



مدیریت حفاظت فیزیکی

(نقش و وظایف انتظامات سازمان)

مؤلفین:

علی برزآبادی فراهانی

یداله کلاتی

مدیریت حفاظت فیزیکی (نقش و وظایف انتظامات سازمان) // مولفین: علیبرزآبادی فراهانی، یداله کلاتی.
تهران: مرکز آموزش و تحقیقات صنعتی ایران، ۱۳۹۲.
۱۶۰ ص.: مصور، جدول، نمودار

۹-۶۸-۰۶۸-۱۷۳-۶۰۰-۹۷۸

ساختمان های اداری- - تدابیر ایمنی

نگهبانان

نیروی انسانی- - مدیریت

برزآبادی فراهانی، علی، ۱۳۳۱-

کلاتی، یداله، ۱۳۵۷-

مرکز آموزش و تحقیقات صنعتی ایران

۴مب/۵۵۲۷ HF

۱۳۹۲

۳۵۲/۳۷۹

۳۳۱۴۶۰۲

انتشارات مرکز آموزش و تحقیقات صنعتی ایران



◀ مدیریت حفاظت فیزیکی

• مولفین: علیبرزآبادی فراهانی- یداله کلاتی

• سال چاپ: ۱۳۹۲

• نوبت چاپ: اول

• تیراژ: ۱۵۰۰ نسخه

• لیتوگرافی: نقش سبز

• چاپ و مصافی: سپیدار

• قیمت: ۶۵۰۰۰ ریال

ISBN : 978-600-173-068-9

• شابک: ۹-۶۸-۰۶۸-۱۷۳-۶۰۰-۹۷۸

• پخش: انتشارات مرکز آموزش و تحقیقات صنعتی ایران

تهران- خیابان ایرانشهر شمالی- شماره ۲۳۳

تلفن: ۸۸۳۰۰۹۷۳ و ۸۸۳۱۰۱۱۳-۲۰ نمابر: ۸۸۳۰۱۲۶۵

حق چاپ محفوظ و مخصوص ناشر است.

فهرست

۵	مقدمه ناشر
۷	پیشگفتار
۹	مقدمه
۹	ضرورت استفاده از تدابیر امنیتی در حفاظت فیزیکی
۲۵	فصل اول: دوربین های مدار بسته
۲۵	سامانه نظارت تصویری
۲۹	دوربینهای دیجیتال مدار بسته CCDP
۳۷	فصل دوم: کنترل دسترسی
۴۰	مجوز عبور
۵۷	فصل سوم: امنیت در برابر آتش
۵۷	امنیت در برابر آتش
۶۹	فصل چهارم: روشنایی
۶۹	روشنایی حفاظتی
۷۵	فصل پنجم: انتظامات
۷۵	ماموران حراست ، تاریخچه و ماموریت
۱۰۷	فصل ششم: نقش انتظامات در تکریم ارباب رجوع و مشتری مداری
۱۱۷	فصل هفتم: گشت زنی
۱۲۱	فصل هشتم: اصول نامه نگاری و گزارش نویسی
۱۲۲	اجزا و ارکان نامه های اداری
۱۲۴	گزارش نویسی

۱۲۶.....	ساختار گزارش.....
۱۳۵.....	فصل نهم: بازرسی.....
۱۴۷.....	فصل دهم: آشنایی با انواع سرقت و پیشگیری از آن.....
۱۶۱.....	فهرست منابع و مراجع.....

www.ketab.ir

مقدمه ناشر

امنیت به عنوان یکی از ارکان اساسی زندگی فردی و اجتماعی در اعصار مختلف مورد توجه اندیشمندان بوده است. در مباحث روانشناسی، جامعه شناسی و مدیریت نیز از امنیت به عنوان یکی از نیازهای اساسی بشر نام برده شده است. نقش امنیت در شکل گیری شخصیت از چنان جایگاه اساسی برخوردار است که ابراهام مازلو که یکی از پیشگامان توسعه روانشناسی انسانگرا است، سلسله مراتبی از نیازها را ارایه کرده و پس از نیازهای فیزیولوژیکی، دومین نیازی را که فرد برای رسیدن به مراتب عالی یعنی مرحله خود شکوفایی نیازمند تأمین آن در حد مطلوب است را امنیت نام برده است. نیاز به امنیت هم در سطح فردی و هم در سطح اجتماعی از بدیهات عقلی است که کلام وحی و لسان انمه اطهار علیهم السلام نیز مؤید آن است. نعمت امنیت نخستین شرط برای زندگی انسان، سکونت در یک منطقه و برای هر گونه عمران و آبادی است.

یکی از محورهای بسیار تعیین کننده در فعالیتهای علمی، تحقیقاتی و آموزشی وجود امنیت می باشد. در صورت تحقق امنیت در مقابله با تهدیدات و نفوذ و رخنه و هرچیزی که موجبات سلب آسایش را فراهم می سازد، دانشجویان، محققین و پژوهشگران می توانند در ارائه خدمات و نتایج کارکردهای خود، تأثیرات مناسب تری در فضای اقتصادی، سیاسی و فرهنگی کشور داشته باشند.

انسان متفکر آماده است بعضی از حقوق خود را نادیده بگیرد تا در ازاء این

محدودیت قدرت مانور تبهکاران را محدود نماید و اصولاً به دنبال ایجاد امنیت است. با نگاهی به آمار منتشره در خصوص دستاوردهای حفاظت فیزیکی مشخص می‌شود که در دوران فعالیت آنان امنیت با ضریب بالائی در محیط استقرار مروهون تلاش و مجاهدت شاغلین در انتظامات بوده که با جانفشانی و ایثار خود به برقراری امنیت کمک شایانی نموده‌اند.

تهدیدات بالقوه و خطراتی که از جنبه فیزیکی متوجه اماکن، تأسیسات و اموال دستگاه‌ها است بایستی با شناسایی و اقدامات مناسب، تدابیر متناسبی که می‌تواند آنها را از تهدیدها و خطرهای مصون نگاه دارد، اتخاذ کرد. البته متناسب با شرایط و ضرورت‌ها می‌توان از تدابیر ابتدایی شناخته شده همچون دیوارهای حفاظتی، سیم خاردار، سیستم روشنایی، برچک‌نمایی و ... تا سیستم‌های نوین حفاظت الکترونیکی که می‌توان ترکیبی از دوربین‌های مدار بسته، دیوارهای الکترونیکی، حس‌گرها، گیت‌های بازرسی و ... را نام برد.

به طور کلی سطح امنیت جامعه با میزان پیشرفت و شکوفایی جامعه دارای رابطه مستقیم بوده و هر نسبت که احساس امنیت افزایش یابد زمینه رشد و خلاقیت نیز افزایش می‌یابد.

تأمین حفاظت فیزیکی در مقایسه با امنیت مجازی امری بسیار ساده و دست‌یافتنی است اما مؤسسات و سازمان‌ها توجه چندانی به حفاظت فیزیکی نشان نمی‌دهند و اهمیت آن را نادیده می‌گیرند و تصور می‌کنند امنیت مجازی از اهمیت بیشتری برخوردار است و تمام امکانات به هیچ وجه نمی‌توانند مانعی بر سر راه رخنه تبهکاران به مراکز دارای اهمیت خاص ایجاد کنند. یکی از زمینه‌های ارتقاء امنیت، افزایش آگاهی سازمان‌ها و افراد می‌باشد. انتشار این کتاب گامی در جهت ارتقاء آگاهی در زمینه امنیت و حفاظت فیزیکی می‌باشد.

در پایان از آقایان علی برزآبادی فراهانی و یداله کلاتی که به تألیف این اثر همت گماشته‌اند تشکر و قدردانی می‌نماید.

علی اصغر توفیق

انتشارات مرکز آموزش و تحقیقات صنعتی ایران

پیشگفتار

امنیت به معنی مقابله با خطر و یا پیشگیری در مقابل از دست دادن چیزی است. از دیدگاه کلی، امنیت رابطه بسیار نزدیکی با ایمنی دارد. تفاوت اصلی این دو موضوع آمادگی در برابر خطرهایی است که از بیرون، یک سیستم را تهدید می‌کنند. افراد یا عواملی که شرایط حفاظتی را بر هم می‌زنند، امنیت را نقض می‌کنند.

در دنیای هماهنگ امروز، جنبه‌های مختلف امنیت، مثل امنیت اطلاعاتی، امنیت فیزیکی یا مقابله با کلاهبرداری مورد توجه قرار گرفته‌اند.

در دنیای امروز مقوله امنیت فیزیکی تا حدود زیادی نادیده گرفته می‌شود. منظور از امنیت فیزیکی تامین امنیت دفاتر شرکت‌ها یا هر مرکز یا تاسیسات و ساختمان دیگر و جلوگیری از ورود و دسترسی افراد غیرمجاز به این اماکن است چون دسترسی افراد تبه‌کار به اینگونه مراکز ممکن است به وارد آمدن خسارت و یا انهدام کامل منجر شود. گرچه امنیت فیزیکی در جهان امروز در مقایسه با امنیت مجازی در درجه دوم اهمیت قرار گرفته است اما نباید فراموش کرد که یک لحظه غفلت در زمینه امنیت فیزیکی می‌تواند یک مرکز حساس و حیاتی را به نابودی بکشاند.

تامین امنیت فیزیکی در مقایسه با امنیت مجازی امری بسیار ساده و دست یافتنی است اما موسسات و سازمان‌ها توجه چندانی به امنیت فیزیکی نشان نمی‌دهند و اهمیت آن را نادیده می‌گیرند و تصور می‌کنند امنیت مجازی از اهمیت بیش‌تری برخوردار است و تمام امکانات و منابع خود را در این راه صرف می‌کنند.

در اینجا این نکته مهم را یادآور می‌شویم که بزرگترین آسیبی که تدابیر امنیتی در معرض آن قرار دارند این واقعیت است که بسیاری از کسانی که مسئولیت و مأموریت حفاظت از سازمان‌ها و موسسات مختلف را بر عهده می‌گیرند از اطلاعات، تجربیات و مهارت لازم برای این کار برخوردار نیستند.

کتاب حاضر می‌تواند به‌عنوان یک مجموعه راهنما برای همکاران محترم حراست موسسات و شرکت‌ها، مسئولین انتظامات و دیگر عزیزانی که این وظیفه خطیر را بر عهده دارند، کاربردی و راهگشا باشد. هدف از تالیف این کتاب، رفع کمبودهای تخصصی و مهارتی کارکنان انتظامات سازمان‌ها است تا آنها بتوانند:

(الف) وظایفی را که بر عهده دارند با دقت، سرعت و کیفیت مطلوب انجام دهند.

(ب) مسئولیت‌های بیشتری را عهده‌دار گردند.

(ج) اصول نوین حفاظت فیزیکی و نگهبانی و مراقبت را فراگیرند.

(د) مهارت‌های ارتباطی و طرز صحیح برخورد رفتاری را رعایت نمایند.

(ه) به‌عنوان یک سرمایه ارزشمند، آگاه و متخصص در خدمت سازمان خود باشند.

در اینجا بر خود لازم می‌دانیم از مدیریت محترم مرکز آموزش و تحقیقات صنعتی ایران و همکاران محترمشان که در آماده‌سازی و چاپ این اثر ما را یاری نموده‌اند تقدیر و تشکر نماییم.

مؤلفین

علی رزآبادی

یداله کلانی

مقدمه

اهمیت و نقش حفاظت فیزیکی و انتظامات در ارتقاء ضریب امنیت و حفاظت از سرمایه‌های ملی و سازمان‌ها بر کسی پوشیده نیست و آموزش و بروز رسانی دانش و مهارت کارکنان واحد انتظامات نقش تعیین کننده‌ای در آمادگی و جلوگیری از تهدیدات و آسیب‌های احتمالی به اماکن و تاسیسات دارد. نقش انتظامات جهت بالا بردن ضریب اطمینان و امنیت دستگاه‌های مختلف اعم از وزارتخانه‌ها، موسسات و کارخانجات صنعتی و خدماتی بسیار حائز اهمیت می‌باشد.

مدیران سازمان‌ها باید اطمینان داشته باشند که برای به حداقل رساندن خطرات طبیعی یا انسانی که به دلیل کمبود منابع، تجهیزات و مواد روی می‌دهند تدابیر حفاظت فیزیکی مناسبی اتخاذ گردیده است. استفاده از راهکارهای علمی و سیستم‌های پیشرفته در حفاظت و کنترل اماکن امری اجتناب ناپذیر می‌باشد.

ضرورت استفاده از تدابیر امنیتی در حفاظت فیزیکی

در دنیای امروز مقوله امنیت فیزیکی تا حدود زیادی نادیده گرفته می‌شود. منظور از امنیت فیزیکی تامین امنیت دفاتر شرکت‌ها یا هر مرکز یا تاسیسات و ساختمان دیگر و جلوگیری از ورود و دسترسی افراد غیرمجاز به این اماکن است چون دسترسی افراد

تبهکار به اینگونه مراکز ممکن است به وارد آمدن خسارت و یا انهدام کامل منجر شود. گرچه امنیت فیزیکی در جهان امروز در مقایسه با امنیت مجازی در درجه دوم اهمیت قرار گرفته است اما نباید فراموش کرد که یک لحظه غفلت در زمینه امنیت فیزیکی می‌تواند یک مرکز حساس و حیاتی را به نابودی بکشاند.

در اینجا این نکته مهم را یادآور می‌شویم که بزرگترین آسیبی که تدابیر امنیتی در معرض آن قرار دارند این واقعیت است که بسیاری از کسانی که مسئولیت و مأموریت حفاظت و حراست از سازمان‌ها و موسسات مختلف را بر عهده می‌گیرند از اطلاعات، تجربیات و مهارت لازم برای این کار برخوردار نیستند. بررسی‌های به عمل آمده در آمریکا نشان می‌دهد که ۸۵ درصد از کسانی که در زمینه حراست به کار گرفته می‌شوند، تحصیلات دانشگاهی مرتبط نداشته و هیچ دوره آموزشی مرتبط را نیز طی نکرده‌اند. ۱۵ درصد بقیه نیز اگر وارد دانشگاه شده‌اند به دریافت دانشنامه نایل نیامده و دوره‌های آموزشی محدودی را پشت سر گذاشته‌اند. هنگام استخدام کارکنان حراست معمولاً پرسش‌های ساده از آنها می‌شود و مصاحبه استخدامی چندان جدی گرفته نمی‌شود. و در نتیجه کسانی که استخدام می‌شوند از کارایی و دانش لازم بی‌بهره‌اند و نمی‌توانند به خوبی از عهده مأموریتی که با آنها محول می‌شود بر آیند.



تدابیر حفاظت فیزیکی پس از ارزیابی تهدیدها و خطراتی که با آن روبرو هستید باید درباره تدابیر امنیتی که می‌تواند شما را از نوع خطرات احتمالی مصون نگه دارد تصمیم‌گیری کنید. در بسیاری از مواقع با تدابیر ابتدایی و شناخته شده همچون بهره‌گیری از دوربین‌های مدار بسته تلویزیونی و تامین روشنایی کامل در محوطه‌ای که قصد حفاظت از آن را دارید می‌توان امنیت مقدمات را فراهم آورد اما در موارد دیگر، تدابیر ویژه‌ای همچون بازرسی بسته‌های پستی ضرورت پیدا می‌کند. استفاده از راه کارهای ویژه به ارزیابی و تحقیق دقیق درباره تهدیدها و خطرات احتمالی و درک صحیح و جامع از این خطرات نیاز دارد چون بدون تحقیق و بررسی‌های لازم ممکن است تجهیزات و سامانه‌هایی خریداری شوند که کارایی لازم را نداشته باشند یا بسیار پرهزینه باشند.

اگر دفتر کار یا شرکت شما در یک مجتمع ساختمانی قرار دارد در آنصورت اتخاذ تدابیر فردی برای پیشگیری از انواع تهدیدها و خطرات از جمله حملات تروریستی نمی‌تواند چندان مؤثر واقع شود و برای کارساز بودن چنین تدابیری باید بین مسئولین همه شرکت‌ها و دفاتر موجود در آن مجتمع ساختمانی تفاهم و همکاری لازم جهت اجرای تدابیر امنیتی از جمله نصب دوربین‌های مدار بسته تلویزیونی فراهم آید. اتخاذ تدابیر جمعی افزون برای برای تامین امنیت گسترده و فراگیر از لحاظ هزینه نیز بسیار مقرون به صرفه خواهد بود. در هرگونه تدابیر امنیتی باید اقدامات لازم جهت پیشگیری و مقابله با آتش‌سوزی مورد توجه قرار گیرد و در عین حال تهدیدات و تدابیر لازم برای جلوگیری از به خطر افتادن سلامت ساکنان یا کارکنان یک ساختمان یا مرکزی که قرار است از آن حفاظت به عمل آید، اتخاذ شوند. برای افزایش کارایی تدابیر حفاظت فیزیکی نکات و مسائلی وجود دارد که رعایت آنها می‌تواند در تامین امنیت بسیار مفید واقع شود

امنیت مجازی-امنیت حقیقی

در بسیاری مواقع درک افراد از امنیت لزوماً به امنیت واقعی مربوط نمی‌شود. مثلاً، ترس از پرواز رایج‌تر از ترس از رانندگی است؛ با این حال رانندگی عموماً پرخطرتر از پرواز است. ابزارها می‌توانند انسان را به اشتباه اندازند. مثلاً در یک شبکه کامپیوتری ممکن است تعدد سیستم‌های امنیتی مختلف باعث تداخل بین آنها شود، اما کاربر احساس می‌کند، این شبکه امن است، چرا که تعداد سیستم‌های امنیتی آن زیاد است.

روی دیگر این سکه "نمایش امنیتی" است که در آن عوامل امنیتی مثل بازرسی تصویری مسافران در فرودگاه، بر اساس داده‌های آماری، افزایش چندانی را در امنیت به همراه ندارد و گاه حتی در برخی از این سیستم‌ها امنیت واقعی کاهش می‌یابد.

همچنین، اگر وجود امنیت در جایی تلقین شود، گاهاً امنیت واقعی نیز افزایش می‌یابد، حتی اگر مفهوم امنیت به اشتباه درک شده باشد. مثلاً، ممکن است بر روی تابلویی وجود دوربین مدار بسته اعلام شود و اگر حتی دوربینی هم در آنجا نباشد، برخی عوامل خرابکار به دلیل احتمال وجود این سیستم، از ورود به این محل خودداری می‌کنند. همچنین در صورت وجود سیستم‌های امنیتی واقعی مثل دزدگیر درب منزل و یا دزدگیر ماشین، اعلام وجود شان می‌تواند امنیت واقعی را چند برابر کند.

وجود این علائم هشدار دهنده باعث می‌شود سارقان و خرابکاران از وجود سیستم‌های امنیتی مطلع شده و به این ترتیب احتمال آسیب رساندن آنها کمتر می‌شود؛ چون ممکن است حتی اقدام به شروع فعالیت خود نیز نکنند.



اگر این علائم وجود نداشته باشند، ممکن است سارق به ماشین نزدیک شده، شیشه را بشکند و سپس با شنیدن صدای آژیر فرار کند. در این حالت، گرچه ممکن است که ماشین یا اشیای داخل آن سرقت نشوند، اما با اعلام وجود سیستم‌های امنیتی، و ایجاد "امنیت ذهنی" حتی ممکن بود شیشه نیز شکسته نشود و به این ترتیب امنیت مالی دارنده خود را نیز تامین گردد.

با این حال، باید بدانیم در هنگام اعلام وجود امنیت، روش‌های از بین بردن آن را اطلاع ندهیم. مثلاً اگر سارق محل نصب دزدگیر یک خانه و یا نوع آن را از قبل بداند، می‌تواند آن را از کار ببرد.

انواع امنیت

در مورد امنیت و دسته‌بندی آن مقالات و مطالب فراوانی وجود دارد. یکی از دلایل امر این است که در اکثر سیستم‌های امنیتی، "ضعیف‌ترین حلقه زنجیر"، مهمترین آنهاست. شرایط در اینجا کاملاً ناعادلانه است، زیرا مدافع باید تمام نقاط را بپوشاند، اما مهاجم فقط باید یک نقطه ضعف را جهت تمرکز و حمله انتخاب کند. برخی انواع امنیت، ترکیبی هستند. مثلاً در امنیت پرواز ترکیبی از منابع انسانی و عوامل مختلف دیگر جهت جلوگیری از تداخل در پرواز به کار گرفته می‌شوند. برخی مفاهیم مربوط به امنیت عبارتند از:

- ریسک - اتفاقی که ممکن است به از دست دادن چیزی بینجامد.
- تهدید - راهی که به ریسکی پر خطر منتهی می‌شود.
- آسیب پذیری - وضعی که باعث می‌شود چیزی یا مکانی در معرض تهدید قرار گیرد.
- سوء استفاده - بهره‌گیری از نقطه آسیب پذیر
- مقابله - جلوگیری و متوقف کردن خطر
- دفاع همه جانبه - استفاده از چندین سیستم امنیتی
- اطمینان - میزان قطعیت از مقابله با خطرات

مدیریت امنیت در سازمان‌ها

در دنیای هماهنگ امروز، جنبه‌های مختلف امنیت، مثل امنیت اطلاعاتی، امنیت

فیزیکی یا مقابله با کلاه برداری مورد توجه قرار گرفته اند. امروزه توجه به رابطه متقابل بین جنبه های مختلف امنیتی بیشتر شده است و اصطلاحاتی از قبیل "امنیت جامع" یا "مدیریت خطرات" نتیجه این نوع نگرش است. رسیدن به این نوع امنیت مستلزم گسترش امنیت تصویری مثل تکنولوژی نظارتی، و دیجیتالی کردن و ایجاد شبکه برای سیستم های امنیت فیزیکی است.

چرا سیستم های حفاظتی؟

استفاده از انواع مختلف سیستم های حفاظتی از زمانی آغاز شده که توجه به دارایی های شخصی وجود داشته است. سیستم های امنیتی ابتدایی، با اینکه از تکنولوژی مدرن امروزی بهره نمی بردند، اما در تامین امنیت افراد و دارایی های آنها موثر بوده اند.

مثلاً، سیستم امنیتی رایج در قلعه ها و باروها، محلی بوده که در اطراف قلعه بر روی برجی بلند ساخته می شده است. با جلوگیری از دسترسی افراد متخاصم به قلعه ها، امکان دفاع از آنها فراهم شده است. دفاع از قلعه تنها در یک سمت لازم بوده و پیروزی از این طریق بسیار آسان می شده است. برخی روش های ابتدایی امنیتی هنوز هم مورد استفاده قرار می گیرند. در زمان جنگ نیزه هایی که با زهر آغشته شده، درون چاله های عمیق در زمین قرار می گرفتند و این چاله ها از دید دشمن مستتر می شدند. (این روش در جنگ ویتنام نیز به کار گرفته شده است)

در بیشتر جوامع مدرن از سیستم های امنیتی با تکنولوژی جدید استفاده می شود. بسیاری از منازل، شرکت ها، فروشگاه ها و مراکز دولتی از سیستم های امنیتی الکترونیکی برای ایجاد امنیت استفاده می کنند. با بکارگیری تکنولوژی، استفاده از سیستم های امنیتی پرکاربردتر و پیاده سازی آنها آسان تر شده است. اگر چه تکنولوژی راه خود را به این سیستم ها باز کرده است، اما روش های فیزیکی باز هم برای افزایش بیشتر امنیت کاربرد دارد. مثلاً، در یک خانه ممکن است سیستم های مدرن امنیتی همراه چفت پشت درب نیز به کار رود.

امروزه سارقین باهوشتر و ماهرتر از قبل شده اند. کارشناسان عقیده دارند که داشتن هر سیستم امنیتی بهتر از نداشتن آن است. حتی ساده ترین این سیستم ها تا حدی امنیت را برای شما تامین می کنند و در نتیجه با تامین امنیت برای خانه یا فروشگاه خود

آسودگی بیشتری خواهید داشت.

راه های خاصی برای جلوگیری از ورود تبهکاران وجود دارد، مثل قفل کردن در و پنجره ها، روشن گذاشتن یک لامپ در منزل. تمام این کارها می توانند مفید باشند، اما دزدها و تبهکاران بازهم راهی برای گذر از این موانع خواهند یافت.

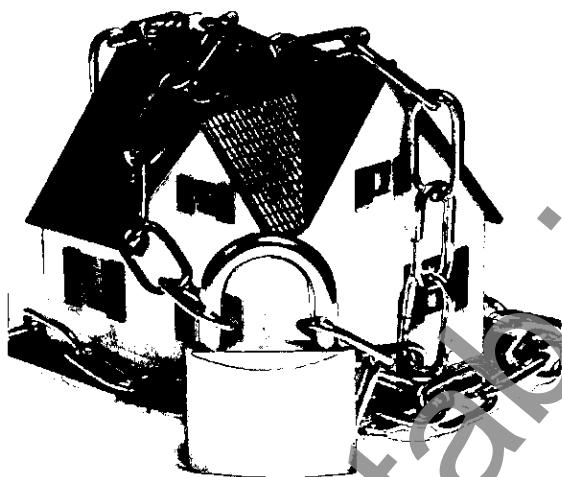
برخی سیستم های امنیتی از یک ایده بسیار ساده نشأت گرفته اند. در برخی سیستم های جدید از ایجاد صدای پارس سگ برای ترساندن دزدها استفاده می شود. در هنگام شنیدن این صدا ممکن است هیکل یک سگ ترسناک و بزرگ به ذهن سارق بیاید. شرکت رکس الکترونیک در آلمان یکی از تولید کننده های این نوع سیستم هاست. این سیستم از تکنولوژی مایکروویو بهره می گیرد.

این نوع سیستم ها روز به روز در حال تغییر می باشند و انواع و اقسام آنها توسط کمپانی های مختلف عرضه می شوند. یکی دیگر از انواع سیستم های دزدگیر سیستم مادون قرمز است. این سیستم با تشخیص حرکت به وسیله اشعه مادون قرمز به کار می افتد. این سیستم ها می توانند به طور همزمان تغییرات دما را نیز کنترل کنند. اما عیب اکثر آنها در این است که نمی توانند از دیوار عبور کنند.

در پیاده سازی گران تر این سیستم ها، در هر اتاق یک سنسور قرار می گیرد. بهترین محل برای نصب این سنسورها سقف اتاق است. این سیستم ها برای درب های اتوماتیک نیز قابل کاربرد هستند. با توجه به آنچه گفته شد، می توان گفت استفاده از سیستم های امنیتی در هر جا تاحدی لازم است. بسیاری از سیستم های مدرن از همان سیستم های پیشین الهام گرفته اند. استفاده از سیستم های امنیتی به میزان حساسیت و اهمیت موضوع، میزان هزینه، و ... بستگی دارد. مسئول امنیت یک شرکت، سازمان یا فروشگاه باید با توجه به نیازها و حساسیت، استفاده از سیستم های مختلف امنیتی و نظارتی مثل دوربین های مدار بسته، سیستم های صوتی، کنترل تردد، و ... را در نظر گرفته و همچنین هماهنگی لازم بین آنها را به وجود آورد.

حفاظت فیزیکی چیست؟

در فرهنگ لغت وبستر واژه امنیت چنین تعریف شده است. احساس امنیت، رهایی از هراس و تردید، حفاظت، حراست. تعریف ارائه شده از امنیت را می توان برای دست اندرکاران مسائل حفاظت و امنیت به معنی کنترل دسترسی نیز تعریف کرد.



در واقع همه جنبه های وظایف و شغل دست اندرکاران مسائل حفاظت و امنیت حول محور تعریف اجرا و پایش دسترسی به اطلاعات متمرکز است. دسترسی شامل دسترسی فیزیکی نیز می شود. زمان استفاده، ابعاد بهره گیری و بهترین شیوه ادغام و یکپارچه سازی حفاظت فیزیکی اطلاعات با شیوه های سنتی تامین امنیت فناوری اطلاعات، مفاهیمی هستند که دست اندکاران حفاظت و امنیت باید با آنها آشنا باشند. کارشناسان مسائل حفاظت فناوری اطلاعات نیازی به داشتن تخصص فراوان در این زمینه ندارند، چون هستند کسان دیگری که تخصص مورد نیاز را تامین می کنند؛ اما دست اندرکاران مسائل حفاظت و امنیت باید با نقاط ضعف و قوت خط مشی و راهبردهای حفاظت و حراست فیزیکی آشنا باشند. موفقیت هر زمینه حفاظت و برقراری امنیت در گرو همکاری نزدیک با اداره حفاظت فیزیکی است. چون مسئولان این اداره وظایف و مسئولیت های گسترده تری نسبت به تامین امنیت فناوری اطلاعات برعهده دارند و محترم شمردن متقابل مسئولیت ها و وظایف بین مسئولین تامین امنیت و اطلاعات و دست اندرکاران حفاظت فیزیکی می تواند ثمربخش باشد. به همین علت، آموزش فرا- قسمتی (قسمت حفاظت فیزیکی اطلاعات و حفاظت فیزیکی دیگر

اموال و دارایی‌ها) به ویژه هنگام بروز حوادث می‌تواند بسیار موثر و ارزشمند باشد. به عبارتی میتوان گفت:

حفاظت فیزیکی به مجموعه‌ای از اقدامات احتیاطی و کنترلی و استفاده از انواع مختلفی از منابع و تجهیزات، شامل نیروی انسانی، سخت‌افزار و نرم‌افزار به منظور کنترل تردد و حفاظت از اموال و دارایی‌های سازمان می‌باشد که به منظور حفظ تاسیسات یا سازمان‌ها و اماکن در مقابل خطرات طبیعی و مصنوعی بکار گرفته می‌شود.

کنترل دسترسی به معنای امنیت

هنگامی که از امنیت صحبت به میان می‌آید، اغلب مسئله چگونگی تحقق و برقراری آن مورد نظر است. در زمینه حفاظت از اطلاعات، بهره‌گیری از گذر واژه فایر وال مطرح می‌شود. در زمینه حفاظت و امنیت شخصی، جلوگیری از تجاوز و زورگیری با دوری جستن از کوچه‌های تنگ و تاریک و افراد مظنون؛ راه حل و چاره کار محسوب می‌شود. اما در زمینه حفاظت فیزیکی از فناوری اطلاعات باید ابتدا این موضوع را بررسی کرد که منظور از حفاظت چیست و صرفاً نباید به چگونگی اجرای تدابیر حفاظتی اندیشید. با تفکر درباره مقوله حفاظت از فناوری اطلاعات به این نتیجه می‌رسیم که مرکز ثقل این مقوله را کنترل دسترسی تشکیل می‌دهد. بدین ترتیب برقراری حفاظت فیزیکی در گرو کنترل دسترسی قرار دارد. گذر واژه‌ها و فایر وال‌ها، دسترسی به شبکه و اطلاعات را کنترل می‌کنند. خودداری از رفت و آمد در کوچه‌های تاریک، جان و اموال ما را از دسترسی تبهکاران دور نگاه می‌دارد. در محیط خانه‌ای با نصب قفل بر روی درها و پنجره‌ها، حفاظت و امنیت مورد نیاز تامین می‌شود. با بهره‌گیری از قفل در واقع دسترسی افراد به محوطه‌ها جلوگیری شده است. با نصب قفل بر روی در، تنها افرادی که کلید آن قفل را در اختیار دارند می‌توانند به مکان حفاظت شده دسترسی داشته باشند، در واقع دسترسی به مکان حفاظت شده را تحت کنترل در می‌آورند. از آنجا که هیچ کس پس از ساعت‌ها نمی‌خواهد از پنجره وارد خانه شود (البته نوجوانان ممکن است دیدگاه متفاوتی داشته باشند)، در نتیجه روی پنجره‌ها قفل نصب نمی‌شود و پنجره‌ها به گونه‌ای ساخته می‌شوند که هیچ کس نتواند از آنها وارد خانه شود. استفاده از زنگ خطر در منازل امروزه با استقبال فزاینده‌ای روبرو شده است. سامانه‌های زنگ خطر نیز نوعی کنترل دسترسی محسوب می‌شوند، چون از دسترسی کسانی که قصد دارند بدون آنکه کسی متوجه شود وارد یک

مکان حفاظت شده شوند جلوگیری می‌کند.

تعریفی که از امنیت ارائه شده، یعنی امنیت به معنای کنترل دسترسی، درباره مفاهیم مربوط به حفاظت از اطلاعات از جمله در دسترس قرار داشتن، مخدوش نشدن و محرمانه ماندن اطلاعات نیز صدق می‌کند.

در دسترس قرار داشتن یعنی هر زمان که ضرورت ایجاب کند باید بتوان به اطلاعات دسترسی پیدا کرد. مخدوش نشدن یعنی اینکه اطلاعات دستکاری یا تغییر نیافته باشند، به همین علت دسترسی به اطلاعات برای ایجاد تغییرات در آنها صرفاً به افراد مجاز یا برنامه‌های ویژه، تغییر یا روزآمد کردن اطلاعات محدود می‌شود.

محرمانه بودن به این معنی است که تنها افراد مجاز می‌توانند به اطلاعات دسترسی داشته باشند، بدین ترتیب محرمانه بودن، یعنی کنترل دسترسی افراد به اطلاعات جهت مطالعه آن. همه این مفاهیم، جنبه‌های گوناگون کنترل دسترسی می‌باشند. میزان اطمینان خاطر از حفاظت و امنیت اموال و دارایی‌ها به میزان و چگونگی تدابیر کنترل دسترسی بستگی دارد. هر چه تدابیر اتخاذ شده برای کنترل دسترسی دقیق تر و مطمئن تر باشند، دسترسی افراد غیر مجاز محدودتر خواهد شد. برای مثال، قفل کردن پنجره تنها درجه اندکی از اطمینان خاطر را به ارمغان می‌آورد، چون فردی که قصد ورود به خانه را دارد می‌تواند به سادگی شیشه را بشکند و وارد خانه شود، اما شکستن شیشه سر و صدا ایجاد می‌کند و این خطر وجود دارد که فرد متجاوز به دام بیفتد.

باید به این نکته توجه داشت که حفاظت بیشتر ضرورتاً به معنی دسترسی کمتر نیست، به بیان دیگر کنترل دسترسی به معنی جلوگیری از دسترسی نیست. پنجره قفل شده بی‌تردید کنترلی است که از دسترسی جلوگیری می‌کند. البته این نوع کنترل از نوع کنترل کامل برای جلوگیری از هرگونه دسترسی است. گرچه قصد این است که با قفل کردن پنجره از هرگونه دسترسی به داخل محوطه حفاظت شده جلوگیری شود. اما این گونه کنترل اطمینان خاطری در زمینه جلوگیری از دسترسی فراهم نمی‌آورد. در واقع، کنترل دسترسی است که می‌تواند بین دسترسی کامل تا عدم دسترسی در نوسان باشد. بدین ترتیب، کنترل دسترسی و نه میزان دسترسی است که می‌تواند امنیت لازم را تأمین کند. اطمینان داشتن از کارایی تدابیر اتخاذ شده برای کنترل دسترسی می‌تواند آرامش خاطر به ارمغان آورد. در اینجا به مبحث بعدی یعنی دفاع چند لایه می‌پردازیم.

دفاع چند لایه

دفاع چند لایه، میزان اطمینان به تدابیر اتخاذ شده برای کنترل دسترسی را به علت تعدد این گونه تدابیر افزایش می‌دهد.



هنگام طراحی دفاع چند لایه، مجری طرح تدابیر امنیتی را با توجه به سه عنصر پهنا، عمق و بازدارندگی به اجرا در می‌آورد.

درباره تدابیر امنیتی که در پهنای محل حفاظت شده به اجرا در می‌آیند می‌توان به پر کردن حفره‌ها و جای پاها در دیوار اطراف محل حفاظت شده اشاره کرد. هر جای پای موجود بر دیوار اطراف ساختمان حفاظت شده در واقع نوع متفاوتی از انواع آسیب‌پذیری است.

حفاظت فیزیکی در پهنا از آن جهت اعمال می‌شود که یک نوع خاجی از کنترل نمی‌تواند انواع آسیب‌پذیری‌ها را از میان بردارد. برای درک بیشتر از این موضوع برای مثال در عرصه فناوری اطلاعات، فرض کنید کسی بخواهد با بهره‌گیری از گذر واژه‌ها (logon)، از دسترسی افراد غیر مجاز به اطلاعات موجود در سامانه‌های اطلاعاتی جلوگیری کند. اما گذرواژه (logon) نمی‌تواند از طریق اطلاعاتی که فرد از طریق اینترنت آن را برای فرد دیگری ارسال می‌کند، حفاظت کند. به همین علت، برای حفاظت از اطلاعات ارسال شده از طریق اینترنت، نوع دیگری از حفاظت (برای مثال رمز نگاری) ضرورت دارد، چون حفاظت بیش تری از اطلاعات به عمل

خواهد آورد.

حفاظت فیزیکی نیز همانند حفاظت از اطلاعات است. فرض کنید، فردی بخواهد از دسترسی افراد غیر مجاز به یک نقطه حساس و مهم در یک انبار کوچک یک طبقه جلوگیری کند. این انبار یک در ورودی در جلوی ساختمان و یک در کوچک در قسمت پشت ساختمان و یک در ماشین رو دارد و پنجره های آن نیز ثابت هستند و نمی توان آنها را باز کرد. استفاده از قفل برای درهای ورودی به این انبار یک نوع از تدابیر کنترل دسترسی است، اما نصب قفل بر روی دربها از شکستن شیشه پنجره ها برای دسترسی غیر مجاز به درون انبار جلوگیری نمی کند. از این رو، نصب حفاظ بر روی پنجره ها می تواند حفاظتی کامل برای انبار فراهم آورد. اصل دوم که حفاظت در عمق است با وجود آنکه مهم ترین عامل در دفاع چند لایه محسوب می شود اما اغلب نادیده گرفته می شود برای واقع گرایی در عرصه مسائل حفاظتی، باید انسان قبول کند که امکان خطا و ناتوانی در تامین امنیت و حفاظت کامل و ناکامی در این زمینه وجود دارد. هر نوع کنترل و تدبیری که برای تامین امنیت و برقراری حفاظت به کار گرفته شده باشد دیر یا زود کارایی خود را از دست خواهد داد. از این رو، با تدابیر حفاظتی که در عمق به اجرا گذاشته می شود لایه های حفاظتی دیگری بر لایه های موجود اضافه می شود. به بیان ساده تر، یک دیوار، به چندین دیوار تبدیل می شود که یکی پس از دیگری ایجاد شده اند. در عرصه حفاظت از اطلاعات، مثال گذر واژه کاربر می تواند موضوع را روشن کند. گذر واژه برای همیشه مخفی نمی ماند، چون کاربرها عادت دارند گذرواژه خود را روی کاغذ بنویسند یا از گذر واژه های یکدیگر استفاده کنند. همه می دانند هر اندازه که کارکنان یک موسسه نسبت به مسائل حفاظتی حساس و پایبند باشند و اینگونه مسائل به آنها یادآوری، شود باز هم گذرواژه نمی تواند به تنهایی حفاظت لازم را از اطلاعات به عمل آورد. از این جهت، به این گفته مشهور متوسل می شویم، چیزی که شما در اختیار دارید، چیزی که شما می دانید و چیزی که شما هستید. گذر واژه همان چیزی است که شما می دانید و دو مقوله دیگر در واقع لایه های حفاظتی در عمق برای تشخیص هویت محسوب می شوند. حفاظت در عمق در واقع افزودن لایه های دیگر به لایه های موجود حفاظتی است، لایه ای همچون کارت هوشمند که مترادف است با آنچه که شما در اختیار دارید. چنانچه گذرواژه فاش شود،

باز همه شما از لایه حفاظتی دیگر برای کنترل دسترسی برخوردار خواهید بود. با وجود این، باید به خاطر داشت که لایه های حفاظتی نیز کاستی های خاص خود را دارند و به همین علت، برای حصول اطمینان از کارایی تدابیر اتخاذ شده برای کنترل، عملکرد این تدابیر باید مورد ارزیابی قرار گیرند. در زمینه حفاظت فیزیکی نیز اوضاع همین گونه است.

در حفاظت فیزیکی، تدابیر حفاظتی در عمق از محیط پیرامون آنچه از آن حفاظت می شود آغاز می شود و در لایه های مختلف تا مرکز محل حفاظت شده ادامه پیدا می کند. از لحاظ تئوری، هر یک از لایه های حفاظتی در واقع دایره ایست که با لایه های دیگر که در اطراف محل حفاظت شده قرار گرفته اند مرکز مشترکی دارند. البته کمتر مرکز حفاظت شده ای وجود دارد که شکل دایره باشد. لایه های حفاظتی اغلب از پیرامون محل حفاظت شده آغاز می شوند، سپس نوبت به ورودی محل می رسد، بعد قسمت خارجی ساختمان، طبقه همکف، هر یک از قسمت های مختلف، سپس هر یک از دفاتر و در مرحله آخر قفسه ها یا گاو صندوق ها.

بازدارندگی

سومین اصل در حفاظت چند لایه، بازدارندگی است. بازدارندگی به این معنی است که برای حفاظت از آنچه مورد نظر است چنان تدابیری اتخاذ شود که تلاش افراد غیر مجاز برای دسترسی به آن یا مقدور نباشد یا در صورت امکان چنان پر هزینه و خطر به دام افتادن آن زیاد باشد، که دسترسی به مکان حفاظت شده، در واقع مقرون به صرفه نباشد. یکی از اشتباهاتی که حتی در اغلب موارد مدیران حفاظت فیزیکی نیز مرتکب آن می شوند این است که هزینه و خسارت ناشی از سرقت را صرفاً برای مالک صاحب شرکت برآورد می کنند و هزینه ای را که کارمند خلاف کار ممکن است بابت سرقت پرداخت کند را نادیده می گیرند. ارزش اشیا و وسائل حفاظت شده برای مالک شرکت باید در ارزیابی خطرات احتمالی و هزینه حفاظت از آن شی در مقابل شی محاسبه شود. برای مثال هیچ کس حاضر نیست برای حفاظت از یک شی پنج هزار تومانی، ده هزار تومان بابت امور حفاظتی هزینه کند. با این وجود، باید هزینه ای که فرد خلافکار در صورت سرقت یک شی ممکن است متقبل شود را در نظر گرفت. یعنی باید دید که اگر کارمند خلافکاری دست به سرقت زد چه توانایی باید پرداخت

کند، چون چنین فردی خود نیز برای اجرای نیت خلاف خود دست به محاسبه می‌زند. برای مثال، برای جلوگیری از به سرقت رفتن سرور پنج میلیون تومانی شاید نصب یک دوربین ۱۰ هزار تومانی کفایت کند، اما نصب یک سامانه ده‌هزار تومانی برای حفاظت از یک وسیله پنج هزار تومانی مقرون به صرفه نخواهد بود.

یکی از مسائل مهم در ارزیابی تدابیر حفاظتی این است که مشخص کنیم چه مقدار از امنیت برقرار شده، سهم تدابیر در عرض و در عمق و چه مقدار آن به تدابیر بازدارنده باز می‌گردد. باید سهم هر یک از این لایه‌ها در تامین امنیت محل حفاظت شده مشخص شود تا از این طریق بتوان با ایجاد توازن بین این تدابیر که مدیریت خطر تحلیلی نامیده می‌شود بهترین تدابیر حفاظتی را برای ردیابی، بازدارندگی و ایجاد تاخیر در دسترسی‌های غیر مجاز به کار گرفت.



خطراتی که تاسیسات را تهدید می‌نماید عبارتند از:

الف) خطرات طبیعی: به آن دسته از خطراتی اطلاق می‌شود که طبیعت در به وجود آمدن آنها دخالت داشته و انسان هیچ نقشی در این مورد ندارد. مانند: زلزله، سیل، آتشفشان و طوفان.

ب) خطرات مصنوعی: به آن دسته از خطراتی اطلاق می‌شود که انسان در بوجود آمدن آنها دخالت دارد. که خود به دو دسته تقسیم می‌شوند.

- خطرات مصنوعی آشکار مانند: جنگ
- خطرات مصنوعی پنهانی مانند: جاسوسی، خرابکاری، سرقت

- سیستم های حفاظت فیزیکی:

سیستم های حفاظتی به دو دسته زیر تقسیم می شوند

۱- سیستم موانع حفاظتی شامل:

الف) موانع طبیعی: آن دسته از موانعی هستند که در طبیعت موجود می باشد. مانند:

کوه، دریا، جنگل و

ب) موانع عامل: شامل روشنایی های حفاظتی و سیستم های اعلام خطر می باشد.

ج) موانع مصنوعی: شامل - حصارها ، - محفظه ها ، - قفل ها و ...

د) موانع انسانی: موانع انسانی شامل نگهبانها می شوند. یک نگهبان قادر به انجام

وظایف زیر می باشد .

- کشف خطر - اعلام خطر - دستگیری - شناسایی

ه) موانع حیوانی: موانع حیوانی معمولاً شامل سگهای نگهبان (آموزش دیده) می شوند.