ملاحظات پدافند غیرعامل در حوزهٔ فناوری اطلاعات سازمان تأمین اجتماعی

تاریخ دریافت: ۱۳۹۳/۱۰/۳۰
تاریخ تأیید: ۱۳۹۳/۱۲/۲۰

ناصر مدیری[۱]
حمیدرضا حدادی نیاسر[۲]

چکیده

این مقاله در سازمان تأمین اجتماعی باهدف شناخت و بررسی ملاحظات پدافند غیرعامل در برابر آسیب‌های فناوری اطلاعات سازمان تأمین اجتماعی با متغیر مستقل ملاحظات پدافند غیرعامل و متغیر وابسته آسیب‌های فناوری اطلاعات و به روش توصیفی– تحلیلی انجام شده است. پژوهش با این فرضیه که؛ «اقدامات و ملاحظات فناوری و مدیریتی پدافند غیرعامل در حوزه فناوری اطلاعات موجب کاهش آسیب‌های ناشی از به‌کارگیری فناوری اطلاعات در سازمان تأمین اجتماعی می‌گردد» به‌دنبال پاسخ‌گویی به این سؤال اساسی است که «اقدامات و ملاحظات پدافند غیرعامل در برابر آسیب‌های فناوری اطلاعات سازمان تأمین اجتماعی کدامند؟» ابزار گردآوری اطلاعات پرسشنامه پژوهشگر و مصاحبه با نخبگان حوزه پدافند غیرعامل و سازمان تأمین اجتماعی است. اعتبار آن نیز با استفاده از روش دلفی تأیید و پایایی آن با استفاده از آزمون ضریب آلفای کرونباخ ۰/۹۴۰۶ تعیین شده است. تحلیل داده‌ها با روش توصیفی و استنباطی و اولویت‌بندی مؤلفه‌ها با آزمون فریدمن انجام شده است. براساس نتایج پژوهش، ملاحظات پدافند غیرعامل در حوزهٔ فناوری اطلاعات و ارتباطات سازمان تأمین اجتماعی شامل دو دسته ملاحظات فناورانه و مدیریتی است که پژوهشگر بر اساس نتایج پژوهش، پیشنهادهای کاربردی و اجرایی خود را ارائه داده است.

کلیدواژه‌ها: *سازمان تأمین اجتماعی، پدافند غیرعامل، فناوری اطلاعات و ارتباطات، آسیب‌ها و تهدیدات.*

۱- استادیار مهندسی رایانه دانشگاه آزاد زنجان (aamn64@gmail.com)
۲- کارشناسی ارشد پدافند غیرعامل گرایش امنیت ملی دانشکده علوم و فنون فارابی (نویسنده مسئول) (haddi.hamidreza@yahoo.com)

مقدمه

هدف از اجرای طرح‌های پدافند غیرعامل رسیدن‌به امنیت بیشتر و کاستن از آسیب‌پذیری نیروی انسانی، بناها و تجهیزات حیاتی و حساس و مهم کشور باوجود حمله‌های خصمانه و مخرب دشمن و استمرار فعالیت‌ها و خدمات زیربنایی و تأمین نیازهای حیاتی و تداوم اداره کشور در شرایط بحرانی ناشی از جنگ است. حضرت امام خمینی (ره) می‌فرمایند: «ما امروز که مواجه هستیم با قدرت‌های بزرگ و شیطنت‌های بزرگ باید مهیا بشویم برای دفاع. البته این احتمال بسیار کم است که ما یک وقت محتاج به دفاع نظامی بشویم. کم است احتمال. برای اینکه قدرت‌های بزرگ هم می‌دانند که نباید حالا هجوم کنند. لکن هر چه هم احتمال کم است لکن از باب اینکه دفاع از یک مملکتی است، دفاع از اسلام است، این محتمل بزرگ است. ازاین‌جهت، ما باید مهیا بشویم. مهیا شدن یکی این است که بالقوه، چه قوه افرادی و چه قوای دیگر، باید مهیا بشود. چنانچه قرآن کریم دستور داده؛ و مهیا شدنمان هم به‌طوری باشد که با این مهیا شدن بترسند آن‌هایی که بنای، خیال هجمه دارند. دشمنانتان بترسند از قوه شما. همه جوان‌ها همه اشخاصی که ازشان کاری برمی‌آید، باید خودشان را مهیا کنند. آن روزی را ملاحظه کنند که یک‌وقت دشمن رو آورد به طرفشان هم باید تجهیزات مهیا بشود به قدری که بترساند دشمن‌ها را و هم باید قوای افراد، قوای نظامی، قوای چریکی، قوای پارتیزانی باید مهیا بشود وهم قوه ایمان باید زیاد بشود.» (امام خمینی (ره) :۱۳۵۹/۱/۲۸)

مقام معظم رهبری نیز می‌فرمایند: «امروز پدافند غیرعامل برای ما مهم است. بخش‌هایی دارند انجام می‌دهند، سپاه هم کارهای خوبی کرده، مطلع هستم؛ اما درعین‌حال بازبایستی کارکرد، تلاش کرد و این امکانات را در اختیار پدافند غیرعامل قرار بدهید» (www.paydarimelli.com ۱۳۸۶/۱/۲۶).

امنیت یک موضوع اجتماعی است و از عوارض زندگی اجتماعی محسوب می‌گردد، به‌عبارت‌دیگر امنیت در ارتباط با پدیده‌ها و افراد دیگر معنا پیدا می‌کند. بخش عمده‌ای از نگرانی‌های فرد، مربوط به محیط اطراف اوست و موضوع حفاظت از خویش در قبال آن بروز می‌کند (وبگاه رسمی سازمان پدافند غیرعامل).

امنیت از نظر مفهومی به وضعیتی گفته می‌شود که نیروهای حفظ‌کننده وضع موجود، توان این محافظت را از نیروهای شناخته‌شده برهم زننده آن داشته باشند. امنیت به سطوح مختلفی ازجمله امنیت فردی، امنیت اجتماعی، امنیت ملی و امنیت جهانی تقسیم می‌شود. همچنین در تحلیل این مفهوم حوزه‌های مختلف نیز از هم متمایز می‌شوند. برای مثال در امنیت ملی؛ امنیت اقتصادی، امنیت قضایی، امنیت فرهنگی، امنیت ارتباطات و... قابل‌تحلیل هستند. امنیت

را بر پایه‌های مفهومی مختلفی شناسایی می‌کنند، ازجمله این مفاهیم پایه، نظم است، یعنی امکان برهم خوردن نظم ناامنی به‌همراه خواهد داشت. دربارهٔ مهم‌ترینیت امنیت و نقش آن در پیشرفت فردی و اجتماعی، همین بس که بدون امنیت هیچ برنامه‌ای قابل اجرا نیست، در سطح ملی، امنیت مهم‌ترینیتی فراتر از بقا و صیانت ذات کشور دارد؛ به‌عبارت دیگر ممکن است دریک زمان تمامیت ارضی، استقلال و حاکمیت یک کشور محفوظ باشد ولی وجود تهدیدات جدی زندگی اجتماعی و سیاسی، آن کشور را دست‌خوش آشوب و هراس و سردرگمی نماید، نبود احساس آرامشی که به این شیوه به‌وجود می‌آید، مهم‌ترین مانع در مسیر حرکت کشور به سمت هدف‌های از پیش تعیین‌شده است.

پدافند غیرعامل بنابه تعریف وب‌گاه رسمی پدافند غیرعامل، «مجموعه اقداماتی است که انجام می‌شود تا در صورت بروز جنگ، خسارات احتمالی به حداقل میزان خود برسد». در پدافند عامل مثل سامانه‌های ضد هوایی و هواپیماهای ره‌گیر و غیره، فقط نیروهای مسلح مسؤلیت دارند. درحالی‌که در پدافند غیرعامل تمام نهادها، نیروها، سازمان‌ها، صنایع و حتی مردم عادی می‌توانند نقش مؤثری برعهده گیرند. با توجه به وجود تهدیدات بالقوه و خطراتی که امنیت ملی، استقلال و تمامیت ارضی کشور را نشانه گرفته است، بحث پدافند غیرعامل در طول سال‌های اخیر از سوی مقامات عالی‌رتبه کشوری و لشکری، مورد توجه فراوان قرار گرفته است و باور هر چه بیشتر مدیران و کارشناسان به این مقوله مهم، می‌تواند ضریب ایمنی کشور را در برابر تهاجم‌های احتمالی بیگانگان افزایش دهد؛ ولی در حال حاضر در زمینه پدافند غیرعامل هنوز در ابتدای راه هستیم. یکی از مؤلفه‌های تأمین امنیت، ایجاد امنیت در حوزه فناوری اطلاعات است که در پدافند غیرعامل نیز نقش مهم و مؤثری دارد و از عوامل تأمین امنیت در حوزه پدافند غیرعامل و اثربخش نمودن آن محسوب می‌شود.

اهمیت و ضرورت

فناوری اطلاعات فرصت‌های بی‌نظیری در اختیار بشر قرار داده است ولی مشابه با هر فناوری نوینی در جهان، چالش‌هایی نیز به‌دنبال دارد. سرقت اطلاعات، خرابکاری، از کاراندازی سامانه‌های رایانه‌ای، کلاهبرداری و جاسوسی ازجمله تأثیرات مخرب فناوری اطلاعات برای زندگی بشری است. همگام با گسترش روزافزون فناوری اطلاعات، ابزارها و شیوه‌های مختلف تهاجمی نیز به‌سرعت گسترش یافته و توان تخصصی و درجه پیچیدگی نفوذگران عامل تخریب یا غارت سیر صعودی پیدا کرده است. علاوه بر پیچیدگی روزافزون ابزارهای مورد استفاده در حمله‌های رایانه‌ای، بر شمار افرادی که قدرت یورش علیه زیرساخت‌ها را دارند هم روز به روز افزوده می‌شود. واپایش کارکردی فناوری اطلاعات براساس تعاریف انجام‌شده در راستای

هدف‌های سازمانی یکی از موارد بسیار مهمی است که هـر سـازمانی بایـد بـه آن توجـه لازم را داشته باشد.

ستاد مرکزی سازمان تأمین اجتماعی معاونت‌هایی تخصصی دارد؛ که بـرای تبـادل اطلاعـات از فناوری اطلاعات استفاده می‌کنند. از آنجایی‌که مالکیت فنـاوری اطلاعـات در اختیـار حریفـان است و کاربردی انسان محور دارد، بنابراین تهدیدها وآسیب‌هایی هم وجود دارد. امکان خطـای کاربری و یا سامانه‌ای وجود دارد، به‌ویژه از آنجایی‌که سازمان تأمین اجتماعی اقشـار مختلـف و گوناگون را حمایت‌های مختلف قرار می‌دهد، بنابراین در سازمان تأمین اجتماعی که بـا جامعـه هدف بیش از ۳۷ میلیونی سروکار دارد و ادامه و اسـتمرار فعالیـت و حیـات اطلاعـات در گـرو تدابیر لازم در حفظ و بقاء آن است لازم است که این پـژوهش علمـی انجـام شـود. در صـورت انجام نشدن این پژوهش متاسفانه سازمان تأمین اجتماعی هم ماننـد خیلـی از مراکـز بـزرگ و حساس کشور که مورد حملـه‌هـای گسـترده اطلاعـاتی و سـایبری قـرار گرفتـه‌انـد مشـکلات بی‌شماری را درپی خواهد داشت و ضرورت پیشگیری قبل از درمان به‌روشنی نمایان است.

هدف، سوال و فرضیه

هدف اصلی این پژوهش بررسی ملاحظات پدافند غیرعامـل در بخـش فناورانـه و مـدیریتی در حوزه فناوری اطلاعات سازمان تأمین اجتماعی اسـت و سـؤال اصـلی پـژوهش ایـن اسـت کـه: اقدامات و ملاحظات پدافند غیرعامل در برابـر آسـیب‌هـای فنـاوری اطلاعـات سـازمان تـأمین اجتماعی کدامند؟

فرضیهٔ مقاله بدین گونه است که: اقدامات و ملاحظات فناورانه و مدیریتی پدافنـد غیرعامـل در حوزه فناوری اطلاعات موجب کاهش آسـیب‌هـای ناشـی از بـه‌کـارگیری فنـاوری اطلاعـات در سازمان تأمین اجتماعی می‌گردد.

پیشینه

صفری نژاد (۱۳۹۱) پروژه‌ای با عنوان آسیب‌شناسی امنیتـی تجهیـزات و سـامانه‌هـای فنـاوری اطلاعات و ارایه راه‌حل‌های عملی و پاسخگو برای رفع آن‌ها در ستاد کل نیروهای مسـلح ارائـه کرده است که به برخی از موضوع‌های کاربردی اشاره شده است.

الف- بومی نبودن سامانه‌های جمـع‌آوری اطلاعـات از مهـم‌تـرین آسـیب‌هـای امنیتـی اسـت و بکارگیری شیوه‌های مدیریتی در حوزه‌های درون سازمانی و برون سازمانی برای رفع آسـیب‌هـا مؤثر است.

ب- بومی نبودن سامانه‌های انتقال اطلاعات از مهم‌ترین آسیب‌های امنیتـی اسـت و بکـارگیری شیوه‌های مدیریتی در حوزه‌های درون سازمانی و برون سازمانی برای رفع آسیب‌ها مؤثر است.

ج- بومی نبودن سامانه‌های پردازش اطلاعات از مهم‌ترین آسیب‌های امنیتی است و بکارگیری شیوه‌های مدیریتی در حوزه‌های درون سازمانی و برون سازمانی برای رفع آسیب‌ها مؤثر است.
د- بومی نبودن سامانه‌های ذخیره‌سازی اطلاعات از مهم‌ترین آسیب‌های امنیتی است و بکارگیری شیوه‌های مدیریتی مانند خلاقیت، نوآوری و کارآفرینی) در حوزه‌های درون سازمانی و برون سازمانی برای رفع آسیب‌ها مؤثر است. راهکارهایی نیز ارایه نموده است که برخی عبارت‌اند از:
- گوش به‌فرمان عملی و جدی به اوامر فرماندهی معظم کل قوا (مدظله‌العالی) در تمامی حوزه‌ها به‌ویژه در زمینه اتاق‌های فکر، علم محوری، خلاقیت و نوآوری و جنبش نرم‌افزاری
- توجه به متغیرهای مشترک بین تفکر سالم و طراحی و تولید فناوری شامل قدرت اندیشه و تفکر، تفکر راهبردی، دانش تفکر، کامل‌اندیشی با تشکیل کارگروه تخصصی، هماهنگ بودن با سازمان اجرایی و همسو بودن با زمان
- توجه کافی و جدی به زنجیره طراحی و تولید فناوری
- به‌کارگیری شیوه‌های خلاقیت و نوآوری در طراحی و تولید فناوری
حسن بیگی، ابراهیم در مقاله‌ای پیرامون گسترش شبکه ملّی دیتا، چالش‌های فرا رو و تهدیدهای متوجه امنیت ملّی که در آن نیز فناوری اطلاعات فرصت‌های بی‌نظیری در اختیار بشر قرار داده اشاره اما مانند هر فناوری نوینی در جهان، چالش‌هایی نیز به‌دنبال دارد. سرقت اطلاعات، خرابکاری، از کاراندازی سامانه‌های رایانه‌ای، کلاهبرداری و جاسوسی ازجمله تأثیرهای مخرب فناوری اطلاعات برای زندگی بشری است. گسترش اینترنت در جوامع و حتی به درون منزل و محل کار مردم و نیز جهانی بودن و وجود خطرهای بالقوه آن، دولت‌ها و سازمان‌ها را با چالش‌های جدیدی روبرو ساخته است. مهم‌ترین مشکلاتی که سازمان‌ها با نقاط تاریک فناوری اطلاعات دارند، عبارت‌اند از: دسترسی غیرمجاز افراد به سامانه‌ها و اطلاعات یک سازمان و خرابکاری، جاسوسی و یا دستکاری داده‌ها.

مفاهیم و مبانی نظری

فناوری اطلاعات و فضای سایبر: فناوری اطلاعات و ارتباطات بیانگر پویایی به دست آمده از همگرایی سامانه‌های رایانه‌ای و ارتباطی است که تبادل سریع و جهانی اطلاعات را فراهم آورده است و ظرفیت دگرگون کردن فرآیندهای کاری ر به خدمات و مانند آن را دارد؛ به همین علت برخی «فناوری اطلاعات» و «فناوری اطلاعات و ارتباطات» را یکسان می‌دانند و فقط برای تاکید بیشتر بر ارتباطات و مخابرات و برجسته‌تر کردن آن، از عبارت «فناوری اطلاعات و ارتباطات» استفاده می‌کنند (مؤسسه آموزشی و پژوهشی صنایع دفاعی، ۱۲:۱۳۸۴).

فناوری اطلاعات و ارتباطات نقطهٔ همگرایی علوم مختلفی ازجمله، اطلاعات، الکترونیک، رایانه و مخابرات است و از طرف دیگر نگاه به این علم از دیدگاه‌های مختلف قابل بررسی است و هر دیدگاه در نوع خود بیان‌کنندهٔ پاره‌ای از ویژگی‌های این علم است. یکی از تعریف‌های فناوری اطلاعات عبارت است از: مجموعه‌ای از روش‌ها، ابزارها، فرآیندها و سامانه‌هایی است که در جمع‌آوری، انتقال، ذخیره‌سازی، پردازش، انتشار و بازیابی اطلاعات به‌کار گرفته می‌شوند. در جایی دیگر به مجموعهٔ فناوری‌هایی که امکان ذخیره‌سازی، پردازش، ارائه و انتقال اطلاعات را در محیط‌های انتقال فرمهم‌ترین می‌نماید، گفته می‌شود. در تعریفی دیگر، به مجموعه‌ای از دانش، روش‌ها، ابزارها سخت‌افزار و نرم‌افزار که به‌منظور تسهیل و انجام فرآیند تولید، گردآوری، سازماندهی، ذخیره، بازیابی و نشر اطلاعات با استفاده از «رایانه» به‌عنوان ابزار پردازش و «شبکه» به‌عنوان شاه‌راه ارتباطی به‌کار گرفته می‌شوند، فناوری اطلاعات گفته می‌شود (کیسی،۱۳۸۷:۷۸).

نقش فناوری اطلاعات در سازمان:

نقش پشتیبانی: فعالیت اصلی و محوری سازمان بدون استفاده از فناوری هم انجام می‌شود، اما به‌کارگیری فناوری به چگونگی انجام فعالیت‌ها کمک بسیار زیادی می‌کند یا اینکه آن‌ها را گسترش می‌دهد. مثل به‌کارگیری سامانهٔ حسابداری برای یک فروشگاه که می‌توان همچنان صورت‌حساب‌ها را در دفترها نگه داشت، اما رایانه انجام عملیات حسابداری را ساده‌تر می‌کند.

نقش محوری: فناوری برای برخی سازمان‌ها نقش محوری دارد به‌طوری که بدون به‌کارگیری آن- اگرچه می‌توان به فعالیت ادامه داد- تفاوت بین به‌کارگرفتن و به‌کار نگرفتن فناوری زیاد است. مثل به‌کارگیری سامانه تایپ رایانه‌ای در یک روزنامه یا انتشاراتی. امروزه تقریباً بدون به‌کارگیری حروف‌چینی رایانه‌ای، اداره یک روزنامه یا انتشار یک کتاب غیرممکن است.

نقش راهبردی: در نقش راهبردی، اصولاً ادامه فعالیت سازمان بدون به‌کارگیری فناوری بی‌معنی است. مثل شبکه ارتباطی برای فروش بلیط هواپیما یا به‌کارگیری رایانه در سامانهٔ بانکی (قاسم‌زاده،۱۳۸۹: ۱۱۵). در کتاب «کلاسیک مدیریت راهبردی اطلاعات تجاری» سه راهبرد رقابتی برای بهره‌برداری از فاوا[1] در تجارت معرفی می‌شود:

۱. قدرت نفوذ اطلاعات: در این راهبرد فاوا، فرآیندهای نوآوری و ابتکار را توانمند و ابعاد رقابتی را تقویت می‌کند. مثال این راهبرد، به‌کارگیری سامانهٔ پیوند داده‌ای برای ارسال اطلاعات هدف به‌صورت بلادرنگ به سلاح است.

۱- فناوری اطلاعات و ارتباطات

۲. محصول اطلاعاتی: در این راهبرد، داده‌های موجود در فرآیندها با هدف ارائهٔ اطلاعات و دانش (به‌عنوان محصول جانبی) جمع‌آوری می‌شود که نسبت به فرآیند اصلی ایجاد برتری می‌کند. فرآیندهای جاسوسی که حجم بالایی از داده را جمع‌آوری می‌کنند، از این راهبرد برای به‌کارگیری مؤثر محصول‌های اطلاعاتی استفاده می‌کنند.

۳. تجارت اطلاعات: این راهبرد، ظرفیت‌های اضافهٔ فاوا، محصول‌های اطلاعاتی و یا خدمات مربوطه را ارائه می‌کند.

نقش تصمیم‌سازی و تصمیم‌یاری فاوا در مدیریت

تصمیم‌گیری و حل مشکل: مدیریت روندی است که به‌وسیلهٔ آن هدف‌های سازمانی با کاربرد منابع (افراد، پول، انرژی، مواد اولیه و زمان) به‌دست می‌آیند. این منابع به عنوان ورودی و دست‌یابی به هدف به‌عنوان خروجی این فرآیند درنظر گرفته می‌شوند. مدیران برای بهینه‌سازی این روند بر آن نظارت می‌کنند. مدیران بر اساس موقعیتشان در سازمان، فرهنگ و سیاست‌های سازمانی و شخصیت خود، کارهای بسیاری انجام می‌دهند. مینتزبرگ[1]، نقش مدیران را به سه دسته تقسیم کرد: بین‌فردی (مقام تشریفاتی، رهبر و رابط)، اطلاعاتی (ناظر، اشاعه‌دهنده و سخنگو) و تصمیم‌گیرنده (کارآفرین، برطرف کنندهٔ مشکل‌ها، تخصیص‌دهنده و مذاکره کننده). سامانه‌های اطلاعات اولیه اساساً از نقش‌های اطلاعاتی مدیر پشتیبانی کردند؛ اما در سال‌های کنونی، سامانه‌های اطلاعات برای پشتیبانی از هر سه نقش گسترش یافته‌اند.

به دلیل ارتباط کار مدیر با تصمیم‌گیرنده، وظایف مدیر به دو مرحله تصمیم‌گیری و برطرف کردن مشکل و تصمیم‌گیری دربارهٔ چگونگی برخورد با آن‌ها.

آنچه مدیران بیش از هر چیز به آن نیازمندند، ابزاری راحت، مطمئن و علمی برای یاری آنان در انجام تصمیم‌ها است که پیوسته یا گه‌گاه با آن روبرو می‌شوند. روش‌های کمی و ابزارهای ریاضی در این راستا کارساز و ثمربخش است (توربان،۱۳۸۶:۸۲۴).

با توجه به حجم بالای داده‌ها و فرآیندها و دادوستدهای مختلفی که درون سامانه‌ها وجود دارد و از طرف دیگر محدودیت توانایی سیستم تصمیم‌گیری مغز انسان، استفاده از شیوه‌های مدیریت کمی اطلاعات و ازجمله روش‌های تصمیم‌گیری که در پژوهش در عملیات مطرح می‌شود اجتناب‌ناپذیر است. از طرف دیگر رشد سریع فناوری‌های اطلاعات و استفاده از نرم‌افزارهای ویژه محاسبه‌های پژوهش در عملیات، ضمن تسهیل در انجام محاسبه‌ها، در فرآیند تصمیم‌گیری نیز سرعت و دقت بیشتری را به ارمغان آورده است. استفاده از این روش‌ها به‌ویژه

1. MintezBerg

در امور نظامی و به‌خصوص هنگامی‌که که مدیران از نظر زمـانی در تنگنـا قـرار دارنـد و حجـم زیادی از اطلاعات به سامانه وارد می‌شود و در یک زمان کوتاه که می‌بایست تصـمیمات مهـم و سرنوشت‌ساز گرفته شود بسیار مؤثر خواهد بود.

تصمیم‌گیری انتخاب بهترین راه برای نیل به هدف‌هاست و فرآیندی است شامل تعریف مسئله، ارزیابی راه‌حل‌ها، گرفتن تصمیم (انتخاب راه‌حل‌ها)، اجرای تصمیم و ارزیابی نتیجه است.

توانایی گرفتن تصمیم‌های جدید در مطالعه‌ای که هربریج‌هاوس[1] در بوستون انجام داد، به‌عنوان اولویت برتر شناخته شد. به نظر می‌رسد روش سـعی و خطـا کـه احتمـالاً رهیـافتی عملـی در تصمیم‌گیری در گذشته بوده، امروزه در بسیاری از موارد گران یا بی‌اثر است. کنتـرل خسـارت، نیز دیگر شیوه دفاع غیرعامل است کـه بـا اسـتفاده از سـامانه‌هـای هشـداردهنده، سـاماندهی امکانات امداد و نجات، تعیین وظایف بخش‌ها، افراد و آموزش و تمرین انجـام مـی‌شـود (جلالـی فراهانی، ۱۳۹۰-۱۳۸۹).

ضرورت توجه به پدافند غیرعامل در کشور: از آنجا که دفاع در برابر هرگونه تهـاجم احتمـالی کاملاً متفاوت از دفاع در برابر هرگونه مهاجم احتمالی دیگری است، کامل‌ترین پیش‌بینـی‌هـای دفاعی، شامل، پدافند عامل و غیرعامل لازم است. از بعد پدافندی، راهبردهای دفاعی زیر که در دوران دفاع مقدس به‌کار گرفته شده‌اند عبارت‌اند از: آمادگی قبل از بحـران و دشـمن شناسـی، بسیج همهٔ نیروها و منابع کشور در خدمت پدافند عامل، اتکا نکردن به سـلاح‌هـای پیشـرفته و روش‌های جنگ منظم؛ در برابر استفاده از نیروی پیاده نظام در سطح گسترده و بـا ترکیبـی از روش‌های جنگ منظم و نامنظم تأکید گردید. از نمونه‌هـای پدافنـد غیرعامـل در دوران جنـگ تحمیلی می‌توان به اعلام خطر در مقابل حمله‌های هوایی و موشکی آن هم فقـط در شـهرهای بزرگ کشور و درخواست از مردم برای رفتن به نقاط امن اشاره کرد. در طول سال‌های میانی و پایانی دوران دفاع مقدس، شاید مهم‌ترین اصل پدافند غیرعامل ایران را بتوان اصل «مقابلـه بـه مثل» دانست که تأکید آن بر استدلال بازدارندگی است. ولی تجربه نشان داد در شرایط تـوازن نسبی قوا، این اصل پدافندی نه تنها نتوانست کارساز باشد بلکه برعکس، موجب تشدید تمایـل دوطرف به توجیه حمله به غیرنظامیان گردید؛ به طوری که اجرای اصل «مقابلـه بـه مثـل» در نهایت موجب پدیدارشدن آنچه که به «جنگ شهرها» شهرت یافت، گردید. در ماه‌هـای پایـانی جنگ و همزمان با حمله‌های موشـکی دشـمن بـه تهـران، در سـطح معـابر عمـومی انـواعی از پناهگاه‌های شنی و بتنی مورد استفاده قرار گرفت. همچنین باتوجه به تهدیدهایی که بـه‌دلیـل

1. Herberig House

استفاده احتمالی دشمن از سلاح‌های شیمیایی وجـود داشـت، در تعـدادی از شـهرهای کشـور رزمایش‌هایی برای آموزش عمومی پدافند غیرعامل زمان حملهٔ شیمیایی برگزار گردیـد. از ایـن رو به‌نظر می‌رسید در این دوران کشور ما راهبرد مشخصی در بعد پدافند غیرعامـل در منـاطق غیرنظامی نبوده و همهٔ اقدام‌های انجام شده بنا بر اقتضای زمـان و بـه‌صـورت مقطعـی صـورت گرفته‌اند. این اقدام‌ها نیز از دو اصل آمـوزش بـرای آمـادگی دربرابـر وقـوع بحـران و رفـتن در پناهگاه‌های موقتی و کم‌ظرفیت پیروی می‌نموده‌اند. حال باتوجه به وجود تهدیدهایی که امنیت ملی، استقلال و تمامیت ارضی کشور را نشانه گرفته‌اند، ضرورت عقلی دفاع کاملاً هویـدا اسـت. بنابراین، به‌کارگیری اصول و معیارهای پدافند غیرعامل به تکمیل زنجیره دفاعی کشـور کمکـی مؤثر و قابل توجه می‌نماید.

تهدیدها و آسیب‌های فناوری اطلاعات و فضای سایبر:

آسیب‌پذیری، هرگونه کاستی یا نقصی است که می‌تواند ازسوی دشمن، برای ضربه زدن به زیـر ساخت‌ها و نیروهای خودی، مورد سوء استفاده قرار گیـرد. آسـیب‌پـذیری، متغیـری اسـت کـه احتمال یک حمله موفقیت‌آمیز را به منظور حمله علیه زیرساخت‌ها نشان مـی‌دهـد (علمـداری و همکاران،۱۳۹۱: ۵۳).

آسیب‌پذیری از نظر امنیتی، «به اقدام یا مجموعه اقداماتی کـه بـه منظـور تخریـب ارزش‌هـای اساسی یک ملت و کشور با چهره‌ای مبهم یا مشخص که نهایتـاً منـافع ملـی و امنیـت ملـی را هدف قرار می‌دهد گفتـه مـی‌شـود.» (سـاوه درودی، ۱۳۹۰: ۱۱۷). امـروزه بسـیاری از سـازمان‌هـا هزینه‌های گزاف را برای برقراری سامانه‌های امن در شبکه‌های خود پرداخت می‌کنند. در مقابل برخی سازمان‌های دیگر هنوز به مهم‌ترینیـت ایـن موضـوع پـی نبـرده‌انـد. انجـام آزمـون‌هـای نفوذپذیری نه‌تنها برای سازمان‌های دسته دوم بلکه برای سازمان‌هایی که اقـدام بـه برقـراری سامانه‌های امن نموده‌اند نیز پیشنهاد می‌شود؛ چراکه حتی درصورت پرداخت هزینـه و برپـایی چنین سامانه‌هایی نیاز به واپایش دائمی سامانه از لحاظ امنیتی موضوعی اجتناب ناپذیر به‌شمار می‌آید. آزمون نفوذپذیری به شبیه‌سازی آنچه نفوذگران واقعی انجام می‌دهند می‌پردازد، امـا در قـالبی قانونمنـد و اخلاقـی و بـرای کشـف و رفـع آسـیب‌پـذیری‌هـای امنیتـی سـامانه‌هـا. تقسیم‌بندی‌های مختلفی از تهدیدهای سامانه‌های اطلاعاتی، انجام شده است. این تهدیـدها بـه دو دستهٔ عمدی و غیر عمدی طبقه‌بندی می‌شود (توربـان،۱۱۵۲:۱۳۸۶). تهدیـدهای غیـر عمـدی شامل خطاهای انسانی، مخاطرات محیطی، اخـتلالات سـامانه‌هـای رایانـه‌ای اسـت. بسـیاری از مشکلات رایانه‌ای در اثر خطاهای انسانی ایجاد مـی‌شـوند. ایـن خطاهـا مـی‌تواننـد در طراحـی سخت‌افزار یا نرم‌افزار یا سامانه‌ای اطلاعات رخ دهد. آن‌ها می‌توانند در برنامه‌نویسـی آزمایشـی،

جمع‌آوری یا ورود داده‌ها، صدور مجوز و دستورالعمل‌ها ایجاد شوند. در بیشتر (حدود ۵۵ درصد) مشکلات مرتبط با واپایش و امنیت بسیاری از سازمان‌ها، اشتباه‌های انسانی دخالت دارند. مخاطرات زیست‌محیطی شامل زمین‌لرزه، طوفان شدید، سیل، اختلال نیرو یا نوسان‌های شدید آن، آتش‌سوزی و انفجارها هستند. اختلال‌های سامانه‌های رایانه‌ای، می‌تواند در نتیجهٔ ساخت ضعیف یا استفاده از مواد نامناسب در ساخت، رخ دهد (توربان،۱۳۸۶:۱۱۵۲).

انواع آسیب و تهدید:

حمله‌های غیرعامل: این حمله‌ها شامل واپایش ارتباط‌های مخابراتی به‌وسیلهٔ رسانه‌های عمومی مانند رادیو، ماهواره، ماکروویو و شبکه‌های سوئیچی عمومی است. برای مقابله با ایم حمله‌ها از شبکه اختصاصی مجازی، شبکه‌های حفاظت‌شده مبتنی بر رمزنگاری و شبکه‌های توزیع حفاظت‌شده مانند شبکه‌های توزیع سیمی که به‌صورت فیزیکی حفاظت می‌شوند استفاده می‌شود. روش‌های این نوع حمله عبارت‌اند از:

۱- پایش: حمله‌کننده با پایش شبکه می‌تواند اطلاعات کاربران را که از انتشار غیرمجاز محافظت نشده باشد بدست آورد.

۲- رمزگشایی اطلاعات رمز شده ضعیف

۳- کشف کلمه عبور: در این نوع حمله با استفاده از تحلیلگرهای پروتکل، کلمه‌های عبور برای استفاده‌های غیرمجاز به‌دست می‌آیند.

تحلیل ارسال و دریافت داده: مشاهده الگوهای ارسال و دریافت داده می‌تواند اطلاعات بسیار خوبی را در اختیار دشمن قرار دهد حتی اگر نتواند اطلاعات رمز شده را رمزگشایی کند. به‌عنوان مثال گسترش شبکه به صحنه نبرد راهکنشی ممکن است زودهنگام بودن عملیاتی از طرف کشور مهاجم را نشان دهد و مانع غافلگیر شدن عناصر خودی شود.

حمله‌های عامل: این حمله‌ها شامل تلاش‌هایی برای شکستن و یا به خطر انداختن جنبه‌های امنیتی شبکه، واردکردن کدهای مخرب (مانند ویروس)، از بین بردن داده و عملکرد درست سامانه است. برای مقابله با این نوع حمله باید به کمک دیواره‌های آتش و محافظها و دست‌یابی افرادی که مدیریت شبکه را انجام می‌دهند با استفاده از تصدیق هویت واپایش شود و از ابزارهای آشکارسازی خودکار ویروس، بازرسی و آشکارسازی نفوذ به شبکه استفاده گردد. در ادامه نمونه‌هایی از این نوع حمله آورده شده است.

۱. تغییر اطلاعات در حال انتقال: به‌عنوان مثال اگر ارتباط‌های مربوط به تجارت الکترونیکی به‌گونه‌ای تغییر داده شود که حجم مبادلات عوض شود و یا مبادلات به‌حساب شخص دیگری واریز شود، منجر به زیان‌های اقتصادی فراوانی خواهد شد.

۲. واردکردن داده: ارسال مجدد پیام‌های ارسال‌شده می‌تواند موجب به تأخیر انداختن عملیات شود.

۳. جعل کاربر یا سرور مجاز: در این حمله شخص خود را به‌عنوان شخص دیگری معرفی می‌کند و بدین ترتیب دست‌یابی تصدیق نشده به منابع و اطلاعات پیدا می‌کند. حمله‌کننده با استفاده از شنودگر یا ابزارهای دیگر اطلاعات مدیر و یا کاربران را جمع‌آوری می‌کند و سپس با استفاده از این اطلاعات به‌عنوان کاربر مجاز وارد شبکه می‌شود.

۴. سوءاستفاده از سامانه‌عامل‌ها و نرم‌افزارهای کاربردی: در این نوع حمله از نقاط آسیب‌پذیر نرم‌افزارهای موجود بر روی سامانه استفاده می‌شود. مشهورترین آن‌ها، استفاده از آسیب‌پذیری ارسال نامهٔ الکترونیکی و سرورهای خانواده ویندوز است. به‌تازگی هشدارهای زیادی درباره نکات آسیب‌پذیر ویندوز و ویندوز سرور داده شده است. تقریباً هر روز نقاط آسیب‌پذیر جدیدی برای نرم‌افزارها و سخت‌افزارها کشف می‌شود.

۵. سوءاستفاده از اجرای داده: حمله‌کننده با قرار دادن کدهای مخرب در نرم‌افزارهایی که به‌ظاهر بی‌زیان به‌نظر می‌رسند و یا ارسال نامهٔ الکترونیکی، کاربران را مجبور به اجرای آن‌ها می‌کنند.

۶. واردکردن کدهای مخرب (اسب تراوا، ویروس، کرم، در تله)؛ حمله‌کننده با استفاده از نقاط آسیب‌پذیری که از قبل تعریف‌شده، می‌تواند دستورهایی را در سامانهٔ کاربران اجرا کند و از این راه به هدف‌های خود برسد. این حمله می‌تواند شامل تغییر نرم‌افزار بر اثر رویدادی که در آینده اجرا شود نیز باشد.

۷. سوءاستفاده از قرارداد و اشکال‌های موجود در زیرساخت‌ها: حمله‌کننده با استفاده از کاستی‌های موجود در قراردادها، می‌تواند کاربران را تقلید کند و یا ارسال و دریافت داده را تغییر مسیر دهد.

۸. جعل خدمات: حمله‌کننده می‌تواند روتری را از شبکه خارج کند و یا شبکه را با ارسال بسته‌های اشتباه شده بمباران کند و یا هاب‌های نامه‌های الکترونیکی را با نامه‌های الکترونیکی اشتباه، بمباران کند.

حملهٔ تقرب: در این حمله فرد غیرمجاز با نزدیک شدن فیزیکی به شبکه‌ها و سامانه‌ها سبب تغییر، جمع‌آوری و یا جلوگیری از دست‌یابی افراد به اطلاعات می‌شوند. نزدیک شدن به منابع سامانه‌های اطلاعاتی با ورود پنهانی، دست‌یابی آزاد و یا ترکیب هردو انجام می‌شود.

به برخی از این حمله‌ها در زیر اشاره شده است:

۱- تغییر داده و جمع‌آوری اطلاعات: این حمله ناشی از نزدیک شدن فیزیکی افراد به سامانه‌ها و تغییر و یا دزدیدن اطلاعات مانند آدرس‌های قرارداد اینترنتی، جدول‌های مشخصات کاربران و کلمه‌های عبور است.

۲- تحریف سامانه: در این حمله شخص به‌منظور تخریب سامانه‌ها مانند ایجاد اشکال به آن‌ها نزدیک می‌شود.

۳- خرابی فیزیکی: شخص با نزدیکی فیزیکی به سامانه‌های اطلاعاتی سبب ایجاد خرابی فیزیکی در آن‌ها می‌شود.

حمله‌های داخلی: حمله‌های داخلی ازسوی افراد مجاز موجود در محدوده فیزیکی سامانه‌های پردازش امنیت اطلاعات و یا افرادی که دسترسی مستقیم به سامانه‌های پردازش امنیت اطلاعات دارند، انجام می‌شود. حمله‌های داخلی به دو دستهٔ بدخواهانه و غیربدخواهانه تقسیم می‌شود. حملهٔ غیربدخواهانه به این علت حمله درنظر گرفته می‌شود که عمل کاربر نتیجه امنیتی به‌دنبال دارد.

حمله داخلی بدخواهانه: پلیس امنیت ملی آمریکا برآورد کرده است که هشتاد درصد حمله و نفوذها از داخل سازمان‌ها بوده است. حمله‌کننده با دانستن چگونگی عملکرد سامانه، محل اطلاعات باارزش و سازوکارهای امنیتی به‌کار رفته، به سامانه‌ها حمله می‌کند. حمله‌کننده داخلی می‌تواند مسؤل نظافت سامانه‌ها، کاربران مجاز و مدیران سامانه با تمایلات متخاصمانه باشد. در این حمله، به اطلاعات و دسترسی سامانه‌ها آسیب می‌رسد و یا سازوکارهای امنیتی سامانه‌ها تغییر پیدا می‌کند. ممکن است حمله‌کننده‌های داخلی با ایجاد راه‌نفوذ مخفی اطلاعات را به خارج از شبکه حفاظت‌شده هدایت کنند. برخی از نمونه‌های این حملهٔ مهم در ادامه آورده شده است:

۱.تغییر داده و یا سازوکارهای امنیتی: افراد داخل محیط شبکه‌ها، می‌توانند به اطلاعات دسترسی داشته باشند و اطلاعات را به‌صورت غیرمجاز تغییر دهند و یا از بین ببرند.

۲.ایجاد ارتباط شبکه‌ای غیرمجاز: گاهی کاربرانی که دسترسی فیزیکی به شبکه‌های طبقه‌بندی‌شده دارند، ارتباطاتی را با شبکه‌هایی که سطح طبقه‌بندی پایین‌تری دارد ایجاد می‌کنند. معمولاً چنین ارتباطی با سیاست امنیتی همخوانی ندارد.
۳.راه‌های نفوذ پنهان: مسیرهای مخابراتی غیرمجازی هستند که برای انتقال اطلاعات از داخل مجموعه به مکانی در خارج آن بکار می‌رود.
۴.آسیب و یا خرابی فیزیکی: افراد با داشتن دسترسی فیزیکی به سامانه‌ها ممکن است به آن‌ها آسیب برسانند و یا آنها را خراب کنند.
حمله داخلی غیربدخواهانه: این حمله ازسوی افراد مجازی که قصد آسیب رساندن به اطلاعات و یا سامانهٔ پردازش اطلاعات را ندارند ولی به‌طور ناخودآگاه به آن‌ها آسیب می‌رسانند، به‌وجود می‌آید.
حمله توزیع: این حمله به تغییرات عمدی سخت‌افزار و نرم‌افزار بین مرحلهٔ تولید و نصب، یا هنگام انتقال آن از یک پایگاه به پایگاه دیگر است. آسیب‌پذیری‌های ممکن در کارخانه‌ها با به‌کارگیری روش‌های واپایش پیکربندی سامانه می‌تواند به کم‌ترین اندازه برسد. با استفاده از سازوکارهای واپایش دست‌یابی، توزیع واپایش‌شده و نرم‌افزارهای تأییدشده می‌توان آسیب‌های این نوع حمله را کاهش داد. روش‌های این نوع تهدید عبارت‌اند از:
۱.تغییر نرم‌افزار و سخت‌افزار محل تولید: در این نوع حمله پیکربندی نرم‌افزار و سخت‌افزار در طول فرآیند تولید تغییر می‌کند. برای مقابله با این نوع حمله می‌توان با واپایش شدید درستی محصول، واپایش پیکربندی مناسب و استفاده از امضاهای رمزنگاری برای محصول‌های نرم‌افزاری استفاده کرد.
۲.تغییر نرم‌افزار و سخت‌افزار در طول فرآیند توزیع: در این نوع حمله پیکربندی نرم‌افزار و سخت‌افزار به هنگام توزیع آن‌ها تغییر می‌کند. مانند جاسازی دستگاه‌های شنود در سامانه (مؤسسه آموزشی و پژوهشی صنایع دفاعی،۱۳۸۲).

عوامل مؤثر بر تهدیدهای سایبری:

نداشتن آگاهی و دانش کافی کاربران: آگاهی و آموزش کاربر دربارهٔ حفظ و نگهداری اطلاعات موجود در ایستگاه کاری برای کاربران فضای مجازی مهم‌ترینیت فراوانی دارد و از اصول اولیه امنیت کاربران است. کاربران شامل دو گروه کاربران عمومی و کاربران متخصص. نبود آگاهی و دانش در کاربران عمومی منجر به از دست دادن اطلاعات شخصی و خانوادگی می‌شود که گاهی منجر به پرداخت هزینه‌های سنگینی می‌گردد. منظور از کاربران متخصص افرادی هستند که مسئولیت نگهداری از شبکه و زیرساخت در سازمان‌ها را به عهده دارند. همچنین

افراد متخصصی که در زمینه تخصصی خود به‌ناچار باید از فناوری اطلاعات استفاده کنند، مثل پژوهشگرها، صنعتگرها، دانشجوها و... جزء کاربران متخصص به‌شمار می‌آیند (ذنوبی، ۱۳۹۰: ۴).

نبود زیرساخت و تجهیزات بومی: جایگاه امنیت فناوری اطلاعات و ارتباطات به‌طور مشخص در همهٔ سطح‌ها از لایه فیزیکی تا لایه برنامه‌های کاربردی را پوشش می‌دهد. رویه‌های اجرایی جمع‌بندی شده‌ای در دنیا طراحی که نیاز است در کشور بومی‌سازی گردد. درصورتی‌که پیش‌بینی‌های آینده و گام‌های اساسی در این باره در راستای دست‌یابی به فناوری بومی برداشته نشود و به زیرساخت‌های بومی و آزارهای امنیتی توجه جدی نشود، هرچه جلوتر می‌رویم، وابستگی مردم به خدمات الکترونیک بیشتر و از طرفی وابستگی زیرساخت‌های سرویس‌دهندگان به صاحبان اصلی فناوری این صنعت در خارج از کشور نیز بیشتر خواهد شد.

جدول شماره ۱: سطح‌بندی تهدیدهای سایبری (جلالی فراهانی،۱۳۹۰: ۱۱).

سطح	منشأ امنیت	سطح امنیت	هدف تهدید	سطح تهدید
فردی	فرد هکر	امنیت فردی	رایانه فرد	فردی
اجتماعی	گروه هکر	امنیت اجتماعی	شبکه‌های کارکردی	اجتماعی
ملی	دولت هکر	امنیت ملی	زیرساخت‌های حیاتی	ملی
بین‌المللی	ترکیبی	امنیت بین‌الملل	زیرساخت‌های بین‌المللی	بین‌المللی

فضای جنگ سایبری: خدمات و شبکه‌های زیرساخت اطلاعاتی در سطح جهانی، ملی و دفاعی است. اینترنت، شبکه‌ها و خدمات ارتباطی، شبکه‌های عمومی داده، شبکه‌های تجاری ماهواره‌ای، شبکه‌های رادیو و تلویزیونی و شبکه‌هایی از این دست، فضای جنگ سایبری را تشکیل می‌دهد (اسکندری، ۱۳۹۰: ۱۱۲ و ۱۱۱).

بررسی وضعیت فضای سایبری و ارتباط آن با پدافند غیرعامل: گسترش روزافزون فضای سایبر در تمام حوزه‌ها در دو دههٔ گذشته، این فضا را به عرصه‌ای بسیار مهم و تأثیرگذار تبدیل نموده است. بنابراین، به‌دلیل ویژگی‌های منحصربه‌فرد آن، به‌کارگیری این فضا در دستور کار تمامی کشورها، سازمان‌ها و افراد قرار گرفته و دامنه این به‌کارگیری همواره در حال گسترش است.

تدابیرفرماندهی معظم کل قوا (مدظله‌العالی): در اسفندماه سال ۱۳۹۰ مقام معظم فرماندهی کل قوا طی حکمی، دستور تشکیل شورای عالی فضای مجازی را صادر فرمودند. در متن این حکم چند نکته دارای اهمیت است:

۱-گسترش فزاینده فناوری اطلاعاتی و ارتباطی به‌ویژه شبکه جهانی اینترنت و آثار چشمگیر آن در ابعاد زندگی فردی و اجتماعی.

۲- لزوم سرمایه‌گذاری گسترده و هدفمند برای بیشترین بهره‌گیری از فرصت‌های ناشی از آن در راستای پیشرفت همه‌جانبه کشور.

۳- ضرورت برنامه‌ریزی و هماهنگی همیشگی به‌منظور پاسداری از آسیب‌های ناشی از آن.

حال با توجه به وجود زمینه تهدیدهای بالقوه و خطرهایی که امنیت ملی، استقلال و تمامیت ارضی کشور را نشانه گرفته‌اند، ضرورت عقلی دفاع کاملاً روشن است. بنابراین، به‌کارگیری اصول و معیارهای پدافند غیرعامل در این راستا می‌تواند به تکمیل زنجیره دفاعی کشور کمکی مؤثر و قابل‌توجه نماید که به این موضوع از سوی مقام معظم رهبری (مدظله‌العالی) به‌طور شایسته‌ای تأکید شده است. به‌نظر می‌رسد نخستین جنگ فضای سایبر، اواسط دهه ۷۰ میلادی در دوران جنگ سرد بین دو قدرت بزرگ آن زمان، ایالات‌متحده آمریکا و شوروی سابق، درگرفته باشد. شواهد نشان می‌دهند که در این دوران (بین سال‌های ۱۹۱۷ تا ۱۹۹۱) جنگ‌های سایبری زیادی رخ داده است؛ هرچند در بیشتر سندها، جنگ کوزوو به‌عنوان اولین جنگ سایبری بیان شده است.

عامل‌های کلیدی مقابله با تهدیدهای سایبری: فرهنگ‌سازی و افزایش سطح آگاهی کاربران نخستین گام کلیدی در مقابله با تهدیدهای سایبری است. نقش آگاهی و آموزش بر امنیت اطلاعات طبقه‌بندی‌شده در فضای مجازی بسیار مهم است. تهدیدهایی مانند، نشر ناخواسته اطلاعات شخصی؛ پاسخ به سؤالات؛ هرزنامه‌ها و روش‌هایی که دزدان سایبری به‌صورت حرفه‌ای از خود کاربران اطلاعات آن‌ها را به سرقت می‌برند، ز موارد نبود امنیت کاربر در فضای مجازی به‌شمار می‌آید که با آگاهی و آموزش قابل پیشگیری هستند.

ساختار در برابر تهدیدهای جمع‌آوری اطلاعات سایبری: جمع‌آوری اطلاعات سایبری رابطه‌ای مستقیم با پیشرفت فناوری‌های ارتباطی دارد و جمع‌آوری سایبری نتیجه پیشرفت فناوری‌های ارتباطی و به‌ویژه رایانه‌ای است. از این‌رو کشورها و یا گروه‌های دارنده فناوری سطح برتر همواره یک‌قدم جلوتر از دیگران هستند. امروزه با پیشرفت فناوری، حریم خصوصی دیگر وجود خارجی ندارد و در صورت به کار بردن روش‌های جدید استراق سمع و شنود و یا سایر

روش‌های جدید به‌صورت صحیح و اصولی می‌توان از محرمانه‌ترین و یا خصوصی‌ترین گفتگوهای افراد مهم سیاسی و نظامی آگاه شد. در خصوص جمع‌آوری سایبری و روش‌های جمع‌آوری رایانه‌ای و یا هجوم رایانه‌ای به‌طورکلی به دو حوزه انسانی و فنی دسته‌بندی می‌شود.

مأموریت پدافند غیرعامل در حوزه سایبر: تضمین امنیت، ایمنی و پایداری زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات، کاهش آسیب‌پذیری‌ها و افزایش آستانه تحمل در روبرویی با تهدیدها، با تأکید بر ایجاد عزم ملی به‌وسیلهٔ فرهنگ‌سازی، سیاست‌گذاری، طرح‌ریزی و برنامه‌ریزی، هدایت راهبردی و تدوین و تصویب چهارچوب‌ها و دستورالعمل‌های عمومی و تخصصی و نظام‌های هدایت بخش کشوری به‌منظور نهادینه نمودن رعایت اصول پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات و نظارت بر اجرای آن با ایجاد قابلیت به‌روزرسانی.

الزامات پدافند غیرعامل:

یکپارچه‌سازی خدمات و فعالیت‌های مرتبط با موضوع پدافند غیرعامل کشور.

هدف‌های کلان پدافند غیرعامل در حوزه سایبر: پیشگیری از اقدامات دشمنان جهانی و منطقه‌ای در آسیب‌پذیر نمودن زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات، امنیت زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در برابر خطرهای محتوایی، ایمنی زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در برابر حمله‌های فیزیکی، پایداری زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در برابر تهدیدها، قانون‌مندی ایجاد و گسترش نظام‌های فنی امنیتی، پژوهش‌های مؤثر در زمینه گسترش، آموزش و آگاهی عمومی، وابسته‌نبودن به محصول‌های غیربومی و صاحبان فناوری، امکان استفاده امن از اطلاعات در سطح ملی، امکان گسترش امن فناوری اطلاعات و ارتباطات همگام با روند جهانی، شناسایی و تشخیص به‌موقع آسیب‌پذیری‌ها در حوزه فناوری اطلاعات و ارتباطات، آمادگی و پیشگیری از تهدیدهای زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات، گسترش اثربخش برنامه‌های پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات.

سازوکارهای امنیتی متداول در پدافند غیرعامل در حوزه سایبر: با بررسی‌های به‌عمل‌آمده، سازوکارهای امنیتی در دفاع سایبری برابر شکل زیر عنوان می‌شود:

شکل سازوکارهای امنیتی در دفاع سایبری

روش، نوع تحقیق، جامعه آماری و تجزیه‌وتحلیل داده‌ها

ازآنجایی‌که در این مقاله به بررسی چگونگی ملاحظات پدافند غیرعامل در حوزه سایبری در سازمان تأمین اجتماعی پرداخته می‌شود بدون اینکه در وضعیت موجود تغییراتی ایجاد و یا متغیر مستقل دست‌کاری شده و اثرش بر متغیر وابسته بررسی و یا رابطه بین متغیرها بررسی شود؛ از روش توصیفی و تحلیلی استفاده شده است. در ادامه با مشورت با استادان خبره، متخصصان و کارشناسان نسبت به بررسی مسائل و رسیدن به سؤال‌های پیش رو، با انتقال محورها در جدول اکسل و رسیدن به سؤال‌های پرسشنامه توانستیم با تأیید این خبرگان به موضوع این پژوهش دست یابیم.

مقاله از نوع کاربردی است و روش آن توصیفی– تحلیلی است. گردآوری آن کتابخانه‌ای و میدانی و روش تجزیه‌وتحلیل کیفی (استدلالی) و کمی (استنباطی) است. در این مقاله معاون‌ها، مدیران، کارشناسان فنی سازمان تأمین اجتماعی تهران در سه سال گذشته و همچنین استادان پدافند غیرعامل دانشکده علوم و فنون فارابی برابر جدول ذیل به‌عنوان جامعه آماری انتخاب شده‌اند:

جدول شمارهٔ ۲: جامعه آماری

ردیف	عنوان جامعه آماری	حجم جامعه آماری
۱	معاونان سازمان تأمین اجتماعی تهران	۱۵
۲	مدیران سازمان تأمین اجتماعی تهران	۴۵
۳	استدان پدافند غیرعامل دانشگاه علوم و فنون فارابی	۱۵
۴	کارشناسان فنی سازمان تأمین اجتماعی تهران	۴۳
جمع		۱۱۸

نظر به مهم‌ترینیت موضوع، پژوهشگر همهٔ جامعه آماری را به‌صورت تمام شمار به‌عنوان جامعه نمونه آماری انتخاب کرده است.

فرضیه اول: اقدامات و ملاحظات فناورانه سخت‌افزاری و نرم‌افزاری پدافند غیرعامل موجب کاهش آسیب‌های ناشی از به‌کارگیری فناوری اطلاعات در سازمان تأمین اجتماعی می‌گردد.

جدول شمارهٔ ۳: آزمون فرضیه یک

طیف	خیلی زیاد	نسبتاً زیاد	زیاد	کم	خیلی کم	جمع
فراوانی	۲۲۶۲	۷۳۳	۴	۴۴	۲۱	۳۰۶۸
درصد	۷۳.۷۳	۲۳.۸۹	۰.۲۶	۱.۴۳	۰.۶۸	۱۰۰
$\overline{P}$	۹۷.۶۲			۲.۳۸		۱۰۰

چون مقدار آماره آزمون (۹۱/۶) از Z_α (مقدار بحرانی ۰۵/۲) بزرگ‌تر است و در ناحیه H1 قرارگرفته است و فرضیه H1 پذیرفته می‌شود و فرضیه مقابل آن یعنی H0 رد می‌گردد. به‌عبارتی‌دیگر با اطمینان ۹۸ درصد می‌توان گفت: اقدامات و ملاحظات فناورانه سخت‌افزاری و نرم‌افزاری پدافند غیرعامل موجب کاهش آسیب‌های ناشی از به‌کارگیری فناوری اطلاعات در سازمان تأمین اجتماعی می‌گردد.

جدول شمارهٔ ۴: آزمون فریدمن با استفاده از نرم‌افزار SPSS برای تعیین متغیرهای تأثیرگذار اصلی:

رتبه	سؤال	شماره	امتیاز
۱	ایمن‌سازی زیرساخت‌های ملی و دفاعی	سؤال ۲	۱۵.۹
۲	بومی‌سازی فناوری شامل سخت‌افزار و نرم‌افزار	سؤال ۱	۱۵.۷
۳	به‌کارگیری مکانیزم های امنیتی ویژه در استفاده از اینترانت	سؤال ۶	۱۵.۱۶
۴	شناسایی و خنثی‌سازی بدافزارها	سؤال ۴	۱۴.۹۴
۵	سازوکارهای امنیت ارتباطات در شبکه‌های رایانه‌ای	سؤال ۷	۱۴.۷۴
۶	به‌کارگیری مکانیزم های امنیتی در سرورها	سؤال ۳	۱۴.۷۱
۷	به‌کارگیری سازوکارهای امنیت داده‌ها	سؤال	۱۴.۵
۸	به‌کارگیری سازوکارهای امنیت برنامه‌های کاربردی	سؤال ۹	۱۳.۹۴

۹	کنترل تجهیزات سخت‌افزاری و نرم‌افزاری از حیث تجهیز	سؤال	۱۳.۹۴
۱۰	به‌کارگیری سازوکارهای امنیت در جلوگیری از نفوذ	سؤال ۵	۱۳.۸۹
۱۱	بازیابی اطلاعات حذف‌شده	سؤال	۱۳.۸۳
۱۲	به‌کارگیری سازوکارهای امنیتی در کاربرها	سؤال	۱۳.۷۲
۱۳	پایش امن و مطمئن تبادل اطلاعات	سؤال ۸	۱۳.۶۱
۱۴	به‌کارگیری سازوکارهای امنیت سیستم عامل	سؤال	۱۳.۶۱
۱۵	به‌کارگیری سازوکارهای امنیت در امضای دیجیتالی	سؤال	۱۳.۳۸
۱۶	به‌کارگیری از ضدویروس‌های بومی و یا مطمئن و امن	سؤال	۱۲.۸۱
۱۷	کنترل مستمر و بدون توقف در کار ابزارهای سخت‌افزاری	سؤال	۱۲.۸۱
۱۸	محافظت از تأسیسات فناوری اطلاعات	سؤال	۱۲.۸۱
۱۹	به‌کارگیری رمزکننده‌های سخت‌افزاری در تأمین ارتباطات	سؤال	۱۲.۷۱
۲۰	به‌کارگیری سازوکارهای امنیت در سامانه تشخیص نفوذ	سؤال	۱۲.۵۹
۲۱	تجهیز و توسعه آزمایشگاه استاندارد پیاده‌سازی امنیت شبکه	سؤال	۱۲.۵۹
۲۲	به‌کارگیری سازوکارهای امنیت در به کارگیری نشانه	سؤال	۱۲.۴۱
۲۳	به‌کارگیری سازوکارهای امنیت در تشخیص هویت	سؤال	۱۲.۴
۲۴	ایجاد اختلال و فریب در فعالیت‌های سایبری حریفان	سؤال	۱۲.۴
۲۵	واپایش برنامه‌های کاربردی اعمال سیاست	سؤال	۱۲.۴
۲۶	استفاده از پوشش حفاظتی تجهیزات در برابر تهدیدات	سؤال	۱۱.۵۹

فرضیه فرعی دوم: اقدامات و ملاحظات مدیریتی پدافند غیرعامل موجب کاهش آسیب‌های ناشی از به‌کارگیری فناوری اطلاعات در سازمان تأمین اجتماعی می‌گردد.

جدول شمارهٔ ۵: آزمون فرضیهٔ دو

طیف	خیلی زیاد	نسبتاً زیاد	زیاد	کم	خیلی کم	جمع
فراوانی	۱۹۶۱	۶۷۳	۱۹	۳۹	۲۲	۲۷۱۴
درصد	۷۲.۲۵	۲۴.۸۰	۰.۷۰	۱.۴۴	۰.۸۱	۱۰۰
$\overline{P}$	۹۷.۰۵		۲.۹۵			۱۰۰

چون مقدار آماره آزمون (۷۶/۶) از $Z\alpha$ (مقدار بحرانی۰۵/۲) بزرگ‌تر است و در ناحیه H1 قرارگرفته و فرضیه H1 پذیرفته می‌شود و فرضیه مقابل آن یعنی H0 رد می‌گردد. به‌عبارتی‌دیگر با اطمینان ۹۸ درصد می‌توان گفت: اقدامات و ملاحظات مدیریتی پدافند غیرعامل موجب کاهش آسیب‌های ناشی از به‌کارگیری فناوری اطلاعات در سازمان تأمین اجتماعی می‌گردد.

جدول شمارهٔ ۶: آزمون فریدمن با استفاده از نرم‌افزار SPSS به‌منظور تعیین اولویت متغیرهای تأثیرگذار اصلی:

رتبه	سؤال	شماره سؤال	امتیاز
۱	به‌کارگیری دستورالعمل‌های امنیت فضای سایبری	سؤال ۶	۱۳.۷۳
۲	بومی‌سازی استانداردها در حوزه سایبری	سؤال ۴	۱۳.۰۸
۳	ایجاد و تجهیز مرکز رخدادهای امنیتی	سؤال ۱۴	۱۳.۰۵
۴	مدیریت صحیح تولید و تأمین سامانه‌های نرم‌افزاری	سؤال ۷	۱۲.۷۹
۵	سناریونویسی و آینده‌پژوهی در مقابله با آسیب‌ها	سؤال ۱۳	۱۲.۶۵
۶	جداسازی شبکه داخلی از شبکه‌های خارجی	سؤال ۱۸	۱۲.۶۵
۷	به‌کارگیری فرایند مناسب اطلاع‌رسانی در خصوص آسیب‌ها و تهدیدات جدید	سؤال ۹	۱۲.۵۶
۸	مدیریت صحیح تولید و تأمین سامانه‌های سخت‌افزاری و نرم‌افزاری	سؤال ۲۰	۱۲.۳۶
۹	به‌کارگیری سازوکارهای امنیتی در صدور مجوزهای دسترسی کاربران	سؤال ۱۵	۱۲.۳۱
۱۰	ارتقاء سطح دانش و آگاهی کاربران	سؤال ۵	۱۲.۶
۱۱	ایجاد بخش سازمانی امنیت فضای سایبری	سؤال ۱۰	۱۱.۹۷
۱۲	واپایش و به‌کارگیری سیاست‌های برون‌سپاری	سؤال ۱۲	۱۱.۹۷
۱۳	انجام اقدامات خودواپایشی	سؤال ۱۶	۱۱.۸۳
۱۴	شناخت توانایی دشمن در تهدیدات	سؤال ۱۱	۱۱.۷۷
۱۵	نظارت بر ترددها و جابجایی در بخش نیروی انسانی و تجهیزات	سؤال ۸	۱۱.۶۸
۱۶	به‌کارگیری مؤثر اصول پدافند غیرعامل (استتار-اختفاء-پوشش-فریب)	سؤال ۳	۱۱.۵۷
۱۷	کسب قدرت واکنش سریع در برابر تهدیدات سایبری	سؤال ۱۹	۱۱.۲۹
۱۸	انجام رزمایش سایبری	سؤال ۲	۱۱.۲۸
۱۹	آموزش و فرهنگ‌سازی دفاع سایبری	سؤال ۱	۱۱.۰۵
۲۰	تعامل با سازمان‌ها و دستگاه‌های متولی امنیت اطلاعات	سؤال ۱۷	۱۱
۲۱	به‌کارگیری ساختارهای مورد نیاز سازمان در روبروی با تهدیدات نوین	سؤال ۲۱	۱۱
۲۲	حفاظت از اطلاعات مربوط به تجهیزات و فناوری و جلوگیری از دسترسی دشمن به آن	سؤال ۲۲	۱۱
۲۳	ایجاد ساختار مناسب جهت تولید و پشتیبانی نرم‌افزاری وسخت افزاری	سؤال ۲۳	۱۰.۸

نتایج حاصل از تجزیه‌وتحلیل داده‌های مربوط به فرضیه اول:

۱. با توجه به گستردگی جغرافیایی بخش‌های مختلف سازمان تأمین اجتماعی و لزوم یکپارچگی اطلاعاتی و سامانه‌ای آن و از سوی دیگر لزوم استفاده از زیرساخت‌های کشور برای این منظور، ایمن‌سازی زیرساخت‌های ملی و دفاعی به‌عنوان یکی از مهم‌ترین اقدامات پدافند

غیرعامل در برابر آسیب‌های ناشی از به‌کارگیری فناوری اطلاعات در سازمان تـأمین اجتمـاعی است.

۲.آسیب‌های ناشی از تجهیز سخت‌افزار و نرم‌افزار، به‌دلیل وابستگی فناوری به کشورهای صاحب فناوری، ازجمله آسیب‌های همیشگی و مهم این حوزه است که به‌کارگیری راه‌کارهای مناسب امنیتی و بیشترین استفاده از فناوری‌های بومی، یک اولویت مهم مطرح باشد.

۳.اینترانت داخلی سازمان، به‌عنوان بستر اصلی گردش اطلاعات است که هرگونه ضعف امنیتی پی‌آمدهای غیرقابل جبرانی را به‌همراه خواهد داشت و بنابراین رعایت اصول امنیتی در این بستر نیز از موضوع‌های اساسی مقابله با تهدیدها و آسیب‌ها خواهد بود.

۴.بدافزارها نیز به دلایل مختلفی ازجمله باز بودن درگاه‌ها و استفاده از واسطه‌های ذخیره‌سازی، جزء آسیب‌های فاوای سازمان تأمین اجتماعی است؛ که شناسایی و مقابله به‌موقع با آنها بسیار مهم و حیاتی است.

۵.یکی از چارچوب‌های مقابله‌ای و امنیتی در فضای سایبر و فاوا، چارچوب دفاع در عمق که هفت لایه دارد، است. گفتنی است که همان‌گونه که در زیر اشاره شده است، چهار لایه آن به‌عنوان راه‌کارهای مهم مقابله‌ای مورد تأیید قرار گرفته است.

- سازوکار های امنیت ارتباطات در شبکه‌های رایانه‌ای
- به‌کارگیری سازوکارهای امنیتی در سرویس‌دهنده‌ها
- به‌کارگیری سازوکارهای امنیت داده‌ها*به‌کارگیری مکانیزم های امنیت برنامه‌های کاربردی

۶. همان‌گونه که اشاره شد، استفاده از تجهیزات غیربومی همواره نگرانی برای دست‌اندرکاران امنیت، به‌همراه دارد. در کنار استفاده از تجهیزات بومی، یکی از راه‌کارهای اساسی برای مقابله با این آسیب و تهدید، واپایش تجهیزات سخت‌افزاری و نرم‌افزاری از نظر اطمینان از نبود سازوکارهای سخت‌افزاری و نرم‌افزاری به‌منظور خرابکاری، اختلال، سرقت اطلاعات و... است.

نتایج به دست آمده از تجزیه‌وتحلیل داده‌های مربوط به فرضیه دوم:

۱- تبیین، به‌کارگیری، اجرا و نظارت بر دستورالعمل‌های امنیت فضای سایبری، تضمین‌کننده فرایندی همیشگی، دقیق، یکنواخت در برقراری سامانه‌ی فناوری اطلاعات و ارتباطات است.

۲- یکی از چالش‌های مهم امنیتی، استفاده از دستورالعمل‌ها و استانداردهای امنیتی غیربومی است. این دستورالعمل‌ها به دلایل مختلف نمی‌توانند الگوی مناسبی برای این مهم به‌شمار آیند.

۳- ازجمله اقدام‌های راهبردی، ایجاد و تجهیز مرکز رخدادهای امنیتی برای دیده‌بانی و پایش همیشگی آسیب‌ها و تهدیدها در فاوای سازمان است که تضمین‌کننده اقدام مقابله‌ای مناسب و به‌هنگام نیز است.

۴- یکی از نقاط آسیب‌پذیری و نفوذ در سامانه‌های فناوری اطلاعات و ارتباطات، سامانه‌های نرم‌افزاری است. بنابراین مدیریت، واپایش و نظارت در رابطه با کارایی و سلامت امنیتی آن‌ها نیز از گام‌های اساسی امنیت در این حوزه است.

۵- داشتن برنامه و نقشهٔ راه برای تهدیدها و آسیب‌ها، از اقدام‌های مدیریتی در حوزه امنیت فاوا است که می‌تواند سامانه را در برابر هر آسیب و تهدیدی مقاوم و پایدار نماید.

۶- راه‌کارهای مدیریت و تصمیم‌های امنیتی ازجمله وظایف مدیران امنیت فاوای سازمان است که می‌بایست با توجه به نیازمندی‌ها، اولویت‌ها و... . تصمیم‌های لازم را در رابطه با جداسازی شبکه داخلی از شبکه‌های خارجی بگیرند.

۷- کاربران سامانه به دلایل مختلف به‌طور عمدی یا سهوی فعالیت سامانه را با مشکل مواجه می‌کنند. به‌کارگیری فرایند مناسب اطلاع‌رسانی دربارهٔ آسیب‌ها و تهدیدها و حتی دستورالعمل استفاده از تجهیزات، بسیاری از این مشکل‌ها را برطرف خواهد کرد.

۸- همچنین نیاز به دانستن که مبنای صدور دسترسی به اطلاعات برای کاربران است می‌بایست به‌عنوان یک موضوع مهم در دستورالعمل‌ها درج شود.

پیشنهادها

۱- تعامل با سازمان‌ها و نهادهای سیاست‌گذار و مؤثر در مدیریت فضای سایبری کشور به‌منظور همسوسازی، دستیابی و استفاده از اسناد بالادستی حوزه دفاع سایبری به‌وسیلهٔتدوین راهبردهای عملیاتی و به‌دست آوردن سیاست‌ها، اولویت‌ها و اهداف کلان دفاع سایبری

۲-ایجاد مرکز رخدادهای امنیت فاوا در مدیریت امنیت فاوا سازمان تأمین اجتماعی

۳- برای ارتباطات درون و برون سازمانی در حوزه امنیت اطلاعات، سامانه جامع و یکپارچه اطلاعاتی پیاده‌سازی و اجرا و اطلاعات بخش‌ها و واحدهای مرتبط درون و برون سازمان به‌صورت یکپارچه در یک پایگاه اطلاعات موجود و قابل دسترسی برای واحدهای مربوط باشد.

۴-با توجه به یافته‌های پژوهش، مدیریت صحیح منابع سخت‌افزار و نرم‌افزار دارای کارکرد پدافند غیرعاملی هست و از اهمیت خاصی برخوردار است در این باره:

۱. همهٔ اطلاعات مربوط به منابع سخت‌افزاری و نرم‌افزاری جمع‌بندی و نوشته شود و فهرستی از آخرین وضعیت آن‌ها و شرح همهٔ جزئیات آن تهیه و تدوین شود.

۲. دربارهٔ چگونگی استفاده از این منابع و اطلاعات مربوط به آن، دستورالعمل و آئین‌نامه‌هایی تهیه و به‌صورت منظم و قانونمند تدوین و تنظیم شود.

۳. دربارهٔ موضوع واپایش دسترسی باید گفت، با توجه به اینکه واپایش دسترسی در سازمان کارکرد پدافند غیرعاملی دارد، پیشنهادهای زیر ارائه می‌شود:

- واپایش و نظارت دقیق بر چگونگی و میزان دسترسی
- تغییر در نوع دسترسی‌ها و از بین بردن دسترسی‌های غیر لازم و غیرضروری و همچنین به سطح دسترسی‌ها نیز واپایش و نظارت دقیق صورت گیرد.
- تجهیزات موجود در شبکه و سازمان شناسایی شده و به‌طور دقیق از آن‌ها حفاظت شود.
- برقراری و ایجاد رمزهای امنیتی و رمز عبورهای مشخص و معین در این خصوص و تغییر و مدیریت آن در بازه‌های زمانی خاص برای ارتقاء سطح امنیت در شبکه و سازمان.

• امنیت منابع انسانی با توجه به یافته‌های پژوهش کارکرد پدافند غیرعاملی دارد و پیشنهاد می‌شود:

- در راستای به‌کارگیری کارکنان اقدام‌هایی ویژه و مهمی صورت گیرد و بررسی سابقه کارکنان در هنگام به‌کارگیری مورد توجه و اهمیت قرار گیرد.
- به‌منظور افزایش سطح آگاهی کارکنان اقدام‌های مؤثری انجام شود بدین منظور دوره‌های آموزشی ویژه امنیت اطلاعات برای کارکنان تشکیل و برگزار شود.
- دسترسی کارکنان و پیمانکاران سازمان بعد از پایان دوره استخدام و قرارداد بازنگری شود و این دسترسی از بین برود.

با توجه به آنچه مورد پژوهش قرار گرفت و نتایج به‌دست آمده امنیت فیزیکی و محیطی کارکرد پدافند غیرعاملی دارد و در این باره پیشنهاد می‌شود:

امنیت فیزیکی در محیط سازمان ازنظر ورود، خروج و محیط اطراف آن با اقدام‌های ویژه و زیربنایی برقرار شود.

- ایمن‌سازی سامانه‌های برق‌رسانی و برقراری امنیت در حوزه فناوری اطلاعات و ارتباطات سیار و کابل‌کشی سامانهٔ مخابرات و تلفن‌های سازمان.

منابع

۱.امام خمینی (ره). (۱۳۷۲)، ***صحیفه نور ج ۱۲***،سخنرانی تاریخ ۱۳۵۹/۱/۲۸، تهران: مؤسسه تنظیم و نشرآثار امام خمینی(ره).

۲.اسکندری، حمید. (۱۳۹۰)، ***دانستنی‌های پدافند غیرعامل ویژه دوره عمومی سطح ۲*** (ویژه کارکنان اداری، شرکت‌ها و متصدیان)، تهران: انتشارات بوستان حمید، اول

۳.پورشمس، امیرحسین. فانیان، علی. (۱۳۹۰)، ***ارزیابی تهدیدهای تجهیزات شبکه غیربومی در دفاع سایبری***، مجموعه مقالات اولین همایش ملی دفاع سایبری، تهران: انتشارات جهاد دانشگاهی.

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

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

۶.خوش‌عمل، حسین. (۱۳۹۱)، ***الزامات، ملاحظات و راهبردهای دفاع غیرعامل در حوزه فناوری اطلاعات*** (به منظور پایداری زیرساخت‌های حیاتی در برابر تهدیدات سایبری)، پایان‌نامه کارشناسی ارشد، تهران: دانشکده علوم و فنون فارابی.

۷.ذنوبی، مجتبی. (۱۳۹۰)، ***شناسایی تهدیدات سایبری و عوامل کلیدی در مقابله با آن***، مجموعه مقالات اولین همایش ملی دفاع سایبری، تهران: انتشارات جهاد دانشگاهی.

۸.ساوه درودی، مصطفی. (۱۳۹۰)، ***راهبردهای سازمانی و مدیریت بحران***، تهران: دانشکده علوم و فنون فارابی.

۹.ساوه درودی، مصطفی. (۱۳۹۰)، ***مدیریت بحران‌های امنیتی***، تهران: دانشکده علوم و فنون فارابی.

۱۰.عالی‌پور، 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.

۱۱.عالی‌پور، حسن. (۱۳۹۰)، ***حقوق کیفری فناوری اطلاعات***، تهران، انتشارات خرسندی.

۱۲.علمداری، شهرام و مشهدی، حسن. (۱۳۹۱)، ***روش‌های آسیب‌پذیری زیرساخت‌ها و مدیریت بحران***، تهران: بوستان حمید.

کدخبر:۶۰۸۶ ۱۳۸۶/۱/۲۶13.www.paydarymelli.com

آسیب‌های امنیتی خط انتقال آب کوهرنگ به استان یزد

جمشید شریفیان[1]
سید محمدرضا مصطفوی[2]
محمدجواد برزگر منشادی[3]

تاریخ دریافت: ۱۳۹۳/۰۲/۲۰
تاریخ تأیید: ۱۳۹۳/۰۳/۲۵

چکیده

آب سرچشمه زندگی و مهم‌ترین نیاز انسان به آب در درجه اول آب آشامیدنی و سپس استفاده از آن در مصارف دیگر است. آب آشامیدنی در بسیاری از مناطق دنیا به کالایی کمیاب تبدیل شده است؛ بنابراین با توجه به شرایط فعلی و آمار و رقم‌های موجود می‌توان گفت ایران در سال ۱۴۱۰جزء کشورهای کم آب قرار خواهد گرفت. با توجه به کم‌آبی قابل توجه کشور و به‌ویژه استان یزد و حساسیت و اهمیت پروژه انتقال آب از سرشاخه‌های کوهرنگ به استان و لزوم حفظ پایداری و امنیت آن از لحاظ کارکردی و ساختاری، آسیب‌های امنیتی این خط انتقال بررسی شده است. سؤال اصلی پژوهش عبارت است از: «آسیب‌های امنیتی خط انتقال آب کوهرنگ به استان یزد چیست؟» و فرضیهٔ اصلی این است که «آسیب‌ها و تهدیدهای امنیتی خط انتقال آب کوهرنگ به استان یزد شامل آسیب‌ها و تهدیدهای انسانی، فنی و طبیعی است». در تحقیق پیش رو مبانی نظری امنیت که مبتنی بر امنیت کارکردی است مورد توجه قرار گرفته و روش پژوهش استفاده شده، توصیفی- تحلیلی است. روش گردآوری اطلاعات به روش کتابخانه‌ای و میدانی انجام شده است. برای گردآوری اطلاعات میدانی ابتدا پرسشنامه بین مسئولان و کارشناسان فنی مرتبط با موضوع و مدیران ارشد امنیتی استان توزیع و تحلیل آماری توصیفی و استنباطی با استفاده از نرم‌افزار SPSS انجام شده است که نتیجه آن اثبات فرضیه اصلی مبنی بر روبرو بودن خط انتقال با آسیب‌های انسانی، فنی و طبیعی است.

کلیدواژه‌ها: *آسیب‌های امنیتی، استان یزد، خط انتقال لوله آب کوهرنگ، تهدیدات انسانی،فنی و طبیعی.*

۱- استادیار روابط بین‌الملل دانشکده علوم و فنون فارابی (jam_sharifian@yahoo.com)
۲- دانشجوی دکترای امنیت ملی دانشگاه عالی دفاع ملی(smrm@gmail.com)
۳- کارشناسی ارشد پدافند غیرعامل گرایش امنیت ملی دانشکده علوم و فنون فارابی (mjb1353@gmail.com)