مقاله

اهرم‌های مهار و ایمنی نظام‌های اطلاع‌رسانی

دکتر اسدالله آزاد[1]

چکیده: هدف از نگارش این نوشتار نشان دادن این نکته است که چگونه سازمان‌ها باید به یاری کندوکاو فنون مهار نظام‌های اطلاع‌رسانی بر منابع اطلاعاتی خود نظارت داشته باشند. اهرم‌های مهار و ایمن داشتن نظام‌های اطلاع‌رسانی به مدد در اختیار داشتن عنان راه‌کارها، تسهیلات و امکانات مادی، محاسبه‌های کاربر نهایی و هزینه‌های نظام اطلاع‌رسانی عمل می‌کند. از این رو، تشریح نیازهای فوق و انواع روش‌هایی که نسبت به کیفیت و ایمنی نظام‌های اطلاع‌رسانی اطمینان خاطر می‌بخشد، موضوع مقاله خواهد بود.

نیاز به مهار و نظارت

ارتباطات نه تنها به صورت وسیله‌ای به منظور انجام عمل تصمیم‌گیری به کار می‌رود، بلکه به صورت عامل مهار، نظارت و هماهنگی، مراکز مختلف اخذ تصمیم و مراکز اجرای عملیات را در یک سازمان به هم مرتبط می‌سازد. مهار یا نظارت عبارت است از "مقایسه میان عملیات و در واقع آنچه اجرا می‌شود، با برنامه‌ها؛ یا به بیان دیگر، مقایسه میان بایدها (پیش‌بینی‌ها و مطلوب‌ها) و هست‌ها (انجام شده‌ها و موجودها) و بررسی اقدامات انجام شده (یا در حال انجام) به منظور حصول اطمینان از اینکه اقدامات مذکور، مطابق هدف‌ها و روش‌های پیش‌بینی شده انجام شود"[1].

در واقع، مهار یا نظارت راهنمایی است که در مراحل مختلف برنامه، طراحان و مجریان را

---

۱. عضو هیأت علمی دانشگاه فردوسی مشهد

در دستیابی به انحرافات، نارسایی‌ها، ناهماهنگی‌ها و همچنین ارائه راه حل‌های مربوط یاری می‌دهد. بنابراین، لزوم نظارت امری دائمی، مستمر، سیال، و روان است و همزمان با اجرای برنامه‌ها و تا انتهای برنامه و گاه نیز پس از خاتمهٔ آن ادامه می‌یابد.

در هر نظام اطلاع‌رسانی، منابع سخت‌افزاری، نرم‌افزاری و داده‌ها باید به یاری اهرم‌های مهار درآید تا از کیفیت و ایمنی آنها اطمینان خاطر فراهم گردد. ثابت شده است که رایانه‌ها می‌توانند حجم انبوهی از داده‌ها را پردازش و با دقتی بیش از نظام‌های دستی محاسبه‌های پیچیده‌ای را انجام دهند. با این حال می‌دانیم که: ۱) در نظام‌های مبتنی بر رایانه خطاهایی روی می‌دهد؛ ۲) از رایانه‌ها به منظور انجام کارهای ساختگی و فریبکارانه سوءاستفاده می‌شود؛ و ۳) نظام‌های رایانه‌ای، نرم‌افزارها، و منابع داده‌های آنها با سوء نیت یا برحسب تصادف نابود می‌شود.

در این نکته که رایانه‌ها آثار تعیین‌کننده‌ای برشناسایی و آشکارسازی خطاها و تقلب‌ها داشته است، سخنی نیست. داده‌پردازی دستی و ماشینی از مدارک کاغذی و دیگر رسانه‌هایی بهره می‌جوید که کارکنان پردازش اطلاعات می‌توانند با چشم به وارسی آنها بپردازند. معمولاً افراد بسیاری به این کار مبادرت می‌ورزند و راه‌کارهای وارسی متقابل به آسانی انجام می‌پذیرد. از سوی دیگر، نظام‌های اطلاع‌رسانی مبتنی بر رایانه از رسانه‌های حِسگر ماشینی نظیر صفحه‌های مغناطیسی و نوار سود می‌جویند. این رسانه‌ها دستکاری‌های پردازشی را درون مدارهای الکترونیکی نظام‌های رایانه‌ای انجام می‌دهند. امروزه، توان وارسی بصری فعالیت‌های پردازش اطلاعات و درونمایهٔ پایگاه‌های داده‌ها به‌طرز چشمگیری کاهش می‌یابد. افزون بر این، تعداد کارکنان نسبتاً اندکی می‌توانند بر فعالیت‌های پردازش حیاتی سازمان نظارت مؤثر داشته باشند، لذا از توان شناسایی خطاها به وسیلهٔ رایانه کاسته می‌شود.

بسا دیده‌ایم که کاربران، برنامه‌نویسان و کاروران[1] مواردی را نادیده می‌گیرند و در داوری‌ها دچار اشتباه می‌شوند. گاه رایانه چنانکه برنامه‌نویسی شده است کار نمی‌کند و به آسانی از کار باز می‌ماند. راه‌کارهای مهار و ممیزی نظام‌های اطلاع‌رسانی و اهرم‌های نظارتی ما را مطمئن می‌سازد که نظام بنابر برنامه کار کند و خطاها و روش‌های کار نامناسب، حتی پیش از راه‌اندازی، بررسی و برطرف شود.

برای آسایش خاطر از ایمنی نظام‌های اطلاع‌رسانی، یعنی دقت، یکپارچگی و سلامت فعالیت‌های نظام و منابع آن، به اهرم‌های مهار مؤثری نیاز است. اهرم‌های مهار می‌تواند خطاها، تقلب‌ها و نابودی خدمات اطلاع‌رسانی سازمانی را به حداقل و بهبود کیفی را به حداکثر رساند.

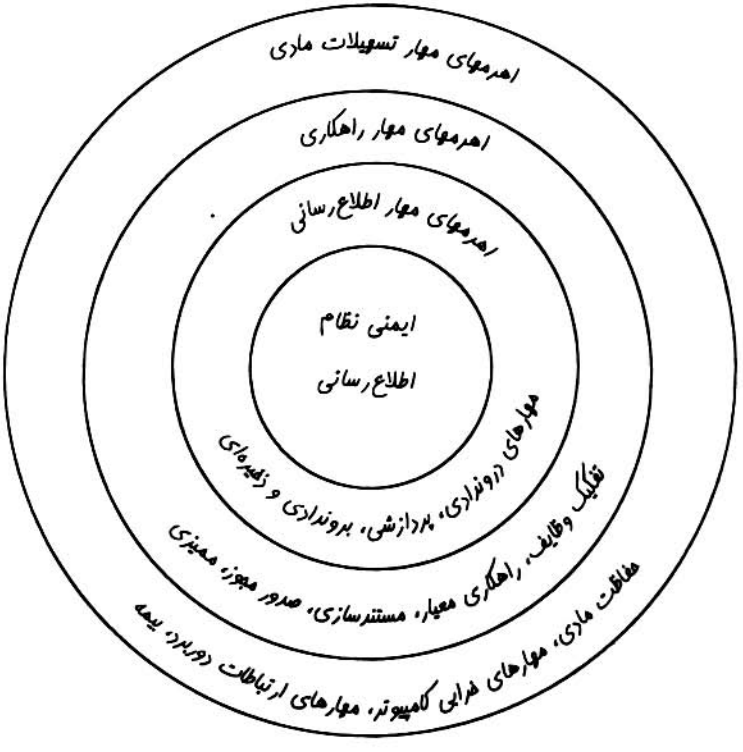
---

1. operators

این مهم از آثار منفی بالقوهٔ نظام‌های اطلاع‌رسانی می‌کاهد و بربقای توفیق‌آمیز آن در راستای بهبود زندگی اجتماعی می‌افزاید.

مهارهای مورد نیاز

برای آسودگی خاطر از کیفیت والا و ایمنی نظام‌های اطلاع‌رسانی به چند نوعْ اهرم عمدهٔ نظارتی نیاز است. این اهرم‌های مهار، چنانکه در تصویر ۱ ملاحظه می‌شود، عبارت است از: اهرم‌های مهار اطلاع‌رسانی، راه‌کاری و تسهیلات و امکانات مادی.

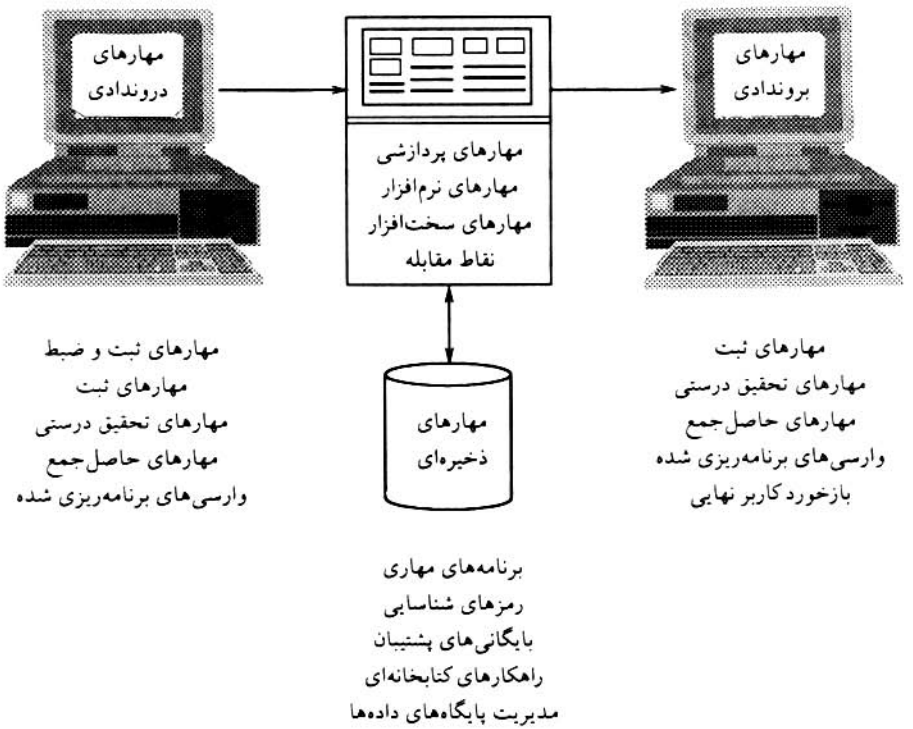


تصویر ۱. اهرم‌های مهار نظام‌های اطلاع‌رسانی

اهرم‌های مهار نظام اطلاع‌رسانی

به سبب خطاهای بالقوهٔ انسانی یا سخت‌افزاری، علاوه بر تهدید جرائم رایانه‌ای، ایجاد اهرم‌های مهار درون‌ساختی برای اطمینان خاطر از درستی، اعتماد، یکپارچگی، و ایمنی

نظام‌های اطلاع‌رسانی، برای هر سازمانی مهم و ضروری است. خطای درونداد داده‌های نادرست می‌تواند سبب تحویل اطلاعات بروندادی ناصواب گردد. کارور رایانه می‌تواند با فراموش کردن کار ممیزی روزانه، بحرانی بیافریند. اهرم‌های مهار نظام اطلاع‌رسانی برای پیشگیری از چنین حوادثی و نیز هزاران رویداد ناخواستهٔ دیگر به‌وجود می‌آید. این اهرم‌ها خطاها را پیش از پردازشگری، در خلال آن، و پس از آن به حداقل می‌رساند یا حذف می‌کند، تا داده‌های ورودی و اطلاعات تولیدی درست و بی‌عیب باشد. ازاین‌رو، چنین اهرم‌هایی برای نظارت و حفظ کیفیت و ایمنی درونداد، پردازش، برونداد، و ذخیرهٔ هر نظام اطلاع‌رسانی طراحی می‌شود (تصویر ۲).



تصویر ۲. انواع اهرم‌های مهار نظام اطلاع‌رسانی

مهارهای دروندادی

آیا هرگز جملهٔ "از درونداد بیهوده، برونداد بیهوده زاید" را شنیده‌اید؟ بدین دلیل برای درونداد درست داده‌ها به نظام اطلاع‌رسانی، به اهرم‌های مهار نیاز است. نمونه‌های این مورد شامل صفحه‌های نمایش آرایش شدهٔ ورودی داده‌ها، رسانه‌های ماشین‌خوان، نمونه‌های روی کلیدهای ابزارهای دروندادی کلیدرانْ و نمونْ‌برگ‌ها (فرم‌ها)ی از پیش ضبط یا شماره‌گذاری شده است. بر درونداد سند منبع نیز می‌توان به یاری ثبت و ضبط آن نظارت داشت. نظام‌های زمان واقعی [بلادرنگ] که به بایگانی‌ها دسترسی مستقیم دارند، اغلب تمامی داده‌های ورودی به نظام را بر نوارهایِ مغناطیسیِ ثبتِ نظارتی ضبط می‌کنند که خود شاهدی بر تمام دروندادهای نظام است.

نرم‌افزار رایانه‌ای می‌تواند در بردارندهٔ دستورالعمل‌هایی برای شناسایی داده‌های درونـدادی نادرست، نامعتبر، یا ناقص باشد. مثلاً برنامهٔ ورودی داده‌ها می‌تواند رمزها، میدان داده‌ها و تراکُنش‌های[1] نامعتبر را وارسی کند. همچنین می‌توان رایانه را چنان برنامه‌ریزی کرد که اگر داده‌های دروندادی از محدوده‌های معینی تجاوز کند یا توالی معقول نادیده گرفته شود، این رویداد مهم را دریابد. چنین کاری محاسبه و نظارت بر حاصل جمع‌هایی گزیده را در برمی‌گیرد.

انواع راه‌کارهای وارسی مختلفی در نرم‌افزارها طراحی می‌شود. دو نمونه از این راه‌کارها عبارت است از:

- وارسی خردپذیری. یعنی اگر حداکثر سفارش شرکتی به کارخانه‌ای ۲۵۰ قلم کالا باشد و سفارش ۲۰۰۰ قلمی وارد شود نسبت به سفارش‌های معمول چنین اطلاعاتی نابخردانه می‌نماید و احتمال خطا به ذهن کارور ورود داده‌ها می‌رسد.
- وارسی محدوده. وارسی محدوده ارزش ورودی راکه مورد انتظار نیست ارزیابی می‌کند. مثلاً مقرراتِ شرکتی هفته‌ای چهل ساعت کار را برای کارمند تجویز می‌کند و اضافه کار پانزده ساعت کار در هفته را مجاز می‌شمارد. وارسی محدودهٔ ساعات کار بر این مهم نظارت می‌کند که این میزان بین چهل تا پنجاه و پنج ساعت باشد.

مهارهای پردازشی

چنانچه داده‌ها به‌درستی به نظام رایانه‌ای وارد شود، پس باید به‌درستی هم پردازش گردد. اصولاً اهرم‌های مهار پردازش برای شناسایی خطای محاسبات و عملکردهای منطقی تهیه

1. transactions

می‌شود. همچنین برای اطمینان خاطر از ناپدید نشدن یا پردازش نشدن داده‌ها از آنها بهره می‌جویند. اهرم‌های مهار پردازش می‌تواند شامل مهارهای سخت‌افزاری و نرم‌افزاری باشد.

مهارهای نرم‌افزاری

برخی اهرم‌های مهار نرم‌افزاری برای اطمینان خاطر از این مسئله طراحی می‌شود که داده‌های درستی پردازش شود. مثلاً نظام عامل یا نرم‌افزاری دیگر، برچسب‌های بایگانی درونی را در آغاز یا انتهای بایگانی‌های نوار مغناطیسی یا صفحه وارسی می‌کند. این برچسب‌ها حاوی اطلاعاتی است که بایگانی را شناسایی و مجموع داده‌های آن را وارسی می‌کند. چنین برچسب‌هایی به نظام اطمینان می‌دهد که از بایگانی مورد نظر استفاده به عمل آورد و با اعتماد تام داده‌ها را پردازش کند.

اهرم مهار نرم‌افزاریِ دیگر، تدارک نقاط مقابله[1] یا وارسی در خلال پردازش برنامه است. نقاط مقابله یا وارسی جایگاه‌هایی در میان برنامهٔ در حال پردازش است که در آنها جمع‌های میانی، سیاهه‌برداری یا روبرداری از داده‌ها بر نوار یا صفحه‌های مغناطیسی نگاشته یا در چاپگر صورت‌برداری می‌شود. نقاط وارسی تأثیر خطاهای پردازشی را به حداقل می‌رساند، چه پردازش می‌تواند از آخرین نقطهٔ وارسی، و نه از آغاز برنامه، دوباره شروع شود. همچنین می‌تواند در ساخت ردّممیزی[2]، که تراکُنش‌ها را در تمام مراحل پردازش دنبال می‌کند، مددکار افتد.

بسیاری از اهرم‌های مهار درونِدادی، پردازشی، برونِدادی، و ذخیره‌ای می‌توانند به یاری بسته‌های نرم‌افزاری نظامی خاص، مشهور و موسوم به "ناظران ایمنی نظام"[3] تهیه شود. ناظران ایمنی نظام برنامه‌ای است که بر استفاده از نظام رایانه‌ای نظارت دارد و منابع نظام را از بهره‌جویی غیرمجاز، تقلّب و نابودی حفظ می‌کند. چنین برنامه‌هایی تنها به کاربران مجاز اجازهٔ دستیابی به نظام را می‌دهد. برای نمونه، رمزهای شناسایی و اسم‌های رمز اغلب بدین منظور به کار می‌رود. ناظران ایمنی نظام همچنین بر استفاده از سخت‌افزار، نرم‌افزار، و منابع داده‌های نظام رایانه‌ای دیده‌بانی می‌کنند. مثلاً احتمال دارد حتی کاربران مجاز از بهره‌جویی از ابزارها، برنامه‌ها، و بایگانی‌های ویژه‌ای محروم باشند. سرانجام، چنین برنامه‌هایی تلاش‌های مربوط به استفادهٔ نادرست را دیده‌بانی و آمارهای مربوط را گردآوی می‌کند.

---

1. checkpoints
2. audit trail
3. system security monitors

مهارهای سخت‌افزاری

اهرم‌های مهار سخت‌افزاری وارسی‌های خاص درون‌ساختی سخت‌افزار برای بررسی درستی کار پردازش رایانه است. این اهرم‌ها برای نمونه عبارت است از:

● شناخت و نمایان‌سازی معایب مدارهای رایانه‌ای که می‌تواند بر عملیات آن نظارت کند. مثلاً برای جلوگیری از پاک شدن تعداد درست رقم‌های دوتایی واحد اطلاعات [بایت] از وارسی‌های توازنی[1] استفاده می‌شود. نمونه دیگر، وارسی‌های پژواکی[2] است که لازمهٔ آن بازگشت طنین از دستگاه یا مداری است که درستی کار را محقق می‌سازد. سایر نمونه‌ها شامل وارسی‌های افزونهٔ مداری[3]، علامت‌های عددی، نشانه‌های زمانگیری و مقدار ولتاژ است.

● مؤلفه‌های افزونه. برای نمونه از وارسی‌های شاخک‌ها [نوک‌ها]ی خواندی ـ نوشتاری چندگانه نوارها و صفحه‌های مغناطیسی برای کمک به‌درستی فعالیت‌های مربوط به خواندن و ضبط استفاده می‌شود.

● راه گزینه‌ها و دیگر ابزارها. برای مثال استفاده از راه‌گزینه‌هایی که می‌توان آنها را برای جلوگیری از نگارش بر نوار یا صفحهٔ مغناطیسی تنظیم کرد. در حلقه نوارهای مغناطیسی، حلقه‌ای فلزی یا پلاستیکی را می‌توان برداشت تا از نگارش بر نوار پیشگیری شود. بُرش‌های نگارشی/حفاظتی صفحه‌های لغزان (لرزان، نرم) هم همین کار را انجام می‌دهد.

● از ریزپردازنده‌های چندمنظوره و مدارهای مربوط می‌توان برای پشتیبانی از امکانات عیب‌شناختی دوربرد و نگهداری استفاده کرد. این کار به فناوران برون‌سازمانی اجازه می‌دهد تا عیب‌یابی کرده و از راه ارتباطات دوربرد و ابزارهای متصل به نظام رایانه‌ای به رفع معایب پردازند.

مهارهای بروندادی

چگونه می‌توان بر کیفیت اطلاعات تولیدی نظام اطلاع‌رسانی نظارت کرد؟ اهرم‌های مهار بروندادی برای اطمینان خاطر از این نکته که اطلاعات تولیدی درست و کامل است و به‌موقع به کاربران مجاز منتقل می‌شود، به وجود می‌آید. این مهارها شبیه مهارهای بروندادی است. مثلاً، سندهای بروندادی و گزارش‌ها اغلب ثبت، با برگه‌های گردش کار مقابله و توسط کارکنان عملیات بازبینی می‌شود. جمع‌بندی برونداد با جمع‌بندی درونداد مقایسه می‌گردد. می‌توان سیاهه‌هایی از نسخه‌های چاپی تمام اسناد و گزارش‌ها فراهم ساخت.

---

1. parity checks
2. echo checks
3. redundant circutry checks

از برگ‌نمون‌های بروندادی از پیش شماره‌گذاری شده می‌توان در نظارت بر حفظ اسناد بروندادی مهم مثل مجوزهای انبار یا چک‌های حقوقی استفاده کرد. سیاهه‌های توزیع کمک می‌کند اطمینان یابیم که تنها کاربران مجاز گزارش‌های حساس را دریافت دارند. نمایش‌های دیداری نظام‌های پردازش زمان واقعی، نوعاً با نرم‌افزار ایمنی مهار می‌شود که برکاربران نهایی مجاز به دریافت مواد از ایستگاه‌های کار و پایانه‌ها نظارت دارد. سرانجام، درباب کیفیت دستاوردهای اطلاعاتی باید به منظور بازخورد با کاربران نهایی تماس گرفت.

مهارهای ذخیره‌ای

چگونه می‌توان از منابع داده‌ها حفاظت کرد؟ نخست، مسئولیت‌های نظارت بر بایگانی‌های برنامه‌های رایانه‌ای و پایگاه‌های داده‌های سازمانی را می‌توان بر عهدهٔ کتابدار یا مدیر پایگاه‌های داده‌ای نهاد. این کارکنان مسئول حفاظت و نگهداری و نظارت بر دستیابی به کتابخانه‌ها و پایگاه‌های داده‌های سازمان‌اند. دوم، بسیاری از پایگاه‌های داده‌ها و بایگانی‌ها از دسترس استفادهٔ غیرمجاز و تصادفی، با برنامه‌ای ایمنی که پیش از استفاده به شناسایی کامل نیازمند است، دور نگه‌داشته می‌شود. به گونه‌ای، نظام عامل یا دیده‌بان ایمنی، پایگاه‌های داده‌های نظام‌پردازش زمان واقعی [بی‌درنگ] را از استفادهٔ غیرمجاز یا پردازش تصادفی حفظ می‌کند. از رمزهای شمارهٔ حساب، اسم رمز و دیگر رمزهای شناسایی، اغلب برای اجازهٔ استفادهٔ کاربران مجاز بهره می‌گیرند. فهرست کاربران مجاز نظام رایانه‌ای را قادر می‌سازد تا کاربران مجوزدار را بشناسد و نشان دهد که مجاز به استفادهٔ چه اطلاعاتی هستند.

به‌طور سنخی، نظام اسمِ رمز سه سطحی به کار می‌رود. نخست، کاربر با واردکردن رمز شناسایی منحصر به فرد خویش با نظام ارتباط برقرار می‌سازد. آنگاه اجازه می‌خواهد تا اسم رمز خود را برای دستیابی به اطلاعات نظام وارد کند. سرانجام، برای دستیابی به یک بایگانی خاص باید نام یگانهٔ بایگانی را بدهد. در برخی نظام‌ها، اسم رمز خواندنِ اندرونهٔ بایگانی با اسم رمز نگارش در بایگانی متفاوت است. این ویژگی، سطح حفاظتی دیگری برای منابع داده‌های ذخیره شده فراهم می‌سازد.

بسیاری از سازمان‌ها از بایگانی‌های پشتیبان نیز استفاده می‌کنند که همان نسخهٔ مکرر یا المثنای بایگانی‌های داده‌ها یا برنامه‌هاست. چنین بایگانی‌هایی ممکن است دور از پایگاه اصلی ذخیره شده باشد. بسیاری از نظام‌های پردازش زمان واقعی از بایگانی‌های تکثیر شده‌ای استفاده می‌کنند که به یاری ارتباطات دوربرد روزآمد می‌شود. بایگانی‌ها به کمک ذخیره‌سازی بایگانی‌های مادر و تراکُنشی دوره‌های پیشین نگهداری می‌شود. اگر بایگانی‌های جاری از میان

برود، بایگانی‌های ادوار پیشین برای بازسازی بایگانی‌های جاری جدید مورد بهره‌برداری قرار می‌گیرد. معمولاً چندین نسل از بایگانی‌ها به منظورهای نظارتی نگهداری می‌شود. بدین‌سان، بایگانی‌های مادرِ ادوار اخیر را می‌توان برای هدف‌های پشتیبانی نگهداری کرد.

اهرم‌های مهار راه‌کاری [1]

در نظام اطلاع‌رسانی، کار به دست افراد یا به یاری نظام رایانه‌ای انجام می‌شود. برنامه‌ها، شیوهٔ کار را به رایانه دستور می‌دهند. راه‌کارها [خط‌مشی‌ها] افراد را هدایت می‌کنند. برخی راه‌کارها جهت اهداف نظارتی درون نظام جای می‌گیرند. این اهرم‌های مهار به سازمان کمک می‌کنند تا درستی و یکپارچگی علمیات و فعالیت‌های توسعه نظام حفظ شود. انواع این گونه اهرم‌ها به شرح زیر است:

تفکیک وظایف. تفکیک وظایف، اصلی بنیانی در مهار راه‌کاری است. این امر ایجاب می‌کند که وظایف توسعهٔ نظام، عملیات رایانه‌ای و مهار داده‌ها و بایگانی‌های برنامه‌ها به گروه‌های مجزایی واگذار شود. برای نمونه، تحلیل‌گران نظام و برنامه‌نویسان نباید با رایانهٔ مادر کار کنند یا داده‌ها و برنامه‌هایی را که در حال پردازش است تغییر دهند. بعلاوه، مسئولیت حفظ بایگانی‌های داده‌های کتابخانه و برنامه‌ها بر عهدهٔ کتابدار یا مدیر پایگاه داده‌ها گذارده می‌شود. سرانجام، بخش نظارت بر تولید می‌تواند بر کارهای اطلاع‌پردازی، ورود داده‌ها و کیفیت داده‌های دروندادی/ بروندادی نظارت داشته باشد.

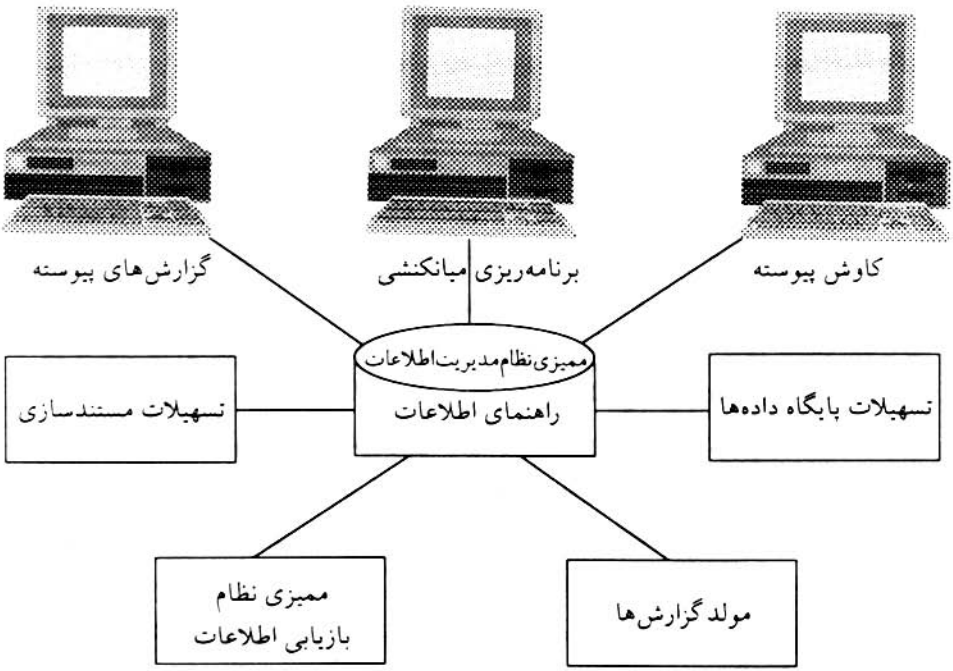
تدوین معیارها و مستندسازی. راه‌کارهای معیار نوعاً در راهنماها و نرم‌افزار درون ساختی می‌آید و در صفحه‌های نمایش کمکی عرضه می‌شود. پیگیری و رعایت راه‌کارهای معیار یکنواختی را رواج داده، امکان خطا و تقلب را به حداقل می‌رساند. این راه‌کارها به کارکنان کمک می‌کند تا آنچه را در اجرای آنها و فراهم‌شدن کیفیت برونداد از آنان طلب می‌شود، بشناسند. این نکته که راه‌کارها هم برای شرایط عملیاتی معمول و هم غیرمعمول تدارک دیده شود، مسئله مهمی است. سرانجام، مستندسازی نظام‌ها و عملیات باید به منظور اطمینان خاطر از پردازش درست هر یک از کاربردها انجام و روزآمد شود. مستندسازی در نگهداری نظام، زمانی که اصلاحات لازم صورت می‌گیرد، نیز بسیار ارزشمند است.

صدور مجوز برای درخواست‌ها. درخواست‌های مربوط به طرح‌های توسعه نظام‌های عمده، تغییر برنامه‌ها یا تبدیل نظام، اغلب پیش از صدور مجوز در معرض بازنگری رسمی قرار

1. procedural controls

می‌گیرد. برای نمونه، تغییر برنامه‌هایی که به دست برنامه‌نویسان مسئول حفظ و نگهداری انجام می‌شود، باید پس از مشاوره با مدیر عملیات رایانه‌ای و مدیر بخش کاربران نهایی، مورد تأیید مدیر قرار گیرد. تعویض و تبدیل سخت‌افزار و نرم‌افزارهای جدید، نصب و راه‌اندازی نظام‌های اطلاع‌رسانی تازه تکوین یافته و تغییر برنامه‌های موجود باید در معرض ملاحظهٔ رسمی، جهت به حداقل رساندن آثار زیانبخش آنها، قرار گیرد و مجوزهای ضروری صادر شود.

ممیزی. بخش خدمات اطلاع‌رسانی را باید به گونه‌ای ادواری بررسی یا به یاری کارکنان ممیزی داخلی سازمان دیده‌بانی کرد. البته، ممیزی ادواری ممیزان خارج از سازمان که از شرکت‌های ممیزی حرفه‌ای دعوت می‌شوند، کار خوبی است. چنین ممیزانی باید وارسی کنند که آیا اهرم‌های مهار نظام‌های اطلاع‌رسانی، مهارهای راه‌کاری، مهارهای امکانات مادی و دیگر مهارهای مدیریتی ایجاد و اجرا شده است یا نه. برای دیده‌بانی فعالیت‌های اطلاع‌پردازی نظام‌های اطلاع‌رسانی مبتنی بر رایانه، دو رهبرد بنیانی وجود دارد. این رهبردها را ۱) ممیزی پیرامون رایانه؛ و ۲) ممیزی در رایانه می‌دانند.



تصویر ۳. نمونه توانایی‌های بسته نرم‌افزاری ممیزی نظام مدیریت اطلاعات

ممیزی پیرامون رایانه شامل تحقیق در درستی و دقت پردازش داده‌هاست. این روش ساده‌تر است که به ممیزان دارای تجربه برنامه‌نویسی نیاز ندارد. هر چند این روش تراکُنشی را دنبال نمی‌کند که به بررسی تمام مراحل پردازش پردازد و به عبارتی دیگر، درستی و یکپارچگی برنامه‌های رایانه‌ای را نمی‌آزماید. بنابراین، تنها توصیه می‌شود از آن به عنوان مکمل دیگر شیوه‌های ممیزی استفاده شود.

ممیزی، در رایانه شامل تحقیق در درستی و یکپارچگی برنامه‌هایی رایانه‌ای است که داده‌ها را می‌پردازد و درونداد و برونداد نظام رایانه‌ای را امتحان می‌کند. ممیزی در رایانه به دانش عملیات و برنامه‌نویسی رایانه‌ای نیاز دارد. احتمال می‌رود برای آزمون درستی پردازش و مهار خط‌مشی‌های درون‌ساخت برنامهٔ رایانه از آزمون‌های خاص داده‌ها استفاده شود. ممیزان می‌توانند برنامه‌های آزمایشی ویژه‌ای تدوین کنند، یا از بسته‌های نرم‌افزاری ممیزی بهره‌جویند (تصویر ۳).

ممیزان قسم‌خورده از این برنامه‌ها برای پردازش داده‌های آزمایشی خود استفاده می‌کنند. آنها نتایج به دست آمده از برنامه‌های آزمایشی خود را با نتایج حاصل از برنامه‌های کاربر رایانه مقایسه می‌کنند. یکی از اهداف چنین آزمونی شناسایی وجود تغییرات غیرمجاز یا وصله‌های[1] برنامه‌های رایانه‌ای است. احتمال دارد وصله‌های برنامه‌های غیرمجاز سبب خطاهای "توضیح‌ناپذیر" یا وسیلهٔ اعمال اهداف فریبکارانه باشد.

ممیزی در رایانه احتمالاً برای برخی کاربردهای رایانه‌ای بسیار گران در می‌آید. بنابراین، ترکیبی از رهیافتهای ممیزی به کار گرفته می‌شود. ردّ پای ممیزی را می‌توان وجود کارِ مستندسازی تعریف کرد که اجازه می‌دهد تراکُنشی در تمام مراحل اطلاع‌پردازی دنبال شود. این پیگیری از حضور فرایند کار در سند منبع آغاز و با تبدیل آن به اطلاعات در سند برونداد‌ی‌نهایی پایان می‌یابد. دیدیم که پیگیری ردّ پای ممیزی نظام‌های اطلاع‌رسانی دستی بسیار آسان و مشاهده‌پذیر بود. اما، نظام‌های اطلاع‌رسانی مبتنی بر رایانه شکل ردّ پای ممیزی را دگرگون کرده است. اطلاعاتی که پیش‌تر به شکل پیشینه‌های دیداری در اختیار ممیز بود، دیگر در دسترس نیست یا بر رسانه‌هایی ضبط است که تنها دستگاه‌ها می‌تواند آن را بررسی و تفسیر کند. زمانی که از پایانه‌های دور دست و دستیابی مستقیم به بایگانی‌ها استفاده می‌شود، اسناد کاغذی و بایگانی‌های تاریخی اغلب حذف می‌گردد.

چنین پیشرفت‌هایی ممیزی این گونه نظام‌ها را پیچیده، اما تکلیفی حیاتی می‌سازد. بنابراین،

1. Patches

کارکنان بخش ممیزی باید در گروه اجرای طرح تمامی طرح‌های توسعه نظام‌های عمده شرکت داشته و مورد مشورت قرار گیرند، پیش از آن که طرح‌های نظام‌های حیاتی به اجرا گذارده شود. بعلاوه، ممیزان باید از تغییرات برنامه‌های رایانه‌ای عمده مطلع شوند، برنامه‌هایی که بر اثر فعالیت‌های حفظ و نگهداری ریخته می‌شود. چنین راه‌کارهایی به ممیزان فرصت پیشنهاد روش‌های حفظ ردّ ممیزی را می‌دهد.

به‌طور کلی سه نوع ممیز نظام اطلاع‌رسانی وجود دارد. این انواع عبارتند از ممیزان توسعه نظام، ممیزان عملیاتی و ممیزان کاربرد.

ممّیزان توسعهٔ نظام. کارکنان بخش ممیزی توسعه نظام رایزنان اعضای گروه طرح توسعه‌اند. دخالت آنان در امور طراحی، نظارت مناسب در طرح نظام اصلی را تضمین می‌کند.

ممّیزان عملیاتی. ممیزان عملیاتی در دوره‌های معینی بر کارهای مدیریت اطلاع‌رسانی نظارت دارند تا مطمئن شوند اهرم‌های مهار نظام موجود است و پیگیری می‌شود. حاصل جمع‌های درهم، وارسی‌های متقابل جمع ستون‌ها و ردیف‌ها و تفکیک وظایف، نمونه‌های چنین نظام‌ها و راه‌کارهایی است. ممیزان از این فنون و شماری شگردهای دیگر برای به حداقل رساندن امکان و فرصت سوء استفاده بهره می‌جویند.

ممّیزیان کاربُرد. هدف ممیزان کاربردِ ادواری، اعتباربخشی به یکپارچگی نظام اطلاع‌رسانی است. در ممیزی کاربردی، ممیزان به این نکته که مدیریت نظام طبق مشخصات طرح عمل می‌کند یا نه، اعتبار می‌بخشد. برای اعتباربخشی به مدیریت نظام اطلاع‌رسانی، ممیزان می‌توانند خلاصه گزارش را تا تراکُنش‌های اصلی و برعکس، دنبال کنند. آنان به عمد می‌کوشند تا فعالیت‌های نظام را به منظور وارسی اهرم‌های درونی تعطیل کنند.

اهرم‌های مهار تسهیلات مادّی

اهرم‌های مهار تسهیلات مادی روش‌های است که ابزارهای مادی و امکانات را از ناپدیدی و نابودی حفظ می‌کنند. مراکز رایانه در معرض خطرهایی چون حوادث ناخواسته، بلاهای طبیعی، اقدامات خرابکارانه، ویرانگری، سوءاستفاده، جاسوسی، نابودی، و دزدی منابع قرار دارد. بنابراین، محافظت مادی و راه‌کارهای نظارتی متعددی برای نگهداری سخت‌افزار، نرم‌افزار و منابع داده‌های حیاتی سازمان‌های استفاده کننده از رایانه لازم است. تصویر ۴ نشانگر راهبردهای عمدهٔ نظارتی و روش‌های خاص مهاری است که برای حفظ منابع نظام‌های اطلاع‌رسانی سازمان‌ها و کاربران نهایی آنها توصیه می‌شود.

مهارهای حفاظت مادّی. تدبیر حداکثر ایمنی و حفاظت در برابر بلاها، به‌هنگام کارگذاری رایانه، به انواع اهرم‌های نظارتی نیاز دارد. تنها کارکنان مجاز از طریق فنونی نظیر نشانه‌های شناسایی کارکنان خدمات اطلاع‌رسانی، قفل‌درهای الکترونیک، دزدگیر، مأمور امنیتی، تلویزیون مدار بسته و دیگر نظام‌های بازرسی و شناسایی می‌توانند به مرکز رایانه دسترسی داشته باشند. بسیاری از مراکز رایانه با تدابیری نظیر تهیه دستگاه تشخیص آتش‌سوزی و آتش‌نشانی، گاوصندوق‌های ضدآتش برای حفاظت از بایگانی‌ها، دستگاه‌های برقی اضطراری، حفاظتهای برقاطیسی و دستگاه‌های دماپا، کنترل رطوبت و گرد و غبار از بلاها محافظت می‌شود.

راهبردهای نظارتی	هدف	تاثیر	شیوهٔ نظارت
سدّ نفوذ[1]	مهار دستیابی	کاهش احتمال	تاثیر بر محیط، کاهش جذابیت هدف
	جداکردن دارایی‌ها	کاهش احتمال	مهار دستیابی به هدف، درپوش نهادن حفره‌ها به عنوان دفاع، دور کردن هدف از تهدید
بازدارندگی[2]	بازداشتن انگیزه‌ها	کاهش احتمال	اعلان تنبیه‌ها
	پیشگیری از تهدیدها	کاهش احتمال	شناسایی زود هنگام، خنثی کردن هجوم
	شناسایی نتایج	کاهش خسارت‌ها	شناسایی تمامی فعالیت‌ها، مرور ردپای ممیزی
ایجاد ابهام و پیچیدگی[3]	پنهان کردن دارایی‌ها	کاهش احتمال	رمزنگاری، مخفی کردن دارایی‌های مادی مهارت اطلاعات خصوصی
	پراکنده‌ساختن دارایی‌ها	کاهش خسارت‌ها	پشتیبانی و بازیافت، پردازش بدیل، محل‌های استقرار چندگانه
بهبود و بازیافت[4]	جایگزینی دارایی‌ها	استفاده از منابع دیگر	جداکردن (ایجاد موانع)، راه‌کارهای فوری، پشتیبانی و بازیافت، برنامه‌ریزی تصادفی، بیمه
	تبدیل خسارت‌ها	جذب خسارت‌های پیشین	

تصویر ۴. راهبردهای مهاری و روش‌های حفاظت منابع نظام‌های اطلاع‌رسانی[1]

1. containment
2. deterrance
3. obfuscation
4. recovery

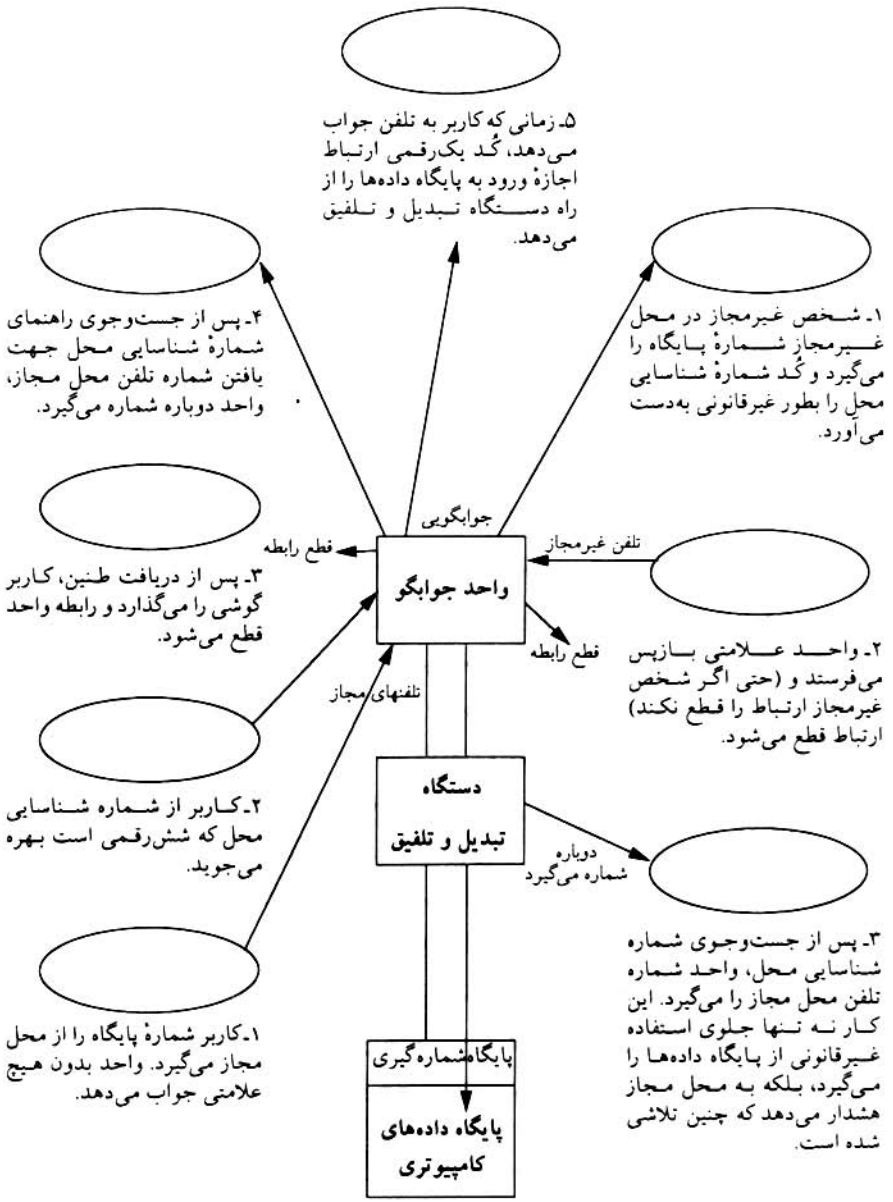
مهارهای خرابی رایانه. جملهٔ: "پوزش می‌خواهم، رایانه خراب است" برای بسیاری از کاربران نهایی بیانی آشناست. رایانه به دلایل متعدد از کار می‌افتد ــ از جمله قطع برق، خرابی مدارهای الکترونیکی، خرابی مکانیکی تجهیزات جانبی، خطاهای پنهان برنامه‌ای و خطاهای کارور رایانه. بخش خدمات اطلاع‌رسانی نوعاً گام‌هایی برای جلوگیری از خرابی‌های تجهیزات و به حداقل رساندن آثار زیانبخش آنها برمی‌دارد ــ مثلاً، احتمال دارد به رایانه‌هایی با توانایی‌های نگهداری خودکار یا از راه دور نیاز باشد. می‌توان برنامه نگهداری پیشگیرانه سخت‌افزاری تهیه کرد. مقدار برق کافی، تهویه، رطوبت و استانداردهای جلوگیری از آتش‌سوزی باید تنظیم شود. می‌توان قدرت نظام رایانه‌ای پشتیبان را با سایر سازمان‌های استفاده‌کننده از رایانه هماهنگ و تنظیم کرد. تغییرات عمده سخت‌افزاری یا نرم‌افزاری را باید به‌دقت برنامه‌ریزی و اجرا کرد تا از مشکلات جلوگیری به عمل آید. سرانجام، کاروران رایانه باید به حد کافی تعلیم دیده باشند و بر کار آنان نظارت شود.

بسیاری از سازمان‌ها، نظام‌های رایانه‌ای بردبار در برابر خطا تهیه می‌کنند تا از معایب احتمالی دوری کنند. این نظام‌ها دارای پردازشگرهای مرکزی چندگانه، ابزارهای جانبی و نرم‌افزارند. این کار احتمالاً توان مصونیت از عیب را در جاهایی که رایانه باید مدام کار کند فراهم می‌سازد، حتی اگر خرابی نرم‌افزاری یا سخت‌افزاری عمده‌ای بروز کند.

مهارهای ارتباطات دوربرد. پردازشگرهای ارتباطات دوربرد و نرم‌افزارهای کنترلی نقشی بزرگ در نظارت بر فعالیت ارتباطی بازی می‌کند. افزودن بر این، داده‌ها می‌تواند به شکل به هم‌ریخته یا منظم توسط نظام رایانه‌ای به کاربران مجاز انتقال یابد. این مهم فرایند "پنهانی" [رمزگذاری[1]] خوانده می‌شود. در این فرایند داده‌های رقمی، پیش از انتقال، به رمزی به هم ریخته بدل می‌شود و آن گاه، هنگام دریافت داده‌ها رمزگشایی می‌گردد. جهت انجام این کار به سخت‌افزار و نرم‌افزار ویژه‌ای نیاز است. روش‌های نظارتی دیگری هم نظیر قطع خودکار دستگاه و نظام فراخوان مجدد ـ مانند تصویر ۵ ـ به کار می رود.

بیمه. برای پشتیبانی از سازمان‌های استفاده‌کننده از رایانه، پوشش بیمهٔ کافی باید تدارک دیده شود. به‌هنگام بروز حوادث، بلایا، تقلب و دیگر خطاها، زیان‌های مالی می‌تواند چشمگیر باشد. بسیاری از شرکت‌های بیمه سیاست‌های ایمنی رایانه‌ای خاصی عرضه می‌دارند. این خدمات شامل بیمهٔ آتش‌سوزی، بلاهای طبیعی، خرابکاری و دزدی؛ تعهد در برابر جبران زیان‌های حاصل از خطاها، یا حذف‌های داده‌پردازی؛ تضمین حمایت از کارکنان خدمات

1. encryption


۵ـ زمانی که کاربر به تلفن جواب می‌دهد، کُد یک‌رقمی ارتباط اجازهٔ ورود به پایگاه داده‌ها را از راه دستگاه تبدیل و تلفیق می‌دهد.
۴ـ پس از جست‌وجوی راهنمای شمارهٔ شناسایی محل جهت یافتن شماره تلفن محل مجاز، واحد دوباره شماره می‌گیرد.
۱ـ شخص غیرمجاز در محل غیرمجاز شمارهٔ پایگاه را می‌گیرد و کُد شمارهٔ شناسایی محل را بطور غیرقانونی به‌دست می‌آورد.
جوابگویی
فطع رابطه
تلفن غیرمجاز
واحد جوابگو
۳ـ پس از دریافت طنین، کاربر گوشی را می‌گذارد و رابطه واحد قطع می‌شود.
قطع رابطه
۲ـ واحد علامتی بازپس می‌فرستد و (حتی اگر شخص غیرمجاز ارتباط را قطع نکند) ارتباط قطع می‌شود.
تلفنهای مجاز
۲ـ کاربر از شماره شناسایی محل که شش‌رقمی است بهره می‌جوید.
دستگاه
تبدیل و تلفیق
دوباره شماره می‌گیرد
۳ـ پس از جست‌وجوی شماره شناسایی محل، واحد شماره تلفن محل مجاز را می‌گیرد. این کار نه تنها جلوی استفاده غیرقانونی از پایگاه داده‌ها را می‌گیرد، بلکه به محل مجاز هشدار می‌دهد که چنین تلاشی شده است.
۱ـ کاربر شمارهٔ پایگاه را از محل مجاز می‌گیرد. واحد بدون هیچ علامتی جواب می‌دهد.
پایگاه شماره گیری
پایگاه داده‌های کامپیوتری

اطلاع‌رسانی در برابر ریاکاری و تقلب است. میزان این گونه بیمه‌ها باید به حدکافی زیاد باشد تا بتوان تجهیزات و امکانات رایانه‌ای را جایگزین کرد. برای هزینه بازسازی بایگانی‌های داده‌ها و برنامه‌ها هم بیمه‌هایی وجود دارد.

مهارهای محاسبه کاربر نهایی

همهٔ سازمان‌ها اقداماتی به عمل می‌آورند تا از کیفیت و ایمنی درخواست‌های کاربرنهایی اطمینان حاصل کنند. اما، آنچه بسیاری از سازمان‌ها دریافته‌اند این نکته است که در مواردی بسیار درخواست‌های کاربرنهایی به کارکردهای بسیار مهمی مربوط است. این درخواست‌ها پشتیبان دستاوردها یا فعالیت‌های مهمی است که برای توفیق و بقای آن سازمان حیاتی است.سازمان‌ها سعی می‌کنند خود را از معایب و حوادث و بلایا دور نگه‌دارند تا بتوانند پاسخگوی درخواست‌های حیاتی باشند. چه کسی در نهایت مسئول است تا از نظارت کامل اِعمال شده در سازمان برای درخواست‌های مهم اطمینان حاصل کند؟ بی‌گمان مدیران بخش کاربرنهایی این مسئولیت را برعهده دارند.

مهار هزینه‌های نظام‌های اطلاع‌رسانی

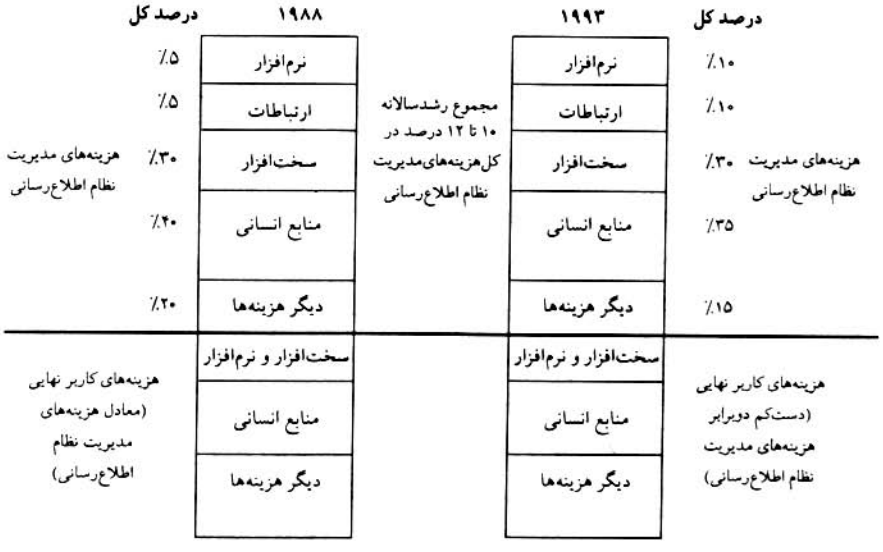
فراهم ساختن و کاربرد منابع نظام‌های اطلاع‌رسانی هزینهٔ بسیاری می‌طلبد. آن گونه که از تصویر ۶ برمی‌آید، هزینه‌های محاسبه کاربرنهایی استثنا به‌شمار نمی‌آید. هزینهٔ سخت‌افزار همواره بخش عمده‌ای از مخارج اطلاع‌پردازی بوده است، اما مدام در حال افزایش است. از سوی دیگر، هزینهٔ نرم‌افزاری هم افزایش پیدا می‌کند. هزینه‌های نرم‌افزاری شامل حقوق برنامه‌نویسان و کسانی است که برنامه‌های مخلی را طراحی می‌کنند و نیز هزینهٔ بسته‌های نرم‌افزاری تهیه شده در خارج از سازمان است. راه دیگر، عنایت به هزینه‌های منابع نظام‌های اطلاع‌رسانی، و میزان هزینه‌های نیروی انسانی را در برمی‌گیرد. این مخارج شامل حقوق تحلیگران نظام‌ها، برنامه‌نویسان، کاروران و کارکنان اداری است. تصویر ۶ نشان می‌دهد که هزینه‌های کارکنان نیز بخش هزینه‌بری در تدارک خدمات نظام اطلاع‌رسانی است.

افزایش هزینه‌های نرم‌افزاری و کارمندی به رشد مخارج تهیه و نگهداری کاربردهای رایانه‌ای تازه وابسته است. علت آن است که حقوق تحلیگران و برنامه‌نویسان نظام، بخش چشمگیری از هزینه‌های خدمات رایانه‌ای را تشکیل می‌دهد. میزان چنین هزینه‌هایی یکی از دلایل عمده روند روی آوردن به سوی خرید بسته‌های نرم‌افزاری در فرایند ایجاد و برنامه‌نویسی نظام‌هاست. بدین‌سان، هزینه تدارک خدمات رایانه‌ای یکی از مخارج عمدهٔ عملیاتی سازمان‌های استفاده

کننده از رایانه شده است. لذا، اگر بنا باشد بر هزینه‌های رایانه‌ای نظارت شود، به برنامهٔ مهار هزینهٔ مفصلی نیاز است.

مهار هزینه‌های توسعهٔ نظام

هزینه‌های توسعه نظام‌ها را باید با برنامه رسمی طرح مدیریت مهار کرد. برای نظارت بر هزینه و جهت طرح توسعه نظام‌ها، ترکیبی از برنامه‌ها، بودجه‌ها، زمان‌بندی و فنون گزارش‌دهی به کار می‌رود. برخی کاربران رایانه بهره‌جویی از برنامه‌نویسی قراردادی یا خدمات طرح نظام‌ها را از سوی کارشناسان خارج از سازمان به صرفه‌تر می‌شمارند تا استخدام کارکنان اضافی لازم برای عرضهٔ چنین خدماتی. سازمان‌هایی دیگر خرید یا اجارهٔ بسته‌های نرم‌افزاری را روش ارزان‌تری برای توسعه نظام‌ها می‌دانند.



تصویر ۶. روند رشد مورد انتظار در هزینه‌های نظام اطلاع‌رسانی

مهار هزینه‌های عملیات رایانه‌ای

برای مهار هزینه‌های عملیات رایانه‌ای فنون متعددی به کار می‌رود. نظام رسمی بازگشت هزینه یکی از فنون عمدهٔ نظارتی است. تمام هزینه‌های صرف شده باید ثبت، گزارش، و توزیع شود و از کاربران خاص رایانه دریافت گردد. با چنین شرایطی، بخش خدمات رایانه‌ای "مرکزی خدماتی" می‌شود که هزینه‌هایش مستقیم از کاربران رایانه دریافت می‌گردد، نه اینکه با دیگر هزینه‌های اداری و خدماتی جمع گردد و به منزلهٔ هزینه سرانه با آن رفتار کنند. می‌توان از دیده‌بان‌های عملکرد نظام برای نظارت و تخصیص هزینه‌های بهره‌جویی از منابع نظام رایانه‌ای سود جست. این دیده‌بان‌ها گزارش‌هایی شامل آمارهای مفصل مربوط به استفاده از منابع نظام، نظیر زمان استفاده از پردازشگر، ظرفیت حافظه، ابزارهای دروندادی/بروندادی و برنامه‌های نظام و کاربردی را فراهم می‌سازد. مدیران عملیاتی از این گزارش‌ها برای برنامه‌نویسی و مهار تخصیص کارآمد منابع نظام رایانه‌ای برای دیگران سود می‌برند. همچنین به عنوان مبنای محاسبهٔ هزینه و نظام‌های بازگشت آن می‌توان از آنها استفاده کرد.

در نهایت، دریافته‌اند که خدمات برونی، که به همت شرکت‌های ادارهٔ تسهیلات، یک‌پارچه‌سازان نظام‌ها و اداره‌های خدمات رایانه‌ای انجام می‌شود، روش ارزان‌تری برای عملیات رایانه‌ای و توسعه نظام‌ها برای برخی سازمان‌های بهره‌جو از رایانه است. این سازمان‌ها چنین خدماتی را روشی سرنوشت‌ساز برای تعیین و کاهش هزینه‌های نظام‌های اطلاع‌رسانی یافته‌اند. به هر حال، چنین مهار هزینه‌هایی باید با زبان مهار عملیاتی روزبه‌روز بر منابع نظام اطلاع‌رسانی سازمان، در کفه‌های ترازو نهاده شود.

ایمنی نظام‌های اطلاع‌رسانی

بی‌گمان یکی از مهم‌ترین ملاحظات مربوط به توسعه و عملکرد مداوم نظام اطلاع‌رسانی، ایمنی است. هر چه نظام‌ها بیشتر به سوی پیوسته شدن پیش‌روند. افراد بیشتری به نظام دسترسی پیدا می‌کنند. هر سازمانی باید بی‌نهایت دقت کند تا به یکپارچگی نظام آن لطمه وارد نیاید. سازمان، به همین‌سان، باید مراقب "موتور" نظام اطلاع‌رسانی، یعنی رایانه، باشد.

نظام اطلاع‌رسانی نقاط آسیب‌پذیر بسیار دارد و بیش از اندازه در معرض نادیده گرفتن تهدیدهای به خطر اندازندهٔ ایمنی نظام اطلاع‌رسانی و مرکز رایانه است. این تهدیدها صورت‌های مختلفی به خود می‌گیرد: از جمله جرایم مدیران، بلایای طبیعی (چون زمین لرزه و سیل)، ویرانگری و بی‌دقتی. جرایم مدیران وجود و واقعیت دارد و در بسیاری جاها به آنها رسیدگی نمی‌شود. این جرایم پیچیده است و به دست مجرمان ماهر انجام می‌شود و فراتر از حدّ

برآورد است. بسیاری از جرایم رایانه‌ای ناشناخته است و اغلب گزارش نمی‌شود. در این قسمت به اقدامات امنیتی لازم جهت خنثی‌کردن تهدیدهای نظام اطلاع‌رسانی یا مرکز رایانه می‌پردازیم. نقاط آسیب‌پذیر مرکز رایانه هر سازمانی عبارت است از سخت‌افزار، نرم‌افزار پایگاه‌های داده‌ها/بایگانی‌ها، ارتباطات داده‌ها و کارکنان.

سخت‌افزار. اگر سخت‌افزار معیوب شود، نظام اطلاع‌رسانی از کار می‌افتد. تهدید از کارافتادگی را می‌توان با دوراندیشی‌های ایمنی که از دستیابی کارکنان غیرمجاز به نظام جلوگیری می‌کند، به حداقل رساند. شیوه‌های معمول ایمنی شامل استفاده از تلویزیون مدار بسته، دستگاه‌های هشداردهنده، ابزارهایی که به کمک رایانه نشانه‌های شناسایی کارمند را وارسی می‌کند، اثر انگشت و غیره است. همچنین تا حد امکان مرکز رایانه باید از محل رفت‌وآمد عابران پیاده دور باشد. برای فرونشاندن آتش باید از مواد شیمیایی استفاده کرد، چه آب بایگانی‌ها و تجهیزات را معیوب می‌سازد.

رایانه‌ها، به‌ویژه رایانه‌های بزرگ، باید منبع نیروی برق مستمر داشته باشد. بسیاری از مراکز رایانه منبع نیروی برقی قطع ناشدنی به کار می‌گیرند. نیروی ضعیف و نامناسب باعث بروز خطا در انتقال داده‌ها و اجرای عملیات می‌شود. در نظامی که از منبع نیروی قطع ناشدنی بهره می‌جویند. نیروی لازم از باطری گرفته می‌شود. اگر برق خارج از مرکز قطع شود، این دستگاه ادامهٔ کار رایانه را برای مدتی تضمین می‌کند، تا فناوران به وصل برق پردازند.

نرم‌افزار. نرم‌افزار نظام اطلاع‌رسانی را می‌توان تعدیل و اصلاح کرد. برای به حداقل رساندن فرصت انجام جرایم با رایانه، مهار شدید نرم‌افزار و اسناد نظام ضروری است. راه‌کارهای مهاری عملیاتی درونساخت نظام اطلاع‌رسانی مدام بر درستی پردازش‌ها نظارت دارد. شاید بهترین راه حفاظت برنامه‌ها از سوء استفاده‌های غیرقانونی، استفاده از راه‌کارهای کنترلی متغیر باشد که تعدیل برنامه‌ها به منظور استفادهٔ شخصی را بسیار مشکل می‌کند.

پایگاه‌های داده‌ها/بایگانی‌ها. پایگاه داده‌ها حاوی مواد خام اطلاعات است. اغلب پایگاه‌های داده‌ها/بایگانی‌ها به منزلهٔ جانمایهٔ سازمان است. وجود چندین نسل از برنامه‌های پشتیبان بایگانی‌ها، به حد کافی سالم ماندن پایگاه‌ها را تضمین نمی‌کند. بایگانی‌های مادر و پشتیبان باید در صندوق‌های نسوز و در اتاقی مجزا، حتی در ساختمانی جداگانه، نگهداری شود.

ارتباطات داده‌ها. صِرف وجود توانایی‌های ارتباطات داده‌ها، جایی که داده‌ها از طریق پل‌های ارتباطی از رایانه‌ای به رایانه دیگر منتقل می‌شود، تهدیدی برای امنیت به شمار می‌رود. مجرمی آگاه می‌تواند از راه دور به نظام دست یابد و از آن سوء استفادهٔ شخصی کند. در یک نظام برخوردار از طرحی پیچیده، این کار آسان نیست، اما می‌تواند آسان شود و انجام پذیرد. برخی

سازمان‌ها از رمزنگاری برای به هم ریختن پیام‌های ارسالی از مجراهای ارتباط داده‌ها استفاده می‌کنند. کسی که بطور غیرقانونی به این پیام‌ها دست یابد، جز سلسله نویسه‌های[1] بی‌معنا چیزی نخواهد یافت. رمزنگاری مشابه استفاده از کتابچهٔ رمز است که برخی جاسوسان یا دست‌اندرکاران امور سرّی از آن بهره می‌جویند. اما، به جای کتابچهٔ رمز، "کلیدی" در سخت‌افزار رمزنگاری /رمزگشایی تعبیه می‌شود تا پیام به هم ریخته را مرتب سازد. فرستنده و گیرندهٔ پیام هر دو آن کلید را دارند که در واقع الگوریتمی است که ساختار پیام را دوباره مرتب می‌کند.

کارکنان. بزرگترین تهدید برای نظام ایمنی یک سازمان کارمندان آنند. مدیران در استخدام افرادی که مجاز به بهره‌جویی از نظام‌های اطلاع‌رسانی‌اند، دقت بسیاری به عمل می‌آورند. نظام اطلاع‌رسانی بسیاری از سازمان‌ها دارای پیامی است که می‌گوید: "تمامی اطلاعات این نظام محرمانه و خصوصی است" این پیام می‌رساند که اگر کارکنان از این اطلاعات سوء استفاده کنند، اخراج خواهند شد. همچنین فردی ناوارد می‌تواند مانند کسی که ذاتاً شرور است به نظام آسیب رساند.

به طور کلی ایمنی نظام‌های اطلاع‌رسانی را می‌توان به دو دستهٔ ایمنی مادی و منطقی تقسیم کرد. ایمنی مادی به سخت‌افزار، امکانات، صفحه‌های مغناطیسی و دیگر ابزارهایی که می‌تواند به طور غیرقانی مورد سوء استفاده، در معرض دزدی یا نابودی قرار گیرد، اطلاق می‌شود. ایمنی منطقی دورنساخت نرم‌افزار است و تنها به افراد مجاز اجازه استفاده از نظام را می‌دهد. ایمنی منطقی نظام‌های پیوسته عمدتاً از راه اسم رمزها و رمزهای مجاز فراهم می‌شود. تنها به کسانی که باید اطلاعات را به دست آورند اسم رمز و رمزهای مجاز داده می‌شود. گاه رمزهای ایمنی به دست افراد ناباب می‌رسد. حفظ این کلیدها از دسترسی مجرمان رایانه‌ای کار ساده‌ای نیست.

چنانچه ملاحظه شد، در مدیریت، فرایند مهار در نظارت یا حصول اطمینان از مطابقت عملیات انجام شده با آنچه مورد نظر بوده و برنامه‌ریزی شده است، وظیفه‌ای اساسی و مهم به شمار می‌آید. فرایند مهار شامل سنجش نتایج عملیات با هدف‌های مطلوب و برنامه‌ریزی شده، و در صورت لزوم انجام اقدامات اصلاحی به منظور حصول اطمینان از نیل به هدف‌های مورد نظر می‌باشد. در سلسله فرایندهای مدیریت، نظارت را می‌توان از اهم فرایندها دانست، زیرا مسئولیت غایی هر مدیری حفظ نظام سازمانی است و با توجه به اینکه هر نظامی که ساخته دست بشر باشد، چنانچه کنترل نشود، دیر یا زود متلاشی خواهد شد، سرنوشت سازمان عملاً در گرو این فرایند مهم مدیریت است. اصولاً، تجربه نشان داده است که هر نظام ساخته دست

1. characters

انسان بدون نظارت نمی‌تواند مدت درازی دوام داشته و به کار خود ادامه دهد.■

مآخذ

۱. کاظمی، بابک. سیستم اطلاعاتی مدیریت. تهران: پیشرو، ۱۳۶۸.

2. O'Brien, James A. *Management Information Systems: A Managerial End User Perspective.* New Delhi: Galgotia Publication Pvt. Tld., 1991.

3. Long, Larry E. *Management Information Systems.* Englewood Cliffs, New Jersey: Prentice Hall, 1989.