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

سال دهم، شمارهٔ ۳۸ (تابستان ۱۴۰۰) صص ۷۰-۳۷

# طراحی و تبیین مدل هوش امنیتی مدیران ارشد حاکمیت

● 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: ۱۴۰۱/۰۲/۳۰ تاریخ پذیرش: ۱۴۰۱/۰۴/۳۰

## چکیده

هدف این پژوهش طراحی و تبیین مدل هوش امنیتی مدیران ارشد حاکمیت است. تحقیق حاضر به لحاظ هدف؛ اکتشافی-کاربردی، به لحاظ روش استنتاج، توصیفی-پیمایشی و به لحاظ ماهیت داده‌ها، کیفی وکمی است. این تحقیق در سه مرحله اصلی انجام شده است؛ درمرحله اول، با استفاده از روش نمونه‌گیری نظری، با ۱۲ نفر از صاحب‌نظران مصاحبه‌های نیمه ساختاریافته به عمل آمد سپس با استفاده از رویکرد تئوری داده بنیاد و با کمک نرم افزار NVivo Plus2020، مصاحبه‌ها تحلیل و طی کدگذاری باز ۲۵۲ مورد به عنوان مفاهیم اولیه از متن مصاحبه‌ها شناسایی شد و در قالب ۲۲ شاخص اصلی و ۱۵۰ شاخص فرعی و در پنج بُعد دسته‌بندی شد. در مرحله پژوهش کمی مدل پس ازآزمون، تأیید گردید. در مرحله دوم بخش کمی تحقیق، جامعه آماری ۲۸۰ نفر بوده، که حجم نمونه آن براساس فرمول کوکران به تعداد ۱۶۲ نفر برآورد گردیده و پرسشنامه‌ها به‌صورت طبقه‌ای نسبی چند مرحله‌ای و تصادفی توزیع شده است. درمرحله سوم پس از تکمیل پرسشنامه ازطریق الگوریتم تحلیل داده‌ها در نرم افزار *PLS*، تجزیه و تحلیل شدند. نتایج تحقیق کیفی نشان داد مدل در ابعاد شرایط علی (۴ شاخص اصلی و۳۲ شاخص فرعی)، شرایط مداخله‌گر(۷ شاخص اصلی و۴۶ شاخص فرعی)، شرایط زمینه‌ای( ۳ شاخص اصلی و ۲۰ شاخص فرعی)، شرایط راهبردی( ۵ شاخص اصلی و ۲۶ شاخص فرعی) و شرایط پیامدی با(۳ شاخص اصلی و۲۵ شاخص فرعی)مورد بررسی قرارگرفته است. همچنین با توجه به نتایج مدل اندازه‌گیری و ساختاری، تحقیق کمی می‌توان نتیجه گرفت که مدل تدوین شده در بخش کیفي از روايي و پايايي قابل قبولي برخوردار است و مي‌تواند به عنوان يك مدل قابل اعتماد براي تبيين مدل هوش امنیتی مدیران ارشد حاکمیت، به‌کارگرفته شود.

**کلید واژگان:** هوش، امنیت، هوش امنیتی، مدیران ارشد، حاکمیت

* این مقاله برگرفته از رساله دکتری با عنوان«طراحی و تبیین مدل هوش امنیتی مدیران ارشد حاکمیت» می‌باشد.

## مقدمه

در حرکت از عصر صنعتی به عصر اطلاعات و با جابه‌جایی مؤلفه‌های قدرت، تغییر سیمای کنونی مرزهای جغرافیایی، فرقه‌ای و قومی، ظهور تهدیدات جدید، استفاده نادرست از فناوری‌های نوین و... ارکان اولیه واقعیت‌های سازمانی را آن‌چنان دگرگون نموده که ممکن است ثبات با هزینه اندک به دست نیاید و یا حتی با هیچ هزینه‌ای نتوان به آن دست یافت (کمیسیون تدوین استراتژی امنیت ملی آمریکا (118:1383) در این فضای به شدت پیچیده و متلاطم، افراد، سازمانها و ملتها در معرض هجوم تغییراتی بیش ازاندازه و خیلی سریع قرار گرفته اند که باعث آشفتگی و از دست دادن ظرفیت آنها برای اتخاذ تصمیمهای هوشمندانه و انطباق پذیر شده است) تافلر، (۴، ۱۳۷)

با افزایش حجم رخدادهای امنیتی و شناسایی تهدیدات و حملات داخلی و خارجی توسط ابزارهای امنیتی نیاز است با رویکرد امنیتی و حفاظتی، بتوان رخدادها و داده‌های گزارش‌شده را مانیتورینگ کرده و بین آنها ارتباط برقرار نمود و از این طریق تهدیدها و آسیب‌ها را تحت کنترل قرار داد (انسی و همکاران، ۱۳۸۸: ۲۳۷).

مدیریت یک سازمان برای انطباق با تغییرات و به منظور بقا و رشد در محیط‌های جدید، ویژگی‌های خاصی را می‌طلبد. یکی از مهم‌ترین خصیصه‌ها که می‌تواند به رهبران و مدیران در پاسخ به این تغییرات و مقابله با تهدیدات و آسیب‌های سازمانی کمک کند، بهره‌گیری از رویکرد امنیتی در رهبری سازمانی است (قریب، ۱۳۸۰: ۲۵). عصر اطلاعات و چالش‌های فراروی آن، فرصتها و تهدیدات جدیدی را مطرح کرده است که تنها مدیران دارای تفکر امنیتی قادر هستند نقاط قوت، ضعف و فرصت‌های محیطی را شناسایی و به تهدیدات پیرامونی پاسخ قاطع دهند (عاطف، ۱۳۸۷: ۱۵).

ویژگی‌های انسان به ویژه هوش و فعالیت‌های هوشمندانه همواره مورد توجه اندیشمندان بوده است و از دیدگاه‌های گوناگون به تعریف، طبقه‌بندی و سنجش هوش پرداخته‌اند. اگرچه تا سال‌ها، منظور از هوش، هوش عقلانی یا منطقی مد نظر بود است اما امروزه در تعریف هوش، موارد دیگری از جمله هوش عاطفی، سازمانی، هیجانی، استراتژیک، معنوی، اجتماعی و... مطرح شده است. از این‌رو، مدیران در سازمان‌ها علاوه بر هوش‌های مطرح شده، باید از هوش امنیتی با قابلیت‌های امنیتی، حفاظتی و مهارت‌های ارتباطی برخوردار باشند زیرا اهمیت و ارزش آن می‌طلبد، به مثابه یک رشته مستقل درکنار سایر انواع هوش مورد توجه قرار گیرد.

## بیان مسئله

در ساختار حاکمیت، مدیران ارشد باید به وضوح بدانندکه از سوی چه افراد، سازمان‌ها، ابزارهای فنی و... مورد تهدید قرار می‌گیرند تا قادر باشند منابع خود را بر مهم‌ترین مسائل متمرکزکنند(اکبرزاده، ۱۳۸۳: ۲۸). جهت تحقق این امر مدیران ارشد باید شناختی گسترده درباره، روندها، رویدادها، توانمندی‌ها و مهم‌تر از همه مقاصد دشمن و نیروی‌های نفوذی آنها در بدنه ساختار حاکمیت داشته باشند. در چنین وضعیتی یک سازمان بدون داشتن مدیرانی با قابلیت هوش امنیتی هم کور است و هم می‌لنگد. در این راستا مقام معظم رهبری(مدظله‌العالی) به جهت رسوخ و نفوذ اطلاعاتی در ساختار حاکمیت توجه ویژه‌ای به موضوع نفوذ داشته، و کلمهٔ نفوذ را به عنوان پرتکرارترین‌کلید واژه درسال‌های اخیر در ابعاد شناختی و هشداردهی به مسئولین مد نظر داشته است. تعریف عملیاتی نفوذ از منظرمقام معظم رهبری(مدظله‌العالی) عبارت است از: تسلط دشمن از طریق ورود پنهانی به مرزهای سیاسی، اقتصادی، فرهنگی و امنیتی توأم با تأثیرگذاری بر ذهن و رفتارمسئولان، سیاسیون، نخبگان، شخصیت‌های سیاسی و آحاد جامعه به منظور تأمین خواسته و تحقق منافع خود (برگرفته از بیانات مقام معظم رهبری۱۳۹۴) و یا تسلط دشمنان بر منافع و ارزش‌های جمهوری اسلامی با نگاه بر باورها، اعتقادات، افکار، ارزش‌های خود چهت اعمال در بدنه حاکمیت (تعریف عملیاتی آن) و انحراف سمت‌وسوی ارزش‌ها و منافع انقلاب اسلامی در جهت اهداف از پیش طراحی شده را گویند. راه برون‌رفت از این پدیده امنیتی توجه ویژه به نگاه امنیتی در ساختار حاکمیت با تأکید بر پرورش مدیرانی با قابلیت هوش امنیتی در اولویت است.

گرچه هوش امنیتی از جمله موضوعاتی است که ذهن انسان پیوسته به آن معطوف بوده و ایجاد سازمان‌های متناظر حکایت از اهمیت وحساسیت این امر دارد. ادبیات هوش امنیتی بیشتر در زمینه هوش مصنوعی (هک و نفوذ و...) بوده اما از دیدگاه محقق، هوش امنیتی در زمینه انسانی بوده نه فنی و به دنبال واکنش‌های هوشمند انسانی از جمله درک شرایط پیچیده، فرآیندهای فکری و شیوه‌های استدلالی و... می‌باشد. هرچند از زمانی که«فرانسیس گالتون» هوش را به عنوان یک ویژگی فردی مورد بررسی قرارداده، انواع هوش تئوری سازی شده و تاکنون موضوع هوش امنیتی با رویکرد انسانی مورد بررسی قرار نگرفته است (دی هار مندرا، ۲۰۱۴: ۱۵). در این راستا با طراحی مدل هوش امنیتی می‌توان موجب کاهش تهدیدات، کاهش سطح عدم انطباق، تسهیل در تصمیم‌گیری امنیتی و خودکارکردن فرآیندهای امنیتی در سازمان‌ها گردید (مهری یحیایی و همکاران، ۱۳۹۵: ۳۵).

مسئله اساسی محقق از موضوع تحقیق، سه هدف عمده بوده که شامل افزودن مفهوم هوش امنیتی در کنار انواع هوش به ادبیات علمی کشور، هوشمند سازی امنیتی ساختار حاکمیت(دولتی، خصوصی) و همچنین اضافه نمودن شرایط احراز صلاحیت مدیران ارشد حاکمیت با رویکرد امنیتی تحت عنوان هوش امنیتی، درکنار صلاحیت عمومی و تخصصی احراز پست سازمانی می‌باشد.

به جهت دغدغه اصلی از بروز بسیاری از مشکلات سازمانی در سطوح کلان مدیریتی و تلاش جهت تحقق منویات مقام معظم رهبری درخصوص نفوذ دشمن و اثرگذاری این پدیده امنیتی بر تصمیم گیران و تصمیم سازان و همچنین آسیب شناسی سازمانی و مدیریتی در حوزه نفوذ و خلاء امنیتی رویکرد مدیران ارشد در ساختار حاکمیت؛ محقق را برآن داشت تا به دنبال ارائه مدلی با عنوان«طراحی و تبیین مدل هوش امنیتی مدیران ارشد حاکمیت» باشد. در این مدل، طراحی و احصاء شاخص‌های مدل، موجب سنجش پذیرشدن ضریب امنیتی ساختار حاکمیتی و توانمندسازی مدیران با رویکرد امنیتی جهت مقابله با نفوذ سازمانی و حفاظت از اهداف، اسناد، دارایی‌های ملموس و غیر ملموس( معنوی)و ... می‌گردد.

لذا پژوهش حاضر، با واکاوی دیدگاه‌های صاحب‌نظران با دید جامع و راهبردی در جهت مدیریت تهدیدات امنیتی از طریق طراحی و تبیین مدل هوش امنیتی مدیران ارشد حاکمیت، مورد مداقه و بررسی قرار داده و به پرسش‌های زیر پاسخ خواهد داد:

- طراحی و تبیین مدل هوش امنیتی مدیران ارشد حاکمیت چگونه است؟
- شرایط علی مدل هوش امنیتی مدیران ارشد حاکمیت چیست؟
- شرایط مداخله‌گر مدل هوش امنیتی مدیران ارشد حاکمیت چیست؟
- شرایط زمینه‌ای مدل هوش امنیتی مدیران ارشد حاکمیت چیست؟
- استراتژی و راهبردهای مدل هوش امنیتی مدیران ارشد حاکمیت چیست؟
- پیامدهای اجرای مدل هوش امنیتی مدیران ارشد حاکمیت چیست؟

## ادبیات و پیشینه پژوهش

هوش یکی از پرمعناترین و کاربردی‌ترین مفاهیمی است که در حوزه‌های مختلف از جمله روانشناسی مورد استفاده قرار می گیرد؛ به همین سبب لزوم شناخت آن بر کسی پوشیده نیست. تعاریف بسیاری از هوش ارائه شده است؛ از آن جمله، هوش عبارت است از توانایی یادگیری و

به‌کار بردن آنچه یاد گرفته شده، در سازگاری با اوضاع و احوال تازه و حل مسائل و مشکلات تازه (مان، ۱۳۷۸: ۲۲۳). هوش یکی از شاخه‌های مهم روان‌شناسی تفاوت‌های فردی است و سابقه مشاهده اختلافات هـوشی افـراد به قدمت تاریخ علم می‌باشـد. به باور اسـلاوین مفهوم هوش از زمان پیش از یونـان بـاسـتان مورد بحث بوده است.

از آن زمان تاکنون انواع هوش تئوریزه شده، به اختصار می‌آید. هوش فرهنگی[1] برای نخستین بار توسط ارلی و انگ[2] (۲۰۰۳) در کتاب «هوش فرهنگی»، از محققـان مدرسهٔ کسب و کار لنـدن مـطرح شـد. تعریفی که از هوش فرهنگی دارند به این صورت است که: توانایی یک فرد در راستای سازگاری موفقیت‌آمیز با محیط‌های فرهنگی جدید که معمولاً با بافت فرهنگی خود فرد متفاوت است (تسلیمی وهمکاران، ۱۳۸۸: ۳۲). هوش هیجانی[3]، هوش هیجانی برای موفقیت شغلی ضروری است و حدود ۶۰ درصد عملکرد در تمام شغل‌ها را در بر می‌گیرد. این ویژگی به تنهایی بزرگترین عامل برای پیش‌بینی عملکرد فرد در محیط کار و قوی‌ترین نیرو برای رهبری و موفقیت است (برادبری و گریوز[4]، ۱۳۸۸: ۳۶). هوش هیجانی در زمینه شناسایی و مدیریت تأثیر عواطف بر تفکر و رفتار از طریق آگاهی دادن بیشتر به افراد با استفاده از روش‌های بین فردی، سبب توسعه توانایی تشخیص تحرکات اجتماعی در محیط کار و درک چگونگی مدیریت روابط و بهبود آنها می‌شود (دیگینز[5]، ۲۰۰۴: ۸).

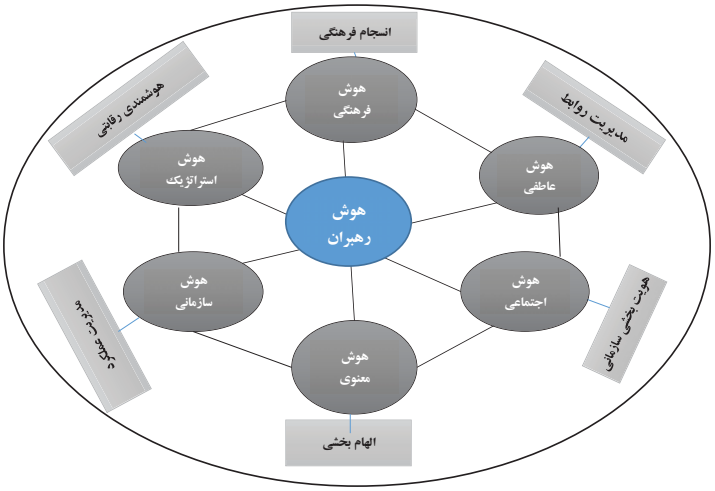
هوش معنوی[6]، مفهوم هوش معنوی برای اولین بار در ادبیات آکادمیک روان‌شناسی، در سال ۱۹۹۶ توسط استیونز[7] و بعد در سال ۱۹۹۹ توسط ایمونز[8] مطرح شد. هوش معنوی عبارت است از خودآگاهی عمیقی که در آن، فرد به جنبه‌های درونی خودآگاه می‌شود (موسوی و همکاران، ۱۳۹۰: ۶۹). هوش عاطفی[9]، ویژگی اساسی هوش عاطفی، فعالیت از طریق واکنش‌هـا اسـت. واکنش‌های غریزی نیز هوش عاطفی هستند. مهم‌ترین خصوصیت هوش عاطفی، ارتباط آن با حیات است. کارویژه اساسی آن، حـفظ حـیات است. ارزش‌دهی و احترام به زندگی، با سطح پیشرفت هوش عاطفی در پیوند است (یوشیدا و ساندا، ۲۰۱۳).

1. Cultural Intelligence
2. Earley and Ang
3. Emotional intelligence
4. Bradbury and Greaves
5. Diggins
6. Spiritual Intelligence
7. Stevens
8. Emmons

هـوش مـصنوعی[۱۰]، هـوش مصنوعی دانشی نوپا و در حال پیشرفت اسـت. نـخستین تلاش‌ها برای ساختن ماشین‌های هوشمند پس از جنگ جهانی دوم آغاز شد و اصطلاح هوش مـصنوعی از سـال ۱۹۵۶ رایج شد. هم اکنون دانش هوش مصنوعی، زیرشـاخه‌های بسیاری دارد؛ از رشته‌های عمومی مـانند یادگـیری و ادراک گرفته، تا موارد خاص، مـانند بـازی شطرنج، ارائه اثبات برای فرمول‌های ریاضی، نوشتن شعر، رانندگی در خیابان‌های شلوغ. این مورد امروزه بـه لطـف فناوری‌های جدید تحقق پیدا کرده است (Russell, 2010, p1). هوش اجتماعی[۱۱]، در هوش اجتماعی درباره یک طبقه کلی صحبت می‌شود، یعنی ظـرفیت انـسان بـرای درک آنچه که در دنیا رخ می‌دهد و پاسخ به آن به شیوه مؤثر شخصی و اجتماعی (کارل آلبـرت، ۲۰۰۴). هوش تحلیلی(عقل)[۱۲]، هوش تحلیلی شامل تـوانایی تحلیل، قضاوت، ارزشیابی، مقایسه کردن امور انتزاعی، پردازش اطلاعات و سازماندهی به مطالب است (استرنبرگ، ۲۰۰۵). هوش اخلاقی[۱۳]، این اصطلاح برای نخستین بار توسط بوربا[۱۴] در سال ۲۰۰۱ در روان‌شناسی وارد شد. وی هوش اخلاقی را ظرفیت و توانایی درک درست از خلاف، داشتن اعتقادات اخلاقی و عمل به آنها و رفتار در جهت صحیح و درست تعریف می‌کند و معتقد است اصول هوش اخلاقی شامل: درستکاری، مسئولیت‌پذیری، دلسوزی و بخشش رعایت می‌باشد (بوربا،۲۰۰۱: ۲۳). هوش استراتژیک[۱۵]، ازنظر لیبو ویتز (۲۰۰۶)، هوش استراتژیک بیان کننده تغییر در اطلاعات است که می‌تواند در تصمیم گیری‌های کلان کسب و کار مورد استفاده قرار گیرد که بر چگونگی موقعیت‌یابی سازمان به منظور مقابله با چالش‌ها و فرصت‌های آینده برای به حداکثر رساندن موفقیت سازمان تأکید دارد (مارک ژو وکای، ۲۰۰۷). هوش چندگانه گاردنر[۱۶]، یکی از نظریه پردازان در زمینه هوش و تفاوت‌های فردی هـوارد گـاردنر مـی‌باشـــد. او با بیان اینکه هوش دارای انواع گوناگونی اســت، معتقد است انسان دارای چند هوش متمایز از هم اســت نه یک هوش خاص. دیدگاه‌های ســنتی هوش بر ابعادی از توانایی‌ها و اســتعدادهای انســان مانند؛ ۱.هوش منطقی/ ریاضی[۱۷] ۲. هـوش زبـانی/کلامی[۱۸] ۳. هوش دیداری/ فضایی[۱۹] ۴. هوش موسیقایی[۲۰] ۵.

9. Emotional Intelligence
10. Artificial intelligence
11. social intelligenc
12. Analytical intelligence (intellect)
13. Moral Intelligence
14. Borba
15. Strategic intelligenc
16. Multiple Intelligences (MI)

هوش بدنی/ جنبشی۶. هوش بین فردی[۲۱] ۷. هوش درون فردی[۲۲] ۸. هوش طبیعت‌گرایی ۹. هوش هستی‌گرایی: تأکید دارد(Gardner ۲۰۱۱). هوش سازمانی[۲۳]، هوش سازمانی یکی از مؤلفه‌هایی است که مدیران عصر حاضر بایستی دارا باشند تا با کسب دانش عمیق نسبت به همه عوامل محیطی باعث هوشمندی سازمان گردیده و در نتیجه آن، بهتر بتوانند سازمان تحت هدایت خود را در دنیای متلاطم و رقابتی امروز مدیریت کنند (عرفانی‌خانقاهی و جعفری،۱۳۸۹: ۵۱). ابعاد هوش سازمانی[۲۴]: به‌طورکلی هوش شش گانه رهبران عبارت‌اند از هوش عاطفی، هوش استراتژی، هوش فرهنگی، هوش معنوی، هوش اجتماعی و هوش سازمانی که در شکل (۱)می‌آید.




شکل(۱) ابعاد هوش سازمانی (عرفانی‌خانقاهی و جعفری،۱۳۸۹)

این مقاله به جهت نو بودن موضوع به دنبال تبیین هوش‌امنیتی در ساختار حاکمیت بوده و در این راستا پس از آشنایی با هوش و انواع آن به صورت مختصر مفهوم امنیت[۲۵] واکاوی گردیده و سپس هوش امنیتی تشریح می‌گردد. بحث درباره امنیت، از دشواری‌های متنوعی برخوردار است که از جمله می‌توان به معنای امنیت و مرزهای نامعلوم آن در مفاهیمی همچون امنیت جامعه، امنیت جمعی،

17. Logical/ Mathematical Intelligence
18. Verbal/Linguistic Intelligence
19. Spatial/Visual Intelligence
20. Musical Intelligence
21. Interpersonal Intelligence
22. Intrapersonal Intelligence
23. Organizational Intelligence
24. Dimensions of organizational intelligence

امنیت انسانی، امنیت ملی، امنیت سازمانی و غیره اشاره نمود. در این بین، تهدیدات امنیتی می‌تواند ثبات و پایداری سازمان‌ها را با تأثیرگذاری بر محرمانه بودن، یکپارچگی و در دسترس بودن سرمایه اطلاعاتی/ ساختاری، مختل کنند. نمونه‌هایی از این پتانسیلِ ایجاد اختلال و اثرات خارجی، شامل سقوط سازمانی، تا ناتوان ساختن زیرساخت‌های کشورهاست (کیسر[۲۶]، ۲۰۱۵: ۴۶).

در همین رابطه بحث درباره تأثیرات رویکرد امنیتی بر مدیران سازمان‌ها در حالی است که امنیت در اکثر سازمان‌ها، به عنوان یک کار درجه دو(کم اهمیت) باقی مانده است، از سویی دیگر، مزیت بهره‌برداری این رویکرد، ایجاد توانمندی در کسب و کارها برای کنترل محدودیت‌های نسبیِ زمانی و جغرافیایی، به عنوان توانمندسازهای سازمانی است (سالوس و دیگران[۲۷]، ۲۰۱۹).

امنیت شامل تعقیب روانی و مادی ایمنی است و اصولاً جزء مسئولیت حکومت‌های ملی است تا از تهدیدات مستقیم ناشی از خارج، نسبت به بقای رژیم‌ها، نظام شهروندی و شیوه زندگی شهروندان خود ممانعت به عمل آورند (ماندل، ۱۳۷۸: ۴۵). از آنجاکه محیط امنیتی برامنیت هر کشور مؤثر بوده (هافندرون،۱۳۷۱:۲۲) و حاصل برآیند عوامل در هم پیچیده محیط داخلی[۲۸] و محیط خارجی[۲۹] (مینایی، ۱۳۸۳: ۱۳۸) و متأثر از محیط بین‌المللی است (درویشی سه تلانیریال، ۱۳۸۴: ۲). امنیت در نگاه سنتی بیشتر باتهدیدات سخت افزاری چون امنیت نظامی شامل تهاجم یا دفاع در مقابل دشمنان خارجی سروکار دارد (هندیانی،۱۳۸۶). اما همان‌گونه‌که بوزان (۱۳۷۸: ۱۵) اشاره می‌کند امروزه دیدگاه به امنیت علاوه بر جنبه نظامی به سایر جنبه‌های نرم افزاری همچون سیاسی، اقتصادی، اجتماعی، رضایتمندی شهروندان و فهم مدیران سازمانی نیز توجه دارد. فرآیند اعمال نفوذ در محیط امنیتی مدرن نیازمند توجه به مراحل سه گانه زیر است: بر هم زدن نظم نسبی موجود، ایجاد نظم جدید و مدیریت نظم جدید. زیرا شناخت و احتمال پیش‌بینی پذیری نفوذ و مدیریت رفتار این پدیده امنیتی در ساختار حاکمیت، بادیدگاه هوش امنیتی پیاده خواهد شد.

هوش امنیتی[۳۰]: امروزه از انواع مختلف هوش در مجامع گوناگون صحبت به میان می‌آید (مانند هوش معنوی، هوش عاطفی، هوش هیجانی، هوش سیاسی، هوش اخلاقی، هوش تجاری،

25. The concept of security
26. Kaiser
27. Sallos et al

۲۸- عواملی همچون ساختار حکومتی، چگونگی توزیع و تمرکز قدرت داخلی، تشکل‌های اجتماعی، فعالیت‌های سیاسی، ایدئولوژی و ارزش‌ها، مشارکت مردمی

۲۹- عواملی مانند ساختار قدرت، نظم و یا بی نظمی جهانی، تکنولوژی، مسابقه تسلیحاتی و موقعیت ژئواستراتژیکی

هوش رقابتی، هوش سازمانی، هوش مدیریتی و ...) و هوش، پیشوند بسیاری از مفاهیم مدیریتی شده است که خود نشان دهنده تغییر نگاه سازمان‌ها و متفکرانشان از هوش سنتی به رویکردهای نوین به این مقوله است که این تحقیق، به مقوله هوش امنیتی پرداخته است:

- هوش امنیتی می‌تواند رخدادها و داده‌های گزارش شده را رصد کرده و بین‌آنها ارتباط برقرار نموده و از این طریق، تهدیدها و آسیب‌ها را شناسایی تا تحت کنترل اطلاعاتی و امنیتی، قرار دهد(رضایت و مرادیان، ۱۳۹۵). پیرک و دیگران[۳۱] (۲۰۱۶)، هوش امنیتی را جمع‌آوری، به 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 فناوری اطلاعات در سازمان تأثیر می‌گذارد، تعریف کرده و معتقدند، هوش امنیتی به دنبال مدیریت همه‌جانبه اطلاعات امنیتی در سازمان است (پیرک و دیگران، ۲۰۱۶: ۲۵). آنچه مشخص است هوش امنیتی دو بخش مهم و اساسی را پوشش می‌دهد؛ یک بخش مربوط به مدیریت تعاملات و همبستگی فناوری‌های مورد استفاده در امور امنیتی سازمان و دیگری، مدیریت یکپارچگی و همبستگی این اطلاعات (ساموناس و دیگران، ۲۰۲۰).

بررسی ادبیات نشان می‌دهد، از هوش تعریف واحدی به دست نیامده و صاحب‌نظران مختلف آن را به گونه‌های متفاوتی تعریف کرده‌اند. نمی‌توان تعریف مشخصی از هوش به دست آورد که مورد توافق همه روان‌شناسان وابسته به رویکردهای مختلف باشد. با این حال عناصری از هوش وجود دارند که مورد توافق غالب پژوهشگران است. این عناصر را با توجه به ادبیات، می‌توان در سه دسته تقسیم کرد:

- **توانایی پرداختن به امور انتزاعی:** منظور این است که افراد باهوش بیشتر با امور انتزاعی (اندیشه‌ها، نمادها، روابط، مفاهیم، اصول) سروکار دارند تا امور عینی (ابزارهای مکانیکی، فعالیت‌های احساسی).
- **توانایی حل کردن مسائل:** یعنی توانایی پرداختن به موقعیت‌های جدید، نه فقط دادن پاسخ‌های از قبل آموخته شده به موقعیت‌های آشنا.
- **توانایی یادگیری:** به ویژه توانایی یادگیری انتزاعیات، از جمله انتزاعیات موجود در کلمات و سایر نمادها و نیز توانایی استفاده از آنها (سیف، ۱۳۹۸: ۲۸).

30. Security intelligence
31. Pirc et al

هوش امنیتی دارای سه جزء اصلی ۱. مدیریت اطلاعات و رخدادهای امنیتی[۳۲]، ۲. مدیریت ریسک[۳۳] و ۳. انطباق قوانین[۳۴] است (پیرک و دیگران، ۲۰۱۶: ۴).

- **مدیریت اطلاعات و رخدادهای امنیتی:** به عنوان قلب هوش امنیتی به شمار 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[۳۵] یا نگاشت، نرمال‌سازی[۳۶] یا هنجارسازی، همبسته‌سازی رویدادها[۳۷]، عکس‌العمل آنی به تهدیدات (پاسخ فعال[۳۸])، امنیت عناصر انتهایی (EPP)[۳۹]، ذخیره سازی وقایع[۴۰] و ارائه گزارشات تحت وب[۴۱].
- **مدیریت ریسک:** هدف مدیریت ریسک یا مدیریت مخاطرات در هوش امنیتی، کاهش زیان‌های ناشی از عملی شدن تهدیدات است که با استفاده از سه شاخص شناسایی، ارزیابی و اولویت گذاری و بر مبنای استاندارد مدیریت ریسک در پنج گام می‌توان به این هدف رسید که عبارت است از:۱.تشخیص و شناسایی تهدیدات،۲.ارزیابی آسیب پذیری-های هدف تهدیدات،۳. تشخیص زیان‌های ناشی از عملی شدن تهدیدات،۴.تعیین راه‌کارهای کاهش مخاطرات و ۵. اولویت گذاری راه‌کارها.
- **انطباق قوانین:** هدف انطباق قوانین در هوش امنیتی، حصول اطمینان از برقراری سه مورد تطابق با استانداردها (استفاده از استانداردها در پیاده سازی هوش امنیتی، همچون استفاده از استاندارد ISO ۵۰۷۷۲ در پیاده سازی مدیریت ریسک در هوش امنیتی)، پایداری در نظارت (نظارت و مانیتورینگ مستمر و دائمی هوش امنیتی بر کلیه فعالیت‌ها و رویدادها) و کامل بودن بازرسی (بررسی همه جانبه و تجزیه و تحلیل کلیه فعالیت‌ها و رویدادها توسط هوش امنیتی). سه جزء

32. Security Information and Event Management
33. Risk Management
34. Regulatory Compliance
35. Log
36. Normalization
37. Event Correlation
38. Active Response
39. Endpoint Protection Platform
40. Event/Incident Storage
41. Web-based Reports

تشکیل دهنده هوش امنیتی، شامل مدیریت اطلاعات و رخدادهای امنیتی، مدیریت ریسک و انطباق قوانین، بر مبنای سه اصل «هوش، یکپارچگی و خودکار سازی» با هم در تعامل بوده تا هدف اصلی هوش امنیتی که تأمین امنیت است تحقق یابد. هوش امنیتی با ایجاد مانیتورینگ و نظارت مستمر و دائمی بر کلیه فعالیت‌ها و رویدادهای سازمان مربوطه و بررسی و تجزیه و تحلیل این فعالیت‌ها و رویدادها هرگونه ناهنجاری و تهدید را شناسایی و از بروز حملات امنیتی جلوگیری می‌نماید(پیرک و دیگران، ۱۲:۲۰۱۶). از این رو روش‌های مبتنی بر به اشتراک گذاری تهدیدات، تلفیق روش‌های پیشگیرانه و واکنش‌گرا نظیر هوشیاری پیرامون تهدیدات، شکار تهدیدات و استفاده از خودکار سازی درکنار راه‌کارهای مبتنی بر یادگیری هوش مصنوعی می‌توانند کلید گشودن قفل بسیاری از مشکلات امنیتی در سازمان‌ها باشند (آدینه، ۱۳۸۹: ۳۵).

بر اساس تعریف پیتر گیل، هوش امنیتی عبارت است از جمع‌آوری اطلاعات و تلاش برای مقابله با تهدیدات در امنیت ناشی از جاسوسی، خرابکاری، فعالیت‌های خارجی به منظور تحلیل به‌هنگام داده‌های هوش امنیتی، طراحی مدیریت جامع ریسک ، توجه به تهدیدات حفاظتی و تشخیص از طریق آموزش را فراهم می‌کند (گاردنر، ۳۶:۲۰۱۳).

هوش امنیتی در واقع با به‌کارگیری مهارت‌های لازم در جهت جمع‌آوری، یکپارچه سازی و تحلیل تمام اطلاعات مذکور به دنبال بهینه سازی و در نهایت افزایش هوشمندی سازمان در امور امنیتی است. برای تهدید هوش امنیتی، دسته‌بندی‌های مختلفی توسط شرکت‌های امنیتی ارائه شده است که کامل‌ترین دسته‌بندی هوش امنیتی تهدیدات شامل یک رده‌بندی چهار سطحی است. براین اساس انواع سطوح هوش امنیتی تهدید عبارت‌اند: هوش امنیتی راهبردی[۴۲] در سطح بالای تصمیم گران ساختار حاکمیت مورد استفاده قرار می‌گیرند. راهبردهای بهبود هوش امنیتی در ساختار حاکمیت به ندرت شامل موارد فنی هستند و بر اطلاعات مرتبط با ریسک تمرکز دارند. از جمله چیزهایی که در این اطلاعات می‌توان یافت موارد مرتبط با تأثیر مالی رخداد سایبری، روندهای حملات آتی، حوزه‌های مستعد برای حمله مهاجمان و حوزه اثرگذار بر تصمیمات کلان و سطح بالای سازمان می‌باشد. چنین اطلاعاتی به سازمان‌ها در تعیین اقدامات، ظرفیت‌ها و بودجه لازم را برای مقابله و کاهش خطر حملات احتمالی کمک می‌کند. هوش امنیتی راهبردی

42. Strategic security intelligence

اغلب به صورت خبر و اطلاعات مربوط به گزارشات انحصاری، مذاکرات و جلسات هستند. بدست آورن این اطلاعات بسیار دشوار است به دلیل اینکه این اطلاعات حاوی راهبردهای مهاجمان هستند بازه زمانی کاربرد آنها بلند مدت(چند سال) است. سطوح هوش امنیتی عملیاتی[۴۳]: این اطلاعات توسط کارمندان امنیتی سطح بالای سازمان (مدیریت لایه میانی) نظیر مدیران امنیت اطلاعات یا سرپرستان واحد پاسخگویی به رخداد مورد استفاده قرار می‌گیرند.سطوح هوش امنیتی تاکتیکی[۴۴]: شامل اطلاعاتی هستند که چگونگی اجرای حملات توسط عامل‌های تهدید را بیان می‌کنند. هوش امنیتی تاکتیکی توسط مدافعان شبکه و متخصان پاسخگویی به رخداد به‌کار گرفته می‌شوند. سطوح هوش امنیتی فنی[۴۵]: این دسته از هوش امنیتی اغلب دارای بازه مصرف کوتاه مدت است و از طریق بررسی یا پایش سیستم به‌دست می‌آید (مانوگران و دیگران[۴۶]، ۲۰۱۷).

## مفاهیم و تعاریف به‌دست‌آمده هوش امنیتی از نظر محقق:

۱. هوش امنیتی کمک می‌کند به هر نوع مسائل روزمره سازمان با حساسیت نگاه کنیم و بینش به منزله کار امنیتی نیست بلکه زمینه‌ساز حفاظت از دارایی مشهود و غیر مشهود سازمان و محیط کاری است.

۲. هوش امنیتی یعنی احساس امنیت کارکنان و مدیران از انعکاس موارد مخل امنیت فردی و سازمانی بدون احساس ترس.

۳. هوش امنیتی یعنی درک و فعال شدن هشدارهای امنیتی پیش رو جهت مقابله با تهدیدات فراسوی آن.

۴. هوش امنیتی، یعنی هوشمندی مؤلفه‌های شناخت افراد دارای شم امنیتی برای احراز پست‌های کلیدی و مشاغل حساس.

۵. هوش امنیتی یعنی رفتار هوشمندانه‌ای در جهت تأمین امنیت، از طریق مدیران و کارکنان.

۶. هوش امنیتی، رفتار هوشمندانه‌ای است برای تأمین امنیت فرد، سازمان و محیط.

۷. هوش امنیتی یعنی، تعریف بررسی علت و چرایی هرپدیده و خسارات امنیتی.

43. Operational Security Intelligence Levels
44. Tactical security intelligence levels
45. Technical security intelligence levels
46. Manogaran et al

۸. برمبنای تحقیق صورت گرفته، اهداف هوش امنیتی عبارت است از عدم غافلگیری در سازمان در پی شناخت مؤلفه‌ها و شاخص‌ها از جمله شناخت مأموریت و شرح وظایف دستگاه‌ها، توجه به گردش اطلاعات در سازمان، تجزیه و تحلیل محیطی جهت آینده نگری و پیش‌بینی، هشدار به هنگام ، سرعت و دقت به همراه اعتمادافزایی نشانه شناسی امنیتی و گماردن افراد دارای ویژگی امنیتی و.....

۹. تعریف نهایی هوش امنیتی از منظر محقق عبارت است از: تلاش برای مقابله با تهدیدات درک شده (حسی و ذهنی) در امنیت ناشی از جاسوسی، خرابکاری، فعالیت‌های خارجی، نشت‌های اطلاعاتی، رسوخ اطلاعاتی در سازمان از طریق انتصاب مدیران ارشد دارای رویکرد امنیتی به منظور مقابله با نفوذ عوامل تهدیدگر در ساختار حاکمیت. در این تعریف مدیران ارشد[۴۷]: به آن دسته از مدیران گفته می‌شود که وظیفه سیاست‌گذاری، خط مشی‌گذاری، برنامه‌ریزی کلان، هدایت و نظارت عالیه بر عملکرد دستگاه را در واحدهای ستادی به عهده دارند (سازمان مدیریت و برنامه‌ریزی، ۱۳۹۵). جیمز برنهام[۴۸] جامعه‌شناس آمریکایی، در سال ۱۹۴۱ درکتاب «انقلاب مدیریتی» خود، ظهور یک طبقه اجتماعی جدید مرکب از مدیران را پیش‌بینی کرده بود. وی گفته جنگ ۱۹۳۹ اولین جنگ بزرگ جامعه مدیریتی است. بنابراین وجود زیردستان، عامل مفیدی در کمک به تعریف و تشخیص انواع مدیران سازمان است (علاقه بند، ۱۳۸۸: ۱۳). مدیر ارشد[۴۹] مدیریت اجرایی یا تیم مدیریتی، به تیمی از افراد در بالاترین سطح از مدیریت یک سازمان اطلاق می‌گردد، که مسئولیت مدیریت آن سازمان یا شرکت را برعهده دارند (رضائیان، ۱۳۸۴: ۲۸). و حاکمیت[۵۰]: مفهوم حاکمیت در عصر حاضر تغییر یافته است و اشاره بر حاکمیت مردم دارد تا حاکمیت هیئت حاکمه و تنها حاکمیت مردمی است که در حقوق بین‌الملل محترم است. حاکمیت ملی در حقیقت به این مفهوم است که کشور را چگونه بسازیم و به دست مردم چگونه به آن شکل بدهیم و در سازماندهی و اداره کشور به دست مردم جامه عمل بپوشانیم. در عصر حاضر اشاره بر حاکمیت مردم دارد تا حاکمیت هیئت حاکمه و تنها حاکمیت مردمی است (کاتوزیان، ۱۳۷۲: ۱۹). در تعریف عملیاتی حاکمیت، شاغلان سطوح مختلف کارشناسی، مدیریتی،

47. Senior Managers
48. James Burnham
49. Senior manager
50. Sovereignty

ریاستی و سایر دستگاه‌های نهادی کشوری و لشکری نظام جمهوری اسلامی ایران را گویند که در مناصب یا جایگاه تصمیم‌گیری یا تصمیم سازی دارای حق قانون تدوین، تصویب، اجرا و اعمال قوانین و دستورات در حوزه‌های سیاسی، اجتماعی، فرهنگی، اقتصادی، امنیتی، نظامی و زیست محیطی می‌باشند. نفوذ درحاکمیت به تسلط دشمنان از طریق ارزش‌ها و منافع خود (اعتقادات، افکار،ارزش‌ها و باورها) در بدنه حاکمیت و انحراف سمت وسوی ارزش‌ها و منافع انقلاب اسلامی در جهت اهداف از پیش طراحی شده را گویند.

بررسی پیشیه تحقیق نشان داد که به‌طورکلی، مطالعات متعددی پیرامون هوش و انواع مختلف آن به‌طور جداگانه صورت گرفته است، ولی آنچه که مشخص گردید این بود که تحقیقاتی در رابطه با طراحی و تبیین مدل هوش امنیتی مدیران ارشد در ساختار حاکمیت تاکنون مورد توجه پژوهشگران قرار نگرفته است. لذا تحقیق حاضر، شکاف تحقیقات ادبیات را مورد بررسی قرار داد تا بتواند با بضاعت علمی اندک چارچوب اولیه‌ای ارائه نماید. در این راستا به برخی از تحقیقات انجام شده با موضوع هوش و امنیت اشاره می‌گردد.

- مجتبی خدادادی و علی حسن پور(۱۳۹۲) درتحقیقی تحت عنوان«نقش هوش هیجانی در توانمندی امنیتی مدیران» با جامعه آماری مدیران عالی سازمان‌های امنیتی کشور انجام گردیده که براین اساس انتظار می‌رود مدیرانی که از هوش هیجانی بالاتری برخوردارند، اثربخشی بالاتری نیز در مدیریت داشته باشند. این امر می‌تواند در انتخاب مدیران شایسته در سازمان‌های امنیتی مورد توجه باشد.
- محمود کلاه‌چیان(۱۳۹۳) در تحقیقی تحت عنوان «مدیریت عملیات پنهان در سازمان‌های امنیتی» بیان می‌دارد دیر زمانی است که پهنه عملیات پنهان با تحولات فنی، تغییرات محیط و تفکرات حاکمیتی دچار فراز و فرودهای چندی گردیده است.
- فریبا شایگان(۱۳۹۱) در تحقیقی تحت عنوان« امنیت پایدار از دیدگاه مقام معظم رهبری» برای دستیابی به نظریات معظم‌له در خصوص امنیت پایدار چهار سؤال؛ ویژگی امنیت پایدار، مشمولان آن، متولیان آن و نیز شیوه‌های ایجاد و حفظ آن را مطرح کرده است.
- بهرام اخوان کاظمی(۱۳۹۶) تحقیقی تحت عنوان« الگوی امنیت در مکتب امنیتی جمهوری اسلامی ایران» انجام داده که در تبیین آن باید اذعان کرد که ایمان و امنیت معنوی، سرچشمه و مبنای اصلی تمام ابعاد امنیت و سازوکارهای تأمین آن بوده است.

- جعفر فینی زاده بیدگلی و همکارن (۱۳۹۵) تحقیقی تحت عنوان «بررسی ویژگی امنیتی شدن یک پدیده (موضوع) درجمهوری اسلامی ایران» انجام داده‌اند و نتایج این تحقیق مشخص می‌کند که، بازیگران و میزان جدی بودن تهدیدات، بالاترین سهم در امنیتی شدن موضوعات ازجمله بحران‌ها را دارند.
- داود فیض و همکاران(۱۳۹۴) در تحقیقی تحت عنوان « شناسایی ذهنیت افراد نسبت به نفوذ دشمن با استفاده از روش کیو با موضوع نفوذ» مورد بررسی و تحلیل قرارگرفت. در نهایت، مشخص گردید بیشترین نفوذ از طریق نفـوذ فرهنگـی، نفـوذ اقتصادی و نفوذ سیاسی-امنیتی بوده است.
- سیامک باقری چوکامی(۱۳۹۶) در تحقیقی تحت عنوان «با توجه به تحول پارادیمی نفوذ و ماهیت شناسی آن» به این نتیجه رهنمون می‌شویم که درجه تهدیدات ناشی از نفوذ فرانوین فوق حیاتی است.
- ناهید اوجاقی و همکاران (۱۳۹۶) در تحقیقی تحت عنوان «رابطهٔ ابعاد هفت‌گانهٔ هوش سازمانی و توانمندی‌های روان‌شناختی کارمندان» انجام که در نهایت، رابطهٔ همهٔ ابعاد هوش سازمانی و توانمندی‌های روان‌شناختی کارکنان مثبت و معنادار به دست آمد.
- جعفر هزار جریبی و همکاران(۱۳۸۵) در تحقیقی تحت عنوان « مفاهیم و گونه‌های مؤثر در شناخت آسیب‌های امنیتی» عنوان می‌دارد آسیب شناسی امنیتی را یک شاخه علمی جدید و بـین رشته‌ای دانسته است.
- حسن کاویانی(۱۳۹۶) در تحقیقی تحت عنوان «بررسی رابطه هوش سازمانی و تفکر راهبردی در یک یگان اطلاعات نظامی» یافته‌های تحقیق نشان می‌دهد در بین هوش سازمانی و تفکر راهبردی سازمان هدف رابطه مثبت و معناداری وجود دارد.

## روش پژوهش

تحقیق حاضر به لحاظ هدف؛ اکتشافی- کاربردی، به لحاظ روش استنتاج، توصیفی- پیمایشی و به لحاظ ماهیت داده‌ها، کیفی و کمی است که درسه مرحله انجام شده است.

**الف) بخش کیفی:** در وهله نخست، پس از مطالعه کتابخانه‌ای، به جهت تبیین مدل هوش امنیتی ساختار حاکمیت، از مصاحبه نیمه ساختاریافته استفاده گردیده است. تحلیل محتوای مصاحبه‌ها

با استفاده از روش گرندد تئوری و کدگذاری در سه سطح؛ باز، محوری وگزینشی انجام شد (کرسول، جان دبلیو، ۱۳۹۶). جامعه آماری این تحقیق را اعضای هیئت علمی دانشکده و پژوهشکده امنیت و مدیران و کارشناسان خبره 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 که یکی از روش‌های نمونه‌گیری هدفمند متوالی یا متواتر است، استفاده شد. در نمونه‌گیری نظری، نمونه‌ها به شکلی 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 فرآیند گردآوری، خزانه داده‌های مورد نیاز را غنی نمایند تا امکان ساختن مدل فراهم شود. در این روش به جای انتخاب یک نمونه ثابت حجم نمونه آنقدر افزایش می‌یابد تا زمانی‌که دیگر کافی باشد و به اشباع نظری برسد (بازرگان‌هرندی و دیگران، ۱۳۹۷:۸۵). بر همین اساس، بعد از انجامِ ۹ مصاحبه، دیده شد که عوامل اصلی و فرعی در مصاحبه‌ها تکرار شده و پاسخ‌ها از روندی تکراری تبعییت می‌کنند اما برای اطمینان بیشتر، علاوه بر تحلیل پنج منبع به‌صورت کتابخانه‌ای، سه مصاحبه دیگر نیز انجام شد و نمونه با ۱۲ نفر مورد تأیید قرار گرفت و به فرآیند مصاحبه پایان داده شد و پژوهشگر به اشباع نظری رسید. پس از پیاده سازی مصاحبه‌ها، یافته‌های تحقیق به صورت متن درآمده، و در نرم افزار NVivo Plus2020، کدگذاری و مقوله‌بندی شده و اقدام به تحلیل آنها گردید. نهایتاً پس از اعتبار نهایی، در قالب ۱۵۰ زیر شاخص فرعی و ۲۲ شاخص اصلی و همچنین پنج بُعد دسته‌بندی شد و با استفاده از مدل یابی معادلات ساختاری، روابط بین مؤلفه‌ها تحقیق برازش کلیه روابط تأیید گردید. در پایان به منظور رسم مدل ساختاری-تفسیری از روش ISM ، استفاده شد.

**ب) بخش کمی:** تحقیق حاضر با استفاده از مدل یابی معادلات ساختاری، انجام پذیرفت. جامعه آماری و روش نمونه‌گیری در این بخش از تحقیق، شامل کارشناسان و مدیران خبره جامعه اطلاعاتی بوده است. جهت تعیین حجم نمونه، از روش ریاضی و فرمول کوکران، استفاده شده است. روش نمونه‌گیری پژوهش حاضر، با توجه به جامعه آماری مورد نظر به تعداد۲۸۰ به صورت نمونه‌گیری طبقه‌ای نسبی چند مرحله‌ای بوده است و پرسشنامه به صورت تصادفی در هر طبقه و به نسبت جمعیت آن طبقه انجام شده است. حجم نمونه تصادفی برای تحقیق حاضر ۱۶۲ نفر تخمین زده شد. بر همین اساس پرسشنامه الکترونیکی تحقیق درپرس لاین طراحی و در اختیار ۱۸۰ نفر از پاسخ دهندگان قرار داده شد. در مجموع تعداد ۱۶۲پرسشنامه تکمیل و برای انجام ادامه

مراحل پژوهش مورد استفاده قرار گرفت. در این بخش از تحقیق مدل مفهومی پژوهش که از نوع ترکیبی است با استفاده از تکنیک مدل یابی معادلات ساختاری به روش حداقل مجذورات جزئی (PLS) آزمون شد. نرم‌افزار مورد استفاده Smart PLS است. روش‌های معادله ساختاری میزان و شدت روابط فرضی میان متغیرها را در یک مدل نظری تخمین می‌زند (جفری ام، ۱۳۹۰).

**ج) بخش کمی دوم:** در این مرحله از تحقیق، الگویابی معادلات ساختاری در دو مرحله به آزمون الگو می‌پردازد، که شامل آزمون الگو اندازه‌گیری و الگوی ساختاری است. در مدل سازی PLS الگوی اندازه‌گیری را مدل بیرونی و الگوی ساختاری را مدل درونی می‌نامند.

الگو اندازه‌گیری به بررسی اعتبار و روایی ابزارهای اندازه‌گیری و سازه‌های پژوهش می‌پردازد و بر این اساس دو شاخص شامل: ۱- روایی همگرا و ۲-روایی واگرا( افتراقی)، مورد بررسی قرار می‌گیرد. در روایی همگرا ابزارهای اندازه‌گیری با استفاده از شاخص واریانس و میانگین استخراج شده، تأیید شد اما روایی واگرا مدل اندازه‌گیری با استفاده از آزمون فورنل- لارکر تأیید شد.

الگوی ساختاری، فرضیه‌ها و روابط بین متغیرهای مکنون را مورد آزمون قرار می‌دهد (هرجر و دیگران[۵۱]، ۲۰۱۷). بر همین اساس با استفاده از تکنیک حداقل مجذورات جزئی(Partial LeastSquares) و با نرم‌افزارSmart Pls ، تمامی روابط هم‌زمان مورد آزمون قرار گرفت. در پژوهش حاضر، جهت بررسی برازش مدل ساختاری، دو شاخص مورد بررسی قرار می‌گیرد که شامل: ۱. ضریب تعیین تعدیل شده(R۲)، ۲. قدرت مدل یا اعتبار افزونگی[۵۲] (Q۲)، است. قدرت پیش‌بینی مدل یا اشتراک افزونگی[۵۳] معیار دیگری برای بررسی برازش مدل ساختاری است. مقادیر به‌دست‌آمده از این آزمون مثبت است که نشان دهنده کیفیت مناسب مدل ساختاری است (سرستدت و دیگران، ۲۰۱۷). با توجه به نتایج مدل اندازه‌گیری و ساختاری، می‌توان نتیجه گرفت که مدل تدوین شده در بخش کیفی شکل(۲) از روایی و پایایی قابل قبولی برخوردار است و می‌تواند به عنوان یک مدل قابل اعتماد برای تبیین مدل هوش امنیتی مدیران ارشد حاکمیت، به‌کار گرفته شود.

51. Hair Jr et al
52. CV-Redundancy
53. CV Red

## یافته‌های پژوهش

جهت اعتبارسنجی نتایج بخش کیفی از محاسبه درصد اعتبار بازآزمون پژوهش در بین مصاحبه شوندگان جدید کُدهای مشخص‌شده در دو آزمون با هم مقایسه شدند. بنابراین درصد اعتبار روش کثرت‌گرایی در مصاحبه‌شونده در این پژوهش برابر ۷۵ درصد است. با توجه به اینکه این میزان پایایی بیشتر از ۶۰ درصد است (Kvale, 1996, p. 237) ، اعتبار مصاحبه شوندگان و روش انتخاب آنها مورد تأیید است. لازم به ذکر است جهت اعتبارسنجی نتایج بخش کیفی در این مطالعه، از روش کنترل اعضا (محققان یافته‌های خود را با سه نفر از افراد مطلع تحت بررسی کنترل نموده و تفاسیر پژوهشگر به تأیید رسیده است، استفاده شده است.

در این قسمت حاصل کدگذاری اولیه یا کدگذاری باز، محوری و گزینشی ارائه می‌شود که در نرم افزار Nvivo استخراج شده است و در قالب جدول شماره(۱) با عنوان تحلیل مصاحبه‌ها ارائه می‌گردد.

جدول (۱): کدگذاری مصاحبه‌ها و استخراج مدل هوش امنیتی مدیران ارشد حاکمیت

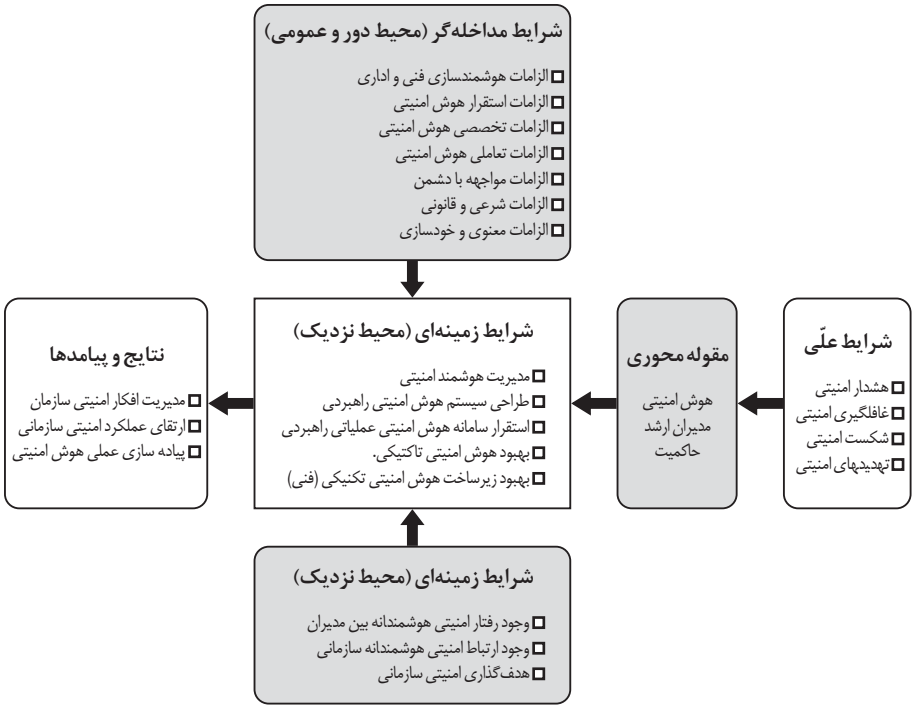
| مقوله‌ها | کدگذاری محوری | کدگذاری باز (اعداد داخل پرانتز نشان‌دهنده تکرار مفاهیم است) |
|---|---|---|
| شرایط علّی | هشدار امنیتی | انتصابات مدیران ارشد بدون توجه به هشدارهای امنیتی(۲۷)- وجود شواهد و قرائن اطلاعاتی مخل امنیت(۹)- بازخورد منفی در ارزیابی رعایت قواعد امنیتی سازمان(۱۳)- رصد نشانه‌های نفوذ ازطریق شم اطلاعاتی مدیر(۷)- وجود رسوخ و نشت‌های اطلاعاتی در سازمان(۶) |
| | غافلگیری امنیتی | وجود خطای تحلیل در پدیده‌های امنیتی(۵)- نبود توانمندی امنیتی در سازمان(۷)- بی توجهی به فرصت محیطی(۱۶)- نداشتن آینده نگری امنیتی(۳)- نبود نگاه صیانتی به سازمان(۱)-غفلت از تدبیر و متعهد نبودن به سازمان(۱۱)- بی توجهی به فرامین ولی فقیه(۳) |
| | شکست امنیتی | سهل انگاری در قراردادها، انتصابات و....(۵)- وجود حفره‌های امنیتی در سازمان (نبودرازداری،تحلیل نادرست، عدم رعایت حیطه‌بندی )(۴)- سهل انگاری در حفظ اسرارسازمانی(۱۱) نفوذ اطلاعاتی در سازمانها(۲۷). انتصاب افراد نااهل(۲۱)چرخش معیوب اطلاعات(۱)افشای اطلاعات درپی رسوخ امنیتی(۱)نقص در جمع آوری اطلاعات(۱۰)سهل انگاری در پوشش سازمانی در مشاغل حساس(۵) نبود اشراف اطلاعاتی جهت شناخت تهدیدات امنیتی(۲). گماردن مدیران بدون در نظرگرفتن هوش امنیتی(۶) |

| مقوله‌ها | کدگذاری محوری | کدگذاری باز (اعداد داخل پرانتز نشان‌دهنده تکرار مفاهیم است) |
|---|---|---|
| | تهدیدات امنیتی | -بد افزارها و نرم افزار مخرب غیربومی(۱)- مهاجمین اینترنتی(هکرها)(۱)- پیمانکاران فاقدصلاحیت امنیتی(۳)- عدم وفاداری کارکنان به سازمان(۲)- عدم ملاحظه امنیتی در ادغام و توزیع اطلاعات(۴)- افشای اطلاعات داده های غیرمجاز(۵)- تغییرات پیاپی غیرضرور(۳)- نفوذ اطلاعاتی جهت جاسوسی(۵)- تحریف و تفسیر نادرست داده‌ها(۶)- بی توجهی به پدافند غیرعامل(سلامت کارکنان وسیستم)(۳) بی‌توجهی به حفظ امنیت حریم خصوصی در ارتباطات مجازی(۲) |
| شرایط زمینه‌ای | رفتار امنیتی هوشمندانه بین مدیران | احساس مسئولیت امنیتی(۳). داشتن ذهن باز(۲). داشتن سوء ظن امنیتی(۳).عدم ترس در ارائه گزارش تخلفات امنیتی(۳). وجود قابلیت پیش‌بینی رفتار ضد امنیتی درسازمان(۴). وجود فرهنگ امنیتی مطلوب بین مدیران(۵) |
| | وجود ارتباط امنیتی هوشمندانه سازمانی | تعامل برون سازمانی(۳). شفافیت ساختارارتباطی(۵). شاخص سازی ارتباطات سازمانی(۶). جهت گیری امنیتی سازمانی(۴). عوامل فنی نفوذ ارتباط(۲). ایمن سازی تبادل اطلاعاتی(۳). اشراف اطلاعاتی جهت مقابله با نفوذ و تحریف امنیتی(۵) |
| | هدف‌گذاری امنیتی سازمانی | داشتن برنامه تاکتیکی، امنیتی(۵). داشتن برنامه عملیاتی امنیتی(۳). داشتن برنامه راهبردی امنیتی(۴). تحقق منابع مالی استقرارهوش امنیتی(۳). واقع‌گرایی در اهداف امنیتی(3). اولویت سنجی امنیتی(۸). هدف‌گذاری بازدارنده امنیتی(۵)تربیت نیرو با قابلیت امنیتی(۶) |
| شرایط مداخله‌گر | الزامات هوشمندسازی فنی و اداری | کمک به انجام کارهای ابتکاری و نو درسازمان(۲). امن سازی پردازش اطلاعات سازمانی(۳). جلوگیری از نشت اطلاعاتی سایبری(۵). کمک به تحقق دولت الکترونیک(۴). نیاز به بومی سازی نرم افزارهای سازمانی(۳)تعریف دسترسی کارکنان به اطلاعات فنی(۲). تعریف انتشار اطلاعات در سازمان(۸). نیاز به بهنگام سازی ساختار سازمانی(۴) |
| | الزامات استقرار هوش امنیتی | حساس بودن به حوادث امنیتی(۱). مشورت امنیتی در قراردادها و...(۲). احصای آسیب و تهدیدات امنیتی(۱۵). وجود سیاست امنیتی در سازمان(۴). پذیرش مسئولیت پذیری امنیتی(۳) ضرورت نظارت و کنترل امنیتی(۴). ایجاد بازدارندگی امنیتی(۵). تجزیه وتحلیل محیط امنیتی سازمانی(۳). وجود مدیران دارای هوش امنیتی(۵) |
| | الزامات تخصصی هوش امنیتی | ارتقای آموزش‌های تخصصی فناوری اطلاعات(۳). کمک به دانش ساخت ابزارهای فنی در داخل(۴). اجرای دقیق شیوه‌نامه‌های نوآوری هوش امنیتی(۲). آموزش تخصصی امنیتی و آگاه سازی حفاظتی(۷). شیوه نامه های اطلاعاتی جدید(۲). به‌کارگیری عوامل اجرایی متخصص(۱۱)ایجاد توانمندی امنیتی سازمان(۳) |
| | الزامات تعاملی هوش امنیتی | رابطه متقابل با مردم(۲). استفاده از تجربیات دیگران(۲). تعامل دستگاه‌های اطلاعاتی(۷). گزارش دهی اطلاعاتی(۱۰). عدم پنهان‌کاری مفرط در مناسبات حساس سازمان(۱۱). رعایت سلسله مراتب سازمانی(۱۱) |

| مقوله‌ها | کدگذاری محوری | کدگذاری باز (اعداد داخل پرانتز نشان‌دهنده تکرار مفاهیم است) |
|---|---|---|
| | الزامات مواجهه با دشمن | هوشیاری در مقابل تهدیدات دشمن(۳). رویکرد تهاجم اطلاعاتی(۴). بی اعتبارساختن دشمن(۵)شناخت راهکار دشمن(۷). ضرورت شناخت اطلاعاتی(۱۰).شناخت ظرفیت امنیتی سازمانی(۱۲). تدوین دستورالعمل امنیتی(۳) |
| | الزامات شرعی و قانونی | رعایت موازین شرعی(۳). توجه به انضباط معنوی(۴). وجود عوامل محوری و ارزشی (۵). خودسازی معنوی(۲).تعهد به ارزش‌های اخلاقی(۴). پیروی از ولایت فقیه(۹) |
| | الزامات معنوی و خودسازی | مراقبت از نفس(۲). اتصال به مبدا هستی(۵). رابطه با قرآن و نماز(۶). ولایت‌مداری (۱۲) |
| استراتژی و راهبردها | مدیریت هوشمند امنیتی | داشتن تهاجم اطلاعاتی(۴). جهت‌گیری امنیتی سازمانی(۲). شیوه سازماندهی امنیتی(۱). استفاده از نقطه نظرات مخالف(۵). توجیه امنیتی مدیران(۴). تأثیر اقدام پنهان بر تصمیم‌گیری(۶). گزینش نیروی دارای تفکرامنیتی(۴) |
| | طراحی سیستم هوش امنیتی راهبردی | ایجاد سطح بالای امنیت اطلاعات(۱)طراحی سیستم به‌هنگام شناسایی رخداد سایبری(۶). طراحی راهکار مقابله با نفوذ در شرکت‌ها(۹). مقابله با اعتبارزدایی حاکمیتی(۲). طراحی سیستم پیش بینی تغییر مخاطرات(۱۱) |
| | استقرار سامانه هوش امنیتی راهبردی | ارتقای سیستم ارزشیابی امنیتی سازمانی(۲). هوشمند سازی آموزش امنیتی(۳). ایجاد ارزیابی و نظارت الکترونیکی(۲)به‌هنگام سازی شناسایی رسوخ اطلاعاتی در سازمان(۲). رصد ۲۴ ساعته وقایع اطلاعاتی(۱) |
| | بهبود هوش امنیتی تاکتیکی | بهبود مدیریت شبکه(۷). ایجاد نوآوری در تاکتیک‌های امنیتی(۹). ارتقای دانش مدیران امنیتی(۱۱). زمان شناسی بحران سازمانی(۱۲) |
| | بهبود زیرساخت هوش امنیتی تکنیکی (فنی) | ارتقای سخت افزاری ابزارهای مقابله با نفوذ(۱). بهینه سازی سخت افزاری و نرم افزاری مقابله با بدافزارهای بومی(۶). بهبود زیرساخت سیستم پایش شبکه(۸). ارتقا و بهبود سرورهای کنترل (۱۰). ایجاد مرکز عملیات امنیت(۱۱) |
| نتایج و پیامدها | مدیریت افکار امنیتی سازمان | اعتماد سازی کارکنان(۳). قدرت اقناع سازی مدیران(۵). شناخت نگرش مدیران(۷) رفع تضاد های امنیتی سازمانی(۸) اثرگذاری امنیتی در حفاظت روانی کارکنان(۹)آگاه‌سازی حفاظتی در مجموعه سازمان(۱۰) |
| | ارتقای عملکرد امنیتی سازمانی | پیشگیری تهدیدات امنیتی(۲). جلوگیری از نفوذ فردی و جریانی(۶). شناسایی مخل امنیت سازمانی(۵). فرهنگ سازی پاسخگویی امنیتی(۷)جلوگیری از رانت اطلاعاتی(۵). برخورد امنیتی با مخاطرات امنیتی(۶). رتبه بندی امنیتی سازمان(۶) توجه به بانک اطلاعاتی(۲). ارزیابی امنیتی عملکرد مدیران(۱۱). به‌کارگیری هوش امنیتی جهت انتصابات مدیران درکنار صلاحیت عمومی و تخصصی(۱۲) |

| مقوله‌ها | کدگذاری محوری | کدگذاری باز (اعداد داخل پرانتز نشان‌دهنده تکرار مفاهیم است) |
|---|---|---|
| | پیاده سازی عملی هوش امنیتی | کاهش تهدیدات(۵). کاهش سطح عدم انطباق(۳). تسهیل تصمیم گیری‌های امنیتی(۲). خودکار نمودن فرآیندهای امنیتی(۴). تحقق اهداف امنیتی در سازمان (حفاظت از دارایی‌های مادی و معنوی)(۳). کاهش ریسک امنیتی در کسب و کار(۲)انتصابات مدیران براساس توان امنیتی(افزایش بعد توانمندی مدیران درکنارصلاحیت تخصصی و عمومی)(۸). جلوگیری از نفوذ(۴).عدم غافلگیری امنیتی با به‌کارگیری مدیران دارای هوش امنیتی(۶) |

با توجه به یافته‌های تحقیق مدل مفهومی پژوهش در قالب الگوی پارادایمی (شکل ۲)، ارائه می‌گردد:




شکل (۲) مدل پژوهش براساس نتایج تحلیل محتوای بخش کیفی

روایی این بخش پژوهش از سه طریق زیر بررسی شده است: روایی محتوا: یکی از روش‌ها برای ارزیابی و تضمین روایی محتوا شکل‌گیری معقول ابزار است و همه گویه‌های پرسشنامه ابتدا به وسیله تعدادی از صاحب‌نظران متخصص این حوزه بررسی شده و بر اساس بازخورد آنها و به منظور کاهش ابهامات، پرسشنامه اولیه اصلاح و پرسشنامه نهایی تدوین شده است لذا می‌توان از روایی محتوایی آن اطمینان پیدا کرد. این پرسشنامه از ۱۵۰ سؤال تشکیل و با استفاده از طیف لیکرت پنج درجه‌ای به عنوان مقیاس مورد نظر طراحی گردیده است.

جهت بررسی روایی ابزارهای اندازه‌گیری و سازه‌های پژوهش، دو شاخص مورد بررسی قرار می‌گیرد. روایی همگرا: منظور از شاخص روایی همگرا سنجش میزان تبیین متغیر پنهان توسط متغیرهای مشاهده‌پذیر آن است. (هر جر و دیگران[۵۴]، ۲۰۱۷). نتایج بررسی مقادیر واریانس استخراج شده متغیرهای پنهان پژوهش نشان داد که همه متغیرها مقادیری بیش از ۰/۵ به خود اختصاص دادند. بر این اساس می‌توان گفت: روایی همگرای ابزارهای اندازه‌گیری با استفاده از شاخص میانگین واریانس استخراج شده[۵۵]، تأیید شد. روایی واگرا( افتراقی) در تحقیق حاضر جهت روایی افتراقی، از آزمون فورنل– لارکر،برای هر یک از متغیرها محاسبه شده است. بر این اساس نتایج به‌دست‌آمده ،جذر میانگین استخراج شده هر متغیر پنهان، بیشتر از حداکثر همبستگی آن متغیر پنهان با متغیرهای پنهان دیگر است. بر این اساس روایی واگرا مدل اندازه-گیری با استفاده از آزمون فورنل- لارکر هم تأیید شد.

پایایی پرسشنامه: به منظور بررسی پایایی پرسشنامه از ضریب آلفای کرونباخ استفاده شد که از طریق نرم افزار اس. پی.اس. اس، محاسبه گردید. مقدار هر سؤالات پرسشنامه برابر ۰/۹۴۵ شد که مقدار قابل توجهی جهت پایا بودن پرسشنامه است. همانگونه‌که در جدول بالا ملاحظه می‌گردد و از آنجایی‌که ضریب آلفای کرونباخ بالاتر از ۰/۷ قابل قبول است، در نتیجه آلفای کرونباخ تمامی سؤالات پرسشنامه مورد قبول است و پایایی پرسشنامه تأیید می‌گردد.

## آمار توصیفی

با توجه به تجزیه و تحلیل داده‌های جمع‌آوری شده از طریق نرم افزار اس.پی.اس.اس می‌توان اطلاعات حاصله را به صورت زیر بیان نمود:

جدول (۲) مشخصات پاسخ دهندگان

| **سطح تحصیلات پاسخ دهندگان** | | | | | |
|---|---|---|---|---|---|
| کارشناس | ۳۸٪/۲۷ | کارشناس ارشد | ۳۸٪/۸۹ | دکتری | ۲۲٪/۸۴ |
| **سن پاسخ دهندگان** | | | | | |
| ۲۰–۳۵ سال | ۱۲٪/۹۶ | ۳۵–۴۰ سال | ۵۴٪/۹۴ | ۴۰ سال به بالا | ۳۲٪/۱۰ |
| **سابقه کاری** | | | | | |
| ۵–۱۰ سال | ۲۸٪/۴۰ | ۱۰–۱۵ سال | ۴۰٪/۷۴ | ۱۵–۲۰ سال | ۲۷٪/۷۸ | ۲۰ سال به بالا | ۳٪/۰۹ |

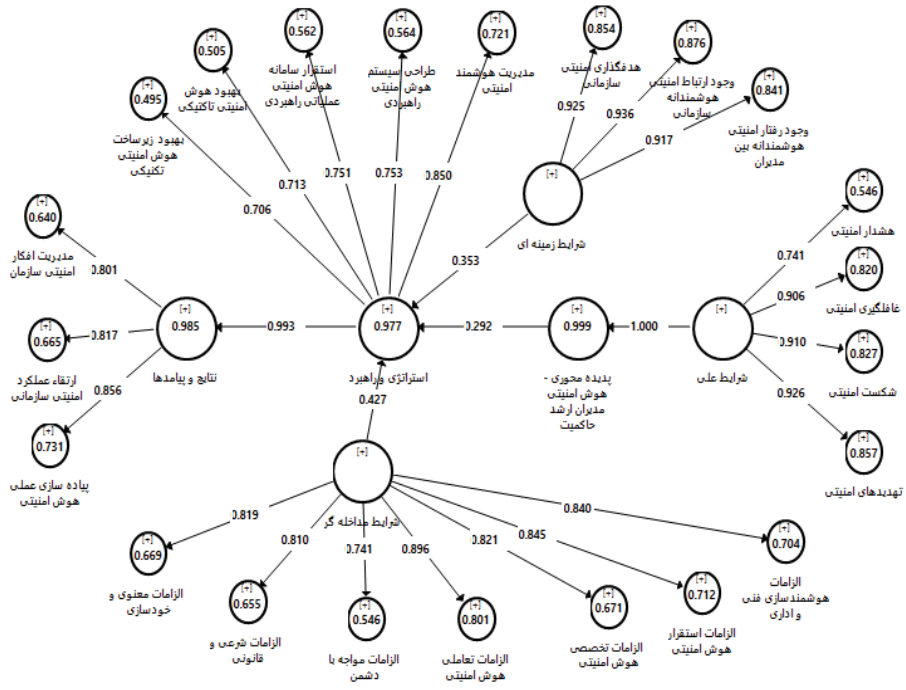
54. Hair Jr et al

55. Average Variance Extracted (AVE)

## ارزیابی مدل‌مفهومی با استفاده نرم افزار smart pls

در این بخش از تحقیق مدل مفهومی پژوهش که از نوع ترکیبی است با استفاده از تکنیک مدل یابی معادلات ساختاری به روش حداقل مجذورات جزئی (PLS) آزمون شد. نرم‌افزار مورد استفاده Smart PLS است. (حبیبی، آرش و مریم عدن ور، ۱۳۹۶) PLS کمترین مجذورات جزئی به‌عنوان یک روش خطی، پیش‌بینی و تبیین و نه تفسیری معرفی می‌شود. استفاده از این روش، قبل از استفاده روش‌های تفسیری مانند رگرسیون خطی چندگانه (SEM Structural Equation Modeling) توصیه می‌گردد (عباس زاده و دیگران، ۱۳۹۳).

مدل پژوهش با استفاده از تکنیک حداقل مجذورات جزئی و با نرم‌افزار Smart Pls مورد آزمون قرار گرفت. در این مدل، تمامی روابط هم‌زمان مورد تحلیل قرار گرفتند. در ادامه مدل پژوهش در حالت ضرایب استانداردشده (شکل (۳) و در حالت مقدار t (معنی داری) جدول(۲) ارائه شده است.




شکل(۳) آزمون مدل پژوهش در حالت ضرایب استانداردشده

با توجه به مدل پژوهش ضرایب استانداردشده، انحراف استاندار، آماره T و مقدار احتمال (P) به صورت جدول زیر است:

جدول (۳) نتایج اجرای مدل ساختاری

| مسیرهای ساختاری | ضرایب مسیر | انحراف استاندارد (STDEV) | آماره T | مقادیر P |
|---|---|---|---|---|
| شرایط علی -> تهدیدهای امنیتی | ۰.۹۲۶ | ۰.۰۱۰ | ۹۶.۴۱۹ | ۰.۰۰۰ |
| شرایط علی -> شکست امنیتی | ۰.۹۱۰ | ۰.۰۱۰ | ۹۲.۰۳۶ | ۰.۰۰۰ |
| شرایط علی -> غافلگیری امنیتی | ۰.۹۰۶ | ۰.۰۱۳ | ۶۷.۸۱۷ | ۰.۰۰۰ |
| شرایط علی -> هشدار امنیتی | ۰.۷۴۱ | ۰.۰۵۸ | ۱۲.۸۶۳ | ۰.۰۰۰ |
| شرایط علی -> پدیده محوری –هوش امنیتی مدیران ارشد حاکمیت | ۱.۰۰۰ | ۰.۰۰۰ | ۳۹۹۰.۱۴۳ | ۰.۰۰۰ |
| پدیده محوری – هوش امنیتی مدیران ارشد حاکمیت -> استراتژی و راهبرد | ۰.۲۹۲ | ۰.۰۴۱ | ۷.۱۲۳ | ۰.۰۰۰ |
| شرایط مداخله‌گر_ -> استراتژی و راهبرد | ۰.۴۲۷ | ۰.۰۳۲ | ۱۳.۲۵۱ | ۰.۰۰۰ |
| شرایط مداخله‌گر_ -> الزامات استقرار هوش امنیتی | ۰.۸۴۵ | ۰.۰۱۵ | ۵۵.۷۵۳ | ۰.۰۰۰ |
| شرایط مداخله‌گر_ -> الزامات تخصصی هوش امنیتی | ۰.۸۲۱ | ۰.۰۲۶ | ۳۲.۱۴۷ | ۰.۰۰۰ |
| شرایط مداخله‌گر_ -> الزامات تعاملی هوش امنیتی | ۰.۸۹۶ | ۰.۰۱۶ | ۵۷.۷۶۸ | ۰.۰۰۰ |
| شرایط مداخله‌گر_ -> الزامات شرعی و قانونی | ۰.۸۱۰ | ۰.۰۲۹ | ۲۸.۱۹۶ | ۰.۰۰۰ |
| شرایط مداخله‌گر_ -> الزامات معنوی و خودسازی | ۰.۸۱۹ | ۰.۰۲۲ | ۳۶.۴۵۳ | ۰.۰۰۰ |
| شرایط مداخله‌گر_ -> الزامات مواجهه با دشمن | ۰.۷۴۱ | ۰.۰۳۷ | ۱۹.۹۶۴ | ۰.۰۰۰ |
| شرایط مداخله‌گر_ -> الزامات هوشمندسازی فنی و اداری | ۰.۸۴۰ | ۰.۰۳۲ | ۲۶.۲۳۳ | ۰.۰۰۰ |
| شرایط زمینه‌ای -> استراتژی و راهبرد | ۰.۳۵۳ | ۰.۰۳۹ | ۹.۰۱۵ | ۰.۰۰۰ |
| شرایط زمینه‌ای -> هدف‌گذاری امنیتی سازمانی | ۰.۹۲۵ | ۰.۰۰۷ | ۱۴۰.۱۵۰ | ۰.۰۰۰ |
| شرایط زمینه‌ای -> وجود ارتباط امنیتی هوشمندانه سازمانی | ۰.۹۳۶ | ۰.۰۱۱ | ۸۸.۹۸۷ | ۰.۰۰۰ |
| شرایط زمینه ای -> وجود رفتار امنیتی هوشمندانه بین مدیران | ۰.۹۱۷ | ۰.۰۱۲ | ۷۴.۱۳۱ | ۰.۰۰۰ |
| استراتژی و راهبرد -> استقرار سامانه هوش امنیتی عملیاتی راهبردی | ۰.۷۵۱ | ۰.۰۲۷ | ۲۷.۸۱۶ | ۰.۰۰۰ |
| استراتژی و راهبرد -> بهبود زیرساخت هوش امنیتی تکنیکی | ۰.۷۰۶ | ۰.۰۴۷ | ۱۵.۱۱۲ | ۰.۰۰۰ |
| استراتژی و راهبرد -> بهبود هوش امنیتی تاکتیکی | ۰.۷۱۳ | ۰.۰۲۸ | ۲۵.۶۸۵ | ۰.۰۰۰ |

| | | | | |
|---|---|---|---|---|
| استراتژی و راهبرد -> بهبود هوش امنیتی تاکتیکی | ۰.۷۱۳ | ۰.۰۲۸ | ۲۵.۶۸۵ | ۰.۰۰۰ |
| استراتژی و راهبرد -> طراحی سیستم هوش امنیتی راهبردی | ۰.۷۵۳ | ۰.۰۳۰ | ۲۴.۸۴۱ | ۰.۰۰۰ |
| استراتژی و راهبرد -> مدیریت هوشمند امنیتی | ۰.۸۵۰ | ۰.۰۱۷ | ۴۹.۵۱۲ | ۰.۰۰۰ |
| استراتژی و راهبرد -> نتایج و پیامدها | ۰.۹۹۳ | ۰.۰۰۱ | ۱۲۲۴.۴۰۱ | ۰.۰۰۰ |
| نتایج و پیامدها -> ارتقای عملکرد امنیتی سازمانی | ۰.۸۱۷ | ۰.۰۳۰ | ۲۷.۱۵۰ | ۰.۰۰۰ |
| نتایج و پیامدها -> مدیریت افکار_امنیتی سازمان | ۰.۸۰۱ | ۰.۰۲۶ | ۳۱.۴۰۷ | ۰.۰۰۰ |
| نتایج و پیامدها -> پیاده سازی عملی هوش امنیتی | ۰.۸۵۶ | ۰.۰۱۴ | ۵۹.۸۱۵ | ۰.۰۰۰ |

با توجه به نتایج به‌دست‌آمده از جدول (۲)، آماره T ، معنی دار بودن روابط متغیرهای مدل را نشان می‌دهد، زیرا مقدار احتمال این آماره کمتر از ۰/۰۵ است. به عبارت دیگر آزمون معنی‌داری ضرایب مسیر، نشان می‌دهد که همه آنها از نظر آماری معنادار و اثر آنها تأیید می‌شود. این موضوع بدین معنی است که مؤلفه‌های تدوین شده در مدل پارادایمی از قابلیت اعتماد مناسبی برخوردار هستند.

## برازش مدل ساختای

در پژوهش حاضر، جهت بررسی برازش مدل ساختاری، دو شاخص مورد بررسی قرار می‌گیرد که شامل:

### ضریب تعیین تعدیل شده($R^2$)،

جدول (۴) نتایج ضریب تعیین و ضریب تعیین تعدیل شده

| متغیرهای مکنون درون‌زای مدل تحقیق | R Square | R Square Adjusted |
|---|---|---|
| شرایط علی | — | — |
| هشدار امنیتی | ۰,۵۵ | ۰,۵۵ |
| غافلگیری امنیتی | ۰,۸۲ | ۰,۸۲ |
| شکست امنیتی | ۰,۸۳ | ۰,۸۳ |
| تهدیدهای امنیتی | ۰,۸۶ | ۰,۸۶ |
| پدیده محوری –هوش امنیتی مدیران ارشد حاکمیت | ۱,۰۰ | ۱,۰۰ |
| شرایط مداخله گر | — | — |
| الزامات هوشمندسازی فنی و اداری | ۰,۷۱ | ۰,۷۰ |
| الزامات استقرار هوش امنیتی | ۰,۷۱ | ۰,۷۱ |
| الزامات تخصصی هوش امنیتی | ۰,۶۷ | ۰,۶۷ |
| الزامات تعاملی هوش امنیتی | ۰,۸۰ | ۰,۸۰ |

| | | |
|---|---|---|
| مدیریت هوشمند امنیتی | ۰,۷۲ | ۰,۷۲ |
| طراحی سیستم هوش امنیتی راهبردی | ۰,۵۷ | ۰,۵۶ |
| استقرار سامانه هوش امنیتی عملیاتی راهبردی | ۰,۵۶ | ۰,۵۶ |
| بهبود هوش امنیتی تاکتیکی | ۰,۵۱ | ۰,۵۱ |
| بهبود زیرساخت هوش امنیتی تکنیکی (فنی) | ۰,۵۰ | ۰,۵۰ |
| پیامدها و نتایج | ۰,۹۹ | ۰,۹۹ |

| متغیرهای مکنون درون‌زای مدل تحقیق | R Square | R Square Adjusted |
|---|---|---|
| مدیریت افکار امنیتی سازمان | ۰,۶۴ | ۰,۶۴ |
| ارتقای عملکرد امنیتی سازمانی | ۰,۶۷ | ۰,۶۷ |
| پیاده سازی عملی هوش امنیتی | ۰,۷۳ | ۰,۷۳ |

ضریب تعیین (R۲) متغیرهای مکنون درون‌زا، معیاری ضروری برای سنجش برازش مدل ساختاری است. چین (۱۹۸۸) مقادیر ضریب تعیین ۰/۶۷، ۰/۳۳ و ۰/۱۹ در مدل مسیر PLS را به ترتیب قابل توجه، متوسط و ضعیف، توصیف می‌کند. اگر سازه‌های مدل درونی خاصی متغیرهای مکنون درون‌زا را تنها با ۱ یا ۲ متغیر مکنون برون‌زا تبیین کنند، ضریب تعیین متوسط (۰/۳۳) قابل قبول است. اما گر متغیرهای مکنون درون‌زا وابسته به چندین متغیر برون‌زا هستند، ارزش ضریب تعیین باید حداقل در سطح قابل‌توجه (۰/۶۷) باشد(هر جر و دیگران، ۲۰۱۷). بر همین اساس برابر جدول شماره(۲) ، نتایج ضریب تعیین و ضریب تعیین تعدیل شده بیان گردیده در سطح قابل قبول قرار دارند.

## قدرت مدل یا اعتبار افزونگی[۵۶] (Q۲)

جدول (۵) نتایج توان پیش‌بینی مدل یا اعتبار افزونگی

| متغیرهای مکنون درون‌زای مدل تحقیق | SSO | SSE | Q² (=1-SSE/SSO) |
|---|---|---|---|
| شرایط علی | — | — | — |
| هشدار امنیتی | ۸۱۰.۰۰ | ۶۳۶.۶۳ | ۰.۲۱ |
| غافلگیری امنیتی | ۱,۱۳۴.۰۰ | ۷۹۲.۸۸ | ۰.۳۰ |
| شکست امنیتی | ۱,۴۵۸.۰۰ | ۱,۰۵۹.۳۸ | ۰.۲۷ |
| تهدیدهای امنیتی | ۱,۶۲۰.۰۰ | ۱,۱۶۳.۷۲ | ۰.۲۸ |

| | | | |
|---|---|---|---|
| پدیده محوری ـ هوش امنیتی مدیران ارشد حاکمیت | ۵,۰۲۲.۰۰ | ۳,۶۶۲.۹۵ | ۰.۲۷ |
| شرایط مداخله‌گر | — | — | — |
| الزامات هوشمند سازی فنی و اداری | ۱,۴۵۸.۰۰ | ۱,۰۸۲.۴۳ | ۰.۲۶ |
| الزامات استقرار هوش امنیتی | ۱,۲۹۶.۰۰ | ۹۲۵.۱۹ | ۰.۲۹ |
| الزامات تخصصی هوش امنیتی | ۱,۱۳۴.۰۰ | ۷۶۵.۲۸ | ۰.۳۳ |

| متغیرهای مکنون درون‌زای مدل تحقیق | SSO | SSE | $Q^2$ (=1-SSE/SSO) |
|---|---|---|---|
| الزامات تعاملی هوش امنیتی | ۹۷۲.۰۰ | ۶۵۰.۳۱ | ۰.۳۳ |
| الزامات مواجه با دشمن | ۱,۱۳۴.۰۰ | ۸۹۷.۵۰ | ۰.۲۱ |
| الزامات شرعی و قانونی | ۹۷۲.۰۰ | ۷۰۱.۵۹ | ۰.۲۸ |
| الزامات معنوی و خودسازی | ۶۴۸.۰۰ | ۴۱۶.۴۰ | ۰.۳۶ |
| شرایط زمینه‌ای | — | — | — |
| وجود رفتار امنیتی هوشمندانه بین مدیران | ۹۷۲.۰۰ | ۶۰۱.۳۴ | ۰.۳۸ |
| وجود ارتباط امنیتی هوشمندانه سازمانی | ۱,۱۳۴.۰۰ | ۷۲۴.۸۵ | ۰.۳۶ |
| هدف‌گذاری امنیتی سازمانی | ۱,۲۹۶.۰۰ | ۸۴۰.۱۶ | ۰.۳۵ |
| استراتژی و راهبرد | ۲۰,۲۵۰.۰۰ | ۱۵,۳۵۸.۷۸ | ۰.۲۴ |
| مدیریت هوشمند امنیتی | ۱,۱۳۴.۰۰ | ۸۱۱.۶۲ | ۰.۲۸ |
| طراحی سیستم هوش امنیتی راهبردی | ۸۱۰.۰۰ | ۶۰۳.۹۵ | ۰.۲۵ |
| استقرار سامانه هوش امنیتی عملیاتی راهبردی | ۸۱۰.۰۰ | ۶۱۳.۷۰ | ۰.۲۴ |
| بهبود هوش امنیتی تاکتیکی | ۸۱۰.۰۰ | ۶۳۲.۵۸ | ۰.۲۲ |
| بهبود زیرساخت هوش امنیتی تکنیکی (فنی) | ۶۴۸.۰۰ | ۴۷۴.۵۵ | ۰.۲۷ |
| پیامدها و نتایج | ۲۴,۳۰۰.۰۰ | ۱۸,۴۲۷.۱۱ | ۰.۲۴ |
| مدیریت افکار امنیتی سازمان | ۹۷۲.۰۰ | ۷۰۰.۹۷ | ۰.۲۸ |
| ارتقای عملکرد امنیتی سازمانی | ۱,۶۲۰.۰۰ | ۱,۲۲۲.۴۵ | ۰.۲۵ |
| پیاده سازی عملی هوش امنیتی | ۱,۴۵۸.۰۰ | ۱,۰۸۵.۳۴ | ۰.۲۶ |

56. CV-Redundancy

قدرت پیش‌بینی مدل یا اشتراک افزونگی[۵۷] معیار دیگری برای بررسی برازش مدل ساختاری است. مقادیر به‌دست‌آمده از این آزمون برابر جدول (۳) مثبت است، که نشان دهنده کیفیت مناسب مدل ساختاری است. در مورد قدرت پیش‌بینی مدل در مورد متغیرهای پنهان درون زا سه مقدار ۰/۰۲، ۰/۱۵ و ۰/۳۵ به ترتیب به عنوان مقادیر ضعیف، متوسط و قوی برای این شاخص معرفی شده‌اند (سرستدت و دیگران، ۲۰۱۷). برهمین اساس، نتایج توان پیش‌بینی مدل یا اعتبار افزونگی بیان‌شده در سطح قابل قبول قرار دارند.

لذا با توجه به نتایج مدل اندازه‌گیری و ساختاری، برابر جداول(۲و۳) می‌توان نتیجه گرفت که مدل تدوین شده در بخش کیفی شکل (۱) از روایی و پایایی قابل قبولی برخوردار است و می‌تواند به عنوان یک مدل قابل اعتماد برای تبیین مدل هوش امنیتی مدیران ارشد حاکمیت، به‌کار گرفته شود.

## نتیجه‌گیری و ارائه پیشنهاد

امنیت در گذشته در پرتو قدرت نظامی تحقق پیدا می‌کرد ولی امروزه با تحولی که در فناوری ارتباطات و اطلاعات به وجود آمده؛ در ابعاد گسترده‌تری اهمیت یافته و احساس ضرورت آن نه تنها 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 گسترده شدن مفهوم امنیت در عصر حاضر شده است. همانطورکه در جهان واقعی، انسان‌های موفق افرادی هستند که استعدادی سرشار داشته و از هوش بالایی برخوردار می‌باشند، قطعاً در سازمان‌ها نیز چنین است؛ به‌خصوص در زمان فعلی هرچه زمان به جلو حرکت می‌کند، به علت پیشرفت علوم و فنون و به وجود آمدن 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 به دنبال مدیریت همه جانبه اطلاعات امنیتی در سازمان است. بخشی از این اطلاعات از طریق گزارشاتی که به صورت دستی و موردی تهیه می‌شوند، تشکیل شده است و بخش دیگری از گزارشات و فعالیت‌ها نیز به صورت خودکار توسط سیستم‌های امنیتی مستقر شده در سازمان تولید می‌شوند. هوش امنیتی در واقع با به‌کارگیری مهارت‌های لازم در جهت جمع‌آوری، یکپارچه سازی و تحلیل تمام اطلاعات مذکور به دنبال مدیریت و در نهایت بهینه سازی و افزایش هوشمندی سازمان در امور امنیتی است.

57. CV Red

در تحقیق حاضر به منظور جمع‌آوری داده‌ها و اطلاعات برای تجزیه و تحلیل بخش کیفی، از مصاحبه و روش گراندد تئوری، استفاده شد. پس از پیاده سازی مصاحبه‌ها، کدگذاری مصاحبه‌ها در سه سطح کدگذاری اولیه، محوری و گزینشی انجام گرفت. کدگذاری در مرحله اول با توجه به کلی بودن و باز بودن، کدگذاری اولیه محسوب می‌شود. در مرحله بعد از این نوع کدگذاری، کدگذاری ثانویه انجام گرفت که در آن کدهای اولیه به علت تعداد فراوان در قالب طبقه‌های مشابه یا همان کدهای ثانویه به یک کد مفهومی تبدیل شدند. در ادامه با استفاده از مدل یابی معادلات ساختاری، مدل تحقیق برازش کلیه روابط تأیید شد.

نتایج تحقیق برابر سؤال‌های تحقیق جهت شناسایی مدل هوش امنیتی مدیران ارشد در پنج سطح تقسیم‌بندی بیان می‌گردد.

- جهت پیاده‌سازی هوش امنیتی مدیران ارشد حاکمیت؛ باید ضرورت توجه به نشانه شناسی امنیتی، هشدار امنیتی، عدم غافلگیری امنیتی، جلوگیری از شکست امنیتی و مهار تهدیدهای امنیتی را مد نظر قرار دهند و به‌عنوان مؤلفه‌های جدید برای انتصاب مدیران در مشاغل حساس و کلیدی در نظر گرفته شود.
- توجه و رعایت به الزامات هوشمندسازی فنی و اداری، استقرار هوش امنیتی، تخصصی هوش امنیتی، تعاملی هوش امنیتی، مواجهه با دشمن، شرعی، قانونی، معنوی و خودسازی در راستای ارتقای فرآیندهای هوش امنیتی را باید به‌کار بندند.
- وجود رفتار امنیتی هوشمندانه مدیران، ارتباط امنیتی هوشمندانه سازمانی و هدف‌گذاری امنیتی سازمانی موجبات افزایش اعتماد کارکنان و تحقق قابلیت هوش امنیتی مدیران ارشد را فراهم می‌آورد.
- با راه‌اندازی مدیریت هوشمند امنیتی، طراحی سیستم هوش امنیتی راهبردی، استقرار سامانه هوش امنیتی عملیاتی راهبردی، بهبود هوش امنیتی تاکتیکی، بهبود زیرساخت هوش امنیتی تکنیکی(فنی) موجب تحقق راهبردهای هوش امنیتی می‌گردد.
- با استقرار هوش امنیتی در سازمان، مدیران می‌توانند ضمن مدیریت بر افکار امنیتی کارکنان، موجب ارتقای عملکرد امنیتی فردی و متعاقب آن سازمانی گردیده و به‌صورت عملیاتی اقدام به پیاده سازی هوش امنیتی نمایند.
- رسیدن به‌هدف غایی زیر از طراحی و تبیین مدل هوش‌امنیتی مدیران ارشد حاکمیت توسط محقق:

• تحقق منویات مقام معظم رهبری(مدظله‌العالی) درحوزه نفوذ با پیاده سازی هوش امنیتی مدیران ارشد حاکمیت.

• فرهنگ سازی هوش امنیتی مدیران جهت مقابله با تهدیدات و آسیب‌های سازمانی.

• ابزاری جهت سنجش هوش امنیتی مدیران برای انتصاب در مشاغل حساس و حیاتی در ساختار حاکمیت.

• تحقق اهداف بنیادی محقق از مدل طراحی شده به‌عنوان تولید علم (خلق واژه هوش امنیتی) با رویکرد بومی‌گزینی.

**با توجه به یافته‌های تحقیق جهت استقرار و پیاده‌سازی هوش امنیتی راه‌کارهای زیر پیشنهاد می‌گردد**

ـ جهت هرگونه انتصاب بایستی الزامات طی گردد از جمله دوره‌های آموزشی توجیه حفاظتی نوبه‌ای و دوره‌های آموزشی حین خدمت که نهایت این دوره‌ها بایستی منجر به تغییر رفتار و باعث ایجاد حساسیت نسبت به امور گردیده و مدیران با رویکرد حفاظتی تقویت گردند.

ـ انتصاب مدیران بر مبنای صلاحیت امنیتی با تأکید بر هوش امنیتی باشد.

ـ شرایط زمینه‌ای هوش امنیتی در هر سازمان نباید بر پایه ایجاد ترس حاکم باشد و باعث ایحاد حساسیت گردد.

ـ توجه به رفتار سازمانی و فرهنگ سازی شناخت تهدیدات سازمانی می‌تواند عامل تعیین کننده هوش امنیتی مدیران و کارکنان باشد.

ـ مورد تشویق قراردادن مدیران دارای رفتار هوشمندانه امنیتی، ضریب هوشی امنیتی و توانمندی ادراکی و ذهنی در حوزه امنیت سازمان متبوع

ـ استقرار سامانه ارزیابی امنیتی در سازمان‌ها جهت تعیین میزان خسارات شکست امنیتی و عملکرد امنیتی مدیران ارشد حاکمیت در سازمان‌ها

ـ نهادینه سازی فرهنگ امنیتی در سازمان در انعکاس موارد خسارات امنیتی بر مبنای وظایف سازمانی

ـ طراحی نرم افزار جهت سنجش هوش امنیتی مدیران ارشد جهت انتصابات

ـ با بهبود مدیریت شبکه، ایجاد نوآوری در تاکتیک‌های امنیتی و ارتقا دانش مدیران امنیتی، بهبود هوش امنیتی تاکتیکی را در ساختارهای حاکمیت، مد نظر قرار دهند.

ـ با سلسله اقداماتی نظیر اعتمادسازی درکارکنان، شناخت نگرش‌های متفاوت مخاطبان، رفع تضادهای امنیتی سازمانی ، اثرگذاری امنیتی در حفاظت روانی کارکنان و آگاه سازی حفاظتی در ساختار حاکمیت نهادینه شود.

## منابع و مآخذ

### الف) منابع فارسی


۱. آدینه، شهرضا (۱۳۸۹)، هوشمند سازی امنیت و مقابله با تهدیدات پیشرفته، تهران: موسسه فرهنگی هنری دیباگران.

۲. اکبرزاده، نسرین (۱۳۸۳)، هوش هیجانی از دیدگاه سالوی و دیگران، تهران: انتشارات فارابی.

۳. الوانی، مهدی و دیگران (۱۳۸۹)، «تحلیل اخلاق سازمانی کارکنان با استفاده از الگوی دایره اخلاق»، فصلنامه اخلاق در علوم و فناوری، سال پنجم، شماره‌های ۳و۴، ۲۵-۳۴.

۴. بازرگان‌هرندی، عباس و دیگران (۱۳۹۷)، روش‌های تحقیق در علوم رفتاری، آگه.

۵. برادبری، تراویس و جین گریوز (۱۳۸۸)،« هوش هیجانی (مهارت‌ها و آزمون‌ها)»، ترجمه مهدی گنجی، تهران: نشر ساوالان.

۶. تسلیمی، محمدسعید و دیگران (۱۳۸۸)،« ارائه راه‌کارهایی برای ارتقایِ هوش فرهنگی مدیران دولتی در امور بین‌المللی»، پژوهش‌های مدیریت، سال ۲، ۲۹-۵۷.

۷. جفری ام، مارویاما (۱۳۹۰)، اصول مدل سازی معادلات ساختاری، ترجمه صمد رسول زاده اقدم، پژوهشکده مطالعات فرهنگی اجتماعی.

۸. حبیبی، آرش و مریم عدن ور (۱۳۹۶)، مدل‌یابی معادلات ساختاری و تحلیل عاملی (آموزش کاربردی نرم‌افزار LISREL)، سازمان انتشارات جهاد دانشگاهی.

۹. درویش سه ثلاثی، فرهاد (۱۳۷۴)، تهدیدات امنیت ملی یک چارچوب نظری مجله سیاست دفاعی، سال سوم شماره ۱۰ و ۱۱.

۱۰. رضایت، غلامحسین و فیض‌اله مرادیان (۱۳۹۵)، ارائه الگوی راهبردی حفاظت اطلاعات اسلامی، دانشگاه عالی دفاع ملی (دانشکده امنیت ملی)، ۶(۲۲)، ۶۹-۹۴.

۱۱. رضاییان، علی (۱۳۸۴)، اصول مدیریت، چاپ هفدهم، تهران: سمت.

۱۲. رمضانی، نبی الله (۱۳۹۴)، ابعاد نفوذ دشمن و راه‌کارهای مقابله با آن، پایان‌نامه کارشناسی ارشد رشته علوم سیاسی، دانشگاه آزاد اسلامی واحد تهران شمال.

۱۳. سایت مقام معظم رهبری(KHAMENEI.IR)

۱۴. سیف، علی اکبر (۱۳۹۸)، روانشناسی پرورشی نوین: روانشناسی یادگیری و آموزش. دوران.

۱۵. عاطف، رضا (۱۳۷۸)، «بررسی اطلاعات»، تهران: دانشکده و پژوهشکده اطلاعات و امنیت.
۱۶. عرفانی‌خانقاهی، معصومه و پریوش جعفری (۱۳۸۹)،« هوش سازمانی و ارتقای آن در دانشگاه»، تهران: فراشناختی اندیشه.
۱۷. عصاریان نژاد، حسین (۱۳۹۴)، تقریرات درسی روش شناسی محیطی، تهران: داعا.
۱۸. علاقه‌بند، علی(۱۳۸۸)، مدیریت عمومی، چاپ بیستم، ویرایش دوم، تهران: روان.
۱۹. قریب، حسین (۱۳۸۰)، «جهانی شدن و چالش‌های امنیتی ایران» ۱۳۸۰ اطلاعات سیاسی-اقتصادی مرداد و شهریور.
۲۰. کاتوزیان، ناصر (۱۳۷۳)، مقدمه علم حقوق، چاپ هجدهم، تهران.
۲۱. کرسول، جان دبلیو (۱۳۹۶)، طرح پژوهش، رویکرد کمی، کیفی و ترکیبی، ترجمهٔ علیرضا کیامنش و مریم دانای طوس، تهران: جهاد دانشگاهی واحد علامه طباطبایی.
۲۲. کریمی، رامین (۱۳۹۴)، راهنمای آسان تحلیل آماری با SPSS. هنگام.
۲۳. ماندل، رابرت (۹۷۳۱)، چهره متغیر امنیت ملی، ترجمهٔ پژوهشکده مطالعات راهبردی، چاپ دوم.
۲۴. میرزایی، سعید (۱۳۹۵)، بررسی عوامل مؤثر بر امنیت اجتماعی شهروندان شهر جدید پرند، در سومین کنفرانس بین المللی پژوهش‌های نوین در علوم انسانی.
۲۵. نای، جوزف (۱۳۸۷)، قدرت نرم ابزارهای موفقیت در سیاست بین‌الملل، ترجمه سید محسن روحانی و مهدی ذوالفقاری، تهران: دانشگاه امام صادق (ع).
۲۶. هافندرون، هلگا (۱۷۳۱)، معمای امنیت، نظریه‌پردازی و ایجاد قواعد در زمینه‌های بین‌المللی، ترجمهٔ علیرضا طیب، تهران: دفتر مطالعات سیاسی و بین‌المللی
۲۷. هندیانی، عبداله (۱۳۸۶)، بررسی تحولات مفهومی در محیط امنیتی، فصلنامه دانش انتظامی، شماره ۳۵،ص ۷-۳۰.
۲۸. یحیائی، مهری و دیگران (۱۳۹۵)، هوش امنیتی، برگرفته از سایت اینترنتی.

**الف) منابع لاتین**

1. Crump, Justin. (2015). Corporate security intelligence and strategic decision making. Crc press.
2. Gardner, Howard. (2006). Intelligence reframed: Multiple intel-

ligences 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. Dong, T.; Cheng, N. & Wu, Y. J.(2014). A study of the social networking website service in digital content industries: The Facebook case in Taiwan, Computers in Human Behavior, 30, pp 708-714
6. Sallos, Mark Paul; Garcia-Perez, Alexeis; Bedford, Denise; & Orlando, Beatrice. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital.
7. Veryard, R (2000), "On Intelligence", Component-Based Business Background Material, 1-13.
8. 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.