دانشگاه جامع علمی کاربردی

کاربرد فناوری اطلاعات و ارتباطات

عین اله جعفرنژاد قمی، فریدون شمس علیئی

درس کاربرد فناوری اطلاعات و ارتباطات : (از جزوه بارگذاری شده مطالب زیر مطالعه شود)

از فصل ۱ : ۱-۴ و ۱-۵ و ۱-۶ و ۱-۷ و ۱-۸

از فصل ۳ : ۳-۱ و ۳-۲ و ۳-۳

از فصل ۴ : ۴-۴

از فصل ۵ : ۵-۵ و ۵-۹ و ۵-۱۲ و ۵-۱۳

از فصل ۶ : ۶-۱۶

از فصل ۹ : ۹-۱ و ۹-۲ و ۹-۳ و ۹-۶ و ۹-۸

کامل مطالعه شود.

مرکز نشر دانشگاهی
۱۵۵۷

علوم پایه (ریاضی، آمار و کامپیوتر)
۱۸۵

کاربرد فناوری اطلاعات و ارتباطات

عین‌اله جعفرنژاد قمی، فریدون شمس علیئی

ویراستار علمی: حسن طنابی
ویراستار ادبی: امیرعلی نصیری
ویراستار و نسخه‌پرداز: نادیا فرهادتوسکی
حروفچین و صفحه‌آرا: مرضیه دین‌پناه
طراح جلد: علیرضا دربانی
ناظر چاپ: حمیدرضا دمیرچی
دانشگاه جامع علمی‌کاربردی؛ مرکز نشر دانشگاهی
چاپ اول ۱۳۹۸
چاپ دوم ۱۳۹۹
تعداد ۳۰۰۰
چاپ و صحافی: شرکت چاپ و انتشارات سازمان اوقاف و امور خیریه
۲۳۰۰۰ تومان

نشانی فروشگاه مرکزی: خیابان انقلاب، روبه‌روی سینما سپیده، پاساژ خبیری، تلفن: ۶۶۴۰۸۸۹۱، ۶۶۴۱۰۶۸۶

فروش اینترنتی: www.iup.ac.ir

17189164721000021111

فهرست‌نویسی پیش از انتشار کتابخانهٔ ملی جمهوری اسلامی ایران

سرشناسه: جعفرنژاد قمی، عین‌الله، ۱۳۳۹ـ
عنوان و نام پدیدآور: کاربرد فناوری اطلاعات و ارتباطات/ عین‌اله جعفرنژاد قمی، فریدون شمس‌علیئی.
مشخصات نشر: تهران: دانشگاه جامع علمی‌کاربردی؛ مرکز نشر دانشگاهی، ۱۳۹۸
مشخصات ظاهری: دوازده، ۱۸۹ ص.: مصور (بخش رنگی).
شابک: 978-600-5607-40-6 978-964-01-1557-2
وضعیت فهرست‌نویسی: فیپا
یادداشت: در ویراست قبلی کتاب حاضر که در سال ۱۳۹۳ توسط انتشارات علوم رایانه و دانش‌بنیان منتشر شده نویسندهٔ دوم فاطمه جعفرنژاد قمی ذکر شده است.
یادداشت: کتابنامه: ص. ۳۲۸.
موضوع: تکنولوژی اطلاعات و ارتباطات
موضوع: *Information and communications technologies
موضوع: علوم کامپیوتر
موضوع: Computer science
شناسه افزوده: شمس علیئی، فریدون، ۱۳۳۹ـ
شناسه افزوده: دانشگاه جامع علمی‌کاربردی، مرکز نشر دانشگاهی
رده‌بندی کنگره: T۵۸/۵
رده‌بندی دیویی: ۰۰۴
شماره کتابشناسی ملی: ۴۷۷۳۰۰۶

بسم الله الرحمن الرحیم

فهرست

عنوان | صفحه

عنوان	صفحه

عنوان	صفحه

عنوان	صفحه

عنوان | صفحه

۱

آشنایی با رایانه (کامپیوتر)

اهداف آموزشی

پس از مطالعهٔ این فصل توانایی‌های زیر را درک خواهید کرد:

مفهوم رایانه را درک می‌کنید.

با سخت‌افزار و نرم‌افزار آشنا می‌شوید.

با عنصرهای جانبی رایانه آشنا می‌شوید.

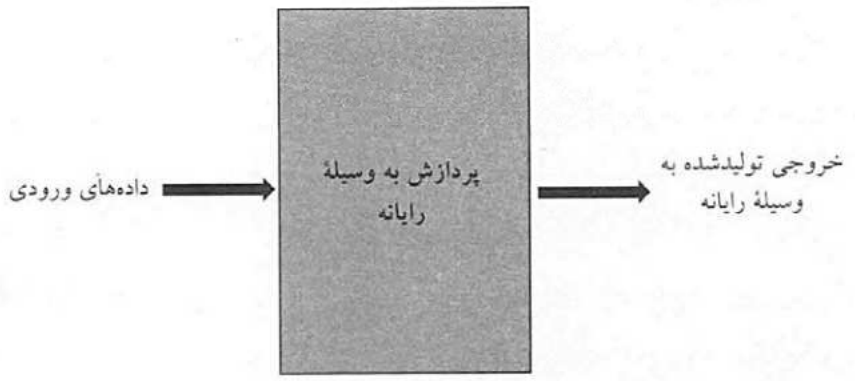
واحدها اندازه‌گیری حافظه را خواهید شناخت.

هر یک از دستگاه‌ها و تجهیزات اطراف ما، یک یا چند هدف را برآورده می‌کنند. خودرو برای جابه‌جایی (حمل و نقل)، خودکار برای نوشتن، تلفن برای مکالمه، رادیو برای پخش صدا و تلویزیون برای پخش و نمایش فیلم و تصویر مورد استفاده قرار می‌گیرد. اما رایانه (کامپیوتر[1]) چگونه؟

رایانه دستگاه ساده‌ای است و کارش این است که ورودی‌هایی را می‌گیرد، آنها را پردازش می‌کند و خروجی‌هایی تولید می‌کند. برای نمونه، رایانه می‌تواند نمره‌ها و شمار واحد هر درس یک دانشجو را به عنوان ورودی بپذیرد، معدل آن را براساس فرمولِ محاسبهٔ

---

1. computer



شکل ۱ـ۱ عملکرد سادهٔ رایانه.

معدل محاسبه کند (نمره‌ها و واحدهای درسی را **پردازش** کند) و سپس معدل را به عنوان خروجی تولید کند. بنابراین، عمل سادهٔ رایانه را می‌توان مانند شکل ۱ـ۱ رسم کرد.

۱ـ۱ سخت‌افزار رایانه

در جهان رایانه‌ها، سخت‌افزار[1] هر قطعه یا عنصری از رایانه است که ساختاری فیزیکی دارد. برای نمونه، صفحه‌کلید، ماوس یا موشی[2] و نمایشگر، هرکدام یک قطعهٔ سخت‌افزاری به شمار می‌روند. حتی قطعه‌هایی که به گونهٔ عادی نمی‌توانید آنها را ببینید؛ یعنی آنهایی که در درون محفظه (کیس[3]) هستند، مانند منبع تغذیه و تخته‌مدار اصلی[4] نیز جنبهٔ سخت‌افزاری رایانه را تشکیل می‌دهند.

اما رایانه تنها سخت‌افزار نیست، بلکه جنبهٔ دیگری به نام نرم‌افزار[5] دارد که در بخش دیگری مورد بررسی قرار می‌گیرد. ابتدا به بخش‌های سخت‌افزاری رایانه می‌پردازیم.

۱ـ۲ عنصرهای اصلی و جانبی رایانه

اگر نگاهی به ظاهر یک رایانه داشته باشیم، خواهیم دید که هر رایانه دارای یک **کیس**، **نمایشگر** یا **مانیتور**، **صفحه‌کلید** و **ماوس** است که عنصرهای اصلی و ضروری آن به شمار می‌روند. البته، در درون کیس اجزای دیگری وجود دارند که فعلاً به آنها نمی‌پردازیم. شکل ۱ـ۲ نمونه‌ای از رایانه را به همراه عنصرهای آن نمایش می‌دهد.

---

1. hardware
2. mouse
3. case
4. motherboard
5. software

شکل ۱ـ۲ نمونه‌ای از رایانه همراه با عنصرهای اصلی.

اما هر رایانه، افزون بر اجزای اصلی، دارای شماری دستگاه و عنصرهای جانبی است که در خارج از کیس رایانه قرار می‌گیرند و بر کمیت و کیفیت عملکرد رایانه می‌افزایند. برخی از این دستگاه‌های متداول عبارت‌اند از:

- چاپگر (printer)
- دوربین‌های اینترنتی یا وب‌بین (webcam)
- دستگاه‌های صوتی مانند بلندگو و میکروفون
- دوربین‌های دیجیتال (digital cameras)
- پویشگر (scanner)
- یوپی‌اس[1] (UPS)
- رسّام (plotter)

۱ـ۲ـ۱ صفحه کلید

صفحه‌کلید، وسیله‌ای است که برای انتقال اطلاعات به رایانه مورد استفاده قرار می‌گیرد. به گونهٔ کلی، کلیدهای صفحه‌کلید به پنج دسته تقسیم می‌شوند (شکل ۱ـ۳).

- کلیدهای الفبا عددی (alphanumeric)
- کلیدهای عددی (numeric keyboard)
- کلیدهای تابعی (function keys)
- کلیدهای ویرایشی (modifier key)
- کلیدهای حرکتی یا مکان‌نما (cursor-movement keys)

1. Uninterruptible Power Supply

شکل ۱ـ۳ انواع کلیدهای صفحه‌کلید.

۱ـ۲ـ۲ ماوس

ماوس یا موشی یک ابزار ضروری برای کار کردن با رایانه است و انواع گوناگونی دارد، مانند **ماوس بی‌سیم** که از فروسرخ یا بلوتوث برای برقراری ارتباط با رایانه استفاده می‌کند و **ماوس باسیم** که از راه سیم به رایانه متصل می‌شود. **ماوس‌های معمولی** بر روی یک سطح صاف حرکت می‌کنند و با حرکت گوی موجود در زیر آن، موقعیت را در صفحه‌نمایش معین می‌کنند. اما **ماوس‌های نوری** فاقد گوی هستند و بخش‌های متحرک کمتری دارند و کنترل بهتری را فراهم می‌سازند. هر ماوس دست کم دو کلید (چپ و راست) دارد و برخی از ماوس‌ها کلید دیگری دارند که برای پیمایش محتوای یک صفحه به کار می‌روند. کلید سوم قابل برنامه‌ریزی است. شکل ۱ـ۴ نمونه‌هایی از ماوس را نشان می‌دهد. به چند نکته در مورد ماوس توجه کنید:

- **کلیک (click):** فشار دادن دکمهٔ سمت چپ ماوس را کلیک کردن می‌گویند.
- **راست‌کلیک (right click):** فشار دادن دکمهٔ سمت راست ماوس را راست کلیک می‌نامند.
- **کلیک دوگانه (double click):** هنگامی که بر روی دکمهٔ سمت چپ ماوس دوبار بدون فاصله کلیک می‌کنید، به آن کلیک دوگانه می‌گویند.

شکل ۱ـ۴ نمونه‌هایی از ماوس.

شکل ۱ـ۵ نمونه‌هایی از نمایشگر LCD.

۱ـ۲ـ۳ نمایشگر (مانیتور)

نمایشگر یکی از عنصرهای اصلی رایانه بوده و متداول‌ترین دستگاه خروجی نیز هست که برای نمایش اطلاعات به کار می‌رود. صفحه‌نمایش به گونهٔ معمول دو نوع است:

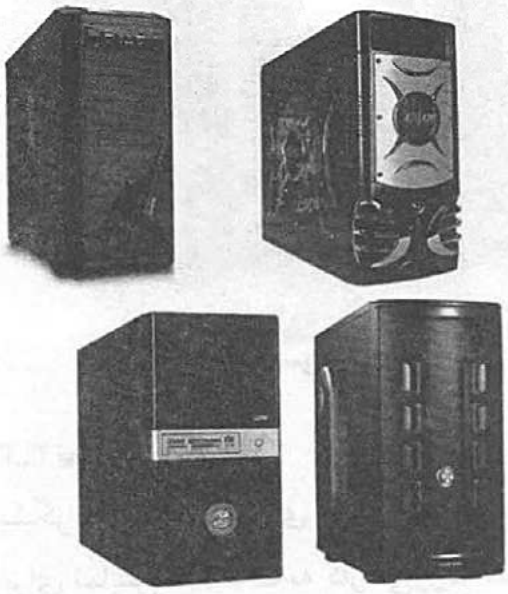
- **نمایشگر CRT قدیمی:** این نمایشگر که لامپ پرتوهای کاتدی (CRT)[1] نامیده می‌شود، فضای زیادی را اشغال می‌کند. این صفحه‌نمایش برق زیادی مصرف می‌کند، در حین کار داغ می‌شود و انواع پرتوها را صادر می‌کند. این نمایشگرها از دور خارج شده‌اند.
- **نمایشگر LCD:** نمایشگرهای LCD [2] که نمایشگر تخت نیز نامیده می‌شوند، از فناوری صفحه‌های رایانه کیفی (لپ‌تاپ) استفاده می‌کنند؛ در نتیجه نازک و سبک هستند و نسبت به نمایشگرهای CRT برق کمتری مصرف می‌کنند؛ گرما و پرتو تولید نمی‌کنند. بیشتر نمایشگرهای LCD به صورت صفحهٔ عریض[3] هستند. شکل ۱ـ۵ نمونه‌هایی از نمایشگرهای LCD را نشان می‌دهد.

۱ـ۲ـ۴ محفظه (case)

محفظه یا کیس رایانه دارای اطلاعات درونی است تا از آسیب احتمالی در امان باشند. درون محفظهٔ رایانه قطعه‌های مهمی وجود دارند که سبب عملکرد رایانه می‌شوند (شکل ۱ـ۶). مهم‌ترین قطعهٔ درون کیس، تخته‌مدار اصلی است که دیگر قطعه‌ها در آن جاسازی می‌شوند. نمونه‌ای از یک تخته‌مدار اصلی را در شکل ۱ـ۷ می‌بینید.

---

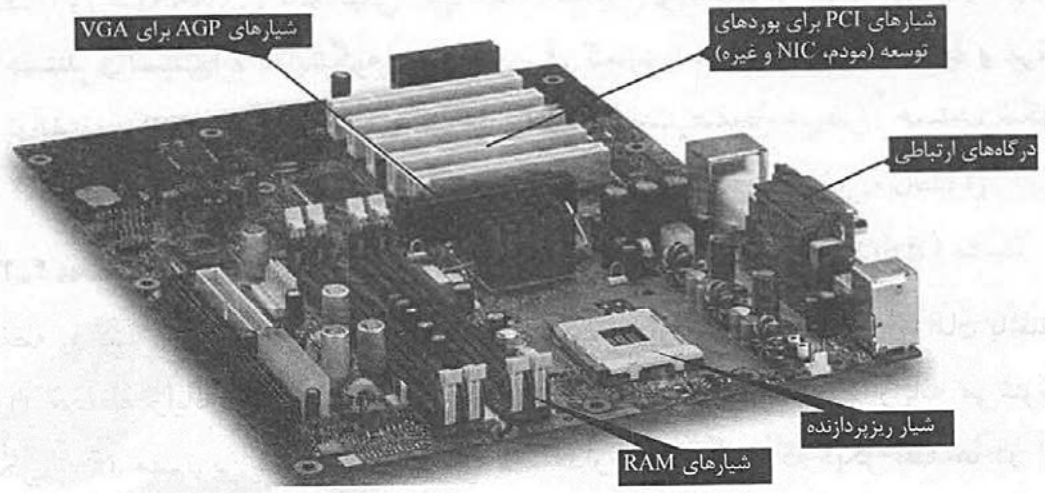
1. Cathode Ray Tube
2. Liquid Crystal Display
3. Wide Screen



شکل ۱ـ۶ نمونه‌هایی از کیس رایانه.

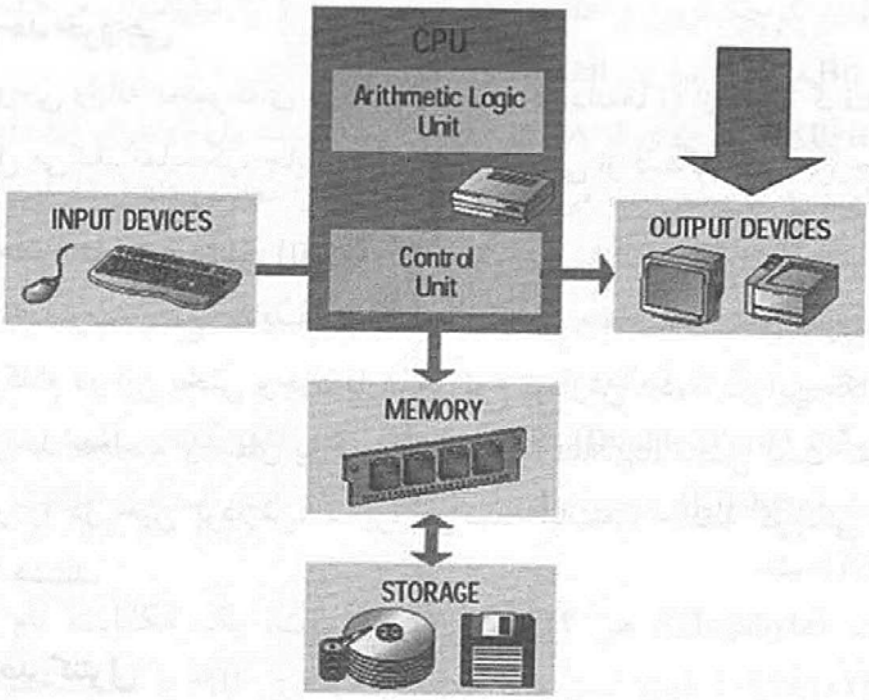
همان‌گونه که در شکل ۱ـ۷ می‌بینید، بورد اصلی دارای مکان‌هایی برای نصب انواع قطعه‌های رایانه است. مکان‌های تخته‌مدار اصلی برای نصب قطعه‌ها را اسلات[1] یا شیار می‌نامند. برخی از قطعه‌های درون بورد اصلی عبارت‌اند از:

- کارت‌های گرافیکی و صدا (graphic & sound cards)
- کارت شبکه (network card)
- مودم یا مبدّل درونی (internal modem)
- منبع تغذیه (power supply)
- حافظه (memory)
- ریزپردازنده (microprocessor)
- درگاه‌های ارتباطی (communication ports)



شکل ۱ـ۷ نمونه‌ای از تخته‌مدار اصلیِ داخل کیس.

1. slot



شکل ۱ـ۸ سازمان رایانه و ارتباط میان واحدها.

۱ـ۳ سازمان رایانه

رایانه باید داده‌ها و اطلاعات را از خارج دریافت کند، آنها را ذخیره و سپس پردازش نماید. نتیجه را به خروجی بُرد و این اعمال را با کنترل و نظارت ویژه‌ای انجام دهد (شکل ۱ـ۸). بنابراین می‌توان گفت که سازمان رایانه شامل پنج بخش یا واحد گوناگون به شرح زیر است:

- واحد ورودی (input unit)
- واحد خروجی (output unit)
- واحد حافظه (memory unit)
- واحد محاسبه و منطق (arithmetic logic unit)
- واحد کنترل (control unit)

۱ـ۳ـ۱ واحد ورودی

واحد ورودی رایانه شامل مجموعه‌ای از دستگاه‌هاست که داده‌ها را از خارج از رایانه گرفته وارد رایانه می‌کنند تا بر روی آنها پردازش‌هایی صورت گیرد. ماوس و صفحه‌کلید دو دستگاه مهم ورودی به‌شمار می‌روند.

۱ـ۳ـ۲ واحد خروجی

واحد خروجی رایانه مجموعه‌ای از دستگاه‌هاست که داده‌ها را از رایانه گرفته به خارج از آن منتقل می‌کند. نمایشگر، چاپگر و رسّام نمونه‌هایی از دستگاه‌های خروجی هستند.

۱ـ۳ـ۳ واحد محاسبه و منطق (ALU)

اعمالی مانند ضرب، جمع، مقایسهٔ دو مقدار، در واحد محاسبه و منطق صورت می‌گیرد و مدار هرکدام در این بخش وجود دارد. هر نوع پردازش داده‌ها در این مکان صورت می‌گیرد. واحد محاسبه و منطق به شماری ثبات یا register متصل است که داده‌ها و دستور کار را در حین پردازش، ذخیره می‌کنند. ثبات‌ها، حافظهٔ کوچکی در درون پردازنده‌ها هستند.

۱ـ۳ـ۴ واحد کنترل

این واحد مسئول مدیریت بر همهٔ منابع سامانه است. واحد کنترل، جریان داده‌ها را در پردازنده و جریان داده‌ها به دستگاه‌ها یا از دستگاه‌های دیگر را کنترل می‌کند. واحد کنترل واحد ریزکدهای[1] پردازنده است، که دارای دستور کارهایی برای انجام همهٔ وظایفی است که پردازنده می‌تواند انجام دهد.

◀**یادآوری:** پردازنده یا CPU دارای واحد محاسبه و منطق و واحد کنترل است که در شکل ۱ـ۸ نیز مشاهده می‌شود.

۱ـ۳ـ۵ واحد حافظه

حافظهٔ رایانه محل نگهداری داده‌ها، اطلاعات و برنامه‌هاست. دو نوع حافظه در رایانه مورد استفاده قرار می‌گیرند:

- حافظهٔ اصلی (MainMemory)
- حافظهٔ جانبی (SecondaryMemory)

در ادامه، مفاهیم مربوط به حافظه را مورد بررسی قرار می‌دهیم.

۱ـ۳ـ۶ واحدهای اندازه‌گیری حافظه

حافظه مانند هر کمیت دیگری دارای مقیاس‌هایی برای اندازه‌گیری است. این مقیاس‌ها عبارت‌اند از:

---

1. microcode

بیت (Bit): کوچک‌ترین واحد حافظه که صفر یا ۱ را نگهداری می‌کند، بیت نام دارد. کلمهٔ Bit مخفف عبارت Binary Digital است.

بایت (Byte): مجموعه‌ای از ۸ بیت می‌توان یک حرف را نگهداری کند، این حرف، بایت نیز نام دارد. با یک بایت می‌توان ۲۵۶ کاراکتر را نمایش داد ($۲^۸$). این کاراکترها دارای مقادیر صفر تا ۲۵۵ هستند.

کلمه (Word): به مجموعه‌ای از دو یا چهار بایت گفته می‌شود که ممکن است از ماشینی به ماشین دیگر فرق کند.

کلمهٔ دوگانه (Double Word): به مجموعه‌ای از دو کلمه گفته می‌شود.

کیلوبایت (Kilobyte): مجموعه‌ای از ۱۰۲۵ ($۲^{۱۰}$) بایت است و علامت اختصاری آن K یا KB است.

مگابایت (Megabyte): هر ۱۰۲۴ ($۲^{۱۰}$) کیلوبایت، یک مگابایت نام دارد. هر مگابایت ۱۰۲۴×۱۰۲۴ بایت است و با علامت اختصاری MB یا M مشخص می‌شود. هر مگابایت برابر با ۸×۱۰۲۴×۱۰۲۴ بیت است.

گیگابایت (Gigabyte): هر ۱۰۲۴ ($۲^{۱۰}$) مگابایت، یک گیگابایت نام دارد. با علامت اختصاری GB یا G مشخص می‌شود. هر گیگابایت معادل ۱۰۲۴×۱۰۲۴ کیلوبایت است و معادل ۱۰۲۴×۱۰۲۴×۱۰۲۴ بایت است. یک گیگابایت برابر با ۸ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ بیت است.

ترابایت (Terabyte): هر ۱۰۲۴ گیگابایت، یک ترابایت نام دارد. با علامت اختصاری TB یا T مشخص می‌شود. هر ترابایت معادل ۱۰۲۴ × ۱۰۲۴ مگابایت، ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ کیلوبایت، ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ بایت و ۸ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ بیت است.

پتابایت (Petabyte): هر ۱۰۲۴ ترابایت، یک پتابایت نام دارد. با علامت اختصاری PB یا P مشخص می‌شود. هر پتابایت معادل ۱۰۲۴ × ۱۰۲۴ ($۲^{۲۰}$) گیگابایت، ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ ($۲^{۳۰}$) مگابایت، ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ ($۲^{۴۰}$) کیلوبایت، ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ ($۲^{۵۰}$) بایت و ۸ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ × ۱۰۲۴ بیت است.

اگزابایت (Egzabyte): هر ۱۰۲۴ پتابایت، یک اگزابایت نام دارد. هر اگزابایت معادل $۲^{۱۰}$ پتابایت، $۲^{۲۰}$ ترابایت، $۲^{۳۰}$ گیگابایت، $۲^{۴۰}$ مگابایت، $۲^{۵۰}$ کیلوبایت، $۲^{۶۰}$ بایت و ۸ × $۲^{۶۰}$ بیت است. علامت اختصاری آن E یا EB است.

نمونه: رایانه‌ای دارای ۳۲ گیگابایت حافظهٔ جانبی است. این رایانه دارای چند مگابایت، کیلوبایت، بایت و بیت حافظه است؟

$1\ GB = 1024\ MB \Rightarrow 32\ GB = 32 \times 1024 = 2^5 \times 2^{10} = 2^{15}\ MB$
$1\ GB = 1024 \times 1024\ KB \Rightarrow 32\ GB = 32 \times 1024 \times 1024 = 2^5 \times 2^{10} \times 2^{10} = 2^{25}\ MB$
$1\ GB = 1024 \times 1024 \times 1024B \Rightarrow 32\ GB = 32 \times 1024 \times 1024 \times 1024 = 2^5 \times 2^{10} \times 2^{10} \times 2^{10} = 2^{35}\ MB$
$1\ GB = 1024 \times 1024 \times 1024 \times 8\ Bit \Rightarrow 32\ GB = 32 \times 1024 \times 1024 \times 1024 \times 8 = 2^5 \times 2^{30} \times 2^3 = 2^{38} Bit$

۱ـ۴ حافظهٔ اصلی (Main Memory)

همان‌گونه که گفته شد یکی از واحدهای رایانه، حافظهٔ رایانه است که داده‌ها و اطلاعات را نگهداری می‌کند. حافظهٔ اصلی رایانه بر دو نوع است:

حافظهٔ تنها خواندنی[1] (ROM). این حافظه دارای دستور کارهایی است که کارخانهٔ سازندهٔ رایانه آنها را می‌نویسد و برای راه‌اندازی رایانه و برخی از اعمال ابتدایی مورد استفاده قرار می‌گیرد. محتوای این حافظه توسط کاربران قابل تغییر نیست. توجه داشته باشید که با قطع جریان برق، محتوای این حافظه از میان نمی‌رود، در نتیجه **پایدار** است.

حافظهٔ RAM[2]. بخشی از این حافظه در اختیار کاربر است که داده‌ها و کد برنامه‌های مورد نیاز پردازنده را ذخیره می‌کند. محتوای RAM به سرعت و بیشتر تغییر می‌کنند. محتوای حافظهٔ RAM با قطع جریان برق از میان می‌رود و در نتیجه **ناپایدار** است.

۱ـ۵ حافظهٔ جانبی (Secondary Memory)

افزون بر حافظهٔ اصلی که شرح آن گذشت، حافظه‌های دیگری برای ذخیرهٔ دائمی اطلاعات به کار می‌روند و به نام حافظهٔ جانبی (ثانویه) شناخته می‌شوند. دو دسته از حافظهٔ جانبی مهم عبارت‌اند از:

- دیسک‌های مغناطیسی (magnetic disks)، مانند دیسک سخت[3]؛

---

1. Read Only Memory
2. Random Access Memory
3. Hard Disk

- دیسک‌های نوری (optical disks)، مانند SD؛
- ممکن است این پرسش مطرح شود که با وجود حافظهٔ RAM برای ذخیرهٔ داده و برنامه‌ها، چرا از حافظهٔ جانبی استفاده می‌شود. دلایل آن عبارت‌اند از:
- حافظهٔ RAM محدود است.
- با قطع جریان برق، محتوای RAM از میان می‌رود (RAM ناپایدار است).
- برخی از اطلاعات به صورت دوره‌ای استفاده می‌شوند.
- حافظهٔ جانبی برای انتقال اطلاعات و برنامه‌ها از رایانهٔ به رایانه دیگر به کار می‌رود.
- محتوای حافظهٔ جانبی با قطع جریان برق از میان نمی‌رود (پایدار است).

۱ـ۵ـ۱ دیسک مغناطیسی

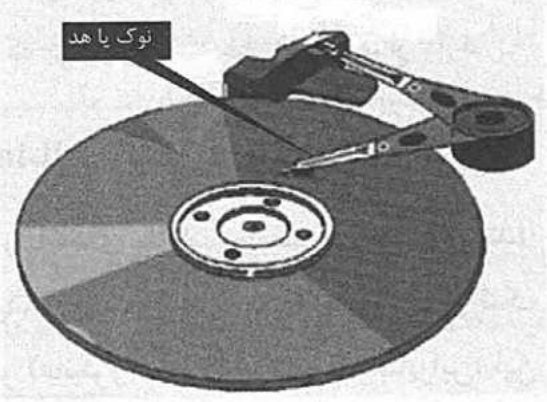
مهم‌ترین نوع دیسک مغناطیسی دیسک سخت است که ظرفیت و سرعت دسترسی بالایی دارد. دیسک‌های سخت از چندین صفحه تشکیل شده‌اند و چندین نوک یا هِد خواندن و نوشتن دارند که برای خواندن اطلاعات از دیسک و نوشتن اطلاعات بر روی آن به کار می‌روند. دیسک‌های سخت بر دو نوع هستند:

- دیسک‌های سخت درونی یا ثابت که در درون رایانه نصب می‌شوند.
- دیسک‌های سخت خارجی که در خارج از رایانه قرار دارند و با یک کابل به رایانه متصل می‌شوند و قابل انتقال از جایی به جای دیگر هستند.

نمونه‌ای از دیسک سخت را در شکل ۱ـ۹ می‌بینید.

۱ـ۵ـ۲ دیسک‌های نوری

دیسک‌های نوری یک صفحهٔ فلزی با پوشش پلاستیکی است که با تابیدن فوتون‌های



شکل ۱ـ۹ دیسک سخت.

نور به سطح دیسک، اطلاعات در آنها ذخیره می‌شود و با زاویهٔ انعکاس نور در سطح دیسک، اطلاعات ذخیره شده در آنها خوانده می‌شود. دو نوع دیسک نوری معروف، CD و DVD هستند که در ادامه شرح مختصری از آنها ارائه می‌شود.

لوح فشرده یا CD. ظرفیت این نوع دیسک‌ها ۵۰ MB یا بیشتر است و برای ایجاد یک CD صوتی یا ذخیرهٔ داده‌ها، باید از یک درایو CD استفاده کنید.

DVD. دیسک فشرده‌ای با ظرفیت بسیار بالاست. DVD نسبت به CD برتری‌های زیر را دارد:

- با هر پخش و گذشت زمان، کیفیت آن پایین نمی‌آید.
- میدان‌های مغناطیسی و الکترومغناطیسی به آن آسیب نمی‌رسانند.
- مقاومت آنها در برابر سرما و گرما زیاد است.

عیب DVD این است که مقاومت آنها در برابر خراش و آلودگی اندک است.

۱ـ۶ حافظهٔ فلش (Flash Memory)

فلش‌ها با حافظهٔ ذخیره‌سازی بسیار بالا و با سرعت مناسب، روش دیگری برای ذخیرهٔ اطلاعات هستند. فلش‌ها برای انتقال اطلاعات از رایانه‌ای به رایانه دیگر، ابزار مناسبی هستند.

۱ـ۷ حافظهٔ نهان (Cache Memory)

حافظهٔ پنهان نوعی حافظه با فناوری دسترسی با سرعت است و آخرین اطلاعات پردازش‌شده در پردازنده را در خود نگه می‌دارد تا در صورت نیاز دوباره پردازنده به آن، با سرعت در اختیارش قرار گیرد. حافظهٔ پنهان به دو صورت در رایانه استفاده می‌شود:

- حافظهٔ پنهان درونی که در درون پردازنده واقع است.
- حافظهٔ پنهان خارجی که بر روی تخته‌مدار اصلی قرار دارد.

۱ـ۸ رایانه‌های All-in-one، کیفی و مالشی

رایانه‌های All-in-one، رایانه‌های فاقد محفظه (کیس) هستند؛ به گونه‌ای که همهٔ تجهیزات لازم برای رایانه، مانند پردازنده، کارت‌های گرافیک و صدا، درگاه‌های ارتباطی و ...، در نمایشگر (مانیتور) جاسازی شده‌اند. بنابراین، این رایانه‌ها فاقد محفظه

هستند و جای بسیار کمتری را اشغال می‌کنند. امکاناتی مانند صفحهٔ لمسی، پردازنده و سامانهٔ صوتی قوی، ویژگی سه‌بعدی، در این رایانه‌ها فراهم است. صفحه‌کلید و ماوس آن نیز بی‌سیم است. نمونه‌ای از رایانه All-in-one را در شکل ۱ـ۱۰ می‌بینید.

شکل ۱ـ۱۰ نمونه‌ای از رایانه All-in-one.

امروزه دو نوع رایانه دیگر، یعنی کیفی (لپ‌تاپ) و مالشی (تبلت) به وفور مورد استفاده قرارمی‌گیرند و همهٔ کسانی که اهل رایانه هستند، این دو نوع رایانه را می‌شناسند.

۱ـ۹ نرم‌افزار

همهٔ برنامه‌هایی که در رایانه مورد استفاده قرار می‌گیرند، جنبهٔ نرم‌افزاری رایانه را تشکیل می‌دهند. نرم‌افزارها به گونهٔ معمول به دو دسته تقسیم می‌شوند:

- نرم‌افزارهای کاربردی (application programs)؛
- نرم‌افزارهای سامانه (system programs)؛

نرم‌افزارهای کاربردی، برنامه‌هایی هستند که برنامه‌نویسان رایانه برای رفع نیاز کاربران می‌نویسند، مانند برنامهٔ حسابداری مورد استفاده در سازمان‌ها.

نرم‌افزارهای سامانه، برنامه‌هایی هستند که امکان استفاده از سخت‌افزار و دیگر نرم‌افزارها را فراهم می‌آورند. یکی از مهم‌ترین نرم‌افزارهای سامانه‌ای، **سیستم‌عامل**[1] است که اگر در رایانه نصب نشده باشد، رایانه قابل استفاده نیست.

۱ـ۹ـ۱ سیستم‌عامل

سیستم‌عامل برنامه‌ای است که اجرای برنامه‌های کاربردی را کنترل می‌کند و به‌عنوان واسط میان کاربردها و سخت‌افزار رایانه عمل می‌کند. سیستم‌عامل سه هدف دارد:

---

1. operating system

- سهولت: سیستم‌عامل سبب سهولت استفاده از رایانه می‌شود.
- کارآمدی: سیستم‌عامل سبب استفادهٔ کارآمد از منابع سامانه رایانه می‌شود.
- قابلیت تکامل: سیستم‌عامل باید به‌گونه‌ای ساخته شود که توسعه مؤثر آن، امتحان و معرفی وظایف جدید بدون تداخل کنونی امکان‌پذیر باشد.

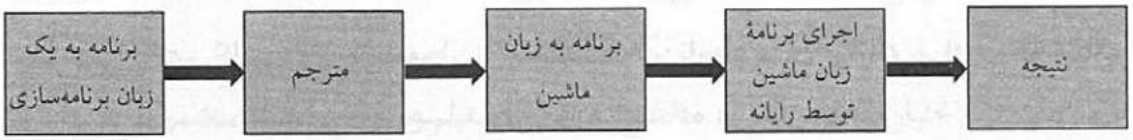
۱ـ۹ـ۲ مفهوم زبان‌های برنامه‌سازی

انسان‌ها هر آنچه را که می‌خواهند توسط رایانه انجام دهند، آن را با استفاده از یک زبان برنامه‌سازی به برنامهٔ رایانه‌ای بدل می‌کنند. سپس برنامهٔ رایانه‌ای را در اختیار رایانه قرارمی‌دهند تا اجرا شود. برخی از زبان‌های برنامه‌سازی متداول عبارت‌اند از زبان C، زبان C++، زبان C#، زبان جاوا، زبان ویژوال بیسیک و زبان پاسکال.

۱ـ۹ـ۳ مفهوم مترجم

برنامه‌هایی که به یک زبان برنامه‌سازی نوشته می‌شوند، مستقیماً توسط سخت‌افزار رایانه قابل درک نیستند؛ زیرا هر رایانه تنها زبان ویژه‌ای به نام زبان ماشین را درک می‌کند. بنابراین، اگر رایانه بخواهد برنامه‌ای که به یک زبانی غیر از زبان ماشین نوشته‌شده اجرا کند، چه می‌کند؟

هر زبان برنامه‌سازی یک مترجم دارد که برنامه‌ای به آن زبان را به برنامه‌ای معادل به زبان ماشین بدل (ترجمه) می‌کند. شکل زیر را ببینید.



۱ـ۹ـ۴ مفهوم فایل

هریک از برنامه‌های رایانه‌ای در یک فایل ذخیره می‌شوند و مجموعه‌ای از داده‌ها و اسناد نیز در فایل‌ها ذخیره می‌شوند. برای اینکه فایل‌ها از هم تمیز داده شوند، دارای نام هستند. نام فایل از دو بخش تشکیل شده است که با نقطه از هم جدا می‌شوند. نام هر فایل به صورت xxxxx.xxx نوشته می‌شود که بخش سمت چپ نقطه را نام فایل و بخش سمت راست را پسوند فایل می‌نامند. مانند test.dat و first.cpp. فایل‌ها به گونهٔ معمول به سه دسته تقسیم می‌شوند:

- فایل اسناد؛
- فایل برنامه‌ها؛
- فایل داده‌ها.

پرسش و پژوهش

۱. مفهوم رایانه را بیان کنید.
۲. اجزای رایانه را با عنصرهای بدن انسان مقایسه کنید.
۳. مفهوم شبکه را بیان کنید.
۴. برخی از اجزای جانبی رایانه و عملکرد آنها را بیان کنید.
۵. در مورد انواع تبلت‌ها پژوهش کنید.

۲

مفاهیم فناوری

اهداف آموزشی

پس از مطالعهٔ این فصل توانایی‌های زیر را کسب خواهید کرد:

جایگاه فناوری را درک خواهید کرد.

با مفهوم فناوری آشنا می‌شوید.

انواع فناوری را خواهید شناخت.

مدل چرخهٔ حیات فناوری را می‌شناسید.

فناوری یا تکنولوژی را می‌توان به معنای ساخت، تغییر، به کارگیری و دانشِ ابزارها، ماشین‌ها، فنون، صنایع، سامانه‌ها و روش‌های سازمان‌دهی دانست که به منظور حل مسئله، بهبود راه‌حل‌های موجود برای حل مسئله، دستیابی به هدف یا انجام یک عمل ویژه مورد استفاده قرار می‌گیرد. افزون بر این، فناوری را می‌توان مجموعه‌ای از این ابزارها، از جمله ماشین‌ها، چیدمان‌ها و رویه‌ها دانست. فناوری به گونهٔ شگفت‌انگیزی بر انسان و دیگر حیوانات اثر دارد تا محیط‌های طبیعی خود را تحت کنترل درآورند و خودشان را با آن محیط‌ها وفق دهند. این واژه می‌تواند به حوزه‌های عمومی یا خصوصی گفته شود، مانند فناوری ساخت، فناوری پزشکی و فناوری اطلاعات.

۲ـ۱ مفهوم فناوری

فناوری یا تکنولوژی از دو واژهٔ یونانی "techne" به معنای هنر و مهارت و "lugio" به معنای علم و دانش تشکیل شده است. به چند نمونه از تعریف فناوری که در زیر آمده است توجه کنید:

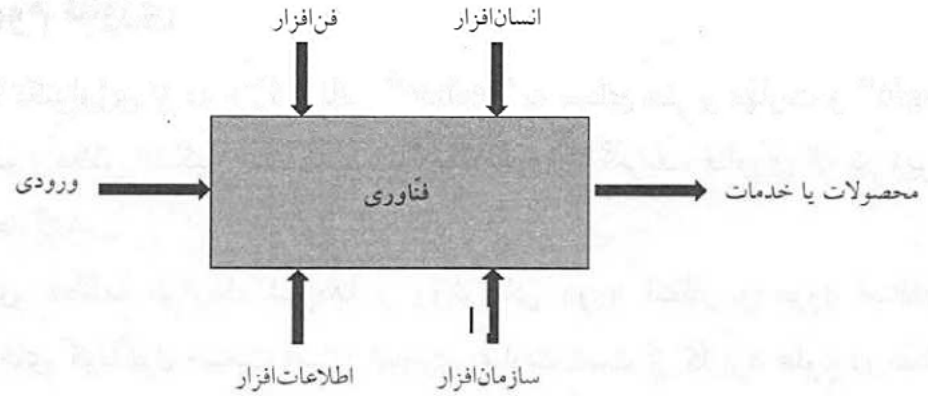
- فناوری، مطالعهٔ ابزارها، شیوه‌ها و روش‌های مورد انتظار و مورد استفاده در حوزه‌های گوناگون صنعت است. فناوری عبارت است از کاربرد علوم در صنایع با استفاده از رویه‌ها و مطالعات منظم و جهت‌دار.
- فناوری عامل تبدیل منابع طبیعی، سرمایه و نیروی انسانی به کالا و خدمات است که عنصرهای تشکیل‌دهنده و ارکان آن عبارت است از سخت‌افزار، انسان‌افزار یا نیروی انسانی متخصص‌فناوری به معنای کاربرد منظم معلومات علمی و دیگر آگاهی‌های نظام یافته برای انجام وظایف عملی است.
- فناوری کاربرد عملی دانش و ابزاری برای کمک به تلاش انسان است و تأثیر بسزایی بر توسعهٔ جوامع بشری دارد.
- فناوری در حوزه‌های گوناگون علمی مورد بهره‌برداری قرار می‌گیرد که برخی از آنها عبارت‌اند از: فناوری اطلاعات و ارتباطات، فناوری هسته‌ای، فناوری نانو و فناوری سلول‌های بنیادین.
- **فناوری اطلاعات و ارتباطات:** در فناوری اطلاعات با رایانه‌ها و نرم‌افزارهایی سروکار داریم که بتوانند فرایند تبدیل، ذخیره‌سازی، حفاظت، پردازش، انتقال و بازیابی اطلاعات را به صورت مطمئن انجام دهند. عنصرهای تشکیل‌دهندهٔ فناوری اطلاعات عبارت‌اند از: انسان، راهبردها، ابزارها و ساختارها.

۲ـ۲ مدل‌های فناوری

در این بخش به معرفی برخی از مدل‌های نظری و ذهنی مباحث فناوری می‌پردازیم. این مدل‌ها عبارت‌اند از مدل اجزای فناوری و مدل چرخهٔ حیات فناوری.

۲ـ۲ـ۱ مدل اجزای فناوری

بر اساس مدلی که سازمان اسکاپ (وابسته به سازمان ملل) مطرح شد، فناوری را



شکل ۲ـ۱ اجزای فناوری اطلاعات.

می‌توان بر اساس چهار عنصر فن‌افزار (ماشین‌آلات و تجهیزات)، انسان‌افزار (مهارت‌ها و توانایی‌های نهفته در انسان)، اطلاعات‌افزار (مستندات و دانش فنی) و سازمان‌افزار (ابعاد مدیریتی و سازمانی) تبیین کرد (شکل ۲ـ۱).

فن‌افزار (Technoware)

فناوری‌های موجود در اشیای مورد استفاده برای تولید کالاها یا خدمات است که شامل تجهیزات، ماشین‌آلات، ابزارها، تأسیسات و تسهیلات فیزیکی و سخت‌افزاری است.

انسان‌افزار (Humanware)

فناوری مطرح در انسان‌هاست، مانند کارگران، مهندسان، مدیران و دانشمندان، که در تکوین، تکمیل، کاربرد و توسعهٔ فناوری به کار گرفته می‌شود. به عبارت دیگر شامل مهارت‌ها، تجربیات، دانش و خرد، نوآوری و خلاقیت انسان‌هاست.

اطلاعات‌افزار (Infoware)

فناوری‌های مطرح در اطلاعات، اسناد مدارک گوناگون مورد استفاده برای تولید کالاها و خدمات را اطلاعات‌افزار می‌گویند، مانند دستور کارها، رویه‌ها، شرح و توصیف فرایندها و دیگر اسناد، یا مجموعه‌های نرم‌افزاری از این دست.

سازمان‌افزار (Orgware)

سازمان‌افزار شامل مجموعه نظام‌های سازمان‌دهی، ارتباطات، رهبری، ایجاد انگیزه برای بهینه‌سازی تصمیم‌گیری‌ها و تأمین اهداف سازمانی است. از این رو، فناوری مطرح در یک سازمان که در تکوین، به کارگیری و توسعهٔ سازمان استفاده می‌شود، سازمان‌افزار نام دارد.

۲ـ۲ـ۲ مدل چرخهٔ حیات

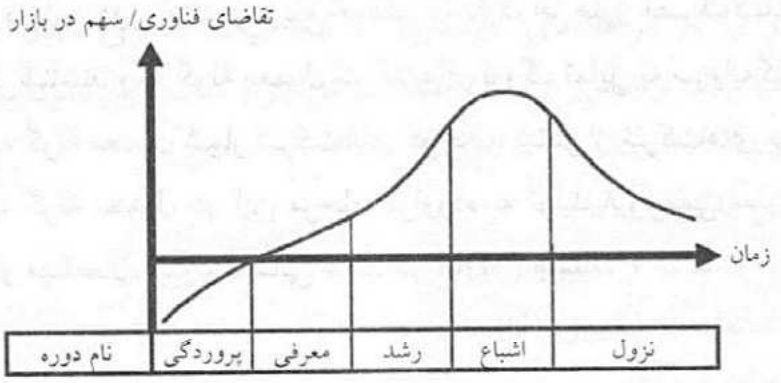
فناوری‌ها یکی پس از دیگری متولد و وارد بازار می‌شوند و مرحله‌های رشد و افول خود را طی می‌کنند و گاهی از رده خارج شده با فناوری‌های دیگر جایگزین می‌شوند. فناوری مانند هر موجود زنده، دوران تولد، رشد، بلوغ و مرگ را طی می‌کند. این مرحله‌ها را **چرخهٔ حیات فناوری** گویند. مرحله‌های دوران حیات فناوری عبارت‌اند از:

- پروردگی[1]؛
- معرفی[2]؛
- رشد[3]؛
- اشباع[4]؛
- نزول[5] (افول).

پیدایش، رشد و کاربرد فناوری، از منحنی ویژه‌ای به نام منحنی S پیروی می‌کند در شکل ۲ـ۲ آمده است. هریک از مرحله‌های چرخهٔ حیات فناوری را به اختصار شرح می‌دهیم.

دورهٔ پروردگی

در این دوره، فراورده‌ها و فرایندهای مرتبط با فناوری در مرحلهٔ نوپایی قرار دارند، به



شکل ۲ـ۲ مرحله‌های تکامل فناوری.

---

1. incubation
2. introduction
3. growth
4. saturation
5. decline

گونه‌ای که مجموعه‌ای از نوآوری‌ها پی در پی رخ می‌دهند تا سرانجام یکی از آنها پیروز شود و فرصت حضور در بازار را پیدا کند (جنگِ ایده‌ها)؛ به عبارت دیگر، در این دوره، فعالیت‌هایی مانند شناسایی و پژوهش دربارهٔ فناوری، تدوین طرح توجیهی، انتخاب فرایند مناسب با فرایند یا تولید، نصب و راه‌اندازی ماشین‌آلات و یادگیری ویژگی‌های فناوری جدید در راستای انتخاب و انتقال فناوری انجام می‌گیرد. ویژگی این دوره، رشد اندک اولیه است که در آن آزمایش‌های تجربی صورت می‌گیرد و دشواری‌های آغازی برطرف می‌شود. در دورهٔ پروردگی، نیروی انسانی شاغل در فناوری، بیشتر پژوهشگران هستند.

پژوهش دربارهٔ فناوری، تدوین طرح توجیهی، انتخاب فرایند مناسب با فرایند یا تولید، نصب و راه‌اندازی ماشین‌آلات و یادگیری ویژگی‌های فناوری جدید در راستای انتخاب و انتقال فناوری انجام می‌گیرد. ویژگی این دوره، رشد اندک اولیه است که در آن آزمایش‌های تجربی صورت می‌گیرد و دشواری‌های آغازی برطرف می‌شود. در دورهٔ پروردگی، نیروی انسانی شاغل در فناوری، بیشتر پژوهشگران هستند.

دورهٔ معرفی

در این مرحله، فناوری وارد بازار شده است، اما بهره‌وری از آن به کُندی صورت می‌گیرد. هرچند که فناوری در این دوره مشتری ویژه خودش را دارد، اما هنوز مصرف‌کنندگان، آن را به گونهٔ کامل نمی‌شناسند و به گونهٔ معمول شرکت‌های بزرگ تمایل به سرمایه‌گذاری در فناوری را ندارند. به گونهٔ معمول شمار شرکت‌های کوچک، بیشتر از شرکت‌های بزرگ، از آن بهره می‌برند. به گونهٔ معمول در این مرحله، فراورده به تولید انبوه نمی‌رسد. در این دوره، پژوهشگران و مهندسان، نیروی انسانی غالب در فناوری هستند.

دورهٔ رشد

در این مرحله، روند استفاده و بهره‌برداری از فناوری به سرعت افزایش می‌یابد. در این مرحله، فعالیت‌هایی مانند حل دشواری‌های موجود در جریان به کارگیری فناوری جدید، افزایش کارایی و گسترش تنوع فراورده‌های تولیدی با به کارگیری فناوری جدید، ارائهٔ آموزش‌های مورد نیاز. برای بهره‌برداری از فناوری جدید صورت می‌گیرد. در این دوره، افزون بر پژوهشگران و مهندسان، تکنسین‌ها نیز نیروی انسانی کارایی تلقی می‌شوند.

دورهٔ اشباع

از آن‌جایی که فناوری در قالب فراورده، خدمات، یا فرایند جلوه می‌کند، رشد آن تا حدودی دوام‌دار و فعالیت‌هایی در راستای اصلاح و بهینه‌سازی شرایط استفاده از فناوری جدید، در دورهٔ اشباع صورت می‌گیرد. مهندسان، تکنسین‌ها و کارگران ماهر، در این دوره از حیات فناوری نقش دارند.

دورهٔ نزول

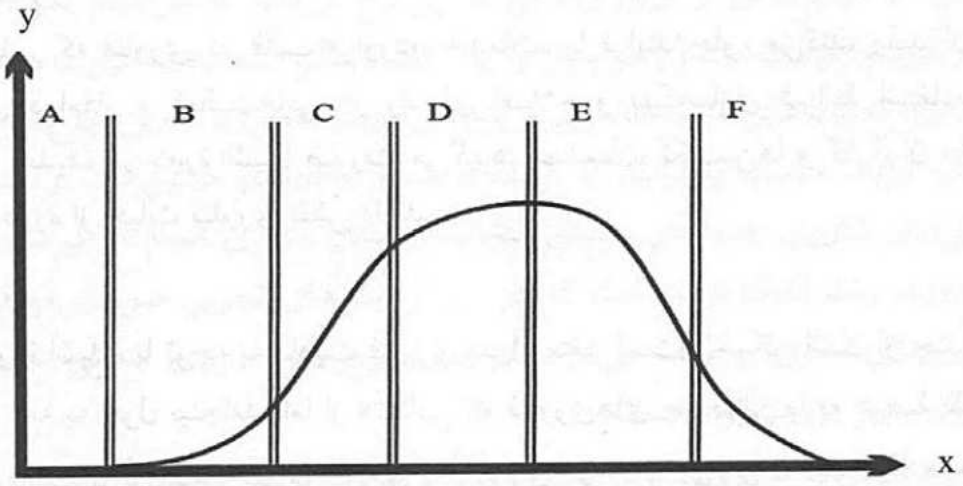
طول دورهٔ اشباع، با توجه به ماهیت فناوری بسیار متغیر است و ممکن است از چند ماه تا چند دهه به طول بینجامد. اما از هنگامی که فناوری‌های جایگزین پا به عرصهٔ ظهور می‌گذارند، مرحلهٔ نزول فناوری قدیمی‌تر آغاز می‌شود. در این مرحله به گونهٔ معمول کشورهای پیشرفته، فناوری‌های منسوخ‌شده را به کشورهای کمتر توسعه‌یافته بفروشند. تکنسین‌ها و کارگران ماهر، اصلی‌ترین کارکنان در این دوره محسوب می‌شوند.

۲ـ۳ رشد بازار در مرحله‌های گوناگون فناوری

هریک از مرحله‌های چرخهٔ حیات فناوری، بر رشد بازار اثر می‌گذارند. تا زمانی که فراورده‌های یک فناوری وارد بازار نشده‌اند، درآمدی ایجاد نمی‌شود. همراه با معرفی و رشد فناوری، فراورده‌های آن نیز وارد بازار می‌شوند و بر توسعهٔ بازار کارایند. شکل ۲ـ۳ بازار را در مرحله‌های گوناگون چرخهٔ حیات فناوری نشان می‌دهد. محور x نشان‌دهندهٔ زمان و محور y نشان‌دهندهٔ ارزش بازار است. این نمودار بر شش بخش A تا F تقسیم شده است:

- پیدایش فناوری (A)
- آغاز به استفاده از فناوری (B)
- رشد استفاده از فناوری (C)
- بلوغ فناوری (D)
- جایگزینی فناوری (E)
- روال فناوری (F)

توجه داشته باشید که در مرحلهٔ پیدایش فناوری، بازار توجهی به فناوری ندارد. در این مرحله، دانشمندان و مهندسان هزینهٔ زیادی را صرف ایجاد فناوری و ساخت و آزمایش نمونهٔ اولیه می‌کنند و مدیران پژوهش و توسعه می‌کوشند تا این دوره به کمینه برسد؛



شکل ۲ـ۳ رشد بازار و مرحله‌های گوناگون چرخهٔ حیات فناوری.

زیرا درآمدی ندارد و هزینهٔ آن نیز بالاست. هنگامی که نخستین کاربردهای فناوری در بازار آشکار شود، ارزش بازار از آن پیروی می‌کند که میزان نفوذ فناوری در بازار به عامل‌هایی مانند نیاز بازار و میزان نوآوری آن بستگی دارد. هنگامی که فناوری به مرحلهٔ بلوغ نزدیک می‌شود، از میزان رشد ارزش بازار کاسته می‌شود و به آرامی کاهش می‌یابد. از این رو، بنگاه‌های اقتصادی‌ای که پس از دورهٔ بلوغ نیز به استفاده از فناوری ادامه می‌دهند، با کاهش نام بازار و در نتیجه کاهش درآمد روبه‌رو می‌شود، تا این که مرحلهٔ زوال و نابودی فناوری فرا رسد.

۲ـ۴ انتقال فناوری در مرحله‌های چرخهٔ حیات

در هر مرحله از چرخهٔ حیات فناوری، به اقتضای شرایط آن مرحله، فضای حاکم بر انتقال فناوری متفاوت است. این فضا را در حالت کلی می‌توان به چهار مرحلهٔ عمده تقسیم‌بندی کرد:

- جابه‌جایی انسان‌ها
- جابه‌جایی دانش فنی
- خرید ماشین‌آلات
- فروش فناوری

اکنون هریک از این چهار مرحلهٔ عمده را مورد بررسی قرار می‌دهیم.

۲ـ۴ـ۱ مرحلهٔ جابه‌جایی انسان‌ها

این مرحله، در عمل متناظر با شرایطی است که فناوری هنوز در مرحلهٔ معرفی قرار

دارد. در این مرحله، فناوری به صورت یک دانش ضمنی یا صریح در اختیار افرادی است که بر روی آن مشغول به کار هستند. در چنین شرایطی نمی‌توان برای در اختیار گرفتن چنین فناوری‌هایی، به خرید ماشین‌آلات یا جابه‌جایی دانش فنی پرداخت. در این شرایط، انتقال فناوری در عمل به معنای انتقال افراد است.

۲ـ۴ـ۲ مرحلهٔ جابه‌جایی دانش فنی

پس از گذر فناوری از مرحلهٔ مصرفی و ورود به فاز رشد فزاینده و بدل دانش ضمنی به دانش صریح، فناوری هستند و مکتوب است، اما در معرض تغییر و تحول قرار دارد و به سرعت رشد می‌کند. در این شرایط می‌توان برای انتقال فناوری، از قراردادهای مبادلهٔ دانش فنی استفاده کرد.

۲ـ۴ـ۳ مرحلهٔ خرید ماشین‌آلات

با گذر از رشد فزاینده و ورود به رشد کاهنده، تمرکز فعالیت‌های نوآوری، از واحد پژوهش و توسعه، به واحد طراحی و مهندسی انتقال می‌یابد و تمرکز اصلی بر بهره‌وری بیشتر از فناوری معطوف می‌شود. در این مرحله، انتقال فناوری در عمل به معنای خرید ماشین‌آلات و دانش فنی است.

۲ـ۴ـ۴ مرحلهٔ فروش فناوری

با گذر از فاز رشد کاهنده و ورود به فاز بلوغ، بهترین راه دسترسی به فناوری، خرید کامل آن است. بنابراین هم برای فروشندهٔ فناوری و هم برای خریدار، به صرفه است که فناوری را مبادله کنند. در این حالت، خریدار، هر آنچه را که می‌خواهد، با پرداخت هزینهٔ آن به دست می‌آورد و از این رو هزینه کردن برای پژوهش و توسعه، توجیه اقتصادی ندارد.

پرسش و پژوهش

۱. فناوری چیست؟
۲. فناوری را از نظر اجزای آن مورد بررسی قرار دهید.
۳. چرخهٔ حیات فناوری را تشریح کنید.
۴. در مورد ارزش بازار و فناوری بحث کنید.
۵. دربارهٔ انتقال فناوری بحث کنید.

۳

مبانی فناوری اطلاعات

اهداف آموزشی

پس از مطالعهٔ این فصل توانایی‌های زیر را کسب خواهید کرد:

فناوری اطلاعات را تعریف کنید.

فناوری اطلاعات و ارتباطات را درک کنید.

عامل‌های کارا بر فناوری اطلاعات را درک می‌کنید.

انجمن فناوری اطلاعات امریکا، فناوری اطلاعات را به این صورت تعریف می‌کند: مطالعه، طراحی، توسعه، کاربرد، پیاده‌سازی، پشتیبانی، یا مدیریت سامانه‌های اطلاعاتی مبتنی بر رایانه. مسئولیت کسانی که در این حوزه کار می‌کنند شامل مدیریت شبکه، توسعه و نصب نرم‌افزار و برنامه‌ریزی و مدیریت چرخهٔ حیات فناوری سازمان است که در اثر آن، سخت‌افزار و نرم‌افزار، نگهداری، روزآمد (آپدیت) یا جایگزین می‌شوند.

۳ـ۱ نگاهی به فناوری اطلاعات

فناوری اطلاعات از دو مؤلفهٔ اصلی تشکیل شده است:

۱. فناوری (technology)

۲. اطلاعات (information)

۳ـ۱ـ۱ مفهوم فناوری

فناوری عبارت است از ابزارها، راهکارها، دانش یا فرایندی که برای بدل ورودی‌ها به خروجی‌ها به منظور ارتقای قابلیت‌های افراد، گروه‌های کاری و سازمان

۳ـ۱ـ۲ مفهوم اطلاعات

- اطلاعات، در کوتاه‌ترین تعریف، داده‌های پردازش شده است و داده‌ها به معنای مواد خام بالقوه معناداری است که از راه روش‌های پژوهشی یا ابزارهای شناختی مانند دستگاه زبان، حواس پنج‌گانه، ذهن و مغز و حتی تجربهٔ خود، از کالا، رویدادها، اشیا، و... به دست می‌آوریم.
- اطلاعات زیرمجموعه‌ای از دانشی است که تصادفاً یا تعهداً از راه پژوهش یا تجربه به دست می‌آید. به عبارت ساده‌تر، اطلاعات، بخشی از سرجمعِ ذخیرهٔ دانش بشری است.

۳ـ۲ مفهوم فناوری اطلاعات

به کارگیری رایانه‌ها و تجهیزات ارتباطات دوربُرد برای ذخیره، بازاریابی، انتقال و پردازش داده‌ها در حوزهٔ تجاری یا هر بنگاه است. این واژه به گونهٔ معمول برای رایانه‌ها و شبکه‌های رایانهٔ به کار گرفته می‌شود، اما فناوری‌های پخش اطلاعات مانند تلویزیون و تلفن را نیز دربر می‌گیرد. صنایع پرشماری به فناوری اطلاعات مربوط می‌شوند، مانند سخت‌افزار رایانه، نرم‌افزار، الکترونیک، نیمه‌رساناها، اینترنت، تجهیزات مخابرات دوربرد، تجارت الکترونیک و خدمات رایانه‌ای.

۳ـ۳ فناوری اطلاعات و ارتباطات

اما مفهوم ارتباطات چیست؟ در هر ارتباطی، یک یا چند پیام منتقل می‌شود و این پیام باید از یک کانال یا محیط ارتباطی بگذرد. بنابراین، در هر ارتباط، چهار عنصر وجود دارد:

- فرستنده؛
- گیرنده؛
- پیام؛
- محیط ارتباطی.

فرستنده، کسی یا چیزی است که پیامی برای ارسال دارد و گیرنده کسی یا چیزی است که پیام دریافت می‌کند و این پیام از راه یک محیط ارتباطی منتقل می‌شود. برای نمونه، دو نفر که با یکدیگر از راه تلفن ثابت ارتباط برقرار می‌کنند، در هر لحظه یکی فرستنده و دیگری گیرندهٔ پیام است و خطوط تلفن به عنوان محیط ارتباطی تلقی می‌شود. گاهی فناوری اطلاعات را هرگونه روشی برای تبادل اطلاعات میان دو یا چند نقطه تعریف می‌کنند. به این ترتیب، مفهوم فناوری اطلاعات و ارتباطات، زیر مفهوم فناوری اطلاعات قرار می‌گیرد و فناوری اطلاعات بار معنایی کامل‌تری دارد.

۳ـ۴ عامل‌های کارا بر توسعهٔ فناوری اطلاعات

سرعت رشد فناوری اطلاعات در مقایسه با دیگر فناوری‌ها بسیار چشمگیر بوده است. در این بخش عامل‌های کارا بر توسعهٔ فناوری اطلاعات را مورد بررسی قرار می‌دهیم:

- **رشد فناوری ریز پردازنده‌ها و کوچک شدن ابعاد آنها:** نخستین رایانه‌ای که ساخته شد مساحتی در حد یک ساختمان بزرگ را اشغال می‌کرد. اما اختراع ترانزیستور و مدارهای مجتمع (آی‌سی) و قرار گرفتن شمار زیادی از ترانزیستورها در تراشه‌ها، سبب کوچک و کوچک‌تر شدن رایانه‌ها شد.
- **کاهش بهای رایانه:** با گذشت زمان، قابلیت‌های رایانه افزایش یافت و بهای آن نیز کاهش چشمگیری پیدا کرد. درنتیجه، به‌آسانی در اختیار همگان قرار گرفت. درواقع، کاهش بهای رایانه‌ها سبب افزایش به کارگیری آنها شده است.
- **توسعهٔ شبکه‌های رایانهٔ و اینترنت:** با رشد فناوری‌های مخابراتی، رایانه‌های موجود در مکان‌های گوناگون از راه شبکه‌های رایانهٔ به هم متصل شدند که سبب سهولت در تبادل اطلاعات شده است.

ظهور اینترنت به عنوان ارائه‌دهندهٔ مدل‌های ارتباطی متفاوت، مانند وب[1]، رایانامه[2]، تلفن‌های اینترنتی، ویدئو کنفرانس و چت[3] سبب شده است که فناوری اطلاعات با رشد فزاینده‌ای روبه‌رو شود. در سال‌های اخیر، سرعت رشد و همه‌گیر شدن اینترنت، از فناوری‌هایی مانند تلفن، رادیو و تلویزیون، به مراتب بیشتر بوده است.

---

1. Web
2. Email
3. Chat

پرسش و پژوهش

۱. مفهوم فناوری اطلاعات را بیان کنید.
۲. فناوری اطلاعات از چه اجزایی تشکیل شده است؟
۳. مفهوم فناوری اطلاعات و ارتباطات را بیان کنید.
۴. عامل‌های کارا بر توسعهٔ فناری اطلاعات چیست؟
۵. دربارهٔ کاربرد فناوری اطلاعات در ایران پژوهش کنید و آن را با کشور مالزی مقایسه کنید.

۴

جامعهٔ اطلاعاتی

اهداف آموزشی

پس از مطالعهٔ این فصل توانایی‌های زیر را کسب خواهید کرد:

با مفهوم جامعه و تکامل جامعهٔ بشری آشنا می‌شوید.

ویژگی‌های جامعهٔ اطلاعاتی و توصیف آن را درک می‌کنید.

در فصل سوم به مفهوم فناوری اطلاعات و عامل‌های توسعه آن پرداختیم. فناوری اطلاعات آثار پرشماری در جوامع بشری داشت و شکل جامعه را عوض کرد و جامعهٔ جدیدی به نام جامعهٔ اطلاعاتی را به وجود آورد. در این فصل به مفهوم جامعهٔ ارتباطی و ویژگی‌های آن، از جمله نیروی کار، کار و اشتغال در این جامعه می‌پردازیم.

۴ـ۱ تکامل جوامع بشری

جوامع بشری از بدو پیدایش، به شکل‌های گوناگونی درآمد و گرفتار تغییرهای زیادی شد. سیر تکامل جوامع بشری را می‌توان به صورت زیر بیان کرد:

- جامعهٔ آغازی که بر زندگی انسان‌های نخستین مربوط می‌شود. در این جوامع، بشر به گردآوری آذوقه و شکار می‌پرداخت.
- جامعهٔ ایلیاتی یا جامعهٔ قبیله‌ای که به اهلی کردن جانوران مربوط است.

- جامعهٔ روستایی که مبتنی بر کشاورزی بود.
- جامعهٔ شهری که با افزایش جمعیت و ایجاد قانون شکل گرفت.
- جامعهٔ صنعتی که مبتنی بر صنعت است.
- جامعهٔ اطلاعات که مبتنی بر اطلاعات است.

۴ـ۲ ویژگی‌های جامعهٔ اطلاعاتی

جامعه‌ای که در آن کیفیت زندگی، پیشرفت‌های اقتصادی، فرهنگی و اجتماعی به گونهٔ فزاینده‌ای به تولید اطلاعات و بهره‌برداری از آن متکی است، جامعهٔ اطلاعاتی نامیده می‌شود.

جامعهٔ اطلاعاتی، جامعهٔ وابسته به خدمات اطلاعاتی و رسانه‌های همگانی است و با سرعتی بیشتر از دیگر جوامع و با سلطهٔ بیشتر بر اندوخته‌های علمی و تجربی پیش می‌رود. در چنین جامعه‌ای، ارتباطات عامل اصلی انتقال اطلاعات برای ایجاد دگرگونی در افراد به منظور دستیابی به اطلاعات است و ارزش اطلاعات، به عنوان عامل اصلی در توسعهٔ جامعه به‌شمار می‌رود. به عبارت دیگر، جامعهٔ اطلاعاتی، جامعه‌ای است که در آن، اطلاعات علمی حاکم است. اما ویژگی‌های جامعهٔ اطلاعات را می‌توان به چند دسته تقسیم کرد:

۱. **ویژگی فناوری:** ویژگی این گروه، تشکیل رسانه‌هاست که یک نظام فراگیر، جامع و گسترده را به همراه آورده و به گونهٔ کامل مسلط بر حیات انسان است؛ و این خود ترکیبی از فناوری‌های اطلاعاتی، ارتباطی، رایانه، دورنگار، چاپگر، ویدئو، ماهواره، تلویزیون و مانند آن است.

۲. **ویژگی اقتصادی:** رویکرد اقتصادی به نقش روزافزون فناوری اطلاعات در فرایند تولید، پخش و مصرف، به‌ویژه در زمینهٔ نوآوری و رقابت اشاره دارد. جامعهٔ اطلاعاتی، نوع جدیدی از تقسیم کار را مطرح می‌کند و در نتیجه مشاغلی از میان می‌روند و شغل‌های جدیدی ایجاد می‌شوند.

۳. **ویژگی شغلی:** یکی از ویژگی‌های مهم جامعهٔ اطلاعاتی، تغییرحرفه‌ها و مشاغل است. هرگاه حرفه‌ها در فعالیت‌های اطلاعاتی تمرکز پیدا کنند، معنایش این است که وارد جامعهٔ اطلاعاتی شدیم.

۴. **ویژگی مکانی:** در جامعهٔ اطلاعاتی، شبکه‌های اطلاعاتی نقاط دور دست را به یکدیگر مرتبط می‌کنند.

۵. **ویژگی فرهنگی:** به لحاظ فرهنگی، دانش مبتنی بر سرمایه، به‌آرامی جای خود را به سرمایهٔ مبتنی بر دانش داده است و آگاهی به نوعی سرمایهٔ فرهنگی تلقی می‌شود و به این ترتیب، اهمیتی که جهان گذشته به سرمایهٔ مالی قائل بود کاهش یافته و سرمایه‌های مبتنی بر آگاهی از اهمیت بیشتری برخوردار شده است.

۴ـ۳ نیروی کار فناوری اطلاعات

با ورود به جامعهٔ اطلاعاتی، مشاغل گرفتار تغییرهای اساسی شدند و درنتیجه نیروی کار این جوامع باید خودشان را با این تغییرهای شغلی وفق دهند تا بتوانند در این جوامع صاحب شغل و کار شوند. ورود به جامعهٔ اطلاعات مستلزم آشنایی با فناوری اطلاعات و استفادهٔ درست از آن است. جامعهٔ اطلاعاتی متکی بر زیرساخت نیروی انسانی ماهر در فناوری اطلاعات و کاربردهای آن است.

۴ـ۳ـ۱ نیروی کار اصلی فناوری اطلاعات

نیروی کار اصلی فناوری اطلاعات آنهایی هستند که نقش مهمی در توسعهٔ فناوری اطلاعات دارند. این نیروها را می‌توان به چهار دسته تقسیم کرد:

دانشمندان رایانه

افرادی هستند که در زمینهٔ پژوهش، طراحی و ساخت رایانه‌های مدرن، توسعهٔ فناوری اطلاعات در کارهای نو، نوآوری‌ها و خلاقیت‌ها در گسترش خدمات فناوری اطلاعات نقش اساسی دارند. این افراد به گونهٔ معمول در دانشگاه‌ها و مراکز پژوهشی فعالیت دارند.

مهندسان رایانه

این افراد در حوزه‌های طراحی و توسعهٔ نرم‌افزار و سخت‌افزار سامانه‌ها فعالیت می‌کنند و ممکن است با دانشمندان رایانه همکاری داشته باشند.

تحلیل‌گران سامانه

آنها با استفاده از دانش و مهارت خود راجع به حل مسئله‌ها، روش‌های مبتنی بر رایانه

را برای رفع نیازهای سازمان‌ها ارائه می‌دهند. این افراد ممکن است سامانه‌های جدید نرم‌افزاری و سخت‌افزاری را طراحی کنند یا کاربرد نرم‌افزارهای جدید را پیشنهاد دهند.

برنامه‌نویسان رایانه

این افراد، با استفاده از روش‌های ارائه‌شده توسط تحلیل‌گران، برنامه‌های لازم را می‌نویسند.

۴ـ۳ـ۲ مشاغل مرتبط با فناوری اطلاعات

مشاغل پرشماری مرتبط با فناوری اطلاعات هستند و روزانه، همراه با پیشرفت فناوری اطلاعات، بر تنوع آنها افزوده می‌شود. برخی از این مشاغل عبارت‌اند از مهندسان و مدیران سامانه‌های رایانه‌ای، تحلیل‌گران سامانه، برنامه‌نویسان رایانه، تکنسین‌های رادیو و تلویزیون، اپراتورهای تجهیزات رایانه‌ای، تعمیرکاران تجهیزات پردازش داده‌ها، اپراتورهای تجهیزات مخابراتی، تعمیرکاران و نصب‌کنندگان خطوط برق و تلفن، تعمیرکاران تجهیزات دقیق الکترونیکی، مهندسان برق و الکترونیک، متخصصان پشتیبان رایانه، دانشمندان رایانه، اپراتورهای ماشین‌های دفتری و محاسبه‌ها، واردکنندگان اطلاعات، متخصصان بازاریابی الکترونیک، متخصصان تبلیغات تجاری اینترنتی، طراحان صفحه‌های وب، برنامه‌نویسان صفحه‌های وب، متخصصان امور هنری وب، طراح گرافیکی وب، طراح شبکهٔ چندرسانه‌ای، برنامه‌نویس چندرسانه‌ای، مدیریت فراورده‌های نرم‌افزاری، مدیریت فراورده‌های مخابراتی، و این سیاهه (لیست) پایان ندارد.

۴ـ۳ـ۳ مهارت‌ها و دانش مورد نیاز نیروی کار فناوری اطلاعات

نیروی کار فناوری اطلاعات به دانش و مهارت متنوعی نیاز دارد تا از عهدهٔ وظایف خود برآید. این مهارت‌ها را می‌توان به سه گروه تقسیم کرد. البته سهم هریک از گروه‌ها در مشاغل گوناگون متفاوت است.

۱. دانش فنی دربارهٔ فناوری اطلاعات؛
۲. دانش صنعتی و تجاری (تشخیص هزینه‌ها، زمانبندی و بودجه)؛
۳. مهارت‌های ارتباطی و سازماندهی (مهارت لازم برای کار تیمی).

۴ـ۴ به‌کارگیری و پیاده‌سازی فناوری اطلاعات در سازمان

به کارگیری فناوری اطلاعات در سازمان‌ها تغییرهای بنیادین را در همهٔ زمینه‌ها نوید می‌دهد. امروزه سازمان‌ها برای بهره‌برداری از فناوری اطلاعات به عنوان یک امتیاز رقابتی، ناگزیر هستند.

۴ـ۴ـ۱ محورهای به‌کارگیری فناوری اطلاعات در سازمان

در به‌کارگیری فناوری اطلاعات در سازمان، سه محور مورد توجه است:

- نیروی انسانی؛
- زیرساخت؛
- کاربردها.

در زمینهٔ نیروی انسانی، مسئلهٔ آموزش، افزایش مهارت و ایجاد فرهنگ سازمانی، به عنوان موضوع‌های اساسی مطرح هستند. در محور زیرساخت، شبکه، تجهیزات فنی، مقررات و قوانین، به عنوان موضوع‌های اصلی مطرح هستند. در محور کاربردها، آموزش الکترونیک، سامانه بدون کاغذ، سخنرانی راه‌دور، دولت الکترونیک، تجارت الکترونیک مطرح هستند.

۴ـ۴ـ۲ پیاده‌سازی فناوری اطلاعات در سازمان‌ها

مطالعات در زمینهٔ پیاده‌سازی فناوری اطلاعات در سازمان‌ها نشان می‌دهد که فناوری اطلاعات باید در دو حوزهٔ پژوهش و اجرا در سازمان‌ها مورد بحث قرار گیرد. بخش پژوهش، وظیفهٔ شبیه‌سازی محیطی و تجربهٔ مجازی با هزینهٔ اندک، همراه با برنامه‌ریزی، مدل‌های تصمیم‌گیری و ایجاد خلاقیت را برعهده دارد. در حوزهٔ اجرای فناوری اطلاعات در زمان‌ها، دو دیدگاه اساسی باید مورد توجه قرار گیرند:

- دیدگاه فنی و مهندسی؛
- دیدگاه مدیریتی.

در هریک از این دو دیدگاه، موضوع‌های ویژه‌ای باید مورد توجه قرار گیرند. موضوع‌های مورد توجه در دیدگاه فنی و مهندسی عبارت‌اند از:

- نرم‌افزار (برنامه‌هایی که برای دریافت، پردازش و تولید اطلاعات)؛
- سخت‌افزار (سخت‌افزارهای لازم برای ایجاد بستر فناوری اطلاعات)؛

- آموزش نیروی انسانی (آموزش نیروهای درگیر و مصرف‌کنندگان فراورده‌های فناوری اطلاعات) آموزش نیروی انسانی (آموزش نیروهای درگیر و مصرف‌کنندگان فراورده‌های فناوری اطلاعات)؛
- اطلاعات و داده‌های خام (داده‌ها که مادهٔ اولیهٔ فناوری اطلاعات است باید دقیق، قابل اعتماد و جدید باشند)؛
- سامانه‌های ارتباطی (برقراری ارتباط میان رایانه‌ها).

اما در دیدگاه مدیریتی، طراحی و پیاده‌سازی سامانه‌های اطلاعات مدیریت (MIS)، سامانه‌های مدیریت منابع سازمان (ERP) مطرح هستند که در سازمان‌های گوناگون پیاده‌سازی و اجرا شده‌اند.

۴ـ۴ـ۳ اجرا و به کارگیری فناوری اطلاعات

بدیهی است که نمی‌توان با یک برنامهٔ جامع فناوری اطلاعات برای همهٔ سازمان‌ها، شرکت‌ها و مؤسسه‌ها، فناوری اطلاعات را پیاده‌سازی و اجرا کرد. مهم‌ترین عامل‌هایی که باید در پیاده‌سازی فناوری اطلاعات در سازمان‌ها در نظر گرفته شود عبارت‌اند از:

فرهنگ: برای اجرای موفقیت‌آمیز فناوری اطلاعات، نیاز به فرهنگ‌سازی است.

اعتقاد و باور مدیران ارشد سازمان: هر چه مدیران ارشد سازمان، به فناوری اطلاعات توجه بیشتری داشته باشند، احتمال موفقیت به کارگیری آن بیشتر است.

آسیب‌شناسی: دشواری‌ها و موانع پیاده‌سازی فناوری اطلاعات در سازمان شناسایی و مرتفع شوند.

حرکت به سمت ساختار فرایندی: ساختار سازمان‌هایی که از فناوری اطلاعات استفاده می‌کنند، باید ازشکل سلسله مراتبی و وظیفه‌ای خارج شود و به شکل فرایندی درآید.

درگیری کلیدی کارکنان سازمان در امور فناوری اطلاعات: همهٔ افراد سازمان، از مدیران ارشد تا کارمندان سطح فرایند باید درگیر به کارگیری فناوری اطلاعات شوند.

بهبود شاخص‌های بهره‌وری: شاخص‌های اندازه‌گیری بهره‌وری در سازمان باید بهبود یابد و از اطلاعات برای تبدیل به دانش استفاده شود.

کوچک‌سازی: خارج کردن فعالیت‌های غیرمحوری از سازمان که منجر به کوچک‌سازی می‌شود.

۴ـ۴ـ۴ موانع به‌کارگیری فناوری اطلاعات در سازمان

این نکته را نباید فراموش کرد که هدف از به‌کارگیری فناوری اطلاعات، ارتقای سطح زندگی و تحصیلی افراد جامعه و گسترش بازارهای درونی است. کمبود دانش مدیران در حوزهٔ فناوری اطلاعات مانع اصلی پذیرش این فناوری در سازمان است، اما عامل‌های دیگر نیز دخالت دارند. بنابراین موانع به‌کارگیری فناوری اطلاعات در سازمان را می‌توان به شرح زیر بیان کرد:

- **مدیران عالی:** بیشتر مدیران عالی، نقش فناوری اطلاعات را به‌اندازهٔ کافی درک نمی‌کنند.
- **کارکنان بخش فناوری اطلاعات:** این افراد نیازهای اطلاعاتی مدیران را به‌درستی درک نمی‌کنند و آمادگی گسترش فناوری اطلاعات را در سازمان ندارند.
- **دیگر کارکنان عملیاتی:** ممکن است این کارکنان تصور کنند که با به‌کارگیری فناوری اطلاعات در سازمان، شغل خود را از دست می‌دهند.
- **کمبود امکانات مالی و عدم الویت‌بندی در تحصیل منابع:** به‌کارگیری فناوری اطلاعات، نیازمند سرمایه‌گذاری و اختصاص بودجهٔ لازم است.
- **آموزش و زیرساخت نامناسب.**

پرسش و پژوهش

۱. مفهوم جامعهٔ بشری را بیان کنید.
۲. جامعهٔ اطلاعاتی چیست و چه ویژگی‌هایی دارد؟
۳. ویژگی‌های نیروی کار فناوری اطلاعات کدام‌اند؟
۴. به نظر شما کشور ما تا چه حدی به جامعهٔ اطلاعاتی نزدیک شده است؟

۵

آشنایی با اینترنت

اهداف آموزشی

پس از مطالعهٔ این فصل توانایی‌های زیر را کسب خواهید کرد:

به مفهوم اینترنت پی می‌برید.

کاربردهای اینترنت را خواهید شناخت.

طریقهٔ وصل شدن به اینترنت را خواهید شناخت.

با مفهوم وب‌سایت و سرورهای اینترنتی آشنا می‌شوید.

یاد می‌گیرید چگونه بارگیری (دانلود) و بارگذاری (آپلود) کنید.

مرورگرهای اینترنت را خواهید شناخت.

اینترنت یک شبکهٔ جهانی از رایانه‌هاست که سبب می‌شود که کاربران در سراسر جهان، اطلاعات و منابع خود را به اشتراک بگذارند و معامله‌های تجاری را انجام دهند. اینترنت از اتصال مجموعه‌ای از شبکه‌های کوچک و بزرگ تشکیل شده است و هر میزبان (هر رایانه که به اینترنت وصل شده است) به شماری از رایانه‌های دیگر وصل است (شکل ۵ـ۱). هنگامی که کاربرِ اینترنت برای دستیابی به اطلاعات و خدمات، به اینترنت وصل می‌شود، می‌گوییم کاربر آنلاین است.

شکل ۵ـ۱ اینترنت یک شبکهٔ جهانی است.

اینترنت از چندین رایانه تشکیل شده است (از یک رایانه شخصی که در خانه یا اداره است تا ابررایانه‌هایی که توسط دولت یا پژوهشگران استفاده می‌شوند) که توسط یک روش ارتباطی به هم وصل شده‌اند که به آن پروتکل می‌گویند. پروتکل مجموعه‌ای از قوانین استاندارد است که دستگاه‌های شبکهٔ رایانه‌ای، هنگام ارسال و دریافت داده از آن پیروی می‌کنند. هر رایانهٔ که به اینترنت وصل می‌شود از پروتکل TCP/IP (Transmission Control Protocol/ Internet Protocol) استفاده می‌کند. TCP/IP سبب می‌شود که رایانه‌های متفاوت با سیستم‌عامل‌های متفاوت بتوانند با هم ارتباط برقرار کنند. در ادامه در مورد TCP/IP و فناوری‌های دیگر اینترنت بیشتر شرح داده شده است.

انتقال اینترنت از راه شبکه‌های فیبر نوری پرسرعت انجام می‌شود که شبکه‌های سراسر جهان را به هم وصل می‌کنند. این شبکه‌های پرسرعت، که بدنهٔ اینترنت را فراهم می‌کنند، چند حامل ارتباطی دارند (ارتباط‌های AT&T، MCI، XO در امریکا، ارتباط Telstra در استرالیا، ارتباط CERNET در آسیا).

اگرچه حامل‌های ارتباطی نقش مهمی دارند، اما اینترنت را کنترل نمی‌کنند. در حقیقت، هیچ سازمان خصوصی‌ای اینترنت را کنترل نمی‌کند. چندین گروه، مانند National Science Foundation (NSF)، InterNIC و Internet Society (ISOC) روی استانداردسازی توسعهٔ فناوری اینترنت کار می‌کنند و برخی از فرایندهای اینترنت را مدیریت می‌کنند.

۵ـ۱ کاربردهای اینترنت

اینترنت بسیاری از کارها را آسان‌تر کرده است. برای نمونه می‌توانید در خانه خود بنشینید، به اینترنت وصل شوید و خریدهای روزانهٔ خود را انجام دهید. به جای رفتن در بانک و صف‌های طولانی، با استفاده از اینترنت کارهای بانکی خود را انجام دهید. اینترنت سبب شده است که در وقت و انرژی انسان صرفه‌جویی شود. در ادامه برخی از کاربردها اینترنت شرح داده شده است.

خرید اینترنتی

برخی از فروشندگان فراورده‌های خود را برای فروش در اینترنت قرار می‌دهند و در وب‌سایت خود ارائه می‌دهند. به این وب‌سایت‌ها فروشگاه اینترنتی می‌گویند. می‌توانید در منزل بنشینید و وارد یک سایت فروشگاه اینترنتی شوید. فراورده دلخواه خود را برگزینید، آن را از نظر کیفیت و بها با کالاهای مشابه مقایسه کنید و سپس مبلغ آن را توسط کارت اعتباری پرداخت کنید. پس از چند روز کالای مورد نظر خود را توسط پست دریافت خواهید کرد. یا پس از دریافت کالا توسط پست، هزینهٔ کالا را به مأمور پست پرداخت خواهید کرد. به این روال خرید اینترنتی می‌گویند.

بانکداری الکترونیک (E-Banking)

به فعالیت‌های بانکی که از راه شبکه‌های رایانهٔ انجام می‌گیرد، بانکداری الکترونیک می‌گویند.

تجارت الکترونیک

تجارت الکترونیک عبارت است از تعامل سامانه‌های ارتباطی، سامانه‌های مدیریت اطلاعات و امنیت که به کمک آنها امکان مبادلهٔ اطلاعات تجاری و الکترونیک، رعایت حقوق مصرف‌کننده از جمله حقوق شخصی، حفاظت از اطلاعات، رعایت قوانین تجاری به منظور ایجاد یک بازار الکترونیک مطمئن و معتبر از اهمیت بالایی برخوردار است.

کتابخانهٔ الکترونیکی (E-Library)

می‌توانید از راه اینترنت کتابخانه‌ها را جستجو کنید و از امکانات اینترنتی کتاب‌ها بهره ببرید. کتابخانهٔ الکترونیک سبب افزایش دسترسی به منابع کتابخانه‌ای، بهبود خدمات،

ارائهٔ خدمات جدید شده است. توسعهٔ استفاده از کتابخانه‌های الکترونیک، کاهش هزینه‌های خرید را به دنبال داشته است.

گفتگوهای اینترنتی (Chat)

کاربران می‌توانند در هر کجای جهان از احوال یکدیگر باخبر شوند و فایل، تصویر یا صوت را برای یکدیگر بفرستند. به کمک سرویس‌دهنده‌ها و سرویس‌گیرنده‌ها می‌توان از سراسر جهان در یک بحث زنده شرکت کرد.

رایانامه (E-Mail)

ینترنت می‌توانید به دیگران نامه بفرستید و از دیگران نامه دریافت کنید. با رایانامه می‌توانید فایل‌های گرافیک را نیز ارسال کنید. با استفاده از اینترنت می‌توانید به دیگران نامه بفرستید و از دیگران نامه دریافت کنید. با رایانامه می‌توانید فایل‌های گرافیکی، صدا و فیلم را نیز ارسال کنید.

مجله‌های الکترونیکی

با گسترش اینترنت در عرصه‌های گوناگون اطلاع‌رسانی، بیشتر ناشران اقدام به راه‌اندازی وب‌سایت کرده‌اند.

گروه‌های خبری

گروه‌های خبری در زمینه‌های سیاسی، اجتماعی، فرهنگی، تجاری و اطلاع‌رسانی فعالیت می‌کنند. عضویت در این گروه‌های خبری، اخبار مربوطه به رایانامه شما فرستاده می‌شود. بهتر است پیش از عضویت در گروه‌های خبری، اخبار و اطلاعات آن را مورد بررسی قرار دهید.

۵ـ۲ وصل شدن به اینترنت

برای برخورداری از مزیت‌های رایانامه، وب، و... ابتدا باید رایانه را به اینترنت وصل شوید. دستیابی به اینترنت در سازمان‌های متفاوت، مانند کتابخانه‌ها، مدارس و محیط کار، متفاوت است. برای نمونه، برخی از کتابخانه‌های عمومی رایانه‌هایی دارند که به اینترنت وصل هستند و همه می‌توانند از آن استفاده کنند. بیشتر شرکت‌ها دستیابی به اینترنت را برای کارمندان خود فراهم می‌کنند. دانشجویان نیز در مرکز رایانه دانشگاه به اینترنت دستیابی دارند.

رایانه‌های کتابخانه‌ها، مدارس، دانشگاه‌ها و سازمان‌های دیگر توسط کابل به شبکهٔ داخلی یا محلی LAN (Local area network) وصل می‌شوند. LAN رایانه‌های درون ساختمان یا دانشگاه را به هم وصل می‌کند، پس کاربران می‌توانند داده و منابع، مانند پرینتر، را به اشتراک بگذارند. هنگامی که سازمان شبکهٔ محلی خود (LAN) را مستقیماً به اینترنت وصل کند، همهٔ رایانه‌های روی شبکهٔ LAN به اینترنت دستیابی خواهند داشت.

۵ـ۳ وب‌سایت‌ها

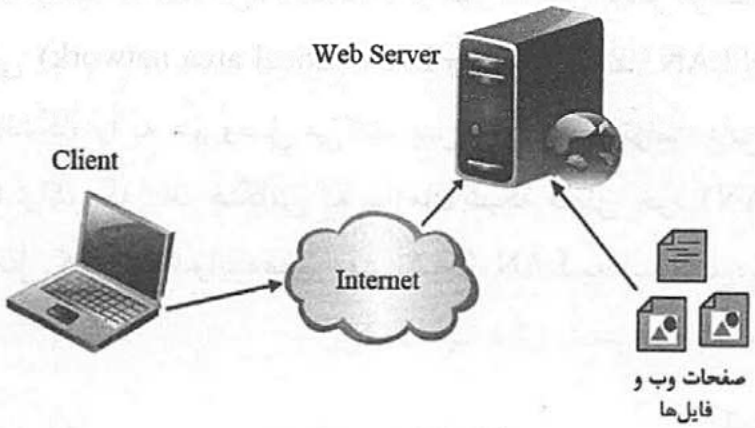
امروزه وب شامل میلیون‌ها وب‌سایت است؛ یک وب‌سایت تجاری یا وب‌سایت یک شرکت شامل چندین صفحه است، که صفحهٔ خانهٔ یا آغازه آن (home page) شامل اطلاعات معرفی و لینک‌هایی به صفحه‌های دیگر وب‌سایت است. برای رفتن به صفحه‌های دیگر باید لینک مربوطه را کلیک کنید تا صفحهٔ آن باز شود. این صفحه‌ها می‌توانند شامل اطلاعاتی در مورد فراورده، سرویس‌ها، کارمندان، تاریخچهٔ شرکت و ... باشند.

وب پورتال یک نوع از وب‌سایت است که درگاهی به سطح وسیعی از محتویات و سرویس‌ها پیشنهاد می‌دهد. برای نمونه وب‌سایت‌های Yahoo و MSN پورتال‌های جذاب و عمومی هستند که اخبارهای بین‌المللی، اخبار آب و هوا و اخبار ورزشی، اطلاعات فروشگاه‌ها، نقشه، ابزار جستجو و لینک‌هایی به سایت‌های دیگر را ارائه می‌دهند. برخی از پورتال‌ها نیز تنها بر روی موردهای ویژه‌ای تمرکز دارند.

۵ـ۴ سرورهای اینترنتی

وب سرور، رایانه‌ای است که صفحه‌های وب در آن قرار می‌گیرند. وب سرور درخواست‌ها را که به صورت http هستند، از کاربران می‌گیرد و پاسخ را به آنها ارسال می‌کند. پاسخ همان صفحه‌های وب هستند که به زبان HTML هستند (شکل ۵ـ۲).

سرور یک رایانه همیشه روشن و همیشه در دسترس است، زمانی که این دسترسی تنها در محدودهٔ یک شبکه درونی باشد، آن را سرور تحت شبکه می‌نامیم و به این معنا خواهد بود که همهٔ رایانه‌های موجود در این شبکه از این رایانه فرمان می‌گیرند و نیازهای



شکل ۵ـ۲ سرور اینترنتی.

شبکهٔ خود را به کمک آن تأمین می‌کنند و سرور نقش آنها را در شبکه معین می‌کند، حال اگر گسترهٔ این شبکه را کمی بیشتر کنیم و آن را متشکل از همهٔ رایانه‌هایی که از راه اینترنت به هم وصل شده‌اند بدانیم، با گروه بسیار بزرگی از رایانه‌های همیشه روشن و همیشه در دسترس از راه اینترنت روبه‌رو هستیم که به آنها سرورهای اینترنتی گفته می‌شود و وظیفه دارند تا اطلاعاتی که در هر زمان از شبانه‌روز، بر روی پهنای اینترنت جستجو می‌کنید را در اختیار قرار دهند. بنابراین به دو دسته‌بندی کلی دست می‌یابیم:

- سرور (server): رایانهٔ که سرویس می‌دهد.
- کلاینت (Client): رایانهٔ که سرویس می‌گیرد.

زمانی که شما به مرور وب و استفاده از انواع خدمات اینترنتی می‌پردازید، در واقع در نقش سرویس‌گیرنده عمل می‌کنید و رایانهٔ که از آن‌سوی شبکه به شما خدمات را ارائه می‌کند، سرویس‌دهنده یا همان سرور نام دارد و جهان اینترنت با ارتباط میلیون‌ها رایانه سرویس‌دهنده و سرویس‌گیرنده شکل می‌گیرد. در شبکهٔ اینترنت، از آن‌جایی که مهم‌ترین فاکتور به هنگام دریافت خدمات، پایداری یک سرور به‌شمار می‌رود، از این رو محل‌های ویژه‌ای در سراسر جهان با نام مرکز داده (Data Center) وجود دارد تا تنها به نگهداری از سرورها بپردازند و با تمرکز بر روی کیفیت شبکه و پشتیبانی قطعه‌ها و نرم‌افزارهای مورد نیاز، به صورت تخصصی شرایط را برای میزبانی وب و استفاده از سرورها به دور از دشواری‌ها و مسئله‌های پرشمار پیرامون آن فراهم آورند.

۵ـ۵ نشانی IP و نام دامنه

نشانی IP (Internet Protocol address)، عدد واحدی است که هر رایانه یا دستگاهی که به اینترنت وصل می‌شود را شناسایی می‌کند. اینترنت با توجه به نشانی IP، داده را به دستگاه یا رایانه درست ارسال می‌کند. هر نشانی IP چهار گروه از اعداد دارد که با فاصله یا نقطه از هم جدا شده‌اند، مانند "۲۱۶.۲۳۹.۳۲.۲۰".

هر رایانه شخصی هنگامی که به اینترنت وصل می‌شود یک نشانی IP دارد. رایانه‌هایی که همیشه به اینترنت وصل هستند، مانند وب سرورها یا رایانه‌های شخصی که اتصال ADSL دارند، نشانی ثابتی دارند که گاهی وقت‌ها تغییر می‌کند. رایانه‌هایی که با اتصال موقت، مانند dial-up وصل می‌شوند در هر اتصال، نشانی IP موقت دارند.

چون به یاد سپردن نشانی‌های IP برای مردم سخت است، وب‌سرورها با نام دامنه ارجاع داده می‌شوند. نام دامنه یک متن معادل برای یک نشانی IP است. برای نمونه، نام دامنهٔ "google.com" معادل نشانی IP، "216.239.32.20" است. هنگامی که نام دامنه در نوار نشانی مرورگر تایپ می‌شود، مرورگر در سرور (Domain Name System DNS)، به دنبال نشانی IP آن می‌شود. DNS دارای نام سرورها است. نام سرور، یک بانک اطلاعاتی از نام‌های دامنه و نشانی‌های IP است. DNS نام دامنه را به نشانی IP ترجمه می‌کند و آن را به مرورگر برمی‌گرداند. سپس درخواست به وب سروری که صفحه در آن ذخیره شده است ارسال می‌شود.

◄ **نکته:** برای به دست آوردن نشانی IP یک نام دامنه، کادر دیالوگ Run را باز کنید. Nslookup را تایپ کنید. سپس دکمهٔ OK را کلیک کنید. پس از فرمان > ، نام دامنه را تایپ کنید. سپس کلید Enter را فشار دهید. نشانی IP آن آشکار می‌شود.

۵ـ۶ نشانی URL

هر صفحهٔ وب نشانی مربوط به خود را دارد. URL (Uniform Resource Locator) یک نشانی واحد است که یک صفحهٔ وب را تعریف می‌کند. URL چند بخش دارد که در شکل ۵ـ۳ می‌بینند.

http: //www.leeds.com/documentation/ch3.html

شکل ۵ـ۳ بخش‌های یک URL.

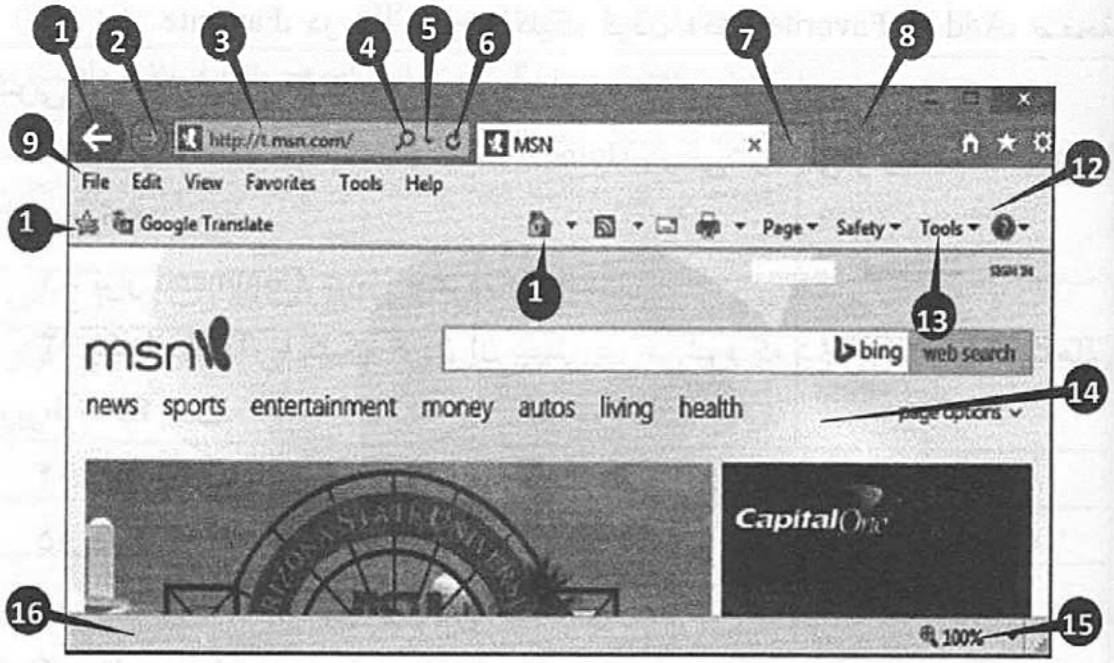
بخش اول، http:// است که یک پروتکل یا مجموعه‌ای از قوانین است که در انتقال یک صفحهٔ وب از سرور به مرورگر وب استفاده می‌شود. بخش دوم نام سرورِ میزبان صفحهٔ وب و به گونهٔ معمول www و نام دامنه است. URL می‌تواند شامل نشانی مسیر و نام فایل یک صفحهٔ وب باشد؛ برای نمونه، در شکل بالا، "documentation/" مسیر و "ch3.html" نام فایل است. هنگامی که کاربر URL را در مرورگر تایپ می‌کند، تایپِ پروتکل http:// و www اختیاری است. اگر URL مسیر و نام فایل نداشته باشد، مرورگر صفحهٔ خانهٔ سایت (آغازه) را نمایش می‌دهد.

۵ـ۷ مرورگر اینترنت

مرورگر اینترنت یک نرم‌افزار است که برای دستیابی و دیدن صفحه‌های وب از آن استفاده می‌شود. چندین مرورگر اینترنت وجود دارد که متداول‌ترین آنها عبارت‌اند از: InternetExplorer، Opera، FireFox و Chrome. محبوب‌ترین آنها مرورگر Internet Explorer (IE) است.

۵ـ۷ـ۱ مرورگر Internet Explorer

مرورگر Internet Explorer یکی از معروف‌ترین نرم‌افزارهای شرکت مایکروسافت است که همیشه به همراه ویندوز وجود دارد. برای باز کردن پنجرهٔ مرورگر، در ویندوز۱۰، در صفحهٔ Start بر روی تایلِ Internet Explorer کلیک کنید. یا در دید دسکتاپ، در نوار فعالیت آیکن Explorer Internet را کلیک کنید. در نسخه‌های پیش‌تر ویندوز، بر روی صفحهٔ دسکتاپ یا در نوار فعالیت وجود دارد. در شکل ۵ـ۴ پنجرهٔ مرورگر IE را می‌بینید.



شکل ۵ـ۴ مرورگر IE.

۱. دکمهٔ Back، یک صفحه به عقب می‌رود.

۲. دکمهٔ Forward، یک صفحه به جلو می‌رود.

۳. نوار نشانی، نشانی URL مورد نظر را در این بخش تایپ کنید.

۴. دکمهٔ Search، رشتهٔ مورد نظر را جستجو می‌کند.

۵. فلش Show Address bar Autocomplete، با کلیک کردن این فلش لیستی باز می‌شود که شامل نشانی سایت‌هایی که به تازگی باز کرده‌اید، History، سیاهه (لیست) Favorite، و ... است.

۶. دکمهٔ Go To، سبب می‌شود که به نشانی‌ای که در نوار نشانی وارد شده است بروید. گاهی این دکمه به دکمهٔ Refresh بدل می‌شود که با کلیک کردن آن، صفحه نوسازی می‌شود. گاهی نیز به دکمهٔ stop بدل می‌شود که با کلیک کردن آنلود شدن صفحه متوقف می‌شود.

۷. New Tab، با کلیک کردن آن، یک صفحهٔ جدید ایجاد می‌شود.

۸. نوار عنوان، در این نوار دکمه‌های Back، Forward، نوار نشانی، دکمهٔ بستن و... وجود دارد.

۹. نوار منو، در این نوار چند منو وجود دارد که هر منو شامل چندین گزینه است.

۱۰. نوار Favorite، در این نوار با کلیک کردن دکمهٔ Add to Favorite، صفحهٔ کنونی به منوی Favorite افزوده می‌شود.

۱۱.دکمهٔ Home، با کلیک آن، صفحهٔ Home باز می‌شود. می‌توانید صفحهٔ Home را معین کنید.

۱۲. نوار Command، شامل چند دستور است.

۱۳. دکمهٔ Tools، با کلیک کردن آن لیستی باز می‌شود که شامل منوها و گزینه‌های مربوط به IE است.

۱۴. بدنه، در این بخش از پنجره، محتویات وب‌سایت نمایش داده می‌شود.

۱۵. دکمهٔ Zoom، صفحه را بزرگ یا کوچک کنید.

۱۶. نوار Status، این نوار در پایین صفحه قرار دارد.

◄ **نکته:** اگر محیط بیشتری برای نمایش نیاز دارید، می‌توانید برخی از منوها و ابزارها را ببندید. در نوار عنوان کلیک راست کنید، از منویی که آشکار می‌شود، موردهای دلخواه را کلیک کنید تا آشکار یا پنهان شوند.

۵ـ۸ کلیدهای میانبر Internet Explorer

با استفاده از کلیدهای میانبر سرعت خود را به هنگام کار با برنامه بالا ببرید. در جدول ۵ـ۱ چند کلید میانبر مربوط به مرورگر IE آمده است.

۵ـ۹ موتورهای جستجو

موتورهای جستجو ابزاری برای بازیابی اطلاعات در اینترنت هستند. بازیابی با سرعت و درست اطلاعات، جستجوی رکوردهای مرتبط، از مزیت‌های موتورهای جستجو هستند. آن‌چه برای کاربران اینترنت اهمیت دارد، صرفه‌جویی در وقت است.

برخی از موتورهای جستجو عبارت‌اند از: Bing، MyStart، Google، و ... . موتور جستجوی Google یکی از قدرتمندترین موتورهای جستجوی وب است. Google با پوشش بیش از ۱,۳۲۶,۹۲۰,۰۰۰ صفحهٔ وب و سرعت بازیابی پذیرفتنی، مدعی است که امکان جستجو به ۲۵ زبان گوناگون جهان را فراهم می‌کند. این موتور جستجو از راه نشانی www.google.com قابل دستیابی است.

جدول ۵ـ۱ کلیدهای میانبر IE

F1	نمایش راهنمای مرورگر. در زمانی که پنجره‌ای باز باشد راهنمای مربوط به همان عنصر را نمایش می‌دهد.
F11	جابه‌جایی بین حالت همهٔ صفحه در مرورگر و پنجره در ابعاد عادی
Tab	حرکت به سمت جلو در بین عنصرهای صفحه وب و نوار نشانی
Shift+Tab	حرکت به سمت عقب در بین عنصرهای صفحه وب و نوار نشانی
Alt+Home	رفتن به صفحهٔ Home
Alt+Right Arrow	رفتن به صفحهٔ بعدی
Alt+Left Arrow	رفتن به صفحهٔ پیشین
Backspace	رفتن به صفحهٔ پیشین
Shift+F10	نمایش منوی آبشاری و میانبر برای یک لینک
Ctrl+Tab	انتقال (ترفندستان) بین فریم‌ها به سمت جلو
F6	انتقال بین فریم‌ها به سمت جلو
Shift+Ctrl+Tab	انتقال بین فریم‌ها به سمت عقب
Up Arrow	حرکت صفحه به سمت ابتدای سند
Down Arrow	حرکت صفحه به سمت انتهای سند
Page Up	حرکت به سمت ابتدای صفحه با انجام پرشی بزرگ‌تر نسبت به دکمهٔ بالا
Page Down	حرکت به سمت انتهای صفحه با انجام پرشی بزرگ‌تر نسبت به دکمهٔ پایین
Home	انتقال صفحه به ابتدای سند
End	انتقال صفحه به انتهای سند
Ctrl+F	نمایش پنجرهٔ جستجو برای صفحهٔ جاری
F5	به‌روزرسانی صفحه در صورتی که نیازی به این کار باشد
Ctrl+R	به‌روزرسانی صفحه در صورتی که نیازی به این کار باشد
Ctrl+F5	به‌روزرسانی صفحه مناسب برای صفحه‌هایی که توسط ISPها Cache می‌شوند
Esc	متوقف کردن فرایند بارگیری (دانلود) در صفحه
Ctrl+O	باز کردن یک مکان (نشانی اینترنتی) دیگر

جدول ۵ـ۱ (ادامه)

Ctrl+L	باز کردن یک مکان (نشانی اینترنتی) دیگر
Ctrl+N	باز کردن یک صفحهٔ مرورگر دیگر
Ctrl+W	بستن صفحهٔ مرورگر جاری
Ctrl+S	ذخیره کردن صفحهٔ جاری
Ctrl+P	چاپ صفحهٔ جاری
Enter	فعال‌سازی پیوند (لینک) برگزیده
Ctrl+E	باز کردن جستجو در نوار مرورگر
Ctrl+I	باز کردن علاقه‌ها در نوار مرورگر
Ctrl+H	باز کردن سابقه در نوار مرورگر
Alt+D	قرار دادن متن برگزیده در نوار نشانی
F4	نمایش نوار نشانی سوابق
Ctrl+Left Arrow	در صورتی که این کلید را در نوار نشانی فشار دهید مکان‌نما به سمت چپ محلی که کاراکتر / قرار دارد منتقل می‌شود
Ctrl+Right Arrow	در صورتی که این کلید را در نوار نشانی فشار دهید مکان‌نما به سمت راست محلی که کاراکتر / قرار دارد منتقل می‌شود
Ctrl+Enter	در نوار نشانی با زدن این کلید رشتهٔ .www به اول متنی که در نشانی باز نوشته‌اید افزوده می‌شود. همچنین رشته .com را به انتهای این رشته می‌افزاید
Up Arrow	در صورتی که ویژگی AutoComplete فعال باشد. در سیاهه (لیست) به سمت بالا حرکت می‌کند
Down Arrow	در صورتی که ویژگی AutoComplete فعال باشد در سیاهه (لیست) به سمت پایین حرکت می‌کند
Ctrl+D	صفحهٔ جاری را به فهرست Favorites می‌افزاید
Ctrl+B	نمایش پنجرهٔ سازمان‌دهی علاقه‌ها
Alt+Up Arrow	بالا رفتن در سیاهه (لیست) در پنجرهٔ سازمان‌دهی علاقه‌ها
Alt+Down Arrow	پایین رفتن در سیاهه (لیست) در پنجرهٔ سازمان‌دهی علاقه‌ها
Ctrl+X	حذف (در صورت امکان) و انتقال کپی عنصر برگزیده به حافظه
Ctrl+C	کپی عنصر برگزیده به حافظه
Ctrl+V	افزودن عنصر درون حافظه در مکان کنونی
Ctrl+A	انتخاب همهٔ عنصرها

۵ـ۱۰ رایانامه

رایانامه یکی از متداول‌ترین مدل‌های ارتباطی در اینترنت است که حجم بالایی از ترافیک اینترنت را تشکیل می‌دهد. به دلیل امتیازهایی که رایانامه دارد به یک مدل ارتباطی قدرتمند بدل شده است. می‌توانید پیامی را به صورت رایانامه به دیگران بفرستید یا از آنها دریافت کنید. برای استفاده از رایانامه باید یک حساب رایانامه داشته باشید. امروزه رایانامه به دو شکل ارائه می‌شود:

- به گونهٔ رایگان، در وب‌سایت‌هایی مانند Google.com و Yahoo.com؛
- در وب‌سایت‌های شخصی، شرکت‌ها و مؤسسه‌ها.

۵ـ۱۱ دانلود از اینترنت

به دریافت فایل از اینترنت دانلود یا بارگیری می‌گویند. کاربران می‌توانند بیشتر برنامه‌ها، نرم‌افزارها و فایل‌های موجود در اینترنت را دانلود کنند، یعنی از رایانه‌های راه‌دور بردارند و روی رایانه خود کپی کنند.

می‌توانید برای دانلود کردن اطلاعات از اینترنت، افزون بر مرورگر از نرم‌افزارهای دانلود اطلاعات استفاده کنید. این نرم‌افزارها سرعت دانلود را افزایش داده و امکانات سودمندی را فراهم می‌کنند.

نرم‌افزار Internet Download Manager که به اختصار IDM نامیده می‌شود، یکی از معروف‌ترین و قدرتمندترین نرم‌افزارهای مدیریت دانلود است.

۵ـ۱۲ تجارت الکترونیک چیست؟

تجارت الکترونیک بر پردازش و انتقال الکترونیک داده شامل متن، صدا و تصویر مبتنی است. تجارت الکترونیک فعالیت‌های گوناگونی مانند مبادلهٔ الکترونیک کالاها و خدمات، تحویل فوری مطلب‌های دیجیتال، اتصال الکترونیک وجوه، مبادلهٔ الکترونیک سهام، روزنامهٔ الکترونیک، طرح‌های تجاری، طراحی و مهندسی مشترک، منبع‌یابی، خریدهای دولتی، بازاریابی مستقیم و خدمات پس از فروش را دربر می‌گیرد. همچنین، فعالیت‌های عمومی تجاری، مانند تبلیغات، آگهی، مذاکره‌ها، قراردادها و تصویر حساب‌ها را نیز دربر گرفته است.

تجارت الکترونیک انجام همهٔ فعالیت‌های تجاری با استفاده از شبکه‌های ارتباطی رایانه است. نوعی تجارت بدون کاغذ است. کاربرد تجارت الکترونیک فراتر از مبادلهٔ کالا، خدمات وجوه است. ویژگی اصلی همهٔ این فعالیت‌ها تسهیل فرایندهای تجاری، حذف فرایندهای غیر ضروری در انجام امور بازرگانی و کاهش هزینه‌ها از راه بهبود و افزایش هماهنگی، کاهش هزینه‌های اداری به ویژه هزینهٔ نامه‌نگاری و کاغذبازی و بهبود دسترسی به بازار و افزایش تنوع برای مشتریان است.

مهم‌ترین ویژگی تجارت الکترونیک از دیدگاه بازاریابی، برقراری ارتباط سازمان یا فرد با کل مخاطبان و سازگار ساختن فراورده‌ها و خدمات با نیازهای فرد به فرد آنهاست. نتیجهٔ آن رقابتی شدن، تنوع عرضه‌کنندگان، خدمات و کاهش هزینه‌ها و افزایش رضایتمندی است.

۵ـ۱۲ـ۱ ویژگی‌های کلی تجارت الکترونیک

ویژگی کلی تجارت الکترونیک عبارت‌اند از:

- جهانی کردن تجارت؛
- برداشتن محدودیت‌های زمانی و مکانی؛
- کاهش هزینه؛
- دسترسی آسان به اطلاعات؛
- تجارت ۲۴ ساعته.

۵ـ۱۲ـ۲ مزایای تجارت الکترونیک

مزایای تجارت الکترونیک عبارت‌اند از:

- تأخیر ناشی از تهیه مدارک را از میان می‌برد.
- امکان بروز اشتباه را کاهش می‌دهد.
- صرفه‌جویی در زمان، نیروی انسانی و هزینه‌های اداری را به دنبال دارد.
- جریان گردش اطلاعات را روان می‌سازد.
- حجم زیاد استانداردهای تکراری را کاهش می‌دهد.

۵ـ۱۳ انواع تجارت الکترونیک

تجارت الکترونیک را می‌توان از حیث تراکنش‌ها به انواع گوناگونی تقسیم کرد که عبارت‌اند از:

- ارتباط شرکت و شرکت (B2B): به الگویی از تجارت الکترونیک می‌گویند که دو طرف شرکت‌ها هستند.
- ارتباط شرکت و مصرف‌کننده (B2C): به الگویی از تجارت الکترونیک می‌گویند که بسیار رایج است و ارتباط مستقیم میان شرکت و مشتریان است.
- ارتباط مصرف‌کننده و شرکت (C2B): در این حالت، اشخاص حقیقی به کمک اینترنت، فراورده‌ها و خدمات خود را به شرکت‌ها می‌فروشند.
- ارتباط مصرف‌کننده و مصرف‌کننده (C2C): در این حالت، تجارت میان مصرف‌کنندگان است.
- ارتباط شرکت و سازمان دولتی (B2A): شامل همهٔ تعامل‌های تجاری میان شرکت‌ها و سازمان‌های دولتی است. پرداخت مالیات و عوارض از این قبیل تعامل‌ها به‌شمار می‌روند.
- ارتباط میان دولت و شهروندان (G2C): الگویی میان دولت و تودهٔ مردم است که شامل شرکت‌های اقتصادی، مؤسسه‌های دولتی و همهٔ شهروندان است. این الگو یکی از مؤلفه‌های دولت الکترونیک است.
- ارتباط میان دولت‌ها (G2G): این الگو شامل ارتباط تجاری میان دولت‌ها در زمینه‌هایی شبیه واردات و صادرات است.

رشد روزافزون فناوری اطلاعات (IT) در جهان، موانع و دشواری‌های زمانی و مکانی مربوط به امور تجاری را کاهش داده است و دسترسی عمومی به اینترنت سبب شده امکان تجارت و کسب‌وکار از راه اینترنت و یا به عبارتی تجارت الکترونیک و کسب‌وکار الکترونیک از جایگاه ویژه‌ای در کشورها برخوردار شود. از این رو بهره‌مندی از این امکان برای همهٔ شرکت‌ها کارا و سودمند است.

۵ـ۱۴ پرداخت اینترنتی

می‌توانید با استفاده از کارت اعتباری از اینترنت خرید کنید و هزینهٔ آن را پرداخت کنید، یا قبوض برق، آب، تلفن و ... را به صورت اینترنتی پرداخت کنید و ... . به این فرایندها پرداخت اینترنتی می‌گویند.

پول از راه اینترنت از حساب مشتری به حساب مقصد، برای نمونه مدیر سایت فروشگاه اینترنتی، واریز می‌شود. بیشتر بانک‌ها مانند ملی، ملت، سامان و پاسارگاد امکان استفاده از اینترنت و خرید اینترنتی را دارند. این بانک‌ها به عنوان درگاه پرداخت عمل می‌کنند.

در هنگام خرید اینترنتی به اطلاعات زیر نیاز خواهید داشت:

- **شمارهٔ کارت:** شمارهٔ کارت بر روی کارت اعتباری درج شده است (شکل ۵ـ۵).
- **رمز خرید اینترنتی (رمز دوم):** برای دریافت رمز دوم، به دستگاه خودپرداز بانک مربوطه مراجعه کنید و رمز دوم را دریافت کنید یا به شعبهٔ بانک خود بروید و درخواست رمز اینترنتی را بدهید.
- **کد CVV2:** کد CVV2 یک عدد سه رقمی یا چهار رقمی است که بر روی کارت اعتباری درج شده است.
- **تاریخ انقضای کارت:** تاریخ انقضای کارت نیز بر روی کارت‌های اعتباری درج شده است.

شکل ۵ـ۵ کارت اعتباری.

پرسش و پژوهش

۱. مفهوم اینترنت را بیان کنید.
۲. کاربردهای اینترنت را بیان کنید.
۳. مرورگر چیست؟
۴. مفهوم موتور جستجو را بیان کنید.
۵. تجارت الکترونیک و انواع آن را بیان کنید.
۶. در ایران تجارت الکترونیک تا چه حدی موفق است؟
۷. دربارهٔ کاربردهای اینترنت در ایران بحث کنید.
۸. به نظر شما فیلترینگ خوب است یا بد؟ بحث کنید.

۶

آشنایی با سیستم عامل ویندوز

اهداف آموزشی

پس از مطالعهٔ این فصل توانایی‌های زیر را کسب خواهید کرد:

با مفهوم سیستم‌عامل ویندوز آشنا می‌شوید.

می‌توانید با ویندوز ۱۰ کار کنید.

با آیکُن‌های گوناگون کار کنید.

با پنجره‌ها کار کنید و فایل‌ها و پوشه‌ها را مدیریت کنید.

سیستم‌عامل مهم‌ترین نرم‌افزاری است که در یک رایانه کار می‌کند. سیستم‌عامل حافظه، پردازش‌ها و همهٔ نرم‌افزارها و سخت‌افزارهای رایانه را مدیریت می‌کند. برپایهٔ رابط گرافیکی طراحی شده است که امکان برقراری ارتباط با رایانه را بدون دانستن زبان رایانه فراهم می‌کند.

در حال حاضر، ویندوز محبوب‌ترین سیستم‌عامل است که فراورده شرکت مایکروسافت است. از ۱۳۸۵ تاکنون نسخه‌های متفاوتی از آن منتشر شده است که برخی از آنها عبارت‌اند از ویندوز ۹۸، ویندوز XP، ویندوز ویستا و ویندوز سون و ویندوز ۸. جدیدترین نسخهٔ آن ویندوز ۱۰ است.

۶ـ۱۴ مدیریت فایل‌ها و پوشه‌ها

فایل یک شیء است که داده را نگه می‌دارد. فایل‌ها می‌توانند متن، عکس، موسیقی، ویدئو، و ... باشند. ویندوز برای نشان دادن یک نوع فایل از یک آیکن ویژه استفاده می‌کند. فایل یک پسوند سه یا چهار حرفی مانند docx. نیز دارد، که ارتباط فایل با برنامه را نشان می‌دهد. ویندوز پسوند فایل را پنهان می‌کند مگر اینکه به‌گونه‌ای تنظیم کنید که نمایش داده شوند. برخی از فرمت‌های فایل عمومی هستند، مانند TEXT (TXT)، JPEG، RTF و TIFF که با چندین برنامه باز می‌شوند. برخی فایل‌ها محلی برنامه‌های کاربردی هستند، مانند DOCX که برای Microsoft Word است و PDF که برای Adobe Acrobat است. فایل‌ها، در پنجره‌ها باز می‌شوند.

۶ـ۱۴ـ۱ گزینش یک فایل

برای گزینش یک فایل، آن فایل را در سامانهٔ فایل پیدا کنید، یک‌بار آن را کلیک کنید تا برگزیده شود.

۶ـ۱۴ـ۲ گزینش چند فایل از یک پوشه

برای گزینش چند فایل که در درون یک پوشه هستند، چند روش وجود دارد:

- برای گزینش فایل‌هایی که در کنار هم هستند (گزینش یک محدوده)، کلید Shift را نگه دارید و ابتدا و انتهای محدوده را کلیک کنید.
- برای گزینش فایل‌هایی که در کنار هم هستند (گزینش یک محدوده)، چهارگوش گزینش را دور گزینش خود بکشید.
- برای گزینش فایل‌های جدا از هم، کلید Ctrl را فشار داده و نگه دارید، سپس هر فایل را کلیک کنید.

۶ـ۱۴ـ۳ گزینش همهٔ فایل‌های یک پوشه

برای گزینش همهٔ فایل‌های درون یک پوشه، در صفحهٔ Home از ریبون، در گروه Select، دکمهٔ Select All را کلیک کنید، یا کلیدهای Ctrl+A را فشار دهید.

برای اینکه فایل‌های برگزیده را از گزینش خارج کنید، در صفحهٔ Home از ریبون، در گروه Select، دکمهٔ Select None را کلیک کنید، یا در یک بخش خالی از پوشه کلیک کنید.

۶ـ۱۴ـ۴ وارونه کردن گزینش

برای وارونه کردن یک گزینش، در صفحهٔ Home از ریبون، در گروه Select، دکمهٔ Invert Selection را کلیک کنید. این دکمه زمانی فعال است که چند فایل را گزینش کرده باشید و بخواهید که فایل‌های گزینش‌نشده را حذف کنید.

هنگامی که یک یا چند فایل گزینش شده‌اند، می‌توانید آنها را با هم حرکت دهید، کپی کنید، یا حذف کنید، ویژگی‌های آنها را تغییر دهید، و ... .

۶ـ۱۴ـ۵ باز کردن یک یا چند فایل

برای باز کردن یک یا چند فایل، چند روش وجود دارد:

- فایل را دوبار کلیک کنید تا در برنامهٔ پیش‌فرض خود باز شود.
- در حالی که یک یا چند فایل برگزیده شده است، Enter را فشار دهید. همهٔ فایل‌های برگزیده در برنامه‌های مربوطه باز می‌شوند.
- برای باز کردن فایل در برنامهٔ پیش‌فرض آن، روی نام فایل کلیک راست کنید و Open را کلیک کنید.
- در نوار نشانی، مسیر را تایپ کنید و در انتهای آن نام فایل را تایپ کنید، سپس Enter را فشار دهید.

۶ـ۱۴ـ۶ تغییر برنامهٔ پیش‌فرض یک فایل

برای تغییر دادن برنامهٔ پیش‌فرضی که فایل را باز می‌کند، مرحله‌های زیر را انجام دهید:

۱. روی فایل کلیک راست کنید، از منوی محلی، گزینهٔ Open With را کلیک کنید.

۲. از زیر منو، گزینهٔ Choose Another App را برگزینید.

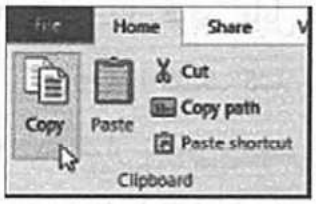
۳. برنامه‌ای را از کادر دیالوگ How Do You Want To Open This File? برگزینید. یا لینک More Options را کلیک کنید، سپس سیاهه (لیست) را حرکت دهید. اگر برنامهٔ مورد نظر شما در لیست نبود، لینک Look for app in the Store یا لینک Look for another app on this PC را کلیک کنید تا گزینه‌های دیگری را ببینید.

۴. کادر کنترل Use This App For Files را برگزینید تا این برنامه، برنامهٔ پیش‌فرض شود و این نوع فایل را باز کند.

۶ـ۱۴ـ۷ کپی کردن فایل یا پوشه

در حالی که یک فایل برگزیده شده است، صفحهٔ Home از ریبون نشان داده می‌شود (شکل ۶ـ۶). این صفحه دارای دکمه‌هایی است که امکان انجام فرایند کپی را فراهم می‌کند:

۱. در گروه Clipboard از صفحهٔ Home، دکمه‌های Cut یا Copy را کلیک کنید تا فایل برگزیده را به کلیپ‌بورد منتقل کنید.

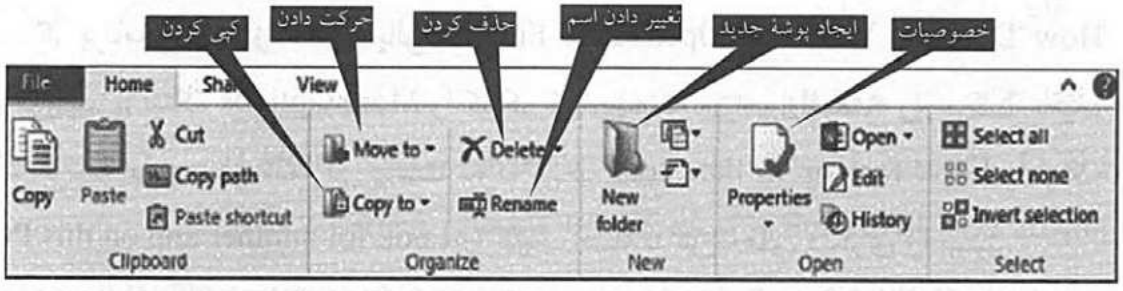


۲. در مکان یا پوشهٔ دلخواه کلیک کنید، سپس گزینهٔ Paste را کلیک کنید تا آنچه که در کلیپ‌بورد وجود دارد در مکان کنونی کپی شود.

می‌توانید کلیدهای Ctrl+X، Ctrl+C، یا Ctrl+V را نیز فشار دهید.

۶ـ۱۴ـ۸ حذف فایل یا پوشه

برای حذف کردن یک فایل یا پوشه، در حالی که گزینش شده‌اند، آیکن Delete را کلیک کنید یا کلید Delete را فشار دهید.



شکل ۶ـ۶ صفحهٔ Home.

۶ـ۱۴ـ۹ تغییر دادن نام فایل یا پوشه

برای تغییر دادن نام فایل یا پوشه، مراحل زیر را انجام دهید:

- فایل یا پوشه‌ای را برگزینید. در ریبون، در صفحهٔ Home (شکل ۶ـ۶)، گزینهٔ Rename را کلیک کنید. نام فایل در کادر متن ویرایش قرار می‌گیرد تا آن را ویرایش کنید.
- روی فایل یا پوشه کلیک راست کنید، گزینهٔ Rename را کلیک کنید. نام جدید را تایپ کنید. کلید Enter را فشار دهید.

۶ـ۱۴ـ۱۰ ایجاد پوشهٔ جدید

برای ایجاد پوشهٔ جدید، در مکان دلخواه (روی دسکتاپ یا درون یک پوشه) کلیک راست کنید، از منویی که باز می‌شود، گزینه New و سپس Folder را کلیک کنید.

◄ **نکته:** می‌توانید از طرق این منوی محلی، برخی از فایل‌های جدید، مانند فایل Wordیا Excel، را نیز ایجاد کنید.

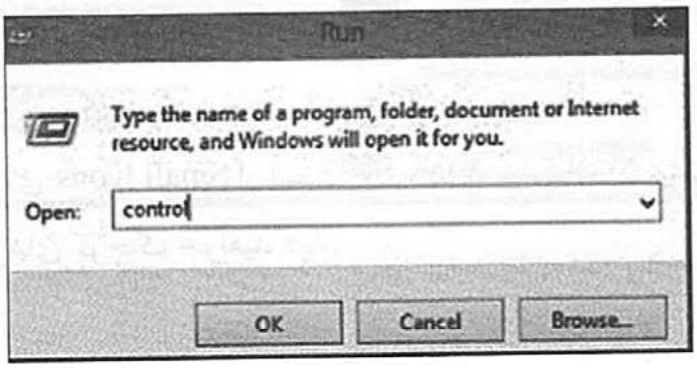
۶ـ۱۵ Control Panel

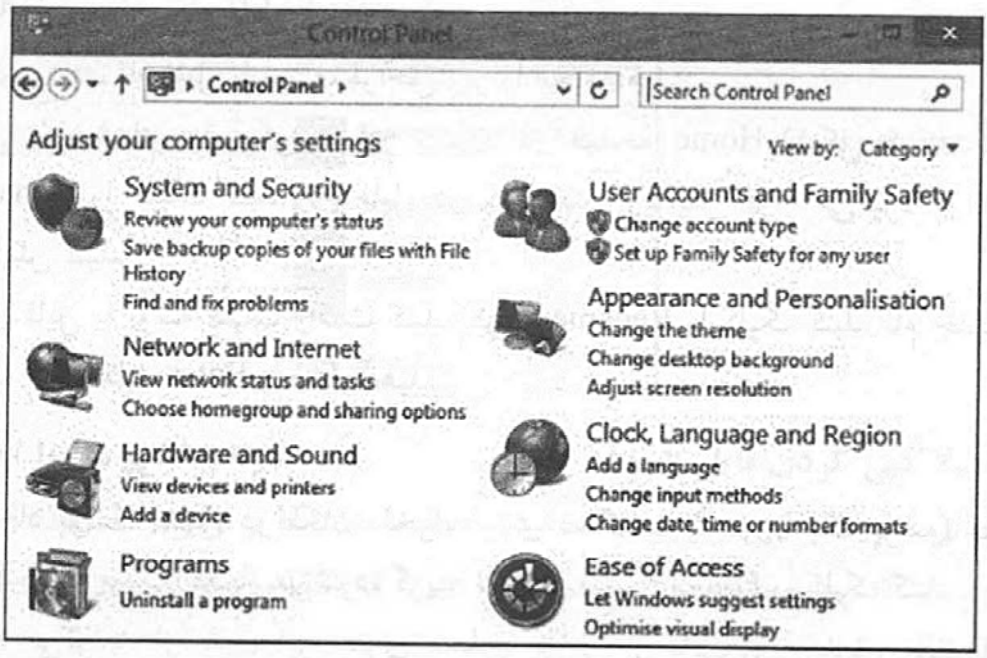
Control Panel مجموعه‌ای از اپلت‌ها، یا برنامه‌های کوچک است، که بخش‌های گوناگون سامانهٔ ویندوز شامل سخت‌افزار، نرم‌افزار، امنیت، پیکربندی و مدیریت حساب کاربر را ویرایش می‌کند. Control Panel یک پوشهٔ ویژه است. همهٔ نسخه‌های ویندوز، Control Panel داشته‌اند.

در شکل ۶ـ۷ صفحهٔ اصلی Control Panel را می‌بینید که هر لینک، پانل کنترل مربوط به خودش یا یک گروه‌بندی دیگر را باز می‌کند.

۶ـ۱۵ـ۱ باز کردن Control Panel

برای باز کردن Control Panel، از روش‌های زیر استفاده کنید:





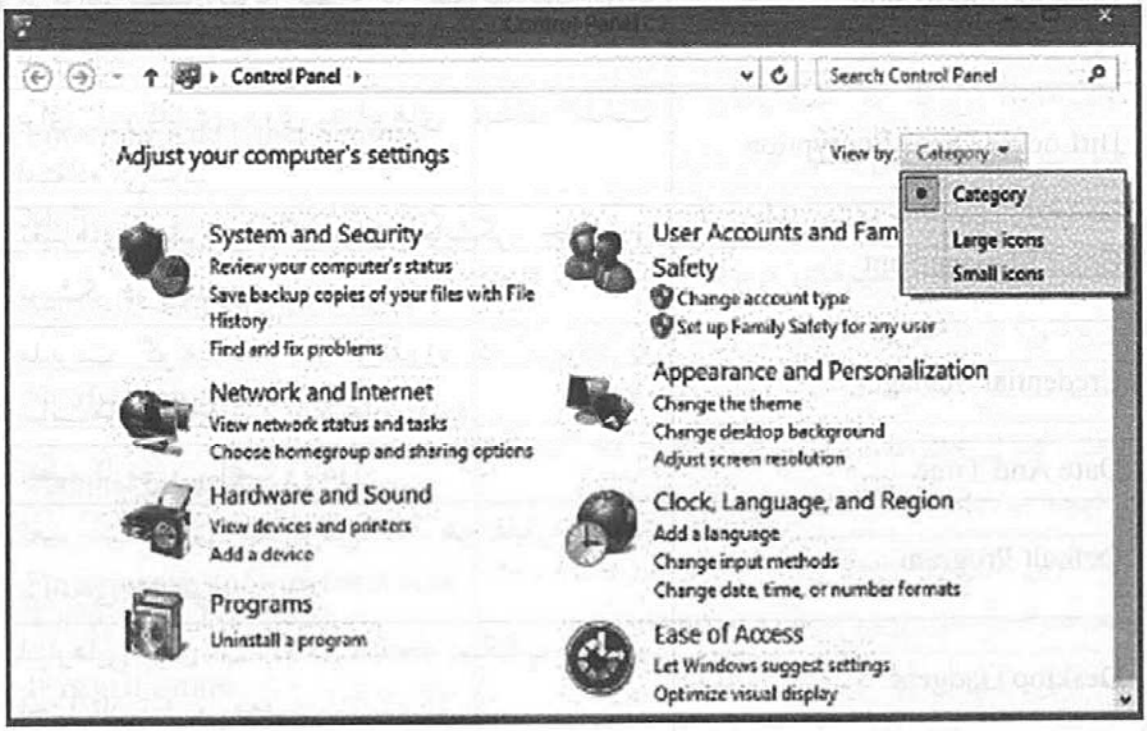
شکل ۶ـ۷ صفحهٔ اول Control Panel دسکتاپ، دسترسی به همهٔ ویژگی‌ها را فراهم می‌کند.

کلیدهای ⊞+R را فشار دهید تا کادر دیالوگ Run باز شود، control را تایپ کنید و به OK ضربه بزنید یا آن را کلیک کنید.

- در صفحهٔ Start، کلمهٔ control را تایپ کنید. آیکن Control Panel به صورت برجسته نمایش داده می‌شود. بر روی آن کلیک کنید.

پس از باز کردن پنجرهٔ Control Panel می‌توانید حالت نمایش گزینه‌های این پنجره را به سه حالت تغییر دهید. بر روی فلش View by کلیک کنید لیستی باز می‌شود (شکل ۶ـ۸).

- نمای Category که همان نمای پیش‌فرض Control Panel است در نمای Category وظایف در زیر طبقه‌بندی اصلی، درج شده است.
- با کلیک بر روی Large Icons از سیاهه (لیست) View by، بیش از ۵۰ آیتم را به سایز آیکن‌های بزرگ خواهید دید. مانند شکل صفحه بعد.
- با کلیک بر روی Small Icons از لیست View by، بیش از ۵۰ آیتم در کنترل پنل را به سایز آیکن‌های کوچک خواهید دید.



شکل ۶ـ۸ می‌توانید این پنجره را به سه حالت نمایش دهید.

۶ـ۱۵ـ۲ آیکن‌های پنجرهٔ Control Panel

برای ورود به بخش Control Panel ویندوز بر روی دکمه Start کلیک کنید و وارد بخش Control Panel شوید. بر روی فلش View by کلیک کرده و گزینهٔ Large Icons را برگزینید تا همهٔ موردهای مربوط به تنظیم‌ها را ببینید. این گزینه‌ها را در جدول زیر شرح دادیم:

Action Center	پیغام‌هایی که توسط ویندوز داده می‌شود، در این بخش قابل مشاهده است و راه کارهایی برای حل آنها نیز ارائه شده است.
Administrative Tools	مربوط به تنظیم‌های مدیریتی رایانه است، تنظیم‌های سامانه‌ای، سرویس‌ها، فایروال پیشرفته و ...
AutoPlay	در این بخش می‌توانید تنظیم‌های پیش‌فرض دستگاه‌های DVD، CD و پلیرها را برای پخش آهنگ و ویدیو تغییر دهید.
Backup And Restore	از همهٔ فایل‌ها و تنظیم‌های مربوط به ویندوز شما می‌تواند پیشتبان‌گیری کند و در صورت نیاز آن را بازگرداند.
BitLocker Drive Encryption	برای رمزگذاری روی درایوهای دیسک سخت استفاده می‌شود.
Color Management	تغییرهای پیشرفته رنگ برای نمایشگر، چاپگر و پویشگر در ویندوز
Credential Manager	مدیریت گواهینامه‌ها در ویندوز، که مربوط به سایت‌های پرداخت و بانک‌ها می‌شود.
Date And Time	تنظیم تاریخ و ساعت ویندوز
Default Program	تغییر برنامه‌های پیش‌فرض، که هر فایلی با چه برنامه‌ای باز شود.
Desktop Gadgets	ابزارهایی برای استفاده در صفحهٔ دسکتاپ شما در اختیارتان قرار می‌دهد.
Device Manager	مربوط به شناسایی سخت‌افزار و به‌روزرسانی راه‌انداز آنها

Devices And Printers	تنظیم‌های دستگاه‌های جانبی نصب‌شده مانند پرینتر و اسکنر در این بخش دیده می‌شود.
Display	تنظیم‌های مربوط به صفحه‌نمایش
Ease of Access Center	تنظیم‌هایی برای ساده کار کردن با ویندوز را داراست
Family Saftey	تغییر تنظیم‌های امنیت خانواده
File History	تاریخچه‌ای از فایل‌های شما نگهداری می‌کند.
Folder Options	تنظیم‌های مربوط به نمایش فایل‌ها و پوشه‌ها
Fonts	محل قرارگیری فونت‌های ویندوز
Getting Start	آموزش دربارهٔ ویژگی‌های ویندوز و شیوهٔ استفاده از آن
Home Group	برای ساخت و استفاده از شبکه‌های Home Group
Indexing Options	تغییر چگونگی فهرست‌بندی آیتم‌های ویندوز برای جستجو با سرعت‌تر
Internet Options	تنظیم‌های نمایش اینترنت شما و تنظیم‌های کانکشن‌های اینترنت
Keyboard	تنظیم‌های مربوط به صفحه کلید در این بخش قرار دارد.
Locations And Other Sensors	تنظیم‌های مربوط به حسگرهای رایانه شما در صورت وجود در این بخش قرار دارد.
Mouse	تنظیم‌های مربوط به موشی (ماوس)
Network And Sharing Center	اتصال، نمایش و تنظیم‌های مربوط به شبکه بی‌سیم (وایرلس) یا داخلی (LAN) در این بخش قرار دارد.
Notification Area Icons	تنظیم نمایش آیکن‌ها در نوار ابزار پایین ویندوز
Parental Control	بخش کنترل خانواده بر عملکرد کودکان، قفل‌گذاری و ایجاد محدودیت در بخش‌های گوناگون
Performance Informations And Tools	اطلاعاتی در مورد عملکرد سامانه و سرعت آن به همراه راه‌حل‌های بهبود عملکرد می‌دهد.
Personalization	شخصی‌سازی محیط دسکتاپ ویندوز
Phone And Modem	برای نصب و تنظیم‌های مودم دیال‌آپ
Power Options	کنترل مصرف انرژی رایانه

Programe And Features	نصب و حذف برنامه‌ها و افزوده‌کردن ویژگی‌های ویندوز
Recovery	ساخت ریکاوری در زمان مشخص از ویندوز و بازگرداندن آن پس از ایجاد مشکل در ویندوز برای حل دشواری
Region And Language	تغییر و افزودن زبان ویندوز
Remote And Desktop Connections	برای وصل شدن از راه دور به رایانه‌های دیگر
Sound	تنظیم‌های مربوط به کارت صدا و افکت‌های ویندوز
Speech Recognition	تنظیم شیوهٔ تشخیص صدای شما برای متن
Storage Space	فایل‌های شما را در برابر صدمه دیدن درایو محافظت می‌کند.
Sync Center	همگام‌سازی فایل‌ها میان رایانه شما و پوشه‌های شبکه
System	اطلاعات دربارهٔ رایانه و تغییر تنظیم‌های سخت‌افزار در این بخش قرار دارد.
Tablet PC Setting	تنظیم‌های صفحه نمایش در تبلت‌ها
Taskbar And Start Menu	تنظیم‌های مربوط به منوی Start ویندوز و نوار Taskbar
Troubleshooting	راهنمای جامع برای گشودن دشواری‌های پیش‌آمده در ویندوز
User Account	ایجاد و تغییر کاربرهای ویندوز و گزینش پسورد برای آنها
Windows Card Space	محل نگهداری اطلاعات کارت‌ها برای استفاده از سرویس‌های آنلاین
Windows Defender	محافظت‌کنندهٔ ویندوز از نرم‌افزارهای جاسوسی
Windows Firewall	تنظیم‌های فایروال ویندوز
Windows To Go	تهیهٔ نسخهٔ قابل حمل از ویندوز
Windows Update	برای به‌روزرسانی ویندوز
Work Folders	دسترسی به همهٔ فایل‌های کاری شما از راه دور

۶ـ۱۶ Task Manager

Task Manager ابزار تشخیصی برتر ویندوز ۱۰ برای بررسی برنامه‌های کاربردی، فرایندها، سرویس‌ها و عملکرد سامانه است. می‌توانید کارهای زیر را در Task Manager انجام دهید:

- ببینید که کدام برنامه‌های کاربردی در سامانه راه‌اندازی شده‌اند.
- بین برنامه‌های کاربردی سوئیچ کنید یا یک برنامهٔ کاربردی را متوقف کنید.
- ببینید که چه فرایندهایی در سامانه راه‌اندازی شده‌اند، ببینید که هر فرایند از چه منابعی استفاده می‌کند و در صورت نیاز یک فرایند را از میان ببرید.
- کاربرد CPU، حافظه و شبکه را در Resource Monitor ببینید.
- سامانه را خاموش یا راه‌اندازی مجدد (restart) کنید.

۶ـ۱۶ـ۱ باز کردن Task Manager

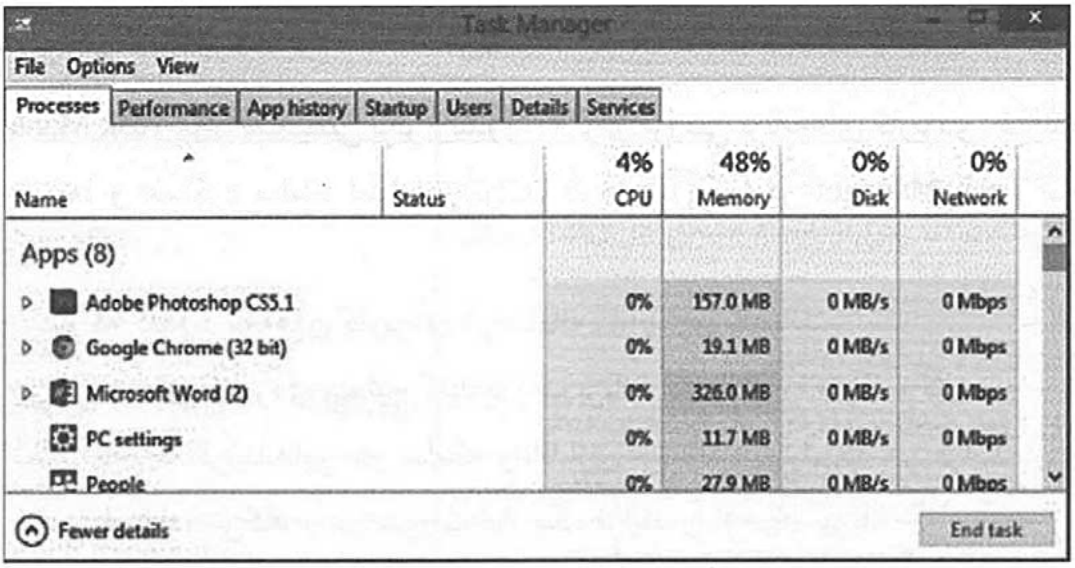
برای رفتن به Task Manager مرحله‌های زیر را انجام دهید:

- کلیدهای Ctrl+Shift+Esc را فشار دهید.
- نوار فعالیت دسکتاپ را کلیک راست کنید و از منوی محلی، دستور Task Manager را کلیک کنید.
- کلیدهای ⊞+R را فشار دهید، taskmgr را تایپ کنید و کلید Enter را فشار دهید.
- کلیدهای Ctrl+Alt+Del را فشار دهید تا صفحهٔ Task را ببینید و دکمهٔ Task Manager را کلیک کنید.
- در صفحهٔ Start، Task Manager را تایپ کنید تا دکمهٔ آن را ببینید.

۶ـ۱۶ـ۲ از میان بردن یک برنامهٔ کاربردی

برای این کار در صفحهٔ Processes عمل زیر را انجام دهید:

- Task Manager را باز کنید (شکل ۶ـ۹).
- یک برنامهٔ کاربردی را کلیک کنید و سپس دکمهٔ End Task را کلیک کنید.
- روی برنامهٔ کاربردی کلیک راست کنید، دستور End Task را کلیک کنید.



شکل ۶ـ۹ Task Manager.

۶ـ۱۶ـ۳ تعویض به برنامهٔ کاربردی دیگر

برای سوئیچ کردن به یک برنامهٔ کاربردی دیگر:

- برای تعویض به برنامهٔ کاربردی برگزیده، دستور Switch To را کلیک کنید یا کلیدهای Alt+Tab یا ⊞+Tab را فشار دهید. تعویض برنامهٔ کاربردی در هنگامی که یک برنامهٔ کاربردی پاسخگو نیست، سودمند است.
- به برنامهٔ کاربردی مورد نظر که می‌خواهید به آن سوئیچ کنید، دوبار ضربه بزنید یا آن را دوبار کلیک کنید.

۶ـ۱۶ـ۴ در مورد یک برنامهٔ کاربردی بیشتر بدانید

برای اینکه در مورد یک برنامهٔ کاربردی بیشتر بدانید:

- از منوی محلی Task Manager، دستور Open File Location را کلیک کنید تا پوشه‌ای که دارای فایل اجرایی برنامه است را ببینید.
- از منوی محلی Task Manager، دستور Search Online را کلیک کنید تا با استفاده از موتور جستجوی مرورگر خود، به جستجوی اطلاعاتی در مورد فایل برنامه بپردازید.
- از منوی محلی Task Manager، دستور Properties را کلیک کنیدتا کادر دیالوگ Properties فایل اجرایی را ببینید.

۶ـ۱۶ـ۵ ایجاد یک وظیفهٔ جدید

برای ایجاد یک وظیفهٔ جدید، مراحل زیر را انجام دهید:

۱. در Task Manager منوی File را کلیک کنید، دستور Run New Task را کلیک کنید.

۲. در کادر دیالوگ Create New Task، برنامه، پوشه، سند، یا منبع اینترنت را در کادرمتن Open وارد کنید؛ سپس OK را کلیک کنید. کادر دیالوگ Create New شبیه به کادر دیالوگ Run است.

۶ـ۱۶ـ۶ نمایش جزئیات در Task Manager

Task Manager را باز کنید و دکمهٔ More Details را از انتهای پنجره کلیک کنید. یا صفحهٔ Details، پنجره‌ها را در زیر برنامهٔ کاربردی مربوطه گروه‌بندی می‌کند.

۶ـ۱۷ نصب کردن یا حذف کردن یک برنامه

ویندوز ۱۰ دو نوع نصب متفاوت دارد. یکی نصبی که به برنامهٔ رابط مبتنی بر تایل مربوط می‌شود و دیگری به برنامهٔ دسکتاپ مربوط می‌شود.

هنگامی که یک برنامه را بر روی دسکتاپ نصب می‌کنید، از نصب‌کنندهٔ ویندوز استفاده می‌کنید. جزئیات نصب برنامه‌های گوناگون متفاوت است، اما به گونهٔ معمول مرحله‌های نصب با دوبار کلیک کردن فایل Setup.exe (اجرایی) آغاز می‌شود. گاهی نیز باید نام برنامه را کلیک کنید.

برنامه‌های قدیمی با استفاده از پانل کنترل Programs and Features حذف می‌شوند.

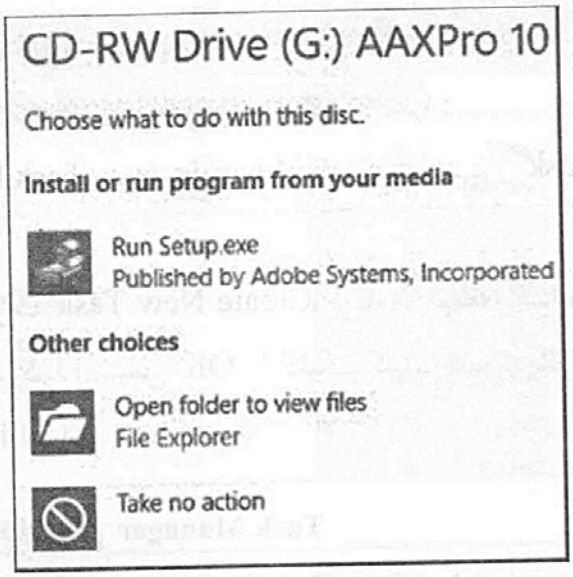
۶ـ۱۷ـ۱ نصب برنامه در رابط مبتنی بر تایل

برای نصب یک برنامه در صفحهٔ Start، مرحله‌های زیررا انجام دهید:

۱. در صفحهٔ Start، تایل Store را کلیک کنید.

۲. برنامهٔ دلخواه را پیدا کنید و به تایل آن ضربه بزنید یا آن را کلیک کنید.

۳. در صفحهٔ توصیف برنامهٔ کاربردی، دکمهٔ Install را کلیک کنید.برنامهٔ کاربردی نصب‌شده و تایل آن به صفحهٔ Start افزوده می‌شود.

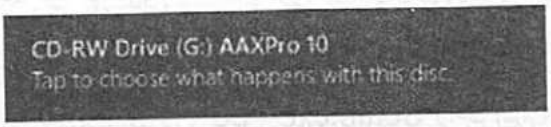


شکل ۶ـ۱۰ گزینه‌های نصب.

۶ـ۱۷ـ۲ نصب از یک رسانه

برای نصب برنامه با استفاده از یک رسانه، مانند CD، DVD، و ...، مرحله‌های زیر را انجام دهید:

۱. دیسک را وارد کنید؛ کمی صبر کنید. ویندوز یک کادر اعلان را نمایش می‌دهد، آن را کلیک کنید.

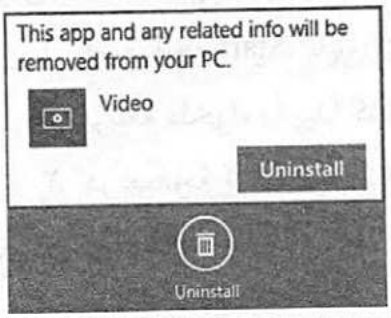


۲. سپس گزینهٔ Run Setup را کلیک کنید تا نصب آغاز شود (شکل ۶ـ۱۰).

۶ـ۱۷ـ۳ حذف برنامهٔ قدیمی

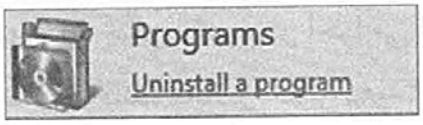
برای پاک کردن یک برنامهٔ قدیمی با استفاده از پانل کنترل Programs and Features مرحله‌های زیر را انجام دهید:

۱. در صفحهٔ Start، روی تایل برنامه کلیک راست کنید تا برگزیده شود.



۲. سپس دکمهٔ Uninstall را از نوار Apps کلیک کنید.

یا در دسکتاپ، پایین، گوشهٔ چپ را کلیک راست کنید و Control Paned را از منو کلیک کنید. سپس

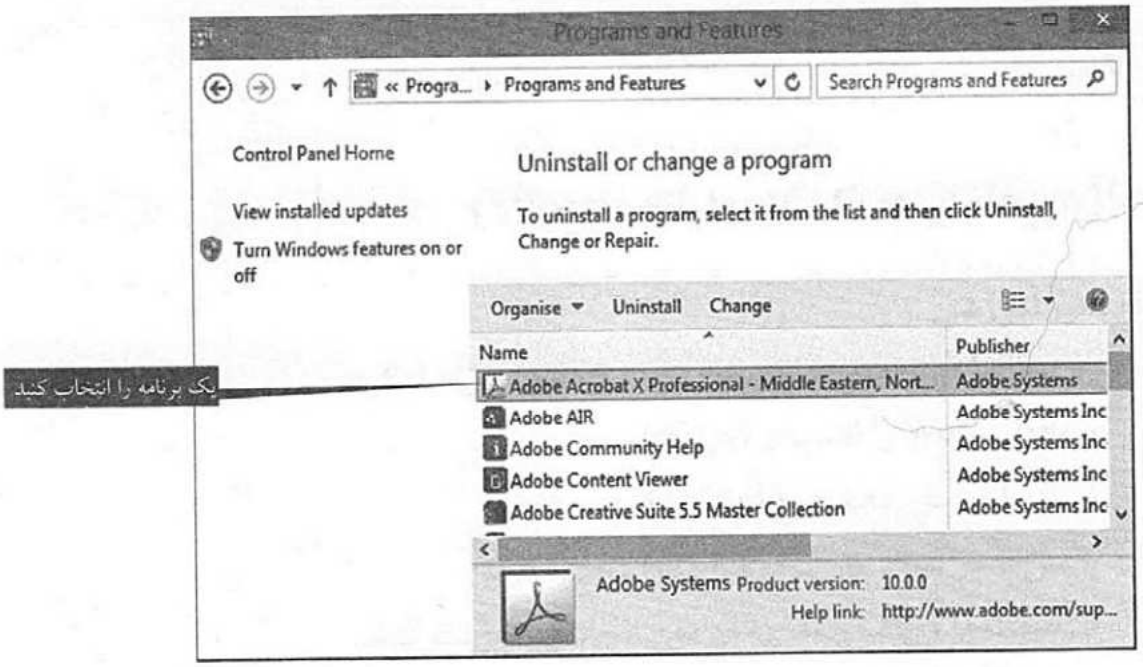


در بخش Program از Control Panel، لینک Uninstall a program را کلیک کنید.

۳. برنامه‌ای را که قصد دارید پاک کنید، پیدا کنید و آن را کلیک کنید تا برگزیده شود.

۴. دکمهٔ Uninstall را کلیک کنید تا برنامهٔ نصب برنامه اجرا شود (شکل ۶ـ۱۱).

۵. دوباره دکمهٔ Uninstall را کلیک کنید تا برنامه پاک شود. ساختار حذف برنامه را دنبال کنید.



شکل ۶ـ۱۱ با استفاده از این پانل کنترل، برنامه‌های قدیمی را پاک کنید.

پرسش و پژوهش

۱. مفهوم سامانه (سیستم) عامل را بیان کنید.

۲. مفهوم تایل و چگونگی گزینش تایل را شرح دهید.

۳. یک حساب کاربری در ویندوز ایجاد کنید که دارای گذرواژه باشد.

۴. ویندوز خود را به سلیقهٔ خود شخصی‌سازی کنید.

۵. شرح دهید که چگونه می‌توانید پس‌زمینهٔ دسکتاپ را تغییر دهید.

۶. برنامه‌ای را در ویندوز ۱۰ چگونه نصب و اجرا می‌کنید؟
۷. چگونه می‌توانید برنامهٔ بازکنندهٔ فایل را تغییر دهید؟
۸. هر چه در مورد نوار فعالیت (taskbar) می‌دانید بیان کنید.
۹. برنامه‌های دلخواه را به نوار فعالیت افزوده یا از آن حذف کنید.

۹

امنیت اطلاعات

اهداف آموزشی

پس از مطالعهٔ این فصل توانایی‌های زیر را درک خواهید کرد:

با چند تعریف امنیت اطلاعات آشنا می‌شوید.

با اصول سه‌گانهٔ امنیت اطلاعات آشنا می‌شوید.

با گام‌های پیاده‌سازی امنیت اطلاعات آشنا می‌شوید.

با ابعاد مرتبط با امنیت اطلاعات آشنا می‌شوید.

با شماری از راهکارهای عملی بهبود امنیت روی ویندوز ۸ به بعد آشنا می‌شوید (رمزگذاری فایل‌ها، تهیه کپی پشتیبان، کنترل لیست نرم‌افزارهای درحال اجرا).

۹ـ۱ امنیت اطلاعات چیست؟

با توجه به ویژگی‌های عصر امروزی که عصر اطلاعات نیز نامیده شده است مهم‌ترین سرمایه برای هر فرد و یا سازمان اطلاعات است از این رو در این عصر، امنیت اطلاعات جزء یکی از مهم‌ترین مسئله‌های امروزی گشته است.

امنیت اطلاعات به حفاظت از اطلاعات و به کمترین رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز اشاره دارد.

۹ـ۲ آشنایی با اصول امنیت اطلاعات

اندیشیدن امنیت اطلاعات برای دستیابی به سه اصل مهم است که با یکدیگر مثلث امنیتی را تشکیل می‌دهند. این عامل‌ها عبارت‌اند از محرمانگی (Confidentiality)، یکپارچگی و صحت (Integrity) و در نهایت در دسترس بودن همیشگی (Availability) این سه عامل (CIA) اصول اساسی امنیت اطلاعات در شبکه و یا بیرون آن را تشکیل می‌دهند به‌گونه‌ای که همهٔ تمهیدات لازمی که برای امنیت اطلاعات اتخاذ می‌شود و یا تجهیزاتی که ساخته می‌شوند، همگی ناشی از نیاز به اعمال این سه پارامتر در محیط‌های نگهداری و تبادل اطلاعات است.

محرمانگی (Confidentiality)

به معنای آن است که اطلاعات تنها در دسترس کسانی قرار گیرد که به آن نیاز دارند و این‌گونه تعریف شده است. برای نمونه از دست دادن این خصیصه امنیتی معادل است با بیرون رفتن بخشی از پرونده محرمانه یک شرکت و امکان دسترسی به آن توسط مطبوعات.

جامعیت (Integrity)

بیشتر مفهومی است که به علوم سامانه‌ای باز می‌شود و به گونهٔ چکیده می‌توان آن را این‌گونه تعریف کرد:

تغییرها در اطلاعات تنها باید توسط افراد یا فرایندهای مشخص و مجاز انجام گیرد.

تغییرها بدون اجازه و بدون دلیل حتی توسط افراد یا فرایندهای مجاز نباید انجام بگیرد.

یکپارچگی اطلاعات باید در درون و بیرون سامانه حفظ شود. به این معنی که یک داده مشخص چه در درون سامانه و چه در خارج آن باید یکسان باشد و اگر تغییر می‌کند باید هم‌زمان درون و برون سامانه از آن آگاه شوند.

دسترسی‌پذیری (Availibility)

این ویژگی تضمین می‌کند که یک سامانه برای نمونه اطلاعاتی همواره باید در دسترس باشد و بتواند کار خود را انجام دهد؛ بنابراین حتی اگر همه موردهای ایمنی مد نظر باشد، اما عامل‌هایی سبب خوابیدن سامانه شوند ـ مانند قطع برق ـ از نظر یک سامانه امنیتی این سامانه ایمن نیست.

اما جدای از مسئله‌های بالا مفاهیم و پارامترهای دیگری نیز هستند که با وجود آنکه از همین اصول گرفته می‌شوند برای خود شخصیت جداگانه‌ای پیدا کرده‌اند. در این میان می‌توان به مفاهیمی مانند Authentication به معنی احراز هویت کاربر، Authorization به معنی مشخص کردن میزان دسترسی کاربر به منابع، Accountability به معنی قابلیت حسابرسی و ثبت لاگ از عملکرد سامانه و کاربران سامانه و ... اشاره کرد.

۹ـ۳ پیاده‌سازی امنیت اطلاعات

برای برقراری مدیریت امنیت اطلاعات شش گام به شرح زیر متصور است:

▪ **گام۱:** توسعه، تصویب و ترویج خط‌مشی امنیت اطلاعات فراگیر:

باید با نظر کارشناسان خبره بخش‌های گوناگون دنباله‌ای از خط‌مشی‌های امنیت اطلاعات را مبنی بر استاندارد موجود توسعه، تصویب واجرا کرد. این دستور کار به صورت رسمی برنامهٔ امنیت اطلاعات سازمان را بیان می‌کند و کارکنان در برابر آن پاسخگو هستند. فهرست زیر شامل مجموعه‌ای از خط‌مشی‌ها رسمی سازمانی را بیان می‌کند و البته فقط محدود به موارد زیر نمی‌شود:

ـ به‌روزرسانی و اجرا کردن خط‌مشی پذیرفتنی در کاربرد رایانه و شبکه به صورت عمومی؛

ـ کنترل دسترسی اطلاعات و تعیین سطح دسترسی به داده‌ها و سامانه‌ها؛

ـ اعلام وصول، ذخیره‌سازی و پردازش و پخش اطلاعات حساس؛

ـ آزمایش و بازبینی امنیتی سخت‌افزار و نرم‌افزار به‌کار گرفته‌شده؛

ـ ممارست در حفاظت از داده‌های عمومی به صورت گزارش‌گیری از تخلف‌ها و تهدیدهای امنیتی؛

ـ مجوزهای قانونی تخریب، پشتیبان‌گیری و وضعیت رسانه‌های دیجیتالی؛

ـ حذف دسترسی‌های کارکنان که فعالیتشان به هر دلیلی پایان یافته است.

ـ ارزیابی و مدیریت مخاطره‌ها (ریسک).

▪ **گام۲:** کارکنان باید آگاه از پاسخگویی دربارهٔ امنیت اطلاعات باشند:

همه کارکنان باید در دورهٔ آشنایی و یادگیری امنیت اطلاعات و به‌کار بردن اصول حفاظت از اطلاعات سازمان شرکت کنند. برنامهٔ آموزشی باید دارای سطح‌بندی انعطاف‌پذیری برای مدیران ارشد، مدیران میانی، مدیران سامانه و شبکه و کارکنان

بخش‌های گوناگون باشد. برنامهٔ آموزشی با توجه به نوع فعالیت هر فرد و پاسخگو بودن در برابر سازمان تنظیم شود. مرحله‌های ساخت برنامه آموزشی شامل معیارهای زیر است:

ـ شناسایی و تحلیل فاصله میان وضعیت جاری و دانش مطلوب؛
ـ تعیین اولویت‌ها؛
ـ توسعهٔ آگاهی (با پست الکترونیک و صفحه‌های وب و خبرنامه‌ها)؛
ـ انتخاب موضوع‌های آموزشی (خط‌مشی‌های قابل اجرا)؛
ـ توسعهٔ آموزش و یادگیری براساس وظیفه و مسئولیت؛
ـ استفاده از فناوری برای آموزش (کاربرد وب، آموزش الکترونیک).

▪ **گام ۳:** ایجاد امور امنیت اطلاعات هر بخش:

در هر بخش فردی که توانایی مناسبی برای پیاده‌سازی و اجرای خط‌مشی‌های مورد نیاز امنیت اطلاعات دارد انتخاب شود. واحد امنیت اطلاعات در موارد زیر پاسخگو است والبته فقط محدود به موارد زیر نمی‌شود:

ـ توسعه، انتشار، نگهداری رویه‌ها، خط‌مشی‌های برنامهٔ امنیت سامانه‌های اطلاعاتی در بخش مربوطه؛
ـ متصدی رسیدگی به اعتراض‌ها، شکایت‌ها و تخلف‌های حوزهٔ تبادل اطلاعات و اهتمام در به نتیجه رساندن آنها؛
ـ متصدی کنترل نقاط اصلی در هنگام وقوع رویدادهای امنیتی و وخیم؛
ـ فراهم کردن پیشنهادهایی برای مدیران راهبردی (استراتژیک) که نیازمندی‌های مدیریت مخاطره‌ها و بحث‌های مربوط به فناوری سامانه‌های اطلاعاتی را پوشش دهد.

متصدی واحد امنیت اطلاعات بخش باید فعالیت‌های غیررسمی پیرامون امنیت اطلاعات نیز داشته باشد. موارد زیر پاسخگویی‌های غیررسمی متصدی واحد امنیت اطلاعات است والبته فقط محدود به این موارد نمی‌شود:

ـ مطمئن ساختن کارکنان به مناسب بودن نسبی خط‌مشی و دستور کارهای امنیت اطلاعات؛
ـ مطمئن شدن از انطباق امنیت پیاده‌شده بر راهبرها و خط‌مشی‌های امنیتی؛
ـ گزارش دادن به مدیر امنیت اطلاعات مبنی بر سنجش و ارزیابی قوانین مصوب مسئولان اجرایی.

▪ **گام ۴:** بنا نهادن فرایندی برای گزارش‌گیری منظم از پیشرفت کارها و ارائهٔ آن به مدیر اجرایی:

دفتر پیاده‌سازی امنیت باید دارای زمان‌بندی مشخصی برای گزارش پیشرفت و توسعه امنیت اطلاعات به رئیس سازمان داشته باشد. این گزارش‌ها در دو بعد قابل استفاده است:

۱) ارزیابی مسئول سازمان از توانمندی پیاده‌سازی امنیت اطلاعات توسط تیم اجرایی؛

۲) برطرف کردن نقص‌ها و ایرادهای خط‌مشی‌های امنیتی تصویب‌شده توسط مسئولان کلان سازمان.

▪ **گام ۵:** پیاده کردن کنترل‌های فعال وگسترده:

تعیین سامانه‌هایی که دارای اطلاعات حساس هستند و مطمئن بودن از استقرار کنترل‌های دسترسی و سامانه‌های اطلاعاتی که هر شخص فقط به اطلاعات مشخصی دسترسی دارد انواع کنترل دسترسی شامل کنترل دسترسی اجباری، احتیاطی، مبنی بر مسئولیت سازمانی و زمانی از روز است. اهم نظارت‌ها در این بخش عبارت‌اند از:

- ارزیابی بخش‌ها در راه‌اندازی خط‌مشی امنیتی؛
- شناسنامه‌دار کردن دستگاه‌ها؛
- تاکید بر پیچیدگی رمز عبور؛
- تاکید بر تغییر رمز به صورت دوره‌ای؛
- ثبت عملکرد کاربران در سامانه‌های اطلاعاتی.

▪ **گام ۶:** پیاده کردن و ارتقای پیوسته و برنامه‌های ترسیم رویدادها:

سازمان باید به صورت پیوسته به تحلیل و ارزیابی مخاطره‌های سازمانی بپردازد و برنامهٔ مشخص بخشی و سازمانی برای حفاظت و ترمیم سامانه‌های حساس، سرویس‌های شبکه و برنامه‌های کاربردی و داده‌ها داشته باشد. برنامه ارتقای مداوم عبارت است از:

- کنترل وارزیابی مخاطره‌ها؛
- تحلیل آسیب‌های حرفه و کسب و کار؛
- توسعهٔ مداوم راهبرد (استراتژی)های حرفه؛

ـ طراحی دفتر واکنش و فرایند؛
ـ آگاهی، آموزش و یادگیری؛
ـ معاونت و نگهداری پیوسته از برنامه‌های سازمانی.

۹ـ۴ ابعاد مرتبط با امنیت

ابعاد مرتبط با امنیت شامل سه بُعد است:
ـ امنیت فیزیکی
ـ امنیت عملیاتی
ـ مدیریت و تدابیر امنیتی

۱. برقراری امنیت فیزیکی (Physcial Security)

منظور از امنیت فیزیکی، حفاظت از دارایی‌ها و اطلاعات در برابر دسترسی فیزیکی افراد یا کارکنان غیرمجاز است. به عبارت دیگر شما مسئول حفاظت از بخش‌هایی هستید که قابل لمس کردن، دیده شدن و دزدیده شدن هستند. این تهدیدها بیشتر توسط سرویس‌کارها، دربان‌ها یا سرایدارها، مشتری‌ها، فروشنده‌ها و حتی کارمندان به‌وجود می‌آیند.

این‌گونه افراد می‌توانند ابزارها را ببینند و یا آنها را خراب کنند، یا از دفتر کار مدارک و اسنادی را به سرقت ببرند و یا در درون آنها اطلاعات ناخواسته قرار دهند، انگیزهٔ آنها در انجام این کارها می‌تواند انتقام گرفتن از شما باشد، حال این انتقام می‌تواند به خاطر به‌وجود آمدن یک سوء تفاهم باشد و یا اینکه به خاطر کینه‌جویی آن فرد نسبت به شما باشد و به همین دلیل، اطلاعات محرمانه شما را به سرقت برده و در اختیار رقیبان شما قرار می‌دهند.

پیاده‌سازی امنیت فیزیکی به نسبت کار آسانی است، شما می‌توانید تأسیسات خود را با استفاده از کنترل کردن دسترسی به دفتر کارتان ایمن کنید، مدارک و اسناد غیرضروری را ریز ریز کنید (نوعی حمله به نام dumpster diving معروف است) سامانه‌های امنیتی نصب کنید و به بخش‌های ویژه‌ای از فعالیت‌های بازرگانی خود محدودیت دسترسی بدهید.

بیشتر سازمان‌های اداری در ساعت‌های غیرفعال کاری محیط اطراف ساختمان را

تحت پوشش امنیتی قرار می‌دهند و به این وسیله آنجا را ایمن می‌کنند، همین کار را می‌توان در ساعت‌های اداری و فعال سازمان‌ها نیز اعمال کرد و چندان هم که به نظر می‌رسد دشوار نیست. بسیاری از سازمان‌ها و شرکت‌ها از سامانه‌های گوناگون امنیتی مانند نگهبان، قفل‌های کنترل ورود و خروج، سامانه‌های الکترونیک رمز ورود، دوربین‌های امنیتی، درگاه‌های کنترل و بازرسی بدنی و بسیاری دیگر از امکانات و تجهیزات امنیتی استفاده می‌کنند. در بیشتر موارد مدیران بخش‌ها به امنیت درونی بخش‌ها که مربوط به رایانه‌ها، اسناد و مدارک شخصی شما است سروکاری ندارند، در واقع حفاظت از این موارد جزء وظایف شخصی شما در آن بخش است.

نخستین جزء امنیت فیزیکی این است که شما وسوسه‌انگیزی سامانهٔ خود را تا حد امکان کم کنید، یعنی اینکه تا جایی که امکان دارد کاری کنید که محیط واقعی کمتر در معرض دید باشد. فرض کنید شما یک فروشگاه جواهرآلات دارید، این طبیعی است که در هنگامی که شما در تعطیلات بسر می‌برید ویترین فروشگاه خود را جمع کرده و آنها را در درون گاوصندوق قرار می‌دهید. دزدان با دیدن جواهر انگیزه بیشتری برای دزدی پیدا می‌کنند، اگر آنها را نبینند و در معرض دید نباشند انگیزه دزدان نیز به مراتب کمتر خواهد شد. این کاملاً طبیعی است که اگر کسی بتواند سرورهای شما را ببیند بیشتر از شخصی که آنها را نمی‌بیند وسوسه نفوذ به آنها را پیدا می‌کند. اگر شرکت یا سازمان شما به صورت تمام وقت باز است دسترسی به منابع تجاری موجود در آن نیز به مراتب آسان‌تر است، شما باید تا حد امکان سازمان خود را از معرض دید دیگران دور نگه دارید. قفل کردن درها، نصب سامانه‌های دیدبانی و نظارتی و نصب انواع هشداردهنده‌ها می‌تواند محیط فیزیکی را تا حد زیادی ایمن کند. در پیش هم به این موضوع اشاره شد که همیشه در این تفکر باشید که در حال هک شدن هستید، بنابراین کوشش کنید با ساده‌ترین فرایندهای ممکن امنیت را بالا برده تا با دشواری‌های ساده به دردسر نیفتید.

دومین بخش امنیت فیزیکی دربرگیرندهٔ تشخیص نفوذ یا دزدی است، شما باید بدانید چه کسی یا چه چیزی وارد شده است و یا از میان رفته است. باید بدانید که چه چیزهایی ناپدید شده است و این تغییرها چگونه روی داده است. دوربین‌های مدار بسته روش بسیار خوبی برای به دست آوردن این اطلاعات است. بیشتر شرکت‌های کوچک برای تشخیص چگونگی رخ دادن دزدی‌ها و اینکه چه کسی آن را انجام داده است از

این گونه دوربین‌ها استفاده می‌کنند. فیلم‌هایی که از این گونه دوربین‌ها به دست می‌آید در بیشتر دادگاه‌ها مدارک و اسناد قابل استنادی به‌شمار می‌آیند. به عنوان یک مدیر شبکه شرکت، شما باید بی‌درنگ پس از رخ دادن دزدی، به هیچ چیز دست نزنید، و با سرعت موضوع را به مراجع قانونی اطلاع دهید تا به بررسی موضوع بپردازند. این نکته را به یاد داشته باشید که در چنین حالتی شما باید به هر کسی که فکر می‌کنید ظنین باشد.

سومین بخش امنیت فیزیکی ارزیابی اطلاعات ازدست‌رفته است. فرض کنید که اطلاعات حیاتی یک شرکت از میان رفته است، چه‌کار باید کرد؟ چگونه یک سازمان پس از به‌وقوع پیوستن یک دزدی یا فاجعه می‌تواند به حالت عادی خود بازگردد؟ با یک نمونه این موضوع روشن‌تر می‌شود، فرض کنید یک خرابکار اتاق سرورهای شما را که همهٔ اطلاعات حیاتی سازمان شما در آن وجود دارد را به آتش می‌کشد و یا در استان گلستان هستید و سیل به‌وجود آمده همهٔ اداره شما را می‌شوید و از میان می‌برد، یا در تهران هستید و زلزله‌ای رخ داده و دفتر کار شرکت به صورت کامل از میان می‌رود، البته فرض را در این می‌گیریم که در همهٔ شرایط بالا شما در امنیت کامل بسر می‌برید و پس از فاجعه فرصت رسیدگی به موضوع را دارید. یا ساده‌ترین نمونه اینکه در هنگام کار کردن با سرورها در اتاق سرور یک پارچ آب به صورت کامل روی سرورها ریخته و همهٔ اطلاعات سرور از میان می‌رود! چقدر طول می‌کشد تا سازمان فعالیت عادی خود را که به اطلاعات یادشده وابسته است را از سر گیرد؟

۲. برقراری امنیت عملیاتی(Operational Security)

امنیت عملیاتی یا اجرایی شیوهٔ انجام دادن کارهای سازمان را بیان می‌کند. در معنای عام می‌توان به عنوان مدیریت اطلاعات از آن نام برد. امنیت عملیاتی پهنه وسیعی را دربر می‌گیرد که شما هم بخشی از آن هستید. اصول امنیت عملیاتی شامل: کنترل دسترسی، شناسایی و مکان‌شناسی (توپولوژی‌های) امنیتی است. موارد یادشده شامل فعالیت‌های روزانه شبکه، اتصال به شبکه‌های دیگر، طراحی شیوهٔ تهیه نسخهٔ پشتیبان و طراحی شیوهٔ بازگردانی آن می‌شود که البته همهٔ این موارد در حالتی امکان‌پذیرند که نصب شبکه کامل شده باشد. اگر بخواهیم امنیت عملیاتی را در یک جمله خلاصه کنیم به این صورت بیان می‌شود: شامل هر چیزی در شبکه شما می‌شود که به طراحی و امنیت فیزیکی شما بستگی ندارد.

در این بخش به جای اینکه تمرکز خود را بر تجهیزات فیزیکی قرار دهیم، بیشتر به مکان‌شناسی (توپولوژی)ها و اتصال‌ها و پیکربندی‌ها توجه می‌کنیم. فرایندی که شما باید در بخش فیزیکی انجام دهید در ابتدا بسیار طاقت‌فرسا به نظر می‌رسد. در بسیاری اوقات شما از نقاط آسیب‌پذیر شبکه بدون اینکه بدانید در حال استفاده هستید و یا بدون اطلاع، خط‌مشی را پیاده‌سازی کرده‌اید که دارای ضعف امنیتی است یا ناقص است. برای نمونه شما خط‌مشی را پیاده‌سازی کرده‌اید که در آن کاربران مجبور هستند که رمزهای گذر خود را هر ۳۰ یا ۶۰ روز عوض کنند، حال اگر در سامانهٔ شما قابلیت استفاده از سامانهٔ چرخش رمز گذر طراحی نشده باشد (این سامانه به شما اجازهٔ استفاده از رمزهای گذر تکراری مورد استفاده در زمان‌های گذشته را نمی‌دهد) شما یک نقطهٔ آسیب‌پذیر جدی در شبکهٔ خود دارید که شاید نتوانید آن را از میان ببرید، در این حالت از نظر دیدگاه فرایندی سامانه قابلیت رمز گذر ضعیفی دارد. در این حالت شما دو گزینه برای انتخاب دارید، یا باید فرایند امنیتی اطلاعات را به‌گونهٔ کامل ارتقا دهید و یا اینکه سیستم عامل را به‌گونهٔ کلی عوض کنید. انجام دادن هریک از این فرایندها دشواری‌های ویژه خود را مانند میزان بودجه، زمان بدل و بی‌میلی سازمان برای انجام این کار را دربر دارد. گفتنی است که متأسفانه یا خوشبختانه در کشور عزیز ما ایران به علت نبود قانون کپی رایت، دشواری تعویض سیستم عامل وجود ندارد زیرا هزینه‌ای برای تعویض آن و تهیه سیستم عامل نو پرداخت نمی‌شود، اما فرض را بر این بگیرید که در شرکتی هستید که به‌گونهٔ متوسط ۲۰۰ عدد سیستم عامل ویندوز ایکس پی در آن مشغول کار هستند، حال اگر باید ۲۰۰ عدد سیستم عامل، دست‌کم ۶۰ دلاری، خریداری شود هزینه‌ها بسیار بالا می‌رود، ذهن خود را درگیر CDهایی نکنید که در بازار یا کنار خیابان فروخته می‌شوند و ۸ سیستم عامل روز جهان را با بهای کمتر از هزار تومان به مردم عرضه می‌کنند.

اما دشواری اصلی، بی‌میلی سازمان و مدیران برای انجام تغییرها در سازمان است. متأسفانه برخی از مدیران سنتی عمل می‌کنند و از انجام دادن تغییرها در روند ایجاد محیطی ایمن می‌هراسند، یا احساس بی‌میلی دارند که از نظر بسیاری از کارشناسان بزرگ‌ترین دشواری موجود در برقراری امنیت عملیاتی همین مورد است، اگر مدیر نخواهد کاری انجام شود، پس نمی‌شود تلاش بیهوده نکنید. اما هر دشواری راهکاری نیز دارد که به آن خواهیم پرداخت.

اگر سیستم عامل شما داری نقاط ضعف امنیتی زیادی باشد متقابلاً وظیفه شما نیز افزایش می‌یابد زیرا همچنان شما مسئول برقراری امنیت در آنجا هستید، برای نمونه: اگر شبکه شما که تا حدی ایمن است به اینترنت متصل شود، هدف نفوذ بسیاری از افراد قرار خواهد گرفت، حال شما می‌توانید با نصب نرم‌افزارها و سخت‌افزارهای امنیتی، امنیت را تا حد مطلوبی افزایش دهید. در هر حال مدیران باور دارند که این گونه ابزارها برای پیاده‌سازی پرهزینه هستند، بنابراین شما کار زیادی نمی‌توانید انجام دهید. تنها راه‌حلِ قانع کردن مدیران، نشان دادن شدت تهدیدهایی است که ممکن است عملکرد شرکت یا سازمان را مختل کند و آن را گرفتار تهدید کند. در زیر می‌توانید چکیده مواد مرتبط با امنیت عملیاتی را ببینید:

رایانه	شبکه	خط‌مشی‌ها
مدیریت	کنترل دسترسی	شناسایی
طرح و نقشه تهیه نسخه پشتیبان و بازگردانی آن		

۳. مدیریت و خط‌مشی‌ها (Management and Policies)

مدیریت و خط‌مشی‌ها در واقع برنامه‌هایی هستند که با توجه به آنها می‌توانیم امنیت یک محیط را پیاده‌سازی کنیم. خط‌مشی‌ها برای اینکه کارا باشند نیاز به پشتیبانی همه جانبه از جانب تیم مدیریتی سازمان دارند. راهنماهای درست نه تنها می‌توانند سبب به‌وجود آمدن ابتکارهای امنیتی در محیط شوند بلکه سبب به‌وجود آمدن یک امنیت کارا نیز هستند. متخصصان امنیت اطلاعات می‌توانند خط‌مشی‌های امنیتی خود را ادامه دهند، اما برای اینکه بتوانند آنها را پیاده‌سازی کنند نیاز به پشتیبانی مدیران دارند، این نکته را همیشه به یاد داشته باشید که شما هیچ وقت نمی‌توانید ادعا کنید که شبکه من ایمن است و این در حالی باشد که از پشتیبانی مدیران برخوردار نیستید.

تصمیم‌هایی که باید در سطح مدیریت و خط‌مشی‌ها اتخاذ شود به گونهٔ کامل سازمان را زیر پوشش قرار می‌دهد و می‌تواند بهره‌وری، روحیه کاری و فرهنگ سازمان را تحت تأثیر خود قرار بدهد. این گونه تصمیم‌ها و خط‌مشی‌ها می‌تواند تأثیر بسزایی بر روی مسئله‌های مرتبط با امنیت نیز داشته باشد. این گونه خط‌مشی‌ها باید به‌گونه‌ای طراحی شوند که هدایت سازمان، آسانی در مواقعی که سازمان در تعطیلات به‌سر می‌برد یا کارمندان به مرخصی می‌روند و یا کار آنان به پایان می‌رسد را به گونهٔ کامل زیر پوشش قرار دهند.

بیشتر افرادی که در یک سازمان فعالیت می‌کنند می‌توانند به‌آسانی به شما بگویند که چه مدت زمانی را در طی سال در مرخصی به‌سر می‌برند و همچنین بسیاری دیگر به شما می‌توانند اطلاعات دقیقی از چگونگی استفاده اطلاعات در سازمان و اینکه خط‌مشی‌ها چگونه پیاده‌سازی شده‌اند را در اختیارتان قرار دهند، پس همیشه کاربران و کارمندان را می‌توانید در نقش یک منبع اطلاعاتی بسیار کارا در پیاده‌سازی فعالیت‌های امنیت خود در نظر بگیرید.

برای برقراری امنیت در یک شبکه چندین خط‌مشی کلیدی وجود دارد، سیاهه (لیست) زیر نشان‌دهندهٔ شماری از این خط‌مشی‌های گسترده است که هر کدام نیاز به طراحی و تفکر دارند:

خط‌مشی‌های مدیریتی (Management Policies)

نیازهای طراحی نرم‌افزار (Software Design Needs)

طرح و برنامهٔ بازیابی از حادثه (Disaster Recovery Plan)

خط‌مشی‌های اطلاعاتی (Information Policies)

خط‌مشی‌های امنیتی (Security Policies)

خط‌مشی‌های مدیریتی کاربران (User Management Polices)

۹ـ۵ تدابیر و فرایند لازم برای امنیت فناوری اطلاعات

اگر می‌خواهیم علاوه بر مصرف‌کنندهٔ اطلاعات، ارائه‌دهندهٔ اطلاعات در عصر اطلاعات باشیم، باید در مراحل بعد، امکان استفاده از اطلاعات ذیربط را برای متقاضیان محلی و جهانی در باسرعت‌ترین زمان ممکن فراهم کنیم.

سرعت در تولید و عرضهٔ اطلاعات ارزشمند، یکی از رموز موفقیت در سازمان‌ها، مؤسسه‌ها و جوامع علمی در عصر اطلاعات است. پس از سازماندهی اطلاعات باید با بهره‌گیری از شبکه‌های رایانه‌ای، زمینه استفاده قانونمند و هدفمند از اطلاعات را برای دیگران فراهم کرد. به موازات حرکت به سمت یک سازمان پیشرفته و مبتنی بر فناوری اطلاعات، باید تدابیر لازم برای حفاظت از اطلاعات نیز اندیشیده شود.

مهم‌ترین برتری و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دستیابی با سرعت و آسان به اطلاعات است. کنترل دستیابی و شیوهٔ

استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای به‌ویژه اینترنت، نگرش به امنیت اطلاعات و دیگر منابع به اشتراک گذاشته‌شده، وارد مرحله جدیدی شده است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند، به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی را پیاده‌سازی و اجرا کند.

نبود نظام مناسب امنیتی، ممکن است پیامدهای منفی و دور از انتظاری را به دنبال داشته باشد. توفیق در ایمن‌سازی اطلاعات منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در برابر حمله‌ها است؛ بدین منظور از سرویس‌های امنیتی پرشماری استفاده می‌شود. سرویس‌های انتخابی باید پتانسیل لازم در خصوص ایجاد یک نظام حفاظتی مناسب، تشخیص به‌هنگام حمله‌ها و واکنش باسرعت را داشته باشند. بنابراین می‌توان محور راهبردی برگزیده را بر سه مؤلفه استوار کرد:

۱. حفاظت
۲. تشخیص
۳. واکنش

حفاظت مطمئن، تشخیص به‌هنگام و واکنش مناسب، ازجمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت کرد. خوشبختانه پژوهش‌های زیادی در زمینهٔ امنیت رایانه و شبکه‌ها در مورد فناوری‌های امنیتی پیشگیرانه (کُنشی) و نیز رویارویی با دشواری‌های امنیتی (واکنشی) انجام گرفته است. نوشته حاضر درصدد بیان، شماری از فناوری‌های موجود دربارهٔ امنیت اطلاعات با یک دیدگاه طبقه‌بندی است.

۹ـ۶ طبقه‌بندی فناوری‌های امنیت اطلاعات از نگاه مؤسسهٔ INFOSE

طبقه‌بندی ارائه‌شده در نوشته حاضر از فناوری‌های امنیت اطلاعات، در وهلهٔ اول براساس دو ویژگی پایه‌گذاری شده است.

۹ـ۶ـ۱ براساس مرحلهٔ ویژه‌ای از زمان

بدین معنا که در زمان تعامل فناوری با اطلاعات، واکنش لازم در برابر یک دشواری امنیتی می‌تواند کنشی (Proactive) یا واکنشی (Reactive) باشد.

غرض از «کنشگرایانه»، انجام فرایندهای پیشگیرانه پیش از وقوع یک دشواری ویژهٔ امنیتی است. در چنین مواردی به موضوع‌هایی اشاره می‌شود که ما را در پیشگیری از وقوع یک دشواری کمک خواهد کرد (چه کار باید انجام دهیم تا...؟).

غرض از «واکنشی» انجام دادن واکنش لازم پس از وقوع یک دشواری ویژهٔ امنیتی است. در چنین مواردی به موضوع‌هایی اشاره می‌شود که ما را در مقابله با یک دشواری پس از وقوع آن، کمک خواهند کرد (اکنون که... چه کار باید انجام بدهیم؟).

۹ـ۶ـ۲ براساس سطوح پیاده‌سازی نظام‌های امنیتی در یک محیط رایانه‌ای

فناوری امنیت اطلاعات را، خواه از نوع کنشی باشد یا واکنشی، می‌توان در سه سطح ـسطح شبکه (Network Level)، سطح میزبان (Host Level) و سطح برنامه کاربردی (Application Level)ـ پیاده‌سازی کرد (همان). بدین منظور می‌توان نظام امنیتی را در سطح شبکه و خدمات ارائه‌شدهٔ آن، در سطح برنامهٔ کاربردی ویژه، یا در محیطی که شرایط لازم برای اجرای یک برنامه را فراهم می‌کند (سطح میزبان) پیاده کرد.

فناوری‌های امنیت اطلاعات کنشگرایانه

رمزنگاری (Cryptography)

به بیان ساده، رمزنگاری به معنای «نوشتن پنهان» و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده‌ها است. این علم شامل اعمال رمزگذاری، رمزگشایی و تحلیل رمز است. در اصطلاح‌های رمزنگاری، پیام را متن آشکار (plaintext or cleartext) می‌نامند. کدگذاری مضامین را به شیوه‌ای که آنها را از دید بیگانگان پنهان کند، (encryption) یا سِرگذاری (encipher) می‌نامند. پیام رمزگذاری‌شده را متن رمزی (ciphertext) و فرایند بازیابی متن آشکار از متن رمزی را رمزگشایی(decryption) یا سِرّگشایی (decipher) می‌نامند.

الگوریتم‌هایی که امروزه در رمزگذاری و رمزگشایی داده‌ها به کار می‌روند از دو روش بنیادی استفاده می‌کنند: الگوریتم‌های متقارن و الگوریتم‌های نامتقارن یا کلید عمومی. تفاوت آنها در این است که الگوریتم‌های متقارن از کلید یکسانی برای رمزگذاری و رمزگشایی استفاده می‌کنند، یا این که کلید رمزگشایی به‌سادگی از کلید رمزگذاری استخراج می‌شود. مانند:

DES (Data Encryption Standard), CCEP (The Commercial Comsec Endoremment Program), IDEA (International Data Encryption Algoritm)

در حالی که الگوریتم‌های بی‌تقارن از کلیدهای متفاوتی برای رمزگذاری و رمزگشایی استفاده می‌کنند و امکان استخراج کلید رمزگشایی از کلید رمزگذاری وجود ندارد. همچنین کلید رمزگذاری را کلید عمومی و کلید رمزگشایی را کلید خصوصی یا کلید محرمانه می‌نامند (مانند RSA).

تجزیه‌وتحلیل رمز (cryptanalysis)، هنر شکستن رمزها و به عبارت دیگر، بازیابی متن آشکار بدون داشتن کلید مناسب است؛ افرادی که فرایند رمزنگاری را انجام می‌دهند، رمزنگار (cryptographer) نامیده می‌شوند و افرادی که در تجزیه‌وتحلیل رمز فعالیت دارند رمزکاو (cryptanalyst) هستند.

رمزنگاری با همهٔ جنبه‌های پیام‌رسانی امن، تعیین اعتبار، امضاهای رقومی، پول الکترونیک و نرم‌افزارهای کاربردی دیگر ارتباط دارد. رمزشناسی (cryptology) شاخه‌ای از ریاضیات است که پایه‌های ریاضی مورد استفاده در شیوه‌های رمزنگاری را مطالعه می‌کند.

رمزنگاری، یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا اطلاعات را پیش از آنکه یک تهدید بالقوه بتواند اعمال خرابکارانه انجام دهد، از راه رمزگذاری داده‌ها ایمن می‌کنند. به علاوه، رمزنگاری در سطوح متنوع، به گونه‌ای که در طبقه‌بندی بیان شد، در سطوح برنامه‌های کاربردی و در سطوح شبکه قابل پیاده‌سازی است.

امضاهای دیجیتال یا رقومی (Digital Signatures)

امضاهای رقومی، معادل «امضای دست‌نوشت» و مبتنی بر همان هدف هستند: نشانه منحصربه‌فرد یک شخص، با یک بدنه متنی. به این ترتیب، امضای رقومی مانند امضای دست‌نوشت، نباید قابل جعل باشد. این فناوری که با استفاده از الگوریتم رمزنگاری ایجاد می‌شود، تصدیق رمزگذاری‌شده‌ای است که به گونهٔ معمول به یک پیام پست الکترونیک یا یک گواهی‌نامه پیوست می‌شود تا هویت واقعی تولیدکننده پیام را تأیید کند.

امضای رقومی یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا پیش از وقوع هر تهدیدی، می‌توان با استفاده از آن فرستندهٔ اصلی پیام و صاحب امضا را شناسایی کرد. افزون بر این، فناوری در سطح یک برنامه کاربردی قابل پیاده‌سازی است. در این سطح، امضای رقومی در یک برنامه کاربردی ویژه و پیش از آنکه به یک گیرنده ویژه فرستاده شود، ایجاد می‌شود.

گواهی‌های رقومی(Digital certificates)

گواهی‌های رقومی به حل مسئلهٔ «اطمینان» در اینترنت کمک می‌کنند. گواهی‌های رقومی متعلق به «شخص ثالث مورد اعتماد» (Trusted Third Parties) هستند و همچنین به «مراجع صدور گواهی» اشاره دارند. مراجع صدور گواهی (Certificate Authorities)، مؤسسه‌های تجاری هستند که هویت افراد یا سازمان‌ها را در وب تأیید و تأییدیه‌هایی مبنی بر درستی این هویت‌ها صادر می‌کنند.

برای به‌دست آوردن یک گواهی، ممکن است از فرد خواسته شود که یک کارت شناسایی (مانند گواهینامهٔ رانندگی) را نشان دهد. بنابراین گواهی‌های رقومی، یک شبکه امن در میان کاربران وب و مکانی برای تأیید صحت و جامعیت یک فایل یا برنامه الکترونیک ایجاد می‌کنند. این گواهی‌ها دارای نام فرد، شماره سریال، تاریخ انقضا، یک نسخه از گواهی نگاهدارنده کلید عمومی (که برای رمزگذاری پیام‌ها و امضاهای رقومی به کار می‌رود) هستند.

گواهی‌های رقومی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا از این فناوری برای پخش کلید عمومی از یک گروه ارتباطی به گروه ارتباطی دیگر استفاده می‌شود. همچنین این روش، پیش از آنکه هر ارتباطی میان گروه‌ها اتفاق بیفتد، اطمینان ایجاد می‌کند. این فناوری در سطح برنامه کاربردی قابل پیاده‌سازی است؛ برای نمونه پیش از آغاز هر ارتباط مرورگر وب، تأیید می‌کند که آن گروه ویژه قابل اطمینان است.

شبکه‌های مجازی خصوصی(virtual private networks)

فناوری شبکه‌های مجازی خصوصی، گذر و مرور شبکه را رمزگذاری می‌کند. بنابراین این فناوری برای تضمین درستی و امنیت داده‌ها، به رمزنگاری وابسته است. این شبکه بسیار امن، برای انتقال داده‌های حساس (ازجمله اطلاعات تجاری الکترونیک) از اینترنت به عنوان رسانه انتقال بهره می‌گیرد. شبکه‌های مجازی خصوصی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا داده‌ها پیش از آنکه در شبکهٔ عمومی منتشر شوند، با رمزگذاری محافظت می‌شوند و این سبب می‌شود که تنها افراد مجاز توانا به خواندن اطلاعات باشند.

افزون بر این، این فناوری در سطح شبکه قابل پیاده‌سازی است و از فناوری رمزگذاری میان دو میزبان شبکه مجازی خصوصی، در مرحله ورود به شبکه و پیش از آنکه داده‌ها به شبکهٔ عمومی فرستاده شود، استفاده می‌شود.

نرم‌افزارهای اسکنر آسیب‌پذیری (vulnerability scanners)

نرم‌افزارهای آسیب‌نما برنامه‌هایی برای بررسی نقاط ضعف یک شبکه یا سامانه یا سایت هستند. بنابراین نرم‌افزارهای آسیب‌نما یک نمونه ویژه از نظام آشکارساز نفوذی از فناوری امنیت اطلاعات هستند.

همچنین این نرم‌افزارها به یک پویش فاصله‌مدار اشاره دارند؛ بدین معنا که میزبان‌های روی شبکه را در فاصله‌های ویژه و نه به گونهٔ پیوسته، پویش می‌کنند. به مجرد اینکه یک نرم‌افزار آسیب‌نما بررسی یک میزبان را پایان داد، داده‌ها در درون یک گزارش، نمونه‌برداری می‌شوند، که به یک عکس فوری (snapshot) شباهت دارد (مانند: cybercop scanner، cisco secure scanner و Net Recon).

نرم‌افزارهای آسیب‌نما، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا از آنها برای کشف عامل‌های نفوذی پیش از آنکه بتوانند با فرایندهای خرابکارانه یا بدخواهانه از اطلاعات سوء استفاده کنند، استفاده می‌شود. نرم‌افزارهای آسیب‌نما در سطح میزبان قابل پیاده‌سازی هستند.

پویشگرهای پاد (ضد) ویروس(Anti- virus)

در دهه‌های گذشته ویروس‌های رایانه‌ای سبب تخریب بزرگی در اینترنت شده‌اند. ویروس رایانه‌ای یک قطعه مخرب نرم‌افزاری است که توانایی تکثیر خودش را در سراسر اینترنت، با یک بار فعال شدن، دارد. ضد ویروس، برنامه‌های نرم‌افزاری هستند که برای بررسی و حذف ویروس‌های رایانه‌ای، از حافظه یا دیسک‌ها طراحی شده‌اند. این برنامه‌ها از راه جستجوی کدهای ویروس رایانه‌ای، آنها را تشخیص می‌دهند. اگرچه برنامه‌های حفاظت از ویروس نمی‌توانند همهٔ ویروس‌ها را نابود کنند، اما کارهایی که این برنامه‌ها انجام می‌دهند عبارت‌اند از:

۱. ممانعت از فعالیت ویروس؛
۲. حذف ویروس؛
۳. تعمیر آسیبی که ویروس عامل آن بوده است؛
۴. گرفتن ویروس در زمان کنترل و پس از فعال شدن آن.

ضدویروس، یک فناوری امنیت اطلاعات از نوع کنشگرایانه است. این نرم‌افزارها در سطوح متنوع و به گونه‌ای که در طبقه‌بندی بیان شده در سطح برنامه‌های کاربردی و در سطح میزبان، قابل پیاده‌سازی هستند.

پروتکل‌های امنیتی (security protocols)

پروتکل‌های امنیتی گوناگونی مانند «پروتکل امنیت اینترنت» (Ipsec)[1] و کربروس (161erberos) که در فناوری‌های امنیت اطلاعات طبقه‌بندی می‌شوند، وجود دارند. پروتکل‌ها، فناوری‌هایی هستند که از یک روش استاندارد برای انتقال منظم داده‌ها میان رایانه‌ها استفاده می‌کنند، یا مجموعه‌ای از مقررات یا قراردادها هستند که تبادل اطلاعات را میان نظام‌های رایانه‌ای، کنترل و هدایت می‌کنند.

پروتکل‌های امنیتی، یک فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا برای حفاظت از اطلاعات حساس از یک پروتکل ویژهٔ امنیتی، پیش از آن که اطلاعات توسط خرابکاران به دست آید، استفاده می‌کنند. این فناوری در سطوح گوناگون ـ سطح برنامهٔ کاربردی و سطح شبکه ـ قابل پیاده‌سازی است. برای نمونه پروتکل «کربروس»، پروتکل و سامانه‌ای است که از آن در تعیین اعتبار سامانه‌های اشتراکی استفاده می‌شود. «کربروس» برای تعیین اعتبار میان فرایندهای هوشمند (مانند از خدمت‌گیرنده به خدمت‌دهنده، یا ایستگاه کاری یک کاربر به دیگر میزبان‌ها) مورد استفاده قرار می‌گیرد و این تعیین اعتبار در سطح برنامه کاربردی و شبکه، قابل پیاده‌سازی است.

سخت افزارهای امنیتی(Security hardware)

سخت افزار امنیتی به ابزارهای فیزیکی که کاربرد امنیتی دارند، اشاره می‌کند؛ مانند معیارهای رمزگذاری سخت‌افزاری یا مسیریاب‌های سخت‌افزاری. ابزارهای امنیت فیزیکی شامل امنیت سرورها، امنیت کابل‌ها، سامانه‌های هشداردهنده امنیتی در زمان دسترسی غیرمجاز یا ذخیرهٔ فایل‌ها پس از استفاده یا گرفتن فایل پشتیبان هستند.

این فناوری یک فناوری امنیت اطلاعات از نوع کنشگرایانه است، زیرا داده‌ها را پیش از آنکه تهدید بالقوه‌ای بتواند تحقق یابد، حفاظت می‌کنند. برای نمونه از رمزگذاری داده‌ها به منظور جلوگیری از فرایندهای خرابکارانه و جرح و تعدیل ابزار سخت‌افزاری استفاده می‌شود. این فناوری در سطح شبکه قابل پیاده‌سازی است. برای نمونه یک کلید سخت‌افزاری می‌تواند در درون درگاه میزبان برای تعیین اعتبار کاربر، پیش از آنکه کاربر بتواند به میزبان متصل شود به کار رود، یا معیارهای رمزگذاری

---

1. Internal Protocol Security

سخت‌افزار روی شبکه، یک راه حل مقاوم به دستکاری را فراهم آورد و در نتیجه ایمنی فیزیکی را تأمین کند.

کیت‌های توسعهٔ نرم‌افزار امنیتی(security software development kits (SDKs))

کیت‌های توسعهٔ نرم‌افزار امنیتی، ابزارهای برنامه‌نویسی هستند که در ایجاد برنامه‌های امنیتی مورد استفاده قرار می‌گیرند. «Java security manager» یا « Microsoft.net SDKs» نمونه نرم‌افزارهایی هستند که در ساختن برنامه‌های کاربردی امنیتی (مانند برنامه‌های تعیین اعتبار مبتنی بر وب) به کار می‌روند. این کیت‌ها شامل سازنده صفحه تصویری، یک ویراستار، یک مترجم، یک پیونددهنده و امکانات دیگر هستند. کیت‌های توسعه نرم‌افزار امنیتی، فناوری امنیت اطلاعات از نوع کنشگرایانه هستند، زیرا از آنها در توسعهٔ نرم‌افزارهای متنوع برنامه‌های کاربردی امنیتی (که داده‌ها را پیش از آن که تهدید بالقوه تحقق یابد، حفاظت می‌کنند) استفاده می‌شوند. افزون بر این، این فناوری در سطوح متنوع- سطح برنامه‌های کاربردی، سطح میزبان، سطح شبکه- قابل پیاده‌سازی است.

فناوری‌های امنیت اطلاعات واکنشی

دیوار آتش (firewalls)

دیوار آتش در اینترنت یک ابزار نرم‌افزاری، به‌ویژه روی یک رایانه پیکربندی‌شده است که به عنوان مانع، فیلتر یا گلوگاه میان یک سازمان درونی یا شبکهٔ امین و شبکهٔ غیرامین یا اینترنت، نصب می‌شود. هدف از دیوار آتش جلوگیری از ارتباطات غیرمجاز در درون یا بیرون شبکه درونی سازمان یا میزبان است. دیوار آتش به عنوان نخستین خط دفاعی در تلاش برای راندن عامل مزاحم، مورد توجه قرار می‌گیرد. اگرچه فناوری رمزگذاری به حل بسیاری از دشواری‌های ایمنی کمک می‌کند، به یک فناوری ثانوی نیز نیاز داریم. فناوری معروف به دیوار آتش اینترنت کمک می‌کند تا رایانه‌ها و شبکه‌های یک سازمان را از ترافیک نامطلوب اینترنت محافظت کند. این فناوری برای پرهیز از دشواری‌های ایجاد شده در اینترنت یا گسترش آنها به رایانه‌های سازمان طراحی می‌شود. دیوار آتش میان نظام‌های سازمان و اینترنت قرار می‌گیرد.

دیوار آتش یک فناوری امنیت اطلاعات از نوع واکنشی است و مهم‌ترین ابزار امنیتی مورد استفاده برای کنترل ارتباطات شبکه‌ای میان دو سازمان است که به یکدیگر

اعتماد ندارند. با قرار دادن یک دیوار آتش روی هر ارتباط خارجی شبکه، سازمان می‌تواند یک دایره امنیتی تعریف کند که از ورود افراد خارجی به رایانه‌های سازمان جلوگیری می‌کند. افزون بر آن، دیوار آتش می‌تواند مانع نفوذ افراد خارجی به منابع موجود در رایانه‌های سازمان و گسترش نامطلوب روی شبکه سازمان شود. این فناوری در سطوح میزبان و در سطح شبکه قابل پیاده‌سازی است.

کنترل دسترسی(access control)

کنترل دسترسی به مجموعه سیاست‌ها و اقدام‌های مربوط به اجازه دادن یا ندادن برای دسترسی یک کاربر ویژه به منابع، یا محدود کردن دسترسی به منابع نظام‌های اطلاعاتی برای کاربران، برنامه‌ها، پردازه‌ها یا دیگر سامانه‌های مجاز گفته می‌شود. هدف از این فناوری، حصول اطمینان است از اینکه یک موضوع، حقوق کافی برای انجام فرایندهای ویژه روی سامانه را دارد. این موضوع ممکن است کاربر، یک گروه از کاربران، یک خدمت، یا یک برنامه کاربردی باشد. موضوع‌ها در سطوح گوناگون، امکان دسترسی به اشیای ویژه‌ای از یک سامانه را دارند. این شیء ممکن است یک فایل، راهنما، چاپگر یا یک فرایند باشد. کنترل دسترسی ابزاری است که امنیت شبکه را از راه تأمین کاراکترهای شناسایی و واژهٔ گذر تضمین می‌کند و فناوری امنیت اطلاعات از نوع واکنشی است، زیرا دسترسی به یک نظام را به محض اینکه یک درخواست دسترسی صورت گیرد، مجاز یا غیرمجاز می‌شمارد. این فناوری در سطوح متنوع- در سطح برنامه کاربردی، در سطح میزبان و در سطح شبکه- قابل پیاده‌سازی است.

واژه‌های گذر (passwords)

واژهٔ گذر، یک کلمه، عبارت یا حرف‌های متوالی رمزی است که فرد برای به‌دست آوردن جواز دسترسی به اطلاعات (برای نمونه یک فایل، برنامه کاربردی یا نظام رایانه‌ای) باید وارد کند. این کلمه برای شناسایی و برای اهداف امنیتی در یک نظام رایانه‌ای به کار می‌رود. به هر کاربر مجموعه معینی از الفبا و عدد اختصاص داده می‌شود تا به همه یا بخش‌هایی از نظام رایانه‌ای دسترسی داشته باشد. واژهٔ گذر، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا به منظور گرفتن مجوز و دسترسی به نظام، به محض اینکه یک فرد یا فرایند بخواهد به یک برنامه کاربردی، میزبان یا شبکه متصل شود، به کار می‌رود. این فناوری در سطوح متنوع- در سطح برنامه کاربردی، سطح میزبان، سطح شبکه- پیاده‌سازی می‌شود.

زیست‌سنجی (biometric)

زیست‌سنجی، علم و فناوری سنجش و تحلیل داده‌های زیستی است. در فناوری اطلاعات، زیست‌سنجی به گونهٔ معمول به فناوری‌هایی برای سنجش و تحلیل ویژگی‌های بدن انسان (مانند اثر انگشت، قرنیه و شبکیه چشم، الگوهای صدا، الگوهای چهره و اندازه‌های دست) به‌ویژه به منظور تعیین اعتبار اشاره دارد. یکی از ویژگی‌های ذاتی علم زیست‌سنجی این است که کاربر باید با یک الگوی مرجع مقایسه شود. اثر انگشت، چهره یا داده‌های زیست‌سنجی دیگر را می‌توان جایگزین کارت هوشمند کرد و کاربران می‌توانند هم از کارت هوشمند و هم از اثر انگشت یا چهره خود برای تعیین اعتبار در امور بازرگانی، بانک‌ها یا ارتباط تلفنی استفاده کنند.

زیست‌سنجی فناوری امنیت اطلاعات از نوع واکنشی است، زیرا از آن می‌توان با استفاده از هندسه بخشی از بدن کاربر برای گرفتن مجوز یا برای جلوگیری از دسترسی به نظام، به محض اینکه کاربر بخواهد به یک برنامه کاربردی، میزبان یا شبکه متصل شود، استفاده کرد. افزون بر این، این فناوری در سطوح متنوع، با توجه به طبقه‌بندی بیان‌شده، قابل پیاده‌سازی است.

واقعه‌نگاری(logging)

واقعه‌نگاری به ثبت اعمال یا تراکنش‌های انجام‌شده توسط کاربر یا یک برنامه، تولید سابقه و ثبت نظام‌مند رویدادهای مشخص به ترتیب وقوع آنها برای فراهم کردن امکان تعقیب و پیگیری داده‌ها در تحلیل‌های آتی گفته می‌شود. واقعه‌نگاری، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا به علت‌جویی رویدادهای امنیتی پس از وقوع می‌پردازد. این فناوری در سطوح برنامهٔ کاربردی، میزبان و شبکه قابل پیاده‌سازی است.

دسترسی از راه دور (remote accessing)

دسترسی از راه دور به دسترسی به یک سامانه یا برنامه، بدون نیاز به حضور فیزیکی در محل توجه دارد. با این حال به گونهٔ معمول دسترسی به خدمات از راه دور، کنترل‌شده نیستند، زیرا ممکن است دسترسی به یک خدمت از راه دور به گونهٔ ناشناس انجام بگیرد که در این مورد دسترسی به خدمت، خطر جعل هویت را به همراه دارد. در این زمینه با توجه به شرایط و امکانات، باید ایمن‌ترین پروتکل‌ها و فناوری‌ها را به خدمت گرفت. برای نمونه شماری از نظام‌ها ممکن است به غلط برای مجوز گرفتن

اتصال، به صورت ناشناس با یک پیش‌فرض پیکربندی کنند، در حالی که اتصال ناشناس بر طبق خط‌مشی امنیتی سازمان نباید اجازه یابد که وارد نظام شود. دسترسی از راه دور، فناوری امنیت اطلاعات از نوع واکنشی است، زیرا یک فرد یا فرایند برای اتصال از راه دور، توانا به دستیابی بر طبق امتیازهای دسترسی است. این فناوری در سطح میزبان قابل پیاده‌سازی است.

۹ـ۷ ضرورت توجه به امنیت اطلاعات

استراتژی «دفاع در عمق» یک چارچوب امنیتی مناسب برای حفاظت و نگهداری ایمن زیرساخت فناوری اطلاعات یک سازمان است. در این مدل، زیرساخت فناوری اطلاعات یک سازمان به عنوان مجموعه‌ای از لایه‌های مرتبط به هم در نظر گرفته شده و به منظور حفاظت و ایمن‌سازی هر لایه از سازوکارها و روش‌های حفاظتی ویژه‌ای استفاده می‌شود.

۹ـ۷ـ۱ بررسی لایه سیاست‌ها، رویه‌ها و اطلاع رسانی

در نخستین لایهٔ مدل امنیتی «دفاع در عمق»، سیاست‌ها و رویه‌های امنیتی تعریف و همهٔ کاربران صرف‌نظر از موقعیت شغلی خود باید با آنان آشنا شوند. با توجه به جایگاه برجسته این لایه و تأثیر آن بر عملکرد دیگر لایه‌ها، باید با حوصله و دقت بیشتری این لایه بررسی و پیش از هر چیز سیاست‌های امنیتی در یک سازمان تعریف شود. در زمان تعریف سیاست‌های امنیتی باید به موارد زیر توجه کرد:

- تعریف عنصرهای زیادی مانند: استفاده پذیرفتنی از منابع موجود، دستیابی از راه دور، حفاظت اطلاعات، تهیه نسخه‌های پشتیبان از اطلاعات، امنیت پیرامون شبکه، ایمن‌سازی و ایمن نگهداشتن دستگاه‌ها و رایانه‌های میزبان و...
- یک سیاست امنیتی مناسب باید قادر به برقراری ارتباط مناسب با کاربران بوده و با ارائهٔ یک ساختار اساسی آنان را در زمان بروز یک رویداد و یا دشواری امنیتی کمک کند.
- تدوین رویه‌های مناسب به منظور برخورد با یک دشواری امنیتی. در این رویه‌ها باید محدودهٔ مسئولیت‌ها به دقت مشخص شود.
- تعیین دقیق نوع و مکان ذخیره‌سازی اطلاعات مهمی که برای یک سازمان ارزش زیستی دارند.

- مشخص کردن اقدام‌هایی که باید پس از بروز یک دشواری امنیتی انجام شود.
- سیاست‌های امنیتی به عنوان اصول فرایندی رویه‌های امنیتی مطرح هستند. بنابراین، باید به اندازهٔ کافی عمومی باشند تا بتوان آنان را با استفاده از فناوری‌ها و پلت فرم‌های موجود پیاده‌سازی کرد.
- سیاست‌های امنیتی باید اطلاعات لازم برای کارشناسان حرفه‌ای فناوری اطلاعات در خصوص شیوهٔ پیاده‌سازی کنترل‌های امنیتی به منظور پشتیبانی از سیاست‌های امنیتی را ارائه کنند.
- محدودهٔ سیاست‌های امنیتی برای یک سازمان، به اندازه و پیچیدگی‌های آن بستگی دارد.
- رویه‌های امنیتی شیوهٔ انجام فرایندی ویژه بر روی دستگاه‌هائی بخصوص مانند شیوهٔ پیکربندی یک سرویس‌دهندهٔ وب جدید را مشخص می‌کنند.
- اطلاع‌رسانی یک عنصر امنیتی است که بیشتر به فراموشی سپرده می‌شود. بیشتر کاربران فعالیت‌های روزمره خود را با نادیده گرفتن مسائل امنیتی انجام می‌دهند. بدون وجود آموزش‌های لازم، بیشتر کارکنان در ابتدا می‌کوشند کار خود را به گونه‌ای که آسان‌تر است، انجام دهند و در مرحلهٔ بعد به امنیت انجام کار فکر کنند. تدوین سیاست‌ها و رویه‌های امنتیی بدون اینکه کاربران نسبت به آنان آگاهی داشته باشند، نتیجه‌های مثبت و مشهودی را در زمینهٔ ایجاد یک سامانهٔ ایمن به دنبال نخواهد داشت.

۹ـ۷ـ۲ تهدیدهای لایهٔ سیاست‌ها، رویه‌ها و اطلاع‌رسانی

- بسیاری از کاربران قوانین امنیتی را به عنوان یک ضرورت در نظر نگرفته و از آنان تبعیت نمی‌کنند. این گونه کاربران متأسفانه نسبت به مسائل امنیتی شناخت مناسبی نداشته و از تبعات زیان‌بار آن آگاهی ندارند. بدیهی است زمانی که کاربران از اهمیت امنیت اطلاعات شناخت مناسبی نداشته باشند، نمی‌توانند از رمزهای گذر خود، حفاظت کرده و یا از اطلاعات سازمان خود محافظت کنند (مانند پیکربندی سخت‌افزارها و یا نرم‌افزارها با رعایت مسئله‌های امنیتی).

تعداد زیادی از حمله‌ها مبتنی بر «مهندسی اجتماعی» است. این نوع حمله‌ها از مزایای ضعف امنیت و رعایت نکردن نکات ایمنی در زندگی روزمره ما استفاده

می‌کنند. یک مهاجم می‌تواند زمان زیادی را در محل کار و یا زمان‌های فراغت خود صرف کند تا بتواند اعتماد یک کاربر را جلب کند. زمانی که یک مهاجم پرسش‌هایی را مطرح و پاسخ آنان را دریافت می‌کند، با قرار دادن اطلاعات بالا در کنار یکدیگر و تجزیه آنان می‌تواند به اطلاعات اررشمندی دست یابد که از آنان به منظور برنامه‌ریزی حمله‌ها استفاده کند.

دو نمونه از حمله‌های مبتنی بر مهندسی اجتماعی

یک مهاجم با مسئول فنی یک مرکز ارائه‌دهندهٔ خدمات اینترنت (ISP) تماس می‌گیرد و در مدت زمان مکالمه تلفنی با وی به این نکته اشاره می‌کند که دارای یک خودرو است که قصد دارد آن را با بهای مناسبی بفروشد. مسئول فنی ISP برای خرید خودرو اظهار تمایل می‌کند. مهاجم به وی پیشنهاد می‌کند که یک mail را که دارای تصویر خودرو است برای وی ارسال خواهد کرد. مهاجم، در برابر ارسال تصویر خودرو (به عنوان یک فایل پیوست) یک برنامه مخرب از نوع backdoor را به همراه email برای مسئول فنی ISP ارسال می‌کند. زمانی که مسئول فنی ISP نامه را دریافت و فایل پیوست را فعال می‌کند، برنامه مخرب ارسالی اجرا و یک حفرهٔ امنیتی را در بطن شبکه ISP ایجاد می‌کند.

یک مهاجم می‌تواند نام‌های مهم کارکنان یک سازمان را از راه تماس با آن واحد به دست آورد. در ادامه وی طی تماس با محل کار و یا منزل و شنیدن پیام دستگاه پیام‌گیر آنان از این موضوع آگاه می‌شود که کدام مدیر در خارج از شهر است. در ادامه، مهاجم با مراجعه به آن سازمان وانمود می‌کند که کلید خود را جا گذاشته است تا بتواند وارد ساختمان شود. پس از ورود مهاجم (که ممکن است از کارکنان همان سازمان باشد) به ساختمان اصلی سازمان مورد نظر، وی وارد دفتر کار کارکنانی می‌شود که در خارج از شهر هستند و بدون نگرانی رایانه وی را بررسی و با به‌کارگیری انواع نرم‌افزارهای موجود تلاش می‌کند که به اطلاعات موجود بر روی رایانه دست پیدا کند.

۹ـ۷ـ۳ حفاظت لایهٔ سیاست‌ها، رویه‌ها و اطلاع رسانی

- برای مقابله با انواع تهدیدها، باید سیاست‌ها و رویه‌های امنیتی به صورت روشن تدوین، پیاده‌سازی و توسط همهٔ کارکنان به کار گرفته شوند. هر فرایند و یا فرایندی که در خصوص سیاست‌های امنیتی تعریف می‌شود، باید دارای دستور کارهای مستند و روشنی باشد.

- کارکنان سازمان باید دربارهٔ سیاست‌ها و رویه‌های امنیتی آموزش ببینند. آموزش امنیت یک امر ضروری است تا این اطمینان به دست آید که کاربران در مورد کارهائی که باید در راستای تأمین سیاست‌ها و رویه‌های امنیتی انجام دهند، توجیه و آنان را رعایت می‌کنند. شیوهٔ آموزش باید به گونه‌ای باشد که تصویری واقعی از جایگاه و اهمیت امنیت اطلاعات را برای کاربران تشریح تا آنان نیاز به امنیت را همواره و در همهٔ سطوح احساس و به آن پایبند باشند.
- یک سیاست امنیتی ترکیبی از خواسته‌ها و فرهنگ یک سازمان است که متأثر از اندازه و اهداف یک سازمان است. برخی سیاست‌ها ممکن است به همهٔ سایت‌ها اِعمال شود و برخی دیگر ممکن است در محیط‌هائی ویژه به‌کار آید. یک سیاست امنیتی باید سطح کنترل را با سطح بهره‌وری بالانس کند. در صورتی که یک سیاست امنیتی محدودیت‌های زیادی را برای کاربران در پی داشته باشد، کاربران روش‌های نادیده گرفتن آن را بررسی و برای آن راه‌حل‌های ویژهٔ خود را پیدا خواهند کرد.
- اطلاع‌رسانی در خصوص مسئله‌های امنیتی باید ترویج و در دستور کار قرار گیرد. برای نمونه می‌توان از پوسترهای امنیتی و کارت‌های checklist برای اطلاع‌رسانی استفاده کرد. پوسترها و کارت‌های checklist دارای کارایی به مراتب بهتری نسبت به مستندات حجیم سیاست‌های امنیتی هستند که ممکن است برای استفادهٔ عموم بر روی شبکه اینترانت سازمان منتشر شده باشد. پوسترها و کارت‌های checklist را باید در مکانی نصب کرد که در معرض دید بیشتری باشند.

به منظور بررسی وضعیت برخی سیاست‌های امنیتی مانند رمزهای گذر و پیکربندی امنیتی، می‌توان از ابزارهائی مانند Microsoft Baseline Security استفاده کرد.

۹ـ۸ بررسی انواع ویروس‌ها و آسیب‌پذیری‌ها و تهدیدهای امنیتی که رایانه را مورد حمله قرار می‌دهند

ویروس‌ها

ویروس‌های رایانه‌ای، متداول‌ترین نوع تهدیدهای امنیتی در سالیان اخیر بوده که تاکنون دشواری‌های گسترده‌ای را ایجاد و همواره از خبرسازترین موضوع‌ها در زمینهٔ رایانه و شبکه‌های رایانه‌ای، بوده‌اند. ویروس‌ها، برنامه‌هائی رایانه‌ای هستند که برنامه‌نویسان

گمراه و در عین حال ماهر می‌نویسند و به گونه‌ای طراحی می‌شوند که توانا به تکثیر خود و آلودگی رایانه‌ها بر اثر وقوع یک رویداد ویژه، باشند. برای نمونه ویروس‌هایی که از آنان با نام «ماکرو ویروس» یاد می‌شود، خود را به فایل‌هایی شامل دستور کارهای ماکرو ملحق کرده و در ادامه، هم‌زمان با فعال شدن ماکرو، شرایط لازم به منظور اجرای آنان نیز فراهم می‌شود. برخی از ویروس‌ها بی‌آزار بوده و تنها سبب بروز اختلالات موقت در روند انجام فرایند در رایانه می‌شوند (مانند نمایش یک پیام مضحک بر روی صفحه نمایشگر هم‌زمان با فشردن یک کلید ویژه). برخی دیگر از ویروس‌ها دارای عملکردی مخرب‌تر بوده و می‌توانند مسئله‌ها و دشواری‌های بیشتری مانند حذف فایل‌ها و یا کاهش سرعت سامانه را به دنبال داشته باشند. یک رایانه تنها زمانی آلوده به یک ویروس می‌شود که شرایط و امکان ورود ویروس از یک منبع خارجی (بیشتر از راه فایل پیوست یک نامه الکترونیک و یا دریافت و نصب یک فایل و یا برنامهٔ آلوده از اینترنت)، برای آن فراهم شود. زمانی که یک رایانه در شبکه‌ای آلوده شد، دیگر رایانه‌های موجود در شبکه و یا دیگر رایانه‌های موجود در اینترنت، دارای استعدادی مناسب به منظور مشارکت و همکاری با ویروس، خواهند بود.

برنامه‌های اسب تروا (دشمنانی در لباس دوست)

برنامه‌های اسب تروا و یا Trojans، به منزلهٔ ابزارهایی برای پخش کدهای مخرب هستند. تروجان‌ها، می‌توانند بی‌آزار بوده و یا حتی نرم‌افزاری سودمندی مانند بازی‌های رایانه‌ای باشند که با تغییر قیافه و با لباسی مبدل و ظاهری سودمند خود را عرضه می‌کنند. تروجان‌ها، توانا به انجام فرایند متفاوتی مانند حذف فایل‌ها، ارسال یک نسخه از خود به سیاهه (لیست) نشانی‌های پست الکترونیک، هستند. این نوع از برنامه‌ها تنها می‌توانند از راه تکثیر برنامه‌های اسب تروا به یک رایانه، دریافت فایل از راه اینترنت و یا باز کردن یک فایل پیوست همراه یک نامه الکترونیک، اقدام به آلودگی یک سامانه کنند.

ویرانگران، بدافزار (Malware)

در وب سایت‌های پرشماری از نرم‌افزارهائی مانند اکتیوایکس‌ها و یا اپلت‌های جاوا استفاده می‌شود. این نوع برنامه‌ها به منظور ساخت انیمیشن و دیگر افکت‌های ویژه استفاده می‌شود و گیرایی و میزان تعامل با کاربر را افزایش می‌دهند. با توجه به دریافت و نصب آسان این نوع از برنامه‌ها، برنامه‌های بالا به ابزاری مطئمن و آسان به منظور

آسیب‌رسانی به دیگر سامانه‌ها بدل شده‌اند. این نوع برنامه‌ها که به «ویرانگران» شهرت یافته‌اند، به شکل یک برنامهٔ نرم‌افزاری و یا اپلت ارائه و در دسترس استفاده‌کنندگان قرار می‌گیرند. برنامه‌های بالا، توانا به ایجاد دشواری‌های پرشماری برای کاربران هستند (از بروز اشکال در یک فایل تا ایجاد اشکال در بخش اصلی یک سامانهٔ رایانه‌ای).

حمله‌ها

تاکنون حمله‌های پرشماری متوجه شبکه‌های رایانهٔ بوده که می‌توان همهٔ آنان را به سه گروه عمده تقسیم کرد:

- **حمله‌های شناسائی:** در این نوع حمله‌ها، مهاجمان اقدام به گردآوری و شناسائی اطلاعات با هدف تخریب و آسیب رساندن به آنان می‌کنند. مهاجمان در این رابطه از نرم‌افزارهای ویژه‌ای مانند Sniffer و یا Scanner به منظور شناسائی نقاط ضعف و آسیب‌پذیر رایانه‌ها، سرویس‌دهندگان وب و برنامه‌ها، استفاده می‌کنند. در این رابطه برخی تولیدکنندگان، نرم‌افزارهایی را با هدف‌های خیرخواهانه طراحی و پیاده‌سازی کرده‌اند که متأسفانه از آنان در جهت اهداف مخرب نیز استفاده می‌شود. برای نمونه به منظور تشخیص و شناسائی رمزهای گذر، نرم‌افزارهای پرشماری تاکنون طراحی و پیاده‌سازی شده است. نرم‌افزارهای بالا با هدف کمک به مدیران شبکه، افراد و کاربرانی که رمز گذر خود را فراموش کرده و یا آگاهی از رمز گذر افرادی که سازمان خود را بدون اعلام رمز گذر به مدیر شبکه، ترک کرده‌اند، استفاده می‌گردند. به هر حال وجود این نوع نرم‌افزارها واقعیتی انکارناپذیر بوده که می‌تواند به منزلهٔ یک سلاح مخرب در اختیار مهاجمان قرار گیرد.
- **حمله‌های دستیابی:** در این نوع حمله‌ها، هدف اصلی مهاجمان، نفوذ در شبکه و دستیابی به نشانی‌های پست الکترونیک، اطلاعات ذخیره‌شده در بانک‌های اطلاعاتی و دیگر اطلاعات حساس، است.
- **حمله‌های از کار انداختن سرویس‌ها:** در این نوع حمله‌ها، مهاجمان سعی در ایجاد مزاحمت به منظور دستیابی به همه و یا بخشی از امکانات موجود در شبکه برای کاربران مجاز می‌کنند. حمله‌های بالا به اشکال متفاوت و با بهره‌گیری از فناوری‌های پرشماری صورت می‌پذیرد. ارسال حجم بالایی از داده‌های غیرواقعی برای یک ماشین متصل به اینترنت و ایجاد ترافیک کاذب در شبکه، نمونه‌هایی از این نوع حمله‌ها هستند.

رهگیری داده (استراق سمع)

بر روی هر شبکه رایانهٔ روزانه اطلاعات متفاوتی جابه‌جا می‌شود و همین امر می‌تواند موضوعی مورد علاقه برای مهاجمان باشد. در این نوع حمله‌ها، مهاجمان اقدام به استراق سمع و یا حتی تغییر بسته‌های اطلاعاتی در شبکه می‌کنند. مهاجمان به منظور رسیدن به اهداف مخرب خود از روش‌های پرشماری به منظور شنود اطلاعات، استفاده می‌کنند.

کلاهبرداری (ابتدا جلب اعتماد و سپس تهاجم)

کلاهبرداران از روش‌های پرشماری به منظور اعمال شیادی خود استفاده می‌کنند. با گسترش اینترنت این نوع افراد فضای مناسبی برای اعمال مخرب خود یافته‌اند (چراکه می‌توان به هزاران نفر در زمانی کوتاه و از راه اینترنت دستیابی داشت). در برخی موردها شیادان با ارسال نامه‌های الکترونیک وسوسه‌انگیز از خوانندگان می‌خواهند که اطلاعاتی ویژه را برای آنان ارسال کرده و یا از یک سایت به عنوان طعمه در این رابطه استفاده می‌کنند. به منظور پیشگیری از این گونه اعمال، می‌بایست کاربران دقت لازم در خصوص درج نام، رمز گذر و دیگر اطلاعات شخصی در سایت‌هایی که نسبت به هویت آنان شک و دو دلی وجود دارد را داشته باشند. با توجه به سهولت جعل نشانی‌های پست الکترونیک؛ باید به این نکته توجه شود که پیش از ارسال اطلاعات شخصی برای هر فرد، هویت وی شناسایی شود. هرگز بر روی لینک‌ها و یا ضمائمی که از راه یک نامه الکترونیک برای شما ارسال شده است، کلیک نکرده و همواره باید به شرکت‌ها و مؤسسه‌هایی که به گونه‌ای شفاف نشانی فیزیکی و شماره تلفن‌های خود را یاد نمی‌کنند، شک و تردید داشت.

نامه‌های الکترونیک ناخواسته

از واژهٔ Spam در ارتباط با نامه‌های الکترونیک ناخواسته و یا پیام‌های تبلیغاتی ناخواسته، استفاده می‌شود. این نوع از نامه‌های الکترونیک، همگی بی‌ضرر بوده و تنها ممکن است مزاحمت و یا دردسر ما را بیشتر کنند. دامنه این نوع مزاحمت‌ها می‌تواند از به هدر رفتن زمان کاربر تا هرز رفتن فضای ذخیره‌سازی بر روی رایانه‌های کاربران را شامل می‌شود.

تهدیدها

زمانی که شما به عنوان مسئول و کارشناس امنیت اطلاعات یک شرکت یا سازمان به شمار می‌آیید، در واقع شما مسئول حفاظت از دارایی‌های اطلاعاتی یک سازمان در برابر کسانی یا چیزهایی هستید که می‌خواهند از آن دارایی‌ها سوءاستفاده کنند. ممکن است برخی از این افراد هم اکنون در سازمان و در کنار خود شما باشند، اما بیشتر این افراد در خارج از سازمان قرار دارند و همیشه قصد نفوذ به شبکه و سازمان را دارند. این جمله طلایی را همیشه به خطر بسپارید: **هیچ چیز برای یک مسئول یا کارشناس امنیت اطلاعات خطرناک‌تر و هولناک‌تر از کاربران خود آن شبکه نیست.**

متأسفانه این عمل چندان هم آسان نیست، در حال حاضر نقاط ضعف و آسیب‌پذیری‌های سامانه‌های تجاری در حال رشد است و این نقاط روز به روز بیشتر و بیشتر می‌شود، حال کافی است شما تنها یک روز از این اطلاعات بی‌خبر باشید و همین کافی است تا به شبکه و سازمان شما نفوذ شود. برای نمونه اگر از ویندوز نسخه اصلی یا اورجینال استفاده کرده باشید و به اینترنت متصل بشوید می‌بینید که همواره در حال به‌روزرسانی خود است به‌گونه‌ای که همه روزه بسته‌های امنیتی خود را بروز می‌کند و بر روی سامانهٔ شما نصب می‌کند، این یعنی اینکه همه روزه حمله‌های گسترده‌ای در سطح جهان به سامانه‌ها انجام می‌شود که سبب ایجاد نقاط ضعف در سامانه‌ها می‌شود و برای جلوگیری از نفوذ از راه این نقاط، بسته‌های امنیتی برای آنها ساخته و عرضه می‌شود.

دشمنان شما می‌توانند به‌آسانی با استفاده از موتورهای جستجو، نقاط ضعف و آسیب‌پذیر هر فرآورده یا سیستم‌عامل را بیابند، آنان برای اینکه بتوانند به شبکه شما وارد شوند و از نقاط ضعف شما بهره‌برداری کنند، می‌توانند کتاب‌های آموزش هک بخرند، به عضویت گروه‌های خبری امنیتی و هک در اینترنت در بیایند و یا به وب سایت‌هایی دسترسی پیدا کنند که در آنها اطلاعات روشن و با جزئیاتی در خصوص شبکه شما وجود دارد.

در بسیاری از موردها شما نرم‌افزاری را خریداری می‌کنید که خود آن نرم‌افزار به صورت ذاتی دارای نقاط ضعف امنیتی است و این نقاط ضعف امنیتی به خودی خود سبب به زیر پرسش رفتن امنیت سازمان شما خواهد شد، برای نمونه نرم‌افزار مجموعه

آفیس را خریداری می‌کنید و در آن نقاط ضعف امنیتی وجود دارد که هکرها می‌توانند از راه آن به سیستم‌عامل حمله و به آن دسترسی یابند.

متأسفانه در کشور عزیز ما ایران به دلیل عدم وجود قانون کپی رایت نرم‌افزارهایی که توسط برنامه‌نویس‌ها نوشته می‌شود زیر نظر هیچ سازمان مرکزی ویژه‌ای قرار ندارند، تا مشکلات احتمالی آنها را بررسی و به آنها رسیدگی کند. البته بخشی در مرکز پژوهش‌های صنایع انفورماتیک ایران برای آزمایش برخی نرم افزارهای ویژه ایجاد شده است اما به هیچ عنوان پاسخ‌گوی این سطح حجیم از نرم افزارهای تولیدی در درون کشور را ندارد، بنابراین اعتماد کردن به این گونه نرم افزارها بسیار سخت است.

۹ـ۹ شماری از راهکارهای عملی امنیت اطلاعات

۹ـ۹ـ۱ فشرده‌سازی و رمزگذاری روی فایل‌ها (بدون استفاده از نرم‌افزار ویژه)

شاید برای شما این پرسش پیش آمده باشد که چرا سایت‌ها، فایل‌های خودشان در فرمت Zip برای بارگیری (دانلود) قرار می‌دهند؟ خوب پاسخ به این سؤال زیاد سخت نیست. یکی از دلایلش کمبود حجم سایت و شاید راحت‌تر بگوییم، هزینه سنگین فضا (حجم اطلاعات بر روی سرور) برای یک وب سایت است. وب سایت‌ها دسترسی به یک فضا مانند فضای هارد دیسک برایشان مقدور نیست؛ به‌دلیل اینکه باید هزینه زیادی برای داشتن چنین قابلیتی صرف کرد که عاقلانه نیست. به همین دلیل تا جایی که امکان دارد صاحبان وب‌سایت‌ها تا می‌توانند، می‌کوشند حجم اطلاعات خودشان را بر روی وب سرور برای دانلود، تا حد قابل ملاحظه‌ای پایین بیاورند.

نرم‌افزار Winrar یکی از برنامه‌هایی است که وظیفه کم کردن حجم اطلاعات بدون افت کیفیت را بر عهده دارد. دقت داشته باشید که این نرم‌افزار در خود ویندوز هم به صورت پیش فرض وجود دارد و نیاز به نصب نرم‌افزار جانبی نیست، اما نرم‌افزاری که در خود ویندوز وجود دارد، دارای امکانات محدود و کیفیت کمتری است که کاربران بیشتر تمایل دارند از نرم‌افزار جانبی استفاده کنند تا از خود ویندوز.

۹ـ۹ـ۲ روش تهیه نسخه پشتیبان و بازیابی اطلاعات (Backup And Restore)

فایل‌های مهم سیستم عامل و داده‌های شما روی درایوهای دیسک سخت همیشه در معرض آسیب‌های پیش‌بینی نشده و آسیب حذف ناگهانی هستند. به منظور جلوگیری

از حذف اطلاعات مهم در رایانه خود، سیستم عامل ویندوز برنامه‌های سودمند Restore و Backup را در اختیار کاربران خود قرار داده است.

الف) تهیهٔ نسخهٔ پشتیبان (Backup) از اطلاعات

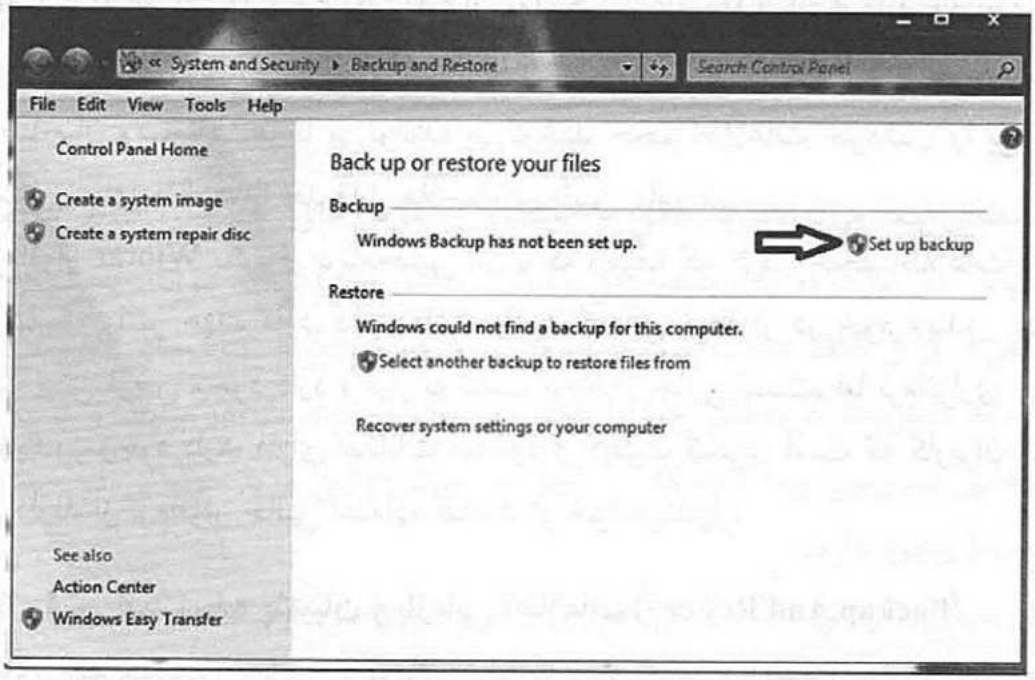
با استفاده از برنامهٔ Backup می‌توانید از پرونده‌ها و پوشه‌های خود، نسخه پشتیبان تهیه کنید. افزون بر این می‌توانید از تنظیم‌های سیستم‌عامل و محتویات رجیستری هم پشتیبان تهیه کنید تا در صورت بروز دشواری در عملکرد سیستم‌عامل، این تنظیم‌ها را به حالت اول برگردانید.

برای آغاز فرایند تهیهٔ نسخهٔ پشتیبان یکی از سه روش زیر را به کار بگیرید:

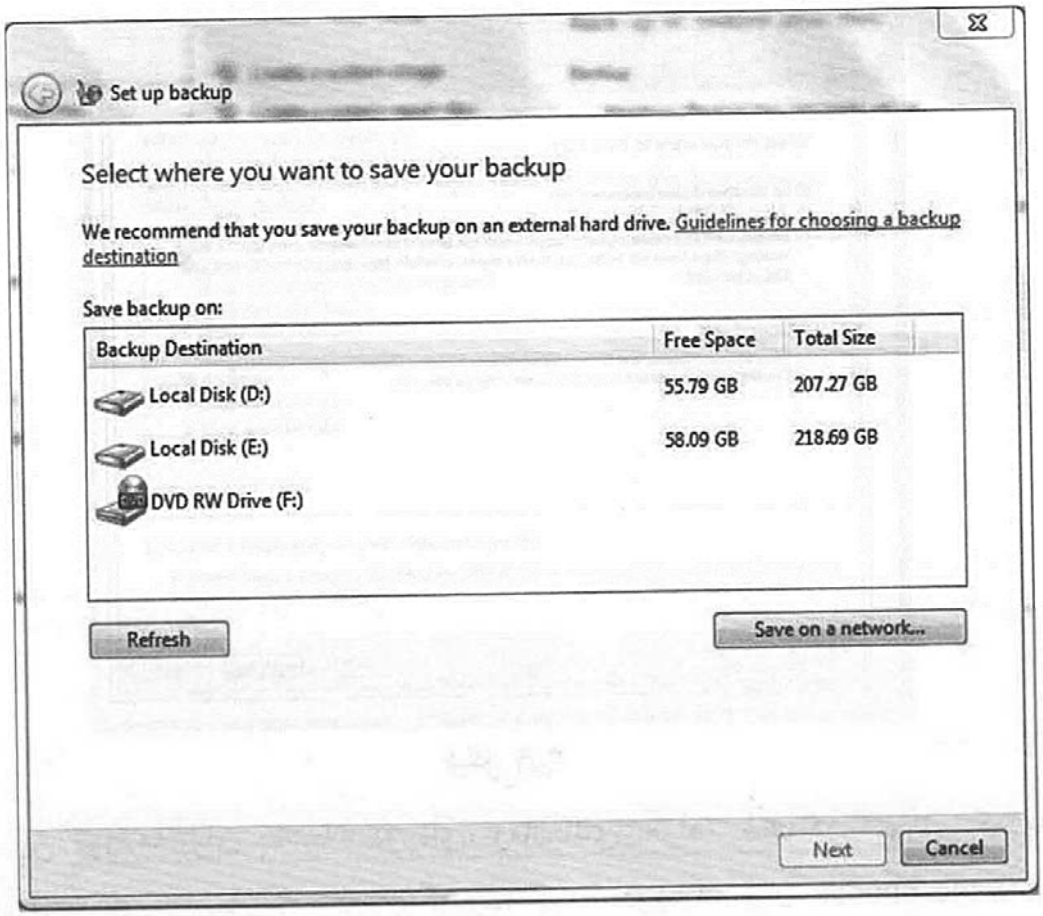
۱. در منوی Start، عبارت Backup را در کادر جستجو و اجرا تایپ کنید و کلید Enter را فشار دهید.

۲. پنجرهٔ Control Panel سیستم‌عامل ویندوز را باز کنید و گزینه‌های آن را با نمایهٔ Small Icon ببینید. سپس روی گزینه Backup and Restore کلیک کنید.

۳. در My computer سیستم‌عامل ویندوز، روی نشانهٔ درایو: C کلیک راست و از منوی میانبر، گزینهٔ Properties را برگزینید. در زبانه Tools روی دکمه ... Backup now کلیک کنید. اکنون برنامه تهیه پشتیبان آشکار می‌شود (شکل ۹ـ۱).



شکل ۹ـ۱

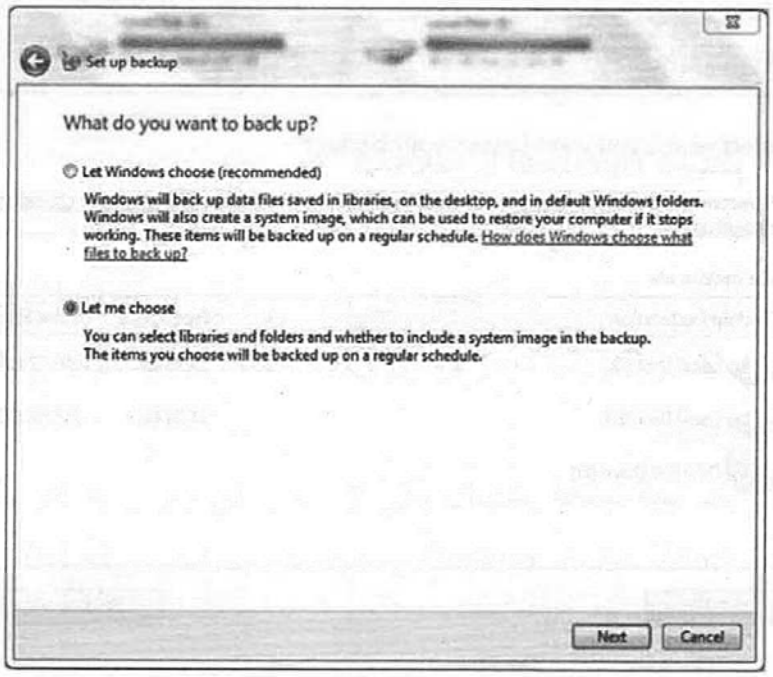


شکل ۹ـ۲

در صورتی که تاکنون از این برنامه استفاده نکرده‌اید، روی عبارت Set up backup کلیک کنید. برنامه ویزارد تهیه نسخه پشتیبان آغاز می‌شود. در مرحلهٔ بعد کادری مانند شکل زیر آشکار می‌شود. در این کادر باید مقصد نگهداری نسخه پشتیبان را معین کنید. توصیه می‌شود که پرونده پشتیبان را روی حافظه جانبی غیر از دیسک سخت (مانند حافظه فلش) ذخیره کنید. با این حال مقصد را می‌توانید از سیاهه (لیست) نشان داده شده، از درایوهای دیسک سخت سامانه نیز برگزینید. در صورت اتصال به شبکه، می‌توانید نسخهٔ پشتیبان را در رایانهٔ دیگر عضو شبکه ذخیره کنید. (شکل ۹ـ۲)

پس از انتخاب درایو مورد نظر، روی دکمهٔ Next کلیک کنید تا کادر what do you want to back up? آشکار شود.

در این مرحله کادری با محتوای شکل زیر آشکار می‌شود. با انتخاب گزینهٔ اول، به سیستم عامل ویندوز اجازه می‌دهید که از پرونده‌ها و پوشه‌های پیش فرض، مانند موردهای موجود در میزکار، پشتیبان تهیه کند و یک دیسک تصویر (Image) به وجود



شکل ۹ـ۳

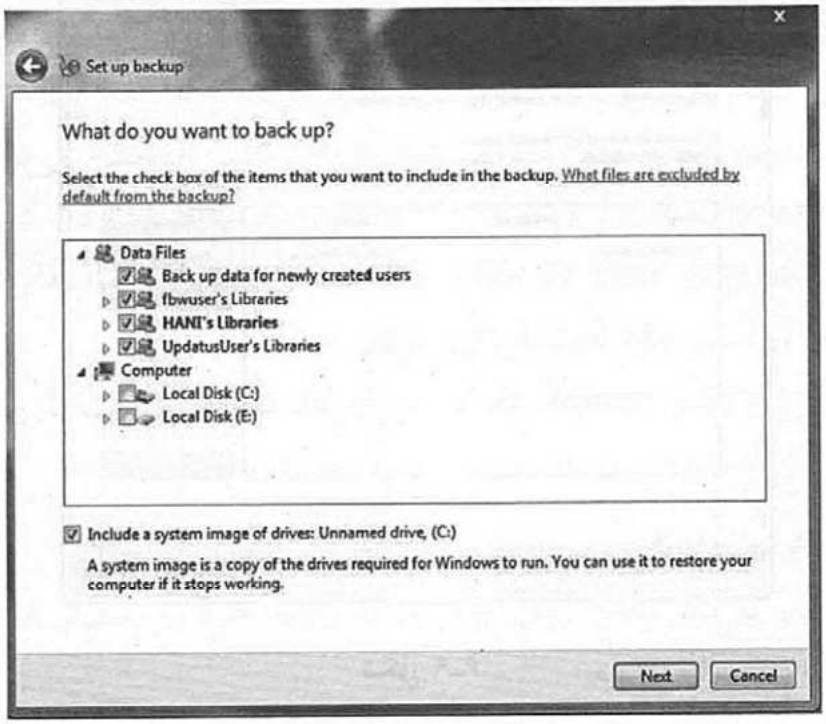
آورد. این موردها برای پشتیبان دوره‌ای، زمان‌بندی خواهد شد. در صورتی که مایل هستید موردهای پشتیبان را خود برگزینید، گزینهٔ دوم با عنوان Let me choose را انتخاب و روی دکمهٔ Next کلیک کنید. (شکل ۹ـ۳)

در این مرحله کادری مانند شکل زیر آشکار می‌شود و شما می‌توانید پوشه‌ها و پرونده‌های مورد نظر برای تهیه پشتیبان را برگزینید. پس از انتخاب روی دکمهٔ Next کلیک کنید. در مرحلهٔ بعد پیش از تهیهٔ پشتیبان، باید موردهای انتخابی را تأیید کنید (شکل ۹ـ۴).

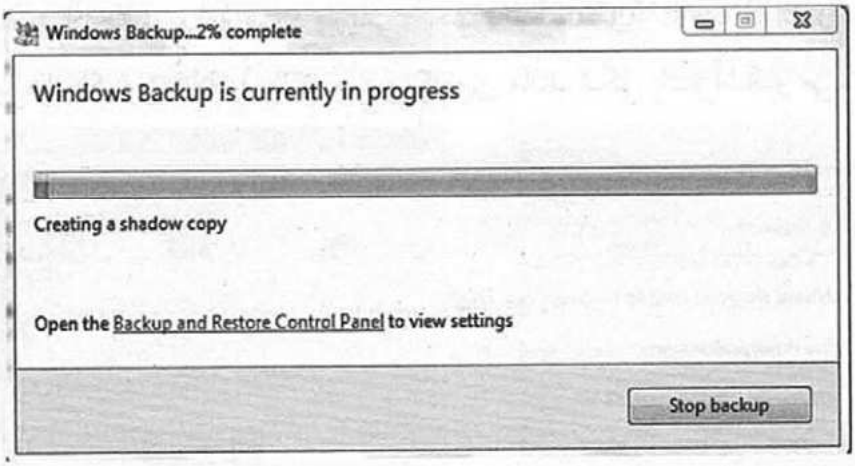
در این مرحله کادری جدید آشکار می‌شود. در این کادر می‌توانید دوره‌های زمانی تهیه پشتیبان را زمان‌بندی کنید. با انتخاب روز، ماه و سال روی دکمه OK کلیک کنید تا وارد مرحله بعد شوید.

در مرحله بعد با نمایش کادری فرایند تهیه پشتیبان آغاز می‌شود. برای دیدن جزئیات کپی شدن اطلاعات، روی دکمه View Details کلیک کنید تا پیشرفت کار را ببینید (شکل ۹ـ۵).

در پایان، پرونده پشتیبان در محل مورد نظر ذخیره خواهد شد. برای برگرداندن کافی است روی آن دوبار کلیک کنید.



شکل ۹ـ۴

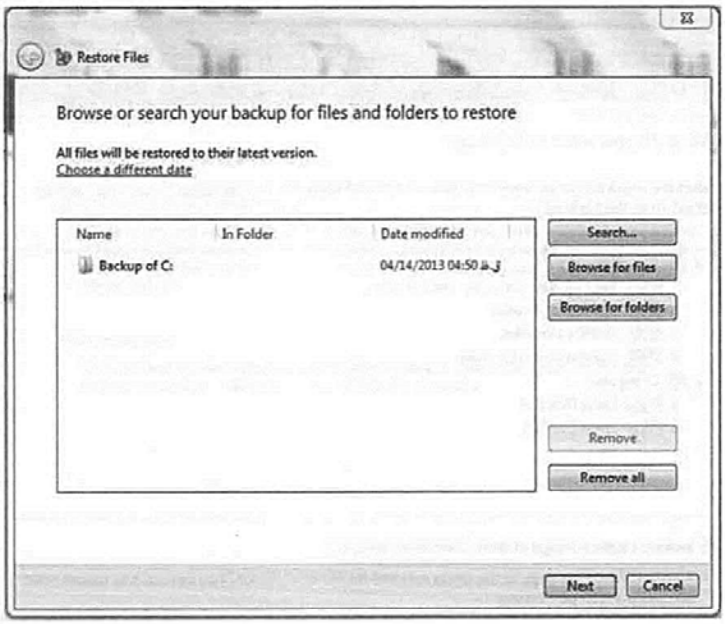


شکل ۹ـ۵

ب) بازیابی (Restore) اطلاعات از نسخهٔ پشتیبان

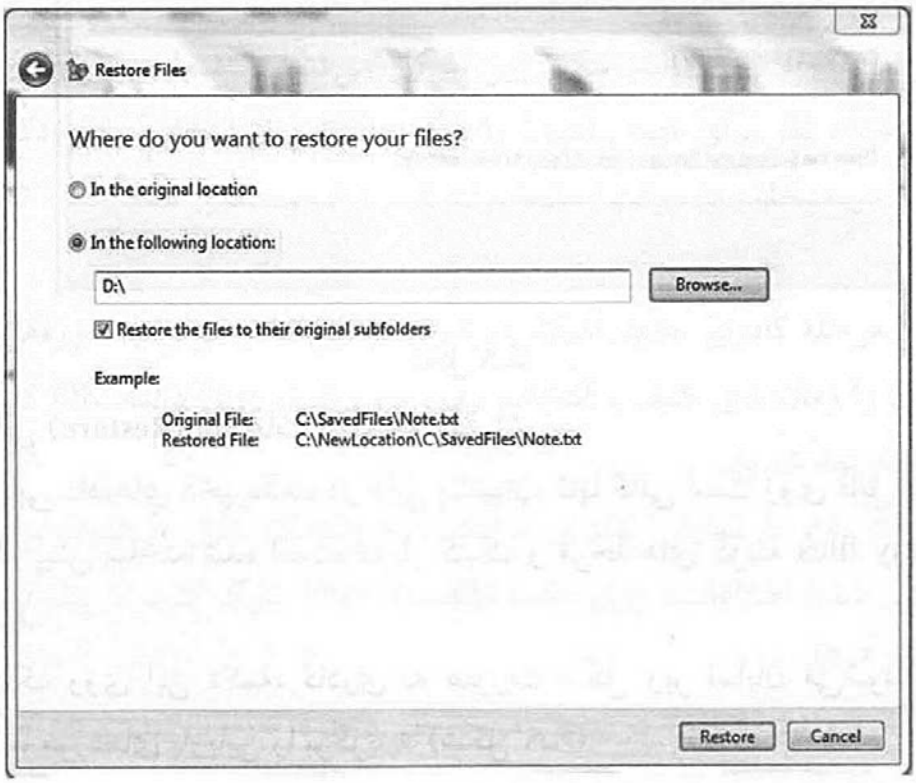
برای بازیابی داده‌های ذخیره‌شده در فایل پشتیبان، تنها کافی است روی فایل پشتیبان که در مرحلهٔ پیش ساخته شده است، دوبار کلیک و مرحله‌های گزینه Restore my files را برگزینید.

با کلیک روی این دکمه، کادری به صورت شکل زیر نمایان می‌شود و از شما می‌خواهد، موردهای بازیابی را برگزینید (شکل ۹ـ۶).



شکل ۹ـ۶

برای انتخاب پرونده‌های مورد نظر برای بازیابی، روی دکمه Browse for files کلیک کنید. به منظور انتخاب پوشهٔ مورد بازیابی، دکمهٔ Browse for folders را برگزینید. پس از انتخاب فایل‌ها، دکمه Next را بزنید. سپس کادری مانند شکل ۹ـ۷ آشکار می‌شود.



شکل ۹ـ۷

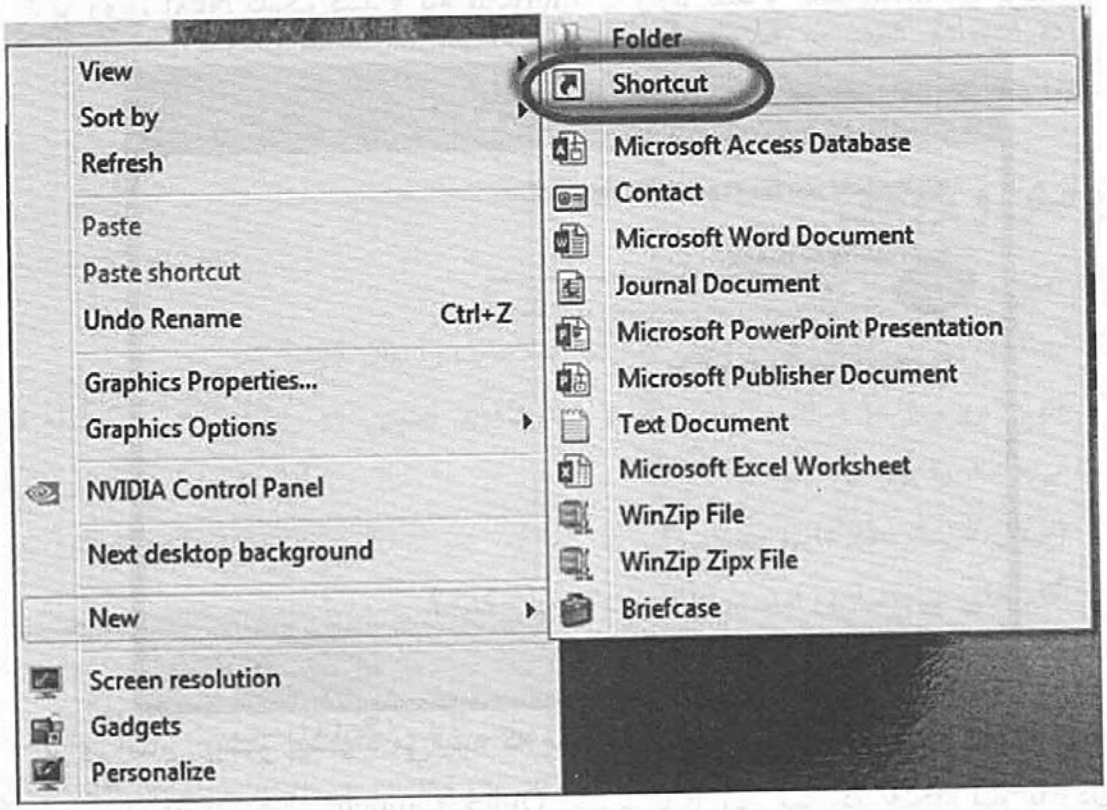
در این کادر با انتخاب In the original location بازیابی پرونده‌ها در محل اصلی پشتیبان‌گیری انجام می‌شود. در صورت انتخاب گزینهٔ In the following location می‌توانید پرونده‌ها را در مسیر مشخص‌شده بازیابی کنید. همچنین می‌توانید با کلیک روی دکمهٔ Browse... مسیر دلخواهی را انتخاب کنید. نشان‌دار بودن گزینهٔ Restore the files to their original subfolders سبب می‌شود پرونده‌های موجود در زیرفهرست‌ها در مسیر اولیه خود بازیابی شوند.

با کلیک روی دکمه Restore کادری باز خواهد شدکه پیشرفت بازیابی را نمایش خواهد داد.

۹ـ۹ـ۳ قفل کردن رایانه

شاید تا به حال به فکر یافتن راهی بوده‌اید که رایانه خود را آسان‌تر از آنچه متداول است در حالت Lock قرار دهید.

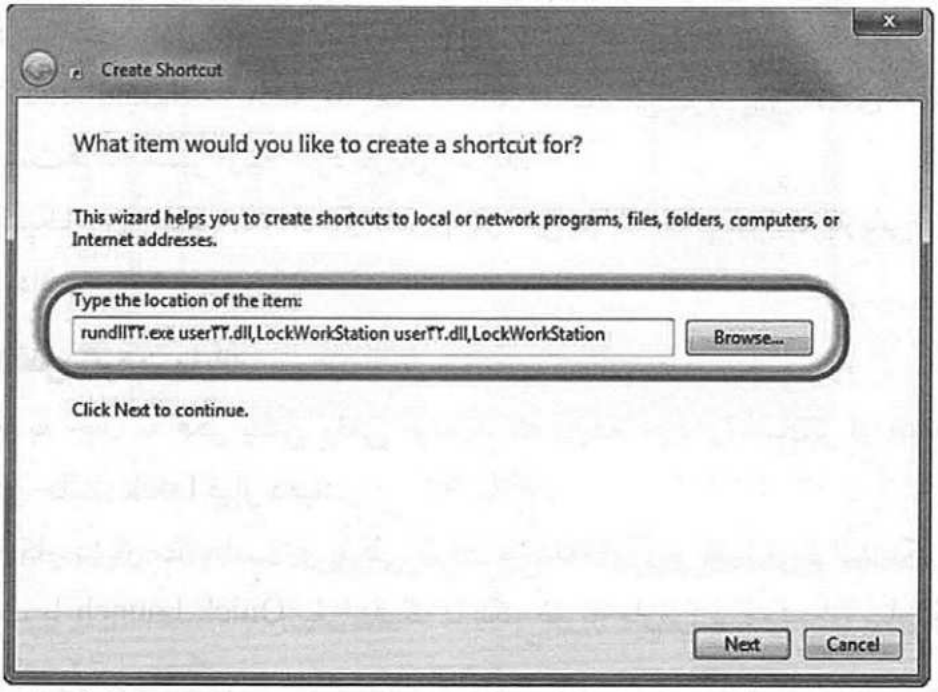
این کار بسیار ساده است و با طی کردن مرحله‌های زیر شما می‌توانید یک Icon به دسکتاپ یا Quick Launch بیفزایید که با یک ضربه ماوس بر روی آن سامانهٔ شما در حالت Lock قرار می‌گیرد.



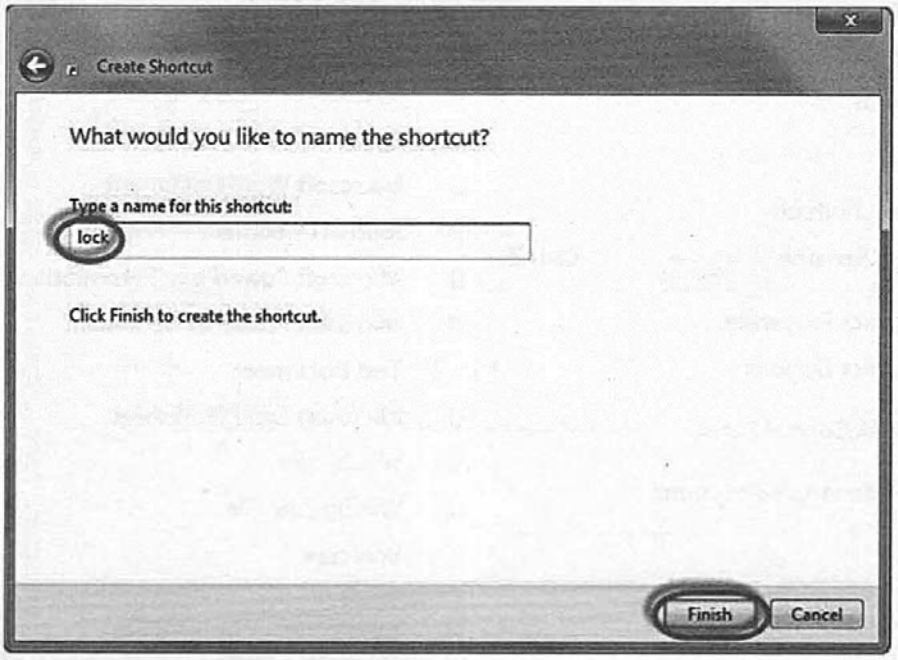
۱. بر روی صفحه نمایش خود Right-Click کنید و از Shortcut، New را برگزینید.

۲. در پنجره‌ای که آشکار شده در بخش Type the location of the item فرمان زیر را بنویسید:

rundll32.exe user32.dll,LockWorkStation user32.dll,LockWorkStation



۳. بر روی Next کلیک کنید و نام Shortcut را وارد کنید و کلید Finish را بزنید.



برای آسانی بیشتر پیشنهاد می‌شود که میانبر (Shortcut) ایجاد شده را با ماوس به یک بخش از فضای خالی Quick Launch بکشید تا از این پس در هنگام نیاز با زدن یک کلید دستگاه شما در حالت Lock قرار گیرد.

۹ـ۱۰ نتیجه‌گیری

اگر چه بیشتر سازمان‌ها تمایل به داشتن شبکه‌های ایمن دارند، ارائه تعریفی واحد از امنیت که همهٔ نیازهای شبکه را تأمین کند ممکن نیست؛ در عوض، هر سازمان باید ارزش اطلاعات خود را ارزیابی کند و سپس یک خط‌مشی امنیتی برای مواردی مشخص کند که باید حفاظت شوند. برای نمونه روش‌های تصدیق هویت زیست‌سنجی از نظر قدرت و در دسترس بودن، در حال بهبود هستند، اما اکنون با نوعی دودلی با آنها برخورد می‌شود و این تردید ناشی از هزینه‌های به نسبت بالا و دشواری‌های مرتبط با دغدغه‌های حفظ حریم خصوصی است. البته نظرهایی وجود دارند که به سبب آنها می‌توان از ترکیب فناوری‌های متنوع امنیتی، برای تشکیل فناوری‌های امنیتی قوی در زمینهٔ امنیت اطلاعات استفاده کرد. برای نمونه، در آینده نزدیک با ترکیب دیوار آتش، نظام‌های آشکارساز نفوذی و فناوری‌های ضد ویروس، به تشکیل یک فناوری نیرومند در زمینهٔ امنیت اطلاعات خواهیم رسید.

برای یک سازمان، شناختن فناوری‌های امنیت اطلاعات قابل دسترس، مهم است، تا از آن برای تدوین خط‌مشی‌های امنیتی با توجه به نوع و حساسیت اطلاعات سازمان خود، استفاده کنند. به علاوه، ارائهٔ این طبقه‌بندی از فناوری‌ها، زمینه‌ساز پژوهش جدیدی خواهد بود.

پرسش و پژوهش

۱. امنیت اطلاعات چیست؟
۲. چند مورد از راهکارهای عملی امنیت اطلاعات را بیان کنید؟
۳. انواع ویروس‌ها و آسیب‌پذیری‌ها و تهدیدهای امنیتی که رایانه را مورد حمله قرار می‌دهند را بررسی کنید
۴. اصول امنیت اطلاعات چیست؟
۵. گام های پیاده‌سازی امنیت اطلاعات را بیان کنید؟
۶. بررسی: باج افزار (Ransomware) چیست؟
۷. بررسی: حمله‌ها از کار انداختن سرویس پخش‌شده (DdoS) چیست؟
۸. بررسی: تفاوت دو پروتکل SSL و TLS چیست؟ سه حمله به پروتکل SSL را نام ببرید؟