مجله علمی ترویجی «پدافند غیرعامل»

سال یازدهم، شماره ٤، زمستان ١٣٩٩، (پیاپی ٤٤): صص ٦-١

علمی- ترویجی

الزامات پدافند غیرعامل در ارتباط با انواع دارایی‌های صنعت توزیع برق

محمدتقی طاحونه[١]، رضا دشتی[٢]*، رضا غفارپور[٣]، غلامرضا جلالی[٤]

تاریخ دریافت: ١٣٩٨/٠٦/٠٣

تاریخ پذیرش: ١٣٩٩/٠٥/٢٥

چکیده

صنعت برق ازجمله صنایع حساس انرژی است که به‌دلیل وابستگی حیات جامعه و زیرساخت‌های آن به این انرژی مهم و حساس همواره مورد انواع تهدیدات و گروه‌های خاصم قرارگرفته است. این صنعت شامل دارایی‌های متنوعی است که هر یک به طریقی متفاوت، آسیب می‌بینند و راهکارهای مصون‌سازی و الزامات پدافند غیرعامل در مورد آن‌ها بسیار متنوع است. این دارایی‌ها که عبارت‌اند از دارایی‌های شبکه، اعم از اصلی، ارتباطی، منابع انسانی، ماشین‌آلات و ابزارآلات و ... به تفکیک در این مقاله مورد بررسی و تحلیل قرار می‌گیرند. سپس با در نظر گرفتن اصول استتار و اختفا، حیله و فریب، مقاوم‌سازی، مکان‌یابی، کوچک‌سازی و پراکنده‌سازی، حرکت و جابجایی، یکسان‌سازی، احیا و آماده‌سازی و انبار یدکی، الزامات و راهکارهای پدافند غیرعامل برای هر دارایی به تفکیک اصول پدافند غیرعامل ذکر می‌شود. بدین ترتیب می‌توان راهکارهای جاری‌سازی پدافند غیرعامل را به‌صورت چارچوبی جامع ارائه نمود.

کلیدواژه‌ها: الزامات، پدافند غیرعامل، دارایی، صنعت برق

[١] دانشگاه علم و صنعت ایران

[٢] استادیار دانشگاه علم و صنعت ایران- (rdashti@iust.ac.ir)- نویسنده مسئول

[٣] استادیار دانشگاه امام حسین (ع)

[٤] استادیار دانشگاه عالی دفاع ملی

۱- مقدمه

عوامل ایجاد تهدید عبارت‌اند از: گروه‌های تروریستی، عوامل خرابکار و کارکنان سامانه و دولت‌های بیگانه. تروریست‌ها به چهار دسته فدائیان، گروگان‌ها، مزدوران و خرابکاران تقسیم‌بندی می‌شوند. انواع تهدیدهای متوجه صنعت برق عبارت‌اند از: گرافیتی، الکترومغناطیسی، لیزری، تروریستی و سایبری.

بحران‌های طبیعی با بحران ناشی از تهدید دشمن تفاوت دارد و ازجمله این تفاوت‌ها این است که شدت آسیب بحران طبیعی وابسته به‌شدت عامل مخاطره طبیعی است اما شدت آسیب بحران ناشی از تهدید دشمن وابسته به هوشمندی دشمن است.
مدل کامل پیشنهادی امنیت سامانه توزیع شامل بازیگران اصلی، بازیگران جانبی، دارایی‌های شبکه، فرآیند مدیریت دارایی و عوامل خارجی مؤثر می‌شود.

خاموشی برق می‌تواند در بخش‌های مختلف مانند بهداشت و درمان، حمل‌ونقل زندگی روزمره، خطرات قطع برق وسایل برقی، صنایع، ادارات، مراکز خدماتی و تجاری، کشاورزی، سامانه‌های مخابراتی، تخریب وسایل منزل اختلال ایجاد کرده و حتی به‌صورت زنجیره‌ای منجر به قطع آب و گاز شهری شود.

آسیب‌پذیری‌های صنعت برق در برابر راهبردهای تهدید این صنعت شامل عدم متنوع سازی نیروگاه‌ها، فرسودگی نیروگاه‌ها، توسعه نامتوازن تولید نیروگاهی، ایجاد نقاط بالقوه آسیب‌پذیر، عدم توجه به اصل بازدارندگی، سرعت توسعه صنعت برق، میزان ذخایر صنعت برق در زمان بحران و در نهایت زمان‌های بحرانی صنعت برق می‌شود.

برگزاری رزمایش و انجام عملیات مدیریت بحران شامل فرماندهی، اطلاعات و شبکه مخابراتی، منابع انسانی، شرکت‌ها و مشارکت‌ها و ابزارآلات و ماشین‌آلات، به‌صورت جامع و دقیق می‌توانند مدیریت بحران را تسهیل نمایند.

در بخش‌های مختلف صنعت برق شامل تولید، انتقال، توزیع و مصرف برق می‌توان رویه‌های تسهیل در مدیریت بحران را تعریف نمود.

مدیریت بحران صنعت برق طبق روند نمای مدیریت بحران که از اطلاع‌رسانی شروع می‌شود و تا عادی‌سازی ادامه می‌یابد، انجام می‌شود. همچنین در هنگام بحران تعاملات مختلفی ازجمله تعامل با مصرف‌کنندگان و پیمانکاران ضروری است.

استراتژی هریک از دارایی‌های صنعت برق پس از وقوع بحران در سه بخش: مصارف و بارهای مختلف، استراتژی کنترل بار و تعیین اقدامات لازم، قابل‌بحث و بررسی است.

می‌توان در ارتباط با انواع دارایی‌های صنعت برق که شامل دارایی‌های شبکه، دارایی‌های کنترلی، دارایی‌های ارتباطی، دارایی‌های سنجش، تحلیل و تصمیم، دارایی‌های منابع انسانی و دارایی‌های ابنیه، ماشین‌آلات و ابزارآلات و همچنین الزامات پدافند غیرعامل را تعریف نمود که در این مقاله بیان‌شده‌اند.

به همین منظور این مقاله به بررسی الزامات پدافند غیرعامل می‌پردازد و الزامات را به تفکیک اصول پدافند غیرعامل برای هر دارایی ارائه می‌دهد.

۲- بررسی صنعت برق از دیدگاه تهدیدشناسی، پیامدشناسی خاموشی و آسیب‌پذیری

۲-۱- تهدیدات و آسیب‌پذیری‌ها

در شبکه توزیع برق به‌صورت پیوسته اطلاعات، پایش یا مانیتور می‌شود. این اطلاعات مانیتور شده توسط مراکز کنترل مورد تحلیل قرار می‌گیرد و در انتها به کمک تحلیل‌های صورت گرفته، تصمیم‌سازی و اجرا انجام می‌شود. قسمت‌های مختلف یک سامانه توزیع که اطلاعات آن‌ها پایش می‌شود عبارت‌اند از: بار، حفاظت، اتفاقات، صورتحساب، ولتاژ و توان راکتیو، کیفیت توان، تعمیرات، منابع پراکنده و بازیگران سامانه. با دست‌کاری هر یک از شاخص‌ها عملاً تصمیم‌گیری اشتباه صورت پذیرفته و صدمات جبران‌ناپذیری را وارد می‌نماید.

جهت تبیین آسیب‌پذیری‌های صنعت برق از تهدیدات می‌بایست کلیه ارکان و دارایی‌های صنعت برق موردبررسی قرار گیرند. دارایی‌های سامانه توزیع برق به چند دسته عمده شامل دارایی‌های اصلی (مبدل‌ها، سیم‌ها و غیره)، دارایی‌های محافظ (رله‌ها، فیوزها و غیره)، دارایی‌های کنترلی (ادوات اندازه‌گیری، نرم‌افزارها و غیره) و دارایی‌های ارتباطی، تقسیم می‌شوند. بازیگران اصلی سامانه توزیع عبارت‌اند از: حاکم دارایی (نظام جمهوری اسلامی ایران)، مالک دارایی (مردم به‌واسطه هزینه از بیت‌المال)، مدیر دارایی (دولت و مشخصاً وزارت نیرو) و مجری دارایی (مدیران اجرایی شرکت‌های توزیع). بازیگران جانبی سامانه توزیع عبارت‌اند از: سازندگان، انواع پیمانکاران ارائه‌دهنده خدمات، مدیران طرح، طراحان و مشاوران، شرکت‌های مخابراتی و در نهایت بازرگانان. علاوه‌بر بازیگران اصلی که به دارایی‌های سامانه توزیع دسترسی داشته و روی آن‌ها تأثیرگذار هستند عوامل خارجی مؤثر شامل عوامل اقتصادی، شهری، جغرافیایی، اجتماعی و فرهنگ‌سازمانی و همچنین فرآیندهای مدیریت

دارایی شامل مدیریت اتفاقات، مدیریت بار، مدیریت حفاظت، مدیریت ولتاژ و مدیریت تعمیرات نیز بر روی دارایی‌ها تأثیرگذاری دارند. این دو عامل یعنی فرآیندهای مدیریت دارایی و عوامل خارجی مؤثر، زیر نظر بازیگران اصلی هستند و با این بازیگران در ارتباط می‌باشند. در انتهای یک سامانه توزیع، مصرف‌کنندگان قرار دارند که تمامی موارد ذکرشده بر امنیت و قابلیت اطمینان برق دریافتی آن‌ها اثرگذار هستند.

۲-۱- پیامدشناسی

حوزه‌های مختلفی که خاموشی برق بر آن‌ها تأثیرگذار است عبارت‌اند از:

- بهداشت و درمان
- صنایع
- کشاورزی
- حمل‌ونقل
- ادارات، مراکز خدماتی و تجاری
- سامانه‌های مخابراتی
- زندگی روزمره
- خطرات قطع برق وسایل برقی
- تخریب وسایل منزل

بدین ترتیب ملاحظه می‌شود جایگاه انرژی برق در پایداری اجتماعی زمان بحران و تداوم خدمات ضروری کلیدی است.

۳- انواع دارایی‌های صنعت برق

شبکه‌های توزیع برق آخرین حلقه از زنجیره برق‌رسانی صنعت برق هستند که انرژی الکتریکی را از مبادی خروجی شبکه‌های انتقال دریافت نموده و به مصرف‌کنندگان تحویل می‌دهند. شبکه‌های توزیع برق دارای چهار دسته دارایی می‌باشند که عبارت‌انداز:

الف) دارایی‌های اصلی شبکه: این دارایی‌ها شامل خطوط فشار متوسط (شامل پایه و هادی)، پست‌ها (شامل ترانسفورماتور و تابلوها)، خطوط فشار ضعیف (شامل پایه و هادی) هستند. ارزش و قیمت و همچنین حوزه تغذیه و میزان اثرگذاری هر یک از این دارایی‌ها بسیار کمتر از دارایی‌های سایر سطوح شبکه‌های صنعت برق است. این دارایی‌ها آخرین دارایی‌های حامل انرژی به بارهای حیاتی، حساس و مهم هستند و می‌توانند مورد هدف گروه‌های تروریستی جهت ایجاد اختلال در عملکرد، قرار گیرند.

ب) دارایی‌های محافظ: این دارایی‌ها شامل رله‌ها، فیوزها، برق‌گیرها و ... هستند که جهت محافظت از دارایی‌های سامانه توزیع در برابر تغییرات جریان و ولتاژ مورد استفاده قرار می‌گیرند. دارایی‌های محافظ از دو دیدگاه مورد ارزیابی قرار می‌گیرند. اول این‌که در زمان ایجاد تغییرات نامطلوب ولتاژ و جریان، ازجمله اضافه ولتاژ یا اضافه جریان شبکه را قطع کنند که این را اعتماد عملکرد می‌گویند و دوم این‌که در مواقع عادی شبکه را قطع نکند که آن را اتکاپذیری می‌گویند. این دارایی‌ها می‌توانند هدف دشمن قرارگرفته و در حالت عادی آن‌ها را وادار به عملکرد نابجا مانند دستور قطع شبکه کنند.

ج) دارایی‌های کنترلی: این دارایی‌ها شامل کلیدها، قطع کننده‌ها، قطع کننده‌های حفاظتی، جداکننده‌ها و ... هستند که جهت کنترل بارگذاری بر روی دارایی‌ها و تغییر مسیر تغذیه به‌کار می‌روند. این دارایی‌ها می‌توانند فرمان‌پذیر از مرکز کنترل باشند و یا به‌طور دستی و در محل، عمل کنترل را انجام دهند. در شرایط فرمان‌پذیری دارایی‌های کنترلی از راه دور، دشمن می‌تواند با حمله سایبری این ادوات را تحت اختیار خود قرار دهد. در صورت عدم پایش دارایی‌های کنترلی و عدم امکان فرمان از راه دور می‌توانند هدف حرکت‌های تروریستی قرار گیرند.

د) دارایی‌های ارتباطی: این دارایی‌ها همان دارایی‌های شبکه مخابراتی هستند که وظیفه انتقال اطلاعات اعم از اطلاعات شبکه‌ای و اداری بین مراکز کنترلی- مدیریتی و نقاط اندازه‌گیری و همچنین تهیه اطلاعات بین مراکز کنترلی مدیریتی و نقاط اعمال تصمیم و دستور و کنترل را برعهده دارند.

تهدیدات فراروی دارایی‌های اصلی را می‌توان به تهدیدات تخریبی تروریستی، بمب‌های الکترومغناطیسی (جهت ایجاد اضافه ولتاژ)، بمب‌های گرافیتی (جهت ایجاد اتصال کوتاه) و بمب‌های لیزری (به‌منظور ایجاد حرارت) تقسیم‌بندی نمود. هر یک از تهدیدات در صورت مکان‌یابی صحیح می‌توانند شبکه را به‌طور کلی از کار بیاندازد و در غیر این صورت صدمات بسیار زیادی را وارد نموده و بخش زیادی از شبکه را در خاموشی فرو ببرند. از تهدیدات فراروی دارایی‌های محافظ می‌توان به دست‌کاری‌های تروریستی جهت عملکرد در مواقع غیرضروری و یا برعکس، بمب‌های الکترومغناطیسی (جهت از کار افتادن دارایی‌های حفاظتی) اشاره نمود.

با توجه به وجود ضریب هم‌زمانی مصارف در تعیین نوع دارایی‌های حفاظتی، در صورت تشویق به‌مصرف هم‌زمان مشترکین، ادوات حفاظتی می‌توانند مشکل‌ساز باشند. تهدیدات فراروی دارایی‌های کنترلی نیز به خرابکاری‌های تروریستی و عوامل انسانی تقسیم‌بندی می‌شوند. تهدیدات فراروی دارایی‌های مخابراتی به‌جز خرابکاری‌های تروریستی و عوامل انسانی عمدتاً به حملات سایبری محدود می‌شوند که در صورت حمله سایبری می‌توانند اختلالات جدی در شبکه ایجاد کنند و کلیه دارایی‌ها را تحت تأثیر قرار دهند.

۴- الزامات پدافند غیرعامل در ارتباط با انواع دارایی‌های صنعت برق

در این بخش دارایی‌ها به ۶ دسته شامل دارایی‌های شبکه، دارایی‌های کنترلی، دارایی‌های ارتباطی، دارایی‌های سنجش، تحلیل و تصمیم، دارایی‌های منابع انسانی و درنهایت دارایی‌های ابنیه، ماشین‌آلات و ابزارآلات تقسیم‌شده است و الزامات پدافند غیرعامل در هر دسته به‌صورت جدول‌هایی مجزا ارائه‌شده‌اند.

الزامات پدافند غیرعامل در دارایی‌های شبکه در جدول (۱) آورده شده است.

جدول(۱): الزامات پدافند غیرعامل در دارایی‌های شبکه.

	دارایی‌های شبکه
استتار و پنهان‌سازی	مشابه‌سازی با مبلمان شهری، مسقف نمودن، احداث زیرزمینی
مقاوم‌سازی	مقاوم‌سازی ساختمانی و مقاوم‌سازی الکتریکالی
مکان‌یابی	عدم عبور فیدرها[1] از عرض خیابان‌های اصلی، احداث پست‌ها در داخل ساختمان‌ها و یا در زیرزمین
کوچک‌سازی	پست‌ها و نیروگاه‌های با ظرفیت کم و تعداد زیاد، امکان‌سازی جزیره‌ای نمودن شبکه، استفاده از تولیدات پراکنده و اضطراری و موبایل، استفاده از ظرفیت تولید مجازی، محلی‌سازی حوزه‌های فرماندهی و تهیه و تجهیز آن‌ها، به‌کارگیری پست موبایل، ایجاد زیرساخت‌های تولیدات مجازی، شبکه‌های فشار ضعیف، کاهش طول فیدرهای فشار متوسط
پراکنده‌سازی	
حرکت و جابجایی	کلید زنی، مانور و تغییر مسیر تغذیه، استفاده از ژنراتورها و پست‌های موبایل، هوشمندسازی
حیله و فریب	طراحی خلاقانه ساختار شبکه، ساختار تغذیه موبایل (متناسب با مبلمان شهری و تغذیه چندگانه)
یکسان‌سازی	یکسان‌سازی ادوات و ابزارآلات و تجهیزات، ساده‌سازی دسترسی‌ها
یدکی	تخمین صدمات و خسارات، تعیین نوع و میزان یدکی‌های موردنیاز جهت انبار
آماده‌باش و احیا	رفع عیب دارایی‌های صدمه دیده، آزمون و بازرسی دارایی‌های سالم، آماده‌سازی اتاق بحران و خودرو بحران

الزامات پدافند غیرعامل در دارایی‌های کنترلی در جدول (۲) آورده شده است.

[1] Fider

جدول(۲): الزامات پدافند غیرعامل در دارایی‌های کنترلی.

	دارایی‌های کنترلی
استتار و پنهان‌سازی	ایجاد پست‌های کلید زنی
مقاوم‌سازی	هوشمند سازی، ارتقاء کیفیت تجهیزات و ارتقاء کیفیت منابع انسانی
مکان‌یابی	احداث کلید خانه در نقاط تحت حفاظت و دور از دسترس
کوچک‌سازی	توسعه و عدم تمرکز نقاط مانور، ایجاد مراکز کنترل محلی
پراکنده‌سازی	
حرکت و جابجایی	هوشمند سازی، تدوین سناریو کلید زنی‌های اضطراری، امکان سازی و ایجاد قابلیت سوییچ از حالت مکانیزه به حالت دستی، سناریوهای کلید زنی محلی
حیله و فریب	ایجاد کلید زنی چندگانه و مخفی
یکسان‌سازی	یکسان‌سازی نوع و نحوه حفاظت
یدکی	امکان یکسره کردن ادوات حفاظتی
آماده‌باش و احیا	احیای زیرساخت‌ها اعم از رله‌ها و شبکه‌های مخابراتی

الزامات پدافند غیرعامل در دارایی‌های ارتباطی در جدول (۳) آورده شده است.

جدول(۳): الزامات پدافند غیرعامل در دارایی‌های ارتباطی.

	دارایی‌های ارتباطی
استتار و پنهان‌سازی	محدودیت دسترس
مقاوم‌سازی	مستحکم سازی مراکز کنترلی سامانه توزیع و ایستگاه‌های اطلاعاتی ازنظر سازه‌ای، استفاده از قفل‌های سخت‌افزاری و نرم‌افزاری، مستحکم سازی شبکه‌های مخابراتی، کنترل ورود و خروج اطلاعات
مکان‌یابی	احداث در درون ساختمان اصلی سامانه توزیع و یا در زیرزمین و یا منطقه‌ای حفاظت‌شده
کوچک‌سازی	ایجاد مراکز کنترل و فرمان محلی، ایجاد مراکز کنترلی فشار ضعیف، ایجاد مراکز کنترل محلی، محلی نمودن مراکز کنترل شبکه
پراکنده‌سازی	
حرکت و جابجایی	هوشمندسازی، ایجاد سامانه مخابراتی جایگزین، امکان سازی و ایجاد قابلیت سوییچ از حالت مکانیزه به حالت دستی
حیله و فریب	-
یکسان‌سازی	یکسان‌سازی نوع داده ارسالی و نحوه ارسال
یدکی	تهیه و نگهداری تلفن همراه ماهواره‌ای، انبار تجهیزات ضروری موردنیاز مخابراتی، ایجاد مراکز کنترلی پشتیبان
آماده‌باش و احیا	احیای زیرساخت‌های شبکه‌های مخابراتی

الزامات پدافند غیرعامل در دارایی‌های سنجش، تحلیل و تصمیم در جدول (۴) آورده شده است.

جدول(۴): الزامات پدافند غیرعامل در دارایی‌های سنجش، تحلیل و تصمیم

	دارایی‌های سنجش، تحلیل و تصمیم
استتار و پنهان‌سازی	استفاده از شبکه‌های فیبر نوری زیرزمینی
مقاوم‌سازی	پیاده‌سازی ملاحظات دفاع سایبری، مقاوم‌سازی مراکز مرکز کنترل و کنترل
مکان‌یابی	مکان‌یابی لوازم اندازه‌گیری، دخالت دادن ملاحظات پدافند غیرعامل در مکان‌یابی مراکز کنترل
کوچک‌سازی	تعدد مراکز کنترل محلی
پراکنده‌سازی	
حرکت و جابجایی	تعیین مراکز کنترل معین، قابلیت دستی نمودن فعالیت‌ها
حیله و فریب	تعیین مراکز کنترل جانشین
یکسان‌سازی	یکسان‌سازی نرم‌افزارها و رویه‌های کنترل
یدکی	قابلیت دستی نمودن فعالیت‌ها
آماده‌باش و احیا	وجود دستورالعمل نحوه جمع‌آوری اطلاعات و تحلیل و اعمال آن‌ها در زمان تهدید و بحران

الزامات پدافند غیرعامل در دارایی‌های منابع انسانی در جدول (۵) آورده شده است.

جدول(۵): الزامات پدافند غیرعامل در دارایی‌های منابع انسانی.

	دارایی‌های منابع انسانی
استتار و پنهان‌سازی	شناسایی و حفاظت از افراد و کارکنان کلیدی در زمان تهدید
مقاوم‌سازی	فرهنگ‌سازی سازمانی، آموزش و انگیزش
مکان‌یابی	مکان‌یابی صحیح اکیپ‌های اتفاقات و تعمیرات
کوچک‌سازی	امکان سازی اداره بومی شبکه و انجام فعالیت‌های مرتبط
پراکنده‌سازی	
حرکت و جابجایی	تعیین اکیپ‌های معین و جانشین
حیله و فریب	تفهیم نحوه اداره و بهره‌برداری از شبکه و کلید زنی‌های خاص در زمان تهدید
یکسان‌سازی	انجام آموزش همگانی، تدوین دستورالعمل‌های زمان تهدید
یدکی	افزایش ظرفیت‌های پیمانکاری
آماده‌باش و احیا	برگزاری مانور، تدوین سناریو در زمان بحران و تهدید

الزامات پدافند غیرعامل در دارایی‌های ابنیه، ماشین‌آلات و ابزارآلات در جدول (۶) آورده شده است.

جدول(۶): الزامات پدافند غیرعامل در دارایی‌های ابنیه، ماشین‌آلات و ابزارآلات.

	دارایی‌های ابنیه، ماشین‌آلات و ابزارآلات
استتار و پنهان‌سازی	مشابه‌سازی ابنیه با مبلمان شهری
مقاوم‌سازی	مقاوم‌سازی ساختمانی و ساختاری، مقاوم‌سازی ساختمان دسپاچینگ
مکان‌یابی	مکان‌یابی بهینه خودروهای عملیات و اتفاقات و مراکز فرماندهی
کوچک‌سازی	ملاحظه گستردگی و سناریوهای تهدیدات در تعداد ماشین‌آلات و مراکز کنترل محلی
پراکنده‌سازی	
حرکت و جابجایی	تعیین خودروهای جایگزین
حیله و فریب	امکان مشابه‌سازی خودروها با سایر خودروهای شهری
یکسان‌سازی	یکسان بودن خودروها و ابزار در کل شرکت
یدکی	وجود خودروهای عملیات یدکی و همچنین قطعات یدکی خودروها
آماده‌باش و احیا	انجام سرویس‌های دوره‌ای خودروها و بازدید و تعویض ابزار

۵- نتیجه‌گیری

همان‌گونه که در این مقاله ملاحظه گردید انواع دارایی‌های صنعت برق اعم از دارایی‌های شبکه، دارایی‌های کنترلی، دارایی‌های ارتباطی، دارایی‌های نرم‌افزاری و سخت‌افزاری، دارایی‌های منابع انسانی و دارایی‌های ابنیه، ماشین‌آلات و ابزارآلات هر یک دارای آسیب‌پذیری‌های متفاوت و کارکردهای متفاوتی هستند. به‌گونه‌ای که پیامد آسیب هر یک متفاوت با دیگری است. بدین‌جهت در این مقاله با در نظر گرفتن کلیه موارد فوق‌الذکر به تفکیک اصول پدافند غیرعامل شامل استتار و پنهان‌سازی، مقاوم‌سازی، مکان‌یابی، کوچک‌سازی، پراکنده‌سازی، حرکت و جابجایی، حیله و فریب، یکسان‌سازی، یدکی، آماده‌باش و احیا به تشریح الزامات پدافند غیرعامل به تفکیک دارایی‌ها پرداخته می‌شود. لازم به‌ذکر است مدیریت دارایی مقاومت دارایی‌ها را نسبت به ضربه افزایش می‌دهد و راهکارهای پیشنهادی در این مقاله جهت بهبود این مورد تمرکز دارد.

۶- مراجع

۱. دشتی، رضا، واکاوی خاموشی‌های سراسری برق و منظر پدافند غیرعامل، سازمان پدافند غیرعامل، ۱۳۹۴.

۲. دشتی، رضا، یوسفی، شقایق، پدافند غیرعامل در سیستم‌های توزیع برق، سازمان پدافند غیرعامل، ۱۳۹۵.

۳. دشتی، رضا، تروریسم و شبکه‌های انرژی برق، سازمان پدافند غیرعامل، ۱۳۹۶.

۴. دشتی، رضا و همکاران، تاب‌آوری در سیستم‌های توزیع برق، انتشارات قائم، ۱۳۹۷.

۵. دشتی، رضا و همکاران، آشنایی با پدافند غیرعامل در صنعت برق، انتشارات دانش اترک، ۱۳۹۷.

۶. دشتی، رضا و همکاران، تهدیدات سایبری در سیستم‌های توزیع برق، انتشارات دانش اترک، ۱۳۹۷.

۷. رضا دشتی و همکاران، تهدیدات خصمانه علیه صنعت برق، انتشارات دانش اترک، ۱۳۹۷.

۸. دشتی، رضا و همکاران، استراتژی‌های پدافند غیرعامل در صنعت برق، انتشارات دانش اترک، ۱۳۹۷.

۹. دشتی، رضا و همکاران، تهدیدات تروریستی علیه صنعت انرژی برق، انتشارات دانش اترک، ۱۳۹۷.

۱۰. دشتی، رضا و همکاران، آسیب‌پذیری شبکه تولید برق در برابر تهدیدات تروریستی، ۱۳۹۷.

۱۱. دشتی، رضا و همکاران، طرح یکپارچه پدافند غیرعامل در صنعت برق، انتشارات ستاره جنوب، ۱۳۹۶.

New Critical Infrastructure Protection Strategies

M. T. Tahooneh, R. Dashti*, R. Ghaffarpour, Gh. Jalali

Abstract

The electrical industry is one of the most sensitive energy-industries as the infrastructure and social life depend on it. This important energy source has always been subject to a variety of threats from hostile groups. This industry has a variety of assets that are each affected in a different way, and therefore a variety of immunization strategies and civil defense approaches are required. In this article these assets are explained separately, and civil defense requirements for each one, are discussed from the viewpoint of passive defense principles. These assets, which include network assets, such as major assets, communications facilities, human resources, machinery and tools, etc. are analyzed separately in this article. Then the relevant requirements and strategies for each asset are presented, according to passive defense principles and taking into account the issues of camouflage, surveillance, trickery, retrofitting, locating, scaling, scaling, moving, aligning, resuscitation and preparation and storage of spare-parts. In this way, executive solutions that can provide a comprehensive framework for passive defense can be presented.

Key Words: *Requirements, Civil Defense, Asset, Electricity Industry*

* Iran University of Science and Technology - (rdashti@iust.ac.ir) - Writer-in-Charge