سياسة أَمَـن المعلومات وحمايتها في مركز الحاسبة الالكترونيَّة في الجامعة التقنية الشماليَّة بين الواقع والطموح

م. م. رأفت رجب فتحي حسين
جامعة الموصل / قسم المعلومات وتقنيات المعرفة

المستخلص:

يهدف البحث إلى التعرف على"واقع سياسةأَمَـن المعلومات"وحمايتها في مركز الحاسبة الإلكترونيَّة في الجامعة التقنية الشمالية،كما يستعرض البحث تعريف"ومفهوم أَمَـن المعلومات وتطوره التاريخي" وأَهميَّته وأَهدافه "ووظائفه وخصائصه وعناصره ومكوناته"ومراحله وأَنواع أَمَـن المعلومات"ومبادئه ومتطلبات ومجالات وتدابير أَمَـن المعلومات ودورها في حفظ وحماية المعلومات، وكذلك يبين البحث أَبرز التأثيرات في حماية المعلومات والبيانات والبنية التحتية "وكذلك المعلومات المخزونة على الحواسيب وإمكانية توفير افضل سبل الحماية لها، وهدف البحث إمكانيَّة التعرف"على إجراءات سياسة أَمَـن المعلومات"والتعرف على أَساليب حمايتها "والتعرف على اهم المخاطر والتهديدات في كافة المؤسسات وتحديد المفاهيم المرتبطة بأَمَـن المعلومات والبيانات.

اتخذ البحث المنهج المسحي"الوصفي في امكانية"إعداده لملائمته طبيعة البحث والدراسة.

وتوصَّل البحث"إلى بعض النتائج وهي كالاتي :

1_تبيَّن أَن لدى مركز الحاسبة الالكترونيَّة سياسة مكتوبة ومخطط لها لأَمَـن المعلومات يتم اتباعها وفق معايير دولية بالإضافة إلى إجراءات فعالة لتقليل المخاطر، كما ان ادارة الجامعة لديها رغبة في تطبيق"سياسة رصينة لأَمن"المعلومات لحماية البيانات .

2_تبين ان مركز الحاسبة يستخدم سياسة التشفير مثلا التوقيع الرقمي في تبادل المعلومات وأَنظمة كشف"الاختراقات قبيل حدوثها لحماية البيانات المخزنة في"الخوادم من الاختراق .

توصي الدراسة ببعض التوصيات وهي كالاتي :

1_القيام بتذليل الصعوبات امام عمل تحليل المخاطر للوقوف على مقتربات القوة والضعف عند التعامل مع المعلومات، ويتوجب على المركز القدرة على تحليل أَسباب"مخاطر أَمَـن المعلومات ومعالجتها واتخاذ كافة التدابير الأَمنية.

2_العمل على ايجاد أَنظمة كشف الاختراق التي تصد أي هجوم يعطل الخدمة كما يمكن توفير برامج يأتي من خلالها تنبيه من اي موقع غير مصرح به من أَي مكان بالعالم.

الكلمات المفتاحية:

أَمَـــن المعلومات, السياسة الامنية, التحديات التقنية, حماية البيانات, مخاطر المعلومات

Security And Protection Policy at The Electronic Computer Center At The Northern Technical University Between Reality And Ambition

Assist. Lect. Rafat Rajab Fathi Hussein

Mosul University / Information and Knowledge Technologies Dept.

Abstract:

The research aims to identify “the reality of information security policy” and its protection in the Electronic Computing Center at the Northern Technical University. The research also reviews the definition of “and the concept of information security and its historical development,” its importance and goals, “its functions, characteristics, elements, and components,” its stages and types of information security, its principles, requirements, fields, and measures. Safe Information and its role in preserving and protecting information. The research also shows the most prominent effects in protecting information, data and infrastructure, as well as information stored on computers and the possibility of providing the best means of protection for it. The aim of the research is the possibility of identifying “information security policy procedures” and identifying methods of protecting it “and identifying the most important Risks and threats in all institutions and defining concepts related to information and data security. The research took the “descriptive” survey method in preparing it to suit the nature of the research and study.

The research reached some results, which are as follows:

1_ It was found that the Electronic Calculator Center has a written and planned policy for information security that is followed in accordance with international standards, in addition to effective procedures to reduce risks, and that the university administration has a desire to implement a “solid policy for information security” to protect data.

2_It was found that the Computer Center uses encryption policy, for example digital signature, in exchanging information and systems Detecting breaches before they occur to protect data stored in servers from hacking.

The study recommends some recommendations, which are as follows:

1_ Overcoming the difficulties in conducting risk analysis to identify strengths and weaknesses when dealing with information. The center must be able to analyze the causes of information security risks and address them. And take all security measures.

2_Work on finding intrusion detection systems that repel any attack that disrupts service. It is also possible to provide programs through which a warning comes from any unauthorized site from anywhere in the world.

Keywords:

Information security, Security policy, Technical challenges, Data protection, Information risks

الاطار العام للبحث

1_المقدمة:

بدأ أَمَـن المعلومات واتسع تطوره مع بداية تكنولوجيا المعلومات وتطورها وبدأت الحواسيب الآلكترونيَّة باحتواء معلومات وبيانات متميَّزة اذ بدأ القلق على أَمَـن المعلومات والأَجهزة التي تعالجها وتخزنها وتنقلها لمبدأ التفكيرفي انجاز تأمين مواقع هذه الأَجهزة والمعلومات وحمايتها، وزاد الأَمرتعقيدً ربط أجهزة الحواسيب حول الكرة الأَرضيَّة بشكبة واحدة هي شبكة الإنترنت، واعتماد كثير من الناس عليها في أَداء أعمالهم، وتنمية تجارتهم وزيادة تحصيلهم العلمي وتواصلهم الاجتماعي وإنهاء إجراءاتهم الحكوميَّة والمؤسسية لو أَنَّ تلك الحلول والخدمات الإلكترونيَّة خالية من التهديدات وآمنة طوال الأوقات لصار الأَمر في منتهى الروعة لازداد التوسع في تقديم مزيد من الخدمات الإلكترونيَّة واتساع الاقبال عليها.

تعدُّ تهديدات أَمَـن المعلومات من المخاطر التي لها أثر كبير للغاية على المنظمة ، ومن ثُمَّ فإنَّ بناء سياسة تغطي متطلبات أَمَـن المعلومات للأمن المرغوبة وتحدد الجوانب الأخرى مثل: أَهداف أَمَـن المعلومات، وملكية السياسة, وتفويض الواجبات سيساعد في إدارة حوادث أَمَـن المعلومات والاستجابة لها بشكل ممتاز، ومن شأن هذه السياسة الفعَّالة بناء أساس سليم لتحديد وتنظيم وترتيب إدارة أُصول المعلومات المؤسسيَّة ونظم المعلومات التي تقوم بتخزين، ومعالجة ونقل واحتواء البيانات المؤسسية، ويتم تأمين مثل هذه السياسة للتأكد من أَنَّ المعلومات مناسبة من الآثار السلبية للمخالفات في السرية والنزاهة والالتزام الَّذي يمكن أَن يحدث بخلاف ذلك.

2_مشكلةالبحث:

دعت تطورات مجال تكنولوجيا المعلومات ومصادرها الإلكترونيَّة وكثافتها وتطورالتقنية بشكل كبير إلى سهولة اختراق المعلومات وظهور العديد من المخاطرالَّتي قد تواجه البيانات والمعلومات المخزونة في الحواسيب، اذ تشكل مشكلة تواجه مجتمع أَمَـن المعلومات بغياب الوعي بأَهميَّة اتباع سياسة امنية لحمايتها من الاختراق،وعدم الحفاظ على سرية المعلومات وتكاملها وسلامتها نتيجة اخطار تتعرَّض لها الأَجهزة من المتسللين إلى المعلومات، لذلك يجب اتاحة سياسة أَمَـن معلومات قادرة على توفير بيئة آمنة، وهذا يشكل محور البحث.

3_ الأَسئلةالبحثية:

"يسعى البحث إلى الاهتمام بالإجابة على التساؤلات الاتية : "

1_ما هي التهديدات الممكنة التي قد تحصل لأَمَـن المعلومات؟

2_ما هي التدابير الأَمنيَّة المهمة اللازمة لحماية المعلومات؟

3_ما مدى توفّر سياسة أَمَـن معلومات قادرة على مواجهة وتهيئة بيئة آمنة لحماية المعلومات والبيانات من الاختراق؟

4_ماهي المتطلبات المتاحة لأَمَـن المعلومات في الحفاظ على البيانات"والمعلومات المخزونة في الحواسيب؟

5_ماهي وسائل المحافظة على أَمَـن المعلومات والبيانات وتأمينها للعمل على تقليل الخسائرالمحتملة من عملية التخريب أوالسرقة للمعلومات؟

4_أَهميَّةالبحث:

"تكمن أَهميَّة البحث من أَهميَّة الموضوع قيد البحث نفسه، إذ يعد البحث اضافة إلى النتاج الفكري والحيوي في مجال المعلومات وتقنيات المعرفة من جانب،وخدمة الباحثين المتخصصين والمستفيدين من ذوي الاهتمام في هذا الموضوع بتسليطه الضوء على الجوانب الحديثة والتدابير التكنولوجية للمحافظة على أَمَـن المعلومات وتتبع سياسة حمايتها.

5_اهداف البحث:

يهدف البحث إلى تحقيق الاهداف وهي كالاتي:

1_التعرف على كافة اساليب حماية المعلومات من السرقة والتخريب والاختراق.

2_التعرف على الجهات المخولة والمأذون لها بالوصول إلى المعلومات.

3_معرفة حجم الخسائر المحتملة من عملية تخريب البيانات او السرقة والحد من تعطل الخدمات والاعمال الرسمية جراء عمليات التخريبية.

4_العمل على معرفة سبل المحافظة على أَمَـن المعلومات والمتطلبات الخاصة بحماية أَمَنها وبياناتها.

5_التعرف على مخاطر امن البيانات والتهديدات الخاصة بأَمَـن المعلومات.

6_منهج البحث:

اعتمد البحث على المنهج المسحي والوصفي لامكانية استعراض أَدبيات موضوع سياسة أَمَـن المعلومات ووصف مضمونه وتغطية كافة جوانبه.

7_حدود البحث:

يقتصر البحث على الحدود الاتية:

1_ الحدود الموضوعية: يشمل أَمَـن المعلومات والجوانب المتعلقة به والمكملة له.

2_الحدود المكانية: مركز الحاسبة الالكترونية موقعه في الجامعة التقنية الشمالية.

3_الحدود الزمنية: يتضمن منتصف العام الدراسي 2023_2024 .

8_ادوات البحث:

1_يتضمن المصادر الخاصة بالمعلومات الورقية والالكترونية.

2_المقابلة الشخصية: حيث اجرى الباحث مقابلة الشخصية مع مدير ومسؤولي الشعب في مركز الحاسبة الإلكترونـيَّة في الجامعة التقنية الشمالية.

أولا: أَمَـــن المعلومات (Information Security)

1_تعريف ومفهوم أَمَـــن المعلومات

يعتمد تعريف أَمَـن المعلومات بشكل كبير على السياق الوارد فيه حيث أن لكلمة الأَمَـن طيفاً متلازما وواسعاً من المجالات في حقل تقنية المعلومات أوخارجها ،كما يشير أَمَـن المعلومات على انه أَمَـن البيانات ونظرا إلى ان المعرفة اصبحت من اهم الاصول في وقتنا الحالي فقد اصبحت الجهود المعطاة للحفاظ على سلامة المعلومات ذات أَهميَّة كبيرة. وعرفته لجنة الأَمَـن القومي الاميريكية من الزاويةالنظرية هو علم يبعث في نظريات وسياسات توفيرالحماية للمعلومات من مخاطر الاختراقات التي تهددها ومن أنشطة الاعتداء عليها ومن ناحية التقنية لمجموعة من الوسائل وادوات واجراءات لازم توافرها لضمان حمايةالمعلومات من المخاطر الداخلية والخارجية **(الراوي،2023: ص27)**

ويعرف بأنه العلم الذي يبحث في سبل حمايةالمعلومات من مخاطر متعددة التي تهددها ويعمل على توفير وتطوير اساليب حديثة قادرة على مكافحة سبل التهديد التقنية الجديدة . **(التطورالتاريخي لامن المعلومات،2023)**

يتبين مما سبق أَمَـن المعلومات انه حماية وتأمين للبيانات والمعلومات والسماح فقط بالوصول إلى المعلومات في الدائرة للأشخاص المصرح لهم وحفاظا على سرية المعلومات من اي انتهاكات وهجمات من قبل مخترقين بهدف الدخول لسرقة البيانات والمعلومات عن طريق وضع كلمة مرور وان الهدف من ألأمن هو الحماية من كافة التهديدات سواء كانت طبيعية من عوامل الحرائق والفيضانات او بشرية كالسرقة او مادية كالهجمات والاختراقات والاعتداءات.

2_التطور التاريخي لأَمَـــن المعلومات

ترجع نشأة هذا النوع من انواع الحماية الرقمية لوكالة الاستخبارات المركزية الاميركية كأداة للتأكد من ان المعلومات في مأَمَـن تام وبعيد جدا عن اي اختراقات إلكترونـيَّة قدتتعرض لها من المخترقين والمعتديين الالكترونيين والتي يفترض ان لاتقع في أيدي المخربين لما تتمتع به من سريةعالية وأَهميَّة كبيرة بالنسبةلهم،وخاصة المعلومات السرية **(تاريخ امن المعلومات،2023)**

ظهر مصطلح الأَمَـن منذ بداية التواصل وتبادل الملفات و المعلومات اذ تمثل تاريخا حافلا لحماية المعلومات السرية ولاسيما العسكرية والامنية منها من التعرض للاختراق او سرقة من قبل جهات غير مصرح بها وخصوصاً الاعداء

كان أَمَـن المعلومات في بادئ الأمر يتضمن حماية معلومات مادية من التعرض للسرقة بعد ذلك تطور المفهوم ليشتمل على المعلومات السيبرانية والتقنيات الإلكترونـيَّة بشكل كامل وعمد المهتمين بحماية المعلومات من تشفيرها وابتكار شفرات سرية محكمة تمكنهم من التواصل وتبادل الرسائل بشكل تام يضمن انعدام محاولة سرقتها، اضافة إلى عدم مقدرة السارق على تفهمها وتسريبها ومن ثُمَّ فشل الاستفادة منها ،ومع التقدم التكنولوجي والأمني اصبح أكثر حماية للمعلومات عبر استخدام وسائل تشفير أكثر فعالية ومن ثُمَّ امكانيةاستخدام وسائل تواصل العادية في نقلها دون الخوف من تعرضها للاختراق،وان أولى الجهات التي تبنت مبدأ حمايتها لضمان حمايةالأَمَـن القومي هي المخابرات المركزيةالأمريكية وامنت الوصول إليها من قبل المخترقين اومن المستثمرين أصحاب الخبرةوالفضول تبلور أَمَـن المعلومات بشكله الحالي بعد أسراع الانترنت والحاسبات والتي تتضمن احتواء معلومات سريةو التي لا يرغب الأفراد والشركات والدول على تسريبها وتعريضها للاختراق وللسرقة والتخريب ،لهذا أخذت الشركات دورها على تطوير وسائل حمايةالمعلومات **(تطور امن المعلومات،2023)**

أَهميَّةأَمَـــن المعلومات :

تتجه أهميته في توفير الحماية الخاصة للبيانات وأصول تكنولوجيا المعلومات من الانتهاكات والوصول غير مصرح به وتسعى الشركات بهدف الاستثمار في مجال أَمَـن المعلومات لضمان توفير الحماية من التهديدات المحتملة،وتكمن أهميته في الاتي :

1_تقليل مخاطرعملية أختراق البيانات والهجمات في أنظمةتكنلوجيا المعلومات.

2_ تطبيق ضوابط صارمة أمنيةلمنع الوصول الغير مصرح به للمعلومات الخاصةاو السرية.

3_حمايةأنظمة وشبكات تكنولوجيةالمعلومات من خطر الهجمات السيبرانية.

4 – الحفاظ على سريةالمعلومات في مأَمَـن خاص وبعيد عن التهديدات الأمنية **(اهمية امن المعلومات،2023)**

5_تمكين حماية البنيةالتحتية المعلوماتية من أجل استمرارالقيام بأعمالها اليومية.

6– الحاجةلأنشاء بيئةإلكترونـيَّةمتوازنةتتسم بالأمان وتخدم القطاعين العام والخاص **(قدايفة،2016 ،مجلة ابعاد اقتصادية،مج6،ع1،ص165)**

أهداف أَمَـــن المعلومات

يهدف بشكل رئيسي إلى تقديم حماية مثلى للمعلومات من الاختراق والتعرض للتخريب المتعمد والغير المتعمد والممنهج،بالإضافة الي تفادي كم هائل من السرقة،وتجدر الإشارة إلى اهداف أَمَـن المعلومات وهي كالاتي : **(اهداف امن المعلومات،2023)**

اولا: تحديد عدد من الجهات المخولة الوصول إلى المعلومات

يتضح ان تحديد جهات مصرح لها بالولوج إلى المعلومات في ضمان عدم دخول اطراف غير مصرح بهم الامر الذي يضمن حماية الملفات المعلوماتية ويضيق نطاق البحث عن الجهةالمسؤولةعن احدى التعديلات عند عدم تعرض المعلومات لأي اختراق اوسرقة، بالأضافة إلى ماتم ذكره يعنى تحديد الجهات المخولةبالوصول إلى المعلومات بتخصيص صلاحيات محددة وواضحة لكل جهةمنهاالامر الذي ينظم ويرتب عمل أَمَـن وحمايةللمعلومات .

ثانيا: تقليل الخسائر المحتملة من عملية التخريب وسرقة المعلومات وتعرضها للخطر

يستفاد من أَمَـن المعلومات في حالة التعرض إلى هجوم أو سرقة مواد بسبب وجود ثغرات أمنية كبيرةاو بسبب قوة الهجوم على المعلومات في حماية اكبر قدرممكن منها اي بلغةأخرى الحد بشكل اوسع من التسرب وحماية المعلومات بأكبر قدر ممكن.

ثالثاً: حماية المعلومات من السرقة و الاختراق والهاكر

تهدف إلى حمايةومنع اختراق البيانات من اطراف خارجية بسبب التسارع التقني وزيادة حجم التنافس بين الأفراد والشركات وتقوم بعض الشركات بمحاولات تخريبية متعمدة بغية ألحاق ضررممكن بالشركات المنافسة،ومن ثُمَّ فسح المجال لها للتقدم والسيطرةعلى حصص سوقيةأكبر ، وتهدف (word press) أَمَـن حماية المعلومات المخزنة في مواقع إلكترونـيَّة وفق اضافات يتم تثبيتها لبرامج ادارةالمواقع إلى زيادة حجم ضمان حماية سريةالمعلومات.

رابعا: امكانية الحد من تعطل الخدمات والاعمال اليومية جراء عمليات التخريب

يحدث وفق إجراءنسخ احتياطيَّة للبيانات بشكل دوري لإتاحةالمجال الواسع امام استرجاعها بعد معرفة تعرضها للتخريب والسرقةالأمر الذي يشير الى تقليل الخسائر المحتملة واختصار الوقت لإصلاح الاضرار الذي يحد من مدةتعطيل انتاجية عمل تلك المؤسسات والشركات ويسمح لها بالتعافي تدريجيا ثم بشكل أسرع.

خامسا : العمل على ضمان تطبيق قوانين وضوابط تمنع تعديلات غير مصرح بها

ان مسار تحديد صلاحيات وجهات مخول لها الوصول للمعلومات يؤمن طريق مبدأ أَمَـن المعلومات حمايتها من تعديلات عشوائية قد تحدث حيث يمكن ان تحتفظ أنظمة أمنة للمعلومات المتقدمة بسجلات تفيدنا في معرفة اي تعديل قامت به جهة من جهات مصرح بها للوصول .

وظائف أَمَـــن المعلومات:

أَبرز وظائف أَمَـن المعلومات وهي كالاتي :(وظائف أَمَـن المعلومات،2023)

1. اختصاصي أَمَـــن المعلومات :

هو موظف مسؤول عن أَمَـن نظام وشبكة الحاسوب في المنظمة، يقوم بمجموعة من المهام الكافية لتحديد مشكلات الأمان المحتملة وتعزيزها في أنظمة المؤسسة، ووضع معايير امان خاصة وتثقيف الإدارة وتنظيمها لأفضل الممارسات التكنولوجية والأمنية، وتحديث برامج أَمَـن المعلومات، ويرصد الاختصاصي جميع النظم العاملة، ويتصدى للانتهاكات الأمنيَّة الصارمة، ويقوم بتطوير عدد من بروتوكولات أمان جديدة للموظفين مع تركيب أجهزة وبرمجيات حديثة متطورة، وامتلاكه مهارات تحليلية وخبرات لحل المشكلات.

2. محلل ومصمم أَمَـــن المعلومات:

يقوم المحلل بمجموعة من المهام الرئيسية من تحليل وتقييم وتصميم والتحقيق في نقاط الضعف في البنية التحتية لتكنولوجيا المعلومات للمؤسسة، ويسهم في حماية المعلومات والأنظمة من أي تهديدات مرتبطة بالإنترنت، ومن مسؤولياته التي يتعين على المحلل القيام بها البحث عن تقنيات أمان جديدة وفعالة لإمكانية حماية المؤسسة على أن تواكب أحدث الاتجاهات الأمنية الحديثة لتكنولوجيا المعلومات، وتثبيت البرامج مثل جدران الحماية وبرامج تشفير البيانات لحماية المعلومات الحساسة، ومراقبة شبكات عمل المنظمة والتحقيق في الانتهاكات.

3. مهندس أَمَـــن التطبيقات والبرمجيات:

تستعين جميع المؤسسات التي تعتمد على تطبيقات البرمجيات في عملياتها بمهندسي أَمَـن التطبيقات والبرمجيات للقيام بمجموعة من المهام الحيوية ومنها وضع معايير امنية وأفضل الممارسات داخل المؤسسة، وتقديم إرشادات للمطورين حول ممارسات الترميز الآمنة والحديثة، والمشاركة في استعراضات الرموز لتحديد نقاط الضعف الأمنية المحتملة الوقوع، كما يقوم مهندس الأَمَـن بالمساعدة مع فرق العمليات لضمان تنفيذ التدابير الأمنية بشكل فعال مستمر في بيئات الإنتاج، والمساهمة في تصميم وتنفيذ وبناء هياكل آمنة للشبكة.

4. محلل البرمجيات الضارة للملفات :

اذ يختص محلل البرمجيات الضارة بتصميم برامج امنة لحماية أصول البرامج والأجهزة، وذلك بالتعاون مع مسؤولي الأَمَـن والمبرمجين والمهندسين والمحللين ، ويقوم بتوثيق تهديدات البرامج الضارة وتشخيصها وتحديد الإجراءات والتقنيات لتجنبها، وتشمل المهام الاضافية للمحلل تصنيف البرامج الضارة وفق تهديدات وقواسم مشتركة، ووضع عدد من الوثائق الخاصة بسياسات أَمَـن الشركة، إلى جانب المشاركة في البحث وايجاد وتطوير وتصميم أدوات حماية البرامج الضارة.

5. مهندس أَمَـــن تكنولوجيا المعلومات والشبكات:

يلعب مهندس الأَمَـن دورًا حيويًا فعالا في الحفاظ على أَمَـن المؤسسات ،إذ يعمل مع اختصاصي أَمَـن المعلومات لتحليل نظام الكمبيوتر والشبكة الخاص بالمؤسسة، ويحدد المشاكل المتعلقة بالانتهاكات الأمنية

اليومية ومنها الاحتيال أو الهجمات الإلكترونـيَّة و البيانات المسربة والعمل على حلها، كما يتولى مهندس الأَمَـن مهام أخرى منها إجراء صيانة روتينية والترقيات على أنظمة وبرامج امان جديدة ،والعمل على إصلاح المشكلات المُقدمة من متخصصي أَمَـن المعلومات والشبكات، والبحث عن حلول لتطوير وتحسين الأنظمة الحالية.

6. محلل الحاسوب الجنائي:

هو شخص تقوم المنظمة بتعيينه ليكون مسؤولًا فعالا عن تحليل البيانات لمواصلة التحقيق في الحوادث والسرقات والجرائم الإلكترونية، واستخدام برمجيات الطب الشرعي للمساعدة في التحقيقات لكشف الجريمة، ويقوم هذا المحلل الجنائي بالوصول الأَمَـن إلى كافة الأجهزة الرقمية واستخراج البيانات منها، ووصوله إلى البيانات المشفرة أو التي جرى حذفها.

خصائص أَمَـــن المعلومات

يتسم أَمَـن المعلومات بعدد من الخصائص منها كما يأتي :

1- **الشمولية:** أتصاف أَمَن المعلومات بالكمال والشمول للمواضيع الذي يفيد متخذي القرار.

2_ **الدقة** : يجب أن تتاح المعلومات بدقة عالية وفق طلب المستخدم والموضوع محل البحث.

3- **التوقيت** : ان تصل المعلومات في وقت مناسب لمستخدمها لإيجاد القرارات العادلة والفعالة.

4_**الوضوح:** يتوجب ان تكون المعلومات خالية من الغموض وواضحة ومفهومة بشكل كبير لمستخدميها وليس مجهولة وتكون اجراءاتها وتعليماتها مبنية وفق مبررات مقنعة وقابلة للتنفيذ.

5_ **الموضوعية:** أن تكون المعلومات موضوعية بشكل جيد وفعالة ومنتظمة وخالية من قصد التحريف والتغيير لغرض التأثير على المستفيدين .

6_**المرونة:** المعلومات والبيانات قابلة للتكييف ومرنة بحيث يمكن استخدامها اكثر من مرة.

7_ **التكلفة:** المقصود أن يكون العائد المتوقع من المعلومات هو اكبر من تكلفة الحصول عليها.

8- **الواقعية:** هو أن تكون المعلومات المتوفرة ممثلة للواقع ومأخوذة من واقع حال المشكلة. **(خصائص أَمَـن المعلومات، 2023)**

9. **القبول** :وجد ان تتمتع سياسة أَمَـن المعلومات بالقبول والرضا والانسجام مع العاملين

(dulany. ,2002v13,15 january.p4)

عناصر أَمَـــن المعلومات

يضم أَمَـن المعلومات مجموعة متناسقة من العناصر كالاتي:

1_**السرية:** يقصد بها التأكد من أن المعلومات لا تكشف ولا يمكن أن يطلع عليها من قبل اشخاص غير مخولين بذلك ،وتعمل مؤسسات المعلومات من خلال انظمة حماية متطورة فرض السرية المعلوماتية عن طريق التشفير

اثناء ارسال واستقبال وخزن المعلومات وتقييد الوصول إلى مواقع يتم خزن البيانات والمعلومات فيها على اكمل وجه.

2- التكاملية وسلامة مضمون المحتوى : التأكد من أن مضمون محتوى المعلومات صحيح ولم يتم تعديله او العبث به من قبل اي جهة وبشكل خاص لن يتم تدمير المحتوى في أي مرحلة من مراحل المعالجة من حذف وتعديل او التبادل سواء في مرحلة التعامل الداخلي مع المعلومات والنقل عبر الشبكات أوعن طريق تدخل خارجي غير مشروع .

3- استمرارية توفر المعلومات والبيانات أو الخدمة: هي التأكد من استمرار عمل النظام المعلوماتي في الموقع بشكل جيد واستمرارية قدرته للتفاعل مع المعلومات وتقديم الخدمات لمواقع المعلوماتية ومستخدم المعلومات لم يتعرض إلى منع استخدامه لها او دخوله اليها .**(الحصيني ،2016.ص5_7)**

مكونات أَمَـــن المعلومات

يعتمد أَمَـن المعلومات بصورة عامة على مكونات اساسية هي كالاتي: **(مكونات امن المعلومات،2023)**

1_أَمَـن الأفراد البشرية والأدارة.

2_أَمَـن المعلومات والوثائق والارشيف الالكتروني بمراكز الحاسوب .

3_أَمَـن موقع بناية مركز الحاسوب الالكتروني.

4_ أَمَـن وتقنيات الأجهزة البيئيةالخاصةبمركز الحاسوب.

5. أَمَـن الاتصالات والشبكات الخاصةبالحواسيب الالكترونية.

6_أَمَـن التطبيقات وأنظمةالتشغيل والبرمجيات.

7_أَمَـن تكنولوجيا أجهزة الحواسيب الالكترونية.

مراحل تطورأَمَـــن المعلومات

شهد مفهوم أَمَـن المعلومات العديد من التغييرات والتحولات والتطورات بدأ من أَمَـن الحواسيب ومرورا بماهية الاجهزة وانتهاءا بما عليه من مفهوم الحالي لامن المعلومات

ويمكن تقسيم مراحل تطور مفهوم الأمن الى ثلاث حقب زمنية كالاتي:

1_مرحلة الستينات :

في هذه المرحلة كانت الحواسيب هي كل ما يشغل العاملين بالأضافة الى كيفية تنفيذ البرامج فلم يكن العاملين مشغولون بأمن المعلومات بقدر اشتغالهم بعمل الاجهزة.

2_مرحلة السبعينات :

في هذه المرحلة تم الانتقال الى أمن البيانات وبدأ استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات إضافة لوضع أجراءات حماية المواقع والحواسيب من الكوارث كما رافقه اعتماد خطط لتخزين نسخ إضافية من البيانات والبرمجيات بعيدا عن مواقع الحواسيب.

3_ مرحلة الثمانينات والتسعينات :

هذه المرحلة تم الانتقال الى مفهوم "أمن الحواسيب وذلك لكثرة التطورات في مجال تكنولوجيا المعلومات و التي سمحت لأكثر من مستخدم للمشاركة في قواعد البيانات ،فأصبح من الضروري المحافظة على المعلومات، وتكاملها وتوفر درجة موثوقيتها وهو المفهوم الذي تحدث عنه في إطار البحث الحالي **(مراحل تطور امن المعلومات، 2023)**

4_ المرحلة الرابعة :

ظهر مصطلح امن الخوادم حيث بدأت هذه المرحلة في مطلع القرن الحالي، إذ يركز أمن الخوادم على حماية البيانات والمعلومات والبرامج والتطبيقات والموارد المخزنة في خوادم خاصة وان الخوادم تعد الاساس لأي مؤسسة معلومات مهما كان حجمها وإمكانيتها المادية والتقنية ، ويمكن حماية البيانات والمعلومات المخزنة في الخوادم من خلال توظيف الادوات والتقنيات التي تساعد في منع عمليات التطفل والقرصنة ومن الضروري الحفاظ على المعلومات وتكاملها وتوافرها والتأكد من درجة موثوقيتها اذ ان الاجراءات الامنية تسهم في ضمان النتائج المرجوة وتقليص أختراق المعلومات والتلاعب بها. **(الموسوي، وفضل الله،2013 ،مجلة كلية بغداد للعلوم الاقتصادية،ص24)**

أنواع امن المعلومات

ان لأمن المعلومات أنواع مختلفة وهي كالاتي:

1_أمان التطبيقات:هو مجال واسع من أمن المعلومات يغطي نقاط الضعف في البرامج وتطبيقات الويب ،والهاتف المحمول وغيرها.

2- الأمان السحابي : يركز على بناء واستضافة التطبيقات الأمنة في البيئات السحابية.

3_التشفير: غالبا ما تستخدم التوقيعات الرقمية في التشفير للتحقق من صحة الوصول للبيانات.

4_أمان البنية التحتية: يتعامل أمان البنية التحتية مع حماية الشبكات الداخلية والخارجية والمختبرات، ومراكز البيانات، والخوادم ، وأجهزة الكومبيتر المكتبية والاجهزة المحمولة.

5- الاستجابة: الاستجابة للحوادث هي الوظيفة التي تقوم بمراقبة السلوك الضار المحتمل والتحقيق فيه بشكل فعال .

6- **أدارة الضعف** : هي عملية مسح البيئة بحثا عن نقاط الضعف (مثلا البرامج الغير مربوطة) وتحديد أولويات المعالجة بناءا على المخاطر **(انواع امن المعلومات، 2023)**

7- **مكافحة الثغرات الأمنية** : يتم ذلك عبرمحاكاة عمليات الاختراق المحتمل وقوعها، مما يساعد الخبراء على تفادي حصولها بالأضافة الى تعزيز وسائل حماية سرية المعلومات**(الجواد،2019:ص21)**

مبادئ أمن المعلومات

هناك مجموعة من المبادئ التي يمكن من خلالها ضمان تحقيق أهداف أمن وحماية المعلومات خاصة في ظل ما تشهده حركة التقدم التقني من تسارع كبير ومن أبرزها:

1_مبدأ المسؤولية:

يجب وضع أطر توضيح سياسة أمن المعلومات بحيث تكون مسؤولياتها واضحة لجميع الموظفين والتركيز على عملية التدقيق تخضع له كافة الأطراف التي تتعامل مع البيانات وترتقي إلى مستوى عال لأمن وسرية المعلومات الذي يعتبر شديد الحساسية للمؤسسات.

2_مبدأ التكاملية :

يجب ان تشكل المعايير والمبادئ والوسائل المتبعة بنية متكاملة تعمل على حماية المعلومات والبيانات وان تكون منسجمة مع الاساليب والسياسة الأمنية التي تعتمدها المؤسسة.

3_مبدأ التناسبية:

وهذه من المبادئ التي يجب أن تحقق مستوى عال من التناسب بين أمن المعلومات مع امكانية إجراء تعديلات يتم من خلالها التعامل مع المخاطر، والاستخدام والافصاح عن المعلومات ،كذلك التأكد من وجود توافق بين أمن المعلومات وكافة أصول المعلومات وقيمتها من خلال إدراك مدى حساسية المعلومات واحتمال تعرضها لمخاطر مقصود وغير مقصودة .

4_مبدأ التوقيت المناسب:

ان عملية الحفاظ على أمن وحماية المعلومات يتطلب معرفة الوقت المناسب للتدخل متى ما تطلب الأمر التدخل السريع، ذلك لان عامل الزمن مهم لمعرفة تحديد التهديدات استنادا الى الاحداث خلال فترة اكتشاف الخطر والوقت المناسب للتدخل للتخفيف من تلك المخاطر إن لم يكن اكتشافها واحتمال حدوثها.

5_مبدأ التقييم :

يجب إجراء عمليات تقييم لإجراءات أمن وحماية المعلومات بشكل دوري حتى يتم التمكن من تحديد المعلومات الحساسة والتركيز على امنها وسريتها وأساليب اختراقها وتصنيف المعلومات حسب درجة حساسيتها وأهميتها وهذا يساعد على توفير الوقت والجهد والتكلفة.

6_الاخلاقيات:

وهي ركيزة مهمة تعكس مدى التزام المنظمات والشركات ومؤسسات المعلومات والجامعات والاشخاص بأخلاقيات التعامل وإدارة العمليات الخاصة بأنظمة المعلومات خاصة وأن المعلومات يتم إدارتها من خلال كادر كبير من الموظفين يختلفون في مستوياتهم الثقافية وظروفهم الاجتماعية، لذا يجب على المؤسسات أن تحدد أمن وسلامة المعلومات بصورة تتوافق مع مستويات الموظفين الثقافية والاجتماعية **(مبادئ امن المعلومات،2023)**

7_مبدأ السرية:

من المبادئ الاساسية الأولى هي السرية وهذا يعني ببساطة أن المعلومات غير متوفرة للأشخاص غير المصرح لهم بمشاهدتها على سبيل المثال يتم الحفاظ على سرية المعلومات المتعلقة بمدفوعات الموظفين ، إذا تمكن الموظف من الوصول إلى سجلات كشوف المرتبات ووجد المبلغ الذي قام بدفعه له زميله ، سيكون ذلك انتهاكا لمبدأ السرية **(سرية المعلومات،2023)**

متطلبات أمن المعلومات:

إن من المتطلبات وضع عدد من القوانين والاجراءات لتحديد الأدوار الرئيسية والحديث عن الاخطار والتهديدات وهذه المتطلبات هي كالاتي **(الجيزاوي،2018:ص41_42)**

1_ ادراج امن المعلومات ضمن الأمن القومي للدولة، باعتبار أن تقنية امن المعلومات بالغة الأهمية لأمن البلاد.

2_ تشكيل لجان قانونية لمتابعة التطور التقني والامني لقطاع المعلومات ومتطلباتها اللازمة لضمان أمن وحماية نظم المعلومات، بما في ذلك خصوصية المعلومات والبيانات الشخصية.

3 . اعتماد العقوبات الرادعة للتحديات والمخالفات غير المشروعة مع مراعاة التحديث المستمر لها لتواكب المستجدات في تقنيه المعلومات.

4_اعتماد استعمال بعض الوسائل الأمنية الالكترونية ومنها البطاقة الذكية لأثبات هوية المستخدم، وكافة المعلومات المتعلقة به واستخدام التوقيع الالكتروني في المعاملات الالكترونية وتطبيق البصمة الالكترونية، وبرامج الحماية المعلوماتية الوقائية.

5_ تقويم أنظمة ولوائح عمل أجهزة الدولة على المستوى الكلي بما يتناسب مع متطلبات العمل الالكتروني، ومنح المستخدمين على اساس شخصياتهم ومراتبهم صلاحيات التعامل والنفاذ للمعلومات الحساسة كل حسب مرتبته الوظيفية وما يكفله له قوانين الامن المعلوماتي والافادة من خبرات الدول التي تعاملت مع المتطلبات القانونية والاطلاع على مشكلات التطبيق فيها.

مجالات أمن المعلومات :

ظهرت عدة مجالات فيما يتعلق بأمن المعلومات وهي كالاتي(**مجالات امن المعلومات،2023**)

1_مسؤول امن المعلومات: يعد المسؤول عن امن المعلومات اللبنة الاولى في أي فريق مختص في حماية المعلومات، أذ يمتلك الخبرات الاساسية التي يجب أن يتمتع بها اي مختص في أمن المعلومات ويقدم مسؤول الأمن الخدمات الضرورية واللازمة للحفاظ على سلامة المعلومات من مختلف المخاطر مثل السرقة والتخريب .

2_مسؤول أمن الشبكات: يعنى مسؤول أمن الشبكات بحماية المعلومات عند تبادلها او تخزينها على منصات التخزين السحابي عبر تهيئة البيئة الأمنة والخالية من المخاطر التي تؤدي إلى تلف المعلومات أو ضياعها أو سرقتها.

3_ مختص أدارة المخاطر: ينطوي العمل الرئيسي لمسؤولي أدارة المخاطر على تقييم حالة أنظمة الشركات وتحديد مواطن الضعف فيها مما يساعد فريق أمن المعلومات على تلافيها بأسرع وقت دون الحاجة لفحص جميع أجزاء الانظمة التي قد تستغرق وقتا أطول .

4_مهندس أو مسؤول تحليل البيانات الأمنية : تتركز مهام مسؤول تحليل البيانات الأمنية في تتبع محاولات الاختراق وذلك من أجل معرفة مصدر الهجمات الالكترونية وموقعها أو معرفة حجم الضرر الذي تسبب حيث تجرم الكثير من الدول محاولات تهديد الأمن الالكتروني وبالتالي يعد الوصول إلى المخترق أمرا مفيدا لملاحقته قانونياً وتسليمة للقضاء المختص.

5- مسؤول البرمجيات والتطبيقات: تعد المهمة الرئيسية أمام مهندس التطبيقات تأمين حفظ المعلومات من مختلف المنصات والعمل على تصحيح أي خطأ من الاخطاء التي قد تهدد أمنها بالإضافة إلى دراسة الأكواد البرمجية الخاصة للتطبيقات للتأكد من سلامتها من البرامج الضارة

6_المخترقون الأخلاقيون : هذا الأمر حيث دفع كثير من الشركات توظيف عدد من خبراء الاختراق الأخلاقي، أي أنهم لا يقومون بعمليات الاختراق لأغراض تخريبية أو بداعي السرقة، حيث يتضمن مجال عملهم الرئيسي هو كشف ثغرات أمنية تجعل المعلومات عرضة للهجمات السيبرانية، وجعل مختصي أمن المعلومات على دراية بها مما يساعدهم على إصلاحها.

تدابير أمن المعلومات

يتضمن امن المعلومات مجموعة من التدابير الاتية:(**تدابير امن المعلومات، 2023**)

1_الاهتمام بالكفاءات البشرية: اختيار مسؤولي الأمن السيبراني من ذوي الخبرة، أي توظيف الشركة واختيار أفضل المرشحين من أجل ملئ مناصب خبراء امن المعلومات، حيث يفيد هذا الأمر في تعزيز الأمن في حال تمتع المسؤولين عن تطبيق أمن البيانات بالخبرات الكافية التي تساعدهم على تفادي الهجمات السيبرانية.

2- تعزيز الأمن الرقمي : يتمثل في اعتماد الشركات والمؤسسات على تثبيت وتنصيب أحدث الاصدارات من برامج الحماية من الفيروسات، بالإضافة الى استخدام برمجيات الجدار الناري الأمر الذي يساهم وبشدة حماية ومساعدة خبراء أمن المعلومات في حماية سرية للمعلومات و حذف البرامج الضارة فور تنزيلها.

3- رسم الخطط المادية: من اهم تدابير امن المعلومات رسم خطط مادية التي تنوي المؤسسات والشركات رصدها لحماية المعلومات، الأمر الذي يعني أختيار الخبراء والبرمجيات التي تتناسب مع إمكانيات الشركة المادية وتقديم دورات وندوات تدريبية أفضل للموظفين.

4_ تدابير التنظيم والتخطيط : تقدم تدابير التنظيم إمكانية رسم هيكلية شاملة لبرامج المعلومات ، حيث يعني ذلك هو تحديد صلاحيات كل من الأفراد المخول لهم بالوصول الى المعلومات.

ثانيا: سياسة أمن المعلومات (Information Security Policy)

مفهوم سياسة امن المعلومات

هي عبارة عن وثيقة تحتوي على مجموعة من القواعد والارشادات التي توجه الافراد الذين يعملون مع أصول تكنولوجيا المعلومات لاتباع إجراءات أمن المعلومات في المؤسسة، وتضمن هذه السياسة أن المعلومات الحساسة لا يمكن الوصول إليها إلا من قبل المستخدمين المصرح لهم، ويتم ذلك من خلال تطبيق الاجراءات والارشادات الموجودة في وثيقة أمن المعلومات .**(مفهوم سياسة امن المعلومات،2023)**

ويعرف ايضا بأنه مجموعة من المبادئ والتعليمات المكتوبة التي توجه عمل المؤسسة لتحقيق أهدافها ،ويجب أن يلتزم جميع العاملين بهذه السياسة من خلال تطبيق القواعد والإجراءات التي تتبع هذه السياسة واتجاهاتها العامة وسياسة امن المعلومات هي مجموعة من القواعد والقوانين التي يتم تطبيقها من اجل حماية معلومات المؤسسة من التخريب والاستخدام الغير مصرح به . **(اللوزي،2008،ص132)**

أهمية سياسة أمن المعلومات

لسياسة امن المعلومات اهمية كبيرة في المؤسسات يمكن تلخيصها كالاتي:

1_يمكن عن طريق سياسة أمن المعلومات تقويض العاملين في المؤسسات بمهام حماية البيانات والمعلومات المخزنة في الخوادم .

2_تعمل على تحديد أهداف المؤسسات التي تعتمد على المعلومات وتمثل الجامعات جزأ منها.

3_يتم من خلالها تحديد موارد المعلومات المهمة التي قد تكون ذات قيمة للمؤسسة وغاية سياسة أمن المعلومات حماية تلك الموارد من حالات الاختراق والهجوم **(رشيد حميد مزيد، حيدر جواد كاظم،2022 :مجلة الدراسات المستدامة ،مج4 ،ع1،.ص344)**

4_يمكن اعتبار هذه السياسة بمثابة مرجع أساسي يتم الرجوع إليه حال تعارض عملية حماية المعلومات مع بعضها البعض او غيرها من العمليات .

5_تحديد سياسة أمن المعلومات مهام العاملين في المؤسسات في ما يتعلق بحماية المعلومات .

6- تحدد هذه السياسة واجبات فريق العمل المكلف بعملية حماية المعلومات.(**القحطاني،2015 :ص188)**

أهداف سياسة أمن المعلومات

لسياسة امن المعلومات مجموعة من الاهداف تسعى لتحقيقها في المؤسسات وهي كالاتي:

1- ضمان حماية جميع البيانات والمعلومات داخل المؤسسة الى المستوى المناسب من خلال توفير بيئة أمنة للبيانات والمعلومات المخزنة في الخوادم.

2- التكامل بين سياسة أمن المعلومات واستراتيجية المؤسسة.

3- أن تحصل المؤسسة على متطلبات سياسة أمن المعلومات الخاصة بها من خلال معرفتها بالمخاطر التي تتعرض لها.

4_ان توفر هذه السياسة مستويات متعددة من الحماية لضمان استمرارية عمل الخوادم حال تعرضها لكوارث أمنية.(**الدنف، أيمن محمد فارس.واقع ادارة امن نظم المعلومات في الكليات التقنية بقطاع غزةوسبل تطويرها._ رسالة ماجستير: غزة الجامعة الاسلامية،2013.ص88)**

5_التأكد من أن جميع المستخدمين في المؤسسات على دراية بهذه السياسة والامتثال لها بما في ذلك السياسات الفرعية وجميع التشريعات الحالية،والتأكد من أن جميع المستخدمين يفهمون مسؤولياتهم الخاصة لحماية سرية وسلامة البيانات التي يتعاملون معها.

6_حماية المؤسسة من الضرر من خلال إساءة استخدام المعلومات.

(information Security Policy ,2023)

7- ترجمة وتوضيح الأمن كما تم تعريفة بالقواعد والمبادئ والأهداف العليا للمؤسسة وتحديد الأليات التي يتم من خلالها تنفيذ وتحقيق المسؤوليات والواجبات لكل مستخدم .

8- تعريف المستخدمين بمسؤولياتهم وواجباتهم تجاه أمن المعلومات الذي يتضمن الأفراد والأجهزة والبرامج والمعلومات،والتخلص من المعلومات الضارة بطريقة آمنة. **(النجار،2010:ص270)**

أنواع سياسة أمن المعلومات

قد تختلف وتتنوع سياسة أمن المعلومات من مؤسسة إلى أخرى ومن جامعة إلى أخرى ويختلف مضمونها تبعا لاختلاف طبيعة الاعمال المكلفة بها،وفيما يلي أنواعها كالاتي:

1_سياسة الأمن المادي: تتضمن الحفاظ على أمن وسلامة المعلومات من مواردها الاصلية تجنبا لتعرضها لأي تهديد تتعرض له المعلومات وقد تكون تهديدات من اشخاص يحاولون الوصول للمعلومات والعبث فيها أواشخاص مسؤولين عنها من خلال استخدام برمجيات تحمل فيروسات ،ومهما كان نوع التهديد تحاول هذه السياسة حماية المعلومات من الاختراق.

2_سياسة كلمات المرور: يكون تركيز سياسة كلمات المرور في الحفاظ على أمن وسلامة البيانات والمعلومات المخزنة فيها من خلال أتخاد إجراءات احترازية وتعزيز أمن المعلومات بإستعمال كلمات مرور تمنع الوصول الى المعلومات من غير المخولين وتؤكد سياسة كلمات المرور على ان تكون كلمات المرور لايمكن تخمينها من قبل المخترقين بما يضمن حماية المعلومات والحفاظ على سريتها .

3_سياسة تحديد الهوية : وتشمل كافه الوسائل التي تمنع الوصول المعلومات وقواعد بياناتها مثل المقاييس الحيوية، وأنظمة الحماية البيئية التي يمكن ان تمنع الوصول الى الاجهزة الخادمة.

4_سياسة الحماية الفنية: تتعلق بوسائل خاصة بحماية الأجهزة وبرامج نظم التشغيل وبرامج التطبيقات وشبكات الاتصال، وسياسات برامج الحماية والجدران النارية، وسياسات التحكم بالوصول ، وسياسة إدارة أصول المعلومات والمستخدمين، تشفير البيانات، وسياسات التعامل مع البريد الالكتروني.

5. سياسات تقدير المخاطر: وتشمل تقدير المخاطر والتهديدات التي تتعرض لها معلومات المؤسسة نتيجة قلة الخبرة والوعي والتدريب وعدم توافر اوضعف الأدوات والأجهزة والبرامج المستخدمة في عملية حماية المعلومات وكشف حالات الاختراق والتهديد.**(الشيتي ،2010: المجلة المصرية للمعلومات._مج11،ع5،،ص 16)**

6- سياسة النسخ الاحتياطي: تتضمن عملية نسخ من البيانات والمعلومات على أجهزة منفصلة أونسخة من البيانات في مكانين مختلفين بحيث يمكن استرجاع البيانات من النسخة الاحتياطية في حالة فقدان الملفات اوالبيانات لاي سبب مثل انقطاع الكهرباء اوتلف القرص الصلب.

7_سياسات مضاد الفيروسات: تتضمن مهمتها عندما يصاب ملف بفيروس ما نستخدم برنامج مكافحة الفيروسات لتعقيم وتنظيف الملف وازالة الفيروس منه، أي أن تعقيم الملف يعني إزالة الفيروس ويوجد العديد من برامج مكافحة الفيروسات ضمن الملفات الموجودة في جهاز الحاسب الآلي لدينا بعملية الفحص او المسح **(أبو العزم،2012 : ص 123 _124)**

8- سياسة حماية أمن الشبكة : من الاساسيات في حقل أمن المعلومات حماية المعلومات الخاصة التي تنقل عبر الشبكات الحاسوبية او النقالة، وهذا الأمر يتكفل به أمن الشبكات ، ويقصد به مجموعة الإجراءات المضادة التي تكفل إدخال المعلومات الرقمية الخاصة المشتركة المعدة للنقل في وضع الأمان عند مرورها عبر شبكه

غيرأمنه "وتتمثل مجموعة الاجراءات المضادة في حماية الشبكة نفسها وفي حماية المعلومات الخاصة التي تمرعبرها ،ويؤدي أمن الشبكات دوره لحماية المعلومات الخاصة في المحيط الالكتروني **(الخالدي،2018:ص60)**

مراحل سياسة أمن المعلومات

تتكون سياسة أمن المعلومات من عدة مراحل وهي كالاتي:

1_مرحلة انشاء السياسة الأمنية: تعد مرحلة انشاء سياسة امن الخطوة الأولى والتي تتضمن دراسة الجدوى من بناء السياسة والتوافق والتخطيط والبحث والتوثيق .

2_المراجعة: تتضمن هذه المرحلة قيام المسؤولين عن إعداد سياسة أمن المعلومات بإجراء المراجعة و التقييم قبل اعتمادها وقبولها بالشكل النهائي .

3_ الموافقة: وهي المرحلة التي يتم من خلالها إبداء المسؤولين موافقتهم عن رسم السياسة الأمنية للمؤسسة والسماح بتنفيذها بشكل رسمي.

4_مرحلة الاتصال: وهي التي يتم فيها نشر وتوزيع بنود وتعليمات سياسة أمن المعلومات على العاملين في المؤسسة والذين سوف يعملون ضمن هذه السياسة .**(Patrick,2002:p2)**

5_مرحلة التدريب والتوعية :يتم فيها تدريب وتوعية العاملين على سياسة أمن المعلومات التي تتبعها المؤسسة، اذ أن وجود مثل هكذا برامج يعد أمرا ضروريا وفي غاية الأهمية ويجب ان تكون هذه البرامج دائمة ومستمرة لتصل إلى أهدافها وهي مساعدة وتطوير العاملين على الفهم الواضح لواجباتهم مع ضرورة أعلام العاملين بخصوص اي سياسة أمن معلومات جديدة .

6- مرحلة فرض التنفيذ: إن مرحلة فرض تنفيذ سياسة أمن المعلومات يتم عن طريق توعيتهم والزام العاملين بضرورة تنفيذ هذ السياسة ومعاقبة كل من يخالف السياسة المتبعة حيث ان العاملين في حال لم يواجهوا العقاب قد يتمادوا في السلوك السلبي، والذي ينعكس على أمن وسلامة المعلومات . **(Ferranti,2012: p67)**

7_مرحلة المراجعة والتحديث: مرحلة مهمة من مراحل تكوين سياسة أمن المعلومات حيث ان السياسة الأمنية تحتاج إلى تطوير وتعديل بصورة دورية نتيجة التطور السريع في تقنيات الحماية المستخدمة في حماية المعلومات والتطور المستمر في أعمال الجامعات ويفضل ان تتم عملية التحديث من قبل فريق عمل أولجنة متخصصة في مجال أمن المعلومات توكل إليهم هذه المهمة .**(الشبلي،2009: ص 346)**

العوامل المؤثرة على سياسة أمن المعلومات

هناك مجموعة من العوامل الداخلية والخارجية المؤثرة في سياسة أمن المعلومات تتمثل هذه العوامل بماياتي: **(Knapp & et al, 2009:p.493)**

1_العوامل الداخلية: يمكن تمثيل العوامل الداخلية اليومية لسياسة امن المعلومات بالإدارة العليا للعاملين في المؤسسات والبنية التحتية التقنية و التهديدات الداخلية والتي تشمل العاملين في المؤسسة.

2- العوامل الخارجية: تتمثل العوامل الخارجية التي تؤمن سياسة أمن المعلومات في القطاع الاقتصادي والمتطلبات القانونية والتشريعية الخاصة بحماية المعلومات من التهديدات الخارجية.

مكونات سياسة امن المعلومات

تتكون سياسة أمن المعلومات من أربعة مكونات أساسية وهي كالاتي:

1_العمليات:هي انشطة واجراءات مسموح بها وغير مسموح بها من تنصيب وتحديث للاجهزة

2_الافراد: (الفنين_المهندسين-المستشارين-فريق الدعم التقني)الذين ينفذون العمليات والخدمات والتي يحتاج تواجدهم بإعداد وتخصصات ملائمة وبخبرات عالية في مجال أمن المعلومات.

3_التكنولوجيا:أي التقنيات المستخدمة في عمليات الخزن والحماية من أجهزة وبرامج حيث يتوفر في سوق العمل عدد كبيرمن المنتجين والموردين والبائعين والموزعين لهذه التقنية .

4_ المعايير: بما أنه لا يمكن أن نضمن حماية للمؤسسة بنسبة 100% لذلك نحن بحاجة الى وضع مجموعة من المقاييس التي يمكن من خلالها تحقيق مستوى ملائم من الأمن ومن أهم المعايير العالمية التي تساعد على تحقيق أمن المعلومات هو الأيزو (ISO).

متطلبات سياسة أمن المعلومات

توجد مجموعة من المتطلبات الخاصة بسياسة امن المعلومات وهي كالاتي:

1_ان تتوافق مع أسلوب أداء الموظفين لاعمالهم لأمن المعلومات وتعاملهم مع العالم الخارجي.

2_أن تلبي المتطلبات القانونية لسياسة وبنية المؤسسة.

3_أن تراعي العوامل الاجرائية لذلك في بعض الأحيان يتم الضحية في بعض المتطلبات الأمنية مقابل تيسير سير العمل في المؤسسة.

4 . أن تكون القيود معقولة بحيث لا يمكن ان تمنع المستفيدين من استخدام أجهزة الحاسوب لديهم بشكل يخدم المؤسسة وبطريقة غير مباشرة .

مسؤولية اعداد سياسة امن المعلومات

لكي تكون سياسة أمن المعلومات فعالة وناجحة وقادرة على تحقيق اهدافها لابد ان يسهم في إعدادها وتنفيذها مراتب وجهات بمستويات وظيفية مختلفة في المؤسسة الواحدة وان تلبي حاجتها من التعاون إلى الدعم والاسناد الكامل ويمكن تصنيف هذه الجهات بما يأتي: **(Information Security Standards,2024)**

1 – الإدارة العليا في المؤسسة .

2_الإدارة القانونية في المؤسسة .

3_مديرو الوحدات المختلفة في المؤسسة .

4_مسؤولو أمن المواقع الإلكترونية .

5_مديرو الشبكات المسؤولون عن تجهيز خدمة الانترنت.

بينما صنف الشبلي المعنيين بسياسية أمن المعلومات إلى ثلاث فئات وهم كالاتي:

1_الإدارة : وتكون مسؤولة عن حماية المعلومات والتكلفة المصاحبة لها.

2_موظفو الدعم الفني: وهم الاشخاص المسؤولون عن تنفيذ وتعديل السياسة عندما تكون هناك حاجة لذلك.

3_المستخدمون: وهم الاشخاص الأكثر تأثيرا وتعاملا مع سياسة أمن المعلومات.

طرق اختراق أمن المعلومات

لا يمنع وجود نظام أمني متكامل لحماية تكنولوجيا المعلومات من التعرض لهجمات الهاكرز من وقت لأخر، ولاسيما أن النظام العام لهذه التكنولوجيا يعد العنصر البشري فيه مكون أساسي من مكوناته، وكون الأخطاء البشرية هي الأكثر تسببًا في حدوث الاختراقات الأمنية لتكنولوجيا المعلومات يمكن ان نبدأ أول طريقة لاختراق أمن المعلومات كالآتي: **(طرق اختراق امن المعلومات،2023)**

1_التعرض للتجسس: من خلال تحميل برامج ووسائط من مواقع غير آمنة تسبب بتحميل برامج خبيثة تسمح لطرف آخر بمراقبة وتسجيل أنشطة المستخدم دون أن يمنح له الآذن.

2_التعرض لهجمات ال (Scare Ware): وهي هجمات تظهر في صيغة تنكرية الهدف منها مساعدتك على إصلاح النظام، إنما في الحقيقة هي من تسبب في تدميره وإتلاف البيانات الهامة.

3_التعرض لفايروس الفدية: وهي هجمات شهيرة تتسبب في التحكم الكامل على قواعد البيانات والمعلومات التي يمتلكها المستخدم وتشفيرها مقابل حصوله مبلغ مالي مرتفع من الضحية.

4_التعرض لهجمات الجذور المخفية: وهي هجمات دقيقة للغاية، حيث تستهدف الوصول إلى البيانات الخفية والحساسة للغاية في الأنظمة التي يتم مهاجمتها، بحيث يمكن ان تصل إلى جذور النظام بشكل كامل ومن ثم تقوم بالسيطرة عليه بحرية.

5_التعرض لهجمات الزومبي: هي شكل من أشكال التجسس لا تنشط الفايروسات إلا بمنح المتسللين الأمر لها بذلك، أي يمكن أن يوجد على نظامك واحدة منها خامدة لا تنشط اليوم ولا شهر ولا سنة، لكن فجأة وبدون مقدمات، تجد نفسك منتهك لخصوصيتك بسبب رغبة المتسلل.

6_هجمات الهندسة الاجتماعية: وهو نوع من الاحتيال الذي يعتمد على ألفة المستخدمين لمجموعة من الأسماء والشعارات والمواقع، وكذلك يقومون باستخدام هذه الألفة في دفعهم إلى زيارات روابط غير آمنة تجعلهم عرضة للاختراق بكل سهولة.

7_هجمات التهديد المستمر أو ما يعرف بالـ(APT): وهي من أنواع الاختراق لأمن المعلومات، اذ يقوم الهاكر بمراقبة النظام والبقاء فيه لفترة طويلة بدون أن يتسبب في تعرضه للتلف ،في الحالات التي يمتلك فيها النظام المخترق ملفات مهمة وحساسة للغاية، إذ يقوم المخترق بتخزين هذه المعلومات وجمعها ويقوم باستغلالها فيما بعد، سواء بتسريبها للعامة أو بيعها.

8_هجمات الـ (DDOS): وهي نوع من الهجمات التي تستهدف التسبب بأضرار كبيرة للخوادم الخاصة بالبيانات، إذ تسبب نوع من الزيادات الغير متوقعة في حركة المرور فيها أو في إجراء سلوكيات غير طبيعية في النظام، أو رفض الخدمة الموزعة إلى شبكات أخرى أو الإبطاء فيها.

9_التهديدات المتعلقة باستخدام الروبوتات الخبيثة: وهي نوع من البوت التي يستهلك ثغرة أو نقطة ضعف ما في النظام المستخدم، ويقوم بإلحاق الضرر بكافة الأجهزة المتصلة بهذا النظام عن بعد، سواء بالسيطرة عليها ومراقبتها، أو بتعريضها للإتلاف أو التخريب المتعمد.

10_التهديدات الداخلية: وهي التهديدات من الأشخاص المخول لهم بالوصول إلى المعلومات الحساسة على الأنظمة وسرقتها وتسريبها للعوام.

11_ضعف أساليب الحماية المستخدمة في الأنظمة السحابية وكذلك سهولة التعرض لخداع عمليات الاحتيال التي تعتمد على المحاكاة الافتراضية لأنظمة التخزين.

كيفية الحماية من هجمات المخترقين

طبقًا لما أوردته (globe newswire) فإن التكلفة الإجمالية التي يمكن أن تتكبدها الشركات بحلول عام 2025م، بسبب الهجمات الإلكترونية قد تصل إلى أكثر من 10.5 تريليون دولار سنويًا، وهو رقم لا يعد مستحيلًا إذا ربطت بين هذه التوقعات، وما بين إحصائيات الجرائم الإلكترونية المتزايدة لما يفوق الـ 600% منذ انتشار فيروس كورونا، وبالرغم من زيادة التشريعات التي تفرضها الدول للحفاظ على الأمن المعلوماتي والحد من الهجمات التقنية والسيبرانية ، إلا إن عالم الهاكر في تطور هو الأخر يكون موازي أو يتقدم بخطوات عن عالم الحماية وأمن المعلومات، وهذا التقدم لا يرجع لضعف الأخير إنما راجع لضعف الاهتمام العام بهذا المجال رغم أهميته سواء من الناحية الأخلاقية لما تمثله المعلومات من خصوصية، أو من الناحية المالية والسياسية التي تصبح فيه تداول بعض المعلومات بمثابة خطر قومي عام من خلال تطبيق هذه النصائح ستساهم أنت في أن

تكون ضلعًا فعال في مقاومة هذه الهجمات والمساهمة في زيادة الوعي الأمني والثقافي لما يخص أمن المعلومات وهي كالاتي: **(كيفية الحماية من هجمات الهاكرز،2023)**

1_تحديد الجهات المخول لها الوصول الى المعلومات واستخدام إجراءات معينة للتأكد من عدم الاحتيال وتزييف الهويات والأسماء.

2_استخدام خدمات النسخ الاحتياطي والتخزين السحابي لتوفير نسخة أخرى من المعلومات في حال التعرض لهجمات الغرض منها إتلاف وتخريب المعلومات.

3_تشفير المعلومات بشكل لا يسمح لأي جهة أو شخص الوصول لها إلا للجهات المخولة فقط.

4_الكشف الدوري عن الثغرات والعمل على حلها قبل أن تتضخم متسببة في حدوث نتائج كارثية قد لا يمكن السيطرة عليها.

5_زيادة الوعي بالثقافة الأمنية للأفراد وتطوير المهارات التقنية الخاصة بهم بحيث لا يتسبب الجهل المعلوماتي في إلحاق الضرر بالأنظمة التي يتعاملون معها.

6_استخدام أكثر من طريقة للمصادقة الآمنة عند الولوج إلى الأنظمة الخاصة.

7_تفعيل جدار حماية قوي للغاية لصد أي هجمات غير متوقعة.

8_تطبيق برامج حماية إلكترونية لاكتشاف الفيروسات والتطبيقات الضارة.

9_التطوير المستمر لتقنيات حماية أمن المعلومات بهدف مواكبتها للتهديدات الحديثة والمحتملة في المستقبل.

التهديدات الممكنة لأمن المعلومات

تتطور التهديدات لأمن المعلومات مع سرعة تطور برامج حماية امن المعلومات وتطور الانترنت مما جعل حصر التهديدات غير ممكنا ولكن تتمثل ابرز التهديدات فيما يلي :

1_الفيروسات:عبارة عن برامج تتسلل الى البيانات المخزونة على المواقع والاجهزة الالكترونية المتصلة بالأنترنت وتحدث ضررا من خلال التأثير السلبي على قدرتهم على العمل بنسب متفاوتة تبعا لقوة الفيروسات ،وتكمن خطورتها في الكثير من الحالات لا يتم ملاحظتها سوى بعد أحداث ضرر بالغ ، ومن أخطر الانواع فيروس روت كيت(rot get)

2_قراصنة الانترنت: عبارة عن محترفين سلبيين في علم البيانات يرسلون قدر كبير من البيانات غير الضرورية المزودة ببرامج ضارة للأجهزة الالكترونية أو الشبكات الالكترونية مما يحد من قدرتهم على العمل بشكل فعال او تدميرهم كليا.

3_ الهندسة الاجتماعية: يعرف مجرمو الانترنيت أن تقنيات التطفل التقليدية لها فترة صلاحية ، لذا فقد تحولوا إلى أساليب غير تقنية، مثل الهندسة الاجتماعية، التي تعتمد على التفاعل الاجتماعي والتلاعب النفسي للوصول إلى البيانات السرية.**(التهديدات الممكنة لأمن المعلومات، 2023)**

4_ ضعف او انعدام التشفير: ليس على مستوى المستخدم الفردي فقط بل حتى في أدق تفاصيل الخدمات التي تقدمها الشركات المتنوعة، على سبيل المثال صناعة "الرعاية الصحية التي تتعامل مع بيانات بالغة الحساسية وتتفهم خطورة فقدانها . **(تشفير المعلومات، 2023)**

وسائل المحافظة على أمن المعلومات

هناك عدد من وسائل الحفاظ على بقاء المعلومة امنة وهي كالاتي: **(وسائل المحافظة على أمن المعلومات،2023)**

1_الحد من مشاركة الأخرين في المعلومات الخاصة مثل : الميلاد والعنوان ورقم الهاتف،ورقم بطاقة الهوية ، والإيميل.

2_استخدام أرقام سرية معقدة جدا بعيدة عن بيانات المعلومات الخاصة مع الحرص على تغييرها بصفة دورية.

3_ تجنب استخدام خاصية تحديد الموقع الجغرافي.

4_عدم فتح الملفات والروابط غير الامنة القادمة من مصدر موثوق فيه.

5_عدم إجراء المعاملات البنكية في الأماكن العامة.

6_تسجيل الخروج من مختلف المواقع بعد انتهاء استخدامها مباشرة وعدم السماح للمتصفح بحفظ بيانات تسجيل الدخول ، بالاضافة الى امكانية مسح ذاكرة المتصفح.

7_إضافة برامج حماية أمن المعلومات على شتى أنواع الاجهزة الالكترونية المتصلة بالانترنت.

8- حفظ نسخ إضافية من البيانات المهمة او السرية.

الجانب العملي
تحليل نتائج المقابلة
اولا : نبذة عن مركز الحاسبة الالكترونية في الجامعة التقنية الشمالية:

لم يكن هنالك جامعة بل كانت هيئة التعليم التقني التابعة لجامعة الموصل والتي تأسست في عام 1979،ولم يكن هنالك مركز للحاسوب في ذلك الوقت، وأستحدث مركز الحاسبة في عام 1998 بأسم مركز الحاسبة الإلكترونية ،حيث بدأ تأسيس الجامعة التقنية الشمالية في عام 2014 ، وانضم اليها مركز الحاسوب ويبلغ عدد العاملين في مركز الحاسبة الالكترونية في الوقت الحالي بمختلف مستوياتهم الوظيفية(22) موظفاً

ويعد مركز الحاسوب مركز خدمي فهو يقدم خدمات علمية والكترونية، كما ان للمركز نشاطات واهداف وهي كالاتي:[1]

1_نشاط المركز:

من نشاطات المركز هو أنجاز العديد من مشاريع طلبة الماجستير والدكتوراه من خلال الحاسوب المركزي وتقديم الاستشارات والدخول على السيرفر، وهو مستمر في تقديم خدماته للأساتذة وموظفي الجامعة والطلبة والباحثين، كما تم ادخال أجهزة الخوادم في مركز الحاسبة الإلكترونية وهي عدد(4)خوادم حيث يتم ادخال قواعد بيانات ومعلومات المركز والجامعة وتمت مشاركتها بشكل الكتروني لخزن البيانات والمعلومات وللحفاظ عليها من التلف والضياع، كما توجد شبكة حواسيب ذات إمكانيات عالية ومواصفات خاصة ذات تقنية متطورة.

2_اهداف المركز:

من اهداف المركز وجود برنامج يتم من خلاله اعداد وتأهيل كادر متقدم من خلال التدريب داخل القطر فقط، حيث تم تزويد المركز من قبل الجامعة بكوادر وكفاءات العلمية بتخصصات علوم الحاسوب وهندسة الحاسوب وهندسة البرمجيات والاتصالات والاختصاصات الساندة الأخرى لغرض الارتقاء بعمل المركز وسرعة تقديم افضل الخدمات، كما تم اضافة اجهزة ومعدات وحواسيب جديدة وبشكل مستمر يتم تجهيز المركز وهي من مقومات نجاح المركز واستمرار عمله على اكمل وجه، حيث بدأ المركز يعتمد بشكل كامل على الحواسيب وشبكاتها منذ عام 2004 والى يومنا هذا، ومن اهداف ومهام مركز الحاسوب نشر المفاهيم الأساسية للحواسيب الإلكترونية داخل الجامعة والمجتمع، حيث بشكل دائمي يصدر كتب وتوجيهات بهذا الخصوص، بالإضافة الى اقامة دورات تدريبية عن برامج وتطبيقات الحواسيب.

يحتوي مركز الحاسبة الالكترونية على (5) شعب مختلفة وهي كالاتي :

1_شعبة صيانة الحواسيب والشبكات:

تعمل في هذه الشعبة كوادر هندسية وفنية كفؤة تشرف على شبكة الاتصالات داخل الجامعة، يبلغ عدد الكادر فيها (5) موظفين في تخصص هندسة الحواسيب ، وتجدر الاشارة هنا إلى أن الجامعة تمتلك شبكة اتصالات واسعة تعتمد منظومة الكيبل الضوئي Fiber Optic داخل الجامعة بحيث تغطي كافة التشكيلات وهدفها ايصال الخدمات في الجامعة بوصفها وسطا لنقل البيانات بين نقاط الشبكة ووصلها بالمنظومة في دائرة الاتصالات في وسط الحرم الجامعي وقد تعددت مهام كادر هذه الشعبة وهي كالاتي: [2]

[1] مقابلة مع السيد انمار برهان مدير مركز الحاسبة الالكترونية بتاريخ2024/5/26.

[2] مقابلة مع السيد عمر محمود عبدالهادي مسؤول شعبة صيانة الحاسبات والشبكات بتاريخ2024/5/26.

1_إيصال خدمة الانترنت إلى جميع اقسام وكليات داخل الجامعة والربط بين تشكيلات الجامعة ومواقعها على كافة مواقع الجامعة والكليات والمعاهد في كركوك وصلاح الدين والحويجة.

2_تشغيل خادم البريد الالكتروني وذلك لربط الكليات ومراكز الجامعة بالدوائر والشعب في رئاسة الجامعة وتأمين التراسل فيما بينها.

3_تنصيب برنامج معالجة الفايروسات (Antivirus) على أجهزة الحواسيب المربوطة على الشبكة وتفعيل انظمة وبرامج وربط السيرفرات.

4- حل مشكلة الخوادم المخصصة للخزن الاحتياطي من خلال تنسيق العمل مع شركات الدعم الفني واجراء الصيانة الدورية للشبكة.

5- معالجة مشاكل مراكز البيانات وتحديث خوادم مراكز بيانات مركز الحاسوب الالكتروني مع تحديث البيانات والمعلومات قبل حزبها في الخادم.

6_صيانة الاجهزة الخاصة بالحواسيب والطابعات في رئاسة الجامعة والتي تضم المكتبة المركزية والكليات والمعاهد التابعة لها.

2_شعبة الموقع الالكتروني :

توجد هذه الشعبة في مركز الحاسوب الالكتروني يبلغ عدد الكادر فيها (3) موظفين في تخصص تكنولوجيا المعلومات وهندسة الحواسيب، من مهام هذه الشعبة التي تم استحداثها في الوقت القريب هي تصميم الموقع الرئيسي للجامعة التقنية الشمالية، وإنشاء المواقع والصفحات الالكترونية التي تقدم الخدمات الإلكترونية للمنتسبين والطلبة و المجتمع كذلك إدارة المواقع الالكترونية للجامعة المتاحة على الخط المباشر على شبكة الانترنت، وتعمل الشعبة أيضا على نقل احدث انشطة الجامعة ،ويوجد اعضاء ارتباط في التشكيلات ولديهم صلاحيات في انشاء الحسابات وادارتها ومنها إنشاء حسابات البريد الالكتروني في الجامعة لكافة الأقسام والشعب والتشكيلات والمؤتمرات الموجودة في الجامعة فضلا عن إنشاء حسابات البريد إلكتروني لطلبة الدراسة الأولية وطلبة الدراسات العليا ضمن برامج التعلم الإلكتروني كجزء منها، وهدف الشعبة هو الحفاظ على نقل احدث انشطة الجامعة وتطبيق الخدمات عبر الانترنت باستخدام احدث التقنيات، ومن الواجبات والمسؤوليات لشعبة الموقع الالكتروني تدريب مطوري مواقع الويب في أقسام ومراكز الجامعة بدورات تدريبية متخصصة، فضلا عن متابعة المواقع الإلكترونية لتشكيلات الجامعة من خلال التقييم الدوري للمواقع الالكترونية، وتطبيق واختبار آخر تحديثات الأمان و الخدمات والأنظمة.[3]

3_شعبة التدريب الفني:

[3] مقابلة مع السيد نور نبيل حازم مسؤول شعبة الموقع الالكتروني بتاريخ 2024/05/27

توجد هذه الشعبة في مركز الحاسوب الالكتروني وتسمى شعبة التدريب الفني التي يبلغ عدد الكادر فيها (3) موظفين في تخصص الحاسوب والاحصاء، تقوم الشعبة بتقديم العديد من الدورات التدريبية داخل الجامعة بمختلف تخصصات الحاسوب والبرمجيات وذلك إسهاما منه في القضاء على الأمية الحاسوبية، إذ شملت هذه الدورات البرامج التشغيلية والبرامج الخدمية والبرامج التطبيقية المساعدة فضلا عن اللغات البرمجية بمختلف أنواعها ، لقد تعدت هذه الدورات منتسبي الجامعة لتشمل منتسبي الجامعات والدوائر التابعة لمحافظة نينوى من خلال مذكرة تفاهم ما بين المحافظة والجامعة وتكون هذه الدورات مجانية وفق مذكرات وكتب رسمية، وقد تميزت هذه الشعبة بإقامة دورات متخصصة في الشبكات الحاسوبية ومعدات الربط وانظمة تشغيل الشبكات يستخدم هذا القسم ثلاث مختبرات مجهزة بأحدث أنواع الحواسيب المحملة بالإصدارات الحديثة للبرامج التدريبية مع استخدام احدث التقنيات في عرض البيانات فضلا عن كون هذه المختبرات مجهزة بالأثاث الحديث بالإضافة الى أجهزة التكييف .[4]

4_شعبة الانظمة والبرمجيات:

تم استحداث هذه الشعبة في مركز الحاسوب عام(2017) ضمن الهيكل التنظيمي الجديد لغرض تصميم واعداد البرامج والانظمة الخدمية والتعليمية والإشراف على قواعد البيانات التابعة للجامعة وتنصيب البرامج والتعريفات لجميع الطابعات المنتشرة في الكليات، ويتألف كادر الشعبة من (4) موظفين في تخصص علوم الحاسوب وهندسة الحواسيب وهندسة الاتصالات والبرمجيات وممن لديهم خبرة جيدة في مجال تحليل وبناء الانظمة ويترأسهم احد اعضاء هيئة التدريس من القسم العلمي في نفس التخصص، لقد شرع هذا القسم بتقديم خدماته لكليات ومؤسسات الجامعة من خلال بناء بعض انظمة ادارة قواعد البيانات نذكر منها نظام الترقية العلمية في رئاسة الجامعة ، نظام الدورات ،وتوزع المهام بين اعضاء هذا القسم تحقيقا لمبدأ العمل الجماعي) ويقوم الأعضاء بمتابعة تطبيق الانظمة والبرامج عند استعمالها من الجهات المستفيدة منها مع اجراء التحديثات عليها بما ينسجم والتغييرات الحاصلة في شكل البيانات والتعليمات الادارية والتقارير المطلوبة، كما ان الشعبة مسؤولة عن السيرفرات في الجامعة وتنصيب برامج الحماية للمعلومات، بالإضافة الى تسجيل الطلبة وادارة معلوماتهم ونتائج الطلبة، وإحصائيات وبرنامج الترقيات، وشؤون المواطنين ،والصحة النفسية، وبرامج كفاءة الحاسوب ،واستمارات طلبات الشراء للأنظمة والبرمجيات .[5]

[4] مقابلة مع السيد عمر فوزي مسؤول شعبة التدريب الفني بتاريخ2024/5/28.
[5] مقابلة مع السيد مهند لقمان احمد مسؤول شعبة الانظمة والبرمجيات بتاريخ2024/5/28.

5_شعبة الشؤون الإدارية :

تعد هذه شعبة من الشعب المهمة والحيوية لما لها من أهمية في متابعة شؤون الأفراد والحفاظ على حقوقهم، اذ بلغ عدد الكادر فيها (2) موظفين في تخصص هندسة الحاسوب وانظمة الحواسيب ، كما بلغ عدد العاملين في المركز بمختلف مستوياتهم الوظيفية (22) موظفاً ،تتمثل مهام الشعبة بتنظيم الشؤون الادارية الخاصة بالمركز ومتابعة سير العمل واصدار الأوامر الإدارية مثل الاجازات والترفيعات، وإعلام العاملين بما يصدر من الإدارة العليا في الجامعة من توجيهات وتعليمات ومخاطبة كافة دوائر الدولة، وتتابع في المركز شؤون الشعب وأعمالها الفنية واعداد الكتب والمذكرات الرسمية وتشكيل اللجان الفنية المتعلقة بأعمال المركز واصدار الأوامر الإدارية الخاصة بمنتسبي المركز وبهذا يكون دورها واضحا في عمل المركز، ومن أهم الوحدات التي تضمها شعبة الشؤون الادارية وحدة الخدمات، وتعد من أكبر وأهم الوحدات في المركز اذ تقوم بالعديد من الاعمال المكلفة حيث توفر الخدمات للطلبة وللمنتسبين داخل وخارج الجامعة ودوائر الدولة والقطاع الخاص، وتوفر دورات في مجال التكنولوجيا والاتصالات والحواسيب والالكترونيك، وانترنت الاشياء والشبكات، وكفاءة الحاسوب للدراسات العليا للتخصصات العلمية والانسانية، ويضاف لمهام عملها ما يسمى بالاختبار الوطني، ويوجد تعاون مع مجلس الخدمة الاتحادي وفق قوانين الدولة اذ يتحتم على اي شخص متقدم للتعيين وفق ضوابط المجلس يخضع لاختبارات تقام من قبل المجلس، حيث توزع المتعينين على مراكز الحاسوب في الجامعة اذ يتم اجراء اختبار لهم قبل التعيين ،بالإضافة الى التعاون مع وزارة العمل لدعم دور الايتام في توفير نوع من الزيارات العلمية والدورات المجانية، والتعاون مع وزارة التربية في توفير مجالات عمل للطلبة الموهوبين .

ومن الأعمال التي يقوم بها المركز استخدام الخوادم لخزن البيانات والمعلومات الخاصة بالجامعة وتشمل بيانات الطلبة الجدد، كما يتم خزن برامج وتطبيقات وانظمة ومنصات القبول المركزي الالكتروني الخاص بالجامعة للطلبة الجدد الذين يتم قبولهم في الدراسة الأولية، وتحتوي أيضا برامج التخطيط والتدقيق الخاص بمنتسبي الجامعة، وتحتوي أجهزة الخوادم على

انظمة تشغيل وتفعيل التطبيقات والروابط مثل (HTTP) كذلك يتم في الخوادم خزن وتفعيل اليوزرات (user) التي يتم التعامل معها سواء للطلبة أو الاساتذة اثناء التعليم المدمج. [6]

ثانيا : تحليل اسئلة المقابلة:

قسمت تلك الاسئلة الى عدة محاور ، وهي كالاتي:

المحور الاول: سياسة امن المعلومات:

1_هل لمركز الحاسوب سياسة امن المعلومات الفعالة وفقا للمعايير الدولية ؟

[6] مقابلة مع السيد محمد سامي نوري مسؤول شعبة الشؤون الادارية بتاريخ2024/5/29.

تبين خلال المقابلة ان لدى مركز الحاسوب الالكتروني سياسة واضحة لأمن المعلومات يتم اتباعها وفق معايير دولية بالإضافة الى اجراءات لازمة وفعالة لدى المركز، كما ان لدى ادارة الجامعة الرغبة في تطبيق سياسة امن المعلومات التي تهدف الى حماية البيانات والمعلومات.

2_ما مدى توافق سياسة أمن المعلومات مع التقنيات المستخدمة لحماية المعلومات؟

تبين ان لدى سياسة أمن المعلومات توافق مع الاجهزة والتقنيات المستخدمة في حماية المعلومات وان لديها اجهزة خاصة بأمن المعلومات، وتعتبر سياسة امن المعلومات حجر الاساس الذي تنطلق منه العمليات والانشطة التي من شأنها حماية المعلومات.

3_مامدى ادراك الجامعة لسياسة امن المعلومات واهميته؟

يوجد اهتمام والمام من قبل الجامعة بأهمية سياسة امن المعلومات وتم تكثيف الجهد وتم تشكيل لجان بهذا الخصوص، وتم تطبيقها لحماية البيانات والمعلومات المخزنة لديها من الهجمات التي

قد تتعرض لها المعلومات، حيث من واجب سياسة امن المعلومات هو تخفيض المخاطر التي قد تتعرض لها المعلومات.

4_هل يتوفر تقييم دولي للالتزام بتطبيق سياسات أمن المعلومات ؟

حيث توجد مراقبة للسيرفرات ومراجعتها بشكل دوري وتقييم لبيان مدى التزام المركز بتطبيق سياسة أمن المعلومات عند تعرضها لحالات الاختراق وفي بعض الاحيان عندما نتعرض لهجمات واختراقات مستمرة من المحافظات ومن خارج العراق حيث يتم اطفاء السيرفرات، كما لدينا طرق فحص واستخدام الذكاء الاصطناعي ونحن بصدد اضافة طبقة اخرى من (Security) الامن ولكنها مكلفة للغاية بالإضافة الى انها تحتاج الى موافقات رسمية.

5_هل تتوفر الخوادم اللازمة والموافقة لسياسة أمن المعلومات في الجامعة؟

حيث تبين انه يتوفر أجهزة الخوادم والتقنيات الملازمة لحمايتها بما يتوافق مع سياسة أمن المعلومات في الجامعة ،وهناك اجراءات وقائية يتبعها المركز عند فتح غرفة السيرفر حيث يأتي اشعار مباشر على جهاز موبايل مدير مركز الحاسبة.

6_ما مدى مساعدة سياسة أمن المعلومات في تقليل المخاطر للمعلومات في الجامعة؟

تبين من خلال المقابلة انه يساعد وجود سياسة أمن المعلومات في تقليل المخاطر التي يمكن ان تتعرض لها المعلومات في الجامعة كحد ادنى لحماية البيانات والمعلومات المخزنة والوصول إلى غرف الخوادم ونظام IDS,IPS لكشف تلك الحالات ومنعها بالإضافة الى وجود بصمة يد وباسوورد.

7_ من الجهة المسؤولة عن رسم سياسة أمن المعلومات في الجامعة ؟

اتضح انه لم يتم تحديد سياسة أمن المعلومات بشكل واضح من قبل الإدارة العليا في الجامعة بالتعاون مع مركز الحاسوب الالكتروني ويكون العاملين ليس على علم بسياسة أمن المعلومات التي يتبعها المركز من اجل القيام بأعمال المركز على اكمل وجه.

المحور الثاني :برامج الحماية لأمن المعلومات: والذي تضمن الاسئلة الاتية:

1_ما الاجهزة المستخدمة لتحقيق كفاءة أمن المعلومات عالية؟

حيث يوجد اجهزة وبرامجيات (Software و Hard were) ،بالإضافة الى استخدام مركز الحاسبة الالكترونية اجهزة جدار النار من اجل تحقيق كفاءة اعلى في مجال أمن المعلومات وحماية المعلومات والبيانات من التسلل والاختراق.

2_هل تتوفر برامجيات خاصة لعمل نسخ احتياطية لمعلومات الجامعة؟

تبين انه يعمل المركز على توظيف البرامجيات الخاصة بعمليات النسخ الاحتياطي كإجراء احترازي لتعزيز أمن وسرية المعلومات المخزنة واسترجاعها حيث يقوم المركز بعملية نسخ احتياطي كل اسبوعين، بالإضافة الى النسخ في اوقات التقديم للدراسات العليا والاولية.

3_هل تتوفر اجراءات تقنية حديثة لحماية تطبيقات امن المعلومات وخوادمها؟

تبين انه في مركز الحاسوب الالكتروني على مدار السنة يوجد تحديث مستمر وهناك خطط ايضا لتحديث الأجهزة والبرامجيات والتطبيقات المستخدمة في حماية أمن المعلومات والخوادم من خلال سياسة استخدام كلمات المرور التي يتبعها المركز وعدم الافصاح عنها لأي سبب وبأي طريقة كانت.

4_ما الوسائل المستخدمة للتحقق من هوية المستخدم الداخلي لنظام المعلومات؟

حيث تبين ان مركز الحاسوب الالكتروني يقوم باستخدام وسائل حماية التعريف للتحقق من هوية المستخدم قبل عملية الدخول إلى نظام المعلومات الخاص بالمركز، وان مواكبة المركز للتطور التكنولوجي المتسارع والتغييرات المستمرة في عملية حماية البيانات والمعلومات ساعدت في ادخال كل ما هو جديد من اجل حماية المعلومات .

5_ما الوسائل المستخدمة في تبادل وحماية المعلومات المخزنة في الخوادم؟

تبين ان مركز الحاسوب الالكتروني يعمل على استخدام سياسة التشفير مثل التوقيع الرقمي في تبادل المعلومات أو انظمة كشف الاختراقات قبل حدوثها لحماية البيانات والمعلومات المخزنة في الخوادم من الاختراق وعدم الافصاح عنها.

المحور الثالث: الحماية المادية والبنية التحتية لسلامة أمن المعلومات: والذي تضمن الاسئلة الاتية:

1_ما المتطلبات الأمنية اللازمة لحماية خوادم المعلومات ؟

اتضح ان المركز يعمل على توفير بعض الاحتياجات الأمنية اللازمة ومنها (الاقفال الالكترونية عن طريق بصمة اليد– بطاقات الدخول الالكترونية)لحماية الخوادم الخاصة بها من أي تدخل خارجي او دخول غير مصرح فيه قد يؤدي الى التسلل وتعطل الخوادم والحاق الضرر فيها.

2_ ما اسس اختيار وسائط التخزين المعلومات وللنسخة الاحتياطية؟

ان المعيار او الالية المعتمدة في اختيار وجودة وسائط التخزين للنسخ الاحتياطي يتضمن معيارين وهما المعيار الاول النسخ المحلي والمعيار الثاني يتم الخزن على الحوسبة السحابية، والتأكد من كفاءتها وكفاية العمر الافتراضي لوسائط التخزين المستخدمة قبل اخذ النسخ الاحتياطي للمعلومات مع توفير اجهزة (USP) للحفاظ على المعلومات اثناء عملية النسخ.

3_ما مدى توفر شبكة اتصالات حديثة وفعالة للوصول المباشر إلى خوادم المعلومات ؟

تبين انه تتوفر في المركز شبكة اتصالات حديثة يستخدمها المركز وتم تطويرها حيث تدعم واي فاي6 وهي شبكة فعالة قادرة على الوصول السهل والسريع إلى الخوادم التي تخزن المعلومات بداخلها.

4_هل تتوفر اجراءات السلامة لحماية غرف خوادم المعلومات؟

تبين انه تتوفر بعض المتطلبات في المركز منها منظومة التبريد واجهزة مكافحة الحرائق واكتشافها والأجهزة والمعدات المتخصصة في عمله لحماية غرف الخوادم من الحالات الطارئة والكوارث ولزيادة كفاءة وضمان عمل الخوادم .

5_ما تقنيات المراقبة المستخدمة لحماية غرف خوادم المعلومات ؟

اتضح ان المركز يستخدم فقط أجهزة الانذار المبكر لحماية غرف الخوادم للتقليل من تعرضها للخطر، اما تقنيات المراقبة مثل الكاميرات حيث ان المركز بصدد الشراء للخادم فقط، وان ادارة الجامعة حريصة على توظيف تقنيات الحماية المختلفة مثل الكاميرات واجهزة الانذار المبكر للحفاظ على امن وسرية المعلومات.

<u>المحور الرابع</u>: ادارة الخطر: والذي تضمن الاسئلة الاتية:

1_هل تتوفر خطط ادارة الأزمات والمخاطر المتعلقة بأمن المعلومات؟

تبين ان المركز قد قام بتوفير خطط مسبقا لصد اي هجوم من قبل القرصنة مثل البرامج التي تراقب الهجمات لمواجهة الأزمات والطوارئ والكوارث المتعلقة بأمن المعلومات مثل الهجمات والقرصنة وعند حدوث مثل هذه الهجمات وبشكل متكرر حيث يقوم المركز بإطفاء السيرفرات لمنع دخول القراصنة الى المعلومات والبيانات الخاصة بالمركز والجامعة، وان هذه الخطط هي المنطلق الرئيسي الذي تنطلق منه تحديد سياسة امن المعلومات.

2_ما الخطط المتاحة لدرء مخاطر امن المعلومات والمتوقعة؟

تبين صعوبة عملية تحليل المخاطر للوقوف على جوانب القوة والضعف عند التعامل مع المعلومات حيث انه ليس لدى المركز القدرة والقابلية على تحليل اسباب مخاطر أمن المعلومات والعمل على معالجتها واتخاذ كافة التدابير الامنية ولم يوفر كافة البرمجيات ووسائل الحماية من اجل ضمان حماية المعلومات من الاختراق وعدم التأكد والحذر من عدم حدوثها في المستقبل.

3_ما مدى توفر انظمة الحماية الفعالة لكشف الاختراقات؟

اتضح ان لدى مركز الحاسوب قلة وجود انظمة كشف الاختراق التي تعمل على صد أي هجوم الذي قد يعطل الخدمة حيث يوجد فقط برامج يأتي من خلالها تنبيه على شكل رسالة الى الإيميل من اي موقع غير مصرح به من اي مكان في العالم.

4_الى اي حد تتوفر اجراءات الرادعة لمنع اي نشاط مجهول يعرض امن المعلومات للخطر؟

هناك بعض الاجراءات والمعالجات يقوم باتخاذها المركز لإيقاف أي بريد غير مرغوب فيه وحذفه الذي يمكن ان يعرض أمن المعلومات إلى المخاطر والتهديدات، حيث يوجد مسؤول عن البريد ويتم فلترته بين فترة واخرى، كما يوجد تعليمات وتنبيهات للموظفين على شكل دورات على الايميل وكيفية التعامل مع مثل هذه المخاطر.

النتائج والتوصيات:

اولا: النتائج: بناء على المفاهيم والجوانب التي تناولها الباحث في الجانب النظري من البحث وبعد اجراء التحليل, توصل الباحث الى مجموعة من النتائج:

1. يتبع مركز الحاسوب سياسة واضحة لأمن المعلومات وفق معايير دولية فضلا عن اجراءات فعالة لتقليل المخاطر تتماشى مع رغبة ادارة الجامعة في مجال أمن المعلومات وحمايتها.
2. توفر اجهزة وبرامجيات خاصة بحماية المعلومات من اجل تحقيق كفاءة اعلى لأمن المعلومات والبيانات من التسلل والاختراق.
3. استخدام مركز الحاسوب سياسة التشفير مثل التوقيع الرقمي في تبادل المعلومات أو انظمة كشف الاختراقات قبل حدوثها في الخوادم.
4. توفير بعض الاحتياجات الأمنية اللازمة مثل الاقفال الالكترونية عن طريق بصمة اليد وبطاقات الدخول الالكترونية لحماية الخوادم لمنع من دخول غير مصرح او التسلل إلى الخوادم وتعطيلها.
5. توفر شبكة اتصالات حديثة حيث تدعم واي فاي (Wi-Fi 6) بهف الوصول السهل والسريع إلى المعلومات المخزونة في الخوادم.

6. استخدام المركز لأجهزة الانذار المبكر فقط لحماية غرف الخوادم للتحذير من تعرضها للخطر، مع افتقاره الماس لتقنيات المراقبة مثل الكاميرات.
7. افتقار المركز للقدرة والقابلية على تحليل اسباب مخاطر أمن المعلومات ومعالجتها واتخاذ التدابير الامنية اللازمة.
8. يتيح المركز فقط برامج تحذيرية يتضمن عملها إرسال رسالة الى الإيميل للتنبيه عن المواقع غير المصرح بها من اي مكان في العالم استخدام الخوادم.

ثانيا: التوصيات:

بناءً على النتائج التي توصل إليها الباحث ، يقدم مجموعة من التوصيات وكالآتي :

1. الحاجة لتوفير الاحتياجات الأمنية إضافية لتأمين عمل الاقفال الالكترونية وبطاقات الدخول لحماية الخوادم.
2. توفير تقنيات المراقبة مثل الكاميرات للخوادم، ومتابعتها المباشرة من قبل ادارة الجامعة.
3. ضرورة تذليل الصعوبات لتسهيل تحليل المخاطر ومعالجتها والعمل على تأمين التدابير اللازمة.
4. يتوجب صياغة سياسة امن معلومات مبنية على نتائج تقييم المخاطر والتهديدات الخاصة بحماية المعلومات في الجامعة.
5. ضرورة اجراء الدراسات والبحوث حول السياسات الحديثة لأمن المعلومات ودورها الفعال في حماية المعلومات.
6. إقامة وورش عمل ودورات تدريبية توعوية لننشر الوعي الامني المعلوماتي بين العاملين في الجامعة بكافة مستوياتهم.
7. العمل على تعزيز التعاون بين الجامعات في مجال امن المعلومات وحمايتها من خلال تبادل الخبرات وعقد المؤتمرات والندوات.

1_قائمة المصادر باللغة العربية:

1. أبو العزم، ايهاب.(2012) الرخصة الدولية لقيادة الحاسب الآلي._ طرابلس : دار الحكمة.
2. انواع امن المعلومات.(2023)، متاح في موقع مساواة على الرابط https://www.mosoah.com ، تاريخ الوصول2023/10/27.
3. اهداف امن المعلومات(2023)، متاح في موقع خمسات على الرابط www.blog.khamsat.com تاريخ الوصول 2023/9/19.

4. اهمية امن المعلومات.(2023)، متاح في موقع مجتمع تكنولوجيا المعلومات على الرابط https://www.itcomunity.com تاريخ الوصول2023/9/17 .
5. تاريخ امن المعلومات.(2023)، متاح في موقع سايبر وان على الرابط https://cyberone.com تاريخ15 الوصول /2023/8.
6. تدابير امن المعلومات(2023)، متاح في موقع خمسات على الربط https://blog.khamsat.com تاريخ الوصول2023/10/30.
7. تشفير المعلومات ،(2023)،متاح في موقع اراجيك على الرابط https://www.arageek.com تاريخ الوصول2023/12/7.
8. تطور امن المعلومات.(2023)، متاح في موقع خمسات على الرابط http://blog.khamsat.com تاريخ الوصول 2023/8/16.
9. التطورالتاريخي لامن المعلومات (2023)، متاح في موقع المساواة على الرابط: https://www.mosoah.com ، تاريخ الوصول 2023/8/14.
10. التهديدات الممكنة لأمن المعلومات (2023)،متاح في موقع مساواة على الرابط https://www.mosoah.com تاريخ الوصول2023/12/6.
11. الجواد، دلال صادق(2019)، أمن المعلومات._عمان: دار اليازوري .
12. الجيزاوي، محمد،(2018)،الادارة الاستراتيجية والاعمال الالكترونية: اشكاليات النظرية والتطبيق_. بيروت: دار الكتب العلمية.
13. الحصيني، أحمد(2016)، مقدمة أمن المعلومات ._الرياض: منتدى الرياض الاجتماعي
14. الخالدي ،ساري محمد،(2018)، اتجاهات في أمن المعلومات وأمانها: أهمية تقنيات التعمية، التشفير._ عمان : دار العبيكان للنشر.
15. خصائص امن المعلومات(2023)، متاح في موقع ستار على الرابط https://www.starshams.com تاريخ الوصول 2023/9/20.
16. الدنف، أيمن محمد فارس (2013)، واقع ادارة امن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها._ رسالة ماجستير: غزة الجامعة الاسلامية..
17. الراوي، مهند محمد منيب(2023)، سياسة أمن المعلومات في جامعة الموصل: خوادم مركز الحاسب الالكترونية انموذجا(رسالة ماجستير)، جامعة الموصل، كلية الاداب، قسم المعلومات وتقنيات المعرفة .

18. سرية المعلومات.(2023)، متاح في موقع المرسال على الرابط https://www.almrsal.com تاريخ الوصول 2023/10/28.

19. الشبلي ، هيثم حمود،(2009)، أدارة مخاطر الاحتيال في قطاع الاتصالات ._عمان: دار صفاء للنشر والتوزيع .

20. الشيتي، إيناس محمد إبراهيم،(2010)، تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية في المملكة العربية السعودية دراسة تطبيقية على جامعة القصيم،*المجلة المصرية للمعلومات*._مج11،ع5.

21. طرق اختراق امن المعلومات(2023)، متاح في موقع إعمل بيزنس على الرابط https://www.e3melbusiness.com تاريخ الوصول25\11\2023.

22. القحطاني، ذيب بن عايض.(2015)، أمن المعلومات._الرياض :مدينة الملك عبدالعزيز للعلوم والتقنية

23. قدايفة، امينة،(2016)، استراتيجية امن المعلومات._ *مجلة ابعاد اقتصادية*، مج6،ع1.

24. كيفية الحماية من هجمات الهاكرز(2023)، متاح في موقع اعمل بيزنس على الرابط https://www.e3melbusiness.comتاريخ الوصول28\11\2023 .

25. اللوزي، خضير كاظم محمود وسلامة، محمود (2008)،مبادئ إدارة الأعمال ._عمان : أثراء للنشر والتوزيع.

26. مبادئ امن المعلومات.(2023)، متاح في موقع خمسات على الرابط http://blog.khamsat.Com ، تاريخ الوصول 2023/10/27.

27. مجالات امن المعلومات(2023)، متاح في موقع خمسات على الرابط https://blog.khamsat.com تاريخ الوصول2023/10/29.

28. مراحل تطور امن المعلومات(2023)،متاح في موقع ستار شمس على الرابط https://www.starshams.com ، تاريخ الوصول 2023/10/25.

29. مزيد، رشيد حميد وكاظم، حيدر جواد.(2022)، واقع إدارة أمن نظم المعلومات في كلية علوم الحاسوب والرياضيات دراسه مسحية، *مجلة الدراسات المستدامة*، مج4،ع1.

30. مفهوم سياسة امن المعلومات،(2023)،متاح في موقع مجتمع على الرابط https://www.itcomunity.com تاريخ الوصول2023/10/30.

31. مكونات امن المعلومات(2023)،متاح في موقع خمسات على الرابط https://blog.Khamsat.com تاريخ الوصول 2023/10/24.

32. الموسوي، منى تركي، وفضل الله، جان سيريل.(2023)، الخصوصية المعلوماتية واهميتها ومخاطر التقنيات الحديثة عليها، *مجلة كلية بغداد للعلوم الاقتصادية.*

33. النجار، فايز جمعة،(2010)، نظم المعلومات الادارية.-عمان: دار الحامد للنشر والتوزيع.

34.وسائل المحافظة على أمن المعلومات،(2023)، متاح في موقع اراجيك على الرابط https://www.arageek.com تاريخ الوصول2023/12/10 .

35.وظائف امن المعلومات(2023)، متاح في موقع بكة على الرابط https://bakkah.com/ar/knowledge-center تاريخ الوصول 2023/9/25.

2_قائمة المصادر باللغة الانكليزية:

1. Ferranti, Knapp,K,(2012). policy Awareness, Enforcement and Maitenance: Critical to Information Security Effectiveness in Organizations.-*Journal of Management policy practice*, vol 13, no5, .

2. Morris Knapp, K & L , R. Marshall & T, Byrd (2009), Information Security policy :An Organizational Level process *Model.,computers Science*,vol25,n07.

3. Patrick ,Howard, (2002), The Security policy Life Cycle: Functions and Responsibilities 0.:Auer Bach publications-CRC prss LLC,USA.

4.,dulany, vein m,(2002)security its not technical, gsec practical assignment,v13,15 *january*.

5.Information Security Standards (2024) ,available at www.iso27001security.com . Accessed on 2024\3\25.

6.university of London (2023), information Security Policy (ISP_001) Available at https://www.london.ac.uk/sites/default/files/governance/ISP_001_information-security-policy.pdf , Accessed on 15-1-2023.

الملحق رقم (1)
أسئلة المقابلة

أسئلة المقابلة:

وقد قُسِّم هذه الأسئلة إلى محاور عديدة، وتضمن كل محور منها مجموعة أَسئلة ضمنية:

المحور الأَوَّل:سياسة أَمَـن المعلومات:

1_أكان لمركز الحاسوب سياسة أَمَـن المعلومات الفعالة وفقا للمعايير الدولية؟

2_هل كان ثمة توافق سياسة أَمَـن المعلومات مع التقنيات المستخدمة لحماية المعلومات؟

3_هل للجامعة إدراك"لسياسة أَمَـن المعلومات واهميته؟

4_هل ثمة تقييم دولي للالتزام بتطبيق"سياسات"أَمَـن المعلومات؟

5- أَكانت تتوافر الخوادم اللازمة والموافقة لسياسة أَمَـن المعلومات في الجامعة؟

6هل كانت مساعدة سياسة أَمَـن المعلومات في تقليل"المخاطر للمعلومات"في الجامعة؟

7_ من هي الجهة المسؤولة عن رسم سياسة أَمَـن المعلومات في الجامعة؟

المحور الثاني: برامج الحماية لأَمَـن المعلومات:

1_أَي الأَجهزة المستخدمة لتحقيق"كفاءة أَمَـن المعلومات"عالية؟

2_أَتتوافر برامجيات خاصَّة لعمل"نسخة احتياطيَّة لمعلومات الجامعة؟

3_أَتتوافر إِجراءات تقنيَّة حديثة لحماية تطبيقات"أَأَمَـن المعلومات وخوادمها؟

4_أَي الوسائل"المستخدمة للتحقق من هويَّة المستخدم الداخلي لنظام المعلومات؟

5_أَي الوسائل المستخدمة في تبادل وحماية المعلومات المخزنة في الخوادم؟

المحور الثالث: الحماية المادية والبنية التحتية لسلامة أَمَـن المعلومات:

1_إِذا كانت المتطلبات الأَمنيَّة اللازمة لحماية خوادم المعلومات؟

2_ أَي أَسس اختيار وسائط التخزين المعلومات وللنسخة الاحتياطيَّة؟

3_هل تتوافر شبكة اتصالات حديثة وفعَّالة للوصول المباشر إِلى خوادم المعلومات؟

4_ هل تتوفر إِجراءات السلامة لحماية غرف خوادم المعلومات؟

5_ما تقنيات المراقبة المستخدمة لحماية غرف خوادم"المعلومات؟

المحور الرابع:إِدارة الخطر:

1_أَتتوافر خطط إِدارة الأَزمات والمخاطر المتعلِّقة بأَمَـن المعلومات؟

2_هل الخُطط المتاحة لدرء مخاطر أَمَـن المعلومات والمتوقعة؟

3_أَ تتوافر أَنظمة الحماية الفعَّالة لكشف الاختراقات؟

4_إِلى أَي حد تتوافر إِجراءات الرادعة لمنع أَي نشاط مجهول يعرض أَمَـن المعلومات للخطر؟