دریافت مقاله: ۱۴۰۰/۰۹/۰۸ فصلنامهٔ مدیریت نظامی
پذیرش مقاله: ۱۴۰۰/۱۲/۲۱ سال بیست و یکم، شمارهٔ ۴، زمستان ۱۴۰۰
**مقاله پژوهشی** ص‌ص ۱۵۵- ۲۰۶

# طراحی الگوی پدافند سایبری در حوزه نگهداری داده‌های یک سازمان داده‌محور

محمدعلی محامد[۱]، نجلا حریری[۲]* ، فهیمه باب‌الحوائجی[۳]

**چکیده**

پژوهش حاضر با هدف طراحی الگوی پدافند سایبری در سازمان‌های داده‌محور در حوزه نگهداری داده انجام می‌شود. این پژوهش، از نوع اکتشافی و کاربردی بوده، با رویکردی آمیخته با بهره‌گیری از دو روش دلفی و پیمایشی صورت می‌گیرد. در ابتدا، با مطالعه اسناد و منابع موجود مرتبط با سازمان‌های داده‌محور، حوزه نگهداری داده به لحاظ اهمیت سایبری آن در مقایسه با سایر سازمان‌ها و همچنین پنج بُعد شامل شناسایی، حفاظت، کشف، پاسخگویی و بازیابی، مؤلفه‌ها و شاخص‌های پدافند سایبری بر اساس چارچوب NIST شناسایی و احصا می‌شوند. پرسش‌نامه‌ای مبتنی بر طیف لیکرت طراحی و با بهره‌گیری از تعداد ۱۵ نفر خبره، طی اجرای دو مرحله دلفی، هر یک از ابعاد، مؤلفه‌ها و شاخص‌ها بر اساس ویژگی نگهداری داده سازمان‌های داده‌محور، پالایش و پرسش‌نامه نهایی‌سازی می‌شود. در نهایت، با استفاده از روش پیمایش تحلیلی به‌منظور پاسخگویی به پرسش اصلی پژوهش، پرسش‌نامه در اختیار حجم نمونه ۲۸۸ نفره که به صورت تصادفی ساده از جامعه مورد مطالعه انتخاب گردیده‌اند، قرار گرفته و با استفاده از الگوسازی معادلات ساختاری و تحلیل عاملی تأییدی مورد بررسی، تحلیل و در نتیجه، الگوی پدافند سایبری ارائه خواهد شد. پنج بُعد همراه با ۲۱ مؤلفه و ۷۰ شاخص پدافند سایبری در حوزه نگهداری داده در سازمان‌های داده‌محور شناسایی و احصا می‌شوند. در ضمن به استناد انجام تحلیل عاملی تأییدی بر روی الگوی احصا شده، تأثیرگذاری هر یک از بُعدهای پدافند سایبری بر سازمان داده‌محور تأیید و داده‌های تجربی، داده‌های نظری را پشتیبانی و در نهایت الگوی پدافند سایبری مربوطه در سازمان‌های داده‌محور ارائه می‌شود.

**واژه‌های کلیدی:** نگهداری داده‌ها در سازمان داده‌محور، پدافند سایبری، روش دلفی، تحلیل عاملی تأییدی، روش پیمایشی.

---

۱. دانشجوی دکترای علم اطلاعات و دانش‌شناسی گرایش مدیریت دانش، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران.
۲. استاد گروه علوم اطلاعات و دانش‌شناسی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران، (*نویسنده مسئول) Nadjlahariri@gmail.com
۳. دکترای علوم اطلاعات و دانش‌شناسی، گروه علوم ارتباطات و دانش‌شناسی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران، ایران.

**مقدمه**

فناوری اطلاعات به عنوان محور توسعه و به منظور استقرار نظام اطلاع‌رسانی جهانی در حال گسترش و مطرح شدن می‌باشد. کشورهای پیشرفته دنیا، دلالت بر سرعت و وسعت روند تغییرات فناوری اطلاعات دارند؛ به گونه‌ای که تحولات شگرفی در تنوع ساختارهای بنیادین ارتباطی جوامع منجر خواهند شد و عدم توجه به این حرکت جهانی و بسترهای رشد و شکوفایی فناوری اطلاعات، ما را از ارتباط جهانی حذف و وادار به تقلید کورکورانه در به‌کارگیری آن خواهد نمود. فناوری اطلاعات موجب تغییراتی در اختیارات سازمانی شده و ممکن است روی تمرکز یا عدم‌تمرکز سیستم‌های تصمیم‌گیری و کنترل سازمانی اثرگذار باشد (اصلانی‌مناف و همکاران، ۱۳۹۶).

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 سازمان-ها، استفاده از داده و تحلیل به‌وسیلهٔ مدیران و کارکنان به بخشی تفکیک‌ناپذیر از جریان‌های کاری روزمره تبدیل شده است. استفاده صحیح و به موقع از دارایی‌های داده به منظور تصمیم-گیری سریع‌تر بستری 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. عزم و جدیت این‌گونه سازمان‌ها به‌منظور جمع‌آوری داده مرتبط با تمامی جنبه‌های کسب و کار این فرصت را برای آنها فراهم می‌آورد که بتوانند با نگرشی عمیق‌تر اقدام به شناسایی دلایل اصلی مشکلات و مسائل مرتبط با سازمان خود نظیر تغییر رفتار مشتریان و یا روند بازار نمایند (فرابر، ۱۳۹۷). از داده و تجزیه و تحلیل آن صرفاً به منظور بهبود تصمیم‌گیری استفاده نمی‌گردد. بسیاری از شرکت‌های اینترنتی مطرح دنیا نظیر گوگل، فیسبوک، آمازون،eBay و غیره از کلان داده‌ها که ماحصل تراکنش‌هایبرخط (آنلاین) است، نه تنها برای حمایت از تصمیم‌گیری استفاده می‌کنند، بلکه از این حجم داده جهت ایجاد محصولات و ارائه پیشنهادات جدید به مشتریان نیز استفاده می‌نمایند.

نیگام و سریواستاوا[1] (۲۰۱۵) با تحلیل و بررسی قوت‌ها، ضعف‌ها، فرصت‌ها و تهدیدهای استفاده از کلان‌داده در دولت دریافته‌اند که بخش تهدیدات آن شامل جرایم سایبری، وابستگی بخش خصوصی به فناوری اطلاعات، نقض امنیت و حق تکثیر، دغدغه‌های اجتماعی و اخلاقی، محدودیت‌های بودجه، تمرکز بر منافع کوتاه مدت می‌باشند (حقیقی و همکاران، ۱۳۹۷). همان طور که مشاهده می‌شود دو محور از شش محور در حوزه تهدیدات سازمان‌های داده‌محور، نقض امنیت و حق تکثیر و ظهور روندها و پارادایم‌های نوین فناوری اطلاعات و ارتباطات نظیر سرویس‌گرایی، شبکه محوری، محاسبات ابری، اینترنت اشیا، انقلاب صنعتی چهارم و غیره باعث ایجاد تأثیرات و تحولات عمیقی بر تهیه چشم‌اندازها، جهت‌گیری‌ها، سیاست‌ها و راهبردهای دولت‌ها و سازمان‌های نظامی و غیرنظامی گردیده است؛ به طوری که شرایط سوءاستفاده را با رویکردهایی همچون دسترسی‌های غیرمجاز، آسیب رساندن به اطلاعات کاربران و حتی بعضاً به عنوان حملات سایبری و به تعبیری جنگ سایبری را میان دول مختلف فراهم نموده است. سازمان‌های داده‌محور 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. این مقاله در نظر دارد الگویی برای پدافند سایبری در حوزه نگهداری از داده‌ها در سازمان‌های داده‌محور برای اولین بار ارائه نماید.

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 کلان داده‌ها و سامانه‌های تعامل‌پذیر یکپارچه گردیده است، تأثیرات جبران‌ناپذیر بسیاری را به همراه داشته است.

اطلاعات در سازمان‌های دولتی، خصوصی و حتی در کاربردهای فردی به عنوان مولد سرمایه فکری و سرمایه سازمانی می‌باشد. همان طور که مجموعه‌ها برای حفظ دارایی‌های سنتی خود

---

۱. Nigam & Serivastara

مجدانه تلاش می‌کنند و از تمهیدات لازم فیزیکی بهره می‌گیرند تا میزان آسیب را به حداقل برسد، با توجه به موارد پیش‌گفته، رصد و پایش مستمر فضای سایبری و به‌کارگیری سامانه های دفاع در عمق در سازمان‌های داده‌محور به منظور حفظ سرمایه‌های اطلاعاتی بسیار حائز اهمیت می‌باشد. به همین دلیل، توجه ویژه به این حوزه ضروری است. ایران یکی از بزرگترین قربانیان تهاجم سایبری در جهان است. تولید دانش بومی در این حوزه اهمیت شایان توجهی دارد. ایجاد و بهره‌برداری از الگوی پدافند سایبری در سازمان‌های داده‌محور باعث دستیابی به موارد زیر می‌گردد:

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

عدم‌دستیابی به چنین الگویی باعث ایجاد موارد زیر خواهد گردید:

- بروز آسیب‌های محتمل بر روی دارایی‌های داده‌ای 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؛
- افزایش ضریب دسترسی‌ها غیرمجاز.

الگوی پدافند سایبری در سازمان‌های داده‌محور، قابل بهره‌برداری و استفاده از طریق کلیه مجموعه‌های دولتی، غیردولتی، سازمان‌های نظامی، غیرنظامی و شرکت‌های داده‌محور می‌باشد که می‌توان آن را در ابعاد سازمانی مربوطه بومی‌سازی و استفاده نمود. با عنایت به موارد گفته شده بالا، هدف کلی از این مقاله، ارائه الگویی جهت پدافند سایبری در سازمان‌های داده‌محور صرفاً در حوزه نگهداری داده می‌باشد. شایان ذکر است آنچه در منابع موجود قابل دسترس می‌باشد، چارچوب‌های کلی امنیت و پدافند سایبری می‌باشند و همچنین سازمان‌های داده‌محور نیز دارای حوزه‌های سایبری متنوعی است که یکی از آنها حوزه نگهداری داده می‌باشد و انجام فرایندهای پدافند سایبری و میزان اهمیت و اولویت هریک از مراحل، مبتنی بر

الگوی مربوطه، متفاوت بوده، توجه به آن از اهمیت بالایی برخوردار است، و عدم‌برنامه‌ریزی و کسب آمادگی سازمان‌ها در این‌خصوص، با توجه به ارزش داده‌ها (به‌ویژه ماهیت داده‌های عظیم) و فضای رقابتی موجود، آسیب جدی را برای سازمان محتمل سازد. الگوی ارائه شده در این مقاله صرفاً الگویی در حوزه نگهداری از داده‌ها در سازمان‌های داده‌محور می‌باشد که بنا بر اطلاعات نگارنده، سابقه‌ای در منابع داخلی و خارجی وجود ندارد. از اهدف ویژه و کاربردی این الگو می‌توان به موارد زیر اشاره نمود:

- شناسایی منشأ مخاطرات سایبری متصور در سازمان‌های داده‌محور؛
- شناسایی ابعاد پدافند سایبری در سازمان‌های داده‌محور؛
- شناسایی مؤلفه‌ها و شاخص‌های پدافند سایبری در سازمان‌های داده‌محور؛
- شناسایی ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری در سازمان‌های داده‌محور؛
- طراحی الگوی پدافند سایبری سازمان‌های داده‌محور.

با عنایت به موارد مطروحه فوق، سؤالات پژوهش حاضر به صورت زیر مطرح می‌گردند:

۱- آیا حوزه نگهداری داده در سازمان‌های داده‌محور نیازمند پدافند سایبری است؟
۲- ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری در سازمان‌های داده‌محور کدامند؟
۳- دیدگاه خبرگان در مورد میزان اهمیت هر یک از ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری در سازمان‌های داده‌محور چیست؟
۴- ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری در سازمان‌های داده‌محور چگونه است؟
۵- الگوی پدافند سایبری سازمان‌های داده‌محور چگونه است؟

**مبانی نظری و پیشینه‌ی پژوهش**

با توجه به مطالعات و بررسی کتابخانه‌ای به‌عمل‌آمده، در خصوص حوزه‌های موضوعی نو و جدید سازمان‌های داده‌محور و پدافند سایبری به صورت مجزا، مطالعات محدودی صورت پذیرفته است که بعضاً به دلایل سطح طبقه‌بندی و حیطه‌بندی آنها در دسترس نیست و یا بعضاً غیرقابل بهره‌برداری می‌باشند و می‌توان به‌جد عنوان نمود که تا این لحظه، پژوهشی به صورت ترکیبی از موضوعات سازمان‌های داده‌محور و پدافند سایبری صورت نپذیرفته است و

حتی در رابطه با موضوع سازمان‌های داده‌محور در کشور پژوهشی انجام نگردیده است. با عنایت به موارد پیش‌گفته، دراین پژوهش، در نظر است الگوی پدافند سایبری در سازمان‌های داده-محور ارائه گردد.

این پژوهش می‌تواند شروع خوبی برای مطالعات متعددی در حوزه سازمان‌های داده‌محور و مطالعه و ارائه الگوهایی جامع و همه‌گیر در حوزه‌های مختلف به ویژه پدافند سایبری باشد و سازمان‌ها به تناسب ماهیت، مأموریت، ساختار و زیرساخت‌های مربوطه در جهت رسیدن به سازمان‌های داده‌محور اقدام و الگوی مربوطه را بومی‌سازی و بهره‌برداری نمایند. به استناد بررسی انجام شده بر روی پیشینه‌ها و مستندات چاپی و اینترنتی در دسترس، پژوهش‌ها و مطالعات متعددی به‌وسیلهٔ سایر پژوهشگران در خصوص موضوعات سایبر، امنیت داده، داده-کاوی، کلان‌داده‌ها و غیره به صورت کلی صورت پذیرفته است که در ذیل به صورت مختصر به چند نمونه از آنها اشاره می‌گردد.

**سازمان‌های داده‌محور**

**الف) پژوهش‌های داخلی**

۱- الفت و زنجیرچی (۱۳۸۹) پژوهشی با موضوع «تحلیل پوششی داده‌ها (ای.دی.اِی)؛ تحلیل پوششی داده‌ها چابکی سازمان‌ها» را با استفاده از روش تحقیق استنادی و کتابخانه‌ای را با هدف رفع سطح مطلوب چابکی سازمان‌ها، تکنیک تحلیل پوششی داده‌ها را با تعریف ورودی‌ها و خروجی‌های چابکی، برای ارزیابی چابکی بنگاه‌های تولیدی انجام داده است.

۲- سعادتی و مهرشاد (۱۳۹۲) پژوهشی را با عنوان «اینترنت اشیا و برنامه‌های کاربردی کلان‌داده‌ها در شهرهای هوشمند پایدار» با استفاده از روش پژوهش استنادی و کتابخانه‌ای انجام داده‌اند و در آن فرصت توسعه چشم‌انداز اطلاعاتی شهرهای هوشمند، با استفاده از کلان داده، برای دستیابی به سطح مطلوب پایداری محیطی بررسی گردیده است.

۳- 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.

۴- مردی‌ها (۱۳۹۸) پژوهشی با موضوع «افزایش داده‌ها و پیشرفت علم» را با استفاده از روش 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.

## ب) پژوهش‌های خارجی

۱- اوپادهیایی[۱] و همکاران (۲۰۱۷) در پژوهشی با عنوان «مسیرهای آینده و نقشه راه در علوم انسانی محاسباتی دیجیتال برای یک سازمان داده‌محور» و در مطالعه‌ای استنادی و کتابخانه‌ای پیوستگی «علوم محاسباتی دیجیتالی» را مورد بررسی قرار می‌دهد و مسیرهای آینده و نقشه راه ایجاد، پایداری و مفید بودن آن را برای سازمان‌های داده‌محور ارائه می‌دهد.

۲- گو[۲] و همکاران (۲۰۱۸) پژوهشی را با رویکرد استنادی و کتابخانه‌ای با عنوان «استقرار داده‌محور و خود سازمان‌دهی مشارکتی در شبکه‌های سلولی کوچک بسیار متراکم» با توجه به چالش‌های کلیدی که شبکه‌های سلول کوچک به واسطه تراکم بالا به‌طور گسترده‌ای به عنوان فعال کننده اصلی شبکه‌های بی‌سیم با ظرفیت بالا شناخته می‌شود، انجام دادند و در آن ابتدا آخرین تحقیقات را در مورد استقرار سلول‌های کوچک مبتنی بر داده با استفاده از داده‌های ساختاریافته و بدون ساختار رسانه‌های اجتماعی، مرور نماید. پس از آن ترکیبی از تکنیک‌های خوشه‌بندی نامنظم برای شناسایی نقاط حساس و الگوریتم‌های پردازش زبان طبیعی به‌منظور شناسایی نقاط سیاه استفاده گردید و در نهایت پیشرفت‌های اخیر در خود سازمان‌دهی

---

۱. Shalini Upadhyay

۲. Weisi Guo

سلول‌های کوچک مورد بررسی و تجزیه و تحلیل قرار داده‌اند؛ به نحوی که داده‌ها چگونه می‌توانند عملکرد خود سازمان‌دهی را بهبود بخشند.

۳- انگل[۱] و همکارش (۲۰۱۹) پژوهشی را با عنوان «نوآوری خدمات مبتنی بر داده‌ها: مرور ادبیات سیستماتیک و توسعه یک دستور کار تحقیقاتی» را از طریق مرور ادبیات سیستماتیک، برای بررسی ادغام داده‌ها و تجزیه و تحلیل‌ها به عنوان یک واحد تحلیلی در زمینه نوآوری خدماتی که به عنوان نوآوری سرویس داده‌محور نامیده می‌شود، انجام داده‌اند.

۴- سوشاک[۲] و همکاران (۲۰۱۹) پژوهشی را با عنوان «مشارکت‌های اجتماعی داده‌ها محور: بررسی روند نوظهور در جستجوی چالش‌ها و سؤالات تحقیق» با استفاده از روش داده‌بنیاد(گرندِد تئوری) انجام داده‌اند، در پژوهش خود چندین مفهوم را که برای توصیف پدیده مشارکت‌های اجتماعی داده‌محور مورد استفاده قرار می‌گیرند، شناسایی کرده و بر اساس آنها تعریف یکپارچه‌ای از «مشارکت‌های اجتماعی داده‌محور» ارائه داده‌اند.

۵- بِرندسون[۳] 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 شدن به یک سازمان داده‌محور به عنوان چشم اندازی برای سازمان‌های مختلف، انجام داده‌اند. بارها در ادبیات ذکر شده است که سازمان‌های مبتنی بر داده احتمالاً موفق‌تر از سازمان‌هایی هستند که به صورت سنتی تصمیم‌گیری می‌کنند.

۶- ساورا[۴] و همکاران (۲۰۲۱) پژوهشی را با عنوان «از داده تولیدی کاربر به نوآوری داده‌محور: تحقیقی مطرح‌شده برای فهم حریم خصوص کاربر در فروشگاه‌های دیجیتال» با هدف ارائه درک جامع از چالش‌های اصلی مربوط به حریم خصوصی کاربران انجام دادند و در آن با استفاده از روش پژوهش سه مرحله‌ای: (۱) مرور ادبیات سیستماتیک؛ (۲) مصاحبه‌های عمیق در مورد نگرانی‌های مربوط به حریم خصوصی

---

۱. Engel
۲. Iryna Sushac
۳. Berndtsson
٤. Jose RamonSaura

کاربران؛ (۳) مدل‌سازی موضوع با استفاده از یک مدل تخصیص نهفته برای استخراج بینش‌های مربوط به موضوع مطالعه، پژوهش انجام گردیده است.

۷- بِرِسیانی[۱] و همکاران (۲۰۲۱) پژوهشی را با عنوان «استفاده از کلان‌داده برای فرایندهای نوآوری مشترک: ترسیم زمینه نوآوری مبتنی بر داده، پیشنهاد تحولات نظری و ارائه دستور کار تحقیقاتی» به عنوان اولین بررسی ادبی سیستماتیک در مورد ارتباط بین کلان داده‌ها و نوآوری مشترک انجام دادند. از کلان‌داده‌ها به عنوان دیدگاه مشترک تجزیه و تحلیل و همچنین مفهوم تجمیع جریان‌های مختلف تحقیق (نوآوری باز، ایجاد مشترک و نوآوری مشارکتی) استفاده می‌گردد.

## پدافند سایبری

### الف) پژوهش‌های داخلی

۱- شهرکی و همکاران (۱۳۹۲) پژوهشی با موضوع «نقش پدافند غیرعامل در فضای سایبری» را با استفاده از روش تحقیق استنادی تحلیلی به انجام رسانده‌اند که هدف پژوهش بررسی فضای سایبر، امنیت سایبری وسپس پدافند غیرعامل در فضای سایبری می‌باشد و یافته‌های پژوهش بیانگر آن بود که در کشور ما برای امنیت فضای سایبر چالش‌ها وموانعی وجود دارد و به منظور اجرای پدافند سایبری باید اقداماتی راهبردی را به‌کارگرفت.

۲- الهیاری و همکاران (۱۳۹۲) پژوهشی را با موضوع «بررسی تأثیر ابعاد عینی امنیت برکاربری سیستم‌های پرداخت الکترونیکی بواسطه ادراک مشتریان از امنیت و اعتماد» با استفاده از روش پیمایشی- کاربردی و با هدف تعیین تأثیرگذاری ابعاد عینی شامل فرایندهای تراکنش، حفاظت‌های فنی و بیانیه‌های امنیتی بر میزان استفاده از سیستم‌های پرداخت الکترونیک با واسطه‌گری دو بُعد ذهنی امنیت و اعتماد درک‌شده در میان مشتریان انجام داد.

۳- قادری و نصرتی (۱۳۹۲) پژوهشی را با عنوان«فضای سایبر؛ چالش‌های حاکمیت و امنیت پایدار» با استفاده از روش توصیفی - تحلیلی و کتابخانه‌ای به بررسی جغرافیای سیاسی فضای مجازی و از دیدگاه جغرافیای سیاسی به چالش‌های حاکمیت دراین

---

۱. Stefano Bresciani

حوزه پرداخته، ظهور بازیگران جدیدی را که وضعیت آنان منحصراً بر بازیگران سنتی انطباق ندارد را بررسی می‌کنند.

۴- فرزام‌نیا و همکاران (۱۳۹۴) پژوهشی با عنوان «بررسی تکنیک‌های نوین جنگ‌های سایبری و ارایه الگو ساختاری پویا برای مقابله با آن» را انجام داده‌اند و در آن به بررسی تکنیک‌های نوین جنگ‌های سایبری پرداخته و مدلی ساختاری جهت مقابله با تهدیدات این فضا به‌صورت پویا ارائه گردیده است که در واقع در آن به مدل ساختار سازمانی در جنگ سایبری اشاره گردیده است.

۵- قوچانی خراسانی و همکاران (۱۳۹۷) پژوهشی را با موضوع «شناسایی عوامل توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری با رویکرد نظریه داده‌بنیاد» با استفاده از روش پژوهش نظریه داده‌بنیاد انجام داده‌اند که در آن با شناسایی عوامل توسعه نوآوری باز در نهادهای تحقیقاتی امنیت سایبری، به دنبال شناسایی آنها با توجه به شرایط محیطی ایران و ارائه راه‌حل‌هایی برای توسعه این عوامل در نهادهای تحقیقاتی امنیت سایبری بوده است.

۶- رمضان‌زاده و همکارن (۱۴۰۰) پژوهشی از نوع کاربردی با عنوان «بررسی قدرت پدافند سایبری نیروهای مسلح با روش برنامه‌ریزی مبتنی بر سناریو»، با استفاده از روش پژوهش رویکرد آینده‌پژوهی و مبتنی بر روش سناریو به‌منظور ارزیابی قدرت سایبری نیروهای مسلح در بُعد پدافند سایبری 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.

۷- کتابچی و بابک‌پور (۱۴۰۰) پژوهشی با عنوان «چالش‌های امنیتِ سایبری در کشورهای «آسه آن»» را با بهره‌گیری از روش پژوهش توصیفی- تحلیلی انجام داده‌اند و در آن به تبدیل‌شدن امنیت سایبری به یک مشکل اساسی در جهان که منجر به «اقدام آسه آن» در خصوص رفع و مقابله با حوادث در سطح منطقه‌ای و ملی گردیده است، پرداخته‌اند و دستیابی به آن را از طریق بررسی شاخص‌های مربوط به امنیتِ سایبری با موضوعات دفاع در برابر حملاتِ سایبری نوآورانه، راهبردهایی در برابرِ تهدیداتِ امنیتِ سایبری، سیاست‌های دولت و محافظت در برابر حریمِ خصوصی، حمایت از زیرساخت‌های رایانه‌ای در دولت و مسائل حقوقی و اخلاقی در فضای سایبری به عنوان هدف منظور نموده‌اند. 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 اعضای «آسه آن» مورد توجه قرار گیرد.

**ب) پژوهش‌های خارجی**

۱- لو و لی[۱](۲۰۱۵) پژوهشی از نوع کتابخانه‌ای و استنادی با عنوان «مدل اتفاقی دفاع سایبری فعال پویا» به انجام رسانده است و در آن به این مهم اشاره نموده که هیچ مدل ریاضی برای توصیف اثربخشی دفاع سایبری فعال وجود ندارد و با فرض اینکه با بهره‌گیری از مدل جدید فرایند مارکوف که بومی تعامل بین حمله سایبری و دفاع سایبری فعال است، می‌تواند این خلأ را پر نماید، مطالعه خود را دنبال نموده است.

۲- کولینی[۲]و همکاران (۲۰۱۵) مطالعه‌ای کتابخانه‌ای و استنادی با عنوان «مدل توانایی دفاع سایبری: رده‌بندی بنیادین» را به انجام رسانید و در آن به این مهم پرداخت که حملات سایبری در چند سال گذشته، جایی که مهاجمان بسیار زیاد هستند، به میزان قابل‌توجهی حرفه‌ای‌تر، سازمان‌یافته‌تر و حمایت شده به‌وسیلهٔ دیگر بازیگران قدرتمند برای طراحی حملات به سمت اهداف خاص افزایش یافته است. ازاین‌رو برای کمک به توسعه یک برنامه راهبردی برای دفاع در برابر حملات در حال ظهور، یک طبقه‌بندی سطح بالا همراه با یک مدل دفاع سایبری به‌منظور بررسی تعامل و روابط بین عناصر طبقه‌بندی ارائه نمودند؛ به‌طوری‌که در پژوهش خود یک مدل مرجع سایبری که به طور گسترده به‌وسیلهٔ نیروی هوایی ایالات متحده استفاده می‌شود، به عنوان پایه‌ای برای توسعه مدل و طبقه‌بندی مورد استفاده قرار دادند.

۳- گوبرینا[۳] و همکاران (۲۰۱۷) مطالعه‌ای موردی با هدف اصلی راهبرد تشخیص مشکلات سازمانی در اجرای امنیت سایبری و گسترش درک اهمیت این موضوع در جامعه جمهوری کرواسی را با عنوان «امنیت سایبری و دفاع سایبری: رویکرد

---

۱. Hualun Li
۲. Kolini
۳. Boris Guberina

راهبردی در سطح ملی» انجام داده‌اند. در پژوهش اشاره شده به امنیت سایبری که شامل طیف وسیعی از شیوه‌ها، ابزارها و مفاهیم مرتبط با امنیت اطلاعات و فناوری اطلاعات می‌باشد و همچنین متمایز بودن امنیت سایبری در استفاده از فناوری اطلاعات برای حمله به دشمنان و اینکه استفاده از واژه «امنیت سایبری» به عنوان یک چالش کلیدی و مترادف امنیت اطلاعات یا امنیت فناوری اطلاعات مشتریان و دست اندرکاران امنیت را گیج کرده و تفاوت‌های اساسی بین این رشته‌ها را پنهان می‌کند، پرداخته است.

۴- وِنگر[۱] و دون‌کاوِلتی[۲] (۲۰۱۷) مطالعه‌ای توصیفی با عنوان «امنیت سایبری با سیاست‌های امنیتی مطابقت دارد: فناوری پیچیده، سیاست پراکنده و علم شبکه‌ای» انجام داده‌اند. در پژوهش اشاره‌شده پس از شناسایی و بحث در مورد شش محرک از زمینه‌های فناوری، سیاست و علم که در تکامل سیاست امنیت سایبری و نحوه مطالعه آن مؤثر بوده‌اند، سه خوشه تاریخی مشروط را توصیف نموده‌اند.

۵- کلارک[۳](۲۰۱۸) در پژوهشی با عنوان «شبکه‌های دانشی امنیت سایبر» در دانشگاه واشنگتن‌دی‌سی آمریکا با هدف درک حوزه‌های علمی که برای امنیت سایبری در سازمان‌ها مهم هستند، به نحوه توزیع دانش در بین نقش‌ها و واحدها در هماهنگی با اهداف حاکمیت سامانه اطلاعاتی پرداخته است.

۶- زو[۴](۲۰۱۹) مطالعه‌ای کتابخانه‌ای و استنادی با عنوان «تحقیق درباره امنیت سایبری اینترنت اشیا: مروری بر مباحث کنونی تحقیق" را به صورت بررسی نظام‌مند امنیت سایبری اینترنت اشیا» را انجام داد.

۷- هوساک[۵]و همکاران (۲۰۲۱) پژوهشی را با عنوان «روش‌های پیش‌بینی در دفاع سایبری: تجربیات و چالش‌های تحقیقاتی کنونی» به انجام رسانده‌اند و در آن

---

۱. Andreas Wenger
۲. Myriam Dunn Cavelty
۳. Clark
٤. Xu
٥. Martin Husák

جنبه‌های مختلف روش‌های پیش‌بینی در دفاع سایبری را مورد بحث قرار دادند. روش اول از داده‌کاوی برای استخراج سناریوهای حمله مکرر استفاده می‌کند. در روش دوم از نمره شهرت موجودیت شبکه پویا برای پیش‌بینی بازیگران مخرب استفاده می‌گردد و در روش سوم از تجزیه و تحلیل سری‌های زمانی برای پیش‌بینی میزان حملات در شبکه استفاده می‌نمایند.

۸- لینِن[۱] و مِیِر[۲] (۲۰۲۱) پژوهشی را با عنوان «هوش مصنوعی و تجزیه و تحلیل کلان‌داده‌ها در حمایت از دفاع سایبری» و با هدف مفید بودن تشخیص الگوها، همبستگی‌ها، روندها و سایر اطلاعات و اینکه تحلیلگران امنیت سایبری، برای پیش‌بینی، شناسایی، توصیف و مقابله با تهدیدات امنیتی به حجم وسیعی از داده‌های رویداد امنیتی متکی هستند، انجام داده‌اند.

۹- میاو[۳] 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 به‌کارگیری راه‌حل‌های تجزیه و تحلیل پیشرفته، حملات جدید سرقت از الگوریتم‌های یادگیری ماشین برای دستیابی به میزان موفقیت بالا و ایجاد خسارت زیاد استفاده پرداخته‌اند، به طوری‌که تشخیص و دفاع در برابر چنین حملاتی چالش‌برانگیز و فوری شناسایی گردیدند و بنابراین دولت‌ها، سازمان‌ها و افراد باید اهمیت زیادی برای حملات سرقت مبتنی بر یادگیری ماشین (حملات هوشمند) که شامل سه دسته از حملات (فعالیت‌های کنترل‌شده کاربر، اطلاعات مربوط به مدل یادگیری ماشین کنترل شده و اطلاعات احراز هویت کنترل‌شده) می‌باشد، قائل شوند.

۱۰- ما[۴] (۲۰۲۲) پژوهشی را با عنوان «رفتار امنیت اطلاعات متخصصان سامانه اطلاعات در سازمان‌های فناوری اطلاعات چین برای حفاظت از امنیت اطلاعات» با بهره‌گیری

---

۱. Louise Leenen
۲. Thomas Meyer
۳. Miao
۴. Ma

از روش پژوهش پیمایشی راه‌های ایجاد انگیزه در متخصصان سامانه‌های اطلاعاتی برای حفاظت از امنیت اطلاعات در برابر خطرات احتمالی، با تکیه بر چارچوب‌های نظری نظریه انگیزش حفاظتی و نظریه رفتار برنامه‌ریزی‌شده 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 قابل‌توجهی تحت‌تأثیر 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 امنیت اطلاعات تأثیر مثبت داشت و ارتباط نزدیک با زیردستان نقش مهمی در تضمین امنیت اطلاعات ایفا می‌کند.

## جمع‌بندی پیشینه‌های مرتبط با پژوهش

به استناد مطالعه و بررسی پیشنیه‌ها، در خصوص مباحث مرتبط با مفاهیم سایبر، داده‌محور و سازمان، مطالعات متنوعی اما محدود (به علت نو بودن مفاهیم داده‌محور و حوزه سایبر) صورت پذیرفته است و حتی در حوزه پدافند سایبری به علت ارزش محرمانگی و حیطه‌بندی محتوا، به واسطه محدودیت‌های نشر آنها برای پژوهشگران سازمانی، دسترسی به این منابع را غیرممکن نموده است.

## نقاط اشتراک

به عنوان نقطه اشتراک مطالعات انجام شده در حوزه سایبر، در اغلب موارد با رویکرد جنگ سایبری (به عنوان عرصه نبرد)، حملات مربوطه و بیشتر از همه به حوزه بدافزارها (کرم، تروجان، ویروس‌ها و غیره) پرداخته است و در حوزه پدافند/امنیت سایبری هم بیشتر مطالعات بر اساس مفاهیمی چون دفاع در عمق (دفاع چند لایه) و ابزارهای مربوط به آن نظیر دیواره آتش صورت پذیرفته است و بیشتر ماهیتی اجرایی و فنی دارند، در حوزه چارچوب‌ها، الگوها و مدل‌های حوزه سایبر نیز عمدتاً مستندات ماهیتی مفهومی، کلی و بدون توجه به سازمانی با ویژگی‌ها/حوزه‌های خاص ارائه گردیده‌اند.

## نقاط افتراق و نوآوری پژوهش فعلی

در بررسی و مطالعه کتابخانه‌ای ساخت‌یافته صورت پذیرفته در خصوص موضوعات داده‌محور، در تعداد زیادی از نتایج جستجو عبارت داده‌محور به رویکرد پژوهش‌های داده‌بنیان ارجاع داده می‌شود (در حالی که دو مفهوم کاملاً مجزا نسبت به یکدیگر می‌باشند) که با بررسی و پالایش روی مستندات و نتایج جستجو، پژوهش‌های ارزشمند، اما محدود که در خصوص ویژگی‌ها و خصوصیات سازمان‌های داده‌محور، نحوه و ارزش تصمیم‌گیری در این سازمان‌ها و همچنین چگونگی تبدیل شدن به این سازمان‌ها، پرداخت شده است. نتایج حاصل از پژوهش حاضر و بررسی سایر مطالعات انجام‌شده 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 احصاشده 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، هویت‌سنجی، نظارت مستمر امنیتی، آموزش و یادگیری سازمانی، هوشمندی، سیاست لایه‌ای و دفاع در عمق، ارتقای 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 می‌باشد. شایان ذکر است هیچ‌یک از مطالعات انجام‌شده، علی‌رغم اشاره به برخی نتایج و شاخص‌های مرتبط با پدافند سایبری، هیچ‌گونه الگو، مدل و یا حتی فرایند در سازمان‌های داده‌محور ارائه ننموده‌اند. نتایج حاصل از پژوهش حاضر، منتج به ارائه الگوی پدافند سایبری در سازمان‌های داده‌محور خواهد شد که بر اساس انجام تحلیل عاملی بر روی داده‌های استخراج‌شده از مرحله کمی پژوهش صورت پذیرفته است، ضمن آنکه در هیچ یک از نتایج حاصل از بررسی مطالعات و منابع به‌روز ارجاع داده‌شده در این پژوهش، تحلیلی بر میزان اثرگذاری ابعاد مختلف بر روی سازمان‌های داده‌محور انجام نشده و صرفاً به ذکر تعریف بسنده شده است. درحالی‌که پژوهش حاضر با عنوان الگوی پدافند سایبری در حوزه نگهداری داده‌های یک سازمان داده‌محور، هم از جنبه حوزه‌های موضوعی (سازمان داده‌محور و پدافند سایبری) و هم از جنبه ارتباط بین حوزه‌ای (پدافند سایبری سازمان‌های داده‌محور) و هم کل موضوع که ارائه الگوی پدافند سایبری مختص سازمان‌های داده‌محور می‌باشد، پژوهشی نو و بدیع می‌باشد.

**تعاریف پدافند سایبری و سازمان داده‌محور**

**الف) پدافند سایبری**

- تعریف نظری: به اقداماتی که برای ایجاد امنیت در فضای سایبر انجام می‌شود، اقدامات پدافند سایبری می‌گویند (ابوالحسینی، ۱۳۹۲).
- تعریف عملیاتی: در این پژوهش کلیه اقداماتی که دارایی‌های سایبری و مأموریت‌های سازمانی وابسته به آن را در برابر هرگونه رخداد یا تهدید سایبری مصون می‌نماید، منظور گردیده است.

**ب) سازمان داده‌محور**

- تعریف نظری: سازمانی است که تفکر استفاده مستمر از داده جهت تجزیه و تحلیل و تصمیم‌گیری مبتنی بر بینش در تار و پود آن پرورش و نهادینه شده باشد (فرابر، ۱۳۹۷).
- تعریف عملیاتی: در این پژوهش سازمان‌هایی رقابتی و مبتنی بر داده (داده‌ها به عنوان اصلی‌ترین سرمایه سازمانی، ارزش‌گذاری می‌گردند)، یک‌سری حوزه‌های سایبری که مختص آنها می‌باشند، آنها را از سایر سازمان‌ها متمایز می‌نماید.

**تعریف، ویژگی و اهمیت کلان‌داده‌ها**

امروزه، در محیط آشوب‌ناک رقابتی، سازمان‌ها با چالش‌های جدی روبرو هستند و هر چه اندازه سازمان‌ها بزرگتر می‌شود، مسائل و مشکلات هم پیچیده‌تر و عمیق‌تر می‌شوند؛ به گونه‌ای که با روش‌های سنتی مدیریت و یا راهبردهای مبتنی بر شهود و یا خبرگی شخصی دیگر امکان پاسخگویی و تدوین راهبردهای اثربخش در سازمان وجود ندارد. از سوی دیگر، سازمان‌های بزرگ با حجم عظیمی از اطلاعات روبرو هستند، که از محیط عملیاتی آنها جمع‌آوری شده است. اطلاعاتی نظیر تراکنش‌های مالی، نظرات و پیشنهادهای مشتریان، تعاملات واحدهای فروش، پرسش و پاسخ واحدهای خدماتی و پشتیبانی، اطلاعات کارکنان، شبکه‌های اجتماعی و ده‌ها منبع داده دیگر که به‌طورمرتب در حال تولید اطلاعات هستند.

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 تحلیل 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[۳] سرعت[۴] تنوع[۵] صحت[۶] اعتبار[۷] نوسان[۸] نمایش[۹] و ارزش[۱۰] می‌باشند (کل‌کلی، منصور؛ رجایی، امیر، ۱۳۹۶).

از دیدگاه کلان، کلان‌داده را می‌توان به عنوان قید یا پیوستگی در نظر گرفت که به شکلی دقیق دنیای فیزیکی، جامعه انسانی و فضای سایبری را به هم متصل می‌کند. اینجا دنیای فیزیکی بازتابی در فضای سایبری دارد، به واسطه اینترنت، اینترنت اشیا و دیگر فناوری‌های اطلاعاتی به شکل کلان‌داده تجسم می‌یابد، در حالی‌که جامعه انسانی کلان‌داده خود را مبتنی بر انگاشت در فضای سایبری به واسطه مکانیسم‌هایی مانند ارتباط انسان - کامپیوتر، ارتباط مغز - ماشین و اینترنت ـ موبایل تولید می‌کند. در این معنا، کلان‌داده می‌تواند اساساً در دو دسته جای گیرد که عبارتند از داده‌هایی از دنیای فیزیکی که معمولاً به واسطه سنسورها، آزمایش‌ها و مشاهدات علمی (مانند داده‌های بیولوژیکی، داده‌های عصبی، داده‌های نجومی و داده‌های سنجش از راه دور) و داده‌هایی از جامعه انسانی که اغلب حاصل چنین منابع یا دامنه‌هایی مانند شبکه‌های اجتماعی، اینترنت، سلامت، امور مالی، اقتصاد و حمل و نقل هستند، به دست می‌آیند. کلان‌داده بر اساس اهمیت و ارزش بسیار زیادی که دارد، اساساً شیوه

---

۱. Data Warehouse
۲. Business Intelligence
۳. Volume
۴. Velocity
۵. Variety
۶. Veracity
۷. Validity
۸. Volatility
۹. Visualization
۱۰. Value

زندگی، کار و تفکرمان را تغییر می‌دهد و دگرگون می‌سازد (شانبرگر[۱] و همکاران، ۲۰۱۳).

**کلان‌داده‌ها در سازمان**

به‌کارگیری فناوری کلان‌داده‌ها در سازمان مستلزم استفاده از طیفی از فناوری‌ها در مجموعه‌ای از فرایندهای 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 به‌صورت غیرمتمرکز اداره کنید؛ چون این روش باعث می‌شود که اعضای تیم یک رویه مشخص را در فرایندها به کار بگیرند. از طرف دیگر تیم‌های متمرکز از کسب و کار فاصله می‌گیرند و این قضیه ممکن است باعث شود که راه‌کارهایی که این تیم تولید می‌کند، غیرعملی باشد و در سازمان پذیرفته نشود. علاوه بر این اضافه کردن یک واحد سازمانی جدید پیچیدگی جدیدی به سازمان اضافه می‌کند، چون این واحد قبلاً جزء واحدهای سازمان نبوده است و از این پس باید تلاش کند تا با خلق ارزش برای سازمان هویتی برای خود کسب کند (دینسمر و چمبر، ۲۰۱۴). مزایای دیگری نیز برای سازمان‌دهی متمرکز وجود دارد. اولاً متخصصان علم داده کمیاب هستند و متمرکزسازی امکان استفاده بهینه از آنها را فراهم می‌کند، همین‌طور می‌تواند به پیشرفت افراد کمک کند، چون اعضای تیم علم داده در کنار هم کار می‌کنند و می‌توانند از هم یاد بگیرند. چنین ساختاری به جذب راحت‌تر نیروها کمک می‌کند، چون تعهد سازمان را به خلق ارزش از داده‌ها نشان می‌دهد. مطالعات شرکت اکسنچر نشان داده است، که متخصصان علم داده در ساختارهای متمرکز بیش‌تر جذب کار می‌شوند و بیش‌تر تمایل دارند در همان شرکت به فعالیت‌های خود ادامه دهند. همین‌طور ساختار متمرکز برای پروژه‌هایی که اهمیت راهبردی دارند، مناسب‌تر است (سهرابی و همکاران، 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 فعالیت‌

---

۱ Schonberger

های 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 معمولاً هماهنگ کار نمی‌کنند و همین امر باعث به‌وجود آمدن مشکلاتی برای تجمیع این فعالیت‌های واحدها می‌شود (دینسمر و چمبرز[۱] ۲۰۱۴). در روش غیرمتمرکز، تعیین اولویت‌های سازمان و استفاده مؤثر از نیروها به دشواری صورت می‌گیرد. این مدل برای سازمان‌های بزرگ با کسب و کارهای متفاوت که اشتراکات کمی دارند، مناسب است. حتی با وجود استفاده از این مدل توصیه می‌شود که گروهی فراتر از واحدهای کسب و کار از متخصصان علم داده تشکیل شود تا بتوانند تجربیاتشان را به اشتراک بگذارند.

در روش ترکیبی ساختارهای متمرکز و غیرمتمرکز با هم ترکیب می‌شوند تا از مزیت هم‌سویی با کسب و کار و به اشتراک گذاشتن تجربیات به طور همزمان استفاده شود و نیروی انسانی کمیاب به درستی به کار گرفته شود. در این روش تیم در مواردی مثل تشکیل گروه، به اشتراک‌گذاری تجربیات و آموزش متمرکز عمل می‌کند و برای هم‌سویی با کسب و کار و پیدا کردن درک عمیق‌تری از آن به صورت غیرمتمرکز عمل می‌کند. هرچه درک اعضای تیم علم داده از کسب و کار بیشتر شود، سازمان بیشتر به نتایج کار آنها اعتماد می‌کند، محصولاتی که تولید می‌کنند، بیش‌تر پذیرفته می‌شود و این امر باعث می‌شود این تیم‌ها بتوانند بیشترین ارزش را برای سازمان‌ها خلق کنند.

**تفاوت‌های سازمان‌های داده‌محور[۲] با سایر سازمان‌ها**

مکافی و همکاران، تفاوت‌های سازمان‌های داده‌محور با سایر سازمان‌ها را در تدوین فرضیه‌ها و حل مسئله 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 سؤال‌هایی که با داده‌ها می‌توان پاسخ داد؛
- فرموله کردن سؤال؛

۱. Dinsmore & Chambers

۲. Data Driven Organization

- بررسی داده‌های فعلی برای یافتن سؤال درست برای مطرح کردن؛
- ایجاد چارچوبی برای اجرای آزمایش روی داده‌ها؛
- تحلیل نتایج برای ایجاد بینش‌های جدید راجع به سؤال.

(Brynjolfsson,e. Mcafee,a. Goldbloom,a. Howard,j. 2014).

**چارچوب امنیت سایبری[۱]**

این چارچوب در سال۲۰۱۴ توسطّ NISTو با هدف ارائه یک چارچوب برای ارتقای 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. همان‌گونه که از نام این چارچوب پیدا است، «مجموعه‌ای از اصول و ایده‌ها است که در زمان تصمیم‌گیری و برنامه‌ریزی (برای شکل‌دهی به این تصمیمات و جهت‌گیری‌ها) بهره‌برداری می‌شوند و همچنین روشی برای سازمان‌دهی مباحث پیرامون امنیت سایبری قلمداد می‌شود. این چارچوب با تکیه بر استانداردها، دستورالعمل‌ها و شیوه‌ها، یک طبقه‌بندی و مکانیسم مشترک را برای سازمان‌ها فراهم می‌کند. چارچوب فوق رهیافتی مبتنی بر مخاطره است و 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،[۳] ۲۰۱۷). هستهٔ چارچوب امنیت سایبر NIST 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،[۴] حفاظت،[۵] کشف،[۶] پاسخ‌گویی، بازیابی؛ این پنج

---

۱. NIST Cyber Security Framework

۲. National Institute of Standards and Technology

۳. NIST

۴. Identify

۵. Protect

۶. Detect

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[۳]، ANSI/ISA[۴]، ISO/IEC و Cobit) به منظور بهره‌برداری معرفی می‌گردند. شرح پنج عملکرد اصلی در زیر ارائه شده است:

- **شناسایی**: ایجاد و توسعه درک سازمانی در رابطه با مدیریت مخاطرات امنیت سایبری سامانه، دارایی‌ها، داده و قابلیت‌ها. فعالیت‌های این عملکرد به عنوان مبنا و پایه‌ای برای استفاده مؤثر از چارچوب قلمداد می‌شوند. درک محیط تجاری (محیط مأموریت‌های 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 راهبردهای مدیریت مخاطره خود متمرکز و اولویت‌دهی نماید.
- **حفاظت**: توسعه و به‌کارگیری حفاظ‌های (کنترل‌های حفاظتی) مناسب به‌منظور اطمینان از استمرار ارائه خدمات زیرساخت‌های حیاتی. فعالیت‌های ذیل این عملکرد توانایی محدودکردن یا مقابله با تأثیرات رویدادهای بالقوه امنیت سایبری را تأمین می‌کنند؛ مثال‌هایی 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.



۱. Respond

۲. Recover

۳. Retrievable from: http://www.counciloncybersecurity.org

۴. Retrievable from: https://www.isa.org/templates/one

- **پاسخگویی:** توسعه و به‌کارگیری اقدامات مناسب به منظور برخورد و واکنش به رویدادهای امنیت سایبری کشف‌شده. این عملکرد امکان محدودکردن دامنه تأثیرات 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 به‌خاطر رویدادهای امنیت سایبری تضعیف یا مختل شده‌اند.

**روش‌شناسی پژوهش**

ماهیت این پژوهش از نوع اکتشافی و کاربردی است؛ از این رو، به منظور حل مسئله در این پژوهش (الگوی پدافند سایبری در حوزه نگهداری داده در سازمان‌های داده‌محور)، از روش و رویکردی آمیخته با بهره‌گیری از روش‌های دلفی (روش کیفی) و پیمایشی تحلیلی (روش کمی) استفاده گردید. ابتدا با بررسی و مطالعه منابع مختلف مشتمل بر کتب، مقالات، منابع اینترنتی و غیره، حوزه نگهداری داده سازمان‌های داده‌محور شناسایی و احصا شد، ضمن مطالعه چارچوب‌های پدافند سایبری، چارچوب NIST با توجه به ماهیت (نو بودن، جامعیت و توصیه خبرگان حوزه پدافند سایبری) شناسایی و انتخاب گردید.

سپس پرسش‌نامه‌ای ساخت‌یافته مبتنی بر ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری و حوزه نگهداری داده سازمان‌های داده‌محور طراحی و با بهره‌گیری از روش دلفی (رویکرد کیفی) و استفاده از نظر خبرگان مورد مطالعه قرار گرفت و در نهایت به منظور سنجش و ارزیابی با بهره‌گیری از روش پیمایشی تحلیلی (رویکرد کمی) و استفاده از الگوسازی معادلات ساختاری، که در واقع روشی کمّی بوده و به محقق کمک می‌کند تا پژوهش خود را از نظر مطابقت مدل نظری (مدل تئوری) با داده‌های واقعی (داده‌های تجربی) که با نمونه‌گیری از جامعه جمع‌آوری به‌دست می‌آید، مورد بررسی قرار دهد، استفاده گردیده است.

**جامعه آماری، روش نمونه‌برداری و حجم نمونه**

در پژوهش حاضر با توجه به ماهیت آن، دو جامعه آماری در هر یک از مراحل پژوهش (دلفی و پیمایشی تحلیلی) مورد استفاده قرار می‌گیرد:

**جامعه اول: بخش مطالعه دلفی (کیفی پژوهش)**

در این مرحله، جامعه مورد مطالعه تعداد ۱۵ نفر از خبرگان و صاحب‌نظران پدافند سایبری و شاغل در سازمان‌های داده‌محور با مدرک تحصیلی کارشناسی ارشد (۱۰ نفر، ۸ نفر مرد و ۲ نفر

زن) و دکتری (۵ نفر مرد) و ۵ سال سابقه کار تخصصی انتخاب گردیدند.

**جامعه دوم: بخش مطالعه پیمایشی تحلیلی (کمی پژوهش)**

با توجه به مطالعات و بررسی‌های انجام‌شده، در مجموع تعداد ۸۶ سازمان شناسایی گردیدند که از این تعداد، ۴۴ سازمان داده‌محور در سطح کشور (مانند ثبت احوال، کارت سوخت، هواشناسی، پست، گمرکات، اپراتورهای تلفن همراه و غیره)، ۳۶ مرکز آپا در مراکز دانشگاهی و ۶ مجموعه پشتیبانی‌کننده و متولی در حوزه پدافند سایبری در سطح کشور (سازمان پدافند غیرعامل و غیره) مورد استفاده قرار گرفتند.

شایان ذکر است اغلب این سازمان‌ها ماهیت دولتی و بعضاً ماهیت نیمه‌دولتی و خصوصی دارند. این سازمان‌ها عمدتاً به منظور پاسخگویی اولیه به آسیب‌های محتمل بر روی سرمایه‌های سایبری، مجموعه‌هایی را در قالب امنیت و پدافند سایبری، سازمان‌دهی نموده‌اند و در مواردی که با آسیب‌های جدید و حساس مواجه می‌شوند، با همکاری سازمان پدافند غیرعامل کشور و مجموعه‌هایی چون مراکز ماهر[۱] مهار[۲] و تعداد ۳۸ مجموعه که در تعدادی از مراکز تخصصی و دانشگاهی کشور (دانشگاه‌هایی نظیر صنعتی شریف، مالک اشتر، امیرکبیر، شیراز، صنعتی اصفهان و غیره) به عنوان آپا[۳] ایجاد گردیده‌اند، عمل می‌نمایند. برای اجرای مرحله کمّی پژوهش حاضر، جمعاً در مجموع ۱۱۴۴ نفر به عنوان جامعه مورد مطالعه در سازمان‌های داده‌محور و مراکز پشتیبانی‌کننده حوزه پدافند سایبری در سطح کشور با مدرک تحصیلی حداقل کارشناسی و حداقل پنج سال سابقه فعالیت در حوزه پدافند سایبری و آگاه نسبت به مفاهیم سازمان‌های داده‌محور و کلان داده‌ها شناسایی گردیدند که با استفاده از فرمول

---

۱. توجه به اهمیت پاسخگویی به رخدادهای فضای تبادل اطلاعات و ایجاد مراکز پاسخگویی به حوادث فضای مجازی که در اغلب کشورها با عنوان مراکز CERT انجام شده است، مرکز ماهر به عنوان CERT ملی ایران در سال ۱۳۸۷ ایجاد و در سطح ملی فعالیت گسترده‌ای را برای پیشگیری و مقابله با حوادث فضای تبادل اطلاعات به‌عهده دارد.

۲ . مرکز مقابله هماهنگ امنیت رایانه‌ای.

۳ . آپا مخفف آگاهی‌رسانی، پشتیبانی و امداد است و معادل کلمه CERT است که از ترکیب کلمات Computer Emergency Response Team به معنای گروه واکنش و هماهنگی رخدادهای رایانه‌ای (گوهر) می‌باشد.

کوکران[۱](به شرح ذیل) تعداد حجم نمونه ۲۸۸ نفر تعیین گردیدند.

$$n = \frac{\frac{z^2 pq}{d^2}}{1 + \frac{1}{N}\left(\frac{z^2 pq}{d^2} - 1\right)}$$

به‌طوری‌که در آن، $n$ بیانگر حجم نمونه، $N$ حجم جامعه آماری، z درصد خطای معیار یا ضریب اطمینان قابل قبول، p نسبتی از جامعه دارای صفت معین (مثلاً، جمعیت مردان)، $q=1-p$ نسبتی از جمعیت فاقد صفت معین (مثلاً جمعیت زنان) و $d$ درجه اطمینان یا دقت احتمالی مطلوب می‌باشند.

**ابزار اندازه‌گیری**

در پژوهش حاضر گردآوری اطلاعات با بهره‌گیری از روش‌های کتابخانه‌ای، دلفی و پرسش‌نامه انجام گردیده است. در ابتدا ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری و همچنین حوزه نگهداری داده سازمان‌های داده‌محور شناسایی گردید و برای تأیید و نهایی‌سازی ابعاد، مؤلفه‌ها و شاخص‌های اشاره‌شده با بهره‌گیری از خبرگان و انجام روش کیفی دلفی و برای پاسخگویی به پرسش‌های پژوهش از روش کمی پیمایشی تحلیلی استفاده شده است. در بخش کیفی و کمی این پژوهش از دو پرسش‌نامه استفاده‌شده و به صورت الکترونیکی و چاپی برای جامعه نمونه پژوهش ارسال گردید و سپس جمع‌آوری و مورد تحلیل قرار گرفت.

**ابزار بخش کیفی پژوهش**

به منظور انجام بخش کیفی، پرسش‌نامه‌ای با درج ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری در سطرها و درج حوزه نگهداری داده سازمان‌های داده‌محور در ستون و با بهره‌گیری از طیف لیکرت پنج‌گزینه‌ای با امتیازهای خیلی‌کم تا خیلی‌زیاد و با ارزش عددی ۱ تا ۵ تهیه گردید و اجرای پنل دلفی در دو دور، دور اول از ۱۳۹۹/۰۲/۲۰ الی ۱۳۹۹/۰۴/۲۰، ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری بر اساس ویژگی نگهداری داده سازمان‌ها با بهره‌گیری از نظرات خبرگان مورد پالایش و تجزیه و تحلیل قرار گرفت و در دور دوم که از ۱۳۹۹/۰۶/۱۰ تا

۱. فرمول کوکران یکی از پرکاربردترین روش‌ها برای محاسبه حجم نمونه آماری است.

۱۳۹۹/۰۸/۲۸ صورت پذیرفت، اهمیت و اولویت آنها به استناد نظرات خبرگان تعیین گردید.

**ابزار بخش کمی پژوهش**

ابزار گردآوری داده‌ها در این مرحله پرسش‌نامه محقق‌ساخته و حاصل از تجزیه و تحلیل داده‌های بخش کیفی می‌باشد که به منظور پاسخگویی به سؤالات پژوهش و به‌صورت چاپی و الکترونیکی برای متخصصان شاغل در سازمان‌های داده‌محور، مراکز آپا و سازمان‌هایی که در کشور متولی صیانت از دارایی‌های سایبری می‌باشند و به صورت تصادفی ساده انتخاب شده بودند، ارسال گردید. پرسش‌نامه اشاره‌شده برگرفته از اجزای ذیل می‌باشند:

- ابعاد پدافند سایبری در قالب پنج بُعد (شناسایی، حفاظت، کشف، پاسخگویی و بازیابی) صرفاً در حوزه نگهداری داده در سازمان‌های داده‌محور).
- مؤلفه‌های پدافند سایبری در قالب بیست و سه مؤلفه در حوزه نگهداری داده سازمان‌های داده محور.
- شاخص‌های پدافند سایبری در قالب هفتاد شاخص در حوزه نگهداری داده سازمان‌های داده‌محور.

**مراحل اجرایی انجام پژوهش**

در پژوهش حاضر با توجه به نو بودن دو حوزه پدافند سایبری و همچنین سازمان‌های داده‌محور، در ابتدا با انجام مطالعه استنادی و کتابخانه‌ای و بررسی بیش از ۱۴۶منبع، مشتمل بر ۵۱ منبع در حوزه پدافند سایبری و ۹۹ منبع در حوزه سازمان‌های داده‌محور مشتمل بر منابع داخلی در بازه زمانی ۱۳۸۴ الی ۱۳۹۹ و منابع خارجی در بازه زمانی ۲۰۱۰ الی ۲۰۲۲، از قبیل کتب، مقالات، استانداردها و گزارش‌های علمی و تخصصی صورت پذیرفت و فرآیند پژوهش طی مراحل ذیل دنبال گردید:

**الف) احصای ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری**

در این قسمت با بهره‌گیری از منابع، مستندات و به‌ویژه چارچوب پدافند سایبری NIST و انجام تحلیل محتوا بر روی اسناد، ابعاد (پنج بُعد: شناسایی، حفاظت، کشف، پاسخگویی و بازیابی)، مؤلفه‌ها (۲۱ مؤلفه) و شاخص‌های پدافند سایبری (۱۳۰ شاخص) احصا شدند.

**ب) احصای حوزه‌های سازمان‌های داده‌محور**

در این قسمت با انجام مطالعه کتابخانه‌ای از منابع، به‌ویژه کتب و مقالات و با توجه به نو بودن و محدود بودن منابع در این حوزه موضوعی، بررسی‌ها بر اساس کلید واژگانی همچون سازمان داده‌محور، داده در سازمان، سازمان‌های داده‌محور کدامند، کلان‌داده‌ها و غیره صورت پذیرفت که با انجام تحلیل محتوا بر روی منابع و درنظر گرفتن میزان تکرار آنها در منابع متعدد، تعداد شش حوزه نگهداری داده‌ها، تنوع داده‌ها، یکپارچگی دسترسی به داده‌ها، یکپارچگی ابزارهای تجزیه و تحلیل داده‌ها، جریان داده‌ها، فرهنگ سازمانی داده‌محور احصا شد و سپس، حوزه نگهداری داده‌ها به‌صورت خاص به لحاظ اهمیت سایبری آن برای بررسی انتخاب گردید.

**ج) تنظیم پرسش‌نامه**

پس از احصا ابعاد، مؤلفه‌ها، و شاخص‌های پدافند سایبری و همچنین درنظر گرفتن حوزه نگهداری داده در سازمان‌های داده‌محور، و با توجه به متدولوژی کیفی این پژوهش که روش دلفی اتخاذ گردیده بود، پرسش‌نامه‌ای به شرح ذیل با بهره‌گیری از طیف لیکرت پنج‌گزینه‌ای با امتیازهای خیلی‌کم، کم، متوسط، زیاد و خیلی‌زیاد و با ارزش عددی ۱ تا ۵، طراحی و هر یک از ویژگی‌ها با توجه به یافته‌ها از منابع مختلف و هم‌فکری با خبرگان، به صورت عملیاتی تعریف گردیدند و به ازای هر مؤلفه، سطری برای درج شاخص پیشنهادی نیز در نظر گرفته شد که در ابتدا پرسش‌نامه، با ۱۰۴ شاخص طراحی و تنظیم گردیده بود. به منظور بررسی روایی و پایایی، پرسش‌نامه در اختیار ۵ نفر از خبرگان حوزه پدافند سایبری و مسلط به سازمان‌های داده‌محور با مقطع تحصیلی دکتری و حداقل ۱۵ سال سابقه کار، قرار گرفت و با نظر و هم‌فکری خبرگان شاخص‌هایی که قابلیت همپوشانی داشتند، بازنگری گردیدند و به ۵ بعد، ۲۱ مؤلفه و ۷۰ شاخص تقلیل یافتند و پس از آن پرسش‌نامه بهینه شده، مورد تأیید ۵ نفر خبره قرار گرفت.

**جدول شماره (۱): وضعیت آمایش ابعاد، مؤلفه‌ها و شاخص‌ها در پرسش‌نامه**

| ردیف | عنوان بعد | تعداد مؤلفه | تعداد شاخص |
|---|---|---|---|
| ۱ | شناسایی | ۵ | ۲۰ |
| ۲ | حفاظت | ۵ | ۲۳ |
| ۳ | کشف | ۳ | ۱۲ |
| ۴ | پاسخگویی | ۵ | ۱۰ |
| ۵ | بازیابی | ۳ | ۵ |

**د) اجرای مرحله کیفی پژوهش به روش دلفی**

پس از تثبیت پرسش‌نامه طی فرایند اشاره شده در بالا، بخش کیفی پژوهش با گزینش تعداد ۱۵ نفر از خبرگان و صاحب نظران حوزه پدافند سایبری مسلط به حوزه سازمان‌های داده‌محور و کلان‌داده‌ها با مدرک تحصیلی کارشناسی ارشد (۱۰ نفر، که ۸ نفر مرد و ۲ نفر خانم می‌باشند) و دکتری (۵ نفر مرد) و حداقل ۵ سال سابقه کار تخصصی، مرحله اول دلفی انجام گردید و پرسش‌نامه‌ها در اختیار این ۱۵ نفر به صورت حضوری و بعضاً رایانامه قرار گرفت. پس از دریافت پاسخنامه‌ها در مرحله اول دلفی، میانگین نظرات به ازای هر شاخص محاسبه و با افزایش دو ستون یکی با عنوان «نظر قبلی شما» و دیگری «میانگین نظرات همه شرکت-کنندگان» پرسش‌نامه به ازای هر نفر خبره به صورت مجزا (با توجه به پاسخ‌های قبلی) تنظیم و در اختیار خبرگان اشاره شده قرار گرفت.


**شکل شماره (۳): نمونه بخشی از پرسش‌نامه مرحله دوم دلفی**

پس از جمع‌آوری سری دوم پرسش‌نامه‌های دلفی، با استفاده از نرم‌افزارSPSS، ضریب همبستگی (کندال)[۱](حبیبی، ۱۳۹۷) برای پرسش‌نامه محاسبه گردید و به استناد آن، در حوزه نگهداری دادهٔ سازمان‌های داده‌محور مورد بررسی و تحلیل قرار گرفت که به دلیل عدم‌توافق نظرات خبرگان، تعداد سه شاخص حذف شدند و پرسش‌نامه با توجه به حذف موارد احصاشده از نتیجه ضریب همبستگی کندال، مجدداً بازنگری و پیاده‌سازی شد و در نهایت پرسش‌نامه به‌صورت شکل شماره (۳) طراحی و به منظور اجرای فاز دوم (کمی) پژوهش آماده گردید.

**ه) اجرای مرحله کمی پژوهش**

روش نمونه‌گیری در این مرحله، تصادفی ساده بوده و جامعه مورد مطالعه در پژوهش حاضر متشکل از ۸۶ سازمان می‌باشد که از این تعداد، ۴۴ سازمان داده‌محور در سطح کشور، ۳۶ مرکز آپا در مراکز دانشگاهی و ۶ مجموعه پشتیبانی‌کننده و متولی در حوزه پدافند سایبری در سطح کشور مورد استفاده قرار گرفتند. مراکز آپا کشور در این پژوهش، دانشگاه صنعتی شریف، دانشگاه صنعتی امیرکبیر، دانشگاه یزد، دانشگاه صنعتی اصفهان، دانشگاه شیراز، دانشگاه تبریز، دانشگاه فردوسی مشهد، دانشگاه قم، دانشگاه گیلان، دانشگاه بیرجند، دانشگاه سیستان و بلوچستان، دانشگاه کرمان، دانشگاه گلستان، دانشگاه شهید چمران اهواز، دانشگاه سمنان، دانشگاه محقق اردبیلی، دانشگاه رازی کرمانشاه، مرکز راهکارهای اطلاعاتی هوشمند، دانشگاه خلیج فارس، دانشگاه بجنورد، دانشگاه جهرم، دانشگاه یاسوج، دانشگاه شهرکرد، دانشگاه اراک، دانشگاه بین المللی امام خمینی (ره) قزوین، دانشگاه زنجان، دانشگاه لرستان، دانشگاه هرمزگان، دانشگاه بوعلی سینا، دانشگاه ایلام، دانشگاه ارومیه، دانشگاه کردستان، دانشگاه خوارزمی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، دانشگاه صنعتی شاهرود و دانشگاه علوم پزشکی ایران می‌باشند. با توجه به بررسی‌های به عمل آمده تعداد ۱۱۴۴ نفر در قالب ۸۶ سازمان اشاره‌شده در بالا شناسایی گردیدند. سپس در نرم‌افزار Excel سازمان‌ها از ۱ تا ۸۶ شماره‌گذاری شده و به تبع آن کارکنان اشاره‌شده از ۱ تا ۱۱۴۴ به تبعیت از سازمان متبوع

---

۱. ضریب همبستگی کندال، یک آزمون ناپارامتریک است و برای تعیین میزان هماهنگی میان نظرات استفاده می‌شود. ضریب کندال بین ۰ و ۱ متغیر است. اگر ضریب کندال صفر باشد؛ یعنی عدم‌توافق کامل و اگر یک باشد؛ یعنی توافق کامل وجود دارد. برای پایان دورهای تکنیک دلفی می‌توان از ضریب هماهنگی کندال استفاده کرد.

خود شماره‌گذاری شدند و به‌صورت تصادفی تعداد ۲۸۸ نفر به عنوان نمونه گزینش گردیدند. پرسش‌نامه به‌صورت الکترونیکی و بعضاً چاپی برای این افراد ارسال و پس از دریافت، با استفاده از نرم‌افزارهای SPSS و AMOS، تحلیل آماری صورت گرفت و در نهایت، مدل پدافند سایبری مورد نظر در سازمان‌های داده‌محور با تکیه بر حوزه نگهداری داده احصا شد که در بخش بعد تشریح می‌گردد.

**یافته‌های پژوهش**

پژوهش حاضر با هدف «ارائه الگوی سازمان‌های داده‌محور در حوزه پدافند سایبری ایران» انجام شد. از آنجا که این پژوهش از نوع پژوهش‌های آمیخته بود، در دو مرحله با بهره‌گیری روش‌های دلفی (مرحله کیفی) و پیمایشی تحلیلی (مرحله کمی)، برنامه‌ریزی و اجرا گردید.

الف) در مرحله اول، داده‌های کیفی مربوط به جامعه اول پژوهش که شامل تعداد ۱۵ نفر از خبرگان و صاحب‌نظران حوزه پدافند سایبری و مسلط به حوزه سازمان‌های داده‌محور و کلان‌داده‌ها که مربوط به پانل دلفی پژوهش بود، به‌منظور بررسی میزان توافق خبرگان در هر یک از شاخص‌ها با استفاده از ضریب توافق کندال، طی اجرای دو مرحله پانل دلفی انجام گردید.

ب) در مرحله دوم، داده‌های کمی به‌دست‌آمده از جمع‌آوری نظرات افراد به‌واسطه نمونه‌گیری تصادفی ساده از جامعه مذکور (جامعه دوم پژوهش)، مورد سنجش و بررسی قرار گرفتند و با استفاده از الگوسازی معادلات ساختاری، روایی الگوی طراحی‌شده مورد بررسی و سنجش قرار گرفت.

در نهایت با بهره‌گیری از تحلیل عاملی تأییدی به‌منظور برآورد مناسب بودن برازش الگو با داده‌های مشاهده‌شده و از طریق معدل‌یابی تحلیل مسیر، الگوی مورد نظر احصا و ارائه می‌شود.

**پاسخ به سؤال اول پژوهش: آیا حوزه نگهداری داده در سازمان‌های داده‌محور نیازمند پدافند سایبری است؟**

با توجه به ماهیت سازمان‌های داده‌محور، به منظور بررسی حوزه‌های سایبری متصور برای این‌گونه سازمان‌ها نیاز بود ابتدا بررسی شود تا ویژگی‌ها و حوزه‌های متمایزکننده سایبری سازمان‌های داده‌محور نسبت به سایر سازمان‌ها احصا شوند. برای این منظور جمعاً تعداد ۶۵ منبع از میان منابع در قالب ۲۳ منبع داخلی (برای سال‌های ۱۳۸۹ الی ۱۳۹۹ ه. ش.) و ۴۲ منبع خارجی (برای سال‌های ۲۰۱۰ الی ۲۰۲۲ م.) گزینش و مورد مطالعه، بررسی و بهره‌برداری قرار گرفتند. با مدنظر قرار دادن میزان تکرار حوزه‌های سایبری سازمان‌های داده‌محور در منابع، تعداد شش حوزه سایبری در سازمان‌های داده‌محور شامل نگهداری داده،

تنوع داده، یکپارچگی دسترسی به داده‌ها، یکپارچگی ابزارهای تجزیه و تحلیل داده‌ها، جریان داده‌ها و فرهنگ سازمانی داده‌محور شناسایی و احصا شدند که از میان آنها، حوزه نگهداری داده جهت طراحی و ارائه الگوی پدافند سایبری انتخاب گردید.

**پاسخ به سؤال دوم پژوهش: ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری در سازمان‌های داده‌محور کدامند؟**

به منظور احصای ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری، جمعاً تعداد ۳۷ منبع از میان منابع در قالب ۱۲ منبع داخلی (برای سال‌های ۱۳۸۴ الی ۱۳۹۷ ه.ش.) و ۲۵ منبع خارجی (برای سال‌های ۱۹۱۲ الی ۲۰۲۱ م.) گزینش و مورد مطالعه، بررسی و بهره‌برداری قرار گرفتند. پس از انجام مطالعه و تحلیل محتوای هر یک از منابع، به ویژه ارجاعاتی که منابع مختلف به چارچوب پدافند سایبری NIST داشتند، مطابق جدول شماره (۲)، پنج بُعد گزینش شده و ۲۱ مؤلفه و ۷۰ شاخص احصا شدند.

**جدول شماره (۲): تفکیک ابعاد، شاخص‌ها ومؤلفه‌های پدافند سایبری**

| ردیف | عنوان بعد | تعداد مؤلفه | تعداد شاخص |
|---|---|---|---|
| ۱ | شناسایی | ۵ | ۲۰ |
| ۲ | حفاظت | ۵ | ۲۳ |
| ۳ | کشف | ۳ | ۱۲ |
| ۴ | پاسخگویی | ۵ | ۱۰ |
| ۵ | بازیابی | ۳ | ۵ |

**پاسخ به سؤال سوم پژوهش: دیدگاه خبرگان در مورد میزان اهمیت هر یک از ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری در سازمان‌های داده‌محور چیست؟**

**نتایج حاصل از نظرات جامعه بخش کیفی پژوهش (اعضای پانل دلفی)**

مشخصات جمعیت‌شناختی جامعه اول پژوهش در جداول شماره (۳) و (۴) نشان داده شده است. با توجه به دو جدول ملاحظه می‌شود بیشتر افراد شرکت‌کننده در پنل دلفی مرد و سطح تحصیلات اکثریت آن‌ها کارشناسی‌ارشد است. لذا برای اجرای مراحل دلفی تعداد ۱۵ نفر از خبرگان پدافند سایبری در سازمان‌های داده‌محور انتخاب گردیدند و در مرحله اول دلفی،

پرسش‌نامه علاوه بر گویه‌های اصلی شامل سؤالات باز در قالب «شاخص پیشنهادی»، برای دریافت نظرات خبرگان و تکمیل شاخص‌ها بود که صاحب‌نظران می‌توانستند شاخص‌های پدافند سایبری را که در فهرست پیشنهادی مستخرج از ادبیات پژوهش موجود نباشد، مطرح نمایند. این پرسش‌نامه بر اساس بازخوردها و نتایج حاصل، مورد ارزیابی صوری و محتوایی قرار گرفت. این ارزیابی باعث برخی اصلاحات در پرسش‌نامه اولیه شد تا فهم آن آسان‌تر شود. سپس با استفاده از نظرات دور اول دلفی، پرسش‌نامه دوم برای دور دوم ارسال و مورد آزمون قرار گرفت. جهت ارزیابی نظرات پانل از شاخص میانگین و انحراف معیار، ضریب کندال و درصد توافق استفاده گردید.

**جدول شماره (۳): جنسیت افراد**

| جنسیت | تعداد | درصد |
|---|---|---|
| مرد | ۱۳ | ۸۶/۶۷ |
| زن | ۲ | ۱۳/۳۳ |
| کل | ۱۵ | ۱۰۰ |

**جدول شماره (۴): سطح تحصیلات افراد**

| سطح تحصیلات | تعداد | درصد |
|---|---|---|
| فوق لیسانس | ۱۰ | ۶۶/۶۷ |
| دکتری | ۵ | ۳۳/۳۳ |
| کل | ۱۵ | ۱۰۰ |

**ضریب توافق در شاخص‌های پژوهش (توسط اعضای دلفی)**

پنل دلفی دو دور اجرا گردید تا از صحت نتایج توسط خبرگان اطمینان بیشتر حاصل شود. نتایج حاصل از اجرای دو دور پنل دلفی در بین ۱۵ نفر از خبرگان و صاحب نظران حوزه پدافند سایبری مسلط به حوزه سازمان‌های داده‌محور و کلان داده‌ها که در جدول (۵) گزارش شده است، نشان داد شاخص‌های ۶۸، ۶۹ و ۷۰ به خاطر ضریب توافق (ضریب کندال) ضعیف، در دور دوم می‌بایست حذف گردند. پس از حذف شاخص‌های با توافق ضعیف برای پاسخ به سؤال چهارم پژوهش حاضر، نمونه‌ای به حجم ۲۸۸ نفر به صورت کاملاً تصادفی از مدیران، کارشناسان و متخصصین در حوزه پدافند سایبری به عنوان جامعه پژوهش کمی (پیمایش تحلیلی) انتخاب و نظرات آنها در مورد هر یک از شاخص‌ها سنجیده شد.

**جدول (۵): نتایج اجرای پنل دلفی پدافند سایبری در حوزه نگهداری داده سازمان داده‌محور**

| پدافند سایبری | مؤلفه | دور اول دلفی | | | | | دور دوم دلفی | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | شاخص | تعداد پاسخ | میانگین | انحراف معیار | ضریب کندال | تغییرات کیفی | تعداد پاسخ | میانگین | انحراف معیار | ضریب کندال | تغییرات کیفی |
| شناسایی | مدیریت دارایی | ۱-شناسایی رایانه‌ها (سخت‌های موجود) | ۱۵ | ٤/۰۰ | ۰,۹۲٦ | ۰/۵۳۸ | تایید | ۱۵ | ۳/۷۳ | /۵۹٤ ۰ | /٦۲۱ ۰ | تایید |
| | | ۲-شناسایی سیستم‌های عامل | ۱۵ | ۳/۸۷ | ۳/۱۸۷ | ۰/٤۵۱ | تایید | ۱۵ | ٤ | /۵۳۵ ۰ | /۸٦۷ ۰ | تایید |
| | | ۳-شناسایی برنامه‌های کاربردی | ۱۵ | ۳/۸۷ | ۱/۰٦۰ | ۰/٤۵٦ | تایید | ۱۵ | ۳/۹۳ | /۵۹٤ ۰ | ۰/۸ | تایید |
| | | ۴-شناسایی داده‌ها | ۱۵ | ٤/۷۳ | ۰/٤۵۸ | ۱/۰۰۰۰ | تایید | ۱۵ | ٤/٦۷ | /۷۲٤ ۰ | /۸٦۷ ۰ | تایید |
| | | ۵-شناسایی ارتباطات و شبکه تبادل داده سازمانی | ۱۵ | ٤/٤۷ | ۰/۹۱۵ | ۰/٦۸٦ | تایید | ۱۵ | ۳/۷۳ | /۷۹۹ ۰ | /٤۷٦ ۰ | تایید |
| | محیط کسب و کار | ۶-شناسایی نقش‌ها و مسئولیت‌های پدافند سایبری ذی‌نفعان | ۱۵ | ۳/۹۳ | ۰,۷۹۹ | ۰/٦۸٦ | تایید | ۱۵ | ۳/۷۳ | /۵۹٤ ۰ | /٦۲۱ ۰ | تایید |
| | | ۷-شناسایی زنجیره تأمین | ۱۵ | ۳/۷۳ | ۰/۷۹۹ | ۰/٦۸٦ | تایید | ۱۵ | ۳/۸۷ | /٦٤۰ ۰ | /٦۸٦ ۰ | تایید |
| | | ۸-شناسایی زیرساخت | ۱۵ | ٤/۱۳ | ۰/۹۹۰ | ۰/۵۳۸ | تایید | ۱۵ | ۳/۷۳ | /۵۹٤ ۰ | /٦۲۱ ۰ | تایید |
| | | ۹-شناسایی مأموریت سازمانی، اهداف و فعالیت‌ها | ۱۵ | ۳/۷۳ | ۰/۷۹۹ | ۰/٤۹۱ | تایید | ۱۵ | ۳/۸ | /۸٦۲ ۰ | /٦۸٦ ۰ | تایید |
| | | ۱۰- شناسایی ارائه و پشتیبانی ازخدمات | ۱۵ | ۳/٦۷ | ۰/٦۱۷ | ۰/٦۰۰ | تایید | ۱۵ | ۳/۸ | /٤۱٤ ۰ | ۰/۸ | تایید |
| | حاکمیت | ۱۱-شناسایی سیاست امنیت داده سازمانی | ۱۵ | ٤/٤۷ | ۰/۷٤۳ | ۰/۸٦۷ | تایید | ۱۵ | ۳/۸ | /٦۷٦ ۰ | /٦۲۱ ۰ | تایید |
| | | ۱۲-شناسایی الزامات قانونی و نظارتی | ۱۵ | ۳/۹۳ | ۰/۹٦۱ | ۰/۵۳۳ | تایید | ۱۵ | ۳/٦ | /۵۰۷ ۰ | ۰/٦ | تایید |
| | ارزیابی مخاطرات | ۱۳-شناسایی آسیب‌پذیری دارایی‌ها | ۱۵ | ٤/۲۷ | ۱/۲۸۰ | ۰/٤۰۵ | تایید | ۱۵ | ٤/۰۷ | /٤۵۸ ۰ | /۹۳۳ ۰ | تایید |
| | | ۱۴-کسب آگاهی از منابع اشتراکی | ۱۵ | ٤/۰۰ | ۱/۲۵٤ | ۰/٤۱۵ | تایید | ۱۵ | ٤/۰۷ | /٤۵۸ ۰ | /۹۳۳ ۰ | تایید |
| | | ۱۵- شناسایی تهدیدات داخلی/ خارجی | ۱۵ | ٤/۲۰ | ۰/٦۷٦ | ۰/۸٦۷ | تایید | ۱۵ | ۳/۷۳ | /۵۹٤ ۰ | /٦۲۱ ۰ | تایید |
| | | ۱۶-شناسایی مشاغل مورد نیاز پدافند سایبری | ۱۵ | ۳/۵۳ | ۰/۹۹۰ | ۰/۵۰۱ | تایید | ۱۵ | ۳/۹۳ | /۲۵۸ ۰ | /۹۳۳ ۰ | تایید |
| | | ۱۷-شناسایی و اولویت‌بندی پاسخ‌های مخاطره | ۱۵ | ٤/٤۷ | ۰/۷٤۳ | ۰/۸٦۷ | تایید | ۱۵ | ۳/۸ | /۵٦۱ ۰ | /٦۸٦ ۰ | تایید |
| | | ۱۸- شناسایی مدیریت ریسک سازمانی | ۱۵ | ۳/۹۳ | ۰/۷۹۹ | ۰/٦٦۷ | تایید | ۱۵ | ٤/۰۷ | /٤۵۸ ۰ | /۹۳۳ ۰ | تایید |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | مدیریت | ۱۹- شناسایی زنجیره تأمین | ۱۵ | ۳/۹۳ | ۰/۵۹٤ | ۰/۸۰۰ | تأیید | ۱۵ | ۳/۸ | ۰/۵٦۱ | تأیید |
| | | ۲۰- شناسایی ریسک تأمین‌کنندگان سیستم‌های مهم اطلاعاتی | ۱۵ | ٤/۰۷ | ۰/۷۰٤ | ۰/۸۰۰ | تأیید | ۱۵ | ۳/٦۷ | ۰/۸۱٦ | تأیید |
| حفاظت | مدیریت هویت و دسترسی | ۲۱- صدور مجوزها و اعتبارنامه‌ها | ۱۵ | ٤/۱۳ | ۰/۸۳٤ | ۰/۷۳۳ | تأیید | ۱۵ | ۳/۸ | ۰/۵٦۱ | تأیید |
| | | ۲۲- کنترل دسترسی | ۱۵ | ٤/٦۰ | ۰/۷۳۷ | ۰/۸٦۷ | تأیید | ۱۵ | ٤/٦۷ | ۰/۰٤۷ | تأیید |
| | | ۲۳- نظارت بر یکپارچگی شبکه | ۱۵ | ۳/۸۷ | ۱/۱۲۵ | ۰/٤۹۷ | تأیید | ۱۵ | ٤ | ۰/٦۵۵ | تأیید |
| | آگاهی و آموزش پدافند سایبری | ۲۴- آموزش و آگاه‌سازی کاربران | ۱۵ | ٤/۱۳ | ۰/۹۱۵ | ۰/٦٦۱ | تأیید | ۱۵ | ٤ | ۰/٦۵۵ | تأیید |
| | | نفعان ۲۵- آموزش ذی | ۱۵ | ۳/۸۰ | ۰/۵٦۱ | ۰/۸۷۳ | تأیید | ۱۵ | ۳/۹۳ | ۰/۵۹٤ | تأیید |
| | | ۲۶- حذفه نقل و انتقال و عرتب‌سازی امن داده ها | ۱۵ | ٤/۸۰ | ۰/٤۱٤ | ۱/۰۰۰ | تأیید | ۱۵ | ٤/٦۷ | ۰/۹۰۰ | تأیید |
| | | ۲۷- حفظ ظرفیت کافی برای نگهداری داده‌ها | ۱۵ | ٤/٦۰ | ۰/۷۳۷ | ۰/۸٦۷ | تأیید | ۱۵ | ٤/٤۷ | ۰/٦٤۰ | تأیید |
| | | ۲۸- کنترل یکپارچگی سخت‌افزار | ۱۵ | ٤/۲۰ | ۱/۰۱٤ | ۰/۵۳۸ | تأیید | ۱۵ | ۳/۸۷ | ۰/۳۵۲ | تأیید |
| | | ۲۹- کنترل یکپارچگی نرم‌افزار | ۱۵ | ۳/۹۳ | ۱/۰۲۳ | ۰/٤۱۵ | تأیید | ۱۵ | ۳/۹۳ | ۰/۵۹٤ | ۰/۸ |
| | | ۳۰- کنترل یکپارچگی اطلاعات | ۱۵ | ٤/٤۷ | ۱/۰٦۰ | ۰/۵۳۸ | تأیید | ۱۵ | ۳/۹۳ | ۰/٤۵۸ | تأیید |
| | | ۳۱- نظارت بر جداسازی محیط(های) توسعه و آزمایش از محیط تولید | ۱۵ | ٤/۲۷ | ۱/۰۲۳ | ۰/۵۵٦ | تأیید | ۱۵ | ٤ | ۰/۳۷۸ | تأیید |
| | مراحل و روش‌های محافظت از اطلاعات | ۳۲- نظارت بر پیکربندی امن سیستم‌های اطلاعاتی | ۱۵ | ٤/۷۳ | ۰/٤۵۸ | ۱/۰۰۰ | تأیید | ۱۵ | ٤/۸ | ۰/۵٦۱ | تأیید |
| | | ۳۳- تهیه نسخه پشتیبان | ۱۵ | ٤/٦۰ | ۰/٦۳۲ | ۰/۹۳۳ | تأیید | ۱۵ | ٤/۸ | ۰/۵٦۱ | تأیید |
| | | ۳۴- نظارت بر اجرای صحیح سیاست‌ها و مقررات | ۱۵ | ٤/۳۳ | ۰/۸۱٦ | ۰/۸۰۰ | تأیید | ۱۵ | ۳/۸۷ | ۰/۳۵۲ | تأیید |
| | | ۳۵- بهبود مستمر فرآیندهای محافظت | ۱۵ | ٤/٤۰ | ۱/۰۵۶ | ۰/۵۳۸ | تأیید | ۱۵ | ۳/۸ | ۰/٤۱٤ | ۰/۸ |
| | | ۳۶- نظارت بر اجرای برنامه‌های بازبابی | ۱۵ | ٤/۵۳ | ۰/۵۱٦ | ۱/۰۰۰ | تأیید | ۱۵ | ٤/٦ | ۰/۸۲۸ | ۰/۸ |
| | | ۳۷- بهبود جذب و نگهداشت متابع انسانی با رویکرد پدافند سایبری | ۱۵ | ٤/۲۷ | ۰/۸۸٤ | ۰/۷۳۳ | تأیید | ۱۵ | ۳/۸۷ | ۰/۳۵۲ | تأیید |
| | | ۳۸- تهیه و اجرای برنامه مدیریت آسیب‌پذیری | ۱۵ | ٤/۱۳ | ۰/۷۴۳ | ۰/۸۰۰ | تأیید | ۱۵ | ۳/۸ | ۰/۵٦۱ | تأیید |
| | نگهداری | ۳۹- تعمیر و نگهداری دارایی‌ها | ۱۵ | ٤/۳۳ | ۰/۸۱٦ | ۰/۸۰۰ | تأیید | ۱۵ | ۳/۷۳ | ۰/۷۰٤ | تأیید |
| | فن‌آوری حفاظتی | ۴۰- مستندسازی سوابق ورود به سیستم | ۱۵ | ٤/۰۰ | ۰/۹۲٦ | ۰/۵۳۸ | تأیید | ۱۵ | ۳/۸۷ | ۰/۳۵۲ | تأیید |
| | | ۴۱- محافظت از رسانه‌های جدا شده و نظارت بر نحوه استفاده مجدد از آن | ۱۵ | ٤/۵۳ | ۰/۷۴۳ | ۰/۸٦۷ | تأیید | ۱۵ | ٤/۷۳ | ۰/۷۰٤ | تأیید |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ۴۲- محافظت از شبکه‌های ارتباطی | ۱۵ | ٤/۲۰ | ۰/۷۷۷۵ | ۰/۸۰۰ | نابید | ۱۵ | ٤/۰۷ | /٤۵۸ ۰ | /۹۳۳ ۰ | نابید |
| | | ۴۳- دسترس‌پذیری پایدار | ۱۵ | ٤/۳۳ | ۰/۶۱۷ | ۰/۹۳۳ | نابید | ۱۵ | ٤/۰۷ | /٤۵۸ ۰ | /۹۳۳ ۰ | نابید |
| کشف | ناهنجاری‌ها و وقایع | ۴۴-تجزیه و تحلیل رویدادهای کشف شده از منابع و حسگرها | ۱۵ | ٤/۲۷ | ۰/۸۸٤ | ۰/۹۳۳ | نابید | ۱۵ | ۳/۹۳ | /۵۹٤ ۰ | ۰/۸ | نابید |
| | نظارت مستمر امنیتی | ۴۵-نظارت بر شبکه شناسایی رویدادهای محتمل | ۱۵ | ٤/۲۰ | ۰/۸۶۲ | ۰/۹۳۳ | نابید | ۱۵ | ٤/۱۳ | /۵۱۶ ۰ | /۹۳۳ ۰ | نابید |
| | | ۴۶-نظارت بر فعالیت‌های سایبری کارکنان | ۱۵ | ٤/۰۰ | ۱/۰۰۰ | ۰/٤۷۶ | نابید | ۱۵ | ٤/۱۳ | /۳۵۲ ۰ | ۱ | نابید |
| | | ۴۷-شناسایی گذرمخرب | ۱۵ | ٤/۲۷ | ۱/۰۳۳ | ۰/۵۳۸ | نابید | ۱۵ | ٤ | /۵۳۵ ۰ | /۹۳۳ ۰ | نابید |
| | | ۴۸-نظارت بر فعالیت امن سایبری ارائه‌دهندگان خدمات خارجی | ۱۵ | ٤/۲۰ | ۱/۱٤۶ | ۰/٤۱۵ | نابید | ۱۵ | ٤/۱۳ | /۵۱۶ ۰ | /۹۳۳ ۰ | نابید |
| | | ۴۹-نظارت بر دسترسی غیرمجاز | ۱۵ | ٤/۶۰ | ۰/۵۰۷ | ۱/۰۰۰ | نابید | ۱۵ | ٤/۷۳ | /۵۹٤ ۰ | /۹۳۳ ۰ | نابید |
| | | ۵۰-نظارت بر تجهیزات غیرمجاز | ۱۵ | ٤/۶۰ | ۰/۷۳۷ | ۰/۸۷۶ | نابید | ۱۵ | ٤/۷۳ | /۵۹٤ ۰ | /۹۳۳ ۰ | نابید |
| | | ۵۱-نظارت بر نرم‌افزار غیرمجاز | ۱۵ | ٤/۲۰ | ۱/۳۷۳ | ۰/٤۱۸ | نابید | ۱۵ | ٤/۰۷ | /٤۵۸ ۰ | /۹۳۳ ۰ | نابید |
| | | ۵۲-اسکن آسیب‌پذیری | ۱۵ | ٤/۰۷ | ۱/۶۲٤ | ۰/۵۲۲ | نابید | ۱۵ | ٤/۰۷ | /۷۰٤ ۰ | /۷۵۱ ۰ | نابید |
| | فرآیندهای تشخیص | ۵۳-تعریف بهینه نقش‌ها و مسئولیت‌های تشخیص وقایع غیرطبیعی | ۱۵ | ۳/۸۳ | ۱/۱۰۰ | ۰/٤۷۸ | نابید | ۱۵ | ٤ | /۵۳۵ ۰ | /۸۶۷ ۰ | نابید |
| | | ۵۴-بهبود مستمر و آزمایش فرآیندهای تشخیص وقایع غیرطبیعی | ۱۵ | ۳/۵۳ | ۱/۰۶۰ | ۰/۵۲۹ | نابید | ۱۵ | ٤/۲۷ | /۵۹٤ ۰ | /۹۳۳ ۰ | نابید |
| | | ۵۵-اطلاع‌رسانی وقایع غیرطبیعی کشف شده | ۱۵ | ۳/٤۷ | ۱/۱۸۷ | ۰/۳۷۸ | نابید | ۱۵ | ٤/۰۷ | /۵۹٤ ۰ | /۸۶۷ ۰ | نابید |
| پاسخگویی | طرح‌ریزی | ۵۶- اجرای طرح پاسخگویی به رخداد سایبری | ۱۵ | ۳/۸۳ | ۱/۲۲۳ | ۰/۲۵۲ | نابید | ۱۵ | ٤/۱۳ | /۵۱۶ ۰ | /۹۳۳ ۰ | نابید |
| | ارتباطات | ۵۷-آگاهی کارکنان از وظایف | ۱۵ | ٤/۲۷ | ۱/۱۶۳ | ۰/٤۱۵ | نابید | ۱۵ | ٤ | /۵۳۵ ۰ | /۸۶۷ ۰ | نابید |
| | | ۵۸-گزارش رویدادها | ۱۵ | ٤/۰۰ | ۱/۱۳٤ | ۰/۳۶۰ | نابید | ۱۵ | ٤/۰۷ | /٤۵۸ ۰ | /۹۳۳ ۰ | نابید |
| | | ۵۹-اشتراک اطلاعات مطابق با طرح‌های پاسخ‌دهی | ۱۵ | ۳/۸۳ | ۱/۱۰۰ | ۰/۳۵۱ | نابید | ۱۵ | ٤/۳۳ | /۶۱۷ ۰ | /۹۳۳ ۰ | نابید |
| | تحلیل و بررسی | ۶۰-بررسی اتلان سیستم‌های شناسایی | ۱۵ | ٤/۰۰ | ۰/۹۳۶ | ۰/۵۳۸ | نابید | ۱۵ | ٤/۱۳ | /۵۱۶ ۰ | /۹۳۳ ۰ | نابید |
| | | ۶۱-درک تأثیر و طبقه‌بندی حوادث | ۱۵ | ۳/۹۳ | ۰/۸۸٤ | ۰/۵۳۸ | نابید | ۱۵ | ٤/۱۳ | /۵۱۶ ۰ | /۹۳۳ ۰ | نابید |
| | | ۶۲-خاورنزدیک | ۱۵ | ۳/۶۰ | ۱/۰۵۶ | ۰/۲۱۸ | نابید | ۱۵ | ٤/۲ | /۵۶۱ ۰ | /۹۳۳ ۰ | نابید |
| | کاهش | ۶۳-انجام اقدامات پیشگیرانه در خصوص کاهش حوادث | ۱۵ | ۳/۸۳ | ۱/٤۵۸ | ۱/۰۰۰ | نابید | ۱۵ | ٤/۵۳ | /۸۳٤ ۰ | /۷۵۱ ۰ | نابید |
| | | ۶۴-ثبت و مستندسازی آسیب‌پذیری‌های تازه شناسایی شده | ۱۵ | ٤/۰۰ | ۱/۱۳٤ | ۰/۳۵۶ | نابید | ۱۵ | ٤/۳۳ | /۶۱۷ ۰ | /۹۳۳ ۰ | نابید |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | پیشرفت‌ها | ۶۵-تدوین برنامه‌های پاسخ و به روزرسانی با استفاده از یادگیری سازمانی | ۱۵ | ۳/۸۷ | ۱/۱۲۵ | ۰/۳۰۵ | تایید | ۱۵ | ٤/۱۳ | ۰/۵۱٦ ۰ | ۰/۹۳۳ ۰ | تایید |
| | برنامه‌ریزی بازیابی | ۶۶-اجرای برنامه بازیابی در حین یا بعد از رویداد | ۱۵ | ۳/۲۷ | ۰/۹۶۱ | ۰/٦٦۷ | تایید | ۱۵ | ٤/۲ | ۰/۵٦۱ ۰ | ۰/۹۳۳ ۰ | تایید |
| | پیشرفت‌ها | ۶۷-تدوین برنامه‌های بازیابی و به‌روزرسانی با استفاده از یادگیری سازمانی | ۱۵ | ٤/٤۷ | ۰/۷٤۳ | ۰/۸٦۷ | تایید | ۱۵ | ٤/۱۳ | ۰/۵۱٦ ۰ | ۰/۹۳۳ ۰ | تایید |
| | ارتباطات | ۶۸-مدیریت روابط عمومی | ۱۵ | ۳/۷٦ | ۰/۹۳٦ | ۰/۸۱٦ | رد | ۱۵ | ۳/۳۳ | ٤٤۸۰ ۰ | ۰/۱۷٤ ۰ | رد |
| | | ۶۹-تصحیح اعتبار بعد از یک رویداد | ۱۵ | ۳/۲۰ | ۰/۵٦۱ | ۰/۱۲۰ | رد | ۱۵ | ۲/٦ | ۰/۶۳۲ ۰ | ۰/۱۷۱ ۰ | رد |
| | | ۷۰-اطلاع‌رسانی فعالیت‌های بازیابی | ۱۵ | ۳/٤۷ | ۱/۳۰۲ | ۰/۸۸۶ | رد | ۱۵ | ۲/۳۳ | ۰/۷۰٤ ۰ | ۰/۱۸۵ ۰ | رد |

**پاسخ به سؤال چهارم پژوهش: "ارتباط میان ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری در سازمان‌های داده‌محور چگونه است؟"**

**نتایج حاصل از نظرات جامعه پژوهش کمی (پیمایش تحلیلی)**

مشخصات جمعیت شناختی جامعه دوم پژوهش که مدیران، کارشناسان و متخصصان مرتبط با پدافند سایبری هستند، در جداول (۶) و (۷) نشان داده شده است. با توجه به جداول ملاحظه می‌شود که ۲۴۸ نفر از افراد نمونه مرد و ۴۰ نفر زن هستند. همچنین، ۲۰۳ نفر از افراد نمونه دارای تحصیلات فوق‌لیسانس و ۸۵ نفر دارای تحصیلات دکتری می‌باشند.

**جدول (۶): فراوانی جنسیت افراد**

| جنسیت | فراوانی | درصد |
|---|---|---|
| مرد | ۲۴۸ | ۸۶/۱۱ |
| زن | ۴۰ | ۱۳/۸۹ |
| کل | ۲۸۸ | ۱۰۰ |

**جدول (۷): فراوانی سطح تحصیلات افراد**

| تحصیلات | فراوانی | درصد |
|---|---|---|
| فوق لیسانس | ۲۰۳ | ۷۰/۴۹ |
| دکتری | ۸۵ | ۲۹/۵۱ |
| کل | ۲۸۸ | ۱۰۰ |

**آمار استنباطی (بررسی نرمال بودن متغیرهای پژوهش)**

برای اجرای روش‌های آماری و محاسبه آماره آزمون مناسب و استنتاج منطقی درباره پژوهش، مهمترین عمل قبل از هر اقدامی، انتخاب روش آماری مناسب برای پژوهش است برای این منظور آگاهی از توزیع داده‌ها از اولویت اساسی برخوردار است. برای همین منظور در این پژوهش از آزمون معتبر کولموگروف اسمیرنوف[۱] برای بررسی فرض نرمال بودن داده‌های پژوهش استفاده شده است، در این آزمون با توجه به فرضیات زیر گام به بررسی نرمال بودن داده‌ها نهاده شده است:

H0: داده‌ها دارای توزیع نرمال هستند؛

H1: داده‌ها دارای توزیع نرمال نیستند.

با توجه به جدول آزمون کولموگروف اگر سطح معناداری برای کلیه متغیرهای مورد بررسی بزرگتر از سطح خطای ۵ درصد باشد، توزیع داده‌ها نرمال می‌باشند.

**جدول شماره (۸): آزمون نرمال بودن عامل‌های مورد بررسی**

| بعد | عامل | حجم نمونه | آماره آزمون | سطح معنی‌داری | نتیجه |
|---|---|---|---|---|---|
| شناسایی | مدیریت دارایی | ۲۸۸ | ۰/۲۰۲ | ۰/۲۰۰ | نرمال |
| | محیط کسب و کار | ۲۸۸ | ۰/۱۵۴ | ۰/۱۷۲ | نرمال |
| | حاکمیت | ۲۸۸ | ۰/۱۴۲ | ۰/۱۱۳ | نرمال |
| | ارزیابی مخاطرات | ۲۸۸ | ۰/۱۶۸ | ۰/۰۹۹ | نرمال |
| | مدیریت ریسک زنجیره تامین | ۲۸۸ | ۰/۱۵۹ | ۰/۱۲۰ | نرمال |
| حفاظت | مدیریت هویت و دسترسی | ۲۸۸ | ۰/۱۸۱ | ۰/۰۸۶ | نرمال |
| | آگاهی و آموزش پدافند سایبری | ۲۸۸ | ۰/۱۴۷ | ۰/۰۷۲ | نرمال |
| | روش‌های محافظت از اطلاعات | ۲۸۸ | ۰/۱۴۵ | ۰/۰۷۸ | نرمال |
| | نگهداری | ۲۸۸ | ۰/۲۰۶ | ۰/۲۲۳ | نرمال |
| | فناوری حفاظتی | ۲۸۸ | ۰/۱۶۳ | ۰/۱۷۲ | نرمال |
| شنا | ناهنجاری‌ها و وقایع | ۲۸۸ | ۰/۱۷۶ | ۰/۱۱۳ | نرمال |

۱ kolmogorov smirnov

| | | | | | |
|---|---|---|---|---|---|
| | نظارت مستمر امنیتی | ۲۸۸ | ۰/۱۵۵ | ۰/۲۳۰ | نرمال |
| | فرایندهای تشخیصی | ۲۸۸ | ۰/۲۰۳ | ۰/۰۹۳ | نرمال |
| پاسخگویی | طرحریزی پاسخ | ۲۸۸ | ۰/۳۲۴ | ۰/۱۱۲ | نرمال |
| | ارتباطات | ۲۸۸ | ۰/۴۵۲ | ۰/۱۷۶ | نرمال |
| | تحلیل و بررسی | ۲۸۸ | ۰/۷۳۲ | ۰/۲۶۸ | نرمال |
| | کاهش | ۲۸۸ | ۰/۶۲۱ | ۰/۳۲۰ | نرمال |
| | پیشرفت‌ها | ۲۸۸ | ۰/۱۴۰ | ۰/۱۸۶ | نرمال |
| بازیابی | برنامه‌ریزی بازیابی | ۲۸۸ | ۰/۴۳۶ | ۰/۱۴۳ | نرمال |
| | پیشرفت‌ها | ۲۸۸ | ۰/۳۳۹ | ۰/۰۶۹ | نرمال |
| | ارتباطات | ۲۸۸ | ۰/۲۵۶ | ۰/۱۵۳ | نرمال |
| سازمان داده‌محور | نگهداری داده‌ها | ۲۸۸ | ۰/۱۹۵ | ۰/۱۴۸ | نرمال |

با توجه به مقادیر جدول فوق که سطح معناداری آزمون برای تمامی متغیرها بیشتر از میزان ۰/۰۵ می‌باشد، می‌توان بیان کرد که فرضیه H0 تأیید شده و لذا توزیع متغیرها از توزیع نرمال پیروی می‌کنند. برای بررسی روابط متغیرهای پژوهش از روش‌های پارامتری استفاده می‌شود.

**الگوسازی معادلات ساختاری**

الگوسازی معادلات ساختاری را می‌توان به روش کمی تلقی کرد که به محقق کمک می‌کند تا پژوهش خود را از نظر مطابقت مدل نظری (مدل تئوری) با داده‌های واقعی (داده‌های تجربی) که با نمونه‌گیری از جامعه جمع‌آوری می‌شود، مورد بررسی قرار دهد. معادلات ساختاری را می‌توان در زمینه‌های مختلف با توجه به اهداف پژوهش به‌کار برد که از موارد استفاده از معادلات ساختاری می‌توان به مواردی نظیر معدل‌یابی علّی یا تحلیل مسیر، تحلیل عاملی تأییدی، تحلیل عاملی مرتبه دوم، مدل‌های مختلف رگرسیون، مدل‌های ساختاری کوواریانس و مدل‌های ساختاری همبستگی اشاره نمود. در پژوهش حاضر از تحلیل عاملی تأییدی و معدل‌یابی تحلیل مسیر استفاده گردید.

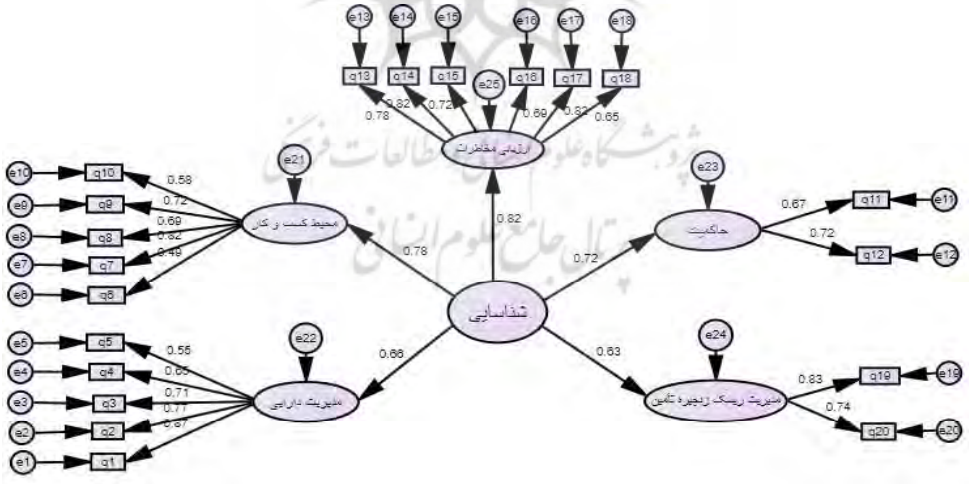
**تحلیل عاملی تأییدی**

در تحلیل عاملی تأییدی، محقق به دنبال یافتن این سؤال است که آیا مجموعه‌ای از پرسش‌ها، یک سازه یا متغیر مشخص را اندازه‌گیری می‌کند؟ به عبارتی، در تحلیل عاملی تأییدی، پژوهشگر به دنبال تأیید یک چارچوب سازه‌ای از پیش تعیین شده است؛ به این معنی که از پیش بر اساس نظریه‌های موجود ارتباط هر عامل با زیرمجموعه خاصی از متغیرها یا سؤالات را

معین ساخته، اکنون به دنبال تأیید آنها می‌باشد. پس از معین شدن الگو، روش‌های متعددی برای برآورد نیکویی برازش کل الگو با داده‌های مشاهده‌شده وجود دارد. به‌طورکلی چندین شاخص برای سنجش برازش الگو، مورد استفاده قرار می‌گیرد، ولی معمولاً برای تأیید الگو، استفاده از ۳ تا ۵ شاخص کافی است. در هر الگوی تحلیل عاملی ارائه شده معناداری، وزن‌های رگرسیونی در سطح اطمینان ۹۵ درصد، بر روایی این الگو دلالت دارد. ضرایب رگرسیونی در الگوی اندازه‌گیری میزان تأثیر هر یک از شاخص‌ها را بر روی مؤلفه و تأثیر هریک از مؤلفه‌ها را بر بُعد نشان می‌دهد. به عبارتی، هر چه میزان ضریب استانداره شده رگرسیونی بیشتر باشد، آن شاخص یا مؤلفه توان بیشتری در تبین متغیر پنهان سطح بالاتر خود دارد.

**الگوی‌های اندازه‌گیری در حوزه نگهداری داده سازمان‌های داده‌محور**

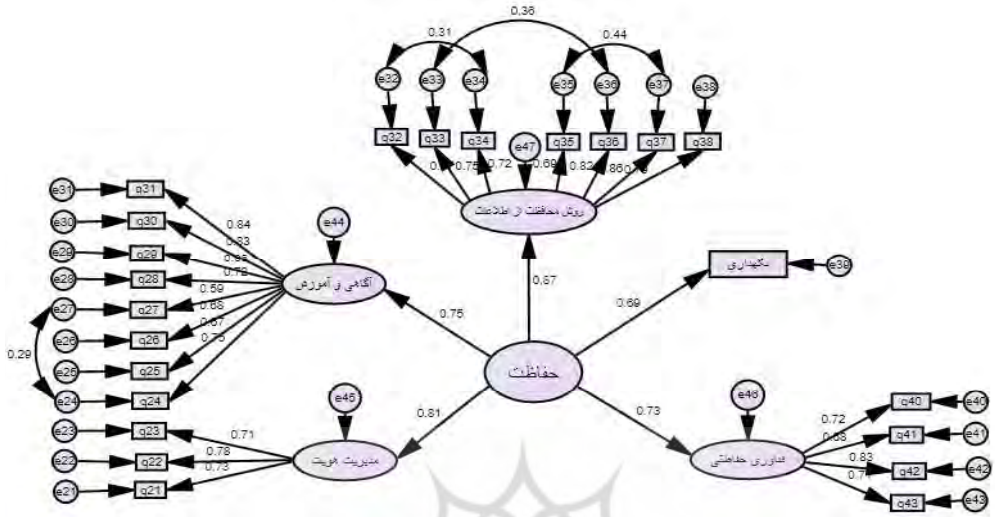
تحلیل مسیر برای آزمون اعتبار مدل علی فرضی مورد استفاده قرار می‌گیرد. در نهایت، شما به ضرایب مسیر نگاه می‌کنید و مشخص می‌کنید که آیا الگویی که از مدل انتظار می‌رود، نمایان می‌شود یا خیر؛ همچنین تحلیل مسیر به شما اجازه می‌دهد تا مدلی که روابط علّی بین متغیرها را مشخص می‌کند با استفاده از روش‌های رگرسیون چندگانه ساده را آزمون کنید. با توجه به الگوی اندازه‌گیری در شکل شماره (۴) عامل ارزیابی مخاطرات بیشترین توان و عامل مدیریت خطرپذیری(ریسک) زنجیره تأمین کمترین توان را در تبین متغیر پنهان شناسایی دارد.




**شکل شماره (۴): الگوی اندازه‌گیری عامل شناسایی در حوزه نگهداری داده**

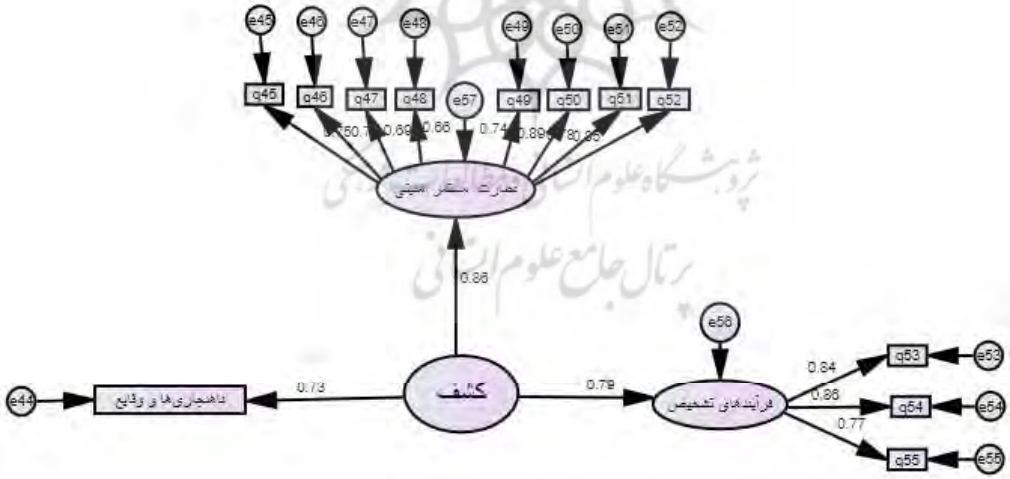
با توجه به شکل شماره (۵) عامل روش محافظت از اطلاعات بیشترین توان و عامل فناوری

حفاظتی کمترین توان را در تبین متغیر حفاظت دارد.



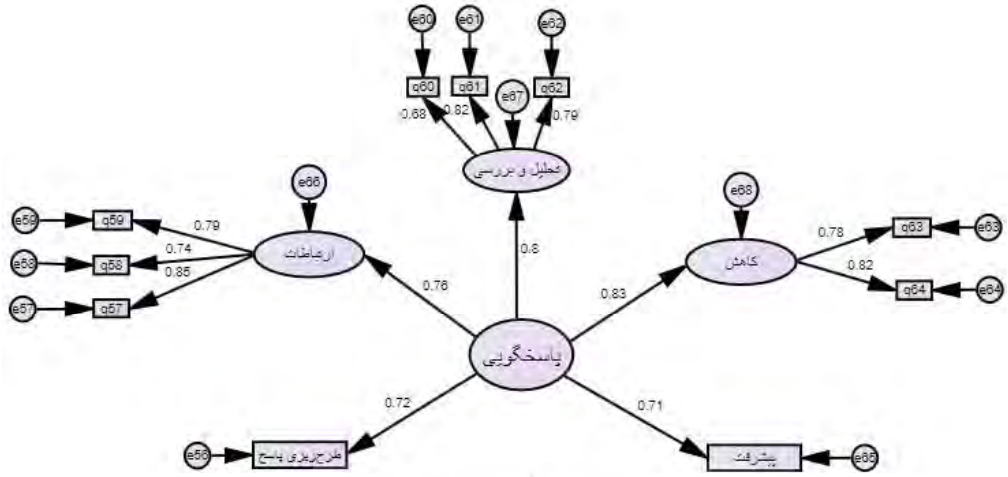

**شکل شماره (۵): الگوی اندازه‌گیری عامل حفاظت در حوزه نگهداری داده**

با توجه به شکل شماره (۶) عامل نظارت مستمر امنیتی بیشترین توان و شاخص ناهنجاری‌های و وقایع کمترین توان را در تبین متغیر کشف دارد.



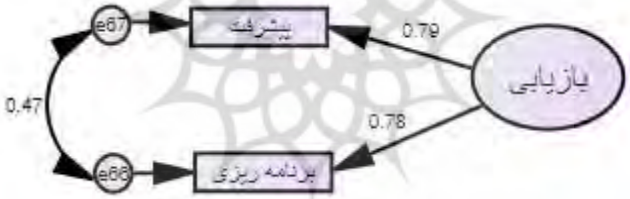

**شکل شماره (۶): الگوی اندازه‌گیری عامل کشف در حوزه نگهداری داده**

با توجه به شکل شماره (۷) عامل کاهش بیشترین توان و شاخص پیشرفت کمترین توان را در تبین متغیر پاسخگویی دارد.




**شکل شماره (۷): الگوی اندازه‌گیری عامل پاسخگویی در حوزه نگهداری داده**

با توجه به شکل شماره (۸) شاخص پیشرفت توان بیشتری را نسبت به شاخص برنامه‌ریزی در تبین متغیر بازیابی دارد.




**شکل شماره (۸): الگوی اندازه‌گیری عامل بازیابی در حوزه نگهداری داده**

**جدول شماره (۹): شاخص‌های برازش الگوی اندازه‌گیری عوامل در حوزه نگهداری داده در سازمان داده‌محور**

| عوامل | CMIN/DF(<5) | NFI(>0.9) | GFI(>0.9) | RMR(<0.09) | RMSEA(<0.08) |
|---|---|---|---|---|---|
| شناسایی | ۱/۸۴۹ | ۰/۹۸۳ | ۰/۹۶۵ | ۰/۰۴۸ | ۰/۰۰۱ |
| حفاظت | ۲/۱۷۸ | ۰/۹۱۵ | ۰/۹۱۲ | ۰/۰۳۸ | ۰/۰۴۶ |
| کشف | ۳/۰۲۳ | ۰/۹۰۳ | ۰/۹۰۲ | ۰/۰۰۳ | ۰/۰۵۴ |
| پاسخگویی | ۱/۴۶۹ | ۰/۹۴۸ | ۰/۹۳۸ | ۰/۰۷۵ | ۰/۰۷۲ |
| بازیابی | ۱/۳۷۱ | ۰/۹۱۱ | ۰/۹۰۶ | ۰/۰۶۹ | ۰/۰۱۶ |

با توجه به جدول شماره (۹)، تمامی شاخص‌های به‌دست‌آمده از برازش مدل در محدوده قابل‌قبول قرار دارند که الگو ارائه شده در هر یک از عوامل را تأیید می‌کند.

**جدول شماره (۱۰): نتایج تحلیل عاملی تأییدی برای عوامل در حوزه نگهداری داده در سازمان داده‌محور**

| | عامل | مقدار بحرانی | بارهای عاملی استاندارد شده | سطح معنی‌داری | نتیجه |
|---|---|---|---|---|---|
| شناسایی | مدیریت دارایی | ۳/۴۱۲ | ۰/۶۶ | <۰/۰۰۱ | تأیید |
| | محیط کسب و کار | ۲/۲۹۰ | ۰/۷۸ | <۰/۰۰۱ | تأیید |
| | حاکمیت | ۲/۵۷۴ | ۰/۷۲ | <۰/۰۰۱ | تأیید |
| | ارزیابی مخاطرات | ۳/۹۳۹ | ۰/۸۲ | <۰/۰۰۱ | تأیید |
| | مدیریت ریسک زنجیره تامین | ۴/۱۵۰ | ۰/۶۳ | <۰/۰۰۱ | تأیید |
| حفاظت | مدیریت هویت و دسترسی | ۲/۷۸۹ | ۰/۸۱ | <۰/۰۰۱ | تأیید |
| | آگاهی و آموزش پدافند سایبری | ۳/۲۴۰ | ۰/۷۵ | <۰/۰۰۱ | تأیید |
| | روش‌های محافظت از اطلاعات | ۲/۶۹۷ | ۰/۸۷ | <۰/۰۰۱ | تأیید |
| | نگهداری | ۲/۹۸۷ | ۰/۶۹ | <۰/۰۰۱ | تأیید |
| | فناوری حفاظتی | ۳/۷۵۴ | ۰/۷۳ | <۰/۰۰۱ | تأیید |
| کشف | ناهنجاری‌ها و وقایع | ۲/۳۶۸ | ۰/۷۳ | <۰/۰۰۱ | تأیید |
| | نظارت مستمر امنیتی | ۲/۸۶۰ | ۰/۸۶ | <۰/۰۰۱ | تأیید |
| | فرایندهای تشخیصی | ۲/۹۶۷ | ۰/۷۹ | <۰/۰۰۱ | تأیید |
| پاسخگویی | طرح ریزی پاسخ | ۳/۰۶۳ | ۰/۷۲ | <۰/۰۰۱ | تأیید |
| | ارتباطات | ۴/۳۵۰ | ۰/۷۸ | <۰/۰۰۱ | تأیید |
| | تحلیل و بررسی | ۳/۱۰۲ | ۰/۸۰ | <۰/۰۰۱ | تأیید |
| | کاهش | ۲/۲۴۰ | ۰/۸۳ | <۰/۰۰۱ | تأیید |
| | پیشرفت‌ها | ۲/۵۶۴ | ۰/۷۱ | <۰/۰۰۱ | تأیید |
| بازیابی | برنامه‌ریزی بازیابی | ۲/۸۷۴ | ۰/۷۸ | <۰/۰۰۱ | تأیید |
| | پیشرفت‌ها | ۳/۳۸۳ | ۰/۷۹ | <۰/۰۰۱ | تأیید |

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

**جدول شماره (۱۱): مقادیر پایایی ترکیبی و روایی همگرا عوامل در حوزه سایبری نگهداری داده در سازمان داده‌محور**

| عامل | پایایی ترکیبی (CR>0.7) | روایی همگرا (AVE>0.5) |
|---|---|---|
| شناسایی | ۰/۷۶۹ | ۰/۵۲۶ |
| حفاظت | ۰/۸۶۲ | ۰/۵۹۶ |
| کشف | ۰/۷۵۳ | ۰/۶۳۲ |
| پاسخگویی | ۰/۸۴۶ | ۰/۵۸۵ |
| بازیابی | ۰/۷۱۶ | ۰/۶۱۶ |

با توجه به جدول شماره (۱۱)، ضریب پایایی ترکیبی برای هر یک از عوامل بیشتر از ۰/۷ می‌باشد و این پایایی قابل قبول الگوی اندازه‌گیری را نشان می‌دهد. همچنین ضریب روایی همگرای هر یک از عوامل بیشتر از ۰/۵ می‌باشد که بیان‌کنندهٔ برازش قابل قبول الگوی اندازه‌گیری است.

**بررسی پایایی ابزار پژوهش (پرسش‌نامه طراحی شده)**

پایایی پرسش‌نامه به نوعی دقت در اندازه‌گیری ابزار طراحی شده را مشخص می‌کند؛ به این معنی که در صورت انجام مجدد مطالعه در همان شرایط، امتیاز یا مقدار حاصل از پرسش‌نامه، تغییری نخواهد کرد. برای اندازه‌گیری پایایی پرسشنامه با توجه به جنبه‌های مختلف طرح پژوهش، دسترسی به آزمودنی‌ها و غیره شیوه‌های مختلفی وجود دارد، برخی از این روش‌های پایایی، شامل روش تکرار آزمایش، روش موازی، روش آلفای کرونباخ، روش‌های دو نیمسازی و غیره می‌باشند.

روش تکرار آزمایش در مواقعی که امکان امکان ارائه پرسش‌نامه به همان گروه از پاسخ‌دهندگان در چند زمان متفاوت فراهم باشد، مورد استفاده قرار می‌گیرد. اهمیت این روش

آن است که پاسخ‌دهندگان، به یک سؤال در چندین بار، پاسخ می‌دهند و سپس، مقایسه پاسخ‌ها در دو یا چند مقطع زمانی اجرا شده، تفاوت‌ها سنجیده می‌شوند. در صورتی که بین پاسخ‌ها یا نمرات حاصل از پرسش‌نامه، همبستگی بالایی وجود داشته باشد، می‌توان نتیجه گرفت که پرسش‌نامه دارای پایایی مناسبی است؛ زیرا دقت نتایج به‌دست‌آمده، زیاد و در حقیقت واریانس یا پراکندگی آنها کم است. در این پژوهش با توجه به ساختار طرح و همچنین جامعه پژوهش از روش تکرار آزمایش استفاده شده است؛ به این صورت که تعداد ۲۱ نفر از افراد جامعه به عنوان نمونه انتخاب گردید و از آنها خواسته شد به هر یک از سؤالات پرس‌شنامه پاسخ دهند. سپس پس از گذشت تقریباً یک ماه از آنها خواسته شد که مجدداً به سؤالات پرسش‌نامه پاسخ دهند. پس از این دو مرحله با توجه به اینکه پاسخ‌ها یک متغیر ترتیبی (طیف لیکرت) بودند، از همبستگی اسپیرمن برای بررسی درجه همبستگی بین پاسخ‌ها در این دو زمان استفاده گردید. مقدار ضریب همبستگی اسپیرمن بین ۱- تا ۱+ قرار دارد و هرچه میزان همبستگی بین دو تکرار آزمایش به ۱+ نزدیک باشد، پایایی ابزار (پرسش‌نامه) تأیید می‌گردد. همبستگی اسپیرمن بالای ۰/۶ نشان از برقراری پایایی برای هر یک از سؤالات در پرسشنامه می‌باشد، نتایج حاصل از بررسی پایایی به روش تکرار آزمایش در جدول شماره (۱۲) ارائه شده است. با توجه به جدول شماره (۱۲) مقدار ضریب همبستگی اسپیرمن برای هر یک از شاخص‌ها به تفکیک ابعاد سازمان داده‌محور بیشتر از ۰/۷ می‌باشد؛ بنابراین ابزار طراحی‌شده از پایایی مطلوبی برخوردار است.

**جدول شماره (۱۲): نتایج حاصل از بررسی پایایی به روش تکرار آزمایش**

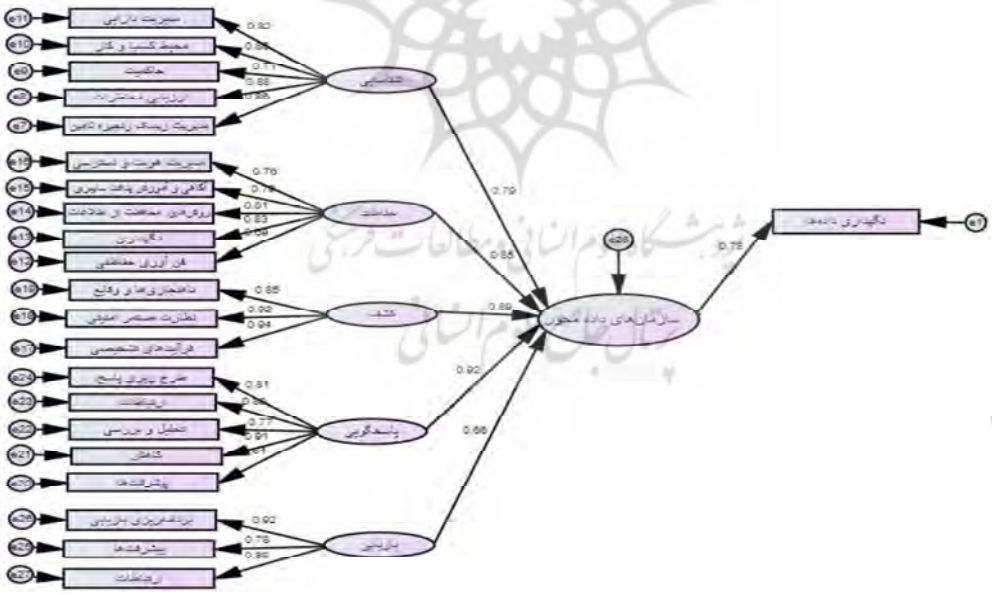
| سازمان داده محور | | | نگهداری داده | |
|---|---|---|---|---|
| پدافند سایبری | مؤلفه | شماره شاخص | شاخص همبستگی | |
| شناسایی | مدیریت دارایی | 1 | 0/821 | |
| | | 2 | 0/867 | |
| | | 3 | 0/802 | |
| | | 4 | 0/867 | |
| | | 5 | 0/736 | |
| | محیط کسب و کار | 6 | 0/789 | |
| | | 7 | 0/886 | |
| | | 8 | 0/763 | |
| | | 9 | 0/820 | |
| | | 10 | 0/832 | |
| | حاکمیت | 11 | 0/754 | |
| | | 12 | 0/796 | |
| | ارزیابی مخاطرات | 13 | 0/833 | |
| | | 14 | 0/863 | |
| | | 15 | 0/865 | |
| | | 16 | 0/847 | |
| | | 17 | 0/764 | |
| | | 18 | 0/775 | |
| | مدیریت | 19 | 0/769 | |
| | | 20 | 0/836 | |
| حفاظت | مدیریت هویت و دسترسی | 21 | 0/881 | |
| | | 22 | 0/751 | |
| | | 23 | 0/756 | |
| | آگاهی و آموزش پدافند سایبری | 24 | 0/773 | |
| | | 25 | 0/852 | |
| | | 26 | 0/873 | |
| | | 27 | 0/910 | |
| | | 28 | 0/702 | |
| | | 29 | 0/861 | |
| | | 30 | 0/867 | |
| | | 31 | 0/873 | |
| | مراحل و روش‌های محافظت از اطلاعات | 32 | 0/746 | |
| | | 33 | 0/921 | |
| | | 34 | 0/869 | |
| | | 35 | 0/872 | |

| سازمان داده محور | | | نگهداری داده | |
|---|---|---|---|---|
| | | 36 | 0/836 | |
| | | 37 | 0/759 | |
| | | 38 | 0/886 | |
| | نگهداری | 39 | 0/836 | |
| | فن‌آوری حفاظتی | 40 | 0/842 | |
| | | 41 | 0/932 | |
| | | 42 | 0/783 | |
| | | 43 | 0/822 | |
| کشف | ناهنجاری‌ها و وقایع | 44 | 0/835 | |
| | نظارت مستمر امنیتی | 45 | 0/896 | |
| | | 46 | 0/791 | |
| | | 47 | 0/821 | |
| | | 48 | 0/870 | |
| | | 49 | 0/806 | |
| | | 50 | 0/815 | |
| | | 51 | 0/796 | |
| | | 52 | 0/773 | |
| | فرآیندهای تشخیص | 53 | 0/825 | |
| | | 54 | 0/764 | |
| | | 55 | 0/715 | |
| پاسخگویی | طرح‌ریزی | 56 | 0/917 | |
| | ارتباطات | 57 | 0/875 | |
| | | 58 | 0/932 | |
| | | 59 | 0/768 | |
| | تحلیل و بررسی | 60 | 0/835 | |
| | | 61 | 0/867 | |
| | | 62 | 0/825 | |
| | کاهش | 63 | 0/768 | |
| | | 64 | 0/872 | |
| | پیشرفت‌ها | 65 | 0/839 | |
| بازیابی | برنامه‌ریزی بازیابی | 66 | 0/799 | |
| | پیشرفت‌ها | 67 | 0/807 | |
| | ارتباطات | 68 | - | |
| | | 69 | - | |
| | | 70 | - | |

**پاسخ به سؤال پنجم پژوهش: الگوی پدافند سایبری در حوزه نگهداری داده در سازمان‌های داده‌محور چگونه است؟**

تحلیل مسیر برای آزمون اعتبار مدل علی فرضی مورد استفاده قرار می‌گیرد. در نهایت، با توجه به ضرایب مسیر مشخص می‌شود آیا الگویی که از مدل انتظار می‌رود، نمایان می‌شود یا خیر؛ همچنین تحلیل مسیر به شما اجازه می‌دهد تا مدلی که روابط علّی بین متغیرها را مشخص می‌کند با استفاده از روش‌های رگرسیون چندگانه ساده را آزمون کنید.

با توجه به اینکه در سؤال چهارم پژوهش ارتباط بین هر یک از ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری یعنی شناسایی، حفاظت، کشف، پاسخگویی و بازیابی در حوزه نگهداری داده در سازمان داده‌محور تأیید شد، حال 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 سازمان-های داده‌محور برازش داده شد. در این مدل هدف بررسی رابطه علّی بین هر یک از ابعاد، مؤلفه ها و شاخص‌های پدافند سایبری بر حوزه نگهداری داده در سازمان‌های داده‌محور می‌باشد، ضریب رگرسیونی استاندارد شده در هر مسیر نشان از میزان تأثیرگذاری آن بعد پدافند سایبری بر سازمان داده‌محور می‌باشد.




**شکل شماره (۹): الگوی معادلات مسیر پژوهش**

با توجه به جدول شماره (۱۳)، تمامی شاخص‌های به‌دست‌آمده از برازش مدل در محدوده قابل قبول قرار دارند که الگوی موردنظر را تأیید می‌کند.

**جدول شماره (۱۳): 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 |

**جدول شماره (۱۴): نتایج اجرای الگویابی معادلات مسیر پژوهش**

| رابطه | عنوان رابطه | ضریب رگرسیونی | مقدار بحرانی | سطح معنی‌داری | نتیجه |
|---|---|---|---|---|---|
| ۱ | تأثیر مثبت عامل شناسایی در پدافند سایبری بر سازمان داده‌محور | ۰/۷۹ | ۵/۲۳۲ | <۰/۰۰۱ | تأیید |
| ۲ | تأثیر مثبت عامل حفاظت در پدافند سایبری بر سازمان داده‌محور | ۰/۸۵ | ۳/۵۶۹ | <۰/۰۰۱ | تأیید |
| ۳ | تأثیر مثبت عامل کشف در پدافند سایبری بر سازمان داده‌محور | ۰/۸۹ | ۲/۸۴۳ | <۰/۰۰۱ | تأیید |
| ۴ | تأثیر مثبت عامل پاسخگویی در پدافند سایبری بر سازمان داده‌محور | ۰/۹۲ | ۴/۵۸۱ | <۰/۰۰۱ | تأیید |
| ۵ | تأثیر مثبت عامل بازیابی در پدافند سایبری بر سازمان داده‌محور | ۰/۶۶ | ۳/۳۶۲ | <۰/۰۰۱ | تأیید |

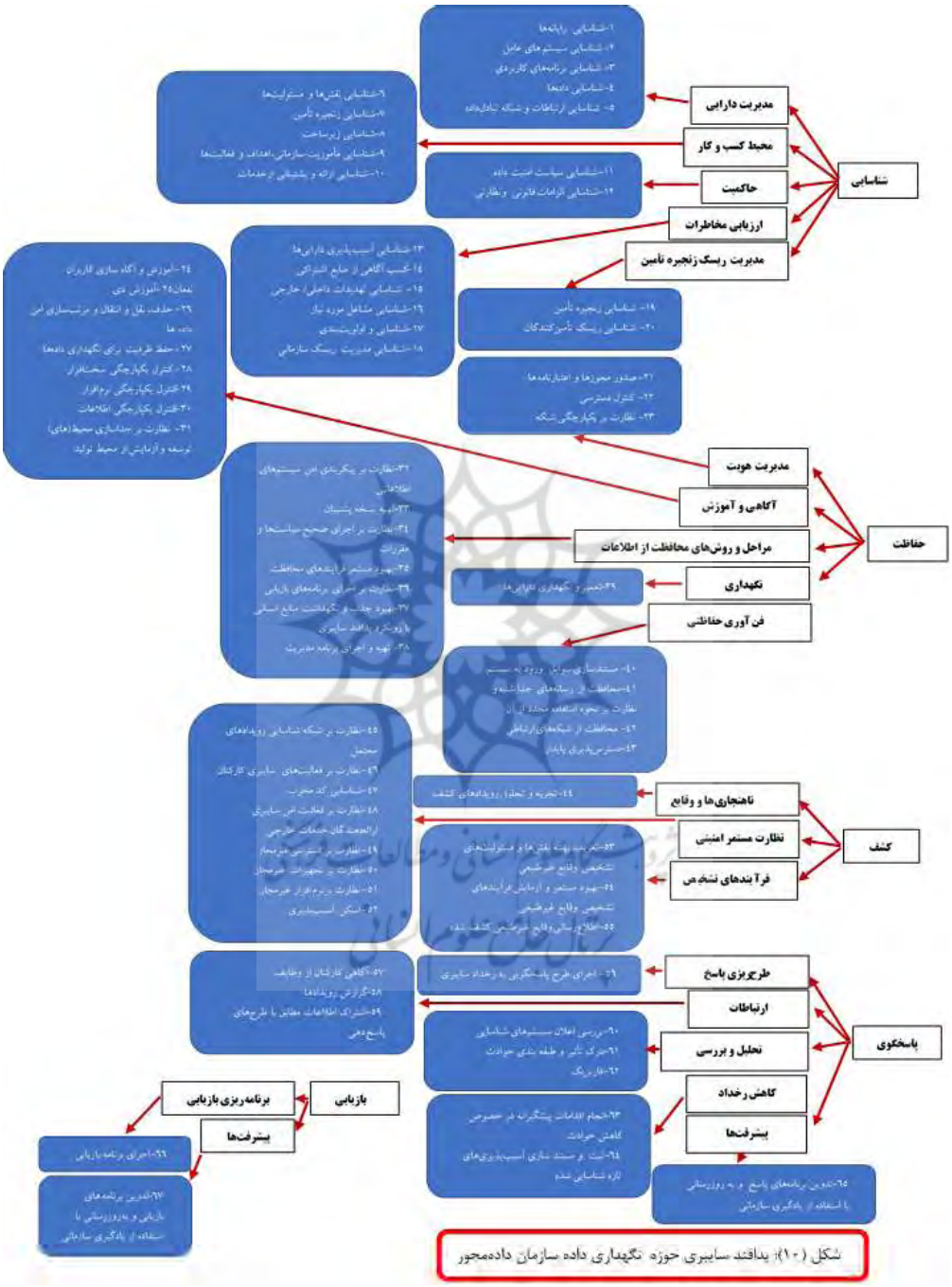
با توجه به جدول شماره (۱۴)، تأثیرگذاری هر یک از بُعدهای پدافند سایبری بر سازمان داده‌محور تأیید گردید و بُعد پاسخگویی بیشترین و بُعد بازیابی کمترین تأثیر را دارد. در خصوص این رابطه‌ها، داده‌های تجربی داده‌های نظری را پشتیبانی کردند و به عنوان یک خروجی مهم از این پژوهش، الگوی عملیاتی (الگوی مفهومی آزمون شده)، برای برنامه‌ریزی در خصوص پدافند سایبری، در شکل شماره (۱۰) قابل ارائه خواهد بود.

## بحث و نتیجه‌گیری

در پژوهش حاضر سؤال اصلی عبارت بود از: «الگوی پدافند سایبری در حوزه نگهداری داده سازمان‌های داده‌محور چگونه است؟» برای پاسخ به این سؤال و صیانت از زیرساخت‌های داده‌ای یک سازمان داده‌محور، ابتدا ابعاد، مؤلفه‌ها و شاخص‌های پدافند سایبری با استفاده از روش اسنادی و کتابخانه‌ای شناسایی شدند. برای تأیید و نهایی‌سازی ابعاد، مؤلفه‌ها و شاخص‌های اشاره‌شده از خبرگان و روش کیفی دلفی و برای پاسخگویی به پرسش‌های پژوهش از روش کمی پیمایشی استفاده گردید.

گردآوری اطلاعات با بهره‌گیری از روش‌های کتابخانه‌ای، دلفی و پرسش‌نامه صورت پذیرفت. جامعه آماری پژوهش شامل ۸۶ سازمان داده‌محور بود که برای انجام مرحله کیفی پژوهش، تعداد ۱۵ نفر از خبرگان و صاحب‌نظران پدافند سایبری و مرحله کمی پژوهش، تعداد

۱۱۴۴ نفر مورد استفاده قرار گرفتند.




شکل (۱۰): پدافند سایبری حوزه نگهداری داده سازمان داده‌محور

ابعاد پدافند سایبری برگرفته از چارچوب NIST در قالب پنج بُعد (شناسایی، حفاظت، کشف، پاسخگویی و بازیابی) در سازمان‌های داده‌محور در حوزه نگهداری داده در تنظیم پرسش‌نامه انتخاب شده و برای مطابقت داده‌های نظری بر روی نتایج تجربی، از تحلیل عاملی تأییدی و معدل‌یابی تحلیل مسیر بهره‌برداری شد. پنل دلفی در دو دور اجرا گردید تا از صحت نتایج به‌وسیلهٔ خبرگان اطمینان بیشتر حاصل شود. نتایج حاصل از اجرای دو دور پنل دلفی در بین ۱۵ نفر از خبرگان و صاحب نظران حوزه پدافند سایبری مسلط به حوزه سازمان‌های داده‌محور و کلان‌داده‌ها، نشان داد برخی از شاخص‌ها به دلیل ضریب توافق ضعیف در دور دوم می‌بایست حذف گردد. پس از حذف شاخص‌های با توافق ضعیف در حوزه نگهداری داده سازمان داده‌محور، نمونه‌ای به حجم ۲۸۸ نفر به صورت کاملاً تصادفی از مدیران، کارشناسان و متخصصین در حوزه پدافند سایبری را انتخاب و نظرات آنها را در مورد هر یک از شاخص‌ها در حوزه نگهداری داده سازمان داده‌محور سنجیده شد. در نتایج به‌دست‌آمده، تمامی شاخص‌های حاصل از برازش مدل در محدوده قابل قبول قرار داشتند که الگوی موردنظر را تأیید می‌کند. همچنین، در مدل پیشنهادی، متغیر پاسخگویی بیشترین تأثیر و متغیر بازیابی کمترین تأثیر را داشته و این مهم بیانگر آن است‌که توجه به پاسخگویی، تداوم و استمرار (تاب‌آوری) در ارائه خدمات به‌وسیلهٔ سازمان‌های داده‌محور بسیار حائز اهمیت است و رویکرد این گونه 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 داده‌شده 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. همچنین، اثبات گردید که ابزار طراحی‌شده (پرسش‌نامه) مبتنی بر روش تکرار آزمایش از پایایی مطلوبی برخوردار است. همان طور که مشاهده گردید، به‌غیر از مؤلفه ارتباطات از بُعد بازیابی، کلیه مؤلفه‌ها و شاخص‌های پدافند سایبری مورد توافق خبرگان قرار گرفت و این بیان‌گر آن است که بازیابی داده‌ها در مخازن نگهداری می‌بایست در زمان بروز رخداد و آسیب به صورت مجزا و حتی بدون توجه به بازیابی زیرساخت ارتباطی تبادل داده با لحاظ نمودن تمامی سیاست‌های پدافند سایبری در سازمان داده‌محور مورد بازیابی قرار گیرند و داده‌ها به عنوان سرمایه‌های سازمانی محسوب می‌گردند.

همچنین، در الگوی ارائه شده در بُعد شناسایی، مؤلفه ارزیابی مخاطرات بیشترین و مؤلفه

عامل مدیریت خطرپذیری(ریسک) زنجیره تأمین کمترین تأثیر را برخوردار می‌باشد که این بدان معناست که انجام پدافند سایبری در حوزه نگهداری داده، می‌بایست با بیشترین طرح‌ریزی، برنامه‌ریزی، سیاست‌گذاری در خصوص ارزیابی امنیتی مخاطرات و تهدیدات متصور بر روی سامانه‌های ذخیره‌سازی (انباره داده) صورت پذیرد. در بُعد حفاظت، مؤلفه روش محافظت از اطلاعات بیشترین و مؤلفه فناوری حفاظتی کمترین تأثیر را برخوردار می‌باشد، این بیانگر ضرورت توجه سازمان‌های داده‌محور در پدافند سایبری از حوزه نگهداری بر روی به‌کارگیری روش‌های متنوع محافظت از داده‌ها (فیزیکی/ منطقی) بر روی سامانه‌های ذخیره‌ساز می‌باشد. در بعد کشف، مؤلفه نظارت مستمر امنیتی از اطلاعات بیشترین و مؤلفه ناهنجاری‌های و وقایع کمترین تأثیر را برخوردار می‌باشد، این مهم بیانگر حساسیت داده‌ها و نحوه نگهداری از داده‌ها و رویکرد تاب‌آوری خدمات مبتنی بر داده در سازمان‌های داده‌محور می‌باشد و ضرورت دارد در فرایندهای پدافند سایبری در سازمان‌های داده‌محور، نظارت‌های مستمر امنیتی برنامه‌ریزی و اجرا گردند، حتی بهتر است از قابلیت‌های هوشمند و برخط در این خصوص استفاده گردد. در بعد پاسخگویی، مؤلفه کاهش آسیب‌ها بیشترین و مؤلفه پیشرفت کمترین تأثیر را برخوردار می‌باشد. با توجه به این نتیجه، رویکرد پدافند سایبری سازمان‌های داده‌محور در حوزه نگهداری داده‌ها می‌بایست مبتنی بر به‌کارگیری روش‌ها و اجرای سیاست‌های امنیتی نظیر دفاع چندلایه (دفاع در عمق: یک مدل حفاظتی لایه‌ای برای اجزای مهم سامانه‌های اطلاعاتی نظیر حفاظت از شبکه و زیرساخت، حفاظت و دفاع از محیط محاسباتی و عملیاتی و زیرساخت‌های حمایتی می‌باشد) باشد تا بدین روش میزان آسیب‌ها تا حد امکان کاهش یابد. در بُعد بازیابی، مؤلفه پیشرفت بیشترین و مؤلفه برنامه‌ریزی کمترین تأثیر را برخوردار می‌باشد. این حاکی از آن است که در حوزه نگهداری از داده‌ها رویکرد بازیابی منابع ذخیره‌سازی داده‌ها می‌بایست رویکردی سریع، هوشمند و پیشرفته و پیش‌دستانه باشد تا بتواند دارایی‌ها و سرمایه‌های سازمانی را از دچار هرگونه آسیب محتمل و غیر قابل پیش‌بینی محافظت نماید.

## منابع و ماخذ:


ابولحسینی، ع. (۱۳۹۲). معرفی و برآورد تهدیدات سایبری. تهران: دیده‌بان.

اصلانی مناف، داود؛ براتی، اکرم. (۱۳۹۶). بررسی تأثیر فناوری اطلاعات بر بهبود کارآیی سازمان، هفتمین همایش سالانه بانکداری الکترونیک و نظام‌های پرداخت، مرکز همایش های برج میلاد، تهران، صص ۶۰-۳۵،

الفت، لعیا؛ زنجیرچی، سید محمود. (تابستان ۱۳۸۹). تحلیل پوششی داده‌ها (DEA)؛ تحلیل پوششی داده‌ها چابکی سازمان‌ها، پژوهش‌های مدیریت در ایران، صص ۲۱-۴۵.

الهیاری، میثم؛ لگزیان، علیرضا، پویا، محمد. (۱۳۹۲). بررسی تأثیر ابعاد عینی امنیت بر کاربری سیستم‌های پرداخت الکترونیکی به‌واسطه ادراک مشتریان از امنیت و اعتماد، دانشگاه فردوسی مشهد، مشهد، دانشکده علوم اداری و اقتصاد.

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

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

حقیقی، محمد علی؛ سعادتی، وحید. (۱۳۹۷). کلان‌داده؛ پیشران نوآوری در خط مشی‌گذاری دولتی، تهران: دانشگاه تهران.

رمضان‌زاده؛ 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 آینده‌پژوهی دفاعی دافوس آجا، صص ۵۹-۸۱.

سعادتی؛ زینب، مهرشاد؛ بتول. (پاییز ۱۳۹۲). اینترنت اشیا و برنامه‌های کاربردی کلان‌داده‌ها در شهرهای هوشمند پایدار، سیاست‌نامه علم و فناوری، صص ۱۷-۳۰.

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

شهرکی، احمد؛ زینی اردکانی، حسین؛ کاظمیان، مهرداد؛ (۱۳۹۲). نقش پدافند غیرعامل در فضای سایبری، مشهد: دانشگاه فردوسی مشهد.

فرابر. (۱۳۹۷). چگونه به یک سازمان داده‌محور تبدیل شویم؟، تهران: گروه پژوهشی فرابر.

فرزام‌نیا، نیما؛ سهیلی، حمیدرضا؛ خزایی، مصطفی. (۱۳۹۴). بررسی تکنیک‌های نوین جنگ‌های سایبری و ارائه مدل ساختاری پویا برای مقابله با آن، تهران: دانشگاه علم و صنعت ایران.

قادری؛ مصطفی، نصرتی؛ حاجت حمیدرضا. (۱۳۹۲). فضای سایبر؛ چالش‌های حاکمیت و امنیت پایدار، پژوهش‌نامه جغرافیای انتظامی، ۸۹-۱۱۴.

قوچانی خراسانی، محمدمهدی و همکاران. (زمستان ۱۳۹۷). شناسایی عوامل توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری با رویکرد نظریه داده‌بنیاد، مطالعات مدیریت کسب و کار هوشمند، صص۳۷-۷۰.

کتانچی؛ الناز، پورقهرمانی؛ بابک، (۱۴۰۰). چالش‌های امنیتِ سایبری در کشورهای «آسه آن»، فصلنامه مطالعات بین‌المللی، ۱۵۶- ۱۳۹.

کلکی، منصور؛ رجایی، امیر. (۱۳۹۶). پردازش داده‌های کلان (Bi g dat a)، کنفرانس سالانه پارادایم‌های نوین مدیریت در حوزه هوشمندی، تهران: پردازش داده، صص ۱-۱۲

مانیان؛ امیر و همکاران. (۱۳۹۵). طراحی الگوی داده‌کاوی پیشنهادی به منظور شناسایی مچرمان، انتظام اجتماعی، ۱۰۹-۱۲۸.

مردی‌ها، م. (زمستان ۱۳۹۸). افزایش داده‌ها و پیشرفت علم، روش‌شناسی علوم انسانی، ۱-۱۴.

Berndtsson,M. Forsberg,D.Stein, D. Svahn, T. (2018). Becoming a data-driven organisation. 26th European Conference on Information Systems: Beyond Digitization (pp. 232-2۴۵). □□□□□□□□□□: □□□□.

Bresciania, Stefano; Ciampib, Francesco; Melib, Francesco; Ferrari, Alberto; (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, 60-۷۵.

Clark, Mark A. Espinosa, J. Alberto & Butina, Mariia. (2018). Cyber security knowledge network. Washington DC: American University.

Dinsmore,T. Chambers,M. (2015). Advanced analytics methodologies: Driving business value with analytics. USA: Pearson Education.

Dunn Cavelty, M. & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Cyber Security Politic, 41-60.

Engel, C. T. & Ebel, P. (2019). Data-Driven Service Innovation: A Systematic Literature Review and Development of a Research Agenda. Twenty-Seventh European Conference on Information Systems (pp. 158-1۷۹). Stockholm, Sweden: Association for Information Systems.

Guberina,Boris;Možnik,Darko;Galinec, Darko; (2017). Cybersecurity and cyber defence: national level strategic approach. Automatika, 273-2۸۶.

Guo, W. Du, Z. & Sun, Y. (2018). Data-Driven Deployment and Cooperative Self-Organization in Ultra-Dense Small Cell Networks. IEEE Access, vol 6, ۲۲۸۳۹-۲۲۸۴۸.

Husák, Martin; aVáclav,Barto. (February 2021). Predictive methods in cyber defense: Current experience and research challenges. Future Generation Computer System, 517-530.

Kolini, F. & Janczewski, L. (2015). Cyber Defense Capability Model: A Foundation Taxonomy. CONF-IRM, 32-52.

Leenen, Louise; Meyer, Thomas. (2021). Artificial Intelligence and Big Data Analytics in Support of Cyber Defense. IGI Global, 1738-1۷۵۳.

Ma, X. (2022). information security behaviour in Chinese IT organizations for information security protection. Information Processing and Management, ۴۷-۶۱.

Miao, y.; Chen, C. Pan,l. Xiang, y. (2022). Machine Learning based Cyber Atacks Targeting on Controlled Information: A Survey. ACM Computing Surveys, 35-47.

McAfee, A. & Brynjolfsson, E. (2012). Big data: The management revolution. Harvard Business Review, 60–68.

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

RamonSaura, Jose; Ribeiro, Domingo; DanielPalacios, Sorianob. (2021). A research agenda to understand user privacy in digital market. International Journal of Information Management, 30-4۵.

Schonberger,Mayer,Cukier,K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt, 193-2۱۵.

Sushaac, I. & Tulder, Å. (2019). Data driven social partnerships: Exploring an emergent trend in search of research challenges and questions. Government Information Quarterly, 112-128.

Upadhyay, S. Upadhyay, N. ( 2017). Future Directions and a Roadmap in Digital Computational Humanities for a Data Driven Organization. 5th International Conference on Information Technol (pp. 1055 – 1۰۶۰). □□□ Delhi: ITQM.

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