جامعة الجزائر 3- ابراهيم سلطان شيبوط-
كلية علوم الإعلام والاتصال
قسم علوم الاتصال

مطبوعة خاصة بمحاضرات في مادة

الأنظمة المعلوماتية

السنة الثانية ماستر
تخصص: اتصال تنظيمي

الدكتورة دليلة العوفي

العام الجامعي: 2021/2020
جامعة الجزائر 3- ابراهيم سلطان شيبوط-

كلية علوم الإعلام والاتصال

قسم علوم الاتصال

رئيس المجلس العلمي	محافظ المكتبة

برنامج المادة وفق عرض التكوين

برنامج المادة وفق عرض التكوين:

- السداسي: الثالث
- اسم الوحدة: التعليم الأساسية
- اسم المادة: الأنظمة المعلوماتية

محتوى المادة:

المحور الأول: مفاهيم عامة حول أمن نظام المعلومات

1. مفهوم المعلومة
   - المعلومة هي أداة سند وتنسيق عمليات التسيير
   - المعلومة هي أداة اتصال داخل المنظمة(المؤسسة)
   - المعلومة هي حامل معرفة الأشخاص
   - المعلومة هي أداة ربط مع المحيط
2. مفهوم نظام المعلومات

3.مفاهيم حول أمن المعلومات وأمن نظام المعلومات

المحور الثاني: إستراتيجية أمن نظام المعلومات

- تقييم أهمية المعلومة من أجل حماية أفضل لها
- كيفية تحديد ما يجب أن يكون محمي؟
- ترتيب المعلومات حسب قيمتها وتقييم المخاطر

المحور الثالث: بناء سياسة أمن ملائمة

- تأمين نظام المعلومات
- التدابير الوقائية
- التدابير العلاجية

المحور الرابع: ماهي الأدوات التي نستخدمها لحماية أدنى لنظام المعلومات ؟

1. أدوات الحماية الأساسية
2. الحماية من الفيروسات. ماهو؟
3. جدار الحماية. ماهو؟

برنامج الوحدة

برنامج الوحدة: يتضمن برنامج الوحدة المحاور التالية:

مقدمة

المحور الأول: ماهية المعلومة وأهميتها في المنظمة

1. تعريف المعلومات
2. خصائص المعلومات وأبعاد جودتها
3. أنواع المعلومات ومصادرها
4. أهمية المعلومات في المنظمة

المحور الثاني: نظام المعلومات

1. تعريف نظام المعلومات.
2. مهام نظام المعلومات و دوره
3. مكونات نظام المعلومات وموارده
4. خصائص نظام المعلومات ووظائفه
5. مراحل تطور نظام المعلومات(أدواره)
6. دورة حياة نظام المعلومات
7. أهمية نظام المعلومات

المحور الثالث: أمن المعلومات

1. تعريف أمن المعلومات
2. المفاهيم المرتبطة بأمن المعلومات
3. مكونات أمن المعلومات (عناصره)
4. عوامل الاهتمام بأمن المعلومات
5. مخاطر أمن المعلومات
6. أبعاد أمن المعلومات

المحور الرابع: أمن نظام المعلومات

1. تعريف أمن نظام المعلومات
2. مواطن الخطر في بيئة المعلومات
3. مصادر الإخلال بأمن نظام المعلومات
4. أسباب الاعتداء على أمن نظام المعلومات(شن الهجمات)
5. أنواع المخاطر التي يتعرض لها نظام المعلومات:

- **الهجمات**
- **التهديدات**
- **الاعتداءات**

1. الأساليب المعتمدة للاعتداء على أمن نظام المعلومات
2. التدابير المتخذة لضمان أمن نظام المعلومات:

- الحماية الفيزيائية
- ضبط الوصول إلى الشبكة و إتاحة مواردها
- تشفير البيانات
- استخدام الجدران النارية
- برامج الحماية ضد الفيروسات
- النسخ الاحتياطي
- طمس البيانات
- الحماية من خلال الأشخاص

خلاصة

مقدمة

مقدمة:

يقاس تقدم المجتمعات اليوم بحجم امتلاكها للمعلومة والتحكم فيها، ففي إطار الشبكة المعلوماتية والمعرفية المعقّدة وإنتاجها أصبحت نواة التنظيم الاجتماعي تتمحور حول المعلومة بكل أنواعها، العلمية والتكنولوجية والإعلامية والاقتصادية والسياسية والتجارية وغيرها.

فقد أدى انتشار الأنترنت المذهل والولوج إلى الشبكة إلى تناول المعلومات بكل أصنافها وإلى تبادلها ونشرها بكل يسر دون الاعتراف بالحدود الجغرافية.

ونظرا للأهمية الإستراتيجية للمعلومة، قامت المنظمات باستحداث أنظمة معلومات تساعدها في اتخاذ القرارات الناجعة والفعالة وفي الوقت المناسب وتسمح لها بمواجهة المنافسة الشرسة لمختلف المنظمات.

لكن، نظرا للتطور السريع والمستمر الذي يشهده قطاع تكنولوجيا المعلومات والاتصالات، تتعرض المعلومات ونظام المعلومات لمختلف المنظمات إلى عدة مخاطر حقيقية تهدد أمنها على المستويين الداخلي والخارجي، مما يتطلب ضرورة توفير سبل الحماية وذلك عن طريق اتخاذ عدة تدابير وإجراءات من شأنها أن تساهم في بناء سياسة استراتيجية أمن المعلومات في المنظمة فعالة.

وعليه نظرا لأهمية المعلومات في المنظمة من جمعها وتخزينها ومعالجتها إلى استعمالها في اتخاذ القرار وكذا حمايتها من مختلف المخاطر التي يمكن أن تتعرض إليها سواء في بيئة المعلومات التقليدية أو في البيئة الرقمية، وبالتالي حماية نظام المعلومات الذي تم استحداثه والذي فرضته التطورات التي عرفتها تكنولوجيا المعلومات والاتصالات من مختلف المخاطر والتهديدات.

أعددنا هذه المطبوعة، لطلبة السنة الثانية، في طور الماستر، تخصص اتصال تنظيمي، علوم الإعلام والاتصال، تساعدهم على معرفة أهمية المعلومة الإستراتيجية في المنظمة ودورها في اتخاذ القرار وسبل حمايتها من أجل تحقيق سياسة أمن معلومات ناجعة وفعالة.

وقد جاءت هذه المطبوعة،على شكل أربعة محاور أساسية مثلما فصلناها في البرنامج المرفق.

حيث تناولنا في المحور الأول، ماهية المعلومة وكل ما يتعلق بها من تعريف وخصائص وأنواع مع إبراز أهميتها وبالتالي قيمتها الاقتصادية للمنظمة.

و تطرقنا في المحور الثاني من المطبوعة، إلى كل ما يتعلق بنظام المعلومات، وقدمنا في بداية المحور أهم التعاريف التي طرحها المختصون، ثم قمنا بتحديد مهام نظام المعلومات مع ابراز دوره، بالإضافة إلى تحديد مكوناته وموارده الأساسية، وانتقلنا بعدها إلى ذكر أهم خصائص نظام المعلومات ووظائفه، و كذا أهم مراحل تطوره ودورة حياته.

و قد خصصنا المحور الثالث من المطبوعة، للشق المتعلق بأمن المعلومات، وفيه قدمنا بعض التعريفات المتعلقة بمفهوم أمن المعلومات وبعض المفاهيم المتداخلة معه، ثم تعرضنا إلى مكونات أمن المعلومات، والعوامل المساعدة للاهتمام بهذا الموضوع الحساس سيما في وقتنا الراهن الذي تسيطر عليه تكنولوجيا المعلومات والاتصالات وفي الأخير ذكرنا أهم المخاطر التي تهدد أمن المعلومات.

و تركنا المحور الرابع والأخير، لأمن نظام المعلومات، حيث حددنا في البداية، مفهوم أمن نظام المعلومات، ثم تناولنا مواطن الخطر في بيئة المعلومات مع ذكر أهم مصادر الإخلال بأمن نظام المعلومات و أسباب الاعتداء عليها .

كما تطرقنا في المحور ذاته إلى أنواع المخاطر التي يتعرض لها نظام المعلومات والمتمثلة في الهجمات والاعتداءات والمخاطر مع التدقيق في تعريفاتها، و انتقلنا بعدها إلى الأسباب المعتمدة للاعتداء على أمن نظام المعلومات مع التدابير المتخذة لضمان أمنها.

المحور الأول

ماهية المعلومة وأهميتها في المنظمة

المحور الأول: ماهية المعلومة وأهميتها في المنظمة

سنتطرق في هذا المحور إلى ماهية المعلومة وأهميتها في المنظمة، باعتبارها الأساس الذي يعتمد عليها في اتخاذ القرار، وهذا من خلال تعريفها وتحديد خصائصها وأبعاد جودتها مع ذكر مصادرها وأشكالها وكذا أهميتها،وهذا ما نفصله آتيا:

1. تعريف المعلومة:

أثير جدل كبير حول تعريف المعلومات ولم يتفق على تحديد تعريف مشترك بين الباحثين وأهل الاختصاص، حيث فاقت تعاريفها 400 تعريف تستخدم في سياقات ومجالات مختلفة.

و سنركز في هذا المحور على المفهوم من وجهة نظر المختصين في حقل نظم المعلومات.

فهناك من يعرف المعلومات على أنها " نتاج معالجة البيانات حاسوبيا أو يدويا أو بالوسيلتين معا،وينتج عن عملية معالجة البيانات قيمة مضافة تتصف باتساق المعنى والدقة وجودة المعطيات التي تقود المستفيد إلى فهم الظاهرة أو المشكلة"[1]

و من المختصين من يعتبرها " بيانات تمت معالجتها و تحويلها إلى معلومات مفيدة ذات معنى تكون سهلة الاستخدام لاتخاذ القرارات الإستراتيجية"[2]

في حين اعتبرها آخرون "أحد مكونات التنظيم، تختص بجمع وتبويب ومعالجة وتحليل وتوصيل البيانات الملائمة لاتخاذ القرارات إلى أطراف خارجية وداخلية".[3]

---

[1] - سعيد غالب ياسين، **أساسيات نظم المعلومات الإدارية و تكنولوجيا المعلومات، 2005**، عمان،(الأردن) ،ط1 ، ص18

[2] – كاظم عبيس، تركي، **نظم المعلومات الإدارية و أهميتها في اتخاذ القرارات**،2010، مجلة جامعة بابل، العلوم الإنسانية، المجلد 18 ، العدد3 ، ص.ص 609-616

[3] محمد إسماعيل محمد السيد، **نظم المعلومات لاتخاذ القرارات الإدارية**،2001،المكتب العربي الحديث، الإسكندرية، (مصر)، 2001،ص37.

ولابد أن نميز بين **البيانات** و **المعلومات**،فبالرغم من أن بعض الباحثين يستخدمونها بشكل تبادلي إلا أنه لابد أن نميز بين المفهومين:

فالبيانات، يعنى بها " المادة الخام المسجلة كرموز والمستخدمة لتمثيل الأحداث وحالتها أو هي أرقام أو جمل وعبارات يمكن للإنسان تفسيرها أو تعليلها" [1] .

أما **المعلومات،** فيقصد بها تلك البيانات التي يتم تحويلها إلى مادة ذات معنى وقابلة للاستخدام من قبل المستفيد الأخير (صاحب القرار).

وهذا يعني أننا لابد أن ننظر إلى المعلومات كبيانات معالجة وموضوعة بشكل يعطيها قيمة عند المستخدم النهائي.

2. خصائص المعلومة وأبعاد جودتها:

تناول بعض الباحثين جودة المعلومات، وعبّر عنها آخرون بالخصائص والسمات الجيدة للمعلومات، وترتبط هذه الجودة بالكيفية التي يمكن بها استخدام المعلومات ودرجة الثقة بها، ولذا توجد علاقة طردية بين[2] قيمة المعلومات وجودتها فكلما زادت قيمة المعلومات زادت جودتها.وهذا ما نوضحه فيما يلي:

أ/ خصائص المعلومات:

لكي تكون المعلومات ذات قيمة ويستفيد منها صانع القرار في المنظمة، لابد من توفر عدة خصائص أساسية، نذكر البعض منها عل سبيل المثال– لا الحصر – فيما يلي:

- **الدقة و الوضوح:**

تعرف الدقة بنسبة المعلومات الصحيحة مقارنة بمجموع المعلومات المنتجة خلال فترة زمنية محددة مع مراعاة عدم وجود أخطاء أثناء إنتاج المعلومة أو تجميعها أو نقلها، كما يشترط في المعلومات أن تكون واضحة بمعنى أن تقدم للمستفيدين منها، دون أي لبس أو غموض

[1] – مصطفي ربحي عليان، **خدمات المعلومات**، دار صفاء،. 2010 عمان،(الأردن)، ص. 27

أو تعارض أو تناقض بالصورة التي تفي باحتياجاتهم مما يساعدهم في اتخاذ القرار الصائب.

وتتوقف دقة المعلومات على دقة البيانات، لذلك يجب الحرص من الأخطاء التي تقع خلال نقل البيانات أو معالجتها أو تسجيلها أو تخزينها، فقد تكون عرضة للخطأ أو للحذف أو التغيير عن قصد، لذا نجد معظم المنظمات خاصةبع انتشار تكنولوجيا المعلومات والاتصالات تسعى لتدعيم عملية الرقابة والمراجعة الداخلية والخارجية.

الملاءمة أو المطابقة:

تعد ملائمة المعلومات ومطابقتها لحاجات المستفيدين ومتخذي القرار العامل الرئيس في تحديد قيمة المعلومات الاقتصادية" فالمعلومات التي لا تلائم حاجات المستفيدين ومتخذي القرار تقترب قيمتها من الصفر بل إن التكاليف التي أنفقت في تجميع المعلومات وتحليلها اتساعها درجة زادت كلما المنتجة المعلومات قيمة وتزيد خسائر، الحالة هذه في تعتبر .القرارات ومتخذي لحاجات المستفيدين و متخذي القرارات " [1]

كما أن المعلومات الملائمة هي التي ترتبط بموضوع القرار وتؤثر على سلوك متخذ القرار وتجعله يعطي قرارا يختلف عن ذلك القرار الذي يصدره في حالة غياب المعلومات.

- **التوقيت المناسب:**

لا قيمة للمعلومات إن لم تكن متوفرة في الوقت المناسب، فلكي تكون المعلومات مفيدة ومؤثرة في اتخاذ القرار لابد أن تقدم في وقتها، فقد تكون المعلومة مفيدة في الزمن الحاضر وغير مجدية بعد فترة زمنية قصيرة، وترتبط هذه الخاصية أيضا بالزمن الذي تستغرقه دورة المعالجة– الإدخال وعملية المعالجة وإعداد تقرير المخرجات للمستفيدين.

[1] - همشرى أحمد، عمر، **المكتبة ومهارات استخدامها،2009**، دار صفاء لنشر والتوزيع، عمان، (الأردن)، .ص24 .

- **الاقتصاد:**

تعد اقتصاديات المعلومات من الأمور المهمة عند مناقشة موضوع المعلومات، وتكون المعلومات اقتصادية إذا كانت قيمتها أكبر من كلفتها، أما إذا كان العكس، فتكون المعلومات غير اقتصادية،و بالتالي تعد خسارة للمنظمة فلا جدوى منها .

- **الشمول:**

و يقصد به احتواء المعلومات المتوفرة أو المنتجة للحقائق الأساسية التي يحتاجها المستفيد أو متخذا القرار، بمعنى أن تكون المعلومات المقدمة كاملة و تغطي مختلف الجوانب التي يحتاجها المستخدم ، و هذا لا يعني إغراق المستفيد أو متخذ القرار بمعلومات كثيرة يختار منها ما يحتاج لأنه بذلك يضيع وقته ويقلل من قيمة المعلومات وفائدتها بالنسبة له،بل تقدم له في شكلها النهائي بصفة مختصرة و دقيقة.

- **عدم التحيز:**

ويقصد به غياب القصد من تغيير أو تعديل ما يؤثر على في معنى المعلومات وقيمتها أو محتواها،ما يؤثر على المستفيدين وتلبية رغباتهم.

- **الشكل:**

تملك المعلومات قدرة هائلة على التميع والسيولة و إعادة التشكل،إذ يمكن تمثيل المعلومات التي تحصلنا عليها في صورة أشكال مختلفة كجداول أو منحنيات بيانية أو دوائر نسبية أو أصوات ناطقة سيما في عصرنا الحالي الذي يمكن إدماج التطبيقات التكنولوجية المختلفة .

- **النقل:**

فالمعلومات لها قابلية النقل عبر وسائط معروفة كالكتب والدوريات والأسطوانات المدمجة و الأقراص المضغوطة وقواعد البيانات و مختلف الدعائم المتاحة.

- **الاندماج:**

حيث تتمتع المعلومات بقدرة عالية على الاندماج ، إذ يمكن بسهولة ضم عدة قوائم بيليوغرافية لمصادر المعلومات في قائمة واحدة أو تكوين نص جديد من أفكار يتم استنتاجها من نصوص سابقة .

- **الوفرة :**

تتسم المعلومات على أنها تنمو وتجدد وتخضع لقوانين العرض والطلب باعتبارها سلعة تباع و تشترى، فمن يملك المعلومة يملك سلطة القرار، مما أفرز مفاهيم أخرى جديدة (توليدية) كأباطرة المعلومات وسماسرة المعلومات ولصوص المعلومات وغيرها من المفاهيم التي تفرض على المنظمات وحتى الدول الاستثمار في حقل المعلومات إن أرادات فرض نفسها في مجتمع لا يؤمن إلا بالمعلومة.

ب/ أبعاد جودة المعلومات

تناول عديد الباحثين مفهوم جودة المعلومة، إلا أنهم لم يتفقوا على تعريف واحد لها، حيث طرحها كل واحد من زاويته الخاصة، حيث ركز البعض منهم على الخصائص الجيدة للمعلومات، وركز البعض الآخر على درجة الاستفادة منها سواء أكانوا أفراد أ منظمات، أما البعض من الباحثين، فلخصوا جودة المعلومات في الدقة والملاءمة والتكامل والوقت المناسب للحصول عليها.

وعموما ترتبط جودة المعلومة بقيمتها، فكلما زادت قيمة المعلومات زادت جودتها،وهذا ما يدفعنا إلى التركيز على كيفية استخدام المعلومة درجة الثقة فيها.

كما تتحدد جودة المعلومات بقدرتها على اتخاذ الفرد للقرارات الأكثر فعالية، وهذا لن يتأتى إلا بتوفر عدد من الخصائص النوعية من خلال **ثلاثة أبعاد** هي البعد الزمني، وبعد المحتوى والبعد الشكلي.

- **البعد الزمني:** يعتبر هذا البعد هام للغاية، حيث يصف الفترة الزمنية التي تتعلق بالمعلومات ومدى تكرارها وزمن استخدامها، أي يتضمن هذا البعد الجوانب المتعلقة بالتوقيت والآنية والتكرار والفترة الزمنية.
- **البعد الشكلي:** ويتعلق بكيفية تقديم المعلومات ويتضمن الجوانب المتعلقة بالتكلفة والتقديم (يمكن تقديمها بمختلف الأشكال: سدي، أرقام، بيانات...) والتفاصيل والسهولة والوضوح والترتيب والمرونة والوسائط المتعددة (تقدم في مطبوعة أو وسائط متعددة. .)
- **بعد المحتوى:** ويتضمن الجوانب التالية (الملاءمة والدقة والشمول والصدق والثبات والواقعية والمدى والأداء).

وبناء على ما ذكرنا، ذكر المختصون **ثلاثة عوامل أساسية تحدد جودة المعلومات** في المنظمة والمتمثلة في:

أولا: منفعة المعلومات:

وتتجسد في عنصرين أساسيين: صحة المعلومات وسهولة استخدامها، وهناك أربع منافع للمعلومات هي: منفعة شكلية، ومنفعة زمانية، ومنفعة مكانية ومنفعة التملك.

ثانيا: درجة الرضا عن المعلومات:

يعدّ هذا العامل أساسي في تحديد جودة المعلومات، حيث أن درجة الرضا عن المعلومات من طرف تتحدد في قدرتها على تحفيز متخذ القرار في أي منظمة ليتخذ موقعا معينا، وفي الوقت ذاته تجعل متخذ القرار يصل إلى قرارات أكثر فعالية.

ثالثا: الأخطاء:

فالكثير من المديرين يفضلون جودة المعلومات على كميتها، ولا شك أن جودة المعلومات تتفاوت باختلاف الأخطاء الموجودة في هذه المعلومات.

3. أنواع المعلومات ومصادرها:

تختلف تصنيف المعلومات وتحديد أنواعها من باحث لآخر، ويتوقف ذلك حسب مجالات الاهتمام ودرجة الاستفادة منها أو الغرض منها، كما تتعدد مصادر المعلومات بتعدد أنواع المعلومات التي تحتاج إليها المنظمة أو صاحب القرار وهذا ما نفصله تاليا:

أ/ أنواع المعلومات (تصنيفاتها):

هناك تصنيفات عديدة للمعلومات، تختلف حسب زاوية اهتمام الباحث بها، وهي تختلف حسب الحقول المعرفية وحسب الغرض من استعمالها وشكلها وحسب طبيعتها،و هذا ما نتطرق اليه فيما يلي:

أولا: تصنف المعلومات إلى:

- **معلومات إنمائية:** وهي المعلومات التي يحتاجها الإداري في تطوير قدراته والفكرية ومكاسبه المعرفية ومهاراته في العمل، مثل المعلومات التي يتحصل عليها خلال الدورات التكوينية أو المنتديات فترات التربص أو وهذا في أطار بناء القدرات البشرية.
- **معلومات إنجازية:** وهي تلك المعلومات التي يحتاجها المسير في اتخاذ القرار أو انجاز عمل أو مشروع ما، مثلما هو الأمر بالنسبة للمعلومات المتعلقة بشراء أجهزة الحاسوب للمنظمة، أو توسيع البنى التحتية أو توظيف عمال جدد.
- **معلومات تعليمية:** وهي المعلومات التي تحتاجها الإدارة في مختلف المنظمات التعليمية كالجامعات والمعاهد والمؤسسات التعليمية بمختلف أطوارها، وتتضمنها المناهج التربوية والتعليمية.
- **معلومات بحثية:** وهي المعلومات التي تشمل التجارب وإجراءاتها ونتائج الأبحاث وبياناتها، التي يمكن أن تكون حصيلة تجارب علمية أو حصيلة أبحاث أدبية.

ثانيا: درجة تصنيف المعلومات، ويعتمد هذا التصنيف في المنظمات عادة باعتبارها الخطوط التي يسترشد لتحديد درجة أهميتها وخاصة سريتها:

- **سري للغاية: TOP SECRET**

وهي أعلى درجات التصنيف، تصنف فيها الوثائق والمعلومات الحساسة جدا والتي لها تأثير كبير على سلامة المنظمة والتي تحاول جهات معينة الحصول عليها.

يقتصر توزيع معلومات هذه الدرجة على كبار المسؤولين عن مصالح المؤسسة في مجال الاختصاص، وتعطى النسخ الورقية من هذه المعلومات أرقاما متسلسلة وتسلم إلى أشخاص محددين بالاسم ولا يسمح لحامل النسخة نفسه بإفشاء معلوماتها.

- **سريSECRET** :الدرجة الثانية من حيث السرية ،

وتصنف بهذه الدرجة الوثائق الأقل أهمية والتي سوف تعرض المؤسسة للخطر عند انتهاكها من قبل غير المخولين، ويقتصر توزيع هذه المعلومات على أفراد مخولين رسميا بحق الاطلاع عليها.

- **CONFIDENTIAL:**

يتضمن جميع الوثائق التي يمكن أن تضر بمصالح المؤسسة أو التفاصيل التي ستكون محرجة للمؤسسة عند افشائها.

- **محدودRESTRICTED**

توجد هذه الدرجة في تصنيف بعض الدول والتي تطبق على المعلومات أو المطبوعات التي ربما لا تخلو من فائدة للجهات المعادية (المنافسة) والتي لا تفضل المؤسسة أن تراها منشورة في الصحف اليومية.

➢ **ب/ مصادر المعلومات:**

هناك نوعان من مصادر المعلومة في المنظمة، نوجزها فيما يلي:[1]

أولا: مصادر المعلومات الداخلية:

هي مختلف الوحدات التنظيمية والإدارية المكونة للمؤسسة وكذلك الأشخاص العاملين فيها، وتعطى هذه المعلومات إما بطريقة مباشرة أو من خلال النشرات والدوريات التي تصدرها المؤسسة، وتشمل الوحدات التنظيمية دائرة الموظفين، دائرة المشتريات، دائرة التخطيط، دائرة المبيعات، دائرة التسويق. ..

أما الأشخاص الذين يعتبرون مصادر المعلومات فهم المدراء، رؤساء الأقسام ،المشرفين، المستخدمين...

وتختلف المعلومات التي نتحصل عليها من مصادر داخلية من منظمة لأخرى، باختلاف الوظائف التي تمارسها وتعددها ويمكن أن تحتوي على: معلومات مالية، أو معلومات تتعلق بالمنتوج، أو معلومات تتعلق بالمشتريات، كما يمكن أن تتعلق المعلومات بالبحث والتطوير وغيرها.

وعادة تحتفظ المنظمة بمعلوماتها على شكل بيانات وتقارير لتستفيد منها في اتخاذ القرارات المتعلقة بالتخطيط وطريقة تصحيح الانحرافات في التسيير أو في التنفيذ وكذا إعداد السياسات الجديدة أو تطوير تلك الموجودة تماشيا مع المعلومات المتوفرة.

ولابد أن نميز بين نوعين من المعلومات، المعلومات التي هي في حالة السكون أو الثبات، وهي المعلومات لا قيمة لها لأنها غير مستغلة، وهي متوفرة في مختلف الدعائم الورقية منها والالكترونية كالكتب والأقراص وذاكرة الحاسوب أو في أرشيف المنظمات أو في المكتبات.

وبين المعلومات في حالة الحركية أو الديناميكية، وفي هذه الحالة تكون ذات قيمة، حيث تستغلها المنظمة وتستفيد منها لاتخاذ القرار.

[1] علي خلف حجاجحة، "**اتخاذ القرارات الإدارية** دار قنديل للنشر والتوزيع، عمان (الأردن)، 2009، ص 109 – 110

ثانيا: مصادر المعلومات الخارجية:

وتتمثل في المعلومات التي تتحصل عليها المنظمة من المحيط الخارجي وقد تكون أشخاص أو هيئات،وقد تكون حكومية أو خاصة، أو المراكز الخاصة بالبحث العلمي. ، وهي بذلك تشمل مصادر أولية وأخرى ثانوية.

أولا: مصادر أولية:

وهو الذي "يؤّمن المعلومات من منبعا الأساسي (مصدرها الأصلي) ،فهي تعبّر عن الحقيقة دون تحريف أو حذف، وتتميز بأنه تتصل بالمشكلة مباشرة مما يوفر لمتخذ القرار الوقت والجهد ويطمئنئه إلى مصادرها، ويتم تجميع هذه المعلومات من المصادر التالية"[1]

- الملاحظة:

يتم فيها الحصول على أجوبة جزئية لمشكلة معينة عن طريق ملاحظة للأحداث المرتبطة بها وهي توفر معرفة أولية عن المشاكل أو العمليات محل الاهتمام

التجربة:

من أجل التحكم أكثر في المعلومات تلجأ المؤسسات في بعض الأحيان للاعتماد على التجريب لتحديد كمية ونوعية هذه المعلومات، ويقدر ما كانت التجربة ناجحة بقدر ما يكون استغلال هذه المعلومات ذو فائدة

التقدير الشخصي:

نحصل على التقدير الشخصي من خلال المسيرين داخل المؤسسة كمدراء أو رؤساء الإدارات أو من خارج المؤسسة كمستشارين وخبراء

ثانيا: مصادر ثانوية:

وهي تلك البيانات التي يتم تجميعها من قبل من طرف جهات أخرى ويتم تعميمها لتكون جاهزة للاستخدام من قبل الأفراد والمنظمات، ومن بين هذه المصادر نجد:

[1] نادرة أيوب، نظرية القرارات الإدارية، دار زهوان للنشر والتوزيع، عمان، (الأردن)، 1997،ص2015.

- المطبوعات و المنشورات والدوريات الصادرة عن الجهات المختصة
- الهيئات الرسمية مثل الوزارات.
- الهيئات البحثية والعلمية
- النقابات المهنية والعمالية

وتكون هذه المعلومات الصادرة من هيئات حكومية، معلومات إستراتيجية ذات أهمية كبيرة بالنسبة للمنظمة، وتترك أثرا واضحا على قرارات المسيرين وفي صياغة استراتيجيات المنظمة وتحديد أهدافها وغاياتها.

ثالثا: بنوك المعطيات:

وقد ظهر هذا النوع من المصادر حديثا ،مع انتشار تكنولوجيا المعلومات والاتصالات، حيث تجمعها وتنظمها وتجهزها منظمات من كافة أنحاء العالم وتعرضها على مواقعها على شبكة الأنترنت الدولية، حتى يستفيد منها الجميع.

و نستنتج من هذه المعطيات بأن المنظمة تعرف تدفقا متنوعا للمعلومات، فهناك تدفقا داخليا وتدفقا من وإلى المحيط الخارجي،ولهذا نميز بين ثلاثة أنواع من التدفق للمعلومات:

- تدفق للمعلومات التي تم إنتاجها داخليا على مستوى المنظمة والتي يستفيد منها مختلف المصالح والأقسام والمديريات.
- تدفق للمعلومات التي تم إنتاجها داخليا على مستوى المنظمة والتي توجه للمحيط الخارجي.
- تدفق المعلومات التي تتحصل عليها المؤسسة من المحيط الخارجي والتي تحتاج إلى استخدامها.

فالمنظمة مهما كان حجمها تحتاج إلى معلومات من مصادر متنوعة، داخلية أو خارجية أو الاثنين معا وكذا بنوك معطيات، مما يؤكد **أهمية المعلومات** و**دورها** في المنظمة وهذا ما نوضحه في الآتي:

4. أهمية المعلومة في المنظمة:

تكتسي المعلومات أهمية بالغة في حياة المنظمات كونها من الموارد النادرة التي لا يمكن أن تستغني عنها في القيام بأعمالها ونشاطاتها المختلفة و المتعددة سيما في عصرنا الحالي الذي يتميز بتطور تكنولوجيات المعلومات و الاتصالات ، و تتضح هذه **الأهمية** في عدة نقاط نستعرض **الأساسية** منها فيما يلي:

- **المعلومة أساس القرار:**

تعد المعلومة عنصرا أساسيا لصنع واتخاذ القرار المناسب وحلا لمشكلات الخاصة بالمنظمة، فلكي يتخذ أي مسؤول بالمنظمة قراره لابد أن تتوفر لديه المعلومة، فهي تساعده

على توفير الأسس المقارنة والاختيار أو المفاضلة بين الحلول والبدائل لاختيار أفضلها وهذا ما يسمح– بدون شك–بتحقيق نجاحها والاستمرار في مجال نشاطها.

- **هي وسيلة تنسيق وفعالية:**

حيث يتم تبادل المعلومات في المنظمة بين مختلف المستويات الإدارية أوفي المستوى نفسه، هذا ما يسمح للمعلومة بأن تربط مختلف وظائف المنظمة فيما بينها. فالتدفق الجيد للمعلومات يكسب المنظمة الفعالية والتنسيق الجيد

- **المعلومات هي أداة اتصال:**

فهي أداة اتصال داخلية بين مختلف أفراد المنظمة، كما تسمح للمنظمة بأن تبقى على اتصال دائم بمحيطها،(مثل سبر أراء مستعملي متعامل الهاتف النقال موبليس).

المعلومات أداة لدعم التسيير:

فأي نشاط داخل المنظمة لابد أن يزود بالمعلومات (مثلنقص العمال،الإنتاج، التموين..)وهذا من خلال استحداث نظام معلومات يعتمد أساسا على جمع المعلومة وتخزينها ومعالجتها ونشرها

- **هي عامل تحفيز وإشراك:**

فبعض المعلومات تساهم بقدر كبير في تحفيز العمال، فحتى يتسنى للفرد أن ينمج في المنظمة يجب أن يكون على علم بقرارات وخيارات الإدارة وأهدافها المرجوة، كما يجب تزويدهم بتقرير يخص درجة كفاءتهم أو تبليغهم بالترقية في الدرجات أو تعيينهم لتمثيل المنظمة في مهام خارجية، مما يؤدي إلى بذل المزيد من الجهد والتفاني في العمل وإتقانه.وكذا الرفع من مستوى الأداء.

تعد المعلومات في وقتنا الراهن أصلا من أصول المنظمة مثل :الرأس المال والعنصر البشري والمواد الخام وغيرها،مما يتطلب من المسيرين و أصحاب القرار أن ينظروا إليها على أنها استثمار يمكن استغلاله استراتيجيا للحصول على مزايا تنافسية، وليس تكلفة يجب التحكم فيها.

- ✓ **هي أداه ربط مع المحيط:**

فالمعلومات تمكّن المنظمة من التعرف على التطورات المختلفة التي تحدث في بيئة عملها،والتي يمكن أن تؤثر عليها، وهذا ما يساعدها في التكيف معها والحفاظ على توازنها في المحيط العام.

- ✓ **المعلومات وسيلة رقابة:.**

إن توفر المعلومات في المنظمة تساعد بقدر كبير في فرض الرقابة الفعالة، وخاصة فيما يتعلق بمستوى أداء العمال الفعلي ومقارنته بالمعايير المعمول بها، ثم التصرف ة اتخاذ القرارات الصائبة.

وبصفة عامة، تساهم المعلومات في بناء استراتيجيات المعلومات سواء على المستوىالوطني أو الدولي.

المحور الثاني
نظام المعلومات

المحور الثاني:نظام المعلومات

مقدمة:

تهتم مختلف المنظمات الحديثة بإنشاء نظم معلومات خاصة بها خاصة مع انتشار تكنولوجيا المعلومات والاتصالات حيث زادت أهميتها باعتبارها جزءا أساسيا في عملية تصميم هيكل المنظمات بمختلف أشكالها.

وقد أدت ثلاثة أسباب رئيسية وهامة إلى إحداث تغيير جوهري في بيئة المنظمات وطبيعتها بأشكالها المختلفة، يتمثل السبب الأول منها في التوجه نحو عولمة الاقتصاد، أما السبب الثاني، فيتمثل في التحول من الاقتصاد الصناعي إلى اقتصاد مبني على خدمات المعلومات والمعرفة، أما السبب الثالث، فيتمثل في التغيرات التي حدثت في طبيعة المنظمات ذاتها.

ونظرا لهذه الأسباب المذكورة ،لا يمكن أن نتصور أي منظمة دون نظام معلومات خاصة بها، لأن ذلك يؤثر على أدائها وعلى كفاءة موظفيها ومردوديتهم، كما أنه يؤثر بشكل كبير على اتخاذ القرار الصحيح وفي الوقت المناسب. وهذا ما سنتطرق إليه في هذا المحور من خلال تعريف نظام المعلومات وإبراز مهامه الأساسية ، تحديد مكوناته وموارده، مع ذكر خصائصه وكذا مراحل حياته، والتطرق إلى مشروع النظام الوطني للمعلومات في الجزائر

1. تعريف نظام المعلومات:

اختلفت التعاريف وتعددت بشأن نظام المعلومات نظرا لاختلاف وجهات نظر الباحثين وتعدد حقولهم البحثية واهتماماتهم المعرفية والأكاديمية.، حيث اعتبره بعض الباحثين " بيئة تحتوي على عدد من العناصر التي تتفاعل فيما بينها ومع محيطها بهدف جمع البيانات ومعالجتها سويا حاسوبيا وإنتاج وبث المعلومات لمن يحتاجها لصناعة القرارات".[9]

[9]عماد الصباغ، جامعة قطر – الدوحة، **نظم المعلومات ماهيتها ومكوناتها**، ط1، الإصدار الأول، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، 2000، ص 11.

كما يعد نظام المعلومات أيضا " مجموعة من العناصر المترابطة معا والتي تعمل بشكل متكامل مع بعضها البعض لغرض تهيئة المعلومات إلى الإدارة لغرض انجاز أعمالها بشكل دقيق"[10]

في حين يعرفه البعض الآخر ب"مجموعة منظمة من الموارد: المادية والبرامج والأفراد والبيانات والعمليات التي تسمح باستقبال ومعالجة وتخزين وبث المعلومات في شكل نصوص وصور وأصوات في المؤسسة".[11]

"مجموعة من المسارات الرسمية لإدخال ومعالجة وتخزين المعلومة، قائم على أدوات تكنولوجية، التي تقدم سندا للمسارات المتعلقة بالمعاملات والقرارات وكذا لعمليات الاتصال المنبثقة من عمليات من متعاملي المنظمات والأفراد أو مجموعة من الأفراد داخل منظمة واحدة أو عدة منظمات".[12]

2. مهام نظام المعلومات ودوره في المنظمة:

أ/ مهام نظام المعلومات:

يؤدي نظام المعلومات عدة **مهام**، يمكن تلخيص **الأساسية** منها فيما يلي:

- جمع المعلومات التي تسمح بمعرفة ملائمة ومستمرة للسوق والفاعلين فيه بما يسمح للمديرين بتكييف القرارات الإستراتيجية التي يتم اتخاذها؛
- السعي للاستجابة لاحتياجات وردود أفعال المستهلكين؛
- الاستجابة لتطورات و نمو السوق ولتكنولوجيا المعلومات المتوفرة؛
- معرفة نقاط قوة المنافسين (المنتجات، الأسعار، حصص السوق)؛

---

[10] علاء محمد عبد الرزاق، محمد حسن السالمي، **الإدارة الإلكترونية**،2008، دار وائل للنشر، عمان،(الأردن)، ص 22.

[11] Henri Mahé de Boislandell , Dictionnaire de gestion : vocabulaire, concepts et outils , édition Economica, Paris, France, 1998, P 432 .

[12] **KefiAbdEssalem**, évaluation des technologies et systèmes d'information– cas d'un entrepôt de données implantédans une institution financière, **thèse de doctorat en sciences de gestion, université de Paris Dauphine, 2001, P38**

- العمل على نشر معرفة المعلومات ونشر اتخاذ القرارات.

ب/ دور نظام المعلومات في المنظمة:[13]

يلعب نظام المعلومات في أي منظمة عدة أدوار، إلا أن المختصين لخصوها في الثلاثة الأساسية:

- **دعم العمليات الإدارية:** مثل دعم العمليات المحاسبة، تنفيذ المعاملات وعمليات البيع والشراء والتخزين وغيرها
- **دعم صناعة القرارات:** ذلك من خلال تجهيز البيانات والمعلومات لكل المستويات الإدارية ولمختلف النشاطات من إنتاج وتسويق وتوظيف.
- **دعم الميزة التنافسية:** إن التفوق على المنافس هو الشغل الشاغل للشركات العالمية،فلا يمكن أن يتحقق ذلك دون معلومات دقيقة عن مواقف المنافسين وعن أحوال السوق، وعن التطور الحاصل في العلوم والتكنولوجيا، كل ذلك يحتاج إلى معلومات إستراتيجية تدعم قرارات الإدارة العليا.

3. مكونات نظام المعلومات نظم المعلومات وموارده:

أولا: مكونات نظم المعلومات:

- **المدخلات:**

وتتعلق بجمع وتوفير البيانات من داخل المنظمة أو من خارجها لغرض الاستفادة منها

- **العمليات:**

حيث تعمل على تحويل البيانات التي سبق جمعها لتصبح ذات معنى ودلالة.

[13] سليم حسنية، نظم إدارة المعلومات، منشورات الجامعة الافتراضية السورية، الجمهورية العربية السورية، 2018، ص 07، متاح على الرابط:
https//: pedia.svuonline.org، تم الاطلاع عليه بتاريخ 2021/05/24، على الساعة 07:30 .

- **المخرجات:**

وتتمثل في المعلومات ونقلها إلى الأفراد الذين يحتاجون إليها، وإلى الإدارات والأقسام والفروع عند ممارسة أعملهم ووظائفهم.

التغذية العكسية:

وتتمثل في ردود أفعال مختلف الأطراف التي استفادت من المعلومة، ومن ثمة تقييم مخرجات نظام المعلومات ووجود احتمالات للتعديل أو التغيير.

بناء على ما سبق ذكره، فإن نظام المعلومات الذي نقصده، هو النظام الذي يعتمد على المعلومات الإستراتيجية والهامة التي تسمح للمسؤول عن المنظمة أو المدير من حماية منظمته من كل خطر محتمل واغتنام كل الفرص المتاحة، وهذا لن يتأتى إلا عن طريق الاستثمار في المعلومة باعتبارها مورد نادر وبناء قواعد معطيات التي تتضمن كافة المعلومات الاستراتيجية التي تسمح بالتخطيط الاستراتيجي والتنبؤ والتفكير في إيجاد الحلول مع انتهاج أفضل الممارسات لاتخاذ القرار الاستراتيجي.

ثانيا: موارد نظم المعلومات:

يتكون نظام المعلومات من عدة موارد، باعتبارها أجزاء تضمن القيام بوظائفه على الشكل الصحيح، وتنقسم إلى خمسة موارد أساسية وضرورية في أي نظام والمتمثلة في:

الموارد البشرية: فأي نظام مهما بلغت درجة المكننة والآلية فيه، لابد وأن يلعب الأفراد دورا أساسيا فيه بصفته المشرف والمسيطر على كل عمليات النظام،ويتكون من المختصين والمستخدمين النهائيين.

أ- **المختص في نظم المعلومات:**

وهو الذي يصمم ويشغل ويحلل نظام المعلومات،

ويشمل كل من محلل النظام والمبرمج ومشغل الحاسوب،"ويقوم محلل النظام بالتصميم بالاستناد إلى الاحتياجات المعلوماتية للمستفيدين النهائيين، ويقوم المبرمجون بإعداد برامج

الحاسوب بناء على المواصفات التي يقدمها محلل النظم، كما يقوم مشغلو الحاسوب بتشغيل الحاسوبات الكبيرة والصغيرة ".[14]

ب- **المستخدم النهائي:**

هو الفرد الذي يستخدم نظام المعلومات التي ينتجها ويمكن أن يكون مدير،محاسب، مهندس.

2/ **الأجهزة: hardware**

وتتمثل في مختلف الأجهزة المادية المستخدمة في تشغيل المعلومات، إذ يفترض في أي نظام معلوماتي أن يكون مكونا من حاسوب على الأقل، ونظام الحاسوب يمكن أن يكون حاسوبا أو مجموعة من الحواسيب.

كما تشمل أيضا أوساط البيانات مثل الأقراص، وكذا الطابعات لاخراج المنتجات أو المعلومات.

3/ البرمجيات: software

هي الأنظمة التي تشغل الأجهزة والبيانات والمعلومات والمعارف وتحدد العمليات التي ستؤديها الأجهزة، وهناك نوعان:

أ- **برمجيات النظم:** وهي البرامج التي تشغل الحاسوب وتجعله قادرا على تنفيذ العمليات، مثل ترتيب العمليات واسترجاعها في الذاكرة

ب-برمجيات التطبيق: وهي التي تقوم بتشغيل بيانات المنظمة مثل برمجيات خاصة بالأجور،برمجيات خاصة بمعالجة النصوص.

ج-**الإجراءات:**

[14] عماد الصباغ، جامعة قطر – الدوحة، **نظم المعلومات ماهيتها ومكوناتها**، ط1، الإصدار الأول ،مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن،2000، ص 25

كافة الخطوات و التعليمات الواجب إتباعها لإنجاز العمليات الحاسوبية ، فمن متطلبات نظام المعلومات تحديد أساليب جمع المعلومات و تصنيفها و فهرستها و ترتيبها و تخزينها، بالإضافة إلى تحديد لوائح حفظ و إتلاف الوثائق و معايير تقسيم المعلومات و أنواع التقارير.

4/ قواعد البيانات:

هي الوعاء الذي يحتوي على كافة البيانات التي تصف كل العمليات التي والأحداث الجارية في المنظمة بكل التفاصيل المهمة الخاصة بنشاطها، على شكل ملفات مسجلة الكترونيا في النظام الآلي، وتكون وظيفة نظم المعلومات هي تحويل هذه البيانات إلى معلومات، لذلك لا يمكن لأي نظام معلومات أو مكونات حاسوبية أن تعمل دون بيانات؛

ويمكن أن تأخذ البيانات أشكالا مختلفة، كالشكل الكتابي التقليدي المتكون من الحروف والرموز والأرقام، أو على شكل بيانات نصية والتي تستخدم في المراسلات المكتوبة المختلفة، كما يمكن أن تكون على شكل بيانات صورية (image data)، مثل الأشكال البيانية والمنحنيات والجداول والدوائر النسبية والرسومات وغيرها، كما يمكن أن تتوفر البيانات كذلك على شكل فيديوهات أو بيانات فيديوية أو صوتية وغيرها.

5/ الشبكات: وتتمثل في الانترانت والاكسترانت ضرورية، وكذا شبكات الاتصال عن بعد من الحاسبات، ومختلف الأجهزة المتصلة بواسطة الاتصالات وكذا نظم تدعيم الشبكات التي تتمثل في جميع الأفراد والمعدات والبرامج وموارد البيانات التي تساهم مباشرة في تشغيل واستخدام شبكة الاتصالات مثل برامج تشغيل الانترنت.

فقد أصبحت المعلومات في عصرنا الحالي الذي تسيطر عليه تكنولوجيا المعلومات والاتصالات تحاج إلى أدوات تكنولوجية حتى تضمن حركيتها، مثل الحواسيب والبرمجيات والأجهزة المتنقلة والأنظمة الذكية والسماح بالاستفادة من بنوك المعطيات، وهذا ما يضمن

ايصالها إلى المستفيدين منها في الوقت المناسب وفي مدة قصيرة وبطريقة مؤمنة وغير مكلفة وذلك عن طريق استحداث شبكات اتصال وربطها بالأنترنت.

4- خصائص نظام المعلومات ووظائفه:

يتميز نظام المعلومات بعدة **خصائص** تعتبر بمثابة معايير مساعدة على تقييم كفاءته وفعاليته في المنظمة، كما أنه يؤدي عدة وظائف وهذا ما نتطرق إليه في الآتي:

أولا / خصائص نظام المعلومات:

أ- **المرونة و الديناميكية** : بحيث يمكن لمستخدميه إحداث التعديلات و التصحيحات اللازمة على النظام كلما اقتضى الأمر ذلك، بهدف مواجهة الاحتياجات الجديدة للمنظمة من المعلومات.

ب-**التكامل بين عناصر النظام:** هذا يعني أن نظام المعلومات يشكل وحدة واحدة متكاملة و متماسكة، الأمر الذي يسهل التفاعل السريع للمنظمة مع كل التغيرات الخارجية

ج-**تحديد التغيرات البيئية:** و يكون ذلك من خلال عملية الترصد و اليقظة المستمرة، لمساعدة المنظمة على اتخاذ القرارات التي تمكنها من استغلال الفرص المتاحة و في نفس الوقت تجنب العراقيل و التهديدات الخارجية

د- **التواصل:** حيث يعتبر نظام المعلومات بالمنظمة شبكة اتصال داخلية تضمن ربط جميع الأقسام و المصالح ببعضها البعض، و خارجية تسمح بتسهيل عملية الاتصال مع كل المتعاملين مع المنظمة.

ب/وظائف نظام المعلومات:

يقوم نظام المعلومات في أي منظمة بمجموعة من الوظائف، تتم بخطوات تمثل دورة تشغيل البيانات والتي تقم بتحويلها من مصادرها المتعددة إلى معلومات للمستخدمين، وتتمثل أهم هذه **الوظائف** فيما يلي:

أولا: جمع البيانات:

تبدأ وظيفة نظام المعلومات بجمع البيانات من مصادرها المختلفة وإدخالها، ثم إعدادها للتشغيل من خلال مجموعة من العمليات، وذلك حسب احتياجات المنظمة

ثانيا:تشغيل البيانات:

معالجة البيانات من خلال مجموعة من العمليات الأساسية لتحويلها إلى معلومات مفيدة لاتخاذ القرارات، وتتمثل هذه العمليات عادة في التصنيف والترتيب والعمليات الحسابية والمقارنة والتلخيص وأخيرا تقديم نتائج عمليات التشغيل.

ثالثا: إدارة البيانات:

ويقصد بها كل الأنشطة الخاصة بتنظيم وإدارة عمليات تخزين واسترجاع وإعادة إنتاج وتجديد وصيانة البيانات.

رابعا:رقابة وأمن البيانات:

وفي هذه المرحلة يقدم فيها مستخدمو نظام المعلومات ملاحظات على مخرجاته لكي تؤخذ في الحسبان في عمليات التشغيل الموالية، كما يتم في هذه المرحلة تقييم النظام والتأكد من أنه يعمل وفقا لإجراءات التشغيل المحددة ويولد معلومات بالخصائص المطلوبة.

وإذا لم تتوفر هذه الخصائص لابد من اتخاذ الإجراءات التصحيحية وإحداث بعض التعديلات اللازمة على المدخلات وعمليات التشغيل حتى ينتج النظام معلومات بالجودة – المطلوبة.

كما تتم في هذه المرحلة اتخاذ إجراءات متعلقة بأمن ومراقبة النظام هدفها اكتشاف أي فقد أو سرقة أو تزوير أو تغيير للبيانات أثناء عمليات التشغيل.

خامسا: تجميع وتوصيل المعلومات:

وفي هذه المرحلة يتم إنتاج المعلومات وتجميعها وتوصيلها للأشخاص المصرح لهم بالحصول عليها أو توصيلها لنظام آخر من النظم الفرعية المكونة للمنظمة في صورة

مفهومة وواضحة ومفيدة، شرط أن يتفق وسيلة وشكل أداة التوصيل ومضمون الرسالة وكيفية التعبير عنها مع رغبات واحتياجات مستقبلي المعلومة.

4. مراحل تطور نظام المعلومات(أدواره):

عرفت نظم المعلومات خلال تطورها عدة تغييرات ومراحل، وكل مرحلة منها تعكس الدور الذي يؤديه هذا النظام في المنظمة ،حيث انتقل من النظام البسيط الذي يعتمد على البيانات البسيطة إلى النظام الحديث الذي يعتمد على المعلومات الإستراتيجية كسلعة تضمن أرباحا طائلة للمنظمة وتضمن مكانتها في سوق التنافسية.

وقد لخص المختصون في هذا المجال، مراحل تطور نظم المعلوماتفي ست مراحل أساسية والمتمثلة في:[15]

مرحلة التركيز على البيانات:

وتعرف بمرحلة تشغيل البيانات، بدأت هذه المرحلة في منتصف الخمسينيات واستمرت حتى منتصف الستينيات من القرن الماضي، وعرفت هذه العملية أيضا بنظم معالجة البيانات **(Data ProcessingSystems)**، وهي النظم التي تؤدي عملية جمع البيانات التي تصف مجالات النشاطات المختلفة للمنظمة، ومعالجتها، وتخزينها لحين الحاجة إليها، وتلخيصها وعرضها في شكل تقارير تحتوي معلومات

يمكن استخدامها.

- **مرحلة التركيز على المعلومات:**

بدأت جذورها في نهاية الخمسينيات وبداية الستينيات من القرن الماضي، واستمرت إلى غاية ما بعد السبعينيات، حيث انتقل التركيز من تخزين البيانات إلى تحليلها واستخلاص النتائج منها. أي تخزين ملفات المعلومات لاسترجاع اختياري منها بعد إجراء معالجات عليها،

[15]سليم حسنية، نظم إدارة المعلومات، منشورات الجامعة الافتراضية السورية، مرجع سبق ذكره، ص 28، متاح على الرابط: https//: pedia.svuonline.org، تم الاطلاع عليه بتاريخ 2021/05/24، على الساعة 07:30 .

والحصول على ملخصات للبيانات المخزنة التي تصف الأنشطة العامة للمنظمة، سواء فيما يتعلق بما حدث في الماضي، أو ما يحدث الآن ،أو ما هو متوقع حدوثه في المستقبل،وعرضها على شكل تقارير دورية أو تقارير خاصة أو تقارير استقصاء عن نشاطات المنظمة، تساعد المديرين على اتخاذ قراراتهم.

- **مرحلة التركيز على نظم دعم القرارات:**

بدأت هذه المرحلة مع نهاية الستينيات من القرن العشرين،وفيها بدأ التركيز على إيجاد نظم تساعد المدير على اتخاذ قراراته في مسألة محددة أو غير مبرمجة مع الأنشطة العامة للمنظمة، وقد سمي هذا النظام بنظام دعم القرار

Decision Support System (DSS)

وظهر هذا النوع من النظام بعد انتشار استخدام الحواسيب في الدول المتقدمة في مجالات الإدارة، وأصبح كل فرد أو مدير يستطيع التعامل مع الحاسوب دون وسيط، أو متخصص في الحاسوب.

تطور هذا النظام لمساعدة فئات محددة أكثر تخصصا من المديرين، مثل نظم دعم الإدارة العليا (Executive Support System(ESS، وهي النظم المصممة لمساندة الادارات العليا في المنظمات، المسؤولة عن وضع الاستراتيجيات والخطط المتعلقة بمصير المنظمة.

- **مرحلة نظم دعم قرارات جماعات العمل: Group Decision Support System (GDSS)**

وهي نوع من أنواع نظم المعلومات الإدارية التي تدعم المديرين عندما يعملون على شكل جماعات (اجتماعات، كمؤتمرات) بالمعلومات التي يحتاجونها في مثل هذه المواقف والنشاطات، حيث تبين الدراسات أن أعمال المديرين غالبا ما تكون على شكل جماعي في المقابلات والاجتماعات واللقاءات متعددة الأطراف، ولهذا تحتاج إلى معلومات من طبيعة خاصة لا توفرها أنظمة المعلومات التقليدية.

- **مرحلة التركيز على نظم معلومات المكاتب:**

- **Systems(OIS)Office Information**

أو **نظم أتمتةالمكاتب (OAS) Office Automatisation System**

ظهر هذا النوع على أتمتة المكاتب في بداية، ولا يزال مستمرا.يهدف إلى تسهيل الاتصالات وزيادة إنتاجية العاملين فيها من خلال استخدام الأجهزة الالكترونية والرقمية. لكن هذه الفكرة بدأت أيضا في منتصف الستينيات، وذلك عندما ظهرت الكاتبات الآلية الالكترونية، ومن ثم ظهر ما يعرف بمعالج الكلمات بوساطة الحاسوب، وظهر ما يعرف بالبريد الالكتروني والرسائل الصوتية وكذا نقل المستندات الكترونيا.

- **مرحلة التركيز على النظم الخبيرة: (ES)Expert Systems**

ظهر التركيز على النظم الخبيرة في الإدارة في بداية التسعينيات، ويعتمد تطور هذا النظام على ما يعرف بتطور الذكاء الاصطناعAI Artificial Intelligence

وتنطلق فكرة هذا النوع من النظم من أنه يمكن برمجة الحاسوب لأداء أعمال منطقية بالطريقة نفسها التي يؤديها الإنسان، فالذكاء الاصطناعي يمثل أكبر تطبيقات الحاسوب رقيا وتقدما، وهي محاكاة السلوك الإنساني في حل المشكلات.

- **النظم المبنية على المعرفة: (KBS) Knowledge – Based Systèms**

يعتمد هذا النموذج في وقتنا الحالي، وهو يقدم النصح والمشورة لمستخدم النظام من خلال قاعدة معرفية كبيرة تعتمد على تقانة الشبكات العصبونية neural network، حيث يستشير المستخدم النظام ويطلب منه النصيحة، فيستجيب النظام لاستشارة المستخدم، ويقدم له النصيحة بناء على تغذية خبراء المعرفة.

وتجدر الإشارة إلا أنه في وقتنا الحالي وأمام التطور المذهل للانترنت ولتكنولوجيا المعلومات والاتصالات ظهر ما يسمى بنظم المعلومات الكوكبية أو (العالمية)

Global Information Systems(GIS)

5. دورة حياة نظام المعلومات:

يقصد بها أهم المراحل التي تتضمنها كل مرحلة في تطوير نظم المعلومات، فهي تسمح بالتحكم والرقابة وكذا ضمان الأهداف المسطرة مسبقا من طرف المسؤولين ومدراء المنظمات مع ضمان أن نظام المعلومات الذي تم استحداثه يفي يلبي حاجيات المنظمة.

وقد أجمع المختصون بأن دورة حياة نظام المعلومات تمر بخمس مراحل أساسية والمتمثلة في الدراسة، التحليل، التصميم، التنفيذ والإدامة، وهذا ما نفصله في الآتي:[16]

أولا: **مرحلة الدراسات الأولية:**

تعد الخطوة الأولى في إجراءات تحليل النظام، ويتمثل الغرض الأساسي منها" في تحديد ما إذا كانت المشكلة أو الاحتياجات الجديدة للمعلومات تتطلب مجهودا كاملا لبناء نظام معلومات جديد أو لتطوير النظام القائم أو استبداله بآخر ،أم هناك مسلكا آخر من العمل يكون مناسبا. وفي هذه المرحلة يقوم محلل النظام بفحص مدى الحاجة إلىنظام جديد للمعلومات من عدمه.

وتتضمن هذه المرحلة ثلاث خطوات رئيسية، هي:

- **تعريف المشكلة:**

وفي هذه الخطوة يتم التعرف إلى الاحتياج إلى نظام جديد أم الاحتفاظ بالنظام القائم، وهذا بعد دراسة كل المعطيات المتعلقة بالمرحلة.

- **دراسة الجدوى:**

فيها يتم " التحقق من الاحتياجات المعلوماتية للمستخدمين المتوقعين، بالإضافة إلىالأغراض والمحددات والمتطلبات الأساسية والكلفة والفوائد وجدوى النظام المقترح".[17]

[16] سليم حسنية، نظم إدارة المعلومات، منشورات الجامعة الافتراضية السورية، مرجع سبق ذكره، ص 72، متاح على الرابط: https//: pedia.svuonline.org، تم الاطلاع عليه بتاريخ 2021/05/24، على الساعة 07:30 .

بمعنى دراسة الجوانب الفنية والتقنية للنظام، من توفر الإمكانيات والبرمجيات القادرة على تلبية حاجيات النظام المقترح التي يمكن شراؤها أو تطويرها من قبل المنظمة في الوقت المطلوب وكذا مدى قبول المستفيدين من هذا النظام للمقترح قدرتهم على التعامل والتكيف معه، ونأخذ بعين الاعتبار التكاليف الخاصة بالمرحلة ،أي الحصول على الفوائد وزيادة الأرباح التي تتجاوز كلفة التطوير والتشغيل للنظام المقترح في إطار ما يسمى بالجدوى الاقتصادية.

- **تقرير الدراسة الأولية:**

وهي أول وثيقة يقوم بإعدادها محلل النظام، يلخص فيها الخطوتين المذكورتين سالفا (المشكلة الأولية والجدوى منها). أي النتائج المتوصل إليها والفائدة من النظام (سواء الذي طور أو الذي استبدل أو الذي تم بنائه).

ثانيا: مرحلة التحليل:

ويطلق عليها أحيانا مفهوم" **الدراسة الشاملة،** وهي دراسة تفصيلية معمقة للمستخدم الأخير واحتياجاته المعلوماتية قبل إكمال تصميم النظام.

وفيها يتم تجميع المعلومات المتعلقة بالمنظمة (الهيكل التنظيمي والإداري، مكوناتها البشرية، نشاطاتها ومهامها..والمنظمات الأخرى التي تتعامل معها).

وكذا المعلومات المتعلقة نظام معلوماتها (إنكان موجودا)، حتى نتمكن من معرفة وتحليل البرمجيات المستخدمة والموارد البشرية وكيفية استغلالها لهذه البرمجيات والنظام ككل.

ويتم في هذه المرحلة أيضا تحديد الاحتياجات أو المتطلبات المعلوماتية للمستخدم النهائي، ولا نقصد بها المتطلبات المادية وإنما المتطلبات المتعلقة بإدخال المعلومات وإخراجها (المحتويات، الرموز التوقيت، التكيف مع النظام، قاعدة البيانات، تأمين المعلومة...)

---

[17] عماد الصباغ، جامعة قطر – الدوحة، **نظم المعلومات ماهيتها ومكوناتها**، ط1، الإصدار الأول ،مكتبة دارالثقافة للنشر والتوزيع، عمان، الأردن،2000، ص 160

ثالثا: مرحلة التصميم:

،للبناء الجديد، أي بحث عن الحل للمشكلة التي Blue printيتم فيها وضع مخطط أولي عرضهاالتحليل.

تهدف هذه المرحلة إلى " تهيئة النظام وإعداده للتطبيق، إضافة إلى عملية اختيار المعدات والأجهزة والبرامج المناسبة لعملية التشغيل، ويجب على مصمم نظام المعلومات أن يأخذ بالحسبان العوامل المؤثرة في النظام الجديد، مثل موارد المنظمة، متطلبات المستفيد ومتطلبات الأجهزة والبرمجيات".[18]

ولابد أن تراعي في هذه المرحلة العوامل المختلفة المؤثرة في النظام الجديد كموارد المنظمة، ومتطلبات المستفيد وكذا متطلبات الأجهزة والبرمجيات.

رابعا: مرحلة التنفيذ (التطبيق):

تتضمن هذا المرحلة شراء المكونات المادية ووضع البرمجيات واختبار البرامج والإجراءات، فلا يمكن تشغيل النظام إلا بعد اختباره وتجريبه للتأكد من صحته وأن جميع البرمجيات تتوافق مع الأجهزة ومع بعضها البعض.

كما تشمل المرحلة أيضا اختبار قاعدة البيانات الخاصة بالنظام، بمعنى التأكد من أن محتويات قاعدة البيانات يمكن الولوج اليها بسهولة وتستجيب لمتطلبات المستفيد ويمكن أيضا تحديثها والحصول على بيانات منها.

كما تشمل مرحلة التنفيذ أيضا، تعليم وتأهيل الموارد البشرية أو بالأخرى بنائها(المستفيدين النهائيين والمتخصصين)حتى تتمكن من التحكم في تسيير نظام المعلومات بكل سهولة ويسر وأمان.

[18] سليم حسنية، نظم إدارة المعلومات، منشورات الجامعة الافتراضية السورية، مرجع سبق ذكره، ص 75، متاح على الرابط: https//: pedia.svuonline.org، تم الاطلاع عليه بتاريخ 2021/05/24، على الساعة 07:30 .

بعد مرحلة الاختبار، تبدأ مرحلة التنفيذ (النظام الجديد)، " الذي يتطلب خطة وجدولة سليمة لعملية التحويل ودراسة متأنية لاختيار الطريقة التي ستتم فيهلا عملية التحويل وتدريب الأفراد الذين سيشغلون النظام الجديد دون التأثير على سير عمل المنظمة "[19]

خامسا: التقييم والإدامة:

تتضمن هذه المرحلة تقويم النظام وتعديله أي إمكانية إجراء التعديلات عليه بمعنى "مراجعة ما بعد التنفيذ" لضمان أن التصميم الجديد يلبي أهداف النظام الموضوعة له، وتتضمن هذه العملية أيضا إجراء التعديلات على النظام والتي تكون مطلوبة نتيجة لأية تغيرات تحدث في المنظمة أو في البيئة التي تمارس فيها المنظمة عملها".[20]

فعملية صيانة النظام أو إدامته، مرحلة مهمة من دورة حياة نظام المعلومات في أي منظمة كونها تعتمد على المراقبة المستمرة للنظام بهدف الحفاظ على أدائه باستمرار.وهي " من أصعب مراحل تطوير حياة النظام ومن أكثرها استهلاكا للوقت، قد يصل إلى 70بالمائة من وقت المبرمجين. ذلك بسبب إهمال مرحلة الصيانة المبرمجة والمدروسة وندرة الأيدي العاملة في الصيانة.

6. أهمية نظام المعلومات:

يؤدي نظام معلومات في أي منظمة أهمية كبيرة تتمثل في:[21]

– تقديم المعلومات إلى الأقسام المختلفة بغية إصدار تقارير سواء كانت تجميعية أو تفصيلية– أو عن أنشطة المنظمة؛

[19] سليم حسنية، نظم إدارة المعلومات،، مرجع سبق ذكره، ص 80 .

[20] عماد الصباغ، جامعة قطر – الدوحة، **نظم المعلومات ماهيتها ومكوناتها**، ط1، الإصدار الأول ،مكتبة دارالثقافة للنشر والتوزيع، عمان، الأردن،2000، ص 170

[21] هارون العشي، فايزة بوراس، أهمية نظم المعلومات الادارية في تحسين عملية اتخاذ القرارات داخل المؤسسة، دراسة حالة شركة الدراسات وإنجاز الأعمال الفنية للشرق، باتنة، مجلة أبحاث اقتصادية وإدارية، المجلد 14، العدد 02، 2020، (**90–91**)

– مساعدة الإدارة في اتخاذ قرارات ناجعة و فعالة و صائبة، من خلال تهيئة المعلومات في الوقت المناسب؛

– تقديم تقارير تفصيلية شهرية أو فصلية أو سنوية عن نشاطات المنظمة؛

– المساعدة في تقييم نشاطات المنظمة و تقييم النتائج بغية تصحيح الانحرافات

– توفير المعلومات للإدارة و تهيئتها في الوقت المناسب لمساعدتها و تحفيزها على اتخاذ القرار الفعال و الصحيح، و استغلال مصادر المعلومات و مواردها داخل المؤسسة و إحكام السيطرة على المعلومات الواردة جميعها؛

– القدرة على تبادل و تشارك المعلومات و التحاور عبر الشبكات و الاتصالات داخل المنظمة و خارجها؛

– القدرة على حفظ و تخزين جميع المعلومات التي تتعامل بها المنظمة و معالجتها و إمكانية استرجاع القدرة على التخطيط و التنبؤ للمستقبل ضمن احتمالات مدروسة و اقتراح بدائل في حالة وجود خلل في تنفيذ الخطط و توقع احتياجات المنظمة المستقبلية الكفيلة بتحقيق الأهداف.

كما ضاف آخرون المهام التالية:

– تحسين القدرة على مواجهة الأزمات والتغلب على المواقف الصعبة وحل المشاكل بما يقلل من الخسائر ويحمي المشروع من تكاليفها الباهضة،

– يتميز هذا النظام بتوفيره للمعلومات عن البيئة، وهو بذلك يساعد في التعرف على الفرص المتاحة في البيئة وكذا التهديدات التي تواجه المؤسسة، كما يوضح نقاط القوة في المؤسسة والعمل على تدعيمها وتنميتها، والتنبيه إلى مواطن الضعف لكي تعمل المؤسسة على تصحيحيها وتداركها أو التقليل من أثارها السلبية.

– تحقيق المعايشة الفعلية والمعرفة الفردية بما يتم داخل المشروع وخارجه بما يكفل سرعة التدخل وفورية التواجد في مواقع الأحداث وقدرة التعامل معها والسيطرة عليها.[22]

[22] محمد أحمد الخضيري، **اقتصاد المعرفة**، مجموعة النيل العربية، القاهرة (مصر)، 2001، ص .ص 14.12.

المحور الثالث

أمن المعلومات

المحورالثالث: أمنالمعلومات

1. تعريف أمن المعلومات:

تباينت الآراء و وجهات النظر بين الباحثين فيما يتعلق بتحديد تعريف دقيق لمفهوم" أمن المعلومات"، بأبعاده المختلفة وأطره المتعددة ومجالاته المتنوعة، فمنهم من اعتمد على الجانب التقني، ومنهم من اعتمد في تعريفه للمفهوم على الجانب الأكاديمي ومنهم أيضا من اعتمد على الجانب القانوني، وهذا الاختلاف يعود أساسا إلى توجهات هؤلاء الباحثين الفكرية و ميولاتهم العلمية.

فأمن المعلومات من الزاوية الأكاديمية:

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

أما **من الناحية التقنية،** فيقصد بأمن المعلومات " الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية

في حين مازال أمن **الزاوية القانونية،** محل دراسات وتدابير حماية وسرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب جرائم الكمبيوتر والأنترنت.[1]

و عموما يقصد بأمن المعلومات " مجموعة من الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر البيانية (من أجهزة وبرمجيات وبيانات وأفراد)من التجاوزات والتدخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل أوكنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة من إدارة هذه المصادر"[2]

[1]خالد ممدوح ابراهيم، **أمن المعلومات الالكترونية**، الدار الجامعية، الاسكندرية(مصر)، 2008،ص27)

[2]دلال صادق، حميد ناصر الفتال، **أمن المعلومات**، دار اليازوري العلمية للنشر والتوزيع، الاردن، 2008، ص. ص 12.11

أو كافة الإجراءات المتخذة التي تهدف إلى الحفاظ على سرية المعلومات والأجهزة والبرمجيات

وكذا مختلف العاملين في هذا المجال.

من خلال التعاريف السابقة نستنتج أن أمن المعلومات يتجسد في:

- منع الذين ليس لهم صلاحية فبالحصول على المعلومة أو التعامل معها
- منع التعامل الخاطئ مع المعلومة
- تمكين الذين لهم الحق أو المسموح لهم قانونا التعامل مع المعلومة.

ويتداخل مفهوم أمن المعلومات مع بعض المفاهيم التي قد تصادفنا خلال بحوثنا ودراساتنا وأبحاثنا الأكاديمية في حقول معرفية مختلفة، لهذا نحاول أن نتطرق إليها باختصار حتى نزيل كل لبس فيما يأتي:

2. المفاهيم المرتبطة بأمن المعلومات:

أ- سياسة أمن المعلومات:

هي مجموعة من التوجيهات واللوائح والقواعد والممارسات التي ترشد إلى كيفية قيام المنظمة أو المؤسسة بإدارة وحماية وتوزيع المعلومات.[1]

ب- **نظم إدارة أمن المعلومات:**[2]هي جزء من النظام العام للإدارة، تقدم نموذجا مبني على منهج مخاطر أنشطة الأعمال لإنشاء وتنفيذ وتشغيل ومراقبة ومراجعة وصيانة وتحسين أمن المعلومات لتحقيق أهداف المنظمة.

[1] رؤى يونس، **دراسة واقع إدارة أمن نظم المعلومات في المؤسسات السورية ، مجلة جامعة البعث ،سوريا، المجلد 93 العدد31 ، عام 2017، ص 71.**

- [2] رؤى يونس، **المرجع نفسه ، ص 72**

ج/ المبادئ الأساسية لنظام إدارة امن المعلومات:

يتطلب نظام أمن المعلومات بعض المبادئ الأساسية لكي يكون تنفيذه ناجحا، نذكرها فيما يلي:[1]

- الوعي بالحاجة لأمن المعلومات
- تحديد المسؤولية عن أمن المعلومات
- تضمين وشمول التزام الإدارة واهتمامات أصحاب المصلحة
- تقييم المخاطر وبالتالي تحديد الضوابط المناسبة للوصول إلى مستويات مقبولة من المخاطر
- الوقاية الفعالة والكشف عن وقائع أمن المعلومات
- إعادة التقييم المستمر لأمن المعلومات وإجراء التعديلات تبعا لذلك.

3. مكونات أمن المعلومات (عناصره):

إن الحديث عن أمن المعلومات لا يقتصر على سريتها، بمعنى عدم الكشف عن المعلومات التي من المفروض أن تبقى سرا ويطلع عليها أو يستفيد منها فقط المخول له بذلك، لكن الحفاظ على سرية المعلومات لا يمثل إلا جانبا واحدا من جوانب أمن المعلومات.

ولهذا يرى المختصون في أمن المعلومات، بأنه لا يمكن أن نتحدث عن أمن المعلومات والهدف منها إلا بتوفير ثلاثة عناصر أساسية مجتمعة ومتكاملة والمتمثلة في **السرية أو الموثوقية، التكاملية وسلامة المحتوى** و**الموفورية** والتي اختصرت في اللغة الأجنبية في رمز CIA، وهذا ما نوضحه آتيا:

أ- السرية أو الموثوقية: CONFIDENTIALITY

ويقصد بها أن المعلومات لا تكشف من طرف أشخاص غير مسموح لهم بذلكولا يطلع عليها إلا من هو مخول له بذلك. فهذا الجانب من السرية " يشمل التدابير اللازمة لمنع إطلاع

[1] رؤى يونس، **مرجع سبق ذكره ، ص 72**

غير المصرح لهم على المعلومات الحساسة أو السرية ومن أمثلة المعلومات التي يحرص على سرياتها، المعلومات الشخصية والوضعية المالية للشركة والمعلومات العسكرية"[1]

ب/ التكاملية وسلامة المحتوى: INTEGRITY

وفي هذه الخاصية لابد أن نتأكد من أن المعلومات المتوفرة لم تخضع لأي تغيير أو استبدال في المراحل المختلفة من المعالجة بمعنى "لابد من التأكد من أن المحتوى لم يتم العبث به،أي أنه لم يتم تدمير المحتوى أو تغيير أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع". [2] مثل تغيير بعض أسماء المقبولين في مسابقة التوظيف الخارجي بالمنظمة واستبدالها بأخرى، أو تغيير مبالغ مالية لمنظمة معينة مثل رواتب العمال بدافع الانتقام من المسؤول أو صاحب القرار مثل تغيير الأرقام الخاصة بمردودية الموظفين، كتحويل 300000دج بدلا من 30000 دج، مما يؤدي إلى وضعية مالية صعبة للمنظمة أو إفلاسها.

ج/استمرارية توفر المعلومات أو الخدمة:AVAIBILITY

ويقصد بها التأكد من عملية استمرارعمل النظام المعلوماتي و تقديم الخدمة لمواقع المعلومات وأن مستخدم المعلومات لن يمنع من استخدامها أو دخوله لها.، فلا قيمة للمعلومات إذا كان من يحق له الاطلاع عليها لا يمكنه الوصول إليها، أو أن الوصول إليها يحتاج لوقت طويل.

نستنتج منهذه العناصر الثلاثة بأن المنظمات ملزمة علىتأمين معلوماتها وحمايتها من:

أولا: مخاطر الوصول غير المشروع:

---

[1] الغثبر خالد بن سليمان، القحطاني محمد بن عبد الله، **أمن المعلومات بلغة ميّسرة**، الطبعة الأولى، مركز التميّز لأمن المعلومات، جامعة الملك سعود، (المملكة العربية السعودية)، 2009)، ص 22

[2] أمن المعلومات، ماهيتها وعناصرها وإستراتيجيتها، متاح على الرابط:
https://www.academia.edu/36404855/%D8%A7%D9%84%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA_%D8%A3%D9%85%D9%86_Information_Security

وفي هذه الحالة نتحدث عن وصول موظفين من المنظمة أو خارجها إلى ملفات أو معلومات غير مسموح بها بهدف الاطلاع عليها أو تعديلها.

ثانيا: مخاطر الفقد أو التلف:

وتتمثل في مختلف المخاطر التي تؤدي إلى فقدان المعلومات أو الملفات أو إتلافها بسبب تغييرها أو حذفها أو تعديلها أو إحداث خلل بها بسبب أشخاص يمنع عليهم الوصول إليها (غير مخولين للوصول إلى المعلومة).

4. عوامل الاهتمام بأمن المعلومات

هناك عدة **عوامل** ساعدت على زيادة الاهتمام بأمن المعلومات بالنسبة للمنظمات أو للدول نذكر البعض منها فيما يلي:[1]

زيادة التعامل مع المعلومات مما يعرضها للمخاطر المختلفة من تعديل وحذف وتغيير وتزوير وغيرها

- ✓ اعتماد معظم القطاعات على نظم المعلومات وهذا ما جعلها معرضة لمخاطر مختلفة كالهجومات والاختراقات والقرصنة و.غيرها.
- ✓ التنافس الكبير في مختلف المجالات الاقتصادية والتكنولوجية والعلمية والفكرية والبحثية خاصة مع الانتشار السريع لتكنولوجيا المعلومات والاتصالات، وتدفق المعلومات، التي أفرزت مخاطر وتحديات عديدة ومتنوعة منها الجرائم عبر الانترنت
- ✓ زيادة انتشار المعرفة والمهارة في استعمال تكنولوجيا المعلومات والاتصالات مما زاد من نسب الهجوم لأسباب أو دوافع متعددة ،مثلما هو الأمر بالنسبة لبعض الشباب الذي يثبتون بأنهم يملكون مهارات للتحكم في أنظمة المعلومات والاعتداء عليها وتغيير محتواها..، أو بالنسبة للبعض الآخر الذي يعتدي المعلومات ويخترق أنظمة المعلومات بهدف ابتزاز صاحي الشركة أو المنظمة.

[1] محاضرات في أمن المعلومات وبرمجيات الحماية، كلية الدراسات العليا، جامعة النيلين، 2017.

5. مخاطر أمن المعلومات:

تتعرض المعلومة في بيئتها لعدة مخاطر تؤثر سلبا على مصادر المعلومة، سواء المعلومة في شكلها التقليدي أو في شكلها الالكتروني، وهذا ما نتطرق إليها في الآتي :

أولا: خرق الحماية المادية:

ويتم هذا الأسلوب عن طريق استخدام أربع تقنيات تساعد على خرق المعلومات من طرف المهاجم الذي يتبع الأساليب التالية:

أ/ التفتيش في المخلفات التقنية::) dumps ter diving

حيث يعتمد في هذه الحالة المهاجم على جميع مخلفات المؤسسة، ويسعى جاهدا إلى إيجاد المعلومات على مستوى المواد التي تركتها المنظمة، أو في القمامة التي تم الاستغناء عنها أو في سلة المهملات الخاصة بالحاسوب.

ب/ الالتقاط السلكيwiretapping:

وفيها يلجأ مخترق نظام المعلومات إلى استخدام التواصل السلكي مع الشبكة.

ج/ استراق الأمواجeavesdropping on émanations:

و في هذه الحالة يتم استخدام لاقطات لتجميع الموجات المنبعثة من النظم باختلاف أنواعها

د/ إلغاء الخدمة:

وفي هذه الحالة يقصد به الأضرار والعوائق التي تمنع تقديم الخدمة المطلوبة.

ثانيا :خرق الحماية المتعلقة بالأنظمة داخليا وخارجيا:

إذ نجد أن الجهة الداخلية تمثل أكبر مشكل لدى المنظمة، حيث أن اختراق وكذا مختلف الهجمات التي مست المعلومات يكون داخل المنظمة، إذ نجد أن المهاجم ينتمي إلى المنظمة ويعمل في إطارها الداخلي مما يصعب تفادي هذا النوع فهو يمثل الخطر الأكبر لأي مؤسسة كانت.

ثالثا :خرق الحماية المتصلة بالاتصالات والمعطيات:

- هجمات المعطيات : data attacks

في هذه العملية يتم التطرق إلي ثلاث برامج وهي [1]

- النسخ غير المصرح به للمعطيات : unauthorized copying of data :

و ينتج عن هذه العملية الدخول غير المصرح به للنظام، وذلك بالاستيلاء علي مختلف النسخ المتعلقة بالمعطيات وتتضمن المعلومات والبيانات والبرمجيات.

- تحليل الاتصالات : traffic analysis :

وفي هذه المرحلة يتم فيها التجسس على مختلف الاتصالات والارتباطات المتعلقة بالنظام، لإبراز نقاط الضعف لدى المستخدمين وممارسة مختلف أساليب الرقابة من اجل استخلاص فترة الهجوم المناسبة على حركة النظام.

القنوات المخفية : covert channels :

حيث يقوم المهاجم هنا بإخفاء مختلف المعطيات والمعلومات التي تم الاستيلاء عليها في موضع معين من النظام، وتعتبر صور من اعتداءات التخزين.

- هجمات البرمجيات: software attacks

توجد في هذا النوع عدة أساليب يتم بواسطتها الدخول إلى النظام ومحاولة تدميره وكذا الاحتيال عليه والعبث بمختلف الوظائف والمعطيات

الخاصة به، وهذا الاختراق يؤدي إلى الاستيلاء على معظم البيانات وكذا الوصول إلى البرامج بطريقة تقنية ومن بين هذه الأساليب نجد أن الشخص يستخدم طرق تقليدية وبسيطة لتنفيذ احتياله كاستخدامه للبرمجيات الخبيثة والمضرة بالمعطيات، إضافة إلى نقل المعلومات عبر أنفاق النقل...الخ.

رابعا :الهجمات والمخاطر المتصلة بعمليات الحماية.

تسعى هذه العملية إلى شن مختلف الهجمات التي تضر بالنظام كالعبث بالبيانات

[1] - منير محمد الجنبيهي، ممدوح محمد الجنبيهي، **أمن المعلومات الالكترونية**، دار الفكر الجامعي، الاسكندرية، مصر، (القاهرة)، ص 24.

ومحاولة تغييرها وخلق بيانات وهمية أثناء الإدخال أو الاستخراج، وكذا استخدام هجمات نشر الفيروسات على مستوى الانترنيت وإلهام المستخدمين بضرورة التقيد ببعض الخطوات من اجل حفظ بياناته وهذا الأسلوب شائع في مختلف استخدامات المؤسسات، إضافة إلى استخدام أسلوب المسح والنسخ الذي يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة مثلا :كلمة السر...الخ.

6. أبعاد أمن المعلومات:

يرتكز أمن المعلومات على عدة أبعاد نذكر منها:[1]

– إن أمن المعلومات مرادف لأمن الحاسب بمختلف مظاهره بما في ذلك امن الشبكات والحاسوب، أمن تكنولوجيات المعلومات وأمن نظام المعلومات ...، رغم أن معظم التعريفات ركزت فقط علي وجه الحصر في مختلف استخداماته غلي سبيل المثال حماية البيانات الالكترونية، وكل مفهوم متعلق بأمن المعلومات يعتبر فرع من فروع وبذلك تغطي البني التحتية والعمليات والخدمات والنظام وغيرها.

– يركز أمن المعلومات علي تأمين كافة موارد المعلومات في المنظمة وذلك من خلال جهود مبذولة لتحقيق غايات جوهرية إلا وهي السرية، والتوفر، السلامة، المسؤولية وقابلية التدقيق وتقوم إدارة امن المعلومات بتحقيق الحماية اليومية لضمان استمرارية العمل وذلك بتحديد المخاطر والتهديدات المترتبة عن هذه الأخيرة وكذلك وضع سياسة أمن المعلومات والتقيد والتنفيذ للضوابط والمعايير.

– إن أمن المعلومات بطبيعته ليس بالمحكم ولا المانع ولم يبلغ حد الكمال فلا يوجد من يقدر علي إزاحة خطر استخدام غير السليم أو المتقلب للمعلومات وكل ما عليه هو تناسب قيمة المعلومات مع مستوى أمن المعلومات المطلوبة.

– ضرورة وجود علاقة بين الجهات المسؤولة لضمان مشاركة جميع الأطراف بهدف تفعيل هذه المشاركة فمن الضروري جعل أمن المعلومات جزءا أساسيا من الوصف الوظيفي في

[1] محمد عبد حسين الطائي، ينال محمود الكيلاني، **إدارة أمن المعلومات**، دار الثقافة للنشر والتوزيع، عمان، (الأردن)، 2015، ص ص38 .42

المنظمة

– وجوب إستراتيجية ملائمة لأمن المعلومات في المنظمة والتي تتناسب مع طبيعة تكنولوجية المعلومات وتطبيقاتها في نظم المعلومات في شبكة الاتصالات المستخدمة داخل المنظمة ويتم تعديل هذه الإستراتيجية وفقا للتغيرات التي تحصل في هذه التكنولوجية مما يستوجب توفر خطة عمل شاملة لأمن المعلومات وذلك بسهولة الفهم والإدراك من قبل أعضاء المنظمة.

– هناك أنواع عدة لخروقات أمن المعلومات منها طرق اختراق أمن المعلومات ومجالاته، طبيعة عرض المعلومات وطرق المستخدمة في معالجتها، تحديثها واسترجاعها، وكذا توصيلها إلي المستفيد والرقابة عليها.

المحور الرابع
أمن نظام المعلومات

المحور الرابع: أمن نظام المعلومات

1. تعريف أمن نظام المعلومات:

قدمت عدة تعاريف لأمن نظم المعلومات، حيث عرفه المكتب الوطني الاسترالي للتدقيق AustralianNational Audit Office " بحماية أنظمة المعلومات بما تشمله البنى التحتية التي تسهل استخداماتها كالتقنيات والعمليات والخدمات والمعلومات.

كما يعرف أمن نظام المعلومات بأنه عبارة عن تلك " العمليات والتدابير والتوجيهات التي تصدرها إدارة المؤسسة بهدف حماية مواردها التقنية وما تحتويه من معلومات في مختلف أشكالها بغض تحقيق سلامتها وتوافرها وسرياتها وفق الصلاحيات و الترتيبات المتعارف عليها "

2. مواطن الخطر في بيئة المعلومات:

توجد أربعة مواطن أساسية تطالها المخاطر والاعتداءات في البيئة الرقمية تتمثل أساسا في:

- **الأجهزة:**

وهي كافة المعدات التي تتكون منها النظم، ومكوناتها الداخلية كوسائط التخزين وغيرها ولهذا وبهدف ضمان أمن المعلومات لابد من التأكد من أن الأجهزة تعمل بطريقة صحيحة

- **البرامج:**

سواء برامج التطبيق أو برامج النظم لابد من التأكد من عمل البرامج بصورة صحيحة ومرضية.

- **المعطيات:**

كافة البيانات والمعطيات في مختلف مراحل معالجتها، سواء في طور الإدخال أو التخزين أو الإخراج أو التبادل بين نظم المعلومات المختلفة عبر الشبكات، حيث تعدّ البيانات المخزنة أكبر مهدد أمني لنظام المعلومات الخاص بالمنظمة، فهي تتعرض لشتى أنواع الإتلاف أو التغيير أو الحذف أو التزوير.

- **الاتصالات:**

وتشمل مختلف شبكات الاتصال التي تربط مختلفة الأجهزة ببعضها البعض سواء محليا أو إقليميا أو دوليا.

لكن يبقى **الإنسان** هو محور الخطر في كل هذه العناصر، فقد يكون المستخدم أو الشخص الذي أسندت له مهام تقنية معينة في نظام المعلومات ،أكبر مهدد أمني لنظام المعلومات لأسباب مختلفة كالانتقام أو الإغراء أو الإهمال أو ضعف التأهيل.

فلكي نحقق أمن نظام المعلومات الشامل لابد من الشخص المكلف بنظام المعلومات أن يدرك حدود صلاحيته وآليات التعامل مع الخطر وكذ الرقابة على أنشطته في حدود القانون، سيما وأن البيئة الحالية ترتكز أساسا على قواعد البيانات والحوسبة السحابية مما يعرضها للخطر الدائم.

3. مصادر الإخلال بأمن نظام المعلومات:

تتعرض أنظمة المعلومات والمعلومات على حد سواء للاعتداء من جبهتين مختلفتين، واحدة داخلية وأخرى خارجية.

أ/ المهاجمونمن الداخل:

يعتبر الأشخاص الذي ينتمون إلى المؤسسات المصدر الأساسي للإخلال بأمن نظام المعلومات،لأنهم أكثر علم ودراية بالمعلومات الموجودة بنظام المعلومات وكذلك طريقة تصميم النظام نفسه وأهم الثغرات التي يمكن استغلالها ، بالإضافة إلى صلاحيات الدخول إلى المعلومات الممنوحة.

كما أن معظم المنظمات تهتم بتحصين أنظمة معلوماتها من الخطر الخارجي على حساب الخطر الداخلي إلي لا تعيره أي اهتمام أويكون الاهتمام بدرجة أقل وهذا ما يكلفها مبالغ باهضة بعد الحدوث الخطر.

وهناك عدة أسباب تدفع الموظف يعتدي على نظام معلومات المؤسسة التي ينتمي إليها والمتمثلة في الانتقام من المسؤول بسبب عدم ترقيته مثلا، أو لاثبات مهارته أو لأسباب مالية.

ومن **بين الأخطار** التي يمكن أن تحدث بسبب **الهجوم الداخلي:**

- مهاجمة الشبكة الداخلية للمؤسسة التي ينتمي اليها الموظف
- مهاجمة المعلومات بالسرقة أو التغيير أو الحذف
- فتح ثغرات في أنظمة الحماية التي وضعتها المؤسسة لتحصين أنظمة المعلومات

ونظرا لكون المهاجم من الداخل أقل عرضة للاحترازات الأمنية من المهاجم من الخارج، يمكن له أن يرتكب بعض الاعتداءات يصعب على المهاجم من الخارج القيام بها مثل:

أ/ تغيير تهيئة نظام المعلومات (_(Configuration) وخلق أبواب خلفية تسمح بنفاذ المهاجمين من الخارج

ب/ ردم الفجوة بين الشبكات المستقلة، فمعظم المؤسسات تقوم بصل شبكاتها الداخلية على شبكة الانترنت، حيث لا تضع في شبكة الأنترنت إلا المعلومات التي تريد أن يستفيد منها العالم الخارجي، في حين تحتفظ بمعلوماتها الإستراتيجية والمهمة في الشبكة الداخلية.

ويقوم المهاجم من الداخل بهدم هذا الفاصل بين الشبكتين، فيقوم مثلا بنقل بعض المعلومات إلى شبكة الانترنت أو نقل بعض البرامج الخبيثة كالفيروسات أو يقوم بتعطيل بعض خصائص أنظمة الحماية.

ب/ المهاجمون من الخارج:

و هم أشخاص من خارج المنظمة مثل قراصنة المعلومات لديهم دوافع مشتركة مع المهاجمين من الداخل، بالإضافة إلى أسباب أخرى دينية أو سياسية أو تجارية...ولهم عدة تصنيفات، لكن نعتمد على التصنيف الذي ركز على **الغرض من الاعتداء، وهم ثلاث فئات أساسية:**

❖ / **المخترقون:**

أ/ الهاركرز hackersles

الهاركرز أو المتسلل هو شخص بارع في استخدام الحاسب الآلي وبرامجه ولديه فضول في استكشاف حسابات الآخرين وبطرق غير مشروعة.

كان هذا المصطلح يطلق على الأشخاص الذين يملكون قدرات عالية المستوى في البرمجة، والذين يتميزون بقدرات إبداعية في معهد مساشوستس للتكنولوجيا، وكذلك المبرمجين المبدعين في ستانفورد وجامعة berkeley[1]

الهاركرز ، متطفلون يتحدون إجراءات أمن نظم الشبكات ، لكن لا تتوفر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي وإثبات الذات و هم عادة مراهقين و شباب عاطل عن العمل .

ويقصد بالقراصنة الهواة (الهاكرز) " مخترق شبكات الحاسب" وهي الفئة التي لا تشكّل أي خطورة على أنظمة المعلومات، هدفها هو التسلية والفضول و"أغلب هذه الطائفة هم من الطلبة والشباب الحاصلين على معرفة في مجال التقنية المعلوماتية، والباعث الأساسي لهذه الطائفة هو الاستمتاع باللعب والمزاح باستخدام هذه التقنية لاثبات مهاراتهم وقدراتهم باكتشاف وإظهار مواطن الضعف في الأنظمة المعلوماتية، دون أي إلحاق ضرر بها، هم لديهم الرغبة في المغامرة والتحرّي والرغبة في الاكتشاف".[2]

و" قد ظهر هذا الأسلوب في الولايات المتحدة الأمريكية، وشاع خاصة عام 1984 على يد جماعة Chaos Computer Club التي نشأت في مدينة هامبورغ الألمانية والتي كانت

[1] خليدة بن بعلاش،لخضر رابحي، **معالجة الجريمة المعلوماتية في ظل التعاون الدولي والاستجابة الوطنية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة،جامعة محمد خيضر، بسكرة، يومي 16 و17 نوفمبر 2015،ص 5.

[2] عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبوتر والانترنت**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص46.

مسؤولة عن عديد الهجمات الالكترونية التي استهدفت مختلف المواقع الحكومية بغرض إثبات وجود ثغرات أمنية على الشبكة وأن مفهوم الأمن المعلوماتي ما هو إلا مفهوم زائف".[1]

ولا يحتاج المخترقون إلى خبرات كبيرة ولا إلى احتراف "حيث أثبتت الدراسات أن 22 بالمائة فقط من الهجمات السيبرانية معقّدة وتحتاج إلى محترفين"،[2]

ويسعى "القراصنة إلى التخصص والتعاون في المشاريع البحثية وتقاسم البرامج والأخبار وكتابة المقالات وتعريف الآخرين بمجالات اختصاصهم. ويدع قراصنة الأنظمة نظاما خاصا لمجال المعرفة الذي يجذبهم ويسمح لهم بتطبيق ما تعلموه في أنشطة هادفة وإن لم تكن قانونية دائما.[3]

ب/ الكراكرز :القراصنة المحترفون: Crackers:

تتميز هذه الفئة بالخطورة، إذ تحدث أضرارا على الأنظمة المعلوماتية، وتعرف هذه الفئة عادة بالمخربين المهنيين، متخصصون في تقنية المعلومات، هدفهم هو تعطيل الحواسيب بهدف الحصول على المعلومات المخزّنة فيها.

وتعتمد هذه الفئة في اعتدائها على أنظمة المعلومات على" استخدام أسلوب القرصنة بالمنع من الاستخدام، بإرسال كم هائل من الحزم البيانية تجاه وصوب النظام المعلوماتي

---

[1]Patrick le Guyader, **Protection des données sur internet** , Edition, HERMES, Lavoisier, Paris, France, 2013, p102

[2]اللجنة الاقتصادية والاجتماعية لغربي آسيا ،(الاسكوا)، **الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية،(2015)**، ص2،الأمم المتحدة، نيويورك (الولايات المتحدة الأمريكية)، متاح على الرابط: https://www.unescwa.org/file/37236/download?token=fNPBBbGo، تم الإطلاع عليه بتاريخ 2021/05/30، على الساعة (06:00).

[3]عبد العالي الديربي، **الجريمة المعلوماتية: تعريفها..أسبابها..خصائصها**، المركز العربي لأبحاث الفضاء الالكتروني، 13 جانفي 2013، ص6.

المستهدف وذلك بشكل يفوق قدرته على التعامل معها مما يسبب ازدحاما معلوماتيا يؤدي إلى إحداث تذبذب في عمل الحاسوب أو الشبكة بصفة مؤقتة أو كلية"[1]

كذلك يستخدمون أسلوبا أخر يتمثل في "اتباع أسلوب نقاط الضعف الموجودة في النظام المعلوماتي واستغلالها في تعطيلها وشل النظام، وعادة ما يستهدف هذا الأسلوب مواقع الأنترنت من خلال جعلها غير متاحة لمدة مؤقتة أو بشكل كلي من أجل الولوج إلى مراكز إيوائها".[2]

وقد يعمد هؤلاء إلى استخدام أسلوب القرصنة باستعمال رسائل مجهولة (spam)وذلك عن "طريق إرسال رسائل البريد الالكتروني لضحاياه دون استئذانهم أو تواصل مسبق بينهم".[3]

وعادة ما تكون رسائل البريد الالكتروني "ذات طابع شخصي تخاطب المستخدم وتدعوه لزيارة مواقع معينة لأجل الإيقاع به والحصول على بياناته الشخصية.[4]

إن مثل هذه الرسائل ما إلا تمهيد لأهداف وغايات أخرى كتعطيل الحاسوب وتلويثه أو إغراقه بالفيروسات أو بهدف الاحتيال على الضحية.

تشكّل هذه الفئة تهديدا فعليا على الدول والحكومات والمؤسسات العسكرية والشركات العالمية ويتم تمويلها من طرف دول معينة ويتميز البعض منها بأنه منظمة على شكل مجموعات احترافية لديها قدرة كبيرة في الاختراق، حيث أبدى نحو" 44%من مستخدمي الأنترنت في دول منطقة الشرق الأوسط وشمال إفريقيا مخاوف كبيرة من تعرض حسابات بريدهم

[1]Nicolas Arpagian, **la cyber guerre**, **la guerre numérique a commencé**, édition Hermès, Science Lavoisier, Paris, France,2013,p 54

[2]Myriam Quéméner- Jean Paul Pinte **Cybersécurité** ,Edition Hermès science, Lavoisier, Paris, France 2013, p55.

[3]Patrick le Guyader- **Protection des données sur inter**net,op.cit , p 109.

[4]Myriam Quéméner- Yves Charpenel – **La Cybercriminalité**- Edition Economica- Paris-France- 2010- p 43

الإلكتروني أو غيره من الحسابات على الأنترنت للاختراق، وهذه النسبة هي أعلى قليلاً مما هي عليه في العالم عموما والتي تقدر بنحو 41%.[1]

ولا تتوقف عملية الاختراق على تغيير المعلومة أو سرقتها أو إزالتها فحسب بل تتعداها إلى تخريب الأجهزة وتعطيلها، وتحريف تصميم مواقع الأنترنت ومعلوماتها، فقد" أثبتت الإحصائيات التي قدمهاهيننغ فيغنر أن نسبة الاختراقات الخاصة بأنظمة البيانات قدرت بـ 62 %خلال الفترة 2013-2014".[2]

ج- الفريكرزphreakers:

وهي الفئة التي تقوم باستغلال شبكات الهاتف بغرض التصنت على مكالمات أو إجراء مكالمات مجانية وذلك عن طريق الدخول واستعمال خاصيات غير متاحة للمستعمل العادي للهاتف، حيث أن "بعض برامج التشغيل الخاصة بأجهزة الهواتف الذكية يسهل اختراقها وخاصة نظام" "الأندرويد" والذي يستخدم في أغلب أنواع الهواتف الذكية مثل "سامسونغ"، "سوني"، "أل جي" وذلك يعود إلى أن النظام ذو مصدر مفتوح ولا توجد فيه درجة كافية من الحماية"،[3]

---

[1] اللجنة الاقتصادية و الاجتماعية لغرب يآسيا،(الاسكوا)،**الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية، فبراير2015**،مرجع سبق ذكره، ص30

[2] هيننغ فيغنر، **الأبعاد الجديدة للمخاطر السيبرانية: انعاش القتال**، الأيام العربية للأمن السيبراني (السنة الخامسة)، مركز البحوث والدراسات القانونية والقضائية- جامعة الدول العربية- بيروت،1-2 ديسمبر 2015، ص3.

[3] هناء محمد، **كيف تعرف أن هاتفك مخترق أو مراقب**،متاح على الرابط: www.almarsal.com، تم الاطلاع عليه بتاريخ 2020/6/04، على الساعة (23:28).

حيث أثبتت الإحصائيات أن معدل نمو الاعتداءات والخسائر تجاوز 80% في بعض الحالات، إذ تذكر بعض الأرقام للفترة 2013–2014" أن الاعتداءات على الهواتف النقالة بلغت نسبة 93% وأن 38% من مستخدميها تعرضوا للاعتداءات.[1]

ويعتقد بعض الأشخاص أن استعمالهم للهواتف النقالة الذكية لا يتعرضون للاعتداءات وأن معلوماتهم مؤمنة، لا يمكن أن تخترق، عكس الذين يستعملون الحواسيب ويقومون بتحميل كل ما يحتاجون إليه وما يريدونه من الأنترنت في حين الواقع أثبت عكس ذلك حيث "أن مخاطر الهواتف النقّالة الذكية هي أكبر من مخاطر أجهزة الحاسوب التي تتمتع بحماية ضد الفيروسات والتجسس، لأن برامج الحماية في الهواتف النقالة ضعيفة؛ لا بل إن معظم التطبيقات على الهواتف الذكية هي من صنع أفراد لا شركات، وقد يخفون داخلها برامج احتيالية . كما أن شركات البرمجة هي أكثر سرعة في صنع التعديلات والتحديثات للبرامج وتوجيه التنبيهات للمستخدم على صعيد الحواسيب منها على صعيد الهواتف الذكية".[2]

❖ **المحترفون:**

تعدّ هذه الطائفة من بين أخطر مجرمي الحاسوب والانترنت تهدف اعتداءاتهم أساسا إلى تحقيق مكاسب مادية أو للجهات التي كلفتهم، كما تهدف اعتداءات البعض منهم إلى تحقيق أغراض سياسية أو دينية...

يتميز أفراد هذه الفئة بالتكتم عكس الأولى،(لا يتبادلون المعلومات فيما يخص نشاطاتهم، يطورون مكاسبهم المعرفية.) وتتراوح أعمارهم بين 25 و40 سنة.

---

[1] هيننغفيغنر، **الأبعاد الجديدة للمخاطر السيبرانية: انعاش القتال**، مرجع سبق ذكره، ص3.

[2] اللجنةالاقتصاديةوالاجتماعيةلغربيآسيا، (الاسكوا)، **الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية،(2015)**، مرجع سبق ذكره، ص49.

❖ **الحاقدون:**

الغرض الأساسي لأفراد هذه الفئة من الاعتداء على نظام المعلومات هو الانتقام والثأر (الموظف ضد مؤسسته) أو لا ينتمون إلى المؤسسة ولكن لديهم دافع للانتقام من هذه المؤسسة.

لا تملك هذه الفئة الاحتراف في التقنية، لكنهم يبذلون كل ما في وسعهم للحصول عليها، ويعتمدون في مختلف أنشطتهم البرامج الضارة وتخريب النظم وإتلاف المعطيات ،أو إنكار الخدمة

تتميز عناصر هذه الفئة بأنها لا تتفاعل فيما بينها، يعملون في السر ويعمدون إلى إخفاء أنشطتهم.

❖ **المخادعون: Fraudeurs:**

يتميز المخادعون بأنهم " يتمتعون بقدرات فنية عالية باعتبارهم من الاختصاصيين في المعلوماتية ومن أصحاب الكفاءات، وتنصب معظم جرائمهم على تحويل الأموال والتلاعب بحسابات مصرفية أو بفواتير الكهرباء والهاتف وتزوير بطاقات الاعتماد".[1]

ويستعمل الجاني في هذه الحالة أسلوب" التصيّد الالكتروني بهدف الحصول على البيانات الشخصية الخاصة بمستخدمي شبكات الأنترنت وذلك عن "طريق رسالة الكترونية في شكل مراسلة تحمل طابعا رسميا كمراسلات البنك أو أي مؤسسة مالية مشهورة وذلك من خلال الاستعانة ببياناتها الرسمية وعلاماتها المميزة وتدعوه هذه المراسلة الالكترونية إلى زيارة موقعها الالكتروني ولسبب غاية في الأهمية وذلك من خلال استعمال أسلوب التحذير

[1] وليد العاكوم، **مفهوم ظاهرة الإجرام المعلوماتي، مؤتمر القانون والكمبيوتر والانترنت**، المجلد الأول، كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية، مركز تقنية المعلومات، الإمارات العربية المتحدة، من 01 إلى 03 مارس 2000، ص 13.

والاستعجال ليتم تحويله بطريقة الغش إلى موقع مطابق للموقع الالكتروني الأصلي مما يسمح للجاني باسترجاع بياناته الشخصية بعد التسجيل"[1]

❖ **الجواسيس Espions:**

يهدف الجواسيس إلى جمع المعلومات لمصلحة جهة معينة ينتمون إليهاقد تكون شخصا أو مؤسسة أو دولة، وهي أخطر فئة كونها تتجسس في مختلف المجالات الحيوية مثل المجال الصناعي أو في المجال التجاري أو في المجال السياسي أو في المجال العسكري.

فتقوم هذه الفئة باختراق الأنظمة المعلوماتية للآخرين بهدف سرقة المعلومات وقد "يعترض المرتكبون خطوط الاتصالات السلكية واللاسلكية (البريد الإلكتروني أو اتصالات الصوت على الأنترنت).

ويتم هذا الأمر إما لغرض المتعة وإثبات المهارة، وإما لكشف أمور سرية وفضحها أمام الجمهور، وإما لبيع المعلومات نظرا لقيمتها التجارية أو لكشف أسرار مالية أو صناعية عن الشركات المنافسة، وإما لسرقة كلمات السر للحسابات المصرفية أو البريد الإلكتروني، أو لأسباب سياسية إذا كان موجهاً ضد دولة معينة "[2]

ولكن، في بعض الحالات لا يستطيع هذا المخترق أو المجرم الاعتداء على المعلومة و نظام المعلومات ، رغم استعماله عدة أساليب لأن ذلك غير كاف مما يستدعي **توفر وسائل وتقنيات ذات طبيعة إلكترونية في شكل برمجيات** يستعين بها للتسلل داخل الأنظمة المعلوماتية أو حذفها أو إجراء التعديلات عليها أو قرصنة المعطيات المخزّنة. فمع التطورات المذهلة والمستمرة التي تعرفها تكنولوجيا المعلومات والاتصالات، تطورت المخاطر والجرائم المعلوماتية وظهرت طرق جديدة لارتكابها حيث "ساهمت تقنيات الغفلية أو تقنيات إخفاء

[1]Myriam Quéméner– YvesCharpenel , **La Cybercriminalité**, op.cit, p50.

[2]اللجنةالاقتصاديةوالاجتماعيةلغربيآسيا،(الاسكوا)، **الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية،(2015)**،الأمم المتحدة، مرجع سبق ذكره، ص 71

الهوية الحقيقية للمستخدم وتنامي تسويق البرامج المعلوماتية التي يستخدمها المخترقون في للاعتداء على أمن المعلومات .

ولم يعد المخترقون يحتاجون إلى خبرات كبيرة، لأن برامج الاختراق أصبحت متوفرة وجاهزة . وقد أظهرت إحدى الدراسات أن 22% فقط من الهجمات السيبرانية معقّدة وتحتاج إلى محترفين،[1] مما يعني أن التطورات التي عرفتها تكنولوجيا المعلومات والاتصالات ومختلف تطبيقاتها التي تتطور باستمرار ساهمت بقدر كبير في الاعتداء على أنظمة المعلومات، وهذا بدوره يؤكد، بأنه كلما تطورت التكنولوجيا تطورت إفرازاتها السلبية.

إذ يلجأ المخترق لأنظمة المعلومات إلى استعمالالبرمجيات التي أعدّت لهذا الغرض، وهو ما اصطلح عليها باسم **البرمجيات الخبيثة أو برامج الدودة**،إذ أكدت بعض التقارير العالمية لشركات مختصة بأنه،تم اكتشاف ما لايقل عن 6.5 مليون برنامج ضار جديد عام 2013 فقط.

4. أسباب الاعتداء على أمن نظام المعلومات: (العناصر الضرورية للاعتداء)

هناك عدة أسباب تساعد على الاعتداء على أمن نظم المعلومات، ويعتبرها المختصون في أمن المعلومات أيضا عناصر والمتمثلة في الثلاثة الآتية:

أولا: وجود الدافع:

وتوجد دوافع متعددة، قد تكون للحصول على مكاسب مالية(مثل ابتزاز الأشخاص أو المنظمات عبر الانترنت)، أو الانتقام من الجهات المستهدفة (الموظف الذي لا يستفيد من الترقية في منظمته)، أو بدافع المنافسة (كأن تطلب شركة من شخص قرصنة موقع الشركة المنافسة لمنع وصول الزبائن إليها) وأحيانا يكون الدافع هو رغبة المهاجم إثبات قدراته الفنية والتكنولوجية.

[1] اللجنةالاقتصاديةوالاجتماعيةلغربيآسيا ،(الاسكوا)، **الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية،(2015)** ،الأمم المتحدة، مرجع سبق ذكره، ص2،

- **الحصول على مكاسب مادية:**

تدفع الحاجة بالبعض إلى البحث عن مختلف الأساليب في شبكة الأنترنت لتحقيق الثراء السريع مثلما هو الأمر في حالة استعمال بطاقة سحب مزورة يدفعه للقرصنة أو السرقة أو الاختلاس عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع غير المكلف، لذا " نجد أن الدافع للاعتداء على أمن نظام المعلومات يمكن أن يكون مجرد سداد الديون المستحقة أو مشاكل عائلية راجعة للنقود أو إدمان ألعاب القمار أو المخدرات لذا فإن بيع المعلومات المختلسة هو نشاط متسع للغاية"[1]

وقد أشارت إحدى المجلات المتخصصة في الأمن المعلوماتي إلى أن الرغبة في تحقيق الثراء من بين العوامل الأساسية للاعتداء، حيث أن": 43% من حالات الغش المعلن عنها قد بوشرت من أجل اختلاس الأموال و23% من أجل سرقة المعلومات و19% إتلاف و15% سرقة وقت الآلة أي الاستعمال غير المشروع للحاسب الآلي لأجل تحقيق أغراض شخصية".[2]

وقد توصلت السلطات القضائية المختصة في الجزائر بعد دراستها لمختلف القضايا التي حولت إليها من طرف السلطات المختصة إلى" أن الكسب المادي يمثل ما نسبته 65%من الدوافع التي أدت إلى ارتكاب الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات خلال الفترة (2005-2010)".[3]

---

[1] عبد العال الديربي: **الجريمة المعلوماتية: تعريفها..أسبابها..خصائصها**، المركز العربي لأبحاث الفضاء الالكتروني، تم الاطلاع عليه عبر الرابط: www.accronline.com، بتاريخ 2021/04/10على الساعة (22:00)

[2] ليلى حسين، **فعالية القوانين الوطنية والدولية في مكافحة الجرائم الإلكترونية**، قسم القانون في الأكاديمية العربية في الدانمارك، ص08،https://platform.almanhal.com، بتاريخ 2021/04/25، على الساعة (22:00)

[3] قراءة في الاحصائيات التي قدمها عبد الرزاق بن سالم في في مداخلة له بعنوان **المنظومة التشريعية الجزائرية في مجال محاربة الجريمة المعلوماتية**، مقدمة في إطار المائدة المستديرة حول"**الجريمة في الفضاء السيبيراني وسبل الوقاية منها**"التي نظمتها وزارة البريد وتكنولوجيات الاعلام والاتصال، يوم 2013/06/27 بمركز البحث للإعلام العلمي والتقني، الجزائر العاصمة.

كما قد يكون الدافع لأغراض سياسية، مثلما حدث في 27 مارس 2003لموقع قناة الجزيرة الذي تعرض للقرصنة، حيث اعتقد المهاجم بأن القناة انحازت للعراق اثناء الغزو الأمريكي لها،حيثوضع العلم الأمريكي في موقع القناة وتحته شعار "دعو االحرية تدق ناقوسها"

- **العوامل الاقتصادية والاجتماعية:**

والتي تلعب دورا هاما في زيادة الاعتداء على أنظمة المعلومات، حيث يؤدي الضغط على مؤسسات القطاع الخاص إلى التقليل من النفقات وخفض مستويات التوظيف، وإجبار الشركات على توظيف متعاقدين من خارج الشركة أو توظيف عمالة مؤقتة ثم أن يصبح العمال في حالة استياء من خفض رواتبهم والخوف من فقدان الوظيفة كل هذا عوامل تزيد من الأعمال الإجرامية الفردية ومن نفوذ الجماعات الإجرامية المنظمة غير المطلعين على شؤون الشركة".[1]

فقد عبّرت بعض الشركات المتخصصة في الأمن المعلوماتي أن التهديدات المحتملة أثناء فترة التراجع الاقتصادي تتمثل في الموظفين السابقين الذين قد تم تسريحهم لوجود فائض في العمالة".[2]

مما يعني أن الأفراد الذين يفصلون من شركاتهم وهم يملكون المعلومات اللازمة والمعرفة الكافية بمختلف الملفات الحساسة والمهمة لهذه الشركات التي كانوا ينتمون إليها، يرتكبون الجريمة ضدها رغبة منهم في الانتقام مما يكبّدها خسائر مالية كبيرة، فقد أثبتت الإحصائيات الناتجة عن دراسات أجريت على بعض المؤسسات التي تعرضت للاعتداءات أن "35 بالمائة من الجرائم المعلوماتية التي تعرضت لها هذه المؤسسات ناتجة عن أفراد

[1] الاتحاد الدولي للاتصالات، شعبة تطبيقات تكنولوجيات الإعلام والاتصالات والأمن السيبراني، دائرة السياسات والاستراتيجيات، قطاع تنمية الاتصالات،**فهم الجريمة السيبرانية، دليل للبلدان النامية**، مشروع أفريل 2009، مرجع سبق ذكره، ص ص 14، 15، متاح على الرابط: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

تم الاطلاع عليه بتاريخ 2021/02/02

[2] الاتحاد الدولي للاتصالات، شعبة تطبيقات تكنولوجيات الإعلام والاتصالات والأمن السيبراني، دائرة السياسات والاستراتيجيات، قطاع تنمية الاتصالات،**فهم الجريمة السيبرانية، دليل للبلدان النامية**، المرجع نفسه، ص 15.

يشتغلون فيها، و31 بالمائة من الجرائم المعلوماتية ارتكبها أفراد لا ينتمون لهذه المؤسسات، في حين 34 بالمائة من الجرائم المعلوماتية ارتكبها أشخاص مجهولون".[1]

وهذا ما يؤكّد أن الموظفين بالمؤسسات يشكلّون خطرا أكبر مقارنة بالأشخاص الآخرين، فالاعتداء على أنظمة المعلومات من طرف أشخاص ينتمون إلى المؤسسات أو الهيئات التي يعملون فيها يمكن أن يكون إما بإلحاق الضرر بالمعلومة أو بالنظام المعلوماتي مع طمس كل آثار تدل على أنهم مرتكبي الفعل، ويمكن لهم:

- مهاجمة الشبكة الداخلية للمنشأة التي يعمل فيها؛
- مهاجمة المعلومات بالسرقة أو التغيير أو الحذف؛
- فتح ثغرات في أنظمة الحماية التي وضعتها الجهة لتحصين أنظمة المعلومات فيها"[2].

كما أن "العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون لضغوطات نفسية كبيرة، ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفرة في حالات معينة، هذه الأمور مثلت في حالات كثيرة قوة محرّكة لبعض العاملين لارتكاب جرائم الحاسوب، باعثها في ذلك الانتقام من المنشأة أو رب العمل. وفي جرائم إتلاف البيانات، والبرامج، أمثلة كثيرة، كان دافع الجناة فيها إشباع الرغبة بالانتقام، وقد تحتل أنشطة زرع الفيروسات في نظم الكمبيوتر النشاط الرئيس للفئة التي تمثل الأحقاد على رب العمل الدافع المحرك للاعتداء على أمن نظام المعلومات.[3]

---

[1]Mira Carignan, **l'origine géographique en tant que facteur explicatif de la cyberdélinquance** ,maitrise avec mémoire, école de criminologie, faculté des arts et des sciences ,université de Montréal,septembre 2015, page 16, disponible sur le lien : www.papyrus.bib.unmontreal.ca, consulté le 15/03/20216 à (21 :00)

[2]خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، **أمن المعلومات بلغة ميّسرة**، الطبعة الأولى،مركز التميز لأمن المعلومات،جامعة الملك سعود، المملكة العربية السعودية، 2009، ص28.

[3] يونس عرب، **جرائم الكمبيوتر والانترنت: المعنى والخصائص والصور وإستراتيجية المواجهة القانونية**، ص92، متاح على الرابط: www.arablaw.org، تم الاطلاع عليه بتاريخ 2021/05/10،على الساعة 20:30.

فهناك حالات خطيرة لموظفين لهم الاستعداد مسبقا للإعتداء على أنظمة المعلومات وتهديدها وكذا اختراقها أي"ارتكاب جرائم معلوماتية كونهم " يملكون برنامج يحمل تعليمات بمسح كافة البيانات في حالة عدم وجود اسمه في كشف الموظفين بالشركة ويقوم عند فصله بالانتقام عن طريق تشغيل البرنامج المذكور، كما أن احتفاظه بكلمة السر يسمح له بالدخول إلى نظام الحاسب الآلي الخاص بالشركة وارتكاب أي جرائم، أو إعطائه لشركة أخرى منافسة لكي تتمكن من الدخول إلى أنظمة تلك الشركة والتجسس على بياناتها"[1]

- **المنافسة:**

تعمل الشركات في مجال المنافسة للحصول على معلومات تقنية حديثة أو أسرار تكنولوجية أو عسكرية أو معلومات عن البنوك والمعاملات المالية مثل الأسهم والسندات المتعامل بها في البورصات العالمية وذلك بواسطة أشخاص مؤجرين لهذا الغرض".[2]

وذلك للوقوف في وجه المنافس أو التغلب عليه.

- **الرغبة في إثبات الذات والتحدي والتفوق على التكنولوجيا:**

حيث يعمل مرتكبو الجرائم المعلوماتية على إظهار تفوقهم وذكائهم إزاء أي تكنولوجية جديدة،إذ تغلب عليهم " الرغبة في قهر النظام أكثر من شهوة الحصول على الربح. ويميل هؤلاء إلى إظهار تفوقهم ومستوي ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإنهم يحاولون إيجاد وغالبا ما يجدون الوسيلة إلى تحطيمها بل والتفوق عليها.[3]

---

[1] خالد ممدوح ابراهيم، **الجرائم المعلوماتية**، دار الفكر الجامعي، الاسكندرية (مصر)، 2009، ص140.

[2] عادل محمود شرف، عبد الله اسماعيل عبد الله، **ضمانات الأمن والتأمين في شبكة الانترنت، مؤتمر القانون والكمبيوتر والانترنت**، المجلد الثاني، كلية الشريعة والقانون بالتعاون مع مركز الامارات للدراسات والبحوث الاستراتيجية، مركز تقنية المعلومات، الامارات العربية المتحدة، من 01 إلى 03 مارس 2000، ص 397.

[3] عبد العال الديربي: **الجريمة المعلوماتية: تعريفها..أسبابها..خصائصها**، مرجع سبق ذكره، متاح عبر الرابط: www.accronline.com، مرجع سبق ذكره، تم الاطلاع عليه بتاريخ 2021/02/05 على الساعة (13:00)

وقد أثبت الواقع أن الكثير من الذين هاجموا الأنظمة المعلوماتية للمنظمات واعتدوا عليها، وارتكبوا مختلف الجرائم، أثبتوا تفوقهم التكنولوجي على المؤسسات التي ينتمون إليها وكذا تحدّيهم لكل التقنيات المستعملة مما جعل الأمر ينذر بالخطر حيث "يخشى 69% من المدراء التنفيذيين الذين أُجريت معهم مقابلات في المنتدى الاقتصادي العالمي من أن الأشخاص الذين يهاجمون مواقع الأنترنت سيظلون أكثر تقدماً وكفاءة من آليات الدفاع في شركاتهم".[1]

ثانيا: وجود طريقة للهجوم:

لا يمكن للمهاجم أن ينجح في هجومه على نظام المعلومات ما لمتكن لدية صورة وتصور وخطة واضحة ،لطريقة هجوم تحقق الغرض، وهذا هو الفرق الحوهري بين المهاجمين المحترفين وغير المحترفين.

ثالثا: وجود ثغرات في نظام المعلومات:(Vulnerability)

وفي هذه الحالة قد تكون نقطة ضعف في التصميم(Design) أو تهيئة(Configuration) البرمجيات، أو قواعد تخزين المعلوماتأو معدات تشغيل الشبكات التي تمر من خلالها المعلومات.ويستغل المهاجم هذه الثغرات في الاعتداء على أنظمة المعلومات.

1-أنواع المخاطر التي يتعرض لها نظام المعلومات:

يتعرض نظام المعلومات لعدة مخاطرنذكر البعض منها على سبيل المثال – لا الحصر – فيما يلي:

أ- التهديدات:Threats

[1] الاتحاد الدولي للاتصالات، **الوثائق الختامية لمؤتمر المندوبين المفوضين**، (المقررات والقرارات) 2014، بوسان (كوريا الجنوبية)، طبع في جنيف، (سويسرا) ،2015، ص 90.

و يعني الخطر المحتمل الذي يمكن أن يتعرض له نظام المعلومات وقد يكون شخصا مثل المتجسس أو المجرم المحترف أو الهاركر، أو شيئا يهدد الأجهزة أو البرامج أو المعطيات أو حدثا كالكوارث الطبيعية المختلفة.

ب- الثغرات أو نقاط الضعف في نظام المعلومات: Vulnerabilities

وهي عبارة عن نقطة أو عنصر أو ثغرة في النظام يمكن أن يستغله المهاجم وينفذ من خلاله الاختراق.

ج- المخاطر: Risks

تستخدم عادة كمرادف للتهديد، غير أنها تتصل بأثر التهديدات عند حصولها، لهذا تعمل المؤسسات على تحليل المخاطر حتى تتعرف على حجمها وطرق التعامل معها ووسائل الوقاية منها

د-الحوادث: Incidents

تشمل الأفعال المقصودة وغير المقصودة (مثل الزلازل، الفيضانات، الحرائق...)

هـ- الهجمات: Attacks

يستعمل هذا المصطلح لوصف الاعتداءات بنتائجها أو موضع الاستهداف، مثل هجمات إنكار الخدمة، هجمات البرمجيات...الهجمات الإرهابية. ..

2-الأساليب المعتمدة للاعتداء على أمن نظام المعلومات:

يستخدم من يقصد الاعتداء على نظام المعلومات، عدة برمجيات تدعى البرمجيات الخبيثة، وهي تتطور بسرعة وباستمرار، نذكر منها:

أولا: الفيروسات:

وهي عبارة عن برامج خبيثة تتسلل إلى البرمجيات وتخربها وتنسخ نفسها عدة مرات، وقد عرفها المركز القومي للحاسوب الأمريكي" بأنها برامج مهاجمة تصيب أنظمة الحاسوب بأسلوب يماثل إلى حد كبير أسلوب الفيروسات الحيوية التي تصيب الإنسان.[1]

ومن بين أبرز طرق انتشار الفيروسات، البريد الإلكتروني أو البرامج التي يتم تحميلها من الأنترنت'، حيث " يتعمّد أشخاص معينون بنشر الفيروسات بإضافتها مع ملفات ترسل بالبريد الإلكتروني، وعندما يقوم المرسل إليه بفتح البريد تفتح هذه الملفات وينتشر الفيروس ويبدأ عمله في التخريب.

هذا ما يؤكد بأن البريد الإلكتروني أصبح من بين أهم النواقل للبرامج الخبيثة نظرا لانتشاره الواسع دون حدود بين مختلف مستعملي الأنترنت، فيمكن أن يتضمن الملفات المرفقة بالرسائل المرسلة عبر البريد الإلكتروني، أو روابط يمكن تحميلها بعد الاطلاع على الرسالة لمواقع مشبوهة أو تحمل فيروسات. ويوجد مئات الآلاف من الفيروسات في العالم، تعمل كلها على "إفساد السير العادي للنظام المعلوماتي بعد استقرارها في ذاكرة الحاسوب".

وتشمل**الفيروسات** بصفة عامة عدة **أنواع** من **البرمجيات الخبيثة** تختلف في أساليب انتشارها وفي تصميمها، نذكر منها:

أ/أحصنة طروادة:

وهو نوع من البرمجيات الخبيثة الأكثر استعمالا في الاحتيال والتخريب بواسطة الحاسوب لا يقوم بإعادة نسخ نفسه وإنما، هي عبارة عن "برنامج حاسوبي يضمر أعمالا خبيثة ومضرة، خلاف ما يظهره من أعمال مفيدة، وهو لا يتكاثر مثل الفيروسات والديدان ،ولكن يكمن في النظام بشكل خفي،يحاول استغلال الحاسوب لشن الهجوم علىحواسيب أخرى "

[1] خالد عياد الحلبي،**اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص75.

وهذا يعني أن هذه البرمجيات تبدو ظاهريا مفيدة للمستخدم لكنها تنتشر لتزرع ذاتها في حاسوب المستعمل وتسيطر عليه، وتكون عادة على شكل موسيقى أو مقاطع فيديو أو يتبادلها المستخدمون الغافلون دون أن يعلموا ما تضمره، فحسب المختصين صمم هذا البرنامج في البداية لغرض مفيد وهو " معرفة مايقوم به الأبناء على جهاز الكمبيوتر في غياب الوالدين، ليتم تطويره بعد ذلك تطويراً سيئاً، حيث يُتيح للمخترق أن يتمكن من الدخول إلى الجهاز بطريقة لا تُثير أي ريبة أو شك نظراً لأنه يُمكنه من الدخول باستخدام كلمة السر التي يستخدمها صاحب الجهاز".[1]

ب/الديدان المعلوماتية:

عبارة عن "برامج صغيرة، صُنعت للقيام بأعمال تدميرية أو بغرض سرقة بعض البيانات الخاصة ببعض المستخدمين أثناء تصفحهم لشبكة الأنترنت أو لإلحاق الضرر بهم أو بالمتصلين بهم، وتلك الديدان تتميز بسرعة الإنتشار وفي الوقت نفسه يصعب التخلص منها نظراً لقدرتها الفائقة على التلون والتناسخ والمراوغة".

ويمكن لهذه البرامج استغلال أية فجوات في نظم التشغيل "من أجل الانتقال من حاسب إلى آخر ومن شبكة إلى أخرى عبر الوصلات الرابطة بينها، وتتكاثر أثناء انتقاله كالبكتيريا بإنتاج نسخ منها حتى تقوم بتغطية شبكة بأكملها ومن ثم تكون لها الإمكانية لتعطيل أو إيقاف نظام الحاسب الآلي بصورة كاملة.

وهذا يعني أن الديدان المعلوماتية أو "ديدان الحواسيب" بإمكانها تعطيل خدمات مختلف القطاعات التي تعتمد على شبكة الأنترنت وخاصة الحساسة منها ويمكن لها النفاذ إلى النظام المعلوماتي للشركات مما يهدد كيانها، فقد "أدّى انتشار الديدان الواسع إلى إضعاف سرعة النقل على الأنترنت، وتعطيل إحدى أكبر شبكات الصراف الآلي في العالم خلال

[1] منير محمد الجنيبهي، ممدوح محمد الجنيبهي، **جرائم الانترنت والحاسب الآلي ووسائل مكافحتها**، دار الفكر الجامعي، الإسكندرية (مصر)، 2006، ص 56

نهاية الأسبوع، وأبطأ أنظمة التحكم الجوي في كثير من المطارات الدولية . كما استطاع أن ينفذ إلى الشبكة الداخلية لمحطة الطاقة النووية في ولاية أوهايو في أمريكا وعطّل الحاسوب المسؤول عن مراقبة حالة المفاعل النووي للمحطة".

ج/ القنبلة المعلوماتية:

ويطلق عليها أيضا "القنبلة المنطقية" أو "القنبلة الزمنية"، وهي عبارة عن برنامج أو جزء من برنامج ينفذ في لحظة معينة أو في كل فترة زمنية محددة بالساعة واليوم والسنة، يتم إدخالها في برنامج وتنفذ في جزء من ثانية أو في ثوان أو دقائق وقد يتم ضبطها لتنفجر بعد عام.[1]

وتتميز القنابل المنطقية على أنها " تظل ساكنة ودون فاعلية ولا يمكن اكتشافها في مدة زمنية معينة، بل ذلك " يحدّدها مؤشر موجود في برنامج القنبلة، وهذا المؤشر لا يقتصر على المدة الزمنية وإنما قد يمتد إلى ما يعرف بتوافر شروط منطقية معينة من داخل برنامج أو ملف معين، وذلك حسب الرمز الذي يحدّده برنامج القنبلة، فإذا حلّ الميعاد أو توافرت هذه الشروط، بدأ البرنامج في القيام بمهامه التخريبية.

ثانيا: برامج التجسس: Espiogiciel:

هي عبارة عن برامج تراقب سلوك مستخدم الأنترنت على جهاز الحاسوب كمراقبة الكتابة والاتصالات والمواقع التي يزورها. وتهدف هذه البرامج أساسا إلى "التجسس الخبيث لاستقاء معلومات سرية، مثل كلمات المرور وأرقام الحسابات البنكية أو لأغراض تجارية مثل معرفة أنماط المستخدم الاستهلاكية، أو محركات البحث الأكثر استخداما أو المواقع التجارية الأكثر تسوقا".[2]

[1] **حسن حماد حميد الحماد**، الإتلاف المعلوماتي، **مرجع سبق ذكره، ص138**

[2] **خالد بن سلمان الغثير، محمد بن عبدالله القحطاني**، أمن المعلومات بلغة ميسرة، **مرجع سبق ذكره، ص 76**

تمتاز هذه البرامج إلى جانب عديد البرامج التي تظهر باستمرار وتتطور بقدرتها الفائقة على التخفي والعمل بشكل عادي داخل الحاسوب، يمكن لها أن تتغلغل بصفة سرية بفعل المجرم المعلوماتي، كما يمكن لها أن تكون جزءا من البرامج التي تسوّق بصفة قانونية دون أن ينتبه إليها المستعمل.

لذلك وبهدف ضمان أمن المعلومات وضمان عدم التعرض للمسؤوليات يوجب التعامل مع الكل على أنهم مصدر للخطر، وليست المسألة إهدار لفكرة حسن النية أو الثقة بالآخرين، إنها الضمان الوحيد للحماية من مصادر خطر بالغة قد تؤدي إلى مسؤوليات وخسائر لا يمكن تقديرها أو تجاوزها.

يتضح مما سبق، أن مخترقي أنظمة المعلومات، يعتمدون أساليب عدة تمكّنهم من الاختراق ومحاولة معرفة نقاط الضعف الموجودة في البرمجيات المستعملة والدخول من خلالها للمعطيات بهدف انتهاك سرياتها، مما جعل بعض المفاهيم التي ذكرناها سالفا ، تفرض نفسها لدى المختصين في أمن المعلومات وخاصة منها المخاطر والثغرات والتهديدات باستعمال الفيروسات المختلفة بطرق متعددة سواء ضد الأفراد أو المؤسسات أو الدول.و هذا ما يستدعي حالة التأهب القصوى عن طريق اتخاذ عدة تدابير تضمن حماية أمن المعلومات و نظام أمن المعلومات

3-التدابير المتخذة لضمان أمن نظام المعلومات:

تعتمد المنظمات عدة تدابير لحماية أنظمتها المعلوماتية من مختلف المخاطر والاعتداءات، وهي بمثابة أساليب، البعض منها فنية والبعض الاخر تقنية، في حين نجد بعض الأساليب إدارية نلخصها فيما يلي:

1-التدابير المتخذة لضمان أمن نظام المعلومات :

تعتمد المنظمات عدة تدابير لحماية أنظمتها المعلوماتية من مختلف المخاطر و الاعتداءات ، و هي بمثابة أساليب ، البعض منها فنية و البعض الاخر تقنية ، في حين نجد بعض الأساليب إدارية نلخصها فيما يلي:

أولاً :أساليب الحماية الفيزيائية

تتمثل في اختيار المكان الملائم والتجهيزات الأكثر حفاظا على الأمن ، و لابد من

– تخصيص غرف مغلقة لحفظ أجهزة خادم الشبكة مركزية، أما إذا لم يكن ذلك متاح فلابد من حفظ أجهزة الخادم ضمن غرف الإداريين.

– اختيار الكابلات الأكثر حماية للمعلومات كلما كان أمن المعلومات ضروريًا للهيئة ، وذلك على اعتبار أ ا تلغي الإشعاع **Fiber Optics** وتتمثل في كابلات الألياف الضوئية 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 .

– 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.

ثانيا: ضبط الوصول إلى الشبكة و إتاحة مواردها: access control system

من الضروري ضبط الوصول إلى الشبكة لحمايتها من التعرض لعمليات الاقتحام ،ولا يقتصر
الأمر هنا على حماية الشبكة من الاقتحام من قبل أشخاص غير مصرح لهم نهائيا بالدخول إليها
واستخدام مواردها، ولكن يتجاوزه إلى حمايتها أيضًا من محاولة دخول أشخاص مصرح لهم إلى
ملفات ومصادر غير مصرح لهم باستخدامها.

ولتحقيق ذلك لابد من تخصيص اسم أو رقم تعريف لكل مستخدم للشبكة
User ID أو كلمة مرور Password ، حيث تعد هذه هي الأولى المتبعة لمنع اقتحام الشبكات يتبعها التحقق من أن المستخدم لديه حقوق ممارسة ما يريد ممارسته على موارد الشبكة مثل حق الإنشاء للملفات والفهارس، أو حق المسح والاستعراض أو التغيير أو الفتح والقراءة أو الكتابة..الخ

ثالثا : تشفير البيانات :

تحظى تقنيات وسياسات التشفير في الوقت الحاضر باهتمام استثنائي في ميدان أمنى المعلومات ، و مرد ذلك أنه يمثل الوسيلة الأكبر لتحقيق وظائف الأمن الثلاث (السرية و التكاملية و الموفورية) .

فالتشفير تقنيات تدخل في مختلف وسائل التقنية المنصبة على تحقيق حماية هذه العناصر ، ويعد التشفير بوجه عام وتطبيقاته العديدة وفي مقدمتها التواقيع الإلكترونية ، الوسيلة
الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر الشبكات الإلكترونية .

وينبغي الحرص على تشفير البيانات عند الرغبة في إرسالها عبر الشبكة، سواء كانت تلك البيانات
كلمات مرور أم أرقام بطاقات الائتمان أم رسائل بريد إلكتروني أم ملف أم غير ذلك .وكلما كانت
سرقة البيانات تمثل خطورة كلما كانت هناك ضرورة اكبر لتشفيرها.

رابعاً :استخدام الجدران النارية:

و الحائط الناري هو برنامج أو عتاد يستعمل لحماية موارد الشبكة من مستخدمي الشبكات الأخرى .

وتعمل هذه الحوائط كفلترة أو مصفاة لاختبار كل محاولات الدخول للشبكة بحيث لا تسمح بالمرور إلا للاتصالات المسموح بها وتحجز كل ما عدا ذلك، وبذلك فإن دورها يشتمل الآتي:

- فحص كل الأنشطة الداخلة إلى الشبكة من مصادر خارجية مثل .
- ضبط المنافذ portsالمستخدمة بحيث يسمح باستخدام منافذ معينة لأغراض معينة
- رفض وصول أنشطة معينة من عناوين محددة

ويراعى في الحوائط النارية إلا تؤدي إلى إعاقة عمل مستخدمي الشبكة الفعليين حتى تؤدي
الغرض منها على النحو المطلوب.

خامسا : برامج الحماية ضد الفيروسات :

توجد عدة برامج ضد الفيروسات ، تنتجها شركات عالمية عملاقة ، و من بين هذه البرامج نذكر **Symantec,Command,Mcafee**

و تعمل هذه البرامج على :

- فحص ذاكرة الحاسب عند بدء تشغيله بحثًا عن أي فيروسات

– فحص أقراص التخزين بحثًا عن أي فيروسات، وفي حالة وجودها يتيح إزالتها أو إلغاء الملفات المصابة بها.

– فحص الملفات المراد تحميلها على جهاز الحاسب سواء كانت تلك الملفات متاحة من خلال الشبكة أو على أقراص مرنة وذلك للتأكد من سلامتها من الفيروسات.

– فحص الملفات سواء المتاحة للمشاركة أم المنقولة عبر الإنترنت أم المرسلة عبر البريد

الإلكتروني للتأكد من خلوها من الفيروسات والتنبيه بوجودها إن وجدت وتوفير الحماية ضدها.

– الفحص المستمر للنظام للتأكد من خلوه من الفيروسات، والتنبيه عنها في حالة وجودها.

سادسا: النسخ الاحتياطي: Backup

على الرغم من الاحتياطات الأمنية المتعددة التي قد تتبع لحماية البيانات إلا انه من المحتمل
وقوع أي نوع من التلف أو التحريف أو الفقدان للبيانات، لذا كان لابد من تأمين طريقة يمكن من خلالها استعادة البيانات التالفة أو المفقودة أو المحرفة لضمان مستوى أعلى من الحماية للنظام.
ويحقق النسخ الاحتياطي للبيانات هذا المستوى من الحماية، حيث يتم من خلاله إنشاء نسخ احتياطية يتم حفظها سواء في نفس مقر العمل أو خارجه، ويتم تحديثها بصورة منتظمة لضمان
أقل قدر من الخسائر في حالة فقدان البيانات الأصلية.

- **سابعا: طمس البيانات**

يعتقد الكثير من مستعملي الحاسوب أن حذف الملف يعني فقده نهائيا، ولا يعلمون بأنه نقل منطقيا إلى سلة المحذوفات ويمكن استرجاعه.ويعتقد الكثير من المستخدمين أيضا بأن حذف

الملف من سلة المحذوفات هو الإتلاف النهائي وهذا غير صحيح." فحذف ملف ما من وحدة التخزين يتم بحذف المؤشر الذي يدل عليه وليس بحذف الملف نفسه، أي أن محتويات الملف تظل في وحدة التخزين، ولكن على هيئة مساحة فارغة يمكن الكتابة عليها.و لهذا يمكن استرجاع الملف عن طريق برامج خاصة بذلك".[1]

ولهذا فإن عملية طمس البيانات تتم بالكتابة المتكررة على البيانات الموجودة ببيانات عشوائية وبعدة مرات.

وهناك معايير معروفة لطمس البيانات، " فقد وضعت وزارة الدفاع الأمريكية مثلا معايير تتطلب طمس البيانات بالكتابة عليها 07 مرات ومعيار بيتر قتمن Peter Gutmann يتطلب الكتاة 35 مرة.".[2]

وتوجد ثلاثة أنواع لطمس البيانات، وتتمثل أساسا في طمس الملف عند حذفه، وطمس المساحة الفارغة في وحدة التخزين، وطمس ملف المبادلة وهو ملف خاص بنظام التشغيل الذي يستخدم لدعم الذاكرة الافتراضية.

:الحماية من خلال الأشخاص

حيث تقوم المنظمة بوضع تشريعات وإجراءات تشترط على الموظف احترامها مثل تلك المتعلقة (بصلاحية المستخدم أو الخصوصية أو كلمات المرور...) بهدف تحديد الأدوار وتحديد المسؤوليات في حالة حدوث الاعتداء على المعلومة أو نظام المعلومات الخاص بالمنظمة.

[1] خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، **أمن المعلومات بلغة ميّسرة**، الطبعة الأولى،مركز التميز لأمن المعلومات،جامعة الملك سعود، المملكة العربية السعودية، 2009، ص121

[2] خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، **أمن المعلومات بلغة ميّسرة**، نفس المرجع، ص121

خلاصة

خلاصة:

تسعى كل المنظمات في وقتنا الراهن إلى الاهتمام بالمعلومة باعتبارها مورد استراتيجي نادر، به تقاس تطور الدول، وهذا لن يتأتى إلا بالتحكم فيها أمام التدفق الهائل للمعلومات الذي لا يعترف بالحدود الجغرافية مع ضمان حمايتها من مختلف المخاطر على المستويين الداخلي والخارجي.

وعليه،يتطلب الأمر استحداث استراتيجية أمن نظام المعلومات فعالة، تعتمد أساسا على تحديد أهمية هذه المعلومة وجودتها وكذا قيمتها بالنسبة للمنظمة، مع تقييم المخاطر التي تهددها، بتحديد حجمها والتكاليف التي قد تسببها لنظام المعلومات وللمنظمة ككل.

فضلا عن التوعية والتحسيس بأهمية ضمان معلومة آمنة وحمايتها من المخاطر والتهديدات التي تتطور بسرعة وباستمرار بتطور التكنولوجيا التي أفرزتها.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

1/ باللغة العربية:

أ- كتب:

1. غالب ياسين سعيد ، **أساسيات نظم المعلومات الإدارية و تكنولوجيا المعلومات، 2005**، عمان،(الأردن) ،ط1.

2. همشرى أحمد، عمر، **المكتبة ومهارات استخدامها،2009**، دار صفاء لنشر والتوزيع، عمان، (الأردن).

3.حجاحجة علي خلف ،"**إتخاذ القرارات الإدارية**"،دار قنديل للنشر والتوزيع، عمان (الأردن)، 2009.

4.ممدوح ابراهيم خالد ، **أمن المعلومات الالكترونية**، الدار الجامعية، الاسكندرية(مصر)، 2008.

5.نادرة أيوب، نظرية القرارات الإدارية، دار زهوان للنشر والتوزيع، عمان، (الأردن)، 1997،ص2015.

6. الصباغ عماد ، جامعة قطر – الدوحة، **نظم المعلومات ماهيتها ومكوناتها**، ط1، الإصدار الأول،مكتبة دارالثقافة للنشر والتوزيع، عمان، الأردن،2000.

7. السالمي محمد حسن ، عبد الرزاق علاء محمد، **الإدارة الإلكترونية**، دار وائل للنشر، عمان،(الأردن)، 2008.

8.محمد أحمد الخضيري، **اقتصاد المعرفة**،مجموعة النيل العربية، القاهرة (مصر)، 2001.

9. الفتال حميد ناصر، صادق دلال ، **أمن المعلومات**، دار اليازوري العلمية للنشر والتوزيع، الاردن، 2008.

10. يونس رؤى ، **دراسة واقع إدارة نظم المعلومات في المؤسسات السورية** ، 2017، مجلة جامعة البعث ، سوريا ، المجلد 93 ، العدد 31.

11.الغثبر خالد بن سليمان، القحطاني محمد بن عبد الله، **أمن المعلومات بلغة ميّسرة،** الطبعة الأولى، مركز التميّز لأمن المعلومات، جامعة الملك سعود، (المملكة العربية السعودية).

12.منير محمد الجنيهي ، ممدوح محمد الجنيهي ، **أمن المعلومات الالكترونية** ، دار الفكر الجامعي، الاسكندرية، مصر.

13.محمد عبد حسين الطائي،2015، إدارة أمن المعلومات ، دار الثقافة للنشر و التوزيع ، عمان، (الأردن) .

14.عبد الفتاح بيومي حجازي، **مبادئ الإجراءات الجنائية في جرائم الكمبوتر والانترنت،** الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006،

15.هيننغ فيغنر، **الأبعاد الجديدة للمخاطر السيبرانية: انعاش القتال،** الأيام العربية للأمن السيبراني (السنة الخامسة)، مركز البحوث والدراسات القانونية والقضائية- جامعة الدول العربية- بيروت،1-2 ديسمبر 2015.

ب- التقارير الدولية :

الاتحاد الدولي للاتصالات، شعبة تطبيقات تكنولوجيات الإعلام والاتصالات والأمن السيبراني، دائرة السياسات والاستراتيجيات، قطاع تنمية الاتصالات،**فهم الجريمة السيبرانية، دليل للبلدان النامية،** مشروع أفريل 2009

ج- مجلات علمية:

1. العشي هارون ، بوراس فايزة ، أهمية نظم المعلومات الادارية في تحسين عملية اتخاذ القرارات داخل المؤسسة، دراسة حالة شركة الدراسات وإنجاز الأعمال الفنية للشرق، باتنة، مجلة أبحاث اقتصادية وإدارية، المجلد 14، العدد 02، 2020.

2. عبيس كاظم ، تركي، **نظم المعلومات الإدارية و أهميتها في اتخاذ القرارات،** مجلة جامعة بابل، العلوم الإنسانية، 2010 ، المجلد 18 ، العدد3 .

ج-ملتقيات علمية:

1. بن بعلاش خليدة ، رابحي لخضر ، **معالجة الجريمة المعلوماتية في ظل التعاون الدولي والاستجابة الوطنية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة، يومي 16 و17 نوفمبر 2015

2.العاكوم وليد ، **مفهوم ظاهرة الإجرام المعلوماتي، مؤتمر القانون والكمبيوتر والانترنت**، المجلد الأول، كلية الشريعة والقانون بالتعاون مع مركز الإمارات للدراسات والبحوث الإستراتيجية، مركز تقنية المعلومات، الإمارات العربية المتحدة، من 01 إلى 03 مارس.

باللغة الفرنسية:

1/ Dictionnaire :

1.Henri Mahé de Boislandell , **Dictionnaire de gestion: vocabulaire, concepts et outils , édition Economica,** Paris, France, 1998, P 432.

2/Livres :

1.Patrick le Guyader, **Protection des données sur internet** , Edition, HERMES, Lavoisier, Paris, France, 2013

2.Nicolas Arpagian, **la cyber guerre, la guerre numérique a commencé,** édition Hermès, Science Lavoisier, Paris, France,2013.

3/Thèses :

1.**Kefi AbdEssalem, évaluation des technologies et systèmes d'information- cas d'un entrepôt de données implanté dans une institution financière,** thèse de doctorat en sciences de gestion, université de Paris Dauphine, 2001.

-الويبوغرافيا:

1.اللجنة الاقتصادية والاجتماعية لغربي آسيا ،(الاسكوا)، **الأمانفي الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية: توصيات سياساتية،(2015)**،الأمم المتحدة، نيويورك (الولايات المتحدة الأمريكية)،متاح على الرابط:
https://www.unescwa.org/file/37236/download?token=fNPBBbGo

3. هناء محمد، **كيف تعرف أن هاتفك مخترق أو مراقب**،متاح على الرابط:www.almarsal.com

فهرس المحتويات

فهرس المحتويات