# ملاحظاتی پیرامون طراحی تفصیلی سیستمها

«قسمت دوم» [1]

نوشته: دکتر شمس‌السادات زاهدی

مقدمه:

قسمت اول این مقاله را در شمارهٔ گذشته با تعریف سیستمها، نحوهٔ طراحی و ایجاد سیستمهای اطلاعاتی، طراحی خروجی سیستم ، ویژگیهای سیستم اطلاعاتی، لزوم هماهنگی محتوای گزارش با سطح مسئولیت، انواع گزارشها، روش نشان دادن خروجی، طراحی ورودی، فهرست گزینه‌ها، طراحی سیستمهای حساس به زبان محاوره‌ای، طراحی فرایند، طراحی تفصیلی به دوصورت ایستا و پویا، مدلهای تشریح فرایند، استفاده از معادلات در طراحی سیستمها و طراحی پایگاه داده‌ها بنظر خوانندگان گرامی رساندیم ، اینک ادامهٔ بحث را با طراحی سیستمهای کنترلی آغاز می‌نماییم.

## طراحی سیستمهای کنترلی

هدف از طراحی سیستمهای کنترلی، محافظت سیستم اطلاعاتی دربرابر مخاطراتی است که آن سیستم را تهدید می‌کند، بعضی از مشکلاتی که ممکن است برای سیستمهای اطلاعاتی پیش آیند عبارتند از: خطاهای ناشی از کمبودهای آموزشی و مهارتی کارشناسان، خرابکاری و دزدی پایگاههای اطلاعاتی، آتش‌سوزی، زلزله، سیل و سایر خطرات محیطی، اتفاقات غیرمترقبه و نقص در سیستم الکتریکی. روشهای جلوگیری از مخاطرات مزبور را می‌توان به سه دستهٔ کلی تقسیم کرد: روشهای پیشگیری [2]، روشهای تشخیصی [3] و روشهای اصلاحی [4].

کنترلهای پیشگیری کننده معمولاً ازطریق کنترل ورودی صورت می‌گیرد. نظر به اینکه داده‌ها ازطریق ورودی به سیستم وارد می‌شوند، اولین موردی که باید تحت کنترل قرار گیرد «ورودی» است. هدف از کنترل ورودی این است که از ورود داده‌های نادرست به داخل سیستم جلوگیری

---

۱ - قسمت اول این مقاله در شمارهٔ ۱۷ فصلنامهٔ تحول اداری، آذرماه ۱۳۷۶به چاپ رسیده است.

2 - Preventive

3 - Detective

4 - Corrective

شود و از تحقق شعار معروف «ورودی نامناسب، خروجی نامناسب را بدنبال دارد» [۵] ممانعت بعمل آید. منظور از این عبارت ، توجه به دقت، صحت و مناسب بودن ورودی است. چنانچه ورودی، ناقص و غلط باشد، بدیهی است که خروجی نیز به‌همان نسبت نارسا و نادرست خواهد بود.

کنترل ورودی با کنترل کُدها آغاز می‌شود. درمورد کنترل کُدها باید دقت کرد که **اولاً** رقمی بَر کُد اضافه‌نشود(مثل ۱۲۴۶۱به‌جای‌کُد ۱۲۴۶)، **ثانیاً** رقمی از کُد حذف نشود (مثل ۱۲۴ به جای کُد ۱۲۴۶)، **ثالثاً** یک کُد غلط به‌جای کُد اصلی قرار نگیرد (مثل ۲۲۴۶ به جای ۱۲۴۶) و **رابعاً** ارقام کُد جابجا نشوند (مثل جابجایی دو رقم: ۱۴۲۶ و جابجایی چند رقم: ۱۶۴۲). هریک از این قبیل اشتباهات و نظایر آنها ممکن است منجر به مشکلات جدی در کار سازمان شود. مثلاً، پولی به‌اشتباه از یک‌حساب به‌حساب دیگر ریخته شود یا نمرهٔ قبولی دانشجویی برای دانشجوی مردود منظور گردد.

## کنترل اعتبار ورودی

داده‌ها را باید در اولین فرصت و در اسرع وقت در نزدیکترین محل به منبع داده، مورد کنترل قرار داد تا اشتباهات احتمالی، قبل از پردازش، مرتفع شوند. کنترل اعتبار در سه سطح زمینه، رکورد و فایل، انجام می‌گیرد. هر زمینه باید ازنظر داده‌های افتاده، جاهای خالی، حروف و اعداد، دامنه، ارقام کنترل‌کننده و اندازه، دقیقاً کنترل شود. رکوردها باید ازنظر منطقی و معقول بودن، اعتبار علائم، اندازه و توالی، مورد بررسی قرار گیرند. فایلها نیز ازنظر برچسبهای داخلی و خارجی، نام فایل، تاریخ ایجاد، زمان به هنگام شدن، تعداد رکوردهای در فایل، برچسب پایانی (مشخصهٔ پایان فایل درصورتی که آخرین رکورد فایل باشد[۶] بررسی شوند.

باکنترل مشخصات و نمره‌های شناسایی استفاده کنندگان می‌توان اطمینان حاصل کرد که هیچ نوع تقلبی صورت نمی‌گیرد. با کمک روش کنترل دسته‌ای مطمئن می‌شویم که هیچ منبعی بیش از یک بار کنترل نمی‌شود و کلیهٔ مستندات منبع، پردازش می‌شوند. ازطریق ردگیری حسابرسی نیز اطمینان به دست می‌آید که مراحل ورودی، پردازش و خروجی نهایی، همگی مورد کنترل قرار گرفته‌اند و چنانچه اشتباهی رخ داده باشد فوراً اصلاح می‌شود.

برای کاهش خطاها باید در یک طرح کلی، انواع خطاها را شناسایی کرد و فراوانی هریک را نشان داد. براساس این طرح می‌توان تصمیمگیری کرد که به کسانی که مسئول جمع‌آوری، آماده‌سازی و **درونداد ورودیها**هستند، آموزشهای بیشتری داد یا نسبت به طراحی مجدد ورودی اقدام کرد[۷].

---

5 - Garbage In Garbage Out : GIGO

6 - End of file (EOF)

7- " I bid.", P.451.

# محافظت سیستم در برابر نرم‌افزارهای غیرمعتبر

برخی از نرم‌افزارهای ویرانگر عبارتند از:

**روشهای سالامی**[8]: در روشهای سالامی، برنامه‌ریز ابتدا از تقلب در مقادیر خیلی پایین شروع می‌کند و سپس در سطح کلان به شیادی می‌پردازد. مثلاً وقتی یک برنامه‌ریز، سود حسابهای مشتریان را محاسبه می‌کند ماندهٔ حسابهایی را که کمتر از یک ریال باشد به حساب خود منظور می‌کند (ظاهراً برای روند کردن یا گِردکردن) و وقتی مبلغ برداشتی خیلی ناچیز باشد کسی متوجه نمی‌شود که مبلغی کسر شده است هنگامی‌که برنامه‌ریز همین کار را با یک مبلغ کلان انجام دهد دیگر خیلی دیر خواهد بود تا بتوان کاری انجام داد.[9]

**اسبهای تروا**[10]: اسب تروا مجموعه‌ای از رویه‌های برنامه‌ریزی است که درعین اجرای عادی برنامه، انجام کارهای غیرمجاز را نیز شامل می‌شود.

**بمبهای منطقی**[11]: به‌کمک بمبهای منطقی می‌توان خرابکاریهای عمدی را در برنامه به وجود آورد. مثلاً وقتی یک برنامه، خوب تنظیم نشود در هنگام اجرا سبب خرابی و از بین بردن داده‌ها یا فایلها می‌شود. یک برنامه‌ریز می‌تواند عمداً یک بمب منطقی را به گونه‌ای تنظیم کند تا از زمان خاصی، پس از انجام یک رویداد مشخص و یا پس از تحقق یک سری از شرایط معین، عمل کند و در کار برنامه اختلال وارد نماید.

**کرمها**[12]: کرمها نیز برنامه‌هایی هستند که مجدداً خود را تکرار می‌کنند (دوباره خود را می‌نویسند و تکرار می‌کنند). این کرمها نیاز به میزبان ندارند و خود را به‌برنامهٔ خاصی نیز متصل نمی‌سازند بلکه مستقلاً عمل می‌کنند و معمولاً در داخل یک رایانه یا شبکه‌ای از رایانه ها گسترش می‌یابند.[13] معروفترین مورد کرمها در سال ۱۹۸۸ در شبکهٔ اینترنت پدید آمد و باعث ازکارافتادن حداقل ۶۲۰۰ رایانه شد و درنتیجه بطور مستقیم و غیرمستقیم سبب ایجاد اختلال در کار بیش از هشت میلیون نفر کارکنان دولت و دانشگاهها گردید. در این مورد، کرم، کنترل همهٔ حافظه‌ها را در اختیار خود گرفت و انجام هر کاری را توسط رایانه غیرممکن ساخت.

**ویروسها**[14]: ویروس عبارتست از یک جزء «**خودتنظیم**» از کُد برنامه که بطور خودکار، تکثیر می‌شود. وقتی که به هر دلیل، ویروسی وارد رایانه شود، چه ازطریق برنامه‌ریز و یا به‌وسیلهٔ دیسک مبتلا به ویروس، کُد

8 - Salami Techniques
9- " Ibid", P.451, 452.
10- Trojan Horses
11 - Logic Bombs
12 - Worms
13- " Ibid." , P.453.
14 - Viruses

ویروسی، کنترل رایانه را دراختیار می‌گیرد و خود را در حافظه کپی می‌کند. زمانی که نرم‌افزارهای جدیدی در رایانه قرار داده شوند، ویروس، خود را در آنها کپی می‌کند و آنها را نیز آلوده می‌سازد. اگرچه ازبین بردن‌کامل‌ویروسها امکان‌پذیر نیست ولی انجام این اقدامات، به کاهش آنان کمک می‌کند: استفاده از برنامه‌های ویروس‌کُش یا واکسنهای موجود برای چند ویروس مشخص، خریدن دیسکها از فروشندگان معتبر، استفاده از ایستگاههای کاری بدون دیسک.

کلیهٔ مخاطراتی که به آنها اشاره شد، می‌توان تاحدود زیادی ازطریق دنبال کردن دقیق مراحل چرخهٔ تکاملی سیستمها و طراحی یک سیستم مؤثر کنترل و آزمون نرم‌افزار، تحت‌کنترل درآورد.[۱۵]

## کنترل خروجی سیستمها

کنترل خروجیهای بسیار محرمانه و تاحدی محرمانه، چه ازطریق سیستمهای زمان واقعی تولید و چه به‌وسیلهٔ سیستمهای دسته‌ای، امری بسیار حیاتی است. کنترل خروجی زمان واقعی، شامل سه بخش عمده است: **وسیلهٔ انتقال، پایانه، و حافظه‌های کمکی قابل تعویض** مثل **دیسکتهای فلاپی**. نوع کنترل موردنیاز به دوعامل عمده بستگی پیدا می‌کند **اول، درجهٔ حساسیت اطلاعات و دوم، طراحی فرایند.** اطلاعات خروجی را می‌توان به چهاردسته تقسیمبندی کرد: **خیلی محرمانه**[۱۶]، **محرمانه**[۱۷]، **محدود**[۱۸] و **عمومی**.[۱۹] اطلاعات بسیار محرمانه از حساسیت بسیار زیادی برخوردارند، مثل اطلاعات دفاعی و یا طرحهایی که برای گسترش فعالیتهای شرکت در دست تدوین هستند. خروجی محرمانه نیز اگرچه حساس است ولی چنانچه به دست افراد ناباب بیفتد به‌آن حدی که اطلاعات خیلی محرمانه ممکن است بر سرنوشت فرد یا مؤسسه تأثیر بگذارد، اثر سوء نخواهد داشت مثل اطلاعات مربوط به مشتریان، کارکنان و حقوق آنان، اسامی صاحبان سهام. اطلاعات محدود برای تعدادی از کاربران در داخل سازمان توزیع می‌شود و نشر آنان در خارج از سازمان ممنوع است (مثل گزارش کارهای تولیدی). خروجی عمومی، جنبهٔ باز داشته و بین سایر سازمانها توزیع می‌شود، مثل ارزش سهام و بورسها، دومین عاملی که بر نوع کنترل خروجی تأثیر می‌گذارد، نحوهٔ طراحی فرایند است. به‌عبارت دیگر تولید خروجی از طریق سیستمهای زمان واقعی و یا ازطریق سیستمهای دسته‌ای برنوع کنترل اثر می‌گذارد. درجهٔ حساسیت‌اطلاعات، شدت کنترل و نحوهٔ طراحی فرایند، نوع کنترل را

15- " Ibid.", P.474.
16 - Top Secret output
17 - Secret output
18 - Restricted output
19 - Public output

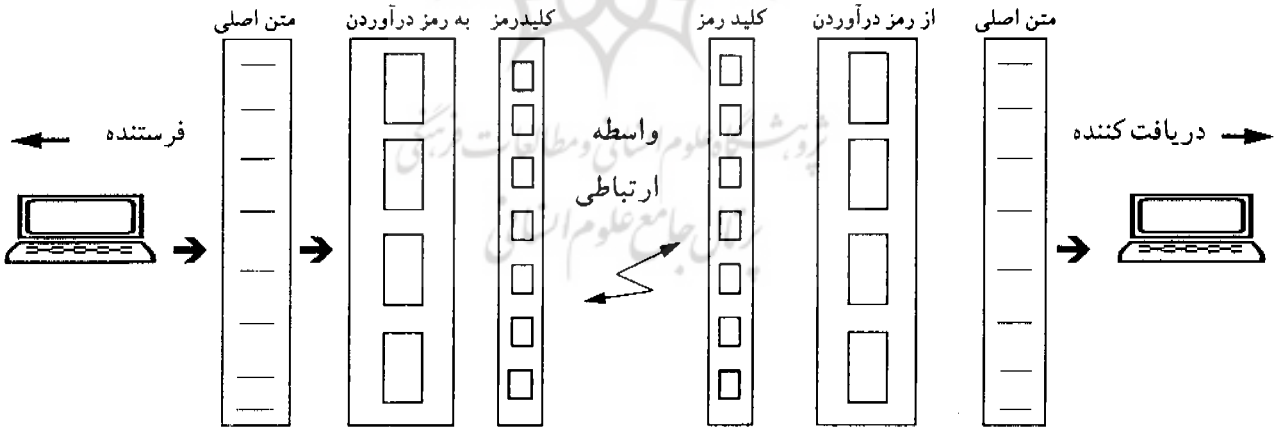
تعیین می‌کند.

در سیستم زمان واقعی، خروجی معمولاً در پایانه‌ها یا در ایستگاههای کار، چاپ شده یا نمایش داده می‌شود و کاربران بطورمستقیم‌باسیستم درتعاملند تا خروجیهای‌موردنیازشان‌رادریافت کنند. دراین مورد باید دقت شود که اولاً در مسیر انتقال خروجی به‌کاربران مجاز، امکان سوءاستفادهٔ افراد غیرمجاز بوجود نیاید و ثانیاً وقتی خروجی در پایانه به نمایش گذارده می‌شود فقط افراد مجاز آن را مشاهده کنند.

برای حفاظت خروجی در مسیر انتقال می‌توان از روش به‌رمز درآوردن استفاده کرد. در این روش داده‌ها به طرق خاصی درهم و برهم، مبهم و یا پنهان می‌شوند به نحوی که افراد غیر و نامحرمان نتوانند به‌معنای اصلی آنها پی ببرند و فقط کاربَر موردنظر به مفهوم آن دست یابد. سیستم به رمز درآوردن[۲۰] به دو دستهٔ کلی تقسیم پذیر است : یک کلیدی و دو کلیدی؛

## روش یک کلیدی[۲۱]

در این روش فرستنده و دریافت کننده هر دو از کلید رمز آگاه هستند، فرستنده، متن پیغام را همراه با کلیدی که آن را بصورت رمز درمی‌آورد برای دریافت کننده ارسال می‌دارد و دریافت کننده بااستفاده از همان کلید، متن رمز را به متن اولیه تبدیل می‌کند و از محتوای آن آگاه می‌شود.




شکل «سیستم به‌رمز درآوردن داده‌ها»

20 - Encrypton

21- The Single - Key Data Encryption Standard Crypto System :DES

# روش دوکلیدی

در روش دوکلیدی [۲۲] از دو کلید که ازنظر ریاضی مکمل یکدیگرند،استفاده می‌شود. دو کلید مزبور یکی برای به رمز درآوردن و دیگری برای از رمز درآوردن بکار می‌روند. با این ترتیب، کاربَر می‌تواند کلید از رمز درآوردن را برای خود حفظ کند و به این‌طریق از مخفی نگهداشتن متنهای موردنظر خویش اطمینان حاصل نماید.

هنگامی که اطلاعات خاص برصفحه نمایش منعکس می‌شوند، ممکن است موردسوءاستفاده‌هایی قرار گیرند، برای جلوگیری از این سوءاستفاده‌ها و اقدامهای خلاف، باید پایانه‌ها را در محلهای حفاظت شده‌ای قرارداد تا تحت کنترل دقیق قرار داشته باشند (مثلاً کنترلهای بیومتریک)، به‌علاوه می‌توان در پایانه‌ها از قلابهای مخصوصی برای حفاظت از اطلاعات استفاده کرد و یا اطلاعات را با تراکم کمتر [۲۳] به‌نمایش درآورد. علاوه بر این پیش‌بینیها، میز کاربَران و نحوهٔ قرار گرفتن رایانه را نیز می‌توان به‌نحوی تنظیم کرد که صفحهٔ نمایش را کسی غیر از او مشاهده ننماید. با چنین تمهیداتی باید تلاش کرد که اطلاعات و خروجیها مورد سوءاستفاده قرار نگیرند.

درمورد استفاده کنندگان غیرمجاز نیز باید پیش‌بینیهای لازم صورت گیرد. سیستم را باید به‌گونه‌ای برنامه‌ریزی و طراحی کرد که استفاده‌کنندهٔ مجاز را از غیرمجاز شناسایی کند. در این مورد نیز می‌توان از کُدها، کلیدهای رمز، واژهٔ عبور، قفل کردن سیستم، ویژگیهای فیزیکی و شخصی کاربَر (مثل اثر انگشت، ارتعاش صوت، الگوی امواج مغزی) استفاده کرد و در فواصل متناوب و معقول، هویت کاربَر مجاز را بررسی نمود. [۲۴]

در سیستم کنترل دسته‌ای، برای حفاظت داده‌ها ابتدا نقاط کلیدی و حساس فرایند کار تشخیص داده می‌شود و در آن نقاط، کنترل صورت می‌گیرد. نقاط حساس در این روش عبارتند از کنترل مستندات، کنترل مرحلهٔ پردازش، مرحلهٔ چاپ مستندات، مرحلهٔ توزیع مستندات و بالاخره زمان نقل و انتقال.

معمولاً کلیهٔ سیستمها چه بصورت زمان واقعی و چه بصورت برنامه‌ای یا دسته‌ای، مستندات زیادی به همراه دارند. مستندات، گاهی اطلاعات بسیار محرمانه‌ای را دربَر دارند که حساسیت آنها را افزایش می‌دهد بنابراین لازم است که آنها را در محل امنی حفظ کرد تا فقط کاربَران مجاز، به آنها دستیابی پیدا کنند برای حفاظت اسناد خیلی محرمانه باید تدابیر خاصی را بکار بُرد (مثلاً می‌توان برای استفاده از آنها امضاء دو فرد مسئول را ضروری دانست).

22- The Double- Key Public Key Cryptosystem

23 - Low Intensity

24- " I bid.", P.471.

فایلها نیز باید فقط به وسیلهٔ افراد مجاز مورد استفاده قرار گیرند. عملگرها نیز باید از موشکافی و کنجکاوی دربارهٔ اطلاعات چاپ شده در گزارشها باز داشته شوند ضمناً باید اطمینان حاصل شود که از گزارشها، فقط به تعداد موردنیاز کپی گرفته می‌شود. گزارشهای چاپ شده نیز باید مورد کنترل دقیق قرار گیرند تا از اشتباهات و خطاها، جاافتادگیها و کاستیها مبرا شوند. زمان و تاریخ تکمیل گزارش و همچنین مشخصهٔ پایان گزارش نیز باید در آنها قید شود. در زمان انقضای مدت اعتبار، خروجی را باید با سوزاندن، یا پاره‌کردن و خلاصه به طریقی مناسب، ازبین برد و یا به شیوه‌ای مناسب، بایگانی کرد.

## حفاظت پایگاههای اطلاعاتی

در پایگاههای اطلاعاتی جدید که امکان دستیابی به اطلاعات مشخصی را برای تعداد زیادی از کاربَران فراهم می‌آورند، این امکان پیش می‌آید که چندین کاربَر بطور همزمان نیاز به مجموعه‌ای از اطلاعات خاص پیدا کنند. بنابراین باید نظام کنترلی خاصی پیش‌بینی شود که کاربَران بتوانند به نوبت به اطلاعات موردنیاز خود دست پیدا کنند و برخوردها بطور منظم حل شود. در برخی از سیستمهای پیشرفته پایگاههای اطلاعاتی رابطه‌ای مثل IBMDB2 یک سیستم خودکار برای قفل کردن، کشف برخوردها و حل آنها بوجود آمده است.

اولین کاربَری که به اطلاعات دست می‌یابد تا پایان عملیات، آن را دراختیار می‌گیرد. وقتی کاربَر دوم با سیستم، تماس اتخاذ می‌کند و همان اطلاع اولیه را می‌خواهد، سیستم منتظر می‌ماند تا عملیات موردنظر کاربَر قبلی پایان بپذیرد و سپس فرامین کاربَر جدید را به‌جریان می‌اندازد[۲۵]

در سیستمهای دسته‌ای برای حفاظت و پشتیبانی داده‌ها از طرح خاصی به نام طرح «**پدربزرگ ـ پدر ـ پسر**» استفاده می‌شود. فایلی که درحال حاضر در جریان است به عنوان فایل پسر خوانده می‌شود. فایل پدر در پوششی مخصوص حفظ می‌شود و فایل پدربزرگ در محلی امن و دور از دسترس قرار داده می‌شود. چنانچه فایل پسر گم شود از فایل پدر استفاده می‌شود، عملیات تکرار می‌گردد و مجدداً فایل پسر ایجاد می‌شود. اگر فایل پدر گم شود نیز از فایل پدربزرگ، استفاده شده، عملیات قبلی تکرار و پدر مجدداً ایجاد می‌شود.

در سیستمهای زمان واقعی همواره یک بده ـ بستان مستمر بین حذف داده‌های کهنه و کپی کردن عملیاتی که داده‌ها را به‌هنگام می‌کنند در جریان است. البته حذف داده‌های کهنه، اگرچه سبب به هنگام شدن سریع داده‌ها می‌شود ولی گران و پرهزینه است. در این زمینه باید درمورد سرعت به هنگام کردن و هزینه و وقت

25- " I bid.", P.461

مصروفه تعادلی برقرار شود. در سیستمهای زمان واقعی از روشهای مختلفی برای پشتیبانی پایگاه اطلاعاتی استفاده می‌شود. یکی از این روشها روش آینه‌ای[۲۶] است. در این روش دو پایگاه اطلاعاتی در دو سیستم رایانه‌ای جداگانه ایجاد می‌شود. یکی از پایگاهها در محل و در دسترس کاربران است و پایگاه آینه‌ای در سیستم رایانه‌ای دیگری جای می‌گیرد.[۲۷] به این ترتیب از پایگاه اطلاعاتی حفاظت بعمل می‌آید.

برخی از سازمانها برای ایجاد محلی امن و مطمئن برای پایگاههای اطلاعاتی خود از پناهگاهها، ساختمانهای قدیمی دولتی، معادن ازکارافتاده و غارها استفاده می‌کنند و کپی‌هایی از پایگاه اطلاعاتی و سایر اسناد مهم و محرمانهٔ خود را در این محلها حفظ می‌نمایند. باوجود همهٔ پیش‌بینیهایی که در این موارد می‌شود همچنان این امکان وجود دارد که به پایگاه اطلاعاتی صدمه بخورد. سازمانهایی که حیاتشان به این پایگاههای اطلاعاتی بستگی دارد (مثل سازمانهای بزرگ داد و ستد اوراق بهادار، شرکتهای هواپیمایی، بانکها) نیاز به سیستمی دارند که داده‌ها را به‌محل پشتیبانی پایگاه اطلاعاتی منتقل کند. کار این سیستمها انتقال الکترونیکی داده‌های مهم به محل اختصاصی برای اختفای پایگاه اطلاعاتی است.[۲۸] از این طریق به‌کمک یک واسطهٔ انتقالی سریع، کلیهٔ عملیات درزمان واقعی به محل پشتیبانی منتقل می‌شود.

شیوه‌ای که به آن اشاره شد در مواردی بکار می‌رود که پایگاه پشتیبان درفاصلهٔ دوری از پایگاه اولیه قرار داشته باشد. داده‌ها را می‌توان در یک محل ولی برروی دو دیسک جداگانه منتقل کرد. این روش رادیسک آینه‌ای[۲۹] می‌نامند. به‌این ترتیب، داده‌ها به محل دور از سیستم ، انتقال نیافته بلکه به یک دیسک دوم منتقل می‌شوند. نرم‌افزار دیسک آینه‌ای، داده‌ها را بر دو دیسک می‌نویسد و اگر یک دیسک، نقصی پیدا کند (مثلاً خط بردارد)، سیستم بطور خودکار، دیسک دوم یا آینه را، بدون حذف هیچ اطلاع و بدون توقف کار سیستم، مورد استفاده قرار می‌دهد. با شبانه‌روزی شدن کار سیستمها استفاده از دیسکهای آینه‌ای روبه ازدیاد است.[۳۰]

## کنترل سخت‌افزار

**رعایت ملاحظات زیر به افزایش ایمنی سخت‌افزارها کمک می‌کند:**

ـ ازنظر فیزیکی باید دقت شود که پایگاههای اطلاعاتی در محل مناسبی استقرار یافته و

---

26 - Mirror database

27- Edwards, Perry. "Opcit.", P.350.

28- Burnch, "Opcit." P. 463.

29 - Disk - mirroring

30- Winship, Sally, " Disk - Mirroring Products Offer True Fault Tolerance, " PC Week, Feberuary 4, 1991, P. 112.

ترجیحاً از درهای ورودی و خروجی سازمان فاصله گرفته و از میدانهای مغناطیسی دور باشند.

ـ تمهیدات حفاظتی و ایمنی ازنظر آتش‌نشانی، کابل تلفن، برق و غیره، اتخاذ شود. درمورد برق نباید به‌برق شهر اعتماد کرد و لازم است که درموارد لزوم از برق اضطراری کمک گرفته شود. درحال حاضر سه نوع سیستم برق لاینقطع وجود دارد: **سیستم ایستا که با باطری کار می‌کند؛ سیستم گردشی که از ژنراتور استفاده می‌کند؛ و سیستم ترکیبی که از باطری و ژنراتور به‌طور ترکیبی استفاده می‌کند**، زمانی که باطریها ضعیف می‌شوند ژنراتورها به کار می‌افتند و تاجایی که سوخت دارند کار می‌کنند.

ـ درمورد رایانه بهتر است از دوشاخه یا سه‌شاخه استفاده نشود زیرا ممکن است سایر وسایل برقی باعث نوساناتی درجریان برق شوند که این امر به ضرر رایانه است. وقتی کار با رایانه تمام شد باید آن را خاموش کرد.

ـ برای محافظت از دیسکها توصیه می‌شود فهرستی از آنها تهیه شده و روی هر دیسک برچسب زده شود. هرکس که از دیسکها استفاده می‌کند باید نام خود را در فهرستی که مخصوص این کار تهیه شده است یادداشت کند و به‌موقع، دیسک را در آلبوم مخصوص و درجای امن قرار دهد. هرگز نباید دیسک را پس از انجام کار، روی میز رها کرد و یا در داخل رایانه جای گذاشت.

## کنترل دستیابی به داده‌ها

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

چون امکان سوء استفادهٔ افراد غیرمجاز از داده‌ها وجود دارد باید تدابیری اتخاذ شود تا فقط کاربَران مجاز به داده‌ها دست یابند. کنترل دستیابی به داده‌ها مبتنی بر موارد زیر است:

**۱ـ کاربَران چه می‌دانند (آنچه که کاربَران می‌دانند)**
**۲ـ کاربَران چه دارند (آنچه که کاربَران دارند)**
**۳ـ کاربَران چه هستند (ویژگیهای خاصی که درکاربَران وجود دارد)**

درمورد اول، امکان دستیابی به اطلاعات برای کاربَرانی فراهم می‌شود که اطلاع خاصی دارند.

اسم رمز یا واژهٔ عبور[۳۱] کلمهٔ منحصر به فردی است که فقط کاربَر از آن اطلاع دارد و ازطریق آن می‌تواند به سیستم دستیابی پیدا کند. این رمز را می‌توان باشمارهٔ شناسایی شخصی (PIN) ترکیب کرد. همچنین می‌توان از سئوالات خاص دیگری که از قبل، برنامه‌ریزی شده‌اند کمک گرفت (مثلاً ازکاربَر سئوال شود که رنگ موردعلاقه‌اش چیست یا فلان ساختمان در کدام خیابان قرار دارد.چنانچه پاسخ همانی باشد که در سیستم، برنامه‌ریزی شده است، سیستم دراختیار کاربَر قرار می‌گیرد). واژهٔ عبور را باید در فواصل نزدیک، تغییر داد. برای این منظور می‌توان سیستم را به‌گونه‌ای طراحی کرد که چنانچه کاربَری واژهٔ عبور خود را برای مدتی طولانی تغییر ندهد، سیستم، اجازهٔاستفاده‌رابه‌اوندهد تا مجبور به‌تغییرواژهٔ عبور خود شود.[۳۲]

در مورد دوم امکان دستیابی به اطلاعات برمبنای آنچه که کاربَران دارند، فراهم می‌آید. در این مورد از کارتهای هوشمند[۳۳] که شبیه کارتهای اعتبار هستند و در درون آنها یک تراشهٔ رایانه قرار داده شده است، استفاده می‌شود. کاربَر با قراردادن کارت هوشمند همراه با شمارهٔ شناسایی شخصی خویش در پایانه می‌تواند به‌اطلاعات، دسترسی پیدا کند. جعل این کارتها بسیار دشوار است بهمین جهت استفاده از آنها رو به ازدیاد است.

درمورد سوم به ویژگیهای شخصی کاربَران توجه می‌شود. اگر یک کاربَر آگاهی خاصی داشته باشد احتمال این که یک شخص غیرمجاز همان اطلاع و آگاهی را به دست آورد، وجود ندارد چنانچه کاربَر یک شئی خاص (مثلاً کارت هوشمند) داشته باشد و از آن برای دسترسی به‌اطلاعات سیستم استفاده کند، احتمال گم شدن یا دزدیده شدن آن شئی وجود دارد، اما ویژگیهای شخصی یک فرد را نمی‌توان دزدید. بنابراین معتبرترین و قابل‌اتکاءترین کنترل، استفاده از ویژگیهای فردی کاربَران است. واژهٔ کنترل بیومتریک[۳۴] برهمین اساس استوار است. کنترلهای بیومتریک به‌دودستهٔ فیزیولوژیکی و رفتاری تقسیم می‌شوند، ویژگیهای فیزیولوژیکی عبارتند از: مشخصات کف دست (مثل اثر انگشت، شکل کف دست)، شبکیهٔ چشم، وزن بدن و غیره. ویژگیهای رفتاری نیز شامل شدت معمولی ضربهٔ انگشتان شخص برصفحهٔ کلید، امضاء (فشار دست و سرعت امضاء)، صدا و غیره هستند. برای سنجش و اندازه‌گیری کلیهٔ ویژگیهای یاد شده ابزارهای خاصی ابداع شده‌اند که به‌راحتی مورد استفاده قرار می‌گیرند.[۳۵]

از میان انواع سه‌گانهٔ کنترل دستیابی، مورد سوم یعنی کنترل براساس ویژگیهای شخصیتی و عملکردی کاربَران، قویترین و قابل اعتمادترین نوع کنترل دستیابی بشمار می‌آید.

31 - Password
32- Burch, "Opcit.", P. 471.
33 - Smart Cards
34 - Biometric Control
35- " Ibid."