محرمانگی اطلاعات در کتابخانه‌ها و آرشیوها

راضیه فرشید

■ **چکیده**

کتابخانه و آرشیو را در گذشته به‌دلیل حفظ و نگه‌داری اسناد و گزارش‌های مخصوص و محرمانه پایه‌گذاری کردند. این پژوهش به معرفی اصول بایگانی، تعریف امنیت اطلاعات و تعاریف پایه از قبیل (محرمانگی، یکپارچگی، دسترسی داده‌ها) و همچنین قوانین و مقررات برای طبقه‌بندی اسناد و داده‌ها می‌پردازد. هدف از این پژوهش بررسی چگونگی حفظ محرمانگی اطلاعات در کتابخانه‌ها و مکان‌های آرشیوی و ارائه تعاریفی برای حفظ و برقراری امنیت است. روش این پژوهش کتابخانه‌ای با بررسی کتاب‌ها و مقالات متعدد است. نتایج به‌دست آمده نشان می‌دهد ایجاد هماهنگی، رعایت نظم‌وترتیب اولیه اسناد دولتی، ارزشیابی و انتخاب اسناد باارزش و نیز اهمیت اسناد سبب می‌شود که بحث امنیت و محرمانگی داده‌ها در آرشیوها به‌صورت پررنگ‌تر نشان داده شود. در ایران تمام مؤسسات و سازمان‌ها موظف هستند که اسناد خود را به آرشیو ملی تحویل دهند و در آنجا گروه ارزشیابی دربارهٔ امحا یا انتخاب آن و نگه‌داری آن در سازمان آرشیو ملی تصمیم‌گیری می‌کند. به‌دلیل ملی‌بودن بسیاری از این اسناد، محرمانگی و امنیت این داده‌ها نقش بسیار حیاتی را ایفا می‌کنند.

کلیدواژه‌ها

آرشیو و کتابخانه؛ محرمانگی اطلاعات.

محرمانگی اطلاعات در کتابخانه‌ها و آرشیوها

راضیه فرشید[1]

مقدمه

امروزه با بالارفتن آمار کاربران اینترنت در کشور و آشنایی آن‌ها با نرم‌افزارهای نفوذ به شبکه‌های رایانه‌ای و همچنین با رشد میزان اطلاعات موجود روی کارسازهای سازمان‌ها، نیاز به نظارت بر امنیت شبکه‌های رایانه‌ای اهمیت به‌سزایی پیدا کرده است. عدم آشنایی بسیاری از کاربران و کارکنان سازمان‌ها، به نفوذگران کمک می‌کند تا به‌راحتی وارد شبکه رایانه‌ای شده و از آن به اطلاعات محرمانه دست پیدا کنند یا اینکه به اعمال خرابکارانه بپردازند. هر چه رشد اینترنت و اطلاعات روی آن بیشتر می‌شود، نیاز به اهمیت امنیت شبکه افزایش پیدا می‌کند.

کتابخانه به مجموعه‌ای از اطلاعات و منابع و خدمات اطلاعاتی گفته می‌شود که یک نهاد عمومی، خصوصی یا یک شخص نگه‌داری و اداره می‌کند. از نگاه سنتی، کتابخانه به‌طورمعمول به مجموعه‌ای از کتاب‌ها گفته می‌شود. کتاب مجموعه‌ای از اطلاعات در مورد یک فرد یا یک جسم یا غیره خاص است که در صفحاتی کاغذی نوشته یا چاپ می‌شود (موگهرجی، ۱۳۷۵).

در حقیقت، سومریان نخستین کسانی بودند که این دستاوردها را به این هدفِ روشن، یعنی حفظ آن برای نسل‌های آینده، ثبت کردند. به‌عبارت‌دیگر سومریان کسانی بودند که به کتاب نقشی اختصاص دادند که تا به امروز با آن در ارتباط است. بدین معنا که دستاوردهای فرهنگی و فنّاوری انسان را پاس دارد و پاسخگوی اهداف قانونی و آموزشی و دیگر نیازهای روزانه او

۱. کارشناسی‌ارشد مطالعات آرشیوی.
raziyeh.farshid@gmail.com

باشد (استیویج، ۱۳۷۳).

کتابخانه‌هایی در معابد و قصرها وجود داشتند و یکی از مهم‌ترین و بهترین نمونه‌های آن‌ها کتابخانه «بورسیپا» است که یکی از شاخص‌ترین کتابخانه‌های عصر باستان بود (استیویج، ۱۳۷۳).

بنای کتابخانه در جهان به دوران کهن و قرن‌ها پیش از میلاد مسیح می‌رسد. نخستین سنگِ بنای کتابخانه را سران و زمامداران کشورها، نه به قصد و نیتِ صرفاً ایجاد کتابخانه، بلکه به‌خاطر حفظ و نگه‌داری اسناد و گزارش‌های مخصوص و محرمانه پایه‌گذاری کردند. در حقیقت، خودِ این عمل بیانگر آن است که در زمان قدیم چندان اختلاف و تفاوت مخصوص و محسوس بین اتاقی که اسناد و گزارش‌ها را در آن نگه‌داری می‌کرده‌اند و کتابخانه، وجود نداشته است (عازم، ۱۳۷۸).

بایگانی به کلیه سوابق و اسناد و مدارک عمومی یا تاریخی که توسط دولت یا یک سازمان دولتی یا اداره یا مؤسسه و یا تأسیساتی از این قبیل نگه‌داری می‌شود و نیز اسناد و مدارکی که خانواده یا فرد در ارتباط با کار خود تهیه و یا دریافت می‌کند و آن‌ها را تحت نظر خود محافظت یا نگه‌داری می‌کنند، گفته می‌شود.

اصول بایگانی:

۱. اصل منشأ یا خاستگاه: این اصل حکم می‌کند که اسناد به‌شکل اولیه‌شان حفظ شوند تا ترتیب آن‌ها به‌هم نخورد.
۲. اصل نظم اولیه: پدیدآورنده بر اساس منظور خاصی اسناد را در کنار هم چیده و فرض بر آن است که آن ترتیب، دارای منطق است و نباید آن را از بین برد (فدایی، ۱۳۸۶).

تعریف امنیت اطلاعات

از زمانی‌که نوشتن و تبادل اطلاعات آغاز شد، همه انسان‌ها مخصوصاً سران حکومت‌ها و فرماندهان نظامی در پی راهکاری برای محافظت از محرمانه‌بودن مکاتبات و تشخیص دستکاری آن‌ها بودند. ژولیوس سزار ۵۰ سال قبل از میلاد یک نظام رمزنگاری مکاتبات ابداع کرد تا از خوانده‌شدن پیام‌های سری خود توسط دشمن جلوگیری کند حتی اگر پیام به‌دست دشمن بیافتد. جنگ جهانی دوم باعث پیشرفت چشمگیری در زمینهٔ امنیت اطلاعات شد و این آغاز کارهای حرفه‌ای در حوزه امنیت اطلاعات شد. پایان قرن بیستم و سال‌های اولیه قرن بیست‌ویکم شاهد پیشرفت‌های سریع در ارتباطات راه دور، سخت‌افزار، نرم‌افزار و رمزگذاری داده‌ها بود. در دسترس بودن تجهیزات محاسباتی کوچک‌تر، قوی‌تر و ارزان‌تر برای پردازش الکترونیکی داده‌ها باعث شد که شرکت‌های کوچک و کاربران خانگی دسترسی بیشتری به آن‌ها داشته باشند. این تجهیزات

به‌سرعت از طریق شبکه‌های رایانه‌ای مثل اینترنت به‌هم متصل شدند.

امنیت اطلاعات یعنی حفاظت اطلاعات و سامانه‌های اطلاعاتی در برابر فعالیت‌های غیرمجاز. این فعالیت‌ها عبارتند از دسترسی، استفاده، افشاء، خواندن، نسخه‌برداری یا ضبط، خراب‌کردن، تغییر، دستکاری.

واژه‌های امنیت اطلاعات، امنیت رایانه‌ای و اطلاعات مطمئناً گاهی به اشتباه به‌جای هم به‌کار برده می‌شود. اگر چه این موضوعات به‌هم مرتبط هستند و همگی دارای هدف مشترک حفظ محرمانگی اطلاعات، یکپارچه‌بودن اطلاعات و قابل دسترس بودن را دارند ولی تفاوت‌های ظریفی بین آن‌ها وجود دارد. این تفاوت‌ها در درجه اول به موضوع امنیت اطلاعات، روش‌های استفاده‌شده برای حل مسئله و موضوعاتی می‌پردازد که بر آن تمرکز کرده‌اند.

امنیت اطلاعات به محرمانگی، یکپارچگی و در دسترس بودن داده‌ها مربوط است بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ، و یا اشکال دیگر (استالین، ۲۰۰۶).

ضرورت توجه به امنیت اطلاعات

- گسترش تهدیدها علیه سرمایه‌های اطلاعاتی سازمان؛
- افزایش دانش و انگیزه نفوذگران شبکه‌ها؛
- پیشرفت فنّاوری‌ها و روش‌های نفوذ به شبکه؛
- افزایش روزافزون انواع ویروس‌های رایانه‌ای؛
- وجود ضعف‌های امنیتی در سیستم‌های عامل و برنامه‌های کاربردی؛
- وجود کاربران غیرحرفه‌ای و آموزش‌ندیده؛
- نتایج بی‌توجهی به امنیت اطلاعات؛
- نفوذ به شبکه و دسترسی به اطلاعات محرمانه؛
- سوءاستفاده مالی؛
- تخریب اطلاعات موجود و نرم‌افزارها؛
- تخریب سخت‌افزاری؛
- از کار انداختن کارسازها و اشغال پهنای باند.

مفاهیم پایه

همان‌گونه که تعریف شد، امنیت اطلاعات یعنی حفظ محرمانگی، یکپارچه‌بودن و قابل دسترس بودن اطلاعات در مقابل افراد غیرمجاز. در اینجا مفاهیم سه‌گانه «محرمانگی»، «یکپارچه‌بودن» و «قابل دسترس بودن» توضیح داده می‌شود.

محرمانگی

توانایی کاربران در حفظ حریم شخصی خود یا حفظ حریم شخصی یک فرد یا گروه و یا حفظ اطلاعات است. مرزها و محتوای آنچه خصوصی است در میان فرهنگ‌ها و افراد متفاوت در نظر گرفته شده است. هنگامی‌که چیزی برای فردی خصوصی است، معمولاً بدان معنی است که چیزی ذاتاً خاص است و یا نسبت به آن‌ها حساس هستیم. حوزه حریم خصوصی حوزه‌ای امنیتی است که می‌تواند مفاهیم استفاده مناسب و همچنین حفاظت از اطلاعات را شامل شود (اولاسویرتا، ۲۰۱۴).

مفهوم حریم خصوصی فرد یک ساختار مدرن است که در درجه اول با فرهنگ غربی، انگلیسی و امریکای‌شمالی در ارتباط بوده و عملاً تا زمان‌های اخیر در برخی از فرهنگ‌ها ناشناخته باقی‌مانده است. به گفته برخی از محققان، این مفهوم در فرهنگ انگلیس و امریکا از هم جدا بوده حتی از فرهنگ اروپای‌غربی مانند فرانسه یا ایتالیایی جداست (ژیمسکای، ۲۰۰۵).

نظریه‌پردازان مختلف حریم خصوصی را به‌عنوان نظامی برای محدودکردن دسترسی به اطلاعات شخصی فرد تصور می‌کنند (سولو، ۲۰۰۸). حفظ حریم خصوصی وضعیتی است از دسترسی ناخواسته دیگران، دسترسی فیزیکی، اطلاعات شخصی و غیره که باید توجه و محافظت شود (بوک، ۱۹۸۹). محرمانگی اطلاعات، حفظ حریم خصوصی است که گاهی‌اوقات به‌عنوان یک گزینه به پنهان‌کاری تعریف شده است. پوسنر حریم خصوصی را حق مردم در پنهان‌کردن اطلاعات در مورد خود می‌داند که ممکن است دیگران از آن اطلاعات به ضرر او استفاده کنند (پوسنر، ۱۹۸۳).

محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیرمجاز (استالین، ۲۰۰۶). نقض محرمانگی ممکن است اشکال مختلف داشته باشد. برای مثال، اگر کسی از روی شانه شما اطلاعات محرمانه نمایش‌داده‌شده روی صفحه نمایش رایانه شما را بخواند یا فروش یا سرقت رایانه لپ‌تاپ حاوی اطلاعات حساس یا دادن اطلاعات محرمانه از طریق تلفن همه موارد نقض محرمانگی است.

یکپارچگی

یکپارچگی یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیرمجاز اطلاعات. یکپارچگی وقتی نقض می‌شود که اطلاعات نه فقط در حین انتقال بلکه در حال استفاده یا ذخیره‌شدن و یا نابودشدن نیز به‌صورت غیرمجاز تغییر داده شود. سامانه‌های امنیت اطلاعات به‌طور معمول علاوه‌بر محرمانه‌بودن اطلاعات، یکپارچگی آن‌را نیز تضمین می‌کنند.

دسترس‌پذیری

اطلاعات باید زمانی که موردِنیاز افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کارکردن و جلوگیری از اختلال در سامانه‌های ذخیره‌سازی و پردازش اطلاعات و کانال‌های ارتباطی موردِاستفاده برای دسترسی به اطلاعات، اطمینان حاصل کرد. سامانه‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت‌افزار و ارتقا سامانه در دسترس باقی می‌مانند. یکی از راه‌های از دسترس خارج‌کردن اطلاعات و سامانه اطلاعاتی درخواست‌های زیاد از طریق خدمات از سامانه اطلاعاتی است که در این حالت چون سامانه توانایی و ظرفیت چنین حجم انبوده خدمات‌دهی را ندارد از خدمات‌رسانی به‌طورکامل یا جزئی عاجز می‌ماند.

برای حراست از اطلاعات، باید دسترسی به اطلاعات کنترل شود. افراد مجاز باید و افراد غیرمجاز نباید به اطلاعات دسترسی داشته باشند. بدین‌منظور روش‌ها و تکنیک‌های کنترل دسترسی ایجاد شده‌اند. دسترسی به اطلاعات حفاظت‌شده باید محدود به افراد، برنامه‌های رایانه‌ای، فرایندها و سامانه‌هایی باشد که مجاز به دسترسی به اطلاعات هستند. این کار مستلزم وجود مکانیزم‌هایی برای کنترل دسترسی به اطلاعات حفاظت‌شده است. پیچیدگی مکانیزم‌های کنترل دسترسی باید مطابق با ارزش اطلاعات حفاظت‌شده باشد. اطلاعات حساس‌تر و با ارزش‌تر نیاز به مکانیزم کنترل دسترسی قوی‌تری دارند. اساس مکانیزم‌های کنترل دسترسی بر دو مقوله احراز هویت و تصدیق هویت است.

احراز هویت، تشخیص هویت کسی یا چیزی است. این هویت ممکن است توسط فرد ادعا شود و یا ما خود تشخیص دهیم. تصدیق هویت عمل تأیید هویت است.

قوانین و مقررات طبقه‌بندی داده‌ها

در زیر به تعریف و توصیف چند مورد از طبقه‌بندی داده‌های دولتی از پایین‌ترین سطح حساسیت تا بالاترین می‌پردازیم:

۱. **اطلاعات طبقه‌بندی‌نشده:** که عموم به‌راحتی به آن‌ها دسترسی دارند و این آزادی دسترسی باعث نقض اصل محرمانگی در داده‌ها نمی‌شود.

۲. **اطلاعات حساس اما طبقه‌بندی‌نشده:** اطلاعاتی که مانند یک راز کوچک است اما فاش‌شدن آن‌ها می‌تواند باعث آسیب‌های جدی شود مانند پاسخ آزمون‌های امتحان که در این گروه قرار می‌گیرند.

۳. **محرمانه:** گروه داده‌هایی که در این بخش قرار می‌گیرند بسیار مهم است و در صورت فاش‌شدن می‌تواند یک کشور را دچار آسیب‌های امنیتی کند؛ مانند اسناد مهم دولتی که

صرفاً باید در دست افراد مجاز باشد.

۴. **سری:** داده‌هایی که در این گروه قرار می‌گیرند در صورت افشا باعث به‌خطر افتادن امنیت ملی یک کشور خواهد بود مانند تصمیمات مهم راهبردی جهت تعیین نوع روابط با دیگر کشورها.

۵. **فوق سری:** این اطلاعات در بالاترین سطح امنیتی قرار دارند و افراد بلندپایه مثل رئیس‌جمهور یک کشور به آن‌ها دسترسی خواهد داشت.

همان‌طور که از این دسته‌بندی مشخص است افراد دارای دسترسی مناسب و موردِنیاز با حیطه کاری خود به داده‌ها دسترسی خواهند داشت (رستمی، ۱۳۹۲)

امنیت اطلاعات و محرمانگی اطلاعات در کتابخانه‌ها و آرشیوها

همان‌گونه که در بالا ذکر شد معنای عام محرمانگی، پنهان‌کردن اطلاعات است که این اصل با اصول کتابخانه‌ای مغایرت دارد. هدف اولیه کتابخانه در دسترس قرار دادن اطلاعات برای همگان و دسترسی راحت به اطلاعات است. در هر کتابخانه‌ای با توجه به سیاست‌های تعریف‌شده مجموعه‌ای جمع‌آوری می‌شود. گاهی برخی از کتاب‌ها با هدف و سیاست آن کتابخانه مغایرت دارد و یا مناسب مخاطبان آن کتابخانه نیست؛ به‌همین‌دلیل آن کتاب هرگز برای کتابخانه تهیه نخواهد شد. در میان انواع کتابخانه‌ها گاهی کتابخانه‌های تخصصی برای اطلاعات خود امنیت بالایی در نظر می‌گیرند و اجازه دسترسی این اطلاعات برای متخصصان همان مؤسسه یا سازمان است گاهی فاش‌شدن این اطلاعات به ضرر مؤسسه مذکور است مانند کتابخانه‌های تخصصی و فنی که نقشه‌ها و اطلاعات را از دیگر مؤسسات و سازمان‌ها و افراد عادی پنهان نگه می‌دارند. بحث امنیت اطلاعات و محرمانگی آن بیشتر در خصوص اطلاعات کاربران در کتابخانه‌ها به‌کار می‌رود زیرا همان‌طور که در بالا گفته شد با اصل اولیه کتابخانه‌ها مغایرت دارد.

امنیت اطلاعات و محرمانگی اطلاعات در آرشیوها می‌تواند معنای بسیار وسیع‌تری نسبت به کتابخانه‌ها داشته باشد. در آرشیوها اسنادی نگه‌داری می‌شوند که ارزش نگه‌داری دائمی را داشته باشند. سازمان‌ها و مؤسسات اسناد را برای ارزشیابی به مرکز اسناد ملی، ارسال می‌کنند. بعد از ارزشیابی، برخی اسناد امحاشده و دیگر اسناد ارزش‌گذاری‌شده، سازمان‌دهی می‌شوند و برای استفاده در اختیار افراد قرار می‌گیرند. برخی اسناد مانند اسناد وزارت‌اطلاعات و وزارت‌خارجه به‌دلیل محرمانگی و امنیت اطلاعات بسیار بالایشان هیچ‌گاه در اختیار مرکز اسناد ملی کشور قرار نمی‌گیرد زیرا مخاطبان آرشیو ملی عموم افراد هستند. اسناد این مراکز در همان مراکز آرشیو می‌شوند.

اسنادی که به‌دست مرکز اسناد ملی اسلامی می‌رسد به چند صورت تهیه می‌شوند: خریداری، اهدایی، امانی و غیره. اغلب اسنادی که از طریق خریداری به مرکز اسناد انتقال داده می‌شود در خصوص محرمانگی و امنیت اطلاعات ممنوعیتی ندارند مگر در شرایط خاص. گاهی اسنادی که به مرکز اسناد ملی اهدا می‌شود، دارای ویژگی‌های خاصی است و فرد اهداکننده به دلایل خاص در ازای اهدای اسناد شرایطی را وضع می‌کند این شرایط شامل شرایطی در خصوص محرمانه‌بودن اطلاعات تا بعد از فوت فرد است. گاهی این اسناد، اسناد هویتی هستند و ممکن است خطراتی برای آبرو و حیثیت خانواده‌شان به‌وجود آورد. رعایت حریم خصوصی این اسناد همواره باید از طرف سازمان رعایت شود و این افراد با خیالی آسوده اسناد خود را در اختیار سازمان قرار می‌دهند و سازمان طی امضا قرارداد به قول‌های خود عمل می‌کند. هنگامی که سازمان آرشیو ملی این اسناد را دریافت می‌کند اگر به تعهدات و قول‌های خود عمل کند این امر سبب به‌وجود آمدن اعتماد دو طرفه بین آن‌ها می‌شود و این اعتماد همه‌گیر خواهد شد. این امر بیشتر نفع ملی دارد زیرا در این سازمان شرایط عالی برای نگه‌داشتن اسناد وجود دارد و در صورت اعتماد افراد به سازمان آرشیو ملی می‌توانند اسناد را به این سازمان تحویل دهند تا حمایت و شرایط بهتری برای اسناد به‌وجود آید. اگر این اعتماد بیشتر شود، افراد می‌توانند سندهای خانوادگی خود را به‌صورت امانی در اختیار سازمان اسناد ملی قرار دهند و هر زمان که خواستار آن باشند می‌توانند آن اسناد را از سازمان تحویل بگیرند و خود این امر سبب ماندگاری بیشتر اسناد مهم می‌شود.

در اسناد آرشیوی باید به این نکته توجه شود که برخی از اسناد شامل تعهدات، موافقت‌نامه‌ها نیز ممکن است برای امنیت کشور خطرناک باشد و حد و مرز آن کشور را تهدید کند و بر علیه آن کشور و مردمان آن کشور استفاده شود؛ به‌همین‌دلیل امنیت و محرمانگی این اطلاعات بسیار حیاتی و ضروری است.

منابع

– استیویچ، الکساندر (۱۳۷۳). کتاب در پویه تاریخ. ترجمه حمید رضا آژیر.

– رستمی، حجت (۱۳۹۲). مزایای طبقه‌بندی اطلاعات و سیاست‌های امنیتی. انجمن امنیت اطلاعات و ارتباطات.

– عازم، پرویز (۱۳۷۸). ساختمان و تجهیزات کتابخانه. تهران: نشر کتابدار.

– فدایی، غلامرضا (۱۳۸۶). مقدمه‌ای بر شناخت اسناد آرشیوی. تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت).

– موکهر، جی، ا. ک. (۱۳۶۸). تاریخ و فلسفه کتابداری. ترجمه اسدالله آزاد. مشهد: آستان قدس رضوی.

- Bok, Sissela (1989). Secrets: on the ethics of concealment and revelation (Vintage Books ed.). New York: Vintage Books. pp. 10–11. ISBN 978-0679724735.

- Oulasvirta, A., Suomalainen, T., Hamari, J., Lampinen, A., & Karvonen, K. (2014). Transparency of Intentions - Decreases Privacy Concerns in Ubiquitous Surveillance. Cyberpsychology, Behavior, and Social Networking, 17(10), 633-638.

- Posner, Richard A. (1983). The economics of justice (5. print ed.). Cambridge, Mass.: Harvard University Press. p. 271. ISBN 978-0674235267.

- Solove ,Daniel J.,(2008) "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy", San Diego Law Review, Vol. 44, 745-772.

- Stalling ,William (2006), Cryptography and Network Security fifth edition For symmetric encryption to work, mediate the establishment of secure communications between them publishing as Prentice Hall.

- Zhimskaya, E. A. (9 April2005). (Features of the Russian language of fourth wave immigrants) " (in Russian). Gramota.ru. Retrieved 24 February 2009