جمهوری اسلامی ایران
وزارت کشور
استانداری آذربایجان شرقی

سال ۱۳۹۸
سال رونق تولید

سازمان پدافند غیرعامل کشور

ماهنامه اداره کل پدافند غیر عامل

شماره ۳۱، فروردین ماه ۱۳۹۸

رئیس سازمان پدافند غیرعامل کشور:

پدافند غیرعامل در سال جدید نباید دچار غافل‌گیری شود.

علیرضا کریمی در مراسم افتتاحیه دومین دوره استانی تربیت راهنمایان سواد فضای مجازی:

فرهنگ سازی و آموزش استفاده صحیح از فضای مجازی لازمه بهره برداری حداکثری از این فضا است.

در این شماره می خوانید:


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

سازمان پدافند غیرعامل کشور

ماهنامه اداره کل پدافند غیر عامل – شماره ۳۱

مدیر مسئول:
علیرضا کریمی

سردبیر:
علی ابراهیمی

دبیر تحریریه:
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

رئیس سازمان پدافند غیرعامل: پدافند غیرعامل در سال جدید نباید دچار غافل‌گیری شود.

سردار سرتیپ پاسدار غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور هم‌زمان با اعیاد شعبانیه در دیدار با کارکنان سازمان پدافند غیرعامل اظهار کرد که در سال جدید معاونت اطلاعات و عملیات برآوردی از تهدیدات و حوادث پیش روی کشور در سال ۱۳۹۸ با همکاری همه معاونت‌ها و قرارگاه‌ها تهیه و تدوین کرده است، این برآورد اطلاعاتی و عملیاتی این پیام را به ما می‌دهد که سازمان پدافند غیرعامل در سال جدید نباید دچار غافل‌گیری شود این برآورد به همه معاونت‌ها و قرارگاه‌ها ابلاغ‌شده است، اولین اولویت آن این است که هر آنچه در این برآورد اطلاعاتی و عملیاتی ارائه‌شده توسط قرارگاه‌های مربوطه مورد بررسی و تحقیق قرار گیرد و پیش‌بینی‌ها و آمادگی‌های لازم را کسب کنند. سازمان پدافند غیرعامل بنا به الزامی که دارد باید کلیه امور در این سازمان را مبتنی بر انجام فعالیت‌ها به‌صورت کاملاً علمی و دانشی پیگیری کند لذا بایستی دانش خود را در حیطه کاری سازمانی خود به روز کرده و از دانش روز دنیا در پیش‌برد اهداف و شناسایی تهدیدات نهایت استفاده را کنیم. در این راستا کارشناسان این سازمان توسط معاونت آموزش دوره‌ها و کلاس‌های آموزشی متناسب با دانش روز را سه‌ماهه نخست سال جدید خواهند گذراند تا یک آموزش ضمن خدمت همگانی در راستای بروز شدن در اطلاعات و دانش علمی در سطح کارشناسان ایجاد شود.

رئیس سازمان پدافند غیرعامل خبر داد: در سال ۱۳۹۸ ما باید از همه ظرفیت‌های فناورانه که در مرحله نخست ۱۵ نرم‌افزار و سامانه پشتیبانی است رونمایی خواهیم کرد و مورد بهره‌برداری قرار خواهیم داد که مبنای برنامه‌های اجرایی سال جدید در سازمان پدافند غیرعامل خواهد بود. این نرم‌افزارها در چهار فاز پیاده‌سازی، آموزش و بهره‌برداری آزمایشی و درنهایت به‌صورت کامل و عملیاتی اجرایی خواهد شد، خبر بعدی که باید به همکاران و همرزمان گرامی بدهم این است که در سال جاری سازمان پدافند غیرعامل یک شبکه اجتماعی درون‌سازمانی با عنوان «شبکه ارتباطی سلمان» را طی دو الی سه ماه آینده طراحی و راه‌اندازی خواهد کرد که یک جمعیت ۲۰۰-۳۰۰ هزار نفری اعم از شرکت‌ها، دانشگاه‌ها، اساتید، دانشجویان، کارکنان، مدیران، مسئولین در آن سازمان‌دهی خواهند شد و می‌توانند از ظرفیت‌های آن در راستای ارتباطات درون‌سازمانی امن، فعالیت‌های پژوهشی، فرهنگ‌سازی، برگزاری همایش‌های مجازی، آموزش‌های مجازی و استفاده از اخبار، جراید الکترونیکی و دیگر خدمات آن بهره‌مند گردند.

اخبـــار اداره کـــل پدافند غیر عامل

جلسه کمیته مقابله با بیوتروریسم پدافند غیر عامل استان برگزار شد.

اولین جلسه کمیته مقابله با بیوتروریسم سال ۱۳۹۸ در روز پنجشنبه ۲۹ فرودین به ریاست جناب آقای علیار راستگو معاون سیاسی امنیتی و اجتماعی استانداری و دبیر کمیته مقابله با بیوتروریسم استان تشکیل شد. در ابتدای جلسه آقای علیرضا کریمی مدیرکل پدافند غیرعامل استانداری گزارشی از فرایند تشکیل کمیته ارائه و اظهار نمودند که در ابتدای امر مسئولیت دبیرخانه این کمیته بر عهده دفتر امنیتی انتظامی بود که با توجه به وظایف پدافند غیرعامل در حوزه زیستی و تهدیدات ناشی از آن، مسئولیت دبیرخانه برابر ابلاغیه وزارت کشور به عهده اداره کل پدافند غیرعامل واگذار شد. با توجه به تهدیدات روز افزون دشمنان در حوزه تهدیدات نرم ضرورت دارد اعضای کمیته در خصوص رصد و پایش تهدیدات و اقدامات پیشگیرانه‌ی این حوزه، وظایف خود را به نحو احسن انجام دهند.

در ادامه جلسه نمایندگان دانشگاه علوم پزشکی و جهاد کشاورزی استان گزارشی از تهدیدات بیوتروریستی مربوط به حوزه خود را ارائه نمودند. در این جلسه جناب آقای راستگو معاون سیاسی امنیتی استانداری ضمن تبریک روز ارتش و فرارسیدن نیمه شعبان اظهار نمودند: دشمنان ایران در طول چهل سال گذشته انواع و اقسام نیرنگ‌ها و ترفندها از جمله جنگ تحمیلی هشت ساله، ترور و تحریم‌ها و ... را برای ضربه زدن به نظام جمهوری اسلامی بکار برده و نتیجه نگرفته‌اند و اکنون با سرخوردگی از اقدامات قبلی رو به جنگ نرم از جمله اقدامات بیوتروریستی آورده‌اند تا به نظام مقدس جمهوری اسلامی ضربه وارد کنند. لذا وظیفه همه ماست که با شناسایی تهدیدات و آسیب شناسی حوزه مدیریتی خود از جمله در حوزه‌های بیولوژیکی و کشاورزی نسبت به تهدیدات پیش رو خود را آماده و مصون‌سازی کنیم که تمام این‌ها در حوزه کاری کمیته بیوتروریسم بوده و وظیفه ما را بیش از پیش سنگین‌تر می‌کند.

رئیس کمیته مقابله با بیوتروریسم استان اعلام داشتند از اعضای جلسه انتظار می‌رود نسبت به شناسایی تهدیدات در حوزه کاری خود اقدام و راهکارهای پیشگیری و برخورد با آن‌ها را به این کمیته ارسال نمایند تا تصمیمات لازم اتخاذ شود.

برگزاری دومین دوره آموزشی تربیت راهنمایان فضای مجازی

دومین دوره آموزشی تربیت راهنمایان فضای مجازی با مشارکت اداره کل پدافند غیرعامل استان و دفتر استانی سازمان فضای مجازی سراج از تاریخ ۲۸ لغایت ۳۰ فروردین ۹۸ به مدت ۳ روز با موضوعات آینده پژوهی فضای مجازی و رویکردها، مبانی سواد رسانه ایی و رژیم مصرف فضای مجازی، مدیریت رسانه و فضای مجازی در خانواده، اعتیاد اینترنتی و خود تنظیمی و درمان، فرهنگ شهرت در فضای مجازی، حقوق و جرائم سایبری و ... با حضور اساتید برجسته کشوری و استانی در محل دانشگاه تبریز برگزار شد.

روز اول: برگزاری مراسم افتتاحیه

در مراسم افتتاحیه کریمی، مدیرکل پدافند غیرعامل استان آذربایجان شرقی، ضمن اشاره به اهمیت و نقش فضای مجازی در زندگی امروزی، در خصوص فرصت‌ها و تهدیدات این فضا مطالبی بیان نمودند. ایشان لازمه بهره‌گیری حداکثری از قابلیت‌های فضای مجازی و کاهش آسیب‌های آن را، فرهنگ‌سازی و آموزش استفاده صحیح از این فضا از طریق ارتقای سواد رسانه‌ای آحاد جامعه به خصوص کودکان و نوجوانان عنوان کردند.

روز دوم: برگزاری نشست مطالبه گری سواد فضای مجازی

در نشستی با عنوان مطالبه گری سواد فضای مجازی مهندس کریمی در خصوص حوزه‌های مختلف کاری پدافند غیرعامل و تهدیدات همه جانبه و روزافزون کشور و استان مطالبی بیان کردند و با بیان گستردگی حوزه فعالیت پدافند غیرعامل در استان، خواستار همکاری و هماهنگی تنگاتنگ کارگروه‌ها و دستگاه‌های مسئول از جمله صدا و سیما، شهرداری، آموزش و پرورش و ... در پیشگیری از تهدیدات و حوادث و کاهش آسیب‌ها و خسارات ناشی از آن‌ها شدند. ایشان علت بسیاری از حوادث و اتفاقات را ناآگاهی و عدم شناخت از تهدیدات و آسیب‌پذیری‌ها عنوان نموده و بر اهمیت امر آموزش و اطلاع رسانی تأکید کردند.

روز سوم: برگزاری مراسم اختتامیه

حجت‌الاسلام و المسلمین دکتر آل هاشم نماینده ولی فقیه در استان و امام جمعه تبریز در مراسم ضمن قدردانی از مهندس کریمی مدیرکل پدافند غیرعامل گفت: امروزه داشتن سواد رسانه‌ای و بصیرت افزایی و آگاهی بخشی در مورد فضای مجازی از اهمیت بالا برخوردار است. فضای مجازی هم منافع دارد و هم مضرات، ما باید برای این فضا برنامه‌ریزی داشته باشیم و باید با استفاده از ظرفیت و فرصت‌های شبکه‌های اجتماعی مفاهیم اسلامی و بحث حجاب و عفاف را ترویج دهیم.

ایشان با اشاره به رعایت اخلاق، تقوا، انصاف و انقلابی گری در فضای مجازی خاطر نشان کردند: اگر از این فضا آگاهی و اطلاعات لازم و کافی نداشته باشیم زمینه بروز رفتارهای ناهنجار فراهم خواهد شد لذا آموزش و شناساندن چالش‌ها و فرصت‌ها و نحوه استفاده از این فضا از ضروریات می‌باشد.

Internet Banking, Cloud Computing: Opportunities, Threats

بانکداری اینترنتی، رایانش ابری: فرصت‌ها و تهدیدها

بانکداری اینترنتی شیوه‌ای کارآمد برای ارائه خدمات به مشتریان و جنبشی بزرگ در خدمات اطلاعاتی است. بانکداری اینترنتی زمان و هزینه انجام فعالیت‌های مالی را کاهش داده و منجر به همکاری مشتریان بانکی در فعالیت‌های بانکداری مانند پرداخت‌ها، انتقال پول و... بدون مراجعه حضوری شده است. رایانش ابری مدل رایانشی بر پایه شبکه‌های رایانه‌ای مانند اینترنت است که الگویی تازه برای عرضه، مصرف و تحویل خدمات رایانشی با بکارگیری شبکه ارائه می‌کند.

با استفاده از رایانش ابری مشتریان می‌توانند سرویس‌های مورد نیاز را کاهش یا افزایش دهند. آن‌ها باید بر اساس میزان خدمات دریافتی هزینه کنند، همچنین قادر به افزایش میزان مصرف و تسهیم منابع هستند. با تقسیم بار کاری در مراکز مختلف، رایانش ابری موجب بهینه‌سازی مصرف زیرساخت فناوری اطلاعات می‌شود. همچنین کاربران قادر به دسترسی به سرویس‌ها از مناطق دیگر هستند. به منظور ارزیابی صحت نتایج و دست یابی به نظرات کارشناسان روش فازی دلفی استفاده شده است.

NIST (موسسه ملی استاندارد و فناوری)، ۵ ویژگی را برای رایانش ابری تعریف کرده است که شامل دسترسی گسترده به شبکه، جمع‌آوری منابع، الاستیسیته سریع و خدمات اندازه‌گیری شده است. همچنین این موسسه چهار مدل برای رایانش ابری از جمله ابر عمومی، ابر خصوصی، ابر جامعه و ابر هیبریدی ارائه کرده است.

ابر عمومی، زیرساخت‌های مشترک میان کاربران مختلف بوده و این سرویس‌ها برای همه ارائه می‌شوند. در ابر خصوصی، زیرساخت فناوری اطلاعات ارائه شده

و برای سازمان‌های خاص پشتیبانی می‌شود. در این مدل، هیچ گونه اشتراک سخت‌افزار و نرم‌افزار میان کاربران مختلف وجود ندارد. در ابر جامعه، زیرساخت ابری در میان جامعه خاص تسهیم می‌شود که دارای اهداف خاصی نظیر بانک‌ها و سازمان‌های نظامی است. ابر ترکیبی، ترکیبی از مدل‌های دیگر برای اهداف خاص می‌باشد.

۱- SWOT برای بانکداری اینترنتی و رایانش ابری

فناوری رایانش ابری شیوه‌ای برای ارائه خدمات در بستر اینترنت است. بانکداری اینترنتی به عنوان یک سرویس می‌تواند از فرصت‌ها و نقاط قوت رایانش ابری برای بهبود خدمات به مشتریان استفاده کند. بانکداری اینترنتی با استفاده از ابر خصوصی و عمومی ارائه می‌شود.

نقاط قوت رایانش ابری

۱. پاسخگویی به تقاضاهای ناخواسته
۲. انعطاف پذیری رایانش ابری به دلیل ظرفیت نامحدود آن
۳. بهبود سرویس IT برای مشتریان و سازمان‌ها
٤. صرفه‌جویی در هزینه و کاهش میزان هزینه‌های خرید، نگهداری و بروزرسانی ابزارها، نرم‌افزار و مناطق توسعه و انتقال هزینه‌ها به عرضه‌کنندگان ابری
۵. کاهش هزینه زیرساخت‌ها و هزینه‌های عملیاتی نگهداری و همچنین کاهش هزینه‌های مربوط به سرورها
٦. رایانش ابری یک انگیزه مهم در شیوه نوآوری و خلاقیت است.

نقاط ضعف رایانش ابری

۱. امنیت مهم‌ترین موضوع در چالش‌های رایانش ابری است.
۲. کاربران برای دسترسی به داده‌ها وابسته به اینترنت هستند. عدم دسترسی به اینترنت مانعی برای سرویس‌های ابری محسوب می‌شود. دسترسی به اینترنت از بستر ارتباطی پایدار مهم است.
۳. ماهیت ابر می‌تواند متفاوت باشد در این صورت اگر مشتری سرویس با تحریم‌هایی مواجه باشد، دسترسی به داده‌ها دچار ابهام می‌شود.
٤. حریم خصوصی
آسیب ناشی از مسائل امنیتی، حریم خصوصی و عدم دسترسی به سرویس موجب آسیب به اعتبار مشتری و سازمان می‌شود. به دلیل خطرات مربوط به فناوری رایانش ابری، در نظر گرفتن اولویت رایانش ابری مهم است.
۵. مدل‌های رایانش ابری برای نرم‌افزار و نوع خدمات، موجب کاهش احتمال سفارشی شدن می‌شود.
٦. تغییر در سطوح سرویس منجر به عدم تحویل سرویس می‌شود. از این‌رو در انتخاب عرضه-کننده، شهرت، اعتبار، سابقه و مسئولیت‌پذیری مهم است.
۷. پرداخت مشتریان بر اساس سرویس‌های ارائه شده منجر به تغییر بودجه IT سازمانی می‌شود. این تغییر موجب چالش سازمان در فرایندهای تخمین بودجه می‌شود.
۸. مسائلی نظیر تحریم موجب عدم دسترسی به اطلاعات سازمانی می‌شود.

فرصت‌های رایانش ابری

۱. تسهیم زیرساخت‌های فناوری اطلاعات توسط

رایانش ابری موجب کاهش هزینه‌های سرمایه IT در کشورهای توسعه یافته‌ای می‌شود که دارای ظرفیت سرمایه‌گذاری پائین می‌باشند.

۲. نرم‌افزار ارائه شده توسط فناوری ابری موجب کاهش هزینه‌های نرم‌افزار و زیرساخت و بهبود مصرف نرم‌افزار می‌شود.

۳. نرم‌افزار به عنوان سرویس در یادگیری الکترونیک و آموزش الکترونیک منجر به بهبود در کیفیت سرویس آن‌ها می‌شود.

٤. دسترسی کاربران به محتوای آموزشی از مراکز آموزشی

٥. رایانش ابری بستری امن برای دولت الکترونیک است که منجر به سرویس با کیفیت بالا در دولت الکترونیک و رأی دهی الکترونیک می‌شود.

٦. رایانش ابری نقش مهمی در انجام دورکاری دارد.

۷. ابر سبز

تهدیدهای رایانش ابری

۱. به دلیل رقابت در ارائه قیمت پائین و کیفیت بالا، جایگزینی با عرضه‌کننده‌های دیگر از تهدیدهایی است که بر رایانش ابری اثر می‌گذارد.

۲. تغییرات در فرهنگ IT در سازمان‌ها

۳. نبود استانداردهای مناسب برای پیاده‌سازی رایانش ابری

٤. عدم دسترسی ناشی از تحریم‌ها

نقاط قوت بانکداری اینترنتی

۱. سرویس‌های ۲٤ ساعته از هر زمان و مکان و سطوح بالای دسترسی برای کاربران

۲. سهولت بکارگیری بانکداری اینترنتی توسط کاربران

۳. کاهش کار کاغذی

٤. فرصت‌های بانکداری اینترنتی شیوه‌هایی را برای سازمان‌ها در راستای ارائه روش‌های نوین و بهبود سطح خدمات، سود و کارایی ارائه می‌کند.

نقاط ضعف بانکداری اینترنتی

۱. آسیب‌پذیری اینترنتی نظیر رد خدمات، نشت اطلاعات، از دست رفتن اطلاعات محرمانه، حملات ویروسی، جعل کارت اعتباری، سرقت اطلاعات حساب و...

۲. اعتماد به سرویس‌های بانکداری اینترنتی به دلیل عدم مواجه چهره به چهره و تعاملات متقابل سخت است. نگهداری سایت و زیرساخت برای ارائه خدمات نیز باید در نظر گرفته شود.

فرصت‌های بانکداری اینترنتی

۱- ایجاد اعتماد به برندهای تجاری

۲- ایجاد محصول و سرویس جدید

۳- پیش‌بینی رفتار خرید مشتری

٤- سودآوری

٥- خدمات ارائه شده و بانکداری اینترنتی منجر به تجربه جدید کاربر و مشارکت کاربر در سرویس‌های بانکداری اینترنتی می‌شود.

تهدیدهای بانکداری اینترنتی

همه تهدیدها در رایانش ابری و اینترنتی در سرویس بانکداری اینترنتی رخ داده است. نشت اطلاعات، تحریم‌ها و مسائل امنیتی موجب به خطر افتادن امنیت کاربران و دسترسی به سرویس می‌شود که در نهایت زیان زیادی را در پی دارد.

۲- نتیجه‌گیری

بانکداری اینترنتی و رایانش ابری از بستر اینترنتی برای مشتریان استفاده می‌کنند. رایانش ابری موجب تسهیم اطلاعات نرم‌افزارها و زیرساخت‌ها از طریق اینترنت می‌شود. با استفاده از وب‌سایت‌ها، بانکداری اینترنتی خدمات مختلفی برای مشتریان ارائه می‌کند. رایانش ابری با کاهش هزینه‌های IT، سود زیادی برای سیستم بانکداری و مشتریان به وجود آورده است.

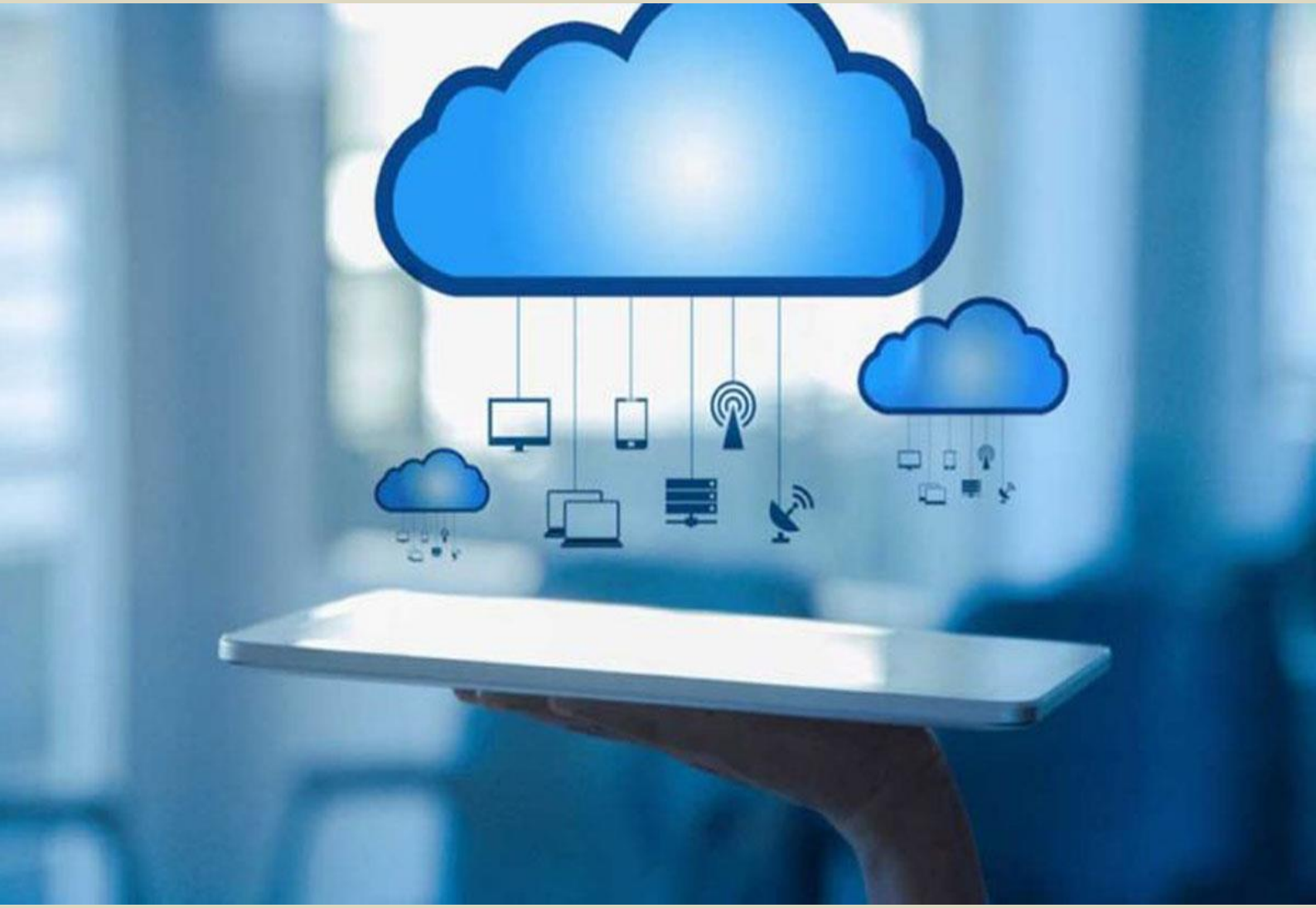
روش دلفی فازی روشی بر اساس روش دلفی و تئوری فازی است. مراحل دلفی فازی شامل:

- انتخاب کارشناس
- تهیه پرسش‌نامه
- دست یابی به تحلیل و نظرات کارشناس
- در صورتیکه اجماع خوبی وجود داشته باشد، فرآیند دلفی فازی به پایان می‌رسد.

منبع:

M. Hosseini, E. Fathi, "Internet Banking, Cloud Computing: Opportunities, Threats", Journal of Information Systems and Telecommunication, Vol. 2, No. 2

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



آشنایی کلی با موضوع اسکان موقت (Temporary Accommodation) در حوادث طبیعی و غیرطبیعی

مقدمه

در سراسر تاریخ حیات بشر، جان و مال انسان‌ها همواره دستخوش حوادث طبیعی و سوانح پیش‌بینی نشده و بعضی مواقع هولناک و مرگ‌بار بوده است. خاطرات و آثار خسارات ناشی از برخی مخاطرات طبیعی مانند زلزله، سیل و طوفان همانند خاطرات جنگ‌های مصیبت‌بار و خونین در تاریخ بشر جاودان مانده‌اند.

در اکثر حوادث طبیعی و غیر طبیعی محل زندگی افراد تخریب و بسیاری از مردم بی‌خانمان می‌شوند. در چنین شرایطی مدیریت بحران و اسکان موقت خسارت دیده‌ها بر اثر حادثه یکی از نیازهای اساسی مردم و وظیفه اصلی دولتمردان است. کشور پهناور ایران نیز از وقوع این حوادث مستثنی نبوده و پیوسته در معرض خطرات و حوادث طبیعی گوناگون قرار داشته و متحمل زیان‌ها و خسارات هنگفت ناشی از آن‌ها شده است، وقوع حوادثی همچون زلزله، سیل، جنگ، بیماری‌ها و ... در سال‌های اخیر در ایران موجب وارد شدن خسارت‌های جانی به هموطنان عزیز از یک طرف و تخریب زیرساخت‌ها کشور، ابنیه و تأسیسات خدماتی شهرها و اموال مردم از طرف دیگر شده است. شهرهای بزرگ ایران در نواحی با مخاطرات طبیعی بالا قرار گرفته‌اند. این امر به ویژه در شهر تبریز و در صورت وقوع بحران تلفات جانی و مالی فراوانی به جای خواهد گذاشت. یکی از مهم‌ترین تدابیر بعد از وقوع تهدید و حادثه، انتقال به مناطق امن جهت در امان ماندن از خطرات ثانویه می‌باشد. آنچه در اینجا ضروری به نظر می‌رسد بررسی پهنه‌های فضایی مناسب

اردوگاه‌های اسکان موقت با رویکرد پدافند غیرعامل جهت ایمنی و رفاه آسیب دیدگان بعد از وضعیت اضطراری می‌باشد. بدیهی است نادیده گرفته شدن رویکرد پدافند غیرعامل و عدم توجه کافی به این متغیرها در شناسایی و انتخاب مکان‌های مناسب جهت اسکان موقت می‌تواند نتایج متصور از تصمیم‌های اتخاذ شده را با شکست مواجه کرده و موجب بروز مسائل فرهنگی، اجتماعی، امنیتی شوند.

آشنایی کلی با سبک جهانی اسکان موقت:

پس از وقوع حوادث بزرگ مانند زلزله، سیل، جنگ و ... روند بازسازی خانه‌ها به کندی صورت می‌گیرد. چادرهایی که برای اسکان موقت در اختیار زلزله‌زدگان قرار داده می‌شود نمی‌توانند تا زمان بازسازی منازل محل مناسبی برای زندگی و ادامه فعالیت‌های معمول افراد باشند. آسیب دیدگان از حوادث تا زمان بازسازی منازلشان نیازمند مسکنی با امکانات مناسب و کافی هستند. آوارگان پیش از آنکه به خانه‌هایشان بازگردند باید محل زندگی خود را ساماندهی نمایند.

مراحل اسکان؛ پل میان فاجعه و زندگی:

اسکان پس از زلزله در جهان به چهار دوره تقسیم می‌شود: سرپناه اضطراری، سرپناه موقت، اسکان موقت و اسکان دائمی یا بازگشت به منازل بازسازی شده.

۱) سرپناه اضطراری: این مرحله از زمان وقوع زمین لرزه تا چند روز پس از آن را شامل می‌شود. در این دوره، افراد در پناهگاه‌های جمعی همچون استادیوم‌های سرپوشیده، سالن‌های والیبال، پارک‌های چند منظوره، اماکن مذهبی و... به‌طور موقت اسکان داده می‌شوند یا به نزد دوستان و آشنایان خود می‌روند. در پایان این مرحله وضعیت به ثبات نسبی می‌رسد.

۲) سرپناه موقت: این مرحله چند هفته نخست پس از وقوع زمین‌لرزه را شامل می‌شود. در این دوره چادرها یا پوشش‌های پلاستیکی به‌عنوان سرپناه مورد استفاده قرار می‌گیرد. این لوازم عموماً توسط صلیب سرخ، هلال‌احمر یا نیروهای نظامی در میان زلزله‌زدگان توزیع می‌شود و در دوره‌ای که زلزله‌زدگان در این چادرها حضور دارند غذا، آب آشامیدنی و لوازم بهداشتی مورد نیاز آنان توسط نیروهای امدادی در اختیارشان قرار می‌گیرد.

۳) اسکان موقت: این مرحله اسکان نسبت به مراحل قبلی طولانی‌تر است و تا زمان بازسازی منازل زلزله‌زدگان و بازگشت آن‌ها به مسکن دائمی ادامه خواهد داشت. امکان بازگشت افراد به روال عادی زندگی در مرحله اسکان موقت فراهم می‌شود. اسکان موقت معمولاً در بناهای کوچکی صورت می‌گیرد که با استفاده از مصالح پیش‌ساخته و ظرف مدت کوتاهی ساخته می‌شوند. در مواردی که تخریب ناشی از زلزله بالاست، بازسازی خانه‌ها مستلزم صرف زمانی چند ساله است. در این مدت، استفاده از امکانات اسکان موقت برای بازسازی اجتماعی و اقتصادی نواحی زلزله زده ضروری است. امکانات اسکان موقت مناسب، زلزله‌زدگان را در برابر شرایط دشوار محیطی محافظت می‌کند، موجب تقویت احساس امنیت و ثبات در آن‌ها می‌شود و ایشان را قادر می‌سازد زندگی و فعالیت‌های روزمره را از سر بگیرند. به این ترتیب اسکان موقت در حکم پلی است که قربانیان زلزله را از شکاف حادثه می‌گذراند و به جریان زندگی عادی بازمی‌گرداند.

هدف از اسکان موقت فراهم آوردن امکان زندگی اعضای خانواده در کنار یکدیگر، برخورداری از سطح مناسبی از حریم خصوصی، بهره‌مندی از امکانات ضروری زندگی همچون محل تهیه غذا و امکانات بهداشتی است. اسکان موقت تنها ساخت مسکن موقت را شامل نمی‌شود، بلکه دسترسی به خدمات و امکانات گوناگون را نیز در بر می‌گیرد. حفظ ساختار اجتماعی منطقه و از سرگیری

فعالیت‌های اجتماعی و اقتصادی در این مرحله در اولویت قرار دارد. در آمریکا، طبق قوانین مواجهه با بلایای طبیعی، اعطای کمک‌های مالی و اجاره مسکن دائمی برای زلزله‌زدگان بهترین گزینه اسکان موقت در نظر گرفته می‌شود. ممکن است کمیته مواجهه با بلایای طبیعی به دلیل گستردگی تخریب یا هزینه اجاره مسکن، این گزینه را رد و تأسیس مرکز اسکان موقت زلزله‌زدگان را به‌عنوان راه حل جایگزین پیشنهاد کنند. در این صورت خانه‌های پیش‌ساخته (مسکن پیش‌ساخته آماده، خانه‌های صنعتی و ...) برای اسکان موقت قربانیان به کار گرفته می‌شوند. تصمیم‌گیری در خصوص محل قرارگیری این سازه‌ها، اسکان جمعیت، ارائه خدمات عمومی و نیز برنامه‌ریزی برای تخلیه و غیرفعال سازی این مراکز بر عهده مقامات محلی است. امکانات اسکان موقت زلزله‌زدگان به‌طور میانگین به مدت ۱۸ ماه مورد استفاده قرار می‌گیرد.

برخی تجربه‌های حوادث اخیر در جهان:

پس از وقوع توفان در فیلیپین، در نوامبر ۲۰۱۳ بسیاری از منازل مسکونی به‌طور کامل تخریب شده بودند. جعبه‌های حمل نوشیدنی که اطراف آن با کیسه‌های سیمان پوشانده شد در زیر سازه‌های اسکان موقت قرار گرفت. از مصالح محلی نظیر چوب‌های بامبو و نیز لوله‌های مقوایی روکش‌دار برای تقسیم فضای داخلی استفاده شد. دیواره‌ها از حصیرهای محلی پوشانده شد و تخته سه‌لا و چوب نارگیل روی کف سازه قرار گرفت. روی پوشش ضدآب سقف نیز لایه‌ای از برگ نخل قرار گرفت.

پس از وقوع زلزله ۱۹۹۵ در کوبه ژاپن سازه‌هایی برای اسکان موقت مورد استفاده قرار گرفت که از تخته‌های سه‌لا با پوشش ضد آب در کف و سقف آن استفاده شده بود و دیواره‌های داخلی با لوله‌های مقوایی روکش‌دار پوشانده شد. از چادرهای ضدآب برای پوشاندن روی سقف سازه و میله‌های فلزی برای اتصال بخش‌ها استفاده شد. این خانه‌ها پس از گذشت ۵ سال و بعد از بازسازی مناطق آسیب‌دیده، باز شدند و به زلزله‌زدگان ترکیه اهدا شدند. در ترکیه به دلیل کمبود امکانات و کثرت افرادی که منازل خود را در زلزله از دست داده بودند، خانه‌های موقت ژاپنی تنها به نظامیان و کارمندان عالی‌رتبه اختصاص یافت. در نپال پس از وقوع زلزله سال ۲۰۱۵ سازه‌هایی مورد استفاده قرار گرفت که از قاب‌های چوبی تشکیل شده بود. داخل این قاب‌های چوبی با پاره‌های آجر پر شد و در سقف سازه نیز از لوله‌های کاغذی روکش‌دار استفاده شد. پوشش ضدآب چادر مانندی برای پوشاندن سقف و دیواره‌های سازه مورد استفاده قرار گرفت. کف سازه نیز از تخته‌های سبک محلی پوشیده شد.

خانه‌های آیکیا:

گروهی از طراحان سوئدی اقدام به طراحی سازه‌هایی برای اسکان موقت پناهندگان یا آسیب‌دیدگان بلایای طبیعی کرده‌اند که با نام «بتر شلتر» (سرپناه بهتر)، عرضه شده‌اند و از صفحات مقاومی تشکیل شده‌اند که به سادگی روی یکدیگر سوار می‌شوند و صفحات خورشیدی تعبیه شده روی سقف این سازه‌ها به تأمین انرژی مورد نیاز ساکنان کمک می‌کند. روشنایی این خانه‌ها با استفاده از لامپ‌های ال‌ای‌دی تأمین می‌شود که از برق تولید شده در صفحات خورشیدی استفاده می‌کنند. سقف این سازه‌ها بلند است و اسکلت فلزی آن‌ها به همراه صفحات مورد استفاده در سقف و دیواره‌ها در ۲ جعبه جای داده می‌شوند؛ یک گروه ٤ نفره می‌توانند ظرف مدت چند ساعت یک واحد ۱۷/۵ متر مربعی را به پایان برسانند و در و پنجره را نیز نصب کنند. این

خانه‌ها هم‌اکنون برای اسکان آوارگان عراقی در این کشور مورد استفاده قرار می‌گیرند.

برخی حوادث اخیر در ایران:

۱) زمین‌لرزه ۱۳۹۶ کرمانشاه به بزرگی ۷٫۳ در مقیاس بزرگای گشتاوری شامگاه یکشنبه ۲۱ آبان ۱۳۹۶ در نزدیکی ازگله، استان کرمانشاه در نزدیکی مرز ایران و عراق در ۳۲ کیلومتری جنوب غربی شهر حلبچه عراق ایران رخ داد. در این حادثه حدود ۶۰۰ نفر از هموطنان جان خود را از دست داده و نزدیک به ۸۰ هزار نفر متحمل آسیب جسمی و خسارات مالی شدند. در جریان اسکان موقت در زلزله کرمانشاه بیشتر از کانکس و چادرهای موقت برای اسکان زلزله‌زدگان استفاده گردید.

۲) زلزله ایی در ساعت ۵:۲۶ دقیقه بامداد جمعه ۵ دی ماه ۱۳۸۲ در بم زلزله‌ای بعد از چند پیش‌لرزه که شب قبل و ساعتی قبل از لرزه اصلی حس شده بود، درست در کنار شهر بم و روی گسل بم رخ داد، با وجودی که بعضی از مردم از شب قبل کمابیش به خاطر چند پیش لرزه بیدار مانده بودند، ولی عملاً حدود یک سوم از جمعیت شهر بم (حدود ۳۰ هزار نفر) در این رخداد کشته شدند. در زلزله بم به علت عدم توجه کافی نظامات فنی و اجرایی (مبحث ۲۱ مقررات ملی ساختمان) و اصول پدافند غیرعامل اکثر ساختمان‌های اداری شهر بم و ارگ بم بزرگترین سازه گلی جهان با قدمت ۲۵۰۰ سال تخریب شدند. اسکان موقت در این حادثه بیشتر با استفاده از چادرهای هلال‌احمر انجام گرفته است.

۳) با توجه به بارندگی اخیر فروردین ۱۳۹۸ و وقوع سیل در چند استان کشور (گلستان، فارس، خوزستان، لرستان، کهکیلویه و بویر احمد و ...) در مرحله اول حفظ جان افراد و نجات مردم گرفتار در سیل و در مرحله بعد اسکان موقت در کانکس، مدارس و چادرهای هلال‌احمر پیش بینی شده و در مرحله بعد بازسازی مورد توجه می باشد.

نتیجه‌گیری:

رعایت نکات ایمنی و اجرای اصول پیشگیرانه از وقوع حوادث و کاهش خسارت ناشی از حوادث طبیعی و غیر طبیعی امری اجتناب پذیر می‌باشد. در کنار اقدامات پیشگیرانه قبل از بحران، در زمان وقوع بحران حفظ خونسردی، همکاری با مسئولین مدیریت بحران و متولیان محلی، پرهیز از هرگونه بزرگ نمایی و سیاه نمایی، ... از عواملی هستند که می‌توانند در اتخاذ تصمیمات درست و مؤثر و مهار بحران مؤثر واقع شوند.

منابع:

۱) دکتر مازیار حسینی؛ کتاب مدیریت بحران؛ موسسه نشر شهر، ۱۳۸۷
۲) مهدی مقیمی؛ مقاله بررسی کلی اسکان موقت کوتاه مدت در ایران، دومین کنفرانس مدیریت بحران ۱۳۹۱

ماهری (رئیس گروه طرح و اجرا پدافند غیر عامل استان) و خوش روا (کارشناس امریه)

بیوتروریسم

بیوتروریسم عبارت است از منتشر کردن عوامل بیولوژیکی یا سمی باهدف کشتن و یا آسیب رساندن به انسان‌ها و یا حیوانات و گیاهان به‌منظور ایجاد رعب و وحشت در جامعه و تن دادن به خواسته‌های آن‌ها.

بیوتروریسم انواع مختلفی دارد و می‌تواند از طریق محیط زیست، امنیت جمعی افراد و امنیت زنجیره غذایی و کشاورزی و اقتصادی و دارویی و پزشکی به جامعه لطمه وارد کند. زمینه‌های پزشکی و کشاورزی امروزه از اهداف عمده بیوتروریسم محسوب می‌شوند.

سلاح‌های بیولوژیکی پزشکی (عوامل بیماری‌زای مقاوم به درمان)

پیشرفت در زمینه علوم سلولی و مولکولی، مهندسی ژنتیک و بیوتکنولوژی از طرفی نگرانی از بابت ایجاد بیماری‌ها را کمتر کرده ولی از طرفی دیگر توان بالای علمی در زمینه دستکاری های ژنی عوامل بیماری‌زا، به ساخت سلاح‌های بیولوژیکی کمک کرده و احتمال تولید پاتوژنهایی که خصوصیات کاملاً منحصر بفردی دارند جامعه بشری را از طریق الحاق ژن مقاومت به آنتی بیوتیک و یا الحاق ژن بیماری‌زایی شدیدتر، احتمال ابتلا به اپیدمی‌های بسیار بزرگ را در آینده ممکن ساخته است.

اگروتروریسم (بیوتروریسم کشاورزی):

بطور کلی هر عاملی که باعث تخریب اکوسیستم، کاهش بازدهی محصول دامی و گیاهی، پخش و شیوع بیماری به‌وسیله احشام یا محصولات شود و امنیت زنجیره غذایی را به خطر بیاندازد، اقدام اگروتروریستی به حساب می‌آید

که این خسارات عواقب اقتصادی و اجتماعی و روانی بسیاری در آن جامعه باقی خواهد گذاشت. از بیوتروریسم می‌توان علیه افراد جامعه با استفاده از روش‌های گوناگون برای ضربه زدن به محصولات کشاورزی، کشوری را مورد حمله بیوتروریسی قرار دهند.

بیوتروریسم از طریق آسیب رساندن به محیط زیست و اکوسیستم

بحث محیط زیست ارتباط مستقیم بر سلامتی جامعه دارد چرا که هرگونه اثر تخریبی بر محیط زیست اثر زیان‌بار بر حیات انسانی دارد و هرگونه اختلال در عناصر سازنده زیست بوم‌ها مثلاً تغییر در جمعیت حشرات و حیوانات یا گیاهان آن منطقه منجر به تهدیدی برای زندگی انسان و سایر موجودات آن محیط خواهد شد.

بیوتروریسم با هدف سلامتی انسان

در مورد کشورهایی که غذای اصلی مردم محصول خاصی (مثلاً برنج و گندم) است، دشمن می‌تواند با دستکاری ژنتیکی در گیاهان، محصولات آن گیاهان را عواملی برای ایجاد بیماری‌ها از جمله سرطان، بدخیمی‌های لاعلاج، بیماری‌های ناشناخته نوظهور، مانند اوتیسم و آلزایمر و افزایش ناباروری و نازایی کند

تغییرات و دستکاری ژنتیکی فقط مختص ژنوم گیاه و جانوران نیست!

روزنامه روسی "کومرسانت (Kommersant)" در ماه می ۲۰۰۷ با انتشار گزارشی اعلام نمود که دولت روسیه صادرات هر نوع نمونه بیولوژیکی انسانی به خارج از کشور را ممنوع اعلام نموده است. بر اساس این گزارش، دلیل ممنوعیت فوق ارائه یک گزارش محرمانه از جانب سرویس مخفی امنیتی روسیه بود که بیان می‌داشت سازمان‌های غربی در حال انجام آزمایشات بر روی "بیوتسلیحات ژنتیکی" هستند که می‌تواند مردم روسیه را مورد هدف قرار دهد. در گزارش مذکور سازمان‌های مختلف آمریکایی از جمله سازمان حفاظت محیط زیست و منابع طبیعی امریکا نام برده شده بودند.

از دیگر مواردی که برای سلامت انسان نگران کننده است وجود ژنی بنام VI است که درRoundup-Ready soybeans و در ذرت MON810 دیده شده که باعث تغییرات ناخواسته فنوتیپی و بیوشیمیایی زیادی در موجودات شده است.

اگر استفاده از بیوتکنولوژی بدون ملاحظات ایمنی و ارزیابی مخاطرات در نظر گرفته شوند، علاوه بر تهدید زندگی انسان‌ها و جوامع انسانی، تهدیدی جدی برای گیاهان و حیوانات ساکن یک اکوسیستم می‌باشد. مثلاً عوامل بیماری‌زای حیوانی و یا مشترک بین انسان و حیوان که دچار دستکاری ژنتیکی شده‌اند (پلاگ، تولارمی، انتراکس) بعلاوه بیماری‌هایی مثل تب برفکی، طاعون گاوی و بروسلوز بطور بالقوه تهدیدی برای دام و حیات‌وحش و جمعیت گونه‌های در معرض خطر انقراض هستند. اخیراً هم شاهد خسارات فراوان ناشی از تب برفکی در برخی کشورها بودیم که عده‌ای بر این باور بودند که فراگیر شدن این بیماری می‌تواند عامدانه و به قصد ضربه زدن به اقتصاد کشور باشد.

تغییر نظم ژنتیکی منطقه، از بین رفتن زمین‌های کشاورزی و تبدیل شدن آن‌ها به زمین‌های بایر به دلیل استفاده از علف‌کش‌های قوی، از بین رفتن حیات‌وحش، بالارفتن سطح بیماری در میان مردم یک منطقه، همگی می‌تواند بطور برنامه‌ریزی‌شده و با هدف برهم زدن نظم یک کشور از طریق ضربه‌های وارده به بخش‌های مختلف آن، انجام گیرد.

با روشن شدن ابعاد جدید بیوتروریسم و خطرات پیش رو ناشی از آن، این پدیده اخیراً در سطح وسیعی در

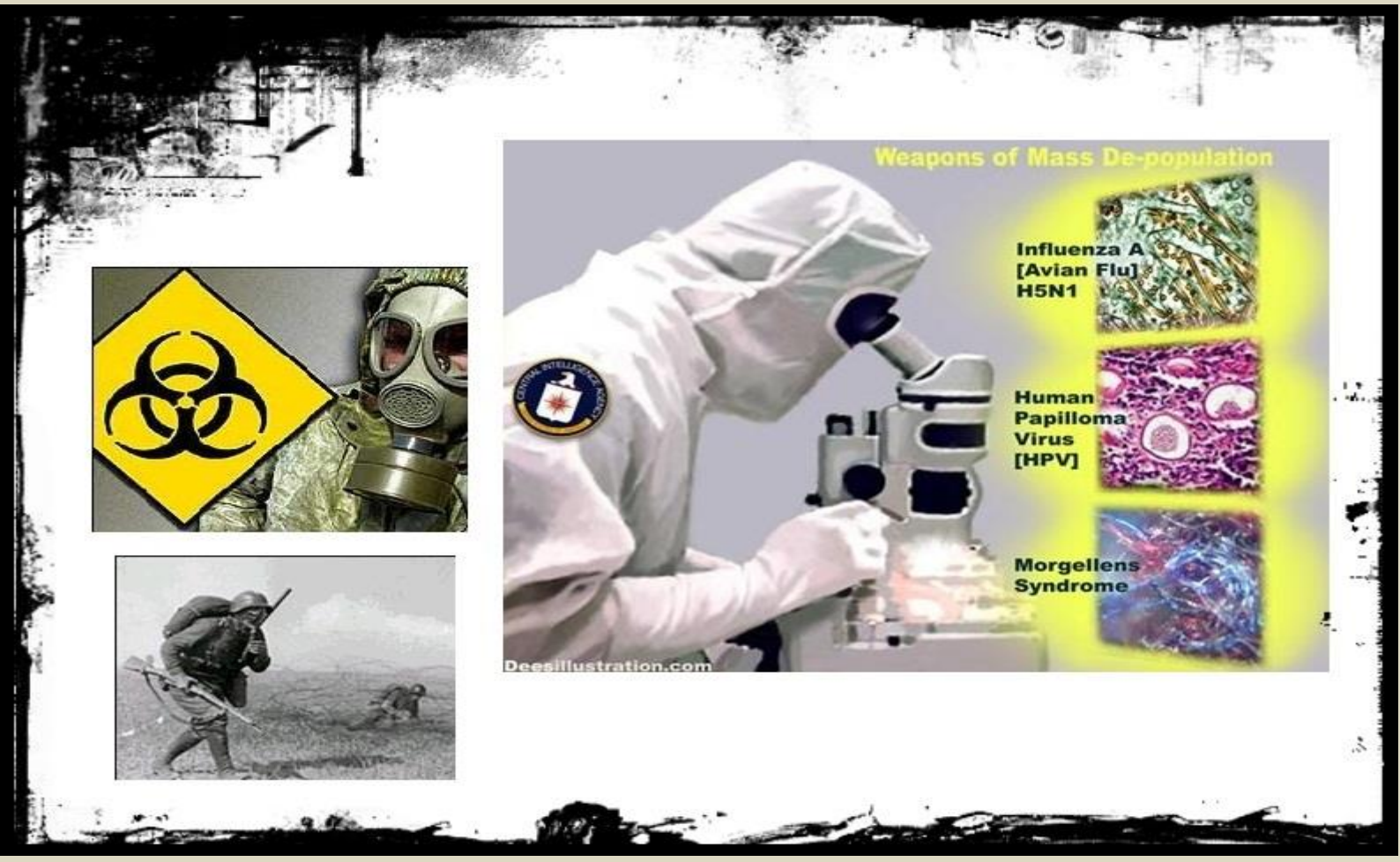
حوزه‌های پزشکی، بهداشتی، سیاست‌گذاری‌های بلندمدت دفاعی و سطوح امنیت ملی کشورها مطرح شده است. باید دانست که پیشگیری از وقوع عملیات بیوتروریستی مهم‌تر و عاقلانه‌تر است. کاملاً مشهود است که مقابله با عملیات بیوتروریستی پس از وقوع مستلزم صرف هزینه و وقت، داشتن تجهیزات و امکانات مورد نیاز برای مقابله با آن است.

از این رو پدافند غیرعامل به عنوان روشی صلح آمیز و پیشگیرانه بدون استفاده از سلاح قادر است ضمن رصد تهدیدات جنگ نوین به خصوص تهدیدات زیستی، زیرساخت‌ها و توانمندی مقابله با این تهدیدات را در کشور چنان افزایش دهد که آسیب پذیری به آن کاهش جدی یابد. مهم‌ترین مسئله در مقابله با بحران‌ها مدیریت سریع و کارآمد است.

منبع:

http://virlan.com

رحیم قدیمی – کارشناس ناظر تخصصی پدافند غیر عامل



اطلاعات کاربران تپسی هک شد

موسسه امنیتی Security Discovery اعلام کرد که توانسته با دسترسی به پایگاه داده یکی از سرویس‌های تاکسی اینترنتی در ایران به اطلاعات بیش از ۶,۷ میلیون کاربر ایرانی دست پیدا کند. براساس تصاویر منتشر شده از سوی این موسسه، این اطلاعات شامل، نام و نام خانوادگی، شماره تلفن همراه و همچنین کد ملی ده رقمی کاربران این سرویس اینترنتی می‌شود. آذری جهرمی، وزیر ارتباطات در صفحه رسمی خود در توئیتر اعلام کرد که دسترسی غیرمجاز هکرها به این اطلاعات کاربران صحت دارد و بررسی‌های تکمیلی از این موضوع توسط مرکز ماهر در حال انجام است. اگرچه در متن توئیت وی نمی‌توان اثری از نام این سرویس حمل و نقل پیدا کرد، اما آذری جهرمی ساعتی پس از انتشار این توئیت در پاسخ به نظر یکی از کاربران اعلام کرد که پایگاه داده‌ای که توسط این هکرها مورد حمله قرار گرفته است مربوط به شرکت تپسی می‌شود.

آسیب‌پذیری بحرانی WinRAR

آسیب‌پذیری CVE-۲۰۱۸-۲۰۲۵۰ در نرم‌افزار WinRAR در حال تبدیل شدن به یکی از پراستفاده‌ترین نقص‌های امنیتی ماه‌های اخیر است. مایکروسافت نیز اخیراً گزارشی را در ارتباط با سوء استفاده از این آسیب‌پذیری در حملات مختلف، منتشر کرده است.

به گزارش معاونت بررسی مرکز افتا، آسیب‌پذیری برنامه پرطرفدار WinRAR یک نقص اجرای کد از راه دور است که به مدت ۱۹ سال در این نرم‌افزار وجود داشته است. پس از انتشار کد اثبات مفهومی این آسیب‌پذیری، حدود ۱۰۰ اکسپلویت مختلف با بهره‌گیری از این نقص توسط مجرمین سایبری ایجاد شده است. سوءاستفاده از این آسیب‌پذیری از طریق فایل‌های فشرده با پسوند ACE انجام می‌شود که با انتشار نسخه beta ۵،۷۱ پشتیبانی از این پسوند متوقف شده است .گزارش مایکروسافت از حملات انجام شده توسط این آسیب‌پذیری، هشداری است برای سازمان‌هایی که هنوز نسخه WinRAR خود را بروزرسانی نکرده‌اند.

توصیه می‌شود تا فایل‌های ACE تحت هیچ شرایطی باز نشوند و برنامه WinRAR بروزرسانی شود. باید توجه شود که مهاجمین می‌توانند برای فریب کاربر پسوند فایل‌های فشرده را تغییر دهند.

آلوده‌شدن هزاران کاربر اندروید در پی حملات Roaming Mantis

کارشناسان امنیتی کسپرسکی اعلام کردند هزاران کاربر در ماه گذشته مورد هدف حملات بدافزاری Roaming Mantis قرار گرفتند تا اطلاعات آنان جمع آوری شود. آخرین موج حملات بدافزار Roaming Mantis بر گسترش لینک‌های فیشینگ از طریق پیامک تمرکز دارد که قربانیان این حملات در کشورهای روسیه، ژاپن، هند، بنگلادش، قزاقستان، آذربایجان، ایران و ویتنام قرار دارند. کاربران اندروید توسط بدافزارهایی آلوده شدند که Trend Micro آن را با نام XLoader و McAfee با نام MoqHao شناسایی می‌کنند. همراه با تکنیک دستکاری DNS که در گذشته انجام شده بود، مهاجمین با استفاده از روش فیشینگ جدیدی، از صفحات فرود جدیدی برای هدف قرار دادن دستگاه‌های iOS استفاده کردند که باعث نصب پیکربندی مخرب در iOS می‌شود. این پیکربندی باعث باز شدن سایت فیشینگ در مرورگر دستگاه‌های هدف می‌شود تا اطلاعات قربانیان جمع‌آوری شوند. در اواخر ماه فوریه ۲۰۱۹، کارشناسان یک URL را شناسایی کردند که مهاجمین از آن برای تغییر DNS مسیریاب استفاده کردند. این حمله تحت شرایطی موفق عمل می‌کند که هیچ احرازهویتی برای کنترل پنل مسیریاب وجود نداشته باشد، دستگاه یک نشست ادمین برای پنل مسیریاب داشته باشد و نام کاربری و گذرواژه پیش‌فرض برای مسیریاب تعیین شده باشد. کارشناسان کسپرسکی هزاران مسیریاب را کشف کردند که از این طریق DNS آن‌ها به آدرس‌های مخرب تغییر یافته است. این نوع حمله توسط فایل sagawa.apkانجام شده است. کارشناسان معاونت بررسی مرکز افتا تأکید می‌کنند برای جلوگیری از نفوذ و آلودگی حملات بدافزار Roaming Mantis ، شناسه و گذرواژه‌های پیش‌فرض تغییر یابد و وصله‌های امنیتی منتشر شده، اعمال شود این کارشناسان همچنین به کاربران اندروید توصیه می‌کنند به هیچ وجه فایل‌های APK را از منابع نامعتبر دانلود نکنند و کاربران iOSنیز از نصب پیکربندی ثالث نامعتبر خودداری کنند.

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

شرکت مایکروسافت آسیب‌پذیری‌های متعددی ازجمله دو آسیب‌پذیری روز صفرم ویندوز که در حملات گسترده مورد سوءاستفاده قرار گرفته‌اند، رفع کرد. در این به‌روزرسانی، بیش از ده آسیب‌پذیری اجرای کد از راه دور و افزایش امتیاز که بر ویندوز و مرورگرهای مایکروسافت تأثیر می‌گذارند، وصله شدند. ۱۵ به‌روزرسانی منتشرشده، در مجموع ۷۴ آسیب‌پذیری منحصربه‌فرد در ویندوز، اینترنت اکسپلورر، Edge، آفیس، SharePoint و Exchange را پوشش می‌دهند.

سیسکو در هفته‌ی اول ماه آوریل اعلام کرد وصله‌های امنیتی جدیدی برای مسیریاب‌های RV320 و RV325 منتشر ساخته است که آسیب‌پذیری‌هایی که طی مدت دو ماه هدف حمله قرار گرفته‌اند را به‌درستی برطرف می‌سازد. هر دوی این آسیب‌پذیری‌ها، مسیریاب‌های واسط مدیریتی مبتنی بر وب Small Business RV320 و Rv325 Dual Gigabit WAN VPN را تحت تأثیر قرار می‌دهند و به گفته‌ی سیسکو به طور گسترده‌ای در حملات مورد سوءاستفاده قرار گرفته‌اند.

بیش از ۹۶۰۰ مسیریاب تحت تأثیر این دو آسیب‌پذیری قرار داشتند و تمامی آن‌ها به دلیل وصله‌های ناقص همچنان در معرض آسیب باقی ماندند. پس از انتشار وصله‌های امنیتی توسط سیسکو، هکرها شروع به سوءاستفاده از نقص‌های این مسیریاب‌ها کردند. پس از انتشار کد اثبات مفهوم برای نقص‌های امنیتی مسیریاب‌های RV320 و RV325، هکرها شروع به اسکن اینترنت کردند تا دستگاه‌های آسیب‌پذیر را بیابند و آن‌ها را در معرض خطر قرار دهند.

با جستجو در موتور جستجوی Shodan برای یافتن مسیریاب‌های آسیب‌پذیر، امکان یافتن ده‌ها هزار دستگاه به صورت آنلاین وجود دارد. کار شناسایی شده در پژوهشی در Bad Packets به نام Troy Mursch، دستگاه‌های آسیب‌پذیر را با استفاده از موتور جستجوی BinaryEdge مورد جستجو قرار داد و ۹۶۵۷ دستگاه را در معرض خطر آنلاین یافت (۶۲۴۷ مسیریاب Cisco RV320 و ۳۴۱۰ مسیریاب Cisco RV325).

این دو آسیب‌پذیری مسیریاب‌های مذکوری که سخت‌افزار نسخه‌های ۱,۴,۲,۱۵ تا ۱,۴,۲,۲۰ را اجرا می‌کنند تحت تأثیر می‌گذارند. سیسکو این آسیب‌پذیری‌ها را با انتشار نسخه‌ی ۱,۴,۲۲ برطرف ساخته است.

گوگل در به‌روزرسانی ماه مارس سال ۲۰۱۹ خود، ۱۱ نقص بحرانی را وصله کرده است. از میان این ۱۱ نقص بحرانی، گوگل سه نقص اجرای کد راه دور، شامل دو آسیب‌پذیری بحرانی چارچوب رسانه‌ای که Android (Nougat) 7.0 و نسخه‌های پس از آن را تحت تأثیر قرار می‌دهد را وصله کرده است.

اوراکل نیز در بروزرسانی امنیتی فروردین ماه خود، ۲۹۷ آسیب‌پذیری در محصولات مختلف این شرکت را رفع کرده است. به نقل از پایگاه اینترنتی GBHackers، محصولاتی که بروزرسانی برای آن‌ها منتشر شده است شامل Oracle Supply Chain Products ،JD Edwards ،MySQL ،Java SE ،Enterprise Manager، Oracle Banking Platform ،Virtualization ،Retail Applications ،E-Business Suite ،Database و غیره هستند.

شرکت VMware چندین بروزرسانی را برای رفع پنج آسیب‌پذیری بحرانی در محصولات vSphere ESXi، VMware Workstation Pro / Player وVMware Fusion Pro / Fusion منتشر کرده است.

به منظور رفع این آسیب‌پذیری‌ها، نسخه‌های زیر منتشر شده‌اند:

- نسخه‌های ۶،۰،۰، ۶،۵،۰ و ۶،۷،۰ برای محصول ESXi
- نسخه‌های ۱۵،۰،۴ و ۱۴،۱،۷ برای محصول VMware Workstation (Pro و Player)
- نسخه‌های ۱۱،۰،۳ و ۱۰،۱،۶ برای محصول Fusion

VMware همچنین یک آسیب‌پذیری سرقت نشست راه دور با شناسه CVE-۲۰۱۹-۵۵۲۳ در VMware vCloud Director for Service Providers را نیز برطرف کرده است. این آسیب‌پذیری در نسخه ۹،۵،۰،۳ محصول vCD رفع شده است.

Adobe و SAP نیز به‌روزرسانی‌های امنیتی مربوطه خود را منتشر کردند. Adobe هفت به‌روزرسانی را برای رفع ۴۳ آسیب‌پذیری در محصولات خود مانند Adobe Reader، Acrobat، AIR، Flash و Shockwave منتشر کرد.

Wireshark نیز سه به‌روزرسانی را برای حل ده آسیب‌پذیری منتشر کرد. Wireshark یکی از ابزارهای نادیده گرفته‌شده‌ی IT است که می‌تواند خطر قابل توجهی را برای محیط اطراف کاربر ایجاد کند.

با توجه به اهمیت آسیب‌پذیری‌های ذکرشده، به‌روزرسانی این محصولات برای رفع نقایص موجود امری ضروری است و به کاربران توصیه می‌شود تا هرچه سریع‌تر وصله‌های منتشرشده را اعمال کنند.

گزارش کسپرسکی در مورد آسیب‌پذیری ۲۰ درصد از سیستم‌های کنترل صنعتی نسبت به نقص‌های بحرانی

طبق گزارش منتشر شده توسط کسپرسکی درباره تهدیدات سیستم‌های اتوماسیون صنعتی در نیمه دوم سال ۲۰۱۸، بیشترین تعداد آسیب‌پذیری‌ها، سیستم‌های کنترل صنعتی را تحت تأثیر قرار می‌دهند که فرایندهای تولید در سازمان‌های مختلف، در بخش انرژی و بخش تأمین منابع آب را کنترل می‌کنند. همچنین، سیستم‌های کنترل صنعتی که در حوزه کشاورزی و صنایع شیمیایی استفاده می‌شوند نیز آسیب‌پذیر هستند. بر اساس گزارش کسپرسکی، بردارهای تهدید اصلی این سیستم‌ها اینترنت (۲۶،۱ درصد)، رسانه‌های قابل حمل (۸،۳ درصد) و ایمیل (۴،۹ درصد) هستند. فیشینگ بیشترین بردار حمله در این سیستم‌ها بوده است و تروجان‌ها در ۲۷،۱ درصد دستگاه‌های ICS آلوده به بدافزار مشاهده شده‌اند.

در سال گذشته، کسپرسکی ۶۱ نقص امنیتی را در دستگاه‌های ICS و IoT/IIoT کشف کرد که تنها برای ۲۹ مورد آن‌ها وصله ارائه شد. از این آسیب‌پذیری‌ها، ۴۶ درصد آن‌ها منجر به اجرای کد راه دور، دسترسی غیرمجاز و حملات انکار سرویس (DoS) می‌شوند. بیشتر آسیب‌پذیری‌های دستگاه‌های ICS (۳۴۲ مورد) بدون احراز هویت و از طریق دسترسی راه دور قابل بهره‌برداری هستند.

گسترش بدافزار خطرناک Scranos در سطح جهان

بدافزار خطرناک جدیدی با نام Scranos در حال گسترش در سطح جهان است که کاربرانی که از برنامه‌های کرک شده استفاده می‌کنند را بیش از دیگران مورد هدف قرار می‌دهد. کارشناسان Bitdefender در گزارشی اعلام کردند که برخی از نرم‌افزارهای کرک شده حاوی بدافزار جدیدی با نام Scranos هستند. مهم‌ترین بخش این بدافزار یک روت‌کیت است که در داخل برنامه‌های آلوده مخفی می‌شود و باعث می‌شود بدافزار در مراحل اولیه آلودگی پایداری بوت و کنترل کامل سیستم قربانی را به دست آورد.

با اینکه Bitdefender بدافزار Scranos را یک بدافزار در حال پیشرفت توصیف کرده است که بسیاری از مؤلفه‌های آن در مراحل اولیه توسعه هستند، اما این بدافزار همچنان یک تهدید بسیار خطرناک بشمار می‌رود. این موضوع به این دلیل است که Scranos یک تهدید مدولار است و پس از آلوده کردن رایانه میزبان، برای دستورهای اضافی با سرور فرمان و کنترل (C&C) ارتباط برقرار می‌کند و سپس ماژول‌های کوچکی را برای انجام عملیات‌های مختلف دانلود و اجرا می‌کند. نکته دیگر درباره این نرم‌افزار مخرب پلتفرم‌های مورد هدف آن است که می‌تواند تمامی نسخه‌های ویندوز از XPتا ۱۰ را آلوده کند. بیشتر قربانیان Scranos کاربران ویندوزهای ۷ و ۱۰ بودند.

معرفی کتاب

پنجاه و یک نکته سودمند در حملات سایبری

در این کتاب ۵۱ نکته‌ی سودمند موجود است که با استفاده از آن‌ها می‌توانید بفهمید که چگونه از رایانه‌های خود محافظت کنید و چه نشانه‌هایی به شما می‌گویند که ممکن است اطلاعات شما تحت نفوذ قرار گرفته باشند. مطالعه‌ی این کتاب برای افراد و صاحبان تجارت ضروریست. تهدیدات سایبری دائماً در حال رشد هستند و اهدافی که پشت آن‌هاست نیز روز به روز تغییر می‌کند. جوانان نیز به صورت روز افزون در این جنایات و جرائم سایبری نقش رنگ‌تری ایفا می‌کنند .تمام انواع تجارت در خطر حملات سایبری قرار دارند و این در حالی است که آن‌ها برای محافظت از خودشان آمادگی‌های لازم را ندارند و این گونه حملات سایبری به فشارهای روحی و نیز ضررهای مالی می‌انجامند. با گذشت سال‌ها، فرآیند هک کردن – که طبق عادت آن‌ها را جرائمی تحت عنوان کد نویسی و ...می‌خوانیم – به طور کلی تغییر کرده است. علاوه بر این هکرها با بکارگیری بد افزارها، به صورت رو به افزایشی از مهندسی اجتماعی برای دستیابی به اهدافشان استفاده می‌کنند؛ بنابراین افزایش آگاهی در زمینه‌ی روش‌ها و نتایج حملات سایبری امری ضروری می‌باشد.

طرح های 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 دانش آموختگان 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.