فصلنامه پژوهش‌های حفاظتی ـ امنیتی
دانشگاه جامع امام حسین(علیه‌السلام)

سال دهم، شمارهٔ ۳۷ (بهار ۱۴۰۰)صص۹۲-۷۳

شناسایی الزامات هوش امنیتی و رتبه‌بندی راهبردهای بهبود آن در ساختار حاکمیت [۱]

محمد مهری کارنامی
دانشجوی دکتری مدیریت رفتارسازمانی، واحدساری، دانشگاه آزاداسلامی، ساری، ایران
مسعود احمدی
استادیار گروه مدیریت دولتی، واحدساری، دانشگاه آزاداسلامی، ساری، ایران
کیومرث خطیرپاشا
استادیار گروه مدیریت آموزشی، واحدساری، دانشگاه آزاداسلامی، ساری، ایران

تاریخ دریافت: ۱۴۰۰/۰۱/۲۰ تاریخ پذیرش: ۱۴۰۰/۰۴/۱۱

چکیده

هدف این پژوهش شناسایی الزامات هوش امنیتی و رتبه‌بندی راهبردهای بهبود آن در ساختار حاکمیت، است. تحقیق حاضر از فرآیندی سه مرحله‌ای تبعیت می‌کند. بدین منظور در مرحله اول، به کمک روش نمونه‌گیری نظری، با ۱۲ نفر از صاحبنظران مصاحبه‌های نیمه ساختاریافته به عمل آمد. سپس، با کمک نرم افزار MAXQDA ، داده ها تحلیل و در طی کدگذاری باز ۴۸ مورد به عنوان مفاهیم اولیه از متن مصاحبه‌ها شناسایی شد که در قالب ۱۰ شاخص فرعی و ۲ شاخص اصلی دسته بندی شد. در بخش کمّی پژوهش، در مرحله دوم به منظور تعیین درجه اهمیت الزامات هوش امنیتی از روش آنتروپی شانون، و در مرحله سوم به منظور رتبه بندی راهبردهای مذکور، از روش ماباک، استفاده گردید. نتایج تحقیق نشان داد که الزامات تخصصی هوش امنیتی، الزامات تعاملی هوش امنیتی، الزامات مواجه با دشمن، الزامات شرعی و قانونی، الزامات فردی و خودسازی و الزامات بکارگیری هوش امنیتی، به ترتیب بالاترین درجه اهمیت را در میان الزامات هوش امنیتی، کسب کردند. همچنین، نتایج تحقیق نشان داد که بهبود زیرساخت هوش امنیتی، بهبود هوش امنیتی تاکتیکی، طراحی سامانه هوش امنیتی راهبردی و مدیریت افکار امنیتی سازمان، به ترتیب بالاترین رتبه را در میان راهبردهای بهبود هوش امنیتی ساختار حاکمیت، به خود اختصاص دادند.

کلید واژگان: *امنیت، هوش امنیتی، راهبرد، ساختار حاکمیت*

۱. این مقاله برگرفته ازرساله دکتری با عنوان"طراحی وتبیین مدل هوش امنیتی مدیران ارشد حاکمیت"می باشد

مقدمه

بحث درباره امنیت، دشواری‌های متنوعی دارد که ازجمله می‌شود به معنای امنیت و مرزهای نامعلوم آن در مفاهیمی همچون امنیت جامعه، امنیت جمعی، امنیت انسانی، امنیت ملی، امنیت سازمانی و... اشاره نمود. برخلاف گذشته که امنیت، امر عینی و واقعی بود، امروزه مفهوم امنیت بیشتر ذهنی و مبتنی بر تصمیم بازیگران است (فام و دیگران،[1] ۲۰۱۹).در این بین، تهدیدهای امنیتی می‌توانند ثبات سازمان‌ها را با تأثیرگذاری بر محرمانه‌بودن، یکپارچگی و دردسترس‌بودن سرمایه اطلاعاتی/ ساختاری، مختل کنند. نمونه‌هایی از این پتانسیلِ ایجاد اختلال و اثرات خارجی، شامل سقوط سازمانی تا ناتوان‌ساختن زیرساخت‌های کشورهاست (کیسر،[2] ۲۰۱۵). در همین رابطه و هنگام بحث درباره تأثیرات امنیت، مدیران سازمان‌ها با توجه به نقش دوگانه توسعه‌دهندگان فنّاوری و تسهیل‌کنندگان استفاده از آن، خود را به‌عنوان محورهای اصلی همه اقدامات معرفی می‌کنند. این در حالی است که امنیت در اکثر سازمان‌ها، به‌عنوان کاری درجه دو (کم‌اهمیت) باقی مانده است؛ زیرا محدودیت‌هایی در راستای علل وجودی سازمان، یعنی کسب درآمد یا خلق ارزش، ایجاد می‌کند (سالوس و دیگران،[3] ۲۰۱۹). از سویی دیگر، مزیت بهره‌برداری از حوزه‌های سایبری، ایجاد توانمندی بدیع در کسب‌وکارها برای کنترل محدودیت‌های نسبیِ زمانی و جغرافیایی، به‌عنوان توانمندسازهای سازمانی است. با این حال، یک اثر جانبی فزاینده از این اعتماد، در حوزه آسیب‌پذیری ناشی از آن نهفته است (کیسر، ۲۰۱۵). عصر اطلاعات و چالش‌های فراروی آن، فرصت‌ها و تهدیدات جدیدی را مطرح کرده است که فقط سازمان‌ها، با مدیرانِ دارای تفکر مؤثر امنیتی، قادر هستند نقاط قوت و ضعف و فرصت‌های محیطی را شناسایی و به تهدیدات پیرامونی پاسخی قاطع دهند (میرزایی، ۱۳۹۵). از همین روی، مدیریت یک سازمان، جهت انطباق با تغییرات و به‌منظور بقا و رشد در محیط‌های جدید، ویژگی‌های خاصی را می‌طلبد. یکی از خصیصه‌های مهم که به رهبران و مدیران، در پاسخ به این تغییرات و مقابله با تهدیدها و آسیب‌های سازمانی کمک می‌کند، بهره‌گیری از رویکرد امنیتی در رهبری سازمانی است (خدادادی و حسن‌پور، ۱۳۹۲). لذا بینش (هوش) امنیتی و اطلاعاتی، رخدادها و داده‌های گزارش‌شده را شناسایی و رصد کرده و بین آن‌ها ارتباط برقرار نموده و از این طریق، تهدیدها و آسیب‌ها را شناسایی می‌کند و تحت کنترل

1.Pham et al
2.Kaiser
3.Sallos et al

اطلاعاتی و امنیتی درمی‌آورد (رضایت و مرادیان، ۱۳۹۵).پیرک و دیگران[1] (۲۰۱۶)، هوش امنیتی را چنین تعریف کرده‌اند: «جمع‌آوری، هنجارسازی، همبسته‌سازی و تحلیل بزرگ داده‌های امنیتی یک سازمان که از طریق کاربران، برنامه‌های کاربردی و زیرساخت‌ها، ایجاد شده است و روی امنیت و مدیریت مخاطرات فنّاوری اطلاعات در سازمان تأثیر می‌گذارد.» آنان معتقدند هوش امنیتی به‌دنبال مدیریت همه‌جانبه اطلاعات امنیتی در سازمان است (پیرک و دیگران، ۲۰۱۶الف). آنچه مشخص است، هوش امنیتی دو بخش مهم و اساسی را پوشش می‌دهد: ۱. بخش مربوط به مدیریت تعاملات و همبستگی فنّاوری‌های مورد استفاده در امور امنیتی سازمان؛ ۲. مدیریت یکپارچگی و همبستگی این اطلاعات (ساموناس و دیگران،[2] ۲۰۲۰).

بیان مسئله

راهبردهای امنیتی سازمان در یک سناریوی «جنگ» ادامه‌دار ریشه دارند که برخلاف «نبردهای» فردی، به‌طور قطعی نمی‌توان در آن برنده شد. به عبارت دیگر، امنیت مسئله‌ای نیست که بتوان آن را برای همیشه «حل» کرد (سالوس و دیگران، ۲۰۱۹). در این بین، ذی‌نفعان سازمانی، مانند کارکنان و مدیران، ممکن است قوانین و راهبردهای امنیتی را به‌طور متفاوت درک کنند. ادبیات موجود نشان می‌دهد که ادراک ذی‌نفعان از هوش امنیتی به موفقیت یا شکست راهبردهای سازمان، کمک می‌کند (ساموناس و دیگران، ۲۰۲۰). لذا پژوهش حاضر، با واکاوی عقاید و دیدگاه‌های صاحب‌نظران، ایجاد یک دید جامع و راهبردی در راستای تشخیص و حفاظت و مدیریت تهدیدهای امنیتی را از طریق شناسایی الزامات هوش امنیتی و رتبه‌بندی راهبردهای بهبود آن در ساختار حاکمیت، به مداقه گذاشته و بررسی می‌کند و به پرسش‌های زیر پاسخ می‌دهد:

ـ الزامات هوش امنیتی در ساختار حاکمیت کدام‌اند؟

ـ چه راهبردهایی را با چه تقدم و تأخری می‌توان در راستای بهبود هوش امنیتی در ساختار حاکمیت اتخاذ نمود؟

1. Pirc et al
2. Samonas et al

در ادامه، ابتدا به مبانی نظری و پیشینه پژوهش‌های مرتبط اشاره می‌شود. سپس روش پژوهش، شامل نوع تحقیق، جامعه و روش نمونه‌گیری بیان می‌شود و در پایان پس از ارائه یافته‌های تحقیق، نتیجه‌گیری و پیشنهادهای پژوهش ارائه می‌گردد.

مبانی نظری تحقیق

امروزه مزیت رقابتی سازمان‌ها در مقدار دانایی، هوش، شایستگی و دانش خردمندانه نیروی انسانی آن‌ها پنهان است. برای تبیین تعریفی جامع از هوش، تلاش‌هایی صورت پذیرفته که همواره با مناقشه و مشکل همراه بوده است. این امر به این دلیل است که هوش، مفهومی است انتزاعی و در حقیقت پایه محسوس فیزیکی و عینی ندارد. هوش برچسبی کلی برای مجموعه‌ای از فرایندهاست که از پاسخ‌های آشکار و رفتار افراد برداشت می‌شود (نجفی شهرضا و دیگران، ۱۳۹۹).برای اولین‌بار در اوایل قرن بیستم، آلفرد بینت[1] هوش ریاضی یا بهره هوشی (IQ) را به دنیا معرفی کرد. به نظر وی، هوش ریاضی زیاد تضمین‌کننده فرایند بسیار مؤثر به‌یادسپاری ارقام است (باقری و دیگران، ۱۳۹۱).

در همین رابطه، هوارد گاردنر و هاتچ[2] (۱۹۹۰) هشت شکل مختلف از دانش را ارائه نمودند که به اعتقاد وی تصویری جامع‌تر از هوش را بیان می‌کند که عبارت است از: هوش زبانی‌کلامی، منطقی‌ریاضی (اعداد و ارقام)، تصویری‌فضایی (ایجاد تصویری ذهنی از واقعیت و تغییر بی‌درنگ و آسان آن)، موسیقیایی یا آهنگینی (توانایی درک و ایجاد الگوهای آهنگینی و نواختی)، جسمانی‌حرکتی (مهارت عضلانی و حرکت جنبشی مناسب)، طبیعت‌گرا، میان‌فردی (توانایی درک دیگران و نحوه تعامل آن‌ها با یکدیگر) و در آخر، هوش درون‌فردی (توانایی درک و شناخت خویشتن) (گاردنر و هاتچ، ۱۹۹۰). گاردنر معتقد بود که با توجه به دو شکل اول، سایر توانایی‌های ذهنی بشر نادیده گرفته می‌شود و فقط بخشی از توانمندی‌های انسان مدنظر قرار می‌گیرد (گاردنر، ۲۰۰۶).

استرنبرگ و دیگران نیز به شیوه‌ای اساسی، دنیای اندازه‌گیری هوش را تکان داد و در دیدگاه سه‌گانه خود درباره هوش، سه نوع هوشمندی را به این صورت ارائه کرد: ۱. توانایی تفسیر جزءبه‌جزء؛ ۲. توانایی تجربی در راستای اندیشیدن به‌صورت خلاق؛ ۳. توانایی زمینه‌ای که فرد را به اجرای بازی مدیریت محیط قادر می‌سازد (استرنبرگ و دیگران، ۲۰۰۱). او آزمون‌هایی برای اندازه‌گیری

1.Alfred Binet
2.Gardner & Hatch

شعور، بصیرت، حل مسئله واقعی، ایجاد تصویر وسیع‌تر از اشیا و سایر امور عملی در زندگی را ایجاد کرد که در موفقیت در زندگی بسیار نزدیک هستند.

بررسی ادبیات نشان می‌دهد، از هوش تعریف واحدی به‌دست نیامده و صاحب‌نظران مختلف آن را به گونه‌های متفاوتی تعریف کرده‌اند. نمی‌توان تعریف مشخصی از هوش به‌دست آورد که همه روان‌شناسان وابسته به رویکردهای مختلف بر آن توافق داشته باشند. با این حال، عناصری از هوش وجود دارند که غالب پژوهشگران بر آن توافق دارند. این عناصر را با توجه به ادبیات، می‌توان در سه دسته تقسیم کرد (سیف، ۱۳۹۸):

ـ توانایی پرداختن به امور انتزاعی: منظور این است که افراد باهوش بیشتر با امور انتزاعی (اندیشه‌ها، نمادها، روابط، مفاهیم و اصول) سروکار دارند تا امور عینی (ابزارهای مکانیکی، فعالیت‌های احساسی)؛

ـ توانایی حل‌کردن مسائل: یعنی توانایی پرداختن به موقعیت‌های جدید، نه‌فقط دادن پاسخ‌های ازقبل‌آموخته‌شده به موقعیت‌های آشنا؛

توانایی یادگیری: به‌ویژه توانایی یادگیری انتزاعیات، ازجمله انتزاعیات موجود در کلمات و سایر نمادها و نیز توانایی استفاده از آن‌ها.

امروزه از انواع مختلف هوش در مجامع گوناگون صحبت به‌میان می‌آید؛ مانند هوش معنوی، هوش عاطفی، هوش هیجانی، هوش سیاسی، هوش اخلاقی، هوش تجاری، هوش رقابتی، هوش سازمانی، هوش مدیریتی و... . در این راستا، هوش، پیشوند بسیاری از مفاهیم مدیریتی شده است که خود نشان‌دهنده تغییر نگاه سازمان‌ها و متفکرانشان از هوش سنتی به رویکردهای نوین به این مقوله است. در ادامه و با توجه به مبحث تحقیق، به مقوله هوش امنیتی پرداخته می‌شود.

هوش امنیتی، بستری مدرن، هوشمند و کارآمد برای تأمین امنیت سیستم‌ها و بسترهای مبتنی بر اطلاعات و شبکه است که با ایجاد یک مانیتورینگ مستمر از تمامی تجهیزات و دستگاه‌ها و جمع‌آوری تمامی لاگ‌ها، کانفیگ‌ها، رویدادها و گزارش‌های اخذشده از این تجهیزات و دستگاه‌ها به‌صورت مبتنی بر عامل یا بدون عامل (مستقل)، پس از عملیات‌های نرمال‌سازی و تجزیه‌وتحلیل، گروه‌بندی و همبسته‌سازی، اضافه‌کردن اطلاعات زمینه، اولویت‌بندی بر اساس میزان مخرب‌بودن، به‌طور خودکار تهدیدها و ریسک‌های امنیتی را تشخیص و از بروز حملات جلوگیری می‌نماید (مانوگران

و دیگران،[1] ۲۰۱۷). به‌طور خلاصه می‌توان گفت هوش امنیتی چنین است: جمع‌آوری، هنجارسازی، همبسته‌سازی و تحلیل بزرگ داده‌های امنیتی یک شبکه به‌منظور خودکارکردن فرایندهای کاهش سطح مخاطرات آن شبکه با تبدیل میلیون‌ها بسته اطلاعاتی به یک اقدام عملی آنی (کرمپ،[2] ۲۰۱۵). ادبیات موجود نشان می‌دهد که هوش امنیتی دارای سه جز اصلی ۱. مدیریت اطلاعات و رخدادهای امنیتی؛[3] ۲. مدیریت ریسک[4] و ۳. انطباق قوانین[5] است(پیرک و دیگران،[6] ۲۰۱۶ب):

مدیریت اطلاعات و رخدادهای امنیتی: به‌عنوان قلب هوش امنیتی به‌شمار می‌آید؛ زیرا زیرساخت اصلی هوش امنیتی توسط این بخش تأمین می‌گردد و از دو بخش مدیریت اطلاعات امنیتی و مدیریت رخدادهای امنیتی تشکیل شده است. مهم‌ترین وظایف بخش مدیریت اطلاعات و رخدادهای امنیتی عبارت است از مدیریت لاگ[7] یا نگاشت، نرمال‌سازی[8] یا هنجارسازی، همبسته‌سازی رویدادها،[9] عکس‌العمل آنی به تهدیدها (پاسخ فعال)[10]، امنیت عناصر انتهایی (EPP)،[11] ذخیره‌سازی وقایع[12] و ارائه گزارش‌های تحت وب.[13]

مدیریت ریسک: هدف مدیریت ریسک یا مدیریت مخاطرات در هوش امنیتی، کاهش زیان‌های ناشی از عملی‌شدن تهدیدهاست که با استفاده از سه شاخص شناسایی، ارزیابی و اولویت‌گذاری و بر مبنای استاندارد مدیریت ریسک در پنج گام می‌شود به این هدف رسید. این پنج گام عبارت است از: ۱. تشخیص و شناسایی تهدیدات؛ ۲. ارزیابی آسیب‌پذیرهای هدف تهدیدات؛ ۳. تشخیص زیان‌های ناشی از عملی‌شدن تهدیدات؛ ۴. تعیین راهکارهای کاهش مخاطرات؛ ۵. اولویت‌گذاری راهکارها.

انطباق قوانین: هدف انطباق قوانین در هوش امنیتی، حصول اطمینان از برقراری این سه مورد است: تطابق با استانداردها (استفاده از استانداردها در پیاده‌سازی هوش امنیتی، همچون استفاده از استاندارد ISO 50772 در پیاده‌سازی مدیریت ریسک در هوش امنیتی)؛ پایداری در نظارت (نظارت

1. Manogaran et al
2.Crump
3.Security Information and Event Management
4.Risk Management
5.Regulatory Compliance
6.Pirc et al
7.Log
8.Normalization
9.Event Correlation
10. Active Response
11.Endpoint Protection Platform
12.Event/Incident Storage
13. Web-based Reports

و مانیتورینگ مستمر و دائمی هوش امنیتی بر کلیه فعالیت‌ها و رویدادها)؛ کامل‌بودن بازرسی (بررسی همه‌جانبه و تجزیه‌وتحلیل کامل کلیه فعالیت‌ها و رویدادها توسط هوش امنیتی).

سه جزء تشکیل‌دهنده هوش امنیتی، شامل مدیریت اطلاعات و رخدادهای امنیتی، مدیریت ریسک و انطباق قوانین، بر مبنای سه اصل هوش، یکپارچگی و خودکارسازی با هم در تعامل بوده تا هدف اصلی هوش امنیتی تحقق یابد که تأمین امنیت است. هوش امنیتی با ایجاد مانیتورینگ و نظارت مستمر و دائمی بر کلیه فعالیت‌ها و رویدادهای سازمان مربوطه و بررسی و تجزیه‌وتحلیل این فعالیت‌ها و رویدادها هر گونه ناهنجاری و تهدید را شناسایی و از بروز حملات امنیتی جلوگیری می‌نماید (پیرک و دیگران، ۲۰۱۶ب).بررسی پیشینه تحقیق نشان داد که به‌طور کلی، مطالعات متعددی پیرامون هوش و انواع مختلف آن به‌طور جداگانه صورت گرفته است؛ ولی تحقیقات انجام‌شده در رابطه با هوش امنیتی مدیران، بسیار ناچیز بوده و پژوهشگران تاکنون به آن توجه نکرده‌اند. لذا تحقیق حاضر، این شکاف تحقیقاتی خاص در ادبیات را بررسی می‌کند.

روش تحقیق

تحقیق حاضر به‌لحاظ هدف، کاربردی، به‌لحاظ روش استنتاج، توصیفی‌پیمایشی و به‌لحاظ ماهیت داده‌ها، کیفی و کمّی است. همچنین از فرایندی سه مرحله‌ای تبعیت می‌کند:

۱. در وهله نخست، پس از مطالعه کتابخانه‌ای، الزامات هوش امنیتی و همچنین راهبردهای بهبود آن در ساختار حاکمیت شناسایی شد. در نوشتار حاضر به‌منظور جمع‌آوری داده‌ها و اطلاعات برای تجزیه‌وتحلیل بخش اکتشافی، از مصاحبه نیمه‌ساختاریافته و سؤالات اصلی زیر استفاده شد:

ـ الزامات هوش امنیتی در ساختار حاکمیت کدام‌اند؟

ـ چه راهبردهایی می‌توان در راستای بهبود هوش امنیتی در ساختار حاکمیت اتخاذ نمود؟

جامعه آماری این تحقیق را اعضای هیئت‌علمی دانشکده و پژوهشکده امنیت و مدیران و کارشناسان فعال در زمینه امنیت و اطلاعات در سازمان‌های نظامی و انتظامی کشور تشکیل دادند. با توجه به حاکمیت رویکرد کیفی در این بخش، از روش نمونه‌گیری نظری استفاده شد که یکی از روش‌های نمونه‌گیری هدفمند متوالی یا متواتر است. در نمونه‌گیری نظری، نمونه‌ها به‌شکلی انتخاب می‌شوند که به خلق تئوری کمک کنند. به عبارت دیگر، پژوهشگر از طیف افراد بالقوه برای مشاهده، کسانی را انتخاب می‌کند که بتوانند در فرایند گردآوری، خزانه داده‌های مورد نیاز را

غنی نمایند تا امکانِ ساختن نظریه فراهم شود. در این روش به‌جای انتخاب یک نمونه ثابت، حجم نمونه آن‌قدر افزایش می‌یابد تا زمانی که دیگر کافی باشد (اشباع نظری) (بازرگان هرندی و دیگران، ۱۳۹۷). بر همین اساس، بعد از انجام ۹ مصاحبه، دیده شد که عوامل اصلی و فرعی در مصاحبه‌ها تکرار شده و پاسخ‌ها از روندی تکراری تبعیت می‌کنند. با این حال، برای اطمینان بیشتر، علاوه بر تحلیل ۵ منبع به‌صورت کتابخانه‌ای، ۳ مصاحبه دیگر نیز انجام شد و نمونه با ۱۲ نفر مورد تأیید قرار گرفت و به فرایند مصاحبه پایان داده شد و پژوهشگر به اشباع نظری رسید. پس از به نوشتار درآوردن صوت مصاحبه‌ها، یافته‌های تحقیق در نرم‌افزار MAXQDA کدگذاری و مقوله‌بندی شد و سپس به تحلیل گذاشته شد.

۲. در مرحله دوم، به‌منظور تعیین درجه اهمیت الزامات هوش امنیتی، از روش آنتروپی شانون[1] استفاده شد. در اکثر مسائل تصمیم‌گیری، چندمعیاره‌دانستن وزن عناصر بسیار مهم است. تکنیک آنتروپی شانون یکی از روش‌هایی است که از آن برای تعیین وزن عناصر استفاده می‌شود. در این تکنیک وزن عناصر بر اساس میزان پراکندگی مقادیر عنصر تعیین می‌شود. روش مذکور اولین‌بار توسط استفان بولتزمن مطرح و در نهایت توسط شانن[2] (۱۹۴۸) به‌صورت کمّی ارائه شد. آنتروپی در حقیقت بیانگر آن است که چگونه از بین عوامل مؤثر یک هدف می‌توان مهم‌ترین عوامل را تخمین زد. به عبارتی، متغیرهایی را مشخص می‌کند که بیشترین تأثیر را در رخداد یک واقعیت دارند.

۳. در مرحله سوم به‌منظور رتبه‌بندی راهبردهای بهبود هوش امنیتی در ساختار حاکمیت از روش ماباک (MABAC) استفاده شده است. روش ماباک از جدیدترین تکنیک‌های تصمیم‌گیری چندمعیاره است که از آن برای رتبه‌بندی گزینه‌ها در مدل‌های تصمیم‌گیری چندمعیاره استفاده می‌شود. این روش اولین‌بار از سوی پاموکار و سیروویچ[3] (۲۰۱۵) ارائه شد. مزایای استفاده از روش ماباک چنین است: ۱. دستگاه ریاضی ساده و نتایج پایدار دارد؛ ۲. با این روش می‌شود نتایج کاملی را به‌راحتی به‌دست آورد؛ زیرا ارزش‌های احتمالی سود و ضرر را در نظر می‌گیرد؛ ۳. ترکیب این روش با رویکردهای دیگر امکان‌پذیر است. از این رو، روش ماباک این توانایی را دارد که نیازهای یک ابزار اولویت‌بندی معتبر را برآورده سازد.

1.Shanon Entropy
2.Shannon
3.Pamucar & cirovic

جامعه آماری و روش نمونه‌گیری در مراحل دوم و سوم به‌دلیل خبره‌محوربودن، همانند بخش کیفی است. بر این اساس، افرادی که در مرحله کیفی مشارکت داشتند، پرسشنامه این دو مرحله را تکمیل کردند.

یافته‌های تحقیق

مرحله اول: شناسایی الزامات هوش امنیتی و راهبردهای بهبود آن در ساختار حاکمیت

در این بخش از تحقیق، نتایج حاصل از کدگذاری اولیه یا کدگذاری باز و محوری ارائه می‌شود. بر این اساس، پس از به نوشتار درآمدن صوت مصاحبه‌ها، کدگذاری روایت‌های آنان در سه سطح مفاهیم، عوامل و مقوله‌های اصلی انجام گرفت. کدگذاری در مرحله اول با توجه به کلی‌بودن و بازبودن، کدگذاری اولیه محسوب می‌شود (مفاهیم). در مرحله بعد، می‌بایست کدگذاری ثانویه انجام گیرد که در آن کدهای اولیه به‌علت تعداد فراوان در قالب طبقه‌های مشابه یا همان کدهای ثانویه، به کد مفهومی تبدیل می‌شوند (عوامل). در انتها نیز با کدگذاری انتخابی، الزامات هوش امنیتی و همچنین راهبردهای بهبود آن در ساختار حاکمیت (مقوله‌ها)، تعیین می‌گردد. گفتنی است که به‌منظور اعتبارسنجی نتایج بخش کیفی در این مطالعه، از روش کنترل اعضا (محققان یافته‌های خود را با چهار نفر از افراد مطلع تحت بررسی کنترل نموده و تفاسیر پژوهشگر به تأیید رسیده است) استفاده شده است.

در ادامه، خلاصه تحلیل مصاحبه‌ها در جدول ۱ بیان شده است:

جدول ۱: کدگذاری مصاحبه‌ها و استخراج الزامات هوش امنیتی و راهبردهای بهبود آن در ساختار حاکمیت

مقوله‌ها	شاخص‌ها	علامت	مفاهیم (اعداد داخل پرانتز نشان‌دهنده شماره مصاحبه‌شونده است)
الزامات هوش امنیتی	الزامات تخصصی هوش امنیتی	C1	ارتقای آموزش‌های تخصصی فنّاوری اطلاعات (۳)، بومی‌سازی دانش ساخت ابزارهای فنی در داخل (٤)، آموزش تخصصی امنیتی و آگاه‌سازی حفاظتی (۷)، به‌کارگیری عوامل اجرایی متخصص (۱۰)
	الزامات تعاملی هوش امنیتی	C۲	انتقال تجربیات موفق به همکاران (۲)، تعامل دستگاه‌های اطلاعاتی (۷)، گزارش‌دهی اطلاعاتی (۱۰)، عدم پنهان‌کاری مفرط در مناسبات حساس سازمان (۱۱)، رعایت سلسله‌مراتب سازمانی (۱۲)

الزامات هوش امنیتی	الزامات به‌کارگیری هوش امنیتی	C۳	مشورت امنیتی در قراردادها و... (۱)، پیش‌بینی آسیب و تهدیدات امنیتی (۳)، احصاء سیاست امنیتی در خط‌مشی‌گذاری‌ها (٦)، مسئولیت‌پذیری امنیتی (۸)، ضرورت نظارت و کنترل امنیتی (۹)، ایجاد بازدارندگی مؤثر امنیتی (۱۱)
	الزامات مواجهه با دشمن	C۴	هوشیاری در مقابل تهدیدهای دشمن (۳)، رویکرد تهاجم اطلاعاتی در مقابل دشمن (٤)، بی‌اعتبارساختن دشمن (٥)، شناخت راهکارهای دشمن (۷)، ضرورت شناخت اطلاعاتی دشمن (۱۰)، شناخت ظرفیت امنیتی دشمن (۱۲)
	الزامات شرعی و قانونی	C5	رعایت موازین شرعی (۱)، توجه به انضباط معنوی (٤)، تعهد به ارزش‌های اخلاقی و قانونی (٥)، پیروی از ولایت فقیه (۹)
	الزامات فردی و خودسازی	C۶	مراقبت از نفس (۲)، اتصال به مبدأ هستی (٥)، قابلیت مواجهه با مشکلات و ناملایمات (٦)، مستقل‌بودن (شهامت) (۱۲)
راهبردهای بهبود هوش امنیتی	مدیریت افکار امنیتی سازمان	A1	اعتمادسازی کارکنان (۳)، قدرت اقناع‌سازی مدیران (٥)، شناخت نگرش مخاطبان (۷)، رفع تضادهای امنیتی سازمانی (۸)، اثرگذاری امنیتی در حفاظت روانی کارکنان (۹)، آگاه‌سازی حفاظتی در مجموعه سازمان (۱۰)
	طراحی سامانه هوش امنیتی راهبردی	A۲	طراحی نرم‌افزارهای بومی و سطح بالای امنیتی در سازمان (۱)، طراحی سیستم بهنگام شناسایی رخداد سایبری (٦)، طراحی راهکار مقابله با نفوذ در سازمان‌ها (۹)، طراحی سیستم پیش‌بینی تغییر مخاطرات (۱۱)
	بهبود هوش امنیتی تاکتیکی	A۳	بهبود مدیریت شبکه (۷)، ایجاد نوآوری در تاکتیک‌های امنیتی (۹)، ارتقای دانش مدیران امنیتی (۱۱)، زمان‌شناسی بحران سازمانی (۱۲)
	بهبود زیرساخت هوش امنیتی	A۴	ارتقای سخت‌افزاری ابزارهای مقابله با نفوذ (۱)، بهینه‌سازی سخت‌افزاری و نرم‌افزاری مقابله با بدافزارهای بومی (٦)، بهبود زیرساخت سیستم پایش شبکه (۸)، ارتقا و بهبود سرورهای کنترل (۱۰)، ایجاد مرکز عملیات یکپارچه (۱۱)

مرحله دوم: تعیین درجه اهمیت الزامات هوش امنیتی

همان‌گونه که بیان شد، در راستای تعیین درجه اهمیت الزامات هوش امنیتی در ساختار حاکمیت، از روش آنتروپی شانون استفاده شد. بر همین اساس، پس از کسب نظر خبرگان (۱۲ نفر) و تحلیل محتوای پنج منبع به‌صورت کتابخانه‌ای به‌کمک پرسشنامه و جمع‌بندی نظرات، گام‌های زیر به‌منظور تجزیه‌وتحلیل داده‌ها انجام شد:

گام اول، تشکیل ماتریس تصمیم: در این پژوهش از طیف لیکرت پنج درجه‌ای (خیلی کم، کم، متوسط، زیاد، خیلی زیاد) برای ارزیابی استفاده شد. با توجه به میانگین نظر خبرگان، ماتریس تصمیم تشکیل گردید. برای تشکیل این ماتریس کافی‌ست چنین عمل نمود: اگر معیارها کیفی هستند از عبارات کلامی، ارزیابی هر گزینه را نسبت به هر معیار به‌دست آورد و اگر معیارها کمّی هستند، عدد واقعی آن ارزیابی را قرار داد. در ماتریس تصمیم پژوهش حاضر، معیارها عبارت‌اند از: الزامات هوش امنیتی و گزینه‌ها؛ راهبردهای بهبود هوش امنیتی در ساختار حاکمیت.

گام دوم، نرمالایز ماتریس تصمیم: در این گام، ماتریس تصمیم را نرمال می‌کنیم و هر درایه نرمال‌شده را p_{ij} می‌نامیم. نرمال‌شدن به این صورت است که درایه هر ستون را بر مجموع ستون تقسیم می‌کنیم. نتایج محاسبات گام اول و دوم در جدول ۲ نشان داده شده است:

جدول ۲: ماتریس تصمیم‌گیری نرمال‌شده (بی‌مقیاس‌شده)

	C۱	C۲	C۳	C۴	C۵	C۶
A۱	۰,۱۹۴	۰,۲۳۰	۰,۲۴۴	۰,۲۱۶	۰,۲۸۰	۰,۲۶۰
A۲	۰,۲۱۷	۰,۲۱۳	۰,۲۲۹	۰,۲۳۷	۰,۲۱۹	۰,۲۲۵
A۳	۰,۲۷۷	۰,۲۵۵	۰,۲۵۶	۰,۲۵۳	۰,۲۵۰	۰,۲۶۵
A۴	۰,۳۱۲	۰,۳۰۱	۰,۲۷۰	۰,۲۹۴	۰,۲۵۰	۰,۲۴۹

گام سوم، محاسبه آنتروپی هر شاخص: آنتروپی Ej به‌صورت زیر محاسبه می‌گردد و k به‌عنوان مقدار ثابت مقدار E_j را بین ۰ و ۱ نگه می‌دارد.

$$E_j = -k\sum_{i=1}^{m} P_{ij} \times Ln\, P_{ij} \;\; , k = \frac{1}{\ln m} \;\; , \;\; i = 1.2. \ldots . m$$

جدول ۳: محاسبه $(-kP_{ij} \times Ln\ P_{ij})$

	C۱	C۲	C۳	C۴	C۵	C۶
A۱	۰,۲۲۹	۰,۲۴۴	۰,۲۴۸	۰,۲۳۹	۰,۲۵۷	۰,۲۵۳
A۲	۰,۲۳۹	۰,۲۳۸	۰,۲۴۳	۰,۲۴۶	۰,۲۴۰	۰,۲۴۲
A۳	۰,۲۵۷	۰,۲۵۱	۰,۲۵۲	۰,۲۵۱	۰,۲۵۰	۰,۲۵۴
A۴	۰,۲۶۲	۰,۲۶۱	۰,۲۵۵	۰,۲۶۰	۰,۲۵۰	۰,۲۵۰

گفتنی است که افزایش در آنتروپی شانون باعث افزایش عدم اطمینان و کاهش اطلاعات در مورد دانش متغیر تصادفی می‌شود. جنبه جالب دیگر آنتروپی شانون ویژگی حداکثر آنتروپی آن برای توزیع یکنواخت است.

گام چهارم، محاسبه فاصله هر شاخص از آنتروپی آن (تعیین درجه انحراف): در ادامه مقدار dj (درجه انحراف) محاسبه می‌شود (E_j-۱=d_j) که بیان می‌کند شاخص مربوطه (dj) چه میزان اطلاعات مفید برای تصمیم‌گیری در اختیار تصمیم‌گیرنده قرار می‌دهد. هرچه مقادیر اندازه‌گیری‌شده شاخصی به هم نزدیک باشند، نشان‌دهنده آن است که گزینه‌های رقیب از نظر آن شاخص تفاوت چندانی با یکدیگر ندارند. لذا نقش آن شاخص در تصمیم‌گیری باید به همان اندازه کاهش یابد.

گام پنجم، تعیین وزن هر شاخص: سپس مقدار وزن Wj محاسبه می‌گردد. در واقع، وزن معیار برابر با هر dj تقسیم بر مجموعdj ها ($w_j=d_j/\sum d_j$) است. نتایج محاسبات گام چهارم و پنجم در جدول ۴ نشان داده شده است:

جدول ۴: محاسبه آنتروپی هر شاخص، درجه انحراف، وزن و رتبه هر شاخص

شاخص‌ها	C۱	C۲	C۳	C۴	C۵	C۶
آنتروپی هر شاخص (Ej)	۰,۹۸۷	۰,۹۹۴	۰,۹۹۹	۰,۹۹۵	۰,۹۹۷	۰,۹۹۹
درجه انحراف هر شاخص (Dj)	۰,۰۱۳	۰,۰۰۶	۰,۰۰۱	۰,۰۰۵	۰,۰۰۳	۰,۰۰۱
وزن هر شاخص (Wj)	۰,۴۳۹	۰,۲۱۳	۰,۰۴۷	۰,۱۶۱	۰,۰۹۳	۰,۰۴۷
رتبه هر شاخص	۱	۲	۶	۳	۴	۵

با توجه به نتایج این بخش، جدول ۴، الزامات تخصصی هوش امنیتی (C1)، الزامات تعاملی هوش امنیتی (C۲)، الزامات مواجهه با دشمن (C۴)، الزامات شرعی و قانونی (C۵)، الزامات فردی و

خودسازی (C6) و الزامات به‌کارگیری هوش امنیتی (C۳)، به ترتیب بالاترین درجه اهمیت را در میان الزامات هوش امنیتی ساختار حاکمیت کسب کردند.

مرحله سوم: رتبه‌بندی راهبردهای بهبود هوش امنیتی در ساختار حاکمیت

در این بخش از تحقیق، به‌منظور رتبه‌بندی راهبردهای بهبود هوش امنیتی در سازمان‌های دولتی، از روش ماباک استفاده شد. بر همین اساس، پس از کسب نظر خبرگان (۱۲ نفر) به‌کمک پرسشنامه و جمع‌بندی نظرات، گام‌های زیر در راستای تجزیه‌وتحلیل داده‌ها انجام شد:

گام اول، تشکیل ماتریس اولیه تصمیم (X): در این گام فرض می‌شود تعداد m گزینه و n معیار موجود است. هر یک از گزینه‌ها به شکل برداری و به صورت Aij= (xi1,xi2,…,xin) نمایش داده می‌شوند که xij وضعیت گزینه iام در معیار jام را مشخص می‌نماید. بر این اساس، ماتریس تصمیم اولیه همان ماتریس مرحله قبل (آنتروپی شانون) است. همچنین xij درایه‌های ماتریس اولیه تصمیم (X) بوده و xi− و xi+ به‌صورت زیر تعریف می‌شوند:

$x_i^+ = \max(x_1 . x_2 . \dots x_m)$: نشان‌دهنده بیشترین مقداری است که در یک معیار مشخص، در میان گزینه‌ها مشاهده شده است.

$x_i^- = \min(x_1 . x_2 . \dots x_m)$:نشان‌دهنده کمترین مقداری است که در یک معیار مشخص، در میان گزینه‌ها مشاهده شده است.

نتایج محاسبات گام اول در جدول ۵ نشان داده شده است.

جدول ۵: ماتریس اولیه (میانگین نظر پاسخ‌دهندگان)

	C۱	C۲	C۳	C۴	C۵	C۶
A۱	۲,۲۶۲	۳,۰۳۳	۳,۳۵۷	۲,۹۵۲	۳,۵۹۵	۳,۴۰۵
A۲	۲,۵۳۳	۲,۸۱۰	۳,۱۴۳	۳,۲۳۸	۲,۸۱۰	۲,۹۵۲
A۳	۳,۲۳۸	۳,۳۵۷	۳,۵۲۴	۳,۴۵۲	۳,۲۱۴	۳,۴۷۶
A۴	۳,۶۴۳	۳,۹۶۷	۳,۷۱۴	۴,۰۲۴	۳,۲۱۴	۳,۲۶۲
+X	۳,۶۴۳	۳,۹۶۷	۳,۷۱۴	۴,۰۲۴	۳,۵۹۵	۳,۴۷۶
-X	۲,۲۶۲	۲,۸۱۰	۳,۱۴۳	۲,۹۵۲	۲,۸۱۰	۲,۹۵۲
W	۰,۴۳۹	۰,۲۱۳	۰,۰۴۷	۰,۱۶۱	۰,۰۹۳	۰,۰۴۷

گام دوم، نرمال‌کردن درایه‌های ماتریس تصمیم اولیه (N): به‌دلیل آنکه ممکن است جنس هر یک از معیارها متفاوت باشند، در گام دوم ماتریس تصمیم نرمال‌شده تا اثر مقیاس متفاوت معیارها خنثی شود. به‌منظور انجام این کار و با توجه به جنس هر معیار، از رابطه $n_{ij} = \frac{x_{ij} - x_i^-}{x_i^+ - x_i^-}$ برای

نرمال‌سازی معیارهای مثبت و از رابطه $n_{ij} = \frac{x_{ij}-x_i^+}{x_i^--x_i^+}$ برای نرمال‌سازی معیارهای منفی استفاده می‌شود. گفتنی است که در این تحقیق شاخص‌های چالش بین بخشی (C۷) و بار کاری (C۱۱)، به‌عنوان معیارهای منفی در نظر گرفته شدند. نتایج این گام در جدول ۶ نشان داده شده است.

جدول ۶: نرمال‌سازی ماتریس اولیه (N)

	C۱	C۲	C۳	C۴	C۵	C۶
A۱	۰,۰۰۰	۰,۵۵۹	۰,۷۹۳	۰,۵۰۰	۰,۹۶۶	۰,۸۲۸
A۲	۰,۱۹۷	۰,۳۹۷	۰,۶۳۸	۰,۷۰۷	۰,۳۹۷	۰,۵۰۰
A۳	۰,۷۰۷	۰,۷۹۳	۰,۹۱۴	۰,۸۶۲	۰,۶۹۰	۰,۸۷۹
A۴	۱,۰۰۰	۱,۲۳۴	۱,۰۵۲	۱,۲۷۶	۰,۶۹۰	۰,۷۲۴

گام سوم، تشکیل ماتریس تصمیم نرمال موزون (V): از آنجا که معیارها دارای وزن متفاوتی در فرایند ارزیابی هستند؛ در این گام می‌بایست درایه‌های ماتریس نرمال موزون بر اساس رابطه $(v_{ij} = w_i(n_{ij}+1))$ محاسبه شوند. در این رابطه، nij درایه‌های ماتریس نرمال (N) و wi وزن معیار i ام است. همچنین vij درایه‌های ماتریس موزون V را تشکیل می‌دهد. این ماتریس به‌صورت زیر تعریف می‌شود.

جدول۷: تشکیل ماتریس موزون (V)

	C۱	C۲	C۳	C۴	C۵	C۶
A۱	۰,۴۳۹	۰,۳۳۲	۰,۰۸۴	۰,۲۴۲	۰,۱۸۳	۰,۰۸۷
A۲	۰,۵۲۵	۰,۲۹۷	۰,۰۷۶	۰,۲۷۵	۰,۱۳۰	۰,۰۷۱
A۳	۰,۷۴۹	۰,۳۸۱	۰,۰۸۹	۰,۳۰۰	۰,۱۵۸	۰,۰۸۹
A۴	۰,۸۷۷	۰,۴۷۵	۰,۰۹۶	۰,۳۶۷	۰,۱۵۸	۰,۰۸۲

گام چهارم، مشخص‌کردن ماتریس مرز تخمین ناحیه (G): مرز تخمین ناحیه برای هر معیار به شکل رابطه $g_i = \left(\prod_{j=1}^{m} v_{ij}\right)^{1/m}$ محاسبه می‌شود. بعد از محاسبه gi برای هر معیار، ماتریس مرز تخمین ناحیه که با G نشان داده می‌شود، تشکیل می‌گردد که در جدول ۸ نشان داده شده است.

جدول ۸: ماتریس مرز تخمین ناحیه (میانگین هندسی هر ستون از ماتریس موزون)

	C۱	C۲	C۳	C۴	C۵	C۶
gi	۳,۷۸۹	۱,۷۴۱	۰,۲۲۵	۱,۲۶۸	۰,۵۲۲	۰,۲۱۰

گام پنجم، محاسبه فاصله گزینه‌ها از مرز تخمین ناحیه (Q): فاصله گزینه‌ها از مرز تخمین ناحیه

مطابق رابطه $Q = V - G$ برابر اختلاف میان درایه‌های ماتریس وزن‌دار (V) و مقدار مرز تخمین ناحیه (G) تعیین می‌شود. پس از مشخص‌شدن مقدار ماتریس Q، می‌توان با تعریف بردار تخمین مساحت (G)، حد بالای مساحت (+G) و حد پایین مساحت (−G) وضعیت هر گزینه را مشخص نمود. بر این اساس، گزینه Ai متعلق به اجتماع مجموعه مذکور است. نواحی مذکور در شکل ۱ نشان داده شده‌اند. در این تعریف، حد بالای تخمین مساحت (+G)، منطقه‌ای است که گزینه ایدئال (+A) در آن منطقه حضور داشته و حد پایین تخمین مساحت (−G) منطقه‌ای است که گزینه ضد ایدآل (−A) در آنجا وجود دارد. میزان تعلق گزینه Ai به اجتماع مذکور، بر اساس رابطه زیر به‌دست می‌آید.

$$A_i \in \begin{cases} G^+ q_{ij} > 0 \\ G q_{ij} = 0 \\ G^- q_{ij} < 0 \end{cases}$$

بر مبنای منطق روش ماباک برای اینکه گزینه Ai بهترین گزینه در مجموعه گزینه‌ها باشد، لازم است تا نسبت به دیگر گزینه‌ها به حد بالای تخمین منطقه‌ای (+G) نزدیک‌تر باشد. به عبارت دیگر، اگر مقدار qij>۰ باشد، بنابراین گزینه Ai نزدیک یا برابر گزینه ایدئال خواهد بود. همین مسئله به صورت معکوس و برای شرایط qij<۰ نیز وجود دارد. به گونه‌ای که اگر qij<۰ باشد، بنابراین گزینه Ai نزدیک یا برابر گزینه ضد ایدئال است. نتایج این گام در جدول ۹ نشان داده شده است.

جدول ۹: محاسبه فاصله گزینه‌ها از مرز تخمین (Q)

	C۱	C۲	C۳	C۴	C۵	C۶
A۱	۳,۳۵۱-	۱,۴۰۹-	۰,۱۴۲-	۱,۰۲۶-	۰,۳۳۹-	۰,۱۲۴-
A۲	۳,۲۶۵-	۱,۴۴۳-	۰,۱۴۹-	۰,۹۹۲-	۰,۳۹۲-	۰,۱۳۹-
A۳	۳,۰۴۱-	۱,۳۵۹-	۰,۱۳۶-	۰,۹۶۷-	۰,۳۶۵-	۰,۱۲۱-
A۴	۲,۹۱۲-	۱,۲۶۵-	۰,۱۳۰-	۰,۹۰۱-	۰,۳۶۵-	۰,۱۲۹-

گام ششم، رتبه‌بندی گزینه‌ها: در آخرین گام از روش ماباک، مقدار توابع معیارها بر اساس مجموع فواصل گزینه‌ها از بردار تخمین مساحت (qi) برای هر کدام، مطابق رابطه $S_i = \sum_{j=1}^{n} q_{ij}$، محاسبه می‌شود. با محاسبه مجموع درایه‌های ماتریس Q به‌صورت سطری، مقدار نهایی توابع معیار برای هر گزینه مشخص شده و مبنای رتبه‌بندی گزینه‌ها قرار می‌گیرد.

جدول ۱۰: رتبه‌بندی گزینه‌ها

رتبه	گزینه‌ها		si
۱	بهبود زیرساخت هوش امنیتی	A4	۵,۷۰۱-
۲	بهبود هوش امنیتی تاکتیکی	A۳	۵,۹۸۹-
۳	طراحی سامانه هوش امنیتی راهبردی	A2	۶,۳۸۰-
۴	مدیریت افکار امنیتی سازمان	A1	۶,۳۹۰-

نتیجه‌گیری و پیشنهادها

امنیت از نیازهای فطری بشر و گرایش به امنیت پایدار، یکی از نیازهای عالی انسانی است که تحقق آن نیازمند محیطی است که بتواند به دور از فشارهای گروهی و در مسیر رشد قرار گیرد. بنابراین آسودگی زیستن به سازوکارهای متعدد و گوناگونی نیاز دارد که سرلوحه آن‌ها، امنیت است. امنیت در گذشته در پرتو قدرت نظامی تحقق می‌یافت؛ ولی امروزه با تحولی که در فنّاوری ارتباطات و اطلاعات به‌وجود آمده، در ابعاد گسترده‌تری اهمیت یافته و احساس ضرورت آن نه‌تنها در ابعاد مادی، بلکه در ابعاد معنوی نیز احساس می‌شود.

نیازمندی‌های نوین بشری از یک‌سو و دشواری و چالش‌های نوپدید از سوی دیگر، منجر به گسترده‌شدن مفهوم امنیت در اثر حاضر شده است. همان‌طور که در جهان واقعی، انسان‌های موفق افرادی هستند که استعدادی سرشار داشته و از هوش وافری برخوردارند، قطعاً در سازمان‌ها نیز چنین است. به‌خصوص در زمان فعلی هر چه زمان به جلو حرکت می‌کند، به‌علت پیشرفت علوم و فنون و به‌وجودآمدن اقتضائات جدید، سازمان‌ها نیز چالشی‌تر و مدیریت آن‌ها سخت‌تر می‌شود. لذا ادامه حیات سازمان‌ها متأثر از قابلیت سازگاری آن‌ها برای تبعیت از تغییرات است. در این بین، هوش امنیتی به‌دنبال مدیریت همه‌جانبه اطلاعات امنیتی در سازمان است. بخشی از این اطلاعات از طریق گزارش‌هایی که به‌صورت دستی و موردی تهیه می‌شوند، تشکیل شده است و بخش دیگری از گزارش‌ها و فعالیت‌ها نیز به‌صورت خودکار توسط سیستم‌های امنیتی مستقر در سازمان تولید می‌شوند. هوش امنیتی در واقع با به‌کارگیری مهارت‌های لازم در راستای جمع‌آوری، یکپارچه‌سازی و تحلیل تمام اطلاعات مذکور به‌دنبال مدیریت و در نهایت بهینه‌سازی و افزایش هوشمندی سازمان در امور امنیتی است.

در تحقیق حاضر به‌منظور جمع‌آوری داده‌ها و اطلاعات برای تجزیه‌وتحلیل بخش کیفی، از مصاحبه، استفاده شد. پس از به نوشتار درآمدن صوت مصاحبه‌ها، کدگذاری انجام گرفت. در طی

کدگذاری باز ۴۸ مورد به‌عنوان مفاهیم اولیه از متن مصاحبه‌های انجام‌شده به‌دست آمد که در قالب ۱۰ زیرشاخص فرعی و ۲ شاخص اصلی دسته‌بندی شد. سپس در مرحله دوم به‌منظور تعیین درجه اهمیت الزامات هوش امنیتی از روش آنتروپی شانون، استفاده شده است. بر همین اساس، پس از کسب نظر خبرگان (۱۲ نفر) و ۵ تحلیل محتوا به‌صورت کتابخانه‌ای به‌کمک پرسشنامه و جمع‌بندی نظرات، پرسشنامه‌ها تجزیه‌وتحلیل شد. در پایان، رتبه‌بندی راهبردهای بهبود هوش امنیتی در سازمان‌های دولتی، با روش ماباک انجام پذیرفت.

بر اساس یافته‌های تحقیق، بهبود زیرساخت هوش امنیتی، بهبود هوش امنیتی تاکتیکی، طراحی سیستم هوش امنیتی راهبردی و مدیریت افکار امنیتی سازمان، به ترتیب بالاترین رتبه را در میان راهبردهای بهبود هوش امنیتی در سازمان‌های دولتی کسب کردند.

در همین راستا به سازمان‌های دولتی پیشنهاد می‌شود:

ـ با ارتقا و بهینه‌سازی سخت‌افزاری و نرم‌افزاری ابزارهای مقابله با نفوذ، بهبود زیرساخت سیستم پایش شبکه، ارتقا و بهبود سِرورهای کنترل و همچنین ایجاد مرکز عملیات یکپارچه، موجبات بهبود زیرساخت هوش امنیتی را در سازمان‌های دولتی فراهم سازند.

ـ با بهبود مدیریت شبکه، ایجاد نوآوری در تاکتیک‌های امنیتی و ارتقای دانش مدیران امنیتی، بهبود هوش امنیتی تاکتیکی را در سازمان‌های دولتی مدنظر قرار دهند.

ـ با طراحی و به‌کارگیری نرم‌افزارهای بومی و سطح بالای امنیتی در سازمان، سیستم بهنگام شناسایی رخداد سایبری، طراحی راهکار مقابله با نفوذ در سازمان‌ها و طراحی سیستم پیش‌بینی مخاطرات امنیتی، سامانه جامع هوش امنیتی راهبردی را در سازمان‌های دولتی محقق سازند.

ـ با انجام سلسله اقداماتی نظیر اعتمادسازی در کارکنان، شناخت نگرش‌های متفاوت مخاطبان، رفع تضادهای امنیتی سازمانی، اثرگذاری امنیتی در حفاظت روانی کارکنان و آگاه‌سازی حفاظتی در مجموعه سازمان، مدیریت افکار امنیتی را در سازمان نهادینه کنند.

منابع و ماخذ

الف)منابع فارسی

۱. بازرگان هرندی، عباس؛ حجازی، الهه؛ سرمد، زهره، ۱۳۹۷، **روش‌های تحقیق در علوم رفتاری**، تهران: آگه.

۲. باقری، مسعود؛ نمازیان، مریم؛ امیری، آتنا، ۱۳۹۱، «**بررسی رابطه بین هوش معنوی با خلاقیت و انگیزه پیشرفت، مورد مطالعه: دانش‌آموزان متوسطه ناحیه یک کرمان**»، مقاله ارائه‌شده در اجلاس ملی کارآفرینی و مدیریت کسب‌وکارهای دانش‌بنیان.

۳. خدادادی، مجتبی؛ حسن‌پور، علی، ۱۳۹۲، «**نقش هوش هیجانی در توانمندی مدیران امنیتی**»، پژوهش‌های حفاظتی و امنیتی، ۵(۲)، ص ۹۵ تا ۱۱۰.

۴. رضایت، غلامحسین؛ مرادیان، فیض‌الله، ۱۳۹۵، «**ارائه الگوی راهبردی حفاظت‌اطلاعات اسلامی**»، دانشگاه عالی دفاع ملی، دانشکده امنیت ملی، ۶(۲۲)، ص ۶۹ تا ۹۴.

۵. سیف، علی‌اکبر، ۱۳۹۸، **روان‌شناسی پرورشی نوین: روان‌شناسی یادگیری و آموزش، دوران.**

۶. میرزایی، سعید، ۱۳۹۵، «**بررسی عوامل مؤثر بر امنیت اجتماعی شهروندان شهر جدید پرند**»، سومین اجلاس بین‌المللی پژوهش‌های نوین در علوم انسانی.

۷. نجفی شهرضا، محمدمهدی؛ احمدی، سید علی‌اکبر؛ کمانی، سید محمدحسین؛ گرامی‌پور، مسعود، ۱۳۹۹، «**طراحی و تبیین الگوی جامع هوش مدیریتی، مورد مطالعه: اداره‌کل آموزش‌وپرورش استان قم**»، پژوهش‌های مدیریت منابع انسانی، ۴۲(۱۲)، ص ۹ تا ۶۲.

ب)منابع لاتین

1.Crump, Justin. (2015). Corporate security intelligence and strategic decision making. Crc press.

2.Gardner, Howard. (2006). Intelligence reframed: Multiple intelligences for the new millennium. Basic Books.

3.Gardner, Howard; & Hatch, Thomas. (1990). Multiple Intelligences Go to School: Educational Implications of the Theory of Multiple Intelligences. Technical Report No. 4.

4.Kaiser, Robert. (2015). The birth of cyberwar. Political Geography, 46, 11-20.

5.Manogaran, Gunasekaran; Thota, Chandu; Lopez, Daphne; & Sundarasekar, Revathi. (2017). Big data security intelligence for healthcare industry 4.0. In Cybersecurity for Industry 4.0 (pp. 103-126). Springer.

6.Pamucar, Dragan; & cirovic, Goran. (2015). The selection of transport and handling resources in logistics centers using Multi-Attributive Border Approximation area Comparison (MABAC). Expert Systems with Applications, 42(6), 3016-3028. https://doi.org/10.1016/j.eswa.2014.11.057

7.Pham, Hiep Cong; Brennan, Linda; & Furnell, Steven. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. Journal of Information Security and Applications, 46, 96-107.

8. Pirc, John; DeSanto, David; Davison, Iain; & Gragido, Will. (2016a). 3 - Security Intelligence. In J. Pirc, D. DeSanto, I. Davison, & W. Gragido (eds.), (J. Pirc, D. DeSanto, I. Davison, & W. Gragido, eds.), Threat Forecasting (pp. 29-45). Syngress.

9. Pirc, John; DeSanto, David; Davison, Iain; & Gragido, Will. (2016b). Threat forecasting: Leveraging big data for predictive analysis. Syngress.

10. Sallos, Mark Paul; Garcia-Perez, Alexeis; Bedford, Denise; & Orlando, Beatrice. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital.

11. Samonas, Spyridon; Dhillon, Gurpreet; & Almusharraf, Ahlam. (2020). Stakeholder perceptions of information security policy: Analyzing personal constructs. International Journal of Information Management, 50, 144-154.

12. Shannon, Claude E. (1948). A mathematical theory of communication. The Bell system technical journal, 27(3), 379-423.

13. Sternberg, Robert J; Grigorenko, Elena L; & Bundy, Donald A. (2001). The Predictive Value of IQ. Merrill-Palmer Quarterly, 47(1), 1-1.