الزامات پدافند غیرعامل در برابر تهدیدهای فضای سایبری با تأکید بر امنیت آجا[1]

مجید اصغرزاده[2]
عابدین سلمانی[3]

تاریخ دریافت: ۱۳۹۴/۰۲/۲۰ تاریخ تأیید: ۱۳۹۴/۰۳/۱۵

چکیده

با توجه به رشد چشمگیر فناوری اطلاعات و ارتباطات در قرن حاضر، لزوم توسعه و به‌کارگیری فناوری در سطح کشور و به‌ویژه در حوزه دفاعی به‌وضوح احساس می‌شود. از طرفی تهدیدهای این حوزه به‌صورت جنگ و حملات سایبری در صورت وقوع زیرساخت‌های حیاتی کشور را مورد هدف قرار خواهد داد مقاله حاضر باهدف شناخت الزامات پدافند غیرعامل در برابر حملات سایبری با تأکید بر امنیت ارتش جمهوری اسلامی ایران به رشته تحریر درآمده است. در این پژوهش از روش توصیفی – تحلیلی استفاده شده است. از دو روش کتابخانه‌ای و روش میدانی برای گردآوری اطلاعات استفاده گردیده است. نتایج تجزیه‌وتحلیل نشان داد که بومی‌سازی کلیه نیازمندی‌های سخت‌افزاری و نرم‌افزاری شبکه‌های رایانه‌ای، رعایت اصول پدافند غیرعامل و ایجاد یک‌لایه امنیتی در شبکه‌های رایانه‌ای، اقدامات پیشگیرانه مانند آموزش و اطلاع‌رسانی به کارکنان در سطح آجا از الزامات پدافند غیرعامل در مقابله با تهدیدهای فضای مجازی است.

واژگان کلیدی: *پدافند غیرعامل، تهدید، فضای مجازی (سایبری)، امنیت*

---

۱. ارتش جمهوری اسلامی ایران

۲. استادیار روانشناسی تربیتی دانشکده علوم و فنون فارابی (majid.shoaa@yahoo.com)
۳ . کارشناسی ارشدپدافند غیرعامل گرایش امنیت ملی دانشکده علوم و فنون فارابی، نویسنده مسئول(mkazmi5691@gmail.com)

مقدمه

استفاده از فناوری شبکه‌های رایانه‌ای برای افزایش کارایی و بهره‌وری مناسب در اغلب زمینه‌ها به‌سرعت در حال گسترش است. شبکه‌های گسترده‌ی رایانه‌ای با انواع روش‌ها و ابزارهای دستیابی به اطلاعات، قدرت و توانایی رایانه‌های موجود در شبکه را فارغ از مکان فیزیکی آن‌ها در دسترس استفاده‌کنندگان قرار داده است. اشتراک منابع سخت‌افزاری و نرم‌افزاری و دستیابی سریع و آسان به اطلاعات، از مهم‌ترین مزیت‌های شبکه‌های رایانه‌ای است. این ویژگی‌ها از راه‌کارهای مورد توجه نهادهای لشکری و کشوری، در اجرای وظایف محوله و ارائه خدمات است.

فضای سایبری (مجازی) یکی از ارکان اساسی جوامع امروزی به شمار می‌آید. چراکه عرضه بخش بزرگی از خدمات عمومی توسط حکومت‌ها به‌واسطه سهولت و سرعت انجام کار بر اساس امکانات گسترده فضای سایبری و فناوری اطلاعات است. هم‌چنین فضای مجازی باوجود آوردن فضای تبادل اطلاعات و یافته‌های علمی و فناورانه مقدمات را برای پیشرفت در تمامی کشورها و زمینه‌ها فراهم آورده است. همگام با بهره‌گیری از پیشرفت‌های فناوری اطلاعات نباید از آسیب‌های آن غافل بود.

چراکه مانند تمامی عرصه‌های جدید استفاده از این فناوری آسیب‌پذیری‌های نوینی را به‌همراه دارد و بهره‌گیری از این امکانات و آسیب‌پذیری‌ها بدون آگاهی نسبت به این وابستگی‌ها می‌تواند ضربه جبران‌ناپذیری را بر سامانه راهبردی مدیریت کشور وارد نماید. امنیت و دفاع سایبری یکی از مباحث جدید در عرصه خدمات‌رسانی عمومی و فناوری اطلاعات و ارتباطات است. این موضوع در بخش مدیریت کشوری در بسیاری از کشورهای جهان جایگاه و نقش ویژه ای دارد. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود، بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا در این فضا، واپایش، مدیریت و بهره‌برداری می‌شوند و

عمده اطلاعات حیاتی و حساس کشور نیز، به این فضا منتقل و یا به‌طور اساسی در این فضا، شکل‌گرفته است (جلالی فراهانی، ۱۳۹۱، ۱۱۲).

در سطح نیروهای مسلح به‌خصوص ارتش جمهوری اسلامی ایران بایستی درپی استفاده از اصول و روش های پدافند غیرعامل در حوزه اطلاعاتی و رایانه‌ای با هدف افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری شبکه و تسهیل مدیریت بحران در جنگ نرم بود. می‌توان چنین نتیجه گرفت که همهٔ سامانه‌های رایانه‌ای و اطلاعاتی خودکار و تجهیزاتی که در ارتباط باهم فرمانده را در طراحی، هدایت و واپایش نیروها در راستای وحدت تلاش‌ها، در عملیات پدافند غیرعامل یاری می‌دهد، ناشی از کاربرد فناوری. شبکه‌های رایانه‌ای است. برای اینکه فرماندهان بتوانند در عملیات پدافند غیرعامل در سطوح بالای فرماندهی و واپایش به‌طور موفق عمل نمایند، باید به‌نوعی به سامانه‌های رایانه‌ای متصل باشند که خاصیت پردازش انبوه داده را با سرعت و دقت بالا داشته باشند.

بیان مسئله

در عصر گسترش فناوری اطلاعات و ارتباطات، لازمه توسعه و پیشرفت همه‌جانبه، حفظ امکانات، منابع و زیرساخت‌ها در برابر تهدیدهای مختلف است. اگر امنیت در زمینه‌های مختلف ایجاد نشود، سرمایه‌گذاری، پرداختن به زیرساخت‌ها، توسعه تجهیزات و فناوری دست یافتنی نیست. با نیم‌نگاهی به راهبردهای دشمن و محیط پیرامونی و امکاناتی که دشمنان منطقه‌ای و فرا منطقه‌ای در اختیار دارند، می‌توان دریافت که همه کشورهای توسعه‌نیافته یا درحال توسعه و حتی پیشرفته به‌گونه‌ای نیازمند دفاع غیرعامل در برابر تهدیدهای هستند. با درک این موضوع و شناخت پدافند غیرعامل و عوامل و مؤلفه‌های تشکیل‌دهنده آن و هم‌چنین تأثیر آن بر امنیت کشور می‌توان راه‌کارهایی را جستجو کرد که به‌وسیله آن بتوان خسارت ها ، ضایعات و تلفات زیرساخت‌ها را کاهش داد (داودی دهاقانی، ۱۳۹۲: ۳۰).

به‌نظر می‌رسد با توجه به گسترش روزافزون تأثیر اقدامات پدافند غیرعامل در عرصه‌های گوناگون علمی و نظامی و با توجه به اینکه یکی از تدابیر کارساز در زمینه دفاع از زیرساخت-های ملی و سازمانی، بهره‌گیری از اقدامات پدافند غیرعامل است، لازم است نقش اقدامات پدافند غیرعامل در کاهش آسیب‌پذیری‌های شبکه‌های رایانه‌ای ارتش جمهوری اسلامی ایران به‌عنوان یکی از زیرساخت‌های مهم کشور، مورد بررسی کارشناسی قرارگرفته و راه کارهای مناسب برای حفظ امنیت و پایداری آن ارائه شود. ارتش جمهوری اسلامی ایران به‌دلیل گستردگی در سطح کشور اقدام به بهره‌برداری از شبکه‌های رایانه‌ای در یگان‌های مختلف در دورترین نقاط کشور نموده است. رشد و گسترش شبکه‌های رایانه‌ای به‌همراه آسیب‌پذیری‌های موجود می‌تواند پایداری و کارایی این زیرساخت حیاتی را در اجا با اختلال روبرو نماید. این پژوهش به‌دنبال ارائه راه‌کارهای افزایش امنیت و پایداری شبکه‌های رایانه‌ای آجا بر اساس اصول پدافند غیرعامل است. درنتیجه مسئله اصلی پژوهش حاضر این است که الزامات پدافند غیرعامل در برابر تهدیدهای فضای سایبری پیش روی شبکه‌های رایانه‌ای آجا کدامند؟

اهمیت و ضرورت

رشد روزافزون فناوری و نیاز به دسترسی هرچه سریع‌تر به اطلاعات، استفاده از فناوری‌های نوین همچون شبکه‌های رایانه‌ای را ناگزیر کرده است. بهره‌گیری از این فناوری، توأم با آسیب-پذیری‌های مخصوص به آن است. با این وضعیت هر سازمان بهره‌بردار از شبکه‌های رایانه‌ای ناگزیر است برای مقابله با تهدیدهای و آسیب‌پذیری‌های رایانه‌ای خود، راه‌کارها و اقدامات پیشگیرانه‌ای را برای ایمن‌سازی و پایداری آن‌ها انتخاب و اجرا نماید. اینجاست که پدافند غیرعامل در برابر تهدیدهای و در راستای کاهش آسیب‌پذیری و افزایش پایداری ضرورت پیدا می‌کند. درواقع می‌توان گفت که یکی از عوامل مهم در رسیدن به اقتدار و امنیت، حفظ و استمرار آن، میزان آگاهی، باور و بهره‌مندی و برخورداری عموم کارکنان نیروهای مسلح نسبت به ماهیت و کاربردهای مختلف پدافند غیرعامل در رویارویی با دشمن است؛ چراکه مشکل نا

آگاهی، از مشکلات خطرآفرین است که سبب تهاجم افکار دشمنان به حوزه اندیشه، باور و ایمان نیروهای مسلح می‌گردد. به‌عبارت‌دیگر هرچند، به‌کارگیری فناوری اطلاعات محاسن و برتری های زیادی دارد، ولی از آسیب‌پذیری زیادی هم برخوردار است، بنابراین اهمیت موضوع در این است که به‌کارگیری فناوری اطلاعات در ج.ا.ا عملاً در حوزه حریف صورت می‌گیرد و درنتیجه از آسیب‌های فراوان برخوردار خواهد بود و به‌منظور کاهش این آسیب‌ها باید راه‌کاری مناسب برگزید. پدافند غیرعامل یکی از این راه‌کارها است. به همین منظور در این پژوهش درپی تدوین و تهیه الزامات پدافند غیرعامل در برابر تهدیدهای سایبری با تأکید بر امنیت آجا هستیم تا بتوان با اجرای مفاد آن از مخاطرات و آسیب‌های فضای سایبر به طور جدی جلوگیری نمود.

ضرورت پژوهش برپایه تهدیدهای مختلف و گوناگون جمهوری اسلامی ایران از سوی دشمنان است. حوزه عملیاتی ما در برابر راهکنش‌های مختلف حریفان متأسفانه در ناحیه برتری آنان قرارگرفته است و برابر تجربه های گذشته و سوابق موجود (که تهدیدهای سایبری در رأس آن قرار دارند)، ازآنجایی‌که احتمال ادامه این برتری همچنان وجود دارد، بنابراین ضروری است راه‌کارهای نوین و مطمئنی در قالب الزامات پدافند غیرعامل در حوزه فناوری اطلاعات به‌منظور پایداری زیرساخت‌های حیاتی در برابر تهدیدهای سایبری تدوین و مورد بررسی قرار گیرد تا هم‌زمان با توسعه و رشد تهدیدهای سایبری روش‌های مقابله با آن نیز پویا و به‌روز گردد.

ضرورت دارد به‌منظور جلوگیری از نفوذ حریفان به شبکه‌های رایانه‌ای با به‌کارگیری الزاماتی همچون بومی‌سازی تجهیزات (نرم‌افزاری و سخت‌افزاری)، ایجاد بستر ارتباطی بومی، نوآوری در تولید تجهیزات، بالا بردن آگاهی تخصصی نیروی انسانی ، ایجاد مدیریت نظارت بر عملکرد، راه‌اندازی سامانه واپایش بومی، رعایت اخلاق اطلاعاتی در گفتگوها، سکوت رادیویی و استفاده مناسب و منطقی از بستر فضای سایبر و... در مقابله با تهدیدهای این فضا (با تأکید بر امنیت

شبکه رایانه‌ای) بررسی و مطالعه کارشناسانه ای انجام شود و راه‌کارهای مناسب برای حفظ امنیت و پایداری آن ارائه گردد. از طرفی بر اساس فرمان مقام معظم رهبری که همه وزارتخانه‌ها و سازمان‌ها را موظف می‌نماید که در اعتبارات عمرانی پروژه‌های حساس و مهم، اعتبار موردنیاز پدافند غیرعامل را منظور نمایند و هم‌چنین بند ۱۱ ماده ۱۲۱ قانون برنامه پنج‌ساله چهارم توسعه کشور و آئین‌نامه اجرایی این بند، موضوع پدافند غیرعامل از اساسی-ترین مباحث مورد توجه در امور دفاعی و برنامه‌ریزی قلمداد می‌شود.

با توجه به رویکرد جدید کشور در استفاده از اقدامات پدافند غیرعامل در طرح‌های کلان، می‌توان با بهره‌گیری از راه‌کارهای آن، در جهت حذف مخاطرات و کاهش آسیب‌پذیری‌های شبکه‌های رایانه‌ای اقدام نمود. هم‌چنین بهره‌برداری از نتایج این پژوهش و ملاحظات آن در طراحی و پیاده‌سازی شبکه‌های رایانه‌ای، منجر به پایداری و ایمنی هرچه بیشتر این زیرساخت مهم در ارتش جمهوری اسلامی ایران خواهد شد.

هدف، سؤال و فرضیه

هدف اصلی پژوهش «شناسایی الزامات پدافند غیرعامل در برابر تهدیدهای فضای سایبری با تأکید بر امنیت آجا» درنظر گرفته شده تا بتوان به یک رویکرد مناسبی در این زمینه رسید.

سؤال اصلی مقاله این است که الزامات پدافند غیرعامل در برابر تهدیدهای فضای سایبری با هدف افزایش بازدارندگی و کاهش آسیب‌پذیری در سطح آجا کدامند؟ و سعی گردید در طول پژوهش به آن پاسخ داده شود.

فرضیه اصلی مقاله هم عبارت است از: الزامات پدافند غیرعامل در برابر تهدیدهای فضای سایبری با تأکید بر امنیت آجا شامل اقداماتی مانند بومی‌سازی همهٔ نیازمندی‌های سخت‌افزاری و نرم‌افزاری شبکه‌های رایانه‌ای، رعایت اصول پدافند غیرعامل و ایجاد یک‌لایه امنیتی در شبکه‌های رایانه‌ای، اقدامات پیشگیرانه مانند آموزش و اطلاع‌رسانی به کارکنان در سطح آجا.

پیشینه

دربارۀ نقش پدافند غیرعامل در مقابله با تهدیدهای فضای سایبری در سازمان‌های نظامی و امنیتی مشابه، یا به‌طور مستقیم پژوهش انجام نشده و یا به‌دلیل طبقه‌بندی محرمانه و حیطه‌بندی اسناد و مدارک، دسترسی به این اسناد محدود شده است؛ ضمن این‌که در آجا نیز تاکنون دربارۀ نقش پدافند غیرعامل در مقابله با تهدیدهای فضای سایبری پژوهشی انجام نشده است. بااین‌حال بخش هایی از پژوهش های زیر که تا حدودی در ارتباط با موضوع پژوهش هستند در این قسمت به آن‌ها اشاره شده است.

در سال ۱۳۸۸ قیدی در پژوهشی با عنوان «بررسی آسیب‌پذیری‌های شبکه اطلاع‌رسانی ستاد نزا جا و ارائه یک الگوی مدیریت امنیت بهینه» آسیب‌های شبکه اطلاع‌رسانی ستاد نزاجا (نرم‌افزاری، سخت‌افزاری و کاربردی) و چگونگی رفع آسیب‌ها را بررسی کرده است.

در زمینه امنیت ارتباطات، در سال ۱۳۸۶ فولادفر پایان‌نامه کارشناسی ارشد خود را با عنوان «امنیت ارتباطات با رویکرد پدافند غیرعامل و ارائه راه‌کارهای عملی» تدوین نموده است.

پژوهش دیگری ازسوی کوهی در سال۱۳۹۰ با عنوان «الزامات پدافند غیرعامل در برابر تهدیدهای شبکه‌های اجتماعی مجازی» انجام شده است.

جدیدترین پژوهش ازسوی خوش عمل در سال ۱۳۹۱ با عنوان «الزامات، ملاحظات و راهبردهای پدافند غیرعامل در حوزه فناوری اطلاعات (به‌منظور پایداری زیرساخت‌های حیاتی در برابر تهدیدهای سایبری)» نگارش یافته است.

طی بررسی‌های انجام‌شده، در سازمان‌های نظامی و غیرنظامی کشور به شیوه‌های مختلفی سعی شده از اقدامات و اصول پدافند غیرعامل برای رویارویی با تهدیدهای فضای سایبری بهره‌گیری شود. در بعضی از سازمان‌ها با طراحی شبکه‌های رایانه‌ای به‌صورت چندلایه، اصل پراکندگی به‌خوبی رعایت شده است. برخی دیگر از سازمان‌ها که دسترسی و حفظ دائمی اطلاعات در کوتاه‌ترین زمان ممکن برای آن‌ها از اهمیت بالایی برخوردار است، با ایجاد

پراکندگی در محل مراکز داده خود، به وسیلهٔ نرم‌افزارها و سخت‌افزارهای مربوطه به‌صورت دائمی از اطلاعات خود پشتیبان تهیه می‌کنند.

مفاهیم و مبانی نظری

مفهوم سایبر[1]: سایبر در ابتدا در چارچوب‌ها و کارکردهای متفاوتی شکل گرفته است. هرچند مفهوم اصلی دفاع، جنگ و امنیت سایبری در ارتش آمریکا شکل گرفته است اما با گذشت زمان و به‌وجود آمدن تحولات و پیشرفت‌ها در مفاهیم و تعریف های سایبری جدای از کارکردهای نظامی که جزء کارکردهای اساسی و اصلی آن بوده است کارکردها و عملکردهای متفاوت و متنوعی بر آن افزوده شده است. توسعه مفاهیم و ابزارهای سایبری در زندگی روزمره مردم نیز خودنمایی می کند. این فضای جدید هم اکنون به یکی از عرصه‌های تقابل میان کشورها و قدرت‌های دنیا تبدیل شده است. امروزه که در حال تجربه نسل چهارم از جنگ‌های بشری هستیم؛ به‌صورت مشخص عوامل سایبری بر عوامل مؤثر بر پیروزی در میدان نبرد تأثیر گذاشته و باعث تعویض موقعیت‌های کلان و راهبردی در تقابل میان کشورهای مختلف می‌شود. این موضوع با واپایش و راهبری اطلاعات و ارتباطات صورت می‌گیرد که تأثیر آن بر شکست و یا پیروزی در میدان نبرد مشخص می‌شود. بسیاری از نبردهای پیشرفته و امروزی به‌طور اساسی و به‌صورت کامل در فضای سایبری شکل گرفته و به پایان می‌رسند (جلالی فراهانی، ۱۳۹۱: ۱۳۰).

فضای سایبر به فضای تبادل اطلاعات الکترونیکی گفته می‌شود و همهٔ شکل های تبادل اطلاعات الکترونیکی به‌صورت دیجیتال و شبکه‌ای را دربر می‌گیرد و این موضوع شامل مفاهیم و عملکردهایی که با شبکه‌های دیجیتالی هدایت می‌گردد نیز می‌شود. زیرساخت اصلی فضای سایبری، فناوری اطلاعات و ارتباطات است که در پنجاه سال گذشته پیشرفت زیادی کرده است؛ به‌ویژه در زمینه‌ای که مردم در سراسر جهان با یکدیگر و همچنین با محیط اطراف خود

1.syber

ارتباط برقرار می‌کنند. آنچه در دو دهۀ گذشته سرعت افزون‌تری داشته و پیشرفت فراوانی یافته است، رسیدگی به امور ضروری زندگی در فضای سایبر است؛ زمینه‌ای جدید که ارتباطات بین رایانه‌ای را آسان نموده است و امروزه از ضروریات پویایی جوامع پیشرفته در زمینه‌های بهداشتی، اقتصادی، اجتماعی، سیاسی و به‌ویژه نظامی به‌شمار می‌رود (واحدی، نصر اصفهانی، ۱۳۹۱: ۳).

مفهوم امنیت: براساس فرهنگ برخط وبستر[1] امنیت به مفهوم «آزادی از خطر، سلامت، آزادی از ترس یا اضطراب» تعریف شده است و اطلاعات به معنی «دانش به‌دست‌آمده از طریق پژوهش، مطالعه، آموزش، اطلاع، اخبار، حقایق، یک سیگنال یا کاراکتر (مانند سامانه‌های ارتباطی یا رایانه‌ای) ارائه داده شده، چیزی مانند عکس، فیلم و... که تغییر را در یک ساختار (مانند طرح و یا یک تئوری) بیان کند که و تجربه‌ای فیزیکی یا فکری را نشان می‌دهد » تعریف می‌شود (واحدی و نصر اصفهانی، ۱۳۹۱: ۳).

با کنار هم قرار دادن دو واژه امنیت و اطلاعات، واژه ترکیبی امنیت اطلاعات به‌دست می‌آید. اصطلاح امنیت اطلاعات به گام‌های جلوگیری کننده‌ای که برای محافظت از اطلاعات و قابلیت‌های آن برداشته می‌شود گفته می‌شود. به‌عبارت‌دیگر امنیت اطلاعات به مجموعه‌ای از تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی گفته می‌شود.

امنیت اطلاعات به حفاظت از اطلاعات و رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز به کمترین اندازه اشاره دارد. امنیت اطلاعات مجموعه‌ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی، خرابکاری و علم مطالعۀ روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز را شامل می‌شود. به‌منظور جلوگیری از سوءاستفاده و یا مخدوش‌سازی اطلاعات که از لحاظ امنیتی دارای اهمّیّت زیادی است، لازم

1. Webster

است سامانه‌های موجود با استفاده از فناوری امنیت اطلاعات به‌صورت امن در اختیار کاربران مجاز قرار داده شود.

امنیت یک فرایند است نه یک محصول و نمی‌توان تنها به یک نوع خاص از امنیت برای محافظت از اطلاعات خود بسنده کرد. همچنین برای محافظت از سامانه‌های رایانه‌ای و شبکه‌های رایانه‌ای نیز نمی‌توان فقط به یک محصول بسنده کرد. حقیقت این است که یک محصول نمی‌تواند امنیت کامل یک رایانه یا شبکه رایانه‌ای را فراهم نماید (میوالد، ۱۳۸۵: ۴۵-۴۶).

مفهوم امنیت در فضای سایبری: استفاده از فضای سایبری، زمانی می‌تواند یک سازمان یا کشور را پیشرو و کارآمد نماید که این فضا دارای امنیت مناسب باشد؛ بنابراین لازم است به مسئله امنیت در فرایند مدیریت امنیت زیرساخت‌های فضای سایبری ازجمله سامانه‌های فناوری اطلاعات و ارتباطات توجه شود (میوالد، ۱۳۸۵: ۴۵-۴۶).

اولین رسالت امنیت، حفاظت از سرمایه‌های یک سازمان است که شامل مؤلفه‌های قابل لمسی همچون صفحه وب یا بانک اطلاعات مشتریان یا مؤلفه‌های غیرقابل لمسی مانند شهرت و اعتبار یک سازمان می‌شود. امنیت یک مسیر است نه یک مقصد و به‌موازات تجزیه‌وتحلیل زیرساخت و برنامه‌های موجود، می‌بایست اقدام به شناسایی تهدیدهای و خطرات ناشی از آنان نمود.

درواقع برای ایجاد امنیت بایستی در سه بعد امنیت، مدیریت امنیت و شبکه رایانه‌ای امن در فضای سایبری اقدام شود که معنای هرکدام به‌شرح زیر است:

امنیت: حفاظت از سامانهٔ رایانه‌ای و داده‌های آن در برابر آسیب‌دیدگی و ازدست رفتن اطلاعات آن.

مدیریت امنیت: سلسله اعمالی که سیاست‌گذاری و به اجرا گذارده می‌شوند تا از صحت اطلاعات اطمینان یابیم. در یک تعریف ساده می‌توان گفت مدیریت امنیت برای اطمینان از این است که تمام کارهای امنیتی از طراحی تا اجرا به‌صورت مؤثر عمل کنند (میوالد، ۱۳۸۵: ۶).

شبکهٔ رایانه‌ای امن: شبکه‌ای است که تمامی عملیات آن همواره تحت تنظیمات و قواعد معینی اجرا گردد (همان: ۱۸۵-۱۸۶).

تهدیدهای سایبری: ازنظر مفهومی هر کنشی را دربر می‌گیرد که امنیت سایبری را از میان بردارد (عالی پور، ۱۳۹۰: ۹).

در جدول ۱ سطح‌بندی تهدیدها سایبری به‌صورت جداگانه تشریح شده است. ترکیبی از دو عامل پیشرفت فنّاوری و فعالان بدخواه، کار حفاظت از اطلاعات و فرآیندهای سایبری را پیچیده می‌سازد. سه نکته مشترک به این امر کمک می‌کند:

اول، جابه‌جایی ارزش‌ها؛ امروزه به‌طور فزاینده‌ای ارزش‌های مادی و معنوی در فضای سایبری دادوستد می‌شود و این امر خواه‌ناخواه توجه طمع‌کاران را به خود جلب می‌کند.

دوم، سامانه‌های باز؛ امروزه نیاز به دسترسی به فضای مجازی به‌طور فزاینده‌ای در حال گسترش است چه در بخش‌های دولتی و چه خصوصی و این توسعه بیشتر به وسیله همان دستگاه‌های قابل‌حملی انجام می‌گیرد که در زندگی روزمره استفاده می‌شود مانند تلفن همراه؛ چنین وسایلی درحالی‌که امکان ارتباط را افزایش می‌دهند، هم‌زمان انواع تهدیدهای امنیتی جدید را نیز دربر دارند؛ هنگامی‌که هکرها دستگاهی را رمزگشایی یا کرک می‌کنند، برای بدافزارها یک مسیر ورود آسان به‌کل شبکه ایجاد کرده‌اند.

سوم پیشرفت، توسعه و پیچیدگی فنّاورانه تهدیدهای؛ حمله و دفاع همیشه دوروی یک سکه بوده‌اند، اما اگر قدرت یکی بر دیگری افزونی یابد، سکه همیشه به همان رو فرود خواهد آمد. فعالیت‌های بدخواهانه روزبه‌روز در حال پیچیده‌تر شدن هستند. سازمان‌های حرفه‌ای جرائم رایانه‌ای، هکرهای سیاسی و گروه‌های تحت حمایت دولت‌های رقیب به لحاظ فنّاوری پیشرفته شده‌اند و در برخی موارد از مهارت‌ها و منابع گروه‌های امنیتی شرکت‌ها پیش افتاده‌اند. هکرها در ازای هر دستگاهی که به آن نفوذ کنند پول کلانی دریافت می‌کنند. در پنج سال گذشته

حملات هدفمند و پیچیده‌تر شده‌اند. امروزه ردیابی ویروس‌ها بسیار مشکل‌تر شده است، اغلب این ویروس‌ها اطلاعاتی را می‌دزدند که سود مالی داشته باشد.

جدول ۱: سطح‌بندی تهدیدهای سایبری

شاخص‌ها	تهدیدهای سایبری کلان	تهدیدهای سایبری خرد
عنوان تهدید	جنگ سایبری	جرم سایبری
عنوان مقابله	دفاع سایبری	امنیت سایبری
منشأ تهدید	یک حکومت، دولت یا گروه وابسته به یک دولت	یک گروه یا خرده هکر
سطح تهدید	به خطر افتادن یکی از مؤلفه‌های امنیت ملی کشور	به خطر افتادن مؤلفه‌های امنیتی کشور
پیامد تهدید	پیامد تهدید در سطح ملی یا منطقه‌ای است.	پیامد تهدید بیشتر امنیتی است.
هدف تهدید	زیرساخت‌های حیاتی و حساس و خیلی مهم کشور	شبکه‌های رایانه‌ای و زیرساخت‌های دارای اهمیت
منابع تهدید	خسارت‌های شدید اقتصادی، مالی، امنیتی و یا تلفات انسانی	خسارت مالی محدود و مشکل امنیتی
سلاح تهدید	استفاده از سلاح‌های پیچیده سایبری و جنگی	استفاده از ویروس‌های مرسوم و معمولی

(جلالی فراهانی، ۱۳۹۱: ۲۵۱)

پدافند در مترادف واژۀ دفاع است، دفاع نیز دو گونه است: دفاع عامل و دفاع غیرعامل.

دفاع عامل مبتنی بر فعالیت نیروهای مسلح و متکی بر تسلیحات و تجهیزات نظامی است، چنین دفاعی بر عهده نیروهای نظامی است. هرچند درصورتی‌که کشور در معرض تجاوزی قرار گیرد، مردم هم در قالب نیروهای بسیج می‌توانند به‌کمک نظامیان بیایند.

در کنار پدافند عامل، نوع دیگری از دفاع وجود دارد که به آن پدافند غیرعامل می‌گویند و به دفاعی گفته می‌شود که متکی به تجهیزات و تسلیحات نظامی نیست. پدافند غیرعامل مجموعه‌ای از برنامه‌ریزی‌ها، طراحی‌ها و اقدام ها است که باعث کاهش آسیب‌پذیری در برابر تهدیدهای دشمن می‌شود. از این مفهوم با عنوان «بازدارندگی» نیز یاد می‌شود. سیاست‌های اصلی پدافند غیرعامل مبتنی بر پایداری و حفظ امنیت است. در منابع لاتین، عبارت «passive defense» معادل دقیق عبارت پدافند غیرعامل به‌کاربرده می‌شود (احسانی، ۱۳۸۸: ۳۶).

ویژگی‌های فضای سایبر

۱- جهانی و فرا مرزی بودن؛ در محیط اینترنت، امکان تولید جهانی فراهم است.

۲- امکان ارتباط دوطرفه به‌صورت آسان؛ این محیط امکان‌های ویژه ارتباط سریع و آسان کاربران، میزبان ها و مدیریت‌کنندگان را امکان‌پذیر می‌سازد. این ویژگی در انواع دیگر رسانه‌ها با محدودیت‌ها و مشکلات خاصی روبروست.

۳- جذابیت و تنوع؛ مشتری‌مداری در تنوع و جذابیت این محیط تأثیر به‌سزایی دارد.

۴- مخاطب خاص و تأثیرگذار؛ این فضا نوعی مرجعیت فکری- سیاسی را برای کاربران ایجاد می‌نماید.

۵- امکان عبور و پایبند نبودن به بخش مهمی از قوانین و محدودیت‌های موجود در سایر رسانه‌ها؛ این امر به‌ویژه در محیط غیررسمی بیشتر رایج است.

۶- تجهیزات ارزان و دردسترس؛ سادگی دسترسی به ابزارهای حمله و جاسوسی و ناچیز بودن هزینه آن‌ها نسبت به جنگ‌افزارهای نظامی، به سازمان‌های تروریستی این امکان را می دهد که با استفاده از تجهیزات پیچیده، پیشرفته و به‌روز سایبری و با ارتباطات پنهان به زیرساخت‌های هدف حمله و به اهداف خود دست یابند (جیستان، ۱۳۹۰: ۴).

زیرساخت‌های شبکه‌های ارتباطی

مفهوم زیرساخت: برای واژه زیرساخت تعریف های گوناگونی وجود دارد. لغت نامه وبستر، این واژه را چنین تعریف می‌کند: «سامانه‌ای از تأسیسات عمومی یک کشور، ایالت یا منطقه» و نیز «شالوده اساسی و چهارچوب بنیادی یک سامانه یا سازمان». هیئت حفاظت از زیرساخت‌های بحرانی آمریکا زیرساخت را چنین تعریف می‌کند: شبکه‌ای از سامانه‌ها و فرآیندهای مستقل، بیشتر در مالکیت بخش خصوصی و ساخته دست بشر که به‌صورت مشارکتی برای تولید و توزیع جریان پیوسته‌ای از کالاها و خدمات ضروری عمل می‌کنند (شهبازی و همکاران، ۱۳۹۰: ۱۰). سازمان پدافند غیرعامل زیرساخت‌های کشور را براساس سه دسته نیازهای درجه یک، دو و سه کشور تقسیم‌بندی کرده است که عبارت‌اند از زیرساخت‌های حیاتی، حساس و مهم.

منظور از زیرساخت‌های حیاتی، زیرساخت‌هایی است که اگر با تهدیدی روبرو شوند کشور دچار مخاطره‌ای جدی خواهد شد. زیرساخت‌های حساس بدین معناست که بروز تهدید برای آن‌ها موجب می‌شود بخشی از کشور با خطر روبرو شود؛ و زیرساخت‌های مهم به معنای تهدیدهای نقطه‌ای و منطقه‌ای است (جلالی، ۱۳۸۹: ۱۸۹).

هدف های کلان پدافند غیرعامل در خصوص زیرساخت‌ها

- در بند یکم هدف‌های عالی پدافند غیرعامل کشور، بر جلوگیری از آسیب‌پذیری زیرساخت‌های حیاتی و کاهش آسیب‌پذیری زیرساخت‌های حساس و مهم کشور در برابر تهدیدهای دشمن تأکید شده است.

●در بند پنجم آن، کاهش آسیب‌پذیری زیرساخت‌ها در ارتباط با تهدیدهای نرم با تأکید بر سایبر و فضای مجازی، رایانه ، تجارت الکترونیک و... آمده است.

●در بند نهم آن، بر دست‌یابی به پایداری امنیت کشور و ایمن‌سازی زیرساخت‌ها در برابر تهدیدهای نرم با استفاده از رویکرد پدافند غیرعامل نرم تأکید شده است (جلالی و همکاران، ۱۳۸۹: ۳۴).

الزامات فضای سایبر در زیرساخت‌های حیاتی

●حفظ اسرار و اطلاعات کشور از دسترسی دشمنان به اطلاعات ارزشمند ملی و حیاتی، حساس و مهم کشور (نظامی و غیرنظامی) از سه جنبه مختلف محرمانگی، یکپارچگی و دسترس‌پذیری.

●ایمن‌سازی زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم با توجه به اهمیت تأسیسات، مرکز یا تشکیلات داده‌ها، مکان‌یابی و به‌کارگیری استانداردهای مرتبط و...

●پایدارسازی زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم با بومی‌سازی تجهیزات سخت و نرم‌افزاری و کاهش وابستگی‌های فناورانه، خدمات و پشتیبانی خارجی، به‌کارگیری روش‌ها و تأمین با موازی‌سازی (خوش عمل، ۱۳۹۱: ۷۷).

برخی از سیاست‌های کلی نظام در حوزه پدافند غیرعامل و دفاع سایبری

۱. تأکید بر پدافند غیرعامل که عبارت است از مجموعه اقدام های غیرمسلحانه ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، افزایش پایداری ملی و تسهیل مدیریت بحران در برابر تهدیدهای و اقدام های نظامی دشمن می‌گردد.

۲. طبقه‌بندی مراکز، اماکن و تأسیسات دارای اهمیت به حیاتی، حساس و مهم و تجدیدنظر در این طبقه‌بندی در صورت نیاز.

۳. تهیه طرح جامع پدافند غیرعامل در برابر سلاح‌های غیرمتعارف مانند هسته‌ای، میکروبی و شیمیایی.

۴. فرهنگ‌سازی و آموزش عمومی درزمینه به‌کارگیری اصول و ضوابط پدافند غیرعامل در بخش دولتی و غیردولتی، پیش‌بینی آموزش‌های متناسب در سطح عمومی و عالی و گسترش پژوهش ها درزمینه پدافند غیرعامل.

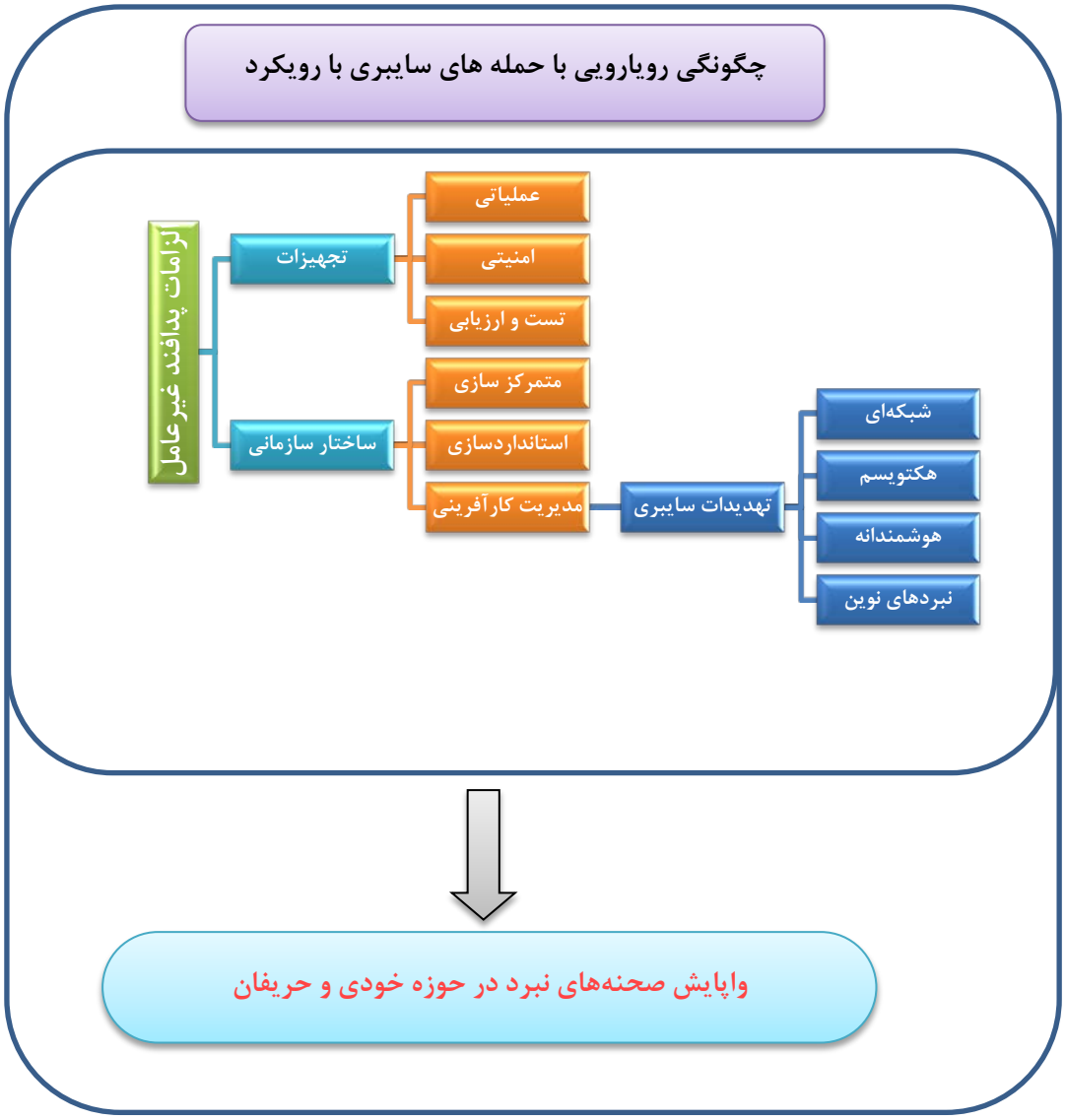
۵. حمایت لازم از گسترش فناوری و صنایع مرتبط با پدافند غیرعامل با تأکید بر طراحی و تولید داخلی.

۶. اصول و ضوابط رویارویی با تهدیدهای نرم‌افزاری و الکترونیکی و سایر تهدیدهای جدید دشمن به‌منظور حفظ و پاسداری شبکه‌های اطلاع‌رسانی، مخابراتی و رایانه‌ای (اسناد بالادستی مرتبط با پدافند غیرعامل، سایت پایداری ملی).

آنچه روشن و مشخص است این است که پایه و اساس فضای سایبر، اصول و پایه‌های علم فناوری اطلاعات است؛ بنابراین در هر مبحثی که موضوع تهدیدهای سایبری مطرح است پایه و اساس آن فناوری اطلاعات است؛ وجود مباحث فناوری اطلاعات در پدافند غیرعامل و توجه به مؤلفه‌های آن، تأثیر شگرفی در رویارویی با تهدیدهای سایبری دارد. در هر کجای پدافند، آن هم از نوع غیرعامل آن که مباحث فناوری اطلاعات پایه و اثرگذار است، به‌شدت بحث تهدید سایبری را افزایش می‌دهد. در نتیجه اینکه، برای رویارویی با تهدیدهای سایبری در موضوع پدافند غیرعامل باید ابتدا خوب فناوری اطلاعات را شناخت، فنون و فناوری‌های این عرصه را بسیار مسلط شد و با توجه به نیاز خود، آن‌ها را بومی ساخت تا در جبهه پدافند غیرعامل با بهره‌گیری از آن بتوان تهدیدهای سایبری را شناخته و آثار آن را به کمترین حد رساند و یا حتی به فرصت تبدیل نمود (الوندی: ۱۳۹۲، ۱۴۱).

با توجه به گسترش روزافزون فناوری اطلاعات و وابستگی رو به رشد زیرساخت‌های خدماتی کشور به سامانه‌های نرم‌افزاری، سخت‌افزاری و ارتباطات دیجیتال در بخش‌های صنعتی، بانکداری، آب، برق، گاز و همچنین گسترش زیاد استفاده از سامانه‌های دیجیتالی در صنایع و ابزارهای نظامی و دفاعی، تأثیر فناوری اطلاعات در پدافند غیرعامل در برابر تهدیدهای سایبری بسیار زیاد به‌نظر می‌رسد (الوندی،۱۳۹۲: ۱۴۵).

شکل ۱ - الگوی مفهومی پژوهش



با توجه به نتایج بدست آمده از ادبیات پژوهش و نظرهای جامعه آماری و خبرگان الگوی مفهومی بالا تبیین شده است.

نوع و روش پژوهش، ویژگی‌های جامعه آماری و تجزیه و تحلیل داده‌ها

این پژوهش از نوع کاربردی است و از روش توصیفی – استنباطی در آن استفاده شده است. به‌این‌ترتیب که با جمع‌آوری اطلاعات به روش کتابخانه‌ای و میدانی تأثیر مؤلفه‌های متغیر مستقل (اثرگذار) بر متغیر تابع (وابسته) مورد شناسایی شد و با انتخاب نمونه آماری از بین خبرگان و صاحب‌نظران با طراحی سؤال‌های مناسب از اطلاعاتی که به‌دست آمد پرسشنامه پژوهش تهیه و با در نظر گرفتن سؤال‌های اصلی و فرعی و فرضیه‌های پژوهش دسته‌بندی شد. سپس برای روایی پرسشنامه به تأیید پنج نفر از متخصصان حوزه شبکه‌های رایانه‌ای رسید. پایان با توجه به نظرهای کارشناسان سؤال های تکمیلی تهیه و در اختیار خبرگان قرار گرفت با دریافت پاسخ خبرگان و پس از انجام محاسبات آماری (توصیفی و استنباطی)، پاسخ‌ها با به‌کارگیری آزمون آماره استنباطی با بهره‌برداری از نرم‌افزار SPSS و EXCEL تجزیه‌وتحلیل شد، پاسخ سؤال ها بدست آمد و فرضیه‌های پژوهش مورد تأیید قرار گرفت. به‌منظور اولویت‌بندی متغیرها و شناسایی متغیرهای مهم تر و تأثیرگذارتر از آزمون فریدمن استفاده شد. جامعه آمار در این پژوهش عبارت اند از تعداد ۱۵۰ نفر از مدیران فنی قسمت‌های مختلف نیروهای آجا، مدیران و کارشناسان فنی حفاظتی، استادان و دانشجویان کارشناسی ارشد پدافند غیرعامل دانشکده علوم و فنون فارابی در دو سال اخیر.

تعیین جامعه نمونه و حجم نمونه آماری با استفاده از روش تعیین حجم نمونه کوکران ۷۴ نفر تعیین شد.

برای اجرای پژوهش از دو روش کتابخانه‌ای (اسنادی) و میدانی (استفاده از نظرسنجی) برای گردآوری اطلاعات استفاده شده است که. با استفاده از روش کتابخانه ای از همه متون و ادبیات مکتوب به‌منظور غنی‌سازی و استفاده از مطالب در بخش ادبیات نظری و پیشینه پژوهشی استفاده شد. با استفاده از روش میدانی نیز به‌منظور استفاده از دیدگاه صاحب‌نظران در بخش ادبیات و نیز تهیه گویه‌های پرسشنامه و نیز استفاده از تجارب آنان در بخش پیشنهادهای اجرایی بهره‌برداری شد. ابزار گردآوری استفاده شده در پژوهش حاضر را یک

پرسشنامه ۲۴ سؤالی محقق ساخته تشکیل می‌دهد که در طیف لیکرت پنج گزینه‌ای (خیلی زیاد، زیاد، متوسط، کم و خیلی کم) طراحی شده است.

در این مقاله از روش روایی محتوایی برای بررسی روایی استفاده شد؛ به این صورت که پس از مطالعه و تدبر در ادبیات پژوهشی و مشورت با استادان و کارشناسان خبره و طی مراحل روان‌سنجی ابزار از آنان در مورد محتوای گویه‌ها درراستای سنجش هدف پرسشنامه سؤال شد و آنان محتوای گویه‌ها را در ارتباط با هدف ابزار تشخیص دادند. از روش آلفای کرونباخ برای سنجش پایایی پرسشنامه استفاده شد و میزان آلفای محاسبه شده (۰/۷۴) نشان داد که پرسشنامه از اعتبار قابل قبولی برخوردار است.

پس از جمع‌آوری اطلاعات به وسیلهٔ منابع، اسناد و مدارک، پرسشنامه‌هایی بین جامعه نمونه پخش شد و شاخص‌های معینی دسترسی به‌دست آمد. سپس به‌کمک جدول ها و نمودارهای متناسب و همچنین با استفاده از روش‌های تجزیه‌وتحلیل آمار و شاخص‌های مختلف (مرکزی، پراکندگی و...) نسبت به تجزیه‌وتحلیل اطلاعات و داده‌های جمع‌آوری‌شده اقدام و پایان برای تأیید مراحل تجزیه‌وتحلیل توصیفی اطلاعات فرض‌ها با استفاده از آمار استنباطی (با آزمون آماری خی دو) آزموده شده است.

آزمون فرضیه: الزامات پدافند غیرعامل در برابر تهدیدهای فضای سایبری با تأکید بر امنیت شبکه‌های رایانه‌ای آجا شامل اقداماتی همچون بومی‌سازی همهٔ نیازمندی‌های سخت‌افزاری و نرم‌افزاری شبکه‌های رایانه‌ای، رعایت اصول پدافند غیرعامل و ایجاد یک‌لایه امنیتی در شبکه‌های رایانه‌ای و اقدام های پیشگیرانه مانند آموزش و اطلاع‌رسانی به کارکنان ارزیابی شد و با به دست آوردن اطلاعات عددی مربوط به همهٔ سؤال‌های فرضیه مشخص شد که گزینه‌های خیلی زیاد و زیاد به‌ترتیب با میانگین ۴۳ و ۲۵ بیشترین سهم را در تاثیرگذاری به خود اختصاص داده‌اند. مقدارهای مربوط به درصدها نیز نشان می دهد که درمجموع همهٔ سؤال‌های این فرضیه در حدود ۹۱/۸۸ درصد پاسخ‌دهندگان در حد زیاد و خیلی زیاد پاسخ داده‌اند. همچنین داده‌های جدول ۲ حاکی از آن است که ارزش خی‌دوی مشاهده‌شده (۶۱/۱۳) از ارزش خی‌دوی بحرانی (۱۱/۳۴) در سطح $P<۰/۰۱$ بزرگ‌تر است، درنتیجه چنین

استنباط می‌شود که فرضیه صفر با ۹۹ درصد اطمینان رد و فرضیه پژوهشی تأیید می‌شود. در نتیجه اقدام هایی همچون بومی‌سازی نیازمندی‌های سخت‌افزاری و نرم‌افزاری شبکه‌های رایانه‌ای، رعایت اصول پدافند غیرعامل و ایجاد یک‌لایه امنیتی در شبکه‌های رایانه‌ای و اقدامات پیشگیرانه مانند آموزش و اطلاع‌رسانی به کارکنان، از الزامات پدافند غیرعامل در رویارویی با تهدیدهای فضای مجازی با هدف افزایش بازدارندگی و کاهش آسیب‌پذیری است.

جدول۲ - آزمون خی دو

	Observed N	Expected N	Residual
2.00	1	18.5	-17.5
3.00	5	18.5	-13.5
4.00	25	18.5	6.5
5.00	43	18.5	24.5
Total	74		

	FARZ1
Chi-Square(a)	61.135
df	3
Asymp. Sig.	.000

نتیجه گیری و پیشنهادها

نتیجه های به دست آمده از بررسی سؤال های پژوهش، آزمون فرضیه‌ها و مطالعات کتابخانه‌ای یکی از مهم‌ترین مبانی ارائه پیشنهادهای در پژوهش است که اگر براساس تحلیل‌های صحیح انجام شود، می‌تواند در حل مشکلات موجود سودمند باشد. این پژوهش با هدف شناخت الزامات پدافند غیرعامل در برابر حمله های سایبری در سطح آجا طرح‌ریزی شد. برای این منظور پس از مشورت با استادان و خبرگان مشخص شد که برای رسیدن به این هدف می‌بایست شناخت الزامات پدافند غیرعامل در رویارویی با تهدیدهای فضای سایبر در سطح آجا با هدف افزایش بازدارندگی، کاهش آسیب‌پذیری به‌صورت جداگانه بررسی شد؛ بنابراین با تهیه فرضیه بر اساس هدف های پدافند غیرعامل، این مهم مورد بررسی قرار گرفت. گفتنی است راه کارهای امنیتی به‌تنهایی منجر به تأمین امنیت شبکه‌های رایانه‌ای نیست بنابراین ضمن رعایت تمام اصول امنیت، راه کارهای پدافندی می‌توانند موجب امنیت پایدار شبکه‌های رایانه‌ای شوند. همچنین باید اشاره نمود که راهکارهای پدافندی، امنیت بیشتری را

برای شبکه‌های رایانه‌ای تأمین می‌کنند زیرا راه کارهای پدافندی، اقدامات امنیت شبکه‌ای که پایداری بیشتری را برای شبکه فراهم می‌کنند توصیه می‌کنند. با بررسی و پژوهش در این مقاله نتیجه می‌گیریم که تدوین الزامات در فضای سایبر با رویکرد پدافند غیرعامل برای شناسایی و پیش‌بینی حمله ها سایبری و خنثی‌سازی تهدیدهای ناشی از تروریسم سایبری و یا به حداقل رساندن آسیب‌پذیری‌های سخت‌افزاری و نرم‌افزاری و بانک‌های اطلاعاتی، در سطح آجا امری ضروری است. به‌غیر از برخی اطلاعات محدود، داده‌های قابل اعتمادی دربارهٔ آمار حملات، آسیب‌پذیری‌ها، پیامدها و خطرهای تروریسم سایبری وجود ندارد که بتوان برای الگوها و ارزیابی تهدیدهای از آن‌ها استفاده کرد. با توجه به یافته‌های پژوهش پیشنهادهای زیر ارائه می‌گردد:

۱. تأسیسات، تجهیزات، پایگاه‌های مرکزی و مراکز داده مهم شبکه‌های رایانه‌ای آجا در زیر زمین پنهان شود تا علاوه بر مخفی ماندن از دید و تیر مستقیم دشمن، دربرابر سلاح‌های نامتعارف آسیب‌پذیری کمتری داشته باشند.

۲. سامانه‌های مختلف شبکه‌های رایانه‌ای آجا به‌وسیله کلمات عبور قوی و مطمئن که دارای ترکیبی از حرف، عدد و نشانه ها هستند محافظت شوند.

۳. برنامه‌ها و درگاه‌های غیرضروری شبکه و برنامه ها و درگاه‌هایی که کمتر از آن‌ها استفاده می‌شود ازجمله اهداف نفوذ گران هستند، بنابراین پیشنهاد می‌شود این برنامه ها و درگاه‌ها شناسایی و محافظت شوند.

۴. برای برقراری ارتباطات بین بخش‌های مختلف آجا و یا نقاطی که ازنظر جغرافیایی در فاصله دوری قرارگرفته‌اند، از شبکه‌های خصوصی مجازی که براساس لایه کاربرد مدل OSI پیاده‌سازی شده‌اند، استفاده شود. ۵-

۵. از دیواره آتش‌های «پروکسی سرور» به‌دلیل قابلیت اختفاء برنامه‌های شبکه در ارتباط با میزبان و برنامه‌های خارجی استفاده شود.

۶. پیشنهاد می‌شود با ترکیب رمزنگاری و پنهان‌نگاری، قدرت اختفاء اطلاعات شبکه-های رایانه‌ای را افزایش دهیم به‌گونه‌ای که کمترین تغییر در اطلاعات در آن‌ها،

قابل‌کشف باشد و نتوان موجودیت پیام پنهان در رسانه را حتی به‌صورت احتمالی آشکار ساخت.

۷. محل‌های برپایی تجهیزات شبکه و اتاق‌های اتصالات و مراکز پایگاه داده با دوربین-های حفاظتی واپایش و محافظت شوند.

۸. به‌دلیل پوشش بالای فیبر نوری دربرابر حمله های استراق سمع و شنود، در شبکه-های رایانه‌ای آجا از تجهیزات فیبر نوری به‌جای کابل‌های مسی و کواکسیال استفاده شود.

منابع

۱.الوندی، سیروس (۱۳۹۲)، الزامات پدافند غیرعامل در حملات سایبری، ***پایان‌نامه کارشناسی ارشد پدافند غیرعامل*** تهران: دانشکده علوم و فنون فارابی.

۲.احسانی، امیرفرهاد (۱۳۸۸)، مداخله در نواحی خرد دارای افت شهری و برقراری امنیت با به-کارگیری رهیافت تجدید حیات شهری با تأکید بر پدافند غیرعامل، ***پایان‌نامه کارشناسی ارشد دانشکده معماری و شهرسازی***، تهران: دانشگاه شهید بهشتی.

۳.جلالی فراهانی، امیرحسین (۱۳۸۹)، ***درآمدی بر آیین دادرسی کیفری جرائم سایبری***، تهران: انتشارات خرسندی.

۴.جلالی فراهانی، غلامرضا (۱۳۹۱)، ***تقریرات درسی تهدیدهای***، تهران: دانشکده علوم و فنون فارابی.

۵.جلالی فراهانی، غلامرضا (۱۳۹۱)، ***چهار گفتار در باب پدافند غیرعامل***، تهران: انتشارات محدث.

۶.جلالی فراهانی، غلامرضا و هاشمی فشارکی، جواد (۱۳۸۹)، ***پدافند غیرعامل در آیینه قوانین و مقررات***، تهران: ناشر سازمان پدافند غیرعامل کشور.

۷.جلالی فراهانی، غلامرضا (۱۳۹۰)، ***نگاهی به تهدیدهای نوین و نقش بسیج در حوزه پدافند غیرعامل***، تهران: انتشارات بوستان حمید.

۸.جیستان، ذبیح‌الله (۱۳۹۰)، دفاع در برابر ابزار پنهان جنگ سایبری، ***مجموعه مقالات اولین همایش ملی دفاع سایبری***، تهران: انتشارات جهاد دانشگاهی.

۹.خوش عمل، حسین (۱۳۹۱)، الزامات، ملاحظات و راهبردهای دفاع غیرعامل در حوزه فناوری اطلاعات (به‌منظور پایداری زیرساخت‌های حیاتی در برابر تهدیدهای سایبری)، ***پایان‌نامه کارشناسی ارشد***، تهران: دانشکده علوم و فنون فارابی.

۱۰.داودی دهاقانی، ابراهیم (۱۳۹۲)، نقش پدافند غیرعامل در کاهش آسیب‌پذیری‌های شبکه‌های رایانه‌ای ناجا، ***پایان‌نامه کارشناسی ارشد***، تهران: دانشکده علوم و فنون فارابی.

۱۱.دهخدا، علی‌اکبر (۱۳۵۱)، ***لغت‌نامه دهخدا***، جلد چهارم، تهران: موسسه چاپ و انتشارات دانشگاه تهران.

۱۲.رشید زاده، فتح‌الله (۱۳۸۴)، ***عصر اطلاعات و جنگ اطلاعات***، فصلنامه امنیت پژوهی، سال چهارم، شماره یازدهم.

۱۳.شهبازی، میثم، شفیعی، مسعود و ابوطالبی، زینت (۱۳۹۰)، ***رویکرد شبکه‌ای به زیرساخت‌های حیاتی***، تهران: ناشر مرکز پژوهشهای استراتژیک.

۱۴.عالی پور، حسن (۱۳۹۰)، ***حقوق کیفری فناوری اطلاعات***، تهران: انتشارات خرسندی.

۱۵.عالی پور، حسن (۱۳۹۰)، امنیت سایبری در چشم‌انداز ۱۴۰۴؛ چالش‌ها و راهکارهای حقوقی رویارویی با بزه‌های امنیتی سایبری، ***مجموعه مقالات اولین همایش ملی دفاع سایبری***، تهران: انتشارات جهاد دانشگاهی.

۱۶.میوالد اریک (۱۳۸۵)، ***مبانی امنیت شبکه***، ترجمه گروه پژوهشی فناوری اطلاعات جهاد دانشگاهی صنعتی شریف، تهران: انستیتو ایزایران.

۱۷.واحدی، مرتضی، نصر اصفهانی، مجید (۱۳۹۱)، ***پدافند غیرعامل و امنیت در فضای سایبری***، تهران: دانشکده علوم و فنون فارابی.

۱۸.***نرم‌افزار حدیث ولایت*** (مجموعه بیانات مقام معظم رهبری از سال ۱۳۶۷- ۱۳۹۳).

15. www.***paydarimelli***.ir.