آیین نامه اجرایی پدافند غیرعامل در حوزه بحران های الکترومغناطیسی شبکه بانکی– حساس

شناسه سند:	
شماره اصلاحیه:	۷
تاریخ تهیه سند:	۱۳۸۷/۱۱/۱۸
تعداد صفحات سند:	۳۳
تاریخ آخرین اصلاحات:	۱۳۸۸/۸/۱۲

فهرست مطالب:

فهرست جداول:

فهرست اشکال:

پیوست۱: تهدیدات الکترومغناطیسی

پیوست۲: آسیب پذیری

پیوست ۳: جدول مبنای ارزیابی، راهبردها و سطوح حفاظتی

پیوست۴: راهکارهای حفاظتی

پیوست۵: تستهای حفاظت الکترومغناطیسی

مقدمه

این آیین نامه به منظور اجرایی کردن اصول پدافند غیرعامل در حوزه بحران های الکترومغناطیسی تدوین شده است.

با گسترش روزافزون سیستمها وتجهیزات الکترونیکی ووابستگی بسیاری از خدمات وارتباطات به الکترونیک ومخابرات، حساسیت نسبت به حفظ سیستم های الکترونیکی مخابراتی ومداومت کاری آنها افزایش پیدا کرده است. تهدیدات الکترومغناطیسی که توسط دشمن خارجی ویا ستون پنجم در زمان جنگ وصلح توسط سلاح الکترومغناطیسی، بمب ویا سیستمهای سیار کوچک در حد وانت ویا کامیون، بکارگرفته می شوند، موضوع اصلی حفاظت الکترومغناطیسی است. درحفاظت الکترومغناطیسی، مخاطرات دیگر مانند جریان های هدایتی والقایی ناشی از رعد و برق، ژنراتورهای برق، سیگنال سیستمهای مخابراتی وهر آنچه که به عنوان سیگنال مزاحم محسوب می شود به حداقل می رسد. طیف فرکانسی تهدیدات طبیعی وناخواسته معمولا محدودتر از طیف تهدیدات الکترومغناطیسی است وبنابراین حفاظت در مقابل تهدیدات الکترومغناطیسی، بقیه موارد را نیز پوشش می دهد. هدف از این آیین نامه، آشنایی با اصول حفاظت الکترومغناطیسی، آموزش ودستورالعملها می باشد. فعالیت های حفاظتی بنابرضرورت در رکها، تجهیزات الکترونیکی ومخابراتی، اتاقها وسالنها، سیستم تغذیه الکتریکی، کابلهای دیتا وصوت، دیواره ها، چاههای زمین و لوله کشیها انجام می گیرد.

فصل اول، به مفاهیم واصطلاحات پدافند غیر عامل در حوزه تهدیدات الکترومغناطیسی پرداخته است. در پیوستهای این فصل، مفاهیم واصطلاحات تخصصی با توضیحات بیشتری ارائه شده است.

فصل دوم، شامل مباحث تخصصی دستورالعملهای پیش از وقوع بحران، حین بحران وپس از بحران می باشد.

فصل سوم، روشهای تست واندازه گیری پارامترهای فنی میزان حفاظت الکترومغناطیسی بخشهای مختلف مرکز، ارائه شده است.

فصل چهارم، بخشهای حساس به تهدیدات الکترومغناطیسی در سازمان وسطح حفاظتی آنها در قالب جداولی آورده شده است. این جداول وپرسش ها برای خودارزیابی حفاظتی سازمان قابل استفاده می باشد.

فصل اول :تعاریف و مراجع

۱-۱-تعاریف

۱-۱-۱ پدافند غیر عامل

شامل کلیه اقدامات به منظور حفظ امنیت، ایمنی وپایداری تجهیزات وشبکه ها می باشد.

۱-۱-۲-تهدید الکترومغناطیسی

تهدیدات الکترومغناطیسی عبارتند از امواج الکترومغناطیسی مخرب که از یک سلاح الکترومغناطیسی بوجود می‌آید. این امواج به صورت پالس بوده ودارای انرژی زیادی می باشند. میدان الکترومغناطیسی حاصل از این امواج، می تواند ولتاژ وجریان بالاتر را به صورت لحظه ای بر کلیه رساناهای موجود، نظیرسیم‌ها، مدارات ولوازم الکتریکی والکترونیکی القاء کند. این پالس باعث سوزاندن ویا مختل کردن، فعال وغیر فعال کردن یک اتصال نیمه هادی ویا تعداد زیادی از آنها در محدوده وسیع می گردد که موجب اختلال درسیستمهای الکترونیکی وارتباطی می شود. منابع بوجود آورنده این بحرانها در دسته بندی سلاحهای غیر کشنده قرار می گیرند(پیوست۱).

مخاطرات الکترومغناطیسی دیگر شامل امواج الکترومغناطیسی انتشاری از سیستمهای رادیویی، مخابراتی، ژنراتورهای الکتریکی وانفجارات اتمی می باشد.

۱-۱-۳- مراکز حیاتی

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات جدی ومخاطره آمیز در نظام سیاسی، هدایت وکنترل وفرماندهی، تولیدی واقتصادی، پشتیبانی، ارتباطی ومواصلاتی، اجتماعی ویا دفاعی با سطح تاثیرگذاری سراسری در کشور گردد.

۱-۱-۴- مراکزحساس

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب وصدمات قابل توجه در نظام سیاسی، هدایت وکنترل وفرماندهی، تولیدی واقتصادی، پشتیبانی، ارتباطی ومواصلاتی، اجتماعی ویا دفاعی با سطح تاثیرگذاری منطقه ای در کشور گردد.

۱-۱-۵- مراکز مهم

مراکزی هستند که در صورت انهدام کل یا قسمتی از آنها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت وکنترل وفرماندهی، تولیدی واقتصادی، پشتیبانی، ارتباطی ومواصلاتی، اجتماعی ویا دفاعی با سطح تاثیرگذاری محلی در کشور گردد.

۱-۱-۶- زمان بحران

زمان بحران، زمانی است که تهدید الکترومغناطیسی به وجود آمده وتجهیزات حفاظت نشده از کار افتاده اند.

۱-۱-۷- آسیب پذیری

در صورتی که قطعات نیمه هادی مدارات منطقی، خازن ومقاومتها در هرمجموعه الکترونیکی در اثر وقوع بحران دچار اختلال در عملکرد شوند به عنوان بخش های آسیب پذیر شناخته می شوند. این آسیب پذیری می تواند معیوب شدن یک قطعه ویا به هم ریختگی و اختلال در عملکرد آنها باشد(پیوست۲).

۱-۱-۸-مقاوم سازی

مقاوم سازی شامل انجام اقدامات حفاظتی لازم برای اطمینان از عدم آسیب پذیری تجهیزات الکترونیکی، مخابراتی، کنترلی وحفظ قابلیت ادامه فعالیت در سیستم ها در زمان وقوع تهدید الکترومغناطیسی می باشد(پیوست٤).

۱-۱-۹- راهبردهای حفاظتی

راهبرد حفاظتی، برای تعیین محدوده تعریف شده ای از سطح عملکرد یک سازمان بر اساس خط مشی های پدافندی، مدیریتی وفنی سازمان در شرایط وقوع تهدیدات الکترومغناطیسی می باشد. این راهبرد می تواند برای یک سازمان بر اساس موارد زیر تدوین گردد(پیوست۳) :

۱ -حفظ کل فرآیند تولید واجرای فعالیتهای مهم به همراه کمترین آسیب پذیری تجهیزات.

۲ -فقط تداوم تولید و فعالیت اصلی.

۳ -حفظ تجهیزات پشتیبان مرتبط با فعالیت اصلی سازمان.

۱-۱-۱۰-سطوح حفاظتی

سطوح حفاظتی به معنی میزان حفاظت یا مقاوم سازی مورد نیاز برای یک بخش از سایت یا مرکز می باشد. این مقدار بصورت عددی وبرحسب دسی بل است وبر اساس پارامترهای فنی مختلف استخراج می گردد. سه سطح حفاظتی برای ساختارهای مختلف تعریف گردیده است(پیوست۳).

۱-۱-۱۱-تداوم کار در زمان بحران

انجام مقاوم سازی الکترومغناطیسی وافزایش توان دفاعی وحفاظتی سیستمها در برابر حملات الکترومغناطیسی آفندی ویا فعالیت های خرابکارانه ستون های نفوذی به صورتی که سیستم قابلیت ادامه انجام کار بدون وقفه ویا با وقفه های محدود را داشته باشد .

۱-۲-منابع

منابع اصلی این آیین نامه جهت تدوین عبارتند از:

۱ -گزارش شناسایی و بررسی پالسهای الکترومغناطیسی ناشی از انفجارات هسته ای.

۲ -بررسی وتحلیل پالسهای الکترومغناطیسی ناشی از بمبهای الکترومغناطیسی.

۳ -شناسایی وبررسی منابع مایکرویوی توان بالا.

۴ -ارائه نقاط آسیب پذیر و میزان نفوذ امواج در تجهیزات وساختارها.

۵ -تحلیل وشبیه سازی میزان حفاظت الکترومغناطیسی نقاط کاهنده بخشهای مختلف ساختارها وتجهیزات.

۶ -تحلیل نفوذ امواج الکترومغناطیسی به محفظه ها

۷ -تحلیل القاء امواج الکترومغناطیسی برکابلها

۸ -بررسی اثرات امواج مایکروویوی توان بالا (HPM) وپالس های الکترومغناطیسی (EMP) بر قطعات ودستگاه های الکترونیکی.

۹ -بررسی وارائه نتایج تستها از میزان خرابی وتعیین سطوح اختلال در سیستم ها با توجه به علائم مشاهده شده ناشی از اختلال پالسهای الکترومغناطیسی.

۱۰ -شناسایی وبررسی استانداردهای سازگاری الکترومغناطیسی

این منابع نزد سازمان صادر کننده این سند موجود می باشند. مراجع علمی، تحقیقاتی واستانداردها در این منابع ذکر شده اند.

۱-۳-لغات اختصاری

EMP: **E**lectro**m**agnetic **P**ulse
HPM: **H**igh **P**ower **M**icrowave
UWB: **U**ltra **W**ide **B**and
HEMP: **H**igh **A**ltitude **E**lectro**m**agnetic **P**ulse
EMC: **E**lectro**m**agnetic **C**ompatibility
EMI: **E**lectro**m**agnetic **I**nterference
SE: **S**hielding **E**ffectiveness
RS: **R**adiated **S**usceptibility
CS: **C**onducted **S**usceptibility
RE: **R**adiated **E**mission
CE: **C**onducted **E**mission
ESA: **E**lectric **S**urge **A**rrester
RF: **R**adio **F**requency
dB: **D**ecibel
II: **I**mpulse **I**mpedance
LISN: **L**ine **I**mpedance **S**tabilization **N**etwork

فصل دوم : دستورالعمل ها و ملاحظات مدیریتی-فنی

۲-۱- ملاحظات مدیریتی و فنی قبل از وقوع بحران

رعایت پاره ای الزامات وپیاده سازی آنها در شرایط صلح وقبل از وقوع بحران از نظر مدیریتی، بصورت موثری می تواند هزینه های ناشی از آسیب دیدگی تجهیزات بخشهای مختلف را در شرایط وقوع بحران به میزان زیادی کاهش دهد. نکات مورد نظر شامل موارد ذیل می باشند:

❖ برنامه ریزی استراتژیک و تدوین دستورالعمل های مدیریتی

برای یک برنامه ریزی استراتژیک لازم است که ساختارها ودسته بندی بخشهای مختلف مراکز از لحاظ آسیب پذیری فرآیند ها و عملکردها در برابر تهدید الکترومغناطیسی مورد بررسی واقع شوند. این امر منجر به عدم غافلگیری واستفاده بهینه از توانمندیهای نیروی انسانی وبرنامه ریزی دقیق در شرایط وقوع بحران ودرنهایت مدیریت بحران خواهد شد. با استفاده از برنامه ریزی های استراتژیک، دستورالعمل های مدیریتی(عملکردی و فرآیندی) برای هر بخش از این مرکز به منظور استفاده در شرایط وقوع بحران تهیه گردد.

❖ برآورد آسیب پذیری، مقاوم سازی و دستورالعمل های نگهداری

بررسی وتحلیل آسیب پذیری سیستمها وتجهیزات حساس در برابر تهدیدات الکترومغناطیسی بصورت کامل ودقیق انجام گیرد. این برآورد دقیق، میزان آسیب پذیری تجهیزات در شرایط وقوع بحران را مشخص نموده تا در فرآیند مقاوم سازی، تهیه وانبار داری برخی قطعات وبخش ها استفاده گردد.

بنابر این باید چک لیست دوره ای از تاسیسات مقاوم سازی شده وعملکرد صحیح سیستم های هشداردهنده تهیه شود.

❖ آموزش های عرضی

مدیران وکارشناسان فنی هر بخش به منظور آشنایی با مفاهیم بحران، نحوه اثرگذاری بحران بر روی سیستمها، ارزیابی آسیب پذیری، عملکرد وفعالیت در زمان بحران باید آموزشهای مهارتی دوره ای را طی کنند.

در ادامه به تشریح هریک از این مراحل پرداخته خواهد شد.

۲-۱-۱- برنامه ریزی استراتژیک و تدوین دستورالعمل های مدیریتی

برنامه ریزی استراتژیک باید بر اساس ارزیابی های صورت گرفته که قبلا ذکر شد انجام پذیرد. از نکات مهم در تدوین این برنامه ریزی، در نظر گرفتن اقدامات مقاوم سازی الکترومغناطیسی می باشد. اهم فعالیتها در این بخش عبارتند از:

- توزیع افراد بر اساس تخصص فنی مورد نیاز تعمیر، نگهداری وپشتیبانی هر بخش با تعیین شرح خدمات مشخص برای تیم مورد نظر .
- دفترچه های تعمیر وراه اندازی سیستمهای حساس وآسیب پذیر مربوط به هربخش با استفاده از تیم خبره فنی.
- توجه دقیق به دستورالعمل راه اندازی سیستمها وتجهیزات بخش مورد نظر در شرایط وقوع بحران و پس از بحران .
- تاکید و نظارت بر مقاوم سازی تجهیزات پشتیبان وارزیابی مستمر آنها در بازه های زمانی.
- در صورت توسعه سایت، پیاده سازی واجرای تجهیزات جدید منطبق با اصول پدافند غیر عامل در حوزه بحران الکترومغناطیسی.

۲-۱-۲- برآورد آسیب پذیری، مقاوم سازی و دستورالعمل های نگهداری

تهیه دستورالعمل های شفاف در زمینه بر آورد آسیب پذیری تجهیزات باید با مشارکت افراد متخصص در آسیب شناسی الکترومغناطیسی ومتخصصین کارفرما انجام شود. این بررسی ها در نهایت برای هر بخش منجر به تهیه چک لیست اولیه از لحاظ نوع آسیب، میزان آسیب پذیری، راهکار رفع آسیب (تعمیر، تعویض یا خاموش وروشن شدن مجدد)، زمان لازم جهت راه اندازی وهزینه رفع آسیب خواهد شد.

چک لیست تهیه شده می تواند معیاری برای استخراج هزینه مقاوم سازی وسرمایه گذاری در هر بخش باشد. از مزایای دیگر آن، شفاف نمودن راهکارهای مقاوم سازی برای هر بخش وسهولت در تصمیم گیری مدیران مرکز می باشد.

با توجه به برآورد بدست آمده ودیدگاه مدیران، برای بعضی از بخشهای مراکز تنها باید به مقاوم سازی با استفاده از تجهیزات پشتیبان اقدام شود.

بر اساس برآورد های صورت گرفته وبا در نظر گرفتن معیارها وعوامل مهمی مانند:

- صرفه اقتصادی
- نیاز واقعی برای مقابله با بحران
- توانمندیهای تکنولوژیک به منظور مقاوم سازی
- توانمندیهای اجرایی و قابلیتهای موجود در ساختار سایت
- سرعت عمل اجراء طرح پدافند الکترومغناطیسی
- ملاحظات عملکردی فعالیتهای مراکز در شرایط وقوع بحران

سه راهبرد حفاظتی برای سیستمها، تجهیزات، ساختارها وتاسیسات در برابر تهدید الکترومغناطیسی به منظور تدام کار در زمان بحران، تعیین شده اند که عبارتند از:

۱- راهبرد حفاظتی اول

در این راهبرد، کل فرآیند تولید واجرای فعالیتهای مهم وهمچنین تجهیزات وساختارهای مورد نیاز برای ادامه فعالیت در شرایط وقوع بحران مقاوم می شوند.

۲- راهبرد حفاظتی دوم

در این راهبرد تنها تجهیزات ضروری مورد نیاز فعالیت مرکز ویا سایت حفاظت می شوند.

۳- راهبرد حفاظتی سوم

در این راهبرد، تنها سیستمها و تجهیزات پشتیبان تولید حفاظت می شوند تا پس از وقوع بحران بتوان مجدد سیستمها وتجهیزات مورد نیاز را راه اندازی نمود.

هر یک از راهبردهای ذکر شده، متناسب با تجهیزات، بخشهای مختلف داخلی وحساسیت سیستمها در تاسیسات مراکز، مد نظر قرار می گیرند.

به منظور دستیابی به هریک از راهبردهای حفاظتی مورد نیاز، رعایت سطوح مقاوم سازی در محدوده فرکانسی یک مگا هرتز تا ۱۵ گیگاهرتز ضروری می باشد.

این سطوح مقاوم سازی عبارتند از:

✓ **سطح اول مقاوم سازی**

مقدار این سطح از حفاظت در محدوده ۸۰ الی ۱۰۰ دسی بل می باشد.

✓ **سطح دوم مقاوم سازی**

مقدار این سطح از حفاظت در محدوده ٦٠ الی ۸۰ دسی بل می باشد.

✓ **سطح سوم مقاوم سازی**

مقدار این سطح از حفاظت در محدوده ٤٠ الی ٦٠ دسی بل می باشد.

۲-۲- دستورالعمل پیش از بحران

۲-۲-۱- مقاوم سازی الکترومغناطیسی مراکز و تجهیزات

دراین بخش راهکارهای مقاوم سازی مورد نیاز برای مراکز و تجهیزات منطبق با سطوح حفاظتی ارائه می شود.

اقدامات مورد نیاز مقاوم سازی شامل موارد زیر می باشد:

- ساختمانها(سالن واتاق شامل درب، دیواره، پنجره، کف).
- کابلهای داخلی ساختمان و محوطه بیرونی
- تابلوهای کنترلی، الکترونیکی، الکتریکی و مخابراتی
- چاه زمین
- مدارات محافظ
- سیستمهای حرارتی و برودتی
- سیستمهای ارتباطی
- سیستمهای اطفاء حریق و اعلام هشدار

این راهکارها بر اساس راهبرد وسطح حفاظتی درنظر گرفته شده برای هر بخش از سایت، باید طراحی واجراء شود.

۲-۲-۲- جدول شرح کار موردنیاز هر یک از تاسیسات

برای بخشهایی که راهبرد اول مد نظر می باشد، باید تلاش در جهت دستیابی به بالاترین سطح مقاوم سازی(سطح اول) صورت گیرد. محدودیتهای اصلی که مانع از دستیابی به این سطوح می شوند عبارتند از:

- محدودیت های ساختار موجود
- حساسیت بالای تجهیزات
- تلاش جهت حفظ عملکرد این سیستمها در تداوم فرآیند اصلی سایت
- هزینه های اجرایی

با توجه به این موارد، برای بخشهای مختلف سیستم که این محدودیتها وجود دارد، سطوح مقاوم سازی متفاوت انتخاب می گردد.

روشهای پیاده سازی هر یک از راهکارها بصورت مشروح مطابق با منابع ذکر شده در پیوست٤، ارائه شده است. برای هر یک از تاسیسات شرح کار لازم برای مقاوم سازی در جدول (۲-۱) ارائه شده است.

نکته: در مواردی، حفاظت قسمتهایی از مراکزهمدیگر را کاملتر می کنند که با توجه به سطح بندی آنها می توان حفاظت بیشتری را بدست آورد، بدین ترتیب اطمینان خاطر حداکثری ایجاد می گردد. در مواردی نیز حفاظت از مراکز و تجهیزات می تواند به صورت پله ای انجام شود. به عنوان مثال با در نظر گرفتن سطح حفاظتی سوم برای ساختمان وسطح سوم برای تابلو های تجهیزات، عملکرد حفاظتی برای سیستم های داخل تابلو ها به سطح دوم ارتقاء خواهد یافت.

جدول۲-۱- فعالیتهای حفاظتی مراکز حساس- شبکه بانکی

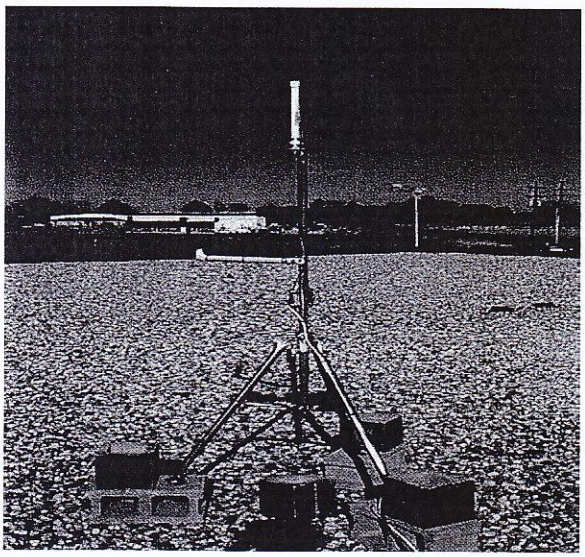
ردیف	نام تاسیسات	راهبرد حفاظتی مورد نیاز	سطح مقاوم سازی مورد نیاز		راهکارهای مقاوم سازی مورد نیاز هریک از تاسیسات															
					دیواره (سطح دوم)	دیواره (سطح سوم)	درب (سطح دوم)	درب (سطح سوم)	پرده	توری زمین	کاتالهای تهویه	مدارات محافظ	پنجره (سطح دوم)	پنجره (سطح سوم)	کابلها	زمین و اتصالات	روکش مقاوم	محفظه مقاوم
۱	دیتا سنتر (بانک مرکزی، شبکه شتاب، شبکه سپهر،سپاد، جام و مشابه)	اول	سالن تجهیزات	سطح سوم	-	√	-	√	√	√	√	√	-	√	√	√	-	-
			اتاق کنترل و مانیتورینگ		-	√	-	√	√	√	√	√	-	√	√	√	-	-
			رک های شامل سوئیچ های مخابراتی/پردازشی		-	√	-	√	-	-	-	√	-	-	√	√	-	-
			کامپیوترها و پردازش کننده ها ی اصلی		-	-	-	-	-	-	-	√	-	-	√	√	-	-
			کامپیوترها و پردازش کننده ها ی پشتیبان	سطح اول	-	-	-	-	-	-	-	-	-	-	-	-	√	√
			سیستمهای ارتباطی پشتیبان	سطح اول	-	-	-	-	-	-	-	-	-	-	-	-	√	√
			سیستمهای ارتباطی موجود	سطح سوم	-	-	-	-	-	-	-	√	-	-	√	√	-	-
			واحد تغذیه	سطح سوم	-	√	-	√	√	√	√	√	-	√	√	√	-	-
۲	ارائه دهنده سرویس ATM سیار (پشتیبان)	اول	اتاق تجهیزات	سطح سوم	-	√	-	√	√	√	√	√	-	√	√	√	-	-
					-	√	-	√	√	√	√	√	-	√	√	√	-	-
			رک های شامل سوئیچ های مخابراتی/پردازشی		-	√	-	√	-	-	-	√	-	-	√	√	-	-
			کامپیوترها و پردازش کننده ها ی اصلی		-	-	-	-	-	-	-	√	-	-	√	√	-	-
			کامپیوترها و پردازش کننده ها ی پشتیبان	سطح اول	-	-	-	-	-	-	-	-	-	-	-	-	√	√
			سیستمهای ارتباطی پشتیبان	سطح اول	-	-	-	-	-	-	-	-	-	-	-	-	√	√
			سیستمهای ارتباطی موجود	سطح سوم	-	-	-	-	-	-	-	√	-	-	√	√	-	-
			واحد تغذیه	سطح سوم	-	√	-	√	√	√	√	√	-	√	√	√	-	-

۳	سیستم آتش نشانی	دوم	سیستمهای ارتباطی پشتیبان	سطح اول	-	-	-	-	-	-	-	-	-	-	-	-	-	-	√	√
			سنسورهای اعلام هشدار	سطح سوم	-	-	-	-	-	-	√	-	-	-	-	-	-	√	-	-
			اتاق مانیتورینگ	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
			سیستمهای ارتباطی موجود	سطح سوم	-	-	-	-	-	-	√	-	-	-	-	-	√	√	-	-
۴	مرکز سیستم برق اضطراری	اول	سطح دوم		√	-	√	-	√	√	√	√	√	-	√	√	-	√	√	-
۵	مرکز مخابراتی	اول	سالن تجهیزات	سوم	-	√	-	√	√	√	√	√	-	√	√	√	√	√	-	-
			تجهیزات ارتباطی پشتیبان	اول	-	-	-	-	-	-	-	-	-	-	-	-	-	-	√	√
			تجهیزات ارتباطی موجود	سوم	-	-	-	-	-	-	√	-	-	-	-	-	√	√	-	-
۶	اتاق مدیریت بحران	اول	سطح دوم		√	-	√	-	√	√	√	√	√	-	√	√	√	√	√	-

۲-۲-۳-شبکه هشدار دهندگی

۲-۲-۳-۱- مشخصات فنی هشداردهنده

سنسورهای هشدار دهنده پالسهای الکترومغناطیسی می توانند هرگونه تهدید الکترومغناطیسی در محدوده فرکانسی ۱ مگاهرتز تا ۱۵ گیگاهرتز را اعلام کنند. این هشدار برای جلوگیری از غافلگیری، شروع آماده باش وعملیات پدافندی لازم است.



شکل۲-۱ – یک نمونه هشدار دهنده تهدید الکترومغناطیسی

۲-۲-۳-۲- محل نصب هشدار دهنده ها

هشدار دهنده ها باید در محلهای مناسبی از نظر انتشار امواج الکترومغناطیسی وفضای سیستم های خودی قرار گیرند. موقعیت نصب هشداردهنده تهدیدات الکترومغناطیسی، با توجه به نوع عملکرد وحساسیت در نظر گرفته شده برای مراکز، بر اساس شرایط زیر انتخاب می شوند:

- میزان گستردگی و بخشهای حساس مراکز، تعیین کننده تعداد هشداردهنده ها ومیزان تراکم آنها می باشد.
- موقعیت مکانی بخش های حساس (داخل یا خارج شهر، موقعیت جغرافیایی زمین ومحوطه بر اساس ملاحظات پدافند غیر عامل)، تعیین کننده محل وتعداد نصب سیستم های هشداردهنده می باشد.

- میزان حساسیت وآسیب پذیری بخشهای حساس مراکز که دارای تجهیزات الکترونیکی، مخابراتی وکنترلی می باشند. این عامل نیزدر تعیین تعداد ومحل نصب هشداردهنده ها موثر است.
- ارتفاع ساختمان و مراکز از سطح زمین نیز در نظرگرفته می شود.

به عنوان مثال: تعداد هشدار دهنده های مورد نیاز یک سایت سرور شبکه بانکی به شرح ذیل است:

- ✓ داخل مرکز سرور : ۱ هشدار دهنده
- ✓ مرکز ستادی: ۱ هشدار دهنده
- ✓ محوطه ساختمان سایت: ۳ هشدار دهنده

۲-۲-۴-آموزش های عرضی

- آموزش مدیران و کارشناسان با مفاهیم بحران الکترومغناطیسی، منابع بحران، آسیب پذیری ها وراهکارهای مقاوم سازی در سطوح مختلف کارشناسی ومدیریتی باید انجام شود. این آموزشها می تواند بصورت کارگاههای آموزشی یک روزه برای مدیران ودوره یک هفته ای برای کارشناسان فنی برگزار شود.

- بروشورها ودفترچه های حاوی اطلاعات کلیدی که دارای نکات مفید پدافندی غیرعامل می باشند باید تهیه ودر اختیار افراد مسئول بخش قرار داده شود.

- آگاه نمودن تیم های تخصصی وآموزش های مستمر جهت راه اندازی بخش آسیب پذیر با کمترین هزینه در شرایط وقوع بحران و پس از بحران انجام شود.

۲-۲-۴-۱- آموزش نصب و قرائت هشدار دهنده ها

این بخش باید بر اساس دستورالعمل نصب، نگهداری وقرائت سیستم هشداردهنده صورت پذیرد.

۲-۲-۴-۲- آموزش آزمایش دوره ای چاه و اتصال زمین

نکات مورد نظر در اجرای اتصال زمین سیستمها وتجهیزات مقاوم شده در برابر تهدید الکترومغناطیسی بصورت ذیل می باشد:

- ساختار ستاره ای یا شعاعی برای زمین باید اجرا گردد. به این دلیل که این نوع زمین دارای تطبیق امپدانس ایمپالسی با ساختار مراکز می باشد. مقاوم سازی در برابر بحران الکترومغناطیسی مسئله ای

اضافه بر مقاوم سازی های متداول می باشد. به همین دلیل باید روش اتصال زمین به اتصالات موجود اضافه گردد.

تطبیق امپدانس ایمپالسی،به منظور تطبیق دادن امپدانس چاه زمین در حوزه فرکانس- زمان (تا محدوده فرکانسی ۱۰۰ مگاهرتز) با امپدانس ساختار مورد نظر می باشد.

- در محل هایی که محافظت کننده ولتاژ وحفاظت کننده های خطوط خارجی سیگنال یا کابلهای ورودی وجود دارد، در نزدیکی آن باید یک ساختار ستاره ای زمین با امپدانس ایمپالسی منطبق با ساختار قرارداده شود.
- لوله ها و مجاری آب باید به سیستم الکترودی زمین(ساختار ستاره ای) متصل شوند تا مانع ورود جریانها به داخل مرکز محافظت شده گردند.
- نول برق AC باید تنها در یک نقطه به زمین متصل شود تا حتی الامکان از خسارتهای ناشی از جریانهای گردشی به ترانسفورمرها جلوگیری شود.

به منظور ایجاد زمین مناسب برای مقاوم سازی در برابر تهدید الکترومغناطیسی وآزمایش دوره ای زمین باید نکات ارائه شده در منابع مورد توجه واقع شود[۱۰].

۲-۲-۴-۳- آزمایش دوره ای اتصالات

برخی نکات قابل ذکر در ارتباط با نحوه اتصالات در یک مجموعه مقاوم شده در برابر بحران الکترومغناطیسی در ذیل ارائه شده است:

- در محل جوشکاری ازجوشهای همگن استفاده شود، در جاهایی که امکان آن وجود دارد. زیرا بهترین روش برای جلوگیری از ورود سیگنال تهدید در محل اتصالات می باشد.
- هنگامی که پیچ برای اتصالات استفاده شده است، بدنه پیچ نباید لحیم یا جوش داده شود. مهره و واشر ها باید در داخل ناحیه شیلد قرارگرفته شوند تا در معرض تابش میدان تهدید نباشد، ملاحظات عایقی نیز رعایت شوند.
- مهره ها باید از لحاظ محکم بودن بصورت دوره ای چک شوند تا در شرایط وقوع بحران اطمینان از عملکرد این بخش وجود داشته باشد.
- لوله ها، کانال لوله وبدنه کانکتورها در محل ورود باید بصورت کامل به بدنه اتاق شیلد لحیم، جوش داده شده باشند ویا از اتصال پیچ ومهره ای مناسب استفاده شود.
- هادی هایی که برای زمین استفاده شده اند نباید به داخل محفظه شیلد و اتاقهای محافظت شده وارد شوند بلکه باید به یک قسمت از بدنه بیرونی با جوش وبست های مناسب اتصال داده شوند.

- اتصالات غیر مستقیم مانند همبندی ها[1] وتسمه ها باید به صورت عملی پهن وتا حد ممکن کوتاه باشند، تا کمترین اندوکتانس برای مسیر جریان ناشی از EMP بوجود آید.

به منظور ایجاد اتصالات مناسب برای مقاوم سازی در برابر تهدید الکترومغناطیسی وآزمایش دوره ای آنها، باید نکات ارائه شده در استانداردها، مورد توجه واقع شود[۱۰].

۲-۳- دستورالعمل های حین وقوع بحران

در شرایط وقوع بحران الکترومغناطیسی، مواردساسی که توسط کارشناسان ومدیران در اسرع وقت باید انجام گیرد عبارتند از:

۱ -به علائم سیستم های هشداردهنده توجه شود.

۲ -صحت عملکرد گیرنده ها وبخشهای مختلف که دارای دریافت کننده های دیتا می باشند، بررسی شود.

۳ -برنامه های اجرایی وبخشهای مختلف الکترونیکی وکامپیوتری بررسی شود.

٤ -دستگاههایی که می توان آنها را خاموش کرد، خاموش شوند.

۵ -سیستمهای اطفاء حریق وعملکرد آنها بررسی شود.

پس از بررسی موارد ذکر شده در بالا، اقدامات ذیل قابل انجام است:

الف: در صورت اعمال شدن راهبرد حفاظتی اول، با توجه به اینکه کل فرآیند وتجهیزات، حفاظت شده واحتمال اختلال در فرآیند اصلی ناچیز است.

- از فرآیند اصلی بازدید وبررسی کلی صورت گیرد.
- سپس از بخش های مختلف تجهیزات، بازدید انجام شود.
- اختلالات احتمالی، شناسایی واقدامات لازم در جهت رفع اختلال صورت گیرد.

ب : در صورت پیاده شدن راهبرد حفاظتی دوم که در آن تجهیزات ضروری حفاظت شده اند، تا در زمان وقوع بحران میزان خسارات مالی زیاد نباشد، به محض هشدار توسط هشدار دهنده ها:

- فرآیند ها خاموش گردد.
- با راه اندازی فرآیند بصورت بخش به بخش، از سالم بودن تجهیزات بخش ها اطمینان حاصل گردد.

---

[1] -Bonding

- در صورت آسیب دیدن بخشی از سیستم، با انجام تعمیرات وتعویض قطعات فرآیند راه اندازی شود.

ج: در صورت پیاده شدن راهبرد حفاظتی سوم، به محض هشدار توسط هشدار دهنده ها، فرآیند از حالت کنترل الکترونیکی خارج گردد. در صورت قطع ارتباطات، سیستمهای ارتباطی پشتیبان حفاظت شده، سیستم های معیوب جایگزین شوند.

دستورالعمل حین وقوع بحران، از لحظه وقوع بحران الکترومغناطیسی آغاز می گردد. عملکرد آن در فعال شدن سیستم هشداردهنده وهمچنین اختلال در عملکرد سیستمها وتجهیزات الکترونیکی، مخابراتی حساس سایت ظاهر می شود. اختلال در عملکرد، سبب وقوع حوادث غیر قابل پیش بینی در سیستمها وتجهیزات مقاوم نشده می شود وتا زمانیکه سیستمها به حالت طبیعی بازنگردند احتمال وقوع هر گونه حادثه ای می باشد.

۲-۳-۱-توجه به هشدار دهنده ها و اعلام آماده باش

تاثیرات مخرب تسلیحات الکترومغناطیسی(وقوع بحران)، ممکن است دارای نشانه های فیزیکی بارز وروشنی نباشند، بدین معنی که تخریب ویا اختلال ایجاد شده در سیستمها را نمی توان براحتی کشف وعیب یابی نمود. حتی ممکن است با خرابی های معمول تجهیزات اشتباه شود.

ماهیت بحران الکترومغناطیسی، انتشار امواج الکترومغناطیسی توان بالا در محیط می باشد. سیستم های هشداردهنده نصب شده در بخشهای مختلف سایت و مراکز، به عنوان گیرنده حساس در برابر این بحرانها می باشند. در صورت وقوع بحران الکترومغناطیسی، این هشداردهنده ها یک واکنش فیزیکی (چراغ هشداردهنده، زنگ های اعلام هشدار و یا علائم بصری مکانیکی) از خود نشان خواهند داد.

در زمان بحران، هنگامی که بخشهای فرآیندی وعملکردی تجهیزات الکترونیکی، مخابراتی، الکتریکی وکنترلی سایت دچار مشکل شده اند، اولین اقدام، بررسی وضعیت سیستم هشداردهنده می باشد. اگر سیستم هشداردهنده فعال می باشد(وجود اعلام خطر) باید دستورالعمل های مربوط به زمان بحران، اجراء شود. در صورتیکه سیستم غیر فعال باشد، تهدید الکترومغناطیسی صورت نگرفته وباید به دستورالعمل های معمول مربوط به تعمیر ونگهداری سیستم ها وتجهیزات مراجعه نمود.

۲-۳-۲- بررسی بخشهای حیاتی و حساس مراکز

در صورت وقوع تهدید وبمنظور جلوگیری از گسترش دامنه آسیب دیدگی، بخشهای حیاتی وحساس مراکز با اولویت اول، باید مورد بازرسی قرار گرفته شود.

پارامترهای مهم در انتخاب بخشهای حیاتی و حساس مراکز شامل موارد ذیل می باشند:

- سیستم های ارتباطی و مخابراتی اصلی به منظور کنترل بحران
- سنسورهای آتش سوزی
- تجهیزات پردازشی و کنترل الکترونیکی

در حین بحران، با توجه به برنامه ریزیهای از قبل صورت گرفته وتوجیه مدیران و کارشناسان فنی هر یک از بخشها، کنترل اوضاع باید بر اساس دستورالعمل های تدوین شده صورت گیرد. به همین منظور جهت مدیریت بحران و کنترل ابعاد آن، آموزشهای پیش از بحران ضروری می باشد.

۲-۴- دستورالعمل های پس از وقوع بحران

۲-۴-۱-توجه به هشدار دهنده ها و اعلام آماده باش

تاثیرات مخرب تهدیدات الکترومغناطیسی برخلاف دیگر تهدیدات دارای نشانه های فیزیکی بارز وروشنی نیستند، بدین معنی که تخریب ویا اختلال ایجاد شده در سیستمها را نمی توان براحتی علت یابی نمود.
ماهیت بحران الکترومغناطیسی، امواج الکترومغناطیسی منتشر شده در محیط می باشد. سیستم های هشداردهنده نصب شده در بخشهای مختلف سایت ومراکز، به عنوان گیرنده حساس در برابر این بحران می باشد. در صورت وقوع بحران الکترومغناطیسی، این هشداردهنده یک واکنش فیزیکی از خود نشان خواهند داد.
پس از گذر از زمان بحران، هشدار دهنده ها بررسی شده ومجدد راه اندازی می شوند ودر صورت خرابی جایگزین می شوند.

۲-۴-۲- برآورد آسیب های وارده

در صورت وقوع تهدید (اعلام خطر توسط سیستم هشداردهنده) ووجود اختلال در عملکرد سیستمها وتجهیزات سایت به دلیل آسیب دیدگی، مراحل ذیل باید به اجرا در آید:

- مراجعه تکنیسین بخش به قسمت آسیب دیده به همراه کارشناسان فنی.

- شناسایی نوع آسیب گذرا یا دائمی بوجود آمده برای بخش.
- ارزیابی عملکرد قطعه یا سیستم آسیب دیده.
- ارائه گزارش مربوط به دسته بندی سیستم ها یا قطعات آسیب دیده به همراه نیازمندیها و ضرورت، به منظور برآورد آسیب جهت راه اندازی مجدد.

نکته مهم:

در شرایط قبل از وقوع بحران، ارزیابی آسیب پذیری سیستمها وتجهیزات حساس این مرکز بصورت کامل انجام گیرد. این امر می تواند به ارزیابی دقیق آسیب پذیری تجهیزات در شرایط وقوع بحران کمک فراوانی نماید. در صورت اجرا شدن این امر، هر بخش دارای چک لیست اولیه از لحاظ نوع آسیب، میزان آسیب پذیری، راهکار رفع آسیب(تعمیر، تعویض یا خاموش و روشن شدن مجدد)، زمان در اختیار جهت راه اندازی وهزینه رفع آسیب خواهد شد. همچنین لازم بذکر است که این چک لیست در فرآیند مقاوم سازی بخش مورد نظر بسیار مفید خواهد بود.

۲-۴-۳-راه اندازی مجدد سیستمها

بر اساس گزارش تهیه شده توسط کارشناسان فنی ونوع آسیب ایجاد شده مراحل زیر باید اجرا شوند.

- بخشهای آسیب دیده از لحاظ ایجاد توقف درعملکرد کلی سیستم باید اولویت بندی شوند.
- با توجه به اولویت مشخص شده، نسبت به راه اندازی آنها اقدام شود.
- در صورتی که آسیب از نوع گذرا باشد، تغذیه سیستم قطع ووصل گردد. در این شرایط امکان راه اندازی وبرگشت به حالت نرمال برای آن وجود خواهد داشت.
- در صورت عدم برگشت به حالت نرمال(با اجرای مرحله قبلی)، متخصصین بخش تعمیر و نگهداری با توجه به دستورالعمل های حفاظتی اقدام نمایند.
- در صورتی که آسیب اساسی باشد، متخصصین بخش تعمیر ونگهداری با توجه به دستورالعمل های حفاظتی اقدام نمایند.

۲-۴-۴-استفاده از سیستمهای پشتیبان حفاظت شده

در شرایط وقوع بحران، امکان آسیب دیدگی برای تجهیزات حساس الکترونیکی ومخابراتی که در انبار قطعات نگهداری می شوند، وجود دارد. توصیه می شود حداقل یک مجموعه از قطعات وتجهیزات اساسی الکترونیکی ومخابراتی که قبلا شناسایی شده اند به صورت پشتیبان در محل امن وحفاظت شده نگهداری شوند تا بعد از بحران بتوان هرچه سریعتر سیستمهای معیوب را تعمیر و بازسازی کرد.

به منظور نگهداری تجهیزات در انبار وهمچنین قطعات وتجهیزات اساسی الکترونیکی ومخابراتی باید به اصول مربوط به مقاوم سازی ارائه شده در پیوست٤ مراجعه نمود.

۲-۴-۵-راه اندازی مجدد فعالیت ها

قبل از وقوع بحران، باید تجهیزات وسیستمهای آسیب پذیری که تداوم فعالیتهای اصلی وابسته به آنها می باشد، شناسایی شوند. جهت راه اندازی مجدد فعالیتهای تولید، نیاز به سیستم و تجهیزات است وباید اصول ذکر شده در بخشهای ۲-٤-۱ تا ۲-٤-٤ به اجرا در آید.

فصل سوم– تست حفاظت الکترومغناطیسی اماکن و تجهیزات الکترونیکی

تهدیدات الکترومغناطیسی بر اساس توضیحات ارائه شده در فصل اول و پیوست ۱ دارای محدوده های فرکانسی وتوان های مختلف می باشند. راههای نفوذ و تاثیر گذاری امواج الکترومغناطیسی بر روی قسمتهای حساس الکترونیکی بخشهای مختلف مراکز شامل موارد زیر می باشد:

- دیواره ها
- درب
- پنجره
- کانالهای تهویه
- آنتن
- زمین
- کابلها و لوله ها

به منظور برآورد وضعیت موجود سایت در برابر این تهدیدها، علاوه بر تئوری، شبیه سازی وتحلیل فنی بخشهای مختلف سایت، نیاز به انجام آزمایش واندازه گیری پارامترهای مختلف است. این آزمایشها پس از اجرای راهکارهای مقاوم سازی الکترومغناطیسی به منظورمحاسبه میزان حفاظت صورت می گیرد. تعیین سطوح مقاوم سازی بر اساس حساسیت تجهیزات داخل مراکز ومیزان حفاظت اولیه ساختار قبل از مقاوم سازی صورت می گیرد.

۳–۱– پارامترهای اندازه گیری در آزمایشها

مبنای انجام روشهای اندازه گیری درآزمایشها استانداردهای معتبر می باشند[۱۰]. معیار تایید یا رد مقاوم سازی های الکترومغناطیسی صورت گرفته برای بخشهای مختلف مراکز، میزان مقاوم سازی تعریف شده برای ساختار وجدول راهکارها می باشد(جدول۲–۱).

امواج الکترمغناطیسی

(محیط بیرون)

[E۲]

[E۱]

(محیط داخل)

شکل۳-۱- نحوه نفوذ امواج الکترومغناطیسی در یک ساختار

اساسی ترین پارامترهایی که در نفوذ والقاء امواج الکترومغناطیسی در بخشهای مختلف باید مورد ارزیابی قرارگیرند عبارتند از:

۱ -اندازه گیری میزان ضریب مقاوم سازی الکترومغناطیسی ساختار

این پارامتر به منظور تعیین اثرات ناشی از وجود شکاف، درزها، بدنه ساختار، کانالهای مختلف ورودی وخروجی هوا، دربها و پنجره ها در ممانعت از ورود میدانهای الکترومغناطیسی به داخل ساختار می باشد. این پارامتر بصورت زیر محاسبه می شود، (شکل۳-۱)[٦].

$$SE(dB)=۲۰\ Log(E_۲/E_۱)$$

$E_۲$: دامنه میدان الکتریکی اندازه گیری شده در شرایط عدم وجود ساختار ویا بر اساس وضعیت موجود در یک نقطه خارجی (بر حسب ولت بر متر).

$E_۱$: دامنه میدان الکتریکی اندازه گیری شده در شرایط وجود ساختار مقاوم سازی شده ویا بر اساس وضعیت مقاوم سازی در یک نقطه داخلی (بر حسب ولت بر متر).

به منظور برآورد مقدار SE برای میدان الکتریکی در محدوده فرکانسی ۱ مگاهرتز تا ۱۵ گیگاهرتز باید اندازه گیری انجام پذیرد.

مقدار SE برای موج الکترومغناطیسی نیز قابل اندازه گیری است که بر حسب توان است.

$$SE(dB)=10\ Log(P_2/P_1)$$

نحوه انجام آزمایش در پیوست۵، ارائه شده است.
با توجه به اینکه منبع تهدید الکترومغناطیسی دارای ماهیت پالسی(گذرا) می باشند، اندازه گیری ها نیز بر اساس این شکل از منابع انجام می شود. این اندازه گیری به عنوان RS[1] نامگذاری شده است[۱۰].

۲ -اندازه گیری میزان القای جریان/ولتاژ ایجاد شده بر روی کابلهای وارد شونده/خارج شونده به ساختار

یکی دیگر از راههای نفوذ امواج الکترومغناطیسی به داخل ساختار حاوی تجهیزات الکترونیکی، کابلهای وارد شونده/خارج شونده متصل به تجهیزات می باشد(پیوست۲، شکل۲-۱). این میدانهای الکترومغناطیسی مخرب، قابلیت القاء جریانهای در حد چند صد آمپر و بالاتر که وابسته به طول کابل وموقعیت نصب آنها می باشد، را دارد. به منظور اطمینان از عملکرد صحیح راهکار مقاوم سازی پیشنهاد شده، نیاز به اندازه گیری پارامتر CS[2] می باشد.

۳ -علاوه بر اندازه گیری پارامترهای ذکر شده، باید برخی آزمایشهای دیگر به عنوان مکمل انجام شود. بررسی اتصالات بین قسمتهای مختلف ناپیوسته(بدنه ساختار وچارچوب درب، درب و چارچوب متصل به آن، همین شرایط برای پنجره ها وکانالها و...) با استفاده از تجهیزات اندازه گیری مقاومت الکتریکی انجام می شود. اتصالات بین زره فلزی کابلها وبدنه فلزی ساختار، قسمتهای مختلف بدنه با یکدیگر نیز از دیگر موارد انجام آزمایش اتصالات می باشد.

٤- پاسخ فرکانسی چاههای زمین طراحی شده در مراکز باید در محدوده فرکانسیDC تا ۱۵ گیگاهرتز، نیازمندی برای مقاوم سازی در برابر تهدیدات الکترومغناطیسی را برطرف نماید. اندازه گیری ها باید نشان دهنده مقاومت در حدود ۵ اهم DC وتطبیق امپدانس با امپدانس ساختار در طیف فرکانسی تهدید را داشته باشد. این اندازه گیریها در محدوده فرکانسی باند پایه اساسی تر است(پیوست۵).

---

[1] - Radiated Susceptibility(RS)
[2] - Conducted Susceptibility(CS)

تذکر: اندازه گیری در بازه فرکانسی ۱ مگاهرتز تا ۱۵ گیگاهرتز انجام می شود.

۳-۲- تجهیزات اندازه گیری مورد نیاز

تجهیزات مورد نیاز جهت اندازه گیری پارامترهای فنی ذکر شده عبارتند از:

- اسپکتروم آنالیزر
- ذخیره ساز دیتا
- آنتنها در محدوده فرکانسی ۱مگاهرتز تا ۱۵ گیگاهرتز
- اسیلوسکوپ حافظه دار
- سنسور میدان مغناطیسی
- تقویت کننده های توان
- تضعیف کننده ها
- LISN[1]
- سیگنال ژنراتور
- پروب اندازه گیری جریان

نکته: میزان حساسیت ونوع تجهیزات اندازه گیری باید بر اساس سطوح حفاظتی مورد نیاز برای بخشهای مختلف سایت، انتخاب واستفاده شود(پیوست۵).

[1] - Line Impedance Stabilization Network

فصل چهارم: خودارزیابی حفاظتی

پس از معرفی تهدیدات الکترومغناطیسی ومکانیزمهای اثر گذاری آنها بر بخشهای مختلف مراکز، دستورالعملهای پیش از بحران، حین وقوع بحران وپس از بحران در دو حوزه مدیریتی و فنی ارائه شده است. به منظور ارزیابی حفاظتی این مرکز پس از مطالعه این بخشها، اقدامات اولیه زیر باید صورت گیرد.

۴-۱- تکمیل پرسشنامه

پرسشنامه ذیل به منظور اطمینان از انجام اقدامات ذکر شده در دستورالعمل ها باید تکمیل گردد (جدول٤-١).

جدول٤-١- پرسشنامه به منظور اطمینان از انجام اقدامات حفاظتی

ردیف	توضیحات	بلی	خیر	تاحدی
١	آیا مدیران مجموعه نسبت به حفاظت سایت توجیه شده اند؟			
٢	آیا آموزشهای لازم به مدیران و پرسنل داده شده است؟			
٣	دستورالعمل های پیش از بحران اجراء شده اند؟			
٤	مراکز و تجهیزاتی که شامل راهبرد اول می باشند، حفاظت شده اند؟			
٥	مراکز و تجهیزاتی که شامل راهبرد دوم می باشند، حفاظت شده اند؟			
٦	مراکز و تجهیزاتی که شامل راهبرد سوم می باشند، حفاظت شده اند؟			
٧	مراکز حفاظت شده تست شده اند؟			
٨	هشداردهنده ها در محل های تعیین شده نصب شده اند؟			
٩	جدول بند٤-٢ که برای مراکز و تجهیزات آن سازمان طراحی شده ، تکمیل شده است؟			

۴-۲- جدول ارزیابی

با توجه به راهکارهای مقاوم سازی مطرح شده در بخشهای قبلی و پیوست ٤، جدول ارزیابی (٤-٢) باید توسط کارشناس ارزیاب تکمیل گردیده و با جدول راهکارهای مقاوم سازی(٢-١) که مشابه همین جدول می باشد مقایسه و درصد محقق شده را محاسبه کند .

جدول٤-٢- ارزیابی حفاظتی مراکز حساس- شبکه بانکی

ردیف	نام تاسیسات	راهبرد حفاظتی مورد نیاز	سطح مقاوم سازی مورد نیاز		ارزیابی راهکارهای حفاظتی														
					دیوار (سطح دوم)	دیوار (سطح سوم)	درب (سطح دوم)	درب (سطح سوم)	پرده	توری زمین	کانالهای تهویه	مدارات محافظ	پنجره (سطح دوم)	پنجره (سطح سوم)	کابلها	زمین و اتصالات	روکش مقاوم	محفظه مقاوم
۱	دیتا سنتر (بانک مرکزی، شبکه شتاب، شبکه سپهر،سیبا، جام و مشابه)	اول	سالن تجهیزات	سطح سوم														
			اتاق کنترل و مانیتورینگ															
			رک های شامل سوئیچ های مخابراتی/پردازشی															
			کامپیوترها و پردازش کننده ها ی اصلی															
			کامپیوترها و پردازش کننده ها ی پشتیبان	سطح اول														
			سیستمهای ارتباطی پشتیبان	سطح اول														
			سیستمهای ارتباطی موجود	سطح سوم														
			واحد تغذیه	سطح سوم														
۲	ارائه دهنده سرویس ATM سیار (پشتیبان)	اول	اتاق تجهیزات	سطح سوم														
			رک های شامل سوئیچ های مخابراتی/پردازشی															
			کامپیوترها و پردازش کننده ها ی اصلی															
			کامپیوترها و پردازش کننده ها ی پشتیبان	سطح اول														
			سیستمهای ارتباطی پشتیبان	سطح اول														
			سیستمهای ارتباطی موجود	سطح سوم														
			واحد تغذیه	سطح سوم														

۱

۳	سیستم آتش نشانی	دوم	سیستمهای ارتباطی پشتیبان	سطح اول														
			سنسورهای اعلام هشدار	سطح سوم														
			اتاق مانیتورینگ	-														
			سیستمهای ارتباطی موجود	سطح سوم														
۴	مرکز سیستم برق اضطراری	اول	سطح دوم															
۵	مرکز مخابراتی	اول	سالن تجهیزات	سوم														
			تجهیزات ارتباطی پشتیبان	اول														
			تجهیزات ارتباطی موجود	سوم														
۶	اتاق مدیریت بحران	اول	سطح دوم															