الفصل الحادي عشر

أمـــن المعلومـــات

مقدمة

يقصد بأمن المعلومات حماية وتأمين كافة الموارد المستخدمة في تخزين ومعالجة المعلومات حيث يتم تأمين المؤسسة نفسها والأفراد العاملين فيها وأجهزة الحواسيب المستخدمة فيها، ووسائط المعلومات التي تحتوي على بياناتها، ويتم ذلك عن طريق إتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات كما يقصد بأمن المعلومات منع إساءة استخدام المعلومات أو تحريفها أو تسربها الأمر الذي يؤدي إلى إلحاق الضرر بالجهات التي تمتلكها من هذا نستطيع تحديد جوانب أمن المعلومات بالآتي :-

١- إمكانية تعرض المعلومات إلى الاستعمال غير المجاز كتحريفها أو إتلافها أو تعديلها وما يترتب على ذلك من ضرر.

٢- تسرب المعلومات الحساسة وتعرض أمن البلدان والمؤسسات والإدارات إلى الخطر.

٣- استغلال المعلومات الشخصية لغير الأغراض التي جمعت من أجلها واحتمال ابتزاز أصحابها.

ومن هنا تأتي أهمية المحافظة على المعلومات وتوفير جميع المستلزمات التي تضمن سلامة هذه المعلومات من الأخطار التي تهدد أمنها، حيث يشكل أمن المعلومات في الوقت الراهن حجر الزاوية في نهضة مراصد تكنولوجيا المعلومات والاتصالات.

وتعود أهمية أمن المعلومات إلى القيمة الحالية التي تمثلها المعلومات بالنسبة لمصارف المعلومات وشبكات الاتصال. فالمعلومات هي حجر الأساس الذي تستند إليه الأوساط المختلفة التي تتعامل معها سواء أكانت هذه الأوساط مؤسسات حكومية أم شركات أم مؤسسات تعليمية أم مصانع، أم الأفراد.

يشكل أمن المعلومات في الوقت الراهن حجر الزاوية في نهضة تكنولوجيا المعلومات الاتصالات فمن المعروف أن المسافة المتاحة للخصوصية تتناسب عكسيا مع التقدم التكنولوجي لأدوات المعلوماتية والاتصالات. لذا، فإنه من المفترض أن بناء تكنولوجيا وطنية لأمن المعلومات والاتصالات قد يسمح بعضوية دائمة في مجلس الأمن التكنولوجي.

كما يتضمن أمن المعلومات إجراءات وضوابط أمن قواعد البيانات بهدف التحكم في الدخول إلى قواعد البيانات والتحكم في تدفق البيانات وتحديد الوسائل التي يتم من خلالها التعرف على المستفيد وتحديد الأفراد المسئولين عن أمن قواعد البيانات، وتحديد الإجراءات والضوابط القانونية الواجب اتخاذها ضد من يحاول اختراق نظم المعلومات، وضد من يسيء استخدام البيانات.

وقد ظهرت العديد من الدراسات السابقة التي تناولت موضوع أمن المعلومات ومن بينها دراسة Rowley-J الصادرة عام ١٩٩٥ م والتي تناولت الجوانب التي تهدد أمن مرافق المعلومات..سواء في شكلها التقليدي أم في غيره بما في ذلك نظام الحواسيب واستعرضت الدراسة السياسات الأمنية ومكوناتها، كما تناولت تأثير التهديد، وفقدان الأمن على مرافق المعلومات مشيرة إلى أنواع المخاطر التي تتعرض لها.

وفي عام ٢٠٠٠ م صدرت دراسة لكل من S-Hawkins وD-C yen وD-C chau وتناولت الطرق المتعددة لتحقيق أمن البيانات للهيئات المرتبطة بشبكة الإنترنت، سواء كان ذلك عند نقل تلك البيانات عبر الشبكة أو عند تخزينها، بما في ذلك التشفير، والحوائط النارية، والشبكات الخاصة.

وفي العام نفسه صدرت دراسة لحسن طاهر داود تناولت مفهوم أمن المعلومات وكيفية تحقيقه سواء على مستوى تطبيق الأمن المادي للمؤسسات أو للأجهزة أو للأفراد، أم من خلال تشفير البيانات، أم ما سوى ذلك من أساليب، كما تناولت جرائم الحاسوب المختلفة وفيروسات الحاسوب وأوضحت الدراسة كيفية تحقيق أمن التطبيقات، وأمن قواعد البيانات، وأمن شبكات نقل المعلومات، وأمن

شبكات انترانت المحلية وأمن شبكة الإنترنت.

أمن البيانات :

يشير أمن البيانات إلى الحاجة لحماية البيانات من التوصل غير المشروع إليها أو من ضياعها المعتمد أو غير المعتمد.

أغراض حماية البيانات الرئيسية :-

١- السرية : التأكيد من أن المعلومات لا تكتشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.

٢- التكاملية وسلامة المحتوى : التأكد من أن محتوى المعلومات صحيح لم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو استقطاعه أو عن طريق تدخل غير مشروع.

٣- استمرارية توفير المعلومات أو الخدمة : التأكد من أن مستخدم المعلومات لن يتعرض إلى إنكار استخدامه لها أو دخوله إليها.

مناطق أمن المعلومات:

١) أمن الاتصالات : ويراد به حماية المعلومات خلال تبادل البيانات من نظام إلى آخر.

٢) أمن الحاسوب : ويراد به حماية المعلومات داخل النظام بكافة أنواعها وأنماطها كحماية نظام التشغيل وحماية برامج التطبيقات وحماية إدارة البيانات وحماية قواعد البيانات بأنواعها المختلفة.

أنماط ومستويات أمن المعلومات :

١- الحماية المادية : وتشمل كافة الوسائل التي تمنع الوصول إلى نظم المعلومات وقواعدها كالأقفال والحواجز والغرف المحصنة وغيرها من وسائل الحماية المادية التي تمنع الوصول إلى الأجهزة الحساسة.

٢- الحماية الشخصية : وهي تتعلق بالموظفين العاملين على النظام التقني المعني من حيث توفير وسائل التعريف الخاصة بكل منهم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن إلى جانب الوعي بمسائل الأمن ومخاطر

الاعتداء على المعلومات.

٣- الحماية الإدارية : ويراد بها سيطرة إدارة نظم المعلومات وقواعدها مثل التحكم بالبرمجيات الخارجية أو الأجنبية عن المنشأة، ومسائل التحقيق بإخلالات الأمن، ومسائل الإشراف والمتابعة لأنشطة الرقابة إضافة إلى القيام بأنشطة الرقابة ضمن المستويات العليا ومن ضمنها مسائل التحكم بالاشتراكات الخارجية.

٤- الحماية الإعلامية – المعرفية : كالسيطرة على إعادة إنتاج المعلومات وعلى عملية إتلاف مصادر المعلومات الحساسة بعدم استخدامها.

المخـــاطر :

١- المخاطر التي تتعرض لها نظم وشبكات المعلومات عن قرب :

- التطاول على التجهيزات المادية لمحاولة استخدامها دون معرفة كافية، مما يؤدي إلى إلحاق الضرر بها.
- إغلاق أجهزة الخادم لإيقاف عمل الشبكة.
- انقطاع الخدمة فجأة بسبب مولد الطاقة.
- التدمير المعتمد للأجهزة مما يؤدي إلى انقطاع الخدمة، والتلاعب في البيانات المعالجة آليا بما في ذلك محوها.
- سرقة الأقراص المحمل عليها البيانات.
- تعرض بعض مكونات الشبكة للعطل.
- قرصنة البرامج.

٢- المخاطر التي تتعرض لها نظم وشبكات المعلومات عن بعد :

- خطر (الهاكرز) Hackers.. وهو الشخص الذي حقق مهارة تكنولوجية عالية ويجد متعة خاصة في الدخول غير المشروع إلى أنظمة الحواسيب عبر الشبكات، وذلك لمجرد سعادته بالتغلب على التحدي متمثلا في اختراق نظام الحماية والأمان الذي تستعمله الشبكة.

- خطر (الكراكر) Cracker.. وهو الشخص الذي يخترق النظم الأمنية بغرض سرقة أو إفساد البيانات وتخريبها.

و يجب التفرقة بين نوعين Hackers وCrackers فأما Hackers فتكون أفعالهم إما من خلال الهواية أو العمل أصلا لتخريب مواقع هامة أو شراء بعض المنتجات والبرامج بطرق ملتوية، وأيضا الحصول على معلومات هامة من أماكن مختلفة وأخطرهم صانعو الفيروسات وملفات كسر الحماية حيث أنهم مبرمجون متخصصون ذوو قدرات عالية جدا، أما Crackers فهو مستخدم عادي أو هاوي لديه القدرة على البرمجة والبحث الجيد على صفحات الإنترنت إلى الوصول إلى ملفات كسر الحماية بغرض استعمالها وأيضا يكون من أصحاب النسخ غير القانوني للبرامج.

- مراقبة خطوط الهاتف والتجسس على مستخدمي الشبكة.
- الفيروسات وما تسببه من تخريب.
- العطل الذي يسببه أحد الأشخاص لنظام الأمن الخاص بالشبكة أو تمكنه من كشف إجراءات الحماية المتبعة.
- التشويش على الإشارات المنقولة عبر الكابلات غير المحمية عن طريق تعليق معدات معينة على هذه الكابلات بغرض التصنت عليها.

الفيروسات :

هي برامج حاسوب مكتوبة لإلحاق الضرر بأجهزة وبرامج الحاسوب، بعض الفيروسات حميدة عندما تقتصر على عرض رسالة أو إبطاء سرعة الحاسوب، ولكنها لا تلحق أي ضرر جدي في العتاد أو البرامج، أما النوع الآخر فهو مصمم لمهاجمة الملفات والبرامج وإلحاق الضرر البليغ بها.

و يمكن تقسيم الفيروسات إلى نوعين رئيسيين هما :

١- فيروس الماكرو macro virus:

وهو عبارة عن برنامج صغير مكتوب باستخدام برمجة داخلية للتطبيقات، ويقوم هذا الفيروس على عمل نسخ من نفسه بداخل الملفات المنشأة باستخدام

البرامج التطبيقية مثل معالج النصوص Word ,Excel ويعمل هذا الفيروس عند فتح أو إغلاق الملف أو عند حفظ ملف أو أثناء تشغيل البرنامج.

٢- فيروس قطاع التشغيل Boot Sector Virus:

وتتركز هذه الفيروسات في قطاع التشغيل لأقراص الحاسوب، ولا يحتاج كالنوع الأول إلى ملفات للدخول إلى جهاز الحاسوب حيث يصاب الجهاز بالفيروس إلى الذاكرة ويحدث عدوى لكل قرص يتم تشغيله على الجهاز،ويقوم الفيروس بكتابة نسخ من نفسه على كل قرص سليم ليصيبه بالعدوى.

وعلى الرغم من أن الانتشار بالنسخ التلقائي يعد أحد السمات المميزة للفيروسات، إلا أن مصطلح فيروس يطلق أيضا على برامج أخرى مصممة لإلحاق الأذى بالحواسيب على الرغم من أنها لا تستطيع أن تنسخ نفسها ومنها ما يلي :

١) أحصنة طروادة Trojan Horses:

وهي برامج تتضمن تعليمات للتخريب وإلحاق الأذى بالنظام على الرغم من انه في ظاهره يبدو كأنما يؤدي أعمال عادية، فهي توحي للمستخدمين بأنها تقوم بعمل معين في حين أنها في واقع الأمر تؤدي عملا تخريبيا في الغالب، فتقوم أحيانا بالتجسس ومتابعة كل ما يتم عمله من إجراءات أو تسجيله من بيانات على الجهاز المصاب بها.و أحيانا تقوم بتشفير البيانات أو مسحها. ولا تتمكن أحصنة طروادة من نسخ نفسها والالتصاق بالبرامج الأخرى ولكنها تؤدي عملا معينا تم تصميمها من أجله.

٢) القنابل المنطقيةLogic Bombs :

هي نوع من أنواع أحصنة طروادة ، وتعمل القنابل المنطقية عند حدوث شرط منطقي محدد مثل بلوغ الموظفين عددا محددا أو رفع اسم الموظفين من كشف الرواتب أو عند تشغيل برنامج معين لعدد محدد من المرات.

٣) القنابل الموقوتة Time Bombs:

القنابل الموقوتة هي نوع من أنواع أحصنة طروادة تعمل وفقا لتوقيت معين مثل ساعة محددة أو يوم محدد.

٤) الديدان worms:

لا تحتاج الديدان إلى برنامج آخر تلتصق به للقيام بدورها كما هو الحال في

الفيروس الذي يلزمه حاضن لتنفيذ مهمته،ولكنها تعمل بمفردها حيث لديها القدرة على إعادة توليد نفسها والانتقال من ملف إلى آخر ومن جهاز إلى آخر متصل بالشبكة لتحقيق الانتشار.

ولا تعمل الديدان على تخريب الملفات وإتلافها كما هو الحال بالنسبة للفيروسات ولكنها تقوم باستهلاك الذاكرة أو المعالج أو الأقراص أو سائر موارد الحاسوب ، وقد تؤدي إلى توقف نظام الحاسوب عن العمل.

٥) باب الفخ أو المصيدة Trapdoor :

وتسمى أيضا الأبواب الخلفية ، وتمثل "شفرة" توضع عمدا عند البرمجة لتجاوز نظم الحماية في البرنامج قد يستغلها البعض لأغراض تخريبية للتجسس وانتهاك الخصوصية وسرية البيانات أو لزرع الفيروسات.

٦) برامج الطوفان flooders:

تتمثل في مجموعة كبيرة جدا(مئات أو آلاف) من الرسائل التي تصل إلى الشبكة من جهات غير معروفة عن طريق البريد الإلكتروني أو عن طريق برامج TPQ، وهي بدون شك تسبب إزعاجا كبيرا حتى وان كانت لا تشكل أضرارا.

٧) برامج الخداع Spoofing:

تؤدي إلى تضليل الشخص المستقبل للمعلومات حيث تبدو أنها مرسلة من جهة معينة أي أنها في واقع الآمر تكون مرسلة من جهة أخرى ، الأمر الذي يسمح بدخول المعلومة إلى الشبكة ويجعل مستقبلها يتعامل معها دون معرفة مرسلها الحقيقي.. وهناك العديد من الشركات قامت بإنتاج برامج للتغلب على هذه الأنواع من الفيروسات من بينها Macafee وتعمل هذه البرامج المضادة للفيروسات الآتي.

١- فحص ذاكرة الحاسوب عند بدء تشغيله بحثا عن أي فيروسات.

٢- فحص قرص التخزين بحثا عن أي فيروسات، وفي حالة وجودها يتم أزالتها أو إلغاء الملفات المصابة بها.

٣- فحص البرامج المراد تحميلها على الحاسوب قبل تحميلها للتأكد من

سلامتها من الفيروسات.

٤- فحص الملفات سواء المتاحة للمشاركة أم المنقولة عبر الإنترنت أم المرسلة عبر البريد الإلكتروني للتأكد من خلوها من الفيروسات والتنبيه عند وجودها وتوفير الحماية ضدها.

٥- الفحص المستمر للنظام للتأكد من عدم وجود فيروسات به وأعطاء تنبيهات في حالة وجود فيروسات.

ويمكن تلخيص المخاطر الأمنية على المعلومات المتداولة بشبكة الإنترنت وطرق الوقاية منها كما هو موضح بالجدول التالي:-

التهديد	المصدر	الضرر	سبل الحماية وطرق الوقاية
الاختراق	(الهاكرز) عبر شبكة الإنترنت	التحكم التام بجهاز الضحية مع احتمالية سرقة المعلومات وجمع كلمات العبور أو تدمير الملفات الهامة	استخدام جدران اللهب (الحماية) مع تعطيل خاصية المشاركة في الملفات و الطباعة واستخدام كلمات عبور ذكية
الفيروسات و الديدان	البريد الإلكتروني والبرامج المجانية من الشبكة	تدمير أو تحريف الملفات والمعلومات في جهازك مع إمكانية نقل العدوى إلى كل من تراسلهم أو تتعامل معهم إلكترونيا	استخدام وتجديد البرامج المضادة للفيروسات بشكل متواصل وعدم فتح الملحقات المشبوهة ذات الطبيعة التنفيذية في الرسائل الإلكترونية وتجنب تنزيل البرامج المجانية مجهولة المصدر
أحصنة طروادة والبرامج	البريد الإلكتروني والمواقع	التجسس والتعرف على كلمات العبور وتدمير الملفات	تعطيل خاصية قبول وتشغيل البرامج في المتصفح مثل الجافا واستخدام برامج الحماية من

التهديد	المصدر	الضرر	سبل الحماية وطرق الوقاية
ذاتية التحميل	المشبوهة التي تستخدم جافا سكريبت وجافا أبلتيس وأكتف أكس		الفيروسات وجدران اللهب و تجنب تنزيل البرامج مجهولة المصدر
الهجوم على المواقع وتعطيلها	(الهاكرز) المحترفون	سرقة خدمة الإنترنت وتعديل المعلومات وتعطيل المواقع باستخدام جهازك دون علمك	وضع كلمات عبور واستخدام جدران اللعب وحماية الخادم ببرامج الكشف عن الحركة من وإلى الأجهزة الخادمة
التجسس على البريد الإلكتروني	(الهاكرز) ومن يشاركونك الجهاز فعليا	الإطلاع على الرسائل فعليا من جهازك أو اعتراض الرسالة أثناء الإرسال أو كتابة وإرسال الرسائل باسمك	استخدام كلمات عبور ذكية مع تجنب استخدام خاصية إكمال وحفظ اسم المستخدم وكلمات العبور وتشفير الرسائل مع الخروج الصحيح أثناء ابتعادك عن الجهاز
التجسس عن طريق رصد ضربات لوحة المفاتيح	مرسلي أحصنة طروادة ومن يستطيعون الوصول إلى جهازك في المنزل أو المكتب	تسجيل كل حرف ورقم تدخله عن طريق لوحة المفاتيح والإطلاع عليها لاحقا	استخدام برنامج مضاد للفيروسات ووضع كلمات العبور في جهازك لتقييد استخدام أي شخص آخر لجهازك

فالأخطار الرقمية تتسلل إلى المؤسسة مع إدخال أول حاسوب شخصي فيها، وتتنامى شدة هذه الأخطار وتأثيرها المخرب على عمل المؤسسة مع ازدياد عدد

الحواسيب الشخصية، ولتصل قمتها عند تأسيس شبكة محلية للربط بينهما ومن ثم الربط بين هذه الشبكة وشبكات الإنترنت والإكسترانت، ففي هذه المرحلة يضاف إلى الأخطار المحلية ضمان استعمال الشبكة والقرصنة المعلوماتية والتي أصبحت الشغل الشاغل في عالم الاتصالات الإلكترونية.

وبشكل عام، يمكن تعريف الأخطار الرقمية Digital Risks.. "بأنها مجموعة من الأخطار التي قد تواجه المؤسسات التي يعتمد نظامها الأساسي على الحاسوب وتشمل هذه الأخطار، عيوب التصميم، وعلة الألفية، والاحتيال والغش، وتخريب البيانات والفيروسات المخربة، والتعدي على حقوق النسخ، والمنظمات والعنف والتخريب المادي للأجهزة.

أسباب زيادة تعريض النظام للخطر:

ونورد فيما يلي حصر للأسباب التي تزيد من درجة تعرض أي نظام للأخطار:

- عدم دعم الإرادة العليا لأمن الحاسوب.
- عدم فعالية الإجراءات الأمنية المتخذة.
- عدم كفاية تدريب وتوعية الموظفين في مجال الأمن.
- عدم ولاء بعض الموظفين.
- عدم فعالية إجراءات إدارة الأخطار في المؤسسة.
- عدم كفاءة وسائل التأمين كطفايات الحريق.
- عدم كفاية إجراءات الرقابة والمراجعة.
- إذا كان نظام التحكم في استخدام الوثائق غير آمن.
- إذا كانت إجراءات استعادة النشاط غير آمنة.
- عدم فعالية أساليب اكتشاف الخطأ في النظام.
- إذا كانت عملية تطوير التطبيقات غير آمنة.
- إذا كانت صيانة النظم والتطبيقات غير آمنة.
- إذا كانت إجراءات قبول البرمجيات غير آمنة.

- إذا كانت خطة الطوارئ غير شاملة.
- إذا كان نظام الاتصالات غير آمن وغير موثوق به.
- إذا كانت إجراءات الإدخال والإخراج غير آمنة.
- عدم فعالية ضوابط دخول الأفراد.
- عدم كفاية ضوابط استخدام الطرفيات والنظام ككل.

الأساليب التي تتبع لحماية أمن المعلومات :

أولا : **أساليب الحماية الفيزيائية** :

و لقد لخصها مارك فيما يلي :

١- حفظ أجهزة الخادم داخل غرف مغلقة أو ضمن الإداريين وتأمين النوافذ خصوصا إذا كانت قريبة من الأرض.

٢- اختيار الكابلات ذات الألياف الضوئية (Fiber Optics) لأنها تلغي الإشعاع الثانوي لكابلات، وبالتالي تمنع التنصت على البيانات خلال نقلها عبر هذه الكابلات خصوصا إذا كانت هذه البيانات غاية في الأهمية.

٣- حماية التمديدات وكابلات الشبكة من أجهزة التنصت من التعرض للثني والقطع في حالة وضعت تحت قطع المفروشات الثقيلة، وذلك بتمريرها عبر الجدران وفوق السقف وتحت الأرض.

٤- استخدام الكابلات المغلقة لتقليل الإشعاع الثانوي المنبثق من خلالها.

٥- استخدام أجهزة إنذار آلية وتوفير المراقبة عن بعد عن طريق الدوائر التلفزيونية المغلقة.

ثانيا : **التحكم في الوصول إلى الشبكة** :

تتلخص الوسائل والأساليب والمعدات المتعلقة بحماية المعلومات من السرقة والانتهاك عبر شبكات الاتصالات فيما يلي:

١- اعتماد الوسائل الكفيلة بالسيطرة على البيانات المنقولة.

٢- اعتماد نقاط تدقيق في البرامج لتسجيل المراحل المختلفة التي تمر بها كل عملية تراسل.

٣- السيطرة على خطوط تناقل البيانات ووضع التحضير اللازم لحماية تناقل البيانات.

٤- وضع أجهزة إلكترونية لتحسس محاولات سرقة المعلومات.

٥- توثيق أساليب استخدام خطوط تناقل البيانات ضمن الوثائق القياسية كمركز الحاسبة المركزية.

٦- تحديد كلمات المرور للدخول إلى البرامج وتغييرها دوريا.

٧- عدم ظهور كلمات المرور على الشاشات للمحطات الطرفية.

٨- ملائمة موقع الحاسوب وكفاءة مستلزمات التشغيل.

٩- تخصيص اسم أو رقم لكل مستخدم للشبكة USER-ID وكلمة مرور PASSWORD مع الاهتمام بأن المستخدم لديه ممارسة ما يريد ممارسته بموارد الشبكة.

١٠- الاستعانة بتقنية البيولوجيا الإحصائية وهي تقنيات تعرف بهوية المستخدم بشكل منفرد عن طريق بصمة إصبعه أو بصمة يـــده أو بصمة صوته أو غير ذلك من معرفات فردية وتستخدم على غرار كلمات المرور.

١١- مراقبة النظام الذي تسمح به أغلب نظم تشغيل الشبكات الحديثة من خلال إتباع سياسة التدقيق Logging Security التي تتيح معرفة من يفعل ماذا على الشبكة.. وذلك عن طريق :

- تقصي محاولات دخول كل مستخدم.
- تقصي محاولات نجاح أو فشل هذا المستخدم لموارد الشبكة.
- تقصي احترام المستخدم لحقوقه.
- تتبع نجاح أو فشل كل محاولة لإعادة تشغيل النظام أو إقفاله.
- تتبع نجاح أو فشل كل محاولة لمعالجة النظام مثل استخدام التطبيقات

وغيرها.

- نظام حماية أمينة للإنترنت عن طريق بناء بوابة أو حاجز عازل بين الشبكات الداخلية العائدة لهيئات خارجية وشبكة الإنترنت حيث يتم التحكم باستخدام هذا الجدار في عملية الخروج من والدخول إلى الشبكة المحلية مما يضفي على الشبكة المحلية نوعا من الحماية.
- حماية الممتلكات على شبكة الإنترنت بما يعرف بـ (شرطة الإنترنت) Internet Police ومهمتها ضبط أي مستخدم من مستخدمي الإنترنت عند قيامه بمحاولة التسلل إلى أي موقع سري أو خاص بأحد المستخدمين.
- نظم خاصة تسمى حواجز النار (جدران الحماية) Firewall.وهي آلية دفاعية تقوم على تقنين تدفق المعلومات من وإلى الشبكة من خلالها وفقا لسياسات ومعايير محددة سلفا والهدف منها هو حجز كل ما هو غير مرغوب فيه خارج البيئة المحمية وقد صنفه الباحثون بأنه من أنجح سبل الحماية التي اتبعت حتى الآن. ووظائف الحواجز النارية تتمثل في الآتي :

١- فحص كل الأنشطة الداخلة إلى الشبكة من مصادر خارجية مثل الإنترنت أو الشبكات الواسعة WAN.

٢- ضبط المنافذ Ports المستخدمة بحيث يسمح باستخدام منافذ معينة لأغراض معينة.

٣- رفض وصول أنشطة معينة من عناوين محددة.

ويراعى في الحوائط النارية ألا تؤدي إلى إعاقة عمل مستخدمي الشبكة الفعليين حتى تؤدي الغرض منها على النحو المطلوب، وتعمل حوائط النار عادة وفقا لقواعد أمنية محددة يضعها مدير الشبكة الداخلية، كأن تسمح سياستها بالمرور من الخارج إلى الداخل نهائيا أو تسمح به في حدود معينة كالسماح بالمرور لمستفيدين دون غيرهم، أو لمواقع دون غيرها أو ما شابه ذلك.

وهناك اتجاهان متبعان لضبط الفعل التلقائي default للحوائط النارية وهما على النحو التالي :-

١- أن يكون الفعل التلقائي default هو الإباحة : ويقصد به أن كل ما لم ينص على منعه فهو مباح.

٢- أن يكون الفعل التلقائي default هو المنع: ويقصد به أن كل ما لم ينص على إباحته فهو ممنوع.

و يعد الاتجاه الثاني هو الأكثر إحكاما للأمن، أما الأول فهو الأفضل بالنسبة للمستفيدين.

التشفير Encryption حيث يتم تشفير البيانات عند إرسالها خلال الشبكة وفكها لدى المرسل إليه (Decryption).. يعرف التشفير بأنه عملية تشكيل البيانات باستخدام خوارزمية معينة تسمى المفتاح Key تصبح بها غير قابلة للقراءة إلا بعد استخدام الخوارزمية لفكها، ويتم عادة تشفير البيانات قبل إرسالها عبر الشبكة وذلك لضمان سلامة وصولها دون التعرض لأي عملية تجسس أو تحريف لمضمونها على أن يتم فك الشفرة لدى مستقبل الرسالة باستخدام مفتاح فك الشفرة.

وينبغي الحرص على تشفير البيانات عند الرغبة في إرسالها عبر الشبكة، سواء كانت تلك البيانات كلمات مرور أو أرقام بطاقات ائتمان أو رسائل بريد إلكتروني أو ملف أو غير ذلك.

ويمكن قراءة البيانات المشفرة واضحة من قبل أي شخص يعرف مفتاح الشفرة.

و يتم في بعض الأحيان كسر الشفرة من قبل آخرين والتعرف على مفتاحها فلهذا ينبغي أن يكون مفتاح الشفرة طويل ليصعب عملية كسره. وعلى سبيل المثال هناك شفرات بطول (٤٠ بت) وكذلك بطول (٥٦ بت) كالمستخدمة من قبل الحكومة الأمريكية والمعتمدة على نظام Data Encryption standars (DES).

و هناك وسائل أمن (حماية) أخرى للمعلومات هي :

١- أمن الأجهزة ويتم ذلك من خلال :

- تأمين الأجهزة داخل غرفة الحاسب (التحكم).
- تأمين النهايات الطرفية والطابعات.
- المواقع البديلة مكان بديل يتم استخدامه في حالة تعذر استخدام الحاسب الأصلي.

٢- أمن وسائط المعلومات :

- توفير مستوى حماية مناسبة للاسطوانات والأشرطة المغنطة والأقراص الضوئية التي تحتوي على المعلومات.
- الاحتفاظ بالنسخ الاحتياطية في مكان بعيد عن الموقع ويتم تخزينها في خزائن مقاومة ضد الحريق والماء والزلازل.
- يجب أن يقتصر الوصول إلى مناطق تخزين هذه الوسائط على الأشخاص المصرح لهم دون غيرهم.
- الاهتمام بإتلاف النفايات والمخلفات.
- الحذر عند استخدام بعض الأجهزة الإلكترونية بقرب وسائط المعلومات، وذلك لاحتمال تأثيرها على البيانات المسجلة.

٣- أمن الأفراد :

- تنظيم ومتابعة تسجيل دخول الموظفين وخروجهم.
- تنظيم دخول الزائرين وضرورة وجود سجل للزوار ومتابعتهم.
- مراقبة اتصال المستفيدين من الخارج ومتابعة استخدامهم للنظام.
- الأخذ في الاعتبار إلغاء أو تعديل الصلاحيات للموظف في حالة الاستقالة أو إنهاء الخدمة أو تغيير مجال العمل.
- اختيار الموظفين بعناية خصوصا الذين يتولون مراكز حساسة تكون لها صلاحيات عالية لاستخدام المعلومات.
- عدم منح الموظف حديث التعيين صلاحيات عالية لاستخدام النظام.
- ضرورة وجود قائمة أو نظام آلي لدى مسئول أمن نظام المعلومات تضم الأشخاص المصرح لهم باستخدام النظام وصلاحياته.
- ضرورة حصول كل مستخدمي النظام على تدريب مناسب حول الأمن والإجراءات اللازمة للنظام.
- يجب أن تتضمن عقود التوظيف شرطا يمنع الموظفين من إفشاء المعلومات

الحساسة أو إفشاء إجراءات الأمن والرقابة.

العلاقة بين الرقابة والأمن :

أن الإخلال بأمن البيانات والمعلومات يمكن أن يكون حادثة عرضية أو أمرا متعمدا ، والجدير بالذكر أن الحوادث العرضية أكثر تأثير كما أنها شائعة الحدوث مقارنة بالحوادث المتعمدة، وللحفاظ على أمن مكونات النظام لابد من توافر الخصائص التالية:

١- الكمال: أي أن يكون النظام كاملا إذا قام بما هو مطلوب منه، ويحاول مصممو النظم بناء نظام يتضمن ما يسمى بالنظام الوظيفي، بمعنى استمرار النظام في العمل حتى إذا كان هناك جزء أو أكثر منه لا يعمل.

٢- القابلية للمراجعة: يقصد بها سهولة اختبار، والتأكد من أداء النظام،ولكي يكون النظام قابلا للمراجعة فلابد من مقابلة اختبار المسؤولية بمعنى وجود شخص واحد مسئول عن الأحداث داخل النظام،أما الاختبار فهو الوضوح بمعنى أن الأداء غير المقبول من النظام يجذب انتباه ويلقى مديرو النظام.

٣- القابلية للرقابة: من أهم وسائل جعل النظام قابل للرقابة هو تقسيمه إلى نظم فرعية، بحيث يتعامل كل نظام فرعي مع مجموعة من العمليات المنفصلة عن النظم الفرعية الأخرى والرقابة تتكون من كافة الوسائل، والسياسات،والإجراءات التنظيمية للتأكد من أمن وأمان الأصول التي تملكها المنظمة،وصدق ودقة السجلات،ومطابقة العمليات لمعايير الإدارة وتتضمن الرقابة على نظم الحاسوب مزيج من الرقابة العامة ورقابة التطبيقات.

أ- الرقابة العامة :

تتناول التأكد من فاعلية العمليات الخاصة بإجراءات البرمجة وهي تشمل:

- الرقابة على عمليات تطبيق النظام: وتهدف إلى التأكد من أن نظم المعلومات المعنية على الحاسوب تقابل احتياجات المستخدم.

- الرقابة على التصميم: يتم بناء خصائص ومعايير الرقابة على تصميم النظم من خلال محللي النظم ، إداريو قاعدة البيانات ، مدير شبكة الحاسبات ، "ويجب مراعاة أن لا تزيد تكلفة الرقابة عن المنافع المترتبة عليها".
- رقابة البرمجيات: يغطي هذا النوع من الرقابة برمجيات تشغيل النظام والتي تقو م بتنظيم إدارة موارد الحاسوب لتسهيل تنفيذ البرمجيات التطبيقية.
- الرقابة على المكونات المادية: يجب حماية الأماكن التي يوجد بها الحاسوب بالطريقة التي تسمح للأفراد المرخص لهم فقط في التعامل مع الحاسوب ،كما يجب كذلك حماية النهايات الطرفية.
- الرقابة على تشغيل الحاسب: وهي تشمل عمل إدارة الحاسوب حيث تساعد على التأكد من أن إجراءات البرمجة متناسقة وتطبق بطريقة صحيحة على تخزين وتشغيل البيانات.وهي تتضمن الرقابة على تجهيز الحاسوب للقيام بوظائفه وتشغيل البرمجيات.
- الرقابة على أمن البيانات :وهي تتضمن التأكد من ان الوصول المعتمد هو الذي له الحق في استخدام البيانات كذلك حماية البيانات ضد التزوير أو السرقة أو التلف وما إلى ذلك..ويصعب تحقيق أمن البيانات في حالة الاتصال والوصول المباشر On-Line عن طريق النهايات الطرفية.

ب ـ الرقابة على التطبيقات.

تشير إلى الرقابة على كل تطبيقات الحاسب بصورة منفصلة مثل الأجور وحسابات الذمم، وتشمل سواء الإجراءات الآلية أو اليدوية الرامية إلى التأكد من ان البيانات المعتمدة والدقيقة هي التي يتم تشغيلها بوساطة التطبيقات. وتهدف الرقابة على التطبيقات إلى تحقيق الأتي:

١- كمال المدخلات وتحديثها.

٢- دقة المدخلات وتحديثها.

٣- الصدق.. يجب مراجعة البيانات بالطريقة التي تتناسب وتتوافق مع العمليات التي تستخدم فيها البيانات".

٤- الصيانة.. يجب ان تظل ملفات البيانات صحيحة وحديثة.

أمن مرافق المعلومات :

و يقصد بأمن مرافق المعلومات توفير الوسائل والإجراءات التي تحقق الحماية من التهديدات التي تؤدي عادة إلى فقد إحدى جزيئات نظام مرفق المعلومات.

وأحيانا يطلق عليه (الأمن الصناعي) وهو ما يوفره الإنسان من وسائل للمحافظة على سلامة وأمن مرفق المعلومات، وما به من أوعية معلومات ويما يضمن سلامة العمل والعاملين والمستفيدين على السواء.

ويقصد بمرافق المعلومات الوحدات الإدارية والتنظيمية المسئولة عن تنظيم خدمات المعلومات وتقوم بتجميع أوعية المعلومات وتنظيمها وتجهيزها لتسيير سبل الإفادة منها وتشمل المكتبات ومراكز المعلومات على اختلاف مستوياتها التي يمكن اللجوء إليها التماسا للمعلومات.

أمنية التكنولوجيا في مرافق المعلومات :

تتعرض مرافق المعلومات إلى عدة مخاطر يمكن أن تكون ناتجة عن أخطاء غير مقصودة أو بسبب أفعال تهدف إلى التدمير والتخريب، وفي كلتا الحالتين لابد من اتخاذ الإجراءات الكفيلة بمنع حدوث الخطر، والتقليل من تأثيره وأضراره إذا ما حدث فعلا، ومن الإجراءات التي يتم اتخاذها لضمان أمن تكنولوجيا المعلومات هي:

١- إيواء التكنولوجيا في أماكن حصينة ومأمونة.

٢- وضع رقابة مشددة على البنية التي تحوي التكنولوجيا.

٣- استخدام عبارات مرور للدخول إلى الملفات، واتخاذ إجراءات أخرى عند السماح بإجراء التعديلات والحذف.

٤- وضع خطة أمنية محكمة للحماية والتقليل من آثار الحوادث التي يحتمل حدوثها.

المسؤولية الإدارية لأمن المعلومات:

١- معرفة متطلبات الحماية الحقيقية للنظم وإتاحتها بشكل يضمن حمايتها

أمنيا.

٢- وضع السياسات المتطورة التي تضمن أقصى درجات الحماية ومتابعة تطويرها.

٣- التعامل مع موردين موثوق بهم.

٤- نشر الوعي التكنولوجي والإداري.

أساليب حماية مرافق المعلومات من الأخطار المختلفة التي عادة ما تهددها:

١- الحماية العامة للمبنى :

يجب اختيار موقع مبنى مرفق المعلومات بعيدا عن الإخطار البيئية المحتملة ويجب العناية بتحديد الأشياء التي يمكن أن ينشأ عنها أخطار كبيرة مثل الوقود وخزانات المياه ويجب استخدام مواد مقاومة للحريق عند البناء.

٢- الوقاية ضد الحريق :

هناك أمور يجب الالتزام بها بكل دقة لتفادي الحريق وتقليل الخسائر ونذكر منها مايلي :-

- استخدام مواد مقاومة للحريق قدر الإمكان.
- منع التدخين في الأماكن الحساسة.
- استخدام خزائن ضد الحريق لوسائط تخزين البيانات.
- استخدام وسائل اكتشاف الحريق والإنذار بحدوثه.

٣- حماية الخدمات الأساسية :

و هي التي يؤثر تعطيلها بشكل كبير على أداء الحاسوب ومن أهمها :

- مصادر الطاقة الكهربائية يجب استخدام مصدر يضمن الإمداد بالطاقة.
- استخدام مولدات احتياطية لتوليد الكهرباء.
- الاتصالات الهاتفية ويجب إجراء الصيانة المستمرة للخطوط الخاصة واستخدام خطوط اتصال بديلة وتأمين خطوط الاتصال ضد التنصت أو

التداخل واحتمال التخريب.

- تكييف الهواء يجب صيانة وحدات التكييف وإعداد وحدات تكييف بديلة.

٤- أمن أجهزة تكنولوجيا المعلومات :

و تشمل تأمين الأجهزة داخل غرفة الحاسوب من خلال التأكد من الدخول والخروج وتأمين مصادر الطاقة وإجراءات الطوارئ.

٥- أمن وسائط المعلومات :

إن الوسائط التي تستخدم لتخزين المعلومات يجب أن تحصل بدورها على القسط الوافر من الاهتمام ويجب اتخاذ الاحتياطات والتدابير لتأمين مرافق تخزين المعلومات من خلال تخزينها في أماكن محمية وملائمة وإجراء النسخ الاحتياطي.

٦- حماية المحتوى :

من بين أهم المسائل الشائكة التي تحتاج إلى نظم حماية كفأه وفاعلة حماية المحتوى " الثروة المعرفية والتكنولوجية " ويمثل المحتوى الموارد الثمينة المتراكمة من المعارف والمعلومات والخبرات والمهارات، ويقع في قلب المحتوى المعرفي تكنولوجيا المعرفة Know-How، ومن بين أهم الوسائل الفاعلة في حماية المحتوى وبخاصة المحتوى المنشور رقميا أو وثائقيا هو تطبيق الملكية الفكرية.

الحماية المادية لمرافق المعلومات :

من أهم الأخطار التي يمكن أن تتعرض لها مرافق المعلومات هي :

" الحريق، انقطاع التيار الكهربائي، انقطاع الاتصالات، الإهمال، السرقة ".

الخطوات المستخدمة في حماية مرافق المعلومات :

- استخدام وسائل اكتشاف ومقاومة الحريق.
- الصيانة المستمرة لوحدات التكييف والتبريد.
- حماية الخدمات الأساسية من مصادر الطاقة بتوفير مولدات احتياطية.
- تأمين خطوط الاتصال وتوفير أجهزة مودم بديلة " احتياطية ".
- إغلاق غرفة الحاسوب ومنع دخول غير المخولين إليها.
- تأمين نوافذ الغرفة القريبة من الأرض وتأمين المداخل والمخارج ووضع أجهزة

إنذار ومراقبة عليها.

- توفير مواقع بديلة لمبنى المرفق.

الحماية الإلكترونية لمرافق المعلومات:

و هي الإجراءات المتبعة التي يتم اتخاذها ضد من يحاول التهديد لغرض الحصول على المعلومات أو إتلافها وهي تعتمد على نوع التهديدات المحتملة وقيمة المعلومات المخزنة وإمكانات مرفق المعلومات المادية وتشمل هذه الحماية الإجراءات التالية :

١- السيطرة على البواب.. بتزويد كل موظف له صلاحية الدخول إلى المرفق ببطاقة ممغنطة لفتح البابا المزود بقفل مغناطيسي يحتوي مجموعة أرقام سرية للموظفين حيث يجب على الموظف إدخال البطاقة مضافا إليها الرقم السري للمرور.

٢- المراقبة بالأجهزة المرئية.. ويتم ذلك من خلال نصب كاميرات مراقبة في أماكن مختارة يتم من خلالها مراقبة الحركة في هذه الأماكن.

٣- الحماية باستخدام أشعة ليزر أو أشعة فوق البنفسجية.. ويعمل هذا النظام بطريقة الانعكاس لحزم متوازية من الأشعة عبر قاعة الحاسوب أو المناطق المطلوب حمايتها وفي حال مرور أي شخص خلال الحزمة الضوئية تقوم بإطلاق صفارة إنذار.

أمن الأجهزة وملحقاتها :

- يجب أن يخضع دخول وخروج الأجهزة لموافقة مكتوبة من مسئول الأمن بمرفق المعلومات.
- تأمين الخدمات التي يسبب توقفها تلفا للأجهزة مثل الكهرباء.
- مرافقة من يقومون بعمليات الصيانة من خارج المرفق خلال عملهم بالمرفق.
- وضع إجراءات تتبع عند إخراج الأجهزة للصيانة خارج المبنى وعند إعادتها.

أمن البيانات :

١. توفير مستوى حماية مناسب لوسائط تخزين المعلومات.

٢. الاحتفاظ بنسخ احتياطية من المعلومات في أماكن خارج الموقع الموجودة به النسخ الأصلية.

٣. عدم السماح بالوصول لهذه الوسائط إلا للأشخاص المصرح لهم بذلك.

٤. إتلاف النفايات والمخلفات مثل البطاقات والمايكرو فيلم وقوائم البرامج وغيرها إتلاف جيد حتى لا يتم استخدامها من قبل الآخرين في الحصول على المعلومات.

٥. مراقبة أماكن الطباعة لتقليل فرص حصول غير المخولين على قوائم أو بيانات مطبوعة.

المشاكل والأخطار التي تتعرض لها الشبكات:

١. انقطاع الخدمة بالسرقة أو التدمير أو تعطيل البرمجيات.

٢. الاستخدام الغير مصرح به.

٣. أعطال خطوط الاتصال وأجهزة المودم.

٤. التشويش على الإشارات المنقولة.

٥. أعطال البرمجيات أو الأجهزة.

٦. اختراق خطوط الاتصال.

٧. إقحام الفيروسات الإلكترونية في الشبكة.

٨. فقد البيانات المرسلة أو حدوث تحريف فيها أثناء نقلها.

الأزمات والكوارث:

تعريف الأزمة:

هي شدة عارضة تؤدي إلى كارثة وقد لا تؤدي إلي كارثة إذا ما أحسن إدارتها،حيث أنها أقل وطأة ، ولاتصل إلى درجة الكارثة ، غير أنها خروج عن السياق اليومي المعتاد سواء في العمل أو في الحياة، إضافة للخسائر المادية والبشرية التي تنتج عنهما.

تعريف الكارثة:

هو الضرر الذي يصيب النفس والممتلكات والمال ، وتعتبر شدة سيئة الآثار على الوضع القائم بالمؤسسة ، وقد تكون بفعل فاعل أو طبيعة مثل الزلازل

والسيول والفيضانات ، وفي جميع الأحوال يجب العمل على التقليل من مضارها قدر الإمكان والتعلم منها ، واكتساب الخبر التي تؤهلنا لتجنبها في المستقبل.

مراحل الكارثة أو الأزمة:

المرحلة الأولى:

وهي المرحلة التي تسبق وقوع الكارثة ، ويتم فيها إجراء الاستعدادات اللازمة ووضع خطط المواجهة وخطط إدارة الأزمة وتوزيع المسؤوليات.

المرحلة الثانية:

وهي مرحلة وقوع الكارثة ، وفيها يتطلب القيام بالمهام والمسؤوليات الطارئة من تقليل حجم الخسائر ، وإنقاذ ما يمكن إنقاذه من أفراد ومقتنيات ومعدات وأجهزة.

المرحلة الثالثة:

وهي مرحلة ما بعد الكارثة ، وفيها تبدأ إدارة مرفق المعلومات القيام بإعادة البناء والإصلاح وإعادة الأمر على ما كان عليه وأفضل.

تصنيف الكوارث والأزمات:

التصنيف الأول :

وهو الذي يربط الكارثة بالفاعل، فإذا كانت الكارثة نتيجة لفعل الطبيعة، تصبح الكارثة طبيعية، وإذا كانت بفعل فاعل من أبناء البشر تصبح الكارثة غير طبيعية أي صناعية.. وتقسم الكوارث إلى طبيعية وصناعية كالتالي :-

- **أولا** : **الكوارث الطبيعية** :

هي تلك التي تتعلق بالتقلبات المناخية مثل : الزلال وتحرك البراكين والعواصف والسيول الشديدة على اختلاف أنواعها، وغيرها من العواصف والرياح المحملة بالأتربة والغبار، وليس لإرادة الإنسان دخل في حدوثها.

- **ثانيا**: **الكوارث الصناعية**:

هي تلك التي تنتج عن أخطاء بشرية،سواء كانت مباشرة في إحداث الكارثة أو غير مباشرة وسواء كانت بفعل متعمد أو نتيجة إهمال وعدم دراية.

التصنيف الثاني:

في هذا التصنيف تقسم الكوارث إلى بسيطة وأخرى مركبة وتعرف كالتالي:

- **أولا**: **الكوارث البسيطة**:

هي تلك التي تقتصر على ظاهرة واحدة،أي أحادية المشكلة،وليست بسيطة بمعنى السهولة واليسر،كالزلازل أو الحريق.

- **ثانيا**: **الكوارث المركبة**:

هي تلك الكوارث التي تكون مزدوجة ،بحيث يجتمع الزلزال والفيضان في الوقت والمكان نفسه ،وتكون مقاومتها في هذه الحالة مشكلة مركبة يصعب مقاومتها في آن واحد ،فازدواج الكارثة يقلل الإغاثة ،ويضاعف الخسائر.

التصنيف الثالث:

هو تصنيف فلسفي يرتبط بالفلسفة اليونانية القديمة ومفاده أن التوازن هو الذي يحكم العناصر الأربع في الكون ، وإذا طغى عنصر على الآخر ،كان عدم التوازن نتيجة حتمية وبذلك يتحول طغيان العنصر إلى دمار وكارثة على الحياة البشرية والنباتية والحيوانية،وهذا التصنيف يعتبر مكملا للتصنيف الأول الذي يفرق بين الكوارث الطبيعية والصناعية.

المبادئ الأساسية لنجاح نشاط مواجهة الكوارث :

إن المبادئ الأساسية التي تمنح نشاط مواجهة الكوارث فرصة طيبة للنجاح وتحقيق الهدف منه يمكن تلخيصها في خمس نقاط.

١- الحصول على الالتزام الإدارة العليا : فبدون التزام الإدارة العليا الواضح والمعلن للجميع عنه، تكون هناك فرصة لهذا النشاط، أي فرصة حقيقية للنجاح فالإدارة العليا هي التي توفر الدعم المالي ودعمها المعلن لهذا النشاط

الذي ستشجعه الإدارات الأخرى على الاهتمام بما تكلف به من أنشطة أو دراسات أو ما يطلب منها من بيانات أو من مشاركة من جانب أفرادها في اللجان المختلفة.

٢- توفير الميزانية اللازمة :نشاط مواجه الكوارث كأي نشاط آخر من أنشطة المؤسسة لابد وان يحتاج إلى نفقات ومن ثم لابد من توفير الميزانية اللازمة له مسبقا لذلك كان من الضروري تقدير المبالغ المطلوبة في وقت مبكر.

٣- إيجاد موقع تشغيل بديل :البديل الاحتياطي ونعني به موقع التشغيل البديل الذي ينبغي إعداده للاستخدام عند تعطل الموقع الأصلي عن العمل ولذلك لابد من الاهتمام بتجهيز هذا الموقع بدرجة الاستعداد المطلوبة، وكذلك معرفة المدة التي سوف يستغرقها إعداد الموقع بالكامل لاستقبال الموظفين والعملاء.

٤- إجراء اختبارات استعادة النشاط باستمرار:نحن نعيش في عالم متغير، فكافة الظروف من حولنا قابلة للتغيير،ولذلك من الضروري ليس فقط إجراء الاختبارات اللازمة للتأكد من سلامة خطة استعادة النشاط ومن أنها سوف تؤدي الغرض منها ، ولكن من المهم إعادة هذه الاختبارات على فترات دورية أو كلما ظهر متغير جديد نتوقع أن يكون له تأثير على الظروف العامة للمؤسسة أو للموقع البديل.

٥- إعداد خطة طوارئ ناجحة: خطة الطوارئ هي عصب نشاط مواجهة الكوارث ،و إعداد خطة ناجحة يكفل نجاح هذا النشاط.

خطة الطوارئ المعلوماتية عند حدوث الأزمة:

أهداف خطة الطوارئ:

خطة الطوارئ هي خطة مكتوبة ومعتمدة ومعدة للتنفيذ في حالة وقوع كارثة لمرفق المعلومات وهي تحدد كافة الإجراءات الواجب اتخاذها لتحسين درجة المقاومة للأخطار وتقليل الخسائر إلى أدنى حد والهدف منها هو التمكن من استعادة النشاط في أقل وقت ممكن وبأقل تكلفة وفق الآتي:

- تحديد الأخطار المتوقعة وكيفية اختيار البدائل.

- وضع التدابير المادية لحماية أجهزة الحاسوب والبرمجيات ووسائط البيانات.
- وضع الإجراءات المناسبة التي تمر بها عملية تدريب الأفراد.

عوامل نجاح الخطة:

١- ضمان دعم الإدارة العليا للخطة.

٢- توعية الموظفين بأهمية الخطة وتدريبهم على تنفيذها.

٣- مراقبة الخطة بشكل دوري واختبارها للتأكد من نجاحها.

٤- أن يكون الهدف منها هو العمل الرئيسي وليس استعادة نشاط الحاسوب فقط.

استعادة نشاط مرفق المعلومات:

١- استعادة النشاط بتشغيل الموقع البديل.

٢- اللجوء إلى النسخ الاحتياطي للبيانات إذا دعت الضرورة إلى ذلك.

٣- توفير الإمكانات المادية والفنية لتسهيل عملية تشغيل المواقع البديلة.

جرائم الحاسوب والإنترنت:

وتعرف جرائم الحاسوب والإنترنت بأنها: " ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتكنولوجيا الحاسوب ونظم المعلومات،لارتكابها أو التحقيق فيه ومقاضاة فاعليها"،كما يمكن تعريفها بأنها"الجريمة التي يتم ارتكابها إذا قام شخص ما باستخدام معرفته بالحاسوب بعمل غير قانوني".

خصائص وأنواع جرائم الحاسوب والإنترنت:

من الصعوبة الفصل بين جرائم الحاسوب وجرائم الإنترنت، وتصنف تلك الجرائم إلى مجموعات:

- المجموعة الأولى: تستهدف_مراكز معالجة البيانات المخزنة في الحاسوب لاستغلالها بطريقة غير مشروعة كمن يدخل إلى إحدى الشبكات ويحصل على أرقام بطاقات ائتمان يحصل بواسطتها على مبالغ من حساب مالك البطاقة،وما يميز هذا النوع من الجرائم أنه من الصعوبة بمكان اكتشافه.

- المجموعة الثانية: تستهدف مراكز معالجة البيانات المخزنة في الحاسوب بقصد التلاعب بها أو تدميرها كليا أو جزئيا ويمثل هذا النوع الفيروسات المرسلة عبر البريد الإلكتروني أو بوساطة برنامج مسجل في أحد الوسائط المتنوعة والخاصة بتسجيل برامج الحاسوب ويمكن اكتشاف مثل هذه الفيروسات في معظم الحالات بوساطة برامج حماية مخصصة للبحث عن هذه الفيروسات ولكن يشترط الأمر تحديث قاعدة بيانات برامج الحماية لضمان أقصى درجة من الحماية ، ومع أن وجود هذه البرامج في جهاز الحاسوب لا يعني إطلاقا الحماية التامة من أي هجوم فيروسي وأن هو إلا أحد سبل الوقاية، وقد يتسلل الفيروس إلى الجهاز بالرغم من وجودها ويلحق أذى بالجهاز ومكوناته خاصة إذا كان الفيروس حديثا وغير معروف من السابق.

- المجموعة الثالثة: تشمل استخدام الحاسوب لارتكاب جريمة ما، وقد وقعت جريمة من هذا النوع في إحدى الشركات الأمريكية التي تعمل سحبا على جوائز اليانصيب حيث قام أحد الموظفين بالشركة بتوجيه الحاسوب لتحديد رقم معين كان قد اختاره هو فذهبت الجائزة إلى شخص آخر بطريقة غير مشروعة.

- المجموعة الرابعة: تشمل إساءة استخدام الحاسوب أو استخدامه بشكل غير قانوني من قبل الأشخاص المرخص لهم باستخدامه ومن هذا استخدام الموظف لجهازه بعد انتهاء عمله في أمور لا تخص العمل.

حماية التخزين الآلي:

توجد أربع وسائل لتحقيق أمن البيانات وبرمجيات الحواسيب وهي:

- التحكم في الدخول إلى البيانات.
- التحكم في تدفق البيانات.
- التحكم في محاولة الاستنتاج.
- تشفير أو توكيد البيانات.

وتم الاتفاق لدى منظمة التعاون الاقتصادي والتنمية OCDE حول الجريمة المعلوماتية ، على ضرورة أن يغطى قانون العقوبات في كل دولة التهديدات التالية:

- التلاعب في البيانات المعالجة آليا بما في ذلك محوها.

- التجسد المعلوماتي ، ويندرج تحته الحصول أو الاقتناء أو الاستعمال غير المشروع للبيانات.
- تخريب المعلومات.
- الاستخدام غير المشروع أو سرقة وقت الحاسوب.
- قرصنة البرامج.
- الدخول غير المشروع على البيانات أو نقلها.
- اعتراض استخدام البيانات أو نقلها.
- وفضلا عن إمكانات تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات في مدة نقل عن الثانية واختراق لشبكات المعلومات الوطنية وتخريبها ، مما يترتب عنه إصابة الدولة وبعض قطاعاتها الحيوية بالشلل، فضلا عن تعريض مصالحها الحيوية للخطر.

ولمواجهة جرائم الحاسوب تستخدم حزمة من تكنولوجيات الحماية مثل التشفير Encryption الذي يقوم على شفرة رياضية يتعذر كسرها إلا لمن يملك المفتاح الخاص بها ، وبالإضافة إلى ذلك تستخدم تكنولوجيا الحماية والتجسس البيولوجي Biometric ضد محاولات النفاذ غير المشروع إلى شبكة الحاسوب ،وذلك باستخدام الخصائص البيولوجية التي تميز كل شخص عن آخر والتي لا يمكن أن تكون مطابقة مع الآخرين مثل بصمة الإبهام ، شكل الجمجمة ، اتساع حدقة العين ملامح الوجه ، تمييز الصوت.....الخ.

إستراتيجية أمن المعلومات:

إن إستراتيجية أمن المعلومات أو سياسة أمن المعلومات هي مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المؤسسة وتتصل بشؤون الدخول للمعلومات والعمل على نظمها وإدارتها.

و تهدف الإستراتيجية إلى الآتي :

تعريف المستخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات وكذلك حماية المعلومات بكافة أشكالها، وفي مراحل

إدخالها ومعالجتها ونقلها وإعادة استرجاعها.

تحديد الآليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة على من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر.

بيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بذلك.

من الذي يعد إستراتيجية أمن المعلومات :

بوجه عام تشمل مسئولي أمن الموقع ومديري الشبكات وموظفي وحدة الحاسوب ومديري الوحدات الأخرى وممثلي مجموعات المستخدمين ومستويات الإدارة العليا إلى جانب الإدارة القانونية.

و تتلخص المنطلقات والأسس التي تبنى عليها إستراتيجية أمن المعلومات القائمة على الاحتياجات المتباينة لكل منشأة من الإجابة على تساؤلات ثلاثة رئيسية هي:-

ماذا أريد أن أحمي ؟

من ماذا أحمي المعلومات ؟

كيف أحمي المعلومات ؟

و قد توصلت الشركات العاملة في تكنولوجيا الاتصالات والحواسيب إلى ما يعرف بـ**Clipper Ch** أو شريحة الجذاذة، وهي طريقة للترميز تعد بمثابة بابا سحريا أو سري تزود بها جميع وسائل الاتصال المرتبطة بطريق المعلومات، والمقصود بالترميز هنا هو عملية إخفاء البريد الالكتروني **E- Mail** أو الملفات الهامة بحيث لا يستطع الاطلاع على المعلومات الحساسة أو السرية إلا الأشخاص المخول لهم بذلك، وهناك أيضا نظم خاصة تسمى **Firewall** أو حاجز النار، وحاجز النار هو آلية دفاعية تقوم على تقنين تدفق البيانات من وإلى الشبكة من خلالها وفقا لسياسات ومعايير محددة سلفا، وتقوم آلية حاجز النار على مزيج من العتاد والبرمجيات التي تلعب دور حارس البوابة الذي يدقق في هوية البيانات الداخلة والخارجة الى ومن الشبكة، ويمنع مرور كل ما هو غير شرعي منها.

و لعل أكثر محاولات الشركات العاملة في مجال تكنولوجيا الاتصالات

والحاسوب تنظيما، هي محاولة مؤسسة **IBM**، فقد قامت بالاشتراك مع خمسة شركات أخرى بتأسيس ما يعرف بشركة **Terisa Systems**، وهي شركة جديدة مهمتها القيام بأعمال الحماية لبعض البرامج على الإنترنت، وعلى سبيل المثال في حالة طلب شراء حزمة برامج جديدة من شركة **Microsoft** العالمية وذلك من خلال الشبكة، فان وسيلة الدفع ستكون هي بطاقة الائتمان الخاصة بالمشترى، ورقمها قد يكون مشاعا ومعلوما لدى الكثيرين، ومن هنا تأتي أهمية الحماية على شبكة الإنترنت.

أمن المعلومات.. مسؤولية من ؟

في دراسة نظرية مهمة تناولت كل من (مارجريت هيجنس) Higgins و(ليزا تاسكاريس) Taskaris مشكلة أمن المعلومات، فأكدتا بأنه لابد من تحديد المسؤولية في الإنسان وليس التكنولوجيا.عرفت مشكلة الأمن بأن لها صلة بحماية شبكات الحواسيب والمعلومات ضد الدخول غير المسموح به أو تدمير البيانات أو مشاهدة بيانات أو معلومات خاصة وعرفتا هذا الدخول من الإنسان المقصود بالمشكلة فهو الذي يتعدى على هذه الشبكة أو ذلك النظام.

لقد أوضحت هذه الدراسة نقلا عن (برانسكومب) Branscomb إن الهجوم على نظم المعلومات يحدث لأسباب عدة جمعيها في ثلاثة أسباب هي :

١- يحصل النظام الأضعف حماية على الاهتمام الأكبر من المتطفلين.

٢- تكون النظم الأكثر إتاحة أمام المتطفلين ليحصلوا منها على أكبر قدر مما يريدون هي النظم الأكثر جاذبية لهم والأوفر حظا في الهجوم وكثرة الدخول غير المشروع لها.

٣- عادة ما ينظر المهاجمون أو المتطفلون إلى النظم التي يستطيعون من خلالها تحقيق أكبر قدر من التخريب والسرقة والعبث.

هذه ببساطة أسباب ألقت اللوم على الإنسان لسوء إدارته لإتاحته نظمه وعدم حمايتها ومتابعتها وسن السياسات والإجراءات اللازمة وتطويع التقنيات المتاحة وتحديثها والاستفادة منها.

إن عدم اختبار أو معرفة النظم التي تعمل في البيئة المستهدفة مثل بيئة مرفق

المعلومات، وعدم معرفة نقاط قوتها وضعفها أو متابعة التطورات التي تطرأ عليها، إضافة إلى استخدام برامج ونظم غير موثقة أو موردين على درجة ضعيفة من الثقة، وغياب الوعي والتثقيف التكنولوجي والإداري والإجرائي، وأخيرا غياب المعايير والسياسات وتطبيق الإجراءات هو الذي يسبب المشاكل الأمنية في مرافق المعلومات ويرفع من نسب حدوثها في مرافق المعلومات أو أي بيئة أخرى.

أمن المعلومات والحقوق الفكرية :

جانب آخر له علاقة بموضوع المعلومات ونظمها الإلكترونية ولا يتم الالتفاف له من الجانب المتعلق بأمن المعلومات هو ذلك الجانب ذو العلاقة بالحقوق الفكرية للأعمال المنشورة إلكترونيا ودور مرفق المعلومات في فهم مسؤولياته وواجباته القانونية والأدبية. فمرفق المعلومات في هذا العصر الحديث يملك من مواد المعلومات الإلكترونية المحملة على وسائط مختلفة أو متاحة عبر شبكة الإنترنت مثل الأدوات الببليوغرافية والوسائط المرجعية والنصوص الكاملة لمقالات ودراسات وتقارير مما يجعله عرضة للمساءلات القانونية في جانب أو العبث من قبل بعض المرتادين في جانب آخر. وقد أوصت (ليزلي هاريس) Harris مديري مرافق المعلومات بتطوير سياسات تخص قضايا حقوق الملكية الفكرية واقترحت عليها الخطوات الخمس عشر الآتية :

١. قم بتعيين مسئول للحقوق الفكرية.
٢. تواصل مع محام عارف بقضايا حقوق الملكية الفكرية.
٣. لابد من معرفة ودراسة المفاهيم الأساسية لحقوق الملكية الفكرية.
٤. تعرف على الكيفية التي يتم بها تطبيق معايير الحقوق الفكرية على المواد الإلكترونية على الأقراص المكتنزة وشبكة الإنترنت.
٥. تعرف على إجراءات الحصول على التراخيص ذات العلاقة ومهام الجمعيات العاملة في المجال.
٦. كون مرفق معلومات صغير بمواد لها علاقة بقضايا حقوق الملكية الفكرية.
٧. استخدام المعلومات المتوفرة عبر الشبكة عن موضوع الحقوق الفكرية.

٨. تعرف على القوانين والإجراءات الدولية ذات العلاقة.

٩. تابع التحديثات الجارية على قوانين الحماية الفكرية بانتظام.

١٠. قم بحضور الدورات والحلقات حول موضوع حقوق الملكية الفكرية.

١١. ساهم في تعليم وتدريب الآخرين في مكان العمل وبشكل دائم حول الموضوع.

١٢. تعلم طرق التفاوض بشأن اتفاقيات منح التراخيص.

١٣. قم بوضع واعتماد سياسة خاصة بالإنترنت والبريد الإلكتروني.

١٤. قم بحفظ الملفات الخاصة بالاتفاقيات والمفاوضات بشكل سهل وأمين بالرجوع لها وقت الحاجة.

١٥. فكر بسياسة تحمي خصوصية الأفراد، وهذه النقطة الأخيرة لها علاقة بالمستفيدين من مرفق المعلومات واستخدامهم لمواقع مرفق المعلومات على الإنترنت وتراسلهم معه واستخدام المعامل أكثر من قضايا الحقوق الفكرية.

قائمة المصـــــادر

١. أبن منظور. لسان العرب.- القاهرة : منشورات مطبعة بولاق، ج ٨، ص ٢٩٠.

٢. أبوبكر محمود الهوش. التقنية الحديثة في المعلومات والمكتبات.- ط٢.- القاهرة : دار الفجر، ٢٠٠٣.

٣. _____. دراسات في نظم وشبكات المعلومات.- القاهرة : مكتب عصمي للنشر والتوزيع، ١٩٩٦.

٤. _____. " العرب أم تحديات مجتمع المعلومات ".- مجلة المكتبات والمعلومات العربية، س ١٩، ع٢، ١٩٩٩.

٥. _____. المعلومات والتنمية.- طرابلس، والجفرة : أكاديمية الدراسات العليا، ومركز الدراسات والبحوث / أمانة مؤتمر الشعب العام، ٢٠٠٣.

٦. احمد أنور بدر." الأخلاقيات المهنية في المكتبات وأجهزة المعلومات المعاصرة ".- الاتجاهات الحديثة في المكتبات وعلم المعلومات مج ٥، ع١، ١٩٩٨.

٧. أحمد بدر، وأخرون. السياسة المعلوماتية وإستراتيجية التنمية.- يستكمل، ٢٠٠١ م

٨. أحمد أنور بدر. علم المعلومات والمكتبات.- القاهرة : دار غريب، ١٩٩٦.

٩. أحمد زكي بدوي. معجم المصطلحات الاقتصادية.- القاهرة بيروت : دار الكتاب المصري ودار الكتاب اللبناني، (د.ت).

١٠. أحمد ماهر. إدارة الموارد البشرية.- الإسكندرية : جامعة الإسكندرية، ١٩٩٦.

١١. ألان كالدر، ستيف واتكينز. الإدارة الدولية الرشيدة في تكنولوجيا المعلومات ID.- ترجمة بهاء شاهين.- القاهرة – مجموعة النيل العربية، ٢٠٠٨.

١٢. أمنية صادق.إدارة الأزمات والكوارث في المكتبات.- القاهرة :الدار المصرية اللبنانية، ٢٠٠٢

١٣. أمين عبد العزيز حسن، استراتيجيات التسويق في القرن الحادي والعشرين.- القاهرة : دار قباء للنشر والتوزيع والإعلان، ٢٠٠١.انتوني ديبونز وأخرون.علم المعلومات والتكامل المعرفي.- تعريب وإضافة احمد أنور بدر، محمد فتحي عبد الهادي.- القاهرة : دار قباء للطباعة والنشر والتوزيع،١٩٩٨.

١٤. أمينة محمود حسين. نظم المعلومات التسويقية.- القاهرة : مركز التعليم المفتوح / جامعة القاهرة، ١٩٩٥.

١٥. انتوني ديبونز وأخرون. علم المعلومات والتكامل المعرفي- تعريب وإضافة احمد أنور بدر، محمد فتحي عبدالهادي- القاهرة : دار قباء للطباعة والنشر والتوزيع، ١٩٩٨.

١٦. باري كشواري. إدارة الموارد البشرية.- القاهرة : دار، ٢٠٠٣.

١٧. بشير عباس العلاق، حميد عبد النبي الطائي. تسويق الخدمات.- عمان : دار زهران للنشر والتوزيع، ٢٠٠١.

١٨. بولين اثرتون. مراكز المعلومات : ترجمة حشمت قاسم.- ط٢.- القاهرة : دار غريب، ١٩٩٦.

١٩. ثابت عبد الرحمن ادريس، جمال الدين محمد المرسي. التسويق المعاصر.- الإسكندرية : الدار الجامعية، ٢٠٠٥.

٢٠. جبريل العريشي."أمن المعلومات".- احوال المعرفة، س٨،ع ٣٠، ٢٠٠٣.

٢١. جون فيزرو بول ستيرجز. دائرة المعارف الدولية لعلم المعلومات والمكتبات.- الترجمة العربية تحرير وأشراف محمد فتحي عبد الهادي.- القاهرة : المجلس الأعلى للثقافة، ٢٠٠٣.

٢٢. حامد الشافعي دياب. إدارة المكتبات الجامعية - القاهرة : دار غريب، ١٩٩٤.

٢٣. حسن الطاهر داوود. الحاسب وأمن المعلومات.- الرياض : مطابع جامعة الملك سعود، ١٩٩٧.

٢٤. حسن عماد مكاوي. تكنولوجيا الاتصال الحديثة في عنصر المعلومات.- القاهرة : الدار المصرية اللبنانية، ١٣٩٣.

٢٥. حسن عواد السريحي." أمن المكتبات ونظم المعلومات / دراسة حالة على مكتبة جامعة الملك عبد العزيز بجدة ".- ورقة مقدمة إلى المؤتمر الثاني عشر للإتحاد العربي للمكتبات والمعلومات ،الشارقة: جامعة الشارقة، ٢٠٠١.

٢٦. حشمت قاسم. خدمات المعلومات.- القاهرة : مكتبة غريب، ١٩٨٤.

٢٧. حليمة بوشاقور. "آليات لتطوير الإمكانات الفكرية والبشرية العربية لغزو الفضاء الالكتروني.- في المؤتمر الحادي عشر للاتحاد العربي للمكتبات والمعلومات، نحو إستراتيجية لدخول النتاج الفكري بالمكتوب باللغة العربية في الفضاء الإلكتروني، القاهرة : ٢- ٢٠٠١/٨/١٦.

٢٨. خالد عبد الرحيم الهيتي إدارة الموارد البشرية.— عمان : دار الحامد، ١٩٩٩

٢٩. خالد مقابلة، علاء السرابي. التسويق السياحي الحديث.- عمان : دار وائل للنشر، ٢٠٠٠.

٣٠. دولت إبراهيم." إدارة المعلومات ". - عالم الكتب، مج ١٢ ، ع ٤.

٣١. رايمون ماكليود. نظم المعلومات الادارية.- تعريب سرور علي إبراهيم سرور.- الرياض : دار المريخ، ٢٠٠٠.

٣٢. ربحي مصطفي عليان. إدارة وتنظيم المكتبات ومراكز مصادر التعلم.- عمان : دار الصفاء، ٢٠٠٢.

٣٣. ربحي مصطفى عليان، ايمان فاضل السامرائي. تسويق المعلومات.- عمان : دار صفاء للنشر والتوزيع، ٢٠٠٤.

٣٤. راوية حسن. إدارة الموارد البشرية رؤية مستقبلية.- الإسكندرية : الدار الجامعية، ٢٠٠٣.

٣٥. راوية حسن. مدخل استراتيجي لتخطيط وتنمية الموارد البشرية.- الإسكندرية : الدار الجامعية، ٢٠٠٣.

٣٦. رمضان الصباغ. الأحكام التقويمية في الأخلاق.- الإسكندرية : دار الوفاء، ١٩٩٨.

٣٧. زكي حسين الوردي، ومجبل لازم المالكي. المعلومات والمجتمع.- عمان : الوراق للنشر والتوزيع، ٢٠٠٢.

٣٨. زين عبد الهادي، اجلال بهجت." تسويق الخدمات المكتبية وخدمات المعلومات في المكتبات ومراكز المعلومات ". الاتجاهات في المكتبات والمعلومات، ع٤ ، ١٩٩٩.

٣٩. سعد غالب ياسين. أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات.- عمان: دار المناهج، ٢٠٠٨.

٤٠. سعد غالب ياسين. نظم المعلومات الإدارية.- عمان : دار اليازوري العلمية، ٢٠٠٢.

٤١. سعد محمد جبر." العربية وتكنولوجيا إدارة المعلومات ".- في أبحاث ودراسات المؤتمر العلمي الرابع لنظم المعلومات وتكنولوجيا الحاسبات حول تطوير مصادر الالكترونية.- القاهرة : المكتبة الأكاديمية ١٩٩٦.

٤٢. سهيلة عباس وعلى حسين على. إدارة الموارد البشرية.- عمان : دار وائل، . ١٩٩٩.

٤٣. سونيا محمد البكري ، إبراهيم سلطان. نظم المعلومات الإدارية.- الإسكندرية: الدار الجامعية ، ٢٠٠١.

٤٤. سيد حسب الله. مباني المكتبات من وجهة نظر المكتبيين.- الرياض : معهد الإدارة العامة، ١٩٧٦.

٤٥. سيد حسب الله، احمد محمد الشامي. الموسوعة العربية لمصطلحات علوم المكتبات والمعلومات والحاسبات.- القاهرة : المكتبة الأكاديمية، ٢٠٠١.

٤٦. سيد محمد جاد الرب. الاتجاهات الحديثة في إدارة المنظمات الصحية.- (د.م)، المؤلف، ٢٠٠٨.

٤٧. سيد محمد جاد الرب. إدارة منظمات الأعمال : منهج متكامل في إطار مدخل النظم.- القاهرة : دار النهضة العربية، ١٩٩٥.

٤٨. شريف درويش اللبان.- تكنولوجيا المعلومات والعلاقات الاجتماعية دراسة في أخلاقيات العصر الإلكتروني.- الاتجاهات الحديثة في المكتبات والمعلومات، ع ١٣ ، ٢٠٠٠.

٤٩. شريف كامل شاهين. نظم المعلومات الإدارية للمكتبات ومراكز المعلومات. – الرياض : دار المريخ، ١٩٩٤..

٥٠. شعبان عبدالعزيز خليفة إدارة المكتبات ومؤسسات المعلومات دائرة المعارف في علوم الكتب والمكتبات والمعلومات مج٤.- القاهرة : الدار المصرية اللبنانية، ٢٠٠٠.

٥١. شوك تشاندا وشلب كابرا. إستراتيجية الموارد البشرية.- ترجمة عبد الحكيم الخزامي.- القاهرة : دار الفجر ، ٢٠٠٢.

٥٢. صلاح الدين عبد المنعم مبارك. اقتصاديات نظم المعلومات المحاسبية والإدارية.- الإسكندرية :دار الجامعة العربية الجديدة، ٢٠٠١.

٥٣. عادل فهمي بدر. بنوك المعلومات وأثرها على التنمية الشاملة – عمان :دار الشرق الأوسط، ١٩٨٦.

٥٤. عارف طرابيشي. االملكية الفردية للبرمجيات في سوريا : بين اخلاقيات المهنة وانتماء المعلوماتيين للدولة.- www.aralipp.org/lectures-I.htm

٥٥. عايدة سيد خطاب. الإدارة الاستراتيجية للموارد البشرية. – ط٢ –القاهرة : المؤلف ، ١٩٩٩.

٥٦. عبد الرحمن الصباح. نظم المعلومات الإدارية.- عمان دار زهران، ١٩٩٨.

٥٧. عبد الرزاق مصطفى يونس. أمن المعلومات الإلكترونية وحقوق الملكية الفكرية ".- في أعمال الندوة العربية الأولى للمعلومات. قسطنطينة: جامعة منتوري، ٢٠٠٠.

٥٨. عبد العزيز بدر. إدارة الأفراد.- بغداد : مؤسسة المعاهد الفنية، ١٩٨٧.

٥٩. عبد العزيز فهمي هيكل. مراكز المعلوملتية.- بيروت : دار الراتب الجامعية، ١٩٨٨.

٦٠. عبد القادر عبد الله الفنتوخ. الانترنت للمستخدم العربي.- الرياض: مكتبة العبيكان، ١٩٩٩.

٦١. علاء الدين السيد فريد حسن. حماية المباني من أخطار الحريق.- أطروحة ماجستير.- كلية الهندسة، جامعة الأزهر، ١٩٩٥.

٦٢. علاء عبد الرزاق السالمي. نظم إدارة المعلومات.- القاهرة : المنظمة العربية للتنمية الإدارية، ٢٠٠٣.

٦٣. علي محمد منصور. " تخطيط القوى العاملة ".- المجلة القومية للإدارة، ع٣، ١٩٨٦.

٦٤. عماد عبد الوهاب الصباغ. علم المعلومات – عمان : الدار العلمية الدولية ودار الثقافة، ١٩٨٨.

٦٥. عمر أحمد همشري. الإدارة الحديثة للمكتبات ومراكز المعلومات.- عمان : دار الصفاء، ٢٠٠١.

٦٦. عمر وصفي عقيلي، وآخرون. مبادئ التسويق / مدخل متكامل.- عمان : دار زهران للنشر، ١٩٩٦.

٦٧. غادة عبد المنعم موسي. دراسات في نظم وخدمات المعلومات.- الاسكندرية : دار

الثقافة العلمية، ٢٠٠٢.

٦٨. فاتن سعيد با مفلح. حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى.- ورقة مقدمة الى المؤتمر الثاني عشر للاتحاد العربي للمكتبات والمعلومات الشارقة : جامعة الشارقة، ٢٠٠١.

٦٩. فايز جمعة النجار. نظم المعلومات الإدارية –ط٢.- عمان : دار الحامد للنشر والتوزيع ٢٠٠٦.

٧٠. فايزة سيف الدين (مترجم)." أخطار الديجيتال وسبل الحماية منها ".- الرائد العربي، س٢٠، ع٧٩، ٢٠٠٣.

٧١. فريد النجار. إدارة ووظائف الأفراد وتنمية الموارد البشرية.- الإسكندرية : مؤسسة شباب الجامعة، ١٩٩٨.

٧٢. فريد كيت. الخصوصية في عصر المعلومات.- ترجمة محمد محمود شهاب.- القاهرة : مركز الاهتمام للترجمة والنشر، ١٩٩٠.

٧٣. ف. ويلفرد لانكستر. خدمات المكتبات والمعلومات قياسها وتقييمها.- ترجمة حشمت قاسم.- الرياض : مكتبة الملك عبد العزيز العامة، ٢٠٠٠.

٧٤. كامل بربر.- إدارة الموارد البشرية وكفاءة الأداء التنظيمي.– بيروت : المؤسسة الجامعية ١٩٩٧

٧٥. كامل السيد غراب، نادية محمد الحجازي ز نظم المعلومات الإدارية.- الرياض : مطابع جامعة الملك سعود، ١٩٩٧.

٧٦. كريستين دي شامب." الكلمة الرئيسية في افتتاح المؤتمر السنوي الثالث عشر للاتحاد العربي للمكتبات والمعلومات "..- بيروت : ٢٠٠٢.

٧٧. كمال دسوقي. ذخيرة تعريفات مصطلحات أعلام علم النفس.- القاهرة: الدار الدولية للنشر، ١٩٨٨.

٧٨. كولن هاريسون، وروز. بينهام. اسس تنظيم المكتبات والمعلومات.- ترجمة سماء زكي المحاسني، وآخرون.- ط٢.– الرياض : مكتبة الملك عبد العزيز العامة، ١٩٩٥.

٧٩. ما زن فارس رشي. إدارة الموارد البشرية – الرياض : مكتبة العبيكان، ٢٠٠١.

٨٠. مبروكة عمر محيريق. التأهيل والتدريب المهني للعلماملين بمرافق المعلومات في العصر الالكتروني.- القاهرة : مجموعة النيل العربية، ٢٠٠٥.

٨١. محمد ابراهيم حسن محمد (ترجمة)." حرية الوصول للمعلومات : قضايا أخلاقية للمكتبين في عصر الإنترنت ". – الاتجاهات الحديثة في المكتبات والمعلومات، مج ١٢ ، ع ٢٤، ٢٠٠٥.

٨٢. محمد بن أحمد. شظايا.- طرابلس : الهيئة القومية للبحث العلمي، ٢٠٠٣.

٨٣. محمد الصيرفي. إدارة الموارد البشرية.- عمان : دار المناهج، ٢٠٠٣.

٨٤. محمد فتحي عبد الهادي. "أخلاقيات المعلومات في المكتبات ومراكز المعلومات " الاتجاهات الحديثة في المكتبات والمعلومات، مج ٧،ع ١٤، ٢٠٠٠.

٨٥. محمد فتحي عبد الهادي. المعلومات وتكنولوجيا المعلومات.- القاهرة : الدار العربية، ٢٠٠٠.

٨٦. محمد فهمي طلبة وآخرون، "فيروسات الحاسب وأمن المعلومات ".- القاهرة : موسوعة دلتا كمبيوتر، ١٩٩٢.

٨٧. محمد مجاهد الهلالي، "قواعد التعامل الأخلاقي".- الاتجاهات الحديثة في المكتبات والمعلومات، القاهرة، ع١١ ، س ٢٠٠٠.

٨٨. محمد محمد إبراهيم، ثابت عبد الرحمن إدريس، المدخل الحديث في إدارة التسويق.- القاهرة : مكتبة عين شمس ١٩٩٠.

٨٩. محمد محمد الهادي. الإدارة العلمية للمكتبات ومراكز التوثيق والمعلومات.- ط٢.- القاهرة المكتبة الأكاديمية، ١٩٩٠.

٩٠. محمد محمود مندورة، محمد جمال الدين درويش. التخطيط الاستراتيجي لنظم المعلومات – موقع مكتب مندورة.**http://mcgsite.com/subs/magalat/page5.htm0**

٩١. محمود عساف. أصول الإعلان.- القاهرة : دار النشر العربي، ١٩٧٧.

٩٢. محي الدين حسين." المعايير الاخلاقية والتنشئة العلمية ".- في مؤتمر اخلاقيات البحث العلمي.- القاهرة : المركز القومي للبحوث الاجتماعية، ١٩٩٥.

٩٣. مؤيد سعيد السالم." التكامل بين التخطيط الاستراتيجي والممارسات الخاصة بإدارة الموارد البشرية في منظمات اعمال العربية ".- في وقائع مؤتمرات إدارة الموارد البشرية وتحديات القرن الجديدة، اربد : جامعة اليرموك، ٢٠٠٠.

٩٤. مصطفي نجيب شاويش. إدارة الموارد البشرية.- عمان : دار الشروق ١٩٩١.

٩٥. مهدي حسين زويلف. إدارة الموارد البشرية – عمان : دار الفكر، ٢٠٠١.

٩٦. ناريمان إسماعيل متولي. اقتصاديات المعلومات.- القاهرة : المكتبة الأكاديمية، ١٩٩٥.
٩٧. نجاح القبلان. " أخلاقيات المكتبات والمعلومات ومكانتها من وجهة نظر العاملين في مكتبة الملك فهد الوطنية".- دراسات في المكتبات وعلم المعلومات. مج ٧، ع ١، ٢٠٠٢.
٩٨. نجلي مرتجي. إدارة وتنمية الموارد البشرية.- القاهرة : جامعة حلوان، ١٩٩٧.
٩٩. هاني محي الدين عطية.- "نحو دستور أخلاقي لأخصائي المكتبات والمعلومات في الوطن العربي".- عالم المعلومات والمكتبات والنشر، مج ١، ع ٢، ٢٠٠٠.
١٠٠. هدي بنت صالح ابوحميد. الجودة الشاملة في إدارة المعلومات.- الرياض : معهد الإدارة العامة، ٢٠٠٦.
١٠١. يونس عرب. خصوصية حماية البيانات في العصر الرقمي.- عمان : اتحاد المصارف العربية، ٢٠٠٣.
١٠٢. _____. دليل أمن المعلومات والخصوصية.- عمان : اتحاد المصارف العربية، ٢٠٠٢.
١٠٣. _____. قانون الكمبيوتر.- عمان : اتحاد المصارف العربية، ٢٠٠١.

104. A.F. Westin. Privacy and Freedom.- New - York: Atheneum.1967.
105. American Library association."Access to electronic information, Services , and networks: an interpretation of the library bill of rights.- 'Chicago: office of intellectual freedom , 1996.
106. A. Miller. The - Assault on Privacy.- Ann Arbor : University of Michigan Press,1971.
107. A.Shrader.In Search of a Name , Information Science and its Conceptual Anteceolents.- LISR , vol.6, 1984.P.227-271.
108. Constitution of Chile ,1980.http:// www.georgetown.edu/LatAmerPolitical/Constitutions/Chile/Chile97.html .
109. Constitution of the Republic of Hungary: http:// centraleurope.com /ceo/country/constit/hucons 0.1 html.
110. Constitution of people's Republic of China-1993 http://www.qis.net/chinalaw/prccon5.htm.
111. Fred R David. Strategic management.-(5th.ed).- Englewood Cliffs, New Jersy : Prentice Hall,.1995.Inc. p.8.

112. John Ivancevich. Human Resource Management.- Irwin : McGraw _ Hill , 2001.
113. J.B Rule.Private Lives and Public Surveillance.- London : Allen Lane ,1973.
114. Jesse. H. Shera. Introduction to Library science.- Litleton Colorado Libraries Unlimited,Inc.1976.
115. J. Michael. Privacy and Human Rights: An International and Comparative Study with Special Reference to Developments in Information Technology.- Dartmouth: 1994.
116. K. Hunten.Issues and Experiments in Electronic Pullihing and Dissemination Information.- Technolgy and Lilaries VOL.13.NO.1994.
117. Lan Bardwell , and Lan Holden. Human Resource Management.- N.Y : Prentice _Hill , 2001.
118. Lee Finks. what do we sland for ?Values with out shame ".- American Libraris, VOL.20,NO.4. 1989.
119. Lesly Ellen Harris,. "Finding your way out of the copyright Maze.".- "computers in labraies , vol 18 , No. 6 ,7.
120. Margaret Higgins and Lisa Laskaris ,'The Human Face Of Electronic Information Security,' In:asis midyear 1997 proccedings.- WWW.asis.org/midyear-97/proceedings/Higgins/html.
121. Marilyn Mason. The Federal Role in Library and Information Services.- White Plains :Knowledge Industry Publications, 1983.
122. Micheal Bayles. Professional ethics.- 2nd ed.- Belmont ,CA: Wadsworth put.co,1989.
123. Micheal Kristiansson. A Framework for Information Policy Analysis Based on Changes in the Global Economic Forces International Forum on Information and Documentation 1996.
124. Peter Hernon. "Discussion Forum: National Information Policy.- Government In-Formation Quarterly vol.6,N03, 1989.
125. Philip Kotler. Marketing for Nonprofit Organingatiios.- Englewood N.J:Prentice Hall,1975.
126. professional ".- Lilbrary Trends , VOL.49,NO. 13,2001.
127. Report of National Internet Advisory Board 1997/1998,September1998.http://www.sba.gov.sg/work/sba/internet.nsf/
128. Richand. O. Mason.For Ethical Issue of Information Age ".Mis

Quastenly,10 Maech 1986.
129. S-HAWKINS & D.C Chou A wareness and challenge of Internet security.- information management and computer security. vol 8(2/3)2000.
130. The Constitution of the Republic of South Africa Act 108 of 1996.http://www.parliament.gov.zal/legislation/1996/saconst.html
131. Thomas Froechlich." Ethical consideration regarding library nonprofessic Competing perspective and value "-. Library trends. V.46,NO.3,1998.
132. Thompson Godfrey ,Library Security.in Library Interior Layton and Design.- Munchen : K.G.Saur.1982.
133. UNESCO - Handbook on the Formation, Approval- Implementations and Operation of a National Policy on Information. Paris: UNESCO, 1990.
134. Z. Yuexiao, Definitions and Science of Information.- Information processing and Management ,Vol, g4 No. 1988.