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

سال نهم، شمارهٔ ۳۵ (پاییز ۱۳۹۹)صص۱۲۴-۹۵

الگوی راهبردی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران

■ رضا تقی پور ■
عضو هیئت علمی گروه سایبر دانشگاه عالی دفاع ملی، تهران، ایران
■ امیر حسین یاوری ■
عضو هیئت علمی دانشگاه علوم انتظامی امین، تهران، ایران
■ سیدکمال هادیان فر ■
عضو هیئت علمی دانشگاه علوم انتظامی امین، تهران، ایران
■جواد جهانشیری ■
عضو هیئت علمی دانشگاه علوم انتظامی امین و دانشجوی سایبر داعا، تهران، ایران

تاریخ دریافت: ۱۳۹۹/۰۶/۱۵ تاریخ پذیرش: ۱۳۹۹/۰۹/۰۵

چکیده

امروزه در کنار فرصت‌ها و قابلیت‌های ایجادشده در زیست‌بوم سایبری کشور، سرمایه‌های سایبری موجود در معرض تهدیدها، آسیب‌ها و مخاطرات هستند. در این راستا، اقدام پیشگیرانه و مقابله‌ای با تهدیدها و آسیب‌ها و جرائم سایبری مستلزم برنامه‌ریزی ملی، فراسازمانی و فرابخشی است. این تحقیق با هدف تبیین و دستیابی به الگوی راهبردی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران انجام شده است.

این پژوهش از نوع تحقیقات کاربردی‌توسعه‌ای و تبیینی و از نظر روش، آمیخته و ترکیبی است. جامعه آماری این پژوهش را خبرگان حوزه سایبر به تعداد ۷۰ نفر تشکیل می‌دهند. ابزار گردآوری در گام اول بر مبنای روش کیفی بوده است که بعد از پیاده‌کردن مصاحبه ۱۴ نفر از خبرگان در شش محور، کدگذاری باز بر روی متون مصاحبه‌ها انجام شده و بر اساس مقوله‌های بخش کیفی، پرسشنامه محقق‌ساخته تدوین گردیده است. برای تجزیه و تحلیل داده‌ها از نرم‌افزارهای SPSS و SMARTPLS استفاده شد. با بررسی برازش اندازه‌گیری مدل از طریق سنجش پایایی (آلفای کرونباخ، پایایی ترکیبی و بارهای عاملی) و روایی واگرا و همگرا ارزیابی شد که از وضعیت مناسبی برخوردار بود. برازش ساختاری مدل از طریق محاسبه ضرایب معناداری Z مقادیر (T-VALUES)، معیارR2 (ضریب تعیین) و معیار Q2 ارزیابی شد که از وضعیت مناسب و قوی برخوردار بود. با استفاده از نتایج برازش‌های فوق، برازش کلی مدل نیز محاسبه شد که مقدار آن ۰,۵۰۸ بود و چون بزرگ‌تر از ۰,۳۶ بود، برازش کلی مدل، قوی ارزیابی شد و امکان بررسی ارزیابی و تأیید مدل ترسیم‌شده در این پژوهش فراهم گردید.

کلید واژگان: *الگوی راهبردی، مدیریت یکپارچه، پیشگیری، فضای سایبر، جرائم سایبری.*

مقدمه

فضای سایبر علاوه بر ارائه خدمات ابزاری، می‌تواند به‌عنوان توانمندساز، نقش هم‌افزایی را در پیشرفت جامعه داشته باشد. کم‌توجهی یا رویکرد نادرست به امنیت این فضا، با توجه به میزان چشمگیر فرصت‌ها، تهدیدها و آسیب‌ها و پیشرفت‌های سخت‌افزاری[۱] و نرم‌افزاریِ[۲] جدید آن، مانعی بزرگ برای پیشروی و گسترش کاربرد فناوری ارتباطات و اطلاعات و ورود به جامعه اطلاعاتی[۳] و هوشمند[۴] بوده و تأمین امنیت بسیار دشوار خواهد شد. لذا رویکرد سیستمی مشارکت کلیه نهادها و سازمان‌های مسئول را می‌طلبد تا تحت مدیریت یکپارچه با تعامل مداوم، برای تأمین امنیت فضای سایبر و پیشگیری از جرائم و در نهایت مقابله با جرائم سایبری اقدام کند. این رویکرد همچنین می‌بایست این نوع مدیریت را به‌عنوان ضرورتی ملی تلقی نماید.

رهبر معظم انقلاب اسلامی حضرت آیت‌الله‌العظمی امام خامنه‌ای(مدظله العالی) در دیدار با اعضای شورای عالی فضای مجازی، با اشاره به تأثیرگذاری گسترده فضای مجازی به‌عنوان یک قدرت نرم در عرصه‌های مختلف ازجمله فرهنگ، سیاست، اقتصاد، سبک زندگی، ایمان، اعتقادات دینی و اخلاقیات، بر لزوم طراحی مناسب و دقیق برای حفظ حریم امنیت فکری و اخلاقی جامعه در این عرصه تأکید نمودند: «لازمهٔ حضور فعال و تأثیرگذار در فضای مجازی، تمرکز در تصمیم‌گیری، جدیت در اجرا بدون ازدست‌دادن زمان، هماهنگی میان دستگاه‌ها و پرهیز از موازی‌کاری و تعارض است» (۱۶ شهریور ۱۳۹۴).[۵]

بر اساس آخرین آمارهای منتشرشده در سال ۲۰۱۹ هر ۱۴ ثانیه، یک نفر قربانی حمله باج‌افزار[۶] و هر ۳۹ ثانیه یک هک سایبری[۷] صورت می‌پذیرد و هر هفته نیز ۸۰هزار سایت با انگیزهٔ مجرمانه ساخته می‌شود. پیش‌بینی شده است که هزینه جرائم سایبری در جهان از سال ۲۰۱۵ با میزان ۳ تریلیون دلار در سال، به ۶ تریلیون دلار[۸] در سال ۲۰۲۱ برسد. انفجار داده نیز در راه است؛ به‌طوری که خدمات اینترنت اشیا[۹] از تعداد ۲ میلیارد دستگاه در سال ۲۰۰۶ که به‌صورت بی‌سیم با هم در

1.Hardware
2.Software
3.Information Society
4.Intelligent
5.Available at: http://www.leader.ir/fa/content//leader.ir
6.https://www.varonis.com/blog/cybersecurity-statistics/
7.https://www.cybintsolutions.com/cyber-security-facts-stats/
8.https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
9.Internet of Things (IOT)

ارتباط هستند، به حدود ۹,۹ میلیارد دستگاه در سال ۲۰۲۰ رسیده و طبق گزارش، این رقم در سال ۲۰۲۵ به ۲۱,۵ میلیارد دستگاه خواهد رسید.

به‌موازات رشد قارچ‌گونه جرائم سایبری در جهان، کشور عزیزمان نیز از این تهدیدها و آسیب‌ها، علی‌رغم همهٔ اقدامات صورت‌گرفته، مستثنا نبوده است. با نگاهی به رشد جرائم سایبری کشور، متوجه می‌شویم این جرائم از سال ۱۳۹۸ نسبت به سال ۱۳۹۷، رشد ۸۰ درصدی داشته است. اگر همین مقایسه نسبت به سال ۱۳۹۰ انجام شود رشد ۲۰۳۹ درصدی را شاهد خواهیم بود (سامانه بهره‌دهی، بازدید: ۱۵ اردیبهشت ۱۳۹۹). در بررسی جرائم سایبری رخ‌داده در جهان و کشور، یکی از مسائل اصلی که موضوع پیشگیری و مقابله با جرائم سایبری با آن مواجه است، چندپارگی مدیریت در عرصه سیاست‌گذاری، تصمیم‌سازی، برنامه‌ریزی، هدایت و نظارت است. حاصل این چندپارگی، پراکنده‌کاری و هم‌پوشانی و موازی‌کاری‌ها در عرصهٔ فضای سایبر است. بنابراین، نپرداختن به مسئلهٔ مطرح‌شده، منجر به اتخاذ تصمیم‌های ناهمگن، نامنسجم، بخشی‌نگر، پراکنده، ناکارآمد و ناموثر در حوزه‌های پیشگیری و مقابله و مبارزه با جرائم سایبری، به‌خصوص در تصمیم‌گیری‌های امنیتی می‌شود. همچنین ضمن موازی‌کاری و صرف هزینه‌های هنگفت مالی، بهره‌دهی مناسب، حاصل نخواهد شد و گاه حتی با شکست‌های اطلاعاتی و امنیتی نیز مواجه و موجب خدشه‌دارشدن امنیت داخلی و ملی و سایبری کشور خواهد شد.

در این راستا، باید اذعان نمود که این مسئله در ایران نیز همانند سایر کشورها خود را نشان داده است؛ به‌طوری که مقام معظم رهبری نیز بر ضرورت اقدام لازم در این خصوص تأکید نموده‌اند. در کشور، شورای عالی فضای مجازی تشکیل شده و هر دستگاهی به تناسب کار خود بخش‌های مشابه را راه‌اندازی نموده است. قوه قضاییه، دادسراهای ویژه جرائم رایانه‌ای را راه‌اندازی نمود و قانون مبارزه با جرائم رایانه‌ای به تصویب مجلس شورای اسلامی رسید. ناجا نیز برحسب نتایج ناشی از عملیات‌های اطلاعاتی در سال ۱۳۸۹ پلیس فتا را راه‌اندازی نمود که تأکید و رسیدگی‌های مکرر فرماندهی محترم ناجا نیز مبین وجود مسئله و ضرورت رفع آن است. به این مسئله به‌قدری توجه شده که در زمرهٔ تحقیقات مورد نیاز دفتر تحقیقات فتا، دانشگاه علوم انتظامی امین، قوه قضائیه و... محسوب شده است. شاید لازم است که تأکید کنیم امروزه پس از طی رویکردهای قضایی، امنیتی، پلیس جامعه‌محور و پلیس داده‌محور تا مرحله پلیس اطلاعات‌پایه قرار گرفته‌ایم. تاکنون در کشور اقدامات درخور توجهی در راستای تأمین امنیت فضای سایبر، چه ساختاری و چه

عملیاتی انجام شده است؛ ولی این اقدامات در راستای مدیریت یکپارچهٔ مقابلهٔ با جرائم سایبری در کشور پاسخ‌گو نبوده و موفقیت لازم را نداشته است. با این توصیف، تحقیقِ پیش‌رو در گام اول به دنبال آن است که به شناخت ابعاد و مؤلفه‌ها و شاخص‌های عوامل مؤثر بر پیشگیری و مقابله با جرائم سایبری، اعم از رصد، تشخیص، پیش‌بینی، پیشگیری و مبارزه با جرائم سایبری در جمهوری اسلامی ایران بپردازد. سپس الگوی راهبردی مناسبی را در راستای مدیریت یکپارچه و هم‌افزای پیشگیری و مقابله با جرائم سایبری، به‌منظور تعیین جهت‌گیری‌ها و مسیرهای آینده، برای وصول به اهداف اتخاذشده، احصا و پیشنهاد نماید. در عین حال، نوشتار حاضر به مشارکت و همکاری همهٔ سازمان‌های ذی‌ربط بر اساس سیاست‌های ابلاغی، قوانین و اسناد بالادستی، توجه دارد و نظرات کارشناسان و خبرگان این حوزه را بررسی می‌کند.

حال این پرسش مطرح می‌شود: «الگوی راهبردی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران کدام است؟»

پیشینه تحقیق

با توجه به اهمیت موضوع تحقیق و به‌منظور آشناشدن با نظرات دیگر صاحب‌نظران داخلی و خارجی، در بررسی انجام‌شده در تحقیقات داخلی و خارجی و اسناد راهبردی، مکتوباتی نیز مطالعه و بررسی اجمالی شدند که جستارهایی هم‌سو با موضوع این تحقیق انجام داده بودند. این مکتوبات، پروژه‌های تحقیقاتی و رساله‌ها و مقالاتی را شامل می‌شدند که حول الگوهای راهبردی، فضای سایبر، جرائم سایبری، دفاع سایبری و مدیریت یکپارچه به نگارش درآمده بودند. لذا خلاصه آن‌ها به شرح زیر ارائه می‌شود:

دکتر کی جایشانکار[1] (جولای ۲۰۱۰) در پروژهٔ تحقیقاتی با عنوان «جرائم سایبری، چالش‌ها و فرصت‌های پیش‌رو» اشاره می‌کند که چون گسترش دامنهٔ نفوذ فضای سایبری در زندگی انسان باعث ایجاد اشکال مختلف جرائم سایبری گردیده، لذا لازم است به‌منظور مقابله با آن، جرم‌شناسی سایبری نیز در درجهٔ اول برای شناسایی و تلاش برای پیشگیری و در درجهٔ دوم برای تعقیب و مجازات مرتکبان آن صورت پذیرد.

گروهی از دانشجویان دوره یکم مدیریت راهبردی فضای سایبری (۱۳۹۷) در رسالهٔ مطالعات

1.Dr K. Jaishankar

گروهی خود با عنوان «طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن» اشاره داشته‌اند که به‌منظور حضور مقتدرانهٔ کشور در فضای سایبر، ضرورت دارد ساختار یکپارچه و بومی دفاع سایبری کشور فراهم شود. لذا برای دستیابی به این هدف، ضمن توجه به ابعاد و مؤلفه و شاخص‌های دفاع سایبری، فرایندها، نهادها و روابط بین آن‌ها بررسی و ترسیم، و در نهایت نیز چارچوب زکمن به‌منظور طراحی نظام مد نظر انتخاب شده است. همچنین با استفاده از سطح راهبردی آن و طی مراحل مختلف، متدولوژی فوق با استفاده از مفاهیم مبانی نظری و مطالعات تطبیقی، فرایندها و نهادهای نظام دفاع سایبری تعیین شده است.

احسان شهیر (۱۳۹۷) در رسالهٔ دکترا با عنوان «طراحی الگوی راهبردی بومی امنیت فضای سایبر» به‌دنبال تدوین الگوی راهبردی بومی امنیت فضای مجازی کشور است. وی چهار بُعد اصلی را مشخص کرده که عبارت‌اند از: ۱. بعد فاعل، حوزهٔ عوامل عملیاتی (بازیگران، نقش‌آفرینان، ذی‌نفعان)؛ ۲. بعد بستر امن؛ ۳. بعد روش، رویکرد بومی‌سازی (تاروپود تلاقی ارزش‌ها و اهداف)؛ ۴. بعد فعل (حوزهٔ فرماندهی و کنترل) (ابعاد عملکردی، اقدامات، راهکارها)، مهندسی امنیت فضای مجازی.

به تعبیر دیگر، بر اساس نظر دکتر شهیر، فضای مجازی به‌عنوان توانمندساز فضای فیزیکی دارای چهار محور و عوامل عملیاتی، حوزهٔ فرماندهی و کنترل، بستر امن و رویکرد بومی‌سازی است. بر این اساس، ایشان در نهایت الگوی راهبردی بومی امنیت فضای مجازی کشور را استخراج نموده است.

غلامرضا شاه‌محمدی و منصور تاهو (۱۳۹۳) در مقاله‌ای با عنوان «بررسی شیوه‌های پیشگیری از جرائم سایبری؛ مبتنی بر فناوری اطلاعات» اشاره داشته‌اند، فضای مجازی با وجود مزایای فراوان، به‌دلیل ویژگی‌های خاص خود کار سازمان‌های متولی برقراری نظم و امنیت را دشوار می‌کند. نتایج تحقیق آن‌ها نشان می‌دهد که شیوه‌های مبتنی بر فناوری اطلاعات شامل ردیابی هویت مجازی مهاجمان، گشت مجازی و نظارت بر فضای سایبر، جمع‌آوری ادلهٔ الکترونیکی جرم و مستندسازی صحنهٔ جرم در پیشگیری از جرائم سایبر تأثیر دارد.

منصور روضه‌ای و همکاران (۱۳۹۶) در مقاله‌ای با عنوان «ابزارهای پیشگیری از جرائم نوظهور در فضای مجازی» اشاره کرده است که عوامل آموزش و آگاه‌سازی کاربران اینترنت درخصوص کلاهبرداری اینترنتی، آموزش کاربران درخصوص خدمات بانکداری الکترونیک از سوی بانک‌ها و

استفاده از نرم‌افزارهای امنیتی و ضد جاسوس افزارها توسط کاربران، بیشترین تأثیر را در کاهش کلاهبرداری اینترنتی داشته‌اند.

جواد جهانشیری و همکاران (۱۳۹۴) در تحقیقی با عنوان «تبیین فرایند تحقیقات مقدماتی در جرائم سایبری» با نگاهی به اقدامات، در قبل و حین و بعد از وقوع جرائم سایبری اشاره داشته‌اند که اقدامات پی‌جویی جرائم سایبری در مراحل رصد، پیش‌بینی، پیشگیری و مبارزه با جرائم، احصا و ملاحظه شد که بیشترین اقدام قانون و روند تحقیقات مقدماتی در مرحلهٔ مبارزه با جرائم سایبری است.

محمدمهدی قوچانی خراسانی و همکاران (۱۳۹۶) در تحقیقی با عنوان «الگوی حکمرانی شبکه‌ای با تأکید بر توسعهٔ فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری» به نهادهای متنوعی اشاره کرده‌اند که در کشور در حوزهٔ امنیت فضای سایبری فعالیت می‌کنند. سپس اظهار داشته‌اند که کشور نیازمند فعال‌سازی ظرفیت این نهادها از طریق تدوین سیاست‌های یکپارچه از سوی شورای عالی فضای مجازی است.

کایرژانوا،[1] موراشبکوف،[2] بیسنف[3] (۲۰۱۵) در مقاله‌ای با عنوان «روش‌های بهبود مبارزه با جرائم اینترنتی در کشورهای توسعه‌یافته» به بررسی روش‌های پیشرفته مبارزه با جرائم اینترنتی در کشورهای توسعه‌یافته می‌پردازند. سپس امکان استفاده از آن‌ها را برای اجرای قانون در جمهوری قزاقستان، به‌عنوان یک کشور در حال توسعه، به سنجش می‌گذارند. آنان اذعان داشتند که فرصت‌های اقتصادیِ فناوری‌های رایانه‌ای موجب جذابیت برای جنایتکاران می‌شود. آنان در این تحقیق، به طبقه‌بندی روش‌های پیشرفتهٔ معاصر در ارتباط با مبارزه با جرائم اینترنتی پرداخته و به نتایجی دربارهٔ کاربرد جامع آن‌ها و برخی از اقدامات دقیق برای بهبود قوانین کیفری جمهوری قزاقستان دست یافته‌اند.

با توجه به تأثیر پیشینه‌های تحقیق در دانش‌افزایی و غنای تحقیقات علمی، پیشینه‌های شناسایی‌شده با موضوع تحقیق قرابت مستقیم ندارند. اغلب آن‌ها بخش‌های خاصی از کاربرد، کارایی، فرصت‌ها، تهدیدها و آسیب‌های حوزهٔ فضای سایبر را بررسی کرده‌اند. اگرچه نمی‌توان نقش پیشینه‌ها را در استفاده و دانش‌افزایی در این تحقیق انکار کرد، باید گفت ازآنجاکه این تحقیق

1.Kirjanova
2.Murashbekov B
3.Beisenov B

الگوی راهبردی مدیریت یکپارچه مقابله با جرائم سایبری کشور را ارائه می‌دهد، با بررسی‌های علمی، چالش‌های مدیریت در حوزهٔ پیشگیری و مقابله با جرائم را شناسایی نموده است. سپس با بررسی‌های لازم در رابطه با زمینه‌های قانونی و مبانی نظری مرتبط با موضوع، به تبیین و ارائهٔ الگویی به‌منظور استقرار مدیریت یکپارچه در حوزهٔ پیشگیری و مقابله با جرائم در کشور پرداخته است.

مبانی نظری تحقیق

مبانی نظری در رابطه با یک موضوع، به توصیف پدیده یا موضوع می‌پردازد و علل شکل‌گیری و زمینه‌ای موضوع مد نظر را تبیین می‌نماید. تجربیات ملی و جهانی نشان می‌دهد که تدوین اسناد بالادستی، ایجاد و راه‌اندازی سازمان‌ها و نهادها در حوزه سایبر به‌تنهایی پاسخ‌گوی نیازهای امنیتی و عملیاتی نیست. بنابراین باید به این موضوع در کنار تغییرات ساختاری، فرهنگ‌سازی و مدیریت هم‌افزا در سطوح مختلف توجه شود.

الگوی راهبردی:[1] بر اساس تعریف مرکز الگوی اسلامی‌ایرانی پیشرفت (۱۳۹۱)، الگو یک نقشهٔ جامع است که هدف و سمت حرکت، شیوهٔ حرکت و نحوهٔ رفتار جامعه را برای تحقق‌یافتن تحول تکاملی جامعه بیان می‌کند. لفظ «راهبرد» نیز از ترکیب دو کلمه راه و بُرد تشکیل شده است. راهبرد راهی است که ما را به هدف می‌رساند، مأموریت را محقق می‌سازد و به چشم‌انداز معنی می‌بخشد. راهبرد به طراحی یک نقشهٔ عملیاتی برای دستیابی به اهداف ازپیش‌تعیین‌شده اطلاق می‌شود. راهبرد عبارت است از برنامه‌ای که مسیر رسیدن به اهداف اساسی را مشخص می‌کند (حسن‌بیگی، ۱۳۹۰: ۴۸). منظور از الگوی راهبردی، الگوی منسجمی است که با تنظیم منطقی عوامل و مؤلفه‌های اصلی راهبردی، روابط بین آن‌ها را به بهترین شکل ممکن ترسیم نموده و چگونگی دستیابی به اهداف را میسر سازد (حمیصی، ۱۳۹۱: ۱۶).

الگوی (مدیریت) راهبردی: الگویی است که در آن ابعاد، مؤلفه‌ها، زیرمؤلفه‌ها و روابط بین آن‌ها را جهت تصمیم‌سازی و تصمیم‌گیری نشان دهد (نظام حکومتی الگو، دانشگاه عالی دفاع ملی).[2]

با توصیف فوق، آنچه در این تحقیق از الگوی راهبردی مد نظر است، الگویی است متشکل از ابعاد و مؤلفه‌ها و روابط بین آن‌ها که در مدیریت راهبردی در راستای رسیدن به اهداف راهبردی

1.Strategic Model
2.5. Available at: http://sndu.ac.ir/content

با توجه به اوضاع داخلی و خارجی یک کشور کاربری دارد. همچنین جهت‌گیری‌ها و مسیرهای آینده را برای وصول به اهداف اتخاذشده تبیین می‌نماید که در این راستا با نظر خبرگان و مدیران، ضمن تعیین اولویت‌ها، میزان مرتبط‌بودن عناصر مؤثر موجود شناسایی می‌شود و در نهایت به‌عنوان الگوی مرجع، تعمیم‌پذیر خواهد بود.

مدیریت یکپارچه:[1] اصول مدیریت شامل برنامه‌ریزی، سازماندهی، بسیج منابع و امکانات، هدایت و سرپرستی، نظارت و کنترل است. با توجه به این تعریف، مدیریت یکپارچه عبارت است از اینکه تمام فعالیت‌های مربوط به ارائهٔ خدمات در هر حوزه تحت مدیریت واحد درآید، بدون آنکه به اصل تقسیم کار بین لایه‌های عملکردی سیستم خدشه‌ای وارد شود (صیدی، ۱۳۹۵: ۲۱). مدیریت یکپارچه، تلاشی منظم و سازمان‌یافته در راستای اتخاذ تصمیم‌ها و مبادرت به اقدامات بنیادی و اساسی است. به‌منظور تحقق یکپارچگی، شناسایی عوامل مؤثر بر یکپارچگی و تفرق در مدیریت ضروری است. چهار عامل شبکه نهادها و سازمان‌های متعدد ذی‌ربط در مدیریت جرم و نظام و روابط قدرت بازیگران عرصهٔ اجتماعی، بستر قوانین و مقررات موجود و همچنین زیرساخت‌های اطلاعاتی و ارتباطی، ازجمله عوامل مؤثر بر یکپارچگی یا عدم یکپارچگی مدیریت هستند. دستاوردها و مزایای مدیریت یکپارچه عبارت‌اند از: بهبود مستمر سیستم‌ها و فرایندها؛ بهبود وضعیت امن؛ کاهش تماس شغلی با عوامل زیان‌آور؛ ارتقاء رضایتمندی؛ ارتقاء دانش سازمانی و عملیاتی با اجرای برنامه‌های مناسب و متناسب آموزشی؛ انطباق با قوانین و مقررات حاکم بر فعالیت‌ها؛ خدمات و ارتقاء مداوم کیفیت خدمات و محصولات در تمام حوزه‌های انسانی.

با توجه به شرح فوق، می‌شود مدیریت یکپارچه را در کشور چنین تعریف کرد: «فرایند به‌کارگیری مؤثر و کارآمد منابع انسانی، فنی، امنیتی و محتوایی کلیهٔ سازمان‌ها و نهادهای دولتی و غیر دولتی در سطح ملی برای برنامه‌ریزی، سازماندهی، بسیج منابع و امکانات، هدایت و کنترل با هدف دستیابی به اهداف ملی و انقلابی، بر اساس نظام ارزشی و دینی به‌منظور پیش‌بینی، پیشگیری، حفظ، حمایت از ارزش‌ها، منافع و دارایی‌های ملی و دینی و مذهبی در مقابل تهدیدها و آسیب‌ها در راستای حفظ دارایی‌های زیرساختی و عمومی و خصوصی.»

عوامل مؤثر بر مدیریت یکپارچه: یکی از مسائل اصلی که امروزه کشور در حوزه‌های مختلف با آن مواجه است، چندپارگی، مدیریت در عرصهٔ سیاست‌گذاری، تصمیم‌سازی، برنامه‌ریزی،

1.Integrated management

هدایت و نظارت است. چندپارگی این سیستم به‌لحاظ مدیریتی آسیب‌زا بوده و باعث به‌وجودآمدن مشکلاتی مانند پراکنده‌کاری‌ها، هم‌پوشانی‌ها و موازی‌کاری‌ها در زمینه‌های مختلف خدماتی و اجرایی شده است. مشکلاتی که در نهایت منجر به ناکارآمدی سیستم مدیریتی می‌شود. به‌منظور تحقق یکپارچگی، شناسایی عوامل مؤثر بر یکپارچگی و تفرق در مدیریت ضروری است. عواملی اعم از محیط، شبکه نهادها و سازمان‌های متعدد ذی‌ربط در مدیریت (اعضا)، نظام و روابط قدرت بازیگران عرصهٔ خدمات (فرایند/ساختار)، بستر قوانین و مقررات موجود و همچنین زیرساخت‌های اطلاعاتی و ارتباطی و اهداف، ازجمله عوامل مؤثر بر یکپارچگی مدیریت است که بر اساس هر حوزه قابل تعمیم و تفسیر موضوعی است.

نظریه‌ها در مدیریت یکپارچه: نظر به ویژگی‌ها، قابلیت‌ها و عوامل موصوف به‌منظور تحقق مدیریت در سطوح کلان و فراسازمانی، لازم است بر اساس اصول منطقی، برنامه‌ریزی و در سایهٔ تعامل، همکاری، هم‌افزایی و یکپارچگی این امر تحقق یابد. لذا برخی نظریه‌ها و روش‌های معمول مدیریتی با رویکردهای نوین عبارت‌اند از:

الف. رویکرد (نگرش) سیستمی: نگرش سیستمی یا کل‌گرایی، تاریخی طولانی در سیر تفکرات جامعهٔ بشری دارد. اصطلاح سیستم برای پوشش‌دادن مجموعهٔ وسیعی از پدیده‌ها به کار می‌رود. چالشی که رویکرد سیستم‌ها با آن روبه‌رو است، این است که چگونه سیستم‌های عملکردی مختلف با یکدیگر مرتبط شود (اسکاگ،[1] ۲۰۱۴: ۳۸). این چالش‌ها باید در یک تفکر سیستمی مد نظر قرار گیرند تا بشود مؤثرترین مداخلات هماهنگ‌شدهٔ استراتژیک و نقاط قابل اتکا را شناسایی نمود (صیدی، ۱۳۹۵: ۳۹ و ۴۰).

ب. رویکرد حکمرانی شبکه‌ای:[2] مفهوم حکمرانی ریشه در تاریخ سیاست دارد. مطالعه بر شبکه‌ها را می‌شود به جامعه‌شناسی نسبت داد. به‌طور کلی حکمرانی شبکه‌ای از طریق شبکه، چهار روند اثرگذار است که شکل بخش‌های دولتی را در سراسر عالم تغییر داده است: ۱. رشد روزافزون برون‌سپاری عمومی؛ ۲. شکل‌گیری دولت یکپارچه؛ ۳. انقلاب فناوری اطلاعات؛ ۴. تقاضای شهروندان (ایمانیان و منوریان، ۱۳۹۴: ۴).

ج. پنجره واحد خدمات: پنجرهٔ واحد، یک سیستم است و به‌عنوان یک مفهوم، فرایند یا محیط توصیف می‌شود. پنجرهٔ واحد افراد و سازمان‌های دولتی را قادر می‌سازد اطلاعات را از

1.Skaug Lene
2.Network Governance

طریق یک نقطهٔ دستیابی به‌دست آورند که در حال حاضر معمولاً به‌صورت الکترونیکی تشکیل می‌شود. پنجره‌های واحد در شکل‌های مختلف اجرا می‌شوند و بر اساس حوزه و دامنهٔ برنامه‌های پوشش‌داده‌شده یا ارجاع‌شده، خدمات متنوعی را ارائه می‌دهند. با وجود این، می‌شود عملکرد مرکزی یک پنجرهٔ واحد را به این صورت تعریف کرد: پنجرهٔ واحد یک ورودی واحد برای ارائهٔ خدمات دولتی در یک میدان موضوعی خاص یا برای یک هدف خاص و گروه هدف مشخص است (ابکن،[1] ۲۰۱۴: ۲).

د. هماهنگ‌سازی سیاستی: هماهنگ‌سازی سیاستی، یک پروسهٔ پیوستهٔ ادغام و تعدیل و اولویت‌بندی اهداف در حوزه‌های مختلف همچون اقتصادی، اجتماعی، فرهنگی و اهداف بوم‌شناختی، به‌منظور فعال‌کردن همکاری‌ها، است. به‌طور کلی هماهنگ‌سازی، اصلی پیوسته و رویه‌ای است که هدف آن چنین است: ۱. اجتناب یا به‌حداقل‌رساندن تکرار (تقلید) و همپوشانی و ناهماهنگی سیاست‌های حکومت و تناقض‌های سیاسی و دیوان‌سالارانه (امور اداری)؛ ۲. توسعهٔ دیدگاه‌های وسیع و منسجم در سطح حکومت و تنظیم اولویت‌ها به‌جای تنظیم دیدگاه‌های محدود و فرعی. هماهنگ‌سازی سیاست، یک مسئلهٔ یا همه یا هیچ نیست، بلکه ممکن است به زمان و حوزه خاصی محدود شود (ویتولا[2] و سنفلد،[3] ۲۰۱۵: ۲).

فضای سایبری:[4] بر اساس تعریف انستیتو شرق ـ غرب آمریکا و انستیتو امنیت اطلاعات دانشگاه دولتی مسکو در واژه‌نامهٔ مشترک اصطلاحات امنیت فضای سایبر: فضای سایبر، محیط الکترونیکی است که اطلاعات در آن تولید، ارسال، دریافت، ذخیره‌سازی، پردازش و حذف می‌شود. به عبارتی، فضای سایبر مجموعه‌ای است از سیستم‌های الکترونیکی و شبکه‌های رایانه‌ای، شامل نیروی انسانی، زیرساخت‌ها، تجهیزات سخت‌افزاری، سیستم‌های ارتباطی و کنترلی و مدیریت، به‌منظور تولید، ذخیره‌سازی، پردازش، تبادل، بازیابی، حذف و بهره‌برداری از داده‌ها (کارگروه مطالعات گروهی دانشجویان، ۱۳۹۲). مرکز ملی فضای مجازی کشور نیز با مبنا قراردادن وجه انسانی و نه بستر فناورانه و تعاملات اطلاعات، فضای مجازی را امتداد فرهنگ و اجتماع انسانی در شبکه‌های اطلاعاتی می‌داند. به‌عبارتی دیگر، فضای مجازی را اجتماع و فرهنگ نوین انسانی می‌داند که در

1.Ebken
2.Vitola Alise
3.Senfelde Maija
4.Cyber Space

بستر فناوری اطلاعات و ارتباطات شکل می‌گیرد. این مرکز مدل چندلایهٔ فضای مجازی را مطابق شکل ۱ ارائه می‌نماید (مرکز ملی فضای مجازی، ۱۳۹۶).

شکل۱: مدل چندلایه فضای مجازی کشور

حوزه‌های اثرگذاری فضای سایبر: جامعیت فضای سایبر ایجاب می‌کند به همهٔ شئون و ابعاد مرتبط با فضای سایبر در هر حوزه و عرصه توجه شود و همچنین به نقش فضای سایبری از زوایای مختلف و مرتبط به‌صورت تخصصی نگریسته شود. در نگاهی کلی می‌توان کارکرد و آثار فضای سایبر را در حوزه‌های نمایان در جدول ۱ دسته‌بندی کرد.

ابعاد و محورهای فضای سایبر	حوزه‌ها																	
	بهداشت و درمان	دینی	فرهنگی	امنیتی	دفاعی	انتظامی	اجتماعی	سیاسی	علم و فناوری	خدمات	حقوقی	اقتصادی	بازرگانی	صنعتی	رسانه‌ای	بین‌المللی	محیط زیست
مدیریتی																	
فنی																	
محتوایی																	
امنیتی																	

جدول ۱: تقسیم‌بندی حوزه‌های اثرگذار فضای سایبر (ثقفی، ۱۳۹۳)

ابعاد فضای سایبر: فضای سایبری به‌دلیل ماهیت سیال ناشی از معماری کلان، ابعاد گسترده و گوناگونی دارد که برای ارتباط صحیح بین آن‌ها نیاز به همبستگی و معماری یکپارچه است. ابعاد فضای سایبر را می‌شود به بعد مدیریتی، فنی، محتوایی و امنیتی تقسیم نمود.

جرائم سایبری: از زمانی که به‌طور جدی جرم سایبری در جهان مطرح شده، نظر نهادها و سازمان‌ها و اندیشمندان و حقوق‌دانان به آن جلب شده است. جرائم سایبری را می‌شود از دو منظر تعریف کرد. در تعریف مضیق، جرم سایبری اساساً منحصر و محدود به نفوذ غیر مجاز، تحریف یا تخریب از طریق کدهای رایانه‌ای، جاسوسی رایانه‌ای، جعل و کلاهبرداری رایانه‌ای است. این تعریف،

آزار و اذیت، سوءاستفاده از پست الکترونیک، سرقت و افترا از طریق سیستم‌های رایانه‌ای را شامل نمی‌شود. در تعریف موسع، جرم سایبری شامل هر فعل یا ترک فعلی می‌شود که از طریق یا به‌کمک رایانه یا از طریق شبکه‌های رایانه‌ای یا از طریق اینترنت، به‌طور مستقیم یا غیر مستقیم انجام می‌شود و قانون آن را منع کرده و برای آن مجازات مالی یا غیر مالی در نظر گرفته است (ترکمان، ۱۳۹۱: ۲۳). به‌طور کلی، هر اقدام مجرمانه در فضای مجازی، مجموعه اعمالی است که برای ایجاد اختلال، قطعی، کاهش کیفیت یا نابودی اطلاعات مقیم در رایانه‌های موجود در فضای سایبری انجام شده و معمولاً بر روی یک یا مجموعه‌ای از سامانه‌های هدف متمرکز می‌شود (حسینی و ظریف‌منش، ۱۳۹۲: ۴۸).

نظر به تعاریف فوق می‌شود جرم سایبری را چنین بیان کرد: جرم سایبری فعل یا ترک فعلی است که موجب ایجاد اختلال، قطعی، کاهش کیفیت، ایراد خسارت، جعل، تغییر یا حذف اطلاعات (سرمایه‌های سایبری) در بستر سامانه‌های مورد بهره‌برداری در فضای سایبری یا شبکه‌های وابسته به آن می‌شود. این بسترها و سامانه‌ها شامل 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) می‌شود. در عین حال، اختلال‌ها ممکن است در ابعاد فنی، محتوایی و امنیتی و هر یک از فرایندهای تولید، پردازش، ذخیره‌سازی، مبادله، بازیابی و بهره‌برداری از اطلاعات باشد که در قانون برای آن مجازات تعیین شده است.

ویژگی‌های جرائم سایبری: جرائم سایبری خصوصیاتی متفاوت از جرائم سنتی دارند که همین موضوع باعث ایجاد روند ویژه‌ای در رسیدگی، تحقیقات و پی‌جویی پرونده‌ها شده است. جدول ۲ به این ویژگی‌ها اشاره می‌کند:

وجوه	توضیح و تبیین ویژگی‌ها
شکل ارتکاب	در جرائم سایبری شکل ارتکاب کاملاً متفاوت و بر اساس پیشرفت سریع فناوری، متغیر است و اختلاف‌های محسوسی دارد.
ابزار ارتکاب جرم	در جرائم سایبری هر روز بر مبنای توسعه فناوری ابزار شکل جدیدتری به خود می‌گیرند که بیشتر در قالب برنامه‌های نرم‌افزاری و ناملموس و نامحسوس است.
انتخاب هدف	در فضای سایبر اهداف و اشیا وجود خارجی ندارند؛ اگرچه دارای نمود خارجی هستند.

زمان ارتکاب جرم	جرم در فضای سایبر وابسته به زمان نیست (امکان انجام جرم در هر ساعت از شبانه‌روز) و به حداقل زمان می‌رسد.
مکان ارتکاب جرم	فضای سایبر فرامرزی است و جغرافیا ندارد و از هر منطقه امکان ارتکاب جرم وجود دارد. لذا در جرائم سایبری، محل ارتکاب، شیوه و شگرد، تعداد مجرمان، ابزارها، تعداد متعدد آماج و هدف‌ها حذف می‌شود.
وسعت	در جرائم سایبری سازمانی ممکن است با وسعت بیشتر از نظر زمانی، مکانی و تعداد جرم مواجه شویم.
بزه‌دیده	در جرائم سایبری مال‌باخته یا بزه‌دیدگان زیادی در کمترین زمان دچار آسیب می‌شوند.
مشارکت در جرم	جرائم سایبری بیشتر به‌صورت انفرادی صورت می‌گیرد؛ مگر در جرائم سازمان‌یافته خاص که نیاز به تخصص‌های متفاوت دارد.
هویت	در جرائم سایبری معمولاً در قبل و حین و بعد از ارتکاب جرم هویت مجرم یا مجرمان پنهان است.

جدول ۲: ویژگی‌های جرائم سایبری (اقتباس از: حسینی و همکاران، ۱۳۹۴: ۸)

وضعیت جرائم و حوادث سایبری در کشور: با راه‌اندازی پلیس فضای تولید و تبادل اطلاعات (فتا) آمار درصد رشد وقوع، کشف و دستگیری مجرمان حوزهٔ جرائم سایبری مشخص شده است.

درصد رشد کشف جرائم سایبری کشور / سال	۱۳۹۰	۱۳۹۱	۱۳۹۲	۱۳۹۳	۱۳۹۴	۱۳۹۵	۱۳۹۶	۱۳۹۷	۱۳۹۸	درصد رشد وقوع جرائم سایبری کشور
۱۳۹۰	*	٪۶۱	٪۱۲۵	٪۲۶۹	٪۳۵۴	٪۴۳۷	٪۱۳۴۴	٪۱۹۳۹	٪۳۶۳۲	
۱۳۹۱	٪۱۶۴	*	٪۵۶	٪۱۲۹	٪۱۸۲	٪۲۳۳	٪۷۹۵	٪۱۱۶۵	٪۲۲۲۷	
۱۳۹۲	٪۳۲۸	٪۶۲	*	٪۴۷	٪۸۰	٪۱۱۳	٪۴۷۲	٪۷۰۸	٪۱۳۸۶	
۱۳۹۳	٪۵۷۹	٪۵۷	٪۵۸	*	٪۲۲	٪۴۵	٪۲۹۰	٪۴۵۱	٪۹۱۴	
۱۳۹۴	٪۶۹۷	٪۲۰۱	٪۸۶	٪۱۷	*	٪۱۸	٪۲۱۷	٪۳۴۸	٪۷۲۵	
۱۳۹۵	٪۸۱۵	٪۲۴۶	٪۱۱۳	٪۳۴	٪۱۴	*	٪۱۶۸	٪۲۷۹	٪۵۹۸	
۱۳۹۶	٪۱۵۶۸	٪۵۳۱	٪۲۸۹	٪۱۴۵	٪۱۰۹	٪۸۲	*	٪۴۱	٪۲۷۹	
۱۳۹۷	٪۱۸۹۰	٪۶۵۳	٪۳۶۵	٪۱۹۳	٪۱۴۹	٪۱۱۷	٪۱۹	*	٪۸۳	
۱۳۹۸	٪۵۱۶۱	٪۱۸۵۴	٪۱۱۰۵	٪۶۲۵	٪۱۱۰۵	٪۴۶۳	٪۲۰۹	٪۸۷	*	

درصد رشد کشف جرائم سایبری کشور

جدول ۳: درصد رشد وقوع و کشف جرائم سایبری کشور

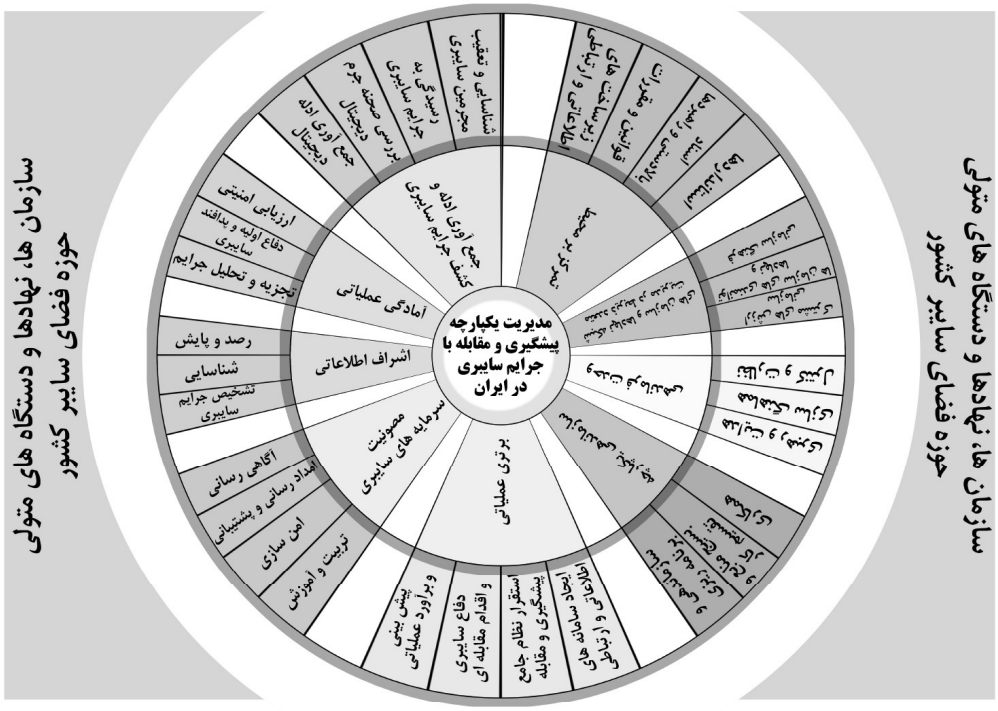
پیشگیری از جرائم سایبری: پیشگیری از جرم به مجموعه اقداماتی گفته می‌شود که برای جلوگیری از فعل و انفعال زیان‌آور محتمل برای فرد یا گروه یا هر دو به‌عمل می‌آید؛ مثل پیشگیری از جرائم جوانان و پیشگیری از حوادث در جاده‌ها (رجبی‌پور، ۱۳۸۲: ۱۵). دربارهٔ دسته‌بندی انواع پیشگیری همواره نگرش‌های متفاوتی بین صاحب‌نظران و جرم‌شناسان وجود دارد. انواع پیشگیری از جرم عبارت است از: پیشگیری اولیه، ثانویه، ثالث، کوتاه‌مدت، بلندمدت، انفعالی، فعال، کیفری، غیر کیفری، قضایی، انتظامی، اجتماعی و... (بیات و همکاران، ۱۳۸۷: ۵). گستردگی و افزایش جرائم سایبری در دههٔ اخیر، امری اجتناب‌ناپذیر بوده است. بدون شک با پیشرفت علم و فناوری، زمینهٔ ارتکاب جرائم جدید که حاصل استفاده از این علوم است، بیشتر از گذشته فراهم خواهد شد. پیشگیری از ارتکاب جرائم سایبری حتی در صورت به‌کارگیری تمامی روش‌های پیشگیری و اصول و قواعد علمی مربوط به علم جرم‌یابی و دیگر علوم ناممکن خواهد بود؛ زیرا به‌دلیل خصایص گستردهٔ فضای سایبر و متغیربودن آن، امکان مقابلهٔ همه‌جانبه و فراگیر از این جرائم وجود ندارد.

مقابله با جرائم سایبری: منظور از مقابله با جرائم در این تحقیق، شناسایی و بررسی و جستجوی اطلاعات مرتبط با جرم یا اشراف و تکمیل اطلاعات افعال مجرمانه در فضای سایبر است که به‌طور مستقیم یا غیر مستقیم در رصد، تشخیص، شناسایی، کشف و مبارزه با جرائم مؤثر واقع می‌شود. از آنجا که هدف از فرایند موصوف پی‌جویی و در نهایت پیشگیری یا کشف جرم است، هدف از مقابله با جرائم سایبری چنین است: ایجاد امنیت در ابعاد فنی، محتوایی، امنیت سامانه‌ها و شبکه‌ها در حوزهٔ زیرساختی؛ تبیین فرایند پیشگیرانه و کنترلی با هدف ایجاد اقدام تشخیصی، کنترلی و برخورد با اهداف ازپیش‌تعیین‌شده. در این راستا، می‌شود تدابیر و راهبردها را در قالب اقدام اسنادی و قانونی (تقنینی) و وظایف و اقدام عملیاتی (مدیریتی و مشارکتی) تبیین و برای هر یک مصادیقی ارائه نمود.

مدل مفهومی تحقیق

از لحاظ مفهومی این چهارچوب فرایندی را تبیین می‌کند که پیش از آنکه جنبهٔ فنی را تبیین کند، بیشتر جنبهٔ مدیریتی و عملیاتی دارد. این چارچوب تمام ابعاد سازمان‌های متولی حوزهٔ پیشگیری و مقابله با جرائم رایانه‌ای نظیر کاربران، بخش‌های امنیت سخت‌افزار، نرم‌افزار، شبکه و نحوهٔ توزیع و دسترسی به سامانه‌ها، فرایندهای حرفه، انگیزهٔ کاربران، راهبردها، مأموریت‌ها، قوانین و استانداردهای ابلاغی و... را در نظر می‌گیرد. در شکل ۲ الگوی نظری (مدل مفهومی) تحقیق

بر اساس جهت‌سازهای نظری و ادبیات موضوعی تدوین و ترسیم شده است. این شکل همچون دریچه‌ای است که محقق از آن منظر به پدیده مورد بررسی نگاه می‌کند.



شکل ۲: مدل مفهومی تحقیق

روش‌شناسی تحقیق

از آنجایی که این تحقیق به دنبال ارائه الگوی راهبردی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در کشور است، روش این تحقیق برحسب نوع (هدف) در زمره تحقیقات کاربردی و تبیینی و به‌لحاظ بسط نتایج تحقیق در زمره کاربردی‌توسعه‌ای است. رویکرد در این پژوهش از نوع آمیخته و ترکیبی است که از تحلیل‌های کمّی و کیفی بهره‌گیری می‌شود. جامعه آماری این تحقیق ۷۰ نفر هستند. از عمده معیارهای این افراد داشتن مشاغل و سوابق اجرایی و مدیریتی، آگاهی‌داشتن از فرصت‌ها و قابلیت‌های فضای سایبر کشور، صاحب‌نظران حوزه انتظامی و قضایی و امنیتی آشنا به اهداف نظام بر اساس اسناد بالادستی و راهبردی و قوانین و مقررات مربوط به جرائم سایبری و... بوده است.

برای آنالیز داده‌ها و سؤال‌های تحقیق از روش‌های موجود در آمار توصیفی و استنباطی با استفاده از نرم‌افزار SPSS26 و نرم‌افزار Smart PLS و با به‌کارگیری آزمون‌های مختلف، داده‌ها، تجزیه و تحلیل شده و سؤال‌ها بررسی شده است.

برای محاسبهٔ ضریب آلفای کرونباخ ابتدا واریانس نمره‌ای هر یک از مؤلفه‌ها و متغیرها و سپس واریانس کل پرسش‌نامه محاسبه شد (جدول). ازآنجاکه مقدار آلفای کرونباخ بالاتر از ۰/۷ است، نشانگر پایایی قابل قبول است. برای بررسی میزان اعتبار و پایایی این تحقیق از نرم‌افزار SPSS26 نیز استفاده شد. این نرم‌افزار واریانس کل پرسش‌نامه را محاسبه کرد و عدد ۰/۸۵۴ به دست آمد. این عدد برای پرسش‌نامه محقق‌ساخته عدد بسیار خوبی است. در راستای کفایت حجم نمونه مبتنی بر هر یک از مؤلفه‌ها از آزمون‌های کولموگروف و اسمینروف[1] (KMO) که مقدار آن برابر با ۰/۹۳۱ به دست آمده، داده‌های تحقیق قابل تقلیل به تعدادی از عامل‌های زیربنایی و بنیادی است. همچنین نتیجهٔ آزمون بارتلت[2] ۵۵۱/۲۷۷ به دست آمد که در سطح خطای کوچک‌تر از ۰/۰۱ معنی‌دار است؛ یعنی از یک طرف بین گویه‌های داخلی هر عامل همبستگی بالایی وجود دارد و از طرف دیگر بین گویه‌های یک عامل با گویه‌های عامل دیگری، هیچ‌گونه همبستگی مشاهده نمی‌شود.

یافته‌های تحقیق

برای تجزیه و تحلیل یافته‌ها در این پژوهش، از دو روش آمار توصیفی و استنباطی استفاده شده است.

الف. یافته‌های کیفی: بعد از انجام مصاحبه با ۱۴ نفر از افرادی که در حوزهٔ مدیریت فضای سایبر و پی‌جویی جرائم سایبری کشور فعالیت داشته و صاحب‌نظر بوده‌اند، نوبت به تجزیه و تحلیل داده‌ها رسید که این کدگذاری‌ها بر پایهٔ اهداف تحقیق و مدل‌های مورد بررسی شکل گرفت. به این ترتیب که ابتدا هر مصاحبه بازخوانی شد؛ سپس با توجه به اهداف، مصاحبه‌های تحقیق به‌صورت کدگذاری باز و محوری مستند به مدل‌های مورد بحث در ادبیات تحقیق انجام شد. البته سؤال‌ها و مقوله‌های محوری به شش دسته حوزه‌های ارتکاب جرائم سایبری، عناوین و مصادیق جرائم سایبری، پیشگیری از جرائم سایبری، مقابله با جرائم سایبری، مدیریت یکپارچه سازمان‌ها و نهادهای متولی حوزه پیشگیری و مقابله با جرائم سایبری تقسیم شد.

ب. یافته‌های کمی: بعد از اتمام کدگذاری محوری، مقوله‌های کیفی در پرسشنامهٔ توصیفی به‌صورت سؤال مطرح شد و به‌صورت شاخص‌های تبیین‌شده به‌همراه مشخصات زمینه‌ای پاسخ‌گویان در پرسشنامه طراحی شد.

1.Colmogrof and Sminrof tests
2.Bartlett's test

یافته‌های توصیفی (جمعیت‌شناختی پاسخ‌گویان): در این پژوهش توصیف داده‌ها مربوط به ویژگی‌های عمومی پاسخ‌دهندگان اعم از سن، سطح تحصیلات، میزان آشنایی با موضوع تحقیق، سابقهٔ کار در حوزهٔ فضای سایبری و ردهٔ شغلی است.

جمعیت شناختی (نمونه)	سن						سطح تحصیلات				رده (شغلی و مأموریتی)			
	۵۰سال به بالا	۴۵ تا ۵۰ سال	۴۰ تا ۴۵ سال	۳۵ تا ۴۰ سال	۳۰ تا ۳۵ سال	کمتر از ۳۰ سال	دکترا	دانشجوی دکترا	کارشناسی ارشد	کارشناسی	عملیاتی، اجرایی	پشتیبانی،عملیاتی	نظارتی و کنترلی	ستادی
فراوانی	۱۰	۲۰	۲۱	۶	۲	۲	۳۰	۲۰	۱۱	۰	۱۵	۶	۱۱	۲۹
درصد معتبر	۱۶,۴	۳۲,۸	۳۴,۴	۹,۸	۳,۳	۳,۳	۴۹,۲	۳۲,۸	۱۸	۰	۲۴,۷	۹,۸	۱۸	۴۷,۵

جمعیت‌شناختی (نمونه)	میزان آشنایی با موضوع تحقیق					سابقه کار در حوزه فضای سایبر					جایگاه مسئولیتی			
	خیلی زیاد	زیاد	متوسط	کم	خیلی کم	۲۱ سال به بالا	۱۶ تا ۲۰ سال	۱۱ تا ۱۵ سال	۶ تا ۱۰ سال	۱ تا ۵ سال	مدیر اجرایی	مدیر میانی	مدیر عالی	عضو هیئت‌علمی
فراوانی	۱۸	۲۳	۲۰	۰	۰	۸	۱۲	۱۷	۱۸	۶	۱۱	۱۶	۲۲	۱۲
درصد معتبر	۲۹,۵	۳۷,۷	۳۲,۸	۰	۰	۹,۸	۲۹,۵	۲۷,۹	۱۹,۷	۱۳,۱	۱۸		۳۶,۱	۱۹,۷

جدول ۴: جمعیت‌شناختی جامعه آماری

بر اساس یافته‌های تحقیق، از تعداد ۷۰ نفر جامعهٔ آماری، ۶۱ نفر به پرسش‌نامه و کل سؤال‌ها پاسخ داده‌اند. بیشترین پاسخ‌دهندگان بیشتر از ۴۰ سال سن دارند (۵۱ نفر؛ ۸۳,۶ درصد) و مدرک دکترا دارند یا دانشجوی دکترا بوده‌اند (۵۰ نفر؛ ۸۲ درصد). نزدیک به ۶۷/۲ درصد پاسخ‌گویان با موضوع تحقیق آشنایی زیاد و خیلی زیاد دارند و بیش از $\frac{3}{4}$ ۶۰/۷ درصد پاسخ‌گویان بیشتر از ۱۰ سال سابقهٔ کار سایبری دارند. در حدود ۴۷/۵ درصد نخبگان دارای مشاغل ستادی و راهبردی هستند و سایر پاسخ‌گویان در سطوح عملیاتی، نظارتی و پشتیبانی اطلاعاتی مشغول به خدمت هستند. بیشترین پاسخ‌گویان را مدیران عالی و راهبردی (۳۶,۱ درصد) تشکیل می‌دهند و بعد از آن مدیران میانی با ۲۶/۲ درصد و اعضای هیئت‌علمی با ۱۹/۷درصد در جایگاه بعدی قرار می‌گیرند.

یافته‌های استنباطی: در راستای معادلهٔ ساختاری متغیرهای مورد تحقیق با استفاده از نرم‌افزار Smart PLS به‌منظور تعیین روابط ساختاری و تحلیل مسیر ضرایب متغیرهای مطرح‌شده، در جدول ۵ و شکل به همراه توضیحات لازم استدلال آماری در سطور صفحه بعد تدوین شده است.

جدول ۵: معیارهای کیفیت و برازش مدل ساختاری و کلی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری؛ تحصیل محقق

متغیر/ابعاد/ مؤلفه	آلفای کرونباخ	پایایی ترکیبی	متوسط واریانس استخراج‌شده	ضرایب z	$Q^2(=1-SSE/SSO)$	ضریب تعیین (R۲)	متوسط مشترک (AVE-)
رصد و پایش	0.827	0.886	0.663	8.965	0.316	0.528	0.663
شناسایی	0.861	0.916	0.784	23.978	0.581	0.749	0.784
تشخیص جرائم سایبری	0.880	0.909	0.625	24.512	0.449	0.736	0.625
اشراف اطلاعاتی	0804	0.872	0.633	35.683	0.475	0.774	0.633
آگاهی‌رسانی	0.870	0.903	0.610	8.998	0.365	0.622	0.610
امدادرسانی و پشتیبانی	0.884	0.921	0.744	29.847	0.585	0.800	0.744
امن‌سازی	0.865	0.899	0.600	43.555	0.486	0.817	0.600
تربیت و آموزش	0.848	0.885	0.528	8.561	0.277	0.568	0.528
مصونیت سرمایه‌های سایبری	0.823	0.895	0.740	24.763	0.510	0.704	0.740
ارزیابی امنیتی	0.882	0.915	0.686	73.635	0.620	0.912	0.686
تجزیه و تحلیل جرائم	0.826	0.877	0.588	69.945	0.488	0.864	0.588
دفاع اولیه و پدافند سایبری	0.863	0.902	0.648	57.696	0.540	0.849	0.648
آمادگی عملیاتی	0.924	0.952	0.868	51.028	0.726	0.840	0.868
شناسایی و تعقیب مجرمان سایبری	0.860	0.899	0.641	16.680	0.373	0.613	0.641
رسیدگی به جرائم سایبری	0.866	0.903	0.651	38.231	0.535	0.833	0.651

متغیر/ابعاد/ مؤلفه	آلفای کرونباخ	پایایی ترکیبی	متوسط واریانس استخراج‌شده	ضرایب z	$Q^2(=1-SSE/SSO)$	ضریب تعیین (R۲)	متوسط مشترک (AVE-)
بررسی صحنهٔ جرم دیجیتال (فارنزیک)	0.877	0.915	0.730	44.416	0.591	0.824	0.730
جمع‌آوری ادلهٔ دیجیتال	0.938	0.955	0.843	22.427	0.576	0.691	0.843
تاب‌آوری و کشف جرائم سایبری	0.874	0.915	0.729	33.278	0.550	0.759	0.729
پیش‌بینی و برآورد عملیاتی	0.868	0.903.	0.613	48.111	0.502	0.839	0.613
انجام دفاع سایبری و اقدام مقابله‌ای	0.847	0.886	0.566	35.955	0.430	0.790	0.566
تبیین نظام جامع پیشگیری و مقابله	0.857	0.895	0.591	44.828	0.488	0.838	0.591
ایجاد سامانه‌های اطلاعاتی و ارتباطی	0.703	0.819	0.534	4.744	0.107	0.223	0.534
برتری عملیاتی	0.810	0.881	0.661	13.584	0.486	0.740	0.661
استانداردها	0.767	0.895	0.810	17.674	0.564	0.710	0.810
اسناد بالادستی و راهبردها	0.815	0.890	0.730	19.021	0.466	0.659	0.730
قوانین و مقررات	0.716	0.824	0.539	35.830	0.399	0.765	0.539
زیرساخت‌های اطلاعاتی و ارتباطی	0.853	0.911	0.773	16.457	0.415	0.558	0.773

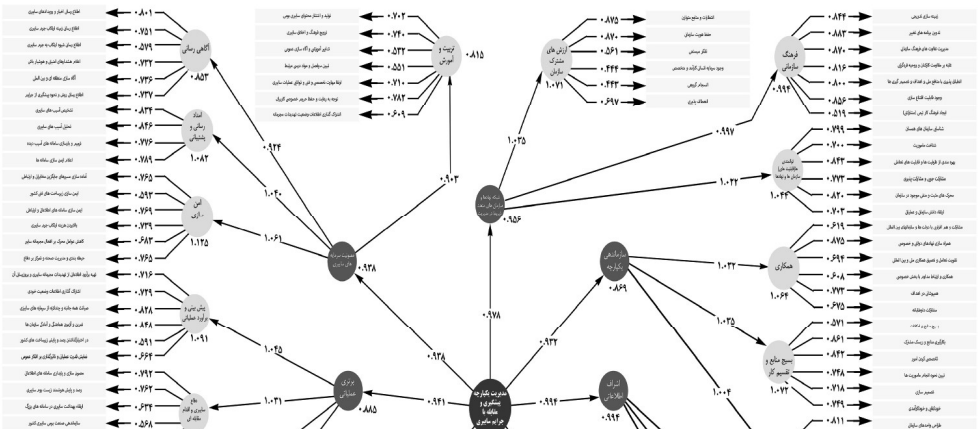
متغیر/ابعاد/ مؤلفه	آلفای کرونباخ	پایایی ترکیبی	متوسط واریانس استخراج‌شده	ضرایب z	Q^2(=1-SSE/SSO)	ضریب تعیین (R۲)	متوسط مشترک (AVE-)
تمرکز بر محیط (زیست‌بوم)	0.828	0.886	0.661	17.063	0.434	0.665	0.661
توانمندی‌های سازمان‌ها و نهادها	0.898	0.923	0.666	60.039	0.539	0.844	0.666
ارزش‌های مشترک سازمانی	0.826	0.870	0.533	45.491	0.405	0.830	0.533
فرهنگ سازمانی	0.923	0.940	0.695	34.780	0.569	0.833	0.695
شبکه نهادها و سازمان‌های متعدد	0.895	0.934	0.826	43.251	0.674	0.821	0.826
سازماندهی	0.877	0.908	0.623	28.041	0.479	0.792	0.623
برنامه‌ریزی و تقسیم کار (نگاشت نهادی)	0.899	0.923	0.668	43.619	0.555	0.756	0.668
همکاری	0.857	0.894	0.586	38.940	0.471	0.819	0.586
سازماندهی یکپارچه	0.882	0.927	0.810	24.160	0.592	0.738	0.810
هدایت و رهبری	0.824	0.876	0.586	71.388	0.476	0.851	0.586
هماهنگ‌سازی	0.875	0.910	0.673	90.916	0.598	0.916	0.673
نظارت و کنترل	0.896	0.924	0.709	64.870	0.609	0.866	0.709
وحدت فرماندهی	0.925	0.952	0.870	42.196	0.675	0.787	0.870
مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری	0.960	0.895	0.757	8.965	0.316	0.528	0.675

نتایج جدول قبل که بیانگر بارهای عاملی هر یک از ابعاد و مؤلفه‌های مدیریت یکپارچه است، به این اشاره می‌کند که تمام بارهای عاملی بیشتر از ۰/۴ بوده و برای برازش این مدل مناسب است. علاوه بر این نتایج، پایایی ترکیبی (مشترک) همهٔ عوامل بیشتر از ۰/۶ است که حکایت از پایایی مدل دارد. در همین راستا، میزان آلفای کرونباخ نتایج جدول فوق بیشتر از ۰/۷ بوده که حکایت از پایابودن مدل دارد. در ادامه نتایج روایی همگرایی حاصل از داده‌های جدول بالا (متوسط واریانس استخراج‌شده یا AVE) مقادیر ارزشی همهٔ عوامل بیشتر از ۰/۵ است و از آنجایی که مبنای مقادیر عوامل باید بالاتر از ۰/۴ باشد؛ بنابراین حکایت از روایی همگرای مناسب مدل دارد. بر اساس نتایج ضرایب معنادار Z (مقادیر t-values) جدول بالا، مقادیر مربوطه نشان‌دهندهٔ این است که تمام ضرایب بالاتر از مقدار معیار ۳,۲۷ بوده است و در سطح معناداری ۹۹,۹ است و در سطح معناداری بسیار خوبی قرار دارند. برابر با خروجی مقادیر Q2 سازه درون‌زای عملکرد الگوی راهبردی مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری از برازش قوی برخوردار است و نشان می‌دهد که قدرت پیش‌بینی قوی برای این سازه وجود دارد و برازش مناسب مدل ساختاری پژوهش را بار دیگر تأیید می‌کند. از منظر دیگر باید بیان کرد، بر اساس نتایج ضریب تعیین R2 در جدول بالا بیش از ۸۳ درصد ابعاد و مؤلفه‌های موضوع مورد پژوهش از برازش قوی در راستای انسجام سازه‌ای برخوردار هستند.

برای برازش مدل کلی پژوهش مد نظر که از دو بخش مدل اندازه‌گیری و ساختاری تشکیل شده است، تأیید برازش و بررسی برازش در یک مدل کلی بنام GOF استفاده می‌شود؛ به نحوی که برای این معیار عددی که به دست می‌آید بین صفر و یک است. سه مقدار به‌عنوان مقادیر ضعیف (۰,۰۱)، متوسط (۰,۲۵) و قوی (۰,۳۶) برای GOF ارائه شده است. این مقدار از جذر حاصل ضرب میانگین ستون «متوسط مشترک»[1] و میانگین «ضریب تعیین» حاصل می‌شود. با توجه به نتیجه نهایی جدول ، همان‌طور که مشاهده می‌شود مقدار برازش کلی الگوی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری معادل ۰,۵۰۸ به دست آمده و چون این مقدار از مقدار معیار ۰,۳۶ بیشتر است، می‌توان برازش مدل کلی را قوی ارزیابی کرد. لذا با تأکید بر نتایج به‌دست‌آمده از یافته‌های جداول، می‌شود ادعا کرد که امکان بررسی ارزیابی و تأیید مدل ترسیم‌شده در این پژوهش فراهم گردیده است.

---

۱. Communality: این عنوان به‌صورت مشخص در نسخه ۲ نرم‌افزار وجود دارد؛ ولی در نسخه ۳ نرم‌افزار از مقدار AVE استفاده می‌شود.



شکل۳ : مدل‌سازی معادلات ساختاری مفهومی پژوهش با بهره‌گیری از نرم‌افزار *Smart PLS*؛ تحصیل محقق

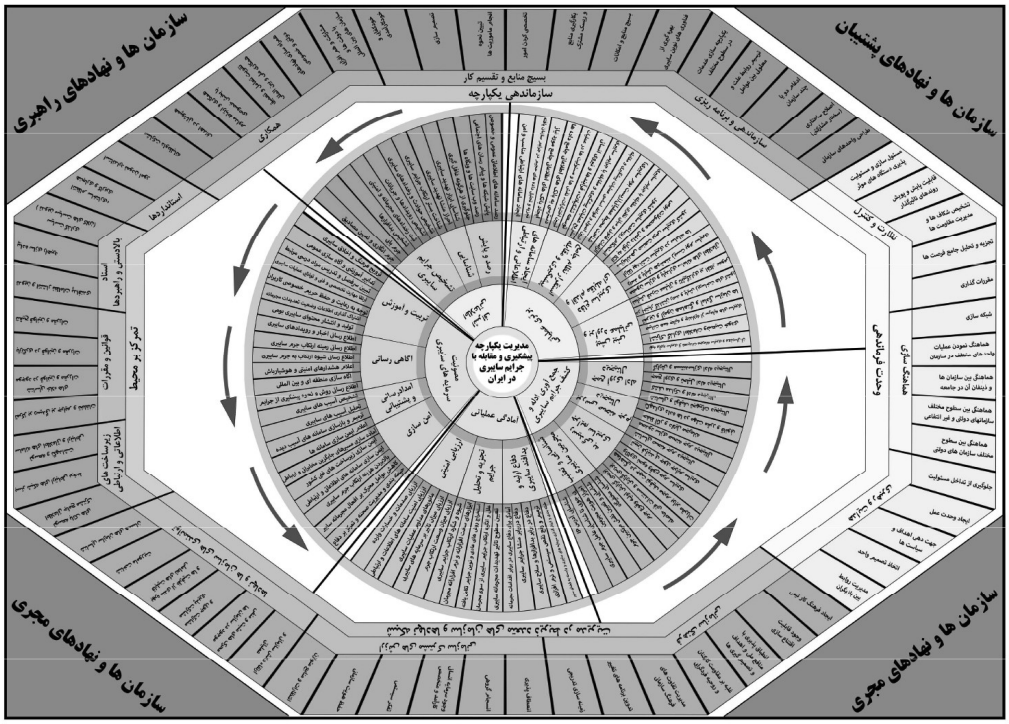
نتیجه‌گیری

پژوهش حاضر در پاسخ به سؤال اصلی تحقیق: «الگوی راهبردی مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران کدام است؟» انجام گرفته است. با گردآوری مبانی نظری و ادبیات تحقیق، تبیین مدل مفهومی بر اساس ادبیات موصوف، جمع‌بندی نتایج تجزیه و تحلیل مدل مفهومی بر اساس نظرسنجی جامعهٔ خبرگانی، جمع‌بندی و پاسخ به سؤال‌های فرعی، نه بُعد به همراه مؤلفه‌ها و شاخص‌های مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران برای طراحی الگوی شناسایی و احصا شده است که در جدول شاخص‌ها و مؤلفه‌های هر بُعد به تفکیک آورده شده است.

نظر به ترسیم مدل مفهومی پژوهش در نرم‌افزار Smart PLS (مدل‌سازی معادلات ساختاری)

و اضافه‌کردن داده‌های اخذشده از پرسشنامه‌ها، الگوریتم حداقل مربعات جزئی اجرا شد (شکل) و در ادامه، ضمن بررسی برازش اندازه‌گیری، برازش ساختاری و برازش کلی مدل، ابعاد حاصله در راستای سؤال‌های فرعی پژوهش ارزیابی شدند. حال بر مبنای ویژگی‌های فضای سایبر که متأثر از قابلیت‌های فناوری اطلاعات و ارتباطات است، تهدید و آسیب‌ها نیز روزبه‌روز پیچیده‌تر و امکان حوادث و رخداد یا جرائم سایبری نوین نیز مشهود است. لذا به‌منظور مدیریت یکپارچه، ضرورت دارد الگوی راهبردی ارائه شود که بر اساس یک چرخهٔ کاربردی طراحی شود که ضمن پویابودن، تمام ابعاد فنی و محتوایی و امنیتی را هم‌زمان در مراحل قبل و حین و بعد از وقوع جرائم سایبری پوشش دهد. در این راستا، از مدل «کیه‌زا» بهره‌گیری شده است که به‌خوبی ابعاد و فرایند راهبرد در محیط‌های پویا را بیان می‌کند. البته با توجه به ماهیت توسعه‌ای و گستردگی فضای سایبر، فراسازمانی و فرابخشی‌بودن آن و ضرورت ایجاد امنیت مستمر بر این فضا، فرایندی مناسب با مدیریت فضای سایبر لازم است. لذا مدل کاربری حلقه «اودا» و مدلی که وینسنت لندرز و همکارانش ارائه نموده‌اند، تداعی‌کنندهٔ فرماندهی و کنترل در فضای سایبر است و امکان تعمیمِ بخشی از آن به الگوی راهبردی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران (شکل ۳) وجود دارد.

الگوی نهایی از ترکیب نُه بعد در چهار فرایند تشکیل شده است. هر یک از فرایندها با توجه به سطحی که در آن قرار گرفته‌اند از طریق سازمان‌ها و نهادهای مشارکت‌کننده در فرایند، هدف مشخصی را دنبال می‌نمایند. در الگوی راهبردی یادشده، ارتباطات به دو دستهٔ کلی تقسیم می‌شوند. در این الگو دایره و هشت‌ضلعی اطراف را ابعاد و مؤلفه‌های مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری تشکیل می‌دهند که با خطوط به مرکز الگو متصل و هم‌زمان در جهت فلش‌ها در حرکت هستند که بیانگر فرایند پی‌جویی جرائم و اثرگذاری همهٔ ابعاد بر یکدیگر در ابعاد زمانی قبل و حین و بعد از وقوع جرائم سایبری است. در چهار زاویهٔ این الگو، سازمان‌ها و نهادهای کنشگر در مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران قرار دارند که در سطوح راهبری، مجری و پشتیبان ایفای نقش می‌کنند و دستگاه‌ها و سازمان‌های مختلفی را شامل می‌شوند که در سطح ملی با مدیریت تعاملی با یکدیگر همکاری نزدیک داشته و دارند.



شکل ۴: الگوی راهبردی مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در جمهوری اسلامی ایران؛ تحصیل محقق

پیشنهادها

با توجه به نتایج به‌دست‌آمده از بررسی پاسخ‌های ارائه‌شده از سوی خبرگان و جامعهٔ آماری و برخی موضوعات که محقق در طول تحقیق به آن‌ها رسیده است، پیشنهادهای زیر ارائه می‌شود.

– افزایش کیفیت و کمیت آموزش و تربیت نیروهای متخصص، متعهد، ماهر، حرفه‌ای و کارآمد در عرصهٔ پیشگیری و مقابله با جرائم سایبری.

– طراحی، اجرا و ایجاد مراکز رصد، پایش، تشخیص و هشدار دائمی رویدادها، جریان حوادث و جرائم سایبری کشور در همهٔ نهادها و سازمان‌ها بر مبنای نقش و وظایف.

– تجزیه و تحلیل و داده‌پردازی اطلاعات جمع‌آوری‌شده به‌منظور ارزیابی صدمات و خسارات، وسعت و میزان اثرگذاری جرائم بر سرمایه‌های سایبری و شناسایی جرائم سازمان‌یافته و سرمنشأ جرائم سایبری کشور و استخراج روش‌های عادی و نوین در ارتکاب جرائم تکامل‌یافته و محض سایبری.

– تدوین دستورالعمل‌های فنی و حقوقی جمع‌آوری ادلهٔ الکترونیکی و استانداردسازی و ایجاد

وحدت رویه فنی‌حقوقی درخصوص ادلهٔ الکترونیکی و ساماندهی آزمایشگاه‌های فارنزیک کشور به‌منظور هم‌پوشانی مناسب در زمان بروز جرائم، حوادث یا حملات سایبری.

– توسعهٔ فناوری‌های نوین در حوزهٔ پیشگیری و مقابله با جرائم سایبری و کاهش سطح اصطکاک بین کاربران و سازمان‌های نظارتی، امنیتی، اطلاعاتی و قضایی با به‌کارگیری تجهیزات مدرن رصد، پایش و شناسایی فنی و اطلاعاتی با استقرار یک نظام هوشمند و فناورانه بازدارنده.

– الزام و همراه‌سازی متولیان حقیقی و حقوقی و سازمان‌ها و نهادهای دولتی و خصوصیِ فعال در حوزهٔ زیرساخت‌ها و سامانه‌های اطلاعاتی مرتبط با سرمایه‌های سایبری خصوصی، عمومی و ملی کشور در استفاده از محصولات سایبری امن بومی.

– تدوین، تنقیح، بازنگری و انتشار قوانین و مقررات سایبری در فرایند پی‌جویی جرائم سایبری، اعم از پیشگیری و مقابلهٔ مؤثر قانونی و حقوقی جرائم و حوادث سایبری در کشور.

– تبیین حدود و ثغور قلمرو و نقشهٔ جامع پیشگیری و مقابله با جرائم سایبری در کشور، به‌منظور جلوگیری از تقابل و موازی‌کاری فعالیت سازمان‌ها و نهادهای دولتی و خصوصی با هدف ایجاد هم‌افزایی و هماهنگی‌های هدفمند در فضای سایبر.

– برنامه‌ریزی، سطح‌بندی، چابک‌سازی و تقسیم کار ملی بین نهادها و سازمان‌های متولی در حوزهٔ پیشگیری و مقابله با جرائم سایبری.

– معماری وظایف و نگاشت نهادی ساختارهای ملی در نظام مدیریت یکپارچهٔ پیشگیری و مقابله با جرائم سایبری در قبل و حین و بعد از وقوع جرم بر اساس سرمایهٔ ملی سایبری.

– تبیین الزامات حقوقی و قانونی اجرای نظام مدیریت یکپارچه پیشگیری و مقابله با جرائم سایبری در کشور.

– آینده‌پژوهی و پیش‌بینی جرائم نوظهور و پیش‌بینی و اقدام پیش‌دستانه در پیشگیری و مقابله با جرائم سایبری.

منابع و مآخذ

الف) منابع فارسی

۱. ایمانیان، زهرا و عباس منوریان، ۱۳۹۴، «***حکمرانی شبکه‌ای و بررسی موقعیت و چالش‌های آن در ایران***»، نخستین اجلاس ملی مدیریت دولتی ایران، تهران: دانشکده مدیریت دانشگاه تهران.

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

۳. ترکمان، مهرداد، ۱۳۹۱، ***نقش پلیس در پیشگیری از جرائم سایبری***، تهران: دانشگاه آزاد اسلامی، واحد علوم و تحقیقات مرکزی و دانشکده علوم انسانی، گروه حقوق.

۴. ثقفی، کامیار، ۱۳۹۳، «***مدیریت پیشرفته فضای سایبر***»، دورهٔ اول مدیریت راهبردی فضای سایبر، دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی: دانشکده امنیت ملی.

۵. جهانشیری، جواد و محمدرضا حسینی و احمد ابراهیمی، ۱۳۹۴، «***تبیین فرایند تحقیقات مقدماتی در جرائم سایبری***»، فصلنامه علمی‌پژوهشی پژوهش‌های اطلاعاتی و جنایی، دوره ۱۰، ش ۳۹، دانشکده علوم و فنون اطلاعات و آگاهی دانشگاه علوم انتظامی امین.

۶. حسینی، پرویز و حسین ظریف‌منش، ۱۳۹۲، «***مطالعه تطبیقی ساختار دفاع سایبری کشورها***»، فصلنامه پژوهش‌های حفاظتی‌امنیتی، دوره ۲، ش ۵، تهران: دانشگاه جامع امام حسین(ع).

۷. حسن‌بیگی، ابراهیم، ۱۳۹۰، «***مدیریت راهبردی***»، تهران: دانشگاه عالی دفاع ملی.

۸. حمیصی، مرتضی، ۱۳۹۱، «***الگوی راهبردی تأسیس و توسعه سازمان‌های مردم‌نهاد ایرانی با تأکید بر منافع امنیت ملی جمهوری اسلامی ایران***»، با راهنمایی دکتر محمدرحیم عیوضی و مشاوره دکتر غلامرضا خواجه سروری و دکتر یوسف ترابی، تهران: دانشگاه عالی دفاع ملی، دانشکده مدیریت راهبردی.

۹. گروه مولفین؛ گرایش امنیت سایبر در قالب گروه مطالعاتی، ۱۳۹۷، «***طراحی نظام دفاع سایبری کشور و تدوین راهبردهای آن***»، با محوریت دکتر مهرداد کارگری و راهنمایی دکتر میثم لطیفی و مهندس محمدرضا فرجی‌پور و مهندس علی محمدی، تهران: دانشکده امنیت ملی داعا.

۱۰. گروه مولفین؛ گرایش مدیریت راهبردی فضای سایبر در قالب گروه مطالعاتی، ۱۳۹۶، «***ارائه راهبردهای علمی و فناوری تحکیم و ساخت درونی قدرت ملی نظام جمهوری اسلامی ایران***»، با محوریت دکتر حسین ساری و راهنمایی دکتر محمد مهدی‌نژاد نوری، دکتر محسن مرادیان و امیر

سرتیپ دوم ستاد دکتر محمدحسین صنیعی، تهران: دانشگاه عالی دفاع ملی، دانشکده امنیت ملی.

۱۱.رجبی‌پور، محمود، ۱۳۸۲، ***«راهبرد پیشگیری اجتماعی از جرم؛ تعامل پلیس و دانش‌آموزان»***، فصلنامه پژوهش‌های دانش انتظامی، سال ۵، ش ۳، پیاپی ۱۹، دانشگاه علوم انتظامی امین، معاونت پژوهش.

۱۲. روضه‌ای، منصور و جعفر توانبخش و حمید حسن‌زاده و احمد کرد، ۱۳۹۶، ***ابزارهای پیشگیری از جرائم نوظهور در فضای مجازی***، تهران: معاونت اجتماعی ناجا.

۱۳. سند امنیت فضای تولید و تبادل اطلاعات ***«افتا»***، مصوب ۱۲ مهر ۱۳۸۷.

۱۴. سند چشم‌انداز ۲۰ساله (۱۴۰۴) جمهوری اسلامی ایران، ۱۳ آبان ۱۳۸۲.

۱۵. سند راهبردی پلیس فضای تولید و تبادل اطلاعات (فتا) نیروی انتظامی ج.ا.ا، مصوب خرداد ۱۳۸۹.

۱۶. کمیته راهبردی پدافند غیر عامل کشور، سند راهبردی پدافند سایبری کشور، مصوب ۲۹ اردیبهشت ۱۳۹۴.

۱۷. شورای عالی فضای مجازی، سند نظام ملی پیشگیری و مقابله با حوادث در فضای مجازی، ۱۵ آبان ۱۳۹۶.

۱۸.سیاست‌های کلی امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا)، ۲۹ بهمن ۱۳۸۹.

۱۹. شاه‌محمدی، غلامرضا و منصور تاهو، ۱۳۹۳، ***«بررسی شیوه‌های پیشگیری از جرائم سایبری؛ مبتنی بر فناوری اطلاعات»***، فصلنامه علمی‌پژوهشی پژوهش‌های اطلاعاتی و جنایی، دوره ۹، ش ۳۵، دانشکده علوم و فنون اطلاعات و آگاهی دانشگاه علوم انتظامی امین.

۲۰. شهیر، احسان، ۱۳۹۶، ***«طراحی الگوی راهبردی بومی امنیت فضای سایبر کشور»***، با راهنمایی دکتر ابراهیم حسن‌بیگی و مشاوره دکتر رضا تقی‌پور، دکتر خراشادی‌زاده و مهندس عبدالمجید ریاضی، تهران: دانشگاه عالی دفاع ملی، دانشکده امنیت ملی.

۲۱. صیدی، فاطمه، ۱۳۹۵، ***«ارائه الگوی مدیریت یکپارچه خدمات اجتماعی در حوزه آسیب‌های اجتماعی؛ نمونه موردی شهر تهران»***، با راهنمایی دکتر محمد زاهدی اصل و مشاوره دکتر علی‌اکبر تاج مزینانی، تهران: دانشگاه علامه طباطبائی، دانشکده علوم‌اجتماعی.

۲۲. قانون مجازات اسلامی، مصوب ۱ اردیبهشت ۱۳۹۲مجلس شورای اسلامی و تأیید ۱۱ اردیبهشت ۱۳۹۲ شورای نگهبان.

۲۳. قانون مبارزه با جرائم رایانه‌ای جمهوری اسلامی ایران، مصوب ۵ خرداد ۱۳۸۸مجلس شورای اسلامی.

۲۴. قوچانی خراسانی، محمدمهدی و داوود حسین‌پور و ابراهیم محمودزاده و سید مهدی الوانی و سید ابوالحسن فیروزآبادی، ۱۳۹۶، «***الگوی حکمرانی شبکه‌ای با تأکید بر توسعه فرایندهای نوآوری باز در نهادهای تحقیقاتی امنیت سایبری***»، نشریه علمی‌پژوهشی بهبود مدیریت، سال ۱۱، ش ۴، پیاپی ۳۸، تهران: مؤسسه آموزشی و تحقیقاتی صنایع دفاعی.

ب)منابع لاتین

1.ECONOMIC AND SOCIAL COMMISSION FOR WESTERN ASIA (ESCWA) (2011) , Key Factors in Establishing Single Window. Printed at ESCWA, Beirut E/ ESCWA/EDGD/United Nations Publication 11-0286 – December 2011 - 472.

2. EUROPEAN COMMISSION (2015), Literature review and identification of best practices on integrated social service delivery.

3. K. Jayeshankar, Ph.D., (June and July 2010), Cybercrime, Challenges and Opportunities, International Journal of Criminology, Criminal Justice and Criminal Justice Association of the University of India, Subscriber Number 1 & 2 Vol. 4.

4. 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.

5. Vitola Alise, Senfelde Maija (2015), An Evaluation of the Cross-Sectoral Policy Coordination in Latvia, VIEŠOJI POLITIKA IR ADMINISTRAVIMAS - PUBLIC POLICY AND ADMINISTRATION, Vol. 14, No 2, p.p 236–249.

6. Skaug Lene (2014), Five Theories in Social Work, Sydney, Australia, Universite tsforlaget.

ج)تارنما

۱. ابروش، رضا، ۱۳۹۶، «***مفهوم‌شناسی سینرژی یا هم‌افزایی و نتایج آن***»، بارگذاری‌شده در ۲۷ مهر ۱۳۹۶، بازدید در ۲۸ مهر ۱۳۹۷، قابل دسترس در:
http://www.modiryar.com/index-management/government/system/6419

۲. وب‌سایت دفتر مقام معظم رهبری حضرت آیت‌الله‌العظمی امام خامنه‌ایK، قابل دسترس در:
http://www.leader.ir/fa/content . http://www. khamenei.ir/fa/content

۳. وب‌سایت شورای عالی فضای مجازی، مرکز ملی فضای مجازی، قابل دسترس در:
http://majazi.ir/general_content/76436

۴. وب‌سایت پلیس فضای تولید و تبادل اطلاعات (فتا)، قابل دسترس در:
http:// www.cyberpolice.ir

۵. هادیان‌فر، سید کمال، ۱۳۹۴، اجلاس بین‌المللی جرائم سایبری در دنیای به‌هم‌پیوسته، پلیس فتا، بارگذاری‌شده در ۵ خرداد ۱۳۹۴، بازدید در ۱۱ مرداد ۱۳۹۶، قابل دسترس در:
http:// www.cyberpolice.ir