العدد 01.
المجلد 05. السنة 2020.

ISSN: 2571-9769, EISSN: 2602-5051 الأفاق للدراسات الإقتصادية
الصفحات 124ــ136

المورد البشري خطر أم حصن للمنظمة؟
مدخل: أمن المعلومات في ظل الذكاء لاقتصادي

Is the human resource a threat or a fortress to the organization?
Introduction: Information security in light of economic intelligence

* ط.د. لخضر دلال
جامعة محمد خيضر، بسكرة، الجزائر.
مخبر مالية بنوك وادارة اعمال
dallel.lakhdar@univ-biskra.dz

د.اسماعيل بن ديلمي
جامعة باتنة1 ، الجزائر.
مخبر LEEGAA.
bendilmiismail@gmail.com

تاريخ الاستلام: 27 /2020/3 تاريخ القبول: 03 /2020/04 تاريخ النشر : 05 /2020/04

ملخص: تهدف هذه المداخلة إلى استعراض أهم المفاهيم المتعلقة بالذكاء الاقتصادي وأمن المعلومات، إذ أصبحت المعلومة تدخل في صميم الحياة اليومية والمهنية، لهذا تضطر المؤسسات إلى إدماج الذكاء الاقتصادي في استراتيجياتها، من خلال الاعتماد على تكنولوجيات الإعلام والاتصال في التكامل مع منظومة المعلومات والمعرفة التي تمتلكها هذه المنظمات، لتكوين الميزة التي تضمن تحقيق المنافسة والبقاء والتطور. لكن الاعتماد على هذه التكنولوجيات فتح الأبواب لدخول مخاطر لم تكن معروفة مسبقا وغير متوقعة. وعليه, سيتم توضيح أنواع المخاطر المتعلقة بمعلومات المنظمة وكذا دور المورد البشري في تسهيل عملية حمايتها، ودور التدريب والولاء للمنظمة في ذلك.

الكلمات المفتاحية: الذكاء الاقتصادي، تكنولوجيات الإعلام والاتصال، حرب المعلومات، أمن المعلومات.

تصنيف jel: L 20 , M15

Abstract: This intervention aims to review the most important concepts related to economic intelligence and information security, as information has become a core part of daily and professional life, so institutions have to integrate economic intelligence into their strategies, by relying on information and communication technologies to integrate with the information system and knowledge that these organizations possess To create a feature that guarantees competition, survival and development. But relying on these technologies has opened the doors to entering previously unknown and unpredictable risks. Accordingly, the types of risks related to the organization's information will be clarified, as well as the role of the human resource in facilitating its protection process and the role of training and loyalty to the organization in that.

Key words: economic intelligence, information and communication technologies, information warfare, information security.

Jel classification codes: L20, M15.

المؤلف المرسل: ط.د. لخضر دلال,

I-تمهيد:

في ظل مناخ يتسم بالتنافسية ويعتمد على استخدام المعلومات، تلجأ المنظمات إلى تبني الذكاء الاقتصادي حتى تتمكن من التكيف مع البيئة المحيطة بها بنجاح وتتمكن من تحقيق أهدافها، فهي تحتاج للمعلومات التي تمثل أساسا متينا ومفتاحا لإيجاد المكانة الإستراتيجية وتكوين الرؤية، لكن التحدي المفروض أمامها هو الوصول إلى المعلومة الصحيحة وليس القريبة، لأنها تساعد في حل المشاكل والوقايةمنها باتخاذ القرارات المناسبة وسبق المنافسين وأيضا تطوير أساليب العمل والتنويع في وقت وجيز.

واليوم مع بروز تقنيات الإعلام والاتصال أصبحت المعلومة متوفرة، لكن الأهم هو كيفية هيكلة هذه المعلومات وتحليلها وإثرائها وتوجيهها للهدف، فطرق البحث والمراقبة ونشر المعارف تتم ضمن نظام للمعلومات يضم مجموعة من الوسائل التنظيمية، "البشرية والتكنولوجية "تستخدم في تسيير المعلومة، فهو المورد الأساسي لها والمسؤول على حمايتها وتوفيرها بالدقة والمرونة المطلوبة لتسهيل تعامل المنظمة مع الظروف والتحديات البيئية المحيطة بها. لذا يجب أن تتمتع هذه الأنظمة بالحصانة الكافية والإعفاء من أي اختراقات أو أعطال قد تضر بمحتواها، فأمن معلومات المنظمة مسؤولية تقع على جميع أفرادها، لأن عواقب انتهاك أو تسرب أي بيانات أو معلومات خاصة بها قد تكون عالية الكلفة وتؤدي إلى تشويه سمعتها. فتوفير الحماية للمعلومات هو في حدّ ذاته عملية استثمارية صحّية وطويلة الأمد للمنظمة وتوضح الجانب الدفاعي للذكاء الاقتصادي.

لذلك وفي ضوء ما سبق تحاول هذه الورقة البحثية توضيح الدور الذي يمكن أن يشكله المورد البشري في المنظمة كجدار حماية أو ثغرة تتسرب منها معلومات المنظمة الإستراتيجية في ظل تبني ما يسمى بالذكاء الاقتصادي، وذلك بالتطرق إلى المحاور التالية:

أولا- الذكاء الاقتصادي وتكنولوجيات الإعلام والاتصال

ثانيا- أمن (حماية) المعلومات والمخاطر التي تعترضها

ثالثا- طرق حماية المعلومات ودور المورد البشري

أولا: الذكاء الاقتصادي وتكنولوجيات الإعلام والاتصال

تحتاج منظمات اليوم إلى الاستجابة السريعة للفرص والتهديدات المحيطة بها، وذلك نظراً للتغيرات السريعة والغير متوقعة الاقتصادية منها والاجتماعية والتكنولوجية والتنافسية... ومن أجل أن تتمكن المنظمة من تحقيق النجاح والبقاء في هذه البيئة يتوجب عليها اتخاذ خطوات مبتكرة، كتبني إستراتيجية الذكاء الاقتصادي والاستعانة بأدوات تكنولوجيا المعلومات لتسهيل نشاطاتها وعملياتها، لكن بداية سيتم التعرف على ماهية الذكاء الاقتصادي.

1.ماهية الذكاء الاقتصادي: يعتبر مصطلح الذكاء الاقتصادي من المصطلحات التي ظهرت كنتيجة لظهور اقتصاد المعرفة الذي تَقَوم أنشطته بصورة أساسية بالاعتماد على المعلومات، من خلال توظيف تكنولوجيات

الإعلام والاتصال في اكتساب المعلومات ومعالجتها وبثها إلى الأفراد للاستفادة منها في حل والقيام بأعمالهم البسيطة والمعقدة منها.

1.1. تعريف الذكاء الاقتصادي: نال موضوع الذكاء الاقتصادي قدرا كبيرا من الاهتمام بناءً على دراسات مكثفة ونقاشات عديدة وقدمت له تعريفات عديدة، أهمها:

- **تعريف هارولد**(Harold Wilensky)**:** "الذكاء الاقتصادي يحدد النشاط الاقتصادي لإنتاج المعرفة في خدمة الأهداف الاقتصادية والإستراتيجية للمنظمة التي جمعت والمنتجة في سياق قانوني وذات مصادر مفتوحة." (www.ces.fr/rapport/rapsec/R5052710.pdf)
- **تعريف مارتر**(Henri Martre)**:** "الذكاء الاقتصادي مجموعة من الإجراءات المنسقة للبحث والتجهيز والتوزيع للاستهلاك للوصول إلى معلومات مفيدة و ذات فعالية اقتصادية."(مسعود ديلمي، 2008)

ونظرا لضرورة اعتماد مدير المنظمة لإستراتيجية تطوير منتج جديد، والاستثمار في سوق جديد، تحسين المردودية، معرفة المنافسين، أخذ القرار الصائب في الوقت المناسب ...الخ، فإن الأمر يتطلب فهم المحيط الذي يتسع ويتعقد باستمرار، وفي هذا الإطار تعتبر المعلومة مادة أولية أساسية للإدارة الجيدة للمنظمة .إلا أن هذا لا يتحقق إلا من جراء وضع ضمانات لحماية مكونات وتراث المؤسسة في ظل أفضل للظروف سواء من ناحية الزمن أو التكاليف، وهي المعلومات التي يحتاج إليها صانعي القرارات من اجل تحقيق إستراتيجيتهم وأهدافهم.

- **تعريف أربيلو**(Christian Harbulot)**:** "الذكاء الاقتصادي بأنه منهجية البحث وتفسير المعلومات المتاحة للجميع من أجل تفعيلها ومعرفة قدرتها "و هذا التعريف له علاقة بالمعلومات المفتوحة مما يجعلها تمتثل للمصداقية والأخلاق، هوية الأطراف الفاعلة فيه أي جميع موظفي الإدارة تشارك في بناء ثقافة المعلومات."(مسعود ديلمي، 2008)
- **وقد عرّفه** Alain Juillet المسؤول الأعلى للذكاء الاقتصادي بفرنسا سنة 2005 على أنه: "الذكاء الاقتصادي يرتكز على حماية المعلومات الإستراتيجية لكل المتعاملين الاقتصاديين، من أجل الحفاظ على تنافسية القطاع الاقتصادي، حماية الاقتصاد، وتعزيز سياسة التأثير."أي أنه يشتمل على السيطرة وحماية المعلومة الإستراتيجية لجميع الأعوان الاقتصاديين." (http://www.medefparis.fr/Livre_Blanc.pdf)

وبالتالي فالذكاء الاقتصادي يتمثل في الأنشطة المنسقة المتعلقة بالبحث عن المعلومة المفيدة للفاعلين الاقتصاديين ومعالجتها وتوزيعها قصد استغلالها. ويتم القيام بهذه الأنشطة قانونيا مع توفير كل الضمانات اللازمة لحماية تراث المؤسسة وفي ظل أفضل ظروف الجودة والآجال والتكلفة. وهنا لابد من التفريق بين الذكاء الاقتصادي واليقظة، والتي تتمثل في رصد وجمع المعلومات في مجالات إستراتيجية من أجل تغذية عملية صنع القرار على المستوى العام والخاص.

كما يجدر التفريق بين الذكاء الاقتصادي الذي تجمع من خلاله المعلومات بصفة قانونية، والتجسس الذي يحصل من خلاله – عبر اقتحام غير قانوني – على معلومات سرية في مكان محفوظ.

2.1.أهمية الذكاء الاقتصادي والهدف من تبنيه في المنظمة: تتمثل في: (بول جامبل، جون بلاكويل،2002)

- **أهمية الذكاء الاقتصادي:** تتمثل أهمية توظيف الذكاء الاقتصادي، في كونه يتيح لمختلف الفاعلين

والشركاء والمتدخلين في العملية التنموية فهم وتحليل المحيط، الذي يشتغلون فيه من أجل تطوير كفاءاتهم وقدراتهم على التلاؤم مع المتغيرات، وتوقع واستباق التطورات الحاصلة، وتجريب الحلول الملائمة لخصوصيات أوضاع المحيط وموارده، ثم الابتكار من أجل تعزيز عاملي التنافسية والأداء.

- **الهدف من الذكاء الاقتصادي:** يهدف الذكاء الاقتصادي إلى التحكم في المعلومة والمعرفة والحفاظ عليها نظرا لأهميتها في تطوير وترقية المؤسسة، ويستدعي أيضا التعرف على كيفية تسيير المعلومة وانتقاء الأهم منها للخروج بما هو ضروري لفائدة المؤسسة لاسيما في مجال اتخاذ القرارات الأساسية. فهو يسعى إلى ربط النظم الفرعية للمنظمة مع بعضها البعض وذلك بجعلها في نظام موحد ومتكامل، وهذا بغرض مراقبة تدفق البيانات والمعلومات بين تلك الأنظمة بشكل دقيق، إضافة إلى التنسيق بين مختلف الأنشطة، وبالتالي ربط هذا النظام بالهدف العام المحدد والمسطر من طرف المنظمة من أجل تحقيقه.

3.1.خصائص الذكاء الاقتصادي: يهتم الذكاء الاقتصادي بدراسة التفاعل التكتيكي والاستراتيجي بين كافة مستويات النشاط المعنية به انطلاقا بداية من القاعدة (المستوى الداخلي للمؤسسة)، مرورا بالمستويات الوسيطة (الجماعات المحلية)، وصولا إلى المستويات الوطنية (الاستراتيجيات المعتمدة لدى مراكز اتخاذ القرار في الدولة)، ثم المستويات المتعددة الجنسيات (المجمعات المتعددة الجنسيات) أو الدولية (استراتيجيات التأثير الخاصة بكل دولة). ومن بين الخصائص الرئيسية نذكر مايلي: (http://bbekhti.online.fr/trv_pdf/TIC.pdf)

- الاستخدام الاستراتيجي والتكتيكي للمعلومة ذات المزايا التنافسية في اتخاذ القرارات.
- وجود إدارة قوية لتنسيق جهود الأعوان الاقتصاديين.
- وجود علاقات قوية بين المؤسسات والجامعات والإدارات المركزية والمحلية.
- تشكيل جماعات الضغط والتأثير.
- إدماج المعارف العلمية، التقنية، الاقتصادية، القانونية والجيوسياسية.
- السرية في نشر المعلومات والحصول عليها بطريقة شرعية.

4.1.مراحل الذكاء الاقتصادي: تظهر أهمية المعلومة في سرعة الحصول عليها من أجل استخدامها واستغلالها، ومنه فالذكاء الاقتصادي يمر بالمراحل: تحديد الحاجة للمعلومة، حيازة المعلومة، معالجتها، بثها، ومن ثم استعمالها، وفيما يلي يتم التطرق لها بالشرح: (http://www.trcsr.com/detail.php?id=7)

- **تحديد الحاجة للمعلومة:** وتعني تحديد المعلومات التي نرغب في الحصول عليها، وهو ما يتطلب من المتخصصين في الذكاء الاقتصادي معرفة جيدة بتنظيم المنظمة.
- **جمع المعلومة:** بمجرد تحديد الحاجة للمعلومة، يتم اختيار أشكال للبحث عن هذه المعلومة، حيث أن كل مستويات المنظمة تتطلب معلومات محددة ودقيقة، الأمر الذي يتطلب تحديد مصادر إيجاد المعلومة، وهذه المصادر تتمثل في:
  - **المصادر الرسمية:** وتتمثل في كل من الصحافة، الكتب، وسائل الإعلام، قواعد المعطيات، والأقراص المضغوطة، مصادر المعلومات الرسمية.

- **مصادر غير رسمية**: أهم مميزات هذا النوع من المصادر أنها تتطلب مجهودا شخصيا من أجل جمعها، ومن بين هذه المصادر: السوق والمنافسين للمنظمة، العلاقات الشخصية، المنتديات والمعارض، البيئة الداخلية للمنظمة.

إن تطوير ممارسة الذكاء الاقتصادي يفرض على كل المؤسسات مضاعفة تدابير الحذر فيما يخص حماية إرثها المعلوماتي عن طريق معرفة واستعمال كل المصادر القانونية المتاحة لهذا الغرض وتسخير كل الوسائل البشرية، المعلوماتية والتنظيمية. (بول جامبل، جون بلاكويل،2002)

- **معالجة المعلومة**: هي خطوة مهمة جدا بالنسبة للذكاء الاقتصادي، فمعاجلة المعلومة تعتمد أساسا على قيمتها بالنسبة للمنظمة على المدى المتوسط والطويل، خاصة إذا تعلق الأمر بالقرارات الإستراتيجية والحساسة. ويقصد بمعالجة المعلومات تجميع كافة البيانات (التي تتحول إلى معطيات بعد المعالجة) أو المعطيات في حد ذاتها المحصل عليها، من أجل تحليلها بشكل متجانس، وتعتبر ترجمة المعلومة خطوة أساسية لإجراء المعالجة، فهي تعطي صورة واضحة تساعد في الغرض المنوط بها. وقيمة المعلومة قد تتأثر بعدة عوامل ممكن أن تؤدي إلى الفهم الخاطئ للمعلومة وتفسيرها وبالتالي الخطأ في اتخاذ القرار، وأهم الأسباب هي كثرة المعطيات ومدى مصداقيتها، وهو ما يتطلب القيام بالعمليات التالية: تقييم البيانات أو المعطيات المتحصل عليها، استخراج المعطيات ذات الجدوى من غيرها بالنسبة للمنظمة ووضعيتها، تحليل المعطيات، وتحويلها إلى شكل مناسب.
- **بث المعلومة من أجل اتخاذ القرار**: هذه الخطوة هي نتيجة لكل المراحل التي تسبقها، حيث يتم طرح المعلومة واستخدامها في المنظمة بما يساهم في خلق القيمة المضافة. إن بث المعلومة يعتبر بمثابة أوامر بتنفيذ خطوات ومراحل مهمة بعدها، إذا تعتبر كمفتاح لعمليات وإجراءات تلها تتم بدقة وجودة عالية من أجل الوصول إلى الهدف وتحقيق الغرض، وتبين التغذية الراجعة ما إذا كانت المعلومة قد أدت إلى تلبية رغبة المستعمل أم لا. ويجب التأكيد على الاحتفاظ ببعض المعلومات السرية والإستراتيجية وحمايتها.

2. تكنولوجيات الإعلام والاتصال: إن لأي تقنية تكنولوجية طبيعة اقتحامية، فهي تقتحم المجتمعات سواء كانت مطلوبة أو غير مطلوبة، مرغوبة أو غير مرغوب فيها، وذلك لما تقدمه من سلع جديدة أو بما تولده من حاجة إلى السلع الجديدة أو الخدمات فتطور ذاكرة المنظمة يتم من خلال نقل وتخزين المعلومات وتوريثها للأجيال باستخدام أساليب ووسائل تكنولوجية مختلفة وتلعب تكنولوجيا المعلومات والاتصالات دورا أساسيا في تكوين البنى التحتية الداعمة لعمليات الذكاء الاقتصادي، لكن رغم ما تقدمه من مزايا، لديها بعض المخاطر التي يجب على المنظمات الاحتراز منها، لكن قبل ذلك فيما تتمثل تكنولوجيات الإعلام والاتصال.

1.2. تعريف تكنولوجيا الإعلام والاتصال: تلك التكنولوجية المتولدة نتيجة التقارب أو التلاحم التكنولوجي بين تكنولوجية معالجة المعلومات (المعلوماتية) وتكنولوجية الاتصال (أقمار صناعية، فاكس، هاتف، شبكات ...إلخ) بغرض جمع، تخزين، معالجة وبث المعلومات سواء أكانت في شكل صوتي، رموز، أشكال، رسوم، نصوص أو صور. وبهذا يمكن التعبير عن تكنولوجية المعلومات بالعلاقة التالية: (B .Martinet,2001)

تكنولوجية المعلومات = الحاسوب + الاتصال

لهذا نجد أن مصطلح تكنولوجية المعلومات اقترن بهذه الأنواع من التكنولوجيا، فنجد مصطلح تكنولوجية المعلومات (الإعلام) والاتصال (**TIC**)*، أو بمصطلح آخر يشير أكثر إلى الديناميكية التي يعرفها هذا القطاع من ابتكارات بـ: تكنولوجية المعلومات (الإعلام) والاتصال الحديثة (**NTIC**)**، وذلك للدلالة أكثر على طبيعة هذه التكنولوجية المتجددة و المتطورة.

2.2.آثار إستخدام تكنولوجية المعلومات في المنظمة: رغم ما تقدمه تكنولوجية المعلومات من مزايا إلا أنه لا يجب النظر إليها على أنها خير خالص بل على العكس من ذلك في بعض الجوانب، فهي وسيلة لخرق حرمة الأشخاص والتنظيمات، عن طريق الدخول في ملفاتهم الخاصة بهم ومعرفة أدق التفاصيل عن حياتهم الخاصة، وهذه الاختراقات قد تطال في بعض الأحيان حتى الرؤساء والشخصيات البارزة، فهي قد تمثل تهديد لأمن المنظمات فضلا عن تدشينها نوع جديد من الحروب هي حروب المعلوماتية، حيث ظهر نوع جديد من الجرائم هي جرائم المعلوماتية.

ومع الانتشار الكبير والشديد لشبكات المعلومات والأعداد المتزايدة لمستخدميها أصبحت مسألة الأمن المعلوماتي قضية بذاتها، تشكل أحد أبرز التحديات التي يواجهها الأفراد والمنظمات على حد سواء في عصر المعلومات.

3.2. حرب المعلومات: تعرف حرب المعلومات أنها: " الصراع (التنافس) من أجل السيطرة (التحكم) في المعلومة والتي تعتبر عنصر أساس للقوة والثورة في عالمنا المعاصر." (P. Guichardaz,1999)

كما تعرف كذلك أنها: " استخدام نظم المعلومات لاستغلال وتخريب وتدمير وتعطيل معلومات الخصم (المنافس) وعملياته المبينة على المعلومات ونظم المعلومات وشبكات الحاسب الآلي الخاصة به، وكذلك حماية ما لدي من كل ذلك من هجوم الخصم لإحراز السبق والتقدم على نظمه العسكرية والاقتصادية، وليس من الضروري أن تشب تلك الحرب بسبب عداء تقليدي، بل قد تنشب مع منافس تجاري أو اقتصادي أو خصم ثقافي. "

فحرب المعلومات هي تلك التي تدور رحاها من خلال الشبكات المعلوماتية، إذ لا تعترف بالحدود والزمان ولا حتى القوانين والتشريعات إذ تقف عاجزة أمامها. هذا و تأخذ هذه الحرب ثلاث مستويات:

- **حرب المعلومات الشخصية:** التي يكون فيها الهجوم على خصوصية الأفراد وكذا العبث بملفاتهم والتصنت عليهم؛
- **حرب المعلومات بين التنظيمات (المؤسسات):** هي التي تدور ضمن إطار المنافسة أكثر من العداء إلا أنها ليست بالشريفة بأي معيار في كثير من الحالات؛
- **حرب المعلومات الدولية (العالمية):** التي تكون بين الدول وبعضها البعض، أو قد تشنها القوى الاقتصادية العالمية ضد بلدان بعينها.وتمتاز حرب المعلومات عن الحروب الكلاسيكية بـ: (P. Guichardaz,1999)

قلة تكلفة الدخول فيها، عدم وجود حدود مادية لها، فحدود حرب المعلوماتية هي الشبكات، المعلومات وتشويهها هي الأساس في الصراع المعلوماتي، صعوبة معرفة مصدر الهجوم، وما هي دوافعه والأدوات المتوفرة

لدى صاحبه، الخسائر في الحرب الكلاسيكية تكون تدميرية تشمل الجانب الاقتصادي والإنساني على حد سواء، أما حرب المعلومات فإنها تحدث خسائر مادية اقتصادية، كارثية، في حين أن الخسائر البشرية في العادة تكون غير مباشرة ومحدودة جدًا.

ثانيا: أمن (حماية) المعلومات والمخاطر التي تعترضها

تشكل المعلومات اليوم البيئة التحتية للمنظمات التي تمكنها من أداء مهامها، إذ أن نوع المعلومات وكميتها وطريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة وعليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، لذا فإن المشكلة التي يجب أخذها بالحسبان هي توفير الحماية اللازمة للمعلومات وإبعادها عن الاستخدام غير المشروع لها.

1. **مفهوم أمن المعلومات**: أمن المعلومات هو توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، وهو الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. هناك العديد من التعريفات لموضوع أمن المعلومات أهمها:

أمن المعلومات: " مفهوم يتسع ليشمل الإجراءات والتدابير الوقائية المستخدمة في المجالين الإداري والفني لحماية المصادر (من أجهزة وبرمجيات وشبكات وقواعد بيانات وأفراد) من التجاوزات والتدخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة في إدارة هذه المصادر." (http://www.saidder.jeeran.com/amn.htm)

وهو أيضا: " مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال." (الجواد دلال، 2008)

وهناك من يعرفه بأنه:" الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضياع والتلف أو من مخاطر الاستخدام غير الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية." (الجواد دلال، 2008) كما عرّف بأنه مجموعة من التدابير الوقائية المستخدمة في المجالين الإداري والفني لحماية مصادر البيانات، من أجهزة وبرمجيات وبيانات، من التجاوزات أو التدخلات غير المشروعة التي تقع عن طريق الصدفة، أو عمدا عن طريق التسلسل، أو الإجراءات الخاطئة المستخدمة من قبل إدارة المصادر المعلوماتية، فضلا عن إجراءات مواجهة الأخطار الناتجة عن الكوارث الطبيعية المحتملة التي قد تؤدي إلى فقدان بعض المصادر كلا أو جزءا، ومن ثم التأثير على نوع ومستوى المعلومة المقدمة.

مما سبق يمكن تعريف الأمن المعلوماتي بأنه ذلك الحقل الذي يهتم بدراسة طرق حماية البيانات المخزونة في أجهزة الحاسوب، إضافة إلى الأجهزة الملحقة وشبكات الاتصالات، والتصدي للمحاولات الرامية إلى الدخول غير المشروع إلى قواعد البيانات المخزونة، أو تلك التي ترمي إلى نقل أو تغيير أو تخريب المخزون المعلوماتي لهذه القواعد.

2. **مراحل تطور مفهوم الأمن المعلوماتي (حماية المعلومات):** مرّ مفهوم الأمن المعلوماتي بمراحل عدة كما يلي:

- في الستينات كانت الحواسيب هي كل ما يشغل العاملين في أقسام المعلومات، وكان همهم هو كيفية تنفيذ البرامج ولم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة، وكان مفهوم الأمنية يدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع الغرباء الخارجيين من التلاعب في الأجهزة، لذلك ظهر مصطلح أمن الحواسيب والذي يعني حماية الحواسيب وقواعد البيانات، ونتيجة للتوسع في استخدام أجهزة الحاسوب وما تؤديه من منافع تتعلق بالمعالجة للأحجام الكبيرة من البيانات، تغير الاهتمام ليمثل السيطرة على البيانات وحمايتها.
- في السبعينات تم الانتقال إلى مفهوم أمن البيانات ورافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات إضافة إلى وضع إجراءات الحماية لمواقع الحواسيب من الكوارث واعتماد خطط لتخزين نسخ إضافية من البيانات والبرمجيات بعيدا عن موقع الحاسوب.
- وفي مرحلة الثمانينات والتسعينات ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات، كل هذا أدى إلى الانتقال من مفهوم أمن البيانات إلى أمن المعلومات، و أصبح من الضروري المحافظة على المعلومات وتكاملها وتوفرها ودرجة موثوقيتها، حيث أن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة وتقلص اختراق المعلومات والتلاعب بها، و كانت شركة **IBM** الأمريكية أول من وضع تعريف لأمن المعلومات، وكانت تركز على حماية البيانات من حوادث التزوير، والتدمير أو الدخول غير المشروع على قواعد البيانات، وأشارت الشركة إلى أنّ توفير حماية تامة للبيانات لا يمكن تحقيقه، لكن يمكن تحقيق مستوى مناسب ومقبول من الحماية.

3. **أبعاد حماية المعلومات:** يجب ضمان توفر العناصر التالية لأية معلومات يراد توفير الحماية الكافية لها: (Arnason , Sigurjon Thor & Willett, Keith D. ,2008)

- **السرية أو الموثوقية Confidentiality:** وتعني التأكد من أن المعلومات لا تكشف، ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- **سلامة المحتوى Integrity:** التأكد من إن محتوى المعلومات صحيح، ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغييره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل خارجي غير مشروع.
- **استمرارية توفر المعلومات Availability:** التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وان مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.
- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به Non-repudiation:** ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها إنكار أنه هو الذي قام بهذا التصرف، بحيث تتوفر قدرة إثبات أن تصرفا ما قد تم من شخص ما في وقت معين.

4. **أنواع التهديدات الأمنية للمعلومات:**بشكل عام هناك أربعة أنواع من التهديدات الأمنية للمعلومات: (http://www.titmag.net.ye/modules.php?name)

- **الانقطاع (الحرمان من الخدمة):** وتشمل أي تأخير أو تعطل العمليات التجارية العادية وتدفق البيانات بين الإدارات المختلفة في المنظمة، مثل مشاكل فيروسات الحاسوب المستمرة وإزالته،ا وهي مشكلة شائعة جداً اليوم.
- **المعترض (الكاشف):** هي أي عملية دخول غير مصرح به للمعلومات، والتي قد تكون أو تؤدي إلى الاستخدام غير المشروع للبيانات، من خلال تصفح الملفات المخزنة ومراقبة شبكة الهاتف أو التحويلات. فهناك المئات من أساليب الوصول غير المصرح بها لأنظمة الكمبيوتر عبر الشبكة خاصة إذا كانت هذه الشبكة هي شبكة الإنترنت العامة، فأي شخص في العالم يمكنه الوصول إليها بسهولة، مما يتيح الوصول إلى البيانات الحساسة كثيرا أو المعرفة اللازمة للحصول على نظم المعلومات فيها، أي سهولة التجسس والاطلاع عليها.
- **التعديل:** العبث بمجرد الوصول للمعلومات ويتم تحقيقه من خلال تغيير في البرامج أو الأجهزة أو تعديل في ضوابط البيانات نفسها، فلابدّ من التفكير في العواقب إذا تمكن متسلل من تغير المبالغ المستحقة على الشركة من قبل الموردين الخارجيين. أو التعديل في جميع الفواتير الخاصة بالعملاء فإن ذلك سوف يؤدي إلى الاعتماد على بيانات غير صحيحة وتعطيل التدفق النقدي خاصة إذا تأخر الكشف المبكر لما قام به المتسلل من تعديل في البيانات التي تعتمد عليها المنظمة.
- **التزوير والتحوير والتلفيق:** هو تعديل بطريقة ما في البيانات لصالح المخترق أو من يعمل لصالحه مما يسبب مشاكل للمنظمة وبالتالي فإنه يمكن أن ينطوي على التعديل بمهارة بإضافة بيانات أو تعرض لنظام الحوسبة مثل تعديل في المعاملات أو إدخال ملفات إضافية على قاعدة بيانات.

5. الأخطار التي يمكن أن تتعرض لها أنظمة المعلومات الحديثة:

تعتبر المخاطر المقصودة أشد خطرا على أداء فعالية النظم وتزداد تلك الخطورة في النظم الإلكترونية. وتكمن خطورة مشاكل أمن المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية، أو تخريبها بالكامل مما يؤدي إلى تعطيل الخدمات الحيوية للمنشأة، أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الاطلاع والتصنت على المعلومات السرية أو تغييرها إلى خسائر مادية أو معنوية كبيرة، وتصنّف المخاطر من وجهات نظر مختلفة إلى: (http://www.cybrarians.info/journal/no3/digitize.htm)

1.5. من حيث مصدرها: تتفرع إلى مصادر داخلية وأخرى خارجية:

- **مخاطر داخلية:**حيث يعتبر موظفي المنظمات هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية وذلك لأن موظفي المنظمات على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق لدى المنظمة، ومعرفة نقاط القوة والضعف ونقاط القصور لهذا النظام ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، ولذلك فإن موظفي المنظمة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها.
- **مخاطر خارجية:** وتتمثل في أشخاص خارج المنظمة ليس لهم علاقة مباشرة بها مثل قراصنة المعلومات

والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام، بهدف الحصول على معلومات سرية عن المنظمة، أو قد تتمثل في كوارث طبيعية مثل الزلزال والبراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام في المنظمة.

2.5. من حيث المتسبب بها: وتصنف إلى:

- **مخاطر ناتجة عن العنصر البشري**: وهي التي يمكن أن تحدث أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام، أو في عمليات تحديد الصلاحيات للمستخدمين، وتشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن و سلامة نظم المعلومات في المنظمات.
- **مخاطر ناتجة عن العنصر غير البشري:** وهذه تشمل الزلازل والعواصف والفيضانات والأعاصير والمشاكل المتعلقة بأعطال التيار الكهربائي والحرائق، إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف والتبريد وغيرها ، وتؤدي هذه الأخطار إلى تعطل عمل هذه التجهيزات وتوقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة واسترداد البرمجيات وقواعد البيانات.

3.5. من حيث أساس العمدية (القصد): وتصنف بدورها إلى:

- مخاطر ناتجة عن تصرفات متعمدة مقصودة.
- مخاطر ناتجة عن تصرفات غير متعمدة غير مقصودة.

4.5. من حيث الآثار الناتجة عنها:إلى:

- مخاطر ينتج عنها أضرار مادية.
- مخاطر فنية ومنطقية.

5.5. المخاطر على أساس علاقتها بمراحل النظام: فقد تكون:

- مخاطر المدخلات - مخاطر التشغيل. - مخاطر المخرجات.

ثالثا: طرق حماية المعلومات ودور المورد البشري

تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة والصعبة والتي تتطلب من إدارة المنظمة الكثير من الوقت والجهد والموارد المالية وذلك للأسباب التالية: (الجواد دلال، 2008)

- العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات.
- توزع الموارد الحاسوبية على العديد من المواقع التي يمكن أن تكون أيضا متباعدة.
- وجود التجهيزات الحاسوبية في عهدة أفراد عديدين في المنظمة وأحيانا خارجها.
- صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية.
- التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة بعد فترة وجيزة من استخدامها.
- التأخر في اكتشاف الجرائم الالكترونية، لا يتيح للمنظمة إمكانية التعلم من التجربة والخبرة المتاحة.
- تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها.

1. **العناصر الأساسية لنظام الأمن المعلوماتي:** من الأفضل تصميم نظام للرقابة ضمن عملية تطوير نظام المعلومات، يركز هذا النظام على مفهوم الوقاية من الأخطار، وأن يشمل النظام الأمني الفعال جميع العناصر ذات الصلة بنظام المعلومات المحوسبة ويمكن تحديدها في ما يلي (www.ao-academy.com/**docs**/45D0~1.**DOC**)

1.1. منظومة الأجهزة الإلكترونية وملحقاتها: إن أجهزة الحواسيب تتطور بشكل بالمقابل هناك تتطور في مجال السبل المستخدمة لاختراقها مما يتطلب تطوير القابليات والمهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب والعبث المقصود في الأجهزة أو غير المقصود.

2.1. الأفراد العاملين في أقسام المعلومات: يلعب الفرد دورا أساسيا ومهما في مجال أمن المعلومات والحواسيب وله تأثير فعال في أداء عمل الحواسيب بجانبيه الإيجابي والسلبي ، فهو عامل مؤثر في حماية الحواسيب والمعلومات ولكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة وسرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير، إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين ووضع تعليمات واضحة لاختيارهم، وذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد، إضافة إلى وضع الخطط لزيادة الحس الأمني والحصانة من التخريب، كما يتطلب الأمر المراجعة الدورية للتدقيق في شخصية وسلوك للأفراد العاملين من وقت لآخر وربما يتم تغيير مواقع عملهم ومحاولة عدم احتكار المهام على موظفين محدّدين.

3.1. البرمجيات المستخدمة في تشغيل النظام: تعتبر البرمجيات من المكونات غير المادية وعنصر أساسي في نجاح استخدام النظام، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية ويمكن أن تحقق حماية للبرامج وطرق حفظ كلمات السر وطريقة إدارة نظام التشغيل وأنظمة الاتصالات، فأمن البرمجيات يتطلب أن يؤخذ هذا الأمر بعين الاعتبار عند تصميم النظام وكتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها وتمنع أي شخص من إمكانية التلاعب والدخول إلى النظام وذلك من خلال تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها، ومحاولة التمييز بين اللذين يحق لهم الإطلاع و الذين لا يحق لهم، وأيضا حسب كلمات السر الموضوعة، وهناك أسلوبان للتمييز إما عن طريق البرمجيات أو استخدام الأجهزة المشفرة.

4.1. شبكة تناقل المعلومات: تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الاتصالات، لأنها سهلت عملية التراسل بين الحواسيب وتبادل واستخدام الملفات، ولكن من جهة أخرى أتاحت عملية سرقة المعلومات أو تدميرها سواء من الداخل كاستخدام الفيروسات، أو من خلال الدخول عبر منظومات الاتصال المختلفة، لذلك لا بد من وضع إجراءات حماية وضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه الأنظمة وتوفير الأجهزة الخاصة بالفحص، كما أن نظم التشغيل المستخدمة والمسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة وقدرة عالية على الكشف عن التسلل إلى الشبكة، وذلك من خلال تصميم نظم محمية بإقفال معقد أو عن طريق المشفرات وربطها بخطوط الاتصال، والتي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة ومعدات لغرض تشفير تناقل المعلومات أو الملفات.

5.1. مواقع منظومة الأجهزة الإلكترونية وملحقاتها: يجب أن تعطى أهمية للمواقع والأبنية التي تحوي أجهزة الحواسيب وملحقاتها، وحسب طبيعة الأنظمة والتطبيقات المستخدمة يتم اتخاذ الإجراءات الاحترازية لحماية

الموقع وتحصينه من أي تخريب أو سطو وحمايته من الحريق أو تسرب المياه والفيضانات، ومحاولة إدامة مصدر القدرة الكهربائية وانتظامها، وتحديد أساليب وإجراءات التفتيش والتحقق من هوية الأفراد الداخلين والخارجين من الموقع ووضع سجل لذلك.

خاتمة:

تعمل المنظمات في ظل تبني الذكاء الاقتصادي على تعبئة وإشراك العاملين في المنظمة على حماية موروثها، والحفاظ على أمن معلوماتها لتتمكن من السيطرة عليها والتحكم فيها، وبما أن أغلب الأخطار الشائعة تكمن في استعمال وسائل وتقنيات تكنولوجيا الإعلام والاتصال فإنها ملزمة بالعمل على تحسين المواقف والولاء للمنظمة من طرف أفرادها وتطوير سياسة الموارد البشرية بها، من خلال فرض ثقافة الذكاء الاقتصادي في المنظمة والعمل على:

- خلق ثقافة المشاركة والحماية للمعلومات، وجها لوجه مع العالم الخارجي،لأن العمل بالذكاء الاقتصادي يرتكز على التكتم والمحافظة على أسرار عمل المؤسسة والمعلومات المتعلقة بالعمل، ما يتيح للمؤسسة فرصة الابتعاد عن المخاطر.
- كذلك زيادة الوعي بالأمن لدى الأفراد المستخدمين والمتعاملين مع نظم المعلومات، والتعرف على أهمية وأهداف أمن المعلومات والممارسات الأحسن لحماية موروث المنظمة.
- تكوين الموارد البشرية، وهو يعتبر مسألة جد حساسة، حيث أصبحت تتكثف البحوث والدراسات حول هذه الأخيرة، لما لها من مردودية وأداء على جميع الأصعدة لاسيما الاقتصادية منها، لذلك يتم السعي للقيام بملتقيات وأيام تكوينية حول تطبيقات الذكاء الاقتصادي ووسائله
- دعم الوعي بأمن المعلومات بالتعرف علي المخاطر الكامنة وتطوير استخدام نظم المعلومات بطريقة ملائمة.
- تبني إستراتيجية لتأهيل أفراد المنظمة على أمن المعلومات والتعامل معه باعتباره ثقافة وسلوك.
- تحفيز الأفراد ماديا ومعنويا لتعزيز الولاء التنظيمي لديهم.ومحاولة معرفة المبادرات المبدعة و المجددة في المنظمة.
- يجب أن تتضمن برامج التعليم والتدريب على موضوعات التوعية بأمن المعلومات التي توجه لفئات المستخدمين ورجال الإدارة علي كافة مستوياتهم الإدارية وأخصائيي الصيانة ومديري نظم المعلومات (مديري البرمجيات، مديري التشغيل، مديري الشبكات) ومديري تطوير البرمجيات والنظم، والمديرين المكلفين بأمن نظم المعلومات ومراجعي نظم المعلومات.
- الحذر من أن تكون المعلومة المتحصل عليها كذبة أو إشاعة، أو اختلاقا من الخيال من طرف الأشخاص والمنظمات المنافسة الممونة بالمعلومات غير الرسمية، وذلك عند القيام بتغيير أو تعديل قرارات المنظمة المستقبلة للمعلومات غير الرسمية عن منافسيها، قبل أن تقع في الفخ المنصوب إليها من خلال ما يسمى بالتعتيم المعلوماتي، والذي يعني تسريب بعض المؤسسات عن معلومات خاطئة حول خطتها الاقتصادية المتبعة، قصد إيقاع المنافس في المتاهات.

الاحالات و المراجع

1- مسعود ديلمي، الذكاء الاقتصادي والعمل الضغطي:الحروب الخفية، مدارات، جريدة القدس، (العدد6061، الخميس 27 نوفمبر2008)، ص 15.

2- بول جامبل، جون بلاكويل، إدارة المعلومات، (دار الفاروق، مصر،2003)، ص16

3- الجواد دلال الفتال، أمن المعلومات، (دار اليازوري، عمّان2008)، ص 14.

4- إبراهيم بختي، تكنولوجيا ونظم المعلومات في المؤسسات الصغيرة والمتوسط، على الرابط

http://bbekhti.online.fr/trv_pdf/TIC.pdf

5- يحي اليحياوي محاضرات على الرابط

http://www.trcsr.com/detail.php?id=7

6- Arnason , Sigurjon Thor & Willett, Keith D. ,2008, How to Achieve 27001 Certification An Example of Applied Compliance Management, (Taylor& Francis Group LLC. New York, USA). P3.

7- B .Martinet, L'intelligence économique, (deuxième édition , Editions d'organisation, Paris, 2001), P4

8- P. Guichardaz, P.Lointier et P. Rosé, **L'info Guerre**, (Dunod, Paris, France, 1999), p 21

9- .www.ces.fr/rapport/rapsec/R5052710.pdf P3.

10- http://www.medefparis.fr/Livre_Blanc.pdf. P 9

11- www.ao-academy.com/docs/45D0~1.DOC .PP137-139.

12- http://www.saidder.jeeran.com/amn.htm

13- http://www.saidder.jeeran.com/amn.htm

14- http://www.titmag.net.ye/modules.php?name

15- http://www.cybrarians.info/journal/no3/digitize.htm

* TIC = **T**echnologies de l'**I**nformation et la **C**ommunication.
** NTIC = **N**ouvelles **T**echnologies de l'**I**nformation et la **C**ommunication