

بسم الله الرحمن الرحيم



دانشگاه افسری امام علی (ع)

معاونت پژوهش

مبانی امنیت در عملیات اطلاعات و ارتباطات (با رویکرد نظامی)

محمد احمدی

مجتبی رمضان زاده

۱۳۹۲

سرشناده:	احمدی، محمد، ۱۳۶۰ -
عنوان و نام پدیدآور:	مبانی امنیت در فناوری اطلاعات و ارتباطات (با رویکرد نظامی) / محمد احمدی، مجتبی رمضانزاده.
مشخصات نشر:	تهران: دانشگاه افسری امام علی (ع)، معاونت پژوهشی، ۱۳۹۱.
مشخصات ظاهری:	۱۸۱ ح.؛ مصور، جدول، نمودار.
شابک:	۹۷۸-۹۶۴-۲۸۹۹-۶۴-۷
وضعیت فهرست نویسی:	فیا
موضوع:	حفاظت اطلاعات -- ایران
موضوع:	مراکز داده پردازی -- اقدامات تأمینی
موضوع:	پایگاه‌های اطلاعاتی -- امنیت
موضوع:	شبکه‌های کامپیوتری -- اقدامات تأمینی
موضوع:	ایران -- نیروهای مسلح -- اقدامات تأمینی
شناسه داده:	رمضانزاده، مجتبی، ۱۳۵۲ -
شناسه افزوده:	دانشگاه افسری امام علی (ع)، معاونت پژوهشی
رده بندی کنگره:	۹۱ الف ۹ / الف ۸۵۳ UA
رده بندی دیویی:	۳۳۰.۹۵ ۵۵
شماره کتابشناسی ملی:	۵۹۱

عنوان کتاب:	مبانی امنیت در فناوری اطلاعات و ارتباطات (با رویکرد نظامی)
مؤلفان:	محمد احمدی، مجتبی رمضانزاده
صفحه آرا و طراح جلد:	مجید کاشانی
مدیر مسئول انتشارات:	حمیدرضا بیات
شمارگان:	۱۰۰۰ نسخه
قیمت:	۱۸۰۰۰۰ ریال
نوبت چاپ:	اول، ۱۳۹۲
شابک:	۹۷۸-۹۶۴-۲۸۹۹-۶۴-۷
صندوق پستی:	۱۳۱۷۸۹۳۴۷
تلفن:	۶۶۴۶۷۴۴۴

نشانی: تهران - خیابان امام خمینی^(۱) - ترسیده به میدان حر - دانشگاه افسری امام علی^(ع) معاونت پژوهش

پست الکترونیکی: Imamali.nashr93@gmail.com

کلیه حقوق برای دانشگاه افسری امام علی^(ع) محفوظ است.

پیشگفتار

کتابی که پیش روی شماست، گامی در جهت فهم و آموزش مفاهیم بنیادی و کاربردی امنیت در فناوری اطلاعات و ارتباطات با رویکرد نظامی می‌باشد. در زمینه امنیت کتب و نشریات متعددی چاپ گردیده است ولی کمتر منبعی به امنیت از منظر نظامی پرداخته است. امروزه امنیت جامع و مانع در نیروهای مسلح نه تنها یک انتخاب است بلکه یک ضرورت می‌باشد. مؤلفان با تجربه چندین ساله فعالیت در فناوری اطلاعات و ارتباطات و تدوین درس امنیت اطلاعات در دانشگاه‌های نظامی و غیر نظامی سعی نموده‌اند که این را آلیف نمایند که برای دانش‌آموختگان دانشگاه‌های نظامی کاربردی باشد.

این کتاب همچنین می‌تواند برای آموزش عموم کاربران و به ویژه مدیران، به منظور تفاهم فنی با کارشناسان شاغل در امور امنیت اطلاعات، مورد استفاده قرار گیرد. علاوه بر این، عمده مطالب کتاب برای استفاده در مسائل امنیتی روزمره مفید بوده و در قالب دوره‌های کوتاه‌مدت نیز قابل ارائه است.

کتاب حاضر مشتمل بر ۳ بخش و ۱۰ فصل است. بخش نخست مبانی امنیت اطلاعات در سه فصل (مفاهیم و تعاریف امنیت اطلاعات، امنیت اطلاعات و روش‌های تأمین امنیت اطلاعات) تبیین شده است. در بخش دوم ملاحظات خاص امنیت اطلاعات در سازمان‌های نظامی به تفکیک هر یک از منابع امنیتی در ۵ فصل آورده شده است. در بخش نهایی، مهارت‌های کاربردی در دو فصل ملاحظات امنیتی در ویندوز و نرم‌افزارهای جاسوسی توضیح داده شده است.

خوانندگان پس از مطالعه مباحث مورد نظر، علاوه بر آشنایی به مبانی امنیت اطلاعات و مفاهیم امنیت شبکه، آمادگی پذیرش مطالب پیشرفته و فنی‌تر در موضوعات مورد علاقه را به دست می‌آورند. در یک کلام می‌توان گفت هدف از انتشار این کتاب

توسعه درک واقع گرایانه و عمیق از ماهیت مشکلات امنیتی موجود به منظور کاهش آسیب پذیری ها و افزایش نقاط قوت فناوری اطلاعات و ارتباطات در سازمان های نظامی می باشد.

امید است در پرتو عنایات حق تعالی بتوانیم با انتشار چنین منابعی گامی هر چند کوچک در جهت اعتلای فناوری اطلاعات و ارتباطات در میهن عزیزمان برداریم. کلیه عزیزانی که این کتاب را مطالعه می نمایند، به ویژه استادان، دانشجویان و دیگر صاحب نظران می توانند نظرات، انتقادات و پیشنهادات خود را به انتشارات ارسال نمایند.

www.ketab.ir

بخش اول: مبانی امنیت اطلاعات

فصل اول: مفاهیم و تعاریف امنیت اطلاعات

۲	۱-۱- مقدمه
۳	۲-۱- دارایی‌های یک سازمان
۵	۳-۱- تعریف امنیت اطلاعات
۶	۴-۱- مؤلفه‌های تضمین امنیت
۷	۵-۱- آسیب‌پذیری‌ها
۱۱	۶-۱- تهدیدات
۱۵	۷-۱- ویروس
۲۴	۸-۱- اسب تراوا
۲۴	۹-۱- کرم
۲۵	۱۰-۱- ایجاد شکاف در کلمه عبور
۲۷	۱۱-۱- تغییر قیافه
۲۷	۱۲-۱- درب‌های مخفی (درب‌های پشتی)
۲۸	۱۳-۱- حملات عدم پذیرش سرویس DOS
۲۹	۱۴-۱- هرز نامه
۲۹	۱۵-۱- کوکی‌ها
۳۰	۱۶-۱- حافظه نهان مرورگر وب
۳۱	۱۷-۱- تهدید چندوجهی
۳۲	خودآزمایی
۳۳	فصل دوم: مدیریت امنیت اطلاعات
۳۴	۱-۲- مقدمه
۳۵	۲-۲- راهبرد امنیت سازمانی

۳۶	۳-۲- سیاست‌های امنیت اطلاعات
۳۸	۳-۲-۱ ملاحظات تدوین سیاست‌های امنیت اطلاعات
۴۰	۳-۲-۲ ممیزی و بازبینی‌های امنیتی
۴۱	۴-۲- استانداردها و راهبردها یا خط‌مشی‌های امنیتی
۴۳	۴-۲-۱ راهبردها
۴۳	۴-۲-۲ انواع استانداردهای ایمنی
۴۴	۴-۲-۳ استاندارد BS7799
۴۸	۵-۲- سیستم مدیریت امنیت اطلاعات (ISMS)
۴۸	۵-۲-۱- تشخیص ریسک به ISMS
۴۸	۵-۲-۲- مراحل اجباری ISMS
۵۱	۵-۲-۳- ساختار سازمانی ISMS
۵۲	۶-۲- مؤلفه‌های حیاتی موفقیت
۵۳	خودآزمایی
۵۵	فصل سوم: روش‌های تأمین امنیت اطلاعات
۵۶	۳-۱- مقدمه
۵۶	۳-۲- دفاع در عمق
۵۸	۳-۲-۱- ساز و کارهای پیشگیری
۵۸	۳-۲-۳-۱- امنیت فیزیکی و محیطی
۶۲	۳-۲-۳-۲- شناسایی و احراز هویت
۶۷	۳-۲-۳-۳- کنترل دسترسی
۶۸	۳-۲-۳-۴- دیواره آتش
۶۹	۳-۲-۳-۵- رمزنگاری
۷۰	۳-۲-۴- ساز و کارهای تشخیص نفوذ

فهرست مطالب

عناوین	صفحه
۳-۵- ساز و کارهای ترمیم و بازیابی	۷۱
خودآزمایی	۷۳
بخش دوم: ملاحظات امنیتی خاص سازمان‌های نظامی	
فصل چهارم: امنیت نرم افزار	۷۶
۴-۱- مقدمه	۷۷
۴-۲- تهیه نرم افزار	۷۷
۴-۳- ملاک‌های انتخاب نرم افزار	۷۹
۴-۴- اصول امنیتی نرم افزار	۸۱
۴-۵- اصول امنیتی پشتیبانی نرم افزار	۸۳
۴-۶- مدیریت امنیت نرم افزار	۸۴
۴-۷- کنترل امنیت نرم افزار	۸۶
خودآزمایی	۸۸
فصل پنجم: امنیت سخت افزار	۸۹
۵-۱- مقدمه	۹۰
۵-۲- اصول امنیتی تهیه سخت افزار	۹۰
۵-۳- توزیع سخت افزار	۹۲
۵-۴- پشتیبانی سخت افزار	۹۴
۵-۵- مدیریت سخت افزار	۹۵
۵-۶- کنترل امنیت سخت افزار	۹۶
خودآزمایی	۹۷

فصل ششم: امنیت شبکه	۹۹
۱-۶- مقدمه	۱۰۱
۲-۶- منابع شبکه	۱۰۰
۳-۶- تهیه و توزیع بستر ارتباطی شبکه	۱۰۱
۴-۶- حراست و ایمنی بسترهای ارتباطی	۱۰۳
۵-۶- ایجاد شبکه رایانه‌ای	۱۰۴
خودآزمایی	۱۰۷
فصل هفتم: امنیت اینترنت	۱۰۹
۱-۷- مقدمه	۱۱۰
۲-۷- امنیت تهیه اطلاعات	۱۱۰
۳-۷- توزیع و بهره‌برداری اطلاعات	۱۱۱
۴-۷- تغییر کاربری و پشتیبانی اطلاعات	۱۱۲
۵-۷- مدیریت امنیت اطلاعات	۱۱۲
خودآزمایی	۱۱۴
فصل هشتم: امنیت نیروی انسانی	۱۱۵
۱-۸- مقدمه	۱۱۶
۲-۸- امنیت نیروی انسانی	۱۱۶
۳-۸- نقل و انتقالات نیروی انسانی	۱۱۷
۴-۸- به کارگیری نیروی انسانی	۱۱۷
۵-۸- تغییر وضعیت نیروی انسانی	۱۱۸
۶-۸- پشتیبانی نیروی انسانی	۱۱۹
۷-۸- آموزش و فرهنگ سازی	۱۱۹
۸-۸- ارزیابی نیروی انسانی	۱۲۱

فهرست مطالب

صفحه	عناوین
۱۲۱	۸-۹-۱- ایمنی نیروی انسانی
۱۲۲	۸-۱۰-۱- کنترل امنیت نیروی انسانی
۱۲۳	خودآزمایی
	بخش سوم: مهارت‌های کاربردی
۱۲۶	فصل نهم: اطلاعات امنیتی در سیستم عامل ویندوز
۱۲۷	۹-۱- مقدمه
۱۲۷	۹-۲- دستورات ابتدایی
۱۳۳	۹-۳- دستورات عمومی
۱۴۸	۹-۴- دستورات پیشرفته
۱۵۶	خودآزمایی
۱۵۷	فصل دهم: نرم افزارهای جاسوسی
۱۵۸	۱۰-۱- مقدمه
۱۵۸	۱۰-۲- نرم افزار جاسوسی
۱۵۹	۱۰-۳- انواع نرم افزارهای جاسوسی
۱۶۲	۱۰-۴- مقابله با نرم افزارهای جاسوسی
۱۶۵	۱۰-۵- دو نمونه از نرم افزارهای جاسوسی
۱۷۰	خودآزمایی
۱۷۱	ضمیمه: تعاریف و اصطلاحات رایج امنیتی
۱۷۷	منابع و مراجع