سال اقتصاد مقاومتی، اقدام و عمل

پدافند غیرعامل

استانداری آذربایجان شرقی
اداره کل پدافند غیرعامل

ماهنامه پدافند غیرعامل

شماره ۱۴ – شهریور ۱۳۹۵

چگونه مودم و شبکه خانگی خود را ایمن تر کنیم؟

این روزها در اغلب منازل می‌توان یک دستگاه مودم مشاهده کرد که شاید فقط یک دستگاه برای اتصال به اینترنت باشد، اما مودم‌ها را باید مهم‌ترین گجت الکترونیکی خواند، چرا که این ابزار به تمام گجت‌های موجود در خانه متصل شده و دروازه‌ی ورود به اینترنت است، از این‌رو مودم‌های مورد استفاده در منازل را می‌توان بهترین گزینه برای نفوذ توسط هکرها خواند.

۱- از بکارگیری مودم‌های بی نام و نشان عرضه شده توسط ISP خودداری کنید.

۲- قطع دسترسی به تنظیمات مودم از طریق اینترنت: برای اغلب کاربران دسترسی تنظیمات مودم از طریق اینترنت و خارج از شبکه‌ی داخلی مودم غیرضروری و بدون استفاده است، از این‌رو، یکی از اصلی‌ترین اقداماتی که باید انجام داد، قطع دسترسی به تنظیمات مودم از طریق اینترنت یا غیرفعال کردن مدیریت از راه دورRemote Management است. در صورتی که وجود چنین قابلیتی ضروری باشد، می‌توان با راه‌اندازی شبکه مجازی خصوصی (VPN)یا (Virtual Private Network)کانالی امن برای دسترسی به شبکه‌ی داخلی و همچنین تنظیمات مبتنی بر وب مودم ایجاد کرد.

۳- محدود کردنIP های درون شبکه که می‌توانند به تنظیمات مودم دسترسی داشته باشند...

(برای دسترسی به کل مطلب روی عنوان اصلی کلیک کنید)

در این شماره خواهید خواند:

خواهشمند است نظرات ، پیشنهادات و یافته های جدید خود را جهت بهبود کیفیت نشریه با ما در میان بگذارید.

شماره تماس: ۳۵۲۹۱۳۳۰

پست الکترونیکی:

padafand.gheyre.amel100@gmail.com

اخبـــــار پدافنـــــــد غیرعامـــــل

اداره کل پدافند غیرعامل استان آذربایجان شرقی با دانشگاه آزاد واحد ایلخچی تفاهم نامه همکاری امضا کرد

به جهت استفاده از ظرفیت ها و توانایی های علمی دانشگاه آزاد واحد ایلخچی، اداره کل پدافند غیرعامل تفاهم نامه همکاری امضا کرد. : هدف از این تفاهم نامه استفاه از توانایی های علمی، پژوهشی و توسعه همکاری های آموزشی، تحقیقاتی و فناوری عنوان شد.

احمد جهانسری مدیرکل پدافند غیرعامل استانداری در خصوص این تفاهم نامه گفت: هدف از این تفاهم نامه استفاه از توانایی های علمی، پژوهشی و توسعه همکاری های آموزشی، تحقیقاتی و فناوری و برطرف کردن نیازهای متقابل است.

جهانسری افزود: دانشجویان تحصیلات تکمیلی دانشگاهها می توانند طرح ها و پروژه های ارشد و دکتری خود را در راستای نیازهای پدافند غیرعامل (اعم از حوزه های زیستی، سایبری، کالبدی و ...) تعریف کنند و از مزایای آن اعم از مزایای مالی یا کاهش مدت زمان سربازی برخوردارد شوند.

هدف سازمان پدافند غیرعامل گفتمان‌سازی و فرهنگ‌سازی مفاهیم غیرعامل است

مدیرکل پدافند غیرعامل آذربایجان شرقی با تاکید بر اهمیت آموزش در توجیه افکار عمومی در این مقوله، گفت: آموزش‌های همگانی ضرورت انکارناپذیر پدافند غیرعامل است.

احمد جهانسری، مدیرکل پدافند غیرعامل آذربایجان شرقی در نشست روسای ادارات ورزش و جوانان شهرستان‌های استان، اظهار کرد: با توجه به ضرورت‌های موجود باید به نهادینه کردن آموزش‌های همگانی روی آوریم و بخش مهم وظایف ما متوجه آحاد مردم و آشنا کردن جامعه با مؤلفه‌های تغییر حملات دشمن و همراه کردن بخش خصوصی است.

وی ادامه داد: هدف سازمان پدافند غیرعامل کشور گفتمان‌سازی و فرهنگ‌سازی مفاهیم غیرعامل است و اگر ما در سطح جامعه بتوانیم به آحاد مردم آموزش‌های لازم را بدهیم در برابر تهدیدات مصون خواهیم ماند.

جهانسری با اشاره به نقشی که حملات سایبری در ایجاد شایعه در جامعه و انحراف افکار عمومی دارد، گفت: یکی از رویکردهای محوری و اصلی پدافند غیرعامل سایبری، شناسایی تهدیدها در این فضاست.

وی بر ضرورت فرهنگ‌سازی و ارائه آموزش‌های لازم برای استفاده از وسایل الکترونیکی و ارتباط جمعی تاکید کرد و ادامه داد: باز بودن تمام برنامه‌های نرم‌افزاری تلفن‌های همراه که استفاده‌ای نیز در کشور ما ندارند، می‌تواند آسیب‌زا باشد.

شناسایی ویروس های کامپیوتری معروف و از بین بردن آنها از طریق ریجستری

محسن محمودی[۱]– نوید غلامزاده[۲]

مقدمه:

ویروس های کامپیوتری از جمله موارد اسرارآمیز و مرموز در دنیای کامپیوتر بوده که توجه اغلب کاربران را بخود جلب می نماید. ویروس های کامپیوتری بخوبی قدرت آسیب پذیری سیستم های اطلاعاتی مبتنی بر کامپیوتر را به ما نشان می دهند. یک ویروس مدرن و پیشرفته قادر به بروز آسیب های کاملا غیرقابل پیش بینی در اینترنت است . مثلا ویروس ملیزا (Melissa) ، که در سال ۱۹۹۹ متداول گردید ، از چنان قدرت و توانی برخوردار بود که شرکت های بزرگی نظیر مایکروسافت و سایر شرکت های بزرگ را مجبور به خاموش نمودن کامل سیستم های پست الکترونیکی نمود. ویروس "ILOVEYOU" ، که در سال ۲۰۰۰ رایج گردید ، باعث آسیب های فراوان در اینترنت و شبکه های کامپیوتری گردید.

❖ تعریف ویروس[۳]

ویروس، یک نوع بدافزار است که در اغلب مواقع بدون اطلاع کاربر اجرا شده و تلاش می‌کند خودش را در یک کد اجرایی دیگر کپی کند.[۴] وقتی موفق به انجام این کار شد، کد جدید، آلوده نامیده می‌شود. کد آلوده وقتی اجرا شود، به نوبه‌ی خود کد دیگری را می‌تواند آلوده کند. این عمل تولید مثل یا کپی‌سازی از خود بر روی یک کد اجرایی موجود، ویژگی کلیدی در تعریف یک ویروس است. معمولاً کاربران رایانه به ویژه آنهایی که اطلاعات تخصصی کمتری درباره کامپیوتر دارند، ویروس‌ها را برنامه‌هایی هوشمند و خطرناک می‌دانند که خود به خود اجرا و تکثیر شده و اثرات تخریبی زیادی دارند که باعث از دست رفتن اطلاعات و گاه خراب شدن کامپیوتر می‌گردند در حالیکه، طبق آمار تنها پنج درصد ویروس‌ها دارای اثرات تخریبی بوده و بقیه صرفاً تکثیر می‌شوند. بنابراین یک ویروس رایانه‌ای را می‌توان برنامه‌ای تعریف نمود که می‌تواند خودش را با استفاده از یک میزبان تکثیر نماید. باتوجه به این تعریف اگر برنامه‌ای وجود داشته باشد که دارای اثرات تخریبی باشد ولی امکان تکثیر نداشته باشد، نمی‌توان آن را ویروس نامید. بنابراین ویروس‌های رایانه‌ای از جنس برنامه‌های معمولی هستند که توسط ویروس‌نویسان نوشته شده و سپس به طور ناگهانی توسط یک فایل اجرایی و یا جا گرفتن در ناحیه سیستمی دیسک، فایل‌ها و یا کامپیوترهای دیگر را آلوده می‌کنند. در این حال پس از اجرای فایل آلوده به ویروس و یا دسترسی به یک دیسک آلوده توسط کاربر دوم، ویروس به صورت مخفی نسخه‌ای از خودش را تولید کرده و به برنامه‌های دیگر می‌چسباند و به این ترتیب داستان زندگی ویروس آغاز می‌شود و هر یک از برنامه‌ها و یا دیسک‌های حاوی ویروس، پس از انتقال به کامپیوترهای دیگر باعث تکثیر نسخه‌هایی از ویروس و آلوده شدن دیگر فایل‌ها و دیسک‌ها می‌شوند. لذا پس از اندک زمانی در کامپیوترهای موجود در یک کشور و یا حتی در سراسر دنیا منتشر می‌شوند. از آنجا که ویروس‌ها به طور مخفیانه عمل می‌کنند، تا زمانی که کشف نشده و امکان پاک سازی آنها فراهم نگردیده باشد، برنامه‌های بسیاری را آلوده می‌کنند و از این رو یافتن سازنده و یا منشاء اصلی ویروس مشکل است.

❖ ویروس ها را در کجای کامپیوتر باید جستجو کرد؟

ویروس هم مانند هر برنامه کامپیوتری نیاز به محلی برای ذخیره خود دارد. ولی این محل باید به گونه‌ای باشد که ویروس‌ها را به وصول اهداف خود نزدیکتر کند. همان گونه که قبلاً ذکر شد اکثر ویروس‌ها به طور انگل‌وار به فایل‌های اجرایی می‌چسبند و آنها را آلوده می‌کنند. اصولاً می‌توان فایل‌ها را به دو گونه کلی «اجرایی» و «غیر اجرایی» تقسیم کرد که عموم ویروس‌ها در فایل‌های اجرایی جای گرفته و آنها را آلوده می‌کنند و واقعاً کمتر ویروسی یافت می‌شود که در یک فایل غیراجرایی قرار بگیرد و بتواند از طریق آن تکثیر شود.

از این نوع فایل‌ها می‌توان به فایل‌های اچ‌تی‌ام‌ال[۴] و مستندات برنامه‌های اداره اشاره کرد که به ترتیب ممکن است شامل اسکریپت و ماکرو باشند.

---

[۱] کارشناس ارشد پیشگیری از جرایم- دانشگاه امین

[۲] کارشناس ارشد مهندسی تجارت الکترونیک، دانشگاه آزاد اسلامی واحد قزوین، دانشکده مهندسی برق و کامپیوتر

[۳] virus

اسکریپت‌ها و ماکروها قسمت‌هایی اجرایی هستند که در دل این فایل‌ها قرار گرفته و کار خاصی را انجام می‌دهند. بنابراین یکی از اصلی‌ترین میزبان‌های ویروس، فایل‌های اجرایی هستند. در اینجا، جهت شناسایی فایل های اجرایی پسوند این فایل ها را آورده ایم:

.com ،.exe ،.dll ،.ovl ،.bin ،.sys ،.dot ،.doc ،.vbe ،.vbs ،.hta ،.htm ،.scr ،.ocx ،.hlp ،.eml

❖ ویروس ها در کامپیوتر چه کار می کنند؟

۱ - بسیاری از ویروس‌ها دارای اثراتی هستند که هرچند تخریبی نمی‌باشد ولی می‌تواند برای کاربر ایجاد مزاحمت کند. مثلاً ممکن است پیغامی نمایش دهد، باعث ریزش حروف صفحه نمایش به پایین شود یا اینکه یک آهنگ پخش نماید. علاوه بر این برخی از ویروس‌ها به علت اشکالات نرم‌افزاری که ناشی از عدم دقت ویروس‌نویس می‌باشد، ممکن است دارای اثراتی غیرقابل پیش‌بینی باشند که گاهی این اثرات می‌توانند تخریبی نیز باشند. از دیدگاه کاربر اهمیتی ندارد که خسارت ایجاد شده بوسیله یک ویروس، یک کار عمدی پیش‌بینی شده توسط نویسنده ویروس بوده باشد یا یک اشتباه برنامه‌نویسی.

۲ - برخی از ویروس‌ها در حافظه کامپیوتر مقیم شده و از این طریق عملیات تکثیر خود را انجام می‌دهند. این عمل ممکن است به گونه‌ای باشد که جایی برای اجرای برنامه‌های دیگر نماند و یا باعث ایجاد تأخیر یا وقفه در حین عملیات سیستم اعم از اجرای برنامه‌ها و یا راه‌اندازی کامپیوتر گردد.

۳ - فرض کنید که شما یک ویروس بر روی کامپیوتر خود داشته باشید. بسیار احتمال دارد که این ویروس به صورت غیرعمدی به یک دوست، همکار یا مشتری منتقل شود که این امر ممکن است باعث از بین رفتن اعتماد آنها به شما و شرکت شما شود.

۴ - ویروس‌ها و برنامه‌های مخرب زیادی وجود دارند که اقدام به سرقت اطلاعات و کلمات عبور کاربر می‌نمایند. بعضی از اینگونه برنامه‌ها با مقیم شدن در حافظه از عباراتی که توسط شما تایپ می‌شود گزارش گرفته و پس از اتصال رایانه شما به اینترنت این اطلاعات را برای مقصد خاصی ارسال می‌کنند. گیرنده این اطلاعات می‌تواند به راحتی از آنها سوء استفاده‌های مختلفی نماید.

علاوه بر همه اینها هیچ ویروسی کاملاً بی‌ضرر نیست و در خوشبینانه‌ترین حالت، آنها وقت شما، وقت پردازنده و فضای دیسک شما را تلف می‌کنند.

در مورد اثرات تخریبی ویروس‌هایی که آنها را به صورت عمدی انجام می‌دهند می‌توان به موارد زیر اشاره نمود:

۱- تخریب یا حذف برنامه‌ها و اطلاعات بخش‌های مختلف دیسک‌ها.

۲- فرمت کردن دیسک‌ها.

۳- کد کردن اطلاعات و برنامه‌ها.

۴- تخریب اطلاعات حافظه فلش ها.

❖ تقسیم بندی انواع ویروس ها بر اساس محلی که آنجا را اشغال می کنند.

۱ - ویروس‌های فایلی[۵] : ویروس‌های فایلی، معمولاً فایل‌های اجرایی را آلوده می‌کنند. فایل‌های آلوده به این نوع از ویروس‌ها اغلب (اما نه همیشه) دارای پسوند .com یا .exe هستند.

۲ - ویروس‌های ماکرو[۶] : ویروس‌های ماکرو، مستندات برنامه‌هایی را که از امکان ماکرونویسی پشتیبانی می‌نمایند مانند (MS Word) و (MS Excel) آلوده می‌کنند. فایل‌های اینگونه برنامه‌ها اجرایی نیستند ولی درون آنها قسمت‌هایی اجرایی به نام «ماکرو» وجود دارد که می‌تواند میزبان مناسبی برای ویروس‌های ماکرو باشد.

---

[۴] HTML

[۵] File Viruses

[۶] Macro Viruses

۳- ویروس‌های بوت و پارتیشن سکتوری[۷] : اینگونه ویروس‌ها سکتور راه‌انداز[۸] دیسک سخت و دیسکت فلاپی یا جدول بخش‌بندی دیسک‌های سخت را آلوده می‌کنند. با راه‌اندازی سیستم از روی دیسکی که به اینگونه ویروس‌ها آلوده شده است، ویروس در حافظه مقیم شده و متعاقباً دیسک‌هایی را که مورد دسترسی قرار گیرند، آلوده می‌کند.

۴ - ویروس‌های اسکریپتی[۹] : این ویروس‌ها که اسکریپت‌های نوشته شده به زبان‌های ویژوال بیسیک یا جاوا می‌باشند، تنها در کامپیوترهایی اجرا می شوند که بر روی آنها اینترنت اکسپلورر[۱۰] یا هر مرورگر وب دیگری با توانایی اجرای اسکریپت‌ها، نصب شده باشد و فایل‌های با پسوند .html ، .htm، .vbs، .js، .htt یا .asp را آلوده می‌کنند.

ویروس‌ها جدا از تقسیم‌بندی فوق، ممکن است در یک یا چند دسته از دسته‌های زیر نیز قرار بگیرند:

- ویروس‌های مقیم در حافظه [۱۱]: اینگونه ویروس‌ها با مقیم شدن در حافظه، هنگام دسترسی به فایل‌های دیگر، آنها را آلوده می‌کنند.
- ویروس‌های مخفی‌کار[۱۲]: اینگونه ویروس‌ها به روش‌های مختلف ردپای خویش را مخفی می‌کنند. به این معنی که فایل‌های آلوده به اینگونه ویروس‌ها به گونه‌ای نشان داده می‌شود که یک فایل غیرآلوده جلوه کند. به عنوان مثال، عموم ویروس‌ها پس از آلوده کردن یک فایل، اندازه آن را افزایش می‌دهند و یا گاهی تاریخ و زمان ضبط فایل را عوض می‌کنند. اما ویروس‌های مخفی‌کار می‌توانند با روش‌های خاص و بدون تغییر وضعیت ظاهری، عملیات خویش را انجام دهند.
- ویروس‌های کدگذاری شده[۱۳]: این ویروس‌ها پس از هر بار آلوده‌سازی، با استفاده از شیوه‌های خود رمزی شکل ظاهری خود را تغییر می‌دهند.
- ویروس‌های چندشکلی[۱۴]: اینگونه ویروس‌ها با استفاده از الگوریتم‌های خاص، علاوه بر تغییر شکل ظاهری خود، ساختار خود را نیز تغییر می‌دهند به طوریکه ممکن است جای دستورالعمل‌ها و حتی خود دستورالعمل‌ها نیز تغییر کنند.
- ویروس‌های فعال‌شونده بر اساس رویداد خاص[۱۵] : ویروس‌هایی هستند که بخشی از عملیات تخریب خود را در ساعت و یا در تاریخ خاص انجام می‌دهند. البته باید توجه داشت که تکثیر و آلوده‌سازی فایل‌ها در تمام اوقات فعال بودن ویروس انجام می‌شود.

❖ نشانه های وجود ویروس در سیستم کامپیوتری

معمولاً سیستمی که به ویروس آلوده می‌گردد نشانه‌هایی را از خود بروز می‌دهد که با دقت در آنها می‌توان به ویروسی بودن احتمالی سیستم پی برد. بعضی از این نشانه‌ها در زیر آمده است. اما باید دقت داشت که این نشانه‌ها ممکن است در اثر عوامل غیرویروسی نیز ظاهر گردد. اما اگر کامپیوتر بطور عادی کار می‌کرده و ناگهان و بدون هیچگونه دستکاری، این علایم را از خود بروز می‌دهد، احتمال وجود ویروس بیشتر است.

۱ - سیستم در هنگام راه‌اندازی قفل می‌کند و احتمالاً پیغام‌های غیرمعمول روی صفحه ظاهر می‌گردد.

۲ - هنگام اجرای برنامه‌ها پیغام کمبود حافظه ظاهر شده و برنامه اجرا نمی‌گردد.

۳ - در کار چاپگر اختلال ایجاد می‌شود یا بدون هیچگونه فرمان چاپی شروع به کار می‌کند.

۴ - امکان دسترسی به برخی از درایوها وجود ندارد.

۵ - هنگام اجرای فایل‌ها، پیغام File is Damaged یا File is Corrupted نمایش داده می‌شود.

۶ - هنگام اجرای یک فایل، کاراکترها و یا پیغام‌های غیرعادی روی صفحه نمایش ظاهر می‌گردد.

---

[۷] Boot Sector and Partition Table Viruses
[۸] Boot Sector
[۹] Script Viruses
[۱۰] Internet explorer
[۱۱] Memory Resident Viruses
[۱۲] Stealth Viruses
[۱۳] Encrypting Viruses
[۱۴] Polymorphic Viruses
[۱۵] Triggered Event Viruses

۷ - هنگام کار در محیط‌های گرافیکی، تصاویر به هم می‌ریزد.

۸ - صداهای غیرمعمول یا موسیقی از بلندگوهای کامپیوتر پخش می‌شود.

۹ - سیستم هنگام اجرای یک برنامه قفل کرده و حتی گاهی فشردن کلیدهای Ctrl+Alt+Del نیز نمی‌تواند سیستم را دوباره راه‌اندازی کند.

۱۰ - اطلاعات بخشی از دیسک سخت و یا تمام آن بطور ناگهانی از بین می‌رود یا دیسک سخت ناخواسته فرمت می‌شود.

۱۱ - اندازه فایل‌های اجرایی افزایش می‌یابد.

۱۲ - خواص فایل‌های اجرایی تغییر می‌کند.

۱۳ - سرعت سیستم بطور نامحسوسی کاهش می‌یابد.

۱۴ - اطلاعات Setup کامپیوتر از بین می‌رود.

۱۵ - برنامه‌ها مراجعاتی به دیسکت انجام می‌دهند که قبلاً انجام نمی‌دادند.

۱۶ - کاهش فضای خالی دیسک بدون اینکه فایلی اضافه شده و یا به محتوای فایل‌ها افزوده شده باشد.

۱۷ - نرم‌افزارهای مقیم در حافظه با خطا اجرا شده یا اصلاً اجرا نمی‌شوند.

۱۸ - بعضی برنامه‌ها سعی در برقراری ارتباط با اینترنت را دارند.

۱۹ - هنگام کار با اینترنت مقدار ارسال و دریافت اطلاعات ناخواسته افزایش یافته و سرعت به شدت افت می‌کند.

۲۰ - نامه‌های الکترونیکی[۱۶] ناخواسته از روی سیستم ارسال شده و یا دریافت می‌گردد.[۱]

---

[۱۶] email

منابع

۱-ویروس ها و بدافزارهای کامپیوتری. دکتر بابک بشری راد، دکتر آرش حبیبی لشکری. انتشارات ناقوس. ۱۳۹۱
۲-مهندسی امنیت شبکه های کامپیوتری،دکتر ناصر مدیری،مهندس مهرداد جنگجو،انتشارات مهرگان قلم،۱۳۸۹
3-Technological networks and the spread of computer viruse, Justin Balthrop, Stephanie Forrest,M. E. J. Newman and Matthew M. Williamson,computer & security 6,19 jul 2004
4-computer viruses theory and experiments,fred cohen,computer &security 6,1987 (22-35)

خلاصه کتاب اصول اولیه امنیت اطلاعات برای شرکت ها و سازمان های کوچک

لیدا رسول اهری[۱۹]

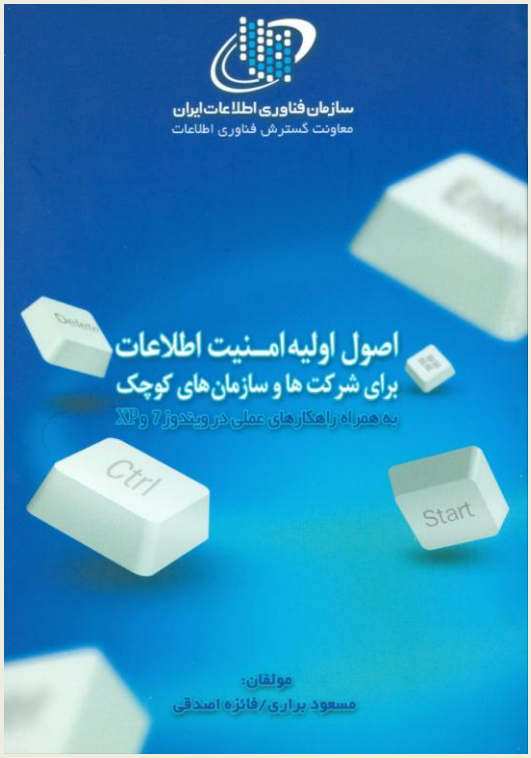
امنیت در شبکه

۱- Simple File Sharing را غیرفعال کنید.

اگر این گزینه فعال باشد، ویندوز به طور پیش فرض به کاربری که بخواهد به این فایل دسترسی داشته باشد کنترل کامل اعطا می کند. بهتر است این گزینه فعال نباشد.

---

[۱۹] کارشناس آموزش و پژوهش اداره پدافند غیرعامل استانداری



در ویندوز 7 :

Control Panel \ Folder Option

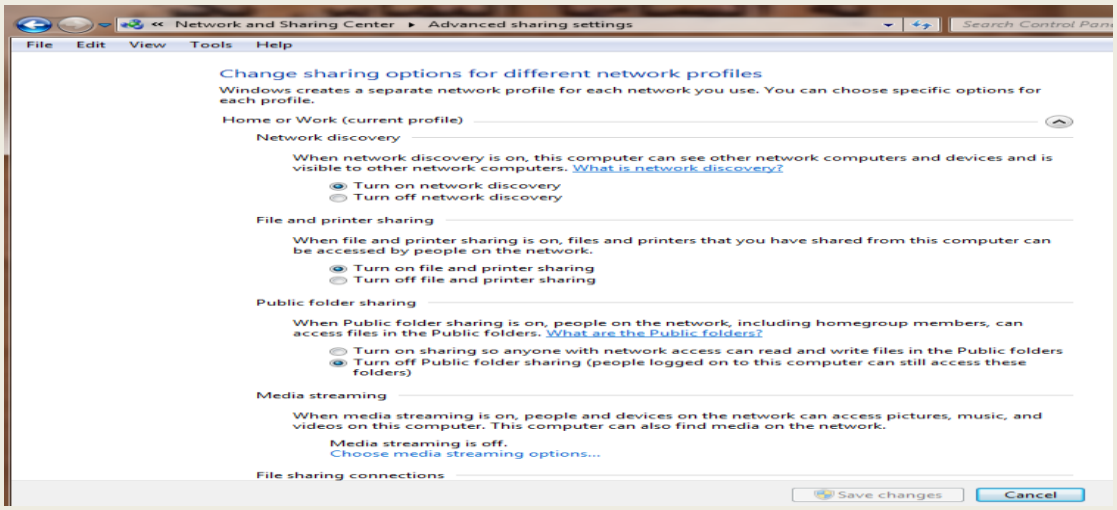
گزینه Use Simple File Sharing را غیرفعال کنید.

۲– غیرفعال کردن به اشتراک گذاری فایل و پرینتر

فایل و منابع به اشتراک گذاشته شده یکی از راه های نفوذ به سیستم توسط هکرهاست.

در ویندوز 7 :

Control Panel \ Network and Sharing Center \ Advanced Sharing Setting



۳– در تنظیمات برنامه های پیغام رسان، بالاترین سطح امنیت را انتخاب کنید.

از رایج ترین راه های نفوذ به کامپیوتر، برنامه های چت و ارتباط آنلاین هستند و مهاجمان از حفره های آن به نفع خود استفاده می کنند.

۴– غیرفعال سازی پیش نمایش در برنامه های مدیریت پست الکترونیکی

برای جلوگیری از ورود ویروس هایی که نامه های الکترونیکی گرافیکی را آلوده می کنند باید پیش نمایش را در برنامه های مدیریت ایمیل از قبیل Outlook غیرفعال کرد.

۵– مرورگر را طوری تنظیم کنید که به طور خودکار به روز شود.

در فایرفاکس:

- Option \ Advanced \ Update \ Automatically Install Update

را فعال کنید.

در مرورگر IE نیز اینکار به طور خودکار همزمان با به روز رسانی ویندوز صورت می گیرد.

۶– ایجاد برخی تغییرات در تنظیمات امنیتی مرورگر

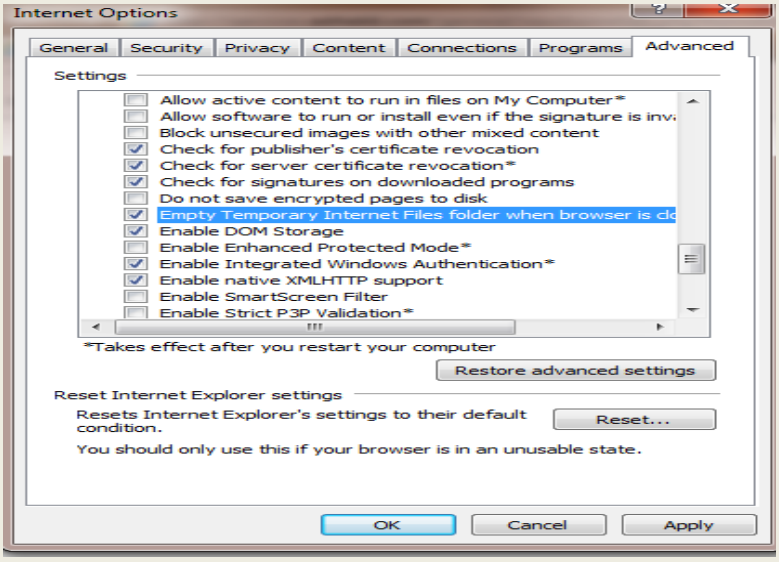
امنیت مرورگر از درجه اهمیت بالایی برخوردار است.

۱– گزینه های زیر باید فعال شوند.

- Check For Publisher s Certificate Revocation
- Empty Temporary Internet File When Browser Is Closed
- Check For Signatures On Downloaded Programs

۲– گزینه زیر غیرفعال شود.

- Enable Install On Demand



۷– در مرورگر خود "جاوا" را غیرفعال کنید.

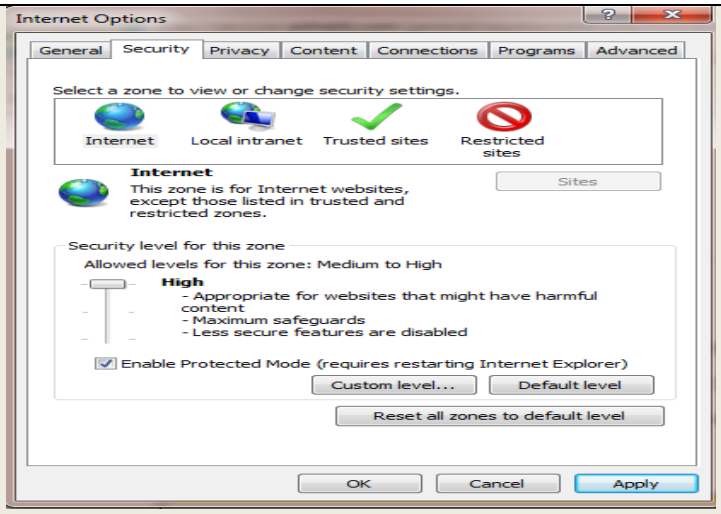
جاوا زبان برنامه نویسی کامل و پیشرفته ای است و اساس آن در برنامه های سمت مشتری برای ایجاد اپلت می باشد. این برنامه های کوچک توسط شبکه اینترنت دریافت شده و درون خود مرورگرها اجرا می شوند. این امکان راه نفوذ مهاجمان به سیستم را مهیا می کند. آنها می توانند کدهای مخرب را در قالب اپلت های قابل اجرا در مرورگرها پیاده سازی کنند و بدون متوجه شدن کاربر، مرورگر آنها را اجرا کند. بهتر است در مرورگر خود جاوا را غیرفعال کنید.

۸– اعمال سیاست های سخت گیرانه بر روی مرورگر

برخی مرورگرها مانند IE سیاست های امنیتی از پیش آماده ای دارند که می توان به راحتی از آن استفاده کرد.

IE \ Tools \ Internet Option \ Security

در هر یک از بخش های اینترنت ، Local Internet ، دکمه Default Level را کلیک کرده، درجه امنیت را روی High تنظیم و در نهایت تغییرات را نهایی کنید.



۹– پروتکل های امنیتی از قبیل SSL و TLS

از راه های افزایش امنیت در هنگام اتصال به شبکه، استفاده از ارتباطات رمز شده است که اطمینان می دهد در صورت شنود اطلاعات، دسترسی به آنها به آسانی ممکن نباشد. باید پروتکل های مربوط به آن از قبیل SSL و TLS در مرورگر فعال باشد.

در IE :

Option \ Advanced

گزینه های SSL و Use TLS را انتخاب کنید.

بررسی تاثیر معماری پایدار در ساختمان های امروزی

با رویکرد پدافند غیرعامل

مسعود میرزاآقاسی[۲۰]

بیان مسئله:

با بررسی کلی در تاریخ معماری و شهرسازی و روش های پدافند غیر عامل در سکونت گاه های انسانی، در می یابیم که حوادث طبیعی و غیر طبیعی (انسان ساز) می تواند در شکل گیری معماری و نحوه زندگی مردم تاثیر بسزائی داشته باشد. در معماری نوین یکی از موضوعات مهم، بحث پایداری بنا وکاهش مصرف انرژی (کاهش هزینه) می باشد،که می توان از این مبحث در جهت پدافند غیر عامل استفاده کرد. بر این اساس نقش و التزام مولفه های معماری پایدار و ابعاد آن در پدافند غیر عامل مورد توجه قرار می گیرد تا بر اساس الگو های پایداری امکان کارآمد ترین رویه مداخلاتی احتمالی در قبل، هنگام و بعد از حوادث طبیعی و غیر طبیعی در بستر نگاهی جامع و فراگیر فراهم شود. الگوهای مهم و تأثیرگذار در طراحی این نوع ساختمانها شامل: حفظ انرژی، هماهنگی با اقلیم، کاهش استفاده از منابع جدید برای مصالح، برآورد نیازهای ساکنان، هماهنگی با سایت و کل گرایی معرفی گردیده است. در ادامه با بررسی الگو های معماری پایدار، معرفی موردی ساختمان هایی که مطابق با این الگو ها هستند و همچنین بررسی میزان تأثیر گذاری معماری پایدار در ساختمان ها(به خصوص ساختمان های دارای اهمیت) و نگاهی ویژه به آینده و نسل های بعد ارائه گردیده است.

کشور ما همواره در معرض بلایای طبیعی و غیر طبیعی(انسان ساز) می باشد و توجه به پدافند غیرعامل در معماری وشهرسازی از موضوعات مهم حال حاضر می باشد.

[۲۰] کارشناس کالبدی اداره کل پدافند غیرعامل استانداری

اما پدافند غیرعامل با رویکرد معماری پایدار از موضوعات ویژه روز دنیا می باشد زیرا امروزه بسیاری از اندیشمندان اعتقاد دارند که توسعه پایدار بدون توجه به مصرف انرژی و محیط پیرامون زندگی بشر امکان پذیر نیست. از این رو فعالیت های انسانی باید در ارتباط با دو مقوله منابع محیطی و مهارت های طراحی هماهنگ با ارزش های اجتماعی و تقویت روابط انسانی انجام پذیرد. معماری پایدار نیز در همین راستا در ارتباط با محیط انرژی و اکولوژی است. در چنین معماری، فضای داخلی به عنوان اجزای به هم پیوسته و یکپارچه، خود دارای هویت مستقلی هستند و در عین حال در فرایندی همه جانبه با فرم ساختمان هماهنگ شده، شاخه های یک معماری پایدار را پدید می آورند(شمیرانی،مدی،۱۳۸۶).

در انتهـا بـا ارائـه راهکارهای پیشنهادی در ساختمان ها(دارای اهمیت) کـه رعایت معمـاری پایـدار در آنها تـأثیر زیـادی در ملاحظات و تقویت دفاع غیرعامل دارد.

اهداف تحقیق

اهداف کلی: بررسی تاثیر معماری پایدار در ساختمان های امروزی با رویکرد پدافند غیرعامل

اهداف جزئی: بررسی الگوهای معماری پایدار در گسترش پدافند غیرعامل در جهت بهینه سازی مصرف، علمکرد مناسب و بیشترین پایداری ساختمان ها در برابر حوادث طبیعی و غیرطبیعی.

مبانی نظری

مفهوم پایداری: ریشه لغوی(sustainable) یا پایداری ازفعل (sustain) به معنای زنده نگه داشتن وتداوم مستمر چیزی است که بنا برتوضیح لغتنامه آکسفورد ازسال درزبان انگلیسی بکار رفته است.

توسعه پایدار: شکلی از توسعه است که با تامین رفاه و سلامت و رفع نیازهای امروز، ضامن سلامت و بقای انسان، محیط زیست و منابع نسل های آینده باشد.

اصول معماری پایدار: صرفه جویی در منابع طراحی برای بازگشت به چرخه زندگی طراحی برای انسان مفهوم معماری پایدار کاربرد مفاهیم پایداری وتوسعه پایدار درمعماری، مبحثی را با عنوان (معماری پایدار)در مباحث معاصر آغاز کرده است.

معماری پایدار

آن گونه از معماری است که شرایط محیطی و سازگاری با اقلیم را مد نظر دارد.
در واقع زیر مجموعه ای از طراحی پایدار است.
عکس العملی منطقی در برابر مسائل و مشکلات عصر صنعت به شمار می رود.

هدف از طراحی ساختمان های پایدار:

بهره‌برداری مناسب از منابع و انرژی
جلوگیری از آلودگی هوا
مطابقت با محیط

چرخه پایداری:

راهکارها و اندیشه های متنوعی در خصوص معماری پایدار مطرح شده است که با عناوین مختلفی از قبیل:

معماری اقلیمی، معماری خورشیدی، معماری سبز، معماری اکولوژیکی، معماری اکو- تک، معماری کربن صفر، معماری با انرژی کم، معماری با انرژی صفر، معماری مبتنی بر انرژی های تجدید پذیرو غیره شناخته شده اند که همه در داخل بحث کلی(معماری پایدار) قرار می گیرند.

معماری پایدار، عکس العملی منطقی در برابر مسائل ومشکلات به وجود آمده عصر صنعت است.

این نوع تعاریف، پایداری را به عنوان مهمترین هدف معماری دانسته وکاهش مصرف انرژی وحفظ

منابع طبیعی برای نسلهای آینده را از مهمترین اقدامات ضروری برای دستیابی به الگوهای پایدار در معماری معرفی می کنند. چارلز جنکز نیز با تأکید بر ابعاد مختلف معماری پایدار سعی می کند تا در بیان اصول کلی این معماری به موارد مختلف مرتبط با آن اشاره کند. او شش اصل کلی را برای معماری پایدار عنوان می کند:

حفظ انرژی

بنا باید طوری ساخته شود که نیاز ساختمان به سوخت های فسیلی را به حداقل برساند.

هماهنگی با اقلیم

- بناها باید طوری طراحی شوند که با اقلیم ومنابع انرژی موجود درمحل احداث، هماهنگی داشته باشند.
- کاهش استفاده از منابع جدید برای مصالح.
- ساختمان ها باید طوری طراحی شوند که میزان استفاده از منابع جدید را تا حد ممکن. کاهش دهند ودر پایان عمر مفید،برای ساخت بناهای جدید بکار روند.

برآورد نیاز های ساکنان

در معماری پایدار برآورده شدن نیازهای روحی وجسمی ساکنان از اهمیت خاصی برخوردار است.

هماهنگی با سایت

بنا باید با سازگاری درمحیط زمین خود قرار گیرد وبا محیط اطراف هماهنگی داشته باشد.

کل گرایی

تمام اصول معماری پایدار باید در یک روند کامل که منجر به ساخته شدن محیط زیست سالم می شود تجسم یابد.

انرژی تجدید پذیر

انرژی تجدیدپذیر (به انگلیسی: (Renewable energy)، که انرژی برگشت‌پذیر نیز نامیده می‌شود، به انواعی از انرژی گفته می شود که منبع تولید آن، بر خلاف انرژی‌های تجدیدناپذیر (فسیلی)، قابلیت آن را دارد که توسط طبیعت در یک بازه زمانی کوتاه مجدداً تجدید شود.

در سال‌های اخیر با توجه به این که منابع انرژی تجدید ناپذیر رو به اتمام هستند این منابع مورد توجه قرار گرفته‌اند. در سال ۲۰۰۶ حدود ۱۸٪ از انرژی مصرفی جهانی از راه انرژی‌های تجدید پذیر بدست آمد. سهم زیست‌توده به‌طور سنتی حدود ۱۳٪، که بیشتر جهت حرارت دهی و ۳٪ انرژی آبی بود.۴/۲٪ باقی‌مانده شامل نیروگاه های آبی کوچک، زیست توده مدرن، انرژی بادی ، انرژی خورشیدی، انرژی زمین گرمایی و سوخت های زیستی می‌باشد که به سرعت در حال گسترش هستند.

انواع انرژی‌های تجدید پذیر عبارتند از:

- انرژی خورشیدی
- انرژی بادی
- انرژی زمین گرمایی
- انرژی آبی (نیروی برق آبی)
- انرژی زیست توده (زیست سوخت)

- انرژی امواج و جزر و مد

سامانه های ایستا:

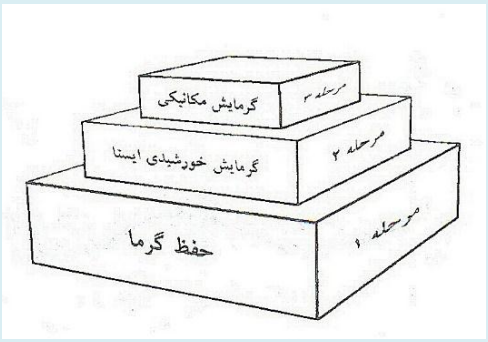
سامانه حرارتی ایستا سیستمی است که در آن عناصر اصلی بنا، انرژی خورشید را جمع آوری، ذخیره و دوباره توزیع می کنند. گرمایش ایستا بر پایه استفاده از انرژی حرارتی خورشید و سرمایش ایستا بر پایه استفاده از کاهنده های گرمایی مختلف استوار هستند. سامانه های ایستا عبارتند از:

۱) هندسه خورشیدی،
۲) سامانه خورشیدی ایستا،
۳) سامانه فتوولتاییک و انرژی خورشیدی پویا،
۴) سایه اندازی،
۵) سرمایش ایستا،
۶) طراحی سایت و برنامه ریزی مجتمع (کی نژاد، 14،1386)

هندسه خورشید:

یکی از نکات قابل توجه درخصوص صرفه جویی در مصرف انرژی توجه به موقعیت قرارگیری خورشید می باشد. توجه به آفتاب زمستانی و پرهیز از آن در تابستان در طراحی اقلیمی از جمله مواردی است که باید به آن توجه نمود و این مهم آنگاه حاصل می شود که در طراحی سایت به آن توجه شود.

سامانه خورشیدی ایستا:



واژه سامانه خورشیدی ایستا به سیستمی اطلاق می شود که انرژی خورشیدی را بدون استفاده از پنکه, پمپ یا کنترل کننده های پیچیده جمع آوری کرده, ذخیره ساخته و دوباره توزیع می کند.

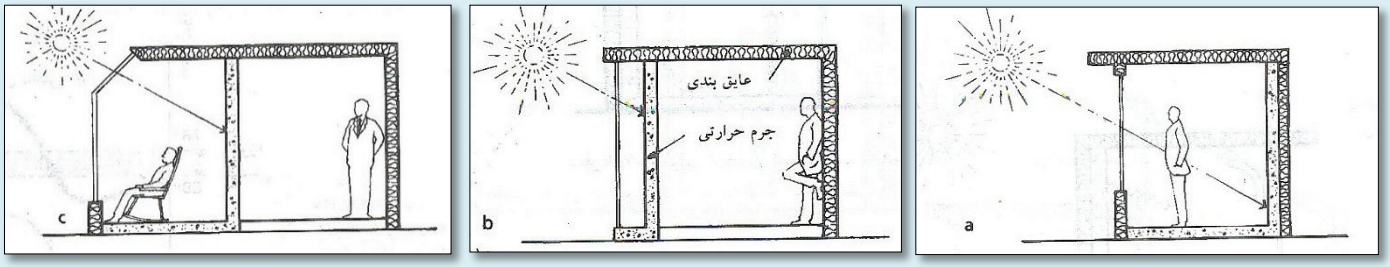
هر سامانه گرمایش خورشیدی ایستا دارای حداقل دو عنصر می باشد:

۱- گرد آور(کلکتور): از شیشه های رو به جنوب تشکیل می شود.

۲- عنصر ذخیره ساز انرژی: از جرم حرارتی نظیرسنگ یا آب تشکیل می شود.

سه نوع اصلی سامانه های خورشیدی ایستا در گرمایش فضا:

الف) جذب مستقیم ب) دیوار ترومب ج) فضای خورشیدی(گلخانه ای)



سامانه جذب مستقیم: هر پنجره ای رو به جنوب یک سامانه جذب مستقیم ایجاد می کند در حالی که پنجره های واقع بر جهت های دیگر, بیش از آنکه گرما را جذب کنند در زمستان, آن را از دست میدهند.جرم حرارتی در داخل ساختمان گرما را جذب می کند تا هم مانع از بر افروختگی ساختمان به هنگام روز شده و هم آن را برای استفاده در شب ذخیره سازد.

سامانه دیوار ترومب: جرم حرارتی در این سامانه ایستا از یک دیوار، درست در سمت داخل شیشه های رو به جنوب تشکیل می شود که همانند سامانه اثر گلخانه ای, امواج تابشی خورشید را محبوس می سازد. از آنجا که سطحی از دیوار که رو به خورشید قرار گرفته است یا با یک پوشش انتخابگر (ورقه سیاه رنگ)پوشانده شده و یا با رنگ تیره, رنگ می شود این سطح در طول روز نسبتا گرم شده و باعث جریان گرما به سمت دیوار می گردد.از آنجا که دیوار ترومب نسبتا ضخیم می باشد اغلب ۱۲ اینچ(۳۰ سانتیمتر) و تاخیر زمانی گرما در آن نسبتا طولانی است گرما تا هنگام عصر به سطح داخلی دیوار نمی رسد.

سامانه فتوولتاییک و سامانه خورشیدی پویا:

سلول های فتوولتاییک که گاه نام سلول های خورشیدی نیز به آنها اطلاق می شود از پولک هایی ساخته می شوند که نور را مستقیما به الکتریسیته تبدیل می کند. کلکتورهای فتوولتاییک و گرد آورهای خورشیدی از نظر تولید انرژی متفاوت هستند.

صفحات فتوولتاییک: انرژی الکتریکی با کیفیت بالا تولید می کنند.

صفحات خورشیدی پویا: انرژی حرارتی کم کیفیت بصورت گرما با دمای پایین تولید می کنند.

اقدامات و فوریتهای پزشکی لازم در مواجهه با حوادث هسته ای

فرزین آقابابایی[۲۱]

چکیده:

از آنجایی خطر حملات هسته ای نسبت به سایر سوانح و بلایا نسبتا جدیدتر است، به نظر می رسد بیشتر اطلاعات مردم در این مورد کم باشد، لذا بـر مـدیران و مسئولان بهداشتی و درمانی است که به روش های مختلف، اطلاعـات لازم را در اختیـار جامعه قرار دهند تا در صورت وقوع چنین حادثه ای هـر کـدام از افـراد جامعه، خود به عنوان یک امدادگر عمـل کننـد . مدیریت بحران چنین حوادثی (چه جنگی و چه غیرجنگی) نیاز به دانسته‌ها و اطلاعاتی خاص اسـت تـا بتوانـد جریان حادثه را به سمت آرامش سوق دهد. ابتدا باید اطلاعات کاملی از محل و چگونگی حادثه اتمی داشته باشد. تعداد تقریبی مصدومان ، وضعیت عمومی آنها ، دوزیمتری منطقه ، نوع ماده آلوده کننده و زمان تقریبی رسیدن مصدوم از محل حادثه تا اورژانس ، از اطلاعات پایه‌ای مدیریت بحران هسته‌ای خواهند بود.

کلمات کلیدی: مدیریت بحران هسته ای، حملات هسته ای، سوخت هسته ای، تهدیدات هسته ای

مقدمه:

نیروگاه‌های هسته‌ای و سوخت هسته‌ای

پس از جنگ جهانی دوم و پس آنکه جهان به عینه به قدرت فوق‌العاده بالای انرژی اتمی پی برد ، متخصصان تولید انرژی متوجه مهار و هدایت کردن این اَبَرانرژی شدند تا از آن برای تولید انرژی الکتریسیته ، نیروی رانشی موتور شناورهای غول‌پیکر ، سفاین فضایی و زیردریایی‌ها استفاده نمایند. از این رو ساخت رآکتورهای هسته‌ای در دستور کار کشورهای صاحب این فنآوری قرار گرفت.

اورانیوم ، فلزی با خاصیت فلزی بسیار بالا ، سوخت چنین رآکتورهایی را تشکیل می‌دهد. سنگ اورانیوم استخراج شده از معادن ، حاوی کانی‌های نامطلوب دیگری است که بایستی پالایش شود. از این رو طی فرآیندی که به «کانه‌آرایی» موسوم است، از سنگ معدن ناخالص ، اورانیوم تقریباً خالص تهیه می‌شود. از این محصول نیز « کیک زرد یا U3O8 » که اکسیداورانیوم می‌باشد ، تهیه می‌گردد.

این کیک زرد نیز طی مراحل پیچیده‌ای به اکسید اورانیوم خالص تبدیل می‌گردد. در این مرحله بسته به اینکه سوخت برای چه رآکتوری تهیه می‌گردد ، مسیر تولید سوخت هسته‌ای وارد دو فرآیند می‌شود. اگر سوخت برای رآکتور آب سنگین تهیه شده باشد ، همین اکسید اورانیوم ، قابل استفاده به عنوان سوخت می‌باشد اما برای رآکتورهای آب سبک بایستی سوخت مورد نظر مراحل پرورش بیشتری را طی نماید. از این رو در کارخانه‌هایی موسوم به « کارخانه‌های UCF » ترکیباتی جدید از کیک زرد تهیه می‌شود که مهمترین آنها UF4 و UF6 می‌باشند. البته گفتنی است در کارخانه‌های UCF محصولات متنوع و سودمند دیگری نیز تولید می‌شوند که در عرصه‌های گوناگون علمی و صنعتی ، از کشاورزی تا پزشکی ، کاربرد دارند. از جمله انواعی از رادیوایزوتوپهای تشخیصی در پزشکی هستند.

UF6 تولید شده که ترکیبی از دو ایزوتوپ اورانیوم با اعداد اتمی 235 و 238 می‌باشد ، وارد دستگاه‌های گریز از مرکز عظیمی می‌شود که به « سانتریفیوژ اتمی » معروفند. این سانتریفیوژهای خاص که دارای عدد گردشی بسیار بالا هستند ، با صرف انرژی زیاد دو ایزوتوپ U235 و U238 را از هم جدا می‌کنند.

---

[۲۱] دکتری مهندسی هسته ای، مدرس دانشگاه

پس از جداسازی ، U235 وارد کارخانه ZPP شده ، از آن قرص سوخت رآکتور آب سبک تهیه می‌شود.
رآکتور آب سنگین می‌تواند از UF6 غنی نشده با غلظت ٪ ۰,۷ استفاده نماید. زیرا در این رآکتورها ، یک پروتون اضافی در هسته اتم هیدروژن سازنده مولکول آب سنگین ، می‌تواند پروتونهای سرعتی را به پروتونهای حرارتی بدل کند. اما در رآکتور آب سبک ، حتماً بایستی از UF6 غنی شده با خلوص بالا استفاده کرد.
سوخت ، در نیروگاه هسته‌ای وارد فرآیند تولید انرژی می‌گردد و طی مراحل پیچیده‌ای یک نوترون به هسته اتم U235 وارد شده و آن را به باریم 144 و کریپتون 90 می‌شکند. حاصل این فرآیند « شکست »، انرژی بسیار بالا و آب خواهد بود. البته در کنار این محصولات ، تا ۲۰۰ نوع ایزوتوپ دیگر نیز تولید می‌شوند که همگی بشدت رادیواکتیو هستند.
حرارت حاصل از سوخت ، به آب خنک کننده منتقل شده ، دمای آن را به ۳۰۰ درجه سانتیگراد می‌رساند. این آب با فشار ۱۵۰ اتمسفر وارد توربین‌های حرارتی تولید برق شده ، باعث چرخش و تولید برق می‌شود. آنچه که مهم است آن است که این بخارات بسیار بسیار رادیواکتیو و سمی هستند. آنگونه که ترکیدن لوله‌های انتقال دهنده آب و بخار ، فاجعه‌بار خواهد بود. در صورت بروز مشکل ، این بخارات با کمک دوش خنک کننده و آب سرد ، به سرعت خنک شده تا به بیرون نشت نکند. گفتنی است حجم آب مورد نیاز برای خنک کردن رآکتورها صدهزار مترمکعب در ساعت است !
امروزه تمامی مراحل شکست اورانیوم و تولید انرژی و حرارت ، درون کره‌ای فلزی با سطح ایمنی بسیار بالا انجام می‌گردد. آنسان که اگر گاز رادیواکتیو به درون کره نشت کند و نتوان آن را با دوش‌های خنک کننده خنک نمود ، از طریق حسگرها ، مجاری کنترلی باز شده و بخار را بعد از فیلتر کردن و جذب خاصیت رادیواکتیوته آن ، وارد دودکشی کرده ، در ارتفاع ۱۰۰ متری زمین به جو وارد می‌کنند.
بهرحال فرآیند تولید انرژی از سوخت هسته‌ای آنچنان پیچیده و محتاج فنآوری پیشرفته است که اختلال در هر مرحله می‌تواند زیانبار باشد. لذا آمادگی علمی و عملی مراکز درمانی نزدیک به این نیروگاه‌ها اجتناب ناپذیر می‌نماید.

تهدیدات هسته‌ای

با توجه به ویژگی‌های حملات هسته‌ای و حوادث تروریستی، این تهدیدها به جبهه جنگ محدود نمی‌شوند و محیط‌های شهری را نیز در معرض خطر قرار می‌دهند. به دنبال چنین حوادثی احتمال آلودگی تعداد زیادی از مردم وجود دارد که با در نظر گرفتن محدودیت‌های بیمارستان‌های نظامی، ضروری است که سایر بیمارستان‌ها نیز آمادگی پذیرش مصدومین را داشته باشند. به گونه‌ای که علاوه بر مداوای بهینه مصدومین، از پخش مواد رادیواکتیو در محیط بیمارستان وآلودگی کادر پزشکی نیز تا حد امکان جلوگیری شود. آماده‌سازی محل پذیرش بیماران، نحوه لباس پوشیدن کادر پزشکی، نحوه خارج کردن لباس‌ها پس از آلودگی‌زدایی و مداوای اورژانس، همگی باید با اصول و ترتیب مشخصی انجام گیرند تا ضمن مداوای مصدومین، سلامت کادر پزشکی نیز در معرض کمترین آسیب قرارگیرد.
پیش از این تماس گسترده با پرتوهای رادیواکتیو در مواردی مانند بمباران اتمی شهرهای هیروشیما و ناکازاکی در جنگ جهانی دوم، بارش اتمی ناشی از آزمایش بمب‌های اتمی، حوادث رآکتورهای هسته‌ای و انتشار مواد از دستگاه‌های رادیوتراپی رخ داده است. در سالهای اخیر با افزایش احتمال وقوع حوادث تروریستی، احتمال وقوع تروریسم هسته‌ای نیز افزایش یافته‌است.
سناریوهای مختلفی در مورد چگونگی وقوع حوادث هسته‌ای مطرح است که از میان آنها می‌توان به انتشار مواد رادیواکتیو با یا بدون استفاده از مواد منفجره ، حمله به رآکتورهای هسته‌ای، انفجار بمب‌های اتمی و سایر سلاح‌های هسته‌ای و حتی انفجار در آزمایشگاه هسته‌ای یک مرکز دانشگاهی اشاره کرد

مدل پیشنهادی، پدافند غیرعامل مبتنی بر مدیریت دانش در زمینه خطرات هسته ای

هدف اصلی این مدل، ایجاد قابلیتهای مدیریت دانش سازمانی برای تسهیل خلق، تبادل، اشتراک، طبقه بندی، نگهداری و به کارگیری دانش برای پدافند غیرعامل است. و این مدل درحوزه های حفاظت فیزیکی، سایبری، انسانی و بهره برداری، ارایه شده است:
مدیریت دانش درموفقیت پدافند غیرعامل از طریق ایجاد استراتژیهای دانش نقش مهمی ایفا میکند .در این زمینه طی بررسیهای به عمل آمده در مورد روشهای استفاده از پدافند غیرعامل و مدلهای علمی مدیریت دانش، مدل ترکیبی پدافند غیرعامل مبتنی بر مدیریت دانش با توجه به شرایط سازمانهای ایرانی ارایه شد به صورتیکه:

۱- ایجاد و استقرار سیستمهای مربوط به هر نهاد و آموزش هر یک از این نهاد ها.
۲- استفاده از تجارب مدیریتی پدافند غیرعامل در زمینه هسته ای از کشورهای دیگر .
۳- حفظ دانش و تجارب از سازمانهای نزدیک مربوطه به پدافند غیرعامل .
۴- جلوگیری از اتلاف هزینه، زمان، دوباره کاری، با تعیین سطح امنیت مناسب.

اقدامات پدافند غیر عامل شامل موارد زیر می باشند:

۱- ارائه مدل اورژانس هسته ای: بدنبال وقوع حوادث هسته ای احتمال آلودگی تعداد زیادی از مردم با مواد رادیو اکتیو وجود دارد که باتوجه به محدودیتهای بیمارستانهای نظامی, ضروری است که سایر بیمارستانها نیز آمادگی پذیرش مصدومین را داشته باشند به گونه ای که علاوه بر مداوای بهینه مصدومین از پخش مواد رادیو اکتیو در محیط بیمارستان، از آلودگی کادر پزشکی نیز تا حد امکان جلوگیری شود. ازآنجا که مدلی در جهت پذیرش مصدومین رادیواکتیو در اورژانس بیمارستانهای کشور وجود ندارد تحقیق کامل و ارائه چنین مدلی برای اورژانس بیمارستانهای کشور ضروری به نظر میرسد که درغالب ارائه طرح تحقیقاتی قابل انجام است.

۲- مطالعه و تحقیقات در زمینه های مختلف : الف) رادیوبیولوژی: مطالعه و تحقیق در زمینه شناخت هرچه بیشتر آثار پرتو های یونساز در سطح سلولی ـ مولکولی و آثار تخریبی آن درپرتوگیریهای حاد ومزمن و آثار زودرس وبخصوص آثار دیررس شامل سرطانها و آثار ژنتیکی و به روزکردن اطلاعات. ب- بیودزیمتری: تحقیقات و بررسیهای آزمایشگاهی در زمینه آثار ناشی از پرتو و تخمین دوز پرتویی هنگام حوادث پرتویی وحملات هسته ای

ج) رادیو تروریسم : ازآنجا که یکی از عوامل موفقیت در میدان نبرد ایجاد وحشت در بین نیروهای مقابل و نیز در بین مردم کشور مورد حمله میباشد و این ایجاد ترور و وحشت میتواند ناشی از عوامل بیولوژیک ،شیمیایی و هسته ای باشد لذا رادیو تروریسم از مسائل مهمی است که باید مورد توجه قرار گیرد رادیوتروریسم شاید به علت وحشت فوق العاده ای که میان مردم ونیرو ها ایجاد میکند بسیار مهمتراز سایر موارد باشد چون به علت عدم آگاهی کامل جامعه از عواقب حوادث هسته ای معمولا ترس شدید و بی مورد درمیان جامعه حاکم میشود و جامعه در مقابل دشمن از لحاظ روانی کاملا خلع سلاح میشود لذا شناساندن عوامل پرتوزا و نحوه برخورد وپیشگیری از عوارض و ایجاد آمادگیهای ذهنی وروانی وکاربردی، تا حدزیادی از این ترس و وحشت می کاهد.

د) مطالعه وتحقیق درزمینه آثار و عوارض انسانی انواع سلاحهای هسته ای و شبیه به آن و نحوه پرتو دهی وتخریب بیولوژیکی آنها.

۳- آشنایی کامل با اجزا و انواع پرتو های ناشی از انفجار هسته ای و ماهیت صدمه رسانی آنها

۴- آشنایی کامل با انواع صدمات ناشی از انفجار هسته ای مانند گرمای فوق العاده، موج انفجار، تشعشعات رادیو اکتیو و الکترومغناطیسی و....

۵- آشنایی کامل به تشخیص نشانه های حملات هسته ای

۶- اقدامات لازم پس از وقوع انفجار؛ مانند تکان ندادن لباسها، بستن دهان و استفاده از ماسک با فیلترهای تنفسی ، همراه نداشتن هر وسیله، پوشاندن بدن با حداکثر البسه خصوصا زخم ها ، استفاده از جلیقه های محافظ ....

۷- توزیع داروهای محافظ پرتو مانند قرص الف : یدید پتاسیم (برای پیشگیری از عوارض غده تروئید)، ب: آمیفوستین (برای پیشگیری از عوارض مخاط دهانی ناشی از پرتو درمانی)، ج: فرآورده های طبیعی بخصوص گیاهان دارویی، (داروهای محافظ پرتو، ترکیباتی هستند که وقتی قبل از حوادث هسته ای و اشعه تجویز شوند، آسیب و مرگ ناشی از

پرتوهای یونیزان را کاهش می دهند .این ترکیبات می توانند قبل از پرتوگیری در بیماران تحت پرتو درمانی، کارکنان مشاغل مرتبط با پرتو و افراد جامعه در مواقع حوادث ناشی از پرتو کاربرد داشته باشند).

۸- اقدامات لازم پس از کم شدن آلودگی یا خروج از منطقه مثل کوتاه کردن مو، شستشوی سریع بدن، بیرون آوردن لباسها، دفع صحیح مواده آلوده، استفاده از عوامل یا داروهای محافظ پرتو و .....

۹- نحوه ساختن جان پناه هسته ای

و به طور کلی درمان مصدومینی که دچار تابش حاد هسته ای مقادیر قابل توجهی از اشعه یونیزان در تمام سطح بدن شده اند از محل بیمارستان و در طی مراحل زیر انجام می پذیرد:

الف: تریاژ : با توجه به اورژانسی نبودن ضایعات پرتویی، تریاژ بر مبنای ضایعات دیگر مثل زخمها و سوختگیها و صدمات تهدید کننده حیات باید صورت گیرد.

ب: اقدامات تشخیصی:

۱- گرفتن شرح حال و تعیین بیماری های زمینه ای و سیستمیک مصدوم(مثل کم خونی، دیابت و)...

۲- پرسش در مورد نحوه ی مواجهه و مکانیسم آسیب (در صورت هوشیاری و داشتن تروما)

۳- بررسی وجود اسهال و استفراغ (زمان بروز اولین استفراغ با دوز جذب شده نسبت مستقیم دارد)

۴- پرسش در مورد وزن مصدوم

۵- انجام دوزیمتری فیزیکی .

۶- پرسش در مورد از دست رفتن سطح هوشیاری و بررسی عملکرد عصبی(خصوصاً سطح هوشیاری)

۷- بررسی وجود علائم سندرم حاد پرتویی .

ج: اقدامات آزمایشگاهی : آزمایشات اولیه جهت مصدوم پرتویی

شامل : شمارش سلول های خونی، لام خون محیطی، آزمایشات بیوشیمی، آنالیز ادرار و مدفوع و الکترولیت های سرم می باشد. اولین اقدامی که باید برای این مصدومین انجام شود : گرفتن نمونه خون برای شمارش کامل سلول های خونی به خصوص تعداد لنفوسیت ها است .

تعداد مطلق لنفوسیت ها، اختصاصی ترین، رایج ترین و مفیدترین شاخص آگاهی دهنده درباره میزان آسیب های پرتویی است که بیمار به آن مبتلا شده است . تعیین سطح پایه تعداد لنفوسیت ها و مقایسه مقادیر بعدی با آن، جهت ارزیابی محدوده ی دوز جذب شده لازم است .در این بیماران باید هر ۶ ساعت تعداد لنفوسیتها را اندازه گرفت . چک مرتب تعداد لنفوسی تها باید حداقل تا ۴۸ ساعت ادامه پیدا کند. به طوریکه در جدول ۱. نشان داده شده است.

جدول ۱. رابطه شمارش مطلق لنفوسیتی با درجه ی وخامت پرتوگیری [3]

شمارش مطلق لنفوسیت‌ها	درجه‌ی وخامت سندرم حاد پرتویی	احتمال زنده ماندن بیمار
۷۰۰ تا ۱۰۰۰	خفیف	قطعی
۴۰۰ تا ۷۰۰	متوسط	احتمالی
۱۰۰ تا ۴۰۰	شدید	ممکن است با درمان های تخصصی زنده بماند
کمتر از ۱۰۰	خیلی شدید	بسیار کم

د: اقدامات درمانی، حمایتی

ه: مراقبت های پرستاری

مراجع:

1. Defence in depth in nuclear safety.158.20.14. INSAG-07 ،2014
2. Radionuclide source terms from severe accidents to nuclear power plants with light water reactors. 212.20.14. INSAG-21 ،2015
3. Basic safety principles for nuclear power plants. 105.12.14. INSAG-08 ،2015
4. INTERNATIONAL ATOMIC ENERGY AGENCY, Decommissioning of Facilities Using Radioactive Material, IAEA Safety Standards Series No. WS-R-5, IAEA, Vienna (2010).
5. INTERNATIONAL ATOMIC ENERGY AGENCY, Regulations for the Safe Transport of Radioactive Material (2012 Edition), IAEA Safety Standards Series No. TS-R-1, IAEA, Vienna (2012).
6. Jarrett D (1999). Medical management if radiation casualties: handbook. AFRRI special publication 99-2. Bethesda, MD.: Armed Forces Radiobiology Research Institute, pp. 69-72.

عناوین رویدادهای مهم خبری	
«برای مشاهده متن کامل خبرها روی آنها کلیک کنید»	
خطرناک‌ترین باج‌افزارهای جهانی به روایت آمار	جنگ بیولوژیک؛ حربه آمریکا برای نابودی نسل‌ها از ویتنام تا منا
نکاتی درباره واکسن آنفلوآنزا	ایران،بزرگترین وارد کننده محصولات تراریخته
نخستین جلسه کارگروه فناوری اطلاعات و ارتباطات پدافند غیرعامل آذربایجان شرقی برگزار شد	رئیس سازمان برنامه و بودجه آذربایجان‌شرقی: مدرسه اقتصاد مقاومتی در استان آذربایجان‌شرقی راه‌اندازی می‌شود
محصولات ضد فرهنگی برای فرهنگی ترین قشر/هجوم خاموش دشمن برای تخریب باورهای دینی دانش آموزان	رئیس نظام پزشکی ایران در گفت‌وگو با تسنیم : پرونده «کیارستمی» مشابه فرآورده‌های خونی آلوده است
مقابله با سونامی فرهنگی نیازمند تولید محتوا برای جوانان است	قوی ترین بمب چربی سوز خانگی

سایت های مرتبط با پدافند غیرعامل	
❖ وب سایت پایداری ملی	http://www.paydarymelli.ir
❖ مرکز مطالعات پدافند غیر عامل	http://www.pdrc.ir
❖ استانداری آذربایجان شرقی – پدافند غیرعامل	http://ostan-as.gov.ir/?PageID=42
❖ پلیس فتا	http://www.cyberpolice.ir/

صاحب امتیاز: اداره کل پدافند غیرعامل استانداری آذربایجان شرقی
مدیر مسئول: سردار احمد جهانسری
سردبیر: دکتر محمد بامدادی
دبیر تحریریه: مسعود میرزا آقاسی
شماره تماس : ۰۴۱-۳۵۲۹۱۳۳۰