ارزیابی اثربخشی سامانه مدیریت امنیت اطلاعات در پدافند غیرعامل(مطالعه موردی)

علیرضا حسن‌زاده[1]
حمیدرضا سوری[2]
وحید امینی[3]

تاریخ دریافت: ۱۳۹۴/۱۰/۲۵ تاریخ پذیرش: ۱۳۹۴/۱۲/۲۰

چکیده

متناسب با حجم و تنوع تهدیدهای فناوری اطلاعات و ارتباطات(فاوا)[4]، آنچه مهم است وجود سامانه‌های مدیریت امنیت اطلاعات است که با رویکردی نظام‌مند، امنیت اطلاعات حساس سازمان‌ها را تأمین کند. ازاین‌رو ارزیابی اثربخشی این سامانه‌ها خود از چالش‌های مدیران امنیتی سازمان‌ها قلمداد می‌شود. این پژوهش با هدف «ارزیابی اثربخشی سامانه مدیریت امنیت اطلاعات در پدافند غیرعامل(حوزه فناوری اطلاعات و ارتباطات)» با متغیر مستقل سامانه مدیریت امنیت اطلاعات و متغیر وابسته پدافند غیرعامل و به روش توصیفی– تحلیلی انجام شده است و با این فرضیه که؛ «سامانه مدیریت امنیت اطلاعات، در تأمین هدف های پدافند غیرعامل(حوزه فناوری اطلاعات و ارتباطات)، اثربخش است، به‌دنبال پاسخ‌گویی به این سؤال اساسی است که «آیا سامانه مدیریت امنیت اطلاعات، در پدافند غیرعامل(امنیت فناوری اطلاعات و ارتباطات) اثربخش است؟»

ابزار گردآوری اطلاعات پرسش‌نامه ساخته پژوهشگر و جامعه آماری ۳۰ نفر از کارشناسان و مدیران حوزه فاوای معاونت برنامه‌ریزی و نظارت راهبردی(سابق) رئیس‌جمهوری و کارشناسان خبره فاوا و مرتبط با پدافند غیرعامل است. اعتبار آن با استفاده از روش دلفی تأیید شده و پایایی آن با استفاده از آزمون ضریب آلفای کرونباخ ۰/۸۸ تعیین شده است. تحلیل داده‌ها با روش توصیفی و استنباطی انجام شده است. نتایج پژوهش ضمن تأیید اثربخشی این سامانه در پدافند غیرعامل، اثربخشی پدافند غیرعاملی هریک از بخش‌های سامانه مدیریت امنیت اطلاعات در امنیت فاوا و به‌طورکلی در پدافند غیرعامل را مشخص کرده است. پژوهشگر براساس نتایج پژوهش، پیشنهادهای کاربردی و اجرایی خود را ارائه داده است.

واژگان کلیدی: *فناوری اطلاعات و ارتباطات، سامانه مدیریت امنیت اطلاعات، پدافند غیرعامل، استانداردهای امنیت فاوا*

---

۱. استادیار فن‌آوری اطلاعات دانشگاه تربیت مدرس(ar_hassanzadeh@modares.ac.ir)
۲. کارشناسی ارشد فناوری اطلاعات و ارتباطات (h_r_souri@yahoo.com)
۲.کارشناسی ارشد پدافند غیرعامل گرایش امنیت ملی و نویسنده مسئول (amini_vahid10@yahoo.com)

مقدمه

امروزه استفاده سازمان‌ها از فناوری اطلاعات، آن‌ها را با مخاطرات تازه‌ای که برخاسته از فضای مجازی است، روبرو کرده است که برای برابره با آن نیاز به مدیریت فراگیر و نظارت دقیق و به‌هنگام است تا از اطلاعات دربرابر تهدیدهای دشمنان حفاظت و از دادوستد و اشتراک‌گذاری امن اطلاعات برای افزایش توانمندی‌های تجارت حمایت گردد. امنیت اطلاعات در محیط‌های مجازی همواره به‌عنوان یکی از چالش‌ها و الزامات اساسی مورد تأکید قرار گرفته است. اگرچه امنیت کامل چه در محیط واقعی و چه در فضای مجازی دست‌نیافتنی است، ولی ایجاد سطحی از امنیت که به اندازه قابل قبول و متناسب با نیازها و سرمایه‌گذاری انجام شده باشد، تقریباً در تمامی شرایط محیطی دست‌یافتنی است. تنها با فراهم بودن چنین شرایط مطلوبی است که اشخاص حقیقی، سازمان‌ها، شرکت‌های خصوصی و سازمان‌های دولتی، ضمن اعتماد و اطمینان به طرف‌های گوناگونی که همگی در یک دادوستد الکترونیکی دخیل هستند و احتمالاً هیچ‌گاه یکدیگر را ندیده و نمی‌شناسند، نقش مورد انتظار خود به‌عنوان گره‌های مؤثر از این شبکه متعامل و هم‌افزا را ایفاء خواهند کرد (صدر آملی و دیگران، ۱۳۸۸: ۳).

بیان مسئله

ایمن بودن سرمایه‌های اطلاعاتی و شبکه‌های زیرساختی در کشور، گذشته از ابعاد گسترده امنیت ملی، عامل اصلی موفقیت در استفاده از فرصت‌های بی‌شمار تجاری و غیرتجاری جدید اینترنتی است؛ به‌عبارت‌دیگر امنیت اطلاعات بسته‌ای از خط‌مشی‌ها و رویکردها، فرایندها، گردش‌کارها، ساختارهای سازمان و فعالیت‌های نرم‌افزاری و سخت‌افزاری به‌منظور حفاظت از اطلاعات در برابر گسترهٔ وسیعی از تهدیدهایی است که تداوم کارها، کمینه کردن خطر و بیشینه نمودن میزان بازده سرمایه‌گذاری‌ها و فرصت‌ها را نشانه رفته است و به‌عبارتی‌دیگر، امنیت اطلاعات، حفظ محرمانگی، تمامیت و در دسترس بودن اطلاعات و همچنین سایر

مواردی مانند تصدیق هویت، مسؤلیت‌پذیری، عدم انکار و قابلیت اطمینان را شامل می‌گردد (صدرآملی و دیگران، ۱۳۸۸: ۴).

معاونت برنامه‌ریزی و نظارت راهبردی رئیس جمهوری ازجمله سازمان‌های بسیار مهم کشوری است که اطلاعات بسیار مهم و ارزشمندی در بستر فناوری‌های اطلاعاتی و شبکه‌های رایانه‌ای در آن جریان دارد. این اهمیت اطلاعات موجود، خود عامل افزایش تهدیدهای فناوری اطلاعات را به‌دنبال دارد که امروزه یکی از مهم‌ترین دغدغه‌های مدیران این سازمان است.

سامانه مدیریت امنیت اطلاعات[1] بخشی از سامانه‌های مدیریتی سازمان قلمداد می‌شود که بر پایهٔ رویکرد مخاطرات کسب‌وکار قرار دارد و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات است. این سامانه درمجموع رویکردی نظام‌مند به مدیریت اطلاعات حساس به‌منظور محافظت از آن‌ها است. همچنین رویکردی تحولی در مدیریت سازمان است که سعی دارد امنیتی سازمان‌یافته، سامانمند و یکپارچه ایجاد کند و با یک دیدگاه کلان‌نگر و بالا به پایین، با ارائه یک روش‌شناسی رسمی، گام‌به‌گام آن را در سازمان پیاده‌سازی نماید. ازآنجاکه تأمین امنیت فاوا در کشور از حوزه‌های پدافند غیرعامل قلمداد می‌شود؛ اثربخشی سامانه مدیریت امنیت اطلاعات، میزان اثربخشی آن و همچنین کارکرد این سامانه در پدافند غیرعامل و شناسایی واپایش‌های این سامانه ازجمله دغدغه‌های پژوهشگر است که در این پژوهش سعی شده است به‌طور موردی در معاونت برنامه‌ریزی و نظارت راهبردی ارزیابی شود.

اهمیت و ضرورت

ایجاد امنیت متشکل از مجموعه‌ای از فرایندهاست و نگاه محصولی به آن امنیت اطلاعات سازمان را با چالش نابودکننده‌ای روبرو می‌سازد. با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش سامانمند به امنیت اطلاعات شکل گرفت. براساس این نگرش،

1. Information Security Management System

تأمین امنیت اطلاعات در یک مجموعه سازمانی با اقدامی یک‌باره شدنی نیست و لازم است این امر به‌صورت فرایندی مداوم و در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح، انجام شود. برای این منظور لازم است هر سازمان براساس یک روش مشخص، ضمن تهیه طرح‌ها و برنامه‌های امنیتی مورد نیاز، تشکیلات لازم برای برپایی و تداوم امنیت اطلاعات خود را نیز ایجاد نماید. برخی از برتری‌های اجرایی مدیریت امنیت فاوا در سازمان عبارتند از:

۱. مدیریت قانونمند امنیت اطلاعات و ارتباطات به‌طور یکپارچه و در تمامی سطوح سازمانی. اطمینان از برقراری هماهنگی بین هدف‌های امنیتی در همه واحدهای عملیاتی یک سازمان. در اختیار قرار دادن مجموعه جامعی از سیاست‌های امنیتی.

۲. مدیریت هزینه‌های زیرساخت: فرآیند مدیریت خطرات امنیتی، به سازمان‌ها کمک می‌کند که با یک وضعیت مطلوب، مقرون‌به‌صرفه و در یک سطح قابل قبول امنیتی فعالیت‌های خود را انجام دهند.

انتخاب استاندارد و چارچوب‌های امنیت فاوا برای سازمان از مهم‌ترین گام‌های اولیه امنیتی است که می‌بایست با وسواسی خاص انجام شود و گام بعدی اجرا و ارزیابی پی‌درپی این چارچوب است که می‌تواند تضمین‌کننده امنیت نسبی اطلاعات در سازمان باشد. برای این منظور می‌بایست قبل از پیاده‌سازی هر سامانه امنیتی میزان اثربخشی و قابلیت‌های آن به‌منظور برابره با تهدیدها سنجیده و با مقایسه با سایر چارچوب‌ها تصمیم‌سازی صحیح و دقیقی برای مدیران تصمیم‌گیر سازمان انجام شود.

با توجه به اهمیت فناوری اطلاعات و ارتباطات در عصر کنونی و رشد نامتوازن ساختار فناوری اطلاعات، این بستر به یکی از نقاط آسیب‌پذیر و خطرناک جهان بدل شده که ضرورت توجه و اقدام سریع و نیز نظام‌مند و هدفمند برای مصون‌سازی این بستر از تهدیدهای موجود برای

حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و درگیری‌های بین‌المللی را می‌طلبد.

مالکیت فناوری اطلاعات در اختیار حریفان است و این عامل باعث شده که آنان در شرایط برتری اطلاعاتی قرار گیرند. به‌دلیل برتری حریفان و تهدیدهای آتی به‌نظر می‌رسد توجه به اصول پدافند غیرعامل در برابر تهدیدهای این حوزه بسیار کارساز خواهد بود و تعیین الزامات، ملاحظات و راهبردهای پدافند غیرعامل در حوزه فناوری اطلاعات به‌منظور پایداری زیرساخت‌های حیاتی در برابر تهدیدهای مربوطه ضروری است (خوش‌عمل، ۱۳۹۱: ۸).

در عصر اطلاعات شاهد شکل‌گیری فضایی هستیم که در آن فعالیت‌های گوناگونی همچون اطلاع‌رسانی، داده‌ورزی، کسب‌وکار، مدیریت، واپایش و ارتباطات، به‌وسیلهٔ سازوکارهای الکترونیکی و مجازی انجام می‌پذیرد. این فضا که از آن با نام «فضای تولید و تبادل اطلاعات» یاد می‌شود، دربرابر چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی مانند ارتکاب جرائم سازمان‌یافته، تخریب بانک‌های اطلاعاتی، حمله‌های مختل‌کننده خدمات، جاسوسی، خرابکاری، شکستن حریم خصوصی و حقوق مالکیت معنوی قرار دارد؛ به‌طوری‌که توجه نکردن یا انتخاب رویکرد نادرست به امنیت این فضا، مانعی بزرگ پیش‌روی گسترش کاربرد فناوری ارتباطات و اطلاعات و ورود به جامعه دانش‌پایه خواهد بود. بسیاری از کشورها به‌سبب اهمیت این فضا، فعالیت عمده خود را به ایجاد امنیت نسبی روی این فضا متمرکز نموده‌اند.

سازمان‌های امروزی و ازجمله سازمان مدیریت‌وبرنامه‌ریزی کشور با توجه به داشتن اطلاعات ارزشمندی که در پیکره آن در جریان است، می‌تواند کانون توجه حریفان برای مقاصد کینه‌توزانه قرار گیرد که لازم است به‌طور ویژه پیش‌بینی‌های برابره‌ای لازم برای حفظ و پاسداری از اطلاعات آن انجام شود.

پیشینه

تاج‌فر و دیگران (۱۳۹۳)، در پژوهشی در شرکت نفت ج.ا.ا با عنوان «رتبه‌بندی موانع پیاده‌سازی سامانه مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف» میزان آمادگی مدیریت اکتشاف را برای پیاده‌سازی سامانه مدیریت امنیت اطلاعات ازلحاظ(مدیریتی، آموزشی، ساختاری، فردی، فرهنگی) کمتر از حد ماز سوی ارزیابی کرده‌اند.

مجتبی بهرامی (۱۳۹۰)، در پژوهشی با عنوان «ارائه روشی مناسب برای بهبود و توسعه شاخص‌های مدیریت امنیت اطلاعات جهت طراحی و پیاده‌سازی در سازمان‌ها» الگویی براساس استاندارد بی‌اس ۷۷۹۹ [1] و ایزو ۲۷۰۰۱ [2] و چرخه ایمن‌سازی آن با عنوان طرح آی‌پی‌دی‌سی‌ای [3] ارائه نموده است که شامل مراحل اولیه(صفر)، طرح و پیاده‌سازی، اجرا، نظارت و ارزیابی و نگهداری و بهبود است؛ که با اجرای آن در بیش از صدوبیست ایستگاه و به‌مدت شش ماه، عملکرد تأمین امنیت آن را بیش از نودوپنج درصد ارزیابی کرده است.

پژوهش نخست، ازآنجاکه یکی از مهم‌ترین سازمان‌های راهبردی کشور ارزیابی شده است قابل بهره‌برداری است. پژوهش بعدی نیز ازآنجاکه روشی بومی شده براساس استانداردهای امنیت اطلاعات ارائه نموده است قابل بررسی و بهره‌برداری است.

با توجه به کمبود پژوهش‌های صورت گرفته در این حوزه و در حوزه پدافند غیرعامل (امنیت فناوری اطلاعات)؛ این پژوهش اثربخشی سامانه مدیریت امنیت اطلاعات را در حوزه پدافند غیرعامل ارزیابی کرده است.

هدف، سؤال و فرضیه

هدف اساسی این موضوع، بررسی و ارزیابی اثربخشی سامانه مدیریت امنیت اطلاعات در پدافند غیرعامل (امنیت فاوا) است.

1.Bs7799
2.Iso27001
3.IPDCA

در این بین به این سؤال پاسخ داده خواهد شد که آیا سامانه مدیریت امنیت اطلاعات، در پدافند غیرعامل (امنیت فناوری اطلاعات و ارتباطات) اثربخش است؟

بنابراین فرضیه پژوهش بر این بنا نهاده شد که سامانه مدیریت امنیت اطلاعات، در تأمین هدف‌های پدافند غیرعامل(امنیت فناوری اطلاعات و ارتباطات)، اثربخش است.

مفاهیم و مبانی نظری

فناوری اطلاعات و ارتباطات: واژه فناوری اطلاعات و ارتباطات بیانگر پویایی به‌دست آمده از همگرایی سامانه‌های رایانه‌ای و مخابراتی است که تبادل سریع و جهانی اطلاعات را فراهم می‌آورد و ظرفیت دگرکون‌سازی فرآیندهای کاری به خدمات و مانند آن را دارد؛ به‌همین علت برخی «فناوری اطلاعات» و «فناوری اطلاعات و ارتباطات» را یکسان می‌دانند و فقط برای تأکید بیشتر بر ارتباطات و مخابرات و برجسته‌تر نمودن آن، از واژه «فناوری اطلاعات و ارتباطات» استفاده می‌کنند (مؤسسه آموزشی و پژوهشاتی صنایع دفاعی، ۱۲:۱۳۸۴).

زیرساخت اطلاعات[1]: شامل تسهیلات فیزیکی، خدمات و مدیریت است که از تمامی منابع پردازش مشترک در سازمان پشتیبانی می‌کند. پنج جزء اصلی زیرساخت عبارت‌اند از: سخت‌افزار، نرم‌افزار، شبکه‌ها و امکانات ارتباطی(شامل اینترنت و شبکه‌های داخلی)، پایگاه داده و کارکنان مدیریت اطلاعات. زیرساخت تمامی این منابع به‌اضافه یکپارچگی، عملیات، مستندسازی، نگهداری و مدیریتشان را دربر می‌گیرد (توربان، ۱۱۷:۱۳۸۶).

امنیت اطلاعات[2]: برای بسیاری از سازمان‌ها، امنیت اطلاعات مهم‌ترین چالشی است که فناوری اطلاعات با آن روبرو است. امنیت اطلاعات دارای چند وجه است؛ ولی هدف اصلی آن، پیاده‌سازی سه اصل: محرمانگی، درستی و دسترس‌پذیری به دارایی‌های اطلاعاتی یک سازمان است (Murphy et al.,2000: 31).

1. Information Infrastructure
2. Information Security

پدافند غیرعامل: مجموعه اقدامات غیرمسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در برابر تهدیدهای و اقدامات نظامی دشمن می‌گردد (اسکندری، ۳۳:۱۳۸۹).

دفاع غیرعامل درواقع مجموعه اقدامات، طرح‌ها و پیش‌بینی‌هایی است که توان دفاعی سامانه را افزایش داده و پیامدهای حوادث و بحران‌ها را کاهش دهد و همچنین امکان بازیابی سامانه‌های آسیب‌دیده را با کمترین هزینه ممکن فراهم سازد. با توجه به گستردگی روزافزون سامانه‌های فناوری اطلاعات و ارتباطات، این بستر به یکی از نقاط آسیب‌پذیر تبدیل شده است که باید در اجرای اقدامات دفاع غیرعامل به‌منظور تأمین امنیت ملی و حریم خصوصی شهروندان توجه ویژه‌ای به آن شود . این اقدامات در حوزه‌ها و سطوح مختلف سبب توسعه ظرفیت دفاع الکترونیکی کشور می‌گردد. در حوزه فناوری اطلاعات و ارتباطات، اجزای مختلف دفاع غیرعامل تعاریف ویژه‌ای پیدا می‌کنند. این اجزاء عبارت‌اند از:

۱. تأمین امنیت و اطمینان یافتن از صحت، دسترس‌پذیری و حفظ محرمانگی داده‌ها و اطلاعات الکترونیکی طبقه‌بندی شده.

۲. ایمن‌سازی زیرساخت‌های شبکه‌ای و بسترهای ارائه خدمات نوین الکترونیکی در برابر تهدیدهای جنگی سخت و نیمه‌سخت.

۳. اطمینان یافتن از پایداری و خلل‌ناپذیری در فعالیت بسترهای شبکه‌ای مدیریت، واپایش و ارائه خدمات عمومی کشور (پور ابراهیمی و بنائی، ۱۳۸۹: ۲۰).

اصول پدافند غیرعامل: اصول دفاع غیرعامل یا پدافند غیرعامل مجموعه اقدامات بنیادی و زیربنایی است که در صورت به‌کارگیری می‌توان به هدف‌های پدافند غیرعامل همچون، تقلیل خسارات و صدمات، کاهش قابلیت و توانایی سامانه‌های شناسایی و آشکارساز، هدف‌یابی و دقت هدف‌گیری جنگ افزارهای آفندی دشمن و تحمیل هزینه بیشتر به وی دست یافت. این اصول

عبارتند از: مکان‌یابی، استتار، اختفا، پوشش، فریب، پراکندگی، تفرقه و جابجایی، مقاوم‌سازی و استحکامات و اعلام خبر (موحدی نیا، ۷۲:۱۳۸۶).

چارچوب نظری

در دنیای امروز اطلاعات نه‌تنها به‌عنوان یکی از منابع و دارایی‌های اصلی سازمان شناخته می‌شوند، بلکه وسیله و ابزاری برای مدیریت اثربخش بر سایر منابع و دارایی‌های سازمان (منابع مالی، نیروی انسانی، غیره) نیز قلمداد می‌شود و از اهمیت و ارزش ویژه‌ای برخوردار است؛ اما این ارزش‌ها تنها درصورتی دست‌یافتنی خواهد بود که اطلاعات بتواند در زمان مناسب، با کیفیت مطلوب و امنیت قابل قبول در اختیار افراد مناسب قرار گیرد و ارتباطات به‌صورت مطلوب و بهینه در سازمان برقرار گردد (ریاضی، ۱۳۸۸: ۴).

اطلاعات مانند خونی است که در رگ‌های سازمان جاری است؛ بدون این اطلاعات مسؤلان سازمان‌ها یا هیئت مدیره نمی‌تواند تصمیم‌های کلیدی بگیرد. قسمت‌های خرید، مالی و کارکنان نمی‌توانند منابع مورد نیاز خود را برای ادامه حیات سازمان به‌دست آورند. هر سازمان که داده‌های صحیح، به‌هنگام و جامع را در اختیار داشته باشد، موفق‌تر است. نقش داده و اطلاعات در مدیریت سازمان‌ها نقش حیاتی و اساسی است. هر چه فضای اطلاعاتی یک سازمان دقیق‌تر، منسجم‌تر و نظامندتر باشد، سازمان بهتر می‌تواند به هدف‌هایش دست یابد. بنابراین امروزه، اطلاعات به‌عنوان منبع مهم راهبردی برای سازمان‌ها مطرح است.

سازمان و فناوری اطلاعات: ارتباطی دوسویه میان فناوری اطلاعات و سازمان وجود دارد. فناوری اطلاعات و سامانه های اطلاعاتی باید با سازمان همراه شوند تا بتوانند اطلاعات مورد نیاز گروه‌های خاص از اعضای سازمان را فراهم نمایند و سازمان نیز باید از تأثیر اطلاعات آگاه باشد و درهای خود را روی آن بگشاید تا از امتیازهای دانش فنی نوین بهره‌مند گردد. سامانه‌های اطلاعاتی بر سازمان اثر می‌گذارند و در طراحی سامانه‌های اطلاعاتی نیز باید نیازهای سازمان را درنظر داشت.

کاسته شدن از اهمیت عناصر محیطی در روابط بین‌الملل، تغییر در مفهوم ژئوپلیتیک را نیز به‌همراه داشته است. این مفهوم به‌طور سنتی، بر پایهِ عناصر فضا و مکان، مانند دسترسی به دریا، وجود مرزهای طبیعی و واپایش تسهیلات ارتباطی عمده استوار بوده است. هرچند اهمیت ابعاد جغرافیا و ژئوپلیتیک همچنان پابرجاست، اما فناوری اطلاعات به‌دلیل فراهم آوردن ارزش‌ها و قدرت غیرمادی از اهمیت عامل مکانی کاسته است. اهمیت جایگاه ژئوپلیتیک یک کشور با مجموعه ارزش‌های تازه‌ای که با مدیریت اطلاعات و جایگاه آن در ساختارهای زیربنایی اطلاعات جهانی به‌دست می‌آید ارزیابی می‌شود (jan, 1399:171).

انواع تهدیدهای فاوا: تقسیم‌بندی‌های مختلفی از تهدیدهای سامانه‌های اطلاعاتی، انجام شده است. این تهدیدهای به دو دسته عمدی و غیرعمدی طبقه‌بندی می‌شود (توربان، ۱۱۵:۱۳۸۶).

تهدیدهای غیرعمدی شامل خطاهای انسانی، مخاطرات محیطی، اختلالات سامانه‌های رایانه‌ای است. بسیاری از مشکلات رایانه‌ای در اثر خطاهای انسانی ایجاد می‌شوند. این خطاها می‌توانند در طراحی سخت‌افزاری، نرم‌افزاری یا سامانه‌ای اطلاعات رخ دهد. آن‌ها می‌توانند در برنامه‌نویسی آزمایشی، جمع‌آوری یا ورود داده‌ها، صدور مجوز و دستورالعمل‌ها ایجاد شوند. در بیشتر(حدود پنجاه‌وپنج 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، انفجارها می‌باشند. اختلالات سامانه‌های رایانه‌ای، می‌تواند درنتیجه ساخت ضعیف یا استفاده از مواد نامناسب در ساخت، رخ دهد (توربان، ۱۱۵:۱۳۸۶).

پدافند غیرعامل در حوزه فناوری اطلاعات: پدافند غیرعامل در حوزه فناوری اطلاعات عامل تضمین امنیت، ایمنی و پایداری زیرساخت‌های حوزه فناوری اطلاعات است؛ که باعث کاهش آسیب‌پذیری‌ها و افزایش آستانه تحمل در رویارویی با تهدیدهای این حوزه می‌شود؛ که این امر با تأکید بر ایجاد عزم ملی با فرهنگ‌سازی، سیاست‌گذاری، طرح‌ریزی و برنامه‌ریزی، هدایت

راهبردی و تدوین و تصویب ضوابط و دستورالعمل‌های عمومی– تخصصی و نظام‌های هدایت بخش کشوری به‌منظور نهادینه نمودن رعایت اصول پدافند غیرعامل در حوزه فناوری اطلاعات و نظارت بر اجرای آن با ایجاد قابلیت به‌روزرسانی امکان‌پذیر می‌شود (دوست محمدیان و دیگران، ۱۳۹۲: ۳۰۲). لازمه یک دفاع موفق در جنگ سایبر همانا بالا بردن سطح امنیتی عناصر درگیر است و این مهم جز با افزایش دانش در حوزه مجازی(سایبر) امکان‌پذیر نخواهد بود.

با رشد و توسعه فزاینده فناوری اطلاعات و گسترش شبکه‌های ارتباطی، آسیب‌پذیری فضای تبادل اطلاعات افزایش یافته است و روش‌های بروز تهدیدهای یادشده گسترده‌تر و پیچیده‌تر می‌شود. ازاین‌رو حفظ ایمنی فضای تبادل اطلاعات ازجمله مهم‌ترین هدف‌های توسعه فناوری اطلاعاتی و ارتباطی قلمداد می‌شود. به‌موازات پیش‌بینی‌های فنی انجام شده لازم است در قوانین و سیاست‌های جاری متناسب با جایگاه نوین فضای تبادل اطلاعات در امور مدیریتی و اطلاع‌رسانی تجدید نظر شده و فرهنگ صحیح به‌کارگیری امکانات یادشده نیز در سطح جامعه ترویج داده شود. بدیهی است که توجه نکردن به تأمین امنیت فضای تبادل اطلاعات و برخورد نادرست با این موضوع مانع از گسترش این فضا در میان مردم جامعه و جلب اعتماد مدیران در به‌کارگیری روش‌های نوین نظارتی و اطلاع‌رسانی خواهد شد. ایجاد یک نظام منسجم در سطح ملی با درنظرگرفتن ویژگی‌های خاص فضای تبادل اطلاعات و امنیت در این فضا یک ضرورت است (پورمند، ۱۳۸۶: ۲).

براساس استانداردهای امنیتی قابل قبول، هر یک از عناصر درگیر در فضای سایبر، باید به اندازه ارزش خود حفاظت گردند. در غیر این صورت، انتخاب سازوکارهای دفاعی چندان بهینه نخواهد بود و بدون شک دارای هزینه‌های غیرضروری است. بدیهی است آن‌هایی که قصد حمله داشته باشند تا دندان مسلح می‌شوند. پس باید ابتدا دارایی‌ها و عناصر اصلی و اساسی اطلاعاتی اشیاء مهم در فضای سایبری را تعریف و تعیین نموده و براساس سیاست‌های کلان و

با درنظر گرفتن تمامی تهدیدها، پیش‌بینی‌های دفاعی را پی‌ریزی نماییم (دوستمحمدیان و دیگران، ۱۳۹۲: ۲۲۳).

بسیاری از سازمان‌ها به‌دنبال ایجاد سامانه‌های امنیتی برای جلوگیری از نشت اطلاعات به بیرون می‌باشند تا بتوانند کل مجموعه خود را حفظ کنند؛ در این راستا ایجاد یک سامانه امنیتی قوی می‌تواند برای حفظ امنیت اطلاعات هر سازمان مؤثر باشد. سامانه‌ای که براساس نیازهای سازمان و میزان اهمیت اطلاعات در آن طراحی شده باشد و از تأمین سرمایه‌های اطلاعاتی حفاظت نماید. به‌طور مسلم نمی‌توان تنها به یک نوع خاص از امنیت برای محافظت از اطلاعات سازمان بسنده نمود. همچنین برای حفاظت از سامانه‌های شبکه‌ای و رایانه‌ای خود نمی‌توانید فقط به یک مرسیدن‌بهبسنده کنید. متأسفانه بعضی از سازندگان ادعا می‌کنند که تولیدات آنها چنین خاصیتی دارد. حقیقت این است که یک مرسیدن‌به هیچ‌گاه نمی‌تواند امنیتی کامل برای سازمان به‌همراه داشته باشد. انواع مختلفی از محصولات برای حفاظت کامل از دارایی‌های اطلاعاتی سازمان مورد نیاز است (میوالد، ۱۳۸۵: ۱۲). سامانه مدیریت امنیت اطلاعات ابزاری مناسب در این راستا برای طراحی و واپایش امنیت اطلاعات است که در این پژوهش بررسی می‌شود.

سامانه مدیریت امنیت اطلاعات: هدف از مدیریت امنیت اطلاعات در یک سازمان، حفظ سرمایه‌های (نرم‌افزاری، سخت‌افزاری، اطلاعاتی‌وارتباطی و نیروی انسانی) آن در برابر هرگونه تهدید(شامل: دسترسی غیرمجاز به اطلاعات، خطرات ناشی از محیط و سامانه و خطرات ایجاد شده از سوی کاربران) است و برای رسیدن به این هدف، نیاز به یک برنامه منسجم است (POA ،2003: 34).

با پیدایش اولین استاندارد مدیریت امنیت اطلاعات در ۱۹۹۵، نگرش سامانمند به ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. براساس این نگرش، تأمین امنیت فضای تبادل اطلاعات در

سازمان‌ها، به یک‌باره امکان‌پذیر نیست و لازم است به‌صورت مداوم در یک چرخه ایمن‌سازی شامل مراحل طراحی، پیاده‌سازی، ارزیابی و اصلاح انجام گیرد (الفت و دیگران،۱۳۹۰: ۳).

دلیل اصلی اجرای طرح تدوین دستورالعمل‌های مدیریت امنیت اطلاعات انجام حرکتی بنیادی برای استانداردسازی فعالیت‌های جاری در حوزه فناوری اطلاعات و ارتباطات است و مبتنی بر سند چشم‌انداز بیست‌ساله جمهوری اسلامی ایران است (ریاضی، ۱۳۸۸: ۳).

مدیریت امنیت اطلاعات برای ایجاد امنیت در پیدایش و تبادل اطلاعات و همچنین دادوستد فیزیکی، براساس یک سامانه مدیریتی برپایه استانداردهایی همچون بی اس ۷۷۹۹، ایزو آی‌ای‌سی۲۷۰۰۱ و گزارش فنی ایزو آی‌ای‌سی[1]، که از برجسته‌ترین استانداردها و راهنماهای فنی در این زمینه قلمداد می‌شوند کار می‌کند (Broderick, 2006:26-31) .

سامانه مدیریت امنیت اطلاعات درواقع بخشی از سامانه مدیریت کلی و سراسری در یک سازمان است که بر پایه رویکرد مخاطرات کسب‌وکار قرار دارد و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگهداری و بهبود امنیت اطلاعات است. سامانه مدیریت امنیت اطلاعات درمجموع یک رویکرد نظام‌مند به مدیریت اطلاعات حساس به‌منظور محافظت از آن‌هاست (پورمند، ۱۳۸۷: ۴).

از مهم‌ترین عوامل لازم برای پیاده‌سازی سامانه مدیریت امنیت اطلاعات می‌توان به زیرساخت‌های لازم در این زمینه، پشتوانه مدیریتی و نیروی انسانی متخصص اشاره کرد. ازجمله دلایلی که مانع پیاده‌سازی این سامانه در سازمان‌ها می‌شود، نبود زیرساخت‌های فناوری اطلاعات در سازمان‌هاست (الفت و دیگران، ۱۳۹۰: ۵). برای سامانه مدیریت امنیت اطلاعات ویژگی‌های گوناگونی بیان شده است؛ برای مثال گفته شده است که باید مدیریت آن متمرکز باشد و واحد و فرایندهایی مجزا از سایر بخش‌های سازمانی(به‌ویژه بخش فناوری اطلاعات) داشته باشد؛ البته باید هماهنگی و هم‌راستایی میان قسمت‌های گوناگون نیز حفظ

1. ISO/IEC TR 13335

شـود (Ernest-Jones, 2006:8-13). همچنـین تأکیـد شـده اسـت کـه رویکـرد صـحیح بایـد تکرارشونده، نظام‌مند، کامل، سازگار و آسان برای درک و تجزیه‌وتحلیل باشد. ویژگی دیگر آنکه رویکرد مدیریت امنیت، باید تعادلی میان حفاظت اطلاعات و دسترسی مجاز باشـد. نکتـه مهـم این است که مدیریت امنیت اطلاعات بایـد در تمـام سـطوح سـازمانی(راهبـردی، راهکنشـی و عملیاتی) مدیریت شود و واپایش‌های لازم انجام شـود. همچنـین بهتـر اسـت مـدیریت امنیـت اطلاعات به‌صورت فرایندی مداوم اجرا شود و شناسایی، ارزیابی و پیاده‌سازی را برای همه اجزاء دربرگیرد (تاج‌فر و دیگران، ۱۳۹۳: ۳). همچنین چارچوب امنیت باید به‌گونه‌ای باشـد کـه اجـرایش آسان، کم‌هزینه و مناسب با نیازهای تجارت الکترونیکی باشد (Zuccato 2007: 256-265).

در زمینه امنیت اطلاعات، کشورهای زیادی هستند که سازمان‌های استاندارد خود را موظف بـه تعریف یک استاندارد ملی کرده‌اند. کشورهایی همچون استرالیا، ایالات‌متحده آمریکا، بریتانیـا و کانادا را می‌توان ازجمله کشورهایی دانست که در تعریف استاندارد امنیـت اطلاعـات قـدم‌هـای موفقی برداشته‌اند. همه این استانداردها در مواردی با هم همخوانی دارند اما وجـه تمـایز همـه آنها در این است که استانداردها براساس قوانین رایج کشور خودشان تعریـف شـده اسـت. تنهـا یک استاندارد بین‌المللی وجود دارد که در زمینهٔ امنیت، سازمان‌هـا را ملـزم بـه رعایـت قـانون کشور خاصی نمی‌کند. سازمان بین‌المللی استاندارد[1] پیروی از قوانین را لازم می‌داند اما پیـروی از یک قانون خاص را به‌عهده سازمان می‌گـذارد. در ج.ا.ایـران نیـز سـازمان اسـتاندارد ج.ا.ا[2] در زمینه امنیت، استانداردهای تعریف شده ازسوی سازمان بـین‌المللـی اسـتاندارد را بـومی‌سـازی می‌کند و در اختیار سازمان‌ها قرار می‌دهد.

استانداردهای مدیریت امنیت اطلاعات: در حال حاضر، مجموعه‌ای از استانداردهای مدیریتی و فنی امنیت اطلاعات ارتباطات، ارائه شده است که استاندارد مـدیریتی بـی‌اس۷۷۹۹ [3] مؤسسـه

1.International Organization for Standardization(ISO)
2.International Organization for Standardization Islamic Republic Of Iran(ISIRI)
3.BS7799

استاندارد انگلیس، استاندارد مدیریتی ایزو آی‌ای‌سی ۱۷۷۷۹ [1] و گزارش فنی ایزو تی‌آر [2] مؤسسه بین‌المللی استاندارد، از برجسته‌ترین استانداردها و راهنماهای فنی قلمداد می‌شود. در این استانداردها، نکات زیر مورد توجه قرار گرفته شده است (دوست‌محمدیان و فاضلی، ۱۳۹۲: ۱۰۵).

- تعیین مراحل ایمن‌سازی و چگونگی شکل‌گیری چرخه امنیت.
- جزئیات مراحل ایمن‌سازی و روش‌های فنی مورد استفاده در هر مرحله.
- فهرست و محتوای طرح‌ها و برنامه‌های امنیت مورد نیاز سازمان.
- ضرورت و جزئیات ایجاد تشکیلات سیاست‌گذاری، اجرایی و فنی تأمین امنیت.
- واپایش‌های امنیتی مورد نیاز برای هر یک از سامانه‌های اطلاعاتی و ارتباطی.

در سال ۲۰۰۰، بخش اول استاندارد بی اس ۷۷۹۹:۲ بدون هیچ‌گونه تغییری ازسوی مؤسسهٔ بین‌المللی استاندارد به‌عنوان استاندارد ایزو آی‌ای‌سی۱۷۷۹۹ منتشر شد؛ اما این استاندارد نارسایی‌هایی داشت. چراکه قابل گواهی نبود. ازآنجاکه ۱۷۷۹۹فقط یک مجموعه گردآوری شده از توصیه‌های امنیتی بود، هیچ الزامی دربر نداشت که برای گواهی شدن سازمان‌ها را مجبور به اجرای آن کند. این نارسایی در استاندارد ایزو ۲۰۰۵[3] برطرف شده است (دبیرخانه شورای عالی امنیت فضای تبادل اطلاعات کشور،۱۳۸۳: ۱۳). استانداردهای سامانه مدیریت امنیت اطلاعات متنوع و با موضوع‌های کاری مشخص می‌توانند به سازمان‌ها کمک کنند. حوزه فعالیت آنها به‌شرح زیر است (بهرامی، ۱۳۹۰: ۲).

- بازبینی و لغت‌نامه سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی/۲۰۰۹
- الزامات سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی۲۷۰۰۵: ۲۰۰۵
- نیازمندی‌های سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی۲۷۰۰۱: ۲۰۰۵

1.ISO/IEC 17799
2.ISO/IEC TR 13335
3.ISO/IEC 27001:2005

- آئین‌نامه کاری سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی۲۷۰۰۲: ۲۰۰۵
- راهنمای پیاده‌سازی سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی۲۷۰۰۳
- اندازه‌گیری و سنجش سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی۲۷۰۰۴
- مدیریت خطر سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی۲۷۰۰۵ :۲۰۰۸
- نیازمندی‌های ممیزها و ارائه‌دهندگان گواهینامه‌های سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی۲۷۰۰۶ : ۲۰۰۷
- راهنمای ممیزی سامانه مدیریت امنیت اطلاعات ایزو آی‌ای‌سی۲۷۰۰۷
- راهنمای سامانه مدیریت امنیت اطلاعات برای سازمان‌های مخابراتی براساس ایزو آی‌ای‌سی۲۷۰۱۱: ایزو آی‌ای‌سی۲۷۰۰۲.

تجزیه‌وتحلیل داده‌ها

- اطلاعات جمعیت‌شناختی:

جدول ۱ - توزیع جامعه آماری برحسب جنسیت پاسخگویان

جنسیت	فراوانی	درصد فراوانی
مرد	۲۵	۸۳/۳
زن	۵	۱۶/۷
جمع	۳۰	۱۰۰

جدول ۲ - توزیع درصد جامعه آماری برحسب سن پاسخگویان

سن	فراوانی	درصد فراوانی
۲۰-۳۰	۵	۱۶/۷
۳۱-۴۰	۱۶	۵۳/۳
۴۱-۵۰	۶	۲۰
۵۱-۶۰	۳	۱۰
جمع	۳۰	۱۰۰

جدول ۳ - توزیع درصد جامعه آماری برحسب رتبه علمی پاسخگویان

رتبه علمی	فراوانی	درصد فراوانی
مربی	۹	۳۰
استادیار	۴	۱۳/۳
دانشیار	۵	۱۶/۷
استاد	۰	۰
بدون پاسخ	۱۲	۴۰
جمع	۳۰	۱۰۰

جدول ۴ - توزیع درصد جامعه آماری برحسب سمت سازمانی پاسخگویان

سمت سازمانی	فراوانی	درصد فراوانی
مدیر	۱۵	۵۰
کارشناس	۱۴	۴۶/۷
کارمند	۱	۳/۳
جمع	۳۰	۱۰۰

• نتایج آمار توصیفی و استنباطی داده‌ها:

پژوهشگر نظرهای جامعه آماری را دربارهٔ اثربخشی سامانه مدیریت اطلاعات در پدافند غیرعامل در یازده بخش زیر (برگرفته از استاندارد ایزو آی‌ای‌سی۲۷۰۰۲) جمع‌آوری و سپس با استفاده از آزمون تی تک‌نمونه‌ای تحلیل و ارزیابی کرده است؛ و در پایان نتایج نهایی را در بخش نتیجه‌گیری ارائه می‌کند.

۱-داشتن خط‌ومشی امنیتی ۲- داشتن ساختار سازمانی برای امنیت اطلاعات ۳- مدیریت دارایی‌ها ۴- امنیت منابع انسانی ۵- امنیت فیزیکی و محیطی ۶- مدیریت عملیات و ارتباطات ۷- واپایش دسترسی ۸- نگهداری، مراقبت و توسعه سامانه‌های اطلاعاتی ۹- مدیریت حوادث مربوط به امنیت اطلاعات ۱۰- مدیریت تداوم کسب‌وکار ۱۱- سازگاری

در اینجا به‌عنوان نمونه، تجزیه‌وتحلیل داده‌های به‌دست‌آمده از سؤال چهارم ارائه می‌شود.

•تجزیه‌وتحلیل و آزمون سؤال چهارم:

سؤال چهارم (ارزیابی اثربخشی امنیت نیروی انسانی در امنیت فاوا):

با توجه به تی به‌دست‌آمده در آزمون تی تک‌نمونه‌ای(t = ۵/۱۸) که میانگین تجربی(x = ۳/۶) را با میانگین نظری(Test Value = ۳) مقایسه کرده است می‌توان دریافت که مقدار t به‌دست‌آمده از نظر آماری معنی‌دار است. با توجه به اینکه میانگین تجربی از میانگین نظری بیش‌تر است می‌توان گفت امنیت منابع انسانی به‌میزان بسیار زیادی در تأمین امیت فاوا و به‌طورکلی در پدافند غیرعامل اثربخش است.

اما با مراجعه به داده‌های به‌دست‌آمده از جدول زیر در رابطه با متغیر امنیت منابع انسانی در بررسی تک‌تک سؤال‌های مربوط به مدیریت دارایی‌ها می‌توان مشاهده کرد که مقدار t تک‌نمونه‌ای برای سؤال ۲۵ و ۲۶ مقدار ۰/۶۴ و ۱/۷۷ است و با توجه به سطح معنی‌داری بالای ۰/۰۵ می‌توان نتیجه گرفت که تفاوت آماری معنی‌داری بین دو میانگین واقعی و مفروض وجود ندارد و این گویه به مقدار بسیار کمی در تأمین امیت فاوا و به‌طورکلی در پدافند غیرعامل اثربخش است.

جدول ۵ - آزمون t در رابطه باسؤال چهارم

Test Value = ۳					
متغیر	N	Mean	Mean Difference	t	Sig. (2-tailed)
سؤال ۱۹	۳۰	۳/۶	۰/۶	۲/۹۸	۰/۰۰۶
سؤال ۲۰	۳۰	۳/۷	۰/۷	۵/۱۱	۰/۰۰۰
سؤال ۲۱	۳۰	۳/۷	۰/۷۳	۴/۶۲	۰/۰۰۰
سؤال ۲۲	۳۰	۳/۵	۰/۵	۳/۳۴	۰/۰۰۲

سؤال ۲۳	۳۰	۳/۸	۰/۷۶	۳/۴۳	۰/۰۰۲
سؤال ۲۴	۳۰	۳/۶	۰/۵۶	۳/۸	۰/۰۰۱
سؤال ۲۵	۳۰	۳/۶	۰/۳۳	۱/۷۷	۰/۰۸
سؤال ۲۶	۳۰	۳/۱	۰/۱۳	۰/۶۴	۰/۵۲
سؤال ۲۷	۳۰	۳/۶	۰/۵۷	۲/۵۹	۰/۰۱۵
امنیت منابع انسانی	۳۰	۳/۶	۰/۶۳	۵/۱۸	۰/۰۰۰

نتیجه‌گیری و پیشنهادها

سامانه مدیریت امنیت اطلاعات براساس استاندارد ایزو آی‌ای‌سی۱۷۷۹۹: ۲۰۰۵ کارکرد و اثربخشی پدافند غیرعاملی دارد. این استاندارد یکصدوسی‌وسه شاخص واپایشی فهرست‌شده دارد که در تحلیل داده‌های پرسش‌نامه این پژوهش مشخص شد. از این یکصدوسی‌وسه واپایش فهرست‌شده یکصدودو فهرست واپایش‌شده دارای کارکرد پدافند غیرعاملی است و سی‌ویک فهرست واپایش‌شده کارکرد پدافند غیرعاملی ضعیفی دارند (فهرست‌های واپایش‌شده‌ای که کارکردی ماز سوی و ماز سوی به پایین دارند، کارکردشان صفر درنظر گرفته شده است). برای این منظور هدف‌های واپایشی زیر هدف‌گذاری می‌گردند:

۱.وجود خط‌مشی امنیتی: دو شاخص واپایشی فهرست‌شده دارد که هدف و هر دو شاخص فهرست‌شده آن در تأمین پدافند غیرعامل (امنیت فاوا) اثربخش است.

۲.ساختار سازمانی: یازده شاخص واپایشی فهرست‌شده دارد که هدف و ده شاخص فهرست‌شده آن در تأمین پدافند غیرعامل (امنیت فاوا) اثربخش است. در بین شاخص‌های فهرست‌شده، شاخص فهرست‌شده مرور مستقل امنیت اطلاعات، اثربخشی ضعیفی در پدافند غیرعامل (امنیت فاوا) دارد.

۳.مدیریت دارایی‌ها: پنج شاخص واپایشی فهرست‌شده دارد که هدف و چهار شاخص فهرست‌شده به اندازه بسیار زیادی در تأمین پدافند غیرعامل (امنیت فاوا) اثربخش است. در بین واپایش‌های فهرست‌شده، واپایش مالکیت دارایی‌ها به‌وسیله واحد مشخصی در سازمان، اثربخشی لازم را در تأمین پدافند غیرعامل (امنیت فاوا) ندارد.

۴.امنیت منابع انسانی: نه شاخص واپایش فهرست‌شده دارد که هدف و هفت شاخص فهرست‌شده به اندازه بسیار زیادی در تأمین پدافند غیرعامل (امنیت فاوا) اثربخش است. در بین شاخص‌های فهرست‌شده، واپایش‌های «فرایند مسؤلیت‌های تغییر یا خاتمه کار کارمندان» و «فرایند بازگشت دارایی‌ها ازسوی کارمندان و پیمانکاران بعد از پایان استخدام یا قرارداد» اثربخشی ضعیفی در پدافند غیرعامل (امنیت فاوا) دارد.

۵.امنیت فیزیکی و محیطی: سیزده شاخص واپایشی فهرست‌شده دارد که هدف و ده شاخص فهرست‌شده به اندازه زیادی در پدافند غیرعامل (امنیت فاوا) اثربخش است. در بین واپایش‌های فهرست‌شده شاخص‌های «واپایش و حفاظت از محیط‌های دسترسی عمومی، تحویل و بارگیری»، «ایمن نمودن موارد مصرفی یا استفاده دوباره از تجهیزات» و «از بین بردن اموال (تجهیزات، اطلاعات و یا انتقال به خارج از سازمان)» اثربخشی لازم را در تأمین پدافند غیرعامل (امنیت فاوا) ندارد.

۶.مدیریت عملیات و ارتباطات: سی‌ودو شاخص واپایشی فهرست‌شده دارد که هدف و بیست‌وشش شاخص فهرست‌شده به اندازه زیادی در تأمین پدافند غیرعامل (امنیت فاوا) اثربخش است. در بین شاخص‌های فهرست‌شده، واپایش‌های «نظارت و بازبینی خدمات شخص ثالث»، «مدیریت تغییرات در خدمات شخص ثالث»، «مدیریت ظرفیتی در استفاده از منابع و طرح‌ریزی ظرفیت آینده»، «معیارهای پذیرش سامانه‌های اطلاعاتی جدید و ارتقاء دستگاه‌ها به‌صورت مستند شده و انجام آزمایش کافی، تبادل اطلاعات بین سازمان و شخص ثالث

به‌وسیلهٔ توافقنامه تبادل اطلاعات» و «ثبت تمامی کاستی‌ها و کمبودها» اثربخشی ضعیفی در پدافند غیرعامل (امنیت فاوا) دارد.

۷.واپایش دسترسی: بیست‌وپنج شاخص واپایشی فهرست‌شده دارد که هدف و بیست‌ودو شاخص فهرست‌شده به‌اندازه زیادی در تأمین پدافند غیرعامل (امنیت فاوا) اثربخش است. در بین شاخص‌های فهرست‌شده، «خط‌مشی پاک نمودن صفحه نمایش و تمیز نمودن میزکاری»، «از بین رفتن مهلت استفاده از یک جلسه (یک جلسه غیرفعال)» و «محدودیت زمان اتصال برای فراهم نمودن امنیت بیشتر در برنامه‌های کاربردی» اثربخشی کمتری در پدافند غیرعامل (امنیت فاوا) دارد.

۸.مراقبت و توسعه سامانه‌های اطلاعاتی: شانزده شاخص واپایشی فهرست‌شده دارد که هدف و چهارده شاخص فهرست‌شده به‌اندازه زیادی در تأمین پدافند غیرعامل (امنیت فاوا) اثربخش است. در بین شاخص‌های فهرست‌شده، «تائید اعتبار داده خروجی برنامه‌های کاربردی» و «بازبینی فنی برنامه‌های کاربردی پس از تغییرات در سامانه‌عامل» اثربخشی ضعیفی در پدافند غیرعامل (امنیت فاوا) دارد.

۹.مدیریت حوادث مربوط به امنیت اطلاعات: پنج شاخص واپایشی فهرست‌شده دارد که هدف و پنج شاخص فهرست‌شده آن به‌میزان زیادی در تأمین پدافند غیرعامل(امنیت فاوا) اثربخش است.

۱۰. مدیریت تداوم کسب‌وکار: پنج شاخص واپایشی فهرست‌شده دارد که هدف و سه شاخص فهرست‌شده به‌میزان زیادی در تأمین پدافند غیرعامل (امنیت فاوا) اثربخش است. در بین شاخص‌های فهرست‌شده، شاخص‌های «چارچوب طرح تداوم کسب‌وکار برای اطمینان از سازگاری تمام برنامه‌ها» و «آزمایش، نگهداری و ارزیابی دوباره طرح‌های تداوم کسب‌وکار» اثربخشی ضعیفی در پدافند غیرعامل (امنیت فاوا) دارد.

۱۱. سازگاری و اطمینان یافتن از مطابقت سامانه‌ها با استانداردها: ده شاخص واپایشی فهرست‌شده دارد که هدف و هفت شاخص فهرست‌شده به‌اندازه زیادی در تأمین پدافند غیرعامل(امنیت فاوا) اثربخش است. در بین شاخص‌های فهرست‌شده شاخص‌های «واپایش شناسایی قوانین کاربردپذیر برای هر سامانه اطلاعاتی»، «حقوق دارایی‌های ذهنی (رویه‌های متناسب تطابق‌پذیری با قوانین، مقررات و الزامات قراردادی)» و «شاخص‌های واپایشی ممیزی سامانه‌های اطلاعاتی» اثربخشی ضعیفی در پدافند غیرعامل (امنیت فاوا) دارد.

با توجه به نتایج، پیشنهادهای کاربردی به‌شرح زیر ارائه می‌شود:

۱. با توجه به اینکه وجود خط‌مشی امنیتی دارای کارکرد پدافند غیرعاملی است پیشنهاد می‌شود که سازمان مورد مطالعه در راستای این موضوع گام برداشته و برای سامانه امنیتی خط‌مشی جامعی تدوین نماید.

۲. با توجه به یافته‌های پژوهش، پیشنهاد می‌شود بخشی در سطح مدیریت با عنوان مدیریت امنیت اطلاعات معاونت برنامه‌ریزی و نظارت راهبردی رئیس‌جمهوری برای هماهنگی بین واحدها، تبیین سیاست‌های امنیتی، ایجاد سامانه‌های امنیتی و... ایجاد شود.

۳. با توجه به اینکه، مدیریت دارایی‌ها در سازمان‌ها دارای کارکرد پدافند غیرعاملی است و در این خصوص از اهمیت خاصی برخوردار است موارد زیر در این باره پیشنهاد می‌شود:

الف- کلیه اطلاعات مربوط به دارایی‌ها گردآوری و مکتوب شود و فهرستی از آخرین وضعیت دارایی‌ها و شرح کلیه جزئیات آن تهیه و تدوین شود تا در زمان لازم قابل‌دسترسی و استفاده باشد.

ب- در خصوص چگونگی استفاده از دارایی‌ها و اطلاعات مربوط به آن، دستورالعمل و آئین‌نامه‌هایی گردآوری و به‌صورت منظم و قانونمند تدوین و تنظیم شود.

۴. امنیت منابع انسانی با توجه به یافته‌های پژوهش دارای کارکرد پدافند غیرعامل است و در این باره پیشنهاد می‌شود:

الف- شرح وظایف و مسؤلیت کارکنان در راستای خط‌مشی امنیتی تدوین شده باشد و برابر با آن گردآوری گردد.

ب- در راستای جذب کارکنان اقدامات خاص و مهمی انجام شود و بررسی سوابق کارکنان در هنگام جذب مورد توجه قرار گیرد.

ج- برای توسعه و افزایش سطح آگاهی کارکنان اقدامات مؤثری انجام شود؛ بدین منظور دوره‌های آموزشی خاص امنیت اطلاعات برای کارکنان برگزار شود. دسترسی کارکنان و پیمانکاران سازمان بعد از پایان دوره استخدام و قرارداد مربوطه مورد بازنگری قرار گرفته و این دسترسی از بین برود.

۵. از یافته‌های پژوهش برمی‌آید که امنیت فیزیکی و محیطی دارای کارکرد پدافند غیرعاملی است و در این باره پیشنهاد می‌شود:

الف- امنیت فیزیکی در محیط سازمان از نظر ورود، خروج و محیط اطراف آن با اقدامات خاص و زیربنایی برقرار شود.

ب- نصب سامانه واپایش تردد (ورود و خروج) در سازمان.

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

۶. با توجه به یافته‌های پژوهش، مدیریت ارتباطات و عملیات نیز دارای کارکرد پدافند غیرعاملی است و اهمیت خاصی دارد که می‌بایست مورد توجه قرار گیرد. بنابراین پیشنهاد می‌شود:

الف- شیوه‌نامه و رویه‌های مستند در حوزه ارتباطات و عملیات تهیه شود.

ب- تهیه نسخه پشتیبان و ثانویه از اطلاعات سازمانی به‌طور کامل و کلی.

ج- برقراری و ایجاد سامانه امنیت شبکه در سازمان و به‌روزرسانی و ارتقاء آن.

د- ایجاد دستورالعمل و آئین‌نامه‌های مدون و مشخص در بارهٔ مدیریت رسانه‌های سازمانی (ورود رسانه‌های جدید، خروج رسانه‌های غیرقابل استفاده و غیرضروری، ذخیره اطلاعات و چگونگی آن).

۷. در خصوص موضوع واپایش دسترسی باید گفت، با توجه به یافته‌های پژوهش و اینکه واپایش دسترسی در سازمان دارای کارکرد پدافند غیرعاملی است، پیشنهادهای زیر ارائه می‌شود:

الف- واپایش و نظارت دقیق بر چگونگی و میزان دسترسی، تغییر در نوع دسترسی‌ها و از بین بردن دسترسی‌های غیرلازم و غیرضروری و همچنین بر سطح دسترسی‌ها نیز واپایش و نظارت دقیق انجام شود.

ب- برقراری و ایجاد کدهای امنیتی و رمز عبورهای مشخص و معین و تغییر و مدیریت آن در محدوده‌های زمانی خاص برای افزایش سطح امنیت در شبکه و سازمان.

منابع

۱.اسکندری، حمید. (۱۳۸۹). ***دانستنی‌های پدافند غیرعامل***، تهران، بوستان حمید.

۲.الفت، لعیا، احمد جعفریان و امیر حسن‌زاده. (۱۳۹۰). « نقش به‌کارگیری مدیریت امنیت اطلاعات در کاهش تقویت‌پذیری سفارش‌ها در زنجیره‌های تأمین»، تهران، ***فصلنامه چشم‌انداز مدیریت صنعتی***، تابستان ۱۳۹۰، شماره ۲.

۳.بهرامی، مجتبی. (۱۳۹۰). «ارائه روشی مناسب برای بهبود و توسعه شاخص‌های مدیریت امنیت اطلاعات جهت طراحی و پیاده‌سازی در سازمان‌ها»، ***هشتمین کنفرانس بین‌المللی انجمن رمز ایران***، مشهد، دانشگاه فردوسی.

۴.تاج‌فر، امیرهوشنگ، محمد محمودی میمند، فاطمه رضا سلطانی و پوریا رضا سلطانی. (۱۳۹۳). «رتبه‌بندی موانع پیاده‌سازی سامانه مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف»، ***فصلنامه مدیریت فناوری***، دوره ۶، شماره ۴، تهران دانشگاه تهران، ص ۵۵۱-۵۵۶.

۵.توربان افرایم، یدنر دورورتی، مک کین افرایم، وترب جمیز. (۱۳۸۶). ***فناوری اطلاعات در مدیریت، دگرگونی سازمان‌ها در اقتصاد دیجیتالی***، ترجمه حمیدرضا ریاحی، پوریا قطره‌نبی، مهدیه توفیقی و حسین صامعی، تهران، دانشگاه پیام نور.

۶.پور ابراهیمی، علیرضا و سجاد بنائی. (۱۳۸۹). ***آشنایی با اصول امنیت محیطی در حوزه‌ی فناوری اطلاعات***، دانشگاه آزاد اسلامی، واحد الکترونیکی، تهران.

۷.پورمند، علی .(۱۳۸۶).« استانداردی برای مدیریت امنیت اطلاعات»، تهران، ***ماهنامه تدبیر***، سال هفدهم-شماره ۱۷۸.

۸.خوش‌عمل، حسین. (۱۳۹۱). ***پدافند غیرعامل در حوزه سایبر***، تهران، مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.

۹.دبیرخانه شورای امنیت فضای تبادل اطلاعات، ***پیش‌نویس سند راهبرد امنیت فضای تبادل اطلاعات کشور***، تهران ۱۳۹۰.

۱۰.دوست محمدیان، حمید و مریم‌السادات فاضلی. (۱۳۹۲). ***مهندسی پدافند غیرعامل در فناوری اطلاعات***، موسسه فرهنگی هنری دیباگران، تهران.

۱۱.ریاضی، عبدالمجید. (۱۳۸۸). ***دستورالعمل‌های اجرایی مدیریت امنیت اطلاعات***، تهران نشر نص.

۱۲.صدرآملی، فریبا و بهروز ترک‌لادانی. (۱۳۸۸). ***تحلیل چالش‌ها و عوامل موفقیت پیاده‌سازی سامانه مدیریت امنیت اطلاعات در ایران***

۱۳.موحدی‌نیا، جعفر. (۱۳۸۶). ***اصول و مبانی پدافند غیرعامل***، دانشگاه صنعتی مالک اشتر، تهران.

۱۴.مؤسسه آموزشی و پژوهشاتی صنایع دفاعی. (۱۳۸۴). ***جنگ و دفاع سایبر، گزارش گام دوم(معرفی امور نظامی و دفاعی سایبر) پروژه الزامات جنگ‌های نوین در فضای مجازی(سایبر)***، تهران، موسسه آموزشی و پژوهشاتی صنایع دفاعی، مرکز آینده‌پژوهی علوم و فناوری دفاعی اندیش‌گاه شریف و اندیشکده کاوشگران آینده.

۱۵.میوالد، اریک. (۱۳۸۵). ***مبانی امنیت شبکه***، ترجمه گروه پژوهشی فناوری اطلاعات جهاد دانشگاهی صنعتی شریف.

16.Broderick, J. S. (2006). ISMS, ***security standards and security regulations***, information security technical report. 11.

17.Ernest-Jones, T. (2006). ***Pinning down a security policy for mobile data***, Network Security.

18.Jan, Melissen. (1999). ***Innovations in Diplomatic Practice***,London: MacMillan Press, 1999.

19.POA. (2003). ***Asset Protection and Security Management Handbook***. Auerbach Publications. POA Publishing LLC.

20.Zuccato, A. (2007). ***Holistic security management framework applied in electronic commerce***. Computer and Securi