دریافت مقاله: ۱۳۹۸/۰۴/۰۱ فصلنامهٔ مدیریت نظامی
پذیرش مقاله: ۱۳۹۹/۰۲/۲۲ سال بیستم، شمارهٔ ۱، بهار ۱۳۹۹
مقاله پژوهشی ص‌ص ۸۱-۱۲۰

ارائه الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی

نیما فرزام نیا[۱*]، بهنام عبدی[۲]، علی رضائیان[۳]

چکیده

فضای سایبری، دامنه‌ای سراسری در محیط اطلاعاتی است که شبکه‌های درهم‌تنیده شامل اینترنت، شبکه‌های مخابراتی، سیستم‌های کامپیوتری، پردازنده‌ها و کنترلرها را در برمی‌گیرد. با توجه به نفوذ روزافزون فناوری اطلاعات و ارتباطات در حوزه‌های مختلف جوامع، سازمان‌ها و کسب‌وکارها، حفظ و ارتقای امنیت فضای سایبری از اهمیت بسیار قابل‌توجهی برخوردار است. در این امتداد، با توجه به نقش و جایگاه سازمان‌های فعال در بخش دفاع، این مهم اهمیتی صدچندان می‌یابد، چراکه به‌طور مستقیم بر امنیت ملی کشور مؤثر است. آمارهای ارائه‌شده از منابع معتبر ملی و بین‌المللی، نشان‌دهنده عدم یکپارچگی فعالیت‌های این حوزه، عدم هم‌راستایی و همگرایی اهداف و سیاست‌ها و به‌طورکلی، عدم توجه کافی به امنیت فضای سایبری و درنتیجه، آسیب‌پذیری جدی کشور در این حوزه است. بر این اساس، دغدغه اصلی پژوهش حاضر، ارائه الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی است. رویکرد پژوهش، استقرایی و نحوه انجام آن، ترکیبی (کیفی و کمی) است که از طریق تحلیل محتوای اسناد و مدارک مرتبط، مصاحبه‌ها با خبرگان و توزیع پرسشنامه با راهبرد نظریه‌پردازی داده بنیاد انجام‌شده است و الگوی نهایی بر اساس مدل پارادایم ارائه شده است. بر اساس یافته‌های پژوهش، حکمرانی خوب امنیت سایبری در سازمان‌های دفاعی مستلزم توجه به مضامین مدیریت استراتژیک سرمایه انسانی، طراحی و پیاده‌سازی چارچوب بومی معماری امنیت سایبری، تطبیق‌پذیری و انعطاف‌پذیری در حوزه امنیت فضای سایبری، مدیریت ریسک امنیت فضای سایبری، بازمهندسی ساختار و فراگردهای سازمانی، مدیریت پروژه‌های مرتبط با توجه به استانداردها و متدلوژی‌های مناسب و توسعه و استقرار فرهنگ‌سازمانی تعالی‌گرا است.

واژه‌های کلیدی: حکمرانی، امنیت فضای سایبری، مدیریت استراتژیک سرمایه انسانی، چارچوب بومی معماری.

---

۱. گروه مدیریت صنعتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران (* نویسنده مسئول)؛ nima.farzamnia@gmail.com
۲. گروه مدیریت فناوری و اطلاعات، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران
۳. گروه مدیریت دولتی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

مقدمه

در سند راهبردی نظام جامع فن‌آوری اطلاعات کشور، اطلاعات نه‌تنها به‌عنوان یکی از منابع و دارایی‌های اصلی سازمان‌ها شناخته می‌شود، بلکه در حکم ابزاری برای مدیریت اثربخش سایر منابع و دارایی‌های سازمان (منابع مالی، سرمایه انسانی و غیره) نیز محسوب می‌شود و لذا از اهمیت و ارزش ویژه‌ای برخوردار شده است؛ اما این ارزش تنها در صورتی محقق و دست‌یافتنی خواهد بود که اطلاعات بتوانند در زمان مناسب، باکیفیت مطلوب و امنیت قابل‌قبول در اختیار افراد مناسب قرارگیری و ارتباطات به‌صورت مطلوب و بهینه در سازمان برقرار گردد. لذا در این سند، امنیت در حوزه وظایف دولت در نظر گرفته‌شده است:

> "دامنه فعالیت دولت در زمینهٔ فن‌آوری اطلاعات به اولویت‌های حاکمیتی در زمینه ارائه خدمات عمومی، قانون‌گذاری، سیاست‌گذاری، معماری سازمان‌های دولتی و گسترش زیرساخت‌های نرم‌افزاری و سخت‌افزاری مربوط می‌شود. توسعه مدیریت دانش با بهره‌گیری از فن‌آوری اطلاعات و برقراری امنیت فضای الکترونیکی تبادل اطلاعات کشور در این حوزه قرار دارد."

در این سند، همچنین، راهبرد و-۴-۶، با عنوان "استقرار نظام امنیت فضای الکترونیکی تبادل اطلاعات کشور" با راهکارهای زیر موردتوجه قرارگرفته است:

و-۴-۶-۱ استقرار نظام مدیریت و راهبری امنیت فضای تبادل اطلاعات کشور؛

و-۴-۶-۲ استانداردسازی محصولات و سازوکار امنیت حوزهٔ فن‌آوری اطلاعات؛

و-۴-۶-۳ توسعه و تقویت صنعت بومی امنیت فن‌آوری اطلاعات؛

و-۴-۶-۴ ایجاد نظام پیشگیری و مقابله با تهدیدات مختلف در حوزه فن‌آوری اطلاعات؛

و-۴-۶-۵ سهولت ایمنی و امنیت جهت شبکه‌های پرسرعت و کارآمد (وزارت ارتباطات و فن‌آوری اطلاعات، ۱۳۸۶).

از طرف دیگر در برنامه پنجم توسعه، در سیاست‌های کلی توسعه در ماده ۳-۴۴، ایجاد سامانه یکپارچه نرم‌افزاری اطلاعاتی، ارتقای سطح حفاظت از اطلاعات رایانه‌ای، توسعه علوم و فناوری‌های مرتبط با حفظ امنیت سامانه‌های اطلاعاتی و ارتباطی به‌منظور صیانت از فضای تبادل اطلاعات، تقویت فنی برای مقابله با تخلفات در فضاهای رایانه‌ای و صیانت از حریم فردی

و عمومی ذکر گردیده است (مجموعه برنامه پنج‌ساله پنجم توسعه، ۱۳۸۹). در ابلاغ سیاست-های کلی برنامه ششم توسعه نیز، موضوع ایجاد، تکمیل و توسعه شبکه ملی اطلاعات و تأمین امنیت آن، تسلط بر دروازه‌های ورودی و خروجی فضای مجازی و پالایش هوشمند آن و ساماندهی، احراز هویت و تحول در شاخص ترافیکی شبکه، به‌طوری‌که ۵۰ درصد آن داخلی باشد، عنوان گردیده است.

همان‌طور که ملاحظه می‌شود، امنیت فضای سایبری در اسناد فرادستی و به‌انحاءمختلف، موردتوجه و تأکید جدی قرارگرفته است، با توجه به تنوع و تعدد تهدیدات موجود در فضای سایبری که دائماً در حال رشد و ارتقاء هستند، برنامه‌ها و اقدامات انجام‌شده در کشور تا حصول وضعیت مطلوب فاصله دارد. تهدیدهای سایبری، فراگیر، رو به رشد و واقعی هستند، صرف‌نظر از اینکه آیا فردی یا سازمانی با آن‌ها به روش یک متخصص سایبری و حرفه‌ای برخورد می‌کند یا به‌طور اتفاقی با جرائم سایبری در تعاملاتش مواجه شده است. تهدیدات سایبری یکی از جدی‌ترین چالش‌های امنیتی، اقتصادی و ملی است که ما با آن مواجه هستیم. با عنایت به سند راهبردی پدافند سایبری کشور که در سال ۱۳۹۴ منتشرشده است، اولین هدف دستیابی به‌نظام جامع پدافند سایبری بومی است که تاکنون محقق نشده است (شورای عالی پدافند سایبری کشور، ۱۳۹۴). از طرف دیگر، جنگ‌های نوین سایبری عملیاتی[۱] و راهبردی[۲]، حملات سایبری مانند تهدیدهای مداوم (APTs)، فیشینگ و غیره، به‌شدت در حال افزایش هستند با پیشرفته‌ای اینترنت اشیاء در دنیا که ورود فضای سایبری به محیط زندگی بشر و سازمان‌ها را هرروز بیشتر از گذشته می‌نماید. یک سازمان با چالش‌های امنیتی جدی در این فضا مواجه است (Behnam Shariati, ۲۰۱۶).

---

۱. جنگ سایبری عملیاتی به عملیات سایبری گفته می‌شود که همزمان و یا قبل از حمله نظامی صورت پذیرفته و حمله نظامی را پشتیبانی و تقویت می‌کند. به عنوان مثال، ممکن است قبل از حمله نظامی به یک کشور، بوسیله حملات هکری شبکه آب، برق، تلفن و یا گاز یک کشور، که همه بوسیله سامانه‌های رایانه‌ای کنترل می‌شوند از کار بیافتد و سپس حمله نظامی صورت پذیرد.

۲. جنگ سایبری راهبردی به عملیاتی سایبری گفته می‌شود که در جهت وارد آوردن فشار استراتژیک به یک کشور انجام شده و هیچ عملیات نظامی را به همراه ندارد. مانند ویروس استاکس نت که برای آسیب رساندن و جلوگیری از برنامه‌های هسته‌ای کشور ایران صورت پذیرفت.

چالش امنیت در فضای سایبری در سازمان‌های بخش دفاع که متولی حفظ امنیت و دفاع از کشور در برابر تهدیدات مختلف هستند، بسیار جدی‌تر و اساسی‌تر است. در این امتداد، برابر سیاست‌های کلی خودکفایی دفاعی و امنیتی ابلاغی مجمع تشخیص مصلحت نظام در اواخر سال ۱۳۹۲، موارد مهمی همچون توسعه و تعمیق فرهنگ خودباوری، خودکفایی، نوآوری و خلاقیت در تمام سطوح و ابعاد دفاعی و امنیتی، ترویج نهضت نرم‌افزاری، تولید و توسعه علوم و فناوری و تحقیقات دفاعی و امنیتی و حرکت در مرزهای دانش با تأکید بر بومی‌سازی و روزآمدی، دستیابی به فناوری‌های برتر موردنیاز دفاعی و امنیتی حال و آینده با تأکید بر نوآوری و پشتیبانی از توسعه آن‌ها، تأکید بر خودکفایی کشور در سامانه‌ها، کالاها و خدمات اولویت‌دار دفاعی و امنیتی توأم با بهسازی تجهیزات موجود و افزایش قابلیت و کار آیی آن، ممنوعیت تأمین نیازهای دفاعی و امنیتی از خارج کشور مگر در حد ضرورت قابل‌توجه هستند؛ بنابراین یکی از ملاحظات اساسی تحقق اهداف تعیین‌شده در سیاست‌های کلی خودکفایی دفاعی و امنیتی، فناوری اطلاعات و ارتباطات و ضرورت تأمین امنیت فضای سایبری به‌عنوان شریان حیاتی بخش دفاع است.

بر این اساس، توجه به مبحث امنیت اطلاعات در بخش‌ها و سازمان‌های مختلف مانند بخش دفاعی کشور، بررسی و استانداردسازی جهت استقرار نظام مناسب امنیت فن‌آوری اطلاعات و مدیریت صحیح آن مشهود هست. در این امتداد، مسئله اصلی قابل‌توجه در این پژوهش، نامشخص بودن ابعاد و مؤلفه‌های مرتبط با امنیت فضای سایبری در سازمان‌های دفاعی کشور و درنتیجه آن، فقدان الگوی بومی، نظام‌مند و مشخص در این رابطه است. همان‌طور که بیان شد، بررسی منابع مختلف نشان می‌دهد باوجود تأکید در اسناد فرادستی، حوزه امنیت فضای سایبری موردتوجه جدی کشور نیست. به‌عنوان نمونه، بر اساس گزارش سازمان جهانی استاندارد[۱] (۲۰۱۴)، ایران در بین ۱۴ کشور خاورمیانه، ازنظر تعداد گواهینامه‌های اخذشده در سیستم مدیریت امنیت سایبری، جایگاه ششم را دارا هست. بر اساس آنچه بیان گردید، به نظر می‌رسد نبود الگوی مناسب با دیدگاه همه‌جانبه نسبت به امنیت، توجه بیشتر به توسعه فنی این حوزه و عدم در نظر گرفتن جنبه مدیریتی آن، سبب بروز این مشکل است. برای رفع این

۱. ISO

مشکل، باید ابعاد مختلف امنیت فضای سایبری ازجمله استراتژی‌ها، استانداردها، چارچوب‌ها، متدولوژی‌ها و ابزارها موردتوجه جدی قرار گیرد. بنابراین، این پژوهش بر این پیش‌فرض[۱] مبتنی است که به‌منظور استقرار نگاه نظام‌مند، جامع و پویا به مبحث امنیت فضای سایبری، تدوین و پیاده‌سازی الگوی حکمرانی خوب امنیت اطلاعات باید مورد توجه جدی قرار گیرد.

با توجه به مسائل و مشکلات مطرح‌شده در بالا در حوزه مدیریت امنیت فضای سایبری در قالب عدم یکپارچگی و عدم هم‌راستایی سیاست‌ها، اقدامات و اهداف و فقدان نگرش جامع و کلی به مبحث امنیت، این پژوهش به بررسی نگاه مدیریتی بومی موردنیاز کشور در قالب حکمرانی خوب امنیت فضای سایبری در بخش دفاع می‌پردازد و درصدد پاسخ به این سؤال است که الگوی مناسب حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی کدام است؟ بر این اساس، یافته‌های این تحقیق می‌تواند به احداث زیرساخت امنیت فضای سایبری سازمان‌ها در ایران کمک چشمگیری نماید. در این مقاله، پس از مرور مفاهیم مرتبط همچون حکمرانی خوب و امنیت فضای سایبری، روش‌شناسی پژوهش ارائه خواهد شد و پس از تحلیل و ارائه یافته‌ها، به جمع‌بندی و نتیجه‌گیری خواهیم پرداخت.

حکمرانی خوب[۲]

درباره حکمرانی، معانی و تفاسیر متفاوتی ارائه‌شده‌اند (Rhodes, ۱۹۹۶)؛ به تعبیری، حکمرانی، دال بر حاکمیت شبکه‌هایی است که جامعه مدنی را با دولت پیوند می‌دهند (Pettai & Illing, ۲۰۰۴) و درواقع، فراگرد رهبری و هدایت جامعه را شکل می‌دهند (Rosenbloom, ۱۹۸۳). به‌عبارت‌دیگر، حکمرانی به گسترش دامنه هدایت و رهبری جامعه اشاره دارد و در پرتو حکمرانی، مرزبندی بخش‌های سه‌گانه جامعه (بخش عمومی، خصوصی و جامعه مدنی) کم‌رنگ‌تر جلوه می‌نمایند؛ زیرا حکمرانی به همه فراگردهای اداره عمومی اشاره دارد که گاهی توسط دولت، گاهی بازار و گاهی شبکه در سازمان‌های رسمی یا غیررسمی و از طریق قوانین، هنجارها، قدرت یا حتی زبان اعمال می‌گردد (Bevir, ۲۰۱۳) و فرایندهای تعامل و تصمیم‌گیری بین کنشگران مرتبط با حل یک مسئله عمومی را در برمی‌گیرد تا منجر

---

۱. Assumption
۲. Good Governance

به خلق، تقویت یا بازتولید هنجارها و نهادهای اجتماعی گردند (Hufty, ۲۰۱۱).

مبنای اساسی طرح این مفهوم، این واقعیت است که اداره صحیح کشور، اساساً معطوف به هدایت اقتصاد و جامعه است و مدیران باید طیفی از الزامات و اقدامات را برای این هدایت در نظر بگیرند. در همین امتداد، ارتباط بین بخش‌های دولتی و خصوصی در قالب مفهوم حکمرانی مطرح می‌شود(Pierre & Peters, ۲۰۰۰) . اساسی‌ترین مفهوم قابل‌درک از واژه حکمرانی، آن است که دیگر نمی‌توان دولت را تنها کنشگر مستقل و دارای قدرت در جامعه (در یک‌زمان خاص) دانست، بلکه امروزه بخش عمومی و بخش خصوصی، به شیوه‌های گوناگون، به هم وابسته بوده، سهم قابل‌توجهی از خط‌مشی‌های بخش عمومی بر اساس مراوده بخش دولتی و بخش خصوصی، توسعه‌یافته و اجرا می‌شود. تغییر به سمت مفهوم حکمرانی برای اهداف جمعی، ملاحظات ناظر بر خط‌مشی قابل‌توجهی درباره نقش مدیریت دارد. این تغییر نگاه به سمت حکمرانی، به این معناست که دولت باید به حالتی فراتر از یک جایگاه ساختاری دارای اختیارات و سلسله‌مراتب حرکت کند (Hall, ۲۰۰۲).

فضای سایبری

مفهوم فضای سایبر قابل‌تغییر و تحول و بسیار بحث‌برانگیز است و تعاریف متعددی برای این فضا وجود دارد، وزارت دفاع آمریکا فضای سایبری را به‌صورت زیر تعریف نموده است "فضای سایبری یک دامنه سراسری[۱] در محیط اطلاعاتی است که شامل شبکه‌های مرتبط به هم از فناوری اطلاعات، شامل اینترنت، شبکه‌های مخابراتی، سیستم‌های کامپیوتری، پردازنده‌ها و کنترلرهای توکار[۲] است.

در سندی مشترک بین روسیه و آمریکا مجموعه‌ای از بیست اصطلاح اساسی فضای سایبری، که کارشناسان نظامی روسی و آمریکایی بر سر تعریف آن‌ها به توافق رسیده‌اند، به زبان‌های انگلیسی و روسی در سال ۲۰۱۱ منتشر شد که فضای سایبری را "یک رسانه الکترونیکی می‌داند که از طریق آن اطلاعات تولیدشده، منتقل‌شده، دریافت شده، ذخیره‌شده،

---

۱. Global Domain
۲. Embedded Processors and Controllers

پردازش‌شده یا حذف می‌شوند." برای شناخت بهتر فضای سایبری این فضا را در سه لایه تصور کنیم: لایهٔ فیزیکی، لایهٔ ساختاری و لایهٔ اطلاعات (معنایی) (Isaac R. Porche et.al,۲۰۱۷).

لایهٔ فیزیکی

تمام دستگاه‌های اطلاعاتی روی یک لایهٔ فیزیکی که متشکل از چندین جعبهٔ و برد الکترونیکی و گاهی چندین سیم یا امواج الکترونیکی قرارگرفته است. با حذف لایهٔ فیزیکی، کل این سیستم محو می‌شود. البته لازم به ذکر است که اگرچه امروزه رابطهٔ جامعی بین فضای سایبری و الکترونیک وجود دارد؛ اما ممکن است که در آینده چنین نباشد؛ زیرا رایانه‌ها را می‌توان بر اساس اصول دیگری استوار ساخت. به‌عنوان‌مثال در اواسط دههٔ ۹۰ میلادی، شاهد کارهای زیادی بر روی DNA بودیم؛ بنابراین اجزاء سخت‌افزاری دستگاه‌های الکترونیکی و رایانه‌ها را می‌توان به‌عنوان مثال‌هایی از این لایه نام برد.

لایهٔ ساختاری

لایه ساختاری شامل دستورالعمل‌هایی است که طراحان و کاربران برای تجهیزات و شیوهٔ تبادل اطلاعات در آن‌ها تعریف می‌کنند و از طریق این دستورالعمل‌ها، دستگاه‌ها باهم تعامل دارند و شامل شناخت طرح، تنظیم اطلاعات، آدرس‌دهی، مسیریابی، قالب‌بندی مستندات، مدیریت پایگاه داده‌ها و غیره است. این همان لایه‌ای است که در آن عملیات هک صورت می‌گیرد و افراد بیگانه به دنبال این هستند تا از طریق آن به اطلاعات طراحان و کاربران نفوذ پیدا کنند. به‌عنوان‌مثال برنامه‌های نوشته‌شده توسط برنامه‌نویسان و یا سایت‌های طراحی شده توسط طراحان یا پروتکل‌های ارتباطی شبکه و الگوریتم‌های رمزنگاری استفاده‌شده را می‌توان جزء این لایه دانست.

لایهٔ معنایی (اطلاعات)

لایهٔ معنایی که بالاترین لایه است، شامل اطلاعات دستگاه است. همان چیزی که کامپیوتر را در جایگاه اول اهمیت قرار داده است و به عبارتی طراحی دولایهٔ دیگر برای پردازش، سازمان‌دهی، تجزیه‌وتحلیل و ذخیره و بازیابی محتوای این لایه بوده و به زبان ساده دولایهٔ دیگر به این لایه خدمات ارائه می‌دهند. اطلاعات سازمان، منابع و یا داده‌های کنترلی نمونه‌هایی از این لایه می‌باشند. معمولاً حمله و نفوذ در فضای سایبری ممکن است در هر

لایه‌ای صورت پذیرد؛ ولی درنهایت باهدف دسترسی، تغییرات، انهدام و یا ساخت اطلاعات در این لایه هست.(F.Schreier,۲۰۱۵:۱۱)

فضای سایبری دارای ویژگی‌های است که تمامی جوامع، دولت‌ها و سازمان‌ها خواسته و یا ناخواسته به سمت آن سوق یافته‌اند. با رشد اینترنت تحولات بنیادی‌تر در این فضا به وجود آمد؛ البته اکنون اینترنت حجمی به‌مراتب وسیع‌تر دارد بنابراین در جهان امروز و به‌تبع آن در کشور ما سرمایه‌ها، دارایی‌ها و منابع سازمان‌ها و افراد، در حال تبدیل و تغییر ماهیت به سمت سرمایه‌های سایبری هست. این سرمایه‌ها می‌تواند اعم از منابع مالی، معنوی، بانکی و حتی دانشی باشد. بدین ترتیب در جهان امروزی به موضوع امنیت و دفاع سایبری باید جدی‌تر نگاه کرد و امروزه مبحث امنیت سایبری در سازمان‌های مختلف و به‌خصوص بزرگ بسیار جدی تلقی شده و بودجه و اعتبارات زیادی را به خود اختصاص داده است

امنیت فضای سایبری

با توجه به اهمیت امنیت فضای سایبری، در سند راهبردی نظام جامع فن‌آوری اطلاعات کشور، راهکارهای "استقرار نظام امنیت فضای الکترونیکی تبادل اطلاعات کشور" عنوان‌شده و در برنامه‌های پنجم و ششم توسعه نیز، موضوع لزوم حفاظت از اطلاعات رایانه‌ای در سیاست‌های کلی توسعه تبیین شده است. امنیت سایبری در سازمان، به‌کارگیری یک استراتژی برای دستیابی به وضعیتی است که مدیران مربوطه، توانایی حفاظت از اطلاعات و ارتباطات سازمانی را در برابر انواع ریسک‌ها، آسیب‌ها و حوادثی که سازمان را تهدید می‌کند، داشته باشند. این استراتژی باید تکرار داشته باشد و مدیریت گردد (ثامنی توسروندانی و همکاران، ۱۳۹۱). اصطلاح "امنیت سایبری"[۱]، حوزه وسیعی ازآنچه را که باید در ارتباط با حفاظت از اطلاعات و دستگاه‌های اطلاعاتی انجام شود، در برمی‌گیرد. تعاریف متعددی برای امنیت سایبری ارائه‌شده است:

۱. محافظت از محرمانگی[۲]، جامعیت[۳] و دسترس‌پذیری[۴] اطلاعات. همچنین می‌تواند

---

۱. Cyber Security
۲. Confidentiality
۳. Integrity
٤. Availability

خصیصه‌های دیگری مثل قابلیت اطمینان[۱]، عدم انکار[۲]، اصالت[۳] و پاسخ‌گویی[۴] را نیز شامل شود.

۲. محافظت از اطلاعات و دستگاه‌های اطلاعاتی در برابر دسترسی، استفاده، افشا[۵]، اختلال[۶]، تغییر[۷] یا امحای[۸] غیرمجاز به‌منظور تأمین محرمانگی، جامعیت و دسترس‌پذیری. هدف امنیت سایبری، محافظت اطلاعات و دستگاه‌های اطلاعاتی از دسترسی و استفاده غیرمجاز، افشا، قطع، تغییر یا خرابی است (Shamala et al, ۲۰۱۷).

۳. یک حوزه مطالعاتی بین‌رشته‌ای و فعالیت حرفه‌ای است که با توسعه و پیاده‌سازی انواع مختلف مکانیسم‌های امنیتی (فنی، سازمانی، دارای منشأ انسانی و قانونی) مرتبط است و هدف آن، دور نگه‌داشتن اطلاعات در همه مکان‌ها (داخل سازمان یا بیرون آن) و حالت‌ها (هنگام ایجاد، پردازش، ذخیره‌سازی، انتقال و امحا) از تهدیدها، به‌منظور دستیابی به اهداف امنیتی است. اهداف امنیتی می‌توانند شامل اصالت، قابلیت اعتماد[۹]، حریم خصوصی[۱۰]، دسترس‌پذیری، جامعیت، محرمانگی، پاسخ‌گویی و قابلیت ممیزی[۱۱] باشند (Haqaf & Koyuncu, ۲۰۱۸).

از نگاه عملیاتی و واقعی، جنبه‌های عملکردی امنیت (شامل محرمانگی اطلاعات، احراز هویت، جامعیت اطلاعات، حفاظت در مقابل حملات، حریم خصوصی و دسترس‌پذیری) و جنبه‌های غیر عملکردی امنیت[۱۲] شامل قابلیت تعامل، قابلیت مدیریت و سادگی توسعه باید موردتوجه قرار گیرند (تمتاجی و همکاران، ۱۳۹۳). پیش‌ازاین، مسائل امنیت اطلاعات در زمینه فن‌آوری موردبررسی قرار می‌گرفت، ولی رشد نیازهای امنیتی، توجه پژوهشگران را به بررسی نقش مدیریت در امنیت سایبری گسترش داده است. باوجود منافع بالقوه فن‌آوری اطلاعات

---

۱. Reliability
۲. Non-repudiation
۳. Authenticity
٤. Accountability
٥. Disclosure
٦. Disruption
۷. Modification
۸. Destruction
۹. Trustworthiness
۱۰. Privacy
۱۱. Auditability
۱۲. Nonfunctional aspects of security

برای سازمان‌ها، به‌کارگیری آن چالش‌های جدی و جدیدی شامل تغییرات اساسی در طرح‌های سازمانی، دستگاه‌های مدیریت داده‌ها، پیامدهای فن‌آوری و ریسک‌های امنیت سایبری را ایجاد نموده است. درگذشته، مدیریت امنیت سایبری بیشتر به‌عنوان یک مسئله فنی موردبررسی قرار می‌گرفت و بیشتر توجهات به راه‌حل‌های فناورانه بود؛ ولی این موضوع کافی نبوده و مطالعات نشان می‌دهد که مسائل امنیت سایبری، باید در یک زمینه مدیریتی نیز در نظر گرفته شود (Hou et al, ۲۰۱۸).

مدیریت امنیت سایبری بخشی از مدیریت اطلاعات است که ضمن تعیین اهداف امنیت و بررسی موانع رسیدن به این اهداف، راهکارهایی را برای آن ارائه می‌دهد. هدف مدیریت امنیت سایبری هر سازمان، حفظ سرمایه‌های سازمان (نرم‌افزاری، سخت‌افزاری، اطلاعاتی و ارتباطی و نیروی انسانی) در برابر هرگونه تهدید (دسترسی غیرمجاز به اطلاعات، خطرهای ناشی از محیط و سیستم و خطرهای ایجادشده از سوی کاربران) است و برای دستیابی به این اهداف، به برنامه منسجمی نیاز دارد. با پیدایش اولین استاندارد مدیریت امنیت فن‌آوری اطلاعات در سال ۱۹۹۵، نگرش نظام‌مند به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. بر اساس این نگرش، امنیت فضای تبادل اطلاعات سازمان‌ها، با تکرار تأمین نمی‌شود، بلکه باید این کار به‌صورت مداوم طی چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح انجام گیرد (Rajab and Eydgahi, ۲۰۱۸). برای این منظور هر سازمان باید بر اساس روش‌شناسی مشخص و برنامه‌ریزی‌شده‌ای به کنترل و نظارت بر اطلاعات و تبادل اطلاعات در سازمان خود بپردازد (موسوی و همکاران،۱۳۹۴).

مؤلفه‌ها و شاخص‌های اصلی امنیت سایبری

امنیت فیزیکی

دستگاه‌های رایانه‌ای، اهداف مناسبی برای تخریب هستند. دلایل تخریب می‌تواند شامل انتقام‌جویی، آشوب، اعتصاب، بیانیه‌های سیاسی و فکری و یا تنها سرگرمی برای نابخردان باشد. اصولاً هر بخش یک سیستم رایانه‌ای، یا ساختمانی که آن را در خود جای‌داده است، ممکن است هدف تخریب قرار گیرد. به‌منظور کنترل این بعد از امنیت سایبری، شاخص‌هایی همچون خطرات محیطی (صاعقه، سیل، زلزله، بمب‌گذاری، حملات تروریستی، قطع کابل ارتباط شبکه)، سرقت (رایانه‌ها و قطعات آن‌ها)، حفاظت از سخت‌افزار (دسترسی فیزیکی افراد

غیرمجاز، حوادث مانند آتش‌سوزی و ترکیدگی لوله، دود، دما، پارازیت‌های الکتریکی، نصب تجهیزات استراق سمع) و انجام تعمیرات قطعات در خارج از سازمان موردتوجه قرار می‌گیرند (Mafaiti and Naicker, ۲۰۱۸).

امنیت نیروی انسانی

نتایج بسیاری از پژوهش‌ها نشان می‌دهند بیش از ۸ درصد مشکلات امنیتی پیش‌آمده در سازمان‌ها، ناشی از خطاهای سهوی و عمدی کارکنان بوده است. از طرف دیگر، موارد مطرح در قسمت کنترل "امنیت کارکنان" از بخش اول استاندارد BS۷۷۹ بر این نکته تأکید دارد که انسان، خدشه‌پذیرترین عنصر در حلقه امنیت سایبری است، ازاین‌رو توجه به آن، ما را دررسیدن به حداکثر ایمنی کمک می‌کند. به دلیل اهمیت بسیار، این مؤلفه به دو مؤلفه آگاهی کاربران و امنیت نیروی انسانی (عوامل تحمیلی بر نیروی انسانی) تبدیل می‌شود تا این مؤلفه، دقیق‌تر بررسی شود. شاخصه‌های مؤثر در امنیت نیروی انسانی که می‌توانند سبب بروز اختلال در فعالیت‌های نیروی انسانی شوند، عبارت‌اند از کار زیاد، نداشتن مهارت کافی و لازم، تداخل مسئولیت‌ها، عدم اطلاع از میزان ارزش سایبری، نداشتن انگیزه، کوتاهی و بی‌مسئولیتی و فراموش‌کاری. شاخص‌های مؤثر که می‌توانند به دلیل عدم آشنایی کاربران سبب بروز اختلال در فعالیت‌های نیروی انسانی شوند، عبارت‌اند از: سیستم‌عامل، دستگاه‌های کاربردی و بسته-های نرم‌افزاری (Torten et al, ۲۰۱۸).

با توجه به این‌که دغدغه اصلی کارکنان، برآورده ساختن درخواست‌ها و انجام وظایفی است که بر عهده آن‌ها است، اولین چیزی که معمولاً نادیده گرفته می‌شود، مسائل امنیتی است. دلیل عمده آن را می‌توان نداشتن قانون مدون و ابلاغ‌شده به کارکنان دانست. نکته بسیار مهم این است که نداشتن مقررات مکتوب باعث می‌شود املا، کارکنان ندانند چه وظایفی نسبت به حفظ اطلاعات سازمان دارند و ثانیاً، در صورت بروز تخلف آن‌ها، مرجعی برای رسیدگی به تخلفات وجود ندارد.

امنیت فنی

امنیت فنی بر مکانیسم‌هایی تمرکز دارد که اطلاعات را از انتشار ناخواسته، تحریف و یا تخریب حفاظت می‌کنند. این بعد از امنیت، معمولاً محرمانگی نامیده می‌شود که از دسترسی یا تغییر در داده‌ها، برنامه‌ها و یکپارچگی سیستم توسط کاربران غیرمجاز جلوگیری می‌کند و

اطمینان می‌دهد، اطلاعات و نرم‌افزارها دست‌نخورده و صحیح باقی بمانند (محمودزاده و رادرجبی، ۱۳۸۵).

پیشینه پژوهش

در این قسمت، پژوهش‌های قبلی مرتبط مرور خواهند شد. نکته قابل‌توجه، نگاه غالب فنی و مدیریتی خرد است و خلأ نگاه کلان حکمرانی و سیاست‌گذاری لمس می‌شود:

۱. محمود زاده و رادرجبی (۱۳۸۵) در پژوهشی بر مدیریت امنیت در دستگاه‌های اطلاعاتی، به شناسایی و سنجش اثر عوامل تأثیرگذار بر امنیت سایبری پرداخته‌اند. در این پژوهش با بررسی روش‌ها و استانداردهای رایج جهان، پرکاربردترین آن‌ها که با ساختار سازمان‌های کشور هماهنگی بیشتری دارد، انتخاب‌شده و در تدوین چارچوب نظری مورداستفاده قرارگرفته است. سپس مدلی طراحی‌شده و مؤلفه‌ها و شاخص‌های کلیدی پژوهش مشخص‌شده‌اند. امنیت نیروی انسانی، امنیت فیزیکی و امنیت سایبری، سه عامل اصلی هستند که اعتبار آن موردسنجش قرارگرفته است. نتایج حاصل از پژوهش نشان می‌دهد مؤلفه عدم آگاهی کاربران، بالاترین تهدید و پس‌ازآن، امنیت نیروی انسانی، دومین تهدید برای امنیت سایبری دستگاه‌های رایانه‌ای است. مؤلفه‌های امنیت فیزیکی و امنیت سایبری به ترتیب در رتبه‌های بعدی قرارگرفته‌اند.

۲. تمتاجی، نقیان فشارکی و طباطبایی (۱۳۹۴) در پژوهشی به بررسی الگوی طبقه‌بندی دارایی‌های اطلاعاتی سازمانی و متدولوژی معماری امنیت سایبری آن پرداخته‌اند. الگوی طبقه‌بندی دارایی‌های اطلاعاتی سازمان مشتمل بر ۳۵۵ نوع مختلف در هفت گروه و سه سطح ارائه‌شده است تا مدیران بتوانند با توجه به اهمیت هر یک از گروه دارایی‌ها، کنترل‌های امنیتی متناظر را برای بقای سازمان طرح‌ریزی کنند. در ادامه، به‌منظور هدایت سازمان در معماری امنیت سایبری اطلاعات خود در محیط رایانش ابری، روش مناسب برای تدوین معماری امنیت سایبری ارائه‌شده است. روش ارائه‌شده، به سازمان کمک می‌کند که پس از شناسایی و طبقه‌بندی دارایی‌های اطلاعاتی خود متناسب با الگوی ارائه‌شده، نسبت به معماری امنیت سایبری اطلاعات به‌صورت بهینه و کارآمد اقدام نماید.

۳. چهارسوقی و همکاران (۱۳۹۲) در مقاله‌ای به بررسی ریسک امنیت سایبری پرداخته‌اند. این مقاله با ارائه شاخص‌هایی برای تعیین احتمال وقوع تهدیدات و شدت

آسیب‌پذیری‌ها و ترکیب آن‌ها با پیامد حوادث، راهکار هوشمند جدیدی را برای ارزیابی ریسک امنیت سایبری ارائه می‌دهد.

۴. مقدم نژاد (۱۳۹۱)، در تحقیق خود به تبیین چارچوب بعضی از آسیب‌های امنیتی حوزه فن‌آوری اطلاعات و مصادیقی از حملات انجام‌شده به شبکه‌های رایانه‌ای پرداخته است. سپس آسیب‌های امنیتی فن‌آوری اطلاعات در حوزه‌های جمع‌آوری، پردازش، ذخیره‌سازی و انتقال اطلاعات استخراج گردیده و عوامل مؤثر بر آن بیان‌شده است.

۵. کاوسوغلو[۱] و همکاران (۲۰۱۲) در مقاله خود، برای ارائه توضیحات نظری در این خصوص که چرا در سطوح منابع کنترل امنیت سایبری (ISCR) در سازمان‌ها تفاوت وجود دارد، مدلی را بر مبنای بینش به‌دست‌آمده از دو تئوری مبتنی بر منبع سازمان و تئوری نهادی توسعه داده‌اند. نتایج به‌دست‌آمده نشان می‌دهد فشارهای نهادی و ارزیابی نیازهای امنیتی داخلی، به‌طور قابل‌توجهی اختلاف در سرمایه‌گذاری سازمانی در منابع کنترل امنیت سایبری را توضیح می‌دهد. به‌طور خاص، فشارهای اجباری و قانونی (هنجاری)، نه‌تنها تأثیر مستقیم بر منابع کنترل امنیت سایبری مستقیمی دارند، بلکه از طریق ارزیابی نیازهای امنیتی داخلی، تأثیر غیرمستقیم نیز بر روی آن دارند.

۶. احمد سومرو، حسین شاه و جواد احمد (۲۰۱۶) در پژوهشی، به بررسی نقش مدیریت در امنیت سایبری پرداخته‌اند. در این پژوهش، ادبیات مربوط به نقش‌های مدیریتی در امنیت سایبری در نظر گرفته‌شده تا فعالیت‌های مدیریتی خاص برای بهبود مدیریت امنیت سایبری، بررسی گردد. نتایج نشان داده است که فعالیت‌های مختلف مدیریتی، به‌ویژه، توسعه و اجرای سیاست‌های امنیت سایبری، آگاهی، انطباق آموزش، توسعه معماری سایبری سازمانی مؤثر، مدیریت زیرساخت فن‌آوری اطلاعات، هم‌راستایی سازمان و فن‌آوری اطلاعات و مدیریت سرمایه انسانی، تأثیر قابل‌توجهی بر کیفیت مدیریت امنیت سایبری دارد. بنابراین این تحقیق، با بحث درباره اینکه رویکرد جامع‌تری به امنیت سایبری موردنیاز است، یک هم بخشی جدیدی را ایجاد نموده و

---

۱. Cavusoglu

راه‌هایی را که با آن مدیران می‌توانند نقش مؤثری را در امنیت سایبری ایفا کنند، پیشنهاد می‌دهد.

۷. السیف، الجعفری و رئوف خان (۲۰۱۵) در مقاله خود به این موضوع پرداخته‌اند که هرچند سازمان‌ها به‌طورکلی بر تهدیدات امنیتی خارجی تمرکز می‌کنند، ولی تهدیدات قابل‌توجهی در داخل سازمان نیز می‌تواند وجود داشته باشد. این مقاله سازمان‌های مختلف عربستان سعودی را برای دستیابی به یک بینش دقیق در رابطه با نحوه رسیدگی سازمان به مسائل بازدارنده نقض امنیت سایبری در داخل سازمان، بررسی کرده است. این مقاله بر روی آگاهی و اثربخشی سیاست‌های امنیت سایبری سازمان در میان کارکنان متمرکزشده است.

۸. مسکویدا و مس[۱] (۲۰۱۵)، تحقیقی را انجام داده‌اند که در آن بهترین تجربه‌های موفق پیاده‌سازی امنیت اطلاعات را در فرآیند چرخه حیات نرم‌افزار در استاندارد ISO ۱۵۵۰۴ بررسی نموده‌اند. در این تحقیق عنوان‌شده است که استاندارد بین‌المللی ISO ۱۵۵۰۴ می‌تواند با چارچوب مدیریت امنیت سایبری ISO ۲۷۰۰۰ هم‌راستا گردد. در این تحقیق، تمام ارتباطات موجود بین بهترین تجارب موفق مبتنی بر توسعه نرم‌افزار ISO ۱۵۵۰۴-۵ با کنترل‌های امنیتی ISO ۲۷۰۰۲ تحلیل‌شده و فرمت امنیت ISO ۱۵۵۰۴ توسعه داده‌شده است. این فرمت، تغییراتی را که شرکت‌های نرم‌افزاری می‌بایست در فرآیند چرخه حیات نرم‌افزار برای پیاده‌سازی موفق کنترل‌های امنیتی مرتبط انجام دهند، توضیح می‌دهد.

۹. بیسی ون سولمز و روسو وون سولمز (۲۰۰۵) در مقاله‌ای عنوان نموده‌اند، امنیت سایبری که مسئولیت حفاظت دارایی‌های اطلاعاتی سازمان در برابر ریسک‌های سازمان است، به‌عنوان یک مؤلفه حیاتی از حاکمیت شرکتی خوب تبدیل‌شده است که بهتر است به‌جای امنیت سایبری، آن را امنیت سازمان دانست.

۱۰. آر اوترو (۲۰۱۵) در پژوهشی به ارائه یک متدولوژی ارزیابی کنترل مدیریت امنیت سایبری برای اطلاعات مالی سازمان‌ها پرداخته است. در این تحقیق بیان‌شده است که متدولوژی‌های سنتی که برای ارزیابی کنترل‌های امنیت سایبری توسعه‌یافته‌اند، دارای نقاط ضعفی هستند که از ارزیابی مؤثر کنترل امنیت سایبری در سازمان‌ها جلوگیری

---

۱. Mesquida & Mas

می‌کند. متدولوژی ارائه‌شده مبتنی بر از نظریه مجموعه فازی بوده که با رسیدگی به نقاط ضعف متدولوژی‌های ارائه‌شده قبلی، یک روش عملی و رویکردی نوآورانه برای کنترل‌های امنیت سایبری (ISC) سازمان فراهم می‌کند.

۱۱. ییلدیریم[۱] و همکاران (۲۰۱۱) در مقاله‌ای به بررسی عوامل مؤثر بر مدیریت امنیت سایبری در سازمان‌های کشور ترکیه و مقایسه آن‌ها با وضعیت سازمان‌های کشورهای مشابه پرداخته‌اند. این مطالعه نشان داده است که وقتی ارتباطات، مدیریت عملیات و سیاست‌های امنیتی سازمان پیشرفت می‌کنند، سایر پارامترهای امنیتی مانند پارامترهای سازمانی، عوامل انسانی، فیزیکی و محیطی امنیتی نیز به‌خوبی بهبود می‌یابند. همچنین یافته‌ها نشان داده است که سازمان‌های کشور ترکیه به‌اندازه سایر سازمان‌های کشورهای همتای خود، به موضوع امنیت فن‌آوری اطلاعات اهمیت نمی‌دهند.

۱۲. دوتوت، برگرون و رایموند (۲۰۱۵) تحقیقی را در خصوص مدیریت اطلاعات برای بین‌المللی کردن سازمان‌های متوسط و کوچک از دیدگاه هم‌راستایی استراتژیک انجام داده‌اند. در این تحقیق بیان‌شده است که از منظر دستگاه‌های اطلاعاتی، یک مسئله مهم، نقش استراتژیک قابلیت‌های فن‌آوری اطلاعات سازمان در پاسخگویی بهتر به عدم اطمینان محیطی و متناظر با آن، نیازمندی‌های اطلاعاتی بیشتر و همچنین امکان عملکرد بین‌المللی سازمان است. با توجه به اینکه چنین جنبه مهمی از تأثیر فن‌آوری اطلاعات بر عملکرد سازمان‌های متوسط و کوچک تاکنون نادیده گرفته‌شده است، این سؤال مطرح‌شده است که تا چه حد مطابقت قابلیت‌های فن‌آوری اطلاعات و نیازمندی‌های اطلاعاتی سازمان، به عملکرد بین‌المللی سازمان کمک می‌کند. مدل این پژوهش بر مبنای بازبینی مدل پردازش اطلاعات "توشمن و نادلر" توسعه داده‌شده است. در این خصوص، ۱۷۴ شرکت متوسط و کوچک کانادایی که دارای فعالیت‌های بین‌المللی می‌باشند، بررسی‌شده‌اند. نتایج نشان داده است که تطابق قابلیت‌های فن‌آوری اطلاعات و نیازمندی‌های اطلاعاتی، تأثیر مثبتی بر عملکرد بین‌المللی سازمان دارد. همچنین قابلیت‌های فن‌آوری اطلاعات سازمان‌ها، از بیرون

---

۱. Yildirim

سازمان به‌وسیله عدم اطمینان محیطی و از درون به‌وسیله وضعیت بین‌المللی سازمان، تأثیر می‌پذیرد.

۱۳. دی میتریوس، سیکاس و ولاچز (۲۰۱۳) در پژوهشی به آنالیز مدل‌های رهبری استراتژیک در فن‌آوری اطلاعات پرداخته‌اند. در این تحقیق بیان‌شده است که توسعه فن‌آوری اطلاعات در حال حاضر، سریع‌ترین و فراگیرترین پیشرفت دهنده در گسترش فرصت‌ها و برنامه‌های کاربردی استراتژیک است. در این تحقیق، مدل‌های رهبری استراتژیک فن‌آوری اطلاعات، مشکلات آن و اهمیت آن در سازمان‌ها در نظر گرفته‌شده است. می‌توان نتیجه گرفت که رهبری استراتژیک، روح هر سازمان است. هم بخش دولتی و هم بخش خصوصی، قبل از اتخاذ تصمیمات، باید به دنبال اطلاعات سازمان‌دهی شده باشند وقتی یک مدل شبیه‌سازی استراتژیک قدرتمند و کاربردی در سازمان ایجاد شود، برای مشکلات مدیریتی راه‌حل‌های خاصی در مدل‌های شبیه‌سازی‌شده ارائه می‌گردد.

رهبری استراتژیک سازمان شامل حکمرانی خوب امنیت سایبری درزمینهٔ ارتباطات سازمان است. سازمان‌ها ایزوله نیستند. فن‌آوری اطلاعات در شکل‌های مختلف، یک توانمند ساز کلیدی استراتژیک در چرخه تعامل ارتباطات است. استراتژی‌های سازمان و نیازمندی‌های سازمان، ترکیب‌شده‌اند تا نیازمندی‌های فن‌آوری اطلاعات را برآورده کنند؛ یک فرآیند دائم در حال انجام که به ساختن تصویری از معماری کلی، طراحی برنامه‌های پیاده‌سازی و مدیریت تبدیل برنامه‌ها به عمل کمک می‌کند.

مهم‌ترین نتایج به‌دست‌آمده از این تحقیقات نشان می‌دهد در دوران کنونی، اطلاعات یکی از مهم‌ترین دارایی‌های سازمان بوده و یک مزیت رقابتی مهم برای سازمان محسوب می‌گردد، بنابراین حفاظت از آن ضروری است. عدم توجه به امنیت سایبری می‌تواند خسارات جبران‌ناپذیری را برای سازمان ایجاد نماید. پرداختن به امنیت سایبری، هم از جنبه فنّاورانه و هم از جنبه مدیریتی، ضروری است. امنیت سایبری باید با یک استراتژی تکمیل شود تا امنیت را با استراتژی‌های سازمآن‌هم‌راستا نماید که منجر به انطباق بیشتر و رخدادهای امنیتی کمتری شود. این هم‌راستایی باید با هر تغییری در استراتژی‌های سازمان تضمین شود، زیرا امنیت فن‌آوری اطلاعات برای موفقیت سازمان ضروری است.

روش‌شناسی پژوهش

این مطالعه از حیث هدف، اکتشافی و درصدد ایجاد دانش و درک بهتر از پدیده مورد بررسی، یعنی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی است. بر این اساس، اجرای پژوهش به‌منظور پاسخ به این سؤال صورت می‌پذیرد که " الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی کدام است؟"؛ بنابراین با بررسی اسناد و مدارک موجود، مصاحبه با خبرگان و جمع‌آوری داده‌های مرتبط با پرسشنامه، به شناسایی و تبیین این مهم پرداخته شده است. رویکرد این پژوهش، استقرایی و نحوه انجام آن، ترکیبی (کیفی و کمی) است و ماهیت بین‌رشته‌ای دارد. پژوهش‌های کیفی برای کمک به پژوهش‌گر، به‌منظور درک افراد انسانی و زمینه‌های اجتماعی و فرهنگی که انسان‌ها در آن زندگی می‌کنند، شکل‌گرفته‌اند (دانایی‌فرد و همکاران، ۱۳۸۶). با توجه به ماهیت پژوهش، از راهبرد نظریه‌پردازی داده بنیاد[۱] استفاده شده است که هدف عمده آن، تبیین یک پدیده از طریق مشخص کردن عناصر کلیدی آن پدیده است و در پنج مرحله طراحی پژوهش، جمع‌آوری داده‌ها، تنظیم داده‌ها، تحلیل داده‌ها و مقایسه با متون، انجام می‌شود (Strauss & Corbin, ۱۹۹۸:۷۶). در این روش برای جمع‌آوری و تحلیل هم‌زمان داده‌ها تلاش شده است. جمع‌آوری و تحلیل هم‌زمان داده‌ها در نظریه‌پردازی داده بنیاد به پژوهشگر این فرصت را می‌دهد که بیندیشد چه داده‌هایی را و از کجا جمع‌آوری کند. این روند را نمونه‌گیری قضاوتی یا نظری خوانده، حاکی از آن می‌دانند که موردها، به‌گونه‌ای انتخاب شوند که از سویی، کیفیت مفاهیم و مقوله‌ها را افزایش داده و از سوی دیگر، نمونه بعدی و مسیر حرکت را مشخص کنند. این روش نمونه‌برداری ادامه یافته و باکفایت نظری پایان می‌یابد. کفایت نظری زمانی حاصل می‌شود که جمع‌آوری هرگونه داده، کمکی به افزایش مفاهیم در یک مقوله یا تولید مقوله‌ای جدید نکند (دانایی فرد و همکاران، ۱۳۸۶:۱۳۴). با توجه به نوع پژوهش و ماهیت آن، نمونه‌گیری در فاز کیفی به روش گلوله برفی و تا اشباع نظری ادامه یافت. در این بخش، ۱۴ مصاحبه با ۱۰ نفر از خبرگان صورت گرفت و از نتایج آن‌ها به همراه داده‌های جمع‌آوری‌شده در نظریه‌پردازی داده بنیاد اسنادی استفاده گردید. اطلاعات مربوط به مشارکت‌کنندگان در مصاحبه در جدول ۱ قابل‌مشاهده است.

---

۱. Grounded Theory

جدول شمارهٔ ۱: اطلاعات جمعیت شناختی خبرگان مصاحبه‌شونده

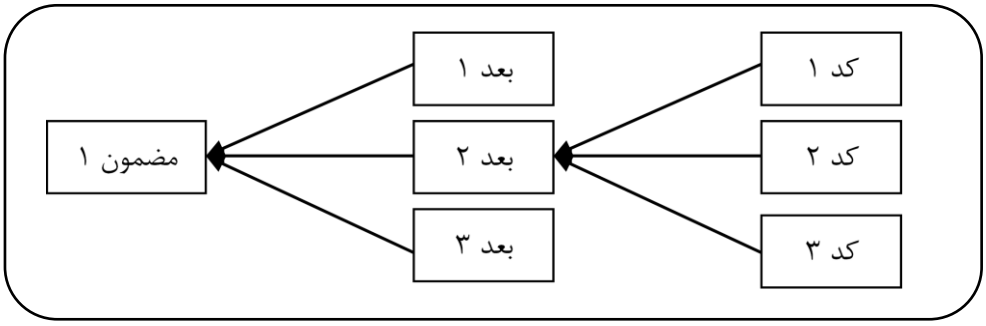
ردیف	مدرک تحصیلی	رشته تحصیلی	تعداد مصاحبه	سابقه کار (سال)	سن (سال)	سمت سازمانی
۱	دکتری	مدیریت فن‌آوری سایبری	۲	۷	۳۶	مشاور
۲	دکتری	مهندسی کامپیوتر- سخت‌افزار	۱	۱۳	۳۷	مدیر
۳	دکتری	مدیریت اجرایی	۲	۱۴	۴۶	مدیر
۴	کارشناسی ارشد	مهندسی کامپیوتر- معماری	۲	۱۱	۴۱	رئیس اداره
۵	کارشناسی ارشد	مهندسی فن‌آوری اطلاعات	۱	۹	۳۹	کارشناس ارشد
۶	کارشناسی ارشد	مهندسی فن‌آوری اطلاعات	۲	۱۲	۴۲	کارشناس ارشد
۷	کارشناسی ارشد	علوم دفاعی	۱	۲۱	۴۵	کارشناس ارشد
۸	کارشناسی ارشد	علوم دفاعی	۱	۱۶	۴۰	معاون
۹	دکتری	مدیریت اجرایی	۱	۱۳	۴۱	مدیر
۱۰	کارشناسی ارشد	مهندسی کامپیوتر- نرم‌افزار	۱	۸	۳۳	کارشناس ارشد

تحلیل یافته‌های پژوهش: فاز کیفی

گام اول، کدگذاری باز: کدگذاری باز، اشاره به بخشی از تحلیل دارد که با عنوان‌گذاری و مقوله‌بندی پدیده، آن‌طور که داده‌ها نشان داده‌اند، سروکار دارد و نیازمند پرسیدن سؤالات و انجام مقایسه‌ها است. محصول عنوان‌گذاری و مقوله‌بندی، "مفاهیم" بوده، رکن اصلی در نظریه‌پردازی داده بنیاد تلقی می‌شود. کدگذاری باز شامل تحلیل و کدگذاری داده‌ها، مشخص نمودن طبقات و تفسیر آن‌ها بر اساس ویژگی‌های هر طبقه است. در ضمن، کدگذاری بازداده‌ها، به بخش‌های مجزا خردشده و برای به‌دست آوردن شباهت‌ها و تفاوت‌های آن‌ها، مورد بررسی قرار می‌گیرند. منظور از خرد کردن و مفهوم‌پردازی این است که به هرکدام از حوادث، رخدادها و ایده‌هایی که در داده‌ها موجود است، نامی می‌دهیم. این نام، برچسب یا

نشانه‌ای است که به‌جای آن حادثه، رخداد یا ایده می‌نشیند. در مرحله بعد، خود مفاهیم بر اساس شباهت‌هایشان مورد طبقه‌بندی قرارمی‌گیرند که به این کار، مقوله‌پردازی گفته می‌شود.

عنوانی که به مقوله‌ها (ابعاد) اختصاص داده می‌شود، انتزاعی‌تر از مفاهیمی (اجزایی) است که مجموعاً آن مقوله را تشکیل می‌دهند. مقولات دارای قدرت مفهومی بالایی هستند؛ زیرا می‌توانند مفاهیم و خرده مقولات را بر محور خود جمع کنند. عنوان یا نامی که برای مقولات انتخاب می‌شود، باید بیشترین ارتباط را با داده‌هایی که مقوله نمایانگر آن است، داشته و آن‌قدر با آن همخوان باشد که بتوان آنچه را که بیان می‌کند، به‌سرعت به خاطر آورد و درباره‌اش فکر کرد. مضامین، از کنار هم قرارگرفتن مقولات مرتبط ایجاد می‌شوند. نحوه کدگذاری و تعیین ابعاد و مضامین گوناگون، به زبان ساده در نمودار ۱ نشان داده شده است:



نمودار شمارهٔ ۱: نحوه کدگذاری و شناسایی ابعاد و مضامین مرتبط با پدیده مورد بررسی، در نظریه‌پردازی داده بنیاد

نتایج فراگرد کدگذاری باز در این تحقیق، در قالب مقوله‌های استخراج شده از مفاهیم در جدول ۲ ذکرشده‌اند. به‌منظور جلوگیری از طولانی شدن حجم مقاله، از ارائه موارد تکراری و تعاریف تفصیلی مقولات ذکرشده، خودداری شده است.

جدول ۲: مضامین و ابعاد استخراج‌شده پژوهش

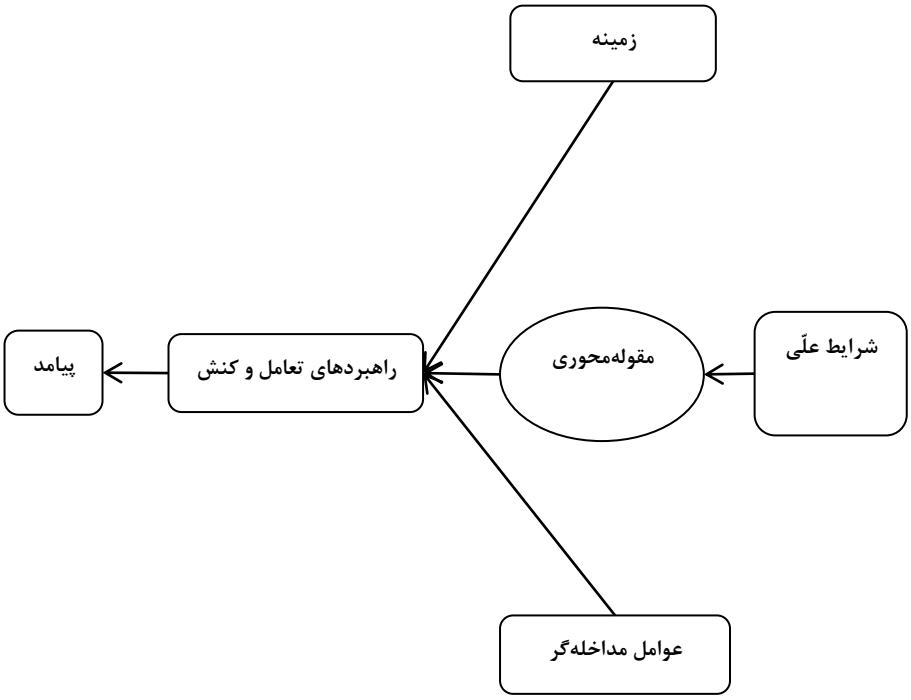
مضامین	ابعاد	تعداد کدها
مدیریت استراتژیک سرمایه انسانی	آموزش‌های استراتژیک به کارکنان	۱۱
	تبیین نقش‌ها و مسئولیت‌های افراد	۱۹
	ارتقاء مسئولیت‌پذیری کارکنان	۱۷
	برخورد جدی با تخلف کارکنان	۱۴
	نظارت جامع بر عملکرد کارکنان	۲۲
	انگیزش کارکنان	۲۴
	ارتقای سطح آگاهی کارکنان	۲۹
طراحی و پیاده‌سازی چارچوب بومی معماری امنیت سایبری	تدوین سند راهبردی شامل چشم‌انداز، اهداف راهبردها	۳۱
	طراحی و تدوین چارچوب بومی معماری امنیت فضای سایبری	۲۷
	تخصیص منابع موردنیاز شامل بودجه، نیروی انسانی و غیره	۲۵
	بومی‌سازی استانداردها با توجه به اصل وابستگی به مسیر	۲۶
	توسعه و به‌کارگیری ابزارها و فناوری‌های امنیتی بومی	۳۲
تطبیق‌پذیری و انعطاف‌پذیری	یکپارچگی امنیت فضای سایبری با سایر حوزه‌های سازمان	۲۸
	هم‌راستایی اهداف امنیت فضای سایبری با اهداف سازمان	۲۴
	ترویج تعامل‌پذیری و توسعه ارتباطات	۲۲
	ارتقاء سطح چابکی سازمانی	۱۹
مدیریت ریسک امنیت فضای سایبری	شناسایی ریسک‌های احتمالی حوزه امنیت فضای سایبری	۲۷
	ارزیابی میزان آسیب ریسک‌های احتمالی حوزه امنیت فضای سایبری	۲۴
	ارزیابی احتمال وقوع ریسک‌های احتمالی حوزه امنیت فضای سایبری	۲۹

	استفاده از استانداردها و متدولوژی‌های مدیریت ریسک امنیت فضای سایبری	۲۳
بازمهندسی ساختار و فراگردهای سازمانی	طراحی و ایجاد ساختار و تشکیلات امنیت سایبری	۲۲
	بازمهندسی ساختار و فراگردهای سازمانی بر اساس شرایط	۲۴
	تدوین خط‌مشی و دستورالعمل‌های موردنیاز	۲۶
	تعیین محدوده و مرزهای امنیت سایبری (قلمرو امنیت فضای سایبری) در سازمان	۳۱
	تعیین و انتخاب معیارها و سنجه‌های امنیت سایبری	۲۷
مدیریت پروژه‌های مرتبط با استانداردها و متدلوژی‌های مناسب	مدیریت استراتژیک پروژه‌های امنیت سایبری	۳۱
	تدوین و اجرای محرک‌های حرکت سازمان در جهت برقراری امنیت سایبری	۸
	پیاده‌سازی سیستم استاندارد مستندسازی	۳۴
	مدیریت منابع پروژه‌های حوزه امنیت فضای سایبری	۲۹
فرهنگ‌سازمانی تعالی گرا	فرهنگ‌سازی امنیت سایبری	۲۴
	تدوین و اجرای استراتژی‌های اشاعه فرهنگ امنیت	
	وجود تفکر استراتژیک در رابطه با امنیت فضای سایبری	۲۸

گام دوم، کدگذاری محوری: کدگذاری محوری، گام دوم نظریه‌پردازی داده بنیاد به روایت استراوس و کوربین است (Strauss & Corbin, ۱۹۹۸:۱۲۲). هدف این مرحله، برقـراری رابطه بین مقولات تولیدشده در مرحله کدگذاری باز است. این کار براساس یک الگو و سرمشق جامع و کلی، موسوم به مدل پـارادایم[۱] انجام می‌شود و به نظریه‌پرداز کمک می‌کند تا نظریه فراگرد اجتماعی مورد مطالعه را راحت‌تر توسعه دهد (نمودار ۱). اساس فراگرد ارتبـاط دهـی در کدگذاری محوری، بر تمرکز و تعیـین یـک مقولـه به‌منزله مقولـه محوری یا اصلی قرار داشته و سپس سایر مقولات به‌مثابه مقـولات فرعی، ذیل عناوین گوناگون مدل پارادایم، به

۱. Paradigm Model

مقوله اصـلی ارتبـاط داده می‌شوند. هدف از کدگذاری محوری، ایجاد رابطه بین طبقات ایجادشده در مرحله کدگذاری باز است. درحالی‌که کدگذاری باز، داده‌ها را به مفاهیم و مقوله‌ها تفکیک می‌کند، کدگذاری محوری، از طریق پیوند دادن یک مقوله و مقوله‌های فرعی آن، داده-ها را به هم پیوند می‌دهند.



نمودار شمارهٔ ۲: مدل پارادایم (Strauss & Corbin, ۱۹۹۸:۱۲۴)

برابر شکل نمودار ۲، بخش‌های گوناگون مدل پارادایم عبارت‌اند از:

شرایط علّی[۱]: این شرایط، باعث ایجاد و توسعه پدیده یا مقوله محوری می‌شوند. این شرایط را مجموعه‌ای از مقوله‌ها به همراه ویژگی‌هایشان تشکیل می‌دهند که بیشترین تأثیر را بر شکل‌گیری مقوله محوری دارند.

---

۱. Causal Conditions

طبقه محوری[۱]: پدیده یا مقوله محوری عبارت است از ایده (انگاره، تصور) پدیده‌ای که اساس و محور فراگرد است. مقوله‌ای که به‌منزله مقولـه محـوری انتخـاب می‌شود باید به‌قدر کافی انتزاعی باشد تا بتوان سایر مقولات اصلی را به آن ربط داد.

زمینه[۲]: به شرایط خاصی که بر راهبردها تأثیر می‌گذارند، زمینه گفته می‌شود. تمیز شرایط زمینه‌ای از شرایط علی مشکل است. در برابر شرایط علی که مجموعه‌ای از متغیرهای فعال است، شرایط زمینه‌ای را مجموعه‌ای از مفاهیم، مقوله‌ها یا متغیرهای زمینه‌ای تشکیل می‌دهند.

راهبردهای تعامل و کنش[۳]: کنش‌ها و برهم‌کنش‌ها، بیانگر رفتارها، فعالیت‌ها و مراودات هدف‌داری‌اند که در پاسخ به مقوله محوری و تحت تأثیر شرایط مداخله‌گر، اتخاذ می‌شوند. به این مقولات، راهبرد نیز گفته می‌شود. البته از آن‌ها تحت عنوان فراگردها نیز یاد می‌شود.

عوامل مداخله‌گر[۴]: شرایط مداخله‌گر، شرایط عمومی و ساختاری هستند که مداخله سایر عوامل را تسهیل یا محدود می‌کنند.

پیامد[۵]: مقوله‌ای که در رابطه با آن، نظریه ارائه می‌شود و نتیجه راهبردهای تعامل و کنش است، پیامد خوانده می‌شود. این مقوله، دارای همان عنوانی (نام یا برچسب مفهومی) است که برای چارچوب یا طرح پدیدارشده، در نظر گرفته می‌شود.

بعد از تعریف مقوله محوری بـا کدگـذاری مجـدد داده‌ها، انـواع شرایط تأثیرگذار بر مقوله محوری (زمینه و شـرایط مداخله‌گر)، کنش‌ها و برهمکنش‌هایی که برای اداره، کنترل یـا پاسـخ بـه مقولـه محوری به وجود می‌آیند (به آن‌هـا راهبـرد نیـز گفته می‌شود) و پیامدهای ناشی از آن‌ها نیز تعریف می‌شوند. در مرحلـــه کدگذاری محوری، سعی شد تا ضمن انتخاب یک مقوله به‌منزله مقوله محوری، بر اساس ساختار مدل پارادایم، داده‌ها مجدداً مورد پـردازش قرار گیرند. بر این اساس، با توجه به ویژگی‌های فـوق کـه به‌وسیله اســتراوس دربــاره مقولــه محــوری مطــرح شــده، مقولــه «مدیریت استراتژیک سرمایه انسانی» به‌منزله مقوله محوری

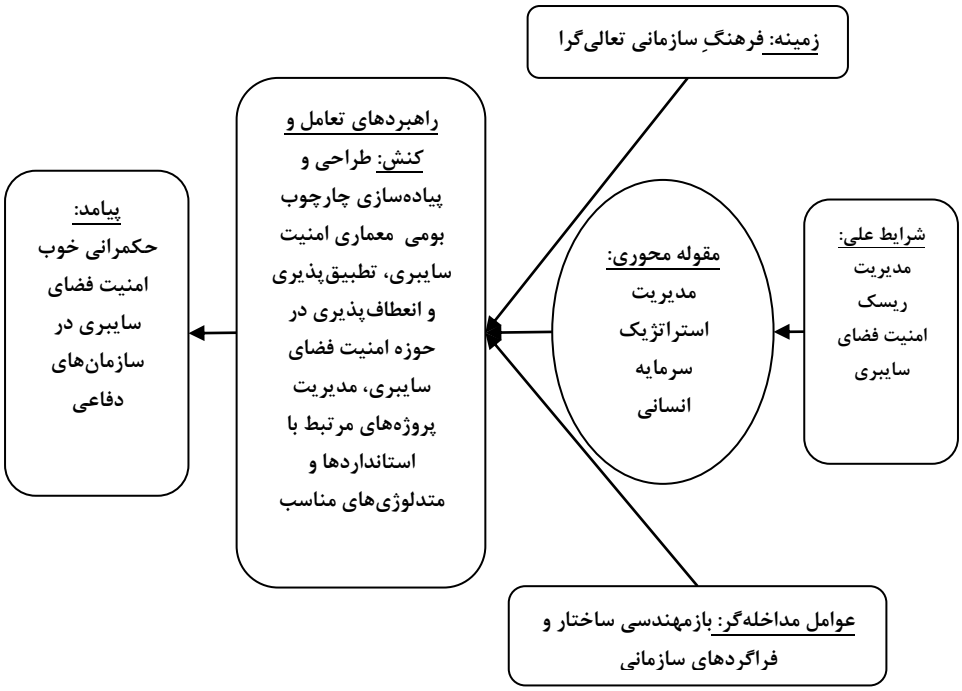
---

۱. Central Category
۲. Context
۳. Action & Interaction Strategies
٤. Intervening Conditions
٥. Outcome

در نظر گرفته شد و با استفاده از مقوله‌های تولیدشده در مرحله کدگذاری باز و همچنین، داده‌های جمع‌آوری‌شده، تلاش شد تا شرایط علی، شرایط مداخله‌گر، زمینه و پیامد برای مقوله محوری، تعریف شوند.

گام سوم، کدگذاری انتخابی: هدف نظریه‌پردازی داده بنیاد، تولید نظریه است نه توصیف صرف پدیده. برای این‌که تحلیل‌ها به نظریه تبدیل شوند، مفاهیم باید به‌طور منظم به یکدیگر ربط یابند. کدگذاری انتخابی، مرحله اصلی نظریه‌پردازی است که بر اساس نتایج دو مرحله قبلی کدگذاری (که به‌منزله مراحل مقدماتی و زمینه‌ساز برای نظریه‌پردازی، مقوله‌ها و روابط مقدماتی را به‌منزله سازه‌ها و اصول اصلی نظریه در اختیار می‌گذارند) به تولید نظریه می‌پردازد؛ به‌این‌ترتیب که مقوله محوری را به شکلی سامان‌مند به دیگر مقوله‌ها ربط داده، آن روابط را در چارچوب یک روایت روشن کرده و مقوله‌هایی را که به بهبود و توسعه بیش‌تری نیاز دارند، اصلاح می‌کند. در این سطح، سعی می‌شود با کنار هم نهادن مقوله‌ها، حول مقوله محوری، به‌منزله مضمون اصلی یک روایت نظری برای پدیده ارائه شده و ضمن آن، حول‌وحوش این رشته اصلی، بین مفاهیم و مقوله‌ها، ارتباطی سامان‌مند ایجاد شود (Strauss & Corbin, ۱۹۹۸:۱۳۱). بنابراین، کدگذاری انتخابی، فراگرد یکپارچه‌سازی و بهبود (پالایش) مقوله‌ها است؛ به‌این‌ترتیب که محقق با ایجاد یک آهنگ و چیدمان خاص بین مقوله‌ها، آن‌ها را برای ارائه و شکل‌دهی یک نظریه (تصویر) تنظیم می‌کند. تئوری حاصل شامل ایده‌ها و نمونه‌هایی است که می‌تواند در پژوهش‌های بعدی مورد بررسی قرار گیرد. این نظریه می‌تواند در قالب مجموعه‌ای از فرضیه‌ها (اصلی و فرعی) بیان شود (Creswell, ۲۰۰۴:۱۹). همان‌طور که اشاره شد، در این مطالعه، ارائه الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی، مورد بررسی و موشکافی قرار گرفت. در مطالعه این پدیده، مقوله‌های نویی به چشم خورد که بر اساس آن‌ها، جداول کدگذاری باز تنظیم شد؛ سپس درمرحله‌کدگذاری محوری، بر اساس مدل پارادایم و با محوریت مقوله «مدیریت استراتژیک سرمایه انسانی»، به‌منزله یک مضمون اصلی، مقوله‌ها توسعه بیش‌تری پیداکرده، بین آن‌ها و مقوله محوری روابطی ایجاد شد و در نهایت، الگوی مربوطه در قالب نمودار ۳ قابل‌مشاهده است:

نمودار شمارهٔ ۳: الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی مستخرج از فاز کیفی (نظریه‌پردازی داده بنیاد)



تحلیل یافته‌های پژوهش: فاز کمی

پس از اتمام فرآیند کدگذاری و به‌منظور ارزیابی نتایج حاصل به‌منظور ارتقای روایی یافته-های حاصل از فاز کیفی، از پرسشنامه استفاده‌شده است. در این مرحله با استفاده از ابزار پرسشنامه به جمع‌آوری داده‌های موردنیاز پرداخته‌شده است. پرسشنامه دارای دو بخش است که در بخش اول، اطلاعات مربوط به پاسخ‌دهندگان شامل تجربه کاری، سن و غیره مورد سؤال قرارگرفته است. در بخش دوم، ابعاد نهایی حاصل از فاز کیفی پژوهش مورد سؤال قرارگرفته است. با توجه به ماهیت پرسشنامه تهیه‌شده و تخصص موردنیاز برای پاسخ‌دهندگان، جامعه آماری شامل ۷۳ نفر از متخصصان حوزه امنیت فضای سایبری قابل‌شناسایی و در دسترسِ فعال در سازمان‌های بخش دفاع در شهر تهران در نظر گرفته شد. با توجه به ساختار جامعه آماری و شناسایی متخصصان مربوطه، نمونه به‌صورت تمام شمار در نظر گرفته شد و پرسشنامه

بین تمامی اعضا توزیع شد. تعداد ۷۳ پرسشنامه توزیع گردید که از این تعداد، ۶۷ پرسشنامه به‌منظور تحلیل داده‌ها قابل‌استفاده بودند. اطلاعات مربوط به مشارکت‌کنندگان در تکمیل پرسشنامه به شرح جدول ۳ است:

جدول شمارهٔ ۳: اطلاعات جمعیت شناختی پاسخ‌دهندگان به پرسشنامه

سطح تحصیلات	تعداد	جنسیت	تعداد
دکتری	۱۱	مرد	۳۹
کارشناسی ارشد	۳۵	زن	۲۸
کارشناسی	۲۱		
سن	تعداد	سابقه	تعداد
۲۵ تا ۳۵ سال	۴۶	کمتر از ۵	۱۹
۳۵ تا ۴۵ سال	۱۴	۵ تا ۱۰	۲۱
بیشتر از ۴۵ سال	۷	۱۱ تا ۱۵	۲۰
		بیشتر از ۱۵	۷

بدین ترتیب از پاسخ‌دهندگان خواسته شد که میزان اهمیت هر یک از ابعاد در حکمرانی خوب امنیت سایبری را بر اساس طیف لیکرت پنج گزینه‌ای مشخص نمایند. به‌منظور ارزیابی تجزیه‌وتحلیل مناسب داده‌های حاصل از پرسشنامه از آزمون تی تک نمونه‌ای بهره گرفته‌شده است.

بررسی روایی پرسشنامه

مفهوم روایی و اعتبار به این سؤال پاسخ می‌دهد که ابزار اندازه‌گیری تا چه حد خصیصه موردنظر را می‌سنجد. بدون آگاهی از اعتبار ابزار اندازه‌گیری نمی‌توان به‌دقت داده‌های حاصل از آن اطمینان داشت (سرمد، ۱۳۸۰). برای تائید روایی پرسشنامه ضمن بررسی دقیق مبانی نظری موجود، جمع‌آوری و تحلیل داده‌ها از منابع مختلف و انجام مصاحبه‌ها، پرسشنامه نهایی قبل از توزیع، در اختیار شش نفر از خبرگان حوزه قرار داده شد و پس از اعمال اصلاحات موردنظر ایشان، مورد تائید قرارگرفته و توزیع شد.

بررسی پایایی پرسشنامه

در آمار، پایایی ملاکی برای همسانی یک مجموعه از سنجش‌ها یا ابزارهای سنجش است که در خصوص آزمون یک‌چیز مشابه به کار می‌روند، پس پایایی مترادف با همسانی آن ابزار است. پایایی یک ابزار یعنی اینکه تا چه حد آن ابزار داده‌های دقیق و درستی را استخراج می‌کند و در طول زمان باثبات است و نتیجه‌های همسان به دست می‌دهد (سرمد، ۱۳۸۰).

یکی از روش‌های برآورد پایایی که برای سنجش پایایی پرسش‌های چندگزینه‌ای توصیه می‌شود، روش آلفای کرونباخ[۱] است. این ضریب برای محاسبه هماهنگی درونی ابزار اندازه‌گیری ازجمله پرسشنامه‌ها یا آزمون‌هایی که خصیصه‌های مختلف را اندازه‌گیری می‌کنند به کار می‌رود. اگر ضریب آلفای کرونباخ ۰/۷ یا بیشتر باشد نشان‌دهنده آن است که پرسشنامه از پایایی مطلوبی برخوردار است و می‌توان از بابت همبستگی درونی سؤالات مطمئن بود. پایایی پرسشنامه با آزمون آماری آلفای کرونباخ بررسی و مورد تائید قرارگرفته است. در پژوهش حاضر برای محاسبه آلفای کرونباخ از نرم‌افزار SPSS استفاده‌شده است و مقدار آلفای به‌دست‌آمده در نمونه اولیه شامل ۳۰ پرسشنامه برابر با ۸۹/. است که نشان‌دهنده این است که پرسشنامه دارای پایایی مناسب است. آلفای محاسبه‌شده برای تمامی پاسخ‌نامه‌ها نیز ۹۵/. است.

جدول ۴: پایایی پرسشنامه

نوع آزمون	مقدار ضریب آلفا	حجم نمونه
آزمون اولیه	۰،۸۹	۳۰
آزمون کلی	۰،۹۵	۶۷

بررسی آزمون توزیع نرمال پرسشنامه

آزمون توزیع نرمال پرسشنامه موردبررسی و تائید قرار گرفت. در این بخش با استفاده از آزمون کلموگروف- اسمیرنف فرض نرمال بودن نمونه‌های موردمطالعه بررسی و تائید شده است.

---

۱. Cronbach Alpha

تحلیل داده‌های پرسشنامه با آزمون تی تک نمونه‌ای (سنجش تأثیر مضامین بر حکمرانی خوب امنیت فضای سایبری)

برای بررسی معناداری ابعاد، با توجه به نرمال بودن داده‌ها از آزمون پارامتریک تی تک نمونه‌ای استفاده می‌شود. آزمون تی، جهت تعیین این‌که آیا میانگین مشاهده‌شده در نمونه که به‌صورت تصادفی از جامعه تی آزمون‌های انتخاب‌شده است، مقداری برابر با میانگین مفروض جامعه دارد یا خیر، به کار می‌رود. در سطح اطمینان ۹۵ درصد چنانچه سطح معناداری کمتر از ۰/۰۵ باشد و میانگین متغیرها از حد متوسط ۳ بیشتر باشد، فرضیه تائید و در غیر این صورت رد می‌شود. تحلیل داده‌های بخش اول پرسشنامه با استفاده از آزمون تی تک نمونه‌ای صورت گرفته است. برای استفاده از آزمون تی تک نمونه‌ای هفت فرض برای مضامین به شکل زیر و به‌صورت جداگانه برای هر مضمون مطرح می‌گردد:

مضامین مدیریت استراتژیک سرمایه انسانی، طراحی و پیاده‌سازی چارچوب بومی معماری امنیت سایبری، تطبیق‌پذیری و انعطاف‌پذیری، مدیریت ریسک امنیت فضای سایبری، بازمهندسی ساختار و فراگردهای سازمانی، مدیریت پروژه‌های مرتبط با استانداردها و متدلوژی‌های مناسب و فرهنگ‌سازمانی تعالی گرا از عوامل مؤثر بر مدیریت امنیت سایبری با رویکرد حکمرانی خوب امنیت سایبری هستند.

فرض‌های آماری در سطح اطمینان ۹۵ درصد تعریف می‌شود که با توجه به تعداد زیاد، یک مورد از آن ذکرشده و از ذکر سایر موارد صرف‌نظر شده است:

فرض صفر (H_0): مدیریت استراتژیک سرمایه انسانی از مضامین مؤثر بر حکمرانی خوب امنیت سایبری نیست. (میانگین برابر یا کمتر از ۳ است)

فرض مقابل (H_1): مدیریت استراتژیک سرمایه انسانی از مضامین مؤثر بر حکمرانی خوب امنیت سایبری است. (میانگین بیشتر از ۳ است)

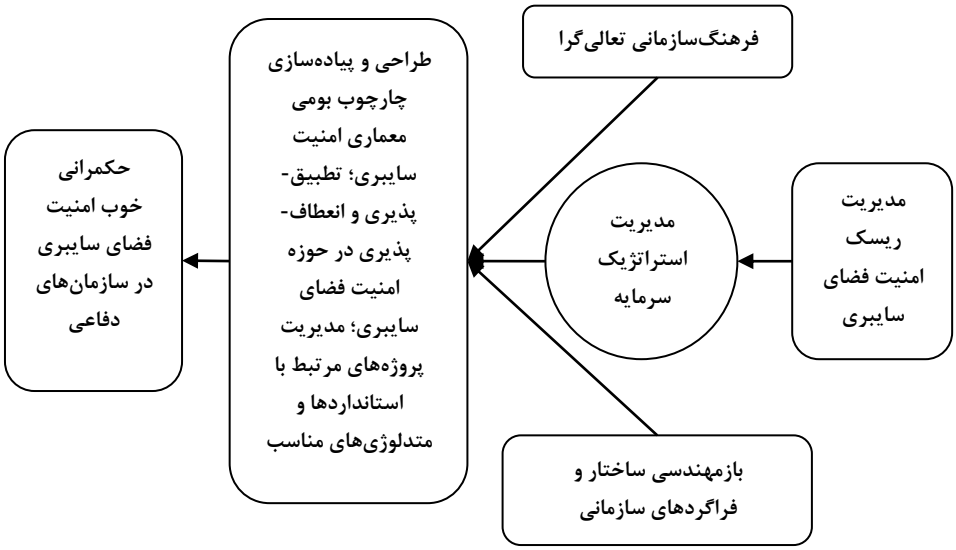
نتایج آزمون در جدول ۶ آمده است.

جدول شمارهٔ ۶: نتایج آزمون تی برای تحلیل میزان تأثیر هر یک از مضامین

ردیف	متغیر	میانگین	سطح معناداری	نتیجه آماری
۱	مدیریت استراتژیک سرمایه انسانی	۴/۱۲۵۰	۰/۰۰۰	تائید فرض مقابل
۲	طراحی و پیاده‌سازی چارچوب بومی معماری امنیت سایبری	۴/۱۵۶۳	۰/۰۰۰	تائید فرض مقابل
۳	تطبیق‌پذیری و انعطاف‌پذیری	۳/۹۳۳۶	۰/۰۰۰	تائید فرض مقابل
۴	مدیریت ریسک امنیت فضای سایبری	۴/۰۷۸۱	۰/۰۰۰	تائید فرض مقابل
۵	بازمهندسی ساختار و فراگردهای سازمانی	۴/۰۱۵۶	۰/۰۰۰	تائید فرض مقابل
۶	مدیریت پروژه‌های مرتبط با استانداردها و متدلوژی‌های مناسب	۳/۸۹۰۶	۰/۰۰۰	تائید فرض مقابل
۷	فرهنگ‌سازمانی تعالی گرا	۴/۱۱۷۲	۰/۰۰۰	تائید فرض مقابل

یافته‌ها در جدول فوق نشان می‌دهد که میانگین تمامی متغیرها از سطح متوسط (۳) بیشتر است و همچنین سطح معناداری کمتر از ۰/۰۵ و معنادار است.

با توجه به یافته‌های فاز کمی، یافته‌های فاز کیفی مورد تائید قرارگرفته و مضامین هفت‌گانه مدیریت استراتژیک سرمایه انسانی، طراحی و پیاده‌سازی چارچوب بومی معماری امنیت سایبری، تطبیق‌پذیری و انعطاف‌پذیری در حوزه امنیت فضای سایبری، مدیریت ریسک امنیت فضای سایبری، بازمهندسی ساختار و فراگردهای سازمانی، مدیریت پروژه‌های مرتبط با توجه به استانداردها و متدلوژی‌های مناسب و فرهنگ‌سازمانی تعالی‌گرا در حکمرانی خوب امنیت فضای سایبری قابل‌توجه هستند.



نمودار ۴: الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی

در ادامه، مضامین هفت‌گانه الگوی حکمرانی خوب امنیت فضای سایبری در سازمان‌های دفاعی به‌اختصار توضیح داده خواهند شد.

مدیریت استراتژیک سرمایه انسانی

مدیریت سرمایه انسانی یعنی مدیریت و اداره راهبردی و پایدار باارزش‌ترین دارایی‌های سازمان یعنی کارکنانی که در آن سازمان کار می‌کنند و در کنار هم دررسیدن به اهداف سازمانی همکاری دارند (انصاری و همکاران، ۱۳۸۹). مدیریت سرمایه انسانی، الگویی از تصمیم‌هایی است که در مورد سرمایه انسانی اتخاذ و اجرا می‌گردد و به‌طورکلی شامل کارکردهای تأمین نیروی انسانی (برنامه‌ریزی، کارمند یابی، انتخاب، توسعه مسیر شغلی، آموزش و توسعه)، ارزیابی عملکرد و پرداخت (تجزیه تحلیل و ارزیابی شغل، ارزیابی عملکرد، ترکیب و ساختار پرداخت) و روابط کار (ایجاد و تقویت رابطه کاری بین فرد و سازمان، نظارت و کنترل، هویت و تعلق سازمانی) است.(سید جوادین و حسین زاده، ۱۳۸۶) مدیریت سرمایه انسانی را می‌توان فرآیند بررسی و شناسایی، انتخاب، استخدام، تربیت و پرورش نیروی انسانی به‌منظور دستیابی به اهداف سازمان تعریف و معرفی کرد. منظور از سرمایه انسانی تمام افرادی است که در سطوح مختلف سازمان مشغول به کار هستند. لذا مدیریت سرمایه انسانی به

استفاده صحیح از سرمایه انسانی جهت دست یافتن به اهداف سازمان توجه بسیاری می‌کند (خوشبخت و همکاران،۱۳۹۱). مدیریت سرمایه انسانی برای رسیدن به اهداف خویش و پیروی از فلسفه وجودی خود در قالب سیاست‌ها و راهبردهای مدیریت سرمایه انسانی، اقدام به تجویز و به‌کارگیری راه‌ها و شیوه‌های اداره سرمایه انسانی در سازمان‌ها می‌نماید.

امنیت دستگاه‌های اطلاعاتی، هم فن‌آوری و هم افراد (عوامل انسانی) را در برمی‌گیرد. کاربران و در کل، عوامل انسانی، ضعیف‌ترین و سست‌ترین عنصر آسیب‌پذیر در مدل‌های امنیت دستگاه‌های اطلاعاتی مطرح‌اند. سازه‌های"حمایت مدیریت عالی، آموزش امنیتی، فرهنگِ امنیتی، مهارت امنیتی، تقویت خط‌مشی امنیتی، تجربیات و خودباوری افراد" به‌عنوان فاکتورهای مؤثر بر اثربخشی امنیت دستگاه‌های اطلاعاتی معرفی می‌شوند (الهی و همکاران، ۱۳۸۸). امنیت سرمایه انسانی، شامل تمامی موارد مربوط به کارکنان است. بخش مهمی از یک طرح امنیتی خوب، مربوط به اداره کارکنان با دسترسی‌های طبقه‌بندی‌شده است (حریری و نظری، ۱۳۹۱). موفقیت امنیت اطلاعات تا حد زیادی به رفتار اثربخش کاربران وابسته است. رفتارهای درست و سازنده توسط کاربران، مدیران سیستم و افراد دیگر می‌تواند اثربخشی امنیت سایبری را تا حد زیادی بالا ببرد؛ درحالی‌که رفتارهای نادرست و مخرب، در حقیقت می‌تواند مانع اثربخشی آن شود. بر اساس یافته‌های پژوهش برای حکمرانی خوب امنیت سایبری، عوامل انسانی مانند آموزش‌های استراتژیک به کارکنان، تبیین نقش‌ها و مسئولیت‌های افراد، ارتقاء مسئولیت‌پذیری کارکنان، برخورد جدی با تخلف کارکنان، نظارت جامع بر عملکرد کارکنان، انگیزش کارکنان و ارتقای سطح آگاهی کارکنان قابل‌توجه هستند.

طراحی و پیاده‌سازی چارچوب بومی معماری امنیت سایبری

معماری امنیت سایبری هر سازمان برای حفاظت از اطلاعات ارزشمند، باید به یک راهبرد خاص پایبند باشد و بر اساس آن، سیستم امنیتی را پیاده‌سازی و اجرا نماید. وجود خط‌مشی امنیت، از مهم‌ترین شاخص‌های تعیین‌کننده برنامه‌های سازمان برای حفظ امنیت منابع دیجیتالی است. خط‌مشی امنیت، گام‌های لازم برای حفاظت سرمایه‌ها را تعریف می‌کند. نخست، مشخص می‌کند از چه چیزی حفاظت می‌شود و چرا. دوم، مسئولیت مربوط به تأمین این حفاظت را مشخص می‌کند. سوم، زمینه‌ای برای تفسیر و حل مشکلات آتی ارائه می‌دهد (حریری و نظری، ۱۳۹۱). بر اساس یافته‌های پژوهش، برای حکمرانی خوب امنیت سایبری،

عواملی نظیر تدوین سند راهبردی شامل چشم‌انداز، اهداف و راهبردها، طراحی و تدوین چارچوب بومی معماری امنیت فضای سایبری، تخصیص منابع موردنیاز شامل بودجه، نیروی انسانی و غیره، بومی‌سازی استانداردها با توجه به اصل وابستگی به مسیر[۱] و توسعه و به‌کارگیری ابزارها و فناوری‌های امنیتی بومی می‌توانند دارای اهمیت باشند.

تطبیق‌پذیری و انعطاف‌پذیری در حوزه امنیت فضای سایبری

تطبیق‌پذیری به معنی ظرفیتِ نشان دادن پاسخ‌های مختلف به چالش‌های درونی و بیرونی سازمان به‌صورت مجموعه‌ای از عملیات و روال‌های پیشگیرانه و واکنشی است که به تطبیق مستمر سازمان با محیط و جذب چالش‌ها کمک می‌کند. دگرگونی‌های اجتماعی، فن‌آوری‌های پرشتاب و چالش زا و تکوین رسالت‌های جدید در سازمان‌ها، ضرورت انعطاف‌پذیری و آمادگی برای رویارویی با شرایط جدید را امری اجتناب‌ناپذیر ساخته است (شوقی و آقاجانی، ۱۳۹۲). سازمان‌هایی که به‌خوبی یکپارچه هستند، به‌سختی تغییر می‌یابند. لذا یکپارچگی درونی و انطباق‌پذیری بیرونی را می‌توان مزیت وبرتری سازمان به‌حساب آورد. این ویژگی با دو شاخص موردبررسی قرار می‌گیرد:

۱. تغییر: سازمان قادر است راه‌هایی برای تأمین نیازهای تغییر ایجاد کند و می‌تواند محیط را بشناسد، به محرک‌های جاری پاسخ دهد و از تغییرات آینده پیشی جوید.

۲. یادگیری سازمانی: میزان علائم محیطی را که سازمان‌ها دریافت، ترجمه و تفسیر می‌کنند و فرصت‌هایی را برای تشویق خلاقیت، سبک دانش و توسعه توانایی‌ها ایجاد می‌کند اندازه می‌گیرد.

بر اساس یافته‌های پژوهش، در حکمرانی خوب امنیت سایبری، توجه به یکپارچگی امنیت فضای سایبری با سایر حوزه‌های سازمان، هم‌راستایی اهداف امنیت فضای سایبری با اهداف

---

۱. برابر این اصل، فراگردهای وابسته به مسیر حرکت گذشته، پدیده‌هایی هستند که نتایج و دستاوردهای آنها، فقط به منزله جزیی از یک فراگرد تاریخی قابل درکند؛ دستاوردها و نتایجی که ضرورتاً بهینه نیستند. هر ملتی، تاریخچه خاص خود را دارد و نهادها و ساختارهای خاص هر ملت، به سیستم ملی خود، یک شخصیت متمایز می‌دهد.

سازمان، ترویج تعامل‌پذیری و توسعه ارتباطات و ارتقاء سطح چابکی سازمانی از اهمیت بالایی برخوردار هستند.

مدیریت ریسک امنیت فضای سایبری

مدیریت ریسک، فرآیندی است برای درک ریسک‌های بالقوه و برنامه‌ریزی به‌منظور از بین بردن، کاهش اثر یا بهره‌برداری از این ریسک‌ها. مدیریت ریسک، ابزار خوبی برای کنترل ریسک است. مدیریت ریسک امنیت فضای سایبری، رویکردی نوین در راستای ارتقای اثربخشی سازمان‌ها بوده که با توجه به ماهیت نامطمئن محیط سازمان، افزایش پیچیدگی ریسک‌ها و لزوم صرف بهینه منابع، از اهمیت انکارناپذیری برخوردار است. مدیریت ریسک امنیت فضای سایبری فعالیت‌های هماهنگ شده برای هدایت و کنترل یک سازمان با توجه به ریسک است (نعمتی و نعمتی زاده، ۱۳۹۴). بدیهی است هر سازمان با توجه به ماهیت کار خود، ریسک‌های گوناگونی را تجربه می‌کند و در شرایط متحول امروز، اساساً موفقیت هر سازمان به تسلط آن بر ریسک‌ها و نوع مدیریتی است که بر انواع ریسک‌ها اعمال می‌کند. مدیریت ریسک امنیت فضای سایبری زمانی معنا و مفهوم پیدا می‌کند که شرایط با احتمال متحمل شدن زیان و عدم اطمینان مواجه شود. این نوع مدیریت شامل حوزه‌های گسترده‌ای است که مسائل مالی، عملیاتی، تجاری، استراتژیک و حوزه وسیع‌تری به نام حوادث خطرآفرین را در برمی‌گیرد. درمجموع، مدیریت ریسک امنیت فضای سایبری، فرآیند سنجش یا ارزیابی ریسک و سپس طرح استراتژی‌هایی برای اداره ریسک است. متفکران چهار استراتژی متداول برای مدیریت ریسک امنیت فضای سایبری برشمرده‌اند: ۱. انتقال ریسک (قبول ریسک توسط بخش دیگر)، ۲. اجتناب از ریسک (عدم انجام فعالیتی که موجب ریسک شود)، ۳. کاهش ریسک (شیوه‌هایی که موجب کاهش شدت زیان شود)، ۴. پذیرش ریسک (قبول زیان در هنگام وقوع) (معمار و رشادت جو، ۱۳۹۳).

بر اساس یافته‌های پژوهش، در حکمرانی خوب امنیت سایبری، شناسایی ریسک‌های احتمالی حوزه امنیت فضای سایبری، ارزیابی میزان آسیب ریسک‌های احتمالی حوزه امنیت فضای سایبری، ارزیابی احتمال وقوع ریسک‌های احتمالی حوزه امنیت فضای سایبری و استفاده از استانداردها و متدولوژی‌های مدیریت ریسک امنیت فضای سایبری دارای اهمیت هستند.

بازمهندسی ساختار و فراگردهای سازمانی

بازمهندسی ساختار و فراگردهای سازمانی، راه یا شیوه‌ای است که به‌وسیله آن فعالیت‌های سازمان تقسیم، سازمان‌دهی و هماهنگ می‌شود (مشبکی و موسوی مجد، ۱۳۹۱). بازمهندسی ساختار و فراگردهای سازمانی تصریح می‌کند که وظایف، چگونه تخصیص داده شوند، چه شخصی به چه کسی گزارش دهد و سازوکارهای رسمی و همچنین الگوهای تعاملی سازمانی که باید رعایت شوند کدام‌اند (قدمی و همکاران، ۱۳۹۲). بازمهندسی ساختار و فراگردهای سازمانی الگو و نقشه ارتباطات و تعاملات میان بخش‌ها و اجزاء یک سازمان است. روابط رسمی افراد، جایگاه مشاغل و پست‌های سازمانی، میزان دسترسی به چارچوب اطلاعات، شرح وظایف (شیوه انجام کارها)، شرح شغل‌ها، چگونگی تخصیص منابع، قوانین و مقررات، مکانیسم‌های تبعیت و اجرای قوانین، ایجاد هماهنگی بین فعالیت‌ها، بخش‌هایی از نتایج ایجاد و طراحی بازمهندسی ساختار و فراگردهای سازمانی است (واعظی و سبزیکاران، ۱۳۸۹). در بازمهندسی ساختار و فراگردهای سازمانی، دو کار مهم صورت می‌گیرد، اول آنکه وظایف اصلی سازمان به وظایف فرعی شکسته می‌شود، وظایف فرعی به پست‌ها و واحدهای سازمانی محول می‌شود و نوعی تقسیم‌کار به وجود می‌آید و سپس از طریق سازوکارهای هماهنگی، همکاری لازم برای دستیابی به هدف مشترک فراهم می‌شود.

در راستای حکمرانی خوب امنیت اطلاعات، یافته‌های پژوهش نشان می‌دهد که طراحی و ایجاد ساختار و تشکیلات امنیت سایبری، بازمهندسی ساختار و فراگردهای سازمانی بر اساس شرایط، تدوین خط‌مشی و دستورالعمل‌های موردنیاز، تعیین محدوده و مرزهای امنیت سایبری (قلمرو امنیت فضای سایبری) در سازمان و تعیین و انتخاب معیارها و سنجه‌های امنیت سایبری، امری حیاتی به‌حساب می‌آید.

مدیریت پروژه‌های مرتبط با استانداردها و متدلوژی‌های مناسب

مدیریت پروژه، هنر هدایت و هماهنگی سرمایه انسانی و موارد و مصالح در سراسر عمر یک پروژه با استفاده از تکنیک‌های مدرن مدیریت جهت دستیابی به اهداف از پیش تعیین‌شده حدود خدمات، هزینه، زمان، کیفیت و ارضای مشارکت قلمداد می‌شود. مدیریت راهبردی پروژه به‌عنوان رویکردی جدید در مدیریت پروژه بر ایجاد مزیت رقابتی برای سازمان تمرکز می‌کند. رویکرد مدیریت راهبردی پروژه به این مطلب اشاره می‌کند که پروژه‌ها برای رسیدن به نتایج

سازمان باید تعریف شوند و مدیریت پروژه بایستی با راهبردهای سازمآن‌همسو گردد. درواقع همسویی مدیریت پروژه با راهبرد سازمان به‌طور قابل‌توجهی می‌تواند دستیابی به اهداف راهبردی سازمان و عملکرد آن را ارتقا بخشد. تیم‌های پروژه باید یاد بگیرند که چگونه نیازهای سطوح بالاتر سازمان را درک کنند و سپس پروژه‌ها را نه‌فقط برای رسیدن به اهداف زمانی و بودجه‌ای بلکه برای خلق ارزش برای مشتری و دستیابی به اهداف راهبردی سازمان برنامه‌ریزی و اجرا کنند. مدیریت راهبردی پروژه بر بهترین استفاده از منابع و هماهنگی این منابع برای دستیابی به چشم‌انداز و اهداف سازمان پروژه محور، توجه می‌کند.

یافته‌های پژوهش بیان‌کننده میزان اهمیت مدیریت استراتژیک پروژه‌های امنیت سایبری، تدوین و اجرای محرک‌های حرکت سازمان در جهت برقراری امنیت سایبری، پیاده‌سازی سیستم استاندارد مستندسازی و مدیریت منابع پروژه‌های حوزه امنیت فضای سایبری است.

فرهنگ‌سازمانی تعالی‌گرا

ضرورت توجه به فرهنگ‌سازمانی تعالی گرا تا جایی است که صاحب‌نظران بر این باورند، اگر قرار است در یک سازمان تغییرات مؤثر و پایدار به وجود آید فرهنگ آن سازمان باید دستخوش تغییر شود. به‌عبارت‌دیگر، موفقیت و شکست سازمان‌ها را باید در فرهنگ آن جستجو نمود. لذا مدیران با دست یازیدن به فرهنگ و بهره گرفتن از آن می‌توانند خود را از بند راه‌حل‌های گذشته رها ساخته و راه‌حل‌های جدیدی برای سازمان و پیشرفت آن فراهم آورند. فرهنگ‌سازمانی تعالی گرا، همان ارزش‌های اساسی، باورها و اصول اخلاقی است که نقش مهمی در یک سیستم مدیریت سازمانی ایفا می‌کند. فرهنگ‌سازمانی تعالی گرا، الگویی از مفروضات اساسی است که توسط گروهی از افراد مطرح گردیده و گسترش پیداکرده است، به‌گونه‌ای که با محیط بیرونی منطبق و موجب انسجام در داخل گروه می‌گردد. مطالعات نشان می‌دهد که فرهنگ‌سازمانی تعالی گرا بر تدوین اهداف، استراتژی، عملکرد سازمانی، انگیزش، رضایت شغلی، خلاقیت و نوآوری، کارآفرینی، نحوه تصمیم‌گیری، میزان مشارکت کارکنان در امور، میزان فداکاری و تعهد، سخت‌کوشی و سطح اضطراب تأثیر می‌گذارد. یافته‌های پژوهش نشان‌دهنده این است که در خصوص این مضمون باید به فرهنگ‌سازی امنیت سایبری، تدوین و اجرای استراتژی‌های اشاعه فرهنگ امنیت و وجود تفکر استراتژیک در رابطه با امنیت فضای سایبری توجه نمود.

نتیجه‌گیری:

حکمرانی خوب امنیت فضای سایبری، رویکردی نوین در مبحث امنیت فضای سایبری است که با نگاه جامع و کلان، حوزه‌های مدیریتی و تصمیم‌گیری در امنیت فضای سایبری را موردتوجه قرار می‌دهد. یافته‌های این پژوهش نشان می‌دهد مضامین هفت‌گانه مدیریت استراتژیک سرمایه انسانی، طراحی و پیاده‌سازی چارچوب بومی معماری امنیت سایبری، تطبیق‌پذیری و انعطاف‌پذیری در حوزه امنیت فضای سایبری، مدیریت ریسک امنیت فضای سایبری، بازمهندسی ساختار و فراگردهای سازمانی، مدیریت پروژه‌های مرتبط با توجه به استانداردها و متدلوژی‌های مناسب و فرهنگ‌سازمانی تعالی گرا در حکمرانی خوب امنیت فضای سایبری در بخش دفاع جمهوری اسلامی ایران و سازمان‌های مربوطه شامل ارتش، سپاه، وزارت دفاع و نیروی انتظامی قابل‌توجه هستند. بر اساس نتایج به‌دست‌آمده، در کنار لزوم استفاده از روش‌های فنی، موضوعات مرتبط با نیروی انسانی مهم‌تر از بقیه موارد شناسایی‌شده‌اند. در تحقیقات پیشین، در حوزه امنیت سایبری بیشتر به مسائل فنی و تکنیکی توجه شده است که در سال‌های اخیر این رویکرد کمی تغییریافته و توجه به حوزه‌های مدیریتی امنیت به‌خصوص مدیریت منابع انسانی و ایجاد فرهنگ‌سازمانی امنیت بیشتر شده است. هرچند استفاده از راه‌حل‌های تکنیکی، ابزارها و فن‌آوری‌های امنیتی جهت برقراری امنیت سایبری امری اجتناب‌ناپذیر است، نتایج این پژوهش ضرورت تغییر رویکرد صرفاً فنی را به ترکیبی از راهکارهای فنی و مدیریتی تائید می‌نماید. بر این اساس، راهکارهای زیر در سازمان‌ها قابل‌توجه خواهند بود:

- داشتن رویکرد کلان و مدیریتی
- تعریف چشم‌انداز، مأموریت‌ها و ارزش‌ها
- تعیین اهداف امنیتی سازمان و ارائه راهکار برای آن
- تدوین خط‌مشی و دستورالعمل‌های امنیتی
- تخصیص بودجه مناسب به آموزش کارکنان، طرح‌ها و پروژه‌های امنیتی
- به‌روزرسانی تجهیزات نرم‌افزاری و سخت‌افزاری بر اساس تحولات امنیتی
- تهیه قوانین مدون و ابلاغ به کارکنان
- توجه به ویژگی‌های سازمان جهت تعیین محدوده و مرزهای امنیت

- تلفیق و یکپارچگی امنیت با حوزه گسترده‌تر در سازمان
- تعامل با محیط کسب‌وکار به‌صورت نزدیک و هماهنگ
- در نظر داشتن منافع سهامداران، کارکنان، عرضه‌کنندگان، سرمایه‌گذاران، نهادهای دولتی و مشتریان
- برنامه‌ریزی فعالیت‌های آتی
- کاهش دادن مقاومت در برابر تغییرات
- از بین بردن فرهنگ‌سازمانی تعالی‌گراناپذیرنده
- ایجاد تعهد سازمانی
- گروه‌بندی (طبقه‌بندی) دارایی‌ها
- تعیین مالکیت داده
- شناسایی تهدیدات و آسیب‌پذیری‌ها
- تحلیل و رتبه‌بندی ریسک‌های امنیت سایبری
- در نظر گرفتن اقدامات پیشگیرانه خاص
- در نظر گرفتن امنیت به‌عنوان یک مسئله سازمان و با اولویت در هیئت‌مدیره
- توسعه شایستگی‌های محوری سازمان

فهرست منابع:

استراس، آنسلم و جولیت کوربین.۱۳۸۵. اصول روش تحقیق کیفی. بیوک محمدی. تهران. پژوهشگاه علوم انسانی و مطالعات فرهنگی، چاپ اول.

امامی، سیدمجید (۱۳۹۲). از جامعه‌شناسی تاریخی ایران تا نظریه سیاستی پیشرفت (توسعه)؛ نقش پارادایم ماهیت گرا در ترسیم الگوی اسلامی ـ ایرانی هویت ملی، فصلنامه مطالعات ملی؛ ۵۶، سال چهاردهم، شماره ۴.

انصاری، محمد اسماعیل؛ و دیگران. ۱۳۸۹. تعهد سازمانی از دیدگاه نظریه‌پردازان و نقش راهبردهای مدیریت منابع انسانی در بهبود آن. دوماهنامه توسعه انسانی پلیس، سال هفتم، شماره ۳۱.

پورعزت، علی‌اصغر و بهنام عبدی (۱۳۹۷). سیستم پشتیبان ارزشیابی عملکرد، انتشارات مهربان، تهران: چاپ اول.

تمتاجی، مصطفی؛ و دیگران.۱۳۹۴. الگوی طبقه‌بندی دارایی‌های اطلاعاتی سازمانی و متدولوژی معماری امنیت. فصلنامه علمی پژوهشی پژوهشگاه علوم و فن‌آوری اطلاعات ایران، دوره ۳۱، شماره۱.

ثامنی توسروندانی، مرضیه؛ و دیگران. ۱۳۹۱. رویکرد نگاشت تهدیدها و قابلیت‌های آسیب‌پذیری در شبکه‌های محلی به کنترل‌های استاندارد ISO/IEC ۲۷۰۰۲ سیستم مدیریت امنیت سایبری. چهارمین کنفرانس مهندسی برق و الکترونیک ایران، دانشگاه آزاد اسلامی گناباد.

چهارسوقی، صدیقه؛ و همکاران. ۱۳۹۲. به‌کارگیری شبکه‌های عصبی مصنوعی در ارزیابی ریسک امنیت سایبری. مجله علمی پژوهشی پدافند الکترونیکی و سایبری، شماره ۴.

حریری، نجلا. نظری، زهرا.۱۳۹۱. امنیت سایبری در کتابخانه‌های دیجیتالی ایران. فصلنامه کتابداری و اطلاع‌رسانی، دوره ۱۶، شماره ۲.

خوش چهره، مجید، نیک بخش حبیبی (۱۳۹۱). اصول پایه ای و عناصر کلیدی الگوی اسلامی-ایرانی پیشرفت از منظر اسناد فرادستی نظام ج.ا.ایران، فصلنامه راهبرد، دوره ۲۱، شماره ۶۲، صص ۲۱۹-۲۴۴.

خوشبخت، میرزاعلی. و دیگران. ۱۳۹۱. شناسایی و اولویت‌بندی عوامل مدیریت منابع انسانی مؤثر بر ارتقای کارآیی کارکنان. فصلنامه مطالعات پژوهشی، سال اول، شماره ۱.

دانایی‌فرد، حسن. امامی، سید مجتبی.۱۳۸۶.استراتژی‌های پژوهش کیفی: تأملی بر نظریه‌پردازی داده بنیاد. انتشارات اندیشه مدیریت.

سرمد، زهره. و دیگران. ۱۳۸۰. روش‌های تحقیق در علوم رفتاری. چاپ پنجم، انتشارات آگاه.

سیف‌الدین، امیرعلی و امیرحسین رهبر (۱۳۹۲). تسهیل گری اسلام در جهت تحقق اقتصاد دانش‌بنیان؛ نگرشی جدید به بستر نهادی الگوی اسلامی ایرانی پیشرفت، فصلنامه سیاست علم و فناوری، سال پنجم، شماره ۴، تابستان.

سید جوادین، سید رضا. حسین زاده، ماشاالله. ۱۳۸۷. بررسی رابطه بین قابلیت‌های استراتژیک کارکنان و سبک‌های مدیریت منابع انسانی در شرکت‌های صنعتی استان تهران. فصلنامه مدرس علوم انسانی، دوره ۱۲، شماره ۱.

شورای عالی پدافند غیرعامل کشور، ۱۳۹۴/۲/۲۹، سند راهبردی پدافند سایبری کشور

شوقی، بهزاد. آقاجانی، طهمورث. ۱۳۹۲. بررسی تأثیر ساختار سازمانی بر فرهنگ‌سازمانی. مجله مطالعات کمّی در مدیریت، سال چهارم، شماره دوم.

قاضی زاده، سید ضیاالدین (۱۳۸۹). الگوی اسلامی ایرانی پیشرفت و نقش نیروهای مسلح، راهبرد دفاعی، دوره ۸، شماره ۳۱، صص ۶۲-۳۱، زمستان.

قدمی، محسن و دیگران. ۱۳۹۲. رابطه فرهنگ با پیچیدگی ساختار سازمانی. مجله مدیریت فرهنگی، سال هفتم، شماره نوزدهم.

کیوان حسینی، سیداصغر و راحله جمعه زاده (۱۳۹۰). پیوندبخشی میان رویکرد دفاع همه‌جانبه و الگوی اسلامی ایرانی پیشرفت؛ چارچوب پیشنهادی، راهبرد دفاعی، دوره ۹، شماره ۳۴، صص ۲۵-۱.

محمودزاده، ابراهیم. رادرجبی، مهدی. ۱۳۸۵. مدیریت امنیت در دستگاه‌های اطلاعاتی. فصلنامه علوم مدیریت ایران، دوره اول، شماره ۴.

مشبکی، اصغر. موسوی مجد، سید محمد. ۱۳۹۱. رابطه هماهنگی استراتژیک بین استراتژی‌های تجاری، استراتژی‌های منابع انسانی و ساختار سازمانی. مجله علمی پژوهشی مدیریت فرهنگ‌سازمانی، دوره دهم، شماره اول.

معمار، علی. رشادت جو، حمیده. ۱۳۹۳. شناسایی عوامل تعیین‌کننده مدیریت ریسک و سنجش تأثیر آن بر مدیریت استراتژیک در شرکت سهامی پتروشیمی تندگویان. فصلنامه مدیریت، سال یازدهم، شماره ۳۴.

مقدم نژاد، عباسعلی. ۱۳۹۱. تبیین آسیب‌های امنیتی در حوزه فن‌آوری اطلاعات و استخراج عوامل مؤثر بر آن. فصلنامه امنیت پژوهی، شماره ۳۷.

موسوی، پریسا و دیگران. ۱۳۹۴. شناسایی ریسک‌های امنیت سایبری سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری. فصلنامه مدیریت فن‌آوری اطلاعات، دوره ۷، شماره ۱.

نعمتی، نرگس. نعمتی زاده، سینا. ۱۳۹۴. توسعه سیستم پشتیبان تصمیم مدیریت ریسک سازمان در شرکت توسعه و نگهداری اماکن ورزشی کشور. فصلنامه آینده‌پژوهی مدیریت، شماره ۱۰۳.

واعظی، رضا. سبزیکاران، اسماعیل. ۱۳۸۹. بررسی رابطه ساختار سازمانی و توانمندسازی کارکنان در شرکت ملی پخش فرآورده‌های نفتی ایران- منطقه تهران. پژوهش نامۀ مدیریت تحول، سال دوم، شمارۀ ۳.

الهی، شعبان و دیگران. ۱۳۸۸. ارائۀ چارچوبی برای عوامل انسانی مرتبط در امنیت دستگاه‌های اطلاعاتی. فصلنامه مدرس علوم انسانی، دوره ۱۳، شماره ۲.

Bevir, M ۲۰۱۳. "Governance: A very short introduction". Oxford. UK: Oxford University Press.

Cavusoglu, H. Cavusoglu, H. Son, J. Benbasat, I. ۲۰۱۵. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Information & Management.

Hall, J.S. ۲۰۰۲. "Reconsidering the Connection between Capacity and Governance". Public Organization Review. ۲. ۲۳-٤٤.

Hufty, M. ۲۰۱۱. "Investigating Policy Processes: The Governance Analytical Framework (GAF)". In: Wiesmann, U. Hurni, H. et al. eds. Research for Sustainable Development: Foundations, Experiences, and Perspectives". Bern: Geographica Bernensia: ٤٠٣–٤٢٤.

Haqaf, Husam & Murat Koyuncu (۲۰۱۸). Understanding key skills for information security managers, International Journal of Information Management, Volume ٤٣, December ۲۰۱۸, Pages ١٦٥-١٧٢.

Hou, Ye, Ping Gao, Brian Nicholson (۲۰۱۸). Understanding organizational responses to regulative pressures in information security management: The case of a Chinese hospital, Technological Forecasting and Social Change, Volume

۱۲٦, January ۲۰۱۸, Pages ٦٤-۷٥.

Naicker, V., and Mafaiti, M. (۲۰۱۸). The Establishment of collaboration in managing information security through multi sourcing, Computers & Security, Available online ۱۲ October ۲۰۱۸.

Pandit, N.۱۹۹٦.The creation of theory: a recent application of the Grounded Theory method, The Qualitative Report.Vol ۲.No ٤.

Pettai V. & Illing E. ۲۰۰٤. "Governance and Good Governance". Journal of Humanities and Social Sciences. Vol. ۸. No ٤.

Pierre, J. & Peters, B.G. Governance, ۲۰۰۰. "The State and Public Policy". Basingstoke: Palgrave.

Rhodes, R.A.W. ۱۹۹٦. "The New Governance: Governing Without Governance". Political Studies. ٤٤. ٦٥۲-٦۷.

Rosenbloom, D.H. ۱۹۸۳. "Public Administration Theory and the Separation of Powers". Public Administration Review.Vol. ٤۳. No. ۳.Rajab, Majed and Ali Eydgahi (۲۰۱۸). Evaluating the Explanatory Power of Theoretical Frameworks on Intention to Comply with Information Security Policies in Higher Education, Computers & Security, Available online ۱۳ October ۲۰۱۸, In Press.

Steinbart, Paul John, Robyn L.Raschke, Graham Gal, William N.Dilla (۲۰۱۸). The influence of a good relationship between the internal audit and information security functions on information security outcomes, Accounting, Organizations and Society, Available online ۲٥ May ۲۰۱۸, In Press.

Shamala, Palaniappan, Rabiah Ahmad, Ali Zolaitc, Muliati Sedek (۲۰۱۷). Integrating information quality dimensions into information security risk management (ISRM), Journal of Information Security and Applications, Volume ۳٦, October ۲۰۱۷, Pages ۱-۱۰.

Torten, Ron, Carmen Reaiche, Stephen Boyle (۲۰۱۸). The impact of security awarness on information technology professionals' behavior, Computers & Security, Volume ۷۹, November ۲۰۱۸, Pages ٦۸-۷۹.

Mesquida, A. Mas, A. ۲۰۱٥.Implementing information security best practices on software lifecycle processes: The ISO/IEC ۱٥٥۰٤ Security Extension. computers & s e c u rity ٤ ۸. ۱ ۹ e۳ ٤.

Yildirim, E. Akalpa,G. Aytac,S. Bayram,N. ۲۰۱۱. Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. International Journal of Information Management.

SHARIATI BEHNAM, ۲۰۱٦, A Continuous Monitoring Framework To Manage Cybersecurity Against Insider Threats, George Washington University.

SHARIATI BEHNAM, ۲۰۱٦, A Continuous Monitoring Framework To Manage Cybersecurity Against Insider Threats, George Washington University.

Department of Defense (Dod) Dictionary of Military and Associated Terms, Joint Publication (JP) ۱-۰۲, Nov. ۲۰۱۰.