جمهوری اسلامی ایران
وزارت کشور
استانداری آذربایجان شرقی

سال ۱۳۹۸
سال رونق تولید

سازمان پدافند غیرعامل کشور

ماهنامه اداره کل پدافند غیر عامل

شماره ۳۳، خرداد ماه ۱۳۹۸

استاندار آذربایجان شرقی:
عدم آمادگی جهت مقابله با چالش‌ها و صیانت از زیرساخت‌ها مشهود است

معاون سیاسی، امنیتی و اجتماعی استانداری آذربایجان شرقی:
مخاطرات ناشی از انواع مواد خطرزا باید بررسی و در این زمینه آسیب‌شناسی شود

سرپرست اداره کل پدافند غیرعامل استان آذربایجان شرقی:
سیاست کلی پدافند غیرعامل در استان، استفاده از ظرفیت های علمی و پژوهشی مراکز دانشگاهی و تحقیقاتی است

در این شماره می‌خوانید:


امروز اهمیت پدافند غیر عامل
قاعدتاً برای مسئولین بایستی
شناخته شده باشد اهتمام شما
کار را پیش می‌برد.
مقام معظم رهبری، فرماندهی کل قوا
حضرت امام خامنه‌ای

جمهوری اسلامی ایران
وزارت کشور
استانداری آذربایجان شرقی

رونق تولید ۱۳۹۸

سازمان پدافند غیرعامل کشور

ماهنامه اداره کل پدافند غیر عامل – شماره ۳۳

مدیر مسئول:

محمد باقر آقایی

سردبیر:

لیدا رسول اهری

نشانی:

تبریز، میدان شهدا، استانداری آذربایجان شرقی، اداره کل پدافند غیرعامل

تلفن: ۰۴۱-۳۵۲۹۱۳۱۸

دورنگار: ۰۴۱-۳۵۲۹۱۳۵۹

فهرست مطالب:

استادان، پژوهشگران و دانشجویان علاقمند، می‌توانند مقاله‌های آموزشی، پژوهشی و ترویجی خود را برای درج در نشریه پدافند غیر عامل به نشانی زیر ارسال کنند.

passivedefense@ostan-as.gov.ir

مراسم تجلیل از برترین‌های مربیان و اساتید نیروهای مسلح انجام شد

تجلیل از دکتر جلالی رئیس سازمان پدافند غیرعامل به عنوان پژوهشگر و استاد نمونه دانشگاه دفاع ملی

در مراسم تجلیل از برترین‌های مربیان و اساتید نیروهای مسلح از سردار جلالی رئیس سازمان پدافند غیرعامل کشور به عنوان پژوهشگر و استاد نمونه دانشگاه عالی دفاع ملی تجلیل به عمل آمد.

این مراسم با حضور سردار سرلشکر پاسدار «محمد باقری» رئیس ستاد کل نیروهای مسلح، امیر سرتیپ «محمد حسن باقری» معاون آموزش و پژوهش ستاد کل نیروهای مسلح، سردار دریادار «علی فدوی» جانشین فرمانده کل سپاه، امیر دریادار «حبیب‌الله سیاری» معاون هماهنگ‌کننده آجا، امیر سرتیپ «محمود شیخ حسنی» معاون هماهنگ‌کننده وزارت دفاع و سردار سرتیپ «محمد علی نوری نژاد» معاون هماهنگ‌کننده ناجا در دانشگاه افسری و تربیت پاسداری امام حسین (ع) برگزار شد. در این مراسم، امیر سرتیپ باقری با اشاره به اینکه امسال برترین‌های آموزش در نیروهای مسلح مورد تجلیل قرار می‌گیرند، اظهار داشت: امروز تعدادی از این افراد شامل برترین‌های دانشگاه‌های آموزش سربازان وظیفه، علوم و فنون، اساتید دانشگاه‌ها، فرماندهان، پیشکسوتان و خانواده‌های معظم شهدا تجلیل شدند.

بنا بر این گزارش در این مراسم از سردار جلالی رئیس سازمان پدافند غیرعامل کشور به عنوان پژوهشگر و استاد نمونه دانشگاه عالی دفاع ملی و خانواده‌های شهیدان محمود خضرایی از نیروی هوایی ارتش، محمد طباطبایی از نیروی زمینی سپاه، رحیم شاهسوند از وزارت دفاع و خدابخش رئیسیان از ناجا، تجلیل به عمل آمد.

استاندار آذربایجان شرقی:

عدم آمادگی جهت مقابله با چالش ها و صیانت از زیرساخت ها مشهود است

اولین جلسه شورای پدافند غیرعامل استان در سال جاری به ریاست دکتر پورمحمدی، استاندار آذربایجان شرقی برگزار شد. در این جلسه استاندار آذربایجان شرقی با ابراز تأسف نسبت به حوادث اخیر سیل کشور و آتش سوزی بازار تبریز افزودند: بایستی از هر حادثه تلخی درس گرفته و با اقدامات مقتضی از بروز حوادث مشابه پیشگیری و یا در حد ممکن خسارات وارده را به حداقل برسانیم. پدافند غیرعامل تکمیل کننده پدافند عامل و مربوط به اقدامات پیشگیرانه و یک گام قبل از بحران‌ها و حوادث بوده که بایستی به صورت جدی مورد توجه قرار گیرد و نباید منتظر وقوع بحران‌ها باشیم تا نسبت به مدیریت و کنترل آن‌ها اقدام کنیم. متأسفانه در بازسازی‌های انجام شده بعد از حوادث قبلی، ملاحظات ایمنی در سیستم تأسیسات زیربنایی و سیم‌کشی برق رعایت نشده و این بار نبایستی اشتباهات گذشته تکرار شود و با رعایت الزامات پدافند غیرعامل و اصول ایمنی نسبت به تجهیز بازار به سیستم‌های اطفاء و اعلان حریق هوشمند و مانیتورینگ یکپارچه بازار اقدام شود. مأموریت اصلی پدافند غیرعامل، مصون‌سازی و کاهش خسارات ناشی از تهدیدات غیرطبیعی و تهاجمات دشمن است، در این راستا تمام دستگاه‌های اجرایی استان بایستی با شناسایی دارایی‌های با اهمیت خود و با توجه به درجه اهمیت آن‌ها نسبت به اجرای طرح‌های ایمن سازی و مصون سازی اقدام نمایند. ایشان با تشبیه کارگاه‌های موجود در خیابان جمهوری تبریز به پلاسکوی افقی، یادآور شدند با توجه به این‌که اکثر این کارگاه‌ها واحدهای تولید کفش بوده و در اکثر آن‌ها مواد آتش‌زا مانند چسب انبار می‌شود، بایستی نسبت به انتقال تدریجی آن‌ها از مرکز شهر اقدام شود. رئیس شورای پدافند غیرعامل استان با خطاب قرار دادن روسای کارگروه‌های تخصصی خواستار اقدامات عملیاتی آن‌ها در حوزه پدافند غیرعامل شده و در خصوص ساماندهی مناطق حاشیه نشین شهر، شناسایی و مقاوم سازی مسکن‌های کم‌دوام و ایمن‌سازی جاده‌های استان برای کاهش صدمات جاده‌ای تأکید کردند. ایشان پدافند غیرعامل را یک امر اولویت‌دار برشمرده و از تمام مدیران دستگاه‌ها خواستند تا اجرای طرح‌های پدافند غیرعامل در صدر هزینه کرد دستگاه‌ها قرار گیرد. دکتر پورمحمدی در پایان به ضرورت جداسازی اینترنت از شبکه داخلی سازمان‌ها و تجهیز و آماده بکار نمودن مولدهای برق اضطراری دستگاه‌های اجرایی استان تأکید کردند. در این جلسه آقایی سرپرست اداره کل پدافند غیرعامل استان ضمن آرزوی قبولی طاعات و عبادات در ماه مبارک رمضان، به ارائه گزارش عملکرد و اقدامات اداره کل در سال ۹۷ پرداختند.

جلسه کارگروه فرهنگی، آموزشی و اجتماعی پدافند غیرعامل استان

اولین جلسه کارگروه فرهنگی، آموزشی و اجتماعی پدافند غیرعامل استان در سال ۱۳۹۸ با محوریت بررسی آسیب‌ها و تهدیدات در حوزه فرهنگی و اجتماعی به میزبانی اداره کل آموزش و پرورش استان با حضور آقایی سرپرست اداره کل پدافند غیرعامل در محل سالن جلسات این اداره تشکیل شد. در ابتدای جلسه، وحدتی رئیس حراست اداره کل آموزش و پرورش استان در خصوص برنامه‌های اجرایی این کارگروه برای سال ۹۸ – تمهیدات فرهنگی و اجتماعی – مطالبی را بیان نمودند. در ادامه سرپرست اداره کل پدافند غیرعامل با تشریح کلی تهدیدات و آسیب‌پذیری‌های حوزه فرهنگی اجتماعی، در خصوص انتظارات از این کارگروه در زمینه آگاهی بخشی و اطلاع‌رسانی آحاد جامعه و بالاخص لزوم تشکیل قرارگاه پدافند فرهنگی مطالبی بیان کردند. ایشان بر ضرورت همکاری و هماهنگی تمامی اعضا به خصوص صدا و سیما، شهرداری و آموزش و پرورش با پدافند غیرعامل در زمینه اطلاع‌رسانی و فرهنگ‌سازی، تولید محتوا و برگزاری دوره‌های آموزشی تأکید کردند. در این جلسه محمد زاده رئیس دفتر سازمان سراج استان و رئیس اتحادیه انجمن‌های اسلامی دانش‌آموزی، ضمن تشریح فضای مجازی، به اهمیت و نقش این فضا در حال حاضر اشاره کردند. ایشان ضمن بیان ارکان چهارگانه فضای مجازی به تشریح کلی بازی‌های رایانه‌ای، شکاف نسلی، رویکرد مواجهه با فضای مجازی پرداختند.

سرپرست اداره کل پدافند غیرعامل استان آذربایجان شرقی:

سیاست کلی پدافند غیرعامل در استان استفاده از ظرفیت های علمی و پژوهشی مراکز دانشگاهی و تحقیقاتی است

دکتر نماینده مدیر کل فنی و حرفه‌ای آذربایجان شرقی با آقایی سرپرست اداره کل پدافند غیرعامل استان در خصوص زمینه‌های همکاری طرفین دیدار کردند.

در این دیدار سرپرست اداره کل پدافند غیرعامل استان با اشاره به اینکه موضوع پدافند غیرعامل در کشور نوپا بوده و برای رسیدن به اهداف پدافند غیرعامل یعنی مصون‌سازی زیرساخت‌های حائز اهمیت و به حداقل رساندن خسارات و تلفات سرمایه‌های انسانی و مادی، زمینه‌های پژوهشی و تحقیقاتی زیادی وجود دارد. از این جهت سیاست کلی پدافند غیرعامل در سطح کشور و بالاخص در استان استفاده از ظرفیت‌های علمی و پژوهشی مراکز دانشگاهی و تحقیقاتی استان برای رسیدن به این اهداف است.

آقایی ابزار امیدواری کرد که اداره کل فنی و حرفه‌ای استان با هدایت طرح‌های پژوهشی و پایان‌نامه‌ها به سمت موضوعات و مسائل پدافند غیرعامل و همچنین در بحث آموزش و تولید محتوا، اداره کل پدافند غیرعامل را یاری کند.

مدیر کل فنی و حرفه‌ای استان نیز در این دیدار با اشاره به ظرفیت‌های بالای آموزشی این اداره کل برای برگزاری دوره‌های تخصصی پدافند غیرعامل برای پرسنل و کارکنان واحدهای تولیدی و شهرک‌های صنعتی استان و استفاده از زیرساخت‌ها و ظرفیت‌های آموزشی موجود در شهرستان‌ها برای آموزش‌های عمومی و تخصصی پدافند غیرعامل در شهرستان‌ها اعلام آمادگی کرد.

در پایان این دیدار مقرر شد در آینده نزدیک تفاهم نامه علمی و آموزشی مابین اداره کل فنی و حرفه‌ای و اداره کل پدافند غیرعامل منعقد گردد.

همزمان با سراسر کشور:
مانور سراسری مدیریت مصرف برق در سطح استان برگزار شد

با توجه به پیش‌بینی افزایش دما طی روزهای آتی، مانور سراسری مدیریت مصرف برق همزمان با سراسر کشور در سطح استان با هدف اثبات توانمندی‌های موجود، جهت کاهش پیک بار شبکه سراسری برق اجرا شد. این مانور با همکاری کلیه صنایع، ادارات، بانک‌ها (دولتی/خصوصی) با هدف بهره‌مندی از کلیه امکانات و پتانسیل‌های موجود جهت کاهش پیک بار شبکه سراسری، در روز دوشنبه ۲۷ خرداد از ساعت ۱۲ الی ۱۶ با اعمال حداکثر صرفه‌جویی و با مدار آوردن کلیه دیزل ژنراتورهای موجود نسبت به قطع یا کاهش مصرف برق انجام شد.

آقایی سرپرست اداره کل پدافند غیرعامل استان در ارتباط با مانور مذکور بیان داشتند: طرح آماده بکار بودن ژنراتورهای ادارات و استفاده از انرژی‌های تجدید پذیر از بهمن ماه سال ۱۳۹۷ در حال پیگیری و اجرا بوده است. ایشان ابراز امیدواری نمودند با همکاری مردم و مسئولین ادارات در مدیریت مصرف برق شاهد قطعی شبکه برق و اختلال در روند خدمات‌رسانی در زمان پیک مصرف برق نباشیم.

معاون سیاسی، امنیتی و اجتماعی استانداری و جانشین شورای پدافند غیرعامل استان آذربایجان شرقی:

مخاطرات ناشی از انواع مواد خطرزا باید بررسی و در این زمینه آسیب‌شناسی شود.

اولین جلسه قرارگاه پدافند شیمیایی استان آذربایجان شرقی در سال جاری به ریاست معاون سیاسی، امنیتی و اجتماعی استانداری و با حضور اعضای قرارگاه برگزار گردید.

آقایی سرپرست اداره کل پدافند غیر عامل استان در این جلسه اظهار داشتند: با توجه به پیشرفت‌های علمی در حوزه‌های مختلف شیمیایی، بیولوژیکی، هسته‌ای، زیستی و ... ناگزیر به همگامی با پیشرفت‌های جهانی هستیم و غفلت از این حوزه‌ها و تهدیدات و آسیب‌های آن‌ها می‌تواند سلامت جان و مال مردم را به خطر اندازد و به نوعی استقبال از خطر است.

آذربایجان شرقی یک استان صنعتی است و تعداد قابل توجهی از واحدهای صنعتی شیمیایی در این استان مستقر هستند. از طرفی این استان در چهار راه مواصلاتی ریلی و جاده‌ای شمالغرب کشور قرار دارد و هر روز شاهد تردد تعداد زیادی از محموله‌های شیمیایی و سوختی پُرخطر در جاده‌ها

و خطوط ریلی هستیم، بنابراین رعایت اصول و الزامات پدافند غیرعامل در حوزه شیمیایی یک امر مهم و حساس به شمار می‌آید که امیدواریم با پویایی قرارگاه پدافند شیمیایی شاهد به حداقل رسیدن آسیب‌ها باشیم.

برای انتقال مراکز و زیرساخت‌های شیمیایی از داخل شهرها به خارج از مناطق مسکونی برنامه‌ریزی و مکاتباتی انجام شده و به دلیل اهمیت موضوع پیگیر تسریع در اجرای آن هستیم. ایشان همچنین خواستار ارتقاء آمادگی استان در برابر حوادث و تهدیدات احتمالی شیمیایی شدند و از برگزاری رزمایش ترکیبی با محوریت و موضوع شیمیایی در استان خبر دادند.

در این جلسه علیار راستگو معاون سیاسی، امنیتی و اجتماعی استانداری با اشاره به لزوم تأسیس اورژانس شیمیایی در استان گفت: باید کاری عملی، جامع و قابل دفاع در این حوزه داشته باشیم. وی خواستار مساعدت سازمان پدافند غیرعامل کشور و نیروهای مسلح در راه‌اندازی اورژانس شیمیایی در استان شد.

قرارگاه پدافند شیمیایی در جهت ساماندهی سیستم دفاعی منطقه با رویکرد مهندسی کاهش خطر و مصون‌سازی زیرساخت‌های شیمیایی و پتروشیمی استان باید فعال‌تر شود. وی همچنین خواستار مشخص شدن وظایف هر یک از دستگاه‌های اجرایی در قرارگاه پدافند شیمیایی شد و بیان داشت: نگاه به پدافند غیرعامل یک نگاه تخصصی است و باید نوع تهدیدات و ابعاد و جنس تهدیدات شناسایی شود تا راهکارهای مقابله با آن تهدیدات تدوین و اجرایی گردد.

ایشان با اشاره به این که مخاطرات ناشی از مواد خطرزا در سه بخش مواد شیمیایی، بیولوژیکی و رادیو اکتیو باید به‌صورت مستمر بررسی و در این زمینه آسیب‌شناسی شود، آموزش‌های لازم به جامعه هدف در زمینه خطرات و مضرات ناشی از این مواد را از ضروریات برشمردند. در وضعیت کنونی مشکلاتی در مدیریت حوادث از جمله نبود اطلاع‌رسانی متمرکز، ازدحام مردم در محل وقوع حادثه مشاهده می‌شود که لازم است پدافند غیرعامل با همکاری دستگاه‌های مرتبط از جمله صدا و سیما در جهت آموزش و آگاه‌سازی مردم اقدامات لازم را انجام دهد.

آموزش امنیت سایبری مدیران

۱- سیاست‌های امنیتی

۱-۱- سیاست‌های تشخیص هویت

سازمان باید با توجه به امنیت مورد نیاز برای هر سرویس و منبع اطلاعاتی که ارائه می‌دهد روش مناسبی را برای تشخیص هویت کاربران بکار گیرد. به عنوان نمونه لیست کلیه کاربران مجاز به دسترسی به هر منبع تعیین شده و هیچ یک از منابع سازمان نباید بدون تشخیص هویت قابل دسترسی باشد. همچنین سازمان باید در خصوص مدیریت رمز عبور کاربران سیاست و دستورالعمل‌هایی را تهیه کرده باشد.

۱-۲- کنترل دسترسی

سیاست‌های کنترل دسترسی عبارتند از:

- هر بخش باید نیازمندی‌های خود برای کنترل دسترسی را تعریف و مستند کند.
- کنترل دسترسی به منظور حفاظت از داده و سرویس‌ها روی یک رایانه و یا در محدوده شبکه، از دسترسی‌های غیر مجاز جلوگیری می‌کند.
- کلیه قوانین دسترسی تعیین شده برای کاربران باید به صورت منظم بازبینی شده و درصورتی‌که نیاز به تغییرات امنیتی یا تجاری در دسترسی وجود داشته باشد، عملیات بروز رسانی انجام شود.

۱-۳- رمزنگاری

ایمن بودن ارتباطات خصیصه‌ای مهم در بسیاری از زمینه‌های ارتباطی است. برای حفاظت از اطلاعات حساس و مهم باید از رمزنگاری استفاده کرد. انتخاب سیستم رمزنگاری به نوع کاربرد و پارامترهای مهمی از قبیل امنیت، کارایی و... بستگی دارد. در انتخاب الگوریتم رمزنگاری مناسب باید با رمزشکنی و حملات علیه سیستم‌های رمزنگاری آشنا بود و الگوریتمی را انتخاب کرد که در برابر حملات شناخته‌شده مقاوم باشد.

۱-۴- محافظت در برابر کدهای مخرب

کدهای مخرب در سیستم‌ها ممکن است از طریق اتصالات خارجی و فایل‌ها و نرم‌افزارهای روی دیسک‌های قابل انتقال، به وجود آیند. همچنین ممکن است در اثر مشکلات حفاظ‌های امنیتی (به عنوان مثال به دست آوردن کلمه عبور)، تخریب اطلاعات یا استفاده بدون مجوز از منابع سیستم تولید شوند. سیاست‌های محافظت عبارتند از:

- تمامی رایانه‌های موجود در شبکه سازمان باید به برنامه سرویس گیرنده ضد کدهای مخرب مجهز باشند.
- نرم‌افزارهای ضد کدهای مخرب باید دائماً و ترجیحاً به طور اتوماتیک از طریق برنامه سرور به‌روز شوند.

- در سازمان باید روال‌هایی برای بازدید و کنترل سیستم‌ها جهت اطمینان از فعال بودن و به‌روز بودن نرم افزارهای ضد کدهای مخرب تهیه شده باشد.

۱-۵- سیستم‌های تشخیص نفوذ

این سیستم عبارت است از یک یا چند سیستم که توانایی تشخیص تغییرات و رفتارهای خاص در سیستم و یا شبکه را دارا باشند. سیاست‌های تشخیص نفوذ عبارتند از:

- سازمان باید برای کنترل سیستم‌های تشخیص نفوذ خود برنامه‌ریزی کند.

- از خصوصیاتی که در انتخاب سیستم‌های تشخیص نفوذ باید رعایت کرد این است که فعالیت‌های خود را در برابر مسائل امنیتی و در امان بودن از دستبرد مانیتور کند.

۱-۶- نظارت و ارزیابی امنیتی

هزینه پیشگیری از یک حادثه امنیتی همیشه کم‌تر از بازیابی و کنترل آن است. به این دلیل ارزیابی استراتژی‌های امنیتی، شناسایی نقاط ضعف و قدرت وضعیت امنیتی فعلی، اندازه‌گیری خطرات امنیتی بر روی زیرساخت‌های IT و داده‌های حیاتی، کشف رخنه‌ها و آسیب‌پذیری‌های امنیتی از جمله امور ضروری برای مدیریت امنیت سازمان است. نظارت بر شبکه، فعالیتی مداوم است که چگونگی سیستم را از لحاظ کاربران و میزان امنیت محیطی تعیین شده آن، بر طبق طرح امنیتی بررسی می‌کند. برخی از سیاست‌های نظارت امنیتی عبارتند از:

- سازمان باید روال‌هایی برای ارزیابی امنیتی سیستم‌ها و شبکه خود داشته باشد که به صورت دوره‌ای بازدید شده، نقاط ضعف برای اصلاح به بخش‌های مربوطه اطلاع داده شود.

- در مرحله اول باید آشنایی کلی از دیدگاه عملیاتی هر سازمان نسبت به مقوله امنیت به دست آورد. مرحله دوم ارزیابی وضعیت امنیت سیستم‌ها، در نهایت برنامه‌های کاربردی، تجهیزات و شبکه است. این ارزیابی به کمک بخش مبارزه با حوادث امنیتی آمده برنامه‌ای برای تشخیص، دفاع و پاسخگویی به حملات رایانه‌ای طراحی می‌شود.

۱-۷- نصب، پیکربندی و کنترل تغییرات

ایجاد تغییرات در سازمان اجتناب‌ناپذیر است. یکی از بخش‌های لازم امنیت، مدیریت تغییرات یا پیکربندی است. هدف از این مقوله اطمینان از اعمال این تغییرات به صورت کاملاً کنترل شده، شناخته شده و مطلوب می‌باشد. برخی از سیاست‌های مدیریت پیکربندی عبارتند از:

- برنامه مدیریت پیکربندی و تغییرات باید در ابتدای ایجاد مدیریت پیکربندی طراحی شود.

- تنها مدیران سیستم باید قادر به نصب نرم‌افزار بر روی سرورها باشند. هم‌چنین کلیه تغییرات از جمله تغییرات فیزیکی و شبکه‌ای باید با اطلاع مدیر تغییرات صورت گیرد. فرد یا افراد مسئول برای مدیریت، پیکربندی و تغییرات باید مشخص شوند.

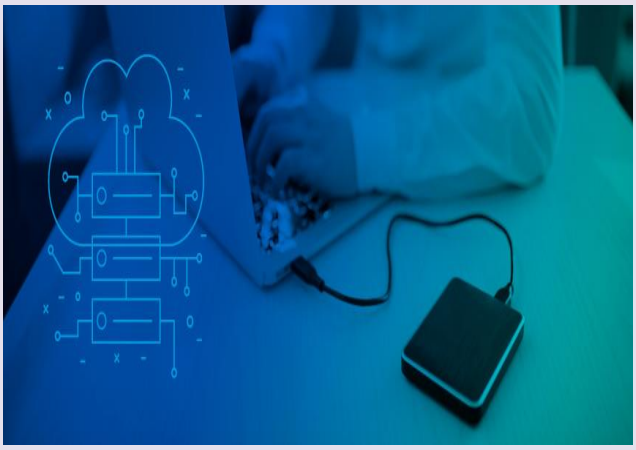
- نصب نرم‌افزارها و سیستم‌عامل‌ها به طور کامل و با کلیه وصله‌های موجود صورت گیرد.

- کلیه تجهیزات، نرم‌افزارها و سخت‌افزارهای هر سیستم باید برای بهره‌گیری امن و محدود کاربران پیکربندی و تنظیم شده باشند.

۱-۸- پشتیبان‌گیری

هر چند که سیستم امنی داشته باشیم ولی گرفتن نسخه

پشتیبان از داده‌های مهم ضروری است. روش‌های مختلفی برای پشتیبان گیری وجود دارد. در روش پشتیبان کامل از کلیه داده‌های موجود پشتیبان تهیه می‌شود، اما در روش پشتیبان افزایشی تنها از فایل‌هایی پشتیبان تهیه می‌شود که بعد از آخرین نوبت پشتیبان گیری تغییر کرده باشند. روش پشتیبان ناهمسانی مانند روش افزایشی است با این تفاوت که هر بار از فایل‌هایی که نسبت به آخرین پشتیبان‌گیری کامل تغییر کرده‌اند پشتیبان گرفته می‌شود.



۱-۹- آموزش و تربیت امنیتی

آگاهی‌رسانی و آموزش امنیتی نقش بزرگی در ایجاد امنیت و تداوم سازمان ایفا می‌کند. هدف برنامه آموزشی سازمان باید حفاظت از محرمانگی، جامعیت و دسترس پذیری سرمایه‌ها و داده‌های آن سازمان باشد. هدف از آگاهی‌رسانی جلب توجه مخاطبین به اهمیت مقوله امنیت در سطح سازمان و ایجاد هوشیاری و آگاهی امنیتی بیشتر توسط ابزارهایی مانند پوستر، بروشور، بولتن، روزنامه، مجله، رسانه صوتی، تصویری و غیره است. هدف از آموزش امنیتی، کسب دانش و تجربه در امر طراحی، پیاده‌سازی و پشتیبانی سیستم‌های امنیتی است. سیاست‌های آموزش و تربیت امنیتی عبارتند از:

- کمیته راهبری امنیت سازمان باید اقدام به سیاست-گذاری و نظارت بر پیاده‌سازی برنامه آگاهی‌رسانی، تربیت و آموزش کند.
- این کمیته ابتدا باید به شناسایی نیازهای مرتبط با آگاهی‌رسانی، تربیت و آموزش سازمان و اولویت‌دهی آن-ها بپردازد.
- سازمان باید برنامه آگاهی‌رسانی، تربیت و آموزش نیروهای انسانی خود را در زمینه امنیت تهیه کند. مراجع و سرفصل‌ها و نحوه اجرای هر برنامه تعیین گردد.
- بودجه مالی برای هر یک از برنامه‌ها پیش‌بینی شود.

منبع: خلاصه‌ای از کتاب

۱- آموزش امنیت سایبری مدیران – ناصر نامخواه – بهار ۱۳۹۰

تهیه و تنظیم: لیدا رسول اهری- کارشناس آموزش و پژوهش اداره پدافند غیر عامل

جنگ اقتصادی عرصه ظهور راهبرد تهدید همه‌جانبه و راهکار مقابله

مقاومت ۴۰ ساله جمهوری اسلامی با محوریت ولایت فقیه باعث شکست و ناکامی‌های راهبردی غرب شده است. نظام سلطه با راه‌اندازی جنگ هوشمندانه و ترکیبی با محوریت آمریکا و متحدانش درصدد فشار به ملت ایران برای دست کشیدن از آرمان‌ها و ارزش‌ها می‌باشد. از سوی دیگر جمهوری اسلامی ایران با پافشاری بر اصول و ارزش‌های خود به سازماندهی طرفداران و دوستداران خود در جهان و نیز تشکیل یک جبهه قوی و منسجم مشغول است.

بر اساس اظهارات خودشان، آمریکایی‌ها طی ۱۷ سال گذشته هفت تریلیون دلار در منطقه خاورمیانه هزینه کرده‌اند، ولی این هزینه هیچ دستاوردی برای آن‌ها نداشته است. از منظر سیاستمداران و نظامیان آمریکایی انقلاب اسلامی ایران مهم‌ترین مانع بر سر راه سلطه آمریکا بر جهان ارزیابی می‌شود. بر همین اساس، آمریکایی‌ها با هدف فروریختن یا وادار کردن جمهوری اسلامی ایران به تغییر رفتار از طریق پذیرش مذاکره در حوزه‌های مختلف، جنگ ترکیبی و هوشمند را علیه ایران به راه انداخته‌اند.

در این جنگ آمریکایی‌ها از طریق فشارهای اقتصادی، روانی و عملی به دنبال به آشوب کشاندن ایران و امنیتی کردن فضای کشور هستند. دشمن تلاش می‌کند از طریق جنگ اقتصادی و پدید آوردن شرایط سخت معیشتی برای مردم، مسئولان و سیاست‌های نظام را از طریق عملیات روانی، عامل اصلی این وضعیت معرفی کند.

رهبر معظم انقلاب اسلامی در خصوص هدف دشمن در جنگ اقتصادی می‌فرمایند: هدف دشمنان اعمال فشار اقتصادی بر مردم ایران برای دلسرد کردن آنان از نظام اسلامی است.

بدون شک، شناخت نقشه‌های دشمن، سیاست‌ها، راهبردها، تاکتیک‌ها و تکنیک‌هایی که او برای رسیدن به اهداف خود به کار می‌بندد از شروط لازم برای ناکام گذاشتن وی در رسیدن به اهداف است.

راهبرد جدید آمریکا و جنگ اقتصادی با ایران

به نظر می‌رسد با خروج آمریکا از برجام راهبرد جدید آمریکا، جنگ اقتصادی علیه ایران است که وارد مرحله نوینی شده که با مشارکت صهیونیست‌ها و لابی آن‌ها در آمریکا همراه شده است. در همین زمینه، اندیشکده بروکینگز، به ارتباط معنایی میان نمایش تلویزیونی نتانیاهو و اعلام ترامپ درباره خروج از برجام اشاره کرده است. بروکینگز معتقد است هدف اصلی نخست وزیر رژیم صهیونیستی از این نمایش، تقویت موضع ترامپ در زمینه توافق هسته‌ای است. نتانیاهو تلاش کرد که نشان دهد آنچه ترامپ درباره برجام می‌گوید، درست است و برجام همان طور که ترامپ گفته بدترین توافق تاریخ برای آمریکا است.

بنابراین فشارهای رژیم صهیونیستی و لابی یهودیان در آمریکا و کشورهای اتحادیه اروپا مسئله‌ای است که نمی‌توان از آن چشم پوشید، لذا رژیم صهیونیستی موضوع هسته‌ای ایران را در صدر دستور کار خود قرار داده است. به دنبال مذاکرات رژیم صهیونیستی با رهبران جهان مسئله هسته‌ای ایران به مسئله اصلی تبدیل شده است. لابی یهودیان در کنگره سنا و بسیاری از نهادهای سیاسی، اقتصادی و تسلیحاتی آمریکا نفوذ بلامنازع دارد. واقعیت آن است که روسای جمهوری آمریکا در برابر فشارهای لابی یهودیان در ایالات متحده ناتوان هستند؛ بنابراین آمریکا در برخورد با موضوعاتی که مربوط به جمهوری اسلامی ایران است از فرمول تهدیدهای

اقتصادی و حتی نظامی با هدف اطمینان دهی به رژیم صهیونیستی پیروی می‌کند.

جنگ اقتصادی ابزار آمریکا علیه ایران

بررسی همه جنگ‌ها نشان می‌دهد که کشورهای آغازگر جنگ هدف‌های اعمالی و اعلامی داشته‌اند که جنگ برای نیل به آن‌ها راه انداخته شد. دشمن با ابزارهای اقتصادی مانند پول، بانک، تحریم، محاصره اقتصادی، جنگ روانی و عملیات اخلال‌گرایانه در بازار پول و سرمایه که با هدف تضعیف و کاهش توان اقتصاد و مقاومت ملی تغییر رفتار یا رژیم را دنبال می‌کند.

کوینسی رایت اندیشمند غربی در این خصوص می‌گوید: «جنگ هنگامی آغاز می‌شود که دولتی نیت خود را برای توسل به آن، از طریق جنگ یا ضرب‌الاجل اعلام می‌دارد.». ماهیت جنگ اقتصادی آمریکا علیه ایران از طریق مواضع ترامپ آشکار شده است. اقدامات آمریکا علیه ایران به وضوح اراده و انگیزه قطعی و نیت دشمنان این کشور برای جنگ اقتصادی علیه ایران را نشان می‌دهد.

اهداف اعلامی آمریکا در جنگ اقتصادی علیه ایران، وادار کردن ایران به تسلیم اصلاحات مورد نظر کاخ سفید در برجام است، اما تحلیل‌گران سیاسی با رصد و رمزگشایی مواضع و عملکرد دولتمردان آمریکا، هدف اعمالی جنگ اقتصادی را تغییر رژیم ایران دانسته‌اند.

اعمال تحریم‌های سال‌های ۲۰۰۶ تا ۲۰۱۳ از سوی آمریکا موجب خارج شدن نفت ایران از بازار جهانی و عدم دریافت پول فروش نفت و قطعی شبکه بانکی بین‌المللی (سوئیفت) و فشارهایی بر بازرگانان ایرانی شد. همچنین بعد از خروج ترامپ از برجام، کنگره آمریکا جنگ قضایی-اقتصادی علیه جمهوری اسلامی ایران به راه انداخت و از این رهگذر به بهانه حمایت ایران از تروریسم اموال ایران در آمریکا را مصادره کرده است.

تحریم اقتصادی مدرن، جدیدترین جنگ اقتصادی است که آمریکایی‌ها طراحی کرده‌اند. بین‌المللی شدن تحریم‌ها یکی از شاخص‌های متمایز جنگ اقتصادی مدرن با گذشته است. آمریکا در دهه اخیر به این نتیجه رسیده که مهم‌ترین ابزار برای برخورد با کشورها استفاده از ابزار مالی است، لذا بیشترین تمرکز وزارت خارجه و خزانه‌داری آمریکا بر نظارت نظام بانکی کشورهاست. آن‌ها نقطه قوت خود را دلار می‌دانند و به طور رسمی اعلام کرده‌اند که دلار را تبدیل به سلاحی اقتصادی برای تحمیل اراده خود به کشورها کرده‌اند.

بدون تردید دشمن میدان کارزاری را برای غلبه بر جمهوری اسلامی ایران مهیا کرده است، روشنگری و بصیرت افزایی مردم راه غلبه دشمن در این جنگ تمام عیار و ترکیبی را مسدود خواهد نمود. در واقع، همه طراحی‌ها و استراتژی‌های «مرد دیوانه» آمریکایی، هرچند با بکارگیری همه ابزارهای فشار اعم از تحریم، تهدید، مذاکره و... کلید خورده است، اما دشمن از فهم این حقیقت ناتوان است که سنت الهی بر پیروزی جبهه حق بر باطل بنا نهاده شده است و ملت مسلمان ایران اعتقاد راسخ دارد که با تدبیر و بصیرت و استقامت، وعده نصرت الهی محقق خواهد شد و مکر دشمنان ناکام خواهد ماند.

راهکار مقابله با جنگ اقتصادی

کشور پهناور ایران با بهره‌مندی از منابع وسیع الهی، اقتصادی و بازار گسترده که سالیان درازی در استثمار کشورهای غربی و به ویژه امریکا بوده است. پس از وقوع انقلاب اسلامی ایران، دست آنان از این منابع کوتاه شد و کشور بر پایه منافع ملی خود حرکت کرد. از این رو، در نخستین روزهای پیروزی انقلاب اسلامی تحریم‌های اقتصادی گوناگون علیه اقتصاد نوپای کشور تازه استقلال یافته شکل می‌گیرد تا بلکه این نهال نوپا از پا بیفتد و از لحاظ اقتصادی زانو زند. لذا قطع روابط، تحریم‌های

اقتصادی در قالب قطعنامه‌های گوناگون، محدودیت‌های اقتصادی و افزایش بیمه تجارت با هدف ایجاد فشارهای سخت اقتصادی بر مردم و ممانعت از پیشرفت و خودکفایی کشور در حوزه‌های صنعت و انرژی هسته‌ای بوده است. این نبرد بی‌منتها سبب نام‌گذاری سال‌های ۱۳۸۸ تاکنون در حوزه اقتصادی با راهبردهای اصلاح الگوی مصرف، همت مضاعف و کار مضاعف، جهاد اقتصادی، تولید ملی، حمایت کار و سرمایه ایرانی، حماسه اقتصادی، اقتصاد مقاومتی اقدام و عمل، اقتصاد مقاومتی تولید - اشتغال و نیز حمایت از کالا و رونق تولید داخلی ایرانی از سوی رهبر معظم انقلاب اسلامی رقم خورد و یکی از جهت‌گیری‌ها و سیاست‌های رهبری نظام را به همراه داشت. امروزه حوزه تهدیدها از تغییر و تحولات بسیار گسترده‌ای بهره‌مند است؛ به گونه‌ای که با مفاهیم جدیدی همچون جنگ‌های نرم، رسانه، بانکی و اقتصادی روبه‌رو هستیم، حوزه اقتصاد از جمله حوزه‌های جدید جنگ است.

اهداف جنگ اقتصادی

هدف ایالات متحده آمریکا از جنگ اقتصادی علیه ایران ضعیف کردن آن به لحاظ بنیه و توان اقتصادی است تا با یک تلنگر نظامی با شکست کامل مواجه شود. این تجربه‌ای است که آمریکا طی سالیان گذشته در برخورد با سایر کشورها به دست آورده است، ولی قابل تحقق بودن آن در مورد ایران جای تأمل بسیاری دارد. اغلب در جنگ‌های کنونی این موضوع به وفور قابل مشاهده است. چنین جملاتی با هدف و رویکرد اقتصادی در جنگ‌ها دنبال می‌شود.

تعریف جنگ اقتصادی

در تمام جنگ‌ها، تهاجم، تخریب و انهدام زیرساخت‌های نظامی و اقتصادی مانند بنادر، پل‌ها، فرودگاه‌ها و کارخانه‌ها وجود دارد. برخی از صاحب‌نظران هدف از جنگ‌ها را کسب منافع اقتصادی می‌دانند. به هر حال امروزه با مفهومی جدید از تهدید و جنگ مواجه هستیم. جنگ اقتصادی یعنی جنگ با ابزارها، مؤلفه‌ها و عوامل اقتصادی مانند؛ پول، بانک تحریم، محاصره اقتصادی و زیرساخت‌های مالی. از این رو، جنگ اقتصادی یعنی با ابزارها و مؤلفه‌های اقتصادی علیه زیرساخت‌های اقتصادی یک کشور اقدام شود.

تهدید اقتصادی

حوزه اقتصاد به دلیل وجود رقابت شدید بر سر منافع از جمله حوزه‌های چالش‌برانگیز است. درون آن طیفی متنوع از اقدام‌ها اعم از همکاری، رقابت، مخالفت و تعارض را می‌توان جست. از جنبه‌های مهم تهدید، تهدید اقتصادی است. تهدید اقتصادی مجموعه خطرهایی است که رشد و توسعه پایدار یک جامعه یا سرزمین را به شیوه‌های مختلف دچار اختلال می‌کند و به شیوه‌های مختلف به اقتصاد یک محدوده جغرافیایی آسیب می‌رساند. انواع تحریم‌ها، رکود، گرانی، نابرابری و توزیع ناعادلانه درآمد در یک جامعه به صورت عمد یا غیر عمد از جمله تهدیدهای اقتصادی به شمار می‌رود. در یک تقسیم‌بندی کلان، می‌توان تهدیدهای اقتصادی را در دو حوزه اصلی تولید و توزیع رده‌بندی کرد؛ درحالی‌که گونه نخست متوجه افزایش میزان تولید متناسب با نیازمندی‌های عمومی است. دومین دسته تهدیدهایی را شامل می‌شود که به تعبیر جان ای رویمر برابری فرصت را در دستیابی به امکانات متأثر می‌سازند. جنگ اقتصادی مجموعه اقدام‌های متعمدانه، خصمانه و اخلال گرایانه دشمن است و برای کاهش توان اقتصاد، قدرت و مقاومت ملی با هدف تغییر رفتار صورت می‌گیرد؛ بنابراین جنگ اقتصادی می‌تواند به منزله ساز و کاری محسوب شود که با استفاده از ظرفیت‌های اقتصادی تلاش توان نظامی و ظرفیت رزم‌آوری دشمن را تقلیل دهد. جنگ اقتصادی

ماهیتی ضد توسعه‌ای دارد و در راستای ممانعت از توسعه پایدار و همه جانبه کشور و افزایش وابستگی صورت می‌گیرد. فساد اقتصادی یکی از مصادیق تهدیدهای اقتصادی به شمار می‌رود و به منزله یک جرم محسوب می‌شود.

اهداف اصلی برپایی جنگ اقتصادی از سوی دشمن را می‌توان در چهار هدف بیان کرد: ۱. کاهش توان مقاومت ملی ۲. کسب تسلط اقتصادی ۳. واپایش جریان‌های اقتصادی ۴. کاهش توان بازسازی، نوسازی و توسعه ملی.

در جنگ اقتصادی نوین، مؤلفه‌هایی متفاوت از نظام اقتصادی مورد هجوم قرار می‌گیرند. بخش‌هایی از اقتصاد در زمره اهداف دشمنان برای اعمال آسیب قرار دارند. این بخش‌ها در الگوهای سنتی جنگ اقتصادی مدنظر نبوده‌اند. جنگ مالی نمونه‌ای از اقدام‌های جنگ اقتصادی هوشمند است. به هر حال همزمان با توسعه الگوی هوشمند جنگ اقتصادی بر شدت راهبردی بودن آثار ناشی از جنگ اقتصادی افزوده و اگرچه اثر اولیه جنگ اقتصادی، زیان اقتصادی است، لیکن اثر ثانویه و کلیدی این است که اجرای جنگ اقتصادی می‌تواند موجب کاهش توان ملی و اقتصادی کشور شود.

چه باید کرد.

حمایت از کالای ایرانی مقوله‌ای مهم و کاربردی است. جهاد در حوزه اقتصاد یعنی باید با حرکت و روحیه انقلابی و جهادی وارد میدان اقتصادی شویم. حرکت باید الهی، مخلصانه و فی سبیل الله باشد و همان‌طور که رهبر معظم انقلاب اسلامی در بازدید از نمایشگاه کالای ایرانی فرمودند: «کارگر ایرانی یکی از بهترین کارگرهای دنیاست و تکیه به بیرون مرزها غلط اندر غلط است». اقتصاد مقاومتی از راهکارهای کاربردی مقابله با تهدیدها و جنگ اقتصادی دشمنان است. ریاضت اقتصادی با اقتصاد مقاومتی متفاوت است. ریاضت اقتصادی به طرحی گفته می‌شود که دولت برای کاهش هزینه‌ها و رفع کسری بودجه به کاهش یا حذف ارائه برخی از خدمات و مزایای عمومی دست می‌زند. این طرح مورد قبول جامعه اسلامی ما نیست، ولی اقتصاد مقاومتی برای مقابله با کسری بودجه، بهبود وضعیت مالی و توانمند کردن کشورها مؤثر است.

اجرای این طرح نتایجی مانند کاهش تقاضا، تورم، رقابت و مقابله با کسری بودجه را به دنبال دارد، لذا آنچه می‌تواند در حل مشکل اقتصادی کشور مؤثر باشد، توجه به تولید داخلی، درست استفاده کردن از منابع و امکانات و اعمال صحیح اقتصاد مقاومتی است. در نهایت، نتیجه می‌گیریم برای مقابله با دشمنان در حوزه جنگ اقتصادی لازم است بخشی در استان با هماهنگی دستگاه‌های امنیتی و دفاعی، قرارگاهی با عنوان قرارگاه دفاع اقتصادی تشکیل شود. در این قرارگاه با تجزیه و تحلیل فعالیت‌های اقتصادی- که علیه ایران صورت می‌گیرد - راهکارهای مقابله و برخورد را یافته و اقدام عملی صورت گیرد.

منابع:

1- islamtimes.org

تهیه و تنظیم: شمسعلی محمودیان – کارشناس پدافند غیرعامل

کاربرد الیاف FRP در بتن‌های ضد انفجار

از زمان پیدایش تکنولوژی انفجار و دانش مربوط به انفجار و بارهای انفجار مدت زیادی می‌گذرد. در این مدت پژوهش‌های نظری و عملی (آزمایشگاهی) بسیاری توسط مهندسان و دانشمندان بر روی مصالح و بارهای انفجاری انجام شده است. امروزه با افزایش تأسف‌بار تهدیدات طبیعی و غیرطبیعی همانند زلزله، جنگ، تهدیدات و حملات تروریستی بیشتر ساختمان‌های ارائه‌دهنده خدمات عمومی مانند بیمارستان‌ها، مدارس، ساختمان های اداری و ... و برخی مراکز دارای ثقل تخریب شده و از ارائه خدمات باز می‌مانند. تحلیل و طراحی سازه‌های مقاوم در برابر انفجار یا نیروی زلزله برای اماکن دارای اهمیت نیز توسعه یافته و آیین‌نامه‌های متعددی توسط مراجع مختلف برای تحلیل و طراحی مقاومت در برابر انفجار و دیگر عوامل تخریبی ارائه شده است. از طرفی با پیدایش مصالح نوین و گسترش کاربرد آن‌ها در مهندسی عمران و کاربری مناسب آن‌ها در مقاوم‌سازی سازه‌های موجود، چشم‌انداز جدیدی در جهت مقابله و کاهش خسارت‌های ناشی از این وقایع فراهم شده است. لذا در این مطلب به بررسی استفاده از مصالح مرکب یا همان الیاف FRP و تأثیر آن بر عملکرد سازه‌های بتنی در برابر انفجار (حملات جنگی، تخریب و خرابکاری و ...) پرداخته شده است. رعایت الزامات و استفاده از تکنولوژی‌های نوین در احداث ساختمان‌های دارای سطح‌بندی (حیاتی، حساس، مهم) مانند FRP ضروری به نظر می‌رسد.

بررسی موضوع:

در اثر تمام انفجارها موجی از هوا آزاد می‌شود که به نام موج ضربه‌ای شناخته می‌شود. این موج هوای بسیار متراکمی می‌باشد که به‌صورت کروی با سرعت بسیار زیاد از منبع انفجار به سمت خارج حرکت می‌کند و اگر این موج به سازه‌ای که در برابر انفجارها مقاوم‌سازی نشده است اصابت کند باعث خسارت‌هایی در اعضای سازه و اختلال در بهره‌برداری از آن سازه می‌شود. برای جلوگیری از این موضوع ماده‌ای اختراع شد بنام الیاف FRP (Fiber reinforcement polymer) یا فیبرهای پلیمری تقویت شده که در مسائل مرتبط با مقاوم‌سازی و پوشش سازه‌ای بتنی و فلزی کاربرد دارند.

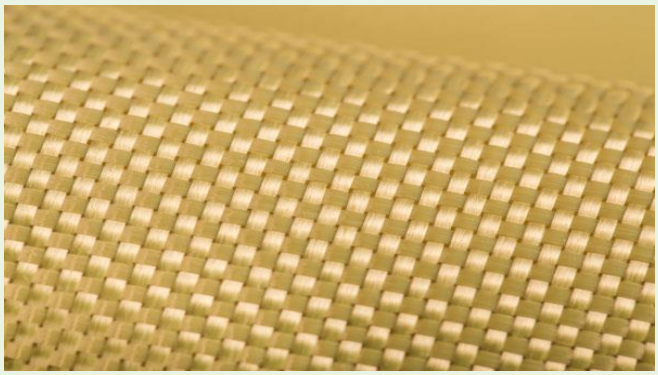
FRP از دو قسمت رزین FRP و فیبر FRP تشکیل می‌شود و کاربردهای متفاوتی در صنایع مختلف و ساختمان دارد. بیشترین کاربرد این مصالح در مقاوم‌سازی سازه‌ها جهت ترمیم، تقویت و مقاوم‌سازی ساختمان‌های بتنی و فلزی است. فیبرهای تشکیل دهنده FRP می‌توانند در یک راستا یا دو راستای عمود بر هم قرار داشته باشند، رزین FRP نیز اصولاً به عنوان یک محیط چسباننده عمل می‌کند که فیبرها را در کنار یکدیگر نگه می‌دارد. فیبرهای FRP با قرار گرفتن و نصب بر روی سطوح بتنی از قبیل دال‌ها، تیرها، ستون‌ها، دیوارهای بتنی و فونداسیون‌های بتنی می‌تواند باعث افزایش مقاومت بتن در ابعاد مختلفی شود. همچنین این فیبرها می‌تواند در ساختمان‌هایی با کاربری مسکونی، تجاری، اداری، صنعتی، نظامی، تأسیسات سنگین و همچنین سازه‌های آبی و دریایی مثل سد و کانال نیز کاربرد داشته باشد. علاوه بر این از فیبرهای FRP می‌توان در مقاوم‌سازی زیرساخت‌های مهندسی از قبیل پل‌های جاده‌ای و ریلی، مخازن آب و مواد شیمیایی، سیلوها و برج‌های خنک کننده نیز استفاده نمود. ساختمان FRP در شکل و ترکیبات مختلف تولید

می‌شود. مهمترین آن‌ها که در کارهای سازه‌ای استفاده می‌شود عبارتند از:

۱- الیاف FRP:

الیاف کامپوزیت FRP ورقه‌هایی با ضخامت چند میلیمتر از جنس FRP یا همان فیبرهای پلیمری تقویت شده هستند و با چسب‌های مستحکم و مناسب به سطح بتن چسبانده می‌شوند. ورقه‌های FRP پوشش مناسبی جهت ایزوله کردن و مقاوم‌سازی بتن سازه‌ها در برابر محیط‌های خورنده مجاور، جهت تعمیر و تقویت سازه‌های آسیب دیده (ناشی از زلزله و خوردگی آب‌های یون دار) و همینطور کاهش تغییر شکل سازه، کرنش‌ها و اثرات تخریب در بتن می‌باشد و تنش در میلگردهای داخل بتن را کاهش داده و از جاری شدن میلگرد جلوگیری می‌کند، همچنین بهترین گزینه جهت مقاوم‌سازی در برابر انفجار هستند.

شکل ۱: الیاف شیشه FRP



شکل ۲: الیاف آرامید

۲- میلگردهای FRP:

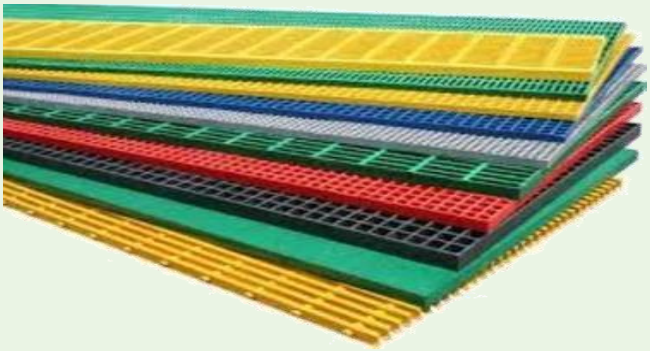
فولادها به‌طور مختصر در مقابل خوردگی به وسیله محیط قلیایی بتن محافظت می‌شوند اما وقتی در محیط‌های مهاجم قرار بگیرند مثل ترکیب رطوبت، افزایش دما و محیط کلریدی، خواص قلیایی بتن را کاهش می‌دهد و سبب خوردگی میلگردها می‌شود. به همین خاطر امروزه از میلگردهای ساخته شده با مواد پلیمری FRP در این سازه‌ها استفاده می‌کنند. به دلیل اینکه میلگردهای FRP برای یک رفتار غیر شکل‌پذیر می‌باشند لذا موارد استفاده این میلگردها محدود به سازه‌هایی می‌شود که مهمترین مشکل آن‌ها خوردگی یا مشکلات الکترومغناطیسی (برای مثال جلوگیری از نفوذ امواج به اتاق سرور) می‌باشد.

شکل ۳: میلگردهای FRP

۳- شبکه‌های کامپوزیتی FRP:

شبکه کامپوزیتی FRP از دیگر محصولات کامپوزیتی هستند که از برخورد میله‌های FRP در دو یا سه جهت ایجاد می‌شوند که از فیبرهای کربن و شیشه‌ای و رزین اپوکسی و یا پلی استر تولید می‌شود و برای مسلح کردن بتن مناسب می‌باشد. در سه مورد یاد شده بالا، الیاف FRP مدنظر بوده و طبق تحقیقات انجام گرفته به دلیل ظرفیت حرارتی بالا مقاومت خوبی در برابر امواج انفجار و ضربه دارد. به‌طور معمول از سه نوع الیاف مسلح کننده در بتن استفاده می‌گردد که عبارتند از:

۱-الیاف GFRP- پلیمرهای FRP مسلح شده با الیاف شیشه (Glass fiber reinforced polymer)



شکل ۴: شبکه‌های کامپوزیتی FRP

الیاف شیشه، الیاف‌های ساخته شده از همان شیشه هستند که با تکنولوژی خاصی تولید می‌شوند؛ به عبارت دیگر به وسیله ذوب سیلیکات‌ها به همراه پتاس یا اکسیدهای فلزی مختلف تولید می‌گردند. از مزایای این نوع الیاف می‌توان به قیمت پایین، مقاومت کششی بالا، مقاومت در برابر عوامل شیمیایی و مقاومت خوب در برابر حرارت بالا و ... اشاره نمود. معایب این نوع الیاف عبارتند از: پایین بودن ضریب ارتجاعی، حساسیت شدید به خراش در هنگام نصب، مقاومت کم در برابر پدیده خستگی در بارگذاری‌های متناوب، افزایش پدیده تردشکنی و ...

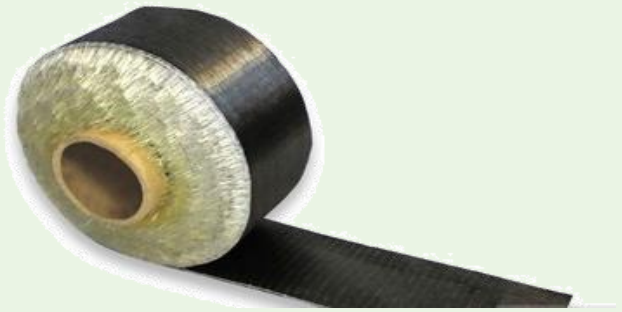
الیاف شیشه علاوه بر مزایای بالا مقاومت نسبتاً خوبی در برابر انفجار دارد چرا که مقاومت خوبی در برابر حرارت‌های بالا از خود نشان می‌دهد. انواع الیاف شیشه برحسب ترکیب مواد بکار رفته در تهیه آن‌ها به انواع گوناگون تقسیم‌بندی می‌شود که عبارتند از:

۱. الیاف شیشه الکتریکی (E-glass) ۲. الیاف شیشه سازه ای (S-glass) ۳. الیاف شیشه شیمیایی (C-glass) ۴. الیاف شیشه مقاوم در برابر قلیایی (GFRP)

در بین این ۴ مورد الیاف شیشه نوع E-glass بیشتر از بقیه کاربرد دارد.

۲-الیاف CFRP- پلیمرهای FRP مسلح شده با الیاف کربن (Carbon Fiber Reinforced Polymers):

فیبر کربن (الیاف کربن) رشته الیافی است که از حرارت دادن مواد عالی که قسمت عمده آن کربن می‌باشد در محیط گازهای بی‌اثر بدست می‌آید. الیاف کربن به الیافی گفته می‌شود که دست کم دارای ۹۰ درصد کربن هستند و از پیرولیز کنترل شده الیافی ویژه بدست می‌آیند. فیبر کربن مشکی رنگ، غیر حلال در آب و بدون بو بوده که در برابر مواد خورنده مثل اسیدها، بازها و مواد عالی مقاومت بسیار بالایی دارد. این الیاف به صورت تک جهته که در آن فیبر کربن موازی با راستای صفر درجه و دو جهته که در آن فیبر کربن به صورت دو راستای صفر و عمود بر آن (۹۰ درجه) قرار گرفته‌اند موجود می‌باشد. فیبر کربن در زمینه‌های متعددی مانند مقاوم سازی ساختمان‌ها، صنایع دفاعی، خودروسازی و بسیاری از صنایع مهم دیگر کاربرد دارد. الیافی که در ساخت فیبر کربن یا همان CFRP ها مورد استفاده قرار می‌گیرد، معمولاً توسط عناصری مثل رزین اپوکسی به المان‌ها و اعضای باربر در سازه‌ها اضافه شده و ظرفیت برشی، خمشی و محوری اعضا را بهبود می‌بخشند.



شکل ۴: الیاف کربن CFRP

فیبر کربن مقاومت بالایی در برابر حرارت دارد که باعث می‌شود آن‌ها را در دسته الیاف غیر قابل انفجار دسته‌بندی کرد. همچنین سبک بودن آن‌ها و مقاومت بالایشان سبب استفاده گسترده از آن‌ها در صنعت کامپوزیت FRP و بهسازی لرزه‌ای سازه‌ها شده است. یکی از مهم‌ترین مزیت‌های فیبر کربن در کنار وزن سبک آن‌ها مقاومت کششی بسیار بالای این الیاف است. در

صنعت ساختمان نیز به خاطر این ویژگی‌ها اصلی ترین کاربردها را دارد که عبارتند از: مقاوم‌سازی ساختمان و تقویت سازه‌ها با کامپوزیت CFRP، ساخت صفحات، ورق‌ها و لمینیت کربن، الیاف تقویت کننده بتن‌های مقاومت بالا، ساخت دیوارهایی با مقاومت بالا و سبک کربنی، ساخت سازه‌های پس کشیده و پیش تنیده کربنی در سازه‌های بتنی، استفاده در جداره داخلی تونل‌ها.

۳-الیاف AFRP– پلیمرهای FRP مسلح شده با الیاف آرامید (Aramid Fiber Reinforced Polymers):

الیاف آرامید (Aramid fibers) نوعی از الیاف مقاوم در برابر حرارت و الیاف مصنوعی قوی می‌باشد. آرامید در هوا فضا و برنامه‌های نظامی، زره بالستیک و مواد مرکب بالستیک مورد استفاده در لاستیک دوچرخه کاربرد دارد. آروماتیک پلی‌آمید (که به اختصار آرامید نامیده می‌شود) اولین بار در اوایل دهه ۱۹۶۰ میلادی توسط شرکت دوپونت و با نام تجاری نومکس معرفی شد. مشخصه اصلی این محصول مقاومت بالا در مقابل گرمای زیاد بود. از این محصول در تهیه پوشاک حفاظتی، تصفیه هوا، عایق حرارتی و الکتریکی و به عنوان جایگزینی برای پنبه نسوز استفاده می‌شد. مدیر تحقیق و توسعه وقت شرکت دوپونت، دکتر ویلفرد سوینی، دانشمندی اسکاتلندی بود. تحقیقات بیشتر بر روی آرامیدها در شرکت دوپونت توسط شیمیدان آمریکایی لهستانی، استفانی کولک، منجر به ساخت پارا آرامید کولار در سال ۱۹۷۳ میلادی شد. در حال حاضر الیاف آرامید با نام تجاری کولار در صنعت شناخته می‌شود. همچنین به نام الیاف AFRP نیز شناخته می‌شود.

ویژگی‌های الیاف آرامید:

مقاومت خوب در برابر سایش، مقاومت خوب در برابر حلال‌های آلی، نارسانا، هیچ نقطه ذوبی ندارد (تخریب از ۵۰۰ درجه سانتی گراد شروع می‌شود)، اشتعال پذیری کم، یکپارچگی خوب پارچه در دماهای بالا، حساس به اسیدهای آلی و نمک، حساس به پرتو فرابنفش. الیاف آرامید به دلیل مقاومت بالا در برابر گرما در مقابل انفجار نیز مقاوم هستند.

طبق مقایسه‌ای که بین الیاف مختلف FRP جهت مقاوم‌سازی در برابر انفجار صورت گرفته است، به ترتیب الیاف با مصالح کربن، شیشه و آرامید بهترین عملکرد پلیمری در بتن را دارند.

مزایای مشترک این الیاف عبارتند از:

۱. دوام بالا، هزینه و قیمت مناسب برای خرید FRP
۲. سبک وزن بودن و چگالی پایین صفحات FRP
۳. مشخصات فنی بالا شامل مدول و مقاومت بالا
۴. قابل کاربرد در برابر محیط‌های اسیدی و ترکیبات شیمیایی (مقاومت ضد اسیدی)
۵. نفوذ ناپذیری مغناطیسی که برای مکان‌هایی مناسب است که در آنجا دستگاه‌های حساس به میدان مغناطیسی وجود دارد.
۶. مقاومت در برابر ضربه
۷. اتصال FRP و همپوشانی آسان در بتن و آهن
۸. ساختمان FRP عایق مناسبی در مقابل محیط اسیدی، شیمیایی و خورندگی می‌باشد.

در دنیای امروز پروژه‌های ترمیم، بازسازی و مقاوم‌سازی بسیار فراگیر شده و نکات و مسائل جدیدی مطرح شده که با استفاده از نشریه‌های سیستم FRP قابل حل هستند. مهمترین این موارد که توسط مصالح FRP مقاوم سازی می‌شوند عبارتند از:

۱. خوردگی و فرسایش سازه‌ای در سیستم‌های صنعتی، پالایشگاه‌ها و پتروشیمی مقاوم‌سازی و تقویت FRP با رزین اپوکسی
۲. ترمیم و تقویت المان‌ها و اجزا توسط FRP
۳. اشتباهات طراحی

۴. افزایش تعداد طبقات ساختمان‌های بتنی

۵. مقاوم‌سازی تیرها و ستون‌های بتنی با استفاده از مواد FRP

۶. افزایش ظرفیت برشی و ...

الیاف‌های FRP را می‌توان در کاربری‌های مختلف بکار برد که مهمترین آن‌ها عبارتند از:

۱. تقویت سازه‌های مقاوم در برابر انفجار

۲. جلوگیری از نفوذ امواج الکترومغناطیس به قسمت‌های مهم مثل اتاق سرور در اماکن حساس و حیاتی و مهم

۳. افزایش ظرفیت باربری و شکل‌پذیری ستون‌ها، تیرها، دال‌ها و اتصالات بتن آرمه

۴. تقویت دیوارهای بتن آرمه

۵. تقویت دیوار تونل‌ها

۶. نشیمن‌گاه تجهیزات راکتورها

نتیجه‌گیری:

الیاف FRP از نظر هزینه در عین مقرون به صرفه بودن مقاومت خوبی در برابر امواج انفجار و ضربه، حرارت، نفوذ امواج الکترومغناطیس (برای مثال به اتاق‌های سرور یا دیتای سازمان‌ها) و خوردگی دارند و می‌توانند گزینه بسیار خوبی برای تقویت بتن سازه در برابر آسیب‌های احتمالی این موارد باشد. این الیاف را می‌توان برای مقاوم‌سازی سازه در برابر زلزله نیز بکار برد که می‌تواند سازه را تا حد زیادی در مقابل نیروی زلزله از آسیب‌های احتمالی به اعضای سازه ایمن نگه دارد.

منابع:

۱. محیا فاضلی پور، محمدرضا توکلی زاده "مقاله بررسی اثر چیدمان ورق‌های CFRP در مقاوم‌سازی دیوارهای بتنی در برابر با انفجار"

۲. کتاب "مقاوم‌سازی سازه‌های بتنی با الیاف FRP " تألیف دکتر موسی کاظم

3.Antonio nanni,Antonio de luca, hany jawaheri zadeh “Reinforced concrete with FRP bars”

تهیه و تنظیم: احد ماهری- رئیس گروه طرح و اجرا اداره کل پدافند غیر عامل، میر رسول حسینی اقدام (کارشناس امریه پدافند غیر عامل)

ضرورت افزایش نشاط اجتماعی در کشور با بسیج امکانات برای نشاط اجتماعی

شادی همیشه با هیجان و خنده و حرکت همراه است؛ در حالیکه در نشاط، احساس بهجت و سرور لزوماً با خنده همراه نیست ولی احساسی است که موجب لذت فرد می‌شود. نشاط فقط خنده و طنز نیست، بلکه یک حس درونی است. به همین ترتیب شادی می‌تواند یک هیجان کاذب و زودگذر حتی منفی باشد، در حالی‌که ماهیت نشاط اصیل، مثبت و با دوام است. شادی‌های کاذبی که توسط محرک‌های متفاوت مثل داروهای روان‌گردان، مواد مخدر، الکل و غیره به دست می‌آید کوتاه و گذرا بوده و پیامدهای اندوه و افسردگی را به دنبال خواهد داشت. لذا در اینجا صحبت از صرفاً شاد کردن جامعه با تمسک به هر ترفندی نیست بلکه منظور روش‌هایی است که شور و هیجان پایا و واقعی را در تمامی زیرگروه‌های جامعه بالا برده و باعث تحرک بیشتر و مؤثرتر جامعه شود و برخلاف عرف و هنجارهای جامعه نباشند.

نشاط اجتماعی شرایطی است که افراد از آن احساس رضایت کرده و پویایی دارند. به عنوان مثال مردم در ماه محرم با شرکت در مجالس عزاداری احساس رضایت، پویایی و نشاط درونی می‌کنند و یا کسی که در حرفه خود می‌تواند کار مفیدی انجام بدهد و یا در کانون‌های فرهنگی، ادبی یا خیریه‌ها فعالیت می‌کند، به علت احساس مفید واقع شدن، نشاط واقعی پیدا می‌کند و از رضایت درونی بسیار بالایی بهره‌مند می‌شود؛ بنابراین جامعه سالم و با نشاط، مهمترین سرمایه و موتور توسعه هر کشوری است که می‌تواند کشور را در ریل پیشرفت و آبادانی نگه دارد.

نشاط اجتماعی در همه کشورها به عنوان یکی از پیش نیازهای توسعه مطرح می‌شود. نمی‌توان انتظار داشت در کشوری که نیروهای انسانی خموده و ناامیدی دارد، بتوان بر مشکلات فائق آمد و راه‌حلی برای غلبه بر مشکلات جاری کشور پیدا کرد. جامعه افسرده و بی‌انگیزه، قادر نخواهد بود از زیرساخت‌ها و امکانات کشور به‌درستی بهره ببرد و پتانسیل‌های پیشرفت به هرز خواهد رفت. در جامعه با نشاط، روابط انسان‌ها بر پایه مهر و احترام بنا نهاده می‌شود و انگیزه‌ها برای کار و تولید، بسیار بالاست.

این روزها کشور ما بیش از هر زمان دیگری به نشاط اجتماعی نیازمند است تا بتواند بر مشکلات و آسیب‌های اجتماعی فائق آید. شادی و نشاط در جمع محقق می‌شود و با اتحاد به دست می‌آید، بنابراین داشتن کشوری بانشاط، مستلزم این است که هر فردی خودش را در برابر حل آسیب‌های اجتماعی مسئول بداند و خود را مبرا از مشکل دیگران نداند.

برای افزایش نشاط اجتماعی، مهم‌ترین مسئله زمینه‌سازی برای رشد شخصیت متعادل و سالم در افراد است. برای این کار، نیاز به برخی راهکارهای تربیتی و آموزشی مستقیم داریم. مثلاً وقتی فردی در شهر زندگی می‌کند، باید مسئولیت‌های شهروندی به او آموزش داده شود، به نحوی که آن فرد، اطمینان داشته باشد حقوق او توسط افراد دیگر رعایت می‌شود و البته او نیز حقوق دیگران را رعایت می‌کند. برای ایجاد چنین فضایی، نیاز به تقویت قانونمندی در افراد داریم. این کار از طریق آموزش‌های عمومی در سطح جامعه و آموزش‌های رسمی در مدارس امکان‌پذیر است. وقتی افراد احساس کنند در جامعه‌ای زندگی می‌کنند که در آن عدالت، قانونمندی، نظم، همدلی، رعایت اخلاق و ارزش‌های انسانی وجود دارد، بدون شک ضریب نشاط اجتماعی بالا خواهد رفت.

برای ایجاد این فضا، به تربیت صحیح همه افراد جامعه و اصلاح ساختارهای اجتماعی نیاز داریم.

یک جامعه برای این که بانشاط باشد، باید در چهار زمینه امنیت اجتماعی، رفاه، سلامت و فرصت برابر آموزشی در وضع مطلوبی قرار داشته باشد. جامعه‌ای که از نشاط اجتماعی دور باشد، خشونت در آن جامعه افزایش پیدا خواهد کرد. ریشه بسیاری از مشکلات اجتماعی مانند بی‌اعتمادی عمومی، خشونت، نزاع‌ها، افسردگی، اعتیاد و... را می‌توان در کمبود شادی و نشاط در جامعه جست‌وجو کرد.

زمانی که مردم جامعه‌ای از نشاط اجتماعی برخوردار باشند وفاق، همبستگی، تعلق اجتماعی، تعاملات اجتماعی مطلوب، رضایت از زندگی و همچنین سلامت روانی و اجتماعی افراد افزایش پیدا کرده و طبیعی است که به موازات آن آسیب‌های اجتماعی نیز کاهش می‌یابد و انگیزه برای کار و تلاش افزایش می‌یابد. در نتیجه چنین جامعه‌ای، مسیر پیشرفت و ترقی را طی خواهد کرد.

گسترش شهرنشینی و به دنبال آن آپارتمان نشینی، دسترسی بیشتر به فناوری‌های نوین از جمله اینترنت و شبکه‌های اجتماعی و ماهواره‌ای، مشغله‌های فراوان کاری و زندگی، تحمیل استرس‌های متعدد بر افراد، تعامل فرهنگی بالا و خطر تضعیف هویت فرهنگی، کاهش ارتباطات عاطفی میان مردم و افزایش اختلالات روانی، از ویژگی‌های جامعه امروزی و زندگی به اصطلاح مدرن است.

داشتن احساس محرومیت ناشی از بالاتر بودن خواسته‌ها از داشته‌ها، عدم انسجام بافت شهری، سرانه پایین فضای فرهنگی، فضای سبز و ورزشی و مشکلات اقتصادی و ... از جمله مهمترین عواملی هستند که موجب کاهش نشاط در شهرها می‌شوند.

عوامل کاهنده نشاط اجتماعی

الف) عوامل فردی، خانوادگی: عواملی چون اشکال در سلامت جسمی، روانی، اجتماعی و معنوی، دستمزد پایین و مشکلات شدید اقتصادی، کمبود وسایل تفریحی و رفاهی، ضعف در مهارت‌های ارتباطی با دیگران و انزوا و گوشه‌گیری، مشکلات خانوادگی و کاهش روابط خانوادگی و اجتماعی و...

ب) عوامل محیطی-اجتماعی: عواملی چون بافت شهر و محله که با استانداردهای روحی و روانی و فرهنگی در تعارض باشند، آلودگی‌های صوتی و سر و صدای شدید و خشن، تنش‌های عصبی، ترافیک، عدم ثبات اقتصادی و تورم و دسترسی سخت و دشوار به امکانات لازم و اولیه برای یک زندگی ساده، بزهکاری‌های اجتماعی، بی‌نظمی و هنجارشکنی‌های اجتماعی، تعارض بین فرهنگ و باورهای دینی با رفتارهای اجتماعی و به روز، شکل‌گیری و نهادینه شدن بعضی ضد ارزش‌ها مانند کم شدن روحیه تعاون و همدلی و نوع‌دوستی یا زیاد شدن ریا و دروغ، از بین رفتن یا کم شدن فضای سبز، جدا شدن انسان از طبیعت و پرندگان و سایر مخلوقات زیبای خداوند، کم شدن جلوه زیبای شهری با بکارگیری رنگ‌های سرد و کدر، عدم استفاده از جلوه‌های ویژه و زیبا از نمادهای هنری و استفاده بسیار محدود از موسیقی آب روان، خرابی‌ها و زشتی‌های پیاده‌روها، خیابان‌ها، دیوارهای منازل و سایر عناصر شهری و ...

منابع:

برگرفته از:

1- didarnews.ir

تهیه و تنظیم: حمید غفارلو- کارشناس حفاظت و امنیت

هشدار مایکروسافت درباره بهره‌برداری مهاجمین از آسیب‌پذیری آفیس

پژوهشگران امنیتی مایکروسافت اخیراً هشداری را مبنی بر یک موج ایمیل اسپم منتشر کرده‌اند که در حال توزیع اسناد مخرب RFT است. فایل RTF منتقل شده در این حملات چندین اسکریپت مخرب با نوع‌های مختلف VBScript، PowerShell، PHP و ... را دانلود و اجرا می‌کند تا payload نهایی بدافزار بارگذاری شود.payload نهایی یک تروجان در پشتی است. پس از انتشار هشدار مایکروسافت، سرورهای فرمان و کنترل تروجان از دسترس خارج شدند. آسیب‌پذیری مورد سوء استفاده در این عملیات CVE-2017-11882 است که خوشبختانه این آسیب‌پذیری در وصله ماه نوامبر ۲۰۱۷ برطرف شده است. این آسیب‌پذیری در مؤلفه Equation Editor مجموعه آفیس قرار دارد و بهره‌برداری از آن به مهاجم اجازه اجرای کد دلخواه را فراهم می‌کند. طبق گزارش Recorded Future، آسیب‌پذیری CVE-2017-11882 سومین نقص پراستفاده در سال ۲۰۱۸ بوده است. همچنین کسپرسکی نیز این آسیب‌پذیری را به عنوان پراستفاده‌ترین نقص امنیتی در سال ۲۰۱۸ معرفی کرده است. نکته قابل توجه درباره این نقص عدم احتیاج به تعامل کاربر برای فعال‌سازی است، بر خلاف سایر آسیب‌پذیری‌ها که کاربر باید ماکروها یا سایر ویژگی‌های امنیتی را غیرفعال کند.

یک پژوهشگر امنیتی آسیب‌پذیری با درجه حساسیت بالا در برنامه‌های ویرایش متن Vim و Neovim در لینوکس را کشف کرده است. این آسیب‌پذیری با شناسه CVE- 2019-12735 ردیابی می‌شود. این آسیب‌پذیری نقص اجرای دستور دلخواه در سیستم‌عامل است و در برنامه‌های خط فرمان Vim و Neovim وجود دارد. این دو برنامه به طور پیش فرض در توزیع‌های لینوکس نصب شده است. آسیب‌پذیری نحوه مدیریت ویژگی modeline در ویرایشگر Vim را تحت تأثیر قرار می‌دهد. ویژگی modeline به کاربران اجازه می‌دهد تا گزینه‌های دلخواه در ابتدا و انتهای یک فایل را تعیین کنند. این ویژگی به طور پیش فرض برای تمامی فایل‌ها فعال است. مهاجم می‌تواند کاربر را فریب دهد تا فایل دستکاری شده را در Vim یا Neovim باز کند که منجر به اجرای دستور در سیستم لینوکسی می‌شود. دو کد اثبات مفهومی (PoC) برای این آسیب‌پذیری منتشر شده است که توسط یکی از آن‌ها مهاجم با دسترسی از راه دور می‌تواند به یک shell معکوس دسترسی یابد. تیم‌های توسعه Vim و Neovim بروزرسانی‌های مربوط به رفع آسیب‌پذیری CVE- 2019-12735 را در نسخه‌های ۸.۱.۱۳۶۵ و ۰.۳.۶ منتشر کرده‌اند. برای کاهش اثرات این نقص، کارشناسان توصیه می‌کنند تا ویژگی‌های modelines و modelineexpr غیرفعال شوند و از افزونه securemodelines استفاده شود.

آسیب‌پذیری اجرای کد در دو برنامه ویرایشگر متن در لینوکس

آسیب‌پذیری حدود یک میلیون سیستم‌های ویندوزی نسبت به نقص BlueKeep

حدود یک میلیون رایانه ویندوزی نسبت به نقص BlueKeep آسیب‌پذیر هستند. این نقص در سرویس Remote Desktop Protocol (RDP) قرار دارد که نسخه‌های قدیمی سیستم‌عامل ویندوز را تحت تأثیر قرار می‌دهد. آسیب‌پذیری BlueKeep که با شناسه CVE-2019-0708 ردیابی می‌شود، در دو هفته گذشته مورد توجه جوامع امنیت سایبری قرار گرفته است. این نقص پس از ارائه وصله ماه می ۲۰۱۹ توسط مایکروسافت، افشا شد. مایکروسافت هشدار داد که نقص BlueKeep می‌تواند مشابه فرایند کرم مورد سوء استفاده قرار گیرد، بدین معنی که مهاجمین و بدافزارها برای توزیع و نشر خود از آن بهره‌برداری کنند. این مورد مشابه اکسپلویت EnternalBlue SMB است که در سال ۲۰۱۷ برای توزیع باج افزارهای WannaCry، NotPetya و Bad Rabbit از آن استفاده شد.

اما علیرغم سطح خطر این آسیب‌پذیری، هیچ حمله‌ای با استفاده از آن ثبت نشده است زیرا هیچ اکسپلویت عمومی که عوامل تهدید بتوانند توسط آن به حملات خود بپردازند، وجود ندارد. وصله‌های رفع این آسیب‌پذیری در دسترس هستند که برای ویندوز XP، ویندوز ۷، سرور ۲۰۰۳ و سرور ۲۰۰۸ ارائه شده‌اند. سازمان‌هایی که از نسخه‌های قدیمی ویندوز استفاده می‌کنند باید نسبت به اعمال وصله‌های منتشر شده اقدام کنند.

حملات بدافزار ثبت‌کننده صفحه کلید HawkEye به کسب و کارها

حملات جدیدی در سطح جهان در دو ماه گذشته گزارش شده که روی کاربران حوزه کسب و کار تمرکز دارد و با استفاده از بدافزار ثبت‌کننده صفحه کلید HawkEye (keylogger) انجام شده است. در این عملیات از ایمیل‌های اسپم استفاده شده است که سازمان‌های بخش‌های مختلف از جمله حمل و نقل و لجستیک، سلامت، واردات و صادرات، بازاریابی، کشاورزی و غیره مورد هدف قرار گرفته‌اند. به گفته پژوهشگران، بدافزار HawkEye به منظور سرقت اطلاعات از دستگاه‌های آلوده طراحی شده است، اما از این بدافزار می‌توان به عنوان بارگذاری کننده سایر بدافزارها از بات‌نت‌ها نیز بهره‌برداری کرد. هدف از انتشار این بدافزار ثبت‌کننده صفحه کلید، سرقت اطلاعات احراز هویت و داده‌های حساس کاربران است.

به طور دقیق‌تر، در این عملیات از HawkEye Reborn v۸،۰ و HawkEye Reborn v۹،۰ استفاده شده که در پیوست ایمیل‌های اسپم برای کاربران ارسال شده است. پیوست ایمیل‌ها یک فایل صورت‌حساب جعلی است که زمانی که کاربر اقدام به باز کردن آن کند، فایل mshta.exe منتقل می‌شود. برای اتصال به سرور کنترل و فرمان (C&C)، این فایل از PowerShell استفاده و بدافزار در ادامه payload های دیگری را نیز منتقل می‌کند.

کسب پایداری در سیستم قربانی با کمک اسکریپت AutoIt انجام می‌شود. این اسکریپت در قالب یک فایل اجرایی با نام gvg.exe به ورودی‌های AutoRun در رجیستری ویندوز اضافه می‌شود. در نتیجه در هر بار راه‌اندازی مجدد سیستم، بدافزار به طور خودکار اجرا می‌شود. همچنین پژوهشگران متوجه فایلی با نام AAHEP.txt شدند که تمامی دستورالعمل‌های مرتبط با بدافزار ثبت‌کننده صفحه کلید Hawkeye در آن قرار دارد. آخرین نسخه این بدافزار، HawkEye Reborn v۹ است که می‌تواند اطلاعات را از برنامه‌های مختلف دریافت کند و سپس از طریق پروتکل‌هایی مانند FTP، HTTP و SMTP آن‌ها را برای اپراتورهای خود ارسال کند.

هدایت بازدیدکنندگان سایت‌های وردپرسی و جوملا به سایت‌های مخرب

پژوهشگران امنیتی اسکریپت هدایت کننده (redirect) مخربی را شناسایی کرده‌اند که بازدیدکنندگان سایت‌های دارای سیستم مدیریت محتوا (CMS) وردپرس و جوملا را به سایت‌های مخرب هدایت می‌کنند. پژوهشگران، اسکریپتی را شناسایی کرده‌اند که قادر به تزریق کد در فایل .htaccess است.

سایت‌هایی که توسط این کد آلوده شده‌اند، بازدیدکننده را به سایت‌های آگهی منتقل می‌کند که در ادامه منجر به نصب نرم‌افزار مخرب در سیستم قربانی می‌شود. پژوهشگران در این حملات یک اسکریپت php را کشف کرده‌اند که در پوشه‌های هاست میزبان، فایل‌های.htaccess را جستجو و آن‌ها را دستکاری می‌کند. پس از دستکاری فایل.htaccess، مراجعین سایت قربانی به یک سایت مخرب که در این حمله آدرس http[:]//portal-f[.]pw/XcTyTp است، هدایت می‌شوند.

اسکریپت php کشف شده برای هر دو سیستم مدیریت محتوا وردپرس و جوملا عمل می‌کند که در این کد در متغیر $wp پوشه‌های مربوط به وردپرس و در متغیر $jm پوشه‌های مربوط به جوملا تعیین شده‌اند. نحوه نفوذ مهاجمین به سایت‌های وردپرس و جوملا در این حمله هنوز مشخص نشده است.

هکرها در حال اسکن اینترنت هستند تا سرورهای ویندوز که در حال اجرای پایگاه داده MySQL هستند را شناسایی کنند و سپس آن‌ها را با باج افزار GandCrab آلوده کنند. این حملات به نوعی جدید هستند و پژوهشگران تاکنون هدف قرار گرفتن سرورهای MySQL را برای نصب باج افزار مشاهده نکرده‌اند. آنان اعلام کرده‌اند که هکرها پایگاه داده‌های MySQL قابل دسترس از اینترنت و قبول کننده دستورهای SQL را اسکن می‌کنند تا در صورت ویندوزی بودن سرور آن، با دستورهای SQL مخرب یک فایل در سرور را هدف قرار داده و باج افزار GandCrab را در فضای میزبان نصب کنند. با این که اکثر مدیران سیستم‌هاُ، با گذرواژه از سرورهای MySQL محافظت می‌کنند، مهاجمین اسکن خود را بر مبنای یافتن سرورهایی که دارای پیکربندی مناسبی نیستند یا برای آن‌ها گذرواژه تعریف نشده است، انجام می‌دهند. پژوهشگران در این حملات یک سرور از راه دور را شناسایی کردند که روی آن HFS یا HTTP File Server در حال اجرا است. HFS یک وب سرور مبتنی بر ویندوز است. در این سرور پنج فایل اجرایی با نام ۳۳۰۶ مشاهده شده و تعداد دانلود هر یک مشخص است. در سرور شناسایی شده یک فایل اجرایی لینوکس ELF با نام RDP نیز وجود دارد که در این حمله از آن استفاده نشده است. در زمان تهیه این گزارش، فایل ۱-۳۳۰۶.exe که در هانی‌پات پژوهشگران شناسایی شده، بیش از ۵۵۰ بار دانلود شده است. همچنین سایر فایل‌ها (۳۳۰۶-۲.exe، ۳-۳۳۰۶exe. و ٤-۳۳۰۶.exe) به همراه فایل اول، در مجموع ۸٤۲ بار دانلود شده‌اند که نشان دهنده قربانیان حمله است. با اینکه دامنه این حمله گسترده و وسیع نیست، اما این گونه حملات تهدیدی مهم برای سرورهای MySQL که پورت ۳۳۰٦ آن‌ها در معرض دسترسی است، تلقی می‌شود.

تلاش مهاجمین برای نصب باج‌افزار از طریق پایگاه‌داده MySQL

مهم‌ترین بروزرسانی های ماه جاری شرکت‌های تولید کننده سخت افزار و نرم افزار

شرکت Adobe در بروزسانی‌های امنیتی مربوط به ماه ژوئن چندین نقص را در محصولات Flash، ColdFusion و Campaign Classic رفع کرده است. از جمله مهم‌ترین آسیب‌پذیری‌های رفع شده مربوط به نرم‌افزار Flash Adobe است که در نسخه‌های ۳۲،۰،۰،۱۹۲ و قبل‌تر در سیستم‌عامل‌های ویندوز، مک، لینوکس و کروم وجود دارد.

مایکروسافت بروزرسانی‌های امنیتی مربوط به ماه ژوئن ۲۰۱۹ را منتشر کرده که در آن ۸۸ آسیب‌پذیری دارای درجه حساسیت بحرانی رفع شده است. چهار مورد از آسیب‌پذیری‌های روز صفر که در ماه گذشته برای نسخه‌های مختلف ویندوز منتشر شدند، در وصله‌های ماه ژوئن مایکروسافت برطرف شده‌اند.

از جمله آسیب‌پذیری‌های وصله شده مربوط به پروتکل RDP موسوم به BlueKeep و آسیب‌پذیری مهم دیگر مربوط به مجموعه محصولات آفیس می‌باشد.

نکته دیگر درباره این بروزرسانی‌ها این است که طبق هشدار مایکروسافت، برخی از کلیدهای امنیتی مبتنی بر بلوتوث ممکن است پس از اعمال وصله‌های این ماه کار نکنند. این مورد به دلیل پیکربندی نامناسب در پروتکل اتصال آن‌ها انجام شده است.

شرکت اینتل ۳٤ آسیب‌پذیری در محصولات مختلف خود از جمله یک آسیب‌پذیری بحرانی در موتور همگرای مدیریت و امنیت (Intel CSME) که سوءاستفاده از آن می‌تواند منجر به افزایش امتیاز شود را برطرف نموده است. در این بروز رسانی، علاوه بر این نقص بحرانی، ۷ مورد آسیب‌پذیری دارای درجه حساسیت «بالا»، ۲۱ مورد «متوسط» و ۵ مورد «پایین» وصله شده‌اند. این نقص‌ها جدا از نقص‌هایی هستند که Intel چندی پیش برطرف ساخته است.

شرکت سیسکو در ماه جاری بروزرسانی‌هایی برای چندین آسیب‌پذیری از جمله سه آسیب‌پذیری با درجه حساسیت بالا در محصولات خود رفع کرده است که یک مهاجم با استفاده از این آسیب‌پذیری‌ها قادر به اجرای کد از راه دور، انجام حمله انکار سرویس (DOS) و همچنین نصب میان‌افزارهای دستکاری شده بر روی برخی از سخت‌افزارهای این شرکت می‌باشد.

بعد از بازی نهنگ؛

خطرات بازی "مریم" چیست؟

در سال گذشته شاهد این بودیم که چگونه بازی نهنگ آبی در بین مردم به سرعت شناخته شد و تعداد بسیاری از مردم که اکثر آن‌ها نوجوانان ۱۳ تا ۱۸ سال بودند جان خود را از دست دادند. بازی نهنگ آبی اپلیکیشن و برنامه خاصی نداشت و در آن مراحل بازی طی پیام‌هایی به کاربران ارسال می‌شد اما در بازی مریم اپلیکیشن خاصی وجود دارد که با نهایت تأسف در مارکت های معروفی همچون گوگل پلی و اپ استور به راحتی در اختیار افراد قرار گرفته است. به دلیل دسترسی راحت به این برنامه قطعاً افراد بیشتری تحت تأثیر این برنامه قرار خواهند گرفت.

بازی مریم ساخت فردی با هویت سعودی است. زبان‌بازی، کاملاً عربی بوده و در صورت عدم آشنایی با این زبان، بازی کردن کمی دشوار خواهد بود. البته زبان انگلیسی نیز در گیم پلی بازی وجود دارد که می‌توان از آن استفاده نمود. اصلی‌ترین شباهتی که باعث می‌شود بازی مریم و نهنگ آبی هر دو در دسته بازی‌های خطرناک قرار گیرند، ایجاد ترس، دلهره، وحشت و تهدید کاربر می‌باشد. در بازی مریم شاهد یک گیم پلی و خط سیر داستانی هستیم. داستان بازی از آنجایی شروع می‌شود که یک دختر جنگ زده ۹ ساله به نام مریم در جنگل گم شده و از کاربر درخواست می‌کند تا او را به خانه‌اش برساند؛ اما در طی مسیر اتفاقات وحشتناکی را تجربه خواهد نمود و کاربر در حین اجرای بازی هیجان زیادی خواهد داشت.

موضوع بازی بیشتر در رابطه با اجنه و جن‌زدگی می‌باشد و در سراسر بازی، شاهد پخش صداهای ترسناک و رعب‌آور هستیم. در ابتدای بازی اطلاعات مختلفی از کاربر درخواست می‌شود که از جمله آن‌ها می‌توان به اسم کاربر، آدرس و اجازه دسترسی به صفحات مجازی اشاره کرد. البته تا زمانی که کاربر این اطلاعات را وارد نکند، اجازه بازی به او داده نخواهد شد. با اشتباه وارد کردن اطلاعات می‌توان وارد بازی شد، اما باید به این نکته نیز توجه داشته باشید که این بازی دسترسی‌های مختلفی را در گوشی شما درخواست می‌کند و می‌تواند به اطلاعات واقعی شما تا حد زیادی دست پیدا کند. آنچه سبب می‌شود این بازی در زمره بازی‌های خطرناک قرار گیرد، اتفاقاتی است که ممکن است بعد از اتمام بازی، گریبان گیر کاربر شود. به عنوان نمونه، پس از اتمام بازی، دقیقاً در ساعت ۳ نصف شب، یک شماره ناشناس با شما تماس خواهد گرفت و عبارتی به معنی این‌که "ما با تو هنوز کار داریم" به صورت رباتی پخش خواهد شد. این عمل مکرراً انجام خواهد شد و هر بار صداهای عجیبی برای کاربر پخش می‌شود تا کاربر را مجاب کند که او جن‌زده شده است.

کشف شبکه گسترده عملیات سایبری تهاجمی علیه ایران

امیر دریابان علی شمخانی در خصوص اقدامات متقابل جمهوری اسلامی ایران در قبال اظهارات مشاور امنیت ملی آمریکا که هفته گذشته تأیید کرد آمریکا در حال انجام عملیات سایبری تهاجمی خارجی است تا به روسیه و دیگران نشان دهد که آن‌ها بهای مداخله‌های خود در امور آمریکا را خواهند پرداخت، گفت: اولاً حمله سایبری علیه کشورها روی دیگر حمله نظامی است که آمریکا به صورت غیر قانونی و برخلاف موازین حقوقی و حتی ادبیات و سیاست‌های امنیتی خود، به آن مبادرت می‌کند و طبیعتاً باید پاسخگوی این اقدام خود در مجامع بین المللی باشد.

در نهمین اجلاس بین‌المللی نمایندگان عالی امور امنیتی کشورهای جهان نیز که سال گذشته در روسیه برگزار شد یکی از اصلی‌ترین موضوعات مورد بحث تهدیدات سایبری و کارکرد آن در توسعه تروریسم و همچنین نحوه همکاری و مشارکت کشورها برای مقابله با آن بود، طبیعتاً اظهارات اخیر بولتون که به نوعی اذعان به تروریسم دولتی است در اجلاس فردا بازتاب خواهد داشت.

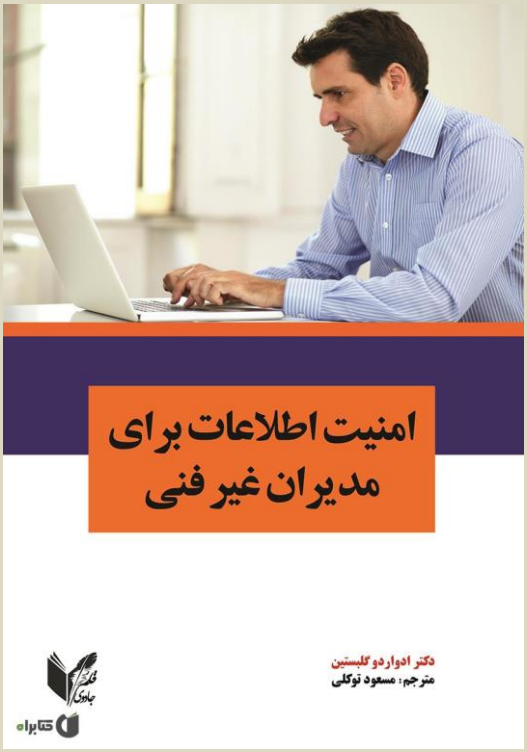
نکته‌ای که جا دارد در این بخش به آن اشاره کنم فاصله معنی‌دار میان توان ادعایی و قابلیت‌های واقعی آمریکا در حوزه‌های سایبری، نظامی و امنیتی است. آمریکایی‌ها علاقمند هستند با هدف ارعاب و لطمه زدن به اراده کشورها برای مقاومت در برابر خوی تجاوزگری این کشور منطق تخیلی فیلم‌های هالیوودی را به عنوان واقعیت به افکار عمومی منتقل کنند.

جالب است بدانید، مدتی قبل یکی از پیچیده‌ترین شبکه‌های سایبری سازمان سیا که در حوزه جاسوسی سایبری به کار گرفته می‌شد و بخش مهمی از ظرفیت‌های عملیاتی سیا در کشورهای هدف امریکا بود توسط دستگاه‌های اطلاعاتی ایران کشف شد و مورد ضربه قرار گرفت.

با توجه به همکاری جاری میان ایران و بسیاری از کشورهای جهان در قالب ایجاد "شبکه ضد جاسوسی بین‌المللی" علیه امریکا، ما اطلاعات شبکه کشف شده را که در چند کشور دیگر نیز فعال بود در اختیار شرکایمان قرار دادیم که منجر به شناسایی و فروپاشی شبکه افسران اطلاعاتی سیا و دستگیری تعدادی از جاسوسان و مجازات آن‌ها در کشورهای مختلف شد. شمخانی تصریح کرد: آمریکایی‌ها این اقدام ایران را " شکست مفتضحانه اطلاعاتی" نام‌گذاری کردند. مستندات این پروژه نیز تماماً موجود است، چون بخشی از ابعاد این کیس قبلاً توسط خود سازمان سیا افشا شده، می‌شود این اسناد را هم منتشر کرد تا مردم در جریان موضوع قرار بگیرند و من از وزارت اطلاعات می‌خواهم فیلم‌ها و بخشی از اعترافات را حتماً منتشر کنند.

معرفی کتاب

معرفی کتاب امنیت اطلاعات برای مدیران غیر فنی



کتاب امنیت اطلاعات برای مدیران غیرفنی نوشته ادواردو گلبشتاین، مختص افرادی است که به دنبال فهم امنیت اطلاعات هستند.

امروزه با توجه به رشد روز افزون فضای کسب و کار و نیز تنوع فرآیندهای تجاری، استفاده از تکنولوژی‌هایی نظیر فناوری اطلاعات و ارتباطات در سازمان‌ها و شرکت‌های مختلف به امری ضروری تبدیل شده است. با توجه به اینکه همه مدیران، لزوماً متخصص رشته فناوری اطلاعات و ارتباطات (ICT) یا رشته‌های فنی وابسته نیستند، مناسب است حداقل افرادی که در این حوزه مدیریت و فعالیت می‌کنند، اطلاعاتی کلی در این خصوص کسب نمایند.

در این اثر آنچه برای حفاظت از دارایی‌های اطلاعاتی لازم است و اینکه نقش آن‌ها چه باید باشد در نظر گرفته شده است. فصول کتاب امنیت اطلاعات برای مدیران غیر فنی، به طور مختصر به دنبال این است که چرا مشکل امنیت اطلاعات تا به حال حل نشده و اینکه چه چیزهایی در استفاده از سیستم‌های کامپیوتری و شبکه‌ها در دنیا دخیل هستند؛ دنیای متصلی که در آن بیش از ۲ میلیارد انسان به اینترنت دسترسی دارند و بیش از ۴ میلیارد آن‌ها دارای گوشی‌های همراه هستند. بسیاری از آن‌ها دانش کافی از نحوه کار این دستگاه‌ها و اینکه چطور می‌توانند سبب اختلال شوند را ندارند.

در نوشتن این کتاب با زبانی ساده از قوانین، مقررات و استانداردهای بین‌المللی جاری، در جهت بیان کلیات موضوع امنیت اطلاعات و دستورالعمل‌های آن بهره برده شده است.

طرح‌های کسر خدمت سربازی

به اطلاع می‌رساند که سازمان پدافند غیرعامل کشور (مرکز مطالعات پدافند غیرعامل کشور و مرکز مطالعات فنی و مهندسی پایداری ملی کشور) برای دانش‌آموختگان و فارغ‌التحصیلان مقاطع کارشناسی ارشد و دکتری طرح‌هایی برای کسر خدمت سربازی و نخبگی (جایگزین خدمت سربازی) در نظر گرفته است. علاقمندان می‌توانند علاوه بر مراجعه به وب‌سایت‌های مربوطه با مراجعه به اداره کل پدافند غیرعامل استانداری آذربایجان شرقی از روند ثبت‌نام مطلع شوند.

- وب سایت مرکز مطالعات فنی و مهندسی پایداری ملی کشور:
  http://mafpa.ir/
- وب سایت مرکز مطالعات پدافند غیرعامل کشور:
  http://www.pdrc.ir

سایت های مرتبط با پدافند غیرعامل	
وب سایت پایداری ملی	http://www.paydarymelli.ir
مرکز مطالعات پدافند غیرعامل	http://www.pdrc.ir
استانداری آذربایجان شرقی – پدافند غیرعامل	http://ostan-as.gov.ir/?PageID=42
پلیس فتا	http://www.cyberpolice.ir/
مرکز مطالعات فنی و مهندسی پایداری ملی	http://mafpa.ir/
سایت دومین کنفرانس ملی پدافند سایبری	hamayesh.iau-maragheh.ac.ir/cp2018

جهت دسترسی به آرشیو نشریه به این لینک مراجعه فرمایید.