

گزارش عملکرد کتابخانه مرکزی و مرکز اسناد دانشگاه از حیث صیانت از ذخایر علمی و راهبردی کشور

الف) بررسی اقدامات دستگاه اجرایی از حیث سازماندهی ذخایر راهبردی علمی

ردیف	عنوان نرم افزار	نام شرکت	مجوز ها	محل نگهداری سرور
۱	نرم افزار کتابخانه‌ای تحت وب آذرسا	پارس آذرخش	دارای مجوز افتا- مجوز معاونت توسعه و نیروی انسانی دانشگاه	مرکز IT دانشگاه علوم پزشکی کرمان

۱- به منظور حفظ، صیانت و ارتقاء آمادگی زیرساخت‌های مرتبط با ذخایر علمی، آموزشی، پژوهشی و اطلاعاتی در کتابخانه مرکزی و ۱۲ کتابخانه واحد های آموزشی تابعه دانشگاه، مجموعه‌ای از اقدامات فنی، مدیریتی، حفاظتی و پدافندی در چارچوب مدیریت ریسک، تداوم خدمت، صیانت از منابع علمی و آمادگی در برابر تهدیدات طبیعی، فنی، زیستی، انسانی و سایبری معمول شده است.

این اقدامات با هدف افزایش ظرفیت تاب آوری و کاهش آسیب‌پذیری منابع علمی، تضمین دسترسی پایدار اعضای هیئت علمی، دانشجویان و پژوهشگران به منابع اطلاعاتی، پیشگیری از اختلال در سامانه‌های کتابخانه‌ای و ایجاد آمادگی برای پاسخ اضطراری در شرایط بحران دنبال می‌شود.

الف) حفاظت و پایداری زیرساخت‌های اطلاعاتی و ذخایر علمی:

در حوزه زیرساخت‌های اطلاعاتی، کتابخانه مرکزی و ۱۲ کتابخانه واحد های آموزشی تابعه دانشگاه با استفاده از نرم افزار کتابخانه‌ای تحت وب آذرسا، نسبت به ساماندهی، ثبت، بازیابی و مدیریت منابع علمی اقدام نموده و تلاش شده است فرآیندهای کتابخانه‌ای به سمت خدمات الکترونیکی، کاهش وابستگی به اقلام فیزیکی و ارتقاء امنیت داده‌ها هدایت شود.

در این راستا، اقدامات زیر مورد توجه قرار گرفته است:

- ثبت و سازماندهی منابع علمی، پایان‌نامه‌ها، رساله‌ها، کتاب‌ها در نرم افزار کتابخانه‌ای تحت وب آذرسا
- حرکت به سمت دریافت و نگهداری نسخه‌های الکترونیکی منابع دانشگاهی، به‌ویژه پایان‌نامه‌ها و رساله‌ها، به جای اتکای صرف به حامل‌های فیزیکی مانند CD و DVD
- کاهش آسیب‌پذیری منابع دیجیتال از طریق ذخیره‌سازی منظم، تهیه نسخه پشتیبان و مدیریت دسترسی کاربران
- تقویت فرآیندهای بازیابی اطلاعات و جلوگیری از وابستگی صرف به نسخه‌های فیزیکی آسیب‌پذیر
- هماهنگی با واحدهای فناوری اطلاعات دانشگاه برای پشتیبانی از سامانه‌ها، سرورها، شبکه و امنیت اطلاعات

این رویکرد علاوه بر حفاظت از منابع علمی، موجب ارتقاء بهره‌وری، کاهش هزینه‌های نگهداری، افزایش سرعت دسترسی و کاهش مخاطرات زیست محیطی شده است.

ب) مدیریت ریسک و شناسایی تهدیدات مؤثر بر کتابخانه و ذخایر علمی:

در کتابخانه مرکزی، تهدیدات مؤثر بر منابع و زیرساخت‌های علمی در چند گروه اصلی مورد توجه قرار می‌گیرد:

- تهدیدات طبیعی مانند زلزله، سیل، طوفان، گردوغبار، رطوبت، آتش‌سوزی و نوسانات دمایی
- تهدیدات فنی و زیرساختی مانند قطعی برق، خرابی تجهیزات، اختلال در شبکه، آسیب به سرورها و تجهیزات ذخیره‌سازی
- تهدیدات سایبری مانند دسترسی غیرمجاز، تخریب داده‌ها، بدافزارها، باج‌افزارها و اختلال در سامانه‌های نرم‌افزاری
- تهدیدات انسانی مانند خطای کاربری، جابه‌جایی نادرست منابع، فقدان کنترل دسترسی، سرقت یا آسیب عمدی و غیرعمدی
- تهدیدات زیستی و بهداشتی مانند همه‌گیری‌ها، آلودگی منابع فیزیکی و محدودیت‌های حضور کاربران در فضای کتابخانه.

بر همین اساس، برنامه‌ریزی کتابخانه صرفاً محدود به حفاظت فیزیکی از منابع نبوده، بلکه ترکیبی از حفاظت فیزیکی، حفاظت دیجیتال، امنیت اطلاعات، تداوم خدمت و مدیریت بحران را شامل می‌شود.

ج) اقدامات پیشگیرانه در برابر آسیب به منابع فیزیکی و دیجیتال:

در بخش منابع فیزیکی، اقدامات حفاظتی شامل کنترل شرایط محیطی، ساماندهی مخازن، رعایت اصول نگهداری منابع، کنترل رطوبت و دما، پیشگیری از آتش‌سوزی، استفاده از تجهیزات ایمنی و جلوگیری از تراکم یا انباشت غیراستاندارد منابع است.

در بخش منابع دیجیتال نیز مهم‌ترین اقدامات عبارت‌اند از:

- تهیه نسخه‌های پشتیبان منظم از داده‌ها و اطلاعات کتابخانه‌ای
- نگهداری نسخه‌های پشتیبان در محل‌های امن و ترجیحاً جدا از محل اصلی داده‌ها
- تعیین سطح دسترسی کاربران، کارشناسان و مدیران سامانه‌ها
- به‌روزرسانی نرم‌افزارها و هماهنگی با واحد فناوری اطلاعات برای کاهش آسیب‌پذیری‌های امنیتی
- پایش دوره‌ای صحت اطلاعات و امکان بازیابی داده‌ها؛
- مستندسازی فرآیندهای فنی، اداری و کتابخانه‌ای برای جلوگیری از وابستگی به افراد خاص.

از منظر علمی، تداوم دسترسی به منابع اطلاعاتی زمانی پایدار خواهد بود که داده‌ها در برابر سه تهدید اصلی یعنی حذف، تخریب و عدم دسترسی محافظت شوند. بنابراین، ترکیب پشتیبان‌گیری، کنترل دسترسی، مستندسازی و آموزش نیروی انسانی از اجزای اصلی صیانت از ذخایر علمی محسوب می‌شود.

د) طرح راهبری عملیات مقابله و پاسخ اضطراری جامع و ترکیبی:

برای مواجهه با شرایط اضطراری، رویکرد کتابخانه مرکزی باید بر مبنای یک طرح جامع و ترکیبی استوار باشد؛ به این معنا که عملیات پاسخ تنها محدود به یک نوع بحران نباشد، بلکه بتواند هم‌زمان با تهدیدات فیزیکی، سایبری، زیرساختی و انسانی مقابله کند.

این طرح می‌تواند در چهار مرحله اصلی راهبری شود:

الف. مرحله پیشگیری و آمادگی

در این مرحله، تمرکز بر کاهش احتمال وقوع بحران و افزایش آمادگی سازمانی است. اقدامات اصلی شامل شناسایی دارایی‌های حیاتی کتابخانه، طبقه‌بندی منابع ارزشمند، تعیین اولویت‌های حفاظت، آموزش کارکنان، تهیه دستورالعمل‌های اضطراری، تست نسخه‌های پشتیبان و هماهنگی با واحدهای پشتیبان دانشگاه است.

ب. مرحله هشدار و فعال‌سازی پاسخ اضطراری

در صورت بروز نشانه‌های تهدید، مانند قطعی گسترده برق، اختلال سامانه‌ای، آتش‌سوزی، نفوذ سایبری، نشت آب، آسیب به مخزن یا بحران بهداشتی، سازوکار اطلاع‌رسانی سریع فعال می‌شود. در این مرحله باید مشخص باشد چه فرد یا واحدی مسئول اعلام وضعیت، چه کسی مسئول تصمیم‌گیری و چه بخش‌هایی مسئول اقدام فوری هستند.

ج. مرحله مقابله و کنترل بحران

در این مرحله، اقدامات عملی برای کاهش خسارت انجام می‌شود؛ از جمله حفاظت از منابع اولویت‌دار، قطع دسترسی‌های مشکوک، انتقال منابع آسیب‌پذیر، فعال‌سازی نسخه‌های پشتیبان، محدودسازی دسترسی فیزیکی یا دیجیتال، هماهنگی با حراست، فناوری اطلاعات، تأسیسات، آتش‌نشانی، پدافند غیرعامل و مدیریت بحران دانشگاه.

د. مرحله بازیابی، ارزیابی و بازگشت به وضعیت عادی

پس از کنترل بحران، بازیابی خدمات کتابخانه‌ای آغاز می‌شود. این مرحله شامل بررسی میزان خسارت، بازیابی داده‌ها، بازگشایی تدریجی خدمات، اصلاح نقاط ضعف، تکمیل گزارش حادثه، به‌روزرسانی دستورالعمل‌ها و آموزش مجدد کارکنان است. هدف اصلی این مرحله، بازگشت سریع، ایمن و کنترل‌شده به شرایط عادی و جلوگیری از تکرار آسیب است.

ه. سازماندهی ساختارها و تقسیم وظایف در شرایط اضطراری

برای ارتقاء هماهنگی و هم‌افزایی عملیات اجرایی، ضروری است ساختار پاسخ اضطراری کتابخانه به‌صورت مشخص و قابل اجرا تعریف شود. در این ساختار، نقش‌ها و مسئولیت‌ها باید از پیش تعیین شده باشند تا در زمان بحران، تصمیم‌گیری و اقدام دچار تأخیر نشود.

ساختار پیشنهادی می‌تواند شامل بخش‌های زیر باشد:

- مسئول راهبری بحران کتابخانه: معمولاً رئیس یا مدیر کتابخانه مرکزی که وظیفه هماهنگی کلی، تصمیم‌گیری و ارتباط با مدیریت دانشگاه را بر عهده دارد.
- گروه حفاظت از منابع علمی: مسئول شناسایی، اولویت‌بندی، انتقال یا صیانت از منابع ارزشمند، پایان‌نامه‌ها، اسناد و منابع مرجع.
- گروه فناوری اطلاعات و سامانه‌ها: مسئول پایداری سامانه‌های کتابخانه‌ای، پشتیبان‌گیری، بازیابی داده‌ها، کنترل دسترسی و مقابله با تهدیدات سایبری.
- گروه ایمنی، تأسیسات و پشتیبانی: مسئول کنترل خطرات فیزیکی مانند آتش، آب‌گرفتگی، قطعی برق، تهویه، دما، رطوبت و ایمنی محیط.
- گروه اطلاع‌رسانی و خدمات کاربران: مسئول اطلاع‌رسانی به کاربران، مدیریت خدمات جایگزین، پاسخگویی به مراجعان و کاهش اختلال در خدمات آموزشی و پژوهشی.

- گروه مستندسازی و ارزیابی: مسئول ثبت اقدامات انجام شده، تهیه گزارش حادثه، تحلیل نقاط ضعف و ارائه پیشنهاد اصلاحی.

این تقسیم وظایف باعث می شود که عملیات مقابله با بحران از حالت فردمحور خارج شده و به شکل سازمان یافته، قابل پیگیری و قابل ارزیابی اجرا شود.

(و) ارتقاء هماهنگی و هم افزایی بین واحدهای اجرایی

از آنجا که حفاظت از ذخایر علمی صرفاً وظیفه کتابخانه نیست، بلکه به زیرساخت های فناوری، اداری، حفاظتی، تأسیساتی و مدیریتی دانشگاه وابسته است، هماهنگی میان بخشی اهمیت ویژه ای دارد.

در این زمینه، تعامل کتابخانه مرکزی با واحدهای زیر ضروری و معمول است:

- مدیریت فناوری اطلاعات دانشگاه برای پشتیبانی نرم افزاری، امنیت شبکه، پشتیبان گیری و بازیابی داده ها؛
- مدیریت حراست برای کنترل دسترسی، حفاظت فیزیکی و مدیریت تهدیدات انسانی؛
- واحد تأسیسات و خدمات برای کنترل برق، سیستم های سرمایش و گرمایش، ایمنی مخازن و پیشگیری از حوادث محیطی؛
- مدیریت پدافند غیرعامل و مدیریت بحران دانشگاه برای هماهنگی در شرایط اضطراری؛
- معاونت تحقیقات و فناوری و حوزه آموزش برای صیانت از پایان نامه ها، رساله ها و دستاوردهای پژوهشی؛
- واحد بهداشت، ایمنی و محیط زیست برای رعایت اصول ایمنی، سلامت محیط و اداره سبز.

این هماهنگی موجب می شود که کتابخانه در زمان بحران، به صورت منفرد عمل نکند و از ظرفیت کل دانشگاه برای حفاظت از منابع علمی استفاده شود.

(ز) آموزش، تمرین و ارتقاء آمادگی کارکنان

یکی از ارکان اصلی آمادگی در برابر تهدیدات، آموزش نیروی انسانی است. حتی پیشرفته ترین سامانه ها نیز بدون نیروی انسانی آگاه، اثربخشی لازم را نخواهند داشت. بنابراین، آموزش کارکنان کتابخانه در زمینه های زیر اهمیت دارد:

- نحوه اقدام در زمان آتش سوزی، زلزله، آب گرفتگی یا قطعی برق؛
- اصول اولیه حفاظت از منابع آسیب دیده؛
- نحوه گزارش سریع حوادث و تهدیدات؛
- رعایت امنیت اطلاعات و پیشگیری از خطاهای کاربری؛
- مدیریت دسترسی به سامانه ها و داده های کتابخانه ای؛
- نحوه ارائه خدمات جایگزین در شرایط اختلال یا تعطیلی فیزیکی کتابخانه.

همچنین اجرای مانورهای دوره ای، ارزیابی آمادگی کارکنان و بازنگری دستورالعمل ها پس از هر تمرین یا حادثه، نقش مؤثری در افزایش تاب آوری کتابخانه دارد.

ح) تداوم خدمات کتابخانه‌ای در شرایط بحران

از آنجا که کتابخانه مرکزی نقش پشتیبان آموزش، پژوهش و درمان را در دانشگاه علوم پزشکی بر عهده دارد، توقف کامل خدمات آن می‌تواند بر فعالیت‌های علمی و دانشگاهی اثرگذار باشد. به همین دلیل، تداوم خدمت یکی از اصول مهم در مدیریت بحران کتابخانه است.

برای تحقق این هدف، اقدامات زیر اهمیت دارد:

- تقویت خدمات الکترونیکی و دسترسی غیرحضور به منابع؛
- استفاده از سامانه‌های کتابخانه‌ای برای جست‌وجو، امانت، تمدید و مدیریت منابع؛
- فراهم‌سازی امکان دسترسی به منابع دیجیتال و پایگاه‌های اطلاعاتی؛
- حفظ نسخه‌های الکترونیکی پایان‌نامه‌ها و منابع پژوهشی؛
- تدوین شیوه‌نامه ارائه خدمات حداقلی در شرایط اضطراری؛
- اطلاع‌رسانی سریع به کاربران درباره وضعیت خدمات، محدودیت‌ها و مسیرهای جایگزین.

این اقدامات سبب می‌شود که حتی در صورت محدودیت دسترسی فیزیکی به کتابخانه، پشتیبانی علمی و اطلاعاتی از جامعه دانشگاهی ادامه یابد.

ت) ارتباط اقدامات با اداره سبز و کاهش آسیب‌پذیری محیطی

یکی از ابعاد مهم ارتقاء زیرساخت‌های ذخایر علمی، حرکت از نگهداری فیزیکی پر هزینه و آسیب‌پذیر به سمت مدیریت دیجیتال منابع است. حذف یا کاهش دریافت لوح‌های فشرده، کاهش مصرف پلاستیک، کاهش نیاز به فضای فیزیکی، کاهش پسماند الکترونیکی و جایگزینی تحویل الکترونیکی پایان‌نامه‌ها و رساله‌ها، علاوه بر مزایای زیست‌محیطی، از منظر پدافندی نیز قابل دفاع است. زیرا حامل‌های فیزیکی مانند CD و DVD در برابر شکستگی، فساد داده، مفقودی، ناسازگاری سخت‌افزاری و فرسودگی بسیار آسیب‌پذیر هستند؛ در حالی که نگهداری الکترونیکی استاندارد، همراه با پشتیبان‌گیری و کنترل دسترسی، امکان حفاظت بهتر، بازیابی سریع‌تر و مدیریت علمی‌تر منابع را فراهم می‌سازد.

۲- تبیین رویکردهای پیش‌بینانه، رصد، پایش و تشخیص زودهنگام در کتابخانه مرکزی در راستای ارتقاء ضریب امنیت پدافندی و صیانت پیشگیرانه از ذخایر علمی دانشگاه علوم پزشکی کرمان، رویکرد اصلی کتابخانه مرکزی از «پاسخ‌گویی انفعالی پس از بحران» به «پیش‌بینی، پایش مداوم و تشخیص زودهنگام مخاطرات» تغییر یافته است. اقدامات و رویکردهای اجرایی معمول‌شده در این حوزه قبل از وقوع هرگونه حادثه، در سه محور اصلی به شرح زیر تبیین می‌گردد:

۱. پایش سایبری و رصد هوشمند سامانه‌های اطلاعاتی (دیجیتال)

با توجه به تمرکز ذخایر علمی در سامانه‌های نرم‌افزاری (نظیر نرم‌افزار جامع کتابخانه‌ای آذرسا و پورتال‌های پژوهشی)، فرآیند رصد پیش‌بینانه به صورت مستمر و با همکاری مدیریت آمار و فناوری اطلاعات دانشگاه انجام می‌شود:

- پایش ترافیک شبکه و تشخیص نفوذ: رصد مداوم درگاه‌های ورودی سامانه‌ها جهت شناسایی رفتارهای غیرعادی کاربری، تلاش‌های ناموفق مکرر برای ورود و نشانه‌های اولیه حملات باج‌افزاری یا سایبری پیش از وقوع تخریب داده‌ها.

- پایش سلامت دیتابیس و سرورها: بررسی مداوم لاگ‌های سیستم، فضای دیسک سرورها، و میزان مصرف منابع سخت‌افزاری برای پیش‌بینی و پیشگیری از خرابی یا Crash ناگهانی سرورهای کتابخانه.
- سنجش دوره‌ای و خودکار آسیب‌پذیری‌ها: ارزیابی دوره‌ای امنیتی نرم‌افزارها و به‌روزرسانی وصله‌های امنیتی سیستم‌عامل‌ها و پورتال‌ها جهت بستن منافذ نفوذ پیش از بهره‌برداری مهاجمان.

۲. پایش محیطی و فیزیکی مخازن و سالن‌های مطالعه

حفظ فیزیکی کتب مرجع، پایان‌نامه‌ها و اسناد پژوهشی نیازمند پایش مداوم فاکتورهای آسیب‌رسان محیطی است:

- سیستم پایش مداوم دما و رطوبت (مراقبت اقلیمی): نصب و کالیبراسیون تجهیزات سنجش دما و رطوبت در مخازن کتابخانه؛ چرا که افزایش ناگهانی رطوبت یا دما، بستر رشد قارچ‌ها، حشرات و پوسیدگی اسناد کاغذی را فراهم می‌کند. تشخیص زودهنگام این نوسانات مانع از تخریب تدریجی منابع می‌شود.
- تجهیزات تشخیص زودهنگام حریق (اعلام حریق هوشمند): سرویس و نگهداری دوره‌ای سنسورهای دود و حرارت در تمامی بخش‌های کتابخانه مرکزی برای شناسایی کوچک‌ترین علائم حریق، پیش از گسترش آن به مخازن اصلی.
- رصد بصری و فیزیکی تاسیسات عبوری: بازدید دوره‌ای کارشناسان تاسیسات از لوله‌های انتقال آب، کانال‌های سرمایشی/گرمایشی و سیم‌کشی‌های برق مجاور مخازن جهت پیش‌بینی و پیشگیری از ترکیدگی لوله‌ها یا اتصال کوتاه برق.

۳. مراقبت‌های بهداشتی، زیستی و پایش سلامت منابع چاپی

با توجه به ماهیت دانشگاه که در حوزه علوم پزشکی فعالیت دارد، مخاطرات زیستی (بیولوژیک) از اهمیت بالایی برخوردار است:

- رصد و مراقبت آفات: اجرای برنامه‌های سم‌پاشی دوره‌ای و تخصصی مخازن کتاب‌ها و فرآیندهای قرنطینه‌سازی کتاب‌های اهدایی یا مستعمل خارجی پیش از ورود به مخزن اصلی، جهت جلوگیری از انتقال حشرات کتاب‌خوار (نظیر بید و مورانه).
- کنترل بهداشتی فضاها در مواجهه با اپیدمی‌ها: تدوین شاخص‌های پایش سلامت محیطی و استفاده از تجهیزات ضدعفونی‌کننده هوا و سطوح در دوره‌های شیوع بیماری‌های واگیردار، جهت مراقبت از سلامت کارکنان و مراجعان.

۴. مدیریت ریسک انسانی و پایش دسترسی‌ها

- کنترل و مانیتورینگ دسترسی فیزیکی: مجهز بودن مبادی ورودی مخازن به دوربین‌های مداربسته جهت رصد تردد افراد غیرمستول و پیشگیری از خروج غیرمجاز یا آسیب به کتب.
- تعیین سطوح دسترسی: پایش مستمر دسترسی کارشناسان به پنل‌های مدیریتی نرم‌افزار کتابخانه (آذرسا) و غیرفعال‌سازی سریع دسترسی‌های مازاد یا دسترسی افراد ترخیص‌شده از سازمان جهت پیشگیری از خطای انسانی یا دسترسی‌های غیرمجاز داخلی.

۳- در راستای کاهش حداکثری سطح غافلگیری سازمانی در مواجهه با تهدیدات و به‌منظور مصون‌سازی زیرساخت‌های علمی دانشگاه علوم پزشکی کرمان، اقدامات و رویکردهای عملیاتی کتابخانه مرکزی در حوزه «کاهش نقاط ضعف و ارتقاء آمادگی‌های مقابله» در سه محور کلیدی زیر تبیین و اجرایی می‌گردد:

۱. حذف نقاط ضعف زیرساختی و برطرف کردن آسیب‌پذیری‌های عمده

این رویکرد بر شناسایی فعالانه و مرتفع نمودن گلوگاه‌هایی تمرکز دارد که در صورت وقوع بحران، می‌توانند خسارات را تشدید کنند:

- انتقال داده‌ها از حامل‌های فیزیکی به فضاهای ذخیره‌سازی ابری و تمرکز: یکی از آسیب‌پذیری‌های عمده کتابخانه، نگهداری نسخه‌های پایان‌نامه‌ها و اسناد علمی بر روی لوح‌های فشرده (CD/DVD) بود که به‌شدت در معرض تخریب فیزیکی، شکستگی، سرقت یا زوال اطلاعات قرار داشتند. با حذف تدریجی این حامل‌ها در چارچوب طرح «اداره سبز» و انتقال کامل اطلاعات به سرورهای پشتیبان‌گیری‌شده دانشگاه، این نقطه ضعف عمده به طور کامل برطرف گردید.

- ارتقاء ایمنی فیزیکی مخازن و سازه: بازطراحی چیدمان قفسه‌ها، مقاوم‌سازی اتصالات قفسه‌های کتاب در برابر لرزش‌های زمین‌لرزه.
- به‌روزرسانی و وصله امنیتی سامانه‌های نرم‌افزاری: رفع باگ‌ها و حفره‌های امنیتی نرم‌افزار جامع کتابخانه‌ای آذرسا و سیستم‌های عامل سرورها با هماهنگی مدیریت فناوری اطلاعات دانشگاه جهت پیشگیری از نفوذ باج‌افزارها و هکرها.
- ۲. اقدامات عملیاتی جهت کاهش غافلگیری (کاهش ریسک و افزایش تاب‌آوری)

هدف از این اقدامات، ایجاد لایه‌های دفاعی و افزونگی در خدمات است تا در صورت بروز هرگونه حادثه ناگهانی، جریان ارائه خدمات علمی دچار وقفه کامل نشود:

- پیاده‌سازی استراتژی پشتیبان‌گیری چندلایه: تهیه حداقل ۳ نسخه پشتیبان از داده‌های علمی دانشگاه، روی ۲ نوع رسانه ذخیره‌سازی مختلف، که حداقل ۱ نسخه از آن‌ها در خارج از ساختمان کتابخانه مرکزی نگهداری می‌شود. این اقدام امکان غافلگیری ناشی از نابودی هم‌زمان سرور اصلی و سرور پشتیبان محلی را از بین می‌برد.

- تأمین زیرساخت‌های موازی و اضطراری: تجهیز کتابخانه به سیستم‌های تامین برق اضطراری (UPS) و هماهنگی جهت اتصال به ژنراتور دانشگاه برای جلوگیری از خاموشی ناگهانی سرورهای محلی و کلاینت‌ها، و همچنین پیش‌بینی پهنای باند و مسیرهای ارتباطی شبکه جایگزین جهت تداوم دسترسی مراجعان به پورتال کتابخانه در زمان قطعی شبکه اصلی دانشگاه.

- به‌روزرسانی مستمر سناریوهای تهدید: بازنگری سالانه کاتالوگ مخاطرات کتابخانه متناسب با تکنولوژی‌های جدید و تغییرات کالبدی دانشگاه، به‌منظور پیش‌بینی تهدیدات نوظهور سایبری و زیستی.

- ۳. ارتقای آمادگی‌های مقابله و توان عملیاتی کارکنان
- حتی با وجود قوی‌ترین زیرساخت‌ها، بدون آمادگی نیروی انسانی امکان مقابله موثر وجود نخواهد داشت. در این راستا اقدامات زیر معمول شده است:

- برگزاری مانورها و تمرین‌های دوره‌ای واکنش در شرایط اضطراری: طراحی و اجرای شبیه‌سازی‌های دوره‌ای قطع ناگهانی دسترسی به سامانه‌ها، حملات سایبری فرضی، حریق در مخازن و سناریوهای تخلیه اضطراری منابع ارزشمند جهت سنجش سرعت عمل و آمادگی کارکنان.

- تدوین دستورالعمل‌های عملیاتی استاندارد: نگارش کارت‌های وظیفه ساده و کاربردی برای هر یک از پرسنل کتابخانه در زمان بحران. به طوری که در شرایط اضطراری، هر فرد دقیقاً بداند چه وظیفه‌ای (اعم از قطع برق بخش‌ها، قفل کردن دسترسی‌های شبکه، هدایت مراجعان یا پوشش حفاظتی اسناد خاص) بر عهده اوست.

- ارتقاء هماهنگی ارتباطی با تیم‌های واکنش سریع دانشگاه: ایجاد خطوط ارتباطی سریع و بی‌واسطه با مدیریت حراست، مدیریت آمار و فناوری اطلاعات (برای پشتیبانی فنی آنی) و حوزه خدمات و پشتیبانی دانشگاه جهت به حداقل رساندن زمان پاسخ‌دهی از لحظه وقوع حادثه تا شروع عملیات مهار.

۴- رویکرد عملیاتی پیشدستانه با هدف برهم زدن تمرکز و انصراف دشمن از اقدام و تحمیل اراده خودی بر آن و دستیابی به شرایط و موقعیت‌های بهتر برای نیروهای خودی انجام می‌گیرد.

در ادبیات و اصول پدافند غیرعامل، دفاع سایبری و پدافند چندبعدی، رویکرد عملیاتی که با هدف برهم زدن تمرکز، ایجاد بازدارندگی، انصراف دشمن از اقدام، تحمیل اراده خودی بر او و کسب دست برتر (موقعیت بهتر) برای نیروهای خودی انجام می‌گیرد، تحت عنوان «رویکرد فعال/پیشدستانه» و در سطوح راهبردی‌تر به عنوان «دفاع پیش‌دستانه با قابلیت بازدارندگی شناخته می‌شود.

در بستر سازمان‌های خدماتی و علمی مانند کتابخانه مرکزی و زیرساخت‌های فناوری اطلاعات دانشگاه علوم پزشکی کرمان، این رویکرد عملیاتی از قالب سخت و نظامی خارج شده و در قالب «پدافند غیرعامل پیشدستانه، امنیت سایبری فعال و فریب تاکتیکی» تعریف و پیاده‌سازی می‌شود. اقدامات عملیاتی ذیل نمونه‌هایی از این رویکرد هستند:

۱. پیاده‌سازی تکنولوژی‌های فریب و تله‌گذاری سایبری

یکی از کارآمدترین روش‌ها برای برهم زدن تمرکز مهاجم و انصراف وی از حمله به سرورهای اصلی (مانند سامانه آذرسا یا پایگاه‌های داده پایان‌نامه‌ها) است:

• اقدام عملیاتی: ایجاد سرورها، دیتابیس‌ها و پورتال‌های شبیه‌سازی‌شده و جعلی که در ظاهر حاوی داده‌های حساس هستند اما در واقع تله‌های امنیتی‌اند.

• پیامد عملیاتی: مهاجم وقت، انرژی و منابع خود را صرف حمله به این اهداف کاذب می‌کند (برهم خوردن تمرکز دشمن). در همین حین، تیم امنیت شبکه دانشگاه ضمن شناسایی آی‌پی‌ها، الگوها و ابزارهای نفوذ مهاجم، دسترسی‌های او را مسدود کرده و دفاع خود را تقویت می‌کند (تحمیل اراده خودی و دستیابی به موقعیت بهتر).

۲. پایش تهاجمی منابع تهدید و تهدیدشناسی پیش‌دستانه

به جای انتظار برای شروع حمله و سپس دفاع، سازمان به صورت پیشدستانه به رصد کانون‌های تهدید می‌پردازد:

• اقدام عملیاتی: رصد مستمر فروم‌های هکری، بازارگاه‌های غیرقانونی تبادل داده و پایگاه‌های اطلاعاتی تهدیدات سایبری در سطح جهان برای کشف زودتر از موعد اکسپلویت‌ها و ابزارهایی که ممکن است علیه زیرساخت‌های دانشگاه یا نرم‌افزارهای کتابخانه‌ای به کار گرفته شوند.

• پیامد عملیاتی: با کشف زودهنگام نیت و ابزار مهاجمان و بستن منافذ پیش از آغاز هرگونه عملیات، دشمن متوجه می‌شود که دیوارهای دفاعی پیشاپیش مستحکم شده‌اند؛ این امر منجر به ناامیدی و انصراف وی از اقدام می‌گردد (کسب دست برتر).

۳. مانورهای شبیه‌سازی تهاجمی تست نفوذ جعبه سیاه

تحمیل اراده خودی بر شرایط بحران از طریق شبیه‌سازی واقعی‌ترین سناریوهای نفوذ و تخریب صورت می‌پذیرد:

• اقدام عملیاتی: استخدام هکرها یا کلاه‌سفید (تیم قرمز) جهت حمله واقعی (بدون اطلاع قبلی پرسنل فنی) به سامانه‌های کتابخانه به منظور کشف عمیق‌ترین لایه‌های آسیب‌پذیری فیزیکی و سایبری.

• پیامد عملیاتی: این اقدام ابتکار عمل را کاملاً در اختیار دانشگاه قرار می‌دهد. شناسایی و رفع حفره‌ها در این سناریوها، هرگونه نقشه احتمالی مهاجمان واقعی در آینده را خنثی ساخته و ابتکار عمل را از آن‌ها سلب می‌کند.

۴. اقدامات حقوقی، حفاظتی و بازدارنده در دسترسی به منابع علمی

• اقدام عملیاتی: استفاده از سیستم‌های پیشرفته واترمارک دیجیتال غیرقابل حذف، سیستم‌های ردگیری دانه‌های انبوه و مانیتورینگ هوشمند رفتار کاربران شبکه.

• پیامد عملیاتی: کاربری که قصد استخراج غیرمجاز، سرقت انبوه یا تخریب اسناد علمی را داشته باشد، بلافاصله با رفتارهای بازدارنده سامانه (مانند مسدودسازی خودکار حساب کاربری و ارسال هشدار امنیتی) مواجه می‌شود. این پاسخ سخت و سریع، فرد را از ادامه اقدام تخریبی منصرف می‌سازد.

(ب) بررسی عملیات و اقدامات اجرایی:

۱- برای مدیریت داراییها، مخاطرات، همافزایی آسیب‌پذیریها و وابستگیهای متقابل، در سطح مدیریت استراتژیک و کارشناسی کتابخانه مرکزی، باید از رویکرد «مدیریت یکپارچه ریسک استفاده کرد. در این سطح، ما دیگر به مسائل به صورت تک‌بعدی (فقط حریق یا فقط هک) نگاه نمی‌کنیم، بلکه به دنبال درک چگونگی اثرگذاری یک حادثه بر کل زنجیره ارزش اطلاعات هستیم.

اقدامات معمول‌شده در چهار حوزه ذیل:

۱. مدیریت دارایی‌ها

پیش از مدیریت مخاطره، باید دقیقاً بدانیم چه چیزی برای حفاظت از آن ارزش قائل هستیم. در کتابخانه مرکزی، دارایی‌ها به دو دسته تقسیم شده و طبقه‌بندی می‌شوند:

دارایی‌های فیزیکی: شامل نسخه‌های خطی، اسناد تاریخی، کتاب‌های مرجع، تجهیزات آرشیوی و زیرساخت‌های ساختمانی. این دارایی‌ها بر اساس «ارزش تاریخی و جایگزینی» رتبه‌بندی می‌شوند.

دارایی‌های دیجیتال: شامل پایگاه داده‌های کتابخانه‌ای (آذرسا)، فایل‌های پایان‌نامه، اسناد پژوهشی دیجیتال، سورس‌کدها و زیرساخت‌های شبکه. این دارایی‌ها بر اساس «تداوم خدمات و حساسیت اطلاعات» طبقه‌بندی می‌شوند.

اقدام عملیاتی: ایجاد یک «سیاست ثبت دارایی» که در آن هر دارایی دارای یک کد شناسایی، مکان ذخیره‌سازی، سطح حساسیت و مالک مشخص است.

۲. مدیریت مخاطرات

پس از شناسایی دارایی‌ها، فرآیند شناسایی، ارزیابی و پاسخ به مخاطرات طبق متدولوژی استاندارد انجام می‌شود:

شناسایی: دسته‌بندی تهدیدها به چهار گروه: طبیعی (زلزله، سیل)، تکنولوژیک (خرابی سرور، باج‌افزار)، انسانی (سرقت، تخریب عمدی، خطای اپراتور) و محیطی (رطوبت، حریق).

ارزیابی ریسک: استفاده از ماتریس ریسک برای محاسبه «شدت اثر» در مقابل «احتمال وقوع». (مثلاً ریسک حریق در مخزن کتاب، به دلیل شدت اثر بسیار بالا، حتی با احتمال کم، یک ریسک بحرانی تلقی می‌شود).

استراتژی‌های پاسخ:

پذیرش: برای ریسک‌های بسیار کوچک.

کاهش: از طریق نصب سنسورها و فایروال‌ها.

انتقال: از طریق بیمه کردن اسناد و تجهیزات گران‌قیمت.

اجتناب: تغییر مکان ذخیره‌سازی از زیرزمین به طبقات بالاتر.

۳. مدیریت هم‌افزایی آسیب‌پذیری

در این سطح، ما به دنبال پدیده‌ای هستیم که در آن دو آسیب‌پذیری کوچک، با ترکیب شدن، یک بحران بزرگ ایجاد می‌کنند.

تحلیل هم‌افزایی: بررسی اینکه چگونه یک نقص کوچک می‌تواند منجر به یک فاجعه بزرگ شود.

اقدام عملیاتی: انجام «تحلیل حالت‌های شکست برای شناسایی نقاطی که در آن نقص‌های زنجیره‌ای ممکن است رخ دهد و تقویت آن‌ها.

۴. مدیریت وابستگی‌های متقابل:

در سازمان‌های مدرن، بخش‌ها از هم جدا نیستند؛ هر بخشی به بخش دیگر وابسته است. مدیریت وابستگی‌ها یعنی درک اینکه خرابی در یک بخش، چگونه سایر بخش‌ها را فلج می‌کند:

وابستگی‌های عملیاتی: اگر سیستم شبکه (IT) دچار مشکل شود، سیستم‌های کنترل دما در مخازن (تأسیسات) نیز ممکن است از کار بیفتند؛ این یعنی یک وابستگی حیاتی بین بخش IT و بخش حفاظت فیزیکی.

وابستگی‌های زنجیره‌ای: اگر تأمین‌کننده برق یا شرکت‌های پشتیبانی نرم‌افزار دچار بحران شوند، توان عملیاتی کتابخانه نیز تحت تأثیر قرار می‌گیرد.

اقدام عملیاتی: تدوین «نقشه وابستگی‌های سازمانی» و اطمینان از وجود «استقلال عملیاتی در شرایط بحران» (مانند داشتن سیستم‌های خود کفا که حتی با قطع شبکه اصلی نیز به کار خود ادامه دهند).

۲- به منظور کنترل و کاهش پیامدهای آسیب، توسعه مصونسازی و قابلیت تاب‌آوری، تداوم کارکرد، بازیابی، بازسازی و بازتوانی، باید تأکید نمود که در نظام جامع پدافند غیرعامل کتابخانه مرکزی، تمامی این مراحل در قالب یک «چرخه حیات مدیریت بحران» طراحی و به‌صورت مستند درآمده‌اند. تدابیر اتخاذ شده جهت اطمینان از استمرار خدمات علمی و حفاظتی، در شش لایه عملیاتی زیر دسته‌بندی و اجرا می‌شوند:

۱. کنترل و کاهش پیامدهای آسیب

این مرحله بر محدود کردن دامنه نفوذ حادثه تمرکز دارد:

• بخش‌بندی: ایزوله‌سازی شبکه‌های داده و تقسیم‌بندی فیزیکی مخازن توسط درب‌های ضد حریق و پارتیشن‌های مقاوم، به‌طوری‌که حریق یا نفوذ سایبری در یک بخش، به سایر بخش‌ها سرایت نکند.

• پاسخ فوری خودکار: استقرار سیستم‌های اطفای حریق گازی در اتاق سرور و مخازن نفیس که برخلاف آب، پیامد ثانویه (تخریب اسناد با رطوبت) را به همراه ندارد.

۲. توسعه مصونسازی و تاب‌آوری

تاب‌آوری به معنای توانایی جذب ضربه و ادامه فعالیت است:

• افزونگی: در بخش دیجیتال، استفاده از سیستم‌های سرور کلاستر به شکلی که اگر یک سرور از کار بیفتد، سرور جایگزین بدون توقف خدمات، بار کاری را بر عهده می‌گیرد.

• مصون سازی کالبدی: مقاومت سازی سازه‌ای قفسه‌ها و تجهیزات و همچنین تقویت زیرساخت‌های الکتریکی با استفاده از فیلترهای نوسان گیر و سیستم‌های ارتینگ استاندارد.

۳. تداوم کارکرد:

اطمینان از اینکه «خدمت‌رسانی» به پژوهشگران حتی در زمان بحران متوقف نمی‌شود:

• سایت پشتیبان: نگهداری نسخه‌ای از پایگاه داده‌های پژوهشی در مکانی جغرافیایی متفاوت (سایت معین دانشگاه) تا در صورت نابودی ساختمان کتابخانه، کل تاریخچه علمی دانشگاه قابل بازیابی باشد.

• عملیات دستی جایگزین: تعریف شیوه‌نامه‌هایی برای تداوم امانت‌دهی و جستجوی منابع به صورت دستی (آفلاین) در زمان قطعی طولانی مدت سامانه‌های نرم‌افزاری.

۴. بازیابی:

فرآیند بازگردانی وضعیت به شرایط عادی:

• بازیابی داده: اجرای متناوب تست‌های بازیابی برای اطمینان از اینکه نسخه‌های پشتیبان سالم هستند و قابلیت بازگردانی کامل دارند.

• تیم‌های واکنش سریع: تشکیل تیم‌های تخصصی با وظایف مشخص (تیم فنی برای بازیابی سرور، تیم حفاظت برای پاکسازی محیط، تیم روابط عمومی برای اطلاع‌رسانی به مراجعان).

۵. بازسازی:

پس از عبور از بحران، تمرکز بر احیای توانمندی‌های اصلی است:

• برنامه بازسازی دارایی‌ها: پیش‌بینی بودجه اضطراری و قراردادهای منعقد شده با پیمانکاران پشتیبانی جهت تعمیر یا جایگزینی سریع تجهیزات آسیب‌دیده.

• اصلاح فرآیندها: درس‌آموزی از بحران و به‌روزرسانی مستندات بر اساس نقاط ضعفی که در طول حادثه خود را نشان داده‌اند.

۶. بازتوانی:

این مرحله به ابعاد انسانی و روانی بحران می‌پردازد:

• حمایت روانی و بازگشت به محیط کار: ارائه مشاوره‌های لازم به کارکنانی که در معرض حادثه بوده‌اند و برگزاری جلسات «بازگشت به کار» برای کاهش استرس ناشی از بحران.

• ارتقای دانش فنی: برگزاری دوره‌های آموزشی تکمیلی برای پرسنل پس از بحران، به منظور اطمینان از اینکه سازمان در برابر تکرار حادثه، هوشمندتر و آماده‌تر شده است.

ج) بررسی عملکرد از حیث نتایج و پیامدها

۱- آیا مجموعه تدابیر و اقدامات معمول شده موجب گردیده است که ذخایر علمی و فعالیت آن حفظ گردیده و خسارات انسانی و مادی ناشی از آن به حداقل برسد؟

این پرسش، در واقع «پرسش بنیادین ارزیابی کارآمدی» در مدیریت بحران است. در ادبیات علمی پدافند غیرعامل، ما پاسخ این سوال را از طریق سنجش میزان «تاب‌آوری» و «تداوم عملیات» به دست می‌آوریم.

پاسخ به این سوال، یک «بله» یا «خیر» ساده نیست، بلکه یک تحلیل مبتنی بر شواهد است. برای اینکه بتوانید با اطمینان علمی به این پرسش پاسخ دهید، باید بررسی کنید که آیا اقدامات شما در سه لایه زیر به هدف خود رسیده‌اند یا خیر:

۱. لایه حفاظتی: آیا «خسارات مادی» به حداقل رسید؟

در اینجا ما فرآیند «پیشگیری» و «کاهش اثر» را می‌سنجیم.

- شاخص موفقیت: اگر حادثه‌ای رخ دهد (مثلاً نشت لوله آب در مخزن یا اتصال کوتاه الکتریکی)، آیا سیستم‌های حفاظتی (مثل سنسورهای رطوبت یا سیستم‌های اطفای حریق گازی) مانند عمل کرده‌اند تا از آسیب به کتاب‌های کمیاب جلوگیری شود؟
- اگر پاسخ مثبت باشد: یعنی تدابیر شما «نقاط آسیب‌پذیری» را شناسایی و مسدود کرده‌اند.
- اگر پاسخ منفی باشد: یعنی اقدامات ما صرفاً «کاغذی» بوده و در مواجهه با تهدید واقعی، محافظت فیزیکی از دارایی‌ها شکست خورده است.

۲. لایه عملیاتی: آیا «ذخایر علمی و فعالیت‌ها» حفظ گردید؟

این بخش مربوط به «تداوم خدمات» است. هدف این است که حتی در زمان بحران، کتابخانه از کار نیفتد.

- شاخص موفقیت: اگر سرور مرکزی کتابخانه یا سامانه «آذرسا» از کار بیفتد، آیا به دلیل وجود «افزونگی» و بک‌آپ‌های خارج از سایت، پژوهشگران همچنان می‌توانند به منابع دسترسی داشته باشند؟
- اگر پاسخ مثبت باشد: یعنی ما از حالت «انفعالی» (منتظر ماندن برای رفع مشکل) به حالت «فعال» (انتقال سریع به سیستم جایگزین) تغییر وضعیت داده‌ایم.
- اگر پاسخ منفی باشد: یعنی وابستگی‌های زنجیره‌ای را به درستی تحلیل نکرده‌ایم و یک نقطه شکست در سیستم وجود دارد.

۳. لایه انسانی: آیا «خسارات انسانی» مدیریت شد؟

این حساس‌ترین بخش است که به «مدیریت بحران و ایمنی» مربوط می‌شود.

- شاخص موفقیت: در صورت بروز حادثه (مثلاً آتش‌سوزی یا زلزله)، آیا کارکنان و مراجعین با استفاده از مسیرهای مشخص و طبق «مانورهای تمرینی»، بدون هرگونه آسیب یا تجمع خطرناک، تخلیه شده‌اند؟
- اگر پاسخ مثبت باشد: یعنی «فرهنگ ایمنی» و «آمادگی روانی» که در برنامه‌ها پیش‌بینی کرده بودیم، در عمل جواب داده است.
- اگر پاسخ منفی باشد: یعنی تمرینات و مانورها فقط جنبه نمایشی داشته‌اند و مهارت‌های واکنش سریع در افراد نهادینه نشده است.

۲- آیا مجموعه اقدامات کتابخانه مرکزی به حدی بوده است که ذخایر علمی در معرض مخاطرات را برای ایستادگی، تحمل، سازگاری و حفظ کارکرد، تطبیق و برگشت‌پذیری در برابر حوادث و تهدیدات، ارتقاء داده و عملیات تداوم کارکرد آن را حفظ نماید؟

پرسش شما اکنون از سطح یک «ارزیابی عملکردی» فراتر رفته و وارد قلمرو «ارزیابی سطح تاب‌آوری استراتژیک» شده است. شما در واقع دارید از فراتر از ایمنی، مفهوم «تاب‌آوری پویای ذخایر علمیرا می‌پرسید.

در پاسخ به این پرسش کلیدی، ما نمی‌توانیم از معیارهای ساده استفاده کنیم. برای پاسخ به اینکه آیا اقدامات انجام شده، ذخایر علمی را در برابر این ۵ رکن (ایستادگی، تحمل، سازگاری، تطبیق و برگشت‌پذیری) مصون داشته است یا خیر، باید از مدل «تاب‌آوری پنج‌گانه» استفاده کرد.

در ادامه، تحلیل می‌کنم که اقدامات کتابخانه چقدر با این مفاهیم همخوانی دارد:

۱. ایستادگی :

آیا اقدامات، اولین ضربه را از ذخایر علمی می‌گیرد؟

وضعیت اقدامات: استفاده از سیستم‌های اطفای حریق گازی، کنترل دمای محیط و تقویت فیزیکی قفسه‌ها.

تحلیل: این اقدامات در لایه «ایستادگی» بسیار عالی عمل می‌کنند. یعنی در برابر تهدیدات اولیه (آتش، رطوبت، ریزش)، یک سد فیزیکی ایجاد می‌کنند تا آسیب در همان لحظه اول متوقف شود.

۲. تحمل :

اگر سد اولیه شکسته شد، آیا سیستم می‌تواند بدون فروپاشی کامل، ضربه را جذب کند؟

وضعیت اقدامات: استفاده از سیستم‌های UPS و کلاسترینگ (Clustering) سرورها.

تحلیل: این اقدامات دقیقاً برای «تحمل» هستند. اگر برق قطع شود یا یک سرور از کار بیفتد، سیستم به جای فروپاشی کامل، از ظرفیت‌های جایگزین استفاده می‌کند تا «توقف ناگهانی» رخ ندهد. این یعنی ظرفیت جذب شوک.

۳. سازگاری:

آیا اقدامات به گونه‌ای است که با تغییر ماهیت تهدیدات، خود را تغییر دهد؟

وضعیت اقدامات: استفاده از هانی‌پات‌ها، مانیتورینگ هوشمند و تحلیل لاگ‌ها.

تحلیل: این بخش از اقدامات، کتابخانه را از حالت ایستا به حالت پویا در می‌آورد. سیستم‌های امنیتی دیجیتال با یادگیری الگوهای نفوذ، خود را با تهدیدات جدید وفق می‌دهند. این یعنی «سازگاری» با محیط متغیر.

۴. تطبیق :

آیا فرآیندها (مثل امانت‌دهی) می‌توانند خود را با شرایط بحرانی هماهنگ کنند؟

وضعیت اقدامات: طراحی سناریوهای «نیمه‌آفلاین» برای تداوم کارکرد.

تحلیل: این یکی از هوشمندانه‌ترین اقدامات است. به جای اینکه در زمان قطع شبکه، کل فعالیت کتابخانه متوقف شود، فرآیندها به حالت «تطبیق یافته» (نیمه‌آفلاین) تغییر می‌کنند. این یعنی حفظ عملیات در عین تغییر ساختار.

۵. برگشت‌پذیری :

پس از پایان بحران، چقدر سریع و با چه کیفیتی به حالت اول برمی‌گردیم؟

وضعیت اقدامات: تعیین شاخص‌های (زمان بازیابی) و (نقطه بازیابی)، و تدوین بودجه اضطراری.

تحلیل: این اقدامات مستقیماً بر «برگشت‌پذیری» تمرکز دارند. بدون داشتن شاخص مشخص، ما نمی‌دانیم چقدر زمان برای بازگشت داریم؛ و بدون بودجه اضطراری، بازگشت فیزیکی غیرممکن است.

۳- مجموعه اقدامات مرتبط با مصون‌سازی، آمادگی، کاهش اثرات تهدیدات و محدودسازی دامنه پیامدهای مخرب تشریح گردد. برای پاسخ به این درخواست، باید اقدامات را در چهار لایه استراتژیک مدیریت بحران طبقه‌بندی کنیم. این ساختار از «جلوگیری از وقوع» شروع شده و به «کنترل خسارت» و در نهایت «بازیابی» ختم می‌شود. در ادامه، تشریح جامع این اقدامات بر اساس استانداردهای پدافند غیرعامل برای کتابخانه مرکزی ارائه می‌گردد:

۱. لایه مصون‌سازی :

هدف: تقویت زیرساخت‌ها برای اینکه تهدیدات نتوانند به هسته اصلی (ذخایر علمی و سامانه‌ها) نفوذ کنند.

- در حوزه فیزیکی:
- مقاوم‌سازی محیطی: استفاده از سیستم‌های اطفای حریق گازی که بدون آسیب رساندن به اسناد و نسخ خطی، آتش را خاموش می‌کنند.
- کنترل محیطی: نصب سنسورهای دقیق دما و رطوبت برای جلوگیری از تخریب بیولوژیکی و شیمیایی منابع.
- امنیت محیطی: نصب دوربین‌های نظارتی و کنترل دسترسی فیزیکی به مخازن حساس.
- در حوزه دیجیتال:
- ایمن‌سازی شبکه: استفاده از فایروال‌های نسل جدید و سیستم‌های تشخیص نفوذ برای بستن راه‌های ورود نفوذگران.
- سخت‌سازی سرورها: غیرفعال کردن سرویس‌های غیرضروری و بستن پورت‌های آسیب‌پذیر در سامانه‌هایی مانند «آذرسا».

۲. لایه آمادگی

هدف: اطمینان از اینکه در صورت وقوع بحران، تیم‌ها و ابزارها آماده واکنش هستند (تمرکز بر عامل انسانی و فرآیندی).

- آمادگی انسانی:
- تیم‌های واکنش سریع: تشکیل تیم‌های تخصصی (IT، تیم اطفای حریق، تیم تخلیه) با وظایف مشخص.
- آموزش و مانور: برگزاری مانورهای شبیه‌سازی شده (مانند شبیه‌سازی حمله باج‌افزاری یا زلزله) برای تبدیل پروتکل‌های کتبی به واکنش‌های غریزی.
- آمادگی فرآیندی:
- تدوین پروتکل‌های: داشتن دستورالعمل‌های گام‌به‌گام برای هر سناریو (مثلاً: «اگر برق قطع شد، قدم اول چیست؟»).
- آمادگی داده‌ای: اجرای منظم پروتکل‌های بک‌آپ‌گیری و، مهم‌تر از آن، تست صحت‌سنجی بک‌آپ‌ها.

۳. لایه کاهش اثرات تهدیدات

هدف: کاهش شدت و احتمال وقوع آسیب‌ها (کاهش احتمالات).

- کاهش ریسک فیزیکی:
- توزیع بار و افزونگی: استفاده از سیستم‌های UPS و ژنراتور برای جلوگیری از نوسانات برق که می‌تواند به تجهیزات حساس آسیب بزند.
- مدیریت چیدمان: استفاده از قفسه‌های مقاوم و چیدمان استاندارد برای کاهش خطر سقوط یا آسیب در اثر لرزش.
- کاهش ریسک دیجیتال:
- مدیریت آسیب‌پذیری: انجام پایش‌های مداوم و به‌روزرسانی برای بستن حفره‌های امنیتی پیش از آنکه مورد سوءاستفاده قرار گیرند.
- رصد کردن تهدیدات جدید در فضای سایبری برای پیش‌دستانه بودن در برابر حملات احتمالی.

۴. لایه محدودسازی دامنه پیامدها

هدف: اگر بحران رخ داد، جلوی گسترش آن را بگیریم (جلوگیری از تبدیل یک حادثه کوچک به یک فاجعه).

- در حوزه دیجیتال:
- ایزولاسیون شبکه: پارتیشن‌بندی شبکه به گونه‌ای که اگر یک بخش (مثلاً شبکه وای‌فای مراجعین) آلوده شد، ویروس نتواند به بخش اصلی (سرور ذخایر علمی) سرایت کند.
- توقف خودکار سرویس‌ها: تنظیم سیستم‌ها برای قطع خودکار ارتباطات در صورت شناسایی رفتارهای مشکوک (مانند شروع رمزگذاری فایل‌ها در حمله باج‌افزاری).
- در حوزه فیزیکی:
- بخش‌بندی فیزیکی: استفاده از درب‌های ضد حریق و دیواره‌های مقاوم برای محدود کردن گسترش آتش یا نشت آب به سایر بخش‌های کتابخانه.
- استفاده از سایت پشتیبان: داشتن کپی‌های از داده‌ها در مکانی کاملاً مجزا، به گونه‌ای که حتی اگر کل ساختمان آسیب ببیند، «حافظه علمی» کتابخانه از بین نرود.

۴- رویکرد عملیاتی عکس‌العملی مربوط به پس از غافلگیر شدن، حین یا پس از حادثه به منظور کم‌اثر نمودن تهدید و با محوریت برگشت‌پذیری به شرایط اولیه و کاهش پیامدها و ضایعات و خسارات تبیین شود.

این درخواست شما، هسته اصلی مدیریت بحران یعنی «مدیریت بحران در لحظه» و «بازیابی پس از فاجعه» را هدف قرار داده است. زمانی که رویکرد از «پیشگیری» به «واکنش» تغییر می‌کند، تمرکز از «ایمنی» به «تاب‌آوری و بقا» تغییر می‌یابد.

در اینجا، رویکرد عملیاتی را در سه فاز زمانی (حین، بلافاصله پس از، و دوره بازیابی) با محوریت کاهش آسیب و برگشت‌پذیری تبیین می‌نمایم:

فاز اول: واکنش در حین حادثه

هدف: کنترل فوری برای جلوگیری از تبدیل یک «حادثه» به یک «فاجعه».

در این مرحله، زمان حیاتی‌ترین متغیر است. اقدامات باید بر «ایزوله کردن تهدید» تمرکز کنند:

۱. ایزولاسیون دیجیتال:
 - اگر حمله سایبری (مانند باج‌افزار) شناسایی شد، اقدام اول «قطع ارتباط شبکه» است. قطع اتصال سرورهای اصلی از شبکه داخلی و اینترنت برای جلوگیری از انتشار ویروس به سایر بخش‌ها یا سرورهای بک‌آپ.
 - توقف خودکار فرآیند کپی/انتقال داده‌ها در صورت مشاهده رفتارهای غیرعادی.
۲. ایزولاسیون فیزیکی:
 - در صورت وقوع آتش‌سوزی یا نشت آب، فعال‌سازی پروتکل‌های ایزولاسیون محیطی (بستن درب‌های ضد حریق یا شیرهای قطع‌کننده اصلی) برای محدود کردن دامنه آسیب به یک اتاق یا بخش مشخص.
۳. تیم واکنش سریع:
 - استفاده از دستورالعمل‌های «توقف عملیات» برای محافظت از جان کارکنان و جلوگیری از ورود افراد غیرمتخصص به منطقه خطر.

فاز دوم: واکنش بلافاصله پس از حادثه

هدف: ارزیابی آسیب‌ها و تثبیت وضعیت برای جلوگیری از تکرار یا گسترش اثر.

در این مرحله، سیستم باید از حالت «تکان خورده» خارج شده و به حالت «ایستا» برسد:

۱. ارزیابی سریع آسیب‌ها:
 - ارزیابی دیجیتال: بررسی سلامت زیرساخت‌های شبکه، سرورها و سلامت فایل‌های ذخیره شده. آیا بک‌آپ‌ها سالم هستند؟ آیا نفوذگر هنوز در شبکه حضور دارد؟
 - ارزیابی فیزیکی: بررسی آسیب‌های ساختاری، میزان خسارت به منابع ارزشمند (کتاب‌ها/نسخ خطی) و سلامت تجهیزات محیطی (تجهیزات سرمایشی/ایمنی).
۲. تثبیت وضعیت:
 - اگر علت حادثه (مثلاً نشت آب یا نفوذ سایبری) هنوز کاملاً حذف نشده، باید اقدامات مهارکننده برای جلوگیری از «آسیب ثانویه» انجام شود (مثلاً خشک کردن محیط برای جلوگیری از از بین رفتن کتاب‌ها توسط رطوبت باقی‌مانده).
۳. فعال‌سازی پروتکل‌های جایگزین:
 - انتقال موقت خدمات به «حالت تداوم عملیات». مثلاً استفاده از سرورهای بک‌آپ یا انتقال خدمات کتابخانه به یک فضای محدود اما امن برای حفظ حداقل خدمات به مراجعین.

فاز سوم: بازیابی و بازگشت به حالت اولیه بازگشت تدریجی به سطح عملیاتی استاندارد و یادگیری از بحران.

این مرحله، تفاوت اصلی یک سازمان «تاب‌آور» با یک سازمان «آسیب‌پذیر» را مشخص می‌کند:

۱. بازیابی داده‌ها و زیرساخت:
 - اجرای فرآیند Restoration بر اساس شاخص‌های تعیین شده قبلی:
 - RTO (زمان بازیابی): چقدر زمان برد تا سیستم دوباره آنلاین شود؟
 - RPO (نقطه بازیابی): چه مقدار از داده‌های بین آخرین بک‌آپ و لحظه حادثه از دست رفت؟
 - بازسازی تدریجی از بخش‌های حیاتی به سمت بخش‌های غیرحیاتی.

۲. پاکسازی و بازسازی فیزیکی:

- استفاده از تیم‌های متخصص برای بازسازی منابع آسیب‌دیده (مثلاً استفاده از روش‌های جرم‌گیری برای کتاب‌های نم‌زده یا تعمیر تجهیزات الکترونیکی).

۳. تحلیل پس از حادثه:

- تحلیل شکاف: چرا سیستم‌های حفاظتی در مرحله اول نتوانستند جلوی حادثه را بگیرند؟ (مثلاً آیا سنسورها کار نکردند؟ یا پروتکل‌ها مبهم بودند؟).
 - به‌روزرسانی نقشه راه: تبدیل نتایج تحلیل به اقدامات اصلاحی برای تضمین اینکه همان حادثه، دیگر «غافلگیرکننده» نباشد.
- برای اینکه این رویکرد از حالت تئوری خارج شده و به یک «ابزار اجرایی» تبدیل شود، یک «پروتکل عملیاتی استاندارد» برای یکی از بحرانی‌ترین سناریوها در کتابخانه دیجیتال تدوین می‌نماییم: «حمله باج‌افزاری و رمزگذاری ناگهانی داده‌های سامانه آذرسا و ذخایر دیجیتال».
- این پروتکل بر اساس رویکرد «مهار در لحظه» طراحی شده تا از گسترش ویروس به بخش‌های دیگر و از دست رفتن بک‌آپ‌ها جلوگیری کند. پروتکل عملیاتی واکنش سریع.

