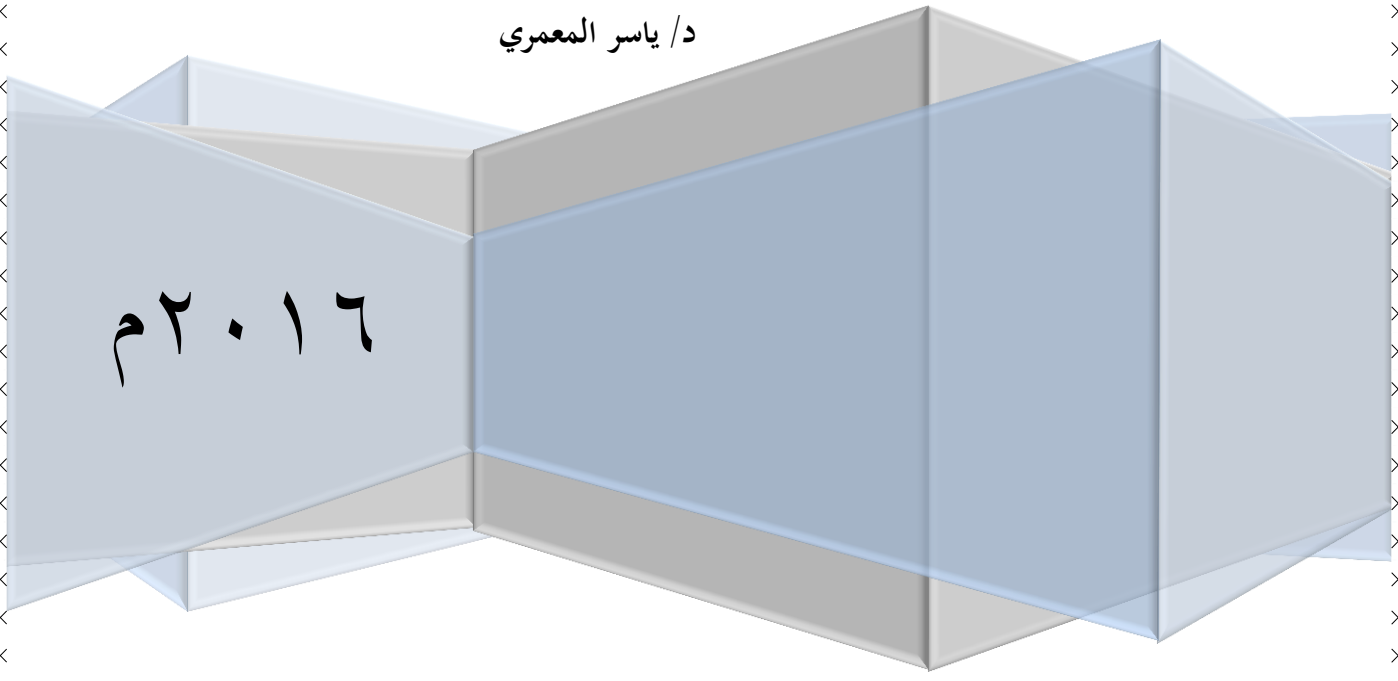
جامعة الاندلس
للعلوم والتقنية
دراسات عليا

# أمن المعلومات الالكترونية

اعداد: سند جمال الأكحلي

اشراف
د/ ياسر المعمري



٢٠١٦م

## المقدمة

لقد فرض عصر العولمة تغيرات كثيرة على شتى مجالات الحياة ، وتسابقت دول العالم لدخول الأسواق العالمية من أوسع أبوابها ، فالكل يحاول إيجاد افضل وأسهل الطرق للدخول في هذا النظام العالمي الجديد بشتى الطرق ، مما جعل العالم أشبه بقرية واحدة.

ولقد ساهمت تكنولوجيا المعلومات ، ومن خلال أشكالها العصرية المتطورة ، والمتسارعة ، والمتغيرة ، والمتعددة في جعل كل من يرغب في الدخول في النظام العالمي الجديد أن يبحث ، وينشئ مقومات وآليات تساعده في خوض هذا السباق.

لقد بدأت الشركات ومنذ عهد قريب باستخدام خدمة ما يسمى بالتجارة الإلكترونية عبر شبكة الانترنيت ، والسبب وراء ذلك يكمن بأن هذه الشبكة الإلكترونية غزت جميع دول العالم وبشكل متسارع وبواسطتها يمكن للشركات تسويق وبيع منتجاتها والوصول للمستهلك أينما كان وبتكلفة قليلة ، ويمكن القول بأن هذه الشبكة قد ألغت الحدود بين الدول.
تقوم حاليا كثير من الشركات بإنشاء موقع لها على تلك الشبكة السحرية يسمى (Web Page) تسوق من خلالها منتجاتها ، ويمكن للعميل إتمام عملية الشراء باستخدام بطاقات الاعتماد والشراء على الحساب وذلك وفقا لقيود وقوانين وروابط مصممة من قبل الشركة صاحبة الموقع.
ولكن وبالرغم من إيجابيات شبكة الانترنيت إلا انه هناك سلبيات و محددات تعد خطيرة جدا على نظام المعلومات المحاسبي والتي تؤثر على فاعليته وكفاءته ومن أهم هذه المحددات أو السلبيات عدم توفر ما يلي:

١- الأمان Security أي "إجراءات تكنولوجية معينة تمنع الآخرين من اختراق النظام المحاسبي المؤتمت عبر موقع الشركة الإلكتروني على شبكة الانترنيت".
٢- التوكيدية Assurance أي "خدمات مهنية تحسن من نوعية المعلومات أو مداخلاتها والمرغوب بها من قبل متخذي القرارات".

٣- الموثوقية Reliability أي "الإجراءات الواجب اتباعها لجعل المعلومات موثوقا بها من قبل أصحاب المصالح بشكل عام ومتخذي القرار بشكل خاص ، وإقناعهم بنجاعتها".

ومن دون توافر البنود الثلاثة المذكورة أعلاه ، يصبح النظام المحاسبي عقيما تماما وقد تصبح فاعليته وكفاءته موضع شك وفي أسوأ الحالات قد يؤدي لانهيار الشركة تماما. ولهذا فان الشركات تسعى بشتى الطرق لتفادي تلك السلبيات ، أو المحددات.

## امن المعلومات

- يعرف أمن المعلومات من زاوية أكاديمية" أنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها"،
- أما من زاوية تقنية فيعرف أمن المعلومات أنه عبارة عن" الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية"،
- ومن زاوية قانونية يعرف أمن المعلومات بأنه" محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة.
- كما يعرف أمن المعلومات بأنه" السياسات والإجراءات والمقاييس الفنية والتي تستخدم لتحول دون الوصول غير المتعمد أو السرقة أو التدمير للسجلات. "

ونستطيع أن نعرف أمن المعلومات بأنه عبارة عن:
العلم الذي يهتم بدراسة النظريات والاستراتيجيات والقوانين التي تهتم بتوفير الحماية لأمن المعلومات من المخاطر التي قد تواجهها والعمل على تطبيق الوسائل والأساليب والإجراءات اللازمة لتوفير تلك الحماية ومواجهة المخاطر والتغلب عليها، وسن القوانين الصارمة لمنع حدوث تلك المخاطر مستقبلا ومعاقبة مرتكبيها.

## استراتيجية أمن المعلومات:

**تعرف استراتيجية أمن المعلومات أو سياسة أمن المعلومات بأنها-:**

- ✓ **"مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها."**
- ✓ **"مجموعة القواعد التي تتعلق بالوصول إلى المعلومات والتصرف فيها ونقلها داخل هيكل يعتمد المعلومة عنصرا أساسيا في تحسين أدائه وبلوغ أهدافه. "**

**ومن خلال ما سبق نصل إلى أن استراتيجية أمن المعلومات عبارة عن القواعد التي تحدد كيفية الوصول إلى المعلومات والتعامل معها.**
**وتعد استراتيجية أمن المعلومات مهمة جدا للحفاظ على أمن نظم المعلومات المحاسبية بحيث تمنع الأشخاص الذين لا يحق لهم الوصول إلى المعلومات أن يصلوا إلى تلك المعلومات أو التعامل معها أو التعرف عليها.**

## أهداف استراتيجية أمن المعلومات:

**ولكي تعتبر استراتيجية أمن المعلومات ناجحة وفعالة وقابلة للتطبيق فلا بد أن يشارك في اعدادها وتنفيذها جميع المستويات الوظيفية التي لها علاقة بتلك الاستراتيجية حيث تسعى تلك المستويات إلى انجاح تلك الاستراتيجية من خلال تحقيق أهداف استراتيجية أمن المعلومات والتي تتمثل في:**

1. **تعريف مستخدمي نظم المعلومات ومختلف الاداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات والمعلومات بكافة أشكالها وفي مختلف مراحل جمعها وادخالها ومعالجتها ونقلها عبر الشبكات واعادة استرجاعها عند الحاجة.**
2. **تحديد وضبط الآليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة لكل من له علاقة بنظم المعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر.**
3. **بيان الإجراءات المتبعة لتفادي التهديدات والمخاطر وكيفية التعامل معها عند حصولها والجهات المكلفة بالقيام بذلك.**

# عناصر أمن المعلومات

من أجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنف تلك العناصر إلى خمسة عناصر وهي:

## ١. السرية أو الموثوقية

وهي تعني التأكد من أن المعلومات لا يمكن الاطلاع عليها أو كشفها من قبل أشخاص غير مصرح لهم بذلك ولتجسيد هذا الأمر يجب على المؤسسة استخدام طرق الحماية المناسبة من خلال استخدام وسائل عديدة مثل عمليات تشفير الرسائل أو منع التعرف على حجم تلك المعلومات أو مسار إرسالها.

## ٢. التعرف أو التحقق من هوية الشخصية

وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم الصحيح لتلك المعلومات أم لا، ويتم ذلك من خلال استخدام كلمات السر الخاصة بكل مستخدم.

## ٣. سلامة المحتوى

وهي تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء كان التعامل داخليا في المشروع أو خارجيا من قبل أشخاص غير مصرح لهم بذلك ويتم ذلك غالبا بسبب الاختراقات الغير مشروعة مثل الفيروسات حيث لا يمكن لأحد أن يكسر قاعدة بيانات البنك ويقوم بتغيير رصيد حسابه لذلك يقع على عاتق المؤسسة تأمين سلامة المحتوى من خلال اتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات أو الفيروسات.

## ٤. استمرارية توفر المعلومات أو الخدمة

وهي تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمات لمواقع المعلومات وضمان عدم تعرض مستخدمي تلك المعلومات إلى منع استخدامها أو الوصول إليها بطرق غير مشروعة يقوم بها أشخاص

لإيقاف الخدمة بواسطة كم هائل من الرسائل العبثية عبر الشبكة إلى الأجهزة الخاصة لدى المؤسسة.

٥. **عدم الإنكار**

ويقصد به ضمان عدم إنكار الشخص الذي قام بإجراء معين متصل بالمعلومات لهذا الإجراء، ولذلك لا بد من توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص للشخص الذي قام به في وقت معين، ومثال ذلك للتأكد من وصول بضاعة تم شراؤها عبر شبكة الإنترنت إلى صاحبها، ولإثبات تحويل المبالغ إلكترونيا يتم استخدام عدة رسائل مثل التوقيع الإلكتروني والمصادقة الإلكترونية.

## العوامل التي تساعد على اختراق نظام المعلومات المحاسبي-:

تعتبر نظم المعلومات المحاسبية الإلكترونية أقل أماناً من نظم المعلومات اليدوية وذلك نظرا لاعتماد النظم المحاسبية الإلكترونية على حفظ بياناتها في ملفات الكترونية يستطيع عدد كبير من الأشخاص الوصول إليها والاطلاع عليها، ولذلك فإن نظم المعلومات المحاسبية الإلكترونية قد تتعرض للعديد من المخاطر التي قد تهدد أمنها وذلك بسبب مجموعة من العوامل وهي كما يلي:

1. نظم المعلومات الإلكترونية تتضمن كم هائل من البيانات ولذلك فإنه يصعب عمل نسخ ورقية لها.
2. صعوبة اكتشاف الأخطاء الناتجة عن التغير في نظام المعلومات المحاسبي الإلكتروني وذلك لأنه لا يمكن التعامل أو قراءة سجلاتها إلا بواسطة الحاسب والذي لا يكشف أي تغيير.
3. صعوبة مراجعة الإجراءات التي تتم من خلال الحاسب وذلك لأنها غير مرئية وغير ظاهرة.
4. صعوبة تغيير النظم الآلية مقارنة بالنظم اليدوية.
5. احتمال تعرض النظم الآلية إلى إساءة استخدامها بواسطة الخبراء غير المنتمين للمنظمة في حال استدعائهم لتطوير النظم.

6. قد تؤدي المخاطر التي تتعرض لها النظم الآلية إلى تدمير كافة سجلات المنظمة وبذلك فهي أشد خطورة على النظم الآلية من النظم اليدوية.
7. انخفاض المستندات التي يمكن من خلالها مراجعة النظام تؤدي إلى انخفاض حالة الأمان اليدوية.
8. احتمال تعرض النظم الآلية إلى حدوث أخطاء أو إساءة استخدام النظام في مرحلة تشغيل البيانات وذلك لتعدد عمليات التشغيل في النظام الآلي.
9. ضعف الرقابة على النظام الآلي بسبب الاتصال المباشر للمستخدم بنظم المعلومات.
10. التطور التكنولوجي في الاتصال عن بعد سهل عملية الاتصال بنظم المعلومات من أي مكان وبالتالي إمكانية الوصول غير المسموح به أو إساءة استخدام نظم المعلومات.
11. استخدام العديد من التطبيقات في مواقع مختلفة لنفس قاعدة البيانات يؤدي إلى إمكانية اختراقها بفيروسات الحاسب وبالتالي امكانية تدمير أو تغيير قاعدة البيانات لنظام المعلومات.

ومن خلال ما سبق نجد أنه ينبغي على إدارة المؤسسة العمل على حماية بياناتها بكافة أشكالها، سواء كانت ورقية أو غير ورقية، كما أن نظام المعلومات المحاسبي الإلكتروني يكون عرضة للمخاطر أكثر من غيره من النظم ولذلك لا بد للإدارة من وضع قيود على المستخدمين تحد من امكانية التلاعب بالبيانات أو العبث بها سواء من أطراف داخل المؤسسة أو خارجها.

## المخاطر التي يمكن أن تتعرض لها نظم المعلومات المحاسبية الالكترونية

يعتبر موضوع حماية البيانات من الأمور الواجب الاهتمام بها في كافة مراحل إعداد نظم المعلومات المحاسبية حيث أن أمن البيانات والمعلومات أصبح من أهم عناصر الرقابة الواجب تطبيقها على المعلومات من خلال التخطيط المستمر خلال دورة حياة نظم المعلومات المحاسبية المستخدمة.

وتعتبر 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 الى خسائر مادية أو معنوية كبيرة ويمكن تصنيف مخاطر تهديدات أمن نظم المعلومات المحاسبية الإلكترونية من وجهات نظر مختلفة إلى عدة أنواع:**

**<u>أولا /من حيث مصدرها</u>**

**أ .مخاطر داخلية**

**ب .مخاطر خارجية**

**<u>ثانيا /من حيث المتسبب بها</u>**

**أ .مخاطر ناتجة عن العنصر البشري**

**ب .مخاطر ناتجة عن العنصر الغير بشري**

**<u>ثالثا /من حيث أساس العمدية</u>**

**أ .مخاطر ناتجة عن تصرفات متعمدة مقصودة**

**ب .مخاطر ناتجة عن تصرفات غير متعمدة غير مقصودة**

**<u>رابعا /من حيث الآثار الناتجة عنها</u>**

**أ .مخاطر ينتج عنها أضرار مادية**

**ب .مخاطر فنية ومنطقية**

**<u>خامسا /المخاطر على أساس علاقتها بمراحل النظام</u>**

**أ .مخاطر المدخلات**

**ب .مخاطر التشغيل**

**ت .مخاطر المخرجات**

## أسباب حدوث المخاطر التي تواجه أمن نظم المعلومات المحاسبية الالكترونية

**تتعرض نظم المعلومات المحاسبية الالكترونية للعديد من المخاطر التي تهدد أمنها وقد تم تقسيم تلك المخاطر إلى أربعة أقسام رئيسية تتعلق بمراحل النظام الأساسية من ادخال وتشغيل ومخرجات والقسم الرابع يتعلق بالمخاطر البيئية وقد ترجع أسباب حدوث تلك المخاطر إلى أسباب تتعلق بالمدخلات والمخرجات وأسباب تتعلق بالتشغيل أو قد نعتبرها أسباب إدارية رقابية وأسباب لها علاقة بالموظفين، وتتلخص تلك الأسباب في البنود التالية :**

1. **عدم كفاية وفعالية الأدوات الرقابية المطبقة لدى إدارة المنشأة.**
2. **ضعف نظم الرقابة الداخلية لدى المنشأة وعدم فعاليتها.**
3. **اشتراك بعض الموظفين في استخدام نفس كلمات السر من أجل الدخول إلى النظام والعبث بمحتوياته.**
4. **عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات المحاسبية في المنشأة.**
5. **عدم وجود سياسات واضحة وبرامج محددة ومكتوبة فيما يختص بأمن نظم المعلومات المحاسبية لدى المنشأة.**
6. **عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر.**
7. **ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب.**
8. **عدم التوصيف الدقيق للهيكل الوظيفي والاداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي لدى المنشأة.**
9. **عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي المنشأة.**
10. **عدم الزام الموظفين بأخذ إجازاتهم الدورية.**
11. **عدم الاهتمام الكافي بفحص التاريخ الوظيفي المهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.**
12. **عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي المنشأة.**

13. عدم وجود الوعي الكافي لدى الموظفين بضرورة فحص أي البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.

## متطلبات أمن نظم المعلومات المحاسبية

تعتبر مسألة حماية أمن نظم المعلومات المحاسبية من المسائل الهامة والضرورية والتي ينبغي على المؤسسة أخذها بعين الاعتبار ووضع خطة حماية شاملة في حدود امكانياتها التنظيمية والمادية ويجب أن تكون تلك الحماية قوية وليست ضعيفة ولذلك فإنه توجد عدة متطلبات لحماية أمن نظم المعلومات المحاسبية تتمثل في :

1. وضع سياسة حماية عامة لأمن نظم المعلومات المحاسبية تتحدد حسب طبيعة عمل وتطبيقات المنشأة.
2. يجب على الإدارة العليا في المنشأة دعم أمن نظم المعلومات لديها.
3. يجب أن توكل مسؤولية أمن نظم المعلومات في المؤسسة لأشخاص محددين.
4. تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة.
5. تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية.
6. الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن.
7. تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط.
8. تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات.

## كيف نحمي أمن نظم المعلومات المحاسبية:

لتحقيق متطلبات أمن وحماية نظم المعلومات المحاسبية فلا بد للمؤسسة من اتباع عدة اجراءات للحماية ومنها:

- ✓ اجراءات الحماية الفيزيائية لنظم المعلومات بما فيها الحماية المادية للأجهزة التي تحتوي على نظم المعلومات.
- ✓ انتقاء العاملين في النظم المعلوماتية بحيث يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة المنشأة وتوعيتهم أمنيا للمحافظة على أمن المعلومات.

- ✓ **إجراءات الحماية الخاصة بنظم تشغيل البيانات والبرامج التطبيقية اللازمة لذلك وضبط الصلاحيات الخاصة بنظم التشغيل.**
- ✓ **إجراءات الحماية الخاصة بالشبكات المعلوماتية ومنع اختراقها.**
- ✓ **العمل على تشفير المعلومات التي يتم تخزينها ونقلها حتى لا يتم معرفة ماهيتها في حالة الحصول عليها من أشخاص غير مصرح لهم بذلك.**
- ✓ **إجراءات حفظ البيانات بصورة عامة وحفظ نسخ منها في مواقع آمنة يمكن الرجوع إليها عند الحاجة لذلك.**
- ✓ **إجراءات ضمان استمرارية عمل وجاهزية نظم المعلومات في شتى الظروف التي قد تواجه النظم، مثل تعطل أو توقف النظم المعلوماتية عن العمل.**

## وسائل الأمن الشائعة

**وسائل أمن المعلومات هي مجموعة من الآليات والإجراءات والادوات والمنتجات التي تستخدم للوقاية من او تقليل المخاطر والتهديدات التي تتعرض لها الكمبيوترات والشبكات وبالعموم نظم المعلومات وقواعدها .**

**وكما أوضحنا ، فان وسائل الأمن متعددة من حيث الطبيعة والغرض ، لكن يمكننا بشكل أساسي تصنيف هذه الوسائل في ضوء غرض الحماية الى الطوائف التالية :-**

- ✓ **مجموعة وسائل الأمن المتعلقة بالتعريف بشخص المستخدم وموثوقية الاستخدام ومشروعيته وهي الوسائل التي تهدف الى ضمان استخدام النظام او الشبكة من قبل الشخص المخول بهذا الاستخدام، وتضم هذه الطائفة كلمات السر بأنواعها، والبطاقات الذكية المستخدمة للتعريف، وسائل التعريف البيولوجية التي تعتمد على سمات معينة في شخص المستخدم متصلة ببنائه البيولوجي، ومختلف أنواع المنتجات التي تزود كلمات سر آنية او وقتية متغيرة الكترونيا ، المفاتيح المشفرة ، بل تضم هذه الطائفة ما يعرف بالأقفال الإلكترونية التي تحدد مناطق النفاذ .**

- ✓ **مجموعة الوسائل المتعلقة بالتحكم بالدخول والنفاذ الى الشبكة وهي التي تساعد في التأكد من ان الشبكة ومصادرها قد استخدمت بطريقة مشروعة ، وتشمل من بين ما تشمل الوسائل التي تعتمد على تحديد حقوق المستخدمين، او قوائم اشخاص**

**المستخدمين أنفسهم، او تحديد المزايا الاستخدامية او غير ذلك من الإجراءات والادوات والوسائل التي تتيح التحكم بمشروعية استخدام الشبكة ابتداء.**

- ✓ **مجموعة الوسائل التي تهدف الى منع افشاء المعلومات لغير المخولين بذلك وتهدف الى تحقيق سرية المعلومات، وتشمل هذه الوسائل من بين ما تشمل تقنيات تشفير المعطيات والملفات، وإجراءات حماية نسخ الحفظ الاحتياطية، والحماية المادة للأجهزة ومكونات الشبكات واستخدام الفلترات والموجهات .**

- ✓ **مجموعة الوسائل الهادفة لحماية التكاملية ( سلامة المحتوى ) وهي الوسائل المناط بها ضمان عدم تعديل محتوى المعطيات من قبل جهة غير مخولة بذلك ، وتشمل من بين ما تشمل تقنيات الترميز والتواقيع الإلكترونية وبرمجيات تحري الفايروسات وغيرها .**

- ✓ **مجموعة الوسائل المتعلقة بمنع الانكار ( انكار التصرفات الصادرة عن الشخص )، وتهدف هذه الوسائل الى ضمان عدم قدرة شخص المستخدم من انكار انه هو الذي قام بالتصرف ، وهي وسائل ذات اهمية بالغة في بيئة الاعمال الإلكترونية والتعاقدات على الخط ، وترتكز هذه الوسائل في الوقت الحاضر على تقنيات التوقيع الإلكتروني وشهادات التوثيق الصادرة عن طرف ثالث.**

- ✓ **وسائل مراقبة الاستخدام وتتبع سجلات النفاذ او الأداء ( الاستخدام )، وهي التقنيات التي تستخدم لمراقبة العاملين على النظام لتحديد الشخص الذي قام بالعمل المعين في وقت معين ، وتشمل كافة أنواع البرمجيات والسجلات الإلكترونية التي تحدد الاستخدام.**

## **ايضاح موجز حول اكثر وسائل الامن شيوعا في بيئة نظم المعلومات :-**

- ✓ **برمجيات كشف ومقاومة الفيروسات.**
- ✓ **الجدران النارية والشبكات الافتراضية الخاصة.**
- ✓ **التحقق من الهوية.**

- ✓ **التشفير تحظى تقنيات وسياسات التشفير في الوقت الحاضر باهتمام استثنائي في ميدان أمن المعلومات ، ومرد ذلك ان حماية التشفير يمثل الوسيلة الاكثر اهمية لتحقيق وظائف الأمن الثلاثة ، السرية والتكاملية وتوفير المعلومات .**

**فان التشفير يمر بمرحلتين رئيستين ، الأولى تشفير النص على نحو يحوله الى رموز غير مفهومة او مقروءة بلغة مفهومة ، والثانية ، فك الترميز بإعادة النص المشفر الى وضعه السابق كنص مفهوم ومقروء ، وهذه المسالة تقوم بها برمجيات التشفير التي تختلف أنواعها ووظائفها. اما من حيث طرق التشفير، فثمة التشفير الترميزي، والتشفير المعتمد على مفاتيح التشفير، التي قد تكون مفاتيح عامة او خاصة او مزيجا منها.**

**تم بحمد الله**