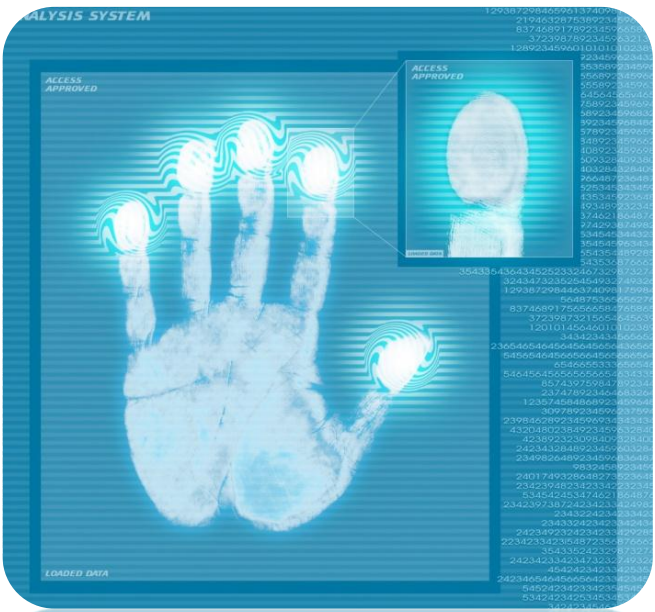
# مقدمه ای بر پدافند غیر عامل در حوزه امنیت فیزیکی و کنترل دسترسی



# فهرست

## مقدمه

اینکه نیروی انسانی فارغ از مسائل و مشکلات روزمره، چگونه ساعت‌ها در یک جای ثابت، با هوشمندی کامل نسبت به مراقبت از مواضع و یا منطقه تحت حفاظت خود اقدام نماید، جای تأمل و بررسی دارد. سامانه های حفاظت و نظارت الکترونیکی، درصورتیکه بطور صحیح طراحی و پیاده‌سازی شوند علاوه بر آنکه خیلی از آسیب ها را به حداقل می‌رسانند، به حداقل سرویس‌دهی و نگهداری نیاز دارند.

در کتابچه حاضر ابتدا به معرفی سامانه های امنیت فیزیکی و کنترل دسترسی پرداخته و سپس ملاحظات پدافندغیرعامل مربوطه بیان شده است؛ در انتها نیز به بیان اهداف، ساختار و وظایف آزمایشگاهی برای بررسی عملکرد و تست سامانه های امنیت فیزیکی و کنترل دسترسی پرداخته شده است.

# فصل ۱

## تجهیزات امنیت فیزیکی و کنترل دسترسی

تجهیزات امنیت فیزیکی و کنترل‌دسترسی شامل سامانههای دوربین مداربسته، حفاظت پیرامونی، کنترل تردد و اعلام و اطفای حریق است.

### سامانه دوربین مدار بسته[1]

این سامانه، مجموعه‌ایست که به تصویربرداری توسط دوربین‌های ویدئویی و انتقال تصاویر برای نمایش محدود می‌پردازد . تهیه تصاویر مداربسته ممکن است اهداف اصلی زیر را دنبال کند:

- حفاظت، حراست و ایمنی
- کنترل، مدیریت و نظارت
- آموزش و تحقیقات

امروزه از این سامانه برای حفاظت و نظارت بر اماکن مهم، پرتردد و یا پرخطر استفاده می‌شود. با بکارگیری این سامانه، امکان شناسایی و ردیابی آسان فراهم می‌گردد. سامانه دوربین مداربسته از بخش‌های ذیل تشکیل شده است:

---

[1] Closed Circuit Television system (CCTV)

- ایجاد تصویر دوربین[1]
- بستر انتقال تصویر[2]
- نمایش تصاویر[3]
- کنترل و ذخیره‌سازی تصاویر[4]

## سامانه حفاظت پیرامونی

روش‌های حفاظت از پیرامون به دو دسته حفاظت فیزیکی و استفاده از سامانه‌های هوشمند الکترونیکی تقسیم می‌شوند:

- حفاظت فیزیکی

جهت ایجاد حفاظت فیزیکی متناسب با استانداردهای جهانی، نیاز به موانع اولیه‌ای به شرح ذیل است:

  - مصنوعی (حصار، برج مراقبت و...)
  - انسانی
  - حیوانی (سگ‌های نگهبان)
  - عامل (مکانیکی، الکتریکی، الکترونیکی)
  - کنترل‌ها و بازدیدها (درب‌های ورود،خروج و بازدیدها)
- سامانه‌های هوشمند الکترونیکی

این سامانه‌ها را به جهت نوع کاربری می‌توان به دو دسته زیر تقسیم کرد:

---

[1] Video Capture
[2] Video Transmission
[3] Video Display
[4] Video Recording & Monitoring Control

۱. محیط داخل[1]

این سامانه‌ها برای شناسایی هر گونه نفوذ به داخل ساختمان یا ناحیه مشخصی از ساختمان به کار می روند.

۲. محیط خارج[2]

این سامانه‌ها برای تشخیص نفوذ به پیرامون یک مجموعه بکار می‌روند. غالباً در فضای آزاد مانند حصار و یا اطراف ساختمان‌های بزرگ نصب می گردند.

## سامانه‌های کنترل، بازرسی و شناسایی

این سامانه‌ها، به منظور مدیریت دسترسی و تردد انسانی (و خودرو) در مناطق تحت حفاظت و نیز مدیریت هشدارهای متناظر با رخداد حوادث به کار گرفته می‌شوند. سامانه‌های کنترل تردد را می‌توان به دو گروه کنترل تردد نفر و کنترل تردد خودرو طبقه‌بندی نمود.

- سامانه‌های کنترل تردد نفر

این سامانه‌ها با توجه به روش دریافت و قرائت اطلاعات که منتج از میزان امنیت مورد نیاز است به سه گروه تقسیم می گردند.

۱. روش‌های غیرزیستی

---

[1] Indoor
[2] Outdoor

دراین روش ها، جهت دریافت اطلاعات و شناسایی افراد از کارت های کنترل تردد، فناوری RFID[1] یا کلمه رمز [2] و PIN[3] استفاده می گردد.

۲. روش‌های زیستی[4]

در این روش‌ها، جهت دریافت اطلاعات و شناسایی افراد از مشخصات فیزیولوژیکی (اثر انگشت، چهره، شبکیه چشم، قرنیه، گوش، دما نگاشت دست یا صورت، شکل دست ، سیاهرگ دست) یا رفتاری (امضاء و صوت) افراد استفاده می گردد.

۳. روش‌های ترکیبی

در این روش‌ها، از ترکیب دو یا چند روش صرفاً زیستی، صرفاً غیرزیستی و یا تلفیقی از سامانه‌های زیستی و غیرزیستی به منظور حصول ایمنی بیشتر استفاده می گردد.

- سامانه‌های کنترل تردد خودرو

نحوه عملکرد این سامانه‌ها به این شکل است که وسیله نقلیه از مسیرهای ویژه و گیت‌های مخصوص، عبور نموده و پس از تعیین هویت خودرو برحسب اینکه مجاز به ورود است یا خیر، اجازه ورود به آن داده شده و یا از تردد آن جلوگیری می گردد. تکنیک‌های متفاوتی برای پیاده‌سازی سامانه کنترل تردد خودرو وجود دارد که مهمترین آن‌ها در ادامه مورد اشاره قرار گرفته است.

---

[1] (Radio Frequency Identification) با استفاده از ارتباطات مبتنی بر فرکانس‌های رادیویی امکان شناسایی خودکار، ردیابی و مدیریت اشیاء، انسان‌ها و حیوانات را فراهم می کند.

[2] Password

[3] Personal Identification Number

[4] Biometric

۱. سامانه‌های قرائت اطلاعات شناسایی خودرو با استفاده از امواج رادیویی[1]
۲. سامانه های قرائت اطلاعات شناسایی خودرو با استفاده از مادون قرمز[2]
۳. سامانه‌های مشابه کنترل تردد نفر؛ در این روش مشخصات خودرو روی کارت تردد آن ثبت می‌گردد.

## سامانه‌های اعلام و اطفاء حریق

سامانه‌های اعلام و اطفاء حریق خودکار، سرمایه و اطلاعات باارزش و جان پرسنل را از گزند صدمات آتش‌سوزی دور نگه خواهد داشت . این سامانه‌ها مبتنی بر آشکارساز[3]های تشخیص دود، حرارت، نشت گاز و شعله، و اعلام خطر خودکار توسط دستگاه‌های مرکزی است.

[1] RFID
[2] Infrared
[3] Detector

# فصل ۲

## ملاحظات پدافند غیرعامل

امنیت فیزیکی در محیط فناوری اطلاعات و ارتباطات در سه بعد «داده‌ها و اطلاعات»، «شبکه و ارتباطات» و «سخت‌افزارها و تجهیزات» قابل بررسی است. در ادامه توضیحات مختصری در خصوص هرکدام از این ابعاد به همراه ملاحظات مربوطه بیان خواهد گردید.

### امنیت فیزیکی داده‌ها و اطلاعات

ارتباط مستقیمی بین میزان امنیت فیزیکی و امنیت داده‌ها و اطلاعات وجود دارد. در حقیقت، هدف بسیاری از حملات و خرابکاری‌های فیزیکی در سامانه‌ها، کارگزارها و شبکه‌ها، نفوذ و دسترسی به اطلاعات و داده‌های حساس سازمان ها است. اهم حوزه‌های امنیت فیزیکی داده‌ها و اطلاعات به شرح ذیل است:

- محفظه‌ها / مخازن داده

ملاحظات

- اطلاعات طبقه‌بندی شده و محرمانه و نیز سامانه‌های اطلاعاتی حساس باید در محفظه‌ها و اتاق‌هایی نگهداری شوند که

دسترسی به آن‌ها محدود بوده و محیط پیرامون آن‌ها نیز دارای حفاظ‌های امنیتی مناسبی باشد.

- ورود به اتاق‌های کارگزارها و مخازن داده‌ها و اطلاعات منوط به اخذ مجوزهای مشخص باشد.
- تا حد ممکن نباید اطلاعات مهم در رایانه‌های شخصی نگهداری شوند. این اطلاعات حتی‌الامکان در رسانه‌های فقط خواندنی ذخیره گردند.
- محفظه‌ها/ مخازن اطلاعات از نزدیکی به مواد و تجهیزات پرخطر در امان باشند.
- اعمالی چون خوردن، نوشیدن، سیگار کشیدن و نظایر آن در مجاورت و درون محفظه‌ها و اتاق‌هایی که حاوی اطلاعات و تجهیزات اطلاعاتی هستند، ممنوع گردد.

- کلیدهای محفظه‌ها/مخازن امنیتی

در این بخش منظور از کلید انواع کلیدهای مکانیکی، شماره شناسایی خصوصی، کارت‌های دسترسی و یا ترکیبی از دو یا چند مورد فوق است.

ملاحظات

- کلیدهای محفظه‌ها/ مخازن امنیتی با توجه به بالاترین درجه حساسیت اطلاعات و یا تجهیزاتی که توسط آن قابل دسترسی هستند، محافظت شوند. کلیدهای محفظه‌ها / مخازن امنیتی باید زمانی که یکی از موارد زیر محقق شد، تغییر کنند:

۱. شواهدی از حمله و یا نفوذ رؤیت شود.
۲. تهدیدات و خطرات غیرقابل قبولی مشاهده شود.
۳. فردی که به این مکان‌ها دسترسی داشته است، تغییر کند.

## داده‌های در حال تبادل

شنود و یا استراق سمع الکترونیکی یکی از هوشمندانه‌ترین راه‌های سرقت داده‌های در حال تبادل محسوب می‌شود. امروزه مهاجمین با کمترین تجهیزات ممکن نیز قادر به شنود و رونوشت تمامی فعالیت‌های انجام شده روی رایانه قربانی هستند؛ نظیر ثبت تمامی کلیدهایی که بر روی صفحه کلید فشار داده می‌شوند، تمامی اطلاعاتی که روی یک مانیتور نمایش داده می‌شوند و تمامی فایل‌هایی که برای چاپگر[1] ارسال می‌شوند. انواع روش‌های شنود و محافظت در مقابل آن‌ها به شرح ذیل ارائه می شود:

۱. شنود از طریق کابل‌ها و سیم‌ها

سیم‌ها و کابل‌های الکتریکی، به خاطر نوع عملکردشان، جزء اولین گزینه‌های انتخابی مهاجمین برای شنود هستند. مهاجم به راحتی می‌تواند مکالمه‌ای را که بین یک جفت سیم در حال انجام است با یک پیوند ساده دنبال کند.

ملاحظات

- به طور منظم تمامی سیم‌هایی که داده‌ها را حمل می‌کنند جهت یافتن آسیب‌های فیزیکی، بازرسی شوند.
- با استفاده از کابل‌های حفاظ‌دار، از امکان نظارت غیرمجاز سیم‌ها کاسته شود.

۲. شنود از طریق اترنت[2]

ملاحظات

- از آنجاکه مهاجمین به طور گسترده از اترنت و سایر شبکه‌های محلی، برای شنود استفاده می‌کنند، اطمینان حاصل شود که سامانه‌ها، زیرشبکه‌ها و شبکه‌هایی که استفاده نمی‌شوند، دارای

---

[1] Printer
[2] Ethernet

پورت‌های کابل‌های دوسویه فعال و یا اترنت در درونشان نیستند.

- تمامی آدرس‌های IP که در شبکه‌ها مشخص شده‌اند به صورت دوره‌ای بررسی شوند تا اطمینان حاصل گردد میزبان غیرمجازی از طریق اینترنت در شبکه فعالیت نداشته است.
- از نرم‌افزارهای رصد LAN استفاده شود، تا به محض تشخیص یک بسته که از یک آدرس ناشناخته استفاده می‌کند، هشدارها فعال شود.

۳. شنود از طریق پورت‌های کمکی روی پایانه‌ها

بسیاری از ترمینال‌های کامپیوتری مجهز به یک پورت پرینتر جهت استفاده و یک پورت برای پرینتر کمکی هستند. اگر مهاجمی بتواند یک ارتباط[1] با پورت‌های چاپگر برقرار کند، می‌تواند از این پورت‌ها برای شنود استفاده کند.

ملاحظات

- اگر از چاچگر کمکی استفاده می‌شود اطمینان حاصل شود که کابل‌های دیگری به پورت چاپگر پایانه متصل نیستند.

پشتیبان داده‌ها

حفاظت فیزیکی یک پشتیبان، به اندازه حفاظت فیزیکی یک کارگزار و یا سامانه اطلاعاتی اهمیت دارد؛ زیرا در صورت خرابی، یا به سرقت رفتن پشتیبان، بخش اعظمی از اطلاعات، نابود یا به سرقت می‌رود.

ملاحظات

- پشتیبان‌ها در مکان‌هایی که توسط عموم قابل دسترسی هستند، قرار داده نشوند.

---

[1] Link

- پشتیبان‌ها ونسخه های اصلی در مکان های جداگانه نگهداری شوند.
- تمامی رسانه‌های ذخیره‌سازی به صورت « غیرقابل نوشتن [1]» ذخیره شوند.
- بمنظور حفاظت از اطلاعات نسخه‌های پشتیبان، از قفل‌های سخت‌افزاری و نرم‌افزاری استفاده شود.
- قبل از دور انداختن رسانه‌های ذخیره‌سازی، اطمینان حاصل شود که داده‌های موجود بر روی آن‌ها کاملاً پاک شده‌اند. از مطمئن‌ترین راه‌های امحاء رسانه‌های ذخیره‌سازی تخریب فیزیکی است.

- رسانه‌های غیرالکترونیکی

رسانه‌های دیجیتالی، تنها منابع ذخیره‌سازی داده‌ها نیستند که باید قبل از دور انداختن پاکسازی کامل شوند، بلکه رسانه‌های دیگری نیز وجود دارند که ممکن است حاوی اطلاعات مهمی برای مهاجمین و قفل‌شکن‌ها باشند؛ از جمله این رسانه‌ها می‌توان به نتیجه چاپی نرم‌افزارها، یادداشت‌ها، مستندات طراحی، کدهای مقدماتی، مستندات برنامه‌ریزی، خبرنامه‌های داخلی، دفترچه‌های تلفن و یادداشت شرکت، راهنمای کاربر و نظایر آن اشاره نمود. برای نمونه اگر مستند چاپ شده طراحی و معماری شبکه در دسترس باشد یک مهاجم می‌تواند با دسترسی به آن از کارگزارها، لینک‌ها و سامانه‌های مختلف مطلع شده، نقاط ضعف توپولوژی را یافته و از آن استفاده نماید.

[1] Write Protected

ملاحظات

- رسانه‌ها می‌بایست در مکان‌های امن نگهداری شوند.
- می بایست به کاربران آموزش داده شود که اطلاعات حساس را بدون رعایت موارد امنیتی به هیچ عنوان در معرض نمایش نگذارند و یا دور نیندازند.

## امنیت فیزیکی شبکه و ارتباطات

شبکه، دارای منابع فیزیکی همچون سامانه‌ها ، دستگاه‌های شبکه ( مسیریاب [1]، سوئیچ [2]، دیوارآتش [3]، هاب [4] و...)، اتاق کارگزار و تجهیزات آن، تجهیزات ذخیره‌سازی و نظایر آن می باشد. شبکه، نحوه ارتباط منابع را با یکدیگر مشخص می‌کند. به عبارت دیگر لینک‌های جریان داده را بین این عناصر مشخص می‌کند.

بنابراین امنیت فیزیکی یک شبکه در بردارنده امنیت موارد زیر است:

- منابع فیزیکی موجود در شبکه
- نحوه ارتباط‌دهی منابع فیزیکی (توپولوژی فیزیکی شبکه)
- لینک‌های موجود بین منابع فیزیکی (کابل‌کشی)
- محیط شبکه (مرز شبکه با بیرون نظیر ارتباطات اینترنت، شبکه محلی، شبکه مجازی خصوصی [5]، برنامه‌های کاربردی و ...)
- دستگاه‌های ایمنی شبکه (مسیریاب، دیوار آتش)

---

[1] Router
[2] Switch
[3] Firewall
[4] Hub
[5] VPN

مهمترین اصل در امن‌سازی منابع فیزیکی موجود در شبکه آن است که دسترسی فیزیکی به این منابع محدود و کنترل شود. بسیاری از روش‌های حفاظتی که روی یک شبکه و یا سامانه اعمال می‌شود، توسط نرم‌افزارها فراهم می گردد، ولی اگر یک مهاجم (داخلی یا خارجی) موفق شود به صورت فیزیکی به یک کامپیوتر و یا شبکه دسترسی پیدا کند، امکان محدود کردن فعالیت‌ها و نفوذهای بعدی وی به شبکه داخلی و محرمانه سازمان، بسیار مشکل خواهد شد. برخی از خطراتی که از جانب مهاجمین، سازمان را تهدید می کنند عبارتند از:

- ورود و خروج غیرمجاز
- نظارت و کنترل از راه دور
- دسترسی غیرمجاز به کامپیوترها و سرورها و منابع اطلاعاتی حساس
- سرقت داده‌ها، اطلاعات و تجهیزات
- نصب سخت‌افزارها و یا نرم‌افزارهای شنود
- تخریب و یا دستکاری ساختارها و کابل‌های ارتباطی
- سرقت کامپیوترها، کارگزارها و سایر عناصر شبکه
- نصب برنامه‌های مخرب، ویروس‌ها و کرم‌ها

پس از دسترسی به اطلاعات و منابع اطلاعاتی وضعیت به مراتب دشوارتر خواهد شد. مهاجمین قادرند اطلاعات را تغییر دهند، پاک کنند، یا اینکه اطلاعات بدست آمده را به رقبا و یا دشمنان بفروشند، آنها را در اینترنت پخش کنند و سازمان ها را از این ناحیه متحمل خسارات فراوانی نمایند.

ملاحظات

- دسترسی به شبکه داخلی از نواحی پذیرش عمومی و سایر نواحی محدود شود.
- جهت ورود به اتاق کارگزار و به طور کلی مکان‌های امن از کارت‌های شناسایی استفاده گردد.
- اتاق کارگزار به تجهیزات نظارت ویدئویی و همچنین UPS مجهز گردد.
- حتی الامکان از پنجره ها در مراکز داده استفاده نشود.
- در اطراف سامانه‌های مهم نظیر کارگزارها، حفاظ های مناسب تعبیه گردد.
- کابل‌ها در زیر زمین جاسازی شده و با پوشش‌های حفاظتی مقاوم شوند.
- مانیتورها و صفحه کلیدها در فواصل دوری از پنجره‌ها و درب‌ها و دریچه‌ها قرار داده شوند.
- کابل‌های شبکه در مقابل سامانه‌های شنود حفاظت شوند.
- صفحه نمایش، میزکار و حتی تابلوهای اتاق کنفرانس پس از اتمام کار پاک گردند.
- درایوهای فلاپی دیسک و CD-ROM و پورت های USB از روی سامانه‌های مهم حذف گردند.
- سطح امنیتی مطلوب برای Rack انتخاب گردد.

## امنیت فیزیکی تجهیزات/سخت‌افزارها

در این بخش سعی شده است محدوده دید ، کوچکتر ش ده و امنیت سامانه های رایانه‌ای و سخت‌افزارهای مربوط به آن‌ها مورد توجه قرار گیرد. نکته مهم اینست که تجهیزات و سامانه‌های اطلاعاتی مهم و با ارزش (نظیر کارگزارها، تجهیزات اطلاعاتی دارای طبقه‌بندی، نمونه‌ها و مدل‌های مهندسی، اطلاعات مالی، سیاسی، نظامی و ... ) باید در مکان‌های ایمن نسبت به مخاطرات ذیل نگهداری شوند.

- بمب الکترومغناطیسی

این بمب در اصل یک موج ضربه‌ای الکترومغناطیس است که یک میدان مغناطیسی بسیار قوی ایجاد می کند، این میدان مغناطیسی به نوبه خود، میدان الکتریکی با قدرت هزاران ولت بر متر به صورت ناپایدار در هادی‌های الکترونیک ایجاد کرده و با وارد شدن به یک دستگاه هادی جریان برق، این دستگاه را با توجه به میزان مقاومت آن بدون هیچ‌گونه سروصدا یا بر جای ماندن نشانه‌ای منهدم کرده و یا به آن آسیب می‌رساند. شناسایی عوامل حملات الکترومغناطیس بسیار دشوار است. از این روش می‌توان برای نابودکردن و ایجاد اختلال در تجهیزات الکتریکی و الکترونیکی بویژه رایانه‌ها، تجهیزات ارتباطی، رادیو یا گیرنده‌های رادار استفاده کرد.

اقدامات حفاظتی در برابر موج الکترومغناطیسی بر پایه جلوگیری از ورود، انتشار و انعکاس انرژی استوار است. بر این اساس، انرژی از قطعات، تجهیزات و ادوات، دور نگه داشته می شود.

ملاحظات

- از پوشش و موانع فلزی کافی در اطراف ادوات و تجهیزات (شیلد الکترومغناطیسی) استفاده شود.
- جلوگیری کننده‌های سریع جریان[1] در خطوط تغذیه، سیگنال و خطوط کنترلی نصب گردد؛ اتصال بین دیواره و جلوگیری کننده‌های سریع جریان و ارتباط این دو به زمین با امپدانس پایین ایجاد گردد و علاوه بر آن نقاط ورودی و محل اتصالات کنترل شود.
- هیچگاه برای شبکه از کابل‌های مسی بر روی زمین (بخصوص در بیرون ساختمان) استفاده نشود مگر اینکه با یک عایق پوشانده شده باشند.
- در سازه‌ها از فیلترهای الکتریکی و کف‌پوش‌های ضدالکتریسیته استفاده شود.

عوامل محیطی مخرب

عملکرد صحیح سامانه‌های رایانه‌ای و سخت‌افزارهای مرتبط با آن ها، شرایط محیطی و فیزیکی خاصی را می‌طلبد. عواملی همچون انفجار، آتش، دود، رطوبت، ضربه، پارازیت الکتریکی، سیل و زلزله می‌تواند تأثیرات مخرب فراوانی در عملکرد و صحت تجهیزات، سامانه‌ها و اطلاعات داشته باشد.

ملاحظات

- از پوشش‌های مستحکم جهت استفاده از تجهیزات و سامانه‌های مهم در نواحی پر خطر استفاده گردد.
- در نزدیکی سامانه‌های مهم، تجهیزات اطفاء حریق نصب و به پرسنل آموزش‌های کاربری لازم ارائه شود.

---

[1] Surge arresters

- علاوه بر رایانه‌ها، کابل‌کشی ساختمان نیز در برابر آتش‌سوزی ایمن باشد.
- با توجه به مضرات دود برای سامانه‌های رایانه‌ای و این موضوع که در برخی مواقع دود علامت خطر آتش‌سوزی است، سامانه‌های تشخیص دود در اتاق‌های حاوی تجهیزات پراهمیت، نصب و راه‌اندازی گردد.
- هرگز در اطراف مکان‌هایی که حاوی اطلاعات و سخت‌افزارهای حساس هستند، از درب‌ها و دیوارهای شیشه‌ای استفاده نشود.
- رایانه‌ها در مجاورت پنجره‌ها و یا در سطوح فوقانی اتاق‌ها قرارداده نشوند.
- از جاسازی تجهیزات سنگین در مجاورت سامانه‌های رایانه‌ای جلوگیری شود.
- حسگرهای تشخیص رطوبت در کف اتاق کارگزار و سایت‌های رایانه استفاده شود. حسگرها طوری تنظیم شوند که هنگام وجود رطوبت آسیب‌زننده به صورت خودکار جریان برق را قطع نمایند.
- برای کارگزارها و سایر سامانه‌های اطلاعاتی مدار الکتریکی جداگانه‌ای به همراه یک محافظ الکتریکی در نظر گرفته شود تا از ایجاد پارازیت جلوگیری شود.

# فصل ۳

## آزمایشگاه امنیت فیزیکی و کنترل دسترسی

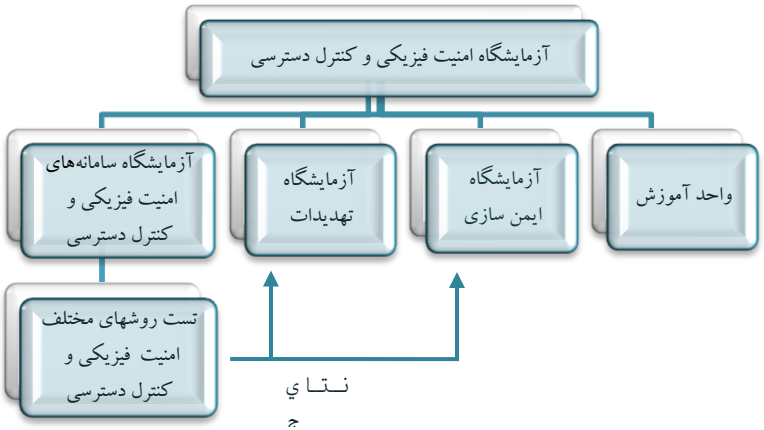
با توجه به اهمیت تأمین امنیت فیزیکی و کنترل دسترسی در برقراری امنیت فضای سایبر نیاز به وجود آزمایشگاه امنیت فیزیکی و کنترل دسترسی بیشتر احساس می شود.

### اهداف آزمایشگاه

- بررسی سامانه‌های مختلف امنیت فیزیکی و کنترل دسترسی، دسته‌بندی آن‌ها و ارائهی گواهینامه
- بررسی آسیب‌پذیری ها و تهدیدات سامانه های امنیت فیزیکی و کنترل دسترسی
- بررسی روش های ایمن سازی سامانه های امنیت فیزیکی و کنترل‌دسترسی
- ارائه خدمات مشاورهای و آموزشهای مرتبط در زمینه امنیت فیزیکی و کنترل دسترسی

## ساختار پیشنهادی آزمایشگاه

آزمایشگاه امنیت فیزیکی و کنترل دسترسی برای رسیدن به اهداف مذکور شامل واحد های ذیل خواهد بود:




ساختار آزمایشگاه امنیت فیزیکی و کنترل دسترسی

- آزمایشگاه سامانه‌های امنیت فیزیکی و کنترل دسترسی

سامانههای امنیت فیزیکی و کنترل دسترسی شامل سامانه های دوربین مدار بسته، کنترل تردد، حفاظت پیرامونی و اعلام و اطفای حریق است. نکته قابل توجه در سامانه‌های فوق این است که یکی از چالش‌ها در حوزه امنیت فیزیکی، بررسی میزان واقعی بودن ادعای سازندگان این تجهیزات است. در نتیجه وجود یک آزمایشگاه برای تأیید مشخصات ارائه شده توسط سازندگان این تجهیزات، ضروری است.

- آزمایشگاه تهدیدات

در این بخش در خصوص آسیب پذیری سامانه‌های امنیت فیزیکی در برابر تهدیدات و میزان مقاومت آن ها در برابر حملات، مطالعات و تحقیقات لازم صورت می گیرد. هدف از این قسمت اجرای حملات جهت بررسی وضع جاری و تشخیص ضعف سامانه‌های امنیت فیزیکی و کنترل دسترسی و کارایی راهکارهای پیشنهادی است.



کارکرد های این آزمایشگاه به قرار ذیل خواهد بود:

- مدلسازی و شبیه سازی انواع تهدیدات و حوادث طبیعی و غیرطبیعی بر روی سامانه‌های امنیت فیزیکی و کنترل دسترسی
- شبیه‌سازی انواع حملات شناخته شده بر روی سامانه های امنیت فیزیکی و کنترل دسترسی

- آزمایشگاه ایمن‌سازی

هدف این بخش، بررسی، پیشنهاد و اجرای راهکارهایی برای مقاوم‌سازی، جبران و بازسازی سامانه امنیت فیزیکی و کنترل دسترسی است.

راهکارهای مقاوم سازی، راهکارهایی از پدافند غیرعامل است که ناظر به پیشگیری و جلوگیری از حملات و صدمات ناشی از آن است.

مفهوم راهکارهای جبران، راه‌حل‌هایی است که منجر به راه اندازی مجدد و یا جایگزینی خدماتی از سامانه امنیت فیزیکی و کنترل دسترسی است که در حین حملات حداقل نیازهای ضروری را برآورده نماید و منظور از راهکارهای بازسازی، روش‌هایی است که درصورت از کار افتادن سامانه امنیت فیزیکی و کنترل دسترسی بتوان با حداقل هزینه و زمان، سامانه را به حالت اول بازگرداند.

با استفاده از این آزمایشگاه کارایی و امنیت سامانه ها پس از اعمال راه‌حل های امنیتی با کمک کارشناسان بخش تهدیدات ارزیابی خواهد شد.

- واحد آموزش

در این واحد به آموزش و تربیت متخصصین برای واحدهای مختلف آزمایشگاه و برگزاری دوره‌های آموزشی تخصصی با هدف آگاه‌سازی و هماهنگی پرداخته می شود. همچنین این واحد مسئولیت آموزش همگانی، اطلاع‌رسانی عمومی و فرهنگ‌سازی در راستای اهداف پدافند غیرعامل در حوزه امنیت فیزیکی و کنترل دسترسی را نیز بر عهده خواهد داشت.