تطور استخدام تكنولوجيا المعلومات والاتصال والأمن المعلوماتي في المؤسسة دراسة ميدانية بمؤسسة مطاحن سيبوس _عنابة

الأستاذة: سامية بوقرة

جامعة عنابة، الجزائر

الملخص:

إن التطورات الحديثة في تقنيات المعلومات أحدثت تغييرات مستمرة ومضطردة في كافة الميادين إذ أصبحت عملية انتقال المعلومات عبر الشبكات و الحواسيب إحدى علامات العصر الرقمي المميزة التي لا يمكن الاستغناء عنها، وذلك لميزتها في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الأعمال وتطوير أساليب إنتاج وتخزين وتوزيع المعلومات، وهذا بدوره أدى إلى تزايد المشاكل والمخاطر المعلوماتية التي تهدد أمن معلومات المؤسسة وتؤثر عليها، مما يستوجب على هذه الأخيرة ضرورة التيقظ لتوفير الأمن اللازم لمعلوماتها خصوصا وأنها تعيش في ظل اقتصاد المعلومات الذي شعاره من يملك المعلومة يملك السيطرة، وطبعا هذا يعني امتلاك المعلومة وحمايتها لتبقى الاستفادة منها مستمرة، ولقد جاءت هذه الدراسة لتركز على ضرورة اهتمام المؤسسة بموضوع الأمن المعلوماتي الذي أصبح مهددا بسبب التطورات الحاصلة في مجال تكنولوجيا الاتصال والمعلومات.

Abstract :

The recent developments in information technology brought about changes continuously and steadily in all fields as it has become a process of transmission of information across networks and computers, one of the signs of the digital age characteristic that can not be dispensed with so as to advantage in facilitating the requirements of modern life by reducing the size of the business and the development of methods of production, storage and distribution of information, this in turn led to increased problems and risks of information that threatens the security of information organization and affect them, which requires the need for vigilance to provide the necessary security for their information, particularly as they live in the information economy whose motto who owns the information owns control, and of course this means the possession of information and protection of the remaining benefit from continuous, I came to this study focuses attention on the need for the institution the subject of information security, which is being threatened because of developments in the field of information and communication technology.

مقدمة :

إن الإعلام الجديد هو إعلام عصر المعلومات، فقد كان وليداً لتزاوج ظاهرتين بارزتين عرف بهما هذا العصر ظاهرة تفجر المعلومات، وظاهرة الاتصالات عن بعد، إذ يعتمد هذا الإعلام على استخدام الحواسيب والاتصالات بشكل كبير، وليست المؤسسات الإعلامية وحدها فقط من تأثرت بهذه التغييرات الحديثة في مجال المعلوماتية والاتصال حتى المؤسسات الاقتصادية أصبحت اليوم تعتمد في انجاز العديد من أعمالها على تكنولوجيا المعلومات والاتصالات خاصة في إنتاج المعلومات ومعالجتها وتخزينها وتوزيعها، مما اختصر الجهد والوقت.

ولكن وبالرغم من هذه السمات الايجابية التي نتجت عن استخدام هذه التكنولوجيات إلا أن مخاطر ومشاكل الأمن المعلوماتي عرفت تطورا موازيا لتطور استخدامها في المؤسسة، وتزايد الإدراك أن البيانات التي يعتمد عليها استمرار عمليات المؤسسة والتيقن أن المعلومات المستخلصة من هذه البيانات هي من ترسم صورة المؤسسة وبيئتها ومستقبلها، حيث تزايدت المخاوف من عدم وجود حماية كافية على عمل الحواسيب وتكنولوجيا الاتصال وهكذا فان انتشار استخدام هذه الأخيرة أدى إلى ضرورة مواكبة سياسات أمن المعلومات للمؤسسات.

سنحاول هذه الدراسة التعرض إلى تطور استخدام تكنولوجيا المعلومات والاتصال وكذا علاقتها بتطور مشاكل ومخاطر أمن المعلومات في المؤسسة، خصوصا أن هذه الأخيرة (المؤسسة) تعيش في ظل اقتصاد المعلومات الذي يرتكز على مفاهيم رئيسية كالمعلومات، التكنولوجيا، الاتصالات وهذا ما يستوجب عليها ضرورة الوعي بأهمية امن المعلومات لتتمكن من حماية معلوماتها التي ستمكنها من اتخاذ القرارات الصحيحة التي تضمن لها النجاح والاستمرار. وسيتم معالجة هذه الإشكالية من خلال الإجابة على السؤال الرئيسي التالي:

إلى أي مدى يمكن أن يساهم تطور استخدام تكنولوجيا المعلومات والاتصال في زيادة مخاطر أمن المعلومات في مؤسسة مطاحن سيبوس-عنابة-؟

وقد تم تقسيم هذا التساؤل إلى الأسئلة الفرعية التالية التاليين:

1. ما مدى تطور استخدام تكنولوجيا المعلومات والاتصال في مؤسسة الدراسة؟
2. ماهي المخاطر المعلوماتية التي خلقتها تكنولوجيا المعلومات والاتصال في مؤسسة الدراسة؟
3. هل توجد برامج تدريبية تكوينية لمواجهة المخاطر التي تهدد أمن المعلومات في مؤسسة الدراسة؟

أهمية الدراسة:

تكمن أهمية الدراسة في أهمية الموضوع في حد ذاته، فهو من أهم المواضيع التي تفرض نفسها خاصة ونحن نعيش في ظل الثورة التكنولوجية، التي تفرض على المؤسسات استخدام تكنولوجيا المعلومات والاتصال الحديثة في انجاز الأعمال، لان عدم استخدام هذه التكنولوجيات ولو نسبيا سيجعلها غريبة في عالم باتت تحكمه التطورات الكبيرة لتكنولوجيا المعلومات والاتصال، هذا بالموازاة مع انتهاجها لآليات وإستراتيجية مضبوطة لمواجهة المخاطر المعلوماتية التي تخلقها هذه التكنولوجيات لتضمن بقاءها .

أهداف الدراسة:

يهدف هذا البحث إلى لفت انتباه المسيرين إلى المخاطر المعلوماتية التي سببها تطور استخدام تكنولوجيا المعلومات والاتصال في المؤسسة والتي أصبحت تهدد امن معلوماتها، وذلك بسبب عدم التخطيط الجيد لاعتماد واستخدام هذه التكنولوجيات، بالإضافة إلى إبراز ضرورة توفير برامج تدريبية لتوعية الموظفين والمستخدمين بأهمية أمن المعلومات بالنسبة للمؤسسة.

مجتمع وعينة البحث:

لقد تم اختيار المؤسسة العمومية مطاحن سيبوس – عنابة- مجتمعا للبحث، وهي مؤسسة تقوم بتحويل الحبوب وإنتاج وتسويق الدقيق وبقايا الطحن، وقد تم اختيارنا لها كميدان للبحث لأنها تعد من المؤسسات ذات الإنتاجية الكبيرة والتي تشكل جزءا مهما من الاقتصاد الوطني، أما عينة البحث فقد تضمنت مديرية الموارد البشرية، مديرية المحاسبة والمالية، قسم المراقبة والتسيير، حيث تم توزيع 35 استمارة استرجع منها 30 استمارة.

أدوات البحث ومنهج الدراسة:

كما سبقت الإشارة إليه فقد اعتمد في جمع البيانات الخاصة بهذا البحث على أداة الاستمارة، أما المنهج المستخدم فهو المنهج الوصفي، حيث اعتمد عليه في تحليل البيانات للوصول إلى نتائج تجيب عن إشكالية هذا البحث.

مفاهيم الدراسة:

- **تكنولوجيا المعلومات:**

تعرف تكنولوجيا المعلومات بأنها: "مجموعة من الأجزاء المرتبطة ببعضها البعض حيث تشتمل على أساليب المعالجة السريعة للمعلومات باستخدام الحاسوب وتطبيق الأساليب الإحصائية والرياضية في حل المشكلات ومحاكاة التفكير من خلال برامج الحاسوب." (1)

- **تكنولوجيا الاتصال:**

يقصد بتكنولوجيا الاتصال: "مجمل الأدوات والوسائل المادية والتنظيمية المستخدمة في جمع المعلومات، ومعالجتها وتخزينها واسترجاعها ونشرها وتبادلها، وتوصيلها إلى الأطراف المعنية". (2)

- **الأمن المعلوماتي:**

يمكن تعريف أمن المعلومات من خلال ثلاثة زوايا:

من الناحية الأكاديمية : هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها .

ومن الناحية التقنية: هي الوسائل، والأدوات، والإجراءات، اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية .

ممن الناحية القانونية: هي محل الدراسات والتدابير اللازمة لضمان سرية وسلامة محتوى المعلومات وتوفرها ومكافحة أنشطة الاعتداء عليها أو استغلالها في ارتكاب جرائم معلوماتية.

وبشكل عام فإنه يقصد بأمن المعلومات:

"حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث تؤمن المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسب المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة وذلك في جميع مراحل تواجد المعلومة (التخزين – النقل – المعالجة)".[3]

القسم الأول: الجزء النظري للدراسة

1. **تكنولوجيا المعلومات والاتصال في عصر المعلومات:**

يعتمد مجتمع المعلومات اعتمادًا أساسيًا على نشر المعلومات واستثمارها بالإضافة إلى توليدها طبعًا .فنجاح المؤسسات والشركات أصبح يعتمد كثيرًا على فعاليتها في جمع المعرفة واستعمالها لرفع الإنتاجية وتوليد سلع وخدمات جديدة، وقد أصبح الاقتصاد يقاد من قبل سلسلة هرمية من شبكات المعرفة التي تتغير فيها المعلومات بمعدلات سريعة[4] [4] ، بالإضافة إلى تكنولوجيا المعلومات والاتصال التي تعتبر القلب النابض لمختلف هذه المؤسسات ومنظمات الأعمال، إذ تساهم في تسهيل انسيابية القرارات الإدارية وفي توجيه وتنفيذ مختلف عملياتها فهي مصدر حيوي لديمومتها وبقائها وتميزها التنافسي خاصة وأنها تعيش في ظل مجتمع المعلومات، الذي يعد اقتصاده معلوماتي بالدرجة الأولى و تكنولوجيا المعلومات والاتصال السمة البارزة المميزة له.

وهنا تجدلا الإشارة إلى أن التطور الحاصل في تكنولوجيا الاتصال وتكنولوجيا المعلومات جعل من الصعب الفصل بينهما، فقد جمعهما النظام الرقمي، وبذلك انتهى عهد استقلال نظم المعلومات عن نظم الاتصال، ودخلنا في عصر للمعلومات والاتصال، حيث تبين من خلال الدراسات أن كمية المعلومات التي أنتجت في السنوات الأخيرة من القرن العشرين أكثر من تلك التي أنتجت في خمسة آلاف سنة مضت، وان تطبيقات العلم وتكنولوجيا المعلومات تزيد (14%) كل سنة وتتضاعف باستمرار، وظهرت تقنيات جديدة لإنتاج الثقافة، حيث تسيطر الثقافة الالكترونية، وهي جاءت من صلب تقنيات المعلومات ، هذا وينظر إلى ثورة المعلومات على أنها المتغيرات التي أحدثتها تقنية المعلومات، واهم متغيرين فيها: تقنيات الاتصال الحديثة، وأجهزة الحاسوب التي تقوم بمعالجتها، والتي لا يمكن الفصل بينهما كما سبق الإشارة لذلك سابقا لان أساسهما تواصل العلم والمعرفة[5].

البنية التحتية لتكنولوجيا المعلومات والاتصال:

تتكون تكنولوجيا المعلومات والاتصال من مجموعة من العناصر المترابطة التي تتفاعل مع بعضها البعض وهي كالتالي:

المكونات المادية:

تمثل المكونات المادية أو أجهزة الحاسوب عموما من ثلاث وحدات أساسية هي :

1. الوحدة المركزية: وتتكون هذه الوحدة من الوحدة الأم والمعالج الذي يعتبر عقل الحاسوب، حيث يقوم بتنفيذ كل العمليات الحسابية والمنطقية، إضافة إلى وحدة الذاكرة الرئيسية التي تكمن وظيفتها في تخزين تعليمات البرامج والمعطيات قيد المعالجة، التي تقوم بمعالجة البيانات بغرض تحويلها إلى شكل أكثر فائدة، إضافة إلى وظيفة السيطرة والتنسيق التي تقوم بها على بقية أجزاء الحاسوب.

2. وحدة التخزين الرئيسية: التي تقوم بالتخزين المؤقت للبيانات ولتعليمات البرنامج أثناء المعالجة.
3. وحدات التخزين الثانوي: التي تقوم بتخزين البيانات والتعليمات، عندما لا تكون مستخدمة في المعالجة، مثال ذالك: الأقراص والأشرطة الممغنطة،....

وسائل إدخال البيانات: التي ترسل وتحول البيانات والتعليمات للمعالجة في الحاسوب، مثل لوحة المفاتيح الفارة، التي تحول البيانات والتعليمات إلى أشكال اليكترونية، بغرض تهيئتها للإدخال في الحاسوب.

4. وسائل إخراج البيانات والمعلومات: التي تعرف البيانات والمعلومات بشكل يفهمه المستخدمون لنظام الحاسوب، مثل الطابعات والتي تقوم بتحرير البيانات الالكترونية المنتجة بواسطة نظام الحاسوب وعرضها بشكل يستطيع المستخدمين فهمها.

البرمجيات:

لغرض أن تلعب الحواسيب دورها المفيد في البنية التحتية لتكنولوجيا المعلومات في المؤسسة ، فهي تحتاج إلى البرمجيات لكي تؤدي عملها المطلوب.

والبرنامج : هو مجموعة منظمة من التعليمات في سياق منطقي تصدر وتعطي للحاسوب من اجل تمكينه من تنفيذ عمل معين، والقيام بالمعالجات المطلوبة لغرض تأدية الحاسوب لوظيفة محددة.

أما البرمجة فهي إجراء متعدد الخطوات (الغرض منها توفير مجموعة من المعلومات التي تشتمل على إرشادات استخدام لغات البرمجة) [5].

نظام الاتصالات عن بعد:

وهي المكون الأخير لتكنولوجيا المعلومات و الاتصالات عن بعد هي عبارة عن تراسل بالمعلومات والمعرفة عن طريق الوسائل الالكترونية، ويكون مثل

هذه التراسل عبر مسافات بعيدة المدى عادة وتشمل مثل هذه التراسلات على بيانات رقمية ، إضافة إلى البث الصوتي[6] .

2. **الأمن المعلوماتي في المؤسسة**

إن موضوع الأمن المعلوماتي يرتبط ارتباطا وثيقا بأمن تكنولوجيا الحاسوب فلا يوجد أمن للمعلومات إذا لم يراعى أمن الحاسوب، و في ظل التطورات المتسارعة في العالم و التي أثرت على الإمكانات التقنية المتقدمة المتاحة و الرامية إلى خرق منظومات الحاسوب بهدف السرقة أو تخريب المعلومات أو تدمير أجهزة الحاسوب ، كان لا بد من التفكير الجدي لتحديد الإجراءات الدفاعية و الوقائية حسب الإمكانات المتوفرة لحمايتها من أي اختراق أو تخريب، و كان على إدارة المنظمات أن تتحمل مسؤولية ضمان خلق أجواء أمنية للمعلومات تضمن الحفاظ عليها[7] .

تكنولوجيا المعلومات والاتصال و مخاطر امن المعلومات في المؤسسة:

يمكن تقسيم المخاطر المعلوماتية التي أفرزتها تكنولوجيا المعلومات إلى التصنيف التالي:

أ_ المخاطر البشرية:

وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو من خلال عمليات البرمجة، أو الاختبار أو التجميع للبيانات، أو أثناء إدخالها للنظام، أو في عمليات تحديد الصلاحيات للمستخدمين، وتشكل هذه الأخطاء نسبة كبيرة في المشاكل المعلوماتية التي تواجهها المنظمات[8].

والتهديدات في ما يتعلق بالمعلومات والأجهزة التي تمتلكها المؤسسات، لا تتمثل في قيام مجرمي الفضاء المعلوماتي بكتابة الرموز الخبيثة في أماكن افتراضية، فقط بل تشمل حتى موظفيها الذين يكونون موضع ثقتها.

حيث يمثل المستخدمون خطراً امنيا لأسباب عديدة منها أن حدود المؤسسات تستمر في الاتساع مع تزايد عدد العاملين المتنقلين لديها وتلاقي استخداماتهم الشخصية والمهنية في النقاط والمراكز الطرفية للمؤسسة التي يعملون فيها، فأجهزة الحاسوب باتت أكثر شخصية ومعبأة بالتطبيقات التي لا تتعلق بالعمل، والتي من شأنها أن تعرض المؤسسة إلى برامج التجسس والمتسللين والتهديدات الأخرى[9].

وثمة أيضا أخطار متزايدة تترصد حب الاستطلاع لدى المستخدمين في المراكز الطرفية هذه. ويكون أسلوب الخداع على شكل موقع في الشبكة، أو رسالة الكترونية مصممة للاحتيال على الموظفين، لكي ينجزوا أعمالا وعمليات لها تأثير كبير على امن المؤسسة، أو فضح معلومات سرية. والأدهى من ذلك أن الموظفين هم في حركة تنقل دائمة بين المؤسسات المتنافسة بسبب قيام هذه المؤسسات بتوظيف الموظفين المهمين طمعا في مهاراتهم، وأيضا للحصول على المعلومات السرية التي يجلبونها معهم. وبشكل إجمالي فان التهديد الداخلي سواء كان مضرا أو غير مضر، فهو أمر لا يمكن التغاضي عنه أبدا

وهناك من المخاطر من هي غير مقصودة، حيث ينتج الانتهاك غير المقصود لسلامة وامن البيانات غالبا عن إجراءات خاطئة وغير سليمة تتراوح بين إجراءات تجهيز وإدخال البيانات وحتى أخطاء التشغيل التي تحدث أثناء المعالجة، مرورا بأخطاء ونقاط الضعف غير المنظورة في البرامج التطبيقية نفسها[10].

- إن غالبية الموظفين بدون قصد كثيرا ما يتخذون خيارات غير صحيحة عندما يتعلق الأمر بالتعاطي مع معلومات المؤسسة وبياناتها. ومثال على ذلك هو انه مع تزايد قيام المستخدمين باستخدام الأجهزة الرقمية والمساعدات الشخصية الرقمية وغيرها، يتوجب على المديرين الأمنيين التذكر أن هذه الأجهزة قضت معظم عمرها موصولة إلى حواسيب المنزل الأقل أمنا. وهذا ما يجعل من السهل على المستخدمين تنزيل فيروس مؤذ من دون قصد، أو

رمز مدمر في أحد حواسيب المؤسسة،بالإضافة إلى الأخطاء التي تحدث سهوا أثناء القيام بالأنشطة اليومية بالمؤسسة.

- الإهمال: وهو يمثل الطريقة الأكثر شيوعا لاختراق المعلومات ويعود السبب في ذلك إلى إهمال الأفراد العاملين وتهاونهم أو ضعف إدراكهم لأهمية الاحتفاظ بسرية المعلومات و العواقب الوخيمة المترتبة لاختراق أمنية المعلومات، إلى جانب عدم معرفتهم المعلومات التي تحتاج إلى الحماية ومن يمتلك الدافع إلى استغلال هذه المعلومات من داخل المؤسسة وخارجها.

ب_ العنصر التكنولوجي:

الفيروسات: وهي عبارة عن برامج ذات أهداف تدميرية تتمثل في إحداث أضرار بنظام الحاسوب أوبرمجيته أو مكوناته، ولقد ولدت فكرة الفيروس الالكتروني منذ بدايات الحاسوب على يد جون فون نيومان الذي أسس لذلك في مقالة نشرها بعنوان: "نظرية وتنظيم الآلة المعقدة ذاتية الحركة" عن إنتاج أوتومات تقوم بعمل نسخة مطابقة لذاتها، وقد كشف عن وجود فيروسات الحاسوب الأولى كين تومبسون سنة 1983.

يستخدم مصطلح الفيروسات للدلالة على برامج صغيرة تلحق نفسها بملف ما وتقوم بإعادة إنتاج نفسها (تكاثر) وتتميز بسرعتها في إعادة إنتاج نفسها، وتظل كامنة في بعض البرامج بانتظار تاريخ أو حدث معين لتقوم بحركتها وتنسخ نفسها من ملف إلى آخر ومن جهاز حاسوب إلى آخر وتعمل بشكل مستقل عن ملفات التشغيل الأخرى وتقوم بالسيطرة على الذاكرة ومساحة القرص[11].

القرصنة: هي عملية الدخول إلى الأنظمة المعلوماتية من طرف أصحاب الخبرة وهم عادة مبرمجون غير مسموح لهم بالدخول إلى تلك الأنظمة ، يهدفون إلى كسر الحواجز الأمنية المحيطة بهذه الأنظمة.

ج. الأخطار البيئية:

وتشمل هذه الأخطار الزلازل والعواصف والفيضانات والأعاصير و المشاكل المتعلقة بأعطال التيار الكهربائي والحرائق إضافة إلى المشاكل القائمة في تعطل أنظمة التكيف والتبريد وغيرها، وتؤدي هذه الأخطار إلى تعطل عمل هذه التجهيزات وتوقعها لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات.[12]

د. مشاكل جودة النظام:

فضلا عن الكوارث والفيروسات والخروقات لأنظمة المعلومات هناك أيضا تخلق البرمجيات والبيانات الناقصة والتي تسبب تهديدا " دائم" لنظم المعلومات مسببة خسائر لا مثيل لها في الإنتاجية والخطأ غير المكتشف في برمجيات ائتمان المعلومات، أو البيانات المالية الخاطئة يمكن أن ينتج عنه خسائر بملايين الدولارات فضلا عن التعطيلات أو الأخطاء في البرمجيات وضعف البيانات كمدخلات.

إن كل هذه المخاطر التي تهدد امن معلومات المؤسسة لها العديد من الأسباب منها:

- عدم وجود مسؤولية واحدة: إذا كان الحاسوب مشترك من قبل عدد من المستخدمين لا احد يعلن مسؤوليته المنفردة للصيانة أو الإشراف أو السيطرة على الجهاز.
- عدم وجود التدقيق: إذا كانت هناك مشكلة، فمن غير الممكن معرفة من الذي وصل للجهاز ومتى؟.
- عدم وجود نسخ أخرى: حتى المستخدمين أصحاب الخبرة ينسون عمل نسخ إضافية للملفات المهمة، وكذلك الأمر بالنسبة للمستخدمين الجدد وذلك لقلة خبرتهم.
- دمج الواجبات: وما ينتج عنه من ضعف في التدقيق والموازنة.

مجالات مخاطر امن المعلومات المرتبطة بتكنولوجيا المعلومات.

أ. المعطيات:

تعد المعطيات العنصر الأساسي للأنظمة وتشمل كافة البيانات المدخلة، والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم و المعطيات، قد تكون في طور الإدخال أو الإخراج أو التخزين أو التبادل بين النظم عبر الشبكات، و قد تخزن داخل النظم أو على وسائط التخزين خارجها.

ومن الأمثلة على التهديدات التي تتعرض لها المعطيات:

- الحذف أو النسخ.
- التشويه الناتج عن مشاكل الأجهزة والبرامج.
- السرقة. [13]

ب. الأجهزة :

المخاطر التي تصاحب كافة المعدات والأدوات المادية التي تتكون منها النظم كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها[14].

ومن الأمثلة على هذه التهديدات:

- الاستخدام الخاطئ أو التصرف الغير سليم أو الحماية غير الجيدة .
- العبث أو التدمير من موظف في عمل الأجهزة والمعدات.
- السرقة (الحاسوب، أو الطابعة أو الموارد الأخرى)[15].

ج.الاتصالات:

وتشمل شبكات الاتصال التي تربط أجهزة التقنية بعضها بعض محليا ونطاقيا ودوليا، وتتيح فرصة اختراق النظم عبرها، كما أنها بحد ذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي .

ومحور الخطر الفرد سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بالنظام فإدراك هذا الشخص حدود صلاحياته وإدراكه آليات التعامل مع الخطر وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية مسائل رئيسية يعنى بها نظام الأمن الشامل تحديدا في بيئة العمل المرتكزة على نظم.

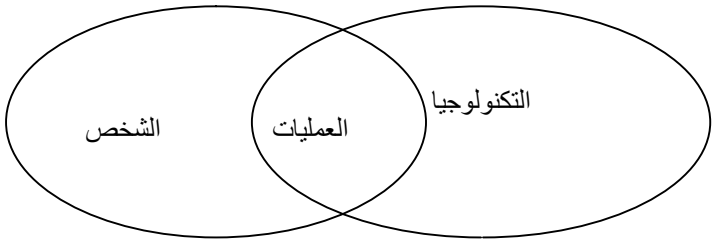
د. البرامج:

وتشمل الأوامر المرتبة في نسق معين لانجاز الأعمال وهي إما مستقلة عن النظام أو مخزونة فيه ومن أمثلة المخاطر المرتبطة بها:

- حذف برنامج عرضيا أو عن غير قصد.
- سرقة برنامج.
- تشويه برنامج إما نتيجة عطل في الأجهزة أو غيرها.
- عيوب ومشاكل البرامج[16].

3. **تأسيس وعي ناضج بأمن المعلومات في ظل التطور الكبير لتكنولوجيا المعلومات والاتصال:**

إن امن المعلومات هو حماية المعلومات والأنظمة التي تدعمهم مباشرة من الاستخدام أو الدخول، أو الكشف، أو التعطيل، أو التخريب غير المصرح به. ويجب على أي منظمة بغض النظر عن حجمها أو عددها باستخدام الآليات التالية لممارسة وتحسين امن المعلومات لديهم. والآليات المستخدمة هي الأشخاص، العمليات، والتكنولوجيا.



شكل1: يوضح تداخل الآليات المستخدمة في امن المعلومات

إن العامل الوحيد المشترك كما هو موضح في الشكل أعلاه إن الأشخاص هم من يقومون بإدارة العمليات والتكنولوجيا، ولذلك فان كل موظف دائم أو مؤقت، أو متعهد... لديه دوره ومسؤولياته في امن المعلومات التي يحتاج إلى إتمامها، ومن هنا تأتي أهمية إيصال معلومات كافية ووافية فيما يخص المسؤوليات الأمنية.

فالوعي بأمن المعلومات شديد الأهمية لأي إستراتيجية أمن خاصة بالمؤسسات ودعم عمليات الأمن المعلوماتي.و على الرغم من أهمية توعية المستخدمين بدورهم ومسؤوليتهم في الأمن المعلوماتي فان 64% من المنظمات في أمريكا، و 48% من منظمات انجلترا، 59% من منظمات الهند فقط تقوم بتوفير برامج توعية أمنية على الرغم من اللوائح التي تأمر بذلك، والكثير من الحوادث التي تؤدي إلى خسارة ملايين الدولارات كغرامات وخسارة السمعة التي كان من الممكن تجنبها، بتوفير وعي وتدريب مناسب للمستخدمين والتقنيين والمديرين.

بالإضافة إلى تشكيل مجموعة تكنولوجيا المعلومات، تهتم خصيصا بقسم تكنولوجيا المعلومات وتتضمن رؤساء الأقسام تتابع متطلبات التدريب التي يحتاجها الموظفين في الأقسام، وتقوم هذه المجموعة أيضا بقياس مدى نجاح التدريب بمقياس تكنولوجيا المعلومات[17].

إن إتباع هذه الإجراءات يعمل على تحقيق الأهداف الإستراتيجية، فهذه الأهداف مرتبطة مباشرة بموثوقية البنية التحتية التكنولوجية للمؤسسات[18].

القسم الثاني: الإيطار التطبيقي للدراسة

جدول (01) إجابات الأفراد المبحوثين حول مستواهم في الإعلام الآلي:

ما هو مستواك في الإعلام الآلي؟	ممتاز	جيد	متوسط	مقبول	لا رأي لي
التكرار	01	07	13	06	03
النسبة المئوية	%03.33	%23.33	%43.34	%20	%10

يمثل الجدول رقم (01) توزيع عينة الدراسة من حيث مستواهم في الإعلام الآلي، حيث مثلت فئة متوسط نسبة:43.34% ، تليها فئة جيد بنسبة: 23.33%، بعدها فئة مقبول بنسبة 20%، تليها فئة لا رأي لي بنسبة: 10% ، وفي الأخير فئة ممتاز بنسبة: 3.33%. ومن خلال النسب يظهر أن أغلبية الموظفين مستواهم متوسط في الإعلام الآلي تليها مجموع فئة مقبول وفئة لا رأي لي وتأتي فئتي جيد وممتاز في الأخير، وهذا يعني أن مستوى الموظفين لا يفي بالغرض الكافي للتحكم في تكنولوجيا الحاسوب ومما افتقارهم للخبرة الكافية لمعرفة أسس تأمينه.

جدول رقم (02) إجابات أفراد العينة حول توفر مكاتبهم بأجهزة الحاسوب ولوازمها:

هل لديك جهاز حاسوب و لوازمه في مكتبك؟	نعم	لا
التكرار	26	04
النسبة المئوية	%86.67	%13.33

يمثل الجدول رقم (02) توزيع عينة الدراسة حسب توفر مكاتبهم على أجهزة الحاسوب ولوازمها، حيث مثلت نسبة 86.67% المكاتب التي تتوفر على هذه الاجهزة، في حين أن نسبة 13.33 % مثلت فئة المكاتب التي لا تحتوي أجهزة الحاسوب ولوازمها، ومن خلال هذه النسب نلاحظ أن المؤسسة تساير تطور تكنولوجيا المعلومات، حيث أن أغلبية المكاتب تحوي هذه التكنولوجيات.

جدول رقم (03) إجابات أفراد العينة حول إن كانت أجهزتهم موصولة بشبكة الانترنيت أم لا:

هل جهاز حاسوبك موصول بشبكة الانترنيت	نعم	لا
التكرار	22	04
النسبة المئوية	%84.62	%15.38

يتضح من خلال الجدول رقم (03) بان المؤسسة المبحوثة توفر شبكة الانترنيت لمكاتب الموظفين، وذلك بمعدل 84.62%، في حين أن نسبة المكاتب التي لا تتوفر على شبكة الانترنيت هي15.38%، وتدل هذه النتائج على أن

المؤسسة تحرص على توفير الاتصال الشبكي لموظفيها وذلك لتدعيم وتسهيل عملية الاتصال وتبادل المعلومات في المؤسسة.

جدول رقم (04) إجابات أفراد العينة حول نوع الاتصال الأكثر استخداما في المؤسسة:

هل عملية الاتصال في المؤسسة تتم بطريقة:	مباشرة	غير مباشرة
التكرار	21	29
النسبة المئوية	%42	%58

الجدول رقم (04) يبين توزيع عينة الدراسة من حيث نوع الاتصال الأكثر استخداما في المؤسسة حيث مثلت فئة غير مباشرة بنسبة (58%) , وهي أعلى نسبة و تليها فئة مباشرة بنسبة (42%) ، وهذا يدل على أن الموظفين في انجازهم لوظائفهم لا يتعاملون بصفة مباشرة بصفة دائمة، و يعود ذلك لكبر حجم هذه المؤسسة، و هذا ما يصعب عملية التحرك و التنقل بسهولة ، لذلك يلجا الموظف إلى الاتصال الغير مباشر بنسبة كبيرة، حتى يتمكن من معرفة كل ما يحتاجه عن المؤسسة وعمله بها وأيضا ليبقى على اتصال دائم بباقي الموظفين.

جدول رقم (05) إجابات أفراد العينة حول وسائل الاتصال الغير المباشر في المؤسسة:

ماهي وسائل الاتصال غير المباشر المستخدمة في العمل؟	الهاتف الثابت	الهاتف النقال	الانترنيت	الانترانيت	الاكسترانيت
التكرار	30	30	22	00	00
النسبة المئوية	%36.58	%36.58	%26.82	%00	%00

يوضح الجدول رقم (05) توزيع مفردات العينة حول وسائل الاتصال المستخدمة في العمل، فكانت النتائج أن جميع المبحوثين يستخدمون الهاتف الثابت بنسبة: 36.58% والنسبة مثلها بالنسبة للهاتف النقال، بعدها تأتي فئة الانترنيت بنسبة:26.82% ، وفي الأخير فئتي الانترانيت الاكسترانيت بنسبة 00% لكل فئة، ويظهر من خلال هذه النتائج الاستخدام الكبير للهواتف بنوعيها وشبكة الانترنيت في الاتصال بين موظفي المؤسسة، ولكن انعدام الشبكة الداخلية والمحلية بالنسبة للمؤسسة يشكل نقطة يمكن أن تنعكس على نجاح المؤسسة بصفة عامة، وعلى خصوصيتها وامن معلوماتها بصفة خاصة، لان توفر مثل هذه الشبكات داخل المؤسسة يجعل عملية الاتصال داخلها أكثر سرعة وسهولة وأمنا، أيضا باعتبار أن اتجاهات سيرورة المعلومات تكون معروفة مما يمكن من اكتشاف الأخطار والتهديدات التي تحيط بنظام المعلومات و بأقل جهد ممكن وأقل تكاليف.

جدول رقم (06) إجابات أفراد العينة حول مصادر المعلومات الأكثر اعتمادا في المؤسسة:

مصادر المعلومات الأكثر اعتمادا من بين المصادر التالية؟	المواقع الالكترونية	الشبكات الاجتماعية	وارد البريد الالكتروني	أخرى تذكر
التكرار	22	10	20	00
النسبة المئوية	%42.30	%19.23	%38.46	%00

يظهر من خلال نتائج الجدول (06) أن المواقع الالكترونية كمصادر للمعلومات الالكترونية جاءت في المرتبة الأولى بنسبة:42.30%، تليها فئة وارد البريد الالكتروني بنسبة: 38.46% ، بعدها فئة الشبكات الاجتماعية بنسبة: 19.23%، في حين لم ترد أي استجابة لفئة أخرى تذكر، وهذا يبين لنا بان المعلومات الالكترونية مهمة بالنسبة للمبحوثين خاصة وان المؤسسة توفر شبكة الانترنيت لمعظم المكاتب، واعتمادهم على هذه المصادر بصفة كبيرة يعود أيضا لما لها من خصائص كالسرعة والتفاعلية.

جدول رقم (07) إجابات أفراد العينة حول رأيهم في المخاطر المعلوماتية التي تخلقها تكنولوجيا المعلومات في المؤسسة:

حسب رأيك ما هي مخاطر المعلومات التي تخلقه تكنولوجيا المعلومات في المؤسسة؟	الفيروسات	القرصنة الالكترونية	مشاكل البرامج وصعوبة تشغيلها	أخرى تذكر
التكرار	25	06	05	00
النسبة المئوية	%69.44	%16.66	%13.88	%00

يبين الجدول رقم (07) مخاطر المعلومات التي خلقتها تكنولوجيا المعلومات في المؤسسة حسب رأي المبحوثين، حيث مثلت فئة الفيروسات 69.44% وهي أعلى نسبة، تليها فئة القرصنة الالكترونية بنسبة: 16.66% ، بعدها تأتي فئة مشاكل البرامج وصعوبة تشغيلها، وفي الأخير جاءت فئة أخرى تذكر حيث بقيت فارغة ولم ترد فيها أية إجابة، ويتبين لنا من خلال هذا أن الفيروسات هي اكبر المخاطر المعلوماتية التي خلقتها تكنولوجيا المعلومات والتي تهدد امن معلومات المؤسسة خاصة وان الفيروسات يمكن أن تكون في أي مكان، فقد تكون في رسائل البريد الالكتروني، أجهزة USB ... وغيرها.

جدول رقم (08) إجابات أفراد العينة حول رأيهم في أسباب المخاطر المعلوماتية:

حسب رأيك ما هي أسباب مخاطر امن المعلومات في المؤسسة؟	الممارسات القصدية الخاطئة عند استخدام تكنولوجيا المعلومات والاتصال	نقص الخبرة	عدم وجود برامج منتظمة لحماية نظام المعلومات	أخرى تذكر
التكرار	06	13	20	00
النسبة المئوية	%15.38	%33.33	%51.28	%00

يوضح الجدول رقم (08) توزيع المبحوثين حسب رأيهم في أسباب المخاطر المعلوماتية، حيث جاءت فئة وجود برامج منتظمة لحماية نظام المعلومات بنسبة 51.28%، تليها فئة نقص الخبرة 33.33%، بعدها فئة الممارسات القصدية الخاطئة عند استخدام تكنولوجيا المعلومات والاتصال بنسبة 15.38%، أما فئة أخرى تذكر فلم ترد أية إجابة فيها، ومن خلال هذه النسب نلاحظ أن أسباب مخاطر المعلومات متعددة ومتنوعة، منها ما هو مرتبط بالأفراد لأن من يستخدم هذه التكنولوجيات هم الأفراد وممارساتهم الخاطئة ونقص الخبرة لديهم هو ما يتسبب في هذه المخاطر، وأخرى مرتبطة بالتنظيم، لان عدم وجود برامج منتظمة لحماية نظام المعلومات تعد أيضا من الأسباب التي لها دور في نشوء هذه المخاطر.

جدول رقم (08) إجابات أفراد العينة حول تدريبهم وتكوينهم على استخدام تكنولوجيا المعلومات والاتصال:

هل هناك برامج لتكوينكم وتدريبكم على استخدام تكنولوجيا المعلومات والاتصال الحديثة؟	نعم	لا
التكرار	04	26
النسبة المئوية	%13.33	%86.67

يبين الجدول رقم (14) الإحصائيات المتعلقة بتكوين الموظفين على استخدام تكنولوجيا المعلومات والاتصال، فنجد نسبة المبحوثين الذين لم يسبق لهم إجراء مثل هذه التكوينات جاءت بالأغلبية الساحقة بـــ: 86.67% ، في حين جاءت نسبة13.33% .للذين استفادوا من تكوين ، و يظهر هنا الحاجة الكبيرة لضرورة التكوين، الذي يساهم في تطوير الموظف في مجال استخدام التكنولوجيات الحديثة للمعلومات و الاتصال، فالتكوين يعتبر عنصر أساسي في مسار الموظف، مما يجعله غير منعزل عن المحيط الذي يعمل فيه، ويجعل المؤسسة كذلك غير معزولة ومواكبة للتطورات المختلفة في هذا الميدان مما يساهم في نجاحها وتطورها.

نتائج الدراسة:

من خلال ما سبق تم التوصل إلى النتائج التالية:

- الاستخدام الكبير لتكنولوجيا المعلومات والاتصال (الحواسيب، الهواتف، الشبكات) وهذا يعني أن هذه الأخيرة تعرف تطورا كبيرا في المؤسسة وانجاز الأعمال المختلفة بها.

- الاعتماد على المصادر الالكترونية بصفة عالية لدى المبحوثين خاصة منها المواقع الالكترونية و البريد الالكتروني
- وجود العديد من المخاطر المعلوماتية التي تهدد امن معلومات المؤسسة، كالفيروسات بالإضافة إلى مخاطر أخرى متعلقة بالبرامج ، والقرصنة الالكترونية.
- أسباب مخاطر المعلومات متنوعة ومتعددة منها ما هو مرتبط بالفرد المستخدم، وأخرى مرتبطة بالتنظيم وقواعد العمل بالمؤسسة.
- ضعف اهتمام المؤسسة بتوفير برامج تكوين في مجال تكنولوجيا المعلومات والاتصال التي بدورها تساهم في توعية الموظفين بأمن المعلومات.

توصيات الدراسة:

- إجراء المزيد من البحث والدراسات حول موضوع الأمن المعلوماتي وعلاقته بتطور استخدام تكنولوجيا المعلومات والاتصال في المؤسسة، لأنه كلما تطورت تكنولوجيا المعلومات كلما تطورت المخاطر التي تنتج عنها.

ضرورة قيام المؤسسة بتدريب الموظفين على استخدام تكنولوجيا المعلومات والاتصال و القيام ببرامج التوعية بأهمية أمن المعلومات بها وكذا كيفية الاستخدام السليم لهذه التكنولوجيات، لان النجاح ليس بمواكبة التطورات فقط بل بالتخطيط ووضع إستراتيجية مضبوطة لتحيق ذلك.

❖ هوامش البحث

(1) عدنان عواد الشوابكة، **دور نظم وتكنولوجيا المعلومات في اتخاذ القرارات الإدارية**، دار اليازوري، عمان،2011، ص176.

(2)عبد الملك ردمان الدناني، **تطوير تكنولوجيا الاتصال وعولمة المعلومات**، المكتب الجامعي الحديث، القاهرة،2005 ، ص 11.

(3) عبدالله بن شائع بيهان، **ثقافة أمن المعلومات**، 2014-09-02، faculty.ksu.edu.sa/A.../

(4) محمد مراياتي، **المصطلح في مجتمع المعلومات، أهميته وإدارته وأدواته**، 2014-09-03 www.yemen.nic.info/content/informatics/...

عبد الستار العلي وآخرون، **المدخل إلى إدارة المعرفة**، دار المسيرة، عمان، 2006، ص214-218(6).

(7) المرجع نفسه، ص.232

(8)نجم عبد الله الحميدي وآخرون، **نظم المعلومات الإدارية**، مدخل معاصر، دار وائل، عمان، 2005، ص263.

(9) المرجع نفسه، ص267.

(10) الشرق الأوسط ، جريدة العرب الدولية، فيفري، 2008، العدد 10675 http://www.aawsat.com

(11) دلال صادق، حميد ناصر الفتال، **أمن المعلومات**، دار اليازوري، عمان، 2008، ص15.

(12) عبد الحميد بسيوني، **الحماية من أخطار الانترنيت**، دار الكتب العلمية، القاهرة، 2003، ص118.

(13) نجم عبد الله الحميدي وآخرون، مرجع سابق، ص 267.

(14) عبد الحميد بسيوني، مرجع سابق، ص215.

(15) منير محمد الجنيهي، ممدوح محمد الجنيهي، **أمن المعلومات الالكترونية**، دار الفكر الجامعية، القاهرة،2006،ص14.

(16) عبد الحميد بسيوني، مرجع سابق، ص 214.

(17) المرجع نفسه، ص215 .

(18) Moataz Salah, **Security Kaizen Magazine, best practice**, july/ sebtember 2012, p 44,
www.bluekaizen.org

(19) Jan H.P.Eloff , **Advances In Information Security Management And Small Systems Security**, K.A .Publishers, USA, 2001,p14.