



استاندار آذربایجان شرقی:

در عرصه یک جنگ سایبری قرار داریم / امنیت اطلاعات باید در اولویت ادارات قرار گیرد

مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی:
انجمن علمی پدافند غیرعامل
استان، بازوی اجرایی اداره کل
پدافند غیرعامل است



انجمن شعبه
تبریز، بر ضرورت همکاری و تعامل بین اداره
کل و انجمن علمی تأکید کرد.

نشست هم‌فکری مدیر کل و کارشناسان پدافند غیرعامل استان با نماینده مردم آذربایجان شرقی در مجلس خبرگان رهبری



مدیرکل پدافند غیرعامل
استانداری آذربایجان شرقی در
نشست همفکری کارشناسان این
اداره کل با آیت‌الله هاشم‌زاده
هریسی، نماینده مردم استان در
مجلس خبرگان رهبری، اظهار
داشت: اهمیت پدافند غیرعامل را
باید به تمام دستگاه‌های اجرایی
تبیین کرده و در اولویت
برنامه‌های اجرایی قرار داد.

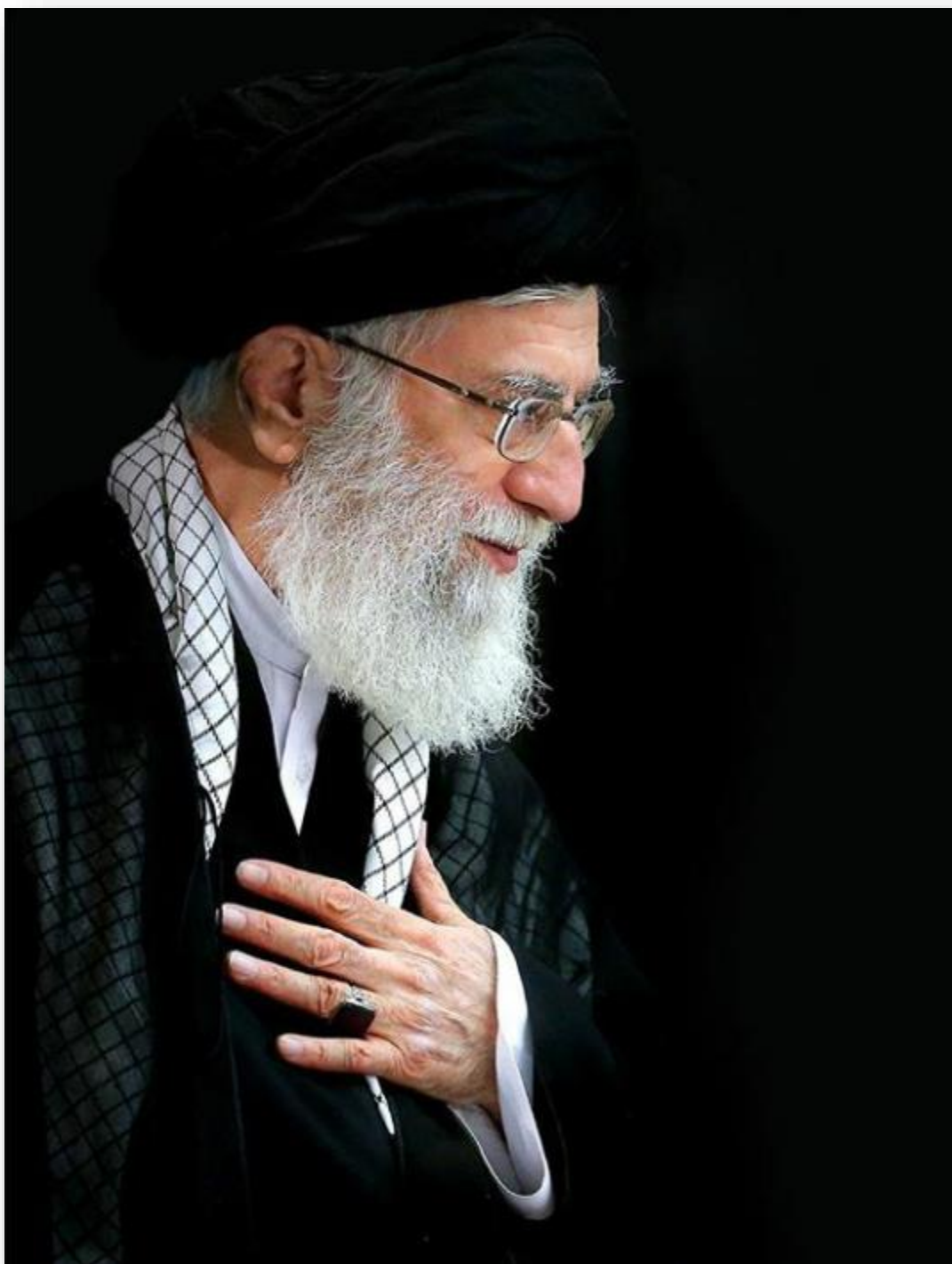
[illegible]

**فراخوان ارسال
مقالات
اولین کنفرانس
ملی پدافند
کالبدی**

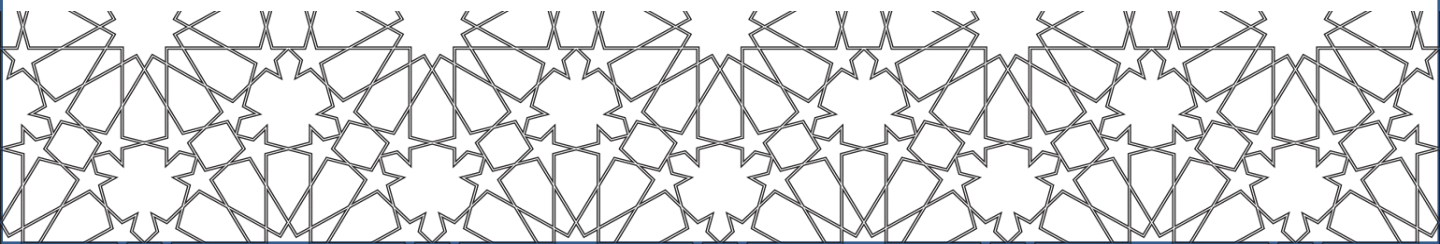
نشست مشترک مدیرکل و کارشناسان پدافند غیرعامل استانداری با معاون هماهنگی امور عمرانی استاندار

مدیرکل پدافند غیرعامل استان آذربایجان شرقی در نشست مشترکی با معاون هماهنگی امور عمرانی استاندار، با اشاره به رسالت حوزه پدافند غیرعامل برای شناسایی تهدیدات و کاهش آسیب‌پذیری‌ها در راستای حفاظت از جان و مال مردم، بر لزوم تعامل این اداره کل با معاونت امور عمرانی تأکید کرد.





باید تدابیر کارساز در باب پدافند غیرعامل را عملی بکنید.





مدیر مسئول : علیرضا کریمی

سر دبیر : محمد بامدادی

دبیر تحریریه : سید هادی سید علیزاده

همکاران این شماره :

علی ابراهیمی، مهرداد مقنی فرسادی، مرتضی
محمدی

نشانی :

تبریز - میدان شهدا - استانداری آذربایجان

شرقی - اداره کل پدافند غیرعامل استان

تلفن : ۰۴۱-۳۵۲۹۱۳۳۰

فکس : ۰۴۱-۳۵۲۹۱۳۵۹



فهرست مطالب

در این شماره خواهید خواند



۵ اخبار پدافند غیرعامل

۸ فراخوان جذب مقاله

۹ معرفی کتاب



۱۰ بخش مقالات و مطالب آموزشی

۱۰ مقاله بررسی فنی اپلیکیشن آپ

۱۱ مقاله بتن های خودترمیم شونده

۱۴ مقاله مقدمه ای بر هوش امنیتی

مقاله اقدامات ایمنی و آمادگی در برابر حوادث

۱۷ هسته ای

۲۰ مطلب علمی

۲۲ عناوین رویداد های مهم خبری

۲۲ طرح های کسر خدمت سربازی

۲۲ سایت های مرتبط با پدافند غیرعامل



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

شماره تماس : ۰۴۱-۳۵۲۹۱۳۳۰



استاندار آذربایجان شرقی:

در عرصه یک جنگ سایبری قرار داریم / امنیت اطلاعات باید در اولویت ادارات قرار گیرد

استاندار آذربایجان شرقی با اشاره به هزینه‌های گزاف در دستگاه‌های اجرایی برای ایجاد و توسعه شبکه‌های کامپیوتری، گفت: اگر به امنیت این شبکه‌ها توجه نکنیم در سر بزنگاه هیچ خاصیتی نخواهند داشت.

دکتر مجید خدابخش در جلسه شورای پدافند غیرعامل استان، با اشاره به اینکه دستگاه‌های اداری در حال گذر از سیستم سنتی به سیستم مدرن هستند، افزود: در این شرایط، نحوه تأمین امنیت منابع هم متفاوت از گذشته است و مدیران باید در این زمینه هوشیار باشند.

وی با بیان اینکه فضای مجازی یک ابزار کمکی برای کارهایی است که در فضای واقعی انجام می‌شود، افزود: مدیران همان‌طور که در فضای واقعی برای امنیت مجموعه‌های تحت مدیریت خود حساسیت دارند در فضای مجازی هم باید این حساسیت را داشته باشند.

استاندار آذربایجان شرقی با اشاره به برخی از آسیب‌های فضای مجازی در دستگاه‌های اداری، بر تفکیک اینترنت و اینترنت در ادارات، آموزش مدیران و نظارت بر نحوه استفاده از اینترنت و نرم‌افزارهای مختلف توسط کارمندان ادارات تأکید کرد.

وی با بیان اینکه هیچ دستگاه دولتی حق ندارد در شبکه‌های اجتماعی ارائه خدمت کرده یا مکاتبات اداری را مبادله کند، اضافه کرد: این کار هیچ ضرورتی ندارد و از نظر قانون جرم است.

خدابخش با بیان اینکه در حال حاضر در عرصه یک جنگ سایبری قرار گرفته‌ایم، گفت: مدیران باید با غیرت و احساس مسئولیت در این عرصه وارد شوند و از امنیت مجموعه‌های تحت مدیریت خود حفاظت کنند.



وی با اشاره به ارزیابی عملکرد دستگاه‌های اجرایی استان از نظر امنیت شبکه، از اداره کل امور مالیاتی استان، پتروشیمی تبریز، مخابرات استان، شرکت‌های توزیع برق تبریز و پالایشگاه تبریز به‌عنوان سازمان‌های موفق در این زمینه قدردانی و به سایر دستگاه‌های اداری استان توصیه کرد از تجربیات این سازمان‌ها استفاده کنند.



استاندار آذربایجان شرقی با بیان اینکه در راستای کاهش مراجعات مردم به ادارات، سامانه‌های دولتی باید به یکدیگر متصل شوند، افزود: این کار با هدف کاهش فساد اداری انجام می‌شود، اما ممکن است موجب افزایش آسیب‌ها و تهدیدهای سایبری نیز بشود که لازم است اقدامات پیشگیرانه در این خصوص صورت گیرد.

نشست همفکری مدیر کل و کارشناسان پدافند غیرعامل استان با نماینده مردم آذربایجان شرقی در مجلس خبرگان رهبری

نماینده مردم آذربایجان شرقی در مجلس خبرگان رهبری اضافه کرد: اصل اول حفظ آرامش و جلوگیری از جنگ بوده و این موضوع در اسلام هم اهمیت دارد؛ اما اگر جنگی را تحمیل کردند، پای پدافند عامل به میان می‌آید. هاشم‌زاده هریسی با بیان اینکه ایستادن در مقابل افراد زورگو کار مقدسی است، خاطرنشان کرد: در شرایط امروز دشمن هر قدر زورگو و فریبکار هم باشد، برنامه‌اش جنگ نظامی با ما نیست، بلکه به دنبال جنگ نرم، جنگ روانی و سایبری است تا بدون هزینه ملت و نظام جمهوری اسلامی ایران را از پای دربیاورد.



نماینده مردم آذربایجان شرقی در مجلس خبرگان رهبری با بیان اینکه امروز در یک جنگ اقتصادی و معیشتی و روانی قرار گرفته‌ایم که هزینه کمتری برای دشمن دارد، ادامه داد: دشمنان جمهوری اسلامی به دنبال جنگ نظامی نیستند و با استفاده از مسائل داخلی می‌خواهند القا کنند که نظام جمهوری اسلامی کارآمد نیست و به کشور ضربه بزنند، که در مقابل این توطئه‌ها پدافند غیرعامل مطرح می‌شود. هاشم‌زاده هریسی اضافه کرد: برای حفظ این نظام خون‌های بسیاری ریخته شده؛ اما نباید در هر کار منتظر معجزه باشیم. امداد غیبی برای زمان درماندگی است و باید براساس قواعد الهی حرکت کرده و به نتیجه برسیم.

مدیر کل پدافند غیرعامل استان آذربایجان شرقی در نشست همفکری کارشناسان این اداره کل با آیت‌الله هاشم‌زاده هریسی، نماینده مردم استان در مجلس خبرگان رهبری، اظهار داشت: اهمیت پدافند غیرعامل را باید به تمام دستگاه‌های اجرایی تبیین کرده و در اولویت برنامه‌های اجرایی قرار داد.

علیرضا کریمی بر استفاده از ظرفیت و جایگاه رفیع روحانیت در راستای نهادینه شدن مفاهیم پدافند غیرعامل تأکید کرد.

نماینده مردم آذربایجان شرقی در مجلس خبرگان رهبری نیز با بیان اینکه جنگ امروز جنگ مشروعیت است، گفت: نظام جمهوری اسلامی ایران بر پایه و اساس مشروعیت شکل گرفته و دشمنان به دنبال این هستند تا مشروعیت نظام را از بین ببرند.

آیت‌الله هاشم‌زاده هریسی با بیان اینکه خوشبختانه در کشور موضوع پدافند غیرعامل مطرح بوده و برنامه‌های خوبی در این خصوص تدوین شده و قابل قدردانی است، اظهار داشت: اما با توجه به وسعت و گستره در برگیری موضوعات در پدافند غیرعامل، نیاز است تا با توجه بیشتر نواقص جبران شود.

وی با بیان اینکه پدافند غیرعامل مهم‌ترین مسأله روز بوده و حتی از پدافند عامل هم مهم‌تر است، اضافه کرد: طی چند سال گذشته موضوع پدافند عامل مقدم تلقی شده و بیشتر بر روی آن کار کرده‌اند، هرچند کارهایی که در این بخش انجام شده مهم بوده و نباید از آن غفلت کرد، اما پدافند غیرعامل باید در اولویت بوده و مقدم بر مسأله پدافند عامل باشد.

مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی: انجمن علمی پدافند غیرعامل استان، بازوی اجرایی اداره کل پدافند غیرعامل است

مدیرکل پدافند غیرعامل استان آذربایجان شرقی در نشستی با اعضای هیأت مدیره انجمن علمی پدافند غیرعامل شعبه تبریز، بر ضرورت همکاری و تعامل بین اداره کل و انجمن علمی تأکید کرد. علیرضا کریمی با اشاره بر پتانسیل بالای انجمن علمی پدافند تبریز، آن را نقطه قوتی برای استان ذکر کرد و گفت: هدف این اداره کل تقویت انجمن و استفاده از پتانسیل بالای آن در امر آموزش است؛ چرا که ما معتقدیم NGOها باید بار اجرایی دولت را برعهده بگیرند و دولت باید ناظر بر عملکرد آن ها باشد.

مدیر کل پدافند غیرعامل استان افزود: برای این کار باید تعاملی شفاف بین دو طرف وجود داشته باشد. کریمی با تأکید بر امر نظارت در دوره های آموزشی گفت: انتظار اداره کل از انجمن علمی ارتقای سطح آموزش ها است و امیدواریم با نظارت و ارزیابی صحیح دوره های آموزشی، این امر صورت گیرد.



وی گفت: باور ما این است که پدافند غیرعامل رفته رفته نقش پر رنگ تری در حوادث جاری دنیا خواهد داشت بنابراین اتاق های فکر انجمن های علمی می تواند راهگشای بسیاری از مباحث جدی مطروحه باشند.

احمد جهانسری، رئیس انجمن علمی پدافند غیرعامل شعبه تبریز و نماینده این انجمن در شمال غرب کشور نیز در این نشست بر ادامه همکاری ها با اداره کل پدافند غیرعامل تأکید کرد و افزود: انجمن علمی با کادر قوی و مجرب خود پتانسیل بالایی در سطح استان و حتی شمال غرب کشور دارد و هدف آن تقویت حاکمیت است.

وی با تشریح اهداف و برنامه های انجمن در سال جاری گفت: تلاش ما این است که ساختار انجمن، کمیته های تخصصی، برنامه های ویژه آموزشی و پژوهشی به طور مفصل در این جلسه تشریح شود و امیدواریم با نظر اعضای هیأت مدیره در خصوص نحوه و چگونگی جذب اعضای جدید نیز تصمیم بگیریم. جهانسری با معرفی دبیران کمیته های علمی تخصصی افزود: ما در معرفی دبیران کمیته های علمی انجمن، افق چند ساله را در نظر گرفته ایم و امیدواریم بتوانیم آموزش ها و همایش های مؤثری را در استان برگزار نماییم.



وی همچنین با تأکید بر شفافیت مالی در انجمن افزود: انجمن علمی از نظارت اداره کل پدافند غیرعامل بر کیفیت و نحوه آموزش ها و همایش ها استقبال می کند و امیدوار است این تعامل و همکاری ثمره قابل قبولی برای استان داشته باشد. در ادامه هر یک از اعضای هیأت مدیره به بیان نقطه نظرات و تشریح برنامه های خود پرداختند.

فراخوان جذب مقاله در اولین کنفرانس ملی پدافند کالبدی



شماره مجوز نمایه در پایگاه استنادی
علوم جهان اسلام ۴۱۰۰۲ - ۹۶۱۷۰



اداره کل پدافند غیرعامل استان آذربایجان شرقی با همکاری دانشگاه های استان برگزار می کند.

کنفرانس دارای تمامی مجوز های علمی از
وزارت علوم، تحقیقات و فناوری می باشد
دارای نمره پژوهشی برای دانشجویان



اولین کنفرانس ملی

پدافند کالبدی با محوریت عمران، معماری و شهرسازی

۲۹ آبان ماه ۱۳۹۷ دانشگاه تبریز



www.ncpd.ir

- مهلت ارسال مقالات کامل: ۱۰ شهریور ماه ۹۷
- اعلام نتایج داوری مقالات: ۲۰ شهریور ماه ۱۳۹۷
- آخرین مهلت ثبت نام در کنگره: ۲۵ شهریور ماه ۱۳۹۷

محور های علمی کنفرانس:

مهندسی عمران

- فناوری های نوین در صنعتی سازی سازه ها با رعایت ملاحظات پدافند غیرعامل
- سیستم های هوشمند در مضمون سازی ساختمان ها و زیرساخت ها
- مبحث ۲۱ مقررات ملی ساختمان
- تولید و کاربرد بتن های توانمند و فوق توانمند
- مصالح نوین ساختمانی از دیدگاه پدافند غیرعامل
- مدیریت ساخت با رویکرد پدافند غیرعامل
- ارزیابی آسیب پذیری و روش های بهسازی و مقاوم سازی سازه ها در برابر ضربه ، نفوذ و انفجار
- مهندسی منابع آب و سازه های هیدرولیکی با رعایت ملاحظات پدافند غیرعامل
- حمل و نقل و ترافیک با رویکرد پدافند غیرعامل
- تاسیسات مکانیکی و برقی در سازه های امن
- برنامه ریزی ، مدیریت و طراحی شهری با رویکرد پدافند غیرعامل
- شهرسازی و توسعه شهری پایدار و تاب آور
- سبک شناسی معماری با رویکرد پدافند غیرعامل
- معماری ایرانی و اسلامی از دیدگاه پدافند غیرعامل
- معماری فضاهای امن سطحی و زیر زمینی
- طراحی معماری صنعتی با رویکرد پدافند غیرعامل
- مرمت ابنیه تاریخی از دیدگاه پدافند غیرعامل
- محاسبه ریسک زیر ساخت های شهری از منظر پدافند غیرعامل
- مکان یابی و مکان گزینی زیر ساخت های شهری از دیدگاه پدافند غیرعامل
- تعیین تاب آوری زیر ساخت ها با رویکرد پدافند غیرعامل
- فناوری اطلاعات و ارتباطات در دفاع شهری
- تهیه الگوی برآورد خطر زیر ساخت ها با استفاده از بستر GIS

مزایای شرکت در کنفرانس:

- نمایه سازی و انتشار مقالات در کتاب و لوح فشرده مجموعه مقالات کنگره، سیویلیکا، ISC
- تمامی مقالات برگزیده بدون نیاز به داوری مجدد و بصورت رایگان در ژورنال ها و مجلات معتبر داخلی و خارجی پشتیبان کنگره به چاپ خواهند رسید
- صدور گواهینامه های بین المللی کنگره از آکادمی Science Nodric
- شرکت در کنگره دارای نمره برای دانشجویان و امتیاز برای مهندسان می باشد.

برنامه های کنفرانس:

- سخنرانی های کلیدی
- جلسه پرسش و پاسخ در پنل های تخصصی
- ارائه مقالات و داوری در پنل های تخصصی
- کارگاه های آموزشی جنبی کنگره
- معرفی پژوهشگران برتر کنگره

حامیان کنفرانس:



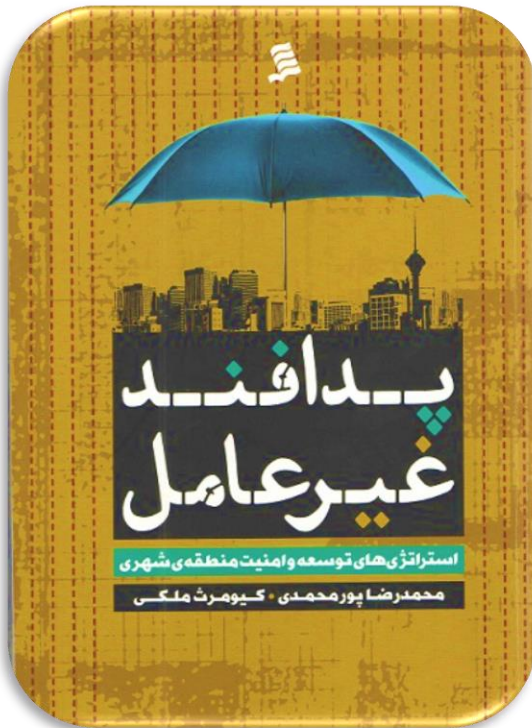
دیرخانه اصلی: تبریز، خیابان جمهوری اسلامی - استانداری آذربایجان شرقی - اداره کل پدافند غیر عامل
تلفن: ۳۳۳۴۴۶۴۶ - ۴۱

دیرخانه اجرایی: کلانشهر تبریز، ولیعصر جنوبی، خیابان سعدی، کوچه شهید ساجید، پلاک ۲/۸۲
پست الکترونیک: info@ncpd.ir تلفن: ۳۳۴۴۶۴۱۲ - ۴۱ فاکس: ۳۳۴۴۲۰۶۳ - ۴۱

<http://ncpd.ir/fa/>

معرفی کتاب

حوزه پدافند کالبدی



کتاب پدافند غیرعامل استراتژی های توسعه و امنیت منطقه شهری نوشته دکتر محمد رضا پورمحمدی و کیورث ملکی می باشد که در سال ۱۳۹۵ منتشر شده است. این کتاب حاصل برخورداری از منابع، آثار و تجارب ارزشمند دیگران و نیز تجارب، تلاش و مطالعه و کار پژوهشی و علمی نویسندگان است که با محوریت و نگرش کامل بر نقش پدافند غیرعامل و با تاکید بر استراتژی های توسعه و امنیت منطقه ی شهری مشتمل بر چهار فصل به ترتیب زیر تدوین و گردآوری شده است.

فصل اول : پدافند غیرعامل : کلیات

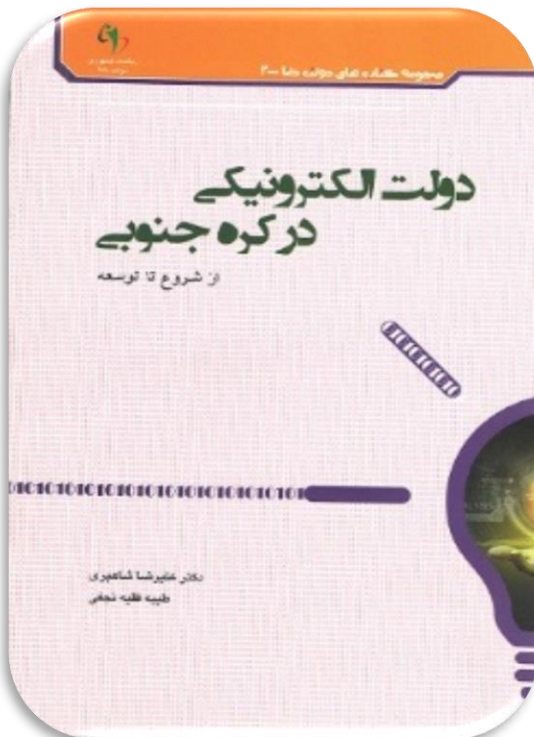
فصل دوم : برنامه ریزی پدافند و الزامات محیط شناسی در منطقه شهری

فصل سوم : راهبردهای اساسی در پدافند غیرعامل

فصل چهارم : سیر تاریخی پدافند غیرعامل و دفاع در شهر و منطقه

البته در ادامه هر یک از این فصل ها، با توجه به ساختار و چارچوب کتاب، واکاوی پدافند غیرعامل و دفاع و امنیت پایدار در حوزه منطقه شهری با توجه به پتانسیل سنجی بحران ها و تهدیدات پیش رو به ایراد مباحث و مطالبی از گذشته تا به امروز پرداخته شده است. در تالیف کتاب حاضر تلاش شده است که آخرین پژوهش ها و مسیرهای پدافند غیرعامل در حوزه منطقه شهری، به ویژه در چند سال اخیر، با استفاده از بیش از ۴۵۰ منبع معتبر علمی به کار گرفته شود و سعی شده است ضمن بررسی مطالب پدافند غیرعامل در حوزه های مرتبط تا حدودی نیز به روش کار نیز اشاره شود تا انطباق و همگرایی مباحث پدافند غیرعامل و استراتژی های توسعه و امنیت در حوزه ی منطقه شهری با هدف پایداری منطقه شهری به روشنی نشان داده شود.

حوزه پدافند سایبری



کتاب دولت الکترونیکی در کره جنوبی از شروع تا توسعه ترجمه دکتر علیرضا شاهپری و طیبه فقیه نجفی که در سال ۱۳۹۴ ترجمه شده است.

دولت الکترونیک، بکارگیری تکنیک ها و ابزارهای فناوری اطلاعات (مانند شبکه های گسترده، اینترنت و ...) برای ارائه خدمات دولتی کارا به شهروندان، کسب و کارها و دیگر سازمان های دولتی می باشد. دولت الکترونیک موجب تسهیل دسترسی شهروندان به خدمات و اطلاعات دولتی شده و باعث ارتقاء کارایی، اثربخشی، شفافیت، پاسخگویی و مشارکت بیشتر دولت می شود. کتاب حاضر مشتمل بر شش فصل به ترتیب زیر می باشد:

فصل اول: مفهوم دولت الکترونیک و وضعیت موجود آن در کره

فصل دوم : مرحله مقدماتی (۱۹۷۸ تا ۱۹۸۶)

فصل سوم : مرحله استقرار زیرساخت (از سال ۱۹۹۶-۱۹۸۷)

فصل چهارم : مرحله ارتقاء کامل (۲۰۰۲-۱۹۹۶)

فصل پنجم : مرحله پیشرفت (سال های ۲۰۰۳-۲۰۱۱)

فصل ششم : عوامل موفقیت دولت الکترونیک کره و دستاوردهای آن برای کشورهای در حال توسعه

در نهایت در فصل آخر وضعیت دولت الکترونیک در کره به طور مختصر ارزیابی و پیامدهای آن ارائه می شود. دلیل موفقیت دولت الکترونیک در کره، علیرغم وجود محدودیت های متعدد بیان می گردد و دستاوردهای دولت الکترونیک کره برای کشورهای در حال توسعه که در حال اجرای دولت الکترونیک هستند، یا برنامه این کار را دارند، مورد بحث قرار می گیرد.



بررسی فنی اپلیکیشن آپ

گوشی های هوشمند جزء جداناپذیر زندگی ما شده اند. روزانه هر فرد چندین ساعت به گوشی خود خیره می شود که این امر اهمیت پرداختن به برنامه های گوشی های هوشمند موسوم به "اپلیکیشن" را مهم جلوه می دهد. اپلیکیشن آپ، یک برنامه کاربردی مالی ایرانی است که با استفاده از بسترهای اینترنتی، تراکنش های مالی را برای کاربران انجام می دهد. در گذشته، عملیات بانکی از طریق مراجعه به بانک ها صورت می گرفت و صف های طولانی پرداخت قبض آب و برق و تلفن، وقت زیادی از مردم می گرفت و شغل های کاذبی چون "فروشنده نوبت" ایجاد می گردید. اما اکنون با داشتن رمز دوم کارت های بانکی به راحتی گستره وسیعی از امور بانکی با گوشی هوشمند انجام می گیرد.

اپلیکیشن مالی آپ متعلق به شرکت آسان پرداخت پرشین است که تا قبل از ورود به بورس از زیرمجموعه های بانک کشاورزی محسوب میشد. آپ توسط بانک های بزرگ کشور و نهادهای مالی معتبر پشتیبانی می شود. این اپلیکیشن یکی از موفق ترین اپلیکیشن های مالی ایرانی است که دارای جامعیت قابل قبول و امکانات بی نظیری می باشد که بسیاری از آنها در اپلیکیشن های مالی مشابه وجود نداشته و یا قدرت و کیفیت آن بسیار فراتر از سایر اپلیکیشن های مشابه در بازار است. اپلیکیشن مالی آپ جزو اولین اپلیکیشن ها بود که توانست مجوز کارت به کارت را از بانک مرکزی دریافت کند. اپلیکیشن آپ بر روی سیستم عامل های android و iOS قابل دریافت و اجرا می باشد و توسعه دهندگان این برنامه تا کنون با توجه به بروز رسانی های این سیستم عامل ها، اپلیکیشن خود را بروز نموده اند.

اکنون آخرین نسخه این اپلیکیشن قابل اجرا بر روی Android Oreo و iOS 12 می باشد.

یکی از اصلی ترین اصولی که معمولاً در مراحل ساخت اپلیکیشن ها در کشور ما نادیده گرفته می شود و معمولاً دلیل اصلی شکست و عدم استقبال این برنامه ها توسط کاربران می شود، عدم استفاده از پروتکل های امن ارسال و دریافت داده و عدم وجود رمزنگاری در تبادل داده می باشد. اپلیکیشن اندروید آپ بر روی رابط برنامه نویسی متن باز android طراحی گردیده و با توجه به توسعه برنامه بر روی یک نسخه کرنل لینوکس بهبود یافته، بایستی تمرکز اصلی برنامه نویسی این اپلیکیشن بر روی تامین امنیت آن باشد. قدرتمندترین و رایج ترین رابط برنامه نویسی اندروید، Android Studio می باشد. چیزی که مسلم است تا کنون این اپلیکیشن از نقطه نظر امنیت دچار مشکل نبوده و حتی یک مورد تراکنش غیرقانونی از این برنامه گزارش نشده است فلذا نشان می دهد این اپلیکیشن کاملاً منطبق بر پروتکل های امنیتی بانکی است و سرورها، پایگاه داده ها، API ها و راه حل های ذخیره سازی کاملاً بصورت امن پیش بینی شده اند. اپلیکیشن آپ حاوی امکانات و بخش های مختلفی همچون بیمه، خرید بلیت هواپیما، ثبت اسناد و املاک و ... می باشد اما یک ویژگی منحصر بفرد این اپلیکیشن، سرویس تله پرداز می باشد که می تواند رقیب پوزهای فیزیکی باشد. با استفاده از این سرویس می توان با مراجعه به هر فروشگاه که سرویس تله پرداز را فعال کرده باشد، بدون نیاز به کارت بانکی، هزینه خدمات و وسایل خریداری شده را پرداخت کرد. برای این کار کافی است کد QR مختص به فروشنده را با استفاده از اسکنر آپ اسکن نموده و سپس با نمایش اطلاعات فروشگاه، مبلغ را وارد کرده و هزینه را پرداخت.

بتن های خودترمیم شونده

مقدمه

امروزه بتن به عنوان یکی از مصالح اصلی در صنعت ساخت و ساز به شمار می آید. تمایل زیاد صنعت به استفاده از مصالح بتنی منجر به انجام تحقیقات زیادی در زمینه اصلاح معایب آن شده است. یکی از معایب اجتناب ناپذیر در بسیاری از سازه های بتنی، به وجود آمدن ترک های ریز ناشی از تنش های کششی و انقباض در این سازه هاست که علاوه بر تغییر شکل ظاهری بتن، باعث نفوذ آب و مواد شیمیایی به درون بتن شده که موجب خوردگی آرماتورها و افت مقاومت سازه می شود و هزینه های ناشی از نگهداری و تعمیر سازه ها را بسیار بالا می برد. بنابراین استفاده از یک مکانیزم خودکار جهت ترمیم ترک خوردگی های بتن می تواند باعث کاهش مشکلات به وجود آمده در این زمینه شود و عمر مفید سازه ها را افزایش دهد. تلاش های محققان در این زمینه سبب شد که مفهوم بتن خود ترمیم شونده، راه خود را به درون صنعت ساخت و ساز باز نماید. دو زمینه تحقیقاتی اصلی در مورد این نوع بتن وجود دارد؛ یکی راه طبیعی مبتنی بر هیدرات برای مهر و موم کردن ترک ها در طول زمان و دیگری راه مصنوعی جهت مهر و موم ترک هایی که به مداخله انسانی نیاز دارد. هدف اصلی این کار، افزایش دوام بتن است که تأثیر مثبت زیادی بر محیط زیست و اقتصاد خواهد داشت. از سوی دیگر، این امر می تواند طرح های معماری را با استفاده از روش های جدید طراحی متحول ساخته و طرح فضای داخلی را تغییر دهد؛ به طوری که این فضا برای انجام عملکردهای متنوع مناسب باشد و در عین حال انعطاف پذیری لازم را نیز ارائه کند.

مفهوم بتن خود ترمیم شونده:

مواد خود ترمیم شونده، موادی هستند که توانایی بازگشت به حالت اولیه را دارند. مفهوم بتن خود ترمیم شونده (SHC) که ترمیم آن به مرور زمان اتفاق می افتد (اتوژنیک)، نخستین بار در حدود دو دهه پیش مطرح شد و می توان آن را در بسیاری از سازه ها مشاهده کرد که به رغم عدم تعمیر و نگهداری قابل ملاحظه، برای مدت زمان طولانی پایدار و پابرجا مانده اند.



روش های خودترمیمی بتن:

در حالت کلی دو روش برای خودترمیمی بتن وجود دارد. اول روش طبیعی با استفاده از فعل و انفعالات سیمان و شرایط موثر طبیعی و دوم روش مصنوعی و انسان ساز با استفاده از عوامل چسبنده.



فازهای اصلی توانایی ترمیم طبیعی، آماس و هیدراتاسیون خمیر سیمان هستند که با ته نشین شدن کربنات کلسیم (CaCO_3) ادامه می یابند و در نهایت باعث انسداد مسیرهای جریان و رسوب ناخالصی های آبی و یا حرکت برخی ذرات بتنی جدا شده در طول فرآیند ترک خوردگی می شود. من جمله عوامل دخیل در روش طبیعی ترمیم می توان از دما، درجه آسیب، چرخه یخ زدگی، طول عمر بتن و وضعیت ملات نام برد.

اما روش مصنوعی ترمیم ترک در بتن، که یک فرایند خود ترمیمی با دخالت انسان است در سال ۱۹۹۴ اختراع شد نخستین و اصلی ترین روش مصنوعی ترمیم بتن، استفاده از یک عامل ترمیم کننده (چسبنده) بود که در داخل یک کپسول کوچک قرار می گرفت. در این روش، شکل گیری ترک باعث شکستن کپسول های میکرو و آزاد شدن عوامل ترمیم کننده ای می شد که بهبود و ترمیم ترک را برعهده داشتند. چسب ها می توانستند در رشته های کوتاه یا لوله های طولانی ذخیره شوند.

لکن محققان دانشگاه کاردیف، دانشگاه کمبریج، دانشگاه BATH و یک شرکت ساختمانی کره جنوبی، مکانیزم های بسیار موثرتری را کشف نمودند. بنابراین در ادامه مطلب به ذکر مزایا و معایب دو رویکرد متمایز و امیدوارکننده ای پرداخته می شود که به زودی در سراسر جهان به کار گرفته خواهند شد.

۱- فرایند خود ترمیمی مبتنی بر باکتری ها:

محققین در دانشگاه Delft هلند به سرپرستی پروفیسور Henk Jonkerz متخصص میکروبیولوژی با الهام از طبیعت و ترکیب علوم زیست شناسی و مهندسی عمران یک باکتری از سنگ آهک و لاکتیک کلسیم به صورت یک کپسول تولید کرده اند که در ترکیب با بتن، ماده جدید با خواص بهبود یافته با نام بتن بیولوژیکی یا همان بیوبتن به وجود می آورد. باکتری های به کار گرفته شده توسط این تیم «باسیلوس سودوفرموس» و یا «سپروسارکینا ساتروی» هستند که در شرایط قلیایی رشد پیدا می کنند و هنگامی که با بتن ترکیب گردند به صورت یکسان روی آن توزیع می گردند و می توانند تا ۲۰۰ سال به طور غیر فعال در جای خود باقی بمانند و تنها هنگامی که بتن ترک می خورد، هوا و رطوبت باکتری را تحریک کرده و شروع به استفاده از لاکتیک کلسیم به عنوان منبع غذایی می کنند و نتیجه این فرایند تولید سنگ آهک می باشد که در مدت زمان سه هفته منجر به آب بندی ترک می شود.

به گفته دکتر ریچارد کوپر از گروه زیست شناسی و بیوشیمی دانشگاه BATH، ترکیب باکتری ها در بتن باعث ایجاد لایه های محافظ می شود که از خوردگی فولاد جلوگیری می کنند.

محدودیت ها:

در حال حاضر، هزینه بالای این ماده، عامل بازدارنده استفاده کلان و همه گیر شدن آن است. زیرا که هزینه تولید آن دو برابر بتن معمولی است که این مسئله استفاده از این بتن را تنها برای پروژه هایی که نشست و خوردگی در آنها بسیار مشکل ساز هستند توجیه پذیر می کند. قیمت بالای لاکتیک کلسیم که یک ماده مغذی برای باکتری محسوب می شود، تاثیر بسزایی برای به وجود آمدن این ماده دارد. اما خوشبختانه محققین بر روی یک جایگزین که ماده اصلی آن را شکر تشکیل می دهد کار می کنند که انتظار می رود بتوان بیوبتن را تبدیل به یک ماده پایدار برای جلوگیری از رشد ترک های بوجود آمده در بتن کند.

۲- پلیمرهای هوشمند (حافظه دار):

مواد هوشمند جدیدی (SMP) که پس از اعمال محرک، توانایی بازگشت به حالت اولیه خود از طریق تغییر شکل را دارند، جزو این گونه از پلیمرها به شمار می روند. این مکانیزم از هر دو اصل اتوژنیک و اتونومیک استفاده می کند. این مواد از یک سیستم ساخت بشر برای افزایش خاصیت خود ترمیمی طبیعی خود بهره می برند و ترک های موجود در بتن را مهر و موم می نمایند. این نوع مواد متشکل از پلیمرهای نیمه بلورینی هستند که دارای ساختار از پیش تعریف شده حافظه داری در خود است و بازگشت پلیمرها به حالت اولیه آنها را منجر می شود.



پلیمرهای هوشمند که قابلیت فعال شدن از طریق گرمایش مستقیم و یا جریان الکتریکی را نیز دارند، به محض ایجاد ترک، فعال شده و فرآیند خود ترمیمی بتن را آغاز می‌کنند. شروع فعالیت پلیمرها، اثر حافظه یا همان انقباضی را به دنبال دارد که به سبب ماهیت محدود مواد، منجر به تولید یک نیروی کششی قوی می‌شود. این نیروی کششی قوی ترمیم خودکار بتن در کوتاه‌ترین زمان ممکن را به دنبال دارد و مانع فروپاشی آن می‌شود.

نتیجه‌گیری:

به طور کلی بتن خود ترمیم شونده بسیار کارآمدتر از بتن معمولی است و قطعاً به زودی طرز تفکر معماران و طراحی‌های آنها را نیز تحت تاثیر قرار خواهد داد. در مقایسه با بتن معمولی، ما متوجه شدیم که مزایای بتن خود ترمیم شونده بسیار بیشتر از معایب آن است و به دلیل میزان انتشار دی اکسید کربن کمتر، بتن را از ماده‌ای آسیب رسان به محیط زیست به ماده‌ای سازگار با محیط زیست تبدیل می‌کند. در حال حاضر بسیاری از مطالعات در حال انجام، از روش‌های مختلفی برای تولید بتن خود ترمیم شونده استفاده می‌کنند. با این حال، امیدوار کننده‌ترین رویکرد، با توجه به سادگی آن در مقایسه با مکانیزم‌های دیگر، بتن خود ترمیم شونده زیستی مبتنی بر باکتری است. در عین حال، معماران باید روش‌های طراحی جدیدی را نیز توسعه دهند؛ و روشهایی را ابداع نمایند که با داشتن پارتیشن‌های قابل جابجایی، انعطاف پذیری بیشتری را در تغییر عملکرد سازه ایجاد نماید.

منابع:

- ۱- سرلک، نرگس، ۱۳۹۶، بتن خودترمیم شونده، چهاردهمین اجلاس سراسری فناوری رسانه
- ۲- زارعیان، محمد سجاد، مرشد، رضا، ۱۳۹۰، بتن خودترمیم شونده، سومین کنفرانس ملی بتن ایران، انجمن بتن ایران
- ۳- بتن خودترمیم، روشگاه معماری دیسامگ (www.disamag.com)
- ۴- بتن خودترمیم شونده؛ از تعریف تا خواص مکانیکی، سامانه جامع صنعت ساختمان کارگشا (www.kargosha.com)

مقدمه ای بر هوش امنیتی

با افزایش حجم رخدادهای گزارش شده توسط سیستم ها و ابزارهای امنیتی، کشف و شناسایی تهدیدات و حملات داخلی و خارجی بسیار دشوار و در مواردی غیرممکن شده است. از این رو نیاز به روش متمرکزی وجود دارد تا بتوان رخدادهای داده های گزارش شده را مانیتور کرده و بین آنها ارتباط برقرار نمود و از این طریق تهدیدها و حملات را شناسایی کرد.

بسیاری از تحقیقات صورت گرفته بیانگر این است که از هر ده رخداد امنیتی، هفت رخداد هیچ وقت در سازمان ها گزارش نمی شوند و در ۳۰ درصد مواقع، حتی خود سازمان مورد حمله نیز متوجه بروز حمله نمی شود. همچنین یک سوم نشت اطلاعات حیاتی در سازمان ها، تا یک ماه بعد هم تشخیص داده نمی شوند و سه پنجم از رخدادهای امنیتی توسط شرکت های بیرونی تشخیص داده می شوند و نه خود سازمان قربانی و ۴۳ درصد از حملات سایبری بر روی دارایی های لیست نشده سازمان ها، رخ می دهند. با وجود این روند تصاعدی بروز تهدیدات جدید، محدودیت های فناوری در تحلیل سریع رخدادهای، انبوه داده های غیریکپارچه در سیستم های مختلف یک سازمان، تغییرات سریع قوانین محلی و جهانی، منابع امنیتی محدود در سازمان از جمله نیروی متخصص، هزینه و فناوری و عدم توجه به مستندسازی اطلاعات، شرکت ها و سازمان ها را به اتخاذ تصمیمات جدی در خصوص امنیت وادار می کند.

✓ آشنایی با هوش امنیتی

استفاده از سخت افزار، نرم افزار، اسکنر یا سیستم های مانیتورینگ، هیچ یک به معنی احساس امن بودن نیست. راه کار پیشنهادی محققین امنیت اطلاعات، هوش امنیتی است که در واقع یک راه کار مدرن امنیتی برای مقابله با تهدیدات امروزی می باشد. جمع آوری، نرمالسازی، همبسته سازی و تحلیل کلان داده های امنیتی یک سازمان به منظور خودکار کردن فرآیندهای کاهش سطح مخاطرات در سازمان یا به عبارت دیگر تبدیل میلیون ها بسته اطلاعاتی به یک اقدام عملی آنی، تعاریفی از هوش امنیتی هستند.

بر اساس تعریف پیتر گیل، هوش امنیتی عبارت است از جمع آوری اطلاعات و تلاش برای مقابله با تهدیدات درک شده در امنیت ناشی از جاسوسی، خرابکاری، فعالیت های خارجی و جمع آوری، نرمال سازی و تحلیل بهنگام داده های هوش امنیتی، یک دید جامع و اجرایی برای مدیریت ریسک ها و تهدیدات، حفاظت و تشخیص از طریق آموزش فراهم می کند.

به دو دلیل مهم Big Data و APT، سازمان ها ناگزیرند که به سمت هوش امنیتی حرکت کنند. کلان داده، به مجموعه هایی از داده با نرخ رشد بسیار بالا گفته می شود که در مدت زمان کوتاهی، باعث ایجاد چنان حجمی از اطلاعات می شوند که ذخیره سازی، جستجو و تحلیل آنها با ابزارهای مدیریت داده موجود در یک زمان قابل قبول و مورد انتظار، غیرممکن است. چهار مشخصه مهم کلان داده ها، حجم بالای داده، سرعت بالای ایجاد داده، تنوع بالای داده و سرعت بالای تغییر داده است. APT، نوعی از حملات ترکیبی و پیچیده سایبری است که هدفی خاص و دقیق دارد و از روش های مختلف برای پنهان ماندن از دید سامانه های پایش استفاده می کند.

✓ رابطه هوش امنیتی و هوش کسب و کار

هوش تجاری یا هوش کسب و کار به مجموعه ای از ابزارها، تکنولوژی ها، چارچوب ها، تکنیک ها و ... اطلاق می شود که بکارگیری آنها باعث افزایش هوشمندی در کسب و کار می شود. هوش کسب و کار به دنبال جمع آوری داده های مهم و تاثیرگذار هر کسب و کار و سپس تحلیل و ایجاد هوشمندی از آن هاست.

این هوشمندی در کسب و کار منجر به مزایای زیر برای سازمان می شود:

- کاهش ریسک در کسب و کار
- تسهیل تصمیم گیری های تجاری
- خودکار نمودن فرآیندهای تجاری

هوش امنیتی در واقع بکارگیری چارچوب هوش تجاری در کسب و کارهای امنیتی است. به این معنا که برای سازمان هایی که کسب و کارشان تامین امنیت یک سازمان است اگر از مفاهیم هوشمندی کسب و کار استفاده شود، می توانند به هوش مورد نظر در امور امنیتی دست یابند. بنابراین مزایای حاصل از بکارگیری هوش امنیتی بسیار مشابه هوش تجاری است با این تفاوت که مزایا مخصوص بحث امنیت است. در واقع مقایسه هوش تجاری با هوش امنیتی مانند مقایسه یک امر کلی با یکی از مصداق های آن است. مانند مقایسه سیستم اطلاعات حسابداری با سیستم های اطلاعاتی. در واقع سیستم حسابداری گونه ای از همان سیستم اطلاعاتی است و مقایسه آن ها از این نظر خالی از اشکال نیست.

مزایای بهره گیری از هوش امنیتی در سازمان عبارتند از:

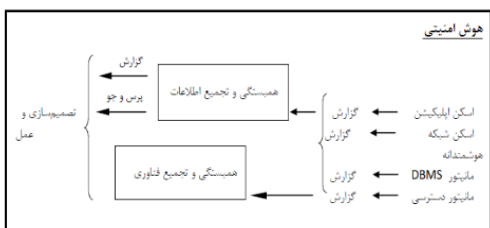
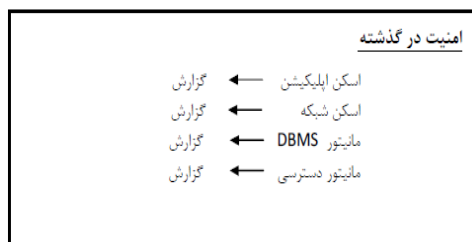
- کاهش تهدیدات
- کاهش سطح عدم انطباق
- تسهیل تصمیم گیری های امنیتی
- خودکار نمودن فرآیندهای امنیتی

مدل امنیتی ده سال پیش سازمان ها، در شرایط کنونی ابداً مؤثر نیست و این مدل در بهترین حالت خود جزایر امنیتی را ایجاد می کند و هرکدام از فاصله بین این اطلاعات استفاده می کنند. جهت برقراری امنیت در روش های سنتی مطابق شکل روبرو، از موارد مذکور گزارشی تهیه می شود.

اما در روش هوش امنیتی پس از تهیه این گزارشات، با استفاده از دو بخش مهم هوش امنیتی، بخش یکپارچگی اطلاعات و همبسته سازی و بخش برهم کنش تکنولوژی و همبسته سازی از گزارش حاصله، می توان تصمیم یا عمل هوشمندی را اتخاذ کرد.

مدیریت رویدادها و امنیت اطلاعات (SIEM)، مدیریت مخاطرات (Management Risk) و پذیرش مقررات (Regulatory Compliance)، سه جزء اصلی یک راه کار هوش امنیتی هستند.

SIEM، مهمترین جزء و متفاوت با Log Management است و ترکیبی از محصولات مدیریت رویدادهای امنیتی (SEM) و مدیریت اطلاعات امنیتی (SIM) می باشد. مدیریت رخداد نگاشت ها (log)، نرمال سازی، همبسته سازی رویدادها، عکس العمل آنی به تهدیدات، امنیت عناصر انتهایی، ذخیره سازی وقایع و ارائه گزارش به صورت Web-based و راه دور، نمونه های از سرویس های SIEM هستند. قسمت زیرساخت در یک راه کار هوش امنیتی توسط SIEM تأمین می شود، وظایف نرمال سازی و همبسته سازی توسط SIEM انجام می شود، در بسیاری از محصولات تجاری SIEM، امکان مدیریت Compliance هم وجود دارد، محصولات تجاری SIEM عمدتاً توسعه پذیر هستند و به دلایل مذکور SIEM، قلب یک راه کار هوش امنیتی است.



هدف مدیریت مخاطرات، کاهش زیان است که از طریق سه شاخص، شناسایی، ارزیابی و اولویت گذاری امکان پذیر است. بر مبنای ISO 27005، پنج قدم مهم در مدیریت مخاطرات وجود دارد که در ذیل آمده است:

- قدم اول: تشخیص و شناسایی تهدیدات
- قدم دوم: ارزیابی آسیب پذیری های هدف تهدیدات
- قدم سوم: تشخیص زیان های ناشی از عملی شدن تهدیدات
- قدم چهارم: تعیین راه کارهای کاهش مخاطرات
- قدم پنجم: اولویت گذاری راه کارها

خروجی های یک راهکار هوش امنیتی

Data silo consolidation: بدون تکنولوژی هوش تجاری، تحلیل کلان داده های تجاری برای تعیین مسیر حرکت یک کسب و کار عملاً ناممکن است. چنین تشبیهی در مورد هوش امنیتی نیز صادق است. بدون هوش امنیتی، دریافت log تجهیزات حتی در صورتی که به طور کامل نیز انجام گردد، باعث ایجاد یک سیلوی جدید می شود. در یک سازمان بزرگ این داده ها به اندازه های زتابایت، یوتابایت و هلابایت هم می رسد. هوش امنیتی به وسیله اضافه کردن Context باعث کاهش حجم اطلاعات امنیتی می شود.

Threat Management: از زمان ظهور اینترنت، مدل تهدیدات امنیتی از یک مدل متمرکز به یک مدل توزیع شده تغییر ماهیت داده است. امنیت دیگر تنها موضوع نصب فایروال نیست. امروزه تمرکز بر روی امنیت لایه های بالاتر مدل OSI بوده و محتوا اهمیت یافته است و حملات APT مطرح شده اند. فعالیتی که برای یک بخش از زیرساخت بی ضرر تشخیص داده می شود، پس از همبسته سازی با سایر منابع اطلاعاتی ممکن است برای بخش دیگری از زیرساخت مهلك تشخیص داده شود. وظیفه هوش امنیتی تشخیص این نوع حملات است.

Fraud Discovery: تشخیص تقلب بدون استفاده از هوش امنیتی عملاً غیرممکن است. تشخیص تقلب نیازمند جمع آوری Log کلیه امان های مسیر حرکت یک بسته اطلاعات یا تراکنش بانکی است که مجدداً با مشکل Big Data روبرو می شود.

Regulatory Compliance: مهمترین خروجی هوش امنیتی است که اهمیت certified بودن برای کسب و کار یک سازمان را دربردارد. در واقع یک بازرس خودکار و real-time است. به جز حوزه های مربوط به منابع انسانی، سایر حوزه های یک استاندارد را پوشش می دهد و قابلیت تنظیم برای استانداردهای بومی، محلی و کشوری را دارد.

چالشهای پیاده سازی هوش امنیتی

فناوری هوش امنیتی مانند سایر فناوری ها با چالش هایی روبروست که نمونه هایی از آنها در جهان و ایران قابل ذکر است. عدم پشتیبانی مدیریت ارشد، بودجه، کمبود نیروی انسانی متخصص، عدم درک درست از هوش امنیتی، پیچیدگی پیاده سازی و عدم توجه کافی به مدیریت ریسک نمونه های از چالش های پیاده سازی در جهان بوده و فرهنگ سازمانی نامناسب، عدم پشتیبانی مستقیم شرکت های فروشنده محصول در ایران و عدم هماهنگی بین سازمان های مختلف در مدیریت امنیتی نمونه هایی از چالش های پیاده سازی در ایران هستند.

منابع:

1. <http://qlikiran.com>
2. <http://www.itpro.co.uk/security/20642/it-executive-guide-security-intelligence>

اقدامات ایمنی و آمادگی در برابر حوادث هسته ای

مشخصات کلی انفجارهای هسته ای:

واکنش انفجارهای هسته ای به بخش های ذیل دسته بندی می شود:

۱- اثر موج انفجاری

۲- اثر تشعشع حرارتی

۳- اثر تشعشع هسته ای

امواج هسته ای آهسته تر از پرتوهای گرمایی حرکت می کنند پس از آنکه شما نور و گرمای انفجار را حس کنید چند ثانیه طول می کشد تا امواج هسته ای حاصل از انفجار به شما برسد که این اختلاف زمانی مابین دیدن رعدبرق و شنیدن صدای آن است.

در نزدیکی محل انفجار سرعت امواج ۱,۵ کیلومتر در ثانیه (معادل ۵۴۰۰ کیلومتر در ساعت) است قسمت زیادی از انفجار به صورت حرارت و نور آزاد می شود و در فواصل بسیار دورتر نیز سبب سوختگی پوست بدن موجودات زنده می گردد. همچنین مقدار زیادی تشعشعات هسته ای تولید می شود که سبب بروز آثار بیولوژیکی، جهش ژنتیکی و ... می شود. در انفجارهای هسته ای درجه حرارت به حدود ده ها میلیون درجه سانتیگراد می رسد.

انرژی حاصل از یک انفجار هسته ای به بخش های زیر مربوط می شود:

- ۱- حدود ۵۰٪ انرژی به صورت موج انفجاری یا موج مکانیکی اثرات مخربی بر روی تاسیسات و ساختمان ها می گذارد.
- ۲- ۳۵٪ انرژی به صورت تشعشع حرارتی ظاهر می شود که بسته به نوع حادثه تا شعاع ۱۰ کیلومتری و یا بیشتر، انفجارهای هسته ای، حرارت جهنمی دارند به طوریکه همه چیز دراین محیط ذوب می شود.
- ۳- ۱۵٪ اثر تشعشع، هسته ای است که به صورت ذره آلفا، ذره بتا، اشعه گاما و نوترون در محیط پخش می شود و به علت بالا بودن نیمه عمر ذرات، آنها مدت های طولانی در محیط اکوسیستم باقی می مانند.

نکات مهم در مورد انفجارهای هسته ای:

مناطق انفجارهای هسته ای به پنج قسمت دسته بندی می شود:

- ۱- منطقه تبخیرحرارتی
 - ۲- منطقه آسیب شدید انفجاری
 - ۳- منطقه تخریب کلی
 - ۴- منطقه آسیب شدید باد و آتش
 - ۵- منطقه آسیب شدید گرمایی
- * منطقه تبخیر حرارتی درجه حرارتی معادل ۳۰۰ میلیون درجه سانتیگراد را داراست که به سبب آن هر موجود زنده و یا حتی فلز که در این درجه حرارت قرار می گیرد آتش نمی گیرد بلکه بخار می شود.
- * اثرات زیانبار تشعشعات هسته ای تا شعاع ۱۱۰ کیلومتری نیز دیده می شود و موج انفجار آن می تواند تمامی دستگاههای الکترونیکی و مخابراتی را از کار بیاندازد.
- * پس از انفجار، تا سالهای طولانی (بسته به نیمه عمرمواد رادیواکتیو) تشعشعات زیانبار رادیواکتیویته مانع ادامه حیات موجودات زنده می شود.
- * رادیواکتیو از ۳ پرتو آلفا، بتا، گاما تشکیل یافته که نوع گامای آن با توجه به جرم انرژی و فرکانس بالا، خطرناک تر از بقیه می باشد که اگر به بدن انسان برخورد کند از ساختار سلولی بدن عبور کرده و در مسیر حرکت خود، باعث تخریب ریبونوکلوئیک اسید یا همان DNA می شود و سرانجام زمینه را برای پیدایش انواع سرطان، جهش ژنتیکی، سندروم و نقایص دیگر فراهم می آورد.

کاهش خطرات هسته ای با بکارگیری الزامات پدافند هسته ای:

واژه پد به معنای دفاع و واژه آفند نیز به مفهوم جنگ می باشد بنابراین پدافند هسته ای به معنای دفاع در مقابل حمله هسته ای می باشد، به طوریکه در مبحث ۲۱ مقررات ملی ساختمان (پدافند غیرعامل) هر اقدام غیر نظامی که موجب کاهش آسیب پذیری نیروی انسانی، ساختمان ها، تاسیسات، تجهیزات و شریانهای اصلی کشور و ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات شود را پدافند غیرعامل می نامند.

پدافند غیر عامل انسانی حفاظت پرسنل و افراد:

حفاظت در برابر پیامدهای غیر مترقبه مواد پرتوزا، بر مفهوم موانع حایل بین منبع پرتوزا و محیط تحت حفاظت، متکی است. در واقع چون اطمینان کافی وجود ندارد که شخص حفاظت شده در معرض ضربه غافلگیرانه قرار نگیرد در نتیجه توره های گیرانداز نیز اضافه می شوند. بر همین اساس شرکتهای سازنده لباس در برابر پرتوهای هسته ای (شرکت آلمانی PSD تاسیس شده در شهر مونیخ لباس های مردانه و زنانه خاص محافظ در برابر پرتوها را تولید می کند) که به قرار زیر می باشند:

لباس های محافظ در برابر پرتوهای هسته ای:

چلیقه محافظ در برابر پرتو که از دو طرف دارای سرب به شعاع ۱،۴ سانتیمتری می باشد که کاملاً انسان را از جلو و عقب محافظت می کند.



پا و کفش جانبی در برابر پرتوهای اشعه ایکس و گاما



محافظ گردن انسان و محافظ برای غده بسیار حساس تروئید میباشد که همه جاتیه از سرب پوشیده شده که در برابر اشعه های مستقیم محافظ است.



این مدل عینک از مواد ناتویی سرب و آلومینیوم و قلع که کاملاً محافظ در برابر اشعه های گاما و نوترونهای پر انرژی می باشند که قاب بندی این عینک ها طوری است که کاملاً چشم انسان را از هر طرف در مقابل تشعشعات حفظ می نماید.



این دستکش از الیاف مواد شامل: ۲۵٪ نایلون کولار و ۵۰٪ مواد ناتو سرب و ۲۵٪ موادعایق سلولزی ساخته شده است که کاملاً مقاوم در برابر اشعه های گاما،... میباشد.



پدافند غیرعامل زیست محیطی هسته ای :

از جمله روشهای پدافند زیست محیطی هسته ای روش Hytrometiation می باشد. این روش، روشی موثر برای حذف آلودگی از خاک، آب زیرزمینی و آب سطحی است که اکنون هم در کشورهای پیشرفته انجام می گیرد. روش دیگر کنترل آلودگی آب های سطحی در حوادث هسته ای، استفاده از روش Dilution است که در این روش رقیق سازی بوسیله آب انجام می گیرد. از دیگر روش ها می توان به افزودن آهک به دریاچه ها، افزودن پتاسیم به دریاچه ها و سدها و منابع آبی، استفاده از ماده ژئولیت برای جذب و حذف سزیم، جلوگیری از ورود روان آب های آلوده به منابع زیرزمینی و.... اشاره نمود.

روش تصفیه و کنترل و مهار آلودگی در بستر خاک عبارتند از:

- ۱- برداشت خاک سطحی از مزارع و دفن آن
- ۲- شخم زدن عمیق خاک: که در اثر این عمل خاک رویی به عمق پایین تر منتقل شده و از دسترسی گیاهان دور می شود.
- ۳- پاک سازی جاده و معابر: با استفاده از روش Wet Vaccaming و Pressure Water (شستشو با استفاده از دترجنتها و آب با فشار قوی)
- ۴- قطع درختان آلوده و نابود کردن گیاهان کم ارتفاع

پدافند هسته ای در معماری:

معماری و شهرسازی به عنوان یک واسطه ، قدرت دفاعی را افزایش می دهد.

- ۱- فرم ساختمانها بر میزان خسارات کلی ساختمانها تاثیر بسزایی دارد زاویه های تند و المانهای پیرامونی می تواند موج شوک هسته ای را به دام بیناندازد و اثر انفجار را تشدید کند. ساختمانهای با شکل U یا L اثر انفجار را تشدید می کنند. به منظور تخلیه انرژی انفجار از فضای مابین ساختمان ها و کاهش آسیب پذیری محیط، باید در فواصل ۲۰ متری انقطاع و ناپیوستگی ایجاد گردد. عرض درز انفصال بین دو دیوار بلوک ساختمان های هم ردیف نباید کمتر از ۵۰ سانتیمتر باشد.
 - ۲- فضاهای سیرکولاسیون: اگر موج انفجار در داخل فضاها، کریدورها و مانند آن منتشر شود به دلیل افزایش جبهه فشار موجی در چنین محیطی، بسیار مخرب خواهد بود. قرار دادن موانع یا پیچ ها در طول این گونه مسیرها باعث کاهش اثر نامطلوب نیروی انفجار می شود.
- تصاویر زیر به عنوان پناهگاه جامع هسته ای در کشور های مختلف است:



مترو مسکو که قابلیت تبدیل شدن به پناهگاه را دارد. پناهگاه مترو کره شمالی در شهر پیونگ یانگ که در عمق ۹۰ متری شهر واقع است.

مراجع:

1. The safe management of sources of radiation Principles and strategies. 158.28.14. INSAG-11, 2013
2. Defence in depth in nuclear safety. 158.20.14. INSAG-07, 2014
3. Radionuclide source terms from severe accidents to nuclear power plants with light water reactors. 212.20.14. INSAG-21, 2015
4. Basic safety principles for nuclear power plants. 105.12.14. INSAG-08, 2015
5. INTERNATIONAL ATOMIC ENERGY AGENCY, Decommissioning of Facilities Using Radioactive Material, IAEA Safety Standards Series No. WS-R-5, IAEA, Vienna (2010).
6. 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).

بات نت

بات‌نت‌ها شبکه‌هایی هستند که با در اختیار گرفتن مجموعه‌ای از کامپیوترها که بات (bot) نامیده می‌شوند، تشکیل می‌شوند. این شبکه‌ها توسط یک یا چند مهاجم که botmasters نامیده می‌شوند، با هدف انجام فعالیت‌های مخرب کنترل می‌گردند. به عبارت بهتر ربات‌ها کدهای مخربی هستند که بر روی کامپیوترهای میزبان اجرا می‌شوند تا امکان کنترل نمودن آن‌ها از راه دور را برای botmaster فراهم نمایند و آن‌ها بتوانند این مجموعه را وادار به انجام فعالیت‌های مختلف نمایند.

اجزای یک بات نت

Bot

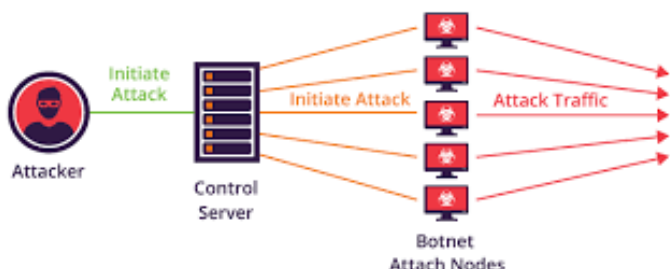
یک برنامه نرم‌افزاری (بدافزار) است که بر روی یک میزبان آسیب پذیر نصب می‌شود. این نرم‌افزار می‌تواند به روش‌های مختلف بر روی کامپیوتر میزبان نصب شود که از جمله آن‌ها می‌توان به مشاهده یک وب سایت آلوده اشاره نمود. ربات‌ها اغلب به نحوی پیکر بندی می‌شوند که هر بار که کامپیوتر قربانی روشن شود، ربات نیز فعال گردد.

Command and Control Infrastructure(C&C)

اقداماتی که ربات‌ها انجام می‌دهند بر اساس فرمان‌هایی هستند که توسط botmaster و از طریق یک کانال کنترلی ارسال می‌شوند. ربات‌ها آسیب پذیری‌های سیستم‌های عامل و یا برنامه‌های کاربردی نیستند؛ بلکه برنامه‌هایی هستند که برای نصب کردن backdoor هایی بر روی ماشین قربانی مورد استفاده قرار می‌گیرند. چیزی که ربات‌ها را از سایر بدافزارها متمایز می‌کند، کانال فرمان و کنترل است.

Botnet

یک بات‌نت، مجموعه‌ای از ربات‌هاست که به یک کانال کنترل و فرمان متصل شده‌اند. به عبارت بهتر شبکه‌ای از ربات‌ها که منتظر دریافت دستوری برای انجام فعالیت‌های مخرب هستند.



Botmaster or Botherder

کاربران مخربی هستند که با ارسال فرمان‌هایی برای انجام فعالیت‌های مخرب، ربات‌ها را کنترل می‌کنند. این کاربران اهداف مختلفی را دنبال می‌کنند.

Vulnerable Hosts

بات‌نت‌ها ماشین‌هایی در اینترنت هستند که توسط نرم‌افزار مخربی که توسط botmaster منتشر شده است، آلوده گردیده‌اند. این ماشین‌ها بعد از آلوده شدن تبدیل به "Slaves" می‌شوند و می‌توانند اهداف مخرب مختلفی را دنبال کنند. مهم‌ترین جزء یک بات‌نت زیربنای C&C است که شامل ربات‌ها و یک واحد کنترل است که می‌تواند به صورت متمرکز و یا غیر متمرکز باشد. Botmaster ها از پروتکل‌های ارتباطی مختلفی برای برقراری ارتباط با slave ها و ارسال دستورات به آن‌ها استفاده می‌کنند. با توجه به این که کانال C&C عموماً به عنوان تنها راه کنترل ربات‌ها محسوب می‌شود و کارایی بات‌نت وابسته به ارتباط پایدار با این کانال می‌باشد، معماری آن می‌تواند تعیین کننده میزان مقاومت (robustness)، پایداری (stability) و زمان واکنش (reaction time) آن باشد. در حالت کلی ربات‌ها به دو دسته متمرکز و غیر متمرکز تقسیم می‌شوند.

گزارش مرکز ماهر در مورد یکی از جدیدترین بات نت ها

شواهد نشان می‌دهد که از ابتدای سال جاری میلادی بات نتی با نام Hide 'N Seek با هدف آلوده‌سازی دستگاه‌های اینترنت اشیاء شایع شده است. این بات نت که برای انتشار خود رفتاری کرم‌گونه دارد، از آسیب‌پذیری CVE-2016-10401 و چندین آسیب‌پذیری دیگر برای انتشار کد بدخواه خود سوءاستفاده می‌کند.

این بات نت پس از Hajime دومین بات نت است که برای ارتباطات خود از شیوه p2p استفاده می‌کند. مقابله با بات‌نت‌هایی که از p2p برای ارتباطات خود استفاده می‌کنند دشوار است و به همین دلیل HNS در ماه‌های اخیر به طور مداوم در حال به‌روز رسانی بوده است. برخی از تغییراتی که در این به‌روز رسانی‌ها مشاهده شده است عبارتند از:

۱- افزودن اکسپلویت‌هایی برای دستگاه‌های وب‌کم AVTECH، روترهای Linksys سیسکو، وب سرور JAWS/1.0 و پایگاه داده‌های Apache CouchDB و OrientDB.

۲- آدرس گره‌های p2p هاردکد شده به ۱۷۱ مورد افزایش یافته است.

۳- افزودن برنامه cpuminer برای کاوش پول دیجیتال

با پشتیبانی از سرورهای پایگاه داده‌ای OrientDB، CouchDB و HNS بات‌نتی نه تنها برای اینترنت اشیاء بلکه بات‌نتی چندسکوپی به شمار می‌رود.

این بات نت برای انتشار در شبکه، با استفاده از کدی مشابه آنچه در بات نت mirai استفاده شده پورت‌های TCP شامل 80 (HTTP Web Service)، 8080 (HTTP Web Service)، 2480 (OrientDB)، 5984 (CouchDB) و 23 (Telnet) را در شبکه اسکن می‌کند و سپس با سوءاستفاده از اکسپلویت‌های زیر خود را بر روی پورت‌های مذکور مستقر می‌کند:

TPLink-Routers RCE

Netgear RCE

new: AVTECH RCE

new: CISCO Linksys Router RCE

new: JAW/1.0 RCE

new: OrientDB RCE

new: CouchDB RCE

هر گره HNS با سایر همتهای p2p خود با استفاده از سه روش زیر ارتباط برقرار می‌کند:

۱- ۱۷۱ آدرس هارد کد شده در برنامه

۲- آرگومان خط فرمان

۳- سایر همتهای p2p

برای مقابله و جلوگیری از آلودگی به این بات نت، به روز رسانی سریع دستگاه‌های اینترنت اشیاء و بستن پورت‌های غیر مود نیاز، تغییر پورت‌های پیش فرض و نیز تغییر رمزعبورهای پیش فرض ضروری به نظر می‌رسد.

مرجع:

1. <http://www.ddos-guard.ir/%D8%A8%D8%A7%D8%AA-%D9%86%D8%AA-botnet>

%DA%86%DB%8C%D8%B3%D8%AA%D8%9F/

2. <https://fa.wikipedia.org/wiki/%D8%A8%D8%A7%D8%AA%E2%80%8C%D9%86%D8%AA>

3 - <https://www.certcc.ir/news/12448>



به اطلاع می رساند که سازمان پدافند غیرعامل کشور (مرکز مطالعات پدافند غیرعامل کشور و مرکز مطالعات فنی و مهندسی پایداری ملی کشور) برای دانش آموختگان و فارغ التحصیلان مقاطع کارشناسی ارشد و دکتری طرح هایی برای کسر خدمت سربازی و خبگی (جایگزین خدمت سربازی) در نظر گرفته است. علاقمندان می توانند علاوه بر مراجعه به وب سایت های مربوطه با مراجعه به اداره کل پدافند غیرعامل استانداری آذربایجان شرقی از روند ثبت نام مطلع شوند.

<http://mafpa.ir/>
<http://www.pdrc.ir>

❖ وب سایت مرکز مطالعات فنی و مهندسی پایداری ملی کشور
❖ وب سایت مرکز مطالعات پدافند غیرعامل کشور :

عناوین رویدادهای مهم خبری

«برای مشاهده متن کامل خبرها روی آنها کلیک کنید»

[اولین جلسه کارگروه راه و شهرسازی پدافند غیرعامل استان آذربایجان شرقی برگزار شد](#)

[اولین نشست کارگروه تخصصی امداد و نجات پدافند غیرعامل استان آذربایجان شرقی برگزار شد](#)

[اولین نشست کارگروه تخصصی فرهنگی اجتماعی و آموزشی استان آذربایجان شرقی در سال ۹۷ برگزار شد](#)

[قطعی برق فرصتی برای شناسایی ضعف ها توسط پدافند غیرعامل](#)

[اولین نشست کارگروه پشتیبانی و خدمات شهری پدافند غیرعامل استان آذربایجان شرقی برگزار شد](#)

[اولین جلسه کارگروه انرژی و آب پدافند غیرعامل استان آذربایجان شرقی](#)

[عمده کار و فعالیت پدافند غیر عامل در زمان صلح باید انجام شود](#)

[تمهیدات ویژه مجلس برای مهار بازار احاره بهای مسکن](#)

[دوروی سکه تراخیخت ها؛ فقرزدایی با حنگ زیستی؟](#)

سایت های مرتبط با پدافند غیرعامل

<http://www.paydarymelli.ir>

وب سایت پایداری ملی

<http://www.pdrc.ir>

مرکز مطالعات پدافند غیرعامل

<http://ostan-as.gov.ir/?PageID=42>

استانداری آذربایجان شرقی - پدافند غیرعامل

<http://www.cyberpolice.ir/>

پلیس فتا

<http://mafpa.ir/>

مرکز مطالعات فنی و مهندسی پایداری ملی

<http://www.ncpd.ir/fa/?id=1&p=0>

سایت اولین کنفرانس ملی پدافند کالبدی