دور التأمين في تسيير مخاطر تكنولوجيا المعلومات

The role of insurance in managing information technology risks

تسوري بن تسوري بهية، جامعة لونيسي علي البليدة 2 (الجزائر)، b.tsouribentsouri@univ-blida2.dz

تاريخ الاستلام: 2021/01/01 تاريخ القبول: 2021/02/16 تاريخ النشر: 2021/03/27

ملخص:

تهدف هذه الدراسة إلى التعرف على المخاطر التي تهدد امن المعلومات في فعاليتها، دقتها وحتى تواجدها. وبما أن العصر الحالي هو عصر التكنولوجيا كان من الضروري حماية المعلومات المتداولة عبرها من كل هذه المخاطر بإتباع بعض الإجراءات الوقائية التي يمكن أن تحميها. بالإضافة إلى ذلك هناك بعض تقنيات التعامل مع المخاطر التي تهدد تكنولوجيا المعلومات قبل، أثناء أو بعد وقوعها والتي تتبعها المنظمات في تسيير مخاطرها بالاحتفاظ بها أو التعامل معها أو نقلها إلى جهات أخرى اقدر منها على تحملها، من بينها التأمين، وسنحاول تسليط الضوء على هذه العملية مبرزين المخاطر القابلة للتأمين منها.

كلمات مفتاحية: مخاطر، تأمين، معلومات، تكنولوجيا.

تصنيفات JEL : **G22**

Abstract:

This study aims to identify the risks that threaten the security of information. It was necessary to protect the information through which all these risks were transmitted by following certain preventive measures that could be protected even. there are some techniques to deal with the risks that threaten information technology before, during or after the occurrence of theorganizations to manage their risk by keeping them,dealing with them or transferring them to others. Among these techniques there is insurance.

Keywords: Risk; insurance; information; technology**.**

Jel Classification Codes: G22

1. مقدمة:

المعلومة كلمة صغيرة من حيث عدد حروفها، بسيطة في معناها، إلا أنها ضخمة بما يمكن أن تكوّنه من نظم، فهي تعتبر المادة الأولية لنظام أصبح من الصعب الاستغناء عليه في جميع المجالات والمنظمات، نظام بات يقترن اسمه مع الوسائل الحديثة لتكنولوجيا المعلومات ويعد من أهم تطبيقاتها، هذا النظام هو نظام المعلومات.

فالمعلومات المتداولة عبر تكنولوجيا المعلومات تترصّدها مخاطر عديدة ومختلفة قد تبطل مفعولها وأهميتها وتهدد سلامتها وقد تلغي وجودها تماما ولهذا كان من الضرورة حمايتها وذلك من خلال ما يعرف بأمن المعلومات أو التقليل من حدة الأضرار المترتبة عن الأخطار التي تتربص بها من خلال تقنيات مختلفة.

إشكالية الدراسة:

على ضوء ما سبق يمكنا طرح الإشكالية التالية:

إلى أي مدى يمكن التأمين على المخاطر الناتجة عن تكنولوجيا المعلومات ؟

فرضيات الدراسة:

وللإجابة عن الإشكالية المطروحة قمنا بصياغة الفرضيات التي يمكن إثباتها أو نفيها من خلال محتوى البحث وتتمثل فيما يلي:

- هناك عدة مخاطر تهدد المنظمات في امن معلوماتها إلا أنها تستطيع تفادي الكثير منها بإتباع إجراءات وقائية معينة.
- تفادي المخاطر التي تهدد تكنولوجيا المعلومات بنسبة 100% أمر يستحيل الوصول إليه ولذا وجب على المنظمات باختلاف أنشطتها إتباع طرق أو تقنيات معينة لإدارتها.
- يعد التامين واحد من التقنيات التي تلجا إليها المنظمات في تسيير بعض مخاطرها والتي تكون قابلة للتامين.

أهداف الدراسة:

تتجلى أهداف الدراسة في:

- التعرف على المخاطر الناتجة عن تكنولوجيا المعلومات.
- التعرف على الإجراءات الوقائية لتفادي المخاطر التي تهدد المنظمات في أمن معلوماتها.
- التعرف على كيفية إدارة المخاطر.
- تحديد قابلية المخاطر الناتجة عن تكنولوجيا المعلومات للتأمين.

منهجية الدراسة:

للإجابة عن التساؤل المحوري والأسئلة الفرعية واختبار مدى صحة الفرضيات المطروحة اعتمدنا على المنهج الوصفي باعتباره المنهج الأكثر ملائمة لطبيعة الموضوع من خلال سردنا لمختلف المفاهيم المتعلقة بالموضوع.

2. مفاهيم أساسية حول مخاطر تكنولوجيا المعلومات:

لقد تزايدت أهمية المعلومات في الآونة الأخيرة حتى باتت أهم سلعة تركز عليها كل المؤسسات الاقتصادية، ونظرا لهذه الأهمية كان من الضروري بما كان إيجاد الوسائل أو الأدوات الكفيلة بجمعها من مصادرها المختلفة وتخزينها لإظهارها عند الحاجة وكذا معالجتها لتصبح أكثر نفعا داخل المنظمة، وقد تسنى لها ذلك من خلال ما نسميه بتكنولوجيا المعلومات.

2-1- مفهوم تكنولوجيا المعلومات:

تكنولوجيا المعلومات تتكون من شقين شق خاص بالتكنولوجيا، والثاني خاص بالمعلومات، وعليه سنقوم الآن بتعريف التكنولوجيا ثم المعلومات لنصل في الأخير إلى تعريف تكنولوجيا المعلومات.

2-1-1- تعريف التكنولوجيا:

تكنولوجيا هي تعريب لكلمة Technology اليونانية، ويترجمها البعض إلى العربية على أنها "تقنية" بينما يراها البعض الآخر أنها "تقانة" (**الكساسبة، 2011، صفحة 33**)

تعني كلمة التكنولوجيا" Technology" دراسة الوسائل الفنية، وهي كلمة مؤلفة من مقطعين: Techno تعني تقنيات، وlogy تعني علم أو دراسة ، فيصبح معناها علم التقنيات أو علم دراسة التقنيات (**الدقس، 2005، صفحة 43**)

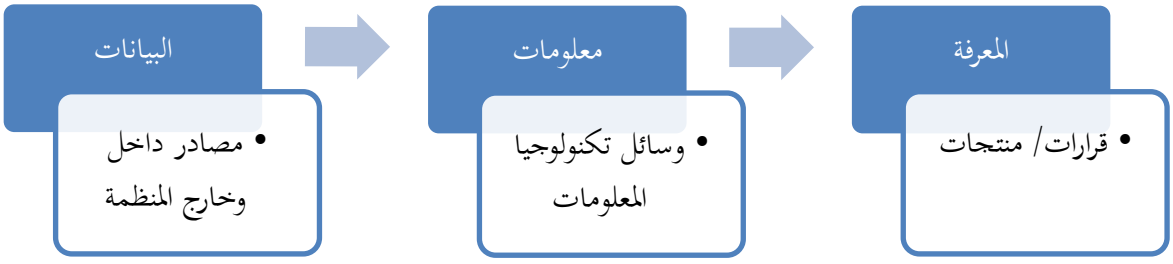
2-1-2- تعريف المعلومات:

اشتقت كلمة المعلومات (informations) من الأصل اللاتيني الذي كان يعني تعليم المعرفة ونقلها، وفي فرنسا كانت تشير كلمة معلومات في العصور الوسطى إلى عمليات جمع المعلومات ونقلها وتوثيقها رسميا، وتشتق كل المعاني المعاصرة من الأصل اللاتيني الفرنسي.(**علوطي، 2008، صفحة 03**)

المعلومات عبارة عن البيانات التي تمت معالجتها بطريقة هادفة لتكون أساس لاتخاذ القرارات فهي وليدة البيانات التي تم جمعها عن موضوع معين وإذا ما تم إعادة تنظيمها وترتيبها ومعالجتها بشكل صحيح ومنظم ستعمل على تغيير أو تعديل الحالة المعرفية للإنسان وبالتالي سوف تؤثر في عملية اتخاذ القرار سواء بالنسبة للأفراد أو المنظمات أو المجتمعات. (**الجاسم، 2005، صفحة 11**)

ومن التعريف يتضح انه هناك علاقة بين البيانات والمعلومات والمعرفة و كما يوضحه الشكل التالي:

الشكل 01: علاقة المعلومات بالبيانات والمعرفة:



المصدر: من إعداد الباحثة بالاعتماد على: (**قنديلجي و الجناب، 2007، صفحة 31**)

2-1-3- تعريف تكنولوجيا المعلومات:

تكنولوجيا المعلومات هي 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. (**الشوابكة، 2011، صفحة 167**)

وبتعبير ابسط يمكن القول أن تكنولوجيا المعلومات هي عبارة عن مجموعة الوسائل التي تعمل على تخزين المعلومات و معالجتها بشكل دقيق في الوقت المناسب مختزلة بذلك تكلفة الوقت والجهد والمال.

2-2- نظام المعلومات:

تطورت نظم المعلومات خلال السنوات الأخيرة بشكل كبير جدا، وقد كان لظهور الحاسوب الدور الكبير في تطورها، وتعد هذه الأخيرة من أهم تطبيقات تكنولوجيا المعلومات.

2-2-1- تعريف نظام المعلومات

نظام المعلومات هو مجموعة من العناصر المختلفة التي تعمل على إنتاج واستغلال المعلومات اللازمة لتحسين تسيير المؤسسة، فالهدف منه هو توفير المعلومات الصحيحة والمناسبة وفي الوقت المناسب وللشخص المناسب من اجل اتخاذ القرارات المناسبة.(**Guilhon, 2004, p. 71**) .

ويعرف أيضا على أنه عبارة عن مجموعة الخطوات والإجراءات التي تتبع لتشغيل نظاماً لمعالجة البيانات لغاية توفير، وتوليد، وجمع، وتنظيم، وتخزين، واسترجاع المعلومات في مؤسسة ما أو أية جهة في المجتمع حول أنشطة أو ظروف خاصة، ويتم ذلك باستخدام مجموعة من المستلزمات، والموارد، والنظم، والأساليب الفنيّة. (**الدويكات، 2016**)

كما يعرف نظام المعلومات بأنه: " مجموعة متجانسة ومترابطة من الأعمال، العناصر والموارد تقوم بتجميع و تشغيل و إدارة ورقابة البيانات بغرض الإنتاج وتوصيل معلومات مفيدة لمستخدمي القرارات من خلال شبكة من خطوط القنوات الاتصال". (**بختي، 2008، صفحة 24**)

من التعريفين السابقين يمكن القول أن نظام المعلومات هو ذلك النظام الذي يمكن من خلاله الاستغلال الأمثل للمعلومات بالاستعانة بالعناصر المختلفة لتكنولوجيا المعلومات للوصول إلى اتخاذ القرارات السليمة.

2-2-2- العمليات اللازمة لتصميم نظام المعلومات:

أدى استخدام الحاسوب إلى ظهور ما يسمى بنظم المعلومات المسندة إلى الحاسوب، وتتضمن هذه النظم المكونات المادية والمكونات البرمجية لتهيئة مهام وأعمال النظام. ويتكون نظام المعلومات المسند إلى الحاسوب من مجموعة من الخطوات والمراحل والعمليات اللازمة لتصميمه وهي: (**العاني و جواد، 2008، صفحة 256،257**)

جمع البيانات ؛ تصنيف البيانات ؛ معالجة البيانات ؛ توليد المعلومات ؛ عرض المعلومات ؛ الاستفادة من المعلومات لصناعة القرارا.

2-2-3- امن المعلومات:

لقد نالت قضية امن المعلومات في الآونة الأخيرة اهتماما كبير من قبل مختلف شرائح المجتمعة باختلاف مستوياتهم، فالجميع بات اليوم يتعامل بوسائل الرقمنة التي تعتمد بدورها على المعلومات، فإذا تامين هذه الأخيرة تتوقف عليه مصالح الجميع، حيث يعرف امن المعلومات على انّه:

- وظيفة تهدف إلى حماية الموارد المحوسبة من الأخطار والتهديدات المقصودة وغير المقصودة التي يمكن أن تؤدي إلى عمليات غير مسموح بها مثل تعديل أو تخريب البيانات أو البرامج.(**أبو عطيوي، 2012، صفحة 27**)
- توفير المستوى المطلوب من الأمان لحماية البيئة المادية والبنية التحتية والحاسبات وخطوط الاتصالات وأيضا الموارد المعلوماتية ضد كل التهديدات التي تتعرض لها مهما كان نوعها. (**السبكي، 2010، صفحة 56**)
- مجموعة من الاستراتيجيات من استراتيجيات إدارة العمليات، والأدوات، والسياسات الضرورية لمنع، وكشف، وتوثيق، ومواجهة التهديدات على المعلومات الرقمية وغير الرقمية، وهذا يشمل حماية المعلومات من التعديل، والتعطيل، والتدمير، والتفتيش. (**أبو عجيب، 2020**)

من خلال التعريفين السابقين يمكن القول أن امن المعلومات هو عبارة عن حماية البيانات و المعلومات والبرامج وكذا كل التجهيزات المادية المستعملة في تكنولوجيا المعلومات والاتصال من المخاطر التي تهددها سواء كانت داخلية أو خارجية، مقصودة أو غير مقصودة.

2-3- المخاطر التي تهدد تكنولوجيا المعلومات في امن معلوماتها:

يعد الخطر تهديدا كبيرا يواجه المعلومات ويضرب بأمنها، من خلال هذا العنصر سنحاول تعريف الخطر، ثم تقسيماته المختلفة لننتقل في الأخير إلى تحديد أهم المخاطر التي تهدد تكنولوجيا المعلومات في امن معلوماتها.

2-3-1- تعريف الخطر:

- "الخطر هو الخوف من تجاوز الخسائر المادية الفعلية للخسائر المتوقعة نتيجة حادث مفاجئ" (احمد، دون سنة النشر، صفحة 17)

و يمكن القول أن الخطر ما هو إلا حدث قد يحدث في المستقبل نتيجة حادث مفاجئ، أي انه غير مؤكد الوقوع، وإذا وقع فانه يترتب عنه خسائر مالية و/أو معنوية.

وبمفهوم ابسط يمكن القول انه ينشأ الخطر عندما يكون هناك احتمال لأكثر من نتيجة والمحصلة النهائية غير معروفة.

2-3-2- أنواع الأخطار:

الجدول الموالي يلخص التصنيفات المختلفة للأخطار.

الجدول 1: أنواع الأخطار

<table>
<tr><td rowspan="5">الأخطار المعنوية والأخطار الاقتصادية:</td><td colspan="3">1- الأخطار المعنوية: هي أخطار لا تسبب ربحا أو خسارة بصورة مباشرة، ولكنها تسبب خسائر معنوية فقط كالأخطار النفسية الناجمة عن الصدمة، وهي أخطار غير قابل للتامين.</td></tr>
<tr><td rowspan="4">2- الأخطار الاقتصادية: وهي التي تؤثر على النواحي الاقتصادية والمالية للأشخاص وبالتالي ينتج عنها خسائر مالية آو اقتصادية مثل خطر الحريق، وهي قابلة للتامين.</td><td colspan="2">*أخطار المضاربة: وهي التي يكون فيها الربح أو الخسارة ممكنا مثل الاستثمار في العقار أو الأسهم.</td></tr>
<tr><td rowspan="3">*الأخطار البحتة (الصافية): هي الأخطار التي تتضمن فقط احتمال الخسارة أو عدم وقوع الخسارة، مثل الوفاة المبكر، حوادث العمل.</td><td>الأخطار الشخصية: هي التي يقع أثرها على الإنسان مباشرة وتؤثر في شخصه مثل الوفاة</td></tr>
<tr><td>أخطار الممتلكات: وهي التي تؤثر على الممتلكات سواء الثابتة أو المنقولة كالسرقة والضياع.</td></tr>
<tr><td>أخطار المسؤولية المدنية: وهي التي يتسبب في تحققها شخص معين وينتج عنها إصابة الغير بضرر مادي في شخصه و/أو ممتلكاته كالأخطاء المهنية للأطباء</td></tr>
<tr><td>الأخطار العامة والأخطار الخاص</td><td colspan="3">1- الأخطار العامة أو الأساسية: هي الأخطار التي تترتب عنها خسائر ليس السبب فيها الإنسان أو تصرفاته، وتلحق أضرارا لجماعات كبيرة من الأفراد ويصعب إرجاع نشأتها أو أثرها لفرد معين، كالأخطار التي تؤثر على اقتصاد بلد ما كالتضخم وأيضا الكوارث الطبيعية، وغالبا ما تتحاشى شركات التامين تأمينها إلا ضمن ظروف معينة كان تقوم بإعادة تأمينها.</td></tr>
</table>

	2- الأخطار الخاصة:هي الأخطار التي تؤثر على الفرد وليس على المجتمع بأكمله مثل الحريق منزل أو سرقة ويمكن أن تؤثر على المجتمع بطريقة غير مباشرة، وهي قابلة للتامين.
أخطار السكون وأخطار الحركة	**1- أخطار السكون**: هي تلك الأخطار التي تحدث حتى ولو كان الاقتصاد مستقرا تمام وتنشا عن التغير غير المنتظم لقوى الطبيعة كالزلازل والبراكين، هذا النوع من الأخطار يسبب خسائر وأضرار مادية ومعنوية للأفراد أو للمجتمع ككل وهي قابلة للتامين.
	2- أخطار الحركة: هي الأخطار التي تنتج عن التغيرات التي تصاحب التقلبات أو عدم الاستقرار الاقتصادي مثل التغيرات في مستوى الأسعار، هذه الأخطار عادة ما يؤثر تحققها على الفرد أو المجموعة دون أن يصل إلى حد إلحاق الخسائر على المجتمع ككل، وهي أخطار يصعب التنبؤ بها أو قياسها كميا وعليه فهي غير قابلة للتامين.

المصدر: من إعداد الباحثة.

2-3-3- المخاطر التي تهدد امن المعلومات:

تتعرض المعلومات المرقمنة في مختلف أشكالها إلى عدة مخاطر سواء عن بعد عبر الشبكات أو عن قرب ومن بين هذه المخاطر نجد: (**بامفلح، صفحة 06،05**)

- تعطل مكونات الحاسوب مثل الأقراص الصلبة على سبيل المثال؛
- إغلاق أجهزة الخادم serveur مما يؤدي إلى توقف الشبكة عن العمل؛
- تخريب الأجهزة سواء بقصد أو بدون قصد مما يؤدي إلى انقطاع الخدمة؛
- التشويش على الإشارات المنقولة عبر الكابلات؛
- مراقبة خطوط الهاتف والتجسس على مستخدمي الشبكة؛
- سرقة الأقراص المحملة عليها البيانات مما يؤدي إلى فقدان البيانات وتفشي الأسرار المتعلقة بالأشخاص و بالعمل؛
- تعطيل أحد الأشخاص لنظام الأمن الخاص بالشبكة أو كشفه لإجراءات الحماية المتبعة،

- تعرض المعلومات لبعض البرامج الخبيثة كالفيروسات سواء كانت فيروسات مزعجة فقط أم مدمرة مما يؤدي الى إتلاف البيانات أو فقدانها تماما؛
- إطلاع الأشخاص المصرح لهم باستخدام الشبكة على معلومات غير مصرح لهم بالاطلاع عليها؛
- تعطيل أحد الأشخاص لنظام الأمن الخاص بالشبكة أو كشفه لإجراءات الحماية المتبعة.

3. الإجراءات الوقائية للحد من المخاطر التي تهدد تكنولوجيا المعلومات وتقنيات التعامل معها.

هناك بعض الإجراءات الوقائية التي من شانها تجنيبنا الوقوع في المخاطر بمختلف أنواعها وخصوصا التي تهدد امن المعلومات، وإذا لم نتبع هذه الإجراءات فسوف نواجهها لا محال، في هذه الحالة هناك بعض الطرق أو التقنيات التي تساعدنا في التعامل معها، وفيما يلي تفصيل في الموضوع.

3-1- الإجراءات الوقائية للحد من المخاطر التي تهدد تكنولوجيا المعلومات:

تصنف الإجراءات الوقائية للحد من المخاطر التي تهدد امن المعلومات إلى صنفين، منها المادية أو الفيزيائية ومنها التقنية.

3-1-1- الإجراءات الوقائية المادية أو الفيزيائية للحد من المخاطر التي تهدد امن المعلومات:

تتمثل في اختيار المكان الملائم والتجهيزات الأكثر حفاظا على الأمن، ولتحقيق هذا المستوى من الحماية لابد من مراعاة ما يلي: (**بامفلح، صفحة 06،07**)

- تخصيص غرف مغلقة لحفظ أجهزة خادم الشبكة serveur في حالة وضعها في غرف مركزية، أما إذا لم يكن ذلك متاح فلابد من حفظ أجهزة الخادم ضمن غرف الإداريين؛
- اختيار الكابلات الأكثر حماية للمعلومات وتتمثل في كابلات الألياف الضوئية وذلك على اعتبار أنها تلغي الإشعاع الثانوي للكابلات وبالتالي تمنع التنصت على البيانات خلال نقلها عبر الكابلات؛

- تركيب تمديدات وكابلات الشبكة في أماكن محمية غير معرضة لوصول غير المختصين لها، بحيث لا تكون ظاهرة للعيان فيمكن على سبيل المثال تمريرها عبر الجدران وفوق السقف وتحت الأرض حتى تتم حمايتها قدر الإمكان من أجهزة التنصت وكذلك حمايتها من التعرض للقطع أو الثني في حالة وضعها تحت قطع المفروشات الثقيلة؛
- استخدام الكابلات المغلفة وذلك لتقليل الإشعاع الثانوي المنبثق من خلالها ويمكن إضافة أكثر من غلاف عليها لمنع الإشعاع نهائيا؛
- تأمين النوافذ والفتحات الأخرى الموجودة في غرفة الخادم خصوصًا إذا كانت قريبة من الأرض؛
- تأمين الأبواب والمنافذ الأخرى كالنوافذ باستخدام أجهزة إنذار آلية تقوم بتشغيل أجراس للتنبيه في حالة دخول أشخاص للموقع في غير أوقات العمل؛
- توفير وسائل مراقبة للموقع مثل الدوائر التلفزيونية المغلقة، وذلك لإتاحة المراقبة بعد ساعات الدوام.

كما يمكن إضافة:

- استخدام مصدر للطاقة الاحتياطية لتوليد الطاقة في حالة انقطاع التيار الكهربائي؛
- وضع أجهزة ومعدات الحاسوب في أماكن بعيدة عن مصادر المياه او عن أي مسبب لشرارة كهربائية.

3-1-2- الإجراءات الوقائية التقنية للحد من المخاطر التي تهدد امن المعلومات:

بالإضافة إلى الإجراءات الوقائية الفيزيائية للحد من المخاطر التي تهدد امن المعلومات هناك أخرى تقنية يجب إتباعها من طرف المنظمات للوصول إلى نطاق حماية أوسع والتي سنوردها فيما يلي: (**أبو عطيوي، 2012، الصفحات 23-25**)

- تطبيق إجراءات مراجعة دورية وغير دورية للتحقق من مستوى الحماية المتاحة للنظام؛
- تدريب العاملين على الإجراءات السليمة والآمنة لتشغيل النظام و استخدام قنوات الاتصال المتاحة للتبليغ والتقرير عن الأعطال والاختراقات الأمنية الطارئة؛

- توعية العاملين بدورهم في حماية كلمات المرور الخاصة بهم؛
- الاستعانة باستشارات المتخصصين في حماية نظم المعلومات.

كما يمكننا حماية مواقع أنظمة الأمن من خلال: (**مرایاتي، 2010، صفحة 85**)

- **برمجيات الحماية المضادة للفيروسات:**

تُمثل هذه الأخيرة الحد الأدنى في أي موقع لأمن المعلومات، تنصب هذه البرمجيات عادة في كل حاسوب يستعمل خدمة الانترنت، يجب أن تبقى ملفات الإرشادات حول البرمجيات المضادة للفيروسات محدثة بشكل منتظم لتعمل بشكل فعال.

- **جدران النار:**

تعد من بين آليات امن المعلومات تمنح الدخول إلى موارد المعلومات الداخلية للمستخدمين الذين يملكون التصريح اللازم و تمنع الوصول إليها من قبل جهة موجودة خارج الموقع المأمون (من الانترنت مثلا). وتكون على شكلين أولها جهاز الكتروني أما الثاني فيتمثل في برنامج، وقد يكون في شكل جهاز لحاسوب معين.

- **آليات التشفير:**

يصلح التشفير في حماية البيانات أثناء عملية الإرسال، ويجب أن تنصب تطبيقات التشفير على كل من الحاسوب المرسل والمستقبل. يقوم الحاسوب المرسل أثناء عملية الإرسال بتشفير البيانات قبل الإرسال، وفور استلامها من قبل الحاسوب المستقبل فانه يقوم بفك التشفير على البيانات.

- **وسائل قطع اتصال الشبكة:**

هي آليات تتكون عادة من برمجيات وتجهيزات تقوم حالا عند الضرورة بقطع الاتصالات السلكية واللاسلكية بين موقع الحماية والمحيط الخارجي عند حدوث اختراق ما أو هجمة الحرمان من الخدمة.

3-2- تقنيات التعامل مع الخطر:

تتعرض المنظمات بشكل مستمر إلى مخاطر متعددة ما استوجب عليها تسييرها وإدارتها بطريقة محكمة والتعامل معها بطرق وتقنيات مختلفة نذكرها فيما يلي: (**بن ديب، 2008، صفحة 07،08**)

3-2-1- الوقاية أو المنع أو تجنب المخاطر:

تعني محاولة تجنب النشاطات التي تؤدي إلى حدوث خطر ما، و مثال على ذلك عدم شراء ملكية ما أو عدم الدخول في عمل ما لتجنب تحمل المسؤولية القانونية. إن التجنب يبدو حلا لجميع المخاطر و لكنه في الوقت ذاته قد يؤدي إلى الحرمان من الفوائد و الأرباح التي كان من الممكن الحصول عليها من النشاط الذي تم تجنبه.

3-2-2- الاحتفاظ أو القبول بالمخاطر:

وتعني قبول الخسائر عند حدوثها، فهذه الطريقة تعتبر إستراتيجية مقبولة في حالة المخاطر الصغيرة، و التي تكون فيها تكلفة التأمين ضد الخطر على مدى الزمن أكبر من إجمالي الخسائر. وعليه فكل المخاطر التي لا يمكن تجنبها أو نقلها يجب القبول بها، و تعد الحرب أفضل مثال على ذلك حيث لا يمكن التأمين على الممتلكات ضد الحرب.

3-2-3- تقليل أو تقليص المخاطر:

تشمل طرقا للتقليل من حدة الخسائر الناتجة عن الخطر، و مثال على ذلك شركات تطوير البرمجيات التي تتبع منهجيات للتقليل من المخاطر، و ذلك عن طريق تطوير البرامج بشكل تدريجي.

3-2-4- تحويل أو نقل المخاطر:

هي وسائل تساعد على قبول الخطر من قبل طرف آخر، و عادة ما تكون عن طريق العقود أو الوقاية المالية، فالتأمين هو مثال على نقل الخطر عن طريق العقود.

3-3- التامين كتقنية للتعامل مع المخاطر التي تهدد امن المعلومات:

يعد التامين احد أهم الطرق التي تلجا إليها المنظمات في تعاملها مع المخاطر التي تواجهها، كون أن الجهات التي توكل إليها مهمة تحمل المخاطر (شركات التامين) تعتبر متخصصة في التعامل معها.

3-3-1- تعريف التامين:

كلمة "امن" عرفت بأنها الحاجة للبقاء، كان يكون الشخص أمنا من الهجمات التي تأتيه، كما تشمل أيضا تامين إمدادات الطعام، ثم اتسع مفهوم الأمن ليشمل الحصول على مكان امن للنوم دون

التعرض للأذى، ومع ظهور مفهوم الأملاك الخاصة ظهر مفهوم تامين هذه الممتلكات. (**السبكي، 2010، صفحة 49،50**) وللتامين شق قانوني وآخر فني كما هو موضح فيما يلي:

- **التعريف القانوني للتامين:**

حسب المادة 619 من القانون المدني الجزائري فإن: "التأمين هو عقد يلتزم المؤمن بمقتضاه أن يؤدي إلى المؤمن له أو إلى المستفيد الذي اشترط التأمين لصالحه مبلغا من المال أو إيراد أو أي تعويض مالي آخر في حالة وقوع الحادث ، أو تحقق الخطر المبين في العقد وذلك نظير قسط أو أي دفعة مالية أخرى يؤديها المؤمن له للمؤمن".(**بن خروف، 1998، صفحة 12**)

- **التعريف الفني للتامين:**

إضافة إلى الجانب القانوني الذي ينظم عملية التامين فان التامين يرتكز على جانب آخر يتمثل في الأسس الفنية والتي تشمل تنظيم التعاون بين المؤمن لهم، وقانون الأعداد الكبيرة وحساب الاحتمالات ، والجمع بين الأخطار القابلة للتأمين، وإجراء المقاصة بين الأخطار.

- **تنظيم التعاون بين المؤمن لهم:** والذي يعمل على تخفيف من حدة الخطر وتوزيعه (**طبايبية، 2014، صفحة 07،08**)
- **قانون الأعداد الكبيرة:** والذي يتعلق باستقرار تكرار بعض الحوادث عند وجود عدد كاف منها. (**فلاح.، 2011، صفحة 12**)
- **الجمع بين الأخطار القابلة للتأمين:** التامين هو عملية تجميع الأخطار المتجانسة أو بعبارة أخرى تجميع عدد كبير من الأفراد معرضين لنفس الخطر (أو لأخطار متشابهة أو متماثلة،) حيث يتفقوا سواء مباشرة أو عن طريق جهات محترفة (شركات وهيئات التامين) على تقسيم ما قد يحدث من خسائر مالية تلحق بعضهم أو تلحق بأي منهم نتيجة تحقق هذا الخطر. (**العمري و عطا، 2012، صفحة 75**)

- **إجراء المقاصة بين الأخطار:** يجب أن يتم الجمع بين أكبر عدد ممكن من الأخطار حتى يكون الرصيد المشترك كافيا للوفاء بالتعويضات، ولن يستطيع المؤمن إجراء المقاصة بين الأخطار إلا إذا كانت متجانسة ومتقاربة من حيث القيمة والمدة. (**طبايبية، 2014، صفحة 09**)

ومن خلال التعاريف السابقة يمكن استنتاج تعريف شامل للتامين على النحو التالي:

التأمين هو الطريق الذي يسلكه الفرد أو المجموعة للحصول على الطمأنينة بنقل عبئ الخسارة التي يمكن أن يتعرضون لها إلى جهة أخرى اقدر منهم على تحملها عن طريق تعويضها في حالة تحقق الضرر، مقابل أقساط أو اشتراكات يدفعونها لها بشكل دوري تحدد بطرق إحصائية مختلفة، حيث ينظم هذه العملية عقد يلتزم ببنوده الطرفان.

3-3-2- قابلية المخاطر للتامين:

حتى تكون المخاطر قابلة للتامين لا بد أن تتوفر فيها شروط نوجزها في الآتي:

- **أن تكون الخسارة مالية:** إمكانية قياس الخسارة ماليا؛
- **أن تكون الأخطار بحتة:** بصورة عامة عدم معرفة الأحداث المستقبلية وما إذا كان ثمة خسارة ستقع أم لا، أي أن يكون للخطر نتيجتان فقط إما خسارة أو لا خسارة؛
- **أن تكون الخسارة طارئة:** عبارة خسارة طارئة تعني خسارة عرضية، وفي هذا السياق تعني أن أي حدث يجب أن يكون خارجا عن سيطرة المؤمن له، أي انه يجب أن يكون عرضيا للمؤمن له.

3-3-3- المخاطر القابلة للتامين والتي تهدد امن المعلومات:

شركات التامين لا يمكنها التامين على جميع المخاطر بل فقط القابلة للتامين منها والتي تتوفر فيها الشروط اللازمة لذلك، الجدول الموالي يلخص المخاطر القابلة للتامين و التي تهدد امن المعلومات.

الجدول 2: مخاطر امن المعلومات القابلة للتامين:

<table>
<tr><td rowspan="3">الأخطار المعنوية والأخطار الاقتصادية:</td><td colspan="2">1-الأخطار المعنوية: من بين الأخطار المعنوية الخاصة بتكنولوجيا المعلومات والاتصال نجد التأثيرات السيكولوجية لشاشات العرض المرئية وكذلك الإدمان عليها ما يسبب التوتر العصبي والقلق والذي قد يصل في بعض الأحيان إلى حالات مرضية،. وهذا النوع من الأخطار غير قابل للتامين.بالإضافة إلى الأضرار التي تمس الأشخاص على شبكة الانترنت تتمثل في ارتكاب جرائم تمس الشرف والسمعة أو نشر الصور، ومثل هذه الأضرار يمكن التأمين ضدها (تتحمل شركات التامين مصاريف إنهاء النزاع).</td></tr>
<tr><td>2- الأخطار الاقتصادية:</td><td>أخطار الممتلكات: من بين هذه الأخطار نجد خطر سرقة معدات ووسائل تكنولوجيا المعلومات والاتصال، أو تخربها نتيجة تعرضها للمياه أو للحريق بفعل شرارة كهربائية مثلا.هذا النوع من الأخطار هو قابل للتامين. بالإضافة إلى أن بعض شركات التامين في الوقت الراهن تقوم بتامين الاختراقات الحاصلة على شبكة الانترنت وسرقة المعلومات أو إتلاف المحتويات أو سرقة أرقام الحسابات البنكية أو أدوات الدفع الالكتروني(تتحمل الشركات التامين مصاريف النزاع)</td></tr>
<tr><td colspan="2">أخطار المسؤولية المدنية: تنشأ الكثير من المنازعات نتيجة استعمال التجارة الالكترونية بسبب تقصير البعض في الوفاء بالتزاماتهم وهو ما يترتب عليه نشوء المسئولية المدنية.وتقوم شركات التامين بالتأمين من المسئولية الناشئة عن تجارة الانترنت، وعادة ما يشمل التأمين تقديم النصائح القانونية والعمل على حل المنازعات بطريقة ودية فإذا لم تفلح تلك المحاولات، تحملت شركات التأمين ما يؤول إليه النزاع القضائي من تعويضات وغرامات مالية في كافة درجات التقاضي إلى أن ينتهي النزاع نهائياً.</td></tr>
<tr><td>الأخطار العامة</td><td colspan="2">من بينها نجد تلف معدات تكنولوجيا المعلومات والاتصال نتيجة الكوارث الطبيعية كالفيضانات أو الزلازل وهي قابلة للتامين.</td></tr>
</table>

المصدر: من إعداد الباحثة بالاعتماد على: (مؤمن، صفحة 13،14)

4. خاتمة:

نتائج الدّراسة

وختاما لهذا الموضوع ومن خلال ما سبق ذكره تم التأكد من صحة الفرضيات التي وضعت كإجابات على التساؤلات المطروحة ومن أهم ما توصلنا إليه نجد:

- تتعرض المنظمات أثناء نشاطها لمخاطر عديدة ومختلفة منها من تهدد تكنولوجيا المعلومات في امن معلوماتها.
- على المنظمات بمختلف أنشطتها إتباع بعض الإجراءات الوقائية التي من شأنها التقليل من حجم المخاطر التي تتعرض لها وتقليص حدتها.
- بالرغم من كل الجهود التي تبذلها المنظمات لتفادي الوقوع في المخاطر وذلك بإتباعها كل الإجراءات الوقائية المنصوح بها إلا أن هناك بعض المخاطر لا يمكنها تفاديها فهي بذلك مرغمة على مواجهتها.
- تتعامل المنظمات مع المخاطر التي تواجهها باستمرار بعدة تقنيات، تختار الأنسب منها والتي تتماشى وأهداف المنظمة المخطط لها.
- يعد التامين واحدة من التقنيات التي تلجأ إليها المنظمة في تعاملها مع المخاطر، فهي بذلك تقوم بتحويلها إلى جهات أخرى اقدر منها عل تحملها، ألا وهي شركات التامين.
- ليست كل المخاطر التي تتعرض لها المنظمات قابلة للتامين بل وفقط تلك التي تتوفر فيها بعض الشروط والتي تجعل شركات التامين تقبل التامين عليها.
- المخاطر التي تهدد المنظمات في امن معلوماتها هي أيضا غير قابلة كلها للتامين.

وفي الأخير يمكن القول أن شركات التامين تتعرض للمنافسة الشديدة ما يستوجب منها مواكبة جميع التطورات الحاصلة، ومحاولة طرح منتجات جديدة في الأسواق، وعليه فان الأخطار غير قابلة للتامين اليوم يمكن أن تكون في المستقبل قابلة للتامين.

التوصيات:

ومن خلال هذه النتائج يمكننا تقديم مجموعة من الاقتراحات والتوصيات نوردها فيما يلي:

- ضرورة اهتمام الدولة بقطاع التأمين كونه واحدة من التقنيات التي تلجأ إليها المنظمة في تعاملها مع المخاطر،
- ضرورة تأمين المنظمات للمخاطر القابلة للتأمين والتي تهدد أمن معلوماتها،
- ضرورة إجراء دراسات أخرى حو ل الموضوع للإلمام به أكثر.

5. قائمة المراجع:

- أبو عطيوي ، رائدة إبراهيم، (2012)، اثر مخاطر استخدام تكنولوجيا المعلومات في المنشات الخاضعة للتدقيق على جودة عمل المدقق الخارجي، رسالة ماجستير في المحاسبة والتمويل،كلية التجارة بالجامعة الإسلامية بغزة، فلسطين.

- الجاسم،جعفر، (2005)، تكنولوجيا المعلومات، عمان، الاردن، دار أسامة للنشر والتوزيع.

- الدقس ،محمد عبد المولى، (2005)، علم الاجتماع الصناعي ، الطبعة الثانية، عمان، دار مجلاوي.

- السبكي، احمد محمد، (2010، دليل امن ونظم تكنولوجيا المعلومات ، الطبعة الاولى، القاهرة، شركة الأمل للطباعة والنشر.

- الشوابكة ، عدنان عواد، (2011)، دور نظم وتكنولوجيا المعلومات في اتخاذ القرارات الإدارية، عملن، الاردن، دار اليازوري العلمية للنشر والتوزيع.

- العاني ، مزهر شعبان ، و جواد ،شوقي ناجي، (2008)، العملية الإدارية وتكنولوجيا المعلومات، عمان، إثراء للنشر والتوزيع.

- العمري ، شريف محمد ، و عطا ،محمد محمد، (2012)، الأصول العلمية والعملية للخطر والتامين، الطبعة الاولى، السعودية، بدون دار النشر.

- الكساسبة، وصفي عبد الكريم، (2011)، تحسين فعالية الأداء المؤسسي من خلال تكنولوجيا المعلومات ، الطبعة الثالثة، عمان، الاردن، دار اليازوري العلمية للنشر والتوزيع.

- بامفلح ، فاتن سعيد، (بلا تاريخ). حماية امن المعلومات في شبكة المكتبات بجامعة ام القرى، من https://www.kau.edu.sa/Files/12510/Researches/63409_34429.pdf، تاريخ الاطلاع: 2017/12/26.

- بختي، إبراهيم، (2008)، تكنولوجيا و نظم المعلومات في المؤسسات الصغيرة و المتوسطة، من : http://bbekhti.online.fr/trv_pdf/TIC.pdf ، تاريخ الاطلاع 2017/08/1818.

- بن خروف ، عبد الرزاق، (1998)، التأمينات الخاصة في التشريع الجزائري، الجزائر، ديوان المطبوعات الجامعية.

- بن ديب ، عبد الرشيد، (2008/11/26)، مدخل استراتيجي لإدارة المخاطرت، الملتقى الدولي الثالث حول إستراتيجية إدارة المخاطر في المؤسسات: الأفاق والتحديات ، صفحة 07،08.

- ريم أبو عجيب، (04 04, 2020)، *ما هو أمن المعلومات*، من arageek مجتمع: https://www.arageek.com/l/%D9%85%D8%A7-%D9%87%D9%88-%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%D8%9F#%D8%A3%D9%86%D9%88%D8%A7%D8%B9%20%D9%88%D8%A3%D8%B4%D9%83%D8%A7%D9%84%20InfoSec، تاريخ الاطلاع 20121/01/16.

- سناء الدويكات. (19 12, 2016)، مفهوم نظام المعلومات،من موضوع: https://mawdoo3.com/%D9%85%D9%81%D9%87%D9%88%D9%85_%D9%86%D8%B8%D8%A7%D9%85_%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA%، تاريخ الاطلاع: 2021/01/16.

– طبايبية ، سليمة، (2014)، دور محاسبة شركات التامين في اتخاذ القرارات وفق معايير الإبلاغ المالي الدولية دراسة حالة الشركات الجزائرية للتامين، اطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير بجامعة سطيف، الجزائر.

– علوطي، لمين، (2008)، أثر تكنولوجيا المعلومات والاتصال على إدارة الموارد البشرية في المؤسسة، أطروحة دكتوراه في علوم التسيير، فرع إدارة أعمال، جامعة الجزائر، الجزائر.

– فلاح ،عز الدين، (2011)، "التامين : مبادئه، أنواعه، عمان، الاردن، دار أسامة للنشر والتوزيع.

– قنديلجي ،عامر إبراهيم ، و الجناب، علاء الدين عبد القاد، (2007)، نظم المعلومات الإدارية، عمان، الاردن، دار المسيرة.

– مراياتي ،محمد، (2010)، "امن تقنية المعلومات، نصائح من خبراء"، الرياض، المنظمة العربية للترجمة.

– ممدوح، حمزة احمد، (دون سنة النشر) إدارة الخطر والتامين، القاهرة.

– مؤمن ،طاهر شوقي، (بلا تاريخ)، التأمين ضد مخاطر استخدام الانترنت، من: https://www.researchgate.net/profile/.../altamyn-dd-mkhatr-astkhdam-alantrnt، تاريخ الاطلاع 2018/01/10.

-Alice Guilhon(2004) , L’intelligence économique dans la PME : visions éparses, paradoxes et manifestations, Paris.