به نام خدا

فهرست :

مقدمه

تجربه جنگ‌های متعدد در تاریخ بشر نشان داده است که یکی از راه‌های مورد استفاده برای درهم‌شکستن مقاومت، حمله به مراکزی است که گرچه الزاماً نظامی نیستند، اما آسیب‌رساندن یا انهدام آن ها می‌تواند توان دفاعی طرف مقابل را بشدت کاهش دهد. این حربه از هزاران سال پیش تاکنون مورد استفاده مهاجمین بوده است؛ روش هایی همچون انهدام زیرساخت های تأمین آب شرب و مواد غذایی، بمباران و انهدام انواع تأسیسات شهری و زیربنایی از شیوه های متداول اعمال فشار در جنگ‌ها بشمار می رود. بنابراین یکی از مسائل مهم در تدوین راهبردهای دفاع ملی، نحوه دفاع از زیرساخت‌هایی است که آسیب‌دیدن آنها در شرایط جنگی می‌تواند توان مدیریتی و دفاعی کل کشور را تحت تأثیر قرار دهد. با توجه به رشد روزافزون کاربردهای فناوری اطلاعات و ارتباطات[۱] و ناگزیر بودن تمامی کشورهای جهان در تلاش برای استفاده هر چه مناسب‌تر از امکانات و قابلیت‌های متعدد آن، طبیعی است که این فناوری در بسیاری از زیرساخت‌های حیاتی به صورت گسترده مورد استفاده قرار گیرد. به همین دلیل بررسی نحوه استفاده از مخاطرات ناشی از این فناوری نیز

[۱] ICT(Information and Communication Technologies)

به یکی از مسائل مورد علاقه کشورهای مختلف تبدیل شده است؛ لذا وجود پایگاه دانش مخاطرات‌امنیتی حوزه فناوری‌اطلاعات و ارتباطات در زیرساخت های حیاتی کشور، اجتناب ناپذیر می باشد. در این کتابچه سعی شده است ضمن پرداختن به مفاهیم و اجزاء یک سیستم خبره و الزامات فنی و معماری جهت پیاده سازی یک پایگاه دانش بعنوان یکی از مهمترین بخش های سیستم خبره،یک دسته بندی اساسی جهت احصاء مخاطرات امنیتی در حوزه های مختلف فناوری اطلاعات و ارتباطات ارائه گردد.

فصل ۱ - مقدمه‌ای بر پایگاه دانش و سامانه‌های خبره

هدف از این بخش آشنایی کلی با تعریف، جایگاه و کارکرد پایگاه دانش و سامانه‌های خبره و نقش این سامانه ها در افزایش توان مدیریت و تصمیم گیری می باشد.

❖ هوش مصنوعی، پایگاه دانش و سامانه‌های خبره

شاخه هوش مصنوعی در علوم رایانه از اواسط دهه پنجاه میلادی با هدف شبیه‌سازی فعالیت‌های ادراکی انسان و نیز ساخت ماشین‌های هوشمند پایه‌گذاری شد. دو زمینه «منطق برای اثبات قضایای ریاضی» و «سامانه‌های مبتنی بر دانش» در سال‌های ابتدایی توسعه هوش مصنوعی مورد توجه بیشتری قرار گرفتند. در زمینه سامانه‌های مبتنی بر دانش، سامانه‌هایی مانند مشاورین خودکار، دستیاران رایانه‌ای و مشاورین مجازی توسعه داده شدند. سامانه‌های خبره نیز زیرمجموعه‌ای از سامانه‌های مبتنی بر دانش محسوب می‌شوند.

"برای اینکه یک برنامه وظیفه پیچیده‌ای را به خوبی انجام دهد، می‌بایست راجع به محیطی که در آن عمل می‌کند، دانسته‌هایی داشته باشد. "

مفهوم ذکر شده، ایده هسته اصلی سامانه‌های مبتنی بر دانش است که سامانه‌های خبره نیز قسمتی از آن محسوب می‌شوند. این سامانه‌ها عموماً برای تبدیل داده به دانش و نگهداری دانش مورد نیاز سامانه به صورتی که قابلیت پردازش داشته باشند استفاده می شوند. سامانه‌های مبتنی بر دانش علاوه بر داده‌های معمولی، ارتباطات معنایی بین داده‌ها را نیز نگهداری کرده و از آنها هنگام کار برای تحلیل داده‌ها استفاده می‌کنند. بصورت کلی به این مجموعه داده‌ها و ارتباطات معنایی میان آنها پایگاه دانش گفته می‌شود. البته از «پایگاه دانش» در تمامی سامانه‌های مبتنی بر دانش استفاده می‌شود. برای متمایزکردن سامانه‌های خبره از سایر سامانه‌های مبتنی بر دانش، معمولاً توانایی ارائه توضیح و یا توجیه‌نمودن آنچه که سامانه به عنوان نتیجه به آن رسیده است، به عنوان شاخص در نظر گرفته می‌شود.

❖ **تعریف سامانه خبره**

سامانه‌های خبره دسته‌ای از برنامه‌های رایانه‌ای هستند که قادر به انجام فعالیت‌هایی مانند راهنمایی، تحلیل، دسته‌بندی، مشاوره، طراحی، تشخیص، کاوش، پیش‌بینی، ایجاد مفاهیم، شناسایی، تفسیر، توجیه، یادگیری، مدیریت، کنترل، برنامه‌ریزی، زمان‌بندی و آزمایش هستند. این برنامه‌ها معمولاً به مسائلی می‌پردازند که حل آنها نیاز به استفاده از متخصصین انسانی دارد.

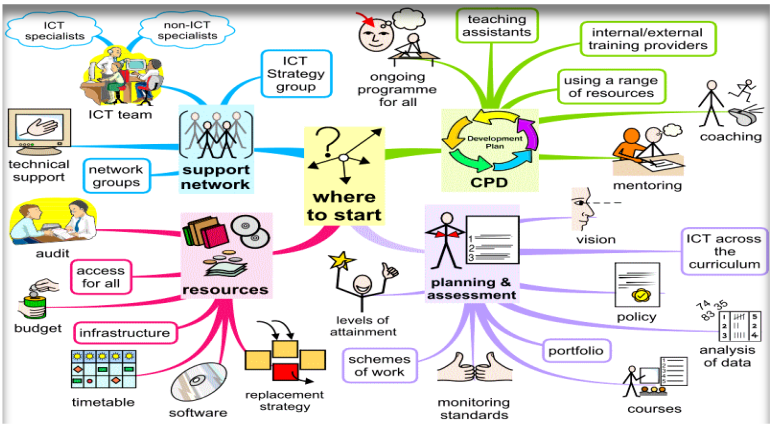
❖ ویژگی‌های سامانه‌های خبره

۱. این سامانه‌ها در سطحی که معمولاً هم‌طراز عملکرد یک متخصص انسانی شناخته می‌شود عمل می‌کنند.

۲. این سامانه‌ها به شدت به یک رشته یا زمینه خاص وابستگی دارند. به بیان دیگر اطلاعات وسیعی در یک زمینه تخصصی خاص دارند.

۳. این سامانه‌ها می‌توانند درباره استدلال خود توضیح دهند. به عبارت دیگر سامانه خبره زمانی به عنوان یک ابزار مفید و کارآمد در نظر گرفته می‌شود که قادر باشد تحلیل و استنتاج خود را توضیح داده و توجیه نماید.

۴. اگر اطلاعاتی که سامانه با آن کار می‌کند، احتمالی یا غیرقطعی باشد، سامانه می‌تواند این احتمال و عدم قطعیت را در مراحل استنتاج در نظر بگیرد.



❖ **مؤلفه‌های اصلی سامانه‌های خبره**

۱- پایگاه دانش

پایگاه دانش بخش اصلی سامانه خبره را تشکیل می‌دهد و حقایق و قوانین جمع‌آوری‌شده از خبره‌های انسانی در زمینه تخصصی سامانه خبره را در بر دارد. این قوانین در فرم ساده خود به صورت مجموعه‌ای از گزاره‌های "اگر – آنگاه" بیان می‌شوند.

۲- موتور استنتاج

موتور استنتاج یکی دیگر از مؤلفه‌های یک سامانه خبره است که وظیفه بکارگیری اطلاعات موجود در پایگاه دانش را برعهده دارد. این مؤلفه که مفسر قانون نیز نامیده می‌شود، وظیفه دارد با اعمال قوانین روی داده‌های موجود، مسیرهای منطقی منتهی به حل مسائل ارائه‌شده به سامانه خبره را بیابد.

موتور استنتاج تعیین می کند که قسمت شرطی کدام قاعده توسط حقایق موجود ارضا شده است.

۳- حافظه کوتاه مدت

موتور استنتاج دارای حافظه‌ای می‌باشد که معمولاً کوتاه‌مدت خوانده می‌شود. بر خلاف پایگاه دانش که می‌تواند به عنوان یک حافظه بلندمدت تلقی گردد، سامانه خبره از حافظه کوتاه‌مدت برای نگهداری مراحل مختلف یافتن پاسخ و مسیر طی‌شده از سئوال به جواب استفاده می‌کند. این حافظه کوتاه‌مدت در برگشت‌های رو به عقب در مسیر حل مسأله و تشریح راه‌حل، پس از یافتن آن مورد استفاده قرار می‌گیرد.

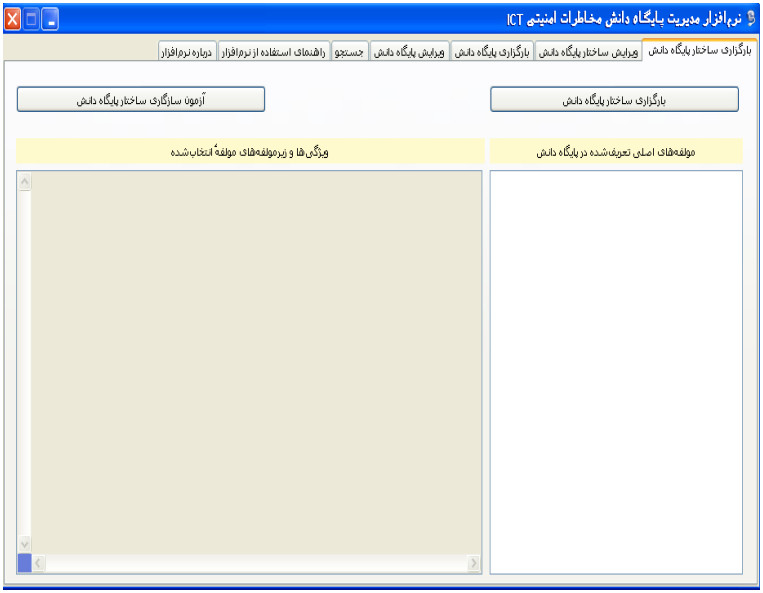
٤- رابط کاربر

این رابط ارتباط میان کاربر و سامانه را برقرار می‌کند و به کاربر اجازه می‌دهد پرسش‌های خود را در اختیار سامانه خبره قرار دهد. علاوه براین با استفاده از این رابط، سامانه پاسخ‌های خود را به کاربر باز می‌گرداند و یا در صورت نیاز، اطلاعات بیشتری از کاربر دریافت می‌نماید.

❖ **نمونه ساختار واسط کاربری**

در این بخش بمنظور آشنایی با یک نرم‌افزار مدیریت پایگاه دانش، واسط کاربری یک نمونه از چنین نرم افزاری بررسی و بخش های اصلی آن مورد تحلیل قرار گرفته است.

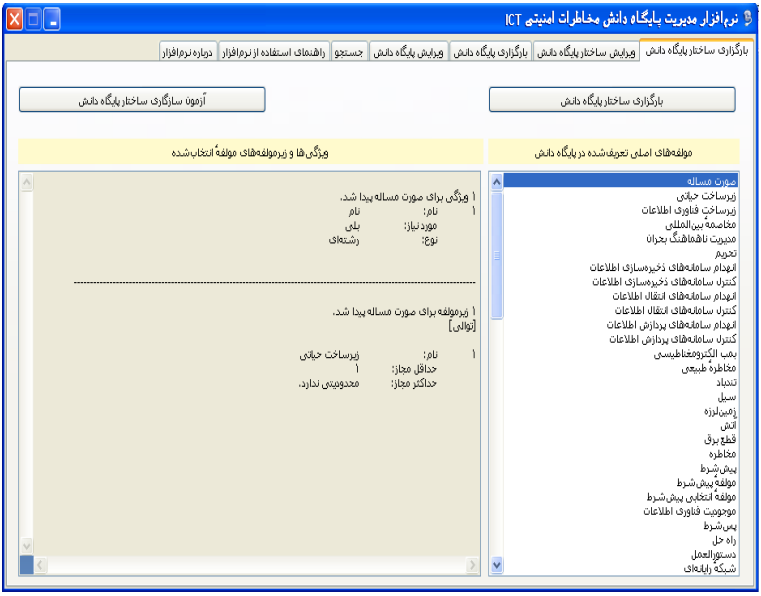
واسط کاربری نرم‌افزار مدیریت پایگاه دانش مخاطرات امنیتی مورد بررسی از پنج قسمت اصلی تشکیل شده است. این پنج قسمت که توسط یک انتخاب‌کننده در قسمت بالای واسط کاربری نرم‌افزار قابل استفاده هستند عبارتند از بارگزاری ساختار و ویرایش ساختار پایگاه دانش، بارگزاری و ویرایش پایگاه دانش و بخش درباره نرم‌افزار.



نمای صفحه شروع واسط کاربری نرم‌افزار مدیریت پایگاه دانش مخاطرات امنیتی ICT

بارگزاری ساختار پایگاه دانش و آزمون سازگاری آن

در صفحه بارگزاری ساختار پایگاه دانش، امکان بارگزاری پرونده حاوی ساختار طراحی‌شده و همچنین آزمون سازگاری آن وجود دارد.



نمایی از صفحه بارگزاری ساختار پایگاه دانش

ویرایش ساختار پایگاه دانش

در صفحه ویرایش ساختار پایگاه دانش امکانات مختلفی برای ویرایش ساختار پایگاه دانش در نظر گرفته شده است.

نمایی از صفحه ویرایش ساختار پایگاه دانش

جستجو روی پایگاه دانش

یکی دیگر از امکانات تعبیه‌شده، امکان جستجو در پایگاه دانش برای یافتن مخاطرات مربوط به یک یا چند مؤلفه از مؤلفه‌های معرفی‌شده به مدل است.

همانگونه که در تصویر نیز مشخص است، در این صفحه امکان جستجو برای یافتن مخاطراتی که به صورت جداگانه در پیش‌شرط یا پس‌شرط آنها یک یا چندین مؤلفه نقش بازی می‌کنند، فراهم شده است. بعنوان مثال در شکل ذیل یک پرس‌وجو برای یافتن مخاطراتی که مؤلفه «هاب[۱]» در ایجاد آنها نقش اصلی ایفا می‌کند یا به دلیل وجود آنها ممکن است تأثیراتی روی سامانه تشخیص نفوذ وجود داشته باشد، و نتیجه آن نمایش داده شده است.

نمایی از صفحه جستجو در پایگاه دانش

[۱] Hub

فصل ۲ - الزامات طراحی و تولید

در این فصل سعی شده است تا به ویژگی‌های مورد انتظار از پایگاه دانش مخاطرات امنیتی از منظر پدافند غیرعامل، اشاره گردد:

۱. پایگاه دانش مخاطرات باید بگونه‌ای طراحی شود که برای ثبت اطلاعات مربوط به مخاطرات امنیتی فناوری اطلاعات و ارتباطات و همچنین شرایط محیطی رخداد آنها در زیرساخت‌های کشور قابل استفاده باشد و پس از تولید دانش مورد نیاز توسط متخصصین یا متولیان این فناوری در هر زیرساخت و ورود دانش به آن، قابل استفاده در مراکز تأمین کننده امنیت همچون SOC[۱] و گروه‌های پاسخگویی به رویدادهای امنیتی[۲] و مقابله با شرایط اضطراری و احیاء سیستم ها باشد.

۲. از آنجا که از منظر پدافند غیرعامل نهایتاً پایگاه دانش باید به پایداری کشور در شرایط خاص کمک کند، لازم است بتوان از این پایگاه دانش برای اتخاذ تصمیم‌ها و یا راهکارهای مناسب در شرایط مختلف استفاده نمود. از آنجا که متناسب با اندازه و مشخصات زیرساخت فناوری اطلاعات و ارتباطات استفاده شده در

---

[۱] Security Operation System

[۲] CERT (Computer Emergency Response Team)

یک زیرساخت حیاتی، ممکن است دانش انبوهی ذخیره شود و سامانه می‌بایست با استفاده از موتورهای استنباطی و با تکیه بر قدرت پردازشی ماشین بتواند این دانش را تجزیه و تحلیل نماید، لذا این پایگاه دانش باید بگونه‌ای ایجاد شود که موتورهای استنباطی آن یا هر سامانه خبره بتواند از آن برای ارائه خدمات بمنظور کمک به تصمیم‌گیری منطقی تر استفاده کند.

۳. مانند سایر کاربردهای مبتنی بر سامانه‌های خبره، در این کاربرد نیز پایگاه دانش باید بگونه‌ای طراحی و ایجاد شود که بتواند با استفاده از یک موتور خبره و قطعات دانش ذخیره شده خود، در صورت امکان دانش اضافه موجود در قطعات دانش را استخراج و از آن برای پردازش بیشتر و تولید دانش افزوده استفاده کند.

❖ **کارکردهای مورد نیاز**

۱. پایگاه دانش هدف می بایست زیرساخت‌محور باشد.
۲. ساختار سامانه ثبت اطلاعات پایگاه دانش هدف می بایست بگونه ای طراحی شود که توانایی ذخیره اطلاعات بر مبنای زیرساخت‌ها و از منظرهای مختلف را داشته باشد.
۳. پایگاه دانش هدف می بایست انعطاف‌پذیر باشد.

❖ **الزامات معماری پایگاه دانش**

۱. طراحی یک ساختار مناسب برای حفظ ارتباط معنایی میان مؤلفه‌های دانش
۲. تأثیر تعداد کاربران بر نحوه مدیریت و نگهداری پایگاه دانش
۳. کنترل دسترسی کاربران و روال‌های استنتاجی به دانش ذخیره‌شده
۴. استفاده از رمزنگاری برای ذخیره اطلاعات در پایگاه‌دانش
۵. مکانیزم حفاظت از همسازی دانش
۶. مکانیزم به‌روزرسانی پایگاه دانش
۷. سازگاری پایگاه دانش با سایر نرم‌افزارها

فصل ۳ - فهرست مخاطرات امنیتی شناسایی‌شده در حوزه ICT

نخستین گام در جهت افزایش ضریب امنیتی و توان بازدارندگی، ایجاد پایگاه دانش مخاطرات امنیتی حوزه های مختلف فناوری اطلاعات و ارتباطات می باشد. اولین قدم در این راه شناسایی و احصاء مخاطرات هر حوزه توسط خبرگان است. این مخاطرات می‌توانند برای زیرساخت‌های حیاتی کشور مشکل ایجاد کرده و موجب کاهش بازدارندگی، افزایش آسیب‌پذیری و یا اختلال در فعالیت‌های ضروری در گستره ملی گردند. در ادامه سعی شده است مخاطرات مرتبط با حوزه های مختلف فناوری اطلاعات و ارتباطات دسته بندی و اجمالاً مورد بررسی قرار گیرند.

❖ مخاطرات امنیتی ICT از منظر مخاصمات بین‌المللی

در این بخش به آن دسته از مخاطرات امنیتی حوزه ICT که ممکن است بر اثر یک مخاصمه بین‌المللی ایجاد شوند؛ پرداخته می‌شود. از این منظر می‌توان مخاطرات ICT ناشی از مخاصمات بین‌المللی را به صورت ذیل دسته بندی نمود:

۱. مدیریت نامتمرکز و ناهماهنگ رویدادهای امنیتی (مدیریت بحران)
۲. تحریم‌های بین‌المللی
۳. انهدام سامانه‌های ذخیره‌سازی اطلاعات
۴. کنترل سامانه‌های ذخیره‌سازی اطلاعات
۵. انهدام سامانه‌های انتقال اطلاعات
۶. کنترل سامانه‌های انتقال اطلاعات
۷. انهدام سامانه‌های پردازش اطلاعات
۸. کنترل سامانه‌های پردازش اطلاعات
۹. بمب الکترومغناطیسی (EMP[۱])

[۱] ElectroMagnetic Pulse

❖ مخاطرات امنیتی ICT از منظر مخاطرات طبیعی

مخاطرات طبیعی اغلب ضربات و آسیب‌های جدی به زیرساخت های فناوری اطلاعات و ارتباطات وارد می‌کنند. این سوانح ممکن است نتیجه تحولات جوی، زمین‌لرزه و یا اقیانوسی باشند.

خرابی‌های شدید ناشی از وقایع طبیعی می‌توانند خسارت‌های بلندمدتی را در تأسیسات زیربنایی از جمله سیستم‌های مخابراتی ایجاد کنند. تندباد، سیل، زمین‌لرزه، آتش، قطع برق و صاعقه برخی از این مخاطرات می باشند.

❖ مخاطرات امنیتی حوزه های مختلف فناوری اطلاعات و ارتباطات

بطور کلی مخاطرات عمده مترتب بر زیرحوزه‌های فناوری اطلاعات و ارتباطات را می‌توان به پنج دسته تقسیم نمود:

۱. قطع دسترسی
۲. دیده‌بانی غیرمجاز اطلاعات و یا فعالیت‌ها[۱]
۳. افشاء غیرمجاز اطلاعات ذخیره شده و یا در حال انتقال[۲]
۴. تغییر یا تخریب غیرمجاز برنامه‌های رایانه‌ای، پایگاه داده‌های شبکه‌ای، اطلاعات ذخیره‌شده و یا قابلیت‌های موجود

---

[۱] Unauthorized Monitoring
[۲] Unauthorized Disclosure

۵. دستکاری رایانه‌ها، شبکه‌های رایانه‌ای، سامانه‌های ارتباطی راه دور یا ماهواره‌ها به گونه‌ای که به تقلبات مالی و یا هرگونه جرم فضای مجازی منجر شود.

همچنین مخاطرات امنیتی از منظر فناوری اطلاعات و ارتباطات را می‌توان به پنج زیرحوزه تقسیم‌بندی نمود:

۱. مخاطرات مربوط به ایستگاه‌های کاری
۲. مخاطرات مربوط به شبکه‌های رایانه‌ای (ارتباطات سیمی)
۳. مخاطرات مربوط به ارتباطات راه دور (ارتباطات بی‌سیم)
۴. مخاطرات مربوط به ماهواره‌ها
۵. مخاطرات ناشی از ارتباطات فیبر نوری

۱.مخاطرات مربوط به ایستگاه‌های کاری

- مخاطرات مرتبط با دسترسی فیزیکی
- مخاطرات مرتبط با دسترسی منطقی
- مخاطرات مرتبط با سخت‌افزارها
- مخاطرات مرتبط با سیستم عامل
- مخاطرات مرتبط با نرم‌افزارهای کاربردی
- مخاطرات مرتبط با داده‌ها

۲.مخاطرات مربوط به شبکه‌های رایانه‌ای (ارتباطات سیمی)

- مخاطرات امنیتی دسترسی فیزیکی به شبکه
- مخاطرات امنیتی دسترسی منطقی به شبکه
- مخاطرات امنیتی معماری شبکه
- مخاطرات امنیتی تجهیزات شبکه
- مخاطرات امنیتی مدیریت و نگهداری شبکه
- مخاطرات امنیتی سرویس‌های شبکه
- مخاطرات امنیتی ساختار آدرس‌دهی و مسیریابی شبکه

۳. مخاطرات مربوط به ارتباطات راه دور (ارتباطات بی‌سیم)

- مخاطرات امنیتی شبکه‌های محلی بی‌سیم (WLAN[۱])
- مخاطرات امنیتی تلفن‌های سلولی[۲]
- مخاطرات امنیتی تلفن‌های بی‌سیم[۳]
- مخاطرات امنیتی شبکه‌های رادیویی دید مستقیم[۴] شامل:
  - سیستم‌های ظرفیت بالای ثابت یا متحرک که در trunk کردن نقطه به نقطه (جریان‌های متفاوتی از داده و صدا که بر روی یک کانال ارتباطی مالتی‌پلکس شده‌اند) کاربرد دارد.

---

[۱] Wireless Local Area Network

[۲] Cellular phone

[۳] Cordless phone

[۴] Line of sight radios

- سیستم‌های ظرفیت پایین متحرک، نیمه متحرک و یا ثابت رادیویی که در مدیریت خطوط صدای نیمه دو طرفه[۱] کاربرد دارد.

- مخاطرات امنیتی شبکه‌های رادیویی بسته‌ای[۲]
- مخاطرات امنیتی سامانه‌های پی‌جو[۳]
- مخاطرات امنیتی شبکه‌های Ad-Hoc(مانند Bluetooth و Infrared)

[۱] Half-Duplex

[۲] Packet radio networks

[۳] Pager

٤. مخاطرات مربوط به ماهواره‌ها

مخاطرات ماهواره‌ها، عموماً به هشت دسته ذیل تقسیم بندی شده اند :

- مخاطرات منجر به تحریف داده
- امکان حمله فیزیکی به سامانه‌های زمینی
- امکان شنود داده
- امکان ایجاد اغتشاش با تزریق نویز
- امکان استفاده از شناسه‌های دروغین
- امکان تکرار فرمان
- امکان خرابی نرم‌افزاری
- امکان دسترسی غیر مجاز

همچنین این مخاطرات بر حسب نوع ماهواره به شش دسته زیر تقسیم بندی می شوند :

۱- مخاطرات مربوط به ماهواره‌های فضایی سرنشین‌دار
۲- مخاطرات مربوط به ماهواره‌های هواشناسی
۳- مخاطرات مربوط به ماهواره‌های مخابراتی
۴- مخاطرات مربوط به ماهواره‌های علمی تحقیقاتی
۵- مخاطرات مربوط به ماهواره‌های ناوبری و جهت‌یابی
۶- مخاطرات مربوط به ماهواره‌های شناسایی و جاسوسی

۵. مخاطرات ناشی از ارتباطات فیبر نوری

- نفوذ و تزریق سیگنال نوری و اغتشاش
- سربار گیرنده
- سطح پایین سیگنال نوری
- گم شدن سیگنال داده
- مخاطرات فیزیکی