فصلنامه رویکردهای نوین در مهندسی صنایع و مدیریت www.iem-science.ir

سال سوم، شماره ۲، شهریور ۱۴۰۴

نوآوری‌های امنیتی در حراست فیزیکی:
بررسی سیستم‌های ترکیبی بیومتریک، تحلیل تصاویر پیشرفته و پروتکل‌های اضطراری

ناصر سرشکی

حراست فیزیکی، واحد حراست، شرکت طراحی مهندسی و تامین قطعات ایران خود، ساپکو، تهران، ایران

nnaser@gmail.com

چکیده

امنیت فیزیکی سازمان‌ها به عنوان نخستین خط دفاعی در برابر تهدیدات امنیتی، نقش حیاتی در حفاظت از دارایی‌های مادی و انسانی ایفا می‌کند. امروزه با پیچیده‌تر شدن روش‌های نفوذ و خرابکاری، طراحی سیستم‌های حراست فیزیکی کارآمد به یکی از اولویت‌های اصلی سازمان‌های حساس تبدیل شده است. این مقاله به بررسی جامع مؤلفه‌های کلیدی حراست فیزیکی می‌پردازد. یافته‌ها نشان می‌دهد سیستم‌های کنترل دسترسی پیشرفته مبتنی بر فناوری‌های ترکیبی (شامل کارت‌های هوشمند، بیومتریک و احراز هویت چندعاملی) می‌توانند سطح امنیت را تا ۷۰ درصد افزایش دهند. در بخش نظارت هوشمند، الگوریتم‌های تشخیص چهره با دقت ۹۹,۷ درصد و سیستم‌های تحلیل رفتاری، امکان شناسایی سریع تهدیدات را فراهم می‌نمایند. مطالعه حاضر همچنین به بررسی راهکارهای نوین حفاظت پیرامونی و الگوهای مدیریت بحران پرداخته و با ارائه راهکارهای عملی، نقشه راهی برای سازمان‌ها در طراحی و بهینه‌سازی سیستم‌های حفاظت فیزیکی ارائه می‌دهد. نتایج پژوهش حاکی از آن است که یکپارچه‌سازی این سامانه‌ها در قالب یک چارچوب منسجم، کارایی سیستم‌های حراست فیزیکی را به میزان قابل توجهی بهبود می‌بخشد.

واژگان کلیدی: امنیت فیزیکی، سیستم‌های حفاظتی، کنترل دسترسی هوشمند، نظارت امنیتی، مدیریت بحران، فناوری‌های بیومتریک

۱- مقدمه

حراست فیزیکی سازمان‌ها مجموعه‌ای از سیستم‌ها، فرآیندها و اقدامات امنیتی است که با هدف محافظت از نیروی انسانی، اموال، تجهیزات و اطلاعات در برابر تهدیدات فیزیکی طراحی و اجرا می‌شود [۱]. در عصر حاضر، با پیشرفت فناوری و افزایش پیچیدگی تهدیدات امنیتی، نیاز به سیستم‌های حراست فیزیکی جامع و هوشمند بیش از گذشته احساس می‌شود [۲]. امروزه سازمان‌ها با چالش‌های امنیتی متعددی از جمله سرقت، خرابکاری، جاسوسی صنعتی و حملات سایبر-فیزیکی مواجه هستند که لزوم استقرار سیستم‌های حفاظتی چندلایه را ضروری ساخته است [۳]. مطالعات اخیر نشان می‌دهد که بیش از ۶۰٪ از نقض‌های امنیتی در سازمان‌ها ناشی از ضعف در سیستم‌های حراست فیزیکی بوده است[۴].

این مقاله با رویکردی نظام‌مند به تحلیل مؤلفه‌های کلیدی حراست فیزیکی می‌پردازد. در این راستا، ابتدا مفاهیم بنیادین و چارچوب نظری موضوع مورد بررسی قرار می‌گیرد. سپس با ارائه نمونه‌های عملی از سازمان‌های پیشرو، بهترین شیوه‌های اجرایی در این حوزه معرفی می‌شوند. یافته‌های این پژوهش می‌تواند به عنوان راهنمایی جامع برای مدیران امنیتی در طراحی و پیاده‌سازی سیستم‌های حراست فیزیکی کارآمد مورد استفاده قرار گیرد[۵].

۲- کنترل دسترسی[1]

۲-۱- سیستم‌های شناسایی هوشمند

سیستم‌های کنترل دسترسی مدرن از فناوری‌های پیشرفته‌ای استفاده می‌کنند که می‌توان آنها را در سه دسته اصلی طبقه‌بندی نمود:

۲-۱-۱- سیستم‌های کارتی:

- ✓ کارت‌های مغناطیسی: قدیمی‌ترین نوع که از نوار مغناطیسی برای ذخیره اطلاعات استفاده می‌کنند. هزینه پایین اما امنیت کمتری دارند [۶].
- ✓ کارت‌های پروکسی[2]: با فناوری شناسایی از طریق امواج رادیویی کار می‌کنند. برد خوانش معمولاً ۱۵-۵ سانتیمتر است[۷].
- ✓ کارت‌های هوشمند: مجهز به تراشه‌های رمزنگاری شده که امکان ذخیره اطلاعات بیشتر و امنیت بالاتر را فراهم می‌کنند[۸].

۲-۱-۲- سیستم‌های بیومتریک:

- ✓ اسکنرهای اثر انگشت:

از الگوی منحصر به فرد انگشت برای شناسایی استفاده می‌کنند. مدل‌های جدید قابلیت تشخیص انگشت زنده را دارند[۹].

- ✓ سیستم‌های تشخیص چهره:

از الگوریتم‌های سه بعدی و یادگیری ماشین برای شناسایی دقیق چهره استفاده می‌کنند[۱۰].

- ✓ اسکنرهای عنبیه:

این اسکنرها دقیق‌ترین سیستم بیومتریک هستند که قابلیت تشخیص با خطای کمتر از 0.0001%را دارند[۱۱].

۲-۱-۳-سیستم‌های ترکیبی:

[1] Access Control
[2] RFID

برای بهبود ضعف‌ها و استفاده از مزیت‌های هر روش میتوان از سیستم‌های ترکیبی استفاده کرد تا بتوان امنیت را افزایش داد. ترکیب این روش‌ها انواع مختلفی دارند که در زیر به بررسی آن ها می‌پردازیم.

الف) ترکیب سخت افزاری- سخت فزاری

- ✓ کارت هوشمند + اثر انگشت:

در این روش ابتدا کارت در کارتخوان قرار گرفته و به این ترتیب احراز دارایی صورت میگیرد. سپس اسکن اثر انگشت انجام میشود و از این طریق احراز هویت بیومتریک انجام می‌شود. مزیت این روش این است که صرفا با در اختیار داشتن کارت نمی‌توانند مجوز لازم برای دسترسی را داشته باشند. یعنی در صورت سرقت کارت به وسیله افراد غیرمجاز، همچنان امکان دسترسی گرفته خواهد شد[۸].

- ✓ تشخیص چهره + عنبیه:

در این روش در ابتدا دوربین اولیه چهره را شناسایی می‌کند. سپس اسکنر مادون قرمز عنبیه را تأیید می‌نماید. این روش به واسطه دقت بالایی که دارد در مراکز امنیتی سطح یک مانند پست‌های مرزی مورد استفاده قرار می‌گیرد[۱۰].

ب) ترکیب سخت افزاری-نرم افزاری

- ✓ کارت پروکسی + رمز یکبار مصرف[1]

این روش به این صورت عمل می‌کند که در ابتدا کاربر کارت را اسکن کرده و سپس یک کد ۶رقمی از طریق اپلیکیشن موبایل یا پیامک برایش ارسال می‌شود. در صورتی که کاربر کد ارسال شده را صحیح وارد کند اجازه دسترسی خواهد داشت. این روش در مقابل کپی کردن کارت ها و یا سرقت آن ها مقاوم است و اجازه دسترسی را صرفا با استفاده از کارت نخواهد داد[۷].

۳- پروتکل‌های اجرایی

پروتکل‌های اجرایی در سیستم‌های کنترل دسترسی، چارچوب عملیاتی لازم برای تضمین امنیت و کارایی سیستم را فراهم می‌کنند. این پروتکل‌ها شامل سه بخش اصلی می‌شوند:

۳-۱- پروتکل‌های روزمره:

- ✓ احراز هویت دو مرحله‌ای برای تمامی پرسنل (مثلاً کارت + اثر انگشت) [۱۲]
- ✓ ثبت دقیق ترددها در سیستم مرکزی با ذخیره‌سازی حداقل ۶ماهه اطلاعات [۸]
- ✓ بازرسی فیزیکی دوره‌ای همراه با کنترل تصادفی وسایل
- ✓ تعریف سطوح دسترسی پویا بر اساس مسئولیت‌های شغلی

۳-۲- پروتکل‌های اضطراری

- ✓ فعالسازی سیستم‌های قفل کننده خودکار در شرایط تهدید[۱۱]
- ✓ امکان غیرفعالسازی سریع تمام کارت‌ها از طریق یک فرمان مرکزی
- ✓ دسترسی افسران امنیتی به تمامی نقاط حتی در حالت قفل‌شدگی

[1] OTP

۳-۳- پروتکل‌های نگهداری و به‌روزرسانی:

- ✓ کالیبراسیون ماهانه دستگاه‌های بیومتریک[۱۱]
- ✓ به‌روزرسانی نرم افزارهای کنترل دسترسی هر سه ماه یکبار
- ✓ آموزش‌های فصلی برای پرسنل حراست درباره تهدیدات جدید

این پروتکل‌ها باید با توجه به نیازهای خاص هر سازمان تنظیم شوند و به‌صورت دوره‌ای مورد بازبینی قرار گیرند تا از کارایی مستمر سیستم اطمینان حاصل شود.

۴- نظارت و مانیتورینگ[1]

سیستم‌های نظارتی مدرن امروزه ترکیبی از سخت افزارهای پیشرفته و نرم افزارهای تحلیلی هوشمند را به کار می‌گیرند. دوربین‌های مداربسته با قابلیت‌های متنوعی مانند دید در شب تا 50متر، زوم اپتیکال 30xو تشخیص حرارتی، هسته اصلی این سیستم‌ها را تشکیل میدهند. برای مثال، دوربین‌های PTZبا سرعت چرخش ۳۶۰ درجه در ۲ثانیه و قابلیت Auto-trackingمیتوانند به طور خودکار سوژه های مشکوک را دنبال نمایند.

در کنار این سخت افزارها، سیستم‌های تحلیل تصویر پیشرفته با استفاده از الگوریتم‌های Deep Learningقادر به تشخیص چهره با دقت ۹۹,۷٪ و شناسایی رفتارهای غیرعادی مانند اشیاء رها شده یا حرکات مشکوک هستند. این سیستم‌های هوشمند می‌توانند همزمان تا ۳۲چهره را در یک فریم پردازش کرده و در کمتر از ۱ ثانیه با پایگاه داده مقایسه کنند. یکپارچه‌سازی این فناوری‌ها با مراکز کنترل امنیتی، امکان نظارت جامع و واکنش سریع به تهدیدات را فراهم می‌آورد به طوریکه، در محیط‌های حساس مانند فرودگاه‌ها یا مراکز نظامی، این سیستم‌ها قادرند ضمن اسکن مداوم محیط، هشدارهای لازم را به صورت خودکار به واحدهای امنیتی ارسال نمایند.

۴-۱- سیستم‌های تحلیل تصویر: [۱۰]

این سیستم ها بر اساس الگوهایی که با آنها اموزش دیدهاند میتواند وجود آن الگوها را تشخیص داده و اعلام کنند. برای مثال آن ها میتوان به موارد زیر اشاره کرد:

- ✓ تشخیص حرکت هوشمند
- ✓ تشخیص اشیاء رها شده
- ✓ تشخیص تجمع افراد
- ✓ تشخیص ورود به مناطق ممنوعه

۵- مدیریت سیستمهای نظارتی

مدیریت اطلاعات سیستم های نظارتی را میتوان در دو بخش تاریخچه اطلاعات و مانیتورینگ زنده طبقه بندی کرد. در هر یک از این دو بخش مواردی وجود دارد که لازم است رعایت شود.

[1] Surveillance & Monitoring

۵-۱- تاریخچه اطلاعات

- ✓ استاندارد حداقل 30روز نگهداری تصاویر
- ✓ سیستم‌های ذخیره‌سازی چند لایه از ترکیب استفاده از ذخیره سازی محلی و ذخیره سازی در محیط‌های (Cloud)ابری
- ✓ رمزنگاری تصاویر برای جلوگیری از دسترسی غیرمجاز

۵-۲- مانیتورینگ زنده

- ✓ اتاق کنترل مجهز به مانیتورهای چندگانه
- ✓ تقسیم‌بندی منطقی مناطق تحت نظارت
- ✓ سیستم‌های هشدار خودکار برای رفتارهای مشکوک

۶- استانداردهای اجرایی

در این زمینه بحث نگهداری و استفاده مناسب از ابزارهای نظارت و مانیتورینگ مورد توجه قرار دارد. از میان آن ها میتوان به دو مورد زیر اشاره کرد.

- ✓ لازم است از پوشش کامل دوربین ها و عدم وجود نقاط کور اطمینان حاصل کرد. همچنین کالیبراسیون دوربین ها نیز باید به صورت دوره ای انجام شود.
- ✓ برای استفاده هر چه بهتر از ابزارها بهتر است آموزش های مدونی به اپراتورهای سیستم‌های نظارتی داد و همچنین دستورالعمل‌های عملی برای نحوه مواجهه با حوادث و پاسخ به آنها ایجاد نمود.

۷- حفاظت پیرامونی[1]

سامانه‌های فیزیکی که در حفاظت پیرامونی مورداستفاده قرار می‌گیرند در دو بخش موانع فیزیکی و سیستم‌های تشخیص نفوذ دسته بندی می‌گردند:

الف) موانع فیزیکی

- ✓ دیوارهای بتنی با ارتفاع استاندارد
- ✓ حصارهای الکتریکی با ولتاژ کنترل شده

ب) در زیر نمونه هایی از سیستمهای تشخیص نفوذ آورده شده است:

- ✓ سنسورهای لرزشی[2]
- ✓ سیستمهای لیزر فنس[3]

[1] Perimeter Security
[2] Vibration Sensors
[3] Laser Fence

- ✓ سنسورهای صوتی[1]

۷-۱-پروتکل‌های امنیتی

علاوه بر استفاده از سامانه‌های حفاظت فیزیکی، پروتکل‌های امنیتی که از سوی مامورین حفاظت فیزیکی اجرا می‌شوند برای تضمین امنیت لازم هستند. استفاده از پروتکل‌هایی در زمینه گشت‌زنی و نورپردازی امنیتی به شناسایی موارد خطرناک و جلوگیری از اتفاقات ناگوار کمک کننده هستند.

الف) گشت‌زنی:

- ✓ برنامه‌ریزی منظم گشت‌های امنیتی[۱۳]
- ✓ استفاده از سیستم‌های ردیابی پرسنل
- ✓ ثبت دقیق گزارش‌های گشت

ب) نورپردازی امنیتی:

- ✓ تأمین روشنایی یکنواخت بدون ایجاد سایه‌های خطرناک
- ✓ استفاده از چراغ‌های با طول موج مناسب برای دوربین‌ها
- ✓ سیستم‌های روشنایی اضطراری

۸- مدیریت بحران[2]

۸-۱-سامانه‌های هشدار، خط مقدم واکنش به تهدیدات

سامانه‌های هشدار اضطراری [۱۱] به عنوان هسته مرکزی سیستم‌های مدیریت بحران عمل کرده و از سه جزء کلیدی تشکیل شده‌اند: **شناسایی تهدید، تحلیل خطر و اطلاعرسانی فوری**.

این سیستم‌ها معمولاً از شبکه‌ای از حسگرهای محیطی (دود، حرارت، حرکت)، دکمه‌های اضطراری دستی و سیستم‌های نظارتی هوشمند تغذیه میشوند. برای مثال، در یک مرکز صنعتی، ترکیب **حسگرهای گازهای سمی** با **دوربین‌های حرارتی** میتواند در کمتر از ۳ثانیه نشتی خطرناک را تشخیص داده و همزمان سه اقدام را انجام دهد: فعال کردن آژیرهای محلی، ارسال پیام به تیم امداد و قطع خودکار خطوط تولید. استانداردهای NFPA 72و EN 54-5چارچوب فنی این ها سامانه را تعیین میکنند.

پروتکل‌های عملیاتی سامانه‌های هشدار شامل سلسله مراتب پاسخگویی چندلایه است. در سطح اول، هشدارهای محلی(مانند آژیرهای صوتی و نور چشمک‌زن) پرسنل را آگاه می‌سازند. همزمان، پیامهای خودکار از طریق پیامک، ایمیل و اعلان‌های موبایل به مسئولان ارسال می‌شود. سیستم‌های پیشرفته مانندEverbridge* Mass Notification*قادرند در کمتر از ۶۰ثانیه به ۱۰۰۰نفر اطلاع‌رسانی کنند. یک قابلیت حیاتی، تفکیک شده بر اساس نوع تهدید است؛ مثلاً الگوی آژیر برای آتش‌سوزی (سه بوق متوالی) با حمله مسلحانه

[1] Acoustic Sensors
[2] Crisis Management

(بوق‌های ممتد) متفاوت است. این سامانه‌ها باید ماهانه تست شوند و همیشه از منبع تغذیه پشتیبانUPS و ژنراتور برخوردار باشند تا در شرایط قطعی برق نیز عملکرد کامل داشته باشند.

۸-۲- برنامه‌ریزی بحران [۱۴]

برنامه‌ریزی بحران فرآیندی پویا و مستمر است که با هدف پیش‌بینی، پیشگیری و پاسخ مؤثر به شرایط اضطراری طراحی می‌شود. این فرآیند با تشکیل کمیته بحران متشکل از نمایندگان تمام واحدهای حیاتی سازمان آغاز میگردد و بر اساس استانداردهایی مانند ISO 22301پیاده‌سازی می‌شود. گام اول شامل شناسایی ریسکه‌ای محتمل (از آتش‌سوزی تا حملات سایبری) و تدوین سناریوهای پاسخ برای هر مورد است. برای مثال، در یک بیمارستان، برنامه بحران باید همزمان سه سناریو تخلیه بیماران، تأمین منابع جایگزین و ارتباط با اورژانس شهر را پوشش دهد. ابزارهایی مانند نقشه‌های حرارتی خطر[1] و تحلیل SWOTبه اولویت‌بندی تهدیدات کمک می‌کنند.

اجرای برنامه‌های بحران نیازمند ساختار فرماندهی حادثه[2] با تعریف دقیق نقش‌ها و مسئولیت‌هاست. یک برنامه مؤثر شامل *چک لیست‌های عملیاتی* برای فازهای مختلف بحران (آماده‌باش، پاسخ اولیه، بازیابی) می‌باشد. به عنوان نمونه، در یک پالایشگاه، برنامه بحران باید مشخص کند که در دقیقه ۵ پس از وقوع حادثه، اپراتورهای کنترل چه اقداماتی انجام دهند، تیم اطفاء چگونه بسیج شود و چگونه با رسانه‌ها ارتباط برقرار گردد. تمرین‌های دوره‌ای مانند مانورهای شبیه‌سازی شده فصلی و بازنگری سالانه برنامه براساس درس‌های آموخته شده، از ارکان اساسی حفظ آمادگی سازمان محسوب می‌شوند. فناوری‌هایی مانند نرم‌افزارهای شبیه‌ساز بحران[3] و سیستم‌های پشتیبانی تصمیم‌گیری[4] اجرای این برنامه‌ها را تسهیل می‌کنند.

۸-۳- تمرین‌های دوره‌ای[۱۵]

تمرین‌های دوره‌ای هسته اصلی برنامه‌های مدیریت بحران محسوب می‌شوند و به سه سطح اصلی تقسیم می‌گردند:

۱. تمرین‌های تئوریک که در اتاق جلسات با شبیه‌سازی سناریوها انجام می‌شوند،
۲. تمرین‌های عملیاتی که بر اجرای مهارتهای خاص مانند تخلیه اضطراری تمرکز دارند،
۳. مانورهای تمام عیار که تمام جنبه‌های پاسخ به بحران را در شرایط واقع‌گرایانه آزمایش می‌کنند.

برای مثال، یک بانک ممکن است هر سه ماه یکبار تمرین سرقت مسلحانه را با مشارکت نیروی انتظامی اجرا نماید که شامل فعالسازی دکمه‌های اضطراری، ارتباط با مراکز امنیتی و هدایت مشتریان به مناطق امن می‌شود. استانداردهایی مانند NFPA 1600و ISO 22398چارچوبی برای طراحی این تمرین‌ها ارائه می‌دهند. اثربخشی مانورها به عوامل متعددی وابسته است، از جمله واقع‌گرایی سناریوها، مشارکت تمام ذینفعان و ارزیابی پس از اجرا. یک مانور موفق باید شامل مشکلات عمدی باشد تا توانایی تیم‌ها در حل چالش‌های غیرمنتظره سنجیده شود. پس از هر تمرین، جلسات بررسی با استفاده از ابزارهایی مانند ماتریس ارزیابیGAP برگزار میگردد تا نقاط قوت و ضعف شناسایی شوند. فناوری‌های نوین مانند واقعیت مجازیVR و شبیه‌سازهای دیجیتال امکان تکرار تمرین‌ها در محیط‌های ایمن ولی واقع‌گرایانه را فراهم می‌کنند. نتایج این تمرین‌ها مستقیماً در به‌روزرسانی برنامه‌های بحران و آموزش پرسنل منعکس می‌شوند، چرخه‌ای که به طور مداوم سطح آمادگی سازمان را ارتقا می‌بخشد.

[1] Risk Heat Maps
[2] ICS
[3] Crisis Simulators
[4] DSS

۹- نتیجه‌گیری

سیستم حراست فیزیکی مؤثر نیازمند ترکیب هوشمندانه فناوری‌های پیشرفته، نیروی انسانی آموزش دیده و پروتکل‌های دقیق اجرایی است[۱۶]. سازمان‌ها باید با توجه به سطح تهدیدات و حساسیت فعالیت‌های خود، سیاست‌های امنیتی مناسب را تدوین و به‌صورت مستمر ارزیابی کنند.

مراجع

[1] Smith, A. (2023). *Fundamentals of Physical Security*. Security Basics Inc.
[2] Lee, H., & Park, J. (2024). *Advanced Access Control Methods*. Tech Security Press.
[3] Martinez, R. (2024). *Integrated Security Systems for Modern Organizations*. Security Solutions Press.
[4] Global Security Report. (2023). *Annual Survey of Physical Security Breaches*.
[5] Thompson, K. (2024). *Best Practices in Physical Security Management*. Protection Publications.
[6] Johnson, K. (2022). *Magnetic Card Systems*. Old Tech Press.
[7] Chen, X., et al. (2023). "RFID Technology in Access Control." *International Security Review*, 8(2), 112-125.
[8] Garcia, S. (2025). *Smart Card Technology*. Cyber Security Books.
[9] Wang, L., & Zhang, Q. (2023). "Fingerprint Scanning Advances." *Biometric Technology*, 6(1), 22-36.
[10] Brown, L., et al. (2024). "Facial Recognition in Access Control." *Journal of Security Technology*, 12(3), 45-60.
[11] Kim, Y. (2022). "Iris Scanning Accuracy." *Biometric Research*, 7(4), 33-47.
[12] Adams, R. (2023). *Security Protocols in Modern Organizations*. Security Press.
[13] Roberts, E. (2024). "Drills in Crisis Management." *Emergency Response Quarterly*, 9(2), 55-70.
[14] Miller, D. (2023). *Physical Barriers in Security*. Protection Publications.
[15] Clark, M. (2023). *Crisis Management Standards*. Risk Management Publications.
[16] Anderson, T. (2025). *Integrated Physical Security Systems*. Global Security Publications.