جامعة محمد بوضياف المسيلة

كلية العلوم الإنسانية والاجتماعية

المحاضرة الثامنة

مطبوعة أكاديمية

طلبة سنة أولى جذع مشترك علوم انسانية

مجالات علم المكتبات والمعلومات

* أمن المعلومات وتسيير المؤسسات الوثائقية *

أولا. مفهوم أمن المعلومات

ثانيا. المبادئ الأساسية لأمن المعلومات

ثالثا. تسيير المؤسسات الوثائقية

رابعا. مجالات التوظيف في ميدان أمن المعلومات وتسيير المؤسسات الوثائقية

إعداد الدكتور: سلامي اسعيداني

أستاذ محاضر أ في الإعلام والاتصال تخصص: اتصال استراتيجي

السنة الجامعية 2023/2024

أولا. مفهوم أمن المعلومات

أمن المعلومات علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لأخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.(Mills,1998, p33)

إن حماية المعلومات هو أمر قديم ولكن بدأ استخدامه بشكل فعلي منذ بدايات التطور التكنولوجيا ويرتكز أمن المعلومات إلى:

- أنظمة حماية نظم التشغيل
- أنظمة حماية البرامج والتطبيقات.
- أنظمة حماية قواعد البيانات.
- أنظمة حماية الولوج أو الدخول إلى الأنظمة.

من العوامل التي تهدد أمن المعلومان نورد الآتي:

1. التطورات التكنولوجية المتسارعة:

وتنبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة على السواء التي قد ترد من مصادر داخلية أو خارجية، كما أنها تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلى عدم الكفاءة اليومية المتوقعة. على سبيل المثال، قد تنتج الأعطال من أعطال كبيرة تؤدي إلى توقف العمل، أو إبطاء العمل بصفة دائمة، أو تقلل قيمة النظام وتفسخ خدماته. وفي هذه الحالة يجب مراعاة توقيتات الأعطال والتشويش الذي يتعرض له النظام عند التخطيط لأمن المعلومات من البداية.(Ruggles,1998, p89)

2. العوامل الفنية:

التي تؤدي لفشل نظم المعلومات عديدة ومتنوعة، كما قد تعتبر غير مفهومة في بعض الأحيان، أو تتغير على الدوام.

3. أخطاء النظام من سوء استخدام الأجهزة والبرمجيات:

الأخطاء الكامنة، التحميل الزائد أو المشكلات التشغيلية وغير ذلك. وقد تظهر الصعوبة في مكون النظام الداخلي كما في حالة أجهزة وملحقات النظام المتعلقة بوحدة الذاكرة، تجميع نظام الحسابات الشبكي أو النظام الموزع؛ أو في برمجيات نظم التشغيل والتطبيقات مثل المحرر، الجامع، شبكة الكمبيوتر المحلية LAN. وقد تكون الصعوبة نابعة من مكون النظام الخارجي كما في حالة دوائر الاتصالات عن بعد أو الأقمار الصناعية، أو نتيجة لتواصل وترابط مكونات النظام المختلفة معا. (Quinn, 1992, p80)

4. الفيروسات:

فغالبا تدخل الفيروسات في النظام من خلال البرمجيات المصابة، المتطفلين، الديدان أو القنابل المنطقية ... الخ. التي تمثل بعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويه، إتلاف أو تحريف بياناته ووظائفه المختلفة.(Howells, 1999, p100)

5- صعوبة صيانة وحماية أمن المعلومات والنظم والشبكات:

قد تنبع من تواجد بيئات متعددة من الأطراف المرتبطة بها كالمتعهدين، الموردين، البائعين، الخ. على سبيل المثال، توجد مشكلة جوهرية تتعلق بعدم توافر برمجيات تحكم ورقابة على الوصول المعتمد التي يتفق عليها كل الأطراف المعنية. ومن مقاييس الأمن الشائعة ضرورة توافق البرمجيات في بيئة الموردين المتعددة. وحتى يمكن التوصل لذلك، يصبح من الضروري موافقة منظمات التوحيد القياسي، الموردين، والمنظمات ومستخدمي نظم المعلومات على المعايير والتوجيهات الحاكمة لقياسات الأمن ذات الطابع الدولي.(Mills,1998, p39)

6- الأحداث البيئية الجسيمة:

وتشمل على الحرائق، الزلازل، الفيضانات، العواصف الكهربائية، الموجات الحرارية المرتفعة، والرطوبة الزائدة وما شابه ذلك. وقد يقع نظام المعلومات يضم الحاسبات الآلية وخطوط الاتصال، حيث قد يكرس له حجرات للحاسبات الآلية وحجرات تخزين البيانات لها ارتباطات وتجهيزات للطاقة الكهربائية والاتصالات تتعرض كلها للأحداث البيئية الجسيمة عند حدوثها. أما أوضاع التجهيزات الطبيعية المعكوسة فقد تظهر من خلال اختراق مقاييس الأمن الطبيعية في حالات انقطاع التيار الكهربائي، سوء استخدام أجهزة التكييف، تسرب المياه، أو بسبب الغبار والأتربة، الخ. وقد يتأثر نظام المعلومات من الإهمال المباشر في الأماكن المخصصة له، أو غير المباشر في نقاط الربط الجوهرية خارج المنظمة كما في إمداد الكهرباء أو قنوات الاتصال عن بعد. كما يساهم البشر وما ينشأونه من

مؤسسات مختلفة اقتصادية، سياسية أو اجتماعية في قصور قيمتها وأدائها مما ينجم عنه مشكلات أمنية أيضا. وقد يؤدي التنوع الكبير لمستخدمي نظام المعلومات والمتعاملين معه (العاملون، المستشارون، العملاء، المنافسون والجمهور العام) فيما يتعلق بتوعيتهم وتدريبهم واهتماماتهم المختلفة والمتفرقة في ظهور صعوبات خاصة بأمن المعلومات ونظمها.(Ruggles,1998, p90)

7- إن نقص التدريب والتوعية الملائمة عن أمن المعلومات وأهميته:

تسهم في الجهل باستخدام نظم المعلومات المناسبة. وبدون تنظيم دورات تدريب ملائمة، قد يجهل كثير من العاملين والمستخدمين بأعراض الأضرار النابعة من سوء استخدام نظم المعلومات، كما قد لا يستخدمون أي مقاييس أمن حتى البدائية منها، مما قد يؤدي إلى مزاولات تعود بالإساءة لأمن المعلومات. ويقدم اختيار كلمة المرور Password الذي يمثل نشاط المستخدم في كل أنحاء العالم بل يمثل النشاط الرئيسي لأي نظام معلومات مثالا واضحا لأمن المعلومات. فعلي الرغم من أن كلمات المرور تطبق عادة على رقابة الوصول إلى معظم نظم المعلومات، لا زال عدد قليل جدا من المستخدمين يعلم بأهمية الحاجة لأمن كلمة المرور بالطريقة التي تتمثل في تحديد أو إنشاء كلمة المرور ومن العواقب التي تتمثل في سوء استخدام النظام. (Quinn, 1992, p85)

على أنه بدون تدريب أو توجيه، يستطيع كثير من المستخدمين اختيار كلمات مرور واضحة يسهل تذكرها والتحقق منها مثل أسماء العائلة، الأسماء القصيرة، أو الكلمات المرتبطة بالمهام، الخ. وبعد الدخول أو الولوج في النظام، قد يترك المستخدمون غير المدربين كلمات المرور الخاصة بهم معروضة وغير مستخدمة على النهايات الطرفية النشطة المرتبطة بنظم الشبكة، كما يفشلون في إنشاء ملفات بيانات إضافية مساندة، ويشتركون في رموز التعريف وكلمات المرور، ويتركون منافذ الرقابة والوصول مفتوحة في مواقع الأمن مما يعرضها للاختراق. وكل ذلك يمثل مشكلات الأمن التي تظهر من الدخول على ملفات الحاسب لآلي، التحويل على الحاسبات أو النهايات الطرفية وامتلاك كلمات المرور وسوء استخدامها.

8- حدوث الأخطاء والاختراقات في تجميع البيانات والمعلومات ومعالجتها وتخزينها وإرسالها وحذفها. كما أن فشل عمل نسخ بديلة ومساندة للملفات والبرمجيات ذات الطبيعة الحرجة يضاعف من آثار الأخطاء والاختراقات ذات الطابع السلبي. وعندما لا توجد سياسة أمن للمنظمة المعينة تتصل بإعداد وحفظ نسخ إضافية مساندة لملفات المعلومات والبرمجيات التي تمتلكها، فإنها سوف تتحمل نفقات وخسائر واضحة ترتبط بالوقت والجهد والمال الذي ينفق في إعادة إنشائها من جديد. (Howells, 1999, p101)

9- سوء الاستخدام المقصود للنظام والوصول غير المعتمد له بغرض التطفل والنزوع للأذى وتعمد التخريب والتدمير والاحتيال أو السرقة تعتبر مخاطر وتهديدات خطيرة تؤثر سلبيا علي قابلية نمو حياة النظام والمنظمة المالكة له بل تؤثر أيضا على القابلية للبقاء والتواجد. على سبيل المثال، استنساخ البرمجيات غير المعتمد المنتشر على نطاق واسع قد يؤدي إلى خسائر كبيرة على النظم والمنظمات. (Ruggles,1998, p91)

ومن المألوف أن جزءا أعظم من التهديدات التي تواجه نظم المعلومات يأتي غالبا من المصادر الخارجية. كما أنه على النقيض من ذلك، فإن الأشخاص الذين منحوا حق الوصول المعتمد للنظام قد يعرضون تهديدات أعظم تواجه نظم المعلومات أيضا. فعلي الرغم من أنهم قد يكونوا مؤتمنين أو عاملين من ذوي النوايا الحسنة فإنهم بسبب التعب أو الإرهاق أو التدريب غير الملائم قد يقترفون أفعاللا غير متعمدة قد تسهم في حذف كميات كبيرة من البيانات الهامة للمنظمة التي يعملون بها. وفي حالة كون الأشخاص غير مؤتمنين فإنهم يسيئون استخدام نظم المعلومات أو يتعمدون الوصول المعتمد على العبث والتلاعب في النظام بطرق متعمدة بغية الاستغلال أو الثراء الذاتي للإضرار بالمنظمة التي يعملون بها.

10- برامج الحاسبات التي تمثل عنصرا مهما من عناصر نظام المعلومات، من المحتمل أن تكون مجالا خصبا للتهديدات التي يتعرض لها النظام، حيث قد تشتمل هذه البرامج على فيروسات الحاسبات الوالجة في النظام مما قد يعرض سرية بياناته وخصوصيتها وتوافرها للخطر المتزايد. بالإضافة لذلك فإن التحميل المتزايد للبيانات والمعلومات في النظام، أو تحويرها وتغييرها، وانتهاكات اتفاقيات الترخيص الممنوحة قد تعرض أمن نظام المعلومات للخطر الإضافي. على سبيل المثال، فإن تبديل البرنامج المرخص به بطريقة غير معتمدة، قد يؤدي إلى قصور الأداء عند تفاعل البرمجيات المعدلة والمراجعة مع أجزاء النظام الأخرى. كما أن إفشاء البيانات الضمنية قد يضر بالوضع التنافسي للمنظمة مما يؤدي إلى خسارتها بل وبقائها.(Mills,1998, p54)

من هذا المنطلق، يجب أن تمتد إجراءات الأمن الملائمة لما بعد النهايات الطرفية وخطوط الاتصال إلى مجال نظام المعلومات بالكامل. فعلي سبيل المثال، عدم ملائمة تداول وسائل تخزين البيانات والمعلومات (سواء كانت ورقية، ممغنطة، ضوئية، الخ)، بالإضافة إلى عدم ملائمة طريقة التخلص أو تدمير التقارير التي تمثل مخرجات النظام تؤدي إلى ثغرات أمنية مكلفة. فمثلا قد تشتمل مخرجات الحاسبات الورقية على معلومات ضمنية أو تنافسية أو مفاتيح تخص الوصول للنظام وأصوله، كما أن كثيرا من الشركات أو المؤسسات المختلفة لا يتوافر لها سياسات واضحة للتخلص أو استبعاد أصولها المعلوماتية مما يجعل أمن المعلومات سهلا في الاختراق.(Quinn, 1992, p88)

وقد يؤدي عدم وجود سياسات واضحة لاستخدام نظام المعلومات إلى مشكلات أمن ضخمة يتعرض لها النظام، كما في حالة أعمال الصيانة والسلامة عند نقص الأفراد المؤهلين، أو بسبب تغيير ودوران العمالة، أو إدخال تكنولوجيات متقدمة تتطلب مهارات جديدة، أو إبطاء العمل أو توقفه التي يجب مراعاتها من بدء التخطيط لنظم الأمن والشفافية المطلوبة.(Howells, 1999, p105)

ثانيا. المبادئ الأساسية لأمن المعلومات

أ- السرية:

السرية هو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالاطلاع عليها أو الكشف عنها. على سبيل المثال، استعمال بطاقة الائتمان في المعاملات التجارية على شبكة يتطلب إدخال رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة. يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من الوصول إلى أماكن تخزين أو ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين الرقم والبيانات بها. اما إذا كان الطرف غير المصرح له قد حصل على رقم البطاقة بأي شكل من الأشكال فإن ذلك يعد انتهاكا لمبدأ السرية في حفظ وتخزين البيانات. خرق السرية يتخذ أشكالا عديدة. تجسس شخص ما على شاشة الحاسوب لسرقة كلمات سر الدخول، أو رؤية بيانات سرية بدون علم مالكها، يمكن أن يكون خرقا للسرية. إذا كان الحاسوب المحمول يحتوي على معلومات حساسة عن موظفي الشركة، فإن سرقته أو بيعه يمكن أن يسفر عن انتهاك لمبدأ السرية. إعطاء معلومات سرية عبر اتصال هاتفي هو انتهاك لمبدأ السرية إذا كان طالب الاتصال غير مخول بأن يحصل على المعلومات. (Ruggles,1998, p93)

ب- التكامل (السلامة)

في مجال أمن المعلومات، التكامل (السلامة) يعني الحفاظ على البيانات من التغيير أو التعديل من الأشخاص غير المخولين بالوصول اليها. عندما يقوم شخص، بقصد أو بغير قصد، بحذف أو انتهاك سلامة ملفات البيانات الهامة أو الإضرار بها، وهو غير مخول بذلك، يعد هذا انتهاكا لسلامة البيانات. وعندما يصيب فيروس حاسوبا، ويقوم بتعديل بياناته أو يتلفها يعد هذا انتهاكا لسلامة البيانات، وكذلك عندما يكون الموظف (غير المخول) قادرا على تعديل راتبه في قاعدة البيانات والمرتبات، وعندما يقوم مستخدم (غير مصرح له) بتخريب موقع على شبكة الإنترنت، كل ذلك يعد انتهاكا لسلامة البيانات. وتعني سلامة البيانات كذلك، أن تكون التغيرات في البيانات مطردة، فعندما يقوم عميل

البنك بسحب أو إيداع، ينبغي أن ينعكس ذلك على رصيده في البنك. إن الإخلال بسلامة البيانات ليس بالضرورة نتيجة عمل تخريبي، فمثلاً، الانقطاع في النظام قد ينشئ عنه تغيرات غير مقصودة أو لا تحفظ تغيرات قد تمت فعلاً.(Howells, 1999, p106)

ج- توفر البيانات

يهدف أي نظام للمعلومات لخدمة غرضه، أن تكون المعلومات متوفرة عند الحاجة إليها. وهذا يعني أن تعمل عناصر النظام الآتية بشكل صحيح ومستمر: (Quinn, 1992, p99)

- الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات.
- الضوابط الأمنية المستخدمة لحماية النظام.
- قنوات الاتصال المستخدمة للوصول.
- نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات.
- منع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، او نظام الترقيات والتحديث.
- ضمان منع هجمات الحرمان من الخدمة.

د- إدارة المخاطر

إن المعالجة الشاملة لموضوع إدارة المخاطر هو خارج عن نطاق هذا المقال. ومع ذلك، سوف تقدم تعريفا مفيدا لإدارة المخاطر تكون كذلك بعض المصطلحات الأساسية ويشيع استخدامه في عملية إدارة المخاطر. ينص التعريف التالي لإدارة المخاطر: إدارة المخاطر هي عملية التعرف على نقاط الضعف والتهديدات الموجهة إلى موارد المعلومات التي تستخدمها المنظمة أو الشبكة المعلوماتية في تحقيق الأهداف التجارية أو الاخرى، والحد والتقليل من نقاط الضعف إن وجدت، لتأخذ في الحد من المخاطر إلى مستوى مقبول، على أساس قيمة موارد المعلومات إلى المنظمة.

هناك أمران في هذا التعريف قد يحتاجان إلى بعض التوضيح:(Mills,1998, p60)

- أولا، عملية إدارة المخاطر هي تكرار العمليات الجارية ويجب أن يتكرر إلى ما لا نهاية لان بيئة العمل المتغيرة باستمرار، والتهديدات الجديدة والضعف تظهر كل يوم.
- الثانية اختيار التدابير المضادة (الرقابة) المستخدمة لإدارة المخاطر يجب أن توازن بين الإنتاجية، والتكلفة، وفعالية التدابير المضادة، وقيمة الموجودات وحماية البيانات.

ثالثا. تسيير المؤسسات الوثائقية

إن المؤسسات الوثائقية عرفت تطورا كبيرا في كل أنواعها، ولا شك أن النمو السريع للتكنولوجيات الحديثة والتطورات السريعة في التقنية والاتصالات، والتغيرات المتواصلة في مهنة المكتبات والمعلومات هي من حتمت هدا التطور فقد انتقلنا من مؤسسة وثائقية تقليدية مرورا بالإلكترونية والرقمية إلى أن وصلنا إلى ما يعرف بالمؤسسات الوثائقية الافتراضية في العديد من البلدان وهي مؤسسات متطورة قادرة على التعامل والتفاعل مع مصادر المعلومات المختلفة.

أ- تعريف المؤسسات الوثائقية:

المؤسسة الوثائقية أداة تربوية فعالة ووسيلة أساسية لا يمكن الاستغناء عنها في أي مجتمع من المجتمعات. وادا كانت المؤسسات الوثائقية تضم مصالح كثيرة تخدم أغراضها، فليس هناك جهاز أكثر ارتباطا ببرامجها مثل المكتبة وليس هناك جهاز يخدمها بصورة مباشرة مثل المكتبة أيضا.

وتتمثل مكونات واحتياجات المؤسسات الوثائقية في النقاط التالية:

- انتقاء المعلومات التي يمكن بثها.
- إدخال المعلومات بأشكال مختلفة، بمعنى أن يكون قادراً على التعامل مع أوعية المعلومات شكلاً ومضموناً.
- مهارات في نظم الاسترجاع، وهي ذات أبعاد تكنولوجية وموضوعية في آن واحد.
- احتياجات قانونية وسياسة تنظيمية، وهذا يأتي في المرتبة الأولى حيث تحدد الحقوق والواجبات للهيئة أو المؤسسة التي يمكن من خلالها بناء استراتيجية واضحة وتحديد الأبعاد والأهداف من هذا المشروع.
- احتياجات بشرية مهتمة بالتخصص الموضوعي
- احتياجات مالية

ب- نشأتها وتطور المؤسسات الوثائقية:

إن المؤسسات الوثائقية لها كرونولوجية واسعة إذ كانت في بداياتها مؤسسات تقليدية (ورقية) تقوم بأداء وظائفها وتقديم خدماتها للمستفيدين بطرق تقليدية محضة. لكنها بدأت تعرف تطورا في دلك عندما انتقل الأمر إلى حوسبة هاته المؤسسات، وبالتالي استخدام الحاسب الآلي في معالجة البيانات وتسيير وتنفيذ العمليات الخاصة بها، ولم تكتفي التطورات بهذا القدر إنما اتسعت إلى استخدام تجهيزات الكترونية في الإدارة والتسيير في بعض أعمالها.

وقد تواصل هدا التغير لهده الأخيرة وصولا لما يعرف بالمؤسسات الرقمية والتي فيها مؤسسات رقمية المنشأ أي ذات أرصدة رقمية المنشأ أو مؤسسات تم تحويلها إلى رقمية من خلال رقمنة أرصدتها

الورقية. ومن هنا اتسع التفكير حول هدا النوع من المؤسسات بحثا عن مؤسسات ذات أرصدة رقمية المنشأ تقدم خدمات بفعالية أكبر ودون التقيد بالمكان والزمان أو بمعنى أخر خلق للمستفيد جو افتراضي يتفاعل فيه وكأنه في الواقع الحقيقي ولكن بطريقة افتراضية وهكذا ظهر ما يعرف بالمؤسسة الافتراضية.

ج- أنواع المؤسسات الوثائقية:

- **المكتبة الرقمية:**

هي مجموعة من المواد (نصوص وصور وفيديو وغيرها) مخزنة بصيغة رقمية ويمكن الوصول إليها عبر عدة وسائط. أهم وسائل الوصول لمحتويات المكتبة الرقمية هي الشبكات الحاسوبية وبصفة خاصة الانترنت.

من أهم مميزاتها:

1_تكون السيطرة على أوعية المعلومات الإلكترونية سهلة وأكثر دقة وفاعلية من حيث تنظيم البيانات والمعلومات وتخزينها وحفظها وتحديثها مما ينعكس على استرجاع الباحث لهذه البيانات والمعلومات

2_ يستفيد الباحث من إمكانات المكتبة الإلكترونية عند استخدامه لبرمجيات معالجة النصوص، ولبرمجيات الترجمة الآلية عند توافرها، والبرامج الإحصائية فضلاً عن الإفادة من إمكانيات نظام النص المترابط والوسائط المتعددة

3_إمكانية الحصول على المعلومات والخدمة عن بعد تخطي الحواجز المكانية والحدود بين الدول والأقاليم واختصار الجهد والوقت، وبإمكان الباحث أن يحصل على كل ذلك وهو في مسكنه أو مكتبه الخاص.

4_يمكن البحث والاستعارة منها في كل الأوقات ومن على بعد.

5_ إمكانية الاستفادة من الموضوع ومطالعته من قبل عدد كبير من الباحثين في وقت واحد

- **المكتبة الافتراضية:**

هي أن تتم معالجة المعلومات وتخزينها واسترجاعها بالطرق الالكترونية الحديثة، وهي أيضا تعتمد على مبدأ المشاركة والتعاون حيث يمكن للباحث الإفادة من المكتبة وزيارتها عن بعد (دون الذهاب إليها) والبحث عن المعلومات المرغوب فيها والاطلاع عليها وتصويرها والاستفادة من جميع مواد المكتبة في أي وقت ومن أي مكان في العالم، وذلك عبر الإنترنت.

من أهم مميزاتها:

- محتويات المكتبة الافتراضية لا تحتاج منك حيزاً مكانياً، فقد تتصفح ملايين الصفحات ولا يكون على طاولة مكتبك ورقة واحدة.

- إن المكتبة الافتراضية وبتوفيرها المصادر الالكترونية تحل كثيراً من إشكالية تداول المعلومات، والتي في أحيان كثيرة يصعب الحصول عليها.

- توفر المكتبة الافتراضية سرعة وسهولة الوصول إلى المعلومة في أي مكان من أماكن وجودها في هذا العالم الممتد.

- هناك نقاط وصول متعددة للمعلومات عبر المصادر الالكترونية المتاحة في المكتبة الافتراضية لا يمكن بحال أن تتوافر في المصادر المطبوعة التقليدية.

- **مراكز المعلومات ومراكز الأرشيف:**

إذ تتمثل مراكز المعلومات في المكان الذي يتم فيه توفير المعلومات بمصادرها المختلفة، ومعالجتها وحفظها واسترجاعها وبثها وتيسير سبل الاستفادة منها باستخدام تقنيات المعلومات الحديثة.

من أهم ميزاتها:

- **طبيعة خدمات المعلومات ومداها:** تقم مراكز المعلومات خدمات أكثر تقدماً وتطوراً من المكتبات مثل خدمات الإحاطة الجارية، البث الانتقائي للمعلومات، الترجمة، استخدام الأساليب المرئية مثل الحواسيب ..... الخ.

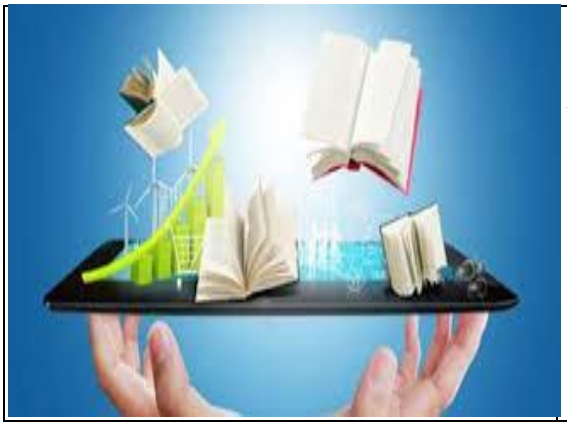
- **مصادر المعلومات:** هناك أنواع أخرى لمصادر المعلومات المعرفة تقليدياً. من هذي الأنواع: الإحصائيات، الخطط الحكومية، التحولات التجارية، التقارير، معلومات عن الشركات الأم أو المؤسسة الأم والشركات الأخرى في نفس المجال (أرقام المبيعات، الشركات المساهمين ' أرقام الإنتاج).

- **المعالجة الفنية للمعلومات:** تكون هذه العمليات بطريقة أكبر وأعمق في التحليل والضبط الموضوعي وعمليات الفهرسة والتصنيف والتكشيف والاستخلاص.

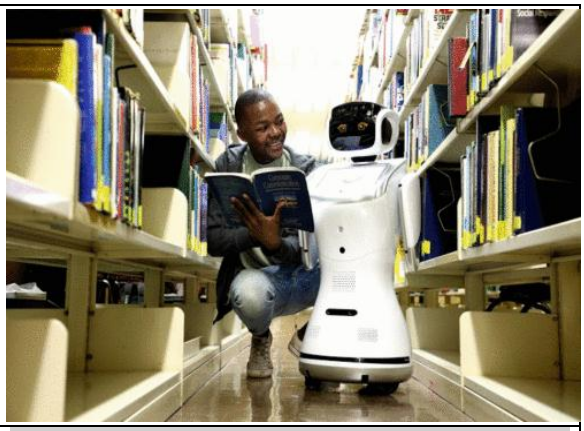
- **العاملين:** تضم نخبة من العاملين في مجال المكتبات والمعلومات (الاختصاصيين، المحررين، المترجمين، محللي النظم، المبرمجين .....الخ)

رابعا. مجالات الوصف الوظيفي في ميدان أمن المعلومات وتسيير المؤسسات الوثائقية

- خدمات المعلومات التي تقدمها المؤسسات الوثائقية:
- الخدمات الفنية أو الخدمات غير المباشرة
- الخدمات العامة أو الخدمات المباشرة
- خدمة الإحاطة الجارية
- خدمة الإجابة عن الاستفسارات

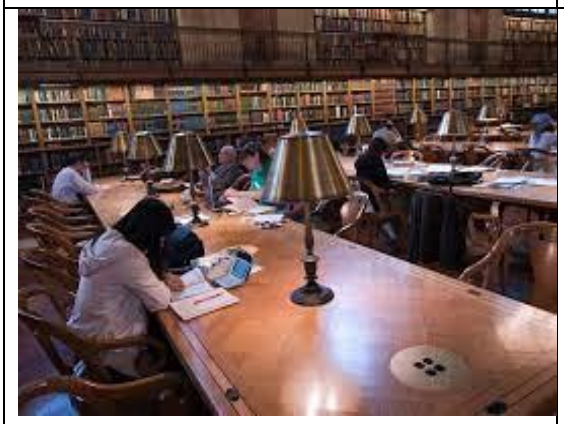


خدمات المعلومات التي تقدمها المؤسسات الوثائقية هي تلك الخدمات التي تقدمها المكتبات ومراكز المعلومات لمجتمع المستفيدين منها بصورة إلزامية سواء قدمت الخدمات يدوياً أو من خلال نظام آلي؛ ومن أمثلتها الاطلاع الداخلي، والخدمة المرجعية، والإعارة، والتصوير.



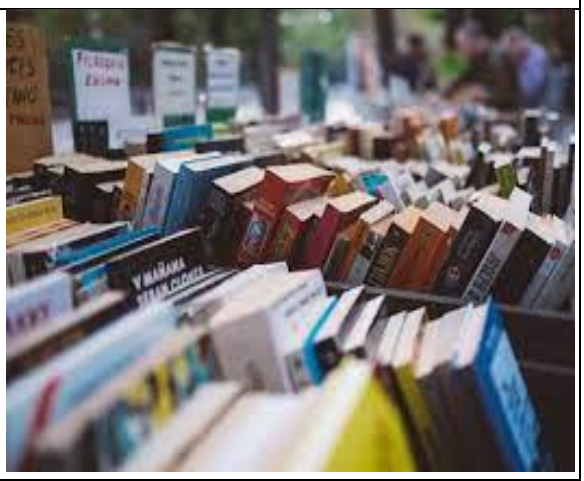
الخدمات الفنية أو الخدمات غير المباشرة

ويقصد بها الخدمات المتعلقة بالإجراءات والعمليات الفنية التي يقوم بها العاملون دون أن يراهم المستفيد مباشرة ولكنه يستفيد من النتائج النهائية لهذه الخدمات وتشمل خدمات المعلومات الفنية المتعلقة بإجراءات تنمية المقتنيات وعملية الفهرسة والتصنيف والتكشيف والاستخلاص



الخدمات العامة أو الخدمات المباشرة

ويقصد بها الخدمات المتعلقة بالإجراءات والعمليات الفنية التي يقوم بها العاملون دون أن يراهم المستفيد مباشرة ولكنه يستفيد من النتائج النهائية لهذه الخدمات وتشمل خدمات المعلومات الفنية المتعلقة بإجراءات تنمية المقتنيات وعملية الفهرسة والتصنيف والتكشيف والاستخلاص



خدمة الإحاطة الجارية

بأنها نظم لمراجعة الوثائق الحديثة من أجل اختيار مواد ومحتويات لها اتصال أو علاقة باحتياجات شخص أو مجموعة، وتسجل هذه المواد والمحتويات ثم إرسال مذكرات عنها إلى الأشخاص أو المجموعات التي تهتم بهذا الموضوع

خدمة الإجابة عن الاستفسارات

تعتمد هذه الخدمة على الخبرة التي يتميز بها اختصاصي المعلومات الذي يتولى الإجابة عن الأسئلة بحيث يتبع أسلوبا خاصا يرشده إلى الطرق الصحيحة التي تساعده في التوصل إلى المعلومات والإجابات المطلوبة.