تأمين تقنيات المعلومات في المكتبات ومراكز المعلومات

أ.د. محمود صالح إسماعيل
قسم المعلومات والمكتبات/ كلية الأداب

المستخلص:

تُعدَّ تقنيات المعلومات من أهم المعدات التي تقتنيها المكتبات ومراكز المعلومات على اختلاف أنواعها.فمعظم هذه المكتبات ومراكز المعلومات تصبح عاجزة عن أداء دورها إذا ما توقفت تقنيات المعلومات التي تملكها عن العمل لأية فترة من الزمن. فهذه التقنيات لا تكون مهمة كمعدات مادية فقط، ولكنها أكثر أهمية للجوانب النوعية المتعلقة بكيفية تمثيل النظام المادي للمكتبة أو مركز المعلومات.فالمكتبات ومراكز المعلومات التي تعتمد على هذه التقنيات أو التي تتبنى النظم المحوسبة في عملياتها كافة قد تصبح عاجزة عن أداء أيسر التزاماتها تجاه مستفيديها إذا فقدت هذه التقنيات.

المقدمة:

تسعى مختلف المكتبات ومراكز المعلومات إلى البحث عن أساليب لتأمين سلامة تقنيات المعلومات التي تقيها من الأخطار التي قد تسبب الضرر أو التلف لهذه المعدات. ولا يشك أحد في أهمية وضرورة توفر تقنيات المعلومات في المكتبات ومراكز المعلومات في الوقت الحاضر. إذ إن هذه التقنيات لم تعد سلعة مادية يمكن للمكتبة أو مركز المعلومات أن تقتنيها حين تشاء وتستغني عنها حين تشاء. فقد أصبحت من أهم معدات المكتبات ومراكز المعلومات، مثلها مثل الملاك الفني، والأبنية، والأثاث وغير ذلك من معدات.

وبسبب هذه الأهمية فقد أصبحت هناك حاجة جديدة في المكتبات ومراكز المعلومات وهي ضرورة توفير المقومات الأمنية لهذه التقنيات. ففي القرن الماضي كانت الحماية المادية للتقنيات من المخاطر الخارجية والداخلية والكوارث الطبيعية كافية لتوفير الحماية المطلوبة. غير أن حدوث بعض الحوادث المدمرة أجبر المكتبات ومراكز المعلومات على ضرورة إعادة النظر في إجراءاتها الأمنية. وقد إزدادت أهمية هذه الإجراءات مع تزايد استخدام تقنيات المعلومات، ومع زيادة اعتماد المكتبات

ومراكز المعلومات على هذه التقنيات. وقد أشارت إحدى الدراسات المنشورة عام ١٩٩٦ إلى أن تأمين تقنيات المعلومات ينصب على الكثير من الجوانب المهمة منها:[١]

١. يمكن أن يسبب أشياء غير مقبولة تؤدي إلى الخسائر المادية والى قلة المنفعة والدقة والسرية.
٢. الحماية الكافية من الكوارث المستقبلية غير المؤكدة وغير المرغوب بها، حيث حدوثها.
٣. ضرورة وضع خطط للطوارئ من أجل القيام بالنشاط الأعتيادي إذا وقع حادث ما يؤدي إلى توقف العمل.
٤. اتخاذ إجراءات للمراقبة المستمرة للكشف عن أي قصور في النظام أو سوء الأستخدام من قبل المستخدمين لهذه التقنيات.

واعتماد المكتبات ومراكز المعلومات المتزايد على تقنيات المعلومات أدى إلى زيادة احتمال تعرض هذه التقنيات إلى الأخطار الطبيعية والبشرية المقصودة وغير المقصودة.وتقنيات المعلومات كما هو معروف تحتاج إلى أساليب حماية متنوعة منها ما هو خارجي ومنها ما يتم داخل التقنية نفسها من أجل ضمان الحماية والجودة. وقد أدى هذا إلى ظهور الكثير من المفاهيم غير المعروفة من قبل، مثل تأمين تقنيات المعلومات وإدارة المخاطر في المكتبات ومراكز المعلومات.

مشكلة البحث:

تعرضت المكتبات ومراكز المعلومات العراقية بعد غزو العراق من قبل الولايات المتحدة الأمريكية وحلفائها عام ٢٠٠٣ إلى التخريب والتدمير وتدمير ما بها من تقنيات معلومات،ونهبها تحت مرأى ومسمع القوات الأمريكية الغازية. ولحسن الحظ لم ينتج عن هذا التخريب والتدمير والنهب أية خسائر بالأرواح،فضلاً عن المطبوعات التي تعرض منها للسرقة والتلف أيضاً. وما حدث في جامعة الموصل مثلاً كان تدمير كل أجهزة الحواسيب وملحقاتها المتواجدة في المكتبة المركزية للجامعة وفي مركز الحاسبة الالكترونية، وفي كل مكتبات الكليات والمراكز التابعة للجامعة. كما تعرضت بقية تقنيات المعلومات المتواجدة في المكتبة المركزية من أجهزة مصغرات وأجهزة عرض سلايدات وتلفزيونات مع معداتها إلى السرقة والتلف أيضاً. لهذا قامت هذه المؤسسات باتخاذ إجراءات أمنية مشددة لحماية تقنيات المعلومات وتأمينها.

---

[١] عماد الصباغ وجمال الدباغ، إدارة الخطر في مراكز الحاسبات: التوجهات الحديثة في علم الحاسوب وأنظمة المعلومات، وقائع بحوث المؤتمر العلمي الأول لكلية العلوم في جامعة فيلادلفيا ٩-١٠ تموز ١٩٩٦ (عمان-الأردن: جامعة فيلادلفيا، ١٩٩٦) ص١٣٨.

وتأمين تقنيات المعلومات هو مصطلح يطلق على كل الإجراءات والمعايير الفنية المتخذة لتجنب الدخول غير المسموح به إلى تقنيات المعلومات، أو التخريب المتعمد أو غير المتعمد للحواسيب والبرامجيات أو البيانات، أو السرقة المادية أو الفكرية أو تدمير السجلات والملفات المادية.[١]

وقد ازداد استخدام هذا المصطلح منذ انتشار فيروسات الحواسيب. فبالرغم من كون الفيروسات هي من المشاكل الموجودة أصلاً، الأ أنها أصبحت معروفة بشكل واسع منذ أكثر من عشرين عاماً. والفيروسات هي برامجيات متقدمة لتدمير أو تخريب القيود والملفات وذاكرات الحواسيب ونظم تشغيلها وغير ذلك.

ويمكننا تطوير تأمين سلامة تقنيات المعلومات من خلال عدد من الأساليب والأدوات التي تستخدم لحماية وحراسة تقنيات المعلومات وبرمجياتها ومعدات الاتصالات والبيانات. وبالرغم من كل الإجراءات والأساليب التي تتخذها المكتبات ومراكز المعلومات، الأ أن الكثير من المكتبات ومراكز المعلومات قد تعرضت إلى الكثير من الحوادث التي أدت إلى خسائر لا تقدر بثمن في تقنيات المعلومات، والسلب والنهب والتخريب الذي تعرضت له المكتبات ومراكز المعلومات العراقية مؤخراً خير دليل.

الأسئلة البحثية:

ما المقصود بتأمين تقنيات المعلومات؟ وكيف يتحقق ذلك؟

١. ما أساليب تأمين تقنيات المعلومات؟وما هي الإجراءات لتحقيق ذلك؟

٢. كيف تخطط المكتبات ومراكز المعلومات للطوارئ وإدارة المخاطر؟ وما مشاكل تأمين تقنيات المعلومات التي تواجهها المكتبات ومراكز المعلومات؟

أهمية البحث:

تنبع أهمية هذا البحث من البيانات التي يمكن توفيرها والتي يمكن اعتمادها في التعريف بمشكلة تأمين تقنيات المعلومات في المكتبات ومراكز المعلومات والنتائج المترتبة على المكتبات ومراكز المعلومات في حالة تعرضها للمخاطر وعدم قيامها بمواجهتها بشكل جيد.كما أن البحث

[1] Kenneth C. Laudon & Jane P. Laudon. Essentials of management information systems. Englewood Cliffs, (NJ): Prentice Hall, 1995.pp: 443-444.

سيسلط الضوء على طبيعة المخاطر التي يمكن أن تتعرض لها المكتبات ومراكز المعلومات وطرق مواجهتها لهذه المخاطر.

المخاطر التي تواجهها تقنيات المعلومات:

هناك أربعة مخاطر تواجهها المكتبات ومراكز المعلومات التي تقتني تقنيات المعلومات وهي: الكوارث الطبيعية،والتخريب المتعمد،والأضرار غير المتعمدة،وجرائم الحاسوب.وتتبع المكتبات ومراكز المعلومات أساليب وإجراءات عديدة لتجنب تأثيرات هذه المخاطر أو تقليلها لأدنى حد:

١. الكوارث الطبيعية:

وتشمل الزلازل، والأعاصير، والفيضانات، التي تقوم بتدمير المكتبة أو مركز المعلومات بالكامل بما فيها من مواد وأجهزة ومعدات وتقنيات. لهذا يحرص المتخصصون منذ بداية استخدام تقنيات المعلومات على ضرورة الحفاظ على هذه التقنيات بوضعها في أماكن محصنة وإبعادها عن المؤثرات الطبيعية.[١]

١-التخريب المتعمد:

ويشمل إشعال الحرائق بشكل متعمد أو استخدام المتفجرات لتدمير الأجهزة وإدخال برامج حاسوبية تدمر ما متوفر من بيانات وبرمجيات على الحاسوب وتعرف هذه البرامج بالفيروسات.[٢]

٢-الأضرار غير المتعمدة:

التي تحدث بسبب الأهمال.فقد تحصل الكثير من الحرائق بسبب التماس الكهربائي أو رمي أعقاب السجائر في غير الأماكن المخصصة لها. وقد تحدث بعض الحوادث نتيجة انسكاب الماء أو السوائل الأخرى على تقنيات المعلومات.

٣-جرائم الحاسوب:

وجرائم الحاسوب تشمل الجرائم التي تتعرض لها أجهزة الحاسوب،من سرقة وتخريب وكذلك الجرائم التي يستفيد فيها مرتكبوها من إمكانيات الحاسوب لتنفيذها.مثل السرقات من الحسابات

[1] Raymond McLeod, Jr. Information Systems Concepts. New York: Macmillan, 1994, pp: 212-213.

[2] James A. Seen.Information Technology in Business: Principles, Practices, and opportunities.Englewood Cliffs, (NJ): Prentice Hall, 1995.p 598.

المصرفية، والتزوير، وتغيير البيانات وغير ذلك. وتتزايد خطورتها من أنها يمكن ارتكابها من أماكن بعيدة. أي: ليس من الضروري تواجد المجرم في مكان ارتكاب الجريمة.فموظف المصرف الذي يعمل في أحد المصارف البريطانية يستطيع أن يفتح الكترونياً باسمه حساب توفير في أحد المصارف السويسرية، ويودع فيه الكترونياً أي مبالغ يرغب بها ويحولها الكترونياً إلى حساب آخر في مصرف آخر في بلد آخر.

وهذه الجرائم في نمو متزايد نتيجة أفعال إجرامية غير مسؤولة لبعض مستخدمي الحاسوب مستغلين إمكانياتهم وصلاحياتهم وانتشار الحواسيب بشكل واسع في مختلف قطاعات المجتمع.وهي تشكل تحدياً أساسياً لتأمين تقنيات المعلومات.[١] وأهم جرائم الحاسوب ما يأتي:-

١-**سرقة الأموال:** وهي من أهم جرائم الحاسوب وتقنيات المعلومات حيث إنها تشكل ٣٦% من جرائم الحاسوب.فقد سرق من مصرف فارغو الأمريكي مبلغ (٢١) مليون دولار.ومن مصرف سيكوريتي باسفيك مبلغ (١٠,٢) مليون دولار عن طريق نقل الحسابات والمبالغ المودعة باستخدام الحاسوب وشبكات الاتصال.وهناك أضعاف هذه الجرائم المكتشفة وغير المكتشفة.

٢-**سرقة الخدمات:** أي: استخدام تقنيات المعلومات لحساب المصلحة الشخصية لأسباب تجارية، وهي تشكل ما يقرب من ٣٢% من كل جرائم تقنيات المعلومات. ومن أمثلتها قيام أحد مدراء مركز الحاسوب باستخدام حواسيب المركز لإنجاز أعمال لحسابه الخاص كان مردوده الشخصي منها بحدود (٥٣) الف دولار.

٣-**سرقة المعلومات:** وهي تمثل ١٢% من جرائم الحاسوب وتتعلق بسرقة البرامج من الحواسيب أو نسخها بشكل غير مسموح به،أو بدون علم مالك الجهاز أو منتجه في معظم الأحيان.

٤-**التلاعب بالبيانات:** فقد أدين أحد موظفي جامعة جنوب كاليفورنيا بسبب قيامه بتعديل درجات الطلبة مقابل دفعات مالية.وهذا أحد أشكال جرائم التلاعب بالبيانات التي تشكل حوالي ٨% من جرائم تقنيات المعلومات.

٥-**التزوير:** ويشمل الحذف والأستبدال المقصود لمحتويات الملفات، وتدمير ملفات بأكملها باستخدام الفيروسات أو أي أسلوب آخر.

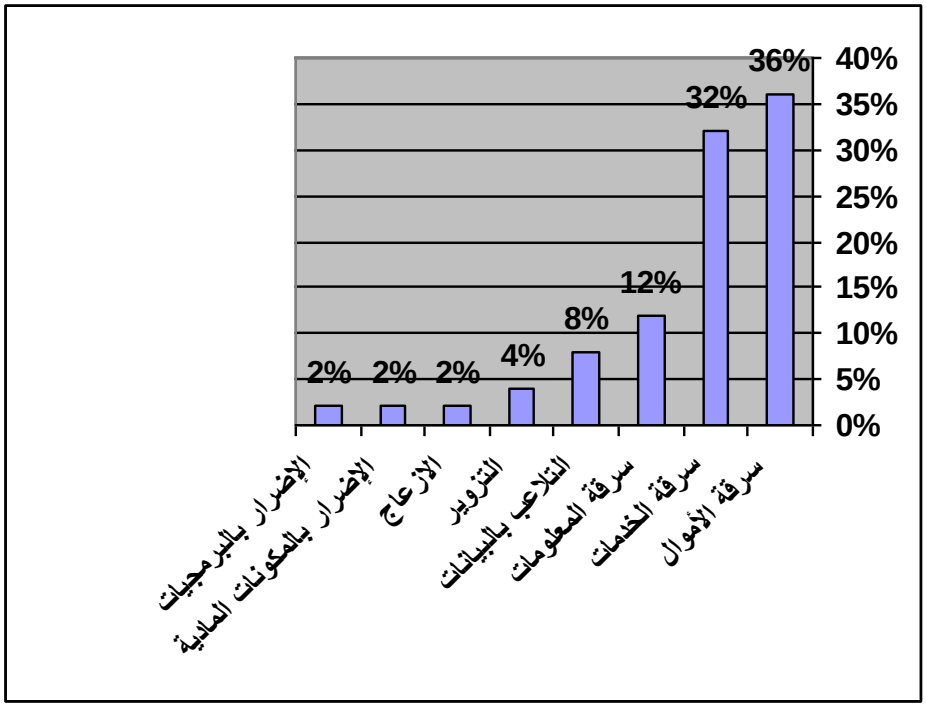
٦-**الأزعاج وانتهاك الخصوصية:** حيث بإمكان تقنيات المعلومات الحديثة أن تسهل عملية انتهاك خصوصية وحرمة الأفراد بالوصول إلى المعلومات السرية المخزونة بغض النظر عن أساليب

[١] عماد الصباغ.الحاسوب في إدارة الأعمال: أنظمة-تطبيقات-إدارة.عمان-الأردن: مكتبة دار الثقافة، ١٩٩٦، ص٣٨٣.

الحماية التي تعتمدها المكتبات ومراكز المعلومات، حيث يتم انتهاك اهتمامات الأفراد القرائية التي تعتبر من الخصوصيات التي يجب حمايتها. الأ أنه في الأنظمة المحوسبة يمكن لأي شخص أن يطلع على سجلات نظام المكتبة أو مركز المعلومات ومن أماكن بعيدة عن المكتبة أو عن مركز المعلومات، وهذا من أبرز الأمثلة على انتهاك خصوصيات الأفراد الواضح.

٧-**الأضرار بالمكونات المادية:** وتشمل تدمير أجهزة الحواسيب ومكونات معدات الاتصال وذاكرات الحواسيب، والطابعات، وأجهزة إدخال البيانات، وأجهزة الأستنساخ، وكل المعدات التي تعتبر من ضمن تقنيات المعلومات.

٨-**الأضرار بالبرمجيات:** وهذه يرتكبها عادة المبرمجون وغيرهم من العاملين في المكتبات ومراكز المعلومات ومراكز الحاسوب. حيث يستطيع هؤلاء الأشخاص القيام بأعمال تؤدي إلى الأضرار بالبرامج من خلال مسح أو حذف أو استبدال أجزاء من البرنامج أو إيعازات أو أوامر.



شكل (١): أهم أنواع جرائم تقنيات المعلومات[١]

فيروسات الحاسوب:

[١] المصدر السابق نفسه، ص٣٨٤.

وهي من أخطر الجرائم التي تتعرض لها تقنيات المعلومات، وتسبب خسائر كبيرة للمكتبات ومراكز المعلومات التي تعتمد في أداء عملها على تقنيات المعلومات.

والفيروس هو برنامج مخبأ يستطيع أن يبدل (دون علم المستخدم) طريقة عمل الحاسوب أو تعديل البيانات والبرامج المخزنة في ذاكرات الحواسيب. ويمكن لمعظم هذه الفيروسات أن تنسخ نفسها على برامج أخرى أو على الأقراص التي يتم إدخالها على النظام، وبهذه الطريقة تنشر نفسها من حاسوب إلى آخر، مثل انتشار الأوبئة. ويمكن انتشارها عن طريق شبكة الأنترنت أيضاً. وإذا لم يتم التعرف على الفيروس لفترة طويلة يمكن له أن يخرب المعلومات المخزنة بشكل كبير.

وأول فيروس تم التعرف عليه هو الفيروس الذي ابتكره طلبة جامعة جنوب كاليفورنيا عام ١٩٨٣ ليثبتوا أن أساليب الحماية التي كانت مستخدمة في الحواسيب المايكروية غير فعالة وغير مجدية.[١] أما في الوقت الحاضر فإن مشكلة الفيروسات تجاوزت في خطورتها محاولة التثبت من إجراءات السلامة والأمانة المهنية لتصبح واحدة من أعقد المشاكل التي تواجهها تقنيات المعلومات، وتعد من أكثر الأعمال التخريبية تحدياً لقدرات الحواسيب في العالم. وقد تم التعرف على أكثر من ١٥٠٠ فيروس لحد الأن.كما يظهر ما يقرب من ٥٠ فيروساً جديداً كل أسبوع.والفيروس موجود في كل أنواع الحواسيب والشبكات في كل أنحاء العالم. كما تم اكتشاف الفيروسات في بعض الأقراص المرنة الأصلية التي تحتوي على برامجيات أكبر شركات البرمجة في العالم.

ولكل فيروس صفاته وميزاته الخاصة (توقيعه) فبعضها يدمر البيانات من خلال كتابة رموز غير مفهومة على الأقراص التي تصيبها. وهناك بعض الفيروسات التي تسيطر على نظم التشغيل وتوقفها عن العمل. وتقوم أنواع أخرى من الفيروسات بإدخال إيعازات إلى نظام التشغيل تؤدي به إلى عرض رسائل على شاشة الحاسوب. وهناك فيروسات تنتقل بين الملفات وتقوم بإجراء تغييرات يسيرة في بعضها، وهي من أصعب الفيروسات في اكتشافها.[٢]

والحواسيب المايكروية تتعرض للفيروسات بسهولة؛ لأنها غير محمية بمعايير الحماية التي تستخدم في الحواسيب الكبيرة، لذا قامت معظم المؤسسات التي تعتمد على الحواسيب المايكروية في عملها بإصدار تعليمات خاصة بحماية هذه الحواسيب من الفيروسات، وتتضمن ما يأتي:[٣]

---

[1] James, A. Seen.Information.Op. Cite.pp: 71-72.
[2] Ibid. p. 549.
[3] Ibid. p. 72.

ضرورة تهيئة نسخ إضافية من البرامجيات والبيانات بصورة دائمية. وتخزين نظم التشغيل على أقراص محمية (Write Protected) وهذه العملية لا تبعد الفيروسات عن الحاسوب وإنما تمكن الأدارة من استعادة النظام إذا تعرض لأية مشكلة.

نصب واستخدام الحزم البرمجية المضادة للفيروسات. وهذه الحزم تعمل بطريقتين: الأولى، على أساس مسح الحاسوب للبحث عن أي فيروس. أما الطريقة الأخرى فتستخدم أساليب الذكاء الأصطناعي للتنبيه إذا كان النظام قد أطاع أي أوامر لنسخ إيعازات غير طبيعية إلى ملفات البرنامج. ولأن عدد محدود من الفيروسات تكون مسؤولة عن أكثر من ٨٠% من الأصابات، فهذه العملية تستمر إلى أن تحقق حماية معقولة للنظام والجهاز.

١. معرفة مصدر البرامج التي يتم التعامل معها، حيث إن معظم فيروسات الحواسيب الشائعة تنتشر حين ينسخ المستفيدون برامجيات العاب وتطبيقات بصورة غير قانونية (قرصنة برامجيات). وتحتوي الكثير من هذه البرامج على فيروسات وضعت بهدف مقصود هو الحماية من القرصنة. أي أن الفيروس يكون موجوداً على القرص الأصلي عند إنتاجه ولكنه غير فعال (نائم) فإذا استنسخ القرص أصبح الفيروس فعالاً بشكل مباشر وأصاب الحاسوب الذي يستخدم القرص المستنسخ ويعطله.

٢. إذا أصيب الحاسوب بفيروس يجب عدم الخوف واتخاذ الإجراءات الأتية:-

أ- خزن ما يمكن تخزينه من البيانات وإطفاء الجهاز فوراً.

ب- استخدام النسخة المحمية (Write Protected) من نظام التشغيل، وتشغيل الحاسوب به.

ج- تشغيل البرمجة المضادة للفيروسات مرتين على الأقل.

د- حين التأكد من أن النظام أصبح نظيفاً، يتم نسخ البرامجيات الأحتياطية لتنصيب البرامج على القرص الصلب من جديد.

لذا علينا تجنب الأصابة بالفيروس، فالحواسيب غير المرتبطة بشبكات تكون إجراءات حمايتها أسهل من الحواسيب المرتبطة بشبكات، حيث تتلخص أساليب حمايتها بتجنب استخدام أقراص البرامجيات الأصلية، وتجنب استخدام الأقراص على حواسيب غير مضمونة النظافة.

السيطرة على تقنيات المعلومات:

لقد أثبتت تقنيات المعلومات أنها تستطيع معالجة كميات هائلة من البيانات وإجراء معالجات معقدة بقدرات عالية الدقة مقارنة بالأساليب التقليدية اليدوية أو النظم الميكانيكية. غير أن هناك

أخطاء تظهر في النظم المحوسبة، وتقنيات المعلومات استخدمت وتستخدم في أغراض إجرامية، والبرامجيات والبيانات والمكونات المادية لتقنيات المعلومات قد دمرت خطأ أو بشكل غير متعمد.[١] لذلك تحتاج تقنيات المعلومات إلى سيطرات، فتقنيات المعلومات تحتاج إلى حماية من خلال سيطرات داخلية لضمان الجودة والتأمين.

والسيطرة مطلوبة لضمان تأمين تقنيات المعلومات ونظمها؛ لأن هذه السيطرة تعمل على تحجيم الأخطاء والجرائم وعمليات التخريب والتدمير إلى أدنى حد في خدمات المعلومات. وهناك ثلاثة أنواع من السيطرة، وهي:

١- السيطرة على المعدات المادية.
٢- السيطرة الأجرائية.
٣- السيطرة على نظم المعلومات.

وفي تأمين تقنيات المعلومات نكون بحاجة إلى السيطرة الأمنية، التي لا توثر على كفاءة المعالجات ودقتها على عكس السيطرات الأخرى، غير أنها تساعد في ضمان معايير متقدمة للنظام والأداء من خلال حماية النظام من الكثير من المشاكل. لأن غياب السيطرة الأمنية يؤدي إلى زيادة احتمال حدوث الأخطار الأتية:[٢]

١- سرقة الخدمات وضياعها.
٢- سرقة الموجودات المادية والبرمجية وضياعها.
٣- سرقة المعلومات الثمينة والحساسة.
٤- الأحتيال والدخول غير المخول بهدف التخريب أو التدمير.
٥- التلف الكبير من جراء الكوارث الطبيعية.

أساليب السيطرة على تقنيات المعلومات:

هناك أسلوبان يستخدمان في السيطرة على مختلف أنواع تقنيات المعلومات في مختلف المؤسسات وهما:

أولاً: أساليب الحماية المادية، وتشمل تزويد التقنيات بمعدات وأجهزة تساعد على حمايتها من الأخطار، ومنها ما يأتي:

[1] James A. O'Brien. Management Information systems: A managerial end user perspective. Homewood, IL: Irwin, 1990. p.542.

[2] عماد الصباغ. المفاهيم الحديثة في أنظمة المعلومات الحاسوبية. عمان، الأردن: مكتبة دار الثقافة، ١٩٩٧. ص ٢٥٥.

١-**السيطرة على المداخل والممرات:** عن طريق الحراسات وسجلات الدخول والخروج، وحمل البطاقات والباجات، والمراقبة عبر شاشات التلفزة المغلقة، واستخدام الأبواب الدوارة وأبواب الطوارئ ذات الأتجاه الواحد.

٢-**الموقع الأمن:** من الضروري وضع تقنيات المعلومات في بنايات منفصلة وغير معروفة لمن لا يهمه الأمر. كما من الضروري تجهيز نسخ إضافية من الملفات والسجلات والبيانات على أن توضع في أماكن حصينة وأمينة.

٣-**الحماية المادية:** وتشمل توفير مولدات كهرباء تعمل بشكل ذاتي في حالة انقطاع التيار الكهربائي. فضلاً عن منظم القدرة (UPS) لضمان استمرار التيار الكهربائي بشكل منتظم. ويفضل أن توضع تقنيات المعلومات في بنايات تكون أرضياتها أعلى من مستوى أرضيات البنايات المجاورة لتجنب المياه. كما ومن الضروري أن يكون في البناية مكيفات هواء وأجهزة ضبط الرطوبة التي تساعد في تقليل الأضرار التي قد تصيب الأجزاء الالكترونية الحساسة من التقنيات.

ثانياً: أساليب السيطرة الأجرائية: من الصعب جداً الفصل بين أساليب السيطرة المادية وأساليب السيطرة الأجرائية لتداخلهما مع بعض. فكلاهما يعملان على السيطرة على المداخل والممرات، الأ أن الفرق بينهما أن أساليب السيطرة المادية هي أساليب تتعامل مع الأجهزة والمعدات، بينما نرى أن أساليب السيطرة الأجرائية هي أساليب حماية وأمان وليس لها علاقة بالمكونات المادية. وفي معظم الأحيان نحتاج إلى استخدام أسلوب السيطرة المادية لتنفيذ أسلوب السيطرة الأجرائية، وأساليب السيطرة الأجرائية تشمل ما يأتي:-

١-تحديد الواجبات، والفصل بين واجبات العاملين المختلفة.

٢-صياغة إجراءات مقننة، وتوثيقها بشكل كامل وواضح وتوفيرها في كتيبات، وفي البرامجيات الحاسوبية أيضاً.

٣-ضرورة الحصول على التخويل قبل السماح لأي كان بإجراء التعديلات والتغييرات المهمة في البرامج والملفات والسجلات والبيانات.[١]

تأمين أجزاء تقنيات المعلومات:

تتكون أجزاء تقنيات المعلومات من عدة أجزاء مترابطة ومتفاعلة مع بعض لإنجاز ما مطلوب منها. وهذه الأجزاء تشمل: الحواسيب، وقواعد البيانات، ومعدات الاتصالات وغيرها. وقد تحدثنا عن تأمين الحواسيب أما تأمين بقية الأجزاء فكما يأتي:

[1] عماد الصباغ. أمنية التكنولوجيا في مراكز نظم المعلومات والمكتبات. بحث غير منشور.

أولاً: تأمين قواعد البيانات:

إن تأمين قواعد البيانات يبدأ من نظم إدارة قواعد البيانات (DBMS) (Database Management systems) التي تستخدم في بناء قواعد البيانات على الحواسيب المايكروية. وتمتاز هذه النظم بميزات وقدرات نظم إدارة قواعد البيانات المستخدمة في الحواسيب الكبيرة نفسها والتي تستخدم عدة طرق لضمان عدم انتهاك إجراءات الحماية من خلال عدم السماح لغير المخولين بالدخول إلى القاعدة. وهناك عدة مستويات من الحماية التي توفرها نظم إدارة قواعد البيانات الحديثة، التي تشبه بعدد من الأسيجة المحيطة بالبيانات، وهذه المستويات هي:[١]

١- **كلمات المرور (Passwords):** حيث يطلب الحاسوب من المستفيد إدخال كلمة مرور (Passwords) قبل أن يسمح له باستخدام برامج الحاسوب. ويمكن لنظم إدارة قواعد البيانات أن يكون لديها كلمات مرور خاصة بها لا يعرفها الأ المستفيد وحده. فبعد الدخول إلى الحاسوب يجب على المستفيد أن يدخل كلمة مروره ليتمكن من الدخول إلى قاعدة البيانات.

٢- **دليل المستفيد (User Menu):** بعد أن يدخل المستفيد عن طريق كلمة المرور يقوم نظام إدارة القاعدة بتدقيق قائمة دليل المستفيد، وهو عبارة عن قائمة بأسماء الأشخاص المخولين باستخدام القاعدة. وتكون هذه القائمة محفوظة في ذاكرة الحاسوب المايكروي. فإذا لم يكن اسم المستفيد مذكوراً في القائمة لا يسمح له بالدخول إلى قاعدة البيانات.

٣- **دليل الحقول (Fields Menu):** بعد اجتياز المستفيد لقائمة دليل المستفيد يقوم نظام إدارة قواعد البيانات باستشارة قائمة دليل الحقول التي تحدد عناصر البيانات التي يسمح للمستفيد التعامل معها وكيفية استخدامها. فقد لا يسمح لمستفيد معين الأ بقراءة القيد فقط، في حين يسمح لآخر بإجراء التعديلات على القيد، وهكذا.

٤- **الترميز (Coding):** يمكن للبيانات أن ترمّز بحيث تصبح بدون معنى لغير المستفيد المخول بقراءتها والذي استطاع بطريقة أو بأخرى المرور إلى قاعدة البيانات. وهذا الترميز يقوم به روتين معين في نظم إدارة قواعد البيانات الحديثة. ولا يملك مفتاح حل الرمز الأ المستفيد المخول.

فقواعد البيانات في المكتبات ومراكز المعلومات مثل (قاعدة الفهرس، أو قاعدة نظام الأعارة، أو قاعدة التزويد والطلب، أو غير ذلك) تكون أكثر أماناً في الوقت الحاضر، بالرغم من عدم وجود وسائل حماية تضمن تأمين القاعدة ١٠٠%.

ثانياً تأمين الاتصالات:

تعد تقنيات المعلومات المرتبطة بشبكة اتصالأت أكثر عرضة للأخطار الأمنية من التقنيات غير المرتبطة بشبكة. ونادراً ما نجد مكتبة أو مركز معلومات في الوقت الحاضر غير مرتبطة بشبكة أو أكثر من شبكات الاتصالات مثل (الأنترنت، وOCLC، وDialog) وغيرها. وتكون هذه

[1] Raymond McLeod, Jr. Information. Op. Cite. p.251.

الشبكات وقنواتها عرضة لعبث مجرمي الحواسيب المتواجدين على بعد الأف الكيلومترات لسرقة المعلومات أو الأموال، أو التخريب، أو إدخال الفيروسات، وغير ذلك من الجرائم.[1] لهذا ينبغي على أية مكتبة أو مركز معلومات تشترك بإحدى شبكات الاتصال أو المعلومات أن تهتم بالنواحي الأمنية بحزم وجدية. وذلك من خلال استخدام عدة إجراءات توفر لها مستوى مقبول من التأمين. وتأمين الاتصالات كأسلوب وقائي يشمل مسؤولية المكتبة أو مركز المعلومات، والسيطرة على البرامجيات، والسيطرة على المعدات والمكونات المادية، وتأمين الأبنية والإجراءات، ووضع خطة لتأمين الاتصالات.

النتائج:

[1] Ibid. pp: 282-284.

ينبغي على المكتبات ومراكز المعلومات التي تقتني تقنيات المعلومات أن تهيئ لها كافة مستلزمات الحماية والتأمين المناسبين، لأنها معرضة للمخاطر.

والمخاطر التي تتعرض لها التقنيات يمكن أن تكون ناتجة عن أخطاء غير مقصودة أو عن أفعال تخريبية وتدميرية. لذا لا بد من اتخاذ الإجراءات التي تمنع حدوث الخطر أو التقليل من تأثيره وأضراره إذا حدث فعلاً.

والأسلوب الناتج في الحد من الحوادث والمخاطر هو تصميم نظام سيطرة فاعل، واستخدام طرق رقابة عالية الدقة والكفاءة، ووضع ضوابط لمنع وصول غير المخولين إلى تقنيات المعلومات، والبيانات، والملفات.

وهناك إجراءات ضرورية لتأمين تقنيات المعلومات هي:

١- وضع التقنيات في أماكن أمينة.
٢- إتباع أساليب رقابة مشددة على الأبنية التي تحتوي التقنيات بحيث يمكن منع الأشخاص غير المخولين من الوصول اليها.
٣- إتباع أساليب الحراسة والأمن.
٤- وضع الأقفال المضمونة على أبواب البنايات التي تحتوي التقنيات والتأكد من إقفالها يومياً.
٥- استخدام كلمة مرور (Passwords) للدخول إلى الملفات. وإتباع بعض الإجراءات اللازمة عند السماح بإجراء التعديلات والحذف على تلك الملفات.
٦- وضع الخطط الأمنية اللازمة التي تكفل الحماية وتقليل آثار الدمار والحوادث التي تحدث.

Securing information technologies in libraries and information centers

Prof. Mahmoud Saleh Ismail

Abstract:
Information technologies are among the most important equipment acquired by libraries and information centers of all kinds. Most of these libraries and information centers become unable to perform their role if the information technologies they own stop working for any period of time. These technologies are not only important as physical equipment, but are more important to the qualitative aspects of how the physical system represents the library or information center. Libraries and information centers that rely on these technologies or that adopt computerized systems in all their operations may become unable to perform their easiest obligations towards their beneficiaries if I lost these techniques.