰۰۱	تایید
	کاهش	۲/۶۴۸	۰/۷۵	<۰/۰۰۱	تایید
	پیشرفت‌ها	۲/۳۵۷	۰/۷۹	<۰/۰۰۱	تایید
بازیابی	برنامه‌ریزی بازیابی	۳/۷۸۹	۰/۸۵	<۰/۰۰۱	تایید
	پیشرفت‌ها	۳/۹۸۲	۰/۸۸	<۰/۰۰۱	تایید
	ارتباطات	۳/۶۴۸	۰/۷۶	<۰/۰۰۱	تایید

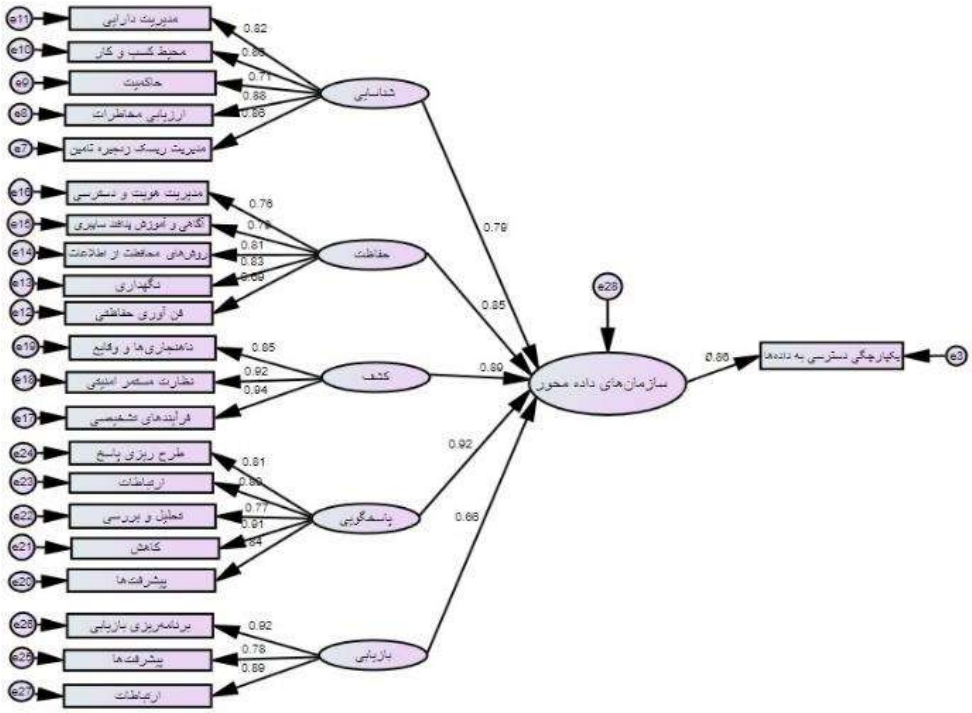
جهت برازش پایایی الگوهای اندازه‌گیری، از ضریب پایایی ترکیبی استفاده شد، در صورتی که بالاتر از ۰/۷ باشد مدل ایجاد شده از برازش مناسبی برخوردار می‌باشد. همچنین، روایی همگرا که معیاری برای برازش الگوهای اندازه‌گیری است و میزان همبستگی یک عامل با شاخص‌های خود را نشان می‌دهد که هرچه این همبستگی بیشتر باشد، مقبولیت برازش نیز بیشتر است.

جدول ٤. مقادیر پایایی ترکیبی و روایی همگرا عوامل

عامل	پایایی ترکیبی (CR>0.7)	روایی همگرا (AVE>0.5)
شناسایی	۰/۸۵۶	۰/۶۴۱
حفاظت	۰/۷۴۸	۰/۵۰۱
کشف	۰/۷۷۹	۰/۶۴۴
پاسخگویی	۰/۸۶۲	۰/۶۰۲
بازیابی	۰/۷۱۲	۰/۷۴۸

با توجه به جدول (۴)، ضریب پایایی ترکیبی برای هر یک از عوامل بیشتر از ۰/۷ است و این پایایی قابل قبول الگوی اندازه‌گیری را نشان می‌دهد، همچنین ضریب روایی همگرای هر یک از عوامل بیشتر از ۰/۵ می‌باشد که بیان کننده‌ی برازش قابل قبول الگوی اندازه گیری است. برای دستیابی به یک الگوی کاربردی از پدافند سایبری در حوزه مذکور، یک مدل کلی شامل متغیرهای مستقل که هر یک از ابعاد پدافند سایبری (خود ابعاد به عنوان متغیر پنهان و مؤلفه‌های هر بعد به عنوان متغیر آشکار) و متغیر وابسته سازمان‌های داده‌محور برازش داده شد. در این مدل هدف بررسی رابطه علی بین هر یک از ابعاد پدافند

سایبری بر حوزه یکپارچگی دسترسی به داده‌ها در سازمان‌های داده‌محور می‌باشد، ضریب رگرسیونی استاندارد شده در هر مسیر نشان از میزان تأثیرگذاری آن بعد پدافند سایبری بر سازمان داده‌محور می‌باشد.



شکل ۱. مدل تحلیل عاملی تاییدی(مدل اندازه گیری تحقیق)

با توجه به جدول (۵)، تمامی شاخص‌های بدست آمده از برازش مدل در محدوده قابل قبول قرار دارند که الگوی موردنظر را تایید می‌کند.

جدول ۵. شاخص‌های برازش الگوی معادلات مسیر پژوهش

شاخص‌ها	(CMIN/DF)	NFI	GFI	RMR	RMSEA
مدل مسیر	۳/۲۳۲	۰/۹۳۲	۰/۹۱۵	۰/۰۴۸	۰/۰۲۵
سطح قابل قبول	<۵	>۰/۹	>۰/۹	<۰/۰۹	<۰/۰۸
نتیجه	مناسب	مناسب	مناسب	مناسب	مناسب

با توجه به الگوی اندازه گیری تحقیق الگوی اندازه گیری تحقیق با ۶۰ شاخص، ۲۳ مولفه و ۵ بعد تایید گردید که در این بین، بعد پاسخگویی با ضریب ۰.۹۲ و بعد حفاظت با ضریب ۰.۸۵ بیشترین قدرت تبیین کنندگی را داشتند.

بحث و نتیجه‌گیری

هدف از پژوهش حاضر، ارائه الگوی پدافند سایبری در حوزه یکپارچگی دسترسی به داده‌ها در سازمان‌های داده‌محور بود. در نتایج بدست آمده، تمامی شاخص‌های حاصل از برازش

مدل در محدوده قابل قبول قرار داشتند. همچنین، در مدل پیشنهادی، متغیر پاسخگویی بیشترین تأثیر و متغیر بازیابی کمترین تأثیر را داشته و این مهم بیانگر آنست‌که توجه به پاسخگویی، تداوم و استمرار (تاب‌آوری) در ارائه خدمات توسط سازمان‌های داده‌محور بسیار حائز اهمیت بوده، و رویکرد اینگونه از سازمان‌ها می‌بایست با ارجح قرار دادن پیش‌گیری نسبت به درمان، صورت پذیرد، ضمن آنکه در هیچ یک از نتایج حاصل از بررسی مطالعات و منابع به‌روز ارجاع داده شده در این پژوهش، تحلیلی بر میزان اثرگذاری ابعاد پاسخگویی و بازیابی بر روی سازمان‌های داده‌محور انجام نشده و صرفاً به ذکر تعریف بسنده شده است.

همانطور که مشاهده گردید، در بُعد شناسایی شاخص‌های شناسایی الزامات قانونی و نظارتی از مولفه حاکمیت و شناسایی مشاغل مورد نیاز پدافند سایبری از مولفه ارزیابی مخاطرات بر اساس نظر خبرگان دارای ضریب توافق پائین بوده و بدان مفهوم است که انجام شناسایی تهدیدات در پدافند سایبری مربوط به این حوزه می‌بایست به صورت پیش‌دستانه حتی بدون در نظر گرفتن الزامات قانونی و نظارتی مد نظر قرار گیرد، و مباحث مربوط به شناسایی نوع و ماهیت مشاغل در اینگونه سازمان‌ها در ایمن نمودن یکپارچگی دسترسی به داده‌ها نقشی ندارد.

در بُعد حفاظت نیز شاخص‌های نظارت بر جداسازی محیط(های) توسعه و آزمایش از محیط تولید (مربوط به مولفه آگاهی و آموزش پدافند سایبری) و نظارت بر اجرای برنامه‌های بازیابی (مراحل و روش‌های محافظت از اطلاعات) نیز با عدم توافق میان خبرگان همراه بود که حاکی از آنست که در مرحله حفاظت از پدافند سایبری حوزه یکپارچگی دسترسی به داده‌ها در سازمان‌های داده‌محور ضرورتی بر آگاهی‌رسانی و اجرای برنامه های آموزشی برای ذی‌نفعان مبنی بر جداسازی محیط توسعه و محیط تولید وجود نداشته و در این قسمت رویکرد، حفظ و مراقبت از خدمات مبتنی بر داده یکپارچه می‌باشد و می‌بایست فرآیند حفاظت معطوف به حوزه کاربردی و عملیاتی منابع داده‌ای یکپارچه گردد.

در بُعد کشف شاخص‌های نظارت بر تجهیزات غیرمجاز و اسکن آسیب‌پذیری (از مولفه نظارت مستمر امنیتی)، اطلاع‌رسانی وقایع غیرطبیعی کشف شده (از مولفه فرآیندهای تشخیص) به‌استناد ضریب توافق بسیار پائین، مورد وفاق خبرگان در اجرای پانل دلفی قرار نگرفت و بدین معنا می‌باشد که انجام عملیات کشف آسیب‌پذیری در حوزه یکپارچگی دسترسی به داده‌ها می‌بایست به صورت کلان‌تر مورد توجه قرار گیرد.

در بعُد پاسخگویی مولفه طرح‌ریزی نیز در پدافند سایبری حوزه یکپارچگی دسترسی به داده‌ها با توجه به پائین بودن میزان ضریب توافق کندال مورد توافق خبرگان قرار نگرفت و بدین مفهوم است که برای پاسخگویی به تهدیدات می‌بایست اقدامات به صورت پیش‌دستانه

و دفاع چند لایه (دفاع در عمق) انجام شود و بعضاً برخی از تهدیدات، نظیر آسیب‌پذیری‌های روز صفر امکان برنامه‌ریزی و طرح‌ریزی برای پاسخگویی وجود ندارد.

در بُعد بازیابی هم شاخص‌های مدیریت روابط عمومی و تصحیح اعتبار بعد از یک رویداد از مولفه ارتباطات به دلیل ضریب توافق پائین نمی‌بایست در فرآیند پدافند سایبری از حوزه یکپارچگی دسترسی به داده مورد توجه قرار گیرند، زیرا رویکرد اصلی این حوزه، استمرار و تداوم ارائه خدمات داده‌ای یکپارچه و دسترس‌پذیر می‌باشد، فلذا ضرورتی بر بازیابی مدیریت ارتباط با ذی‌نفعان/ مشتری و تصحیح اعتبار آنان، توسط متولیان پدافند سایبری وجود ندارد.

همچنین، در الگوی ارائه شده در بعد شناسایی، مولفه ارزیابی مخاطرات بیشترین و مولفه مدیریت دارایی کمترین تاثیر را برخوردار می‌باشد، این مهم بیانگر آنستکه به منظور یکپارچگی دسترسی به داده‌ها به صورت امن ضرورت دارد، سازمان‌های داده‌محور مخاطرات مرتبط با آن را با انجام ارزیابی‌های امنیتی احصاء و نسبت به رفع آن با انجام بهینه‌سازی پیکربندی‌ها و بکارگیری وصله‌های امنیتی مربوطه جدای از انجام مدیریت دارایی‌های سایبری به انجام برسانند (تیم‌های ارزیابی می‌بایست از حوزه مدیریتی و نگهداری دارایی‌های سایبری مجزا باشند، تا قابلیت ارزیابی، احصاء و اعلام آسیب فراهم گردد). مجمع تشخیص مصلحت نظام (۱۳۸۲) از مصادیق وجود نظم، سنجش و مقایسه وضعیت در هر مقطع زمانی، ارزیابی عملکرد و پایش نتایج در پایان هر مرحله و تعیین میزان پیشرفت را مطرح و وزارت فن‌آوری اطلاعات و ارتباطات (۱۳۹۶) نیز به ارزیابی خدمات و محصولات کلان داده‌ها توجه ویژه نموده‌اند، اِن.آی.اِس.تی (۲۰۱۷) نیز ارزیابی ریسک را در چرخه پدافند سایبری ضروری دانسته، ضمن آنکه والتر (۲۰۱۵) در سند معماری فن خود از ارزیابی مخاطرات به‌منظور دستیابی به تحلیل دقیق‌تر در حوزه فعالیت‌های آفندی و پدافندی سایبر استفاده نموده است. لذا از آنجائیکه داده‌ها به‌صورت توزیع شده و بدون توجه به مالکیت در سازمان‌های داده‌محور نگهداری و بهره‌برداری می‌گردند، در هیچ‌یک از مطالعات موجود، به مدیریت دارایی‌ها در حوزه سایبری نپرداخته است.

در بعد حفاظت، مولفه روش محافظت از اطلاعات بیشترین و مولفه فناوری حفاظتی کمترین تاثیر را برخوردار می‌باشد، و این بیانگر آنستکه، متولیان پدافند سایبریِ سازمان‌های داده‌محور به منظور امن‌سازی یکپارچگی دسترسی به داده‌ها ضروریست روش‌ها و تکنیک‌های محافظتی را فارغ از هر نوع وابستگی تجهیزاتی احصاء و در فرآیندهای فیزیکی (محیطی) و منطقی (پیکربندی و ماهیت داده‌ای) مورد بهره‌برداری قرار دهند. عرب سرخی (۱۳۹۶) به محافظت از اطلاعات به عنوان ارزشمندترین دارایی هر سازمان، سنگانی (۲۰۱۸) توصیه به انجام محافظت با دقت از داده‌های سازمان‌ها در برابر تهدیدات بیرونی و

دی.او.دی (۲۰۱۸) نیز به همین صورت با نتیجه بدست آمده هم نظر می‌باشند و در هیچ یک از مطالعات انجام شده به مبحث فنآوری‌های حفاظتی اشاره‌ای نگردیده است و این نشـان از اهمیت پائین آن می‌باشد.

در بعد کشف، مولفه نظارت مستمر امنیتی از اطلاعات بیشترین و مولفه ناهنجـاری‌هـا و وقایع کمترین تاثیر را برخوردار می‌باشد، با توجه به حوزه یکپـارچگی دسترسـی بـه داده‌هـا، ضروریست به منظور کشف آسیب‌های این حوزه فرآیندهای نظـارتی بـه صـورت هوشـمند، ساختارمند و مستمر توسط متولیان سایبری منظور و طرح‌ریزی گـردد. سـهرابی و همکـاران (۱۳۹۴)، سنگانی (۲۰۱۸) و گاست بلوگار (۲۰۱۶) نیز در مطالعات خـود کنتـرل و نظـارت را برای استفاده از داده‌ها بسیار حائز اهمیت دانسته و حتی بعضاً آن‌را باعث کـاهش کیفیـت در ارائه خدمات مطرح نموده‌اند و تقریباً در هیچ‌یک از مطالعات انجام شده موضوعات مرتبط بـا مولفه ناهنجاری‌ها و وقایع مطرح نگردیده است، که این نشان از اهمیت پایین آن می‌باشد.

در بعد پاسخگویی، مولفه تحلیل و بررسی بیشترین و مولفـه ارتباطـات کمتـرین تـاثیر را برخوردار می‌باشـد، لـذا متولیـان پدافنـد سـایبری در سـازمان‌های داده‌محـور ضـرورت دارد پاسخگویی به آسیب‌های حوزه یکپارچگی دسترسی به داده‌ها را بـر اسـاس انجـام تجزیـه و تحلیل و بررسی آسیب، با بهره‌گیری از تکنیک‌های ارزیابی تهدیدات صرف نظر از ارتباطات و تبادل داده به انجام برسانند. کلکلی و همکـاران (۱۳۹۶)، انسـتیتو شـرق – غـرب آمریکـا؛ انستیتو اطلاعات دانشگاه دولتی مسکو (۲۰۱۲) پاسخ‌گویی را به‌عنوان ویژگی فضـای سـایبر یاد می‌کنند و اِچ.پی.ای (۲۰۱۶) و والتر(۲۰۱۵) نیز مدیریت پاسخگویی رویدادهای امنیتی را دربردارنده قابلیت‌هایی می‌دانند که در تمام سطوح دفاع سایبری قابل به‌کارگیری بوده و ایـن نشان از ارزش و اهمیت آن می‌باشد و والتر (۲۰۱۵) به تحلیل و بررسـی دقیـق‌تر رخـدادها و اطلاعات مربوط به تهدیدات، حملات و رویدادهای سایبری توصیه نموده، و اسـمیت (۲۰۰۶) نیز تحلیل و بررسی را به عنوان پایه و شالوده علم داده معرفی نموده است.

در بعد بازیابی، مولفه پیشرفت بیشترین و مولفه برنامه‌ریزی و ارتباطات کمتـرین تـاثیر را برخوردار می‌باشد، بیانگر آنستکه فرآیندهای بازیابی داده‌ها می‌بایست به نحوی در نظر گرفته شوند، به صورت هوشمند (به ویژه رویکرد یادگیرندگی) و بر خط بدون نیاز به برنامـه‌ریزی و حتی صرف نظر از ارتباطات به ازای هر آسیبی بتواند در اسـرع زمـان و بـدون اتـلاف وقـت داده‌های آسیب دیده‌ای را که می‌تواند یکپارچگی دسترسی به داده‌ها مختل نماید را بازیابی و در اختیار ذی‌نفعان قرار دهد. اسمیت (۲۰۰۶) به اهمیت سرعت در بازیـابی، سـازمان پدافنـد غیرعامل کشور (۱۳۹۴)، کـیم و همکـاران (۲۰۱۴)، کلکلـی و همکـاران (۱۳۹۶) و عـالی‌پور (۱۳۹۶) در مطالعات خود نگهداری و انباشت داده‌هـا و اطلاعـات را بـه‌عنوان یکـی از اجـزاء

زیرساخت سایبری و فضای سایبری مطرح نموده و توجه به بازیابی اطلاعات را امری ضروری قلمداد می‌نمایند. آرنُت و پِروان (۲۰۱۴) و سهرابی و همکاران (۱۳۹۴) نیز توجه ویژه‌ای به بهره‌گیری از قابلیت‌های هوشمندی و هوش مصنوعی در شناسایی تهدیدات و بازیابی اطلاعات داشته‌اند.

با توجه به نتایج حاصل از این پژوهش، پیشنهاداتی به شرح ذیل ارائه می‌گردند:

۱- حرکت تحولی سازمان‌ها در فضای رقابتی به سمت داده‌محور شدن.

۲- بومی‌سازی و پیاده‌سازی الگوی ارائه شده در سازمان داده‌محور امن، با رویکرد صیانت از سرمایه‌ها و دارایی اطلاعاتی.

۳- برنامه‌ریزی و اقدام متولیان پدافند سایبری در سازمان‌های داده‌محور در خصوص ارزیابی مستمر امنیتی مخاطرات و تهدیدات متصور بر روی مخازن و سامانه‌های ذخیره‌سازی داده‌ها، و همچنین، شناسایی و بکارگیری روش‌های متنوع محافظت از داده‌ها، چه از منظر شرایط فیزیکی و چه منطقی (ساختار نرم‌افزاری) مخازن نگهداری داده‌ها.

۴- پیاده‌سازی الگوی یکپارچه‌سازی امن داده‌ها با رویکرد تصمیم‌گیری بهینه مبتنی بر داده‌های عظیم و همچنین، با رویکرد دسترسی امن.

منابع

اصلانی مناف، داود؛ براتی، اکرم. (۱۳۹۶). بررسی تاثیر فن آوری اطلاعات بر بهبود کارآیی سازمان. *هفتمین همایش سالانه بانکداری الکترونیک و نظام‌های پرداخت، تهران: مرکز همایش برج میلاد*، ۳۵-۶۰.

حبیبی، آرش. (۱۳۹۷). آموزش کامل SPSS و راهنمای تصویری نرم‌افزار SPSS. *تهران: پارس مدیر*.

حبیبی، آرش. (۱۳۹۹). آموزش روش تحقیق کیفی. *تهران: پارس مدیر*.

حقیقی، محمد علی؛ سعادتی، وحید. (۱۳۹۷). کلان داده؛ پیشران نوآوری در خط مشی گذاری دولتی. *تهران: دانشگاه تهران*.

رمضان زاده؛ مجتبی، غیوری ثالث؛ مجید، احمدوند، علی‌محمد، آقایی؛ محسن، نظری فرخی؛ ابراهیم. (۱۴۰۰). بررسی قدرت پدافند سایبری نیروهای مسلح با روش برنامه‌ریزی مبتنی بر سناریو. *فصلنامه آینده پژوهی دفاعی دافوس آجا*، ۶(۲۰) , ۵۹-۸۱.

سازمان‌پدافندغیرعامل‌کشور. (۱۳۹۴). *سند راهبردی پدافند سایبری کشور*، بازیابی از سازمان پدافند غیرعامل کشور: *http://vcmdrp.tums.ac.ir/files/padafand*.

سهرابی، بابک؛ ایرج، حمیده. (زمستان ۱۳۹۴). علم داده: مفاهیم و مهارت ها. *تهران: جهاد دانشگاهی*.

عالی‌پور، حسن. (مرداد ۱۳۹۶). حقوق کیفری فناوری اطلاعات (جرایم رایانه‌ای)، *تهران: خرسندی*.

فرابر. (۱۳۹۷). چگونه به یک سازمان داده محور تبدیل شویم؟. *تهران: گروه پژوهشی فرابر*.

فرزام نیا، نیما؛ سهیلی، حمیدرضا؛ خزایی، مصطفی . (۱۳۹۴). بررسی تکنیکهای نوین جنگ هـای سـایبری و ارایه مدل ساختاری پویا برای مقابله با آن. *تهران: دانشگاه علم و صنعت ایران.*

قوچانی خراسانی، محمدمهدی و همکاران. (زمستان ۱۳۹۷). شناسایی عوامل توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری با رویکرد نظریه داده بنیاد. *مطالعات مدیریت کسب و کار هوشـمند*، ۷(۲۶)، ۷۰-۳۷.

کتانچی؛ النار، پورقهرمانی؛ بابک،. (۱۴۰۰). چالشهای امنیتِ سـایبری در کشـورهای « آسـه آن». *فصـلنامه مطالعات بین المللی*، ۱۸(۱)، ۱۵۶- ۱۳۹ .

کلکی، منصور؛ رجایی، امیر. (۱۳۹۶). پردازش داده های کلان (Big data). *کنفرانس سالانه پـارادایم‌هـای نوین مدیریت در حوزه هوشمندی*، تهران: پردازش داده.

مانیان؛ امیر و همکاران. (۱۳۹۵). طراحی الگوی داده کاوی پیشنهادی به منظور شناسـایی مجرمـان. *انتظـام اجتماعی*، ۸(۳)، ۱۰۹-۱۲۸.

مردیها، مرتضی. (زمستان ۱۳۹۸). افزایش داده ها و پیشرفت علم. *روش شناسی علوم انسـانی*، ۲۵(۱۰۱)، ۱-۱۴.

وزارت فن‌آوری اطلاعات و ارتباطات. (۱۳۹۶). *نخستین پیمایش کلان داده*. تهران: پژوهشگاه ارتباطات و فن آوری اطلاعات وزارت ICT.

Arnott, D., and Pervan, G.(2014). A Critical Analysis of Decision Support Systems Research Revisited: the Rise of Design Science. *Journal of Information Technology*, 29(4), 269-293.

Benjamin D. Sawyer ،Sunny Fugate. (2016). The Human Factors of Cyber Network. *Research Article USA*, 12(3), 322-326.

Berndtsson,M., Forsberg,D., Stein, D. and Svahn, T. (2018). Becoming a Data-Driven Organisation. 26th European Conference on Information Systems: Beyond Digitization. *Portsmouth: ECIS*, June 23-28.

Bresciania, S., Ciampib, F., Melib, F. and Ferrari, A.(2021). Using Big Data for Co-innovation Processes: Mapping the Field of Data-Driven Innovation, Proposing Theoretical Developments and Providing a Research Agenda. *International Journal of Information Management*, 60(1), 60-75.

Bron, M., Van Gorp, J. and De Rijke, M.(2016). Media Studies Research in the Data-Driven Age: How Research Questions Evolve. *Journal of the Association for Information Science and Technology*, 67(7), 1535-1554.

Dunn Cavelty, M. and Wenger, A.(2020). Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science. *Contemporary Security Policy*, 41(1), 5-32.

Engel, Ch. and Ebel, Ph.(2019). Data-Driven Service Innovation: a Systematic Literature Review and Development of a Research Agenda. *In Proceedings of the 27th European Conference on Information Systems (ECIS)*, Stockholm and Uppsala, Sweden, June 8-14.

Guberina,B. Možnik, D. and Galinec, D.(2017). Cybersecurity and Cyber Defence: National Level Strategic Approach, *Automatika*, 58(3), 273-286.

Guo, W., Du, Z. and Sun, Y.(2018). Data-Driven Deployment and Cooperative Self-Organization in Ultra-Dense Small Cell Networks. *IEEE Access*, 6, 22839-22848.

Husák, M. and Václav, B.(2021). Predictive Methods in Cyber Defense: Current Experience and Research Challenges. *Future Generation Computer System*, 115(3), 517-530.

Lange, M.(2017*). Recommendations for Model-Driven Paradigms for Integrated Approaches to Cyber Defense*, Germany: University of Lübeck.

Leenen, L. and Meyer, T.(2021). *Artificial Intelligence and Big Data Analytics in Support of Cyber Defense*. In Research Anthology on Artificial Intelligence Applications in Security (pp. 1738-1753). IGI Global.

Ma, X.(2022). Information Security Behaviour in Chinese IT Organizations for Information Security Protection. *Information Processing and Management*, 59(1), 47-61.

Miao, Y., Chen, C., Pan, L. and Xiang, Y.(2022). Machine Learning Based Cyber Atacks Targeting on Controlled Information: A Survey. *ACM Computing Surveys*, 54(7), 35-47.

NIST. (2017*). Framework for Improving (Critical Infrastructure Cybersecurity)*. USA: National Institute of Standards and Technology.

RamonSaura, J., Ribeiro, D. and DanielPalacios, S.(2021). A Research Agenda to Understand User Privacy in Digital Market. *International Journal of Information Management*, 60(3), 30-45.

Sangani, S.(2018). *Characteristics of a Data-Driven Organization-Today's Data-Focused Organization-Click through for seven characteristics of a data-driven organization,*USA: Alation's CEO.

Smith, f.(2006). Data Science as an Academic Discipline. *Data Science Journal*, 5(1), 163-164.

Sushaac, I. and Tulder, Å.(2019). Data Driven Social Partnerships: Exploring an Emergent Trend in Search of Research Challenges and Questions. *Government Information Quarterly*, 36(1), 112-128.

Upadhyay, S. and Upadhyay, N.(2017). Future Directions and a Roadmap in Digital Computational Humanities for a Data Driven Organization, *5th International Conference on Information Technol, New Delhi: ITQM*, 1055 – 1060.

Walter, M.(2015). Defining Against Databeaches: Internal Controls for Cybersecurity. *Protiviti*,3(1), 1-37.

Xu, L. D. (2019). Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet of Things Journal*, 6(2), 2103 - 2115.