تقدیم به شهدای دانش‌پژوه

انقلاب اسلامی ایران

آموزش امنیت سایبری
متخصصین

مولف

مهندس ناصر نا

سرشناسه: نامخواه، ناصر، ۱۳۴۰
عنوان و نام پدیدآور: **آموزش امنیت دنیای سایبر – متخصصین**
مشخصات نشر:
مشخصات ظاهری: ۳۰۶ ص. ، مصور، جدول، نمودار
شابک:
وضعیت فهرست نویسی: فیپا
یادداشت: واژه‌نامه
یادداشت:
کتابنامه: ص۳۰۶
موضوع:
موضوع :
شناسه افزوده
رده بندی کنگره:
رده بندی دیویی:
شماره کتابشناسی ملی:
کد پیگیری:

نام کتاب : آموزش امنیت سایبری – متخصصین

تألیف : مهندس ناصر نامخواه
نوبت چاپ : بهار ۱۳۹۰
ناشر :
صفحه آرایی:مجید بهمنی
طراح جلد: مجید بهمنی
شابک :
تیراز :
قیمت : ریال

مقدمه

در طول تاریخ توسعه و امنیت همیشه مانند دو بال پرندگان در کنار یک‌دیگر نبوده‌اند. قبل از اختراع برق که شاید بتوان از آن به عنوان شروع عصر جدید انسان‌ها نام‌برده عصری که امروزه از آن با عنوان دوره نوین و در برخی موارد عصر دیجیتال نام بردند، امنیت همپای توسعه دارای رشد مناسبی بوده است. هر میزان دسترسی انسان‌ها به علم و فن‌آوری تا این زمان منجر به افزایش امنیت می‌گردید. ابزار تولیدی در مسیر توسعه همراه با خود امنیت فکری و اجتماعی انسان‌ها را افزایش می‌داد. با ورود بشریت به دوره جدید که برخی شروع آن را هم زمان با اختراع برق نامیده و اختراع ابزاری مانند ترانزیستور و مدار مجتمع و تجهیزات الکترونیکی تهدیدات جدیدی فراروی انسان‌ها گشوده شد.

سرعت رشد تکنولوژی در اعصار جدید از سرعت بسیار بالاتری برخوردار بوده است، لکن به نظر می‌رسد که هر توسعه جدیدی همراه با خود ناامنی‌های جدید را به ارمغان می‌آورد. این مطلب باعث شده است پژوهش‌های مختلف ارتباط بین امنیت و توسعه را رابطه‌ای معکوس بنامند لذا به نظر می‌رسد یکی از راه‌های وصول به امنیت در دنیای دیجیتال شناخت واقعی این عرصه ابزار مرتبط با آن می‌باشد.

با گسترش فعالیت مباحث پدافندی غیر عامل در کشور و حرکت تخصصی این فعالیت‌ها به مرور شاهد نشر دانش تخصصی در عرصه پدافند غیر عامل فاوا با رویکردهای علمی و عملی در زمینه تهدیدات موجود و راه‌های شناخت آسیب‌پذیری‌ها و مقابله با آن‌ها توسط سازمان‌ها، نهادها و کاربران و مدیران در این عرصه می‌باشیم.

کتابی که در پیش روی دارید که یکی از چهار جلد کتابی است که با هدف آشنایی افراد مرتبط با این گونه ابزار و به منظور حفاظت از منابع و سرمایه‌های ملی نظام جمهوری اسلامی،

ایجاد ثبات در کاربرد سیستم‌ها و اطمینان از استمرار و سلامت اجرای فرآیند فعالیت‌های کاربران مختلف جمع‌آوری و تألیف گردیده است.

در این کتاب تلاش بر این گردیده است متخصصین که به نوعی از رایانه‌ها و ابزار دیجیتال به صورت کاربردی در زندگی شخصی و اجتماعی و کاری بهره می‌برند، از زاویه دفاع سایبری با این ابزار آشنا شده و ضمن آشنایی با عرصه‌های امنیتی این ابزار بتوانند به‌ترین روش امنیت، پایداری و ایمنی این گونه وسائل را انتخاب و به کار بگیرند.

در کتاب اول که با هدف آشنایی کاربران عمومی به رشته تحریر درآمده است تلاش گردیده است زمینه استنباط علمی این گروه از عزیزان در حد بضاعت فراهم گردیده و نیازمندی‌های علمی و امنیتی آنان در کتاب مربوط به ایشان جمع آوری و ارائه گردد.

با توجه به این که مدیران، یکی از حساس‌ترین لایه‌های درگیر با استفاده از ابزار رایانه‌ای و دیجیتال و ارتباطی می‌باشند و منابع هر سازمان با گرایش مدیر مربوطه در این زمینه‌ها مصروف می‌گردد. در کتاب سوم که ویژه مدیران محترم در سطوح عملیاتی استراتژیک تنظیم گردیده است، مطالب سمت و سوی کاربردی مدیریتی پیدا نموده و مطالب مرتبط و مورد نیاز این قشر از جامعه جمع‌بندی و تقدیم گردیده است.

تمام دستورالعمل‌ها و اسناد عملیاتی تنظیمی در لایه‌های مختلف سازمان و هر جامعه‌ای می‌بایست به روش‌های علمی و عملیاتی و در برهه‌های مختلف از زمان می‌بایست ممیزی گردد و میزان کارآیی آن‌ها و قابلیت اعتماد به روش‌های اجرایی آن سنجیده شود.

در کتاب چهارم که به نام ممیزان تقدیم می‌گردد کوشش گردیده است روش‌های ممیزی و امنیت در دنیای دیجیتال و راه‌های عملیاتی نمودن این گونه ارزیابی از اجرای عملیاتی دستورالعمل‌ها سنجیده شود. در کتاب ممیزان تلاش گردیده است بیش‌تر روش ممیزی ارائه شود تا دستورالعمل‌های بی‌روح ممیزی.

امید است این تحفه‌های ناقابل که قطعاً با نقادی صاحب‌نظران در اقصی نقاط کشور و مجامع علمی و دانشگاهی سیر رشد و تعالی خود را طی خواهد نمود زمینه‌های گسترش حرکت علمی در زمینه‌های پدافند غیر عامل فاوا را در کشور (ولو هر چند اندک) بتواند ایجاد نموده و از نظرات و پیش‌نهادهای صاحب‌نظران علمی استقبال نموده و با تکمیل آن‌ها در کتب آتی بتوانیم در هرچه پربارتر نمودن این گونه کتاب‌ها کوشا باشیم.

کتاب حاضر در ۱۱ فصل تقدیم می‌گردد. در انتهای هر فصل اهداف هر فصل برشمرده شده و پس از بررسی مطالب فصل، در انتهای فصل سئوالاتی با انگیزه کمک به هر چه به‌تر یادگیری مطالب کتاب به صورت خود آموز طراحی گردیده تا خوانندگان محترم بتوانند با مرور

بر پاسخ آن‌ها یک بار دیگر فصل را بررسی و به ماندگاری مطالب در ذهن کمک بیش‌تری داشته باشد.

در فصل اول مباحث مربوط به مقدمات و مبانی مورد نیاز برای ورود به بحث اصلی پرداخته شده و ضمن آشنایی با اطلاعات و اسناد و انواع تهدیدات و فرصت‌های کلی در امنیت دیجیتال با قاعده اصلی پدافند غیر عامل در حوزه فاوا که همان قابلیت اتکا به سازندگان این گونه ابزار است آشنا شده و با انواع آسیب‌های دیجیتال آشنا می‌شویم.

فصل دوم به آشنایی با پدافند غیر عامل در حوزه فاوا پرداخته و ضمن ارائه مفاهیم امنیت، ایمنی و پایداری در این حوزه با انواع سرمایه‌ها و تهدیدات از این منظر آشنا می‌گردیم.

در فصل سوم که اختصاص به امنیت اطلاعات دارد با اسناد به عنوان یکی از اصلی‌ترین ابزار نقل و انتقال اطلاعات که نیاز به امنیت دارند آشنا شده و به اطلاعات ذخیره شده در ذهن انسان‌ها پرداخته می‌شود و با انواع اطلاعات موجود در ابزار دیجیتال که نیاز به امنیت دارند آشنا می‌شویم.

فصل چهارم اختصاص به امنیت شبکه‌های رایانه‌ای دارد. در این فصل با انواع شبکه‌های رایج در کشور که برای امنیت خود از طریق لایه‌های محتلف با مدل مرجع osi اقدام می‌نمایند، آشنا شده و چگونگی تامین امنیت انتقال اطلاعات در این شبکه‌ها مورد بحث و بررسی قرار می‌گیرد.

انواعی از حملات این گونه شبکه‌ها را تهدید می‌کند که تلاش شده حملات رایج در این قسمت از کتاب، مورد بحث و بررسی قرار گرفته و وظایف کاربران و ساختار سازمانی و مدیران در رابطه با این حملات تبیین گردند.

فصل پنجم اختصاص به امنیت بانک‌های اطلاعاتی و مراکز دیتا سنتر دارد. امروز تقریباً تمام اطلاعات دیجیتال مورد نیاز در بانک‌های اطلاعاتی گردآوری و توسط این نرم‌افزارها برای استفاده ارائه می‌گردد. به منظور رعایت حیطه بندی بین کاربران مختلف برای دسترسی به هر لایه، روش‌های ایمنی خاصی در نظر گرفته می‌شود. در این فصل تلاش شده است انواع این روش‌ها و راه‌های ایجاد آن مورد بحث و بررسی قرار گیرند.

اتوماسیون اداری هرچند که دیرتر از انواع دیگر نرم‌افزارهای کاربردی به کار گرفته شده، لیکن با توجه به سهولت سازی کاربران سازمان‌ها برای چرخش اطلاعات به سرعت و با ضریب نفوذ بالایی تقریباً در کلیه سازمان‌ها به کار گرفته شده است. تلاش گردیده است در فصل ششم امنیت اتوماسیون اداری با نگرش سیستم‌های اطلاعات مبتنی بر رایانه مورد بحث قرار گیرد.

در اتوماسیون اداری لایه‌های مختلفی از کاربران از قبیل طراحان و برنامه نویسان و مدیران و سیاست‌گذاران نقش دارند. سعی شده است نقش هر کدام از این لایه‌ها در بهبود امنیت سیستم‌های اداری مورد بررسی واقع شود.

فصل هفتم اختصاص به امنیت اینترنت داشته و از زاویه نگاه سلطه گران به اینترنت نگاه شده و با ذکر تاریخچه‌ی پیدایش اینترنت، نقش آن به عنوان یکی از اصلی‌ترین روش‌های اشرافیت بر اطلاعات تولید در مبدأ و در خدمت سلطه‌گران مورد تجزیه و تحلیل قرار گرفته است.

اینترنت همراه با خود واژه‌های جدیدی از قبیل سلاح‌های سایبری و جنگ اطلاعات و جنگ رسانه‌ای را ارمغان آورده است که در ادامه فصل این گونه واژه‌ها نیز مورد واکاوی قرار می‌گیرند.

کلیه اطلاعات از طریق ارتباطات دیجیتال ایجاد شده مورد تعامل با دیگران قرار می‌گیرند. در فصل هشتم ضمن آشنایی با سیستم‌های ارتباطی به مقوله امنیت این سیستم‌ها پرداخت می‌شود.

انواع شبکه‌های با سیم و بی‌سیم و ماهواره‌ای و دیجیتال در این فصل بررسی شده و امنیت و دلایل نفوذپذیری این گونه شبکه‌ها بحث می‌شود.

در فصل نهم به امنیت محیطی و فیزیکی پایگاه‌های داده‌ای و دیجیتال پرداخت می‌شود. عدم رعایت نکات حفاظتی در طراحی و اجرای طرح‌های حفاظت فیزیکی می‌تواند ساختارها را به چالش کشیده و باعث از دست دادن اطلاعات گردد.

رعایت اصول پدافند غیر عامل در جایابی شبکه‌های رایانه‌ای و ارتباطی می‌تواند از خطرات قابل پیش بینی و یا پیش‌بینی نشده جلوگیری نماید.

سیاست‌ها و استانداردها و مدیریت امنیتی که در فصل دهم بررسی می‌گردد می‌تواند با مدیریت ریسک باعث کاهش آسیب‌پذیری‌ها شده و به نوعی عوامل موفقیت را به ارمغان آورد.

در صورت وقوع بحران می‌بایست اقداماتی انجام داد که در ادامه این فصل آن‌ها نیز مورد بررسی قرار می‌گیرند. هرچند امروزه در بسیاری از کشورهای مختلف استانداردهایی برای این کار تأکید شده است لکن با توجه به آسیب‌پذیر بودن برخی از آن‌ها نکات مربوط که می‌بایست مدنظر قرار گیرند مورد مداقه قرار می‌گیرد.

فصل پایانی کتاب که همان فصل یازدهم می‌باشد به بررسی ابزارهای امنیتی و تست نفوذ ابزار دیجیتال می‌پردازد.

نام بردن از ابزارهای خاص در این فصل نشان دهنده تأیید و یا تکذیب آن‌ها نمی‌باشد بلکه تلاش شده است از هر گونه از ابزار که امروز با عنوان چاقوی دولبه (امنیت و ضدامنیت) استفاده می‌شود بررسی شده و صرفاً نقش و شیوه کاربرد آن‌ها مدنظر بوده است.

امیدواریم با بهره‌گیری از این کتب بتوانیم نقشی ولو اندک در حفظ امانات شهدای گران‌قدر انقلاب اسلامی که همانا اطلاعات و اسناد نظام جمهوری اسلامی می‌باشد داشته و با توصیف واقعیت‌های موجود در امنیت و ایمنی و پایداری این ابزار توانسته باشیم دریچه‌ای با نگاه جدید به روی متخصصین گرامی باز نمائیم.

مؤلف

فهرست

۱

فصل اول – تعاریف

مطالبی که در این فصل خواهید آموخت:

- **تعریف اطلاعات**
- **تعریف اسناد**
- **تعریف امنیت**
- **تقسیم بندی سرمایه‌ها و مناطق قابل حفاظت**
- **تعریف پدافند عامل**
- **تعریف پدافند غیر عامل**
- **تعریف تهدید نرم**
- **تعریف مدیریت تهدید**
- **امنیت در دنیای سنتی و نوین**

۱- تعاریف

با توجه به این که امروزه اصطلاحات، عبارات و کلمات تخصصی معانی مختلفی پیدا کرده‌اند و برد استفاده از آن‌ها گستردگی فراوانی پیدا نموده است در این فصل ابتدا با تعاریف مورد نیاز برای ادامه کار آشنا شده و تعاریف عملیاتی و اختصاصی خاصی را که در ادامه کتاب به آن نیاز داریم بررسی می‌نماییم.

۱-۱- تعریف اطلاعات

با توجه به این که اطلاعات جمع اطلاع بوده و اطلاع به معنی آگاهی یافتن و واقف شدن بر کاری می‌باشد می‌توان اطلاعات را به هرگونه اقدام یا روشی که منجر به آگاه شدن از هر مطلب و مسئله‌ای می‌باشد تلقی نمود. هرگونه ابزار و یا حرکت یا نوشته و ایما و اشاره‌ای که منجر به آگاهی رسانی شود را می‌توان در حیطه اطلاعات تعریف نمود. با توجه به این که امروزه برای اطلاعات تقسیم بندی‌های مختلف انجام می‌دهند رایج‌ترین نوع اطلاعات را اطلاعات خام[۱] نامیده و شامل کلیه آگاهی رسانی‌های بدون ارزیابی شده و تمام انواع اطلاعات را در بر می‌گیرد.

با توجه به این که رایج‌ترین نوع اطلاعات را امروزه از اسناد استنتاج می‌نمایند ذیلاً به صورت تفصیلی به این مطلب می‌پردازیم.

۱-۲- تعریف اسناد

به موجب ماده ۱۲۸۴ قانون مدنی ایران سند عبارت است از «هر نوشته که در مقام اثبات دعوا یا دفاع قابل استناد باشد».

۱-۳- تعریف امنیت

در تعریفی عام امنیت عبارت است از مکانیزم‌های پیش‌گیری یا کاهش احتمال وقوع رخدادهای خطرناک و جلوگیری از تمرکز قدرت در هر نقطه از شبکه و احیای شبکه در حین

---

[۱] data

وقوع رخدادهای ناخوشایند (وقتی که رخدادهای خطرناک حادث می‌شوند) هر عاملی که به‌طور بالقوه بتواند منجر به وقوع رخدادی خطرناک شود یک تهدید امنیتی به شمار می‌آید.

امروز برای امنیت تعاریف مختلفی ارایه شده است و برخی امنیت را در بعد فیزیکی آن مورد بررسی قرار داده و برخی در ابعاد روانی آن را مورد بررسی قرار داده‌اند. امروزه برخی امنیت را مترادف با کلمه حفاظت دانسته و از این زاویه به آن نگاه می‌کنند. واژه security در فرهنگ فارسی معادل واژه‌هایی همچون امن، محفوظ، مطمئن، محفوظ داشتن، تامین کردن آمده است. امنیت عمدتاً به نوعی احساس روانی اطلاق می‌گردد که به‌خاطر نداشتن ترس، وضعیت آرامش و اطمینان خاطر حاصل می‌گردد. امنیت به حداقل رساندن خطر یا تهدید است که این خطرها نه فقط از نوع سنتی و نظامی هستند بلکه تهدیدات جدید غیر نظامی را نیز در بر می‌گیرند. فقدان تهدید، عنصر اساسی تعریف امنیت است گرچه عده‌ای فقدان تهدید را امری ناممکن و دست نیافتنی دانسته و از این‌رو به حداقل رساندن تهدید را مفهوم اصلی امنیت می‌دانند.

۱-۴- تقسیم بندی سرمایه‌ها و مناطق قابل حفاظت:

امروزه با توجه به اهمیت سرمایه‌ها و مناطق قابل حفاظت آن‌ها را به دسته بندی‌های مختلفی تقسیم می‌نمایند.

۱-۴-۱- عادی

تقریبا کلیه سرمایه‌ها و مراکز عام را که انسان‌ها با آن مراوده دارند در این گروه قرار می‌گیرد. گروه عادی گروهی است که انسان‌ها به صورت عادی تلاش خاصی برای حفظ و نگهداری آن انجام نمی‌دهند و صرفاً با مالکیت قانونی یا عرفی و شرعی آن را به تصرف درآورده و در تمام دنیا برای حفظ آن قوانین مدون و غیر مدونی وجود دارد و با احترام به این قوانین و رعایت آن عملاً حفاظت از این گروه از سرمایه‌ها، مناطق انجام می‌پذیرد.

۱-۴-۲- مهم

مراکز مهم مراکزی هستند که در صورت انهدام یا بروز آسیب در کل یا قسمتی از آن‌ها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی و دفاعی با سطح تاثیر گذاری محلی و موضعی وارد می‌گردد.

۱-۴-۳- حساس

مراکز حساس مراکزی هستند که انهدام یا ایجاد اختلال در کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره آمیز در نظام‌های سیاسی، هدایت، کنترل و مدیریت، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری منطقه‌ای یا بخشی در کشور می‌گردد.

۱-۴-۴- حیاتی

مراکز حیاتی عبارتند از مراکزی که انهدام یا ایجاد اختلال در کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و مدیریت، اقتصادی و تولیدی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و دفاعی با سطح تاثیرگذاری فرابخشی یا در سراسر کشور می‌گردد.

۱-۵- تعریف پدافند عامل

پدافند عامل عبارت از رویارویی و مقابله مستقیم و به کارگیری جنگ افزارهای مناسب و موجود توسط نیروهای نظامی به منظور دفع حمله و خنثی کردن اقدامات آفندی و در واقع شامل عملیاتی در برگیرنده حمله، مقابله و دفاع نظامی با ابزارها و سلاح‌های جنگی، می‌باشد.

۱-۶- تعریف پدافند غیر عامل

پدافند غیرعامل مجموعه‌ای از اقدامات، طرح‌ها و تمهیداتی است که توان دفاعی سیستم را افزایش داده، پیامدهای حوادث و بحران‌ها را کاهش دهد و هم‌چنین امکان بازیابی سیستم‌های آسیب‌دیده را با حداقل هزینه‌ی ممکن فراهم سازد.

۱-۶-۱- امنیت

امنیت اطلاعات از سه جنبه مختلف مدنظر قرار می‌گیرد: محرمانگی[۱]، یکپارچگی[۲] و دسترس‌پذیری[۳].

- محرمانگی به معنای اطمینان از این موضوع است که تنها افراد مجاز به اطلاعات دسترسی دارند.

---

[۱] Confidentiality

[۲] Integrity

[۳] Availability

- یک‌پارچگی به معنای اطمینان از دقیق و کامل بودن اطلاعات و روش‌های پردازش آن است.
- دسترس‌پذیری به معنای اطمینان از دسترسی افراد مجاز به اطلاعات در صورت لزوم است.

۱-۶-۲- ایمنی

ایمنی به مفهوم امن بودن در مقابل تهدیدها و حملات سخت و نیمه سخت می‌باشد. هر سیستمی به منظور تداوم بقا و توان ارائه تولیدات و خدمات باید ایمن باشد.

۱-۶-۳- پایداری

هرچند امنیت و ایمنی سیستم‌ها از منظر پدافند غیر عامل بسیار مهم و ضروری است اما به مفهوم تامین سیستم دفاعی کامل نمی‌باشد. یکی از نکات مهم، وجود پایداری در تولید و ارائه خدمات در مراکز حیاتی، حساس و مهم است. پایداری به این معنی است که یک مرکز در شرایط عادی و یا در صورت بروز حمله و خدشه‌دار شدن هر دو یا یکی از دو جزء ذکر شده، یعنی امنیت و ایمنی، باید امکان تداوم ارائه تولیدات و خدمات خود را داشته باشد.

۱- ۷- تعریف تهدید نرم

برای تعریف تهدید نرم تعاریف مختلفی ذکر شده است. تهدید نرم عبارت از «نوعی تلاش برنامه‌ریزی شده برای بهره‌گیری از ابزارها و روش‌های تبلیغی رسانه‌ای، سیاسی و روان شناختی برای تاثیر نهادن بر حکومت‌ها و مردم کشورهای خارجی به منظور تغییر نگرش‌ها، ارزش‌ها و رفتارهای آنان است. » (الیاسی ۴۶:۱۳۸۸) همچنین تهدیدهای نرم آن دسته از تهدیداتی است که اهداف متفاوتی را موضوع خود قرار داده و به جای تمامیت ارضی، هویت، هنجار، فرهنگ و. . . را هدف قرار می‌دهند. (گفتگوی علمی، فصلنامه میثاق۱۳۸۶ : ۱۴۵)

۱- ۸- تعریف مدیریت تهدید

مدیریت تهدید یا جنگ نرم از چه منظری یا با چه نگاه تئوریکی به مقوله تهدید و جنگ نرم نگریسته شود، متفاوت خواهد بود؛ از این لحاظ اگر با منظر گفتمان سلبی، در حوزه نظریات به مقوله تهدید نگریسته شود، مدیریت خاص خودش را می‌طلبد. زیرا از بعد سلبی، امنیت عبارت است از عدم وجود تهدید، در این گفتمان امنیت ماهیت برون‌گرایی و سخت‌افزاری دارد. مکاتب رئالیسم و نئورئالیسم چنین تعریفی را ارائه می‌دهند. اساسا واقع‌گرایان از منظر قدرت به

امنیت می‌نگرند و امنیت را از مشتقات قدرت تلقی می‌کنند. آن‌ها ضمن آن که امنیت را واقعیتی «عینی» می‌دانند. تنها بر بعد «عینی» امنیت نیز تأکید دارند و آسیب‌های داخلی در این نگاه اساساً مورد عنایت نیست.

اگر گفتمان ایجابی مبنای نگرش به تهدید باشد، مدیریت تهدید بیش از این که نگاه برون‌گرایی داشته باشد، به داخل و سرمایه اجتماعی تکیه دارد. زیرا از این منظر، از بُعد ایجابی امنیت به معنای رضایت و تناسب بین داشته‌ها و خواسته‌ها است. (افتخاری ۱۳۸۳) در این دیدگاه امنیت دارای بستر و مجموعه متکثری است که اگر شاخص‌های آن آماده باشد، برای انسان نوعی آرامش و اطمینان به‌وجود می‌آورد در غیر این صورت ناامنی محل ظهور پیدا خواهد کرد. به عبارت دیگر، این رویکرد برای امنیت و تهدید، ماهیت تأسیسی قائل است و بر این باور است که تهدید، تنها در وضعیتی وجود دارد که آن جامعه در سطح قابل قبولی از اطمینان برای تحصیل و پاسداری از منافع ملی و ارزش‌های حیاتی‌اش نباشد. (افتخاری، ۱۳۸۴، ص ۱۶) اگر این گفتمان را ملاک قرار دهیم قبل از ظهور "تهدید عینی" یا جنگ نرم، دوره تکوین و شکل‌گیری راه را برای طراحی و اجرای مدیریت‌های پیش‌گیرانه هموار می‌سازد. این تلقی که تحت "نظریه فضایی" در کتاب کالبد شکافی تهدید مطرح شده است، بدان معنی است که سیکل حیات تهدید در سه فضای اجتماعی، سیاسی و امنیتی معنا پیدا می‌کند و در هر فضایی الزامات و شرایط خاص خودش را دارد. در این میان حیات تهدید در فضای اجتماعی بسیار قابل توجه است و مدیریت پیش‌گیری بیش‌تر در این مرحله معنا و مفهوم پیدا می‌کند. در این فضا تلقی این است که تهدیدات در یک شبکه روابط اجتماعی شکل می‌گیرند؛ در فضای سیاسی پدیده مورد نظر با قدرت رسمی به‌صورت ایجابی و سلبی ارتباط پیدا می‌کند. فضای امنیتی عبارت است از قلمروی از بحث که در آن پدیده مورد نظر به‌صورت ایجابی و سلبی با ثبات نظام ملی ارتباط برقرار می‌کند.

بر این مبنا، مدیریت پیش‌گیری مبتنی بر این نظریه است که تهدیدات قبل از ورود به مقطع ظهور عینی شان، حضور دارند. از این رو، پدیده‌ها قبل از آن که در فضای خارجی، هویتی عینی بیابند، دارای هویتی اجتماعی درون ساختار جامعه می‌باشند. (افتخاری،فصلنامه میثاق ۱۳۸۵: ۷)

۱-۹- امنیت در دنیای سنتی و نوین

تحولات جوامع بشری را می‌توان به اعتبار شیوه و متد مدیریتی حاکم بر آن، به چهار عصر تقسیم نمود که هر یک از آن‌ها برای ادامه حیات خود نیازمند به ابزار و لوازم خاص خود بودند

و از این جهت هر یک از این تحولات شرایط و ویژگی‌های خود را دارا می‌باشند، این چهار عصر عبارتند از :

۱) عصر شکار

در این عصر که اولین مدل مدیریتی بشر می‌باشد، هدف همه ابنا بشر جمع آوری شکار بود. گروه‌های کوچک مردم که همواره در حال حرکت و مهاجرت و تحرک بودند همه مشغول تهیه مایحتاج زندگی و غذای خود بودند. در این عصر هر کس که کار می‌کرد سهم غذا داشت در غیر این صورت امکان ادامه حیات نداشت. سبک مدیریت در این عصر قدرت زور و چماق بود.

۲) عصر کشاورزی

در این عصر توانائی بشر به حدی رسیده بود که بتواند برای خود غذا تولید نماید تا افرادی که توانائی انجام کار را ندارند نیز از غذا بهره‌مند شوند. در عصر کشاورزی انسان یاد گرفت که می‌تواند در یک منطقه سکنی گزیند و نیازی به مهاجرت دائم از یک منطقه به منطقه دیگر ندارد.

۳) عصر صنعتی

در این عصر انسان و بشر با استفاده از ماشین آلات و ابزار تولید توانست افزایش فوق‌العاده‌ای را در تولیدات مصرفی و محصولات کشاورزی ایجاد نماید.

۴) عصر فراصنعتی (اطلاعات)

در این عصر اکثر افراد در خدمت تولید فرآورده‌ای به نام اطلاعات هستند و پیش‌بینی می‌شود که این روند روزبه‌روز نیز افزایش یابد و عده‌ی قلیلی در امر تولید محصولات کشاورزی و مواد غذایی باقی بمانند و در عوض عده‌ی بیش‌تری در امر تولید و پردازش اطلاعات قرار گیرند.

عنصر با ارزش این عصر اطلاعات است و فن‌آوری‌های اطلاعات و ارتباطات کشورها را به سوی جامعه اطلاعاتی سوق می‌دهد. ظهور شبکه‌ای رایانه‌ای جهانی به مدد فن‌آوری‌های پیش‌رفته مخابراتی دنیای جدیدی به وجود آورد که عده‌ای آن‌را دنیای مجازی یا دیجیتال نامیدند. انقلاب دیجیتال و مجازی شدن همه چیز از کار و آموزش و مدیریت گرفته تا مناسبات اجتماعی و حتی جنگ از نشانه‌های شروع عصر جدیدی در جهان است.

توسعه شگفت انگیز تکنولوژی اطلاع رسانی در عصر انفجار اطلاعات نوید زمان بی‌نظیری را می‌دهد که همه ابعاد تمدن بشری از آن تاثیر پذیرفته است. در عصر اطلاعات و جامعه اطلاعات

محور اقتصاد، سیاست، فرهنگ، هنر و اصولاً تمامیت دانش بشری با ابزارها و شیوه‌های تبادل الکترونیکی اطلاعات پیوند دارد.

فشرده شدن کار در واحد زمان از مشخصه‌های بارز دنیای جدید است. رشد و توسعه تکنولوژی هر روز بر این فشردگی می‌افزاید. از طرفی فشردگی کار در واحد زمان موجب می‌شود که رشد تکنولوژی با نسبتی چند برابر ادامه یابد. حافظه‌های الکترونیکی و اَبَر رایانه‌های موجود بر فشردگی مزبور می‌افزایند و هر لحظه شرایط جدیدی را برای دست‌یابی سریع‌تر به نیازمندی‌های بشر فراهم می‌آورند.

۱-۹-۱- تهدیدات و فرصت‌ها در دنیای سنتی

در دنیای حقیقی انسان‌ها باید در گروه‌ها جمع شوند تا بتوانند تاثیر گذاری در گروه‌ها داشته باشند ولی در دنیای مجازی انسان‌ها به‌صورت انفرادی می‌توانند تاثیر گذار باشند.

در دنیای حقیقی سیاست جغرافیایی مفهوم دارد ولی در دنیای مجازی سیاست مبتنی بر جغرافیا نداریم و به‌جای آن سیاست مبتنی بر زمان و تندی داریم.

در دنیای حقیقی مرزهای فیزیکی وجود دارد ولی در دنیای مجازی مرزی وجود ندارد.

۱-۹-۲- تهدیدات و فرصت‌ها در دنیای نوین

در دنیای حقیقی ما حوزه‌های هم‌پوشان منافع نداریم (یا بسیار کم داریم) ولی در دنیای مجازی مرزهای هم‌پوشان و حوزه‌های هم‌پوشان داریم.

در دنیای حقیقی با تضاد تضادها سروکار داریم – مانند امنیت و عدم امنیت – ولی در دنیای مجازی می‌توان تضادها را با هم جمع کرد.

در دنیای مجازی امنیت و ناامنی مطلق نداریم بلکه مخلوطی از آن را داریم.

در دنیای حقیقی حذف تهدیدها داریم ولی در دنیای مجازی حذف تهدیدها نداریم بلکه قابلیت هم‌زیستی با تهدیدها داریم. یعنی قابلیت تهدید پذیری و تهدید زدایی افزایش پیدا می‌کند.

۱-۹-۲-۱- انواع تهدیدات:

تهدیدات انواع و اقسام مختلفی داشته و از زوایای مختلفی می‌توان آن‌ها را تقسیم بندی نمود. در این کتاب تلاش بر این شده است تا از زاویه منشا این تهدیدات تقسیم بندی صورت پذیرد.

۱-۹-۲-۱-۱- تهدیدات فنی

در عصر فن‌آوری اطلاعات یکی از مهم‌ترین و رایج‌ترین تهدیدات این نوع از تهدید می‌باشد. در بسیاری از مواقع خطراتی که جوامع را تهدید می‌کند به علت گستردگی ضریب نفوذ ابزار فنی، این نوع از تهدید می‌باشد. در قرن اخیر به علت دست‌یابی انسان به ابزار پیش‌رفته فنی و نقش این ابزار در زندگی بشر استفاده از این ابزار جزئی از زندگی آدمی شده است و بدون آن‌ها در بسیاری از مواقع ادامه حیات بسیار سخت خواهد شد و به این خاطر گرایش به سمت استفاده هر چه بیش‌تر از این ابزار می‌باشد.

۱-۹-۲-۱-۱-۱- تهدیدات سخت‌افزاری

این گونه تهدیدات از جانب سخت‌افزارهایی است که استفاده می‌شود. به طور مثال استفاده از انواع ابزار نوین مانند رایانه‌ها و خودروها و هواپیماها و لوازم اداری و صنعتی که استفاده می‌شود در این تقسیم بندی قرار می‌گیرد. قبل از استفاده از ابزار صنعتی، تهدیدات مربوطه نمی‌توانست یک کشور را از راه دور تهدید نماید لیکن در عصر حاضر کشورهایی که استراتژی خود را بر مبنای صنعت قرار داده‌اند به مجرد این که صنعت آنان به هر علتی با رکود مواجه شود باعث خواهد شد تا امنیت ملی آن کشور نیز به خطر افتد و به همین خاطر تلاش دارند تا به هر شکل ممکن این ابزار را از خطرها دور نگه دارند و دشمنان آنان نیز تلاش دارند از این ناحیه خطر را متوجه آن کشور نمایند.

۱-۹-۲-۱-۱-۲- تهدیدات نرم‌افزاری

تهدیدات نرم‌افزاری تهدیداتی را تشکیل می‌دهند که بیش‌تر مغز افزار می‌باشند تا سخت‌افزار. این گونه تهدیدها در مواقعی خط مشی‌ها و روش‌های زندگی و نوع نگرش و نوع رفتار و الگوی رفتاری و این گونه موارد را در بر می‌گیرد و در برخی موارد نرم‌افزارهای رایانه‌ای که وظیفه مدیریت بر سخت‌افزارهای به کار گرفته را بر عهده دارد در بر می‌گیرد. در صورت ایجاد تهدیدات بالقوه در نرم‌افزارهای رایانه‌ای و به مجرد بالفعل تبدیل شدن این تهدیدات، متخاصمین خواهند توانست از راه دور و در زمان مورد نیاز اشرافیت اطلاعاتی خود را بر کشور دیگری مسلط نموده و به نوعی فکر و فرهنگ و فیزیک آن کشور را به دست بگیرند.

۱-۹-۲-۱-۱-۳- تهدیدات سیستم‌های ارتباطی

با توجه به این که امروزه کلیه کشورهای دنیا از طریق سیستم‌های ارتباطی ملی و بین‌المللی به یک‌دیگر پیوند خورده و بدون این ارتباطات عملاً هیچ کشوری قادر به ادامه حیات نخواهد بود و کلیه تحرکات خود را در ابعاد مختلف سیاسی، اقتصادی، اجتماعی، فنی، ارتباطی و دیگر مسائل از این طریق با داخل و خارج خود پیوند می‌دهد، در صورت دسترسی هر

ساختاری به این ابزار ارتباطی عملاً اشرافیت بر اطلاعات تبادلی نیز صورت خواهد پذیرفت. اشرافیت بر ارتباطات به علت سهل‌الوصول بودن و استفاده از تکنولوژی‌های کنترل از راه دور معمولاً کم هزینه پرفایده می‌باشد و بسیاری از سلطه گران به علت این که این ابزار تولید آن‌ها می‌باشد به راحتی امکان تسلط بر این ابزار را از راه دور داشته و بدون حضور فیزیکی امکان اشرافیت بر اطلاعات را برای خود مهیا می‌کنند.

۱-۹-۲-۱-۱-۴- تهدیدات الکترومغناطیسی

با پیش‌رفت علم و فن‌آوری در حوزه نیمه‌هادی‌های الکترونیکی، استفاده از تجهیزات رایانه‌ای، مخابراتی و الکترونیکی کاربردهای فراوانی پیدا کرده است. امروزه تمام ابزار اداری، صنعتی و نظامی از تجهیزات الکترونیکی استفاده می‌کنند و این مسئله آن‌ها را در مقابل لطمات الکترو مغناطیسی آسیب‌پذیر نموده است.

مدارات بردهای الکترونیکی که از ابتدا لامپی بوده‌اند و با ولتاژهای بالایی کار می‌کردند با پیدایش ترانزیستور تبدیل به قطعات بسیار کوچک‌تری شدند که با ولتاژهای پایین‌تری کار می‌کنند. با کاهش حجم و مصرف انرژی، استفاده از نیمه هادی‌های الکترونیکی رواج بیش‌تری پیدا کردند.

با توجه به این که ادامه حیات سرمایه‌های زندگی انسان‌ها که همان ابزار کاربردی می‌باشند به قطعات و سیستم‌های الکترونیکی، رایانه‌ای و مخابراتی وابسته است به همین دلیل یکی از جدّی‌ترین مخاطرات موجود تهدیدات الکترومغناطیسی می‌باشد. که هم به صورت طبیعی و هم ساخت دست بشر وجود دارد. از این تهدیدها می‌توان به رعد و برق، سویچینگ خطوط انتقال برق، دستگاه جوش ژنراتور الکتریکی، تسلیحات الکترومغناطیسی و انفجارات اتمی اشاره نمود.

۱-۹-۲-۱-۲- تهدیدات مصنوعی (انسان ساخت):

تهدیدات عمدی (که بیش‌ترین خسارت و دشوارترین راه مقابله را دارند) عبارت است از «هر گونه اقدام برنامه‌ریزی شده جهت افشا، نابودی یا تغییر در داده‌های حیاتی شبکه یا ایجاد اختلال در خدمات معمول سرویس دهنده‌ها». به‌طور عامّ هرگونه اقدام برنامه‌ریزی شده برای تحقق یک « رخداد خطرناک »، یک « تهدید امنیتی عمدی » تلقّی می‌شود.

۱-۹-۲-۱-۲-۱- تهدیدات برنامه ریزی شده

سازندگان سخت‌افزار و نرم‌افزار بنا بر سیاست‌های استراتژیک خود در زمان تولید این ابزار با اهداف مختلفی امکاناتی را بر روی آن‌ها تعبیه می‌نمایند تا در زمان مورد نیاز بتوانند به

صورت آشکار و پنهان از راه دور و نزدیک به این ابزار دسترسی داشته و مدیریت آن‌ها را به دست بگیرند. ساده انگارانه‌ترین این اقدام برای تعمیر این ابزار از راه دور می‌باشد و بدبینانه‌ترین آن اشرافیت پنهانی بر اطلاعاتی که توسط این ابزار در مبدا به کارگیری تولید می‌شود و هم‌چنین مدیریت استراتژیک این ابزار در زمان جنگ می‌باشد.

در کشورهای مختلف همچون امریکا برای این کار تدابیر قانونی نیز اندیشیده شده است تا تولید کنندگان بدون رعایت این مطلب این ابزار را به دیگر کشورها صادر ننمایند.

۱-۹-۲-۱-۲-۲- تهدیدات با منشا خطای انسانی

تهدیدات غیر عمد از اشتباهات سهوی و نا خودآگاه عوامل انسانی (همانند مدیران شبکه، کارکنان و کاربران) ناشی می‌شود و می‌تواند منجر به افشا یا نابودی اطلاعات یا اختلال در خدمات معمول شبکه و گاه تحمیل خسارت‌های کلان به جمیع کاربران شود. از این تهدیدات غیر عمد، می‌توان به موارد ذیل اشاره کرد:

۱. طراحی نا صحیح زیر ساخت شبکه یا عدم وجود افزونگی در تجهیزات شبکه
۲. عدم تهیه‌ی نسخه‌های پشتیبان از داده‌های حیاتی
۳. سهل‌انگاری در وظایف روزمره (مثل بررسی مستمر سیستم‌ها از لحاظ آلودگی به ویروس)
۴. نا آگاهی کاربران از ماهیت عملیات خطرناک
۵. بروز اشکالات پیش بینی نشده[۱] در سطح سخت‌افزار، نرم‌افزار یا سیستم عامل
۶. عدم اعمال صحیح سیاست‌های انتخاب و تعویض مداوم کلمات عبور توسط عوامل درگیر در شبکه

۱-۹-۲-۱-۳- تهدیدات طبیعی

این تهدیدات از عواملی مانند زلزله، سیل، گردباد، رعد و برق، آتش سوزی، آتشفشان و نظایر آن از قوّه به فعل می‌رسند و نسل بشر چنین تهدیداتی را به عنوان حقایق زندگی پذیرفته است. این تهدیدها همان گونه که زندگی را هدف گرفته‌اند می‌توانند در درجات خفیف‌تر منجر به نابود شدن یا افشای اطلاعات محرمانه و اختلال در سرویس‌های مؤلفه‌های اساسی شبکه شوند. از آن‌جا که خدمات شبکه‌های رایانه‌ای مرزهای جغرافیایی را در نوردیده است لذا تهدیدات طبیعی می‌توانند در خارج از محدوده‌ی بَلا دیده نیز منجر به اختلال در عملیات روزمره‌ی افراد و انتشار بحران در سطح وسیع شوند. لذا اگرچه تهدیدات طبیعی خارج از قدرت

[۱] BUG

بشرند ولی برای بازگرداندن خدمات شبکه از وضعیت بحران به وضعیت عادی، از همان ابتدای طراحی شبکه، تمهیداتی برای جلوگیری از گسترش دامنه‌ی بحران به مناطق دیگر پیش‌بینی و اجرا می‌شود. به عنوان مثال ایجاد تراز پشتیبان در دیگر مناطق جغرافیایی و بهره‌گیری از خطوط ماهواره‌ای در کنار خطوط فیبر نوری در این رده از تمهیدها قرار می‌گیرد.

۱-۹-۳- شناخت اطلاعات دیجیتال

اسناد دیجیتال(رایانه‌ای) : شامل داده‌های رایانه‌ای، دیسکت‌های رایانه‌ای، سی دی‌های رایانه‌ای، امواج مخابراتی. یعنی تمام اطلاعات رایانه‌ای از هر نوع که باشد به‌عنوان "اسناد دیجیتال" تلقی می‌شود. آن چه که در این جا مهم می‌باشد آن است که بدانیم اطلاعات دیجیتال به مجرد تولید شدن، قابل از بین بردن نمی‌باشند و در صورت امحا می‌توان آن‌ها را به روش‌های مختلفی بازیابی کرد یا نمی‌توان با استفاده از رمزگذاری این اطمینان را حاصل نمود که کسی به اطلاعات ما دستبرد نزند. رابطه رشد علم و فن‌آوری تولید سند با امنیت سند رابطه‌ای معکوس است. یعنی هر چه علم و فن‌آوری پیش‌رفته‌تر می‌شود امنیت آن به همان میزان پائین‌تر می‌آید. پس امروز باید نگاهمان را به امنیت اسناد تغییر دهیم و ضمن شناخت ابزار تولید سند(سخت‌افزار، نرم‌افزار، شبکه‌های مربوطه،) دیدگاهِمان را نسبت به مقوله امنیت اسناد عوض کنیم.

۱-۹-۳-۱- انواع اطلاعات دیجیتال

اطلاعات دیجیتال در ابزار ذخیره ساز انواع و اقسام مختلفی دارند و بر مبنای آن مورد استفاده‌های خاصی قرار می‌گیرند.

۱-۹-۳-۱-۱- اطلاعات ذخیره شده

این گونه اطلاعات کلیه اطلاعاتی است که در ابزار ذخیره ساز به شکل‌های مختلف ذخیره شده و حفظ و نگهداری می‌شود و در صورتی که فردی به صورت مجاز و یا غیر مجاز به این ابزار دسترسی پیدا نماید می‌تواند به این اطلاعات دسترسی پیدا کرده و آن‌ها را در اختیار بگیرد. به‌طور مثال در صورت مفقود شدن و یا به سرقت رفتن ابزار ذخیره‌سازی کلیه اطلاعاتی که در آن زمان بر روی این ابزار وجود دارد از نوع اطلاعات ذخیره شده می‌باشد و افراد بدون این که تلاش خاصی داشته باشند می‌توانند به این اطلاعات دسترسی و آن‌ها را مورد استفاده قرار بدهند.

۱-۹-۳-۱-۲- اطلاعات پشتیبان

به منظور اطمینان از این که همیشه اطلاعات تولید شده قابل استفاده می‌باشد در زمان‌های مختلف از اطلاعات پشتیبان تهیه شده و در صورتی خرابی اطلاعات موجود می‌توان از این اطلاعات بهره‌برداری نمود اطلاعات پشتیبان در ابزار ذخیره‌سازی جانبی کپی برداری شده و در محل‌های امن نگهداری می‌گردد درصورتی‌که فردی به صورت مجاز و یا غیر مجاز به این ابزار دسترسی پیدا نماید می‌تواند اطلاعات آن را مورد بهره‌برداری قرار بدهد.

۱-۹-۳-۱-۳- اطلاعات در حال عبور

اطلاعات در حال عبور همان اطلاعات تعاملی می‌باشند. در شبکه موجودیت‌ها در فاصله‌های دور از هم قرار دارند برای این که کلیه کاربران بتوانند از اطلاعات شبکه استفاده نمایند می‌بایست از طریق امکانات مخابراتی به یکدیگر وصل گردند اطلاعاتی که در بستر شبکه‌های مخابراتی در حال حرکت می‌باشند از موجودیتی به موجودیت دیگر منتقل می‌شوند و اطلاعات در درون سیستم‌های ارتباطی در حال حرکت می‌باشد چنان چه فرد غیر مجازی در مسیر عبور داده‌های اطلاعاتی که از طریق یک سیستم مخابراتی و در یک بستر شبکه‌ایی در حال تبادل و عبور هستند قرار گیرد؛ خواهد توانست از اطلاعات در حال عبور بهره‌برداری نماید.

۱-۹-۳-۲- سابقه امنیت دیجیتال

سابقه امنیت دیجیتال به قدمت دسترسی انسان‌ها به ابزار دیجیتال می‌باشد. از همان روزی که انسان‌ها توان این را پیدا کردند تا در عصر حاضر از ابزار دیجیتال در زندگی خود استفاده نمایند اولین مطلبی که ذهن آن‌ها را مشغول نمود مسئله امنیت اطلاعات دیجیتال می‌باشد. بدون امنیت دیجیتال عملاً اطلاعات تولید شده توسط دشمنان به راحتی قابل دسترسی می‌باشد.

۱-۹-۳-۲-۱- اصول امنیت دیجیتال:

در امنیت دیجیتال اصول مختلفی حاکم می‌باشد و با توجه به رعایت این اصول افراد تلاش می‌کنند تا امنیت اطلاعات خود را تأمین نمایند. بدون رعایت این اصول عملاً تأمین امنیت قابل اتکا نخواهد بود. امنیت دیجیتال مانند زنجیره‌ای به هم پیوسته می‌باشد و در صورت عدم رعایت امنیت در یکی از زنجیره‌ها عملاً امنیت در کل آن مخدوش خواهد شد.

۱-۹-۳-۲-۱-۱- اصل کلی- قابلیت اعتماد و اتکاپذیری

این اصل به مفهوم آن می‌باشد که قبل از این که هر ابزار دیجیتالی را مورد استفاده قرار داد ابتدا باید بررسی نمود تولیدکنندگان این ابزار با چه هدف و با چه نیتی این ابزار را تولید و در اختیار دیگران قرار داده‌اند. آیا در چرخه دسترسی به اطلاعات دیگران از مبدا تولید و با

هدف دسترسی به این اطلاعات این ابزار تولید شده است. آیا این ابزار توسط دوست و یا دشمن تهیه شده است. آیا تولیدکننده این ابزار برای صدور آن به دیگر کشورها دارای دستورالعمل یا آیین‌نامه خاصی می‌باشد یا خیر. به‌طور مثال یکی از قوانین آمریکا برای صدور سخت‌افزار و نرم‌افزار به دیگر کشورها وجود نقاط آسیب‌پذیر در آن که به تایید اف بی آی رسیده باشد می‌باشد و فقط در صورت تأیید این ابزار قابلیت صدور به دیگر کشورها را پیدا می‌کند. در این گواهی اف بی آی تأیید می‌نماید که ابزار لازم برای دسترسی از راه دور و به دست گرفتن مدیریت ابزار از راه دور در این سخت‌افزار و نرم‌افزار تأمین شده و به راحتی از راه دور می‌توان آن را به دست گرفت و بر مبنای نیاز تغییراتی در آن در زمان جنگ ایجاد نمود.

۱-۹-۳-۲-۱-۲- اصول فرعی (مبانی نقد پذیر ISMS):

علاوه بر اصل ذکر شده که با عنوان پایه اصلی امنیت اطلاعات می‌باشد و در تامین امنیت اطلاعات دارای نقش اساسی می‌باشد و بدون در نظر گرفتن اصل کلی و صرفاً رعایت اصول فرعی امنیت اطلاعات در درون سیستم تأمین شده و از خارج از سیستم به راحتی امکان اشرافیت بر اطلاعات به شکل آشکار و پنهان قابل تامین می‌باشد این مسئله باعث خواهد شد در زمان جنگ و صلح به راحتی تولیدکنندگان ابزار سخت‌افزاری و نویسندگان نرم‌افزاری به صورت آشکار و پنهان عملاً قادر به دست گرفتن مدیریت از راه دور اطلاعات باشند.

۱-۹-۳-۲-۱-۲-۱- محرمانگی

به مجموعه مکانیزم‌هایی که تضمین می‌کند داده‌ها و اطلاعات مهم کاربران از دسترس افراد بیگانه و غیر مجاز دور نگاه داشته شود، «سرویس محرمانگی» اطلاق می‌شود. این سرویس‌ها عموماً با روش‌های رمزنگاری تحقق می‌یابند. روش‌های مختلف رمزنگاری اطلاعات، زیربنای مابقی سرویس‌های امنیتی است.

۱-۹-۳-۲-۱-۲-۲- در دسترس بودن

مکانیزم‌هایی که دسترسی به کوچک‌ترین منابع اشتراکی شبکه را تحت کنترل درآورده و هر منبع را بر اساس سطح مجوز کاربران و پروسه‌ها در اختیار آن‌ها قرار می‌دهد، «کنترل دسترسی» خوانده می‌شود.

۱-۹-۳-۲-۱-۲-۳- صحت و یک‌پارچگی اطلاعات

مجموعه‌ی مکانیزم‌هایی که از هرگونه تحریف، دست‌کاری، تکرار[۱]، حذف یا آلوده سازی داده‌ها پیش‌گیری می‌کنند یا حداقل باعث کشف چنین اقداماتی می‌شوند، «سرویس تضمین صحت اطلاعات» نامیده می‌شود.

[۱] Reply

۱-۱۰- رابطه بین رشد علم و فن‌آوری و امنیت

در دنیای فیزیکی رابطه بین رشد علم و فن‌آوری و تأمین امنیت رابطه‌ای مستقیم می‌باشد یعنی هرچه علم و فن‌آوری پیش‌رفته‌تر می‌شود امنیت به‌تر قابل تمدید خواهد بود. اما این مسئله در دنیای نوین کاملاً بالعکس می‌باشد یعنی هر چه حد علم و فن‌آوری پیش‌رفته می‌کند امنیت به همان میزان کاهش پیدا می‌کند دلیل آن ابداع روش‌های دسترسی پنهان در ابزار دیجیتال می‌باشد. هر وسیله‌ای دیجیتال که ساخته می‌شود همراه با خود ناامنی‌های جدیدی به همراه دارد. با قرار گرفتن این ابزار در کنار ابزار دیگر ناتوانی‌های جدید به شکل تصاعدی بیش‌تر شده و زمینه را برای دسترسی غیرمجاز عناصر بیگانه فراهم می‌آورند.

۱-۱۱- تحقیقات اجمالی انجام شده در رابطه با کلیات امنیت در دنیای دیجیتال

در جهان سنتی و فیزیکی اندیشمندان امنیتی همیشه بر این باور بودند که با افزایش علم و فن‌آوری ، امنیت نیز حداقل به همان میزان افزایش پیدا می‌کند. اگر به دنبال حفظ و حراست از کالای گران قیمت بودند، در تلاش برای استفاده از فن‌آوری‌های نوین برای حفظ آن نیز بوده‌اند. دیوارها را بلندتر می‌ساختند تا هر چه می‌توانند فاصله بین نا امن گرایان را با متاع گران قیمت خود بیش‌تر سازند. اگر طلای خود را می‌خواستند هر چه بیش‌تر از دست سارقان دورتر نگهدارند از ابزار نوین آنالوگ مانند انواع دزدگیر و. . . استفاده می‌نمودند. و همیشه این‌اندیشه در ذهن آنان غالب بود که با افزایش علم و فن‌آوری و ابداعات در دنیای فیزیکی امنیت را می‌توان بالاتر برد.

اما در سال ۲۰۰۰ میلادی نتیجه پژوهشی که توسط دانشگاه برکلی (com .berkley) امریکا منتشر شد این نظریه را کاملا منسوخ ساخت.

این تحقیق که به مدت بیست و پنج سال از سال ۱۹۷۵ الی ۲۰۰۰ میلادی انجام شد نشان می‌داد که هر چقدر که از سال ۱۹۷۵ به سمت جلوتر حرکت می‌کنیم علم و فن‌آوری و نوآوری و میزان دسترسی انسان‌ها به ابداعات و ابتکارات جدید و کشفیات بیش‌تر می‌شود. اما اگر در سال ۱۹۷۵ برای دسترسی غیر مجاز به اطلاعات دیجیتال می‌بایست چندین مهندس کار کشته و باتجربه باید در کنار هم و با کار گروهی تلاش می‌کردند تا بتوانند به یک دسترسی کوچک به این اطلاعات دسترسی پیدا نمایند، این کار در سال ۲۰۰۰ بسیار راحت‌تر شده بود و

یک نوجوان ۱۷ ساله، بدون تحصیلات دانشگاهی و به تنهایی می‌توانست یک دسترسی نسبتاً بزرگی به صورت غیر مجاز به اطلاعات مهم داشته باشد.

نتیجه بیست سال از تحقیقات بیست و پنج ساله منتشر شده است ابتدا دسترسی غیر مجاز مشکل‌تر بوده است اما هر چه جلوتر می‌رویم این کار راحت‌تر می‌شود.

دانشگاه برکلی آمریکا به دو علت عمده به این نتیجه رسیده است:

- دسترسی ارزان‌تر و آسان‌تر به ابزار دسترسی غیر مجاز به اطلاعات دیجیتال

همان گونه که ملاحظه می‌نمایید هر چه به سمت سال ۲۰۰۰ حرکت می‌کنیم در طی سالیان مختلف ابزار نفوذ غیر مجاز بیش‌تری نوشته شده و به صورت ارزان و همه گیر از طریق اینترنت در اختیار همگان قرار گرفته است و هر کس می‌تواند با دسترسی به اینترنت و سی دی‌های ارزان قیمت که در همه جای دنیا قابل تهیه است به این ابزار دسترسی پیدا نموده و با استفاده از آن‌ها شانس خود را برای دسترسی غیر مجاز به اطلاعات به آزمون بگذارد.

- افزایش فراوانی آسیب‌پذیری با افزایش تولید ابزار نوین جدید

هرچقدر ابزار جدید تولید می‌شود همراه با خود آسیب‌پذیری‌های جدید را به ارمغان می‌آورد. اگر زمانی که فقط پول کاغذی وجود داشت یک دغدغه خاطر وجود داشت و آن حفظ پول از دست سارقان بوده است، اما به مجرد دسترسی به پول الکترونیکی باید این پول در مکان‌های مختلف که سارقان به شکل‌های مختلف به آن دسترس داشتند مورد حفاظت قرار گیرد تا با هک[1] شدن رمز ورود و کارت بانکی و شبکه بانکی و شبکه مخابراتی و. . . . به دست دیگران نیفتد.

۱-۱۲- آسیب‌های امنیتی (سلطه اطلاعاتی):

در دنیا تمام سلطه‌گران به دنبال اهدافی هستند. آن‌ها با توجه به این اهداف به دنبال گسترش ابزار خود در تمام دنیا بود و با استراتژی از قبل تعیین شده نسبت به تولید و توسعه این ابزار اقدام می‌نمایند.

۱-۱۲-۱- اشرافیت بر ارتباطات

یکی از اهداف سلطه گران اشرافیت در ابزار ارتباطی به کل ارتباطات در دنیا می‌باشد. امروز سیستم‌های مخابراتی ملی به بین‌المللی وظیفه ارتباط بین کلیه آحاد مختلف در دنیا را به عهده دارند. اگر چنان‌چه ساختاری بتواند به این ابزار دسترسی پیدا کند عملاً قادر خواهد بود در

[1] Hack

مسیر چرخش اطلاعات بین کلیه ابزار دیجیتالی که توسط کاربران مورد استفاده قرار می‌گیرد قرار بگیرد و بر آن اشرافیت داشته باشد.

۱-۱۲-۲- اشرافیت بر اطلاعات

هدف اصلی سلطه‌گران اشرافیت بر اطلاعات می‌باشد کلیه اقداماتی که به منظور اشرافیت بر ارتباطات انجام می‌دهند با هدف اشرافیت بر اطلاعات بوده و تمام سرمایه‌گذاری‌ها برای تولید ابزار اطلاعاتی و ارتباطی از ابتدا با استراتژی اشرافیت بر اطلاعات تولید شده در مبدا توسط کاربران بوده و این یک نوع سرمایه‌گذاری اقتصادی محسوب می‌شود.

۱-۱۳- آسیب‌های دنیای دیجیتال:

- **از بین رفتن کیان و کارکرد خانواده**

در جوامع سنتی، خانواده نهادی اجتماعی با مرکزیت و محوریت مشخص است و هویت افراد، با توجه به خانواده‌هایشان شناخته می‌شود. اعضای خانواده سنتی را پدر و مادر، فرزندان، پدر بزرگ‌ها و مادر بزرگ‌ها تشکیل می‌دهند و جایگاه و احترام هر کدام مشخص و حفظ می‌شود.

سرپرست خانواده، رفتار و منش اعضای خود را کنترل می‌کند و اگر زمانی فرزندان با ازدواج یا ادامه تحصیل، از خانواده جدا بشوند، باز هم از کنترل و نظارت خارج نیستند و در مواقع لزوم نیز خانواده به یاری آنان همت می‌گمارد.

دین، باورها و آداب و رسوم مذهبی، در خانواده‌های سنتی جایگاه ویژه‌ای دارد و ارتباط مستقیمی میان دین و سلامت اخلاقی و رفتاری افراد خانواده وجود دارد. از این رو، در خانواده‌های سنتی ناهنجاری‌های کنتری دیده می‌شود. معمولاً سرلوحه همه رفتارهای خانواده سنتی، محبت و فداکاری و از ویژگی‌های آشکار این خانواده‌ها، رسیدن اعضای آن به احساس آرامش و سلامت روانی است. در مقابل، تاثیری که تمدن، تکنولوژی، ماهواره و اینترنت بر خانواده‌های به اصطلاح مدرن امروزی گذاشته، آن‌ها را با نوعی کاستی و سردی در روابط و مناسبات روبه رو کرده است. در نتیجه، دوام و پایداری آن‌ها دست خوش تهدیدهای جدی قرار گرفته است.

آسیب‌های خانواده، به دو دسته بیرونی و درونی تقسیم می‌شوند. نادیده گرفتن مسائل اخلاقی و حقوقی و رعایت نکردن امور مربوط به روابط انسان‌ها، از آسیب‌های درونی هستند که متوجه اعضای خانواده می‌شود.

عوامل آسیب‌زای بیرونی را نیز باید در خارج از محیط خانواده یافت. در عصر حاضر با ورود وسایل ارتباط جمعی مانند روزنامه، کتاب، رادیو، تلویزیون، ماهواره و شبکه‌های اینترنتی، نوع زندگی خانوادگی تغییر کرده و پی‌آمدهای گوناگون و دشواری را به همراه داشته است. مدرن و به روز بودن، اصل هویت خانواده را با درگیری‌های جدی روبه‌رو ساخته است و تکنولوژی‌ها و اختراعات مختلف که برای رفاه بخشیدن به زندگی جوامع امروزی پدید آمده‌اند، خانواده را دچار سردرگمی کرده و مصرف گرایی را ترویج کرده‌اند. فعالیت‌های بیش از حد والدین نیز آسیب‌های عاطفی بسیاری را متوجه فرزندان کرده و خانواده را در به انجام رساندن مسئولیت‌هایش با مشکل روبه رو ساخته است.

ناهماهنگی و نبود تعادل در خانواده، شادابی و پویایی را نیز از جامعه می‌گیرد و بی‌توجهی به بهداشت روانی خانواده، از مشکلات مهم زندگی‌های امروزی است. پژوهشگران، بالا رفتن آمار افسردگی در مردم را از پی‌آمدهای نوع زندگی قرن بیستم می‌دانند؛ که در آن، خانواده‌ها از هم گسسته‌اند و بیش‌تر مردم در کنار خانواده و با ترتیب درست و اصولی آنان رشد نمی‌کنند. در این شرایط، والدین وقت کافی برای همراهی موثر فرزندان خود ندارند و در نتیجه، استرس‌های گوناگون، افراد را در معرض افسردگی و بیماری‌های روانی قرار می‌دهد.

افزایش زمینه‌های تحریک جنسی نیز در پی گسترش و تنوع وسایل جدید تکنولوژی، خانواده‌ها را با گرفتاری‌های نگران کننده‌ای روبه‌رو کرده است. دنیای مدرن، عصر تنوع و هیجان و نوآوری است. تعدد مشاغل مردان و فشار بیش از حد ناشی از فعالیت زنان خانه و مشاغل رسمی آنان در جامعه، همراه با افزایش استرس‌ها و ضعف مهارت زوجین در برقراری ارتباط سالم جنسی نیز کارکرد تربیت جنسی خانواده را ضعیف می‌کند.

امروزه مسئولیت خانواده‌ها در تربیت فرزندان بیش از گذشته است و پرورش فرزندانی که ثبات شخصیت و هویت اجتماعی داشته باشند، دشوارتر شده است. فرزندان نیز با وظایف سنگین حاضر و بحران‌های پیش آمده، بسیار ضعیف و شکننده عمل می‌کنند و فرزند سالاری، در بسیاری از خانواده‌ها، اقتدار و نظارت والدین را بر هم زده است. بر این اساس، هر کدام از کارکردهای خانواده، نقش مهمی در استحکام و تقویت بنیان خانواده ایفا می‌کند. با این حال، مسئله ناخوشایند این است که در بسیاری از خانواده‌های مدرن، وظایف خانواده، به درستی انجام نمی‌شود.

از آفت‌هایی که خانواده امروزی را تهدید می‌کند، بی اعتباری تدریجی هنجارها، اخلاق، باورهای دینی و ارزش‌های مذهبی و سنتی و در کنار آن، گسترش انواع انحراف‌ها و رفتارهای ناپسند در جامعه است.

کم توجهی به ارزش‌ها در جوامع مدرن که با کنار گذاشتن خدا، دین و اخلاق همراه است، به انسان امروزی، جرات دست زدن به هر کاری را می‌دهد. اخلاق مدرن، ریشه خود را در عقل گرایی جست‌وجو می‌کند و به همین سبب، با اخلاق سنتی و دینی فاصله گرفته است. آسیب‌پذیری خانواده امروزی، ناشی از نادیده گرفتن بایدها و نبایدهای دینی و اخلاقی است. بشر امروزی، هنوز به این نتیجه نرسیده است که زندگی بدون ایمان و معنویت، رنج و عذاب روانی و همیشگی را همراه او خواهد کرد.

- **از بین رفتن حریم‌های خصوصی**

در دنیای سنتی، ارتباطات هم سنتی بود، که شامل ارتباطات انسانی، شفاهی، چهره به چهره و بی واسطه فردی و گروهی بود که به رغم ظاهر ساده و ابتدایی می‌تواند کارکردی پیچیده و متنوعی داشته باشد. این نوع ارتباطات گرچه به دلیل گسترده و پیچیده شدن جوامع انسانی کارکرد گذشته خود را از دست داد. اما هنوز هم از نفوذ و اعتبار خاصی برخوردارند زیرا بر طبیعت انسانی و نیازهای عاطفی او نزدیک‌ترند. در فرهنگ اسلامی ایرانی ما در دنیای سنتی مراسماتی چون نقالی، شاهنامه خوانی، حضور در میادین روستا و شهرها و ... حاکم بوده است که کارکردهای مثبت فراوانی داشته که در گستره زمان جای خود را به رادیو، تلویزیون و امروز به اینترنت و ماهواره داده است و دیگر از آن کارهای مثبت و سازنده خبری نیست و بر عکس آثار زیان بار و مخربی همچون نفوذ به حریم خصوصی افراد سوغات فن‌آوری جدید بشر یعنی اینترنت می‌باشد.

اینترنت به عرصه تبدیل و انتقال آزاد و افکار گردیده و حد کنار سرعت دادن به ارتباطات بشری خود معضلی جدی گردید.

اینترنت به عرصه فعالیت متصدیان جمع آوری اطلاعات در سراسر جهان تبدیل شده است. عملیات نفوذ به سیستم با نرخی هشدار دهنده افزایش یافته است، زیرا اینترنت به محلی کاملاً راحت و جالب برای هکرها تبدیل شده است. اینترنت را با رعایت مسایل حفاظتی طراحی نکرده‌اند. اینترنت شبکه‌ای عظیم و ظریف بوده و حاوی بسیاری کاستی‌های نرم‌افزاری است. به راحتی می‌توان در شبکه بدون ذکر نام خویش فعالیت کرد. چون همه چیز به هم مرتبط است، هر چیزی قابل نفوذ بوده و متجاوزی حرفه‌ای می‌تواند با ایجاد ردپایی در میان ده‌ها سیستم در چندین کشور مختلف ردپای خود را گم کند. بسیاری از ابزار مورد استفاده هکرها که در سال‌های قبل نیاز به دانشی عمیق داشت، اکنون خودکار شده و به راحتی قابل استفاده می‌باشد.

شکسته شدن حریم خصوصی افراد از هر قشر و رده‌ای، باعث ناامنی روانی و اجتماعی می‌شود و می‌تواند پیامدهای جبران ناپذیری به همراه داشته باشد.

هم‌زمان افراد تلاش وافری در حفظ اطلاعات شخصی خود به هر شکل ممکن می‌کنند و این تلاش همیشگی دو طرفه برای کشف و حفظ اسرار شخصی افراد موجب ایجاد چالشی جدی در جوامع بشری است.

در این میان میثاق‌ها، بیانیه‌ها و قطعنامه‌های متعددی که منتشر می‌شود دست و پا زدن‌های انسان عصر مدرن را می‌ماند که سعی می‌کند خفگی‌اش را اندکی به تاخیر بیندازد.

- **فضای دیجیتال**

بر اساس تحقیقات انجام شده ۵۱٪ از نفوذ و تخریب سیستم‌های دیجیتال توسط ویروس‌ها و۲۷ ٪ توسط کارکنان ناراضی، ۱۵٪ خراب‌کاری از بیرون، ۷٪ توسط جاسوسان صنعتی انجام می‌شود.

الف : ویروس‌ها و سایر امراض نرم‌افزاری

ویروس قطعه‌ای کوچک از کد رایانه‌ای است که درون برنامه رایانه‌ای دیگری پنهان می‌شود. مثل ویروس واقعی، ویروس رایانه‌ای می‌تواند خود را تکثیر کرده و سایر رایانه‌ها را بیمار کند و سپس بدون حرکت طی ماه‌ها یا سال‌ها باقی مانده و دوباره حمله کند. ویروس تنها یکی از چندین نوع رشته منطقی است که می‌تواند رایانه‌یا کل شبکه را صدمه بزند.

کرم‌ها، بمب‌های منطقی، و اسب‌های تروا امراضی مشابه هستند که معمولاً با ویروس‌های رایانه‌ای گروه بندی می‌شوند. کرم رایانه‌ای مثل ویروس پراکنده می‌شود اما به جای آن که درون برنامه دیگری پنهان شود، خود برنامه‌ای مستقل است. بمب منطقی برنامه‌ای است که معمولاً در اعماق رایانه اصلی پنهان شده و منتظر می‌ماند تا در مرحله‌ای خاص در آینده فعال شده و داده‌ها را خراب کند. اسب‌تروا را در قالب برنامه‌ای نرم‌افزاری و مشروع پنهان می‌سازد و منتظر می‌ماند تا آن که نوعی رویداد از قبل تعیین شده یا تاریخی مقرر سر برسد و آن گه بار خود را تحویل می‌دهد و بدین‌ترتیب فایل‌ها یا دیسک‌ها را منهدم می‌کند.

ب : هکرها

نکته: وقتی به اینترنت وصل می‌شوید، به رایانه‌های سراسر جهان متصل می‌شوید و مهم‌تر این که آنان نیز به رایانه شما وصل می‌شوند. کاربر رایانه از ارتباط دیگران خبری ندارد، اما هر ارتباطی با سایت روی اینترنت، در واقع مثل خیابانی دو طرفه می‌ماند !

هکرهای متخصص، ابزار نرم‌افزاری پیچیده‌ای را ایجاد کرده و برای دیگران می‌فرستند، تا آنان بتوانند از نقاط ضعف انسانی و فنی موجود در حفاظت از سیستم‌های رایانه‌ای دیگران

استفاده کنند. این ابزار مشتمل است بر استفاده از ابزار کشف کلمات عبور، شماره گیرهای جنگی، اسکنرهای نقاط آسیب پذیر، بویشگرها، رباینده‌گان ای . پی و از این قبیل، چون بسیاری از این ابزار روی اینترنت موجود است، تازه واردها چه بسا از آن‌ها استفاده کرده و اقدام به دانلود آن‌ها نمایند، و سطح پیچیدگی همه انواع هکرها را افزایش دهند.

اکنون با توسعه شبکه‌های بی‌سیم، هکرها فرصت‌های تازه‌ای برای کسب دسترسی به رایانه شما یافته و از طریق شما به کل کشور دسترسی می‌یابند.

نکته: هدف نخست هکر عبارت است از نیل دسترسی به تمامی شبکه شما به منظور خواندن فایل‌ها. در اغلب موارد، کلمات عبور بی اثر، مودم‌های نا امن، و به گفته هکرها، مهندسی اجتماعی، نخستین روزنه را به سوی سیستم می‌گشایند.

ج- مهندسی اجتماعی

مهندسی اجتماعی در اصطلاح هکرها عبارت است: از فریب کاربران مشروع رایانه برای تامین اطلاعات مفید برای هکرها به منظور دسترسی غیر مجاز به سیستم‌های رایانه‌ای.

هکری که از مهندسی اجتماعی استفاده می‌کند، اغلب خود را شخصی مشروع در یک سازمان معرفی کرده و از داستان ساختگی قابل باوری استفاده می‌کند تا کاربر رایانه را با نیرنگ مجبور به ارایه اطلاعات مفید کند. این امر معمولاً با تلفن انجام می‌شود، اما شاید با پیام‌های جعلی ایمیل یا ملاقات رو در رو نیز صورت پذیرد.

نکته: اکثر افراد تصورات نادرستی از سرقت‌های رایانه‌ای دارند و فکر می‌کنند این سرقت‌ها کاملا فنی بوده و در نتیجه نقص‌های فنی سیستم‌های رایانه‌ای متجاوزان امکان توفیق در کار خود را می‌یابند. حقیقت این است که به هر حال، مهندسی اجتماعی معمولاً نقش بزرگی را در کمک به هکرها برای رد شدن از موانع امنیتی بر عهده دارد. چنان چه هکر هیچ گونه مجوز دسترسی به سیستمی را نداشته باشد، فقدان آگاهی امنیتی و زودباروی کاربران رایانه معمولاً موجب رخنه آسان وی به درون سیستم حفاظت شده می‌شود.

د : تهدید نیروهای داخلی (کارمندان ناراضی)

عموما معتقد هستند حفاظت از رایانه‌یعنی مقابه با تهدید گروه کثیری از هکرهای بداندیش که در حال حاضر وجود دارند و بر همین اساس تمرکز بسیاری از اقدامات حفاظت رایانه به روی دور نگه داشتن افراد بیرونی از دسترسی به رایانه‌ها می‌باشد و این کار را از طریق اقدامات فیزیکی و فنی مثل دروازه‌های ورود، نگهبانان، قفل‌ها، دیوارهای آتش، کلمات عبور، و غیره انجام می‌دهند. با همه این‌ها اگر چه تهدید از ناحیه افراد بیرونی در واقع در همان حد

تصور موجود، گسترده است، اما نیروهای داخلی بد طینت نیز با دسترسی مجاز به سیستم تهدید حتی بزرگ‌تر از تهدید نیروهای بیرونی محسوب می‌شوند!

تحقیقات پیاپی حکایت از آن دارد که اغلب خسارات را نیروهای داخلی یعنی افراد دارای دسترسی به شبکه رایانه‌ای وارد کرده‌اند. بسیاری از نیروهای داخلی از دسترسی و دانش لازم برای نفوذ و ایجاد اختلال در سیستم‌ها و شبکه‌های رایانه‌ای برخورد هستند.

افزون بر رخنه نیروهای اطلاعات خارجی حریف به سیستم، شبکه رایانه‌ای که در اختیار دارید در معرض خطراتی از جانب انواع نیروهای بیرونی نیز قرار دارد.

ه : نیروهای بیرونی

از نمونه نیروهای بیرونی به موارد زیر می‌توان اشاره کرد :

- دلالان آزاد اطلاعات.
- رقبای خارجی یا داخلی.
- سرویس‌های نظامی کشورهای متخاصم که سرگرم توسعه قابلیت خود برای استفاده از اینترنت به عنوان سلاح نظامی هستند.
- سازمان‌های تروریستی که برای آن‌ها هک کردن سازمان یافته، عاملی بالقوه و کم هزینه، کم خطر و در عین حال همراه با منافع بالا به حساب می‌آید.
- سندیکاهای جرم و جنایت و کارتل‌های مواد مخدر.
- هکرهای ماجراجو که برای سرگرمی یا انجام خراب کاری‌های تفریحی وارد سیستم شما می‌شوند.
- سارقان عادی که متخصص در سرقت و فروش مجدد رایانه‌ها و لپ‌تاپ هستند.

۱-۱۳-۱- ایجاد شکست در فرآیند مدیریت

با توجه به این که مدیریت در هر سیستمی اصلی‌ترین عامل به کارگیری منابع و سازمانی بوده و راهبرد اصلی سازمان توسط مدیران طراحی و اجرا می‌گردد. بسیاری از صاحب نظران مدیریت را علم همراه با هنر مدیر تعریف کرده‌اند. مدیریت اقدامی نیست که در یک مرحله شروع و در همان مرحله نیز به اتمام برسد، بلکه مدیریت فرآیندی است که ازیک مدیر در سازمان شروع شده و به آخرین لایه‌های ساختاری رسوخ پیدا می‌نماید. به همین دلیل هرگونه تاثیری در مدیریت می‌تواند در کلیه امور یک سازمان و یا یک کشور اثر گذار باشد و به همین دلیل سلطه‌گران به این نتیجه رسیده‌اند که با اثر گذاری در فرآیند مدیریت می‌توانند در دیگر

لایه‌های سازمانی نیز اثر گذار باشند. هر گونه شکستی در این لایه برابر است با شکست در اهداف سازمان.

۱-۱۳-۲- هدایت مدیریت به سمت مسیر خود خواسته

سلطه‌گران در رابطه با اعمال نقطه نظرات خود به‌صورت پنهان و آشکار سرمایه گذاری‌های فراوانی انجام می‌دهند. اینان به دنبال آن هستند تا با کم‌ترین سرمایه گذاری مادی و معنوی به بیش‌ترین اثرات نائل شوند. هم‌چنین با اجرای عملیات خود ، کم‌ترین آثار و تبعات ملی و بین‌المللی را به همراه داشته باشند. سلطه جویان می‌خواهند در مقابل واژه‌های خودساخته‌ای مانند حقوق بشر که امروزه تبدیل به ابزار سلطه‌گری شده است کم‌تر پاسخ‌گو بوده و به همین دلیل تلاش دارند تا فرآیند مدیریت را به سمت استفاده از ابزار مدیریت قابل هدایت از راه دور به صورت پنهان و آشکار سوق دهند تا در زمان مورد نیاز ابتکار عمل را خود به دست گرفته و در شرائط خاص بهره‌برداری خاص خود را ببرند.

۱-۱۳-۳- سرقت اطلاعات

سرقت اطلاعات در دنیای آنالوگ کاملاً آشکار بود و پس از سرقت می‌توان سریعاً متوجه این مطلب شد که کالایی به سرقت رفته است اما سرقت اطلاعات در دنیای دیجیتال به صورت کاملاً پنهان انجام می‌گیرد سرقت کننده به دنبال این می‌باشد که به صورت پنهانی این سرقت را انجام دهد تا مسیر برای سرقت‌های بعدی بسته نشود چنان‌چه سرقت اطلاعات در ابزار دیجیتالی صورت بگیرد ممکن است تا زمان زیادی مالکت اطلاعات متوجه این کار نشود.

۱-۱۳-۴- حملات ویروس

ویروس‌ها برنامه‌های اجرایی کوچکی می‌باشند که به مجرد اجرا شدن بر روی رایانه قربانی می‌تواند تغییرات مورد نظر را به صورت پنهان و یا آشکار بر روی رایانه ایجاد نماید.

۱-۱۳-۵- آسیب‌های اتفاقی

منظور از آسیب‌های اتفاقی آسیب‌هایی است که بدون داشتن هیچ هدفی و با استفاده کردن از ابزار به وقوع می‌پیوندد این گونه آسیب‌ها دارای هدف اولیه نبوده و با در کنار هم قرار گرفتن سخت‌افزارها و نرم‌افزارها به وجود می‌آید.

۱-۱۳-۶- خراب‌کاری و دست‌کاری

هرگاه داده‌های در حال جریان بین مبدأ و مقصد توسط شخص غیر مجاز به هر نحو دست‌کاری یا تحریف شود، حمله‌ی «دست‌کاری داده‌ها» رخ داده است.

۱-۱۳-۷- شکستگی اطلاعات

در بانک‌های اطلاعاتی از کنار هم قرار گرفتن فیلدهای اطلاعاتی رکوردها تشکیل می‌شود این فیلدها با نظم خاصی در کنار هم قرار دارند به طور مثال در کنار هر نام یک فیلد نام خانوادگی وجود دارد و در هر حال نام به نام خانوادگی مربوطه متصل می‌شود. در صورت ایجاد شکستگی در اطلاعات عملاً کل اطلاعات به هم ریخته و مخدوش خواهند شد این کار ممکن است با ارتقا یا تنزل یک فیلد ایجاد شود.

۱-۱۳-۸- خطای در سیستم‌های ارتباطی

با توجه به این که سیستم‌های یک شبکه از طریق سیستم‌های ارتباطی با هم متصل می‌باشند هر گونه خطایی در سیستم‌های ارتباطی قادر خواهد بود در شبکه اثرگذار باشد. این اثرگذاری ممکن است عمدی و یا غیرعمدی صورت بگیرد.

۱-۱۳-۹- استراق سمع

هرگاه یک شخص غیر مجاز به هر نحو بتواند نسخه‌ای از داده‌های در حال جریان بین مبدأ و مقصد را به نفع خود شنود کند، حمله‌ی «استراق سمع» به وقوع پیوسته است.

۱-۱۴-۱۰- افزایش اطلاعات ناخواسته

هرگونه افزایش و کاهش اطلاعات به صورت ناخواسته می‌تواند اطلاعات را مخدوش نماید. به‌طور مثال افزایش ۱۰ و یا کاهش آن در یک حساب بانکی می‌تواند آن را به ۱۰٪ کاهش و یا ۱۰ برابر افزایش دهد.

۱-۱۳-۱۱- اقدامات مداخله گرایانه

هرگونه اقدامی که نتیجه آن به هم ریختن منطق موجود سیستم باشد اقدامات مداخله گرایانه نام دارد. اقدامات با هدف اولیه مخدوش سازی سیستم و در نتیجه به دست گرفتن مدیریت سیستم و یا به هم ریختن اطلاعات صورت می‌پذیرد

۱-۱۳-۱۲- آسیب‌های سیستم عامل

نرم‌افزارها انواع و اقسام مختلفی دارند یکی از بارزترین نرم‌افزارها سیستم عامل می‌باشد. وظیفه سیستم عامل مدیریت بر سخت‌افزار و نرم‌افزار رایانه می‌باشد. با توجه به نقش مهم این نرم‌افزار در مدیریت رایانه آسیب‌های آن نیز شکل ویژه‌ای به خود می‌گیرد به همین دلیل نفوذگران تلاش می‌کنند تا از آسیب‌پذیری‌های سیستم عامل برای مدیریت بر سیستم استفاده نمایند.

۱-۱۳-۱۳- آسیب‌های سخت‌افزاری

تمام سخت‌افزارها می‌توانند دارای نقاط آسیب‌پذیر از قبل تعریف شده و یا پس از استفاده باشند این گونه نقاط آسیب‌پذیر در صورت شناسایی می‌تواند باعث دسترسی به اطلاعات از راه دور باشد. هرگونه آسیب سخت‌افزاری عملاً باعث آسیب رسانی به اطلاعات خواهد شد.

۱-۱۳-۱۴- آسیب‌های نرم‌افزاری

با توجه به این که نرم‌افزارها از کدهای به هم پیوسته تشکیل شده است عملاً می‌توان با نوشتن کدهای خاص، نرم‌افزار را به سمت خاصی هدایت نمود. چنان‌چه نویسنده نرم‌افزار در نرم‌افزار خود از کدهای پنهان استفاده نماید می‌تواند باعث آسیب‌های نرم‌افزاری گردد و آسیب‌های نرم‌افزاری به صورت عمدی و یا غیرعمدی در نرم‌افزارها قرار داده شود.

۱-۱۳-۱۵- آسیب به اطلاعات خصوصی

هر کاربر زمانی که با رایانه کار می‌کند هم‌زمان تولید اطلاعات خصوصی می‌نماید. به‌طور مثال درصورتی‌که در نظر داشته باشد بر روی اینترنت از آدرس ایمیل استفاده نماید باید از قبل با ارائه اطلاعات خصوصی آن را ایجاد نماید و یا چنان‌چه در نظر داشته باشد برای استعلام قبولی و یا عدم قبولی در کنکور استعلامی انجام دهد باید اطلاعات خصوصی را در رایانه وارد نماید و یا اگر در نظر داشته باشد اطلاعات بانکی خود را کنترل نمایند باید اطلاعات خصوصی را در رایانه وارد نماید تجمیع این اطلاعات در رایانه می‌تواند باعث آسیب رسانی به اطلاعات خصوصی گردد.

۱-۱۳-۱۶- کلاهبرداری در اطلاعات

سوءاستفاده کنندگان از اطلاعات به دنبال دسترسی به اطلاعات می‌باشند تا بتوانند بر اساس آن از افراد کلاهبرداری نمایند یکی از خطراتی که رایانه و اطلاعات آن را تهدید می‌کند دسترسی افراد کلاهبردار به اطلاعات و سواستفاده از آن می‌باشد.

۱-۱۴- امنیت چالش اصلی جهان نوین

با توجه به این که در کلیه کشورهای جهان مسائل زیر به عنوان یکی از اولین اولویت‌های استفاده از ابزار نوین می‌باشد، مسئله امنیت آن نیز اولویت اول را در بر می‌گیرد. تمام کشورهای دنیا به خاطر حفظ امنیت ملی خود تلاش بر این دارند تا امنیت ابزار نوین دیجیتال خود را حفظ نمایند و این مسئله به چالشی جهانی تبدیل شده است.

در تمام دنیا:

- افزایش اطلاعات
- تبدیل اطلاعات آنالوگ به دیجیتال

- استفاده از اطلاعات در مبدأ تولید
- افزایش توان بهره‌برداری از اطلاعات
- سرعت بخشی به تبدیل اطلاعات به تصمیم

جزو دغدغه‌های اصلی تمام کشورها می‌باشد.

۱-۱۵- سئوالات خودآزمایی

۱. ضمن تعریف اطلاعات، نقش اسناد در امنیت اطلاعات را بیان نمایید.
۲. پدافند غیر عامل را تعریف کرده و اختلاف آن را با پدافند عامل بیان نمایید.
۳. اختلاف بین تهدیدات و فرصت‌ها در دنیای سنتی و نوین را بیان نمایید.
۴. انواع تهدیدات را نوشته و تهدیدات انسان ساخت را توضیح دهید.
۵. انواع اطلاعات دیجیتال را نام برده و توضیح دهید.
۶. پنج نوع از آسیب‌های دنیای دیجیتال را نام برده و توضیح دهید.
۷. اصل کلی و اصول فرعی امنیت دیجیتال را نام برده و توضیح دهید.

۲

فصل دوم - آشنایی با پدافند غیر عامل فاوا

-

آن‌چه در این فصل خواهید آموخت:

- **تعریف فاوا**
- **تعریف پدافند غیر عامل**
- **تعریف پدافند غیر عامل فاوا**
- **سابقه پدافند غیر عامل فاوا**
- **مفاهیم امنیت در فاوا**

۲- آشنایی با پدافند غیر عامل فاوا

پدافند غیر عامل از ابتدا تاکنون در حوزه‌های تخصصی مختلفی نمود داشته و عرصه اقدامات پیش‌گیرانه را به روی کاربران گشوده است. یکی از عرصه‌های آسیب‌پذیر دنیای ارتباطات و فن‌آوری اطلاعات می‌باشد که در این فصل اختصاصاً به آشنایی با پدافند غیر عامل در حوزه فاوا[1] خواهیم پرداخت.

۲-۱- تعریف فاوا

هر چند به نظر می‌رسد مفهوم فن‌آوری اطلاعات، و فن‌آوری اطلاعات و ارتباطات (فاوا) روشن باشد اما در واقع چنین نیست. تعاریف مختلفی از فن‌آوری اطلاعات توسط افراد مختلف ارائه شده است. از جمله می‌توان به تعاریف زیر اشاره نمود:

- مطالعه، طراحی، توسعه و مدیریت کلیه نرم‌افزارها و سخت‌افزارهایی که در یک شبکه و یک محیط ارتباطی با هم کار می‌کنند.
- منظور از فن‌آوری اطلاعات همه شکل‌های فن‌آوری است که به وسیله آن‌ها عملیات دستیابی، ذخیره سازی و مبادله اطلاعات به شکل‌های گوناگون مثل متن، تصویر، صدا و نمایش چند رسانه‌ای انجام می‌شود.
- فن‌آوری اطلاعات دانشی است که به بررسی ویژگی‌ها و چگونگی اطلاعات نیروهای حاکم بر جریان اطلاعات و ابزار آماده سازی آن‌ها برای به حداکثر رساندن دست‌یابی به اطلاعات و قابل استفاده کردن آن می‌پردازد. آماده سازی اطلاعات شامل تفکیک اطلاعات دقیق، علمی و مستند، جمع آوری، سازمان دهی، ذخیره، بازیابی، تفسیر، اشاعه و استفاده از آن می‌شود. (مؤسسه فن‌آوری جورجیا، ۱۹۶۲ – نقل از اترتون،۱۹۹۷).
- اصطلاح فن‌آوری اطلاعات برای توصیف فن‌آوری‌هایی به کار می‌رود که ما را در ضبط، ذخیره سازی، پردازش، بازیابی، انتقال و دریافت اطلاعات یاری می‌کند. این اصطلاح، فن‌آوری‌هایی مانند رایانه، انتقال از طریق دورنگار، ارتباط از راه دور، تلفن، ماشین حساب، چاپ و حکاکی را نیز در بر می‌گیرد (کیت بهان و دیانا هولمز، ۱۹۹۸).

---

[1] فن‌آوری اطلاعات و ارتباطات

- فن‌آوری اطلاعات به مجموعه به هم پیوسته‌ای از روش‌ها، سخت‌افزارها، نرم‌افزارها، و تجهیزات ارتباطی که اطلاعاتی را در اشکال گوناگون (صدا، تصویر و متن) جمع آوری، ذخیره سازی، بازیابی، پردازش، انتقال و یا عرضه می‌کند، اتلاق می‌شود (دبیرخانه شورای عالی انفورماتیک، ۱۳۷۸).
- فن‌آوری اطلاعات متشکل از سخت‌افزار، نرم‌افزار، نیروی انسانی، اطلاعات، مدیریت، تولید و نگهداری است که در ارتباط متقابل با یک‌دیگرند و فضایی مملو از اطلاعات ذخیره شده به صورت نظام‌دار و با قابلیت دسترسی آسان پدید می‌آورند. این فضا در خدمت نیازهای اقتصادی، اجتماعی و فرهنگی جامعه قرار می‌گیرد و سبب بهره‌وری و افزایش کیفیت و محصولات سازمان‌های متبوع می‌شود (اسکاپ ESCAP).
- فن‌آوری اطلاعات همانند محور و مرکز مجموعه‌ای از فعالیت‌های هدایت شده است که کنترل مدیریت، بهره‌وری، تولید، آموزش و ارتقای یک سیستم (اعم از سازمان یا پایگاه اطلاعاتی و. . .) را با یک مرکزیت بر عهده دارد. همه سازمان‌ها، ارگان‌ها، نهادها و وزارتخانه‌ها ناگزیر از برقراری ارتباط با یک‌دیگر و انتقال اطلاعات هستند. سازمان فن‌آوری اطلاعات مسؤول برقراری این ارتباطات در اشکال پیش‌رفته الکترونیکی است و به طور کلی مسؤلیت کلی تولید، حفظ، ذخیره، بازیابی و انتقال اطلاعات در یک شبکه پیچیده را بر عهده دارد (محمدی، ۸۲).
- فن‌آوری اطلاعات، نقطه هم‌گرایی الکترونیک، پردازش داده‌ها و ارتباطات دور که شامل تعدادی رایانه قوی، فن‌آوری‌های ارتباطی و هم‌چنین نرم‌افزار است، که نیاز به آن بر اثر سه عامل ایجاد می‌شود. اول آن که فن‌آوری اطلاعات خود صنعتی راهبردی (استراتژیک) و بسیار سودآور در جهان است. دوم آن که فن‌آوری کلیدی است و در همه صنایع و خدمات کاربرد دارد. سوم آن که زیر بنای اساسی است که به همه مؤسسات و واحدهای اقتصادی امکان می‌دهد تا در استفاده از دانش بشری و انتقال آن سهیم شوند ؛ سبب کاهش هزینه‌ها می‌شود و در نتیجه به افزایش بهره‌وری و کیفیت محصول می‌انجامد (سازمان راهبردهای فن‌آوری اطلاعات آمریکاNSIT).
- فن‌آوری اطلاعات تنها در ارتباط با رایانه‌ها، نرم‌افزار و یا خدمات وابسته به آن‌ها نیست. فن‌آوری اطلاعات ترکیبی از همه این موارد است با این نگرش که چگونه

این فن‌آوری می‌تواند کمکی به سازمان و رسیدن به اهداف آن کند. . . . فن‌آوری اطلاعات باعث می‌شود انجام کارهای زیاد و طولانی با عملیات کمی انجام گیرد (Sutter ۲۰۰۳).

- فن‌آوری اطلاعات نوعی از فن‌آوری است که در آن انتقال داده، اطلاعات و دانش انجام می‌گیرد. این مفهوم ضرورتاً وابسته به رایانه‌ها نیست، هر چند که امروزه رایانه‌ها به عنوان ابزاری در گسترش و ایجاد راه‌هایی بسیار قدرتمند در انجام امور هستند. نقشه‌کشی، هندسه تحلیلی، دستگاه‌های کپی، تلگراف، تلفن، فاکس و غیره به خوبی نمونه‌هایی از فن‌آوری اطلاعات هستند (Fischiner ۲۰۰۰).
- برای بسیاری از مردم این واژه مترادف است با « فن‌آوری جدید» که از ماشین‌هایی که بر مبنای ریز پردازنده‌ها کار می‌کنند، استفاده می‌کند. به عبارت دیگر گفته می‌شود که « فن‌آوری اطلاعات » به طور ساده، بیانگر کوششی است برای ممکن نمودن توسعه و پیشرفت محرک‌های تجارتی به طور الکترونیکی و هم‌چنین ایجاد حرکتی سیاست گونه برای کنترل دسترسی به اطلاعات (Zorkoczy and Nicholas ۱۹۹۵).
- در سال‌های اخیر، کتاب‌ها، مجلات، مقالات و کنفرانس‌ها، راه‌هایی را برای ارتباط پژوهشی و علمی ایجاد نموده‌اند. امروزه فن‌آوری به ویژه فن‌آوری اطلاعات، در حال تاثیر گذاری بر روی هر یک از این سیستم‌های ارتباطی است. نشر الکترونیکی، متن الکترونیکی، پیام مبتنی بر صدا و کنفرانس‌های تصویری، چند نمونه از اثر فن‌آوری اطلاعات هستند. فن‌آوری اطلاعات به ما راه‌های جدیدی برای ارتباط می‌دهد و اساساً این امکان را به وجود می‌آورد تا سیستم‌های ارتباطی موجود نیز مورد تصحیح و بهبود قرار گیرند. این کار آسان به نظر می‌رسد که تغییر و تحول از سیستم‌هایی که از تنظیمات دستی استفاده می‌کنند به سیستم‌های الکترونیکی انجام گیرد (Karamouzis ۱۹۹۹).
- فن‌آوری اطلاعات ترکیبی از دو مفهوم فن‌آوری و اطلاعات است. اطلاعات مفهوم گسترده‌ای را در بر دارد و به یک سری محتویات اشاره می‌شود، در حالی که فن‌آوری به ابزارهایی که برای دست‌کاری این محتویات به کار می‌رود، گفته می‌شود. فن‌آوری یک عنصر ضروری درتراکنش‌های پردازش اطلاعات است که مشاهده، آگاهی و تجربه از یک رابطه سلسله مراتبی در آن برخوردار هستند. اطلاعات منجر به پیدایش آگاهی شده، و از به وجود آمدن آگاهی زیاد، تجربه

حاصل می‌گردد. اطلاعات از داده‌هایی که ضرورتاً قابل احساس و ادراک هستند نشأت می‌گیرد. هنگامی که داده‌ها برای استفاده در برخی امور سودمند به دسته‌ها و طبقه‌هایی دسته بندی و سازمان دهی می‌شوند، تبدیل به اطلاعات می‌گردند (Chaurasia ۲۰۰۳).

- فن‌آوری اطلاعات هر مجموعه‌ای از ابزارها، روش‌ها و رسانه‌ها است که برای ثبت، ذخیره، و انتقال اطلاعات به کار گرفته می‌شود. معمولاً امروزه هنگامی که این اصطلاح را به کار می‌بریم، در حقیقت در مورد زیر مجموعه خاصی از فن‌آوری اطلاعات صحبت می‌کنیم: فن‌آوری اطلاعات دیجیتالی شبکه‌ای (Willis ۲۰۰۲).
- فن‌آوری اطلاعات عبارت است از سخت‌افزار، نرم‌افزار، ارتباط مخابراتی و سرویس‌ها و خدماتی از کارمندان فن‌آوری اطلاعات (Effy Oz ۲۰۰۲).
- فن‌آوری اطلاعات، حوزه‌ای نسبتاً جوان در مقابله با اکثر نظام‌های علمی دیگر است. با این وجود، در حدود ۵۰ سال، این فن‌آوری به عنوان بخشی از علم و دانش در آمده که به خوبی قابل استدلال بوده و تقریباً پیچیده‌تر از نظام‌های علمی سنتی از قبیل ادبیات یا روانشناسی، و یا پیچیده‌تر از حوزه‌های حرفه‌ای از قبیل کسب و کار یا قانون است. در هر صورت، فن‌آوری اطلاعات، اساساً متفاوت از این نظام‌ها در برخی از نسبت‌های مهم بوده، و بنابراین سواد فن‌آوری اطلاعات، ضرورتا متفاوت از سواد در حوزه‌های دیگر است(Ralph ۱۹۹۷).

اما به نظر می‌رسد هیچ‌یک از تعاریف، نتواند ابعاد حقیقی مفهوم فاوا را به درستی تبیین نماید. این‌ها واژه یکسانی را برای مفاهیم مختلف به کار می‌برند. لازم به تذکر است که مفهومی که مستقل از یک واژه، با توجه به معنای لغات و صرف نظر از موارد کاربردی و استدلالات به کار برندگان آن، استنباط می‌شود، ممکن است با مفهومی که این واژه در تبیین آن مفهوم رواج دارد، متفاوت باشد. هدف ما در این جا، شناسایی آن مفهوم است. به نظر می‌رسد سه دیدگاه مختلف، و سه دسته مختلف از تعاریف – مفاهیم برای فاوا وجود داشته باشد :

دسته اول: این دسته، مفهوم فن‌آوری اطلاعات (و ارتباطات) را به نوعی همان فن‌آوری رایانه و سیستم‌های رایانه‌ای اطلاعاتی و ارتباطی، در وجود نرم‌افزار و سخت‌افزار و شبکه و نظایر آن و مسائل مدیریتی مربوط به آن می‌دانند. اغلب تعاریف از این دسته‌اند

دسته دوم: این دسته فن‌آوری اطلاعات را از بُعد اطلاعات محض آن که حتی شامل مواردی نظیر مستند سازی و کتاب‌داری نیز می‌شود، مورد توجه قرار می‌دهند. در این دسته تمرکز بر خود اطلاعات است و فن‌آوری اطلاعات، هرگونه استفاده از ابزارها و روش‌ها و

تکنیک‌هایی است که مدیریت و سازماندهی این اطلاعات را فراهم می‌کند. تعریف‌های اولیه و با سابقه بیش‌تر از این دسته‌اند. البته این مفهوم شاید نزدیک‌ترین مفهوم به معنای مستقیم واژه فاوا باشد. از جمله تعریف مؤسسه فن‌آوری جورجیا از این دسته است.

دسته سوم: این دسته، برای فاوا نقشی کلیدی و محوری نسبت به سایر فن‌آوری‌ها و کاربردها قائل می‌شود. این دسته با زاویه‌ای فراتر از زاویه‌های دو دسته قبلی به فاوا نگاه می‌کند. اما مشکل این دسته آن است که به درستی نمی‌تواند ابعادی را که برای فاوا از این زاویه مشاهده می‌کند، توضیح دهد و در یک عبارت و تعریف مشخص، بیان کند. از جمله تعریف سازمان راهبردهای فن‌آوری آمریکا (NSIT) و تعریف آخر از این دسته‌اند.erfan۲۰۰۰persiangig.ir

۲-۲- تعریف پدافند غیر عامل

علاقه به حیات و حفظ بقاء به صورت غریزی در هر انسانی وجود دارد. لذا در طول تاریخ، بشر برای دست‌یابی به ملزومات حیاتی خود از جمله غذا و انرژی به گسترش و توسعه مراتع و زمین‌های کشاورزی و معادن پرداخته یا به جهت دفع تجاوز دشمنان خود جنگ‌ها و منازعات بسیاری را پشت سر نهاده است. سلاح‌هایی که جوامع بشری قبل از دوران صنعتی در جنگ‌ها به کار می‌بردند دست ساز و بسیار ساده بود. بین روند رشد دانش و فن‌آوری با نوع سلاح‌هایی که جوامع بشری برای بهره گیری از آن‌ها در جنگ ابداع و اختراع می‌کرده‌اند، ارتباط نزدیکی وجود داشته است.

در دوران معاصر، این پیوستگی در اثر تحولات و پیشرفت‌های عظیم در فن‌آوری رو به فزونی نهاده است. پس از وقوع انقلاب صنعتی که توسعه‌ی همه‌جانبه‌ای را در همه‌ی سطوح فن‌آوری پدید آورد، تحولات گسترده‌ای در نوع و کیفیت استفاده از تجهیزات تسلیحاتی نیز ایجاد شد.

اساساً جنگ‌ها و منازعات در طول تاریخ به دلیل تعارض منافع و تمایل ذاتی انسان‌ها به برتری جویی روی داده است. در درگیری‌ها، طرفین درگیری تمایل دارند خواسته‌های خود را در حوزه‌های مختلف بر گروه مقابل تحمیل کنند و این کار در صورت عدم موفقیت در عرصه‌ی دیپلماسی منجر به جنگ می‌گردد.

ماهیت جنگ‌ها و تخاصمات بشری در دوره‌های مختلف تاریخ دستخوش تغییرهای زیادی گردیده است. در عصر حاضر پس از پشت سر گذاشتن سه نسل از جنگ‌ها، در چهارمین دوره از منازعاتی قرار داریم که از ابتدای تاریخ بین افراد و جوامع مختلف در گرفته است. در ادامه به بررسی نسل‌های مختلف جنگ می‌پردازیم.

نسل اول جنگ

از زمان پیدایش پدیده جنگ بین گروه‌های جمعیتی (قبایل و. . .) و با تشکیل حکومت‌ها توسط انسان بین ملت‌ها یا کشورها تا ورود سلاح‌های آتشین به میدان جنگ در این نسل از جنگ‌ها قرار می‌گیرند که عموماً متکی به تعداد نفرات و زور و بازو یا توان برخی افراد و مهارت آن‌ها در بکارگیری سلاح‌های سرد بوده است. گرچه نبوغ فرماندهان و طراحان جنگ همیشه نقش اساسی داشته است.

نسل دوم جنگ

با ورود سلاح‌های آتشین به عرصه جنگ‌ها، بسیاری از اصول و مبانی طرح ریزی و فرماندهی جنگ تغییر کرد. اهمیت زور و نیروی بدنی و تعداد نفرات تا حدودی کاسته شد. میدان درگیری و مانورها و حرکات تغییر کرد، برج و باروها و. . . آسیب پذیر شدند و بدین‌ترتیب انسان نسل دوم جنگ‌ها را تجربه کرد.

نسل سوم جنگ

انقلاب صنعتی موجب تحول و شکوفایی بشر در عرصه اختراعات و تولید فن‌آوری‌ها و ماشین‌های مختلف گردید. ورود فن‌آوری‌ها و ماشین‌ها (خودروها، تانک، نفربر، هواپیما، زیردریایی و تجهیزات پیش‌رفته) به عرصه جنگ‌ها، یک‌بار دیگر حوزه‌های طرح ریزی و فرماندهی جنگ را بشدت تحت تأثیر قرار داده و متحول ساخت. تعاریف و مفاهیم (قوی و ضعیف و. . .) تغییر کرد. عرصه‌های درگیری و نبرد به طرز حیرت آوری توسعه یافت و بشر یک دوره نسبتاً طولانی و بسیار خسارت‌بار با تلفات انسانی غیرقابل تصور از جمله دو جنگ جهانی و صدها جنگ منطقه‌ای و محدود را از این نسل جنگ‌ها تجربه کرده و در حال تجربه کردن می‌باشد.

نسل چهارم جنگ

تدوام رشد علوم و فن‌آوری‌ها موجب شد که قدرت‌های سلطه‌گر تحمیل منافع و نظرات خود بر رقبا و کشورهای ضعیف را بدون جنگ فیزیکی و نظامی و با بکارگیری ابزارهای قدرت اقتصادی، سیاسی، تبلیغاتی، فرهنگی و. . . طرح ریزی و تعقیب نمایند و ضربه و جنگ نظامی را به عنوان آخرین حربه در اولویت آخر قرار دهند تا ضمن ارائه ریاکارانه چهره‌ی مسالمت‌جو، خود را از عوارض (هزینه‌ها، تلفات و. . .) جنگ نظامی دور نگه دارند و بدین‌ترتیب بشر سال‌های نخست نسل جدید جنگ یعنی جنگ‌های نسل چهارم را آغاز کرده است.

این تغییرات که از آن به نسل چهارم جنگ‌ها تعبیر می‌شود، منجر به بروز جنگ‌های اقتصادی و اجتماعی گردیده است. در این نسل نوپا از درگیری‌ها، دشمنان با استفاده از

حربه‌های اقتصادی، فرهنگی و اجتماعی و با به کارگیری همه‌ی مؤلفه‌های قدرت به زورآزمایی می‌پردازند. منازعات نسل چهارم در قدیمی‌ترین شیوه‌ی خود در تحریم‌های اقتصادی نمود یافت. اما استفاده از ابزارهای نوین اطلاع‌رسانی، گسترش شبکه‌ی جهانی اینترنت و به وجود آمدن شبکه‌های اجتماعی در بستر آن و نیز خدمات پردازش سیار به گسترش این دسته از منازعات در عرصه‌ی اجتماعی کمک شایانی نموده است. در واقع مهاجمان در این نوع درگیری‌ها با اجرای انواع توطئه‌های اقتصادی و سیاسی و نیز با گسترش فضای نارضایتی اجتماعی از طریق شبکه‌های ارتباطی و اطلاع‌رسانی، حریف خود را درگیر مشکلات داخلی و بین‌المللی نموده و از این طریق وی را به پذیرش اغراض سیاسی خود در میدان زورآزمایی‌های داخلی یا فرامنطقه‌ای مجبور می‌سازند.

در قبال این نوع منازعه تجهیز به ابزارهای دفاعی یا پدافندی تنها منحصر به نظامیان و لشکریان نیست. بلکه لازم است کلیه‌ی افراد، سازمان‌ها و مجموعه‌ها را با فرآیندها و روش‌هایی غیرنظامی برای مقابله آماده ساخت.

پدافند غیرعامل به مجموعه اقداماتی اطلاق می‌گردد که مستلزم به کارگیری جنگ افزار نبوده و با اجرای آن می‌توان از وارد شدن خسارت به تجهیزات و تاسیسات حیاتی و حساس نظامی و غیرنظامی و تلفات انسانی جلوگیری نموده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد.

در ادبیات موضوع، علاوه بر پدافند غیرعامل، به مفهومی به نام دفاع غیرنظامی برمی‌خوریم که عبارت است از تقلیل خسارات مالی و صدمات جانی وارده بر غیرنظامیان در جنگ یا در اثر حوادث طبیعی نظیر سیل، زلزله، طوفان، آتش‌فشان، آتش‌سوزی و خشک‌سالی.

در منابع تخصصی سایر کشورها، وظایف دفاع غیرمسلحانه شامل چهار عنوان می‌باشد:

- اقدامات پیش‌گیرانه و کاهش دهنده[۱]
- آماده سازی و امداد رسانی[۲]
- هشدار و اخطار[۳]
- باز سازی مجدد[۴]

---

[۱] Mitigation

[۲] Preparation

[۳] Response

[۴] Recovery

اقدامات دفاع غیرعامل شامل اصول اساسی و ملاحظاتی است که در اغلب کشورهای جهان، با کمی اختلاف پذیرفته شده‌اند ولی شیوه به کارگیری آن‌ها ابتکاری، هنرمندانه و خردمندانه است. به همین دلیل وسعت این اقدامات به خلاقیت‌های فکری بشر و شرایط زمان و مکان بستگی دارد و بعضاً نمی‌توان حد و مرزی برای آن تعیین کرد.

در تعریف دیگری پدافند غیرعامل به کلیه‌ی اقدامات و تدابیری گفته می‌شود که بدون استفاده از سلاح موجب کاهش آسیب‌پذیری، تلفات و خسارات و افزایش پایداری شود.

به طور خلاصه می‌توان گفت پدافند غیرعامل یعنی دفاع در مقابل تهدید، بدون استفاده از سلاح. به عبارتی دفاع غیرعامل، مکمل دفاع عامل است و در حوزه‌ی امنیت ملی مفهوم دفاع، تلفیقی از دفاع عامل و دفاع غیرعامل است.

اقدامات پدافند غیرعامل در سطوح مختلفی طراحی و اجرا می‌گردند. این سطوح شامل موارد زیر است:

۱. سطح استراتژیک: اقداماتی است که در سیاست‌های کلی کشور و تأمین مبانی و پشتوانه‌های قانونی، حقوقی و سیاست‌های برنامه بلندمدت توسعه کشور تأثیرگذار است.
۲. سطح عملیاتی: اقداماتی است که در برنامه‌های ۵ ساله‌ی توسعه‌ی سازمان‌ها تأثیرگذار است.
۳. سطح تاکتیکی: اقداماتی است که در برنامه‌های سالانه‌ی سازمان مؤثر است.
۴. سطح اقدامات ویژه: که شامل اقداماتی است که تأثیر آن در اولویت‌های خاص و نقاط مهم می‌باشد.

اگر بخواهیم به صورت فهرست‌وار به برخی از اقدامات پدافند غیرعامل در حوزه‌های غیر از فن‌آوری اطلاعات اشاره کنیم، موارد زیر قابل ذکر است :

- مکان یابی مناسب
- انتخاب مقیاس بهینه
- پراکندگی در سایت
- استفاده از عمق زمین
- توزیع عمل‌کرد
- فریب در نمای عمل‌کردها
- داشتن طرح پوشش و فریب
- مدیریت بحران ناشی از جنگ

- موازی سازی اقدامات
- کاهش وابستگی
- پوشش اطلاعاتی
- چند منظوره کردن عمل‌کردها
- کاهش امکان تهدید
- استفاده از فن‌آوری بومی
- توسعه شبکه پایش و هشدار امنیتی
- ایجاد اهداف مجازی وکاذب
- ایمن سازی سیستم فرماندهی وکنترل
- نامرئی سازی در برابر دشمن
- تولید موانع دومنظوره و چند منظوره

از منظر امنیت ملی، پدافند غیرعامل بستر مناسبی برای توسعه‌ی پایدار اقتدار ملی کشور در حوزه‌ی دفاعی است. هم‌چنین پدافند غیرعامل با سیاست‌های تنش‌زدایی هم‌راستا است. چراکه کشورهایی که توسعه پدافند غیر عامل را به عنوان یک سیاست دفاعی مستمر در دستور کار خود قرار می‌دهند هیچگاه در مظان اتهام تهدید بر علیه کشورهای دیگر قرار نمی‌گیرند.

اقدامات پدافند غیرعامل به دلیل غیرنظامی بودن، پایدارترین و ارزان‌ترین روش دفاع و هم‌چنین مناسب‌ترین راهکار افزایش آستانه‌ی مقاومت می‌باشد. این دسته از اقدامات مناسب‌ترین شیوه‌ی کاهش مخاطرات و آسیب‌پذیری‌ها و از طرفی مهم‌ترین ابزار بازدارندگی هستند. به عبارت دیگر کشورهایی که پدافند غیر عامل را به عنوان یک راه کار اصلی بر می‌گزینند به شرایطی از نظر کاهش آسیب‌پذیری دست می‌یابند که مطامع کشورهای تهدید کننده بر علیه آن‌ها کاهش می‌یابد.

در جهان امروز کشورهایی که نقاط آسیب‌پذیری آن‌ها فراوان است و دشمن می‌تواند با ضربات سریع، حیاتی‌ترین منابع آنان را منهدم نماید، عوامل تهدید بیرونی را تحریک و دشمنان را تحریص می‌نمایند. از این رو برای دست‌یابی به یک توسعه‌ی پایدار با سطح قابل قبولی از امنیت، پدافند غیرعامل در سطح کشور باید به یک فرهنگ عمومی تبدیل شود. (پدافند غیرعامل کشور – پورابراهیمی و بنابی -۱۳۸۹)

اقدامات پدافند غیرعامل باید در سه حوزه امنیت، ایمنی و پایداری طرح‌ریزی و اجرا شود. مجموعه این اقدامات در کنار یک‌دیگر و به عنوان سه جزء اساسی و غیر قابل تفکیک می‌باشند. ترکیب این سه جزء در کنار یک‌دیگر می‌تواند در تأمین دفاع غیرعامل و کاهش آسیب‌پذیری

زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم کشور در مقابل تهدیدها از طریق فرهنگ‌سازی، سیاست‌گذاری، طرح‌ریزی و برنامه‌ریزی راهبردی و تدوین ضوابط و دستورالعمل‌های تخصصی با قابلیت هدایت بخش‌های کشوری و لشکری موفق باشد.

به بیان ساده‌تر می‌توان گفت ایجاد بازدارندگی دفاعی کشور از طریق اقدامات پدافند غیرعامل مستلزم :

- حفظ اسرار و اطلاعات کشور و ممانعت از دسترسی دشمنان به اطلاعات ارزشمند ملی و بخشی کشور
- ایمن‌سازی زیر ساخت‌های ملی و مراکز حیاتی، حساس و مهم.
- پایدار سازی زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم کشور

می‌باشد.

در نگرش سیستمی این عوامل سه جزء یک سیستم می‌باشند که در تعامل با یک‌دیگر مفهومی تحت عنوان توسعه‌ی دفاع غیرعامل و افزایش قدرت بازدارندگی را شکل می‌دهند.

۲-۲-۱- امنیت

امنیت اطلاعات از جنبه‌های مختلف حائز اهمیت می‌باشد که محرمانگی و در دسترس بودن و حفظ تمامیت از جمله آن‌ها می‌باشد. امروزه بدون بومی سازی نمی‌توان انتظار ایجاد امنیت مطلوب را داشت. امنیت از جمله مواردی می‌باشد که معمولاً در تضاد با برون سپاری بوده و می‌بایست توسط نیازمند به امنیت و به صورت بومی تولید و ایجاد گردد.

۲-۲-۲- ایمنی

ایمنی به مفهوم امن بودن در مقابل تهدیدها و حملات سخت و نیمه سخت می‌باشد. هر سیستمی به منظور تداوم بقاء و توان ارائه تولیدات و خدمات باید ایمن باشد. به منظور تامین ایمنی باید در خصوص هر یک از مراکز حیاتی، حساس و مهم طرح‌های لازم تهیه گردد. برای این منظور باید نسبت به تعریف و درجه بندی میزان حفاظت برای هر طرح در برابر تهدید اقدام شود.

هر چند در هر برنامه‌ریزی، تحلیل هزینه- فایده باید مد نظر قرار گیرد، در مواردی که تأمین ایمنی مراکز حیاتی، حساس مورد نظر است این اقدامات باید با اولویت بالا تامین هزینه شود. چرا که باید در مقابل منافع ظاهری، منافع مؤثر در امنیت ملی در این حوزه نیز مورد توجه باشد.

برخی از اقداماتی که در این حوزه می‌توان انجام داد عبارتند از:

- سطح بندی (تعیین میزان اهمیت تأسیسات، مرکز یا تشکیلات)
- تعیین اهمیت واولویت طرح‌ها
- تعیین سطح ایمنی مورد نیاز
- مکان یابی
- طراحی
- تعیین شاخص‌ها واستانداردهای پدافند غیرعامل در استقرار عمل‌کردها
- تعیین شاخص‌های عمل‌کردی هر سیستم در استقرار
- تعیین مجموعه ضوابط واستانداردها برای استقرار
- بررسی نقاط امن در پهنه‌ی جغرافیای مورد نظر
- انتخاب گزینه‌های نقاط امن برای استقرار عمل‌کردها
- تعیین شاخص‌های مناسب مکان گزینی پدافند غیرعامل
- امتیاز دهی و وزن دهی به شاخص‌ها بر اساس اهمیت و وزن
- انتخاب جای‌گزین بهینه در مکان‌گزینی مناسب برای استقرار طرح‌ها

۲-۲-۳- پایداری

هرچند امنیت و ایمنی سیستم‌ها از منظر پدافند غیر عامل بسیار مهم و ضروری است اما به مفهوم تامین سیستم دفاعی کامل نمی‌باشد. یکی از نکات مهم، وجود پایداری در تولید و ارائه خدمات در مراکز حیاتی، حساس و مهم است. پایداری به این معنی است که یک مرکز در شرایط عادی و یا در صورت بروز حمله و خدشه دار شدن هر دو یا یکی از دو جزء ذکر شده، یعنی امنیت و ایمنی، باید امکان تداوم ارائه تولیدات و خدمات خود را داشته باشد. برای این تداوم و پایداری سیستم‌ها راه کارها و شیوه‌های مختلفی وجود دارد. برخی از این راه کارها عبارتند از:

- موازی سازی
  - تأمین ظرفیت‌های موازی
  - پیش بینی روش‌های موازی
- تأمین احتیاط[۱]
- کاهش وابستگی

[۱] Back up

- وابستگی فن‌آورانه، علمی و. . . به خارج از کشور
- وابستگی خدمات و پشتیبانی به سایر بخش‌ها (داخلی یا خارجی)
- تنوع منابع پشتیبانی

- توسعه اشتراک منافع
- توسعه و ارتقاء موقعیت بین المللی (به‌دست آوردن فرصت‌های منطقه‌ای و بین‌المللی)

۲-۳- تعریف پدافند غیر عامل فاوا

هر اقدام غیر مسلحانه‌ای که موجب کاهش آسیب‌پذیری نیروی انسانی، ساختمان‌ها، تاسیسات، تجهیزات، اسناد و شریان‌های کشور در مقابل عملیات خصمانه و مخرب دشمن گردد، پدافند غیرعامل خوانده می‌شود.

به بیان ساده‌تر پدافند غیرعامل، مجموعه اقداماتی است که انجام می‌شود تا در صورت بروز جنگ و حتی در زمان صلح، خسارات احتمالی به حداقل میزان خود برسد.

هدف از اجرای طرح‌های پدافند غیرعامل کاستن از آسیب‌پذیری نیروی انسانی، تجهیزات حیاتی و حساس و مهم کشور علی‌رغم حملات خصمانه و مخرب دشمن و استمرار فعالیت‌ها و خدمات زیر بنایی و تامین نیازهای حیاتی و تداوم اداره کشور در شرایط بحرانی ناشی از جنگ است.

به عنوان مثالی ساده، از پدافند غیرعامل می‌توان به استتار، اختفا و ایجاد سرپناه برای تاسیسات مهم و استراتژیک اشاره کرد.

در پدافند عامل مثل سیستم‌های ضد هوایی و هواپیماهای ره‌گیر، فقط نیروهای مسلح مسئولیت دارند. در حالی که در پدافند غیرعامل تمام نهادها، نیروها، سازمان‌ها، صنایع و حتی مردم عادی می‌توانند نقش مؤثری بر عهده گیرند.

دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد. چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب‌دیده را با کم‌ترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد، ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. به‌کارگیری تمهیدات

و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارآیی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

با پیچیده‌تر شدن جنگ‌ها و به کارگیری تکنولوژی و فن‌آوری در جنگ‌های نوین، پدافند غیر عامل نیز چهره‌های متفاوتی را به خود گرفته است. امروزه مردم برای ادامه زندگی نیازمند خدمات متفاوتی هستند و احتیاج به محیط آرام و قابل سکونت درون شهرها دارند و بایستی ایمنی و آسایش کافی داشته باشند.

درحال حاضر عمده‌ترین هدف پدافند غیرعامل، ایمن سازی و کاهش آسیب‌پذیری زیرساخت‌های مورد نیاز مردم است تا به تدریج شرایطی را برای امنیت ایجاد نماید. این گونه اقدامات مهم در اکثر کشورهای دنیا انجام شده و یا در حال اقدام است. این اقدامات اگر به صورت یک برنامه ریزی و با طراحی در توسعه کشور (توسعه پایدار) نهادینه شود، خودبه‌خود بسیاری از زیر ساخت‌هایی که ایجاد می‌شود، در ذات خود ایمنی خواهند داشت. برای اصلاح زیرساخت‌های فعلی هم می‌توان با ارائه راهکارهایی مثل مهندسی مجدد، آن‌ها را مستحکم کرد.

اهداف پدافند غیرعامل:

- کاهش قابلیت و توانایی سامانه‌های شناسایی، هدف یابی و دقت هدف‌گیری تسلیحات آفندی دشمن.
- بالا بردن قابلیت بقاء، استمرار عملیات و فعالیت‌های حیاتی و خدمات رسانی مراکز حیاتی، حساس و مهم نظامی و غیر نظامی کشور در شرایط وقوع تهدید، بحران و جنگ.
- تقلیل آسیب‌پذیری و کاهش خسارت و صدمات تاسیسات، تجهیزات و نیروی انسانی مراکز حیاتی، حساس و مهم نظامی و غیر نظامی کشور در برابر تهدیدات و عملیات دشمن.
- سلب آزادی و ابتکار عمل از دشمن.
- صرفه جوئی در هزینه‌های تسلیحاتی و نیروی انسانی.
- فریب و تحمیل هزینه بیش‌تر به دشمن و تقویت بازدارندگی.
- افزایش آستانه مقاومت مردم و نیروی خودی در برابر تهاجمات دشمن.
- حفظ روحیه و انسجام وحدت ملی و حفظ سرمایه‌های ملی کشور.
- حفظ تمامیت ارضی، امنیت ملی و استقلال کشور.(Persianblog. padafand-gh-amel.ir)

۲-۳-۱- امنیت دیجیتال

امنیت دیجیتال عبارت است از قابلیت اعتماد به تولید کنندگان ابزار دیجیتال که برای حفظ محرمانگی و یک‌پارچگی و دسترس‌پذیر بودن این ابزار اقداماتی را انجام داده‌اند تا در عین

این که افراد مجاز به آن بتوانند دسترسی داشته باشد افراد غیر مجاز قادر به دست‌یابی و استفاده سو از آن‌ها نباشند.

۲-۳-۲- ایمنی سرمایه‌های دیجیتال

ایمنی سرمایه‌های دیجیتال به امن نگهداشتن این سرمایه‌ها در مقابل انواع تهدیدات سخت و نیمه سخت و نرم‌افزاری می‌پردازد. با توجه به این که هر سیستمی برای ادامه بقاء خود نیازمند به ایمن بودن دارد می‌بایست با تحلیل هزینه – فایده موارد تامین ایمنی هرکدام از سرمایه‌های دیجیتال مورد تجزیه و تحلیل و بررسی قرار گرفته و به‌ترین و سودمندترین روش را که با به صرفه بودن همراه است انتخاب و به کارگیری گردد.

۲-۳-۳- پایداری سامانه‌های دیجیتال

در تامین سیستم دفاعی کامل علاوه بر مد نظر داشتن امنیت و ایمنی باید به استمرار قابلیت ادامه حیات این سرمایه‌ها نیز عنایت نمود. یکی از این نکات مهم قابلیت ارائه خدمات دیجیتال در مراکز مهم، حساس و حیاتی می‌باشد. این قابلیت زمانی می‌تواند وجود داشته باشد که در صورت حمله به این مراکز و به خطر افتادن امنیت و یا ایمنی سرمایه‌های دیجیتال هم‌چنان بتوانند به حیات خود ادامه دهند و در این زمینه پایداری لازم را داشته باشند. بدون پایداری به مجرد به خطر افتادن امنیت و ایمنی کل سرمایه دیجیتال با خطر از بین رفتن روبرو خواهد شد.

۲-۴- سابقه پدافند غیر عامل فاوا

می‌توان ادعا نمود که قدمت پدافند غیر عامل به قدمت تمدن بشری باز می‌گردد. لیکن این موضوع برای نسل‌های بشر به صورت تلاش آن‌ها برای حراست و مراقبت در برابر دشمنان طبیعی و انسانی نمایان شده است و در طول تاریخ همواره تمهیداتی را برای در امان ماندن از این حوادث مد نظر داشته است. برج و باروهای حفاظتی شهرها، قلعه‌ها و حصارها نمونه‌های بارزی در این خصوص می‌باشند.

در عصر جدید با توجه به مقتضیات عالم جدید و ایجاد دولت‌ها، این موضوع از حیطه شهری به گستره ملی انتقال پیدا نمود. با بروز جنگ جهانی اول و دوم و کشیده شدن پای جنگ به شهرها این موضوع اهمیت بیش‌تری یافت و شکل علنی به خود گرفت. پس از آن جنگ سرد و چالش‌های جهانی مرتبط با سلاح‌های کشتار جمعی اهمیت این بحث را بیش‌تر

نمود. در نهایت با وقوع حادثه ۱۱ سپتامبر و جنگ‌های دهه اخیر بین کشورها، این مبحث وارد فاز جدیدی از مطالعات و برنامه‌های اجرایی شد.

جایگاه پدافند غیر عامل در قانون برنامه چهارم توسعه:

هیات وزیران در سال ۱۳۸۴ آیین‌نامه اجرائی بند پ تبصره ۱۷ قانون بودجه سال ۸۴ کل کشور را به تصویب رسانده و در فصل ۱۰ این قانون که قوانین مرتبط با امنیت ملی مطرح شده است و در بند ۱۱ ماده ۱۲۱ به موضوع پدافند غیر عامل اشاره دارد و مطابق متن زیر مواردی را در این خصوص برای خود لازم الاجرا نموده است.

رعایت اصول پدافند غیر عامل در طراحی و اجرای طرح‌های حساس و مهم و در دست مطالعه و نیز تأسیسات زیربنایی و ساختمان‌های حساس و شریان‌های اصلی و حیاتی کشور و آموزش عمومی مردم توسط دستگاه‌های اجرایی و تخصصی موضوع ماده (۱۶۰) قانون برنامه چهارم توسعه، به منظور پیش‌گیری و کاهش مخاطرات ناشی از سوانح غیرطبیعی مد نظر بوده و این دستگاه‌ها موظف‌اند بر اساس سیاست‌ها، الویت‌ها و دستورالعمل‌های کارگروه دائمی پدافند غیر عامل کشور درصدی از اعتبارات تملک دارائی‌های سرمایه‌ای خود را جهت اجرای طرح‌های مصوب کارگروه اختصاص دهند. بر اساس این قانون کمیته‌های دائمی پدافند غیر عامل در دستگاه‌های اجرائی و تخصصی کشور به منظور اجرائی کردن اهداف پدافند غیر عامل تشکیل و فعالیت خواهند داشت.

هم‌چنین در مهر ماه سال ۸۶ سندی را با عنوان سند راهبردی پدافند غیرعامل کشور توسط مجمع تشخیص مصلحت نظام تهیه و به تصویب رسانده شده، که بخش عمده‌ای از طرح جامع پدافند غیر عامل کشور در آن پیش‌بینی شده است که شامل چشم‌انداز و همسو با چشم‌انداز ۲۰ ساله، اهداف کلان و بلند مدت، اهداف کوتاه مدت، سیاست‌های اجرایی و راهبردی می‌باشد.

تلاش برای توسعه پایدار کشور و تحقق اهداف چشم‌انداز ۲۰ ساله توسعه‌ای کشور ایجاب می‌کند، که عنصر پدافند غیر عامل که به معنی ارزیابی آسیب‌پذیرها و تهدیدهای احتمالی و برنامه‌ریزی برای حذف این موارد در اجرای طرح‌های اقتصادی، اجتمائی و توسعه‌ای کشور است، مورد توجه ویژه قرار گیرد.

موارد زیر اشاره به برخی موارد در خصوص تامین بودجه در سال ۸۶ در بخش پدافند غیر عامل با توجه به اهمیت موضوع دارد که در سال (۸۷) نیز این اعتبارات به صورت تکمیلی‌تر در قانون بودجه کشور لحاظ شده است:

۱) تبصره ۲۰ بند ر، بخش ششم از قانون بودجه سال ۸۶

بند "ر" ـ در اجرا طرح‌های پدافند غیرعامل و انسداد مرزها با اولویت مرز شرقی اجازه داده می‌شود، حداکثر مبلغ دو هزار و هشتصد و هفتاد و چهار میلیارد(۰۰۰. ۰۰۰. ۰۰۰. ۲. ۸۷۴) ریال اعتبار ردیف ۵۰۳۹۱۸ قسمت چهارم و ۲۰۲۰۱۰۲۴ پیوست شماره یک این قانون براساس پیش‌نهاد دستگاه‌های اجرایی و تصویب کمیته دائمی پدافند غیرعامل کل کشور در خصوص اعتبار ردیف ۵۰۳۹۱۸ پدافند غیرعامل در اختیار دستگاه‌های اجرائی ذی‌ربط قرارگیرد تا براساس شرح عملیات موافقتنامه مبادله شده با سازمان مدیریت و برنامه‌ریزی کشور به مصرف برسد. این اعتبارات از شمول قانون محاسبات عمومی و سایر مقررات کشور مستثنی می‌باشد.

۲) تبصره ۱۷ بند د، بخش ششم از قانون بودجه ۸۶

بند"د" ـ در اجرای طرح‌های پدافند غیر عامل موضوع آئین‌نامه اجرایی بند (۱۱) ماده (۱۲۱) قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران اجازه داده می‌شود حداکثر مبلغ چهارصد و چهل میلیارد ریال اعتبار ردیف ۵۰۳۹۱۸ قسمت چهارم این قانون، براساس پیش‌نهاد دستگاه‌های اجرایی و تصویب کمیته دائمی پدافند غیرعامل کل کشور در اختیار دستگاه‌های اجرایی ذی‌ربط قرار گیرد تا براساس شرح عملیات موافقتنامه مبادله شده با سازمان مدیریت و برنامه‌ریزی کشور (معاونت برنامه ریزی و نظارت راهبردی ریاست جمهوری) به مصرف برسد.

جایگاه فنی پدافند غیر عامل :

ریشه بحث‌های پدافند غیر عامل به نیازهای انسان برای زندگی بر می‌گردد، با مروری بر هرم نیازهای انسانی، نقش بسیار مهم خواسته ایمنی و امنیت آشکار است. پدافند غیر عامل به منظور تامین ایمنی و امنیت انسان در برابر پتانسیل‌های بروز خطر، می‌باشد. از طرفی دیگر پدافند غیر عامل را می‌توان از زاویه مدیریت بحران مورد تحلیل قرار داد، در این صورت شناسایی پتانسیل‌های بحران خیزی، نحوه مدیریت و کنترل بحران به عنوان ورودی‌های سیستم‌های پدافند غیر عامل شناخته می‌شوند.

هم‌چنین پدافند غیر عامل را از زاویه دید آسیب‌پذیری نیز مورد بررسی قرار می‌دهند، که در این صورت شناخت جایگاه‌هایی که به عنوان نقطه ضعف سیستم می‌باشند، به عنوان ورودی‌های سیستم بوده. ضلع دیگر مباحث پدافند غیر عامل بحث‌های ایجاد ایمنی و امنیت عمومی می‌باشد که به صورت آموزش و همکاری همگانی تبلور می‌یابد.

اهمیت، ضرورت و اهداف پدافند غیرعامل

برابر آمار سرشماری سال ۱۳۷۸، تعداد شهرهای کشور ۶۰۰ و تعداد روستاهای آن ۶۵۰۰ روستا بوده است، پدافند هوائی مراکز حیاتی و حساس موجود کشور در شهرها صرفاً با توپ ضد

هوائی ۲۳ میلیمتری، نیازمند ۲۴۰۰۰۰ قبضه توپ، یک میلیون و دویست هزار نفر نیروی انسانی (خدمه)، ۳۰۰۰۰ آتشبار و ۷۵۰ گردان ویژ پدافند هوایی خواهد بود که امکان تامین، تشکیل، سازماندهی و پشتیبانی آن دور از دسترس می‌باشد.

دفاع غیرعامل در واقع مجموعه تمهیدات، اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد. چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب‌دیده را با کم‌ترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد، ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارآیی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

امروزه با توجه به توسعه فاوا در کلیه امور زندگی انسان‌ها باید به این نکته توجه داشت که وارد عصر جدیدی از زندگی شده و می‌بایست با نگاه جدیدی به پدافند غیر عامل نگریست. باید باز تعریف جدیدی از امنیت و ایمنی و پایداری در عرصه فاوا ارائه نمود. این مطلب در برنامه چهارم توسعه به خوبی خود را نشان داده است. با توجه به این که بسیاری از ارکان زندگی در عصر حاضر با فاوا گره خورده است بدون در نظر گرفتن این مسئله عملاً بسیاری از اقدامات در زمینه پدافند غیر عامل می‌تواند به هدر رفته و هدف اصلی از دیده‌ها پنهان گردد.

۲-۵- مفاهیم امنیت در فاوا

با توجه به روند جنگ‌ها و شرایط حال حاضر دنیا (چه از لحاظ تکنولوژیکی و چه از لحاظ سیاست‌های راهبردی) رویکردهای زیر برطرح پدافند غیرعامل حاکم است:

۱- به عنوان یک فرض مسلم و قطعی، پرداختن و توجه ویژه به مقوله پدافند غیرعامل از لحاظ کمی و کیفی و بررسی سامانه‌هایی که می‌بایست مورد توجه پدافند غیرعامل قرارگیرند، نقش مهم و ارزشمندی را در تعیین سرنوشت جنگ بر عهده خواهد داشت.

۲- نظر به اهمیت در خور توجه و بایسته پدافند غیرعامل و سامانه‌های آن، وحدت فرماندهی و هماهنگی در خصوص نحوه و چگونگی اجرا، هدایت و راهبرد عملیات استتاری در سطوح عمودی و افقی نیروهای مسلح کشور و سایر منابع ملی، لازمه موفقیت در عملیات‌های پدافند غیرعامل و کارآمدی مدیریت راهبردی این نوع پدافند مبتنی برشیوه‌های نوین است.

۳- بدون شک پیشرفت‌های روز افزون در حوزه‌های ارتباطات، مخابرات و سیستم‌های شناسایی و جمع‌آوری اطلاعات، تغییرات قابل توجهی را در مکانیسم‌ها و ساز و کارهای حاکم بر فعالیت‌ها و چالش‌های نظامی و دفاعی به‌وجود آورده است. هم‌چنین شرایط حاضر جهانی بسیار متغییر بوده و روند رو به رشد سیستم‌های مزبور بسیار شتاب‌آلود و سریع است.

۴- از آن‌جا که روش‌های طراحی، مراقبت و نگهداری، برنامه‌ریزی و توسعه میدانی در پدافند غیرعامل نوین با توجه شرایط و نحوه رویارویی و تقابل با دشمن از نظر سیاسی و جغرافیایی متفاوت است، تنوع شرایط و راهکارها، انعطاف و پویایی مفهوم فرماندهی و کنترل عملیات پدافند غیرعامل را در پی دارد.

۲-۵-۱- تهدیدات سیستم‌های ارتباطی از منظر پدافند

همان گونه که در مغز انسان ارتباطات عصبی و انتقال اطلاعات از طریق تارهای عصبی و نرون‌ها برقرار می‌شود و به مجرد آسیب رسانی به هر کدام از این تارها، تار دیگری این وظیفه را بر عهده می‌گیرد. در دنیای فاوا نیز سیستم‌های ارتباطی مختلفی برای تعامل و انتقال اطلاعات به کار گرفته می‌شوند. در صورت آسیب‌رسانی به هر کدام از این سیستم‌های ارتباطی در صورت عدم وجود سیستم ارتباطی جای‌گزین ادامه حیات ابزار دیجیتال و انتقال اطلاعات میسر نخواهد بود. آسیب‌پذیری‌های که سیستم‌های ارتباطی را تهدید می‌نمایند به دنبال هدف از بین بردن تعاملات اطلاعاتی بوده و اصل اشرافیت بر اطلاعات را منظور نظر خود قرار می‌دهند.

۲-۵-۲- تهدیدات سیستم‌های رایانه‌ای با نگاه پدافندی

سیستم‌های رایانه‌ای از جمله سیستم‌های می‌باشند که از راه دور و نزدیک و با استفاده از ابزار دیجیتال و آنالوگ قابلیت تهدید پذیری دارند. در صورت تبدیل هر کدام از این تهدیدات از بالقوه به بالفعل عملاً ادامه عمل‌کرد سیستم‌های رایانه‌ای امکان پذیر نبوده و با اختلال مواجه خواهد شد. با توجه به این که در عصر حاضر بسیاری از روش‌های زندگی بر مبنای به کار گیری این ابزار پایه گذاری شده است، آسیب‌پذیری ابزار دیجیتال منجر به آسیب رسانی به امنیت و ایمنی و پایداری بقاء انسان‌ها خواهد شد.

۲-۵-۳- تهدیدات سیستم‌های اطلاعاتی مبتنی بر رایانه در پدافند غیر عامل

سیستم‌های اطلاعاتی مبتنی بر رایانه[۱] از انواع مختلفی تشکیل شده است. کوچک‌ترین این سیستم‌ها بانک اطلاعات می‌باشد که در ابعاد بزرگ و کوچک توسط سازمان‌ها و شرکت‌ها و موسسات و حتی افراد به صورت خصوصی به کار گرفته می‌شوند. هر چه سیستم گسترده می‌شود سیستم‌های تصمیم‌گیری[۲] به آن اضافه شده و برخی از تصمیم‌گیری‌ها روشمند شده و توسط سیستم‌ها انجام و اعمال می‌گردد. عملاً کنترل بسیاری از ابزار دیجیتال به صورت روزمره به این گونه از سیستم‌ها واگذار می‌شود و هر کس که بتواند آگاهانه یا نا آگاهانه به این سیستم‌ها دسترسی داشته و بر آن اثر گذار باشد این قابلیت را خواهد داشت تا بر خروجی سیستم نیز اثر گذار باشد. به همین دلیل امن نگه داشتن این سیستم‌ها به منزله امن نگه داشتن کل فرآیند می‌باشد.

۱ (CBIS) computer based information system

۲ (DSS) decision support system

۲-۶- سئوالات خودآزمایی

۱. فاوا مخفف چیست ؟ توضیح دهید.
۲. اصول کلی پدافند غیرعامل را نام برده و توضیح دهید.
۳. پدافند غیر عامل در حوزه فاوا را توضیح دهید.
۴. سابقه پدافند غیرعامل فاوا در ایران را بنویسید.
۵. تهدیدات سیستم‌های ارتباطی از منظر فاوا کدامند؟ توضیح دهید.
۶. تهدیدات سیستم‌های رایانه‌ای از منظر فاوا کدامند؟ توضیح دهید.
۷. تهدیدات سیستم‌های اطلاعاتی مبتنی بر رایانه از منظر فاوا کدامند؟ توضیح دهید.

۳

فصل سوم – امنیت اطلاعات

آن چه در این فصل می‌خوانید:

- **امنیت**
- **علل سرمایه گذاری در رابطه با امنیت اطلاعات**
- **جهانی شدن امنیت**
- **مهندسی اجتماعی و امنیت**
- **ردیابی اطلاعاتی و بر چسب امنیتی**
- **شناسایی اسناد کاربران امنیت در اطلاعات**
- **تعیین سطوح طبقه بندی مجاز برای اطلاعات ساختار**

۳- امنیت اطلاعات

با توجه به این که اطلاعات دارای انواع و اقسام مختلفی می‌باشد، در این فصل ضمن آشنایی با اطلاعات و انواع آن به روش‌ها و شیوه‌های امن نگهداری اطلاعات خواهیم پرداخت.

۳-۱- امنیت

۳-۱-۱- تعریف امنیت

امروز برای امنیت تعاریف مختلفی ارایه شده است و برخی امنیت را در بُعد فیزیکی آن مورد بررسی قرار داده و برخی در ابعاد روانی آن را مورد بررسی قرار داده‌اند. امروزه برخی امنیت را مترادف با کلمه حفاظت دانسته و از این زاویه به آن نگاه می‌کنند. واژه security در فرهنگ فارسی معادل واژه‌هایی همچون امن، محفوظ، مطمئن، محفوظ داشتن، تامین کردن آمده است. امنیت عمدتاً به نوعی احساس روانی اطلاق می‌گردد که به‌خاطر نداشتن ترس، وضعیت آرامش و اطمینان خاطر حاصل می‌گردد. امنیت به حداقل رساندن خطر یا تهدید است که این خطرها نه فقط از نوع سنتی و نظامی هستند بلکه تهدیدات جدید غیر نظامی را نیز در بر می‌گیرند. فقدان تهدید، عنصر اساسی تعریف امنیت است گرچه عده‌ای فقدان تهدید را امری ناممکن و دست نیافتنی دانسته و از این رو به حداقل رساندن تهدید را مفهوم اصلی امنیت می‌دانند.

۳-۱-۲- تاریخچه امنیت

برای امنیت نمی‌توان شروع زمانی خاصی را مد نظر قرار داد. از زمانی که انسان پای بر روی کره زمین نهاد به دنبال امنیت بوده است و شاید بتوان گفت دلیل این که انسان پس از خروج از بهشت و پای گذاشتن بر روی کره زمین به دنبال توبه و جبران خطای خود بوده است رسیدن به امنیت بوده است. امنیت زمانی امنیت فیزیکی می‌باشد و زمانی امنیت روحی و روانی. با بررسی نظریه مازلو مشخص می‌گردد بدون تامین امنیت در لایه‌های پایین‌تر نمی‌توان انتظار داشت که نیاز به امنیت در لایه بالاتر حس شده و انسان به دنبال تامین آن باشد. انسان‌های نخستین به دنبال تامین امنیت زندگی و غذایی خود بودند و انسان‌های قرن حاضر به دنبال

تامین امنیت در فضای سایبری. نقطه اشتراک تمام آن‌ها را می‌توان در تلاش برای ممانعت از تهدیدات و به دنبال ایمن ساختن فضای کار دانست.

۳-۱-۳- انواع امنیت

همان گونه که گفته شد امنیت انواع و اقسام گوناگونی داشته و بسته به این که از چه منظر به آن نگاه شود می‌توان تقسیم بندی‌های مختلفی را برای آن در نظر گرفت. امروزه انسان‌ها بیش‌ترین امنیت را در طبیعت و دنیای فیزیکی و ابزار دیجیتال دنبال می‌نمایند.

۳-۲- اسناد

یکی از مهم‌ترین ابزار و روشی که در تعاملات اطلاعاتی به کاربرده شده و توسط آن اطلاعات بین افراد مختلف انتقال می‌یابد اسناد است. از زمانی که انسان‌ها آموختن را یاد گرفتند اسناد نیز هم پای انسان‌ها تولید شده و رشد نمود. بستگی به دوره‌ای که انسان‌ها در آن زندگی می‌کنند اسناد انواع و اقسام مختلف داشته و به روش‌های مختلف از آن حفظ و نگهداری می‌شود.

۳-۲-۱- سند در قانون

آیین‌نامه اجرائی قانون رسیدگی به تخلفات اداری

ماده ۱۶ _ کلیه کارمندان، مسئولان مربوط و روسای کارمند متهم به ارتکاب تخلف، مکلفند همکاری‌های لازم را با هیأت‌ها به عمل آورده و مدارک و اسناد و اطلاعات مورد نیاز را در مهلت تعیین شده از طرف هیأت‌ها در اختیار آن‌ها قرار دهند، در مورد اسناد طبقه بندی شده، رعایت مقررات و قوانین مربوط الزامی است.

قانون مجازات اسلامی جاسوسی

ماده ۵۰۱ - هر کس نقشه‌ها یا اسرار یا اسناد و تصمیمات راجع به سیاست داخلی یا خارجی کشور را عالماً و عامداً در اختیار افرادی که صلاحیت دسترسی به آن‌ها را ندارند قرار دهد یا آن‌ها را از مفاد آن مطلع کند به نحوی که متضمن نوعی جاسوسی باشد، نظر به کیفیات و مراتب جرم به یک تا ده سال حبس محکوم می‌شود.

ماده ۵۰۲ - جاسوسی در قلمرو ایران به نفع یک دولت بیگانه و به ضرر دولت بیگانه دیگر هر کس به نفع یک دولت بیگانه دیگر در قلمرو ایران مرتکب یکی از جرائم جاسوسی شود به نحوی که به امنیت ملی صدمه وارد نماید، به یک تا پنج سال حبس محکوم خواهد شد.

تخلیه‌ی اطلاعاتی

ماده ۵۰۶ - چنان‌چه مأمورین دولتی که مسئول امور حفاظتی و اطلاعاتی طبقه بندی شده می‌باشند و به آن‌ها آموزش لازم داده شده است در اثر بی مبالاتی و عدم رعایت اصول حفاظتی توسط دشمنان تخلیه‌ی اطلاعاتی شوند به یک تا شش ماه حبس محکوم می‌شوند.

تعدیات مامورین دولتی نسبت به دولت

ماده ۵۹۸ _ هر یک از کارمندان و کارکنان ادارات و سازمان‌ها یا شوراها و یا شهرداری‌ها و موسسات و شرکت‌های دولتی و یا وابسته به دولت و یا نهادهای انقلابی و بنیادها و موسساتی که زیر نظر ولی فقیه اداره می‌شوند و دیوان محاسبات و موسساتی که به کمک مستمر دولت اداره می‌شود و یا دارندگان پایه قضایی و به طور کلی اعضا و کارکنان قوای سه گانه و هم‌چنین نیروهای مسلح و مامورین به خدمات عمومی اعم از رسمی و غیر رسمی و وجوه نقدی یا مطالبات یا حوالجات یا سهام و سایر اسناد و اوراق بهادار یا سایر اموال متعلق به هریک از سازمان‌ها و موسسات فوق الذکر یا اشخاصی که برحسب وظیفه به آن‌ها سپرده شده است را مورد استفاده غیر مجاز قرار دهد بدون آن که قصد تملک آن‌ها را به نفع خود یا دیگری داشته باشد، متصرف غیر قانونی محسوب و علاوه بر جبران خسارات وارده و پرداخت اجرت المثل به شلاق تا ۷۴ ضربه محکوم می‌شود و در صورتی که منتفع شده باشد علاوه بر مجازات مذکور به جزای نقدی معادل مبلغ انتفاعی محکوم خواهد شد و هم‌چنین است در صورتی که به علت اهمال یا تفریط موجب تضییع اموال و وجوه دولتی گردد و یا آن را به مصارفی برساند که در قانون اعتباری برای آن منظور نشده یا در غیر مورد معین یا زائد بر اعتبار مصرف نموده باشد.

طرز نگهداری اسنادسری و محرمانه

ماده ۶- منظور از نگاهداری اسنادسری و محرمانه مجموعه اعمالی است که از ابتدای انشای این اسناد تا تاریخ خروج آن‌ها از حالت سری یا محرمانه بودن انجام می‌شود تا اشخاص غیر مجاز به اسناد مذکور دست نیابند یا بر مفاد آن‌ها واقف نشوند.

تبصره – کسی که لازم نیست سندسری یا محرمانه را روئیت کند یا از مفاد آن مطلع شود در هر مقام و موقعی که باشد شخص غیر مجاز محسوب است و حق مراجعه به سند سری یا محرمانه را ندارد.

ماده ۷- شیوه‌های مربوط به نگاهداری اسنادسری و محرمانه را هریک ازسازمان‌ها به مقتضای وظائف و طبع کار خود وکیفیت وکمیت اسنادی که در اختیار دارند با توجه به طبقه بندی مندرج درماده ۱ این آیین‌نامه طی دستورالعمل موضوع ماده ۴ تعیین خواهند کرد. میزان مراقبتی که دراین دستورالعمل‌ها پیش‌بینی می‌شود نباید از آن‌چه دراین آیین‌نامه مقرر است کم‌تر باشد.

ماده ۸- اسناد طبقه‌ی اول و دوم باید در صندوق‌های نسوزی که حداقل به قفل رمز سه چرخی و در موارد استثنائی شش اهرمی مجهز باشند، نگاهداری شوند.

ماده ۹- اسناد طبقه‌ی سوم باید در صندوق فلزی یا قفسه‌های کشویی فلزی (فایل کابینت) نگاهداری شوند، درمواردی که رعایت این‌ترتیب مقدور نباشد، استفاده و موقت از صندوق یا گنجه چوبی که به میله‌های فلزی و قفل مطمئن مجهز باشد جایز خواهد بود.

ماده ۱۰- محل بایگانی اسناد طبقه‌ی اول و دوم و سوم باید محفوظ و در غیر مواقعی که مراجعه به این اسناد لازم است مقفل باشد. کسی که مسئولیت نگاهداری اسناد مذکور را عهده دار است باید در پایان کار اداری با بازرسی محل از اجرای مقررات مربوط به نگاهداری اسناد مذکور و مقفل بودن محفظه آن‌ها مطمئن شود.

ماده ۱۱- اسناد طبقه‌ی چهارم باید در محلی که خارج از دسترس اشخاص غیر مجاز باشد نگاهداری شوند.

ماده ۱۲- اگر سند متعلق به یک کشور خارجی یا یک سازمان بین‌المللی باشد و برای نگاهداری آن مقررات خاصی وجود داشته باشد طبق مقررات مذکور و الا طبق مقررات این آیین‌نامه عمل خواهد شد.

ماده ۱۳- اسناد طبقه‌ی اول و دوم نباید به خارج اداره مربوط منتقل شوند مگر برای استفاده در جلسات رسمی که در خارج اداره تشکیل می‌شوند. این اسناد نباید به اقامتگاه خصوصی اشخاص برده شوند.

ماده ۱۴- اسناد طبقه سوم و چهارم را در مواردی که ضرورتی ایجاب کند می‌توان به اقامتگاه خصوصی اشخاص برد به شرط آن که موافقت کتبی رئیس سازمان یا مقام مادون از طرف او جلب شده باشد.

ماده ۱۵- مطالعه اسناد سری و محرمانه در معابر و امکنه عمومی ممنوع است.

ماده ۱۶- برای ارسال اسناد سری و محرمانه از محلی به محل دیگر باید سند را در دو پاکت قرار داد، به روی پاکت خارجی فقط عنوان سازمان یا واحدی که سند را تحویل خواهد گرفت و به روی پاکت داخلی نوع و طبقه سند و نام شخص گیرنده یا عنوان شغلی او درج می‌شود. در صورتی که سند بنام شخص معینی فرستاده شده باشد تسلیم آن به غیر او مجاز نخواهد بود. ولی تسلیم سندی که عنوان شغلی گیرنده اصلی را دارد به قائم مقام او بلامانع است. اگر سند سری باشد باید برگ رسیدی نیز در درون پاکت داخلی گذاشته شود تا گیرنده سند، برگ مذکور را امضا کند و برای فرستنده عودت دهد. پاکت داخلی مربوط به اسناد سری

باید لاک و مُهر شود، پاکت خارجی در همه حال فاقد لاک و مُهر خواهد بود. نوع و طبقه‌ی سند بر روی پاکت خارجی درج نمی‌شود.

ماده ۱۷- نقل و انتقال اسناد سری در داخل سازمان مربوط و ارسال این اسناد به خارج سازمان باید به وسیله‌ی مامورانی که واحد حفاظت معرفی می‌کند انجام شود. اسناد محرمانه را می‌توان با پست سفارشی به خارج سازمان مربوط ارسال داشت.

ماده ۱۸- نحوه ارسال اسناد سری و محرمانه‌ی دولتی به خارج کشور و حداقل و مراقبتی که ضمن این کار برای حفظ اسناد مذکور لازم است طی دستورالعملی به مراجع مربوط ابلاغ خواهد شد.

ماده ۱۹- در موردی که سند سری یا پرونده یا جدا از آن به محلی فرستاده می‌شود باید رونوشتی از آن در بایگانی اصلی باقی بماند.

ماده ۲۰- رونوشت اسناد مذکور در ماده ۱۹ پس از اعاده اصول آن‌ها نابود می‌شود. اوراق باطله و پیش‌نویس‌ها و کاغذهای کاربن و استنسیل و نظائر آن‌ها که به امور سری و محرمانه مربوط می‌شود نیز باید نابود شوند.

تبصره- نابود کردن اوراق باید به طور کامل انجام شود به‌طوری که ازآن‌ها چیزی که قابل استفاده باشد باقی نماند.

ماده ۲۱- مقررات این آیین‌نامه در مورد اسناد سری و محرمانه نسبت به اطلاعات سری و محرمانه نیز تا آن‌جا که قابل اعمال باشد جاری خواهد بود. منظور از اطلاعات معلوماتی است که در جلسات رسمی اظهار یا شفاهاً در اختیار افراد مجاز گذاشته می‌شود. نوع و طبقه اطلاعاتی که ماخوذ از سندی است نوع و طبقه سند ماخذ است.

ماده ۲۲- دستورالعمل‌هایی که بر مبنای این آیین‌نامه تهیه می‌شود بر حسب مورد داخل در یکی از طبقات سوم یا چهارم ماده۱ قرار می‌گیرند.

ماده ۲۳- نیروهای مسلح ایران از شمول مقررات این آیین‌نامه مستثنی بوده وتابع مقررات آئین نامه‌های مربوط به خود می‌باشد

۳-۲-۲- اسناد ذهنی

ذهن در معنای لغوی به معنای فهم، دریافت، یاد، هوش، قوه باطنی که مطالب را به یاد نگه می‌دارد می‌باشد.

از آن‌جایی که از معانی لغوی ذهن بر می‌آید، ذهن مجموعه‌ای از فهم و درک، دریافت اطلاعات، یادآوری و بازیابی و موضوع هوش که موارد فوق به‌ترتیب مربوط به بخش‌هایسه گانه ذیل می شود:

۱. ادراک

۲. تفکر

۳. نظام حسی و شناختی

۳-۲-۲-۱- ادراک:

اختلالات ادراکی نظیر توهم- خطای حسی ممکن است در ارتباط با خود شخص یا محیط باشد.

در خطای حسی محرک‌های خارجی حسی واقعی وجود دارند لکن فرد در ادراک دچار اشتباه می‌شود.

در مورد توهم، ادراک بدون محرک، سیستم‌های حسی درگیر مثل دستگاه شنوایی، بینایی، بویایی یا لامسه می‌باشد. گاهی اوقات توهمات در اثر شرایط استرس آمیز در بعضی بیماران پدید می‌آید مثل احساس مسخ شخصیت و مسخ واقعیت (گسستگی شدید از خود و از محیط) و یا احساس حرکت حشرات روی پوست یا زیر پوست که اختلال ادراکی است که ناشی از مصرف کوکائین است.

اظهار مطالبی از سوی بیمار که صداهایی می‌شوند که دیگران نمی‌شنوند یا دیدن چیزهایی که دیگران نمی‌بینند از موارد توهم است.

۳-۲-۲-۲- تفکر:

تفکر در اصل دو بخش است:

۱- یکی فرآیند تفکر یعنی فرم یا شکل اندیشیدن

۲- دوم محتوای فکر.

۳-۲-۲-۱- فرآیند تفکر یا فرم و شکل اندیشیدن که شامل نحوه پیوند دادن عقاید و تداعی‌ها و شکل تفکر فرد اطلاق می‌شود. فرآیند تفکر ممکن است منطقی، یا کاملاً غیر منطقی و حتی غیر قابل فهم باشد.

بیمار ممکن است فراوانی یا فقر عقاید داشته باشد. ممکن است تفکر سریع داشته باشد که در نوع شدید آن پرش افکار نامیده می‌شود. بیمار ممکن است تفکر کند یا تردیدآمیز نشان دهد. تفکر ممکن است مبهم یا تهی باشد بیمار تفکر هدفمند دارد. پاسخ‌هایش مربوط هستند

یا نامربوط؟ آیا ربط علت و معلولی آشکار در توصیف‌های بیمار وجود دارد؟ آشفتگی‌های تداوم فکر عبارتند از اظهاراتی که حاشیه پردازانه، مماسی، نامربوط، طفره آمیز یا تکراری است.

انسداد تفکر به متوقف شدن ناگهانی رشته افکار قبل از تکمیل یک نظریه اطلاق می‌شود. بیمار ممکن است نتواند آن‌چه را می‌گفت یا می‌خواست بگوید، به خاطر آورد. حاشیه پردازی حاکی از عدم توانایی برای تفکر هدفمند است. بیمار در توضیح یک عقیده، جزئیات نامربوط و جملات معترضه زیادی را وادار می‌کند، اما بالاخره به موضوع اصلی آن بر می‌گردد.

در تفکر مماسی بیمار رشته کلام را گم می‌کند و افکار حاشیه‌ای را که تحت تاثیر محرک‌های درونی و بیرونی برانگیخته می‌شود و تعقیب می‌نماید و هرگز به موضوع اول بر نمی‌گردد.

۳-۲-۲-۲-۲- محتوی تفکر:

محتوی تفکر به آن‌چه بیمار در مورد آن می‌اندیشد گفته می‌شود عقاید، باورها، دل مشغولی‌ها و وسواس‌های ذهنی.

اختلال در محتوای فکر شامل موارد زیر است:

هذیان- اشتغالات ذهنی – وسواس فکری – وسواس عملی – فوبی‌ها – طرح‌ها و نقشه‌ها – مقاصد – افکار انتحاری و دگرکُشی – نشانه‌های خود بیمار انگاری – امیال ضد اجتماعی خاص

۳-۲-۲-۳- نظام حسی و شناختی:

در خصوص وضعیت روانی ارزیابی اعمال عضوی مغز و هوش بیمار، توانایی تفکر انتزاعی و سطح بینش و قضاوت بحث می‌کند. در نظام حسی و شناختی، موضوعات زیر مطرح می‌گردد:

- آگاهی و سطح هشیاری
- جهت یابی (زمان و مکان و شخص)
- تمرکز و توجه
- سطح (ذخیره) اطلاعات عمومی و هوش

اختلالات سطح هوشیاری معمولاً حاکی از اختلال عضوی مغز است. تیرگی شعور اصطلاحی است که برای توصیف کاهش کلی آگاهی از محیط به کار می‌رود. بیمار ممکن است قادر به حفظ توجه به محرک‌های محیطی یا تداوم تفکر یا رفتار هدفمند نباشد. بیماری که دچار تغییر در سطح هوشیاری است معمولاً کم و بیش اختلال در جهت یابی نشان می‌دهد.

اصطلاحاتی که برای توصیف سطح هوشیاری بیمار بکار می‌رود عبارتند از: تیرگی – خواب آلودگی – اغماء – بهت – بی حالی – آگاهی – حالت گریز مرضی.

اختلال جهت یابی به طور معمول بر حسب زمان، مکان و شخص تعیین می‌شود. یعنی احساس زمان قبل از احساس مکان منتقل می‌شود. در خصوص زمان، این که آیا بیمار می‌داند کدام روز هفته است، تاریخ تقریبی و موقع روز را می‌داند. آیا اسم جا و مکانی که در آن است می‌داند؟ آدرس منزلش را می‌داند، از کجا می‌شود به سر خیابان رفت؟ آیا بیمار معاینه کننده را می‌شناسد؟ من کی هستم؟ خودت کی هستی؟ اسم اطرافیان را می‌داند و می‌شناسد؟ تمرکز و توجه بیمار، ممکن است به دلایل مختلف مختل شود. اختلال شناختی، اضطراب، افسردگی و محرک‌های درونی توهمات شنوایی همگی می‌توانند در اختلال تمرکز نقش داشته باشند.

تفریق زنجیره‌ای ۷ از ۱۰۰، آزمون ساده‌ای است که مستلزم بی نقص بودن تمرکز و توانایی شناختی است. آیا بیمار می‌تواند به طور پیاپی ۷ را از ۱۰۰ کم کند و آیا بیمار می‌تواند جواب ۴×۵ یا ۹×۴ را بدهد.

هجی کردن معکوس یک کلمه مثل دنیا توسط بیمار و یا اعلام ۵ کلمه که با حروف مشابهی شروع می‌شوند، از تست‌های آزمایشی است و یا طرح یک مسئله ریاضی که اگر خریدی ۱۳۵ تومانی داشته باشد و ۲۰۰ تومان بدهد چقدر باید پس بگیرد.

در یک تحقیق، به منظور ارزیابی انگیزه مجرمان در فراموش کردن جنایات خود یا تظاهر به فراموشی از خود آنان درباره بروز فراموشی و ارزیابی آن‌ها، پرسشنامه‌هایی مورد سوال قرار گرفتند. در این تحقیق از ۱۸۲ زندانی و مجرم که دوران حبس خود را در زندان‌های سوئد می‌گذراندند، بررسی صورت گرفت. نیمی از مجرمان قاتل و نیمی از مجرمان با سنین ۶۳-۲۰ سال بوده که دوره حبس آن‌ها ۱ الی ۳ سال بوده است. از مجرمان فوق به صورت پرسشنامه‌ای سوال شده بود که ارزیابی کنند، مجرمان معمولاً برای اجتناب از محکوم شدن تا چه حد به از دست دادن حافظه خود تظاهر می‌کنند. فقط ۲٪ از مجرمان قاتل معتقد بودند مرتکبان این نوع جنایات هرگز تظاهر به از دست دادن حافظه نمی‌کنند. در سئوال دیگر پرسیده شد که آیا پیش آمده است که خواسته باشند جنایتی را که مرتکب شده‌اند، فراموش کنند که ۵۳ درصد از مجرمان قاتل و ۳۵ درصد مجرمان تجاوز به عنف به این سوال جواب مثبت داده‌اند. (ص ۳۴ - حافظه مجرمان).

در تحقیق دیگری اثر فراموش ساختگی بر تضعیف حافظه تایید شد. درمطالعه شبیه سازی شده در ۱۹۹۹ جزوه قتلی را بین سوژه‌ها پخش کردند و خواستند که با مجرم احساس همدردی کند. سپس به گروهی از سوژه‌ها گفتند، نقش مجرم مبتلا به فراموشی را طی تکلیفی

شامل مجموعه سئوالاتی درباره ماجرا، اجرا کنند. گروه شاهد را ترغیب کردند که تا آن‌جا که می‌توانند این کار را انجام دهند. پس از یک هفته سوژه‌ها به آزمایشگاه برده شدند و دوباره به سئوالاتی درباره ماجرای قبل پاسخ دادند. از همه خواسته شد که این تکلیف را انجام دهند. طی جلسه اول، سوژه‌های که نقش مجرم فراموش‌کار را بازی می‌کردند جواب صحیح کم‌تری در مقایسه با گروه شاهد دادند که اهمیت چندانی نداشت و فقط نشان می‌داد که سوژه‌های مبتلا به فراموشی، نقش خود را جدی گرفته‌اند. اما در تستی که پس از یک هفته انجام گرفت، عمل‌کرد شبیه سازی‌های قبلی هم چنان در سطح پایین‌تری از گروه شاهد بود. همانند نتایج به دست آمده از مطالعات مشابه، نتایج این تحقیق نشان می‌دهد فراموشی ساختگی دارای اثر تضعیف حافظه است.

الگوهای پیش‌رفته با استفاده از FMRI قادرند با اطمینانی بسیار زیاد معلوم کنند که آیا شخص آشکارا دروغ می‌گوید یا خیر و یا این که آن‌چه می‌گوید را باور دارد یا باور ندارد. در نتیجه، عمل‌کرد مغز شیوه‌ای منتخب است که بر دستگاه‌های دروغ سنج که فعالیت الکترودرمال و جزیی را اندازه گیری می‌کنند، برتری دارد و حتی ناهنجاری‌های ریخت شناسی که با MRI معمولی قابل تشخیص‌اند، ممکن است نشانه رفتار منحرفانه باشند که یانگ در ارتباط با دروغگوها نشان داد.

وقتی متهمی ادعا می‌کند جرم خویش را فراموش کرده، این فراموشی ممکن است بر حسب انتظارات موجود، واقعی (یعنی گسسته یا ارگانیک) و یا ساختگی باشد. تظاهر به فراموشی شگردی رایج برای به حداقل رساندن مسئولیت جرم است و مجرمین با بهره هوشی کم‌تر و عمل‌کرد اجرایی ضعیف‌تر، بیش‌تر تظاهر به فراموشی می‌کنند.

تست‌هایی شامل SVT و GKT از تست‌های سنجش حافظه می‌باشد. تست SVT یا تست نشانگان محص، شامل روند اجباری است که طی آن، آگاهی متهم از جرم را به واسطه سئوالاتی مرتبط با جرم و صحنه جرم می‌سنجد. در تست SVT با طرح سوالاتی از مجرم در خصوص صحنه جرم و جزئیات آن مجرم برای هر سئوال، یکی از دو جواب که به شکل یکسانی قابل قبول هستند لکن یکی غلط و دیگری صحیح است، دست به انتخاب بزند، فراموشی واقعی جرم باید به عمل‌کردی اتفاقی در تست SVT به میزان حدود ۵۰٪ درست و ۵۰٪ غلط منجر شود و انتخاب جواب‌های غلط توسط مجرم، عمل‌کرد خیلی بیش‌تر از ۵۰٪ را خواهد داد که نشانه ادعای کذب نابودی حافظه وی است.

در تست GKT یا تست اطلاعات مقصر، به جای تشخیص دروغ، تشخیص اطلاعاتی دقیق که مجرم دانستن آن‌ها را انکار می‌کند می‌باشد. در این تست مجموعه‌ای سئوال که هر سئوال،

۵ جواب دارد، مطرح می‌شود. هنگام پاسخ‌گویی متهم به سئوالات، واکنش‌های الکترودرمال کف دست‌های مجرم را (یعنی فعالیت غدد عرق زا) ثبت می‌گردد و از آن‌جا که فعالیت الکترودرمال به محرک‌های آشنا و تحریک کننده هیجان حساس است، مجرمان گناهکاری که تظاهر به فراموشی می‌کند به جواب صحیح واکنش الکترودرمال افزایش یافته، نشان می‌دهند. میزان خطا در تست GKT ۰/۰۰۸ است و نتایج مطالعات نشان می‌دهد تست GKT قادر است به میزان ۸۰٪ سوژه‌های مقصر را شناسایی نماید.

۳-۲-۳- امنیت اطلاعات اسناد ذهنی

امروزه بسیاری از اطلاعات انسان ها در ذهن قرار گرفته و ذخیره سازی می شود. این اطلاعات در ابزار ذخیره ساز دیگری قرار نداشته و برای دسترسی آن می بایست به ذهن انسان دسترسی پیدا شود تا بتوان از آن مطلع گردید. ذهن یکی از ذخیره ساز هایی است که تا زمان وجود اراده برای حفظ آن نمی‌توان به محتویات آن دسترسی پیدا نمود لذا سلطه‌گران در تلاش خواهند بود ابتدا انسان را مسلوب الاراده نموده و سپس به اطلاعات درون آن دسترسی پیدا کنند و برای این کار از روش های مختلفی استفاده می شود که ذیلا به برخی از آنها اشاره می‌گردد.

۳-۲-۳-۱- داروهای کنترل رفتار

- تاکنون تعدادی از انتقال دهنده‌های عصبی به‌طور کامل شناخته شده‌اند. ماده‌ای به نام استیل کولین (ach) از آن جمله‌اند که مسئول انقباض عضلانی در برابر تحریکات بیرونی است برخی از سموم و داروها (مانند بوتولینوس یا کورار) که مانع آزاد شدن این ماده از انتهای یاخته می‌شوند موجب فلج عضلات از جمله عضلات تنفسی می‌شوند.
- اثر برخی داروهای روان گردان بر ترشح مواد انتقال دهنده
- آرام بخش‌ها (باربیتورات‌ها، بنزودیازپین‌ها، الکل، و. .)
- محرک‌ها (آمفتامین‌ها،کوکایین، دز پیرامین، ایمیپرامین)
- مواد ضد روان پریشی (کلرپرومازین، رزرپین،)
- مواد افیونی (هرویین، مرفین و. . . .)
- ایجاد کننده‌های روان‌پریشی (اتروپین، موسکارین، مسکالین، حشیش، ال اس دی، پسیلوسیبین

- برخی دیگر از داروها نظیر داروهای موثر بر خلق و خو (کلرپرومازین) از طریق تغییر در فضای سیناپسی موجب می‌شوند که پیام‌های کم‌تری انتقال یابند.
- کند کننده‌های عصبی : الکل، هروییین

این مواد کند کننده جریان انتقال پیام‌های عصبی بین نورون می‌باشند اثرات رایج : اختلال در تکلم و بینایی، توهم و در موارد حاد جنون می‌باشد.

محرک‌ها و تشدید کننده‌ها : برعکس مواد بالا عمل می‌کنند. آمفتامین‌ها،کوکایین که با برچسب‌های تجاری متدرین، دکسدرین و بنزدرین به فروش می‌رسند و در افواه به سرعت، بالابر شهرت دارند از این جمله‌اند. (غلبه بر خستگی، بیدار ماندن، احساس سرور و سرخوشی از برخی آثار آنی آن است)

مواد و داروهای توهم زا : (ال اس دی، مسکالین، پسیلوسین، دی ام تی، ماری جوانا، تی اچ سی) دارای تظاهراتی چون تغییرات ادراکی چشم‌گیر،توهمات رنگ و صدا، حالات رمز آمیز، و بعضا وحشت‌زدگی و. . . هستند.

۳-۲-۳-۲- هیپنوتیزم

۳-۲-۳-۲- ۱- برخی کاربردهای هیپنوتیزم

- افزایش یا کاهش کنترل حرکتی
- تحریف حافظه
- واپس روی ذهنی
- ایجاد توهمات مثبت یا منفی
- کاهش درد در درمان سوختگی‌های شدید، دندان پزشکی و جراحی
- تلقین پذیری شدید
- بازیابی اطلاعات ضمیر ناخود آگاه (بخشی از اطلاعات که رمز گذاری و دسته بندی نشده‌اند و عموما در بازگویی آن افراد حساسیتی ندارند.) و ایضا خود آگاه

۳-۳-جهانی شدن و امنیت

۳-۳-۱- دهکده جهانی

مارشال مک لوهان برای اولین بار در دهه ۶۰ صحبت از دهکده جهانی به میان آورد که در آن زمان تنها یک رویای آرمان شهری به نظر می‌رسید اما امروزه جهانی شدن یکی از

پیچیده‌ترین پدیده‌های قرن بیستم است. جهانی شدن[۱] فرآیندی است که از گسترش فعالیت‌های اقتصادی، فرهنگی و اطلاعاتی در سطح جهان ناشی شده است. اوج گیری این پدیده از دهه گذشته و در پی فروپاشی نظام بین‌المللی دو قطبی شروع شده و می‌رود که همه ابعاد زندگی انسان‌ها را درنوردد.

نخستین بار در جهان شبکه CNN موفق شد عنوان آغازگر جهانی شدن را از آن خود کند. هر چند پدیده جهانی شدن تنها بُعد رسانه‌ای را در بر نمی‌گیرد و شامل کلیه ابعاد زندگی بشر می‌شود اما در طول تاریخ کم‌تر پدیده‌ای مانند جهانی شدن تا این حد با دیدگاه‌های متفاوت و بعضاً متعارض روبرو بوده است. جهانی شدن پدیده نوظهوری نیست بلکه فرآیندی است که همگام با افزایش آگاهی انسان نسبت به خود و محیط طبیعی و اجتماعی، از آغاز تاریخ وجود داشته است. از جنگ جهانی دوم به بعد با رشد تجارت جهانی،افزایش تحرک سرمایه در سطح بین‌المللی، مهاجرت نیروی کار و کاهش موانع تجاری بر اساس قراردادهای بین‌المللی، شکل دیگر و سرعت بیش‌تر پیدا کرد. در سال‌های اخیر هم با سرعت فزآینده دانش و فن‌آوری و فروپاشی ابرقدرت شرق و پایان دوران جنگ سرد، شتاب بی سابقه‌ای گرفته است.

واژه GLOBALIZATION را گاهی به جهانی شدن و زمانی به جهانی گرایی ترجمه می‌کنند. این دو ترجمه به لحاظ بار معنایی و واقعیت کاربردی و ابزاری با هم تفاوت دارند. در جهانی شدن، القای نوعی اداره و اختیار مورد نظر است و می‌خواهد این پیام را به خواننده منتقل کند که جهانی شدن، واقعیتی است ملموس و ضرورتی است گریز ناپذیر که هر جامعه اگر خواهان رفاه شهروندانش باشد، چاره‌ای ندارد جزء این که خود را با این جریان نیرومند، ضروری و مفید به حال جامعه بشری، سازگار کند و با طیب خاطر و اراده آزاد به مقتضیات آن گردن نهد.

دگرگونی انقلاب کشاورزی به انقلاب صنعتی و بعد از آن به انقلاب اطلاعاتی، گسترده‌تر و نیرومندتر از آن بود که به تلاش‌های یک گروه و یا یک طبقه خاص نسبت داده شود. به زعم طرفداران این دیدگاه، غرب از آن جا که ارزش‌هایش در جهان مقبولیت عام پیدا کرده و از پشتوانه ابزارهای نیرومند مادی و تکنولوژیک هم برخوردار است به‌تر از دیگر جوامع قادر به بهره‌برداری از فرصت‌هایی است که از بطن جهانی شدن زاده می‌شود.

در جهانی گرایی سعی بر این است که به واقعیت دیگری اشاره شود و آن این که جهانی گرایی طرحی است که توسط کشورهای ثروتمند و قدرتمند دنیا و در راس آن‌ها آمریکا، تدوین

---

[۱] GLOBALIZATION

شده و منظور از آن ادامه سلطه اقتصادی، سیاسی و نظامی بر دیگر کشورهای عالم است. آمریکا از مدت‌ها قبل از فروپاشی شوروی، سودای رهبری دنیا و دست‌یابی بیش‌تر به منابع کشورهای دیگر به ویژه کشورهای جهان سوم را در سر داشته است.

جهانی گرایی طرحی است که مخلوق ذهن و اراده عده‌ای خاص است و توسط آن‌ها طراحی شده و کنترل می‌شود. قدرت کنترل این پدیده جهان معاصر، در اختیار نظام سرمایه داری جهانی است.

شون هیلی که از مخالفان جهانی شدن است، آن‌را فرآیندی برنامه ریزی شده و پروژه‌ای تحمیلی می‌داند و بر این باورست که در عرصه فعالیت‌های بشری، تنها حوزه‌های مخصوصی جهانی شده است. از جمله این که در خلال دهه ۹۰ و از آن پس تاکنون نه تنها ثروت جهانی نشده بلکه در دست اقلیتی متمرکز گردیده است. فن‌آوری هم با وجود این که بسیار تواناتر ومتنوع‌تر از گذشته است جنبه جهانی پیدا نکرده و رشد اقتصادی نیز که پایه برتری تاریخی سرمایه‌داری است جهانی نشده است. آن‌چه جهانی شده به عقیده هیلی سرمایه پولی است که به کمک وسایل ارتباطی الکترونیک می‌تواند در کوتاه‌ترین زمان ممکن از هر نقطه گیتی جابه‌جا شود.

۳-۳-۲- نظم نوین جهانی

جهان امروز، جهانی با تحولات شگرف در ابعاد مختلف است. به نحوی که سیاست خارجی و دیپلماسی کشورها نیز متأثر از این دگرگونی‌هاست. میخائیل گورباچف با اعلام این مطلب که «عصر ابرقدرت‌ها به پایان رسیده است» نخستین کسی بود که از جای‌گزینی همکاری به جای رویارویی میان شرق و غرب سخن گفت.

روح نظم نوین جهانی در چارچوب منافع واشنگتن و غرب پایه‌ریزی شده است و با منافع کشورهای جهان سوم منافات دارد. نظم نوین مورد نظر آمریکا چیزی جزء اصطلاح فریب دهنده‌ی افکار عموم و چپاول منافع و ثروت‌کشورها را به دنبال ندارد. سرویس‌ها و سازمان‌های جاسوسی و اطلاعاتی جهان استکبار، فعالیت‌ها و عملیات خود را در سراسر جهان گسترش داده و با توجه به افول ایدئولوژی کمونیسم، چرخش اهداف خود را به سوی اسلام دنبال خواهند کرد و سعی دارند که افکار عمومی کشورهای اسلامی را از اصول و قوانین شریعت الهی منحرف نمایند. ابزارهای اطلاعاتی هم در دوران جدید شکل تازه‌ای گرفته، استفاده از سیستم‌های فنی و الکترونیکی بیش از گذشته اهمیت پیدا کرده است. با شروع جنگ خلیج فارس و حضور برتر

آمریکا، جرج بوش اعلام کرد: جنگ خلیج فارس نخسین آزمون برای پدیدار شدن یک نظم نوین بود، جهانی که در آن یک نظام حاکم است.

۳-۳-۳- شرکت‌های فرا ملیتی

از پیش‌تازان جهانی کردن اقتصاد، شرکت‌های فرا ملیتی هستند. یکی از دلایل رغبت این شرکت‌ها به سرمایه گذاری در کشورهای جهان سوم، بالا بردن قدرت خرید شهروندان در کشور میزبان و ایجاد بازارهای مصرف است. آن‌چه برای شرکت‌های فرا ملیتی مهم است یکسان شدن مقررات کمرگی در کشورهای جهان سوم است تا این شرکت‌ها، مختصر موانع قانونی ناشی از حق حاکمیت ملی کشورهای جهان سوم را هم در پیش روی نداشته باشند و با سرعت و سهولت به هرگونه فعالیت آشکار یا پنهان سیاسی و اقتصادی مبادرت ورزند و سیطره خود را بر منافع کشورهای جهان بیش‌تر کنند.

۳-۳-۴-جهانی شدن و دنیای دیجیتال

امروزه مفهوم جهانی شدن دگرگونی بسیار چشم‌گیری در فن‌ها و دانش‌های ارتباطی و اطلاعاتی پدید آورده است و زبان دیجیتالی را همگانی کرده است به گونه‌ای که بنیادهای مادی جامعه انسانی را تغییر داده و باعث آن شده که گوشه‌گیری و کناره‌جوئی از میان برود و هیچ کشوری نتواند مرزهای خود را به روی شبکه جهانی ببندد و از جریان‌های اطلاعاتی به دور بماند. اینترنت به نحوی شگفت‌آور ماهیت روابط اجتماعی درون ملت‌ها و میان ملت‌ها را تعریفی دوباره می‌کند. محیط‌های مجازی و جامعه‌های اطلاعاتی در سرتاسر جهان رو به گسترش‌اند و این امر از تاکید اهمیت زمان و مکان کاسته است.

با تبدیل اینترنت به وسیله‌ای روزمره و قابل دسترس از هر نقطه جهان، واحدهای جغرافیایی که از لحاظ زمانی و مکانی از هم جدا شده‌اند، هر چه بیش‌تر به تمامی انواع روابط اطلاعاتی متصل خواهند شد. قابلیت این فن‌آوری برای پیوند دادن نظام‌های متنوع و گوناگون فرهنگی، اقتصادی و سیاسی با روابط جدید اطلاعاتی می‌تواند یک دهکده جهانی واقعی را بیافریند و تعریف مرسوم از سرزمین جغرافیایی و حاکمیت ملی نمی‌تواند مانعی بر سر راه این روند ایجاد کند.

انقلاب ارتباطات نوع جدیدی از ارتباطات مجازی را که خالی از روح حاکم بر روابط واقعی اجتماعی است به‌وجود آورده است. از طریق ماهواه، اینترنت و. . . جهان جدیدی به موازات جهان واقعی به وجود آمده است که دو ویژگی دارد:

۱- مخاطبان وسیع و متکثر دارد.

۲- فاصله زمانی و مکانی در آن از بین رفته است.

۳-۳-۴-۱-تحول مفهوم امنیت یا چهره جدید امنیت در عصر جهانی شدن

۱- امنیت در سطح فردی: چهره سنتی امنیت که در جنگ سرد مرسوم بود بعد از فروپاشی شوروی کاملا دگرگون شد. در سطح فردی در عصر جهانی شدن بیش‌تر با بحران هویت و معنا و بحران‌های روحی و احساسات تنهایی و تعارض شخصیتی گره می‌خورد.

۲- در سطح ملی (فشار از درون و بیرون): ظهور بازیگران غیر دولتی که ماهیتی غیر نظامی و غیر امنیتی دارند و انتقال بازی از عرصه نظامی به عرصه‌های اقتصادی تکنولوژیک و دانش فنی، ماهیت قدرت و تهدیدات را عوض کرده است. تهدیدات جدید امنیتی برای دولت‌ها بیش‌تر پیامد مهاجرت، مسایل ناشی از وابستگی متقابل و مسایلی از قبیل محیط زیست، حقوق اقلیت‌ها و قاچاق مواد مخدر و انسان و اسلحه است.

۳- نظم و امنیت بین‌المللی: با فروپاشی شوروی ادعای نظم نوین جهانی سر داده شد. پایان تاریخ، مرگ ایدئولوژی، نظریاتی بودند که در تعریف نظم جدید بین‌المللی و مفهوم امنیت در شرایط نوین مطرح شدند منتهی در آن شرایط شناسایی و تعریف نظم جدید و ماهیت آن خود به موضوع بحث برانگیزی تبدیل شد.

فردی مثل ویلیام زارتمند در کتاب خود هفت نوع نظم بالقوه را به عنوان جای‌گزین جنگ سرد پیش بینی می‌کند. ۱- مدل تک قطبی ۲- سیستم چند قطبی ۳- محوریت سازمان ملل ۴- حاکمیت قانونی دولت‌ها ۵- شکاف شمال و جنوب ۶- نظم مبتنی بر دموکراسی ۷- جهانی از مناطق عمده جهان بر حسب قدرت. واقعیت این است که هیچ کدام از این مدل‌ها کامل نیستند بلکه به نظر می‌رسد ساختار جدید نظم جهانی در تکثر، نسبی گرایی و تاحدودی تعارضات و تناقضات ارزشی و منطقه‌ای متجلی خواهد شد.

۳-۳-۴-۲-شکاف دیجیتال

در دهه ۱۹۹۰ و قبل از ورود رسانه‌های دیجیتالی متفکران به وجود "شکاف آنالوگی" اشاره می‌کردند و از این اصطلاح وجود تمایز و تفاوت بر حسب تولید محتوا و دسترسی به فن‌آوری‌های رسانه‌های سنتی نظیر رادیو، تلویزیون و تلفن را مراد می‌کردند.

در دنیایی که هر روز بیش از پیش، ارتباط افراد در فضای مجازی شکل می‌گیرد، بی‌شک امکان دسترسی به تکنولوژی برای ادامه چنین حیاتی، اجتناب ناپذیر خواهد بود.

به راستی در چنین شرایطی، وضعیت ۶۲ درصد از افراد این کره خاکی که در طول عمر خود حتی یک بار از تلفن استفاده نکرده‌اند و یا ۴۰ درصد از ساکنینی که از نعمت برق محروم‌اند، چه خواهد شد؟

چگونه این افراد به فضای مجازی شکل گرفته در عصر حاضر که تنها در اختیار تعداد محدودی از ابرقدرت‌های رسانه‌ای است، دست خواهند یافت؟ از این واقعیت تحت عنوان "شکاف دیجیتالی"[۱] یاد می‌شود.

این اصطلاح طی ده سال گذشته کاربرد وسیعی برای بیان تغییرات گسترده در دسترسی به فن‌آوری‌های اطلاعات و ارتباطات در سراسر جهان یافته است.

[۱] Digital Divide

۳-۳-۴-۲-۱- پیامدهای شکاف دیجیتال

چنان‌چه شبکه‌های اینترنت در آینده به کانون جهانی داد ستد مبدل گردد، در آن صورت چه سرنوشتی در انتظار میلیون‌ها نفری که اتصال به اینترنت برای آن‌ها امکان پذیر نیست، خواهد بود. شاید هرگز نتوان برای این سئوال، پاسخی به‌دست آورد.

سرعت پیشرفت فن‌آوری نشان می‌دهد که جهان به دو بخش مجزا تقسیم خواهد شد. بسیاری از کشورها به عقب ماندگی روز افزون گرفتار می‌شوند و کشورهای صاحب تکنولوژی هم روز به روز پیشرفت خواهند کرد و به همین‌ترتیب بهره کشی از کشورهای توسعه نیافته افزایش خواهد یافت.

بروز شکاف دیجیتالی تاثیرات زیادی در تجارت الکترونیک، اقتصاد و آموزش خواهد داشت. حاصل این امر عقب افتادگی در علوم و فن‌آوری کشورهای در حال توسعه خواهد بود. عمیق‌تر شدن این شکاف به معنای فاصله گرفتن اقتصادی، سیاسی، اجتماعی و فرهنگی کشورها که نتیجه آن تحمیل کالاها و تولیدات فرهنگی صاحبان تکنولوژی برای سست کردن باورها، سنت‌ها و فرهنگ‌های کشورهای در حال توسعه که پیامدش نوعی استثمار فرهنگی، بحران بی‌هویتی نسل جوان، یاس و افسردگی در سطح جوامع خواهد شد.

جوامعی که متحمل بروز ناهنجاری‌های اجتماعی روز افزون از قبیل بزه‌کاری، دزدی، میل به اعتیاد، افزایش طلاق و سست شدن بنیان‌های خانوادگی و. . . خواهد شد. این مسئله مهم‌تر از ناهمگونی جوامع مختلف بشری در دست‌یابی به تکنولوژی است، لذا لازم است که نسبت به تکنولوژی فن‌آوری اطلاعات به عنوان امری لازم و ضروری نگاه کرد.

۳-۳-۴-۲-۲-راهکارهای برطرف کردن شکاف دیجیتال

شکاف دیجیتالی یک مسئله پیچیده است که به صورت‌های مختلفی در کشورها بروز می‌کند و باعث چالش‌های عملیاتی و سیاسی در آن کشور می‌شود. علاوه بر این روشن است راه حل‌هایی که در کشورهای پیش‌رفته کاربرد دارند نمی‌توانند در کشورهای در حال توسعه کاربرد داشته باشند. راه حل‌ها باید بر اساس درک و فهم شرایط و نیازهای آن کشور ارائه شوند. مهم‌ترین مسائل در پرکردن شکاف دیجیتالی توجه به سواد و بالا بردن سطح علمی افراد، توزیع صحیح دسترسی به اینترنت، ایجاد شرایطی برای دسترسی همه مردم به تکنولوژی و فن‌آوری، توضیح و تشریح ضرورت استفاده از تکنولوژی اینترنت در عرصه تجارت، برنامه ریزی مناسب و مدون برای تجهیز مدارس به شبکه‌های اینترنتی و. . . است.

زیرا در حال حاضر نیمی از افراد جامعه کشورهای آفریقایی، عربی و خاور میانه، سواد خواندن و نوشتن ندارند و از امکان تحصیل محروم هستند. نمی‌توان پیش‌بینی کرد که تا چه اندازه در عصر ارتباطات و اطلاعات این جوامع متضرر خواهند شد. ولی می‌توان تصور کرد در حالی که جامعه اطلاعاتی در حال تغییر دادن شیوه‌های اقتصاد جهانی است، کشورهای در حال توسعه چه سرنوشتی پیدا خواهند کرد.

اعداد و ارقام به‌دست آمده آشکارا نشان‌دهنده این واقعیت است که میزان دسترسی به اینترنت و همچنین تعداد خبرگان علوم رایانه‌ای درکشورهای جهان متفاوت یا به عبارتی نابرابر است.

فعالان و اندیشمندان دانشگاهی که در زمینه از میان بردن شکاف دیجیتالی فعال هستند، ادعاهای مشابهی دارند که با زبانی غیر رسمی آن را بیان می‌کنند.

۳-۳-۴-۲-۳- موافقان و مخالفان

مایک برادی[۱] در کتاب خود با نام " عصر تجارت الکترونیکی" که در اوت سال ۲۰۰۰ انتشار یافت می‌نویسد :

"شکاف دیجیتالی بحران به‌شمار نمی‌رود. چرا که بحران‌های واقعی جهان، گرسنگی، جنگ‌ها، ایدز و تخریب محیط زیست هستند. هرگاه اینترنت بتواند از عهده حل مشکلات فوق برآید، آنگاه ضروری خواهد بود که هر فرد یک رایانه در اختیار داشته باشد. همچنین باید در نظر داشت تکنولوژی با سرعت مناسبی در حال پیشرفت است. تعداد افرادی که درگیر بحث شکاف دیجیتالی هستند کم است، این امر گویای آن است که گرسنگی، جنگ و ایدز موضوعاتی به مراتب مهم‌تر از دسترسی عموم مردم به اینترنت هستند. "

کارلسون بنیان‌گذار شرکت ورلدلینکس- براین باور است که کمک به کودکی که به واسطه ابتلا به بیماری ایدز درحال احتضار است به‌وضوح از توانمند ساختن کودکان در استفاده از رایانه مهم‌تر است. هم‌چنین معتقد است که تدارک برای دسترسی به آموزش و پرورش و ارتباطات به منظور دست یافتن به منابع اطلاعاتی می‌تواند در برطرف ساختن موانع ناشی از جنگ، گرسنگی و مبارزه با بیماری ایدز کارگشا باشد.

این شیوه می‌تواند به‌عنوان بخشی از راه حل مبارزه با مشکلات توسعه‌ای به‌شمار آید، نه همه آن. برخی در خصوص شکاف دیجیتالی استدلال می‌کنند که این شکاف باعث شده است که اغلب کشورهای جهان در دام عقب ماندگی دائمی گرفتار شوند.

---

[۱] Mike Brady

برخی دیگر فن‌آوری دیجیتالی را به عنوان عامل بالقوه‌ای برای نجات مردم عقب مانده جهان می‌دانند. این دسته خوشبینانه استدلال می‌کنند شیوه اقتصادی جهان به گونه‌ای دگرگون شده که به ایجاد فرصت‌های جدید برای تولید ثروت منجر شده است و برای بهره‌برداری از یک چنین فرصت‌هایی، چاره‌ای جزء استفاده از فن‌آوری دیجیتالی (شبکه جهانی اینترنت) وجود ندارد.

تعدادی از منتقدان ادعا می‌کنند اجرای چنین پروژه‌هایی پیامدهای ناگواری به‌دنبال خواهد داشت. آن‌ها معتقدند استفاده از رایانه نمی‌تواند فاصله زیاد میان کشورهای فقیر و غنی را برطرف سازد مگر آن که دسترسی کشورهای در حال توسعه به اینترنت و افزایش توان مالی آنان به میزان زیادی باعث بهبود زیرساخت‌های ارتباطی شود.

۳-۴- ردیابی اطلاعاتی و بر چسب امنیتی

۳-۴-۱-انواع ردیابی :

" ردیابی لحظه به لحظه[۱] " و " ردیابی خاموش و غیر فعال[۲] "

۳-۴-۱-۱- " ردیابی لحظه به لحظه "

مدل طراحی شده برای این سرویس، یک سیستم پیش‌رفته است که برای نمایش هم‌زمان موقعیت وسیله نقلیه و ارسال اطلاعات حرکت (سرعت خودرو، مختصات جغرافیائی، ارتفاع، زمان. . .) به دفتر مرکزی استفاده می‌شود. با نصب این تجهیزات روی خودروها و رایانه دفتر مرکزی مدیران قادر خواهند بود در هر لحظه از موقعیت خودروها آگاه شوند و به کمک نرم‌افزار مربوطه حرکت خودرو را با دقت‌های مختلف برروی نقشه‌های جهانی، کشوری، استانی و یا حتی محلی مشاهده نمایند.

علاوه بر نمایش حرکت خودرو، اطلاعات لحظه‌ای حرکت خودرو نیز قابل دسترسی می‌باشد. یکی از مهم‌ترین توانمندی‌های سیستم هم‌زمان، امکان برقراری ارتباط دوطرفه بین مرکز و خودرو می‌باشد. به کمک این سیستم می‌توان برای کلیه خودروهای تحت پوشش پیام متنی[۳] ارسال نمود یا برعکس هریک از خودروها می‌توانند پیام‌های از پیش تعین شده را برای مرکز ارسال نمایند.

---

[۱] Online

[۲] Passive

[۳] Text

تجهیزات این سرویس در حالت کلی شامل سه بخش است که در یک سامانه به‌صورت کلی تعبیه شده است:

- بخش گیرنده اطلاعاتGPS
- بخش فرستنده وگیرنده اطلاعات رابط میان خودرو و مرکز
- صفحه نمایش برای نشان دادن اطلاعات دریافتی

سیستم LIV-TRK در وسیله نقلیه نصب شده و اطلاعات کامل موقعیت را از طریق ارتباط رادیویی و شبکه مخابراتی به مرکز کنترل ارسال می‌کند. این سیستم به‌صورت بر خط[۱] کار می‌کند.

این سیستم در مدل‌های مختلف از تکنیک‌های متعدد ارتباط رادیویی استفاده کرده و قابل عرضه است. این ارتباط مخابراتی از طریق شبکه GSM موبایل و مناسب برای پوشش ملی و کنترل و ردیابی وسایل نقلیه در نقاط داخل کشور ارتباط ماهواره‌ای و مناسب برای کنترل و ردیابی وسایل نقلیه ترانزیت ارتباط از روش‌های دیگر رادیویی مانند HF و Wireless-LAN طراحی شده است. . این سیستم مخابراتی می‌تواند شبکه رادیوئی(بی سیم) موجود در ادارات باشد.

۳-۴-۱-۲- سرویس " ردیابی خاموش و غیر فعال[۲] ":

با نصب مدل طراحی شده برای این سرویس روی خودروها،کلیه اطلاعات مربوط به مسیرهای طی شده توسط خودرو روی حافظه ذخیره شده و با مراجعت خودرو به دفتر مرکزی می‌توان مسیرهای طی شده، نقاط توقف، سرعت حرکت، مسافت طی شده، خروج از مسیر برنامه ریزی شده، و سایر اطلاعات حرکتی خودرو را بازسازی نمود و روی نقشه نمایش داد. محصولات این سرویس در حالت کلی شامل دو بخش می‌باشد:

- بخش گیرنده اطلاعات GPS
- بخش ذخیره سازی اطلاعات

۳-۴-۱-۲-۱- امکانات و قابلیت‌های ردیاب:

۱. امکان بازسازی مسیر طی شده بر روی نقشه‌های مختلف
۲. امکان رد زنی[۳] روی نقشه

---

[۱] Online
[۲] Passive
[۳] zoom

۳. امکان فراخوانی هر یک از خودروهای تحت پوشش به وسیله وارد کردن شماره شناسایی[۱] مربوطه

۴. امکان تعریف متحرک بر اساس مشخصات فردی راننده و یا مشخصات خودرو

۵. دسترسی به اطلاعات حرکت خودرو به صورت فایل متنی[۲]

۶. امکان ارسال پیام برای متحرک در حالت لحظه به لحظه [۳]

۷. امکان تعریف پیام اضطراری برای متحرک

۸. امکان جست‌جو و فراخوانی بر اساس تاریخ، ساعت، ارتفاع، سرعت، و سایر مشخصات متحرک

۳-۴-۱-۲-۲ - فن‌آوری‌های شناسایی و ردیابی

پایگاه داده‌ای را تصور کنید که کاملاً قابل حمل و بدون نیاز به اتصال آنی به رایانه باشد و یک واسطه‌ی ارتباطی کاغذی که برچسب یا کارتی با اطلاعات قابل خواندن برای ماشین ایجاد کند را به همراه داشته باشد که شامل متن، عکس، اطلاعات پزشکی و دیگر انواع داده‌ها و نیز قابلیت تبدیل مجدد به صورت اول به سرعت، به سادگی و با هزینه کم را داشته باشد. تمامی این قابلیت‌ها یک‌جا در بارکد PDF۴۱۷ جمع شده است.

این بارکد را می‌توان نماینده‌ای از بارکدهای دوبُعدی دانست. یک بارکد از این نوع می‌تواند به تنهایی بیش از یک کیلو بایت داده را در فضایی به‌اندازه‌ی یک بارکد معمولی در خود جای دهد و برخلاف بارکدهای قدیمی تک‌بُعدی که نیاز به یک ارتباط بلادرنگ با یک پایگاه داده‌ای بزرگ‌تر داشتند، PDF۴۱۷ خود یک پایگاه داده است و در یک جمله PDF۴۱۷ با انسان برروی کاغذها، بسته‌ها و قطعات سفر می‌کند.

این بارکد را می‌توان سودآور، سهل‌الاستفاده و آسان برای ایجاد کردن معنی کرد. با یک‌بار کاربری PDF۴۱۷، مزایای ارتباطات داده‌ی دیجیتالی با استفاده از بارکد معلوم می‌شود که عبارت است از کم خرج بودن، قابلیت چاپ برروی انواع رسانه‌ها با استفاده از ابزار رایج چاپ، سادگی در پشتیبانی و قابلیت تصحیح بسیار زیاد خطاها و علاوه بر این PDF۴۱۷ به وسیله‌ی برجسته‌ترین سازمان‌های جهانی به رسمیت شناخته شده است.

---

[۱] ID

[۲] Text

[۳] on line

قابل ذکر است که هر سازمان دولتی و بازرگانی و یا خدماتی باید از سرمایه گذاری کم خطر و طولانی مدت خود مطمئن باشد که دراین‌باره می‌توان کارآیی دستگاه‌های بارکدخوان PDF۴۱۷ را در خواندن دیگر انواع مرسوم تک بعدی بارکد در نظر گرفت.

PDF۴۱۷ : فراتر از آن‌چه که به نظر می‌رسد این بارکد پاسخی به نیاز ذخیره، بازیابی[۱] و انتقال حجم عظیم داده‌ها با کم‌ترین خرج می‌باشد. PDF۴۱۷ می‌تواند انواع پرونده‌های داده (متن، عدد و دودویی) را در خود جای داده و نیز توانایی به‌رمزکردن تصاویر، اثر انگشت، لیست اجناس‌ترابری، انتقال داده‌ها به‌صورت الکترونیکی، راهنمای درجه بندی تجهیزات و دیگر انواع داده‌ها را دارد.

PDF۴۱۷ امکان ایجاد ارتباطات قوی بدون نیاز به پایگاه داده خارجی را ایجاد کرده است و به واقع می‌توان بدون خرج بیش‌تر PDF۴۱۷ را به محتویات یک مستند یا برچسب که قبلاً بدون آن چاپ می‌شد، اضافه کرد.

این بارکد را می‌توان یک پایگاه داده مستقل دانست که با آزادی تمام، می‌تواند با شخص یا بر روی یک شئ، بسته، فرم، مستند، کارت یا برچسب جابه‌جا شود.

PDF۴۱۷ قابلیت انجام کاری را دارد که شبکه‌های رایانه‌ای از انجام آن عاجزند یعنی دسترسی به اطلاعات بدون نیاز به قرار گرفتن در مکانی خاص. همچنین PDF۴۱۷ توانایی به رمز کردن داده‌ها در زمانی که به امنیت بیش‌تری نیاز باشد را ایجاد می‌کند.

بدلیل خوانده شدن PDF۴۱۷ به وسیله‌ی ماشین، دو مشکل اساسی اتلاف وقت و اشتباه در آن وجود ندارد. این بارکد به صورت یک حافظه رایانه‌ای کاغذی عمل می‌کند که می‌تواند یک بار نوشته شده و سپس بارها خوانده شود و همانند یک زبان ماشینی جهانی است که با تمامی سیستم عامل‌ها رابطه برقرار می‌کند.

PDF۴۱۷ تمامی کدها و داده‌های رقمی را در خود جای داده و از یک الگوریتم بسیار پیچیده و سطح بالا برای تصحیح خطاها استفاده می‌کند که قابلیت بازیابی اطلاعات حتی با از بین رفتن نیمی از بارکد را برای آن ایجاد می‌کند. این الگوریتم به بارکد قابلیت خود بازبینی نیزمی‌دهد که برای کاربر بالاترین سطح اطمینان را ایجاد می‌کند

۳-۴-۱-۲-۳- قابلیت PDF

[۱] Capturing

یک بارکد تک بعدی شامل یک کد دسترسی به اطلاعات درون یک پایگاه داده است. ولی PDF۴۱۷ خود شامل تمامی رکوردهای یک پایگاه داده بوده و نیازی به اتصال به پایگاه داده ندارد. داده‌های ذخیره شده به آسانی با اسکن شدن قابل استفاده خواهند بود.

بارکدهای دو بعُدی برای کاربردهایی که بارکدهای تک بعدی در آن‌ها محدودیت دارند بسیار ایده‌آل هستند. با خوانده شدن یک بارکد PDF۴۱۷ ، به سادگی حجم عظیمی از داده‌ها انتقال داده می‌شود. به علاوه بخش تصحیح خطا در PDF۴۱۷ آن را برای استفاده در محیط‌های سخت آماده کرده است.

۳-۴-۱-۲-۴- فن‌آوری قابل انعطاف

برخلاف دیگر فن‌آوری‌های جدید،PDF۴۱۷ نیازمند دانستن روش‌های جدید و تعویض و تغییر در سخت‌افزارها و نرم‌افزارها و یا سرمایه‌گذاری مجدد در امکانات و سیستم‌ها نیست. PDF۴۱۷ با کمی تغییر در نرم‌افزارهای کنونی و با استفاده از چاپ‌گرها و تجهیزات رایج قابل استفاده خواهد بود.

PDF۴۱۷ با تمامی چاپ‌گرهای معمولی[۱] قابل چاپ است و همچنین این بارکد را می‌توان روی هر نوع ماده‌ای چاپ نمود (کاغذ، کارت، برچسب، پلاستیک و. . .) و حتی می‌توان آن‌را فکس کرد. PDF۴۱۷ را می‌توان با هر کیفیتی (که بستگی به بارکد خوان دارد) چاپ نمود.

۳-۴-۱-۲-۵- ردیابی اطلاعات با امواج رادیویی RFID[۲]

۳-۴-۱-۲-۵-۱- تاریخچه RFID

تصور بسیاری از افراد این است که RFID یک فن‌آوری نوظهور و نوپا است. علت این تصور نادرست این است که فن‌آوری RFID به تازگی توسعه داده شده است. RFID از دهه ۷۰ میلادی وجود تجاری داشته اما به دلیل هزینه پالایش در پیاده‌سازی تاکنون گسترش چندانی پیدا نکرده است. اکنون با پیشرفت فن‌آوری در زمینه سیستم‌های اطلاعاتی، ظهور ریز پردازنده‌های قدرتمند و نسبتا ارزان و. . . می‌توان با هزینه‌های کم‌تری RFID را پیاده‌سازی کرد و چون دنیای تجاری امروزی نیاز حیاتی‌تری نیز به این گونه سیستم‌ها دارد، می‌توان آن را راحت‌تر در حوزه تجارت گسترش داد.

---

[۱] Laser Printer، Ink Jet، Thermal Direct، Thermal Transfer

[۲] radio frequency identification

اگر به مفهوم RFID دقت کنیم، می‌توان ادعا کرد که از زمان جنگ جهانی دوم این فن‌آوری حضور داشته است. سیستم مشابهی در آن زمان برای شناسایی هواپیماهای خودی و تفکیک آن‌ها از هواپیماهای دشمن توسط انگلیسی‌ها ساخته شده بود که IFF [۱] نام داشت.

در سال ۱۹۴۵ میلادی نیز فردی به نام لئون‌ترمین دستگاهی جاسوسی اختراع کرد که فن‌آوری آن مشابه RFID است.

و در نهایت این که RFID شکل امروزی توسط مخترعی به نام ماریو کاردلو ساخته شد که به علت گرانی بسیارش تا سال ۱۹۷۰ استفاده‌ای از آن در تجارت نشد.

اساس شکل‌گیری RFID به کشف انرژی الکترومغناطیس توسط فارادی در سال ۱۸۴۶ برمی‌گردد. راداری که در سال ۱۹۳۵ ساخته شد نیز می‌تواند یک RFID مقدماتی باشد. کاربرد RFID برای شناسایی حیوانات نیز در سال ۱۹۷۹ آغاز شد.

در حدود سال ۱۹۸۷ نیز کار جمع‌آوری عوارض خودروهای ایالات متحده توسط این فن‌آوری آغاز شد و از سال ۱۹۹۴ به بعد نیز کل خودروهای این کشور با استفاده از فن‌آوری RFID شناسایی می‌شود.

بیش‌ترین استفاده از RFID از سال ۲۰۰۰ به بعد انجام شده است، مثلا در سال ۲۰۰۳ شناسایی کانتینرها در جنگ آمریکا و متحدان علیه عراق به کمک RFID انجام می‌شد.

اکنون نیز در سیستم زنجیره تامین محصولات تجاری شرکت‌های پیش‌رفته، از مرحله قبل از تولید کالا تا تحویل آن به مشتری از RFID استفاده می‌شود.

۳-۴-۱-۲-۵-۲- چگونگی ردیابی اطلاعات با امواج رادیویی RFID

تراشه برچسب‌های شناسایی رادیویی یا RFID از خود سیگنال‌های ساده رادیویی مرتبط با بارکدی ویژه را در هر زمان و در هر مکانی ساطع می‌کند. محققان آینده نگر معتقدند چنین تراشه‌هایی را می‌توان به راحتی در زیر پوست بازوی افراد کار گذاشت.

تاکنون دولت مکزیک این تراشه‌ها را که ابعادی برابر یک دانه برنج دارند بر روی پوست بخش بالایی بازوی کارمندان دفتر کل دادگستری مکزیکوسیتی کار گذاشته است. این‌تراشه‌ها حاوی کدهایی است که پس از خوانده شدن توسط اسکنرهای ویژه، اجازه ورود به ساختمان‌های محافظت شده را به کارمندان داده و از ورود گروه‌های مافیایی به این محدوده قانونی جلوگیری خواهد کرد.

---

[۳] IFF اختصار عبارت Friend or Foe Identify به مفهوم تشخیص دوست از دشمن است و مکانیزم آن نیز شبیه RFID است.

محققان تایوانی نیز طی مطالعاتی جدید تاکید کرده‌اند استفاده از این‌تراشه‌ها می‌تواند پس از وقوع بلایای طبیعی از قبیل زلزله جان بسیاری از افراد را نجات دهد. در عین حال می‌توان برای کارمندان سازمانی تراشه‌هایی حاوی اطلاعات شناسایی برای ورود و خروج و برای مراجعان تراشه‌های موقتی برای ورود به محدوده‌های خاصی از یک سازمان یا اداره را صادر کرد. به گفته این محققان اطلاعات کارمندان بیمارستان و بیماران بستری را نیز می‌توان به چنین تراشه‌هایی افزود.

"ساموئل. جی. پالمیسانو" رئیس شرکت IBM در کنفرانسی صنعتی اعلام کرد: " جهان ما در حال ابزاری شدن است و امروزه در ازای هر انسان در حدود بیلیون‌ها ترانزیستور وجود دارد که تولید هر یک از آن‌ها هزینه‌ای برابر یک ده میلونیوم سنت در بر دارد. تاکنون در حدود ۳۰ بیلیون برچسب وتراشه RFID در جهان تولید و مورد استفاده قرار گرفته است. "

در صورتی که افراد مختلف بتوانند از چنین تراشه‌هایی استفاده کنند، نگرانی خانواده‌ها نسبت به فرزندانشان کاهش پیدا کرده و نجات جان انسان‌ها از خطر آسان‌تر خواهد شد. در عین حال بسیاری از فعالیت‌های روزمره از قبیل باز کردن در یا روشن کردن خودرو تنها با تکان دادن دست امکان پذیر خواهد شد. اما این آینده ایمن و ابزاری برای بسیاری از طرفداران آزادی مدنی ترسناک و دلهره آور است به‌اندازه‌ای که حتی استفاده از این‌تراشه‌ها بر روی گواهی‌نامه رانندگی یا کارت شناسایی هویت ملی انتقاد شدید بسیاری از این افراد را برانگیخته است.

به گفته این افراد و گروه‌ها استفاده از سیستم‌های ردیابی به منظور کنترل مسیر کشتی‌های باربری و کنترل حیوانات خانگی با کمک چنین تراشه‌هایی سودمند نیز هست اما استفاده از آن برای ردیابی انسان با وجود تاکید بر بی خطر بودن تراشه‌ها برای انسان و حیوان توسط سازمان دارو و غذای آمریکا، زیاده روی بوده و در حال حاضر بسیاری از مردم را ترسانده است.

از دیگر استفاده‌های تراشه‌های رادیویی استفاده در صنعت پزشکی است. برای مثال شرکتی از این تراشه‌ها به عنوان ابزاری پزشکی برای کنترل میزان گلوکز خون در بیماران دیابتی استفاده می‌کند. این استفاده‌های پزشکی به‌اندازه سیستم‌های ردیابی فردی بحث برانگیز نبوده و مورد انتقاد واقع نمی‌شوند. اما به دلیل این که این تراشه‌ها مانند کارت‌های هوشمند از فواصلی دور قابل ردیابی و دست‌یابی هستند نگرانی‌هایی را در زمینه سرقت اطلاعات ثبت شده بر روی‌تراشه‌ها برانگیخته‌اند.

براساس گزارش فاکس نیوز، با این همه دانشمندان معتقدند تا زمانی که پاسخی شفاف و قانع کننده برای مسائل ایمنی که در استفاده از این تراشه‌های رادیویی مطرح شده ارائه نشود، این فن‌آوری در لابراتوارها در قالب یک طرح باقی خواهند ماند.

تکنولوژی شناسایی مبتنی بر امواج رادیویی (RFID) روشی برای شناسایی خودکار است که با استفاده از تجهیزات RFID به نام تگ یا ترانسپوندر اطلاعات را بدون تماس فیزیکی ذخیره یا بازیابی می‌کند.

مزیت بزرگ تکنولوژی RFID بر دیگر تکنولوژی‌ها، این است که برای قرائت برچسب‌های RFID نیاز به قرار دادن دقیق آن‌ها در کنار قرائت‌گر نیست.

کاربرد فن‌آوری RFID به سرعت در حال گسترش بوده و هم‌زمان میزان و نرخ شکست‌های به‌وجود آمده نیز قابل توجه می‌باشد. برخلاف موفقیت‌های عمده اقتصادی ناشی از به کارگیری این فن‌آوری در غرب، بسیاری از شرکت‌های ناموفق در پیاده سازی این فن‌آوری، درکشورهای توسعه نیافته و شرکت‌های متعلق به آن‌ها بوده‌اند.

براساس بررسی‌های صورت گرفته عمده این عدم موفقیت‌ها ناشی از شیوه مدیریت و به‌کارگیری روش‌های سنتی هنگام مواجهه با فن‌آوری‌های نو می‌باشد. مهم‌ترین کاربرد فن‌آوری RFID در زنجیره تأمین کالا، سیستم‌های شناسایی و ردیابی و مدیریت اسناد می‌باشد.

۳-۴-۱-۲-۵-۳- اجزای سیستم RFID

سیستم‌های RFID از فن‌آوری مبادله اطلاعات بی سیم برای شناسایی انحصاری اشیا، انسان و حیوانات استفاده می‌نمایند. توانمندی این گونه سیستم‌ها مدیون به‌کارگیری سه عنصر اساسی زیر است.

برچسب (که به آن فرستنده خودکار[۱] نیز گفته می شود)، شامل یک‌تراشه نیمه‌هادی، یک آنتن و در برخی موارد یک باطری است.

بررسی کننده (که به آن کدخوان و یا دستگاه نوشتن و خواندن نیز گفته می شود)، شامل یک آنتن، یک ماژول الکترونیکی RF و یک ماژول کنترلی است.

کنترل کننده (که به آن‌هاست نیز گفته می شود)، اغلب یک رایانه شخصی و یا ایستگاه کاری است که بر روی آن بانک اطلاعاتی و نرم‌افزار کنترلی اجرا شده است.

یک گزارش گیری در سال ۲۰۰۸ توسط گروه تحقیقاتی VDC انجام شده است و میزان تقاضای جهانی RFID را مورد جستجو و بررسی قرار داده است. با وجود شرایط اقتصادی

[۱] Transponder

فعلی و مشکلاتی که در رابطه با تکمیل کردن پروژه‌های RFID وجود دارد، گروه تحقیقاتی VDC معتقد است که بازار کارت هوشمند و تکنولوژی RFID آینده روشن و درخور توجهی دارد. برطبق نتایج تحقیقاتی گروه VDC سود حاصل از کارت‌های هوشمند و تکنولوژی رادیو فرکانسی در جهان، نزدیک به ۷۰۰میلیون دلار امریکا در سال ۲۰۰۸ بوده است و پیش بینی می‌شود که تا سال ۲۰۱۳ هر سال ۲۶٪ رشد داشته باشد.

جالب‌ترین چیز در این گزارش این است که چندین زمینه در مورد کاربرد RFID به رشدی متفاوت و فوق‌العاده دارند و در فاصله زمانی کم‌تری به میزان فروش مورد نظر می‌رسد. VDC اشاره می‌کند پرداخت از طریق کارت‌های بدون تماس[۱] و بلیت‌های الکترونیکی نمونه‌های بارز این کاربردها هستند که رشد زیادی دارند. هر دوی این نمونه کاربردها که ذکر گردید، پیش از این توسط اختاپوس کارت‌ها[۲] در هنگ کنگ به‌طور برجسته مورد استفاده واقع شده بودند.

فقط کافی است نگاهی به کشورها در سرتاسر جهان بیاندازیم که از اختاپوس کارت‌هاهوشمند بدین منظور استفاده می‌کنند. در برداشت و تصور ما استفاده از کارت‌های هوشمند برای محدوده وسیعی از موارد نظیر: خرید، مجوز ورود به ساختمان، تجارت الکترونیکی در یک حوزه، آن هم حوزه شناسایی با استفاده از کارت هوشمند قرار می‌گیرد.

تکنولوژی RFID در حال حاضر در دنیا در حال شکل گرفتن است. گرچه آسیا به طور واضح یکی از پیشگامان این عرصه بوده است،اما چیزی که مردم مشتاقانه منتظر آن هستند کاربردهای تحت وب کارت هوشمند و RFID است.

RFID از فن‌آوری‌هایی است که سال‌هاست بشر آن را به خدمت گرفته، اما توجه چندانی به آن نداشته است و در واقع چیز چندان جدیدی نیست. برای توضیح عمل‌کرد آن می‌توانید فروشگاه بزرگی را در نظر بگیرید که با هزاران نوع کالای مختلف سروکار دارد و به راحتی می‌تواند ورود و خروج اجناس خود را تنها با نصب یک‌تراشه کوچک و ساده روی آن‌ها کنترل کند.

---

[۱] contactless

[۲] Octopus Carrd

امروزه با سیستم‌های شناسایی و ردیابی اطلاعات مختلفی سروکار داریم و البته ممکن است با قضایای پشت پرده برخی از آن‌ها چندان آشنا نباشیم؛ فن‌آوری‌هایی همچون OMR[۱] که یکی از موارد کاربری آن تصحیح برگه‌های امتحانات چهار جوابی کنکور است،

OCR [۲] که کار آن تشخیص هوشمند دست‌نوشته‌ها است و در سال‌های اخیر در ثبت نام آزمون ورودی رشته‌های تحصیلی مقاطع عالی به کار گرفته می‌شود.

کارت‌های هوشمند، بارکد، سیستم‌های شناسایی اشخاص از طریق صوت، اسکن مردمک چشم و بعضی از فن‌آوری‌های بیومتریک دیگر، همه و همه ابزارهایی هستند که به بشر در کار شناسایی و جمع‌آوری و ردیابی اطلاعات کمک می‌کنند. RFID نیز یکی از همین موارد است.

۳-۴-۱-۲-۵-۴- مزایای استفاده از RFID:

- بی‌نیازی قطعه Tag به قرار گرفتن در معرض دید مستقیم گیرنده (امتیازی عمده در مقایسه با بارکد).
- نداشتن استهلاک و فرسودگی به دلیل بی‌نیازی از تماس مستقیم.
- توانایی عبور سیگنال‌های رادیویی از میان مواد غیر فلزی، هوای بارانی و مه‌آلود و برفی و حتی محیط‌های کثیف و سطوح رنگ شده.
- توانایی قرائت هزاران Tag در ثانیه توسط دستگاه کدخوان RFID.
- افزایش ضریب امنیت، کنترل امور غیر قابل رویت و. . .

ضرورت به‌کارگیری RFID در گردش‌کار سازمان‌ها و مراکزی که با حجم قابل توجهی از کالاها و اقلام مختلف محصول سروکار دارند، پدیده‌ای محتمل است. این فن‌آوری در بسیاری از مراکز ـ دست کم در حد مطالعاتی مطرح است.

کشور ما نیز از نظر کاربرد تگ‌های RFID در آغاز راه است، ولی شرکت‌های نرم‌افزاری و IT با هوشیاری این روند را زیر نظر دارند و خود را برای ایفای نقش در این زمینه آماده می‌کنند. از آن‌جا که کاربردهای غیربسته بندی شانس بیش‌تری دارند، توجه این شرکت‌ها بیش‌تر متوجه امور لجستیکی سازمان‌های بزرگ است و صنعت بسته بندی به دنبال آن‌ها حرکت می‌کند.

---

[۱] Optical Mark Reader

[۲] Optical Character Recognition

کشور ما آمادگی به‌کارگیری این تکنولوژی را دارد و پس از استانداردسازی و ایجاد برخی زیرساخت‌های ضروری و نیز ارزان شدن نسبی سیستم‌های RFID انتظار می‌رود طی دو، سه سال آینده با شتاب چشم‌گیری به تولید و کاربرد برچسب‌هایRFID روی بیاورد. با این شرایط کشور ما در باید در آستانه‌ی تحولات زیرساختی برای به کارگیری این تکنولوژی به‌صورت گسترده و عمومی قرار گیرد.

۳-۴-۱-۲-۶- هولوگرام یا برچسب امنیتی[۱]

هولوگرام یکی از مناسب‌ترین ابزار جهت جلوگیری از رقابت‌های ناسالم و ایجاد امنیت است.

مزیت اصلی هولوگرام سختی و گرانی جعل پذیری است. بنابر این به‌ترین ابزار جهت حفظ اسناد و محصولات می‌باشد زیرا مدل اولیه هولوگرام به هیچ وجه با روش‌های معمول قابل تولید یا کپی نیست و با روش‌های بسیار پیچیده و در شرایطی خاص در آزمایشگاه‌های ویژه و با استفاده از نیروهای متخصص ایجاد می‌گردد. هولوگرام به‌طور روز افزونی به عنوان جزء لاینفکی از اسناد و برنامه‌های امنیتی در امور دولتی و تجاری قرار می‌گیرد.

هم‌چنین هولوگرام در اوراق و اسناد، پول و کارت‌های شناسائی مورد استفاده واقع می‌شود، قابلیت مهم هولوگرام که آن را غیر قابل تقلب می‌سازد این است که می‌توان لایه‌ها و سطوح مختلفی از اطلاعات و تصاویر قابل رؤیت و غیرقابل رؤیت را در آن درج نمود.

هولوگرام‌ها کاملا در برابر کپی برداری مصون بوده و در مقابل روش‌های رایج کپی برداری با استفاده از پیچیده‌ترین اسکنرها و یا فتوکپی‌ها مقاوم است.

هولوگرام غیر قابل انتقال از روی کالایی به کالای دیگر است حتی با استفاده از روش‌هایی همچون حرارت، بخار و. . .

هولوگرام دارای حساسیت بالایی است و غیر قابل مخدوش شدن با دست‌کاری می‌باشد.

۳-۴-۱-۲-۶-۱- گروه بندی هولوگرام

۳-۴-۱-۲-۶- ۱-۱- هولوگرام‌های شماره سریال‌دار :

در این نوع هولوگرام برای ایجاد امنیت بیش‌تر و هم‌چنین مدیریت و کنترل اجناس و مدارک، شماره سریال‌هایی بر روی برچسب به کار گرفته می‌شوند.

۳-۴-۱-۲-۶- ۱-۲- هولوگرام‌های مخصوص کارت شناسائی :

[۱] HoloGram

هولوگرام‌های شفافی هستند که بر روی کارت‌های شناسائی یا سایر مدارک حاوی نشانه، امضا و. . . قرار می‌گیرند که علاوه بر افزایش طول عمر کارت، از تقلب و کپی‌کردن کارت جلوگیری می‌نماید.

۳-۴-۱-۲-۶- ۱-۳- هولوگرام‌های نقش برگردان :

این نوع هولوگرام‌ها تصویر یا متن خاصی را در هنگام کنده شدن از خود به جای می‌گذارند. برخی به‌صورت طرحی از برچسب جدا شده و بر روی سطح قرار می‌گیرند و برخی دیگر نیز به‌صورت چاپی و با رنگ‌های مختلف بر روی سطح باقی می‌مانند.

۳-۴-۱-۲-۶- ۱-۴- هولوگرام‌های دارای طرح مخفی :

در این نوع هولوگرام‌ها، متن یا تصویر خاصی درون هولوگرام قرار می‌گیرد که در حالت عادی غیر قابل رؤیت است و فقط با استفاده از دستگاه‌های لیزر خوان مخصوص قابل رؤیت خواهد بود. از این نوع هولوگرام در مواردی که امنیت بالایی مدنظر باشد، استفاده می‌شود.

۳-۴-۱-۲-۶-۱-۵- فویل‌های هات استامپ :

در این نوع هولوگرام به‌صورت حرارتی برروی سطح مورد نظر مانند پارچه، فلزات، پلاستیک، چرم، کاغذ و. . . . منتقل می‌شود و با ماشین‌هات استامپ مورد استفاده قرار می‌گیرد.

۳-۴-۱-۲-۶-۱-۶- هولوگرام با استفاده از UV :

ایجاد رمز و تصویر نامرئی در برچسب و رویت تصویر مخفی با استفاده از نور UV ممکن است.

۳-۴-۱-۲-۶-۱-۷- هولوگرام تصویر محافظ [۱]:

ایجاد رمز و تصویر نامرئی در برچسب و رویت آن به وسیله نور ماورای بنفش یا فیلتر مخصوص. مورد مصرف در اسناد دولتی و اسکناس.

۳-۴-۱-۲-۶-۱-۸- هولوگرام شفاف [۲]:

در این نوع هولوگرام از فویل‌های شفاف استفاده می‌شود که معمولاً بر روی اسناد الصاق شده و به گونه‌ای است که متن زیر برچسب قابل مشاهده می‌باشد.

۳-۴-۱-۲-۶-۱-۹- هولوگرام ضد سرقت [۳] :

هولوگرام ضدسرقت (ضدجعل) خود به دو دسته طرح دار و ساده تقسیم می‌شود که هنگام برداشتن برچسب از روی سطح، تخریب می‌شود.

۳-۴-۱-۲-۶-۱-۱۰- هولوگرام معمولی [۴] :

این نوع برچسب‌ها در هنگام انتقال از روی سطح چسبیده شده، خراب نمی‌شوند.

۳-۴-۱-۲-۶-۱-۱۱- هولوگرام چاپ گرم [۵] :

---

[۱] Filter Image

[۲] Transparent Hologram Sticker

[۳] Anti conterfeiting Hologram Sticker

[۴] Ordinery Hologram Sticker

[۵] Hot Stamping Hologram Sticker

طرح این نوع هولوگرام روی لایه نازکی از ماده‌ای مثل آلومنیوم که در روی آن لایه پلی استر با ضخامت کم قرارداده شده است، حک می‌شود. سپس توسط اعمال فشار و حرارت با ماشین چاپ گرم و به واسطه عمل‌کرد چسب آن به صفحه کاغذ یا کارت پلاستیکی منتقل می‌شود و پس از آن جزء جدائی ناپذیر سطح الصاق شده گردیده و به هیچ وجه قابل جداسازی نمی‌باشد. کاربرد این نوع هولوگرام در موارد خاص ایمنی و اسناد و مدارک می‌باشد.

۳-۴-۱-۲-۶-۱- ۱۲- نوار هولوگرام :

این نوارها به منظور محافظت از جعبه کارتن و یا هربسته دیگری که نیاز به محافظت در سطح بالایی داشته باشند مورد استفاده قرار می‌گیرند که در کنده شدن کلماتی مانند بی‌اعتبار[۱] ، باطل شده[۲] و. . . . ازخود برجای می‌گذارد که نشان می‌دهد بسته باز شده است. در این نوع هولوگرام همانند سایر هولوگرام‌ها می‌توان از جلوه‌های گرافیکی یا مکانیسم‌های امنیتی هولوگرام استفاده کرد.

[۱] void

[۲] Canceled

۳-۵ - سئوالات خودآزمایی

۱. امنیت را تعریف نموده و تاریخچه مختصر آن را بنویسید.
۲. انواع امنیت را نام برده و توضیح دهید.
۳. انواع کلی اسناد را نام برده و توضیح دهید.
۴. نقش داروهای کنترل رفتار در حفاظت اسناد را بیان نمایید.
۵. رابطه‌ی بین جهانی شدن و امنیت را بنویسید.
۶. منظور از برچسب امنیتی چیست؟ توضیح دهید.
۷. چالش‌های امنیتی را نام برده و توضیح دهید.
۸. تقسیم‌بندی کلی اطلاعات را نوشته و توضیح دهید.

۴

فصل چهارم : امنیت شبکه‌های رایانه‌ای

آن چه در این فصل می‌خوانید:

- **تعریف شبکه‌های رایانه‌ای**
- **تاریخچه شبکه‌های رایانه‌ای**
- **انواع بهره‌برداری از شبکه‌های رایانه‌ای**
- **استراتژی امنیتی حاکم بر شبکه‌های رایانه‌ای**

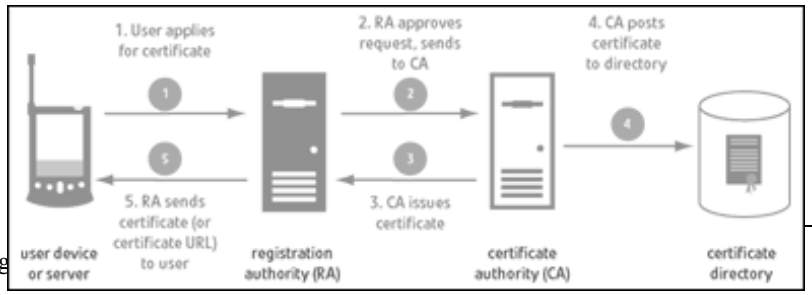
۴- امنیت شبکه‌های رایانه‌ای

۴-۱- آشنایی با پروتکل‌های امنیتی

۴-۱-۱-پروتکل PKI

پروتکل PKI، اطمینان لازم در محیط‌های دیجیتالی را فراهم می‌کند. PKI مبتنی بر گواهی دیجیتالی است (گواهی دیجیتالی به نوعی معادل با گذرنامه است که در دنیای فیزیکی مورد استفاده قرار می‌گیرد). گواهی دیجیتالی برای تائید ماهیت شخص یا مؤسسه‌ای است که در برقراری ارتباط نقش دارد و باعث تراکنش‌های دیجیتالی می‌شود. یک سیستم مبتنی بر گواهی، سرویس‌های امنیتی تصدیق اصالت، صحت داده، محرمانگی و عدم انکار را تأمین می‌کند.

اجزای اصلی PKI شامل مرجع ثبت[۱] و مرجع گواهی[۲] است (شکل زیر). مرجع ثبت یا RA، وظیفه‌ی تصدیق اصالت و ثبت کاربران جدید و درخواست گواهی برای آن‌ها را دارد. مرجع گواهی یا CA، براساس تقاضاهای صورت گرفته به‌وسیله‌ی RA، صدور را انجام داده و آن‌ها را ارسال می‌کند. یک مدل PKI، هم‌چنین شامل سیاست‌ها، رویه‌ها[۳] و قراردادهایی است که نحوه‌ی صدور گواهی، صدور مجدد و ابطال گواهی را تعیین می‌کنند. کاربردهایی که ازPKI پشتیبانی می‌کنند، می‌توانند مدیریت گواهی‌های کاربران و تولید گواهی دیجیتالی را بر روی



[۱] Reg

[۲] Certificate Authority

[۳] Procedures

PC، تلفن‌های همراه و غیره انجام دهند.

۴-۱-۲- SET[1]

SET یک پروتکل پرداخت را در سطح شبکه‌ی ارتباطی میان خریدار، فروشنده، بانک و دروازه‌ی پرداخت فراهم می‌کند. SET یک توصیف امنیتی و رمزنگاری باز، برای حفاظت از تراکنش‌های الکترونیکی انجام شده بر روی اینترنت است که کاربران را برای به‌کارگیری امن کارت‌های اعتباری در یک شبکه‌ی باز (مانند اینترنت) قادر می‌سازد. برای استفاده از این پروتکل بایستی دارنده‌ی کارت اعتباری و فروشنده دارای گواهی باشند. این گواهی‌ها از طرف یک مرجع گواهی صادر می‌شوند. در طرف خریدار، بایستی نرم‌افزار SET نصب شده و یک حساب کارت اعتباری که از SET پشتیبانی کرده و گواهی مورد نیاز را فراهم می‌کند، افتتاح شود. فروشنده نیز باید نرم‌افزار را نصب کرده و آن را در ترکیب با یک نرم‌افزار مبتنی بر وب که ارائه‌ی خدمات فروش کالا را انجام می‌دهد، برای استفاده‌ی مشتریان بر روی وب قرار دهد. نرم‌افزار مورد استفاده توسط فروشنده اندکی پیچیده‌تر است چرا که نیاز به برقراری ارتباط با هر دو طرف خریدار و دروازه‌ی پرداخت دارد.

به‌طورکلی، می‌توان مزایا و معایب SET را به‌صورت زیر بیان نمود:

- مزایا: حفاظت درمقابل استراق‌سمع، حفاظت در مقابل سوءاستفاده‌ی فروشنده ازکارت اعتباری خریدار، ایجاد اطمینان بیش‌تر برای بانک، حفظ محرمانگی خریدار نسبت به فروشنده.
- معایب: نیاز به گواهی دارد که دارای مکانیزم مدیریتی پیچیده‌ای است. عدم وجود سیستم‌های SET کامل، عدم امکان ایجاد مکانیزم گمنامی به‌طور کامل.

SET، یک تراکنش مابین مشتریان (صاحبان کارت‌های اعتباری)، بانک، طرف تجاری، سازمان‌های پردازش پرداخت پول و مراجع گواهی به‌وجود می‌آورد و تمامی امکانات مورد نیاز برای تراکنش‌های مربوط به کارت‌های اعتباری بر روی اینترنت را دارا می‌باشد. این امکانات شامل موارد زیر است:

محرمانگی اطلاعات: امنیت اطلاعات دارنده‌ی کارت و فروشنده در زمان انتقال بر روی شبکه حفظ می‌شود. یک ویژگی مهم و جالب توجه SET این است که از فاش شدن شماره و مشخصات کارت اعتباری، برای طرف حساب تجاری ممانعت می‌کند و این اطلاعات تنها از طریق بانک قابل دسترسی است. معمولاً از روشی مانند DES برای رمزنگاری استفاده می‌شود.

[1] Secure Electronic Transaction

صحت داده‌ها: SET تضمین می‌کند که اطلاعات تراکنش‌های مختلف، بدون هیچ‌گونه تغییری انتقال می‌یابند. از امضای دیجیتالی RSA با استفاده از کدهای درهم‌سازی[۱] SHA-۱ برای تحقق این امر استفاده می‌شود.

تصدیق اصالت دارنده‌ی کارت اعتباری[۲]: SET، طرف تجاری را قادر می‌سازد تا از اعتبار دارنده‌ی کارت، اطمینان حاصل کند. برای این منظور از گواهی و امضای دیجیتالی استفاده می‌شود.

تصدیق اصالت طرف تجاری[۳]: صاحبان کارت اعتباری نیز می‌توانند با بهره‌گیری از امکانات SET، اعتبار طرف تجاری خود و ارتباط آن‌ها با مؤسسات مالی (جهت حصول اطمینان از این‌که امکان استفاده از کارت اعتباری برای انجام پرداخت‌ها وجود دارد)، را مورد بررسی قرار دهند.

۴-۱-۲-۱-مدل SET

مطابق با شکل زیر، موجودیت‌های شرکت‌کننده درتراکنش‌های SET به شرح زیر می‌باشند:

دارنده‌ی کارت: در یک محیط الکترونیکی، مشتریان و خریدارها با دریافت کارت‌های اعتباری به وسیله‌ی خطوط اینترنت با طرف تجاری خود وارد معامله می‌شوند.

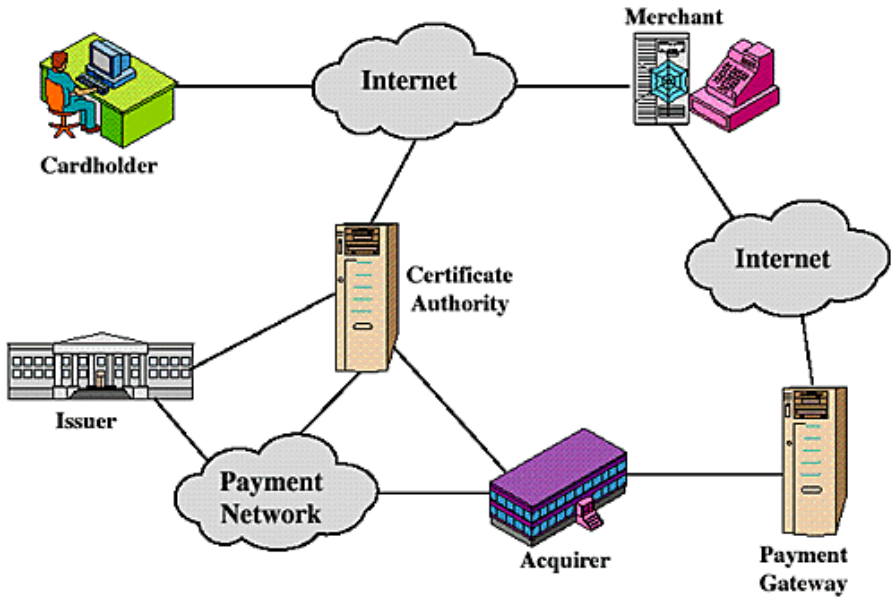
طرف تجاری: فرد یا سازمانی است که فروش کالا و خدمات تجاری را به صاحبان کارت اعتباری ارائه می‌کند. این کالاها و خدمات از طریق سایت‌های وب و یا پست الکترونیکی به مشتریان عرضه می‌شوند.

---

[۱] Hash Codes

[۲] Cardholder

[۳] Merchant



صادرکننده[۱]: یک مؤسسه‌ی مالی از قبیل بانک که افتتاح حساب و صدور کارت اعتباری را برای مشتریان (ازطریق اینترنت و یا به شکل حضوری) انجام داده و مسئولیت کلیه‌ی تراکنش‌های مالی، از جمله مسئولیت بدهی‌های دارندگان کارت را بر عهده دارد.

Acquirer: ارائه دهندگان کالا و خدمات فروش (فروشندگان) بایستی با یک مؤسسه‌ی مالی که بررسی پرداخت‌ها و تائید اعتبار آن‌ها را انجام می‌دهد ارتباط داشته باشند. acquirer بعد از انجام بررسی‌های لازم، فعال بودن یک کارت اعتباری خاص و عدم تجاوز از مقدار اعتبار دارنده‌ی کارت را به فروشنده اطلاع می‌دهد. هم‌چنین انتقال الکترونیکی پول پرداخت شده به حساب فروشنده نیز از این طریق انجام می‌شود.

دروازه‌ی پرداخت[۲]: به‌عنوان یک واسط مابین SET و شبکه‌های پرداخت بانکی عمل می‌کند و وظیفه‌ی آن بررسی مجوزها و انجام عملیات مربوط به پرداخت‌ها و انتقال پول می‌باشد. طرف تجاری با استفاده از پیغام‌های SET، با دروازه‌ی پرداخت ارتباط پیدا می‌کند

[۱] Issuer

[۲] Payment Gateway

(ازطریق اینترنت). درحالی‌که دروازه‌ی پرداخت به نوبه‌ی خود باacquirer از طریق شبکه و یا به‌طور مستقیم اتصال دارد. به این ترتیب، پردازش پیام‌های فروشندگان از طریق این بخش انجام می‌شود.

مرجع گواهی(CA[۱]) : مرجعی است که گواهی کلید عمومی را با استانداردX. ۰۹۷۳۵ برای دارندگان کارت اعتباری، فروشندگان و دروازه‌های پرداخت صادر می‌کند.

S-HTTP -۳-۱-۴

S-HTTP[۲] ضمیمه‌ای برای HTTP[۳] است که سرویس‌های امنیتی را تدارک می‌بیند. HTTP پروتکلی است که اساس وب جهانی را تشکیل می‌دهد و انتقال مستندات چندرسانه‌ای را بر روی وب میسر می‌سازد. S-HTTP برای تدارک محرمانگی، غیرجعلی بودن، تمامیت و عدم انکار طراحی شده است. این پروتکل از چندین مکانیسم مدیریت کلید و الگوریتم رمزنگاری پشتیبانی می‌کند. استفاده از این مکانیسم‌ها و الگوریتم‌ها به‌صورت توافق بین طرفین یک تراکنش قابل انجام است. S-HTTP می‌تواند از چهار متد برای تبادل کلیدهای رمزنگاری استفاده کند. این متدها عبارتند از: RSA، out-band، in-band و kerberos. چنانچه RSA استفاده شود، کلیدهای رمزنگاری توسط سیستم رمز با کلید عمومی RSA تبادل خواهند شد. منظور از out-band، یک قرارداد کلید خارجی است. منظور از in-band یک کلید است که در یک پیغام حفاظت شده‌ی S-HTTP در یک session دیگر انتقال یافته است. در متد kerberos، کلید از یک سرویس دهنده‌ی kerberos به دست می‌آید. الگوریتم‌های رمزنگاری که توسط S-HTTP پشتیبانی می‌شوند، شامل DES، DES سه‌مرحله‌ای دو کلیدی و سه کلیدی، DESX، IDEA، RC۲ و CDMF هستند.

S-MIME -۴-۱-۴

S-MIME[۴] پروتکلی است که امضای دیجیتال و رمزکردن را به پیغام‌های اینترنتی MIME می‌افزاید. MIME یک قالب استاندارد پیش‌نهادی برای پست الکترونیکی اینترنتی است. پیغام‌های پست الکترونیکی شامل دو قسمت هستند: عنوان و بدنه. قسمت عنوان، مجموعه‌ای از زوج‌های فیلد/مقدار است که اطلاعات ضروری برای انتقال پیغام را تدارک

[۱] Certificate authentication

[۲] Secure Hypertext Transfer Protocol

[۳] Hypertext Transfer Protocol

[۴] Secure/ Multipurpose Internet Mail Extensions

می‌بینند. ساختار بخش عنوان در RFC-۸۲۲ تشریح شده است. قسمت بدنه معمولاً بدون ساختار است مگر این که پست الکترونیکی در فرمت MIME باشد. MIME نحوه‌ی تعریف بدنه‌ی پیغام پست الکترونیکی را به‌صورت ساخت‌یافته مشخص می‌کند. فرمت MIME اجازه‌ی استفاده از متون بهبود یافته، گرافیک، صوت و. . . را در پیغام‌های پست الکترونیکی می‌دهد. اما خود MIME هیچ سرویس امنیتی را تدارک نمی‌بیند. هدف S/MIME، تعریف چنین سرویس‌های ی براساس دستورات گفته شده در PKCS ۷ برای امضاهای دیجیتال و رمزکردن می‌باشد. قسمت بدنه‌ی MIME، یک پیغام PKCS ۷ را انتقال می‌دهد که این پیغام، نتیجه‌ی پردازش رمزنگاری برروی سایر قسمت‌های بدنه‌ی MIME می‌باشد. اخیرا، S/MIME مورد تایید تعدادی از شرکت‌های بزرگ مانند ConnectSoft، Frontier، FTP Software، Qualcomm، Lotus، Microsoft، Wollongong، Banyan، NCD، SecureWare، Netscape، VeriSign و Novell قرار گرفته است.

SSL-۵-۱-۴

پروتکل SSL[1] توسط شرکت Netscape Communications برای تدارک امنیت و محرمانگی برروی اینترنت توسعه یافته است. این پروتکل از تصدیق اصالت در سمت سرویس‌دهنده و سرویس‌گیرنده پشتیبانی می‌کند. پروتکل SSL وابسته به کاربرد می‌باشد و به پروتکل‌هایی نظیر HTTP، FTP و telnet اجازه می‌دهد تا به‌صورت لایه‌ای برروی آن قرار گیرند. پروتکل SSL قادر است به توافق درباره‌ی کلیدهای رمزنگاری و نیز تصدیق سرویس‌دهنده قبل از تبادل اطلاعات توسط لایه‌های بالاتر اقدام نماید. پروتکل SSL، امنیت و تمامیت کانال انتقال را با استفاده از رمزکردن، تصدیق اصالت و کدهای تصدیق پیام حفظ می‌کند.

پروتکل SSL شامل ۲ مرحله‌ی تصدیق سرویس‌دهنده و تصدیق سرویس‌گیرنده است. از این میان، مرحله‌ی دوم اختیاری است. در مرحله‌ی نخست، سرویس‌دهنده در پاسخ به درخواست سرویس‌گیرنده، گواهی تصدیق خود را به همراه موارد دلخواهش برای رمزکردن، ارسال می‌کند. سپس، سرویس‌گیرنده یک شاه‌کلید تولید می‌کند، آن را با کلید عمومی سرویس‌دهنده رمز می‌نماید و شاه‌کلید رمز شده را به سرویس‌دهنده ارسال می‌کند. سرویس‌دهنده، شاه‌کلید را بازیابی کرده و با بازگرداندن یک پیغام (که با شاه‌کلید رمز شده است) به سرویس‌گیرنده، خودش را تصدیق می‌کند. داده‌های بعدی، به وسیله‌ی کلیدهای

[1] Secure Socket Layer

مشتق شده از این شاه‌کلید رمز می‌شوند. در مرحله‌ی دوم (اختیاری)، سرویس‌دهنده یک دستور شناسایی به سرویس‌گیرنده ارسال می‌کند. سرویس‌گیرنده برروی دستور شناسایی که دریافت کرده است امضای دیجیتال خودش را تولید می‌کند و آن را به همراه گواهی تصدیق کلید عمومی خود به سرویس‌دهنده باز می‌گرداند.

الگوریتم‌های رمزنگاری گوناگونی توسط SSL پشتیبانی می‌شوند. در زمان انجام فرایند Handshaking، از سیستم رمز RSA استفاده می‌شود. بعد از تبادل کلید، تعدادی رمزنگار از قبیل RC۲، RC۴، DES، triple-DES و MD۵ استفاده می‌شوند.

SEPP-۶-۱-۴

SEPP[۱] یک مشخصات علنی و باز است که توسط IBM، Netscape، GTE، CyberCash و MasterCard برای ایمن‌سازی تراکنش‌های کارت‌های بانکی برروی اینترنت توسعه یافته است. SEPP تجسمی از پروتکل iKP است که برای تراکنش‌های HTTP در نظر گرفته شده است و با پرداخت‌های کارت‌های بانکی تطبیق یافته است. پیغام‌های SEPP به وسیله‌ی MIME ارسال می‌شوند.

PCT-۷-۱-۴

PCT[۲] پروتکلی است که توسط Microsoft و Visa International برای ارتباط امن برروی اینترنت توسعه یافته است. PCT مکمل پروتکل SSL و قرینه‌ی پروتکل STT می‌باشد. این پروتکل از بسیاری جهات شبیه SSL است. در حقیقت، فرمت پیغام‌ها آن‌قدر شبیه هستند که یک سرویس‌دهنده می‌تواند هم با سرویس‌گیرنده‌های پشتیبانی‌کننده از SSL و هم با سرویس‌گیرنده‌های پشتیبانی‌کننده از PCT تعامل داشته باشد. بر اساس مشخصات موجود، PCT برخی از نقایص و ضعف‌های SSL را تصحیح می‌کند یا بهبود می‌بخشد. موارد اختلاف عبارتند از:

- PCT نسبت به SSL پیغام‌های کم‌تری را بین سرویس‌گیرنده و سرویس‌دهنده جابه‌جا می‌کند و البته خود پیغام‌ها در PCT کوتاه‌تر هستند.
- PCT نسبت به SSL انتخاب‌های بیش‌تری را برای الگوریتم و فرمت‌های داده در نظر گرفته است.

---

[۱] Secure Electronic Payment Protocol

[۲] Private Communication Technology

- تصدیق پیغام و رمزکردن آن در PCT با کلیدهای متفاوتی انجام می‌گیرد. در SSL، هر دو فرآیند مذکور با یک کلید انجام می‌شوند. بدین ترتیب، در PCT می‌توان تصدیق پیغام را با کلیدهای طولانی‌تری نسبت به رمزکردن پیغام انجام داد و به امنیت بیشتری دست خواهیم یافت.
- در پروتکل تصدیق PCT، پاسخ سرویس‌گیرنده به الگوریتم رمز مورد مذاکره بستگی دارد؛ در حالی‌که در SSL این‌گونه نیست. این ویژگی در حکم یک دیواره آتش[۱] است چون اگر دشمن موفق به بازیابی کلید رمزنگاری در یک نوبت[۲] شود و یک انتخاب برای الگوریتم (مثلا یک الگوریتم ضعیف) داشته باشد، باشد، نمی‌تواند در دفعات بعدی یک session با یک الگوریتم دیگر (مثلاً یک الگوریتم قوی) آن را مورد مخاطره قرار دهد. SSL چنین دیواره آتشی را تدارک نمی‌بیند.
- PCT برای برقراری کلید، از الگوریتم‌های RSA، Diffie-Hellman و Fortezza استفاده می‌کند؛ الگوریتم‌های رمزنگاری مورد استفاده شامل DES، triple-DES، RC۲ و RC۴ هستند. هردو امضای دیجیتال RSA و DSA پشتیبانی می‌شوند.

۴-۲- انواع حملات تحت شبکه:

یک شبکه ممکن است توسط انواع مختلفی از حملات مورد هجوم قرار گیرد. در ذیل تعرضات معروف به شبکه ذکر شده و برخی از آن‌ها توضیح داده می‌شوند:

۴-۲-۱- حملات معروف:

۱. Back door
۲. Spoofing
۳. Man in the middle
۴. Replay
۵. Tcp /ip hihacking
۶. Dns poisoning
۷. Denial of servise
۸. Distributed denial of services

---

[۱] firewall
[۲] session

۹. Social engineering
۱۰. Birthday
۱۱. Brite force
۱۲. Dictionary
۱۳. Software exploitation
۱۴. War dialing
۱۵. Buffer overflow
۱۶. Syn flood
۱۷. Smurfing
۱۸. Sniffing
۱۹. Ping of death
۲۰. Port scanning
۲۱. Fragmentation attack
۲۲. Buffer overflow exploits
۲۳. دست‌کاری در پارامترهای cgi-bin
۲۴. دست‌کاری در فیلدهای مخفی در فرم‌های html
۲۵. نمایش دایرکتوری‌ها
۲۶. دست‌کاری cookies/session
۲۷. نفوذ به وسیله پسوردها و acl ضعیف
۲۸. Cross-site scripting(xss)
۲۹. تزریق دستورات به سرور
۳۰. تزریق sql-
۳۱. جمع آوری داده حساس توسط عدم کنترل خطاها
۳۲. ضعف‌های موجود در پیکربندی سرور
۳۳. آسیب پذیری‌های مشهور
۳۴. Zero-day exploits
۳۵. استفاده از share
۳۶. استفاده از نرم افزارهای جست‌جو کننده تروجان
۳۷. استفاده از passwordهای ذخیره شده

۴-۲-۲- شرح برخی از حملات رایانه‌ای:

۴-۲-۲-۱- حملات از نوع DoS[۱]

هدف از حملات DoS، ایجاد اختلال در منابع و یا سرویس‌هائی است که کاربران قصد دست‌یابی و استفاده از آنان را دارند (از کار انداختن سرویس‌ها). مهم‌ترین هدف این نوع از حملات، سلب دست‌یابی کاربران به یک منبع خاص است. در این نوع حملات، مهاجمان با بکارگیری روش‌های متعددی تلاش می‌نمایند که کاربران مجاز را به منظور دست‌یابی و استفاده از یک سرویس خاص، دچار مشکل نموده و به‌نوعی در مجموعه سرویس‌هایی که یک شبکه ارائه می‌نماید، اختلال ایجاد نمایند. تلاش در جهت ایجاد ترافیک کاذب در شبکه، اختلال در ارتباط بین دو ماشین، ممانعت کاربران مجاز به منظور دست‌یابی به یک سرویس، ایجاد اختلال در سرویس‌ها، نمونه‌هایی از سایر اهدافی است که مهاجمان دنبال می‌نمایند. در برخی موارد و به منظور انجام حملات گسترده از حملات DoS به عنوان نقطه شروع و یک عنصر جانبی استفاده شده تا بستر لازم برای تهاجم اصلی، فراهم گردد. استفاده صحیح و قانونی از برخی منابع نیز ممکن است، تهاجمی از نوع DoS را به دنبال داشته باشد. مثلاً یک مهاجم می‌تواند از یک سایت FTP که مجوز دست‌یابی به آن به صورت مستعار و بدون اسم[۲] می‌باشد، به منظور ذخیره نسخه‌هایی از نرم افزارهای غیرقانونی، استفاده از فضای ذخیره سازی دیسک و یا ایجاد ترافیک کاذب در شبکه استفاده نماید. این نوع از حملات می‌تواند غیرفعال شدن رایانه و یا شبکه مورد نظر را به دنبال داشته باشد. حملات فوق با محوریت و تاکید بر نقش و عملیات مربوط به هر یک از پروتکل‌های شبکه و بدون نیاز به اخذ تأییدیه و یا مجوزهای لازم، صورت می‌پذیرد. برای انجام این نوع حملات از ابزارهای متعددی استفاده می‌شود که با کمی حوصله و جست‌جو در اینترنت می‌توان به آنان دست‌یابی پیدا کرد. مدیران شبکه‌های رایانه ی می‌توانند از این نوع ابزارها، به منظور تست ارتباط ایجاد شده و اشکال زدائی شبکه استفاده نمایند. حملات DoS تاکنون با اشکال متفاوتی، محقق شده‌اند. در ادامه با برخی از آنان آشنا می‌شویم.

- Smurf/smurfing : این نوع حملات مبتنی بر تابع Reply پروتکل ICMP ۳، بوده و بیش‌تر با نام ping شناخته شده می‌باشند. (Ping، ابزاری است که پس از فعال شدن از طریق خط دستور، تابع Reply پروتکل ICMP را فرا می‌خواند). در این نوع حملات، مهاجم اقدام به ارسال بسته‌های اطلاعاتی Ping

---

[۱] Denial of service

[۲] anonymous

[۳] Internet Control Message Protocol

به آدرس‌های Broadcast شبکه نموده که در آنان آدرس مبداء هر یک از بسته‌های اطلاعاتی Ping شده با آدرس رایانه قربانی، جای‌گزین می‌گردد. بدین ترتیب یک ترافیک کاذب در شبکه ایجاد و امکان استفاده از منابع شبکه با اختلال مواجه می‌گردد.

- Fraggle : این نوع از حملات شباهت زیادی با حملات از نوع Smurf داشته و تنها تفاوت موجود به استفاده از UDP [۱] در مقابل ICMP، بر می‌گردد. در حملات فوق، مهاجمان اقدام به ارسال بسته‌های اطلاعاتی UDP به آدرس‌های Broadcast (مشابه تهاجم Smurf) می‌نمایند. این نوع از بسته‌های اطلاعاتی UDP به مقصد پورت ۷ (echo) و یا پورت ۱۹ (Chargen)، هدایت می‌گردند.
- Ping flood : در این نوع تهاجم، با ارسال مستقیم درخواست‌های Ping به رایانه قربانی، سعی می‌گردد که سرویس‌ها بلاک یا فعالیت آنان کاهش یابد. در یک نوع خاص از تهاجم فوق که به ping of death، معروف است، اندازه بسته‌های اطلاعاتی به حدی زیاد می‌شود که سیستم (رایانه قربانی)، قادر به برخورد مناسب با این‌چنین بسته‌های اطلاعاتی نخواهد بود.
- SYN flood : در این نوع تهاجم از مزایای three-way handshake مربوط به TCP استفاده می‌گردد. سیستم مبداء اقدام به ارسال مجموعه‌ای گسترده از درخواست‌های SYN [۲] نموده بدون این که ACK [۳] نهائی آنان را ارسال نماید. بدین ترتیب TCP(ارتباطات نیمه فعال [۴])، ایجاد می‌گردد. با توجه به این که پشته TCP، قبل از reset نمودن پورت، در انتظار باقی خواهد ماند، تهاجم فوق، سرریز بافر اتصال رایانه مقصد را به دنبال داشته و عملاً امکان ایجاد ارتباط وی با سرویس گیرندگان معتبر، غیر ممکن می‌گردد.
- Land : تهاجم فوق، تاکنون در نسخه‌های متفاوتی از سیستم‌های عامل ویندوز، یونیکس، مکینتاش و IOS سیسکو، مشاهده شده است. در این نوع حملات، مهاجمان اقدام به ارسال یک بسته اطلاعاتی SYN [۵] که دارای آدرس‌های مبداء

---

[۱] User Datagram Protocol
[۲] synchronization
[۳] acknowledgment
[۴] half-open sessions
[۵] TCP/IP synchronization

و مقصد یکسان به همراه پورت‌های مبداء و مقصد مشابه می‌باشد، برای سیستم‌های هدف می‌نمایند. بدین ترتیب سیستم قربانی، قادر به پاسخ‌گوئی مناسب بسته اطلاعاتی نخواهد بود.

- Teardrop : در این نوع حملات از یکی از خصلت‌های UDP در پشته TCP/IP برخی سیستم‌های عامل (TCP پیاده سازی شده در یک سیستم عامل)، استفاده می‌گردد. در حملات فوق، مهاجمان اقدام به ارسال بسته‌های اطلاعاتی fragmented برای سیستم هدف با مقادیر افست فرد در دنباله‌ای از بسته‌های اطلاعاتی می‌نمایند. زمانی که سیستم عامل سعی در بازسازی بسته‌های اطلاعاتی اولیه fragmented می‌نماید، قطعات ارسال شده بر روی یک‌دیگر بازنویسی شده و اختلال سیستم را به دنبال خواهد داشت. با توجه به عدم برخورد مناسب با مشکل فوق در برخی از سیستم‌های عامل، سیستم هدف، Crash و یا راه اندازی مجدد می‌گردد.
- Bonk : این نوع از حملات بیش‌تر متوجه ماشین‌هایی است که از سیستم عامل ویندوز استفاده می‌نمایند. در حملات فوق، مهاجمان اقدام به ارسال بسته‌های اطلاعاتی UDP مخدوش به مقصد پورت ۵۳ DNS، می‌نمایند بدین ترتیب در عمل‌کرد سیستم اختلال ایجاد شده و سیستم Crash می‌نماید.
- Boink : این نوع از حملات مشابه تهاجمات Bonk می‌باشند. با این تفاوت که در مقابل استفاده از پورت ۵۳، چندین پورت، هدف قرارمی گیرد.

Service	Port
Echo	۷
Systat	۱۱
Netstat	۱۵
Chargen	۱۹

FTP-Data	۲۰
FTP	۲۱
SSH	۲۲
Telnet	۲۳
SMTP	۲۵
TACACS	۴۹
DNS	۵۳
HTTP	۸۰
POP۳	۱۱۰
Portmap	۱۱۱
SNMP	۱۶۱/۱۶۲
HTTPS	۴۴۳
RADIUS	۱۸۱۲

۴-۲-۲-۲- متداول‌ترین پورت‌های استفاده شده در حملات DoS

یکی دیگر از حملات DoS، نوع خاص و در عین حال ساده‌ای از یک حمله DoS می‌باشد که با نامDDoS [۱]، شناخته می‌شود. در این رابطه می‌توان از نرم افزارهای متعددی به منظور انجام این نوع حملات و از درون یک شبکه، استفاده به عمل آورد. کاربران ناراضی و یا افرادی که دارای سوء نیت می‌باشند، می‌توانند بدون هیچ‌گونه تاثیری از دنیای خارج از شبکه سازمان خود، اقدام به از کار انداختن سرویس‌ها در شبکه نمایند. در چنین حملاتی، مهاجمان نرم افزاری خاص و موسوم به Zombie را توزیع می‌نمایند. این نوع نرم افزارها به مهاجمان اجازه خواهد داد که تمام و یا بخشی از سیستم رایانه ی آلوده را تحت کنترل خود درآورند. مهاجمان پس از آسیب اولیه به سیستم هدف با استفاده از نرم افزار نصب شده Zombie، تهاجم نهایی خود را با بکارگیری مجموعه‌ای وسیع از میزبانان انجام خواهند داد. ماهیت و نحوه انجام این نوع از حملات، مشابه یک تهاجم استاندارد DoS بوده ولی قدرت تخریب و آسیبی که مهاجمان متوجه سیستم‌های آلوده می‌نمایند، متاثر از مجموع ماشین‌هائی (Zombie) است که تحت کنترل مهاجمان قرار گرفته شده است.

به منظور حفاظت شبکه، می‌توان فیلترهایی را بر روی روترهای خارجی شبکه به منظور دورانداختن بسته‌های اطلاعاتی مشمول حملات DoS، پیکربندی نمود. در چنین مواردی می‌بایست از فیلتری دیگر که امکان مشاهده ترافیک (مبداء از طریق اینترنت) و یک آدرس داخلی شبکه را فراهم می‌نماید، نیز استفاده گردد.

[۱] Distributed DoS

۴-۲-۳- حملات از نوع در پشتی[۱]

در پشت ، برنامه‌ای است که امکان دست‌یابی به یک سیستم را بدون بررسی و کنترل امنیتی، فراهم می‌نماید. برنامه نویسان معمولاً چنین پتانسیل‌هایی را در برنامه‌ها پیش‌بینی تا امکان اشکال زدایی و ویرایش کدهای نوشته شده در زمان تست بکارگیری نرم افزار، فراهم گردد. با توجه به این که تعداد زیادی از امکانات فوق، مستند نمی‌گردند، پس از اتمام مرحله تست به همان وضعیت باقی مانده و تهدیدها امنیتی متعددی را به دنبال خواهند داشت.

برخی از متداول‌ترین نرم افزارها ئی که از آنان به عنوان در پشتی استفاده می‌گردد، عبارتند از :

- Back Orifice : برنامه فوق یک ابزار مدیریت از راه دور می‌باشد که به مدیران سیستم امکان کنترل یک رایانه را از راه دور (مثلاً از طریق اینترنت)، خواهد داد. نرم افزار فوق، ابزاری خطرناک است که توسط گروهی با نام مکتب ارتباطات تضعیف کننده روحیه[۲] ، ایجاد شده است. این نرم افزار دارای دو بخش مجزا می‌باشد : یک بخش سرویس گیرنده و یک بخش سرویس دهنده. بخش سرویس گیرنده بر روی یک ماشین اجراء و زمینه مانیتور نمودن و کنترل یک ماشین دیگر که بر روی آن بخش سرویس دهنده اجراء شده است را فراهم می‌نماید.
- NetBus : این برنامه نیز نظیر Back Orifice، امکان دست‌یابی و کنترل از راه دور یک ماشین از طریق اینترنت را فراهم می‌نماید. برنامه فوق تحت سیستم عامل ویندوز (نسخه‌های متفاوت از NT تا ۹۵ و ۹۸)، اجراء و از دو بخش جداگانه تشکیل شده است : بخش سرویس دهنده (بخشی که بر روی رایانه قربانی مستقر خواهد شد) و بخش سرویس گیرنده (برنامه‌ای که مسئولیت یافتن و کنترل سرویس دهنده را برعهده دارد). برنامه فوق، به حریم خصوصی

[۱] Back Door

[۲] Cult of the Dead Cow Communications

کاربران در زمان اتصال به اینترنت، تجاوز و تهدیدها امنیتی متعددی را به دنبال خواهد داشت.

- SubSeven (Sub۷)، این برنامه نیز تحت ویندوز اجراء شده و دارای عمل‌کردی مشابه Back Orifice و NetBus می‌باشد. پس از فعال شدن برنامه فوق بر روی سیستم هدف و اتصال به اینترنت، هر شخصی که دارای نرم افزار سرویس گیرنده باشد، قادر به دست‌یابی نامحدود به سیستم خواهد بود.

نرم افزارهای Back Orifice، NetBus، Sub۷ دارای دو بخش ضروری سرویس دهنده و سرویس گیرنده، می‌باشند. سرویس دهنده بر روی ماشین آلوده مستقر شده و از بخش سرویس گیرنده به منظور کنترل از راه دور سرویس دهنده، استفاده می‌گردد. به نرم افزارهای فوق، " سرویس دهندگان غیرقانونی " گفته می‌شود.

برخی از نرم افزارها از اعتبار بالایی برخوردار بوده ولی ممکن است توسط کاربرانی که اهداف مخربی دارند، مورد استفاده قرار گیرند :

- VNC[۱]: نرم افزار فوق توسط آزمایشگاه T&AT و با هدف کنترل از راه دور یک سیستم، ارائه شده است. با استفاده از برنامه فوق، امکان مشاهده محیط Desktop از هر مکانی نظیر اینترنت، فراهم می‌گردد. یکی از ویژگی‌های جالب این نرم افزار، حمایت گسترده از معماری‌های متفاوت است.
- PCAnywhere : نرم افزار فوق توسط شرکت Symantec، با هدف کنترل از راه دور یک سیستم با لحاظ نمودن فن آوری رمزنگاری و تائید اعتبار، ارائه شده است. با توجه به سهولت استفاده از نرم افزار فوق، شرکت‌ها و موسسات فراوانی در حال حاضر از آن و به منظور دست‌یابی به یک سیستم از راه دور استفاده می‌نمایند.
- Services Terminal : نرم افزار فوق توسط شرکت مایکروسافت و به همراه سیستم عامل ویندوز و به منظور کنترل از راه دور یک سیستم، ارائه شده است.

۴-۳- چگونگی برآورد نیازهای امنیتی شبکه

۴-۳-۱- بازبینی شبکه و سرویس‌های فعال در آن

- بازبینی فیزیکی شبکه

[۱] Virtual Network Computing

- تهیه لیست انواع سخت افزارهای معمول و یا امنیتی مورد استفاده در شبکه (سوئیچ،هاب، دیواره آتش، کارت شبکه و غیره)
- نوع و نحوه ارتباطات شبکه‌ای
- ظرفیت‌ها اتصالات فعال و آماده به کار
- تهیه دستورالعمل حفاظت فیزیکی از تجهیزات ارتباطی شبکه به منظور عدم امکان دسترسی غیر مجاز کاربران به تجهیزات داخل (Rack) رک‌ها و سایت اصلی و. . .
- ارائه امکان تعریف LANهای مجازی امن به صورت متمرکز و توزیع شده

۴-۳-۲- بازبینی ساختار شبکه، گردش اطلاعات و مدخل‌های ورودی و خروجی اطلاعات

- انواع سیستم عامل‌های فعال به‌عنوان سرویس دهنده در شبکه
- انواع سیستم عامل‌های فعال به‌عنوان ایستگاه کاری
- تهیه لیست انواع نرم افزارهای مورد استفاده بر روی ایستگاه‌های کاری
- تهیه لیست انواع نرم افزارها و سرویس‌های فعال در درون شبکه و سرویس‌های فعال خارجی
- تهیه لیست انواع نرم افزارهای دفاعی موجود
- بررسی نحوه دسترسی به شبکه و اینترنت از طریق شبکه
- بررسی فن‌آوری‌های بین شبکه‌ای
- بررسی نحوه تبادل اطلاعات
- بررسی نحوه مدیریت اطلاعات و امنیت آن در شبکه
- بررسی نحوه نگهداری و ذخیره اطلاعات
- تشخیص و تعیین مدخل‌های ورودی و خروجی اطلاعات
- بررسی امنیت اینترنت و پست الکترونیک
- بازبینی نحوه تهیه فایل‌های پشتیبان و نحوه بازسازی آن

۴-۳-۳- تنظیم لیست موضوعی ملزومات شبکه و مخاطرات آن‌ها

- تنظیم لیست کامل سرمایه‌های سازمانی (سخت افزاری، نرم افزاری و غیره)
- تهیه لیست مخابرات مربوط به سرمایه‌ها
- تعیین میزان خطر پذیری هر سرمایه و اولویت بندی آن‌ها

- تعیین اولویت‌های اجرایی
- تهیه شناسنامه امنیتی کاربران

۴-۳-۴- تعریف و تعیین مشخصات لایه‌های دفاعی

- تعریف و تعیین نقاط ضعف موجود
- تعیین لایه‌های دفاعی مورد نظر
- تشریح مزایا و معایب هر لایه از لایه‌های دفاعی پیش‌نهادی
- تعریف و تعیین مشخصات اجرایی هر یک از لایه‌های دفاعی به تفکیک

۴-۴- چگونگی ارزیابی تهدیدها و ارائه راه حل آن‌ها

۴-۴-۱- تعیین اهداف امنیتی مورد نظر برای ایستگاه‌های کاری

- رمز عبور و قابلیت دسترسی در سیستم عامل
- تعیین استراتژی ضد ویروس
- کنترل دسترسی از خارج
- کنترل محتوا
- کنترل برنامه‌های ناخوانده
- رمز گذاری اطلاعات و ارائه الگوریتم‌ها و استاندارد پیش‌نهادی در این زمینه
- تهیه فایل پشتیبان
- طرح کنترل دستگاه‌های ورودی و خروجی
- ارائه قوانین کنترل دسترسی برای کاربران در کلیه سطوح
- نحوه ذخیره سازی امن فایل‌ها
- ثبت وقایع و ردگیری فعالیت‌های کاربران

۴-۴-۲- طرح توسعه استراتژیکی برای سایر تجهیزات شبکه

- دسترسی فیزیکی به تجهیزات شبکه
- تنظیمات سوئیچ‌ها و تقسیم بندی‌های مجاز
- نقاط قابل اتصال و بدون استفاده در شبکه
- تعیین لایه‌های دفاعی و کنترل‌های مورد نیاز در شبکه پیرامونی
- بررسی موارد مربوط به سایر تجهیزات

۴-۴-۳- بررسی نقاط احتمالی ورود ویروس و آلودگی در محل‌های ذخیره داده و تبادل اطلاعات در شبکه

- نقاط ارتباطی مستقل
- رایانه‌های قابل حمل
- سرویس دهنده‌هایی با سیستم عامل‌های غیر ویندوز در صورت استفاده از این سیستم عامل‌ها در شبکه
- سرویس دهنده‌های فایل
- سرویس دهنده‌های پست الکترونیک

۴-۴-۴- تعیین استراتژی دفاعی برای کنترل محتواهای خطرناک نظیر ویروس‌ها و یا هرزنامه‌ها و طراحی آن

- تعیین ابزارهای دفاعی برای هر پروتکل
- تعیین نوع فایل‌های مورد نظر برای کنترل
- تعیین نحوه برخورد با فایل‌های غیر قابل کنترل (رمز گذاری شده)
- اندازه و حجم فایل‌های مورد تبادل
- تعیین موضوعات مشکوک و یا خطرناک

۴-۴-۵- تعیین نحوه استقرار، مدیریت و پیکربندی ابزارهای دفاعی

- محل نصب و یا استقرار
- تعیین استثناها
- نحوه بروز رسانی
- اجرای عملیات زمان‌بندی شده
- گزارش دهی
- اخطارها
- بیان نحوه استفاده از سیستم‌های بلادرنگ (IDS) و یا سیستم‌های آنالیز فایل‌های Log و تشخیص تهاجم و سیستم‌های مونیتورینگ [۱]

۴-۴-۶- تعیین خط مشی فعالیت‌های آموزشی

- برنامه آگاهی رسانی

---

[۱] Monitoring

- دوره‌های کوتاه مدت کاربردی
- آموزش‌های تخصصی

۴-۴-۷- بازنگری برنامه‌های مربوط به حوادث غیر مترقبه

- حوادث طبیعی
- خطاهای انسانی غیر عمدی
- خطاهای انسانی عمدی

۴-۴-۸- طرح اجرای اصلاحیه‌های نرم افزارها در کل شبکه

- طرح استفاده از نرم افزارهای خودکار
- طرح بازبینی‌های دوره‌ای

۴-۵- تشریح مدیریت امنیت در شبکه

۴-۵-۱- ارائه طرح معماری امنیتی

- تشریح جنبه‌های مختلف درگیر در محدوده استاندارد امنیتی و تعیین محدوده مورد نظر برای کارفرما
- آگاهی از ارتباطات درون سازمانی
- تدوین چهارچوب ساختار امنیتی بر اساس استاندارد امنیتی
- تدوین چهارچوب مقررات امنیتی بر اساس استاندارد امنیتی

۴-۵-۲- تهیه و تدارک مقررات امنیتی

- تدوین پاره‌ای از مقررات امنیتی در شبکه
- انتشار و بررسی تاثیر مقررات جدید
- بازبینی و اصلاح مقررات در صورت لزوم

۴-۵-۳- ارائه روش گسترش روال‌های امنیتی در شبکه به منظور:

- بازدارندگی، کاهش امکان ظهور تهدید
- ممانعت، کاهش یا حفاظت در مقابل آسیب‌پذیری منابع
- تصحیح، کاهش بازتاب یا خطرات ناشی از خسارت
- تشخیص، شناسایی حملات یا ضعف‌های امنیتی و ممانعت از بروز آن
- ترمیم، بازسازی و جای‌گزینی
- جبران، تدارک راه کارهای جانبی برای جبران خسارت

۴-۵-۴- ارائه نحوه بازنگری و بازبینی کل طرح دفاعی

- تعیین میزان امنیت برقرار شده
- بازبینی مستندات

- بازنگری مسئولیت‌ها
- ارزیابی و نگرش مدیریت سازمان به طرح دفاعی
- تدوین طرح اصلاحی

۴-۶- نرم افزارهای بررسی امنیت شبکه:

برای آشنایی بیش‌تر بررسی امنیت شبکه، ذیلا لیست برخی از ابزارهای خاص (بدون تایید یا تکذیب هریک) درج می‌گردد:

- Netscan tools
- Neotrace
- Tele port
- Sam spade
- Smartwhois
- Netscan
- Nslookup
- Neotrace
- Visualtrace
- Email tracker
- Saminside
- Nessus
- Retina
- Net cat

۴-۷- سئوالات خودآزمایی

۱. شبکه‌های رایانه‌ای را به صورت کلی توضیح دهید.
۲. انواع استراتژی‌های امنیتی حاکم بر شبکه‌های رایانه‌ای را نوشته و توضیح دهید.
۳. پنج نوع از حملات رایج در شبکه‌ها را نام ببرید.
۴. نقش‌تروجان‌ها در ناامنی شبکه را توضیح دهید.
۵. ضمن توضیح نقش فایروال‌ها در امنیت شبکه، ارتباط بین عادات امنیتی و فایروال‌ها را توضیح دهید.

فصل پنجم : امنیت بانک‌های اطلاعاتی و مراکز دیتا سنتر

آن چه در این فصل می‌خوانید:

- **تعریف بانک اطلاعاتی**
- **تاریخچه بانک اطلاعاتی دیجیتال**
- **تهدیدات و فرصت‌ها در بانک‌های اطلاعاتی**
- **انواع بانک‌های اطلاعاتی دیجیتال**
- **رمز در بانک اطلاعاتی**
- **استانداردهای مراکز دیتا سنتر**
- **ثبت وقایع در بانک اطلاعاتی**
- **ضعف‌های مکانیزم امنیتی ثبت وقایع**
- **دسترسی به بانک اطلاعاتی**
- **رمز نگاری در بانک اطلاعاتی**

پشتیبان گیری از بانک اطلاعاتی

۵- امنیت بانک‌های اطلاعاتی

امروزه برای حفظ و نگهداری و دسترسی آسان و سریع به اطلاعات از بانک‌های اطلاعاتی استفاده می‌گردد و بدون استفاده از بانک اطلاعاتی عملاً بسیاری از اطلاعات غیر قابل استفاده خواهند بود. به همین خاطر پرداختن به امنیت بانک‌های اطلاعاتی می‌تواند در بسیاری از مواقع امنیت اطلاعات را به دنبال داشته باشد.

۵-۱- تهدیدات و فرصت‌ها در بانک‌های اطلاعاتی

بانک‌های اطلاعاتی دارای فرصت‌ها و تهدیدات مختلفی می‌باشد.

مزایا و ویژگی‌های بانک اطلاعاتی :

۱. امکان مدل سازی داده‌های عملیاتی بر اساس روابط و قواعد خاص
۲. ذخیره و بازیابی داده‌ها براساس یک کنترل متمرکز و کارا
۳. شاخص گذاری و سایر امکانات ذخیره سازی کارا
۴. اشتراک داده‌ها بین کاربران
۵. کاهش افزونگی داده
۶. سهولت دست‌یابی به داده
۷. تامین جامعیت و پیش‌گیری از تناقض و ادغام
۸. تامین امنیت داده‌ها
۹. امکان‌ترمیم داده‌ها یا ریکاوری
۱۰. تامین استدلال داده‌ای در دو سطح فیزیکی و منطقی
۱۱. بهینه سازی پرس‌وجوها
۱۲. تهدیدات بانک‌های اطلاعاتی
۱۳. امکان دسترسی به اطلاعات متمرکز
۱۴. دسترسی پنهان به اطلاعات متمرکز
۱۵. امکان اعمال تغییرات ناخواسته در اطلاعات
۱۶. جابه‌جایی و شکست در اطلاعات

۱۷. مشکلات در تامین امنیت توزیع شده
۱۸. پنهان سازی نرم‌افزارهای مخرب در بانک‌های اطلاعاتی
۱۹. از دست دادن بخش وسیعی از اطلاعات در صورت عدم پیش بینی‌های اولیه

۵-۲- رمز در بانک اطلاعاتی

۵-۲-۱- معرفی و اصطلاحات

رمزنگاری علم کدها و رمزهاست. یک هنر قدیمی است و برای قرن‌ها به‌منظور محافظت از پیغام‌هایی که بین فرماندهان، جاسوسان، عشاق و دیگران ردوبدل می‌شده، استفاده شده است تا پیغام‌های آن‌ها محرمانه بماند.

هنگامی که با امنیت دیتا سروکار داریم، نیاز به اثبات هویت فرستنده و گیرنده پیغام داریم و در ضمن باید از عدم تغییر محتوای پیغام مطمئن شویم. این سه موضوع یعنی محرمانگی، تصدیق هویت و جامعیت در قلب امنیت ارتباطات دیتای مدرن قرار دارند و می‌توانند از رمزنگاری استفاده کنند.

اغلب این مسئله باید تضمین شود که یک پیغام فقط می‌تواند توسط کسانی خوانده شود که پیغام برای آن‌ها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده این مسئله باشد "رمزنگاری" نام دارد. رمزنگاری هنر نوشتن به‌صورت رمز است به‌طوری که هیچ‌کس به‌غیر از دریافت کننده موردنظر نتواند محتوای پیغام را بخواند.

رمزنگاری مخفف‌ها و اصطلاحات مخصوص به خود را دارد. برای درک عمیق‌تر به مقداری از دانش ریاضیات نیاز است. برای محافظت از دیتای اصلی[۱]، آن‌را با استفاده از یک کلید (رشته‌ای محدود از بیت‌ها) به‌صورت رمز در می‌آوریم تا کسی که دیتای حاصله را می‌خواند قادر به درک آن نباشد. دیتای رمزشده [۲] به‌صورت یک سری بی‌معنی از بیت‌ها بدون داشتن رابطه مشخصی با دیتای اصلی به‌نظر می‌رسد. برای حصول متن اولیه دریافت‌کننده آن‌را رمزگشایی می‌کند. یک شخص ثالث (مثلا یک هکر) می‌تواند برای این که بدون دانستن کلید به دیتای اصلی دست یابد، کشف رمز نوشته[۳] کند. به خاطرداشتن وجود این شخص ثالث بسیار مهم است.

---

[۱] plaintext
[۲] ciphertext
[۳] cryptanalysis

رمزنگاری دو جزء اصلی دارد، یک الگوریتم و یک کلید. الگوریتم یک مبدل یا فرمول ریاضی است. تعداد کمی الگوریتم قدرتمند وجود دارد که بیش‌تر آن‌ها به‌عنوان استانداردها یا مقالات ریاضی منتشر شده‌اند. کلید، یک رشته از ارقام دودویی (صفر و یک) است که به‌خودی‌خود بی‌معنی است. رمزنگاری مدرن فرض می‌کند که الگوریتم شناخته شده است یا می‌تواند کشف شود. کلید است که باید مخفی نگاه داشته شود و کلید است که در هر مرحله پیاده‌سازی تغییر می‌کند. رمزگشایی ممکن است از همان جفت الگوریتم و کلید یا جفت متفاوتی استفاده کند.

دیتای اولیه اغلب قبل از رمزشدن بازچینی می‌شود؛ این عمل عموماً به‌عنوان scrambling شناخته می‌شود. به‌صورت مشخص‌تر، hash functionها بلوکی از دیتا را (که می‌تواند هر اندازه‌ای داشته باشد) به طول از پیش مشخص‌شده کاهش می‌دهد. البته دیتای اولیه نمی‌تواند از hashed value بازسازی شود. Hash functionها اغلب به‌عنوان بخشی از یک سیستم تایید هویت مورد نیاز هستند؛ خلاصه‌ای از پیام (شامل مهم‌ترین قسمت‌ها مانند شماره پیام، تاریخ و ساعت، و نواحی مهم دیتا) قبل از رمزنگاری خود پیام، ساخته و hash می‌شود.

- چک تایید پیام یا MAC[۱] یک الگوریتم ثابت با تولید یک امضاء برروی پیام با استفاده از یک کلید متقارن است. هدف آن نشان دادن این مطلب است که پیام بین ارسال و دریافت تغییر نکرده است. هنگامی که رمزنگاری توسط کلید عمومی برای تایید هویت فرستنده پیام استفاده می‌شود، منجر به ایجاد امضای دیجیتال۲ می‌شود.
- کلید عمومی[۳] اعداد یا کلماتی که با یک شخص یا سازمان در ارتباط می‌باشد. کلید عمومی جزئی از جفت کلید عمومی/خصوصی می‌باشد وبه صورت عمومی در دسترس کسانی که قصد انتقال اطلاعات رمز شده را دارند، می‌باشد.
- کلید خصوصی[۴] اعداد یا کلماتی که با یک شخص یا سازمان در ارتباط می‌باشد. کلید خصوصی جزئی از جفت کلید عمومی/خصوصی می‌باشد. کلید خصوصی

---

[۱] Message Authentication Check

[۲] digital signature)

[۳] Public Key

[۴] Private Key

فقط در دسترس مالک جفت کلید عمومی/خصوصی می‌باشد و برای بازگشایی اطلاعاتی که توسط کلید عمومی رمزگذاری شده استفاده می‌شود.

- ایجاد کننده‌های جفت کلید برای ایجاد یک جفت کلید عمومی و خصوصی طبق یک الگوریتم رمزگذاری مشخص استفاده می‌شود.
- Key Factories برای تبدیل کلیدهای نامشخص به کلیدهای مشخص به کار می‌رود.
- Keystores بانکی که برای مدیریت تعدادی از کلیدها به کار می‌رود.

۵-۲-۲- الگوریتم‌ها

طراحی الگوریتم‌های رمزنگاری مقوله‌ای برای متخصصان ریاضی است. طراحان سیستم‌هایی که در آن‌ها از رمزنگاری استفاده می‌شود، باید از نقاط قوت و ضعف الگوریتم‌های موجود مطلع باشند و برای تعیین الگوریتم مناسب قدرت تصمیم‌گیری داشته باشند. اگرچه رمزنگاری از اولین کارهای شانون[۱] در اواخر دهه ۴۰ و اوایل دهه ۵۰ بشدت پیشرفت کرده است، اما کشف رمز نیز پابه‌پای رمزنگاری به پیش آمده است و الگوریتم‌های کمی هنوز با گذشت زمان ارزش خود را حفظ کرده‌اند. بنابراین تعداد الگوریتم‌های استفاده شده در سیستم‌های رایانه‌ای عملی و در سیستم‌های برپایه کارت هوشمند بسیار کم است.

۵-۲-۲-۱-سیستم‌های کلید متقارن

یک الگوریتم متقارن از یک کلید برای رمزنگاری و رمزگشایی استفاده می‌کند. بیش‌ترین شکل استفاده از رمزنگاری که در کارت‌های هوشمند و البته در بیش‌تر سیستم‌های امنیت اطلاعات DEA[۲] وجود دارد که بیش‌تر به‌عنوان DES شناخته می‌شود. DES یک محصول دولت ایالات متحده است که امروزه به‌طور وسیعی به‌عنوان یک استاندارد بین‌المللی شناخته می‌شود. بلوک‌های ۶۴بیتی دیتا توسط یک کلید تنها که معمولاً ۵۶بیت طول دارد، رمزنگاری و رمزگشایی می‌شوند. DES از نظر محاسباتی ساده است و به راحتی می‌تواند توسط پردازنده‌های کند (به‌خصوص آن‌هایی که در کارت‌های هوشمند وجود دارند) انجام گیرد.

---

[۱] Shannon

[۲] data encryption algorithm

این روش بستگی به مخفی‌بودن کلید دارد. بنابراین برای استفاده در دو موقعیت مناسب است: هنگامی که کلیدها می‌توانند به یک روش قابل اعتماد و امن توزیع و ذخیره شوند یا جایی که کلید بین دو سیستم مبادله می‌شوند که قبلاً هویت یک‌دیگر را تایید کرده‌اند عمر کلیدها بیش‌تر از مدت تراکنش طول نمی‌کشد. رمزنگاری DES عموماً برای حفاظت دیتا از شنود در طول انتقال استفاده می‌شود.

کلیدهای DES ۴۰ بیتی امروزه در عرض چندین ساعت توسط رایانه‌های معمولی شکسته می‌شوند و بنابراین نباید برای محافظت از اطلاعات مهم و با مدت طولانی اعتبار استفاده شود. کلید ۵۶ بیتی عموماً توسط سخت‌افزار یا شبکه‌های به‌خصوصی شکسته می‌شوند. رمزنگاری DES سه‌تایی عبارتست از کدکردن دیتای اصلی با استفاده از الگوریتم DES که در سه مرتبه انجام می‌گیرد. (دو مرتبه با استفاده از یک کلید به سمت جلو (رمزنگاری) و یک مرتبه به سمت عقب (رمزگشایی) با یک کلید دیگر:

این عمل تاثیر دوبرابر کردن طول مؤثر کلید را دارد؛ بعداً خواهیم دید که این یک عامل مهم در قدرت رمزکنندگی است.

الگوریتم‌های استاندارد جدیدتر مختلفی پیش‌نهاد شده‌اند. الگوریتم‌هایی مانند Blowfish و IDEA برای زمانی مورد استفاده قرار گرفته‌اند اما هیچ‌کدام پیاده‌سازی سخت‌افزاری نشدند بنابر این به‌عنوان رقیبی برای DES برای استفاده در کاربردهای میکروکنترلی مطرح نبوده‌اند. پروژه استاندارد رمزنگاری پیش‌رفته دولتی ایالات متحده (AES) الگوریتم Rijndael را برای جای‌گزیتی DES به‌عنوان الگوریتم رمزنگاری اولیه انتخاب کرده است. الگوریتم Twofish مشخصاً برای پیاده‌سازی در پردازنده‌های توان-پایین مثلاً در کارت‌های هوشمند طراحی شد.

در ۱۹۹۸ وزارت دفاع ایالات متحده تصمیم گرفت که الگوریتم‌ها Skipjack و مبادله کلید را که در کارت‌های Fortezza استفاده شده بود، از محرمانگی خارج سازد. یکی از دلایل این امر تشویق برای پیاده‌سازی بیش‌تر کارت‌های هوشمند برپایه این الگوریتم‌ها و تشویق دیگران به استفاده از این نوع رمزنگاری‌ها و در نتیجه اشرافیت از راه دور به این اطلاعات بود.

برای رمزنگاری جریانی[۱] (که رمزنگاری دیتا در حین ارسال صورت می‌گیرد به‌جای این که دیتای کدشده در یک فایل مجزا قرار گیرد) الگوریتم RC۴ سرعت بالا و دامنه‌ای از طول کلیدها از ۴۰ تا ۲۵۶ بیت فراهم می‌کند. RC۴ که متعلق به امنیت دیتای RSA است، به‌صورت عادی برای رمزنگاری ارتباطات دوطرفه امن در اینترنت استفاده می‌شود.

---

[۱] streaming encryption

۵-۲-۲-۲- سیستم‌های کلید نامتقارن

سیستم‌های کلید نامتقارن از کلید مختلفی برای رمزنگاری و رمزگشایی استفاده می‌کنند. بسیاری از سیستم‌ها اجازه می‌دهند که یک جزء (کلید عمومی[۱]) منتشر شود در حالی که دیگری (کلید اختصاصی[۲]) توسط صاحبش حفظ شود. فرستنده پیام، متن را با کلید عمومی گیرنده کد می‌کند و گیرنده آن را با کلید اختصاصی خودش رمزنگاری می‌کند. به‌عبارتی تنها با کلید اختصاصی گیرنده می‌توان متن کد شده را به متن اولیه صحیح تبدیل کرد. یعنی حتی فرستنده نیز اگرچه از محتوای اصلی پیام مطلع است اما نمی‌تواند از متن کدشده به متن اصلی دست یابد، بنابراین پیام کدشده برای هرگیرنده‌ای به‌جز گیرنده مورد نظر فرستنده بی‌معنی خواهد بود. معمول‌ترین سیستم نامتقارن به‌عنوان RSA شناخته می‌شود [۳]. اگرچه چندین طرح دیگر وجود دارند. می‌توان از یک سیستم نامتقارن برای نشان دادن این‌که فرستنده پیام همان شخصی است که ادعا می‌کند استفاده کرد که این عمل اصطلاحاً امضاء نام دارد. RSA شامل دو تبدیل است که هرکدام احتیاج به بتوان‌رسانی ماجولار با توان‌های خیلی طولانی دارد:

امضاء، متن اصلی را با استفاده از کلید اختصاصی رمز می‌کند؛ رمزگشایی عملیات مشابه‌ای روی متن رمزشده اما با استفاده از کلید عمومی است. برای تایید امضاء بررسی می‌کنیم که آیا این نتیجه با دیتای اولیه یکسان است؛ اگر این‌گونه است، امضاء توسط کلید اختصاصی متناظر رمزشده است.

به بیان ساده‌تر چنان‌چه متنی از شخصی برای دیگران منتشر شود، این متن شامل متن اصلی و همان متن اما رمز شده توسط کلید اختصاصی همان شخص است. حال اگر متن رمزشده توسط کلید عمومی آن شخص که شما از آن مطلعید رمزگشایی شود، مطابقت متن حاصل و متن اصلی نشان دهنده صحت فرد فرستنده آن است، به این ترتیب امضای فرد تصدیق می‌شود. افرادی که از کلید اختصاصی این فرد اطلاع ندارند قادر به ایجاد متن رمزشده نیستند به طوری که با رمزگشایی توسط کلید عمومی این فرد به متن اولیه تبدیل شود.

اساس سیستم RSA این فرمول است: $X = Yk \pmod r$

---

[۱] public key

[۲] private key

[۳] حروف اول پدیدآورندگان آن Rivest، Shamir و Adlemen

که X متن کد شده، Y متن اصلی، k کلید اختصاصی و r حاصل‌ضرب دو عدد اولیه بزرگ است که با دقت انتخاب شده‌اند. [۱]

این شکل محاسبات روی پردازنده‌های بایتی به‌خصوص روی ۸ بیتی‌ها که در کارت‌های هوشمند استفاده می‌شود بسیار کند است. بنابراین، اگرچه RSA هم تصدیق هویت و هم رمزنگاری را ممکن می‌سازد، در اصل برای تایید هویت منبع پیام از این الگوریتم در کارت‌های هوشمند استفاده می‌شود و برای نشاندادن عدم تغییر پیام در طول ارسال و رمزنگاری کلیدهای آتی استفاده می‌شود.

سایر سیستم‌های کلید نامتقارن شامل سیستم‌های لگاریتم گسسته می‌شوند مانند Diffie-Hellman، ElGamal و سایر طرح‌های چندجمله‌ای و منحنی‌های بیضوی. بسیاری از این طرح‌ها عمل‌کردهای یک‌طرفه‌ای دارند که اجازه تایید هویت را می‌دهند اما رمزنگاری ندارند. یک رقیب جدیدتر الگوریتم RPK است که از یک تولیدکننده مرکب برای تنظیم ترکیبی از کلیدها با مشخصات مورد نیاز استفاده می‌کند. RPK یک پروسه دو مرحله‌ای است: بعد از فاز آماده‌سازی در رمزنگاری و رمزگشایی (برای یک طرح کلید عمومی) رشته‌هایی از دیتا به‌طور استثنایی کاراست و می‌تواند به راحتی در سخت‌افزارهای رایج پیاده‌سازی شود. بنابراین به خوبی با رمزنگاری و تصدیق‌هویت در ارتباطات سازگار است.

طول‌های کلیدها برای این طرح‌های جای‌گزین بسیار کوتاه‌تر از کلیدهای مورد استفاده در RSA است که آن‌ها برای استفاده در چیپ‌کارت‌ها مناسب‌تر است. اما RSA محکی برای ارزیابی سایر الگوریتم‌ها باقی مانده است؛ حضور و بقای نزدیک به سه‌دهه از این الگوریتم، تضمینی در برابر ضعف‌های عمده بشمار می‌رود.

۵-۳-روش‌های رمزگذاری

۵-۳-۱-روش متقارن [۲]

در این روش هر دو طرفی که قصد رد و بدل اطلاعات را دارند از یک کلید مشترک برای رمزگذاری و نیز بازگشایی رمز استفاده می‌کنند. در این حالت بازگشایی و رمزگذاری اطلاعات دو فرآیند معکوس یک‌دیگر می‌باشند. مشکل اصلی این روش این است که کلید مربوط به رمزگذاری باید بین دو طرف به اشتراک گذاشته شود و این سئوال پیش می‌آید که دو طرف

[۱] برای اطلاع از جزئیات بیش‌تر می‌توان به مراجعی که در این زمینه وجود دارد رجوع کرد.

[۲] Symmetric

چگونه می‌توانند این کلید را به طور امن بین یک‌دیگر رد و بدل کنند. انتقال از طریق انترانت و یا به صورت فیزیکی تا حدی امن می‌باشد اما در انتقال آن در اینترنت به هیچ وجه درست نمی‌باشد در این قبیل سیستم‌ها، کلیدهای رمزنگاری و رمزگشایی یکسان هستند و یا رابطه‌ای بسیار ساده با هم دارند. این سیستم‌ها را سیستم‌های متقارن یا " تک کلیدی " مینامیم. به دلیل ویژگی ذاتی تقارن کلید رمزنگاری و رمزگشایی، مراقبت و جلوگیری از افشای این سیستم‌ها یا تلاش در جهت امن ساخت آن‌ها لازم است در بر گیرنده " جلوگیری از استراق سمع " و " ممانعت از دست‌کاری اطلاعات " باشد.

۵-۳-۲-روش نامتقارن[۱]

این روش برای حل مشکل انتقال کلید در روش متقارن ایجاد شد. در این روش به جای یک کلید مشترک از یک جفت کلید به نام‌های کلید عمومی و خصوصی استفاده می‌شود. در این روش از کلید عمومی برای رمزگذاری اطلاعات استفاده می‌شود. طرفی که قصد انتقال اطلاعات را به صورت رمزگذاری شده دارد اطلاعات را رمزگذاری کرده و برای طرفی که مالک این جفت کلید است استفاده می‌شود. مالک کلید، کلید خصوصی را پیش خود به صورت محرمانه حفظ می‌کند. در این دسته، کلیدهای رمزنگاری و رمزگشایی متمایزند یا این‌که چنان رابطه پیچیده‌ای بین آن‌ها حکم فرماست که کشف کلید رمزگشایی با در اختیار داشتن کلید رمزنگاری، عملا ناممکن است.

۵-۳-۳- مقایسه رمزنگاری الگوریتم‌های متقارن و الگوریتم‌های کلید عمومی:

بحث‌های زیادی شده که کدام یک از این الگوریتم‌ها بهترند اما جواب مشخصی ندارد. البته بررسی‌هایی روی این سوال شده به طور مثال Needham و Schroeder بعد از تحقیق به این نتیجه رسیدند که طول پیغامی که با الگوریتم‌های متقارن میتواند رمزنگاری شود از الگوریتم‌های کلید عمومی کم‌تر است. و با تحقیق به این نتیجه ریسیدند که الگوریتم‌های متقارن الگوریتم‌های بهینه‌تری هستند. اما وقتی که بحث امنیت پیش می‌آید الگوریتم‌های کلید عمومی کارایی بیش‌تری دارند. و به‌طور خلاصه می‌توان گفت که الگوریتم‌های متقارن دارای سرعت بالاتر و الگوریتم‌های کلید عمومی دارای امنیت به‌تری هستند. در ضمن گاهی از سیستم ترکیبی از هردو الگوریتم استفاده می‌کنند که به این الگوریتم‌ها الگوریتم‌های ترکیبی[۲]

---

[۱] Asymmetric

[۲] hybrid

گفته می‌شود. اما اگر به طور دقیق‌تر به این دو نگاه کنیم آنگاه متوجه خواهیم شد که الگوریتم‌های کلید عمومی و الگوریتم‌های کلید متقارن دارای دو ماهیت کاملا متفاوت هستند و کار بردهای متفاوتی دارند به طور مثال در رمزنگاری‌های ساده که حجم داده‌ها بسیار زیاد است از الگوریتم متقارن استفاده می‌شود زیرا داده‌ها با سرعت بالاتری رمزنگاری و رمزگشایی شوند. اما در پروتکل‌هایی که در اینترنت استفاده می‌شود، برای رمز نگری کلیدهایی که نیاز به مدیریت دارند از الگوریتم‌های کلید عمومی استفاده می‌شود.

۵-۳-۴- کلیدهای قراردادی[۱]

همان‌طور که در بالا گفته شد به علت کند بودن و محدودیت رمزگذاری با روش نامتقارن از این روش فقط برای رمزگذاری کلید مشترک استفاده می‌شود. اما این روش نیز یک مشکل دارد و آن این است که هر شخص نیاز به کلید عمومی و خصوصی مربوط به خود را دارد و باید برای انتقال اطلاعات آن‌را برای طرف مقابل بفرستد. یک راه برای حل مشکل استفاده از کلید عمومی و یک مکانیزم به نام کلیدهای قراردادی می‌باشد که به طبق آن یک توافق بر روی کلید مخفی بین طرفین به وجود می‌آید و به این ترتیب نیازی به انتقال کلید نمی‌باشد. وقتی که یک بار بر روی یک کلید مشترک توافق حاصل شد از آن می‌توان برای رمزگذاری و رمزگشایی اطلاعات مربوطه استفاده کرد. معمولا در این روش از الگوریتم Diffie-Hellman استفاده می‌شود. مراحل انتقال اطلاعات از این روش به صورت زیر می‌باشد: - آغازگر ابتدا یک جفت کلید عمومی و خصوصی ایجاد کرده و کلید عمومی را همراه با مشخصات الگوریتم[۲] به سمت طرف مقابل می‌فرستد. - طرف مقابل نیز یک جفت کلید عمومی و خصوصی همراه با مشخصات الگوریتم آغازگر ساخته و کلید عمومی را برای آغازگر می‌فرستد. - آغازگر یک کلید مخفی بر اساس کلید خصوصی خود و کلید عمومی طرف مقابل ایجاد می‌کند. - طرف مقابل نیز با استفاده از کلید خصوصی خود و کلید عمومی آغازگر یک کلید مخفی می‌سازد. الگوریتم Diffie-Hellman تضمین می‌کند که کلید مخفی هر دو طرف یکسان می‌باشد.

۵-۴- الگوریتم‌های رمزنگاری کلید خصوصی

رمزهای کلید خصوصی بر مبنای نوع عملکرد، چگونگی طراحی و پیاده سازی و کاربردهایشان به دو گونه رمزهای قطعه‌ای و رمزهای دنباله‌ای تقسیم می‌شوند. که در هر یک از آ نها عملکرد رمز نگاری به صورت یک عملکرد دوجانبه بین دو طرف فرستنده و گیرنده می‌باشد که با ایجاد یک ارتباط اولیه با یک‌دیگر روی کلید خصوصی توافق می‌کنند به گونه‌ای که دشمن آن کلید را نداند. فرستندهS می‌خواهد پیام m۱،.... mi را به گونه‌ای به طرف گیرنده R بفرستد که او بتواند به محتوای پیام دست یابد و در عین حال حریف مخالف A

[۱] Agreement Key

[۲] Algorithm Specification

نتواند محتوای پیام را درک کند حتی اگر A تمامی آنچه بین R و S انتقال می‌یابد را دریافت نماید.

به همین منظور فرستنده S هر متن روشن mi را به وسیله الگوریتم رمزگذاری E و کلید خصوصی به متن رمز شده تبدیل می‌کند ودریافت کننده نیزکه متن رمز شده را دریافت کرده می‌تواند با الگوریتم رمز گشائی D و کلید خصوصی متن اصلی را بدست آورد.

۵-۴-۱- رمزهای دنباله‌ای

در طراحی رمزهای دنباله‌ای یک مولد بیت شبه تصادفی نقش تولید کننده رشته کلید را برای سیستم رمزدنباله‌ای دارد. در واقع این مولد می‌تواند مولد رشته کلید نیز محسوب شود. از دیدگاه رمز نگاری یک مولد رشته کلید امن باید دارای سه پارامتر مهم زیر باشد :

۱- پریود رشته کلید تولید شده باید به حد کافی بزرگ باشد تا با طول پیام ارسال شده سازگاری داشته باشد.

۲- دنباله بیت خروجی حاصله از مولد باید به راحتی قابل تولید کردن باشد.

۳- بیت‌های خروجی باید به سختی قابل پیش‌بینی باشند.

در واقع با در اختیار داشتن مولد و اولین n بیت خروجی a(۰)، a(۱) ..... a(n-۱) از لحاظ محاسباتی پیش‌بینی بیت n+۱ ام یعنی a(n+۱) در دنباله با احتمال بیش‌تر از ½ باید غیر ممکن باشد.

حال مسئله اصلی این است با کدام مبنا واصولی می‌توان این نتیجه گیری را انجام داد که سیگنال‌های خروجی از یک مولد رشته کلید به سختی قابل پیش‌بینی است ؟ به طور کلی اصولی قابل بررسی و کاربردی ارائه شده است تا امنیت مولدهای بیت را ضمانت کند. در واقع تاکنون روش‌های بسیاری برای تولید رشته کلیدهای امن پیش‌نهاد شده است و در مقابل نیز تحلیل‌هایی طرح شده است که با توجه به پیچیده‌ترشدن دنباله‌ها به صورت ماهرانه‌تری به تحلیل دنباله‌ها می‌پردازند. در ادامه به برخی از روش‌های تولید بیت‌های شبه تصادفی می‌پردازیم.

۵-۴-۱-۱-ساختار مولدهای بیت شبه تصادفی و رمزهای دنباله‌ای

غیر قابل پیش‌بینی بودن یک دنباله همانند تصادفی بودن آن تعبیر می‌شود برای این که یک دنباله تصادفی باشد پریود آن باید به حد کافی بزرگ باشد و هم‌چنین تکه‌های گوناگون درون دنباله دارای توزیعی تا حد ممکن یک‌نواخت باشند. در این‌جا به طور خلاصه چند روش

تولید بیت‌های شبه تصادفی و دنباله‌های شبه تصادفی شرح داده شده است. در این روش‌ها به طور مشخص ثبات‌های انتقال خطی برای ساختن مولدها به کار گرفته شده‌اند.

۵-۴-۱-۲- مولدهای همنهشتی خطی(LCG)

در این روش برای تولید اعداد شبه تصادفی از روابط بازگشتی نظیر $x_{j+1}=ax_j+b$ بهره گرفته می‌شود. در اینجا سه تایی(m،b، a) پارامترهایی را مشخص می‌کنند ،که مولد را شرح می‌دهند از این سه تایی به عنوان کلید مخفی می‌توان استفاده کرد. با توجه به این‌که x. هسته مولد می‌باشد، اگر پارامترها به‌دقت انتخاب شوند اعدادی نظیر xj به صورت تکراری نخواهیم داشت مگر آن‌که تمامی اعداد صحیح درون فاصله [۰، m-۱] در خروجی ظاهر شده باشند. «بویر» نشان داد که دنباله‌های تولید شده توسط LCG هـا از نظر رمز نگاری امن نیستند. درواقع با در اختیار داشتن قطعه‌ای طولانی ازدنباله می‌توان با روش‌هایی پارامترهای mو b و a را بازسازی نمود.

۵-۴-۱-۳-ثبات‌های انتقال پس خور (FSR)

دنباله‌های مورد استفاده در رمزنگاری می‌توانند بر مبنای ثبات‌های انتقال طراحی بشوند حتی وقتی که دارای پس خوری خطی باشند. یک ثبات انتقال پس خور از N فلیپ فلاپ و یک تابع پس خور تشکیل شده است. تابع پس خور هر عنصر جدید همانند a (t) از دنباله را به صورت جزئی از عناصری که از قبل تولید شده‌اند همانند a(t-۱) ،..... a(t-n-۱)، a(t-n) بیان می‌کند. گونه‌ای از توابع پس خور وجود دارند که به صورت زیر عمل می‌کنند:

a(t-n+۱))□ a(t-،..... a(t-۲)،a(t) =g(a(t-۱)

n)

بسته به اینکه آیا تابع g خطی است (با عملگر Xor تنها قابل اجراست) یانه، مولد یک ثبات انتقال پس خور خطی (LFSR) یا ثبات انتقال پس خور غیر خطی (NLFSR) خوانده می‌شود.

پریود دنباله تولید شده به‌وسیله یک FSR به تعداد مراحل ذخیره سازی و جزئیات اتصال پس خور بستگی خواهد داشت و به‌طور کلی حداکثر پریود یک دنباله که توسط یک FSR دارای n مرحله تولید می‌شود، ۲^n خواهد بود.

۵-۴-۱-۴-ثبات‌های انتقال پس خور غیر خطی (NLFSR)

دیاگرام حالت گونه‌هایی از FSR هـا می‌تواند شامل چرخه‌های کوچک باشد و حالات تکراری داشته باشد و دنباله اگر در یکی از این حالات قرار بگیرد ممکن است نا امن شود. یک روش مناسب طراحی ثبات انتقال n مرحله‌ای که دنباله‌هایی با حداکثر پریود ۲^n تولید

می‌نماید و دنباله‌های « دی بروئن » می‌باشد. که تعداد دنباله‌های ممکنn مرحله‌ای آن به بزرگی $۲^{(۲n-۱)-n}$ می‌باشد. که همگی آن‌ها دارای توزیع‌های ایده آلی می‌باشند. اما این دنباله‌ها که از ثبات‌های انتقال غیر خطی ساخته می‌شوند دارای مشکلاتی برای پیاده سازی توسط الگوریتم‌های شناخته شده هستند. همچنین تولید سریع این دنباله‌ها به سختی صورت می‌گیرد. همچنین برخی از خواص همبستگی بین عناصر تولید شده می‌تواند راهکارهای مناسبی برای تحلیل این دنباله‌ها ایجاد نماید.

۵-۴-۱-۵-ثبات‌های انتقال پس خور خطی (LFSR)

این ثبات‌ها مدت‌ها برای کدهای کنترل خطا، آزمایش‌های VLSI و مخابرات طیف گسترده مورد استفاده بوده‌اند و از جمله مهم‌ترین اجزاء در ساختار مولدهای شبه تصادفی می‌باشند آن‌ها توابع پس خوری به شکل زیر دارند.

□ c(n-۱) a(t-n-۱) □ a(t-n) .a(t) =c۱ a(t-۱)□ c۲ a(t-۲) □ .....

۱]،c i□[۰

و با چند جمله‌ای پس خور زیر نشان داده می‌شوند.

$x^{(n-۱)} + x^{(n)} + c_{(n-۱)}$ . .f(n) = ۱+ c۱x + c۲$x^{۲}$ + ...

به طور کلی برای این‌که حداکثر پریود ممکن ۲^{n}-۱ را برای دنباله خروجی از یک LFSR داشته باشیم، چند جمله‌ای پس خور آن می‌باید اولیه باشد. تعداد چند جمله‌ای‌های اولیه درجه n از رابطه □(۲ ^{n} −۱)/n بدست می‌آید که(n) □ نمایانگر تابع اویلر می‌باشد که تعداد اعداد صحیح مثبت و اول کوچک‌تر از عدد n را نشان می‌دهد.

به هر صورت با توجه به توابع توزیع احتمال این دنباله‌ها با حداکثر پریود دیده می‌شود که خواص آماری مطلوبی در این دنباله‌ها به وجود می‌آید. اما در برابر این خصوصیات مولدهای شبه تصادفی و به علت استفاده گسترده از ثبات‌های انتقال در این گونه مولدها روش‌های تحلیل فراوانی نیز برای تحلیل دنباله خروجی حاصل طرح شده که استفاده از این ثبات‌ها را در ساختار مولدهای بیت شبه تصادفی دچار مشکل می‌کند.

۵-۴-۱-۶-کاربردهای رمزهای دنباله‌ای، مزایا و معایب

بسیاری از رمزهای دنباله‌ای کاربردی بر مبنای LFSRها عمل می‌نمایند و از آن‌جایی که یک ثبات انتقال در واقع آرایه‌ای از بیت‌های حافظه و یک سری فیدبک می‌باشد و با یک سری Xor قابل پیاده سازی است، می‌توان امنیت قابل توجهی را تنها با تعداد کمی گیت منطقی بدست آورد. بنابراین رمزهای دنباله‌ای می‌توانند برای مصارف سخت افزاری بسیار مؤثر و کارا باشند.

اما در عین حال مشکلی که LFSRها و در نتیجه رمزهای دنباله‌ای مبتنی بر آن‌ها دارند، ناکارآمد بودن آن‌ها در نرم افزار است. در واقع برای مناسبت‌های نرم افزاری چند جمله‌ای‌های فیدبک و تعداد فیدبک‌ها بسیار مهم می‌باشد. در حالی‌که مؤثر انتخاب نکردن این چند جمله‌ای‌ها امکان حملات وابستگی را نیز ممکن است فراهم آورد.

بنابراین رمزهای دنباله‌ای حتی انواع ساده‌تر آن‌ها در اجراهای نرم افزاری نمی‌توانند سریع‌تر از رمزهای قطعه‌ای عمل نمایند. رمزهای دنباله‌ای به علت پیاده سازی مؤثرتر سخت افزاری کاربردهای فراوانی در صنایع نظامی به خصوص خطوط مخابرات نظامی دارند. از آن‌جا که در این‌گونه رمزها هر یک از بیت‌های داده‌های اصلی به صورت مستقل رمز می‌شوند، بکارگیری این‌گونه رمزها در لینک‌های مخابراتی پر از اغتشاش و نویز به جهت امکان آشکارسازی و تصحیح خطاها مؤثرتر می‌باشد. در عین حال که برای رمز نمودن حجم عظیمی از داده‌ها به‌علت سرعت اجرای بالا، رمزهای دنباله‌ای می‌توانند گزینه مناسبی باشند. همان‌طور که در سیستم‌های امنیت مخابراتی و رمزنگاری نظیر BEUها دیده می‌شود.

تحلیل و آنالیز نمودن رمزهای دنباله‌ای نیز معمولاً ساده‌تر از رمزهای قطعه‌ای صورت می‌گیرد. در عین حال امکان طرح حملات وابستگی بر روی این‌گونه سیستم‌ها که بر مبنای ثبات‌های انتقال خطی عمل می‌نمایند، بیش‌تر است اغلب رمزنگارها سعی می‌نمایند اجزای مختلف این‌گونه الگوریتم‌ها را در حالتی غیرخطی ترکیب نمایند و یا از ثبات‌های انتقال غیرخطی استفاده نمایند تا مصونیت وابستگی لازم پدید آید.

۵-۴-۱-۷- نمونه‌های رمزهای دنباله‌ای پیاده سازی شده

رمزهای دنباله‌ای بسیاری در طرح‌های مختلف پیاده سازی شده‌اند.

A۵ یک الگوریتم رمز دنباله‌ای است که برای رمز نمودن سیستم ارتباط گروهی موبایل و یا در واقع سیستم مخابراتی GSM به کار می‌رود. این الگوریتم برای رمز نمودن لینک ارتباطی میان گوشی تلفن به ایستگاه پایه به کار می‌رود.

الگوریتم XPD/KPD که توسط شرکت هیوز طراحی شده است، در رادیوهای تاکتیکی نظامی ارتش و تجهیزات جهت یاب به کار رفته است.

الگوریتم رمز دنباله‌ای NaNoTEQ که نام یک شرکت الکترونیکی در آمریکای جنوبی است برای رمز نمودن ارتباطات و مراسلات از طریق فاکس در اداره پلیس آمریکای جنوبی به کار رفته است.

می‌توان انواع دیگر رمزهای دنباله‌ای طرح شده را بیان نمود، اما آن‌چه مشخص است این‌گونه رمزها در تجهیزات مخابراتی و سخت افزاری کاربرد گسترده و فراوان دارند. به خصوص

در خطوط رادیوئی که امکان اغتشاشات و نویزهای فراوان در آن‌ها موجود می‌باشد. اما به علت سرعت نامناسب اجرای نرم افزاری آن‌ها، برای استفاده در شبکه‌های رایانه‌ای یا ایجاد امنیت در پروتکل‌های امنیت اینترنت بکار نمی‌روند.

۵-۴-۲- رمز قطعه‌ای

رمزهای قطعه‌ای که از جمله پر کاربردترین رمزهای کلید خصوصی هستند، به علت قابلیت‌های فراوان که در اجرای سریع‌تر و برقراری امنیت و ایجاد مقاومت در برابر انواع حملات متن منتخب و سایر انواع حمله‌های رمزنگاری دارند. یک رمز قطعه‌ای قدرتمند قابلیت آن را دارد که توسط روش‌های مختلف بکارگیری به عنوان یک رمز دنباله‌ای قوی استفاده شود یا این‌که ایجاد یک سامانه احراز هویت نماید. بر همین مبنا همواره سعی می‌شود یک الگوریتم رمز قطعه‌ای بر مبنای راهکارها و دستاوردهای نوین روش‌های طرح این‌گونه رمزها و با توجه به تحلیل‌های جدیدتر سامانه‌های رمز و حمله‌هایی که بر مبنای این تحلیل‌ها برروی رمزهای قطعه‌ای طرح می‌شوند، بدست آید ودر عین حال یک ساختار منظم، قابل توسعه و در عین حال نوین از رمزهای قطعه‌ای معرفی شود که در صورت نیاز به توسعه در طول کلید سری مورد استفاده و یا طول قالب داده‌های ورودی به الگوریتم، اصل ساختار الگوریتم توانایی این توسعه را بدون از دست دادن ساختار کلی شبکه رمز، عملگرها و مبناهای بکارگرفته شده داشته باشد. الگوریتم رمز طرح شده باید بتواند امنیت مورد نیاز اطلاعات محرمانه را ایجاد نماید و حاشیه امنیت لازم برای حمله‌های نوین ارائه شده و قابل توسعه را نیز داشته باشد. در طراحی الگوریتم، امنیت کامل وقابل اثبات در مقابل حمله‌های مؤثر و پرکاربردی نظیر حمله‌های تفاضلی و خطی و سایرحمله‌هایی که مبنای تازه‌تری برای تحلیل رمزهای قطعه‌ای دارند، هدف اولیه بوده و در ادامه نیز پیاده سازی و اجرای موثر رمز که لازمه طراحی می‌باشد جزء اهداف در نظر گرفته می‌شود. چنین طرحی می‌تواند با ایجاد حداکثر امنیت ممکن در یک سامانه اطلاعاتی به سرعت اجرا شود و حوزه کاربردهای مختلف اطلاعات را برآورده سازد. در واقع با توجه به نوع اطلاعات مورد استفاده از لحاظ استراتژیک و تاکتیکی بودن می‌توان در کاربردهای مختلف مورد نیاز طرح کلی این الگوریتم را استفاده نمود.

رمزهای قطعه‌ای که تعریف آن‌ها بر مبنای ترکیب توابع جای‌گزینی و جای‌گشتی می‌باشد، ساختارهای متعددی دارند که هر یک مزایا و کاربردهای متعدد مربوط به خود را دارند. خواص رمزهای قطعه‌ای امن را به صورت زیر می‌توان بیان نمود.

۱- دست‌یابی به متن اصلی از طریق متن رمزگذاری شده بدون در اختیار داشتن کلید باید غیرممکن باشد. می‌توان این خصلت را با یک‌طرفه بودن الگوریتم رمزنگاری مقایسه نمود. در واقع کلید خصوصی الگوریتم دریچه تابع رمزنگاری می‌باشد که با در اختیار داشتن آن می‌توان از متن رمز شده، متن اصلی را بدست آورد.

۲- آگاهی از الگوریتم نباید سبب تضعیف رمز شود. مخفی نگاه داشتن جزئیات الگوریتم در امنیت آن نقشی ندارد و امنیت الگوریتم باید تنها به کلید سری بستگی داشته باشد.

۳- هر بیت متن رمزشده باید به تمامی بیت‌های متن اصلی وابسته باشد. در اینصورت کوچک‌ترین تغییر در متن اصلی، متن رمزشده متفاوتی ایجاد می‌نماید. به این‌گونه از رمزها کامل گفته می‌شود.

۴- هر بیت متن رمزشده می‌بایست به تمامی بیت‌های کلید سری وابسته باشد که در این حالت در صورت کوچک‌ترین تغییر در کلید، متن رمزشده متفاوتی ایجاد می‌شود.

۵- تغییر هر بیت در داده‌های ورودی بدون تغییر کلید، باید موجب تغییرات عمده در قطعه خروجی شود.

۶- تغییر هر بیت در کلید سری بدون تغییر متن اصلی، باید موجب تغییرات عمده در متن رمزگذاری شده گردد.

۷- الگوریتم باید دارای عمل جانشینی بیت‌ها تحت کنترل داده‌های ورودی وکلید باشد.

۸- الگوریتم باید دارای عملکرد جابه‌جایی بیت‌ها تحت کنترل داده‌های ورودی وکلید باشد.

۹- الگوریتم رمز نباید دارای ساختار جبری ساده باشد. در غیر این صورت تابع رمزگذاری با یک رابطه دارای بیان جبری ساده معادل خواهد شد.

۱۰- طول متن اصلی باید با طول متن رمز شده برابر باشد.

۱۱- تمامی کلیدهای سری بکار گرفته شده باید رمز قوی تولید نمایند.

خصوصیاتی که بیان شد شرایط لازم برای طرح یک رمز قطعه‌ای قوی می‌باشد در حالی که شروط لازم و کافی برای ارزیابی و حصول اطمینان از امنیت هر سیستم رمزی، مقاومت آن در برابر حملات نوع اول، دوم و سوم در رمزنگاری می‌باشد.

در سال‌های گذشته به‌علت نیازهای فراوانی که برای کاربردهای غیرنظامی رمزنگارها وجود داشته است، بحث استاندارد سازی الگوریتم‌های رمزنگاری مطرح شده است. که نمونه‌های استاندارد شده آن در سال‌های گذشته DES با ساختاری به صورت فیستل و در سال‌های اخیر AES بوده که الگوریتم رایندال را با ساختاری نوین و به گونه‌ای مربعی به کار برده است.

الگوریتم DES از انجام عملیات بر روی قطعه‌های ۱،۴،۶و ۲۸ بیت بهره می‌گیرد که این عملکردها پیاده سازی الگوریتم را برای مصارف نرم افزاری با مشکل روبرو می‌سازد. اما الگوریتم‌هایی نظیر FEAL که به منظور پیاده سازی سریع نرم افزاری طراحی شده است، از زیر عملیات‌هایی بر روی قطعات ۸ بیتی بهره می‌گیرد. بنابراین دیده می‌شود که یک الگوریتم رمزنگاری متناسب با پیاده سازی نرم افزاری لزوماً از عملوندهای منطبق با بایت و یا ضرایبی از بایت بهره می‌گیرد.

۵-۴-۲-۱- احراز هویت و شناسائی و توابع درهم ساز

کاربردهای گوناگون رمزهای قطعه‌ای را می‌توان توسط مدهای کاربردی که تعیین کننده گستره وسیع کاربردی رمزهای قطعه‌ای در مصارفی نظیر احراز هویت پیام، مولدهای بیت شبه تصادفی، توابع درهم ساز و مدیریت کلید می‌باشد، بیان نمود.

رمزهای قطعه‌ای در حالات ECB، OFB، CBC و CFB بکاربرده می‌شوند. حالات بکارگیری رمز در مدهای CFBو OFB در ایجاد مولدهای بیت شبه تصادفی و طراحی رمزهای دنباله‌ای کاربردهای فراوان دارند. در حالی که مد OFB دارای مزایایی نظیر امنیت بالا، انتشار خطای محدود و ایمنی در برابر حمله‌های لغت نامه‌ای و فعال می‌باشد و در عین حال سنکرون نبودن این گونه سیستم‌ها می‌تواند معایبی را در این نوع کاربرد به وجود آورد.

مزایای به کارگیری روش‌های CBCو CFB را می‌توان در جامعیت پیام‌های ارسالی و قابلیت دسترسی گسترده به داده‌ها و تامین ایمنی در برابر حملات لغت نامه‌ای و مهم‌تر از همه تامین کد هویت و شناسائی پیام دانست. که قابلیت احراز هویت را به کاربردهای رمزهای قطعه‌ای می‌افزاید. اما این دو حالت به کارگیری عیوب عمده‌ای نظیر انتشار خطا در خطوط ارتباطی را می‌توانند در بر داشته باشند.

استاندارد X۹۰۹ الگوریتم DES را در حالت CBC به عنوان روش احراز هویت بیان می‌کند که در هر هفته در حدود ۱/۵ تریلیون دلار از طریق آن میان مؤسسات مالی به شکل عمده مبادله می‌شد.

تکنیک‌های فراوانی نیز موجود می‌باشد که در آن‌ها نشان داده شده است که از رمزهای قطعه‌ای می‌توان در طراحی توابع درهم ساز که از ملزومات روش‌های احراز هویت و امضاهای دیجیتال می‌باشند، استفاده نمود.

۵-۴-۲-۲- سیاست‌های رمزنگاری

در هر کشوری سیاست‌های رمزنگاری وابسته به میزان خطراتی است که اطلاعات آن کشور را تهدید می‌نماید این سیاست‌ها می‌تواند ساده و یا پیچیده طراحی گردد. نکته مهم این است که هیچ سیاست وارداتی و غیربومی رمزنگاری قادر به حفظ اطلاعات یک کشور نبوده و هر کشور می‌بایست بسته به مقضیات خود این سیاست را بومی نگاری نماید.

۵-۵- ثبت وقایع در بانک اطلاعاتی

یکی از روش‌های مدیریت امنیتی بر بانک‌های اطلاعاتی اطلاع حاصل نمودن از کلیه تحرکاتی است که به صورت مستقیم و یا غیر مستقیم در رابطه با بانک اطلاعاتی به وقوع می‌پیوندد. این کار با ثبت کردن وقایع اتفاقیه حاصل می‌شود. این عمل را در رایانه اصطلاحاً log نمودن وقایع می‌نامند که انواع و اقسام مختلفی دارد که ذیلاً به مهم‌ترین آن‌ها اشاره می‌شود:

- ثبت وقایع موضوعی
- ثبت وقایع زمانی
- ثبت وقایع کاربردی
- ثبت وقایع اتفاقیه
- ثبت وقایع رخدادی و اتفاق نیفتاده
- ثبت تغییرات در بانک
- ثبت روال‌های انجام شده
- ثبت errors
- ثبت تهیه پشتیان
- ثبت اقدامات غیر متقربه
- ثبت اعتبار کاربران

۵-۶- ضعف‌های مکانیزم امنیتی ثبت وقایع

اگر چنان‌چه سیستم ثبت وقایع به هر دلیلی از کار بیفتد در بررسی امنیت سیستم مدیر بانک اطلاعاتی را با مشکل روبرو می‌نماید. یکی از روش‌های آمادگی برای نفوذ در بانک‌های اطلاعاتی، از کارانداختن تمام یا بخشی از سیستم ثبت وقایع می‌باشد. ممکن است در یک سیسم نگارش log برخی از اقدامات ثبت و برخی دیگر ناقص صورت پذیرد و قابلیت اطمینان به اطلاعات تولید شده را از بین ببرد. برای ممانعت از این کار می‌بایست در زمان‌های مختلف با

انجام دادن آزمایشات حفاظتی از این مسئله اطمینان حاصل نمود که سیستم به صورت از پیش طراحی شده عمل نموده و با اشکال تعریف شده و یا تعریف نشده روبرو نمی‌باشد.

۵-۷-دسترسی به بانک اطلاعاتی

دسترسی مجاز و غیر مجاز به بانک اطلاعاتی می‌تواند به روش‌های مختلف صورت بگیرد.

- دسترسی محلی
- دسترسی از راه دور
- دسترسی برنامه ریزی شده
- دسترسی مستقیم
- دسترسی غیر مستقیم (دسترسی به اطلاعات)
- دسترسی از روش ثالث

برای این که انواع دسترسی به بانک‌های اطلاعاتی را کنترل نموده و به صورت متمرکز نسبت به ایجاد امنیت در آن اقدام نمود معمولاً سازمان‌ها تلاش دارند تا با ایجاد دیتا سنتر و پایگاه‌های اطلاعات ، سیاست‌های امنیتی خود را به صورت متمرکز برقرار سازند. مراکز متمرکز حفظ و نگهداری اطلاعات یا همان دیتا سنترها برای حفاظت از بانک‌های اطلاعاتی دارای استانداردهای امنیتی می‌باشند که در ذیل به یکی از انواع آن اشاره می‌گردد.

۵-۷-۱- ساختار دیتا سنتر

مراکز داده، به صورت کلی می‌توانند شامل قسمت‌های زیر باشند. این قسمت‌ها، بسته به دسته بندی مراکز داده می‌توانند متغیر باشند:

۱. ساختار فیزیکی دیتا سنتر:

- سیستم‌های توزیع و کنترل برق و برق اضطراری(UPS)
- سیستم‌های تهویه هوا(HVAC) و کشف رطوبت
- سیستم‌های اعلام و اطفاء حریق
- سیستم‌های کنترل دسترسی فیزیکی
- سیستم‌های پشتیبان (افزونه (N+۱))
- سیستم‌های ساختمان هوشمند(BMS)

۲. ساختار شبکه‌ایی دیتا سنتر:

- تجهیزات فعال شبکه مانند سوییچ‌ها و روترها
- تجهیزات امنیتی مانند دیواره‌های آتش، IDSها و IPSها، ضدویروس‌ها و سایر سامانه‌های امنیت شبکه

- سیستم‌های مدیریتی و پایش شبکه
- سرورها و برنامه‌های مورد نیاز آن‌ها
- Storages
- تجهیزات غیرفعال شبکه

۳. برنامه‌های کاربردی:

- سیستم‌های امنیت اطلاعات و حفظ امنیت نرم افزار
- سیستم‌های مدیریت سیستم‌های عامل، بانک‌های اطلاعاتی
- سیستم‌های یک‌پارچه سازی اطلاعات
- پایگاه‌های داده، فایل سرورها و برنامه‌های مربوط به داده‌های عملیاتی
- سیستم‌های ذخیره‌سازی و بازیابی اطلاعات

۵-۷-۲- ویژگی‌ها

معماری دیتا سنتر باید به گونه‌ای باشد که در آن اعمال تغییرات به صورت پویا امکان‌پذیر باشد. پنج عامل مهم در طراحی دیتا سنتر عبارت است از:

- سادگی[۱]
- قابلیت انعطاف[۲]
- مقیاس پذیری[۳]
- ماژولار بودن[۴]
- منطقی بودن[۵]

۵-۷-۳- استانداردهای دیتا سنتر

در آوریل ۲۰۰۵، TIA استاندارد TIA-۹۴۲ را برای دیتا سنتر منتشر کرد. این استاندارد مطالب زیر را پوشش می‌دهد:

---

[۱] Simplicity

[۲] Flexibility

[۳] Scalability

[۴] Modularity

[۵] Sanity

۵-۷-۳-۱- فضای سایت و ترکیب بندی آن

فضای اختصاص یافته به دیتا سنتر باید به گونه‌ای باشد که این فضا به سادگی قابل توسعه بوده و اعمال تغییرات محیطی در آن به سادگی امکان پذیر باشد. طراح باید بین هزینه‌های ترکیب بندی آغازی وپیش‌بینی فضای مورد نیاز آتی تعادل برقرار کند.

در دیتا سنتر باید "فضای خالی" در نظر گرفت به گونه‌ای که این فضای خالی بتواند رک‌ها و کابینت‌های مورد نیاز آتی را در خود جای دهد. فضای اطراف دیتا سنتر نیز باید به درستی برای توسعه و الحاقات آتی طراحی شود.

بخش عمده‌ی این استاندارد به مشخصات فنی دیتا سنتر مربوط می‌شود. این استاندارد محیط‌های عملیاتی خاصی را در راستای کمک به تعیین مکان تجهیزات براساس طراحی توپولوژی ستاره‌ای توصیه می‌کند. طراحی دیتا سنتر با این محیط‌های عملیاتی امکان اضافه شدن و به روزشدن برنامه‌های کاربردی و سرورها را با حداقل مدت زمان از کار افتادگی فراهم می‌کند. براساس این استاندارد یک دیتا سنتر باید شامل محیط‌های عملیاتی کلیدی زیر باشد:

یک یا چند اتاق ورودی[۱] مکانی برای سیستم‌های ایجاد دسترسی و نقاط مرزی است. این بخش ممکن است درون یا بیرون اتاق رایانه (بخشی از دیتا سنتر که تجهیزات پردازش داده در آن قرارگرفته‌اند) باشد. استاندارد برای ایمنی بیش‌تر توصیه می‌کند که این اتاق بیرون اتاق رایانه باشد.

۵-۷-۳-۲- منطقه توزیع اصلی (MDA) [۲]

بخش مرکزی که درخود، تجهیزات اصلی اتصال مانند روترها و سوییچ‌های هسته‌ای[۳] را جای داده است. مطابق با استاندارد هر دیتا سنتر حداقل به یک DMA نیاز دارد. استاندارد نصب رک‌های جداگانه برای کابل‌های فیبر نوری، UTP را توصیه می‌کند.

۵-۷-۳-۳-منطقه توزیع افقی (HAD)[۴]

---

[۱] Entrance Room

[۲] Main Distribution Area

[۳] Core Switch

[۴] Horizontal Distribution Area

نطقه توزیع کابل شی و تجهیزات اتصال شبکه مانند سوئیچ‌ها را می‌گویند. که مانند MDA استاندارد، نصب رک‌های جداگانه برای کابل‌های فیبر نوری، UTP را توصیه می‌کند. علاوه براین، استاندارد توصیه می‌کند که برای اتصال سوییچ و Patch Panel از Patch Cord با حداقل طول و Cable Management استفاده شود.

۵-۷-۴- محیط‌های عملیاتی کلیدی دیتا سنتر

۵-۷-۴-۱- منطقه توزیع تجهیزات(EDA) [۱]:

این منطقه مکانی برای تجهیزات کابینتی و رک‌ها است و مسیرکابل‌ها به Patch Panel ختم می‌شود. استاندارد توصیه می‌کند برای داشتن یک راهروی سرد و گرم جهت کاهش گرمای تولید شده توسط تجهیزات و رساندن سرما به درجه لازم، رک‌ها و کابینت‌ها به صورت یک درمیان نصب شوند.

۵-۷-۴-۲- منطقه توزیع جدا شده (ZDA) [۲]:

یک لینک اختیاری بین HDA و EDA که می‌تواند به عنوان نقطه تقویتی برای پیکربندی دوباره مطمئن یا برای جادادن تجهیزات مستقل [۳] مانند سرورها و Mainframeهایی که به Patch Panel وصل نمی‌شوند عمل کند به ازای هر ۲۸۸ اتصال تنها یک ZDA مجاز است. در این بخش وجود تجهیزات فعال شبکه و یا اتصال شبکه مجاز نیست.

۵-۷-۴-۳-کابل کشی ستون فقرات و کابل کشی افقی [۴]

ارتباط بین MDA، HDA و اتاق ورودی و هم‌چنین ارتباط بین HDAها می‌تواند از نوع کابل کشی ستون فقرات [۵] باشد.

۵-۷-۴-۴- TIA-۹۴۲:

استانداردی است که توسط انجمن علمی صنعت ارتباطات (TIA) در سال ۲۰۰۵ برای تعیین راهکارهای عملی برای طراحی و ساخت Data Centerها مخصوصا با توجه به سیستم‌های کابل کشی و طراحی شبکه، ایجاد شده است. این استاندارد، در دستورالعمل‌های

---

[۱] Equipment Distribution Area

[۲] Zone Distribution Area

[۳] Freestanding

[۴] Backbone and Horizontal Cabling

[۵] Backbone

خود هر دو نوع رسانه فیبر نوری و کابل‌های مسی را مد نظر قرار داده است. TIA-۹۴۲ هم‌چنین مرجعی تعیین کننده برای نیازمندی‌های خاص نواحی خصوصی و عمومی Data Center در مورد برنامه‌های کاربردی و دستورالعمل‌های اجرایی می‌باشد. به طور مثال:

۱- معماری شبکه
۲- طراحی الکتریکی
۳- ذخیره سازی و تهیه نسخه پشتیبان
۴- افزونگی سیستم
۵- امنیت و کنترل دسترسی به شبکه
۶- مدیریت پایگاه داده
۷- میزبانی Web و برنامه‌های کاربردی
۸- توزیع محتوا
۹- کنترل محیط
۱۰ - حفاظت در برابر اتفاقات فیزیکی (طوفان، زلزله، آتش سوزی و. . . .)

مزایای اصلی طراحی Data Center مطابق با استاندارد TIA-۹۴۲ شامل نام‌گذاری استاندارد قطعات و تجهیزات، اطمینان از کارکرد بدون اشکال و خرابی، حفاظت قوی در برابر آسیب‌های طبیعی یا مصنوع بشری و قابلیت اطمینان، توسعه پذیری و مقیاس پذیری برای مدت طولانی است.

۵-۷-۴-۵-اهداف استاندارد TIA-۹۴۲

هدف مهم این استاندارد، تهیه نیازمندی‌ها و راهنمایی‌های لازم برای طراحی و نصب Data Center و یا اتاق رایانه می‌باشد. این استاندارد مد نظر طراحانی است که احتیاج به فهم گسترده در مورد طراحی Data Center شامل طرح ریزی ساختمان، سیستم‌های کابل کشی و طراحی شبکه دارند.

۵-۷-۴-۵-۱-مدل Data Center منطبق بر استاندارد TIA-۹۴۲

استاندارد TIA-۹۴۲ چهار ناحیه اصلی را در Data Center متصور شده است که عبارتند از:

۱-اتاق ورودی
۲-اتاق رایانه شامل نواحی:
- ناحیه توزیع اصلی(MDA)
- ناحیه توزیع افقی(HAD)

- ناحیه توزیع دسته بندی شده(ZDA)
- ناحیه توزیع تجهیزات(EDA)

۳-اتاق مخابرات

۴-اتاق تجهیزات مکانیکی و الکتریکی

۵-۷-۴-۵-۲- Tierهای Data Center بر اساس استاندارد TIA-۹۴۲

Data Centerها با توجه به استاندارد TIA-۹۴۲ به چهار Tier زیر تقسیم می‌شود:

Tire ۱:

این Tier یک Tier ساده و بدون تجهیزات پیچیده است.

این Tier فاقد اجزاء افزونه و تجهیزات محافظ در برابر آتش و تجهیزات خنثی کننده می‌باشد.

برای توزیع برق، هوا و ارتباطات شامل مسیرهای اضافی نیست.

تنها از یک دسترسی دهنده، سرویس دریافت می‌کنند.

هر گونه قطع در تجهیزات و مسیرها باعث از کار افتادن کل Data Center می‌شود.

توقف، برنامه ریزی شده و برنامه ریزی نشده دارد

در یک سال تا ۴۰ ساعت Downtime دارد

Tire۲:

در این Tier نسبت به Tier یک برای سیستم الکتریکی پشتیبان در نظر گرفته می‌شود

فقط مسیر توزیع برق و سیستم‌های تهویه و کابل‌های ارتباطی منظور می‌شود.

تنها از یک فراهم کننده دسترسی سرویس دریافت می‌شود.

یک سیستم اطفای حریق و تجهیزات خنثی کننده در این Tier منظور می‌گردد

توقف برنامه ریزی شده و برنامه ریزی نشده دارد (کم‌تر از Tier یک)

در یک سال تا ۲۲ ساعت Downtime دارد

Tire۳:

کلیه تجهیزات شبکه اعم از مسیر یاب‌ها و سوئیچ‌ها و. . . دارای پشتیبان هستند.

برای سیستم توزیع برق، تهویه هوا و ارتباطات دو مسیر منظور می‌گردد (یکی فعال و دیگر به عنوان پشتیبان و در حالت عادی غیر فعال)

حداکثر از دو فراهم کننده دسترسی، سرویس گرفته می‌شود.

سیستم برق ، ژنراتورها و UPS همگی دارای پشتیبان هستند.

سیستم شناسایی و اطفای حریق و پیش خنثی کننده دارد

سیستم ایمنی CCTV دارد
تنها برای فعالیت‌های برنامه ریزی شده متوقف می‌شود
در یک سال تا ۱. ۶ ساعت Downtime دارد

Tire۴:

کلیه تجهیزات شبکه اعم از مسیر یاب‌ها و سوئیچ‌ها و. . . دارای پشتیبان هستند.
برای سیستم توزیع برق، تهویه هوا و ارتباطات دو مسیر منظور می‌گردد (هر دو فعال)
حداقل از دو فراهم کننده دسترسی، سرویس گرفته می‌شود.
سیستم برق ، ژنراتورها و محافظ برق[۱] همگی دارای پشتیبان هستند.
سیستم شناسایی و اطفای حریق و پیش خنثی کننده دارد
سیستم ایمنی CCTV دارد
تنها برای فعالیت‌های برنامه ریزی شده متوقف می‌شود
در یک سال تا ۴۰ ساعت Downtime دارد

۵-۸-پشتیبان گیری از بانک اطلاعاتی

برای امن نگهداشتن اطلاعات بانک اطلاعاتی از اتفاقات ناخواسته معمولاً به صورت نوبه‌ای و یا غیر نوبه‌ای از بانک‌های اطلاعاتی پشتیبان تهیه می‌گردد تا اگر چنان‌چه اتفاق خاصی برای اطلاعات افتاد بتوان از اطلاعات پشتیبان با جای‌گزین کردن استفاده و خطر از دست دادن اطلاعات را به حداقل رساند.

روش‌های مختلفی برای تهیه اطلاعات پشتیبان وجود دارد.

۵-۸ -۱- تهیه پشتیبان سیستمی

در این روش نرم افزار نویسان با قرار دادن روش‌های سیستمی در بانک اطلاعاتی و ارائه آن به راهبران و یا کاربران بانک اطلاعاتی به تهیه پشتیبان کمک می‌نمایند. در این روش مطالب مورد نظر نویسنده سیستم پشتیبان گیری شده و کاربران بانک اطلاعاتی نمی‌توانند در نوع تهیه دخالتی داشته باشند و ممکن است نیازمندی واقعی استفاده کنندگان از اطلاعات با نیازمندی‌های دیده شده توسط برنامه نویس با یک‌دیگر منطبق نباشد.

اگر در ابتدای استفاده از بانک اطلاعاتی به این نکته توجه نگردد و چنان‌چه اتفاق خاصی برای اطلاعات بیفتد نمی‌توان انتظار داشت که حتما اطلاعات پشتیبان بتواند به صورت کامل مشکل را مرتفع

[۱] UPS

سازد.

۵-۸-۲- تهیه پشتیبان غیر سیستمی

در این روش کاربران و یا راهبران سیستم به صورت غیر اتوماتیک و به روش‌های مختلف خارج از بانک اطلاعاتی نسبت به تهیه اطلاعات پشتیبان اقدام می‌نمایند.

هر چند که این روش می‌تواند منطبق با نیازمندی‌های بومی استفاده کنندگان از بانک اطلاعاتی باشد لیکن می‌تواند همراه با ریسک نادیده گرفتن برخی از نیازمندی‌ها و ضروریات باشد.

این روش نسبت به روش سیستمی وقت گیرتر بوده و زمان زیادی را نیاز دارد.

۵-۸-۳-کنترل صحت پشتیبان

اگر چنان‌چه پس از گرفتن پشتیبان اطلاعات پشتیبان گیری شده کنترل نگردیده و صحت برگشت پذیری آن بررسی نگردد ممکن است به علت اتفاقات ناخواسته در زمان نیاز به اطلاعات عملاً نتوان از آن استفاده نمود.

لذا تاکید می‌گردد بعد از هر مرتبه تهیه اطلاعات پشتیبان به روش مطمئنی از امکان برگشت پذیری اطلاعات اطمینان حاصل نمود.

۵-۸-۴-امنیت نگهداری اطلاعات پشتیبان

یکی از راه‌های دسترسی عناصر غیر مجاز به اطلاعات دسترسی به اطلاعات پشیبان می‌باشد. باید توجه داشت که تمام حساسیت‌های در نظر گرفته شده برای بانک‌های اطلاعاتی باید برای پشتیبان‌ها نیز در نظر گرفته شود.

یکی از خطاهای رایج برای حفظ و نگهداری اطلاعات پشتیبان در نگهداری آن‌ها در مجاورت اطلاعات اصلی می‌باشد.

در صورت وقوع مشکلات فیزیکی از قبیل سیل و آتش سوزی و سرقت برای اطلاعات اصلی ، به دلیل این که اطلاعات پشتیبان نیز در آن‌جا حفظ و نگهداری می‌شوند ممکن است این اطلاعات نیز همراه با اطلاعات اصلی از بین رفته و کلیه هزینه‌های انجام شده برای تهیه و حفظ و نگهداری اطلاعات پشتیبان بی ثمر گردند. لذا توصیه می‌گردد اطلاعات پشتیبان حتماً در محل امنی و خارج از محل بانک اطلاعاتی حفظ و نگهداری گردد.

۵-۸-۵-زمان بندی تهیه پشتیان

در برخی مواقع مشاهده گردیده است که در زمان تهیه اطلاعات پشتیبان برای اطلاعات اصلی اتفاق افتاده و هم‌زمان اطلاعات پشتیبان نیز غیر قابل استفاده شده‌اند.

پیش‌نهاد می‌گردد اطلاعات پشتیبان (بستگی به اهمیت و حساسیت اطلاعات) در دو یا سه زمان مختلف و به صورت مجزا تهیه گردد تا اگر با چنین اتفاقای مواجه شدیم بتوان از دیگر اطلاعات پشتیبان استفاده نمود.

۵-۹- سئوالات خودآزمایی

۱. بانک اطلاعاتی را تعریف نمایید.
۲. تهدیدات و فرصت‌ها در بانک‌های اطلاعاتی سنتی و دیجیتال چه اختلافاتی با یک‌دیگر دارند؟
۳. انواع رمز در بانک اطلاعاتی را نوشته و توضیح دهید.
۴. ثبت وقایع بانک اطلاعاتی چه نقشی می‌تواند در امنیت آن داشته باشد.
۵. اصطلاحات زیر را توضیح دهید.
   أ) ثبت وقایع اتفاقی
   ب) ثبت تغییرات در بانک اطلاعاتی
   ج) ثبت errors
   د) ثبت تهیه پشتیبان
۶. سیستم هایی که باید در ساختار فیزیکی دیتا سنتر مد نظر قرار گیرد را نام ببرید.
۷. در استاندارد TIA برای دیتاسنتر ترکیب بندی فضای سایت به چه شکلی باید باشد.
۸. محیط های عملیاتی کلیدی دیتاسنتر را نام برده و توضیح دهید.

۶

فصل ششم : امنیت اتوماسیون اداری

آن‌چه در این فصل می‌خوانید:

- **تعریف اتوماسیون اداری**
- **تاریخچه اتوماسیون اداری**
- **انواع اتوماسیون اداری**
- **انواع پایلوت اتوماسیون اداری**
- **امنیت اتوماسیون اداری**
- **مدل‌های کنترل دسترسی در اتوماسیون اداری**
- **ثبت اطلاعات و وقایع بهره‌برداری از اتوماسیون اداری**
- **نظارت امنیتی و کنترل بر اتوماسیون اداری**
- **انواع دسترسی به اتوماسیون اداری**
- **استراژی حاکم بر بهره‌برداری از اتوماسیون اداری**

۶- امنیت اتوماسیون اداری

۶-۱- تعریف اتوماسیون اداری

بسیاری از تکنولوژی‌های جدید بر پایه این جمله به وجود آمده‌اند "انسان فکر کند، ماشین کار کند". با وجود گذشت سال‌ها از پیاده سازی انواع سیستم‌های مکانیزه مالی و صنعتی در سازمان‌ها و موسسات اقتصادی، امور اداری و دفتری و گردش اسناد مالی اغلب این موسسات به طریقه سنتی انجام می‌گیرد. سرعت پایین، افزایش بوروکراسی، وابسته شدن سیستم به افراد و نیز عدم هماهنگی این روش با سیستم‌های مکانیزه سبب افزایش قابل ملاحظه خطاهای انسانی و کاهش بهره‌وری در سازمان‌ها شده است.

نتیجه اهداف، اندیشه‌ها و اقدامات انجام شده در هر سازمان به‌صورت اسناد و مدارک نگهداری می‌شود. این اسناد که با صرف وقت و هزینه‌های زیاد فراهم می‌آیند، حاوی اطلاعات و تجربیات گران‌بهایی می‌باشد که در دست‌یابی به اهداف سازمان نقش مهمی داشته و یکی از ابزارهای مهم مدیریت در تهیه برنامه‌ها و تصمیم گیری‌های استراتژیک محسوب می‌گردد.

حجم کارها و اهمیت اطلاعات در کلیه سازمان‌ها و شرکت‌ها با وجود استفاده از پرسنل متعدد شاهد رشدی روزافزون است. برنامه‌ریزی، سازمان‌دهی، کنترل و نظارت بر عمل‌کرد فعالیت‌های درون سازمانی یکی از مهم‌ترین معیارها و پیش نیازها در توسعه و کاربرد فن‌آوری اطلاعات در سازمان‌های امروزی محسوب می‌شوند. تحقیقات گروه (تحقیقات انجمن مدیریت جریان کار[۱] - ۲۰۰۶) نشان می‌دهد سازمان‌ها و شرکت‌های سنتی در محصولات و خدمات خود عملاً تنها از ۳۰٪ زمان فرآیندها ارزش افزوده دریافت می‌کنند و از ۷۰٪ زمان باقیمانده غیر از اتلاف وقت و هزینه چیزی عایدشان نمی‌شود. این آمار حتی در شرکت‌ها و بنگاه‌های اقتصادی موفق که گردش کاری سنتی را دنبال می‌کنند به‌صورتی واضح‌تر نمود پیدا می‌کند.

خودکارسازی اداری مجموعه‌ای از روش‌های کاری و نرم‌افزار و سخت‌افزار رایانه است که برای ذخیره و بازیابی و مبادله اسناد و اطلاعات اداری به کار می‌رود.

---

[۱] WFMC

۶-۲- تاریخچه اتوماسیون اداری

امروزه مدیریت برگردش کار و مکاتبات اداری و هم‌چنین مدیریت زمان در سازمان‌ها و موسسات اقتصادی به کلی متحول شده است و استفاده از روش‌های کند و مشکل ساز اداری غیرمکانیزه قابل قبول نمی‌باشد. حجم بالای اطلاعات و مکاتبات و دسترسی کُند، مسئولین و مدیران را که به مدیریت زمان در مجموعه تحت رهبری خود بها می‌دهند، به سوی اتوماسیون اداری در ابعاد مختلف رهنمون ساخته است.

اتوماسیون اداری، به‌ترین ابزار برای رسیدن به راه کارهای مفید در جهت صرفه جویی زمان و استفاده بهینه از وقت در سازمان می‌باشد. راه‌حل‌های مکانیزه به گردش مکاتبات سازمان سرعت بخشیده و هم‌چنین مدیریت بر گردش کارها را میسر می‌سازد. دراین فرآیند، حذف مکاتبات کاغذی، صرفه جویی و استفاده بهینه از زمان، عملی می‌گردد.

از زمانی که سیستم اداری متوجه گردید مشکلات فراوانی در رابطه با روش سنتی نگهداری و بازیابی و چرخش اطلاعات وجود دارد، تلاش نمود تا با روش‌های نوین نسبت به حل این مشکلات اقدام نماید. ذیلاً به رئوس این مشکلات اشاره می‌گردد:

- دسترسی کُند به مکتوبات و زمان‌بر بودن فرآیندهای اداری
- عدم اطلاع از سوابق و چرخه نامه در سازمان و نداشتن ابزاری مناسب برای پی‌گیری نامه‌های مدت دار
- عدم دسترسی به گزارشات و اطلاعات جامع از نامه‌ها و مراودات سازمان
- اجرا نشدن سلسله مراتب اداری و به طور کلی سیاست‌های اداری
- عدم دسترسی و امکان رسیدگی به اطلاعات و کارها از خارج سازمان
- عدم امکان پی‌گیری یک نامه و چرخه طی شده آن درهر لحظه
- نبود نظارت بر نظام اداری، گردش نامه و عمل‌کرد افراد
- کنترل سطح دسترسی کاربران به اطلاعات
- مشکلات بایگانی از لحاظ حجم و دسترسی کُند و محدودیت زمانی و موضوعی اطلاعات
- نگهداری و استفاده از دستگاه‌های متعدد فکس و مدوّن نبودن فکس‌های دریافتی
- مشکلات زمان‌بر بودن ارسال فکس‌های متعدد و مشخص نمودن زمان بندی ارسال
- نبودن یک محیط یک‌پارچه برای دسترسی به کل محتویات و اطلاعات مورد نظر شامل نامه‌ها، پیش‌نویس، فکس‌ها، نامه‌های الکترونیکی، کارهای ارجاعی، اطلاعات پروژه‌ها و...
- مشکلات نظام اداری غیر مکانیزه (مدیریت کارها) را به سمت خودکارسازی و اتوماسیون اداری حرکت کردند. توسعه علم و فن‌آوری رایانه‌ای به این امر کمک شایانی نمود.

۶-۳- انواع اتوماسیون اداری

اتوماسیون اداری با اهداف مختلفی در سازمان‌ها توسعه یافته‌اند که مهم‌ترین آن‌ها را می‌توان به شکل ذیل تقسیم بندی نمود:

- درگاه سازمانی
- کارتابل پرسنل
- تقویم و برنامه ریزی روزانه
- سیستم روابط عمومی
- بایگانی و آرشیو اسناد
- موتور جست‌جوی اسناد تحت وب
- مدیریت فرآیندهای کسب و کار
- موتور گردش کار
- طـراح گردش کار
- مدیریت صورت‌جلسات
- مدیریت دبیرخانه
- ارجاع الکترونیکی
- کتابخانه الکترونیک
- سیستم کنترل رفت و آمد اشخاص
- پردازش تصویر - تشخیص حرکت توسط دوربین مدار بسته
- تلفن گویا
- اطلاع رسانی گویا
- داشبوردهای دیجیتال مدیریت استراتژیک سازمان
- مدیریت ارسال و دریافت پیام کوتاه
- مدیریت ارسال و دریافت پیام چند رسانه‌ای
- مدیریت ارسال و دریافت فکس
- مدیریت ارسال و دریافت ایمیل
- دفترچه یادداشت روزانه
- گفت‌وگو و تبادل پیغام
- مدیریت زمان‌بندی گزارش‌ها
- مدیریت و امنیت ۶ لایه

- گزارش ساز پویا
- تحلیل داده‌ها در کسب و کار هوشمند
- فرم ساز پویا
- دسترسی از راه دور به سیستم - تحت وب

برای دسترسی به این اهداف سازمان‌ها به یکی از سه طریق زیر نسبت به خودکارسازی اهداف اداری خود اقدام می‌نمایند:

۶-۳-۱- مستقل درون سازمانی

در این روش سازمان‌ها با استفاده از شبکه‌های مستقل رایانه‌ای خود اتوماسیون اداری را پیاده سازی می‌نمایند. چنان‌چه محدوده سازمانی این اقدام از شبکه داخلی سازمان فراتر نرفته و به شبکه‌های مخابراتی متصل نگردند می‌توان حداقل خطرات را بر آن مترتب دید و این به شرطی می‌باشد که علاوه بر نرم‌افزار و سخت‌افزار استفاده شده در شبکه با طراحی حفاظتی مسائل امنیتی کاربران و اطلاعات را نیز در نظر گرفته و برای آن راه حلی ارائه نمود. البته در این روش با توجه به عدم استفاده از ارتباطات در گسترش اتوماسیون اداری برخی از اهداف پوشیده نخواهد شد.

۶-۳-۲-ترکیبی درون سازمانی – MIS

در این روش سازمان‌های بزرگ تلاش دارند تا با استفاده از شبکه‌های مخابراتی ارتباط بین شبکه‌های مختلف درون سازمانی را با یک‌دیگر برقرار نموده و تمام سازمان را درگیر با سیستم اتوماسیون اداری نمایند. در این روش در صورت نزدیک بودن سازمان‌ها به یک‌دیگر اصلح استفاده از امکانات ارتباطی درون سازمانی که مستمراً بر آن نظارت می‌گردد می‌باشد و استفاده از سیستم‌های ارتباطی مخابراتی باعث اتصال شبکه‌های اتوماسیون اداری به سیستم مخابراتی بین‌المللی را فراهم نموده و از هر نقطه دنیا امکان تهدید اطلاعات انباشته شده در اتوماسیون اداری که به صورت MIS به هم پیوسته شده است فراهم می‌گردد. نباید این نکته را فراموش نمود که در صورت دسترسی دشمن به اطلاعات از روش پنهان و آماده به‌کار، وی تلاش خواهد داشت این ارتباط را هرچه بیش‌تر پنهان نگهدارد تا امکان هرچه بیش‌تر استفاده سو را برای خود مهیا سازد.

۶-۳-۳- ترکیبی برون سازمانی – CBIS

در این روش سازمان‌های مختلف در گیر اداری با یک‌دیگر چاره‌ای به جزء استفاده از ارتباطات مخابراتی برای ارتباط با یک‌دیگر را ندارند. معمولاً برای یک ساختار بزرگ اداری ایجاد

بستر ارتباطی موازی با سیستم مخابراتی کشور برای این کار مقرون به صرفه نخواهد بود و به همین خاطر میل سازمان‌ها در استفاده از شبکه‌های مخابراتی برای کاهش در هزینه‌ها می‌باشد. چنان‌چه در این روش ارتباطی از سیستم‌های مخابراتی بومی کشور که مرتبط با شبکه‌های بین‌المللی نمی‌باشند استفاده گردد خطرات کم‌تری اطلاعات آن سازمان‌ها را تهدید می‌کند. در صورت استفاده از سیستم‌های ارتباطی متصل به شبکه‌های مخابراتی بین‌المللی به راحتی افراد غیر مجاز خواهند توانست تا با اشرافیت بر ارتباطات به قلب سازمان‌ها که همان مراکز اسناد می‌باشند به راحتی نفوذ نموده و در مبدا تولید اطلاعات نسخه‌ای از آن را به‌دست آورند.

۶-۴- انواع پایلوت اتوماسیون اداری

همان گونه که گفته شد سازمان‌ها برای ایجاد ارتباط بین موجودیت‌های مختلف اتوماسیون اداری از سیستم‌های ارتباطی مختلفی استفاده می‌نمایند که می‌توان از آن‌ها به عنوان پایلوت و بستر ارتباطی نام برد.

۶-۴-۱- شبکه‌های سازمانی

ممکن است این بسترهای ارتباطی شبکه‌های مستقل درون سازمانی باشند. چنان‌چه این شبکه‌ها توسط طراحان بومی و با استفاده از تکنولوژی بومی طراحی شده و ارتباط آن‌ها با خارج از شبکه مسدود شده و عدم ارتباط استمرار سازمانی داشته و با تغییر در مدیریت‌ها این استراتژی حفظ گردد کم‌ترین خطرات متوجه اطلاعات سازمانی که در این بستر در حال حرکت می‌باشد متوجه خواهد شد.

۶-۴-۲- اینترنت

برخی از سازمان‌ها به علت مباحث اقتصادی یا تحت تاثیر تبلیغات نظام سلطه که همیشه اینترنت را به عنوان یک بستر مناسب و ارزان مخابراتی تبلیغ می‌نماید قرار گرفته و بدون این که متوجه خطرات بزرگ این مسئله باشند نسبت به این کار اقدام می‌نمایند و عملاً با بودجه و امکانات و هزینه خود امکان استفاده غیر مجاز دیگران از اطلاعات تولید شده را فراهم می‌سازند. با توجه به این که این دسترسی تا زمان استفاده از این پایلوت استمرار خواهد داشت می‌توان چنین نتیجه گیری نمود که نام سلطه با تبلیغات وسیع خود مدیران را تشویق به این کار خواهد نمود تا بتواند هرچه بیش‌تر با اشرافیت اطلاعاتی بر اینترنت به اطلاعات مورد نظر دسترسی داشته باشد.

۶-۵- امنیت اتوماسیون اداری

امنیت اتوماسیون اداری را نمی‌توان امری بسیط فرض نمود که صرفاً با تامین امنیت وارداتی بر روی شبکه و یا سخت‌افزار به آن دست یافت. امنیت سیستم‌های اتوماسیون اداری مسئله مرکبی است که عوامل بسیاری بر آن دخالت دارند.

۶-۵-۱- امنیت اتوماسیون اداری در مرحله طراحی

مرحله طراحی اولین مرحله شروع یک اتوماسیون اداری می‌باشد. در این مرحله سازمان کل اقداماتی را که انجام می‌دهد و انواع اطلاعاتی را که تولید می‌کند و افرادی را که اطلاعات تولید می‌کنند را به ریزه کاری‌های مربوطه به طراح سیستم معرفی می‌نماید.

۶-۵-۲- امنیت اتوماسیون اداری در مرحله برنامه نویسی

در مرحله برنامه نویسی بر مبنای طراحی انجام گرفته شده نرم‌افزار نویسان روش‌ها را تبدیل به برنامه نموده و ارتباط بین ساختارها را با کدهای برنامه نویسی تنظیم می‌نمایند.

۶-۵-۳- امنیت اتوماسیون اداری در مرحله بهره‌برداری

در مرحله بهره‌برداری کاربران مجاز به بهره‌برداری از اتوماسیون اداری صرفاً در چهارچوب برنامه نوشته شده قادر خواهند بود و خارج از آن هیچ اقدامی را نمی‌توانند انجام دهند و هرگونه درخواست تغییر می‌بایست مجدد طراحی و پیاده سازی گردد.

۶-۵-۴- امنیت اتوماسیون اداری در مرحله انتقال اطلاعات

در این مرحله کلیه اطلاعات تولید شده از طریق سیستم‌های ارتباطی که اجزا مختلف اتوماسیون اداری را به هم متصل می‌نماید صورت می‌پذیرد و عملاً هیچ اطلاعاتی خارج از این روش‌های ارتباطی نمی‌توانند مبادله گردند.

۶-۶- مدل‌های کنترل دسترسی در اتوماسیون اداری

برای کنترل دسترسی در اتوماسیون اداری مدل‌های مختلفی ارائه شده است. لیکن باید در استفاده از مدل، موارد ذیل را مد نظر قرار داد:

- بایستی مدلی ارائه شود تا تعیین گردد که چه دسترسی‌هایی مجاز و چه دسترسی‌هایی غیر مجاز است.

- پایگاه‌های داده با توجه به متمرکزسازی داده‌ها در آن بیش‌تر مورد توجه قرار می‌گیرند.
- مدل کنترل دسترسی نقش- مبنا به عنوان یک مدل کنترل دسترسی بسیار مرسوم و پرکاربرد مطرح است.

۶-۷- ثبت اطلاعات و وقایع بهره‌برداری از اتوماسیون اداری

دسترسی به اطلاعات در سیستم اتوماسیون اداری در زمان‌های مختلف و توسط کاربران مختلف و با استفاده از ابزار مختلف و برای بهره‌برداری‌های مختلف صورت پذیرفته و اقدامات مختلفی بر روی آن انجام می‌پذیرد. درصورت ثبت شدن این وقایع می‌توان با بررسی آن‌ها تحلیل جامعی در رابطه با اعتبار و روایی کار انجام شده ارائه نمود و اگر کلیه وقایع مرتبط با اتوماسیون اداری و دسترسی‌های مجاز و تلاش به منظور دسترسی غیر مجاز ثبت نگردند عملاً نمی‌توان هیچ کنترلی بر روند استفاده از این سیستم داشت. لذا سازمان‌های استفاده کننده می‌بایست با طراحی دقیق و مشخص نمودن مسئول انجام این کار، وقایع را ثبت و بهره‌برداری نمایند.

۶-۸- نظارت امنیتی و کنترل بر اتوماسیون اداری

با توجه به این که در اتوماسیون اداری کلیه اطلاعات مهم سازمان تجمیع شده و مسیر حرکت اطلاعات و نوع بهره‌برداری از آن و شیوه استفاده و قیمت آن برای سازمان در این سیستم متمرکز می‌گردد برای سازمان از اهمیت وافری برخوردار می‌باشد لذا می‌بایست به‌صورت دائم توسط ساختار مشخص شده‌ای در سازمان که در قبال اختیار داده شده دارای مسئولیت پاسخ‌گویی باشد نظارت و شیوه‌های دسترسی و بهره‌برداری از آن مورد دقت قرار گیرد.

۶-۹- انواع دسترسی به اتوماسیون اداری

برای استفاده از اتوماسیون اداری نیاز به دسترسی به اجزا اتوماسیون اداری می‌باشد که این دسترسی معمولاً به دو روش می‌تواند انجام شود:

۶-۹-۱- دسترسی مجاز

در این روش دسترسی، توسط مدیر یا مدیران اتوماسیون اداری سطح دسترسی مورد نیاز هر فرد مشخص شده و بنابر وظیفه اداری و نیاز سازمانی و حیطه دسترسی کاربر مربوطه، سطح

دسترسی وی تعریف شده و کاربر در حیطه تعریف شده مجاز به دسترسی به سیستم و استفاده از آن می‌باشد. کاربران قادر خواهند بود صرفاً در حیطه‌ای که برای آنان مشخص شده است حرکت نمایند و اختیار تولید اطلاعات و اعمال تغییرات در محدوده‌ای که برای آنان مشخص شده است را دارا می‌باشند و خارج از آن نمی‌توانند اقدامی انجام دهند. کلیه اقدامات انجام شده توسط کاربران مجاز ثبت شده و در قبال آن به لحاظ حقوقی پاسخ‌گو می‌باشند و با توجه به عدم انکارپذیری که در سیستم تعبیه شده است موظف به پاسخ‌گویی در قبال اقدامات انجام شده می‌باشند.

۶-۹-۲- دسترسی غیر مجاز

در دسترسی غیر مجاز کابران به صورت غیر مجاز و خارج از چهارچوب تعیین شده امکان دسترسی به سیستم را برای خود مهیا می‌سازند. در این نوع دسترسی که یا به‌وسیله کاربران کنجکاو برای ارضا حس کنجکاوی انجام شده یا این که توسط عوامل غیر مجاز برای اشرافیت بر اطلاعات تولید شده و دسترسی غیر مجاز به اطلاعات و بهره‌برداری سو از اطلاعات انجام می‌شود. در بسیاری از مواقع افراد غیر مجاز اولین اقدام خود را با استفاده از ضعف در مدیریت سیستم سو استفاده نموده و برای خود ایجاد نموده و به مرور نسبت به گسترش سطح دسترسی اقدام می‌نمایند. مهم‌ترین مطلب برای این گونه افراد عدم متوجه شدن مدیر سیستم یا سیستم کنترل کننده شیوه‌های دسترسی می‌باشد و تلاش دارند خود را به عنوان کاربر مجاز به سیستم معرفی نمایند تا در کنترل‌ها کم‌ترین مشکوکیت را ایجاد نموده و به این کار خود ادامه دهند.

نوع دیگر این سوء استفاده کنندگان تولید کنندگان غیر بومی سخت‌افزار و نرم‌افزارهای استفاده شده در سیستم اتوماسیون اداری می‌باشد که با اهداف سلطه جویانه از ابتدای تولید این ابزار راه‌های نفوذی را تحت عنوان درپشتی[1] یا نکات مدیریتی پنهان بر روی این سخت‌افزار و نرم‌افزار قرار داده‌اند تا ضمن هم‌خوانی با اقدامات آن‌ها و به مجرد استفاده در هر سیستمی خود را با آن هماهنگ نموده و نسبت به ارسال اطلاعات مد نظر و یا مدیریت پنهان بر سیستم استفاده نمایند این همان نیمه پنهان استفاده از ابزار غیر بومی و ناشناخته در مهم‌ترین قسمت‌های سازمان که همان مراکز اسناد و مراکز تولید اطلاعات هستند می‌باشد.

۶-۱۰- استراژی حاکم بر بهره‌برداری از اتوماسیون اداری

[1] backdoor

برای بهره‌برداری از سیستم‌های اتوماسیون اداری می‌توان در لایه‌های مختلف استراتژی‌های مختلفی‌ترسیم نمود. سمت و سوی امنیتی حاکم بر سیستم‌ها را استراتژی از قبل مشخص شده بیان می‌نماید.

۶-۱۰-۱- استراتژی درون سازمانی

برخی از این استراتژی‌ها درون سازمانی می‌باشند. اگر چنان‌چه استراتژی سازمان صرفاً انجام امور اداری با سرعت هر چه تمام‌تر بدون در نظر گرفتن دیگر مسائل همچون امنیت باشد نتیجه آن کسب سرعت بدون امنیت خواهد بود. نتیجه آن با سرعت هر چه بیش‌تر تولید اطلاعات و در اختیار دیگران قرار دادن خواهد بود. لذا در طراحی‌ها استراتژیک می‌بایست چند منظوره و از جوانب مختلف به سیاست گذاری نگاه نمود.

۶-۱۰-۲- استراتژی حاکمیتی

برخی از استراتژی‌ها حاکمیتی می‌باشند که در قوانین موضوعه کشورها یا برنامه‌های کوتاه مدت یک ساله یا برنامه‌های میان مدت ۵ ساله یا برنامه‌های بلند مدت بیست ساله کشورها به آن اشاره می‌شود. اگر چنان‌چه در طراحی و استفاده از سیستم‌های اتوماسیون اداری به این نکات توجه گردد معمولاً خطر کم‌تری سازمان را تهدید می‌نماید لیکن مشکل در بسیار از مواقع نادیده گرفتن این قوانین کلی تحت نام مصلحت‌اندیشی سازمانی یا ضعف در مدیریت سازمانی می‌باشد.

۶-۱۱- خلاهای امنیتی در اتوماسیون اداری

با توجه به مطالبی که در رابطه با مراحل تولید سیستم اتوماسیون اداری مطرح گردید در هر مرحله می‌تواند خطراتی اطلاعات سازمان را تهدید نماید.

۶-۱۱-۱- ضعف در طراحی

چنان‌چه طراحی توسط افراد غیر بومی صورت بگیرد عملاً کلیه اطلاعات سازمان همراه با ریزه کاری‌های مربوطه در اختیار افراد غیر مجاز قرار گرفته و هیچ‌گونه امکان تغییر در آن میسر نخواهد بود زیرا طراحی بر مبنای اطلاعات مکتسبه صورت پذیرفته و سازمان بر روی این که عمل‌کرد باید در اتوماسیون اداری انجام پذیرد به نتیجه رسیده است. معمولاً در مرحله طراحی اطلاعات پیش نیاز تولید شده به خارج از سازمان منتقل شده و در خارج از سازمان مورد بررسی و تجزیه و تحلیل و پردازش قرار می‌گیرد. این اطلاعات بر روی ابزار ذخیره سازی قرار می‌گیرند که در کنترل سازمان نمی‌باشد و در مراحل طراحی و اتمام طراحی سازمان اصلی بر روی آن‌ها

اشرافیت نداشته و ممکن است به روش‌های ناخواسته تکثیر و مورد بهره‌برداری سو قرار گیرند. حتی اگر پیمانکار معتقد به حفظ و نگهداری اطلاعات نیز باشد پس گذشت مدتی از طراحی و تولید نرم‌افزار اتوماسیون اداری اطلاعات مربوطه حساسیت خود را از دست داده و با اطلاعات جدید جای‌گزین می‌شوند.

ابزار ذخیره ساز قدیمی شده و از سیستم اداری خارج و همین مسئله می‌تواند به عنوان یکی از گلوگاه‌های مورد علاقه افراد غیر مجاز برای به‌دست آوردن اطلاعات سازمانی که آن‌ها را به درون راه نمی‌دادند قرار گیرد.

۶-۱۱-۲- ضعف در برنامه نویسی

برنامه نویسی گسترده‌ای مانند برنامه نویسی اتوماسیون اداری از تیم‌های مختلفی برای برنامه نویسی استفاده می‌کنند. برنامه نویس اصلی برنامه را به قسمت‌های کوچک‌تری تقسیم نموده و هر ماژول را به یک برنامه نویس سفارش می‌دهد. برنامه نویسان معمولاً در ابزار ذخیره ساز خود شروع به برنامه نویسی می‌نمایند. با داشتن کدهای برنامه نویسی افراد غیر مجاز قادر خواهند بود به مجرد دسترسی فیزیکی به برنامه‌های اتوماسیون اداری آن‌ها را با کدهای تقلبی برنامه نویسی تعویض نموده و برای جریان اطلاعات مسیرهای جدیدی را ایجاد نمایند که به صورت آشکار اطلاعات تولید شده را به کاربر اصلی ارسال و به صورت پنهان یک نسخه از اطلاعات را به مسیر پنهان مشخص شده ارسال می‌نماید.

کدهای برنامه نویسی بر روی ابزار ذخیره ساز مختلف و خارج از کنترل سازمان متقاضی اتوماسیون اداری قرار گرفته و سوء استفاده کنندگان غیر مجاز به خوبی راه قرار گرفتن در مسیر برنامه نویسی و جا زدن خود به عنوان برنامه نویس حرفه‌ای را یاد گرفته‌اند.

۶-۱۱-۳- ضعف در اعتبارسنجی کاربران

شیوه اعتبار سنجی کاربران نشان دهنده شیوه دسترسی آن‌ها به اطلاعات تولید شده یا توان دسترسی آن‌ها به اطلاعات می‌باشد. چنان‌چه در این مرحله توابع مربوطه به صورت غیر کنترل شده مورد استفاده قرار گیرد این امکان را ایجاد می‌نماید تا بتوان هر کاربر مجازی مد نظر را با هر دسترسی که بعداً نیاز است به سیستم معرفی نموده و آن‌ها را از شیوه کنترل جاری سیستم خارج نگه داشت.

۶-۱۲- تهدیدات و فرصت‌های امنیت شبکه در امنیت اتوماسیون اداری

نرم‌افزارهای اتوماسیون اداری دارای فرصت‌ها و تهدیدات بی‌شماری می‌باشند. با توجه به این که در ابتدای فصل به فرصت‌های آن اشاره گردید در این قسمت به برخی از تهدیدات آن اشاره می‌گردد.

۶-۱۲-۱- آسیب‌پذیری استفاده از اتوماسیون اداری در بسته

برای مراکز مهّم و حیاتی استفاده از این گونه نرم‌افزارها (هرچند تولید داخل کشور باشد) توصیه نمی‌شود و پیش‌نهاد می‌گردد با فرض تولید داخل بودن یک‌بار به صورت کامل با مهندسی مجدد کد خوانی شده و پس از تایید مورد بهره‌برداری قرار گیرد و به هیچ وجه نباید در مقابل شرکت‌های که اجازه دسترسی به منبع نرم‌افزاری را به مصرف کننده نمی‌دهند در این گونه مواقع کوتاه آمد.

۶-۱۲-۱-۱- اتوماسیون‌های اداری تولید داخل کشور

نرم‌افزارهای اتوماسیون اداری تولید داخل کشور به دو نوع می‌باشد. در نوع اول نرم‌افزار مربوطه توسط طراحان بومی داخل کشور طراحی شده و سپس نرم‌افزار نویسان داخل کشور با استفاده از تجربیات خود آن‌ها را تبدیل به کدهای نرم‌افزاری نموده و با توجه به نیازهای داخل کشور تولید شده و در اختیار مصرف کنندگان قرار می‌گیرد. این‌گونه نرم‌افزارهای نوشته شده درصدی از مشکلات امنیتی را نداشته و نسبت به دیگر انواع از مشکلات کم‌تری برخوردار می‌باشند.

۶-۱۲-۱-۲- اتوماسیون‌های اداری تولید خارج از کشور

این‌گونه نرم‌افزارها توسط دیگر کشورها با اهداف اقتصادی و بسیاری اوقات با داشتن پشت پرده اطلاعاتی نوشته شده و بیش‌تر با هدف اشرافیت اطلاعاتی بر اطلاعات تولید شده توسط دیگر کشورها با پوشش‌های علمی و اقتصادی و شرکتی به کشورهای مد نظر ارسال می‌گردد. این گونه نرم‌افزارها را شاید بتوان با قیمت کم‌تر خریداری یا به‌دست آورد لیکن این نکته را باید مدنظر داشت که نرم‌افزارهای آماده خریداری شده از خارج از کشور را نمی‌توان حتی با بررسی‌های مو شکافانه فنی بررسی کامل نموده و اختیار اطلاعات سازمان را به دست آن داد. این نرم‌افزارها معمولاً حلقه مفقوده طرح‌های اشرافیتی نظام سلطه مانند طرح اشلون را تکمیل می‌نمایند.

۶-۱۳- کنترل‌های در مسیر طراحی و برنامه نویسی اتوماسیون اداری

اگر چنان‌چه در سازمان اجازه شروع و اتمام طراحی و نوشتن نرم‌افزار اتوماسیون را به فرد و یا گروه یا شرکتی داده و انتظار این را داشت که در انتهای آماده سازی می‌توان آن را تست و کنترل امنیتی نمود، معمولاً این کار امکان‌پذیر نمی‌باشد و در صورت امکان پذیر بودن توان و زمان لازم برای این کار وجود نخواهد داشت چون همیشه با فشار سازمان برای شروع کار روبرو خواهیم بود. پیش‌نهاد می‌گردد تیم کنترل کننده هم زمان با تیم طراحی و برنامه نویسی کار خود را شروع نموده و حتی یک قدم از آنان جلوتر حرکت نماید تا از موضع انفعالی خارج شده و با موضع بالاتری نسبت به این کار اقدام نماید.

۶-۱۴- تأثیر اتوماسیون اداری در تغییر حساسیت‌های امنیتی سازمان

یکی از آثار طبیعی استفاده از اتوماسیون اداری در یک سازمان چرخش کار از فضای سنتی به سمت دیجیتال می‌باشد و با توجه به فرآیندهای تعریف شده در سیستم برخی از فرآیندهای اداری دچار تحول می‌گردند. هر چند که بسیاری از تحولات ممکن است به نفع سازمان باشد لیکن در بررسی تحولات انجام شده می‌بایست نکات امنیتی مد نظر را مورد توجه قرار داد و با بصیرت و چشم باز آن‌ها را شناسایی کرده و پس از اشرافیت کامل بر محاسن آن و ممانعت از ایجاد تهدیدات جدید آن را قبول نمود.

۶-۱۵- سئوالات خودآزمایی

۱. تعریف اتوماسیون اداری را از دیدگاه امنیتی بنویسید.
۲. انواع اتوماسیون اداری را نوشته و توضیح دهید.
۳. مراحل ایمن سازی اتوماسیون اداری را نام ببرید.
۴. امنیت اتوماسیون اداری در مرحله بهره‌برداری را توضیح دهید.
۵. انواع مدل‌های کنترل دسترسی در اتوماسیون اداری را نوشته و توضیح دهید.
۶. انواع دسترسی به اتوماسیون اداری را نوشته و توضیح دهید.
۷. استراتژی‌های امنیتی حاکم در بهره‌برداری از اتوماسیون اداری را توضیح دهید.
۸. انواع خلأهای امنیتی در اتوماسیون اداری را نام ببرید.
۹. ارتباط تهدیدات و فرصت‌های امنیت شبکه با اتوماسیون اداری را توضیح دهید.
۱۰. نقش لایه‌های مختلف را در امنیت اتوماسیون اداری بنویسید.

فصل هفتم : امنیت اینترنت

آن چه در این فصل می‌خوانید:

- **تعریف اینترنت**
- **تاریخچه اینترنت**
- **استراتژی نظام سلطه در طراحی اینترنت**
- **ساختار و پیکربندی کاربردی اینترنت**
- **نیمه پنهان ساختاری اینترنت از دیدگاه نظام سلطه**
- **جنگ اینترنتی**
- **اینترنت به عنوان اصلی‌ترین روش بر اشرافیت بر اطلاعات**
- **همکاری و هماهنگی بین سه عنصر اینترنت اشلون و فن‌آوری‌های هوشمند**
- **اطلاعات تبادلی از طریق اینترنت**

۷- اینترنت و نظام سلطه

۷-۱- مفهوم اطلاعات

امروز برای اطلاعات مفاهیم و معانی مختلف در نظر گرفته اند. برخی آن را یک فرآیند نامیده و برخی آن را یک محصول می‌دانند. برخی نیز این اعتقاد را دارند که اطلاعات فرآیندی است که به محصول منتج می‌شود.

وزارت دفاع آمریکا اطلاعات را چنین تعریف می‌کند "محصول جمع آوری، پردازش، یک‌پارچه سازی، تحلیل، ارزش‌یابی و تفسیر داده‌ای موجود راجع به کشورها و یا منطق خارجی"

گادسون اطلاعات را چنین تعریف می‌کند " تلاش از سوی دولت یا یک فرد یا نهاد خصوصی به منظور جمع آوری، تحلیل، تولید، توزیع و استفاده از داده‌های که به یک دولت، گروه سیاسی، حزب، نیروی نظامی، جنبش یا جمعیت دیگر مربوط است و به نظر می‌رسد با امنیت آن دولت یا فرد یا نهاد مربوط است. "

با ملاحظه این تعاریف یک ویژگی منحصر به فرد اطلاعات، جمع آوری مخفیانه رازهای دیگران است تا وقتی این رازداری حفظ شود کشور می‌تواند با دست‌یابی به این اطلاعات تهدید را کاهش داده و یا حتی ان را خنثی نماید.

امروزه تمام کشورها برای ادامه حیات خود نیاز به دسترسی به اطلاعات می‌باشند و در راه این دسترسی امکانات مختلفی را برای خود مهیا می‌سازند.

اطلاعات برای آگاهی رسانی به سیاست‌گذاران کشور راجع به شرایط کنونی، روندها، توانمندی‌ها و مقاصد دیگران طراحی می‌شود. اطلاعات ابهام را به طور ذاتی کاهش می‌دهد.

هنری کیسنجر، وزیر امر خارجه اسبق ایالات متحده امریکا، در نطق پیش از دستور در مورد مقررات نظارت در کمیته سنا در امور عملیات دولتی نیاز به اطلاعات را چنین می‌گوید : "سیاست خارجی ما باید با مشکلات پیچیده‌ای مقابله کند که بر زندگی صدها میلیون نفر تأثیر گذارد. در رویارویی با این چالش‌های بزرگ، اهداف ما باید با توجه به رشد یک جهان دارای نظم

منطقی تنظیم گردد. ما باید بر تسلیحاتی تمرکز کنیم که می‌توانند منابع ما را در جهت رسیده به اهدافی که در آینده این مملکت نقش بسزایی دارد. اطلاعات ابزاری ضروری در دست‌یابی به این هدف محسوب می‌گردد. "

در این سخنرانی به مسایل ذیل اشاره شده است:

- نیاز به اطلاعات برای بقا آمریکا یک اصل اساسی است.
- سهم بزرگی از این اطلاعات می‌بایست از منابع خارجی تامین گردد.
- باید برای این دسترسی به اطلاعات جهانی نظم منطقی را در جهان حکم فرما نمود.
- اهداف جمع آوری اطلاعات جهانی باید باشد.
- دسترسی به اطلاعات به عنوان یک ابزار تسلیحاتی قلمداد می‌شود.
- دسترسی به اطلاعات یک هدف برای آمریکا می‌باشد.

جرالد فورد در اظهارات مشابهی نظرات خود را چنین ارایه می‌نماید:" تا وقتی که تضاد و برتری خواهی در جهان وجود دارد، توانمندی‌های اطلاعاتی ما باید در جهان نظیر نداشته باشد. ناکارآمدی سرویس‌های اطلاعات خارجی، خطر درگیر شدن ما در تضادهای مستقیم و مسلحانه را افزایش می‌دهد. بدون توانمندی کار آمد اطلاعاتی، ما لنگ و چشم و گوش بسته‌ایم "

ملاحظه می‌گردد در این اظهارات مجددا بر مسایل زیر تاکید می‌گردد:

- امریکا نیازمند به توانمندی اطلاعاتی بی نظیر است.
- بدون توانمندی اطلاعاتی امریکا ناتوان است.
- سرویس‌های خارجی امریکا به دنبال توانمندی اطلاعاتی با تعریف جدید می‌باشند.

امروزه زمینه‌های جمع آوری اطلاعات بر اساس منابع مختلف اطلاعات به صورت زیر تقسیم بندی شده است:

- اطلاعات انسانی
- اطلاعات آشکار
- اطلاعات علایم
- اطلاعات اندازه گیری و علایم
- اطلاعات تصویر نگاری
- .....

با توجه به بررسی نقطه نظرات سیاستمداران امریکایی این نکته قابل درک است که ادامه حیات کشوری مانند امریکا بدون دسترسی به اطلاعات عملاً غیرممکن یا خیلی مشکل خواهد بود و به همین خاطر درگیر جنگ بودن این کشور برای دست‌یابی به اطلاعات و سرمایه گذاری کلان برای به دست گرفتن کنترل چرخه تولید و دسترسی به اطلاعات تمام دنیا برای این کشور و اقمار آن قابل توجیه خواهد بود. در گذشته کشورهای مختلف برای به دست آوردن نیازمندی‌های استراتژیک خود با در دست گرفتن سلاح‌های آتشین دست به کار شده و دیگران را تحت سلطه خود می‌آوردند لیکن امروزه تسلیحات با آن چیزی که در گذشته بوده است کاملاً متفاوت است. امروزه شاهد سیستم‌های تسلیحاتی و سایر فنون تهاجمی برای به دست آوردن اطلاعات می‌باشیم. تسلیحات امروز از نظر کیفیت بسیار متفاوت با گذشته می‌باشد. به عبارت دیگر امروزه زورمندان نیازمند به روش‌های جمع آوری اطلاعات می‌باشند.

در قرن حاضر با توجه به این‌که مهم‌ترین کالا برای تمام کشورها کالایی به نام اطلاعات می‌باشد تمام کشورها در تلاش برای این هستند که به این کالای گران قیمت دسترسی پیدا نموده و آن را در انحصار خود درآورند. انحصاری سازی اطلاعات همیشه باعث این خواهد شد تا نیازمندان به آن همیشه به دنبال رفع نیازمندی خود باشند و به این ترتیب روش نوینی از تسلط و سلطه سازی در دنیا شکل می‌گیرد. برای ادامه این تسلط و برای این‌که بتوان به اطلاعات به شکل‌های مختلف دسترسی پیدا نموده و گلوگاه اصلی این کالا را به صورت انحصاری به دست گرفت نیاز به ابزار مختلفی وجود دارد و رایج‌ترین این ابزار نیاز به دسترسی به اطلاعات در لحظه تولید در مبداء بوده و به مجرد تولید اطلاعات بتوان آن را به دست آورد و مهم‌تر از آن این که بتوان تولید کنندگان اطلاعات را به روش‌های مختلف به سمتی هدایت کرد که اطلاعات خاص و مورد نیاز را تولید کنند و احساس کنند که این اطلاعات را برای خود تولید می‌کنند تا با انگیزش هر چه بیشتر در این جهت حرکت کنند.

۷-۲- تاریخچه پیدایش اینترنت:

به صورت کلی بسیاری از مورخین تاریخچه پیدایش اینترنت را به شکل زیر ثبت نموده‌اند:

پیدایش اینترنت به دهه ۱۹۶۰ بر می‌گردد زمانی که دولت ایالات متحده براساس طرحی موسوم به ‘‘Arpa’’ مخفف " آژانس تحقیق پروژه‌های پیش‌رفته" که در آن زمان برای کارکردهای دفاعی به‌وجود آمده بود، این طرح را اجرا نمود. طرح این بود که رایانه‌های موجود در شهرهای مختلف (در آن زمان چیزی بنام رایانه شخصی وجود نداشت بلکه سازمان‌های

بزرگ و دانشگاه‌ها و مراکز دولتی معمولاً دارای سیستم‌های رایانه بزرگ[۱] بودند) و هر کدام اطلاعات خاص خود را در آن ذخیره می‌کردند، بتوانند در صورت نیاز با یک‌دیگر اتصال بر قرار نموده و اطلاعات را به یک‌دیگر منتقل کرده و یا در صورت ایجاد بستر مناسب اطلاعات را در حالت اشتراک قرار دهند. در همان دوران سیستم‌هایی به‌وجود آمده بود که امکان ارتباط بین رایانه‌های یک سازمان را از طریق مختص همان سازمان فراهم می‌نمودند طوریکه رایانه‌های موجود در بخش‌ها یا طبقات مختلف با یک‌دیگر تبادل اطلاعات نموده و امکان ارسال نامه بین بخش‌های مختلف سازمان را فراهم می‌کردند اکنون به این سیستم ارسال نامه پست الکترونیک می‌گویند. اما برای اتصال و ارتباط دادن این شبکه‌های کوچک و پراکنده که هر کدام به روش و استانداردهای خودشان کار می‌کردند استانداردهای جدید و مشخصی که همان پروتکل‌ها هستند توسط کارشناسان وضع شد. سرانجام درسال ۱۹۶۱ تعداد ۴ رایانه در ۲ ایالت مختلف باموفقیت ارتباط بر قرار کردند و با اضافه شدن واژه نت به طرح اولیه نام آرپانت[۲] برای آن منظور شد. در دهه ۱۹۷۰ با تعریف پروتکل‌های جدیدتر از جمله "TCP" که تا به امروز رواج دارد و نیز مشارکت رایانه‌های میزبان بیش‌تر به آرپانت وحتی گسترده شدن آن به برخی نواحی فراتر از مرزهای ایالات متحده، آرپانت شهرت بیش‌تری یافت وایده اینترنت همراه با جزییات بیش‌تر راجع به شبکه‌های رایانه‌ای مطرح گشت تا این‌که طی سال‌های پایانی دهه ۱۹۷۰ شبکه‌های مختلف تصمیم گرفتند به صورت شبکه‌ای با یک‌دیگر ارتباط بر قرار نمایند و آرپانت را به‌عنوان هسته اصلی انتخاب کردند. بعدها در سال ۱۹۹۳ نام اینترنت روی این شبکه بزرگ گذاشته شد. وب[۳] که مخفف "تار جهان گستر"[۴] می‌باشد توسط آزمایشگاه اروپایی فیزیک ذرات Cern بخاطر نیاز آن‌ها به دسترسی مرتب و آسان به اطلاعات موجود روی اینترنت ابداع گشت. در این روش اطلاعات به صورت مستنداتی صفحه‌ای بر روی شبکه اینترنت قرار می‌گیرند و به‌وسیله یک مرورگر وب قابل مشاهده هستند و هم اکنون کارکردهای بسیاری دارند. (وبلاگ پارسیفا)

با توجه به بررسی تاریخچه فوق می‌توان موارد زیر را از آن استخراج نمود:

---

[۱] MainFrame

[۲] ArpaNet

[۳] www

[۴] WorldWideWeb

۱. شروع پروژه اینترنت از پروژه‌ای به نام آرپانت [۱] آغاز گردید. آرپا از دارپا [۲] که به مفهوم سازمان پروژه‌های پیش‌رفته دفاعی[۳] است گرفته شده است. این سازمان مجری پروژه آرپانت بوده است. این پژوهش در رابطه با ایجاد یک سیستم شبکه‌ای قابل اعتماد بود تا بتواند تمام سازمان‌های دست اندر کار پژوهش‌های نظامی از جمله عرضه کنندگان تجهیزات دفاعی، آزمایشگاه‌ها، پیمان‌کاران پژوهش‌های نظامی و دانشگاه‌ها را به وزارت دفاع متصل کند.
۲. ابتدا قرار بر این بود که آرپانت در مقیاسی محدود سه رایانه را در ایالت کالیفرنیا به یک رایانه در ایالت یوتا متصل نماید، اما به سرعت گسترش یافته و تمام قاره آمریکا را در بر گرفت. چون این پژوهش بسیار موفقیت آمیز بود تمام دانشگاه‌های آمریکا خواهان اتصال به این شبکه بودند. این مطلب اولین جرقه شروع گسترده سازی یک پروژه نظامی به سطح دانشگاهی و غیر نظامی بوده است.
۳. با توجه به این که عموماً ساختارهای عمومی و غیر دولتی کم‌تر خواهان تعامل با سازمان‌ها و مراکز نظامی بوده و بیش‌تر میل به این دارند که با مراجع علمی و دانشگاهی ادامه فعالیت دهند و یکی از اشکالات عمومی آرپانت این بود که به نام دفاعی و نظامی شهرت یافته بود باید تلاش می‌گردید تا به نحوی این نقیصه را در بین اذهان پاک نمود این اتفاق به یمن گسترش آرپانت در مجامع دانشگاهی تحت عنوان پروژه دانشگاهی کالیفرنیا افتاد.

با مطالعه در تاریخچه اینترنت می‌توان از زاویه دیگری به این مطلب نگاه کرد.

اتحاد جماهیر شوروی آن زمان موشکی با نام «اسپونیک»[۴] را به فضا می‌فرستد و نشان می‌دهد دارای قدرتی است که می‌تواند شبکه‌های ارتباطی آمریکا را توسط موشک‌های بالستیک و دوربرد خود از بین ببرد. آمریکایی‌ها در پاسخ‌گویی به این اقدام روس‌ها، موسسه پروژه‌های تحقیقی پیش‌رفته "ARPA" را به‌وجود آوردند. هدف از تاسیس چنین موسسه‌ای پژوهش و آزمایش برای پیدا کردن روشی بود که بتوان از طریق خطوط تلفنی، رایانه‌ها را به هم مرتبط

[۱] arpanet
[۲] darpa
[۳] Defence advanced research project agency (darpa)
[۴] Spotnik

نمود. به طوری که چندین کاربر بتوانند از یک خط ارتباطی مشترک استفاده کنند. در اصل شبکه‌ای بسازند که در آن داده‌ها به صورت اتوماتیک بین مبداء و مقصد حتی در صورت از بین رفتن بخشی از مسیرها جابه‌جا و منتقل شوند. در اصل هدف "ARPA" ایجاد یک شبکه اینترنتی نبود و فقط یک اقدام احتیاطی در مقابل حمله احتمالی موشک‌های اتمی دوربرد بود. هر چند اکثر دانش امروزی ما درباره شبکه به‌طور مستقیم از طرح آرپانت گرفته شده است. شبکه‌ای که همچون یک تار عنکبوت باشد و هر رایانه آن از مسیرهای مختلف بتواند با همتایان خود ارتباط داشته باشد واگر اگر یک یا چند رایانه روی شبکه یا پیوند بین آن‌ها از کار بیافتاد بقیه باز هم بتوانستند از مسیرهای تخریب نشده با هم ارتباط بر قرار کنند.

این ماجرا با وجودی که بخشی از حقایق به‌وجود آمدن اینترنت را بیان می‌کند اما نمی‌تواند تمام واقعیات مربوط به آن را تشریح کند. باید بگوییم افراد مختلفی در تشکیل اینترنت سهم داشته‌اند آقای پل باران[۱] یکی از مهم‌ترین آن‌هاست. آقای باران که در دوران جنگ سرد زندگی می‌کرد می‌دانست که شبکه سراسری تلفن آمریکا توانایی مقابله با حمله اتمی شوروی سابق را ندارد. مثلاً اگر رییس جمهور وقت آمریکا حمله اتمی متقابل را دستور دهد، باید از یک شبکه تلفنی استفاده می‌کرد که قبلا توسط روس‌ها منهدم شده بود. در نتیجه طرح یک سیستم مقاوم در مقابل حمله اتمی روس‌ها ریخته شد. آقای باران تشکیل و تکامل اینترنت را به ساخت یک کلیسا تشبیه کرد و معتقد بود، طی سال‌های اخیر هر کس سنگی به پایه‌ها و سنگ‌های قبلی بنا اضافه می‌کند و انجام هر کاری وابسته به کارهای انجام شده قبلی است. بنابر این نمی‌توان گفت، کدام بخش از کار مهم‌ترین بخش کار بوده است و در کل پیدایش اینترنت نتیجه کار و تلاش گروه کثیری از دانشمندان است. داستان پیدایش اینترنت با افسانه و واقعیت در هم آمیخته شده است.

در اوایل دهه ۶۰ میلادی آقای باران طی مقالاتی پایه کار اینترنت امروزی را ریخت. اطلاعات و داده‌ها به صورت قطعات و بسته‌های کوچک‌تری تقسیم و هر بسته با آدرسی که به آن اختصاص داده می‌شود به مقصد خاص خود فرستاده می‌شود. به این ترتیب بسته‌ها مانند نامه‌های پستی می‌توانند از هر مسیری به مقصد برسند. زیرا آن‌ها شامل آدرس فرستنده و گیرنده هستند و در مقصد بسته‌ها مجددا یک‌پارچه می‌شوند و به صورت یک اطلاعات کامل در می‌آیند.

---

[۱] Paul Baran

آقای باران طی مقالاتی این چنینی ساختمان و ساختار اینترنت را پیش‌گویی کرد. او از کار سلول‌های مغزی انسان به عنوان الگو استفاده کرد، او معتقد بود: وقتی سلول‌های مغزی از بین بروند، شبکه عصبی از آن‌ها دیگر استفاده نمی‌کند و مسیر دیگری را در مغز انتخاب می‌کند. از دیدگاه وی این امکان وجود دارد که شبکه‌ای با تعداد زیادی اتصالات برای تکرار ایجاد شوند تا در صورت نابودی بخشی از آن، هم‌چنان به صورت مجموعه‌ای به هم پیوسته کار کند. تا نیمه دهه ۶۰ میلادی کسی به نظرات او توجه‌ای نکرد. تا این که در سال ۱۹۶۵ نیروی هوایی آمریکا و «آزمایشگاه‌های بل» به نظرات او علاقه‌مند شدند و پنتاگون با سرمایه‌گذاری در طراحی و ساخت شبکه‌ای براساس نظریات او موافقت کرد.

ولی آقای باران بنابر دلایلی حاضر با همکاری با نیروی هوایی آمریکا نشد. در این میان دانشمندی با نام تیلور وارد موسسه آرپا شد. او مستقیما به آقای هرتسفلد رییس موسسه پیش‌نهاد کرد: آرپا هزینه ایجاد یک شبکه آزمایشی کوچک با حداقل چهار گره را تامین کند که بودجه آن بالغ بر یک میلیون دلار می‌شد. با این پیش‌نهاد تیلور تجربه‌ای را آغاز کرد که منجر به پیدایش اینترنت امروزی شد. او موفق شد در سال ۱۹۶۶، دو رایانه را در شرق و غرب آمریکا به هم متصل کند. با این اتصال انقلابی در نحوه صدور اطلاعات در دنیای ارتباطات رخ داد که نتیجه آن را امروز همگی شاهد هستیم. این شبکه به بسته‌هایی[۱] از داده‌ها که به وسیله رایانه‌های مختلف ارسال می‌شدند اتکا داشت. پس از آن که ازمایش‌ها سودمندی آن‌را مشخص کردند سایر بخش‌های دولتی و دانشگاه‌ها پژوهشی تمایل خود را به وصل شدن به آن اعلام کردند. ارتباطات الکترونیکی به صورت روشی موثر برای دانشمندان و دیگران به منظور استفاده مشترک از داده‌ها در آمد. در همان زمان که آرپانت در حال رشد بود تعدادی شبکه پوشش محلی (LAN) در نقاط مختلف آمریکا به وجود آمد. مدیران LANها نیز به وصل کردن رایانه‌های شبکه‌های خود به شبکه‌های بزرگ‌تر اقدام کردند. پروتکل اینترنت ARPAnet IP زبان استاندارد حکم‌فرما برای برقراری ارتباط رایانه‌های شبکه‌های مختلف به یک‌دیگر شد. تاریخ تولد اینترنت به طور رسمی اول سپتامبر ۱۹۶۹ اعلام شده‌است. زیرا که اولین "IMP" در دانشگاه "UCLA" واقع در سانتاباربارا در این تاریخ بارگذاری شده است.

با بررسی این نوع از نگاه به تاریخچه اینترنت می‌توان اذعان داشت:

- شروع اینترنت یک اقدام تدافعی در جنگ سرد بین شوروی و آمریکا بوده است. و در تقابل با اقدام نظامی شوروی که ارسال موشک به فضا بوده است صورت

---

[۱] packet

گرفته است و اصل آن برای پیدا کردن راهی نظامی – فنی برای اقدام تهاجمی شوروی‌ها علیه سیستم‌های مخابراتی امریکا بوده است.

- اولین بار ایده استقبال از اینترنت در نیروی هوایی امریکا و پنتاگون پشتیبانی گردید و با اهداف کاملا نظامی شکل گرفت.
- ایده استفاده ازتحلیل‌گران و دانشمندان غیر نظامی برای کمک به اهداف نظامی شکل گرفت و این ایده به عنوان ایده غالب در بین اندیشمندان و سیاستمداران امریکایی به عنوان ایده برتر قبول شد.
- در دهه ۱۹۷۰ استراتژیست‌های نظام سلطه به این نتیجه رسیدند که بدون نقاب غیر نظامی زدن به اینترنت نمی‌توانند آن را در بین عامه مردم و نخبگان و دانشمندان و دانشگاهیان و... رایج سازند و به همین خاطر در این دهه تصمیم گرفتند ظاهر آن را از حالت نظامی خارج ساخته و در بین مردم رایج ساخته و پروتکل‌های ساده‌ای را که می‌توان با آن اعتماد مردم را جلب نمود ایجاد نمایند.

در سال ۱۹۴۸ اتفاق دیگری با هدف نظامی در دنیا افتاد و آن ایجاد پیمان یوکوزا[۱] بین پنج کشور انگلیسی زبان بود. کشورهای امریکا، انگلیس، کانادا، استرالیا و زلاند نو با اتحاد با یک‌دیگر این پیمان را در مقابل پیمان ورشو که بین شوروی و کشورهای هم پیمانش بود بستند و هدف آن‌ها مقابله با اقدامات شوروی در ابعاد نظامی و جنگ سرد بود.

در این پیمان مقرر داشتند تا ضمن استاندارد کردن کلید واژه‌های دفاعی خود روش‌های ایمنی و امنیتی را با هم هماهنگ نمایند. و این گونه اطلاعات خود را با هم‌دیگر به اشتراک بگذارند. این تفاهم نامه سپس به مواردی مانند اصول دیپلماتیک و جاسوسی صنعتی و اهداف سیاسی و نظامی تسری پیدا کرده و تحت نظر N. S. A [۲] (آژانس امنیت ملی امریکا) نیازمندی‌های مشترک خود را دنبال کرده و منجر به تشکیل پروژه اشلون [۳] گردید.

پروژه اشلون بعد از پایه گذاری، اقدامات خود را به مدت ۶۰ سال به صورت پنهانی پیش برده و گزارش رسمی در این رابطه منتشر نکرد. اولین گزارش رسمی در رابطه با عمل‌کرد

---

[۱] UKUSA

[۲] National security agency

[۳] ECHELON

اشلون در سال ۲۰۰۰ منتشر گردید و در این گزارش تقریبا بر روی محورهای زیر تاکید گردیده بود.

- این پروژه زیر نظر N. S. A فعالیت می‌نماید.
- تعداد ماهواره‌های بکار گرفته در این طرح ۱۲۰ ماهواره می‌باشد.
- پایگاه‌های زمینی متصل به این ماهواره‌ها ۱۱۰۰ پایگاه در تمام نقاط دنیا می‌باشد.
- در این طرح روزانه تعداد سه میلیارد تعامل اطلاعاتی کسب، تجزیه و تحلیل و مورد بهره برداری واقع می‌شود.

با توجه به این گزارش مشخص می‌گردد که این طرح کاملاً طرحی نظامی – اطلاعاتی بوده و به اهداف جمع آوری اطلاعات با بالاترین پتانسیل مشغول می‌باشد.

ماموریت اولیه اشلون با توجه به جنگ سرد که بین دو قطب موجود در آن روز جهان وجود داشت جمع آوری اطلاعات از اقصی نقاط جهان برای بهره برداری در این جنگ بوده است. در جنگ سرد دنیا تبدیل به دو قطب جدای از هم شده بود و هر کدام از قطب‌ها در تلاش بوده‌اند بتوانند در رابطه با اطلاعات مورد نیاز خود از کشورهای حریف و رقیب اطلاعات را جمع آوری نمایند. حداکثر فضای جمع آوری به کشورهای قطب مقابل و نیازمندی‌های اطلاعاتی محدود به اطلاعات مورد نیاز در این رابطه بوده است. شیوه جمع آوری اطلاعات در طی سالیان مختلف به مسایل مختلف مرتبط می‌باشد:

- نوع نیاز به اطلاعات
- شیوه جمع آوری اطلاعات
- هدف از جمع آوری اطلاعات

در بین سیاستمداران امریکایی، هوارد دین، نامزد ریاست جمهوری آمریکا، بیش‌ترین حمایت مالی را از طریق اینترنت جمع آوری کرده است. دین که وب لاگ خود را در نیمه مارس به راه انداخت در فاصله کم‌تر از یک هفته شخصاً به جهان وبلاگ پیوست. وی دیدگاه‌های خود را در مورد اینترنت چنین برمی‌شمرد و هفت اصل برای آن بیان می‌کند.

مستقل از این که چه میزان با دیدگاه‌های وی همراه باشیم، شنیدن نظر یک سیاستمدار آمریکایی درباره چیزی که هر روزه با آن سر و کار داریم خالی از لطف نیست:

۱. اینترنت صاحب ندارد

اینترنت در خدمت منافع گروه خاصی نیست. اینترنت متعلق به تمام شهروندان و ساکنان کره زمین است.

۲. هر کسی باید متصل باشد.

فواید اجتماعی، اقتصادی و آموزشی اینترنت واقعی هستند. دسترسی همگانی به اینترنت مستقل از توانایی اقتصادی یا محل زندگی باید یک هدف دولت فدرال باشد.

۳. ارزش اینترنت مبتنی بر باز بودن آن است

اینترنت امکان جدیدی برای دسترسی به دانش بشر فراهم کرده است. این مسئولیت نسل جدید است که اطمینان حاصل کند دانش برای تولید خلاقیت و فرهنگ قابل دسترسی است.

۴. باز بودن اینترنت باید ترویج شود

اینترنت از ابتدا چنان طراحی شده بود که حرکت اطلاعات از یک نقطه به نقطه دیگر بدون تبعیض صورت پذیرد. به این ترتیب هر کس با یک ایده خوب (یا بد) می‌تواند آن را منتشر کند و تلاش نماید تا نتایج دلخواهش را بگیرد. این باز بودن اینترنت، ارزشی ضروری برای آن به عنوان میدانگاهی برای خلاقیت و تلاقی ایده‌ها است.

۵. اینترنت دموکراسی صداها است، نه فقط رسانه‌ای برای اطلاع‌رسانی

گرچه اینترنت می‌تواند برای پخش مطالب و پیام‌ها از یک نقطه به صدها و میلیون‌ها نقطه دیگر به کار گرفته شود، مهم‌ترین تأثیر اجتماعی و اقتصادی آن در تبدیل مدل اطلاع‌رسانی است. بیش از «آزادی بیان متعلق به صاحبان آن» هرکسی اکنون می‌تواند به هر کسی که می‌خواهد دسترسی داشته باشد. اینترنت مردم را تشویق می‌کند که با صدای خود در مورد چیزهایی که به آن‌ها مربوط می‌شود حرف بزنند. این اختیار سخن گفتن و گفت‌وگو عمیقاً در راستای ایده‌آل‌های دموکراسی امریکایی است.

۶. اینترنت کمال‌پذیر نیست

اینترنت کامل نیست، و هیچ وقت هم به کمال نخواهد رسید. اینترنت شبکه‌ای جهانی است که امکان اتصال نوابغ و جیب‌برها و بدتر از آن را فراهم می‌کند. اما نیاز داریم که کاربردهای قانونی و خبیثانه برای سوءاستفاده کنندگان از کودکان یا افراد آسیب پذیر جامعه‌مان را تفکیک و مشخص کنیم.

۷. اینترنت تازه در آغاز راه است

گرچه اینترنت تاکنون بیش از هفتصد میلیون نفر را در سطح جهان به یک‌دیگر متصل کرده است اما تازه در ابتدای راه خود است. باید بپذیریم که هنوز هیچ کس قابلیت‌های انیترنت را به تمامی نمی‌داند. تمام آن‌چه نیاز داریم انجام دهیم این است که حمایت‌های سیاسی و فنی لازم برای رشد اینترنت را فراهم کنیم تا به ظرفیت کامل خودش به عنوان یک نیروی جهانی برای دموکراسی دست یابد. (فن‌آوری اطلاعات برای مدیران)

امروزه نمونه‌های فراوانی از اعترافات دولت مردان امریکایی در رابطه با اخذ اطلاعات پنهان مردم از طریق اینترنت را شاهد هستیم:

به گزارش فارس به نقل از لس آنجلس تایمز، نه تنها ارسال پیام‌ها با استفاده از رایانه‌های شخصی و نوت بوک‌ها در محل کار در آمریکا کنترل و بررسی می‌شود، بلکه حتی اگر برای این کار از تلفن‌های همراه نیز استفاده شود حریم شخصی افراد حفظ نخواهد شد. یک وکیل که به نمایندگی از دولت آمریکا در جریان منازعه‌ای حقوقی در دادستانی آمریکا حضور یافته بود، تصریح کرد که بخش عمده کارکنان نهادهای دولتی در زمان حضور در محل کار نباید انتظار حفظ حریم شخصیشان را داشته باشند و چنین مسأله‌ای در زمان استفاده از رایانه و تلفن همراه معنا ندارد.

به گفته وی، هزاران کارفرمای دولتی چنین سیاست‌هایی را اعمال می‌کنند و هیچ یک از آن‌ها نمی‌توانند ادعا کنند که در این زمینه به حریم شخصی کارمندانشان توجه می‌کنند. تاکنون بارها و بارها اخباری در زمینه جاسوسی دولت آمریکا در پیام‌های الکترونیک مردم عادی و شهروندان منتشر شده بود و این خبر نیز نشان‌گر عمق بی توجهی دولت این کشور به لزوم حفظ حریم شخصی مردم است. (farsnews.ir)

۷-۳- بررسی ساختار فنی اینترنت:

برای این که بتوانیم برداشت واقعی از فضایی که به نام اینترنت توسط عامه مردم استفاده می‌شود داشته باشیم باید این فضا را کاملاً شناخته و به آن اشرافیت داشته باشیم. اگر چنان چه در فضای ناشناخته‌ای قدم بزنیم و یا این که فضا را ناشناخته و با برداشت اشتباه درنوردیم باید انتظار این را داشته باشیم که هر لحظه خطری ما را تهدید نماید. لذا به‌ترین کار این است که قبل از ورود به هر فضایی آن را به صورت واقعی شناخته و درک کنیم.

بسیاری از کاربران گمان بر این دارند که فضای اینترنت محدود به فضایی است که سرویس‌های مختلف از قبیل جست‌وجوی اطلاعات، ایمیل، وبلاگ و. . . . در آن ارایه شده و کاربران به صورت مستقیم از آن‌ها استفاده می‌نماید. این مقدار از فضا صرفاً بخش بسیار کوچکی از فضای اینترنت بوده و شاید یک ده هزارم فضای واقعی را تشکیل دهد. بسیاری از فضای اینترنت استفاده زیر ساخت‌های حیاتی کشورها مانند ارتباطات مخابراتی و ارتباطات سیستم‌های اقتصادی که با آن که بخشی از آن می‌باشد و سیستم‌های ماهواره‌ای و فرودگاه‌ها و انواع روش‌های ارتباطی و حمل و نقل و پالایشگاه‌های نفتی و فراورده‌های نفتی و کارخانجات تولید انرژی هسته‌ای و برق و سدها و. . . . بخشی از آن می‌باشد.

امروزه با توجه به جمع‌بندی که در سال ۲۰۰۲ میلادی انجام گرفت ۹۸ درصد از اطلاعات بشریت بر روی ابزار نوین که توسط اینترنت به یک‌دیگر متصل شده است تولید و نگهداری و پردازش و توسط این ابزار توزیع می‌گردد. هر ساختاری بتواند به این ابزار دسترسی پیدا نموده و یا بر روی آن اشرافیت داشته باشد عملاً مالک آشکار و یا پنهان کل اطلاعات جهان بوده و روند دسترسی به آن را رقم میزند.

کاربران اولیه اینترنت و فن آوری اطلاعات بر اثر تبلیغات مختلفی که صورت گرفته و هر روز این تبلیغات با استفاده از سیستم‌های هدایت اطلاعات برای کاربران عادی بیش‌تر توسعه می‌یابد به این باور رسیده‌اند که باید برای بیسواد قلمداد نشدن کل اطلاعات خود را بر روی ابزار و شبکه‌های که به نوعی با اینترنت در ارتباط می‌باشند قرار دهند. بسیاری از کاربران از خصوصی‌ترین اطلاعات خود تا اطلاعات عمومی خود را بر روی این ابزار قرار می‌دهند. بسیاری از سازمان‌ها تحت عنوان ایجاد دنیای بدون کاغذ[۱] یا کمترین استفاده از کاغذ[۲] اطلاعات طبقه بندی شده عادی خود را با استفاده از نرم افزارهای مختلف مکانیزه کرده و بر روی سیستم قرار می‌دهند و چون اینترنت را به لحاظ اقتصادی به‌ترین وسیله انتقال اطلاعات و سریع‌ترین وسیله تشخیص داده‌اند از آن استفاده می‌نمایند.

با توجه به این‌که امروزه ۹۸درصد از اطلاعات بشریت برروی ابزار دیجیتال تولید، ذخیره، پردازش و توزیع می‌گردد تمام نیازمندان رسمی و غیر رسمی به اطلاعات به دنبال راه‌هایی می‌باشند تا بتوانند به این سهم عظیم اطلاعات دسترسی پیدا نموده و نیاز اطلاعاتی خود را مرتفع سازند.

ویژگی‌های عصر اطلاعات به شرح ذیل می‌باشد:

- سرعت در ارسال اطلاعات
- دقت در نگهداری اطلاعات
- گمنامی در دسترسی به اطلاعات
- ساده‌گی استفاده از اینترنت
- وجود شاهراه‌های ارتباطی و اطلاع رسانی از قبیل انواع اینترانت و اکسترانت و اینترنت

[۱] Paper less

[۲] Less paper

تمام این ویژگی‌ها باعث می‌گردد دارندگان عادی اطلاعات که بیش‌ترین سطح اطلاعات را شامل می‌شود؛ به دنبال راه‌هایی باشند تا بتوانند هرچه بیش‌تر از این امکانات بهره مند شوند.

به دنبال این هستند تا اطلاعات خود را از بسترهای ارتباطی دیگر به این ابزار منتقل نموده و از امکانات آن بهره مند شوند.

به دنبال این هستند تا هر چه سریعتر و ارزانتر با مخاطبین خود از طریق این سیستم ارتباط برقرار نمایند.

به دنبال این هستند تا هر چه بیشتر می‌توانند از این امکانات برای انتقال دقیق اطلاعات خود سود ببرند.

به دنبال این هستند تا هر چه می‌توانند با آموزش کمتر به کاربران خود بتوانند از امکانات ایجاد شده بیش‌ترین بهره را ببرند زیرا به این نتیجه رسیده‌اند که سادگی در استفاده از این امکانات به حدی کاهش یافته است که با کم‌ترین آموزش می‌توان از آن استفاده نموده و مخاطبین خود را به حداکثر رسانید.

به دنبال این هستند تا بتوانند بدون این که مسئولیت‌های قانونی را برای خود افزایش دهند از این ابزار بیش‌ترین بهره را ببرند زیرا این گونه تبلیغ شده است که استفاده کنندگان از این ابزار می‌توانند در گم‌نامی به سر برده و دیگران پی به اقدامات آن‌ها نبرند.

تمام این موارد و موارد دیگر که هر روزه تبلیغ می‌شود باعث این شده است تا کاربران اعم از خانگی و بسیاری از کاربران اداری اغواگرانه به این ابزار نگاه کرده و هر روز بیش از پیش به این ابزار اعتماد نموده و اطلاعات بیش‌تری را بر روی آن قرار دهند.

سیستم‌های شخصی به این نتیجه برسند این وسیله ابزار ارزان قیمت ارسال و دریافت اطلاعات بوده و می‌توانند ضمن اعتماد به آن بیش‌ترین اطلاعات شخصی را بر روی آن قرار دهند. به این نتیجه برسند که می‌توانند محرمانه‌ترین و خصوصی‌ترین اطلاعات را اعم از نوشته و عکس و فیلم و تحقیقات انجام داده شده و. . . . . را بر روی آن قرار داده و برای محارم اطلاعاتی خود ارسال نمایند.

به این نتیجه می‌رسند که این ابزار جزیی از زندگی آن‌ها تلقی شده و می‌تواند در محرمانه‌ترین قسمت‌های منزل قرار گرفته و همراه با آنان زندگی نماید.

به این نتیجه می‌رسند که قرار دادن رایانه که دارای دوربین و امکانات دیگر بوده در قسمت‌های مختلف خانه اعم از اتاق نشیمن و اتاق کار و اتاق خواب و. . . . بدون اشکال بوده و به راحتی می‌توانند به آن اعتماد نمایند زیرا در کتاب‌ها و جزوات و مقالات مختلف هر روزه

تبلیغ می‌گردد. این امکانات دارای امنیت بوده و می‌توان آن‌ها را توسط کاربر مدیریت نموده و امنیت و ایمنی بر روی آن برقرار ساخت !

امروزه در سیستم‌های عمومی و دولتی این اعتماد به رایانه و ابزار رایانه‌ای به شدت ترویج می‌شود و تمام ساز و کار مربوطه توسط سازندگان با این نیت طراحی می‌شود تا هر چه راحت‌تر و دوستانه‌تر و بدون استفاده از ابزار و روش مازاد بتواند کاربران را با سرعت هر چه تمام‌تر از به یک‌دیگر متصل نماید تا بتوانند اطلاعات را با یک‌دیگر تبادل نموده و در کم‌ترین زمان به مقصود خود نایل شوند.

امروزه شاهد این هستیم که بر استفاده از اینترنت به علت این که دارای فرصت‌های عمومی گوناگونی به شرح زیر می‌باشد؛ در تمام ساختارهای عمومی و خصوصی تاکید می‌گردد.

فرصتهای عمومی اینترنت را این گونه تعریف می‌نمایند:

- تجارت الکترونیک
- بهره برداری علمی
- کاهش مصرف انرژی
- هم‌نشینی‌های دیجیتال

تبلیغ بر این فرصت‌های عمومی، کاربران را به این سمت سوق می‌دهد تا به اینترنت به عنوان یک ابزار ارزان و سریع و. . . . نگاه کرده و با اعتماد به آن اطلاعات خود را بروی آن قرار داده و برای یک‌دیگر ارسال نمایند.

این اعتماد باعث می‌گردد:

- یک مدیر به راحتی موافقت نماید اطلاعات درونی یک سازمان تحت عنوان سایت اطلاع رسانی و. . . . بر روی اینترنت قرار گیرد
- یک مدیر به راحتی موافقت می‌کند سیستم مکاتباتی درونی سازمان از طریق اینترنت و بستر ارتباطی آن با قسمت‌های مختلف اداری ارتباط داشته باشد.
- یک مدیر موافقت می‌نماید پیش نویس نامه‌های تهیه شده قبل از این‌که از طریق سیستم رسمی سازمان توزیع گردد تحت عنوان نظرات مشورتی از طریق ایمیل برای دیگر همکاران ارسال و درخواست نظریه گردد.
- یک مدیر سازمان موافقت می‌نماید صورت‌جلسات و دعوت به جلسات و مذاکرات اداری از طریق سرویس‌های مختلف اینترنتی در اختیار قرار گیرد.

- یک مدیر سازمان در رابطه با این‌که پرسنل سازمان از طریق انواع و اقسام سرویس‌های اینترنتی که هر روزه نیز در حال گسترش می‌باشد اطلاعات را با یک‌دیگر تبادل نمایند.
- یک مدیر سازمان موافقت می‌نماید ارتباطات صوتی و تصویری بین اعضا سازمان به علت دوری راه (اعم از داخل کشور و یا خارج از کشور) از طریق اینترنت انجام شود.
- و بدتر از تمام این ها یک مدیر سازمان موافقت می‌نماید سیستم ارتباطی سازمان اعم از تلفن ثابت و یا همراه و یا شبکه یک سازمان به شبکه اینترنت وصل تا اعضای سازمان بتوانند بدون هزینه سیم کشی و. . . از امکانات بانک اطلاعاتی سازمان بهره برداری نمایند.

تمام این اقدامات همان چیزی بود که در بررسی طرح اشلون و سیاست استراتژیک سردمداران شیطان بزرگ به این نتیجه رسیده بود تا بعد از دهه ۱۹۷۰ با عمومی نمودن اینترنت بتوانند به آن دست یابند. این واقعیت مطلبی نبود غیر از برنامه ریزی کلان برای دسترسی به اطلاعات در مبداء تولید.

در طرح اشلون به این نتیجه رسیدیم یکی از راه‌های کسب اطلاعات اشلون دسترسی به اطلاعات در لحظه تولید و در مبداء تولید می‌باشد و متاسفانه به کمک کاربرانی که نا آگاهانه و یا آگاهانه به این امر کمک می‌نمایند میسر می‌گردد.

امروزه دلایل روی آوری کاربران مختلف به اینترنت را می‌توان به شرح ذیل طبقه بندی می‌گردد:

- هزینه
- کارایی
- سرعت
- حفاظت

قبل از این‌که به امنیت در رابطه با اینترنت بپردازیم نیم نگاهی به امنیت در یک شبکه خواهیم داشت.

یک شبکه از موجودیت‌های مختلف سخت افزاری و نرم افزاری تشکیل شده است که با پروتکل‌های مختلف ارتباطی به هم پیوند خورده اند.

این موجودیت‌ها عبارتند از دستگاه‌های سرور و کلاینت‌ها و سویچ‌ها وهاب‌ها و کابل‌های ارتباطی و. . . که وظیفه آن‌ها اتصال انواع سخت افزار شبکه به یک‌دیگر می‌باشد و هر سخت افزار جدیدی که به شبکه وصل شود می‌تواند کارایی زیر را داشته باشد:

- امکان تبادل اطلاعات با یک‌دیگر

هر سخت افزاری که به شبکه وصل باشد این اجازه را خواهد داشت با اطلاع و یا بدون اطلاع مدیر سیستم با دیگر ابزار سخت افزاری شبکه ارسال و دریافت اطلاعات داشته و در این رابطه نیازمند به کم‌ترین آگاهی از رایانه می‌باشد.

- امکان شناخت اتوماتیک ابزار جدیدی که به شبکه افزوده می‌شود بدون این‌که برای کاربر مشکلی از نظر زمان و امکانات ایجاد نماید و به قول معروف به صورت دوستانه به شبکه اضافه می‌شود تا کار بر با کم‌ترین دغدغه خاطری ترغیب به استفاده از این ابزار گردد.

در پروتکل‌های قدیمی کاربران به سمت اطلاعات می‌رفتند و اطلاعات مورد نیاز را پیدا نموده و با اجازه‌ای که مدیر سیستم می‌داد می‌توانستند به آن دسترسی پیدا نمایند لیکن در پروتکل‌های جدید برای افزایش سرعت دسترسی به اطلاعات توسط کاربران، این گونه طراحی شده است که بسته‌های اطلاعاتی به مجرد تولید در کل شبکه توزیع گردد و بر مبنای ویژگی‌هایی که در هر کدام از بسته‌های اطلاعاتی قرار داده شده است دریافت کنندگان اطلاعات می‌توانند به اطلاعات خود دسترسی داشته و از آن استفاده نمایند.

با توجه با این‌که اینترنت را نوعاً شبکه شبکه‌ها مینامند. مفهوم این نام گذاری این است که هر امکانی که در یک شبکه وجود داشته باشد به طریق اولی و به صورت کامل‌تر در اینترنت وجود دارد و دسترسی‌ها در اینترنت راحت‌تر از دسترسی در یک شبکه محلی می‌باشد.

در اینترنت تمام سخت افزاری که به اینترنت وصل می‌گردد می‌تواند با دیگران اطلاعات را به اشتراک بگذارد.

در اینترنت تمامی سخت افزاران و نرم افزاران این قابلیت را پیدا می‌کنند تا به صورت آشکار و پنهان با یک‌دیگر تبادل اطلاعات داشته باشند.

هر سخت افزار و یا نرم افزاری که به صورت فیزیکی و از طریق هرکدام از سیستم‌های ارتباطی که به اینترنت وصل شوند جزیی از موجودیت‌های اینترنت خواهد بود و تمام موارد گفته شده در رابطه با آن مصداق خواهد داشت.

کاربران عمومی اینترنت معمولاً از سرویس‌های عمومی اینترنت استفاده می‌کنند و بسیاری از آن‌ها گمان بر این دارند که کل اینترنت محدود به همین سرویس‌هایی است که آن‌ها از آن

استفاده می‌نمایند و این سرویس‌ها هر روزه به شکل عمومی‌تری در حال توسعه بوده و در اختیار کاربران قرار می‌گیرند. لیکن این‌گونه استفاده از اینترنت صرفاً استفاده از یک هزارم فضای اینترنت بوده و اینترنت ابعاد مختلفی دارد. در این استفاده محدود از اینترنت خطرات گوناگونی کاربران را تهدید می‌نماید که می‌توان آن‌ها را به شکل زیر تقسیم بندی نمود:

تهدیدات عمومی استفاده از اینترنت:

- تقسیم دیجیتالی دنیا
- دسترسی حریف به محتوای در حال تبادل
- دسترسی حریف به اطلاعات ذخیره شده
- تخریب اطلاعات
- انجام روان سنجی ناخودآگاه
- انجام عملیات فیزیکی
- انجام عملیات روانی

این‌گونه جمع آوری اطلاعات از طریق اینترنت صرفاً جمع آوری عمومی بوده و جامعه هدف آن کاربران عمومی اینترنت می‌باشد و شاید یکی از رایج‌ترین اهداف جمع آوری اطلاعات در بین نیازمندان به اطلاعات می‌باشد.

مهم‌ترین بخش از جمع آوری اطلاعات مربوط به ۰/۹۹۹۹ درصد دیگر بهره برداری از اینترنت می‌باشد.

امروز تقریبا ارتباط اصلی بین کشورهای مختلف اعم از ارتباط بی‌سیم و باسیم از طریق اینترنت برقرار می‌گردد و بخش اعظم این برقراری ارتباط از دید کاربران نهایی پنهان است.

امروزه ارتباط اصلی بین ماهواره‌های مختلف از طریق اینترنت برقرار می‌شود و این از دید کاربران عادی پنهان است.

امروزه ارتباط رادیو وتلویزیون از طریق اینترنت برقرار می‌شود و این از دید کاربر نهایی پنهان است.

امروزه ارتباط بین تمام ابزار دیجیتال اعم از خانگی و اداری از طریق اینترنت برقرار می‌شود و این از دید استفاده کنندگان از این سیستم‌ها پنهان است.

در جمع‌بندی کلی اطلاعات انسان‌ها از طریق اینترنت برقرار شده و کاربران نهایی صرفاً آخرین دریچه ارتباطی و آخرین گلوگاه ارتباطی را مشاهده نموده و کم‌تر به قسمت‌های دیگر می‌پردازند و به این علت بیش‌ترین اعتماد را به اینترنت داشته و اطلاعات خود را از طریق آن

ردوبدل می‌نمایند. و نظام سلطه در امتداد استراتژی اولیه خود در رابطه با اینترنت به دنبال این وسیله می‌باشد:

- ایجاد حس اعتماد کاربر به اینترنت
- بهره برداری از اطلاعات در مبداء تولید

همان گونه که می‌دانید اطلاعات دیجیتال بر سه نوع تقسیم شده است:

- اطلاعات ذخیره شده
- اطلاعات در حال انتقال
- اطلاعات پشتیبان تهیه شده

و طالبین اطلاعات هر سه نوع اطلاعات را رهگیری و جست‌جو می‌کنند.

این بخش از جمع آوری اطلاعات فقط بخشی اندکی از وظیفه اینترنت برای نظام سلطه می‌باشد. امروزه وظیفه اینترنت بسیار فراتر از این رفته است.

با توجه به این‌که اینترنت علاوه بر خانه‌های مردم و ادارات دولتی و عمومی به ساختارهای حیاتی کشورها نیز رسوخ نموده است. بسیاری از زیر ساخت‌های حیاتی کشورها از طریق اینترنت به یک‌دیگر متصل شده و از آن طریق مدیریت و کنترل و نظارت می‌گردند. بسیاری از پالایشگاه‌ها و سدها و کارخانجات عظیم صنعتی و نیروگاه‌های انرژی هسته‌ای و وزارتخانه‌ها و سازمان‌های حساس و. . . . از طریق اینترنت به یک‌دیگر متصل شده و نظارت اتوماتیک و غیر اتوماتیک به این روش صورت می‌پذیرد.

امرزه سیاستمداران کشورها برای مدیریت بر کشور خود نیاز به استفاده از انواع سیستم‌های نظارتی و کنترلی و تولید کنندگی اطلاعات و. . . دارند و تحت عنوان سیستم‌های مدیریتی مبتنی بر رایانه از آن‌ها استفاده می‌نمایند و در حقیقت اطلاعات استراتژیک را به نوعی به اینترنت متصل نموده و از آن بهره برداری می‌نمایند و برای استفاده از آن نیز هر روزه تشویق می‌شوند. در دوره‌های مدیریت و کلاسیک و تنظیم سیاست‌ها و. . . بر آن تکیه می‌نمایند و آن را در بین جامعه دانشگاهی و نخبگان تشویق می‌نمایند. استفاده از این ابزار را به عنوان ملاک و شاخص نخبگی تبلیغ می‌نمایند و خودآگاه و یا ناخودآگاه جامعه را به سمت استفاده از این ابزار وامکانات سوق می‌دهند. و این همان چیزی است که نظام سلطه به دنبال آن می‌باشد:"بهره برداری از اطلاعات در لحظه تولید"

۷-۴- جنگ اینترنتی

جنگ‌های آینده با به کارگیری رایانه انجام می‌شود و فن‌آوری نوین اطلاع رسانی هر چه بیش‌تر در خدمت ارتش‌ها قرار خواهد گرفت. برای سربازان آینده، جنگ بدون رایانه بی‌معنی است و چرخ بال‌ها، تانک‌ها، نفربرها و حتی تجهیزات سبک و فردی سربازان هرچه بیش‌تر الکترونیکی خواهند شد. سربازان آینده در زمان وقوع یک جنگ حقیقی، با فن‌آوری پیش‌رفته اطلاع رسانی، سیستم‌های ویدئویی و اینترنت لحظه به لحظه از جایگاه خود، موقعیت دشمن را زیر نظر می‌گیرند. نخستین نمونه‌های به کارگیری چنین روش‌هایی به عنوان نمونه در جریان جنگ بالکان و جنگ دوم خلیج فارس صورت گرفت.

به گزارش بنگاه سخن پراکنی بریتانیا[۱] دولت انگلیس قصد دارد برای نهایی کردن به کارگیری چنین سیستم‌ها و تجهیزاتی تا سال ۲۰۱۱ میلادی، نزدیک به یک میلیارد پوند هزینه کند. این در حالی است که در فرانسه، آلمان، اسپانیا و ایتالیا نیز طرح‌های مشابه‌ای در نظر گرفته شده است. این گزارش می‌افزاید: ایالات متحده آمریکا نیز می‌کوشد تا پایان سال ۲۰۱۰ میلادی، بیش از چهار میلیارد دلار در برنامه بهینه سازی پیاده نظام خود سرمایه گذاری کرده و ۵۰ میلیارد دلار برای استفاده از فن‌آوری نوین اطلاعاتی _ ارتباطی در ارتش خود هزینه کند.

۷-۵- همکاری و هماهنگی بین سه عنصر اینترنت اشلون و فن آوری‌های هوشمند

امروزه فن‌آوری‌های هوشمند به عنوان یکی از توانمندی‌های تکنولوژی نوین در اختیار تمام کاربران قرار گرفته است. در این فن‌آوری کلیه امکانات و اطلاعات مورد نیاز به صورت هوشمندانه و به صورت پیش تعریف شده در سیستم قرار داده شده و هر سخت‌افزار و نرم‌افزاری که به کار گرفته می‌شود این قابلیت را خواهد داشت تا محیط را شناسایی نموده و خود را به محیط به عنوان یک ابزار مجاز شناسایی نموده و در آن محیط قادر به انجام ماموریت از پیش تعریف شده باشد و برای انجام این ماموریت در کوتاه‌ترین زمان ممکن و بدون استفاده از هرگونه عامل بیرونی غیر از پیش تعریف شده به عامل جدیدی نیاز نداشته باشد و برای به روز رسانی خود به صورت هوشمندانه عوامل محیطی و محاطی را شناسایی نموده و خود را با شرایط جدید تنظیم و به روز رسانی نماید.

---

[۱] B. B. C

از طرف دیگر در طرح اشلون با استفاده از ماهواره‌ها و ارتباطات زمینی که در پایگاه‌های مختلف در اقصی نقاط جهان به کار گرفته می‌شوند نظام سلطه به دنبال این می‌باشد تا هر چه بیش‌تر این امکانات را به صورت هوشمندانه توسعه داده و ماموریت از پیش تعریف شده و استراتژی خود را که همان اشرافیت کامل بر ارتباطات و اطلاعات جهان می‌باشد به خوبی انجام داده و تمام اطلاعات در مبداء تولید را به دست آورده و با کلید واژه‌های از قبل تعریف شده آن‌ها را شناسایی و در راستای نیات پلید نظام سلطه به کار گرفته و بیش از پیش تلاش در گسترش این سلطه بر تمام دنیا دارد.

این دو مولود نابهنجار به دنبال این بوده و هستند تا بتوانند ارتباطات خود را از روش‌های که خود عاملین شوق در به کارگیری آن داشته باشند را گسترش دهند.

با این شرایط همکاری و هماهنگی بین سه عنصر اینترنت و اشلون و فن آوری‌های هوشمند شکل می‌گیرد. یکی از این عوامل تلاش می‌نماید تا هر چه بیش‌تر در زندگی انسان‌ها نفوذ نموده و در مبادی تولید اطلاعات قرار گرفته و شیوه و نوع اطلاعات تولید شده را به آسان‌ترین روش و مقبول‌ترین روش مدیریت نماید و دیگری به دنبال این می‌باشد که به اطلاعات تولید شده اشرافیت داشته و با طبقه بندی اطلاعات آن‌ها را به صورت موضوع بندی شده و مرتبط با یک‌دیگر به کار بگیرد و سومی مسیر ارتباط بین این دو مولود را برای ارتباط هرچه به‌تر و سریع‌تر و ارزان‌تر و مورد علاقه‌مندتر فراهم سازد.

۷-۶- اطلاعات تبادلی از طریق اینترنت

با توجه به این که اینترنت در تمام عرصه‌های زندگی انسان‌ها وارد شده است اطلاعات مختلفی از طریق آن متبادل می‌شود که به مهم‌ترین آن‌ها اشاره می‌شود.

۷-۶-۱- بانک‌های اطلاعاتی

تقریبا تمام بانک‌های اطلاعاتی دنیا با توجه به تعاریفی که در رابطه با بانک اطلاعاتی ارائه شد به اینترنت متصل بوده و از این طریق منابع اطلاعاتی را بین نیازمندان به آن توزیع می‌نماید. تمام پژوهش‌گران از این طریق به اطلاعات دسترسی پیدا نموده و اطلاعات تولیدی خود را به دیگران عرضه می‌نمایند. سیستم‌های صنعتی از این طریق بر صنعت نظارت و کنترل می‌نمایند. سیستم‌های اقتصادی از آن به عنوان رگ‌های انتقال جریان اقتصاد استفاده می‌نمایند. سیاسیون از آن به عنوان کانال ارتباطی استفاده می‌کنند. سیستم‌های توزیع اطلاعات از آن به عنوان شاه را ارتباط با مشتریان بهره می‌گیرند.

۷-۶-۲- رایانه‌های شخصی

تمام چند میلیارد نفری که امروزه به عنوان کاربران اینترنت شناسایی شده و در آمارهای مختلف به آن اشاره می‌شود از طریق رایانه‌های شخصی خود با اینترنت در ارتباط می‌باشند و در این رایانه اطلاعات شخصی خود را قرار داده‌اند. همان‌گونه که قبلاً توضیح داده شد هر سخت‌افزار و نرم‌افزاری که به هر شکل و برای هر زمان به اینترنت متصل می‌شوند به عنوان یکی از بازیگران در این عرصه ایفای نقش نموده و جوی از اینترنت می‌شوند و همان‌گونه که از چند میلیارد نفر اطلاعات می‌گیرند خودشان نیز جزئی از آن خواهند بود که این امکان را برای دیگران فراهم می‌نمایند تا از اطلاعات قرار داده شده بر روی رایانه شخصی خودشان، دیگران بتوانند بهره ببرند.

۷-۶-۳- ایمیل

ارسال ایمیل بدون استفاده از اینترنت امکان پذیر نخواهد بود. با توجه به سهولت و سرعت در استفاده از ایمیل مروزه تقریبا تمام کاربرانی که از اینترنت استفاده می‌نمایند اعم از این که این استفاده شخصی، تجاری، عمومی و یا خصوصی باشد از ایمیل استفاده می‌نمایند و اطلاعات خود را بر روی سایت‌ها و سرورهای قرار می‌دهند تا دیگران با مراجعه به آن‌ها بتوانند از این اطلاعات بهره‌برداری نمایند.

۷-۶-۴- انواع چت

در عصر ارتباطات انواع چت متنی، صوتی و تصویری تبدیل به یکی از به‌ترین و راحت‌ترین روش‌های ارتباطی بین دو یا چندین نفر در اقصا نقاط دنیا شده است. با توجه به این که سرورهایی که امکان برقراری چت را فراهم می‌سازند باید بتوانند بر این نوع ارتباط مدیریت نمایند قبل از این که اطلاعات چت را به طرف مقابل برسانند آن‌ها را ذخیره نموده و به صورت فایل برای دیگران ارسال می‌نمایند. این ذخیره سازی باعث این خواهد شد تا بتوان به صورت مجاز و غیر مجاز، آشکار و پنهان بتوان بر این اطلاعات مدیریت نمود.

۷-۶-۵- اتوماسیون‌های اداری

ساختارهای مختلف دولتی و عمومی و در بسیاری مواقع خصوصی به دنبال این می‌باشند تا روش ارتباطی ارزان‌تری را برای ارتباط بین سازمانی خود پیدا نمایند. با توجه به نقشی که برای اینترنت تعریف شده است تقریباً تمام آن‌ها با استفاده از اینترنت این نوع نیاز خود را برآورده

می‌نمایند و این باعث خواهد شد تا اطلاعات سیستم‌های اتوماسیون اداری به جزئی از اینترنت تبدیل شده و همان نقش تعریف شده از قبل را بازی نماید.

۷-۶-۶- سیستم‌های اقتصادی

- اطلاعات بانکی و موجودی مالی افرادی که در این شبکه گردش مالی دارند
- توان سنجی مردم هر کشور ار نظر مالی و رشد یا پسرفت مالی افراد کشورها در طی سالیان مختلف و در تقابل با اتفاقات مختلف که در دنیا می‌افتد
- اعتبار سنجی میزان اعتماد مردم به دولت با توجه به بررسی تعامل مالی و بانکی مردم آن کشور در بانک‌ها در طی اتفاقاتی که در آن کشور می‌افتد
- توان آن کشور در استفاده از اعتبارات مالی مردم در به چرخش در آوردن اقتصاد خرد و کلان آن کشور
- ورودی‌های اصلی سیستم اقتصادی آن کشور و میزان و درصد هر کدام از آن ورودی‌ها
- توان سنجی نوع ورودی‌های اقتصادی هر کشور در طی سالیان مختلف
- میزان وابستگی کشور به منابع اقتصادی کشور در طی سالیان مختلف و بر اساس اتفاقات داخلی و خارجی
- نوع و میزان اثرگذاری منابع اقتصادی کشور و فرصت‌ها و تهدیدات اقتصادی که از جانب آن متصور است
- نوع توزیع استراتژیک کشور در رابطه با منابع اقتصادی
- نوع و میزان و توان جذب منابع اقتصادی کشور توسط بنگاه‌های توسعه اقتصادی کشور
- نگاه حاکمیتی کشور به چرخش اقتصادی کشور
- نوع تغییرات برنامه ریزی استراتژیک کشور از زاویه اقتصادی

امروزه در جوامع مختلف یک واژه جدید ابداع گردیده است و در حال گسترش می‌باشد. این واژه چیزی نیست به غیر از "جاسوسی اقتصادی". در این نوع جاسوسی کشورهایی که جاسوس اعزام می‌کنند به شکل‌های مختلف به دنبال نیاز سنجی اقتصادی کشورها و به دست آوردن توان اقتصادی کشورها می‌باشند. در گذشته این کار با اعزام جاسوسان اقتصادی یا جذب عناصر اقتصادی کشورها صورت می‌پذیرفت و امروزه با دسترسی به اطلاعات اقتصادی کشورها صورت می‌پذیرد و دسترسی به شبکه‌ها یکی از رایج‌ترین این روش‌ها می‌باشد.

۷-۶-۷- سیستم‌های آموزشی

- لیست و مشخصات افرادی که در مقاطع مختلف تحصیلاتی اعم از کلاسیک و غیر کلاسیک مشغول به تحصیل می‌باشند
- ظرفیت سنجی افرادی که مشغول به تحصیل می‌باشند
- گرایش‌های عمومی و اختصاصی افرادی که مشغول به تحصیل می‌باشند
- نوع و میزان سرمایه گذاری دولت در طبقه‌های مختلفی که مشغول به تحصیل می‌باشند
- استراتژی عمومی و اختصاصی دولت در رابطه با سرمایه گذاری بر روی تحصیل و نوآوری
- توان سرمایه گذاری و میزان بهره‌برداری دولت از این نوع سرمایه گذاری
- روند رشد کشورها در سالیان مختلف در رابطه با علم و تحصیل
- توان نوآوری و خلاقیت کشورها در زمینه‌های علمی
- اکتشافات و زمینه‌های اکتشافی در علوم و فنون مختلف و نوع امکان اثر گذاری بر روی آن افراد و شیوه کنترل و اشرافیت بر روی آن فرد یا افراد
- سمت و سوی سرمایه گذاری علمی دولت
- میزان استقبال عامه مردم از علم و فن آوری

با توجه به این که امروزه یکی از توانمندی‌های هر کشور را علم و دانائی تشکیل می‌دهد. با توجه به این که در هر کشوری میزان رشد علم و تخصص یکی از شاخصه‌های اصلی پیشرفت آن کشور می‌باشد و با توجه به این که با به دست آوردن این توانائی می‌توان بر علیه آن کشور برنامه ریزی اطلاعاتی داشت به همین خاطر کشورهای سلطه‌گر و متخاصم به دنبال آن می‌باشند تا با جذب نخبگان علمی و فرهنگی کشورها نفوذ پذیری خود در آن کشورها را افزایش دهند و یکی از این راه‌ها و مقدمات آن دسترسی به اطلاعات علمی و تحصیلاتی و آموزشی آن کشور می‌باشد. با توجه به دیجیتالی شدن این اطلاعات و ثبت آن در شبکه‌های مختلف رایانه‌ای، این اطلاعات در شبکه‌ها وجود داشته و دسترسی عناصر غیر مجاز به این شبکه‌ها برابر است با دسترسی به اطلاعات علمی و تحصیلاتی و آموزشی آن کشورها.

۷-۶-۸- سیستم‌های سیاسی

- اطلاعات سیاست مداران و اثرگذاران در سیاست کشور
- اطلاعات گرایش‌های مختلف سیاسی در کشور

- اطلاعات مردمی که در گرایش‌های مختلف اثر گذاری دارند
- نوع و میزان سرمایه گذاری دولت در گرایش‌های مختلف سیاسی
- میزان و توان دولت و سیاسیون در استفاده از فرصت‌های ایجاد شده در زمینه‌های سیاسی
- توان مقابله دولت یا اشرافیت در راستای استفاده از توان سیاسی
- میزان آرا و توان سنجی تغییر آرا در عرصه‌های مختلف سیاسی و اجتماعی
- سرمایه گذاری عمومی حاکمیتی در راستای پهنه آرائی سیاسی کشور

مسلم است هر سازمان جاسوسی که بتواند به صورت غیر مجاز به این اطلاعات دسترسی کند به بخش اعظمی از اطلاعاتی که بتواند با اثر گذاری بر روی آن‌ها بر روی کشور تاثیرات سیاسی بگذارد دسترسی پیدا نموده است و می‌تواند برای آن برنامه ریزی نماید.

امروزه در علوم سیاسی این امر یک مسئله طبیعی است تا کشورها به دنبال این باشند تا با روش‌های سیاسی بر دیگر کشورها اثرگذار باشند. این اثرگذاری در سیاست‌ها متقابل می‌باشد و برخی مواقع به دنبال زمینه‌های براندازی فکری و فرهنگی و نرم و در نهایت براندازی سخت و حاکمیتی در آن کشور می‌باشند.

زمانی که کشور متخاصمی توان این را داشته باشد تا با دسترسی به شبکه‌های سیاسی کشور دیگر این اطلاعات و امکانات را به دست آورد مسلم است به عوض گسیل جاسوسان انسانی در تلاش خواهد بود تا با دسترسی به شبکه‌های سیاسی آن کشور این گونه اطلاعات را در زمان‌اندک و با هزینه کم و بی خطر انجام دهد.

۷-۷- تفاوت بین جنگ و جرم سایبری

یکی از مسایلی که در حوزه‌ی دفاع غیرعامل مطرح می‌گردد، دفاع در برابر جنگ‌هایی است که بدون جنگ‌افزار فیزیکی صورت می‌پذیرد.

با پیشرفت فن‌آوری و ظهور فن‌آوری‌های نوین از جمله فن‌آوری اطلاعات و ارتباطات، ارزش اطلاعات در افزایش قدرت بازدارندگی یا ایجاد برتری در جنگ بالاتر رفته است. این افزایش ارزش اولاً به دلیل افزایش بسیار زیاد حجم اطلاعات تولید شده در دنیای کنونی از یک سو و ثانیاً به دلیل ایجاد قابلیت‌های پردازش و تحلیل دقیق اطلاعات به وجود آمده است. به همین دلیل است که به اذعان همه‌ی متخصصان، اطلاعات به عنوان مهم‌ترین منبع لازم برای کلیه‌ی فعالیت‌ها در سطوح مختلف اعم از فردی، سازمانی و ملی معرفی گردیده است. بنابراین

حفظ برتری در سطح سیاسی کشورها، چه در شرایط صلح چه در جنگ رابطه‌ی مستقیمی با برتری اطلاعاتی آن‌ها دارد.

با توجه به آن‌چه در خصوص ارزش اطلاعات برای افراد، سازمان‌ها و کشورها گفته شد، طبیعی است تخاصماتی بین رقبا، در همه‌ی سطوح، نه به صورت سابق که با رویکرد جمع‌آوری اطلاعات یا ارائه‌ی اطلاعات مخدوش به حریف در می‌گیرد.

در یک تعریف جنگ‌هایی این‌گونه که در شکل سنتی صورت نمی‌گیرد، جنگ اطلاعاتی نامیده شده است. در تعریف دیگری ایده‌ها و نظریه‌های مرتبط با اثرگذاری و روش تفکر انسان‌ها و از آن مهم‌تر، روش بهره‌گیری از اطلاعات برای دست‌یابی به اهداف ملی یک کشور نیز جنگ اطلاعاتی نامیده می‌شود. این اهداف ممکن است در زمینه‌های سیاسی، اقتصادی یا نظامی باشند. در استراتژی جنگ اطلاعاتی، اعتقاد بر این است که به جای تسلیحات با حجم تخریب زیاد، باید از تسلیحات به صورت دقیق علیه نقاط ضعف و آسیب‌پذیر سیستم استفاده شود. جنگ اطلاعات شامل عملیات معین برای حفظ یک‌پارچگی سیستم اطلاعات خودی در برابر تخریب، گسیختگی یا بهره‌برداری دشمن است، در حالی که به طور هم‌زمان بهره‌برداری، انهدام یا تخریب یک سیستم اطلاعاتی دشمن و فرآیند کسب برتری اطلاعاتی را در به کارگیری نیروها نیز انجام می‌دهد.

۷-۸- سئوالات خودآزمایی

۱. تاریخچه مختصر اینترنت را از دیدگاه نظام سلطه بنویسید.
۲. جنگ اینترنتی چیست؟ توضیح دهید.
۳. دسترسی به اطلاعات محلی از طریق اینترنت را توضیح دهید.
۴. نقش شبکه‌های اجتماعی موجود در اینترنت را در براندازی حاکمیت‌ها را توضیح دهید.
۵. پنج نوع از اطلاعات تبادلی از طریق اینترنت را نام برده و توضیح دهید.
۶. جنگ سایبری را توضیح دهید.
۷. تفاوت بین جنگ و جرم سایبر را توضیح دهید.
۸. مبانی و اصول امنیت رایج در اینترنت را بنویسید.
۹. نقش شخصیت مجازی در ناامنی اینترنت را توضیح دهید.
۱۰. انواع روش‌های اخذ اطلاعات پنهان از طریق روش‌های رایج در روی اینترنت را بنویسید.

فصل هشتم :ماهواره‌ها

آنچه در این فصل می‌خوانید:

- **مدارهای ماهواره‌ای**
- **استقرار ماهواره‌ها**
- **شبکه ماهواره‌ای جاسوسی اشلون**
- **کاربرد نظامی ماهواره‌ها**

۸- ماهواره‌ها

۸-۱ - مدارهای ماهواره‌ای :

ماهواره‌ها به دور زمین دریک مسیر بسته که آن را مدار می‌نامند، درحال گردش هستند. ناظری که درخارج منظومه شمسی قرار گرفته و به زمین می‌نگرد، مشاهده می‌کند که ماهواره‌ها در مسیرهایی به دور زمین درحال چرخشند. این مسیرها می‌توانند دایره‌ای یا بیضی شکل باشند اما مرکز زمین در هرحالت در مرکز این مسیر یا در نقطه کانونی آن قرار دارد. ماهواره درصورتی که تحت تاثیر نیروهای جاذبه دیگری قرار نگیرد، همواره در صفحه‌ای به نام صفحه مداری به گردش خود به دور زمین ادامه می‌دهد. حرکت این صفحه مداری به پریود مدار و زاویه صفحه با مدار استوا بستگی دارد. اگر این زاویه صفر باشد، صفحه مداری منطبق بر صفحه استوایی زمین می‌شود. انواع مدارهایی که ماهواره‌ها در آن مستقر می‌شوند، عبارت‌اند از:

۱- مدارهای پایین زمین[۱]
۲- مدارهای هم‌زمان زمینی[۲]
۳- مدارهای ثابت زمینی[۳]

۸-۱-۱-مدارهای پایین زمین :

ماهواره‌های مدارهای پایین زمین در ارتفاعات چند صد کیلومتری سطح زمین قرار دارند و زمان یک دور چرخش به دور زمین در این مدارها، حدود ۹۰ دقیقه است. این مدارها در ارتفاع نسبتاً کمی قرار دارند، درنتیجه می‌توان اجسام نسبتاً سنگین را با یک سیستم پرتاب کننده ساده در آن‌ها قرارداد. گفتنی است که بیش‌تر ماهواره‌هایی که در این مدارها مستقرند، درصد زیادی (حدود ۵۰ درصد) از وقت خود را در سایه زمین می‌گذرانند و باید مجهز به باتری‌هایی

---

[۱] LEO - Low earth orbit

[۲] Geosynchronous earth orbit

[۳] GEO -Geostationery earth orbit

باشند که بتوانند وسایل الکترونیکی را در این مدت تغذیه کنند. این مدارها معمولاً برای مشاهدات و فعالیت‌های ماهواره‌های نظامی به کاربرده می‌شود.

۸-۱-۲-مدارهای هم‌زمان زمینی :

مدارهای هم‌زمان زمینی دارای پریودی درست برابر گردش زمین هستند. این مدار، مدار۲۴ ساعته نیز خوانده می‌شود.

۸-۱-۳-مدارهای ثابت زمینی :

مدار ماهواره ثابت زمینی نوعی ازمدار هم‌زمان زمینی است که درآن، زاویه صفحه‌ای که مداردرآن قرار گرفته و صفحه‌ای که از استوای زمین می‌گذرد، صفر است. در نتیجه این دو صفحه بر هم منطبق می‌شوند. مدار ثابت زمینی و مدارهای هم‌زمان زمینی در فاصله ۳۵۷۸۸ کیلومتری زمین قراردارند. ماهواره‌ها با سرعتی حدود سه کیلومتر درثانیه در مدارثابت زمینی حرکت می‌کنند. برای ردیابی ماهواره احتیاج به سیستم پیچیده‌ای نیست ماهواره‌ها درمدار ثابت زمینی، با تعدادکم، امکان ایجاد پوشش زیادی را در روی زمین دارند. به عنوان مثال سه ماهواره در روی این مدار برای پوشش بیش‌تر سطح زمین (به جزء قطب‌ها) کافی هستند.

بعضی مدارها بر اساس ارتفاع ماهواره‌ها از سطح زمین طبقه‌بندی می‌شوند. اگر ارتفاع ماهواره‌ها از سطح زمین تا ۱۰۰۰ کیلومتر باشد مدار را مدار پایین گویند. چنان‌چه ارتفاع ماهواره ازسطح زمین بین ۱۰۰۰ کیلومتر تا حدود ۲۰۰۰۰ کیلومتر باشد، ماهواره را در مدار متوسط نامند. اگر ارتفاع ماهواره از سطح زمین بیش‌تر از ۲۰۰۰۰ کیلومتر باشد، مدار را مدار بالا گویند.

۸-۲-مدار

در حالت کلی، ماهواره‌ها بروی ۴ نوع مدار یا Orbit که بسته به نوع استفاده ماهواره دارد، قرار می‌گیرند :

LEO : Low Earth Orbit
POLAR :Polar orbit
GEO : Geosynchronous Equatorial Orbit
Elliptical : Elliptical Orbit

۸-۲-۱- ماهواره‌های LEO [۱]:

به ماهواره‌هایی که در در فاصله کمی از سطح زمین قرار دارند، گفته می‌شود. بیش‌ترین ارتفاع این نوع ماهواره‌ها بین (۳۲۰ - ۸۰۰ kilometers) است.

به‌دلیل نزدیکی فاصله این نوع ماهواره‌ها از سطح زمین، سرعت حرکت این ماهواره‌ها خیلی بیش‌تر از سرعت دوران زمین بدور خود است تا سقوط نکنند. (چرا؟) گاهی سرعت این نوع ماهواره‌ها به (۲۷،۳۵۹ کیلومتردر هر ساعت)! نیز می‌رسد.

در واقع با این سرعت، این نوع از ماهواره‌ها می‌توانند در هر ۹۰ دقیقه، یک دور کامل بدور زمین بگردند.

ماهواره‌های هواشناسی، ماهواره‌های Remote Sensing و ماهواره‌های جاسوسی از این نوع اند. مسیر حرکت از غرب به شرق و هم جهت با دوران زمین بدور خود.

۸-۲-۲- Polar Orbit:

نوعی از ماهواره‌های LEO را گویند که مسیر مدار حرکت آن‌ها عمود بر خط استوا و مسیر دوران از قطب‌های شمال و جنوب می‌گذرد. مسیر دوران از شمال به جنوب.

ماهواره‌های هواشناسی، ماهواره‌های Remote Sensing و ماهواره‌های جاسوسی از این نوع اند.

۸-۲-۳- GEO:

در حالت کلی بروی مدار Geosynchronous Equatorial Orbit و بر بالای خط استوا، در فاصله ۳۳۶۰۰ کیلومتری از سطح زمین قرار دارند.

این نوع ماهواره‌های در فضا در مکانی ثابت قرار دارند و دوران زمین بدور خود، هم‌زمان می‌گردند و به‌دلیل همین ثبات دارای سایه‌ای ثابت به نام Footprints بر زمین هستند.

به مدار geosynchronous مدار GeoSTATIONARY Orbit یا مدار کلارک نیز گفته می‌شود.

تمام ماهواره‌های مخابراتی و تلویزیونی بروه این نام خوانده می‌شوند.

۸-۲-۴- Elliptical:

به معنی بیضی بوده و ماهواره‌هایی که دارای مداری بیضوی مانند شکل فوق هستند گفته می‌شود.

---

[۱] Low Earth Orbit

این ماهواره‌ها دارای دو قسمت مداری هستند :

۱) قسمتی که به سطح زمین نزدیک می‌شوند به نام نقطه حضیض[۱] یا نامیده می‌شود.

۲) قسمتی که از سطح زمین دور می‌شود به نام نقطه اوج یا apogee نامیده می‌شود.

مانند ماهواره‌های polar مسیر حرکت و دوران این نوع ماهواره از سمت شمال به جنوب است.

همان طور که گفتیم اکثر ماهواره‌های مخابراتی در مدار GEO قرار گرفته‌اند، ولی این ماهواره‌ها هیچ پوششی بروی قطب‌های شمال و جنوب ندارند. به همین دلیل و جهت پوشش قطب‌ها از این نوع ماهواره‌ها استفاده می‌شود.

در واقع این نوع از ماهواره‌ها، شمالی‌ترین و جنوبی‌ترین قسمت نیمکره‌ها hemispheres را پوشش می‌دهند.(aerocenter. ir)

۸-۳- شبکه ماهواره‌ای جاسوسی اشلون

ایستگاه‌های گیرنده شبکه جاسوسی اشلون در تمام دنیا مستقر است آژانس امنیت ملی ایالات متحده (NSA) سیستم جاسوسی جهانی با اسم رمز اشلون۲ را طراحی کرده است. این شبکه به کلیه تماس‌های تلفنی، فاکس‌ها و پیام‌های تله تکس و پست‌های الکترونیکی که در هر نقطه از دنیا رد و بدل می‌شوند، دسترسی دارد و آن‌ها را بررسی می‌کند. شبکه اشلون از سوی آژانس امنیت ملی آمریکا کنترل می‌شود و با همکاری سازمان‌هایی چون، ستاد ارتباطات کل در انگلیس، مقر امنیتی ارتباطات در کانادا، ریاست امنیت دفاعی استرالیا و دایره‌ی امنیت ارتباطات کل در نیوزلند، فعالیت می‌کند. این سازمان‌ها تحت یک توافق‌نامه خیلی محرمانه در سال ۱۹۴۸ آغاز به کار کرد. نحوه فعالیت سیستم اشلون به این گونه است که ایستگاه‌های گیرنده داخلی خود را در همه نقاط دنیا مستقر می‌کند تا کلیه ماهواره‌ها، طول موج‌های کوتاه، ترافیک‌های ارتباطاتی سلولی و فیبرنوری را به دام بیاندازد و سپس آن را به رایانه‌های انبوه و با قابلیت بالای آژانس آمریکایی مزبور برای تجزیه و تحلیل و بررسی دقیق ارسال کند. این پیام‌های مختلف پس از دریافت توسط ایستگاه‌های شنود، شامل مکالمات و مکاتبات هستند که توسط یک سیستم تحلیلی هوشمند به دقت بررسی می‌شوند. هدف اصلی از فعالیت آژانس

---

[۱] perigee

[۲] ECHELON

مزبور ردیابی و کشف گروه‌های سیاسی ناشناس و فعالیت‌های آن‌ها است. سیگنال‌های بسیار اندکی می‌توانند از دام این گیرنده‌های الکترونیکی فرار کنند. بهره‌گیری از ایستگاه‌های گیرنده زمینی، کشتی‌های هوشمند در آب‌های هفتگانه‌ی دنیا و ماهواره‌های سری قوی در ارتفاعات ۲۰ هزار مایلی از سطح زمین قدرت فعالیت آژانس امنیت ملی آمریکا و اعضای پیمان UKUSA را افزایش داده است. مناطق جغرافیایی مختلف در سرتاسر دنیا بین اعضای این پیمان تقسیم شده است؛ به طوری که آمریکا در بخش بررسی سیگنال‌های ارتباطاتی قاره آمریکا، انگلیس در بخش اروپا، آفریقا و غرب روسیه، استرالیا در بخش آسیای جنوب شرقی، جنوب غربی اقیانوسیه و مناطق شرقی اقیانوس هند، نیوزلند در بخش شرکت‌های غربی اقیانوس آرام و بالاخره کانادا در بخش بررسی سیگنال‌های شمال روسیه، اروپای شمالی و هم‌چنین ارتباطات آمریکایی، فعالیت می‌کنند. روش کار اشلون به این نحو است که می‌تواند بخش زیادی از ارتباطات را با استفاده از رایانه ردیابی کند این کار به‌صورت خودکار و با استفاده از کلید واژها مورد نظر صورت می‌گیرد. که کلید واژه‌ها می‌توانند نظامی، سیاسی، امنیتی و حتی اقتصادی باشند. به‌عنوان مثال اتحادیه اروپا در سال ۸۱ اعلام کرد جاسوسی صنعتی بین سیزده تا یک‌صد و چهل و پنج میلیارد دلار به شرکت‌های اروپایی صدمه زده است.(hamshahri. org)

۸-۴-کاربرد نظامی ماهواره‌ها

۸-۴-۱-کاربرد ماهواره‌ها در عملیات زمینی

امروز استفاده نظامی از تصاویر ماهواره‌ای، به چند گروه تقسیم می‌شود. طراحی نظامی، مستلزم اطلاعات جاسوسی، برای ایجاد اطمینان از امکان بکارگیری نیروها در یک منطقه نا آشناست. این اطلاعات هر قدر کارآمدتر و امن‌تر باشد برای وارد آوردن حداکثر خسارات به نیروهای مقابل مفیدتر خواهد بود.

با توجه به آن چه گفته شد مهم‌ترین کاربردهای نظامی به صورت زیر خلاصه نمود.

۱. مطالعات جوی و پیش بینی وضع هوا در زمان جنگ برای مدت نسبتاً طولانی با توجه به پوشش وسیع داده‌های ماهواره‌های هواشناسی.

۲. تعیین موقعیت و آرایش یگان‌های پیاده، زرهی، توپخانه دشمن و تشخیص سنگرهای تجمعی و برآورد استعداد آن‌ها از نظر نیرو و امکانات.
۳. مطالعات زمینی و بررسی کیفیت و بافت زمین برای برآوردن امکان یا عدم نقل و انتقال یگان‌ها و ادوات و کاربرد مهندسی رزمی.
۴. بررسی و تشخیص موقعیت مراکز فرماندهی، قرارگاه‌ها و مراکز آمار دشمن.
۵. تشخیص نقل و انتقالات نظامی نیروها و ادوات نظامی دشمن و انجام فعالیت‌های مهندسی رزمی با توجه به مطالعات دوره‌ای تصاویر ماهواره‌ای و مقایسه تصاویر در زمان‌های مختلف.
۶. بررسی نتایج عملیات زمینی، هوایی، موشکی و برآورد خسارات وارده به دشمن.
۷. بررسی وضعیت آرایش نیروهای خودی و بررسی نقاط ضعف و تشخیص محل‌های شکاف و نقاط کور و ایجاد هماهنگی بین یگان‌ها.
۸. دست‌یابی به اطلاعات مربوط به موقعیت و وضعیت مراکز حساس مانند : تونل‌ها، مراکز آمادی، نقاط راهبردی و حساس نظامی در عقبه دشمن و تعیین هر یک از آن‌ها در تامین و پشتیبانی نیروهای دشمن.
۹. تشخیص موانع طبیعی و مصنوعی اعم از دپوها، کانال‌های حفر شده توسط دشمن، میادین مین، کمینگاه‌ها و تشخیص مراکز استتار و اختفا.
۱۰. تشخیص ادوات و نیروهای استتار شده دشمن با استفاده از مادون قرمز، شناسایی ادوات اصلی از ماکت‌ها و فریب دهنده‌ها.
۱۱. تشخیص سیستم‌ها و شیوه‌های آفندی و پدافندی دشمن.
۱۲. تولید مدل رقومی منطقه عملیات، تنظیم ساعت تک و چگونگی اختفا نیروها با تغییر مؤلفه‌های نوردهی و انتخاب معبرهای مناسب و مسیرهای دست‌یابی نیروها به هدف، تحلیل شیب زمین و استفاده از آن در جنگ، هدایت موشک‌های زمین به زمین هوشمند.
۱۳. شناسایی مناطق آلوده به مواد شیمیایی و میکروبی.
۱۴. امکان دیده بانی فعالیت‌های دشمن در شب و هوای ابری با استفاده از سنجندهای راداری.
۱۵. تولید عکس و نقشه برداری آشنایی با منطقه عملیاتی، در این روش نیروها قادر خواهند بود قبل از ورود به یک منطقه، آن جا را به‌طور دقیق مورد بررسی قرار داده و کلیه عوارض را به صورت بصری مشاهده و تحلیل کنند.

۱۶. استفاده از تصاویر سه بُعدی منطقه عملیاتی برای اندازه‌گیری شیب راه‌ها، هم‌چنین تحلیل نظامی منطقه از نظر توپوگرافی و امکان سنجی برای حرکت در شب با توجه به زاویه تابش نور مهتاب، هم‌چنین بررسی منطقه از نظر انتخاب نحوه سازمان‌دهی استقرار نیروها.

۱۷. استفاده از سیستم تعیین موقعیت جهانی جی. پی. اس در ناوبری و هدایت نیروها

۸-۴-۲-کاربرد تصاویر ماهواره‌ای در نیروی دریایی

۱. مطالعات جوی و پیش بینی وضع هوا در زمان و مکان مورد نظر

۲. تشخیص مسیرها و گذرگاه‌های دریایی و هم‌چنین بررسی عمق و عرض گذرگاه‌ها برای تعیین امکان حرکت یگان‌های شناورهای مختلف از نظر حجم و وزن آن‌ها (مدل سازی ارتفاعی بستر دریا).

۳. تشخیص موانع طبیعی اعم از برونزدهای صخره‌ای کف دریا و هم‌چنین رسوبات موجود در مسیرهای دریایی و امکان پهلو گرفتن کشتی‌ها جنگی و تدارکاتی هم‌چنین « ژئومورفولوژی »

۴. بررسی سواحل از نظر کیفیت زمین شناسی و بررسی این سواحل برای انتخاب تجهیرات مناسب به منظور جنگ در ساحل و پیاده شدن نیروها در آن

۵. شناسایی دقیق جزایر برای بهره‌گیری از آن‌ها در عملیات دریایی و یا هجوم به آن‌ها در صورتی که در دست دشمن باشد. معمولاً یک جزیره می‌تواند امکانات زیادی را برای عملیات و پشتیبانی نیروهای عمل کننده در خود داشته باشد.

۶. تعیین موقعیت دشمن و یگان‌های شناور مربوط به آن و هم‌چنین برآورد استعداد نیروهای دشمن.

۷. بررسی نقل و انتقالات دشمن اعم از نیرو و ادوات جنگی.

۸. بررسی وضعیت نیروهای خودی و تعیین نقاط ضعف آن‌ها در جزایر، سواحل و بر روی سطح آب.

۹. تشخیص جریان‌های آب گرم و سرد دریاها، هم‌چنین بررسی دمای سطحی آب.

۱۰. اندازه گیری جزر و مد دریا با مقایسه تصاویر ماهواره‌ای در زمان‌های مختلف

۱۱. دست‌یابی به اطلاعات مربوط به موقعیت مر اکز حیاتی، استراتژیک و حساس دشمن، هم‌چنین تعیین نقش آن‌ها در تدارکات نیروهای جبهه در دریا و سواحل.
۱۲. بررسی نتایج عملیات دریایی و خسارات وارده به دشمن در اثر عملیات دریایی و هوایی.
۱۳. بررسی و برآورد میزان آلودگی ناشی از جنگ دریایی.
۱۴. تشخیص موانع دریایی که توسط دشمن ایجاد گردیده است.
۱۵. اندازه گیری عمق دریا و سواحل با استفاده از تصاویر سنجندهای راداری.
۱۶. رهگیری و شناسایی زیردریایی‌ها با استفاده از تصاویر راداری. (فصلنامه خبری آموزشی فرماندهی ستاد، فخری مجید، ۱۳۷۸)

۸-۴-۳-کاربرد تصاویر ماهواه‌ای در نیروی هوایی

ماموریت نیروی هوایی در بالاترین سطح، ضربه زدن به توانایی دفاعی دشمن در عمق سرزمین وی می‌باشد. که این امر مستلزم داشتن اطلاعات دقیق از تاسیسات حیاتی، مراکز عمده صنعتی و نظامی است. تصاویر ماهواره‌ای امکان کسب آخرین اطلاعات از موارد ذکر شده را فراهم می‌آورد. کاربرد نیروی هوایی معمولاً در تک به آماجهایی درعمق موثر است و با انهدام و گسیختگی نیروهای دشمن آنان را از بکارگیری موثر نیروها در زمان و مکان دلخواه باز می‌دارد. ماموریت نیروی هوایی تاکتیکی است که مستقیماً به عملیات زمینی و دریایی کمک می‌کند. این عملیات عبارت است از:

تک به خطوط مواصلاتی دشمن، پشتیبانی نزدیک هوایی، عملیات ویژه ترابری هوایی، شناسایی و مراقبت فعالیت‌های موثر برای کسب برتری هوایی و تک به خطوط مواصلاتی دشمن که می‌تواند قابلیت انعطاف پذیری نیروهای دشمن را محدود ساخته مانع تقویت آنان می‌شود و برای فرماندهان خودی فرصت به‌دست گرفتن ابتکار عمل را از طریق آفند متقابل افزایش می‌دهد.

خلاصه‌ای از کاربرد تصاویر ماهواره‌ای در عملیات هوایی به شرح ذیل است:

۱. تشخیص مراکز مهم نظامی و استراتژیک دشمن.
۲. بررسی مسیر پرواز از نظر توپوگرافی با روش مدل سازی یا سه بُعدی و بهره‌گیری از امکانات پرواز دریا با یک دید نسبتاً واقعی از منطقه. « سیمولاتور[۱] »

[۱] Simulator

۳. شناسایی مسیرهای احتمالی نفوذ هواپیمای دشمن به کشور.
۴. بررسی مسیر پرواز از نقطه نظر مسائل امنیت پرواز.
۵. ارزیابی عملیات هوایی و بررسی خسارات وارده به دشمن، در بسیاری از عملیات‌ها، ارزیابی خسارات وارده در زمان هجوم امکان پذیر نیست اما دقایق و ساعاتی بعد تصاویر ماهواره‌ای کمک شایانی در تعیین میزان خسارات یا از کارافتادگی مورد هجوم ارائه می‌دهد.
۶. انتخاب محل مناسب برای استقرار یگان‌های پدافند هوایی.
۷. انتخاب محل مناسب برای نصب تجهیزات راداری و باند فرود اضطراری.
۸. شناسایی هواپیماهای ماکت از اصلی در پایگاه‌های هوایی دشمن (نشریه علمی و خبری ماهواره ها، عابدینی،مهدی، ۱۳۷۹)

۸-۵- سئوالات فصل:

۱. انواع مدارهای زمینی برای استقرار ماهواره ها را نام ببرید.
۲. مدارهای ثابت زمینی را توضیح دهید.
۳. شبکه ماهواره ای جاسوسی اشلون را توضیح دهید.
۴. کاربرد ماهواره ها در عملیات زمینی را توضیح دهید.
۵. کاربرد تصاویر ماهواره ای در نیروی هوایی را توضیح دهید.

فصل نهم: امنیت محیطی و فیزیکی

آن‌چه در این فصل می‌خوانید:

- **تعریف امنیت محیطی و فیزیکی**
- **خصوصیات فیزیکی محل نگهداری دیتا سنتر**
- **خصوصیات توپولوژیک محل نگهداری دیتا سنتر**
- **امنیت فیزیکی محل نگهداری سرور شبکه‌های ناامن**
- **امنیت فیزیکی محل نگهداری شبکه‌های مهم حساس و حیاتی**
- **کنترل دسترسی فیزیکی به محل نگهداری شبکه‌ها**
- **نکات ایمنی کابل کشی شبکه**
- **رعایت امنیت ابزار دیجیتال در زمان ارسال برای گارانتی و تعمیر و**
- **بازرسی دوره‌ای از محل نگهداری فیزیکی رایانه و چک لیست‌های لازم**
- **رعایت اصول پدافند غیر عامل در جایابی شبکه‌های رایانه‌ای**

۹- امنیت محیطی و فیزیکی

۹-۱-امنیت فیزیکی

امنیت فیزیکی یکی از جنبه‌های بسیار مهمی است که باید در امنیت شبکه‌های رایانه ی، مد نظر قرار بگیرد. امنیت فیزیکی را باید از دو دیدگاه مد نظر قرار داد: امنیت در برابر نفوذ افراد نامعتبر، امنیت در برابر شرایط اقلیمی و آسیب‌های ناشی از آن.

۹-۲-کنترل دسترسی فیزیکی

کنترل دسترسی فیزیکی، دسترسی به منابع رایانه و تجهیزات را محدود می‌کند و سیستم‌ها را در برابر خرابی‌های مختلف و صدمه‌های داخلی و خارجی، تا آنجایی که ممکن است، محافظت می‌کند. قبل از آنکه هر نوع سیستم کنترلی و امنیتی در یک مکان کاری پیاده‌سازی شود، در ابتدا باید سطح امنیتی که سیستم به آن نیاز دارد و برای تجهیزات مختلف مورد بررسی قرار گیرد، پس از آن بخش‌ها از دیدگاه در دسترس عموم بودن تقسیم‌بندی می‌شود: بخش‌های عمومی، بخش‌های در دسترس کارمندان، بخش‌های مراقبت شده، بخش‌هایی که تنها با مجوز قابل دسترسی است.

برای پیاده‌سازی کنترل دسترسی دو رویکرد وجود دارد: کنترل پیش‌گیرانه و کنترل امنیتی آشکارساز که سعی در تشخیص و تعیین حوادث غیرمترقبه، بعد از رویداد آن دارد. برای یک سیستم امنیتی کامل، هر دو نوع سیستم کنترل باید پیاده سازی شوند.

کنترل پیش‌گیرانه: در مورد کنترل پیش‌گیرانه می‌توان به موارد زیر اشاره نمود:

- از گاردهای امنیتی[۱] که اغلب در محل ورودی ساختمان‌ها و تجهیزات واقع می‌شوند برای جلوگیری از ورود و خروج افراد و تجهیزات غیر مجاز یا بازرسی و گشت زنی استفاده می‌شود.
- با ایجاد حصار پیرامون سازمان و ساختمان‌های حساس، می‌توان حداقل از ورود افراد غریبه جلوگیری کرد. این حصارها، باید دارای سیستم‌های هشدار دهنده باشند و یا تحت نظارت مداوم گاردهای امنیتی یا تلویزیون‌های مداربسته قرار داشته باشند.

---

[۱] Security Guards

- از کلیدها و قفل‌های رمزدار[۱]، برای کنترل دسترسی به بخش‌های محدود شده استفاده می‌شود.
- کنترل دسترسی افراد از طرق روش‌های تعیین هویت مانند داشتن کارت مخصوص و یا به صورت بیومتریک و با معیارهایی همچون اثر انگشت، اثر کف دست، صدا، نمونه‌های امضا و مرور عنبیه چشم و DNA افراد استفاده می‌شود.

کنترل امنیتی آشکار ساز: کنترل به روش آشکارسازی، نیازی به انجام روزانه توسط کارمندان ندارد، به عبارتی این سیستم‌ها در حالت نامرئی هستند، تا زمانی که شخص نامعتبر وارد سیستم شده باشد یا حادثه غیر مترقبه‌ای رخ داده باشد و ما نیازمندیم بدانیم چه حادثه‌ای رخ داده است (به کمک سیستم‌های مراقبتی و هشدار دهنده‌ها). مواردی را که در کنترل امنیتی آشکار ساز می‌توان مد نظر قرار داد عبارتند از:

- تشخیص دادن حرکات و جنب و جوش‌ها در سیستم
- تشخیص دادن دود وآتش
- سیستم‌های مراقبت بصری
- هشدار دهنده‌های الکترونیکی.

۹-۳- اعتبار سنجی فیزیکی

هدف از اعتبارسنجی فیزیکی، تعیین اعتبار افراد و دادن مجوز به آن‌ها می‌باشد تا از ورود و دسترسی افراد نامعتبر به سازمان و پیامدهای ناشی از آن جلوگیری شود. هر شخص برای دسترسی به بخش‌های محدود شده، باید از یک تست تعیین اعتبار، بگذرد. تست تعیین اعتبار، مجوز عبور برای افراد می‌باشد که می‌تواند شامل کارت‌های ورود (کارت معمولی، کارت تعیین هویت تصویری[۲]، کارت کدشده نوری[۳]، کارت نوار مغناطیسی[۴]، کارت‌های هوشمند)، سیستم علامت[۵] یا معیارهای بیومتریک (اثر انگشت، شبکیه یا عنبیه چشم، صدا، چهره افراد، شکل هندسی دست، سیستم DNA و نمونه امضا) باشد.

---

[۱] Cipher lock

[۲] Photo ID Card

[۳] Optical-coded Card

[۴] Magnetic Strip card

[۵] Badge system

۹-۴-منبع تغذیه وقفه ناپذیر[۱]

منبع تغذیه وقفه ناپذیر، برای محافظت تجهیزات در برابر وقفه‌ها و آسیب‌های الکتریکی، استفاده می‌شود. از واحدهای UPS کوچک می‌توان برای تجهیزات شبکه استفاده‌کرد، ولی اگر یک سیستم هشداردهنده در شبکه موجود نباشد که قبل از خالی شدن منابع تغذیه اصلی پیغامی مبنی بر restore کردن منابع به کاربرها بدهد، باعث به‌وجود آمدن مشکلاتی در شبکه می‌شود.

با استفاده ازUPS[۲] می‌توان مشکل هموار نگه داشتن ولتاژ را برطرف کرد. رایانه‌ها را به UPS وصل می‌کنند، اگر منبع تغذیه اصلی قطع شود، UPS ولتاژ کافی را برای رایانه‌ها فراهم می‌کند تا کاربرها بتوانند بعد از ذخیره اطلاعات، رایانه‌ها را خاموش کنند. اکثر UPSها، سیگنالی (پیغامی) مبنی بر قطع منبع تغذیه اصلی، به رایانه‌ها می‌فرستند.

۹-۵-سیاست‌های امنیت فیزیکی

بخش‌های مختلف سازمان بر حسب موقعیت و میزان امنیت مورد نیاز باید برای جلوگیری از بروز حوادث و کاستن اثرات آن‌ها تمهیداتی بیندیشد. برای این کار داشتن یک طرح مناسب برای دست‌یابی به اطلاعات حساس، حائز اهمیت می‌باشد. سیاست‌های امنیتی لازم جهت برقراری امنیت فیزیکی در سازمان را می‌توان در دسته‌بندی زیر ارائه داد.

۹-۵-۱-محافظت ساختمانی و جلوگیری از دزدی

- حفاظ‌های فیزیکی برای حفاظت یک ساختمان شامل کنترل دسترسی‌های فیزیکی، دیوارهای محکم، درها و پنجره‌ها می‌باشد. مناطق امن به همراه ساختمان‌ها باید از دسترسی‌های غیر مجاز، به‌وسیله‌ی کنترل دسترسی‌های فیزیکی، حفاظ‌ها و. . . حفاظت شوند.
- ساختمان‌ها، به جز در ساعت‌های کاری باید قفل شده باشند. ساختمان‌ها، خصوصاً اتاق‌های رایانه‌ای و بخش‌های مهم مربوط به سیستم‌ها (اتاق ارتباطات)، باید ۲۴ ساعت تحت نظارت پرسنل امنیتی باشند. اتاق‌های رایانه باید قفل باشند، اگر امکان دارد، این کار باید با کارت‌های الکترونیکی انجام شود. تنها باید تعداد محدودی از کارکنان به این بخش‌ها دسترسی داشته باشند و دسترسی به

---

[۱] UPS

[۲] Uninterruptible Power Supply

این بخش‌ها باید به‌صورت تصویری ضبط و ثبت شود. اطلاعات حساس تنها باید در اختیار کارمندانی قرار بگیرد که نیاز به داشتن آن دارند. در ضبط اطلاعات مربوط به دسترسی باید مواردی از قبیل چه کسی، به چه اطلاعاتی، در چه زمانی، و برای چه مدت ضبط شود.

- نگه داشتن لیستی از افرادی که اجازه دسترسی به بخش‌های خاصی مانند اتاق‌های رایانه، اتاق‌های سرور و اتاق ارتباطات دارند، از اهمیت بالایی بر خوردار است. باید مطمئن شد که حداقل جزئیات افرادی که اجازه دسترسی به بخشهای خاصی را دارند، مانند نام شخص، تاریخ و زمان ورود و خروج ثبت شود.
- دسترسی به مناطق خاص و محدود شده، باید مداوماً نظارت شود. روش‌های نظارت می‌تواند شامل: گاردهای امنیتی، سیستم‌های تشخیص الکترونیکی، یا سیستم‌های کنترل دسترسی الکترونیکی با ضبط اطلاعات مبنی بر قابلیت دسترسی به بخش باشد.
- تجهیزات موجود در ماجول سرورها، دسترسی از راه دور، تجهیزات توزیع و دسترسی، هسته و اینترنت بایست در رک‌های در بسته و در اتاق سرورها به صورت کاملاً امن نگهداری شوند. اتاق سرورها بایست سنسورهای تشخیص دود و کپسول‌های آتش نشانی، سنسورهای تشخیص‌دهنده حرکت نصب شوند. پنجره این اتاق‌ها باید پوشانده شود و درب آهنی و محکم برای آن‌ها سفارش داده شود.
- جهت اعمال کنترل بر سرمایه‌ها، همه‌ی اقلام تجهیزات باید دارای شناسه‌ی یکتا باشند و در فهرست اموال ثبت شوند. نگهبانان امنیتی باید به کنترل تجهیزات یا رسانه‌هایی که از اتاق‌ها/فضاها یا ساختمان‌ها بدون اجازه خارج می‌شوند، بپردازند. اطلاعات حساس و نرم افزارهای اختصاصی نگهداری شده روی رسانه‌های قابل حمل (مانند دیسکت و. . .) باید به‌صورت ویژه‌ای حفاظت شوند.
- تمامی افرادی که اجازه دسترسی به بخش‌های محدود شده را دارند، باید به اصطلاح علامت‌گذاری شوند و نیاز به پوششی که شامل علامت دسترسی تائید شده می‌باشد، دارند. علامت دسترسی باید دارای حداقل اطلاعات از جمله: شماره سریال کنترل علامت که باید مُهر زده باشد، تصویر رنگی از شخص و پیوست خاص بخش محدود شده، باشد.

- در سایت‌های مختلف برای نگهداری فیزیکی رایانه‌ها و سایر تجهیزات سخت‌افزاری بایست مسئول سایت وجود داشته باشد.
- برای محافظت از نسخه‌های پشتیبان اطلاعات سازمان باید سیاست‌های امنیتی شدیدی جهت جلوگیری از ورود افراد غیر مجاز به محل نگهداری پشتیبان‌ها طراحی نمود.

۹-۵-۲-محافظت در برابر آتش

- تجهیزات و فضاهای بسته، باید در برابر گسترش آتش، از جای دیگر در ساختمان، یا نزدیک ساختمان‌ها محافظت شود. خطر آتش در نزدیکی اتاق‌ها/فضاهای قرارگیری تجهیزات باید به حداقل برسد. هم‌چنین باید اتاق‌ها/فضاهای قرارگیری تجهیزات کلیدی و مهم در برابر شروع آتش محافظت شوند. حفاظ‌ها باید شامل ردیاب‌ها، زنگ خطرها و بازدارنده‌های آتش و دود باشند. توجه به این نکته ضروری است که محافظت در برابر آتش، منجر به خسارت از طریق آب یا سایر ابزارهای خاموش کننده‌ی آتش نشود.
- باید سنسورهایی برای کنترل دمای اتاق، میزان رطوبت، میزان غبار و گرد و خاک، در مکان‌های مهم نصب شده باشد که گزارش‌های مربوطه را از طریق SNMP یا SYSLOG به مسئولین اعلام نماید.
- باید از عواملی که می‌تواند باعث بروز آتش شود شامل نگهداری نادرست مواد آتش‌زا، کمبود عایق و روکش روی کابل‌های اصلی و مرکزی، نبود سیستم‌های اعلان خطر به هنگام حریق و. . . جلوگیری نمود. روش‌هایی که می‌توان برای جلوگیری و کنترل آتش در پیش گرفت شامل نصب دستگاه‌های یابنده‌ی دود نزدیک به سیستم‌ها، نصب سنسورهائی در مجراهای ورودی و خروجی سیستم‌های تهویه، استفاده از آبپاش‌های اتوماتیک و کپسول‌های دی‌اکسیدکربن و استفاده ازسیستم‌های تخلیه هالون می‌باشد.

۹-۵-۳-محافظت در برابر آب / مایعات

- تمهیدات یا امکانات مورد نیاز، در هر فضایی که ممکنست خطر اتفاق افتادن سیل یا چکیدن آب یا دیگر مایعات وجود دارد نباید قرار گیرند. حفاظت مناسب باید در جایی که خطر سیل وجود دارد، اعمال شود.

- عواملی که می‌تواند باعث جاری شدن آب به داخل ساختمان‌ها شود شامل باران، قطع و شکستگی در منابع آب، نقص در سیستم‌های آب پاش، خراب‌کاری عمدی در مسیر جریان آب در لوله‌ها و مسدود کردن عمدی آن‌ها و. . . می‌باشد که باید امکان وجود آن‌ها را به دقت بررسی نموده در صورت امکان آن را برطرف نمود. روش‌هایی که برای پیش‌گیری از نشت آب می‌توان در نظر گرفت شامل نگهداری عایق‌های ضد آب در کنار تجهیزات رایانه‌ای، نصب سنسورهای حساس به آب روی کف ساختمان و. . . هستند.

۹-۵-۴-محافظت در برابر حوادث طبیعی

- ساختمان‌های محل قرارگیری تجهیزات مهم، باید در برابر رعد و برق محافظت شوند. هم‌چنین خود تجهیزات باید در برابر آثار رعد و برق محافظت شوند. حفاظت در برابر دیگر حوادث طبیعی، با اجتناب از فضاهایی که مستعد اتفاق افتادن آن حوادث هستند، و با داشتن راهبرد و طرح استمرار تجارت سازمان در محل مناسب قابل اجرا است.
- در صورتی که تجهیزات و سیستم‌ها در منطقه زلزله‌خیز واقع شده باشند، باید برای پیش‌گیری از وارد آمدن صدمات ناشی از نوسانات به سیستم‌ها و تجهیزات می‌توان راهکارهای زیر را در پیش گرفت: تجهیزات و سیستم‌ها در جای خود محکم شده، ترجیحاً بر روی پایه‌های لاستیکی قرار داده شوند. از قرار دادن تجهیزات و سیستم‌ها در زیر وسایل سنگین یا در جاهای بلند پرهیز شود. هم‌چنین از تجهیزات ضد زلزله و نوسان برای رایانه‌ها استفاده گردد.

۹-۵-۵-محافظت از سیم کشی‌ها

- سیم کشی‌های متداول یا داده را حمل می‌کند؛ یا سرویس‌های ICT را که باید از قطع، آسیب و بار اضافی، حفاظت شوند، پشتیبانی می‌کند. سیم‌کشی باید به صورت فیزیکی در برابر آسیب‌های عمدی یا غیر عمدی، محافظت شود. دقت در طراحی و توجه به توسعه در آینده، می‌تواند از به وجود آمدن مشکلات زیاد، پیش‌گیری کند. هر جایی که ممکن باشد، باید سیم‌کشی‌های اختصاص یافته، در برابر استراق سمع حفاظت شوند.
- کابل‌های فیبرنوری و UTP عبوری از کانال‌ها بایست با دقت انتقال یابند و در لوله‌های PVC قرار گیرند. دسترسی به کابل‌های موجود در کانال‌ها توسط افراد

عادی نبایست به راحتی امکان‌پذیر باشد. درب کانال‌ها بایست همیشه بسته باشد.

۹-۵-۶-محافظت در مقابل برق

- همه‌ی تجهیزات ICT باید در صورت نیاز، در برابر قطع برق محافظت شوند. یک منبع برق مناسب باید تولید برق برای تجهیزات را بدون هیچ‌گونه قطعی، تأمین نماید.
- برای سیستم‌های خاص و مهم مثل سیستم‌های تلفنی، رایانه‌های سرور، یا تجهیزاتی که کنترل فرآیند را در صنعت و بیمارستان‌ها بر عهده دارند، از واحدهای UPS برخط که در آن‌ها رابط اصلی بین مصرف‌کننده‌های توان و منابع تغذیه اصلی UPS بوده، تمامی ولتاژهای مصرف‌کننده‌ها از طریق آن فراهم می‌شود، استفاده نمود.
- سیستم‌های Line-Interactive UPS، به‌ترین نوع برای وضعیت‌هایی است که نوسان منبع، یک رویداد عادی محسوب می‌شود. در این UPS نوسانات می‌تواند به کمک مبدل‌های داخل UPS به جای باتری، کنترل شود. از آن جایی که، این نوع سیستم‌ها، دائماً در تمام مدت زمان کاری، خط منبع را نظارت می‌کنند، و همیشه در حالت آماده‌باش قرار دارند، زمان تبدیل آن، خیلی کم‌تر از سیستم‌های برون خط می‌باشد که در آن‌ها مصرف کننده‌های توان، مستقیماً از منابع تغذیه اصلی تغذیه شده، تنها در صورت بروز خرابی، به‌طور اتوماتیک به UPS وصل می‌شوند.
- معمولاً در انتخاب UPS، آن چه که پیش‌نهاد می‌شود آن است که گنجایش سیستم UPS، حداقل ۲۵٪ بیش‌تر از کل مجموع نیازهای توان تجهیزات متصل به منبع اصلی باشد. برای نمونه رایانه رومیزی که با توان بین ۱۸۰ تا ۲۸۰ ولت‌آمپر کار می‌کند، نیاز به UPS با توان ۳۰۰ ولت‌آمپر دارد.
- بخش‌هایی که در آن‌ها، رایانه‌ها، در یک اتاق قرار دارند، می‌توانند تمامی تجهیزات را به یک UPS مرکزی وصل کنند که این عمل از لحاظ هزینه نیز به صرفه می‌باشد. در هر صورت، هنگامی که تجهیزات در اتاق‌ها و مکان‌های مختلف قرار دارند، منطقی است که از UPS توزیع شده در مکان‌های مناسب، استفاده شود.

۹-۶- تعیین هویت و تصدیق اصالت (I & A)

تعیین هویت روشی است که به‌وسیله آن شخص هویت ادعا شده خویش را برای سیستم، اثبات می‌کند. در تصدیق اصالت، اعتبار این دعوی تصدیق می‌شود. در عمل تشخیص هویت اولین گام از امنیت است. این فرآیند به سه صورت کلی صورت می‌پذیرد:

- براساس آن‌چه یک فرد می‌داند (کلمه‌ی عبور، شماره شناسایی، کلید رمزنگاری)
- آن‌چه یک فرد همراه دارد (کارت ATM، کارت هوشمند)
- آن‌چه یک فرد هست (خصوصیات زیستی مانند اثر انگشت، صدا، دست خط)

البته روش‌های تشخیص هویت ترکیبی نیز وجود دارد که از مزایای چندین روش بهره می‌برد.

از مزایای روش اول می‌توان به سادگی، کم هزینه بودن، قابلیت تعویض ساده و امن بودن محل نگهداری آن اشاره کرد و از معایب آن می‌توان از سادگی نفوذ به سیستم، مشکل به خاطر سپردن و فراموش کردن نام برد. علی‌رغم معایب زیاد آن به علت سادگی، پراستفاده‌ترین روش است.

در روش دوم اساس کاربر استفاده از یک کلید است که می‌تواند قفل ساختار اطلاعاتی سیستم را باز کند. این کلید می‌تواند نرم‌افزاری و با کمک تکنولوژی رمزنگاری (که در بخش مربوطه بحث خواهد شد) باشد و یا سخت‌افزاری و با کمک یک نشانه[۱] که برای نگهداری فیزیکی اطلاعات سری به کار می‌رود.

از مزایای این روش این که معایب روش فوق را ندارد و از معایب آن این که هزینه نسبتاً بالایی دارد، به سخت‌افزارهای اضافی روی هر رایانه نیاز است و ممکن است گم یا دزدیده شود.

در روش سوم اعتبارسنجی با عنوان بیومتریک شناخته می‌شود و از ویژگی‌های منحصر به فرد هر انسان جهت شناسایی او استفاده می‌کند. از مزایای آن این که امکان به اشتراک‌گذاری، احتمال گم شدن یا فراموش شدن ندارد و از معایب آن این که بسیار پرهزینه بوده احتمال خطای تشخیص رایانه در مورد شباهت‌های زیاد مثل دوقلوها وجود دارد و در صورتی که آن ویژگی بیومتریک در مورد کسی از بین برود (مثلاً انگشت دست او قطع شود) دیگر قادر به کار با سیستم نخواهد بود.

---

[۱] Token

از روش‌های ترکیبی می‌توان به روش استفاده از نشانه و کلمات عبور یک بار مصرف است. در روش کلمات عبور یک بار مصرف[۱] کاربر در هر بار ورود به سیستم از کلمه عبور جدیدی استفاده می‌کند. این کلمه عبور معمولاً به صورت ترکیبی از بعضی پارامترهای تصادفی تولید شده توسط سیستم به همراه کلمه رمزی کاربر ایجاد می‌شود.

۹-۶-۱- سیاست‌های تشخیص هویت

- سازمان باید با توجه به میزان نیاز امنیت برای هر سرویس و منبع اطلاعاتی که ارائه می‌دهد روش مناسب تشخیص هویت کاربران را تعیین کرده، جهت اجرای طرح انتخابی برنامه‌ریزی کند. به عنوان مثال برای دسترسی به اطلاعات شعبات مرکزی بهتر است از تشخیص هویت به صورت بیومتریک برد.
- لیست کلیه کاربران مجاز به دسترسی به هر منبع تعیین شده باشد و هیچ یک از منابع سازمان نباید بدون تشخیص هویت قابل دسترسی باشد.
- سازمان باید درخصوص مدیریت رمز عبور کاربران سیاست و دستورالعمل‌هایی تهیه کرده باشد. این سیاست‌ها باید حداقل حاوی مطالب زیر باشد:
  - استفاده از رمز عبور در سیستم‌عامل ایستگاه‌های کاری و سرورها و تجهیزات شبکه با ذکر حداقل طول آن
  - استفاده از ترکیب حروف کوچک و بزرگ و اعداد در رمز عبور
  - تغییر رمز عبور پیش‌فرض کلیه نرم‌افزارها و سخت‌افزارها
  - عدم استفاده از رمز عبور یکسان در موارد مختلف
  - سیاست‌هایی برای تغییر دوره‌ای رمز عبور کاربران و مدیران و تعیین حداکثر مدت مجاز آن
  - حذف Accountهای غیرضروری

۹-۷-کنترل دسترسی[۲]

دسترسی به معنای توانایی انجام کاری با یک منبع اطلاعاتی و رایانه‌ای است و کنترل دسترسی فرآیندی است که از طریق آن این توانایی فعال یا محدود می‌شود. کنترل دسترسی شامل دسترسی فیزیکی هم هست که در بخش امنیت فیزیکی به آن پرداختیم. هدف از این کار

---

[۱] One-time Password

[۲] Access control

تأمین محافظت از منابع، با جلوگیری از دسترسی غیرمجاز، جامعیت و دسترس‌پذیری با محدود کردن تعداد کاربران و فرایندها، اطمینان از اطلاعات است.

فرآیند پیاده‌سازی کنترل دسترسی شامل تعریف اطلاعات و مجوزهای دسترسی به آن اطلاعات و بعد از آن نسبت دادن این مجوزها و اختیارات برای دست‌یابی به داده‌ها به کاربران یا نقش‌های آن‌ها است. به طور کلی مجوز دسترسی شامل اجازه خواندن، نوشتن، به‌روزرسانی، ایجاد و حذف است. هم‌چنین مجوزهایی برای شروع یا متوقف کردن یک برنامه یا سرویس و یا دست‌یابی به سیستم‌های دیگر نیز در این دسته قرار می‌گیرد.

کنترل دسترسی براساس موارد زیر صورت می‌گیرد:

- هویت و شناسه‌های یکتا
- نقش‌ها
- موقعیت‌های فیزیکی یا منطقی منابع
- زمان
- تراکنش
- محدودیت‌های یک سرویس و حالت‌های مختلف دسترسی

مکانیزم‌های زیادی برای کنترل دسترسی‌های داخلی و خارجی وجود دارد که برخی آن‌ها به صورت زیر است:

- کنترل دسترسی داخلی: به معنای جداسازی آن‌چه کاربران می‌توانند با منابع سیستم انجام دهند و آن‌چه نمی‌توانند، است که ممکن است از طرق مختلف مانند استفاده از کلمات عبور، رمزنگاری، لیست‌های کنترل دسترسی یا ACLها که لیستی از کاربران و نوع دسترسی آن‌هاست، استفاده از اینترفیس‌های کاربر محدود شده از طریق منوها، منظرهای بانک اطلاعاتی و. . . که به کاربر اجازه تقاضای اطلاعات غیرمجاز را نمی‌دهد و برچسب‌های امنیتی[۱] اعمال شود.
- کنترل دسترسی خارجی: استفاده از تجهیزات حفاظت پورت یا PPD[۲] ، دیواره‌های آتش یا دروازه‌های امن، امنیت فیزیکی، مکانیزم‌های تشخیص هویت. . . که در اینجا منظور از کنترل دسترسی همان نوع اول می‌باشد.

۹-۷-۱-سیاست‌های کنترل دسترسی

[۱] Security Label

[۲] Port Protection Device

- هر بخش باید نیازمندی‌های خود را برای کنترل دسترسی تعریف و مستندسازی کند. قوانین کنترل دسترسی برای هر کاربر یا گروه کاربران باید به طور واضح در سیاست‌های دسترسی شرح داده شود و به کاربران و فراهم‌کنندگان سرویس باید دستورالعمل‌های واضحی از نیازمندی‌های تجاری بر پایه کنترل دسترسی ارائه شود. این دستورالعمل‌ها به صورت پروفایل‌های استاندارد دسترسی کاربران برای هر دسته مشخص از شغل‌ها طراحی و موجود باشد.
- برای هر کاربر یا گروهی از کاربران، سیاست کنترل دسترسی باید به وضوح تعریف شده باشد. این سیاست باید امتیاز دسترسی را بر طبق نیازمندی‌های تجاری، مانند دسترسی پذیری و سودمندی، اهداء نماید. ایده‌ی اصلی باید به‌صورت "در صورت لزوم امتیاز بیش‌تر، در صورت امکان امتیاز کم‌تر" باشد.
- در تعریف قوانین دسترسی باید همه اطلاعات و موقعیت‌ها را در نظر گرفت برای این کار توصیه می‌شود قوانین به صورت "همه موارد ممنوع به جز. . . " تعریف شود به جای "همه موارد مجاز به جز. . . ".
- برای نام‌نویسی ورود کاربران و خروج آن‌ها به منظور دست‌یابی به همه سیستم‌های اطلاعاتی چند کاربره و سرویس‌های آن‌ها باید روال‌هایی رسمی وجود داشته باشد. اختصاص و استفاده از اختیارات باید محدود و کنترل شده باشد. تخصیص کلمات عبور کاربران باید کنترل شده و از یک فرآیند مدیریت رسمی صورت گیرد.
- کنترل دسترسی به رایانه به منظور جلوگیری از هرگونه دسترسی غیر مجاز به رایانه ، انجام می‌شود. این امر باید امکان پذیر باشد که هرکاربر مجاز و رویدادنامه‌ی [۱] مربوط به تلاش موفق یا ناموفق برای ورود به سیستم را، بتوان تعیین هویت و بازبینی کرد. در این حفاظ می‌توان از کلمات رمز یا هرگونه روش‌های دیگر I&A نیز استفاده کرد.
- کنترل دسترسی باید جهت محافظت از داده و سرویس‌ها روی یک رایانه و یا در محدوده شبکه، از دسترسی‌های غیر مجاز جلوگیری به عمل آورد. این کنترل‌ها می‌تواند با کمک مکانیزم‌های I&A مناسب، واسط مناسب بین سرویس‌های

[۱] Log file

شبکه و پیکربندی شبکه به‌طوری که تنها دسترسی‌های مجاز روی سرویس‌های IT امکان پذیر باشد (محدودیت تخصیص امتیازات)، انجام شود.

- کلیه قوانین دسترسی تعیین شده برای کاربران باید به‌صورت منظم بازبینی شوند و در صورتی که نیاز به تغییرات امنیتی یا تجاری در دسترسی وجود داشته باشد، عملیات به روز آوری صورت گیرد. امتیازات دسترسی‌های تعیین شده باید به‌صورت مکرر، جهت اطمینان از عدم سوءاستفاده، بازبینی شوند. امتیازات دسترسی باید در صورتی که طولانی‌تر شدن آن لزومی نداشته باشد، پس‌گرفته شود.
- کلیه وظایف انجام شده در جهت پشتیبانی IT، باید در رویدادنامه ثبت شود. رویدادنامه‌ها شامل‌تلاش‌های موفق و ناموفق برای ورود به سیستم، ورود به سیستم جهت دست‌یابی به داده، عمل‌کردهای مورد استفاده سیستم و. . . می‌باشد. هم‌چنین نقائص باید ثبت شود، و این رویدادنامه‌ها باید به‌طور منظم بازبینی شود. این داده‌ها باید مطابق با قوانین حفاظت داده‌ها و محرمانگی، استفاده شوند. برای مثال، داده‌ها ممکن است برای یک دوره‌ی زمانی محصور شده و تنها در هنگام تشخیص نقض امنیت استفاده شوند.
- یک فرآیند رسمی به طور منظم و در فواصل زمانی مناسب باید حقوق دست‌یابی کاربران را مرور و در صورت لزوم بازنگری نماید.
- کاربران باید فقط به طور مستقیم و به سرویس‌های ی که برای آن‌ها مجاز است، دست‌یابی داشته باشند.
- دست‌یابی برای کاربران راه دور، باید بخشی از روال شناسایی و تصدیق اصالت باشد.
- دست‌یابی به پورت‌هایی که برای عیب‌یابی از راه دور استفاده می‌شوند، باید کنترل شده باشد.
- برای گروه‌های مجزا در شبکه، کنترل‌هایی به منظور سرویس‌های اطلاعاتی، کاربران و سیستم‌های اطلاعاتی باید معرفی شوند.
- در شبکه‌های اشتراکی باید کنترل‌های مسیریابی به منظور اطمینان از اتصالات رایانه‌ها و جریان اطلاعات برطبق سیاست کنترل، دست‌یابی کاربردهای فعالیت‌های تجاری سازمان صورت گیرد. دست‌یابی به سرویس‌های اطلاعاتی باید توسط یک فرآیند ورود امن صورت گیرد.

- همه کاربران برای فعالیت‌هایشان باید دارای یک شناسه منحصر به فرد قابل ردگیری و کنترل باشند. یک سیستم مدیریت کلمه عبور در جایی که بتواند به طور مؤثر و متعامل از کیفیت کلمه عبور اطمینان حاصل نماید، باید وجود داشته باشد. فعالیت‌های غیرمجاز باید ثبت شده، سیستم‌های نظارتی برای کنترل دست‌یابی باید وجود داشته باشد. استفاده از برنامه‌های سیستم باید به دقت کنترل و محدود شده باشد.

۹-۸- آسیب‌های سیستم می‌تواند از طریق موارد زیر کاهش یابد :

۹-۸-۱-دفاع در عمق :

مدیریت آسیب‌پذیری از طریق سطوح مختلف حفاظت در مقابل دسترسی افراد غیرمجاز به اطلاعات طبقه بندی شده اجازه انعطاف می‌دهد.

حفاظت پیش‌گیرانه، از مسیر چند لایه معروف به «دفاع در عمق» استفاده می‌کند. دفاع در عمق یعنی ترکیب اقدامات مختلف برای سخت نمودن دسترسی افراد کنجکاو یا کارمندانی که نیازی به دانستن ندارند. این اقدامات باید یک‌دیگر را حمایت نمایند. آن‌ها ممکن است امور زیر را کنترل نمایند :

- فضای فیزیکی
- آیین نامه‌ها
- کارمندان
- فن آوری

اقدامات حفاظت فیزیکی باید به گونه‌ای طراحی شود که با تهدیدات افراد مریض که در گذشته صلاحیت تردد به سازمان، ساختمان یا منطقه امن داشته‌اند مقابله نماید، چه رسد به افراد خارجی و بی ارتباط با سازمان.

دفاع‌های اصلی فیزیکی آن‌هایی است که به اطلاعات حفاظت شده، نزدیک‌تر است. در یک سازمان دولتی با اطلاعات طبقه بندی شده زیاد، ممکن است اقدامات احتیاطی دیگری برای دفاع در عمق یا حفاظت در مقابل اشتباه انسانی نیاز داشته باشد. این اقدامات ممکن است شامل موارد ذیل شود :

- حفاظت از کلیدها و مخزن‌هایی که اطلاعات طبقه‌بندی شده در آن نگهداری می‌شود.
- اقدامات مربوط به کنترل دسترسی‌ها
- سیستم‌های هشدار دهنده‌ی حفاظتی برای کشف دسترسی‌های غیر مجاز و اعلام خطر

- موانع فیزیکی برای بازداشتن، کشف و تأخیر در ورود افراد غیرمجاز

اقدامات فیزیکی ممکن است با گام‌های شخصی و آیین‌نامه‌ای مانند موارد ذیل تکمیل شود:

- اصل دانستن در حد نیاز، محدود کردن دسترسی به اطلاعات رسمی به کسانی که برای انجام وظایف‌شان بدان نیاز دارند.
- یک سیستم طبقه‌بندی حفاظتی، اطلاعاتی را که نیاز به حفاظت خاص دارند شناسایی می‌کند.
- یک سیستم حفاظت کارکنان که صلاحیت مناسب برای دسترسی به اطلاعات رسمی را تضمین نماید.
- مراقبت‌های قانونی که آسیب‌پذیری سیستم‌های فن‌آوری اطلاعات اداره را کاهش می‌دهد.
- برنامه آموزشی یا تربیتی

۹-۸-۲- تطبیق محیط :

طرح مراقبتی لایه بندی داخل سازمان، ساختمان یا منطقه امن می‌تواند آسیب‌ها و زیان‌های حفاظتی را کاهش دهد.

۹-۸-۳- محیط حفاظت فیزیکی :

حفاظت فیزیکی می‌تواند از تشکیل چند محیط حفاظتی اطراف مرکز ذخیره‌ی اطلاعات طبقه بندی شده، به‌وجود آید. یک محیط حفاظتی، هر مانع حفاظتی چون دیوار، کارت کنترل‌تردد یا میز پذیرش کارکنان می‌باشد.

تعیین آسیب‌پذیری به تصمیم گیری در خصوص موقعیت، استحکام و طبیعت هر مانع کمک می‌کند.

یک محیط ممکن است :

- مرزهای طبیعی
- قفس یا دیوار
- دیوارهای بیرونی ساختمان
- تقسیم بندی داخل ساختمان باشد.

هدف یک محیط، منع فیزیکی، روان شناسی یا قانونی افراد غیرمجاز می‌باشد.

حفاظت محیط ممکن است به وسیله روش‌های زیرافزایش یابد :

- سیستم کشف مزاحم محیطی
- نور افکن‌های حفاظتی
- تلویزیون‌های مدار بسته
- نگهبانان حفاظتی
- تابلوها و اعلامیه‌های هشدار دهنده.

۹-۹-کنترل دسترسی به شبکه :

هدف : حفظ دسترسی به شبکه

نحوه‌ی دسترسی به خدمات شبکه‌های داخلی و خارجی باید کنترل شود.

کنترل‌ها از این جهت ضروری است که کاربران به خدمات شبکه‌ها و خود شبکه دسترسی دارند.

خدمات شبکه که باید افشا شوند شامل موارد زیر می‌شود :

- واسطه بودن متناسب بین شبکه سازمان و شبکه‌های عمومی یا شبکه‌های مربوط به سازمان‌های دیگر.
- مکانیسم‌های شناسایی کاربران و تجهیزات.
- کنترل دسترسی کاربران به خدمات اطلاعاتی.

۹-۹-۱-مدیریت شبکه :

دسترسی به شبکه و رایانه باید به وقت مدیریت شود تا :

- خدمت بهینه به کارمندان ارائه شود.

دائماً تدابیر حفاظتی از طریق سیستم‌های اطلاعاتی به کار روند.

کنترل‌های آیین نامه‌ای برای اشراف و حفظ حفاظت شبکه‌ای می‌تواند موارد ذیل را در بر گیرد :

- تجمع و یا تفکیک مسئولیت‌ها
- کشف مزاحم و یا سوء استفاده
- راهنمایی برای مدیریت ابزار همچون مسیریاب‌ها (روتِرها) دیواره آتش (فایروال)
- مدیریت کلیدها و تجهیزات رمز

سازمان‌ها ممکن است به ارتباط داخلی یا شبکه رایانه‌ای خارج از مرزهای سنتی نیاز داشته باشند. ریسک دسترسی غیرمجاز و نقض مقررات حفاظت رایانه‌ای است. عوامل حفاظتی

برای شبکه‌ها که حدود سازمانی را به هم وصل می‌کند باید کنترل اضافی به شرح ذیل به عمل آورد :

- داخل شبکه‌ها برای جدا کردن گروهای کاربر
- بین شبکه‌ها، برای حفظ اطلاعات به هنگام انتقال

۹-۹-۲- ایزوله کردن سیستم فعال :

به طور خاص سیستم‌های حساس ممکن است روی رایانه‌ی خاص نصب شوند یا با شراکت دیگر سیستم‌های ابزاری مورد اعتماد به پردازش منابع اطلاعات بپردازد. حساسیت یک سیستم ابزاری باید به طور واضح شناسایی و در سیاست حفاظتی سیستم و برنامه حفاظتی آن ثبت گردد.

دسترسی از طریق کنترل از راه دور به یک شبکه‌ی اداری باید مرتب و مدیریت گردد:

- فقط اجازه‌ی خدمات مورد نیاز را بدهد.
- فقط به هنگام نیاز در دسترس قرار گیرد.
- فقط مورد استفاده کاربران خاص و شناسایی شده قرار گیرد.

۹-۹-۳-کنترل دسترسی سیستم عامل :

هدف : ممانعت از دسترسی غیرمجاز به رایانه

تجهیزات حفاظتی در سطح سیستم عامل باید دسترسی به منابع رایانه را محدود سازد. این تجهزات باید :

کاربر مجاز را شناسایی و اگر لازم بود پایان یا موقعیت دسترسی موفق و ناموفق سیستم را ثبت نماید.

هر کجا مناسب بود دفعات ارتباط را محدود کند.

روش‌های دیگر کنترل دسترسی مانند :

مقابله به مثل.

ممکن است به‌وسیله آسیب کاری توجیه شود. کنترل نحوه و سطوح دسترسی به اطلاعات که شامل مدیریت کاربران، مسئولیت‌های کاربران، کنترل دسترسی به شبکه، کنترل دسترسی راه دور و نمایش دسترسی‌ها می‌باشد.

مطابق توضیحات دامنه کنترل دسترسی، شامل این بخش‌هاست : ۱) تعریف ۲) علل اهمیت ۳) انواع کنترل ۴) مدل‌های کنترل ۵) کشف مخاطرات ۶) علائم منفرد روی سیستم‌ها ۷) شناسایی و اعتبارسنجی

متخصصین سیستم‌های امنیت اطلاعات باید نسبت به پیاده سازی کنترل دسترسی به منظور حفظ موجودیت، قابلیت اعتماد و جامعیت اطلاعات اطمینان حاصل کنند.

در دنیای شبکه‌های رایانه‌ای همان‌گونه که کنترل دسترسی در سیستم‌های توزیع شده اهمیت پیدا می‌کنند در سیستم‌های متمرکز نیز حائز اهمیت می‌باشند.

متخصصین باید دانش کافی نسبت به حمله‌ها، مخاطرات و آسیب‌ها که با زیرساخت‌های سیستم‌های اطلاعات ارتباط نزدیکی دارند، داشته باشند و نسبت به ممانعت از نفوذ آسیب‌ها اقدام کنند.

منظور از یک سیستم کنترل دسترسی، سیستمی است که بر پایه یکی از مکانیزم‌های شناسایی به جای‌گزینی یک قفل و کلید مکانیکی می‌پردازد.

به طور مثال در یک سیستم AC که با روش رمز شناسایی (PIN) کار می‌کند، با وارد نمودن یک رمز خاص قفل برقی متصل به چارچوب در، عمل نموده و در باز می‌شود. بر مبنای این تعریف یک سیستم AC به رفع مشکل ذاتی تمام سیستم‌های مکانیکی مزیت دارد و آن محدودیت تکثیر کلید است به طوری که برای یک قفل فقط می‌توان یک کلید را مشابه سازی نمود و برای افراد مختلف استفاده کرد، بدیهی است که در صورت گم شدن کلید امنیت قفل خدشه‌دار می‌گردد. سهولت اختصاص کلیدهای شناسایی مختلف به یک قفل و نیز سهولت حذف و مدیریت کلیدها از مهم‌ترین مزایای بهره گیری از یک سیستم AC می‌باشد. کنترل دسترسی در سیستم‌های اطلاعات و شبکه‌ها به منظور حفظ قابلیت اعتماد، جامعیت و دسترس پذیری آن‌ها ضروری می‌باشد.

در ادامه هر یک از این موارد تشریح شده‌اند.

قابلیت اعتماد :

باعث جلوگیری از فاش شدن اطلاعات برای افراد یا فرآیندهایی که مجاز نمی‌باشد، می‌گردد.

جامعیت :

از طریق اهداف زیر بیان می‌گردد :

۱- ممانعت از تغییر اطلاعات توسط افراد غیرمجاز

۲- ممانعت از تغییر غیرعمدی توسط افراد مجاز

۳- محافظت از سازگاری داخلی و خارجی

الف- سازگاری داخلی باعث تضمین سازگاری داده‌ها می‌شود. به عنوان مثال، فرض کنید یک بانک اطلاعاتی تعداد واحدهای یک قلم خاص در هر دپارتمان یک سازمان را نگهداری

می‌کند. مجموع تعداد واحدها در هر دپارتمان باید با تعداد واحدها که در داخل بانک اطلاعاتی ضبط شده یکسان باشد.

ب- سازگاری خارجی متضمن سازگاری داده‌های ذخیره شده در بانک اطلاعاتی با دنیای واقعی است. مثال تشریح شده در قسمت قبلی را برای سازگاری خارجی این گونه می‌توان عنوان کرد که اقلام ضبط شده در بانک اطلاعاتی برای هر دپارتمان برابر با تعداد اقلام فیزیکی موجود در هر دپارتمان می‌باشد.

دسترس پذیری :

تضمین کننده این مطلب است که کاربران مجاز سیستم می‌توانند دسترسی به موقع و بی‌وقفه به اطلاعات سیستم داشته باشند. علاوه بر هدف دسترسی پذیری می‌توان به سودمندی و قابلیت اعتماد اشاره کرد.

این اهداف و سایر اهداف مرتبط از سیاست امنیتی سازمان نشأت می‌گیرد که این امر توسط مدیریت ارشد سازمان به منظور تعیین دسترسی‌های لازم توسط اشخاص مجاز تدوین می‌گردد.

نکته قابل توجه که در طراحی و پیاده سازی مکانیزم‌های کنترل دسترسی باید لحاظ شود سه مورد تهدیدهای موجود برای سیستم، آسیب‌پذیری سیستم در برابر این تهدیدها و مخاطراتی که ممکن است توسط این تهدیدها ایجاد شود، می‌باشد. در ادامه توضیحات بیش‌تری در مورد این سه مورد ذکر می‌شود :

تهدید :

واقعه یا فعالیتی که پتانسیل آسیب رسانی به اطلاعات سیستم‌ها یا شبکه‌ها را دارا می‌باشد.

آسیب پذیری :

ضعف یا کمبود محافظ، که می‌تواند توسط تهدید به وقوع بپیوندد و باعث آسیب رسانی به اطلاعات سیستم‌ها یا شبکه‌ها شود.

مخاطره :

پتانسیل برای آسیب رسانی و گم شدن اطلاعات سیستم‌ها یا شبکه‌ها می‌باشد و احتمال به وقوع پیوستن تهدیدها خواهد بود.

۹-۹-۳-۱-تعریف کنترل دسترسی :

کنترل‌ها به منظور کاهش مخاطره و پتانسیل مفقود شدن اطلاعات سیستم‌ها یا شبکه‌ها پیاده سازی می‌شوند. کنترل می‌توانند به سه صورت : ممانعت، تشخیص و تصحیح باشند. کنترل‌های ممانعتی جهت جلوگیری از وقایع مضر بکار گرفته می‌شوند، کنترل‌های تشخیصی برای کشف وقایع مضر ایجاد شده‌اند و کنترل‌های تصحیحی برای بازیابی سیستم‌هائی که مورد حمله‌های مضر واقع شده‌اند، استفاده می‌شوند.

برای پیاده سازی این سنجه‌ها کنترل‌ها می‌توانند به صورت : راهبری، منطقی یا فنی، و فیزیکی باشند.

۹-۹-۳-۱-۱-کنترل‌های راهبری :

شامل سیاست‌ها و رویه‌ها، آموزش آگاهی امنیتی، رسیدگی موجودیت فردی جهت اهداف امنیتی، بررسی روش کار، بازبینی تاریخچه تعطیلات، و افزایش نظارت می‌شوند.

۹-۹-۳-۱-۲-کنترل‌های منطقی یا فنی :

شامل محدودیت‌های دسترسی به سیستم‌ها و محافظت از اطلاعات می‌شوند. نمونه‌هائی از انواع این کنترل‌ها عبارتند از :

رمز گذاری، کارت‌های هوشمند، لیست‌های کنترل دسترسی و پروتکل‌های انتقال.

۹-۹-۳-۱-۳-کنترل‌های فیزیکی :

این کنترل‌ها باعث یکی شدن محافظان با ساختمان امنیتی می‌شوند، به عنوان مثال قفل کردن درها، امن سازی اتاق‌های سرور، محافظت از کابل‌ها، جداسازی وظائف و پشتیبان گیری از فایل‌ها را می‌توان ذکر کرد.

کنترل‌ها پاسخ‌گوئی اشخاصی را که به اطلاعات حساس دسترسی دارند را تأمین می‌کند. این پاسخ‌گوئی از طریق مکانیزم‌های کنترل دسترسی تکمیل می‌گردد که نیازمند شناسائی و صدور مجوز و توابع ممیزی می‌باشد. این کنترل‌ها باید با سیاست‌های امنیتی سازمان مطابق باشند.

رویه‌های تضمین باعث می‌شوند که مکانیزم‌های کنترلی، سیاست امنیتی را در کل چرخه حیات سیستم‌های اطلاعاتی به درستی پیاده سازی نمایند.

در استاندارد ISO ۱۷۷۹۹ مجموعاً ۱۰ دامنه وجود دارد که هر کدام پیرامون بخشی از حوزه‌های امنیت تدوین شده‌اند. هر دامنه دارای چندین کنترل است. کنترل دسترسی ششمین آنهاست. مبحث کنترل دسترسی[۱] یکی از دامنه‌های مورد نظر در استانداردهای امنیت اطلاعات

[۱] access control

(از جمله ایزو ۱۷۷۹۹ و BS-۷۷۹۹) می‌باشد. واضح است که در بازرسی‌ها و ممیزی‌هایی که از یک سازمان به عمل می‌آید تا میزان امن بودن آن سازمان سنجیده شود (مثلاً مطابق با استاندارد ممیزی ایزو ۲۷۰۰۱) این دامنه را نیز تحلیل خواهند کرد. اما جدای از این مورد، کنترل دسترسی تقریباً در تمام سازمان‌ها از اهمیت ویژه‌ای برخوردار است، در اغلب سازمان‌ها وقتی در اجرای دامنه‌های ایزو ۱۷۷۹۹ بحث محدودیت مالی و منابع پیش آید و نیاز به رتبه بندی و اولویت سنجی دامنه‌ها باشد، دامنه کنترل دسترسی غالباً رتبه «ارجح‌ترین» را می‌گیرد.

۹-۱۰- چرا کنترل دسترسی اهمیت دارد؟

کنترل دسترسی روشن‌ترین نماد امنیت است. در واقع آن را قلب امنیت هم می‌دانند. هم‌چنین برای به اجرا درآمدن اهداف CIA[1] در بحث امنیت از نگاه ISMS، این دامنه یک مبنا و پیش نیاز به حساب می‌آید. کنترل دسترسی برای تحقق سه هدف عمده به کار گرفته می‌شود که عبارتند از : ۱) جلوگیری از دسترسی کاربران غیرمجاز به امکانات تغییر اطلاعات ۲) جلوگیری از دست‌کاری اطلاعات به صورت غیرعمدی توسط کاربران ناآشنا و غیر مجاز ۳) حصول اطمینان از سلامت اطلاعات و ثبات اطلاعات داخلی و خارجی

۹-۱۱- انواع کنترل دسترسی :

کنترل دسترسی و به طور کلی کنترل از دیدگاه‌های مختلفی می‌توان تقسیم بندی کرد از یک دیدگاه انواع کنترل عبارتند از :

۱) پیش گیرانه (که جلوی چیزی که قبل از حادث شدن می‌گیرند)
۲) شناسایی کننده (شناسایی مخاطرات)
۳) اصلاح کننده (که تعمیر یا تصحیح امور را انجام می‌دهند)
۴) بازیاب (که چیزی را بازیافت و دوباره احیا می‌کنند)
۵) باز دارنده

اما از دیدگاه اجرایی و عملیاتی کنترل‌ها سه دسته‌اند :

۱) کنترل‌های مدیریتی شامل سیاست‌ها، رویه‌ها، آموزش و کنترل سابقه کاری و. . . می‌باشند.
۲) کنترل‌های منطقی / فنی مثل رمز گذاری و تهیه و استفاده از لیست کنترل دسترسی

[1] Confidentiality، Integrity، Authentication

۳) ACL کنترل‌های فیزیکی مانند درها، حصارها، گاردها و. . .

۹-۱۲-کنترل دسترسی در ISO ۱۷۷۹۹-۲۰۰۵ :

دامنه کنترل دسترسی به عنوان یکی از دامنه‌های استاندارد امنیتی ایزو ۱۷۷۹۹ دارای هفت بخش کلی است که هر کدام از آن‌ها نیز از چندین زیربخش تشکیل شده‌اند. فهرست این بخش‌ها به شرح زیر است :

۱- ملزومات مورد نیاز برای پیاده سازی
۱-۱-سیاست‌های کنترل دسترسی
۲-مدیریت دسترسی کاربران
۲-۱- ثبت کاربر
۲-۲- مدیریت امتیازات خاص کنترل
۲-۳- مدیریت رمز عبور کاربران کنترل
۲-۴- بررسی حقوق دسترسی کاربر کنترل
۳-مسئولیت‌های کاربر
۳-۱- کاربرد رمز عبور
۳-۲- تجهیزات دور از توجه مستقیم کاربر
۳-۳- سیاست تمیز نگاه داشتن میزکار و صفحه نمایش تجهیزات الکترونیکی
۴- کنترل دسترسی به شبکه
۴-۱- سیاست چگونگی استفاده از رویس‌های شبکه
۴-۲- تصدیق اعتبار کاربرد برای ارتباطات و تماس‌های از خارج از سازمان
۴-۳- شناسایی و تعیین هویت تجهیزات در شبکه
۴-۴- مراقبت از پورت‌هایی که برای اجرای تنظیمات و رفع نقص‌ها از راه دور
۴-۵- تفکیک و جداسازی در شبکه‌ها
۴-۶- کنترل تماس با شبکه
۵- کنترل دسترسی به سیستم عامل
۵-۱- فرآیندهایی امن برای ورود به سیستم
۵-۲- شناسایی و تصدیق هویت کاربران
۵-۳- سیستم مدیریت رمز عبور
۵-۴- استفاده از برنامه‌های مزیتی سیستم

۵-۵- مهلت زمانی نشست‌ها
۵-۶- محدودیت زمان برقراری ارتباط
۶- کنترل دسترسی به برنامه‌های کاربردی و اطلاعات
۶-۱- ممنوعیت دسترسی به اطلاعات
۶-۲- جداسازی سیستم‌های حساس
۷- شبکه‌های بی سیم و ارتباطات سیار راه دور
۷-۱- محاسبات و ارتباطات سیار
۷-۲- کار کردن از راه دور

۹-۱۳- مدل‌های کنترل دسترسی :

کنترل دسترسی بر اساس موضوع (یک موجودیت فعال مثل اشخاص یا فرآیندها) به یک شیيء که شامل تنظیم قوانین دسترسی است. این قوانین می‌توانند به سه مدل یا رسته دسته بندی شوند.

۹-۱۳-۱- کنترل دسترسی اجباری :

مجوز دسترسی موضوع به یک شیيء بستگی به برچسب‌ها، که نمایان کننده اختیار و کلاسه بندی با حساسیت شیيء می‌باشد. برای مثال مستندات طبقه‌بندی شده نظامی به غیرسری، کمی محرمانه، محرمانه و خیلی سری، به همین نحو، یک شخص می‌تواند یک اختیار محرمانه یا خیلی محرمانه داشته باشد تا به اطلاعات طبقه بندی شده مرتبط با محدودیت‌های تعیین شده، دسترسی داشته باشد.

این محدودیت این است که اشخاص باید یک نیاز برای آگاهی مرتبط با مستندات طبقه‌بندی شده درگیر را داشته باشند. بنابراین، مستندات باید برای اشخاص به جهت تکمیل وظایف مرتبط ضروری باشند.

تا زمانی که اشخاص مطابق با طبقه‌بندی مورد نیاز مشخص نشده‌اند نباید به اطلاعات دسترسی داشته باشند.

کنترل دسترسی بر مبنای قانون یک نوع از کنترل دسترسی اجباری است زیرا این کنترل بر اساس قوانین تشخیص داده می‌شود و نه به تنهایی توسط موجودیت موضوعات و اشیا به تنهایی.

۹-۱۳-۲- کنترل دسترسی احتیاطی

موضوع اختیار لازم به همراه محدودیت‌های مسلم برای مشخص کردن این که کدام اشیا دسترس پذیر هستند را دارد. برای مثال لیست‌های کنترل دسترسی قابل استفاده هستند.

این نوع از کنترل دسترسی به صورت محلی، در موقعیت‌های پویایی که موضوعات باید احتیاط‌هایی برای مشخص کردن این که به چه منابعی کاربران مسلمی مجاز برای دسترسی هستند، بکار می‌رود.

زمانی که یک کاربر با محدودیت‌های مسلم، حق جابه‌جایی کنترل دسترسی به اشیاء مسلمی را دارد، این اصطلاح بکار می‌رود :

«کاربر هدایت شده با دسترسی احتیاطی»

یک کنترل دسترسی بر اساس موجودیت یک نوع از کنترل دسترسی احتیاطی است که بر مبنای موجود یا اشخاص می‌باشد. در بعضی نمونه‌ها، یک رویکرد پیوندی بکار می‌رود، که‌ترکیبی از قابلیت‌های کنترل دسترسی احتیاطی بر مبنای کاربر و بر مبنای موجودیت می‌باشد.

۹-۱۳-۳-کنترل دسترسی غیر احتیاطی

یک اختیار مرکزی مشخص می‌کند که چه موضوعاتی می‌توانند دسترسی به اشیاء مسلمی بر مبنای سیاست امنیتی سازمان داشته باشند. کنترل‌های دسترسی ممکن است بر مبنای نقش اشخاص در سازمان یا در پاسخ‌گویی‌های موضوع و وظایف باشند. در یک سازمانی که تغییرات دائمی پرسنل را داریم، کنترل دسترسی غیراحتیاطی مفید است زیرا کنترل دسترسی بر اساس نقش اشخاص یا سمت در سازمان می‌باشد. این کنترل دسترسی هر وقت که پرسنلی دارای نقشی دیگر می‌شود نیاز به تغییر ندارد. نوع دیگری از کنترل دسترسی غیر احتیاطی کنترل دسترسی بر مبنای شبکه[۱] می‌باشد. این نوع کنترل، یک مدل شبکه‌ای بکار رفته است. در یک مدل شبکه‌ای زوجی از اجزا موضوع و شیء می‌باشند و موضوع بیش‌ترین کران پایین و کم‌ترین کران بالای حق دسترسی به شیء را دارد.

۹-۱۴- ترکیبات کنترل دسترسی :

با ترکیب کنترل‌های ممانعت کننده و تشخیص دهنده، انواع پیاده ساز راهبری، فنی (منطقی) و فیزیکی شامل زوج‌های زیر می‌شوند :

---

[۱] lattice-based

(مانع / راهبر) (مانع / فنی) (مانع / فیزیکی) (تشخیص دهنده / راهبر) (تشخیص دهنده / فنی) (تشخیص دهنده / فیزیکی)

هر کدام از این شش زوج و عناصر کلیدی آن‌ها را ذیل مطرح می‌گردند.

۹-۱۴-۱- ممانعت / راهبری

در این نوع، اهمیت بر اساس مکانیزم‌های «نرم» که پشتیبان اهداف کنترل دسترسی است، می‌باشد. این مکانیزم‌ها شامل سیاست‌های سازمانی و رویه‌ها، موافقت نامه‌های کارمندان، رویه‌های اختتامیه کارکنان به صورت دوستانه یا غیردوستانه، زمان‌بندی تعطیلات، برچسب بر روی مواد حساس، آگاهی‌های رفتاری و رویه‌های نشانه گذاری برای حصول شبکه‌ها و سیستم‌های اطلاعاتی و. . . می‌باشند.

۹-۱۴-۲- ممانعت / فنی

این نوع از تکنولوژی به منظور اجبار سیاست‌های کنترلی استفاده می‌کند. این کنترل‌های فنی هم‌چنین به عنوان کنترل‌های منطقی شناخته می‌شود و می‌توانند در سیستم عامل، نرم‌افزارهای کاربردی یا در سخت‌افزارها و یا نرم‌افزارهای الحاقی گذاشته شوند.

بعضی از انواع کنترل‌های ممانعت / فنی شامل پروتکل‌ها، کدگذاری‌ها، کارت‌های هوشمند، بیومتریک‌ها (برای اخذ مجوز)، بسته‌ای نرم‌افزاری کنترل دسترسی از راه دور، رمزها، منوها، پوسته‌ها، بانک‌های اطلاعاتی، نرم‌افزارهای تشخیص ویروس می‌باشند.

پروتکل‌ها، کدگذاری‌ها، کارت‌های هوشمند مکانیزم‌های فنی برای محافظت اطلاعات و رمزها از افشاسازی می‌باشند.

بیومتریک‌ها در تکنولوژی‌هایی نظیر اثرانگشت، شبکیه چشم و جست‌جوی عنبیه برای اخذ مجوز از اشخاص برای دسترسی به منابع بکار می‌روند.

۹-۱۴-۳- ممانعت / فیزیکی :

تعداد زیادی از سنجه‌های مانع / فیزیکی قابل حس و درک هستند. این سنجه‌ها به عنوان محدود کننده دسترسی فیزیکی به نواحی‌ای که اطلاعات حساس سیستم نگهداری می‌شود. نواحی مورد محافظت قرار گرفته توسط یک فضای امنیتی حلقوی تعریف می‌شود که تحت نظرکنترل دسترسی می‌باشد.

کنترل‌های ممانعت / فیزیکی شامل : حفاظ‌ها، امضاها، درهای چندگانه (به عنوان مثال وجود چندین در پشت هم که در صورت ورود به یکی با درهای دیگر مواجه می‌شویم)، سیستم

ورودی کارت‌های مغناطیسی، بیومتریک‌ها به منظور تعیین صلاحیت، گاردها، سگ‌ها، سیستم‌های کنترل محیط (مانند درجه حرارت، رطوبت و. . .) و ساختمان و نواحی دسترسی.

سنجه‌های ممانعت / فیزیکی هم‌چنین برای نواحی که برای پشتیبان گیری فایل‌ها بکار می‌روند، کاربرد دارد.

۹-۱۴-۴- تشخیص دهنده / راهبری

تعداد زیادی از کنترل‌های‌ای از نوع کنترل‌های مانع / راهبر هم‌پوشانی دارند و این هم‌پوشانی می‌تواند در ممانعت از تخلفات سیاست امنیتی آینده یا تشخیص تخلفات موجود، ظاهر گردد. نمونه‌هایی از این کنترل‌ها سیاست‌های سازمان و رویه‌ها، زمان‌بندی تعطیلات، برچسب گذاری مواد حساس و. . . می‌باشند. کنترل‌های اضافی تشخیص دهنده / راهبری شامل گردش کار؛ تسهیم مسئولیت‌ها و بررسی رکوردهای ممیزی هستند.

۹-۱۴- ۵- تشخیص دهنده / فنی

سنجه‌های کنترلی تشخیص دهنده / فنی به منظور آشکارسازی تخلفات ناشی از سیاست امنیتی با کاربری فنی بکار می‌روند. این سنجه‌ها شامل موارد سیستم‌های تشخیص حمله و گزارشات خودکار تخلفات از اطلاعات ارزیابی شده می‌باشند. این گزارشات می‌توانند واریانس‌هایی از عملیات نرمال نمایان سازند یا تشخیص امضاهای دسترسی‌های غیرمجاز را داشته باشند.

۹-۱۴-۶- تشخیص دهنده / فیزیکی

کنترل‌های تشخیص دهنده / فیزیکی معمولاً نیازمند نیروی انسانی برای ارزیابی ورودی از سنسورها یا دوربین‌ها برای تشخیص تهدیدها و حملات موجود می‌باشند. بعضی از انواع این کنترل‌ها تشخیص دهنده حرکت و جنبش هستند یا تشخیص دهنده‌های حرارتی و دوربین‌های ویدئویی می‌باشند.

۹-۱۵- سئوالات خودآزمایی

۱. امنیت محیطی و فیزیکی را تعریف نمایید.
۲. امنیت فیزیکی محل نگه داری دیتا سنتر را توضیح دهید.
۳. انواع کنترل دسترسی به محل نگهداری شبکه‌ها را توضیح دهید.
۴. اصول پدافند غیر عامل در جایابی شبکه‌های رایانه‌ای را بنویسید.

۱.

۱۰

فصل دهم: سیاست‌ها و استانداردها و مدیریت امنیتی

آن‌چه در این فصل می‌خوانید:

- **سیاست‌های امنیتی**
- **راهبردهای میان مدت و بلند مدت**
- **تعیین سطوح طبقه بندی اطلاعاتی که نمی‌توان بر روی ابزار دیجیتال قرار داد**
- **سیستم‌های امنیتی**
- **مدیریت ریسک**
- **مدیریت بحران و تصمیم گیری**
- **استانداردها و گواهی نامه‌های امنیتی**
- **نقد استانداردهای رایج و محدودیت پذیری آن‌ها**
- **نظام مدیریت امنیت اطلاعات**
- **سیاست‌های امنیتی**

۱۰- سیاست‌ها و استانداردها و مدیریت امنیتی

۱۰-۱- مدون نمودن سیاست‌های امنیتی

به‌ترین روش برای دست‌یابی به امنیت اطلاعات، فرموله نموده سیاست امنیتی است. مشخص نمودن سرمایه‌های اصلی که باید امن شوند و تعیین سطح دسترسی افراد (به عبارت دیگر این که چه افرادی به چه سرمایه‌هایی دسترسی دارند)

در اولین گام باید انجام شود. هدف اصلی از سیاست امنیتی این است که کاربران بدانند مجاز به چه کارهایی هستند.

۱۰-۲- ضرورت تدوین آیین نامه‌های امنیتی

سیاست امنیتی یک سازمان سندی است که برنامه‌های سازمان برای محافظت سرمایه‌های فیزیکی و مرتبط با فن‌آوری ارتباطات را بیان می‌نماید. به سیاست امنیتی به عنوان یک سند زنده نگریسته می‌شود، بدین معنا که فرآیند تکمیل و اصلاح آن هیچ‌گاه متوقف نشده، متناسب با تغییر فن‌آوری و نیازهای کاربران به روز می‌شود. چنین سندی شامل شرایط استفاده مجاز کاربران، برنامه آموزش کاربران برای مقابله با خطرات، توضیح معیارهای سنجش و روش سنجش امنیت سازمان و بیان رویه ارزیابی موثر بودن سیاست‌های امنیتی و راه کار به روز رسانی آن‌ها می‌باشد.

هر سیاست امنیتی مشخص کننده اهداف امنیتی و تجاری سازمان است ولی در مورد راه کارهای مهندسی و پیاده سازی این اهداف بحثی نمی‌کند. سند سیاست امنیتی سازمان باید قابل فهم، واقع بینانه و غیر متناقض باشد، علاوه بر این از نظر اقتصادی امکان پذیر،از نظر علمی قابل انعطاف و متناسب با اهداف سازمان و نظرات مدیریت آن سطح حفاظتی قابل قبولی را ارائه نماید.

۱۰-۳- نگاه سیستمی به امنیت دیجیتال

به منظور مواجهه صحیح و عقلایی با موضوعات، ابتدا باید آن‌ها را به درستی شناخت، تا بتوان براساس این شناخت برای اقدامات آتی طراحی مناسبی انجام داد. اساساً شناخت صحیح،

یکی از مهم‌ترین مراحل تحلیل مسایل و ارائه‌ی راه‌حل است به گونه‌ای که در صورت غلط یا ضعیف اجرا شدن این مرحله، کلیه‌ی اقدامات بعدی در جهت حل مشکل، با شکست مواجه می‌شود.

از طرف دیگر نگاه همه جانبه و کلی‌نگر به مسئله‌ها هم‌زمان با دقت کافی در شناسایی جزئیات لازم به صورت پویا و در طول زمان، ضامن ارائه‌ی راه‌حلی همه جانبه برای برطرف کردن مشکلات و حل مسایل است. اگر رویکرد صاحب مشکل به مسأله‌ی مورد بررسی متوقف به زمان حال بوده و نگاهی به گذشته و سابقه‌ی مسأله نداشته باشد، راه‌حل ارائه شده نیز به صورت راه‌حلی با اثرگذاری کوتاه مدت و بدون توجه به عوارض آینده خواهد بود. برای این‌که بتوان در حل مسایل در دراز مدت موفق بود، رویکرد سیستمی ابزار مناسبی تلقی می‌گردد.

در شرایط کنونی که اغلب مدیران و تصمیم‌گیران، درگیر انواع بی شماری از مسائل سازمانی هستند، برقراری یک الگوی سیستمی در سازمان‌ها بسیار ضروری است. این موضوع به‌اندازه‌ای حیاتی است که تعیین کننده موفقیت یا شکست سازمان در رسیدن به اهدافش محسوب می‌شود. به عبارت دیگر عدم استفاده از یک دید سیستمی و کل‌نگر، منجر به ارائه‌ی راه‌حل‌هایی می‌شود که اگرچه در کوتاه مدت عوارض مسأله را برطرف می‌کند، اما در طولانی مدت منجر به بروز عوارضی می‌گردد که سازمان را با مشکلات پیچیده‌تری مواجه خواهد کرد.

برای رسیدن به یک ذهنیت مشترک در مورد واژه‌ی سیستم، ابتدا لازم است تعریفی دقیق و واقعی از این واژه ارائه دهیم. پس از این تعریف نیز لازم است درباره چگونگی استفاده از رویکرد سیستمی به عنوان روشی برای تحلیل وقایع و طراحی اقدامات آینده، به بحث و گفت‌و گو به پردازیم.

هرچند نگرش سیستمی به پدیده‌های طبیعی و اتفاقات فیزیکی و غیرانسانی از دیرباز در بین اندیشمندان مطرح بوده است، اما استفاده از این رویکرد، به عنوان یک روش علمی برای شناخت و تحلیل پدیده‌های انسانی در جهان کنونی و ارائه‌ی راه‌حل‌های مبتنی بر این نگرش بحثی نو در مراکز دانشگاهی و سازمان‌های بزرگ است. دیدگاهی کل‌نگر، نسبت به همه سیستم‌های زنده اعم از افراد، گروه‌ها و سازمان‌ها به منظور تلاش برای بقاء و پیشرفت در محیط پویا و متغیر امروز.

دنیای اطراف ما متشکل از کل‌هایی به نام سیستم است. سیستم به عنوان یک کل، متشکل از اجزایی است که برای تحقق هدف خاصی با یک‌دیگر و با سایر سیستم‌های جهان به تعامل و هم‌کاری می‌پردازند. آن‌چه اجزای یک سیستم را از اجزای سایر سیستم‌ها متفاوت

می‌سازد، تفاوت هدفی است که این جزء به دلیل عضویت در این سیستم با جزء دیگری در یک سیستم دیگر دارد. به عبارت دیگر هدف فعالیت کل سیستم، هدف فعالیت هر جزء از آن است.

سیستم‌ها خواصی دارند که صرفاً از جمع خواص اجزای آن‌ها حاصل نمی‌شود. بنابر این برای شناخت هر سیستم، نمی‌توان آن را به اجزای تشکیل دهنده‌اش تجزیه نمود. برای هر سیستم بسته به نوع نگرش و تحلیل، می‌توان مرز مشخصی با سایر سیستم‌ها که آن‌ها را محیط اطراف می‌نامیم تعیین نمود. این مرز یک مفهوم مجرد بوده و با مرزهای اداری و جغرافیایی متفاوت است.

در نگرش سیستمی به هر پدیده به عنوان یک کل، موارد زیر باید مشخصاً مد نظر قرار گیرند :

- دلایل وجودی و اهداف سیستم
- محیط سیستم
- اجزای تشکیل دهنده‌ی سیستم و تعامل آن‌ها

اگر مرزهای سیستم درست تعریف شده باشد، می‌توان علل وقوع هر پدیده را در داخل سیستم جست‌جو کرد و برای حل مشکل راه‌کارهای داخلی ارائه نمود. البته باید توجه داشت که در پیاده‌سازی نگرش سیستمی، محدودیت‌ها و شرایط زمانی و مکانی، تعریف مرز بهینه‌ی سیستم را تحت تأثیر قرار می‌دهند.

در نگرش سیستمی، هر سیستم به عنوان یک کل، خود به عنوان جزئی از یک سیستم بزرگ‌تر است. به عبارت دیگر، هر چه حوزه‌ی تصمیم‌گیری بزرگ‌تر می‌شود، تصمیم‌گیر با تعداد بیش‌تری از سیستم‌ها طرف نخواهد بود، بلکه با یک سیستم بزرگ‌تر مواجه است.

بر همین اساس در حوزه‌های ملی، تمام افراد و سازمان‌ها اجزای سیستم کل به حساب می‌آیند و کل، موضوعات حوزه‌ی ملی است که با این اجزا تفاوت دارد.

۱۰-۴- ویژگی‌های سیستم

۱- اصالت با «کل» است: در نگرش سیستمی، اصالت با کل است و اجزا در اولویت بعدی قرار دارند.

۲- باید ابتدا سیستم و محیط آن درک شود. محیط در واقع سیستم‌های دیگری هستند که به عنوان یک کل با سیستم موردنظر ما تعامل دارند. به عبارت دیگر تعامل سیستم با محیط تعامل دو جزء با یک‌دیگر نیست، بلکه تعامل دو کل با یک‌دیگر است.

۳- هر سیستم کارکرد و ویژگی‌هایی دارد که هیچ یک از اجزای آن به تنهایی نمی‌توانند تمامی آن کارکرد و ویژگی‌ها را دارا باشند. به عبارت دیگر ماهیت سیستم به عنوان یک کل، با ماهیت هر جزء آن متفاوت است.
۴- فلسفه وجودی و هدف سیستم، تعیین کننده‌ی اجزا و روابط مناسب آن‌ها با یک‌دیگر است. به عبارت دیگر اجزا و روابط درونی آن‌ها پس از تعیین هدف سیستم در محیط آن است که معنی پیدا می‌کند.
۵- اجزای سیستم کل را پشتیبانی می‌کنند. به این مفهوم که اجزای سیستم در ارتباط صحیح با یک‌دیگر برای تأمین هدف سیستم فعالیت می‌کنند.
۶- سیستم‌ها را نمی‌توان به بخش‌های مجزا تقسیم کرد. یک سیستم، هنگامی که بخشی از کلیت خود را از دست می‌دهد، ماهیت و عمل‌کردش دست‌خوش تغییر می‌شود.
۷- توجه ویژه به هر یک از اجزا به کل لطمه می‌زند. یعنی تمرکز روی یک عنصر یا زیر سیستم منجر به بزرگ‌نمایی اهداف فرعی و کم‌رنگ شدن هدف کلی می‌شود.
۸- سیستم‌ها سرعتی طبیعی برای خود دارند. تلاش برای رشد سریع‌تر منجر به بروز نتیجه‌ی معکوس می‌شود.
۹- رابطه‌ی علت و معلول‌ها در نگرش سیستمی خطی نیست. اگرچه پدیده‌ای ممکن است امروز معلول یک پدیده‌ی دیگر باشد، اما ممکن است خود باعث بروز پدیده‌هایی شود که بر علت اولیه مؤثر باشند.
۱۰- هر جزء یک سیستم به عنوان یک زیرسیستم می‌تواند جزئی از سیستم‌های مختلفی باشد. به عبارت دیگر اگرچه یک جزء سیستم در یک نگاه در محدوده‌ی آن سیستم فعالیت می‌کند اما می‌تواند در داخل یک سیستم دیگر نیز با رویکردی دیگر وظیفه‌ی دیگری بر عهده داشته باشد.
۱۱- راه حل‌های مقطعی اگر چه در کوتاه مدت به نتایج مطلوب می‌انجامد، اما ممکن است منجر به بروز مشکلات عمیق‌تر در دراز مدت می‌شود.

۱۰-۴-۱- ضرورت تفکر سیستمی در جهان امروز

گستردگی، تنوع و پیچیدگی روز افزون مسایل و پدیده‌های پیش روی افراد و سازمان‌ها در عصر حاضر، استفاده از یک نگاه کل نگر و همه جانبه را از یک راه‌کار قابل انتخاب به یک

ضرورت انکارناپذیر تبدیل کرده است. از طرفی نگرش جزئی‌نگر به پدیده‌ها، نه تنها راه طولانی‌تری برای حل مشکلات است بلکه منجر به تصمیم‌های ناصحیحی می‌شود که اصلاح عوارض آن‌ها ممکن است از توانایی تصمیم‌گیران خارج باشد.

در عصر مدرن، ماشین‌ها، اصلی‌ترین نقش را در یک سازمان و حتی در سطح کشورها ایفا می‌کردند. به عبارت دیگر عصر ماشین، عصر سخت‌افزار بود. در تفکر ماشینی، اجزاء سیستم هر یک دارای ماهیت مستقل بودند. با گذر از دوره‌ی سخت‌افزار به نرم‌افزار و رسیدن به دوره‌ی مغزافزار در عصر حاضر، این انسان‌ها هستند که عنصر تأثیرگذار سیستم‌ها می‌باشند و همین ماهیت انسانی است که موجب تجزیه ناپذیری سیستم‌هایی شده که تعاملات و تصمیم‌های انسانی جزء اساسی آن‌ها است.

تفکر سیستمی علاوه بر کل‌نگری و تجزیه‌ناپذیری بر پایه‌ی مفهوم دیگری نیز استوار است که نگاه پویا نامیده می‌شود. نگاه پویا، تصمیم‌گیران را مکلف می‌کند تا برای تصمیم‌گیری درباره‌ی یک سیستم، به رفتارهای آن در طول زمان توجه کنند. این تحلیل باید در مورد رفتارهایی انجام شود که از زمان گذشته شروع شده و تا آینده ادامه خواهد داشت. در ادامه به مهم‌ترین خصوصیات و نتایج تفکر سیستمی می‌پردازیم.

۱۰-۴-۲- خصوصیت‌های تفکر سیستمی

تفکر سیستمی به عنوان یک مفهوم جدید معادل کل‌نگری در نظر گرفته می‌شود. در ادبیات نوین سیستم، تحلیل پویای سیستم‌ها یک رویکرد برای درک پیچیدگی رفتار سیستم‌ها به شمار می‌رود. از این منظر تفکر سیستمی:

۱- الگو و روشی برای مفهوم بخشیدن به فلسفه زندگی است زیرا تمامی موجودات زنده سیستم به شمار می‌روند.

۲- روشی برای درک آسان‌تر هر پدیده‌ی جدید است. زیرا قوانین اصلی از سیستمی به سیستم دیگر تغییر نمی‌کنند.

۳- چارچوبی برای تشخیص، تحلیل و حل مسأله و تصمیم‌گیری در سیستم است. راه روشن‌تری را برای مشاهده و درک آن چه در درون سازمان یا هر سیستمی رخ می‌دهد، می‌نمایاند. درک مسایل پیچیده را با شناسایی روابط درونی اجزا و چرخه‌های چند وجهی علت و معمولی، آسان‌تر می‌کند.

۴- روشی برای مدیریت فراهم می‌کند. تمرکز بر کل، اجزای تشکیل دهنده آن، روابط درونی (تعاملی) اجزاء از ویژگی‌های آن است و تلفیق به‌تری از ایده‌های نو را هنگام مشاهده مسایل فراهم می‌کند.

۵- روشی برای شناخت ریشه‌ای مسایل مبتنی بر الگوها و روابط و هم‌چنین ارائه‌ی راه‌حل‌های کوتاه مدت و دراز مدت برای حل آن‌ها است.

۶- چارچوبی برای بررسی و تحلیل عوامل محیطی و آثار آن‌ها بر سیستم ارائه می‌دهد.

در این‌جا باید بار دیگر به این واقعیت اشاره کرد که نگاه سیستمی به پدیده‌ها و روابط حاکم بین اجزای آن‌ها به خصوص با توجه به پیچیدگی غیرقابل انکار و سرعت وقایع دنیای کنونی تنها راه درک صحیح و ارائه‌ی راه‌کارهای مناسب برای حل مسایل و اجرای فعالیت‌های مختلف است.

۱۰-۴-۳- ماهیت سیستمی حوزه‌ی فن‌آوری اطلاعات و ارتباطات

تمامی فن‌آوری‌هایی که تولد آن‌ها پس از پایان عصر انقلاب صنعتی رخ داده، مبتنی بر نظریه‌ی سیستم‌ها شکل گرفته‌اند. به عبارت دیگر نظریه‌ی سیستم‌ها و کاربرد آن در توسعه‌ی علوم و فن‌آوری‌ها موجب پایه‌گذاری عصر جدیدی در زندگی بشر شده است.

یکی از مؤلفه‌های اصلی در این عصر جدید، تغییر نگرش به سیستم‌ها از ماشینی به انسانی است به نوعی که قواعد ماشینی حاکم بر تعامل سیستم‌ها، به مرور به رویکرد انسانی تبدیل گردیده. این روند امروزه منجر به ایجاد رویکردهای انسانی، اجتماعی در تحلیل و راهبری سیستم‌ها گردیده و به سوی سیستم‌های متعالی ادامه دارد. در سطوح سیستم‌های انسانی و بالاتر از آن، بر خلاف سیستم‌های ماشینی، نمی‌توان عمل‌کرد سیستم را فقط بر مبنای برآیند عمل‌کرد اجزای آن تحلیل نمود بلکه توجه به هم‌افزایی که یکی از اصول اساسی سیستم‌های انسانی است لازم می‌باشد.

رسیدن به درک صحیحی از نگرش سیستمی در تحلیل پدیده‌ها، تنها راه کاربردی کردن فن‌آوری‌های نوین در فعالیت‌های سازمان‌ها و افراد است. بدون نگرش سیستمی پیاده‌سازی فن‌آوری‌های نوین و استفاده از آن‌ها، موجب بروز مخاطرات جدی برای کاربران و سازمان‌ها شده و هر اقدامی نتایج غیر منتظره‌ای را برای مدیریت و راهبران سازمان در پی خواهد داشت.

گسترش و فراگیر شدن شبکه‌های ارتباطی و اطلاعاتی تمامی جوانب زندگی بشر از جمله فرآیندهای سازمانی را تحت تأثیر عمیق قرار داده است. هوشمند سازی ماشین‌ها موجب شده تا

ماهیت سیستم‌های مبتنی بر فن‌آوری اطلاعات و ارتباطات با سایر فن‌آوری‌های عصر صنعتی متفاوت باشد. تعامل این دسته از سیستم‌ها برخلاف سیستم‌های عصر صنعتی بر اساس روابط انسان- ماشین ایجاد گردیده است. از طرف دیگر ماهیت به هم پیوسته و درهم‌تنیده‌ی سیستم‌های مبتنی بر فن‌آوری اطلاعات و ارتباطات سبب پیچیده‌تر شدن ساختارها و دشوارتر شدن تصمیم‌گیری‌ها شده است.

هنر تفکر سیستمی آن است که بتوان پویایی ساختارهای پیچیده و نهفته در سازمان‌ها را تشخیص داد و با اصلاح راهکارها و ساختارها به نتایج مطلوب دست یافت.

مدیران غالبا در پی آن هستند که از فن‌آوری اطلاعات و ارتباطات، به عنوان مهم‌ترین دستاورد عصر نوین، در ساختارهای سنتی و بدون اصلاح فرآیندها و سازمان‌دهی استفاده کنند. در نتیجه شکاف موجود بین ساختار و تفکر سنتی با ماهیت سیستمی فن‌آوری اطلاعات و ارتباطات موجب بروز مشکلات می‌گردد.

با گسترش به کارگیری محصولات و خدمات فن‌آوری اطلاعات و ارتباطات، یک‌پارچگی سیستم‌ها در سطوح سازمانی و بالاتر از آن در سطح ملی به صورت ملموس‌تری در معرض دید سیاست‌گذاران این حوزه‌ها قرار گرفته است. به طوری که مسایل، مشکلات و دغدغه‌های تصمیم‌گیری در سطوح بالا مانند سطوح منطقه‌ای و ملی، ارتباط تنگاتنگی با مسایل زیرسیستم‌ها که هریک در محدوده‌ی خود یک سیستم کامل به شمار می‌روند دارد. به تعبیر دیگر سیستم‌های فن‌آوری اطلاعات و ارتباطات در سطح سازمانی یا منطقه‌ای، یک جزء از سیستم فن‌آوری اطلاعات و ارتباطات ملی هستند و ملاحظات خاص خود را در سیاست‌گذاری‌های کلان خواهند داشت.

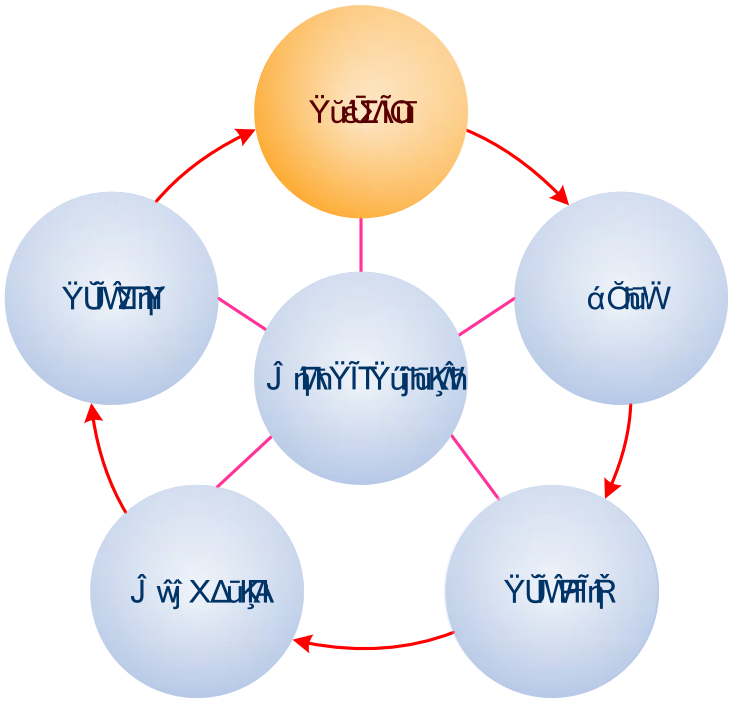
۱۰-۵- برنامه‌ریزی امنیتی

برای پیاده سازی امنیت در یک سازمان به دو نوع برنامه‌ریزی در آن نیاز است. برنامه‌ریزی کلان‌تر برای خط مشی‌ها و برنامه‌ریزی جزئی‌تر برای سیاستهای امنیتی. در ادامه با این دو دسته بیش‌تر آشنا خواهیم شد.

۱۰-۵-۱-برنامه‌ریزی استراتژیک امنیت

استراتژی یک جهت‌دهی یا خط مشی است که برای رسیدن به هدف یا اهدافی اتخاذ می‌شود. هدف از برنامه‌ریزی استراتژیک برای امنیت فراهم آوردن اطلاعات لازم جهت مدیریت و تصمیم‌گیری در مورد سرمایه‌گذاری‌های امنیتی است. برنامه استراتژیک عمل‌کردهای امنیتی را به خط‌مشی‌های تجاری و حرفه پیوند می‌دهند. استراتژی‌های امنیتی رسیدن به اهداف حرفه

را با شناسایی و آدرس‌دهی نیازمندی‌های امنیتی در عمل‌کرد آن سازمان، فراهم آوردن زیرساخت‌ها، افراد و فرآیندهایی که آن نیازمندی‌ها را فراهم کند ممکن می‌سازد. همان‌طور که در شکل زیر مشخص است در حقیقت استراتژی‌های امنیتی هسته اصلی برای چرخه طراحی و پیاده‌سازی یک سیستم امنیتی را تشکیل می‌دهد.



استراتژی‌ها با استفاده از اهداف حرفه و اهداف امنیتی و میزان قابلیت فعلی برای تأمین این اهداف طراحی می‌شود. برای مثال ممکن است هدف یک بانک به‌دست آوردن سرمایه بیش‌تر باشد و استراتژی آن جذب بیش‌تر مشتریان باشد. یک هدف امنیتی ایجاد اتصال بیش‌تر در کنار کم کردن خطر هک[۱] و ویروس تا سطح قابل قبول باشد و هدف امنیتی دیگر اطمینان از برآورده شدن انتظارات قابل دسترس بودن مشتریان باشد. بنابراین استراتژی امنیتی مربوطه

[۱] hack

با توجه به محدودیت‌های داخلی و خارجی سازمان می‌تواند افزایش میزان مانیتور کردن اتصالات در جهت کاهش ریسک ویروس و هک و فراهم آوردن افزونگی[۱] برای افزایش میزان دسترس‌پذیری[۲] و اطمینان باشد.

۱۰-۵-۲- سیاست‌های برنامه‌ریزی استراتژیک

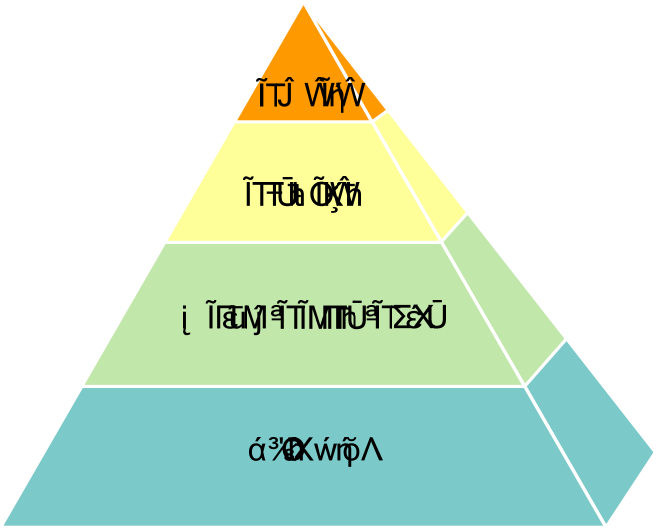
- استراتژی‌ها باید به طور دوره‌ای بازبینی و اصلاح شوند تا اجازه تغییر و رشد به فرآیند حرفه مربوطه داده شود.
- شعبات سازمان باید هماهنگ با یک‌دیگر و با توجه به خط‌مشی‌های ابلاغ شده از سوی نهادهای مرکزی بانک به طراحی استراتژی‌های خود بپردازند.

۱۰-۵-۳- برنامه‌ریزی سیاست‌های امنیتی

سیاست[۳] در ارتباط با مدیریت امنیت معانی زیادی دارد. سیاست به معنای دستورات، قوانین و تصمیم‌های مدیر امنیتی برای ایجاد یک برنامه امنیتی، پایه‌ریزی کردن اهداف و تخصیص دادن مسئولیت‌هاست. پس از تعیین خط‌مشی‌های یک سازمان، سیاست‌های آن برنامه‌ریزی شده، استانداردها و سپس روال‌ها و راهنماهای امنیتی مربوطه برای پیاده‌سازی آن سیاست‌ها در یک محیط واقعی توسعه داده شده در اختیار کاربران و مدیران قرار داده می‌شود. این سیاست‌ها برای رسیدن به امنیت مورد نظر در سازمان باید به طور کامل پیاده‌سازی و اجرا شوند. تمام افرادی که به این منابع دسترسی دارند تحت تأثیر این سیاست‌ها قرار می‌گیرند و ملزم به رعایت و اجرای آن‌ها خواهند بود. این سیاست‌ها با دقت و توجه فراوان باید تدوین شوند. هر گونه اشتباه در این مرحله ممکن است امنیت سیستم را دچار مشکل کند.

---

[۱] Redundancy
[۲] Availability
[۳] Policy



سیاست‌های امنیتی که خوب تدوین شده باشند ویژگی‌های زیر را دارا هستند:

- توسط مدیران سیستم قابل پیاده‌سازی و اجرا هستند.
- رویه‌های تدوین شده ساده، قابل اجرا و مورد پذیرش هستند.
- توسط ابزارهای تأمین کننده‌ی امنیت موجود قابل اعمال هستند.
- به طور مشخص مسئولیت‌ها و وظایف کاربران، کادر فنی و مدیران را تعیین می‌کنند. به هنگام تدوین سیاست‌های امنیتی به سئوالات زیر باید پاسخ داد:
- چه کسانی اجازه دارند از منابع استفاده کنند؟
- چگونه افراد مجاز شناسایی می‌شوند؟
- استفاده‌ی صحیح و مناسب از منابع چیست؟
- چه کسی اجازه‌ی بخشیدن دسترسی و بالا بردن سطح دسترسی را داراست؟
- چه افرادی سطح دسترسی مدیران[1] را دارا هستند؟
- حق و حقوق کاربران و هم‌چنین مسئولیت‌های آن‌ها چیست؟
- حق و حقوق مدیران فنی و هم‌چنین مسئولیت‌های آن‌ها چیست؟
- با اطلاعات حساس چه کار باید کرد؟
- فعالیت‌های انجام شده در سیستم چگونه و تا چه حد نگهداری می‌شوند؟

[1] Administration privilege

- با متخلفین و کسانی که از سیاست‌ها و قوانین پیروی نمی‌کنند چگونه برخورد می‌شوند؟

سیاست امنیتی باید در حوزه‌های بسیاری از هر سازمان باید تعیین شود که از آن جمله می‌توان به موارد زیر اشاره نمود:

- سیاست دسترسی: مشخص می‌کند که چه افرادی و یا چه بسته‌هایی اجازه‌ی دسترسی به منابع مختلف را دارا هستند. سطح و میزان دسترسی آن‌ها نیز در همین بخش مشخص می‌شود. در این بخش هم‌چنین قوانینی برای ارتباطات بیرونی، انتقال داده‌ها، اتصال تجهیزات به شبکه و اضافه کردن نرم‌افزارهای جدید تدوین می‌شود.
- سیاست تشخیص هویت: نحوه‌ی شناسایی افراد و بسته‌های مختلفی که متقاضی ورود به شبکه و استفاده از منابع هستند را مشخص می‌کند. یکی از مواردی که در این بخش مشخص می‌شود سیاست کلمه عبور(کلمات عبور اولیه، محدودیت در چگونگی کلمات عبور، حداکثر زمان‌ها و. . .) است. در این بخش هم‌چنین تعیین‌هویت‌های فرآیندهای نرم‌افزاری (مثلاً در پروتکل‌های مسیریابی به هنگام دریافت بسته‌های routing-update) نیز مورد بررسی قرار می‌گیرد.
- سیاست حساب‌داری: چگونگی نگهداری اتفاقاتی که در شبکه می‌افتند را مشخص می‌کند. در این بخش مشخص می‌شود که انواع مختلف فعالیت‌های انجام شده چگونه جمع‌آوری و نگهداری می‌شوند. باید تمام اطلاعات و فعالیت‌های افراد تشخیص و تأیید هویت شده‌اند (نام، شماره‌ی خط و یا میزبانی که از آن طریق login کرده‌اند، میزان دسترسی قدیم و جدید، تلاش‌های احتمالی انجام شده برای تغییر سطح دسترسی و. . .) با زمان دقیق نگهداری شوند.
- سیاست گزارش تخلفات: مشخص می‌کند که انواع تخلفات کدامند و این تخلفات چگونه و به چه کسانی گزارش داده می‌شوند.
- سیاست حریم خصوصی افراد: در این بخش مشخص می‌شود که مدیران تا چه حد و در چه شرایطی می‌توانند mailها را مانیتور کنند، دسترسی به فایل‌های کاربران و مدیران زیربخش‌ها داشته باشند، از فعالیت‌های خصوصی افراد log بگیرند، desktopها را مشاهده کنند و. . .

- سیاست نگهداری شبکه: نگهداری خارجی و داخلی را مشخص می‌کند و میزان دسترسی افراد خارجی که برای نگهداری یا بهینه‌سازی شبکه با شرکت همکاری می‌کنند را تعیین می‌سازد. چگونگی مدیریت از راه‌دور نیز در این بخش مشخص می‌شود.
- سیاست دسترس‌پذیری: میزان توقع و انتظار کاربران و مدیران از دسترس‌پذیری منابع را مشخص می‌کند و براین اساس افزونگی[۱] منابع و فرآیند باریابی آن‌ها را مورد تحلیل قرار می‌دهد.
- سیاست‌های آگاهی‌رسانی: چگونگی آموزش کاربران، کادر فنی و مدیران در این بخش مشخص می‌شود. در این بخش هم‌چنین مشخص می‌شود که کدام قسمت و چه افرادی باید به سؤالات کاربران و مدیران در زمینه‌ی امنیت و در هنگام بروز حوادث امنیتی پاسخ دهند و به آن‌ها کمک کنند.

پس از تعیین سیاست‌ها، رویه‌های امنیتی باید برای کاربران نهایی، مدیران شبکه و مدیران امنیتی و سایر افراد درگیر نوشته شوند. رویه‌های امنیتی هم‌چنین باید چگونگی برخورد با حوادث مختلفی که رخ می‌دهند را مشخص کنند. این رویه‌ها باید به کاربران و مدیران شبکه آموزش داده شوند.

پس از آنکه قدم‌های فوق برداشته شدند دیواره‌های آتش، ضدویروس‌ها، سیستم‌های تشخیص تهاجم و. . . برای امن‌سازی سازمان به خدمت گرفته می‌شوند و رویه‌های امنیتی پیاده‌سازی می‌شوند.

سیاست‌های امنیتی، تکنولوژی و متدولوژی استفاده از سیستم‌های امن و روال، گام‌های جزئی برای دنبال کردن وظایف امنیتی مربوطه را مشخص می‌کند. در این راستا پس از شناخت وضعیت معماری موجود و تهیه معماری امنیتی مطلوب باید برنامه‌ای برای حرکت از سمت معماری موجود به سمت معماری مطلوب طراحی و اجرا و کنترل نمود. سیاست‌های امنیتی باید در دسته‌های مدیریت امنیتء امنیت اطلاعات، امنیت پرسنل، امنیت شبکه و سیستم شامل سیاست‌های توسعه نرم‌افزار، سیاست‌های شبکه و مدیریت سیستم و برنامه‌ریزی تداوم تجارت ارائه شود، که از آن جمله ما برای نمونه به بررسی سیاست‌های مدیریت امنیت بسنده می‌کنیم.

---

[۱] Redundancy

۱۰-۵-۴- استراتژی‌های طراحی سیاست‌ها

- در سازمان باید تشکیلاتی برای تأمین امنیت شبکه از نقطه‌نظر ساختار، شرح وظایف و جایگاه آن در چارت سازمانی و برنامه‌های تأمین نیروی انسانی آن طراحی شود. این تشکیلات در سه سطح سیاست‌گذاری، مدیریت اجرایی و سطح فنی به طراحی، نظارت و اجرای طرح‌ها و برنامه‌های امنیتی می‌پردازد.
- برنامه‌ریزی‌ها باید به دو صورت کوتاه‌مدت و بلندمدت (یا میان‌مدت) با توجه به اهداف امنیت سازمان طراحی شود.
- برای اینکه سیاست‌های امنیتی به خوبی پیاده‌سازی شوند تمام افرادی که وظیفه‌ی نگهداری و محافظت سیستم را به عهده دارند باید در پیاده‌سازی آن‌ها همکاری کنند.
- برای برنامه‌ریزی و دادن طرح‌ها و رویه‌های امنیتی ابتدا باید سرمایه‌ها و ریسک‌ها را شناسایی و درجه‌بندی نمود. که در بخش مدیریت ریسک به آن خواهیم پرداخت.
- پس از طراحی برنامه امنیت سازمان، طراحی برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت در سازمان باید و هم‌چنین طرح پشتیبانی حوادث امنیتی سازمان را نیز طراحی نمود.
- سیاست‌های امنیتی باید برای موارد مختلفی از جمله موارد زیر طراحی شود: سیاست‌های دسترسی کاربران به شبکه داخلی، دسترسی کاربران به شبکه اینترنت، سیاست‌های امنیتی در مورد سرویس‌هایE-mail، وب، ویدئو کنفرانس، وب‌هاستینگ، Wireless، دسترسی از راه دور، سرویس‌های اشتراک، دسترسی و انتقال فایل‌ها، دسترسی به بانک‌های اطلاعاتی، دسترسی کاربران به سخت‌افزارها، سیاست‌های انتخاب سیستم عامل، سیاست‌های انتخاب و تنظیم ایستگاه‌های کاری، سیاست‌های نصب نرم‌افزار، سیاست‌های پشتیبان‌گیری، سیاست‌های محافظت در مقابل ویروس، سیاست‌های بازرسی دوره‌ای امنیت ایستگاه‌های کاری، سیاست‌های امنیتی استفاده از سخت‌افزارهای مختلف، سیاست‌های دسترسی کاربران به نرم‌افزارها و سرویس‌های شبکه و سیاست‌های امنیت فیزیکی و. . .

- در هر سازمان پس از تهیه سیاست‌ها و استانداردها و روال‌های امنیتی، معماری موجود سازمان بررسی شود، رخنه‌ها و خطرهای آن مشخص شوند. سپس با توجه به اهداف و سیاست‌ها نیازمندی‌های امنیتی شامل جزئیاتی مانند TDSها، UPNها، دسترسی از راه دور، حفاظت از میزبان (host protect) و حتی طراحی‌های شبکه مانند تغییر توپولوژی. . . شناسایی و اولویت‌بندی گردد.
- پس از انتخاب هدف‌ها و سیاست‌های امنیتی باید به تهیه روال‌ها و دستورالعمل‌های اجرایی جهت عملیاتی کردن آن سیاست‌ها پرداخت.

۱۰-۶- طبقه بندی ریسک

یکی از مواردی که به عنوان مقدمه برای سیاست گذاری امنیتی در یک سازمان باید مد نظر قرار گیرد مدیریت ریسک می‌باشد و در آن ارزیابی ریسک برای تعیین چگونگی سیاست گذاری از اهمین ویژه‌ای برخوردار است.

۱۰-۶-۱- ارزیابی ریسک

محاسبه ریسک آخرین مرحله نیست. حال باید در مورد پذیرش یا عدم پذیرش ریسک، تصمیم گیری نمود. یا این که سیستم را طوری تغییر دهیم که تأثیر ریسک‌ها آن کاهش یابد. ارزش‌یابی ریسک بدین معنی است که ریسک را بر اساس یک سری معیارها یا شاخص‌های مشخص، اولویت بندی شوند. البته یک معیار جهانی در مورد پذیرش ریسک وجود ندارد زیرا آن‌چه که براساس آن‌ها در مورد ریسک تصمیم‌گیری می‌شود، ممکن است مسائل سیاسی، قانونی اجتماعی یا بشر دوستانه باشد که همه این موارد بستگی به اهداف شرکت یا سازمان مربوط دارد.

۱۰-۶-۱-۱- روش اجرا

نخستین گام اجرای فرآیند ارزیابی ریسک، شناسایی تمامی دارایی‌های اطلاعاتی موجود در حوزه مورد بررسی است تا پس از آن بتوان ریسک‌های متوجه هر یک از آن‌ها را به‌طور کامل مشخص نمود. دارایی‌ها به چهار دسته دارایی‌های اطلاعاتی، نرم‌افزاری، سخت‌افزاری و انسانی تقسیم شده و برای هر یک، نمونه‌هایی ذکر شده است.

۱۰-۶-۱-۱-۱- بندی دارایی‌ها:

سرمایه عبارتست از دارایی فیزیکی یا اطلاعاتی که برای سازمان دارای ارزش و اهمیت بوده و باید به‌طور خاص مورد محافظت قرار گیرد.

۱۰-۶-۱-۱-۱-۱- دارایی‌های سخت‌افزاری

شامل سرورها، رایانه‌های شخصی، انواع CD، فلاپی، پرینتر، اسکنر، نوت بوک، Flash memory، درایورهای قابل حمل، اجزاء شبکه ارتباطی از قبیل روترها، مودم، سوئیچ، . . .

۱۰-۶-۱-۱-۱-۲- دارایی‌های نرم‌افزاری

- نرم‌افزارهایی که در داخل سازمان تولید شده و در راستای مأموریت و فعالیت‌های سازمان مورد استفاده قرار می‌گیرند. - نرم‌افزارهایی که در خارج از سازمان تهیه شده و در راستای مأموریت و فعالیت‌های سازمان مورد استفاده قرار می‌گیرند مانند سیستم‌های اتوماسیون اداری، نرم‌افزارهای مالی، انبارداری و. . . . - نرم‌افزارهای معمول و موجود در بازار که برای انجام امور عادی و روزمره مورد استفاده قرار می‌گیرند مانند نرم‌افزارهای تایپ و صفحه گسترده، نقشه کشی و. . . . - سایر موارد.

۱۰-۶-۱-۱-۱-۳- سرمایه‌های اطلاعاتی

شامل هر نوع اطلاعات (چه فیزیکی از قبیل کاغذ و نامه و. . .) و چه غیر فیزیکی (داده‌ها) که برای سازمان دارای ارزش باشند. - اطلاعات کاری و سازمانی از قبیل سوابق پروژه‌ها و فعالیت‌های انجام شده، مأموریت و گزارشات سازمانی موجود، روندها و طرح‌های سازمانی و. . . - اطلاعات پرسنلی از قبیل اطلاعات حقوقی، اطلاعات شخصی، سوابق کاری و خدمتی، شماره حساب‌های بانکی و. . . - اطلاعات امنیتی از قبیل کلمات عبور، اطلاعات مربوط به رمزنگاری و احراز صلاحیت و احراز هویت کاربران و. . . - بانک‌های اطلاعاتی موجود بر روی سرورها، فایل‌های اطلاعاتی ذخیره شده بر روی سرورها یا رایانه‌های کاربران - سایر موارد.

۱۰-۶-۱-۱-۱-۴- سرمایه‌های انسانی

سرمایه‌های انسانی شامل تمامی کارکنانی می‌شود که در سازمان مشغول بکار بوده و در صورت از دست دادن آن‌ها، به روند اجرایی سازمان و روال‌های کاری و سازمانی لطمه وارد خواهد شد. نظیر: - مدیران ارشد قسمت‌های مختلف سازمان و جانشینان و معاونین آن‌ها - رؤسای بخش‌ها و دوایر - پرسنل متخصص و با سابقه - مدیران و کارشناسان بخش IT و امنیت اطلاعات - پرسنل متخصص و تکنیکی موجود در دوایر و بخش‌ها - سایر موارد.

پس از تعیین و شناسایی دارایی‌ها، تیم ارزیابی اقدام به شناسایی ریسک‌های مربوط به هر یک از دارایی‌ها می‌نماید. همان‌طور که از تعریف ارائه شده برای ریسک استنباط می‌شود، هر

ریسک از سه عنصر یا جزء تشکیل شده است. لذا تعریف ریسک به معنی تعیین دقیق این سه عنصر است. این سه عنصر عبارتند از عامل تهدید، سرمایه و اثر تهدید. به‌عبارت دیگر:

ریسک = عامل تهدید + سرمایه + اثر تهدید

همان‌گونه که از رابطه فوق بر می‌آید، با تغییر هر یک از اجزاء موجود در طرف چپ تساوی فوق، ریسک جدیدی حاصل می‌شود. در نتیجه در اغلب موارد امکان دارد که برای یک دارایی مشخص، چندین ریسک مختلف را با توجه به نوع عامل تهدید و انواع اثرات آن، بتوان شناسایی نمود. در این صورت، برای هر مورد، یک شناسنامه ریسک به‌طور مجزا تهیه خواهد شد.

۱۰-۶-۱-۲- ارزیابی مستمر و شناسایی مداوم ریسک‌های مربوط به ماموریت IT

بسیاری از پروژه‌ها که فرض می‌شود تحت کنترل هستند، با ریسک به عنوان رخدادی شناخته نشده روبرو گردیده و کوشش می‌کنند آن را کنترل کنند. اکثر پروژه‌ها چنین رخدادهایی را به خوبی از سر رد می‌کنند ولی با یک تلاش جامع مدیریت ریسک، رویدادهای ریسک قبل از وقوع، شناسایی و کنترل می‌گردند و یا برنامه‌ای تهیه می‌شود که در زمان وقوع این رویدادها با آن‌ها مقابله کند.

با درنظر گرفتن این مفاهیم پایه‌ای، امکان مقابله با ریسک به وجود می‌آید. لذا ابتدا باید نسبت به شناسایی ریسک‌های محتمل پروژه اقدام کرد. این کار با دسته‌بندی ساختار کارها و با پرسش چند سئوال از خود یا اعضای گروه پروژه، امکان‌پذیر است.

ممکن است سئوال‌های دیگری نیز به ذهن شما خطور کند که البته این سئوال‌ها سرآغاز خوبی است که شما را در مسیر درست هدایت کند. هرچیزی که به مغز شما خطور می‌کند فهرست کنید، سپس در مرحله بعد تعیین کنید که آیا نیاز به مقابله و پیش‌گیری ریسک است یا بایستی تا زمان وقوع آن صبر کرد. اگر ریسک‌ها را مشخص کنید و تصمیم بگیرید که هیچ عملی نباید انجام گیرد باز به‌تر از آن است که آن‌ها را شناسایی نکرده باشید. پس از این مرحله تمام ریسک‌های شناسایی شده را کمی کنید ؛ ابتدا ریسک‌ها را دسته‌بندی و سپس احتمال وقوع هر ریسک را تعیین کنید. برای تخصیص مقادیر احتمالی به ریسک‌ها از مقادیر پیش‌نهادی زیر می‌توانید استفاده کنید :

اکنون احتمال وقوع هر ریسک قابل محاسبه است. راه دیگر، نسبت دادن درصد وزنی به هریک از ریسک‌هاست. مشکل اصلی این روش آن است که همواره داده‌های تجربی به‌اندازه کافی در دسترس نیستند تا این کار به دقت انجام گیرد. در این روش معمولاً افراد باتجربه‌ای مبادرت به این کار می‌کنند که تجارب جامعی از انواع رویدادها در پروژه‌های مختلف کسب کرده‌اند ؛ مجموع درصدهای تخصیصی به رویدادها بایستی صد باشد.

در مرحله بعد به هر ریسک، یک مقدار نسبت دهید. این مقدار می‌تواند در صورت نیاز برحسب هزینه یا زمان باشد ؛ به عنوان مثال اگر هدف تعیین زمان اتمام پروژه است، هر ایده‌ای در مورد مدت زمان فعالیت‌ها می‌تواند یک سناریوی ریسک محسوب شود. در این مرحله می‌توان مقدار حقیقی ریسک را با محاسبه حاصل‌ضرب مقادیر تخصیص داده شده به ریسک و احتمال وقوع آن به دست آورد و با توجه به نتایج حاصل می‌توان نسبت به انجام عملی یا به تعویق انداختن آن تصمیم‌گیری نمود. بعد از انجام مراحل مدیریت ریسک، می‌توانید فرآیندهای نگهداری مجموعه ریسک را آغاز کنید. برای این کار بازنگری دوره‌ای ریسک را آغاز کنید که مبتنی بر پیچیدگی و مدت پروژه و وقوع تغییرات پروژه است.

آغاز اجرای این کار ممکن است بیهوده و هزینه‌زا به نظر آید اما چنان‌چه یک‌بار این کار را انجام دهید و ریسک‌ها را شناسایی و به صورت کمی آن‌ها را کنترل کنید در آن صورت به ارزش مدیریت ریسک پی خواهید برد. بنابر این در مرحله نخست اقدام به شناسایی ریسک‌های پروژه در بالاترین سطح WBS کنید و از این که راه به سطوح پایین‌تر می‌یابید نگران نباشید. بعد از چند بار انجام این کار، مسأله خیلی واضح‌تر خواهد شد.

ما در دنیای مخاطرات ریسک زندگی می‌کنیم. باید ریسک‌ها را تحلیل کنیم ؛ اگر با آن‌ها برخورد داریم باید آن‌ها را شناسایی و در مجموع تمام ریسک‌ها و عواید آن‌ها را باید ارزیابی کنیم. منافع حاصل از مدیریت ریسک ممکن است تا غلبه پروژه بر آن ملموس نباشد اما به خاطر داشته باشید که کسی که از برنامه‌ریزی اجتناب کند به طور حتم برنامه شکست پروژه خود را طرح‌ریزی نموده‌است !

۱۰-۶-۱-۲-۱-فهرست نمونه‌ای از انواع ریسک‌های قابل اعمال بر سازمان مبتنی بر IT:

- خرابی‌هارد رایانه سرور/ شخصی بدلیل سهل انگاری مسئول/ کاربر مربوطه
- خرابی‌هارد رایانه سرور/ شخصی به‌دلیل نفوذ ویروس از طریق اینترنت
- خرابی‌هارد رایانه سرور/ شخصی بدلیل نفوذ ویروس از طریق کاربران
- دسترسی غیر مجاز به اطلاعات موجود در رایانه سرور/ شخصی توسط کاربران داخلی
- دسترسی غیر مجاز به اطلاعات موجود در رایانه سرور/ شخصی از طریق اینترنت
- افشای غیر مجاز اطلاعات موجود در رایانه سرور/ شخصی به دلیل سهل انگاری کاربر مجاز
- افشای غیر مجاز اطلاعات موجود در رایانه سرور/ شخصی از طریق اینترنت
- سرقت اطلاعات موجود در رایانه سرور/ شخصی از طریق اینترنت

- سرقت اطلاعات موجود در رایانه سرور/ شخصی به دلیل سهل انگاری کاربر مجاز
- عدم سرویس دهی رایانه سرور/ شخصی به‌علت نفوذ ویروس از طریق اینترنت
- عدم سرویس دهی رایانه سرور/ شخصی به‌علت نفوذ ویروس از طریق کاربر مجاز
- عدم سرویس دهی رایانه سرور/ شخصی به‌علت قطع برق و نبود UPS

۱۰-۶-۱- ۳-شرح ریسک‌های مرتبط با محرمانگی سرمایه‌های اطلاعاتی سازمان:

- داده / اطلاعات به‌طور نادرستی توسط مسئول مربوطه یا کاربر برچسب گذاری شود.
- داده / اطلاعات به‌طور نادرستی توسط مسئول مربوطه یا کاربر دسته بندی شود.
- داده / اطلاعات قبل از این‌که از طریق کانال‌های مناسب انتشار یابد به اشتراک گذاشته شود.
- استفاده از سیستم‌های غیر امن برای انتقال داده / اطلاعات حساس
- افشای اطلاعات و نقض قوانین حریم شخصی و مالکیت
- عدم وجود توضیحات شفاف در مورد قوانین محرمانگی
- محافظت نامناسب از فهرست کلمات عبور
- وجود در پشتی[۱] در نرم‌افزارها داده‌ها و برنامه‌های کاربردی
- مدیر اجرایی عصبانی و ناراضی که دارای امتیازات و توانایی‌های امنیتی بالایی باشد.
- عدم بررسی کامل اثرات نهفته و مخفی قبل از اعمال نمودن تغییرات مورد نیاز بر روی سیستم‌ها و برنامه‌های مورد استفاده سازمان
- توانایی حدس زدن مشخصات فردی دیگر توسط کاربران سازمان یا هکرها
- کارمندان و افراد از طریقه نحوه صحیح انتشار یا ذخیره کردن اطلاعات موجود بر روی وب ناآگاه باشند.
- دست‌پاچه و گیج شدن مسئولین امنیتی شبکه در مورد جایی که اطلاعات حساس در آن‌جا ذخیره شده است.
- دادن قابلیت دسترسی به افرادی که از نظر شغلی نیازی به داشتن این امتیاز نداشته باشند.
- اطلاعات مربوط به سیستم‌های داخلی به‌طور سهوی انتشار یابند که ممکن است در آینده برای حمله به سیستم مورد استفاده قرار گیرند.
- استفاده از IDهای مشترک توسط کاربران سازمان

[۱] backdoor

- دسترسی به فایل‌های پشتیبانی کننده توسط مدیر اجرایی سیستم به‌طور مناسبی کنترل نشود.

– تکنولوژی‌های جدید باعث نفوذ در مسایل محرمانگی شوند.

– تلاش‌ها وتصمیماتی برای تغییر دادن مدل امنیتی صورت گیرد.

- عدم تشریح مسایل محرمانگی برای افراد غیر کارمند موجود در سازمان - ردیابی بسته‌ها توسط افراد غیر مجاز از خارج سایت اینترنتی سازمان

- جریمه‌های در نظر گرفته شده برای تخطی کردن از مقررات امنیتی آنقدر کافی نباشد که باعث جلوگیری کردن از فعالیت‌های نامناسب افراد گردد.

- امکان وجود تجهیزات استراق سمع الکترونیکی در محل‌های مختلف مجموعه مورد نظر

۱۰-۶-۱-۴-شرح ریسک‌های مرتبط با تمامیت سرمایه‌های اطلاعاتی سازمان:

- پایگاه داده توسط خطای سخت‌افزاری، نرم‌افزار بد، یا نادرست خراب شود.

- عدم گزارش کردن نکات و موارد مربوط به تمامیت توسط کاربران سازمان

- اجرای ناقص یک روند یا عدم توانایی در اجرای صحیح روند توسط افراد باعث خراب شدن داده شود.

- نبود پردازش‌های داخلی برای ایجاد کنترل و مدیریت داده در حین انجام فعالیت‌های مختلف

- عدم تشخیص و اعلام مشکلات تمامیت به‌وجود آمده توسط کاربران و مسئولین امنیتی شبکه سازمان

- امکان دسترسی اشخاص ثالث به اطلاعات محرمانه موجود در سازمان

- عدم تعیین صلاحیت منشای تقاضا کننده درخواست در روال‌ها و سیاست‌های موجود در سازمان

- عدم قابلیت دسترسی به اطلاعاتی که مجاز به دسترسی به آن‌ها می‌باشید.

- کارمندان مربوطه آموزش‌های لازم برای انجام تغییرات مورد نیاز را دریافت نکرده باشند.

- عدم پاسخ دهی مناسب به تقاضاهای انجام شده در مدت زمان مورد نظر

- تغییرات انجام شده در داده/نرم‌افزارهای سیستم یا برنامه‌های کاربردی ذخیره نشده باشند.

- استفاده کاربران از کپی‌هایی از داده که از رده خارج شده باشند.

- وجود مشکلات هم‌سان سازی و یک‌نواخت کردن در هنگام استفاده از وسیله‌های جبران ساز و بازگرداننده توسط کاربران
- تغییر داده‌ها به‌علت وجود ویروس
- عدم گزارش کردن به‌موقع وضعیت کاربران، توسعه دهندگان، پشتیبانی کنندگان وغیره... توسط مسئولین مربوطه

۱۰-۶-۱-۵-شرح ریسک‌های مرتبط با در دسترس بودن سرمایه‌های اطلاعاتی سازمان:

- هکرها سایت مجموعه مورد نظر را تعطیل نمایند.
- نفوذکنندگان قادر به دسترسی فیزیکی به تجهیزات و امکانات مجموعه مورد نظر شوند.
- وجود خطای سخت‌افزاری در مورد سرور اینترنت
- ارتباطات موجود با تهیه کننده سرویس قطع شود.
- سایت میزبان، محافظ‌های فیزیکی مناسبی برای اطلاعات نداشته باشد.
- ارتباط با سیستم‌های پشتیبان اداره قطع شود.
- طراحی کلی سیستم پیچیده باشد.
- ایجاد تغییرات نادرست نرم‌افزار یا سخت‌افزار سیستم توسط کاربران مجاز
- مقادیر و پیش بینی‌های مورد استفاده و معمول غیر قابل انتظار باشند.
- روندهای برنامه استمرارپذیری سازمان آزمایش نشده باشند.
- هیچ تضمینی برای آماده بودن سرور توسط تهیه کننده سرویس داده نشده باشد.
- اقدامات و اعتصاب‌هایی در سازمان تهیه کننده سرویس، به‌وقوع بپیوندد.
- تعمیر و نگهداری برنامه ریزی شده معمولی، باعث آماده و در دسترس نبودن سرویس شود.
- طراحی توپولوژی مانع کارایی / قابل قبول بودن میزان در دسترس بودن سرویس‌های عمومی شود.
- سرمایه گذاری‌های نامناسب سازمان برای قابلیت‌های پشتیبانی
- حملات برنامه ریزی شده توسط معترضان و مخالفین سازمان
- ساختار بندی سیستم برای در دسترس بودن زیاد مناسب نباشد.
- منابع و افراد تکنیکی سازمان آموزش‌های مناسب ندیده باشند.
-تراکم موجود در اینترنت باعث عدم رضایت کاربران شود.
- به‌علت وجود ویروس، ممکن است داده / اطلاعات در دسترس نباشند.

- به‌علت عدم نظارت کافی بر سایت وب سازمان، ممکن است آماده نبودن سیستم گزارش نشود.
- به‌علت نقص در روتر یا دیواره آتش، ممکن است دسترسی به سرویس‌ها امکان پذیر نباشد.
- پشتیبان‌های موجود در سازمان کافی نباشند.
- سوء استفاده کاربران از امکانات شبکه، کلمات عبور سایر افراد

۱۰-۶-۲- عوامل موفقیت در مدیریت ریسک فن آوری

- ضمانت اجرائی
- تعریف یک لیست مشخص از افرادی که در مقوله امنیت ذی‌نفع می‌باشند.
- وجود بلوغ سازمانی در ارتباط با مدیریت ریسک‌ها امنیتی:
- وجود یک فضای فکری باز برای کارگروهی :
- دید سیستماتیک نسبت به سازمان :
- اختیارات لازم برای گروه مدیریت ریسک‌ها امنیتی :

۱۰-۷- انواع بحران

پیچیدگی فزآینده جوامع مختلف و گسترش ارتباط و وابستگی چند جانبه صنایع، زمینه مساعدی برای رشد کمی و کیفی فرصت‌ها و تهدیدات محیط، فراهم ساخته است. چنان‌چه از یک سو رشد و توسعه تکنولوژی انسان را در جدال با رخدادهای طبیعی قدرتمند ساخته و از سویی دیگر پیچیدگی و ارتباط تنگاتنگ صنایع سبب بروز معضلات همه جانبه در رخدادهای ظاهراً واحد شده است. مقایسه قطع برق یک روستا با مورد مشابه در یکی از شهرهای بزرگ جهان به‌خوبی نشان‌گر درجه آسیب‌پذیری جوامع پیش‌رفته است. مقایسه فوق قبل از این که مقایسه دو نوع جامعه باشد، نشان‌گر گسترش دامنه هرنوع بحران در جوامع پیچیده است. مرور کوتاهی برچند نمونه بارز از بحران‌های مختلف بیست سال گذشته جهان نکات زیر را نشان می‌دهد:

O صنایع خاصی ظرفیت بالقوه بیش‌تری برای بروز بحران دارند. از جمله، شیمیایی و پتروشیمی، برق، حمل و نقل هوایی، کشتیرانی؛

O باوجود تفاوت این بحران‌ها، ویژگی‌های مشترک زیادی در بحران‌های مختلف به چشم می‌خورد؛

O آمادگی قبلی در کاهش ابعاد خسارت نقش تعیین‌کننده دارد؛

O تصمیم‌گیری‌های عجولانه براساس اطلاعات ناقص دامنه خسارت را چند برابر افزایش می‌دهد؛

O ارتباطات در ابعاد مختلف نقش بسیار تعیین کننده‌ای در کنترل بحران دارد.

وظیفه مدیریت بحران اتخاذ تصمیمات موثر براساس اطلاعات صحیح درجهت کاهش خسارات و کنترل سریع بحران است.

باید در تمام برنامه‌ریزی‌های بحران جایی را برای موقعیت‌های پیش‌بینی نشده درنظر گرفت.

بحران عبارت است از وضعیتی که نظم سیستم اصلی یا قسمت‌هایی از آن را مختل کرده و پایداری آن را برهم زند.

غافل‌گیری اولین عامل مخرب در بحران‌هاست.

تصمیم‌گیری‌های مهم همواره از ضروریات بحران در لحظات اول است.

اتخاذ تصمیم‌های درست به‌هنگام بروز بحران به دسته‌بندی و اقعیت‌ها بستگی دارد.

بحران چیزی جزء تجلی برخورد تمام عواملی که یک مرتبه از حالت نظم به حالت بی‌نظمی درآمده، نیست.

هیچ بحرانی شبیه دیگری نیست و درک تشابهات کلیدی برای برنامه‌ریزی به‌منظور رویارویی با آن و تخفیف اثرات سوء بسیار ضروری است.

دولت‌ها و شرکت‌ها به شناخت روش‌های برخورد با تغییرات ناگهانی روی آورده‌اند و مدیریت بحران بخشی از تمام برنامه‌های استراتژیک آن‌ها شده است.

نکات فوق‌انگیزه‌ی مثبتی برای تجربه اندوزی از بحران‌های گذشته ایجاد می‌کند، لیکن حداقل سه دلیل سبب می‌شود نتایج حاصل از بررسی بحران‌های گذشته شناخت لازم و کافی را به پژوهش‌گران ارائه ندهد. نخست این که نوشته‌های تاریخی محدود به وصف واقعه است و تحلیل‌های تطبیقی لازم پابه‌پای شرح رخداد ارائه نشده است. نکته دوم متأثر از نگرشی است که هر بحران را در نوع خود بی‌نظیر می‌داند و سومین دلیل این که مفهوم عمومی بحران بسیار ابهام برانگیز است. اکثر تحلیل‌گران موقعیت‌های حاد و اضطراری را بازگو کرده‌اند در صورتی که بحران دارای ویژگی‌هایی است که صفات مشخصه آن‌را تعیین می‌کند، در نتیجه وجود شرایط کمی و کیفی خاصی، امکان توجیه رویداد در الگوی بحران را فراهم می‌سازد.

بنابراین نه‌تنها بررسی بحران‌های گذشته، بلکه فعالیت‌های سیستماتیک دیگری نیز به‌منظور دست‌یابی به عوامل و عناصر مشترک در بروز بحران‌ها و یافتن الگوهایی برای پیش‌بینی و پیش‌گیری آثار ناشی از آن‌ها ضروریست.

۱۰-۸- استانداردها و گواهی نامه‌های امنیتی

۱۰-۸-۱- استاندارد iso ۱۷۷۹۹

این استاندارد در ده بخش و بیش از **۱۲۷** نوع متد جهت سنجش امنیت سیستم سازمان‌دهی گردیده است. هر بخش بر روی یک سرفصل یا محدوده عمل‌کرد مجزا تعریف شده است. ده عنوان و اهداف آن عبارتند از:

۱) **طرح تداوم خدمات تجاری :** اهداف این بخش شامل جلوگیری از منقطع شدن فعالیت‌های تجاری و فرآیندهای بحرانی اقتصادی بر اثر حوادث ناگوار و یا ناتوانی در ارائه خدمات در سطح وسیع می‌باشد.

۲) کنترل بر نحوه دست‌یابی به سیستم : اهداف این بخش شامل :

۲-۱) کنترل دسترسی به اطلاعات.

۲-۲) جلوگیری از دست‌یابی غیر مجاز به سیستم اطلاعاتی.

۲-۳) ایجاد تضمین در نحوه خدمت رسانی حمایت شده شبکه.

۲-۴) جلوگیری از دست‌یابی غیر مجاز به رایانه‌ها.

۲-۵) بازرسی و نظارت بر فعالیت‌های غیر مجاز.

۲-۶) اطمینان حاصل کردن از امنیت اطلاعات در زمانی که در شبکه از تجهیزات شبکه بی‌سیم و یا تلفن سیار استفاده می‌گردد.

۳) پشتیبانی کردن و توسعه دادن سیستم :

اهداف این بخش شامل :

۳-۱) اطمینان از امکانات امنیتی ایجاد شده در درون سیستم‌های قابل کنترل.

۳-۲) ممانعت از گم شدن، تغییر و سوءاستفاده از داده‌های کاربران در سیستم‌های کاربردی.

۳-۳) حمایت از جنبه‌های محرمانگی، صحت و تمامیت اطلاعات.

۳-۴) اطمینان از پروژه‌های IT و فعالیت‌های حمایتی آن که در یک چارچوب امن هدایت خواهند شد.

۳-۵) پشتیبانی امنیتی از داده‌ها و نرم‌افزارهای کاربردی.

۴) ایجاد امنیت فیزیکی و محیطی:

اهداف این بخش شامل:

۴-۱- ممانعت از دسترسی غیر مجاز،

۴-۲-آسیب رسانی و دخالت در بنیادهای اقتصادی و اطلاعات ؛

۴-۳- ممانعت از گم شدن،

۴-۴- آسیب دیدن و مصالحه بر سر دارایی‌ها برای تعلیق فعالیت‌های اقتصادی مؤسسه ؛

۴-۵- ممانعت از مورد مصالحه قرار گرفتن یا سرقت اطلاعات و هم‌چنین امکانات پردازش اطلاعات می‌گردد.

۵) مورد قبول واقع شدن:

اهداف این بخش شامل :

۵-۱) اجتناب از بروز هرگونه رخنه‌ای که مجرمانه بوده یا قوانین مدنی، قوانین موضوعی، قوانین تنظیمی یا قراردادهای الزام‌آور و هر نوع نیاز امنیتی را مورد هدف قرار دهد.

۵-۲) ایجاد اطمینان از هم‌خوانی سیستم‌ها با سیاست‌های امنیتی و استانداردهای سازمانی.

۵-۳) به حداکثر رساندن تاثیرات کارا و به حداقل رساندن فرآیندهای اخلال کننده سیستم مراقبت امنیتی وارد شده بر سیستم یا صادر شده از سیستم.

۶) امنیت شخصی:

اهداف این بخش شامل:

۶-۱- کاهش خطرات ناشی از خطاهای انسانی،

۶-۲- دزدی، تقلب یا سوءاستفاده از امکانات ؛

۶-۳-ایجاد اطمینان از این‌که کاربران از تهدیدها امنیتی موجود بر روی اطلاعات واقف و نگران بوده و در روش‌های کاری معمول خود، در جهت حمایت از سیاست‌های امنیتی، شراکت خواهند داد ؛

۶-۴- به حداقل رساندن خسارت‌های ناشی از بروز حوادث امنیتی و سوء عمل و هم‌چنین درس گرفتن از این رخدادهای امنیتی می‌باشد.

۷) ایجاد امنیت سازمانی:

اهداف این بخش شامل :

۷-۱) مدیریت امنیت اطلاعات در محدوده شرکت.

۷-۲) پشتیبانی از امکانات امنیت فرآیندهای اطلاعاتی سازمانی و دست‌یابی به دارایی‌های اطلاعاتی به واسطه عوامل ثالث[۱].

۷-۳) پشتیبانی از امنیت اطلاعات در زمانی که وظیفه پردازش اطلاعات شرکت، به‌صورت Outsource به سازمان دیگری سپرده شده باشد.

۸) مدیریت رایانه و عملیات:

اهداف این بخش شامل :

۸-۱) ایجاد اطمینان از عملیات موجود و امنیتی بر روی امکانات پردازش اطلاعات.

۸-۲) به حداقل رساندن خطرات ناشی از ناتوانی‌های سیستم.

۸-۳) حمایت از تمامیت اطلاعات و نرم‌افزار.

۸-۴) پشتیبانی از در دسترس بودن و تمامیت پردازش اطلاعات و ارتباطات.

۸-۵) ایجاد اطمینان از امن نگهداشتن اطلاعات در شبکه‌ها و حمایت از زیربنای پشتیبانی کننده.

۸-۶) ممانعت از آسیب رسیدن به دارایی‌ها و تعلیق فعالیت‌های اقتصادی.

۸-۷) ممانعت از گم شدن، تغییر دادن و سوءاستفاده از اطلاعات در حال مبادله مابین سازمان‌ها.

۹) کنترل و طبقه بندی دارایی‌ها:

اهداف این بخش شامل:

پشتیبانی مناسب حمایتی از دارایی‌های مشترک و اطمینان از این که دارایی‌های اطلاعاتی در یک سطح مناسب امنیتی دریافت می‌گردد، می‌باشد.

۱۰) امنیت اطلاعاتی:

اهداف این بخش شامل:

ایجاد مدیریت هدفمند و حمایتی برای امنیت اطلاعات می‌گردد.

۱۰-۸-۲- استاندارد ۲۷۰۰۱

استاندارد **ISO۲۷۰۰۱** حفاظت از اطلاعات را در سه مفهوم خاص یعنی قابل اطمینان و محرمانه بودن بودن اطلاعات[۲]، صحت اطلاعات (یک‌پارچگی)[۳] و در دسترس بودن اطلاعات

---

[۱] Third Party
[۲] Confidentiality
[۳] Integrity

(قابلیت دسترسی)[۱] تعریف می‌نماید. در زیر جهت نحوه عمل‌کرد و مدیریت سیستم امنیت اطلاعات توضیحاتی بیان گردیده است. برخی از تعاریف موجود در این استاندارد بیان گردیده که جهت درک به‌تر به آن می‌پردازیم :

اطلاعات [۲] : دانشی که ممکن است از هر منبعی برگرفته شود و یا به‌عبارتی داده‌های پردازش شده‌ای که جزء دارایی‌ها محسوب می‌شوند. معمولاً ۳۶٪ اطلاعات برروی کاغذ، ۲۰٪ در اسناد الکترونیکی و ۴۴٪ دیگر در ذهن افراد ذخیره می‌گردد.

دارایی [۳] : هر چیزی که برای سازمان دارای ارزش می‌باشد.

قابلیت دسترسی: ویژگی در دسترس و قابل استفاده بودن، به محض تقاضای یک موجودیت مجاز. (اطلاعات در صورت نیاز باید به‌طور صحیح در دسترس باشد.)

محرمانه بودن : ویژگی که اطلاعات در دسترس افراد، موجودیت‌ها یا فرآیندهای غیر مجاز قرار نگرفته یا فاش نشود. (تنها افراد مجاز به اطلاعات دسترسی خواهند یافت.)

یک‌پارچگی: کامل بودن و صحت اطلاعات و روش‌های پردازش اطلاعات مورد نظر هستند.

امنیت اطلاعات : حفظ محرمانه بودن، یک‌پارچگی و قابلیت دسترسی اطلاعات، هم‌چنین ویژگی‌هایی از قبیل سندیت، پاسخ‌گویی، انکار ناپذیری و قابلیت اطمینان، می‌توانند لحاظ شوند.

رخداد امنیت اطلاعات : رخداد شناسایی شده یک سیستم، خدمت یا شبکه، که دلالت بر نقص احتمالی خط مشی امنیت اطلاعات یا نقص حفاظتی، یا وضعیتی که ممکن است با امنیت مرتبط بوده و قبلاً شناخته نشده باشد.

رویداد امنیت اطلاعات : یک یا مجموعه‌ای از رویدادهای امنیت اطلاعات ناخواسته یا پیش بینی نشده که به احتمال زیاد، عملیات کسب و کار را به خطرانداخته و امنیت اطلاعات را تهدید کنند.

این استاندارد بین المللی دارای ۸ بند است که از بند ۴ تا ۸ بندهای اصلی استاندارد شروع می‌شود. هم‌چنین این استاندارد دارای ۱۱ هدف کنترلی است و هر گروه شامل چندین زیر مجموعه می‌باشد که به پیوست استاندارد ارائه شده است. (بند ۵ تا ۱۵ استاندارد

---

[۱] Availability
[۲] information
[۳] asset

ISO/IEC۱۷۷۹۹:۲۰۰۵) هیچ یک از بندهای استاندارد بجز اهداف کنترلی و با ذکر دلیل قابل استثناء کردن نمی‌باشد. این گروه‌های کنترلی عبارتند از :

۱- خط مشی امنیت (سیاست‌های امنیتی)
۲- امنیت سازمان
۳-کنترل و طبقه بندی دارایی‌ها(مدیریت دارایی‌ها)
۴- امنیت منابع انسانی(امنیت فردی)
۵- امنیت فیزیکی و محیطی
۶- مدیریت ارتباطات و عملیات‌ها
۷- کنترل دسترسی‌ها
۸- نگهداری سیستم‌های اطلاعاتی و اکتساب توسعه
۹- مدیریت رویداد امنیت اطلاعات
۱۰- مدیریت پیوسته کسب و کار
۱۱- سازگاری با موارد قانونی

این استاندارد بین المللی سازگار با سری استانداردهای مدیریت کیفیت (ISO۹۰۰۱:۲۰۰۰) و مدیریت زیست محیطی (ISO۱۴۰۰۱:۲۰۰۴) می‌باشد. هم‌چنین این استاندارد بین المللی، قابل استقرار در تمامی سازمان‌ها بوده و الزاماتی را برای ایجاد، اجرا، پایش، بازنگری، نگهداری و بهبود یک سیستم مدیریت امنیت اطلاعات مستند نموده و با در نظر گرفتن مفهوم ریسک کلان، کسب و کار سازمان را مشخص می‌کند. جهت استقرار سیستم مدیریت امنیت اطلاعات موارد زیر می‌بایست صورت پذیرد:

۱) ایجاد سیستم امنیت اطلاعات:

الف) تعریف دامنه کاربرد و مرزهای ISMS بر مبنای ویژگی‌های کسب کار سازمان، مکان، دارایی‌ها و فن‌آوری.

ب) تعرف خط مشی ISMS بر مبنای ویژگی‌های کسب و کار، سازمان، مکان، دارائی‌ها و فن‌آوری.

ج) تعریف رویکرد ارزیابی ریسک سازمان (ISO/IEC TR۱۳۳۳۵-۳)

د) شناسایی ریسک (شناسایی دارائی‌ها، تهدیدهای اموال، آسیب‌پذیری‌های ناشی از تهدیدها، آسیب‌های ناشی از دسترس بودن، محرمانه بودن، یک‌پارچگی و قابلیت دسترسی به دارائی‌ها.)

ه) تحلیل و ارزیابی ریسک (نقص‌های امنیتی و احتمال بروز نقص‌های امنیتی).

و) شناسائی و ارزیابی گزینه‌هایی برای اصلاح ریسک.
ز) انتخاب اهداف کنترلی و کنترل‌ها برای اصلاح ریسک.
ح) دریافت مصوبه مدیریت برای ریسک باقیمانده پیش‌نهادی.
ط) دریافت مجوز مدیریت برای اجرا و عمل نمودن ISMS.
ی) تهیه بیانیه قابلیت کاربرد.

۱۰-۸- ۳- نقد استانداردهای رایج و محدودیت پذیری آن‌ها

باید این نکته را مد نظر داشت که استانداردها با توجه به نیازمندی‌های هر فرهنگ و هر کشوری ایجاد شده است و بدون بومی سازی آن‌ها نمی‌توان به صورت کورکورانه و تبعیت محض از استانداردهای وارداتی انتظار تامین امنیت را داشت. همیشه باید مد نظر داشت که امنیت نمی تواند وارداتی باشد و می‌بایست به صورت بومی و با توجه به نیازهای واقعی هر کشور و هر سازمانی نسبت به تعیین استانداردهای مورد نیاز اقدام نمود.

برخی از استانداردها در تمام دنیا قابل پیاده سازی شدن می‌باشند ولی بسیاری از آن‌ها چنان‌چه بدون شناخت واقعی از موقعیت‌های سازمانی و انطباق و یا عدم انطباق با شرایط داخلی مورد استفاده قرار گیرند معمولا دارای تبعات بالعکسی خواهند بود.

نکته بعد این‌که باید در نظر داشت استانداردها هرچند که کامل هم باشند به عنوان کف اقدامات امنیتی می‌باشند و نه سقف اقدامات. برخی از متخصصین استانداردها را سقف اقدامات در نظر گرفته و صرفاً به آن‌ها بسنده می‌کنند و در آینده سازمان را با مخاطرات نا شناخته‌ای روبرو می‌سازند.

۱۰-۹- انواع سیاست

سیاست‌ها و پروسه‌های کاری زیادی وجود دارد که تعیین کننده چگونگی پیاده سازی امنیت سازمان است. اما در تمام این سیاست گذاری‌ها، سه بخش مشترک وجود دارد که عبارتند از :

۱- **هدف :** در هر روش و سیاست گذاری، اهم مطالب توضیح داده شده باشد. در بخش هدف سند سیاست‌گذاری باید به وضوح گفته شود چرا سیاست‌گذاری ایجاد شده است و سازمان مربوطه به چه منافعی خواهد رسید ؟

۲- **حوزه عمل :** لازم است هر سیاست‌گذاری شامل بخشی باشد که قابلیت اجرای آن‌را تعیین کند. برای مثال ممکن است سیاست‌گذاری امینتی به تمام سیستم‌های رایانه‌ای و شبکه‌ها اعمال شود در حالی که سیاست گذاری اطلاعاتی به تمام پرسنل یک سازمان اعمال می‌شود.

۳- **مسئولیت :** در این بخش تعیین می‌شود برای اجرای درست و کامل یک پروسه چه کسی مسئول است. مسئولیت به هر کسی سپرده شود لازم است به درستی آموزش داده شود و از نیازهای آن سیاست‌گذاری مطلع گردد.

۱۰-۹-۱- ملاحظات اجرای سیاست‌های امنیتی

هدف سیاست امنیتی عبارتست از ایجاد بنیان اولیه سیستمی حاوی تعدادی فرآیند و شیوه اجرایی که باعث ارتقاء امنیت یک سازمان، و ایجاد آگاهی عملیاتی از اهداف امنیت در ذهن کارکنان و ذی‌نفعان سازمان می‌شود. فرآیندها و دستورالعمل‌ها ابزار لازم برای اجرای امنیت را فراهم می‌آورد، و آگاهی امنیتی باعث تداوم آن در سازمان می‌شود.

اصل اول : در سیاست امنیتی این است که کارکنان سازمان انسان‌های معقول و سلیم النفسی هستند.

اصل دوم : در سیاست امنیتی بر این باور تاکید دارد که جریان و سرعت گردش اطلاعات و صحت و قابلیت دسترسی اطلاعات در اثر هیچ گونه عملیاتی نباید مختل شود.

اصل سوم : دموکراسی سازمانی بر جریان آزاد اطلاعات تاکید دارد و سعی سازمان بر این است که محتوای اطلاعاتی هر چه بیش‌تر، کارآمدتر و مفیدتری در اختیار ذی‌نفعان سازمان قرار گیرد

اصل چهارم : سیاست و عملیات امنیت اطلاعات با نگرش به حفظ دست‌آوردهای سازمانی، آرامش و اطمینان کارکنان و ذی‌نفعان و جریان سالم و توسعه‌ای دانش سازمانی تدوین و اعمال می‌شود و نه ایجاد محدودیت یا بازدارندگی.

چرا تمهیدات امنیتی ضرورت دارند؟

مهم‌ترین دلایل این مسئله عبارتند از:

• ارزش سرمایه گذاری روی تجهیزات سخت‌افزاری وبرنامه‌های نرم‌افزاری

نکته قابل توجه این است که رایانه‌ها و بسته‌های نرم‌افزاری بسیار گران قیمت هستند و جای‌گزینی آن‌ها پرهزینه و دشوار است. حتی اگر دریک رخداد امنیتی نرم‌افزارها و سخت‌افزارها کاملا از بین نروند ممکن است مشکلات امنیتی ما را وادار به نصب مجدد همه نرم‌افزارها کنند و متعاقباً لازم شود کلیه نیازهای اساسی مجدداً تعریف گردند. این امرمستلزم صرف زمان بسیار زیادی است؛ خصوصاً اگر فرد مسئول، اطلاعات فنی کافی در این زمینه نداشته باشد.

• ارزش داده‌های سازمانی

با ارزش‌ترین محتویات بر روی یک رایانه، اطلاعات و داده‌های ایجاد شده توسط کاربر می‌باشد و شاید وجود همین اطلاعات که ضرورت استفاده از رایانه یا شبکه را توجیه می‌نماید.

سیستم‌های عامل و نرم‌افزارها را در بسیاری از موارد و هم‌زمان با بروز مشکل در سیستم می‌توان مجددا نصب نمود ولی داده ایجاد شده در نوع خود منحصر به فرد بوده و در صورت از دست دادن برخی داده‌های مهم می‌تواند در نهایت منجر به زیان‌های عمده و غیر قابل جبران گردد.

• ارزش داده‌های فردی

ممکن است داده‌های فردی ارزش مادی چندانی نداشته باشند ولی از دست دادن آن‌ها بسیار زیان آور باشد و برای ایجاد دوباره اطلاعات زمان بسیار زیادی لازم باشد.

• تهدیدها جنایتکاران رایانه‌ای

همگام با پیشرفت‌های فن‌آوری، گروهی از خرابکاران که از دزدی داده‌های رایانه‌ای سود می‌برند نیز به‌وجود آمده‌اند. در مواردی این کار صرفاً برای لذت و سرگرمی صورت می‌گیرد و برخی افراد نیز تنها به‌خاطر خودنمایی در برابر دوستان خود دست به چنین کارهایی می‌زنند؛ اما در بعضی موارد این‌کار برای دست‌یابی به منافع شخصی و سازمانی انجام می‌گیرد. در تمامی موارد مذکور این اشخاص باعث ایجاد خسارت و گسترش بی اعتمادی می‌شوند و در حد گسترده‌تر مشکلات بحرانی به‌وجود می‌آورند که به اشخاص و موقعیت‌های شغلی صدمه وارد می‌کند. باید گفت از زمانی که اینترنت در مقیاس جهانی در اختیار کاربران قرار گرفته، تعقیب و متوقف کردن مهاجمین هرچند همچنان امکان‌پذیر می‌باشد ولی بسیار پیچیده شده است.

چرا معمولاً دربرنامه‌های نرم‌افزاری از بعُد امنیت ضعف وجود دارد؟

برنامه‌های نرم‌افزاری غالباً بدون درنظر گرفتن مسائل امنیتی تولید می‌شوند.

این مسئله چند دلیل دارد:

• سهل انگاری

برنامه نویسان و طراحان از اهمیت نکات امنیتی اطلاعی ندارند.

• اولویت پایین

تا چندی قبل حتی کسانی که نسبت به نکات امنیتی آگاهی داشتند نسبت به آن اقدام چندانی نمی‌کردند و درنتیجه مسائل امنیتی مورد توجه لازم واقع نمی‌شد.

• محدودیت زمان و هزینه

بعضی افراد تصور می‌کنند اقدامات امنیتی جهت طراحی، کد نویسی و آزمایش در طول فرآیند تولید نرم‌افزار هزینه گزافی در بر داشته و زمان زیادی را به خود اختصاص می‌دهد.

• خلاقیت تبهکاران

انسان موجود خلاقی است و افراد باانگیزه همیشه برای غلبه بر موانع امنیتی و کشف اشتباهاتی که منجر به نقایص امنیتی شوند راهی پیدا خواهند کرد.

• سطح پایین آگاهی کاربران

کاربران معمولی (قربانیان تخلفات امنیتی) به‌طور طبیعی از تهدیدهای اطراف خود آگاهی ندارند و به همین دلیل در پی راه‌های مناسب جهت تضمین امنیت داده‌ها و سیستم‌های خود نیستند.

• نگاه غیرواقعی قربانیان

برخی کاربران نسبت به نکات امنیتی آگاهی دارند ولی آن‌ها را جدی نمی‌گیرند؛ چون گمان می‌کنند که حمله‌ای علیه آن‌ها صورت نخواهد گرفت.

۱۰-۱۰- سئوالات خودآزمایی

۱. سرمایه‌های دیجیتال که نیاز به تأمین امنیت دارند را نام برده و توضیح دهید.
۲. در یک سازمان متولی بررسی و تصویب سیاست‌های امنیتی چه ساختاری می‌باشد؟
۳. راهبردهای میان مدت را در سیاست‌های امنیتی دیجیتال بنویسید.
۴. نظریه جهانی‌سازی چه نقشی در امنیت دیجیتال دارد آن را توضیح دهید.
۵. نظریه نسبی بودن امنیت اطلاعات دیجیتال را توضیح دهید.
۶. انواع روش‌های مدیریت ریسک را نوشته و توضیح دهید.
۷. ارزیابی مستمر و شناسایی مداوم ریسک‌های مربوط به فاوا چه نقشی می‌تواند در امنیت آن داشته باشد.
۸. مدیریت بحران را تعریف کرده و نقش آن را در امنیت دیجیتال بنویسید.

۱۱

فصل یازدهم: تست نفوذ و ابزارهای امنیتی

آن‌چه در این فصل می‌خوانید:

- **نفوذ و تست نفوذ**
- **حمله به نرم‌افزارهای کاربردی**
- **اسکن شبکه‌ها**
- **اسب‌های‌تراوا و نرم‌افزارهای مخرب نفوذ**
- **ثبت کننده‌ای صفحه کلید**
- **اجزا و آناتومی هک**
- **اطلاع از شیوه‌های نفوذ از داخل و خارج شبکه**
- **روش‌های شناسایی و ممانعت از حملات**
- **نرم‌افزارهای ضد ویروس و استفاده هکرها**
- **تست نرم‌افزار و سخت‌افزار خریداری شده**

۱۱- تست نفوذ و ابزارهای امنیتی

۱۱-۱- نفوذ و تست نفوذ

آشنایی با تست نفوذپذیری

تست نفوذپذیری[۱] که گاهاً به آن pentest نیز می‌گویند، به روشی برای ارزیابی امنیت یک رایانه یا یک شبکه با استفاده از شبیه سازی حملات با هدف خرابکاری یا سرقت اطلاعات اطلاق می‌شود. معمولاً حملات شبیه سازی شده از نظر روش انجام کار تا حد امکان شبیه به روش حمله یک هکر کلاه سیاه[۲] می‌باشد. شروع کار با تجزیه و تحلیل کلیه منابع سیستم برای شناسایی نقاط پرخطر جهت نفوذ به سیستم آغاز می‌شود. نقاط پرخطر یک سیستم بر اثر یکی از موارد ذیل ایجاد می‌شود:

- پیکربندی نامناسب یا اشتباه سخت افزار
- پیکربندی نامناسب یا اشتباه نرم افزار
- اشکال در نحوه کاربری سیستم
- کاستی در پیاده سازی اقدامات پیش‌گیرانه

نتیجه این تجزیه و تحلیل مشخص شدن نقطه یا نقاط پرخطر سیستم می‌باشد که می‌توان از ضعف تکنیکی آن‌ها جهت نفوذ به سیستم استفاده کرد. در اولین اقدام پس از تجزیه و تحلیل، حفره‌های امنیتی بدست آمده به همراه گزارش ارزیابی خطراتی که متوجه سیستم می‌باشد، در اختیار مشتری قرار داده می‌شود. در اکثر موارد طرح پیش‌نهادی جهت کاهش خطرات با استفاده از تجهیزات جدید یا بکارگیری اقدامات فنی پیش‌گیرانه نیز به مشتری ارائه می‌شود.

آزمون نفوذ دو هدف اصلی را دنبال می‌کند:

۱- آگاهی از مخاطرات دیجیتالی ونقاط ضعف امنیتی در بخش فن‌آوری.

---

[۱] Penetration Test

[۲] Black Hat Hacker

(آیا امکان نفوذ به سیستم وجود دارد؟ و درصورت موفقیت آمیز بودن نفوذ، تاچه حد سیستم به خطر می‌افتد؟)

۲- مستحکم سازی و رفع مخاطرات یا به تعبیری ایمن سازی مکانیزم انتقال، ذخیره سازی اطلاعات و داده‌های دیجیتالی سازمان

- پیکربندی نامناسب یا اشتباه سخت افزار
- پیکربندی نامناسب یا اشتباه نرم افزار
- اشکال در نحوه کاربری سیستم
- کاستی در پیاده سازی اقدامات پیش‌گیرانه
- عدم بروز رسانی نرم افزارها و سیستم عامل‌ها
- عدم توجه به اصلاحات الزامی و اعلام شده از سوی تولید کنندگان
- عدم طراحی استاندارد شبکه و ساختار آن
- عدم وجود چک لیست‌های راه اندازی و نگهداری
- عدم تدوین چگونگی عمل‌کرد در وقایع احتمالی
- عدم وجود بازبینی‌های امنیتی
- عدم وجود راه کارهای بحران
- و در مجموع عدم تدوین دارایی‌ها، ریسک‌ها، راه کارها و مانورهای کنترلی

تصور این‌که تست نفوذ پذیری را فقط یک بار باید انجام داد، کاملاً اشتباه بوده و نمی‌توان برای آن محدودیت دفعات تعریف کرد و باید در بازه‌های سالیانه و حین کار این تست انجام شود. منظور از بازه‌های حین کار، زمان‌هایی است که سیستم تغییر می‌کند، مثلاً یکی از پرسنلی که به اطلاعات حساس دسترسی دارد از کار برکنار می‌شود یا یک سرور از سیستم حذف یا به آن اضافه می‌شود، در هر دو حالت انجام تست نفوذپذیری توصیه می‌شود.

۱۱-۲- روش‌های انجام تست نفوذپذیری

تیم فنی مورد نظر برای انجام تست نفوذپذیری را می‌توان به طرق مختلفی هدایت کرد. مهم‌ترین تفاوت در میزان آشنایی تیم از جزئیات پیاده سازی سیستم می‌باشد. بر این اساس می‌توان روش‌های انجام تست را به شرح ذیل دسته بندی کرد :

۱) تست جعبه سیاه[۱]

در این روش هیچ‌گونه اطلاعاتی در خصوص ساختار سیستم در اختیار تیم قرار داده نمی‌شود. تیم در ابتدا باید سیستم را جهت مشخص کردن نقطه‌ای که می‌توان از آن نفوذ کرد، مورد تجزیه و تحلیل قرار دهد.

۲) تست جعبه سفید[۲]

در این روش اطلاعات کاملی در خصوص ساختار سیستم مورد تست در اختیار تیم قرار داده می‌شود. اطلاعاتی همچون : دیاگرام شبکه، Source code، پلان آدرس دهی IP

۳) تست جعبه خاکستری[۳]

اطلاعاتی که در اختیار تیم قرار داده می‌شود کم‌تر از تست جعبه سفید می‌باشد.

بر پایه دانشی که تیم از سیستم مورد تست در اختیار دارد می‌توان دسته بندی‌های مشابه انجام داد:

۱) افشاسازی کامل[۴] (جعبه سفید)

۲) افشاسازی جزئی[۵] (جعبه خاکستری)

۳) تست کورکورانه[۶] (جعبه سیاه)

خصوصیاتی منحصر به فرد مربوط به هر تست را می‌توان به این شرح بیان کرد :

تست جعبه سیاه

• حملاتی را شبیه سازی می‌کند که از جانب یک شخص خارجی و نا آشنا با سیستم انجام می‌شود.

• یک تست کاملا دستی(در مقابل اتوماتیک) و گران قیمت نیاز دارد که تیم تست کننده حداکثر تلاش خود را در جهت کاهش خطراتی که ممکن است حین تست برای سیستم اتفاق بیافتد به کار بندد.

تست جعبه سفید

---

[۱] Black Box Test
[۲] White Box Test
[۳] Gray Box Test
[۴] Full disclosure
[۵] Partial disclosure
[۶] blin

• حملاتی را شبیه سازی می‌کند که توسط شخصی از داخل سیستم یا شخصی که به اطلاعات حساس دسترسی داشته و از کار برکنار شده انجام می‌شود

• فرد مهاجم به اطلاعاتی همچون Source code، پلان شبکه و به برخی از کلمه‌های عبور دسترسی دارد.

یک تست کاملاً اتوماتیک و ارزان قیمت

با توجه به اصول کلی فوق نوبت طرح سئوالاتی رسیده که مشخص کننده نیاز یا عدم نیاز سازمان شما به تست نفوذپذیری می‌باشد. با در نظر گرفتن شرایط سازمان خود آیا می‌توانید جواب مشخصی برای سئوالات زیر ارائه دهید؟

• آیا می‌توان به داخل سازمان شما نفوذ کرد؟

• آیا می‌دانید در صورت رخنه به سازمان شما، تا چه میزان متضرر می‌شوید؟

• آیا برقراری امنیت تنها با خرید دیواره آتش یا دستگاه‌های مشابه برقرار می‌شود؟

• آیا انجام تست نفوذپذیری برای سازمان شما مورد نیاز است؟

۱۱-۳- اسکن شبکه‌ها

۱۱-۳-۱- اسکنرهای پورت

اسکن یک پورت فرآیندی است که مهاجمان با استفاده از آن قادر به تشخیص وضعیت یک پورت بر روی یک سیستم یا شبکه می‌باشند.

مهاجمان با استفاده از ابزارهای متفاوت، اقدام به ارسال داده به پورت‌های TCP و UDP نموده و با توجه به پاسخ دریافتی قادر به تشخیص این موضوع خواهند بود که کدام پورت‌ها در حال استفاده بوده و از کدام پورت‌ها استفاده نمی‌گردد و اصطلاحاً آنان باز می‌باشند.

مهاجمان در ادامه و بر اساس اطلاعات دریافتی، بر روی پورت‌های باز متمرکز شده و حملات خود را بر اساس آنان سازمان‌دهی می‌نمایند. عمل‌کرد مهاجمان در این رابطه مشابه سارقانی است که به منظور نیل به اهداف مخرب خود (سرقت)، درابتدا وضعیت درب‌ها و پنجره‌های منازل را بررسی نموده تا پس از آگاهی از وضعیت آنان (باز بودن و یا قفل بودن)، سرقت خود را برنامه ریزی نمایند. (parsiblog. com)

۱۱-۳-۲- اسکنرهای آسیب‌پذیری

وظیفه این اسکنرها پیدا کردن آسیب‌پذیری‌های شناخته شده بر روی رایانه‌ها و شبکه‌های مختلف می‌باشد. با پیدا کردن آسیب‌پذیری‌ها افراد غیر مجاز قادر خواهند بود از طریق آن‌ها به

درون شبکه‌ها رخنه نموده و اطلاعات مورد نیاز خود را ازآن خارج نمایند. آسیب‌پذیری‌ها به منزله دریچه‌های پنهانی می‌باشند که با کم‌ترین تقلایی می‌توان آن‌ها باز کرده و از طریق آن به درون شبکه‌ها راه پیدا نمود.

۱۱-۳-۳- اسکنرهای اطلاعات

نفوذگران قبل از نفوذ علاقمند می‌باشند تا اطلاعات موجود در رایانه‌ها و شبکه‌ها را شناسایی نموده و بر مبنای نیاز خود برای دست‌یابی به آن‌ها سرمایه گذاری نمایند. یکی از راه‌های متوجه شدن نوع اطلاعات و شناسایی نوع اطلاعات موجود در شبکه‌ها و رایانه‌ها استفاده از این نوع اسکنرها می‌باشد. در جست‌جوی دستی و بدون استفاده از اسکنر ممکن است پیدا نمودن اطلاعات خاصی ساعت‌ها زمان ببرد لیکن با استفاده از این نوع اسکنرها می‌توان در چند دقیقه اطلاعات را شناسایی و محل آن‌ها و نوع حمله به آن‌ها را شناسایی نمود.

۱۱-۳-۴- اسکنرهای شبکه

با توجه به این که شبکه‌های مختلفی ممکن است به یک‌دیگر متصل شده و هر کدام از آن‌ها دارای تعداد زیادی رایانه بهره‌بردار باشند و ممکن است گاهی تا هزاران دستگاه وجود داشته باشد و برای مهاجمین پیدا کردن اطلاعات اولیه مربوط به شبکه‌ها و رایانه‌های متصل به آن‌ها بسیار وقت گیر می‌باشد.

در صورت دسترسی فیزیکی به شبکه، عناصر غیر مجاز قادر خواهند بود تا با استفاده از این نوع اسکنرها، حداکثر طی چند دقیقه اطلاعات ذی‌قیمتی را از شبکه و رایانه‌های متصل پیداکرده و از طریق این اطلاعات به شبکه حمله نمایند.

۱۱-۳-۵- اسکنرهای نرم‌افزارهای مخرب

برخی از عناصر غیر مجاز به دنبال این هستند تا از نرم‌افزارهای مخرب نصب شده توسط دیگران بهره‌برداری سو مجدد نمایند و به نوعی کار خود را راحت‌تر انجام داده و از توان مدیریتی این نرم‌افزارها بهره‌برداری کنند. این نوع از اسکنرها به سارقان اطلاعات کمک می‌نماید تا با کم‌ترین زحمت و با استفاده از ابزار دزدان دیگر به اطلاعات دسترسی پیدا نمایند.

۱۱-۴- نفوذ در سیستم‌ها به‌وسیله سازندگان

بسیاری از تولید کنندگان اصلی سیستم‌ها امروزه توسط سرسپردگان نظان سلطه یا طراحی و یا از طرف آنان پشتیبانی می‌گردند و برخی از کشورهای سلطه گر به صورت آشکار به این مطلب اشاره می‌نمایند:

در کشور آمریکا مقررات گمرکی صرفا اجازه صور نرم افزار و سخت افزار را به شرکت‌هایی می‌دهد که قبلاً بر روی نرم افزار و یا سخت افزار خود bug امنیتی و مدیریتی قرار داده و آن را با تایید اف بی آی برسانند و بدون این تاییدیه امکان صدور آن‌ها به دیگر کشورها میسر نمی‌باشد.

نرم افزار postgre-sql در سایت خود رسماً اشاره به این می‌نماید که این نرم افزار توسط پنتاگون پشتیبانی می‌گردد

چهار نفر از مدیران اصلی شرکت php در شرح رزومه خود اشاره به این داشته اند که یا متولد رژیم اشغالگر قدس می‌باشند و یا این‌که در آن‌جا فارغ التحصیل شده‌اند:

Andi gutmans مدیر هماهنگ کننده فارغ التحصیل از موسسه تکنولوژی نکنیون رژیم اشغالگر قدس

Zeev suraski مدیر عالی فن آوری فارغ التحصیل از موسسه تکنولوژی نکنیون رژیم اشغالگر قدس

Eldad maniv مدیر ارشد بازاریابی و فروش فارغ التحصیل از دانشکده مدیریت تل آویو

Moshe mor عضو هیئت مدیره فارغ التحصیل از دانشگاه تل آویو در MBA

مسلم است که این گونه افراد به دنبال اعمال نظریات سلطه گرانه کشورهای مدنظر خود خواهند بود

۱۱-۵- ابزارهای امنیتی

امروزه بسیاری از ابزار نرم افزاری و سخت افزاری توسط شرکت‌ها و افراد مختلف برای دسترسی غیر مجاز به اطلاعات تولید شده و با قیمت بسیار اندک و یا به صورت مجانی در اختیار دیگران قرار گرفته است و افراد قادر خواهند بود با داشتن کم‌ترین اطلاعات رایانه‌ای از طریق این ابزار به صورت غیر مجاز به اطلاعات دیگران دسترسی داشته باشند.

اموز دیگر نمی‌توان عناصر غیر مجاز را صرفاً سازمان‌های جاسوسی دشمن و دشمنان نقاب دار فرض نمود بلکه می‌بایست به آن عناصر ناآگاهی را که این ابزار را که عملاً به صورت غیر مستقیم در اختیار نظام سلطه می‌باشند را نیز باید به این افراد اضافه نمود.

در ذیل چند نمونه کوچک از این ابزار بدون این‌که تاییدی بر استفاده از آن باشد و صرفاً به منظور آشنایی متخصصین با این ابزار قید می‌گردند.

Accounting information system (AIS)

با توجه به این که برای دسترسی کاربران به اطلاعات در رایانه‌ها و شبکه‌های رایانه‌ای برای هر کاربر حساب مشخصی تعریف می‌شود. کاربران با داشتن این حساب و با گذاشتن رمز بر روی آن می‌توانند به اطلاعات مشخص شده دسترسی داشته باشند. با استفاده از این نرم‌افزار افراد غیرمجاز قادر خواهند بود کلیه کاربران را که در سیستم تعریف شده است را شناسایی نموده و در صورت دسترسی به شبکه از اطلاعات آن بهره‌برداری سوء نمایند.

Bios۳۲۰

در رایانه برای ایجاد امنیت در استفاده از آن در قسمت‌های مختلف رمز گذاشته می‌شود. یکی از رمزها در قسمت سخت‌افزاری اولیه رایانه قرار داده می‌شوند دارندگان این رمز قادر خواهند بود به سیستم عامل دسترسی داشته باشند و از آن برای مدیریت بر رایانه و دسترسی به اطلاعات استفاده نمایند. در صورت نداشتن این رمز امکان استفاده از رایانه میسر نخواهد بود. بسیاری از کاربران به این مطلب اعتماد نموده و با گذاشتن رمز اولیه برروی رایانه آن را در اختیار افراد غیرمجاز قرار می‌دهند و اعتقاد بر این دارند با وجود این رمز دیگران قادر به دسترسی به اطلاعات آن‌ها نخواهند بود. افراد غیرمجاز با استفاده از این نرم‌افزار قادر خواهند بود رمز اولیه رایانه را حذف یا آن را با رمزمدنظر جای‌گزین نمایند.

Cain

برروی رایانه رمزهای مختلفی گذاشته می‌شود و با توجه به نوع سیستم عامل این رمز دارای کلیدهای رمز مختلفی می‌باشند. کاربران به این مسئله اعتماد نموده و اطلاعات خود را بر روی این رایانه‌ها قرار داده و رایانه‌ها را برای تعمیر یا تنظیم در اختیار دیگران قرار می‌دهند. این نرم‌افزار نشان می‌دهد که چگونه می‌توان در دقایقی به رمزهای رایانه با استفاده از فایل‌های مربوطه دسترسی پیدا نمود.

Exebundlers

یکی از راه‌های انتقال نرم‌افزارهای مخرب به درون رایانه‌ها اتصال آن به نرم‌افزارهای مجاز می‌باشد. نرم‌افزار نویس قادر خواهد بود تا از طریق نوشتن کدهای برنامه این کار را انجام دهد. نفوذگران آماتور برای این کار از نرم‌افزارهای خاصی استفاده می‌نمایند. این نرم‌افزارها برای اتصال پنهان دو یا چند نرم‌افزار اجرایی به یک‌دیگر و ایجاد یک نرم‌افزار اجرایی خاص استفاده می‌شود. این نرم‌افزار قادر خواهد بود تا نرم‌افزارهای مخرب را به نرم‌افزارهایی اجرایی دیگر متصل نمود و آن را در درون نرم‌افزارهایی مجاز پنهان نماید.

۱۱-۶-اطلاعات قابل دسترسی در صورت دسترسی عناصر غیر مجاز

در صورتی که عناصر غیر مجاز به رایانه‌ای که به اینترنت متصل است دسترسی داشته باشند و یا این‌که در زمان تعمیر و یا انجام تنظیمات رایانه به صورت فیزیکی به آن دسترسی پیدا نمایند می‌توانند به اطلاعات ذی‌قیمتی دسترسی یابند که در ذیل به برخی از آن‌ها اشاره می‌گردد:

۱- شماره ip
۲- نوی سیستم عامل نصب شده
۳- فایل‌های موجود بر روی رایانه
۴- فایل‌های حذف شده از رایانه که در سطل بازیافت قرار دارند
۵- فایل‌های حذف شده از رایانه از زمان فورمت شدن سیستم تاکنون
۶- فایل‌ها و دایرکتوری‌ها و فولدرها و درایوهای پنهان شده
۷- ارتباطات انجام شده بات شبکه‌های مختلف
۸- ارتباطات انجام شده از طریق مودم
۹- شماره تلفن‌های گرفته شده از طریق مودم
۱۰- نام کاربری‌های استفاده شده بر روی مودم
۱۱- رمزهای به کار گرفته شده از طریق مودم
۱۲- رمزهای به کار رفته در نرم افزارهای مختلف
۱۳- نرم افزارهای نصب شده بر روی رایانه
۱۴- نرم افزارهای نصب شده بر روی setup رایانه
۱۵- سخت افزار به کار گرفته شده در سیستم
۱۶- آدرس سایت‌های مشاهده شده از طریق سیستم
۱۷- تاریخ‌های که در آن زمان سایت‌ها مشاهده شده‌اند
۱۸- فایل‌های دانلود شده از طریق اینترنت
۱۹- نام کاربران استفاده کننده از سیستم
۲۰- احتمال بدون رمز بودم کاربر مدیر سیستم
۲۱- احتمال بدون رمز بودن و فعال بودن کاربر میهمان
۲۲- رمزهای ذخیره شده بر روی رایانه

۲۳- رمزها و نام کاربران ایمیل استفاده شده به وسیله سیستم
۲۴- سیستم‌های رمز مورد استفاده در رایانه
۲۵- امکان ایجاد کاربران معادل مدیر سیستم
۲۶- امکان تغییر رمز کاربران سیستم
۲۷- امکان به اشتراک گذاشتن کلیه اطلاعات دستگاه
۲۸- امکان اجرا کردن تروجان بر روی دستگاه
۲۹- امکان اجرا کردن یک کی‌لاگر بر روی دستگاه
۳۰- امکان پیدا کردن رمز استفاده شده در نرم افزارهای کاربردی در سیستم
۳۱- امکان پیدا کردن رمزهای استفاده شده در اینترنت اکسپلورر
۳۲- امکان قرار دادن یک برنامه به صورتی که در زمانی که می‌خواهد اجرا شود
۳۳- امکان فهمیدن این‌که چه برنامه‌های در حال استفاده شدن می‌باشند
۳۴- امکان فعال کردن و یا غیر فعال کردن یک برنامه در مرورگر
۳۵- امکان مشخص کردن درایورهای و محل نصب آن‌ها در رایانه
۳۶- دسترسیی به رمزهای ارتباطی با sql-server
۳۷- امکان تغییر ساعت و تاریخ یک یا چند فایل مد نظر
۳۸- امکان پیدا کردن کلیه فولدرهای ایجاد شده بر روی سیستم
۳۹- پیدا کردن پسوندهای مورد نظر بر روی رایانه
۴۰- پیدا کردن رمزهای استفاده شده برای دسترسی از راه دور به شبکه

این امکانات صرفا بخشی از امکاناتی است که یک فرد غیر مجاز می‌تواند در صورت دسترسی به یک رایانه از راه دور به آن‌ها دسترسی داشته باشد و بسیاری دیگر از اطلاعات وجود دارد که سازندگان سخت افزارها و تولید کنندگان نرم افزار غیر مجاز که عناصر نظام سلطه از آن جمله می‌باشند می‌توانند در صورت رعایت نکردن نکات کلیدی پدافندی و امنیت بومی رایانه می‌توانند به آن‌ها دسترسی داشته باشند و تمام تلاش و سعی عناصر غیر مجاز در این است که با سواستفاده از اهمال کاری کاربران ناآگاه به بیش‌ترین اطلاعات دسترسی پیدا نمایند.

البته مشخص است که در صورت داشتن چنین دسترسی تلاش بر این دارند تا بدون حساس نمودن کاربران این دسترسی‌ها را ادامه داده و هر چه بیش‌تر از اطلاعات بهره برداری سو نمایند و می‌دانند که در صورت آشکار نمودن این دسترسی دیگر امکان ادامه آن برایشان میسر نخواه بود. برخی از کاربران و متخصصین کم آموزش دیده با عنوان کردن این‌که اگر این

دسترسی‌ها وجود داشته باشد پس چطور ما تاکنون متوجه این مطلب نشده‌ایم کمک به استمرار دسترسی عناصر غیر مجاز می‌نمایند.

۱۱-۷- سئوالات خودآزمایی

۱. انواع روش‌های حمله به SETUP رایانه را نوشته و توضیح دهید.
۲. ارتباط بین سیستم عامل ویندوز و امنیت را توضیح دهید.
۳. اجزاء آناتومی هکرها نوشته و توضیح دهید.
۴. تست نرم‌افزار و سخت‌افزار خریداری شده، چه نقشی می‌تواند در امنیت رایانه داشته باشد.
۵. در زمان ارسال رایانه برای تعمیر و تنظیم چه مشکلات امنیتی ممکن است ایجاد شود؟
۶. سیستم‌های IDS وIPS چه نقشی در امنیتی رایانه دارند؟
۷. نفوذ در سیستم‌ها به وسیله سازندگان به چه روش‌هایی انجام می‌شود؟
۸. نقش اسکنرها در امنیت رایانه و شبکه را توضیح دهید.

فهرست منابع

کتب:

۱. اظهری علی – رازهای پنهان هیپنوتیزم – انتشارات میر – ۱۳۷۷
۲. اللهیاری فرد، م، ارزیابی گسترش بانک‌داری الکترونیک در کشورهای اسلامی ، تازه‌های اقتصاد
۳. باطنی محمدرضا – ساخت و کار ذهن – انتشارات واژه – ۱۳۶۹
۴. بانک مرکزی و بانک‌داری الکترونیک ، بانک‌داری الکترونیک، ۱۳۸۷، ۳، ۲۲.
۵. پزشکی، ی، دباغ رضایی، س، ۱۳۸۴ نقش فن‌آوری اطلاعات و ارتباطات در رشد اقتصادی ، تدبیر، ۱۳۸۴، ۱۶۳.
۶. پورابراهیمی و بنابی - آشنایی با اصول امنیت محیطی در حوزه فن‌آوری اطلاعات و ارتباطات – پدافند غیرعامل کشور –۱۳۸۹
۷. جمالیان سید رضا – قدرت خود هیپنوتیزم – انتشارات اسپرک – ۱۳۶۸
۸. جنگ و دفاع سایبر
۹. جهانگیری، ف، ۱۳۸۶ بررسی عوامل موثر در آمادگی الکترونیکی برای بانک‌داری الکترونیکی در بانک صادرات پایان نامه کارشناسی ارشد، دانشگاه‌تربیت مدرس۱۳۸۶
۱۰. چالش‌های تحول الکترونیکی- پرتو ملت، ۲۰و۲۱، ۱۳۸۶، ۵۲-۴۹.
۱۱. خدادادی مهدی – مصاحبه تشخیص – انتشارات مدبر – ۱۳۸۵
۱۲. دهستانی مهدی – آسیب شناسی روانی – انتشارات طیف نگار – ۱۳۸۶
۱۳. رشیدی، د، زادگان باوی، ه، بانک‌داری متمرکز؛پیش نیازی برای تحول در ارائه خدمات بانکی تازه‌های اقتصاد، ۳۱-۲۵
۱۴. سید محمدی یحیی – آسیب شناس روانی – انتشارات نشر روان – ۱۳۸۶
۱۵. سید محمدی یحیی – روانشناس عمومی – انتشارات نشر ارسباران – ۱۳۸۶
۱۶. طاووس شعبان – روانشناس هیپنوتیزم – انتشارات کابوک – ۱۳۵۶
۱۷. عزبدفتری بهروز – ذهن و جامعه – انتشارات فاطمی – ۱۳۷۲

۱۸. عزیزی سرخنی، م. ج، اله قلی زاده آذری، م، کردلوئی، ح. ر، بررسی زیر ساخت‌های موجود بانک تجارت برای استقرار بانک‌داری الکترونیکی، (پژوهشگر)مدیریت، ۱۳۸۷، ۱۰، ۱۱.
۱۹. فرس پل – روانشناسی تجربی – سازمان انتشارات آموزش انقلاب اسلامی - ۱۳۶۹
۲۰. فکور ثقیه، ا. م- تاثیر فن‌آوری اطلاعات بر صنعت بانک‌داری مدیریت، ۱۸، ۱۳۸۵، ۱۰۷-۱۰۸.
۲۱. کریستااسون – حافظه مجرمان از جرایم خشونت بار – انتشارات نشر آگاه – ۱۳۸۸
۲۲. کلمان ژاگوپل – روش‌های علمی مانیتیسم، هیپنوتیسم، تلقین – انتشارات ققنوس – ۱۳۸۳
۲۳. گنجی حمزه – مصلحی زیبنده – ایزد دوست یوسف – روان شناسی – چاپ و نشر ایران – ۱۳۷۲
۲۴. مجوز عبدالله – دنیای خود هیپنوتیزم و بهبودی با تلقین – موسسه فرهنگی انتشاراتی حیان – ۱۳۷۶
۲۵. محمدزاده علی اکبر – ولیزاده صمد – روانشناس هیپنوتیزم – انتشارات تلاش
۲۶. مدیریت ریسک - سایت اینترنتی هیراد انجمن ایرانیان
۲۷. مک فی نیل –تری راجر – هنر مخفی مصاحبه با افراد – انتشارات نشر آگاه – ۱۳۸۸
۲۸. منجمی علیرضا – روش‌های تقویت حافظه – نشر آزاد مهر – ۱۳۸۸
۲۹. هیپنوتیزم‌هارتلند – جمالیان سید رضا – انتشارات جمال الحق – ۱۳۷۵

ترجمه:

۱. ترجمه بخشی از کتاب : security risk - biringer rodolph .by betty E assessment and management
۲. کتاب مدیریت ریسک – نوشته : سی آرتور ویلیامز،دیچارد دام. هینز – ترجمه : دکتر داور ونوس و گودرزی
۳. نگاهی به بانک‌داری خرده فروشی درآینده ترجمه جندقی، م، ماهنامه آموزشی، خبری بانک ملی ایران، ۱۳۸۶، ۲۱-۱۹. ۱۳۵.

فصلنامه و ماهنامه:

۱. ایلداری، س، "تاثیر تجارت الکترونیک بر بانک‌داری خرد، ماهنامه بانک صادرات، ۳۰.

۲. دو مانع پیش روی بانک‌داری الکترونیک"ماهنامه بانک‌داری الکترونیک" ۱۳۸۷، ۵، ۱۰.
۳. فخری,مجید, "سنجش از راه دور و کاربردهای نظامی اطلاعات ماهواره ای, فصلنامه خبری آموزشییء فرماندهی ستاد,تهران ,سال دوم,شماره ۵ , ۱۳۷۸
۴. فصلنامه میثاق بسیج متخصصین، سال سوم، شماره ۱۱، پاییز ۸۹
۵. عابدینی , مهدی, "ماهواره‌ها و تحولات نظامی" نشریه علمی و خبری ماهواره‌ها , تهران : مرکز ماهواره‌ها , سال اول , شماره اول , ۱۳۷۹
۶. کیمیایی، پ، ۱۳۸۱"بانکداری سنتی و بانک‌داری الکترونیکی تقابلی اجتناب ناپذیر" فصلنامه بانک، شماره۲۲.

مقالات:

۱. مقاله مدیریت ریسک - نوشته‌ی دکتر محمد علی بابایی و حمید رضا وزیر زنجانی
۲. مقاله مدیریت ریسک استراتژیک – نویسنده : آلن ورینگ و حسن مهدی زاد
۳. مقاله نقش فن‌آوری اطلاعات در مدیریت ریسک، نشریه جهان اقتصاد

سایت:

۱. سایت اینترنتی هیراد انجمن ایرانیان- مدیریت ریسک
۲. سایت فن‌آوری اطلاعات برای مدیران

منابع لاتین:

۱. Agence France Press ،Mar ،۲۸ ،۲۰۰۱
۲. Air Force ،Operation Iraqi Freedom ،Information Operation Lessons Learned:
۳. Airpower Journal ،July ،۱۹۹۶
۴. Appraisal: The Changing Role of Information in Warfare ، RAND ،۱۹۹۹ ،
۵. CANADIAN FORCES COLLEGE ،ADVANCED MILITARY STUDIES

٦. Carrington ،M ،١٩٩٧ ،" The banking Revolution : how Technology in creating winners and losers " ،Great Britain ، pitman publishing company.
٧. Center ،Beijin Special Lecture ،Mar ،١٩٩٧ ،
٨. Charles F. Hawkins ،China Defense Science & Technology Information
٩. Col. Andrew Borden ،USAF ،What is Information Warfare? The Information
١٠. Col. Timothy Thomas ،Russian Views on Information-Based Warfare ،
١١. Conflict in the Information Age ،RAND ،١٩٩٧ ،
١٢. Costas Courcoubetis and Richard Weber ،Pricing Communication Networks ،John Wiley and Sons Publishing ، ٢٠٠٣.
١٣. COURSE ٢ ،NOV ،١٩٩٩ ،
١٤. David Alexander ،http://www. davidalexanderbooks. Com /www /informat. htm
١٥. David Fulghum ،Sneak Attack ،Aviation Week & Space Technology ،June ٢٨ ،
١٦. David Ruppe ،Directed-Energy Weapons: Possible U. S. Use Against Iraq
١٧. DoD dictionary of Military and Associated Terms ،
١٨. Dorothy Denning ،Information Warfare and Security ،Addison-Wesley ،١٩٩٩
١٩. Durhin ،M. ،Howcroft ،B. ،٢٠٠٣ ،" Relationship marketing in the banking sector " ،marketing Intelligence and planning ،vol ٢٧.
٢٠. Elaine Grossman ،Officials: Space ،Info Targets largely Cobbled on-the-fly for
٢١. Feb ٢ ،٢٠٠٣ ،http://www. globalsecrutiy. org/org/news

۲۲. Frenchelon ،The large ears made in France ،
۲۳. Frist Look ،http://www. cadre. maxwell. af. mil/ warfarestudies /iwac /downloads ،
۲۴. Giampiero Giacomello ،Measuring digital wars: Learning from the experience
۲۵. IAnewsletter ،Vol. ۳ ،No. ۴
۲۶. InfoWarCon ،۲۰۰۰ ،Sep ۱۲ ،۲۰۰۰ ،Washington D. C.
۲۷. Iraq ،Inside Pentagon ،May ۲۹ ،۲۰۰۳
۲۸. ITU-toolkit page\ICT Regulation Toolkit. htm
۲۹. Jack Moteff ،Critical Infrastructures: Background & Early Implementation of
۳۰. James Mulvenon ،The PLA and Information Warfare
۳۱. John Arquilla and David Ronfeldt (Ed) In Athena's Camp: Preparing for
۳۲. Joint Information Operations Planning Handbook ،
۳۳. Jr۰۲-۲۰۰۹ tracking ghostnet
۳۴. Kajaluoto. h ،Kaoivumaki. t ،and Salo. j ،۲۰۰۳ ،"Individual difference in privat banking:empirical evidence from finlandhngs of the ۳ ،th hawii international conference on system sciences(H۱CSS) ،big island ،Hawaii ،p۱۹۶.
۳۵. Lester W. Grau and Timothy L. Thomas ،A Russian View of Future War: m
۳۶. LU. J. ،L iu ،c. ،Yao J. ،۲۰۰۳ ،" Technoloyy Acceptance Model for wireless internet " ،Electronic Networking Applications and policy ،vol ۱۳ ،No۳.
۳۷. Megan Burns ،Defining Information Warfare: Easier Said than Done ،۱۹۹۹ ،
۳۸. Mesic ،Strategic Information Warfare Rising ،RAND ،۱۹۹۸ ،
۳۹. Military Strategic Research Center ،Beijing ،May ،۱۹۹۶

۴۰. Network Centric Warfare ،Department of Defense Report to Congress ،
۴۱. News Release ،US Space Command ،Sep ۲۹ ،۲۰۰۰ ،
۴۲. of peace research and arms control ،The Information Warfare Site ،
۴۳. Other countries developing cyber attack capability ،CIA says ، Feb ،۲۰۰۰ ،PDD-۶۳
۴۴. Peter Cartwright ،Interconnect Costing ،BWCS ltd ،United Kingdom ،۲۰۰۱.
۴۵. Proceeding of the ۲۰۰۱ IEEE Workshop on Information Assurance and
۴۶. Raymond C. Parks and David Duggan ،Principles of cyber-warefare ،
۴۷. Roger C. Molander ،Peter W. Wilson ،David A. Mussington ، Richard F.
۴۸. Ronald Fogleman and Sheila Widnall ،Cornerstones of Information Warfare ،
۴۹. Security ،Untied States Military Academy ،West Point ،NY۵ ـ۶ June ،۲۰۰۱
۵۰. Smart Card Security and Applications، Mike Hendry، ۲nd Edition، ©ARTECH House INC۰۲۸. Pdf. ۱۳۵.۱۹۹۶. ۲۰۰۴
۵۱. The White House ،A National Security Strategy for a New Century ،Dec ،۱۹۹۹
۵۲. Theory and Direction ،The Journal of Slavic Military Studies ، Issue ۹. ۳ ،Sep
۵۳. Threaten International Regims ،Global Security Newswire ، Agust ۱۶ ،۲۰۰۲ ،
۵۴. U. S Military concerned about China's cyberwarfare capabilities: General ،

۵۵. US Strategic Command Fact File ،http://www. stratcom. af. Mil /factsheet. shtml
۵۶. USAF Doctrine of Information Operations ،
۵۷. Warfare Site ،http://www. iwar. org. uk /iwar /resources /airchronicles /borden. htm
۵۸. WIK-Consult ،Analytical Cost Model Broadband Network ، ۲۰۰۵
۵۹. Will Dunham ،U. S may debut secret microwave weapons versus Iraq ،Reuters ،
۶۰. Wordnet Princeton University ،http:///wordnet. princeton. edu
۶۱. Yiu. c. s ،Grant. k ،Adgar. d ،۲۰۰۷ ،"Factors affecting the adoption of Internet Banking in Hong kong-implication for the banking sector"International Journal of Informetion management ،۲۷۳۳ ،۶-۳
۶۲. Zalmay Khalizad ،John P. White ،Andrew W. Marchal (Ed) ، Strategic

اینترنت:

۱. http:// www. microsoft. com
۲. http://www. aerocenter. ir/forum/showthread. php?t=٦٨٨٠&page=١
۳. http://www. af. mil/lib/corner. html
٤. http://www. ahmady aghma. blogfa. com
٥. http://www. articles. com
٦. http://www. bashg. net
۷. http://www. beheshtnet. . blogfa. com
۸. http://www. berkley. com
۹. http://www .berkley .Com
۱۰. http://www. cs. cmu. edu/~burnsm/InfoWarfare. html
۱۱. http://www. daneshnameh. roshd. ir
۱۲. http://www. dod. mil/nii/NCW/
۱۳. http://www. dtic. mil/doctrine/jel/doddict/data/i/index. html
۱٤. http://www. duzli-oghlan. blogfa. com
۱٥. http://www. ege. eslsca. fr
۱٦. http://www. fa. wikipedia. org
۱۷. http://www. farya. com

۱۸. http://www. firooz. ir
۱۹. http://www. forum. silvapc. com/index. php?topic=۲٦۷٦. ۰% ۳bwap۲
۲۰. http://www. forun. manuatoo. com
۲۱. http://www. georgetown. edu/sfs/programs/stia/students/vol. ۰۳ / Johnson _IW. ht
۲۲. http://www. giganews. ir
۲۳. http://www. globalsecrutiy. org/org/news
۲٤. http://www. hamedbanaei. com
۲٥. http://www. hamshahri. Org
۲٦. http://www. herolibrary. org/iwa٤web. htm
۲۷. http://www. imi. ir/tadbir/tadbir-۱۳٤/article-۱۳٤/٤. asp
۲۸. http://www. infoguerre. com
۲۹. http://www. insidedefense. Com / secure / data _ extra / pdf۳ / dplus ۲۰۰٤ _۲٦٥. pdf
۳۰. http://www. iricap. Com
۳۱. http://www. it .behdasht .gov .ir
۳۲. http://www. it .behdasht .gov .ir/uploads/۱۰۱_۱۱۹۱_security .doc
۳۳. http://www. itirn. com
۳٤. http://www. iwar. org. uk/infocon
۳٥. http://www. iwar. org. uk/iwar/resources/jiopc/io-handbook. pdf
۳٦. http://www. iwar. org. uk/iwar/resources/usaf/maxwell/students/۲۰۰۱/۰۱-
۳۷. http://www. networkworld. com/news/۲۰۰۰/۰۲۲٤cia. html
۳۸. http://www. noorportal. net
۳۹. http://www. p۳۰lords. com/forum/archive/index. php/t-۹۲٦۳. html
٤۰. http://www. parsiblog. Com
٤۱. http://www. peace. ca/canadianinformationoperations. htm
٤۲. http://www. ponemonen. com
٤۳. http://www. rand. org/publications/MR/MR۹٦٤/MR۹٦٤. pdf
٤٤. http://www. rand. org/pubs/monograph_reports/MR۱۰۱٦/
٤٥. http://www. rand. org/pubs/monograph_reports/MR۸۸۰/index. html
٤٦. http://www. sans. org/newlook/resources/IDFAQ /solar_sunrise. htm
٤۷. http://www. shabakeh-mag. com/articles/Show. aspx?n=۱۰۰۳٤۱٤
۴۸. http://www.shabakeh-mag. com/articles/Show. aspx?n = ۱۰۰۳۴۱۴& p = ۳
۴۹. http://www. social. iran-emrooz. net
٥۰. http://www. spacecom. af. mil/usspace/re۱۱٥-۰۰. htm
٥۱. http://www. srco. ir/articles/docview. asp۲id=۱۸۲

۵۲. http://www. tebyan. net/science _ technology / computermagazine /interview_report/۲۰۰٤/۱۳/۵۸۰۲. html
۵۳. http://www. tebyan-ardebill. ir
۵٤. http://www. thefreedictionary. com/IW
۵۵. http://www .vaya .ir/index .php?option = com _ content&view = article&id = ۳۷۷&Itemid=۷۱
۵٦. http://www .vaya .ir/index .php ? option = com _ content & view = article&id =٤٤۳&Itemid=۲۳۰
۵۷. http://www. zdnet. fr/actu/tech/secu/a۰۰۱٤۷٦۸/html
۵۸. http://www.dehckade-danesh. mihanblog. com/post/۱۰
۵۹. http://www.dehckade-danesh. mihanblog. com/post/۹
٦۰. http://www.emmaf۲. isuisse. com/emmaf۲/iw/what. htm
٦۱. http://www.en. wikipedia. org/wiki/Command_and_control_warfare
٦۲. http://www.farsnews. ir
٦۳. http://www.padafand-gh-amel .persianblog .Ir

واژه نامه

مدیریتی:	administrative
نرم افزار کاربردی:	application
ارزیابی:	assessment
قابلیت دستیابی:	availability
رخنه درب پشتی:	backdoor
محرمانگی:	confidentiality
شکستن غیر مجاز رمز:	crack
بانک اطلاعاتی:	database
ردپا گذاری:	fingerprint
دیواره آتش:	firewall
صحت و یک‌پارچگی:	integrity
رمز عبور:	password
نفوذ:	penetration
سیاست:	policy
امنیت:	security
تهدیدات:	threats
تروجان:	trojan
مجازی:	virtual
آسیب پذیری:	vulnerability
ارزیابی آسیب پذیری:	vulnerabilityassessment

اندیکس

ت

ج

ح

خ

د

ر

س

ش

ف

ک

م

و

ه