فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی، سال شانزدهم
شمارهٔ دوم، تابستان ۱۴۰۰

نقش سازمان‌ها و نهادها در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران[1]

تاریخ دریافت: ۱۳۹۹/۰۹/۱۵ تاریخ پذیرش: ۱۴۰۰/۰۱/۲۵

از صفحهٔ ۴۷ تا ۷۲

جواد جهانشیری[2]، رضا تقی‌پور[3]، امیرحسین یاوری[4]، سید کمال هادیانفر[5]

چکیده

زمینه و هدف: با توسعهٔ فناوری‌های نوین اطلاعاتی و ارتباطی و فراگیر شدن بهره‌برداری از فضای سایبر، نیاز به ایجاد سازوکار قانونی و حقوقی در امر پیشگیری و مقابله با جرائم سایبری بر مبنای اسناد راهبردی کشور صورت گرفته و در این تحقیق تلاش بر آن است تا جایگاه و نقش سازمان‌ها و نهادها در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران با رویکرد نگاشت نهادی تبیین شود.

روش: این پژوهش از حیث هدف، کاربردی و از نظر روش جمع‌آوری اطلاعات در زمرهٔ تحقیقات پیمایشی است. جامعهٔ آماری پژوهش را خبرگان حوزهٔ مدیریت، پیشگیری و مقابله با جرائم سایبری به تعداد ۶۱ نفر از سازمان‌ها و نهادهای عضو شورای عالی فضای مجازی کشور تشکیل می‌دهند. ابزار گردآوری، پرسشنامه‌ای محقق‌ساخته است که پس از تأیید نهایی روایی، سنجش پایایی آن از طریق ضریب آلفای کرونباخ به دست آمد. برای تجزیه و تحلیل داده‌ها، با به‌کارگیری آزمون‌های آماری توصیفی، فراوانی متغیرهای زمینه‌ای جامعهٔ موردمطالعه تحلیل و با انجام آزمون فریدمن و آزمون کای‌دو، داده‌ها با استفاده از نرم‌افزار SPSS مورد تحلیل و رتبه‌بندی قرار گرفتند.

یافته‌ها: نظر به بهره‌گیری از ابزارها و آزمون‌های مناسب، در میان سازمان‌ها و نهادهای کشور ۳۵ سازمان و نهاد کنشگر در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری نقش مؤثر دارند که در سه گروه راهبری، مجری و پشتیبان ساماندهی و رتبه‌بندی شده‌اند.

نتیجه‌گیری: نتایج حاصل بیانگر این است که علی‌رغم پیچیدگی‌ها، تعامل و همکاری در زیست‌محیط سایبری کشور، ۳۵ نهاد و سازمان در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری نقش راهبری، مجری و پشتیبانی دارند که می‌توان با ارائه راهکارهای اجرایی با ایجاد برنامهٔ منسجم در جهت پیشگیری و مقابله با جرائم سایبری در سطح کشور اقدام و در رفع موانع موجود و پیشگیری از موازی‌کاری مؤثر واقع شوند.

کلید واژه‌ها: پیشگیری و مقابله، جرائم سایبری، سازمان و نهادها، مدیریت یکپارچه، نگاشت نهادی.

استناد: جهانشیری، جواد؛ تقی‌پور، رضا؛ یاوری، امیرحسین و هادیانفر، سیدکمال (تابستان ۱۴۰۰). نقش سازمان‌ها و نهادها در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در ج. ا. ایران. فصلنامهٔ پژوهش‌های اطلاعاتی و جنایی. ۱۶(۶۲)، صص۴۷-۷۲. DOR: dorl.net/dor/20.1001.1.17359367.1400.16.1.10.8

---

۱. برگرفته از رسالهٔ دکترای مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی با موضوع «ارائه الگوی راهبردی مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران».

۲. استادیار مدیریت راهبردی فضای سایبر دانشگاه علوم انتظامی امین، تهران، ایران (نویسندهٔ مسئول)، jahanshiri@nict.ir
۳. عضو هیئت علمی دانشگاه عالی دفاع ملی، تهران، ایران، taghipour@sndu.ac.ir
۴. دانشیار مدیریت منابع انسانی دانشگاه علوم انتظامی امین ملی، تهران، ایران، yadyar@chmail.ir
۵. عضو هیئت علمی دانشگاه علوم انتظامی امین، تهران، ایران، hadianfar@cyberpolice.ir

مقدمه

نظر به مفهوم کلان و میان‌رشته‌ای فضای سایبری و ویژگی‌های خاص این فضا ایجاب می‌کند در اهداف و سیاست‌های کلی نظام ابعاد این فضا اعم از فنی، محتوایی و امنیتی در حوزه‌های اقتصادی، اجتماعی، فرهنگی، دینی و مذهبی، سیاسی، انتظامی و امنیتی، نظامی و دفاعی، روانی و بهداشتی، علمی و فناوری، حقوقی و بین‌المللی، زیست‌محیطی و غیره مورد توجه قرار گیرد. مقام معظم رهبری حضرت آیت‌الله‌العظمی امام خامنه‌ای (مُدَّظِلُّهُ‌العالی) در بدو تشکیل شورای عالی فضای مجازی (۱۷ اسفند ۱۳۹۰)، «اشراف کامل و به‌روز نسبت به فضای مجازی در سطح داخلی و جهانی»، «مواجهه فعال و خردمندانه کشور»، «بهره‌گیری حداکثری از فرصت‌ها»، «ضرورت برنامه‌ریزی و هماهنگی مستمر به‌منظور صیانت از آسیب‌ها» مورد تأکید قرار داده‌اند (تارنمای دفتر مقام معظم رهبری، ۱۳۹۰). با نگاهی به تعداد کاربران اینترنت که از دو میلیارد نفر در سال ۲۰۱۵ به ۴ میلیارد و ۶۴۸ میلیون نفر (۵۹ درصد جمعیت کل دنیا) در می[1] ۲۰۲۰ رسیده است و پیش‌بینی می‌شود که این تعداد تا سال ۲۰۲۲ به ۶ میلیارد نفر (حدود ۷۵ درصد جمعیت جهان) و در سال ۲۰۳۰ به ۷ میلیارد و ۵۰۰ میلیون نفر (حدود ۹۰ درصد جمعیت جهان) برسد (پایگاه اینترنتی آمار جهانی استفاده از اینترنت، برآوردهای سال ۲۰۲۰، برداشت ۱۳۹۹). توسعه‌یافتگی در بعد فنی، محتوایی و امنیتی فضای سایبر مشهود و ملموس است؛ لذا همین گستردگی و توسعهٔ فراگیر آن موجب شده تا بسیاری از ابعاد آن ناشناخته بوده و محل مناسبی برای مجرمان در اجرای عملیات مجرمانهٔ آن‌ها باشد. در فرآیند پیشگیری و مقابله با جرائم اعم از رصد، پیش‌بینی، پیشگیری و مبارزه، سازمان‌ها و نهادهای متعددی دخالت دارند که مهم‌ترین آن‌ها حوزه‌های زیرساختی و فنی، مراکز آموزشی، تربیتی و فرهنگی، دستگاه قضایی، پلیس و ضابطان خاص، کارشناسان دادگستری، فعالان حوزه امنیت و محتوا و ... می‌باشند. شناخت نقش، جایگاه و تشکیلات این دستگاه‌ها در آگاه‌سازی، آموزش، پیشگیری و مبارزه با جرائم

1. May

احتمالی و در نهایت مدیریت مناسب در سایه اقدامات هماهنگ، یکپارچه و هم‌افزا تأثیر بسیار دارد. هرچند از عمده‌ترین وظایف نظام مقدس جمهوری اسلامی ایران در سطح جامعه برقراری امنیت و صیانت از حریم خصوصی و اجتماعی است که به‌منظور برقراری امنیت و اعمال حاکمیت، ابزارها و سازمان‌ها و نهادهایی در حوزه‌های آموزشی، پژوهشی، اجتماعی، دینی و فرهنگی، امنیتی، انتظامی و قضایی از برجسته‌ترین آن‌هاست. لذا هر یک از این سازمان‌ها می‌تواند براساس وظایف و مأموریت‌های خود در ایجاد امنیت مناسب فضای سایبر برابر برنامه مدیریتی مناسب و یکپارچه نقش بسزایی را ایفا نمایند. لذا این تحقیق با هدف بررسی نقش سازمان‌ها و نهادها در مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری کشور پرداخته و در نهایت جایگاه هر نهاد و سازمان را تبیین که می‌توان به سازمان‌های مربوطه به‌ویژه در ابعاد فنی، محتوایی و امنیتی فضای سایبر کشور پیشنهادهای عملیاتی و اجرایی و غیره ارائه دهد. حال این سؤال مطرح می‌شود که: «نقش سازمان‌ها و نهادها در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران چیست؟».

حوزهٔ فناوری اطلاعات و ارتباطات و فضای سایبر در کشور و تبیین وظایف سازمان‌ها در چندین سال گذشته سازمان‌ها و نهادهای متولی را به تهیه و تولید اسناد و برنامه‌های ملی نموده است، در بخش منابع موجود در برخی از مؤسسات، دانشگاه‌ها، مراکز آموزش عالی و علمی سازمان‌ها در خصوص نقش و تأثیر سازمان‌ها و نهادها در حوزه جرائم سایبری به بررسی پرداخته و مشخص شد هیچ پژوهشی به‌طور مستقیم به موضوع این تحقیق نپرداخته‌اند. در ادامه، به تحقیقاتی که به حوزهٔ جرائم سایبری پرداخته‌اند اشاره می‌شود.

عبیری و علوی (۱۳۹۸) در تحقیقی با عنوان «ارائه الگوی راهبردی مدیریت فضای سایبر ج.ا.ا براساس اوامر و تدابیر حضرت امام خامنه‌ای (مدظله‌العالی)»، به عنوان هدف اصلی تحقیق، الگوی موصوف را معرفی و نفی نظام سلطه در مدیریت فعلی فضای سایبر را مستلزم بهره‌گیری از رهنمودهای مقام معظم رهبری (مدظله‌العالی) در جهت مدیریت و ارتقای امنیت ملی کشور معرفی و اشاره داشته‌اند، با توجه به رهنمودهای غنی، جامع

و کامل معظم له در خصوص فضای سایبر، اجرای تدابیر مستلزم بررسی، تحقیق، گردآوری، تجزیه و تحلیل و ارائه الگوی راهبردی مطرح شده است. صبوری و ثقفی (۱۳۹۸) نیز در مقاله‌ای با عنوان «بررسی جرائم سایبری حوزهٔ اجتماعی و راهبردهای پیشگیری و مقابله با آن در ج.ا.ایران» بیان کرده‌اند که با توجه به گسترهٔ وقوع جرائم در ابعاد ملی و تأثیرپذیری فضای سایبر از عوامل داخلی و عوامل محیطی، مبارزه با آن مستلزم اجرای راهبردهای کلان و فراگیر در سطح ملی است. یافته‌های تحقیق حاکی از این است که حوزهٔ اجتماعی فضای سایبر جمهوری اسلامی ایران دارای موقعیت راهبردی و برای پیشگیری و مقابله با جرائم سایبری این حوزه باید تعداد ۱۲ راهبرد برتر احصاء شده مورد استفاده قرار گیرد.

تقی‌زاده (۱۳۹۶) در پژوهشی با عنوان «مطالعهٔ تطبیقی نظام حقوقی حاکم بر جرائم سایبری (مطالعهٔ تطبیقی نظام حقوقی حاکم بر جرائم سایبری)»، به اهمیت فضای سایبر به عنوان پدیده‌ای نوین اشاره کرده است. با توجه به ویژگی‌های این فضا از جمله پویایی و تغییرپذیر بودن آن در حوزه‌های مختلف خلأها و چالش‌هایی وجود دارد، این روند در کشورهای پیشرفته و در حال توسعه رخ می‌دهد و به همین دلیل، دولت‌ها با انجام اقدامات لازم در زمینه‌های گوناگون از جمله ساختاری، قانون‌گذاری و تدوین سیاست‌ها سعی در غلبه بر مشکلات دارند. کشورهای پیشرفته در این حوزه که به‌نوعی الگوی سایر کشورها در این خصوص می‌باشند. با تدوین و تصویب اسناد از جمله راهبردها، دستورالعمل‌ها، قوانین، ایجاد سازمان‌ها اقدامات مرتبط و البته ایجاد هماهنگی به مقابله با حملات و جرائم سایبری می‌پردازند. این پژوهش تأکید بر بومی‌سازی الگوهای مجرد توسط کشورها را پیشنهاد می‌نماید. وطنی و اسدی (۱۳۹۵) نیز در تحقیقی با عنوان «سیاست جنایی جمهوری اسلامی ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم» آورده‌اند که پیشگیری و مقابله با جرائم، محور اصلی سیاست جنایی هر کشور محسوب می‌شود و برای تحقق آن، در سیاست جنایی تقنینی، وظیفهٔ قانون‌گذاری در کشور است که در خصوص جرائم سایبری، با استفاده از تدابیر فنی جهت تحقق امنیت فضای سایبر اقدام نماید؛ در سیاست جنایی مشارکتی، برای

پیشگیری از جرم و مبارزه با آن از اسباب و وسایل مختلف دولتی و غیردولتی کمک گرفته می‌شود و در سیاست جنایی قضایی که در تصمیم‌ها و رویه‌های قضایی به دادسراها و دادگاه‌ها منعکس می‌شود، قوه قضائیه با رویکرد پیشگیرانه در حوزه جرائم سایبری با کمک نهادهایی مانند مرکز ماهر و مراکز آپا و پلیس فتا اقدام کند.

کایرژانوا[1]، موراشبکوف[2] و بیسنف[3] (۲۰۱۵) نیز در مقاله‌ای با عنوان «روش‌های بهبود مبارزه با جرائم اینترنتی در کشورهای توسعه‌یافته»، با بررسی روش‌های پیشرفته مبارزه با جرائم اینترنتی در کشورهای توسعه‌یافته و امکان استفاده از آن‌ها برای اجرای قانون در جمهوری قزاقستان به عنوان یک کشور در حال توسعه می‌پردازد. فرصت‌های اقتصادی فن‌آوری‌های رایانه‌ای موجب جذابیت برای جنایتکاران می‌شود. تحقیق انجام شده، قادر به طبقه‌بندی روش‌های پیشرفته معاصر در ارتباط با مبارزه با جرائم اینترنتی و دستیابی به نتایجی در مورد کاربرد جامع آن‌ها و برخی از اقدامات دقیق برای بهبود قوانین کیفری جمهوری قزاقستان شده است.

با توجه به مطالعات صورت گرفته و بررسی تحقیقاتی که از لحاظ موضوعی و مفهومی نزدیک‌تر و مرتبط‌تر با این تحقیق بود، اکثر محققان به ارزیابی بخش‌هایی از فضای سایبر، جرائم سایبری و رایانه‌ای و موضوعات پیشگیری و مقابله‌ای این حوزه، فرصت-ها، تهدیدات و آسیب‌پذیری‌های فضای سایبر، فرآیند وقوع جرم سایبری و برخی از ویژگی‌های آن پرداخته‌اند، اگرچه نمی‌توان نقش پیشینه‌ها را در استفاده و دانش‌افزایی در این تحقیق انکار کرد، اما وجه تمایز این تحقیق در تبیین نقش سازمان‌ها و نهادها در مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران است.

در جهت تکامل هرچه بیشتر دانش زمینه‌ای موردنیاز برای شروع تحقیق، در پژوهش حاضر در قالب چندین بخش محتوایی مجزا، ادبیات مرتبط با موضوع تحقیق بیان شده است.

---

1. Kirjanova
2. Murashbekov
3. Beisenov

مدیریت یکپارچه[1]**:** اصول علم مدیریت ایجاب می‌کند که تمام فعالیت‌های لازم برای انجام یک وظیفه یا تمام وظایف مربوط به ایفای یک نقش خاص، تحت مدیریتی واحد انجام گیرند، بدون آنکه اصل تقسیم‌کار بین لایه‌های عملکردی این سیستم دچار خدشه شود (کاظمیان و سعیدی رضوانی، ۱۳۸۳، ص۱۶). مدیریت یکپارچه برخلاف مدیریت راهبردی که فقط وظیفه مدیریت عالی است (زیرا متوجه آینده بوده و برای سازمان مسیر و جهت تعیین می‌کند) در تمام سطوح مدیریتی لازم و ضروری است. مدیریت یکپارچه تمام سازمان‌ها را به صورت یک سیستم نگریسته و اهداف سازمان‌ها را با منافع افراد و جامعه به‌طور یکپارچه مشخص می‌نماید. مدیریت یکپارچه روشی منطقی، عینی و سیستماتیک براساس اتخاذ تصمیمات بزرگ و هدفمند در سازمان است که هم بر تجزیه و تحلیل علمی استوار است و هم بر شهود و بصیرت تکیه دارد و از همه مهم‌تر که در عرصه عملیات براساس اسناد راهبردی هم‌سو با سایر سازمان‌های اثرگذار بدون موازی کاری به اجرای مأموریت می‌پردازد. با توجه به شرح فوق، تعریف مدیریت یکپارچه در کشور را می‌توان فرآیند به‌کارگیری مؤثر و کارآمد منابع انسانی، فنی، امنیتی و محتوایی کلیه سازمان‌ها و نهادهای دولتی و غیردولتی در سطح ملی برای برنامه‌ریزی، سازماندهی، بسیج منابع و امکانات، هدایت و کنترل با هدف دستیابی به اهداف ملی و انقلابی براساس نظام ارزشی و دینی به‌منظور پیش‌بینی، پیش‌گیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملی، دینی و مذهبی در مقابل تهدیدات، آسیب‌ها جهت حفظ دارایی‌های زیرساختی، عمومی و خصوصی دانست (جهانشیری، ۱۳۹۹، ص۴۸).

ادغام سیستم‌های مدیریت: ادغام سیستم‌های مدیریت می‌تواند به‌عنوان فرآیند به‌کارگیری همزمان سیستم‌های مدیریتی با وظیفه خاص تحت یک سیستم مدیریت یکپارچه ساده‌تر و اثربخش‌تر معرفی شود. درجه چنین ادغامی بسیار متفاوت است و به عواملی چون شرایط حاکم بر سازمان، نیازمندی‌های استانداردها و استراتژی‌ها بستگی

1. Integrated management.

دارد (بک‌مهاگن، برگ و کارپتاوچ ویلبرن[1]، ۲۰۰۳، ص۵). ادغام سیستم‌های مدیریت ممکن است در هر یک از درجات هماهنگ‌سازی، همکاری، آمیختگی، هم‌افزایی و شبکه‌سازی صورت گیرد.

الف) هماهنگ‌سازی[2]: یک سازمان برای نائل شدن به اهداف موردنظرش نیاز به چارچوبی دارد که فعالیت‌های بخش‌های مختلف سازمان را هماهنگ نموده و ارتباط مناسبی بین آن‌ها برقرار کند. با طراحی واحدهای سازمانی و تعیین اداره‌ها و بخش‌های مختلف، کارها میان واحدهای اصلی تقسیم می‌شود و امکان استاندارد کردن کارها و تخصصی کردن فعالیت کارکنان فراهم می‌گردد، ولی موفقیت سازمان در تحقق اهدافش مستلزم هماهنگ ساختن فعالیت‌های مذکور است. (صیدی، ۱۳۹۵، ص۳۳).

ب) همکاری[3]: در گزارشی که «بنیاد مک‌نایت[4]» برای پیشرفت کار تدوین کرده، چنین آمده است: «همکاری موجب دسترسی آسان‌تر، سریع‌تر و منسجم‌تر به خدمات و منافع و تأثیری وسیع‌تر بر سیستم‌ها می‌شود. هرچند هم‌افزایی کوشش‌های همکاران اغلب باعث خلق راه‌های خلاق برای غلبه بر موانع می‌شود».

پ) آمیختگی[5] (ترکیب): امروزه یکی از موضوع‌های اصلی اصلاح ساختار در نظام های اداری بحث ترکیب و ادغام است. ادغام[6] ناظر بر ترکیب دو یا چند سازمان با یکدیگر و ایجاد سازمان جدید است (شرمن و هارت[7]، ۲۰۰۶، ص۱۱). آلائو[8] (۲۰۱۰) نیز ادغام را ترکیب دو یا چند سازمان را در یک سازمان بزرگ‌تر می‌داند (۵۵۵). ترکیب و اقدام اگر موفقیت‌آمیز باشد، زمینه موفقیت آن سازمان نیز فراهم می‌شود.

---

1. Beckmerhagen, Berg & Karapetrovic
2. Synchronization.
3. Cooperation
4. Mcknight Foundation
5. Mixture
6. Merge
7. Sherman & Hart
8. Alao

ت) هم‌افزایی[1]: هم‌افزایی پدیده‌ای است که باعث تشدید اثر می‌شود، لذا در حوزه مطالعات مدیریت و سازمان نیز برای بیان اثر فعالیت گروهی و افزایش بازده کار گروهی نسبت به فعالیت‌های فردی و مستقل، از این واژه استفاده می‌شود و بیان می‌دارد؛ که «گروه‌ها، استعداد هم‌نیروزایی را فراهم می‌آورند و بیش از جمع توانائی‌های تک‌تک اعضای خودکار انجام می‌دهند» (رضاییان، ۱۳۸۱، ص۲۲۱).

ث) شبکه‌سازی[2]: شبکه‌سازی یکی از اشکال همکاری بین سازمان‌ها محسوب می‌شود. به نظر آلتر و هیج[3] شبکه‌ها نوعی ساختار شناختی محسوب می‌شوند که در آن‌ها نوعی تقسیم‌کار وجود دارد و سازمان‌های یادگیرنده‌ای هستند که خودآگاهی مهم‌ترین ویژگی آن‌هاست. شبکه‌ها از طریق سازوکارهای ارتباطی و ارزشیابی مستمر، دانش و آگاهی‌شان را از خود افزایش می‌دهند. تقسیم‌کار حاکم بر شبکه نیز این اطمینان را به وجود می‌آورد که هر یک از اعضای شبکه برای سایر اعضا ارزشمند بوده و این امر به‌تدریج نوعی وابستگی متقابل را بین اعضا پدید می‌آورد (صیدی، ۱۳۹۵، ص۲۸).

سازمان: واژهٔ سازمان[4] که گاهی در فارسی به صورت «ارگان یا نهاد» هم به کار می‌رود، برای همهٔ افراد کم و بیش آشناست. برای بسیاری از ما، سازمان به عنوان یک مجموعهٔ بزرگ با مأموریت‌های ویژه و غالباً دولتی جا افتاده است، هرچند سازمان در محیط‌های گوناگون کاربردهای متفاوتی دارد. در مجموع، سازمان «مجموعه‌ای هدفمندی است که پیرو یک نظام (سیستم) است و دارای مرزها و حدودی است که آن را از محیط خود جدا می‌سازد (تارنمای دانشگاه علوم پزشکی تبریز، ۱۳۹۹/۱۱/۲۴).

سازمان‌های راهبر: راهبری سازمانی یکی از روش‌های مدرن نظارت اثربخش بر سازمان‌های دولتی است که در بخش دولتی به عنوان مجموعه‌ای از مسئولیت‌ها و روش‌ها، سیاست‌ها و رویه‌هایی که به‌وسیله مدیران سازمان‌ها جهت فراهم نمودن مسیر

---

1. Synergy
2. Networking
3. Alter and Hage
4. Organization

راهبردی، اطمینان از دستیابی به اهداف، مدیریت ریسک‌ها و استفاده مسئولانه از منابع با روشی شفاف به کار می‌رود، تعریف می‌شود (اسلام‌زاده و همکاران، ۱۳۹۶، ص۱). لذا سازمان‌های راهبر علاوه بر انجام مأموریت سازمانی خود تلاش می‌کنند با طراحی و پیاده‌سازی نظام مدیریت، برنامه محوری، نگاه سیستمی و توان راهبردی، در چارچوب اسناد بالادستی و در اجرای وظایف قانونی به‌صورت اجماع برای خود و سایر سازمان‌ها در حوزه فضای سایبر و پیشگیری و مقابله با جرائم سایبری به تبیین راهبرد، چشم‌انداز، سیاست‌گذاری، روش و رویه اجرایی و عملیاتی را ترسیم کنند.

سازمان‌های مجری: سازمان‌های مجری و عملیاتی برابر نقشه راه و برنامهٔ عملیاتی دقیق تدوین‌شده برای رسیدن به اهداف به صورت کامل و جامع اقدام می‌نماید. برای سازمان‌های مجری معمولاً یک طرح عملیاتی به‌صورت گام‌به‌گام ترسیم شده و گروه یا افراد را برای رسیدن به هدف غایی هدایت می‌نماید، این اقدامات، پایه‌های اصلی و بنیان مأموریت و وظایف را تقویت بخشیده و موجب استحکام عملیات سازمانی و وظایف در بازه‌های زمانی برنامه‌ریزی‌شده در حوزهٔ مدیریت و امنیت فضای سایبر و پیشگیری و مقابله با حوادث و جرائم سایبری شود.

سازمان‌های پشتیبان: پشتیبانی و توسعهٔ منابع، امکانات و تجهیزات فنی، محتوایی، امنیتی و پژوهشی در مجموع وظیفهٔ سازمان‌های پشتیبان است. بدون شک، پشتیبانی صحیح و قوی در حوزه‌های فناوری اطلاعات و ارتباطات اعم از زیرساخت، نرم‌افزار و سخت‌افزار یکی از ابزارهای اصلی دستیابی به اهداف مدیریت یکپارچه و هماهنگ و امنیت جامع فضای سایبر است.

سازمان‌ها و بازیگران فضای سایبر در کشور: در حال حاضر، گسترش روزافزون فضای سایبری در عرصه‌های مختلف زندگی بشر و استفاده آن در مجموعه‌ای وسیع از فعالیت‌ها، آثار و پیامدهای مختلفی را در زمینه‌های گوناگون به همراه داشته است. رشد مدیریت نشده و کنترل نشده استفاده از فضای سایبر حتی در زیرساخت‌های حیاتی، امروز کشور را با تهدید مواجه ساخته است و مواجهه با این تهدید و غلبه برآن از اولویت‌های اصلی در این حوزه قلمداد می‌شود. بازیگران فضای سایبر کشور اعم از

سیاست‌گذاران، قانون‌گذاران، ناظران، مجریان، مدیریت امنیت فضای مجازی، بهره‌برداران، اپراتورهای خدمات و محتوا و غیره‌اند که عملاً، ذینفعان فضای مجازی کشور را نیز تشکیل خواهند داد.

جرائم سایبری: از زمانی که به‌طور جدی جرم سایبری در جهان مطرح شده است نظر اندیشمندان، حقوقدانان و نهادها و سازمان‌ها را به خود جلب کرده است. پلیس جنائی فدرال و ایالتی آلمان تعریفی مبتنی بر جرم‌شناسی در مورد جرائم سایبری ارائه داده است: «جرم رایانه‌ای شامل همه شرایطی است که در آن پردازش الکترونیک داده‌ها، وسیله‌ای برای ارتکاب و یا موضوع (هدف) تخلف باشد و بیانگر دلایلی برای تردید (ظن) راجع به ارتکاب جرم است» (شیرزاد، ۱۳۸۸، ص۳۵). در تعریف و مفهوم جرائم سایبری، منظور از آن هر فعل و ترک فعلی که از تجهیزات و شبکه‌های ارتباطی و اطلاعاتی به‌طور مستقیم یا غیرمستقیم به‌عنوان ابزار، هدف یا محل و محیط ارتکاب استفاده و در قانون منع و برای آن مجازات تعیین شده باشد جرم سایبری تعبیر می‌شود (جهانشیری، حسینی و ابراهیمی، ۱۳۹۴، ص۱۵). نظر به تعاریف موجود می‌توان در تعریف و مفهوم، جرم سایبری را هر فعل یا ترک فعلی که موجب ایجاد اختلال، قطعی، کاهش کیفیت، ایراد خسارت، جعل، تغییر و یا حذف اطلاعات (سرمایه‌های سایبری) در بستر سامانه‌های مورد بهره‌برداری در فضای سایبری و یا شبکه‌های وابسته به آن، اعم از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطی، سامانه‌های رایانه‌ای و الکترونیکی، پردازنده‌های تعبیه‌شده، کنترل‌کننده‌ها، تجهیزات سخت‌افزاری و نرم‌افزاری، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان (کاربران) در ابعاد فنی، محتوایی و امنیتی و هر یک از فرآیندهای تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات انجام گیرد و در قانون برای آن مجازات تعیین‌شده باشد جرم سایبری نامیده می‌شود.

پیشگیری از جرائم سایبری: مرکز بین‌المللی پیشگیری از جرم[1] پیشگیری را چنین تعریف می‌کند: «هر عملی که به روش علمی، باعث کاهش بزهکاری، خشونت، ناامنی از طریق مشخص کردن و حل کردن عوامل پدیدآورندهٔ این مشکلات شود، پیشگیری از جرائم است»؛ در تعریف، مشخص کردن (شناسایی و کشف کردن) و همچنین حل کردن یعنی مسئله‌یابی آن‌هم با تأکید به روش علمی بسیار حائز اهمیت است (رجبی‌پور، ۱۳۸۳، صص۱۷-۱۵). در مورد دسته‌بندی انواع پیشگیری همواره نگرش‌های متفاوت بین صاحب‌نظران و جرم‌شناسان وجود دارد. انواع پیشگیری از جرم عبارت‌اند از: پیشگیری اولیه، ثانویه، ثالث، کوتاه‌مدت، بلندمدت، انفعالی، فعال، کیفری، غیر کیفری، قضایی، انتظامی، اجتماعی و غیره (بیات، شرافتی و عبدی، ۱۳۸۷، ص۵). جرائم سایبری جرائمی هستند که در فضای سایبر در محیطی وسیع و توسط کاربران با تنوع فراوان (علیه اشخاص، اموال، امنیت) در حال وقوع است با توجه به ویژگی‌های خاص این جرائم استفاده از طرق و شیوه‌های نوین جهت مقابله و پیشگیری امری ضروری است. پیشگیری از جرائم با توجه به آثار و ویژگی‌های خاص جرائم سایبری از جایگاه ویژه‌ای برخوردار است، به‌کارگیری ابزارها و شناسایی نحوه واقع‌شدن جرم در فضای سایبر جهت پیشگیری از ارتکاب بزه از اهمیت بسزایی برخوردار است.

مقابله با جرائم سایبری: کلیه اقداماتی که در قبل، حین یا پس از وقوع جرم به‌منظور شناسایی، جمع‌آوری، بررسی، تجزیه و تحلیل آثار و دلایل جرم و همچنین شناسایی، دستگیری و بازجویی متهم در جهت روشن شدن حقیقت و انتساب و عدم انتساب جرم به متهم و در نهایت صدور حکم توسط مقامات قضایی صورت می‌گیرد را می‌توان مقابله با جرم تلقی نمود. مقابله با جرائم سایبری باید با همکاری تنگاتنگ نهادها، سازمان‌ها و بخش‌های دولتی و همچنین بخش‌های خصوصی فعال در فضای سایبر کشور صورت گیرد و از آنجایی‌که تمام جرائم سایبری صرفاً در فضای مأموریتی

1. International Centre for the Prevention of Crime (ICPC)

پلیسی و قضایی خلاصه نمی‌شود، در این راستا می‌توان تدابیر و راهبردها را در قالب اقدامات و وظایف تبیین و برای هریک تعریف نمود (جهانشیری، ۱۳۹۹، ص۱۲۶).

اقدامات عملیاتی (مدیریتی و مشارکتی): علاوه بر استفاده از ابزارهای قانونی و قضایی، در نظر گرفتن آثار ضرورت حیاتی ایجاد و حمایت از ابزارها و اهرم‌های تقویتی دیگری اعم از سازمانی، نهادی و مردمی در کنار قوه قضاییه و پلیس به‌منظور اعتبار بخشیدن به موضوع پیشگیری و مقابله با جرائم سایبری، لازم و ضروری است تا با الهام از مبانی فقهی و توجه به مباحث جدید علمی پیرامون این موضوع، ضوابط و مقررات قابل‌توجهی برای مشارکت سازمان‌ها، نهادها و جامعه مدنی در این زمینه فراهم شود؛ که برجسته‌ترین جنبهٔ آن، مشارکت یکپارچه متولیان حوزه امنیت سایبری براساس مأموریت تعریف‌شده در اسناد بالادستی برای پیشگیری و مقابله با جرائم خواهد بود. در پرتو یک سیاست جنایی مشارکتی هر یک از این گروه‌ها باید در مراحل مختلف فرآیند جنایی یعنی پیشگیری و مقابله با جرم، کشف جرم و تعقیب مجرم، مرحله رسیدگی به جرم و مجازات مجرم نقش‌آفرینی کنند تا ضمن کاستن از بار دستگاه‌های قضایی و انتظامی به مقابله هرچه گسترده‌تر و دقیق‌تر با جرم پرداخته شود.

نگاشت نهادی: چارچوب نگاشت نهادی رویکردهای جدیدی را به ساختارهای نهادی و حاکمیت برای مدیریتی یکپارچه ارائه می‌دهد. نظریه این‌که بخش زیادی از مدیریت یکپارچه ممکن است به فناوری‌های جدید نیاز پیدا کند از جمله برنامه‌ریزی، مدیریت، مدل‌ها و وسایل، پس آن را می‌توان از طریق نهادهای مربوط انتقال داد که سعی بر تأمین تغییرات روشی دارند که مبتنی بر آن روش به فعالیت‌های خو می‌پردازند و همچنین مرتبط به نحوه درک آن‌ها از یکدیگر است (دسیلوا[1]، ۲۰۰۸). چارچوب نگاشت نهادی ارتباط با درک ما از توزیع قدرت است. اشکال متعدد قدرت ممکن است توسط فرد یا سازمانی به عنوان سهام‌دار اصلی به‌منظور اثرگذاری بر روی نتیجه یک فرایند تصمیم‌گیری استفاده شود که می‌توان به مواردی چون تهدید، اطلاعات،

1. Dasilva

نظرات احساسی و هیجانی و نفوذ سیاسی اشاره کرد. اما قدرت مؤثر بر موفقیت یا جذب هر انتخاب ویژه مدیریتی را نوآوری اساساً نهادهای متبوع لحاظ شده است. چارچوب نگاشت نهادی مبتنی بر نقش‌آفرینان اصلی و تعامل آن‌ها است یعنی جایی که قدرت جای دارد، یا کسی که توانایی نفوذ بر تصمیمات را دارد (به عبارتی بر روی تصمیمات نافذ و تأثیرگذار است) و کسی که تصمیماتی را اتخاذ می‌کند و به بررسی منابع تأمین بودجه می‌پردازد (مک‌فادن، پریست و گرین[1]، ۲۰۱۰؛ به نقل از هداوند، فاتح‌راد و طباطبائیان، ۱۳۹۵، صص۴-۵). در این تحقیق منظور از چارچوب نگاشت نهادی، فرایندی است که در آن، اجزاء سیستم، فعالیت‌ها و کارکردهای آن‌ها، وابستگی‌ها، تعاملات، نقش و جایگاه آن‌ها مورد بررسی واقع می‌شود.

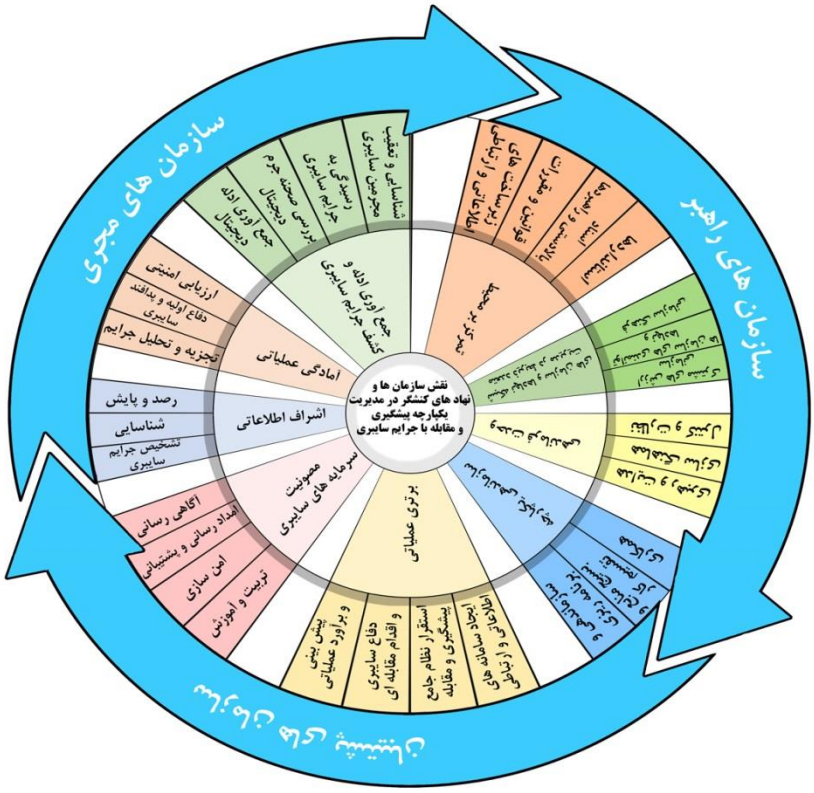
شیوه تبیین مدل نظری تحقیق: مبنا در چارچوب نظری این تحقیق جهت تبیین نقش و جایگاه سازمان‌ها و نهادهای کنشگر در مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران مبتنی بر تفکر و نگرش راهبردی است که به‌صورت کلی، تفکر راهبردی، خلاقیت، بدیع بودن و تصویرسازی از آینده‌ای متفاوت است که برای تبیین موضوع از مدل کیه‌زا[2] که به خوبی ابعاد و فرایندها را در محیط‌های پویا بیان می‌کند (با یک‌بار اجرا متوقف نمی‌شود، بلکه بارها تکرار خواهد شد و این تکرار امکان تطبیق سازمان با یک محیط پویا را فراهم می‌آورد) بهره‌گیری شده است. لذا از لحاظ مفهومی این چهارچوب فرآیندی را تبیین می‌کند که پیش از آن‌که جنبه فنی را تبیین کند، بیشتر جنبهٔ مدیریتی و عملیاتی دارد. این چارچوب تمام ابعاد سازمان‌های متولی حوزه پیشگیری و مقابله با جرائم سایبری نظیر کاربران، بخش‌های امنیت سخت‌افزار، نرم‌افزار، شبکه و نحوه توزیع و دسترسی به سامانه‌ها، فرآیندهای حرفه‌ای، انگیزه کاربران، راهبردها، مأموریت‌ها، قوانین و استانداردهای ابلاغی و... را در نظر می‌گیرد و بر مبنای محتوا و داده، اطلاعات محور است. این رویکرد با محیط خود نوعی

1. McFadden, Priest & Green
2. Chiesa

سطح‌بندی را اعمال می‌نماید اما می‌توان با تبیین روابط کاری بین سازمان‌ها و نهادها از آن در راستای مدیریت یکپارچه مورد استفاده قرار داد. البته با بررسی‌های انجام‌شده، مدل کاربری حلقه «اودا[1]» که در سال ۲۰۰۵م (۱۳۸۲ه.ش) برای مدیریت و امنیت فضای سایبر توسط برناردت برهمر[2] ارائه شده است، با اقدامات تقنینی و عملیاتی جمهوری اسلامی ایران نیز تا حدودی منطبق است و همان‌گونه که در قبل اشاره شد در فرمایشات مقام معظم رهبری حضرت آیت‌الله‌العظمی امام خامنه‌ای (مُدَّظِلُّهُ‌العالی) در دیدار اعضای شورای عالی فضای مجازی در تاریخ ۱۳۹۴/۰۶/۱۶ با اشاره به گسترش روزافزون و پرسرعت پدیدهٔ عظیم و بی‌نظیر فضای مجازی تأکید فرمودند که لازمهٔ حضور فعال و تأثیرگذار در فضای مجازی، «تمرکز در تصمیم‌گیری»، «جدیت در اجرا بدون از دست دادن زمان»، «هماهنگی میان دستگاه‌ها» و «پرهیز از موازی کاری و تعارض» است که مدل موصوف را تأیید و مدیریت مناسبی و یکپارچه‌ای را در راستای پیشگیری و مقابله با جرائم ارائه می‌نماید، هرچند مفاهیم مطرح در پژوهش براساس مدل‌های مطرح در حوزه‌های متفاوت مورد واکاوی قرار گرفته است و اما بیشتر روش‌ها انطباق با مدل حلقه بوید «اودا» و فرآیند رسیدگی به جرم سایبری در حوزه پیشگیری و مقابله با جرائم سایبری و مدل «وینسنت لندرزف» و چرخه دمینگ در حوزه مدیریت یکپارچه است و این چارچوب نشان می‌دهد که طراحی و جامعیّت‌بخشی به موضوع موردنظر مستلزم مشارکت تمامی سطوح راهبردی، میانی و عملیاتی سازمان‌ها که در بخش‌های اقدامات اسنادی و قانونی (تقنینی) و عملیاتی مقابله با جرائم سایبری به نوعی از آن‌ها نام‌برده شده است. با این توضیح، در این مرحله، مدل مفهومی تکامل یافته و بر همین اساس در الگوی نظری این تحقیق، فرایند تبیین نقش هر سازمان و نهاد دارای اهمیت ویژه‌ای است؛ در شکل ۱، الگوی (مدل) نظری تحقیق براساس جهت‌سازهای نظری و ادبیات موضوعی تدوین و ترسیم شده است و همچون دریچه است که محقق از آن منظر به پدیدهٔ مورد بررسی نگاه می‌کند.

---

1. OODA
2. Berndt Brehmer



شکل ۱ - مدل مفهومی تحقیق

مدل فوق از ۹ محور تشکیل شده است که ۴ محور به عنوان ابعادی مدیریتی بیشتر ملموس و ۵ محور را به موضوعات پیشگیری و مقابله با جرائم سایبری می‌توان تعمیم داد و اما به نحوی طراحی شده‌اند که به‌صورت کلی به ابعاد مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری پرداخته و مورد استفاده قرار می‌گیرد، مهم‌ترین نظریه‌های حوزه مدیریت یکپارچه رویکرد (نگرش) سیستمی، رویکرد حکمرانی شبکه‌ای، پنجره واحد خدمات، هماهنگ‌سازی سیاستی است که نظریه پنجره واحد خدمات و رویکرد حکمرانی شبکه‌ای قابل‌تعمیم به وضعیت مدیریت پیشگیری و مقابله با جرائم در ایران است که از ایجاد زمینه‌ها، امکانات و شرایطی که مدیران حوزه امنیت فضای تولید و تبادل اطلاعات به‌ویژه در عرصه‌های پیشگیری و مقابله با حوادث و جرائم سایبری بتوانند قدرت رصد، تشخیص،

پیش‌بینی و مقابله با تهدید و آسیب را داشته و به بهترین راه‌حل‌های مسائل موجود را براساس منافع، مصالح و امنیت فردی، عمومی و ملی در زمان مناسب با بیش‌ترین سطح جامعیت و قابلیت اطمینان در همکاری، مشارکت و مسئولیت‌پذیری کلیه سازمان‌ها، نهادها و غیره داشته باشند.

روش

پژوهش حاضر از لحاظ نوع و هدف، در زمرهٔ تحقیقات کاربردی و از لحاظ روش جمع‌آوری اطلاعات، در زمرهٔ تحقیقات پیمایشی جای می‌گیرد. جامعهٔ آماری پژوهش را تعداد ۶۱ نفر به‌صورت هدفمند از خبرگان که در امر مدیریت فضای سایبری و جرائم سایبری کشور مشغول‌اند، تشکیل می‌دهد و به دلیل محدود بودن جامعهٔ آماری، کلیهٔ افراد جامعه به شیوهٔ تمام شماری انتخاب و مورد ارزیابی قرار گرفتند.

جدول ۱ - جامعهٔ آماری پژوهش

جامعهٔ آماری	مدیران، خبرگان و متخصصان در مسائل راهبردی فضای سایبر	کارشناسان، طراحان و خبرگان حوزهٔ اسناد بالادستی	مدیران کل فتاناجا و روسای پلیس فتا سراسر کشور	مدیران قضایی و قضات ویژه دادسراهای مبارزه با جرائم رایانه‌ای	جمع
کمی	۲۴	۲۰	۱۲	۵	۶۱

ابزار گردآوری داده‌ها را پرسشنامهٔ محقق‌ساخته تشکیل داده و برای تعیین پایایی آن از ضریب آلفای کرونباخ استفاده شد که نتیجهٔ آن (α=۰/۸۵۴) بوده و بیانگر قابلیت اعتماد و پایایی بسیار بالای پرسشنامه است و جهت تعیین روایی پرسشنامه از ضریب لاشه استفاده شد. بدین ترتیب، مشخص شد که پرسشنامهٔ طراحی‌شده از اعتبار کافی برای ارزیابی شاخص‌ها برخوردار است. برای آنالیز ابتدا داده‌هایی که از پرسشنامه جمع‌آوری و در جدول‌های آماری سازمان‌دهی شد و با استفاده از نرم‌افزار SPSS با به‌کارگیری آزمون‌های آماری توصیفی فراوانی متغیرهای زمینه‌ای جامعه مورد مطالعه تحلیل و با انجام آزمون‌های فریدمن[1] و آزمون کای دو[2] (خی‌دو) داده‌ها مورد تجزیه و تحلیل و مورد رتبه‌بندی قرار گرفتند.

1. Friedman Test
2. Chi-Square

یافته‌ها

توصیف جمعیت‌شناختی پاسخگویان: در این پژوهش، توصیف داده‌ها مربوط به مهم‌ترین ویژگی‌های جمعیتی جامعه مورد اشاره در جدول ۲ به اختصار توضیح داده شده است.

جدول ۲ - خلاصهٔ توزیع فراوانی متغیرهای زمینه‌ای جامعهٔ مورد مطالعه

متغیرهای زمینه‌ای	توزیع فراوانی
سن	۵۱ نفر پاسخ‌دهندگان بالای ۴۰ سال سن دارند (۸۳,۶ درصد) و ۱۶,۴(۱۰ نفر) زیر ۴۰ سال سن
سطح تحصیلات	کارشناسی ارشد (۱۱ نفر برابر با ۱۸ درصد). دانشجوی دکترا و دکترا (۵۰ نفر برابر با ۸۲ درصد)
میزان آشنایی با موضوع تحقیق	افرادی که به‌صورت متوسط با موضوع تحقیق آشنایی داشته‌اند ۲۰ نفر (۳۲,۸ درصد)، زیاد ۲۳ نفر (۳۷,۷ درصد) و خیلی زیاد ۱۸ نفر (۲۹,۵ درصد) بوده‌اند.
سابقهٔ کار در حوزهٔ فضای سایبر	بین ۱ تا ۵ سال برابر با ۶ نفر (۱۳,۱ درصد) / بین ۶ تا ۱۰ سال برابر با ۱۸ نفر (۱۹,۷ درصد)/ بین ۱۱ تا ۱۵ سال برابر با ۱۷ نفر (۲۷,۹ درصد) / بین ۱۶ تا ۲۰ سال برابر با ۱۲ نفر (۲۹,۵ درصد) / از ۲۱ به بالا ۸ نفر (۹,۸ درصد).
رده (شغلی و مأموریتی)	پاسخ‌گویان دارای مشاغل ستادی ۲۹ نفر در حدود (۴۷,۵ درصد)، مشاغل نظارتی و کنترلی ۱۱ نفر (۱۸ درصد)، مشاغل پشتیبانی عملیاتی ۶ نفر (۹,۸)، عملیاتی و اجرایی ۱۵ نفر (۲۴,۷ درصد)
جایگاه مسئولیتی	اعضای هیئت علمی برابر با ۱۲ نفر (۱۹,۷ درصد)/ مدیران عالی برابر با ۲۲ نفر (۳۶,۱ درصد)/ مدیران میان برابر با ۱۶ نفر (۲۶,۲ درصد) مدیران اجرایی ۱۱ نفر برابر با (۱۸ درصد).

از دیدگاه جامعهٔ نخبگان، سازمان‌ها یا نهادهای کنشگر در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در سه گروه راهبری، مجری و پشتیبان قرار گرفتند.

نقش راهبری سازمان‌ها و نهادهای کنشگر در مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری

جدول ۳ - نتایج انجام آزمون فریدمن و کای‌دو برای نقش و جایگاه راهبری سازمان‌های کنشگر

تعداد داده‌های هر زیرمؤلفه	معناداری آماری	سطح خطا (α)	آمارهٔ کای‌دو	درجهٔ آزادی	نتیجهٔ آزمون
۶۱	۰/۰۰۰	۰/۰۵	۴۳,۳۹۹	۹	تأیید می‌شود

با توجه به جدول ۳، مقدار معناداری آماری[1] کمتر از ۵ درصد است. بنابراین، فرض صفر رد و فرض مقابل تأیید می‌شود. به عبارت دیگر، میزان تأثیر هر یک از زیرمؤلفه‌های مؤلفه راهبری متفاوت است. حال جهت تعیین اولویت، میانگین رتبه‌ها مورد بررسی قرار می‌گیرد، نتایج مربوط به میانگین رتبه‌ها در جدول ۶ آمده و هرچه میانگین رتبه بیشتر باشد، نقش و جایگاه راهبری آن سازمان و نهاد (زیرمؤلفه) در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری جمهوری اسلامی ایران بیشتر است. ملاحظه می‌شود زیرمؤلفهٔ شورای عالی فضای مجازی، نیروی انتظامی جمهوری اسلامی ایران، مرکز ملی فضای مجازی و قوهٔ قضائیه در رتبهٔ اول تا چهارم قرار دارند.

جدول ٤ - میانگین رتبه‌های زیرمؤلفه‌های نقش و جایگاه راهبری سازمان‌های کنشگر

ردیف	ترتیب اولویت	میانگین رتبه‌ها	سازمان یا نهاد	فراوانی	درصد
۱	۱	۶,۳۹	شورای عالی فضای مجازی	۵۵	۹۰,۲
۲	۲	۶,۳۴	نیروی انتظامی جمهوری اسلامی ایران	۵۵	۹۰,۲
۳	۳	۶,۰۶	مرکز ملی فضای مجازی	۴۸	۷۸,۷
۴	۴	۶,۰۰	قوهٔ قضاییه	۴۷	۷۷
۵	۵	۵,۸۹	وزارت اطلاعات	۴۲	۶۸,۹
۶	۶	۵,۴۴	شورای عالی امنیت ملی	۳۸	۶۲,۳
۷	۷	۴,۹۸	ستاد کل نیروهای مسلح ج.ا.ایران	۳۷	۶۰,۷
۸	۸	۴,۶۵	وزارت ارتباطات و فناوری اطلاعات	۳۴	۵۵,۷
۹	۸	۴,۶۵	پدافند غیرعامل، قرارگاه سایبری	۳۴	۵۵,۷
۱۰	۹	۴,۶۱	قوهٔ مقننه (مجلس شورای اسلامی)	۳۱	۵۰,۸

نقش مجری سازمان‌ها و نهادهای کنشگر در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری

جدول ٥ - نتایج انجام آزمون فریدمن و کای‌دو برای نقش و جایگاه مجری سازمان‌های کنشگر

تعداد داده‌های هر زیرمؤلفه	معناداری آماری	سطح خطا (α)	آمارهٔ کای‌دو	درجهٔ آزادی	نتیجهٔ آزمون
۶۱	۰/۰۰۰	۰/۰۵	۷۳,۵۶۹	۱۶	تأیید می‌شود

[1]. P-Value.

با توجه به جدول ۵، مقدار معناداری آماری کمتر از ۵ درصد است. بنابراین، فرض صفر رد و فرض مقابل تأیید می‌شود. به عبارت دیگر، میزان تأثیر هر یک از زیرمؤلفه‌های مؤلفه مجری متفاوت است. حال جهت تعیین اولویت، میانگین رتبه‌ها مورد بررسی قرار می‌گیرد، نتایج مربوط به میانگین رتبه‌ها در جدول ۶ آمده و هر چه میانگین رتبه بیشتر باشد، نقش و اهمیت زیرمؤلفه (سازمان‌ها و نهادهای مجری) در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری جمهوری اسلامی ایران بیشتر است. مشخص است زیرمؤلفهٔ کارگروه تعیین مصادیق مجرمانه، اتحادیهٔ کسب‌وکارهای اینترنتی و پارک علم و فناوری در رتبهٔ اول تا سوم قرار دارند. البته برخی نهادها و سازمان‌ها مانند ردیف ۵ تا ۷ جدول ۶، جایگاه مشترک و مشابه دارند.

جدول ٦ - میانگین رتبه‌های زیرمؤلفه‌های نقش و جایگاه مجری سازمان‌های کنشگر

ردیف	ترتیب اولویت	میانگین رتبه‌ها	سازمان یا نهاد	فراوانی	درصد
۱	۱	۱۱,۵۲	کارگروه تعیین مصادیق مجرمانه	۵۵	۹۰,۲
۲	۲	۱۰,۷۸	اتحادیهٔ کسب‌وکارهای اینترنتی	۵۵	۹۰,۲
۳	۳	۹,۷۶	پارک علم و فناوری	۵۵	۹۰,۲
۴	۴	۹,۶۰	وزارت صنعت، معدن، تجارت	۵۱	۸۳,۶
۵	۵	۹,۴۳	سازمان صداوسیما	۴۶	۷۵,۴
۶	۵	۹,۴۳	سپاه پاسداران انقلاب اسلامی	۴۶	۷۵,۴
۷	۵	۹,۴۳	سازمان تبلیغات اسلامی	۴۶	۷۵,۴
۸	۶	۹,۳۹	سازمان نظام صنفی رایانه‌ای کشور	۴۴	۷۲,۱
۹	۷	۹,۰۲	مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخداد رایانه‌ای)	۴۲	۶۸,۰۹
۱۰	۷	۹,۰۲	بنیاد ملی بازی‌های رایانه‌ای	۴۲	۶۸,۰۹
۱۱	۸	۸,۹۶	مراکز آپا (مرکز آگاهی‌رسانی، پشتیبانی و امداد حوادث رایانه‌ای)	۴۱	۶۷,۲
۱۲	۹	۸,۶۴	وزارت فرهنگ و ارشاد اسلامی	۴۰	۶۵,۶
۱۳	۹	۸,۶۴	شرکت ارتباطات زیرساخت	۴۰	۶۵,۶
۱۴	۱۰	۷,۶۷	سازمان تنظیم مقررات و ارتباطات	۳۹	۶۳,۹
۱۵	۱۰	۷,۶۷	بانک مرکزی	۳۹	۶۳,۹
۱۶	۱۱	۷,۱۰	مرکز مدیریت راهبردی افتا ریاست	۳۳	۵۴,۱
۱۷	۱۲	۶,۹۵	سازمان فناوری اطلاعات ایران	۳۱	۵۰,۸

نقش پشتیبان سازمان‌ها و نهادهای کنشگر در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری

جدول ۷ - نتایج انجام آزمون فریدمن و کای‌دو برای نقش و جایگاه پشتیبانی سازمان‌های کنشگر

تعداد داده‌های هر زیرمؤلفه	معناداری آماری	سطح خطا (α)	آمارهٔ کای‌دو	درجهٔ آزادی	نتیجهٔ آزمون
۶۱	۰/۰۰۰	۰/۰۵	۸۶،۱۵۳	۷	تأیید می‌شود

با توجه به جدول ۷، مقدار معناداری آماری کمتر از ۵ درصد است. بنابراین، فرض صفر رد و فرض مقابل تأیید می‌شود. به عبارت دیگر، میزان تأثیر هر یک از زیرمؤلفه‌های مؤلفه پشتیبانی متفاوت است. حال جهت تعیین اولویت، میانگین رتبه‌ها مورد بررسی قرار می‌گیرد، نتایج مربوط به میانگین رتبه‌ها در جدول ۸ آمده است. هر چه میانگین رتبه بیشتر باشد، نقش و جایگاه پشتیبانی آن سازمان و نهاد (زیرمؤلفه) در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری جمهوری اسلامی ایران بیشتر است. لذا زیرمؤلفهٔ وزارت آموزش و پرورش، شورای عالی انقلاب فرهنگی، سازمان‌های مردم‌نهاد و حوزه‌های علمیه در رتبهٔ اول تا چهارم قرار دارند.

جدول ۸ - میانگین رتبه‌های زیرمؤلفه‌های نقش و جایگاه پشتیبانی سازمان‌های کنشگر

ردیف	ترتیب اولویت	میانگین رتبه‌ها	سازمان یا نهاد	فراوانی	درصد
۱	۱	۵،۷۴	وزارت آموزش و پرورش	۵۰	۸۲
۲	۲	۵،۵۷	شورای عالی انقلاب فرهنگی	۴۹	۸۰،۳
۳	۳	۵،۳۵	سازمان‌های مردم‌نهاد	۴۸	۷۸،۷
۴	۴	۴،۵۲	حوزه‌های علمیه	۴۳	۷۰،۵
۵	۵	۴،۱۴	وزارت دفاع و پشتیبانی نیروهای مسلح	۳۹	۶۳،۹
۶	۶	۴،۰۱	وزارت علوم، تحقیقات و فناوری	۳۸	۶۲،۳
۷	۷	۳،۵۸	ارتش جمهوری اسلامی ایران	۳۶	۵۹
۸	۸	۳،۰۹	وزارت امور خارجه	۳۰	۴۹،۲

بحث و نتیجه‌گیری

بی‌شک پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران یا هر نقطه از جهان منوط به اقدامات میان‌بخشی و با تعامل و همکاری بین نهادها و سازمان‌های متولی امکان‌پذیر خواهد بود و این امر مستلزم مدیریت یکپارچه و مناسب در این حوزه خواهد بود. در بخش اقدامات عملیاتی (مدیریتی و مشارکتی) براساس وظایف و مأموریت‌های سازمانی و قانونی، شاخص‌ترین و عمده متولیان (سازمان‌ها و نهادها) در حوزهٔ پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران مشخص شدند و جایگاه کنشگری سازمان‌ها در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری از دیدگاه جامعهٔ نخبگان در سه گروه راهبری، مجری و پشتیبان و ضرورت و اهمیت اثرگذاری هر گروه تبیین شد.

از بین ۳۵ سازمان و نهاد موردسنجش در هر طیف، رتبه و اولویت آن‌ها براساس آزمون‌های آماری، درصد و فراوانی حاصله مشخص است. براساس یافته‌های تحقیق در حوزهٔ راهبری، ۱۰ سازمان و نهاد در مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری جمهوری اسلامی ایران ایفای نقش بیشتر دارند که شورای عالی فضای مجازی، نیروی انتظامی جمهوری اسلامی ایران، مرکز ملی فضای مجازی و قوهٔ قضاییه در رتبهٔاول تا چهارم قرار دارند. با توجه به نتایج حاصله، نقش و اهمیت ۱۷ سازمان‌ها و نهادها در حوزهٔ اجرایی و عملیاتی نمایان شد که کارگروه تعیین مصادیق مجرمانه، اتحادیهٔ کسب‌وکارهای اینترنتی و پارک علم و فناوری، وزارت صنعت، معدن و تجارت، سازمان صداوسیما و سپاه پاسداران انقلاب اسلامی در اولویت مأموریت‌های اجرایی قرار دارند. تعداد ۸ سازمان و نهاد نیز نقش و جایگاه پشتیبانی در مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری جمهوری اسلامی ایران دارند که وزارت آموزش و پرورش، شورای عالی انقلاب فرهنگی، سازمان‌های مردم نهاد و حوزه‌های علمیه در امر پشتیبانی نهادها و سازمان‌های مجری و راهبری، نقش بیشتری دارند.

در مورد نهادهای مورد وصف در پژوهش، می‌توان اظهار داشت ساختار بیشتر این نهادها که در پیشگیری و مقابله با جرائم سایبری نقش دارند از قبل ایجاد شده است،

مانند قوای قضاییه و مقننه، شورای امنیت ملی، نیروهای مسلح اعم از نیروی انتظامی، ارتش و سپاه پاسداران، وزارت‌خانه‌ها، سازمان صداوسیما و غیره که به‌عنوان سازمان‌های راهبری، اجرایی و پشتیبان نقش برجسته‌ای را در حوزهٔ پیشگیری و مقابله با جرائم سایبری ایفاء می‌کنند. برخی سازمان‌ها نیز اگرچه به‌صورت مستقل در کشور وجود ندارد، ولی وظایف آن‌ها در سازمان‌ها و وزارتخانه‌های مختلف انجام می‌پذیرد، مانند شرکت ارتباطات زیرساخت، سازمان تنظیم مقررات و غیره با همکاری وزارت فناوری اطلاعات و ارتباطات قابل‌دستیابی خواهد بود. بخش دیگر، نقش‌های جدیدی هستند که نهادی در کشور برای آن قبل از بروز قابلیت‌های فضای سایبر، پیش‌بینی نشده بود که با توسعهٔ زیرساخت‌های فناوری اطلاعات و ارتباطات، فرصت‌های ایجاد شده در بستر فضای سایبر و تهدیدات و آسیب‌های فضای سایبر شکل گرفتند، مانند شورای عالی فضای مجازی، مرکز ملی فضای مجازی، پلیس فضای تولید و تبادل اطلاعات، دادسراهای ویژه جرائم رایانه‌ای و غیره. بنابراین، لازم است هنوز هم برای فرآیندهای مشابه نهادهایی ایجاد یا بازمهندسی و در قوانین و مقررات جاری و تبیین روابط کاری اهتمام بیشتری شود. نگاشت نهادی در این تحقیق توانست با اختصاص نقش‌ها و کارکردها به سازمان‌های موجود در کشور، فرآیندها و نقش‌های بر زمین مانده را مشخص کند و پیشنهادهایی را ارائه کند که در در دو زمینهٔ کاربردی و پژوهشی بر مبنای آنچه در پژوهش مورد بررسی و تأیید قرار گرفت، ارائه شده است.

- برای دستیابی به مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در کشور می‌بایست ساختار برخی از نهادها و سازمان‌ها مانند وزارت فناوری اطلاعات و ارتباطات و شرکت‌های وابسته، مرکز ملی فضای مجازی، بازمهندسی شود و از طرف دیگر، نهادهایی برای نقش‌های جدید ایجاد شود؛

- در نظر گرفتن اولویت پیشگیری و مقابله با جرائم سایبری در سازمان‌های مجری و پشتیبان نسبت به شناسایی ابزار، بستر و منشأ جرائم و واکنش به‌موقع در مقابل جرائم؛

- تقویت دستگاه امنیتی، انتظامی و قضایی کشور و ظرفیت‌های اجرای قانون در حوزه مبارزه با جرائم سایبری؛

– تولید و انتشار محتوای آموزش سایبری بومی توسط سازمان‌ها و نهادهای مجری و پشتیبان مانند سازمان صداوسیما، وزارت فرهنگ و ارشاد اسلامی، وزارت علوم و تحقیقات، وزارت آموزش و پرورش، حوزه‌های علمیه و غیره در سطوح مختلف سنی با شیوه‌ها و ابزارهای بروز و مدرن به‌منظور ارتقای سواد و دانش سایبری، ترویج فرهنگ و اخلاق سایبری و شناخت فرصت‌ها، تهدید و آسیب‌های فضای سایبر؛

– تبیین کنندگان قانون در سطح راهبری (قوهٔ قضاییه، شورای عالی فضای مجازی، قوهٔ مقننه و غیره) و مجریان قانون با امکان‌سنجی و نیازسنجی ارکان مختلف نظام حقوق کیفری و مدنی در جرائم سایبری را جزء برنامه‌های اصلی و با اولویت خود قرار دهند.

– الزام و همراه‌سازی سازمان‌ها و نهادهای پشتیبان در حوزهٔ زیرساخت‌ها و سامانه‌های اطلاعاتی مرتبط با سرمایه‌های سایبری خصوصی، عمومی و ملی کشور در استفاده از محصولات سایبری امن بومی در جهت کاهش از وابستگی به فناوری‌ها و محصولات غیربومی؛

– برنامه‌ریزی، سطح‌بندی، چابک‌سازی و تقسیم کار ملی بین نهادها و سازمان‌های متولی در هر یک از حوزه‌های راهبری، مجری و پشتیبان با نگاه پیشگیرانه از اقدامات موازی کاری؛

– بررسی و مطالعهٔ تطبیقی فرآیند مدیریت پیشگیری و مقابله با جرائم سایبری کشور با سایر کشورها در حوزهٔ فضای سایبر؛

– ارزیابی و تنقیح قوانین به‌منظور یکنواخت سازی رویهٔ رسیدگی به جرائم سایبری و بررسی خلأ قانونی؛

– روش‌های تحکیم همکاری‌های منطقه‌ای و بین‌المللی در راستای مبارزه با جرائم سایبری؛

– مطالعهٔ تطبیقی اقدام سازمان‌های منطقه‌ای و بین‌المللی در حوزهٔ پیشگیری و مبارزه با جرائم سایبری.

سپاسگزاری

شایسته است از کلیهٔ مسئولان دانشکده امنیت ملّی دانشگاه عالی دفاع ملّی که بسترساز اجرای این پژوهش بودند و اساتید بزرگوار که با تلاش بی‌دریغ، دلسوزانه و با صرف وقت زیاد، نسبت به تصحیح و ارائه راهکار مناسب از هیچ کوششی دریغ نفرمودند و همهٔ عزیزانی که در طول این تحقیق ما را یاور و همراه بودند، تقدیر و تشکر کنیم.

منابع

- اسلام‌زاده، امید؛ ایزدی‌نیا، ناصر و فروغی، داریوش (۱۳۹۶). *شناسایی مؤلفه‌های راهبری سازمانی در سازمان‌های دولتی با روش دلفی فازی*. کنفرانس ملی تحقیقات علمی جهان در مدیریت، حسابداری، حقوق و علوم اجتماعی شیراز.

- بیات، بهرام؛ شرافتی‌پور، جعفر و عبدی، نرگس (۱۳۸۷). *پیشگیری از جرم با تکیه بر رویکرد اجتماع‌محور*. تهران: معاونت اجتماعی ناجا.

- تارنمای آمار جهانی استفاده از اینترنت. برآوردهای سال ۲۰۲۰. قابل بازیابی از: https://www.internetworldstats.com/stats.htm

- تارنمای دانشگاه علوم پزشکی و خدمات درمانی تبریز. قابل بازیابی از: https://b2n.ir/k03716

- تارنمای دفتر مقام معظم رهبری حضرت آیه‌الله العظمی امام خامنه‌ای (مُدَّظِلُّهُ‌العالی).

- تقی‌زاده، مهرداد (پاییز ۱۳۹۶). مطالعهٔ تطبیقی نظام حقوقی حاکم بر جرائم سایبری. *فصلنامهٔ علمی مطالعات بین‌المللی پلیس*. ۸(۳۱)، صص۱۱۵-۱۴۸. قابل بازیابی از: https://b2n.ir/p81315

- جهانشیری، جواد (۱۳۹۹). *الگوی راهبردی مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران*. رسالهٔ دکترای مدیریت راهبردی فضای سایبر دانشگاه و پژوهشگاه عالی دفاع ملی.

- جهانشیری، جواد؛ حسینی محمدرضا و ابراهیمی، احمد. (پاییز ۱۳۹۴). تبیین فرآیند تحقیقات مقدماتی در جرائم سایبری. *فصلنامهٔ علمی پژوهش‌های اطلاعاتی و جنایی*. ۱۰(۳۹)، صص۹-۳۳. قابل بازیابی از: https://b2n.ir/u14074

- رجبی‌پور، محمود (پاییز ۱۳۸۲). راهبرد پیشگیری اجتماعی از جرم «تعامل پلیس و دانش آموزان». *فصلنامهٔ پژوهش‌های دانش انتظامی*. ۵(۱۹)، صص۷-۳۴. قابل بازیابی از: https://b2n.ir/m76389
- رضائیان، علی (۱۳۸۱). *مبانی مدیریت رفتار سازمانی*. تهران: انتشارات سمت. چاپ سوم.
- سند نظام ملّی پیشگیری و مقابله با حوادث در فضای مجازی (۱۳۹۶/۰۸/۱۵).
- سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا) (۱۳۸۹/۱۱/۲۹).
- شیرزاد، کامران (۱۳۸۸). *جرائم رایانه‌ای از منظر حقوق جزای ایران و حقوق بین-الملل*. تهران: انتشارات شرکت نشر بهینهٔ فراگیر.
- صبوری، رضا و ثقفی، کامیار (زمستان ۱۳۹۸). بررسی جرائم سایبری حوزهٔ اجتماعی و راهبردهای پیشگیری و مقابله با آن در جمهوری اسلامی ایران. *فصلنامهٔ امنیت ملی*. ۹(۳۴)، صص۱۲۵-۱۵۲. قابل بازیابی از: https://b2n.ir/j78742
- صیدی، فاطمه (۱۳۹۵). *ارائه الگوی مدیریت یکپارچهٔ خدمات اجتماعی در حوزهٔ آسیب‌های اجتماعی(نمونهٔ موردی؛ شهر تهران)*. پایان‌نامهٔ کارشناسی ارشد دانشکدهٔ علوم اجتماعی دانشگاه علامه طباطبائی.
- عبیری، داوود و ولوی، محمدرضا (تابستان ۱۳۹۸). ارائه الگوی راهبردی مدیریت فضای سایبر ج.ا.ا براساس اوامر و تدابیر حضرت امام خامنه‌ای (مدظله‌العالی). *فصلنامهٔ امنیت ملی*. ۹(۳۲)، صص۱۷۱-۲۰۰. قابل بازیابی از: https://b2n.ir/f83743
- فرمان تشکیل شورای عالی فضای مجازی (۱۳۹۰/۱۲/۱۷).
- قانون مجازات اسلامی (۱۳۹۲). مصوب ۱۳۹۲/۰۲/۰۱مجلس شورای اسلامی و تأیید ۱۳۹۲/۰۲/۱۱ شورای نگهبان.
- کاظمیان، غلامرضا و سعیدی رضوانی، نوید (۱۳۸۳). *امکان‌سنجی واگذاری وظایف جدید به شهرداری‌ها؛ امکان‌سنجی واگذاری وظایف جدید به شهرداری‌های ایران*. جلد اول تا پنجم. تهران: انتشارات سازمان شهرداری‌های کشور.
- وطنی، امیر و اسدی، حمید (بهار و تابستان ۱۳۹۵). سیاست جنایی جمهوری اسلامی

ایران در جرائم سایبری با تأکید بر ویژگی‌های خاص این جرائم. *دوفصلنامهٔ پژوهشنامهٔ حقوق اسلامی*. ۱۷(۳۴)، صص۹۹-۱۲۶: قابل بازیابی از: https://b2n.ir/z25956

- هداوند، مرضیه؛ فاتح‌راد، مهدی و طباطبائیان، سید حبیب‌الله (۱۳۹۵). تحلیل فرآیند سیاست‌گذاری در نظام ملی نوآوری ایران با استفاده از چارچوب نگاشت نهادی. *فصلنامهٔ سیاست‌های راهبردی و کلان*. ۴(۱۶)، صص۱-۸. قابل بازیابی از: https://b2n.ir/t18997

منابع لاتین

- Alao, R.O. (2010). Integration and attraction in the Nigerian banking industry: A fan of three mega banks. Journal of European Social Sciences 15 (4), 554.

- Beckmerhagen,I.A, Berg,H.P. & Karapetrovic, S.V. (2003). Integration of management systems: focus on safety in the nuclear industry, International Journal of Quality & Reliability Management, Vol. 20 Issue: 2, pp.210-228. *https://doi.org/10.1108/02656710310456626*.

- Desilva, C, Sutherland, A. & Green, C. (2008). Learning Alliance Briefing Note 15/; Instisonal mapping. SWITCH Project. Retrived Jan. 26, 2011.

- Kieranganova, Mireshbekov Yessenov (November 2015). Improvement of the fight against cybercrime in developed countries, Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan, Internet Banking and Trade Magazine, Volume 20.

- McFadden, L., S. Priest and Green, C. (2010). Introducing Institutional Mapping: Report a Guide For SPICOSA SCIENTISTS. Flood Hazard Research Centre, Middlesex University, London. Retrieved from: *https://b2n.ir/p57380*

- Sherman, A.J. & Hart, M.A. (2006). Integration and Recruitment: From A to Z, New York: American Management Association.