بسم الله الرحمن الرحیم

مدیریت حفاظتی فن‌آوری‌های نوین

تألیف

ناصر کامیار

دانشگاه اطلاعات و امنیت ملی

مؤسسه چاپ و انتشارات

۱۳۹۷

سرشناسه	: کامیار، ناصر
عنوان و نام پدیدآور	: مدیریت حفاظتی فن‌آوری‌های نوین / تالیف ناصر کامیار
مشخصات نشر	: تهران: دانشگاه اطلاعات و امنیت ملی، موسسه چاپ و انتشارات، ۱۳۹۶.
مشخصات ظاهری	: ۳۹۵ ص. ش ۳۹۵
وضعیت فهرست‌نویسی	: فیپا
موضوع	: تکنولوژی اطلاعات – تدابیر ایمنی
موضوع	: Information technology—Security measures
موضوع	: کامپیوترها – ایمنی اطلاعات
موضوع	: Computer security
موضوع	: منابع اطلاعاتی الکترونیکی – کنترل دستیابی- حفاظت داده‌ها
موضوع	: Electronic information resources—Access control—Data protection
شناسه افزوده	: دانشگاه اطلاعات و امنیت ملی. معاونت پژوهش و تولید علم
شناسه افزوده	: دانشگاه اطلاعات و امنیت ملی. موسسه چاپ و انتشارات
رده بندی کنگره	: ۱۳۹۶ ٤م٢٤ک/٥/٥٨ T
رده بندی دیویی	: ۳۰۳/۸۳۳
شماره کتابشناسی ملی	: ۵۰۶۵۹

مشخصات

عنوان: مدیریت حفاظتی فن‌آوری‌های نوین

تألیف: ناصر کامیار

ناشر: مؤسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی

تاریخ انتشار: ۱۳۹۷

نوبت چاپ: اول

شمارگان: ۵۰۰ نسخه

بها: ۲۰۰,۰۰۰ ریال

شابک: ۹۷۸-۶۰۰-۸۸۸۵-۲۹-۰

تلفن: ۲۲٤٦۹۷۳۹

تهران: صندوق پستی ۱٤۳۸ـ ۱٦۷٦٥

فهرست مطالب

فصل سوم
دولت سیار

فصل چهارم
اسناد غیر دیجیتال

فصل پنجم
اطلاعات ذهنی

فصل ششم

تهدیدات فن‌آوری‌های نوین سازمانی در مراحل مختلف به‌کارگیری

فصل هفتم

رمز و رمزنگاری در ابزار نوین

فصل هشتم

مدیریت ریسک مرتبط با اطلاعات ابزار نوین

فصل نهم

مدل‌سازی امنیتی

فصل دهم

قوانین حاکم بر فن‌آوری‌های نوین

فصل یازدهم

آینده پژوهی در امر اطلاعات مرتبط با فن‌آوری‌های نوین

پیشگفتار

با ظهور و رشد فن‌آوری‌های نوین، فضای سایبر یکی از ارکان اساسی اداره جوامع امروزی به شمار می‌رود. عرضه بخش بزرگی از خدمات عمومی و سهولت و سرعت انجام کار و امکانات گسترده فضای سایبری و فن‌آوری اطلاعات آن را به مهم‌ترین عرصه برای فعالیت سرمایه‌های ملی تبدیل نموده است.

آمریکا شیطان بزرگ و ابرقدرت بزرگ‌ترین بازیگر فعال در فضای مجازی محسوب می‌شوند که با طراحی و سرمایه‌گذاری در تولید دانش و فن‌آوری‌های نوین بیش‌ترین بهره‌برداری از فضای مجازی را کسب نموده و فضای سایبر را به میدان برنامه‌ریزی راهبردی و هدایت مزیت‌های تاکتیکی در جهت دستیابی به اهداف سلطه طلبانه و به یکی از عرصه‌های تقابل میان کشورها و قدرت‌های ملی تبدیل نموده است.

اسناد و مدارک طبقه‌بندی شده هر کشور جزء دارایی‌های با ارزش آن محسوب شده و حفاظت از آن‌ها بر مبنای دلایل عقلی و قانونی اجتناب‌ناپذیر بوده و یکی از وظایف واحدهای مسئول در این رابطه می‌باشد، زیرا افشای آن‌ها و دسترسی افراد غیرمجاز به‌ویژه دشمنان، رقبا و کسانی که به هر دلیلی به دنبال سوءاستفاده از آن اسناد واطلاعات می‌باشند ضربات جبران‌ناپذیری به اساس حکومت، منافع ملی، منافع کشور و یا یک سازمان وارد می‌کند.

از دیرباز تاکنون افشاء غیرمجاز اطلاعات و اسناد طبقه‌بندی شده مشکلات عدیده‌ای برای حکومت‌ها، دولت‌ها و سازمان‌ها ایجاد کرده و در برخی موارد موجب به‌روز جنگ‌ها و آشوب‌هایی شده و خسارت‌های سنگین جانی و مالی به ملت‌ها تحمیل نموده است. در کشورمان نیز نمونه‌های متعددی از جمله مواردی در طی دوران دفاع مقدس و پس از آن وجود داردکه تبعات جبران ناپذیری برای نظام داشته است.

فرآیند تولید، گردش و نگهداری اسناد طبقه‌بندی شده و بهره‌برداری بهینه از آن‌ها و انجام امور حفاظتی مربوطه و نظارت بر واحدهای زیر مجموعه مستلزم استقرار یک نظام صریح و اصولی در امر حفاظت از اسناد و اجرای دقیق آن از سوی مدیران و کارکنان می‌باشد. دستیابی و افشای غیرمجاز اسناد و مدارک طبقه‌بندی شده دلایل متعددی دارد که از مهم‌ترین آن‌ها عدم شناخت و آگاهی نسبت به ارزش اطلاعات و اسناد طبقه‌بندی شده در اختیار، عدم اطلاع از تبعات افشاء آن‌ها، سهل انگاری، بی‌توجهی و بی‌دقتی در انجام وظایف محوله اداری و اصول حفاظتی است.

در رابطه با حفظ و نگهداری اطلاعات احادیث بسیاری از ائمه وارد شده است که آگاهی از آن وظیفه همه را در این رابطه سنگین‌تر می‌نماید.

الإمامُ الصّادقُ علیه السلام: سِرُّکَ مِن دَمِکَ فلا یَجرِیَنَّ مِن غیرِ أوداجِکَ

راز تو جزئی از خون توست، پس نباید که در گفتگوی غیر تو جریان یابد (بحارالانوار، ج۷۲: ۷۱).

در سازمان‌های مختلف دولتی و عمومی مسئولیت حفظ و نگهداری اطلاعات تولید شده بنا بر ابلاغ صریح شورای عالی امنیت ملی با تولید کننده اطلاعات بوده و معمولاً مدیران سازمان‌ها این وظیفه را به قسمت‌های حراست سازمان خود تفویض اختیار می‌نمایند.

برای ایفای این نقش، افراد و مدیران شاغل در حراست و یا حفاظت مجموعه نیازمند آشنایی بیش‌تر با وظایف خود می‌باشند. در این کتاب وظایف مدیریتی و فنی مورد نیاز مدیران حراست فن‌آوری اطلاعات سازمان‌ها مورد بحث قرار می‌گیرد.

مخاطب اصلی این کتاب دانشجویان کارشناسی ارشد رشته حفاظت و مشابه آن در دانشگاه اطلاعات و امنیت ملی می‌باشد و به صورت عمومی کلیه افرادی که در قسمت‌های حراستی و یا حفاظتی به عنوان مدیر و یا کارشناس مشغول به خدمت بوده و یا علاقه‌مند به خدمت در این‌گونه مشاغل می‌باشند می‌توانند از مطالب کتاب در راستای مدیریت به خود استفاده نمایند.

این کتاب در پانزده فصل تقدیم خوانندگان شده و در هر فصل ضمن برشمردن نکاتی در مورد یکی از وظایف مدیریتی در راستای حفاظت از فن‌آوری‌های نوین، دارای سؤالاتی در انتهای فصل می‌باشد که خوانندگان با توانایی بر پاسخ آن می‌توانند دانسته‌های خود را مورد آزمون قرار دهند. اساتید محترم نیز پس از بهره‌برداری از این کتاب به عنوان منبع اصلی درس مدیریت حفاظتی بر فن‌آوری‌های نوین می‌توانند از سؤالات انتهای هر فصل به عنوان آزمون‌های پایان ترم بهره بگیرند.

اساتید محترم در اثنای تدریس هر فصل از مصادیق موجود در سازمان‌های هم‌عرضی که دانشجویان در آن‌جا مشغول به‌کار می‌باشند بهره گیری فرمایند تا یادگیری دانشجویان عینی‌تر باشد.

در فصل اول کتاب اصول کلی مرتبط با فن‌آوری‌های اطلاعات و مبحث حفاظت برای یادآوری دانشجویان به صورت کلی بیان شده است تا مخاطبان با تعاریف عملیاتی که در طول کتاب درباره حفاظت و مدیریت و فن‌آوری‌های نوین قید می‌گردد دارای مفاهیم یکسانی باشند.

وظیفه سیستم‌های اطلاعاتی در قانون و بخشنامه‌های صادره بالادستی در کشور به صورت شفاف بیان شده است. برخی از این وظایف در سطح کلان کشور و منطقه بوده و برخی از آن‌ها کاربرد ملی و درون سازمانی دارند. به این‌گونه مباحث در فصل دوم پرداخته شده است تا دانشجویان با این نقش‌ها آشنا شده و بر آن مبنا بتوانند مطالب را فرا گیرند.

در فصل سوم به بحث دولت الکترونیک و در همان راستا عبور از دولت الکترونیک و تبدیل شدن آن به دولت سیار پرداخته شده است. امروزه با رشد فن‌آوری‌های نوین اطلاعاتی و ارتباطی، کشورها الزاماً می‌بایست به این عرصه وارد شوند تا بتوانند نیازهای مردمان کشور خود را در کوتاه‌ترین زمان و به بهترین شکل و با دقت و سرعت لازم برآورده نمایند و این کار به غیر از ورود در عرصه دولت سیار امکان‌پذیر نمی‌باشد. در این فصل دانشجویان با ویژگی‌های عمومی و حفاظتی دولت سیار آشنا شده و نقش نیروهای حراستی در این گونه اعمال حاکمیت را فرا می‌گیرند و با وظایف صیانتی خود در دولت سیار آشنا می‌شوند.

سازمان‌ها در حال گذر از اطلاعات سنتی به سمت اطلاعات دیجیتال می‌باشند و در این گذر الزاماً تا سالیان سال نمی‌توان نقش اسناد غیر دیجیتال در سازمان‌ها را نادیده گرفت. در این دوره گذر بعضاً از ابزار نوین برای مدیریت بر اسناد غیر دیجیتال در سازمان‌ها استفاده می‌شود. در فصل چهارم این مسئله مورد بحث و بررسی قرار می‌گیرد تا دانشجویان ضمن آشنایی با ویژگی‌های این دوره گذر بتوانند بهترین مشورت‌های صیانتی را به مدیران سازمان ارائه نمایند.

فصل پنجم به اطلاعات رسوب شده در حافظه می‌پردازد. ذهن از جمله ابزار ذخیره‌سازی است که به هیچ شکل دیگری غیر از خود کنترلی شاید نتوان بر آن مدیریت نمود. در این فصل وضعیت و شیوه‌های رسوب اطلاعات در ذهن و نوع به

یادآوری و ارائه آن به بیرون از ذهن و شیوه‌های کمک به خود مدیریتی افراد مورد بحث و بررسی قرار می‌گیرد. اطلاعات در چرخه‌ای کامل در سازمان‌ها تولید، پردازش، نگهداری و توزیع می‌شود. قبل از تولید نیز فرآیندهای خاص مدیریتی و حراستی در سازمان‌ها انجام می‌شود تا آسیب‌پذیری تولید و ادامه فرآیند را ایمن‌تر نماید.

در فصل ششم به این مهم پرداخته شده و در هر قسمت از آن وظایف صیانتی که می‌بایست توسط کارمندان حراست که همان دانشجویان فعلی می‌باشد یا باید به‌کار بسته شوند و بر اساس آن استنتاج برای شیوه برخورد با مسئله به دست آید عنوان شده است. با توجه به این‌که یکی از روش‌هایی که دشمنان می‌توانند به اطلاعات دسترسی یابند در مرحله تبلیغ می‌باشد و اگر اطلاعات با شیوه صحیحی رمزنگاری شده باشند دشمن یا توان دسترسی به اطلاعات را نخواهد داشت و یا این‌که هزینه و زمان بسیار زیادی را باید صرف نماید.

در فصل هفتم به مسئله انواع رمز و رمزنگاری و نکاتی که می‌بایست توسط نیروهای حراستی مد نظر قرار گیرد پرداخته شده است. با توجه به این‌که امروزه علاوه‌بر رمزنگاری از شیوه‌های پنهان‌سازی اطلاعات نیز بهره گرفته می‌شود در این فصل تلاش شده است به بحث استگانوگرافی که همان پوشش دادن به اطلاعات می‌باشد نیز پرداخته شود تا دانشجویان بتوانند با شیوه‌های حراستی از این روش‌ها آشنا گردند. در دوره سیستمی هر اقدامی که بخواهد انجام شود معمولاً باید از یک مدل استاندارد تبعیت نماید و امروزه برای اعمال دسترسی به اطلاعات در شیوه‌های مختلف برنامه‌نویسی از مدل‌هایی استفاده می‌نمایند که در بسیاری از مناطق دنیا به صورت استاندارد درآمده است. در فصل نهم دانشجویان با انواع مدل‌های رایج مورد استفاده در کنترل دسترسی آشنا شده و توان خود را در نظارت مربوطه در سازمان‌ها افزایش می‌دهند.

فصل دهم به قوانین موضوعه در امر فن‌آوری اطلاعات در کشور پرداخته و انواع قوانینی که برای ایفای نقش حفاظتی و حراستی دانشجویان به آن نیاز دارند مورد بحث و بررسی قرار گرفته است. در این فصل تلاش نشده است که وارد مباحث فنی حقوقی شویم ولی به میزانی که دانشجویان برای ایفای نقش صیانتی خود به آن نیاز دارند پرداخته شده است.

در انتهای کتاب در فصل یازدهم بحث آینده پژوهی و نگاه به آینده فن‌آوری نوین و نقش صیانتی در آن پرداخته شده است و دانشجویان با گذرانیدن این فصل توان آن را پیدا خواهند کرد تا با نگاه آینده پژوهانه به استقبال خطراتی که در آینده در بعد مدیریت حفاظتی بر فن‌آوری‌های نوین روبرو خواهند شد پرداخته می‌شود.

در انتهای هر فصل از کتاب سؤالاتی که در برگیرنده کل فصل بوده و با ارزش آزمونی دو نمره از بیست نمره تهیه شده است. اساتید محترم می‌توانند برای آزمون پایان کلاس از سؤالات فوق بهره‌برداری نمایند.

با امید موفقیت تمامی سربازان و حافظان نظام مقدس جمهوری اسلامی ایران.

ناصر کامیار

زمستان ۹۶