مقاله پژوهشی:
ارائه مدل مدیریت راهبردی امنیت فضای سایبر بر اساس کلان‌داده‌های فضای سایبر

مجید حقی[1]

تاریخ دریافت: ۱۳۹۷/۱۰/۱۸ تاریخ پذیرش: ۱۳۹۷/۱۲/۰۹

چکیده

شدت تغییرات در فضای سایبر و متناظر آن تنوع گونه‌های ناامنی و ضرورت پاسخگویی به تهدیدات روزآمد این فضا، به‌ویژه جایگاه راهبردی خدمات و اطلاعات موجود در این فضا، ضرورت داشتن مدلی برای مدیریت راهبردی امنیت این فضا را لاجرم ساخته است. از سوی دیگر داشتن اطلاعات محیطی اعم از محیط داخلی و خارجی به‌خصوص با توجه به سرعت تغییرات آن‌ها و لزوم داشتن اطلاعات دقیق، ما را برای مدیریت امنیت به‌سوی کلان‌داده‌های این فضا رهنمون می‌سازد. شناخت محیطی برای انتخاب راهبردی‌های مناسب در کلیه مدل‌های مدیریت راهبردی جزئی از ارکان مدل‌ها می‌باشد. کلان‌داده‌های فضای سایبر علاوه بر آنکه حاوی اطلاعات بلادرنگ فضای سایبر می‌باشند، امکان ارزیابی و شناسایی کاملی از محیط را فراهم می‌سازند. همچنین در این پژوهش با استفاده از چارچوب استاندارد ایزو ۳۱۰۰۰ مدل نهایی پیاده‌سازی گردیده است. در این استاندارد بخش ارزیابی مخاطره با توجه ظرفیت‌های کلان‌داده‌های موجود در فضای سایبر، توابع چگالی احتمال تهدیدات، به روش‌های مختلف داده‌کاوی استخراج گردید. مقدار مخاطرات در هر یک از مؤلفه‌های استخراج‌شده، امنیت فضای سایبر با بهره‌گیری از توابع احتمالات شرطی شبکه بیز، محاسبه و با استفاده از مدل مارکف مدوله‌شده با توزیع پواسن و از ترکیب چرخه مارکف با تابع چگالی احتمال پواسن و توابع شرطی آن در شبکه بیز، استخراج‌شده از کلان داده‌های فضای سایبر، ارزیابی مخاطرات انجام شد. در بخش تدوین راهکارهای مقابله با مخاطرات نیز با به‌کارگیری المان‌های استخراج‌شده از مطالعات انجام‌شده بر مدل‌های مدیریت راهبردی و مدیریت مخاطرات، پیاده‌سازی استاندارد ایزو ۳۱۰۰۰ کامل گردید. در نهایت مدل به‌دست‌آمده با نمونه‌ای از سناریوی تهدیدات سایبر در خصوص شبکه‌های اجتماعی شبیه‌سازی شده است.

کلیدواژه‌ها: مدیریت راهبردی، امنیت سایبر، مدیریت امنیت، کلان‌داده‌های فضای سایبر

۱. دانشجوی دکتری دوره اول امنیت سایبر دانشگاه عالی دفاع ملی. mhaghi@chmail.ir

مقدمه

در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات، از طریق سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد. این فضا که از آن با نام «فضای تولید و تبادل اطلاعات» یاد می‌شود، در معرض چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی؛ نظیر ارتکاب جرائم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حملات مختل‌کننده خدمات، جاسوسی، خرابکاری، نقض حریم خصوصی و نقض حقوق مالکیت معنوی قرار دارد؛ به‌طوری که نپرداختن یا رویکرد نادرست به امنیت این فضا، مانعی بزرگ پیش روی گسترش کاربرد فناوری ارتباطات و اطلاعات و ورود به جامعه اطلاعاتی خواهد بود (سند راهبردی امنیت فضای تولید و تبادل اطلاعات کشور، ۱۳۸۷).

فناوری اطلاعات و ارتباطات در دنیای کنونی نه صرفاً به‌عنوان پیشرانی فناورانه بلکه یک منبع قدرت تمام‌عیار محسوب می‌شود. اطلاعات و ارتباطات منابع و فرآیندهای تولید، تغییر و جریان قدرت را متحول نموده‌اند. به نحوی که توان و شایستگی در اطلاعات به‌عنوان یکی از عناصر قدرت ملی، سایر عناصر قدرت ملی را تحت تأثیر قرار داده است. فناوری اطلاعات ابزار اداره و تسخیر دنیا، جایگزین قدرت هسته‌ای و بستر جهانی‌سازی شده است (دیوسالار، ۱۳۹۱: ۲۳).

در علوم سیاسی، قدرت و امنیت دو مفهوم کاملاً وابسته به هم می‌باشد و به جرأت می‌توان گفت شاید نتوان اندیشمندی را در این حوزه یافت که وابستگی این دو مفهوم را به یکدیگر رد کند (خلیل‌پور رکن‌آبادی و دیگران، ۱۳۹۱: ۱۸۰)؛ بنابراین پرواضح است که دامنه تأثیرگذاری امنیت فضای سایبر دربرگیرنده مفهوم امنیت در حوزه‌هایی است که فضای سایبر در دنیای کنونی نقش تعیین‌کننده‌ای در آن‌ها ایفا کرده و هم‌زمان تولید قدرت می‌نماید. به همین دلیل است که در ارزیابی از تهدیدات امنیت ملی و بین‌المللی، مفهوم امنیتی فضای سایبری، وارد اسناد پایه‌ای امنیتی شده است؛ بنابراین، امنیت فضای سایبری با توجه به اتکای روزافزون عمده بازیگران جوامع امروزی به آن، بی‌تردید مقوله‌ای راهبردی و نیازمند مدیریتی در این سطح بر زوایا و ابعاد مرتبط می‌باشد.

بیان مسئله

وضعیت و امنیت فضای سایبر، حاصل انواع تعاملات فی‌مابین کاربران، جمعیت‌ها، سازمان‌ها و دولت‌ها و ... از طریق ماشین‌های متصل به یکدیگر در فضای سایبر است. از این رو شاهد تولید حجم انبوهی از اطلاعات و داده‌ها در اندازه، قالب و سرعت‌هایی متفاوت خواهیم بود؛ به‌ویژه با ظهور مفهومی به نام اینترنت اشیا در آینده‌ای نه‌چندان دور حجم این اطلاعات به‌شدت افزایش خواهد یافت. بر اساس گزارش‌های بین‌المللی حجم کلی کلان‌داده تولیدشده و کپی‌شده در دنیا از حدود ۱/۸ زتا بایت در سال ۲۰۱۱ میلادی به ۱۵ زتا بایت در سال ۲۰۱۷ میلادی رسیده و بر اساس پیش‌بینی‌ها به ٤٥ زتا بایت در سال ۲۰۲۰ میلادی خواهد رسید (گزارش نخستین پیمایش کلان داده‌ها، ۱۳۹٦).

از این رو یکی از مباحث مطروحه، پتانسیل روش‌ها و فناوری‌های مربوط به تجزیه‌وتحلیل و مدیریت کلان‌داده‌ها به‌منظور رصد و شناخت محیطی فضا و امنیت فضای سایبر می‌باشد. پرواضح است حجم عظیم کلان‌داده‌ها که مستمراً در تعاملات انسان- انسان، انسان- ماشین و ماشین-ماشین در فضای سایبر تولید می‌شود، به‌ویژه آنکه با آمیختگی عمده عملیات و مأموریت‌های دولت‌ها و ملت‌ها در بخش‌های مختلف اقتصادی، اجتماعی، فرهنگی و ... با فضای سایبر می‌توان با تجزیه‌وتحلیل این داده‌ها اطلاعات کامل و به‌هنگامی از تغییرات فضای سایبر در این حوزه‌ها به دست آورد.

از سوی دیگر یکی از مهم‌ترین و کلیدی‌ترین نیازمندی‌ها در طراحی راهبردهای مدیریت و مقابله با مخاطرات داشتن اطلاعات دقیق و به‌هنگام محیطی است. خصوصاً در مدیریت مخاطرات فضای سایبر که سرعت تغییرات در آن بسیار بالا می‌باشد. از این رو بهره‌برداری از ظرفیت‌های اطلاعاتی کلان‌داده‌ها در شناسایی محیط، رصد تغییرات و سرعت این تغییرات، امکان مدیریت مؤثری بر مخاطرات فضای سایبر را فراهم خواهد ساخت. ژبنابراین مسئله اصلی در این پژوهش چیستی ابعاد، مؤلفه‌ها و روابط مدلی است که می‌توان بدان‌وسیله و با بهره‌گیری از ظرفیت‌های کلان‌داده‌های فضای سایبر و در یک سطح راهبردی، امنیت در فضای سایبر را مدیریت نمود.

اهمیت و ضرورت پژوهش

در باب اهمیت پژوهش لازم به ذکر است که امنیت ملی امروزه با تهدیدات بی‌شماری مواجه است، اما در این میان، تهدیدهای سایبری پدیده جدیدی است که همراه با گسترش ارتباطات گریبان‌گیر دولت‌ها شده است. از این رو اهمیت تحقیق را می‌توان در سه بخش مطرح نمود:

۱. مدل مدیریت راهبردی امنیت فضای سایبر چارچوبی است که باعث شکل‌گیری تصویری مشترک و همگرایی بین بازیگران و ذینفعان این حوزه و در نهایت ارتقای سطح امنیت سایبری کشور خواهد گردید.
۲. بهره‌برداری از کلان‌داده‌های فضای سایبر به‌عنوان دقیق‌ترین و به‌هنگام‌ترین اطلاعات مورد نیاز در فرآیند مدیریت راهبردی امنیت فضای سایبر باعث کارآمدی در فرآیند تصمیم‌گیری‌های راهبردی می‌شود.
۳. پرداختن به مدیریت امنیت فضای سایبر در یک سطح راهبردی و در قالب این فعالیت علمی و پژوهشی به‌ویژه با توجه به ترسیم جایگاه و نقش کلان‌داده‌ها، باعث بسط و توسعه ادبیات و گفتمان در این زمینه خواهد شد.

انجام این تحقیق با توجه به موارد زیر ضرورت دارد:

۱. عدم وجود چارچوبی برای مدیریت امنیت در فضای سایبر که امکان مقابله و مدیریت بهنگام و مؤثر و متمرکز بر مخاطرات و تهدیدات سایبری را فراهم سازد.
۲. با توجه به رویکرد جدید دشمنان در جایگزینی تهدیدات سایبری به‌جای تهدیدات کلاسیک و نظامی، فقدان یک نگاه راهبردی در حوزه مدیریت امنیت فضای سایبر به‌ویژه با توجه به ظرفیت عظیم کلان‌داده‌ها در افزایش سرعت و دقت در مدیریت امنیت این فضا، زمینه بروز آسیب‌های جدی در این حوزه را فراهم خواهد نمود.
۳. فضای سایبر به‌عنوان یک منبع عظیم داده (کلان‌داده‌ها) از ظرفیت‌های قدرت تمام‌عیاری در بستر جهانی برخوردار شده است. بی‌توجهی راهبردی در امنیت این فضا باعث کاهش ابتکار عمل و اقتدار کشور خواهد شد.

٤. کلان‌داده‌های فضای سایبر منبعی ذی‌قیمت و روزآمد برای رصد تهدیدات و مخاطرات فضای سایبر هستند. عدم استفاده از این منبع، توان تصمیم‌گیری‌های راهبردی و به‌هنگام از مدیریت کشور را سلب می‌کند.

سؤالات پژوهش

سؤالات این پژوهش که ما در پی یافتن آن‌ها هستیم عبارت است از:

- کلان‌داده‌های حوزه فضای سایبر جمهوری اسلامی ایران کدامند؟
- ابعاد و مؤلفه‌های امنیت فضای سایبر کدامند و روابط بین آن‌ها کدامند؟
- مدل مدیریت راهبردی امنیت فضای سایبر بر اساس کلان‌داده‌های فضای سایبر جمهوری اسلامی کدام است؟

مبانی نظری

فضای سایبر

در سند راهبردی امنیت فضای تبادل اطلاعات (افتا)[1]، به فضای سایبری، فضای تبادل اطلاعات (به اختصار فتا) گفته‌شده و به‌صورت زیر تعریف می‌شود:

«در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی از قبیل اطلاع‌رسانی، داده‌ورزی، ارائه خدمات، مدیریت و کنترل و ارتباطات، از طریق سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد. از این فضا با نام فضای تبادل اطلاعات (فتا) یاد می‌شود».

تعریف مشترک روسیه و آمریکا برای فضای سایبری (Rauscher and V. Yaschenko,2011) مناسب‌ترین تعریف به نظر می‌رسد که در ادامه ارائه می‌شود: «یک رسانه الکترونیکی که از طریق آن اطلاعات تولیدشده، منتقل‌شده، دریافت‌شده، ذخیره‌شده، پردازش‌شده یا حذف می‌شوند».

[1]. شورای عالی امنیت فضای تبادل اطلاعات کشور، مجموعه مستندات سند راهبردی امنیت فضای تبادل اطلاعات کشور، ۱۳۸٤.

بنابراین تعریف فضای سایبر در این تحقیق به شرح ذیل در نظر گرفته می‌شود که: «فضای سایبر رسانه الکترونیکی است که با استفاده از سازوکارهای الکترونیکی اقدامات گوناگون مثل داده‌ورزی، تولید و تبادل اطلاعات و همچنین ذخیره و پردازش آن‌ها انجام می‌شود».

امنیت سایبری

امنیت سایبری وابسته است به سیاست دولت‌ها. این اصطلاح عموماً توسط مؤسسات دولتی و سیاست‌گذاران ملی در اسناد، قوانین و پروژه‌های تحقیقاتی استفاده می‌شود و کمابیش مترادف با «امنیت اینترنت» است. تفاوت این دو اصطلاح چندان زیاد نیست؛ بلکه امنیت رایانه‌ها، شبکه‌ها و داده‌ها تا حد زیادی با مفاهیم روزمره امنیت در فضای سایبر به هم گره خورده‌اند (سادوسکای و دیگران،۱۳۸٤: ١٦).

بنابراین امنیت سایبری به این ترتیب در نظر گرفته می‌شود که «امنیت سایبر عبارت است از رفع یا محدودسازی تهدیدات سایبری به‌منظور کاهش مخاطرات اثرگذار بر امنیت ملی از طریق فضای سایبر».

ابعاد و مؤلفه‌های امنیت فضای سایبر

مجموعه سه‌گانه اهداف امنیتی[1] در فضای سایبر عبارت است از محرمانگی، دسترس‌پذیری و یکپارچگی[2](National Institute of Standards and Technology, 2011) . با توجه به اهمیت مالکیت معنوی خدمات و محتوا در یک‌سو و انتشار و بهره‌برداری از خدمات و محتوا در سوی دیگر و آثار امنیتی این موضوع از مدل چهارگانه ابعاد و مؤلفه‌های امنیت فضای سایبر که در جدول (۱) ارائه شده است در این پژوهش بهره‌برداری گردید.

1. Cuber Security Objectives
2. National Institute of Standards and Technology, (2011)

به عبارتی تهدیدات سایبری از طریق نقض چهار بعد (محرمانگی، دسترس‌پذیری، یکپارچگی و کاربرد) می‌توانند تولید ناامنی نمایند. از سوی دیگر هر یک از این ابعاد خود نیز می‌توانند در صورت نقض، روی شش مؤلفه (سیاسی، اجتماعی، اقتصادی، فرهنگی، نظامی و زیست‌محیطی) تأثیرگذار باشند (حقی و دیگران، ۱۳۹۸).

جدول (۱): ابعاد و مؤلفه‌های امنیت فضای سایبر (همان)

مولفه های امنیت ملی متاثر از فضای سایبر	ابعاد امنیت سایبر
اقتصادی	یکپارچگی
اجتماعی	محرمانگی
فرهنگی	دسترس پذیری
نظامی	کاربرد
سیاسی	
زیست محیطی	

کلان‌داده

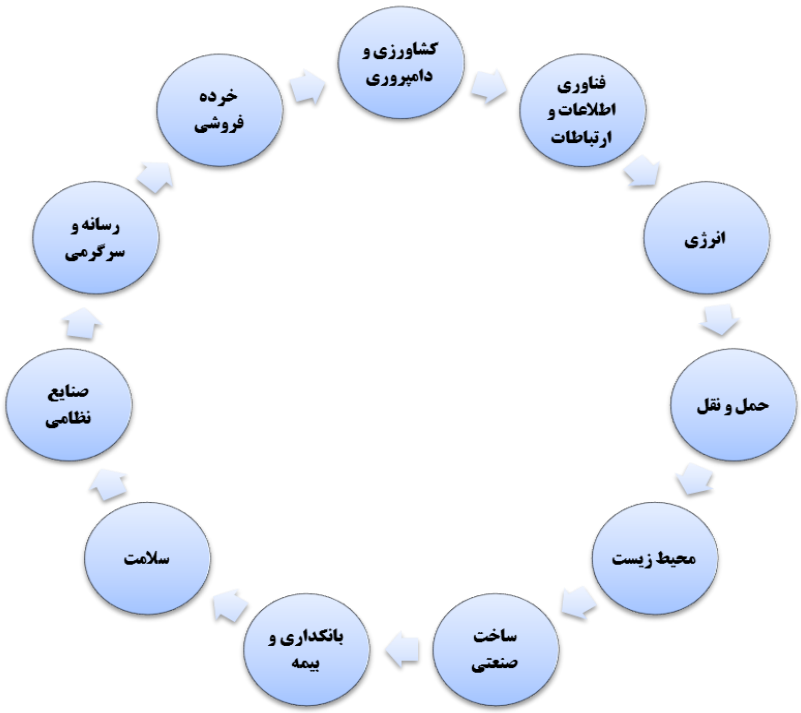
کلان‌داده[1] واژه‌ای است وسیع برای مجموعه داده‌های بسیار بزرگ یا پیچیده که برای پردازش این داده‌ها روش‌های سنتی مناسب نمی‌باشد.

کلان‌داده را می‌توان بر اساس ابعادی همچون حجم، تنوع، سرعت، متغیر، صحت، واقعی بودن و ارزش تعریف کرد (C.EVANS JR.,2016).

کلان‌داده‌ها در ایران

کلان‌داده‌های فضای سایبر جمهوری اسلامی ایران متشکل از یازده حوزه می‌باشد که در شکل (۱) نشان داده شده است.

1. Big Data



شکل (۱): حوزه‌های مرتبط با کلان داده‌های ایران بر اساس نخستین پیمایش انجام شده توسط پژوهشگاه فناوری اطلاعات و ارتباطات

زیست‌بوم کلان‌داده‌ها در ایران[۱]

در ادبیات نظری و استانداردهای مختلف دارای نقش‌ها و بازیگران مختلفی است. به‌منظور شناسایی ذینفعان زیست‌بوم کلان‌داده، به‌طور مستقیم و غیر مستقیم از مدل‌های مختلفی همچون مدل ارائه‌شده توسط گروه‌های استانداردسازی ITU[۲]، NIST[۳] و ISO[٤] در ادبیات نظری استفاده شده است که بسیار به یکدیگر نزدیک و شبیه می‌باشند. شکل(۲) ارائه‌کننده زیست‌بوم کلان داده‌های کشور می‌باشد.

۱. گزارش نخستین پیمایش کلان‌داده‌ها در ایران، پژوهشگاه فناوری اطلاعات و ارتباطات، (۱۳۹٦ ه.ش)

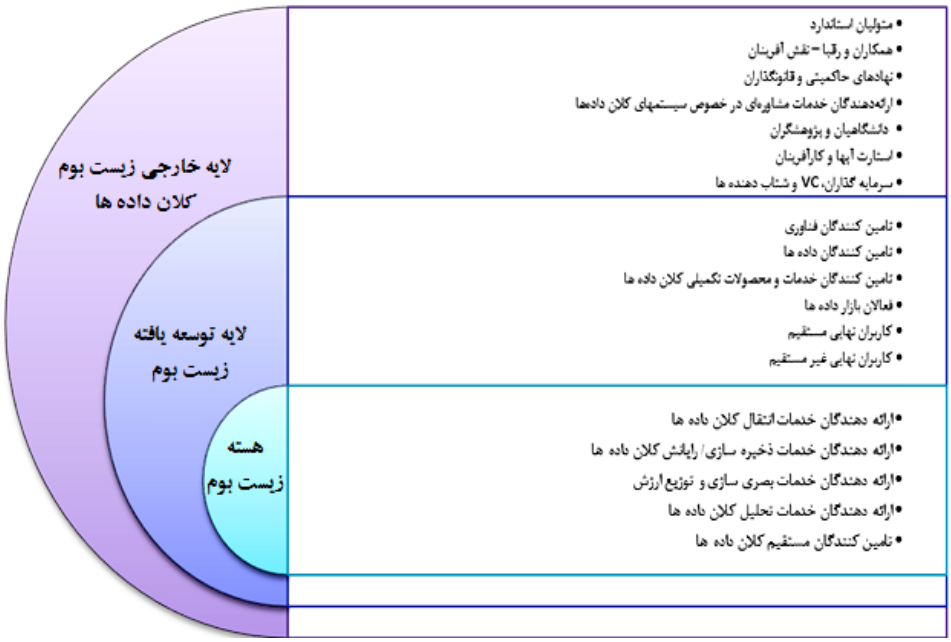
2. International Telecommunication Union
3. National Institute of Standards and Technology
4. International Organization for Standardization

این زیست‌بوم دارای سه بخش کلی بوده که عبارت هستند از:

هسته زیست‌بوم: مشتمل بر ذی‌نفعانی که در زنجیره ارزش کلان‌داده‌ها قرار می‌گیرند.

لایه توسعه‌یافته: بازیگرانی که به‌طور مستقیم با ذی‌نفعان هسته زیست‌بوم در ارتباط هستند ولی نسبت به ذی‌نفعان لایه هسته تأثیرگذاری کمتری بر کسب‌وکار کلان‌داده‌ها دارند.

لایه خارجی: بازیگران که به‌طور غیر مستقیم با کسب‌وکار کلان‌داده‌ها در تعامل هستند.



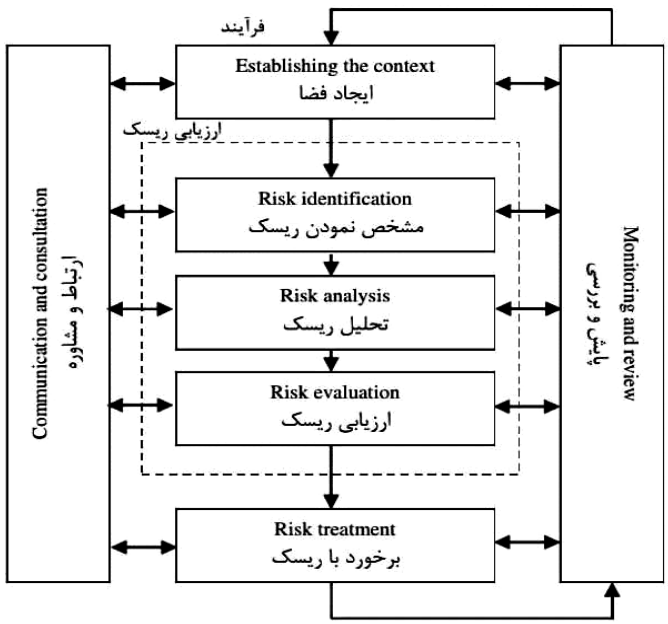
شکل (۲): زیست بوم کلان داده‌ها در ایران

مدل‌های مدیریت راهبردی، مدیریت مخاطرات و مدیریت رخدادهای پیچیده

به‌منظور دستیابی به توافق اولیه در خصوص شکل و نحوه اجرای فرآیند مدیریت راهبردی نیاز به شناخت توالی اقدام‌های رایج در مدل‌های مختلف مدیریت راهبردی داریم. تاکنون مدل‌های مفهومی متعددی برای انجام مدیریت راهبردی توسعه یافته‌اند که برخی از آن‌ها جهت بهره‌برداری در تدوین مدل نهایی مورد بررسی قرار گرفتند. این مدل‌ها عبارت هستند از (جعفری، ۱۳۸۵):

- الگوی مدیریت راهبردی (هانگر[1])؛
- الگوی برنامه‌ریزی راهبردی (بیت من و اسنل)؛
- فرآیند طراحی راهبردی[2] (دانشگاه ایالتی کالیفرنیا)؛
- الگوی مدیریت راهبردی (پیرس و رابینسون)؛
- الگوی جامع برنامه‌ریزی راهبردی[3] (فرد دیوید)؛
- الگوی تدوین راهبرد (طارق خلیل)؛
- مدل پالایش راهبرد بین‌المللی RAND؛
- فرآیند برنامه‌ریزی راهبردی (جان برایسون)[4].

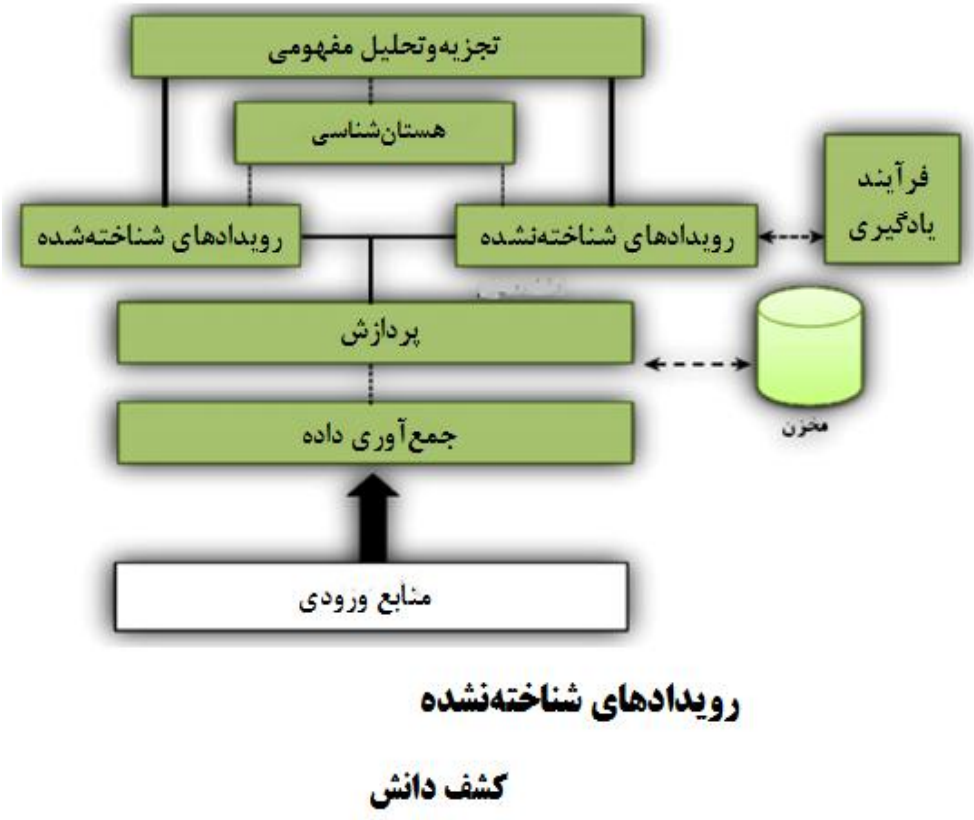
همچنین با توجه به استانداردهای اختصاصی بخش مدیریت مخـاطرات، اسـتاندارد ISO31000 نیز در تدوین مدل نهایی مدیریت راهبردی امنیت مورد بهره‌برداری قرار گرفت، شکل (۳).



1. Hunger
2. Strategic Planning Process
3. Strategic Planning Comprehensive Model

شکل (۳): فرآیند استاندارد ۳۱۰۰۰

در ادامه و با توجه به ویژگی‌های فضای سایبر و ضرورت سرعت پاسخگویی به رخدادهای پیچیده این فضا، مدل پردازش رویدادهای پیچیده مورد بررسی قرار گرفت، شکل (٤)، این فرآیند با یک سیستم یادگیری یکپارچه شده است که وقایع ناشناخته را آنالیز نموده و هم‌زمان مورد تجزیه‌وتحلیل قرار می‌دهد (kotevska&others,2016).

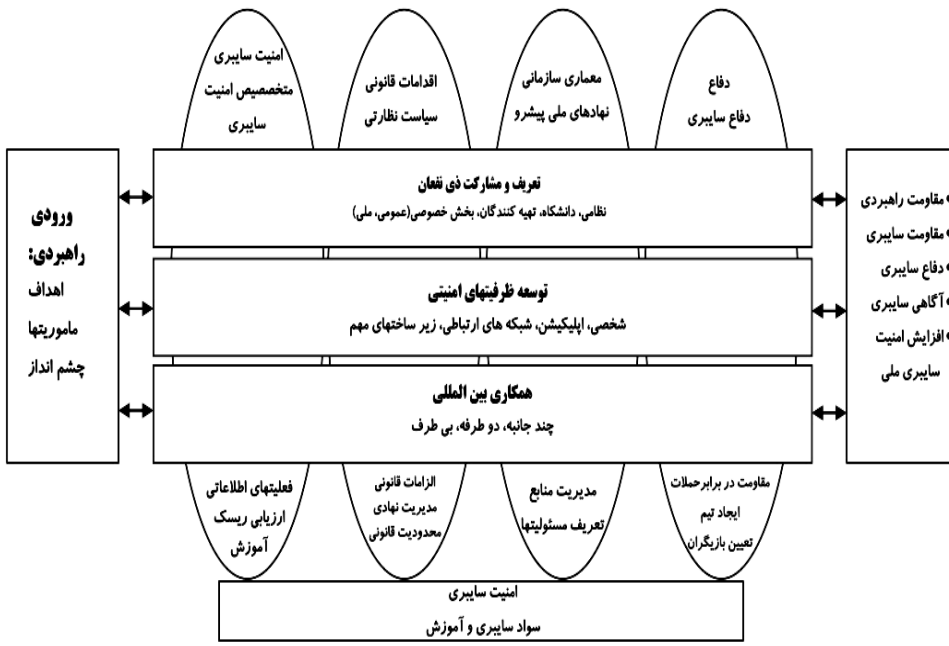


شکل (٤): فرآیند پردازش رویدادهای پیچیده

همچنین در ادامه و همان‌طور که در شکل‌های (۵) و (٦) ملاحظه می‌شود جهت استفاده از تجربیات دیگر کشورها مدل‌های مطرحی مورد بررسی قرار گرفته است.

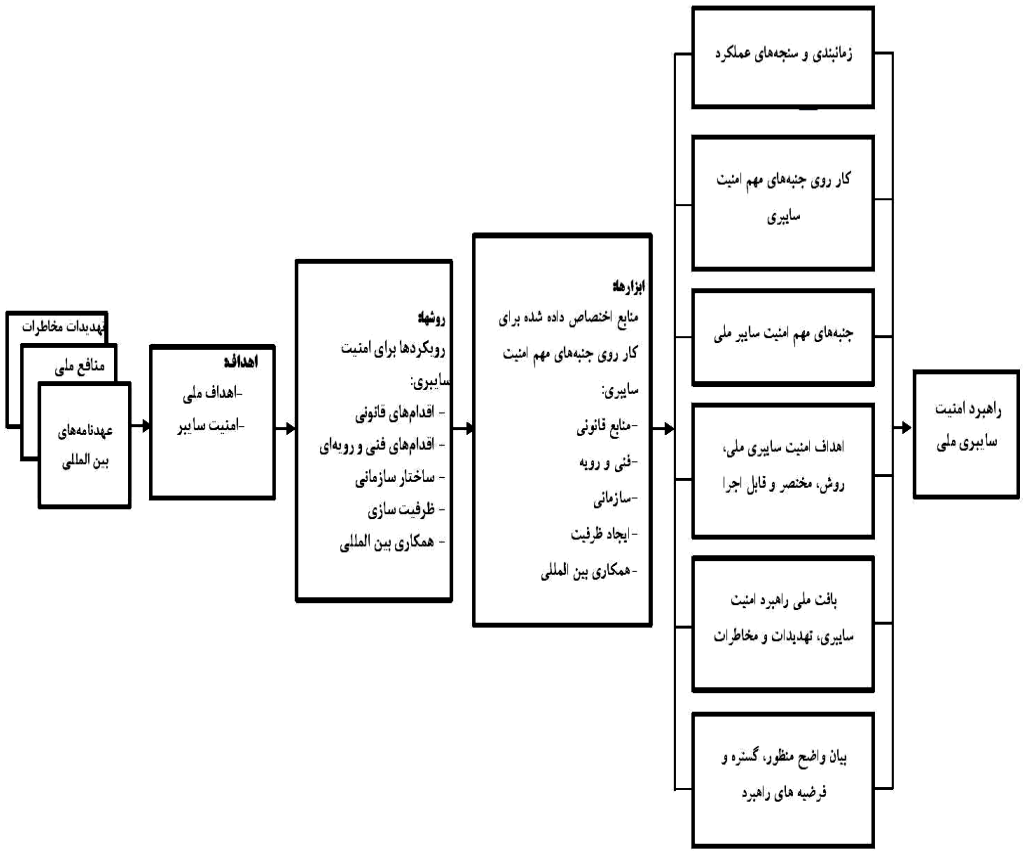
مدل راهبردی امنیت سایبری ملی[1]

این مدل شامل ویژگی‌های ورودی خاصی است تا بتواند مؤثر باشد. درنتیجه، نتایج خاص این مدل به دلیل تغییر مستمر ماهیت فضای مجازی، نیاز به ارزیابی مداوم دارد. این مدل بر اساس توصیه‌هایی است که اتحادیه بین‌المللی ارتباطات از راه دور[2]، ناتو[3]، سازمان همکاری اقتصادی و توسعه[4] و اتحادیه اروپا[5] معرفی کرده‌اند (R.Sabillon&others,2016).



شکل (۵): مدل کلی راهبردی امنیت سایبر ملی (همان)

1. National CyberSecurity Strategy Model (NCSSM)
2. International Telecommunication Union(ITU)
3. North Atlantic Treaty Organization(NATO)
4. Organisation for Economic Co-operation and Development(OECD)
5. European Union(EU)



شکل (٦): مدل راهبرد ملی امنیت سایبری

مدل راهبرد ملی امنیت سایبری[1]

اتحادیه بین‌المللی ارتباطات در سال ۲۰۱۱ میلادی سندی با عنوان سند راهنمای در حوزه راهبرد ملی امنیت سایبر منتشر نمود که مدل راهبرد ملی امنیت سایبر بخشی از این سند می‌باشد که در شکل (٦) ارائه شده است (اتحادیه بین‌المللی ارتباطات،۲۰۱۱).

1. National Cybersecurity Strategy Model

جدول (۲): شرح مفاهیم موجود در مدل راهبرد ملی امنیت سایبری

مفهوم	شرح
تهدیدات سایبری	نقض بالقوه ویژگی‌های امنیتی سایبری (محرمانگی، دسترس‌پذیری، یکپارچگی) است.
اقدام‌های قانونی[1]	تدوین راهبردهایی برای توسعه مدل قابل اجرا در سطح جهانی و قانون‌گذاری سازگار با جرائم سایبری.
اقدام‌های فنی و رویه‌ها	آسیب‌پذیری نرم‌افزارها را مورد توجه قرار داده و قصد دارد نوعی طرح تأیید اعتبار، پروتکل و استانداردهایی را توصیه کند که در سطح جهانی قابل قبول باشد.
اهداف ملی امنیت سایبری	اهداف ملی امنیت سایبری، موضوعات اقتصادی، اجتماعی و امنیت ملی را پوشش می‌دهد و امنیت ملی، پیشران امنیت سایبری به شمار می‌رود.
ظرفیت‌سازی[2]	هدف بیان ماهرانه راهبردهایی است که به بهبود دانش و تخصص در ارتقای امنیت سایبر بر اساس دستور کار سیاست ملی کمک می‌کند.
همکاری بین‌المللی	راهبردهای مربوط به همکاری‌ها، گفتگوها و هماهنگی‌های بین‌المللی را مورد توجه قرار می‌دهد.

مفاهیم ارائه‌شده در شکل (٦)، در جدول (۲) ارائه شده است.

شایان ذکر است اتحادیه بین‌المللی ارتباطات در این سند اشاره‌ای دارد به آنکه تخصص اتحادیه مذکور در قلمروی توسعه و حوزه فنی بوده و از ورود به موضوعات امنیت ملی و دفاع ملی حذر می‌نماید (وامالا، فردریک، ۲۰۱۱).

در جدول (۳) ویژگی‌های مدل‌های مورد بررسی ارائه شده است.

1. Ligal Measures
2. Capacity Building

جدول (۳): بررسی مدل‌های مدیریت راهبردی، مدیریت مخاطرات و مدیریت رخدادهای پیچیده

	ویژگیهای مشترک				ویژگیهای اختصاصی				
	کاربرد ملی	کاربرد در مدیریت امنیت	ارزیابی نتایج	تدوین راهبرد	۱	۲	۳	۴	۵
مدل RAND	۷	۷	۷	۷	بررسی دیدگاهای جهانی	اهمیت عنصر خلاقیت در تدوین راهبرد	در نظرگرفتن مصالح ملی	تاثیر وضعیت آینده در تدوین راهبردها	تاثیر توانمندیها و قابلیتهای ویژه در تدوین راهبردها
مدل برایسون	۷	۷	۷	۷	بررسی جامع محیط داخل و خارج و تاثیر آن در تدوین راهبردها	تاثیر ارزشها و ماموریتها بر تدوین راهبردها	توافق اولیه به منظور جلب حمایت وهمکاری تصمیم گیرندگان کلیدی	تعیین موضوعات راهبردی پیش رو	۱
استاندارد ایزو ۹۰۰۱	۷	۷	۷	۷	شناسایی داراییها	شناسایی آسیب پذیریها	ارزیابی ریسک	کنترل ریسک	
استاندارد ایزو۳۱۰۰۰	۷	۷	۷	۷	شنایایی داراییها	شناسایی آسیب پذیریها	ارزیابی ریسک	کنترل ریسک	
فرآیند پردازش رویدادهای پیچیده	۷	۷	-	-	واکنش بر خط	فرآیند یاد گیری	حافظه رویدادهای قبلی	-	
مدل کلی راهبردی امنیت سایبری ملی	۷	۷	۷	۷	بررسی ابعاد جهانی	در نظر گرفتن کلیه ذینفعان	لحاظ نمودن سازوکارهای جاری مقابله	لحاظ نمودن قوانین جاری	۱
مدل راهبرد ملی امنیت سایبر(ITU)	۷	۷	۷	۷	بکارگیری توسط کشورهای جهان	دارای دسته بندی روشها و ابزارها			

ارزیابی مخاطره

ریشه ناامنی و به‌تبع آن تولید مخاطره از بروز رخداد یا تهدید آغاز و از طریق ابعاد مختلف محتوا، محرمانگی، دسترس‌پذیری و یکپارچگی و سپس در قالب هر یک از مؤلفه‌های اقتصادی، اجتماعی، فرهنگی، سیاسی، نظامی و زیست‌محیطی ظهور و بروز می‌یابد.

ارزیابی مخاطره به روش تجزیه‌وتحلیل درخت رخداد[1] با بررسی آثار مخاطره در ابعاد چهارگانه و پس از آن تعیین سهم اثرپذیری هر یک از مؤلفه‌های شش‌گانه انجام می‌شود.

بنابراین در گام اول احتمال موفقیت تهدیدات اصلی و پایه مورد بررسی قرار می‌گیرد.

1. Event Tree Analysis

هر یک از این تهدیدات اینترنتی متناسب با روش و جامعه هدف، احتمال موفقیت متفاوتی را خواهند داشت. همچنین اثرگذاری یا موفقیت این تهدیدات در بازه‌های زمانی متفاوت با توجه به تغییرات محیطی و تغییرات کاربران به لحاظ اطلاعات دریافتی و ... دارای مقادیر احتمال متفاوتی خواهد بود. لذا در بررسی این بخش به دو موضوع می‌بایست پرداخته شود، که در ادامه به این موضوعات پرداخته شده است.

- احتمال موفقیت تهدیدات اینترنتی و تابع احتمال آن؛
- تغییرات تابع احتمال در بازه‌های زمانی مختلف؛

احتمال موفقیت تهدیدات اینترنتی و تابع احتمال آن- گستره شبکه‌های متصل به اینترنت در این پژوهش مورد توجه می‌باشد. این گستره شامل گره‌هایی است که از طریق تجهیزات به شبکه اینترنتی متصل شده‌اند. این گره‌ها، روزانه هدف تهدیدات و حملات متعددی قرار می‌گیرند.

اگر n تعداد گره‌های فعال و متصل به شبکه اینترنت باشد، بیان تعداد حملات به این تعداد گره در بازه زمانی مشخص از طریق تابع پواسن دارای تخمین مناسبی و قابل قبولی می‌باشد (N. Bazyar &others, 2017).

استفاده از توزیع پواسن تحت شرایط زیر محقق می‌شود:

- ررخداد دارای احتمال وقوع بسیار کمی باشد. به عبارتی احتمال وقوع رخداد باید کمتر از ۰.۱ باشد.
- ررخداد به‌صورت اتفاقی به وقوع می‌پیوندد و مستقل می‌باشد. به عبارتی وقوع رخداد وابسته به رخدادهای دیگر نمی‌باشد و قابل پیش‌بینی نمی‌باشد.

توزیع پواسن توسط یک پارامتر توصیف می‌شود (λ) که میانگین وقوع رخدادها در یک بازه زمانی می‌باشد. چگالی توزیع احتمال پواسن در امنیت سایبر مورد استفاده قرار می‌گیرد. این توزیع برای مشخص نمودن رفتارهای غیر معمول و ناهنجاری‌ها[1] در ترافیک شبکه‌های کامپیوتر مورد استفاده قرار می‌گیرد. انواع این ناهنجاری‌ها شامل یک حمله، یک

1. Anomaly

نفوذ، ویروس کامپیوتری و مواردی از این دست می‌باشد. تابع توزیع چگالی احتمال پواسن همچنین برای وروی هکرها کامپیوتری به سامانه‌ها مورد استفاده قرار می گیرد(S.K.Dutta, 2013).

همچنین موفقیت هر حمله مبتنی بر احتمال وجود آسیب‌پذیری، شناسایی و دفع حمله می‌باشد. تابع چگالی احتمال نمایی نیز بیان مناسبی از احتمال دفع حمله می‌باشد. از سویی مقدار احتمال مخاطره، برابر حاصل ضرب احتمال حمله در احتمال موفقیت در مقدار پیامد می‌باشد (N. Bazyar &others, 2017).

در خصوص مدل نمودن احتمال حمله سایبر اگرچه تابع توزیع پواسن تخمین مناسبی است، لیکن در عمل میانگین حملات در بازه زمانی مشخص، تغییر می‌کند و لازم است برای استفاده واقعی از تابع توزیع غیر همگن[1] استفاده شود (M. Eling& others, 2015).

روش‌شناسی تحقیق

این تحقیق از منظر هدف تحقیقی کاربردی می‌باشد چراکه سعی می‌شود نتایج حاصل از این تحقیق را مورد استفاده عملی قرار داده و با کمک نتایج آن، مشکلات کشور در حوزه امنیت سایبر رفع شود. ابعاد و مؤلفه‌های امنیت فضای سایبر که در پژوهش دیگر محقق از طریق تحلیل محتوا به‌دست‌آمده و با تأیید خبرگان نهایی‌سازی شده است، با استفاده از پارامترهای توصیفی ابعاد، مؤلفه‌ها، تبیین و توسط جامعه آماری محرز گردیده و در نهایت با استفاده از معادلات ساختاری و تحلیل مسیر، چارچوب مدل و پارامترهای همبستگی تدوین و قواعد آن‌ها با تغییر زمان، احصا شده است.

اما این تحقیق از منظر گردآوری اطلاعات تحقیقی از منابع کتابخانه‌ای و اسناد و مدارک معتبر و قابل دسترسی، توصیفی-پیمایشی می‌باشد. تدوین مدل نهایی مدیریت راهبردی امنیت فضای سایبر بر اساس چارچوب مدل استاندارد ISO31000 و یافته‌های مطالعات

1. non homogenic

انجام‌شده، صورت گرفته و ارزیابی مخاطرات با استفاده از تئوری شبکه بیز و مدل مارکوف مدوله‌شده با توزیع پواسن و به‌کارگیری ابرداده‌های فضای سایبر نهایی‌سازی انجام می‌شود.

یافته‌ها و تجزیه‌وتحلیل داده‌ها

الف: یافته‌های تحقیق

تخمین حداکثر درست‌نمایی تابع چگالی احتمال پواسن با استفاده از ابرداده‌های فضای سایبری برای به‌دست آوردن تابع پواسن با حداکثر درست‌نمایی برای مقادیر مشاهده $X_1,X_2,\dots,X_n$ داریم:

$$P(X=x)=\frac{\lambda^x}{x!}e^{-\lambda}$$

$$=log\lambda\sum_{i=1}^{n}X_i-n\lambda-\sum_{i=1}^{n}logX_i!$$

$$\frac{\partial l}{\partial\lambda}=\frac{1}{\lambda}\sum_{i=1}^{n}x_i-n=0 \quad \rightarrow \hat{\lambda}$$

$$=\frac{1}{n}\sum_{i=1}^{n}x_i$$

تغییرات تابع احتمال در بازه‌های زمانی مختلف- تهدیدات سایبری در طول زمان و با توجه به تغییرات مختلف فضای تهدید، احتمال تأثیرگذاری متفاوتی را خواهند داشت. به عبارتی فضای تهدید در اثر تغییر در عوامل انسانی، تجهیزاتی، دانش مرتبط با موضوع تهدید، مقاوم‌سازی آسیب‌پذیری‌ها و ... تغییر می‌کند.

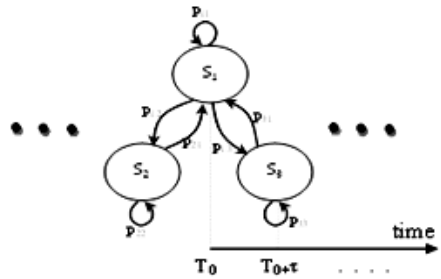
این تغییر گاهی باعث افزایش اثرگذاری و گاهی باعث کاهش اثرگذاری تهدیدات خواهد بود. اقدامات هدفمند برای کاهش اثرگذاری تهدیدات به‌عنوان اقدامات کاهش مخاطره در بخش‌های بعدی مورد بررسی قرار می‌گیرد. در این بخش فرض تشدید تأثیر تهدیدات مورد بررسی قرار گرفته است و نحوه اثرگذاری آن‌ها در مدل ارائه‌شده بیان می‌شود.

به عبارتی در بازه‌های زمانی τ شاهد تغییر در تابع احتمال موفقیت تهدید خواهیم بود و این تغییرات نیز خود با توجه به تابع احتمال تغییرات، تغییر خواهد نمود.

در شکل زیر فرآیند تغییرات مذکور در قالب زنجیره مارکف بیان شده است.

در مدل زنجیر مارکف شکل (۷) زنجیره دارای حداقل سه حالت است که طی ماتریس احتمال حالات Ps از یک حالت به حالت دیگر انتقال می‌یابد. به عبارتی تغییر وضعیت و حرکت از یک وضعیت به وضعیت دیگر یا ماندن در وضعیت موجود تابع، توابع احتمالی است که در ماتریس احتمال بدان‌ها اشاره شده است.

$$P_s = \begin{bmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{bmatrix}$$



شکل (۷): مدل زنجیره مارکف

همان‌طور که مشاهده می‌شود هر وضعیت به حالت قبلی وابستگی دارد. در واقع دنباله‌ای از متغیرهای تصادفی $X_1,X_2,\ldots X_1,X_2,\ldots$ را که تغییر وضعیت آن‌ها از زمان t_0 به $t_0+\tau$ تابع احتمالات مشخصی باشند را یک زنجیره مارکوف می‌نامند. این گزاره را به بیان متغیرهای تصادفی و تابع احتمال به‌صورت زیر نشان می‌دهیم.

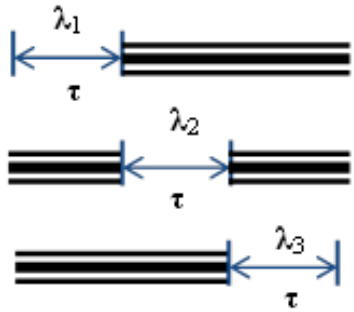
$$Pr(Xt_0+\tau=x|X1=x1,X2=x2,\ldots,Xn=xn)=Pr(Xt_0+\tau=x|Xt_0=xt_0)$$

این رابطه مبین این موضوع است که هر وضعیت با یک احتمال وابسته است به وضعیت قبلی خود و با یک احتمال وضعیت پس از خود را بیان می‌کند.

مدل مدوله مارکف بر فرآیندهای پواسن[1]- در بخش‌های گذشته اشاره گردید که احتمال k حمله در n گره اتصال به شبکه اینترنت تابع توزیع پواسن است. در مدل مدوله

1-Modulated Markov Poisson Process

مارکف بر فرآیندهای پواسن همان‌طور که در شکل (۸) ارائه شده است، متناظر هر یک از حالات $s_1,\ldots,s_n$ یک توزیع پواسن با λ متفاوت بیانگر حجم تهدیدات می‌باشد. مقدار λدر تابع توزیع پواسن نشانگر میانگین، واریانس و امید ریاضی[1] تابع است. از این رو پارامتر λ نشان‌دهنده نرخ رخداد پیشامد در واحد زمان است. به این معنی که این پارامتر را می‌توان متوسط تعداد رخداد پیشامد با بیشترین احتمال در یک فاصله با بازه زمانی در نظر گرفت.



شکل (۸): مدل مدوله مارکف بر فرآیند پواسن

مدل نهایی ارزیابی ریسک – شبکه بیز حاصل ارتباطات شرطی نودهای شبکه است که از ارتباطات شرطی شبکه با تابع احتمال ابتدایی والد pt آغاز می‌گردد. احتمال pt نیز به‌نوبه خود حاصل تغییرات λ در توزیع پواسن می‌باشد که این تغییرات در طول زمان با فرآیند زنجیره مارکف مدوله‌شده با توزیع پواسن[2] بیان گردیده است.

از این رو مدل نهایی ارزیابی مخاطرات حاصل، مطابق شکل (۹) شامل دو بخش زیر می‌باشد:

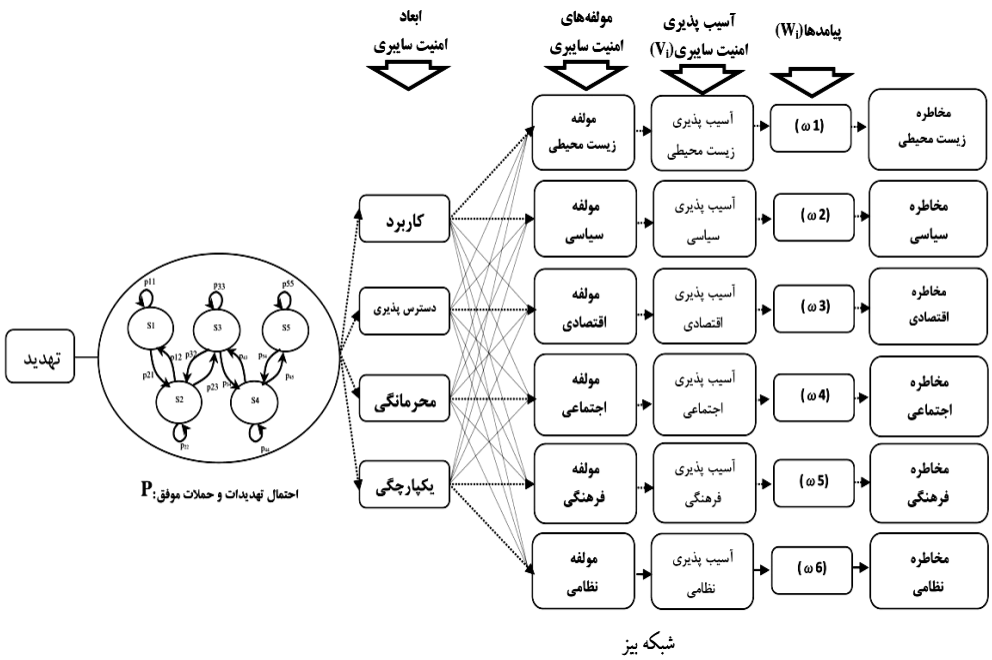
- بخش اول شامل تابع پواسن مدوله‌شده بر زنجیره ماکوف به‌عنوان تابع والد pt
- بخش دوم شامل شبکه بیز با توابع احتمال شرطی با شرط اولیه و والد pt

1. Mathematical Expectetion
2. Markov Modulated Poison Process (MMPP

۱- کاهش احتمال موفقیت تهدید، pt، در مدل ارائه شده

۲- روند میرای λ در فرآیند زنجیره مارکف مدوله‌شده با توزیع پواسن

۳- کاهش پیامدهای تهدیدات



شکل (۹): مدل ارزیابی مخاطره

تجزیه‌وتحلیل و ارائه مدل مدیریت راهبردی امنیت فضای سایبر

چارچوب استاندارد ۳۱۰۰۰[1] چارچوبی کامل و دربردارنده کلیه نیازمندی‌های تشخیص، ارزیابی، مدیریت و پایش مخاطرات می‌باشد و در تدوین مدل نهایی این چارچوب به‌عنوان چارچوب مرجع در نظر گرفته شده است که المان‌های مورد نیاز در این چارچوب با استفاده از مدل‌های زیر جانمایی شده است.

1. http: //www.isiri.gov.ir/portal/home/?news/150911/148455/562448/معرفی-استاندارد-ایزو-۳۱۰۰۰-مدیریت-ریسک

- مدیریت راهبردی برایسون
- تجزیه‌وتحلیل رویدادهای پیچیده
- مدیریت راهبردی RAND
- مدل راهبردی امنیت سایبری ملی

نتایج حاصل از نگاشت مدل‌های اشاره‌شده در چارچوب استاندارد ۳۱۰۰۰ در جداول (٤) و (٥) ارائه شده است همان‌طور که در این جداول مشاهده می‌شود لازم است برخی از نیازمندی‌ها به مدل نهایی افزوده شود. مدل نهایی مدیریت راهبردی امنیت فضای سایبر با استفاده از کلان‌داده‌های این فضا و بهره‌گیری از مدل ارزیابی مخاطره، شکل (۹) و همچنین استفاده از مدل‌های مدیریت راهبردی برایسون، RAND، مدل تجزیه‌وتحلیل رویدادهای پیچیده و مدل راهبردی امنیت سایبری ملی در شکل (۱۰) ارائه گردیده است.

جدول (٤): تناظر بین نیازمندی‌های پیاده‌سازی استاندارد ۳۱۰۰۰ و مدل‌های مورد استفاده قرار گرفته

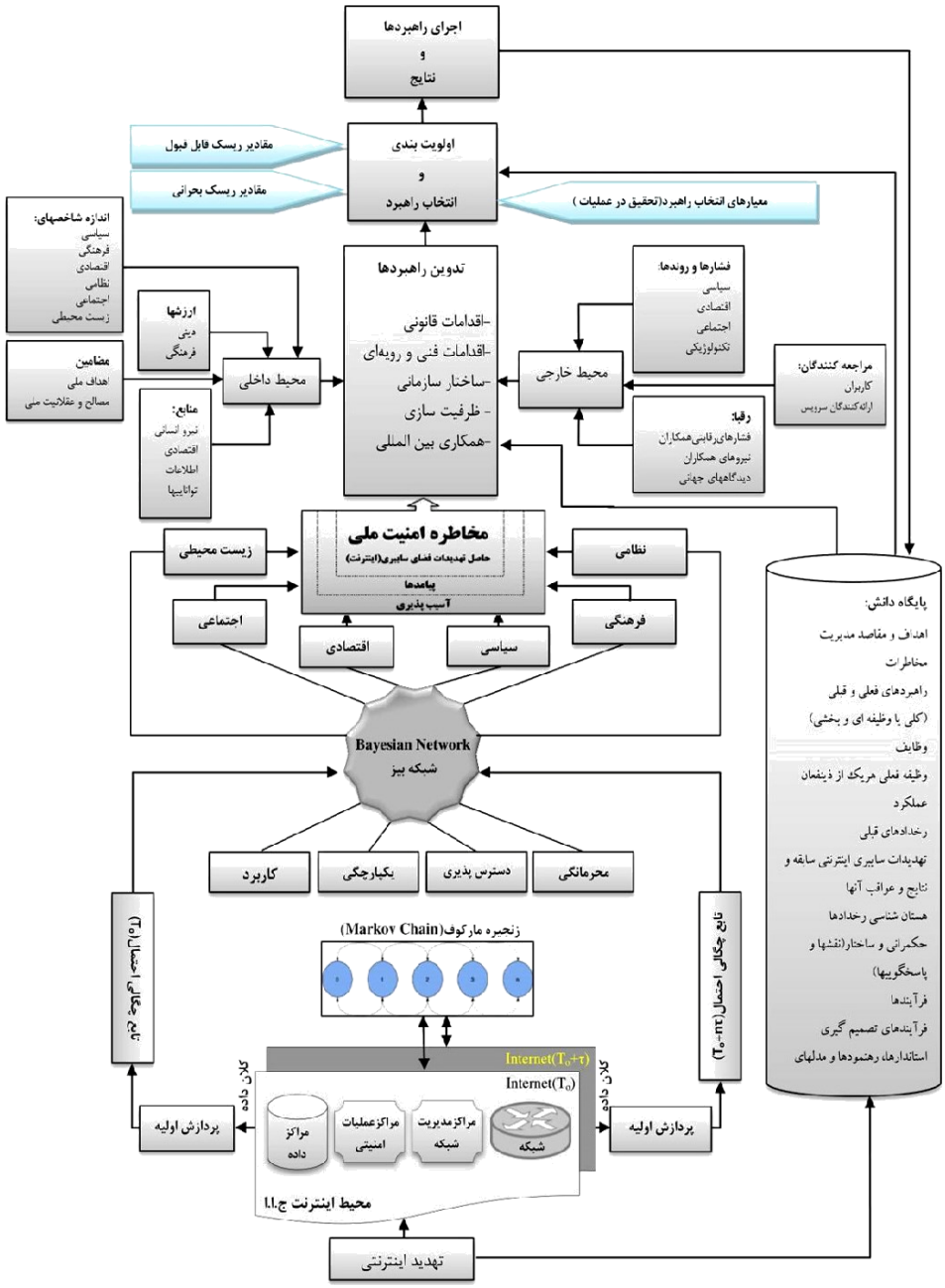
	محیط داخلی									محیط خارجی							
	حکمرانی و ساختار(نقشها و پاسخگوییها)	سامانه‌ها و خط مشی ها	توانمندیها				فرهنگ حاکم	فرآیندهای تصمیم گیری	استانداردها، رهنمودها و مدلهای اتخاذ شده	اهداف و مقاصد مدیریت مخاطرات	اجتماعی	سیاسی	نظارتی	اقتصادی	فناوری	رقابتی	محرکها و روندهای کلیدی	روابط باذینفعان و ادراکها و ارزشهای آنان
			اقتصادی	افراد	فرآیندها	سیستمها و فناوریها												
مدل مدیریت راهبردی برایسون		√	√	√		√					√	√		√	√	√		
مدل مدیریت راهبردی RAND							√										√	√
مدل پردازش فرآیندهای پیچیده																		
موارد افزایشی به مدل	√				√			√	√	√			√					
مدل راهبردی امنیت سایبر ملی		√																√
مدل راهبرد ملی امنیت سایبر(ITU)													√					√

جدول (۵): تناظر بین نیازمندی‌های پیاده‌سازی استاندارد ۳۱۰۰۰ و مدل‌های مورد استفاده قرارگرفته

	شناسایی ریسک					تحلیل ریسک			ارزیابی ریسک			برخورد با ریسک		
	منابع ریسک	حوزه تاثیرات	رخدادها(تغییرات در اوضاع و احوال)	دلایل و عواقب آن	فهرستی از ریسکها	درنظر گرفتن دلایل و منابع ریسک، عواقب مثبت و منفی آنها و احتمال وقوع این عواقب	شناسایی قواقب و احتمال اثر تاثیر گذاری	وابستگی متقابل ریسکها ومنابع آنها	تعیین اولویتهای برخورد با ریسکها	سنجش ریسک	تعیین برخورد با کنترل ریسک	ارزیابی برخورد با ریسک	تصمیم در این خصوص که سطح ریسک باقیمانده قابل تحمل است	در صورتی که قابل تحمل نباشد ایجاد برخورد با ریسکی جدید و ارزیابی اثر بخشی این ریسک
مدل مدیریت راهبردی برایسون									√			√	√	√
مدل مدیریت راهبردی RAND														
پردازش فرآیندهای پیچیده			√	√	√	√	√	√			√			
مدل ارزیابی ریسک	√	√		√		√	√		√	√			√	
موارد افزایشی به مدل	√	√								√			√	
مدل راهبردی امنیت سایبر ملی														
مدل راهبرد ملی امنیت سایبر(ITU)		√							√		√	√		

اعتبار مدل

همان‌طور که اشاره‌شده مدل نهایی مدیریت راهبردی امنیت فضای سایبر بر اساس کلان‌داده‌های فضای سایبر مبتنی بر مدل استاندارد ایزو ۳۱۰۰۰ و پیاده‌سازی این مدل می‌باشد. همچنین و از سوی دیگر اجزای به کار گرفته شده در این پیاده‌سازی از مدل‌های معتبر برگرفته شده است، مضافاً ابعاد و مؤلفه‌های امنیت سایبر نیز از طریق پرسشنامه به تأیید خبرگان رسیده است. در مجموع هم چارچوب مدل نهایی و هم اجزای آن داری اعتبار بوده که در مجموع مدل ارائه‌شده نیز از اعتبار کامل برخوردار می‌باشد. همچنین در ادامه انجام شبیه‌سازی با استفاده از یک سناریوی مفروض، ارائه گردیده است.



شکل (۱۰): مدل نهایی مدیریت راهبردی امنیت فضای سایبر بر اساس کلان‌داده‌های فضای سایبر

شبیه‌سازی

شبیه‌سازی انجام‌شده در قالب یک سناریو به شرح زیر انجام شده است.

سناریوی شبیه‌سازی: تهدید سایبری که در شبیه‌سازی لحاظ شده است، انتشار لینک دانلود یک نرم‌افزار فیلترشکن در یکی از پیام‌رسان‌های اینترنتی است. این تهدید در بررسی انجام‌شده مشخص گردید بدافزاری است که علاوه بر قابلیت جاسوسی و سرقت اطلاعات، امکان دسترسی به محتواهای غیر مجاز را نیز فراهم می‌کند. این بدافزار در شبکه‌ای از کاربران که ۱۰۰ میلیون نود متصل به شبکه دارد، توزیع می‌شود. شبکه توزیع اینترنت متشکل از ده ارائه‌کننده سرویس اینترنتی[1] (ISP1…ISP10) است که کاربران هر یک متناسب شرایط اجتماعی، فرهنگی، اقتصادی و ... دارای رفتارهای متفاوتی هستند؛ لیکن در مجموع احتمال موفقیت حملات را برای همه کاربران ۰.۵ در نظر گرفته‌ایم. روند توزیع و موفقیت حملات تا یک هفته مورد رصد قرار گرفته و برای ده هفته پیش‌بینی و تخمین زده شده است.[2]

موفقیت تهدید و افزایش مخاطرات: در جدول (٦) احتمال اثرگذاری تهدید بر ابعاد امنیت سایبر، دسترس‌پذیری، محرمانگی، یکپارچگی و کاربرد ارائه شده است. همچنین در جداول (۷)، (۸)، (۹)، (۱۰) نیز احتمال اثرگذاری تهدید بر مؤلفه‌های امنیت سایبر متناظر با هر یک از ابعاد و پیامدهای آن‌ها ارائه شده است. در شکل (۱۱) و شکل (۱۲) مقادیر λ برای یک هفته رصد شده و ماتریس انتقال متناظر این تغییر ارائه شده است. در نمودار شکل (۱۳) نیز شاهد مجموع مخاطره در هر یک از مؤلفه‌ها هستیم. همان‌طور که مشاهده می‌شود بیشترین مخاطره را مؤلفه‌های سیاسی، اقتصادی و فرهنگی دارا می‌باشند. نمودار شکل (١٤) نیز نمودار تغییرات مجموع مخاطرات در کلیه مؤلفه‌های می‌باشد.

1 Internet Service Provider

۲ اطلاعات کامل شبیه سازی در پیوست ۱ ارائه شده است

جدول (٦): احتمال تأثیر تهدید برابعاد امنیت فضای سایبر

	احتمال تهدید در هر یک از ابعاد
مؤلفه یکپارچگی	0.1
مؤلفه محرمانگی	0.2
مؤلفه کاربرد	0.6
مؤلفه دسترس پذیری	0.1

جدول (۷): احتمال تأثیر تهدید بر مؤلفه‌های امنیت فضای سایبر و ضریب پیامدها/آسیب‌پذیری‌ها در بعد محرمانگی

	احتمال تهدید در هر یک از مؤلفه‌ها		ضریب (پیامد-آسیب پذیری)(۱-۱۰)
محرمانگی	0.6	مؤلفه اقتصادی	4
	0.1	مؤلفه اجتماعی	2
	0.1	مؤلفه فرهنگی	3
	0.05	مؤلفه نظامی	6
	0.2	مؤلفه سیاسی	5
	0.05	مؤلفه زیست محیطی	4

جدول (۸): احتمال تأثیر تهدید بر مؤلفه‌های امنیت فضای سایبر و ضریب پیامدها/آسیب‌پذیری‌ها در بعد کاربرد

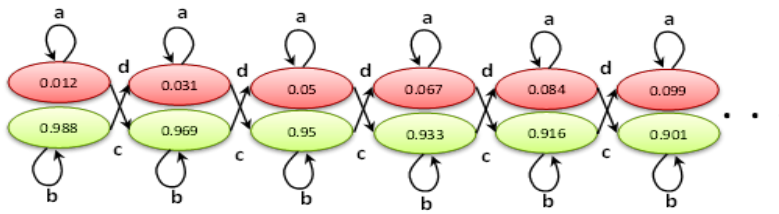
	احتمال تهدید در هر یک از مؤلفه‌ها		ضریب (پیامد-آسیب پذیری)(۱-۱۰)
محتوا	0.1	مؤلفه اقتصادی	4
	0.1	مؤلفه اجتماعی	2
	0.5	مؤلفه فرهنگی	3
	0.05	مؤلفه نظامی	6
	0.2	مؤلفه سیاسی	5
	0.05	مؤلفه زیست محیطی	4

جدول (۹): احتمال تأثیر تهدید برمؤلفه‌های امنیت فضای سایبر و ضریب پیامدها/آسیب‌پذیری‌ها در بعد دسترس‌پذیری

	احتمال تهدید در هر یک از مؤلفه‌ها		ضریب (پیامد-آسیب پذیری)(۱-۱۰)
دسترس پذیری	0.35	مؤلفه اقتصادی	4
	0.30	مؤلفه اجتماعی	2
	0.1	مؤلفه فرهنگی	3
	0.05	مؤلفه نظامی	6
	0.15	مؤلفه سیاسی	5
	0.05	مؤلفه زیست محیطی	4

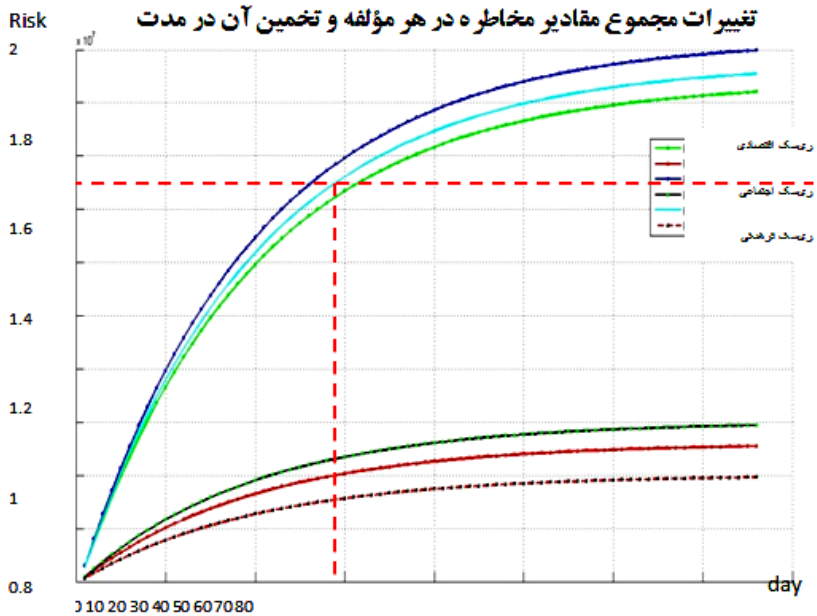
جدول (۱۰): احتمال تأثیر تهدید بر مؤلفه‌های امنیت فضای سایبر و ضریب پیامدها/آسیب‌پذیری‌ها در بعد یکپارچگی

	احتمال تهدید در هر یک از مؤلفه‌ها		ضریب (پیامد-آسیب پذیری)(۱-۱۰)
یکپارچگی	0.4	مؤلفه اقتصادی	4
	0.2	مؤلفه اجتماعی	2
	0.1	مؤلفه فرهنگی	3
	0.05	مؤلفه نظامی	6
	0.2	مؤلفه سیاسی	5
	0.05	مؤلفه زیست محیطی	4

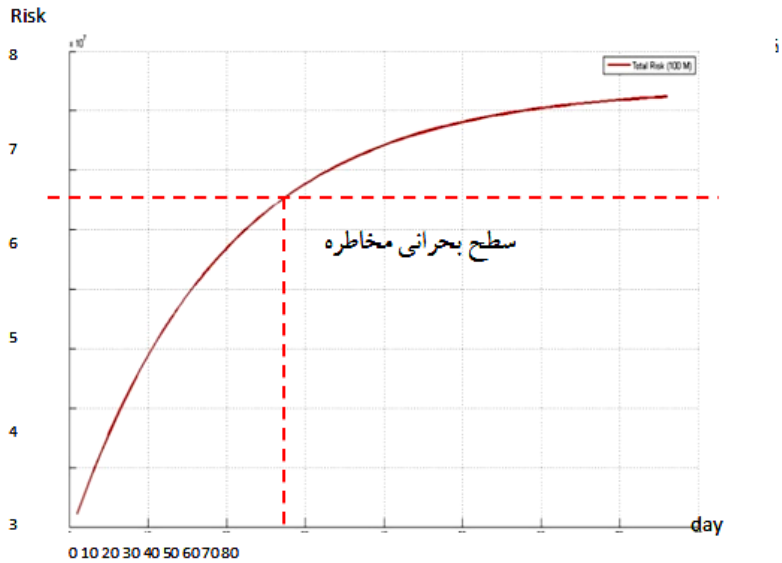


$$\begin{bmatrix} a & d \\ c & b \end{bmatrix} = \begin{bmatrix} 0.97 & 0.03 \\ 0.02 & 0.98 \end{bmatrix}$$

شکل (۱۱): ماتریس انتقال زنجیره مارکف



شکل (۱۲): تغییرات مجموع مقادیر مخاطرات در هر مؤلفه و تخمین آن در مدت ۱۰ هفته



شکل (۱۳): تغییرات مجموع مقادیر مخاطرات در همه مؤلفه‌ها و تخمین آن در مدت ۱۰ هفته

مدیریت مخاطرات

همان‌طور که در نمودارهای شکل‌های (۱۲) و (۱۳) مشاهده می‌شود مقدار عددی مخاطرات در مؤلفه‌های مختلف در طی هفته‌های متوالی در حال افزایش است. اگر سطح بحرانی مخاطرات را مقداری که در شکل‌ها نشان داده شده است فرض کنیم، روند افزایش مخاطره در نمودار شکل (۱۳) در مؤلفه‌های سیاسی و فرهنگی و اقتصادی و شکل (١٤) در مجموع مخاطرات در کمتر از ٤ هفته از این سطح بحرانی عبور می‌کنند و لازم است پیش از رسیدن به این مقدار با استفاده از راهبردهای مناسب کنترل شده و به مقادیر قابل قبول بازگردند.

انتخاب راهبرد مطابق شکل (۱۰) به دو صورت قابل انجام است:

الف- با عنایت به سوابق قبلی تدوین و انتخاب راهبرد، در پایگاه دانشی مدل در حداقل زمان قابل دسترسی می‌باشد.

ب- در صورت عدم وجود سوابق قبلی و جدید بودن تهدید، تدوین راهبرد با تجزیه‌وتحلیل محیط خارجی و داخلی صورت می‌گیرد.

پس از تدوین راهبردهای قابل قبول، انتخاب بهترین راهبرد در شبیه‌سازی انجام‌شده، مبتنی بر معیارهای زیر صورت می‌گیرد:

اگر $S_1,S_2,\dots,S_n$ راهبردهای قابل قبول، $T_1,T_2,\dots,T_n$ زمان اجرای هر یک، $G_1,G_2,\dots,G_n$ اثرگذاری آن‌ها و $C_1,C_2,\dots,C_n$ هزینه اجرای هر یک از راهبردها باشند آنگاه راهبردهایی مورد پذیرش نهایی قرار می‌گیرند که:

$$T_{s_j} \leq 4 \text{ هفته}, j = 1,2,\dots \sum_j (S - C)_j \leq L$$

(رابطه ٤-۲۵)-۲٦)

آنگاه با توجه به مفروضات جدول (۱۱) انتخاب راهبرد صورت می‌گیرد.

جدول (۱۱): وضعیت راهبردها به لحاظ سه پارامتر G، C و T(مفروضات سناریو)

راهبرد	زمان اجرا (روز)	هزینه (برحسب L)	ضریب اثرگذار	راهبرد منتخب
S_1	۲۰	L	٤	
S_2	٤٥	L/2	٥	
S_3	١٦	L/2	۳	√
S_4	۱۷	3L/5	٤	
S_5	۲۲	L/2	۳	√

به عبارتی راهبردهایی مورد پذیرش نهایی هستند که علاوه بر آنکه تأمین‌کننده محدودیت زمانی پاسخگویی به تهدید می‌باشند؛ به لحاظ تأثیرگذاری و کاهش مخاطره و همچنین هزینه اجرای (امکان‌پذیری) نیز مناسب تشخیص داده شوند.

نتیجه‌گیری و پیشنهاد

نتیجه‌گیری

یافته‌های این پژوهش نشان داد که ناامنی در فضای سایبر مؤلفه‌های امنیت ملی را نیز تحت تأثیر قرار می‌دهد. آنچه می‌تواند در افزایش سرعت مدیریت مخاطرات و پیش‌بینی روند رشد مخاطره به طرز قابل توجهی تعیین‌کنندگی داشته باشد تجزیه‌وتحلیل داده‌های برآمده از این فضا (کلان داده‌ها) می‌باشد.

تغییرات در فضای سایبر دربرگیرنده تمامی اجزای این فضاست. فنّاوری‌های تولید داده‌ها، روش‌های مختلف با سرعت‌های متفاوت برای انتقال و ذخیره داده‌ها و همچنین کارکردها، خدمات و سرویس‌های نوین و جدید، همه و همه گویای سرعت تغییر و تحول در اجزای فضای سایبر است.

این شرایط امکان اختصاص فرصت زیادی را برای پرداختن به فرآیندهای متداول مدیریت جهت مدیریت فضای سایبر فراهم نمی‌سازد. این موضوع به‌ویژه در مورد مدیریت امنیت فضای سایبر حائز اهمیت و توجه بیشتری است. کلان‌داده‌های فضای سایبر و به‌تبع

آن کلان‌داده‌های این فضا بروندادهای واقعی و به‌هنگامی هستند که حاوی اطلاعات لازم برای مدیریت به‌هنگام فضای سایبر و امنیت حاکم بر آن هستند.

از سوی دیگر تهدیدات سایبر تأثیرات متفاوتی را بر مؤلفه‌های تأثیرگذار بر امنیت ملی خواهند داشت و رشد مخاطره در قالب هر یک از مؤلفه‌ها با رشد مخاطره در دیگر مؤلفه‌ها تفاوت دارد و لازم است راهبردها با توجه به آثار آن‌ها در کنترل و تأثیر ایشان بر مؤلفه‌های بیشتر در معرض مخاطره قرارگرفته، تدوین شود.

همچنین کشور در زمان‌های مختلف نسبت به سطح مخاطره در هر یک از مؤلفه‌ها دارای سطح حساسیت و مقدار قابل قبول متفاوتی است. به عبارتی کشور در بزنگاه‌های مختلف دارای سطوح حساسیت و قابل قبول متفاوتی از مخاطرات مؤلفه‌های مختلف تأثیرگذار بر امنیت ملی است و لازم است راهبردها از حیث سرعت تأثیرگذاری ایشان و تناسب آن‌ها با سرعت رشد مخاطره و زمان رسیدن سطح مخاطرات به سطوح قابل قبول مخاطره تدوین شود.

پیشنهادات

مدل ارائه‌شده در این پژوهش قالبی است کلان که دربردارنده کلیه تهدیدات در فضای سایبر است که برای توسعه این مدل پیشنهادات زیر قابل اجرا می‌باشد:

۱. مدل ارائه‌شده نیازمند محاسبات و تحلیل‌های گسترده‌ای در شرایط عملیاتی می‌باشد. پیاده‌سازی مدل در قالب نرم‌افزار می‌تواند به‌عنوان ادامه مسیر این پژوهش مورد توجه پژوهشگران قرار گیرد.

۲. تهدیدات مختلف فضای سایبر دارای رفتارهای مختلفی هستند که داده‌های مرتبط با این رفتارها به روش‌های مختلف و از درگاه‌های متعددی با چگالی اطلاعات متفاوت در حال تولید است. در بررسی تهدیدات فضای سایبر در بخش‌های مختلف از قبیل تهدیدات حاصل از شبکه‌های اجتماعی، پیام‌رسان‌ها، نرم‌افزارهای کاربردی موبایلی، بازی‌ها و... و تدوین رفتار تهدیدات در هر یک

از موارد اشاره‌شده، کلان‌داده‌های متأثر در هر یک از تهدیدات و همچنین راهبردهای متداول در هر یک از تهدیدات نیز می‌تواند در ادامه این پژوهش انجام گردد.

۳. مؤلفه‌های مختلف در بازه‌های مختلف زمانی دارای حساسیت‌ها و آستانه‌های تحمل متفاوتی هستند. یکی دیگر از مواردی که نیاز به بررسی بیشتر دارد تحلیل حساسیت و بررسی تأثیر حساسیت هر یک از مؤلفه‌ها در زمان‌های مختلف برای تدوین راهبردها می‌باشد.

فهرست منابع ومآخذ

الف. منابع فارسی

۱. جعفری، مجتبی (۱۳۸۵)، برنامه راهبردی امنیت فضای تبادل اطلاعات وزارت ارتباطات و فناوری اطلاعات.

۲. جورج سادوسکای، جیمزاکس. دمپزی، آلن گرینبرگ، باربارا جی. مک، آلن شوارتز، (۱۳۸٤)، راهنمای امنیت فناوری اطلاعات.

۳. حقی مجید؛ فیروزآبادی ابوالحسن؛ خراشادی‌زاده محمدرضا (۱۳۹۸)، ارائه مدل مدیریت راهبردی امنیت فضای سایبر بر اساس ابرداده‌های فضای سایبر.

٤. خلیل پور رکن‌آبادی، ع؛ نورعلی وند (۱۳۹۱)، تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصلنامه مطالعات راهبردی شماره ٥٦.

٥. دیوسالار، عبدالرسول (۱۳۹۱)، قدرت اطلاعات، تیسا.

٦. سیاست‌های کلی نظام در امور «امنیت فضای تولید و تبادل اطلاعات و ارتباطات و سند راهبردی امنیت فضای تولید و تبادل اطلاعات».

۷. وامالا، فردریک (۲۰۱۱)، سند راهنمای اتحادیه بین‌المللی مخابرات در حوزه راهبرد ملی امنیت سایبری.

الف. منابع لاتین

1. Martin Elinga, Jan Hendrik Wirfs, (2015), Modelling and Management of Cyber Risk Institute of
2. Insurance Economics, University of St. Gallen, Rosenbergstrasse 22, 9000 St. Gallen, Switzerland
3. C.EVANSJR., (2016), DATA GOVERNANCE FRAMEWORK IMPLEMENTATION PLAN.
4. Neda Bazyar Shourabi & Richard Dean& Farzad Moazzami& Yacob Astatke, (2017), A MODEL FOR CYBER ATTACK RISKS IN TELEMETRY NETWORKS
5. G. Bradley, (2011), A Guid To Risk Management.
6. O. Kotevska, A. Lbath, and S. Bouzefrane, (2016), Toward a Real-Time Framework in Cloudlet-Based Architecture.
7. Saurav K.Dutta, (2013),Statistical Techniques for Forensic Accounting Understanding the theory and Application of Data Analysis,
8. Matthew A. Levin, MD, Jonathan P. Wanderer, MD, MPhil, and Jesse M. Ehrenfeld, MD, MPH, (2015), Data, Big Data, and Metadata in Anesthesiology
9. Rauscher & Yaschenko (2011). bilateral on cybersecurity: Critical terminology foundations. New York: NY: East-West Institute.
10. Lowe, Deidre. Metadata (1999), "8th International Dublin core metadata initiative workshop" (2000). Available at: http://www.ifla.org/udt/dc8/ (2007.50.29.(
11. Sabillon, Regner, cavaller, Victor, (2016), National Cyber Security Strategies: Global Trends in Cyberspace
12. National Institute of Standards and Technology Attn: Computer Security Division, Information Technology Laboratory 100 Bureau Drive, (2011)