

بسمه تعالی

دوره تکنولوژی اطلاعات و ارتباطات ICT

شرکت برق منطقه ای

کد دوره : ۸۶۳۴

برگزار کننده دوره: دانشگاه صنعتی شیراز – مرکز آموزش های آزاد

مدرس : مهندس مریم کیخا

تیر ۱۴۰۰

فناوری اطلاعات و ارتباطات





به نظر شما جامعه سنتی و جامعه دیجیتالی چه تفاوت‌هایی دارند؟



کاربرد فناوری اطلاعات در رشته تحصیلی شما چیست؟



تفاوت کسب‌وکار الکترونیکی با تجارت الکترونیکی چیست؟



کاربرد اطلاعات موجود در شبکه‌های اجتماعی چگونه است؟



معمای دگردیسی دیجیتالی را می‌دانید؟

فناوری اطلاعات و ارتباطات

با ظهور هر پدیده جدید، مفاهیم، محصولات و فرایندها تغییر می کنند یا در شکل جدیدی خلق می شوند. برای مثال می توان به اختراع و همه گیر شدن هواپیما اشاره کرد. با ورود هواپیما به عرصه حمل و نقل، محصولات و خدمات مرتبط با آن وجود آمده مانند فرودگاه ها، بلیت فروشی ها و ... ، ضمن آنکه نحوه انجام سفرهای طولانی نیز تغییر کرده است.



محصولات و خدمات مرتبط با ظهور فناوری هواپیما

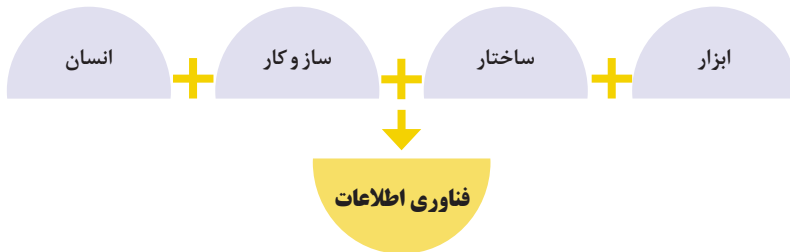
در دنیای امروز تغییر و تحول در خصوص فناوری اطلاعات بسیار محسوس است، تغییرات بسیار سریع ایجاد شده در این حوزه، کاربردها، مفاهیم و روش های نوینی را خلق کرده است. با فراگیر شدن فناوری اطلاعات، حوزه خبررسانی تغییرات فراوانی کرده است. برای مثال بسیاری از مجلات و روزنامه های کاغذی جای خود را به انواع الکترونیکی داده اند.

RSS^۱ نمونه ای از ابزارهای جدید ارائه اخبار هستند. RSS ها یا خبرخوان ها نرم افزارهایی هستند که بر اساس علاقه مندی های کاربر، مطالب مورد نظر را از سایت های مختلف جمع آوری کرده و در یک صفحه نمایش می دهند. این امر ضمن آسان کردن جمع آوری اطلاعات برای کاربر، صرفه جویی در زمان را به همراه دارد.

فناوری اطلاعات و ارتباطات به اختصار «فاوا» نامیده می شود.

فناوری اطلاعات

«مطالعه، طراحی، توسعه، پیاده‌سازی، پشتیبانی یا مدیریت سیستم‌های اطلاعاتی مبتنی بر رایانه را فناوری اطلاعات می‌گویند.» به عبارت دیگر فناوری اطلاعات ترکیبی از انسان، رویه‌ها (سازوکارها)، ساختار و ابزار (سخت‌افزار، نرم‌افزار، شبکه و داده‌ها) است.



- **ابزار:** ترکیب داده و اطلاعات در بستر شبکه و پردازش آنها در سخت‌افزارها (دستگاه‌های مختلف)، توسط الگوریتم‌های مختلف (نرم‌افزارها)
- **سازوکارها:** رویه‌ها و استانداردها
- **ساختار:** هدف و چهارچوب معین
- **انسان:** طراحی، ایجاد و کاربری

فناوری ارتباطات

با افزایش ظرفیت انتقال داده‌ها و اطلاعات و ایجاد انواع جدید ارتباط مانند ارتباطات بی‌سیم و موبایل (سلولی)، راه برای مرتبط ساختن دستگاه‌های مختلف هموار شد. در ابتدا اولین شبکه‌های انتقال اطلاعات به صورت درونی و محدود (درون یک مجموعه، شرکت یا سازمان و ...) ایجاد شدند که به آن اینترنت گفته می‌شود. شبکه درون ساختمان وزارت آموزش و پرورش نمونه‌ای از آن است. سپس نوع گسترده‌تری از شبکه‌ها ظهور یافتند که بین چند شرکت یا سازمان ارتباط برقرار می‌کردند که به آن اکسترانت گفته می‌شود. مانند شبکه‌ای که بین سازمان ثبت‌احوال و آموزش و پرورش وجود دارد. در نهایت با پیشرفت فناوری، شبکه جهانی اینترنت ظهور یافت.



کاربردهای فناوری اطلاعات و ارتباطات

بیشتر پیشرفت‌های بشری از جمله فناوری اطلاعات در مسیر پاسخ به سؤالات و ابهامات موجود و ساده‌تر کردن زندگی صورت گرفته است. سازوکارهای بی‌شمار موجود و آتی فناوری اطلاعات باعث ایجاد کاربردهای جدید و روزافزون خواهد شد. پزشکی از راه دور یکی از کاربردهای فاوا می‌باشد که این علم و تکنولوژی مدرن به پزشکان امکان می‌دهد بیماران خود را در خانه بیمار و یا در بیمارستان دیگری در هر جای دنیا از راه دور از طریق کامپیوتر و شبکه‌های ارتباطی چون اینترنت ویزیت و درمان کنند و تصویر و صدای بیمار، علائم حیاتی و حتی پارامترهای تخصصی لازم را دریافت و توصیه‌های لازم را صادر کنند. در نتیجه، تأخیر در درمان به حداقل می‌رسد و نیاز به جابه‌جایی بیمار برطرف می‌شود و در هزینه‌های ناشی از حمل‌ونقل بیمار نیز صرفه‌جویی می‌گردد.

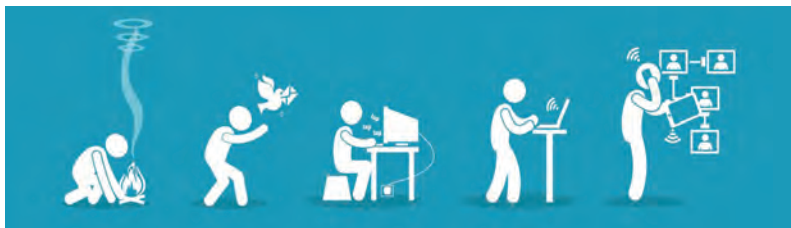


همان‌طور که می‌توان از فاوا برای تسهیل امور بهره برد می‌توان از آن برای جاسوسی و سرقت اطلاعات، وارونه‌سازی حقایق در سطح جهانی و القای مفاهیم به‌صورت گسترده استفاده کرد. در نتیجه نمی‌توان به تمامی اطلاعات موجود در شبکه‌های اجتماعی اطمینان کرد.

نکات ایمنی
و حفاظتی



راه‌های ارتباط میان انسان‌ها، از گذشته تا به امروز تغییرات فراوانی کرده است. در ابتدا ارتباط تنها به صورت ایما و اشاره و اصوات بی معنی بود. پس از به وجود آمدن زبان، ارتباط کلامی شکل گرفت و پس از به وجود آمدن خط، ارتباطات نگارشی (مانند نامه) به وجود آمد. اکنون با پیشرفت بشر، راه‌های ارتباطی جدید، مانند ارتباط در لحظه ممکن شده است. تلفن‌های همراه، دورنگار (فکس)، اینترنت، پست الکترونیکی (ایمیل) و تماس‌های تصویری (ویدئویی)، نمونه‌هایی از وسایل و امکانات نو ارتباطی هستند.



ویدئوکنفرانس از دیگر ابزارهای جدید در حوزه فاوا است که بستر برگزاری جلسه واحد میان افراد از نقاط مختلف جغرافیایی را در یک زمان و به صورت تصویری فراهم می‌کند. این امکان، ضمن سهولت، موجب صرفه‌جویی قابل توجهی در وقت و هزینه‌های ایاب و ذهاب می‌شود.



آلودگی‌های زیست‌محیطی، گرم‌شدن کره زمین، تغییر زیست‌بوم‌ها توسط فعالیت‌های انسانی و... باعث آسیب به محیط‌زیست می‌گردد. فناوری اطلاعات می‌تواند با سازوکارهای خود، اثر بسیاری از موارد مخرب را کاهش دهد. انجام خدمات الکترونیکی بانکی نمونه‌ای از آن است که باعث کاهش سفرهای درون‌شهری و در نتیجه کاهش مصرف سوخت و آلودگی زیست‌محیطی می‌شود. از سوی دیگر فناوری اطلاعات امکان انجام انواع پایش برای محیط‌زیست را ایجاد می‌کند.



کاربرد فاوا در کشاورزی

سنجش از دور، پایش تغییرات آب‌وهوا و توسعه مزارع هوشمند، از کاربردهای فاوا در بخش کشاورزی هستند. به‌وسیله «سنجش از دور» می‌توان تغییرات زیست‌محیطی منطقه که موجب تأثیرات مثبت یا منفی بر محصولات کشاورزی می‌شود را بررسی و با برنامه‌ریزی مناسب باعث تولید محصولات در حالت بهینه شد.

ربات‌های هوشمند می‌توانند سطح مزرعه را بررسی کرده و اطلاعاتی درباره رطوبت، آفات گیاهی و رشد محصول و غیره به کشاورز گزارش کنند. بررسی و تحلیل این اطلاعات و تصمیم‌گیری بر اساس آنها می‌تواند کیفیت محصولات کشاورزی را افزایش دهد.



کاربرد فاوا در صنعت

فناوری اطلاعات می‌تواند در کشف نیازهای مشتریان، طراحی، تأمین مواد اولیه، خودکارسازی تولید، کنترل در لحظه فرایندها، ایجاد تغییرات در برنامه تولید بدون حضور در محل کارخانه، فروش و غیره تأثیرگذار باشد.

فاوا در ۱۰ سال اخیر، چه تغییراتی در رشته تخصصی شما ایجاد کرده است؟ با استفاده از سواد فناورانه خود چه آینده‌ای را برای آن متصور هستید؟ ■ برای جلوگیری از ایجاد شکاف مهارتی، چه مهارت‌هایی نیاز است؟



کاربرد فناوری اطلاعات و ارتباطات در هنر

پویایی هنر مستلزم خلق، نمایش و عرضه آثار هنری است. فناوری اطلاعات از طریق تسهیل آموزش، جمع‌آوری اطلاعات و ایده‌یابی (با ارائه منابع اطلاعاتی وسیع) به خلق و فروش این آثار کمک می‌کند.

فناوری اطلاعات و ارتباطات چگونه ایجاد و عرضه آثار هنری را متحول ساخته است؟



کاربرد فاوا در خدمات

محسوس‌ترین حوزه نفوذ فناوری اطلاعات بخش خدمات است. استفاده از فاوا باعث تغییرات بسیار زیادی در نحوه ارائه خدمات شده است. بانک‌ها از نمونه‌های بارز بهره‌گیران از فناوری اطلاعات در سطح وسیع هستند. در گذشته برای پرداخت قبوض باید صف‌های طولانی بانک را تحمل می‌کردید. اما امروزه با اسکن بارکد قبض، به وسیله تلفن همراه در برنامه همراه بانک و زدن یک دکمه، قبض پرداخت می‌شود.



پرونده‌های سلامت الکترونیکی، تشخیص در لحظه بیماری، معاینه از راه دور و سیستم‌های خبره پزشکی تنها بخشی از کاربردهای فناوری اطلاعات در سلامت و پزشکی است. با ورود فناوری اطلاعات، یک پزشک می‌تواند کلیه سوابق بیمار خود را در لحظه بررسی کرده و تصمیم بهینه را اتخاذ کند.

تاکسی اینترنتی از جمله خدمات جدیدی است که به واسطه توسعه فاوا و ارتباطات ممکن شده است. امروزه درخواست تاکسی محدود به تاکسی‌های بی‌سیم و تلفنی نیست و می‌توان با مشخص کردن مبدأ و مقصد بر روی نقشه الکترونیک، با زمان انتظار بسیار کم، نزدیک‌ترین خودرو موجود را یافت و قبل از سفارش، از هزینه آن مطلع شد.



■ در حوزه خدمات هنوز بسیاری از موارد به صورت غیرالکترونیکی انجام می‌شود.

دنیای مجازی دنیایی در امتداد دنیای واقعی است. به عبارت دیگر، در دنیای مجازی انسان به وسیله مؤلفه‌هایی، دنیای واقعی را به نحوی شبیه‌سازی کرده که به شکل برنامه‌ریزی شده، اهداف سازندگان و افراد درون آن را دنبال می‌کند. ترکیب دنیای مجازی با واقعی باعث ایجاد زمینه‌های جدید به صورت واقعیت مجازی و واقعیت افزوده، شده است.

واقعیت افزوده^۱

ترکیب دنیای مجازی و واقعی با نام «واقعیت افزوده» مطرح است. واقعیت افزوده نمایش اطلاعات بر روی تصویر زنده است. سیستم‌های حضور و غیاب جدید را در نظر بگیرید. در گذشته این سیستم‌ها به وسیله اثر انگشت فرایند شناسایی افراد را انجام می‌دادند. اما اکنون با شناسایی چهره افراد، اطلاعات را بر روی تصویر زنده فرد نمایش می‌دهند. این مثال، نمونه‌ای از واقعیت افزوده است.



واقعیت مجازی^۱

واقعیت مجازی، شبیه‌سازی دنیای واقعی با تعامل فیزیکی است. برای مثال دستگاه‌های شبیه‌ساز پرواز^۲ را در نظر بگیرید. در این دستگاه تمام اتفاقات، حرکات و محیط‌ها، شبیه‌سازی شده بر اساس واقعیت هستند. فردی که در درون دستگاه است اطلاعات واقعی را به صورت مجازی دریافت کرده و با آن تعامل می‌کند. نمونه‌هایی از دستگاه شبیه‌ساز پرواز و عینک‌های واقعیت مجازی را در شکل می‌بینید.



با پیشرفت تمدن بشری، اولین اجتماعات انسانی شکل گرفت. این اجتماعات ایجادکننده قبایل، روستاها و بعد شهرها بوده‌اند. با بزرگ‌تر شدن اجتماعات انسانی اولین جوامع به‌وجود آمدند.

اجتماعات مجازی شکل‌دهنده شبکه‌های اجتماعی هستند. درون یک شبکه اجتماعی، گروهی از انسان‌ها باهم تعامل دارند. در شبکه‌های اجتماعی افراد به‌وسیله انتشار دیجیتال اطلاعات، حضور دیجیتالی دارند. حضور دیجیتالی نیازمند حضور فیزیکی همیشگی نیست. فرض کنید یک پیام از طریق پست الکترونیکی دریافت کرده‌اید؛ شما به واسطه حضور دیجیتالی پیام را گرفته‌اید اما ممکن است در زمان دیگری آن را مشاهده کنید، یا در لحظه ارسال پیام در سرویس ایمیل خود حضور نداشته باشید.

تفاوت وب ۱ و ۲ با ۱ و انواع آن

در برخی از وب‌سایت‌ها کاربران فقط می‌توانند محتوای موجود را دریافت کنند و نمی‌توانند در آن محیط با دیگران تعامل داشته باشند. این وب‌سایت‌ها مبتنی بر وب یک (نسل اول وب) هستند. درحالی‌که وب دو (نسل دوم)، تعامل را به‌عنوان رکن اصلی معرفی می‌کند. شبکه‌های اجتماعی مبتنی بر وب دو است. وب دو به‌واسطه ابزارهای تعاملی آن از وب یک متمایز می‌شود. شبکه‌های اجتماعی، ویکی‌ها، بلاگ‌ها و RSS از انواع ابزارهای وب دو هستند.

ویکی‌ها، وب‌سایت‌هایی هستند که در آن افراد مختلف (عضو و غیر عضو) می‌توانند صفحاتی را با موضوعات مختلف ایجاد کرده و برای آن محتوا ایجاد کنند. دسترسی و ویرایش به این صفحات برای همه آزاد بوده و افراد می‌توانند به‌مرور زمان محتوای موجود را بهبود بخشیده و در صورت نیاز تصحیح کنند. باید دانست که به دلیل قابل ویرایش بودن مطالب توسط هر فرد، مطالب موجود در ویکی‌ها قابل استناد نیست.

کاربردهای شبکه‌های اجتماعی

شبکه‌های اجتماعی به‌عنوان قوی‌ترین و کامل‌ترین ابزار تعاملی (و در نتیجه وب دو) دارای کاربردهای بسیار فراوانی نظیر برقراری ارتباط، دریافت اطلاعات عمومی و تخصصی، انجام فعالیت‌های تجاری، آموزش و غیره هستند.

جوامع دیجیتالی و شبکه‌های اجتماعی همانند جوامع سنتی از انسان‌ها تشکیل شده‌است. وجود انسان‌های بسیار زیاد در این جوامع و برداشته شدن مرزهای جغرافیایی، فرهنگی و تخصصی باعث می‌شود شبکه‌های اجتماعی مانند شمشیر دو لبه، هم سازنده و هم مخرب باشند.

استفاده از اطلاعات تخصصی افراد مختلف و تعامل با صاحب‌نظران از مزایای شبکه‌های اجتماعی است. از سوی دیگر افراد هویت دیجیتالی خود را از طریق اطلاعاتی که به اشتراک می‌گذارند تعریف می‌کنند. این اطلاعات می‌تواند به صورت عمدی یا غیرعمدی ناصحیح باشد و موجب گمراهی کاربران دیگر شود. از سوی دیگر بسیاری از اطلاعات افراد، بدون اینکه خود بدانند، برای سایر اعضای یک شبکه قابل‌رؤیت است. در نتیجه با تعامل در شبکه‌های اجتماعی ممکن است برخی از اطلاعات به صورت ناخواسته افشا گردد.



امنیت و حریم خصوصی

افراد برای حضور دیجیتالی خود سطوح مختلفی از اطلاعات شخصی مانند نام، سن، اطلاعات بانکی، اطلاعات تماس و غیره را ارائه می‌کنند. تصمیم‌گیری در مورد ارائه این اطلاعات در سایت‌های معتبر باید پس از مطالعه قسمت «حریم خصوصی» انجام شود. تمامی ارائه‌کنندگان خدمات دیجیتالی موظف به رعایت قوانین حریم خصوصی هستند.



در شبکه‌های اجتماعی اطلاعات با آزادی بیشتری منتقل می‌شوند و این امر امکان سوءاستفاده از آنها را بیشتر می‌کند. امروزه مهندسی اجتماعی به‌عنوان یکی از راه‌های سوءاستفاده در شبکه‌های اجتماعی متداول است. «مهندسی اجتماعی» راه دریافت اطلاعات از کاربر توسط افراد سودجو است به‌طوری‌که کاربر متوجه نیت سوء آن افراد نباشد. برای مثال: افرادی که به دریافت اطلاعات حساب بانکی و یا وجه به نام سازمان‌های خیریه اقدام می‌کنند.

ابزارهای مخرب

راه‌های بسیاری برای دریافت اطلاعات و سوءاستفاده از کاربران وجود دارد. ویروس‌ها، تروجان‌ها، ترس‌افزارها و غیره، انواع مختلفی از ابزارهای سوءاستفاده هستند.

برای مثال: در ابتدای نشانی سایت بانک‌ها <https> قرار دارد. حرف S نشانگر وجود کانال ارتباطی ایمن بین سایت مقصد و کاربر است. در این حالت اطلاعات منتقل‌شده بین وب‌سایت و کاربر رمزگذاری می‌شود و در مقابل حملات رایانه‌ای ایمن است.

داده‌کاوی

وجود اطلاعات بسیار زیاد در شبکه‌های اجتماعی موجب می‌شود که بتوان با رعایت نکات اخلاقی، قانونی، اجتماعی و فنی به حجم انبوهی از اطلاعات دست یافت و آنها را با اهداف مختلف تحلیل کرد. به‌عنوان مثال تولیدکنندگان تلفن همراه با تحلیل اطلاعات کاربران شبکه‌های اجتماعی، سلاقی، اطلاعات جمعیت‌شناختی و نوع دستگاه‌های مورد استفاده را مشخص کرده و بر آن اساس محصولات خاص هر منطقه جغرافیایی را طراحی می‌کنند.

فرض کنید می‌خواهید یک محصول یا خدمت جدید تولید کنید. برای این منظور به اطلاعاتی در مورد طراحی، تولید، بازار هدف و غیره نیاز است. شبکه‌های اجتماعی، محل مناسبی برای جمع‌آوری و تحلیل این اطلاعات هستند. «داده‌کاوی» راه انجام این کار است. به بیان دیگر داده‌کاوی استخراج اطلاعات نهان یا الگوها و روابط مشخص در حجم زیادی از داده‌ها است. لذا می‌توان اطلاعات لازم را در چرخه عمر محصول به‌وسیله داده‌کاوی به‌دست آورد. «چرخه عمر» محصول با معرفی آن به بازار شروع می‌شود. پس از آنکه محصول در بازار شناخته شد، از نظر فروش رشد می‌کند، به بلوغ می‌رسد و پس از مدتی حضور در بازار با ورود رقبا، فناوری‌های جدید یا مدل‌های به‌روز، فروش آن افت پیدا می‌کند.



تحلیل اطلاعات مربوط به نیازهای مشتریان آتی محصول، ویژگی‌های بازار هدف، تکنولوژی‌های موجود و ...

توسعه

تحلیل اطلاعات مورد نیاز برای تبلیغات و معرفی محصول، تفاوت با رقبا، ویژگی‌های جدید

معرفی

تحلیل اطلاعات بازخوردهای مشتریان، اثربخشی تبلیغات، پیشنهادات تشویقی

رشد

تحلیل اطلاعات مشتریان برای نگهداشتن بیشتر محصول در رقابت، تبلیغات، بازاریابی، کشف بازارهای جدید

بلوغ

تحلیل اطلاعات در رابطه با رقبا، ویژگی‌های مورد انتظار برای اضافه‌شدن به‌منظور کاهش سرعت افول و ...

افول

کسب و کار و تجارت الکترونیکی

هر توافقی که با ردوبدل کردن پول و یا معادل آن انجام شود تجارت است. کسب و کار مفهومی گسترده‌تر دارد و تجارت، بخشی از آن است. کسب و کار، فعالیت اصلی است که می‌تواند هدف مالی یا غیرمالی داشته باشد. برای مثال مدرسه یک نوع کسب و کار است؛ همچنین ادارات دولتی ارائه‌کننده خدمات عمومی نیز می‌توانند در دسته کسب و کارها قرار گیرند.

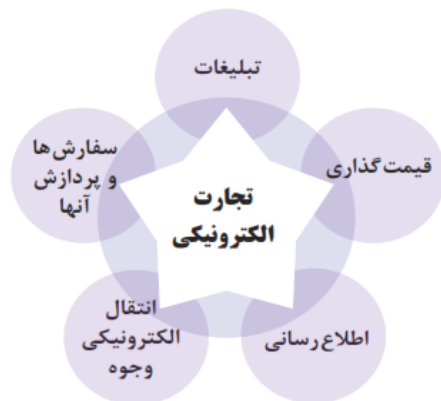
کسب و کارها را می‌توان براساس میزان انجام فعالیت‌های خود به صورت دیجیتالی دسته‌بندی کرد. یک فروشگاه اینترنتی فعالیت‌های دریافت سفارش و وجه را به صورت دیجیتالی انجام می‌دهد اما کالا به صورت فیزیکی به دست شما می‌رسد. پس در کسب و کار الکترونیکی فعالیت‌های مختلفی صورت می‌گیرد که ممکن است کاملاً دیجیتالی نباشند.

بلیت‌های الکترونیکی یکی از انواع مزایای ایجاد کسب و کارهای الکترونیک است. دیگر نیاز به ایستادن در صف‌های طولانی برای تهیه بلیت نیست.



تجارت الکترونیکی

معمولاً فعالیت‌های بازاریابی و تبلیغات، فعالیت‌های فروش، قیمت‌گذاری و غیره را می‌توان به صورت الکترونیکی انجام داد. در شکل زیر برخی فعالیت‌های مرتبط با تجارت الکترونیکی نشان داده شده است.



پروانه ابتدا که از تخم بیرون می‌آید به صورت یک کرم است. این کرم، پیله‌ای به دور خود می‌تند، سپس در داخل پیله فرایند تبدیل شدن به پروانه آغاز می‌شود و در نهایت تبدیل به یک پروانه کامل می‌شود. به این فرایند «دگردیسی» می‌گویند. در دنیای نوین نیز تحول یک فرایند، کالا یا خدمت با بهره‌گیری از سازوکارهای دیجیتالی را دگردیسی دیجیتالی می‌گویند.

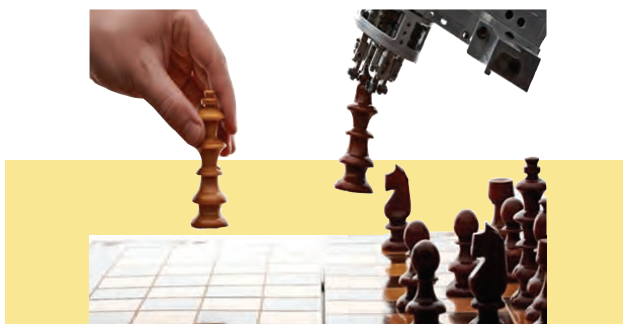


دگردیسی دیجیتالی با عناصر آن قابل شناسایی است. مطابق تعاریف مختلف، عناصر متنوعی برای دگردیسی دیجیتالی وجود دارد. برخی از عناصر دگردیسی دیجیتالی به شرح زیر است:



هوش مصنوعی

از دیرباز برای فهماندن دنیای پیرامون به ماشین، باید از زبان‌های قابل فهم برای ماشین استفاده می‌شد. این زبان‌ها کامل نبوده و استفاده از آنها دشوار بوده‌است. تعامل خودکار ماشین با انسان و محیط و فهم ماشین از دنیای پیرامون بدون ترجمه یک نفر واسطه به معنی هوش مصنوعی است. به عبارت دیگر «هوش مصنوعی» به سیستم‌هایی گفته می‌شود که می‌توانند واکنش‌هایی مشابه رفتار انسانی برای درک، یادگیری و ارائه راه‌حل برای شرایط از پیش تعریف نشده را از خود نشان دهند. تعاریف مختلفی برای هوش مصنوعی وجود دارد ولی به صورت عمومی، **هوش مصنوعی** عبارت است از اینکه چگونه می‌توان کامپیوترها را وادار به انجام کارهایی کرد که در حال حاضر انسان‌ها آنها را صحیح یا بهتر انجام می‌دهند. بازی‌های رایانه‌ای نمونه‌ای از هوش مصنوعی هستند که در آن، نرم‌افزار بازی، با فرد بازی‌کننده تعامل دارد.



هوش مصنوعی سطوح مختلفی دارد. سیستم‌های هوشمند معمولی در تولید صنعتی نمونه ساده آن هستند. ربات‌های صنعتی بر اساس دما، رطوبت و فشار هوا مکان نقاط جوش را تغییر می‌دهند تا از استاندارد موجود انحراف پیدا نکنند. رانندگی خودکار اتومبیل‌ها از نمونه‌های پیشرفته‌تر هوش مصنوعی محسوب می‌شود. هوش مصنوعی موجود در این خودروها بر اساس حسگرها، رادارها، اطلاعات ماهواره‌ای (GPS)^۱ و مسیریابی، بهترین مسیر را انتخاب کرده و با پایش محیط اطراف، تشخیص تابلوها و شناخت محیط جاده، فعالیت رانندگی را انجام می‌دهد. ربات‌های امدادی که می‌توانند بدون کمک انسانی مسیر خود را در شرایط مختلف پیدا کرده و فعالیت‌های امدادی انجام دهند انواع پیچیده‌تر هوش مصنوعی هستند. آنها با توجه به شرایط مختلف تصمیم‌گیری کرده، مسیر مناسب را انتخاب می‌کنند و شرایط اولیه موجود را گزارش می‌دهند.



اینترنت اشیا

اینترنت اشیا این امکان را ایجاد می‌کند تا اطلاعات از اشیا جمع‌آوری و پردازش شود. خانه‌های هوشمند با تحلیل میزان رفت و آمد، سنجش نور، دما و کنترل لوازم خانگی سعی می‌کنند تا مصرف انرژی بهینه باشد. این خانه‌ها می‌توانند اطلاعات مربوط به خرید موارد مورد نیاز را برای خانه، به تلفن همراه بفرستند.

یک درخت که به اینترنت متصل است به همراه سیستم آبیاری خودکار، و حسگر میزان نور آفتاب، می‌تواند امکان آبیاری و کود دادن خودکار را برای درختان فراهم کند و یا در زمان مورد نیاز از طریق برنامه موجود در تلفن همراه به کاربر اطلاع دهد. بسیاری از اشیا و وسایل محیط پیرامون که بتوانند به شبکه اینترنت متصل شده و توسط برنامه‌ها و نرم‌افزارها (موجود در کامپیوتر، تلفن همراه و غیره) کنترل و مدیریت شوند را می‌توان «اینترنت اشیا» نامید.

مزارع هوشمند بر اساس حسگرهای موجود در سطح مزرعه، اطلاعات مربوط به زمان آبیاری و سطح مواد مغذی خاک (کود دادن) را برای کشاورز می‌فرستند، در سطح پیشرفته‌تر، فرایند آبیاری و کود دادن نیز به‌طور خودکار انجام شده و نتایج به کشاورز گزارش داده می‌شود.

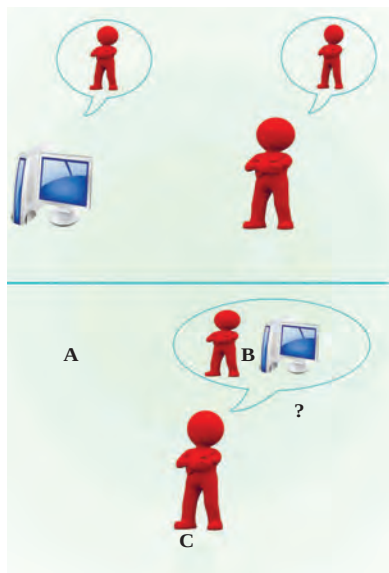
به زبان ساده، ارتباط حسگرها و دستگاه‌ها با شبکه‌ای که از طریق آن می‌توانند با یکدیگر و کاربران‌شان تعامل کنند را می‌توان اینترنت اشیا دانست. این مفهوم می‌تواند به‌سادگی ارتباط یک گوشی هوشمند با تلویزیون یا به پیچیدگی نظارت بر زیرساخت‌های شهری و ترافیک باشد.



هوش مصنوعی

در سال‌های اخیر تولیدکنندگان کالاها و محصولات سخت‌افزاری و نرم‌افزاری، در نام‌گذاری برخی از محصولات خود از واژه هوشمند مانند: تلویزیون هوشمند، تلفن همراه هوشمند، لوازم خانگی هوشمند یا برنامه هوشمند حسابداری استفاده می‌کنند. آنها ادعا می‌کنند در ساخت این نوع محصولات از هوش مصنوعی استفاده شده است. برخی از لوازم خانگی هوشمند به وسیله حسگرها اطلاعات محیط را می‌گیرند و به‌طور خودکار اعمال مختلفی را انجام می‌دهند. ممکن است با برخی بازی‌های رایانه‌ای نسل جدید آشنا باشید، در این بازی‌ها با رقیبان رایانه‌ای که هوش مصنوعی دارند به رقابت پرداخته و مشاهده می‌کنیم چه عملکرد هوشمندانه‌ای نسبت به بازی‌های قدیمی دارند.

هوش مصنوعی شاخه‌ای از علم رایانه است که ضمن مطالعه و توسعه نرم‌افزارها و دستگاه‌های هوشمند با شبیه‌سازی توانایی‌های انسان در ماشین، سعی در تقلید رفتارهای هوشمندانه انسان دارد.



شکل ۴- آزمون سنجش میزان هوشمندی ماشین

از ابتدای پیدایش رایانه‌ها این سؤالات مطرح شده است که چه ماشینی را می‌توان هوشمند نامید و برای سنجش میزان هوشمندی ماشین از چه روشی می‌توان استفاده کرد؟ دانشمندان علوم رایانه در شاخه هوش مصنوعی مواردی از این قبیل که انسان چگونه فکر می‌کند، نحوه یادگیری و تصمیم‌گیری در انسان چگونه رخ می‌دهد را مطالعه کرده‌اند و نتایج این مطالعات را به‌عنوان پایه‌ای برای توسعه نرم‌افزارها و سیستم‌های هوشمند قرار داده و به این نتیجه رسیده‌اند که باید آن ماشین در جنبه‌های مختلف هوش، مانند انسان باشد و بتواند توانایی‌های انسان هوشمند را تقلید کند و برای سنجش میزان هوشمندی یک ماشین، آزمونی پیشنهاد کردند.

آزمون به این صورت انجام می‌گیرد که یک شخص به‌عنوان قاضی (C)، با یک ماشین (A) و یک انسان (B) گفت‌وگو می‌کند، به نحوی که قاضی، انسان و ماشین را نمی‌بیند و سعی در تشخیص ماشین از انسان دارد. در صورتی که ماشین بتواند پس از گفت‌وگو با قاضی، وی را به‌گونه‌ای فریب دهد که در قضاوت خود دچار اشتباه

شود و او را به‌عنوان انسان شناسایی کند، توانسته است آزمون را با موفقیت پشت سر بگذارد. برای آسان‌تر و استاندارد کردن شرایط برگزاری آزمون و پرهیز از پیچیدگی‌های اضافی، آزمون به محاوره روی کاغذ محدود شود تا مشکلاتی مانند تبدیل متن به گفتار شفاهی و تنظیم تن صدا و لهجه در کار نباشد (شکل ۴).

کاربردهای هوش مصنوعی

به خاطر گستردگی تأثیر هوش مصنوعی بر جنبه‌های مختلف زندگی بشر، در این پودمان نمی‌توان تمامی آنها را بررسی و یا حتی معرفی کرد اما انتظار می‌رود در پایان این بخش آگاهی و تفکر شما تا حدی افزایش پیدا کند و بتوانید به سایر جنبه‌هایی که اشاره نشده است نیز بیندیشید. در شکل ۶ برخی از حوزه‌های کاربردی و تأثیرات هوش مصنوعی معرفی شده است. حال به بررسی برخی از موارد فوق می‌پردازیم.



شکل ۶- حوزه‌های کاربرد هوش مصنوعی

- حوزه شغلی

یکی از جنبه‌های مهمی که هوش مصنوعی بر آن تأثیر

به‌سزایی خواهد داشت، حوزه شغلی است. طبق پیش‌بینی‌های صورت گرفته طی سال‌های آینده، میلیون‌ها شغل از بین خواهند رفت و برخی نیز اهمیت خود را به میزان زیادی از دست خواهند داد؛ اما بعد از یک دوره گذار و یا به‌طور هم‌زمان هوش مصنوعی می‌تواند میلیون‌ها شغل جدید در سراسر دنیا ایجاد کند. توجه کنید میلیون‌ها شغل، نه میلیون‌ها شاغل! تعداد مشاغلی که در صنایع مختلف به هوش مصنوعی وابسته‌اند، متفاوت است. انتظار می‌رود در سال‌های آینده بخش‌های بهداشت و درمان، خدمات عمومی و آموزش بیشترین



میزان افزایش تقاضا برای این مشاغل را داشته باشند. در واقع هوش مصنوعی در بسیاری از مشاغل، ضمن کاهش یا حذف شغل‌هایی که مناسب انسان نیستند، شغل‌های رده بالاتر و با بازدهی بهتری ایجاد می‌کند که به مهارت‌های خاصی نیاز دارند و حتی ممکن است از انسان وقت کمتری بگیرند.

- شغل‌های خطرناک

ربات‌ها از پیشرفته‌ترین فناوری‌های هوش مصنوعی بهره می‌برند. امروزه ربات‌ها کارهای بسیار سخت و خطرناکی را انجام می‌دهند. محققان معتقدند فهرست بزرگی از کارهای خطرناک وجود دارند که اگرچه انسان‌ها قادر به انجام آنها نیستند؛ اما نسل جدید ربات‌ها در نقش یک ابرقهرمان ظاهر می‌شوند و به‌راحتی از عهده انجام آنها برمی‌آیند. برای



شکل ۷- ربات آتش‌نشان

نمونه می‌توان به حضور این ربات‌ها در عملیات آتش‌نشانی و تلاش برای خاموش کردن آتش‌سوزی‌ها در جنگل، خنثی کردن بمب و نجات انسان‌ها از زیر آوار اشاره کرد. شغل جوشکاری به تولید مواد سمی، گرمای شدید و سروصدا شناخته شده است، ربات‌ها در بسیاری از موارد می‌توانند به افراد در این شغل کمک کنند.



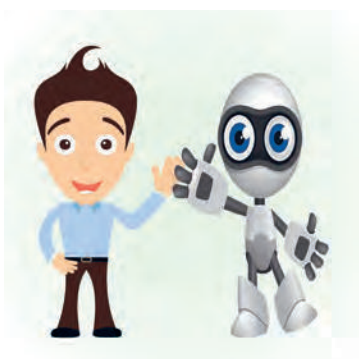
شکل ۸- نمای داخلی خودروی خودران

- حمل و نقل

استفاده از هوش مصنوعی به میزان زیادی سبب کاهش سفرها خواهد شد و جنبه‌های مختلفی از حوزه حمل و نقل را تحت تأثیر قرار خواهد داد. یکی از مهم‌ترین آنها حمل و نقل خودکار و خودروهای خودران است.

- ربات دوست مصنوعی ما

دانشمندان و متخصصان رباتیک مدعی شدند به زودی یک ربات هوشمند، مفهوم فلسفی عشق، علاقه و دوستی را درک خواهد کرد. این ربات‌ها با دسترسی به شبکه‌های اجتماعی، پایگاه‌های داده، ثبت و طبقه‌بندی صحبت‌ها



و انتخاب‌های ما، خواهند توانست به دوستی ارزشمند برای ما تبدیل شوند. آنها می‌توانند با دریافت اطلاعات بیشتر از رسانه‌های اجتماعی و با دسترسی به موتورهای جست‌وجو در اینترنت، اظهار نظر کرده، مانند یک شخصیت زنده در مکالمات شرکت کنند. با این اوصاف و با نزدیکی بیشتر بین انسان و ربات به عنوان دوست، باید کمی نگران روابط اجتماعی و خانوادگی بود؛ اما اگر فناوری در جهت مثبت خود به کار گرفته شود، می‌تواند تأثیرات بسیار مفیدی بر زندگی انسان بگذارد. پس تصمیم نهایی با انسان است که چگونه از آن بهره‌مند شود.

- حوزه فرهنگی، اجتماعی و آموزشی

با توجه به وسعت این حوزه، گوشه‌ای از آن در قالب دو سؤال و پاسخ به آنها بیان می‌شود

- آیا می‌توان برای حل برخی معضلات اجتماعی مانند مشکل تخصیص شغل به افراد بیکار از هوش مصنوعی استفاده کرد؟

این کار را می‌توان با ثبت اطلاعات شهروندی افراد در طول زندگی آنها در یک سیستم امن تحت مدیریت برنامه‌های هوش مصنوعی اجرایی کرد. همچنین یک بانک اطلاعاتی از مشاغل فعال و نیازمند به افراد تشکیل شود تا هنگامی که افراد مختلف جامعه برای دریافت یک شغل خاص اقدام می‌کنند، همه آنها بر اساس معیارهای متفاوت دسته‌بندی شوند و دیگر تحصیلات و یا رابطه، تنها ملاک برای اخذ شغل نباشد. در اینجا هوش مصنوعی قادر به شناسایی شغل مناسب برای هر شهروند است و آن را بر اساس سابقه کاری فرد، مهارت‌ها و ترجیحات شخص پیشنهاد خواهد کرد.

- آیا می‌توان برای اصلاح روش پذیرش دانشگاه‌ها به جای آزمون سراسری از هوش مصنوعی استفاده کرد؟
پذیرش دانشگاه‌ها را می‌توان به یک سیستم هوش مصنوعی سپرد تا رشته دانشگاهی متناسب با استعداد و علاقه دانش‌آموز را بر اساس عملکرد کل دوران تحصیل و علاقه‌مندی‌های دانش‌آموز به وی پیشنهاد کند. هوش مصنوعی در راستای هدایت تحصیلی و دادن مشاوره به دانش‌آموزان و والدین می‌تواند بسیار مفید باشد.

حوزه امنیت

بینایی ماشین در این حوزه نقش چشمگیری دارد. از سیستم‌های امنیتی می‌توان، سیستم خودکار تشخیص اثرانگشت را نام برد. به گوشی‌ها و رایانه‌های قابل حمل جدید قابلیت finger print اضافه شده است که می‌توانند صاحب خود را به وسیله اثرانگشت شناسایی کنند.

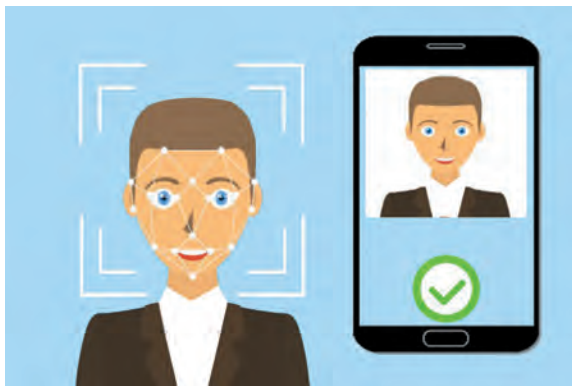
کد امنیتی دیگری که همیشه همراه انسان حمل می‌شود، چشم انسان است. دانشمندان ثابت کرده‌اند که الگوی بافت‌های موجود در عنبیه چشم هر انسان منحصر به فرد است و الگوهای بافتی عنبیه چشم هیچ دو فردی در دنیا دقیقاً مثل هم نیست. از همین روش برای شناخت افراد و سیستم‌های امنیتی استفاده می‌شود.

حوزه راهنمایی و رانندگی

- با تشخیص پلاک خودروها هنگام بنزین زدن و پارک خودرو در پارکینگ‌ها دیگر نیازی به پرداخت پول نقد و یا حتی استفاده از کارت اعتباری نیست.

- با استفاده از پردازش ویدیویی تصاویر دوربین‌های مدار بسته در خیابان‌ها به صورت خودکار، خودروهای سرقت شده شناسایی می‌شود.

- با پردازش تصاویر دوربین‌های نصب شده در تقاطع‌ها می‌توان زمان، سرعت، جهت حرکت و پلاک خودروها را به دست آورد و بدین ترتیب تخلفات متنوعی از جمله عبور از چراغ قرمز، توقف روی خط عابر پیاده و تخطی از سرعت مجاز هنگام عبور از تقاطع را ثبت و اعمال قانون کرد.



شکل ۱۶- کاربرد تشخیص چهره در تلفن همراه هوشمند

حوزه تشخیص چهره (Face Recognition)

- باز شدن درهای امنیتی در ورودی ساختمان‌ها به صورت خودکار

- باز شدن قفل گوشی تلفن همراه

- بی‌نیازی به کارت اعتباری در فروشگاه‌ها برای پرداخت پول

- شناسایی مجرمین در حال تردد در خیابان‌ها، ایستگاه‌های قطار، اتوبوس و فرودگاه‌ها به صورت خودکار

- حضور و غیاب دانش‌آموزان و کارمندان

حوزه کشاورزی

کشاورزان می‌توانند با استفاده از تصاویر ماهواره‌ای یا تصاویری که با استفاده از پهپادها یا کوادکوپترهای کنترلی از مزرعه خود می‌گیرند و پردازش این تصاویر با یک برنامه نرم‌افزاری به راحتی وجود آفت، نیاز به آبیاری و رسیدگی در قسمتی از مزرعه و یا باغات را تشخیص دهند (شکل ۱۷). همچنین با این فناوری می‌توان محل علف‌های هرز را در مزرعه تشخیص داد و از بین برد و با پهپادهای مخصوص کشاورزی که به تازگی تولید شده‌اند به سم‌پاشی نیز پرداخت.



شکل ۱۷- کوادکوپتر

[illegible]



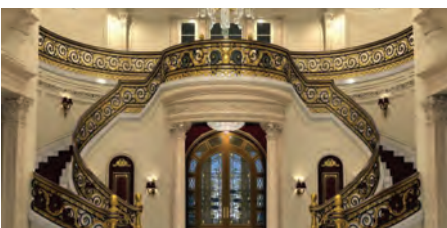
آیا می‌دانید سواد فناورانه چیست و چه رابطه‌ای با سواد علمی دارد؟



آیا در مورد تاریخ فناوری در رشته تحصیلی خود اطلاعاتی دارید؟



آیا به نحوه تأثیر فناوری‌های نو بر مشاغل امروزی اندیشیده‌اید؟



آیا می‌دانید فناوری‌های جدید علاوه بر فوایدی که دارند، می‌توانند منشأ برخی مشکلات در جامعه باشند؟



آیا می‌دانید که می‌توان فناوری را در خدمت توسعه فرهنگی قرار داد؟

«سواد» چه مفهومی دارد؟

واژه «سواد» را در زندگی روزمره زیاد شنیده‌اید، اما تا به حال به معنای آن فکر کرده‌اید؟ بین سواد و دانش تفکیک قائل می‌شوید یا برای هر دو یک معنا و مفهوم را در نظر می‌گیرید؟ سواد در مفهوم سنتی آن به معنای مهارت خواندن و نوشتن است ولی دانش اطلاعات کاربردی و سازمان‌دهی شده برای حل مسئله می‌باشد. در دنیای کنونی، هر روز فناوری جدیدی به وجود می‌آید و فناوری‌های دیگر به سرعت توسعه پیدا می‌کنند. همهٔ اینها برای پاسخ‌گویی به رشد سریع جمعیت، محدودیت منابع و افزایش تقاضای دنیای بشری است. بر این اساس، اکنون مفهوم سنتی سواد به چالش کشیده شده است، زیرا فناوری‌های نوین، مهارت‌های جدیدی را نیاز دارند که آن مفهوم سنتی نمی‌تواند پاسخ‌گو باشد. امروزه دانشمندان از انواع متعدد سواد، از قبیل سواد علمی، سواد فناورانه، سواد رایانه‌ای، سواد رسانه‌ای، سواد فرهنگی و سواد بصری یاد می‌کنند که افراد برای تأمین رفاه خود باید سرشته‌ای از آنها داشته باشند و در زندگی روزمره خود به کار برند.



سواد فناوریانه چیست؟

امروزه در همه کشورهای جهان «سواد فناوریانه» به عنوان بخشی از سواد پایه، در آموزش رسمی مدارس گنجانده شده است؛ زیرا بدون این سواد نمی‌توانید از ابزارهایی مانند رایانه، دستگاه تصویربرداری، پمپ بنزین، عابربانک و... استفاده کنید. بنابراین، آموزش سواد فناوریانه بخشی از آموزش شهروندی محسوب می‌شود. شهروندانی که از این سواد بی‌بهره باشند، در زندگی روزمره خود دچار مشکل شده و از رفاه و آسایشی که فناوری‌های نوین برای زندگی انسان به ارمغان آورده‌اند، محروم می‌مانند.



اکنون که با برخی کاربردهای سواد فناوریانه آشنا شدید، به چستی «سواد فناوریانه» فکر کنید.

فناوری مجموعه‌ای از دانش، تجربه

و مهارت است که انسان با به‌کارگیری آن، محصولات یا خدماتی را برای افزایش رفاه و غلبه بر مشکلاتش، تولید می‌کند. برای مثال انسان برای غلبه بر گرسنگی به فکر کشاورزی، ذخیره‌سازی مواد غذایی و تهیه آتش افتاد و سپس از طریق سلطه بر طبیعت توانست فناوری‌های لازم را برای آن اهداف، خلق کند. به همین دلیل، می‌توان گفت: فناوری عبارت است از کلیه دخل و تصرف‌های انسان بر طبیعت که برای بهبود شرایط زندگی و تأمین نیازهای



روشن کردن آتش با سنگ چخماق

روزمره صورت می‌گیرد. مطابق تعریف فوق، فناوری، فهرست بلندبالایی از اختراعات و نوآوری‌های انسان اولیه (از قبیل سنگ چخماق، اهرم و چرخ) تا انسان مدرن، از قبیل فناوری نانو، فناوری اطلاعات، فناوری شناختی، زیست‌فناوری، فناوری هوا و فضا، فناوری انرژی‌های نو و... را شامل می‌شود.



نمونه‌هایی از فناوری‌های جدید

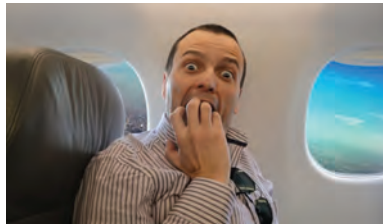
نمونه‌هایی از فناوری‌های نوین



فناوری‌ها علاوه بر مزایایی که دارند، می‌توانند مضراتی هم داشته باشند. به همین دلیل، انسان در استفاده از یک فناوری ممکن است سه نوع رفتار متفاوت از خود نشان دهد: فن‌هراسی افراطی، فن‌دوستی افراطی و استفاده محتاطانه و عالمانه. سواد فناورانه فن‌دوستی افراطی را تأیید نمی‌کند، بلکه نگاهی میانه به فناوری دارد و انسان را به استفاده عالمانه و محتاطانه از فناوری‌ها تشویق می‌کند.



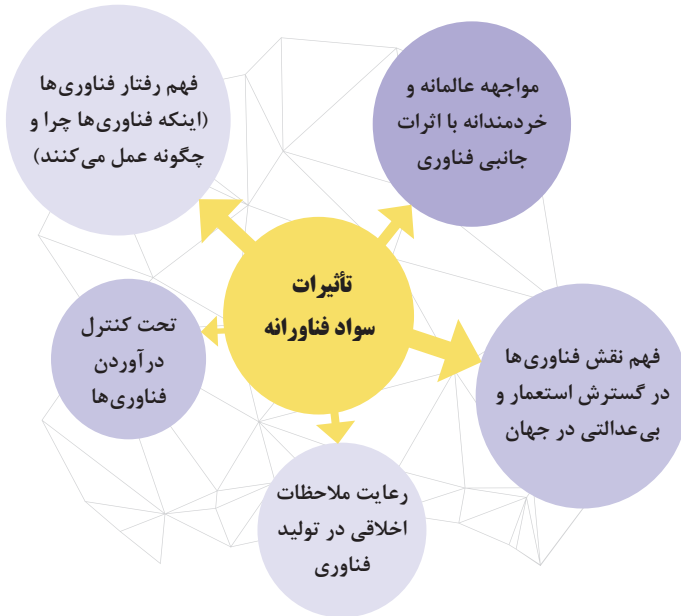
فن‌دوستی افراطی



فن‌هراسی افراطی

تعریف و تأثیرات سواد فناورانه

با توجه به مطالب فوق می‌توان گفت سواد فناورانه مجموعه‌ای از دانش، تجربه و مهارت است که به ما کمک می‌کند مزایا و خطرات یک فناوری را بشناسیم و به صورت عالمانه و محتاطانه از آن استفاده کنیم. افرادی که سواد فناورانه دارند نسبت به پیدایش فناوری‌های جدید و استفاده و به‌کارگیری آن عالمانه برخورد می‌کنند و در رفتارشان افراط و تفریط دیده نمی‌شود. این سواد در فکر و عمل آنان تأثیراتی خواهد داشت که برخی از آنها در تصویر زیر آمده است.



ضرورت سواد فناورانه

برای فهم ضرورت سواد فناورانه، به داستان ورود اینترنت به ایران فکر کنید. می‌دانید که نخستین اتصال به اینترنت در ایران، در اوایل دههٔ هفتاد شمسی؛ فقط به فاصله یک سال پس از تولد آن در غرب بوده است. در حقیقت جامعهٔ ایرانی در نخستین سال‌های تولد اینترنت، به این شبکه جهانی پیوست. به همین سبب، شهروندان ایرانی بی‌مقدمه و شتاب‌زده به دنیای هزار توی اینترنت پرتاب شدند. اینترنت تأثیرات مثبت زیادی برای جامعه داشت، ولی نبود آمادگی در جامعه، چالش‌های فرهنگی و امنیتی متعددی را برای جامعهٔ ایرانی ایجاد کرد و ذائقهٔ فرهنگی و سبک زندگی را تحت تأثیر قرار داد.



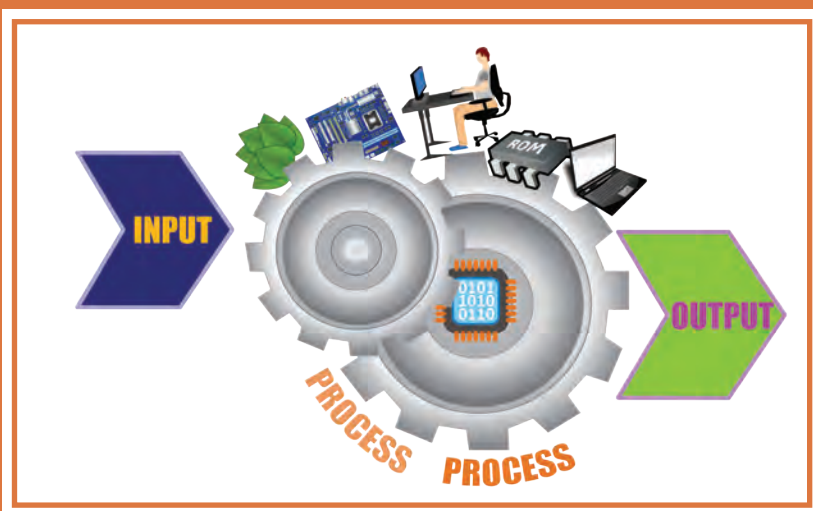
ورود گوشی‌های هوشمند و فناوری‌های جدید ارتباطی، این چالش‌های فرهنگی و امنیتی را تشدید کرد؛ در صورتی که اگر پیش از ورود این فناوری‌ها، سواد فناورانه، به‌ویژه سواد دیجیتالی، آموزش داده می‌شد، می‌توانستیم به‌راحتی بسیاری از چالش‌ها و تهدیدات جانبی این فناوری‌ها را پیش‌بینی و مدیریت کنیم.



**مخاطرات اینترنت
و گوشی همراه**



کلیات رایانه



قرن حاضر به شدت زیرسایه فناوری اطلاعات و ارتباطات و یافته‌های نوظهور آن است. افزایش روزافزون اطلاعات، نیاز به دسته‌بندی مناسب و بازیابی سریع و دقیق آن را اجتناب‌ناپذیر کرده است. مشاغل و کسب و کارهای مختلفی در حوزه فناوری اطلاعات و ارتباطات پدید آمده و اقتصاد جهانی را تحت تأثیر قرار داده است.

امروزه رایانه در بیشتر جنبه‌های زندگی مانند آموزش، کار و کسب، سرگرمی، سفر و... نقش بسزایی دارد. امروزه برای انسان‌ها سرعت و کیفیت انجام کارها اولویت دارد و سبب شده است که استفاده از رایانه‌ها اجتناب‌ناپذیر باشد.

تعریف رایانه



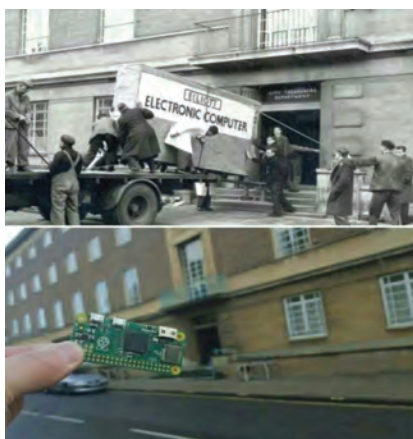
نام کامپیوتر در ایران از سال ۱۳۴۱ استفاده می‌شد که از واژه لاتین Compute به معنی محاسبه کردن گرفته شده است. در دو دهه اخیر واژه رایانه جایگزین واژه کامپیوتر شده است. رایانه دستگاهی است که بر اساس مجموعه دستوراتی به نام برنامه کار می‌کند. برنامه داده‌ها را دریافت، ذخیره و دست‌کاری کرده، به اطلاعات قابل بهره‌برداری شامل اعداد، متن، تصویر، صدا، فیلم یا سیگنال‌های الکترونیکی تبدیل می‌کند.



شکل ۱- رایانه‌های قدیم و جدید

به‌طور کلی به هر نوع وسیله محاسباتی رایانه گفته می‌شود. چرتکه یکی از ساده‌ترین و اولین رایانه‌هاست.

تاریخچه رایانه



شکل ۲- رایانه در گذر زمان

انسان‌های اولیه از انگشتان خود برای شمارش استفاده می‌کردند؛ نیاز انسان به شمارش، موجب شکل‌گیری محاسبه شد و به تدریج نقش آن اهمیت پیدا کرد. اولین وسیله‌ای که بشر در این زمینه از آن کمک گرفت چوب‌خط بود. در گذر زمان ابزارهای مشابهی از جمله چرتکه برای انجام محاسبات به کار گرفته شد. فقط ۶۰ سال فاصله زمانی بین دو تصویر شکل ۲ وجود دارد، ۶۰ سال بعد صنعت رایانه چگونه خواهد بود؟

کاربردهای رایانه

کاربرد رایانه در حمل و نقل



شکل ۳- کاربرد رایانه در حمل و نقل جاده‌ای

امروزه ارتباط با فواصل دور از طریق وسایلی مانند تلفن و اینترنت و به کارگیری سیستم‌های ماهواره‌ای بسیار آسان شده است ولی لزوم ارتباط‌های مستقیم از بین نرفته است. پیشرفت در تمامی سیستم‌های حمل و نقل اعم از جاده‌ای، راه‌آهن، دریایی، هوایی و دیگر وسایل حمل و نقل بر پایه استفاده مناسب از رایانه بوده است (شکل ۳).

کاربرد رایانه در آموزش



شکل ۴- به کارگیری رایانه در آموزش

یکی از کاربردهای مهم رایانه به کارگیری آن در آموزش است. در کشور ما نیز از روش‌های مختلف آموزش الکترونیکی (E-Learning)، در مدارس، دانشگاه‌ها، مراکز علمی و... استفاده می‌شود (شکل ۴). در تولید برنامه‌های آموزشی استفاده از محتواهای چندرسانه‌ای (Multi Media) شامل متن، صدا، تصویر، فیلم و پویانمایی امر آموزش را بهبود می‌بخشد.

کاربرد رایانه در شهر الکترونیک

شهر الکترونیک شهری است که شهروندان می‌توانند خدمات شهری مورد نیاز خود را به صورت برخط (online) از سرویس‌های دولتی و سازمان‌های بخش خصوصی دریافت کنند. به این ترتیب دیگر نیازی به حرکت فیزیکی شهروندان برای دسترسی به خدمات دولت و نهادهای خصوصی نیست.



شکل ۵- خانه هوشمند

کاربرد رایانه در پزشکی



ج) نمایش علائم حیاتی بیمار به وسیله رایانه



ب) استفاده از رایانه در مواقعی که تشعشعات برای انسان ضرر دارد.



الف) جراحی از راه دور به کمک رایانه

شکل ۶- کاربرد رایانه در پزشکی

«حرکت به سمت صنعتی شدن باید هوشمندانه باشد و گر نه ممکن است به محیط زیست آسیب برساند.»



شکل ۸- Data center های گوگل روی یخ های قطبی فنلاند



شکل ۷- زباله های الکترونیکی

زباله های الکترونیکی (E-Waste)، به دستگاه ها یا قطعات الکترونیکی غیرقابل استفاده، اطلاق می شود. برخی از آنها شامل مواد خطرناک مانند سرب و جیوه هستند (شکل ۷) و برای سلامت انسان و محیط زیست مضرند. این زباله ها بیشتر غیرقابل تجزیه بوده و در محیط زیست باقی می ماندند. امروزه با گسترش استفاده از گوشی های هوشمند، رایانه و تبلت ها توجه به این آلاینده های زیست محیطی افزایش یافته است.

در محیط های اداری و سازمان ها، استفاده از سیستم های نامه نگاری بدون کاغذ (Paperless) به عنوان روشی نوین، به جریان کار سرعت می بخشد و می توان یک نامه را حتی از یک شهر به شهر دیگر به سرعت ارسال کرد و علاوه بر کاهش هزینه ها و افزایش سرعت، از آلوده شدن محیط زیست نیز جلوگیری کرد.

رایانش سبز (Green Computing)

رایانش سبز یکی از راه های کاهش خطرات آلودگی زیستی صنایع است. رایانش سبز یعنی استفاده از رایانه و منابع آن به صورت سازگار با محیط زیست. به این معنی که هم در چرخه تولید، هم زمان استفاده و هم در برخورد با زباله های الکترونیکی تولید شده کمترین آلودگی زیست محیطی ایجاد شود. برای مثال دانشمندان قادر به ساخت ترانزیستوری از نانو الیاف سلولز شده اند که علاوه بر قیمت ارزان و قابل حمل بودن، به راحتی در طبیعت تجزیه شده و با محیط زیست سازگار است. نکته جالب اینکه با رها کردن ترانزیستور در محیط طبیعی، قارچ ها آن را تجزیه کرده و به کودهای امن و قابل استفاده تبدیل می کنند.



شکل ۹- رایانش سبز

در کشور ما نیز چند شرکت در زمینه بازیافت زباله های الکترونیکی فعالیت می کنند. نخستین کارخانه بازیافت الکترونیک کشور در مشهد زباله های الکترونیکی مانند تلفن همراه و رایانه های مستعمل را به پسماندی شامل طلا، مس، قلع و سرب تبدیل می کند و برای مصارف صنعتی به چرخه تولید باز می گرداند.

اجزای رایانه

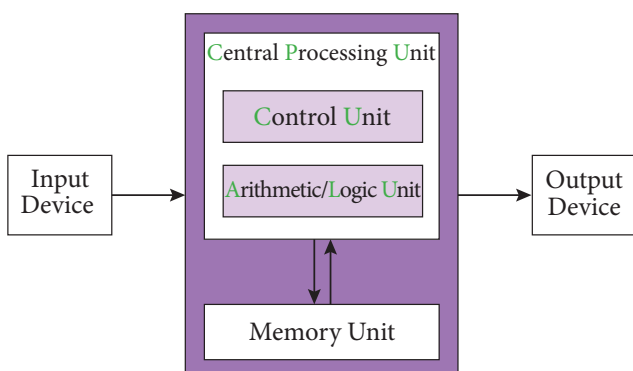


هر رایانه از دو جزء اصلی سخت افزار و نرم افزار تشکیل شده است و متناسب با کاربرد آن، از سخت افزارها و نرم افزارهای متفاوتی استفاده می کند.

سخت افزار: به مجموعه ای از اجزای فیزیکی شامل قطعات الکترونیکی و الکترومکانیکی گفته می شود که یک رایانه را می سازد.

نرم افزار: به مجموعه ای از برنامه ها و داده ها می گویند که تعیین می کنند رایانه چه عملی را انجام دهد.

سخت افزار



به هر قسمت رایانه که فیزیکی و قابل لمس باشد، سخت افزار گفته می شود.

الگوی ساخت تمام رایانه های امروزی معماری فون نویمان است^۱.

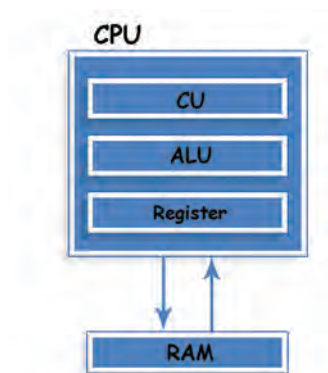
شکل ۱۰- معماری فون نویمان برای سخت افزار رایانه

سخت افزار رایانه شامل چهار واحد اصلی است: پردازش مرکزی - ورودی - خروجی - حافظه

۱- واحد پردازش مرکزی (Central Processing Unit)

ما انسان ها تقریباً همیشه در ذهن خود در حال پردازش هستیم. عمل پردازش به وسیله مغز انجام می شود. رایانه روی داده های ورودی پردازش انجام می دهد و آنها را به واحد خروجی ارسال کرده و واحد خروجی، آن را نمایش می دهد. مغز رایانه واحد پردازشگر مرکزی (CPU) نام دارد.

۱- این معماری برای اولین بار در سال ۱۹۴۵ در گزارشی به قلم ریاضی دان مجارستانی، جان فون نویمان توضیح داده شد.



شکل ۱۱- بخش های اصلی واحد پردازش مرکزی

بخش های اصلی واحد پردازش مرکزی عبارت اند از:
■ واحد محاسبه و منطق (ALU): وظیفه تجزیه و تحلیل و اجرای دستورات را در CPU بر عهده دارد و عملیات ریاضی مانند جمع، تفریق و عملیات منطقی مانند اعمال مقایسه ای را انجام می دهد.

■ واحد کنترل: بر عملکرد واحدهای رایانه نظارت می کند و عمل هماهنگی و هدایت واحدهای رایانه و کنترل جریان انتقال داده ها بین واحدهای رایانه را بر عهده دارد.

■ ثبات (Register): حافظه موقتی که داده های در حال پردازش (CPU) در آن قرار می گیرد. واحد محاسبه و منطق و کنترل با آن در ارتباط هستند.

یکی از شاخص های تعیین سرعت رایانه، سرعت CPU است.

در معماری فون نویمان، CPU به صورت هم زمان یک کار را پردازش می کند (پردازش تک هسته ای). این معماری به تدریج گسترش پیدا کرد و تولیدکنندگان پردازنده به فکر ساخت CPUهایی افتادند که دارای چند قسمت پردازشی باشند تا هر کدام بتوانند نقش یک CPU مستقل را ایفا کرده و یک کار را پردازش کنند (پردازش چند هسته ای).



۲- واحد ورودی

واحد ورودی به آن دسته از سخت افزار رایانه گفته می شود که وظیفه انتقال داده را از سوی کاربر یا حسگر به رایانه دارند.



شکل ۱۲- دستگاه های ورودی

رایانه برای دریافت داده‌ها از واحد ورودی استفاده می‌کند. داده‌ها می‌توانند از نوع صدا، متن، تصویر و... باشند.

۳- واحد خروجی

واحد خروجی به آن دسته از سخت‌افزار رایانه گفته می‌شود که وظیفه انتقال اطلاعات را از رایانه به کاربر یا هر دستگاه دیگری دارند.



شکل ۱۳- چاپ خروجی رایانه روی کاغذ

درگاه (port)

رایانه دارای مجموعه‌ای از درگاه‌ها (ports) برای اتصال رسانه‌های جاشدنی و دستگاه‌های خارجی به رایانه است.



شکل ۱۴- درگاه‌های کیس

درگاه‌های پرکاربرد رایانه

درگاه‌های پرکاربرد رایانه عبارت‌اند از:

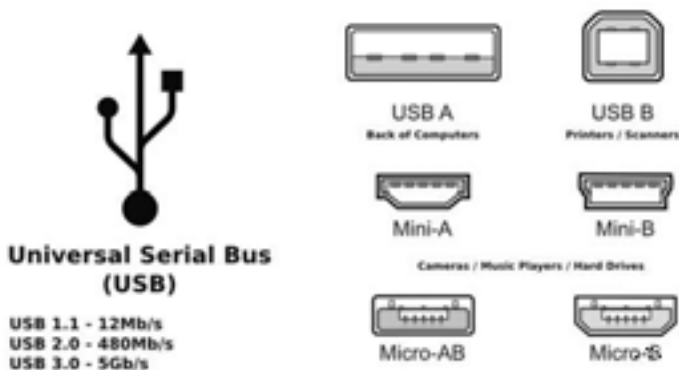
درگاه سریال عمومی (USB): این درگاه داده‌ها را به صورت سریال و با سرعت بسیار بالا انتقال می‌دهد.

دستگاه‌های جانبی متصل به درگاه USB به صورت خودکار حتی در زمان روشن بودن سیستم، تشخیص داده شده، پیکربندی می‌شوند و نیاز به راه‌اندازی مجدد سیستم نیست. به این ویژگی اتصال گرم (hotplug) می‌گویند. نسل‌های USB عبارت‌اند از:

- ۱- **USB 1:** سرعتی حدود ۱۲ Mbit/s (معادل ۱/۵ مگابایت بر ثانیه) داشت.
- ۲- **USB 2:** این درگاه با سرعت بسیار بالاتری نسبت به نسل قبلی خود عرضه شد. سرعتی حدود ۶۰ مگابایت بر ثانیه (معادل ۴۸۰ Mbit/s) دارد.

۳- **USB3:** نسل سوم و آخر که **USB3** نام دارند از سرعت انتقال اطلاعاتی بسیار بالایی برخوردار هستند (تقریباً 5 Gbit/s) که سازگار با نسل USB2.0 هستند و امروزه بیشترین کاربرد را دارند.

انواع درگاه‌های USB :



شکل ۴-۷- انواع درگاه USB

USB-type A: شناخته شده‌ترین درگاه USB نوع A است. تمامی رایانه‌های شخصی مجهز به این درگاه هستند. همچنین تمامی حافظه‌های فلش و وسایل دیجیتالی دیگر نیز قابلیت پشتیبانی و اتصال با رایانه از طریق این درگاه را دارند.



شکل ۴-۸- کانکتور USB-type A

USB-type B: این مدل از درگاه‌ها بیشتر در وسایل جانبی مانند چاپگر و اسکنرها مورد استفاده قرار می‌گیرند.



شکل ۴-۹- کانکتور USB-type B

Mini USB-type A and B: این نوع درگاه‌ها اندازه کوچک‌تری دارند و در وسایل دیجیتالی کوچک‌تر مانند MP3 Playerها و برخی از تلفن‌های همراه مورد استفاده قرار می‌گیرند. این نوع درگاه به دو مدل Mini A و Mini B تقسیم‌بندی می‌شوند.



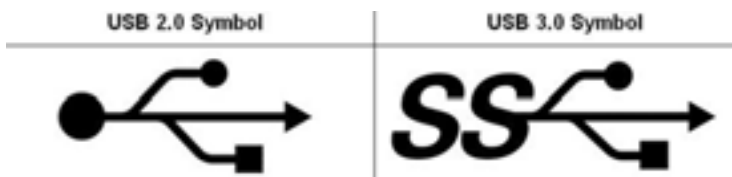
شکل ۴-۱۰- کانکتور Mini USB-type A,B

Micro USB-type A and B: آخرین نوع USBها Micro نام دارد. و از نظر اندازه کوچک‌ترین مدل در USBها است. Microها مانند نوع Mini، دارای دو مدل Micro A و Micro B هستند که امروزه این نوع درگاه‌ها به دلیل ساختار کم‌حجم و اندازه‌ی کوچک بیشترین کاربرد را در تلفن‌های همراه دارند.

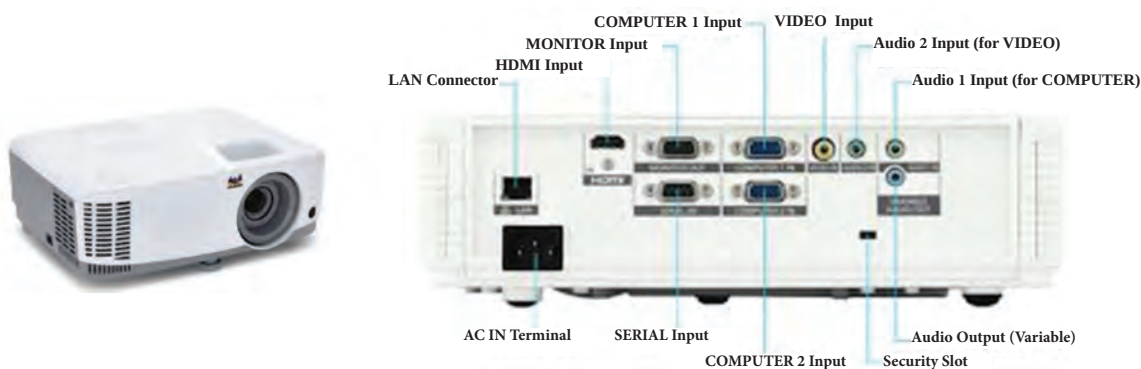


شکل ۴-۱۱- کانکتور Micro USB-type B

این درگاه پرکاربردترین درگاه در میان استفاده‌کنندگان تجهیزات رایانه‌ای است.



شکل ۴-۱۲- نماد درگاه USB



شکل ۱۵- درگاه‌های ویدئو پروژکتور



شکل ۱۶- دانگل ماوس

دانگل (Dongle) یک قطعه سخت‌افزاری است که به رایانه متصل می‌شود تا بعضی نرم‌افزارهای خاص بتوانند با ضریب امنیت بالاتر اجرا شوند (شکل ۱۶). نوعی از آنها با اتصال به درگاه USB می‌توانند دستگاه‌های مختلف مانند ماوس و صفحه‌کلید و... را به صورت بی‌سیم به رایانه متصل کنند.

برخی از دستگاه‌های جانبی رایانه، قابلیت اتصال و اجرا (plug & play) دارند؛ بدین معنی که سخت‌افزار پس از اولین اتصال به رایانه به صورت خودکار و بدون انجام تنظیمات توسط کاربر شناسایی می‌شود. بیشتر سیستم‌عامل‌های جدید با فناوری plug & play سازگاری دارند و می‌توانند سخت‌افزار جدید را شناسایی و در صورت نیاز به صورت خودکار نصب کنند. سخت‌افزارهایی از جمله ماوس، صفحه‌کلید و دیسک‌های سخت SATA این قابلیت را دارند. برخی سخت‌افزارها برای اینکه بتوانند وظایف خود را درست انجام دهند نیاز به یکسری دستورات و استانداردهای قابل فهم برای رایانه دارند که به صورت یک پرونده نصبی روی سیستم نصب می‌شوند و به آن راه‌انداز (driver) می‌گویند.

تقریباً تمامی وسایلی که دارای حافظه فلش هستند، برای ارتباط با رایانه از رابط اتصال گرم (Hot plugging) استفاده می‌کنند. اتصال گرم به این معناست که کاربر می‌تواند وسیله دارای حافظه فلش را هنگام روشن بودن رایانه به آن متصل کند و نیاز نیست رایانه را خاموش کرده یا راه‌اندازی مجدد کند. یکی از معمول‌ترین درگاه‌های اتصال گرم، درگاه USB است.

۴- واحد حافظه



شکل ۱۷- داده ورودی از چشم دریافت می‌شود. بعد از پردازش انجام شده توسط مغز، خروجی چه خواهد بود؟

به این تصویر نگاه کنید. اولین نکته‌ای که به ذهن شما می‌رسد چیست؟ جریانی که اتفاق می‌افتد مربوط به مرور حافظه است. در حافظه ما این تصویر به نام حافظ نقش بسته است. در واقع تصویر آرامگاه، به وسیله چشم دریافت و به مغز ارسال می‌شود. مغز شما این جریان دریافت داده را پردازش می‌کند و برای بیان واژه آرامگاه حافظ شیرین سخن، از حافظه کمک می‌گیرد و آن را بیان می‌کند.

رایانه هم مانند انسان حافظه دارد. همان‌طور که ما به حافظه اکتفا نمی‌کنیم و اطلاعات ضروری مثل شماره تلفن، نشانی و موارد مشابه را با کمک ابزارهای گوناگون مانند کاغذ، نوار ضبط صوت و... به صورت دائمی نگهداری می‌کنیم؛ رایانه هم می‌تواند برای ثبت و نگهداری اطلاعات از انواع حافظه استفاده کند.

رایانه دو نوع حافظه دارد: حافظه اصلی و حافظه کمکی

حافظه اصلی: حافظه‌ای است که در صورت عدم وجود آن به هیچ عنوان نمی‌توان از رایانه استفاده کرد. اگر رایانه حافظه اصلی نداشته باشد شما هیچ تصویری را پس از روشن کردن رایانه، روی صفحه نمایش نخواهید دید.

انواع حافظه اصلی

Random Access Memory

RAM
(رم)

این حافظه تا زمانی که رایانه روشن است حاوی اطلاعات بوده و به محض خاموش شدن رایانه اطلاعات آن از بین می‌رود؛ به آن حافظه **موقت، نامانا یا فرار** نیز می‌گویند.

برنامه‌ها، دستورالعمل‌ها و داده‌هایی در این حافظه قرار می‌گیرند که پردازشگر بخواهد بر روی آنها کاری انجام دهد.

پردازنده می‌تواند هم در این حافظه بنویسد و هم از آن بخواند به همین دلیل حافظه خواندنی-نوشتنی یا RWM (Read-Write Memory) نیز نامیده می‌شود.

Laptop



Desktop



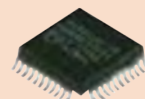
Read Only Memory

ROM
(رام)

هنگام خاموش شدن رایانه اطلاعات این نوع حافظه از بین نمی‌رود و اطلاعات آن **مانا** است.

اطلاعات داخل این حافظه به وسیله کارخانه سازنده برد اصلی (Mainboard) نوشته می‌شود و برنامه‌های داخل آن به محض روشن شدن رایانه اجرا می‌شوند. در این حافظه‌ها، تنظیمات ساختاری سخت‌افزار رایانه و همچنین چگونگی آزمایش و راه‌اندازی قسمت‌های گوناگون قرار داده می‌شود.

اطلاعات این حافظه فقط خواندنی است و پردازنده قادر به تغییر اطلاعات این نوع حافظه نیست؛ و فقط می‌تواند اطلاعات آن را بخواند.

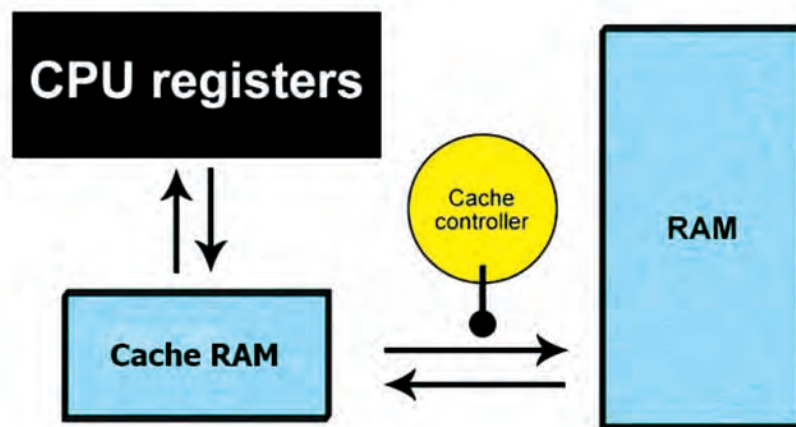


حافظه نهان

حافظه‌ای میان RAM و پردازنده است و اطلاعات مورد نیاز پردازنده را به صورت موقت در خود جای می‌دهد تا پردازنده بتواند به سرعت به آنها دسترسی داشته باشد.

ثبات

حافظه‌ای سریع درون پردازنده است که برای سرعت بخشیدن به اجرای برنامه‌ها به کار می‌رود.



شکل ۱۸- ارتباط حافظه نهان و ثبات با RAM

حافظه جانبی

در انواع مختلف، حافظه اصلی جایی برای ذخیره دائمی اطلاعات کاربر وجود ندارد؛ بنابراین به حافظه دیگری برای نگهداری اطلاعات کاربر یا ذخیره دائمی اطلاعات و همچنین نصب نرم‌افزارهای دلخواه، نیاز است که به آن حافظه جانبی می‌گویند.

امروزه از انواع حافظه‌های جانبی مانند Flash Disk, SD Card, SSD, CD, DVD, Blu-Ray و... استفاده می‌شود.



اندازه گیری حافظه



شکل ۱۹- پیام عدم وجود فضای کافی در حافظه

حافظه های الکترونیکی از سلول هایی تشکیل شده است که محتوای آنها معادل صفر یا یک است. اصطلاحاً به هر سلول حافظه بیت می گویند. بیت کوچک ترین جزء حافظه است. برای ذخیره کردن حروف و اعداد از واحدی به نام بایت استفاده می شود که هر بایت از ۸ بیت مجاور هم به دست می آید.

مثلاً حرف A در حافظه رایانه در ۸ بیت کنار هم و به صورت زیر ذخیره می شود:

۰	۱	۰	۰	۰	۰	۰	۱
---	---	---	---	---	---	---	---

جدول زیر واحدهای بزرگ تر از بایت را نشان می دهد.

واحد	نماد	پیشوند	معادل	بایت به توان ۲	اندازه به بایت
کیلوبایت	KB	Kilo	۱۰۲۴B	۲ ^{۱۰}	۱۰۲۴
مگابایت	MB	Mega	۱۰۲۴KB	۲ ^{۲۰}	۱۰۲۴*۱۰۲۴
گیگابایت	GB	Giga	۱۰۲۴MB	۲ ^{۳۰}	۱۰۲۴*۱۰۲۴*۱۰۲۴
ترابایت	TB	Terra	۱۰۲۴GB	۲ ^{۴۰}	۱۰۲۴*۱۰۲۴*۱۰۲۴*۱۰۲۴

برای تبدیل هر واحد به واحد بزرگ تر، آن عدد را بر ۱۰۲۴ یا ۲^{۱۰} تقسیم می کنیم و برای تبدیل هر واحد به واحد کوچک تر آن عدد را در ۱۰۲۴ یا ۲^{۱۰} ضرب می کنیم.

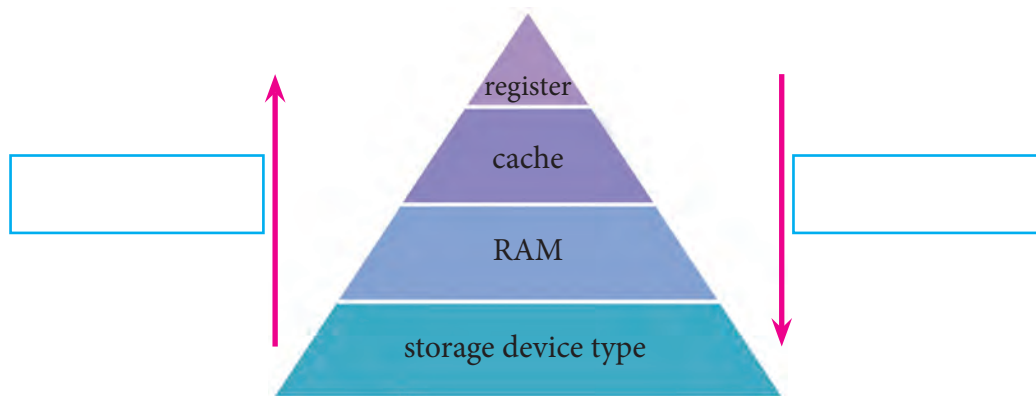
برای مثال در تبدیل ۴ ترابایت به کیلوبایت، عدد ۴ را سه بار در ۱۰۲۴ ضرب می کنیم. چون کیلوبایت سه واحد کوچک تر از ترابایت است؛ بنابراین

$$4 \text{ TB} = 4 \times 1024 \times 1024 \times 1024 = 4 \times 2^{30}$$

مقایسه انواع حافظه

حافظه اصلی رایانه از جنس نیمه‌رسانا (الکترونیکی) است و در نتیجه، سرعت دسترسی به اطلاعات موجود در آنها در مقایسه با انواع حافظه جانبی مانند دیسک سخت، لوح فشرده و فلش بالاتر است، اما حافظه‌هایی مانند ثبات و حافظه نهان که به پردازنده نزدیک‌تر هستند، گران‌تر بوده و از ظرفیت کمتری برخوردارند و از سرعت دسترسی بالاتری بهره می‌برند.

در شکل ۲۰ با توجه به جهت فلش‌ها که کم به زیاد را نمایش می‌دهد، فلش سرعت و ظرفیت را مشخص کنید.



شکل ۲۰- هرم حافظه

دسته‌بندی رایانه‌ها

از لحاظ قدرت پردازش، بزرگی و سرعت، رایانه‌ها به چهار دسته تقسیم می‌شوند؛ که به ترتیب، اندازه، سرعت، قیمت و تعداد پردازنده‌ها و تعداد کاربرانی که می‌توانند هم‌زمان از رایانه استفاده کنند کاهش می‌یابد.

■ **ابر رایانه (Super computer):** ابر رایانه‌ها، رایانه‌های بسیار بزرگی هستند که حافظه و قدرت پردازش فوق‌العاده زیادی دارند و در امور فضایی، دفاعی، هواشناسی و پروژه‌های بسیار بزرگ علمی و تحقیقاتی استفاده می‌شوند. اولین ابر رایانه ایران در سال ۱۳۸۰ به‌وسیله محققان مرکز تحقیقات پردازش‌های فوق سریع دانشگاه صنعتی امیرکبیر به بهره‌برداری رسید.



شکل ۲۲- آخرین ابررایانه ساخت ایران که جزء ۵۰۰ ابررایانه برتر دنیا قرار گرفته است.



شکل ۲۱- یک ابر رایانه سریع

■ **رایانه‌های بزرگ (Mainframe computer):** در مراکز تجاری بزرگ، دانشگاه‌ها و برخی مراکز دولتی که حجم محاسباتی بسیار زیادی دارند استفاده می‌شوند. این رایانه‌ها مانند ابر رایانه‌ها می‌توانند به رایانه‌های دیگر سرویس دهند.



شکل ۲۴- رایانه بزرگ قدیمی



شکل ۲۳- رایانه بزرگ جدید

■ **رایانه کوچک (Minicomputer):** در مراکز تجاری، دانشگاهی و برخی مراکز دولتی که حجم محاسباتی متوسط دارند استفاده می‌شوند. نام جدید این دسته از رایانه‌ها، رایانه‌های میانه (Midrange) است.



شکل ۲۵- رایانه کوچک

■ **رایانه ریز (Microcomputer):** رایانه‌هایی که فقط یک یا دو پردازنده دارند و به دو صورت قابل حمل (portable) و غیرقابل حمل هستند.

انواع ریز رایانه



شکل ۲۶- رایانه رومیزی

ریز رایانه‌ها از لحاظ ظاهر، اندازه و قدرت پردازشی به چند دسته تقسیم می‌شوند. بعضی از انواع آن را در ادامه بررسی می‌کنیم:

■ **رایانه‌های رومیزی (Desktop):** برای کار در یک محل ثابت و بر روی میز طراحی شده و از برق شهری استفاده می‌کنند. به آنها PC (Personal Computer) هم گفته می‌شود.



شکل ۲۷- Thin client



شکل ۲۸- رایانه کیفی

■ **تین کلاینت (Thin client):** تولیدکنندگان برای اینکه بتوانند محصولات کوچک‌تری عرضه کنند، برخی از سخت‌افزارهای یک رایانه معمولی مانند خنک‌کننده پردازنده، دیسک گردان لوح فشرده و... را تغییر داده یا حذف کردند. مصرف برق پایین، اندازه کوچک، قیمت ارزان‌تر از جمله مزایای تین کلاینت است.

■ **رایانه‌های کیفی (Laptop):** از لحاظ امکانات و نوع کار مثل رایانه‌های رومیزی هستند؛ ولی با باتری هم کار می‌کنند. این رایانه‌ها قابل حمل هستند. رایانه‌های کیفی به‌طور کلی دارای همان اجزایی هستند که در یک رایانه رومیزی وجود دارد با این تفاوت که تا حد ممکن از وزن و اندازه آنها کاسته شده است. رایانه‌های کیفی دارای یک صفحه‌کلید سرخود هستند و به جای ماوس از یک صفحه لمسی استفاده می‌کنند اما می‌توان صفحه‌کلید و ماوس جداگانه نیز به آنها وصل کرد.



شکل ۲۹- تلفن هوشمند

■ **تلفن‌های هوشمند (Smartphone):** با استفاده از گوشی‌های هوشمند علاوه بر برقراری تماس تلفنی امکان دسترسی به اینترنت، سازمان‌دهی اطلاعات تماس، ارسال نامه‌های الکترونیکی و پیام‌های متنی و بازی، و گرفتن عکس نیز وجود دارد.



شکل ۳۰- تبلت

■ **تبلت یا لوح رایانه (Tablet PC):** لوح رایانه ترکیبی از یک لپ‌تاپ و یک تلفن همراه است. تبلت از یک تلفن همراه، بزرگ‌تر است و به جای صفحه‌کلید از یک صفحه نمایش لمسی بهره می‌گیرد.



شکل ۳۱- عینک گوگل

■ **رایانه‌های پوشیدنی (Wearable computers):** رایانه‌هایی هستند که افراد آن را می‌پوشند و بدون کمک از دست به راحتی از آن استفاده می‌کنند. این رایانه‌ها کاربردهای مختلفی دارند. ساعت هوشمند، کلاه هوشمند نمونه‌هایی از این رایانه‌ها هستند.



شکل ۳۲- برد ماشین لباس‌شویی

■ **رایانه‌های نهفته یا توکار (Embedded):** رایانه‌های نهفته، امروزه برای کنترل بسیاری از دستگاه‌ها به کار می‌روند. مشخصه کلیدی این رایانه‌ها، طراحی اختصاصی برای انجام یک کار مشخص است و مهندسين طراح می‌توانند محصول را برای کاهش اندازه و قیمت، بهینه کنند.

امروزه استفاده همه‌گیر از ابزارهای سیار (Mobile Device) مانند لپ‌تاپ، تبلت، تلفن‌های همراه و... سبب شده که فناوری‌های جدیدتر و همراه با این ابزارها جهت ارتباط با محیط بیرون پدید آیند. استفاده از ارتباطات بی‌سیم و رادیویی، سامانه شناسایی با استفاده از فرکانس رادیویی، بارکد و کدهای دوبعدی و... فناوری‌هایی هستند که طی آن تجهیزات سخت‌افزاری یا نرم‌افزاری قادر به خواندن، دریافت، تشخیص یا نگهداری داده‌ها به‌طور خودکار هستند.

هر یک از تصاویر زیر چه کاربردی را نشان می‌دهند؟



برای دیدن فیلم علاوه بر تجهیزات سخت افزاری مانند صفحه نمایش و بلندگو، به برنامه‌ای نیاز است تا فیلم را پخش کند. به این برنامه نرم افزار گفته می‌شود. کاربر از طریق نرم افزار با رایانه ارتباط برقرار می‌کند. برای انجام هر کاری در رایانه، برنامه یا نرم افزار مخصوص به آن نیاز است.

نرم افزار مجموعه‌ای از داده‌ها و برنامه‌ها است که کنترل و هماهنگی فعالیت‌های سخت افزاری رایانه و پردازش را بر عهده دارد.

نرم افزارها به دو دسته تقسیم می‌شوند:



نرم افزار کاربردی

زمان پخش فیلم، کشیدن نقشه و یا رسم یک تصویر از نرم افزارهای خاص استفاده می‌کنیم که برای انجام وظایف خاص، بر اساس نیاز کاربران، طراحی و تولید شده‌اند و به آنها نرم افزار کاربردی می‌گویند.



نرم افزار QR Reader



شکل ۳۳- کد QR

کدهای QR راهی سریع برای دسترسی به محتوا از طریق گوشی‌های هوشمند است؛ این برنامه‌ها به کاربر اجازه می‌دهد با پویش (Scan) کد مورد نظر و تبدیل آن به اطلاعات معنی‌دار، به تحلیل محتوای رمزنگاری شده بپردازد. برای نمونه می‌توانید کد زیر را پویش کرده و به اطلاعات موجود در آن، که نشانی اینترنتی تارنمای دفتر چاپ است، دسترسی پیدا کنید.



شکل ۳۴- کد QR تارنمای اداره کل نظارت بر نشر و توزیع مواد آموزشی

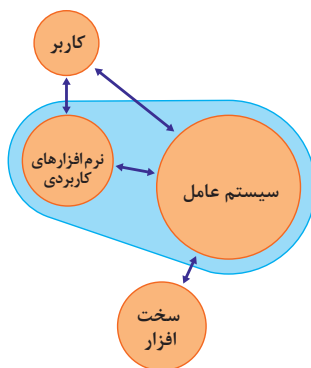
کدهای QR فاقد هرگونه اجزای الکتریکی بوده و نیاز به فناوری سخت‌افزاری خاصی ندارند. کدهای QR تنها نوعی از کدهای سیاه و سفید است که روی کاغذ چاپ‌شده و می‌توان آن را به کمک گوشی‌های هوشمند پویش و رمزگشایی کرد.

نرم‌افزار سیستمی

نرم‌افزارهای سیستمی مدیریت رایانه را بر عهده دارند و واسطی بین کاربر و سخت‌افزار یا ماشین هستند. نرم‌افزار سیستمی خدماتی را فراهم می‌کند که دیگر نرم‌افزارها می‌توانند برای انجام کارهای خود از آن استفاده کنند.

برنامه‌های راه‌انداز سیستم: اولین برنامه‌هایی که با روشن شدن رایانه روی سخت‌افزار اجرا می‌شوند تا رایانه را برای اجرای عملیات آماده کنند و عبارت‌اند از:

- **برنامه عیب‌یاب (post):** قسمت‌های اصلی رایانه شامل حافظه و پردازشگر مرکزی را آزمایش می‌کند و اگر اشکالی در این قسمت‌ها باشد به‌وسیله این برنامه اطلاع داده می‌شود.
- **برنامه شناسایی دستگاه‌های ورودی و خروجی (BIOS):** شناسایی و راه‌اندازی دستگاه‌های ورودی و خروجی بر عهده این برنامه است.
- **بارگذاری سیستم‌عامل (loader):** بخش‌های اصلی سیستم‌عامل به‌وسیله این برنامه به حافظه اصلی منتقل می‌شود و تا رایانه روشن است در حافظه باقی می‌ماند.



سیستم‌عامل‌ها: مهم‌ترین نرم‌افزار سیستمی که بقیه نرم‌افزارها به‌وسیله آن مدیریت می‌شوند، سیستم‌عامل نام دارد. سیستم‌عامل مجموعه‌ای از برنامه‌ها است که برای مدیریت و کنترل عملیات رایانه مورد استفاده قرار می‌گیرد و به عنوان واسطی بین کاربر و سخت‌افزار عمل می‌کند. دستورهای کاربر برای اجرا در رایانه به سیستم‌عامل اعلام می‌شوند و نتایج حاصل از اجرای دستورها به‌وسیله سیستم‌عامل به اطلاع کاربر می‌رسد (شکل ۳۵).

انواع مختلفی از سیستم‌عامل به وسیله شرکت‌های مختلف تولید می‌شوند. Dos، Windows، Unix، Linux و Macintosh نمونه‌ای از سیستم‌عامل‌های رایانه‌های شخصی هستند.

شکل ۳۵- ارتباط سیستم‌عامل با کاربر، سخت‌افزار و نرم‌افزارهای کاربردی

مترجم‌ها: برای اینکه بتوانیم به رایانه دستورات قابل فهم بدهیم تا اجرا کند باید از زبان ماشین استفاده کنیم که یادگیری آن برای انسان سخت و پیچیده است. به همین دلیل زبان‌هایی قابل فهم برای انسان اختراع شدند که به زبان محاوره‌ای نزدیک هستند. برای تبدیل این زبان‌ها به زبان ماشین مترجم‌ها به وجود آمدند.

مترجم نرم‌افزار سیستمی است که برنامه نوشته‌شده با یک زبان برنامه‌نویسی را به زبان قابل فهم برای ماشین تبدیل می‌کند.

برنامه‌های کمکی: برنامه‌های کمکی برای مدیریت سیستم به کاربر کمک کرده و استفاده از رایانه را ساده‌تر می‌کنند. نرم‌افزارهای امنیتی و مدیریت حافظه نمونه‌هایی از برنامه‌های کمکی هستند.



مونتاز رایانه

آشنایی با قطعات سخت‌افزاری و انتخاب و نصب قطعات رایانه از مهارت‌های کاربردی در یادگیری علوم رایانه است. مشخصات اصلی قطعات در انتخاب آنها بسیار تأثیرگذار بوده، در کارایی و سرعت سیستم نقش اساسی دارد. در بسیاری از مواقع بهترین نرم‌افزارها به علت نبود سخت‌افزار مناسب یا سازگار نبودن اجزای سخت‌افزاری ناکارآمد خواهند بود؛ بنابراین در انتخاب قطعات علاوه بر مشخصات قطعه باید به سازگاری آن با قطعات دیگر رایانه هم توجه شود. برای خرید یا ارتقای رایانه توجه به نیاز کاربر و میزان بودجه او در انتخاب قطعات بسیار مهم است و بی‌توجهی به نیاز کاربر سبب هدر رفتن هزینه خواهد شد.

شناسایی و انتخاب قطعات رایانه رومیزی

سرهم کردن و وصل کردن قطعات پیش ساخته را مونتاژ می گویند. برای مونتاژ رایانه، شناسایی و انتخاب قطعات بسیار ضروری است.

کاربرد کیس در رایانه های رومیزی

تصور کنید قطعات تشکیل دهنده یک رایانه روی یک میز به یکدیگر متصل شده اند (شکل ۱). هنگام استفاده از این رایانه چه مشکلاتی پیش خواهد آمد؟



شکل ۱- رایانه بدون کیس

از زمان تولید اولین رایانه های رومیزی، اجزای تشکیل دهنده رایانه را درون جعبه ای فلزی جاسازی می کردند. یک جعبه که در عین زیبایی بتواند تمامی مشکلات بالا را رفع کند. نام این جعبه کیس (Case) است. جنس بدنه کیس ها معمولاً از آلایژی فلزی ساخته می شود. این آلیاژ سبک و ضد زنگ بوده، با لایه ای از رنگ پوشیده شده است و از قطعات در مقابل تشعشعات الکترومغناطیسی محافظت می کند و به تهویه داخل کیس کمک می کند.

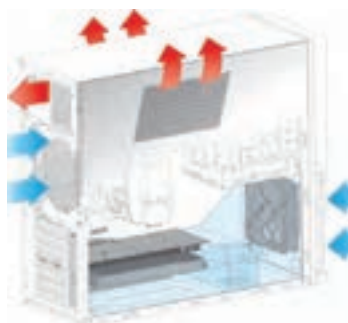
انواع کیس

با توجه به نوع کاربرد، انواع مختلفی از کیس ها وجود دارند که هر کدام در اندازه های مختلف طراحی و ساخته می شوند (شکل ۲).

به طور کلی کیس ها به دو دسته ایستاده (Tower) و رومیزی (Desktop) تقسیم می شوند. کیس های ایستاده در اندازه متوسط (Middle Tower) از متداول ترین کیس ها هستند. این کیس ها برای کاربردهای اداری و خانگی استفاده می شوند. در جاهایی که کمبود فضا وجود دارد، استفاده از کیس های رومیزی توصیه می شود.



شکل ۲- انواع کیس



شکل ۳- تهویه کیس به وسیله فن ها

اجزای کیس عبارت‌اند از:

- پوشش کیس (Cover)
- شاسی (Chassis)
- پنل جلو (Front Panel)

۱ شاسی کیس

به اسکلت اصلی کیس که قطعات به آن متصل می‌شوند، شاسی گفته می‌شود. در شاسی، بخش‌هایی برای نصب اجزای سیستم با اندازه استاندارد در نظر گرفته شده است (شکل ۴).

۲ کابل برق رایانه را جدا کرده، پوشش کیس را باز کنید.

پوشش کیس برای حفاظت از قطعات داخلی در برابر صدمات فیزیکی و تشعشعات به کار می‌رود و در بیشتر کیس‌ها به صورت درهایی در طرفین کیس است (شکل ۵).



شکل ۴- شاسی کیس



شکل ۵- پوشش کیس

۳ بخش‌های مختلف پنل جلویی کیس

قسمت جلوی کیس‌ها دارای طرح‌ها و شکل‌های مختلفی است و هر کدام زیبایی خاص خود را دارند. کاربران با توجه به رنگ و طرح مورد علاقه خود کیس را انتخاب می‌کنند. پنل کیس دریچه‌هایی برای دسترسی به درایوهای نوری دارد. علاوه بر این دریچه‌ها، پنل دارای کلید فشاری خاموش و روشن (Power Button)، کلید فشاری راه‌اندازی مجدد (Reset Button)، دو عدد دیود نوری (LED) برای نمایش وضعیت روشن بودن سیستم (Power LED) و نمایش عملکرد دیسک سخت (HDD LED)، درگاه‌های USB، درگاه‌های میکروفن و هدفن است که هر یک به وسیله کانکتورهای مخصوص به برد اصلی متصل می‌شوند (شکل ۶). پنل جلوی برخی از کیس‌ها دارای یک صفحه نمایش کوچک برای نمایش سرعت چرخش فن پردازنده، دمای داخل کیس، دمای پردازنده و تاریخ و ساعت است (شکل ۷).



شکل ۶- پنل جلوی کیس



شکل ۷- پنل جلوی کیس



شکل ۸ - برد اصلی با فرم فاکتور ATX

برد اصلی در اندازه‌های مختلفی طراحی و ساخته می‌شود و در هر طرح چیدمان اجزا متفاوت است. به شکل، اندازه و چیدمان اجزای برد اصلی، فرم فاکتور (FormFactor) می‌گویند. امروزه بیشتر رایانه‌ها دارای فرم فاکتور ATX هستند (شکل ۸). برد اصلی قطعه‌ای است که تمامی قطعات دیگر، روی آن نصب شده و یا به وسیله کابل به آن متصل می‌شوند. ارتباط بین قطعات از طریق برد اصلی صورت می‌گیرد. اجزای مهم برد اصلی عبارت‌اند از:

- سوکت پردازنده (CPU socket)
- شکاف‌های توسعه (Expansion slots)
- کانکتورها (Connectors)
- گذرگاه‌ها (BUS)
- جامپر (Jumper)
- بانک‌های حافظه (Memory slots)
- درگاه‌های ورودی و خروجی (port)
- مجموعه تراشه‌ها (Chipset)
- قطعات سرخود (Onboard)



شکل ۹ - سوکت پردازنده

محل نصب پردازنده روی برد اصلی را سوکت پردازنده می‌گویند که ارتباط پردازنده را با برد اصلی برقرار می‌کند.



شکل ۱۰ - بانک حافظه

در برد اصلی محل‌هایی برای نصب حافظه اصلی تعبیه شده است، که به آن بانک حافظه می‌گویند (شکل ۱۰). در راهنمای برد اصلی، در جدول مشخصات (Specifications)، ردیف Memory، نوع و تعداد بانک‌های حافظه مشخص شده است. تعداد این بانک‌ها یکی از معیارهای انتخاب برد اصلی است. امروزه بیشتر بانک‌های حافظه از نوع DIMM هستند.



شکل ۱۱ - شکاف توسعه

برای توسعه سخت‌افزاری سیستم، شکاف‌هایی روی برد اصلی در نظر گرفته شده است تا بردهای سخت‌افزاری مانند کارت گرافیک، کارت شبکه، کارت TV و در آن قرار گیرد. شکاف‌های توسعه انواع مختلفی دارند. دو نوع رایج آن PCI-E و PCI است (شکل ۱۱). تعداد و نوع شکاف‌های توسعه در راهنمای برد اصلی و در جدول مشخصات، ردیف Expansion slots آمده است که از معیارهای تأثیرگذار در انتخاب برد اصلی است.

به قطعاتی که در شکاف‌های توسعه نصب می‌شوند قطعات داخلی (Internal) می‌گویند.

برای اتصال دستگاه‌های خارج از کیس به برد اصلی رایانه، درگاه‌هایی طراحی شده است که به آنها درگاه‌های ورودی و خروجی می‌گویند (شکل ۱۲). تعداد و نوع درگاه‌های ورودی و خروجی در راهنمای برد اصلی، جدول مشخصات، ردیف Rear panel ports آمده است. درگاه‌هایی مانند USB, PS/2, LAN نمونه‌ای از این درگاه‌ها هستند.



شکل ۱۲- درگاه‌های برد اصلی

کانکتورها، ارتباط برد اصلی با اجزای داخلی کیس را برقرار می‌کنند. در دفترچه راهنمای برد اصلی، مشخصات این کانکتورها در بخش Internal Connectors آمده است. برخی از این کانکتورها عبارت‌اند از:

- کانکتور پنل سیستم
- کانکتور درگاه USB
- کانکتور SATA
- کانکتور تغذیه برد اصلی
- کانکتور صدا



شکل ۱۳- مجموعه تراشه

تراشه یا مدار مجتمع (Integrated Circuit)، ارتباط و کنترل اجزای داخلی رایانه را برقرار می‌کند. برای کنترل بهتر و کوچک کردن ابعاد برد اصلی، برخی از تراشه‌ها را با هم در یک مجموعه قرار می‌دهند که به آن مجموعه تراشه می‌گویند (شکل ۱۳). قیمت، توانایی و قابلیت‌ها برد اصلی به وسیله مجموعه تراشه‌های

آن مشخص می‌شود. نام مجموعه تراشه برد اصلی در جدول مشخصات راهنما برد اصلی، ردیف Chipset آمده است. ROMBIOS یکی از تراشه‌های روی برد اصلی است که یکی از محتویات آن BIOS است و عملکرد رایانه را کنترل می‌کند. سیستم رایانه قادر به پشتیبانی از سخت‌افزارهایی است که در BIOS مشخص شده است. محتویات تراشه ROMBIOS به وسیله سازنده برد اصلی یا به سفارش سازنده نوشته می‌شود.

گذرگاه‌ها مسیرهایی برای تبادل داده بین دو یا چند قطعه هستند. به گذرگاهی که اجزای بسیار سریع سیستم مانند پردازنده و حافظه را به هم وصل می‌کند، گذرگاه سیستم می‌گویند. گذرگاه‌ها روی برد اصلی به صورت دسته‌ای از خطوط، قابل مشاهده هستند.

به هر قطعه‌ای که روی برد اصلی در زمان طراحی تعبیه شده باشد، قطعه سرخود (onboard) می‌گویند. برخی بردها علاوه بر شکاف‌های توسعه برای کارت‌هایی مانند گرافیک، صدا و یا شبکه دارای کارت‌های سرخود هستند.



شکل ۱۴ - جامپر Clear CMOS

جامپرهای پین‌های فلزی ۲ و ۳ و یا چندپایه روی برد اصلی هستند که برای انجام تنظیمات سخت‌افزاری به کار می‌روند. جامپر Clear CMOS برای پاک کردن تنظیمات انجام شده در BIOS استفاده می‌شود (شکل ۱۴).

پردازنده مهم‌ترین بخش سخت‌افزاری هر سیستم رایانه‌ای است که دستورات نرم‌افزاری را اجرا می‌کند و نتایج به دست آمده را در حافظه‌ها ذخیره کرده، یا به دستگاه‌های خروجی می‌فرستد. مشخصات اصلی پردازنده عبارت‌اند از:

- فرکانس کاری
- تعداد هسته‌ها (Core)
- میزان حافظه نهان (Cache)
- توان مصرفی

مشخصات پردازنده سیستم

با استفاده از سربرگ Performance برنامه Task Manager ویندوز، مشخصات پردازنده سیستم را مشاهده کنید

فرکانس کاری پردازنده

به تعداد دفعات انجام یک عمل در واحد زمان (یک ثانیه) فرکانس می‌گویند. با افزایش فرکانس، سرعت افزایش می‌یابد. سرعت پردازنده از فرکانس کاری آن مشخص می‌شود. واحد این مشخصه هرتز (Hz) است.

تعداد هسته‌ها

هر پردازنده دارای واحد پردازش است. به تعداد واحدهای پردازش واقعی هر پردازنده، هسته می‌گویند که خواندن و اجرای دستورات یک برنامه را انجام می‌دهد. برای افزایش کارایی و عملکرد بهینه پردازنده‌ها تعداد هسته‌های آنها را افزایش می‌دهند و به آنها پردازنده‌های چند هسته‌ای می‌گویند.

میزان حافظه نهان

حافظه نهان، حافظه‌ای است که با نگهداری اطلاعات و دستورالعمل‌هایی که اخیراً مورد استفاده پردازنده قرار گرفته است، مراجعات پردازنده به حافظه اصلی را کاهش می‌دهد و باعث افزایش کارایی و سرعت سیستم می‌شود. این حافظه‌ها درون پردازنده قرار دارند و از نظر ظرفیت و سرعت دارای سه سطح L1, L2, L3 هستند. به ترتیب از L1 به L2 و L3 سرعت کاهش و ظرفیت افزایش می‌یابد.

حافظه نهان

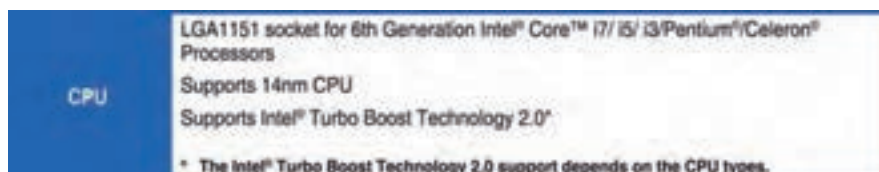
حافظه نهان در پردازنده قرار دارد. هدف اصلی حافظه نهان، کم کردن تعداد مراجعه به حافظه اصلی و در نتیجه افزایش سرعت پردازش است. حافظه نهان، میان حافظه اصلی و ثبات‌های پردازنده قرار دارد و داده‌های موردنظر پردازنده را در اختیار ثبات‌ها قرار می‌دهد و محتویات آن شامل بخشی از داده‌های حافظه اصلی است. چندین نکته مهم در رابطه با حافظه نهان وجود دارد:

- (۱) فناوری حافظه نهان، استفاده از حافظه‌های سریع ولی با ظرفیت کوچک است که به منظور افزایش سرعت انتقال داده استفاده می‌شود.
 - (۲) زمانی که از حافظه نهان استفاده می‌شود، برای دسترسی به داده‌ها ابتدا باید محتویات این حافظه موردبررسی قرار گیرد. در صورت موفقیت، این فرایند را Cache hit می‌گویند. در صورتی که اطلاعات موردنظر در حافظه نهان موجود نباشند (Cache miss)، پردازنده باید در انتظار تأمین داده‌های خود از حافظه اصلی سیستم باشد.
 - (۳) اندازه حافظه نهان محدود بوده، سعی می‌شود که ظرفیت این حافظه در بالاترین مقدار خود باشد، باین وجود اندازه آن نسبت به سایر ابزار ذخیره‌سازی بسیار کم است.
 - (۴) این امکان وجود خواهد داشت که از چندین لایه حافظه نهان استفاده شود.
- در بسیاری از پردازنده‌ها که اغلب برای سرورها استفاده می‌شوند حتی سطح سوم حافظه نهان نیز به کار برده می‌شود.

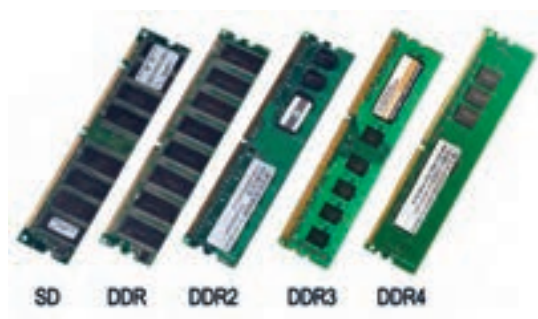
توان مصرفی

میزان مصرف انرژی الکتریکی هر پردازنده را توان مصرفی پردازنده می‌گویند و اندازه آن بر حسب وات ساعت (Wh) بیان می‌شود.

از آنجا که هر برد اصلی فقط دارای یک نوع سوکت پردازنده است، امکان نصب هر نوع پردازنده‌ای روی آن وجود ندارد. در جدول مشخصات راهنمای برد اصلی ردیف CPU، نوع سوکت و پردازنده‌های قابل نصب روی برد اصلی مشخص شده است.



شکل ۱۵- مشخصات پردازنده در راهنمای برد اصلی



تشخیص ماژول‌های حافظه اصلی سازگار با برد اصلی
حافظه اصلی از مهم‌ترین قطعات رایانه است. به مجموع چند تراشه حافظه که روی یک برد و در کنار هم قرار گرفته‌اند، ماژول حافظه می‌گویند. ماژول‌های حافظه در بانک حافظه برد اصلی قرار می‌گیرند. امروزه ماژول‌های حافظه در دو نوع DDR3 و DDR4 و در ظرفیت‌های گوناگون طراحی و تولید می‌شوند.

شکل ۱۶- انواع ماژول‌های حافظه

برد اصلی باید با نوع ماژول حافظه سازگار باشد. برای مثال

ماژول حافظه DDR3 فقط روی بانک حافظه DDR3 قابل نصب است. در بین پایه‌های ماژول حافظه شکافی برای تعیین جهت نصب وجود دارد. تفاوت انواع ماژول‌های حافظه در شکل ظاهری، محل شکاف، تعداد پین‌های اتصال، ولتاژ تغذیه و سرعت انتقال داده‌های آنها است. در شکل ۱۶ به تفاوت ظاهری و نیز محل شکاف برد انواع ماژول‌های حافظه DDR تا DDR4 دقت کنید.

مشخصات اصلی هر ماژول به صورت برچسبی روی آن قرار دارد و از روی این برچسب می‌توان نوع ماژول حافظه، سرعت انتقال اطلاعات و ظرفیت حافظه را تشخیص داد.



شکل ۱۷- ماژول حافظه

مشخصات ماژول حافظه شکل ۱۷ بر اساس برچسب آن در جدول آمده است.

نوع ماژول حافظه	DDR4
سرعت ماژول حافظه	2133MHZ
ظرفیت ماژول حافظه	4 GB

در راهنمای برد اصلی نوع ماژول حافظه، حداقل و حداکثر سرعت انتقال اطلاعات و حداکثر ظرفیت ماژول حافظه قابل پشتیبانی را می‌توان مشاهده کرد.

شکل ۱۸ نمونه‌ای از مشخصات درج‌شده در راهنمای برد اصلی است.

Memory	4 x DIMM, max. 64GB, DDR4 3466(O.C.)/3400(O.C.)/3333(O.C.)/3300(O.C.)/3200(O.C.)/3000(O.C.)/2800(O.C.)*2666(O.C.)*2400(O.C.)*2133 MHz; Dual channel memory architecture
--------	--

شکل ۱۸- نمونه‌ای از مشخصات درج‌شده در راهنمای برد اصلی

حداکثر تعداد ماژول‌های حافظه قابل نصب روی برد اصلی برابر با تعداد بانک‌های حافظه برد اصلی است ولی می‌توان از تعداد ماژول‌های حافظه کمتری نیز استفاده کرد. حداقل و حداکثر ظرفیت هر یک از ماژول‌های حافظه‌ای که برد اصلی از آنها پشتیبانی می‌کند، در راهنمای برد اصلی بخش تنظیمات حافظه مشخص می‌شود. در برخی از راهنماها برد اصلی فهرستی از ماژول‌های حافظه سازگار با برد اصلی، بر اساس نام سازنده‌ها پیشنهاد شده است. برای کارایی بالاتر سیستم بهتر است، ماژول حافظه را از این فهرست انتخاب کنید.

تعیین نوع کارت توسعه (Expansion Card)

روی برخی از بردهای اصلی کارت صدا، شبکه و گرافیک به صورت سرخود وجود دارد. در صورت نیاز به استفاده از کارت‌های دیگر مثل کارت TV، کارت شبکه بی‌سیم و یا کارت‌های حرفه‌ای و پیشرفته صدا، شبکه و گرافیک از کارت‌های مجزا (internal) استفاده می‌شود که به آنها کارت‌های توسعه می‌گویند.

کارت گرافیک

کارت گرافیک تصاویر را برای صفحه نمایش آماده می‌کند. هر قطعه فیلم و انیمیشن شامل تصاویری است که پشت سر هم نمایش داده می‌شوند. هر تصویر از نقاط زیادی تشکیل شده است و به هر کدام از این نقاط پیکسل (Pixel) می‌گویند. برای نمایش تصاویر، انیمیشن، بازی‌های رایانه‌ای و فیلم‌ها نیاز به پردازش پیکسل‌ها است که این عملیات وقت زیادی از پردازنده اصلی را می‌گیرد؛ بنابراین طراحان سخت‌افزار رایانه برای بالابردن کارایی سیستم از یک پردازنده دیگر استفاده می‌کنند که به آن واحد پردازش گرافیکی (Graphic Processing Unit) یا GPU می‌گویند. در سیستم‌های رایانه‌ای واحد پردازش گرافیک به یکی از صورت‌های زیر است:



شکل ۱۹- کارت گرافیک

- تعبیه‌شده در کارت گرافیک مجزا (internal card)
- به صورت یکپارچه با برد اصلی (onboard)
- به صورت مجتمع در پردازنده اصلی (integrated)

در اکثر پردازنده‌های جدید، واحد پردازش گرافیک در کنار هسته‌های پردازنده مرکزی است و با هم در یک تراشه قرار گرفته‌اند که به آن پردازنده مجتمع می‌گویند. در هنگام خرید پردازنده این ویژگی به عنوان مزیت پردازنده در نظر گرفته می‌شود.

تفاوت کارت‌های گرافیک در ظرفیت حافظه، سرعت و قدرت پردازنده آنها است. کارت گرافیک روی شکاف توسعه‌ای با نام PCI_E (PCI Express) در برد اصلی نصب می‌شود.

کارت صدا

برای پخش و ضبط صدا در رایانه از کارت صدا استفاده می‌شود. این کارت دارای کانکتورهایی برای میکروفن و بلندگو و دستگاه‌های صوتی است. وظیفه کارت صدا آماده‌سازی صدا برای پخش به وسیله بلندگو، دریافت صدای ورودی از میکروفن یا دستگاه‌های صوتی و آماده کردن آنها برای ذخیره در رایانه است. بیشتر بردهای اصلی جدید مجهز به کارت صدا هستند و تنها در صورت نیاز به انجام کارهای حرفه‌ای لازم است که کارت صدای حرفه‌ای به صورت مجزا در شکاف توسعه نصب شود. کارت صدا در شکاف توسعه PCI نصب می‌شود.



شکل ۲۰- کارت صدا



شکل ۲۱- کارت شبکه

کارت شبکه

برای اتصال به شبکه نیاز به کارت شبکه (LAN Card) است. این کارت دارای دو نوع با سیم و بی سیم است. کارت شبکه‌های رایج دارای کانکتوری متناسب با نوع کابل و کارت شبکه بی سیم دارای آنتن برای اتصال به شبکه است. بیشتر بردهای اصلی امروزی مجهز به کارت شبکه هستند و در صورت نیاز به نصب کارت شبکه، این کارت به صورت مجزا در شکاف توسعه PCI نصب می‌شود.

انتخاب منبع تغذیه

برای شارژ تلفن همراه یا رایانه قابل حمل از چه وسیله‌ای استفاده می‌شود؟ آیا شارژر وسایل مختلف را می‌توان به جای هم استفاده کرد؟ آیا همه وسایل با ولتاژ یکسانی کار می‌کنند؟

تمامی قطعات و اجزای داخلی رایانه برای کار نیاز به جریان الکتریسیته دارند. از طرفی هر قطعه برای کار، به ولتاژ مخصوص به خود نیاز دارد. برای کارکرد بهینه و حفظ ایمنی رایانه به قطعه‌ای نیاز داریم که تمامی ولتاژهای مورد نیاز قطعات مختلف را تولید کند و همچنین از نوسانات برق و آسیب‌های ناشی از آن جلوگیری کند. این قطعه منبع تغذیه نام دارد.

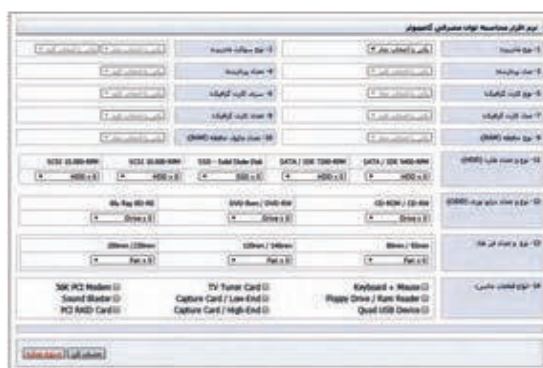


شکل ۲۲- منبع تغذیه

منبع تغذیه دارای بدنه فلزی است. در یک سمت بدنه آن، منافذ ریزی برای عبور جریان هوا تعبیه شده است. در سمت دیگری از بدنه (معمولاً زیر منبع تغذیه) یک فن برای کمک به تهویه هوا و دفع گرمای ناشی از کارکرد منبع تغذیه قرار دارد که به تهویه هوای داخل کیس نیز کمک می‌کند (شکل ۲۳).



شکل ۲۳- جهت تهویه هوا در منبع تغذیه



شکل ۲۴- نرم‌افزار برخط محاسبه توان مصرفی قطعات

برای اطمینان بیشتر و دقت بالاتر می‌توان از نرم‌افزارهایی برای محاسبه توان مصرفی قطعات استفاده کرد (شکل ۲۴). این نرم‌افزارها در بیشتر سایت‌های سازنده منبع تغذیه وجود دارند و با یک جست‌وجوی ساده اینترنتی قابل دستیابی هستند.

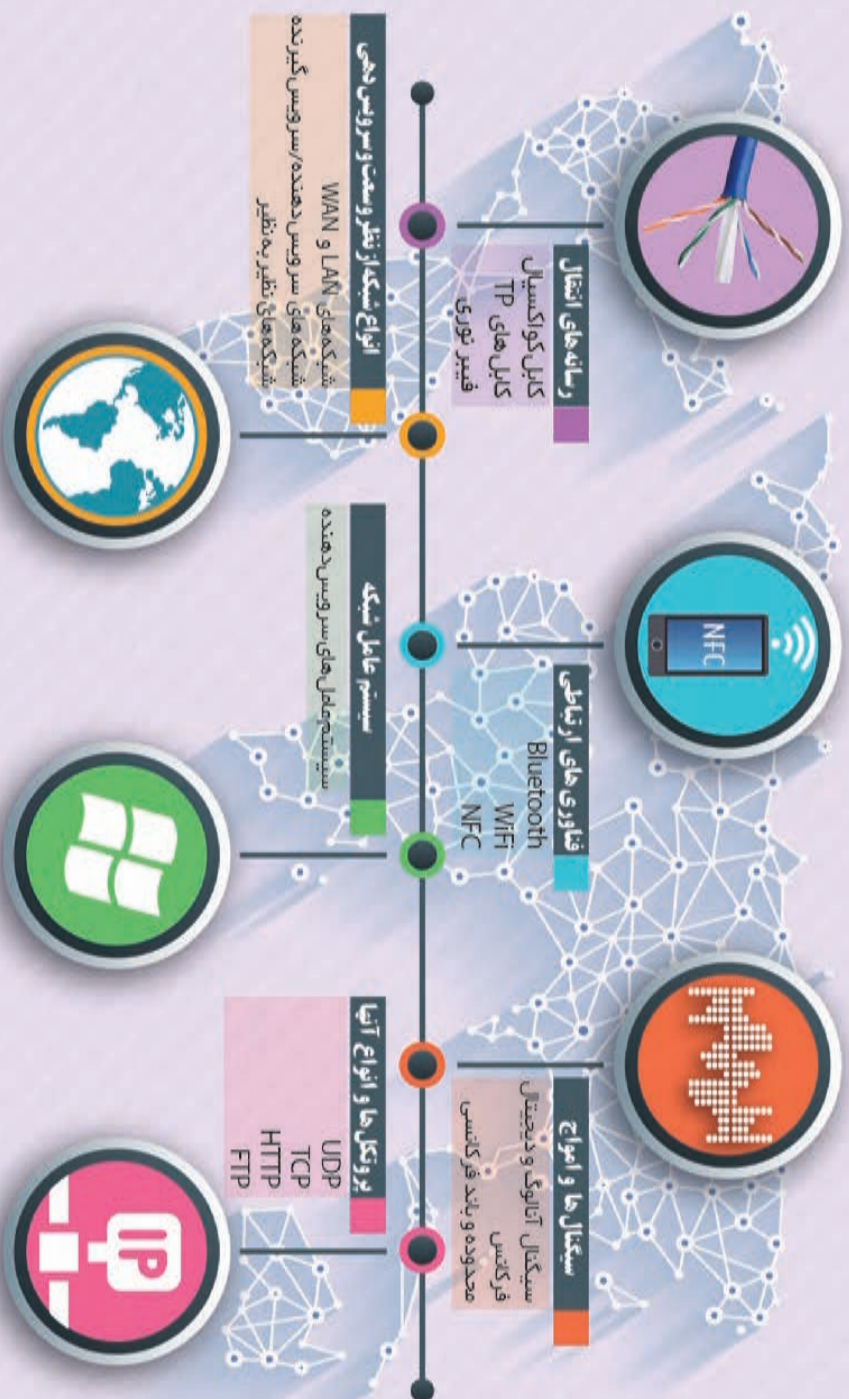
تعیین مشخصات رایانه به کمک نرم‌افزار

برای مشاهده مشخصات سخت‌افزاری هر رایانه، نرم‌افزارهای زیادی وجود دارند که یکی از معروف‌ترین آنها نرم‌افزار کم حجم CPU-Z است. این نرم‌افزار مشخصات قطعات اصلی رایانه را نشان می‌دهد. نصب این نرم‌افزار بسیار ساده است و به راحتی روی ویندوزهای مختلف اجرا می‌شود. این نرم‌افزار مشخصات پردازنده، برد اصلی، ماژول‌های حافظه و کارت گرافیکی را نمایش می‌دهد.

شبکه



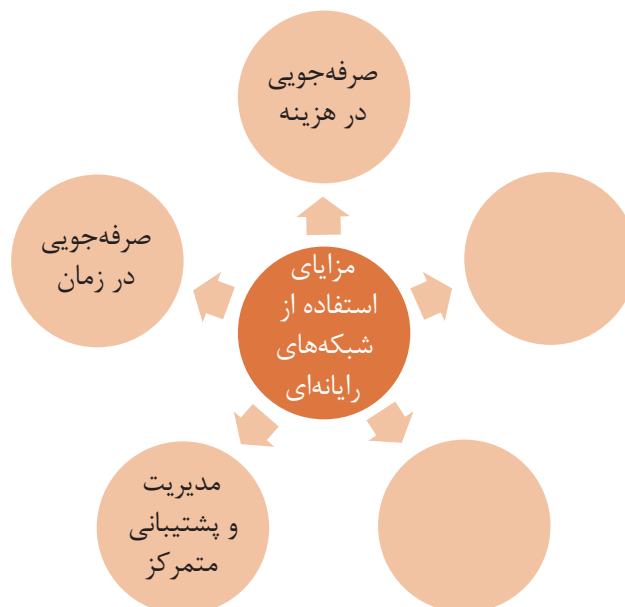
فناوری اطلاعات و ارتباطات بخش جدایی ناپذیر زندگی روزمره و مشاغل امروزی است. فعالیت‌های وابسته به فناوری اطلاعات و ارتباطات در بستر شبکه انجام می‌شوند که مهم‌ترین این فعالیت‌ها انتقال داده است. کیفیت تبادل داده در شبکه رایانه‌ای به نوع و معماری شبکه و تجهیزات مورد استفاده در آن بستگی دارد. در معماری شبکه نوع رسانه انتقال و استاندارد چیدمان اجزای فیزیکی شبکه تعیین می‌شود.



تاکنون در اطراف خود با چه شبکه‌هایی سر و کار داشته‌اید؟
به نظر شما علت ایجاد شبکه‌های مختلف چیست؟
شبکه‌های رایانه‌ای در کجا کاربرد دارند و ویژگی استفاده از آن‌ها چیست؟

شبکه رایانه‌ای به طور ساده می‌تواند دو رایانه متصل به یکدیگر باشد یا در حالت پیچیده‌تر مثل اینترنت می‌تواند شامل میلیون‌ها رایانه در سراسر جهان باشد. کارگاه رایانه نیز یک شبکه رایانه‌ای است. هر وسیله‌ای (Device) مانند رایانه و چاپگر که به یک شبکه رایانه‌ای متصل می‌شود و نشانی منحصر به فرد دارد، یک **گروه (node)** می‌نامند.

در شبکه رایانه‌ای نیز هر رایانه دارای یک نام یکتاست که به این نام آدرس IP می‌گویند. آدرس IP مجموعه‌ای از چند عدد است و در شبکه باید آدرس IP هر رایانه یکتا باشد.



شکل ۱- مزایای استفاده از شبکه‌های رایانه‌ای



شکل ۲- اجزای شبکه رایانه‌ای

اجزای شبکه رایانه‌ای (شکل ۲) عبارت‌اند از: **سرویس گیرنده (Client):** رایانه‌ای است که درخواست استفاده از منابع سخت‌افزاری یا نرم‌افزاری موجود در شبکه را دارد. به این رایانه‌ها **ایستگاه کاری (Workstation)** نیز می‌گویند.

سرویس دهنده (Server): رایانه‌ای است که خدماتی را به رایانه‌های شبکه ارائه می‌دهد و به درخواست‌های

رایانه‌های سرویس گیرنده برای دسترسی به منابع مورد نیاز پاسخ می‌دهد.

به هر یک از خدماتی که به وسیله سرویس دهنده‌ها در اختیار دیگر کاربران یا رایانه‌های شبکه قرار می‌گیرد، سرویس می‌گویند.

محیط انتقال (Communication media): ارتباط بین رایانه‌ها به وسیله یک رسانه (Media) انجام می‌شود که می‌تواند به صورت سیمی (Wired) و یا بی‌سیم (Wireless) باشد.

سیستم عامل شبکه: سیستم عامل رایانه باید قابلیت‌های ویژه‌ای داشته باشد تا رایانه بتواند از خدمات شبکه استفاده کند. سیستم عامل شبکه، سرویس‌های شبکه‌ای را به رایانه‌های متصل به شبکه ارائه داده، اجازه برقراری ارتباط به آنها را می‌دهد.

پروتکل (Protocol): به مجموعه قوانین و قراردادهایی گفته می‌شود که تعیین می‌کند چگونه رایانه‌های درون شبکه با هم ارتباط برقرار کنند.

انواع شبکه بر اساس مدل سرویس دهی

شبکه‌ها به دو نوع شبکه مبتنی بر سرویس دهنده یا SB (Server Based) و شبکه‌های نظیر به نظیر یا P2P (Peer To Peer) تقسیم می‌شوند.

■ شبکه مبتنی بر سرویس دهنده

در چنین شبکه‌هایی یک یا چند رایانه فقط نقش سرویس دهنده دارند و سرویس‌های خاصی را ارائه می‌کنند. به همین دلیل به آنها شبکه‌های **سرویس دهنده/سرویس گیرنده** می‌گویند. مانند یک شرکت که تمام اطلاعات خود را روی چندین پایگاه داده متمرکز قرار می‌دهد و کاربران از راه دور به آن دسترسی دارند. در این آرایش، پایگاه داده‌ها روی رایانه‌های پر قدرتی به نام سرویس دهنده (server) قرار دارند و کاربران، مشتری یا سرویس گیرنده (Client) نامیده می‌شوند.

به این شبکه‌ها، شبکه Domain نیز گفته می‌شود.

■ شبکه‌های نظیر به نظیر

امروزه همه رایانه‌های شبکه می‌توانند هم‌زمان به صورت سرویس دهنده و سرویس گیرنده عمل کنند. برای مثال یک رایانه صرف نظر از اینکه سیستم عامل آن از نوع سرویس دهنده یا سرویس گیرنده باشد، می‌تواند پرونده‌های خود را برای دیگر رایانه‌های شبکه به اشتراک بگذارد و به پرونده‌های به اشتراک گذاشته شده دیگر رایانه‌ها نیز دسترسی داشته باشد. به همین دلیل به آنها شبکه‌های **نظیر به نظیر** می‌گویند.

انواع شبکه بر اساس ابعاد و گستردگی جغرافیایی

از نظر گستردگی جغرافیایی شبکه‌ها را به دو گروه LAN (Local Area Network) و WAN (Wide Area Network) تقسیم می‌کنند.

■ شبکه محلی (LAN)



شکل ۳- شبکه محلی

این شبکه شامل مجموعه‌ای از رایانه‌هاست که با فاصله کم از یکدیگر در محلی مانند یک اتاق، طبقه، یک یا چند ساختمان نزدیک هم قرار دارند (شکل ۳). چند نمونه از شبکه‌های محلی عبارت‌اند از:

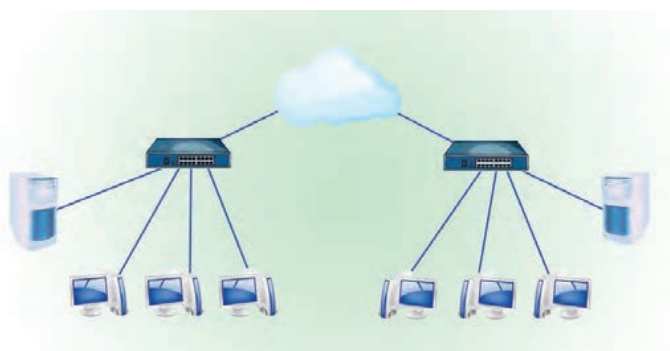
- الف) شبکه‌ای متشکل از دو رایانه خانگی
- ب) شبکه رایانه‌های یک اداره واقع در یک ساختمان
- ج) شبکه رایانه‌ای کارگاه های رایانه

شبکه محلی کوچکترین شکل شبکه از نظر ابعاد و گستردگی جغرافیایی و پایه شبکه‌های دیگر است.

■ شبکه گسترده (WAN)

شبکه‌های گسترده، یک حوزه جغرافیایی گسترده نظیر یک شهر، استان و یک کشور را تحت پوشش قرار می‌دهند. این شبکه‌ها معمولاً از امکانات ارائه شده به وسیله شرکت‌های مخابراتی استفاده می‌کنند (شکل ۴). چند نمونه از شبکه‌های گسترده عبارت‌اند از:

- الف) شبکه بین شعب مختلف بانک‌های کشور
- ب) شبکه بین هنرستان‌های یک استان
- ج) شبکه اینترنت



شکل ۴- شبکه گسترده

انتقال داده در شبکه

هنگام ارسال داده‌ها در شبکه، داده‌ها به واحدهای کوچکی به نام بسته (Packet) تقسیم می‌شوند. سپس بسته‌ها در قالب سیگنال (Signal) روی رسانه فرستاده می‌شوند. سیگنال‌ها امواجی هستند که به وسیله یک منبع، تولید و منتشر می‌شوند. ماهیت سیگنال به رسانه شبکه بستگی دارد. ۳ نوع متداول سیگنال برای ارتباط در شبکه عبارت‌اند از:

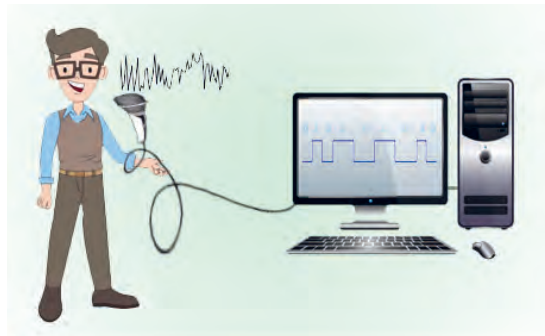
الکتریکی: شبکه‌هایی که نوع رسانه آنها کابل مسی است، برای ارسال داده‌ها از سیگنال‌های الکتریکی استفاده می‌کنند.

نوری: کابل‌های فیبر نوری داده‌ها را به صورت پالس نوری ارسال می‌کنند. همچنین برخی از شبکه‌های بی سیم از نور مادون قرمز برای انتقال داده استفاده می‌کنند.

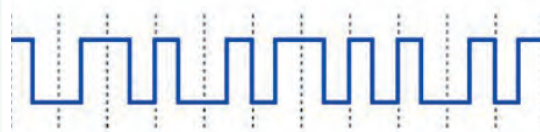
رادیویی: بیشتر شبکه‌های بی سیم از سیگنال رادیویی برای ارتباطات شبکه استفاده می‌کنند.

سیگنال‌های داده به دو صورت دیجیتال یا آنالوگ هستند. سیگنال‌های آنالوگ در کابل و هوا منتشر می‌شوند. صدای انسان نمونه‌ای از سیگنال آنالوگ است. هنگام صحبت کردن به وسیله ارتعاش تارهای صوتی، سیگنال‌های رادیویی به صورت آنالوگ ایجاد می‌شوند و در فضا حرکت می‌کنند و گوش افراد می‌تواند به دریافت و تشخیص

سیگنال‌های صوتی پیردازد. این سازوکار توانایی صحبت کردن و شنیدن را برای انسان‌ها فراهم می‌کند (شکل ۵). سیگنال‌های دیجیتال در دستگاه‌های دیجیتال مانند رایانه‌ها، گوشی‌های هوشمند و... ارسال و دریافت می‌شوند. این سیگنال‌ها فقط دو حالت دارند و ارزش عددی آنها در واحدهای زمانی مختلف صفر یا یک است (شکل ۶).



شکل ۵- تبدیل سیگنال آنالوگ صدا به دیجیتال



شکل ۶- سیگنال دیجیتال

در حوزه ارسال اطلاعات علاوه بر مفهوم سیگنال، لازم است با مفاهیم فرکانس (Frequency)، باند فرکانسی (Frequency band) و پهنای باند (Bandwidth) نیز آشنا شویم.

فرکانس: تعداد تکرار یک سیگنال در واحد زمان را فرکانس می‌نامند. فرکانس سیگنال‌ها با واحد هرتز (Hz) سنجیده می‌شود. یک هرتز معادل یک بار تکرار سیگنال در ثانیه است.

باند فرکانسی: به محدوده مشخصی از فرکانس‌ها یک باند فرکانسی گفته می‌شود.

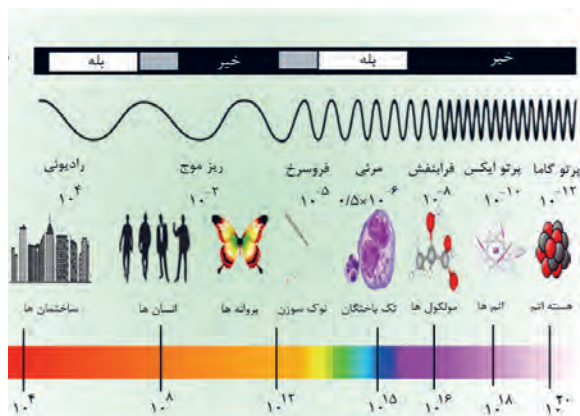
گوش انسان فقط قادر به شنیدن محدوده مشخصی از فرکانس‌هاست. برای مثال انسان‌ها نمی‌توانند صدای پای مورچه را بشنوند چون فرکانس آن بسیار پایین است. دستگاه‌های گیرنده الکترونیکی نیز قادر به دریافت محدوده مشخصی از فرکانس‌ها هستند. برای مثال باند فرکانسی موج FM فرکانس‌های بین ۸۸ مگاهرتز تا ۱۰۸ مگاهرتز است و دستگاه گیرنده رادیوی FM فقط قادر به دریافت سیگنال‌های بین این محدوده است. استفاده از باندهای فرکانسی نیازمند کسب مجوز از دولت است. بیشتر دولت‌ها باند فرکانسی خاصی را به صورت آزاد در اختیار همه کاربران قرار می‌دهند که استفاده از آن نیاز به کسب مجوز ندارد و هر کاربر می‌تواند به شرط تداخل نداشتن، اطلاعات خود را روی آن ارسال یا دریافت کند. معمولاً کاربران از این باند فرکانسی برای دستگاه‌های صنعتی یا کاربردهای پزشکی استفاده می‌کنند که به آن ISM (Industrial Scientific Medical) می‌گویند.

قابل نفوذ در جو زمین

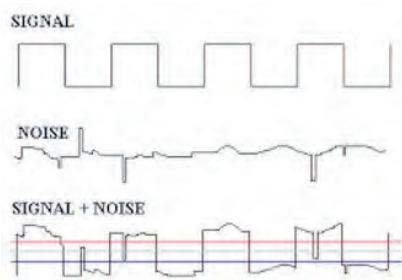
نوع پرتو
طول موج (متر)

اندازه تقریبی طول موج

فرکانس (هرتز)



پهنای باند: پهنای باند مفهومی است که در علوم مخابرات و رایانه تعاریف متفاوتی دارد. در علم مخابرات، پهنای باند فرکانسی بدین صورت تعریف می‌شود: هر سیستم انتقال، توانایی محدودی در انتقال امواج دارد. به صورتی که پایین‌ترین و بالاترین فرکانسی که یک رسانه برای انتقال اطلاعات استفاده می‌کند، مشخص است. فاصله بین پایین‌ترین و بالاترین فرکانس، پهنای باند رسانه نامیده می‌شود. اما در علم رایانه تعریف پهنای باند به معنی نرخ ارسال اطلاعات در رسانه است. به بیان ساده‌تر پهنای باند حداکثر تعداد بیت‌هایی است که می‌تواند به طور هم‌زمان از رسانه منتقل شود. یک خیابان دو طرفه و یک آزاد راه با چند باند را در نظر بگیرید، بدیهی است که هرچه عرض جاده بیشتر باشد، خودروهای بیشتری می‌توانند در آن حرکت کنند. پهنای باند نیز مانند عرض جاده تأثیر زیادی در سرعت تبادل اطلاعات دارد. در واقع پهنای باند، ظرفیت انتقال اطلاعات به وسیله رسانه است که با واحد بیت بر ثانیه (bit per second) bps سنجیده می‌شود.



نویز
نویز عامل مخربی است که شکل یا مقدار سیگنال ارسالی را تغییر می‌دهد. این تغییر شکل سبب می‌شود اطلاعات ارسال شده قابل تشخیص نباشند یا تشخیص آنها مشکل باشد. نسبت سیگنال به نویز یکی از معیارهای ارزیابی سیستم‌های ارتباطی است. هرچه این عدد بزرگتر باشد یعنی میزان دخالت نویز کمتر است و سیگنال‌ها کمتر دچار خرابی شده‌اند.

سرعت انتقال اطلاعات با پهنای باند ارتباط مستقیم و با نویز ارتباط معکوس دارد.

عوامل مختلفی باعث ایجاد نویز می‌شوند. برخی از آنها در شکل ۷ بیان شده است.

به اثرگذاری میدان مغناطیسی یک کابل در کابل مجاور آن، هم‌شنوایی گفته می‌شود. این نویزها می‌توانند به وسیله کابل‌های برق فشار قوی یا رعد و برق ایجاد شوند.

هم‌شنوایی

حرارت باعث می‌شود تا الکترون‌ها به صورت تصادفی حرکت کنند. این حرکت ممکن است باعث تغییر در اندازه و شکل سیگنال شود.

حرارتی

نویز القایی از موتورهای مکانیکی مانند موتور ماشین یا وسایل الکتریکی مانند موتورهای الکتریکی موجود در لوازم خانگی تولید می‌شود. این وسایل مانند یک آنتن فرستنده عمل کرده، نویز را ارسال می‌کنند و کابل شبکه مانند آنتن گیرنده عمل کرده، نویز را دریافت می‌کند.

القایی

شکل ۷- عوامل ایجاد نویز

با توجه به محیطی که داده‌ها در آن انتشار می‌یابند، می‌توان برای کاهش نویز از رسانه‌های انتقال مناسب استفاده کرد.

رسانه‌های انتقال

برای برقراری ارتباط بین دو رایانه لازم است تا داده‌ها به وسیله سیگنال‌های الکتریکی مبادله شوند. سیگنال‌ها به وسیله محیط یا رسانه انتقال جابه‌جا می‌شوند. به محیطی که اجازه عبور سیگنال‌ها را می‌دهد رسانه انتقال گفته می‌شود. رسانه‌ها به دو نوع کلی هدایت‌پذیر یا سیمی مانند سیم مسی و فیبرنوری و هدایت‌ناپذیر یا بی‌سیم مانند امواج رادیویی تقسیم می‌شوند.

۱- رسانه‌های انتقال سیمی

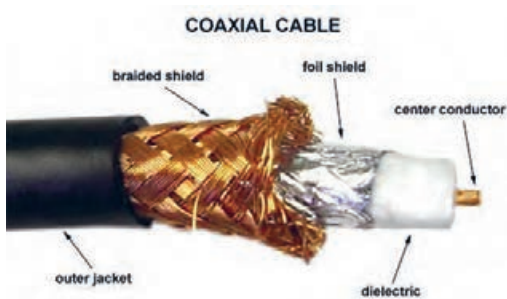
رسانه‌های انتقال هدایت‌پذیر زوج سیم به هم تابیده (Twisted-Pair)، کابل کوکسیال (Coaxial cable) و فیبرنوری هستند. هر یک از این رسانه‌ها می‌توانند برای اتصال رایانه به شبکه و انتقال داده‌ها در شبکه استفاده شوند.

■ زوج سیم به هم تابیده

در زوج سیم به هم تابیده (TP)، سیم‌های هادی دوبه‌دو به هم تابیده شده‌اند. این تابیدگی باعث می‌شود تا اختلالات الکترومغناطیسی و اثرات نویز خنثی شود. همچنین یک لایه محافظ به نام شیلد (shield) برای محافظت از داده‌ها و جلوگیری از نویزهای هم‌شنوایی و القایی روی سیم‌ها وجود دارد.

■ کابل کوکسیال

واژه coaxial ترکیبی از Co و Axial به معنی هم محور است. امروزه استفاده از کابل کوکسیال در شبکه منسوخ شده است. این کابل از چهار بخش تشکیل شده است (شکل ۸).



شکل ۸- اجزای کابل کوکسیال

۱ مغزی مسی: که وظیفه آن هدایت سیگنال الکتریکی است و می‌تواند مفتولی و یا چند رشته‌ای باشد.

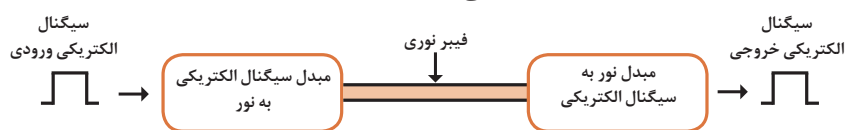
۲ عایق داخلی: عایق بین مغزی مسی و محافظ سیمی (توری) است.

۳ محافظ توری سیمی یا شیلد: سیگنال‌های انتقالی را در مقابل نویز حفاظت می‌کند.

۴ عایق بیرونی: روکشی پلاستیکی است که کل کابل را پوشش می‌دهد.

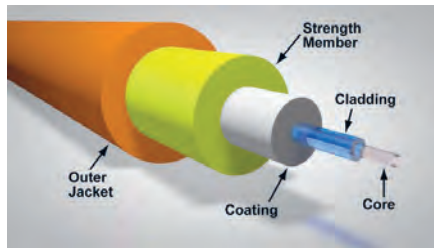
فیبر نوری

برخلاف کابل‌های TP و کوکسیال که از سیگنال‌های الکتریکی برای انتقال داده استفاده می‌کنند، فیبرهای نوری داده‌ها را به صورت پالس‌های نوری و با استفاده از پدیده شکست نور انتقال می‌دهند. بنابراین در دو سر فیبرهای نوری باید از مبدل‌های سیگنال الکتریکی به نور و برعکس استفاده شود (شکل ۹).



شکل ۹- تبدیل سیگنال الکتریکی به نور و برعکس در فیبرنوری

یک کابل فیبرنوری از پنج بخش تشکیل شده است (شکل ۱۰).



شکل ۱۰- اجزای فیبر نوری

۱ هسته: قسمت شیشه‌ای یا پلاستیکی کابل است که در مرکز آن قرار دارد. نور در این بخش از فیبر جریان می‌یابد.

۲ روکش: از جنس شیشه یا پلاستیک با ضریب شکست متفاوتی نسبت به هسته ساخته می‌شود. استفاده از ضریب شکست‌های مختلف بین هسته و روکش سبب می‌شود نور از محیط فیبر خارج نشده و در آن انتقال یابد.

۳ غلاف: روکشی رنگی و محکم است که از هسته و روکش در مقابل رطوبت و عوامل خارجی محافظت می‌کند. برخی از مدل‌های فیبرنوری دارای خاصیت ضدآب (Waterproof)، ضدجوندگی (Anti-Rodent) و ضد اشعه ماوراءبنفش (Anti-UV) هستند. این روکش رنگی سبب می‌شود سر دیگر فیبر برای اتصال سوکت‌ها قابل تشخیص باشد.

۴ الیاف تقویتی: برای بالا بردن قدرت کشش کابل فیبرنوری استفاده می‌شود.

۵ روکش بیرونی کابل: روکش بیرونی کابل فیبرنوری است که از پلاستیک ساخته می‌شود.

هر رشته فیبرنوری می‌تواند داده‌ها را در یک جهت انتقال دهد. بنابراین دستگاه‌هایی که از این رسانه انتقال برای تبادل داده استفاده می‌کنند باید از دو رشته فیبرنوری، یکی برای ارسال اطلاعات و دیگری برای دریافت اطلاعات استفاده کنند. از فیبرنوری برای انتقال داده با سرعت بالا و تا حدود ۱۰ گیگابیت بر ثانیه استفاده می‌شود. قدرت انتقال هر رشته فیبرنوری تقریباً معادل ۹۰۰ زوج سیم مسی است.

۲- رسانه‌های انتقال بی‌سیم

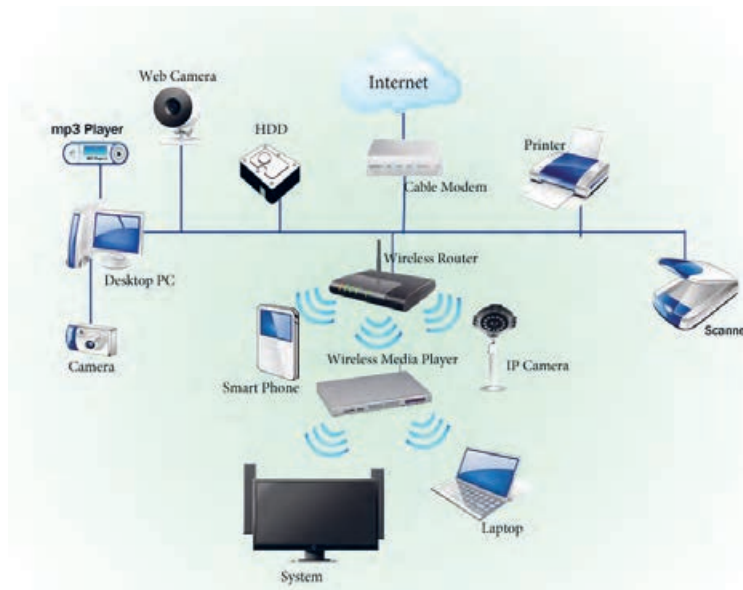
تبادل اطلاعات در محیط انتقال بی‌سیم از طریق امواج رادیویی یا الکترومغناطیسی، لیزر یا نور مادون قرمز انجام می‌شود. استفاده از رسانه‌های کابلی نیازمند تعیین دقیق محل قرارگیری رایانه است و هنگام استفاده از این رسانه‌ها جابه‌جایی رایانه‌ها بسیار محدود یا ناممکن است. انتقال داده به صورت بی‌سیم سبب می‌شود رایانه‌ها محدود به مکان خاصی نبوده، بتوانند به صورت سیار از شبکه استفاده کنند.

■ مخابرات رادیویی

امواج رادیویی کاربرد زیادی در انتقال اطلاعات در فضای سرپوشیده و باز دارند. زیرا به راحتی تولید می‌شوند و می‌توانند از ساختمان‌ها و موانع عبور کنند. ویژگی‌های امواج رادیویی به فرکانس آنها وابسته است. امواج فرکانس پایین به راحتی می‌توانند از موانع عبور کنند؛ اما توان آنها در اثر افزایش مسافت افت می‌کند. شبکه‌های رایانه‌ای بی‌سیم به راحتی به وسیله امواج رادیویی تبادل اطلاعات می‌کنند.

در شبکه بی‌سیم قبل از نوع شبکه از پیشوند W به معنای بی‌سیم یا Wireless استفاده می‌شود. مانند شبکه‌های WLAN که به شبکه‌های LAN بی‌سیم اشاره دارد.

هر شبکه بی‌سیم وسعت و محدوده پوشش مشخصی دارد و ارتباط با آن فقط در صورتی امکان‌پذیر است که در محدوده پوشش آن شبکه قرار گیریم (شکل ۱۱).



شکل ۱۱- شبکه بی سیم

■ مخابرات مایکروویو

امواج مایکروویو امواجی هستند که فرکانس بالای ۱۰۰MHz دارند و به صورت مستقیم حرکت می کنند. این امواج نسبت سیگنال به نویز بالایی دارند و برای ارسال اطلاعات حجیم به صورت بی سیم کاربرد فراوانی دارند. این امواج برخلاف امواج رادیویی فرکانس پایین نمی توانند به خوبی از موانع عبور کنند، به همین خاطر باید بین فرستنده و گیرنده هیچ مانعی نباشد. استفاده از امواج مایکروویو در مخابرات راه دور، تلفن های همراه و تلویزیون بسیار رایج است؛ زیرا نسبتاً ارزان است و با نصب آنتن های فرستنده و گیرنده می توان به راحتی از این امواج استفاده کرد.

فناوری های انتقال بی سیم

فناوری بلوتوث (Bluetooth) و NFC (Near Field Communication) برای تبادل داده از انتقال بی سیم استفاده می کنند.

بلوتوث

به کمک این فناوری می توان داده ها را حداکثر ۱۰۰ متر و با استفاده از سیگنال های الکترومغناطیسی و به صورت بی سیم منتقل کرد. سیگنال های الکترومغناطیسی می توانند از موانعی مانند دیوار عبور کنند و داده ها را بین تجهیزاتی تبادل کنند که موانعی بین آنها است. هدف اصلی طراحی این فناوری حذف کابل ارتباطی بین رایانه و تجهیزات جانبی مانند همدست، صفحه کلید، ماوس و... است. در این فناوری همیشه سعی شده است تا دستگاه از لحاظ قیمت، اندازه و توان مصرفی در حداقل باشد. دستگاه هایی که از فناوری بلوتوث استفاده می کنند، داده ها را در باند فرکانسی ۲/۴GHz تا ۲/۴۸GHz ارسال یا دریافت می کنند.



NFC

از فناوری NFC برای ارتباط در فاصله حدود ۴ سانتیمتر استفاده می شود. دستگاه های مجهز به NFC می توانند در باند فرکانسی ۱۳/۵۶GHz داده ها را با سرعت ۴۲۴Kbps انتقال دهند. یکی از کاربردهای NFC استفاده از آن در پرداخت های مالی غیر نقدی مانند کارت های بانکی، اتوبوس و مترو و همچنین در دستگاه هایی است که از اینترنت اشیا پشتیبانی می کنند.

پروتکل

پروتکل، زبان مشترک برای برقراری ارتباط بین رایانه‌هاست. شیوه تقسیم‌بندی، ارسال، جمع‌بندی مجدد بسته‌های ارسالی در مقصد و کنترل زمان تبادل اطلاعات از وظایف پروتکل است. برای ارتباط در شبکه، پروتکل‌های متعددی وجود دارد که از نظر سرعت، قابلیت اطمینان، سادگی و... با یکدیگر تفاوت دارند؛ اما مسأله مهم این است که دو طرف ارتباط از پروتکل یکسان استفاده کنند و زبان یکدیگر را بفهمند.

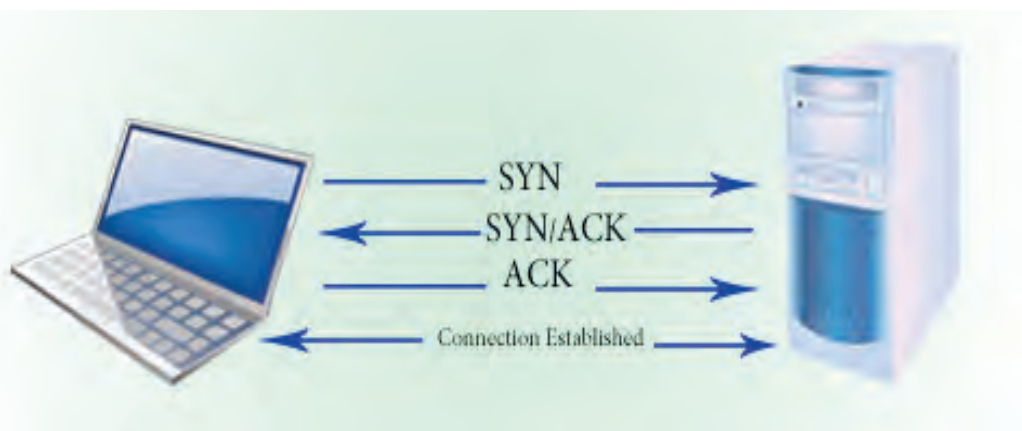
برای تبادل داده‌ها در شبکه از مجموعه‌ای از استانداردها و پروتکل‌ها استفاده می‌شود.

پروتکل FTP: از این پروتکل برای انتقال پرونده بین دو رایانه استفاده می‌شود. پروتکل (File Transfer Protocol) FTP مشابه به اشتراک گذاشتن پرونده روی یک رایانه نیست و اجازه دسترسی به پرونده روی سرویس دهنده را نمی‌دهد، بلکه با استفاده از این پروتکل می‌توان پرونده را در سرویس گیرنده کپی کرد.

پروتکل ICMP: معمولاً از پروتکل ICMP (Internet Control Message Protocol) برای بررسی وضعیت ارتباط و تشخیص خطا در شبکه استفاده می‌شود. در صورت بروز خطا در شبکه می‌توان نوع خطا و منبع ایجاد آن را با استفاده از این پروتکل گزارش داد.

پروتکل TCP: با استفاده از پروتکل (Transmission Control Protocol) می‌توان ارتباط بین رایانه‌های فرستنده و گیرنده را برقرار کرد. این پروتکل یک پروتکل اتصال‌گرا است. در پروتکل اتصال‌گرا قبل از اینکه هر گونه تبادل داده‌ای با استفاده از آن رخ دهد، رایانه‌های فرستنده و گیرنده اطلاعات، باید برخی هماهنگی‌ها مانند تعیین مسیر ارتباط را انجام داده، سپس اقدام به تبادل اطلاعات کنند. اتصال‌گرا بودن پروتکل تضمین می‌کند که همه داده‌ها سالم و بدون هیچ خطایی به مقصد خواهند رسید؛ اما در عوض ارسال و دریافت در این پروتکل با تأخیر همراه است.

پروتکل TCP برای برقراری ارتباط و همچنین قطع ارتباط، روال‌های خاصی دارد. روند برقراری یک ارتباط TCP به روش دست تکانی سه مرحله‌ای معروف است (شکل ۱۲).



شکل ۱۲- برقراری ارتباط در پروتکل TCP

در این روش از یک سری بسته‌های خاص استفاده می‌شود. در ابتدا فرستنده، یک بسته به نام SYN ارسال می‌کند و تقاضای برقراری ارتباط دارد. رایانه گیرنده در صورت تمایل برای برقراری ارتباط در پاسخ، یک بسته SYN/ACK ارسال می‌کند، سپس رایانه فرستنده نیز برقراری ارتباط را با بسته ACK تایید کرده، ارتباط ایجاد می‌شود.

پروتکل UDP (User Datagram Protocol): UDP یک پروتکل غیراتصال‌گرا است. در پروتکل‌های غیراتصال‌گرا بدون برقراری یک ارتباط مشخص، فرستنده بسته‌هایش را ارسال می‌کند. با استفاده از این پروتکل می‌توان داده‌ها را ارسال کرد؛ ولی هیچ تضمینی در رابطه با رسیدن اطلاعات به مقصد وجود ندارد، زیرا هماهنگی‌های اولیه انجام نمی‌شود و فرستنده در ابتدای کار شروع به ارسال بسته می‌کند. در اینجا ممکن است برخی از بسته‌های اطلاعاتی مفقود شوند و از بین بروند؛ اما در عوض سرعت بالایی در ارسال وجود دارد.

درگاه (Port)

به گروهی که در ارتباطات شبکه به عنوان مبدأ یا مقصد تعیین می‌شود، میزبان می‌گویند. برای برقراری ارتباط بین دو میزبان در شبکه ممکن است از پروتکل‌ها و سرویس‌های مختلفی استفاده شود. تفکیک این سرویس‌ها از یکدیگر با استفاده از ارتباطات مجازی به نام درگاه انجام می‌شود. داده‌های هر سرویس از طریق درگاه مخصوص آن سرویس به رایانه وارد یا از آن خارج می‌شوند. شناسایی هر یک از این درگاه‌های مجازی با استفاده از یک شماره انجام می‌شود که عددی بین ۰ تا ۶۵۵۳۵ است. درگاه‌ها به دو نوع TCP و UDP تقسیم می‌شوند و از بین درگاه‌های مختلف، درگاه‌های ۰ تا ۱۰۲۳ برای کاربردهای سیستم‌عامل استاندارد رزرو شده‌اند و دیگر درگاه‌ها آزاد هستند. برخی از ویروس‌های رایانه‌ای و برنامه‌های مخرب می‌توانند با استفاده از این درگاه‌ها در رایانه اختلال ایجاد کنند؛ بنابراین بهتر است برای جلوگیری از ایجاد اختلال، با استفاده از روش‌های مناسب نظیر دیوار آتش، درگاه‌های بدون استفاده را بست.

برخی از درگاه‌های پرکاربرد و شماره آنها در جدول ۱ آمده است.

جدول ۱- درگاه‌های استاندارد

شماره درگاه	نوع درگاه	پروتکل	کاربرد
۲۰	TCP	FTP / data (File Transfer Protocol)	پروتکل انتقال پرونده
۲۱	TCP	FTP / control	پروتکل FTP فرمان کنترل
۲۲	TCP	SSH (Secure Shell)	پروتکل مدیریت و دسترسی به شبکه از راه دور
۲۳	TCP	Telnet	دسترسی از راه دور
۸۰	TCP	HTTP (Hyper Text Trasfer Protocol)	پروتکل انتقال ابرمتن
۸۰۸۰	TCP	HTTP	درگاه جایگزین وب سرور
۳۳۸۹	TCP / UDP	RDP (Remote Desktop Protocol)	پروتکل دسترسی از راه دور میزکار

نحوه چیدمان و آرایش رایانه‌ها در هر شبکه مهم است و ممکن است با دیگر شبکه‌ها متفاوت باشد.

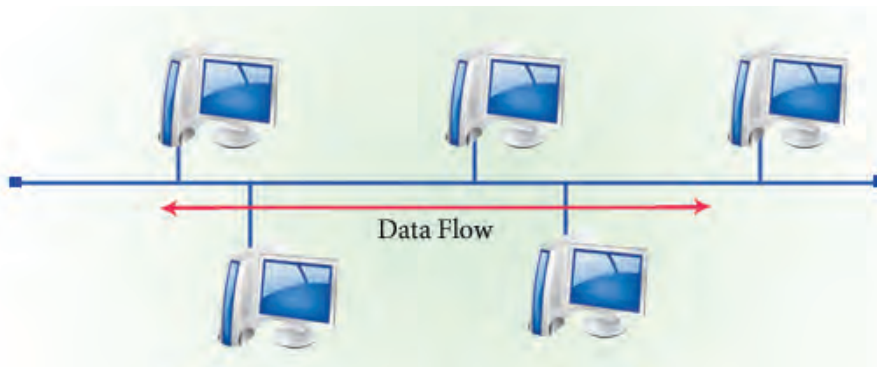
همبندی شبکه

اجزای یک شبکه را می‌توان به روش‌های مختلفی مبتنی بر یک طرح یا نقشه مشخص به یکدیگر متصل کرد، به این طرح و نقشه اتصال، همبندی (Topology) شبکه می‌گویند. عواملی از قبیل هزینه و قابلیت اطمینان در انتخاب نوع همبندی یک شبکه مهم است. در شبکه‌های رایانه‌ای همبندی‌های خطی (Bus)، حلقوی (Ring)، ستاره‌ای (Star)، مش (Mesh) و ترکیبی (Hybrid) استفاده می‌شوند.

همبندی خطی

همبندی خطی یکی از همبندی‌های قدیمی شبکه است. در این همبندی تمامی اجزای شبکه به یک کابل اصلی متصل می‌شوند و از آن برای انتقال داده‌ها استفاده می‌کنند (شکل ۱۳). از ویژگی‌های این همبندی می‌توان به موارد زیر اشاره کرد:

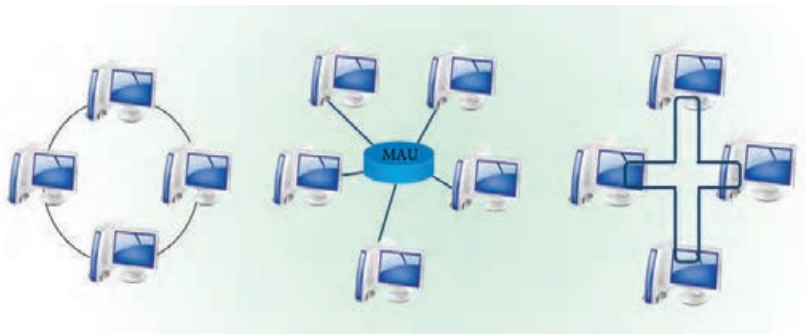
- ۱ ساختار ساده‌ای دارد، ارزان‌ترین نوع همبندی است.
- ۲ نسبت به بقیه همبندی‌ها کابل کمتری مصرف می‌کند.
- ۳ افزایش یا کاهش سیستم‌ها به راحتی انجام می‌شود.
- ۴ سرعت کمتری نسبت به بقیه همبندی‌ها داشته و در صورتی که یک بخش از کابل قطع شود، ارتباط کل شبکه قطع خواهد شد.
- ۵ فرایند عیب‌یابی شبکه مشکل و زمان‌بر است.



شکل ۱۳- همبندی خطی

همبندی حلقوی

در این همبندی هر رایانه به صورت منطقی به رایانه‌های مجاور خود متصل است و آخرین رایانه نیز به اولین رایانه وصل می‌شود. رایانه‌ها یک حلقه را تشکیل می‌دهند. این همبندی شبیه به همبندی خطی است با این تفاوت که در آن دو سر کابل به هم متصل شده‌اند. برای ایجاد ساختار منطقی حلقه، از سخت‌افزاری به نام MAU (Multistation Access Unit) استفاده می‌شود (شکل ۱۴).



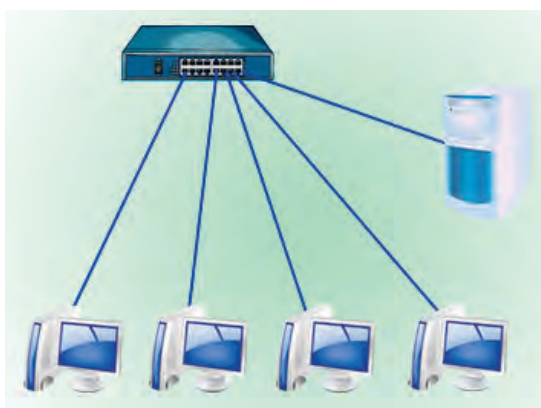
شکل ۱۴- همبندی حلقوی

در این شبکه‌ها وجود عیب در MAU و یا قطعی یک بخش از کابل باعث می‌شود تا کل شبکه از کار بیفتد. در ضمن افزودن و حذف رایانه‌ها در شبکه به سادگی ممکن نیست و مصرف کابل و هزینه پیاده‌سازی آن نسبت به همبندی خطی بیشتر است.

همبندی ستاره‌ای

در این همبندی از سخت‌افزاری به نام سوئیچ (Switch) استفاده می‌شود و هر رایانه با یک کابل مجزا به سوئیچ متصل می‌شود. در این همبندی داده‌ها ابتدا از مبدأ به سوئیچ، سپس از آن به رایانه مقصد ارسال می‌شوند (شکل ۱۵). از ویژگی‌های این همبندی می‌توان به موارد زیر اشاره کرد:

- ۱ در این شبکه از کابل بیشتری استفاده می‌شود ولی اگر اشکالی در شبکه رخ دهد، عیب‌یابی آن آسان است.
- ۲ در این شبکه خرابی یک کابل روی عملکرد کل شبکه تأثیری ندارد و فقط رایانه‌ای که کابل آن خراب شده است از شبکه خارج می‌شود.
- ۳ خرابی سوئیچ باعث از کار افتادن کل شبکه می‌شود.
- ۴ نوع کابل استفاده‌شده در این همبندی از نوع TP بوده، معمولاً حداکثر فاصله یک رایانه تا سوئیچ ۹۰ متر است.



شکل ۱۵- همبندی ستاره‌ای

همبندی مش

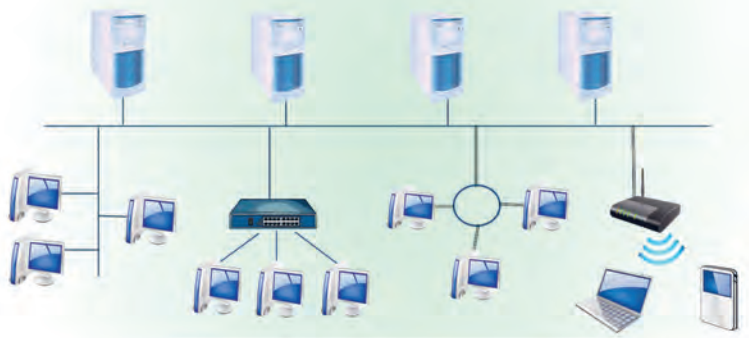
تمام رایانه‌های موجود در این شبکه به صورت دو به دو و با یک کابل مستقل یا به صورت بی‌سیم به هم متصل شده‌اند (شکل ۱۶). در این حالت به شبکه **مش کامل** می‌گویند، ولی اگر یک یا تعدادی از اتصالات برقرار نباشد به آن **مش ناقص** می‌گویند. مزیت اصلی این همبندی وجود بیش از یک مسیر بین گره‌های شبکه است و اگر به هر دلیلی بخشی از اجزای شبکه از کار بیفتد، باز هم می‌توان ارتباط را حفظ کرد و داده‌ها را انتقال داد. این همبندی مطمئن‌ترین و پایدارترین نوع ارتباط را نسبت به دیگر همبندی‌ها دارد ولی هزینه برپایی آن بالاست. یکی از کاربردهای شبکه مش، اتصال مراکز تلفن بین شهری به یکدیگر است.



شکل ۱۶- همبندی مش ناقص و کامل

همبندی ترکیبی

همبندی شبکه‌ای که با بیش از یک نوع همبندی ایجاد شده است را **همبندی ترکیبی** می‌نامند. این همبندی مزایا و معایب همبندی‌های به کار گرفته شده را دارد. اینترنت بهترین مثال از بزرگترین همبندی ترکیبی است (شکل ۱۷).



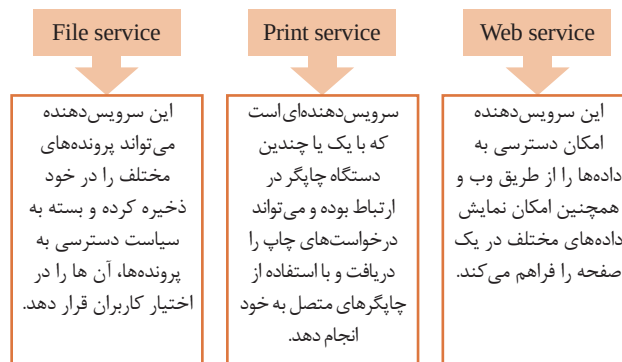
شکل ۱۷- همبندی ترکیبی

سیستم عامل شبکه

اینترنت یک شبکه در وسعت جهانی است که از ترکیب تعداد زیادی شبکه LAN و WAN با همبندی‌های متفاوت ایجاد شده است. به عبارتی می‌توان اینترنت را به عنوان ترکیبی از شبکه‌های دانشگاهی، اداری، نظامی، خانگی و... معرفی کرد و از آن به عنوان شبکه‌ای شبکه‌ها نام برد. اطلاعات و سرویس‌های فراوان و متنوعی در اینترنت وجود دارند که از آن جمله می‌توان به سرویس‌های وب (Web)، رایانامه (Email) و انتقال پرونده (FTP) اشاره کرد. سرویس‌هایی که در اینترنت ارائه می‌شود، از طریق پروتکل‌های مختلفی در اختیار سرویس‌گیرنده‌ها قرار می‌گیرد. از آنجایی که اینترنت از ترکیب هزاران شبکه با اندازه‌ها و پروتکل‌های مختلف و روش‌های ارتباطی گوناگون درست شده است؛ اکثر مواقع آن را به صورت یک ابر نشان می‌دهند که داخل این ابر انبوهی از سرویس‌ها و شبکه‌ها وجود دارد.

سیستم عامل سرویس دهنده

سیستم عامل سرویس دهنده، سیستم عاملی است که علاوه بر انجام کارهای معمول یک سیستم عامل، بتواند سرویس‌ها و خدمات مورد نیاز مدیران شبکه را ارائه کند. به عنوان نمونه‌ای از این سرویس‌ها می‌توان به سرویس چاپ یا اشتراک پرونده و... اشاره کرد. برخی از ویندوزها که به نام ویندوز سرور مشهورند، توانایی ارائه بیشتر سرویس‌های مورد نیاز شبکه را دارند و بسته به نیاز کاربران می‌توان آن سرویس را در سیستم عامل‌ها، فعال یا غیرفعال کرد. امکان ارائه این سرویس‌ها در بسیاری از سیستم عامل‌های غیر از ویندوز مانند لینوکس نیز فراهم است.



شکل ۱۸- برخی از سرویس های سرویس دهنده شبکه

سیستم عامل شبکه نسبت به سیستم عاملی که روی سایر رایانه ها نصب شده است باید توانایی های خاصی را داشته باشد که عبارت اند از:

■ **امنیت (Security):** یکی از مهم ترین ارکان کار سیستم عامل های شبکه، امنیت است. سیاست های امنیتی ممکن است باعث کند شدن سرعت سیستم شوند؛ ولی نمی توان از آنها صرف نظر کرد. امنیت یک سیستم عامل شبکه ای را می توان در حوزه های مختلفی بررسی کرد.

– **امنیت در دسترسی به دیسک و پرونده (Disk & File System Security):** در صورت تنظیم سیاست های امنیتی می توان دسترسی کاربران به برخی از پرونده ها یا دیسک ها را محدود کرد.

– **امنیت عملیات:** برای مثال نباید همه کاربران امکان تغییر تنظیمات سخت افزاری و نصب نرم افزار (Hardware & Software Installation) و یا تغییر پارامترهای مربوط به اجرای برنامه ها را داشته باشند.

– **امنیت در حوزه شبکه و اطلاعات تبادلی (Network Services)**

– **امنیت در ورود به سیستم (System Logon)**

■ **پشتیبانی از چندین پردازنده (Multi-processor):** در بیشتر اوقات لازم است تا یک سرویس دهنده در آن واحد به چندین سرویس گیرنده پاسخ دهد. برای بالا بردن قدرت پردازشی یک سرویس دهنده می توان از چندین پردازنده روی برد اصلی آن رایانه استفاده کرد. سیستم عامل شبکه باید بتواند همه پردازنده های نصب شده را شناسایی و از آنها استفاده کند.

■ **تحمل خطا (Fault Tolerance):** در صورت بروز مشکل، سرویس دهی نباید با تأخیر انجام شود. قابلیت تحمل خطا باعث می شود هنگام بروز خطا سیستم عامل از تجهیزات جایگزین استفاده کرده، بدون تأخیر یا با تأخیر بسیار کم به سرویس دهی ادامه دهد. در سیستم های با قابلیت تحمل خطا، زمان قطع شدن سرویس بسیار کوتاه بوده، عملیات جایگزینی بدون استفاده از عوامل انسانی و به صورت خودکار انجام می شود.

■ **امکان تهیه نسخه پشتیبان:** سیستم عامل شبکه باید شامل ابزارهای قوی و کاربرپسند برای ایجاد نسخه پشتیبان از تمامی پرونده‌ها و تنظیمات سیستم باشد. این ابزار باید امکان پشتیبان‌گیری از پرونده‌های در حال استفاده و مجوزهای امنیتی را فراهم کند.

■ **ابزارهای مدیریتی ساده و یکپارچه (Simple & Unified Management Tools):** سیستم عامل شبکه باید ابزارهای مدیریتی متنوع و ساده‌ای را داشته باشد تا به راحتی بتوان تنظیمات و سیاست‌های آن را تغییر داده و مدیریت کرد. استفاده از ویزاردهای مختلف جهت تغییر پیکربندی سیستم عامل می‌تواند امکان انجام تغییرات را حتی برای کاربرانی فراهم کند که دانش تخصصی رایانه‌ای ندارند.

■ **قابلیت اطمینان و پایداری (Reliability & Stability):** سیستم عامل شبکه حتی با وجود تغییرات و انجام تنظیمات مختلف باید بتواند به تمامی کاربران شبکه سرویس‌دهی کند. برای مثال زمانی که در حال تغییر پیکربندی یک سرویس در شبکه هستیم نباید این سرویس یا دیگر سرویس‌های مورد نیاز از دسترس خارج شوند.

استاندارد تجهیزات شبکه

شرکت‌ها و مؤسسات زیادی وجود دارند که تجهیزات شبکه را تولید می‌کنند. وجود این تنوع باعث می‌شود هر شرکت در رابطه با روش استفاده از رسانه انتقال یا شکل کابل یا ... نظرات مختلفی داشته باشد. با وجود تنوع تجهیزات شبکه، برای اتصال تجهیزات مختلف به شبکه و بهره‌گرفتن از همه آنها باید توافقی مشخص بین سازندگان تجهیزات شبکه وجود داشته باشد تا سازگاری آنها حفظ شود. این توافقات که مورد قبول همه شرکت‌ها و کاربران است، به استاندارد معروف است. در این استانداردها نوع رسانه انتقال، اتصالات، همبندی و سرعت انتقال مشخص شده است. استفاده از استاندارد باعث می‌شود بتوان تجهیزات ساخته شده به وسیله سازندگان مختلف را در یک شبکه به کار برد. سازمان‌های بسیاری در زمینه تهیه استانداردهای شبکه فعالیت می‌کنند. یکی از این سازمان‌ها (IEEE) (Institute of Electrical and Electronics Engineers) نام دارد که استانداردهای مختلفی را در زمینه شبکه‌های رایانه‌ای ارائه کرده است. در ابتدای دهه هشتاد میلادی کمیته IEEE برای استانداردسازی شبکه‌های اولیه شروع به کار کرد. این مؤسسه تمامی استانداردهای مربوط به شبکه‌های رایانه‌ای را با نام 802.x مشخص کرد که x عدد معرف استاندارد مورد نظر است.

استانداردهای مختلف IEEE

استاندارد Ethernet که در سال ۱۹۸۳ ارائه شد، با استفاده از پروتکل دسترسی به کانال انتقال، سرعت انتقال داده را در شبکه افزایش می‌دهد.

IEEE 802.3

در سال ۱۹۹۷ مؤسسه IEEE اولین استاندارد شبکه محلی بی‌سیم (WLAN) را تدوین کرد. این استاندارد بعدها توسعه پیدا کرد و استانداردهای a/b/g/n/ac/ad/af/ah و 802.11 مطرح شد.

IEEE 802.11

این استاندارد به نام WiMAX شناخته می‌شود و حداکثر نرخ انتقال در این استاندارد ۷۵ Mbps و برای دستگاه‌های سیار تا فاصله ۵۰ کیلومتر است.

IEEE 802.16

این استاندارد (MBWA) (Mobile Broadband Wireless Access) نام دارد که ضمن هماهنگی با دیگر استانداردهای خانواده ۸۰۲ می‌کوشد تا پیاده‌سازی شبکه‌های سیار بی‌سیم با پهنای باند وسیع (Broad band) را در سرتاسر جهان آسان کند.

IEEE 802.20

امنیت در فاوا



در دنیای فناوری اطلاعات و ارتباطات، داده‌ها و منابع اطلاعاتی سرمایه‌های باارزشی هستند که حفظ امنیت آنها بسیار مهم است. منابع اطلاعاتی همواره در معرض انواع تهدیدهای امنیتی و حملات هستند. بنابراین شناسایی انواع تهدیدهای امنیتی در دنیای فناوری اطلاعات و ارتباطات و نحوه پیشگیری از آنها برای حفظ پایداری ارتباط در شبکه ضروری است.



مفهوم امنیت

- مراد از امنیت: کنترل دسترسی
- محرمانگی، جامعیت، دسترس پذیری



غزارش رخداد و مدارک

- خطر پنهان کاری در امنیت
- پدافند غیر عامل
- مهارت های مورد نیاز برای کار در امنیت فناوری و شبکه



مدیریت خطر پذیری در سیستم

- اهمیت و روش های پشتیبان گیری
- مراحل تحلیل مخاطرات
- فهرست وارسی قبل از حمله، زمان حمله، بعد از حمله
- اهمیت مستند سازی در امنیت
- مدیریت یکپارچه تهدیدها

○ دیوار آتش چیست

اهمیت تست رخدادها در امنیت

○ سیستم های تشخیص حمله



انواع تهدیدهای فناوری

- مهندسی اجتماعی
- حمله اختلال سرویس
- امنیت در مقابل اختلال سرویس (Sniff)
- شنود



اهمیت رمزنگاری

- رمزنگاری یک طرفه (symmetric)
- رمزنگاری متقارن (asymmetric)
- و نامتقارن (asymmetric)
- گواهی دیجیتال

بشر به طور فطری نیاز به آرامش دارد و از هرآنچه که ترس او را برمی‌انگیزد دوری می‌کند. در اطراف انسان‌ها عواملی وجود دارند که جان و مال آنها را به خطر انداخته، با ایجاد ناامنی، آرامش را از آنها می‌گیرند. در شرایط ناامنی هر لحظه ممکن است این عوامل دست به کار شده، با **تهدید** و **حمله** به **دارایی‌ها** سبب خسارت شوند. انسان همیشه در این شرایط سعی کرده است تا با کنترل و کاهش این عوامل ناامنی از به خطر افتادن آرامش خود جلوگیری کند و **امنیت** را به وجود آورد. با تغییر و تحول در عوامل ناامن‌کننده موجود، ممکن است عوامل جدیدی ایجاد شود به همین علت حفظ امنیت نیاز به مراقبت مداوم و همیشگی دارد.

در دنیای فناوری اطلاعات و ارتباطات دو نوع دارایی وجود دارد:

۱ داده‌ها و اطلاعات

۲ منابع: هر بخش فیزیکی یا مجازی که داده‌ها و اطلاعات به شمار نیاید.



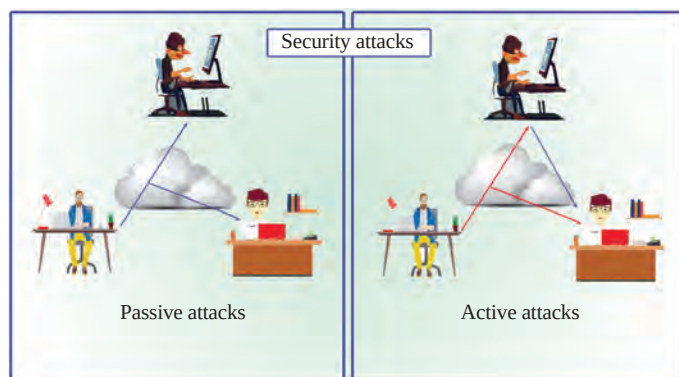
هر عامل ناامنی ممکن است دارایی‌های ما را تهدید کند و هنگامی که این تهدید عملی شود حمله به دارایی‌های ما رخ داده است.

عامل ناامنی ← تهدید ← حمله

در دنیای فناوری اطلاعات و ارتباطات دو نوع حمله وجود دارد:

۱ فعال: در حمله فعال، تغییر در دارایی و یا خسارت وارد شده به وضوح حس می‌شود و قابل مشاهده است.

۲ غیرفعال: در حمله غیرفعال، به داده‌ها دسترسی غیرمجاز صورت گرفته است؛ اما در دارایی‌ها تغییر ظاهری یا خسارتی ایجاد نشده است، حتی ممکن است اثری از حمله دیده نشود.



محرمانگی (Confidentiality)، جامعیت (Integrity) و دسترسی پذیری (Availability) به عنوان سه هدف مهم از اهداف مورد نظر در امنیت محسوب می شوند (شکل ۱).



شکل ۱- مثلث امنیت

محرمانگی عبارت است از اینکه اطلاعات حساس در دست افراد غیرمجاز قرار نگیرد. این کار با کنترل دسترسی افراد انجام می شود و فقط به افراد مجاز اجازه دسترسی به اطلاعات داده می شود. برای مثال استفاده از گذرواژه برای ورود به تلفن همراه، به منظور افزایش سطح محرمانگی اطلاعات شخصی است.

دسترسی پذیری به این معنا است که افراد بتوانند به اطلاعات یا دارایی های خود در شرایط و مکان های مختلف دسترسی داشته

باشند. برای مثال فرض کنید شما مقداری پول در یک حساب بانکی دارید. اگر برداشت از حساب بانکی فقط از شعبه خاص، در مکانی خاص و به وسیله شخص شما ممکن باشد، ظاهراً امنیت بالا است؛ اما دسترسی پذیری به پولتان برای شما کم است. اکنون فرض کنید در مسافرت هستید و به پول نیاز دارید، با اینکه پول دارید و جای پول شما هم امن است، اما چون در لحظه نیاز به این پول دسترسی ندارید، آرامش شما در آن لحظه از بین می رود و امنیت کم می شود.

جامعیت یا یکپارچگی به قابل استناد بودن اطلاعات گفته می شود. فرض کنید برای خرید از یک فروشگاه از کارت بانکی استفاده کرده اید. بعد از انجام مراحل و تعیین مبلغ، کلید تأیید را فشار می دهید. دستگاه کمی منتظر مانده، سپس پیامی ظاهر می شود که تراکنش ناموفق بوده است. هم زمان پیامکی دریافت می کنید که پول از حساب شما کسر شده است. در این حالت که در اطلاعات خدشه ایجاد شده است یا اعتبار ندارد، گفته می شود جامعیت اطلاعات دچار مشکل شده است.

مراحل کار در حفظ امنیت

فعالیت های ما در برابر حملات به سه بخش پیش از حمله، زمان حمله و پس از حمله تقسیم می شود. در فعالیت های پیش از حمله سعی می شود تا امکان تهدید و حمله کاهش داده شده یا حذف شود. این مرحله مهم ترین و اصلی ترین بخش امنیت سیستم ها به شمار می آید که اگر این بخش انجام نشود دو بخش بعدی هیچ سودی نخواهد داشت.

بیشترین تلاش ما در زمان حمله باید بر تشخیص حمله و توقف آن باشد. توقف حمله از طریق شناسایی سریع، تشخیص شیوه حمله و از بین بردن نقاط ضعف موجود انجام می شود.



شکل ۲- چرخه فعالیت ها برای حفظ امنیت

فعالیت های پس از حمله شامل بررسی شیوه حمله، تعیین خسارت، بازیابی سیستم، تهیه گزارش و پیشنهادهای لازم برای تکرار نشدن حمله است. اطلاعات و نتایج این بخش برای رفع ناامنی موجود ضروری است. پس از این بخش می توان دوباره به مرحله پیش از حمله وارد شد. حفظ امنیت یک فرآیند همیشگی و پیوسته از فعالیت های پیش، هم زمان و پس از حمله است (شکل ۲).

کنترل دسترسی

یکی از فعالیت‌های پیش از حمله، کنترل دسترسی است. کنترل دسترسی به این معناست که بتوان مشخص کرد چه کسی به چه مواردی دسترسی داشته باشد. کنترل دسترسی در رسیدن به هدف محرمانگی بسیار حائز اهمیت است. کنترل دسترسی شامل سه بخش **احراز هویت** (Authentication)، **اعتبارسنجی** (Authorization) و **حسابرسی** (Accounting) است.

مثال: فرض کنید برای یک بازی آنلاین، نام کاربری و گذرواژه خریده‌اید. هنگامی که می‌خواهید به تارنمای بازی وارد شوید، این نام کاربری و گذرواژه را وارد می‌کنید. این کار را احراز هویت می‌نامند که در واقع کنترل ورود و خروج است. پس از ورود به تارنما، با توجه به نوع کاربری که دریافت کرده‌اید برخی بازی‌ها را می‌توانید انجام دهید و به برخی دیگر اجازه دسترسی ندارید. این که پس از ورود چه مجوزهایی دارید، اعتبارسنجی است. با توجه به هزینه پرداختی، نام کاربری و گذرواژه‌ای که به شما داده شده است، تارنمای بازی به شما اجازه بازی به مدت ۳۰ روز را می‌دهد. به این محاسبه تعداد بازی‌ها و میزان حضور شما در تارنمای بازی، حسابداری می‌گویند.

اهمیت قطعات اطلاعاتی در امنیت فناوری

شما مسئول رایانه یک شرکت هستید. این شرکت برنامه حسابداری و کنترل حضور و غیاب دارد. **رخداد اول:** برنامه نشان می‌دهد که در روزهای کاری، حسابدار وارد برنامه حسابداری شده است. آیا این یک اتفاق غیرعادی است؟

رخداد دوم: در برخی از زمان‌ها برنامه حضور و غیاب نشان می‌دهد که حسابدار وارد شرکت نشده است. آیا امنیت فناوری مانند یک تصویر بزرگ در نظر گرفته می‌شود. اگر هر قطعه اطلاعات مانند یک نقطه از این تصویر فرض شود، معنای خاصی نمی‌دهد و در ظاهر تک تک این قطعه‌ها بی‌معنا و کم اهمیت هستند؛ اما وقتی این نقطه‌ها کنار هم قرار می‌گیرند، معنا پیدا می‌کنند و به یک تصویر مهم تبدیل می‌شوند. اگر بتوان قطعه‌های مناسب را جمع‌آوری کرد، ممکن است از یک نقطه ضعف یا خطر مهم آگاه شد.

انواع تهدیدهای فناوری اطلاعات و ارتباطات

اکنون سؤال این است که ناامنی در دنیای فناوری اطلاعات و ارتباطات به چه دلیل رخ می‌دهد؟ در واقع غفلت یا اشتباه در یکی از مراحل کار باعث ناامنی می‌شود. این اشتباه ممکن است در مراحل تولید یک نرم‌افزار، ساخت سخت‌افزار، فرستادن اطلاعات یا حتی با پاسخ به یک تماس تلفنی بدون بررسی هویت فرد تماس‌گیرنده رخ دهد.

مهندسی اجتماعی

شرکتی برای مشتریان خود حساب اینترنتی با امکان واریز پول به حساب باز کرده است. امروز یکی از مشتریان با پشتیبانی تماس گرفت و اعلام کرد گذرواژه خود را فراموش کرده است و امکان دسترسی به حساب خود را ندارد. از آنجایی که این مشتری گردش مالی زیادی دارد، برای شرکت جلب رضایت او از اهمیت زیادی برخوردار است. اکنون شما به عنوان کارشناس امنیت چه تصمیمی می‌گیرید و چه کاری انجام می‌دهید؟

اتفاق ماه گذشته: در ماه قبل یک مشتری ادعا کرده بود گذرواژه خود را فراموش کرده است؛ بنابراین گذرواژه جدیدی برای او تنظیم شد. روز بعد مشتری تماس گرفت که چرا نمی‌تواند وارد حساب خود شود! گذرواژه مجدد تغییر کرد و بعد از ورود به حساب خود ادعا کرد حسابش خالی است! با او در مورد تغییر گذرواژه روز قبل صحبت شد و او اظهار بی‌اطلاعی کرد!

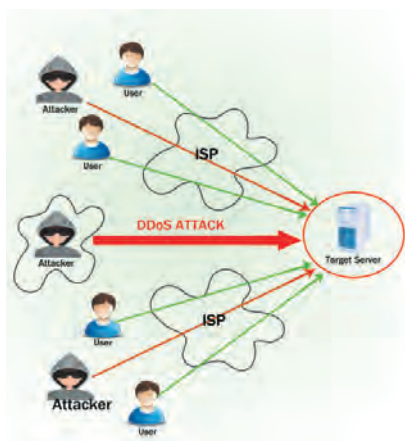
در دنیای فناوری ممکن است افرادی با دروغ بخواهند دیگران را فریب دهند. آنها معمولاً با اطلاعات کمی که قبلاً به دست آورده‌اند سعی می‌کنند با افراد ارتباط برقرار کرده، بر اساس علایق آنها رفتار و اعتمادشان را جلب کنند تا به هدف خود برسند. این سارقان بر اساس روابط اجتماعی از فرصت‌های ارتباطی با افراد سوءاستفاده کرده، به نوعی ذهن طرف مقابل را مهندسی می‌کنند. این فرآیند به **مهندسی اجتماعی** معروف است. بعضی اوقات مهندسی اجتماعی برای کسب اطلاعات بیشتر در مرحله بعدی صورت می‌گیرد. برای مثال یک رایانامه به شما اعلام می‌کند در یک مسابقه برنده شده‌اید و برای دریافت جایزه، باید فرم اطلاعات شخصی خود را پر کنید. شما این کار را بدون خطر می‌دانید! پس فرم را بدون بررسی بیشتر پر می‌کنید، غافل از اینکه فردا یک نفر با داشتن اطلاعات شخصی شما با شرکت تماس می‌گیرد و با دادن آن اطلاعات، درخواست تغییر گذرواژه شما را می‌دهد!

بهترین راه برای مقابله با مهندسی اجتماعی این است که برای انجام کارها مراحل مشخصی تعریف شود و همه موظف به رعایت آن باشند تا خطر سوءاستفاده از بین برود.



در پایان وقت اداری، ناگهان یک حافظه فلش کنار میز خود مشاهده می‌کنید! روی برچسب آن، عبارت «فیلم‌های جدید» نوشته شده است و به نظر می‌رسد پر از فیلم است. کنجکاو شده‌اید که بدانید داخل حافظه فلش چیست؟ رایانه شرکت روشن است، کار هم تمام شده است و شاید فرصت مناسبی باشد تا حافظه فلش را بررسی کنید! برای یافتن صاحب آن هم شاید لازم باشد محتویاتش را مشاهده کنید. در این موقعیت چه می‌کنید؟ آیا فلش را بررسی می‌کنید؟

یکی از روش‌های نفوذ به سیستم‌ها، ایجاد یک برنامه مخرب روی یک حافظه فلش یا لوح فشرده است. معمولاً کاربران با روش مهندسی اجتماعی فریب داده می‌شوند و این برنامه‌ها را اجرا می‌کنند و با اجرای این برنامه‌های مخرب، رایانه کاربر در اختیار مهاجم قرار می‌گیرد. البته مشکل اصلی مهاجم این است که چطور کاربر را تحریک کند تا حافظه فلش یا لوح فشرده را باز کند. آیا پیشنهادی دارید؟



حمله اختلال سرویس (DoS)

هر خدمتی محلی از شروع تا پایان دارد که به آن خدمت، سرویس و به انجام آن خدمت، سرویس‌دهی می‌گویند. هزینه و زمان لازم برای انجام سرویس با توجه به شرایط مختلف متفاوت است. کاهش سرعت دریافت خدمت به هر دلیلی را اختلال سرویس می‌گویند. بدترین حالت اختلال سرویس، نقص یا توقف کامل یک خدمت است. دلیل اختلال سرویس ممکن است عمدی یا غیرعمدی باشد. این دلیل می‌تواند ناشی از یک اتفاق ساده مانند قطع برق، رخداد طبیعی یا یک تصمیم اشتباه باشد. اما در هر صورت

وقتی که سرویس‌دهی درست انجام نشده باشد، اختلال سرویس رخ داده است.

برای مثال فرض کنید تارنمایی بخواهد برای ۶۰۰ نفر کارنامه اعلام کند. توان تجهیزات تارنما نمایش ۱۰ کارنامه در دقیقه است. تارنما به صورتی طراحی شده است که ابتدا صفحه ورود مشخصات نمایش داده می‌شود و پس از فشردن کلید جست‌وجو، پردازش لازم انجام شده، کارنامه مشاهده می‌شود. اگر افراد با نظم و به نوبت برای مشاهده کارنامه اقدام کنند، زمان کار تجهیزات برای اعلام همه نتایج در حدود ۶۰ دقیقه معادل یک ساعت خواهد بود؛ اما اگر تمام افراد بخواهند در همان شروع اعلام نتیجه همزمان وارد تارنما شوند ازدحام رخ می‌دهد، حتی ممکن است تا چند ساعت صفحه اول تارنما هم باز نشود و در عمل برای مدتی اختلال سرویس رخ دهد. این اختلال سرویس غیرعمدی است و با افزایش توان تجهیزات یا زمان‌بندی افراد برای مراجعه به تارنما قابل پیشگیری است.

اما کارها همیشه به همین خوبی پیش نمی‌رود. فرض کنید فردی یک برنامه مخرب نوشته است که با ارسال درخواست‌های مکرر به تارنمای ذکر شده در مثال بالا، صفحه اول آن را چند هزار بار در دقیقه فراخوانی می‌کند. به ظاهر کار خطرناکی صورت نگرفته و آسیبی به دستگاه‌ها و تارنما وارد نشده است؛ اما تارنمای موردنظر به طور مداوم در حال نمایش صفحه اول و پاسخگویی به درخواست برنامه مخرب است که باعث می‌شود هیچ یک از کاربران دیگر موفق به مشاهده صفحه اول تارنما یا دریافت کارنامه خود نشوند. این یک مثال از حمله اختلال سرویس (Denial of Service) است.

مدیر شبکه با تشخیص حمله اختلال سرویس، برای اینکه حمله صورت گرفته از بین برود و کارها به حالت عادی بازگردد، می‌تواند دسترسی آن فرد و برنامه مخرب را قطع کند.

اکنون فرض کنید این فرد برنامه‌ای را که نوشته است، مانند یک ویروس در تمام رایانه‌های یک شهر پخش کند و این رایانه‌ها به طور همزمان به تارنمای موردنظر درخواست ارسال کنند، در این مورد با حمله اختلال سرویس توزیع شده (DDoS (Distributed Denial of Service)) روبه‌رو هستیم که متأسفانه این نوع حمله به راحتی قابل رفع نیست.

بیشتر دانشگاه‌ها انتخاب درس در هر نیم‌سال تحصیلی را به صورت اینترنتی انجام می‌دهند. معمولاً دانشگاه‌ها، افراد را بر اساس حروف الفبا یا سال ورود به دانشگاه، در روزهای متفاوتی ملزم به انجام این کار می‌کنند. دلیل این زمان‌بندی چیست؟

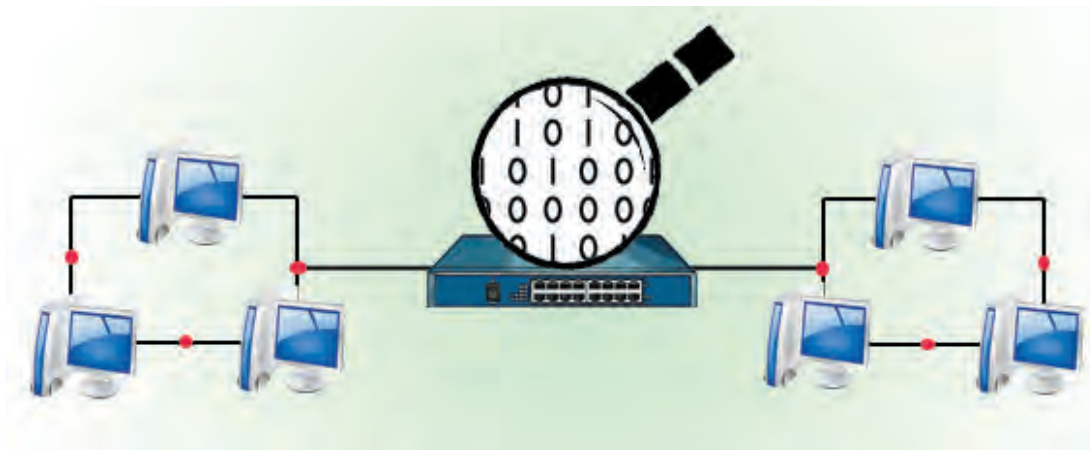
امنیت در مقابل اختلال سرویس

فرض کنید برای دیدن بازی فوتبال به ورزشگاه رفته‌اید. برای ورود نیاز به ارائه بلیت است. این موضوع باعث کاهش سرعت ورود به ورزشگاه و ایجاد صف شده است. در این بازی علاوه بر دریافت بلیت قرار است برای جلوگیری از ورود اشیاء ممنوعه، افراد بازرسی شوند. آیا بهتر نیست برای جلوگیری از تجمع و ایجاد صف، بررسی بلیت ورود به ورزشگاه یا وسایل ممنوعه هنگام ورود انجام نشود؟

روان‌ترین و سریع‌ترین روش انجام کارها این است که هیچگونه امنیتی بررسی نشود. اما هرگاه لازم باشد امنیت حفظ شود، باید کنترل‌هایی صورت بگیرد که این کنترل‌ها، هزینه اضافی یا اختلال در انجام کار خواهند داشت. این هزینه‌ها و اختلالات، خود نوعی اختلال سرویس به‌شمار می‌آیند. به همین دلیل باید مراقب بود که امنیت تا جایی اضافه شود که باعث توقف یا اختلال در کار اصلی نشود. نقطه تعادل میان سطح امنیت و اختلال سرویس برای هر کار بر اساس اهداف، حساسیت و اهمیت آن کار متفاوت است و تشخیص این نقطه تعادل از وظایف مهم یک کارشناس امنیت است.

شنود (Sniff)

هنگامی که دو نفر با تلفنی صحبت می‌کنند، اگر شخص سومی بتواند به هر روشی حتی داشتن یک تلفن دیگر روی خط، صدای آنها را بشنود در واقع **شنود** انجام داده است. در دنیای شبکه شنود به شکل دیگری هم رخ می‌دهد. برای مثال هنگامی که برای ورود به یک تارنما، نام کاربری و گذرواژه وارد می‌شود، در واقع نام کاربری و گذرواژه ارسالی به صورت بسته‌های اطلاعاتی به تارنمای مورد نظر فرستاده می‌شود. ممکن است فرد دیگری روی شبکه دستگاهی نصب کرده باشد که از هر بسته اطلاعاتی که از شبکه عبور می‌کند یک نسخه تهیه کند. اکنون این فرد نام کاربری و گذرواژه شما را می‌داند!

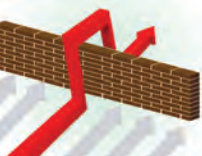


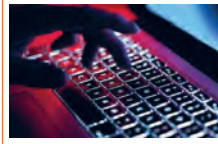
به برداشت غیرمجاز اطلاعات در یک ارتباط، بدون اطلاع فرستنده و گیرنده، شنود گفته می‌شود.

در جنگ تحمیلی فرمانده‌های ایران برای هماهنگی با مرکز فرماندهی با دستگاه بی‌سیم تماس داشتند. دشمن هم برای اینکه بتواند از فرمان‌های پایگاه اصلی مطلع شود، سعی می‌کرد با دستگاه بی‌سیم مشابه به مکالمه‌ها گوش کند. برای اینکه این اتفاق رخ ندهد، افرادی که با بی‌سیم‌ها کار می‌کردند آموزش‌های ویژه‌ای می‌دیدند. آیا می‌توانید یکی از این آموزش‌ها را حدس بزنید؟

شنود در دنیای فناوری اطلاعات و ارتباطات غیرقابل اجتناب است. برای مثال وقتی با تلفن همراه هوشمند یا رایانه قابل حمل به صورت بی‌سیم به اینترنت متصل هستید، چه بخواهید و چه نخواهید امواج دستگاه بی‌سیم در فضای اطراف شما پخش می‌شود و افرادی که در نزدیکی خانه شما هستند می‌توانند این امواج را دریافت کنند. در مثالی دیگر وقتی شما نام کاربری و گذرواژه را در یک تارنمای اینترنتی وارد می‌کنید، در مسیر بین شما و تارنمای مورد نظر، بسته‌های اطلاعاتی از دستگاهی به نام مسیریاب (Router) عبور می‌کنند، این دستگاه به راحتی امکان ذخیره و شنود این بسته‌ها را دارد و هیچ تضمین صد درصدی وجود ندارد که بسته‌ها در دنیای اینترنت از مسیریاب‌های دشمن شما عبور نکنند.

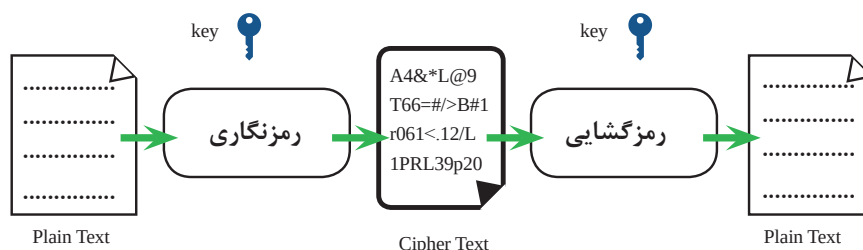
خطرهای امنیتی بر اساس ملاک‌های مختلف قابل دسته‌بندی است؛ اما به صورت کلی با توجه به منبع اصلی اشتباه، موارد زیر را می‌توان نام برد:

ریشه و پایه تهدید	شرح و خلاصه
مهندسی اجتماعی 	در میان این دسته‌بندی شاید بتوان گفت خطرناک‌ترین و غیرقابل کنترل‌ترین نوع، همان تهدیدهای مهندسی اجتماعی است. زیرا عامل اصلی در آن، اشتباه نیروی انسانی است که غیرقابل پیش‌بینی است و گستردگی تهدید نیز غیرقابل اجتناب است. به همین دلیل خبر انواع حملات مهندسی اجتماعی هر روزه در رسانه‌ها دیده می‌شود.
بدافزاری 	بدافزار یک برنامه برای خرابکاری است. بدافزارها بر اساس شیوه کار، روش ورود به رایانه، نوع تکثیر و نوع خسارت به انواع مختلفی تقسیم می‌شوند. یکی از مثال‌های معروف بدافزارها اسب تروا (Trojan) است. این برنامه در ظاهر به صورت یک برنامه مفید و کار راه‌انداز به کاربر داده می‌شود ولی در عمل ممکن است رایانه قربانی را تحت کنترل بگیرد یا اطلاعات حساس را سرقت کند.
شبکه 	به قراردادهایی که برای هماهنگی کار شبکه‌ها طراحی شده است، پروتکل گفته می‌شود. تهدیدهای بر پایه شبکه در واقع تهدیدهایی هستند که ریشه در پروتکل‌های شبکه‌ها دارند. به عنوان نمونه می‌توان به حمله اختلال سرویس روی پروتکل عیب‌یابی شبکه (ICMP) اشاره کرد. پروتکل‌های عیب‌یابی برای بررسی و رفع اشکالات شبکه ساخته شده‌اند؛ اما اگر تعداد زیادی پیام عیب‌یابی به یک تارنما فرستاده شود، آن تارنما متوقف می‌شود و کاربران نمی‌توانند با آن کار کنند و اختلال سرویس رخ خواهد داد.

ریشه و پایه تهدید	شرح و خلاصه
ساختار نرم افزارها 	این نوع تهدیدها به شیوه کارکرد نرم افزارها بستگی دارند. به عنوان نمونه شما برنامه‌ای را برای کنترل رایانه از راه دور نصب می‌کنید. این یک امکان مفید است؛ اما اگر این نرم افزار، ایراد یا ضعف امنیتی داشته باشد ممکن است حمله‌کننده بتواند رایانه شما را از راه دور کنترل کند.
ساختار سخت افزار (فیزیکی) 	برخی سخت افزارها نقاط ضعف دارند. برای مثال هنگامی که یک کلید را در یک صفحه کلید معمولی فشار می‌دهید، با فشار دادن کلید، یک ضربه مغناطیسی ایجاد می‌شود که شبیه به صدای ضربه‌ای است که روی طبل زده می‌شود و به صورت امواجی در فضا منتشر می‌شود. این امواج فقط با دستگاه‌های قوی و در فاصله‌ای خاص قابل دریافت هستند که از طریق آنها می‌توان مشخص کرد کدام کلید فشرده شده است. فرض کنید کاربر در حال ورود گذرواژه بوده است. به همین دلیل برای مکان‌ها و رایانه‌های حساس نباید از هر صفحه کلید معمولی استفاده کرد.

اهمیت رمزنگاری

در هر ارتباطی حداقل سه بخش وجود دارد: فرستنده اصلی پیام، مسیر (Channel) ارتباطی، گیرنده اصلی پیام. فرستنده یک **پیام ساده** (PlainText) را با انجام مراحل، رمزنگاری (Encryption) می‌کند. اکنون فرستنده این **متن رمز شده** یا اصطلاحاً کدشده (CipherText) را روی **کانال ارتباطی** می‌فرستد. گیرنده متن کدشده را دریافت می‌کند. در همین زمان دشمن روی کانال ارتباطی در حال شنود است و متن کدشده را دریافت می‌کند! اما متن دریافتی برای دشمن مفهومی ندارد چون کلید معما را ندارد! ولی گیرنده اصلی کلید را دارد و با انجام مراحل **رمزگشایی** (Decryption) روی متن کدشده، دوباره متن ساده را از آن به دست می‌آورد (شکل ۳). در واقع همه گیرنده‌ها چه گیرنده اصلی و چه دشمن پیام را دریافت می‌کنند؛ اما فقط افرادی می‌توانند مفهوم آن را درک کنند که **کلید رمزنگاری** را دارند.



شکل ۳- رمزنگاری پیام

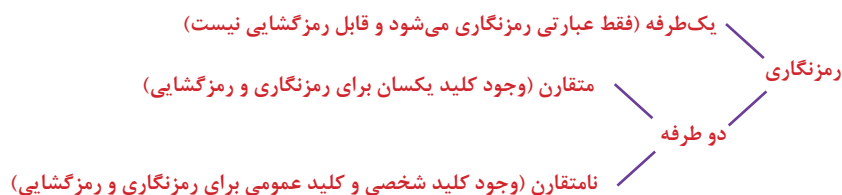
اصل مهم امنیت فناوری اطلاعات و ارتباطات : همیشه فرض کنید کانال ارتباطی در حال شنود است! بنابراین قبل از فرستادن اطلاعات باید رمزنگاری را فعال کنید تا اطلاعات به صورت رمز شده فرستاده شوند. به این کار **امن کردن کانال** ارتباطی می‌گویند و همیشه قبل از فرستادن باید کانال ارتباطی را امن کرد.



برای خرید یک قفل به مغازه‌ای مراجعه کرده‌اید. فروشنده به شما یک ردیف قفل نشان داده است تا یکی را انتخاب کنید. اما همه قفل‌ها مشابه یکدیگر هستند! پس چه تضمینی وجود دارد که قفل خریداری شده به وسیله فرد دیگری باز نشود؟ آیا مشابه بودن قفل‌ها سبب خطر باز شدن آنها به وسیله دیگران می‌شود؟

در معمایی که حل کردید روش رمزنگاری "جابه‌جایی حرف" است و کلید آن ۱ است. یعنی هر حرفی به اندازه ۱ حرف بعدی تعویض شده، فرستاده می‌شود. گیرنده هم آن را دریافت می‌کند و با همان روش یعنی جابه‌جایی حرف و با داشتن کلید یعنی یک حرف جابه‌جایی، متن اصلی را به‌دست می‌آورد. پس واژه maher به nbifs تبدیل می‌شود. البته ممکن است شما کلید ۲ را انتخاب کنید در این صورت واژه maher با جابه‌جایی با ۲ حرف به ocjgt تبدیل می‌شود.

این روش یکی از قدیمی‌ترین و البته ساده‌ترین روش‌های رمزنگاری است که در تاریخ بشر ثبت شده است. امروزه با سرعت و توانایی رایانه‌ها، کلید رمز این روش به راحتی کشف می‌شود و باید روش‌های پیشرفته‌تری را به کار برد. علم ریاضی در این موضوع به کمک فناوری آمده و روش‌های بسیار جالبی را اختراع کرده است. تمام سازندگان وسایل ارتباطی، روش‌ها را می‌دانند و از آن استفاده می‌کنند. فرستنده و گیرنده روش رمزنگاری را می‌دانند و حتی دشمن هم روش رمزنگاری را می‌داند! تنها چیزی که محرمانه است **کلید** رمزنگاری است. هر چه کلید رمزنگاری پیچیده‌تر و بزرگ‌تر باشد، شکستن رمز سخت‌تر می‌شود. پس بسیار مهم است که کلید رمزنگاری فاش نشود. انواع رمزنگاری در شکل زیر آمده است.



شکل ۴- انواع رمزنگاری

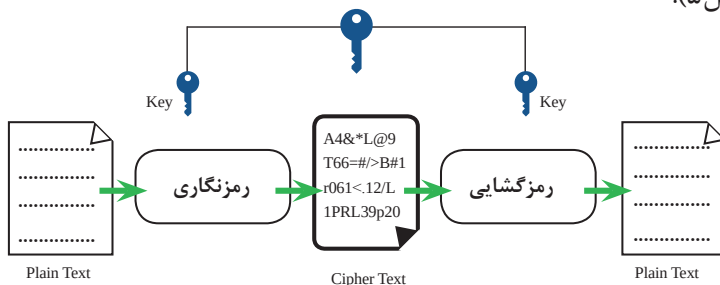
رمزنگاری یک طرفه و کاربرد آن

رمزنگاری‌هایی که تاکنون گفته شد دوطرفه و بازگشت‌پذیر بوده است. یعنی متن معمولی به متن گذشته رمزنگاری می‌شود و متن گذشته نیز دوباره می‌تواند با کلید رمزگشایی، به متن معمولی برگردانده شود؛ اما در رمزنگاری یک طرفه، متن معمولی به صورتی رمز می‌شود که دیگر نتوان از آن متن اصلی را به‌دست آورد. رمز نگاری یک طرفه غیر قابل بازگشت است.

چرا تارنماهای مختلف پیشنهاد می‌کنند برای گذرواژه حتماً از ترکیب حروف بزرگ و کوچک، ارقام و چند علامت استفاده کنید و طول گذرواژه هم کمتر از ۱۰ نویسه نباشد؟

رمزنگاری متقارن (Symmetric) و نامتقارن (Asymmetric)

برای رمزنگاری و رمزگشایی دو طرفه، کلید لازم است. اگر کلید فرستنده و گیرنده اصلی یکسان باشد به آن **رمزنگاری متقارن** گفته می‌شود (شکل ۵).

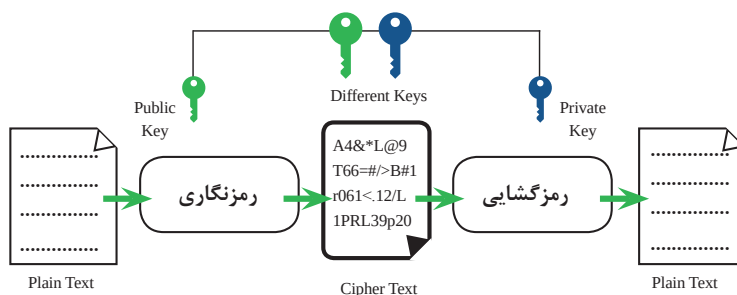


شکل ۵- رمزنگاری متقارن

دانا و بینا می‌خواهند برای ارسال پیام، کانال ارتباطی را امن کنند. برای این کار می‌خواهند از روش رمزنگاری متقارن استفاده کنند. دانا چگونه باید کلید اصلی را به بینا برساند؟ یک مشکل جدی، رساندن کلید به طرف دیگر است! دقت کنید که اگر قرار باشد فرستنده، کلید را روی کانالی که هنوز رمزنگاری نشده است برای گیرنده ارسال کند، دشمن هم کلید را می‌بیند! پس ادامه کار دیگر چه فایده‌ای دارد! برای ارسال محرمانه کلید نیاز به کانال امن دارید و برای داشتن کانال امن ابتدا باید کلید رمزنگاری یکسان در فرستنده و گیرنده داشته باشید! (داستان مرغ و تخم مرغ!)

این موضوع به ظاهر ساده، یکی از بزرگترین مشکلات دنیای رمزنگاری بوده است و حتی در جنگ جهانی دوم هم باعث تغییر سرنوشت چند جنگ مهم شده است زیرا باید به روشی کلید به گیرنده‌ها می‌رسید و مدیریت فرستادن کلیدها سخت بود و روش فرستادن به راحتی فاش می‌شد.

تنها راه حل ممکن، استفاده از دو کلید متفاوت است! یک کلید نزد فرستنده بماند و یک کلید به طرف مقابل فرستاده شود. به کلیدی که نزد فرستنده است کلید خصوصی (Private Key) و به کلیدی که برای طرف مقابل فرستاده می‌شود کلید عمومی (Public Key) می‌گویند. قانون کار این است که اگر پیام با کلید عمومی رمزنگاری شود فقط با کلید خصوصی قابل رمزگشایی و باز شدن است. این نوع رمزنگاری که در آن کلید رمزنگاری با کلید رمزگشایی متفاوت است را رمزنگاری نامتقارن می‌گویند (شکل ۶).



شکل ۶- رمزنگاری نامتقارن

تنها مسئله باقی مانده این است که چطور می‌شود کلید خصوصی و عمومی را ساخت که با یکی متن رمزگذاری و با دیگری رمزگشایی شود؟ تعدادی ریاضی‌دان شیوه انجام این کار را در سال‌های ۱۹۷۰ تا ۱۹۷۳ با استفاده از محاسبات ریاضی پیدا کردند.



شکل ۷- شنود پیام‌ها به وسیله هکر

شیوه‌های رمزنگاری خطر شنود را تا حدود زیادی کاهش داده است، اما آیا هکرها هیچ راه‌حلی برای فریب ما ندارند؟

شکل ۷ را ببینید و حدس بزنید چگونه یک هکر توانسته است با این همه رمزنگاری، پیام‌های ارسالی را کشف کند! راهنمایی: کاربر ۱ واقعا تصور می‌کند که مستقیماً با کاربر ۲ در ارتباط است!

گواهی دیجیتال

با روش‌های رمزنگاری می‌توان از طریق یک کانال ناامن کلید اصلی رمزنگاری را بدون نگرانی از لو رفتنش فرستاد. اما باز هم یک مشکل وجود دارد. ممکن است سیستمی میان ما و سیستم اصلی قرار گرفته باشد که خود را به جای سیستم اصلی جا بزند و حتی یک کانال امن برقرار کند! این سیستم همه اطلاعات ما را با این حيله مشاهده خواهد کرد! در واقع این نوع از فریبکاری فقط به یک روش قابل کشف است، آن هم وجود نفر سومی است که بتواند هویت مکانی را که به آن متصل شده‌ایم، تأیید کند. به همین دلیل در دنیای فناوری، **گواهی (Certificate)** دیجیتال ایجاد شده است.

گواهی دیجیتال یک **سند الکترونیکی** است که به وسیله مرجع صدور گواهی دیجیتال که هویت آن برای ما **تأیید شده** است صادر می‌شود و در اختیار ما قرار می‌گیرد. سیستم ما قبل از فرستادن اطلاعات به مقصد ابتدا گواهی دیجیتال مقصد را با آن مقایسه می‌کند. برای داشتن گواهی دیجیتال دو روش معمول است:

۱ گواهی دیجیتال بین‌المللی: معمولاً دارای هزینه زیاد است؛ اما به وسیله تمام سیستم‌های فناوری اطلاعات بین‌المللی قابل استفاده است.

۲ گواهی دیجیتال داخلی شرکت‌ها یا سازمان‌ها: هزینه بسیار کمتر است ولی فقط برای محدوده داخلی معتبر است و نیاز به تنظیم سیستم‌های داخلی شرکت یا سازمان مربوط دارد.

اهمیت ثبت رخدادها در امنیت

بسیاری از برنامه‌ها وقوع اتفاقات و رخدادها را در پرونده‌هایی ثبت می‌کنند. اطلاعاتی مانند زمان و تاریخ اجرا، نام برنامه و جزئیات دیگر به انتهای این پرونده‌ها اضافه می‌شوند و حتی برخی مواقع برنامه کوچک و مستقلى از برنامه‌های اصلی بدون اطلاع آنها این وقایع را ثبت می‌کند. این پرونده‌ها را **پرونده ثبت رخداد** یا به صورت خلاصه **log** می‌گویند. در مواقعی که خطا یا مشکلی در سیستم رخ می‌دهد، بررسی رخدادهای ذخیره شده در این پرونده‌ها می‌تواند روشن‌کننده داستان و حتی سرخى برای پیدا کردن مشکل و دلیل بروز آن باشند.

سیستم‌های تشخیص نفوذ



در زمان حمله، عکس‌العمل سریع می‌تواند باعث کاهش قابل توجه خسارت شود. اما عکس‌العمل سریع‌تر وقتی ممکن است که بتوانیم وقوع حمله را هر چه زودتر تشخیص دهیم. به سیستم‌های خودکاری که مدیر سیستم را از وقوع یک حمله آگاه می‌کنند، **سیستم‌های تشخیص نفوذ (IDS)** می‌گویند. سیستم تشخیص نفوذ با مقایسه شرایط عادی و غیرعادی، کاربرش را از احتمال وقوع یک حمله آگاه می‌کند. یکی از روش‌های تشخیص

حمله بررسی دائم و خودکار پرونده‌های ثبت رخداد است. اگر بتوان این پرونده‌ها را به صورت لحظه‌ای بررسی و با شرایط عادی مقایسه کرد، ممکن است بتوان از وقوع یک حمله اطلاع پیدا کرد.

سیستم‌های پیشرفته‌تر می‌توانند بعد از تشخیص حمله، عکس‌العمل مناسبی انجام دهند. سیستمی که بتواند حمله را تشخیص دهد و با عکس‌العمل مناسب جلوی حمله یا ادامه آن را بگیرد، **سیستم جلوگیری از نفوذ (IPS)** نام دارد.

دیوار آتش

در زمان‌های دور یکی از مشکلات ساحل‌نشین‌ها حمله غارتگران از دریا به ساحل بود. ساحل‌نشین‌ها برای در امان ماندن از حمله دشمنان از سمت دریا، یک راه‌حل هوشمندانه داشتند. آنها در فاصله مشخصی از ساحل مشعل‌ها و مواد سوختنی را روی آب شناور می‌کردند و در زمان حمله دشمن آتش می‌زدند! در آن زمان کشتی‌ها چوبی بود و دشمن نمی‌توانست با کشتی‌های چوبی به ساحل نزدیک شود چون کشتی خود آنها آتش می‌گرفت. با این کار گویی دیواری از آتش جلوی ورود دشمن را می‌گرفت. البته در حالت عادی این دیوار برای خروج ماهی‌گیران از ساحل به سمت دریا روشن نمی‌شد و همه چیز عادی بود. فقط وقتی فردی ناشناس می‌خواست از بیرون (دریا) به سمت داخل (ساحل) وارد شود، دیوار آتش فعال شده، جلوی ورود او را می‌گرفت.

آیا هنگام خروج از خانه، به کلیدی برای باز کردن در خانه از داخل نیاز دارید؟ آیا در خانه شما از بیرون نیز به راحتی بدون کلید باز می‌شود؟ آیا در خانه می‌تواند نوعی دیوار آتش به‌شمار آید؟



روی رایانه شما، روی مودم اینترنت یا هر جای شبکه ممکن است نرم‌افزار کوچکی وجود داشته باشد که اجازه برقراری اتصال از داخل به بیرون را بدهد؛ اما اجازه اتصال از بیرون به داخل را مسدود کند یا فقط با شرایط خاصی اجازه ورود بدهد. به این سرویس، **دیوار آتش (FireWall)** گفته می‌شود. فایروال‌های امروزی امکانات بیشتری دارند و علاوه بر ورود حتی خروج را بر اساس شرایط مختلف بررسی می‌کنند.

مدیریت خطرپذیری در سیستم



عوامل ناامنی به نوعی خطر احتمالی به‌شمار می‌آیند. کنترل یا حذف خطرها از اهداف اصلی امنیت فناوری است. به شیوه کنترل یا رفتار در برابر خطرهای احتمالی، **مدیریت خطرپذیری** گفته می‌شود. در این زمینه، اولین قدم بررسی و تحلیل **مخاطرات** است. در واقع تفاوت و کیفیت روش کار کارشناسان امنیت به سبب تفاوت **تحلیل خطر** به‌وسیله آنها است. کارشناسان امنیت ۶ مرحله برای تحلیل مخاطرات معرفی می‌کنند که باید به ترتیب انجام شود:

- ۱ تشخیص ارزش یا دارایی
- ۲ بررسی آسیب‌پذیری ارزش‌ها یا دارایی‌های مشخص شده (خطر احتمالی)
- ۳ شناسایی عامل فعال‌ساز خطر یا استفاده‌کننده از نقطه ضعف برای ایجاد خطر
- ۴ بررسی اندازه احتمال عملی شدن تهدید و خطر
- ۵ تعیین شدت تأثیر و خسارت ناشی از بروز خطر
- ۶ تدوین عکس‌العمل و رفتار مناسب در برابر خطر

دقت کنید که هر مرحله پیش‌نیاز مرحله بعد است و باید مراحل به ترتیب انجام شود. معمولاً برای شدت یا احتمال، مقادیر عددی مانند درجه یا درصد و یا کیفیتی مانند کم، متوسط یا زیاد بیان می‌شود. مرحله آخر یعنی تدوین عکس‌العمل معمولاً شامل یک یا چند رفتار است که در ۵ حالت کلی دسته‌بندی می‌شود. مدیران

سیستم‌ها معمولاً علاقه دارند پررنگ‌ترین حالت را اعلام کنند؛ ولی تقریباً در همهٔ عکس‌العمل‌ها درصدی از ۵ حالت وجود دارد:

- **اجتناب:** کارها یا روش‌هایی مانند دقت و نظارت بیشتر از وسایل در برابر احتمال سرقت که باعث می‌شود احتمال بروز خطر کمتر شود.

- **کاهش تأثیر:** روش‌هایی که در صورت بروز خطر، شدت تأثیر آن را کم‌تر کند. برای مثال پشتیبان‌گیری از اطلاعات می‌تواند اثر خطر آتش‌سوزی برای اطلاعات شرکت را تا حد زیادی کاهش دهد.

- **پذیرش:** مواقعی که جلوگیری از بروز خطر غیرممکن است و بخشی از خسارت با تمام تلاش‌ها غیرقابل اجتناب است و باید به روشی با آن کنار آمد. مانند تسویه و اتمام همکاری با تعدادی از کارکنان برای جلوگیری از ورشکستگی شرکت.

- **انتقال:** انتقال مسئولیت یا جبران خسارت به بخش یا فرد دیگر مانند بیمهٔ آتش‌سوزی یا بیمهٔ سرقت خودرو

- **بازدارندگی:** معمولاً با ایجاد رویه‌ها یا ساختارهای فیزیکی یا قانونی، احتمال یا انگیزهٔ فعال شدن عاملان خطرساز را از بین می‌برند. به عنوان نمونه وجود نگهبان یا دوربین مداربسته و موانع سخت و محکم در مقابل سرقت، انگیزه سارق را برای ارتکاب سرقت از بین می‌برد.

ردیف	عنوان دارایی	خطر برای دارایی	عامل فعال‌کننده خطر	احتمال رخ دادن (درصد / سطح)	شدت تأثیر در کار (عدد / کیفیت)	روش مقابله و عکس‌العمل در برابر خطر
۱	رایانهٔ قابل حمل	مفقود شدن، سرقت، فراموش کردن	سارق، حواس پرتی	کم	بالا	دقت و مراقبت بیشتر برای جلوگیری از سرقت
۲	اطلاعات نرم‌افزاری	ویروس، سوختن دیسک سخت	حافظهٔ فلش آلوده، نوسان برقی	متوسط	بالا	پشتیبان‌گیری از اطلاعات حساس و به‌روز رسانی ویروس‌یاب

پشتیبان‌گیری



داستان یک اتفاق: حسن در یک شرکت برنامه‌نویسی کار می‌کند. او یک رایانه داشت که تمام پروژه‌های خود را روی آن ذخیره کرده بود و برای جلوگیری از حمله‌های اینترنتی و یا ویروسی شدن، تمام پیش‌بینی‌های لازم را کرده بود. دیشب باد شدیدی وزید. حسن باخبر شد که ساختمان شرکت به دلیل طوفان و اتصال برق دچار آتش‌سوزی شده، تمام تجهیزات شرکت در آتش سوخته است! اکنون با سوختن آن رایانه، اطلاعات، پروژه‌ها و به نوعی سرمایه‌وی از بین رفته است.

آیا احتمال آتش‌سوزی، سیل یا دیگر حوادث طبیعی می‌تواند یک عامل ناامنی به‌شمار آید؟ آیا می‌توان جلوی حوادث طبیعی را گرفت؟

در برخی موارد پیش‌بینی نشده مانند حوادث طبیعی، ممکن است امکان توقف یا جلوگیری از رخ دادن آن حادثه وجود نداشته باشد. به همین دلیل بهتر است یک **نسخهٔ پشتیبان (Backup)** از دارایی‌های اطلاعاتی خود تهیه و آن را در جای امن و مناسبی حفظ و نگهداری کرد. به این کار پشتیبان‌گیری می‌گویند. در صورت بروز حادثه و از بین رفتن اصل اطلاعات، می‌توان از نسخهٔ پشتیبان اطلاعات استفاده کرد و اطلاعات را برگرداند. این کار را **بازیابی (Restore)** می‌نامند.

انواع روش‌های پشتیبان‌گیری

پروانه مسئول فناوری یک شرکت تبلیغاتی است. به طور متوسط روزی یک گیگابایت به حجم پرونده‌ها و پوشه‌های پروژه‌های مختلف شرکت افزوده می‌شود. پروانه می‌خواهد برای افزایش امنیت، پشتیبان‌گیری را انجام دهد. او می‌تواند به سه روش این کار را انجام دهد:

۱ کامل: هر روز از همه اطلاعات یک بار به صورت کامل پشتیبان بگیرد.

۲ افزایشی: هر روز فقط از تغییرات همان روز پشتیبان بگیرد.

۳ تفاوتی دوره‌ای: در یک دوره زمانی مشخص (هفته یا ماه) یک پشتیبان کامل بگیرد و در طول دوره هر روز، از تغییرات از ابتدای همان دوره پشتیبان بگیرد. این روش به نوعی ترکیبی از دو روش قبلی است. پروانه می‌خواهد بداند کدام روش برای شرایط او بهتر است. برای مقایسه سه عامل: زمان لازم برای گرفتن پشتیبان، حجم پرونده‌های پشتیبان گرفته شده و زمان لازم برای برگرداندن پشتیبان برایش مهم است.

فهرست واریسی پیش از حادثه، در زمان حادثه، پس از حادثه

یک کارشناس خبره امنیت دائماً باید چرخه ارزیابی، تحلیل و عکس‌العمل به مخاطرات را تکرار کند تا همیشه



بتواند در برابر خطرات کمترین آسیب‌پذیری را داشته باشد و به‌روز بماند. اما این سطح از تلاش، تحقیق و کار را نمی‌توان به همه افراد شرکت یا سازمان آموزش داد یا از آنها درخواست کرد که آن را انجام دهند. به همین دلیل معمولاً دستورالعمل‌هایی به صورت **فهرست واریسی**، نمونه برگ یا راهنمای مراحل انجام کارها برای پیش از اتفاق، زمان اتفاق و پس از اتفاق به وسیله کارشناسان امنیت تهیه شده، افراد موظف به انجام آن می‌شوند. این فهرست‌های واریسی از نتایج حاصل از جدول تحلیل خطرپذیری قابل استخراج هستند.

اهمیت مستندسازی در امنیت



به ثبت و نگهداری وقایع و پردازش‌ها در قالب اسناد دسته‌بندی شده، **مستندسازی** می‌گویند.

مستندسازی می‌تواند شامل تصویر، فیلم یا موارد دیگر هم باشد؛ ولی معمولاً نوشته‌ها یا یادداشت‌ها به صورت کتبی یا دیجیتال بیشترین کاربرد را دارند. هرگونه فعالیت یا تغییر در کارها باید مستندسازی شود و برخی اوقات یک اقدام مستند نشده و طبیعتاً فراموش شده ممکن است باعث به خطر افتادن کل کار شود.

گزارش رخداد و مدارک



داستان یک اتفاق ساده: ابراهیم مسئول کنترل ورود و خروج یک شرکت طلاسازی است. کارمندان شرکت برای رفت و آمد و استفاده از پارکینگ مخصوص، باید کارت داشته باشند. ابراهیم خودش مسئول ثبت و تحویل کارت‌ها است. امروز صبح ابراهیم متوجه شد کارتش را گم کرده است. او با خودش فکر می‌کند که کارت او چیز مهم و حساسی نیست و به نظر می‌رسد اگر حرفی نزد اتفاق خاصی

نمی‌افتد و برای خودش هم یک کارت دیگر برمی‌دارد. از طرفی اگر خبر گم شدن کارتش پخش شود آبروی خودش به عنوان مسئول همین کار می‌رود!

اکنون ابراهیم گم شدن کارتش را به بخش فناوری اطلاع بدهد؟

یکی از مهمترین فعالیت‌های پس از هر اتفاق نوشتن گزارش آن برای مدیر یا مسئول مرتبط در شرکت یا اداره

است. البته کارشناسان با تجربه امنیت فناوری، معمولاً نمون برگ‌هایی را تهیه می‌کنند که افراد غیرفنی نیز با پاسخ به گزینه‌ها و پرکردن آن، اطلاعات مهم یک اتفاق را ارائه کنند. این نمون برگ‌ها و گزارش‌ها معمولاً دارای ۶ بخش زیر هستند:

- ۱ مشخصات گزارش‌دهنده: معمولاً شامل اطلاعات فردی، آدرس تماس با نویسنده یا تکمیل‌کننده گزارش است.
- ۲ طبقه‌بندی و فوریت: گزارش‌ها ممکن است حساسیت بالایی داشته باشند و هر چه سریع‌تر باید به‌وسیله مدیر مربوطه بررسی شوند. بعضی اوقات هم ممکن است گزارش یا پیوست‌ها دارای گذرواژه یا اطلاعات مهمی باشند که نباید برای همه پخش شود. در این موارد باید عنوان یا درجه اهمیت یا سطح محرمانگی گزارش حتماً ذکر شود تا مدیر مربوطه بهتر و سریع‌تر بتواند تصمیم بگیرد. معمولاً شرکت‌ها یا سازمان‌ها برای محرمانگی و فوریت، سطح‌هایی مانند محرمانه، سری، فوری، عادی و... را تعریف می‌کنند.
- ۳ شرح خلاصه اتفاق: در این قسمت باید علائم ظاهری یا موارد مشاهده شده، فارغ از نظر شخصی یا قضاوت نوشته شود. جزئیات زیاد و ریز فنی بهتر است به صورت پیوست گزارش قرار داده شود و از ذکر آن در این قسمت خودداری شود. معمولاً در این شرح باید به صورت خلاصه، سریع و با کمترین کلمات، اتفاق رخ داده را اعلام کرد و دریافت‌کننده گزارش در صورت نیاز برای جزئیات به پیوست مراجعه کند.
- ۴ اعلام سطح خسارت: برآورد تقریبی خسارت احتمالی در این بخش اعلام می‌شود. این برآورد برای تصمیم‌های بعدی و سرعت رسیدگی اهمیت دارد.
- ۵ اعلان راهکار و پیشنهاد برای توقف یا کاهش خسارت
- ۶ مدارک پیوست: معمولاً یک نسخه از پرونده‌های ثبت رخداد، پرونده آلوده به بدافزار، یک نسخه از سیستم مورد حمله یا هر مورد ضروری دیگری، برای بررسی دقیق‌تر به همراه گزارش ارائه می‌شود.

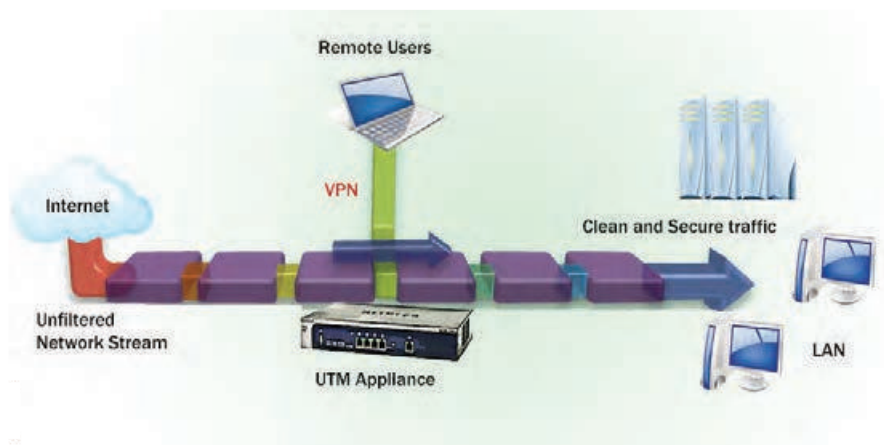
خطر پنهان کاری در امنیت

هنگامی که یک اتفاق مشکوک کوچک و به‌ظاهر کم‌اهمیت رخ می‌دهد، کارشناس یا کارمند مربوطه ممکن است احساس کند لازم نیست این اتفاق کوچک و کم‌اهمیت را اعلام کند. اما در مواقعی گزارش همان اتفاق ساده و ظاهراً کم‌ارزش، ممکن است باعث کشف یا جلوگیری از یک خطر بزرگ شود. **مخفی‌کاری** و پنهان‌کاری از اشتباه‌های بسیار خطرناک کارمندان یک شرکت در امنیت به‌شمار می‌آید و کارمندان در رابطه با محدوده کاری نباید مخفی‌کاری انجام دهند. یکی از دلایل پنهان‌کاری، **احساس کم‌اهمیت بودن** یک موضوع است. به همین دلیل کارشناس امنیت باید روال منظم و خاصی را ایجاد کند تا کارمندان اتفاق‌های رخ داده را بدون توجه به سطح اهمیت آن به مدیر یا مسئول مربوطه گزارش دهند.

خطر جدی: هر فردی که احساس کند خود یا سیستم تحت مدیریتش دارای ارزش یا اهمیت خاصی نیست، یک فرصت خوب برای نفوذگران به‌شمار می‌آید و ممکن است نفوذگران از طریق سیستم آن فرد که بدون امکانات امنیتی است، دست به حمله اصلی بزنند. این افراد معمولاً اهمیتی به رخداد‌های اطراف خود نداده، ناخواسته نوعی پنهان‌کاری را انجام می‌دهند که ممکن است باعث خسارت‌های سنگینی شود.

مدیریت یکپارچه تهدیدها (UTM)

هماهنگی و سیاست گذاری متمرکز در حفظ امنیت یکی از روش های مدیریتی است. به همین دلیل معمولا امکانات سخت افزاری و نرم افزاری ساخته شده در قالب استانداردهای مشخصی می توانند به یکدیگر متصل شده، یک سیستم یکپارچه را تشکیل دهند که به **سیستم مدیریت یکپارچه تهدیدها** (Unified Threat Management) معروف است. شرکت های مختلف سعی کرده اند سیستمی تولید کنند که بتواند تمام این امکانات را به صورت یکپارچه و متمرکز به کار بگیرد. حتی بعضی از تولیدکنندگان، تمام امکانات امنیتی مورد نظر را در قالب یک دستگاه تولید کرده اند. سیستم های مدیریت یکپارچه تهدید معمولا دارای دیوار آتش، سیستم تشخیص و توقف حمله، تحلیل گر محتویات، آنتی ویروس و موارد مشابه هستند و مزیت آنها مدیریت متمرکز برای افزایش امنیت است. در مقابل، عیب این سیستم ها این است که اگر به هر دلیل، سیستم اصلی دچار مشکل شود بلافاصله تمام بخش های دیگر و کل کار متوقف می شود.



نقطه تجمع، نقطه ای است که در مواردی مانند آتش سوزی یا اتفاقات مشابه، دیگر کارکنان یا اعضای آن مجموعه باید هر چه سریع تر در آن نقطه جمع شوند تا بتوانند مدیریت پس از حادثه را بهتر انجام دهند. این نقطه معمولا در فضای امن روباز، دور از احتمال تخریب یا ریزش و دور از مواد آتش زا یا مضر است.



پدافند غیرعامل



برای هر کشوری در دنیا، حفظ امنیت و تمامیت ارضی، جانی و مالی مردم بسیار بااهمیت است. مدل امنیت کشورها در واقع مدل بزرگی است که از تعداد زیادی زیربخش تشکیل شده است. بخش‌هایی مثل امنیت غذایی، بهداشت، آموزش، فرهنگ و موارد مشابه دیگر که از جهت حفظ امنیت دارای ابعاد بسیار متنوعی است. بعضی مواقع حوادث یا اتفاق‌هایی رخ می‌دهد که نتایج و اثرات آن مانند خسارت یک حمله نظامی است. به همین دلیل امنیت یک کشور علاوه بر نیروی نظامی به تمام بخش‌های دیگر نیز وابسته است.

مثال: فرض کنید برق تمام شهر برای یک روز قطع شود، در آن صورت سردخانه‌ها، مغازه‌ها، رایانه‌ها و هزاران بخش دیگر از کار می‌افتند. در

چنین شرایطی خسارت و ناامنی ایجاد شده از این اتفاق تا حدی ممکن است شبیه به خسارت یک حمله نظامی باشد! پس فعالیت‌ها و اقدامات لازم برای اینکه در چنین شرایطی بتوان برق شهر را از روش‌های دیگر دوباره وصل کرد، به نوعی دفاع در برابر چیزی شبیه به یک حمله است، اگر چه اصلاً موضوع نظامی نیست! در این مثال، ممکن است به روش **غیرنظامی** خسارتی به کشور ما وارد شود که به اندازه خسارت نظامی باشد! در واقع بحث از **دفاع بدون سلاح** است. به این اقدام‌ها **پدافند غیرعامل** می‌گویند. به عبارت دقیق‌تر و کامل‌تر پدافند غیر عامل عبارت است از:

مجموعه **اقدامات** غیرمسلحانه‌ای که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تسهیل مدیریت بحران در مقابل تهدیدها و اقدام‌های دشمن می‌شود. تقریباً تمام صنایع، نیروگاه‌ها و بخش‌های مهم به‌وسیله شبکه‌های رایانه‌ای اداره می‌شوند؛ بنابراین امنیت فناوری در این امور بسیار مهم است و تمام اقدامات کارشناسان امنیت فناوری به نوعی در زیرمجموعه پدافند غیرعامل قرار می‌گیرد.

مهارت‌های مورد نیاز برای امنیت فناوری و شبکه

انجام هر کاری مهارت خاص خود را نیاز دارد. برای شغل‌های مرتبط با امنیت فناوری و شبکه نیز حداقل مهارت‌هایی مورد نیاز است که در ادامه به صورت



مختصر معرفی می‌کنیم:

۱ توانایی کار با سیستم عامل لینوکس: همه برنامه‌های اجرایی روی سیستم‌عامل اجرا می‌شوند. شناخت، آگاهی و یا حتی دستکاری برنامه‌ها و خود سیستم‌عامل برای یک کارشناس امنیت فناوری بسیار ضروری است. به همین دلیل آشنایی با دنیای متن‌باز (Open Source) و به‌خصوص مهارت در استفاده از سیستم‌عامل لینوکس که کد برنامه‌نویسی آن برای همه در دسترس است، از ضرورت‌های کاری کارشناس امنیت فناوری است.

۲ **مهارت در یک زبان برنامه‌نویسی بر پایه زبان C:** سیستم‌عامل‌ها و اکثر برنامه‌ها با زبان‌هایی نوشته شده‌اند که بسیار شبیه به زبان C هستند. مانند سی‌شارپ، جاوا، پایتون، PHP و بسیاری دیگر. دانستن حداقل یکی از این زبان‌ها برای کارشناس امنیت فناوری ضروری است.

۳ **آشنایی با یک پایگاه داده:** در دنیای امروز اطلاعات، ثروت واقعی است و محل تجمع و ذخیره داده‌ها یا پایگاه داده بسیار با ارزش است. دانستن شیوه کار و استفاده از حداقل یک پایگاه داده ترجیحاً متن باز بسیار ضروری است.

علاوه بر موارد گفته شده یک کارشناس امنیت شبکه همیشه باید در حال مطالعه و تحقیق باشد. معمولاً برای آموزش ابزارهای اختصاصی و تست امنیت، دوره‌هایی در دانشگاه‌ها یا مراکز علمی برگزار می‌شود و مدارک معتبر نیز برای درج در رزومه کاری به فراگیر داده می‌شود. آموزش‌ها در دو دسته کلی هستند:

■ **دوره‌های رسمی دانشگاهی:** دانشگاه‌های معتبر در موضوع امنیت فناوری اطلاعات و شبکه، دارای رشته‌های تحصیلی رسمی هستند. ورود به این رشته‌ها معمولاً با آزمون‌های ورودی و با داشتن مدارک تحصیلی ممکن است.

■ **دوره‌های آزاد:** دوره‌های آزاد غیررسمی در همه دانشگاه‌های معتبر یا مجتمع‌های آموزشی وجود دارد که برای ورود، نیاز به مدرک یا آزمون خاصی ندارند و شرکت در آنها برای عموم علاقه‌مند به امنیت آزاد است.

Security+

CEH - Certified Ethical Hacker

CISSP - Certified Information Systems Security Professional

برنامه ریزی و مدیریت استراتژیک فناوری اطلاعات



مدیریت استراتژیک چیست؟

مدیریت راهبردی یا مدیریت استراتژیک تجزیه و تحلیل در خصوص مسایل مهم سازمان می باشد و توسط راهبران ارشد سازمان، به منظور کنترل منابع در محیط های خارج از سازمان گرفته می شود. این فرایند شامل مشخص کردن مأموریت، چشم انداز، دارایی های سازمان و توسعه برنامه ها و سیاست های سازمان است.

تعریف دیگر ارائه شده در باب مدیریت استراتژیک عبارت است از راهکارها و تصمیم هایی که قرار است به ما و سازمان ما کمک کند تا در مسیر موفقیت و دستیابی به اهداف حرکت کنیم. در تعریف ساده تر کجا هستیم و قرار است به کجا برسیم. در این مسیر مدیریت استراتژیک ما را یاری خواهد کرد و موجب تعیین عملکرد بلندمدت یک شرکت است.

ضرورت استفاده از مدیریت استراتژیک در تصمیم گیری مدیران

با نگاهی دقیق به مفهوم مدیریت استراتژیک می توان به ضرورت استفاده از آن پی برد. با توجه به تغییرات محیطی که در حال حاضر شتاب زیادی به خود گرفته است و پیچیده شدن تصمیمات سازمانی، لزوم بکارگیری برنامه ای جامع برای مواجهه با اینگونه مسائل بیشتر از گذشته ملموس می شود. این برنامه چیزی جز برنامه ریزی مدیریت استراتژیک نیست. مدیریت استراتژیک با تکیه بر ذهنیتی پویا، آینده نگر و جامع نگر راه حل بسیاری از مسائل سازمان های امروزی است.

پایه های مدیریت استراتژیک بر اساس میزان درکی است که مدیران از شرکت های رقیب، بازارها، قیمت ها، عرضه کنندگان مواد اولیه، توزیع کنندگان، دولت ها، بستانکاران، سهامداران و مشتریانی که در سراسر دنیا وجود دارند، قرار دارد و این عوامل تعیین کننده موفقیت تجاری در دنیای امروز است. پس یکی از مهمترین ابزارهایی که سازمان ها برای حصول موفقیت در آینده می توانند از آن بهره گیرند مدیریت استراتژیک خواهد بود.

جایگاه و نقش فناوری اطلاعات در سازمان

در دنیای امروز و محیط اقتصادی پویا و شدیداً رقابتی، فناوری اطلاعات توانسته است به یکی از بازیگران اصلی و مهم تبدیل گردد و جایگاه خود را تا رسیدن به یک سرمایه استراتژیک ارتقاء دهد. فناوری اطلاعات می تواند یک سازمان را به سمت نوآوری، افزایش بهره وری و تولید ارزش برای مشتریان هدایت کند و به عنوان یک مزیت رقابتی مطرح گردد. با توجه به اهمیت بی بدیل فناوری اطلاعات، بدیهی است که بکارگیری موثر آن مسائل و چالش های متعددی را نیز به دنبال داشته باشد. یکی از مهمترین چالش ها، میزان و نحوه همسوئی فناوری اطلاعات با کسب و کار است.

جایگاه و نقش فناوری اطلاعات در سازمان شما کجا است؟ آیا فناوری اطلاعات توانسته است به سازمان شما کمک کند تا به اهداف کسب و کار خود سریع تر برسد؟ تا چه میزان فناوری اطلاعات و کسب و کار زبان همدیگر را متوجه می شوند؟ تا چه میزان فناوری اطلاعات توانسته است خود را در راستای اهداف کسب و کار قرار دهد و با آن هم راستا و یا همسو باشد؟ با توجه به ماهیت پویای نیاز های کسب و کار در یک سازمان زنده، آیا فناوری اطلاعات می تواند با حضوری فعال و پویا صندلی خود را به درستی در کنار صندلی کسب و کار قرار دهد؟

جایگاه فناوری اطلاعات در یک سازمان را می توان در چهار سطح مختلف بررسی کرد.

- فناوری اطلاعات به عنوان یک عامل هزینه : فناوری اطلاعات صرفاً یک ارائه دهنده کالا (به عنوان نمونه تجهیزات جانبی) و یا سرویس های خاصی نظیر سیستم های حسابداری و مالی درون سازمان است. در چنین مواردی فناوری اطلاعات نظیر یک

بچه ضرور است که هم دوستش داریم، هم باید باشد، هم باید توان بودن آن را با کمترین هزینه پرداخت کرد و هم مزاحمت های فراوان آن را لاجرم تحمل کرد. در این سطح، فناوری اطلاعات هیچگونه تاثیری بر روی کسب و کار ندارد.

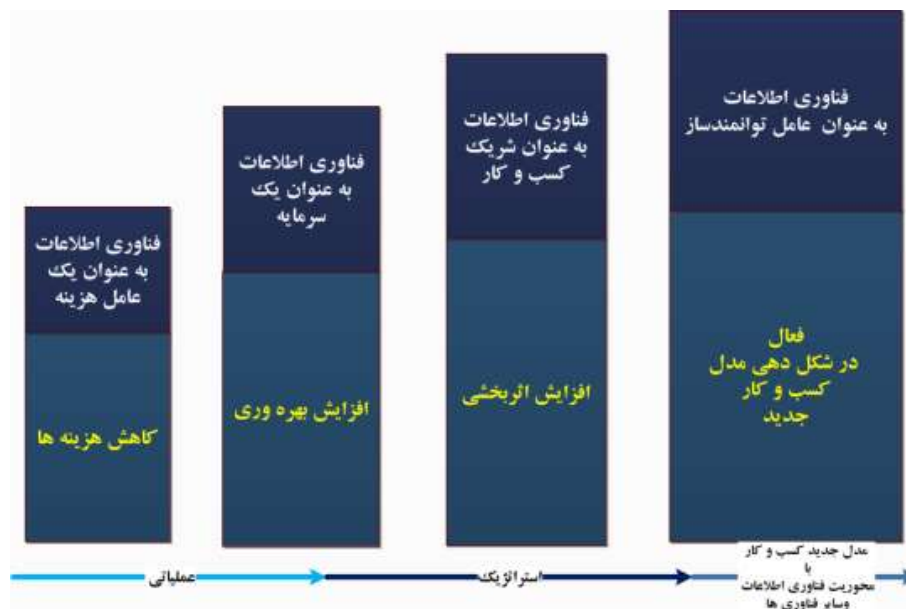
- فناوری اطلاعات به عنوان یک سرمایه : راه حل های فناوری اطلاعات به عنوان بخش لاینفک فرآیندهای اصلی کسب و کار و تحقق مسائل امنیتی و رعایت نیازهای تعریف شده قانونی در نظر گرفته می شوند. کعبه آمال نهایی فناوری اطلاعات، تعالی عملیات است و در همین راستا بیشترین تاکید را بر روی اثربخشی بیشتر و ارتقاء کیفیت در کسب و کار از طریق بهبود فرآیندهای کسب و کار و تصمیم گیری دارد. فناوری اطلاعات می بایست یک پایگاه عملیاتی مقرون به صرفه را ارائه نماید و بتواند راندمان و بهره وری کسب و کار را بهبود بخشد. در این سطح، فناوری اطلاعات برای ایجاد ارزش برای سازمان مشارکت می نماید و به نوعی در ارائه پیشنهادات لازم در این خصوص حضور پر رنگ تری دارد.
- فناوری اطلاعات به عنوان یک شریک کسب و کار : فناوری اطلاعات توسط کسب و کار به عنوان یک شریک با کلاس بالاتر که حرف های بیشتر و مهمتری برای گفتن دارد پذیرفته می شود که می توان سخن آن را در زمان تدوین استراتژی سازمانی نیز شنید و به آن ترتیب اثر داد. (نه صرفا پیشنهاد دهنده ای برای خلق ارزش و بهبود عملیات کسب و کار). فناوری اطلاعات با اعتماد به نفسی که پیدا کرده است این امیدواری را دارد که بتواند داده های ارزشمندی را برای اتخاذ تصمیمات مهم و اثربخشی عملیات (به عنوان نمونه استاندارد کردن فرآیندهای حمایت از کسب و کار) ارایه نماید. بررسی اثرات ایده ها و میزان وابستگی بین آنها در تعامل بین فناوری اطلاعات و کسب و کار از دیگر وظایف فناوری اطلاعات است. فناوری اطلاعات لازم است در عمل توانمندی خود را نشان دهد و بر اساس ساختارهای انعطاف پذیر به نیازهای کسب و کار به سرعت و مقرون به صرفه پاسخ دهد تا سازمان به استناد آنها بتواند در مسیر صحیح رو به جلو حرکت کند.
- فناوری اطلاعات به عنوان یک عامل توانمند ساز: با رشدی که فناوری اطلاعات در مراحل قبل داشته است، اعتقاد مدیران کسب و کار به آن بیشتر شده است و از وی جهت تعریف و شکل دهی مدل های جدید کسب و کار دعوت بعمل می آید. مدیران کسب و کار که دارای قابلیت پیش بینی نیازهای آتی می باشند، ظرفیت فناوری اطلاعات و سایر فناوری ها را از دریچه ای جدید بررسی می کنند و فرصت های کسب و کار جدید را به سرعت شکار می کنند. در ادامه ، ساختارهای فناوری اطلاعات به آنها کمک می کند تا به سرعت خود را با نیازهای جدید تطبیق و متعاقب آن تغییر بدون درنگ داشته باشد. فناوری اطلاعات خودش را به عنوان بخش جدائی ناپذیر از کسب و کار می بیند که می تواند ایده های کسب و کار جدیدی را از طریق قابلیت ها و ظرفیت فناوری های موجود و فناوری های نوآورانه و ابتکاری عملی سازد.

شکل ۱ ، جایگاه فناوری اطلاعات و سطوح مختلف آن را نشان می دهد.

چگونه می توان فناوری اطلاعات را با استراتژی کسب و کار همسو کرد؟

همانگونه که در شکل ۲ ، مشاهده می گردد با بکارگیری مفهومی با نام معماری سازمانی می توان بین استراتژی کسب و کار یک معماری سازمانی (Enterprise Architecture) شامل مدل های کسب و کار، فرآیندها ، داده ها، سیستم های پشتیبانی کننده، شبکه و همچنین زیرساخت های فناوری است که از آنها به منظور ترجمه استراتژی کسب و کار به نقشه راه فناوری اطلاعات استفاده می گردد.

شکل ۳ ، ارتباط بین استراتژی کسب و کار، استراتژی فناوری اطلاعات و جایگاه معماری سازمانی را نشان می دهد.



شکل ۱ : جایگاه فناوری اطلاعات



شکل ۲ : جایگاه معماری سازمانی



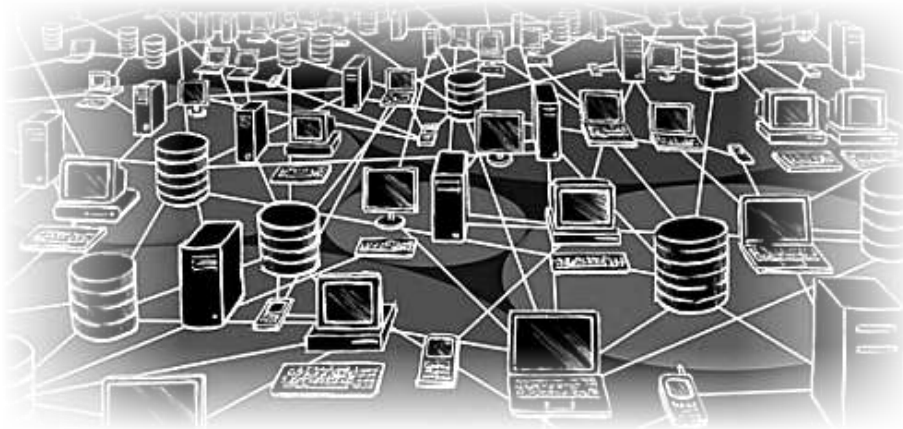
شکل ۳: ارتباط بین استراتژی کسب و کار ، استراتژی فناوری اطلاعات و جایگاه معماری سازمانی

فناوری اطلاعات و مشکلات موجود

در کنار موضوعاتی نظیر جهانی شدن، ادغام شرکت ها در یکدیگر، رقابت ها و سرعت بالای چرخه ابداع و نوآوری لازم است سازمان ها با جدیت بیشتری بر روی مدل های کسب و کار خود تمرکز نمایند و در صورت نیاز سریعاً به دنبال بازنگری اصولی آنها باشند. بپذیریم میزان چالاکی یک سازمان، توان تشخیص ضرورت تغییر و سرعت العمل در انجام تغییرات یکی از قابلیت های طلایی هر بنگاه کسب و کار در عصر حاضر است. راه حل های مبتنی بر فناوری اطلاعات، می توانند به عنوان یکی از گزینه های مهم و تاثیرگذار به منظور پاسخگویی سریع به نیازهای کسب و کار مطرح باشند به شرطی که هر چیز در جایگاه درست خود باشد و از همه مهمتر، مسیر به درستی انتخاب و طی شود.

ممکن است این موضوع مطرح شود که راه حل های مبتنی بر فناوری اطلاعات در عمل کار را مشکل تر و خود نیز عامل بروز مشکلات جدیدی برای کسب و کار شده اند. برای روشن شدن این موضوع باید به نکاتی چند اشاره کرد که به نوعی ما را به نقطه ای خواهد رساند که بتوانیم دلایل بروز چنین مسائلی را یافته و با ارایه یک راه حل، مشخص نمائیم که چگونه می توان از فناوری اطلاعات در کنار کسب و کار بطور مفید و هوشمندانه استفاده کرد.

شکل ۱، وضعیت متداول بکارگیری فناوری اطلاعات در بسیاری از سازمان ها را نشان می دهد. تغییر مستمر نیازهای کسب و کار در طول زمان باعث چشم اندازی این چنین شده است. پیچیدگی و ناهمگونی فوق در عمل، امکان واکنش سریع نسبت به تحولات بازار و نیازهای کسب و کار، مدیریت زمان و هزینه ها را غیر ممکن می سازد.



شکل ۱ : وضعیت بکارگیری فناوری اطلاعات در بسیاری از سازمان ها

وضعیت فوق بیانگر مجموعه ای از سیستم های درهم آمیخته در لایه های مختلفی نظیر فرآیندهای داخلی، فناوری ها، متدها و استانداردها است. اگر در چشم انداز فوق بر روی هر عنصر جزء متمرکز شویم، متوجه این موضوع خواهیم شد که تولد آن با یک داستان خوب آغاز شده است و در خوشبینانه ترین حالت، هم اینک نیز دارای عملکرد مناسبی است. پس مشکل کار کجا است؟

در بسیاری از سازمان ها چشم انداز فوق در طی چندین سال شکل پیدا کرده است. هر سیستم بر اساس نیاز یک بخش و یا دپارتمان خاص در سازمان ایجاد می گردید و به نوعی اولین مأموریت آن پاسخگویی به نیازهای آن بخش بود. نیازهایی که بررسی آنها در سطح کل سازمان انجام نگرفته بود و صرفاً یک بخش بخصوص را هدف قرار داده بود. بدین ترتیب ما شاهد تولد سریع سیستم هایی در سازمان ها شدیم که مهمترین وجه مشترک آنها حضور عملیاتی در بخش های مختلف یک سازمان بود. ارتباط و یا یکپارچگی

بین این نوع سیستم ها آرزویی بیش نبود و اگر هم الزامی به تحقق این چنین آرزویی بود شاهد تولد یک اینترفیس جدید برای ارتباط دو سیستم با یکدیگر بودیم. اینترفیسی که در عین مفید بودن هم یک وابستگی جدید را ایجاد می کرد و هم پای یک فناوری دیگر را به مجموعه باز می کرد.

تغییر در نیاز های کسب و کار باعث تشدید فشار بر روی گروه فناوری اطلاعات سازمان می گردید و از آنها درخواست می گردید که راه حلی برای پاسخگویی به این نیازها ارائه نمایند. پیاده کنندگان در اغلب موارد به سراغ یک راه حل مستقل جدید می رفتند و به نوعی یک سیلوی جدید به جمع جزایر اطلاعاتی در سازمان اضافه می گردید.

کارشناسان فناوری اطلاعات همواره تحت تاثیر فشار مدیریت سازمان برای پاسخگویی به نیاز ها، به سراغ ساده ترین راه حل می رفتند: پیاده سازی یک راه حل مستقل جدید دیگر و تمایل نداشتند که دست به سیستم های موجود بزنند و ضمن پایبندی به شعار "سیستمی که داره کار می کنه بهش دست نزنید"، همیشه نگران بروز فاجعه و از کار افتادن برخی سیستم ها در سازمان خود پس از اعمال کمترین تغییرات بودند.

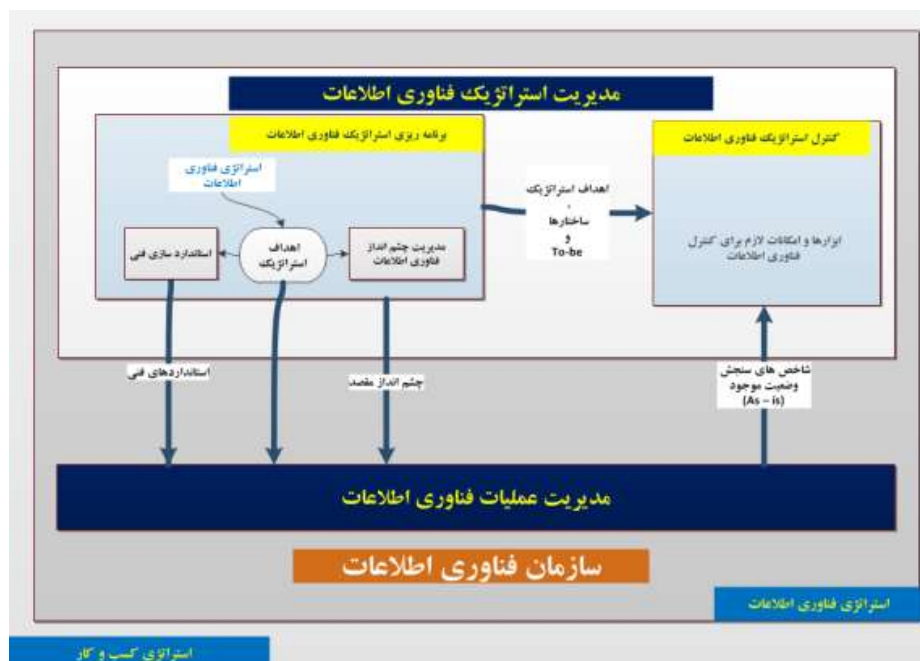
وضعیت فوق با ظهور فناوری های جدید، الزامات قانونی، انتظارات بیش تر امنیتی و تبعیت از مجموعه قوانین جدید تشدید گردید. مهمترین اثر منفی ظهور فناوری های جدید، از رده خارج شدن فناوری های قدیمی بود که به نوعی هزینه پشتیبانی و نگهداری آنان روز به روز بیش تر می گردید. چراکه بسیاری از کارکنان سازمان ها که با این فناوری های قدیمی کار می کردند به مرور زمان بازنشسته می شدند و در عمل مستندات قابل قبولی نیز برای انتقال به کارکنان بعدی وجود نداشت.

اگر بخواهیم یک جهش اصولی و منطقی در حوزه فناوری اطلاعات داشته باشیم باید فکری به حال این وضعیت آشفته و به هم ریخته کرد. **ماموریت مدیریت استراتژیک فناوری اطلاعات، پاسخ منطقی، همه جانبه و کاملاً سیستماتیک به وضعیت فوق است.**

مدیریت استراتژیک فناوری اطلاعات

مدیریت استراتژیک فناوری اطلاعات کار خود را با بررسی ساختارهای موجود در فناوری اطلاعات سازمان، نحوه تعامل با اهداف کسب و کار و میزان اثربخشی هر یک از آنها آغاز می کند. این کار محدوده و پارامترهای تاثیر گذار در مدیریت استراتژیک فناوری اطلاعات را مشخص می کند تا به کمک آن بتوان برنامه ریزی مناسب در خصوص آن چیزی که لازم است اتفاق بیافتد را انجام داد. شکل ۲، عناصر اصلی برای برنامه ریزی مدیریت استراتژیک فناوری اطلاعات را نشان می دهد.

مدیریت چشم انداز فناوری اطلاعات تمامی فرایندها جهت مستند سازی، تجزیه و تحلیل چشم انداز، نظارت و کنترل روند تکاملی و همسوئی با اهداف استراتژیک کسب و کار را شامل می شود. شناخت بهتر وضعیت کلی سازمان و این که فناوری اطلاعات چگونه می تواند به یک سازمان جهت موفقیت اهداف کسب و کار کمک نماید، یکی از مهمترین تعهدات مدیریت استراتژیک فناوری اطلاعات است. همچنین، ایجاد یک زبان مشترک بین کسب و کار و فناوری اطلاعات از دیگر تعهدات مدیریت استراتژیک فناوری اطلاعات می باشد.



شکل ۲: مدیریت فناوری اطلاعات

اکثر سازمان ها در مواجهه با فناوری اطلاعات غافلگیر شده و بنا به ضرورت و به صورت بخشی به استقرار سیستم های اطلاعاتی و فناوری اطلاعات پرداخته اند. اما به تدریج بخشهای مختلف به جزیره های اطلاعاتی که مستقیماً به طراحی، تجهیز، بهره برداری و پشتیبانی سیستم های اطلاعاتی خود اقدام می نمایند تبدیل شده اند که موجب تعامل نامناسب بین بخش های سازمان، افزایش دوباره کاری، عدم هماهنگی توسعه فناوری اطلاعات با اهداف کلان و استراتژی سازمان و ... شده است، این مضرات سازمان ها را به فکر واداشته که این جزایر سرگردان و پراکنده را تحت یک نظام واحد سازماندهی نمایند و برای فناوری اطلاعات در سازمان خود برنامه ریزی نمایند. نخستین تلاش ها به منظور برنامه ریزی و کنترل سیستم های فناوری اطلاعات در دهه های ۵۰ و ۶۰ میلادی صورت گرفت. در این سالها بیشترین بخش منابع مصرفی در توسعه نرم افزارهای کاربردی جدید و یا اصلاح نرم افزارهای موجود به کارگرفته می شد.

بنابراین در ابتدا تمرکز اصلی برنامه ریزان حول این دو محور بود. سازمان ها روش های مختلفی را برای توسعه سیستم ها و کنترل پروژه آنها برقرار نمودند که البته این فعالیت ها بیشتر در لایه برنامه ریزی عملیاتی سازمان انجام می پذیرفت. اما هر چه کاربری سازمان ها از سیستم های اطلاعاتی پیچیده تر شد تأکید و تمرکز برنامه ریزی از لایه عملیاتی به سطح برنامه ریزی مدیریتی و کنترل تخصیص منابع انتقال یافت.

برنامه ریزی استراتژیک فناوری اطلاعات برای هر سازمان، سندی است که معماری اطلاعات سازمان را در پرتو ملاحظات استراتژیک مانند مأموریت، اهداف و اولویت های سازمان تعیین کرده و برنامه اجرایی لازم برای دستیابی به سیستم ها و پایگاه های اطلاعاتی را در سطح سازمان تعیین می کند. به عبارت دیگر، برنامه ریزی استراتژیک فناوری اطلاعات منشور و برنامه کلان سازمان در زمینه سیستم های اطلاعاتی و به طور کلی، فناوری اطلاعات است.

چهار دلیل عمده برای گرایش سازمان ها به برنامه ریزی استراتژیک فناوری اطلاعات وجود دارد که عبارتند از:

- گسترش و بهبود فناوری
- کمبود نیروی انسانی متخصص
- محدودیت منابع سازمان
- پیدایش سیستم یکپارچه

برنامه ریزی استراتژیک فناوری اطلاعات با اهداف زیر تهیه میشود:

- کسب شناخت از محیط سازمان و استراتژی های آن
- تعیین استراتژی ها و سیاست های کلان فناوری اطلاعات برای پشتیبانی از مأموریت و اهداف سازمان
- تدوین معماری اطلاعاتی شامل فهرست، مشخصات و ارتباط سیستم های اطلاعاتی
- تعیین نیازهای اجرایی عمده برای توسعه و اجرای سیستم های اطلاعات در سازمان
- تعیین مشخصات زیرساخت های سخت افزاری و ارتباطی فناوری اطلاعات
- تعیین مشخصات نیروی انسانی مورد نیاز سازمان برای پیاده سازی و اجرای سیستم های اطلاعات

استراتژی و بالطبع آن نیازهای کسب و کار به سرعت تغییر می کند و فناوری اطلاعات می بایست بداند استراتژی کسب و کار چیست و چگونه می تواند در یک بازه زمانی قابل قبول از آن حمایت کند. مدیریت استراتژیک فناوری اطلاعات مسیر فوق را هموار کرده و با نگاهی نو در تلاش است که از ظرفیت های واقعی فناوری اطلاعات در کنار کسب و کار یک سازمان استفاده بهینه نماید.

اهمیت داده در استراتژی کسب و کار

اهمیت داده در دنیای کسب و کار امروزی بر کسی پوشیده نیست. رهبران کسب و کار لازم است به داده در سازمان خود در عمل اهمیت داده و زیرساخت های لازم جهت همسوئی آن با استراتژی کسب و کار را فراهم نمایند. داده خوب و یا بهتر بگوئیم داده ای که بتوان به آن اعتماد کرد، بیش از همیشه دارای اهمیت است و لازم است با نگاهی نو به جایگاه آن در تولید ارزش برای کسب و کار توجه گردد. شکل ۱، نیاز فراگیر تمامی بخش های یک سازمان به داده خوب و قابل اعتماد را نشان می دهد.



شکل ۱ : داده خوب و قابل اعتماد یک نیاز فراگیر در تمامی بخش های یک سازمان

بپذیریم که داده علی رغم این که یکی از عناصر مهم و قدرتمند در هر سازمان است ولی متأسفانه به دلیل عدم وجود زیرساخت های لازم و یا مشکلاتی که به مرور زمان ایجاد و انباشته شده اند، مدیریت آن در جهت تبدیل به یک سرمایه استراتژیک بسیار ضعیف است.

هر یک از ما به دفعات این موضوع را شنیده ایم و احتمالاً با آن موافق هستیم که : هم اینک در یک اقتصاد اطلاعاتی زندگی می کنیم. علی رغم این که اکثر سازمان ها به این موضوع اذعان دارند ولی نمی توانند ترجمه ای مناسب از آن را برای کسب و کار خود داشته باشند و به این پرسش پاسخ دهند که این موضوع برای ما چه معنایی دارد؟ به عنوان نمونه از طریق تحلیل داده می توان متوجه این موضوع شد که چه محصول و یا خدماتی تحت چه شرایطی و به کدام مشتری فروخته شده است و یا این که بهترین زمان و مکان ارائه یک محصول جدید چیست؟ سوالاتی از این نوع می تواند تاثیر فراوانی را بر روی کسب و کار شما داشته باشد که پاسخ دقیق به آنها مستلزم وجود داده ای با کیفیت بالا و قابل اعتماد در یک سازمان است.

- داده به عنوان بخش لاینفک ارائه محصولات و خدمات : داده به بخش لاینفک محصولات و یا سرویس هایی که سازمان شما به مشتریان خود عرضه می کند، تبدیل شده است. به عنوان نمونه با ارائه اطلاعات مرتبط، صحیح و با معنی به مشتریان در هنگام خرید محصول و یا سرویس خاصی از سازمان شما، مشتریان ارزش بیشتری را دریافت خواهند داشت.
- اطلاعات در بازار رقابتی امروز نمادی است از قدرت : آگاهی جامع (نگرش ۳۶۰ درجه ای) از مشتری ، تامین کنندگان کالا ، رقبای و محیط عملیاتی یک مزیت رقابتی را ایجاد می کند که به شما در جهت برنامه ریزی صحیح، علمی و منطبق بر واقعیت های موجود کمک خواهد کرد. این کار میسر نمی شود مگر با اتکاء به داده خوب، با کیفیت، یکپارچه و قابل اعتماد.
- تاثیر حجم و سرعت تولید داده بر روی مدل های عملیاتی : سازمان هایی که در ابعاد وسیع تری عملیات خود را انجام می دهند و به نوعی حجم داده بسیار زیادی را با سرعت بالا تولید می کنند در معرض ریسک بیشتری قرار دارند چراکه فرآیندهای کسب و کار قدیمی و سیستم هایی که که در حال کار می باشند می بایست قادر به مدیریت سیلاب داده در سازمان خود در جهت تولید ارزش از آنها باشند.
- نگاه به داده به عنوان محصول و کسب درآمد از طریق داده : امروزه شاهد تولد شرکت ها و سازمان هایی می باشیم که مدل کسب و کار آنها مبتنی بر نگرش های سنتی نمی باشد. این نوع سازمان ، اطلاعات و داده را مستقیماً به محصول و یا محصولاتی تبدیل و آن را در اختیار متقاضیان قرار می دهند. کسب درآمد از طریق داده به یکی از مهمترین رویکردهای موجود در فضای کسب و کار مبتنی بر فناوری اطلاعات تبدیل شده است.

چرا به یک تغییر نگرش جامع در حوزه داده نیاز داریم؟

- داده های عظیم (Big data) : در صورتی که سازمان شما دارای یک زیرساخت مناسب برای حمایت از داده ای که با سرعت زیاد، حجم بالا و از منابع مختلف تولید می شود، نباشد، قدم در میدانی گذاشته است که احتمال پیروزی آن بسیار ضعیف است.
- تغییر الگوی مصرف داده : ما از دوران طراحی راه حل هایی که صرفاً کاربران از طریق یک کامپیوتر شخصی ساده به برنامه ها دستیابی پیدا می کردند، فراتر رفته ایم و هم اینک کاربران از داده و برنامه ها به کمک دستگاه های موبایل نظیر گوشی های هوشمند و ... استفاده می کنند.

- نیازهای به مراتب پیچیده تر برای مدیریت داده : کاربران و یا برنامه ها نیازمند نقل مکان داده از سیستم های غیرمتجانس، ادغام، تحلیل و یکپارچگی می باشند.
- تقاضای داده توسط برنامه های بیشتر : چارچوب مدیریت داده می بایست از برنامه های front office نظیر CRM و برنامه های back office نظیر ERP حمایت کند.
- نیاز به دستیابی سریع داده : خواسته ما از سیستم ها به سرعت به سمت real time و یا near-real time در حال حرکت است.
- وجود گزینه های بیشتر برای استقرار سیستم ها : با توجه به این که هم اینک می توان معماری فناوری اطلاعات را در مکان های متعدد و یا cloud (چه به صورت خصوصی ، عمومی و ترکیبی) مستقر کرد، نیاز به داده سازمان در ابعاد وسیع تری معنی پیدا خواهد کرد.
- نیازهای مختلف برای نقش های گوناگون : استراتژی مدیریت داده می بایست قادر به پاسخگویی نیاز کاربران مختلف با وظایف و مسئولیت های متفاوت باشد (از ناظرین داده تا کارشناسان حرفه ای فناوری اطلاعات تا مدیران کسب و کار ...)
- یک تفکر جدید در خصوص معماری : زمانی که در خصوص مفاهیم معماری سازمانی فکر می کنیم و قصد ایجاد سیستم های جدیدی را داریم، معماری داده جایگاه مختص به خود را دارد.

ما با باید به سمت مدیریت استراتژیک داده در مقابل مدیریت تاکتیکی حرکت کنیم.

ضرورت نگاه استراتژیک رهبران سازمان به داده

اعتقاد داریم، می بایست به دنبال یک تفکر نو در حوزه داده بود تا بتوان در بازار رقابتی امروز و آینده همواره حرفی برای گفتن داشت. سازمان ها می بایست داده را به عنوان یک سرمایه بطور چالاک و نوآورانه مدیریت نمایند. شروع این کار نمی تواند از پائین به بالا و یا از تیم فناوری اطلاعات شروع شود و می بایست با نگاهی از بالا به پائین آن را مدیریت و این نیاز را به یک دغدغه اساسی برای کسب و کار تبدیل کرد.

با این که استراتژی داده می تواند از پتانسیل های فناوری برای تضمین موفقیت خود استفاده کند، در مرکز ثقل آن، مواردی از قبیل تعریف مسائل کسب و کار، فرصت ها، آشنایی با داده مورد نیاز کسب و کار و عناصر سازمانی دیگری قرار دارند که لازم است به درستی در جایگاه خود قرار بگیرند تا بتوان با مدیریت صحیح از مزایای آن به عنوان یک مزیت رقابتی استفاده کرد. این نگرش مستلزم یک تغییر و تحول اساسی در حوزه داده است.

اگر با همان تفکرانی که مشکلات را ایجاد کرده ایم به دنبال حل آنها باشیم است به نتیجه نخواهیم رسید. حل مشکلات در حوزه داده و نقش آفرینی آن در یک سازمان به منظور همسوئی با استراتژی کسب و کار، مستلزم نگاهی نو به فلسفه وجودی داده، جایگاه واقعی آن در نظام تصمیم گیری و عملیاتی یک سازمان و نحوه بکارگیری موثر آن همسو با اهداف کسب و کار است. پاسخ به سؤالاتی نظیر : وضعیت فعلی داده در سازمان ما به چه صورت است؟ انتظار ما از وضعیت مطلوب چیست؟ چگونه مسیر حرکت از وضعیت فعلی به سمت وضعیت مطلوب را طی کنیم؟ به چه زیرساخت هایی نیاز داریم؟ می تواند تکلیف داده در یک سازمان و انتظاری که از آن در آینده وجود دارد را به خوبی مشخص کند.

مدیریت استراتژیک در قالب یک تیم رقابتی همواره سعی میکند که با تقویت سیستم ارتباطات و روابط متقابل بین مدیران و کارکنان در سطوح مختلف سازمانی نقش خود را به نحو احسن ایفا کند. یک مدیریت استراتژیک خوب به

ترکیب قضاوت های شهودی و تجزیه و تحلیل های علمی می پردازد چرا که مدیریت استراتژیک یک علم محض نیست و قضاوت های شهودی بسیار در آن نقش دارند. البته نباید فراموش کرد که رونق و بقای بسیاری از سازمان های موفق امروزی به سبب وجود مدیرانی نخبه، باهوش و الهام بخش است.

ضرورت داشتن یک استراتژی مدون در حوزه داده

داده یکی از منابع حیاتی هر سازمان است که با مدیریت صحیح و تبعیت از یک استراتژی مدون می توان آن را به یک مزیت رقابتی برای کسب و کار تبدیل کرد. به منظور موفقیت در محیط مبتنی بر اطلاعات امروزی، داده می بایست به عنوان قلب مدل کسب و کار و استراتژی سازمان شما در نظر گرفته شود. بدون داشتن یک استراتژی مدون در حوزه داده نمی توان از ظرفیت های داده در تولید ارزش برای سازمان خود استفاده کرد.

استراتژی داده چشم انداز سازمان شما برای مدیریت داده به عنوان یک سرمایه و تلاش هدفمند برای تقویت آن در جهت ایجاد یک مزیت رقابتی است. کسب و کارهای فعلی به سرعت به سمتی پیش می روند که داده در آن دارای یک نقش محوری و کلیدی است و یا کسب و کارهای جدیدی به سرعت در حال شکل گیری می باشند که به نوعی هدف آنها کسب درآمد از طریق داده است. استراتژی داده می بایست مستقیماً با استراتژی کسب و کار سازمان و مدل عملیاتی آن همسو باشد.

قبل از توجه به ضرورت تدوین یک استراتژی مدون و یکپارچه در حوزه داده، بد نیست چند سوال را با هم مرور کنیم تا شاید از این طریق روزنه ای جدید برای حرکت به سمت مدیریت سیستماتیک داده در ذهن ایجاد شود.

- آیا سازمان شما دارای یک استراتژی داده برای موفقیت در بازار به شدت رقابتی امروز است ؟
 - آیا سازمان شما به دنبال آرایه طرح ها و پروژه هایی با ماهیت داده محور است ؟
 - آیا سازمان شما به درستی داده را به عنوان یک سرمایه استراتژیک مدیریت می کند ؟
 - آیا سازمان شما فکر می کند مالکیت داده و مدیریت آن می بایست توسط بخش فناوری اطلاعات انجام شود؟
- تدوین استراتژی داده در یک سازمان بالغ که دارای سبدهای از برنامه ها و داده های مرتبط با آنها است، با ممیزی داده هر یک از برنامه ها شروع می شود.

شکل ۱، ممیزی داده به عنوان تولید یکی از ورودهای تدوین استراتژی داده را نشان می دهد .



شکل ۱ : ممیزی داده به عنوان تولید یکی از ورودهای تدوین استراتژی داده

هر استراتژی داده می بایست قابلیت پیاده سازی و عملیاتی شدن را دارا باشد و نحوه تعامل و ارتباط آن با استراتژی کسب و کار و استراتژی فناوری اطلاعات نیز مشخص گردد.

ایجاد زیرساخت های لازم جهت مدیریت داده، پیش فرض اولیه برای تولید ارزش از داده به عنوان یک سرمایه در سازمان و حرکت به سمت یک سازمان داده محور است. شکل ۲، برخی از زیرساخت های مورد نیاز جهت مدیریت داده به منظور تبدیل آن به یک سرمایه استراتژیک را نشان می دهد.



شکل ۲: زیرساخت های لازم جهت مدیریت داده به منظور تبدیل آن به یک سرمایه استراتژیک

حرکت به سمت یک سازمان داده محور محقق نمی شود مگر این که تکلیف سازمان خود را با داده مشخص کنیم و به دنبال ایجاد یک استراتژی منسجم در خصوص داده باشیم. استراتژی داده با استراتژی فناوری اطلاعات و معماری سازمانی مرتبط است و از طریق تعامل با معماری داده و اطلاعات که بخشی از معماری سازمانی است، پیاده سازی و عملیاتی خواهد شد. ماهیت وجودی استراتژی داده، عرضه مزیت برای کسب و کار و مشارکت جهت نیل به استراتژی کسب و کار است. استراتژی داده می بایست به یک چارچوب عملیاتی ترجمه شود تا این اطمینان حاصل گردد که استراتژی تدوین شده در عمل محقق می گردد.

بدون تغییر نگرش اساسی به داده و مدیریت آن، نمی توان به سمت یک سازمان داده محور حرکت کرد و در عمل از داده به عنوان یک سرمایه حیاتی در جهت تولید ارزش در فضای رقابتی امروز استفاده کرد. این کار مستلزم ایجاد و مدیریت زیرساخت های مورد نیاز جهت حاکمیت داده در یک سازمان است.

اگر با همان تفکراتی که مشکلات را ایجاد کرده ایم به دنبال حل مشکلات باشیم به نتیجه نخواهیم رسید. حل مشکلات، مستلزم نگاهی نو به فلسفه وجودی فناوری اطلاعات، جایگاه واقعی آن و نحوه بکارگیری موثر آن همسو با اهداف کسب و کار است. پاسخ به سؤالاتی نظیر: الان کجا هستیم؟ به کجا می خواهیم برویم؟ چگونه این مسیر را طی کنیم؟ می تواند تکلیف فناوری اطلاعات در یک سازمان و انتظاری که از آن در آینده وجود دارد را به خوبی مشخص کند.