رقابة وأمن المعلومات

لماذا الرقابة على أنظمة المعلومات؟

- نتيجة لتطور الحاسبات والبرمجيات وأنظمة التكنلوجيا ظهرت الحاجة الى دور الرقابة
- استخدام قواعد بيانات متعددة قاد الى الحاجة لنظم رقابة فاعلة للحماية والحد من التلاعب او العبث في البينات

أهمية الرقابة على البيانات والمعلومات: وترجع أهمية تحقيق الرقابة إلى:

١- تحقيق درجة معقولة من التأكد بأنّ أهداف كل نظام يتم تحقيقها.

٢ - تحقيق درجة معقولة من التأكد بأنّ الاعتبارات القانونية يتم أخذها في الاعتبار

جرائم الحاسب وسوء الاستخدام:

يشير مصطلح جرائم الحاسب إلى أي أفعال تمثل عدواناً على نظام المعلومات مثل:

- تعديل السجلات للحصول على أموال،
- تدمير بيانات قيّمة، الاستيلاء على معلومات مملوكة للغير،
- عمل نسخ من البرمجيات بطريقة غير قانونية.

- بمعنى اخر: استخدام الحاسوب بصورة غير أخلاقية مثل استخدام نظم المعلومات لأغراض شخصية

امثلة على جرائم الحاسوب وسوء الاستخدام:

١- اختراق البيانات المحمية والمؤمنة.

٢- إلحاق الضرر المتعمد بالحاسوب.

٣- سرقة الأسرار التجارية.

٤- نسخ غير شرعي لبرامج وحقوق الملكية الفكرية مثل: المقالات، الكتب، الموسيقى والأفلام.

٥- استخدام البريد الالكتروني للتهديد والأذى.

٦- التزوير وغسيل الأموال.

- تعدّ الإدارة مسؤولة ضمناً عن إيقاف تلك الجرائم والحد منها بصفة عامة عن حماية المنظمة من أي استخدام سيء،
- وكذلك توفير سبل الرقابة الكافية للتأكد من أنّ أهداف المنظمة يتم تحقيقها.
- جرائم الحاسوب المصرح بها تمثل نسبة (٢٠-٥٠%) من اجمالي الجرائم المرتكبة فعليا-
- وتلك النسب تعكس بشكل تكاليف وخسائر عالية تتحملها المنظمة

العلاقة بين الرقابة والامن على نظم المعلومات

- تطبيق وتقييم نظم المعلومات تتضمن الرقابة كل أنشطة تخطيط، تحليل، تصميم، وتطبيق نظم المعلومات، أي أنّ الرقابة كعملية مرادفة للتقييم يجب أن تشتمل كل مراحل دورة تطوير حياة النظام.
- وللرقابة على نظم المعلومات أهمية كبيرة تتجلى في تأثيرها المباشر على كفاءة وفعالية أداء النظام وعمله، وكذلك في دور الرقابة المهم والمباشر في حماية أمن وسلامة النظام لمكوناته وموارده من البيانات، المعلومات، البرامج وقواعد البيانات.

ابعاد مفهوم الرقابة على نظم المعلومات:

١- **البعد الأول:** يتصل بأنشطة الرقابة والمراجعة وتصحيح الأخطاء، وكشف الانحرافات بصورة مباشرة، وذلك بهدف تحسين كفاءة أداء نظام المعلومات وبالتالي جودة مخرجاته من المعلومات.

٢- **البعد الثاني:** له علاقة بأنشطة حماية نظام المعلومات وأمن موارد النظام وسلامته، حماية النظام يعني بناء وتطبيق إجراءات وأعمال تمنع كل أشكال التخريب، الاختراق، الاستخدام غير الشرعي للأجهزة، النفاذ غير المسموح إلى مستودعات البيانات، وكل أمر يتعلق بجرائم الحاسوب والإنترنت.

٣- **البعد الثالث:** يتصل بعملية تقييم أنشطة وعمليات نظام المعلومات، وتحليل المنافع/ التكاليف من منظور شامل ومتكامل، أي بمعنى تقييم نظام المعلومات من خلال تحليل ما يحققه من فائدة أو منفعة، وما ينتجه من قيمة للأعمال مقابل ما تتحمله المنظمة من تكلفة منظورة وغير منظورة.

خصائص وشروط مكونات الرقابة على امن نظم المعلومات

١ـ الكمال:

يكون النظام كاملاً إذا أدى ما هو مطلوب منه، ويحاول مصممو النظام بناء نظام ما يسمى بالتكامل الوظيفي، بمعنى استمرار النظام في العمل حتى إذا كان هناك جزء أو أكثر منه لا يعمل.

٢ـ القابلية للمراجعة:

يقصد بها سهولة الاختيار والتأكد من أداء النظام، ولكي يكون النظام قابلاً للمراجعة فلا بدَ من مقابلة اختبار المسؤولية، بمعنى وجود شخص واحد مسؤول عن الأحداث داخل النظام، أما الاختبار الآخر فهو الوضوح بمعنى أنّ الأداء غير المقبول من النظام يجذب انتباه واهتمام مديرا النظام.

٣ـ القابلية للرقابة:

من أهم وسائل جعل النظام قابلاً للرقابة تقسيمه إلى نظم فرعية، بحيث يتعامل كل نظام فرعي مع مجموعة من العمليات المنفصلة عن النظم الفرعية الأخرى.

إجراءات الرقابة على امن المعلومات

عملية الرقابة؟

١- إعداد أدلة لاستخدام عتاد وبرامج النظام.

٢- إعداد دليل الأخطاء المحتملة وسبيل المعالجة.

٣- تحديد امتيازات المستفيدين.

٤- الرقابة على التدفقات الداخلية للنظام عبر الشبكات والوسائط الرقمية الأخرى.

٥- الاستخدام الفعّال لتقنيات حماية بيانات نظام المعلومات.

٦- تحديد إجراءات الرقابة على المعالجة التقليدية لمعاملات الأعمال.

٧- وضع نسخ احتياطية لملفات وقواعد البيانات.

٨- المحافظة على أمن المعاملات الالكترونية (التجارة الالكترونية تحديداً) التي تتم على شبكة الإنترنت.

أهداف الرقابة على امن المعلومات

١- أهداف الرقابة على نظام العمليات: (وسائل الرقابة على العمليات)

ويمكن أن نحصر أهم أهداف الرقابة على نظام العمليات بالنقاط الآتية:

- **ضمان فعالية العمليات عن طريق تحقيق الأهداف المحددة للنظام.**
- **ضمان كفاءة استخدام الموارد.**
- **ضمان أمان الموارد المستخدمة.**

٢- فيما يتعلق بتسجيل المعاملات:

- ضمان صحة المدخلات:

الهدف أن يحتوي الخرجات تعكس المدخلات (بافتراض صحة المعالجة)، بالتالي المعلومات صحيحية وذات ثقة عالية.

-ضمان اكتمال المدخلات:

ضرورة إدخال كافة البيانات الصحيحة المتعلقة بالتعامل في ملف المعاملات المناسب، بالتالي نجد أنّ هذا الهدف يختص بعدد المعاملات المسجلة في ملف المعاملات، وهذا يعني الإجابة على السؤالين الآتيين لضمان تحقيق الهدف:

أ- هل كل المعاملات الحادثة تم الحصول عليها ؟.

ب - هل كل المعاملات التي حصلنا عليها قد أدخلت في ملف المعاملات ؟

- ضمان دقة المدخلات:

مطابقة البيانات المدخلة مع التي حصلنا عليها نتيجة التعامل، نقصد الدقة الحسابية والكتابية للبيانات.

وهناك سؤالان رئيسان يلخصان هذا الهدف:

أ- هل تمّ الحصول على البيانات بصورة صحيحة ؟.

ب- هل تمت عملية إدخال البيانات بصورة صحيحة ؟.

٢- فيما يتعلق بالملف الرئيسي:

وتهدف إدخال التعديلات على الملفات الرئيسية، وفيما يلي نقوم بتعريف بعض المصطلحات الهامة:

- **Update Files:** إدخال تعديلات على ملف موجود أساساً، من خلال إضافة أو استبعاد أو استبدال جزئيات من ذلك الملف.

- الملف الرئيسي

هو مجموعة من البيانات الدائمة والمحتفظ بها لمدد طويلة نسبياً، ويعدّ الأستاذ العام مثالاً لهذا الملف الرئيسي في النظام المحاسبي.

وهناك نوعان من التعديلات اللازم إدخالها على مثل هذه الملفات وهي:

أ ـ تسجيل المعاملات:

يتضمن تسجيل البيانات المتعلقة المعاملات الاقتصادية كافة مثل المعاملات المحاسبية، وكذلك العمليات الداخلية مثل الإنتاج، ويترتب على تسجيل تلك المعاملات إدخال التعديلات في الملفات الرئيسية للمعلومات

ب- صيانة الملفات:

تتضمن عمليات الإضافة والاستبعاد والتعديل للبيانات الرئيسية الدائمة في الملفات الرئيسية.

ـ اكتمال الإضافة للملف:

يتعلق هذا الهدف بالتأكد من أنّ كل البيانات المدخلة يتم تسجيلها في الملفات الرئيسية المتعلقة بها، ويسري هذا الهدف على النظام الآلي المرتبط بالحاسب والنظام اليدوي.

دقة الإضافة للملف:

يتم هذا الهدف بضمان أنّ البيانات التي يتم إدخالها إلى الحاسب يتم إدخالها كتعديلات على الملفات الرئيسية بصورة صحيحة ودقيقة.

أخطاء تشغيل البيانات

١- أخطاء البرمجة: (أخطاء فنية اثناء تشغيل البيانات)

أ-وقوع خطأ في إعداد تلك البرامج أو في تشغيلها.

ب- أخطاء تشغيلية:

ترجع هذه الأخطاء إلى مشغلي البيانات أنفسهم فمثلاً قد يقوم مشغل البيانات باستخدام أرصدة حسابات العملاء عن يوم سابق بدلاً من استخدام الرصيد الأخير لتلك الحسابات.

خطط الرقابة على نظم المعلومات: (تتعلق بتشغيل البيانات وإجراءاتها)

تسعى إلى تحقيق الأهداف الرقابية المنشودة، وبصفة عامة يمكن القول إنّ هناك نوعين من الخطط الرقابية (الخطط الرقابية الانتشارية، والخطط الرقابية التطبيقية).

١- الخطط الرقابية الانتشارية:

تتعلق بالأهداف الواسعة على التطبيقات، كما تتصف بأنها تنطبق على التطبيقات النظام كافة، وليس نوعاً واحداً على وجه الخصوص، وتتكون الخطط الرقابية الانتشارية من أربع مجموعات رقابية أساسية:

أولاً. خطط رقابية خاصة بالأفراد:

أ- خطط رقابية خاصة بالاختيار والتعيين

ب- خطط رقابية خاصة بالاحتفاظ بالأفراد:

ج- خطط رقابية خاصة بتنمية الأفراد:

د- خطط رقابية خاصة بإدارة الأفراد: حيث تقوم على نقاط رئيسية هي:

١- تخطيط الاحتياجات للأفراد:

٢- توصيف الوظائف

٣- الإشراف:

٤- تأمين ضد انحراف الأفراد:

٥- انتهاء خدمة العاملين:

ثانياً. الخطط الرقابية الخاصة بالتنظيم:

- فإنّ الاستقلال التنظيمي يعدّ عاملاً حيوى اً في نظام الرقابة في ظل الحاسب الآلي، وهذا يعني بالضرورة أن تتعلق الخطط الرقابية الخاصة بالتنظيم بالإجراءات المتعلقة بالفصل بين المهام، وتهدف تلك الإجراءات إلى الوقاية من حدوث أخطاء في عمليات إدخال البيانات، وكذلك عمليات تعديل البيانات، مما قد يؤدي إلى إنتاج بيانات غير صحيحة تتسبب في اتخاذ قرارات خاطئة.

ثالثاً. الخطط الرقابية الخاصة بأمان الموارد:

١. **خطط رقابية خاصة بالحد من سوء استخدام الحاسبات الآلية:** وتنقسم تلك الخطط إلى:

أ - **خطط رقابية تمنع من الوصول إلى استخدام أجهزة الحاسب لغير المسموح** لهم باستخدامها، وتشمل كافة القيود المادية بما يتعلق بأجهزة الحاسب والمباني التي تحوي تلك الأجهزة، وأيضا وجود الحراس وأجهزة الأمن.

ب- **خطط رقابية تحد من الوصول إلى البرامج والملفات والبيانات**، وتتعلق تلك الخطط بمحتويات أجهزة الحاسب الآلي من برامج وملفات (تحديد المصرح لهم-والمستويات والصلاحيات الممنوحة).

ج - **خطط رقابية خاصة بالحد من سوء استعمال أصول المنظمة:** حماية أصول المنظمة من نقدية ومخزون وأصول ثابتة من سوء الاستعمال أو السرقة أو التلف،

رابعا. الخطط الرقابية الخاصة بالسياسات:

- تهتم هذه الخطط الرقابية بالتأكد من أنّ سياسات المنظمة كافة يتم تسجيلها وتوثيقها بصفة أساسية حتى يكون هناك مرجع دائم لتلك السياسات. وتشمل خطط رقابية بتشغيل الطلبيات /المبيعات- وارسال الفواتير للعملاء:- المتحصلات والمدفوعات النقدية - وخطط رقابية خاصة بأنظمة الأجور:

خامسا-الرقابة على التطبيقات:

أ- الرقابة على المدخلات

ب- الرقابة على التشغيل: (التأكد من دقة واكتمال تحديث اليانات)

ج- الرقابة على المخرجات:

سادسا-بناء نظام أو هيكل الرقابة (التكلفة والعائد):

-١درجة أهمية البيانات

-٢ درجة استخدام البيانات

-٣ مستوى المخاطر

مفهوم أمن المعلومات

يمكن تعريف أمن المعلومات من 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

- **من الناحية القانونية:**

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

امن البيانات والمعلومات:

- العلم الذي يبحث في نظريات وأساليب حماية البيانات والمعلومات، و يضع الأدوات والإجراءات اللازمة لضمان حمايتها، و يسهم في وضع التشريعات التي تمنع الاعتداء على المعلومات و معاقبة المعتدين عليها .

- يستخدم مصطلح امن المعلومات (Information Security) لوصف مهام حماية المعلومات بشكلها الرقمي. ويمكن ان تكون هذه المعلومات قيد المعالجة ضمن وحدة المعالجة المركزية او مخزنة على قرص صلب او منقولة باستخدام شبكة ما.

- 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)".

تعريف إدارة نظم امن المعلومات

يشمل إيجاد بيئة تنظيمية، ووضع سياسات امنية، وتخطيط أنشطة الامن المعلوماتي، وتحديد المسؤوليات والممارسات والإجراءات والعمليات، والموارد اللازمة لإدارة امن المعلومات بكفاءة وفاعلية.

أهمية امن المعلومات

١. القطاعات الأمنية والعسكرية والاقتصادية تعتمد على صحة ودقة المعلومات.
٢. حاجة الدول لوجود إجراءات أمنية قابلة للتطبيق تغطي المخاطر تظهر عند التعامل مع الأطراف الأخرى.
٣. الحاجة المتزايدة لإنشاء بيئة إلكترونية آمنة تخدم القطاعين الخاص والعام.
٤. النمو السريع في استخدامات التطبيقات الإلكترونية والتي تتطلب بيئة آمنة.
٥. الحاجة إلى حماية البنية التحتية للشبكة المعلوماتية وذلك من أجل استمرارية الأعمال التجارية.
٦. مع تطور التقنية المعلوماتية وازدهارها توفرت فرصاً للإجرام الإلكتروني.

لذلك فأهمية امن المعلومات تعكسها النقاط الاتية:

١- منع سرقة ٢- احباط سرقة الهوية ٣- منع التبعات القانونية ٤- الحفاظ على الانتاجية

٥-احباط الإرهاب السبراتي:

هجوم متعمد ذات طابع سياسي ضد معلومات او أنظمة حاسوبية او برامج او معطيات- يسبب اذى لأهداف غير مقاتلة من قبل مجموعات دولية او عملاء سريين لهدم مجالات صناعية-عسكرية- كهربائية..الخ

- **يُعرَّف الأمن السيبرانى على النحو المحدد فى التوصية الاتحاد الدولى للاتصالات)- ITU**

T X.1205بأنه: مجموعة الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ومنهُج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وسبل الضمان والتكنولوجيات التي يمكن استخدامها في حماية البيئة السيبرانية والمنظمة وأصول المستعملين.

- وتشمل المنظمة وأصول المستعملين تجهيزات الحواسيب الموصولة، والموظفين، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات، والحصيلة الكلية للمعلومات المرسلة و/أو المخزنة في البيئة السيبرانية.

- ومن شأن خدمات الأمن السيبراني كفالة تحقيق والحفاظ على الخواص الأمنية للمنظمات وأصول المستعملين إزاء المخاطر الأمنية ذات الصلة في البيئة السيبرانية.

- **لحماية أمن المعلومات وتضييق الفجوة الإلكترونية أمام الاختراقات يستلزم الآتى:**

- **بنى تحتية موثوقة وآمنة.**
- **سياسات لخلق الثقة.**
- **إطار قانوني مناسب.**
- **إدارة الأدوات الأمنية للمعلومات وإدارة المخاطر.**
- **إدارة أمنية قادرة على خلق الثقة في التطبيقات والاستخدامات المقدمة.**
- **فريق متخصص قادر على إدارة كل ما ورد في أعلاه ومدرب تدريباً عالياً، وذو معلومات محدثة وعلى اتصال مع فرق مشابهة في بقية بلدان العالم.**

الأمن السيبراني (Cybersecurity): يُطلق عليه أيضاً **"أمن** المعلومات" و**"أمن** الحاسوب"، وهو فرع من فروع التكنولوجيا يُعنى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية التي تهدف عادة للوصول إلى المعلومات الحساسة، أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال أو تعطيل العمليات التجارية.

- أما في مرحلة ما بعد التسعينيات بعد عام ٢٠٠٠ فقد تطورت هذه الجرائم بنحوٍ أوسع، وتم استخدام المعلومات في الإرهاب المنظم من خلال ضرب البنى التحتية للدول سواء أكانت مرافق عامة أم خدمات أم البنى العسكرية والاقتصادية المتمثلة بالبنوك، وغيرها.

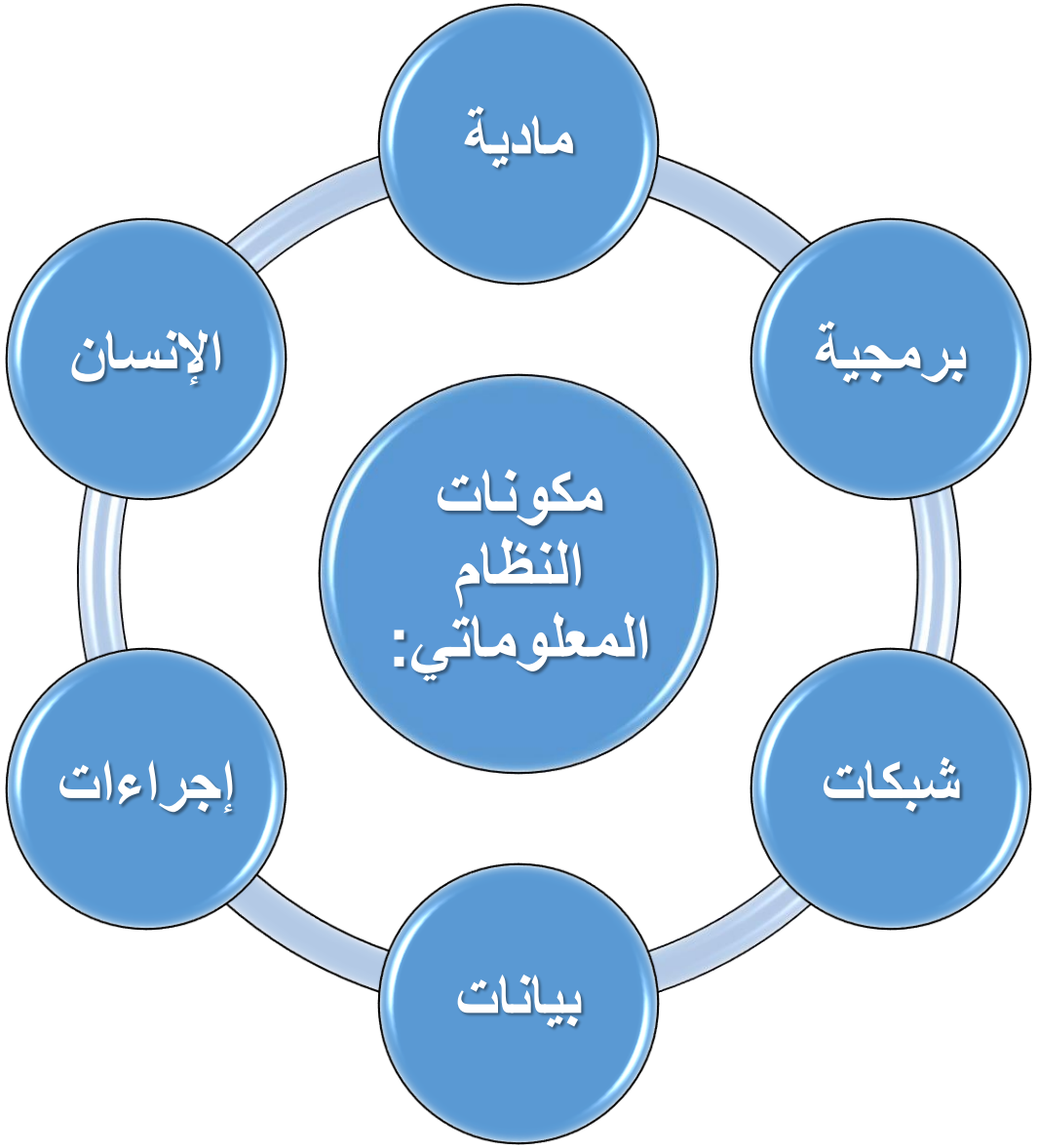
- الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. والأمن السيبراني هو سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول.

- وفي عصر التكنولوجيا أصبح لأمن المعلومات الدور الأكبر صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة، وأيضًا حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني.

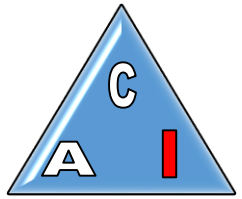
أو **(Cybersecurity)**ويُعرف المصطلح أيضًا باسم **أمن تكنولوجيا المعلومات (Information Technology Security)**أو **أمن المعلومات الالكترونية (Electronic Information Security)**. هي الممارسات والإجراءات المتّبعة لحماية الأجهزة الحاسوبية والخوادم والهواتف والأنظمة الإلكترونية والشبكات وقواعد البيانات من الهجمات الضارّة.

الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير ...

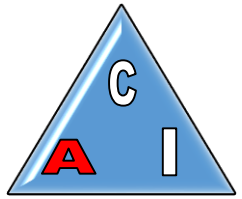
مكونات النظام المعلوماتي:



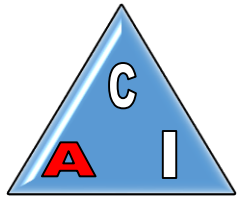
أركان أمن المعلومات :



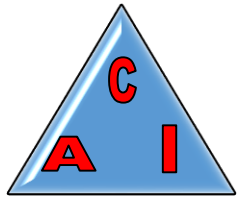
أخطاء مدخلين



حذف معلومات



الحرمان من الخدمة



الكراكر

عناصر أمن المعلومات

مفهوم أمن المعلومات

ما هو أمن البيانات المعلومات (Data Security)

هو العلم الذي يبحث في نظريات وأساليب حماية البيانات والمعلومات . ويضع الأدوات والإجراءات اللازمة لضمان حمايتها ويسهم في وضع التشريعات التي تمنع الاعتداء على المعلومات ومعاقبة المعتدين عليها.

عناصر أمن المعلومات

١- السرية.

تعني منع الوصول إلى المعلومات إلا من الاشخاص المصرح لهم فقط سواء عند تخزينها أو عند نقلها عبر وسائل الاتصال. وكذلك تحديد صلاحية التعديل والحذف والإضافة .

٢- السلامة.

المقصود بها أن تكون المعلومة صحيحة عند إدخالها ، وكذلك أثناء تنقلها بين الأجهزة في الشبكة وذلك باستخدام مجموعة من الاساليب والانظمة.

٣- التوافر والاتاحة.

تعني بقاء المعلومات متوفرة للمستخدم وإمكانية الوصول إليها. وعدم تعطل ذلك نتيجة لخلل في أنظمة قواعد البيانات أو وسائل الاتصال.

أمن المعلومات علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية.

- يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية

المبادئ الأساسية

من أهم المفاهيم، ومنذ أكثر من عشرين عاما، وأمن المعلومات قد حددت:

١- بالسرية سرية (مبدأ)

٢- والتكامل سلامة البيانات

٣- والتوافر تواجدية (المعروفة باسم الثالوث (سي آي ايه)(CIA)،

- (أعضاء InfoSec التقليديون الثالوث (-السرية والتكامل والتوافر)

ثالثا- مراحل تطور امن المعلومات

- ان مفهوم الأمن المعلوماتي مر بعدة مراحل تطورية ادت الى طهور ما يسمى بأمنية المعلومات ، ففي الستينات كانت الحواسيب هي كل ما يشغل العاملين في قسم المعلومات حيث لم يهتموا بأمن المعلومات بقدر اهتمامهم بعمل الاجهزة . بعد دلك ظهر مصطلح امن الحواسيب والدي يعني حماية الحواسيب و قواعد البيانات.
- وفي السبعينات تم الانتقال الى مفهوم امن البيانات Data Security ورافق ذلك استعمال كلمات السر البسيطة للسيطرة على الوصول للبيانات و حماية مواقع الحواسيب من الكوارث واعتماد خطط لخزن نسخ اضافية من البيانات والبرمجيات بعيدا عن موقع الحاسوب.
- وفي مرحلة الثمانينات و التسعينات ازدادت اهمية استخدام البيانات حيث تم الانتقال من مفهوم امن البيانات الي امن المعلومات حيث ان الاجراءات الامنية المناسبة يمكن ان تساهم في ضمان النتائج المرجوة وتقلص اختراق المعلومات او التلاعب بها.
- **وكانت شركة IBM الامريكية اول** من وضع تعريف لأمن المعلومات و اشارت الى ان امنا تاما للبيانات لا يمكن تحقيقه ولكن يمكن تحقيق مستوى مناسب من الامنية.

سابعاً: العناصر الأساسية لنظام الأمن المعلوماتي

أ. منظومة الأجهزة الإلكترونية وملحقاتها:

ب. الأفراد العاملين في أقسام المعلومات:

ت. البرمجيات المستخدمة في تشغيل النظام:

ث. شبكة تناقل المعلومات:

ه- مواقع منظومة الأجهزة الإلكترونية وملحقاتها:

التغلب على المشاكل المرتبطة بالتغذية الكهربائية

ضعف كلمات المرور، إن موثوقية كلمات المرور هي معيار التحكم بحق على أجهزة الحاسب Passwordوكلمة المرور IDالوصول إلى أنظمة الحاسب.

ثامناً: حماية نظام المعلومات

- **Controlling Accessالتحكم بالوصول**
- **جدران النار Firewall -**
- **-التشفير وفك التشفيرEncryption and Decryption-**
- **الحماية من المخترقين**
- **تجنب الخداع**
- **حماية مواقع التجارة الإلكترونية**
- **اعتماد بصمة الأصبع أو العين أو الصوت**
- **-Backupإجراء النسخ الاحتياطي**

تاسعاً: الخصوصية

المجالات أو الحالات التي تشملها خصوصية المعلومات:

١- تشمل الخصوصية أي معلومات عن الأشخاص مخزنة في أنظمة الدولة

٢- الخصوصية تشمل أجهزة الحاسب الشخصية (المحمولة أو المكتبية)

٣- تشمل الخصوصية أجهزة الهاتف المحمولة

٤- تشمل الخصوصية أيضاً المؤسسات والشركات وخصوصاً المصرفية

ويتم حماية البيانات وخصوصيتها كما يلي:

- التأكيد على حق الوصول
- استخدام كلمات المرور ومعرّفات الاستخدام دوماً
- استخدام التشفير للملفات أو عناوين جهات الاتصال
- لا تترك الجهاز مفتوحاً على بيانات هامة أو شخصية
- إذا قمت باستعراض بريدك الإلكتروني على جهاز حاسب عام)في مقهى انترنت مثلاً(لا تترك الحاسوب
- النسخ الاحتياطية :هامة وأساسية لحماية البيانات

إدارة امن نظم المعلومات:

احد وظائف الإدارة في المنظمة الناجحة، تعمل على التأكد من ان نظم المعلومات الإدارية تم تنفيذها حسب الخطط، ويعمل لتحقيق الأهداف التي وضع من اجلها، وان العمليات امنة من أي عبث او استخدام سي لها.

ويختص نظم امن المعلومات بثلاثة مناطق رئيسية هي (التطوير- التصميم- التشغيل).

خواص نظم امن المعلومات الفعالة:

١- السلامة

٢- القابلية للمراجعة المالية

٣- القابلية للمراقبة

فوائد نظم امن المعلومات:

١- الامتثال للقوانين والتشريعات والأنظمة وحمايتها

٢- تحسين الفعالة التشغيلية

٣- تخفيض التكاليف (ترشيد عمليات-تخفيض التكلفة والجهد والوقت واعمال الرقابة الفعالة)

٤- استرجاع المعلومات وقت الحاجة لها بجودة عالية وبصورة مستمرة

٥- تحقيق الميزة التنافسية (بنا الثقة والجدارة بين منظمات الاعمال)

تقنيات امن المعلومات:

- تفاصيل تطبيقات الرقابة الفنية لحماية السرية
- السلامة
- وتوفير المعلومات وحماية أصول (اجهزة) المعلومات
- ودراسة حماية الأدوات- وأساليب العمل- التكنولوجيا من التهديدات الداخلية والخارجية

مسؤوليات امن المعلومات:

- المحافظة على معيارية برامج الحماية مثل الجدران النارية
- منع توقف (تصلب) أنظمة التشغيل
- تعقب المتطفلين على الأنظمة
- حماية الشبكات المحاكية (الافتراضية) الخاصة

مسؤوليات أنظمة إدارة امن المعلومات وخصائصها: حدد معيار الايزو ٢٧٠٠١ الحقول الاتية:

-السرية
- التكاملية والسلامة
- الاتاحة
- عدم التنصل

تلك العناصر تمثل العناصر الأساسية لحماية أي نظام

المجالات الرئيسية الاحد عشر لأنظمة امن المعلومات: (تم إصدارها في عام ٢٠٠٥)

١- اشهار السياسة العامة لنظام امن معلومات المنظمة
٢- تنظيم امن المعلومات (التنظيم الداخلي والخارجي)
٣- إدارة أصول المنظمة
٤- حماية الموارد البشرية
٥- ادارة امن التجهيزات
٦- إدارة العمليات والاتصالات
٧- الولوج الى المعلومات
٨- امتلاك أنظمة المعلومات وتطويرها وصيانتها
٩- إدارة حوادث امن المعلومات
١٠- إدارة الاستمرارية في العمل
١١- الالتزام بالقوانين والانظمة

تهديدات امن المعلومات

١- انتحال الشخصية.

- في هذه الحالة يتم استخدام هوية المستخدم (اسم المستخدم وكلمة المرور) للحصول على معلومات سرية أو امنية أو مبالغ نقدية .
- يتم ذلك بعدة طرق منها :-
- ١- تخمين اسم المستخدم وكلمة المرور
- ٢- إرسال رسائل للمستهدفين يطلب منهم تحديث بياناتهم .
- ٣- إرسال رسائل للمستهدفين يطلب منهم تحديث بياناتهم
- ٤- استخدام أجهزة أو برامج تقوم بتسجيل كل ما يتم النقر عليه
- ٥- الاتصال مباشرة على المستهدفين.

٢- التنصت.

- يتم الحصول على المعلومات بهذه الطريقة عن طريق التنصت على حزم البيانات اثناء تنقلها عبر شبكات الحاسب .

فيدو عن امن وحماية أنظمة المعلومات

الفيروسات: أخطارها وأنواعها

ماهو الفيروس؟؟؟

كلمة فيروس أطلقت مجازا على برنامج حاسوبي يقوم بأعمال تخريبية في برامج الحاسوب والمعلومات المخزنة فيه . كمحتويات القرص الصلب وتغيير نظام تقسيمه، هذا بالإضافة الى تغيير بيانات نظام التشغيل وتخريب الرقائق الخاصة بذلك وبكل التطبيقات.

كيف ينتقل؟؟؟

يمكن أن ينتقل الفيروس عن طريق القرص المرن أو المتنكر أو الصلب أو عن طريق شبكة الانترنت.

٣- الفيروسات وانواعها:-

الفيروسات: برامج قام بتطويرها وكتابتها مبرمجين محترفين ، بهدف تنفيذ أوامر معينة في جهاز الضحية كإلحاق الضرر بالحاسب و ما يحتويه من بيانات أو فتح منافذ في الحاسب يمكن عن طريقها اختراقه أو مراقبته.

- هي رمز خبيث يعيد انتاج نفسة داخل الحاسوب

-عبارة عن برامج قام بتطويرها وكتابتها مبرمجين محترفين بهدف تنفيذ اوامر معينة في جهاز الضحية كإلحاق الضرر بالحاسب وما يحتويه من بيانات.

١- الفيروس / هو برنامج تنفيذي يهدف الى تحقيق اهداف محددة او إحداث خلل في نظام الحاسب.

٢- الدودة (worm) / سميت بذلك لا نها قادرة على نسخ نفسها والانتشار سريعا عبر وسائل الاتصال كالبريد الالكتروني .

٣- حصان طروادة (Trojan Horse) / سمي بالقصة الشهيرة لحرب مدينة طروادة وطريقة التغلب على جيشها من قبل اليونان .

٤- الاختراق / محاولة الوصول الى اجهزة وانظمة الافراد والمنظمات.

٥- برامج التجسس / نوع من الاختراق يقتصر على معرفة محتويات النظام المستهدف بشكل مستمر .

تحديدات أمن المعلومات

انتحال الشخصية

الفيروسات

التنصت

الفيروس

الدودة

حصان طروادة

الاختراق

التجسس

انتحال الشخصية

- استخدام هوية مستخدم ما (اسم المستخدم وكلمة المرور) للحصول على معلومات سرية أو أمنية أو مبالغ نقدية

التنصت

- التنصت على حزم البيانات أثناء تنقلها عبر شبكات الحاسب (تكون اسهل في حالة حزم البيانات غير مشفرة)

الفيروسات

- برامج قام بتطويرها و كتابتها مبرمجين محترفين ، بهدف تنفيذ أوامر معينة في جهاز الضحية كالحاق الضرر بالحاسب و ما يحتويه من بيانات أو فتح منافذ في الحاسب يمكن عن طريقها اختراقه و مراقبته

أنواع الفيروسات

الفيروس : برامج تنفيذية تهدف الى احداث خلل في نظام الحاسب

الدودة : سميت بذلك لأنها تقوم على نسخ نفسها والانتشار سريعاَ عبر وسائل الاتصال كالبريد الالكتروني.

حصان طروادة : ((سمي بذلك لأنه يذكر بالقصة الشهيرة لحصان طروادة حيث اختبأ الجنود اليونان داخله و استطاعوا اقتحام مدينة طروادة والتغلب على جيشها)) ،بالتالي فهذا الفايروس يكون مرفقاَ مع برنامج دون علم المستخدم و يهدف لسرقة البيانات و كشف كلمات المرور والحسابات المصرفية .

الاختراق: محاولة الوصول إلي أجهزة و أنظمة الأفراد أو المنظمات والشركات باستخدام برامج خاصة عن طريق ثغرات في نظام الحماية بهدف الحصول على معلومات أو تخريب تلك الأنظمة و الحاق الضرر بها .

التجسس : نوع من الاختراق يقتصر على معرفة محتويات النظام المستهدف بشكل مستمر دون الحاق الضرر به .

أنواع الفيروسات

الفيروس	تأثيره
فيروس رئيسي	يؤدي إلى تخريب المعلومات بشكل تدريجي بطيء.
فيروس ثانوي	يسبب تغييرا لواحد أو أكثر من الملفات القابلة للتنفيذ.
فيروس معتدل	يدمر جميع الملفات عن طريق إعادة التهيئة.
فيروس مبتدئ "عادي"	يقوم بالتكاثر ولا يسبب أي تخريبا متعمدا للأقراص.
فيروس غير محدد الضرر	يستهدف شبكات الكومبيوتر لمعرفة كلمة السر للمستخدمين.

الفيروسات وانواعها

١- برمجي:

يصيب ملفات البرامج التنفيذية

٢- فيروس ماكرو:

سلسلة من التعليمات ضمن مجموعة لأمر واحد بهدف اتمتة مجموعة معقدة او مكررة من المهام

٣- المقيم:

يتم تحميلة ضمن ذاكرة RAM

٤-الإقلاع:

يصيب سجل الإقلاع الرئيسي MBR

٥- فيروس المرافق:

يضيف برامج الى نظام التشغيل وهو تقليد لبرنامج نظامي

٦- الديدان:

برنامج صمم للاستفادة من ضعف تطبيق او نظام تشغيل بهدف الوصول الى الحاسوب

حماية الأعمال الالكترونية من الفيروسات

أولا: التشفير:

هو ما يشتمل على استخدام حسابات رياضية أو مفاتيح لتحويل البيانات إلى رموز مجمعة عند إرسالها ومن ثم فك هذه الرموز عند استلامها.. وهذه الوسيلة تسوق وتباع كمنتج مستقل.

ثانيا: رفض أو إعاقة الخدمة:

هي عبارة عن خطوات تتبعها المنظمات لغرض حماية نظم معلوماتها من هجمات اعاقة الخدمة من قبل الفيروسات.

ثالثا جدران النار:

هو عبارة عن حارس بوابة يقوم بحماية الانترنت والشبكات الحاسوبية الأخرى من التطفل عن طريق مصفاة أو نقطة نقل آمنة في الوصول من و إلى الانترنت.

أنواع تشفير الشبكات اللاسلكية

WEP/1

- 64 Bit يسمى بـ"التشفير المشترك "يتكون مفتاح التشفير من ١٠ خانات و يستخدم لكتابة الأرقام من (٠) إلى (٩) و الحروف الانجليزية من (A)إلى (F) فقط (تسمى بالارقام الست عشرية)
- 128 Bit يكتب مفتاح التشفير بنفس الطريقة السابقة و لكن يجب أن يكون طولها (٢٦) خانة تنتمي جميعها الى الارقام الست عشرية.

WPA/2 يتكون مفتاح التشفير من (٨) خانات يستخدم فيها جميع الأرقام و الأحرف الانجليزية .

WPA2 /3 مشابه تماما للنظام (WPA) لكنه يستخدم خوارزميات حديثة و أقوى للتشفير و يعد أفضل أنواع التشفير للشبكات اللاسلكية .

جرائم المعلوماتية:

- هي تعبير شامل يشير إلى جريمة تتعلق باستعمال إحدى وسائل تقنية المعلومات لغرض خداع الآخرين وتضليلهم، أو من أجل تحقيق هدف معين لجهة معينة.

- تُكبد جرائم المعلوماتية الحكومات والمنشآت خسائر تقدر بمليارات الدولارات سنوياً.

- في أحدى الدراسات التي أجريت على قطاع المصارف أن نسبة ٧٠% من هذه الجرائم تتم بتواطؤ المجرمين والمبرمجين وموظفي المصارف.

تصنيف جرائم المعلوماتية:

١. جرائم هدفها نشر المعلومات:

مثل الحصول على أرقام البطاقات الائتمانية، والحسابات المصرفية ومعلومات استخباراتية.

٢. جرائم هدفها نشر معلومات غير صحيحة:

مثل نشر المعتقدات الخاطئة أو التشكيك في القرآن والسنة.

٣. استخدام تقنية المعلومات كوسيلة لأداء الجريمة:

مثل تزوير بطاقات الائتمان والتحويل بين الحسابات المصرفية.

٤. جرائم لها علاقة بانتشار تقنية المعلومات:

مثل قرصنة البرامج الأصلية والتي تكون أسعارها ٥٠٠٠$ لتباع بأقل من ١٠$

المخترقون:

- هم أشخاص يتمتعون بموهبة وقدرة عاليتين على كتابة وتصميم البرامج، وفهم عميق لكيفية عمل الحاسب الآلي مما يسهل عليهم اختراق أنظمتها وتغييرها.
- **هناك نوعين من المخترقين:**

الأول : الهاكر (White Hat).

هم في العادة أشخاص فائقو الذكاء يسيطرون بشكل كامل على الحاسب، ويجعلون البرامج تقوم بأشياء أبعد بكثير مما صممت له أصلا. لذلك نجد أن بعض الشركات العملاقة توظف أمثال هؤلاء الهاكر لتستفيد من مواهبهم سواء في الدعم الفني، أو حتى لإيجاد الثغرات الأمنية في أنظمة هذه الشركات.

الثاني: الكراكر(Black Hat).

هم من يسخرون ذكائهم بطريقة شريرة، وهم يهتمون بدراسة الحاسب والبرمجة ليتمكنوا من سرقة معلومات الآخرين الشخصية، ويغير أولئك المخربون، أحيانا، المعلومات المالية للشركات، أو يكسرون أنظمة الأمان، ويقومون بأعمال تخريبية أخرى.

الفرق مابين الهاكر و الكراكر:

الكراكر:

١. يمتلك القدرة على اختراق أنظمة التشغيل والبرامج الغير مجانية والتلاعب في برمجتها وإعطاؤها رقم خاص لكي تعمل.
٢. ويقوم بكسر الأنظمة الأمنية لأهداف تخريبية، فقد يكون هدفه سرقة معلوماتك أو في أسوأ الأحيان القضاء على النظام المعلوماتي الإلكتروني، بشكل كلي.
٣. كثير منهم يقوم بسرقة البرامج و توزيعها مجانا لهدف، فمنهم من يضع ملف الباتش بين ملفات هذا البرنامج.
٤. الكراكر دائما عمله تخريبي ولا ينفع سوى نفسه أو من يدفع له.

الهاكر:

١. يحاول فقط أن يتعرف على كيفية عمل النظام والبرامج لكي يساعد في تطويرها وتحسينها.
٢. لديه القدرة الكاملة على اختراق أنظمة التشغيل عبر الانترنت.
٣. يقوم الهاكر بحل المشاكل و بناء الأشياء، و يؤمن بالعمل التطوعي.
٤. الهاكر دائما عمله بناء ومفيد و ينفع الآخرين.

أمثلة لمواقع مخترقة: وكالة الاستخبارات المركزية الأمريكية

الموقع المخترق

الموقع الأصلي

وسائل الحماية:

وسائل الحماية المادية:

وهي الأجزاء **المحسوسة** من وسائل الحماية.

من أمثلتها:

١. الكاميرات (الفيديو أو الفوتوغرافية)
٢. أجهزة الإنذار .
٣. الجدران والأسوار والمفاتيح.
٤. بطاقات دخول الموظفين.
٥. أجهزة اكتشاف الأصوات والحركة.

وسائل الحماية الفنية:

وهي تقنيات تحديد وإثبات هوية المستخدم وصلاحياته ومسئولياته.

من أمثلتها:

١. كلمة المرور.
٢. القياس الحيوي.
٣. التشفير.
٤. الجدران النارية.
٥. البرامج المضادة للفيروسات.
٦. التوقيع الالكتروني.

وسائل الحماية الإدارية:

وهي إعداد وصياغة سياسات أمن المعلومات وتتضمن:

- تشريعات داخل المنشأة لتنظيم أمن المعلومات وتحديد المسئوليات والأدوار.
- تحدد ما هو مسموح به وما هو غير مسموح به للتعامل مع المعلومات ومع نظم المعلومات.

من أمثلتها:

١. **اتفاقية صلاحيات المستخدم وقبول استخدام النظام.**
٢. **الخصوصية.**
٣. **كلمات المرور.**
٤. **البريد الالكتروني.**

- لاختيار كلمة المرور:

١. **يُفضل أن تحتوي على أحرف وأرقام.**
٢. **يُفضل أن لا تقل عن ٨ خانات.**
٣. **يُفضل أن لا تكون مشهور ومتداولة.**
٤. **يمكن استخدام معادلة بسيطة لإنشاء كلمة المرور، مثلاً**

نضع حرف ، ثم الرقم الأول، ثم الرقم التالي يكون ثلاثة أضعاف الرقم السابق وهكذا.

القياس الحيوي Biometrics:

- **BioMetrics** هي كلمة إغريقية مكونة من جزئيين "BIO" ومعناها الحياة و "METRICS" ومعناها قياس.

- والتعريف الدقيق **للقياس الحيوي** : هو العلم الذي يستخدم التحليل الإحصائي لصفات الإنسان الحيوية وذلك للتأكد من هويتهم الشخصية باستخدام صفاتهم الفريدة.

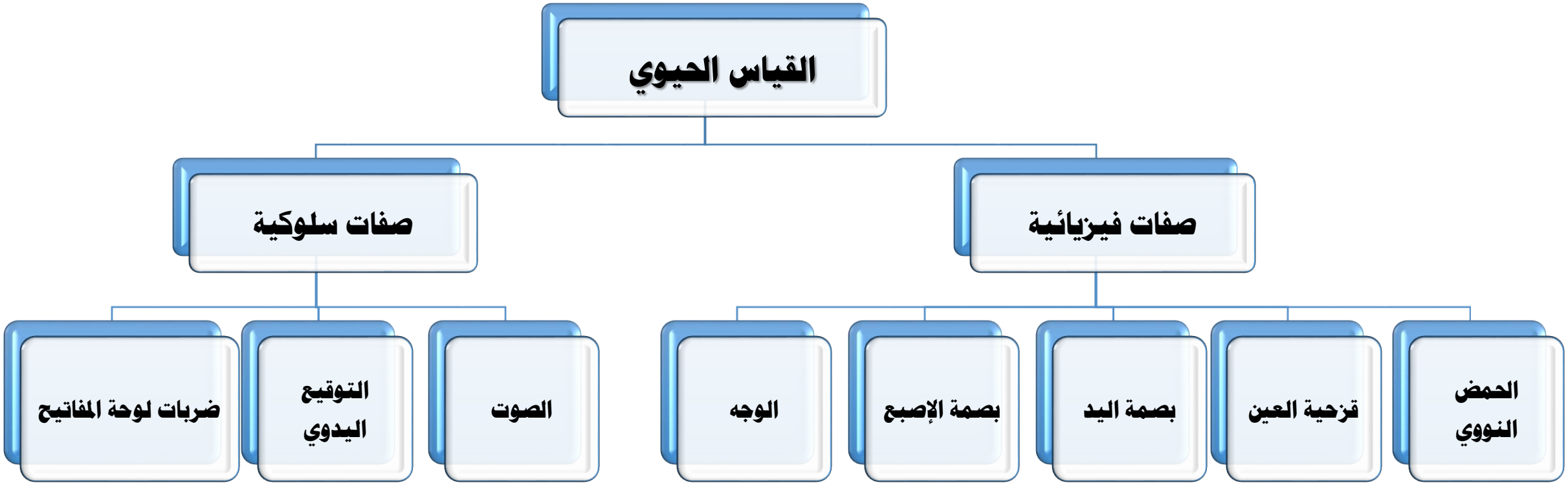
أقسام القياس الحيوي:.

١.الصفات الفيزيائية:

وهي الصفات التي تتعلق بجزء من جسم الإنسان.

٢.الصفات السلوكية:

وهي الصفات التي تتعلق بسلوك الإنسان.



مزايا القياس الحيوي:

* **يوفر لنا القياس الحيوي عدد من المزايا منها:**

١. الأمن والخصوصية:

- يمنع الأشخاص الآخرين من الدخول الغير مصرح على البيانات الشخصية.
- إيقاف سرقة الهوية،مثل استخدام البطاقات الائتمانية أو الشيكات المسروقة.

٢. البديل لحمل الوثائق الثبوتية مثل:

- بطاقة الهوية الوطنية. - رخصة القيادة. - بطاقة الائتمان.

٣. البديل لحفظ وتذكر الأرقام السرية.

٤. البديل لحمل المفاتيح للدخول إلى:

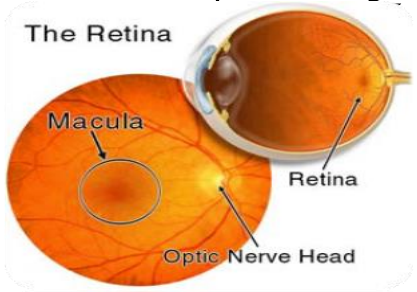
- السيارات. - المنازل. -المكاتب.

٥. تأمين سرية العمليات المالية مثل:

-مكائن الصراف الآلي ATM - التجارة الإلكترونية.

- **شبكية العين Retina Scanning:**

- هذه الطريقة تستخدم مصدر ضوء منخفض لعمل مسح للشعيرات الدموية خلف العين. عيب هذه الطريقة أن المستخدم يجب أن ينظر ويركز على الماسحة وهذا يسبب للمستخدم عدم الرغبة للتعامل مع النظام.



الوجه Facial Scanning:

هذا النظام يعتمد على أخذ صورة كاملة للوجه من آلة تصويرٍ، وقيام النظام بمقارنتها مع ما خزن فيه مسبقًا .مازالت هذه التقنية في أوج التطوير، وما هو موجود حالياً من الأنظمة المعتمدة على صورة الوجه لا تعطي دقة عالية.

- **الصوت Voice Verification:**

برامج تدقيق الصوت تعد من الإضافات الشائعة لأجهزة الكمبيوترات الخاصة لدى معظم الشركات والبنوك .لكن أنظمة القياس الحيوي ألمعتمدة على الصوت، فإنها تحلل ترددات الصوت بشكل أكثر دقة لكي تعطي نتائج صحيحة يُعتمد عليها .ولذلك يجب أن تكون بيئة هذا النظام هادئة، حيث أن أي ضجة تؤثر على النتيجة و أجهزة هذا النظام قد تكون مستقلة بحد ذاتها أو مدمجة مع أنظمة الهاتف التي قد تساعد في مجالات عديدة منها الأنظمة المصرفية.

- **التوقيع اليدوى Signature Verification:**

هذا النظام يعتمد على الطريقة التقليدية لتوقيع الشخص، ولكنها تتم من خلال توقيع الشخص على شاشة حساسة للمس باستخدام قلم ضوئي. ويتم من خلالها تحويل توقيعه إلى شكل رقمي ومن ثم مقارنته مع ما خزن مسبقًا في النظام.

الحمض النووى DNA Scanning:

هذا النظام يعتمد على الشريط الوراثي للشخص DNA. وهو نظام معقد جدًا ويستحيل تغييره بين الأشخاص، وهذا النظام مكلف جدًا لذلك قليلاً ما يُستخدم.

- **ضربات لوحة المفاتيح keystroke Dynamics:**

هذا النظام يقوم تسجيل ضربات الشخص على لوحة المفاتيح .ومن خلال هذه العملية يقوم بمراقبة الوقت بين ضرب مفتاح والانتقال الأصابع لضرب مفتاح آخر .

وكذلك يراقب الوقت الذي يأخذه المستخدم وهو ضاغط على المفتاح .وحيث أنه يجب على المستخدم أن يتذكر أسم المستخدم والرقم السري.

الحلول المقترحة

- تحليل العلاقات الخاصة بالموضوعات الأخلاقية والاجتماعية والسياسية التي تثيرها نظم المعلومات وتكنولوجياتها.
- تحديد الأبعاد والمبادئ الرئيسية لمجتمع المعلومات واستخدامها كمؤشرات للقرارات.
- تقويم تأثيرات نظم المعلومات والانترنت على حماية الخصوصية والممتلكات الفكرية.
- اجراء تقويم لتأثيرات نظم المعلومات على الحياة اليومية.
- تحديد التحديات الإدارية الأساسية لنظم المعلومات وتقديم الحلول.

- **لا يزل الجدل محتدم !!!**
- في وسط محاولات ايجاد التوازن بين السلامة العامة وتحقيق متطلبات الامن القومي من جهة وبين الحرية الفردية أو الخصوصية من جهة أخرى...

والأمثلة على ذلك كثيرة في كافة دول العالم.

*** كاميرات المراقبة :**

في الانفاق والموانئ والحدود والبنوك والمخازن.

*** قواعد البيانات:**

مثل قاعدة بيانات طلبات تأشيرات الدخول وقواعد البيانات الطبية ..

*** الأقمار الصناعية الرقابية:**

كالتي تستخدمها المخابرات الأمريكية CIA لمراقبة الأفراد.

*** صلاحيات المراقبة والتصنت الالكتروني :**

ومن أهمها صلاحيات وكالة التحقيقات الفيدرالية FBI للمراقبة أيضا.