آینده‌پژوهی دفاعی، سال هشتم، شماره ۲۸، بهار ۱۴۰۲

تاریخ دریافت: ۱۴۰۰/۱۲/۱۴ تاریخ پذیرش: ۱۴۰۲/۰۳/۱۰

از صفحه ۷ تا صفحه ۳۱

واکاوی تهدیدات امنیتی شبکه‌های رایانه‌ای سازمان‌ها با رویکرد آینده‌پژوهی (مطالعه موردی ستاد فرماندهی نیروی پدافند هوایی آجا)

ابراهیم ایجابی[۱]

خلیل کولیوند[۲*]

نوع مقاله: پژوهشی

چکیده

آینده‌پژوهی، دانش نوظهوری است که می‌تواند منجر به سودمندی اقتصادی، دفاعی، نظامی و اجتماعی بشود. ماهیت فناوری در حال تغییر و تحول بوده و سرعت این تغییر از هر زمان دیگری در زمان کنونی بیشتر است. آینده‌پژوهی فناوری‌ها، یک ابزاری برنامه‌ریزی است که احتمال ایجاد فناوری و تاثیر آن در دستیابی به آینده مطلوب را مشخص می‌نماید. این مقاله با هدف واکاوی تهدیدات امنیتی شبکه‌های رایانه‌ای سازمان‌ها با رویکرد آینده‌پژوهی (مطالعه موردی ستاد فرماندهی نیروی پدافند هوایی آجا) با استفاده از روش چرخه آینده و تلفیق این روش با پنل خبرگی و جلسات ذهن‌انگیزی انجام گردید. با بهره‌گیری از پنل خبرگان ۷۸ تهدید امنیتی شناسایی که با استفاده از رتبه‌بندی و تعیین ارزش تهدیدات احصاء شده، تعداد ۴۴ تهدید مهم و اثرگذار تعیین شد. در ادامه پرسشنامه‌ای به منظور بررسی ارزش هر یک از ۴۴ تهدید به دست آمده تهیه و در اختیار کارشناسان و خبرگان مربوطه قرار گرفت و با استفاده از الگوی فریدمن و بر اساس معدل‌گیری یک تا پنج بر مبنای طیف لیکرت از میان ۴۴ تهدید امنیتی آن دسته از تهدیداتی که نمره کمتر از میانگین را کسب نمودند به عنوان تهدیدات کم اهمیت حذف و تعداد ۲۰ عامل تهدیدزا که نمره بالاتر از میانگین را به خود اختصاص دادند جهت بررسی نهایی انتخاب گردیدند. در نهایت با استفاده از نرم‌افزار آینده‌پژوهی Mic-Mac و با به کارگیری روش تحلیل ماتریس متقاطع، تعداد هفت عامل تهدیدزا دارای نقش تأثیرگذار به عنوان مهمترین تهدیدات شناسایی گردید.

واژه‌های کلیدی:

تهدیدات امنیتی، شبکه رایانه‌ای سازمان‌ها، پانل خبرگان، چرخه آینده، نرم‌افزار آینده‌پژوهی Mic-Mac.

[۱] استادیار آینده‌پژوهی دانشگاه فرماندهی و ستاد آجا، تهران، ایران.

[۲] دانشجوی کارشناسی ارشد آینده‌پژوهی دفاعی، دانشگاه فرماندهی و ستاد آجا، تهران، ایران.

[*] نویسنده مسئول: k.koulivand@casu.ac.ir

CC BY NC ND

10.22034/DFSR.2022.550053.1581

مقدمه

الگوی نبردها در قرن جدید الگوی کاملاً متفاوت با دهه‌های گذشته است. جنگ‌های نوین متحول شده و هم دولت‌ها و سازمان‌ها و گروه‌های تروریستی با اهداف متنوع، متعدد و متفاوت از گذشته به جنگ می‌پردازند و هم روش‌های رزم نوین با توجه به ورود سیل عظیم فناوری های برتر به عرصه نظامی تغییر یافته است. مطالعه روند تحقیقاتی نظامی کشورهای غربی (آمریکا، فرانسه و ایتالیا) بیانگر این واقعیت است که چالش جدیدی به نام جنگ‌های اطلاعاتی به وجود آمده است. در جنگ‌های نسل پنجم و ششم ماهیت حملات به گونه‌ای است که زیرساخت نامرئی و ناشناخته را برای عامه جامعه مورد هدف قرار می‌دهد. در این نوع حملات عمدتاً یک شبکه رایانه‌ای[1] که حاصل پیوند پروتکل‌های استفاده شده و پورت‌های باز می‌باشد مورد حمله قرار می‌گیرند. از این‌رو کارشناسان امنیت اطلاعات، با تمرکز بر محورهای بالا، شبکه‌ای ایمن و مقاوم در مقابل انواع حملات ایجاد و نگهداری می‌نماید. (رستمی، ۱۳۹۴). [2]

همراه با رشد شبکه‌های رایانه‌ای، تهدیدهای مختلف امنیتی نیز برای این شبکه‌ها به وجود آمده است. حمله بدافزارها[3] و استفاده از تکنیک‌های آلوده‌سازی که منجر به اختلال در عملکرد شبکه و سرویس‌های آن می‌شوند، تهدیدهای جدی امنیتی در هر شبکه رایانه‌ای قلمداد می گردد. محققان بسیاری در زمینه شناسایی بدافزارها، شناخت طبیعت و شیوه عملکرد بدافزارها، نحوه انتشار و نیز راهکارهای مقابله با اثرات مخرب آنها مطالعه و تحقیق می‌نمایند. شرکت‌های بزرگ آنتی ویروس[4]، آنتی اسپم[5] و... روزانه هزاران تهدید امنیتی را کشف و خنثی می‌کنند (عنایتی و همکاران، ۱۳۹۹).

جامعه جهانی در حال گذر از دنیای فیزیکی به دنیای مجازی است. ورود به عصر اطلاعات و زندگی اثربخش در جامعه اطلاعات محور امروز مستلزم شناخت ویژگی‌های آن است (حمیدی و همکاران، ۱۴۰۰).

بکارگیری فناوری اطلاعات (IT)[6]، تحول گسترده‌ای در امور اداری و سامانه‌های اطلاعاتی به وجود آورده است، طوری که امکان انتقال الکترونیکی داده‌ها، مدارک، اسناد و مکاتبات مختلف از طریق رایانه و خطوط ارتباطات مخابراتی فراهم شده است. فناوری اطلاعات چنان تاثیر

---

[1] Camputer Networks

[2] نگارندگان مقاله با رعایت مالکیت معنوی منابعی که از آن‌ها در تدوین این مقاله استفاده کرده‌اند، بجای تلفظ انگلیسی کلمات در متن مقاله، از کلمات معادل فارسی مناسب مصوب فرهنگستان فارسی به‌کار گرفته‌اند.

[3] Malware

[4] Anti-Virus

[5] Anti-Spam

[6] Information Technology

شگفتی بر سازمان‌ها داشته است که تقریباً اجرای هر برنامه سازمانی بدون در نظر گرفتن فناوری اطلاعات سازمان غیرممکن می‌نماید (Leek, 2000: 86).

یک تهدید امنیتی شبکه تلاشی است برای نفوذ غیرقانونی در شبکه سازمانی، گرفتن اطلاعات بدون اطلاع یا اجرای سایر اقدامات مخرب. در صورت وجود ضعف یا آسیب‌پذیری در شبکه رایانه‌ای، امنیت شبکه در معرض خطر یا آسیب‌پذیری قرار می‌گیرد. آسیب‌پذیری‌های شبکه نقص‌ها یا ضعف‌های سخت‌افزاری، نرم‌افزاری یا سایر دارایی‌های سازمانی شناخته شده است که می‌تواند توسط مهاجمان مورد سوء استفاده قرار بگیرد. هنگامی که امنیت شبکه توسط یک تهدید به خطر بیفتد، می‌تواند به یک نقص شدید امنیتی منجر شود. بیشتر آسیب پذیری‌های امنیتی شبکه اغلب توسط مهاجمین رایانه‌ای مورد استفاده قرار می‌گیرند. هدف برخی تهدیدات امنیتی شبکه به جای جمع‌آوری بی‌صدای اطلاعات برای جاسوسی یا انگیزه های مالی، اختلال روند و عملکرد سازمان می‌باشد (عباس نژاد ورزی، ۱۳۸۹).

شبکه و استفاده از ابزارهای اطلاعاتی و ارتباطی آن، یکی از ضروریات مسلم امروز سازمان‌ها در عصر انفجار اطلاعات می‌باشد. اما منطق واقع‌گرایی اقتضا می‌کند که هرگز نباید تک بعدی به فناوری‌های مرتبط با آن پرداخت، بلکه بایستی تهدیدات و مخاطره‌های احتمالی آن را نیز شناسایی نمود. وضعیت امروز سازمان‌ها به‌گونه‌ای است که شبکه به صورت شمشیر دولبه‌ای برای آن‌ها عمل می‌کند؛ از یک سو فرصت‌های ارزشمندی را برای تسهیل در ارتباطات و انتقال سریع اطلاعات به وجود آورده و از سوی دیگر ساختارهای امنیتی را با تهدید مواجه ساخته است. سطوح تاثیرگذاری این تهدیدات در حوزه‌های امنیتی گاهی باعث رفتار حکومت‌ها و گاهی حتی تا آستانه فروپاشی دولت‌ها نیز رفته و در ابعاد کوچک‌تر آن موجب شکست در اهداف سازمانی و ماموریت‌های محوله سازمان گردیده است (گروسی و همکاران، ۱۳۹۴).

در سال‌های اخیر و با توجه به سایبر تروریسم بین‌المللی، چالش‌های امنیتی و اطلاعاتی گسترده‌ای در شبکه‌های سازمان‌های داخلی کشور از سوی عوامل بیگانه و بعضاً عناصر خود فروخته داخلی وارد آمده که برای مثال می‌توان به حملات وارده به تاسیسات هسته‌ای کشور از سوی بدافزار استاکس‌نت[1]، حملات سایبری به وزارت راه و شهرسازی و راه‌آهن ج. ا ایران، اختلال در سامانه‌های رایانه‌ای بندر شهید رجایی و دوربین‌های مدار بسته زندان اوین و همچنین از کار افتادن شبکه توزیع سوخت در کشور که منجر به خارج شدن پمپ بنزین‌ها در سطح کل کشور بود؛ اشاره نمود.

[1] Stuxnet

ستاد فرماندهی نیروی پدافند هوایی آجا به عنوان هسته مرکزی هدایت، فرماندهی، رهبری و کنترل نیروی پدافند هوایی ارتش ج. ا ایران از شبکه رایانه‌ای داخلی برخوردار است و دچار شدن به انواع مختلفی از این دست حملات برای این شبکه و زیرساخت‌های آن به دلیل شباهت همه شبکه‌های رایانه‌ای به یکدیگر امری اجتناب‌ناپذیر است.

اهمیت و ضرورت این پژوهش از آنجا نمود پیدا می‌کند که امنیت شبکه و به تبع آن شناسایی و تبیین تهدیدات مربوط به آن، به عنوان یک امر ضروری در سازمان‌ها و به طور خاص شبکه داخلی ستاد فرماندهی نیروی پدافند هوایی آجا می‌باشد که متضمن شناسایی، ارزیابی و طرح‌ریزی اقدامات پیشگیرانه به منظور جلوگیری از ورود غیرمجاز به شبکه رایانه‌ای می‌باشد. در این خصوص هم تکالیفی داریم که اگر به‌موقع و با کیفیت مطلوب به آنها نپردازیم:

- اخلال در شبکه رایانه‌ای ستاد فرماندهی نیروی پدافند هوایی آجا به عنوان مرکز فرماندهی و هدایت نیرو، فرایند ماموریت نیرو را با چالش عظیمی مواجه می‌سازد؛
- خسارات‌های زیان‌باری به مجموعه بدنه نیروهای مسلح وارد می‌گردد که بعضاً قابل جبران هم نیست.

هدف پژوهشگران از این پژوهش واکاوی تهدیدات امنیتی مؤثر بر شبکه رایانه‌ای داخلی سازمان‌ها با رویکرد آینده‌پژوهانه و به طور خاص ستاد فرماندهی نیروی پدافند هوایی آجا است و سؤال اصلی این است که تهدیدات امنیتی تأثیرگذار بر شبکه رایانه‌ای داخلی سازمان‌ها کدام اند؟

مبانی نظری و پیشینه‌های پژوهش

مبانی نظری پژوهش

آینده‌پژوهی[1]: پژوهشی است در حیطه واقعیت‌های انسانی – اجتماعی که هدف آن تدوین تجویزهایی است که عمل به آنها تحقق مطلوب‌ترین آینده ممکن را نوید می‌دهد (وند بل[2]، ۲۰۰۴).

تهدید[3]: نیات، قابلیت‌ها و اقدامات بالفعل و بالقوه دشمنان که موجودیت، اهداف و منافع، دستاوردها و در یک کلام کل مجموعه را به خطر اندازد و یا عامدانه در مسیر تحقق آن مانع فیزیکی و یا غیرفیزیکی جدی ایجاد نماید (احمدیان، ۱۳۹۴).

---

[1] Futuers Studies
[2] Wendell Bell
[3] Threats

امنیت: مجموعه تمام روش‌ها و فعالیت‌هایی می‌باشد کـه اطمینـان مـی‌دهـد حادثـه‌ای ناخوشایند هرگز روی نخواهد داد و یا احتمال پیشامد آن‌ها را کاهش می‌دهد و یا اجازه می دهد وقتی که حادثه‌ای خطرناک اتفاق افتاد، شرایط در سریع‌ترین زمان و با کمترین هزینـه به شکل عادی برگردد (بختیاری و همکاران، ۱۳۹۷).

تهدید امنیتی: هر عاملی که به طور بالقوه بتواند باعـث بـروز حادثـه‌ای خطرنـاک بشـود تهدید امنیتی گفته می‌شود. تهدیدهای امنیتی از عوامل زیر ناشی می‌شوند:

- تهدیدهای طبیعی: این تهدیدها ناشی از عواملی چون سیل، زلزله و... می‌باشد.
- تهدیدهای غیرامن: این تهدیدها از اشتباهات، خطاهای سهوی و ناخودآگاه انسانی نشئت می‌گیرند که می‌تواند باعث افشا و یا نابودی اطلاعات شوند.
- تهدیدات عمدی: به فعالیت‌های برنامه‌ریزی شده‌ای گفته می‌شود که سبب فاش‌شدن، نابودی و یا تغییر در داده‌های شبکه با ایجاد اختلال در خدمات سرویس‌دهنده می‌شوند (همان منبع، ۱۳۹۷).

ماهیت آینده‌پژوهی

ماهیت آینده‌پژوهی دانش تحلیل، طراحی و برپایی هوشمندانه‌ی آینده است (باباغیبی، ۱۳۸۹). مجموعه تلاش‌هایی است که با استفاده از تجزیه و تحلیل منابع، الگوها و عوامل تغییر و یا ثبات، به تجسم آینده‌های بالقوه و برنامه‌ریزی برای آنها می‌پردازند. آینده‌پژوهی منعکس می‌کند که چگونه از دل تغییـرات یا تغییر نکردن امروز واقعیت فردا متولد می‌شـود. مهمترین کارکرد آینـده‌پژوهی ایجاد تصویری از آینده برای بهبود بخشیدن به آن است (کورنیش، ۲۰۰۷) و به همگان اجازه می‌دهد تا بدانند که به کجاها می‌توانند بروند، به کجاها باید بروند و از چه مسیرهایی می‌توانند با سهولت بیشتری به آینده‌های مطلوب خود برسند.

در واقع آینده‌پژوهی یک ضرورت است، زیرا تجربه نشان داده موفقیت سازمان‌ها در گرو درک سریع متغیرهای محیطی و پیش‌بینی تهدیدات و فرصت‌ها و احراز آمادگی‌های لازم است. مضافاً که هدف آن، ادراک و غلبه بر نیروهای دراز مدت تغییر، به جهت ارائه تصویرهای بدیل و مطلوب از آینده به‌منظور حفظ و گسترش رفاه و آسایش بشر است (تقی‌نایبج، ۱۳۹۲).

حملات در شبکه‌های رایانه‌ای

حملات در یک شبکه رایانه‌ای حاصل پیوند سه عنصر مهم سرویس‌های فعال، پروتکل‌های استفاده شده و پورت‌های باز می‌باشد. یکی از مهم‌ترین وظایف کارشناسان فنآوری اطلاعات، اطیمنان از ایمن بودن شبکه و مقاوم بودن آن در مقابل حملات است (مسئولیتی بسیار خطیر و سنگین) (European Treaty Series - No. 185).

در خصوص ایمن‌سازی یک محیط شبکه، تدوین، پیاده‌سازی و رعایت یک سیاست امنیتی است که محور اصلی برنامه‌ریزی در خصوص ایمن‌سازی شبکه را شامل می‌شود (2014 ,Gercke).

شبکه داخلی نیروی پدافند هوایی آجا:

شبکه رایانه‌ای داخلی ستاد فرماندهی نیروی پدافند هوایی اجا با محوریت معاونت فاوا در سطح کلیه معاونت‌ها، فرماندهی‌های مستقل مستقر در ستاد فرماندهی، مدیریت‌ها و ریاست های تابعه گسترش یافته که وظیفه نصب، راه‌اندازی، پشتیبانی و ایمن‌سازی آن بر عهده معاونت پیش گفته می‌باشد (دستورالعمل نصب، راه‌اندازی، پشتیبانی و ایمن‌سازی شبکه، بازنگری سال ۱۳۹۹).

پیشینه‌های پژوهش

درک واقع‌بینانه از تهدیدات امنیتی در گرو توجه به عوامل نرم‌افزاری است که در واقع حلقه واسط بین محیط امنیتی کشورها و سخت‌افزارها قرار دارند و بدین جهت برداشت‌ها از مفهوم امنیت در این فضا به چالش کشیده شده است. به عقیده اکثر صاحب‌نظران، یکی از ضروری ترین و مهمترین سرمایه‌گذاری‌های توسعه شبکه‌ها و فناوری اطلاعات در هر کشور، طراحی و اجرای سامانه‌ها به‌طور کاملاً امن است که به‌عنوان یک سرمایه و اعتبار ملی به‌حساب می‌آید (مقدسی و همکاران، ۱۳۹۷).

امروزه شبکه‌های رایانه‌ای با ابعاد گسترده‌ای از تهدیدات سخت، نرم و نیمه سخت مواجه هستند که جنبه‌های نرم آن دارای ابعاد متعددی مثل جنجال‌سازی، ایجاد و گسترش تنش‌های اجتماعی متراکم، تضعیف سرمایه‌های اجتماعی، توانمندسازی جنبش‌های مدنی و سیاسی، تحریف یا جعل مفاهیم فرهنگی و تمدنی می‌باشد (نورمحمدی، ۱۳۹۰).

جهت بررسی پیشینه تحقیق و مطالعات گذشته، در بانک اطلاعات رساله‌ها و مطالعات گروهی دانشگاه عالی دفاع ملی، سامانه پژوهشگاه علوم و فناوری اطلاعات ایران، بانک اطلاعات پژوهشی نیروهای مسلح، سایر پایگاه‌های علمی داخلی و خارجی (Sience Direct, Ieee, Google Scholar) اقدام به جستجو در موضوعات مرتبط با عنوان پژوهش انجام گردید.

در میان مطالعات کتابخانه‌ای در پژوهش‌های انجام شده، پژوهشی که به‌طور مستقیم و کامل هم‌راستا با موضوع تحقیق حاضر باشد یافت نگردید ولیکن موضوعاتی که به‌نوعی در راستای تحقیق بوده و نتایج حاصله در پیشبرد این پژوهش مؤثر است به‌طور خلاصه در ادامه و در جدول شماره (۱) ارائه شده است.

جدول (۱) پیشینه تحقیقات انجام شده مرتبط با موضوع پژوهش

پژوهشگر	سال	نوع پژوهش	روش پژوهش	نتایج
Christos Douligeris Aikaterini Mitrokotsa	۲۰۰۳	مقاله	این مقاله با توسعه طبقه‌بندی حملات DDoS و مکانیزم‌های دفاعی DDoS، یک رویکرد ساختاری به مساله DDoS ارائه می‌کند.	مکانیزم‌های دفاعی را در یک طبقه‌بندی قرار داده تا درک بهتری از حملات DDoS حاصل شود و مکانیسم‌های دفاعی موثرتری را نسبت به آنها ابداع کنند.
Zhang Chao-yang	۲۰۱۱	مقاله	آنالیز حملات دیداس (DDoS) و تحلیل کامل از تکنیک‌های پیش گیری	معرفی سه روش جلوگیری از حملات دیداس (DDoS) به سه شامل استفاده از یک حمله داس روتر، افزایش ماژول پلت فرم مورد اعتماد و افزایش دفاع سامانه
علی وری‌نیا	۱۳۹۴	مقاله	بررسی تعاریف جرایم سایبری، جرایم سایبری در ایران، انواع طبقه‌بندی از جرایم سایبری برای تدوین قوانین مرتبط با آنها و تشریح بیشتر مصادیق جرایم سایبری	بهترین روش برخورد درست با مجرمان فضای سایبر در ایران وقتی قابلیت اجرا پیدا می‌کند که نقش مردم در آن به خوبی دیده شود و بتوان بخشی از آموزش درست استفاده کردن از فضای سایبر را به مردم واگذار کرد.
هادی غلامی	۱۳۹۵	مقاله	روش تحقیق موردنظر به صورت توصیفی تحلیلی	در این تحقیق ارتباط بین شاخص‌هایی چون اعلان‌های قرمز، مجرمان بین‌المللی، ناامن کردن جهان، بازگرداندن مجرمان و تشریفات گسترده بازگرداندن مجرمان میان کشورها مورد بررسی قرار می‌گیرد.
بهزاد بابایی	۱۳۹۷	مقاله	طرح دیدگاه‌های صاحب نظران حوزه فضای مجازی و شبکه‌های اجتماعی	بیان فرصت‌ها و تهدیدهای این حوزه در عصر کنونی و دغدغه‌های امنیتی ناشی از عضویت کارکنان ناجا در فضای مجازی و تهدیدها و آسیب‌هایی که کارکنان و در راس آن امنیت داخلی ناجا را تهدید می کند.

پس از جمع‌بندی پیشینه پژوهش مواردی در قالب نقاط اشتراک، نقاط افتراق و نقاط مغفول مانده در ادامه آمده است.

الف- نقاط اشتراک

• یکی از موضوعات مهم کاربردی در اغلب این منابع پرداختن به تهدیدات در حوزه خاصی است.

• تعدادی از منابع برای بیان جرایم سایبری و مفهوم تهدیدات سایبری هستند.

• در اکثر منابع به موضوع تهدیدات سایبری با رویکرد زیرساختی پرداخته شده است.

ب- نقاط افتراق

• برخی از این منابع تهدیدات سایبری را تهدیدات شبکه تلقی نموده‌اند.

• به علت تفاوت در منافع ملی کشورها، نگاه متفاوت به تهدیدات فضای مجازی و به ویژه تهدیدات شبکه وجود دارد.

پ- نقاط مغفول مانده

• به تهدیدات شبکه به مفهوم خاص آن در قالب کلیه تهدیدات پرداخته نشده است.

• شناسایی و ارزیابی تهدیدات شبکه در سازمان‌ها و به طور خاص برای سازمان‌های نیروهای مسلح ج. ا ایران پرداخته نشده است.

روش‌شناسی پژوهش

روش‌های مطالعه آینده عموماً برای کمک به درک بهتر آینده به منظور اتخاذ تصمیم‌های بهتر در زمان کنونی طراحی شده‌اند (منزوی بزرگی و همکاران، ۱۳۹۷). در واقع آینده‌پژوهی، اصول و روش مطالعه و سپس تصمیم‌گیری، طرح‌ریزی و اقدام در خصوص علوم و فناوری مرتبط با آینده است. آینده‌پژوهی، تفکرات فلسفی و روش‌های علمی و الگوهای مختلف بررسی و مطالعه آینده را مطرح و با استفاده از آن‌ها، آینده‌های بدیل و احتمالی را ترسیم می‌نماید. لذا، آینده پژوهی ابزاری برای معماری و مهندسی هوشمندانه آینده است (وقوفی و همکاران، ۱۳۹۶). با ظهور علم آینده‌نگاری و استفاده وسیع از قابلیت‌های آن، روش‌ها و فنون آینده‌نگاری وارد بطن برنامه‌ریزی شده است (مینائی و همکاران، ۱۳۹۵). آینده‌پژوهی حوزه‌ای فرا رشته‌ای است که در برگیرنده مجموعه تلاش‌هایی برای ارایه تصاویر و بدیل‌هایی از آینده است (یوسفی و همکاران، ۱۳۹۸).

نرم‌افزار MIC-MAC نخستین بار توسط موسسه Institut d'Innovation Informatique l'Entreprise pour در اندیشکده تحقیقاتی در زمینه راهبردی مربوط به آینده و سازمان، توسط میشل گودت در کشور فرانسه بوجود آمد. این رویکرد به عنوان یک تفکر تحلیلی است که از طریق سیستماتیک اقدام به ارائه راه‌حل‌های یک مسأله می‌پردازد (Fauzi, 2019). در این روش، تجزیه و تحلیل ساختار به عنوان یک واقعیت، تحت عنوان یک سامانه مورد مطالعه است

و عناصر این سامانه وابستگی تنگاتنگی با یکدیگر دارند (Mojica, 2005). در عین حال این روش به ملاحظه متغیرهای کیفی و کاوش آینده‌های چندگانه و نامعلوم می‌پردازد (Jiménez, 2009). به منظور تجزیه و تحلیل متغیرها و رابطه بین متغیرها به صورت مستقیم از طریق شناسایی تأثیر متغیرها بر یکدیگر توسط متخصصان و طبق نظر خبرگان استفاده می‌شود (Putra et al, 2020) که دارای سه مرحله اساسی است: شناسایی عناصر (متغیرها)، توضیح روابط بین متغیرها و آنالیز و شناسایی متغیرهای کلیدی (Wihaya et al, 2020).

مدل مفهومی پژوهش

گام‌هایی اجرایی این پژوهش در قالب مدل ارائه شده در شکل شماره (۱) نشان داده شده است.

شکل (۱) گام‌های اجرایی پژوهش

روش جمع‌آوری، ابزار اطلاعات و روش انتخاب جامعه نمونه

با توجه به ماهیت موضوع، تحقیق پیشرو از لحاظ هدف و نتیجه از نوع کاربردی-توسعه‌ای می‌باشد و از لحاظ ماهیت و روش تلفیقی از روش‌های توصیفی و موردی - زمینه‌ای می‌باشد. روش جمع‌آوری اطلاعات شامل مصاحبه با خبرگان و پرسشنامه و ابزار گردآوری اطلاعات، استفاده از اسناد و منابع کتابخانه‌ای شامل کتب، مجلات و مقالات پذیرفته شده در فصلنامه‌ها، همایش‌ها، کنفرانس‌های ملی و بین‌المللی می‌باشد.

گام‌هایی اجرایی این تحقیق همان‌گونه که در شکل شماره (۱) ارائه شده، به شرح زیر می‌باشد:

۱- در گام نخست با مطالعه اسناد و سوابق علمی پیشین صورت پذیرفته مرتبط سوابق پژوهشی انجام شده احصاء گردید.

۲- در گام دوم با استفاده از نظر خبرگان و کارشناسان دارای زمینه علمی دانشگاهی و سابقه کاری مرتبط با امنیت شبکه (شامل اساتید دانشگاه، مسئولین امنیت شبکه، پژوهشگران

و محققان شاغل در مراکز علمی و تحقیقاتی نیرو) تهدیداتی که امنیت یک شبکه رایانه‌ای را تحت تاثیر قرار می‌دهد، استخراج گردید. نفرات خبره و کارشناس با بهره‌گیری از روش نمونه گیری هدفمند انتخاب شدند. انجام مصاحبه با متخصصین رایانه و شبکه تا مرحله اشباع نظری داده‌ها صورت گرفت.

۳- در گام سوم با بهره‌گیری از چرخ آینده، پیامدهای رده یکم، رده دوم و رده سوم در قالب شکل شماره (۲) ارائه گردید.

شکل (۲) چرخ آینده معرف تهدیدات امنیتی حوزه شبکه

۴- در گام چهارم و با بهره‌گیری از چرخ آینده ترسیم شده، جلسات ذهن‌انگیزی برگزار و حلقه‌های مربوط تکمیل و مولفه‌های‌کلیدی تهدیدات امنیتی مرتبط در حوزه شبکه‌های رایانه ای شناسایی گردید.

۵- در گام پنجم مجدداً با تشکیل پانل خبرگی، تهدیدات مرتبط با همدیگر و اثرگذار، با یکدیگر ادغام و در ادامه با استفاده از پرسشنامه و استفاده از طیف لیکرت، عوامل مهم و اثرگذار رتبه‌بندی و تعیین اثر شدند. این پرسشنامه به‌صورت گزینه‌ها و انتخاب‌های چندگانه و به شیوه طیف لیکرت (کاملاً موافق، موافق، بی‌تفاوت، مخالف و کاملاً مخالف) طراحی و در اختیار کارشناسان و خبرگان مربوط قرار گرفت، تا توسط متخصصین و کارشناسان مورد نظر، اولویت‌بندی و میزان تاثیرگذاری تهدیدات مذکور شناسایی گردد.

۶- در انتها و در گام ششم با استفاده از نرم‌افزار آینده‌پژوهی Mic-Mac و به‌کارگیری روش تحلیل ماتریس متقاطع (رسم یک ماتریس n×n به تعداد تهدیدات)، بر اساس میزان تأثیرگذاری عوامل بر یکدیگر، تهدیداتی که از اولویت بالاتری برخوردار بودند، شناسایی گردید. البته این به آن معنی نیست که سایر تهدیدات دارای اهمیت نبوده و یا نیستند بلکه با توجه به نظر خبرگان حوزه تخصصی، این تهدیدات از درجه اهمیت بالاتری برخوردارند.

تجزیه و تحلیل

تعیین تهدیدات امنیتی مرتبط با شبکه‌های رایانه

در گام نخست تعداد **۷۸** تهدید امنیتی پیش روی شبکه‌های رایانه‌ای مطابق جدول (۲) شناسایی گردید.

جدول (۲) تهدید امنیتی پیش روی شبکه‌های رایانه‌ای

R	عنوان تهدید امنیتی	R	عنوان تهدید امنیتی
۱	عدم بهره‌گیری و استفاده از مکانیزم‌های دسترسی دیجیتالی جهت اتاق سرور	۲	حملات سرقت ارتباطی[۱] و Man In The Middle Attacks
۳	عدم کنترل صحیح تجهیزات سخت‌افزاری شبکه	۴	تزریق کدهای مخرب[۲]
۵	عدم محدودسازی دسترسی به تجهیزات شبکه با استفاده از قفل‌های دیجیتالی و ایمن	۶	عدم ارتقا به موقع پچ‌های امنیتی در سامانه عامل میزبان شما به منظور جلوگیری از حملات Dos

[۱] Session Hijacking

[۲] SQL Injection

R	عنوان تهدید امنیتی	R	عنوان تهدید امنیتی
۷	دسترسی افراد غیرمجاز به تجهیزات سرور شبکه	۸	بکارگیری انواع حملات روی رمزهای عبور[۱]
۹	عدم استفاده از دوربین‌های پایش درب ورودی محل های استقرار تجهیزات شبکه	۱۰	استفاده از حملات خارج از سرویس کردن یا عدم دسترسی توسط هکرها و افراد غیرمجاز
۱۱	عدم استفاده از سامانه مدار بسته کنترلی جهت کنترل اتاق‌های اتصالات و مراکز پایگاه داده	۱۲	حملات ضد امنیت منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه
۱۳	متمایز نبودن محل استقرار تجهیزات سرور شبکه	۱۴	حمله برای غیرفعال‌سازی کامل شبکه اجرایی
۱۵	عمل شنود بر روی کابل‌های شبکه	۱۶	حمله به قصد دستیابی به سطح کنترل
۱۷	چگونگی چینش و نوع منابع تغذیه شبکه	۱۸	حمله برای ایجاد نقص در سرویس دهی
۱۹	عدم طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه	۲۰	عدم نگهداری نسخ پشتیبان از پرونده‌های مختص پیکربندی
۲۱	عدم وجود منبع یا منابع تغذیه پشتیبان	۲۲	عدم استفاده از کانال رمز شده در حین ارتباط
۲۳	احتمال حریق در تجهیزات سرور شبکه	۲۴	عدم استفاده از کانال‌های VPN مبتنی بر IPsec
۲۵	به دست آوردن اطلاعات[۲] توسط افراد غیرمجاز	۲۶	شنود[۳] یا استراق سمع[۴] اطلاعات توسط نفرات غیر
۲۷	فعال نکردن سامانه رمزنگاری رموز بر روی مسیریاب یا دیگر سخت‌افزارهای مشابه	۲۸	نبود قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع حملات
۲۹	جعل[۵]	۳۰	عدم امکان بررسی ترافیک شبکه
۳۱	عدم وجود قابلیت تشخیص منبع حملات	۳۲	عدم توانایی تشخیص بسته‌های به قصد حمله
۳۳	حملات رمزنگاری اطلاعات[۶]	۳۴	نداشتن پیکربندی فایروال
۳۵	دسترسی افراد غیرمجاز به روزرسانی‌ها و نصب‌ها	۳۶	فعال نکردن قابلیت مشاهده کامل شبکه
۳۷	به‌کارگیری کدهای مخرب یا بدافزارها	۳۸	شناسایی سامانه عامل و فناوری‌ها[۷]
۳۹	حملات درب‌های پشتی[۸]	۴۰	حملات بالا بردن سطح دسترسی‌های معمول[۹]
۴۱	حملات دسترسی غیر مجاز[۱۰]	۴۲	حملات اجرای کدهای دلخواه[۱۱]

[1] Password Attacks
[2] Information Gathering
[3] Sniff
[4] Eavesdropping
[5] Spoofing
[6] Cryptography Attacks
[7] Target Foot printing
[8] Backdoor
[9] Privilege Escalation
[10] Unauthorized Access
[11] Arbitrary Code Execution

R	عنوان تهدید امنیتی	R	عنوان تهدید امنیتی
۴۳	حملات مربوط به اعتبارسنجی فیلدهای ورود اطلاعات[1]	۴۴	حملات احراز هویت و سطح دسترسی[2]
۴۵	حملات مدیریت پیکربندی[3]	۴۶	تهدیدات افشای اطلاعات[4]
۴۷	مشکلات و تهدیدات مدیریت ارتباطی	۴۸	تهدیدات مربوط به بافر کردن شبکه
۴۹	تهدیدات مربوط به مدیریت خطاهای سامانه و پیغام های خطای سامانه	۵۰	نداشتن سازوکارها و ابزارهای اساسی برای شناسایی و طبقه‌بندی تهدیدات امنیتی شبکه
۵۱	تهدیدات مربوط به ممیزی و لاگ‌برداری	۵۲	مسموم کردن[5]
۵۳	عدم نظارت بر بسته‌های ارسالی در شبکه به منظور حفاظت از ورود بسته‌های تقلبی	۵۴	نبود نرم‌افزارهای ضد آنتی ویروس بر روی رایانه های کلاینت‌ها
۵۵	بازبودن پورت‌های رایانه‌های متصل به شبکه	۵۶	عدم به کارگیری سیاست‌های امنیت فیزیکی
۵۷	مشخص نبودن یک شخص واحد جهت نصب برداشت و جابجایی مسیریاب‌ها	۵۸	عدم تعیین شخصی به عنوان مسئول صدور مجوز نگهداری و تغییر در سخت‌افزار و پیکربندی فیزیکی مسیریاب‌ها
۵۹	عدم معین شدن روش‌های دسترسی از راه دور	۶۰	عدم روند انجام تعمیرات فیزیکی مسیریاب‌ها
۶۱	تعریف نشدن سیاست‌های مربوط به رمزهای عبور مربوط به مدیران و سطوح امنیتی مختلف مسیریاب‌ها	۶۲	عدم کنترل بر روی دسترسی به درگاه‌های فیزیکی و کنترل‌های مربوط به مسیریاب‌ها
۶۳	عدم تعیین روش‌های مدیریت خودکار و ابزار کنترل مسیریاب‌ها و محدودیت‌های آنها	۶۴	عدم تعیین روش‌ها و تدوین راهنمایی‌های لازم برای کشف و مقابله با حملات
۶۵	عدم مشخص کردن پروتکل‌ها و پورت‌های نرم‌افزاری و سرویس‌هایی که اجازه عبور دارند	۶۶	عدم عدم به کارگیری استانداردهای موجود به منظور صحت‌سنجی امنیت نرم‌افزاری
۶۷	عدم شناسایی کاربران به صورت مجزا	۶۸	عدم تعیین پروتکل‌های مسیریابی
۶۹	عدم به‌کارگیری سامانه تشخیص هویت مبتنی بر شبکه	۷۰	نبود سامانه هویت سنجی برای پیشگیری از نفوذ در شبکه
۷۱	عدم امکان تشخیص بسته‌های خطرناک در داخل ترافیک معمولی شبکه	۷۲	عدم توانایی در جلوگیری کردن از تلاش‌های نفوذی برای ورود به ترافیک شبکه
۷۳	شکستن کلمات عبور به روش‌های علمی و غیرعلمی برای تشخیص هویت	۷۴	عدم توانایی تشخیص سامانه در فرار نفوذگر از سامانه تشخیص نفوذ
۷۵	عدم حفاظت داده‌های حساس در هنگام نقل و انتقال	۷۶	عدم تعیین اعتبار آدرس مدیران شبکه و منبع آنها
۷۷	پروتکل انتقال متن رمز شده ناامن	۷۸	استفاده نکردن از سامانه شناسایی نفوذ

[1] Data Input Validation
[2] Authentication and Authorization Attacks
[3] Configuration Management
[4] Information Disclosure
[5] ARP Poisoning

تجمیع و ادغام تهدیدات امنیتی شبکه

در ادامه و با بهره‌گیری از روش پنل خبرگی، از کارشناسان و خبرگان مربوطه خواسته شد از میان موارد تهدیدزای احصاء شده در مرحله اول، تعدادی از تهدیداتی که دارای اشتراک، شباهت و تجانس با هم‌دیگر هستند را شناسایی و معرفی نمایند. نتیجه این اقدام منجر به معرفی تعداد ۴۴ عامل تهدیدزا از میان تهدیدات اولیه گردید که در جدول شماره (۳) نشان داده شده است.

جدول (۳) شناسایی تهدیدات هم‌جنس و مشابه و ادغام آنها با یکدیگر

R	عنوان تهدید امنیتی	R	عنوان تهدید امنیتی
۱	دسترسی افراد غیر مجاز به تجهیزات سرور شبکه - حمله برای غیرفعال‌سازی کامل شبکه اجرایی - حمله به قصد دستیابی به سطح کنترل - حمله برای ایجاد نقص در سرویس‌دهی	۲	حملات سرقت ارتباطی و Man In The Middle Attacks - تزریق کدهای مخرب SQL – بهره‌گیری یا مسموم کردن ARP Cache
۳	عدم محدودسازی دسترسی به تجهیزات شبکه با استفاده از قفل‌های دیجیتالی و ایمن - عدم بهره‌گیری و استفاده از مکانیزم‌های دسترسی دیجیتالی جهت اتاق سرور	۴	نداشتن پیکربندی فایروال - عدم مشخص کردن پروتکل‌ها و پورت‌های نرم‌افزاری و سرویس‌هایی که اجازه عبور دارند - نبود نرم‌افزارهای ضد آنتی ویروس بر روی رایانه‌های کلاینت ها
۵	عدم استفاده از دوربین‌های پایش درب ورودی محل‌های استقرار تجهیزات شبکه - عدم استفاده از سامانه مدار بسته کنترلی جهت کنترل اتاق‌های اتصالات و مراکز پایگاه داده - فعال نکردن قابلیت مشاهده کامل شبکه	۶	چگونگی چینش و نوع منابع تغذیه شبکه - عدم طراحی صحیح منابع تغذیه در شبکه بر اساس محل استقرار تجهیزات شبکه - عدم وجود منبع یا منابع تغذیه پشتیبان
۷	استفاده از حملات خارج از سرویس کردن یا عدم دسترسی توسط هکرها و افراد غیرمجاز	۸	حملات ضد امنیت منطقی برای مسیریاب‌ها و دیگر تجهیزات فعال شبکه - عدم تعیین پروتکل‌های مسیریابی
۹	متمایز نبودن محل استقرار تجهیزات سرور شبکه - احتمال حریق در تجهیزات سرور شبکه	۱۰	عدم نگهداری نسخ پشتیبان از پرونده‌های مختص پیکربندی
۱۱	تهدیدات مربوط به ممیزی و لاگ‌برداری	۱۲	عدم استفاده از کانال‌های VPN مبتنی بر IPsec
۱۳	به دست آوردن اطلاعات توسط افراد غیرمجاز - شنود یا استراق سمع اطلاعات توسط نفرات غیرمجاز	۱۴	عدم وجود قابلیت تشخیص منبع حملات - نبود قابلیت بازداری از حمله و اعمال تدابیر صحیح برای دفع آنها
۱۵	فعال نکردن سامانه رمزنگاری رموز بر روی مسیریاب یا دیگر سخت‌افزارهای مشابه - نداشتن سازوکارها و ابزارهای اساسی برای شناسایی و طبقه‌بندی تهدیدات امنیتی شبکه	۱۶	عدم امکان بررسی ترافیک شبکه - عدم توانایی تشخیص بسته‌های به قصد حمله بر روی شبکه - تهدیدات مربوط به بافرشدن شبکه - عدم امکان تشخیص بسته‌های خطرناک در داخل ترافیک معمولی شبکه
۱۷	جعل	۱۸	بکارگیری انواع حملات روی رمزهای عبور
۱۹	دسترسی افراد غیرمجاز به روزرسانی‌ها و نصب‌ها	۲۰	شناسایی سامانه عامل و فناوری‌ها
۲۱	حملات اجرای کدهای دلخواه - بکارگیری کدهای مخرب یا بدافزارها	۲۲	مشکلات و تهدیدات مدیریت ارتباطی - عدم استفاده از کانال رمز شده در حین ارتباط

R	عنوان تهدید امنیتی	R	عنوان تهدید امنیتی
۲۳	حملات درب‌های پشتی	۲۴	حملات دسترسی غیر مجاز
۲۵	حملات بالابردن سطح دسترسی‌های معمول	۲۶	حملات مربوط به اعتبارسنجی فیلدهای ورود اطلاعات
۲۷	حملات مدیریت پیکربندی	۲۸	حملات احراز هویت و سطح دسترسی
۲۹	حملات رمزنگاری اطلاعات	۳۰	تهدیدات افشای اطلاعات
۳۱	عمل شنود بر روی کابل‌های شبکه و عدم کنترل صحیح تجهیزات سخت‌افزاری شبکه	۳۲	تهدیدات مربوط به مدیریت خطاهای سامانه و پیغام های خطای سامانه
۳۳	عدم نظارت بر بسته‌ها ارسالی در شبکه به منظور حفاظت از ورود بسته‌های تقلبی	۳۴	عدم ارتقا به موقع پچ‌های امنیتی در سامانه عامل میزبان شما به منظور جلوگیری از حملات Dos
۳۵	مشخص نبودن یک شخص واحد جهت نصب برداشت و جابجایی مسیریاب‌ها	۳۶	باز بودن پورت‌های رایانه‌های متصل به شبکه - عدم به کارگیری سیاست‌های امنیت فیزیکی - عدم حفاظت داده‌های حساس در هنگام نقل و انتقال الکترونیکی
۳۷	عدم کنترل بر روی دسترسی به درگاه‌های فیزیکی و کنترل‌های مربوط به مسیریاب‌ها - تعریف نشدن سیاست‌های مربوط به رمزهای عبور مربوط به مدیران و سطوح امنیتی مختلف مسیریاب‌ها	۳۸	عدم به کارگیری استانداردهای موجود به منظور صحت سنجی امنیت نرم افزاری - عدم توانایی در جلوگیری کردن از تلاش‌های نفوذی برای ورود به ترافیک شبکه - عدم تعیین اعتبار آدرس مدیران شبکه و منبع آنها
۳۹	عدم شناسایی کاربران به صورت مجزا	۴۰	عدم معین شدن روش‌های دسترسی از راه دور
۴۱	عدم به کارگیری سامانه تشخیص هویت مبتنی بر شبکه - شکستن کلمات عبور به روش‌های علمی و غیر علمی برای تشخیص هویت - نبود سامانه هویت‌سنجی برای پیشگیری از نفوذ در شبکه - عدم توانایی تشخیص سامانه در فرار نفوذگر از سامانه تشخیص نفوذ - استفاده نکردن از سامانه شناسایی نفوذ (IDS)	۴۲	عدم تعیین شخصی به عنوان مسئول جهت صدور مجوز نگهداری و تغییر در سخت‌افزار و پیکربندی فیزیکی مسیریاب‌ها - عدم روند انجام تعمیرات فیزیکی مسیریاب‌ها - عدم تعیین روش‌های مدیریت خودکار و ابزار کنترل مسیریاب‌ها و محدودیت‌های آنها
۴۳	پروتکل انتقال متن رمز شده نا ایمن	۴۴	عدم تعیین روش‌ها و تدوین راهنمایی‌های لازم برای کشف و مقابله با حملات

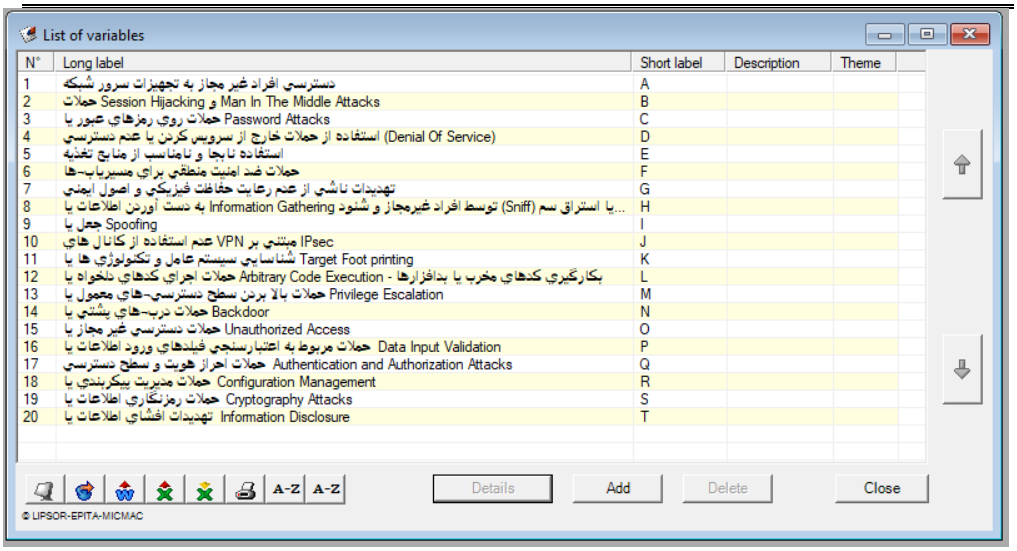
رتبه‌بندی و تعیین ارزش تهدیدات امنیتی

بعد از در ادامه پرسشنامه‌ای به منظور بررسی ارزش هر یک از ۴۴ تهدید امنیتی به دست آمده در مرحله پیشین تهیه و در اختیار کارشناسان و خبرگان مربوطه قرار گرفت و با استفاده از الگوی فریدمن و بر اساس معدل‌گیری یک تا پنج بر مبنای طیف لیکرت از میان ۴۴ تهدید امنیتی کلی آن دسته از تهدیداتی که نمره کمتر از میانگین را کسب نمودند به عنوان تهدیدات کم اهمیت حذف و تعداد ۲۰ عامل تهدیدزا که نمره بالاتر از میانگین را به خود اختصاص دادند جهت بررسی نهایی انتخاب گردید. تهدیدات احصا شده در نرم افزار **MIC-MAC** وارد گردید که برای وارد کردن آنها در نرم‌افزار ابتدا آنها را با یک نام اختصاری کدگذاری نمودیم و به

همین منظور مطابق جدول (۴) عناوین تخصیص داده شده به هر یک از تهدیدات را مشاهده می‌کنید که کدهای اختصاری معرفی آنها نیز تعریف شده است (شکل ۳).

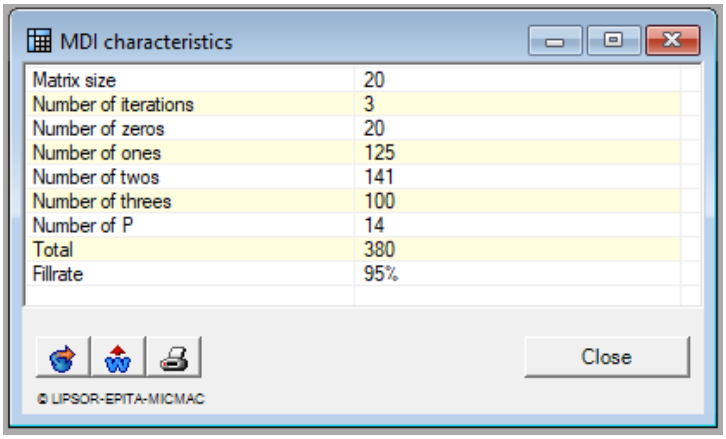
جدول (۴) کدگذاری تهدیدات امنیتی جهت ورود به نرم‌افزار MIC-MAC

R	Long Lable	Short Lable
۱	دسترسی افراد غیر مجاز به تجهیزات سرور شبکه	A
۲	حملات سرقت ارتباطی و Man In The Middle Attacks	B
۳	حملات روی رمزهای عبور	C
۴	استفاده از حملات خارج از سرویس کردن	D
۵	استفاده نابجا و نامناسب از منابع تغذیه	E
۶	حملات ضد امنیت منطقی برای مسیریاب‌ها	F
۷	تهدیدات ناشی از عدم رعایت حفاظت فیزیکی و اصول ایمنی	G
۸	به دست آوردن اطلاعات توسط افراد غیرمجاز و شنود	H
۹	جعل	I
۱۰	عدم استفاده از کانال‌های VPN مبتنی بر IPsec	J
۱۱	شناسایی سامانه عامل و فناوری‌ها	K
۱۲	حملات اجرای کدهای دلخواه - بکارگیری کدهای مخرب	L
۱۳	حملات بالا بردن سطح دسترسی‌های معمول	M
۱۴	حملات درب‌های پشتی	N
۱۵	حملات دسترسی غیرمجاز	O
۱۶	حملات مربوط به اعتبارسنجی فیلدهای ورود اطلاعات	P
۱۷	حملات احراز هویت و سطح دسترسی	Q
۱۸	حملات مدیریت پیکربندی	R
۱۹	حملات رمزنگاری اطلاعات	S
۲۰	تهدیدات افشای اطلاعات	T



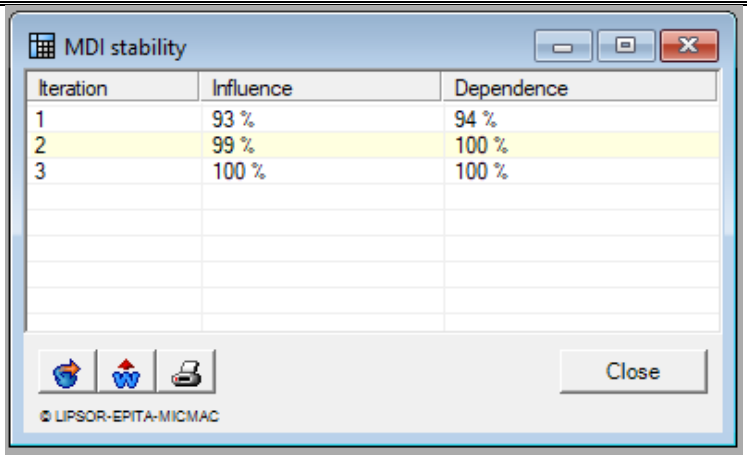
شکل (۳) تعداد ۲۰ تهدید احصاء شده با حروف اختصاری وارد شده در نرم‌افزار MIC-MAC

سپس در ادامه با تشکیل یک ماتریس ۲۰×۲۰ با کمک کارشناسان و خبرگان امتیازاتی در بازه ۰ تا ۳ به میزان اثرگذاری تهدیدات امنیتی بر یکدیگر داده شد. آمار داده‌های ورودی ماتریس به صورت شکل شماره (۳) می‌باشد. میزان پایایی ماتریس به تقریب ۹۵٪ است (شکل ۴). این رقم نشان‌دهنده تاثیرگذاری بالای تهدیدات می‌باشد.



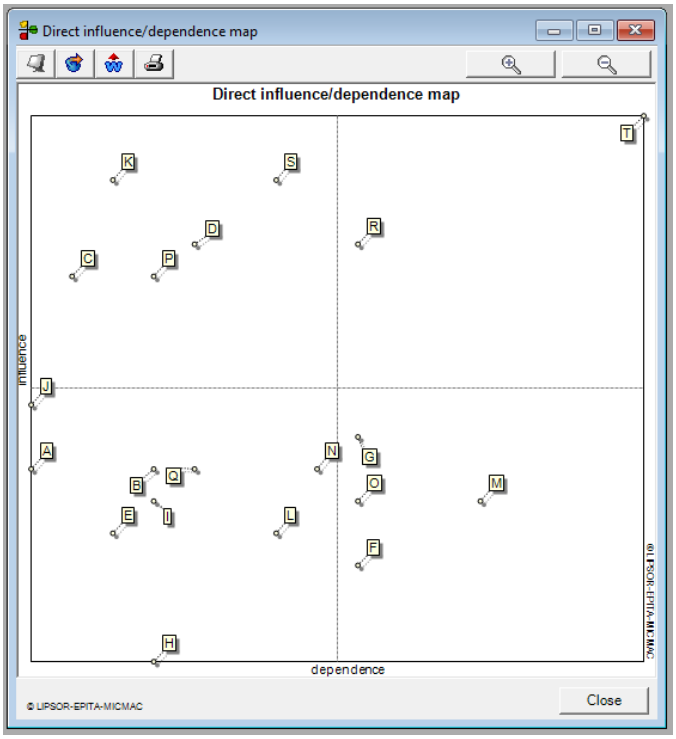
شکل (۴) آمار داده‌های ورودی ماتریس

مطابق شکل شماره ۵، محقق در نرم‌افزار با استفاده از شاخص‌های آماری اقدام به محاسبه پایداری نمود که با دوبار چرخش داده تاثیرات مستقیم از مطلوبیت و پایداری ۱۰۰٪ بهره‌مند هستند. این امر نشان‌دهنده روایی و پایایی بالای پرسشنامه و پاسخ‌های آن می‌باشد.



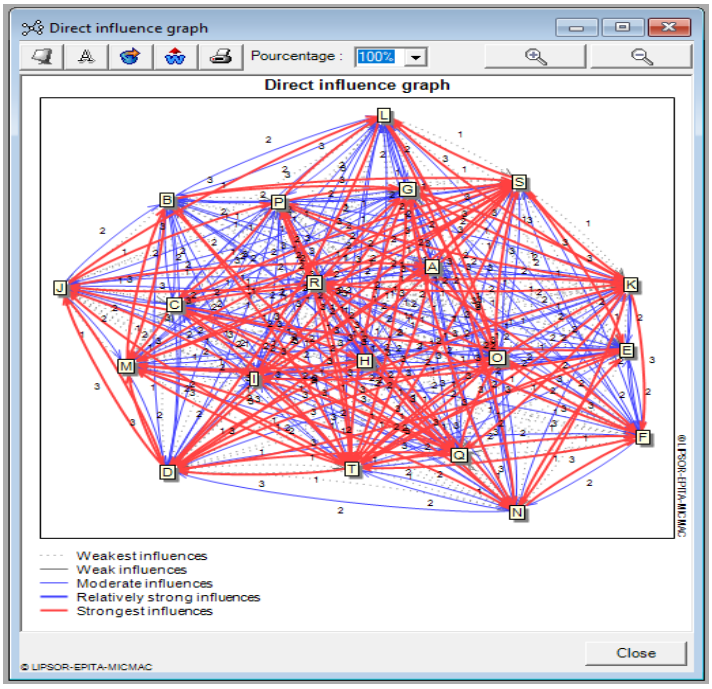
شکل (۵) پایایی حاصل تاثیر داده‌ها در ماتریس

نمودار اثرگذاری و اثرپذیری تهدیدات مطابق شکل (۶) می‌باشد. با توجه به تحلیل موجود از نمودار بالا و محل قرارگیری عوامل در آن، عوامل **R، H، K، O، T، I** و **A** به عنوان متغیرهای ریسک (تهدیدات اهم) ما شناخته شدند. به این معنی که با توجه به اهمیت این تهدیدات بایستی توجه بیشتری به آنها صورت پذیرد.

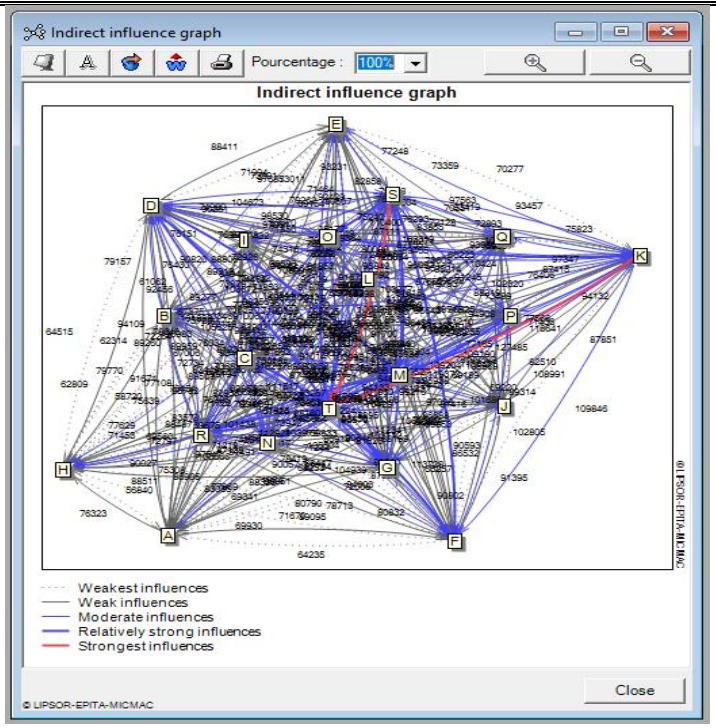


شکل (۶) نمودار اثرگذاری و اثرپذیری مستقیم عوامل بر یکدیگر

نمودارهای تأثیرات مستقیم و غیرمستقیم تهدیدات امنیتی مطابق شکل‌های (۷) و (۸) می باشد. نمودار اثرگذاری نشان‌دهنده روابط متغیرها و چگونگی اثرگذاری آنها بر همدیگر است. این نمودار در قالب خطوط قرمز آبی و نقطه چین ترسیم می‌شود. به این صورت که خطوط قرمز با مقدار عددی ۳ با توجه به شدت از اثرگذاری بیشتر ضخیم‌تر بوده و خطوط آبی با مقدار عددی ۲ با تفاوت در ضخامت روابط متوسط را نشان می‌دهد. خطوطی که به صورت نقطه چین نمایش داده شده است بیانگر وجود اثرگذاری ضعیف تهدیدات و یکدیگر است و با مقدار عددی یک مشخص شده است انتهای هر بردار بیانگر جهت اثرگذاری تهدید امنیتی است. تعداد بردارهایی که به یک تهدید وارد و یا از آن خارج می‌شوند، نشان‌دهنده میزان تاثیرپذیری و اثرگذاری آن می‌باشد و این تعداد هر چه بیشتر باشد میزان اهمیت آن به صورت مستقیم و غیرمستقیم بیشتر است. همانطور که در شکل‌های (۶) و (۷) مشاهده می‌کنید تاثیرگذاری و تاثیرپذیری عوامل **R، H، K، O، T، I** و **A** به صورت مستقیم و غیرمستقیم از سایر تهدیدات بیشتر است.



شکل (۷) نمودار تاثیرات مستقیم



شکل (۸) نمودار تاثیرات غیرمستقیم

نتیجه‌گیری

این پژوهش به منظور آینده‌پژوهی تهدیدات امنیتی شبکه‌های داخلی سازمان‌ها و به طور خاص شبکه رایانه‌ای موجود در ستاد نیروی پدافند هوایی آجا انجام گردید. اینکه در نهایت تعداد هفت عامل مهم تهدیدزا معرفی گردیده است به معنی آن نیست که سایر عوامل، تهدید به حساب نمی‌آیند و از کنار آنها بایستی بگذریم. این تهدیدات با اولویت و اهمیت بالاتری از سوی خبرگان و متخصصین حوزه شبکه و رایانه تشخیص داده شدند و ضروری است با توجه به آنچه عنوان شد زمینه‌های بروز و ظهور این ۷۸ تهدید در بستر شبکه‌های رایانه‌ای سازمان‌ها شناسایی و مرتفع گردد. از میان ۷۸ تهدید امنیتی شناسایی شده برای شبکه‌های رایانه‌ای که از اهمیت بالایی برخوردار بودند تعداد ۴۴ تهدید امنیتی نهایی به دست آمد و نتایج حاصل از خروجی نرم‌افزار MIC-MAC منجر به شناسایی تعداد ۲۰ عامل گردید که از این میان تعداد ۷ مورد زیر به عنوان تهدیدات کلیدی شناسایی گردیدند:

- دسترسی افراد غیرمجاز به تجهیزات سرور شبکه؛
- به دست آوردن اطلاعات توسط افراد غیرمجاز، شنود و استراق سمع؛
- جعل؛

- شناسایی سامانه عامل و فناوری‌ها؛
- حملات دسترسی غیرمجاز؛
- حملات مدیریت پیکربندی؛
- تهدیدات افشای اطلاعات.

با توجه به روند رو به رشد توانایی استفاده از فناوری اطلاعات و توسعه فناوری و رشد به کارگیری شبکه‌های باز مانند اینترنت و در عین حال چالش‌های پیش روی آنها، برای جلوگیری از نفوذ از طریق تجهیزات فیزیکی به شبکه‌های رایانه‌ای سازمان‌های نیروهای مسلح از جمله فرماندهی نیروی پدافند هوایی ارتش جمهوری اسلامی ایران، در کنار توجه به کلیه موارد امنیتی که بایستی در خصوص شبکه‌ها مدنظر قرار گیرد، اولین نکته‌ای که باید به آن توجه شود امنیت فیزیکی و رعایت اصول ایمنی آنهاست؛ چرا که با دسترسی فیزیکی و با داشتن یک رایانه همراه و یک کابل و مقداری دانش نفوذ به شبکه، افراد قادر خواهند بود با استفاده از روش‌های بازیابی رمز عبور کنترل کامل تجهیزات شبکه را مانند سوئیچ‌ها، روترها و مسیریاب‌ها را به دست بگیرد و کلیه این تهدیداتی که در موارد احصاء شده این پژوهش مطرح گردید، برای شبکه رخ بدهد.

پیشنهادات

امروزه فناوری اطلاعات بر شاهرگ حیاتی جریان اطلاعات خیمه زده و شاخه‌های خود را در تمامی ارکان سامانه‌های فرماندهی و کنترل اعم از نرم‌افزارها و سخت‌افزارها و بسترهای ارتباطی فرو برده، تابع تصمیم‌گیری‌های مسئول امنیتی و راه‌اندازی شبکه می‌باشند. به منظور حفظ، حراست، برقراری امنیت اطلاعات و داده‌های با ارزشی که از طریق تهدیدات احصاء شده ممکن است تجهیزات ارتباطی و شبکه را متوجه خود نماید، اقدامات زیر پیشنهاد می‌گردد:

- گزارش‌گیری مرتب از وضعیت تجهیزات شبکه، مسیریاب‌ها و تغییرات در پیکربندی آنها؛
- ایجاد آزمایشگاه جهت تست امنیتی تجهیزات شبکه؛
- استفاده از سوئیچ‌هایی با ساختار سلسله مراتبی؛
- کنترل دسترسی پورت‌های پیکربندی سوئیچ‌ها؛
- بکارگیری تجهیزات امنیتی مناسب در شبکه شامل مانیتورینگ فعالیت کاربران، فایروال‌های بومی و تایید شده؛
- نصب و راه‌اندازی نرم‌افزارهای تشخیص نفوذ به منظور شناسایی حملات شناخته شده؛

- آنالیز آماری ترافیک غیرنرمال کنترل و آنالیز فعالیت کاربران و رایانه‌ها و آنالیز ترافیک نرمال و ثبت رویدادها؛
- تهیه نسخه پشتیبان دوره‌ای و منظم از اطلاعات سرویس‌دهنده و سرویس‌گیرنده‌ها؛
- مدیریت آدرس‌های IP شبکه از طریق نصب دامین بر روی سامانه‌های شبکه؛
- اعمال سیاست‌گذاری مناسب در خصوص شرایط تعیین کلمه عبور کاربران و تعیین زمان‌بندی مناسب جهت تغییر آنها در فواصل زمانی منظم به صورت رمزهای حداقل با پیچیدگی متوسط به بالا.

قدردانی

از مشارکت و همراهی اساتید و خبرگان توانمندی که در مراحل مختلف این پژوهش، دانش خویش را سخاوت‌مندانه در اختیار محققان قرار دادند، تشکر و قدردانی می‌نماییم.

منابع

- احمدیان، علی اکبر. (۱۳۹۴)، تهدیدشناسی از منظر رهبر انقلاب اسلامی ایران، *مجله سیاست دفاعی*، ۲۳(۹۱)، ۳۹-۹.
- باباغیبی ازغندی، علیرضا. (۱۳۸۹)، آینده‌پژوهی رهیافتی نو در مدیریت جامع حمل و نقل شهری، *فصلنامه مدیریت ترافیک*، ۵(۱۶)، ۱۰۰-۷۷.
- بختیاری، حسین. و صالح‌نیا، علی. (۱۳۹۷)، اولویت‌بندی تهدیدات امنیت ملی جمهوری اسلامی ایران با روش تحلیل سلسله مراتبی، *فصلنامه مطالعات راهبردی سیاستگذاری عمومی*، ۸(۲۷)، ۲۵۵-۲۷۷.
- تقی‌نابیج، غلام‌حسین. و مؤمن‌زاده، محمدمهدی. (۱۳۹۲)، ارائه چهارچوب مفهومی تدوین چشم‌انداز، ارزیابی و گزارشگری سرمایه فکری در نظام بانکی، *فصلنامه تحقیقات حسابداری و حسابرسی*، ۵(۲۰)، ۲۵-۱.
- بیگدلی، حمید. و حمیدی، محمد علی. (۱۴۰۰)، ارزیابی خسارت در عملیات نظامی با استفاده از یادگیری عمیق و پردازش تصاویر، *مجله علمی – پژوهشی رایانش نرم و فناوری اطلاعات*، ۱۰(۳)، ۱۰-۱.
- دادی، زهره. و عنایتی، الهام. (۱۳۹۹)، مطالعه یک مدل انتشار بدافزار در شبکه‌های رایانه‌ای، *مجله علمی – پژوهشی رایانش نرم و فناوری اطلاعات*، ۹(۳)، ۱۵۰-۱۴۰.

- دستورالعمل نصب، راه‌اندازی، پشتیبانی و ایمن‌سازی شبکه نیروی پدافند هوایی ارتش ج. ا ایران، بازنگری سال ۱۳۹۹.
- رستمی، علی. (۱۳۹۴)، شیوه‌های مناسب مقابله اطلاعاتی اجا در برابر تهدیدات امنیتی فرامنطقه‌ای، *فصلنامه علوم و فنون نظامی*، ۱۱(۳۲)، ۷۹-۵۳.
- عباس نژاد ورزی، رمضان. و فرجی، آتنا. (۱۳۸۹)، *آشنایی با مبانی امنیت شبکه (امنیت اطلاعات)*، چاپ اول، بابل، انتشارات فناوری نوین.
- علی‌وری‌نیا، اکبر. و انواری، آمنه. (۱۳۹۴)، جرایم سایبری در ایران، مصادیق جرایم سایبری و راهکارهای مقابله با آن، *کنفرانس بین‌المللی علوم‌انسانی، روانشناسی و علوم اجتماعی*، ایران، تهران، مرکز همایش‌های بین المللی صدا و سیما.
- غلامی، هادی، (۱۳۹۵)، بررسی نقش پلیس بین‌الملل (اینترپل) در جرائم مجازی و رایانه‌ای (سایبری)، *فصلنامه علمی – تخصصی دانش انتظامی پلیس پایتخت*، ۹(۲۹)، ۸۱-۶۳.
- گروسی، اکرم. و گروسی، حسین. (۱۳۹۴)، بررسی جرم شناختی شبکه بر امنیت، پژوهشنامه نظم و امنیت انتظامی، ۸(۴)، ۵۴-۴۳.
- مقدسی لیچاهی، امیرحسین. و همت، حمید. (۱۳۹۷)، ارائه الگوی امنیت در فضای سایبر جمهوری اسلامی ایران با رویکرد آینده‌پژوهانه، *فصلنامه آینده‌پژوهی دفاعی*، ۳(۱۰)، ۱۲۰-۱۰۳.
- منزوی بزرگی، جواد. احمدی، صادق. و علیئی، محمدولی. (۱۳۹۷)، آینده‌پژوهی امنیت گذار و سیاست‌های جمعیتی ج. ا. ا و ارائه سناریوهای محتمل، *فصلنامه امنیت ملی*، ۸(۳۰)، ۹۵-۶۵.
- مینائی، حسین. حاجیانی، ابراهیم. دهقان، حسین. و جعفرزاده‌پور، فروزنده. (۱۳۹۵)، تعیین پیشران‌های‌اصلی دیپلماسی دفاعی ایران در سطوح منطقه‌ای و بین‌الملل، *فصلنامه آینده پژوهی دفاعی*، ۱(۱)، ۲۶-۷.
- نورمحمدی، مرتضی. (۱۳۹۰)؛ جنگ نرم، فضای سایبر و امنیت جمهوری اسلامی ایران، *فصلنامه راهبرد فرهنگ*، ۴(۱۶)، ۱۴۵-۱۲۷.
- وقوفی، امید. قاسمی، علی اصغر. و حاجیانی، ابراهیم، (۱۳۹۶)، تبیین عوامل و پیشران‌های کلیدی آینده یمن تا سال ۱۴۰۶، *فصلنامه آینده‌پژوهی‌دفاعی*، ۲(۴)، ۱۰۷-۸۷.
- وندل، بل. (۲۰۰۴)، *مبانی آینده پژوهی*، ترجمه تقوی، مصطفی. و محقق، محسن. چاپ چهارم، تهران، موسسه آموزشی و تحقیقاتی صنایع دفاعی.

- یوسفی، اشکان. کشاورز ترک، عین‌الله. و نهادی، هادی. (۱۳۹۸)، بررسی‌تأثیرمؤلفه‌های فرهنگی و اجتماعی دفاع مقدس بر آینده امنیت ملی ج. ا. ایران، *فصلنامه راهبرد دفاعی*، ۱۷(۶۶)، ۹۶-۶۹.

انگلیسی

- Andrew D. Murray (2007). *The Regulation of Cyberspace: Control in the Online Environment***,** Rout Ledge-Cavendish Publication.
- Cornish, E. (2007). *The Study of the Future: An Introduction to the Art and Science of Understanding and shaping tomorrow's World*. USA: World Future Society.
- *Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment* (2001/413/JHA).
- Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: a classification," *Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795)*, 2003, pp. 190-193, doi: 10. 1109/ISSPIT. 2003. 1341092.
- European Treaty Series, 2001, *Convention on Cybercrime*, Council of Europe - No. 185.
- Fauzi, A. (2019). *Teknik Analisis Keberlanjutan*. Gramedia Pustaka Utama.
- Jiménez, M. (2009). *Herramientas para el análisis prospectivo estratégico. Aplicaciones MICMAC [Tools for strategic prospective analysis*. Applications MICMAC]. Estado de México: Hersa Ediciones.
- Leek, Colin, 2000, "*Information Systems Frameworks for strategy", Industrial Management and Data Systems*, MCB University Press, Volume 97. Number3, PP. 86.
- Marco Gercke (2014*). Understanding Cybercrime: Phenomena, Challenges and Legal Responses*, ITU.
- Mojica, F. J. (2005). *La construcción Del futuro. Concepto y modelo de prospectiva estratégica, territorial y tecnológica*. Books, 1.
- Putra, G. B. B. Sudharma, I. W. P. A. , & Rahmadani, D. A. (2020). Key Variables on Property Marketing in Bali: Application of Micmac Method. *Asia*
  Pacific Journal of Management and Education, 3(1), 28-34.
- Sandelowski, M. Barroso, J. , & Voils, C. I. (2007). Using qualitative Meta summary to synthesize qualitative and quantitative descriptive findings. *Research in nursing & health*, 30(1), 99-111.
- Vega, R. I. (1996). De la anticipación a la acción: manual de prospectiva yestrategia. *Faces: revista de la Facultad de Ciencias Económicas y Sociales*, 2(3), 132-134.

- Wijaya, P, Kawiana, I. Suasih, N. , Hartati, P. , & Sumadi, N. (2020). SWOT and MICMAC analysis to determine the development strategy and sustainability of the Bongkasa Pertiwi Tourism Village, Bali Province, Indonesia. *Decision Science Letters*, 9(3), 439-452.
- Z. Chao-yang, "DOS Attack Analysis and Study of New Measures to Prevent," 2011 *International Conference on Intelligence Science and Information Engineering*, 2011, pp. 426-429, doi: 10. 1109/ISIE. 2011. 66.