



پدافند غیر عامل در حوزه فناوری اطلاعات و ارتباطات

دکتر محمد مردانی شهر بابک
(عضو هیأت علمی دانشگاه جامع امام خمینی (ع))

مهندس علیرضا زحلی



سرشناسه: دکتر محمد مردانی شهر بابک

عنوان و نام مؤلفین: پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات - دکتر محمد مردانی شهر بابک -

مهندس علی رضا زحلی.

مشخصات نشر: تهران، سپاه پاسداران انقلاب اسلامی، قرارگاه سازندگی خاتم الانبیاء (ص)، قرب نوح (ع)، ۱۳۹۴.

مشخصات ظاهری: ۳۵۰۰ م. مصور، جدول.

شایک: ۵۶-۰ ۵۹۲ ۶۰-۶۲۸

وضعیت فهرست نویسی: فیا

موضوع: دفاع - نیروی اطلاعات و ارتباطات - شبکه های کامپیوتری - ایران - تدابیر ایمنی.

شناسه افزوده: تهران، سپاه پاسداران انقلاب اسلامی، قرارگاه سازندگی خاتم الانبیاء (ص)، قرب نوح (ع)، ۱۳۹۴.

ردہ بندی کنگرہ: ۱۳۹۴ ۳ پ/۶ UA

۱۳۹۴ ۴ پ ۱۳۹۴

رده‌بندی دیویی: ۳۶۳/۳۵۰۹۵۵

شماره کتاب‌شناسی ملی: ۴۹۹۷۴۹۸

نام کتاب: پدافند غیرعامل در حوزه فناوری اطلاعات

مؤلفین: داکٹر محمد مردانی، شہر بانک - مهندس علی رضا حلی

وہ استادانِ فنم: دکتہ علی رضا پور اب اہم۔ - مہندس، غلامعلی م

ناش: قدار گاه سازندگ. خاتم الانباء (ص) - قرب نهج (ع)

دستور: توارکاء شاربندى سلاطین اور بیگم (ص) - عربی لوح (ح)

صفحه بندی و ویرایش: سعید قراسیانی - جعفر شعبانی مقدم

طرح جلد: محمدرضا علیمردانی

نوبت چاپ: اول

تیراڑ: ۱۰۰۰ نسخه

تاریخ انتشار: ۱۳۹۴

قیمت: ۱۲۰,۰۰۰ ریال

کلیه حقوق اعم از چاپ و تکثیر، نسخه‌برداری و سایر موارد برای قورگاه سازندگی زیست محیطی محفوظ است.

(نقل، مطالب با ذکر مأخذ و امانت است).

تهران - بزرگراه شهید عباس دوران - جنب ستاد نیروی دریایی سپاه - قرارگاه سازندگی نوح (ع)

تلفن: ۳۳۲۱۹۲۳۴-۳۵ نمابر: ۳۳۲۱۹۲۳۴ پست الکترونیکی: E-mail: Nooh@Khatam.net

تہران - پزرگراہ حکیم غرب - بعد از پزرگراہ اشرفی اصفہانی - خیابان خجستہ پور - کوچہ کاشفی نیک -

بلاک ۲ - گروه تخصصی سماوات - تلفن ۴۴۹۶۰۲۸۰-۸

فهرست مطالب

صفحه	عنوان
۱۹	پیش گفتار.....
۲۳	فصل اول - اصول و مبانی پدافند غیرعامل.....
۲۳	۱-۱- مقدمه.....
۲۳	۱-۲- تعاریف.....
۲۳	۱-۲-۱- پدافند عامل.....
۲۳	۲-۲-۱- پدافند غیرعامل.....
۲۳	۳-۲-۱- دُفعی غیر نظامی.....
۲۴	۴-۲-۱- مراکز حیاتی.....
۲۴	۵-۲-۱- مراکز حساس.....
۲۵	۶-۲-۱- مراکز مهم.....
۲۵	۷-۲-۱- استتار و اختفاء.....
۲۵	۸-۲-۱- پراکندگی.....
۲۵	۹-۲-۱- تفرقه و جابجایی.....
۲۶	۱۰-۲-۱- استتار، اختفاء و ماکت فریبنده.....
۲۶	۱۱-۲-۱- فریب.....
۲۶	۱۲-۲-۱- مقاوم سازی و استحکامات.....
۲۶	۱۳-۲-۱- اعلام خبر.....
۲۷	۱۴-۲-۱- مکان یابی.....
۲۸	۱۵-۲-۱- مواد جاذب هوشمند.....
۲۸	۱۶-۲-۱- ماهواره سنجش از راه دور.....
۲۸	۱۷-۲-۱- منعکس کننده های زاویه ای (گوشه دار).....
۲۹	۱۸-۲-۱- فرستنده های الکترونیکی فریب (طعمه ها).....
۲۹	۳-۱- اهداف پدافند غیرعامل.....
۳۰	۴-۱- اصول و ملاحظات پدافند غیرعامل.....
۳۰	۱-۴-۱- اقدامات اساسی دفاع غیرعامل.....
۳۱	۲-۴-۱- ملاحظات پدافند غیرعامل.....

۳۲	۵-۱- رویکرد جامع به مقوله پدافند غیرعامل
۳۴	۶-۱- جهت‌گیری کلان پدافند غیرعامل فاوای کشور
۳۷	فصل دوم - تعاریف و مفاهیم پدافند غیرعامل در حوزه سایبری (پدافند سایبری)
۳۷	۱-۲- تعاریف
۳۷	۱-۱-۲- فضای سایبری
۳۷	۲-۱-۲- آسیب‌پذیری سایبری
۳۷	۳-۱-۲- تهدیدات سایبری
۳۷	۴-۱-۲- جنگ سایبری
۳۸	۵-۱-۲- منشأ جنگ سایبری
۳۸	۶-۱-۲- پداند سایبری
۳۸	۲-۲- آشنایی با مفهوم «نایاب» اطلاعات در جهان نوین
۴۰	۳-۲- تاریخچه، عوامل و اندیشه‌های پیدایش اینترنت
۴۲	۴-۲- روند تکامل شبکه آرپانت
۴۵	۵-۲- بررسی ارتباط پروژه اشلون و شبکه اینترنت
۴۷	۶-۲- مخاطرات و تهدیدهای ناشی از پدیده اینترنت
۵۲	۷-۲- بررسی اهداف و انگیزه‌های شیوع بدافزارنویسی
۵۵	۱-۷-۲- سازمان‌های انتظامی و قضایی
۵۵	۲-۷-۲- سازمان‌های امنیتی و اطلاعاتی
۵۶	۸-۲- کارکرد پنهان دهکده جهانی
۵۷	۱-۸-۲- بدافزار فانوس جادویی
۵۸	۲-۸-۲- همکاری‌های رسمی با مراکز و شرکت‌های حوزه فاوا
۶۱	فصل سوم - امنیت در فضای تبادل اطلاعات
۶۱	۱-۳- مقدمه
۶۱	۲-۳- منظور از امنیت چیست؟
۶۲	۱-۲-۳- در چه مرحله‌ای باید به مقوله امنیت پرداخت؟
۶۲	۲-۲-۳- جرایم فضای تبادل اطلاعات چیست؟
۶۲	۳-۲-۳- قانون جرایم رایانه‌ای در جمهوری اسلامی ایران

۶۳	۳-۳- ماهیت جنگ اطلاعات
۶۴	۳-۳-۱- سابقه جنگ اطلاعات
۶۴	۳-۳-۲- انواع جنگ افزار اطلاعاتی
۶۸	۳-۳-۳- تأثیر جنگ افزارهای اطلاعاتی از ابعاد گوناگون
۷۳	فصل چهارم - معرفی و بررسی استانداردهای فناوری اطلاعات و ارتباطات
۷۳	۴-۱- مقدمه
۷۳	۴-۲- استانداردهای ISO ۱۷۷۹۹ و ISO ۲۷۰۰۱
۷۵	۴-۳- استاندارد NIST ۸۰۰
۷۷	۴-۴- استانداردهای FIPS
۸۱	فصل پنجم - امنیت نرم افزاری رایانه های شخصی
۸۱	۵-۱- مقدمه
۸۳	۵-۲- ویژگی های یک فایل رایانه ای
۸۵	۵-۲-۱- ویژگی های یک فایل
۸۵	۵-۳- انواع نرم افزار
۸۶	۵-۳-۱- نرم افزارهای سیستم عامل
۹۷	۵-۴- دلایل و روش های نرم افزاری دسترسی به اطلاعات
۱۰۳	فصل ششم - امنیت سخت افزاری رایانه های شخصی
۱۰۳	۶-۱- مقدمه
۱۰۳	۶-۲- حافظه های سخت افزاری و نقش آن در امنیت رایانه
۱۰۳	۶-۲-۱- صفحه کلید و نقش آن در امنیت رایانه
۱۰۷	۶-۲-۲- ست آپ و نقش آن در امنیت رایانه
۱۱۲	۶-۳- حافظه فقط خواندنی و نقش آن در امنیت رایانه
۱۱۲	۶-۴- نقش سخت افزارهای دیگر در امنیت رایانه
۱۱۵	فصل هفتم - آشنایی با مفاهیم تست نفوذ در نرم افزارها
۱۱۵	۷-۱- مقدمه
۱۱۵	۷-۲- تست نفوذپذیری
۱۱۷	۷-۳- متدولوژی اجرای پروژه
۱۲۲	۷-۴- خروجی ها

فصل هشتم - پدافند غیرعامل در حوزه امنیت فیزیکی و کنترل دسترسی	۱۲۵
۱-۸- مقدمه	۱۲۵
۲-۸- تجهیزات امنیت فیزیکی و کنترل دسترسی	۱۲۵
۱-۲-۸- سامانه دوربین مدار بسته	۱۲۵
۲-۲-۸- سامانه حفاظت پیرامونی	۱۲۶
۳-۲-۸- سامانه‌های کنترل، بازرسی و شناسایی	۱۲۷
۴-۲-۸- سامانه‌های اعلام و اطفاء حریق	۱۲۸
۳-۸- ملاقات پدافند غیرعامل	۱۲۸
۳-۸- امنیت فیزیکی داده‌ها و اطلاعات	۱۲۸
۲-۳-۸- امنیت فیزیکی شبکه و ارتباطات	۱۳۲
۳-۳-۸- امنیت فیزیکی تجهیزات/سخت‌افزارها	۱۳۴
۴-۸- آزمایشگاه امنیت فیزیکی و کنترل دسترسی	۱۳۶
۱-۴-۸- اهداف آزمایشگاه	۱۳۶
۲-۴-۸- ساختار پیشنهادی آزمایشگاه	۱۳۷
فصل نهم - پدافند غیرعامل در حوزه تهدیدات الکترومغناطیسی	۱۴۱
۱-۹- مقدمه	۱۴۱
۲-۹- تهدیدات الکترومغناطیسی	۱۴۱
۱-۲-۹- آسیب‌پذیری در اثر بحران الکترومغناطیسی	۱۴۴
۲-۲-۹- راهبردهای حفاظتی و سطوح مقاوم‌سازی	۱۴۵
۳-۹- دستورالعمل‌های پدافند غیرعامل	۱۴۶
۱-۳-۹- دستورالعمل‌های قبل از بحران	۱۴۶
۲-۳-۹- دستورالعمل‌های حین وقوع بحران	۱۵۰
۳-۳-۹- دستورالعمل‌های پس از وقوع بحران	۱۵۱
فصل دهم - پدافند غیرعامل در حوزه شبکه ارتباطات ثابت	۱۵۵
۱-۱۰- مقدمه	۱۵۵
۲-۱۰- آشنایی با شبکه تلفن ثابت	۱۵۵
۱-۲-۱۰- شبکه تلفن ثابت PSTN	۱۵۵
۲-۲-۱۰- معرفی دیگر شبکه‌های ارتباطات کابلی و ثابت	۱۵۷

۱۵۹	۳-۱۰- تاریخچه شبکه تلفن ثابت
۱۶۱	۱-۳-۱۰- انواع تهدیدات و حملات در شبکه PSTN
۱۶۳	۴-۱۰- راهکارهای مقابله با تهدیدات
۱۶۹	فصل یازدهم- پدافند غیرعامل در حوزه شبکه‌های ارتباطات سیار
۱۶۹	۱-۱۱- مقدمه
۱۶۹	۲-۱۱- نسل‌های شبکه‌های ارتباطات سیار
۱۶۹	۱-۲-۱۱- نسل «۱»
۱۷۱	۲-۱۱- نسل «۲»
۱۷۱	۲-۱۱- نسل «۲/۵»
۱۷۲	۴-۲-۱۱- نسل «۳»
۱۷۲	۵-۲-۱۱- نسل «۴»
۱۷۲	۳-۱۱- آشنایی با شبکه ارتباط دینار GSM
۱۷۳	۱-۳-۱۱- ویژگی‌های شبکه GSM
۱۷۴	۴-۱۱- آشنایی با شبکه ارتباط سیار GPRS
۱۷۵	۵-۱۱- مشکلات امنیتی شبکه‌های ارتباطی GSM و GPRS
۱۷۵	۱-۵-۱۱- مشکلات امنیتی شبکه GSM
۱۷۶	۲-۵-۱۱- مشکلات امنیتی شبکه GPRS
۱۷۸	۶-۱۱- معیارها و راهکارهای امنیتی در شبکه‌های ارتباطات سیار
۱۷۸	۱-۶-۱۱- محورهای دفاع غیرعامل در شبکه‌های ارتباطات سیار
۱۷۸	۲-۶-۱۱- راهکارهای پدافند غیرعامل در شبکه‌های ارتباطات سیار
۱۸۷	فصل دوازدهم- پدافند غیرعامل در مسیریاب
۱۸۷	۱-۱۲- مقدمه
۱۸۷	۲-۱۲- ساختار مسیریاب
۱۹۰	۱-۲-۱۲- تقسیم‌بندی مسیریاب‌ها بر اساس کارکرد
۱۹۱	۳-۱۲- بومی‌سازی مسیریاب
۱۹۲	۴-۱۲- تشریح مشخصات و ویژگی‌های مسیریاب
۱۹۵	۵-۱۲- بررسی نقاط آسیب‌پذیر مسیریاب
۱۹۵	۱-۵-۱۲- تشریح تهدیدات و حملات الکترونیکی بر روی مسیریاب

- ۱۹۶-۱۲-۶- آسیب پذیری ها و مخاطرات مسیر یاب ها ۱۹۶
- ۱۹۸-۱۲-۶-۱- دامنه تأثیر حملات علیه مسیر یاب ها ۱۹۸
- ۱۹۹-۱۲-۶-۲- مخاطرات مربوط به مسیر یاب ۱۹۹
- ۲۰۱-۱۲-۷- روش های مقابله با مخاطرات امنیتی و ایمنی در مسیر یاب ۲۰۱
- ۲۰۱-۱۲-۷-۱- بررسی نکات و دستور العمل های امنیتی دسترسی به مسیر یاب ۲۰۱
- ۲۰۴-۱۲-۷-۲- بررسی نکات و دستور العمل های امنیتی پروتکل های مسیر یابی ۲۰۴
- ۲۰۵-۱۲-۸- مخاطرات ناشی از جنگ و مخاصمات بین المللی روی مسیر یاب ها ۲۰۵
- ۲۰۶-۱۲-۱- جنگ اطلاعات ۲۰۶
- ۲۰۷-۱۲-۸-۲- مخاطرات ناشی از مخاصمات بین المللی ۲۰۷
- ۲۰۷-۱۲-۹- ملاحظات پدافند غیرعامل ۲۰۷
- ۲۱۱- فصل سیزدهم- پدافند غیرعامل در سامانه بانک اطلاعاتی ۲۱۱
- ۲۱۱-۱۳-۱- مقدمه ۲۱۱
- ۲۱۱-۱۳-۲- تاریخچه ۲۱۱
- ۲۱۴-۱۳-۳- کاربرد بانک اطلاعاتی و نقش آن در جامعه اطلاعاتی ۲۱۴
- ۲۱۴-۱۳-۳-۱- پایگاه داده چند رسانه ای ۲۱۴
- ۲۱۴-۱۳-۳-۲- پایگاه داده بلا درنگ ۲۱۴
- ۲۱۴-۱۳-۳-۳- پایگاه داده فضایی ۲۱۴
- ۲۱۴-۱۳-۳-۴- پایگاه داده زمانی ۲۱۴
- ۲۱۴-۱۳-۳-۵- پایگاه داده سیار ۲۱۴
- ۲۱۴-۱۳-۳-۶- پایگاه داده XML ۲۱۴
- ۲۱۵-۱۳-۳-۷- پایگاه داده موازی ۲۱۵
- ۲۱۵-۱۳-۳-۸- پایگاه داده توزیع شده ۲۱۵
- ۲۱۵-۱۳-۳-۹- پایگاه داده مقیم در حافظه ۲۱۵
- ۲۱۵-۱۳-۳-۱۰- پایگاه داده استنتاجی ۲۱۵
- ۲۱۵-۱۳-۳-۱۱- پایگاه داده بیولوژیکی ۲۱۵
- ۲۱۶-۱۳-۴- معماری بانک اطلاعاتی ۲۱۶
- ۲۱۶-۱۳-۴-۱- طبقه بندی سامانه مدیریت پایگاه داده ۲۱۶
- ۲۱۶-۱۳-۴-۱-۱- سامانه های مدیریت پایگاه داده از منظر عملکرد ۲۱۶

۲۱۷	۱۳-۴-۲- سامانه‌های مدیریت پایگاه‌داده از منظر پیاده‌سازی
۲۱۸	۱۳-۵- مؤلفه‌های اساسی یک سامانه مدیریت پایگاه‌داده
۲۱۸	۱۳-۵-۱- مؤلفه‌های معماری از منظر نرم‌افزاری
۲۱۹	۱۳-۵-۲- مؤلفه‌های معماری از منظر نماهای مختلف داده
۲۲۱	۱۳-۵-۳- مؤلفه‌های معماری از منظر کارکردها و مؤلفه‌های درونی
۲۲۴	۱۳-۵-۴- سایر مؤلفه‌ها
۲۲۵	۱۳-۶- امنیت در سامانه مدیریت پایگاه‌داده
۲۲۶	۱۳-۶-۱- اهداف امنیت
۲۲۶	۱۳-۶-۲- نام‌های اساسی در تأمین امنیت پایگاه‌داده
۲۲۷	۱۳-۶-۳- رمزنگار و اثر آن در امنیت سامانه مدیریت پایگاه‌داده
۲۲۸	۱۳-۷- نیازها و ویژگی‌های بانک اطلاعاتی
۲۳۰	۱۳-۸- استانداردهای بانک اطلاعاتی
۲۳۲	۱۳-۹- ملاحظات پدافند غیر عامل
۲۳۷	فصل چهاردهم- پدافند غیر عامل در پست الکترونیکی
۲۳۷	۱۴-۱- مقدمه
۲۳۸	۱۴-۲- تاریخچه
۲۳۹	۱۴-۳- آشنایی با پست الکترونیکی
۲۴۲	۱۴-۴- معماری و پروتکل‌های ارتباطی
۲۴۵	۱۴-۵- تهدیدات و مخاطرات ناشی از پست الکترونیکی
۲۵۱	۱۴-۶- ملاحظات پدافند غیر عامل در کاربری پست الکترونیک
۲۵۵	فصل پانزدهم- پدافند غیر عامل در ضد بدافزارها
۲۵۵	۱۵-۱- مقدمه
۲۵۵	۱۵-۲- آشنایی با بدافزارها
۲۵۹	۱۵-۳- نحوه عملکرد ضد بدافزارها
۲۵۹	۱۵-۳-۱- ردیابی
۲۶۲	۱۵-۳-۲- شناسایی
۲۶۲	۱۵-۳-۳- پاک‌سازی
۲۶۴	۱۵-۴- روش‌های ارزیابی ضدبدافزارها

- ۱۵-۵- انواع ضدبدافزار..... ۲۶۹
- فصل شانزدهم- پدافند غیرعامل در سیستم مدیریت تهدید یکپارچه..... ۲۷۵
- ۱۶-۱- مقدمه..... ۲۷۵
- ۱۶-۲- مدل امنیت لایه‌بندی شده..... ۲۷۶
- ۱۶-۳- سیستم مدیریت تهدید یکپارچه چیست؟..... ۲۷۸
- ۱۶-۴- مشخصه‌های یک سیستم مدیریت تهدید یکپارچه خوب..... ۲۷۹
- ۱۶-۴-۱- دیراره آتش..... ۲۸۰
- ۱۶-۴-۲- سیستم تشخیص نفوذ..... ۲۸۲
- ۱۶-۴-۳- شبکه اختصاصی مجازی..... ۲۸۳
- ۱۶-۴-۴- آنتی ویروس..... ۲۸۴
- ۱۶-۴-۵- آنتی اسپم..... ۲۸۴
- ۱۶-۴-۶- فیلترینگ..... ۲۸۵
- ۱۶-۴-۷- مدیریت پهنای باند..... ۲۸۵
- ۱۶-۴-۸- وب کشینگ..... ۲۸۶
- ۱۶-۴-۹- نوع سیستم عامل مورد استفاده در سیستم مدیریت تهدید یکپارچه..... ۲۸۷
- ۱۶-۵- سخت‌افزار تشکیل‌دهنده سیستم مدیریت تهدید یکپارچه..... ۲۸۷
- ۱۶-۶- سامانه مدیریت تهدید یکپارچه و علل استفاده از آن..... ۲۸۸
- ۱۶-۷- حالت‌های کاری سامانه‌های مدیریت تهدید یکپارچه..... ۲۹۰
- ۱۶-۷-۱- حالت مسیریاب..... ۲۹۰
- ۱۶-۷-۲- حالت شفاف..... ۲۹۰
- ۱۶-۷-۳- حالت پراکسی..... ۲۹۰
- ۱۶-۸- قابلیت‌های امنیتی سامانه‌های مدیریت تهدید یکپارچه..... ۲۹۱
- ۱۶-۸-۱- دیواره آتش..... ۲۹۲
- ۱۶-۸-۲- ضد بدافزار..... ۲۹۲
- ۱۶-۸-۳- شبکه اختصاصی مجازی..... ۲۹۳
- ۱۶-۸-۴- تشخیص و جلوگیری از نفوذ..... ۲۹۴
- ۱۶-۸-۵- مدیریت و پالایش محتوای وب..... ۲۹۵
- ۱۶-۸-۶- کنترل برنامه‌های کاربردی..... ۲۹۵

۲۹۶	۱۶-۸-۷- ضد هرزنامه
۲۹۸	۱۶-۸-۸- AAA
۲۹۸	۱۶-۸-۹- گزارش‌دهی، رویدادنگاری و نظارت
۲۹۹	۱۶-۹- سایر امکانات سامانه‌های مدیریت تهدید یکپارچه
۲۹۹	۱۶-۹-۱- مدیریت پهنای باند
۲۹۹	۱۶-۹-۲- مسیریابی و پشتیبانی از NAT
۲۹۹	۱۶-۹-۳- مدیریت چند لینک ارتباطی
۳۰۰	۱۶-۹-۴- وجود امکان دسترسی بالا
۳۰۰	۱۶-۹-۵- وجود امکان توازن یا اشتراک بار
۳۰۰	۱۶-۹-۶- وجود مکان سیستم مجازی یا دامنه مجازی
۳۰۱	۱۶-۹-۷- وب سایت دامنه مدیریت تهدید یکپارچه
۳۰۱	۱۶-۹-۸- سرویس‌های عمومی
۳۰۱	۱۶-۱۰- مشخصه‌های متمایز کننده سامانه‌های مدیریت تهدید یکپارچه
۳۰۱	۱۶-۱۰-۱- نحوه ارائه امکانات
۳۰۲	۱۶-۱۰-۲- میزان گذردهی و کارایی
۳۰۲	۱۶-۱۰-۳- نوع پردازش بسته‌ها
۳۰۳	۱۶-۱۰-۴- نوع سیستم عامل مورد استفاده در سیستم مدیریت تهدید یکپارچه
۳۰۳	۱۶-۱۰-۵- وجود مستندات کامل، پشتیبانی مناسب و مکان روزرسانی
۳۰۳	۱۶-۱۰-۶- بومی بودن محصول
۳۰۷	فصل هفدهم - پدافند غیرعامل در دیواره آتش
۳۰۷	۱۷-۱- مقدمه
۳۰۷	۱۷-۲- ضرورت استفاده از دیواره آتش
۳۰۸	۱۷-۳- فواید استفاده از دیواره آتش
۳۰۹	۱۷-۴- ویژگی‌های دیواره آتش
۳۱۰	۱۷-۵- مکانیسم‌های امنیتی در دیواره آتش
۳۱۰	۱۷-۵-۱- بسته صافی
۳۱۱	۱۷-۵-۲- ترجمه آدرس
۳۱۱	۱۷-۵-۳- دسترس‌پذیری بالا

۳۱۲	۱۷-۵-۴- مدیریت پهنای باند
۳۱۳	۱۷-۵-۵- شبکه خصوصی مجازی
۳۱۳	۱۷-۵-۶- سیاست امنیتی در دیواره آتش
۳۱۳	۱۷-۵-۷- مدیریت دیواره آتش
۳۱۷	۱۷-۶- معماری و جایگاه دیواره آتش در شبکه
۳۱۷	۱۷-۶-۱- معماری دیواره آتش در شبکه
۳۱۹	۱۷-۶-۱- دیواره آتش ساده
۳۱۹	۱۷-۶-۳- دیواره آتش با چند پورت
۳۲۲	۱۷-۶-۴- استفاده از چند دیواره آتش
۳۲۷	فصل هجدهم - مرکز عملیات امنیت
۳۲۷	۱۸-۱- مقدمه
۳۲۸	۱۸-۲- اهمیت و ضرورت مرکز عملیات امنیت
۳۲۹	۱۸-۳- اهمیت پیاده‌سازی مرکز عملیات امنیت در زیرساخت‌های اطلاعاتی
۳۳۱	۱۸-۴- اهداف، وظایف و اجزای مرکز عملیات امنیت
۳۳۲	۱۸-۴-۱- اهداف پیاده‌سازی مرکز عملیات امنیت
۳۳۲	۱۸-۴-۲- ساختار و وظایف مرکز عملیات امنیت
۳۳۷	۱۸-۵- ویژگی‌های ساختاری مرکز عملیات امنیت
۳۴۱	فصل نوزدهم - پدافند سایبری در سیستم‌های کنترل صنعتی
۳۴۱	۱۹-۱- مقدمه
۳۴۲	۱۹-۲- مفهوم حمله به سامانه‌های اسکادا
۳۴۳	۱۹-۲-۱- انواع حمله‌ها به سامانه‌های اسکادا
۳۴۴	۱۹-۲-۲- دفاع از سامانه‌های اسکادا
۳۴۵	۱۹-۳- ارزیابی امنیتی و پدافندی سیستم‌های کنترل صنعتی (شبکه اسکادا)
۳۵۳	منابع و مآخذ

پیش‌گفتار

با پیشرفت فناوری اطلاعات و ارتباطات، دستگاه‌های اجرایی برای انجام عملیات خود جهت تولید، ذخیره‌سازی، پردازش، نگهداری، بازیابی و ارائه گزارش اطلاعات به سامانه‌های اطلاعاتی رایانه‌ای وابسته شده‌اند. در برنامه توسعه کشور قرار بر آن است که در آینده نزدیک بیش از هفتاد درصد خدمات دولتی با بهره‌گیری از سامانه‌های خودکار و داده‌های الکترونیکی انجام شود. بدین ترتیب اجرای مأموریت‌ها و ارائه خدمات به عموم مردم بدون استفاده از این سامانه‌ها ممکن نخواهد بود. بنابراین امنیت اطلاعات و پدافند غیرعامل در دستگاه‌های اجرایی از اهمیت ویژه‌ای برخوردار خواهند بود تا اطمینان از حفظ محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات و سامانه‌های اطلاعاتی حاصل شود.

پدافند غیرعامل به عنوان یکی از مؤثرترین و پایدارترین روش‌های دفاع در مقابل تهدیدات، همواره مد نظر اکثر کشورهای جهان قرار دارد. این به سبب افزایش توان بازدارندگی، نقش بسزایی در کاهش احتمال درگیری نظامی داشته و در صورت پیاده‌سازی درست قادر است که اثرات حوادث پیشرو را به مقدار قابل‌توجهی کاهش دهد. پدافند غیرعامل به معنای کاهش آسیب‌پذیری در هنگام بحران، بدون استفاده از اقدامات نظامی و صرفاً با بهره‌گیری از فعالیت‌های غیرنظامی، فنی و مدیریتی است.

اقدامات پدافند غیرعامل شامل: پراکندگی، جابجایی، فریب، مکان‌یابی، اعلام خبر، قابلیت بقا، استحکامات، استتار و شبکه امن می‌شود. در سامانه‌های کلی پدافند غیرعامل که از سوی مقام معظم رهبری ابلاغ گردید، بر پدافند غیرعامل به عنوان مجموعه‌ای از اقدامات غیرمسلحانه تأکید شده که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌شود.

امروزه کشورهایی که تخریب‌ها و خسارات جنگ را تجربه کرده‌اند؛ توجه ویژه‌ای به پدافند غیرعامل دارند. پدافند غیرعامل در زمینه‌ی فناوری اطلاعات و ارتباطات به منظور فراهم آوردن امنیت اطلاعات، افزایش امنیت سیستم‌های مدیریت تحت شبکه در مقابل حملات سایبری مخرب و پایین آوردن خسارات احتمالی و نیز بالا بردن ضریب اطمینان شبکه‌های ارتباطی در مواجهه با حوادثی از قبیل حملات سایبری و بلایای طبیعی بسیار

تأثیرگذار است. بنابراین پدافند غیرعامل در حوزه فناوری اطلاعات و ارتباطات نقش جلوگیری و پایین آوردن میزان آسیب‌پذیری را دارا است.

برای اجرای صحیح پدافند غیرعامل در زمینه فناوری اطلاعات، نیاز است که زیرساخت‌های آن به خوبی معرفی و مورد تحلیل قرار گیرند. در این شرایط است که نقاط ضعف و قوت این سیستم‌ها قابل شناخت و بررسی می‌باشد. با مطالعه و روشن‌سازی ارتباطات و واسطه‌های بین سامانه‌های فناوری اطلاعات با سایر بخش‌ها و ایجاد اقدامات مناسب می‌توان گسترش دامنه آسیب‌ها، تحت کنترل داشت. هرچه دامنه شناخت انسان از اجزای این سامانه‌ها، وظایف و فعالیت‌های آن بیشتر شود، تسلط بر رفتار و اثرات ناشی از آن بیشتر خواهد بود.

بنابراین هدف کتاب این است که با معرفی اجزاء و وظایف سامانه‌های فناوری اطلاعات و ارتباطات، تصویر روشنی از آسیب‌ها و حجم آن‌ها در این حوزه را ارائه دهد. همچنین راه‌های کاهش آسیب‌پذیری‌ها و محدود کردن دامنه آن‌ها به سایر بخش‌ها و افزایش قابلیت بقا و پایداری سازمان‌ها و شبکه‌های حوزه فناوری اطلاعات و ارتباطات ارائه می‌گردد.

در پایان از زحمات و تلاش‌های مؤثران گرامی، سازمان پدافند غیرعامل و همچنین آقایان مهندس مهدی چیت‌ساز خوئی و مهندس حسن پارسا که در این راستا نهایت همکاری را داشتند تقدیر و تشکر می‌کنیم.

معاونت فنی و مهندسی گروه تخصصی سموات - قرارگاه مرکزی خاتم‌الانبیاء(ص)