جـــــــــــــــامعة سعيدة – د. الطاهر مولاي –

كـــــــــــلية الحقوق والعلوم السياسية.

قـــــــــــسم العلوم السياسية.

الأمن المعلوماتي وسبل حمايته في الجزائر

دراسة حالة مؤسسة اتصالات الجزائر –سعيدة–

مذكرة مكملة لنيل شهادة الماستر في العلوم السياسية تخصص: تسيير وإدارة الجماعات المحلية.

إعداد الطالب: بغداد محمد

إشـــراف الدكتور: موكيل عبد السلام

أعضاء لجنة المناقشة:

- الدكتورة: عياشي حفيظة..... رئيساً.
- الدكتور موكيل عبد السلام.....مشرفا ومقررا.
- الأستاذة: حلوي خيرة.....عضوا مناقشا.

السنة الجامعية:

2018/2017م

1439/1438هـ


بسم الله الرحمن الرحيم

﴿قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ﴾

(سورة البقرة : الآية 32)

شكـــــــــــر وتقديـــــــــــر

اللهم علمنا ما ينفعنا وانفعنا بما علمتنا وزدنا علما نافعا ولسانا ذاكرا وقلبا خاشعا وجسدا على البلاء صابرا

ومن لم يشكر الناس لم يشكر الله تعالى.

نشكر الله الذي وفقنا لهذا ثم الشكر لكل إنسان أمد لي يد المساعدة من قريب أو بعيد وعلى رأسهم الأستاذ المشرف موكيل عبد السلام كما أتوجه بالشكر الجزيل إلى أعضاء لجنة المناقشة الدكتورة عياشي حفيظة والأستاذة حلوي خيرة اللذين قبلوا مناقشة هذه المذكرة.

إهـــــــــــداء

قبل كل إهداء اشكر الله عز وجل على كل نجاح حققته في حياتي وعلى توفيقي في هذا العمل.

إنه لا يسعني في هذا المقام إلا أن أهدي ثمرة جهدي إلى:

الى جدتي والولدين الكرمين أطال الله في عمرهما

إلى جميع اخواني الى جميع عماتي.

إلى من أتقاسم معهم المحبة الأسرية، إلى جميع الأقارب والأصدقاء والأحباء، بوبكر فارس، خلف حسين، ريشاوي زين العابدين، أشعيبي سلام، بوعزة عبد القادر زينب، سميحة وسهام

أستاذي المشرف الذي أشرف على هذه الدراسة وأمدنا والأفكار فكان نعم الموجه فجزاك الله خيرا.

أعضاء لجنة المناقشة الأفاضل الذين شرفوني بقبول مناقشة الدراسة ولدورهم الكبير في إثراء الدراسة من علمهم وخبرتهم.

إلى كل من ساهم في إتمام هذه الدراسة ولو بكلمة واحدة.

قائمة المختصرات:

الاختصار	الدلالة باللغة الأجنبية	الدلالة باللغة العربية
NTIC	New Technology of Informations and Communications	تكنولوجيا المعلومات والاتصالات الجديدة
TIC	Technology of Informations and Communications	تكنولوجيا المعلومات والاتصالات
LAN	Local Area Network	الشبكة المحلية
WAN	Wide Area Network	الشبكة الواسعة
RMS	Réseau Multi Services	شبكة متعددة الخدمات
VPN	Virtual Private Network	شبكة افتراضية خاصة
TCP	Transmission Control Protocol	بروتوكول التحكم في النقل
IP	Internet Protocol	بروتوكول الأنترنت
ISO	International Organization for Standardization	المنظمة الدولية للمقاييس
Ed	Edition	الطبعة
ط	Edition	الطبعة
ع	Vol	العدد

مقدمة

مقدمة:

يشهد العالم مند منتصف القرن العشرين، ثورة جديدة اصطلح على تسميتها بالثورة المعلوماتية، وهذا إشارة للدور البارز الذي أصبحت تلعبه المعلومات، حيث أصبحت هذه الأخيرة تعرف على أنها نفط القرن الواحد والعشرين، فهي مقياس لقوة الشعوب وتطورها فمن يملك المعلومات يملك القوة في ظل تنامي دور المعلومات والأجهزة والتكنولوجيات الحديثة المعالجة لها.

لقد أحدثت تكنولوجيا المعلومات والاتصالات قفزة نوعية، وبهذا أصبحت المؤسسات باختلاف أنواعها وأشكالها والحكومات وغيرها تعتمد على أنظمة معلوماتية مختلفة، أضحت هذه الأنظمة والتكنولوجيات العمود الفقري للمؤسسات والحكومات وغيرها، ولكن وفي القابل فتحت هذه التكنولوجيا المجال أمام أنواع جديدة من الجرائم والتي تعرف بالجرائم المعلوماتية، والتي أصبح لها تأثير كبير في مختلف النواحي و المجالات ألأمنية، الاقتصادية والسياسية وهذا ما أدى الى التفكير في ضرورة تأمين هذه البيانات والمعلومات والحفاظ على سريتها، واستحداث وتطوير الوسائل والتقنيات الكفيلة بذلك.

يعتبر الامن الركيزة الاساسية للمجتمع، بحيث لا يمكن تصور نمو اي نشاط بعيدا عن تحققه، سواء اكان ذلك، على المستوى التقني، ام على المستوى القانوني. وقد تحول الامن، مع بروز مجتمع المعلومات، والفضاء السيبراني، الى واحد من قطاع الخدمات، التي تشكل قيمة مضافة، ودعامة اساسية، لأنشطة الحكومات والافراد، على حد سواء كما هو الحال، مع التطبيقات الخاصة بالحكومة الالكترونية، والصحة الالكترونية، والتعليم عن بعد، والاستعلام، والتجارة الالكترونية، وغيرها الكثير. الا ان الوجوه المتعددة للأمن المعلوماتي، ومضاعفاته الخطيرة التي لا تقف عند حدود الاساءة الى الافراد، والمؤسسات، بل تتعداها الى تعريض سلامة الدول والحكومات، تزيد مهمة القيمين على الموضوع تعقيدا وصعوبة، وتستدعي مقاربة، شاملة، ومتكاملة، لجميع التحديات، التي يطرحها الفضاء السيبراني.

إن الحديث عن تأمين المعلومات والحفاظ على سلامتها وسريتها يقودنا الى اتخاذ جملة من الإجراءات والتدابير والتي تركز أساسا على كل من العنصر البشري، والتقني لأن التكنولوجيا مهما بلغت من تطورات لا يمكن أن تحل محل النصر البشري.

1) أهمية الموضوع:

تتجلى أهمية هذه الدراسة في حيوية الموضوع الذي تناولناه، وكذلك لقلة الدراسات التي في موضوع الأمن المعلوماتي ومهدداته وتقنيات تأمينه باللغة العربية.

2) أهداف الدراسة:

يمكن اجمال أهداف هده الدراسة في النقاط التالية:

- التعرف على مفهوم أمن المعلومات والمصطلحات المرتبطة به.
- التعرف على المخاطر التي تهدد أمن وسرية المعلومات.
- تسليط الضوء على مختلف اطرق والإجراءات اللازمة للحفاظ على أمن المعلومات.

3) مبررات اختيار الموضوع:

ان اهتمام أي باحث ورغبته في تناول موضوع معين عن غيره من المواضيع الأخرى راجع الى جملة من الاعتبارات المرتبطة بشخصية الباحث واهتماماته، وأخرى موضوعية ترتبط بمواصفات موضوع الدراسة من حيث حداثته وقيمته العلمية.

1.3) المبررات الذاتية:

وهي تنطلق من اهتمامي الشخصي بالمجال لتقني بما في ذلك الأمن المعلوماتي والتقنيات الحديثة لمحافظة على أمن وسرية المعلومات الالكترونية، في ظل التطورات التقنية المتسارعة.

2.3) المبررات الموضوعية:

وهي تتعلق بالقيمة العلمية لموضوع الدراسة، إضافة الى محدودية الدراسات والأبحاث في هذا الموضوع، وهذا ما سيفتح المجال حتما أما الباحثين للاجتهاد أكثر في إثراء هذا الموضوع.

4) أدبيات الدراسة:

ورد في هذا الموضوع جملة من الأدبيات والدراسات، والتي ركزت أغلبها على الأمن المعلوماتي، إضافة الى المخاطر والتحديات التي تواجهه، ومختلف التقنيات لتأمينيه نذكر منها:

- مذكرة ماجستير تحت عنوان: "واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها" وقد هدفت هذه الدراسة الى معرفة واقع أمن نظم المعلومات في الكليات التقنية بقطاع غزة، من خلال معرفة المهددات المحتملة بهذه الكليات ومختلف الطرق المتبعة لتجاوزها.
- دراسة بعنوان "مهددات الأمن المعلوماتي وسبل مواجهتها دراسة مسحية على مستوى مرز احاسب الالي بالقوات البحرية للملكة العربية السعودية هدفت هذه الدراسة الى التعرف على مهددات الأمن المعلوماتي وطرق مواجهتها في ضوء تزايد معدلات الاختراقات والحاجة المتزايدة لا تخاد وسائل الحماية اللازمة للبينات والمعلومات.
- جاءت هذه الدراسة لإعطاء نوع من التجديد للموضوع كون أن الموضوع يعالج جوانب تقنية بالدرجة الأولى، وهذه الأخيرة تتسم بالتغير والتطور المتسارع والمستمر، وكذلك للإعطاء لمحة عن أحدث التقنيات والتدابير والإجراءات بمختلف أنواعها التي تستخدم للحفاظ على أمن وسرية البيانات الرقمية.

5) إشكالية الدراسة:

في ظل التزايد المستمر في الاعتماد على التكنولوجيا الحديثة من قبل الافراد والمؤسسات والحكومات أصبح من الضروري تأمين هذه التقنيات من المخاطر والتهديدات التي قد تواجهها، ومن هذا المنطلق نطرح الإشكالية التالية:

إلى أي مدى يمكن الحديث على أمن المعلومات ومهدداته؟ وماهي الطرق والتقنيات المتبعة من طرف مؤسسة اتصالات الجزائر لتامين نظام معلوماتها؟

وتتفرع الإشكالية الرئيسية الى جملة من التساؤلات الفرعية يمكن اجمالها فيما يلي:

- **ما مفهوم الأمن المعلوماتي؟**
- **هل الوسائل التكنولوجية كافية لضمان أمن وسرية المعلومات؟**
- **هل يمكن تحقيق نظام امن تماما؟**
- **هل التقنيات المستخدمة لتامين المعلومات تؤثر في طريقة التعامل مع أنظمة المعلومات؟**

- **ما مدى كفاءة الأساليب المتبعة من طرف مؤسسة اتصالات الجزائر لحماية نظام معلوماتها.**

6) فرضيات الدراسة:

تقدم هذه الدراسة مجموعة من الفرضيات والتي من شأنها أن تجيب على الإشكالية الرئيسية وأسئلتها الفرعية يمن اجمالها فيما يلي:

- أمن المعلومات هو جملة من الأدوات والتقنيات الكفيلة بالحفاظ على سرية وسلامة المعلومات في مختلف مراحل معالجتها.
- يمكن حماية امن المعلومات بالاعتماد فقط على الوسائل التكنولوجية والتقنية.
- لا يمكن في أي حال من الأحوال وباي طريقة كانت تحقيق نظام امن تماما.
- يمكن للتقنيات والأدوات والأساليب المستخدمة أن تؤثر في طريقة تعامل المستخدمين مع نظام المعلومات.

7) حدود الدراسة:

جاءت حدود هذه الدراسة كلاتي:

- **الحدود الموضوعية:** تغطي هذه الدراسة موضوع الأمن المعلوماتي، ومهدداته ومختلف الطرق والتقنيات للحفاظ على امن وسلامة المعلومات.
- **الحدود المكانية:** شمل الإطار المكاني لهذه الدراسة مؤسسة اتصالات الجزائر لولاية سعيدة.
- **الحدود الزمانية:** امتدت هذه الدراسة في الفترة ما بين شهر فيفري 2018 إلى غاية شهر ماي من نفس السنة.

8) الإطار المنهجي:

قصد الإلمام بموضوع الدراسة تم الاعتماد على مجموعة من المناهج نذكر من ضمنها:

- **المنهج الوصفي:** الذي يرتكز على الوصف الدقيق لموضوع الدراسة وهذا من أجل الحصول على نتائج علمية بطريقة موضوعية ويتجلى الاعتماد على هذا المنهج من خلال سرد ووصف وتحليل لكل من مفهوم تكنولوجيا المعلومات والاتصالات وكذلك أمن المعلومات.
- **المنهج التاريخي:** كما تم توظيف المنهج التاريخي وهذا لغرض رصد التطور التاريخي لتكنولوجيا المعلومات والاتصالات وكذلك تاريخ أمن المعلومات.

- **منهج دراسة حالة:** أضافة الى ذلك اعتمدنا منهج دراسة حالة وذلك بهدف جمع الحقائق والبيانات حول الحالة المدروسة.

9) أدوات البحث العلمي:

تمت الاستعانة بمجموعة من أدوات البحث العلمي أثناء القيام بهذه الدراسة والتي من بينها:

الملاحظة: تعتبر من أهم الأدوات والوسائل التي يستخدمها الباحثون الاجتماعيون في جمع المعلومات بالحقل الاجتماعي، لأنها تعطي مجال للباحث للملاحظة سوءا كانت على المبحوثين أو على المواضيع التي تحتاج للمعاينة للحصول على المعلومات اللازمة.[1]

والاستعانة كذلك بالمقابلة والتي وظفت خلال الدراسة التي أجريت بمؤسسة اتصالات الجزائر –سعيدة– مع المكلفة بنظام المعلومات بالمؤسسة وبعض رؤساء المصالح.

المقابلة: وهي عبارة عن محادثة يقوم بها الفرد مع الأخر أو مع مجموعة من الأفراد بهدف الحصول على مجموعة من المعلومات لاستخدامها في البحث العلمي أو الاستعانة بها في عمليات التوجيه.[2]

10) صعوبات الدراسة:

لا يخلو أي بحث أو دراسة من الصعوبات ونحن في إطار انجاز هذه الدراسة وجهتنا جملة من الصعوبات نذكر منها:

- صعوبة الحصول على بعض المراجع.
- قلة الدراسات التي تناولت موضع الأمن المعلوماتي في الجزائر.
- أغلب المؤسسات الجزائرية ليس بها قسم أو مصلحة أو حتى شخص مسؤول عن الأمن المعلومات ما صعب علينا القيام بدراسة حالة، إضافة إلى نقص التعاون من طرف المؤسسة محل الدراسة، حيث اتسمت بعض الإجابات بالغموض والسطحية وعدم الدقة، إضافة الى صعوبة التواصل مع بعض المسؤولين بالمؤسسة، ما أدى الى عدم تمكننا من الحصول على بعض المعلومات المهمة التي تخدم دراستنا.

[1] عمار بحوش، **دليل الباحث في المنهجية**، الجزائر: المؤسسة الوطنية للكتاب، 1985، ص 40.

[2] محمد عبد الحميد، **تحليل المحتوى في بحوث الاعلام**، مصر: ديوان المطبوعات الجامعية، 1979، ص 308.

11) هندسة الموضوع:

قصد الالمام بحيثيات ومتطلبات البحث، تم ادراج مضامنة وعرض محتويات في ثلاثة فصول مقسمة على النحو التالي:

الفصل الأول: تحت عنوان إطار مفاهيمي حول تكنولوجيا المعلومات والاتصالات وامن المعلومات، تضمن هذا الفصل مبحثين، الأول خصصناه لعرض الإطار المفاهيمي حول تكنولوجيا المعلومات والاتصالات، حيث تطرقنا في مطالبه الى مفهومها، تاريخها، خصائصها ومميزاتها، مكوناتها واختتمنا المبحث بإشكاليات وتحديات هذه التكنولوجيات.

أما المبحث الثاني فخصصناه للتعريف بالأمن المعلوماتي والمصطلحات المرتبطة به، ثم تطرقنا الى تاريخه، عناصره وأخيرا تحدياته.

الفصل الثاني: جاء بعنوان مهددات أمن المعلومات وأساليب حمايته وقسمنا هذا الفصل الى مبحثين.

المبحث الأول مهددات أمن المعلومات وأساليبها التقنية تضمن هذا المبحث جملة من الأخطار والمهددات مقسمة كالاتي: المهددات من حيث مصدر وقوعها، مهددات البنى التحتية، المهددات الصادرة عن المورد البشري.

اما المبحث الثاني فتطرقنا فيه الى مختلف الأساليب والتقنيات للحفاظ على سرية وسلامة المعلومات وقسمنا هذه الأساليب كالاتي:

أساليب الحماية المادية، أساليب الحماية البرمجية والتقنية، أسالب الحماية الإدارية والتنظيمية.

الفصل الثالث: كان عبارة عن دراسة حالة مؤسسة اتصالات الجزائر–سعيدة– تضمن هذا الفصل بدوره مبحثين، الأول تطرقنا فيه الى عرض عام وتعريف بالمؤسسة أما الثاني فتناولنا من خلاله نظام المعلومات الموجود داخل المؤسسة ومختلف الاخطار التي تهدده إضافة الى الطرق المتبعة ممن طرف المؤسسة لتأمينه.

الفصل الأول:

إطار مفاهيمي حول تكنولوجيا المعلومات و الاتصالات وأمن المعلومات

شهد العالم في النصف الأخير من القرن الماضي تطورات عديدة، شملت العديد من المجالات وأفرزت العديد من المصطلحات، ومن بين هذه المصطلحات تكنولوجيا المعلومات والاتصالات والتي لعبت دورا بارزا في تحسين الخدمات وتطويرها وتقديمها بجودة عالية وفي أقل وقت ممكن وبأقل التكاليف.

وفي المقابل تواجه هده التكنولوجيات الحديثة العديد من التحديات والمشاكل، ولعل من أبرزها هو مشكل الإبقاء على سرية وسلامة هذه المعلومات وحمايتها من مختلف التهديدات الإلكترونية، ومن هنا وجب على المؤسسات سوءا كانت عامة أو خاصة الاهتمام بمجال الأمن ألمعلوماتي خاصة مع الازدياد المستمر في الجرائم الإلكترونية، والتطور الهائل الحاصل في تقنيات وطرق الاختراق وذلك عن طريق وضع قسم مسئول عليه، ووضع سياسة لأمن المعلومات داخل المؤسسة تحدد صلاحيات كل موظف إضافة إلى توعية الموظفين بأهمية هذا المجال.

ولتوضيح مضامين هذه المفاهيم والعلاقة بينهما قمت بتقسيم هذا الفصل إلى مبحثين كالاتي:

المبحث الأول: مدخل مفاهيمي لتكنولوجيا المعلومات والاتصالات.

المبحث الثاني: أمن المعلومات مفهومه، تاريخه، عناصره وتحدياته.

المبحث الأول: مدخل مفاهيمي لتكنولوجيا المعلومات والاتصالات.

أصبحت تكنولوجيا المعلومات والاتصالات من بين أهم العناصر الواجب توفرها في الإدارات والمؤسسات الحديثة، سنطرق في هذا المبحث الى إطلالة على مختلف التعريفات المقدمة لهذه التكنولوجيات.

المطلب الأول: مفهوم تكنولوجيا المعلومات والاتصالات.

1) تعريف التكنولوجيا:

يرجع أصل كلمة تكنولوجيا الى اليونانية وهي تتكون من مقطعين هما:

(**Techno**) وتعني التشغيل الصناعي و(**Logos**) وتعني العلم أو المنهج، وعلية فمصطلح التكنولوجيا يعني علم التشغيل الصناعي.

وعرفت التكنولوجيا كذلك من طرف المهتمين بنظرية المنظمة على أنها "العلم والفن المستخدم في إنتاج وتوزيع السلع والخدمات، وتخفيض تكاليف الإنتاج وتطوير أساليب العمل، أي العمليات والتقنيات والمكائن والأعمال المستخدمة لتحويل المدخلات (الموارد، المعلومات، الأفكار) إلى مخرجات (منتجات وخدمات)."

علما أن وجود التكنولوجيا داخل المنظمات يكون على ثلاثة مستويات كالاتي:

- **المستوى الفردي**: حيث يقصد بالتكنولوجيا هنا، المهارات الشخصية والمعرفة التي يمتلكها الفرد في التنظيم.
- **المستوى الوظيفي**: يقصد بالتكنولوجيا هنا، مجموعة الإجراءات، والأساليب التي تستخدمها كافة الوحدات والأقسام داخل المنظمات ودلك للأداء أعمالها.
- **المستوى التنظيمي**: وتتمثل في الظريفة التي يحول بها التنظيم المدخلات إلى مخرجات.[1]

وعرف معجم (**Webster**) التكنولوجيا على أنها "لغة تقنية وعلم تطبيقي وطريقة فنية، لتحقيق هدف عملي، إضافة إلى أنها مجموعة من الوسائل التي تساعد في توفير كل ما هو ضروري لمعيشة الأفراد وتحقيق رفاهيتهم."[2]

---

[1] بلقيدوم صباح، أثر تكنولوجيا المعلومات والاتصالات الحديثة على التسيير الاستراتيجي للمؤسسات الاقتصادية، **أطروحة دكتوراه** في علم التسيير، جامعة قسنطينة 2: كلية العلوم الاقتصادية وعلوم التسيير، قسم علوم التسيير، 2013/2012، ص 131-132.

[2] Webster's, **dictionary of English usage**, Merriam webster inc, 1989, p 890.

2) تعريف المعلومات:

ان المصطلح العلمي لتعبير المعلومة عربي، ويقابله بلاتينية (**Information**) وفيما يلي جملة من التعريفات التي قدمت لهذا المصطلح:

عرفها معجم الأوراس العربي الحديث على أنها: "الأخبار والتحقيقات، أو كل ما يؤدي إلى كشف الحقائق وتوضيح الأمور."

أما معجم مكنز المكتبات والمعلومات فيعرفها بأنها: "عملية توصيل حقائق أو مفاهيم من أجل زيادة المعرفة."

وتناولت موسوعة (**Comptons encyclopedia**) تعريف المعلومة بأنها: "أي شيء يزيل عدم التأكد من أمر ما وبمعنى أخر هي كل شيء يوصل الى اليقين من حقيقة ما."[1]

وعرفت المعلومة كذلك على أنها: "البيانات المدونة على شكل مكتوب أو شفهي أو في أقراص مرنة أو على شكل إلكتروني."

"هي البيانات التي تمت معالجتها لتحقيق هدف معين أو لاستعمال محدد لغرض اتخاذ القرارات، أي البيانات التي أصبح لها قيمة بعد تحليلها، تفسيرها أو تجميعها في شكل ذي معنى والتي يمكن تداولها، تسجيلها، وتوزيعها في صورة رسمية أو غير رسمية."

"هي تلك الحقائق والأفكار التي يتبادلها الناس في حياتهم العامة، ويكون هذا التبادل عادة عن طريق وسائل الاتصالات وعبر مراكز ونظم المعلومات المختلفة."[2]

3) تعريف تكنولوجيا المعلومات والاتصالات:

عرفت هده التكنولوجيا العديد من التسميات، فقد وصفت في أول ظهور لها على أنها التكنولوجيا الحديثة للمعلومات والاتصالات وهي اختصار ل (**NTIC**) وبعدها حذفت كلمة حديثة لتصبح تكنولوجيا المعلومات

[1] محمد فاروق عبد الحميد كامل، **المعلومة الأمنية**، ط1، الرياض: أكاديمية نايف للعلوم الأمنية، 1999، ص 11.

[2] بوزاوية زهرة، مجتمع المعلومات والكفاءات الجديدة، لدى أخصائي المعلومات دراسة ميدانية بالمؤسسات الوثائقية بولاية وهران، **مذكرة ماجستير**، جامعة وهران 1 أحمد بن بلة: كلية العلوم الإنسانية، قسم علم المكتبات، 2015/2014، ص 16.

والاتصالات (**TIC**) نظرا لزوال الحداثة عنها وهذا بعد ظهورها في منتصف السبعينيات حتى القرن العشرون وذلك من خلال إطلاق أول حاسوب تحت أسم (**Altair**) وبدايات الانترنت في التسعينيات.[1]

يرى **هربرت سيمون** (**Herbert Simon**) بان هذه التكنولوجيا تساعد على جعل كل معلومة قادرة على الوصول للإنسان على شكل شفهي أو رمزي، متوفرة ومخزنة في الذاكرات الالكترونية من خلال القيام بالتقاط ومعالجة واسترجاع وإيصال المعلومات سواء في شكل معطيات رقمية، نص، صوت أو صورة.

وتبرز هذه التكنولوجيا من خلال ظاهرتين أساسيتين هما الجمع بين الكلمة المكتوبة، المنطوقة والصورة الساكنة والمتحركة وبين الاتصالات السلكية واللاسلكية، ثم تخزين المعلومات واستعمالها عن طريق اعتماد الأسلوب الرقمي (**Digital**) للقيام بهذه العمليات.[2]

عرفت تكنولوجيا المعلومات والاتصالات على أنها: "المجال الذي يهتم بإنتاج المعلومات، ومعالجتها وتخزينها ولإدارتها سوءا كانت نصا، صورة أو كل طريقة تدمج بينهما."[3]

"يتضمن مفهوم تكنولوجيا المعلومات كل الأدوات والتقنيات التي تستخدمها نظم المعلومات لتنفيذ الأنشطة الحاسوبية على اختلاف أنواعها."

كما عرفتها وزارة التجارة البريطانية على أنها: "عملية الحصول عل البيانات ومعالجتها وتخزينها وتوصيلها وإرسالها في صورة رقمية، وذلك بواسطة توليفة من الآلات الالكترونية وطرق الموصلات السلكية واللاسلكية."[4]

---

[1] Jamod véronique, **l'impact des innovations technologiques et organisationnelles sur les performances des entreprises**, **une évaluation non paramétrique**, 2004, p2.

[2] توامي يعقوب، أثر استخدام تكنولوجيا المعلومات والاتصال على الأداء المالي للمؤسسة الاقتصادية دراسة حالة مجمع المؤسسة الوطنية للأشغال في الآبار(E.N.T.P) ، **مذكرة ماستر**، جامعة قاصدي مرباح ورقلة: كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، تخصص مالية المؤسسة، 2013/2012، ص 5.

[3] عدنان يحي، **تكنولوجيا المعلومات**، ط1، فلسطين: وزارة التربية والتعليم العالي، 2005، ص 3.

[4] دري وردة، استخدام تكنولوجيا المعلومات وتأثيرها على وظائف المؤسسة دراسة حالة مؤسسة اتصالات الجزائر وحدة ورقلة، **مذكرة ليسانس**، جامعة قاصدي مرباح ورقلة: كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، 2013/2012، ص 15.

ويمكن تصنيف التعريفات المقدمة لتكنولوجيا المعلومات والاتصالات، إلى أربعة مجموعات موضحة في الجدول الاتي:

جدول رقم (1) مفاهيم متعددة حول تكنولوجيا المعلومات والاتصالات

البيان	مفهوم تكنولوجيا المعلومات والاتصالات
المجموعة الأولى: مفاهيم تركز على الأجهزة التي تشملها تكنولوجيا المعلومات والاتصالات	• يعرف **بالفيا (Palvia)** تكنولوجيا المعلومات والاتصالات بأنها: "جميع الجوانب المتعلقة بالحاسبات الإلية والمكونات المادية والبرامج الجاهزة ومعدات الاتصال عنب بعد." • أما **أوزر (Ozer)** فيرى إن تكنولوجيا المعلومات والاتصالات: "هي المكونات المادية للحاسبات الإلية، والبرامج الجاهزة ونظم الاتصال."
المجموعة الثانية: مفاهيم تركز على أجهزة تكنولوجيا المعلومات والأنشطة التي تقوم بها	• يرى البعض أن مفهوم تكنولوجيا المعلومات والاتصالات يتمثل في: "معالجة، تخزين، إرسال: عرض، إدارة، تنظيم ثم استرجاع المعلومات." • يرى **روفل (Rofle)** أن تكنولوجيا المعلومات والاتصالات: "هي التكنولوجيا المبنية على الإلكترونيات والتي يمكن أن تستخدم في جمع، تخزين ومعالجة ووضع هذه المعلومات في حزم متكاملة ومن تم الوصول إلى المعرفة. • ويرى **باترسون(Patterson)** أن مفهوم تكنولوجيا المعلومات والاتصالات يقصد به: "تطبيق النظم التكنولوجية الحديثة في معالجتها، إرسالها، تخزينها واسترجاعها بسرعة ودقة وكفاءة ومن أهم هذه النظم تكنولوجيا توصيل البيانات، تكنولوجيا الاتصالات عن بعد، تكنولوجيا الحاسبات الإلية والبرامج الجاهزة."
المجموعة الثالثة: مفاهيم تركز على الأجهزة والأفراد	• يرى **تيربان (Turban)** أن تكنولوجيا المعلومات والاتصالات: "تصمن جميع أنظمة المعلومات المبنية على تكنولوجيا المعلومات إضافة إلى جميع المستفردين منها."

المصدر: عبد الله علي فرغلي موسى، **تكنولوجيا المعلومات ودورها في التسويق التقليدي والالكتروني**، ط1، مصر، إتراك للطباعة والنشر والتوزيع، ص، ص 25-28.

تشمل تكنولوجيا المعلومات والاتصالات فرعيين أساسين هما:[1]

- **تشغيل المعلومات:** ويشمل هذا النوع الوظائف التي تتناول عمليات التشغيل الآلي للمعلومات، وتعتبر الأساس في المؤسسات وتدعيم قدرة الإدارة على اتخاذ القرارات، ويتمثل المحور المركزي لهذا الفرع في تطبيقات الإعلام الآلي في تطبيقاته المختلفة.
- **نقل وإيصال المعلومات:** يمثل هذا الفرع عملية نقل وإيصال المعلومات، التي تم تشغيلها بين المواقع المتباعدة للحواسيب ووحدتها الطرفية المتباعدة وذلك باستخدام وسائل الاتصال عن بعد.

وعليه فان تكنولوجيا المعلومات والاتصال ناتجة عن التقارب والتلاحم بين تكنولوجيا معالجة المعلومات (المعلوماتية) وبين تكنولوجيا الاتصال (أقمار صناعي، فاكس، هاتف، شبكات.)

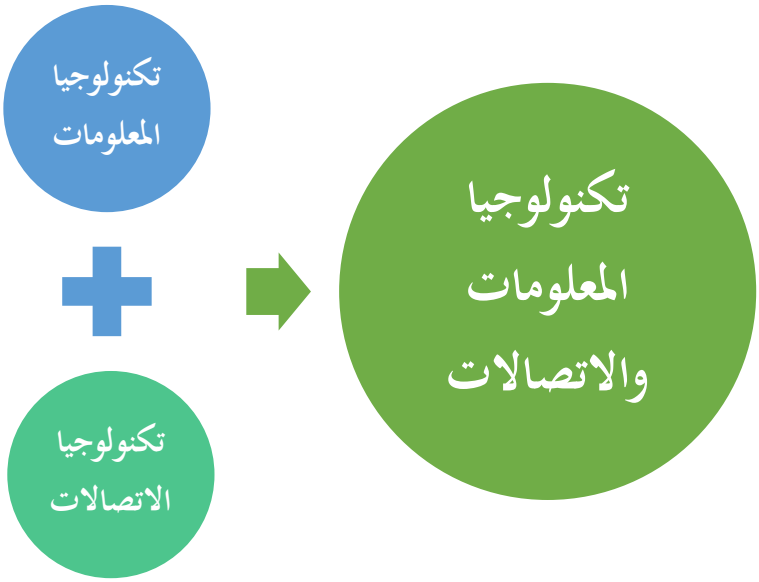
ويمكن التعبير عنها بالعلاقة التالية:

تكنولوجيا المعلومات والاتصالات = تكنولوجيا المعلومات + تكنولوجيا الاتصالات

.

[1] توامي يعقوب، **مرجع سابق**، ص 05.

شكل رقم (1) يوضح التلاحم والتقارب بين تكنولوجيا المعلومات وتكنولوجيا الاتصالات



المصدر: من إعداد الطالب.

وفي ضوء التعريفات السابقة لتكنولوجيا المعلومات والاتصالات، ينصح أنها تنطوي على:

- تغذية ومعالجة وتخزين وبث واستخدام المعلومات.
- تعتمد على العلم والخبرة والمعرفة.
- استخدام تقنيات الحاسب الآلي والاتصالات.
- تحقيق نتائج أفضل من الأساليب والوسائل التقليدية
- توفير الوقت والجهد والتكلفة
- تتكون من الأجهزة ونظم التشغيل والبرامج
- تتمتع بقدر كبير من الدقة.

وكتعريف شخصي يمكن القول بان تكنولوجيا المعلومات والاتصالات: "تركز أساسا على الجانب الآلي إضافة إلى البرامج والشبكات وغيرها من التقنيات وذلك للقيام بعمليات إدخال: معالجة وتنظيم وعرض الباتات وتحويلها إلى معلومات ذات قيمة وذلك للاستعانة بها في عمليات اتخاذ القرارات وغيرها من الأعمال الأخرى وهذا كله لتحقيق رغبات وتطلعات المستفيدين، عن طريق تقديم الخدمات بجودة عالية وفي أقل وقت وبأقل جهد."

المطلب الثاني: التطور التاريخي لتكنولوجيا المعلومات والاتصالات.

يعد العالم الذي نعيش فيه رهبن التطور والتغير السريع والمتواصل مما يعجزنا عن رصد التطور التاريخي لتكنولوجيا المعلومات والاتصالات بشكل دقيق، ولكن الأمر المسلم به هو أن تكنولوجيا المعلومات والاتصالات هي ثمرة للتطورات الحاصلة عبر الزمن ويمكن إجمال مراحل هذا التطور فيما يلي:[1]

1. **مرحلة ثورة المعلومات والاتصالات الأولى:** وتتمثل هذه المرحلة في اختراع الإنسان للأحرف ومعرفته للكتابة ومن بينها الكتابة السومرية وهذا ما نتج عنه إنهاء لعصر المعلومات الشفوية والتي تنتهي بمجرد وفاة الإنسان أو صعق قدراته الذهنية.
2. **مرحلة ثورة المعلومات والاتصالات الثانية:** وتشمل هذه المرحلة ظهور الطباعة، إذ يعد الألماني **يوهان غوتنبرغ** *(**Johannes Gutenberg**) ، بطل هذه الفترة من الفرن 16موالفاعل الأساسي في نشر المعلومات والاتصالات وذلك من خلال نشر مطبوعاته من جهة، وظهور عصر التنوير من جهة أخرى، ما أعطى للفارة الأوروبية الأسبقية للتقدم في العالم.
3. **مرحلة ثورة المعلومات والاتصالات الثالثة:** وتتمثل في اكتشاف التيليغراف سنة 1937م والذي أعطى فعالية اكبر في تبادل المعلومات إصابة إلى اكتشاف الهاتف من طرف **غراهم بل**.(**Graham Bell**)
4. **مرحلة ثورة المعلومات والاتصالات الرابعة:** بدأت هذه المرحلة من النصف الثاني من القرن العشرين حتى يومنا هذا وهي تعتمد بالدرجة الأولى على الأقمار الصناعية وشبكة الألياف البصري ذات السرعة الفائقة في نشر المعلومات والبيانات.

ويمكن إجمال أهم محطات التطور التي غرفتها تكنولوجيا المعلومات والاتصالات في الجدول التالي:

---

[1] طويهري فاطيمة، استخدام تكنولوجيا المعلومات والاتصال أداء الموارد البشرية في المؤسسة الجزائرية دراسة حالة شركة انتاج الكهرباء بتيارت، **مذكرة ماجستير**، جامعة وهران 2، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ص 19.

***يوهان غوتنبرغ** (بالألمانية: **Johannes Gutenberg**) (1398 م – 1468 م) مخترع ألماني ولد في 1398م وتوفى في 3 فبراير 1468م. قام في سنة 1447 بتطوير قوالب الحروف التي توضع بجوار بعضها البعض ثم يوضع فوقها الورق ثم يضغط عليه فتكون المطبوعة. مطوراً بذلك علم الطباعة الذي اخترع قبل ذلك في كوريا في سنة 1234م، ويعتبر مخترع الطباعة الحديثة.

جدول رقم (2) أهم محطات تطور تكنولوجيا المعلومات والاتصالات

التاريخ	التطور التاريخي لتكنولوجيا المعلومات والاتصالات
1824	اكتشاف العالم الانجليزي **وليام ستيرقون** (**William Sturgon**) الموجات الكهرومغناطيسية.
1833	اكتشاف آلة الحساب الأوتوماتكية وكانت، تحت اسم (Babbage).
1837	اكتشاف التلغراف من طرف **صامويل مورس** (**Samuel .F.B Morse**)، وهو أول نظام اتصال رقمي بعبد المدى.
1866	نصب كيبل للتلغراف عبر المحيط الأطلسي.
1876	اكتشاف الهاتف من قبل **ألكسندر غرهام بل** (**Alexander Graham Bell**). في الولايات المتحدة الأمريكية.
1895	اكتشاف اللاسلكي من قبل العالم الإيطالي **جيليلموني ماركوني** (**Gelilmoni Marconi**) حيث تم انتقال الصوت الى مسافات بعيدة من دون أسلاك
1915	خدمات الاتصالات البعيدة التي وصلت من الساحل الشرقي للولايات المتحدة الأمريكية الى سانفرانسيسكو عن طريق شركة (**AT&T**).
1921	استخدام تكنولوجيا الفاكسيميل (**Facsimile**) في الولايات المتحدة الأمريكية.
1929	ارسال اول صورة عبر ذبذبات الراديو.
1927	بداية الخدمات الهاتفية بين لندن ونيويورك وكانت مكلفة حوالي 25 دولارا للدقيقة الواحدة.
1929	أول عرض عام للجمهور عبر التلفزيون الأبيض والأسود.
1944	اكتشاف أول حاسوب الكتروني ميكانيكي(**Electro–Mechanical**) تحت إسم (**Mark1**).
1946	اكتشاف أول حاسوب الكتروني قابل للبرمجة تحت اسم (**Eniac**).
1957	إطلاق أول قمر صناعي (**Sputnik**) أطلقه الاتحاد السوفياتي سابقا.
1969	إنشاء شبكة المعلومات المحوسبة المعروفة باسم (**Arpanet**) والتي كانت نواة الانترنت فيما بعد.

1977	ظهور أول حاسوب شخصي.
1979	أول عرض لتقنية الإبعاد الثلاثية المتلفزة (**3D-TV**).
1985	اعلان شركة مايكروسوفت عن نظام التشغيل (**Windows**).
1987	ربط عشرة ألاف حاسوب بشبكة الانترنت (**Internet**)
1988	ظهور فيروس (**Worm**) على شبكة (**Arpanet**) حيث اصاب ستة الاف حاسوب من أصل ستين ألف موصول بالشبكة.
1989	البدايات الأولى لشبكة الانترنت (**Internet**). ربط أزيد مئة ألف حاسوب بشبكة الانترنت (**Internet**).
1990	تم تطوير أول محركي بحث تحت اسم (**Veronica**) و(**Archie**).
1992	ربط أزيد مئة مليون حاسوب بشبكة الانترنت (**Internet**).
1993	قيام المختبر الأوروبي لفيزياء الجسيمات (**CERN**) بتطوير معمارية لغة النص المترابطة (**HTML**) والذي أصبح من اهم وسائل استرجاع المعلومات للشبكة العنكبوتية (**WEB**).
1997	ظهور خدمة الاتصالات الهاتفية عبر الانترنت.
1998	بدايات بث التلفزيون الرقمي(**HD-TV**).
1995	اطلاق شركة ويندوز (**Windows**) لنظام تشغيلها ويندوز 95.(**Windows 95**) لغة البرمجة جافا (**Java Programming Language**)

المصدر: حسين العلمي، دور الاستثمار في تكنولوجيا المعلومات والاتصالات في تحقيق التنمية المستدامة دراسة مقارنة بين ماليزيا تونس والجزائر، **مذكرة ماجستير**، جامعة فرحات عباس سطيف كلية العلوم الاقتصادية والتجارية وعلوم التسيير، تخصص إدارة أعمال وتنمية مستدامة، 2013/2012، ص27-28 بتصرف.

المطلب الثالث: خصائص ومميزات تكنولوجيا المعلومات والاتصالات

أولا: الخصائص

- **الفعالية:** وهي تعني تبادل الأدوار بين المرسل والمستقبل، أي إن هناك ادوار مشتركة بينهما في العملية الاتصالية.
- **تحديد المستفيد:** أي انه ستتم عملية تبادل المعلومات بدرجة كبيرة من التحكم في معرفة المستفيد الحقيقي من معلومات معينة دون غيرها، وعادة ما يستخدم في هذه الحالة شخص يدعى المنسق الذي يقوم بترتيب هذه العملية، عن طريق معرفة رغبات المستفيدين وحاجياتهم من المعلومات مقابل خدماته.
- **اللاتلازمية:** هي إمكانية تراسل المعلومات بين أطراف العملية الاتصالية، من دون شرط تواجدها في وقت إرسالها، وبمعنى أخر استقبالها في الجهاز وتفحصها واستعمالها عند الحاجة.
- **قابلية التحرك والحركة:** وتعني إمكانية بث المعلومات واستقبالها من أي مكان إلى أخر، إثناء حركة المرسل والمستقبل.
- **قابلية التحويل:** ويقصد بها إمكانية نقل المعلومات من وعاء (وسيط) لأخر باستعمال تقنيات تسمح بالتحويل بين الأوعية، مثل تحويل رسالة مسموعة إلى رسالة مطبوعة.
- **قابلية التوصيل:** إمكانية استعمال أجهزة مصنعة من طرف شركات مختلفة والتواصل فيما بينها، يغض النظر عن الشركة أو البلد الذي تم فيه التصنيع.
- **العالمية والكونية:** إمكانية تبادل المعلومات بين المستفيدين من مختلف دول العالم، دون عائق المكان ومن دون الانتقال بين الحدود الدولية.
- **تقليص الوقت:** تتيح قواعد البيانات الضخمة إمكانية الوصول للمعلومات المخزنة بسهولة، وفي أقل وقت.[1]

[1] فادن عالية، أثر تكنولوجيا المعلومات والاتصال في اتخاذ القرارات الاستراتيجية دراسة حالة مطاحن الزيبان بسكرة، **مذكرة ماستر**، جامعة محمد خيضر بسكرة: كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، 2015/2014، ص 9-10.

ثانيا: المميزات:

- السرعة والدقة في انجاز الأعمال المطلوبة.
- تقليل التكاليف والحد من استخدام الملفات الورقية، والتي تأخذ حيزا كبيرا في المؤسسة.
- تحسين الكفاءة وزيادة الفعالية، وذلك من خلال القيام بالأعمال المطلوبة بالطريقة الصحيحة، مع زيادة القدرة على التنسيق بين مختلف الدوائر والأقسام.
- تحديد قنوات الاتصال بين المستويات الإدارية المختلفة، داخل المؤسسة.
- تهيئة الظروف المناسبة لاتخاذ القرارات الفعالة، وذلك عن طريق تجهيز المعلومات بشكل مختصر وفي الوقت المناسب.
- المساعدة على التنبؤ بمستقبل المؤسسة، والاحتمالات المتوقعة بغية اتخاذ الاحتياطات اللازمة في حال وجود إي خطا أو خلل في تحقيق الأهداف.
- مواكبة التطورات العالمية فيما يتعلق بأساليب خدمة الزبائن وتنويعها.[1]

[1] العربي عطية، "أثر استخدام تكنولوجيا المعلومات على الأداء الوظيفي للعاملين في الأجهزة الحكومية المحلية"، **مجلة الباحث**، العدد 10، الجزائر، 2012، ص 322.

المطلب الرابع: مكونات تكنولوجيا المعلومات والاتصالات.

يمكن تقسيم مكونات تكنولوجيا المعلومات والاتصالات إلى ثلاثة مكونات رئيسية كالاتي:[1]

1. **الأجهزة (Hardware)**: وتعرف على أنها الجزء المادي لتكنولوجيا المعلومات والاتصالات وهي تشمل:

الحواسيب بجميع أنواعها أصافة إلى جميع الأجهزة التابعة لها والمستخدمة في تنفيذ مجموعة من المهام.

2. **البرامج (Software)**: هي عبارة عن مجموعة من المكونات المعنوية لنظام الحاسب الآلي، بدءا من نظام التشغيل، تعليمات، إجراءات، برامج ولغات برمجة وتكمن مهمة هذه البرامج في عدة مهام أساسية من أهنها:
   - إدارة عمليات الحاسوب.
   - تخزين واسترجاع البيانات.
   - دعم تطبيقات الأعمال.
3. **الشبكات (Networks)**: هي عبارة عن مجموعة من الحواسيب تنظم معا، وتربط بخطوط اتصال بحيث يمكن لمستخدميها المشاركة في الموارد المتاحة، نقل وتبادل المعلومات فيما بينهم، وتستخدم هذه الشبكات لتحقيق مجموعة من الأغراض مثل:

توفير الاتصال بين الأشخاص والوصول للمعلومات عن بعد والتجارة الالكترونية وغيرها، وهناك العديد من الشبكات نذكر منها:

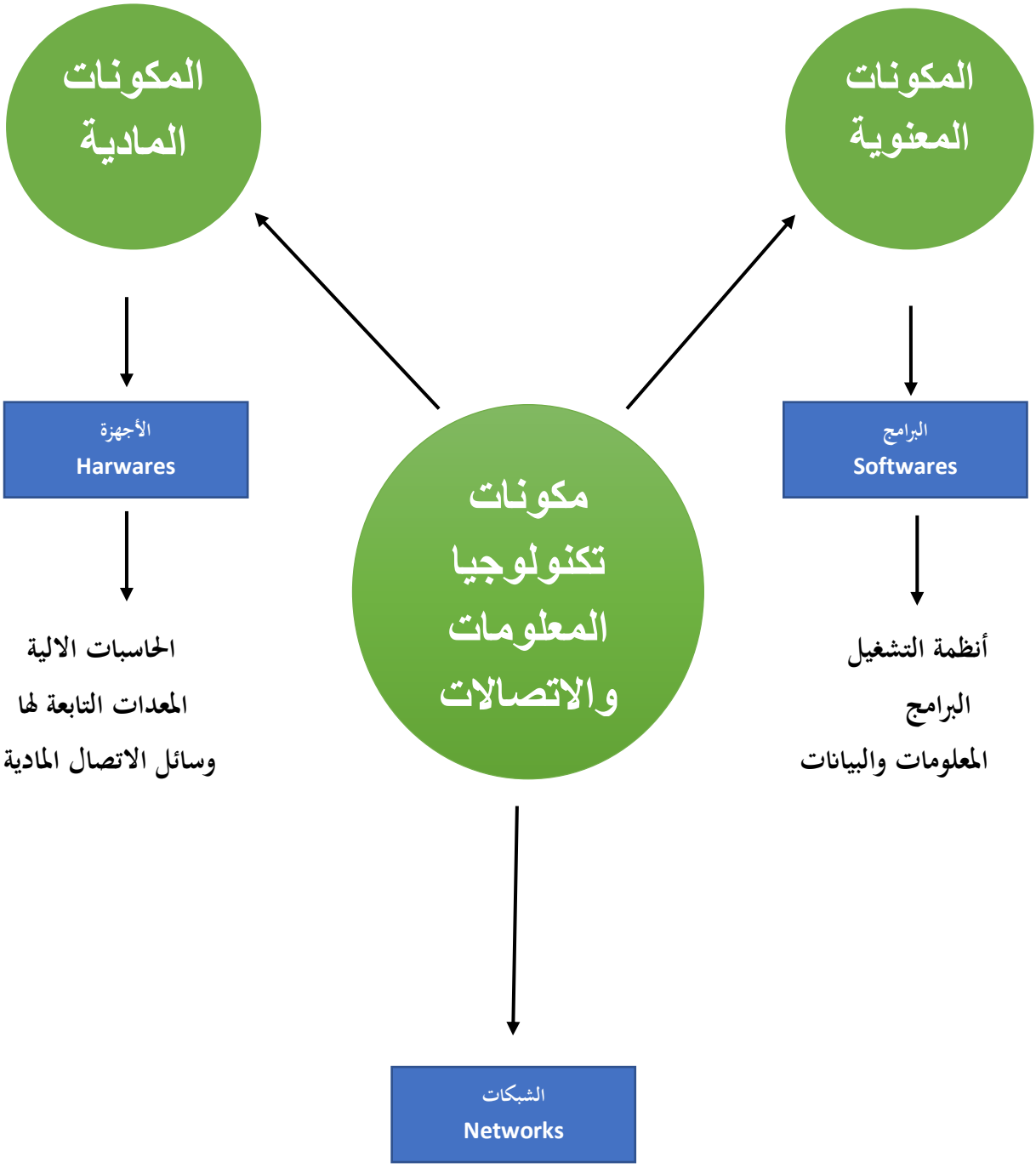
- **الشبكة المحلية(LAN)** : وهي عباره عن شبكه من الحاسبات تنقل المعلومات بسرعه عالية ضمن حيز جغرافي محدود ويكون اما ببنايه واحده أو عدة بنايات هذه الشبكة مجموعه من محطات العمل مع بعضها وهذا لإتاحة تشارك موارد الشبكة من عتاد(**Hardware**) **وبرمجيات** (**Software**) بين المحطات اضافه الى تمكين مستعملي الشبكات، من تبادل الملفات والاتصال فيما بينهم من خلال البريد الالكتروني(**E-mail**) والجلسات الحوارية (**Chat**).

[1] توامي يعقوب، **مرجع سابق**، ص 6-7.

- **الشبكة المدينة (MAN)**: يمتد مجال هذه الشبكة الى مجال او مساحة أكبر من مجال او مساحة، الشبكة المحلية، حيث تعمل الشبكة المدينة بنفس مبادئ عمل الشبكات الواسعة، الا انها تكون مقيدة بمنطقة جغرافية تكون أقل مساحة، هي تغطي عاصمة، او مدينة، او إقليم معين زمن الأمثلة على هذه الشبكات هو التغطية التليفزيونية لمنطقة معينة عن طريق الربط السلكي.
- **الشبكة الواسعة (WAN)**: هي عبارة عن شبكة لتبادل المعلومات الرقمية ضمن مجال جغرافي واسع قد تشمل عدة دول، وهي أكبر من الشبكة المدينة، قد تستخدم خطوط الهاتف، والأقمار الصناعية وغيرها من الوسائط نقل البيانات وفي بعض الأحيان قد تتكون الشبكة الواسعة من عدة شبكات محلية، وتكمن فائدة هده الشبكات فأنها تتيح نقلا سريعا للمعلومات.
- **الانترنت (Internet)**: أو ما يعرف بالشبكة العنكبوتية وهي مشتقة من وتمثل هذه الأخيرة واحدة من شبكات الحاسب الآلي وتتميز بانتشارها الواسع في مختلف بلدان العالم وهي تعتبر أكبر وسيلة للاتصال والمعلوماتية. [1]

[1] شادلي شوقي، أثر استخدام تكنولوجيا المعلومات والاتصال على أداء المؤسسات الصغيرة والمتوسطة بولاية الجزائر، **مذكرة ماجستير**، جامعة قاصدي مرباح ورقلة: كلية العلوم الاقتصادية، قسم العلوم الاقتصادية، تخصص تسيير المؤسسات الصغيرة والمتوسطة، 2008/2007، ص 16.

شكل رقم (2) يوضح مكونات تكنولوجيا المعلومات والاتصالات



المصدر: من إعداد الطالب.

المطلب الخامس: إشكاليات وتحديات تكنولوجيا المعلومات والاتصالات

تعددت إشكاليات وتحديات تكنولوجيا المعلومات والاتصالات في العصر الحالي، فمنها ما تُعدّ إشكاليات وتحديات مباشرة ومنها ما تعدّ غير مباشرة، ومن أهمها:

1) **الجريمة السيبيرانية (Cyber crime)**: تعرّف الجريمة السيبيرانية بأنها أي نشاط تستخدم فيه الحواسيب أو الشبكات كأداة أو هدف أو مكان لممارسة النشاط الإجرامي. وهي أيضاً أنشطة معتمدة على الحاسوب تُعد إما غير قانونية أو غير مشروعة من جانب أطراف معينة، ويمكن الاضطلاع بها عن طريق الشبكات الإلكترونية العالمية. ويمكن التفريق بين أربعة أنواع مختلفة من الجرائم السيبيرانية هي: "الجرائم التي تستهدف سرية البيانات والنظم الحاسوبية وتكامليتها، الجرائم المتعلقة بالحاسوب، الجرائم المتعلقة بالمحتوى، والجرائم المتعلقة بحقوق المؤلف[1].

2) **القرصنة التقنية وأمن المعلومات (Hacking and information security)** :

إن القرصنة التقنية المتمثلة في نسخ محتويات الأقراص المضغوطة (مثل برامج الكمبيوتر) تشكل خطرًا كبير يهدد الملكية الفكرية إذ أنّه تمثل انتهاكًا لحقوق الغير، تمنعهم من استيفاء حقوقهم كاملة. إنه من السهل حماية ملكية الأشياء من معدات وموارد طبيعية، لكن الأمر أكثر تعقيدًا بالنسبة لحماية الملكية الفكرية.

3) **هجرة الأدمغة (Brain Drain)** : تشكل هجرة الأدمغة جزءا مهما من التدفق المعرفي في عصر العولمة، وتتأثر بالتحولات في البيئات التمكينية الجاذبة منها أو الطاردة . فالحاجة للكفاءات والخبرات والموارد البشرية ازدادت بشكل ملحوظ في جميع أرجاء العالم، بما في ذلك أوروبا والولايات المتحدة الأمريكية التي لم تعد قادرة على إنتاج المهارات محليا وبالتالي أصبحت تبحث عنها في الدول النامية بشكل خاص، وتمثل ظاهرة هجرة الأدمغة نزيفًا حقيقيا يكبد البلد الأصلي خسائر اقتصادية جد معتبرة، حيث أن النفقات الطائلة التي صرفت للاستثمار في الرأسمال البشري لم يجد منها البلد العائد المنتظر.

4) **الفجوة الرقمية (Brain drain)** : هناك العديد من المصطلحات تتقارب مع هذا الموضوع مثل مصطلح الفجوة المعرفية والتي تدل على زيادة دور المعرفة مقارنة مع الأرض ووسائل الإنتاج، وهناك مصطلح

[1] M. Gercke, Understanding **Cyber Crime ITU Telecommunication Development Sector**, 2nd Ed, 2011, p 25.

الفجوة التقنية والذي يشير إلى الفروق بين من يملك التقنية ومن لا يملكها، وهو يركز على حيازة بلدان ما بعد الثورة الصناعية على تقنيات الإنتاج بمختلف أنواعها مدعومة بنتائج الثورة العلمية و التكنولوجية.

أما مصطلح الفجوة الرقمية فهو استكمال لمصطلح الفجوة التقنية مع التركيز على أخر مستجدات العلوم وخصوصا ما يتعلق بالمنتجات المعرفية كالبرمجيات وغيرها بالتوازي مع حاملها الأساسي شبكة الانترنت.

إن التطور السريع في مجال تكنولوجيا المعلومات والاتصالات سيؤدي حتما إلى توسع الفجوة الرقمية بين اللذين يملكون التكنولوجيا وبين اللذين لا يملكونها، وخطورة الفجوة الرقمية وإن خطورة الفجوة الرقمية لا تتعلق بانعكاساتها التلقائية المباشرة على الدخل بقدر ما تتعلق بانعكاساتها على النفوذ، والتي تعود بسلسلة من الانعكاسات السلبية المتصاعدة على الأمن والصحة والتعليم والعلاقات الإنسانية والدخول، وكذلك على الحق الإنساني في الإبداع وفي الاستفادة من المعلومات.[1]

[1] حسين العلمي، **مرجع سابق**، ص 29-30

المبحث الثاني أمن المعلومات مفهومه تاريخه، عناصره وتحدياته.

يوما بعد يوم يزداد حجم المعلومات والبيانات المتداولة في العالم، ويزداد الاهتمام بها في المجالات المدنية العسكرية والسياسية والاقتصادية وغيرها، ومع هذا التوسع الكبير في استعمال والاعتماد على المعلومات تزداد الحاجة للمحافظة عليها والإبقاء على سريتها، خاصة عندما يتعلق الأمر بالمعلومات الحساسة.

سنتطرق في هذا المبحث إلى أهم المصطلحات التي لها علاقة بأمن المعلومات ثم مفهومه، تاريخه وتختم المبحث بأهم عناصره وتحدياته.

المطلب الأول: مفاهيم أساسية حول امن المعلومات.

- **الثغرات الأمنية (Vulnerability)**: هو مصطلح يطلق على مناطق الضعف الموجودة في مختلف نظم المعلومات، وأنظمة التشغيل وغيرها والتي يمكن من خلالها التسلل إلى هذه الأنظمة، ومن ثم يتم التعديل على المعلومات الموجودة داخلها، حذفها أو التجسس عليها وتشمل هذه الثغرات كذلك برامج الحاسب وتكون نتيجة أخطاء برمجيه يرتكبها المطورون إثناء تطويرهم لهذه البرامج.
- **التهديد (Threat)**: هو عبارة عن إي ظرف أو حدث يمكنه إن يؤثر سلبا على الأصول، الإفراد، نظم المعلومات أو الحواسيب والشبكات التي توجد داخل المؤسسة ويكون ذلك عن طريق الوصول الغير المصرح أو تعديل المعلومات او حتى الحرمان من الخدمات المقدمة من طرف هذه المؤسسة الكترونيا.
- **الهجوم (Attack)**: هو عمليه تتم من خلالها محاوله الوصول الغير مصرح به للمعلومات أو إلحاق الضرر بالأنظمة الداعمة لها ويكزن ذلك إما بصورة متعمدة أو غير متعمدة.
- **الاختراق (Hacking)**: الاختراق أو القرصنة هو عبارة عن عملية يتم من خلالها استخدام الشخص لقدراته، خبراته ومهاراته في المجال التقني، للوصول إلى نظم المعلومات أو الوصول إلى نظم حاسوبية ليس له الحق في الوصول إليها أو الاطلاع عليها.[1]

[1] HL7 Secure Transactions, **Glossary Of Acronyms**, **Abbreviations and Terms Related To Information Security In Healthcare Information Systems**, 1999, p 09-10.

- **الاختراق الأخلاقي (Ethical Hacking)**: هي عملية اختراق تكون مصرحة ويكون الغرض منها ليس السرقة والتجسس ولا تعطيل الخدمات وإنما تكون لأغراض أخرى كالكشف عن نقاط الضعف والثغرات الأمنية ومعالجتها.
- **الأصول (Assests)**: هي جميع ممتلكات ومواد المنظمة والتي يجب حمايتها، يمكن إن تكون هذه الأصول معنوية كمواقع الانترنت، والمعلومات والبيانات الخاصة بالموظفين أو العملاء، وقد تكون مادية كالمستخدمين والأجزاء المادية.
- **الخصوصية المعلوماتية:** ويقصد بها الحفاظ على البيانات والمعلومات الشخصية من الاستخدام الغير المخول، كالإضافة عليها أو تعديلها أو حذفها تماما.
- **السرية المعلوماتية:** ويقصد بها الحفاظ على البيانات والمعلومات الشخصية من السرقة وذلك باستخدام تقنيات مختلفة، ككلمات المرور والتشفير وغيرها.
- **الاستغلال (Exploit)**: هو عبارة عن برنامج يسمح للمهاجمين الوصول إلى الأنظمة وكسرها بشكل آلي (اتوماتيكيا) ويتم هذا عن طريق استغلال الثغرات الأمنية.
- **نظام المعلومات(Information System)** : هو عبارة عن نظام يتكون من الإفراد، المعلومات، وسجلات البيانات يعمل على جمع، معالجة، صيانة، استخدام، مشاركة، نشر والتصرف بالمعلومات.
- **تسريب المعلومات (Data leakage)**: هو مصطلح يستخدم لوصف العملية التي يتم من خلالها الإفراج عن بيانات الشركات الحساسة، ترتبط هذه المعلومات عادة بالتمويل العملاء أو الملكية الفكرية، وغيرها من المعلومات السرية الأخرى.
- **Dumpster Diving** : يستخدم هذا المصطلح في سياق تكنولوجيا المعلومات، ويشير إلى العملية التي يتم من خلالها البحث عن البيانات والمعلومات المحذوفة، وذلك للحصول على معلومات بإمكانها مساعدة المهاجم في القيام بهجماته قد تكون هذه البيانات إما كلمات مرور، أرقام سرية أو رموز الوصول.[1]
- **سرقة الهوية (Identity Theft)**: تحدث سرقة الهوية عند قيام شخص ما بسرقة معلومات شخصية خاصة بشخص أخر، وذلك لاستخدامها للأغراض غير مشروعة كالاحتيال مثلا.

[1] **Ibid**, p 14-15.

- **فحص الضعف:** هي عملية آلية الهدف منها التحديد المسبق للثغرات الأمنية في النظم الحوسبة، لمعرفة ما إذا كانت قابلة للاستغلال (**Exploit**) أو الاختراق (**Hacking**).
- **التوقيع الالكتروني (Digital Signature)**: هو عبارة عن عملية، تشفير مكونة من حروف، رموز، أو أرقاما الكترونية، تصدر عن يعص الجهات الشخصية والمعترف بها حكوميا ودوليا، يعمل على توثيق الملفات بشتى أنواعها المتناقلة عبر الانترنت فيتم من خلاله ربط هوية الموقع بالوثيقة بحيث يمكن مستلم الوثيقة التحقق من صحة التوقيع، والتأكد من المحتوى الأصلي للرسالة.
- **البيانات (Data)**: هي عبارة عن كلمات، حروف، أرقام أو رموز أو حتى صور لم تتم معالجتها وإنما يتم جمعها لهدف معالجتها وبالتالي يمكننا القول بان البيانات هي المعلومات التي لم يتم معالجتها بعد.
- **المعلومات (Informations)**: هي البيانات التي تمت معالجتها بحيث تصبح ذات معنى وقيمة عند الأشخاص الذين يستقبلونها.
- **الجريمة الالكترونية (Cyber Crime)**: هي عبارة عن كل عمل غير قانوني، يتم استنادا على الحواسيب والانترنت وتشمل هذه الجريمة التجسس، سرقة الهوية وسرقة معلومات بطاقات الائتمان وغيرها.[1]
- **المواصفة الدولية (ISO 27001:2005)**: تحدد المواصفة الدولية (**ISO 27001:2005**) متطلبات إنشاء وتطبيق وتشغيل مراقبة وإعادة النظر في صيانة وتحسين نظام موثق لإدارة أمن وسرية المعلومات من خلال الإطار العام لإدارة مخاطر العمل داخل المؤسسات. كما تحدد المواصفة متطلبات تطبيق ضوابط لأمن وسرية المعلومات بما يتناسب مع احتياجات المؤسسات أو بعض إدارتها أو جهات تابعة لها من الممكن أن تطبق هذه المواصفة بأية جهة مهما كان نشاطها أو مجال عملها.[2]

[1] ICAEW, **Glossary of IT security terms**, London, Uk, 2013, p 60…62.

[2] الشريف بوفاس وفاطمة الزهراء طلحي، نحو بناء نظم لإدارة حماية المعلومات ISO27001 في المؤسسات الجزائرية، **المؤتمر الدولي الثاني للذكاء الاقتصادي حول اليقظة الاستراتجية ونظم المعلومات في المؤسسة الاقتصادية**، جامعة باجي مختار عنابة، 2014، ص 6.

المطلب الثاني: مفهوم أمن المعلومات

إن مصطلح أمن المعلومات سابق على وجود التقنيات المعلوماتية المرتبطة بالحاسب الآلي، إلا أن الصدارة التي احتلتها هذه التقنيات من سرعة في النقل والاتصال والتخزين جعلت مصطلح امن المعلومات يرتبط بها.

سنتطرق في هذا المطلب إلى تعريف مختصر لمصطلح الأمن، ثم نعرض جملة من التعريفات حول امن المعلومات

1) تعريف الأمن:

يعترف علماء الأمن والاستراتيجية في الغرب صراحة بغموض وتشابك مفاهيم الأمن، حتى أصبح من الصعوبة عندهم الاتفاق على تعريف موحد للأمن يحصى بقبول علمائه والمهتمين بدراسته.

وقد اجتهد نخبة من الباحثين والكتاب في محاولة تأصيل هذا الحقل ومنهم **دانييل كوهمان (Daniel Kohman)** وغيرهم في كتابه، الأمن الوطني الهيكل التحليلي، والذي جاء فيه بان مصطلح الأمن يتسم بالغموض وشدة الاختلاف في المعنى من مجتمع لأخر بحسب ثقافة كل مجتمع وموقعه، وقد عرفه بذلك على انه: "حماية الأمة والمحافظة عليها من أي عدوان خارجي **(Protection From External Threats)**".

ويقر وزير الدفاع السابق في الولايات المتحدة الأمريكية **براون (Brown)** بان الأمن هو: "المقدرة على المحافظة على الأمة وعلى كرامتها وأراضيها واقتصادها وحماية مواردها الطبيعية، ودستورها من إي اعتداء خارجي."[1]

ويمكن تعريف الأمن باختصار على انه ثلاثة أشياء:

- الحماية **(Prevention)**: ويقصد بها الإجراءات الوقائية لحماية الممتلكات من التضرر.
- كشف وقوع الضرر **(Detection)**: اكتشاف شيء تم سرقته، تعديله أو تخريبه.
- رد الفعل **(Reaction)**: الإجراءات التي يجب القيام بها عند حدوث خرق للأمن.[2]

[1] محمد جمال مظلوم، **الأمن الغير تقليدي**، ط1، الرياض: جامعة نايف للعلوم الأمنية، 2013، ص 15.

[2] خالد ياسين الشيخ، أمن نظم المعلومات والرقابة، **مذكرة ماجستير**، جامعة دمشق، المعهد العالي للتنمية الإداري، تخصص التأهيل والريادة والإدارة والإبداع، 2015/2014، ص 14.

ويرى **هنري فايول** (**Henry Fayol**) في كتابه "الإدارة العامة والصناعية" الصادر سنة 1916يرى أن هناك ستة أنشطة هامة تقوم بها الإدارة وذكر من بينها الأمن (**Security**)ومن هنا عرفه على انه: "حماية الأفراد والممتلكات والأصول والمعلومات الخاصة بالمؤسسة."[1]

شكل رقم (3) يوضح الأنشطة التي تمارسها الإدارة حسب هنري فايول (Henry Fayol)

Source : V.S Bagad, **Financial and industrial management**, 1st edition, india: technical publication pune, 2008, p10.

[1] **Ibid**, p 9.

2) **تعريف أمن المعلومات:**

اختلف الباحثون والدارسون لهذا المجال على وضع تعريف موحد لأمن المعلومات فمنهم من عرفه من زاوية أكاديمية، ومنهم من عرفه من زاوية تقنية ويمكن إجمال هذه التعريفات فيما يلي:

عرف **فلاديمير قوان (Vladimir Gnuan)** امن المعلومات على أنه: "جميع الوسائل التي يتم توفيرها للحد من ضعف نظام المعلومات، ضد مختلف التهديدات سوءا المفاجئة أو المتعمدة. وبعبارة أخرى هي مجموع التقنيات التي تضمن لموارد نظام المعلومات سوءا (الأجهزة أو البرامج) الاستخدام الأمثل وفي السياق المحدد."

وبصفة عامة فان منهجية أمن المعلومات تقوم على ثلاثة عناصر مهمة كالاتي:

1) **إجراء تحليل للمخاطر (Effectuer une analyse des risques)**: وذلك لأنه من غير الممكن حماية أصول المؤسسة من المخاطر التي لست على علم بها، ويتم ذلك عن طريق قياس احتمال حصولها والآثار المحتملة الناجمة عنها.

ويعبر المختصون عن الخطر وفقا للمعادلة التالية:

الخـــــــطر = الضـــــــرر x احتمـــــــال الحدوث

2) **وضع سياسة أمنية:** ويتم ذلك مباشرة بعد إجراء فحص أو تحليل للمخاطر ويكون الهدف من هذه السياسة هو:
   - تحديد إطار استخدام موارد المعلومات.
   - تحديد التقنيات الأمنية التي سيتم توفيرها في مختلف مصالح المؤسسة.
   - توعية الموظفين والمستخدمين حول أهمية امن المعلومات.
3) **تنفيذ التقنيات الأمنية:** هذه التقنيات هدفها هو تلبية المتطلبات الأساسية لسلامة تكنولوجيا المعلومات داخل المؤسسة.[1]

[1] Vladimir aman Gnuan, **Concevoir la sécurité informatique en entreprise**, 2014, p 13…15.

ويعرف **ادام شوستاك** (**Adam Shostack**) أمن المعلومات على انه: "التأكد من أن نظم المعلومات يمكن أن تعمل بالشكل المطلوب وعلى النحو المقصود في بيئة معادية."[1]

وعرفه **فارمان** (**Warman A.R**) على انه: "مجموعة من الإجراءات والتدابير الوقائية والتي تستخدم سوءا في المجال التقني أو الوقائي بهدف الحفاظ على المعلومات، الأجهزة والبرمجيات، فصلا عن الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال."

ويرى **دومين** (**Doomun**) ان الامن هو ذات أهمية قصوى اذ ينبغي على المنظمة خدمة العديد من المنافسين والمستهلكين المباشرين ولذا ينبغي الحفاظ على السرية التامة للمعلومات المرسلة إليهم.[2]

وفيما يلي جملة التعريفات حول أمن المعلومات:

"هو العلم المختص بتامين المعلومات المتداولة عبر الشبكة من المخاطر التي تهددها، وهو كذلك العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها، أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية والخارجية."[3]

"هو مجموعة الإجراءات والضوابط والقواعد والتشريعات التي توضع للحفاظ على سلامة وتكامل نظام المعلومات من التخريب والعبث والفقدان، وكذلك من التغيير والاستعمال الغير المصرح به سوءا كان هذا التغيير او التخريب مقصودا ام غير مقصود."[4]

[1] Adam Shostack, "the evolution of information security", **the next wave**, vol 19, N° 2, 2012, p 8.

[2] ندى إسماعيل جبوري، "حماية امن انظمة المعلومات دراسة حالة مصرف الرافدين"، **مجلة تكريت للعلوم الإدارية والاقتصادية**، مجلد رقم 7، ع رقم 21، بغداد، 2011، ص 67.

[3] **https://ar.wikipedia.org/wiki/امن المعلومات** page consulter le 19/02/2018 23 :41.

[4] عبد الرحمان شعبان عطيات، **أمن الوثائق والمعلومات**، ط1، الرياض: جامعة نايف العربية للعلوم الامنية، 2003، ص 122.

"وتعرف هيئه الاتصالات وتقنيه المعلومات السعودية امن المعلومات بانه إبقاء معلوماتك تحت سيطرتك المباشرة وعدم امكانيه الوصول اليها من طرف شخص أخر دون اذنك وأن تكون على علم بالمخاطر المترتبة عند السماح لشخص ما بالوصول الى معلوماتك الخاصة."[1]

ويعرف امن المعلومات كذلك على انه: "حماية المعلومات ونظام المعلومات من الاستخدام أو الوصول الغير المصرح، أو الكشف والتعطيل أو التدمير والتعديل، ووفقا للقانون الأمريكي فان أمن المعلومات هو السعي لحماية البيانات الخاصة بك مهما كانت حساسيتها من هؤلاء الذين يريدون إساءة استخدامها."

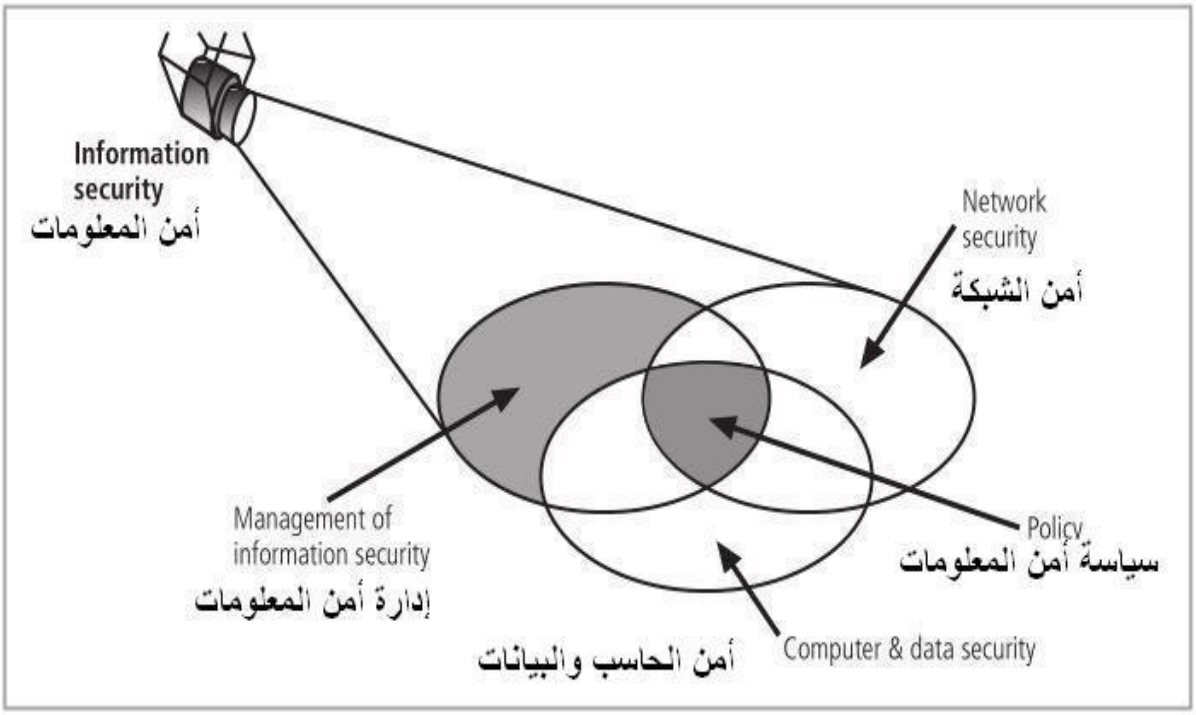
"وهو كذلك الأساليب والوسائل المعتمدة، للسيطرة على كافة أنواع ومصادر المعلومات وحمايتها من النسخ، السرقة او التعديل أو الابتزاز أو التلف أو الضياع أو حتى التزوير والاستخدام الغير قانوني، فهو الإحساس الفعلي بعدم وجود إي تهديد للبنية المعلوماتية، وتجهيز البدائل لمجابهة إي تهديد حقيقي."[2]

ويوضح الشكل في الأسفل أن أمن المعلومات يشمل مجالات واسعة لإدارة امن المعلومات، أمن الحاسب والبيانات، وأمن الشبكات

[1] **https://www.internet-gov.sa/learn-the-web-ar/guides-ar/information-security-and-the-internet-ar**. Page consulter Le 19/02/2018 à 00:54.

[2] Jason Andress, **the basics of information security**, 2nd Ed, 2014, Usa, p3.

شكل رقم (4) يوضح مكونات امن المعلومات.



Source : Michael whitman and Harbert Mathord, **principles of information security**, 5th Ed, usa, 2012, p4.

وكتعريف شخصي يمكن القول بان امن المعلومات هو:

- **من الناحية الأكاديمية:** هو العلم الذي يبحث في نظريات واستراتيجيات وتقنيات توفير الحماية للمعلومات من مخاطر الاعتداء عليها.
- **أما من الناحية التقنية:** هي الوسائل والإجراءات الواجب توفرها لضمان حماية المعلومات من مختلف التهديدات المتوقعة.
- **ومن الناحية القانونية:** فهي جميع القوانين والتشريعات سواء سوءا كانت وطنية أو دولية التي تهدف إلى مكافحة الجرائم المرتكبة ضد المعلومات ونظمها ومن تم معاقبة مرتكبي هذه الجرائم.

المطلب الثالث: تاريخ أمن المعلومات

ارتبط تاريخ امن المعلومات مع تاريخ امن الحاسب، فامن الحاسب يركز على تامين المواقع المادية، والأجهزة والبرامج من التهديدات التي ظهرت خلال الحرب العالمية الثانية، حيث كان امن المعلومات خلال هذه السنوات عبارة عن عملية بسيطة تشمل غالبا الأمن المادي، وكانت التهديدات الرئيسية لأمن المعلومات في هذه الفترة تتمثل في السرقة المادية للمعدات والتجسس على منتجات المنظمات والتخريب.

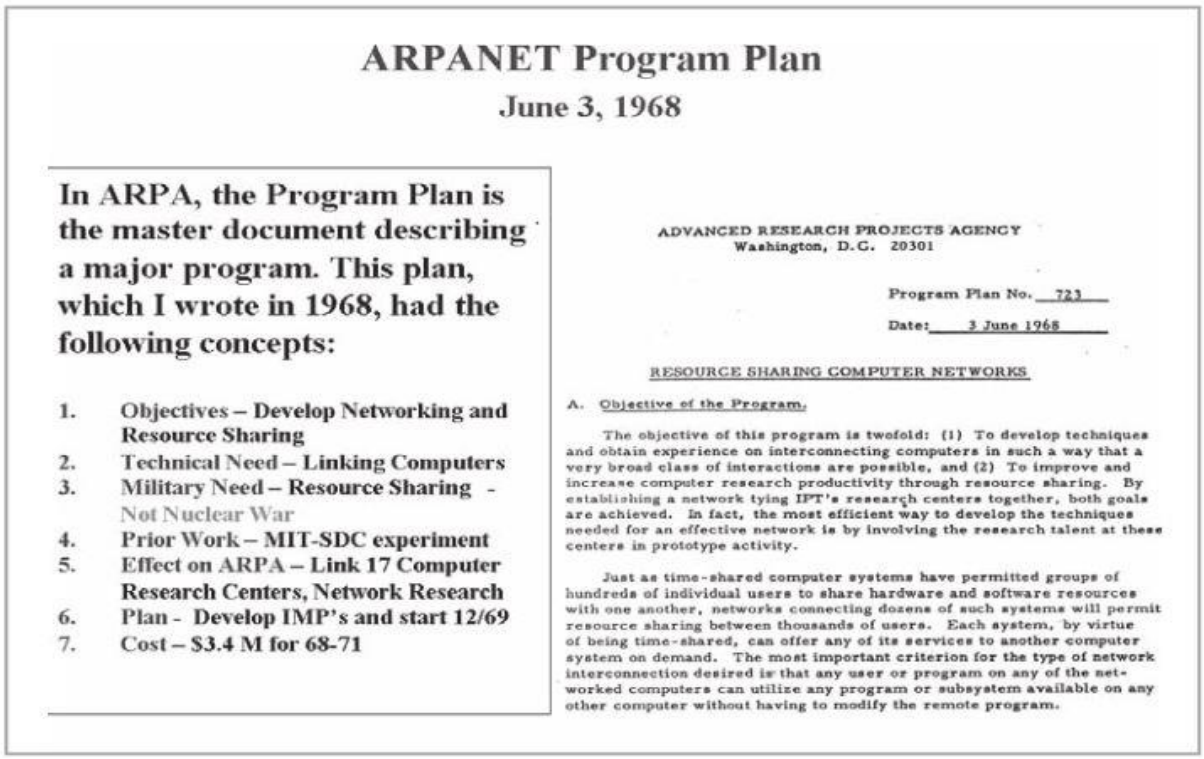
ولعل واحدة من أولى المشاكل التي وقعت خارج المهددات التي كانت مألوفة في تلك الفترة هي حين كان مسئول نظام يعمل على ملف به رسالة وكان الأخر يعمل على تحرير ملف كلمة المرور، ومع حدوث خلل في إحدى البرامج تم الخلط بين الملفين مما ترتب عنه طباعة كلمة المرور على جميع المخرجات.

ويمكن استعراض أهم تطورات أمن المعلومات فيما يلي:

- **من 1960 إلى 1970**:خلال الحرب الباردة تم جدب العديد من الإطارات للقيام بمجموعة من المهام وكانت هذه الأخيرة تتسم بنوع من التعقيد، ولدا أصبح من الضروري تمكين هذه الإطارات من التواصل عبر عمليات اقل تعقيدا مما كانت عليه في السابق واستجابة لهذه الحاجة بدأت وكالة مشاريع البحوث المتقدمة التابعة لوزارة الدفاع الأمريكية **Advanced Research Project** (**A**.**R**.**P**.**A**) **Agency** دراسة إمكانية إنشاء شبكة اتصالات، وشبكة تدعم نقل المعلومات العسكرية وتبادلها وهذا ما حدث فعلا حيث قام **لاري روبرتس** (**Larry Roberts**) والذي أطلق علية لقب مؤسس الانترنت قام بتطوير المشروع و الذي سمي **بالاربانت** (**Arpanet**).[1]

[1] **Ibid**, p 4-5.

شكل رقم (05) يوضح تطوير خطة برنامج الاربانت(Arpanet)


ARPANET Program Plan
June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Source :**Ibid**, p 4.

- **من 1970 الى 1980**: خلال هذه الفترة أصبحت شبكة **الاربانت** (**Arpanet**) أكثر شعبية وأصبحت تستخدم على نطاق واسع مما كانت عليه في الفترة السابقة.

وفي ديسمبر من عام 1973 ومع تطوير بروتوكول (**Ethernet**) والذي يعد واحدا من بروتوكولات الشبكات الأكثر شعبية والذي يعود الفضل في تطويره الى **روبرت بوب** (**Robert Bob**)، حيث صاحب هذا التطوير العديد من المشاكل الأمنية على شبكة **الاربانت** (**Arpanet**) فلم يكن لذا المواقع الفردية الناشئة ضوابط كافية وضمانات لحماية البيانات من المستخدمين الغير مصرح لهم رؤيتها، لم يكن هذا هو المشكل الوحيد بل العديد من المشاكل كضعف بنية كلمة المرور، عدم وجود إجراءات السلامة للاتصالات الهاتفية، عدم تحديد هويات المستخدمين وصلاحيات مستعملي النظام، كل هذه المشاكل أدت الى تسريب العديد من ارقام الهواتف، ومن هنا بدا الاهتمام بالأمن المعلوماتي والذي تجاوز الحماية المادية كما كان الحال في الستينات.

وفي سنة 1967 شكات وكالة مشاريع البحوث المتقدمة **Advanced** (**A**.**R**.**P**.**A**) **Research Project Agency** فريق عمل لدراسة تامين نظم المعلومات حيث اجتمعت هده اللجنة وصاغت العديد من التوصيات جاءت تحت اسم تقرير (**R609–1**) وبعد هذا الأخير بمثابة اول وثيقة منشورة حددت قضايا واشكاليات امن الحاسب، وأكدت ان الاستخدام الواسع لمكونات الشبكات ونظم المعلومات من طرف الجيش الأمريكي قد ادخل العديد من المخاطر والتهديدات الأمنية والتي لا يمكن الحد منها عن طريق الممارسات الروتينية التقليدية اضجت هذه الوثيقة محورية في تاريخ امن المعلومات ووسعته من النطاق الضيق الذي كان عليه الذي كان يشمل سلامة المعدات المادية ليصبح يشمل ما يلي:

- تامين البيانات.
- الحد من الصول العشوائي والغير مصرح به لهذه البيانات.
- اشراك الموظفين من مختلف المستويات في المسائل المتعلقة بأمن المعلومات.[1]

- **1990**: مع نهاية القرن العشرين أصبحت شبكات الحواسيب أكثر شيوعا، مما أدى الى ظهور شبكة الانترنت وهي أول شبكة عالمية متاحة لعامة الناس والتي كانت حكرا على الأوساط الحكومية، الأكاديمية والعسكرية فيما قبل إضافة الى التطورات التي حصلت فهذه الفترة وظهور العديد من الخدمات كالبريد الالكتروني (**E–mail**) وغيره أصبحت المعلومات أكثر عرضة للمهددات والمخاطر.
- **من 2000 الى يومنا هذا:** أصبحت الانترنت تجلب العديد من المستخدمين، و شهدت السنوات القليلة الماضية وعيا متزايدا بأمن المعلومات، ومع تزايد المعلومات الالكترونية والاعتماد على التكنولوجيات الحديثة، زادت معدلات الهجمات الالكترونية مما جعل الحكومات و الشركات تولي اهتماما بالغا بهذا المجال، حيث شهد هذا الأخير تطورات عديدة خاصة في التقنيات المستخدمة لحماية المعلومات، وأصبحت هناك شركات ناشئة متخصصة هدفها الكشف عن الثغرات الأمنية ومن تم محاولة إصلاحها، وكمثال على ذلك نجد شركة *(**VUL9 Security Solutions**) وهي تعمل مع كبرى الشركات العالمية، وكذلك مع

[1] **Ibid**, p 6-7.

***Vul9 Security Solutions**: هس عبارة عن شركة ناشئة ومتكاملة مختصة في الأمن السيبيراني، متعددة المهام تهدف الى بناء فضاء سيبيراني أكثر امانا في دول الخليج وشمل افريقيا، تم تأسيسها من طرف مغربيان وتقع في دبي وسيتم افتتاح فروع لها في شمال افريقيا قريبا.

جهات وادارات حكومية في كل من المغرب، السودان والامارات العربية، فضلا عن استحداث العديد من المعايير والمواصفات الدولية في هذا المجال.

المطلب الرابع: عناصر أمن المعلومات

حدد بعض الباحثين والمهتمين بأمن المعلومات ثلاثة عناصر أساسية ينبغي توفيرها والاهتمام بها لفهم وتوفير أمن المعلومات وجاءت هذه العناصر تحت مسمى ثالوث أو مثلث امن المعلومات (**The CIA Triad**) وكان هذا سنة1987.

ويمكن تعريف هذه العناصر على انها: "مجموعة من المكونات الواجب توفرها للحفاظ على المعلومات الثابتة والمنقولة من أي نوع من أنواع الاستغلال والاعتداء، بحيث لا يطلع عليها سوى الأشخاص المصرح لهم، حيث ان كل عنصر من هذه العناصر مهم للإبقاء على سرية وسلامة البيانات وان أي نقص في عنصر من هذه العناصر سيؤدي حتما الى المساس بسرية وسلامة المعلومات."

أ. وجاء نودج ثالوث امن المعلومات (**The CIA Triad**) بثلاثة عناصر كالاتي: [1]

1. **سرية المعلومات** (**Data Confidetiality**): الغاية من هذا العنصر، هو التأكد من ان المعلومات السرية و الحساسة لا تكشف ولا يتم الاطلاع عليها من قبل اشخاص غير مخولين او غير مصرح لهم بذلك وهذا يعني ان المعلومة مؤمنة، ولا يطلع عليها الى من طرف الأشخاص او الأقسام الذين لهم صلاحيات الاطلاع، ومن هنا يجب الحرص على درجة السرية، وتقسيم المعلومات حسب درجة أهميتها وحساسيتها، وفي المقابل يتم تصنيف الأشخاص الذين يحق لهم الوصول لهذه المعلومات وكذلك نوع هذا الوصول هل هو للطلاع فقط ام للنسخ و التعديل كما ان هؤلاء الأشخاص الذين يطلعون على معلومات معينة قد لا يكون لديهم الحق في الاطلاع على معلومات أخرى.
2. **توفر المعلومات** (**Data Availability**): يشير هذا العنصر الى وجوب ديمومة وتوفر المعلومات، أي ان تكون المعلومات متوفرة ومتاحة لدى الطلب من قبل الأشخاص المخولين بالاطلاع، وبمعنى اخر حماية المعلومة من أي خطر من اخطار الهجوم او التعدي وباي أسلوب كان هذا التعدي.

[1] عبد الرحمان شارع العتيبي، دور الامن السيبيراني في تعزيز الامن الإنساني، **مذكرة ماجستير**، جامعة نايف للعلوم الأمنية: كلية العلوم الاستراتيجية، قسم الامن الإنساني، 2015، ص 14-15.

3. **سلامة المعلومات وتكاملها (Data Integrity)**: ويقصد بهذا العنصر أن تكون المعلومات سليمة في محتواها، ولم تتعرض لأي محاولة للإتلاف أو التغيير سوآءا كانت هذه المحاولة مقصودة أو غير مقصودة، ويوضح الشكل في الأسفل نموذج مثلث أمن المعلومات.

شكل رقم (06) يوضح نودج مثلث أمن المعلومات (The CIA Triad)

Source : http://www.marianowo.org/network-security-cia-seven-exciting-parts-of-attending-network-security-cia-225 page consulter le 05/04/2018 à 19:23.

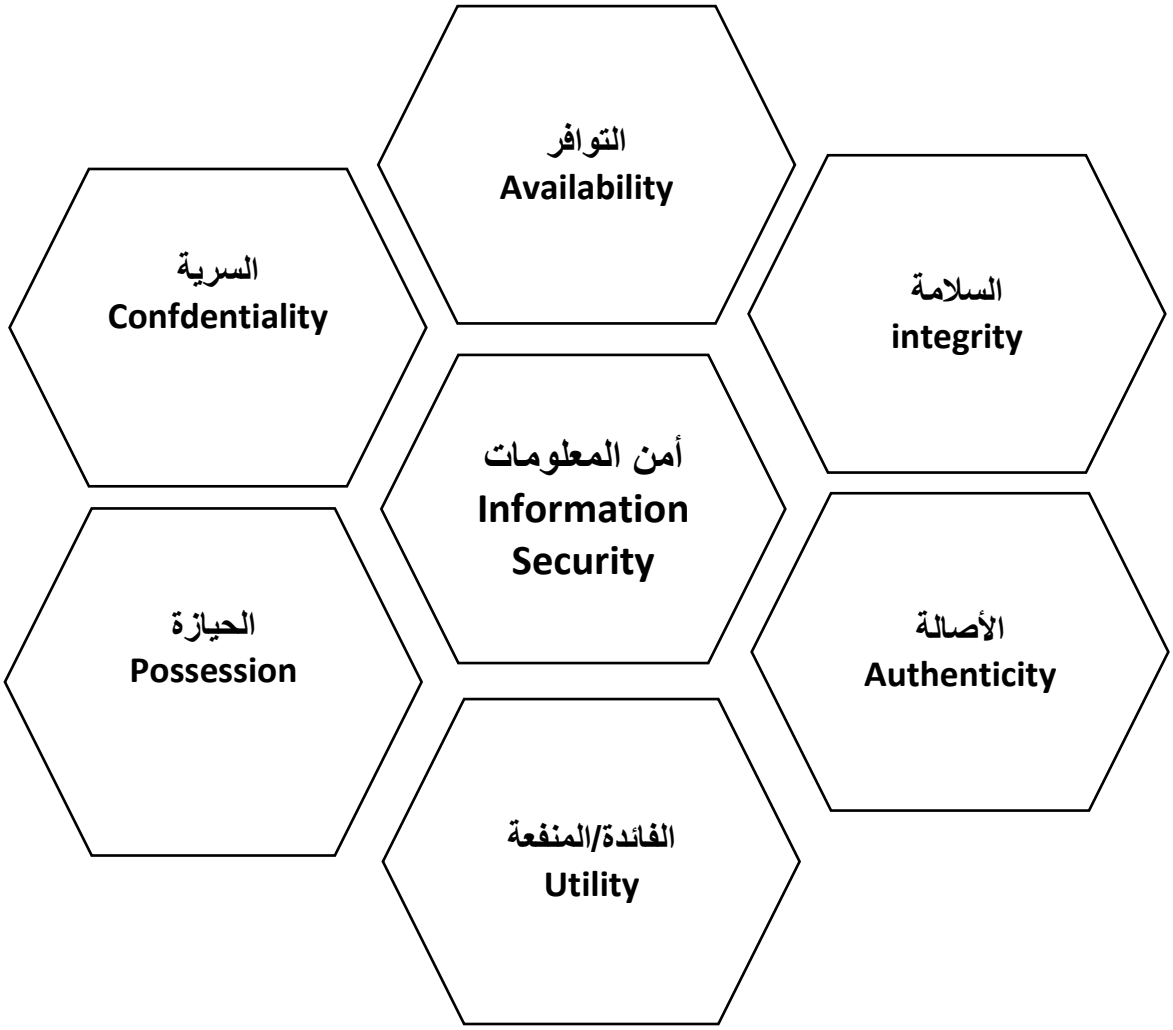
ب.سداسي باركر لأمن المعلومات: وفي سنة 2002 قدم **دون باركر (Donn B.Parker)** وهو باحث ومستشار في امن المعلومات وجهة نظر بديلة حول عناصر أمن المعلومات، فإضافة الى العناصر الثلاثة السابقة التي جاءت في النموذج السابق أضاف باركر ثلاثة عناصر أخرى وهي:

1. **الحيازة (Possession)**: يعتبر عنصر الحيازة أو امتلاك التحكم واحدا من إضافات باركر للنموذج السابق، وتمت اضاقة هذا العنصر انطلاقا من فرضية مفادها أن المعلومات يمكن ان يتحكم فيها فرد أو مجموعة من الافراد لا يمتلكون الحق في ذلك، فانطلاقا من هذا العنصر يمكن إعطاء صلاحيات التحكم في المعلومات للأشخاص المعنين فقط.

2. **الأصالة (Authenticity)**: يقصد بهذا العنصر التحقق من شخصية وهوية الأشخاص أو الجهات التي تطلع على المعلومات، وهل هم مخولون فعلا ولديهم صلاحيات الوصول والاطلاع على هذا النوع من المعلومات.
3. **المنفعة/الفائدة (Utility)**: يساعد هذا العنصر في الإشارة إلى المعلومات ذات الفائدة والقيمة وهذا هو العنصر الأخير من سداسي باركر لأمن المعلومات، ويركز هذا العنصر على مفهوم يتم اغفاله تماما أو الخلط بينه وبين عنصر التوافر وهو فائدة هذه البيانات، فهذه الأخيرة قد تكون متاحة وقابلة للاستخدام ولكن ليس بالضرورة ان تكون في شكل مفيد ذو قيمة.[1]

[1] Umesh Hodeghtta and Umeshaa nayak, **The info sec Handbook an introduction to information security**, Apress open, New york, p 52.

شكل رقم (07) سداسي باركر(Parker) للأمن المعلومات.



Source : Georgie penbey, **the parkerian Hexad**, **cia model expanded**, p7.

المطلب الخامس: إشكاليات وتحديات أمن المعلومات.[1]

مع التزايد المستمر للتعقيد التقني، والمصاعب القانونية وتوقعات حماية الخصوصية ارتفعت تحديات أمن المعلومات بشكل متسارع خلال السنوات الماضية إذ أن الانتشار الكبير لاستعمال التطبيقات القابلة للعمل مع شبكة الانترنت (**Web Enabled**)*في تسعينيات القرن الماضي وتزايد حصة هذا الاستثمار في سوق الأسهم غالبا ما دفع بمرتبة عمليات أمن المعلومات إلى مستوى الأفضلية.

وتشمل التحديات التي تواجهها إدارات تقنيات امن المعلومات ما يلي:

1) عدم الفهم والخلط أحيانا بين العديد من تقنيات أمن المعلومات المختلفة والمتضاربة
2) معرف من يمكن له ومن لا يمكن له الوصول للمعلومات، والأنظمة والشبكات فأحيانا قد لا تبلغ سجلات الموظفين الدقيقة بسرعة إلى إدارة تقنية المعلومات.
3) عدم وجود معايير شاملة ومتفق عليها للأمن المعلوماتي.
4) تحديد مستوى الصلاحيات الصحيح لكل موظف وكل مستخدم للنظام لكي يقومون بإعمالهم من دون السماح للجميع بالنفاد الكامل لجميع الملفات والأنظمة.
5) معرفة من يمكن أن تثق فيهم من الموردين والشركاء والزبائن من أجل التزويد بالمعلومات فليست كل المعلومات سواء فقد تحتوي مرفقات البريد الالكتروني على فيروسات أو رسائل، صور أو نصوص آو حتى تسجيلات صوتية مخفية بتقنية(**Stegnography**) **.
6) جلب مؤهلين وأخصائيين وخبراء في امن المعلومات.
7) المحافظة على مقدرة هندسية للاستجابة السريعة ضد مختلف التهديدات والهجمات من الإفراد الذين يحاولون الوصول إلى معلومات قيمة.

---

[1] لورنس م. اوليفا، ترجمة **محمد مراياتي امن تقنية المعلومات نصائح من خبراء:** المنظمة العربية للترجمة، ب س ن، ص 25-26.

***Web Enabled**: هي عبارة عن مجموعة من تطبيقات الحاسوب والتي تم انشاؤها باستخدام لغة **HTML** ويمكن الوصول اليها انطلاق من متصفحات الانترنت.

****Stegnography**: هو غلم، طريقة أو تقنية لإخفاء البيانات الرقمية داخل وسيط أخر كإخفاء رسالة نصية داخل صورة مثلا بشكل يمكن سوى المرسل والمستلم الاطلاع على المحتوى المخفي وأصل كلمة (**Stegnography**) هو اغريقي مشتق من الكلمة (**Stegosgraphia**) وهي مكونة من كلمتين **stegos** وتعني الصفف أو الغطاء و **Graphia** وتعني الكتابة أول تسجيل لاستخدام هذا المصطلح كان سنة 1499 من قبل **يوهانس تريثيموس** (**Johannes Trithemius**).

8) ضف إلى ذلك التحديات القانونية والتشريعية خاصة في دول العالم الثالث فأغلبية هذه الدول تفتقر لإطار القانوني والتشريعي لردع مرتكبي الجرائم المعلوماتية.

خاتمة الفصل:

لم يعد أمن المعلومات اليوم مجرد مهمة مؤقتة بالنسبة إلى المؤسسات سوءا كانت حكومية أو خاصة، بل أصبح عملية مستمرة في كل دقيقة وثانية، ومع التزايد الكبير في الجرائم المعلوماتية بمختلف أنواعها وأشكالها وأساليبها، أصبحت المؤسسات تولي اهتماما بالغا بهذا المجال إيقانا منها بان إبقاء معلوماتها الحساسة سوءا المالية وغيرها، وكذلك معلومات وبيانات زبائنها في سرية تامة من شانه ان يوثق الصلة بينها وبين متعامليها وكذلك يكسبها الميزة التنافسية في محيط عملها.

الفصل الثاني:

مهددات أمن المعلومات وأساليب حمايته.

تتعدد الطرق والتقنيات التي يتم من خلالها انتهاك البنية التحتية لنظم المعلومات والتعدي عليها الا ان هذه الطرق والتقنيات في تغير وتطور مستر، فاذا تحدثنا عن مهددات الامن المعلوماتي في سنة 2010 مثلا فهي مختلفة تماما على ماهي علية في يومنا الحالي.

وفي ظل كل هذه التهديدات والمخاطر تسعى الكثير من المؤسسات لإيجاد السبل والوسائل الوقائية الإجرائية التي تمكنها من مواجهة التهديدات الأمنية لكي تتمكن من القيام بوظائف أمن المعلومات، ويتزايد الاهتمام بحماية نظم المعلومات سعياً لتقليل التكاليف ولضمان استمرارية العمل وجودة المعلومات المقدمة وهو ما من شأنه تعزيز استقرار المؤسسات للقيام بدورها في تقديم الخدمات والتي أصبحّ جلها يقدم بصورة آلية.

سنقدم في هذا الفصل المهددات المنشرة في السنوات الأخيرة وكان هذا استنادا على مجموعة من التقارير الحديثة المختصة في أمن المعلومات والامن السبيراني بصفة عامة وبالتالي قسمت هذا الفصل الى مبحثين كالاتي:

المبحث الأول: مهددات امن المعلومات واساليبها التقنية

المبحث الثاني: الأساليب والتقنيات الحديثة للحفاظ على أمن المعلومات

المبحث الاول: مهددات أمن المعلومات وأساليبها التقنية

مع الاعتماد المتزايد، في حياتنا اليومية، على الانظمة المعلوماتية، والاجهزة المتصلة بالشبكة العالمية للمعلومات وتشعب طبيعة هذه الاجهزة، من هواتف خليوية، واجهزة حوسبة شخصية، يزداد عدد المتصلين بالفضاء السيبراني، وتزداد احتمالات الاعتداءات والجريمة. فقد أشار تقرير صادر عن **ماكينزي** (**Mckinsey**)، الى توقع زيادة المعلومات الرقمية، بمعدل 44%، خلال الاعوام الممتدة من 2009 إلى 2020. كما تشير العديد من التقارير، الى توالي حوادث إختراق الانظمة وسرقة البيانات وتسربها.

المطلب الاول: المهددات من حيث مصدر وقوعها

إن المعلومات والأنظمة التي تحتفظ بهذه المعلومات تكون عرضة للهجوم من جهتين مختلفتين، من الداخل ومن الخارج ويجمع اغلب المهتمين بهذا المجال أن الهجمات من الداخل تشكل خطرا كبيرا على المؤسسة مقارنة بالهجمات الخارجية.

1. **المهاجمون من الداخل:** يقصد بالمهاجمين من الداخل، أولئك الإفراد الذين ينتمون إلى الجهة المستهدفة، غير أنهم يقومون بإعمال تصادم جهود الجهة الرامية إلى حماية أنظمة المعلومات والمهاجمون من الداخل لا يزالون دوما الخطر الذي تواجهه أي جهة سوءا كانت هذه الجهة منظمة شركة أو حتى دولة.

1.1. **دوافع الهجوم من الداخل:** هناك أسباب عديدة قد تدفع الفرد لشن هجوم ضد أنظمة معلومات الجهة التي يعمل بها، ومن أهم هذه الأسباب ما يلي:

- **عدم الرضا:** أيا كانت مسببات عدم الرضا هذا إلى أن الواقع شهد أن التقنية الحديثة جعلت من مهاجمة لنظم المعلومات امرأ يشعره بالانتقام وبعث البهجة في نفس الشخص الذي نفد الهجوم.
- **إثبات الشخص لمهاراته وقدراته على تنفيذ هجوم الكتروني:** هناك طائفة عريضة من الناس يداخلهم الشعور بالفخر إذا تمكنوا من اختراق مواقع على شبكة الانترنت آو وصل والى قواعد بيانات محمية، إذ يجدون في ذلك امرأ يباهون به اقرأنهم، والحقيقة أن كثيرا من هؤلاء قد لا يملكون المعرفة لشن هجمات الكترونية على المعلومات.[1]

[1] خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني، **أمن المعلومات بلغة ميسرة**، ط1، الرياض: مركز التميز لأمن المعلومات، 2009، ص27-28

- **تحقيق المكاسب المالية:** قد يهاجم شخص ما أنظمة الجهة التي يعمل بها لسرقة معلومات سرية يستخدمها لاحقا لابتزاز الجهة لدفع غرامة مالية.

2.1. **حجم التهديد الداخلي:** أن الهجوم من الداخل يمكن أن يخل باي عنصر من عناصر امن المعلومات التي تناولنها مسبقا، أي انه يمكن أن يلحق الضرر بسرية المعلومات وسلامتها، أو يعيق الوصول إليها.

والمهاجم من الداخل إذا كان ماهرا في التعامل مع هذه التقنيات والأجهزة يستطيع طمس أي اثأر تدل على ارتكابه للهجوم، واهم جوانب الإخطار التي تأتي من الهجوم الداخلي ما يلي:

- مهاجمة الشبكة الداخلية للمنشاة التي يعمل بها.
- مهاجمة المعلومات إما بالتغيير، السرقة آو الحذف.
- فتح ثغرات في أنظمة الحماية التي وضعتها المؤسسة لتحصين نظم معلوماتها.

إصافة إلى ذلك فان المهاجمون من الداخل يتمتعون بميزة لا يتمتع بها المهاجم من الخارج، وهي أنه ليس عرضة للكثير من الاحترازات الأمنية التي يتعرض لها المهاجم من الخارج.[1]

2. **المهاجمون من الخارج:** يمكن ان تنشا التهديدات الخارجية من الإفراد العاملين خارج المؤسسة، هؤلاء الإفراد ليس لديهم حق الوصول المصرح لأنظمة المعلومات أو الشبكات، ومن بين التهديدات الخارجية نجد الإفراد الذين لا ينتمون إلى المؤسسة المستهدفة كالمخترقين مثلا.[2]

[1] **المرجع نفسه**، ص29.

[2] Mouna jouini et fatima ben arefa, "Classification of security threats in information systems", **procedia computer science**, Vol 32, p 494.

المطلب الثاني: مهددات البنية التحتية

أ. **القرصنة او الاختراق (Hacking)**: يشير هذا المصطلح الى استخدام وسائل الاتصال وتكنولوجيا المعلومات الحديثة في ممارسات غير مشروعة، بهدف التحايل على أنظمة المعالجة الالية للبيانات، أو الكشف عن البيانات الحساسة او تغييرها او التأثير على سلامتها او حتى اتلافها. وبعبارة أخرى فان لقرصنة ماهي الى عملية دخول غير مصرح به الى أجهزة الغير وشبكاته الالكترونية.

أي أن توجه هجمات إلى معلومات الكمبيوتر او خدماته بقصد المساس بسرية وسلامة المحتوى وتكامليته أو تعطيل قدرة وكفاءة الأنظمة المعلوماتية للقيام بأعمالها.[1]

ويقوم بعمليات القرصنة اشخاص هواة او محترفون تم تعريفهم كالاتي: "اشخاص لهم القدرة على التعامل مع أنظمة الحاسب الالي والشبكات بحيث تكون لهم القدرة على تخطي أي إجراءات أو أنظمة حماية، وهؤلاء المخترقون يمكن تصنيفهم كالاتي:

- **الهاكرز (Hackers)**: هم الأشخاص الذين لديهم القدرة الفائقة على اختراق الأنظمة والشبكات الا انهم لا يقومون باي إجراءات من شانها ان تؤدي الى احداث اضرار بنظم المعلومات والحاسبات الالية وغيرها.
- **الكراكرز (Crackers)**: يطلق عليهم كذلك اسم المخربون، وهم يتشابهون مع الهاكرز في قدرتهم الفائقة على الاختراق وتحطي إجراءات وبرامج الحماية الا انهم يقومون بالعبث بالبيانات والمعلومات المخزنة في نظم المعلومات أو الحاسبات والشبكات.

وتعود بدايات القرصنة الى الستينات وارتبط ظهورها مع ظهور أولى الحواسيب الا ان أولى عمليات القرصنة سجلت في عام 1878 بإحدى شركات الهاتف المحلية الامريكية، ويعتبر الخبراء الفترة ما بين 1980 و1989 العصر الذهبي للقرصنة، وتجدر الإشارة الى أشهر حروب النت على الاطلاق هي حرب الهاكرز العظمى التي كانت بين عامي 1990 و1994 بين فريقين من الهاكرز حيث سعى كل فريق لاختراق حاسوب الاخر.

[1] ليتيم فتيحة وليتيم نادية، "الامن المعلوماتي للحكزمة الالكترونية وإرهاب القرصنة"، **مجلة الفكر**، ع 12 ص 242.

ولعل واحد من أشهر القراصنة على الاطلاق هو الأمريكي **كيفين مثنك** (**Kevin Mitnick**) وكذلك هاكر أطلق على نفسه (**The Mentor**) والذي قام بنشر دراسة شهيرة بعد اعتقاله، والتي أصبحت تعرف ببيان الهاكرز وهو بيان رسمي لأهداف ووجهات نظر القرصان وقد نشر هذا البيان في المجلة الالكترونية (**Phrack**) ولايزال هذا البيان واحدا من أشهر ما كتب حول الهاكرز.

- **كيفية خرق الامن المعلوماتي عن ظريف القرصنة:** لمحاولة خرق الأمن المعلوماتي يتم استخدام برنامج خاص بالقرصنة، يستعمل هذا الأخير نوعين من الملفات الأول يسمى (**Client.exe**) والثاني (**Server.exe**) يعمل الملف الأول على فتح الثغرة في الحاسب المستهدف ليتمكن الملف الثاني من الدخول الى الحاسب انطلاقا من هذه الثغرة.[1]

ووفقا لتقرير (**Data Breach Investigations Report**) لسنة 2017 يعتبر الاختراق واحدا من أكثر التقنيات المستعملة لخرق وكسر حماية أنظمة المعلومات والحاسبات والشبكات.[2]

ب. : التزوير (Fabrication):

ويسمى هذا الانتهاك إقتحام المعلومات وتعديلها (**Data Injection and Modification**) حيث يقوم مهاجم نظام المعلومات عبر الشبكة بتغيير، أو تعديل البيانات ومن ثم إعادة إرسالها وهو بذلك قد يلجأ لاستخدام أساليب أخرى كالتنصت أو الاقتحام. ولحل هذه الإشكالية يلجأ خبراء أمن المعلومات إلى المجموع الاختباري (**Checksum**) وهو عبارة عن رقم يتم احتسابه بناء على مجموعة من البيانات، ويستخدم للتأكد من سلامة البيانات المنقولة، بحيث يقوم الطرف المرسل باحتسابه قبل إرسال البيانات، ويقوم الطرف المستقبل بالشيء نفسه والغرض من ذلك اكتشاف أي تغيير متعمد للبيانات قد قام به الشخص المهاجم.[3]

[1] **نفس المرجع**، ص 243.

[2] Verizon, **Data breach investigations report**, 10th Ed, 2017, p 4.

[3] داوود حسن طاهر، **أمن شبكات المعلومات**، ط1، الرياض: معهد الإدارة العامة، 2004، ص 138.

ج. الفيروسات والبرمجيات الضارة:

- **الفيروسات:**

الفيروسات: "عبارة عن برامج أو مجموعة من التعليمات التي تلحق ضرارا بنظم المعلومات والحواسب ولها القدرة على التخفي الانتشار والتوسع."

وتكمن خطورة الإصابة بالفيروس في أنه يؤدي الى تعطيل عمل البرامج وتقليل من كفاءة وسرعة الأجهزة، وقد يؤدي إلى مسح منطقة جدول التقسيم، وهو ذلك الفهرس الذي يحتوي على أسماء الملفات وأماكن وجودها في القرص الصلب.[1]

ان ظاهرة الفيروسات ليست وليدة العصر الحالي، بل تعود الى أواخر الاربعينيات من القرن الماضي وقد ورد ذكرها لأول مرة في مقال نشره **جون فون نيومان** (**John Von Neumann**) سنة 1949 وظهرت بعض أعراض الفيروسات في أوائل الخمسينيات الا ان انتشارها كان محدودا، وكان أول انتشار للفيروسات في الأجهزة الشبكية سنة 1983 حيث ظهرت مع نظام التشغيل (**UNIX**) وقد اثار هذا ضجة كبيرة في العالم ولم تسلم كبرى الشركات من هذه الفيروسات ووصلت خسارة الشركات لما يقل عن 100 مليون دولار.[2]

ويتكون الفيروس عادة من أربعة أجزاء رئيسية هي:[3]

- **الية التكرار**: وهو الجزء الذي يمكن الفيروس من نسخ نفسه.
- **الية التخفي**: وهو الجزء الذي يجعل الفيروس قادرا على الاختفاء، ويمكن أن يتضمن تشفيرا لمنع برامج مضادات الفيروسات من اكتشافه.
- **الية التنشيط**: وهو الجزء الذي يسمح للفيروس بالانتشار.
- **الية التنقيد**: وهو الجزء الذي ينفد الفيروس بعد تنشيطه، ويكون عبارة عن مجرد رسالة على الشاشة أو مسح للملفات.

---

[1] نادية أمين محمد علي، ورقة في الفيروسات وطرق الوقاية منها كأمن البيانات، **المؤتمر الدولي لأمن المعلومات الالكترونية معا نحو تعامل رقمي أمن**، سلطنة عمان، 2005، ص 200.

[2] مقال بعنوان، فيروسات الحاسوب من أطلق الشرارة الأولى؟، متوفر على الرابط: https://www.syr-res.com/article/7928.html اطلع عليه بتاريخ 2018/05/22 على الساعة 23:38 بتصرف.

[3] ليتيم فتيحة وليتيم نادية، **مرجع سابق**، ص 245.

- **البرمجيات الضارة (Malware):**

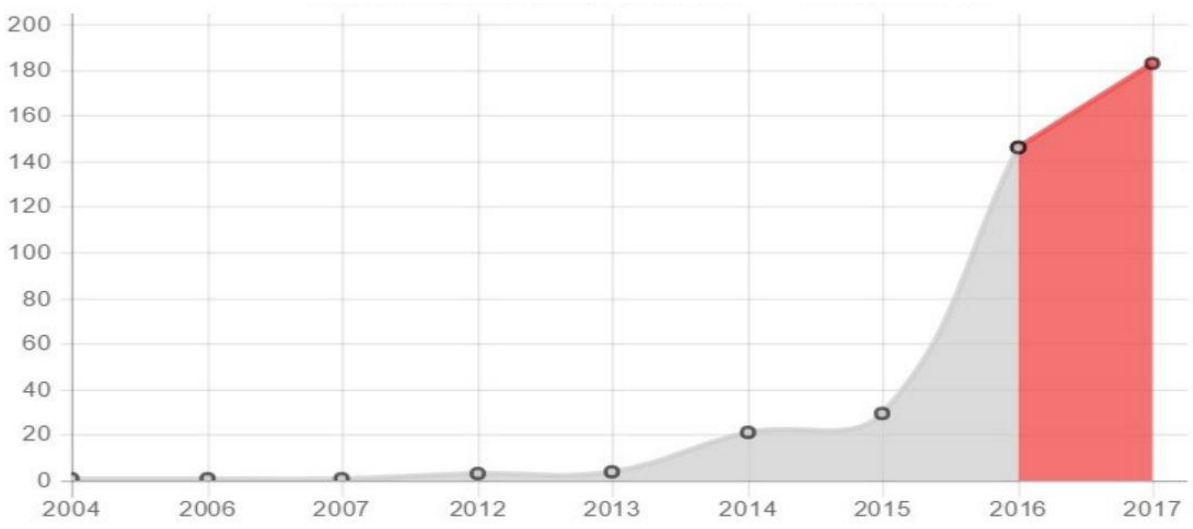
هي اختصار ل (**Malicious Software**) وتعني برمجية خبيثة وهي عبارة عن برامج تهدف لألحاق الضرر بالحاسوب، ونظم المعلومات وتعطيلها وجمع المعلومات والتجسس عليها.

تجدر الإشارة أن هناك العديد من البرمجيات الخبيثة ولكن بعد اطلاعي على أحدث التقارير الصادرة من منظمات عالمية مختصة في هذا المجال، سنطرق الى واحد ن أخطر البرمجيات الخبيثة انتشارا في السنوات الأخيرة ويجمع الخبراء أن معظم الهجمات الأخيرة تمت عن طريقه وهو (**Ransomware**).

برمجية (Ransomware):

هو نوع من أنواع البرمجيات الخبيثة والذي يمنع الشركة أو الشخص المستهدف من الوصول إلى اصوله، ثم يقوم بتشفيرها، وينبه المستخدم بإصابته بهذه البرمجية ويصاحب هذا التنبيه طلب دفع فدية وموعد محدد لدفعها لاسترجاع التحكم والوصول الى بياناته ومعلوماته، إذا لم يتم الدفع في المدة المحددة فانه يتم تدمير المعلومات والبيانات لتصبح عديمة الفائدة، وأما إذا تمت عملية الدفع فان الضحية سيحصل على ملف لفك تشفير معلوماته ولكن هذا الامر لا يحدث دائما.

شكل رقم (8) يوضح تطور انتشار واستعمال برمجية (Ransomware) ما بين 2004-2017



Source : Calyplix Security, **top security threats what's ahead and how to prepare**, 2017 report, p 3.

- **أسباب التوسع في استخدام (Ransomware):**

- **سهولة الوصول:** قبل سنوات كان الخبراء فقط من يستطيعون شن هجوم لتشفير معلومات الضحية لكن اليوم أصبح بمقدرة الأشخاص العاديين فعل ذلك، باستخدام برمجية (**Ransomware**).
- **المال السريع:** اكتشف اللصوص نوعا جديدا من التقنيات لكسب المال، فحتى إذا كانوا ذوي خبرة متواضعة في المجال التقني، يمكن لمستخدمي هذه البرمجية جني الالاف من الدولارات عن طريق نشرها في حواسيب الغير.[1]

د. **الهندسة الاجتماعية (Social Engineering):**

ليس هناك تعريف شامل لهذا المصطلح لكن أقرب التعريفات تقول بانها: "استخدام المهاجم لحيل نفسية كي يخدع بها مستخدمي الحاسب ليتمكن من الوصول الى معلومات معينة."

يعرف **كيفين مثنك (Kevin Mitnick)** الهندسة الاجتماعية على أنها: "استخدام النفود والاقناع لخداع الناس ومن تم الكشف عن معلوماتهم."

سئل أحد المهتمين بهذا لمجال: ماهي الهندسة الاجتماعية؟

فأجاب هي: "ان تكذب على الناس للحصول على معلوماتهم."[2]

تعتبر الهندسة الاجتماعية واحدة من أنجح الطرق التقنية التي يستخدمها المهاجم وذلك لسهولتها مقارنة مع الوسائل الأخرى، لأنها تهاجم العنصر البشري الذي يعتبر أضعف نقطة في منظومة حماية المعلومات.

- **جوانب الهجمات باستخدام أسلوب الهندسة الاجتماعية:**

يرى بعض الباحثين ان الهجمات باستخدام أسلوب الهندسة الاجتماعية يمكن ان ينشئ من عدة اصعدة نذكرها كالاتي: [3]

[1] **Ibid**, p 3.

[2] Christopher Hadnagy, **Social Engineering the art of human hacking**, Wiley publishing Inc, Usa, 20111, p 31.

[3] خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني، **مرجع سابق**، ص 33-34.

1) **مكان العمل:** يدخل المهاجم مكان العمل متظاهرا بانه أحد، الموظفين او المتعاقدين مع جهة العمل، أو انه منم عمال النظافة او الصيانة وإذا تمكن المهاجم من الدخول فانه يطوف ليجمع ما يمكن جمعه من كلمات المرور التي قد تكون ملصقة على شاشة الحواسيب أو لوحة المفاتيح.
2) **الهاتف:** يستخدم بعض المهاجمين الهاتف لشن هجوم باستخدام أسلوب الهندسة الاجتماعية، وأكثر الأشخاص تعرضا لهذا الهجوم هم العاملون في مراكز تقديم الدعم الفني

(**Help Desk Or Help Line**) فالمهاجم مثلا قد يتصل بمركز تقديم الدعم الفني هاتفيا ويطلب منهم بعض المعلومات الفنية، وتدريجيا يحصل على ما يريد من معلومات ككلمات المرور وغيرها ثم يستخدمها في شن الهجوم على حواسيب المؤسسة.

3) **سلة المهملات:** قد يستغرب البعض إذا علم أن هذه الطريقة من أكثر الطرق شعبية في مجال الهندسة الاجتماعية، والسر من وراء شعبيتها هو أن المهاجم يستطيع جمع العديد من المعلومات المهمة دون أن يلفت انتباه أحد، ومن بين المعلومات التي قد يجدها في سلة المهملات كلمات المرور، الهيكل التنظيمي، دليل هواتف الشركة، وغيرها من المعلومات المهمة.

هـ. **الاصطياد الالكتروني (Phishing):**

يعتبر واحدا من أهم وأكثر التقنيات شيوعا الغاية منه سرقة معلومات شخصية، عن طريق ارسال المهاجم لبريد الكتروني الى شخص معين يزعم من خلاله انه من أحد البنوك او المؤسسات او الإدارات التي يتعامل معها الضحية، ويكون محتوى الرسالة على انه هناك مشكل في حسابه البنكي او يدعوه لتحديث بياناته ويكون هذا البريد مرفق برابط الكتروني مزيف يشابه عنوان موقع المؤسسة وبعد الضغط على الرابط تنبثق نافذة لإدخال بياناته الشخصية سوآءا اسم المستخدم أو كلمة المرور وبهذا قد يكون أعطى بياناته للمهاجم. يدرك العديد من المستخدمين اليوم هذا النوع من سرقة المعلومات ويتجنبون قدر الإمكان النقر على روابط مزيفة ولكن ليس الجميع حذرا ولا يزال ها النوع من الهجوم فعالا الى يومنا هذا.[1]

[1] Chuck Erstton, **computer security Fundaentals**, 3rd Ed, Deason publishing Inc, Usa, 2016, p 65.

و. عرقلة الخدمة (Denial Of service):

واحد من أكثر أشكال الهجوم وأكثره شيوعا على النظام. لا يحاول هذا الهجوم التطفل على نظامك أو الحصول على معلومات حساسة. انما يهدف ببساطة لمنع المستخدمين الشرعيين من الوصول الى النظام.[1]

ويتم ذلك عن طريق إغراق النظام أو الشبكة بالرسائل أو طلبات المعلومات بحيث يقضي النظام أو الشبكة كل الوقت في محاولة الاستجابة لهذه الرسائل والطلبات لكن دون جدوى وكثيراً ما يحدث تعاون بين مجموعة من المهاجمين حيث يقومون في توقيت معين بمهاجمة خدمة معينة عن طريق إغراق نظم المعلومات بطلبات مشروعة ومصرح بها ولكنها أكبر من الحجم المسموح.[2]

[1] **Ibid**, p 87

[2] داوود حسن طاهر، **مرجع سابق** ص 148.

المطلب الثالث: المهددات الصادرة عن المورد البشري.

يعتمد أمن المعلومات أولاً وأخيرً على أمانة الأفراد المتعاملين معه فلا يكفي التأكد من أخلاقيات الموظف وأهليته عند تعيينه بل يجب إن تستمر مراقبته طيلة فترة عمله لأن التغيير في السلوك متوقع في أي وقت كذلك يجب عدم الاعتماد على موظف واحد بأي حال من الأحوال وان كان لابد من ذلك فيجب أن يشمل ذلك الموظف إشرافا ومراقبة دقيقة وتوثيقا دقيقا لأعماله وأن يكون هنا كتدريب لمساعدين لهم، وعند انتهاء خدمات أي موظف يجب سحب صلاحيته قبل فترة كافية فهناك عدة حوادث انتقام من موظفين أنهيت خدماتهم.

وتشمل التهديدات التي تصدر من الأفراد المتعاملين مع نظم المعلومات ما يلي:[1]

1) التصرفات الخاطئة من قبل المتعاملين:

يضم هذا النوع الأفعال والتصرفات غير المتعمدة والتي يتم أداؤها بواسطة أفراد موثوق بهم داخل المنظمة ومرخص لهم التعامل مع أنظمة المعلومات حيث تؤدى أفعالهم إلى حدوث أخطاء ومشكلات عند تعاملهم مع هذه الأنظمة، ويعود ذلك إلى عدة عوامل منها قلة الخبرة والتدريب الكافي للعمل في النظام ومن هذه الأفعال:

- عرض معلومات حساسة.
- إدخال بيانات خاطئة.
- حذف البيانات أو تعديلها عن طريق الخطأ.

2) الأفعال المتعمدة (المدروسة):

تضم هذه المجموعة المهددات التي تهدف بصورة رئيسية إلى إلحاق الضرر بالمنشأة وأنظمة معلوماتها ومواردها. وتضم الأنواع التالية:

[1] أيمن محمد فارس الدنف، واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، **مذكرة ماجستير**، جامعة غزة الإسلامية: كلية التجارة، قسم إدارة الاعمال، 2013، ص 68.

3) أفعال التعدي المقصودة:

يمثل هذا النوع فئة واسعة من الأنشطة البشرية والالكترونية التي يمكن أن تؤثر سلباً على السرية وخصوصية المعلومات، عندما يصل أو يطلع أحد الأفراد غير المرخص لهم على معلومات تعمل المنظمة على حمايتها، يعتبر مثل هذا التصرف تعدى مقصود ويعتبر مرتكبيه مثالا لمجرمي هذه التصرفات المتعدية المقصودة.

4) أفعال الابتزاز المقصودة:

يمثل هذا النوع من الأفعال المتعمدة مهدداً للسرية عن طريق استخدام المعلومات كوسيلة للضغط على المنشأة أو ابتزازها من أجل تحقيق غرض معين خاص بالجاني. مثلا: أن يقوم شخص بالحصول على معلومات حساسة جدا عن المنظمة، ثم يهدد بإفشاء هذه المعلومات إذا لم يدفع له مبلغ معين.

5) أفعال التخريب المقصودة:

ينشأ هذا النوع من المهددات من وجود فرد أو عدة أفراد يريدون تخريب أو تدمير نظام حاسوب أو أداء عدد من الأفعال الضارة بأصول المنشأة المعلوماتية وسمعتها. مثل تعريض موقع الويب للتخريب أو إلحاق الضرر به ومثل ذلك الفعل يؤدي إلى التأثير على صورة المنشأة وفقدان الكثير من أرباحها وعملائها نتيجة لفقدان الثقة فيها من قبل الزبائن.

6) أفعال السرقة المقصودة:

يمثل هذا النوع من الأفعال تهديدا للمنظمة، حيث تتعرض مكونات نظم المعلومات للسرقة، وربما يكون ما يتعرض للسرقة مكون مادي مثل تغيير في ذاكرة الحاسوب أو المعالج وقد يكون ملك الكتروني مثل برامج أو بيانات، ويمكن التحكم في السرقة المادية بسهولة مثل أحكام إغلاق الأبواب واستخدام أجهزة التنبيه ولكن يصعب التحكم في السرقة الالكترونية.[1]

[1] **نفس المرجع**، ص 69.

المبحث الثاني: الأساليب والتقنيات الحديثة للحفاظ على أمن المعلومات

يدرك العديد من المهتمين والمختصين في مجال أمن المعلومات العديد من المشاكل المرتبطة بأمن المعلومات ولكن اختلفوا حول أفضل الطرق لحل هذه المشاكل فمنهم من يرى أن حل هذه المشاكل يتطلب تطوير الإجراءات الإدارية داخل المنظمة، فيما يرى البعض الأخر ان الحد من هذه المشاكل يتعلق بالأمور الفنية والتقنية، ويركز أخرون على أن أمن وسلامة المعلومات يجب أن يبدا من أمن المنظمة نفسها، ثم أمن البرامج والأنظمة وصولا الى أمن الأفراد.

سنطرق في هذا المجث الى جملة من الأساليب والتقنيات لتامين المعلومات، وقد قسمت هذه الأساليب على النحو التالي:

المطلب الأول: أساليب الحماية المادية

الأمن المادي أو الامن الفيزيائي ويشمل أمن المباني، وأجهزة الحاسوب، والمعدات الأخرى، وأجهزة الاتصالات، والتكييف والطاقة ويتحقق هذا الأخير من خلال:[1]

1. السيطرة على المداخل:

يجب العناية بالحماية المادية لمراكز المعلومات من حلال احكام السيطرة والرقابة على مداخلها للوصول الى القدر المطلوب من أمن المعلومات، حيث تصمم إجراءات الامن المادية لمواجهة الاخطار الناتجة عن الأشخاص ذوي النوايا السيئة أو الذين لديهم تصاريح الدخول للمنشاة، بالإضافة الى المتسللين من خارج المنشاة لذا يجب اتخاذ اجراءات شاملة ضد الأخطاء من خلال تحديد حركة الدخول والخروج ليلا ونهارا.

2. نظام الدائرة التلفزيونية الغلقة (CCTV):

هي مجموعة من كاميرات التصوير التليفزيونية التي يمكن التحكم فيها، وتراقب هذه الكاميرات مداخل المنظمة ومداخل غرف النظام، وهي متصلة بأجهزة انذار وعند حدوث أي خطر تتم عملية التنبيه. [2]

[1] غبد الرحمان شعبان عطيات، **أمن الوثائق والمعلومات**، ط1، الرياض: جامعة نايف للعلوم الأمنية، 2003 ص 123.

[2] الحميد محمد دباس ونينو، **حماية أنظمة المعلومات**، عمان: دار حامد للنشر والتوزيع، 2007، ص45.

المطلب الثاني: أساليب الحماية البرمجية والتقنية.

أولا: التشفير(Cryptoptography)

تتراكم التهديدات والمخاوف من جرائم محدقة بنظم المعلومات مما أستدعى الحاجة إلى خصوصية المعلومات وحماية البيانات السرية ويمكن للتشفير أن يعطي درجة عالية من الأمن بأقل كلفة، وتتوالى عمليات تطوير تقنيات جديدة في مجال التشفير بحيث تعطي مستويات أعلى من الأمن عند تطبيقها على نظام المعلومات، وفي ظل التطور المتسارع للحاسوب وشبكات الاتصال باتت الحاجة ملحة لطرق تشفير قوية، ومن مبررات ذلك لأن زيادة سرعة الكمبيوتر تعني تقصير الوقت الذي يحتاجه الكمبيوتر لكسر أو كشف مفتاح تشفير معين. [1]

ويمكن تعريف التشفير ببساطة على أنه: " علم الكتابة السرية."

والتشفير أو ما سماه العرب قديماً علم التعمية ليس جديداً بل أستخدمه المصريون القدماء منذ آلاف السنوات، ويعرف كذلك بأنه: "العلم الذي يحول المعلومة الواضحة إلى معلومة سرية غير قابلة للفهم"، ونذكر هنا ضرورة التشفير حال الاتصال عبر وسائط غير موثوقة، وخصوصاً في حالة التراسل من خلال الانترنت. وتتم عملية التشفير بنقل معلومة من طرف لآخر عبر قناة وسيط، إذن هنالك ثلاث أجزاء هامة لفهم عملية التشفير.

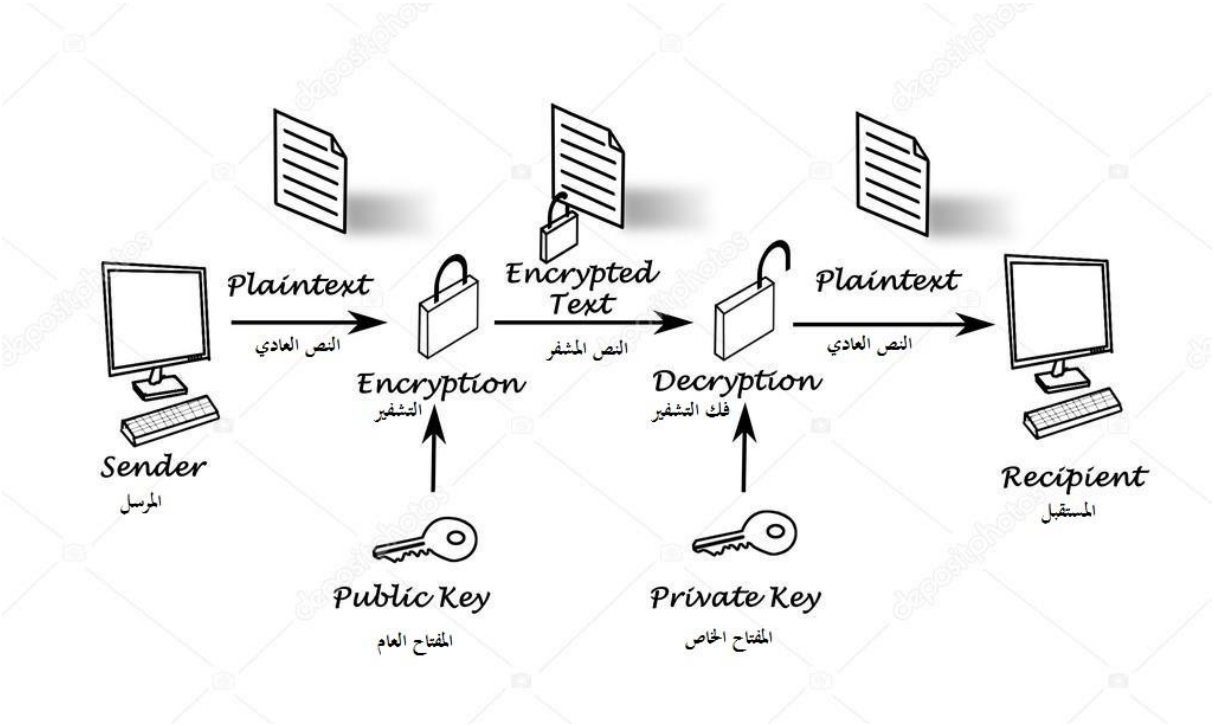
وتعتمد تكنولوجيا التشفير الحديثة على النظرية التالية: تمتلك كل جهة أو فرد مفتاحين، واحد لتشفير البيانات والاخر لفك تشفيرها، المفتاح الأول هو المفتاح الخاص ويكون فقط بحوزة الجهة المخولة المؤسسة او إدارة حكومية مثلا والمفتاح الثاني هو المفتاح العام، ويتم نشره على الشبكة الداخلية للمؤسسة من أجل استخدامه من طرف الجهة الأخرى الافراد لتشفير المعلومات والبيانات المراد ايصالها الى المؤسسة، ويوضح الشكل في الأسفل طريقة عمل التشفير. [2]

[1] Dorothy Elizabeth, **Cryptography and data security**, Addison-Wesley Publishing Company, Inc, 1982, p 1.

[2] عبد الفتاح بيومي حجازي، **التجارة الالكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والانترنت**، الإسكندرية: دار الفكر الجامعي، 2006، ص 259.

ويوضح الشكل في الأسفل طريقة عمل التشفير

شكل رقم (9) يوضح طريقة عمل التشفير



Source : Laurent Bloch et Christophe Wolfhugel, **Sécurité Informatique principes et méthode de l'usage des DSI RSSI et administrateurs**, 2éme Ed,eyrolles, p 84.

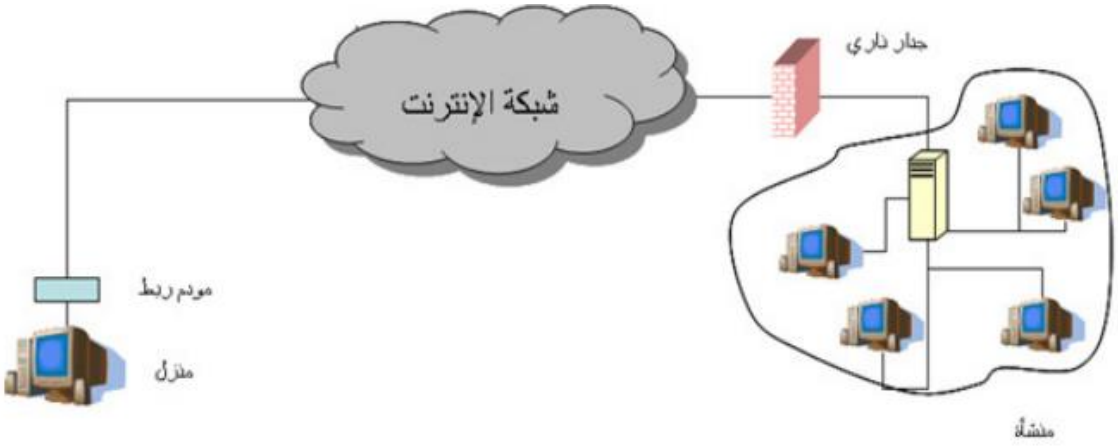
ثانيا: جدران الحماية او الجدران النارية (Firewalls): [1]

هو أداة تصفي أو تحجز مرور البيانات بين الشبكة الداخلية المحمية والشبكة الخارجية التي نخشى منها، والهدف منه هو حجز المستخدم في حيز سياسة أمنية معينة، وهذه السياسة قد تكون مثلاً منع أي دخول من الخارج مع السماح بالمرور من الداخل إلى الخارج. أو قد تكون هذه السياسة السماح بالدخول من أماكن معينة فقط أو من جانب مستفيدين معينين أو تسمح بدخول لأنشطة معينة دون باقي الأنشطة، ويستطيع المستخدم من خلال الجدار الناري الخروج إلى عالم الانترنت ولكن لا يستطيع من في الخارج الدخول إلى الجهاز من خلاله.

[1] يحياوي محمد، "مخاطر القرصنة المعلوماتية على الحكومة الالكترونية"، **مجلة البحوث والدراسات العلمية**، العدد 05، 2011، الجزائر، ص 280.

ولتقريب المعنى للأدهان فان فكرة جدار الحماية تشبه فكرة نقطة التفتيش التي تسمح بمرور أناس وتمنع مرور أخرين وهذا بناءا على تعليمات مسبقة[1]

شكل رقم (10) يوضح عمل جدار الحماية (Firewalls)



المصدر: خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني، مرجع سابق، ص 84.

ثالثا: برامج مكافحة الفيروسات:

برمجيات مكافحة الفيروسات البرنامج المضاد للفيروسات هو برنامج يستخدم لمنع واكتشاف فيروسات الحاسوب، والديدان، وأحصنة طروادة، وبرامج التجسس، وغيرها من أشكال البرمجيات الخبيثة لكن ومهما كانت برامج مكافحة الفيروسات مفيدة، فأنه في بعض الأحيان يمكن أن تكون لها عيوب، فيمكن لبرامج مكافحة الفيروسات أن تقلل أداء الحاسوب إذا لم تكن مصممة بكفاءة وقد يواجه المستخدمين غير الخبراء مشكلة في فهم الأوامر والقرارات التي يقدمها برامج الحماية من الفيروسات وقد يؤدي القرار غير الصحيح إلى الإخلال بالأمن.[2]

رابعا: أدوات منع وكشف الاختراقات:

تضاف أدوات صد أو منع الاختراقات إلى مستويات الحماية التي يجب توفيرها للنظم، وتعتبر هذه الإضافات بمثابة حماية مبكرة للنظام ولكن فيما لو تمكن مهاجم أو برنامج محدد من إحداث خلل بالنظام فإن أدوات أخرى

[1] **نفس المرجع**، ص 83.

[2] مقال بعنوان، **مضاد الفيروسات**، متوفر على الرابط https://ar.wikipedia.org/wiki/ مضاد_فيروسات_(برمجة) اطلع عليه بتاريخ 2018/03/28 على الساعة 10:30.

يجب استخدامها تسمى أدوات الكشف عن الاختراقات ويجب ان يتم فحص هذه الوسائل من فترة لفترة حتى يتمكن النظام من العمل بفعالية، كما أنها تفيد مسئولي النظم في توظيف التقارير التي تنتجها النظم آلياً في وضع احصائيات محددة ووضع تصورات حول أنشطة النظام وأمنه وتختلف عن الجدران النارية بأنها تحتاج إدارة ومتابعة أكبر من قبل مراقبي نظم المعلومات والقائمين على تتبع أمن نظم المعلومات[1].

خامسا: النسخ الاحتياطي والاستعادة (Backup and Restore):

يعتبر واحد من الضروريات وتستطيع المؤسسة من خلاله استعادة المعلومات وغيرها في حال وقوع أي تلف عند اختراق القراصنة للنظام المعلوماتي، ويترجم هذا العمل بأجراء نسخ احتياطية في تواريخ معينة، كما ان امن الحواسيب ليس مضمونا مئة في المئة لذلك يجب ان تستعد لاحتمالية سقوط أي نظام رقمي وفي هذه الحالة اما ان تجازف بأنظمة العمل او ان تعتمد نظام للنسخ الاحتياطي للبيانات بهدف استعدتها عند الضرورة.[2]

ولابد من تحديد ما ينبغي نسخه احتياطيا ومتى يتم نسخه ويعتمد ذلك على درجة الحماية المراد تحقيقها وكذلك على درجة أهمية البيانات المخزنة.

سادسا: استخدام وسائل التعرف والتحقيق من شخصية المستخدم:

قبل استخدام مكونات الحاسب، أو نظام المعلومات فإن المستخدم يجب أن يطلب ذلك وفي هذه الحالة يجب أن يتعرف نظام الحاسب على المستخدم كما يجب أن يتحقق من شخصيته قبل أن يسمح له باستخدام مكونات النظام.

والتعرف (**Identification**) يعتبر أول خطوة في سبيل منح حق الدخول إلى النظام والمقصود به الاسم الذي يعرف به المستخدم، وهذا التعرف لا يكون كافيا لتحقيق أمن البيانات، حيث أنه يتوجب التحقق أو الوثوق من شخصيه المستخدم (**Authentication**) وهو يعني التأكد من المستخدم بأنه الشخص صاحب الاسم الذي تم إدخاله، ويمكن تقسيم وسائل التحقق من شخصية المستخدم الى ثلاثة مجموعات كالاتي:

[1] عبد الفتاح بيومي حجازي، **مرجع سابق**، ص 275.

[2] خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني، **مرجع سابق**، ص 133.

شيء ما يرتبط بذات الشخص او موجود فيه (Something you are):

يطلق عليها كذلك الصفات البيولوجية (**Biometrics**) ومن أهمها:

جهاز الكشف عن بصمة الاصبع (Finger Print Scanner) :

هو جهاز يقو بمضاهاة العلامات المميزة لكل بصمة من خلال تصوير بصمات الاصبع للعاملين في المنظمة عن طريق الماسح الضوئي والاحتفاظ بها في ذاكرة الحاسب الالي المتصل بجهاز الكشف عن بصمة الاصبع ويتم التعرف على الشخص بعد تطابق بصمته مع البصمة المسجلة بالجهاز.[1]

جهاز الكشف عن ملامح الوجه (Face Recognition):

يتكون من دائرة تليفزيونية مغلقة متصلة بالحاسب الالي، حيث تقوم الكاميرا بتصوير العامليين المصرح لهم استخدام النظام من مختلف الزوايا وتخزين صورهم في ذاكرة الحاسب الالي، عند محاولة استخدام النظام من قبل أي شخص تقوم الكاميرا بتصويره ومن تم اجراء المقارنة مع الصور المخزنة في قاعدة البيانات فاذا تطابقت صورة الشخص مع احدى الصور المخزنة يفتح النظام.[2]

جهاز الكشف على قزحية العين (Iris Recognition Device) :

يتم تسجيل بيانات مستخدمي النظام من خلال نظرهم الى الكاميرا التي تقوم بتصوير القزحية وإنتاج صور غير ملونة، زمن تم وضعها في شكل رموز رياضية في قاعدة البيانات لتشكل نموذج مرجعي يمكن العودة اليه عند القيام بعمليات المقارنة، حيث يجب على مستخدم النظام ان يقف امام الكاميرا بمسافة محددة لكي يتم التقاط صورة لتفاصيل القزحية وتحليلها وتحويلها الى رموز رياضية ومقرنتها بالرموز المسجلة وعند مطابقة الرموز يسمح له باستخدام النظام.[3]

---

[1] العيد عادل بن عبد الرحمان والفوزان محمد بن عبد الرحمان، **الحاسب الالي في علم البصمات**، الرياض: مكتبة الملك سعود، 2000، ص 78.

[2] Samir nanavati, **Biometrics identity verification in an networked world**, john wiley & sons inc, canada, 2002, p 64.

[3] Salvatore Tocci, **High-Tech ID's From Finger Scans to Voice Patterns**, Children's Press, 2000, p 64.

شيء ما يملكه الشخص (Something You Have):

البطاقات الممغنطة ((Magnetic Cards:

مخصص لها مكان في الحاسب الالي وتستخدم هذه الأخيرة لفتح الأبواب للمصرح لهم فقط، وتمكن هذه البطاقة حاملها من الدخول الى المنظمة او غرفة الحاسي الالي او النظام ولذلك يجب الحفاظ عليها، لأنها تمكن أي فرد من اختراق لنظام في حال العثور عليها.

شيء ما يعرفه الشخص (Something you know):

الرقم السري او كلمة المرور: (Password Or secret Code)

يتكون من عدد من الأرقام والحروف التي لا يفتح باب غرفة النظام او الحاسب الالي الى بعد ادخال هذا الرقم السري، ولذا فان معرفة هذا الأخير يعرض لخطورة بالغة ليس على مستخدم النظام، ولكن على النظام وشبكاته بأكملها. [1]

سابعا: التحديثات التلقائية (Automatic Updates):

إن بناء البرمجيات وأنظمة التشغيل عملية معقدة ولا تخلو من الأخطاء، كما أنها بحاجة الى تحسينات مستمرة تبعا لتغير ظروف استخدامها، وتزايد قدرات الأجهزة، ومن ناحية أخرى فان الحاجة الى التحديث والتطوير المستمر راجع ال وجود الثغرات الأمنية التي تكتشف بشكل مستمر في هذه البرمجيات والأنظمة مما يحتم اصلاح تلك الثغرات قبل أن يتم استغلالها من طرف المخترقين، وهذه العملية تتطلب إطلاق تحديثات دورية لسد تلك الثغرات.

وبعبارة أخرى فان عملية تحديث وتطوير البرامج يفرضها أمران هما:

- ادخال وظائف جديدة أو تحسين في الوظائف الموجودة في البرامج والأنظمة.
- سد الثغرات الأمنية المكتشفة في هذه البرامج والنظم للحد من إمكانية اختراقها.[2]

[1] محمد بن عبد الله القاسم وعبد الرحمان بن عبد العزيز الحمدان، **أساسيات امن المعلومات، د د ن**، عمان، 2008، ص 79.

[2] خالد بن سليمان الغثبر ومحمد بن عبد الله القحطاني، **مرجع سابق**، ص 99.

ثامنا: توفير مصدر احتياطي للطاقة الكهربائية:

يجب تغذية مراكز الحاسب الآلي بالطاقة الكهربائية باستمرار من خلال مصدرين مختلفين، بحيث يعمل أحدهما عند تعطل الآخر لصمان استمرار عمل مركز الحاسب الآلي في إنجاز مهامه.

ومن أهم مصادر الطاقة الكهربائية التي تستخدم في مراكز المعلومات مزود الكهرباء المستمر (**UPS**)، وهو جهاز يقوم بتخزين الطاقة الكهربائية في بطاريات داخلية لصمان استمرارية العمل في أجهزة الحاسب عند انقطاع التيار الكهربائي من مصادره الخارجية لفترة محددة. ولذلك يجب اختيار وصيانة البطاريات الخاصة بهذا الجهاز باستمرار. وفي حالة عدم توافر هذا الجهاز وتوقف مصدر الطاقة الكهربائية عن العمل، فإن ذلك يؤدي إلى توقف أجهزة الحاسب الآلي عن العمل وقوفا غير طبيعيا، ومن ثم تلف ملفات البيانات. وكذلك تستخدم مولدات الطاقة الكهربائية الاحتياطية، وهي مولدات تعمل في حالة توقف مصدر الطاقة الأساسي ينهار النظام وتتلف البيانات وملفاتها، وبصفة خاصة الملفات التي توقف الجهاز وهي ما زالت فيد الاستخدام، ومن المهم فحص المولدات الاحتياطية دوريا لضمان عملها بكفاءة وفاعلية، وكذلك التأكد من كفاية وفعالية مولد الطاقة الاحتياطي، وذلك يتطلب إجراء الصيانة الدورية والفورية عند الضرورة.[1]

[1] منصور بن سعيد القحطاني، مهددات المن المعلوماتي وسبل مواجهتها، **رسالة ماجيستر**، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، 2008، ص 48.

المطلب الثالث: أساليب الحماية التنظيمية والادارية

أ. تصنيف المعلومات:

تصنف المعلومات حسب أهميتها وحساسيتها وذلك بغرض معرفة درجة الحماية التي تطلبها، فمن المعلومات ما لا يحتاج إلى حماية بالمطلق ويحصل عليها من يريد ومتى يشاء، ومنها ما يحتاج إلى مستوى من الحماية ويمكن لأشخاص معينين أن يحصلوا عليها، ومنها ما يتطلب حماية قصوى ولا يتوفر إلا لشخص بعينه أو مجموعة يحددها. أن ضمان غايات أمن المعلومات كلها أو بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كل المعلومات تتطلب السرية وضمان عدم الافشاء، وليس كل المعلومات في منشأة واحدة بذات الاهمية من حيث الوصول لها أو ضمان عدم العبث بها.[1]

ب. التوعية داخل المؤسسة وخارجها:

لا يمكن تحقيق الامن المعلوماتي من دون وعي شامل وكامل بهذا الموضوع وخطورته، اذ ان من الضروري على المؤسسة مباشرة جملة من الحملات التوعوية لموظفيها وكذلك للمتعاملين معها، تشرح لهم المخاطر الأمنية المحتملة وكيفية تفاديها.[2]

وتستند التوعية الفعالة على المدى الطويل والمتوسط لتشجيع التغير في السلوكيات، العادات والمعتقدات.[3]

ج. الحماية عن طريق القوانين والتشريعات والاتفاقيات الدولية:

تتمثل هذه الوسائل أساسا في ضرورة تطوير اتفاقيات دولية في محال الامن المعلوماتي بصفة خاصة والامن السيبيراني بصفة عامة اذ يجب على اي دولة في العالم ان تملك اتفاقيات ثنائية او جماعية مع الدول الخارجية ومن المفيد ان يتم تطوير هذه الاتفاقيات تماشيا مع التطورات والتغيرات الحاصلة في المجال الرقمي، وفي المقابل يجب على الحكومات سن قوانين والعقوبات الرادعة لمرتكبي الجرائم المعلوماتية.

---

[1] عرب، يونس، **دليل أمن المعلومات والخصوصية جرائم الكمبيوتر والانترنت**، ط1، ألأردن: منشورات اتحاد المصارف العربية، 2002، ص 3.

[2] ليتيم فتيحة وليتيم نادية، **مرجع سابق**، ص 250.

[3] Vladimi Aman Gnuan, **Op.cit**, p 100.

د. وضع سياسة لأمن المعلومات:

قال **ابن خلدون**: "لابد للعمران البشري من سياسة ينتظم بها أمره"

سياسة أمن المعلومات هي: "مجموعة من القواعد والقوانين والممارسات التي تضبط عمل المؤسسة وتحمي مصادرها لتحقيق غايات أمنية خاصة، ولتكن جدية وممكنة يجب أن تمنح هذه القوانين الأفراد القدرة على تحديد الأفعال الحسنة والأفعال التي تتنافى مع هذه السياسات."

وعرفت سياسة أمن المعلومات أيضا على أنها:" مجموعة من التوجيهات واللوائح والقواعد والممارسات التي ترشد إلى كيفية قيام المنظمة بإدارة وحماية وتوزيع المعلومات."

بينما يعرفها **ديلاني** (**Dulany**) أنها:" مجموعة قوانين أمنية تسيطر على نظام المعلومات وتزوده بمستوى حماية موثوق به. وهذه السياسات يجب أن توجه الإدارة وسبل الحماية والمصادر المرتبطة بالمعلومات وبنظام المعلومات، ويرتبط مستوى قسوة تلك السياسات عادة بمستوى المخاطر المراد تجنبها."

- **متطلبات سياسة أمن المعلومات:**[1]

- أن تكون تكلفتها معقولة ومناسبة.
- أن تتوافق مع أسلوب أداء الموظفين لأعمالهم وتعاملهم مع العالم الخارجي.
- أن تلبي المتطلبات القانونية في بيئة المؤسسة.
- وأن تراعي العوامل الإجرائية ولذلك ففي أحيان كثيرة يتم التضحية ببعض المتطلبات الأمنية اليسيرة في مقابل تيسير سير العمل في المؤسسة.
- أن تكون القيود معقولة بحيث لا تمنع المستفيدين من استخدام أجهزة الحاسب لديهم بشكل يخدم المؤسسة بطريقة غير مباشرة.

[1] اود حسين طاهر، **أمن شبكات المعلومات**، ط2، الرياض: معهد الإدارة العامة، د س ن، ص 119-120.

- **خصائص وثيقة أمن المعلومات:**

ان معرفة وفهم أبرز الخصائص لوثيقة سياسة أمن المعلومات يعود بالأثر الإيجابي على التنقيد الصحيح لتلك الوثيقة، ويرى خبراء أمن المعلومات أن هـ=هـ الوثيقة يجب ان تكون مكتوبة بشكل تفصيلي، ومن أهم فات هذه الوثيقة ما يلي:[1]

- **أن تكون مكتوبة بلغة واضحة سهلة الفهم والتطبيق:** يجب أن تكون بنود السياسة الأمنية من إجراءات وقواعد واضحة ومقنعة بالنسبة للمستفيد
- **أن تحدد بوضوح مسؤوليات كل شخص:** يجب أن تحدد السياسة الأمنية، وجبات ومسؤوليات كل من الإدارة والموظف، ومسؤول أمن المعلومات حتى يتسنى لكل واحد منهم القيام بالمهام المطلوبة منه.
- **استخدام لغة بسيطة عند صياغة السياسة الأمنية:** يجب أن تصاغ السياسة الأمنية بلغة واضحة بسيطة بعيدة عن التعقيد واستخدام الكثير من المصطلحات والتي قد تكون غير مفهومة بالنسبة للمستفيدين.
- **سلطة فرض السياسة:** يجب أن توضح سياسة أمن المعلومات من لهم السلطة والصلاحية في حرمان المستفيد من الخدمة عند المخالفة.
- **اتاحة المجال للتعديل:** لابد من تعديل سياسة أمن المعلومات مع مرور الوقت، وذلك نتيجة لظهور مستجدات وظروف وتقنيات جديدة.

- **محتويات وثيقة سياسة أمن المعلومات:**

من أهم محتويات وثيقة سياسة امن المعلومات هي البنود التالية:

- الإجراءات اللازم اتخاذها فيما يخص أمن المعلومات وموارد المنشأة عند التوظيف وانهاء الخدمة.
- تحديد صلاحيات المستخدمين.
- وضع الشروط والقيود اللازمة لكلمات المرور لضمان حماية حسابات المستخدمين.
- تحديد المستخدمين الذين يسمح لهم بإضافة أجهزة أو برامج إضافية على أجهزتهم.
- الإجراءات الواجب اتباعها لحماية الشبكة الداخلية من الفيروسات والبرامج الضارة.
- شروط وقيود استخدام شبكة الانترنت والاتصال بها.

[1] الحميد محمد دباس وينينو، **مرجع سابق**، ص 31.

- الية النسخ الاحتياطي مع تحديد مسؤوليات وصلاحيات ذلك. [1]

هـ. وضع خطط الطوارئ:

لابد من وضع الخطط لاستمرارية عمل نظم المعلومات في حالة المشاكل الكبيرة كتعطل أجهزة الحاسوب تعطلاً طويلاً أو غير ذلك من الحالات الطارئة، ولابد من قياس المشاكل التي سيوجهها مستخدم النظام في هذه الحالات ووضع البدائل على ضوء ذلك، وفي بعض الأنظمة يستوجب وجود نظام مساند يعمل بطريقة فورية في حالة الطوارئ في حين أن هناك أنظمة أخرى يمكنها الاستغناء عن الحاسوب عدة أيام دون إن تتأثر تأثراً كبيراً هذا من ناحية الاستمرار التشغيلي المباشر للحواسيب، أما النواحي الأخرى الهامة غير المباشرة أو المساندة كالكهرباء المستمرة والثابتة أو التبريد الموزون المستمر فهي ضرورية للتشغيل الخالي من الأخطاء إذ أن الزيادة الشديدة في التيار الكهربائي والارتفاع في درجات الحرارة كلها تؤدي إلى أخطاء في تشغيل ومعالجة البيانات كذلك يجب مراعاة إن الانقطاع المفاجئ للتيار والإطفاء المباشر لأجهزة الحاسوب كثيرا ما يؤدي إلى فقدان بعض المعلومات أو السجلات.[2]

[1] محمد رنيف مسعد، فاعلية تضمين سياسات أمن المعلومات، في تامين مراحل بناء وتطوير الأنظمة المعلوماتية السعودية دراسة تحليلية، **رسالة ماجستير** في العلوم الاستراتيجية، جامعة نايف للعلوم الأمنية: كلية العلوم الاستراتيجية قسم الدراسات الاستراتيجية، 2013، ص 31.

[2] أيمن محمد فارس الدنف، **مرجع سابق**، ص 75.

خاتمة الفصل:

يتضح مما سبق أنه توجد العديد من الطرق والتقنيات، لتامين المعلومات من مختلف الاخطار والمهددات، الا ان هذه الأخيرة هي في تطور وتغير مستمر، فكل يوم الا وتظهر طرق جديدة لاختراق الأنظمة والاستلاء عليها أو اتلافها وتغيرها وهذا ما يقود الى ضرورة التفكير في أساليب حماية حديثة تتوافق مع ما هو حاصل من تطورات في أساليب الاختراق، إضافة الى ضرورة تطوير الاتفاقيات الدولية في هذا المجال، والاستفادة من خبرات الدول الرائدة في محال أمن المعلومات.

الفصل الثالث:

دراسة حالة مؤسسة اتصالات الجزائر –سعيدة–

بعد ان تطرقنا للجانب النظري للموضوع من خلال دراسة مفاهيم تكنولوجيا المعلومات والاتصالات وأمن المعلومات، والتعرف على المخاطر والتهديدات، وعرض مختلق الطرق والتقنيات والإجراءات الأمنية للحد من هذه المخاطر.

سنحاول في هذا الفصل اسقاط المفاهيم النظرية فعلى الجانب التطبيقي، وللقيام بذلك قسمنا هدا الفصل الى ثلاثة مباحث كالاتي:

المبحث الأول: عرض عام حول مؤسسة اتصالات الجزائر فرع –سعيدة–

المبحث الثاني: الاخطار التي تهدد نظام المعلومات والتقنيات المستخدمة ممن طرف المؤسسة لتأمينه

المبحث الأول: عرض عام حول مؤسسة اتصالات الجزائر

المطلب الأول: تقديم عام عن مؤسسة اتصالات الجزائر.

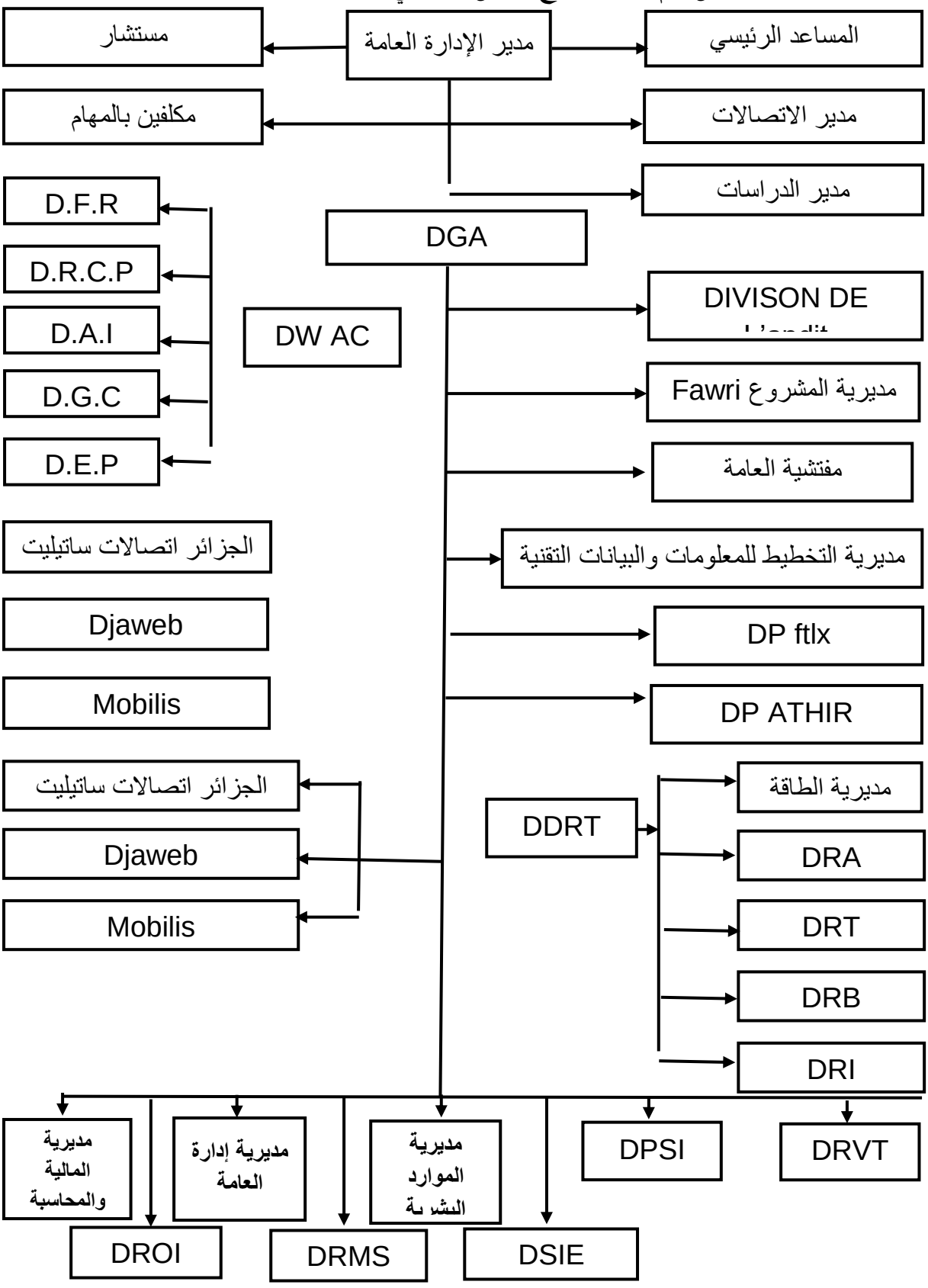
أ. التعريف بالمؤسسة:

اتصالات الجزائر تعتبر المتعامل التاريخي لقطاع الاتصالات في الجزائر وهي شركة ذات أسهم تابعة للدولة بنسبة 100 % =حيث كانت تابعة للوظيف العمومي إلى حين صدور القرار رقم 5في 2003/11/11 حيث أصبحت اتصالات الجزائر مؤسسة قائمة بذاتها وفي تاريخ 2005/09/14 أجريت تعديلات في هيكلة المؤسسات ومهامها بموجب مرسوم رقم 05/558 تحت 05/437.

في نهاية سنة 2005 استقل فرع شبكة الهاتف النقال موبيليس الذي أنشأ في 2002/12/31 عن الوكالة المركزية لاتصالات الجزائر ومن ثم أصبحت تنشط في سوق الهاتف الثابت والحلول الشبكية لتحويل المعطيات والصوت بالنسبة للشركات والخواص حيث تعد اتصالات الجزائر الرائد في هذا المجال بالجزائر.

وتعد اتصالات الجزائر مؤسسة ذات أسهم ملك للدولة بنسبة 100% وهي المتعامل التاريخي في سوق الحلول الشبكية وخدمات الاتصالات) الهاتف الثابت، اللاسلكي تم إنشاءها بموجب تطبيق بند 12 للقانون رقم 03/2000 مؤرخ في 5 أوت 2000 المتعلق إعادة هيكلة قطاع البريد والاتصالات وبموجب هذا القرار تم الفصل بين نشاطات البريد ونشاطات الاتصالات ومنه فإن مؤسسة اتصالات الجزائر هي وليدة هذا القانون وأصبحت مؤسسة ذات أسهم قائمة بذاتها تمارس أنشطتها بشكل رسمي ابتداء من 01 جانفي 2003.

الشكل رقم (11) يوضح الهيكل التنظيمي لمؤسسة اتصالات الجزائر



المصدر: معلومات مقدمة من طرف مصلة الموارد البشرية.

وسنتناول ذكر مختصر لمهام بعض المصالح:

الرئيس المدير العام (P.D.G) Président directeur générale

هو رئيس مجلس الإدارة ويعد المسؤول الأول عن الأعمال القائمة حيث يتولى مع مساعديه مهمة تحقيق الأهداف المرسومة من قبل المصالح المتخصصة ومن مهامه السهر على:

- الحفاظ على الحصص في السوق.
- تطوير ثقافة الشركة في سوق المنافسة.
- تطوير التسويق العملي.
- لسهر على تطبيق البرامج الموافق عليها والتنسيق بين المصالح.
- مراقبة تسيير النشاطات المختلفة في المؤسسة من خلال التقارير التي تصل إليها من المصالح المختلفة.
- لنظر في الاقتراحات المقدمة.
- المحافظة على السير الحسن والعادي في الشركة.

مديرية التخطيط للمعلومات والبيانات ال تقنية information des données Technique (IDT)

وتنحصر مهامه فيما يلي:

- تغذية الإعلامية العامة.
- تطبيق المهام الموكلة عند طلب رئيس المدير العام.
- التنسيق بين المديريات عبر المعلوماتية.
- لاطلاع على كل ما يخص الفواتير من تخليص أو عدم تخليص أو تعطيلات أو ما شابه ذلك. [1]

[1] معلومات مقدمة من طرف مصلحة الموارد البشرية بالمؤسسة.

المفتشية العامة(Inception Générale) :

- تكون تحت رقابة مباشرة للمدير وهي مكلفة ب:
- مراقبة قاعدة الأعمال السنوية.
- تنفيذ المهام المفاجئة للتفتيش بطلب من المدير العام شخصيا.
- القيام بتحقيقات في حالة ظهور أي مشكلة في الشركة.
- نسيق ومتابعة ومراقبة مصالح المتفشيات الإقليمية.
- تطبيق المخطط السنوي الجهوي بموافقة المدير العام.

مديرية الطاقة والمحيط (DEE):

وهي مكلفة بكل ما يخص الطاقة المستعملة من طرف الشركة بالإضافة إلى دراسة المحيط العام لها.

مديرية الموارد البشرية (DRH):

هي تعتبر العمود الفقري للشركة من مهامها:

إعداد الدراسات وإنشاء والإحصائيات ومتابعة مؤشرات التسيير.

المشاركة في إعداد المخططات التنموية مع الأخذ بعين الاعتبار تسيير المال والكفاءات.

إنشاء مخططات وبرامج التكوين وتنشيطها وفقا لوضعها العملي.

تسيير أنظمة المكافآت والتحفيزات

مديرية المالية والمحاسبة (DFC)وهي مكلفة ب:

- تقديم المساعدة للهياكل العملية.
- تنشيط السير المحاسبي والمالي للشركة.
- تسيير الميزانية والجباية.
- إعداد و وضع القواعد و الإجراءات و السهر على تطبيقها.

مديرية الإدارة العامة والإمدادات (DGAL) وتقوم ب:

- معالجة النصوص التنظيمية الأساسية لتنشيط أنظمة الشركة.[1]
- المحافظة على هياكل الشركة ومعالجة المسائل القضائية.
- تسيير وحماية الذمم المالية، وإعادة تسجيل عقود الملكية وإعادة الملفات العقارية.
- تهيئة وتسيير المراكز التابعة للشركة.
- تنشيط التسيير الإداري باستنتاج ومعالجة الصفقات.

التنظيم العام لاتصالات الجزائر مقسم حسب المبادئ العامة إلى ثلاثة مستويات:

المستوى الأول: المديرية العامة للمؤسسة وهي مقسمة إلى:

خمسة مديريات مركزية والمكونة من:

- مديرية تخطيط وتنظيم الإعلام.
- مديرية المالية.
- مديرية التسيير التقني لشبكات الاتصالات.
- مديرية الموارد البشرية.
- مديرية الإدارة العامة التشريعية.

رعين مركزيين من:

- فرع التسويق وتسيير النوعية.
- فرع تطوير شبكات الاتصالات.

المستوى الثاني: المديريات الإقليمية للاتصالات بعدد يبلغ ثمانية وهي مكونة من:

- عدة وحدات عملية للاتصالات.
- فريق عمل مكون من: خمسة مديريات فرعية

[1] معلومات مقدمة من طرف مصلحة الموارد البشرية بالمؤسسة.

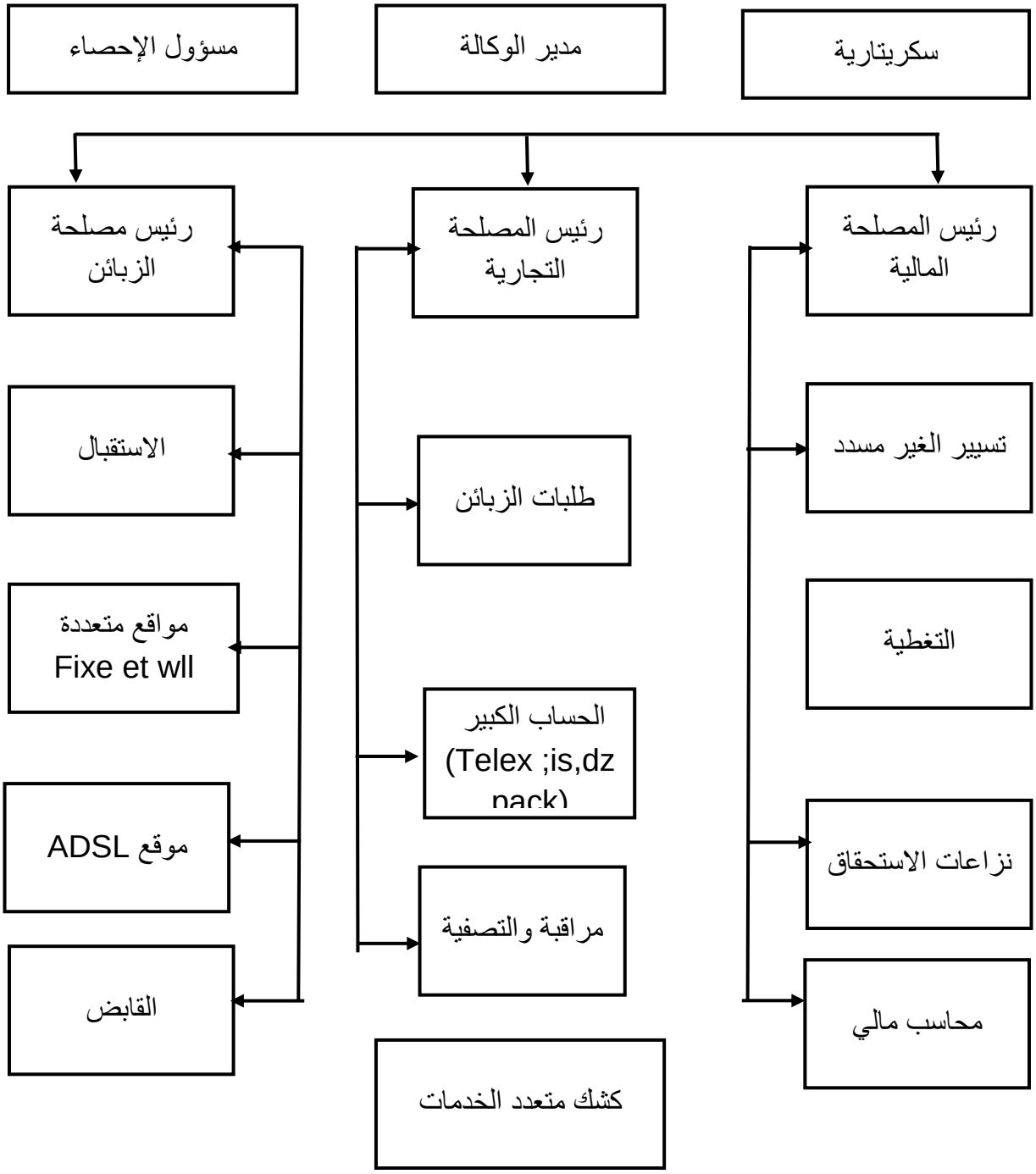
- مفتشية جهوية.
- لمستوى الثالث: الوحدات العملية للاتصالات:
- بعدد ثمانية وأربعون أي واحدة في كل ولاية وهي مكونة من:

- مركز عملي: مركز الاتصالات الهاتفية، وكالة تجارية للهاتف، **CECLI** وخدمات أخرى.
- فريق عمل. [1]

معلومات مقدمة من طرف مصلحة الموارد البشرية بالمؤسسة.

المطلب الثاني: الهيكل التنظيمي لمؤسسة اتصالات الجزائر فرع –سعيدة–

الشكل رقم (12) يوضح الهيكل التنظيمي لمؤسسة اتصالات الجزائر فرع –سعيدة–



المصدر: معلومات مقدمة من طرف مصلحة الموارد البشرية.

المطلب الثالث: مهام وأهداف مؤسسة اتصالات الجزائر

في هذا المطلب سوف نتطرق إلى مختلف المهام التي تقدمها مؤسسة اتصالات الجزائر بالإضافة إلى أهدافها

1. مهام مؤسسة اتصالات الجزائر:

تتكفل مؤسسة اتصالات الجزائر بتنمية المجتمع الإعلامي الجزائري وهي تنشط في سوق الهاتف الثابت والحلول الشبكة بتحويل المعطيات والصوت بالنسبة للشركات والخواص حيث تعد اتصالات الجزائر الرائد في قطاع الاتصالات بالجزائر لذا فهي تسهر على تقديم أحسن وأرقى الخدمات لزبائنها كما يلي:

- تتكفل بالخدمات الهاتفية ومختلف الارسالات على الأقمار الصناعية، حيث توفير للغير خدمات إرسال المعلومات أو الحصول عليها أصوات صور معطيات "عن طريق أي واسطة كهربائية أو راديو كهربائية بصرية أو كهرومغناطيسية كانت وذلك بغية رفع تحديات معقدة ومتعددة.
- العمل على استقطاب الكفاءات والخبرات الضرورية من مهندسين وتقنيين خاصة في مجال الاتصالات.
- زيادة عرض الخدمات الهاتفية وتسهيل وصول خدمات الاتصال إلى عدد كبير من المواطنين خاصة في المناطق الريفية.
- تمويل مصالح الاتصالات بما تسمح بنقل الصوت والصورة والرسائل المكتوبة والمعطيات الرقمية.
- تطوير واستمرار وتسيير شبكات الاتصالات العامة والخاصة.
- إنشاء واستثمار وتسيير الاتصالات الداخلية مع كل متعاملي شبكة الاتصالات.
- محاولة تصميم نظام معلوماتي متميز (**GAIA**) وفاء للزبائن يتمثل النشاط الرئيسي لمؤسسة اتصالات الجزائر في:
  - تقدير حاجيات الزبائن وتلبيتها.
  - مردودية الهياكل القاعدية والمحافظة عليها ،لاسيما فيما يتعلق بصيانة أفضل.
  - عرض خدمات ذات نوعية لا يعاب عليها.
  - تحصل الديون في اجلها المستحقة. [1]

[1] https://www.algerietelecom.dz/siteweb.php?p=presentation Consulter le 01/05/2018 à 15:00

2. أهداف مؤسسة اتصالات الجزائر:

اتصالات الجزائر تعمل في عالم تكنولوجيا الإعلام والاتصال ذلك بأربع أهداف هي:

- زيادة في نسبة العرض بالنسبة للخدمات الهاتفية، وتسهيل الولوج لخدمات الاتصالات وذلك للوصول لعدد أكبر من المستعملين، وبالخصوص المناطق الريفية.
- زيادة وتنمية في جودة الخدمات المعروضة، وسلسلة أو مجموعة التشكيلات المقدمة، وجعلها أكثر تنافسية في مجال خدمات الاتصالات.
- تطوير شبكة وطنية محلية للاتصالات، مرنة وموصولة بطرق الإعلام.
- المشاركة كممثل رئيسي في مجال فتح برنامج تطوير لمؤسسة الإعلام والاتصال في الجزائر. وتتمحور نشاطات المؤسسة حول:
  - تمويل مصالح الاتصالات بما يسمح بنقل الصورة والصوت والرسائل المكتوبة والمعطيات الرقمية.
  - تطوير واستمرار وتسيير شبكات الاتصالات العامة والخاصة.
  - إنشاء واستثمار وتسير الاتصالات الداخلية مع كل متعاملي شبكة الاتصالات.[1]

[1] https://www.algerietelecom.dz/siteweb.php?p=presentation Consulter le 01/05/2018 à 15:00.

المبحث الثاني: الاخطار التي تهدد نظام المعلومات والتقنيات المستخدمة ممن طرف المؤسسة لتأمينه

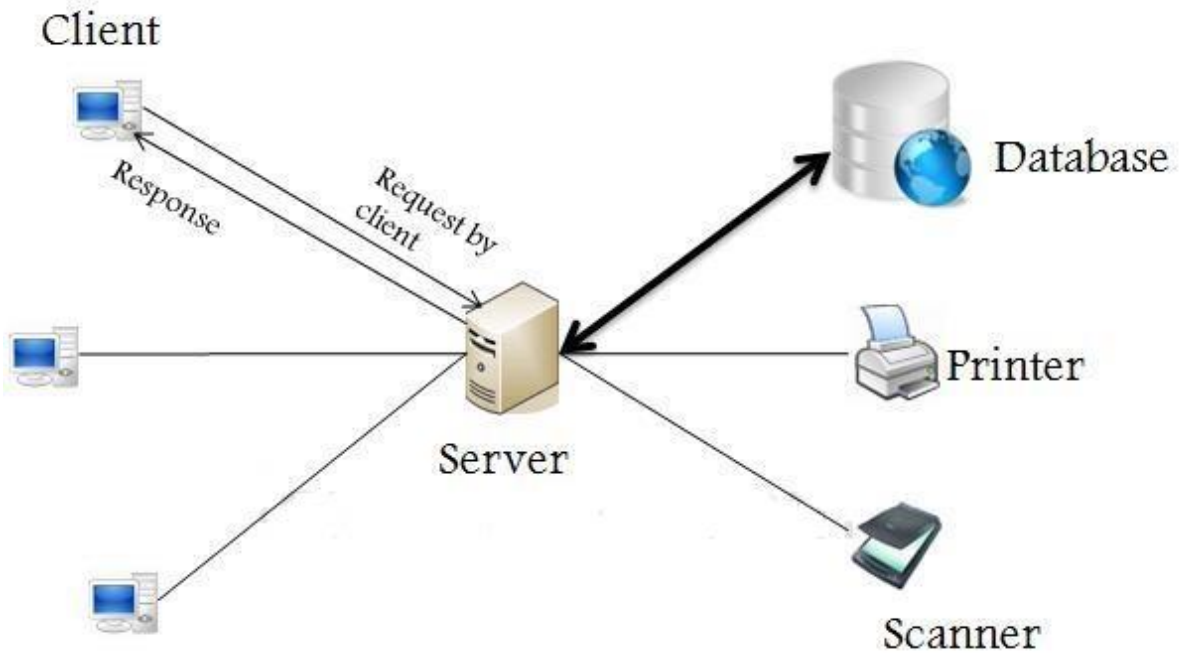
المطلب الأول: نظام المعلومات في المؤسسة.

1. وصف النظام:

بناءا على المقابلة التي أجريت مع المكلفة بنظام المعلومات اتضح أن نظام المعلومات يتكون من:

الأجهزة والمعدات، البرمجيات، قواعد البيانات والشبكات. ويعتمد على تقنية خادم/زبون كما يوضحه الشكل في الأسفل:[1]

شكل رقم (13) يوضح تقنية خادم/زبون



Source : https://www.ianswer4u.com/2011/05/client-server-architectures.html consulter le 19/05/2018 a 18: 17

[1] معلومات مقدمة من طرف المكلفة بنظام المعلومات بالمؤسسة.

يمثل الشكل السابق تمثيل لتقنية خادم/زبون، حيث يتواجد في المركز خادم واحد أو مجموعة ممن الخوادم، ترتبط مع أجهزة تسمى الزبائن قد يكون هذا الزبون محطة طرفية، أو حاسوب محمول أو طابعة أو غيرها من الأجهزة الأخرى.

أ. الأجهزة والمعدات:[1]

يتكون نظام المعلومات من مجموعة من الأجهزة موضحة في الجدول التالي:

جدول رقم (03) يوضح مكونات نظام المعلومات بالمؤسسة

الجهاز	العدد	الملاحظة
الموجه (Router)من نوع Cisco	02	
جدار الحماية من نوع (Stonesoft)	02	
خوادم (Servers) من نوع (Bull)	05	تصل السعة التخزينية الى 15 Tb
مولد كهربائي	01	
مكيفات هواء	06	

المصدر: من اعداد الطالب استندا على معلومات مقدمة من طرف المكلفة بنظام المعلومات بالمؤسسة.

[1] معلومات مقدمة من طرف المكلفة بنظام المعلومات بالمؤسسة.

البرمجيات: يحتوي النظام على نوعين من البرمجيات برنامج التشغيل (نظام التشغيل) ونظام التسيير (**GAIA**) وهو عبارة عن نظام معلومات مطور من طرف شركة سوفركوم الفرنسية

(**Sofrecom Telecom**) موجه خصيصا للمتعاملين في ميدان الاتصالات، وهو يسمح بتسيير الجانب التجاري والتقني للزبائن، حيث استثمرت اتصالات الجزائر في هذا النظام مند 2004 وهو مازال مستمر حتى الأن وهو في تطور مستمر.

ب. **قاعدة البيانات:** بنيت قواعد البيانات لنظام المعلومات بقواعد المعطيات اوراكل (Oracle) وهو نظام قوي كما يقبل لغة البرمجة الاستعلامية، التي تسمح بمحاورة قواعد البيانات بسلاسة.

ج. **الشبكات:** تعتبر الشبكات واحدة من بين أهم عناصر نظام المعلومات كونها تسمح للزبائن بالاتصال بالخوادم المركزية، وتتوفر اتصالات الجزائر بحكم نشاطها على مجموعة من الشبكات نذكرها كالاتي:

- **شبكة (RMS)**: وهي شبكة عملاقة مكونة من مجموعة من الموجهات الكبيرة، والمجمعات، تتحكم في كامل الشبكة تمر عبرها مختلف البيانات لمختلف الخدمات
- **شبكة (LAN)**: وهي شبكة محلية تستعمل البروتوكول **TCP/IP** كقاعدة للاتصال، وتكون محدودة المكان.
- **شبكة (VPN)**: وهي عبارة عن شبكة وهمية تستعمل الانترنت كقاعدة للاتصال.

2. خصائص نظام: المعلومات (GAIA):

- قراءة الية لملفات التحصيل.
- تحميل معطيات خارجية من ملفات النظام.
- وسيط تحويل من محاسبة الزبائن الى المحاسبة العامة
- وسيط دفع بين الهيئات البنكية الأخرى.[1]

[1] معلومات مقدمة من طرف المكلفة بنظام المعلومات بالمؤسسة.

المطلب الثاني: الاخطار التي تهدد نظام المعلومات في المؤسسة.

بعد القيام بمقابلة مع المكلفة بنظام المعلومات باتصالات الجزائر فرع –سعيدة– اتضح أن الأخطار التي تهدد نظام المعلومات هي كالاتي:

- أكبر خطر يهدد نظام المعلومات هو تعطله، بسبب خلل في الشبكة.
- الأخطاء الغبر متعمدة من طرف المتعاملين مع النظام أثناء عمليات ادخال البيانات.
- الهجمات الفيروسية وتعطل الأجهزة الخاصة بنظام المعلومات.

المطلب الثالث: التقنيات التي تتبعها المؤسسة لحماية نظام المعلومات.

من خلال الأسئلة التي طرحت على المكلفة بنظام المعلومات

- فان المؤسسة لا تعتمد سوى على أساليب حماية برمجية فقط والمتمثلة في مضاد للفيروسات والموجود على مستوى الحواسيب إضافة الى الجدار الناري.
- اغلب الحواسيب محمية بكلمة مرور الا انه لا يتم تغيرها بشكل دوري، ولا وجود للتقنيات الحديثة للتعرف على المستخدم كبصمة الاصبع وغيرها.
- يتم عمل نسخ احتياطي للنظام بصفة دورية.
- لا وجود لسياسة أمنية داخل المؤسسة توضح صلاحيات المستخدمين والمتعاملين مع النظام.
- لا يوجد قسم او مصلحة مختصة أو مكلفة بأمن المعلومات.[1]

[1] معلومات مقدمة من طرف المكلفة بنظام المعلومات بالمؤسسة.

خاتمة الفصل:

كان هذا الفصل عبارة عن دراسة حالة مؤسسة اتصالات الجزائر فرغ –سعيدة– وذلك لأسقاط ما تم التطرق الية في الجانب النظري.

وكانت النتائج المتوسل اليها من خلال الفصل كالاتي:

- هناك العديد من المخاطر التي تهدد نظام المعلومات داخل المؤسسة لكن تبقى هذه المخاطر متواضعة مقارنة مع التهديدات التي تطرقنا لها في الجانب النظري، وهذا ما يفسر استخدام المؤسسة لتقنيين فقط لتامين نظام المعلومات.
- يمكن التقليل من هذه المخاطر عن طريقة وضع سياسية أمنية توضح صلاحيات ومهام المتعاملين مع النظام.
- يجب أن تصاحب هذه السياسة حملة من الحملات التوعوية والتحسيسية بأمن المعلومات والمخاطر المرتبطة به.

بينت الدراسة ان هناك قصور كبير في الأمور المتعلقة بأمن وسرية المعلومات بالمؤسسة وعليه يمكن اقتراح جملة من الإجراءات والتدابير للحفاظ على درجة عالية من الأمان في النظام نوضحها في ما يلي:

- استقطاب خبراء ومتخصصين في مجال أمن المعلومات
- وضع سياسة واضحة لأمن المعلومات بالمؤسسة
- استخدام الوسائل البيولوجية لتحديد شخصية مستخدمي نظام المعلومات.
- تخصيص ميزانية لأمن المعلومات ضمن الميزانية الخاصة بتكنولوجيا المعلومات

خاتمة

خاتمة:

أصبح الأمن المعلوماتي اليوم واقعا تفرضه التطورات الحديثة في تقنية المعلومات والتي بدورها أحدثت تغيرات مستمرة في أساليب العمل في كافة الميادين اذ أصبحت عملية انتقال المعلومات عبر الشبكات المحلية و الدولية وأجهزة الحاسوب من الامور الروتينية واحدى علامات العصر المميزة التي لا يمكن الاستغناء عنها لتأثيرها الواضح في تسهيل متطلبات الحياة العصرية من خلال تقليل حجم الاعمال وتطوير اساليب تخزين و توفير المعلومات ،حيث ان انتشار انظمة المعلومات المحوسبة ادى الى ان تكون عرضة للاختراق لذلك أصبحت هده التقنية سلاحا دو حدين تحرص المنضمات والمؤسسات على اقتنائه و توفير سبل الحماية له.

تطرقنا في بحثنا هذا الى واحد من أهم المواضيع العصر أهمية والمتمثل في أمن المعلومات وسبل حمايته، قسمن هذه الدراسة الى فصلين نظريين وأخر تطبيقي، اخترنا أن يكون في مؤسسة اتصالات الجزائر وهي واحدة من المؤسسات الوطنية الرائدة في تكنولوجيا المعلومات والاتصالات.

وقد توصلنا من خلال هذه الدراسة الى مجموعة من النتائج نجملها كالاتي:

- إنه من الصعب جدا بل من المستحيل الوصول الى نظام آمن وسري لقاعدة ما بشكل كامل ولكن يمكن القول اننا نسعى دائما للتوصل الى درجة عالية من الثقة في النظام المعلوماتي.
- الأمن يتناسب عكسيا مع تعقيد النظام أي كلما كثرت الإجراءات الأمنية المستخدمة لتامين نظام المعلومات كلما تعقدت عمليات التعامل مع النظام.
- لا يمكن للوسائل التكنولوجية وحدها تحقيق درجة عالية من الأمان في نظام ما بل يجب ان يكون هناك مزيج بين العديد من الطرق والأساليب والتقنيات الإدارية القانونية والبشرية.
- في أي مؤسسة يمثل العنصر البشري أحد أهم الموارد وفي المقابل هو أول مهدد وخطر على أمن المعلومات.

ويمكننا الإشارة الى الاقتراحات التالية:

- في هذا الإطار من الضروري على الدول خاصة العربية منها والتي تعاني من قصور في مجال الأمن المعلوماتي الاطلالة على ما انتجته الجهود الدولية في هذا المجال والاستفادة من الخبرات المتراكمة للدول الرائدة في مجال الأمن والحماية المعلوماتية.
- نقرح على المؤسسات الجزائرية ضرورة التركيز على المفاهيم الحديثة التي تسلط الضوء على كل ماله علاقة بدورة حياة المعلومة، وضرورة الاتجاه نجو تطبيق المواصفة الدولية **ايزو 27001** لأن هذه المؤسسات اليوم

خاتمة:

أصبحت تتسم: بتزايد هائل في المعلومات الأمر الدي يتوجب معه توجيه الأنظار نحو المفاهيم والأنظمة التي من شانها تسهيل وتنظيم التعامل مع هذا القدر الهائل من المعلومات، فضلا عن أن حصول هذه المؤسسات على شهادة **ISO** في هذا المجال سوف يمكنها من الحصول على ميزة تنافسية واكسابها الطابع العالمي من خلال حصولها على شهادة دولية، كما نشير أنه من خلال بحثنا في المواقع المتخصصة والمواقع الرسمية لم نجد مؤسسات جزائرية حاصلة على شهادة **الإيزو 27001** في حين أن أهم الشهادات التي توجهت إليها بعض المؤسسات الجزائرية الذي يعد قليلا جدا كانت تتمحور حول شهادة **الإيزو9001** لتطبيق أنظمة الجودة، **الإيزو 14001** المتعلقة بأنظمة البيئة، **الإيزو 22000** المتعلق بالسلامة الغذائية ، **الإيزو 1800** المتعلق بالصحة و السلامة المهنية.

- نشير إلى ضرورة استفادة المؤسسات الجزائرية من الخبرات والاستشارات الخارجية، خاصة بالنسبة للمؤسسات الأجنبية التي لها فروع في الجزائر كالبنك العربي الذي يطبق نظاما لأمن وحماية المعلومات يتوافق مع **الإيزو 27001** وهو من الحالات القليلة جدا التي وجدناها من خلال بحثنا في المواقع المتخصصة ذات الصلة بالموضوع.
- ضرورة قيام الجهات الحكومية الجزائرية بإنشاء مركز متخصص يعنى بقضايا أمن المعلومات ويهدف لمساعدة الهيئات والمؤسسات العامة والخاصة في تطوير جودة نظمها لمواكبة الأحداث والمستجدات خاصة في مجالات أمن المعلومات.
- على المؤسسات والإدارات الجزائرية سوءا كانت عامة أو خاصة التعاقد مع شركات ومؤسسات مختصة في الأمن المعلوماتي وهي الخطوة التي خطتها بعض الدول العربية كالمغرب والسودان والامارات العربية المتحدة.
- استخدام نظام فعال للحوافز المادية والمعنوية لتشجيع المبدعين والمتميزين في مجال أمن المعلومات.
- ضرورة الانفتاح على التجارب العالمية في مجال أمن المعلومات والاستفادة منها.

ستسمح هذه الدراسة حتما بالولوج الى مواضيع أخرى يمكن ان تكون مواضيع بحث مستقبلية فالحديث عن موضوع الأمن المعلوماتي تجعل من الصعب الوقوف عند حد معين ولذا بمكن البحث في مواضيع مثل:

واقع أمن المعلومات في المؤسسات الجزائرية بين القوانين الوطنية والمعايير الدولية.

الملاحق

ملحق رقم (01) يوضح نموذج لوثيقة سياسة أمن المعلومات.

سياسة أمن المعلومات:

أمن معلوماتك

إن المحافظة على سرية وأمن معلوماتك الشخصية من أهم الأولويات في البنك العربي حيث اتخذنا التدابير المناسبة لحماية سرية معلوماتك الشخصية ووقايتها من الدخول غير المصرح به، إذ أن حماية معلوماتك الشخصية تعتبر مسئولية كل موظف من موظفينا .

ويقوم البنك العربي بشكل متواصل بمتابعة التطورات المتعلقة بحماية المعلومات وتحديث عملياته وإجراءاته لضمان الالتزام بأعلى ممارسات الصناعة المصرفية في هذا المجال. وسواء اخترت التعامل معنا من خلال مراكزنا المالية/فروعنا، أو أجهزة الصراف الآلي، أو الخدمات المصرفية عبر البنك الناطق أو الإنترنت، فإننا نلتزم بالمحافظة على حماية معلوماتك سواء عند جمعها أو استخدامها أو مشاركتها .

للحصول على معلومات إضافية حول إجراءاتنا لحمايتنا خصوصية المعلومات، يرجى الضغط على الرابط التالي سياسة خصوصية المعلومات في البنك العربي .

حماية كلمة السر

تعتبر كلمات السر المفاتيح إلى حساباتك ومعلوماتك الشخصية. وفيما يلي بعض الخطوات التي يمكنك القيام بها لحماية معلوماتك الشخصية من الدخول غير المصرح به.

لا تعمل	اعمل
*لا تستخدم أسماء أشخاص	*استخدم ستة حروف على الأقل
*لا تستخدم معلومات شخصية	*استخدم حروف وأرقام
*لا تستخدم كلمات من القاموس	*استخدم أحرفا خاصة إذا كان
*لا تكتبها على ورق لاصق ولا تحفظها	بالإمكان(@#&$)
على شاشة الحاسوب	*استخدم الحروف الكبيرة والصغيرة
*لا تحفظ كلمة السر في الدرج	(A a)
*لا تستخدم نفس كلمة السر لعدة	
تطبيقات	*قم بتوحيد الكلمات في كلمة واحدة أو
*لا تعيد استخدام كلمات السر القديمة	استخدم تهجئه خاطئة
	*قم بالتغطية أثناء إدخال كلمة السر
	*غير كلمة السر بشكل دوري

أحذر من سرقة بياناتك الشخصية عبر الإنترنت "Phishing"

هو نوع من أنواع الخداع المعد للحصول واستخدام معلوماتك الشخصية واستخدامها (مثل أرقام بطاقات الائتمان، كلمات السر، بيانات حسابك، الخ) لأغراض احتيالية .

قد يقوم محترفو الاحتيال عبر الانترنت (قراصنة الانترنت) بإرسال الآلاف من الرسائل الإلكترونية المزيفة التي يبدو وكأنها صادرة عن مواقع الكترونية موثوقة، مثل الموقع الخاص بالبنك الذي تتعامل معه أو موقع شركة بطاقة ائتمانك، حيث تطلب هذه الرسائل الإلكترونية إعطاء معلومات شخصية عنك من خلال البريد الإلكتروني أو على موقع غير مشروع على شبكة الإنترنت يكون منشئا من قبل هؤلاء القراصنة لغايات احتيالية .

نصائح لحمايتك من سرقة بياناتك الشخصية عبر الإنترنت "Phishing"

في حالة استلامك رسالة الإلكترونية مشكوك فيها بحيث تبدو أنها صادرة عن البنك العربي، يرجى القيام بما يلي :

- لا تقم بالرد على الرسالة، أو بالنقر على أي رابط إلكتروني، أو بأجراء اية تغييرات على الرسالة الإلكترونية بأية طريقة .
- اتصال بنا فورا وقم بشطب رسالة البريد الإلكتروني بعد تبليغنا عنها .
- قم بالتأكد من أن برنامج الحماية من الفيروسات وبرامج الحماية من التجسس الإلكتروني-anti " "spywareمحدثة وخاصة إذا قمت بالنقر بالخطأ على الرابط أو المرفق بالرسالة الإلكترونية .

نصائح أخرى لحماية معلوماتك الشخصية

- كن شديد الحذر عند التسوق عبر الإنترنت. لا تقم بإدخال رقم بطاقة الائتمان أو معلوماتك الشخصية إلا إذا قمت أنت بإنشاء هذه العملية وعلى موقع الكتروني موثوق .
- عند إدخالك لأرقام بطاقة الائتمان أو معلوماتك الشخصية تأكد من أنك تستخدم موقعا الكترونيا آمنا. تأكد من وجود شهادة حماية أمنية للموقع الالكتروني قبل إدخال معلوماتك الشخصية .
- استخدم الخدمات المصرفية الإلكترونية بشكل منتظم)ومثالها: الخدمات المصرفية عبر الإنترنت أو الهاتف النقال "SMS" أو البنك الناطق أو عن طريق أجهزة الصراف الآلي ("ATM" للكشف عن أية عمليات احتيالية إن وجدت .
- أغلق الرابط الإلكتروني على الشبكة عند الانتهاء من استخدامه وخاصة إذا كنت تستخدم المودم أو DSLللدخول إلى شبكة الإنترنت .ادرس إمكانية استخدام برنامج الحماية الشخصي (Personal Firewall).

إدارة المعلومات التي يتم الحصول عليها إلكترونياً

ان المعلومات الشخصية المستلمة عبر الرسائل إلكترونية، بما في ذلك الدخول إلى الموقع الإلكتروني للبنك العربي، أو الخدمات مصرفية عبر الإنترنت، أو الطلبات الواردة إلكترونيا، أو البريد إلكتروني، يتم المحافظة عليها لضمان حماية خصوصية معلوماتك. هذا وقد نقوم باستخدام هذه المعلومات في تلبية احتياجاتك المصرفية وتحسين المنتجات

والخدمات ومعرفة عدد الزائرين لموقعنا الإلكتروني بالإضافة إلى التعرف على الفرص التي تمكننا من خدمتك بشكل أفضل .

تتبع استخدام الموقع الإلكتروني "Cookies"

عند الدخول لأي موقع الإلكتروني، فأن جهازك سيقوم بتخزين معلومات معينة بشكل مؤقت على شكل ملفات تصنف بألكوكيز. يتم استخدام الكوكي للتعرف / تتبع أجهزة الحاسوب التي قامت بزيارة الموقع حيث أنها لا تقوم بجمع أية معلومات تتعرف عليك بشكل شخصي ولا تستخدم لأغراض جمع المعلومات المخزنة على جهازك. يمكنك إبطال عمل "الكوكيز" من خلال القيام بالتعديلات اللازمة على جهازك مستخدما الأدوات على المتصفح "browser"الخاص بك .

كيف نقوم بحمايتك؟

حماية أمن المعلومات

ان الحفاظ على سرية وأمن معلوماتك الشخصية والمالية من أهم المسؤوليات المناط بنا. ستبقى معلوماتك في حماية نظرا للتدابير الأمنية المتخذة مثل: التشفير/الترميز، وتوثيق الدخول، وبرامج الحماية من الفيروسات، وبرامج كشف الدخول غير المصرح به، الموجودة الأنظمة والخدمات التي نقدمها .

الوقاية من سرقة الهوية

ان النشاطات الإجرامية، بما في ذلك سرقة الهوية والأعمال الاحتيالية، قد أصبحت تنتشر اليوم بشكل أكثر عما كانت عليه في السابق. حيث أن المجرمون في سعيهم للحصول على معلومات شخصية عنك ، قد يقوموا بالاتصال بك مدعيين بأنهم يمثلون مؤسسة ما تتعامل معها، لهذا السبب فانه يجب أن تتأكد من انك تعرف أو يمكنك التحقق من هوية الشخص أو الجهة التي قامت بمخاطبتك للحصول على معلومات شخصية أو معلومات ذات صفة مصرفية سواء أكان ذلك شفويا أو كتابياً. يرجى العلم بأن البنك العربي لا يقوم بطلب مثل هذه المعلومات سواء عبر الهاتف أو البريد الإلكتروني، وفي حالة استلامك لطلب مماثل، الرجاء الاتصال بنا للإبلاغ عن ذلك فورا .

تغيير هذه السياسة

قد يلزمنا من وقت أخر تغييرات على سياسة أمن المعلومات الخاصة بنا. سيتم الاحتفاظ بالنسخة المحدثة على الموقع الإلكتروني الخاص بالبنك العربي .

للحصول على مزيد من المعلومات

في حالة وجود أية استفسارات إضافية حول هذه السياسة أو في حال رغبتك الحصول على مزيد من المعلومات عن إجراءاتنا الخاصة لحماية الخصوصية، يرجى الرجوع الجزء الخاص بسياسة خصوصية المعلومات في البنك العربي أو الاتصال بنا.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

1. المصادر:

أ. القرءان الكريم.

ب. المعاجم والقواميس:

1. Webster's **dictionary of English usage**, Merriam webster inc, 1989.
2. HL7 Secure **Transactions**, **Glossary Of Acronyms**, **Abbreviations and Terms Related To Information Security** In Healthcare Information Systems, 1999.
3. ICAEW, **Glossary of IT security terms**, London, Uk, 2013.

2. المراجع:

أ. الكتب باللغة العربية:

1. اود حسين طاهر، **أمن شبكات المعلومات**، ط2، الرياض: معهد الإدارة العامة، د س ن.
2. بحوش عمار، **دليل الباحث في المنهجية**، الجزائر: المؤسسة الوطنية للكتاب، 1985.
3. داوود حسن طاهر، **أمن شبكات المعلومات**، ط1، الرياض: معهد الإدارة العامة، 2004.
4. عبد الحميد محمد، **تحليل المحتوى في بحوث الاعلام**، مصر: ديوان المطبوعات الجامعية، 1979.
5. عدنان يحي، **تكنولوجيا المعلومات**، ط1، فلسطين: وزارة التربية والتعليم العالي، 2005.
6. عرب يونس، **دليل أمن المعلومات والخصوصية جرائم الكمبيوتر والانترنت**، ط1، ألأردن: منشورات اتحاد المصارف العربية، 2002.
7. عطيات شعبان غبد الرحمان، **أمن الوثائق والمعلومات**، ط1، الرياض: جامعة نايف للعلوم الأمنية، 2003.

8. عطيات عبد الرحمان شعبان، **امن الوثائق والمعلومات**، ط1، الرياض: جامعة نايف العربية للعلوم الامنية، 2003.

9. العيد عادل بن عبد الرحمان والفوزان محمد بن عبد الرحمان، **الحاسب الالي في علم البصمات**، مكتبة الملك سعود، الرياض، 2000.

10. الغثبر خالد بن سليمان ومحمد القحطاني بن عبد الله، **أمن المعلومات بلغة ميسرة**، ط1، الرياض: مركز التميز لأمن المعلومات، 2009.

11. فرغلي موسى عبد الله علي، **تكنولوجيا المعلومات ودورها في التسويق التقليدي والالكتروني**، ط1، مصر، إتراك للطباعة والنشر والتوزيع.

12. القاسم محمد بن عبد الله ولحمدان عبد الرحمان بن عبد العزيز، **أساسيات امن المعلومات، د د ن**، 2008.

13. كامل عبد الحميد محمد فاروق، **المعلومة الأمنية**، ط1، الرياض: أكاديمية نايف للعلوم الأمنية، 1999.

14. لورنس م. اوليفا، ترجمة **محمد مراياتي امن تقنية المعلومات نصائح من خبراء**: المنظمة العربية للترجمة، ب س ن.

15. مظلوم محمد جمال، **الأمن الغير تقليدي**، ط1، الرياض: جامعة نايف للعلوم الأمنية، 2013.

16. وينينو الحميد محمد دباس، **حماية أنظمة المعلومات**، دار حامد للنشر والتوزيع، عمان، 2007.

ب.الكتب بالغة الأجنبية:

17. Jamod véronique, **l'impact des innovations technologiques et organisationnelles sur les performances des entreprises**, **une évaluation non paramétrique**, 2004.

18. M. Gercke, Understanding **Cyber Crime ITU Telecommunication Development Sector**, 2nd Ed, 2011.

19. V.S Bagad, **Financial and industrial management**, 1st Ed, india: technical publication pune, 2008.

20. Vladimir aman Gnuan, **Concevoir la sécurité informatique en entreprise**, 2014.

21. Jason Andress, **the basics of information security**, 2nd Ed, Usa, 2014.

22. Michael whitman and Harbert Mathord, **principles of information security**, 5th Ed, usa, 2012.

23. Umesh Hodeghtta and Umeshaa nayak, **The info sec Handbook an introduction to information security**, Apress open, New york.

24. Christopher Hadnagy, **Social Engineering the art of human hacking**, Wiley publishing Inc, Usa, 20111.

25. Chuck Erstton, **computer security Fundaentals**, third edition, Deason publishing Inc, Usa, 2016.

26. Dorothy Elizabeth, **Cryptography and data security**, Addison-Wesley Publishing Company, Inc, 1982.

27. Laurent Bloch et Christophe Wolfhugel, **Sécurité Informatique principes et méthode de l'usage des DSI RSSI et administrateurs**, 2émé Ed eyrolles.

28. Samir nanavati, **Biometrics identity verification in an networked world**, john wiley & sons inc, canada, 2002.

29. Salvatore Tocci, **High-Tech ID's From Finger Scans to Voice Patterns**, Children's Press, 2000.

ج. الدوريات والمجلات:

30. العربي عطية، "أثر استخدام تكنولوجيا المعلومات على الأداء الوظيفي للعاملين في الأجهزة الحكومية المحلية"، **مجلة الباحث**، العدد 10، الجزائر، 2012.

31. ندى إسماعيل جبوري، "حماية امن انظمة المعلومات دراسة حالة مصرف الرافدين"، **مجلة تكريت للعلوم الإدارية والاقتصادية**، مجلد رقم 7، العدد رقم 21، بغداد، 2011.

32. ليتيم فتيحة وليتيم نادية، "الامن المعلوماتي للحكزمة الالكترونية وإرهاب القرصنة"، **مجلة الفكر**، العدد 12.

33. يحياوي محمد، "مخاطر القرصنة المعلوماتية على الحكومة الالكترونية"، **مجلة البحوث والدراسات العلمية**، العدد 05، 2011، الجزائر.

34. Adam Shostack, "the evolution of information security", **the next wave**, vol 19, N° 2, 2012.

35. Mouna jouini et fatima ben arefa, "Classification of security threats in information systems", **procedia computer science**, 32.

د. التقارير:

36. Verizon, **Data breach investigations report**, 10th Edition, 2017.

37. Calyplix Security, **top security threats what's ahead and how to prepare**, 2017 report.

هـ. الرسائل والأطروحات الجامعية:

38. لقيدوم صباح، أثر تكنولوجيا المعلومات والاتصالات الحديثة على التسيير الاستراتيجي للمؤسسات الاقتصادية، **أطروحة دكتوراه** في علم التسيير، جامعة قسنطينة 2: كلية العلوم الاقتصادية وعلوم التسيير، قسم علوم التسيير، 2013/2012.

39. بوزاوية زهرة، مجتمع المعلومات والكفاءات الجديدة، لدى أخصائي المعلومات دراسة ميدانية بالمؤسسات الوثائقية بولاية وهران، **مذكرة ماجستير**، جامعة وهران 1 أحمد بن بلة: كلية العلوم الإنسانية، قسم علم المكتبات، 2015/2014.

40. توامي يعقوب، أثر استخدام تكنولوجيا المعلومات والاتصال على الأداء المالي للمؤسسة الاقتصادية دراسة حالة مجمع المؤسسة الوطنية للأشغال في الآبار(E.N.T.P) ، **مذكرة ماستر**، جامعة قاصدي مرباح ورقلة: كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، تخصص مالية المؤسسة، 2013/2012.

41. دري وردة، استخدام تكنولوجيا المعلومات وتأثيرها على وظائف المؤسسة دراسة حالة مؤسسة اتصالات الجزائر وحدة ورقلة، **مذكرة ليسانس**، جامعة قاصدي مرباح ورقلة: كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، 2013/2012.

42. طويهري فاطيمة، استخدام تكنولوجيا المعلومات والاتصال أداء الموارد البشرية في المؤسسة الجزائرية دراسة حالة شركة انتاج الكهرباء بتيارت، **مذكرة ماجستير**، جامعة وهران 2، كلية العلوم الاقتصادية والتجارية وعلوم التسيير.

43. حسين العلمي، دور الاستثمار في تكنولوجيا المعلومات والاتصالات في تحقيق التنمية المستدامة دراسة مقارنة بين ماليزيا تونس والجزائر، **مذكرة ماجستير**، جامعة فرحات عباس سطيف كلية العلوم الاقتصادية والتجارية وعلوم التسيير، تخصص إدارة أعمال وتنمية مستدامة، 2013/2012.

44. فادن عالية، أثر تكنولوجيا المعلومات والاتصال في اتخاذ القرارات الاستراتيجية دراسة حالة مطاحن الزيبان بسكرة، **مذكرة ماستر**، جامعة محمد خيضر بسكرة:كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، 2015/2014.

45. شادلي شوقي، أثر استخدام تكنولوجيا المعلومات والاتصال على أداء المؤسسات الصغيرة والمتوسطة بولاية الجزائر، **مدكرة ماجستير**، جامعة قاصدي مرباح ورقلة: كلية العلوم الاقتصادية، قسم العلوم الاقتصادية، تخصص تسيير المؤسسات الصغيرة والمتوسطة، 2008/2007.

46. خالد ياسين الشيخ، أمن نظم المعلومات والرقابة، **مذكرة ماجستير**، جامعة دمشق، المعهد العالي للتنمية الإداري، تخصص التأهيل والريادة والإدارة والإبداع، 2015/2014.

47. منصور بن سعيد القحطاني، مهددات المن المعلوماتي وسبل مواجهتها، **رسالة ماجيستير**، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الإدارية، 2008.

48. عبد الرحمان شارع العتيبي، دور الامن السيبيراني في تعزيز الامن الإنساني، **مذكرة ماجستير**، جامعة نايف للعلوم الأمنية: كلية العلوم الاستراتيجية، قسم الامن الإنساني، 2015.

49. أيمن محمد فارس الدنف، واقع إدارة امن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها، **مذكرة ماجستير**، جامعة غزة الإسلامية: كلية التجارة، قسم إدارة الاعمال، 2013.

50. محمد رنيف مسعد، فاعلية تضمين سياسات أمن المعلومات، في تامين مراحل بناء وتطوير الأنظمة المعلوماتية السعودية دراسة تحليلية، **رسالة ماجستير** في العلوم الاستراتيجية، جامعة نايف للعلوم الأمنية: كلية العلوم الاستراتيجية قسم الدراسات الاستراتيجية، 2013.

و. الملتقيات والندوات:

51. نادية أمين محمد علي، الفيروسات وطرق الوقاية منها كأمن البيانات، **المؤتمر الدولي لأمن المعلومات الالكترونية، معا نحو تعامل رقمي امن**، سلطنة عمان، 2005.

52. الشريف بوفاس وفاطمة الزهراء طلحي، نحو بناء نظم لإدارة حماية المعلومات **ISO27001** في المؤسسات الجزائرية، **المؤتمر الدولي الثاني للذكاء الاقتصادي حول اليقظة الاستراتجية ونظم المعلومات في المؤسسة الاقتصادية**، جامعة باجي مختار عنابة، 2014.

ز. المواقع الالكترونية:

- https://www.wikipedia.org/
- https://www.internet-gov.sa/
- https://www.syr-res.com/
- https://www.ianswer4u.com/
- https://www.algerietelecom.dz/
- http://www.marianowo.org/

فهرس المحتويات

فهرس المحتويات:

فهرس المحتويات:

قائمة الأشكال والجداول

قائمة الأشكال والجداول:

أ. قائمة الأشكال:

ب.قائمة الجداول:

الملخص:

ان ظهور وانتشار التكنولوجيات الحديثة وازدياد اعتماد المؤسسات والحكومات عليها، بات يؤكد أهمية موضوع الامن المعلوماتي، لاعتباره الأداة الفعالة للحفاظ على سرية وسلامة المعلومات.

ان الهدف من هذه الدراسة هو التعرف على امن المعلومات وإبراز مختلف المصطلحات والمفاهيم المرتبطة به، ومن تم عرض مختلف مهدداته والإجراءات والتقنيات الحديثة لتأمينه وهذا استنادا على العديد من التقارير الأمنية الصادرة من منظمات وشركات رائدة في المجال التقني، وأخيرا حاولنا اسقاط ما تطرقنا اليه في الجانب النظري على الجانب التطبيقي من خلال دراسة حالة لمؤسسة اتصالات الجزائر–سعيدة–.

الكلمات المفتاحية: تكنولوجيا المعلومات والاتصالات – أمن المعلومات – المهددات – تقنيات الحماية – مؤسسة اتصالات الجزائر.

Résumé :

L'émergence et la prolifération des nouvelles technologies Confirme L'importance de la sécurité informatique comme un outils très important et très efficace pour préserver la confidentialité et l'intégrité des informations.

Le but de cette étude est de définir la sécurité de l'information et de mettre en évidence les différents termes et concepts qui sont associés à ce domaine, on a présenté les déférentes menaces de la sécurité informatique et les différentes procédures et techniques modernes pour le sécuriser, cela été basé sur des rapports de sécurité très recentres Publié par des organisations et des entreprises leaders dans le domaine technique, Enfin, on a essayé de faire ressortir ce que nous avons abordé théoriquement sur le plan pratique à travers une étude de cas dans l'entreprise Algérie Telecom -Saida-.

Mots clés : Technologies de l'information et de la communication - Sécurité de l'information - Menaces - Techniques de protection – Entreprise d'Algérie Télécom.

Abstract :

The emergence and proliferation of new technologies Confirms The importance of information security as a very important and highly effective tool to preserve the confidentiality and integrity of information. as a very important and very effective tool for preserving the confidentiality and integrity of informations.

The Objective Behind this study is to define the security of information and to highlight the different terms and concepts that are associated with this domain, we presented the different threats of Information security and the different modern procedures and techniques to secure it, this was based on very recent security reports Published by leading organizations and companies in the technical field, Finally, we tried To bring down what we have discussed in the theoretical framework on the practical side through a case study in the company of Algeria Telecom -Saida-.

Key Words : Information and communication technologies - Information security - Threats - Protection techniques – Company of Algeria Telecom.