فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال ششم، شماره‌ی ۲۱ (بهار ۱۳۹۶): صص ۷۸- ۵۵

# نقش امنیت فاوا در جنگ سایبری علیه سازمان‌های امنیتی با رویکرد پدافند غیرعامل

**وحید یادگاری**[۱]
**ناصر یسیلیانی**[۲]
**احمد رضا متین فر**[۳]

تاریخ دریافت:۱۳۹۶/۰۱/۱۵
تاریخ پذیرش:۱۳۹۶/۰۴/۱۵

## چکیده

*امروزه جایگاه فناوری اطلاعات در تحقق مأموریت‌های سازمان‌های امنیتی، جایگاهی بسیار مهم و اثرگذار است. ازاین‌رو می‌بایستی با پایش دائم وضعیت امنیتی و فنی فناوری اطلاعات سازمان، تهدیدها و آسیب‌ها را شناسایی و در جهت پایداری سامانه‌ها و رفع مشکلات آن‌ها اقدام نمود. لذا در این تحقیق بررسی وضعیت امنیت فناوری اطلاعات و ارتباطات در یکی از سازمان‌های امنیتی و سنجش آمادگی آن با رویکرد پدافند غیرعامل در مقابله با جنگ‌های سایبری انجام شده است. سؤال اصلی تحقیق به این صورت طرح شده است که: «نقش امنیت فناوری اطلاعات و ارتباطات در جنگ سایبری علیه سازمان‌های امنیتی با رویکرد پدافند غیرعامل چیست؟». در این تحقیق حجم نمونه و آماری یکی بوده و از نوع تمام شمار است جامعه آماری شامل ۳۵ نفر از خبرگان این موضوع در فاوا و امنیت می‌باشد. در این پژوهش پس از بررسی چک‌لیست‌های پایش امنیت فناوری اطلاعات، الزامات پدافند غیرعامل حوزه فاوا و روش‌های متصور جنگ‌های سایبری، پرسشنامه محقق ساخته با ۳۵ سؤال بسته با استفاده از طیف لیکرت تهیه و پس از توزیع بین ۱۲ نفر خبره، پایایی و روایی آن با محاسبه آلفای کرونباخ صورت پذیرفته و پس‌ازآن پرسشنامه به‌صورت تمام شمار هدفمند بین تمامی افراد جامعه نمونه توزیع و پس از جمع‌آوری و تحلیل با نرم‌افزار SPSS، مشخص گردید وضعیت امنیت فناوری اطلاعات در جنگ‌های سایبری علیه سازمان با رویکرد پدافند غیرعامل در حد خیلی خوب قرار دارد.*

**کلید واژه‌ها:** *پدافند غیرعامل، امنیت فناوری اطلاعات و ارتباطات، جنگ سایبری، سازمان‌های امنیتی*

---

۱-کارشناس ارشد مهندسی فناوری اطلاعات-دانشگاه تربیت مدرس v.yadegari58@yahoo.com
۲-کارشناس ارشد پدافند غیرعامل-دانشکده امام هادی (علیه السلام)
۳-عضو هیئت‌علمی دانشگاه جامع امام حسین (علیه السلام)

## مقدمه

با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع و درعین‌حال نامتوازن ساختار فناوری اطلاعات، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در جهان بدل شده است که ضرورت توجه و پرداخت سریع و درعین‌حال نظام‌مند، معقول و هدفمند به‌منظور مصون‌سازی این بستر از تهدیدات موجود در جهات حفظ امنیت ملی و حریم شخصی شهروندان در فضای جنگ و مخاصمات امروز بین‌المللی را می‌طلبد. در پاسخ به این ضرورت، پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات و جنگ سایبر به‌منظور امنیت، ایمنی و پایداری زیرساخت‌های حیاتی کشور در مقابل تهدیدهای دشمن از ناحیه فناوری اطلاعات و ارتباطات شکل گرفته است. در جمهوری اسلامی ایران نیز همگام با پیشرفت‌های فناوری اطلاعات و ارتباطات، ارکان مختلف کشور نیاز مبرم داشته‌اند تا از این ظرفیت نهایت استفاده را ببرند. به‌عنوان‌مثال در سالیان اخیر، سازمان امنیتی هدف، به‌واسطه گستره فعالیت‌ها و مأموریت‌ها و همگام با فناوری‌های روز، توانسته با استفاده حداکثری از ظرفیت فناوری اطلاعات در راستای چابک سازی سازمان و بهبود فرآیند کاری اقدام نماید که این مهم خوشبختانه با طراحی بیش از ۱۵۵ سامانه نرم‌افزاری و زیرسامانه و راه‌اندازی شبکه اینترانت در حال استفاده می‌باشد. بدون شک این ظرفیت ایجادشده، با توجه به اهمیت کاربردی آن همواره به‌عنوان نشانگاه هدف دشمنان داخلی و خارجی در حوزه جنگ‌های سایبری و اطلاعاتی می‌باشد که سعی دارند با روش‌های مختلف در این سیستم‌ها نفوذ و بهره‌برداری‌های لازم را انجام دهند. ازاین‌رو نیاز است مقوله امنیت فناوری اطلاعات و استانداردهای پدافند غیرعامل موردتوجه جدی قرارگرفته و ضمن هزینه کرد در این حوزه، شاخص‌های آن جهت حفظ و پایداری سامانه‌ها و دفع دسیسه‌ها و نیات پلید دشمن موردتوجه باشد. این تحقیق با این رویکرد صورت پذیرفته است. در قسمت اول تحقیق ضمن طرح صورت‌مسئله، اهمیت و ضرورت پرداختن به موضوع مطرح‌شده و سپس در قسمت دوم به تشریح فناوری اطلاعات و ارتباطات، نقش جنگ در توسعه فناوری اطلاعات و ارتباطات، استانداردهای مدیریت امنیت فناوری اطلاعات، نقش و اجزای فناوری اطلاعات در سازمان و دستورالعمل‌های موجود در زمینه امنیت و پدافند غیرعامل فاوا پرداخته و درنهایت به تحقیقات صورت پذیرفته و مدل مفهومی تحقیق اشاره شده است. در ادامه

تحقیق با تحلیل نتایج پرسشنامه خودساخته وضعیت موجود تحلیل و پیشنهادهای کاربردی به محققان و مدیران ارائه شده است.

## ۲-کلیات تحقیق:

### ۲-۱-سؤال اصلی تحقیق:

نقش امنیت فناوری اطلاعات و ارتباطات در جنگ سایبری علیه سازمان با رویکرد پدافند غیرعامل چیست؟

### ۲-۲- سؤالات فرعی تحقیق:

- انواع جنگ سایبری و روش‌های متصور آن در سازمان کدامند؟
- وضعیت امنیت فناوری اطلاعات و ارتباطات در سازمان با رویکرد پدافند غیرعامل چگونه است؟
- وضعیت اجرای محورهای پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات چگونه است؟

### ۲-۳-اهمیت و ضرورت تحقیق:

**اهمیت**

در سالیان اخیر سازمان به‌واسطه گستره فعالیت‌ها و مأموریت‌ها و همگام با فناوری‌های روز، توانسته با استفاده حداکثری از ظرفیت فناوری اطلاعات در راستای چابک سازی سازمان و بهبود فرآیندهای کاری اقدام نماید که این مهم خوشبختانه با طراحی بیش از ۱۵۵ سیستم و زیرسیستم و راه‌اندازی شبکه اینترانت در حال استفاده می‌باشد. بدون شک این ظرفیت ایجادشده، با توجه به اهمیت کاربردی آن همواره به‌عنوان نشانگاه هدف دشمنان داخلی و خارجی است که سعی دارند با روش‌های مختلف در این سیستم‌ها نفوذ و بهره‌برداری‌های لازم را انجام دهند. ازاین‌رو نیاز است مقوله امنیت فناوری اطلاعات و استانداردهای پدافند غیرعامل موردتوجه جدی قرارگرفته و ضمن هزینه کرد در این حوزه، شاخص‌های آن جهت حفظ و پایداری سیستم و دفع دسیسه‌ها و نیات پلید دشمن موردتوجه باشد.

**ضرورت**

با توجه به اهمیت این تحقیق می‌توان گفت ضرورت دارد تا پایش مستمر مقوله امنیت فناوری اطلاعات و استانداردهای پدافند غیرعامل موردتوجه جدی قرارگرفته و نتایج حاصل از انجام تحقیق برای دفع تاکتیک‌های دشمن در بهره‌گیری از فنون جنگ‌های سایبری علیه سیستم‌های فناوری اطلاعات استفاده گردد تا در صورت اجرای تهدیدها، پایداری را ارتقاء، آسیب‌پذیری‌ها را کاهش و به تداوم خدمات ضروری بر بستر فناوری اطلاعات از سوی سازمان در زمان بحران کمک کند. در صورت عدم تحقیق و اجرای نتایج حاصله، سیستم فاوا در مقابله با تهدیدها، بسیار آسیب‌پذیر بوده و در جنگ‌های سایبری، خسارت حداکثری را متحمل مجموعه خواهد کرد.

## ۴-۲-تعریف مفاهیم و اصطلاحات:

- **پدافند غیرعامل:**

مجموعه اقدامات غیرمسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل در مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌باشد. (قرارگاه پدافند هوایی خاتم‌الانبیا، طرح جامع پدافند غیرعامل)

- **فناوری اطلاعات و ارتباطات:**

به مجموعه سخت‌افزار، نرم‌افزار و تئوری‌هایی اطلاق می‌شود که به نحوی اطلاعات را در اشکال مختلف جمع‌آوری، ذخیره، بازیابی، پردازش و با استفاده از شبکه‌های کامپیوتری منتقل می‌کنند (محمدی،۱۳۸۹:۱۱).

- **فضای سایبر:**

مجموعه‌ای از سیستم‌ها و شبکه‌های کامپیوتری شامل نیروی انسانی، زیرساخت‌ها، تجهیزات، سخت‌افزار، نرم‌افزار و سیستم‌های ارتباطی، کنترلی و مدیریتی است که به‌منظور تولید، ذخیره‌سازی، پردازش، تبادل و بهره‌برداری از اطلاعات ایجاد و سازمان‌دهی شده‌اند. (سند دفاع سایبری جمهوری اسلامی ایران)

- **جنگ سایبری:**

جنگ سایبر به هرگونه عمل خصمانه علیه سیستم‌های رایانه‌ای، شبکه‌های رایانه‌ای یا پایگاه‌های داده رایانه‌ای دشمن اطلاق می‌شود که با هدف کاهش کارایی یا ناتوان‌سازی صورت پذیرد. حملات سایبری، سیستم‌های هدف خود را غیرقابل استفاده نموده، کارایی آن‌ها را کم کرده، با تزریق اطلاعات غلط تصمیم‌گیری کاربران را کاهش می‌دهند و حتی منجر به سرقت اطلاعات می‌شوند. به بیانی دیگر جنگ سایبر عبارت است از به‌کارگیری برنامه‌ریزی‌شده عملیات آفندی و پدافندی که در آن توسط یک ابزار رایانه‌ای علیه ابزار رایانه‌ای دیگر حملاتی صورت می‌گیرد ضمن این‌که به‌کارگیری تعمدی ابزارها و شبکه‌های رایانه‌ای به‌منظور اثرگذاری بر تصمیم‌گیری مخاطبان را نیز باید در زمره جنگ سایبر به حساب آورد (محمدی،۱۳۸۹:۱۱).

- **امنیت فناوری اطلاعات و ارتباطات:**

تأمین و حفظ امنیت فناوری اطلاعات بر محورهای محرمانگی، جامعیت، دسترس‌پذیری و عدم انکار.

محرمانگی به معنا و مفهوم حفاظت داده‌های سیستم‌های رایانه‌ای در برابر دسترسی‌های غیرمجاز، جامعیت یا یکپارچگی به مفهوم تأمین دقت و جامعیت اطلاعات و نرم‌افزارهای رایانه‌ای، دسترسی یا دسترس‌پذیری، به مفهوم ضمانت دسترسی به اطلاعات و خدمات حساس در زمان موردنیاز و عدم انکار تبادل اطلاعات می‌باشد. (پورمراد،۱۳۹۳: ۱۰).

- **پدافند غیرعامل در فناوری اطلاعات:**

پدافند غیرعامل در حوزه فاوا یعنی توسعه امن زیرساخت‌ها و رعایت اصول پدافند غیرعامل در مراکز فاوا به‌منظور ارتقای ضریب امنیت، ایمنی و پایداری. از مهم‌ترین مأموریت‌های پدافند غیرعامل در فاوا می‌توان موارد زیر را نام برد:

- ایجاد و حفظ امنیت زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در برابر مخابرات محتوایی.
- ایمنی زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در قبال حملات فیزیکی.
- پایداری زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در مواجهه با تهدیدات و ادامه مأموریت در شرایط بحران.

- صیانت از زیرساخت‌های حوزه فناوری اطلاعات و ارتباطات در مقابل حملات غیرمترقبه، بلایای طبیعی و مواقع اضطراری.
- ارتقاء و توسعه عزم ملی، باور و فرهنگ عمومی و سازمانی در خصوص رعایت اصول پدافند غیرعامل (استتار، اختفا، پوشش، پراکندگی، استحکام بنا، فریب و...) در حوزه فناوری اطلاعات و ارتباطات کشور
- تولید دانش فنی و بومی و بهره‌گیری آگاهانه از فناوری مناسب و روزآمد کشور در خصوص دفاع غیرعامل فاوا به‌وسیله توسعه جهاد علمی.
- کاهش آسیب‌پذیری زیرساخت‌های کلیدی و مراکز حیاتی، حساس و مهم کشور در حوزه فناوری اطلاعات و ارتباطات در برابر تهدیدات و اعمال ملاحظات، سیاست‌ها و ضوابط خاص پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات در برنامه‌های در دست مطالعه کشور.
- تدوین معماری کلان پدافند غیرعامل فناوری اطلاعات و ارتباطات کشور (www.ipfn.ir)

## ۴-پیشینه تحقیق:

محسن آزاد زاده و دیگران در مقاله «مبانی پدافند غیرعامل در حوزه امنیت فناوری اطلاعات»، عنوان نموده‌اند که تأمین امنیت اطلاعات سازمان‌ها در محیط امروزی که از شبکه‌های به‌هم‌پیوسته تشکیل‌شده کاری مشکل است و با ورود هر محصول الکترونیکی و هر ابزار نفوذ و جاسوسی این کار سخت‌تر نیز می‌شود. هم‌چنین با توجه به رشد روزافزون حملات در شبکه‌های کامپیوتری تلاش برای مقاوم‌سازی آن‌ها در برابر حملات و در نظر گرفتن مسائل مربوط به پدافند غیرعامل امری حیاتی محسوب می‌شود. امروزه عوامل بسیاری وجود دارد که امنیت یک شبکه را تهدید می‌کند. از جمله این عوامل؛ حملات گسترده هکرها که از نقاط آسیب‌پذیر سیستم‌ها برای رسیدن به اهدافشان استفاده می‌کنند با هک کردن یک سرور میزبان صدها یا شاید هزاران سایت هک می‌شوند؛ بنابراین نیازمند حفاظت از سرور و شبکه خود و لحاظ کردن مسائل پدافند غیرعامل با امکانات امنیتی هستیم. در این مقاله بعد از بررسی تهدیدات داخلی و خارجی و حفاظت از سیستم‌ها، به ضرورت نیاز به تأمین امنیت پرداخته و مسائل مربوط به امنیت فناوری اطلاعات در عصر دیجیتال و مباحث مربوط به رایانه‌های شخصی و اینترنت بحث می‌شود (آزادزاده و دیگران، ۱۳۹۲).

در پایان‌نامه رضا نیک‌نفس با عنوان «بررسی شاخص‌های پدافند غیرعامل در فاوا نیروی انتظامی استان همدان» به بررسی زیرساخت‌های فناوری اطلاعات متناسب با استانداردهای سازمان پدافند غیرعامل پرداخته‌شده و محقق به این نتیجه رسیده است که علی‌رغم متوسط بودن وضعیت، به جهت این‌که سیستم‌های فناوری اطلاعات در بستر یک شبکه محدود یعنی اینترانت می‌باشد، نمی‌توان تهدیدهای کلی را در مورد شبکه سازمان جدی ارزیابی کرد (رضا نیک‌نفس،۱۳۹۲).

در مقاله «اصول و ملاحظات پدافند غیرعامل در فضای سایبری»، جواد داوری و دیگران به تشریح سرمایه‌های فضای سایبر اعم از زیرساخت‌ها، سیستم‌ها و روش‌های ارزیابی پرداخته است. منظور از ارزیابی فناوری فهرستی از فعالیت‌ها است که تقریباً در هر ارزیابی کاربرد دارند. این مقاله به ارزیابی فناوری اطلاعات و اصول و ملاحظات پدافند غیرعامل در فضای مجازی مورداستفاده در سطح سازمان‌ها طی سال‌های اخیر پرداخته است. تحقیق حاضر سعی نموده است پیوند مناسبی بین ملاحظات پدافند غیرعامل و مدیریت فناوری اطلاعات به انجام رساند تا نتایج مطلوب‌تری از ارزیابی فناوری اطلاعات در فضای مجازی به دست آید (داوری، ۱۳۹۲).

در مقاله نقش اصول پدافند غیرعامل در رفع تهدیدات سایبری و تأثیر آن بر امنیت ملی، علی خادمه مولوی و دیگران در پی پاسخ‌گویی به این پرسش می‌باشند که چگونه اصول پدافند غیرعامل در حوزه سایبری می‌تواند در جهت رفع تهدیدات سایبری مفید واقع شود و نقش این اقدامات در جهت افزایش امنیت ملی چگونه است. در پاسخ می‌توان گفت این تهدید به علت برخورداری از ویژگی‌هایی چون قیمت پایین ورود، عدم شناسایی و تأثیرگذاری گسترده و عمیق، پدیده‌ای به نام بحران تهدیدات سایبری را به وجود آورده است که نه‌تنها باعث شده دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند، بلکه منجر به ورود بازیگران جدیدی همچون شرکت‌ها، گروه‌های سازمان‌یافته و افراد به معادلات قدرت جهانی شده است؛ بنابراین، این پدیده امنیت ملی را از ابعاد مفهوم امنیت، دولت‌محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه، تحت تأثیر قرار داده است (خادمه مولوی و دیگران، ۱۳۹۵).

در مقاله «ارائه راه‌کارهایی برای مدیریت امنیت اطلاعات با رویکرد مدیریت استراتژیک فناوری اطلاعات»، عنوان شده که اطلاعات از مهم‌ترین دارایی‌های هر سازمان است و حفاظت از آن نقش مهمی در بقای سازمان‌ها دارد. روند رو به رشد فناوری اطلاعات، نقش استراتژیک فناوری اطلاعات در سازمان و اهمیت امنیت دارایی‌های اطلاعاتی، موجب گسترش نیازمندی سازمان‌ها به راه‌کارهای مدیریت امنیت اطلاعات شده است. سازمان‌های مختلف با توجه به میزان اهمیت اطلاعات موجود، نیازمند مدیریتی قوی در جهت حفظ امنیت این اطلاعات در راستای اهداف استراتژیک سازمان می‌باشند. هر قدر سازمان‌ها از سیستم‌های اطلاعاتی بیشتر استفاده کنند، اهمیت موضوع امنیت اطلاعات نیز بیشتر می‌شود. در این پژوهش توصیفی- مروری سعی شده است با به‌کارگیری پژوهش‌های انجام شده، راه‌کارهایی برای اجرای موفق مدیریت امنیت اطلاعات با رویکرد مدیریت استراتژیک فناوری اطلاعات ارائه گردد. با به‌کارگیری این راه‌کارها، سازمان‌های بزرگ و حتی کسب‌وکارهای کوچک می‌توانند به اهداف امنیتی خود دست پیدا نموده، مزیت رقابتی خود را حفظ کرده و حتی ارتقا دهند (رضائی نیارکی و دیگران، ۱۳۹۵).

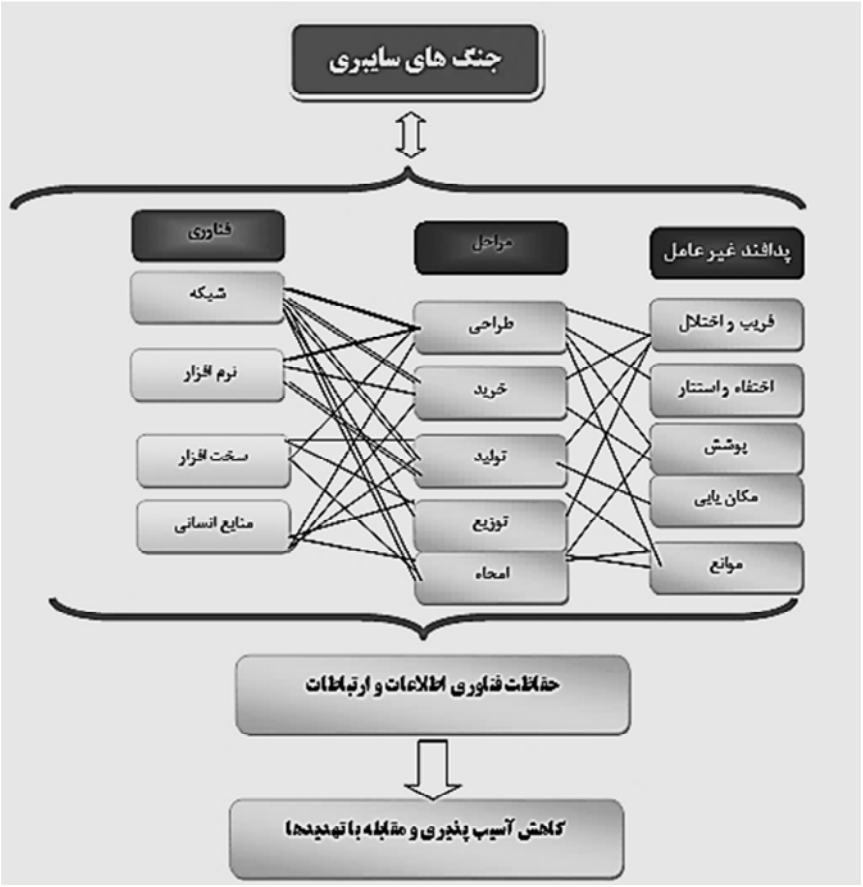
در مقاله زاراجا و همکاران سیستم‌های اطلاعاتی و امنیت اطلاعات در سازمان‌ها مدنظر قرار دارد. با پیشرفت روزافزون فناوری اطلاعات و افزایش استفاده از این فناوری در جامعه، سازمان‌ها برای انجام فعالیت‌هایشان به کاربرد سیستم‌های اطلاعاتی نیازمند می‌شوند. خطرات ناشی از جمع‌آوری و نگهداری اطلاعات در سیستم‌های اطلاعاتی، امنیت این سیستم‌ها را به بحثی مهم و مؤثر در نحوه استفاده بهینه از سامانه‌های اطلاعاتی تبدیل کرده است. امنیت دستگاه‌های اطلاعاتی، مدیریت امنیت آن‌ها و پیاده‌سازی مدیریت امنیت آن سیستم‌ها موجب شده است که عوامل متفاوتی در این بحث لحاظ شود؛ عواملی همچون عوامل سازمانی، محیطی، تکنولوژی و ... ((Zárraga-Rodríguez, M. & Álvarez, M.J. (2015)

در مقاله ریضا، سعی شده تا به‌صورت مروری به چرایی رویکرد بهینه‌سازی استراتژی امنیت فناوری اطلاعات پرداخته شود. در این مقاله موضوعات استراتژی امنیت فضای سایبر و امنیت اطلاعات موردتوجه بوده و محقق عنوان داشته است امنیت فضای سایبر، تعریف جامع‌تری نسبت به امنیت اطلاعات دارد و در ادامه نیز مؤلفه‌های امنیت فضای سایبری تشریح شده است. برای

اجرای این هـدف بـزرگ در بـیش از ۵۴ کشـور، به‌صـورت مـرتبط و یکپارچـه مؤسسـه NCSS تشکیل‌شده است که در خصوص تهدیدهای سایبری، امکان همکاری و تعامل را خواهنـد داشـت و این امر باعث ارتقای توان سایبری خواهد بود (Riza Azmi,2016)

## ۵-مدل مفهومی تحقیق:

نظر به مدل تحلیلی تحقیق در رابطه با طرح پژوهش، الگوی زیرین پیشنهاد می‌گردد:



## ۶-روش تحقیق:

### ۶-۱- جامعه آماری:

جامعه آماری این تحقیق شامل کارکنان حوزه فاوا و امنیت فناوری اطلاعات و ارتباطات سازمان هدف می‌باشد و تعداد کل جامعه آماری تحقیق به‌صورت تمام شمار و هدفمند ۵۳ نفر اعلام گردیده است.

### ۶-۲- روش نمونه‌گیری و حجم نمونه:

با توجه به محدود بودن تعداد متخصصان حوزه امنیت فناوری اطلاعات و ارتباطات در این سازمان، تعداد ۳۵ نفر از متخصصان به‌صورت تمام شمار و هدفمند انتخاب گردیده‌اند.

### ۶- ۳ روش و ابزار تهیه پرسشنامه:

برای تهیه پرسش‌نامه، دستورالعمل حفاظت فناوری اطلاعات، دستورالعمل‌های حوزه فاوا سازمان، پدافند غیرعامل، استانداردهای بین‌المللی حوزه امنیت فناوری اطلاعات شامل ISMS و پایان‌نامه‌های انجام شده مرتبط، مطالعه و در مرحله اول ۱۵۰ سؤال استخراج گردید و سپس در اختیار تیمی از متخصصان خبره حوزه امنیت فناوری اطلاعات قرار گرفت. درنهایت با حذف و یا تجمیع بعضی از سؤالات تعداد ۵۰ سؤال به‌عنوان سؤالات پیشنهادی استخراج و تصویب گردید و سپس مراحل پایایی و روایی انجام شد.

### ۶-۴- گردآوری اطلاعات:

در این پژوهش گردآوری اطلاعات به روش کتابخانه‌ای و پیمایشی و تحلیلی توصیفی با بهره‌گیری از ابزار پرسش‌نامه بسته بوده است. بر همین تعداد ۳۵ نسخه پرسشنامه پس از انجام بررسی‌های لازم و با استفاده از روش طیف لیکرت تدوین و بین متخصصان حوزه امنیت فناوری اطلاعات و ارتباطات توزیع گردید.

### ۵-۶-تجزیه‌وتحلیل یافته‌های تحقیق:

تجزیه‌وتحلیل داده‌های جمع‌آوری‌شده با نرم‌افزار SPSS انجام شده است. برای تحلیل داده‌های تحقیق از تحلیل درصد فراوانی استفاده شده است.

### ۶-۶-پایایی و روایی سؤالات:

برای سنجش روایی یا قابلیت اعتماد، از روش صوری استفاده شده است. روایی صوری از مشتقات روایی محتوایی است. روایی صوری به این مطلب اشاره می‌کند که سؤال‌های یک آزمون تا چه حد در ظاهر شبیه به موضوعی هستند که برای اندازه‌گیری آن تهیه شده‌اند. برای این کار ابتدا تعدادی پرسشنامه بین تعداد ۱۲ نفر از کارکنان نخبه فناوری اطلاعات سازمان توزیع گردید و کلیه ابهامات متخصصان و صاحب‌نظران در رابطه با سؤالات مشخص شد. بدین ترتیب تعدادی از سؤالات حذف، یا اصلاح و تعدادی دیگر جایگزین شد و درنهایت پس از شفاف شدن و رفع ابهامات، پرسشنامه نهایی تهیه و توزیع گردید. برای محاسبه پایایی از آلفای کرونباخ استفاده شده است. منظور از پایایی، اعتبار آزمون، دقت اندازه‌گیری و ثبات آن است. منظور از دقت اندازه‌گیری این است که نمره کسب‌شده توسط فرد تا چه حدی می‌تواند بیانگر نمره حقیقی وی باشد (نگهبان،۱۳۸۴:۶۷). ضریب آلفای محاسبه‌شده که در جدول زیر نشان داده شده است از طریق نرم‌افزار Spss، برای مجموع گویه‌ها ۵۰) گویه(در مؤلفه‌های مربوط به وضعیت موجود Alpha =0.708 محاسبه‌شده است؛ بنابراین با توجه به نتیجه حاصله می‌توان گفت که پرسشنامه موردنظر از پایایی لازم برخوردار می‌باشد.

## ۷-تجزیه‌وتحلیل پرسشنامه‌ها:

پس از اتمام مرحله گردآوری اطلاعات، محقق انبوهی از اطلاعات را در اختیار دارد که باید برای انجام اقدامات بعدی استفاده کند. این مرحله از تحقیق اهمیت زیادی دارد. در این تحقیق، تجزیه‌وتحلیل داده‌ها به‌صورت آمار توصیفی و استنباطی مورد ارزیابی قرار می‌گیرد و از طریق تنظیم جدول و رسم نمودار نمایش داده می‌شود.

### ۱-۷-آمار توصیفی:

### توزیع فراوانی سطح تحصیلات کارکنان:

| وضعیت | فراوانی | درصد فراوانی | درصد تجمعی |
|---|---|---|---|
| کارشناسی ارشد | ۲۰ | ۵۷،۱۴ | ۵۷،۱۴ |
| کارشناسی | ۱۵ | ۴۲،۸۶ | ۱۰۰ |
| کاردانی | ۰ | ۰ | ۱۰۰ |
| جمع کل | ۳۵ | ۱۰۰ | |

جدول ۱-توزیع فراوانی سطح تحصیلات کارکنان

همان‌طور که در جدول توزیع فراوانی سطح تشکیلات مشاهده می‌گردد، سطح تحصیلی بیشترین تعداد پاسخگویان را مقطع کارشناسی ارشد با تعداد ۲۰ نفر یعنی ۵۷،۱۴ در صد کل پاسخگویان تشکیل داده‌اند.

## تحلیل یافته‌های سؤال فرعی ۱:

سؤال فرعی ۱: انواع جنگ سایبری و روش‌های متصور آن در سازمان کدامند؟

| ردیف | گویه | نمره |
|---|---|---|
| ۱ | جایگاه و نقش فناوری اطلاعات در تحقق اهداف مأموریتی سازمان | ۱۹/۳۱ |
| ۲ | جایگاه و اهمیت سامانه‌ها و زیرساخت‌های فناوری اطلاعات سازمان در سطح کشوری | ۱۸/۷۴ |
| ۳ | جایگاه و اهمیت سامانه‌ها و زیرساخت‌های فناوری اطلاعات سازمان در نزد دشمنان به‌عنوان هدف و نشانگاه عملیاتی جنگ سایبری | ۱۸/۱۷ |
| ۴ | جایگاه و اهمیت سامانه‌ها و زیرساخت‌های فناوری اطلاعات سازمان در نزد مخالفان، اخلال‌گران و سود جویان داخلی به‌عنوان هدف و نشانگاه عملیاتی جنگ سایبری | ۱۵/۰۸ |
| ۵ | وجود آسیب‌پذیری و استفاده از امواج الکترومغناطیس برای ایجاد اخلال و تخریب زیرساخت‌های فاوا سازمان (نفوذ فنی) | ۱۵/۱۴ |
| ۶ | وجود آسیب‌پذیری و وقوع عملیات‌های شبکه‌ای با هدف ایجاد اختلال، سرقت اطلاعات، جاسوسی و...از طریق هک و نفوذ شبکه‌های ارتباطی و زیرساخت‌ها (نفوذ فنی) | ۱۳/۰۲ |
| ۷ | وجود آسیب‌پذیری و وقوع عملیات اطلاعاتی با هدف دستکاری، سرقت، جاسوسی و اشرافیت بر سیستم‌های اطلاعاتی نرم‌افزاری سازمان از محیط بیرونی (نفوذ فنی) | ۱۲/۰۵ |
| ۸ | مهندسی اجتماعی و یا بهره‌گیری هدفمند عوامل درون‌سازمانی به‌عنوان سرپل نفوذ از سوی دشمنان برای تحقق اهداف جنگ سایبری علیه سازمان (نفوذ اجتماعی) | ۱۸/۰۵ |
| ۹ | مهندسی اجتماعی و یا بهره‌گیری هدفمند از پیمانکاران (تیم‌های برنامه‌نویسی، طراح شبکه و...) به‌عنوان سرپل نفوذ از سوی دشمنان برای تحقق اهداف جنگ سایبری علیه سازمان (نفوذ اجتماعی) | ۱۷/۱۴ |
| ۱۰ | تولید سخت‌افزار و نرم‌افزار و تجهیز به بدافزارها و کنترل‌های راه دور و فروش هدفمند در پوشش‌های مختلف به سازمان برای تحقق اهداف جنگ سایبری (نفوذ اجتماعی) | ۱۶/۴۵ |

جدول ۲–میانگین آماری سؤال فرعی ۱

میانگین نمره سؤالات بعد اول یعنی جنگ‌های سایبری متصور علیه سازمان، ۱۶/۳۸ می‌باشد که بالاتر از خوب بوده و مناسب است؛ اما آنچه در بررسی سؤالات مشهود است این است که هنوز عامل انسانی و مهندسی اجتماعی برای نفوذ کارکرد فراوانی دارد و علی‌رغم تمامی هزینه‌های صورت گرفته برای امن سازی سامانه‌ها و زیرساخت‌ها، استفاده از کاربران سیستم‌ها و پیمانکاران سامانه‌ها به‌عنوان سرپل نفوذ به سیستم‌های فناوری اطلاعات سازمان موردنظر دشمن می‌باشد.

**نتیجه‌گیری سؤال فرعی اول:** بهره‌گیری از فناوری اطلاعات در سازمان در راستای مأموریت‌های سازمانی جایگاه ویژه‌ای دارد و امروزه بیش از ۲۰۰ سیستم و زیرسیستم در سازمان فعال می‌باشد که همگی دارای اطلاعات ارزشمندی می‌باشند و ازاین‌رو نقشی ویژه نیز در سطح فناوری اطلاعات کشور و تحقق دولت الکترونیک ایفا می‌کنند. بررسی اطلاعات میدانی بیانگر این موضوع است، درصد هک و نفوذ به زیرساخت‌های سازمان و نرم‌افزارهای سازمانی به‌واسطه داشتن اینترانت اختصاصی بسیار سخت می‌باشد و تاکنون روش سؤال ۸ یعنی مهندسی اجتماعی و یا بهره‌گیری هدفمند عوامل درون‌سازمانی به‌عنوان سرپل نفوذ از سوی دشمنان برای دسترسی به سیستم‌های جامع سازمان و تحقق اهداف جنگ سایبری علیه سازمان (نفوذ اجتماعی) مسبوق به سابقه بوده است که با نتایج پرسش‌نامه هم‌خوانی دارد.

### تحلیل یافته‌های سؤال فرعی ۲:

سؤال فرعی ۲: وضعیت امنیت فناوری اطلاعات و ارتباطات در سازمان چگونه است؟

| ردیف | گویه | نمره |
|---|---|---|
| ۱۱ | خرید و تولید نرم‌افزارهای منطبق با سیاست‌های ابلاغیه ن.م شده است (تکنولوژی، معماری، امنیت) | ۱۷/۲۷ |
| ۱۲ | پیش‌بینی و ایجاد لایه‌ها و قابلیت‌های امنیتی مورد تأیید مراکز ذی‌صلاح در نرم‌افزارها با هدف کنترل امنیت آن‌ها. (واپایش سامانه‌ها به جهت کنترل دسترسی‌ها و لاگ‌ها، کنترل محتوا، تأییدیه امنیتی و...) | ۱۷/۳۷ |

| | | |
|---|---|---|
| ۱۳ | واگذاری بدون کنترل و نظارت امور نگهداشت و مدیریت سامانه‌های سازمان به پیمانکاران. | ۱۶/۵۷ |
| ۱۴ | آگاهی طراحان و تولیدکنندگان نرم‌افزار به مباحث حفاظتی تولید نرم‌افزار | ۱۶/۵۷ |
| ۱۵ | واگذاری بدون کنترل و نظارت اطلاعات طبقه‌بندی‌شده و تجهیزات به پیمانکاران | ۱۶/۳۴ |
| ۱۶ | ناآگاهی و یا عدم توجه مدیران به ضوابط برون‌سپاری پروژه‌های فناوری اطلاعات (ضوابط امنیتی و حفاظتی تولید، پشتیبانی و رفع عیب نرم‌افزار و...) | ۱۶/۵۷ |
| ۱۷ | دسترسی به سیستم‌های جامع سازمان به‌صورت برخط در محیط اینترنت | ۱۸/۵۱ |
| ۱۸ | یکپارچه‌سازی و تعامل‌پذیری بدون کنترل و نظارت سامانه‌های سازمان با سایر سازمان‌ها | ۱۷/۰۲ |
| ۱۹ | نصب و به‌کارگیری نرم‌افزارهای غیر مصوب و فاقد مجوز | ۱۵/۷۷ |
| ۲۰ | تنظیمات امنیتی سیستم‌عامل، سرویس‌دهنده‌ها، نرم‌افزارها و سرویس‌های امنیتی نرم‌افزاری مثل فایروال‌ها و... | ۱۵/۷۷ |
| ۲۱ | اجرای سیاست‌ها، خط‌مشی‌ها و دستورالعمل‌های پشتیبان گیری از نرم‌افزارها و بانک‌های اطلاعاتی، بازیابی اطلاعات امحا (تهیه مستمر نسخه پشتیبان، نگهداری در جای امن و به‌دوراز نسخه اصلی و...) | ۱۶/۶۸ |
| ۲۲ | تأمین سخت‌افزار از داخل کشور و از طریق مراکز مصوب | /۴۲<br>۱۵ |
| ۲۳ | حصول اطمینان از داشتن تأییدیه امنیتی سخت‌افزارهای تهیه شده. | ۱۶/۱۱ |
| ۲۴ | حصول اطمینان از عدم استفاده از سخت‌افزارهای اهدایی، مکشوفه و یا بلا صاحب در سازمان | ۱۶/۶۸ |
| ۲۵ | نظارت و کنترل بر تهیه سخت‌افزارها بر اساس الگوی پیش‌بینی‌شده. | ۱۶/۹۱ |

| | | |
|---|---|---|
| ۲۶ | توجه به حفاظت و عایق‌کاری مراکز فاوا به‌منظور مقابله با بمب‌های الکترومغناطیسی | ۱۵/۵۴ |
| ۲۷ | حفاظت از اطلاعات مورد مبادله در مقابل جنگ الکترونیک | ۱۶/۳۴ |
| ۲۸ | طراحی و پیاده‌سازی شبکه‌های ارتباطی استاندارد و امن و منطبق بر سیاست‌های ابلاغی | ۱۶/۸ |
| ۲۹ | توزیع کلیدهای رمز و تجهیزات امنیتی بسترهای ارتباطی برای امن سازی بستر و ایجاد حیطه‌بندی در توزیع سرویس‌های بسترهای ارتباطی | ۱۷/۶ |
| ۳۰ | رعایت کامل اصول حفاظتی در تعمیر و پشتیبانی تجهیزات امنیتی مربوط به بسترهای ارتباطی | ۱۷/۹۴ |
| ۳۱ | رعایت استاندارد و طرح‌های حفاظت فیزیکی مراکز و اماکن به‌منظور جلوگیری و پیشگیری و مقابله با تهدیدات طبیعی و مصنوعی | ۱۷/۰۲ |
| ۳۲ | فراوانی پاسخگوی‌ان به سؤال ۳۲: بهره‌گیری از سیستم‌های هوشمند و آنی برای تحلیل مخاطرات و هشدار دهی مثل مرکز امنیت اطلاعات (soc) | ۱۵/۵۴ |
| ۳۳ | پیش‌بینی و تأمین نیروهای واکنش سریع و امدادرسانی در مواقع بحران (cert) | ۱۶/۴۵ |
| ۳۴ | صلاحیت و تسلط علمی کاربران و کارشناسان متخصص سیستم‌های فاوا | ۱۷/۳۷ |
| ۳۵ | صلاحیت و تسلط علمی ممیزان امنیتی برای کنترل و نظارت مراحل پیاده‌سازی و بهره‌برداری سیستم‌ها و شبکه‌ها (طراحی، تولید، اجرا، خرید، بهره‌برداری، نگهداری و تعمیر | ۱۶/۵۷ |

جدول ۳–میانگین آماری سؤال فرعی ۲

**نتیجه‌گیری سؤال فرعی دوم:** نتایج بررسی میدانی امنیت فناوری اطلاعات و آمار بیانگر این موضوع است که وضعیت امنیت فناوری اطلاعات در سطح خیلی خوبی قرار دارد و در بسیاری از مسائل مباحث مرتبط به پدافند غیرعامل در حوزه فناوری اطلاعات نیز اجرایی گردیده است. به‌طور میانگین با ضریب بالای ۹۰٪ می‌توان امنیت فناوری اطلاعات سازمان را نمره دهی کرد. البته نتیجه بررسی‌های میدانی با نظریه خبرگان اختلاف ۱۰ درصدی دارد که قابل‌قبول می‌باشد. بااین‌حال شاخص‌های جدول ۶، بیانگر نمرات کمتر از میانگین می‌باشد که تواند موردتوجه بیشتر باشد.

| شماره سؤال | شرح سؤال | نمره |
|---|---|---|
| سؤال ۱۹ | نصب و به‌کارگیری نرم‌افزارهای غیر مصوب و فاقد مجوز | ۱۵/۷۷ |
| سؤال ۲۰ | تنظیمات امنیتی سیستم‌عامل، سرویس‌دهنده‌ها، نرم‌افزارها و سرویس‌های امنیتی نرم‌افزاری مثل فایروال‌ها و... | ۱۵/۴۲ |
| سؤال ۲۲ | تأمین سخت‌افزار از داخل کشور و از طریق مراکز مصوب | ۱۵/۵۴ |
| سؤال ۲۶ | توجه به حفاظت و عایق‌کاری مراکز فاوا به‌منظور مقابله با بمب‌های الکترومغناطیسی | |
| سؤال ۳۲ | بهره‌گیری از سیستم‌های هوشمند و آنی برای تحلیل مخاطرات و هشدار دهی مثل مرکز امنیت اطلاعات (SOC) | ۱۵/۵۴ |

جدول ۴–لیست و نمرات سؤالاتی که کمتر از میانگین می‌باشند.

## تحلیل یافته‌های سؤال فرعی ۳:

سؤال فرعی ۳: وضعیت شاخص‌های پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات سازمان چگونه است؟

| ردیف | گویه | نمره |
|---|---|---|
| ۳۶ | راه‌اندازی و نهادینه کردن جایگاه پدافند سایبری در دبیرخانه پدافند غیرعامل سازمان –به جهت اهمیت، همراهی مدیریتی، تخصیص بودجه و... در سطح سازمان و زیرمجموعه ها با شرح وظایف مشخص | ۱۷/۷۱ |
| ۳۷ | تهیه شیوه‌نامه اجرایی اصول پدافند غیرعامل اعم از اختفا، استتار، مقاوم‌سازی، پراکندگی و پشتیبان سازی در حوزه فاوا | ۱۶/۶۸ |
| ۳۸ | رعایت سایر اصول پدافند غیرعامل اعم از اختفا، استتار، مقاوم‌سازی، پراکنده‌سازی، پشتیبان سازی و جلوگیری از آنالیز، تضعیف، اختلال، فریب و... | ۱۶/۲۲ |
| ۳۹ | همراهی و همکاری مدیران بابت تأمین بودجه و...حوزه‌های امنیت و پدافند غیرعامل در حوزه فناوری اطلاعات | ۱۶/۵۷ |
| ۴۰ | شناخت و تهیه سند وضع موجود سایبری سازمان اعم از اماکن، سخت‌افزارها و ارتباطات، نرم‌افزارها (معماری و کد برنامه‌ها و...)، اولویت‌بندی و سطح امنیتی، شناخت نقاط ضعف و آسیب و... | ۱۶/۸ |
| ۴۱ | تأمین ارتباطات امن و پایدار بین مراکز پدافندی سایبری دستگاه | ۱۶/۴۵ |
| ۴۲ | ساماندهی و راه‌اندازی ساختار مدیریت امنیت اطلاعات، مراکز امداد و نجات رایانه‌ای (CERT)، مراکز امنیت عملیات (SOC) | ۱۵/۵۴ |
| ۴۳ | تأمین نیازمندی‌های پشتیبانی فنی مثل خطوط برق موازی و اضطراری، خطوط ارتباطی موازی برای بخش‌های کلیدی و مراکز حیاتی حساس | ۱۳/۹۴ |
| ۴۴ | ایجاد ظرفیت‌های احتیاط و پشتیبان برای بخش‌های کلیدی با ویژگی امنیت، ایمنی و پایداری متناسب با سطح طبقه‌بندی آن | ۱۶/۵۷ |
| ۴۵ | آموزش و توجیه نیروی متخصص و کارآمد برای حفظ پایداری سیستم‌ها در مواقع بحران | ۱۶/۲۲ |
| ۴۶ | تهیه دستورالعمل‌های تخصصی فنی و اجرایی برای انجام اقدامات مقابله‌ای و توجیه کارکنان | ۱۶/۸ |

| | | |
|---|---|---|
| ۴۷ | استفاده از سامانه‌های نرم‌افزاری، الگوریتم‌های رمز و سخت‌افزاری بومی و یا تأییدشده | ۱۵/۲ |
| ۴۸ | تعیین و به‌کارگیری استانداردهای دفاعی و امنیتی بومی‌شده متناسب با مأموریت و وظایف تعیین‌شده | ۱۶/۲۲ |
| ۴۹ | شناخت تهدیدات عمده و جاری (عمومی و تخصصی) و بررسی و ارزیابی تأثیرات آن‌ها بر امنیت، ایمنی و پایداری زیرساخت‌ها | ۱۶/۱۶ |
| ۵۰ | تدوین سناریوهای محتمل ناشی از تهدیدات سایبری و سطح‌بندی آن‌ها و مشخص نمودن دامنه آسیب‌پذیری و نقاط آسیب‌پذیر و پیگیری راه‌حل‌های مقابله‌ای | ۱۶/۸ |

جدول ۵–داده‌های مربوط به سؤال فرعی سوم

## نتیجه‌گیری سؤال فرعی سوم:

رعایت امنیت با شاخص‌های پدافند غیرعامل دارای مؤلفه‌هایی می‌باشد که خوشبختانه در سازمان موردتوجه بوده و سازوکار آن به‌طور کامل طراحی و در دست اجرا و کنترل می‌باشد. البته بعضی از موارد به شرح جدول ذیل دارای نمره پایین‌تری نسبت به میانگین نمرات هستند که بایستی بیشتر موردتوجه باشند.

| شماره سؤال | شرح سؤال | نمره |
|---|---|---|
| سؤال ۴۲ | ساماندهی و راه‌اندازی ساختار مدیریت امنیت اطلاعات، مراکز امداد و نجات رایانه‌ای (CERT)، مراکز امنیت عملیات (SOC) | ۱۵/۵۴ |
| سؤال ۴۳ | تأمین نیازمندی‌های پشتیبانی فنی مثل خطوط برق موازی و اضطراری، خطوط ارتباطی موازی برای بخش‌های کلیدی و مراکز حیاتی حساس | ۱۳/۹۴ |
| سؤال ۴۷ | استفاده از سامانه‌های نرم‌افزاری، الگوریتم‌های رمز و سخت‌افزاری بومی و یا تأییدشده | ۱۵/۲ |

جدول ۶–شاخص‌هایی که نمره پایین‌تر از میانگین دارند

## ۸-پیشنهادها:

### ۸-۱-پیشنهاد به مسئولان:

۱. آموزش مستمر کاربران سیستم‌های جامع سازمان در جهت آشنایی بیشتر با شکست‌های حفاظتی فاوا
۲. برگزاری رزمایش‌های مختلف برای حفظ و ارتقای آمادگی فاوا در مقابل بحران‌ها
۳. استفاده از هکران حرفه‌ای برای شبیه‌سازی نفوذ در سیستم‌ها و سنجش وضعیت امنیت فاوا
۴. پایش مستمر امنیت فاوا با استفاده از آخرین استانداردهای امنیت فاوا در جهان مثل ISMS
۵. راه‌اندازی مرکز پدافند غیرعامل و امنیت فناوری اطلاعات فاوا جهت برنامه‌ریزی و رصد مستمر
۶. راه‌کارهای بررسی و کنترل نصب و به‌کارگیری نرم‌افزارهای غیر مصوب و فاقد مجوز، بررسی و کنترل تنظیمات امنیتی سیستم‌عامل، سرویس‌دهنده‌ها، نرم‌افزارها و سرویس‌های امنیتی نرم‌افزاری مثل فایروال‌ها و... مورد تأکید و توجه باشد.
۷. استانداردهای پدافند غیرعامل در حوزه سیستم‌عامل و نرم‌افزارها، فایروال‌ها، ارتباطات، عایق‌کاری مراکز فاوا به‌منظور مقابله با بمب‌های الکترومغناطیسی مطابق استانداردهای سازمان پدافند مورد تأکید و توجه باشد.
۸. تأمین سخت‌افزار از داخل کشور و از طریق مراکز مصوب
۹. تخصیص بودجه و تکمیل فرآیندهای پدافند غیرعامل در حوزه فناوری اطلاعات (زیرساخت، نیروی انسانی و...)
۱۰. ساماندهی و راه‌اندازی ساختار مدیریت امنیت اطلاعات، مراکز امداد و نجات رایانه‌ای (CERT) و...
۱۱. تأمین نیازمندی‌های پشتیبانی فنی مثل خطوط برق موازی و اضطراری، خطوط ارتباطی موازی برای بخش‌های کلیدی و مراکز حیاتی حساس
۱۲. آموزش تخصصی برای ارتقای کارشناسان با رویکرد پدافند غیرعامل مدنظر قرار گیرد
۱۳. کمیته‌ای مشترک در سطح سازمان‌های امنیتی برای هدایت موضوع پدافند غیرعامل حوزه فاوا تشکیل و وظیفه سیاست‌گذاری و نظارت راهبردی را بر عهده داشته باشد
۱۴. استفاده از سامانه‌های نرم‌افزاری، الگوریتم‌های رمز و سخت‌افزاری بومی و یا تأییدشده

## پیشنهاد به محققان:

۱-روش‌های کنترل هوشمند شناسایی تخلفات و نفوذ و اخلال از سوی کارکنان در بانک‌های اطلاعاتی و زیرساخت‌های سازمان

۲-آسیب‌شناسی حفاظتی کاربران سیستم‌های جامع سازمان

۳-شناسایی ساختار و شیوه روش‌های متصور جنگ‌های سایبری علیه سازمان مثل جنگ‌های الکترومغناطیسی و ...

۴-شناسایی و پیاده‌سازی سیستم‌های هوشمند پایش امنیت

۵-آسیب‌شناسی استفاده از سیستم‌ها و الگوریتم‌های غیربومی در حوزه فناوری اطلاعات

۶-راه‌کارهای تولید سیستم‌ها و الگوریتم‌های بومی

۷- استخراج استانداردها، شاخص‌های بین‌المللی و الزامات حوزه پدافند غیرعامل در فناوری اطلاعات و روش‌های اجرایی استانداردها موردتوجه جدی باشد. با توجه به این‌که سیستم‌های سازمان در یک بستر امن یعنی اینترانت داخلی ارائه گردیده، پیشنهاد می‌گردد در تحقیق‌های بعدی وضعیت امنیتی و پدافندی غیرعامل درصورتی‌که سازمان از تکنولوژی‌های جدید مثل ابر اطلاعات، برنامه‌های کاربردی موبایل، سرویس‌های اینترنتی و... استفاده نماید موردبررسی قرار گیرد. به نظر می‌رسد امنیت مطلوب فعلی بیشتر به جهت محدود بودن در اینترانت داخلی بوده و به نظر کارشناسان خبره و محققان با توجه به توسعه روزافزون اینترنت و دولت الکترونیک و از طرفی خدمات سازمان از طریق سیستم‌ها، سازمان نیز باید همانند سایر سازمان‌های مشابه در کشورهای جهان بسیاری از خدمات خود را در محیط اینترنت ارائه نماید.

## منابع و مآخذ:


۱–امیر صوفی، رحمت‌الله، جنگ‌های اطلاعاتی،مجتمع دانشگاهی فناوری اطلاعات،ارتباطات و امنیت دوره پدافند غیر عامل–پنهان

۲–اوروسخانی،علی،حفاظت ارتباطات:انتشارات کوثر

۳–پدافند غیرعامل در حوزه تهدیدات الکترومغناطیسی،تهیه‌کننده:مرکز پدافند غیرعامل فاوا، ناشر:شرکت مخابرات ایران

۴–پورمراد،مجید،حفاظت فناوری اطلاعات و ارتباطات: انتشارات کوثر

۵–پدافند غیرعامل در حوزه جنگ سایبر تهیه‌کننده:مرکز پدافند غیرعامل فاوا: ناشر:شرکت مخابرات ایران

۶–خاکی، غلامرضا (۱۳۸۷)، روش تحقیق در مدیریت، چاپ سوم، تهران، انتشارات بازتاب.

۷–دادگر، هانیه، بررسی نقش جنگ در توسعه فناوری اطلاعات، و فناوری اطلاعات در جنگ

۸–دستورالعمل‌های جامع امنیت فناوری ناجا

۹–دلاور، علی (۱۳۷۶)، احتمالات و آمار کاربردی در روان‌شناسی و علوم تربیتی، تهران ، انتشارات رشد.

۱۰–دوست محمدیان، حمید(۱۳۸۹)،پدافند غیرعامل در حوزه فناوری اطلاعات

۱۱–دوست محمدیان،حمید–اصول و مبانی پدافند غیرعامل(۱۳۸۹)

۱۲–دوست محمدیان،حمید افشانی(۱۳۸۹)بررسی متقابل هیستوژئوپولتیک جنگ‌ها در پیشرفت‌های امروزی

۱۳–دوست محمدیان،حمید(۱۳۹۲)،مهندسی پدافند غیرعامل در فناوری اطلاعات(امنیت به روش پیشگیری الکترونیکی)

۱۴–رمضان زاده، فایل آموزشی آمار و کاربرد نرم‌افزارهای آن در پژوهش،۱۳۹۲، تهران، دانشگاه علوم انتظامی.

۱۵–ساروخانی، محمدباقر(۱۳۸۵)، روش‌های تحقیق در علوم اجتماعی(جلد اول اصول و مبانی)، تهران، انتشارات پژوهشگاه فرهنگی.

۱۶–مارکزیک، جوفری و دیگران. ترجمه مریم خسروی،(۱۳۸۶)، اصول طرح تحقیق و روش‌شناسی، تهران، انتشارات پژوهشگاه وزارت
علوم تحقیقات و فناوری.
۱۷–ماهنامه پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات
۱۸–مقدمه‌ای بر پدافند غیرعامل در حوزه امنیت فیزیکی و کنترل دسترسی، تهیه‌کننده:مرکز پدافند غیرعامل فاوا،ناشر:شرکت مخابرات ایران
۱۹– نگهبان، علیرضا و همکار(۱۳۸۴)، راهنمای روش تحقیق به کمک پرسشنامه SPSS ، تهران، انتشارات جهاد دانشگاهی.
۲۰–یادگاری،وحید(۱۳۹۲)،هوشمند سازی سیستمهای فناوری اطلاعات
۲۱–یادگاری،وحید(۱۳۹۲)ارائه چارچوبی برای تحقق رویکرد آفندی ولایت در جنگ‌های سایبری