تحديَّات أَمن المعلومات والأَمن السيبراني في مؤسسات المعلومات

مهند محمد منيب * و سمية يونس الخفاف**

تأريخ التقديم: 2022/9/30 تأريخ القبول: 2022/10/15

المستخلص:

استهدف هذا البحث التعرُّف على التحديَّات المتعلِّقة بأَمن المعلومات والأَمن السيبراني، وقد تمثَّلت هذه التحديات في التحديات الطبيعية، مثل: الزلازل والأعاصير والفيضانات والنيران وارتفاع درجات الحرارة والرطوبة، والتحدِّيات البشرية وتتمثل بالأَعمال التخريبية الَّتي يقوم بها الأَفراد سواء كانت بطرائق مقصودة أَم جرائم المعلومات، وتكون بنشر المعلومات السريَّة الَّتي حصلنا عليها بطرائق غير مشروعة، والثغرات وهي عبارة عن نقاط الضعف التي توجد أَثناء عملية التصميم أَو تهيئة البرمجيات وقواعد تخزين المعلومات أَو الأَجهزة التي تحفز بها المعلومات ومعدات وبرامج تشغيل الشبكات التي بها يستطيع المهاجم أَن يتسلل لأحداث ما يريده من عمليات تخريب، فضلًا عن إِمكانية التشويش ويتم بمعدات مخصَّصة لعمل التشويش أَو قد يكون التشويش ناتج عن بعض العوامل والظروف الطبيعية غير المقصودة، واستخدم الباحثان المنهج الوصفي وكانت أَبرز النتائج التي توصَّلوا إِليها استخدام تقنية جدار النارFIREWALL في حماية المعلومات يقلل من خطر التحديات والتهديدات التي تطلق باتجاه مؤسسات المعلومات عدم إِجراء التحديثات لبرامج مكافحة الفايروسات بصورة دورية لخادم الشبكة وجميع محطات العمل المستخدمة في مؤسسات المعلومات يؤدِّي لتعرض المعلومات للفايروسات في أَي وقت, وتواجه الكثير من مؤسسات المعلومات تحديات أَمنية عديدة مثل التحديات البشرية بقصد أَو غير قصد وأَخطاء فنية وتحديات طبيعية كالزلال والفيضانات, يعدُّ الخطأ والسهو عند

* طالب ماجستير/قسم المعلومات وتقنيات المعرفة/كلية الآداب/جامعة الموصل.

** أُستاذ مساعد/قسم المعلومات وتقنيات المعرفة/كلية الآداب/جامعة الموصل.

الموظفين من أكثر التحديدات التي تواجهها مؤسسات المعلومات ويعد التدريب المستمر والجيد من أفضل أساليب الحماية الأمنية للمعلومات.

الكلمات المفتاحية: أمن المعلومات– الأمن السيبراني– تحديات أمن المعلومات.

1- المقدّمة:

يعيش العالم اليوم في عصر سيطر عليه توظيف التكنولوجيا، وصار العالم يشهد ثورة تكنولوجية امتدت لجميع مجالات الحياة، ومع التطور التكنولوجي ودخول نظم المعلومات لجميع مجالات الحياة العسكرية والاقتصادية، والطبية، والتعليمية، ومع توظيف شبكات الإنترنت العالمية في تبادل ونقل هذه المعلومات، الَّتي قد تكون في بعض الأحيان على درجة عالية من السرية والخطورة؛ ونتيجة لهذه الطفرة التي حدثت في وسائل الاتصال، وشبكات نقل المعلومات ظهرت مخاطر وتهديدات جديدة لم تكن معروفة من قبل، الأمر الذي أدى للبحث عن سبل حماية هذه المعلومات وتوفير أقصى درجات الحماية لها ، ومن هنا بدأ الاهتمام بمصطلح أمن المعلومات والأمن السيبراني، الذي صار ضرورة لا غنى عنها في مؤسسات المعلومات المختلفة للحفاظ على خصوصية وسرية معلوماتها وبياناتها, تشير الأبحاث الحديثة إلى أنَّ مؤسسات المعلومات تحتل المرتبة الثالثة في انتهاكات البيانات، فضلًا عن ذلك فقد أشار تقرير الأمن السيبراني المؤسسي لعام 2021 إلى أنَّ انتهاكات البيانات كانت المصدر الرئيسي للمخاطر بالنسبة لمؤسسات المعلومات لا ينبغي أن يكون ذلك مفاجأة مع المزيد من المؤسسات التي تضع العمليات القديمة بالتحول الرقمي والمزيد من المستخدمين لتكنولوجيا المعلومات والتوسع في استخدام البيانات والمعلومات وخزنها واسترجاعها وتبادلها لذلك فإنَّني في هذه الدراسة سوف أسعى إلى التعرف على مفهوم أمن المعلومات، والأمن السيبراني، والفرق بينهما، والتحديات التي تواجه أمن المعلومات والطرائق المتبعة من المؤسسات لمواجهة الهجمات السيبرانية وحماية بياناتها.

2-مشكلة الدراسة:

إنَّ حماية المعلومات في عصر العولمة صار أَمرًا بالغ الأهمية لضمان استمراريه الاعمال؛ إذ ان عمليه التصدي للتهديدات الأَمنية لنظام المعلومات صار تحدي يواجه العديد من مؤسسات المعلومات خاصة في ظل الاستخدام المكثف والمستمر لتكنولوجيا المعلومات؛ إذ ان الكثير من مؤسسات المعلومات تحتفظ ببيانات ومعلومات على درجة عالية من السرية لذلك تواجه المعلومات مجموعة من التحديات مثل السرقة والاختراق والتلاعب والفقدان وعلى مؤسسات المعلومات تركيز الجهود لحماية هذه المعلومات من مجرمي الإنترنت وانطلاقًا مِمَّا تقدم تسعى الدراسة للإجابة على الأَسئلة البحثية الآتية:

1-ماهو مفهوم أَمن المعلومات ؟.

2-ماهي أَهميَّة وعناصر أَمن المعلومات؟.

3-ماالمقصود بالأَمن السيبراني ؟.

4-ماهو الفرق بين أَمن المعلومات والأَمن السيبراني ؟.

5-ماهي أَبرز التحديات التي تواجه أَمن المعلومات في مؤسسات المعلومات ؟

3-أَهداف الدراسة :

1- التعرف على مفهوم أَمن المعلومات والأَمن السيبراني.

2- التعرف على الفرق بين أَمن المعلومات والأَمن السيبراني.

3- التعرف على التحديات التي تواجه أَمن المعلومات في مؤسسات لمعلومات.

4- التعرف على أَبرز التدابير الأَمنية لحماية أَمن المعلومات .

4-أَهميَّة الدراسة:

تنبع أهمية الدراسة من عاملين أَساسيين أَوَّلهما تحديد التحديات الأَمنية التي تواجه مؤسسات المعلومات وثانيهما قلة البحوث والدراسات المرتبطة بحماية أَمن المعلومات على حد علم الباحثين، والبحث قد يكون ذات فائدة كبيرة لمؤسسات المعلومات بنتائجه ووضع الحلول المناسبة للتغلب على التحديات التي تستنزف عمل المؤسسات بصورة شبه يومية.

5-منهج الدراسة:

اختار الباحثان المنهج الوصفي بما يتلاءم مع طبيعة هذه الدراسة والوصول إِلى نتائج بالاطِّلاع على ادبيات الموضوع بصورة شاملة .

5-حدود الدراسة:

1-الحدود الموضوعية/تحديات أَمن المعلومات والأَمن السيبراني في مؤسسات المعلومات.

2-الحدود الزمانية /العام الدراسة 2022-2023.

6-الدراسات السابقة:

1- دراسة أسماء، فيلالي، وعبد اللطيف شليل. تهديدات أَمن المعلومات وسبل التصدي لها، مجلة البشائر، مج4،ع3، 2018.

هدفت هذه الدراسة إِلى تحديد تهديدات أَمن المعلومات وسبل التصدي لها، وتكمن أهمية هذه الدراسة في كونها تقدم حلول عملية يمكن أن تساهم في زيادة أَمن المعلومات بوجود منظومة متكاملة مكونة من عناصر مادية تتمثل في المواقع والأَجهزة الضرورية لاحتواء المعلومات، وعناصر مادية تتمثل في العناصر التقنية هي البرامج والتطبيقات الضرورية، وأهم عنصر في الحماية وهو العنصر البشري الذي يمثل في نفس الوقت تهديد أَو ثغرة أمنية، وقد استخدم الباحثان المنهج الوصفي في دراستهما، وقد توصلت دراستهما إِلى مجموعة من الاستنتاجات مفادها أَنَّ التهديدات التي تصل أنظمة المعلومات تتطور باستمرار، ومن الصعب السيطرة عليها باتباع سبل الحماية التقليدية، أكثر التهديدات خطورة تأتي من داخل المؤسسة وهي تغطي النسبة الأكبر من التهديدات، أن أَمن المعلومات اليوم هو ضرورة حتمية ليس مجرد رفاهية، وأن عملية الحماية هي عمليه متكاملة تشمل المكونات المادية والبرمجية والعنصر البشري. [1]

[1] - فيلالي, اسماء، شليل عبد اللطيف . تهديدات امن المعلومات وسبل التصدي لها0- مجلة البشائر الاقتصادية, مج4,ع3 ,2019 :ص20

2-دراسة علوطي لمين .تحديات الأَمن الإلكتروني في المؤسسة .مجلة ابحاث اقتصادية وادارية ,ع6, 2009.

هدفت الدراسة إلى اظهار أَبرز المفاهيم المتعلقة بالأَمن الإلكتروني وسبل تحقيقه في مؤسسات المعلومات مع الاستخدام المتزايد لتكنولوجيا المعلومات مع تشخيص المشاكل الأَمنية والعمل على إيجاد الحلول المناسبة لها وقد اتبع الباحث المنهج الوصفي التحليلي هذا وقد توصلت الدراسة إلى مجموعة من النتائج كان من اهمها ضرورة حماية المعلومات الحساسة في المؤسسات باستخدام منظومة متكاملة تضم حماية المكونات البرمجية والمادية والتنبه عند التعامل مع العنصر البشري وان أَمن مؤسسات المعلومات ضرورة حتمية من أَجل استمرار المؤسسات للقيام بمهامها وان الغالبية العظمى من التهديدات تأتي من الداخل فضلًا عن ان الهجمات الإلكترونيَّة في تطور مستمر ومن الصعب السيطرة عليها عند استخدام الأَساليب التقليدية القديمة [1] .

3-دراسة ياسمين,بلعسل بنت نبي ,عمروش الحسين. التهديدات الإلكترونيَّة والأَمن السيبراني في الوطن العربي. مجلة نوميروس الاكاديمية,مج2,ع2 ,2021

هدفت الدراسة إلى توضيح مجمل التحديات والتهديدات السيبرانية التي تنتج عن الفضاء الإلكتروني إذ يُعَدُّ هذا الموضوع من المواضيع المهمة على الساحة الدولية بسبب كثرة الصراعات والتجاذبات على المستوى المحلي والاقليمي والدولي وقد استخدم المنهج الوصفي والمنهج التاريخي للإلمام بالموضوع والوقوف على التحديات التي تواجه المنطقة العربية والعمل على تعزيز أَمنها السيبراني ومن أَبرز النتائج التي توصلت إليها الدراسة تعرف التهديدات الإلكترونيَّة على انها استغلال تكنولوجيا المعلومات في تدمير وتخريب البنية التحتية المعلوماتي للخصم واختراق انظمة المعلومات والبريد الإلكتروني لمؤسسات المعلومات والمنظمات ورؤساء الدول والتجسس عليهم وفق خطط عمل ممنهجة, بهدف مكافحة الجرائم المعلوماتية عملت العديد من الدول العربية على تفعيل الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

[1] - لمين ,علوطي.تحديات الامن الالكتروني في المؤسسة 0- مجلة ابحاث اقتصادية وادارية .ع6, 2009:ص45

وقد تم ذلك بتاريخ 2010/12/21كما توصلت الدراسة إلى ان الفضاء السيبراني مجال جديد للصراعات بين الاطراف سواء بين الدول والمؤسسات أم الأفراد إذ تبلورت الحروب السيبرانية في خصائص ليس لها علاقة بالحروب التقليدية [1].

وقد اختلفت هذه الدراسة عن الدراسات الأُخرى إذ اشارت الدراسة إلى تفصيل اكثر عن موضوع أمن المعلومات والأمن السيبراني وحصر الأنواع المختلفة من التحديات التي تواجه عملية حماية المعلومات في القرن الحادي والعشرين وتأثيرها على مؤسسات المعلومات الامر الذي قد يؤدي إلى تعطيل عمل ونشاط تلك المؤسسات وتكبدها خسائر فادحة؛ لذلك صار من الضروري على المؤسسات الإلمام بالطرائق والأساليب الحديثة المتبعة في حماية المعلومات كون الأساليب القديمة المتوافرة وقفت عاجزة أمام تحديات أمن المعلومات .

اولا أمن المعلومات

1-تعريف أمن المعلومات:

لأمن لمعلومات مفاهيم عديدة وإن اختلفت من حيث الشكل لكنَّها تتفق من حيث المضمون, فقد عرف أمن المعلومات بأنَّه(1) حماية الموارد المستخدمة في معالجة المعلومات، إذ يتم تأمين المؤسسات والأفراد والعاملين فيها، وأجهزة الحاسوب، ووسائط المعلومات التي تحتوي على بيانات ومعلومات المؤسسة[2]

(2)وأيضًا يعرف أمن المعلومات بأنه مجموعة من الطرائق والوسائل المعتمدة للسيطرة على كل أنواع ومصادر المعلومات وحمايتها من السرقة، والتشويه والابتزاز، والتلف، والضياع، والتزوير، والاستخدام غير المرخص وغير القانوني.[3]

---

[1] – ياسمين,بلعسل بنت نبي,عمروش الحسين.التهديدات الالكترونية والامن السيبراني في الوطن العربي0- مجلة نوميروس الاكاديمية ,مج2,ع2, 2021:ص60

[2] – باجحزر، أبرار، والعمري، أحمد، أمن المعلومات في البطاقات الذكية، التحديات الجيوفيزيائية، والاجتماعية والإنسانية في بيئة متغيرة، المؤتمر العلمي الدولي العاشر، إسطنبول- تركيا،2019، ص50

[3] – بن جمعة، جمعة بن علي، الأمن العربي في عالم متغير،القاهرة: مطبعة مدبولي، 2010,ص8

(3)أيضًا يتم تعريف أمن المعلومات (المعروف أيضًا باسم Info Sec) على أنه "حماية المعلومات وأنظمة المعلومات من الوصول غير المصرح به أو الاستخدام أو الكشف أو التعطيل أو التعديل أو التدمير من أجل توفير السرية والنزاهة والتوافر[1]".

ويعرف الباحثان أمن المعلومات بأنها مجموعة الوسائل المادية والبرمجية التي تتبناها مؤسسة ما للحفاظ على سرية معلوماتها وخصوصيتها من التلف أو السرقة أو النشر العام ومن ثُمَّ بالتعريفات السابقة يتضح للباحثين أن الحفاظ على أمن المعلومات هو مهمة معقدة لا يمكن أن تتم باتخاذ تدابير تقليدية، أو عادية بل تحتاج إلى مُعدَّات خاصة وأنَّ هذه التعريفات تعكس أهمية أمن المعلومات بالنسبة للمؤسسة، وللأفراد على حد سواء.

2-مراحل تطور مفهوم أمن المعلومات:

مر مفهوم أمن المعلومات بعدة مراحل انتقل فيها من مفهوم أمن الحواسيب إلى أمن المعلومات الَّذي لازال يستخدم في الوقت الحاضر وقد صنف الحميدي واخرون مراحل تطورات هذا المفهوم إلى ثلاث حقب زمنية تمثلت بما يأتي :

- المرحلة الأُولى / مرحلة الستينات وفي هذه المرحلة كانت أجهزة الحواسيب هي كل ما يشغل العاملين في حقل تكنولوجيا المعلومات فضلًا عن تعلم كيفية تنصيب البرامج ولم يكن العاملون في ذلك الوقت مشغولون بأمن المعلومات بقدر انشغالهم بعمل الأجهزة وقد كان موضوع الأمن في تلك المُدَّة يدور حول تحديد الوصول والاطِّلاع على البيانات والعمل على منع أي جهة خارجية من التلاعب في الأجهزة ومن هنا ظهر مصطلح أمن الحواسيب الَّذي يعني حماية الحواسيب وقواعد بياناتها .
- مرحلة السبعينات / في هذه المرحلة تم الانتقال إلى مفهوم أمن البيانات واهم ما يميز هذه المرحلة هو استخدام كلمات السر البسيطة للسيطرة على الوصول إلى البيانات فضلًاعن إلى استحداث إجراءات امنية لحماية مواقع الحواسيب من

[1] Golden,Mathew, The Handbook of Information Security for Advanced Neuroprosthetics, Second EditionPublisher: Synthypnion Academic, 2017, p44

الكوارث وقد رافق ذلك اعتماد خطط لتخزين نسخ اضافية من البيانات والبرمجيات بعيدا عن مواقع الحواسيب[1] .

- مرحلة الثمانينات والتسعينات / في هذه المرحلة تم الانتقال فعليًا إلى مفهوم أَمن المعلومات بسبب التطورات الهائلة في مجال تقنيات المعلومات الَّتي سمحت للمستخدمين من سهولة الوصول إلى قواعد البيانات فصار من الضروري الحفاظ على أَمن وسلامة المعلومات وتكاملها وتوفير درجة عالية من الموثوقية وهو المفهوم الذي سيتم التحدث عنه في هذا البحث[2] .

3-أهمية أَمن المعلومات:

زادت أَهميَّة أَمن المعلومات مع استمرار الانفجار المعلوماتي الَّذي يستوجب توفير حماية متعددة الجوانب الَّتي قد تكون معرضة للتهديد والاستهداف والاختراق أَو التخريب أَو التدمير في أَي قت بصورة مباشرة أَو غير مباشرة[3] وعليه يمكن تحديد أَهميَّة أَمن المعلومات في النقاط التالية:

- العديد من مؤسسات المعلومات تعتمد على صحة ودقة معلوماتها.
- الحاجة المتزايدة لتطبيق إِجراءات امنية معلوماتية تغطي المخاطر والتهديدات التي قد تظهر عن التعامل مع الأَطراف الأُخرى.
- الحاجة لحماية البنية التحتية لمؤسسات المعلومات من أَجل الاستمرار في العمل.
- الحاجة لبناء بيئة إِلكترونيَّة مؤمنة تخدم مؤسسات المعلومات.
- مع تطور تقنيات المعلومات وازدهارها توفرت فرص الإِجرام الإِلكتروني [4].

---

[1] – الحميدي واخرون .نظم المعلومات الادارية 0 مدخل معاصر, عمان: دار وائل للنشر 2005,:ص265

[2] – ان سعيد ابراهيم عبد الواحد . سياسات أمن المعلومات وعلاقتها بفاعلية نظم المعلومات الإدارية في الجمعات الفلسطينية 0– رسالة ماجستير .جامعة الازهر .كلية الاقتصاد والعلوم الادارية 2015.:ص15

[3] – اليحاوي 'يحيى .في القابلية على التواصل–التواصل على محك الانترنيت وعولمة' المعلومات, منشورات عكاظ 201:ص84

[4] – نهاد عبد اللطيف عبد الكريم، خلود هادي الربيعي.أمن و سرية المعلومات و أثرها

4- أهداف أمن المعلومات:

يُعَدُّ أمن المعلومات من الركائز الضرورية التي تعتمد عليها حماية الدول واقتصاديات الدول والمنظمات والمؤسسات والأفراد من الاضرار الناتجة عن وجود قصور للأمن وأنَّ الهدف الأساسي لأمن المعلومات هو الحفاظ على سلامة وحماية المعلومات الَّذي من شأنه أن يقلِّل من حالات الاختراق ومنع الدخول غير المصرح به ومن ثُمَّ تامين عدم حدوث أي خسائر في المنظومة المعلوماتية [1] ويمكن ايجاز أهداف أمن المعلومات التي حددها المركز القومي لأمن المعلومات بالنقاط التالية :

- **حماية المعلومات/ وتعني حماية خصوصية المعلومات الخاصة بمؤسسات المعلومات والأفراد ويسعى القائمون على عملية أمن المعلومات توفير الحماية التامة وتشمل حماية الأجهزة بالعمل على تحديث إجراءات الأمن وبشكل دوري مع تامين السبل الكفيلة التي من شانها توفير الإطار العام لأمن وحماية المعلومات .**
- **تكامل البيانات والمعلومات /وتعني توفير الحماية الكاملة لأمن وحماية البيانات والمعلومات بالعمل على المحافظة عليها ضد حالات الاختراق والوصول غير المصرح به وكذلك الحفاظ عليها من عمليات التغيير والتبديل والتعديل من الأشخاص المخولين لهم بالدخول إليها ولأيتم تحقيق التكاملية الأمن في توفر الأساليب والإجراءات الكفيلة والضامنة للحماية المعلوماتية .**
- **اتاحة الخدمة/ وتعني القدرة على الحصول على المعلومات بطرائق سهلة عند الحاجة إليها ومن ثُمَّ فإنَّ المستخدمين يجب أن لا يواجهون أي صعوبات عند تعاملهم مع المعلومات مع ضرورة توفير إجراءات احترازية تضمن عدم تعرض المعلومات لأي هجمات واعتداءات ناتجة عن عومل داخلية أو خارجية أو تعرض المنظومة لأي خلل طارئ يمكن ان يلحق بالأضرار بأمن وسلامة البيانات والمعلومات.**

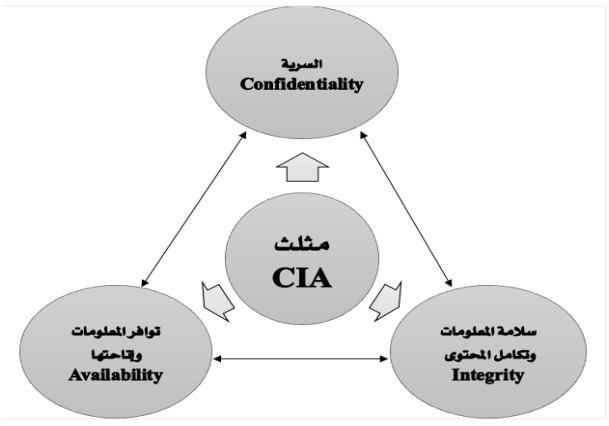
على الأداء التنافسي دراسة تطبيقية على شركتي التامين العراقية العامة والحمراء0-مجلة دراسات مالية ومحاسبية,مج8,ع28:ص297

[1] – ابو ذيوب,قتيبة عاهدمسلم .مدى الالتزام بسياسات امن وحماية المعلومات المحاسبية في البنوك التجارية .– رسالة ماجستير.جامعة ال البيت .كلية الدراسات العليا ,2019:ص5

- عدم انكار التصرف المرتبط بالمعلومات/ وتعني ضمان عدم انكار الشخص الذي قد يقوم بتصرف ما متصل بالمعلومات أَو مواقعها بحيث تتوفر القدرة على اثبات بان تصرفا معين قد تم من شخص معين في وقت معين .
- السرية والموثوقية /وتعني التأكد من ان المعلومات لا يمكن كشفها والاطِّلاع عليها بالأَشخاص المخولين بذلك .
- التحقق من الشخص المستخدم /وتعني المصادقة على هوية الأَشخاص الذين يسمح لهم بالدخول إِلى المعلومات [1].
- ويرى الباحثان أَنَّ هدف أَمن المعلومات من الصعب تحقيقه ان لم يتم حماية المعلومات ضد الوصول غير المصرَّح به والأَمن من أَي شخص يحاول الوصول إِلى المعلومات ويتم ذلك بتحديد صلاحيات الدخول والاستخدام لها كلا حسب صلاحيته الامر الذي من شانه تعزيز أَمن المعلومات.

5-عناصر أَمن المعلومات:

يعتمد أَمن المعلومات على ثلاثة عناصر أَساسيَّة لابدَّ من توافرها في المعلومات الواجب حمايتها وهي السرية **Confidentiality** وسلامة المعلومات وتكامل محتواها **Integrity** وتوافر المعلومات واتاحتها **Availability** الَّتي تعرِّف بمثلث **CIA** وسوف نتكلم عنها بشيء من التفصيل والشكل رقم واحد يوضح ذلك:



شكل رقم (1) عناصر أَمن المعلومات

[1] -- امينة ,قدايفة .استراتيجية امن المعلومات0-مجلة ابعاد اقتصادية,2016:ص165

– السرية Confidentiality/ أي القدرة على الحفاظ على خاصية سرية المعلومات بمنع الدخول غير المصرح للمعلومات بغض النظر عن وسائط التخزين المتوفرة سواء كانت هذه الوسائط مادية أَم يتم خزنها عبر وسائل الاتصال الإلكترونيَّة والتأكد عدم الافصاح عنها فضلًا عن التأكد من عدم الوصول إليها إلَّا من الأَشخاص المخولين المصرح لهم بذلك.

– سلامة المعلومات وتكامل محتواها Integrity/اي التأكد من الحفاظ على محتوى المعلومة نفسها وعدم تعرضها للعبث والتعديل والتخريب والنسخ والتغيير ويمكن تحقيق ذلك عن طريق منع الوصول إلى المحتوى.

– توافر المعلومات واتاحتها Availability/تعني ضمان توافر المعلومات والقدرة على إتاحتها وتقديمها لمن يطلبها في الوقت المناسب والتأكد من أَنَّ الأَشخاص الذين بحاجة إلى هذه المعلومة لم يتم منعهم من الوصول إليها [1].

ثانيًا: الأَمن السيبراني:

1–تعريف الأَمن السيبراني:

الأَمن في معجم المعاني مأخوذ من الفعل أَمن وهو يعني الاطمئنان فهو يعني الطمأنينة وعدم الخوف أَمَّا الأَمن في الاصطلاح فهو يعني القدرة التي تمكن الدولة من إطلاق مصادر قوتها الداخلية والخارجية في شتى المجالات لمواجهة أَي خطر قادم من الداخل أَو الخارج في السلم والحرب.[2] أما كلمة سيبرانية أَو سايبر أَو سيبراني تعتبر ترجمة حرفية للكلمة الانجليزية cyber وهي مشتقة من الكلمة cybernetics واستخدم هذا المفهوم لأول مرة من عالم الرياضيات الامريكي نوربرنت وينر عام

---

[1] -- John M. Broky, Thomas H. Bradley. Protecting Information with Cybersecurity, Berlin: Springer International Publishing AG, 2019, Pp. 350-351, Available At: http://08102q3xn.1104.y.https.link.springer.com.mplbci.ekb.eg/content/pdf, Access Date: 15/9/2022

[2] – المطيري, خالد ظاهر.التشريعات الجزائية في حماية الأمن السيبراني لدول مجلس التعاون الخليجي.– مجلة البحوث الفقهية والقانونية, ع38, 2022:ص993

١٩٤٨، ويُعَدُّ مصطلح كلمة سايبر دخيل على معجم اللغة العربية فلا يوجد مصطلح مقارب له ولكن ورد معنى هذه الكلمة في قاموس المورد الحديث تحت مسمى "الكمبيوتري " أَو العصري وورد فيه مصطلح سيبراني بأَنَّه علم الضبط أَو علم التحكم الأوتوماتيكي[1] أَمَّا بالنسبة للأمن السيبراني فهو يعني بكل شيء يتم ربطه بالشبكات الإلكترونيَّة والإنترنت، اذن نجد ان الأَمن السيبراني **cyber security** هو: الحماية المتكاملة للأشياء باستخدام وسائل تكنولوجية ومعلوماتية بين الأَجهزة والبرمجيات وهو يتمثل بمجموعة الإجراءات التي توفر نظام الحماية للفضاء السيبراني من أَي هجمات بالوسائل التقنية والتنظيمية والادارية التي تمنع الوصول للمعلومات الإلكترونيَّة بطرائق غير مشروعة أَو استغلال المعلومات بطرائق غير قانونية أَو نظامية من أَجل الحفاظ على استمرارية أنظمة المعلومات وحمايتها بكل خصوصية وسرية [2]. والأَمن السيبراني بحسب وزارة الدفاع الأَمريكيَّة يعني ذلك المجال العالمي الذي يتضمن بيئة المعلومات ويتكون من شبكات مترابطة للبنى التحتية لتكنولوجيا المعلومات والبيانات ويشمل أَيضًا الإنترنت وشبكات الاتصالات وانظمة الكمبيوتر والمعالجات وأَجهزة التحكم المدمجة.[3] وبعد استعراض التعريفات السابقة يمكن تعريف الأَمن السيبراني اجرائياً من الباحثين بأَنَّه مجموعة الإجراءات المتبعة لحماية بيئة المعلومات بشكل عام بكل ما تحتويه من شبكة إنترنت وحواسيب وخوادم وبرمجيات حماية متكاملة ضد الهجمات السيبرانية.

2-الفضاء السيبراني:

أطلق عليه البعض مسمى اليد الرابعة للجيوش وهناك من اعطاه مسمى البعد الخامس لا يوجد تعريف ثابت وموحد لمصطلح الفضاء السيبراني نتيجة لاختلاف طبيعة ونظام

---

[1] – موصلي, نور أمير. الهجمات السيبرانية في ضوء القانون الدولي الانساني .– رسالة ماجستير الجامعة الافتراضية السورية، سوريا، ٢٠٢١: ص8

[2] – السمحان، منى عبد الله. متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود0– مجلة كلية التربية، جامعة المنصورة، ع111, 2022: ص14

[3] – حارك، فاتح.الفضاء السيبراني والتحول في شكل الحروب.المؤتمر الافتراضي الاول ,2021:ص7

كل دولة فنجد أن البعض عرفه على أنه علم افتراضي متداخل مع العالم المادي ويؤثران ببعضهما بطرائق غير مباشرة بعلاقة تكاملية ويتكون الفضاء السيبراني من أجهزة الحاسوب وشبكة المعلومات.[1] والفضاء السيبراني أيضًا هو مجال افتراضي من صنع الانسان يعتمد على انظمة الحاسوب وشبكات الإنترنت وهو عبارة عن بيئة تفاعلية حديثة وتشمل على عناصر مادية وغير مادية فهو يعتمد على أجهزة رقمية وانظمة الشبكات والبرمجيات.[2] والفضاء السيبراني أيضًا هو البيئة الإلكترونيَّة غير الملموسة والمعقدة التي يتم بها بناء نماذج لظواهر أو صور إلكترونيَّة وظواهر شبه حقيقية في التفاعلات والتعاملات البعيدة فهو يشمل شبكة إلكترونيَّة تتكون من مجموعة خوادم إلكترونيَّة تتفاعل هذه الشبكات (تحتوي على قواعد بيانات) مع بعضها بعضًا بوسائل اتصال افتراضية فتتجاوز كل الحدود الجغرافية والسياسية لتحسين القدرة على الاتصال والتعامل الإلكتروني.[3]

3-الهجوم السيبراني cyber Attacks:

لا يوجد مفهوم عام وشامل للهجوم السيبراني نتيجة لاختلاف المواقف الدولية في مواجهة الهجمات السيبرانية والهجوم السيبراني وفق المركز الديمقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية هو الاستخدام المتقن للطاقة لمواجه أفراد أو مؤسسات من أجل اضعاف قدرة المستهدف وهو أيضًا عبارة عن مجموعة الرسائل التي يرسلها المهاجمون مما يسبب في تعطيل مفاعل نووي أو انقطاع تيار كهربائي أو ايقاف المرافق الصحية وانظمة المطارات للسيطرة على موارد الدولة

[1] – حميد، عبد الوهاب كريم، الامن السيبراني والقيود والتحديات في ضوء قواعد القانون الدولي0- مجلة العقد الاجتماعي.مركز البحوث القانونية في وزارة العدل في اقليم كردستان العراق ،٢٠٢١:ص٣١٥

[2] – زروقة، اسماعيل. الفضاء السيبراني والتحول في مفاهيم القوة والصراع.0- مجلة العلوم القانونية والسياسية ,مج10,ع1, 2019 :ص1017

[3] – كلاع، شريفة . الأمن السيبراني وتحديات الحوسبة والاختراقات الالكترونية للدول عبر الفضاء السيبراني,جامعة الجزائر ,مج15,ع1 ,2022:ص294

المستهدفة وتدمر اقتصادها.[1] لذلك نجد ان التعاريف التي تناولت مفهوم الهجوم السيبراني اشتركت في معنى متقارب وهو استهداف للمواقع الإلكترونيَّة أَو لنظام كمبيوتر أَو جهاز كمبيوتر بوسائل اتصال إلكترونيَّة مما يهدد سرية وسلامة المعلومات المخزنة، وتكون الهجمات من مصدر مجهول هدفه سرقة المعلومات أَو تدمير هدف معين باختراق نظام حساس[2]. والهجمات السيبرانية أَيضًا هي فعل يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض شخصي أَو سياسي باستغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام ويكون الهدف منها سرقة للمعلومات وانتهاك سريتها أَو تعديلها أَو منع الوصول إليها. [3]

4-الفرق بين الأَمن السيبراني وأمن المعلومات:

أَوَّلًا من حيث المفهوم:

الأَمن السيبراني يعني " جميع الإجراءات والتدابير والتقنيات والأَدوات المستخدمة لحماية سلامة شبكات والبرامج والبيانات من الهجوم والتلف أَو الوصول إليها بطرائق غير مشروعة لحماية الأَجهزة والبيانات.[4]

أمن المعلومات "هو مجموعة الإجراءات والتدابير المستخدمة في المجال الاداري والمجال الفني لحماية المصادر من التجاوزات أَو التداخلات غير المشروعة سواء كانت بصورة متعمدة أَم عن طريق الصدفة.

ثانيًا: من حيث الهدف:

---

[1] – سليمان علي فاضل.حق الدفاع الشرعي على الهجمات السيبرانية.مجلة جامعة تكريت للحقوق السنة الرابعة,بغداد:الجامعة العراقية ,مج4,ع4,ج1:ص35

[2] – الموصلي، نور امير، الهجمات السيبرانية في ضوء القانون الدولي الانساني، مصدر سابق، ص٧

[3] – البهي, رغدة. الردع السيبراني المفهوم والاشكاليات والمتطلبات0– مجلة الدراسات الاعلامية المركز الديمقراطي العربي,ع1, 2018:ص208

[4] – السمحان، منى عبد الله..متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود0– مجلة كلية التربية، جامعة المنصورة، ع111, 2022: ص14

الأَمن السيبراني هدفه الدفاع وحماية الفضاء السيبراني من أي هجمات سيبرانية الأَمن المعلومات الهدف هو حماية نظم المعلومات والمعلومات من الوصول أَو الاستخدام غير المشروع أَو تسريب أَو تخريب أَو تعديل والحرص على توفير السرية والنزاهة.

ثالثا من حيث النوع

الأَمن السيبراني له ثلاث انواع هي أَمن شبكات وأمن تطبيقات، وأمن معلومات امن المعلومات له ثلاث انواع أَمن يتعلق بالأَفراد، أَمن يتعلق بأَجهزة الحاسوب والمنظومات، أَمن يتعلق بنظم الاتصالات، أَمن يتعلق بأنظمة التشغيل[1]

رابعًا: الكيفية وطرائق حماية المعلومات:

أمن المعلومات يحافظ على أمان البيانات سواء كانت إِلكترونيَّة أَم مستندات ورقية وبالتالي هو أوسع من الأَمن السيبراني، والأَمن السيبراني يحمي فقط البيانات الموجودة بشكلها الإِلكتروني والموجودة على أَجهزة الكمبيوتر والخوادم وشبكات والأَجهزة المحمولة من التعرض لأي خطر أَو هجوم قادم من الفضاء الإِلكتروني فقط.

خامسًا: عناصر الأَمن السيبراني:

الأَمن السيبراني يتكون من التقنية والأَشخاص والاستراتيجيات والأَنشطة والعمليات أَمن المعلومات عناصره الخصوصية والتوافر والسلامة للمعلومات المصرَّح بها للأَشخاص المسموح لهم فقط بالحصول عليها[2] .

سادسًا: من حيث المنطلق:

الأَمن السيبراني ينطلق بتامين الاشياء المعرضة للخطر بتكنولوجيا المعلومات والاتصالات .

---

[1] – عوض الله أحمد حسني. أثر خصائص أمن المعلومات على تحقيق التميز المؤسسي عبر قدرات التعلم التنظيمية في الجامعة الاردنية، السودان :الجامعة ,2018:ص42

[2] – سابا، غسان. أمن الشبكات والبنية التحتية المعلوماتية0– رسالة ماجستير، الجامعة الافتراضي السورية ،٢٠١٨: ص4

أَمن المعلومات ينطلق لحماية المعلومات التي تركز على سرية وسلامة وتوافر المعلومات ويرى بعضهم أَنَّ الأَمن السيبراني مجموعة فرعية عن أَمن المعلومات .

والأَمن المعلومات يحمي البيانات من أَي شكل من اشكال التهديد بينما أَمن السيبراني يعتني بحماية استخدام الفضاء الإلكتروني من الهجمات الإلكترونيَّة فهو يحمي أَي شيء موجود في عالم الإنترنت ويحمي المعلومات بغض النظر عن مكان وجودها.[1]

ثالثًا: التحديات:

1-تحديات أَمن المعلومات:

للمعلومات اهمية كبيرة؛ لأَنَّها تستخدم من الجميع كالأَفراد والمؤسسات والدول لذلك فهي هدف للاختراق وربَّما تكون الفاصل بين المكسب والخسارة للمؤسسات وفي العصر الحديث لم تكن المشكلة في طريقة الحصول على المعلومات وانما كيفية الحفاظ على أَمن وسلامة هذا الفيض من المعلومات، وقد أَدركت الكثير من مؤسسات المعلومات وجود حواجز تقييد حماية معلوماتها خاصة عندما تكون مثل هذه المعلومات ذات قيمة, نظرا للبيئة المعلوماتية المتقلبة[2] هناك مجموعة من التحديات والتهديدات الواجب علينا اخذها بنظر الاعتبار عند دراسة أَمن المعلومات والأَمن السيبراني وإيجاد الحلول المناسبة لمثل هذه التحديات :

- التحديات الطبيعية/ مثل الزلازل والأعاصير والفيضانات والنيران وارتفاع درجات الحرارة والرطوبة التي قد تؤدي إلى حدوث انقطاع في التيار الكهربائي أَو

[1] – هيئة الاعلام. الأمن السيبراني، قسم الدراسات والاتصال والعلاقات العامة، الاردن،٢٠٢١، ص ١٣

[2] – العابد,سكينة.امن المعلومات عبر شبكات التواصل الاجتماعي 0-المجلة العربية للمعلوماتية وامن المعلومات,مج1,ع1,2020:ص207

حدوث عطل في أحدى الأَجهزة والتقنيات المستخدمة في نظام أَمن المعلومات مثل توقف الخادم عن العمل أَو عطل في أحد الحواسيب وشبكات الاتصال[1] .

– التحديات البشرية/يعتمد نظام أَمن المعلومات إِلى حد كبير على نزاهة وثقافة الأَشخاص، قد لايكفي التأكد من نزاهة وكفاءة الموظف عن التعيين بل من الواجب الاشراف على اعماله ومراقبته عن كثب ويجب عن انتهاء عمل الموظف في مؤسسة ما سواء كانت الحالة انهاء خدماته أَم نقله يفترض سحب كل الصلاحيات الممنوحة له وان يتم ذلك قبل مُدَّة كافية تجنبًا حدوث تصرفات انتقامية يقوم بها الموظف المنتهية خدماته.

– التحديات الفنية /يقصد بها التحديات الناتجة بسبب القصور والأَخطاء الفنية في نظام أَمن المعلومات الَّتي يغلب عليها العامل الفني مثل الأَخطاء التي قد تحدث اثناء وبعد عمليات التجهيز والتصميم والبرمجة والاختبار وتجميع البيانات والمعلومات أَو أَخطاء في عمليات منح الوصول للمعلومات وتعتبر مثل هذه الأَخطاء الغالبية العظمة للمشاكل والتحديات المرتبطة بأمن وسلامة المعلومات.

– الجرائم الإِلكترونيَّة/تمثل الجرائم الإِلكترونيَّة تحديًا كبيرًا لأَمن المعلومات لما تسببه من خسائر كبيرة بالوصول والاستخدام والتعديل والتدمير غير المصرَّح للبيانات والمعلومات والبرمجيات والموارد المادية فضلًا عن النسخ والنشر غير المفوض للمعلومات وتقييد المستفيد من الوصول إِلى بياناته ومعلوماته[2].

ويمكن تمثيل الجرائم المعلوماتية بما يأتي :

ا–القرصنة/أَي الاختراق وهو القدرة على الوصول إِلى هدف معين(المعلومات) أَو الأَجهزة بطريقة غير شرعية وباستغلال الثغرات الموجود في نظام حماية المعلومات

[1] – الدنف، ايمن، واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها0– رسالة ماجستير في إدارة الأعمال، الجامعة الإسلامية، غزة،٢٠١٣، ص٥٧

[2] – نهاد عبد اللطيف عبد الكريم,خلود هادي الربيعي .امن وسرية المعلومات واثرها على الاداء التنافسي دراسة تطبيقية على شركتي التامين العامة والحمراء .مصدر سابق:ص294

بهدف التجسس والسرقة والاطِّلاع على خصوصيات الاخرين والحاق الضرر بهم ويطلق مصطلح(Hacker) على الشخص الذي يقوم بمثل هذه الافعال [1] .

ب- الفيروسات/بدأ ظهورها في سبعينات القرن الماضي وقد كانت درجة تأثيرها بسيطة نوعا ثم صارت أكثر تاثيرًا وخطورة نظرًا لتطور استخدام تكنولوجيا المعلومات وانتشار خدمات الإنترنت وقد وضح فيرناندو جورجيل.

ان الفيروسات هي برامج تصيب برامج أُخرى بتغييرها ونسخها مرات عديدة داخل الحاسبات الإلكترونيَّة [2] .

ج-جرائم الفضاء الرقمي /تتزايد حجم مخاطر التقنيات الرقمية الحديثة المسؤولة عن حماية المعلومات كتقنيات كاميرات الفيديو وبطاقات الدخول الإلكتروني والوصول إلى قواعد البيانات الشخصية وتقييد البريد الإلكتروني وحجب الاتصالات؛ إذ يمكن استرجاع ونقل كميات هائلة من البيانات والمعلومات المؤتمتة الشخصية التي تم جمعها من مؤسسات المعلومات في ثواني وبتكاليف قليلة الأمر الذي يكشف مدى خطورة التهديد الرقمي[3] .

د-الثغرات / الثغرات وهي عبارة عن نقاط الضعف التي توجد أثناء عملية التصميم أَو لتهيئة البرمجيات وقواعد تخزين المعلومات أَو الأَجهزة التي تخزن بها المعلومات والمعدات وبرامج تشغيل الشبكات التي بها يستطيع المهاجم أَن يتسلل لأحداث ما يريده من عمليات تخريب أَو سرقة أَو تدمير للمعلومات .

---

[1] - دخيل,احمد نوري,سعد عبد السلام طلحة.اختراقات امن المعلومات وطرق تفاديها0- المجلة الدولية المحكمة للعلوم الهندسية وتقنية المعلومات,مج2,ع2, 2016:ص20

[2] - Fernando Georgel Birleanu Peter Anghelescu, Nicu Bizon. Malicious and Deliberate Attacks and Power System Resiliency, Switzerland: Springer Nature AG, 2019, P. 230, Available At: http://08102qrbe.1104.y.https.link.springer.com.mplbci.ekb.eg/content/pdf, Access Date18/9/2022

[3] - جبوري, ندى اسماعيل0- مجلة تكريت للعلوم الادارية والاقتصادية. حماية امن انظمة المعلومات ,مج7,ع21 2011:ص77

و- خطر التشويش/ ويتم ذلك بمجموعة من العوامل التي تؤثر على إرسال واستقبال البيانات والمعلومات عن طريق شبكات المعلومات, ويكون ذلك بمعدات مخصصة لعمل التشويش أو قد يكون التشويش ناتج عن بعض العوامل والظروف الطبيعية غير المقصودة, ومن مخاطر التشويش انكار الخدمة بمجموعة من الأنشطة التي تمنع المستخدم الشرعي ان يحصل على المعلومات أو الخدمة [1] .

2-التدابير الأمنية:

إنَّ عملية حماية المعلومات من المهام الصعبة والمعقدة الَّتي تحتاج موارد مالية والكثير من الوقت والجهد وقبل الحديث عن طرائق الحماية لابد من الإشارة إلى أبرز الاسباب التي تؤدي إلى جعل المعلومات معرضة للتهديدات والاخطار:

1-ارتباط شبكة مؤسسة المعلومات الداخلية بشبكة الإنترنت العالمية .

2-التطور التقني السريع يجعل الكثير من الطرائق والوسائل المستخدمة متقادمة بعد مُدَّة قليلة من استخدامها.

3-تكاليف حماية المعلومات تكون عالية بحيث لا تستطيع الكثير من مؤسسات المعلومات خاصة في لدول النامية تحملها .

4- التأخر في اكتشاف الجرائم المعلوماتية بسبب عدم اقتناء الكثير من مؤسسات المعلومات أجهزة الانذار المبكر وتقنيات المراقبة وتوظيفها في مجال حماية أمن المعلومات.

5-قلة الوعي بأهمية أمن المعلومات.

6- قلة الكوادر البشرية المؤهلة والمدربة والمتخصصة في مجال أمن المعلومات والأمن السيبراني[2] .

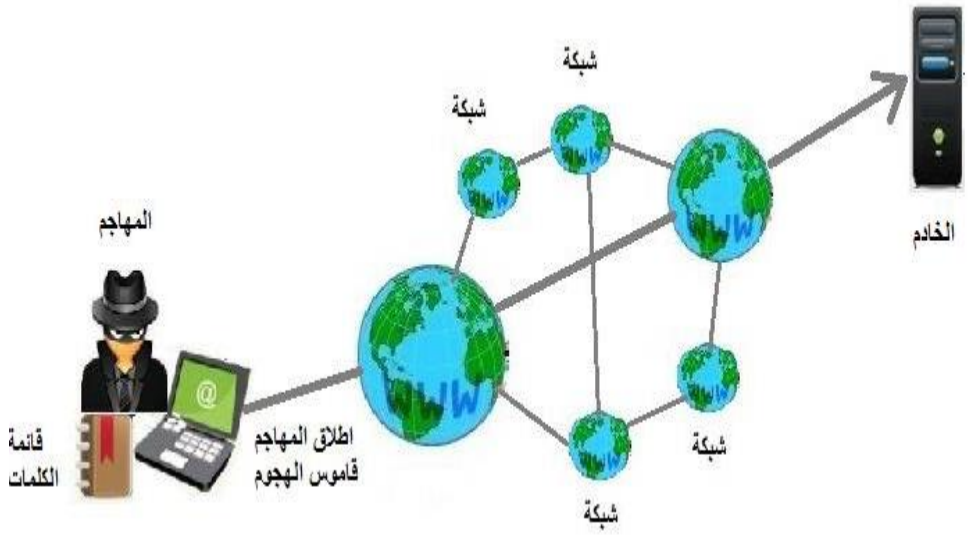
---

[1] - عوض الله احمد. أثر خصائص أمن المعلومات على تحقيق التميز المؤسسي عبر قدرات التعليم التنظيمية في الجامعات الأردنية، مصدر سابق: ص62

[2] - Labusshagne, L. & Eloff , Electronic Commerce : The Information Security Challenge", Information Management & Computer Security V0l.17 ,No.1, 2009, PP.154 – 157

الإجراءات التي يجب اتباعها من المؤسسات لحماية معلوماتها وتدعيم أمن المعلومات لديها وتتمثل هذه الطرائق في التالي:

1-كلمات المرور/تعتبر كلمات المرور من ابسط إجراءات حماية المعلومات فهي تعمل على حماية البيانات والمعلومات الشخصية والمؤسسية والحكومية وفي كثير من الاحيان تكون كلمات المرور اسلوب لحماية الأنشطة والافعال من السرقات في الحسابات البنكية والمشتريات وتبادل المعلومات ولأهمية كلمات المرور يجب مراعاة النقاط التالية عند اختيارها والشكل رقم 2 يوضح عمل كلمات المرور:



شكل رقم (2) يوضح التقاط كلمات المرور

-استخدم كلمات المرور الخليطة من الحروف والارقام والرموز.

-اختر كلمة مرور صعبة ولامكن التنبؤ بها.

-تجنب اطلاع الآخرين عليها .

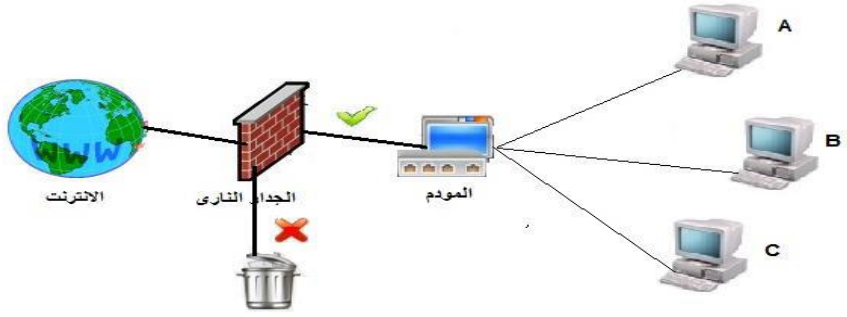
-ان لا تقل كلمة المرور عن عشر خانات .

-لا تجعل كلمة المرور كلمة واحدة.

-ان لا تتضمن كلمة المرور بيانات شخصية مثل حروف الاسم أو تاريخ ميلاد [1].

- الجدران النارية/ ظهرت هذه التقنية في ثمانينات القرن الماضي وبالتحديد مع ظهور شبكة الإنترنت العالمية بهدف ايقاف الخروقات الأمنية التي تتعرض إليها الشبكة ويعرف الجدار الناري على انه أي تقنية يتم وضعها في شبكة المعلومات لها القدرة على غربلة عملية نقل المعلومات الداخلة والخارجة[2] ,كما يعرف بانه أداة تعمل على تصفية وحجز مرور البيانات بين الشبكة الداخلية المحمية والشبكة الخارجية التي نخشى منها وان الهدف من الجدار الناري هو حجز المستخدم في حيز سياسة امنية معينة مثلا منع مرور أي شخص من خارج الشبكة إلى موارد المعلومات إلَّا عن طريق كلمات مرور متفق عليها مسبقا اومن يتم الوصول إلى المعلومات من أشخاص معينين فقط[3] ويعرف أيضًا بانه برنامج يفصل بين المناطق الموثوق بها والمناطق غير الموثوق بها في شبكات المعلومات الَّذي يقوم بدوره بعمليات المراقبة على طول الشبكة ويقرر الرفض أو الدخول

وفق قواعده .



شكل رقم(3) يوضح عمل الجدران النارية

[1] -- دخيل,احمد نوري,سعد عبد السلام طلحة.اختراقات امن المعلومات وطرق تفاديها. مصدر سابق :ص23

[2] – الملط احمد الخليفة .الجرائم لمعلوماتية0– الاسكندرية : دار الفكر الجامعي ،2006 ,ص 69

[3] – المناعسة ,أسامة أحمد وآخرون 0– جرائم الحاسب الالي والأنترنت .–عمان: دار وائل للطباعة والنشر,2001:ص80

– برامج مكافحة الفايروسات /هي أداة تبحث عن البرامج والتطبيقات الضارة لذلك تسمى برامج مكافحة البرامج الضارة ,تستخدم برامج مكافحة الفايروسات العديد من الطرائق للتميز بين الملفات والوثائق والبرامج والتطبيقات المثبتة في أجهزة الحواسيب وبين البرامج الضارة التي يستخدمها المهاجمين لتحقيق غاياتهم كما تعمل هذه البرامج على تحديد اوقات الاختراق بواسطة الفايروسات وعندما يتعثر برامج مكافحة الفايروس على أي برنامج ضار موجود داخل النظام يقوم بوضع خيارات عزل ذلك الفايروس وتعطيل عملها وجعلها غير قادرة على القيام بمهامها التي أُوكلت إليها بل تقوم بحذفها نهائيا [1].

– نظام الإنذار المبكر Early Warning System / يكثف مخترقو شبكة المعلومات الإنترنت جهودهم بتقنيات متطورة تسهل عليهم عملية الاختراق والهجوم، بينما يقوم المدافعون تدريجياً بتحديث تدابيرهم الأمنية النموذجية، إلَّا أن هذه الهجمات يكون في أغلب الأحيان من الصعب اكتشافها باستخدام تقنيات اكتشاف التسلل النموذجية. لذلك يتم تفعيل أنظمة الإنذار المبكر الَّتي تهدف إلى التنبيه لمثل هذه المحاولات في مراحلها الأولى باستخدام مؤشرات أولية.[2]

– التحكم في الوصول (Access Control)/ تخزن أنظمة المعلومات كمية هائلة من البيانات والمعلومات وتسمح بتحقيق الآلاف من العمليات على هذه البيانات كل يوم. في هذه الحالة، يبدو من الضروري وجود الأساليب والتقنيات والأدوات التي يمكن أن تجعل من الممكن تطوير نظام المعلومات على مستوى يعكس المتطلبات الحالية. من المهم أيضًا أن تقوم المؤسسة بتطوير نظام الأمان الذي يؤمن نظام المعلومات ضد التهديدات الخارجية. مرحلة مهمة جدا من بناء حماية البيانات في نظام المعلومات هي إنشاء نموذج عالي المستوى، مستقل عن البرنامج، يلبي احتياجات حماية وأمن النظام. وأحد المفاهيم الأساسية لنماذج الحماية هو التحكم في الوصول، والغرض من

---

[1] --.ممدوح شحات صقر . امن المعلومات ,ايس كوم ,مج9,ع1, 2008:ص12
https://search.mandumah.com تاريخ المراجعة 2022/9/15

[2] – جوهري ,عزة فاروق. امن المعلومات الرقمية وسبل حمايتها. المجلة المصرية لعلوم المعلومات ,مج7،ع1,2020:ص192

التحكم في الوصول إلى البيانات في نظام المعلومات هو التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام تقييد الإجراءات أو العمليات التي يمكن لمستخدمي النظام تنفيذها ونستنتج أن الهدف من التحكم في الوصول هو إجراء لأمن البيانات يسمح للمؤسسات بالتعامل مع الأشخاص المصرح لهم بالوصول إلى معلومات المؤسسة وموارده. يستخدم التحكم في الوصول الأمن السياسات التي تختبر المستخدمين على النحو الذي يدعونه وتوفر مستويات وصول تحكم مناسبة للمستخدمين. وكذلك من التقنيات المطبقة في الواقع يمكن القول إنَّ التحكم في الوصول يتضمن عمومًا بوابات أو أبواب أو حواجز مقفلة يمكن فتحها باستخدام طرائق مصادقة الهوية مثل بطاقات الوصول RFID أو الرموز السرية أو التعرف على الوجوه أو بصمات الأصابع أو الهواتف الذكية لتمكين الدخول إلى مبنى أو منطقة معينة[1] .

– تشفير البيانات (Data encryption)/ التشفير وهو عبارة عن عملية يتم فيها تحويل المحتوى الرقمي إلى رموز واشارات خاصه وذلك من أجل حماية المحتوى الرقمي اثناء عملية نقل أو ارساله عبر شبكات الإنترنت إذ يتم تحويله إلى شكل غير مألوف يصعب قراءته (محتوى مشفر)، بخوارزميات محدده ولا يستطيع أحد قراءة هذا المحتوى إلَّا بعد فك التشفير وتعتبر ميزة التشفير ناجحة تمام عند ضياع جهاز الحاسوب الخاص بك أو الذاكرة الخاصة بنقل البيانات، فعندما يتم تشفير المعلومات لا يمكن لأحد قراءتها أو فهمها. بهذه الطريقة إذا فقدت الكمبيوتر المحمول أو محرك أقراص فلاش USB خارج المكتب، فلن يتمكن أحد من الوصول إلى المعلومات أو قراءتها، وستكون محمية. أفضل طريقة لحماية معلوماتك مع الحفاظ على الوصول إليها هي تشفير المعلومات قبل مغادرة المكتب أو المنزل.

– التخزين الاحتياطي: (Backup storage)/ قصد بها عملية نسخ ملفات الجهاز على أجهزة تخزين منفصلة، أو حفظ نسخة من البيانات في مكانين مختلفين؛ بحيث

[1] -- دخيل,احمد نوري .اختراقات امن المعلومات وطرق تفاديها.مصدر سابق :ص24

يمكن استرجاع البيانات من النسخة الاحتياطية في حالة فقدان الملفات والبيانات لأي سبب مثل انقطاع التيار، أو تلف القرص الصلب.

- التوقيع الرقمي/هو مخطط رياضي يستخدم لغرض التحقق من سلامة المعلومات والبرامج والملفات والوثائق الرقمية ويعتمد التوقيع الرقمي على عملية التشفير لإيجاد حل لمشاكل سرقة المعلومات والاحتيال الإلكتروني وضمان عدم تعديل والتلاعب بمحتويات المعلومات اثناء نقلها عبر شبكة الإنترنت كما يوفر التوقيع الرقمي معلومات اضافية حول اصل الرسالة وحالتها ومصدرها .وقد ظهر مصطلح التوقيع الرقمي عام 1976 ويستخدم اليوم في الكثير من المجالات ومن ابرزها التجارة الإلكترونيَّة وان التوقيع الإلكتروني طريقة موثوقة للغاية إذ انه يحدد هوية المرسل والمستقبل إلكترونيًا لذلك تعتمده الكثير من مؤسسات المعلومات في حماية نفسها من الاحتيال وعمليات النصب التي قد تتعرض لها [1] .

النتائج:

1-تواجه الكثير من مؤسسات المعلومات تحديات أَمنيَّة عديدة مثل التحديات البشرية بقصد أَو غير قصد وأَخطاء فنية وتحديات طبيعية كالزلال والفيضانات .

2-التحديات الأَمنية لمؤسسات المعلومات في تطور مستمر وان عملية السيطرة عليها باستخدام الطرائق التقليدية صعبة جدا لذا صار من الضروري وجود أَمن معلومات لضمان استمرار اعمالها اليومية .

3-النسبة العظمى من التحديات التي تواجهها مؤسسات المعلومات تأتي من داخل المؤسسة نفسها وليس من الخارج .

4-حماية البيانات والمعلومات داخل المؤسسة يتطلب توظيف جميع المكونات المادية والبرمجية ضمن منظومة امنية متكاملة يكون هدفها الحماية والحفاظ على أَمن المعلومات.

[1] - مزيد,حميد رشيد.واقع ادارة امن نظم المعلومات في كلية علوم الحاسوب والرياضيات جامعة ذي قار :دراسة مسحية 0- مجلة الدراسات المستدامة ,مج4,ع1, 2022:ص340

5-عدم إجراء التحديثات لبرامج مكافحة الفايروسات بصورة دورية لخادم الشبكة وجميع محطات العمل المستخدمة في مؤسسات المعلومات يؤدي لتعرض المعلومات للفايروسات في أي وقت.

6-استخدام تقنية جدار النارFirewall في حماية المعلومات يقلل من خطر التحديات والتهديدات التي تطلق باتجاه مؤسسات المعلومات.

7-قلة العاملين في مؤسسات المعلومات من الكوادر البشرية المؤهلة والمدربة في مجال تكنولوجيا المعلومات بشكل عام وأَمن المعلومات بشكل خاص يجعل مؤسسات المعلومات ارض خصبة للمخترقين.

التوصيات:

1-العمل على تدريب العاملين والقيام بالعديد من ورش العمل والدورات التدريبية التي تنمي مهارات وقدرات العاملين المعرفية والتقنية في مجال أَمن المعلومات.

2-توعية المستخدمين انفسهم على حماية بياناتهم الشخصية .

3-تقييم المخاطر والتهديدات التي تتعرض لها مؤسسات المعلومات وبشكل دوري للوقوف على الإِجراءات الواجب اتخاذها لزيادة فاعلية أَمن المعلومات.

4-توحيد الجهود الدولية لعمل تشريع موحد يظهر فيه العقوبات المناسبة لمرتكبي الجرائم المعلوماتية.

5-وضع البرامج المجدولة لعملية النسخ الاحتياطي الطارئ والتحقق من صحة عمليات النسخ الاحتياطي.

6-مواكبة التطورات في أَساليب وتقنيات الجرائم الإِلكترونيَّة عن طريق اقتناء وتنصيب البرامج المضادة للحد من الجرائم المعلوماتية التوصيات.

7- هناك حاجة ضرورية على المستوى العالمي لاستحداث بنية تقنية قابلة للتحديث والاستخدام من مؤسسات المعلومات يكون هدفها حماية المعلومات والحفاظ على أَمنها وسلامتها من الوصول والنسخ والتغيير والفقدان.

References

- Filali, Asmaa, Shaleel Abdel Latif. (2019) **Information security threats and ways to address them** 0 - Al-Bashaer Economic Magazine, Vol. 4, p. 3,

- Lamine, Alouti (2009) **Challenges of Electronic Security in the Organization** 0 - Journal of Economic and Administrative Research. P6,.
- Yasmine, Bel'asal Bint Nabi, Amroush Al-Hussein. (2021) **Electronic Threats and Cybersecurity in the Arab World** 0- Numeros Academic Journal, Vol. 2, P. 2,.
- Baghazar, Abrar, and Al-Omari, Ahmed, (2019) **information security in smart cards, geophysical, social and human challenges in a changing environment,** the Tenth International Scientific Conference, Istanbul - Turkey,.
- Bin Jumaa, Jumaa Bin Ali (2010) **Arab Security in a Changing World**, Cairo: Madbouly Press,.
- Golden, Matthew (2017) **The Handbook of Information Security for Advanced Neuroprosthetics**, Second Edition Publisher: Synthypnion Academic,.
- Al-Hamidi and others. (2005) **Management Information Systems 0 Contemporary Introduction**, Amman: Wael Publishing House,.
- That Said Ibrahim Abdul Wahid. (2015) **Information Security Policies and their Relationship to the Effectiveness of Management Information systems in Palestinian communities** - Master's thesis. Al-Azhar University. Faculty of Economics and Administrative Sciences..
- Al-Yahawi, “Yahya. On the Ability to Communicate - Communication on the Touch of the Internet and the Globalization of Information,” Okaz Publications 201.
- Nihad Abdel-Latif Abdel-Karim, Kholoud Hadi Al-Rubaie. The security and confidentiality of information and its impact.
- An applied study on the competitive performance of the two Iraqi general and Al-Hamra insurance companies - Journal of Financial and Accounting Studies, vol. 8, p. 28.
- Abu Dhiub, Qutayba Ahed Muslim. 2019) **Extent of Commitment to Policies of Security and Protection of Accounting Information in Commercial Banks**. - Master's thesis. Al al-Bayt University. College of Graduate Studies,.

- Amina, Qadayfa. (2016) **Information Security Strategy** - Economic Dimensions Magazine,
- John M. Broky, Thomas H. Bradley. **Protecting Information with Cybersecurity, Berlin**: Springer International Publishing AG, 2019, Pp. 350-351, Available At: http://08102q3xn.1104.y.https.link.springer.com.mplbci.ekb.eg/content/pdf, Access Date: 9/15/2022
- Al-Mutairi, Khaled Zaher. **Penal legislation in Protecting the Cyber Security of the Gulf Cooperation Council Countries**. - Journal of Jurisprudential and Legal Research, p. 38, 2022.
- Mosly, Nour Amir (2021) **Cyber Attacks in Light of International Humanitarian Law**. - Master's thesis, Syrian Virtual University, Syria,.
- Al-Samhan, Mona Abdullah. (2022) **Requirements for Achieving Cyber Security for Administrative Information Systems at King Saud University** 0 - Journal of the College of Education, Mansoura University, p. 111,
- Harik, Fatih (2021) **Cyberspace and the Transformation in the Form of Wars.** The first virtual conference: p. 7
- Hamid, Abdul Wahab Karim**,** (2021) **Cybersecurity, Restrictions and Challenges in Light of the Rules of International Law** - Journal of the Social Contract. Legal Research Center in the Ministry of Justice in the Kurdistan Region of Iraq.
- Zaruka, Ismail. (2019) **Cyberspace and the Shift in the Concepts of Power and Conflict**. 0 - Journal of Legal and Political Sciences vol. 10, p. 1,: p. 1017
- Clay, honest. Cybersecurity and the challenges of computing and electronic penetrations of countries through cyberspace, University of Algiers, Vol. 15, p. 1, 2022.
- Suleiman Ali Fadel**. The Right to Legal Defense Against Cyber Attacks**. Journal of Tikrit University for Law, Fourth Year, Baghdad: Al-Iraqiya University, Vol. 4, Part 4, Part 1.
- Al-Mawsili, Nour Amir, Cyber Attacks in Light of International Humanitarian Law, previous source, p. 7

- Al-Bahi, Raghda. **Cyber Deterrence: Concept, Problems, and Requirements** 0 - Journal of Media Studies, Arab Democratic Center, No. 1, 2018.
- Al-Samhan, Mona Abdullah.. **Requirements for achieving cybersecurity for administrative information systems at King Saud University** 0 - Journal of the College of Education, Mansoura University, p. 111, 2022.
- Awad Allah Ahmed Hosni. **The impact of information security characteristics on achieving organizational excellence through organizational learning capabilities at the University of Jordan**, Sudan: University, 2018.
- Saba, Ghassan. **Network Security and Information Infrastructure** - Master Thesis, Syrian Virtual University, 2018.
- Media Authority. **Cybersecurity,** Department of Studies, Communication and Public Relations, Jordan, 2021.
- Al-Abed, Sakina. **Information security through social networks** 0 - The Arab Journal of Informatics and Information Security, Vol. 1, p. 1, 2020: p. 207
- Al-Danaf, Ayman, The reality of information systems security management in technical colleges in the Gaza Strip and ways to develop it. 0 - Master's thesis in Business Administration, Islamic University, Gaza, 2013.
- Nihad Abdel-Latif Abdel-Karim, Kholoud Hadi Al-Rubaie. The security and confidentiality of information and its impact on competitive performance. An applied study on the General and Al-Hamra insurance companies. Previous source.
- Dakhil, Ahmed Nouri (2016) Saad Abdel-Salam Talha. **Information Security Breaches and Ways to Avoid Them**. The International Journal of Engineering Sciences and Information Technology, Vol. 2, p. 2,: p. 20
- Fernando Georgel Birleanu Peter Anghelescu, Nicu Bizon. Malicious and Deliberate Attacks and Power System Resiliency, Switzerland: Springer Nature AG, 2019, p. 230, Available At: http://08102qrbe.1104.y.https.link.springer.com.mplbci.ekb.eg/content/ pdf, Access Date 9/18/2022

- Jubouri, Nada Ismail 0 - Tikrit Journal of Administrative and Economic Sciences. Protecting the security of information systems, Vol. 7, No. 21 2011.
- Labusshagne, L. & Eloff, Electronic Commerce: The Information Security Challenge", Information Management & Computer Security V0l.17, No.1, 2009.
- Al-Malt Ahmed Al-Khalifa. Informatics Crimes 0- Alexandria: Dar Al-Fikr Al-Jami'i, 2006.
- Al-Manasah, Osama Ahmed and others - **Computer and Internet Crimes** - Amman: Dar Wael for Printing and Publishing, 2001: p. 80
- Mamdouh Shahat Saqr(2008). **Information Security**, Icecom, Vol. 9, No. 1.
- Johari, Azza Farouk. **Digital Information Security and Ways to protect it**. The Egyptian Journal of Information Sciences, Vol. 7, p. 1, 2020.
- Meziad Hamid Rashid. The reality of information systems security management in the College of Computer Science and Mathematics, Dhi Qar University: a survey study 0 - Journal of Sustainable Studies, Vol. 4, p. 1, 2022.

Information and Cyber Security Challenges at Information Institutions

Muhannad Muhammad Munib Al-Rawi*

Sumaya Younes Saeed **

Abstract

This research aimed to identify the challenges related to information security and cyber security, and these challenges were represented in natural challenges such as earthquakes, hurricanes, floods, fires, high temperatures and humidity, and human challenges

* **Master student /Department of Information and Knowledge Technologies/College of Arts/University of Mosul.**

** **Asst.Prof /Department of Information and Knowledge Technologies/College of Arts/University of Mosul.**

represented by sabotage acts carried out by individuals, whether by intentional ways or information crimes and through the dissemination of information Confidentiality obtained illegally, and loopholes which are weaknesses that

exist during The process of designing or creating software and rules for storing information or devices that stimulate information and network equipment and programs through which the attacker can infiltrate the events of what he wants from sabotage operations, as well as the possibility of jamming is done through equipment dedicated to the work of jamming, or the interference may be caused by some Unintended natural factors and conditions. The researchers used the descriptive approach, and the most important results they reached were that information security is that science that is concerned with studying methods of protecting data and information for information institutions stored in computers and servers and working to counter all attempts aimed at illegal entry into the data base or those that aim to change the data base. and
transfer information to another place, and many information institutions face many security challenges, such as human challenges, intentionally or unintentionally, technical errors, and natural challenges such as earthquakes and floods.

Key words: Information Security/Cyber Security/ Information/Security Challenges.