الجامعة الإسلامية– غزة
عمادة الدراسات العليا
كلية التجارة
قسم إدارة الأعمال

واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها

إعداد الطالب
أيمن محمد فارس الدنف

المشرف
د.عصام محمد البحيصي

قدمت هذه الدراسة إستكمالاً لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال من الجامعة الإسلامية بغزة – كلية التجارة

1434هـ – 2013 م

بسم الله الرحمن الرحيم

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

سورة البقرة، آية(32).

Abstract

The study aimed to identify actual situation of information systems security management in Gaza Technical Colleges and the ways to improve it.

The researcher used the analytical descriptive method. For the purpose of gathering data, the researcher used questionnaires and interviews as tools. The questionnaires were analyzed with the SPSS.

The study sample consisted of 123 employees representing all the college's IT centers engineers and the users of Information Systems in the following technical colleges: Palestine Technical college-Deir El-Balah,The University College for Applied Sciences-Gaza,College of Science and Technology - Khan Younis, The Arab College for Applied Sciences - Rafah, Gaza Training College- UNRWA.

Of the 123 employees included in the study sample, only 97 employees responded to the questionnaires in avalid way.

The study concluded with the following findings:

- Information system IS infrastructure are available in the colleges at intermediate level.
- All technical colleges haven't any written IS policy, and only some college's higher manangement know about it .
- There are differences between the Technical Colleges in applying the information security management due to the age, training levels, staff experience years, rate of security budget .

The study recommended the following :

- Establishing and developing Information security policy in the technical colleges.
- Increasing the financial budget of information security processes.
- Increasing the capabilities of employees in security fields through training.
- Improving the contract conditions with IT-Outsourcing vendors.

الملخص

هدفت الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة، واستخدم الباحث المنهج البحثي الوصفي التحليلي، وتكون مجتمع الدراسة من العاملين على نظم المعلومات في الكليات التقنية وجمعت أدوات الدراسة بين الاستبانة والمقابلة ، وتوصلت الدراسة إلى مجموعة من النتائج أهمها :

- تتوفر البنى التحتية لنظم المعلومات في الكليات التقنية بدرجة متوسطة.
- تدرك الإدارات العليا للكليات التقنية أهمية سياسات أمن المعلومات إلا أنه لا يوجد في أي من الكليات سياسات معمول بها ومطبقة على أسس واضحة.
- تتفاوت الكليات التقنية مجتمع الدراسة في درجات إستخدام تعهيد نظم معلوماتها .
- توجد فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة

وفي ضوء هذه النتائج فقد أوصى الباحث بالتالي :

- ضرورة الاستمرار بالاهتمام بالبنى التحتية لنظم المعلومات وتطويرها لتجاري المستحدثات التكنولوجية السريعة .
- ضرورة أن تقوم الكليات التقنية ببناء سياسات أمن نظم المعلومات الخاصة بها، والعمل على نشرها و تطبيقها، والقيام بتطويرها ومراجعتها وتقييم المخاطر بشكل دوري للوقوف على ما يمكن عمله وإيجاد السبل الكفيلة بإستعادة العمل ووضع خطط الطوارئ اللازمة لضمان أمن نظم المعلومات.
- ينصح بأن تقوم الكليات التقنية بالاعتناء بدور أكبر بالتدريب وزيادة الموازنات المالية المخصصة لعمليات أمن المعلومات.
- ضرورة قيام الجهات الحكومية بإنشاء مركز متخصص يعنى بقضايا أمن المعلومات.

إهـــــــداء

إلى أبي وأمي . . . أطال الله في عمرهما ومنحهما الصحة والعافية .

إلى إخواني وأخواتي الأعزاء

إلى زوجتي و أولادي (محمد وعبدالله) شركائي في كل نجاح .

إلى شهداء الإسلام وفلسطين وشهداء الحرية أجمعين .

إلى كل الجنود المجهولين والمعروفين الذين جاهدوا على ثرى فلسطين .

إلى مشاعل الحرية خلف القضبان . . . أسرانا البواسل

إلى كل طلاب العلم

أهدي هذا العمل المتواضع

شكر وتقدير

الحمد لله رب العالمين، حمداً كثيراً مباركاً فيه، الذي أنعم علي بالتوفيق في إنجاز هذا العمل المتواضع، والصلاة والسلام على أشرف المرسلين سيدنا محمد بن عبدالله الصادق الأمين وآله وصحبه وبعد:

يسرني بعد أن تمكنت من إنجاز هذا البحث بعون وتوفيق من عند الله تعالى العلي القدير أن أسجل عرفاناً مني واحتراماً وتقديراً بالفضل لأستاذي الدكتور/ **عصام محمد البحيصي**، الذي تفضل علي بعلمه الوفير وجهده الصادق المتواصل في العطاء بالاشراف على هذه الرسالة وتقديم التوجيهات الرشيدة والآراء السديدة في إثراء خبرتي العلمية والعملية، بارك الله في علمه وسدد خطاه .

كما يسعدني أن أقدم شكري وإمتناني للجنة المناقشة : الدكتور/ **وسيم إسماعيل الهابيل** كمناقشاً داخلياً، والدكتور/ **نبيل إسماعيل البحيصي** كمناقشاً خارجياً .

وأتقدم بوافر التقدير وعظيم الامتنان للأساتذة الأفاضل الذين شاركوا في تحكيم ومراجعة الاستبانة، والزملاء في مراكز الحاسوب بالكليات التقنية الذين ساهمت مشاركتهم في إثراء هذا العمل .

ويسعدني أن أشكر من درسني و زملائي على مقاعد الدراسة ومن شاركوني في مهام الدراسة طوال فترات دراستي .

وأخيراً أتقدم بالشكر الجزيل لجميع الزملاء العاملين في الكليات التقنية بقطاع غزة عامة، وكلية فلسطين التقنية على وجه الخصوص لما قدموه من تعاون وعون ومساعدة في إنجاح هذا العمل .

وجزى الله خيراً كل من كان له دور من قريب أو بعيد في إتمام هذه الدراسة.

قائمة المحتويات

قائمـــة الجداول[1]

[1] [2-2] :الرقم الى اليمين يعني رقم الفصل، وإلى يسار د رقم العنصر

قائمـــة الأشكال

قائمـة الملاحق

الفصل الأول

الإطار العام للدراسة

1.1 مقدمة الدراسة .

1.2 مشكلة الدراسة وأسئلتها .

1.3 فرضيات الدراسة .

1.4 متغيرات الدراسة.

1.5 أهداف الدراسة.

1.6 أهمية الدراسة.

1.7 منهجية وإجراءات الدراسة.

1.8 الكليات مجتمع الدراسة.

1.9 حدود الدراسة.

1.1 مقدمة:

يشهد عالم اليوم تغييراً مستمراً في بيئة الأعمال، وتطويرا لا يتوقف على صعيد إنجاز المهام اليومية والتعامل مع جمهور العملاء في مختلف القطاعات، ولقد أصبحت تكنولوجيا المعلومات ضرورة من ضرورات عصرنا الحالي وأداة من أدوات العمل الرئيسية، بل وأصبحت أداة إستراتيجية تسهل الوصول إلى الميزة التنافسية الدائمة، ونتيجة لهذه الطفرة الكبيرة التي حدثت في وسائل الاتصالات وشبكات المعلومات والدخول في عصر العولمة والانترنت، ظهرت مخاطر وتهديدات جديدة في ساحة الأعمال وهو ما يستدعي أخذ كافة الوسائل المتاحة والممكنة لتعزيز أمن نظم المعلومات وحمايتها .

إن أمن المعلومات عبارة عن مجموعة من الإجراءات والتدابير الوقائية التي تستخدم للحماية من جرائم الحاسوب والانترنت (السالمي،2008،ص281)، ومهددات استخدام التقنية قد تطال إما سرية المعلومات أو سلامتها أو توافرها أو قد ترتبط بأجهزة الحاسوب نفسها كأن تطالها السرقة أو يتم استخدام أجهزة الحاسوب وشبكات المعلومات كوسيط في ارتكاب الجرائم.
وقد تطال جرائم الحاسوب والانترنت البيانات الشخصية المتصلة بالحياة الخاصة، كما أن هذه الجرائم تطال الملكية الفكرية وتنصب على برامج الحاسوب وقواعد البيانات وعلى محتويات مواقع الويب(الهادي، 2006،ص40).

وكما باقي المنظمات والمؤسسات والشركات، عمدت الكليات التقنية الفلسطينية العاملة بقطاع غزة إلى استخدام تكنولوجيا المعلومات والاتصالات واستثمرت في بناء نظم وتطبيقات الحاسوب للقيام بعملياتها التشغيلية على صعيد الأعمال اليومية الروتينية والعمليات الإدارية المعقدة واتخاذ القرارات والتعليم الالكتروني ووفرت للطلاب إمكانات الاتصال بالانترنت للتواصل مع مدرسيهم في حلقات التعليم الالكتروني المباشرة وغير المباشرة، ومكنت الطلاب من التعرف على معلوماتهم الأكاديمية والتسجيل والدفع الالكتروني ووفرت للكثير من أصحاب العلاقة الآخرين إمكانات مختلفة للوصول للمعلومات التي تناسبهم عبر الشبكات المحلية أو من خلال مواقع الويب العامة الوصول، وكان لهذا كله الأثر الكبير في ضرورة تفعيل أكبر لدور أمن المعلومات ليكون حاضراً أمام كل هذه التحديات المتجددة، وتسعى الكليات لتطوير نظم معلوماتها بقدراتها الذاتية أو من خلال الاستعانة بأطراف خارجية (المتعهدين).

وتعتمد قدرة المنظمة في الإستفادة من مزايا وفرص السوق والحلول عبر المتعهدين، على مستويات الإتاحة والقدرة على توفير بيئة آمنة لحماية المعلومات(Allen,2005).

ويتحدد مقدار الجهد والموارد اللازمة لحماية أمن المعلومات، بمقدار حساسية المعلومات، فليست كل المعلومات لها نفس القدر من الأهمية، كما أنه لا يجري المساواة بين الثغرات الأمنية عند معالجتها (الغثبر وآخرون، 2009).

ولضمان برنامج ناجح لأمن المعلومات في المؤسسات لابد من إجراء عملية إدارة المخاطر بفعالية، بحيث لا تقتصر فقط على حماية موجوداتها وممتلكاتها المعلوماتية ويكون الهدف الرئيسي للمؤسسة حينها حماية تحقيق رسالتها، ولا يجب النظر إلى عملية إدارة المخاطر على إنها عملية تقنية بحتة يقوم بها خبراء أمن ونظم المعلومات ولكن يجب أن تكون وظيفة ضرورية من وظائف الإدارة في المنظمة(Bowen,2006,P84).

فاليوم باتت الحلول الإدارية وسيلة ناجعة للحماية وتعزيز أمن المعلومات بما يمكن أن تتضمنه من دراسة للمنافع والتكاليف(Cost- Benefits Analysis) للحلول الفنية والبرمجية.

1.2 مشكلة الدراسة:

تتزايد تحديات أمن المعلومات في البيئة الرقمية كلما أوغلنا في تبني التقنيات والحوسبة الحديثة، ومع اتساع نطاق المؤثرات الداخلية والخارجية تصبح التقنيات وحدها عاجزة عن التغلب على المخاطر الأمنية التي تحدق بهذه النظم.

وتتم معالجة قضايا أمن المعلومات في الكليات التقنية حالياً بالنظر إلى الزاوية التقنية فقط، ومن الزاوية العملية فإن مشكلات أمن المعلومات تحمل الكثير من التعقيدات التي تشمل في طياتها الجوانب التقنية والتنظيمية والبشرية، ولعل الحل يكمن بإدارة أفضل لأمن نظم المعلومات عبر ممارسة عملية تقييم وإدارة المخاطر وإيجاد الحلول الأمنية كسياسات أمن المعلومات، ومراجعة أنظمة الرقابة والتحكم والحلول الإستراتيجية الأخرى الممكنة .

ومن خلال هذه الدراسة يستطيع متخذي القرار في الإدارات العليا للكليات التقنية التعرف على واقع إدارة أمن نظم المعلومات والوقوف على جوانب الخلل ومعالجة أو إيجاد حلول لقضايا أمن نظم المعلومات .

ومن خلال ما سبق يمكن صياغة مشكلة الدراسة بالتساؤلات التالية:

1. ما هو واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة ؟
2. ما هي سبل تطوير إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة؟

1.3 فرضيات الدراسة:

وتتبثق عن أسئلة الدراسة : (ما هو واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة ؟ وما هي سبل تطويرها؟) الفرضيات التالية:

1. الفرضية الأولى : تؤثر حماية البنية التحتية بصورة ايجابية على إدارة أمن نظم المعلومات عند مستوى دلالة إحصائية $\alpha = 0.05$ ،وتتبثق عن هذه الفرضية الفروض الفرعية التالية:

1.1 – يؤثر توفر الحماية المادية على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

1.2– يؤثر توفر الحماية البرمجية على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

1.3– يؤثر توفر حماية الأفراد على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

2. الفرضية الثانية : يؤثر توفر سياسة لأمن المعلومات على إدارة أمن نظم المعلومات داخل الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.
3. الفرضية الثالثة : يؤثر التحكم بالوصول لنظم المعلومات على إدارة أمن نظم المعلومات في الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.
4. الفرضية الرابعة: يؤثر توفر الإجراءات التنظيمية لضبط نظم المعلومات على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.
5. الفرضية الخامسة : يؤثر استخدام التعهيد في نظم المعلومات IT– Outsourcing على إدارة أمن نظم المعلومات في الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.
6. الفرضية السادسة : تتوفر طرق وسبل جيدة لتطوير إدارة أمن نظم المعلومات في الكليات التقنية عند مستوى دلالة إحصائية $\alpha = 0.05$.
7. الفرضية السابعة: لا توجد فروق ذات دلالة إحصائية في آراء عينة الدراسة عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى للمتغيرات التالية : (الكلية، الموازنة الأمنية لكل كلية، مستوى التدريب، مدى توافر إدارة لأمن نظم المعلومات، العمر ، سنوات الخبرة، المؤهل العلمي، التخصص العلمي).

1.4 متغيرات الدراسة :

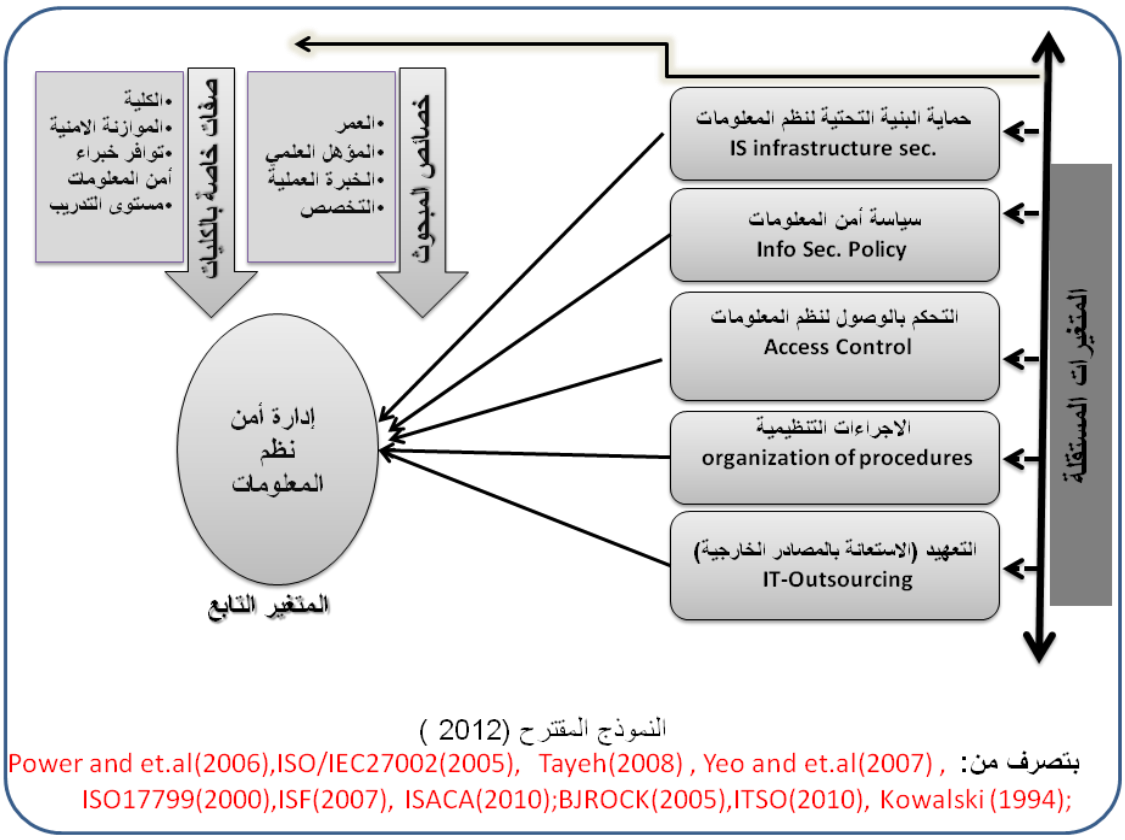
راجع الباحث الأدبيات السابقة وشملت الكثير من الدراسات المتخصصة ومنظمات القياسات العالمية مستخلصا شبكة من المتغيرات المتقاربة مع الأهداف التي سبق وضعها.

والملحق رقم (1) يوضح مدى تقارب المتغيرات ومجالات تطبيق وتحقيق أمن المعلومات وعلاقتها بالمتغيرات المستخلصة.

- **المتغير التابع: إدارة أمن نظم المعلومات**
- **المتغيرات المستقلة:**

1. حماية البنية التحتية لنظم المعلومات(مادية – برمجية – بشرية)
2. سياسة أمن المعلومات .
3. التحكم بالوصول لنظم المعلومات.
4. الاجراءات التنظيمية لضبط نظم المعلومات
5. استخدام التعهيد في نظم المعلومات IT-Outsourcing.
6. صفات الكليات(**الكلية– استخدام نظم المعلومات –توافر إدارة أمن معلومات – مستوى التدريب – الموازنة الأمنية**).
7. صفات شخصية(العمر، المؤهل العلمي، التخصص العلمي، الخبرة العملية، الجنس).

ويظهر في الشكل (1–1) نموذج متغيرات الدراسة:



النموذج المقترح (2012)

بتصرف من: Power and et.al(2006),ISO/IEC27002(2005), Tayeh(2008) , Yeo and et.al(2007) , ISO17799(2000),ISF(2007), ISACA(2010);BJROCK(2005),ITSO(2010), Kowalski (1994);

1.5 أهداف الدراسة:

1. التعرف على واقع أمن نظم المعلومات في الكليات التقنية بقطاع غزة.
2. الكشف عن مهددات أمن نظم المعلومات في الكليات التقنية بقطاع غزة.
3. التحقق من فعالية أساليب أمن المعلومات المستخدمة .
4. تحديد سبل تطوير إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وفق آراء المبحوثين.
5. بيان مدى استخدام التعهيد (الاستعانة بالاطراف الخارجية) في الكليات التقنية.
6. وضع مقترحات وتوصيات بشأن تطوير أمن نظم المعلومات في الكليات التقنية.

1.6 أهمية الدراسة:

1. تنبع أهمية هذه الدراسة كونها تلقي الضوء على قضية هامة حيث ستناقش إدارة أمن نظم المعلومات و تزداد أهميتها بالبيئة محل الدراسة وهي أحدى أهم أعمدة التعليم العالي إنها الكليات التقنية التي تعتبر منهلاً للكفاءات المتخصصة والمدربة.
2. تفيد هذه الدراسة العاملين في مراكز تكنولوجيا المعلومات في الكليات التقنية المختلفة.
3. إن الأمن المعلوماتي لم يعد قضية يتولاها فنيون وتكنوقراط داخل المنشآت والمؤسسات كل على حدة بشكل مجزأ، بل أصبحت من القضايا التي يتولاها سياسيون وإستراتيجيون وصناع قرار يترجمونها في سياسات واستراتيجيات وطنية تعمل ضمن منظومة الأمن الوطني الشامل وتضبط العلاقة بين أمن المعلومات والأمن الوطني وتوجهها في مسارها الصحيح (غيطاس،2007)
4. تأتي الدراسة مكملة لدراسات سابقة عديدة على الصعيد المحلي والدولي، لكنها تجسد مفاهيم جديدة وبيئة جديدة لم تدرس من قبل وتعتبر ذات أهمية من منطلق تعزيز مفهوم إدارة المخاطر والمنافع وتحقيق إدارة سليمة لأمن المعلومات بما يؤكد استمرارية العمل .

كما تكمن أهمية الدراسة ميدانياً في الجوانب التالية:

5. إبراز أهمية أمن نظم المعلومات في الكليات التقنية خاصة والمؤسسات التعليمية عامة.
6. يأمل الباحث أن يتوصل البحث إلى نتائج وتوصيات يمكن أن تفيد المسؤلين في الكليات التقنية بأهمية تطبيق إدارة أمن نظم المعلومات .

7. تساعد الجهات المشرفة على الكليات التقنية في التعرف إلى واقع إدارة أمن نظم المعلومات في الكليات التقنية في محافظات غزة.
8. رسم صورة واقعية حول واقع الكليات التقنية وأمن نظمها من خلال وجهة نظر العاملين فيها لكونهم الفئة المستفيدة من تطوير مثل هذه الإدارات أمنياً .

1.7 منهجية وإجراءات الدراسة :

لتحقيق أهداف الدراسة تم استخدام المنهج الوصفي، وذلك من خلال القيام بالخطوات التالية :

1) تحديد الإطار النظري للدراسة حيث جرى مراجعة الأدبيات السابقة كمصادر ثانوية للبيانات من خلال الكتب والمجلات المحكمة والنشرات والدوريات والرسائل و الأطروحات الجامعية.
2) الإجراءات الميدانية كمصدر أولي للبيانات وشملت :

- بناء أداة الدراسة من خلال استبانة تضمنت مجموعة من المؤشرات الدالة على واقع إدارة أمن نظم المعلومات في الكليات التقنية وسبل تطويرها في الكليات التقنية، ومن ثم حكمت الاستبانة، وأجريت الدراسة الاستطلاعية، ثم وزعت الاستبانة على عينة الدراسة، وجمعت البيانات واجريت المعالجات الاحصائية عليها للوصول لتحليل النتائج .
- المقابلة : تم تصميم نموذج للمقابلة حيث صممت أسئلة المقابلة بشكل مفتوح لأهداف تجميع أكبر قدر من المعلومات وترك الحرية للمجيب، و من ثم أجريت مقابلات شخصية مع رؤساء أقسام مراكز الحاسوب(نظم المعلومات) في الكليات مجتمع الدراسة، والملحق رقم(5) يظهر أسئلة المقابلة والنموذج المصمم .

3) مناقشة نتائج الدراسة واقتراح بعض الاجراءات التي من شأنها تطوير واقع أمن نظم المعلومات في الكليات التفنية.

1.8 الكليات مجتمع الدراسة:

تم تحديد مجتمع الدراسة بالأفراد العاملين ضمن نظم المعلومات في الكليات التقنية وهم موظفي أقسام ومراكز الحاسوب المطورة لنظم المعلومات ، وموظفي وموظفات الأقسام الأخرى التي تستفيد في تنفيذ أعمالها بنسبة عالية من الخدمات التي تقدمها مراكز الحاسوب في الكليات التالية الواردة في الجدول رقم (1-1).

جدول رقم (1-1): الكليات مجتمع الدراسة

اسم الكلية	مجتمع الدراسة
كلية فلسطين التقنية – دير البلح	50
الكلية الجامعية للعلوم التطبيقية	55
كلية العلوم والتكنولوجيا – خانيونس	45
كلية تدريب غزة – الوكالة	16
الكلية العربية للعلوم التطبيقية	14
حجم المجتمع الإجمالي	180

1.9 حدود الدراسة:

الحدود المكانية : تمت الدراسة في محافظات قطاع غزة .

الحدود الزمنية : طبقت الدراسة في الفترة من 2012/9 حتى 2013/2.

الحدود الموضوعية : ركزت الدراسة في التعرف على واقع إدارة أمن نظم المعلومات في الكليات التقنية بمحافظات غزة وسبل التطوير الممكنة لها من الواقع الذي تم دراسته.

الحدود المؤسساتية: تناولت الدراسة خمس كليات تقنية في محافظات غزة : (كلية تدريب غزة – غزة، كلية العلوم والتكنولوجيا ـ خانيونس، كلية فلسطين التقية ـ دير البلح، الكلية الجامعية للعلوم التطبيقية ـ غزة، كلية المجتمع العربية ـ رفح).

الحدود البشرية : تمت الدراسة على أعضاء أقسام / مراكز الحاسوب بالكليات التقنية وكذلك العاملين بالأقسام المختلفة في الكليات التقنية الذين يستخدمون نظم المعلومات بشكل أساسي في أعمالهم اليومية.

الفصل الثاني

الدراسات السابقة والإطار المفاهيمي

- **المبحث الأول : الدراسات السابقة.**

اولاً :/ الدراسات العربية.

ثانياً:/ الدراسات الأجنبية.

ثالثاً:/ التعليق على الدراسات السابقة وما يميز الدراسة عن غيرها.

- **المبحث الثاني : الإطار المفاهيمي للدراسة و نظريات أمن المعلومات .**

المبحث الأول

الدراسات السابقة

مقدمة:

اشتملت مراجعات الدراسات السابقة على الدراسة المتعمقة لكل مصادر الأدبيات المتاحة، من كتب، مجلات علمية محكمة، رسائل وأبحاث، وقائع مؤتمرات، ومواقع الويب المتخصصة بأمن المعلومات، ثم سُجلت الدراسات ذات الصلة الأكبر بموضوع الدراسة ليتسنى للباحث ربط ما يتوصل له بنتائج وتوصيات الدراسات السابقة، ثم صنفت الدراسات السابقة حسب التاريخ والمكان، فلقد رتبت الدراسات إلى عربية وأجنبية، ومن ثم جرى ترتيبها حسب التاريخ من الأحدث إلى الأقدم، وفي جزء التعليق على الدراسات السابقة وضع الباحث تصوراً للتشابهات و الاختلافات في دراسته عن الدراسات السابقة.

أولاً/الدراسات العربية:

1. **دراسة عرفان نبي وآخرون (2010)، بعنوان : دراسة عملية حول أمن المعلومات في المنظمات السعودية**

هدفت الدراسة إلى استكشاف حالة أمن المعلومات والعمل على تحقيق فهم أفضل للحقائق السائدة في هذا المجال داخل العربية السعودية، واستخدمت الدراسة المنهج الاستقصائي حيث جرى انتقاء مسبق لمجموعة من 120 منظمة سعودية مثلت المساهمين من أربع قطاعات رئيسية، و قام الباحثون بتنظيم ورشة عمل لممثلين عن تلك المنظمات المختلفة، كما أعد الباحثون استبانه تم توزيعها على المشاركين وكانت نسبة الاستجابة 75.7% .

وتوصلت الدراسة للنتائج الآتية :

- أهمية سياسة أمن المعلومات في ضمان اتخاذ عوامل تحكم مناسبة، وبينت الدراسة أن أكثر من نصف المنظمات يمتلك سياسة أمن المعلومات وغالبيتها يميل إلى تطبيقها، و89% يعمد لمراجعة دورية لتلك السياسة.
- اعتبار التحكم في الوصول الى الشبكة Access Control أمراً حاسماً لأمن المعلومات، وتبين أن المنظمات على علم وتطبيق لهذه القوانين وخاصة في الشبكات السلكية أما في الشبكات اللاسلكية فيتم التغاضي عن هذا الجانب رغبة في تسهيل تعامل المستخدمين.
- تتسم معالجة قضايا أمن المعلومات بالتمييز بين حساسية المعلومات، حيث بينت الدراسة أولويات المعالجة لهذه الثغرات وافترضت عدم المساواة في التعامل مع هذه المعلومات، فليست كل المعلومات لها نفس القدر من الأهمية.

وأوصت الدراسة بأهمية إرساء الوعي الأمني داخل المؤسسات من خلال التدريب المتخصص والمعرفي .

2. **دراسة العتيبي (2010)، بعنوان : الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية والدولية.**

هدفت الدراسة إلى التعرف على مدى توافق الأمن المعلوماتي للمواقع الالكترونية للأجهزة الأمنية والمدنية في الرياض في المملكة العربية السعودية مع المعايير المحلية والدولية، واستخدمت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة للدراسة وتكون مجتمع الدراسة من جميع العاملين بالمواقع الالكترونية، وتم أخذ عينة عشوائية طبقية (195) توزعت (111) للأجهزة الأمنية و(84) للأجهزة المدنية.

وتوصلت الدراسة للنتائج التالية :

- درجة توافق استراتيجيات الأمن المعلوماتي وتنظيم الأمن المعلوماتي في المواقع الالكترونية للقطاع المدني والأمني مع المعايير الأمنية والمدنية متوسطة.
- درجة توافق تقنيات الأمن المعلوماتي وبيئة الأمن المعلوماتي والأمن المعلوماتي للعنصر البشري في المواقع الالكترونية للقطاعين مع المعايير الدولية والمحلية مرتفعة.

وأوصت الدراسة إلى حاجة الجهات الحكومية لتطبيق جزء لا بأس به من المعيار الدولي لأمن المعلومات ونصح الباحث بضرورة حصول الأجهزة الحكومية على الشهادات الدولية في ذلك، كما أوصت بتوحيد الجهات المسئولة عن تطبيق ومتابعة الأمن المعلوماتي الحكومي لتكون عبر هيئة تديرها الحكومة .

3. **دراسة تايه (TAYEH,2008) بعنوان : مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في فلسطين " Effectiveness of Information Security Management at the Palestinian Information Technology Companies"**

هدفت الدراسة للتعرف على مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في الأراضي الفلسطينية، وأعتمدت الدراسة على معيار ISO17799 ومجالاته العشرة الخاصة بقياس مدى جودة نظم أمن المعلومات، واستخدمت الدراسة المنهج الوصفي وصممت استبانه لجمع البيانات حول مدى الالتزام بتطبيق المعايير العشر لأمن المعلومات التي أعتمدتها الدراسة، وتوصلت الدراسة للنتائج التالية :

- تتحقق فعالية إدارة أمن نظم المعلومات بمقدار توفر سياسة أمن المعلومات.
- الأمن التنظيمي لا يؤثر على كفاءة وفعالية إدارة أمن نظم المعلومات، وأرجعت الدراسة ذلك إلى عدم وجود آلية مراجعة دورية نظامية لسياسة أمن المعلومات

- يؤثر أمن الأفراد إلى حد ما في كفاءة إدارة أمن نظم المعلومات، على الرغم من أن المبحوثين ابدوا شكواهم من نقص في التدريب.
- يؤثر الأمن المادي للمكونات البرمجية والمادية في كفاءة إدارة أمن نظم المعلومات.
- تؤثر قواعد إدارة الحواسيب والشبكات بفاعلية على إدارة أمن نظم المعلومات، وتوصلت دراسته إلى رغبة المبحوثين في التعامل مع الآليات والأساليب المختلفة.

وأوصت الدراسة :

- أهمية بذل مزيد من الجهود من أجل تفعيل دور أكبر للأمن التنظيمي .
- زيادة التوعية الأمنية عبر مزيد من التدريب، وإصدار النشرات الداخلية والتقارير حول ما يدور من اختراقات و ثغرات أمنية واطلاع الكوادر المتخصصة بآليات الحل .
- انه لمن الضروري أن تقوم الحكومة الفلسطينية بإصدار قانون أو تشريع خاص بحقل أمن نظم المعلومات .

4. **دراسة البحيصي والشريف(2008) بعنوان : مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة**

هدفت الدراسة للتعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، وأهم الأسباب التي تؤدي إلى حدوث تلك المخاطر، والإجراءات التي تحول دون وقوع تلك المخاطر، واعتمدت الدراسة المنهج الوصفي التحليلي وتم إعداد استبيان خاص تم توزيعه على البنوك العاملة في محافظات قطاع غزة، وتوصل الباحثان إلى مجموعة من النتائج :

- عدم حدوث مخاطر نظم المعلومات المحاسبية في المصارف العاملة في قطاع غزة بشكل متكرر.
- يرجع حدوث مخاطر نظم المعلومات المحاسبية الالكترونية إلى أسباب تتعلق بموظفي البنك نتيجة قلة الخبرة والوعي والتدريب، إضافة إلى أسباب تتعلق بإدارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى المصرف.
- تتبع المصارف إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية

وأوصت الدراسة بجملة من التوصيات كان أبرزها :

- الحاجة لوضع ضوابط أمن ورقابة على المعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أم الكترونية يجري نقلها عبر اتصالات سلكية أو لاسلكية أو عبر الإنترنت .
- ضرورة وضع خطة حماية أمنية شاملة والتي تنعكس على انخفاض النفقات الناتجة عن توظيف الحلول الجزئية للأمن.
- ضرورة وضع إجراءات تضمن إستمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الأزمات
- استخدام تشفير البيانات عند الحفظ والنقل والتخزين، كي لا يتمكن أحد من اختراقها.

5. دراسة القحطاني (2008) بعنوان : مهددات الأمن المعلوماتي وسبل مواجهاتها، دراسة مسحية على منسوبي الأجهزة مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض.

هدفت الدراسة للتعرف على مهددات الأمن المعلوماتي وسبل مواجهتها في ضوء تزايد معدلات الاختراقات والحاجة المتزايدة لاتخاذ وسائل الحماية اللازمة للبيانات والمعلومات، واستخدمت الدراسة المنهج الوصفي التحليلي، وصممت استبانه متخصصة لجمع البيانات بالطريقة المسحية، وتوصلت الدراسة للنتائج التالية:

- مصدر تهديد أمن نظم المعلومات بدرجة قوية هو عدم ضبط الاتصال بشبكة الانترنت.
- مخاطر الاتصال المباشر بشبكات الميكروويف، وإساءة الاتصال بشبكات خارجية مع مصادر المعلومات الخارجية، وإساءة الاتصال الداخلي بين الأفرع تعتبر مصادر تهديد متوسطة الدرجة.
- استخدام الفيروسات في إتلاف المعلومات وتغيير البيانات، والتنصت على حزم المعلومات، وسرقة المعلومات هي أشكال التهديدات المحتملة التي تهدد الأمن المعلوماتي بدرجة متوسطة.
- استقطاب وتشغيل خبراء حماية نظم المعلومات، و تزويد المراكز بالتقنيات المتطورة، و استخدام مكافحات الفيروسات المتطورة هي أهم السبل المقترحة بدرجة كبيرة لتطوير قدرات المراكز .

وأوصت الدراسة بضرورة استخدام فعال للحوافز المادية والمعنوية لتشجيع المبدعين والمتميزين في مجال أمن المعلومات، كما أقرت بضرورة معاقبة من يتسبب في تسريب المعلومات، وأن يتم استحداث تكنولوجيا الحماية المادية المتبعة، الحرص على استخدام البرمجيات الأصلية، كما أوصت الدراسة بإنشاء إدارة من أصحاب الخبرة والدراية بأمن المعلومات لتحديد التقنيات اللازمة لحماية مراكز الحاسوب .

6. دراسة الهادي(2006م) بعنوان (توجهات أمن وشفافية المعلومات في ظل الحكومة الالكترونية)

تناولت الدراسة أمن المعلومات في ظل الحكومة الالكترونية، وخدمات البيئة الرقمية، كما ناقشت الدراسة متطلبات الأمن الطبيعي لنظم المعلومات، وتعرضت الدراسة لبعض الاعتبارات والابعاد المتعلقة بأمن المعلومات، كما ناقشت الغرض من المعايير الأمنية خاصة معيار (ISO 17799)، وتطرقت لسياسات هذا المعيار، وقد اوصت الدراسة بضرورة إيجاد توجهات ومعايير لأمن المعلومات فيما يتعلق بالغرض العام منها ومجالها والمفاهيم الخاصة بها، بالاضافة الى تحديد المبادئ العامة منها، وكيفية تنفيذ أمن المعلومات من حيث تطوير سياساته بالانسجام مع المعايير الدولية.

ثالثاً/الدراسات الاجنبية :

7. دراسة Kazemi et al (2012) بعنوان :تقييم عوامل نجاح إدارة أمن المعلومات " Evaluation Of Information Security Management System Success Factors: Case study of Municipal Organizations"

هدفت الدراسة للتعرف على أولويات عوامل نجاح تطبيق نظام إدارة أمن المعلومات في المنظمات الإيرانية، واستخدمت الدراسة الاستبانة كأداة لجمع البيانات، واحتوت(21) سؤالاً غطت سبعة مواضيع أساسية، وتم توزيع (35) استبانة على عينة الدراسة وكانت نسبة الاستجابة 100% .

ولتفسير نتائج تحليلاتهم، قام الباحثون بمقارنة ما توصلوا له مع دراسة فنلندية بحثت نفس العوامل التي وضعوها، وتوصلوا للنتائج التالية:

- دعم الإدارة العليا، وسياسة أمن المعلومات، والوعي والتدريب هي أكثر العوامل المهمة في إنجاح تطبيق إدارة أمن المعلومات في البلديات الإيرانية من وجهة نظر خبراء أمن المعلومات
- عامل الاستعانة بالخبرات الخارجية(التعهيد) هو الأقل أهمية في إنجاح تطبيق إدارة أمن المعلومات
- ترتيب أهمية العوامل بين الدراسة التي أجراها الباحثون والدراسة التي تمت مقارنة نتائجها (الدراسة الفنلندية)جاء متوافقا بنسبة كبيرة، وأرجع الباحثون أهمية عامل دعم الإدارة العليا لأنه دون هذا الدعم لن يتم تطبيق أي من خطط وبرامج أمن المعلومات، وكذلك حاجة المؤسسات إلى سياسات مكتوبة في أمن المعلومات ويأتي بالمرتبة الثالثة الوعي والتدريب والذي يتشكل بنجاح العاملين السابقين.

وأوصى الباحثون بضرورة البحث في أسباب تضاؤل أولوية الإستعانة بالمصادر الخارجية في نجاح تطبيق إدارة أمن المعلومات.

8. دراسة Jorro (2011) بعنوان : جاهزية تدقيق أمن نظم المعلومات، دراسة حالة :مؤسسات الحكومة الأثيوبية "Information System Security Audit Readiness Case study: Ethiopian Government Organizations"

حاولت الدراسة التعرف لجاهزية المؤسسات الحكومية الإثيوبية لإجراء مراجعات حول أمن نظم المعلومات، وهدفت لمساعدة الحكومة في التغلب على مشاكل أمن نظم المعلومات التي تعيق تطبيق الخدمات الالكترونية، ومحاولة وضع سياسات وإجراءات تنظم وظيفة أمن المعلومات، و استخدمت المعايير الدولية في بناء استبانة الدراسة التي وزعت على ثمانية عشر مؤسسة، وقد توصلت الدراسة للنتائج التالية:

- مؤسسات الحكومة الأثيوبية في مستوى استعداد منخفض تجاه قضايا أمن نظم المعلومات.
- قدرة المؤسسات على إجراء مراجعات في أمن نظم المعلومات والاتصالات تعتمد على توفر السياسات والإجراءات التي تفتقد إليها المؤسسات قيد الدراسة.

- نقص الكفاءات المدربة في حقل أمن نظم المعلومات.

وأوصت الدراسة بضرورة تطوير إطار عام لمراجعة قضايا أمن المعلومات، حيث سيمكن المؤسسات من معرفة المتطلبات اللازمة من أجل الالتزام بمعايير أمن المعلومات .

9. دراسة Kreicberga(2010) بعنوان: التهديدات الداخلية لأمن المعلومات–التدابير المضادة والعنصر البشري . " Internal Threats to Information Security-Countermeasures and Human Factor within SME."

تحدد الغرض العام من الدراسة لاستيضاح المعرفة حول دور العامل البشري في حقل أمن نظم المعلومات وتساءلت الدراسة حول العوامل التي تؤثر على السلوك الأمني للموظفين؟، وكيف ينظروا تجاه التدابير الأمنية المضادة للتهديدات الداخلية؟

واستخدم المنهج الكيفي(النوعي) وكانت أدواته المقابلات التي أجريت مع مسؤولي أمن المعلومات والمستخدمين بالإضافة لمراجعة وتحليل الوثائق والمستندات، والملاحظة المباشرة لسلوك المستخدمين وتوصلت الدراسة إلى :

- رضا وقبول الموظفين والتدابير الأمنية عناصر مهمة في تحقيق سلوك أمن تجاه أمن نظم المعلومات.
- يواجه الموظفون صعوبة ومقدار من التعقيد في فهم الوثائق المتعلقة بأمن المعلومات.
- تطبيق المتطلبات البشرية لأمن المعلومات يحتاج إلى حالة وعي بأهمية أمن نظم المعلومات.
- يتأثر أمن نظم المعلومات بالعادات التي يسلكها الموظفون .

وأوصت الدراسة بأنه لتحسين أمن المعلومات يتوجب إجراء تقييم لسلوك الموظفين تجاه القضايا الأمنية المختلفة، وأن يتم إعلامهم بالمنافع التي ستتحقق من تطبيق التدابير المضادة لتهديدات أمن نظم المعلومات التي تواجهها المؤسسة من الداخل .

10. دراسة SALVATI (2008) بعنوان : إدارة مخاطر نظم المعلومات " Management of Information Systems Risks".

هدفت الدراسة لتوفير بيئة قادرة على إتخاذ القرار بصدد إدارة مخاطر أمن المعلومات من خلال إيجاد حلول ونماذج للقياس، واعتمدت المنهج التحليلي الرياضي من خلال بيانات احصائية حقيقية من واقع مخاطر نظم المعلومات لدى البنوك والمؤسسات المالية في ألمانيا واستنتجت الدراسة:

- نجاح النموذج في تخفيض درجة الغموض في وصف مخاطر نظم المعلومات بنسبة كبيرة .
- قياس وحساب احتمالات التهديد والهجوم أصبحت قائمة، ومكنت متخذي القرارات من اعتمادها كبديل لمفاضلة التخمينات .
- متخذو القرار باتوا أكثر قبولاً لدراسة احتمالات تقييم التدابير الأمنية، وعزز ذلك من تفويض اتخاذ القرارات لمستويات أدنى في الهرم التنظيمي .

11. دراسة Lane (2007) بعنوان:"إدارة أمن نظم المعلومات في الجامعات الاسترالية" Information Security Management In Australian Universities –An Exploratory Analysis

هدفت الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الجامعات الأسترالية، وما هي العوامل الأساسية التي تؤثر في فعاليتها، وكيف يمكن تحسينها، وأجريت الدراسة على 38 جامعة أسترالية، وطرحت الاسئلة على رئاسات الجامعات ومديري اقسام تكنولوجيا المعلومات ومسئولي أمن المعلومات، عبر مقابلة استخدم فيها أسلوبي الأسئلة المفتوحة والمغلقة، وتوصلت الدراسة للنتائج التالية:

- يختلف واقع إدارة أمن المعلومات من جامعة لأخرى ويعود ذلك لعدة عوامل منها : منهجية الإدارة الأمنية، واهتمام الإدارة العليا وإنخراطها، وحجم الإنفاق على أمن المعلومات، والجهد المبذول على مواجهة التهديدات الأمنية، ومستوى أهمية تكنولوجيا المعلومات، والثقافة العامة للمؤسسة.
- أهم العوامل المؤثرة في فاعلية دور إدارة أمن المعلومات تعود لأسباب: نقص الخبرات وضعف هيكلية إدارة أمن المعلومات، و وجود فجوة بين ما هو مأمول وما هو معمول به من وعي بأمن المعلومات وسبب ذلك هو قلة الإكتراث بالمخاطر والتهديدات، وتطوير السياسات الأمنية بشكل واضح وقابل للعمل ويتم الامتثال له ضمن القواعد الأمنية والقانونية.
- للتغلب على ضعف إدارة أمن نظم المعلومات فأنه من الضروري تطوير فاعلية العناصر والكوادر البشرية كأحد أهم مرتكزات إدارة أمن نظم المعلومات .

وقد أوصت الدراسة بالتالي :

- تعزيز دور الإدارات العليا في فهم وإدراك الأفراد تجاه حماية المعلومات و تبني سياسات أمنية متوافقة مع المعايير المطبقة
- تطبيق معايير لإدارة أمن نظم المعلومات لتكون قابلة للإنجاز والفهم في سبيل التنفيذ، بما يحقق رؤية الجامعات ويحد من التكاليف
- وضع برامج التوعية بأمن المعلومات وفق آليات تضمن سهولة تطبيقها، ويستخدم التعلم والتدريب المستمر وتشجيع ورعاية ثقافة تضمن تطبيق سياسات وتوجهات الجامعات، على الصعيد السلوكي والتقني بما يحقق إدارة كفؤة لأمن نظم المعلومات.

12. دراسة ISF (2007) بعنوان (معايير الممارسة الجيدة لأمن المعلومات The Standard of Good Practice of Information Security)

تناولت الدراسة تعزيز الممارسة الجيدة لأمن المعلومات بالمنشآت، وتعزيز مستوى الأمن لديها وتقليل المخاطر إلى مستوى مقبول، والمساعدة في تطوير المعايير العملية التي تسهم بفاعلية في تقليل مخاطر المعلومات، وطبقت الدراسة على المنشآت المحلية والعالمية لمشاركة في منتدى أمن

المعلومات ISF على الانترنت www.securityforum.org و يجمع المنتدى أكثر من 300 منظمة قيادية تتعاون في البحث العلمي لأمن المعلومات، واعتمدت الدراسة على محاور تتدرج تحتها عدة مواضيع فرعية، وهي : تطوير المعيار، محتويات المعيار، تقييم المعيار، تطبيق المعيار.

وخرجت الدراسة بنتائج من أهمها تعتبر المعايير أداة رئيسية لتطوير جودة وكفاءة أدوات التحكم بأمن المعلومات المطبقة بأي منشأة .

13. دراسة Onder(2007) بعنوان : تصميم نظام إدارة أمن المعلومات " A Security Management System Design"

هدفت الدراسة إلى تحسين القدرات الرقابية على أنظمة المعلومات، وتقديم معايير حول أداء الأنظمة للإدارة العليا، وتزويد الإدارة بإمكانات متطورة لحل مخاطر أمن الشبكات والنظم.

وذلك عبر تطوير نموذج على الويب يتم من خلاله تسهيل عمليات حصر المخاطر وإدارة عمليات الشبكات والتعرف إلى المشاكل والتهديدات الأمنية التي تواجه النظم، وتمكين الإدارات العليا في المنظمة من إدارة أمن النظم والشبكات بتوفير بيئة خاصة.

وتوصلت الدراسة أن الحاجة لنظام إدارة الشبكات يلزمه انخراط الإدارة العليا من أجل إنجاحه، و أوصت الدراسة الإدارة العليا باستخدام النموذج الذي أقترح كأداة تمكن من تنفيذ إدارة أمن النظم والشبكات بآليات تنسجم مع توجهات المنظمة نحو فعالية وكفاءة الإدارة في مواجهة المخاطر التي تتهددها .

14. دراسة YEO etal. (2007) بعنوان :دراسة العوامل المؤثرة في نجاح تقييم مخاطر أمن المعلومات– دراسة حالة مؤسسات التعليم العالي في استراليا . "Understanding Factors Affecting Success of Information Security Risk Assessment: The Case of an Australian Higher Educational Institution"

هدفت الدراسة للتعرف واستكشاف العوامل التي تؤثر في نجاح عملية تقييم المخاطر التي تتعرض لها نظم المعلومات في مؤسسات التعليم العالي في استراليا، وقد افترضت الدراسة ستة من العوامل المؤثرة على النحو التالي :(مشاركة الإدارة العليا، الأعضاء البارعين، الأدوات والآليات، سياسات نظم المعلومات، وعي الأفراد، والطلاب، والاستراتيجيات الواضحة)، وقد أعتمدت الدراسة المنهج الكيفي عبر إجراء التحليل الاستكشافي، واستخدمت المقابلات كأداة لجمع البيانات بالاضافة إلى مراجعة وثائق سياسات أمن المعلومات، وتوصلت الدراسة بأنه يوجد أثر لعوامل جديدة كاستخدام برمجيات وأدوات مناسبة في عملية إدارة مخاطر نظم المعلومات.

وأوصت الدراسة :

- ضرورة إجراء دراسات حول أثر مزيج من العوامل في كل مرحلة من مراحل تقييم المخاطر.
- إجراء دراسات موسعة حول العوامل الثقافية المؤثرة في إدارة مخاطر نظم المعلومات في قطاع التعليم العالي بدول العالم الثالث.

15. دراسة Bjrock (2005) بعنوان:"استطلاع إدارة أمن المعلومات " Discovering Information System Management".

استندت الدراسة على انه لتحقيق الكفاءة في تكاليف نظام أمن المعلومات يتوجب الانطلاق من استيضاح واقع ممارسة إدارة أمن المعلومات .

وكان هدف الدراسة وضع نظام متوازن لإدارة أمن نظم المعلومات؛ وتساءلت الدراسة عن المشاكل الأمنية التي تواجه المنظمات؟ ، والمعوقات التي تهدد إدارة أمن نظم المعلومات؟ ، وما هي الاعتبارات الواجب اتخاذها كعوامل مشجعة على نجاح إدارة أمن نظم المعلومات؟.

واستخدمت الدراسة المنهج الكمي بالإضافة للمنهج الكيفي النوعي حيث توزعت أدوات جمع البيانات بين الاستبانه، والمقابلة، وتكون مجتمع الدراسة من خبراء ومدققي أمن المعلومات العاملين في معهد المعايير الأمنية السويدية Swedish7799 .

وتوصلت الدراسة للنتائج التالية :

- لا يجب أن تتبع وظيفة أمن المعلومات وظيفياً لمراكز تكنولوجيا المعلومات IT Department .
- تحقيق الأمن هو جزء من الجودة، وبذلك يجب أن تهتم الإدارة العليا للمنظمة بتحسين واقع إدارة أمن المعلومات و تحقيق الكفاءة والفاعلية هي برهان على توفر أمن نظم المعلومات.
- جهود إدارة أمن المعلومات تتطلب عمل مكثف، يحقق إستراتيجية المنظمة كعمل متكامل .
- تنظر الإدارة العليا إلى عمليات إدارة أمن نظم المعلومات على أنها عملية إدارة للمخاطر.
- أهمية دور أمن العناصر البشرية في تحقيق أمن المعلومات.

وأوصت الدراسة :

- ضرورة عدم إغفال التهديدات من داخل المنظمة .
- أهمية تحفيز الموظفين من اجل زيادة الوفاء لأمن المعلومات، باعتبار المعلومات هي أصل من الأصول التي يجب صيانتها والحفاظ عليها .

رابعاً:/ التعليق على الدراسات السابقة وما يميز الدراسة عن غيرها:

بعد مراجعة الدراسات السابقة يمكننا تلخيص الملاحظات التالية عليها :

- يتضح من الدراسات السابقة التي تم عرضها أن هناك اهتمام متزايد وتوجه ايجابي لدراسة أمن المعلومات، وهذا الاهتمام لا يقتصر على نوع بعينه من المؤسسات بل يشمل المؤسسات الحكومية، وغير الحكومية، والربحية وغير الربحية والمؤسسات التعليمية والصحية والخدمية .
- أظهرت الدراسات السابقة أهمية موضوع أمن المعلومات كونه يمس عضد المؤسسات في عصر الرقميات وأعتبرت نظم المعلومات أحدى مقومات بقاؤها وهي التي ما فتئت تحقق الميزة التنافسية .

- وركزت الدراسات السابقة على معوقات ومهددات تحقيق أمن المعلومات من جهة، ومن جهة أخرى بينت مدى فعالية إدارة أمن المعلومات قياساً لتطبيق معايير دولية بهذا الشأن، واستطرق البعض متخصصاً لدراسة أثر العنصر البشري في تحقيق كفاءة نظم أمن المعلومات.

- وتنوعت مناهج بحث الدراسات السابقة بين الكيفي والكمي، وبذلك استخدمت الأدوات المختلفة كالاستبيانات و المقابلات وحتى المشاهدات والملاحظة المباشرة .

- تناولت دراسة تايه (2008) مدى فعالية إدارة أمن المعلومات تطبيقاً على شركة من القطاع الخاص، واستند الباحث لأحد المعايير الدولية ISO17799، ويرى الباحث أن الدراسة الحالية تفترض نموذجا يحتوي متغيرات مختلفة إلى حد ما وإن تشابهت بعضها مع عناصر محددة من المعيار الدولي الذي استخدمته دراسة(تايه).

- ربما تلتقي دراسة Lane (2007) مع الدراسة الحالية في مجال تطبيق الدراسة إلى حد ما ، ولكنها تختلف في منهج الدراسة، ونموذج الدراسة حيث سيعرض الباحث متغيرات مختلفة .

- تقاربت آليات وسبل التطوير التي طرحها الباحث إلى حد ما مع دراسة القحطاني(2008)، وقد وضع الباحث نموذجاً إجرائياً لتقييم المخاطر متصلاً إلى حد ما مع آليات تطبيق سبل التطوير التي افترضها ووضعها أمام المبحوثين، بينما لم يقم القحطاني بذلك.

- تضمنت دراسة كل من Kreicberga(2010), Jorro(2011), Kazemi et al(2012) البحث في دعم الإدارة العليا بشكل مباشر كأحد عناصر نجاح إدارة أمن نظم المعلومات، بينما سينظر الباحث إلى هذه العنصر الهام من زاوية البحث في الاجراءات التنظيمية .

- وتتميز هذه الدراسة عن غيرها في أن الدراسات السابقة المختلفة غطت جوانب كدراسة عوامل التأثير في أمن المعلومات، أو الأثر البشري في أمن المعلومات، أو أولويات أمن المعلومات، بينما الدراسة الحالية ستركز على دراسة وتحليل واقع إدارة أمن المعلومات في الكليات التقنية – بقطاع غزة، من جوانب معرفة واقع ممارسة و إدارة أمن المعلومات، والكشف عن مواطن الضعف والخلل، وأسباب تعثر تنفيذ الخطط والتدابير الأمنية، وسيتم دراسة آليات تطوير نظم إدارة أمن المعلومات في الكليات محل الدراسة، وبالتالي ستكون الدراسة أكثر فاعلية ومصداقية من وجهة نظر الباحث.

المبحث الثاني

إطار المفاهيم

Conceptual Framework

في الآونة الأخيرة باتت الحاجة متزايدة لضرورة توجيه البحوث الأكاديمية حول أمن المعلومات في شتى الميادين وربما قلَّ ما بحث المهتمون في مجال تطبيق أمن المعلومات في حقل التعليم العالي، ولعل كثير من توصيات الدراسات قد أوصت بضرورة الإهتمام بالناحية الإدارية والتنظيمية عند وضع برامج ناجحة لأمن المعلومات.

وقد بينت مجموعة من الدراسات السابقة في مجال أمن المعلومات أهمية إضفاء وجهة النظر الإدارية لعدة عوامل منها :

- اتساع مجالات أمن نظم المعلومات وتصاعد أهميتها.
- تزايد أدوار الإدارات الأمنية.
- الحاجة إلى السياسات والمعايير والتنظميات والقواعد التي تضبط الأمن .
- رؤية المؤسسة وما ينجم عنها من إجراءات عملية .
- موازاة السياسات الأمنية مع إستراتيجية المنظمة .
- مؤشرات القياس والتقييم للبرامج الأمنية المستثمرة.
- أصبحت دراسة أمن المعلومات من الناحية الأكاديمية علماً متشعباً واعداً.

(Cegielski,2008; Hazari,2002; Hentea&Dhillion,2006; Hertig,2002; Logan,2002)

واستنتج Tudor(2001) أن أي هيكلية أمنية تشتمل على خمس مكونات هي :

- البنية التحتية للأمن والأمن التنظيمي.
- السياسة الأمنية، والاجراءات والمعايير.
- تقييم المخاطر .
- برامج التدريب والوعي الأمني.
- التجاوب والموافقة .

وتعتمد إدارة أمن نظم المعلومات على نماذج إدارة المعرفة حيث تستخدم كتدقيق لأمن المعلومات التي تتداخل بها الأفراد والتكنولوجيا والعمليات (Zaliwski, 2005)

وقد راجع الباحث مستنداً إلى Hong and et. al.(2003) مجموعة من النظريات التي تناولت أمن نظم المعلومات ومنها نظرية سياسة أمن المعلومات، ونظرية إدارة المخاطر، ونظرية التدقيق والتحكم، ونظرية إدارة النظم، ونظرية خطط الطوارئ.

ولخص الباحث هذه النظريات في الجدول رقم (2-1) مبيناً الأنشطة الإدارية المصاحبة، والاجراءات الإدارية الواجبة، وملامح ومميزات كل من هذه النظريات، وأصول هذه النظريات ومراجعها .

جدول رقم (2-1) :النظريات التي تناولت أمن نظم المعلومات

النظرية	الأنشطة الادارية	الاجراءات الادارية	سمات النظرية	المراجع
سياسة أمن المعلومات	- إعداد السياسة الأمنية - تنفيذ السياسة الأمنية - مراجعة السياسة الأمنية	متعاقبة دورية	- التركيز على السياسة - تعزيز التعاقب والاجراءات المركبة	Flynn(2001); Gupta et l.(2001) ;Kabay(1996)
إدارة المخاطر	- تقييم المخاطر - التحكم بالمخاطر - المراجعة والتعديل	متعاقبة دورية	- تفهم البيئة و - تجاهل السياسة الأمنية وآليات تدقيق المعلومات - دور أكبر للإجراءات	Luthan(1976); Wright(1999)
التدقيق والتحكم	- إعداد نظم التحكم - تنفيذ نظم التحكم - تدقيق المعلومات	متعاقبة دورية	- تركز على التحكم الداخلي وتدقيق المعلومات - تتجاهل السياسة الأمنية وإدارة المخاطر - تفتقد إلى متطلبات التخطيط وخطط الطوارئ في حالات عدم التوقع.	ISO/IEC 1779(2000) COBIT(1998)
إدارة النظم	- إعداد السياسة الأمنية - معرفة المجال الأمني - تطبيق إدارة المخاطر	متعاقبة	- تجاهل تدقيق المعلومات - نقص الفحص الدوري - نقص التغذية الراجعة	BS7799(1999); Schultz et al.(2001)
خطط الطوارئ	- استراتيجية أمنية - استراتيجية إدارة مخاطر - استراتيجية تحكم وتدقيق - استراتيجة إدارة النظم	طارئة	- تأخذ بالإعتبار بيئة المنظمة الداخلية والخارجية وتحدد الاستراتيجية الأمنية المناسبة - تفتقر للتكامل والتسلسل	Lee et al.(1982); Kaplan(1964); Tudor(2002); Drazin et al. (1985)

المصدر بتصرف: Hong and et. al.(2003)

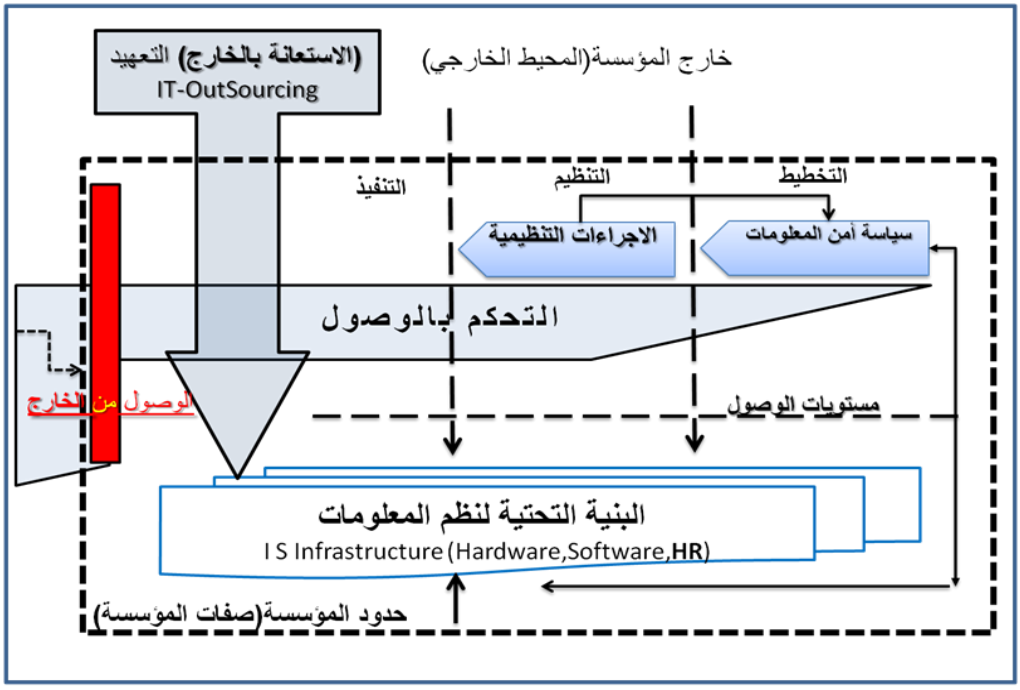
وبحسب ISACA(2009) فإن البعض ينظر إلى أمن المعلومات على أنه مجال فني بإمتياز، ولكن الأدوات التي تقدمها التكنولوجيا لا يمكن أن تشكل وحدها منفردة الحل لمشاكل أمن المعلومات .

لذلك تتولد الحاجة لفهم كيف تتداخل المنظمة مع مواردها البشرية وعملياتها وبناها التقنية التحتية، ويجب معرفة كيف تستطيع المنظمة فهم العوامل الثقافية والبشرية المؤثرة من أجل إدارة المخاطر التي تواجهها والسعي لحماية نظم معلوماتها .

وينطلق الباحث في بحثه بمزج النظريات التي ساهمت في تطوير إدارة ناجحة لأمن المعلومات حيث لاقت رواجاً بين كثير من الباحثين السابقين والممارسين لنظم المعلومات وأمنها . وقد وضع الباحث الإطار المفاهيمي للدراسة بعد قيامه باشتقاق متغيرات الدراسة من مستوحى دراسات عديدة والرجوع إلى معايير ومقاييس وهيئات عالمية تعنى بأمن نظم المعلومات وتمت عملية مزاوجة المتغيرات المتقاربة وعنيَّ الباحث بوضع متغيرات ذات صلة ببيئة الدراسة ومناسبة لتقييم واقع إدارة أمن نظم المعلومات في الاطار العام لأهداف الدراسة وتم صياغة كيفية إشتقاق المتغيرت كما في الملحق رقم (1).

وبذلك يعرض الباحث تصوره ومنطلقاته في الدراسة من خلال تداخل متغيرات الدراسة مع بيئة الدراسة والبيئة الخارجية ويوضح الشكل التالي رقم (2-1) الاطار المفاهيمي للدراسة.

شكل رقم (2-1):إطار مفاهيم الدراسة



هياكل مفاهيم الدراسة - Conceptual Framework
إدارة أمن نظم المعلومات(إعداد الباحث،2012)

الفصل الثالث

الإطار النظري للدراسة

- ❖المبحث الأول : نظم المعلومات
- ❖المبحث الثاني : تطوير نظم المعلومات والتعهيد
- ❖المبحث الثالث: أمن نظم المعلومات
- ❖المبحث الرابع: تهديدات أمن نظم المعلومات وإدارة المخاطر
- ❖المبحث الخامس : وسائل حماية أمن نظم المعلومات
- ❖المبحث السادس : الكليات التقنية في قطاع غزة

المبحث الاول

نظم المعلومات

مقدمة:

تتطور التكنولوجيا من حولنا، وتحمل معها جديد التغيير، وتتبدل معها أشكال نقل المعلومة وتتفتح آفاق جديدة في تمثيل البيانات بهيئات وأنماط متعددة منها ما كان معروفاً وتطور ومنها ما ابتكر وتغير !

ويحاول الباحث من خلال هذا المبحث القاء الضوء على مفهوم نظم المعلومات، ويعطي تصوراً للفرق بين مفهوم تكنولوجيا المعلومات ونظم المعلومات ثم يشرح مكونات نظم المعلومات والصفات الجيدة للمعلومات ويتطرق بالحديث عن كفاءة نظم المعلومات وتكلفة المعلومات لينهي هذا المبحث بالحديث حول أنواع نظم المعلومات.

تعريف ماهية نظم المعلومات :

بحسب مفهوم نظرية النظم والتي تقضي بأن النظام بشكله المعقد يتكون من عدة نظم منفردة وتؤكد على علاقة الأجزاء والمكونات بجميع الوحدات ثم علاقة جميع الوحدات بالنظم الأخرى ، وأتخذ خبراء نظم المعلومات الإدارية ونظم المعلومات المحوسبة كمهاد فلسفي في فهم وإدراك عمل النظم المحوسبة .

وبذلك يعرف ياسين(2006،ص19) نظام المعلومات بأنه : التكوين المتفاعل بين مكونات جوهرية للنظم والمعلومات ويتوسع ليعرفه على أنه توليفة أو تركيبة منظمة من الأفراد، المكونات المادية للحاسوب، البرامج، شبكات الاتصالات، وموارد البيانات التي يتم جمعها ومعالجتها وتحويلها لمعلومات وبالتالي توزيعها إلى المستفيدين في المنظمة.

ويرى الباحث أن التعامل مع مصطلح نظام المعلومات إنما يُعنى به الحديث عن جزء من النظام الكلي للمعلومات وسيجري التعامل بصيغة الجمع أي نظم المعلومات تعزيزاً لمفهوم نظرية النظم.

تكنولوجيا المعلومات Information Technology :

يسميها البعض تقنية المعلومات حيث تعرب الكلمة الانجليزية (Technology) إلى تقنية، كما وتعرف اختصاراً (IT).

وقد عرفها Paquin (1990,p17) بأنها الوسائل المستعملة لإنتاج، معالجة، تخزين، استرجاع، وإرسال المعلومة، سواء كانت في شكل صوتي أو كتابي أو صورة.

ويعرفها الهادي(1994،ص205) بأنها نتاجاً مناسباً للتلاحم والتكامل بين كل من تكنولوجيا الحاسوب وتكنولوجيا الاتصالات .

ويركز تعريف الهادي على الجمع بين التقنيات التي تحقق تكاملاً معلوماتياً سواء الحاسوبية منها أو تقنيات الشبكات والاتصالات وهو بذلك يشمل كل المكونات المادية لنظام المعلومات، كما سنرى لاحقاً..

آثار تكنولوجيا المعلومات على إدارة المؤسسة :

- المساعدة على تركيز الإدارة في المهام الإستراتيجية والتخفيف من الأعباء الروتينية.
- المساعدة في تخفيض حجم الهيكلية الإدارية وتقليص النفقات.
- توزيع قدرة الإدارة العليا على التخطيط والرقابة والسماح بدرجة أكبر من اللامركزية وتفويض السلطة.
- توسيع وتنمية وتنشيط قنوات الاتصال وابتكار أساليب جديدة في الاتصالات.
- المساعدة على سرعة التأقلم والتكيف ومعرفة التغيرات نتيجة سرعة العلم بها.
- المساعدة على تطوير وسائل الإنتاج واستحداث المنتجات الجديدة وتحديث أساليب التسويق.

تكنولوجيا المعلومات أَم نظم المعلومات :

يخلط الكثيرون بين مفهوم تكنولوجيا المعلومات ونظم المعلومات، وذلك لتداخل المكونات وربما الأهداف التي تتحقق ،لكن لا يمكن القول بان كلاهما بديل للآخر حيث أن تكنولوجيا المعلومات تتضمن المكونات المستخدمة على نطاق واسع في أنشطة ومعالجة وتخزين البيانات واسترجاع وعرض المعلومات بأشكالها المختلفة (نصوص، أرقام، صور، أفلام، ووسائط متعددة).

ولأن تكنولوجيا المعلومات ليست غاية وإنما هي وسائل تستخدمها النظم ضمن إطار التوليفة الشاملة لدعم نظم المعلومات، فإن الباحث يرى أن تكنولوجيا المعلومات هي إحدى مكونات نظم المعلومات.

مكونات نظام المعلومات IS Infrastructure :

يتضمن نظام المعلومات مجموعة من المكونات التي يشار لها بالبنية التحتية المكونة لنظم المعلومات وتترابط جميع هذه المكونات ليتم ادخال ومعالجة، وحفظ، استرجاع، ونشر وتوزيع المعلومات ومن ثم تنفيذ التغذية العكسية، وإجراء عمليات التحكم في الأنشطة والمهام، وهي :

1. **المكونات التقنية (مكونات تكنولوجيا المعلومات) :**

وتشمل مكونات التقنية الملموسة وغير الملموسة وتسمى تكنولوجيا المعلومات(IT) أو تكنلوجيا المعلومات والاتصالات(CIT) وتضم (Stair & Reynolds,2010) :

1.1. المكونات المادية للحاسوب Hardware

وتشمل كل انواع الحاسوب وما يتصل به من معدات كالطابعات والماسحات الضوئية وأجهزة الرسوم و أي أجهزة أخرى تشملها تستحدثها تكنولوجيا المعلومات.

1.2. المكونات البرمجية للحاسوب Software

وتشمل لغات البرمجة التقليدية والحديثة بكل مستوياتها والبرامج التي تعد بها ونظم التشغيل المختلفة، وقواعد البيانات ونظم دعم القرارات وقواعد المعرفة والنظم الخبيرة ولغات الذكاء الاصطناعي .

1.3. الشبكات ووسائط الاتصال

تتشكل شبكة الحاسوب من ربط مجموعة أجهزة حاسوب باستخدام وسائط الاتصال لتكوين شبكة تتبادل البيانات والمعلومات بين نظم الحاسوب المرتبطة بالشبكة .

ومن مبدأ أهمية الشبكات فقد ذكر الكثيرون أنه لا معنى ولا قيمة لأي حاسوب يوجد منفرداً ويعمل بصورة مستقلة من دون اتصاله من خلال الشبكة مع نظم الحاسوب الاخرى(ياسين،2006،ص162) .

2. الأفراد Human Resources

يرى الكثيرون أن أثمن مورد في بنية نظم المعلومات هو ما لدى النظام من ثروة معرفية وفكرية وإدارية وتنظيمية متمثلة بالعاملين في إدارة هذه النظم، بل إن العامل الجوهري والحاسم الذي يرجح نجاح اوفشل نظم المعلومات يتمثل بالإدارة ومواردها الانسانية وكوادرها التقنية المتخصصة (ياسين،2006،ص172)

ويمكن تحديد فئات الموارد البشرية إلى (Laudon&Laudon,2010):

- المستفيد النهائي End User

وهو كل من يستخدم نظم المعلومات في داخل دائرة النظام او خارجه، حيث يشمل من يستفيد من مخرجات النظام في تنفيذ الوظائف والمهام الموكلة اليه ولتنفيذ عمليات وأنشطة الأعمال وعادة يوجدون ضمن ال .

- العاملون في حقل المعرفة Knowledge Worker

وهم من يقوم بإنتاج المعرفة، تخزينها وتوزيعها ويقعون في المستويات التنظيمية العليا .

- المختصون في مجال تكنولوجيا المعلومات .

ويشمل هؤلاء العاملون في حقل نظم المعلومات من لجان الاشراف ومراقبة نظم المعلومات ومطوري النظم ومحللي النظم، مهندسي الحاسوب، المبرمجين، مديري الشبكات، والفنيين وغيرهم .

3. **الاجراءات والسياسات**

هي عمليات تتضمن وصف وترتيب مجموعة الخطوات والتعليمات المحددة لإنجاز العمليات الحاسوبية حيث ترسم السياسة العامة لنظام عمل الأجهزة والبرمجيات وتنسيق عمل الأفراد ضمن منظومة تحقق أهداف نظام المعلومات الجزئي أو نظم المعلومات بشكل كلي .

4. **البيانات والمعلومات**

وهي بمثابة الوقود المشغل لنظام المعلومات، وعصب المؤسسة ومحركها الي تدور فيه للتطوير والبناء.

وتلخيصاً لما تقدم من مكونات لنظم المعلومات يوضح الشكل التالي هذه المكونات .

شكل رقم (3-1) يوضح مكونات نظم المعلومات .

مكونات نظم المعلومات التقليدية

المصدر : Course Technology – Cent age Learning

خصائص المعلومات الجيدة :

يتطلب المستخدم أشكال متعددة من المعلومات، وهذه المعلومات التي يتم الحصول عليها يمكن أن تصدر بشكل رسالة، أو تقرير، أو نموذج، ويمكن ان تكون بهيئة صوتية أو مرئية أو مكتوبة .

وتحتاج الإدارة للتقارير للأسباب التالية (Bagad,2008,p15):

- لتحسين عملية اتخاذ القرارات .
- لإطلاع الادارات المختلفة أو المختصة على ما يجري في المنظمة .
- لتحفيز وتوزيع المهام داخل المنظمة .
- لدعم الإدارة العليا في العمل المدروس المبني على اسس معلوماتية

- لتقييم القرارات الحالية
- ابراز ولفت انتباه الادارات حول المعلومات المتوفرة.

ويضيف(Bagad,2008,p15) أن المعلومات الجيدة يجب ان تتصف بالخصائص التالية :

- الوقتية : وهي تشير إلى أن المعلومات يجب ان تتوافر في الوقت المناسب
- الايجاز : حيث ان تلقي المستخدم لمعلومات موجزة سيوفر عليه الوقت ويمكن الوصول للايجاز عبر تلخيص البيانات ذات الصلة .
- الشمولية : وهي ان تحتوي المعلومات كل البيانات المطلوبة لاتخاذ القرار.
- الدقة : وهي نسبة المعلومات الصحيحة إلى المجموع الكلي من البيانات المعالج خلال فترة محددة.
- التناسبية (وثيق الصلة) : وتعني ان المعلومات تعطى على قدر الصلاحيات، وبقدر من الحاجة لها .
- الوضوح: وتعني ان المعلومات يجب ان تقدم بهيئة واضحة ومقروءة، وبالتالي يجب على من يقدم المعلومات ان يكون على علم بمستوى معرفة المستقبل وثقافته وماذا يحب .

خصائص ثانوية للمعلومات :

ولكي يتاح الاعتماد على المعلومات والوثوق إليها يلزم توافر مجموعة من الخصائص الفرعية (الثانوية) وهي: (Bodnar &William S, 1995)

1. يمكن الوصول إليها :أي انه يمكن الوصول للمعلومة عندما نحتاجها وبالشكل الذي نريده.
2. قابلة للتحقيق : بمعنى أن تكون المعلومات واقعية يمكن تحقيقها، أي ليست هناك صعوبة في تحقيقها
3. الحيادية : بمعنى أن تكون المعلومات خالية من أي تحيز أو مآرب شخصية وأن تعكس الأحداث والنشاطات بطريقة عادلة ومهنية .
4. لها قيمة تنبؤية : بمعنى أن المعلومة مفيدة لمتخذ القرار كي يتنبأ بمآل الحال التي سيتم اتخاذ القرار بشأنه
5. لها قيمة رقابية : بمعنى أن تكون المعلومة مفيدة لمتخذ القرار للرقابة والتقييم من خلال عمليات التغذية العكسية وتصحيح الأخطاء التي يمكن أن تنتج عن سوء الاستخدام أو عدم الكفاءة

6. الثبات : بمعنى الثبات على استخدام نفس الطرق والأساليب المعتمدة في قياس وتوصيل المعلومات من فترة لأخرى، وإذا ما دعت الحاجة إلى أي تغيير فيجب التنويه عن ذلك لكي يتم اخذ ذلك بالاعتبار من قبل المستخدم.
7. قابلة للمقارنة : أي أن تصاحب المعلومات قدرة على إجراء المقارنات من فترة محددة مع وحدات مشابهة في مؤسسات أخرى ضمن نفس المجال.

فوائد ووظائف نظام المعلومات :

يلخص الشيخ (1998،ص46) وظائف نظام المعلومات في ثلاث مجالات اساسية :

- يشكل مصدر متوفر وسريع للمعلومات التي تساعد الادارات في عملية صناعة القرارات .
- يساهم في تعزيز الانتاجية والفاعلية، ورضا العملاء .
- يعمل على تحسين أداء وظائف الادارات المختلفة في المؤسسات .

كفاءة نظام المعلومات :

تعني الكفاءة مدى تحقيق النظام للأهداف التي أنشئ من أجلها، أي الوصول إلى الصورة الواقعية لما تحقق ومقارنة ذلك مع ما هو مستهدف تحقيقه في فترة زمنية محددة، وتتحدد كفاءة نظام المعلومات بمقدرته على توفير المعلومات الضرورية عن الماضي والحاضر والمستقبل بالدقة والملائمة والوقت والتكلفة المناسبة، وبمقدار مساهمته في مساعدة الإدارة في مهام التخطيط و الرقابة واتخاذ القرارات(McMahon,1993).

مقاييس كفاءة نظام المعلومات:

ويرى المغربي (2002) أن الكفاءة تقررها اربعة مؤشرات هي:

1. الدقة : وتعني ان تتوفر درجة مناسبة من الدقة في المعلومات المعدة لاستخدامها بدرجة عالية من الثقة في الاغراض الادارية مثل التخطيط والرقابة واتخاذ القرارات .
2. الملائمة : وتعني أن تتطابق انواع ومواصفات البيانات والمعلومات مع احتياجات المستخدمين.
3. الوقت المناسب : وتعني مراعاة عامل الزمن عن توفير البيانات والمعلومات لأغراض اتخاذ القرارات.

وتشكل هذه المؤشرات الثلاثة الطرف الاول في موازنة الكفاءة، وذلك لأن الخلل في أي من هذه المؤشرات سوف يؤثر سلباً على المنافع المتأتية من النظام، وتتراوح هذه السلبية بين التأثير في القرارات المتخذة في حال عدم دقة المعلومات (حالة انعدام مؤشر الدقة) إلى انعدام القيمة من هذه المعلومات (حالة عدم الملائمة، أو لم يتم الحصول عليها في الوقت المناسب)

4. مؤشر التكلفة المناسبة:

ويمثل هذا المؤشر الطرف الثاني في موازنة الكفاءة، إذ يجب توفر المعلومات الضرورية بالتكلفة الملائمة، أي أن المنافع المتأتية من نظام المعلومات يجب أن يوازي أو يفوق التكاليف المترتبة على استخدام هذا النظام وإلا اختلت الموازنة وانعدمت أو تدنت الكفاءة تبعاً لذلك .

تكلفة إنتاج المعلومات :

تتضمن تكلفة إنتاج المعلومات كل من الوقت والموارد المستنفذة في:

- جمع البيانات
- معالجة البيانات
- تخزين البيانات
- توزيع المعلومات على مستخدميها.

ويرى البعض إن تكلفة المعلومات ومنفعتها من الصعب احتسابها وخاصة عندما تريد التوصل إلى معرفة تؤهلك لصناعة قرار .

ويرى الباحث ان تكلفة الحصول على البيانات قد تكاد تكون منخفضة جداً هذه الايام بسبب توافر العديد من مصادر المعلومات المجانية عبر شبكة الإنترنت ولكن التعقيدات تكمن في أنك كيف ستستطيع استثمار هذه البيانات بالطريقة التي ستعدم التكلفة.

أنواع نظم المعلومات :

يمكن أن تصنف نظم المعلومات كأحدى التصنيفات التالية:

- نظم العمليات التشغيلية Transaction Processing Systems (TPS)

تعالج حجم كبير من البيانات والأعمال الروتينية

- نظم معلومات إدارية Management Information Systems (MIS)

هي عبارة عن أنظمة معلومات محوسبة تدعم مجموعة واسعة من وظائف الأعمال أكثر من أنظمة معالجة بيانات.

- أنظمة أتمتة المكاتب Office Automation Systems (OAS)

تعالج المعلومات مع السماح بالمشاركة على مستوى المنظمة مثل البرمجيات Spread Sheet والمعالجة باستخدام Word والبريد الالكتروني

- أنظمة دعم القرارات Decision Support Systems (DSS)

هي أنظمة معلومات تستخدم قواعد البيانات الخاصة والنماذج في دعم متخذي القرارات شبه المهيكله في المراحل المختلفة.

- النظم الخبيرة Expert Systems (ES)

تستخدم خبرة متخذي القرار في تقديم المشورة والنصح للمدراء في اتخاذ القرارات الصعبة

- نظم دعم الإدارة العليا Executive Support Systems (ESS)

تصمم لدعم الإدارة العليا بالمعلومات والنماذج التحليلية اللازمة لصنع القرارات غير المهيكلة (الاستراتيجية)

- التجارةالالكترونية E-Commerce(Laudon&Laudon,2010)(Rainer&Cegielski,2011) .

ومن الممكن تقسيم وتصنيف نظم المعلومات، على أساس المستويات التنظيمية الأساسية التي تقدم الدعم لها، ابتداء من المستوى الأدنى، وصعوداً إلى المستويات الأعلى، وكآلاتي:

(1) مستوى العمليات Operational Level: والذي يمثل القاعدة الأساسية لحركة المنظمة، ويشتمل على إدارة عملياتها

(2) المستوى المعرفي Knowledge Level : والذي يشتمل على العاملين في مجالات البيانات والمعلومات والمعرفة

(3) المستوى الإداري Management Level : والذي يشتمل على إدارات المنظمة الوسطى

(4) المستوى الإستراتيجي Strategic Level : والذي يشتمل على الإدارات العليا، أو إدارات العمل الاستراتيجي في المنظمة (قنديلجي والجنابي،2008).

المبحث الثاني

تطوير نظم المعلومات والتعهيد

مقدمة :

تمر نظم المعلومات بدورة حياة شبيهة بدورة حياة الأنسان، وهي دورة تمر بمراحل أساسية مترابطة ومتداخلة وتحتاج عملية التطوير جهود مستمرة يتم فيها تحديد فجوة المعلومات والتغلب عليها من أجل التوصل إلى إنجازات تستفيد من استخدام واستثمار التكنولوجيا داخل المنظمة .

يهدف الباحث هنا إلى تسليط الضوء على كيفية تطور نظم المعلومات وبعض الخدمات التي من الممكن الاستفادة منها كالإستعانة بالمصادر الخارجية، ويأمل الباحث أن يقدم هذه المفاهيم بسلاسة ويسر.

دورة حياة تطوير النظام :

تعتبر من أهم المنهجيات لتحليل وتصميم وتطوير نظم المعلومات وخصوصاً نظم المعلومات الادارية، وهي طريقة ذات طابع هيكيلي منظم وتتكون من مراحل أساسية مترابطة ومتكاملة .

ويتم تمثيل عملية التطوير باستخدام النموذج التدفقي Waterfall Model حيث ان مخرجات الأنشطة الفرعية في أي مرحلة سابقة تعتبر مدخلات المرحلة التالية والشكل (3-2) يبين نموذج التدفق لدورة حياة النظم (ياسين،2006،ص179).

شكل رقم (3-2)يوضح مراحل التدفق لدورة حياة نظم المعلومات .

المصدر(Satzinger&Jakson,2009),Systems Analysis and Design in a Changing World-5th edition , P.41

ويلاحظ من الشكل السابق(3-2) ان النموذج يسير في إتجاه دوراني مستمر ليمثل عمليات التقييم وإجراء التغذية العكسية وعمليات الرقابة على المراحل المختلفة، وذلك حتى يتمكن مطوري النظم من معرفة مواطن الخلل وإصلاحها.

ويقوم مطوري النظم بإجراء عمليات التقييم المباشر قصير الأجل من خلال مقارنة التكاليف الفعلية مع المنافع أو الفوائد المنظورة ، كما يظهر في الجدول رقم (3-1).

جدول رقم (3-1) : يبين مقارنة التكاليف الفعلية بالمنافع المنظورة

التكاليف الفعلية	المنافع المنظورة
تكلفة المكونات المادية للحاسوب	زيادة الانتاجية
تكلفة المكونات البرمجية للنظام	تحسين جودة الخدمات المقدمة
تكلفة مكونات ومستلزمات وإعدادات الشبكة ووسائط الاتصال	تخفيض لتكاليف التشغيلية
تكلفة تأسيس الاجهزة وصيانتها	تحسين الاداء الكلي للمنظمة
تكلفة تدريب الأفراد	السرعة في حل المشكلات
تكلفة تشغيل الأفراد	الرضا المتزايد للمستفيدين

المصدر : (ياسين، 2006،ص186)

مداخل تطوير نظم المعلومات :

تستخدم منهجيات عديدة في عملية تطوير النظم وتتنوع هذه المنهجيات بين المعقدة والمكلفة للوقت والمال بما تتطلبه من فرق من المحللين والمبرمجين والمراجعين، وبين منهجيات تعتمد على المستخدم نفسه في اقتناء وتطوير نماذج عمل خاصة باستخدام الحزم البرمجية المكتبية سهلة الاستخدام والموجهة لهذا المستخدم والتي أصبحت تساعده في تسيير أعماله دون إنتظار حلول محللي ومبرمجي النظم .

حيث تتجه بعض المنظمات إلى اقتناء برمجيات نظم المعلومات عبر تطوير نظمها من خلال حزم برامج التطبيقات التي تقدمها شركات البرمجيات الكبرى والمتخصصة في إيجاد الحلول لتطوير نظم المعلومات المختلفة في كافة الميادين، ولكن ذلك يقع تحت قائمة من المعايير للمفاضلة بين حزم برامج التطبيقات عند الاختيار والشراء وقد ذكر (ياسين،2006،ص:194-195) مجموعة من اهم هذه المعايير :

- معيار الوظيفة: حيث يتساءل عن الوظائف المطلوبة من البرنامج، التكاليف الإضافية المطلوبة، كيف سيساعد الإدارة في تلبية احتياجاتها .

- معيار المرونة : ويتساءل إلى أي درجة يمكن تعديل وتغيير برنامج التطبيق، إمكانات التطوير في المستقبل، هل يمكن تحقيق التعاضد والاتصال والتوافق مع برمجيات أخرى
- معيار الصداقة وسهولة الاستخدام : ويتساءل حول الكفاءة التي سيجنيها المستفيد، سهولة وبساطة البرنامج، ووجود تسهيلات المساعدة
- معيار العائد والتكلفة حيث يجري مقارنة التكاليف المنظورة وغير المنظورة مع العائد المتحقق من جراء استخدام هذا النظام الجديد.
- معيار التوافق مع المكونات المادية الحالية لنظم المعلومات.

قبول نظم المعلومات من قبل الأفراد :

ويعني القبول أن يكون النظام مقبولاً من قبل المستفيدين ومستخدمي هذه النظم بشكل مباشر، ذلك لأنه مهما بلغت قدرة النظام الجديد وفاعليته، فلا يمكن إستمراره دون تعاون وقبول من قبل الاطراف المستفيدة والمسئولة عن تشغيله وإدارته، لذلك فإن المصمم مدعو لإتاحة الفرصة أمام الأفراد المتأثرين بالنظام بأن يشاركوا بفاعلية في تصميم النظام الجديد، لأنهم في الواقع سيقع عليهم عبء تشغيل هذه النظم، لذا فإن السعي نحو بناء نظام كفء ومرن وبسيط وموثوق لابد أن يتكامل مع السعي لتحقيق قبول النظام بما يلعب الأفراد من دور كبير في تقرير مدى نجاح أو فشل نظم المعلومات.

ومن هنا لابد من توافر درجة ملائمة من الاقتناع من جانب أولئك الأفراد بأهمية هذه النظم لهم وللمنظمة من أجل تجنب المقاومات التي قد يبديها هؤلاء الأفراد، فالطبيعة البشرية تمتاز بميل إلى مقاومة التغيير (الحسنية،2002).

ويعلق الباحث بأن مسألة أمن المعلومات قد تكون أحد أهم مبررات مقاومي هذه النظم، حيث أن الهاجس الأمني يلعب دوراً هاماً في تصور قبول هذه النظم لدى الأفراد، وكلما أزداد الامر تعلقاً بالأسرار والأموال ازداد الرفض والمقاومة، وعلى مطوري النظم وخبراء أمن المعلومات الإستجابة لمثل هذه الهواجس .

التعهيد (الأستعانة بالمصادر الخارجية) IT-Outsourcing

مع تطور نظم المعلومات واتساع تأثيرها في منظمات الأعمال الحديثة ومع التغير والتعقيد في تكنولوجيا المعلومات بالإضافة إلى تزايد حصة الأعمال وأدوات تكنولوجيا المعلومات والاتصالات في إجمالي النفقات الرأسمالية في الشركات الكبيرة التي تبلغ حوالي النصف، فقد لجأت معظم منظمات الأعمال المتوسطة والكبيرة إلى البحث عن بيوت خبرة متخصصة لإقتناء وشراء وتطوير نظم وشبكات الحاسوب بمختلف أشكالها وأنواعها وتلجأ معظم المنظمات نحو الاعتماد على مصادر وجهات خارجية لإقتناء أو تطوير نظم المعلومات الإدارية ليس بسبب الفوائد الحالية المتوقعة التي تحصل عليها وإنما أحياناً لأن هذه المنظمات لا تملك القدرات التنظيمية والتقنية والمعرفية اللازمة للشروع بتحليل وتصميم وتشغيل نظم المعلومات المحوسبة بالاعتماد على الموارد المتاحة (ياسين،2006،ص198).

ويشير عثمان(2012) أنه كثر تداول كلمة التعهيد في الآونة الأخيرة، والحقيقة أن كلمة التعهيد دائماً تحمل معنيين معني لغوي Linguistic meaning ومعني اصطلاحي Technical meaning، والمعني اللغوي للتعهيد هو أن يتعهد طرف ما بتقديم خدمة أو عمل إلي طرف آخر بمقابل مادي يتفق عليه الطرفان، أما المعني الاصطلاحي هنا فسيكون من منظور تقني حيث يتعهد ذوي الخبرات الذين لديهم قدرة علي الإبداع والابتكار في مجالات البرمجة وتكنولوجيا المعلومات بنقل خبراتهم من دول غنية بالخبرات مثل الهند والصين إلي دول أخري غنية بالمال مثل أمريكا وأوروبا وتعتبر هذه المنظومة المتحضرة بمثابة صناعة إستراتيجية يطلق عليها البعض " صناعة التعهيد Outsourcing .

وعرف محفوظ(2010،ص4) التعهيد بأنه وصف لما يقوم به طرف من التعهد بتقديم خدمة لطرف اخر بمقابل يتفق عليه الطرفين، وهو وصف لما تلجأ اليه المؤسسات أو الشركات عندما تعهد لجهات خارجية متخصصة بأداء بعض من أعمالها بالنيابة عنها، حتى تستطيع التركيز على أعمالها الرئيسية.

ويعرفه ياسين(2006،ص198) بأنه العملية التي تتضمن شراء الحزم المتكاملة لنظم المعلومات الحاسوبية، شبكات اتصالات البيانات، نظم تخطيط موارد المشروع، نظم التجارة الالكترونية، برامج ونظم الحكومة الالكترونية وغيرها من شركات تكنولوجيا المعلومات والاتصالات أو من الشركات المنتجة للبرمجيات وبيوت الخبرة العلمية .

ويضيف ياسين(2006) أن التوريد الخارجي أو التعهيد قد يكون في مجالات أخرى غير المكونات المادية والبرمجية والتكنولوجيا الشبكية لنظم المعلومات الحاسوبية حيث تعقد اتفاقيات

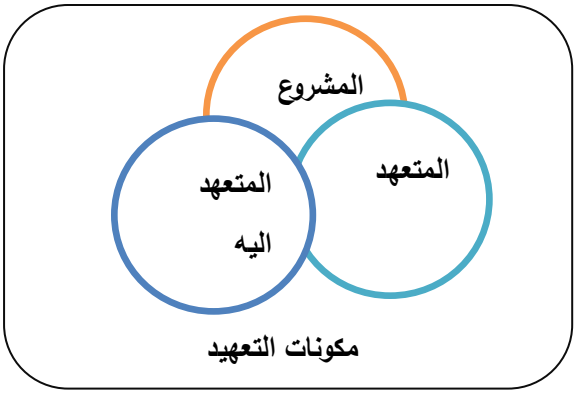
التعهيد لتنفيذ تسهيلات أو الحصول على خدمات الكترونية أو من أجل تلقي الاستشارات من شركات التدريب والاستشارات العالمية .

وعرفه Power an et. al (2006,p4) بأنه العملية التي يتم من خلالها تحويل انتاج عمل ما لجهة خارجية، وهذا المفهوم العام يتشابه مع ما تواجه المنظمات من قرارات تتعلق بإدخال مصادر جديدة والتوسع بذلك لإنتاج منتج أو خدمه معينة أم القيام باقتنائه عبر طرف خارجي .

وقد حدد تعريف Power ثلاث من الجهات التي تتكون منها عملية التعهيد، ويظهر الشكل (3-3) مكونات التعهيد حسب التعريف السابق وتشمل :

- المتعهد إليه : وهو مستقبل الخدمة أو من يجري عملية التعهيد بغرض جلب الفائدة
- المتعهد : وهو مقدم الخدمات
- المشروع : وهو ما يجري فيه التعهيد، الخدمات المرجو ان يقدمها المتعهد للمتعهد إليه.

شكل رقم (3-3) : مكونات التعهيد



المصدر بتصرف: Power and et al.(2006), The Outsourcing Handbook

وبناءاً على ما سبق يعرفه الباحث بأنه : عملية تتضمن التعاقد مع طرف خارجي بهدف تزويد المؤسسة بخدمات تكنولوجيا المعلومات وخاصة البرمجيات أو تطوير البرمجيات الحالية، وتسعى المؤسسات من خلال ذلك لتقليل التكاليف والتغلب على نقص الخبرات في هذا المجال.

أنواع التعهيد :

يقسم التعهيد طبقاً لحجم العمل إلى :

- تعهيد على مستوى عملية محددة
- تعهيد على مستوى المشروع ككل

ويقسم حسب المكان إلى :

- داخلي (في المؤسسة نفسها)

- خارجي وهو بدوره ينقسم إلى :
  - محلي (داخل الدولة نفسها)
  - خارج الدولة

ويسهم التعهيد في نقل بعض مخاطر الحوادث الأمنية، وتسعى غالبية المنظمات إلى تعهيد عمليات مخاطر الكوارث أملاً منها في تقليل الخسائر وتحقيق اهداف الاستمرارية في العمل (Pipkin,2000,p84)

مزايا التعهيد:

1. الاقتصاد في التكاليف : حيث أن اعتماد استراتيجية التوريد الخارجي هو أقل تكلفة من مداخل التطوير والتصميم الأخرى (في معظم الحالات) وذلك لأن لبيوت الخبرة العالمية معارف وخبرات ومهارات تقنية عالية ومتراكمة وبالتالي تستطيع تقديم عروض منافسة لمشروعات تصميم وتطوير نظم المعلومات الحاسوبية وبمواصفات قياسية عالمية .
2. جودة الخدمة المعلوماتية : تقدم بيوت الخبرة العالمية وشركات تكنولوجيا المعلومات والاتصالات وشركات تطوير البرمجيات خدمات تقنية راقية وبمعايير عالمية لا تستطيع شركات التكنولوجيا المحلية أن تفي بها .
3. الموثوقية : عقود تطوير نظم المعلومات الحاسوبية أو تأسيس نظم وأدوات تكنولوجيا المعلومات محدد بفترة معينة وبسعر ثابت وبالتزامات واضحة من قبل جميع الأطراف. ومن الصعب جداً تغيير بنود العقود أو التهرب منها لأن ذلك سيحمل الطرف غير الملتزم إجراءات جزائية مؤلمة وباهظة .
4. المرونة: حيث يمكن الاستفادة من القدرات التقنية للمورد الخارجي في بناء وتطوير نظم معلومات تتصف بالمرونة الكافية لاستيعاب النمو الذي قد يحصل في أنشطة أعمال المنظمة المستفيدة(Poulin,2006,p27).

عيوب التعهيد:

ذكر ياسين (2006) مجموعة من العيوب وهي :

1. ضياع فرص الاعتماد على الذات

لا يوجد أغلى من فرص الاعتماد على الذات وتطوير المهارات والقدرات المتاحة بالنسبة لمنظمات الإعمال والمؤسسات الاقتصادية والاجتماعية العامة في الدول النامية . والاعتماد يتطلب الانفتاح والتفاعل الحي بين الفعاليات المختلفة

2. فقدان السيطرة

عندما تفوض المنظمة المستفيدة مسؤولية تطوير نظم أعمالها لشركات أجنبية من المحتمل فقدان السيطرة على وظائف وأنشطة هذه النظم وما تحتويه من تقنيات وأدوات.

3. فقدان الأسرار

الأسرار الاقتصادية والتجارية والتكنولوجية قد تتسرب إلى المنافسين بسبب الاعتماد على مصادر خارجية في تطوير نظم المعلومات وبخاصة إذا كانت هذه النظم موجهة نحو هدف اكتساب أو امتلاك الميزة التنافسية المستدامة.

وفي دراسة أجراها Khalfan (2003) حول تعهيد خدمات نظم المعلومات في المؤسسات العامة والخاصة بالكويت والمخاطر المترتبة عنها تبين أن أكثر خمسة مخاطر مترتبة عن التعهيد يواجهها القطاع الخاص هي :

1- القضايا الأمنية

وكانت دراسة(Collins and Millen ,1995) للقطاع الخاص في الولايات المتحدة قد توصلت لنفس النتيجة لحالة التكاليف الكامنة والتي لم تيتم تحديدها في عقود التعهيد.

وهو نفس العامل الذي لاحظه Barthelemy (2001) حيث أوضح أنه على الرغم من وضوح منافع التعهيد إلا انها غالباً ما تضمحل وتتآكل نتيجة لتكاليف كأمنة لا يأخذها صانعي قرار التعهيد بالحسبان.

2- فقدان المرونة والسيطرة.

وتوصلت دراسة اجراها Lacity, Hirschheim and Willcocks (1994) بأن 53% من مبحوثي العينة المختارة قد وافقوا هذا العامل .

3- نقص خبرات وفن التعامل مع التعهيد.

4- القدرة على إدارة وتشغيل النظم الجديدة.

بينما كانت أكثر خمسة مخاطر يواجهها القطاع العام هي :

1- القضايا الأمنية (وثوقية البيانات).

2- القدرة على إدارة وتشغيل النظم الجديدة.

3- نقص في الموظفين ذوي الخبرات .

4- التكاليف الكامنة (التي لم يتم ذكرها في عقد التعهيد).

5- عدم المقدرة على التخطيط والإدارة .

وبذلك يرى الباحث أنه من الضروري أن تتم دراسة المتطلبات اللازمة والمخاطر المتأتية من عمليات التعهيد بعناية، كما أنه يجب أن لا تكون التخوفات والمعوقات لتبني التعهيد بمثابة حاجز لعدم استخدامه لما فيه أيضاً من فوائد ومنافع للمؤسسات وخاصة لترشيد التكاليف .

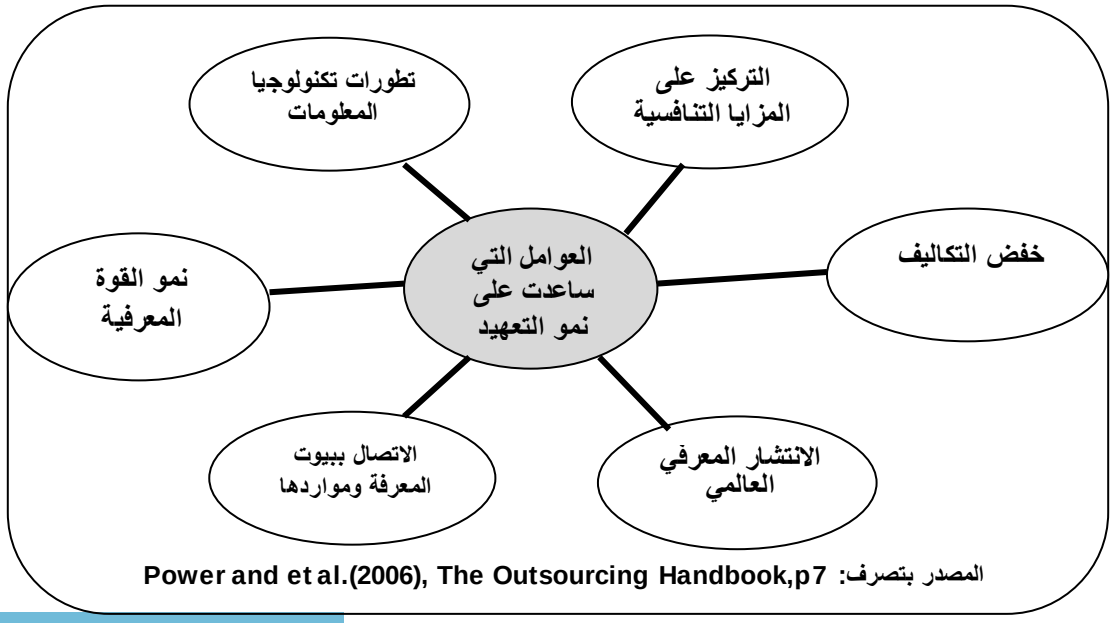
نماذج التعهيد (يسر، 2007،ص17-18):

1. التعهيد التقليدي : وهو النموذج الكلاسيكي للتعهيد، ويسمي التعهيد للمصادر الخارجية بشكل كامل، حيث يسلم مزود خدمة واحد فقط الخدمة إلى العميل وهو قليل التبعات ويقلل النفقات .
2. التعهيد الثنائي : حيث يستخدم في حالة كون نطاق العمل أكبر من قدرة أو طاقة متعاقد واحد وعادة يكون أحد المزودين داخلياً أو مباشراً (المتعاقد الرئيسي) والآخر خارجيا ويسمى المتعاقد الثانوي .
3. التعهيد المتعدد : ويطلق عليه أيضا (التعهيد الإنتقائي) حيث تقوم المؤسسة بالتعامل مع جميع المزودين وهي مسئولة عن التنسيق بينهم وضمان التكامل بين الخدمات من قبل المتعهدين ويسعى لاختيار المزودين الأكثر ملائمة له طبقاً لكفاءتهم والتكاليف المطلوبة .
4. التحالف(الائتلاف) : حيث يندمج أكثر من متعهد لتزويد الخدمة، ويعين أحدهم كمتعهد رئيس يقوم بإدارة علاقة الائتلاف وعناصره.
5. التضامن : ويكون عندما تؤسس شركتين مستقلتين أو أكثر شركة جديدة لتقديم خدمة معينة لا يستطيع ان يزودها أي من الشركتين بشكل منفرد .
6. الاستعانة بمصدر داخلي (التعهيد الداخلي): حيث تخصص المؤسسة إحدى الإدارات الداخلية وتعاملها ككيان خارجي لتزويدها بالخدمات من خلال عقود غير رسمية وتسمح لهذه الإدارة بتزويد الخدمات لعملاء آخرين في السوق .

عوامل نمو التعهيد :

يرى Power and et al. (2006) أن هنالك مجموعة من العوامل التي ساعدت على اتساع التعهيد ويلخص هذه العوامل إلى ستة عوامل أساسية.

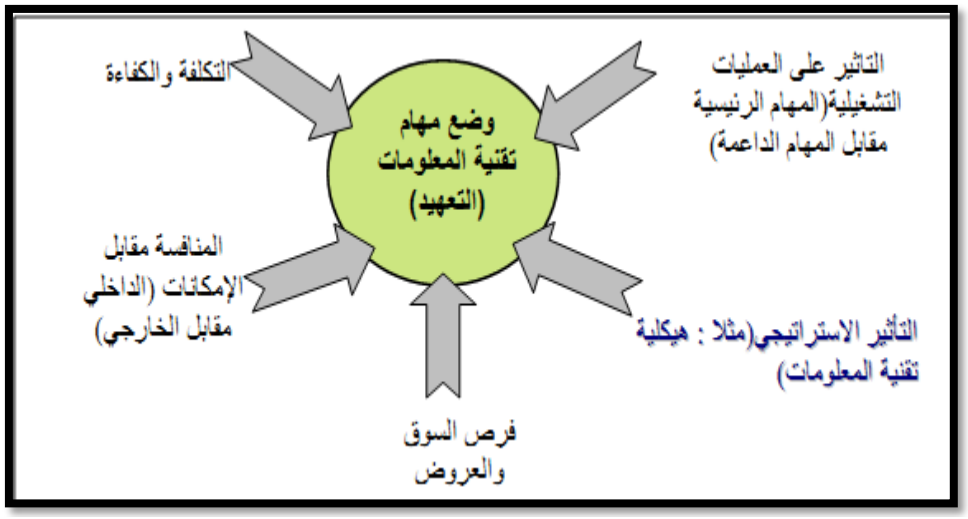
شكل (3-4) يوضح العوامل المساعدة لانتشار التعهيد



المصدر بتصرف: Power and et al.(2006), The Outsourcing Handbook,p7

وتتحدد العوامل الأساسية المؤثرة في استراتيجية التعهيد كما في الشكل التالي:

شكل (3-5):العوامل الاساسية المؤثرة في استراتيجية التعهيد



المصدر (يسر، 2007،ص54)

المبحث الثالث

أمن نظم المعلومات

مقدمة :

تشكل المعلومات للمنظمات البنية التحتية التي تمكنها من أداء مهامها، إذ أن نوع المعلومات وكميتها وطريقة عرضها تعتبر الأساس في نجاح عملية صنع القرارات داخل المنظمات المعاصرة وعليه فإن للمعلومات قيمة عالية تستوجب وضع الضوابط اللازمة لاستخدامها وتداولها ووضع السبل الكفيلة بحيازتها، لذا فإن المشكلة التي يجب أخذها بالحسبان هو توفير الحماية اللازمة للمعلومات وإبعادها عن الاستخدام غير المشروع لها.

وسيتناول الباحث في هذا المبحث الحديث حول تعريف الأمن، مفهوم أمن نظم المعلومات، مكونات ومحاور أمن نظم المعلومات، الغرض من تحقيق الأمن، تصميم النظام الأمني، والعائد على الاستثمار في أمن نظم المعلومات.

الأمن:

الأمن في اللغة نقيض الخوف يقول سبحانه وتعالى في سورة قريش آية (4) : ((الذي أطعمهم من جوع وأمنهم من خوف))، والأمن في الإسلام لا يقتصر على النواحي المادية وإنما يتجاوزها فيشمل الأمن على الدين والنفس والعقل والعرض والمال. وبحسب سلم أولويات الحاجات الضرورية لدى علماء النفس والاجتماع أمثال ماسلو يقع الأمن في المرتبة الثانية ويشمل الأمن الشخصي، والأمن الوظيفي، والأمن الاقتصادي، والأمن الاجتماعي، والأمن العسكري، ويتسع مفهوم الأمن ليشمل الأمن المعلوماتي كأحد أهم المجالات الأمنية التي يتطلبها الفرد والمجتمع في العصر الحديث.

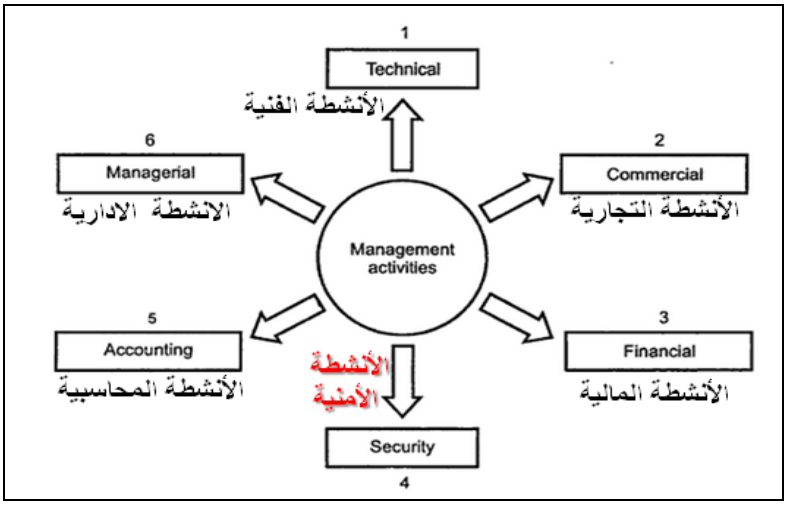
الأمن أحد أنشطة المؤسسة :

أورد هنري فايول[2] في كتابه الإدارة العامة والصناعية الصادر عام 1916م، ستة أنشطة هامة من مهام ومسؤوليات الإدارة وذكر من ضمنها الأمن (Security)، والذي عرفه بأنه حماية الأفراد والممتلكات بما فيها من أصول ومعلومات وتقارير خاصة بالمؤسسة .

[2] نقلاً عن : (Bagad,2008b,p10)

ويوضح الشكل رقم(3-6) مجموعة الأنشطة الإدارية التي تمارسها إدارة المؤسسة ومن ضمنها الأمن من وجهة نظر فايول.

شكل رقم (3-6): يوضح الأمن كأحد الأنشطة الادارية



المصدر : (Bagad,2008b,p10)

وأكد Dickie (1996) بأن أمن نظم المعلومات هي مسئولية إدارية، وتعتبر واحدة من نظم التحكم الداخلية بما تقوم به من رقابة وتدقيق للأعمال المتعلقة بنظم المعلومات، وبذلك فهو يرى أن تحقيق الأمن مسألة تتعدى تطبيق الضوابط والإجراءات التقنية.

مراحل تطور مفهوم أمن المعلومات :

خطى مفهوم أمن المعلومات بمراحل تطور متلاحقة، ففي الستينات كانت أجهزة الحاسوب وعملها هي شغل العاملين في أقسام المعلومات، وكان همهم هو كيفية تنفيذ البرامج والأنشطة المحوسبة ولم يكونوا مشغولين بأمن المعلومات بقدر انشغالهم بعمل الأجهزة وكان مفهوم الأمن يدور حول تحديد الوصول أو الإطلاع على البيانات من خلال منع كل غريب من التلاعب في الأجهزة لذلك ظهر مصطلح أمن الحاسوب Computer Security والذي يعني حماية الحواسيب وقواعد البيانات (Saussure, 1966) و(Pierce ,1958) ، ونتيجة للتوسع في استخدام أجهزة الحاسوب وما تؤديه من منافع تتعلق باتساع أحجام معالجة البيانات، تغير الاهتمام ليمثل السيطرة على البيانات وحمايتها وفي السبعينات تم الانتقال إلى مفهوم أمن البيانات (DataSecurity) ورافق ذلك استخدام كلمات السر البسيطة للسيطرة على الوصول للبيانات إضافة إلى وضع إجراءات الحماية لمواقع الحواسيب من الكوارث واعتماد خطط لتخزين نسخ إضافية من البيانات والبرمجيات بعيدا عن موقع الحاسوب، وفي مرحلة الثمانينات والتسعينات ازدادت أهمية استخدام البيانات، وساهمت التطورات في مجال تكنولوجيا المعلومات بالسماح لأكثر من مستخدم للمشاركة في قواعد البيانات، كل هذا أدى إلى الانتقال من مفهوم أمن البيانات إلى أمن المعلومات، وأصبح من

الضروري المحافظة على المعلومات وتكاملها وتوفرها ودرجة موثوقيتها، حيث أن الإجراءات الأمنية المناسبة يمكن أن تساهم في ضمان النتائج المرجوة وتقلص اختراق نظم المعلومات و التلاعب بها .

تعريف أمن المعلومات:

عرفه السالمي (2000،ص294) بأنه مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال، وذكر كل من Whitman& (2011) Mattord في كتابهما المعنون "مبادئ أمن المعلومات" بأنه " الحفاظ على سرية وتوفر وسلامة المعلومات كأصل، في مراحل المعالجة والحفظ والنقل، ويتحقق ذلك عبر التطبيق الفعلي للسياسات الأمنية ومن خلال تعزيز الوعي والتعلم والتدريب "

ويرى كلاهما أن أي مؤسسة تهدف لتحقيق إدارة لأمن نظم المعلومات فإنه يجب أن يشمل المكونات التالية :

- الأمن المادي : بما يشمله من مصادر وممتلكات ومباني لمنع الوصول غير المشروع
- أمن الأفراد : لحماية الأفراد والمجموعات الذين لهم حق الوصول للمعلومات
- أمن العمليات: لحماية الأنشطة والعمليات التي يقوم بها المخولون
- أمن الاتصالات :لحماية الوسائط والتكنولوجيا المستخدمة والمحتوى
- أمن الشبكات : لحماية مكونات الشبكة والتراسل والمحتويات
- أمن البيانات : لحماية سرية وسلامة وتوافر المعلومات .

أما المشهداني (2001) فقد عرفه بأنه الحفاظ على المعلومات المتواجدة في أي نظام معلوماتي من مخاطر الضياع والتلف أو من مخاطر الاستخدام غير الصحيح سواء المتعمد أو العفوي أو من مخاطر الكوارث الطبيعية، وجاء في تعريف المنظمة الامريكية للتكنولوجيا والمقاييس(CNCS,1994) أن المصطلح يعني:

"حماية المعلومات والعناصر التي تساهم في ذلك كالمكونات المادية المستخدم في معالجة وتخزين ونقل المعلومات "، وذكر مجمع اللغة العربية في معجم الحاسبات تعريفاً لأمن المعلومات بانها : " حماية المعلومات من الكشف أو الاستنساخ أو التدمير من قبل اشخاص غير مصرح لهم سواء كان عرضاً أو عمداً (معجم الحاسبات،1995).

ويرى غيطاس(2007) إن أمن المعلومات هو تلك الرؤى والسياسات والإجراءات التى تصمم وتنفذ على مستويات مختلفة، فردية ومؤسسية ومجتمعية، وتستهدف تحقيق عناصر الحماية

والصيانة المختلفة التي تضمن أن تتحقق للمعلومات السرية أو الموثوقية، والسلامة والتوافر حين الحاجة.

ومن الواضح أن التعريفات جميعها اتفقت على أن أمن المعلومات لابد وأن يشمل في جملة الغرض منه تحقيق (السرية، والسلامة، التوفر) وهو ما يسمى بالثالوث أو المثلث ويختصر بالانجليزية CIA اختصاراً للمصطلحات (Confidentiality ,Availability ,Integrity) .

ويلاحظ ان التعريفات السابقة تحتوي الخصائص التالية:

- اجراءات الأمن ادارية وفنية
- تهدف للمحافظة على مكونات نظام المعلومات المادية
- كما وتهدف للحفاظ على المكونات(غير المادية) البرمجية والكادر البشري
- تتسم بوجود شرعية على حدود وصلاحيات استخدام المعلومات والأجهزة
- ينطوي الأمن على الحماية ضد الاختراقات والتجسس والملوثات والسرقة والتبديل والتلف المتعمد أو غير المتعمد أو الاطلاع بغير تخويل .

وبذلك يمكن للباحث أن يضع تعريفاً لأمن المعلومات بأنه: مجموعة الاجراءات المستخدمة لتوفير سلامة وسرية وتوفر المعلومات حين طلبها وفق صلاحية دخول لنظام المعلومات معروفة مسبقاً وموافقاً عليها.

أمن نظم المعلومات:

وقد يتساءل البعض ما بال الباحث قد اختار مفهوم أمن نظم المعلومات ولم يختر أمن المعلومات، الإجابة هنا تكمن في أن الباحث قد رأى بعد بحثه الموسع، أننا من الجانب الاداري لدراسة المشكلة بحاجة إلى تفصيل المشكلة في جوانبها المختلفة وبمنظور أوسع، بمعنى أننا أمام حالة تتجاوز الهدف من الأمن ألا وهو حماية المعلومات، لتشمل حماية الأوعية والموارد التي تحقق وتعزز هذه الحماية .

وقد عرفه المكتب الوطني الاسترالي للتدقيق (Australian National Audit Office, 2006) بأنه حماية أنظمة المعلومات بما تشمله من البنى التحتية التي تسهل استخداماتها كالتقنيات والعمليات والخدمات والمعلومات .

وعليه يعرف الباحث أمن نظم المعلومات بأنها: العمليات والتدابير والتوجيهات التي تصدرها إدارة المؤسسة بهدف حماية مواردها التقنية وما تحتويه من معلومات في مختلف أشكالها بغرض تحقيق سلامتها وتوافرها وسريتها وفق الصلاحيات والترتيبات المتعارف عليها .

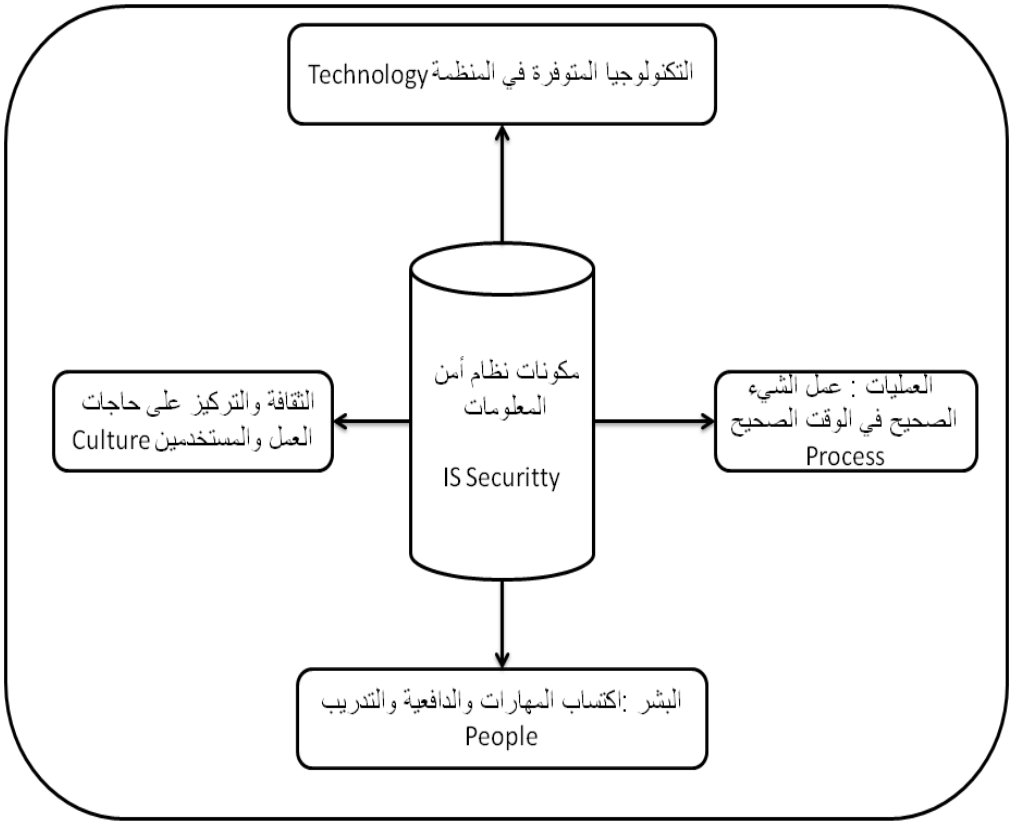
وبذلك فإنه يوجد فرقاً جوهريا بين أمن المعلومات وأمن نظم المعلومات حيث يركز المفهوم الأول على تعريف الأمن من منظور حماية للمعلومات دون ذكر لنظام المعلومات بما يشمله من تقنيات واستراتيجيات لإدارة هذه النظم .

مكونات ومحاور أمن نظم المعلومات:

ويرى الهادي (2006) ان بيئة نظام أمن نظم المعلومات تتكون من أربع مكونات أساسية وهي:

1. التكنولوجيا
2. العمليات
3. البشر
4. الثقافة

شكل رقم (3-7) مكونات نظام أمن المعلومات



المصدر :حسب الهادي(2006)

الغرض العام من تحقيق أمن نظم المعلومات :

أشار Whitson (2003,p.57) أن المنظمات إذ تسعى لتحقيق أمن نظم المعلومات فإن غايتها تحقيق الثالوث المسمى (CIA Triangle) ويعني السرية والخصوصية Confidentiality، التكاملية والسلامة Integrity، والتوفر والإتاحة Availability.

ويرى الباحث ان هذه الغايات المرجو تحقيقها، إنما هي الصفات التي يجب توافرها في المعلومات كصفات تؤهلها لتصبح ذات قيمة .

وعند ذكر كلمة أمن المعلومات فإن أول ما يتبادر إلى الذهن غالباً هو كشف معلومات كان يجب أن تبقى سراً، والحقيقة أن الحفاظ على سرية المعلومات لا يعدو أن يكون جانبا واحداً من جوانب الأمن، أما المتخصصون فيرون لأمن نظم المعلومات مكونات ثلاثة على درجة واحدة من الأهمية (الغثبروالقحطاني،2009).

وتعتبر هذه العناصر أو المكونات بمثابة مبادئ أساسية لابد من تواجدها وهي:

- **السرية**:

حيث أن النظام الآمن هو النظام الذي يضمن سرية وخصوصية البيانات المخزنة فيه، وبالتالي إتاحة هذه البيانات فقط لأصحابها، إضافة إلى تأمين الطرق المناسبة لحمايتها من القراءة أثناء نقلها عبر شبكة الاتصال ويحقق ذلك من خلال مجموعة من الطرق تقدم مستويات مختلفة من درجات الأمان وسرعة نقل المعلومات .

- **التكاملية والسلامة:**

تعني سلامة المعلومات بصفة عامة حيث يؤمن النظام الأمن تكاملية البيانات المخزنة فيه، ويقصد بالتكاملية حماية البيانات من عمليات الحذف والتخريب، ويتم تأمين ذلك من خلال مجموعة من الأساليب توفرها نظم قواعد البيانات كقوائم الولوج والصلاحيات بالإضافة إلى علاقات الترابط ما بين البيانات المخزنة فيها.

ويتكون عنصر سلامة المعلومة من شقين :الاول سلامة المعلومة ويعني عدم تغيير المعلومات بشكل غير ملائم سواء عن عمد أو بغير بقصد، والثاني سلامة المصدر وتعني الحصول على المعلومة من مصدرها الأصلي(أبو مغايض،2004،ص271).

- **التوفر و الاتاحة :**

يؤمن النظام الآمن استمرارية وصول المستخدمين إلى المعلومات الخاصة بهم دون أي تأخير، ولهذه الخاصية عدد من الخصائص المتمثلة في:

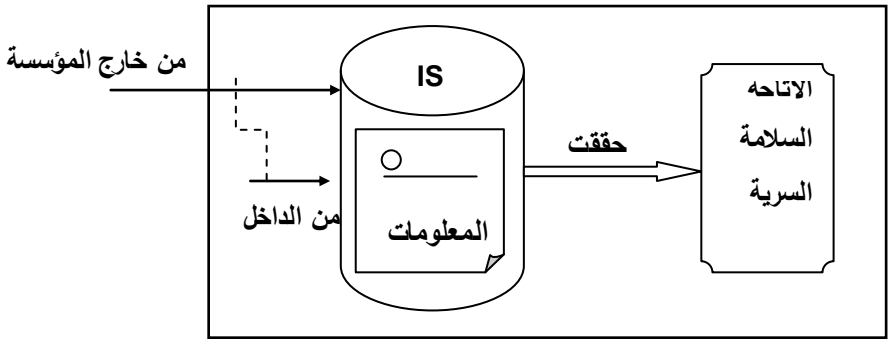
- المقاومة وهي قدرة النظام على الحفاظ على نفسه من العمليات التي تجعله غير متاح للمستخدمين المخولين باستخدامه، (على سبيل المثال أن يكون النظام قادرا على منع تنفيذ استعلامات تتطلب حجز حيز كبير من ذاكرة الخادم) .
- وسهولة الاستخدام.
- المرونة والمتمثلة في توفر الإمكانيات والأدوات التي تمكن من إدارة النظام دون أن يستدعي ذلك إلى توقفه.

– المقدرة على التوسع لسد الحاجات المستقبلية (جامعة الدول العربية،2012،ص6).

ويمكن القول أن الأبعاد الأساسية الثلاثة لإدارة أمن المعلومات (السرية، والسلامة، والتوفر) لابد من توفرها في كل النظم، ولكن قد يغلب أحدها على الآخر حسب طبيعة المعلومات والمنظمة والظروف المحيطة بها، والأهم من ذلك كله التوازن بين المنع و الاستخدام ومن المعروف أن اتخاذ قرار المنع الكلي سهل جداً ولكنه غير مناسب وغير مفيد(القاسم،2007).

وبذلك يقترح الباحث الشكل التالي لإجمال الأغراض العامة من جراء استخدام أمن نظم المعلومات

شكل رقم (3-8) : يوضح أهداف تحقيق أمن المعلومات



لماذا يجرى إدارة لأمن المعلومات :

قد لا يختلف اثنان حول أهمية أن تكون عمليات أمن المعلومات، موكلة لأشخاص محترفين ومتمكنين وتتوفر لهم قسط كافٍ من التدريب والتعليم و الإمكانات التعليمية المستمرة لمتابعة الجديد والمتغير في هذا الحقل .

ويرى خبراء أمن المعلومات في المؤسسة الوطنية للمقاييس والتكنولوجيا (NIST,2006) أن:

- أمن المعلومات هي جزء أساسي من عمليات الإدارة الناجحة
- أمن المعلومات يجب أن تحقق رؤية وأهداف المؤسسة .
- أمن المعلومات يجب أن تنفذ برؤية اقتصادية فعالة
- دراسة أنظمة أمن المعلومات شاملة ومتكاملة.
- مسئولية المعنيين بأنظمة المعلومات هي داخل وخارج المؤسسة
- تحقيق أمن المعلومات يتطلب دراسة واعية لإدارة المخاطر .
- أمن المعلومات يتأثر بالعوامل الاجتماعية .
- تتطلب برامج أمن نظم المعلومات إعادة تقييم دورية .

ويعتبر أمن المعلومات أحدى العناصر التي تقاس بناءاً عليها نجاحات نظم المعلومات، أي أنه أصبح أحد الركائز الهامة في تقييم جودة نظم المعلومات (Al-adaileh,2009,P.232)

وتنجم المشكلات الأمنية في نظم المعلومات المنقولة عبر الانترنت بسبب :

- عدم التواجد الفعلي، حيث أن التواجد افتراضي
- سهولة النسخ والتعديل للمعلومات
- إحداث أنشطة آلية تعمل عبر برامج وبعضها يضر بالنظم
- إمكانية الدخول للمعلومات من أي جهة كانت وفي أي وقت وهو ما يسمى (شيوع التواجد). (داوود،2004،ص 42-44)

وبالرغم من أن هناك فوائد عديدة لا يمكن إنكارها أو عدم استخدامها لشبكة الانترنت إلا أنها باتت سلاح ذو حدين، حيث قام البعض باستخدامها بصورة سلبية، كالسرقة والغش والانتحال، مما ترتب عليه بروز ظاهرة جديدة يطلق عليها الجرائم المعلوماتية أو القرصنة الالكترونية، حيث طوعها بعض المجرمين لأغراضهم السيئة مستفيدين من إتاحة المعلومات، وعدم وجود ضوابط صارمة تكبح جماح الظاهرة (Harms,2006).

تصميم نظام الأمن :

من منطلق أن الإخلال بالأمن قد يكون مدبراً أو قد يكون حادثة غير مدبرة، فعلى سبيل المثال الحريق كأحدى الحوادث الممكنة يمكن أن يحدث نتيجة ماس كهربائي فهو بالتالي حادثة غير متعمدة، أو أن ينتج بسبب أشخاص يتعمدون التخريب.

وعليه يتبين أن تصميم نظام الأمن من الموضوعات المعقدة، ومروراً بالكثير من الاجتهادات التي وضعت تصاميم وخطوات واعتبارات عدة، نجد طلبة وآخرون (1997،ص226-227) قد حدد خطوات أو مراحل أسياسية لهذا التصميم تتخلص في الآتي:

أ. الوقاية : وتعتبر من أمثل المفاهيم النظرية ولكن يصعب تنفيذها وذلك لكثرة تكاليف الإحتياطات الخاصة بها ولكنها رغم ذلك تعبر أهم مراحل تصميم نظام الأمن.

ب. الكشف: وهو يوجد عادة من الوقاية في نظام الأمن، فمثلاً قد يوفر النظام الوقاية ضد الدخول غير المسموح به كما يسجل محاولات الدخول الفاشلة لكشف نوع النشاطات التخريبية وكذلك الأشخاص القائمين بهذه النشاطات.

ج. الردع: يحب توفير الردع المناسب للنشاطات التخريبية لأن ذلك يؤدي إلى خوف المخربين من إكتشاف أمرهم ومحاسبتهم.

د. إستعادة الأجزاء المفقودة: يجب اتخاذ الإجراءات اللازمة لسرعة إستعادة الأجزاء المفقودة من النظام، وذلك باستخدام النسخ الاحتياطي.

هـ. الإبطال وإعادة الإنتاج: عندما تفشل جميع إجراءات الأمن في التغلب على تهديد معين فإن الوسيلة الوحيدة الباقية هي إعادة تصميم النظام مرة أخرى مع اتخاذ الإجراءات الأمنية الجديدة التي تعمل على منع مثل هذا التهديد.

العائد على الاستثمار في أمن نظم المعلومات:

أشارت دراسات عدة بالجدوى والأهمية الاقتصادية لتطبيق أمن نظم المعلومات في المؤسسات على اختلافها، فأهميتها لا تقتصر على المؤسسات التي تبتغي السرية ومزيد من الخصوصيات فقط، بل وتشمل المؤسسات الأخرى التي ربما يكون هدفها تمكين نظم المعلومات من القيام بواجباتها في تحقيق سلامة واتاحة المعلومات للمستفيدين في الوقت والمكان المناسب، ومن الناحية التنفيذية توجد بدائل لتطبيق أمن نظم المعلومات وبالتالي فإن القرار هنا رهين بحالة علمية مدروسة، يجب أن تكون قادرة على إبراز قرار سليم، ولربما أن استخدام العائد على الاستثمار في أمن نظم المعلومات ROSI يعتبر أحد أهم هذه الأدوات .

ويعرف Sonnenreich et al.(2005) العائد على الاستثمار في الأمن ROSI بأنه المنافع التي تحققها المؤسسة نتيجة للانفاق على الأفعال المتعلقة بأمن نظم المعلومات، بمعنى أي من الخيارات سوف يمنح المؤسسة القيمة الأفضل مقابل ما سأدفعه من مال.

ويستخدم العائد على الاستثمار ROSI للمقارنة بين بدائل استراتيجيات الإستثمار الأمني، ولضبط حجم الاستثمار عند المستوى المطلوب .

وبهدف تعظيم منافع الاستثمار في الأمن فإن الطريقة المتكاملة في التعاطي مع تطبيق أمن المعلومات والتي تأخذ التكاليف بعين الاعتبار تمتد لتشمل الأفراد والعمليات والتكنلوجيا في كل مناحي عمل المؤسسة ،وعليه فإن الاستثمار في الأمن يتصدر تصميم نظم المعلومات وإعادة هندسة العمليات وتحتاج المؤسسات لنشر ثقافة التعاون وقبول التغيير .

احتساب العائد على الاستثمار في أمن نظم المعلومات:

أ- لإيجاد ROSI فإننا سنستخدم معادلة العائد على الاستثمار في صورتها العادية ROI .

المعادلة العامة للعائد على الاستثمار :

$$ROI = \frac{\text{Expected Returns - Cost of Investment}}{\text{Cost of Investment}}$$

معادلة(1)العائد على الاستثمار = $\frac{\text{العائد المتوقع – تكلفة الاستثمار}}{\text{تكلفة الاستثمار}}$ **(Rico,2004)**

فلو افترضنا أن العائد المتوقع سيكون حاصل ضرب المخاطر التي ستتعرض لها المؤسسة × نسبة ما تم معالجته من هذه الاخطار، وتكلفة الاستثمار هي تكلفة الحل الأمني الذي تم/سيتم استخدامه فإن المعادلة الجديدة ستكون على النحو التالي:

ب-المعادلة المخصصة لاحتساب العائد على الاستثمار في أمن نظم المعلومات

$$ROSI = \frac{(\text{Risk Exposure} \bullet \%\,\text{Risk Mitigated}) - \text{Solution Cost}}{\text{Solution Cost}}$$

معادلة(2) لـــــ Sonnenreich et al.(2005,P.46)

$$\text{لاحتساب العائد على الاستثمار في الأمن} = \frac{(\text{نسبة التعرض للخطر} \times \text{نسبة الخطر}) - \text{تكلفة الأمن}}{\text{تكلفة الأمن}}$$

متطلبات تحقيق بيئة معلوماتية آمنة :

لكي نصل إلى تحقيق بيئة معلوماتية أمنة يلزم تحقيق عناصر الأمن التالية :

- التحقق من الشخصية (Authentication)
- الترخيص بالاستخدام (Authorization)
- الخصوصية وسرية المعلومات (privacy and confidentiality)
- صحة وسلامة البيانات (Integrity)
- الثقة في المعلومات (Trust)

وتختلف درجة الأمان المطلوبة في نظم المعلومات تبعاً لأهمية المعلومات المطلوب تأمينها، ومدى تعرض هذه المعلومات للخطر، ومدى الضرر الذي يخشى من وقوعه في حالة فقد أي من هذه العناصر (داوود،2004، ص45).

المبحث الرابع

تهديدات أمن نظم المعلومات وإدارة المخاطر

مقدمة:

توجد كثير من التحديات التي تؤثر على الأداء السليم لوظائف نظم المعلومات في ظل التطورات التكنولوجية المتسارعة، والمشكلات الفنية المتزايدة، والأحداث البيئية المتغيرة، والضعف البشري، وعدم ملائمة المؤسسات الاجتماعية والسياسية والاقتصادية الراهنة للمتغيرات المتلاحقة، الخ. ، وتتبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة على السواء التي قد ترد من مصادر داخلية أو خارجية، كما أنها تتراوح من أحداث مفاجئة أو أحداث ثانوية تؤدي إلى عدم تحقيق الغايات الأمنية.

وقد تنشأ أخطاء النظام من سوء استخدام الأجهزة والبرمجيات بما تحدثه من الأخطاء الكامنة، أو التحميل الزائد أو المشكلات التشغيلية وغير ذلك، والعوامل الفنية التي تؤدي لفشل نظم المعلومات عديدة ومتنوعة، كما قد تعتبر غير مفهومة في بعض الأحيان أو تتغير على الدوام و قد تنتج الأعطال من أعطال كبيرة تؤدي إلى توقف العمل أو إبطاء العمل بصفة دائمة أو تقلل قيمة النظام وتفسخ خدماته وفي هذه الحالة يجب مراعاة توقيتات الأعطال والتشويش الذي يتعرض له النظام عند التخطيط لأمن المعلومات من البداية (الشبلي،2009،ص 226).

والصعوبة في صيانة و حماية نظم المعلومات والشبكات قد تستدعي أحياناً الاستعانة بالأطراف الخارجية كالمتعهدين IT-OUTSOURCE، الموردين، البائعين، الخ.، و تتولد مشكلة جوهرية تتعلق بعدم توافر برمجيات تحكم وتراقب الوصول المعتمد الذي يتفق عليه كل الأطراف المعنيين مما ستوجب ضرورة توافر المعايير والتوجيهات الحاكمة لقياسات الأمن(الشبلي،2009،ص 232).

ولكي نقف عند حجم الأثر الذي تتركه حوادث أمن المعلومات لنتخيل ما ورد من أرقام وإحصاءات في تقرير تعده شركة نورتون العالمية(2012) سنوياً لرصد واقع حوادث أمن المعلومات عالمياً ويتضح إن "الفاتورة" الإجمالية لجرائم أمن المعلومات عالميا في 2012 وحده تقدر بحوالي 388 مليار دولار أميركي، أما التكلفة النقدية المباشرة لهذه الجرائم والمتمثلة في الأموال المسروقة ونفقات إزالة آثار الهجمات فتقدر بحوالي 114 مليار دولار، ومعنى ذلك أن القيمة المالية لجرائم المعلومات أكبر من السوق السوداء لمخدرات الماريجوانا والكوكايين والهيروين مجتمعين، وأعلى من الإنفاق السنوي لمنظمة الأمم المتحدة للأمومة والطفولة "اليونيسيف" بحوالى 100 ضعف، وقد بلغ المعدل الزمني لوقوع جرائم المعلومات حول العالم 50 ألف جريمة واعتداء في الساعة، تأثر

بها 589 مليون شخص، وهو رقم أكبر من عدد سكان الولايات المتحدة وكندا وغرب أوروبا مجتمعين، ويعادل 9% من إجمالي سكان العالم[3].

ويفيد التقرير بأن جرائم المعلومات باتت أداة جديدة في الصراع السياسي والاقتصادي حيث تخطى الأمر كل الحدود المعتادة، وصارت جولات صراع مكشوفة بين الدول وبعضها البعض.

إدارة مخاطر أمن نظم المعلومات:

يتوجب على أي منظمة تسعى لتحقيق نظام معلومات آمن وخالي من المشاكل والعقبات التي تحد من توافر الخصائص والمتطلبات الأمنية الرئيسية الثلاثة (التوافر و التكامل و السرية)، أن تجري عمليات إدارة المخاطر بهدف معرفة الوضع التي عليه المنظمة و ما هي نقاط ضعفها، وما هي الثغرات الأمنية، وحصر المهددات الطبيعية والمتعمدة وغير المتعمدة .

وعرف حماد(2008) مفهوم إدارة المخاطر بشكل عام بأنها :"منهج أو مدخل علمي للتعامل مع المخاطر البحتة عن طريق توقع الخسائر العارضة المحتملة وتصميم وتنفيذ إجراءات من شأنها أن تقلل إمكانية حدوث الخسارة أو الأثر المالي للخسائر التي تقع إلى الحد الأدنى ".

ويعرف ابوشنب(2009) الخطر بأنه احتمال أن شيئا ما سيئا سيحدث متسبباً بالأذى لأحد الأصول المعلوماتية أو الخسارة في مكونات نظم المعلومات بشكل عام.

و يعرف أبوشنب (2009،ص8) مخاطر أمن المعلومات بأنها: أثر غير مرغوب به أو ضار بسبب إختراق او خلل بأمن المعلومات ناتج عن تهديد أمني محتمل.

و يعرف إدارة مخاطر أمن المعلومات بأنها عملية قياس و تقييم للمخاطر الأمنية و تطوير إستراتيجيات لإدارتها، تتضمن هذه الإستراتيجيات نقل المخاطر إلى جهة أخرى لتجنبها، أو تقليل آثارها السلبية، و قبول بعض أو كل تبعاتها .

بينما عرفت NIST (2002) إدارة المخاطر بأنها عملية تتيح للقائمين على تكنولوجيا المعلومات الموازنة بين التكاليف التشغيلية، والاقتصادية لأدوات الحماية وبين المنافع المكتسبة من حماية المنظمة وتحقيق رسالتها .

---

[3] ولكن مقارنة بعدد مستخدمي تقنيات الحاسوب والانترنت، فقد تتجاوز هذه النسبة 36% من سكان العالم الذين يستخدمون التقنية، لأنه عالمياً لا يستخدم التقنية والانترنت الا 25% من سكان العالم، حسب تقديرات الامم المتحدة –اليونسكو، في تقرير النفاذ للانترنت 2007.

ويتفق أبو شنب(2009) وطلبة وآخرون(1997) أن أهداف إدارة المخاطر والتهديدات تتمحور حول أربعة أهداف رئيسية :

1- منع الاستخدام الغير مسموح به من قبل الاشخاص الغير مسموح لهم .
2- منع الإتلاف لملفات ومعلومات مهمة للشركة مما يؤدي لمنع الوصول إليها.
3- منع الكشف عن معلومات غير مصرح بالكشف عنها أو سرقتها من قبل الغير مالكين لها.
4- منع التغيير الغير مرغوب به في معلومات المنظمة أو مصادر المعلومات الخاصة بها.

ويرى طلبة وآخرون (1997،ص313) أن المخرجات التي يتم الحصول عليها من إدارة المخاطر تتمثل في استنباط وسائل جديدة لتعزيز أمن نظم المعلومات من خلال استخدام أجهزة أو معدات جديدة أو برمجيات أو أفراد جديدين.

وتشمل عملية إدارة مخاطر نظم المعلومات الخطوات التالية :

1- تحديد وتقييم موجودات وأصول المنظمة(المادية، والغير مادية كمصادر المعلومات) والتي يمكن أن تكون عرضة للتهديد .
2- تحديد المخاطر التي من الممكن ان تتعرض لها هذه الاصول، وعادة تتعرض الأصول أو الممتلكات الممنوعة من الوصول لضرر أكبر من غيرها من الممتلكات .
3- تحديد مستوى الأثر الذي من الممكن أن تحدثه التهديدات الخاصة بخطر معين .
4- تحليل قابلية تعرض أمن الأنظمة المعلوماتية للخطر وهي نسبية تختلف من منظمة لآخرى بحسب مستوى الحماية الذي توفره المنظمة، وآليات تحديد المخاطر، وخبرات المنظمة السابقة .

وانطلاقاً من عمليات إدارة المخاطر تصدر الجهات المختصة تقريرها الذي يبين توصياتها حول درجة المخاطر، ويجري تصنيف الاجراءات الخاصة بتحليل المخاطر، حيث تتضح العلاقة بين مدى قابلية المنظمة للتعرض للمخاطر و الأثر الناتج عن الخطر ويتضح ذلك من خلال الشكل رقم (3-9)(أبو شنب، 2009،ص10).

شكل (3-9): يوضح العلاقة بين مدى قابلية المنظمة للتعرض للمخاطر والأثر الناتج عن التهديدات .

المصدر : (أبو شنب، 2009،ص10)

ومما تقدم يعرف الباحث إدارة مخاطر نظم المعلومات بأنها مجموعة من الأنشطة المدروسة التي تستهدف تحليل قابلية تعرض أمن الأنظمة المعلوماتية للخطر عبر تحديد وتقييم المخاطر التي من الممكن أن تتعرض لها البنى التحتية لنظم المعلومات و دراسة التهديدات الفعلية التي ستنشأ عن المخاطر وكل أثر يمكن ان تحدثه .

وقد صنف Kaeo (1999) [4] أنواع المخاطر في ثلاث مجموعات عامة هي :

- الاستخدام غير المرخص به .
- انتحال الشخصية .
- عرقلة الخدمة .

تقييم الأثر الناتج عن تهديد أمن نظم المعلومات :

هناك اتجاهان لتقييم الأثر الناتج عن المخاطر المحتملة إحداهما كمي والآخر نوعي .

حيث أنه باستخدام التقييم الكمي يمكن ترجمة الخسائر المتوقعة إلى قيمة مالية، حتى لو كانت الخسارة معنوية، بمعنى أن تكون خسارة يصعب تقديرها بقيمة مالية .

لتقدير قيمة الخسارة المالية المتوقعة تستخدم المعادلة التالية:

الخسارة المالية المتوقعة = قيمة المورد الفعلية أو المقدرة × نسبة تعرض المورد للخطر%

ويجب أن يشمل حساب الخسارة المتوقعة تكلفة الوقت اللازم لإستعادة أو استمرار العمل ومدة توقف المنظمة عن العمل (داوود،2004،ص110).

[4] نقلا عن داوود،2004 – ص 100

أما التقييم النوعي فيستخدم حين نعجز عن تحديد الأثر الناجم عن أحداث يصعب التكهن بمدى أثرها وخسارتها مثل فقدان السمعة أو الإساءة للمركز السياسي للدولة أو التسبب بحرج دبلوماسي.
ويرى أبو شنب (2009،ص10) أن أي تقرير ينتج عن عمليات إدارة مخاطر نظم المعلومات يجب بالضرورة ان يشتمل على :

- وصف الخطر الذي تم دراسته
- مصدر الخطر
- درجة الخطورة (بحيث انه تذكر كنسبة ويستعان بمقياس تدرج)
- أنظمة أو تقنيات الحماية التي تم توظيفها وتطبيقها
- صاحب الجهة المعنية بالخطر.
- ما هي التوصيات بالتعامل مع الخطر في الحالات المماثلة.
- المدة الزمنية التي تتطلبها عملية التعامل معه (سواء بإزالته تماماً، أو بتخفيف أثره).

ويتم التركيز علي المخاطر التي سيكون لها تأثير اقتصادي سلبي علي المؤسسة، ومن المتوقع أن تسبب خسائر متنوعة مثل:

- خسائر تشغيلية : ناتجة عن تأثر مستوي التشغيل المعتاد لمنظومة العمل واستمرارية تقديم الخدمات التجارية بسبب أعمال التخريب، أو إصابة نظم المعلومات بالمؤسسة بفيروسات الكمبيوتر أو توقف الخدمة المقدمة للعملاء.
- خسائر قانونية : نتيجة العقوبات المالية المنصوص عليها في عقود قانونية نتيجة إفشاء المعلومات لأفراد أوجهات أو منافسين لم يكن من المفترض حصولهم عليها.
- خسائر مالية : خسائر في الإيرادات بسبب الإخلال باتفاقيات وفقدان السرية، والنزاهة، والخصوصية، أو إتاحة المعلومات لأفراد أو جهات لم يكن من المسموح لهم الإطلاع عليها .
- خسائر استراتيجية : ناتجة من تأثر الإيرادات المستقبلية وفقدان العملاء أو الإخلال بحقوق الملكية الفكرية
- تأثر سمعة المؤسسة : نتيجة لفقد ثقة العملاء والجمهور في المؤسسة (عبيد،2009)

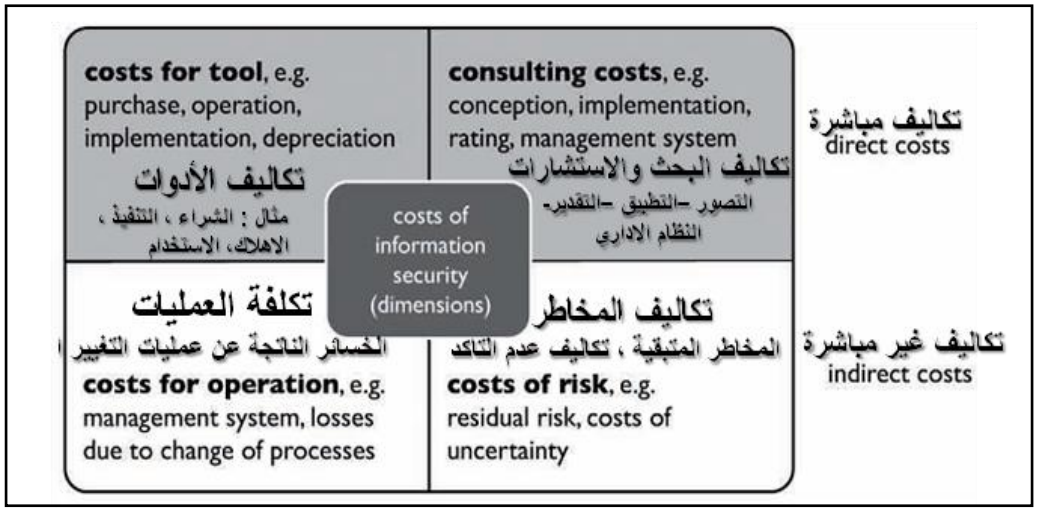
ويتطلب أمن نظم المعلومات من النظرة الاقتصادية إحداث موازنة بين تكاليف عمليات أمن نظم المعلومات وبين الخسائر التي من الممكن أن تنتج عن السرقة أو التخريب أو حرمان الخدمة أو كل ما من شأنه العبث بأهداف تحقيق البيئة الآمنة لنظم المعلومات (Pipkin,2000,P.13).

ويرى الباحث أن عمليات تحليل المخاطر يجب ان تقاس بمعايير التكلفة والعائد Cost/Benefits Analysis حيث يجب إجراء عمليات المقارنة بين التهديدات المتوقعة وما سوف تكلفه مقابل ما يمكن أن توازيه من تكلفه على صعيد الاجراءات الأمنية المضادة والتي تمثل حلولاً، ولكن أحيانا تحتاج المنظمة إلى توفير المضادات الأمنية تحت سقف أي تكلفة، وهذا ما يتفق جزئياً مع ما طرحه (Panko,2004,p.37)

ويضيف الباحث أنه تجدر الإشارة إلى أنه ليس من الممكن تحديد جميع المخاطر، كما انه ليس من الممكن القضاء على كل الأخطار وما تبقى من مخاطر يسمى المخاطر المتبقية.

ويرى Humpert and et al. (2004) أن تكاليف أمن نظم المعلومات تقع في أربعة أبعاد هي تكاليف التطوير التي تشمل البحث والاستشارات وتكاليف الأدوات المستخدمة التي تتطلبها حماية نظم المعلومات وتعتبر تكاليف مباشرة، وأما التكاليف الغير مباشرة فتشمل تكلفة المخاطر بما فيها من حالات عدم التأكد والمخاطر المتبقية والبعد الرابع هو تكلفة العمليات ويشمل الخسائر غير المباشرة الناتجة عن عمليات التغيير .

شكل رقم (3-10) يوضح أبعاد تكاليف نظم المعلومات كتكاليف مباشرة وغير مباشرة



المصدر : (http://www.kes.info/archiv/online/kostencontrolling.html)

ويرى ابو شنب (2009،ص7) أن الخطر يقع عندما يتمكن تهديد ما من استغلال إحدى الثغرات الأمنية، ويعرف نفسه الثغرة الأمنية (Vulnerability) بأنها : نقاط الضعف في النظام مثل عدم وجود برنامج مضاد للفيروسات، أو عدم وجود حراسة أمنية للمبنى، أو عدم وجود إجراءات لإنهاء خدمات موظف.

تهديدات أمن نظم المعلومات :

يعرف أبو شنب (2009،ص7) تهديدات نظم المعلومات على أنها الأشخاص والمؤسسات والآليات والأحداث التي يمكن أن تحمل تأثيراً سلبياً ومضراً على مصادر المعلومات،في حين يرى (Rittinghouse and Ransome,2005,p23) بأن التهديد هو أي نوع من أنواع التهديدات الطبيعية (كالزلازل والفيضانات وارتفاع درجات الحرارة) أو التهديدات من صنع الإنسان (كالأخطاء البشرية والتجسس الإنساني والصناعي)

ويعرفها الباحث بأنها كل انتهاك أو خرق لنظام المعلومات، و هو ما يعرض المعلومات للفقد، أو المنع، أو التعديل.

مصادر التهديدات :

المهددات تتدرج من المخاطر التقليدية كأي مال منقول، إلى مخاطر خاصة بطبيعة عمل جهاز الحاسوب كأحد مكونات نظام المعلومات ووظائفه، وتنتهي بأن يكون هذا الجهاز مصدر تهديد للآخرين. كما علينا أن ندرك أيضاً أننا كل يوم أمام جديد من التقنيات والبرمجيات والبروتوكولات التي قد تستغل في أعمال غير مشروعة، وعليه فان تصنيف وتحديد المخاطر يتباين بحسب النظرية والمعايير المختلفة ولكنها لاتختلف في جملتها عن بعضها(عرب،2002،ص87)

فمثلاً صنف الحميد ونينو (2007،ص38-40) مصادر التهديدات إلى داخلية وخارجية :

أ- التهديدات من الداخل :

- وهي التهديدات التي تنشأ من داخل المنظمة من خلال العاملين في المنظمة الذين يضطلعون على أنشطتها ويعملون كجزء من أنظمة معلوماتها، ويقومون باستخدامها في تحقيق مصالح معينة، فإذا عرف أحد الموظفين غير المخولين كلمة المرور الخاصة بأحد أنظمة المعلومات ثم قام بالدخول إلى النظام، تتعرض المنظمة للتهديد حتى لو لم يقم باستخدام كلمة المرور للدخول لحظة معرفته للكلمة، أما إذا استخدمها فإن الخطر يكون قد وقع .
- تسريب المعلومات عن طريق مستخدمو النظام ومن لهم الحق في الولوج للنظام عن قصد أو غير قصد.

ب-التهديدات من الخارج :

وهي التهديدات من خارج المنظمة، وتكمن الخطورة فيها بعدم أو صعوبة معرفة المخترق، وأهدافه من وراء الاختراق، ومدى اختراق النظام، وتتمثل أهم التهديدات فيما يلي :

- تهديدات البرمجيات : وتشمل حذف البرنامج، أو سرقته، أو تشويهه بسبب تعطيل الاجهزة، أو إصابتها بالفيروسات.
- تهديدات الاجهزة : وتشمل سرقة الاجهزة، أو العبث فيها أو تدميرها أو تعريضها للتلف من خلال الحريق او فيضانات المياه أو الطاقة الكهربائية .
- تهديدات المعلومات : وتشمل حذف المعلومات أو المسح، أو التشويه الناتج عن مشاكل الأجهزة والبرامج، وأخيراً السرقة.

وقد ذكر الشبلي(2009،ص:30-32) أن الاعتقاد السائد أن الجزء الأعظم من تهديدات نظم المعلومات يأتي غالبا من المصادر الخارجية، ولكن على النقيض من ذلك فإن الأشخاص الذين منحوا حق الوصول المعتمد للنظام قد يكونون أكثر فتكاً بنظم المعلومات أيضاً، فعلى الرغم من أنهم قد يكونوا مؤتمنين أو عاملين من ذوي النوايا الحسنة فإنهم ربما بفعل التعب أو الإرهاق أو التدريب غير الملائم قد يقترفون أفعالا غير متعمدة قد تسهم في حذف كميات كبيرة من البيانات الهامة للمنظمة التي يعملون بها، وفي حالة كون الأشخاص غير مؤتمنين فإنهم يسيئون استخدام نظم المعلومات من خلال العبث والتلاعب في النظام بطرق متعمدة بغية الاستغلال أو الثراء الذاتي للإضرار بالمنظمة التي يعملون بها.

تهديد نقص التدريب والتوعية:

إن نقص التدريب والتوعية الملائمة في أمن المعلومات وأهميته تسهم في الجهل باستخدام نظم المعلومات المناسبة، وبدون تنظيم دورات تدريبية ملائمة قد يجهل كثير من العاملين والمستخدمين بأغراض الأضرار النابعة من سوء استخدام نظم المعلومات، كما قد لا يستخدمون أي مقاييس أمن حتى البدائية منها، مما قد يؤدي إلى ممارسات وأفعال تعود بالإساءة لأمن نظم المعلومات.

وقد يؤدي التنوع الكبير لمستخدمي نظام المعلومات والمتعاملين معه (العاملون، المستشارون، العملاء، المنافسون والجمهور العام) فيما يتعلق بتوعيتهم وتدريبهم واهتماماتهم المختلفة والمتفرقة في ظهور صعوبات خاصة بأمن المعلومات ونظمها(الشبلي،2009،ص228).

ولقد قسم الحمدان والقاسم (2004،ص58) التهديدات التي تؤثر على نظم المعلومات إلى:

أ- التهديدات الطبيعية كالزلال، والأعاصير، والفيضانات، والنيران، وإرتفاع درجات الحرارة، والرطوبة العالية.

ب-التهديدات الناتجة عن أسباب تقنية كانقطاع التيار الكهربائي أو حدوث عطل في أحد مكونات نظم المعلومات كالأعطال الخاصة بتكنولوجيا المعلومات كتوقف خادم عن العمل أو عطل في أحد الحواسيب أو شبكات الاتصال أو البرامج .

ت-التهديدات الناتجة عن أعمال تخريبية بفعل الانسان وتتضمن:

- الافعال المقصودة (المتعمدة)
- الافعال غير المتعمدة .

وأفاد حاج علي(2008،ص2)" في أمن المعلومات الأعمال غير المقصودة يتم التعامل معها بإعتبارها مقصودة لأن كثيراً من الأعمال المقصودة يدعي فاعلوها بأنها غير مقصودة"

ويرى الباحث أنه لا توجد آليات لمعرفة وتحديد ما هي الأفعال والأعمال التخريبية التي نتتجت عن فعل مقصود أو غير مقصود، وبالتالي فأنه لربما يعتبر هذا التصنيف للتهديدات بمثابة طوق نجاة، كمن أراد تبرئة يداه من دم يوسف !!

بينما قسم طلبة وآخرون (1998،ص223) تهديدات أمن نظم المعلومات إلى ثلاث مجموعات كالآتي:

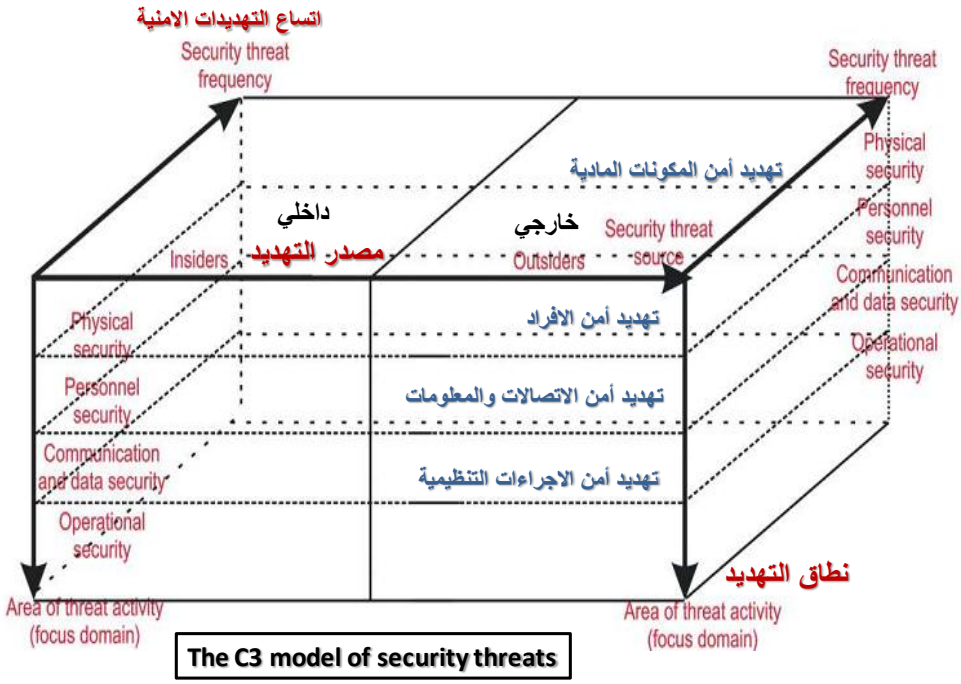
أ- تهديدات تنتج من نظم المعلومات نفسها مثل أخطاء التشغيل

ب-تهديدات تنتج عن أفعال ضارة لبعض المخربين

ج-تهديدات تنتج عن الكوارث الطبيعية والبيئية.

وقد جاء التصنيف الذي وضعاه (Geric and Hutinski,2007,P.59) عام 2007 ليكون التصنيف الأكثر جدلاً، حيث افترضا نظاماً ثلاثي الأبعاد لتصنيف مهددات أمن نظم المعلومات، وكانت هناك ثلاث محاور رئيسية كما يوضحها الشكل التالي رقم (3-11) حيث المحور الأول هو مدى تكرار(إتساع) التهديدات، والمحور الثاني هو مصدر التهديد (داخلي، خارجي)، والمحور الثالث هو نطاق التهديد أي الجهة(مكون نظم المعلومات) التي تتعرض لهذا التهديد.

شكل رقم (3-11) يوضح النموذج ثلاثي الابعاد لتصنيف تهديدات نظم المعلومات



Gerić Sandro, Hutinski Željko (2007)"Journal of Information and Organizational Sciences "

من خلال ما تقدم، يضع الباحث تقسيماً لتهديدات وانتهاكات أمن نظم المعلومات كالتالي:

- التهديدات الداخلية .
- التهديدات الخارجية وبدورها تنقسم إلى :
  - تهديدات البنية التحتية لنظم المعلومات .
  - تهديدات الأفراد .
  - تهديدات الطبيعة وما تحدثه الكوارث الطبيعية كالزلازل أو الفيضانات أو ظروف البرد القارس، أو موجات الحرارة الشديدة .
  - تهديدات الاحتلال الصهيوني (بالقصف و التدمير الشامل – الحصار)[5] .

وبعد تقديم التصنيف السابق، سيتناول الباحث فيما يلي دراسة هذه المهددات باستيضاح أكثر.

[5] وهي تهديدات قائمة بالفعل، وتعتبر بمثابة أشد الاخطار التي تواجه أمن نظم المعلومات تدميراً في فلسطين المحتلة وقطاع غزة تحديداً، وقد تعرض النظم للتدمير الشامل، وسبق إن حدث هذا مع جهات مشابهة كما حدث مع الجامعة الإسلامية بغزة في 1-2009.

تهديدات البنية التحتية لنظم المعلومات :

تتعدد طرق وآليات انتهاك البنية التحتية لتكنولوجيا المعلومات، وتهدف هذه الأساليب لمهاجمة نظم المعلومات بحيث ينال المقتحم أو المهاجم من وراء ذلك منافع وفوائد، ومنهم من قد يلجأ للتخريب و التدمير.

وقد يلجأ الطرف المنتهك لاستخدام أسلوب أو أكثر من الأساليب التالية، أو قد يكون أحداهما مقدمة لاستخدام أسلوب آخر .

ومن هذه المهددات التي تهدد أمن نظم المعلومات :

أولاً: الفيروسات :

ظاهرة فيروسات الكمبيوتر ليست جديدة بل تعود إلى نهاية الاربعينات، وقد ورد ذكرها لأول مرة في مقال نشره (جون فون نيونان) سنة 1949، وظهرت بعض عوارض الفيروس في أوائل الخمسينات إلا انها بقيت محدودة، وكان أول انتشار للفيروسات في الأجهزة الشبكية عام 1983، حيث ظهرت مع نظام التشغيل Unix وقد أثارت ضجة في الساحة العلمية والعملية، ولم تسلم كبريات الشركات من هذا الفيروس، ووصلت خسارة الشركات لما لا يقل عن 100 مليون دولار(نزار، 1994) .

وتنتشر الفيروسات اليوم بما يشبه انتشار النار في الهشيم، وقد أصبحت الفيروسات الآن خطراً يهدد الاقتصاد والحكومات والأفراد (Parker,1998;Elliot,2000) وشبه داوود (2004) إنتشار الفيروسات في ظل عهد الانترنت وكأنك منحت الأسماك بحيرة من الماء ترتع فيها وتتكاثر، حيث ستتوافر أكبر عدد من الأجهزة وبأقل فترة زمنية ممكنة .

ولنتدبر مخاطر الفيروسات كمهدد لأمن نظم المعلومات تخيل أنه في مقابلة مع قناة العربية (2010) أبلغ المشرف على كرسي أبحاث أمن المعلومات عن إرسال 540 مليون فيروس حاسوب إلى المملكة العربية السعودية خلال الربع الثاني من عام 2010 من جهات مجهولة، لذلك اعتبرها الكثير من الباحثين أمثال (Parker,1998;Elliot,2000) أنها من أكثر جرائم الحاسوب إمعانا في الشر .

ولم تأت تسمية الفيروس بهذا الاسم عبثاً من قبيل الصدفة، بل إن هنالك ثمة نقاط مشتركة ما بين الفيروس البيولوجي و الفيروس المعلوماتي .

فالفيروس سواء كان معلوماتياً، أو بيولوجياً هو تشويش في نقل المعلومات، ففيما يتعلق بالفيروس البيولوجي فأنه ينقل معلومات الخلايا الوراثية، وهو ما يؤدي إلى نسخ طبعة الأصل من الخلية

(النواة المعلوماتية) المصابة مما يؤدي إلى إصابة الجسم كله، وتتعد أنواع الفيروس في المجالين وفي كلتا الحالتين هناك أنواع متشابهة في الخطورة أو في طريق التكوين، كما أنها تتشابه في طريقة التكاثر (نزار، 1994).

تعريف الفيروس :

يعرف Hyatt (2001) الفيروس بأنه أي برنامج أو مجموعة من التعليمات قد تلحق ضرراً بنظام المعلومات أو ما يحتويه من معلومات، ولديها القدرة على التخفي و التوسع والانتشار .

وترجع عوامل انتشار الفيروسات بحسب Macgraw&Morriset (2000) إلى :

- انتشار الشبكات : حيث تزداد الهجمات في بيئة الانترنت، وربما يحدث ذلك آلياً دون تدخل من البشر .
- زيادة تعقيد الأنظمة : حيث تزداد الثغرات التي من الممكن أن تشكل أداة لتفاقم المشكلة الأمنية.
- سهولة الإضافة إلى النظم : حيث أن الإضافات (Add Plug in) وأدوات التوسعة (Extension systems) وما يطلق عليه (Scripts) تقوم بدور بارز في إنهاك الأنظمة الاصيلة .

البرمجيات الضارة :

ينفرد متخصصو تقنيات المعلومات في التفريق بين الأنواع المختلفة من الفيروسات، حيث لا يميز الكثير من الناس بين الفيروسات وغيرها مما يعرض الحواسيب للخطر كالديدان وأحصنة طروادة، و غيرذلك...

وتجمل كل أنواع الضرر التي تلحق بأنظمة المعلومات تحت عنوان أشمل وهو البرمجيات الضارة Malicious Software حيث تعمل على تقليص اداء موارد النظام .

وقد عرف الألفي وآخرون (2011،ص581) البرامج الضارة بأنها البرامج التي تُضمن أو تُدخل عمداً في نظام ما لغرض ضار وتشمل :

- الفيروسات
- الديدان : وهي برامج حاسوبية مستقلة بذاتها، تجد ضالتها في الانتشار عبر أجهزة الشبكة المحلية .
- أحصنة طروادة (Trojans): وهي برامج تبدو عادية لكنها تحمل في جوانبها الخطر الغير متوقع بما تقدمه من ضرر خفي، وسميت بهذا الأسم نسبه إلى القصة التاريخية الشهيرة لخدعة حصان طروادة الخشبي الشهير في الأدب الإغريقي الذي استخدمه جنود اسبرطة للاختباء في جوفه بعد ان تظاهروا بالانسحاب، وقام اهل طروادة بسحب الحصان إلى

داخل المدينة المنيعة التي استعصت على الهجوم، حتى إذا هدأت المدينة، وبعد أن نام الحراس خرج الجنود المختبئين من الحصان الخشبي، وفتحوا أسوار المدينة، وتدفق جنود الاعداء إلى المدينة واستولوا عليها (بسيوني،2007،ص99).

وبذلك يعرفه الحمامي والعاني (2007،ص22) بأنه عبارة عن برنامج صحيح وقانوني لإجراء عمل مفيد ولكن ضمنه تنفذ شفرات مخفية والتي قد تكون فيروس يسمح بوصول غير مخول للحاسوب بهدف تدمير البيانات والملفات.

ومن أمثلة هذه البرامج الضارة ما يسمى بالقنابل الموقوتة والقنابل المنطقية و باب المصيدة وكلها تهدف لتجاوز نظم الحماية وأمن المعلومات.

- برامج التجسس : وهي برمجيات تقوم بجمع معلومات شخصية بدون معرفة الناس أو بدون إذن منهم، ثم تقوم بإرسال هذه المعلومات إلى طرف ثالث (اشخاص،أو شركات، أو خادمات Servers)، وبطبيعة الحال فإن هذه المعلومات قد تكون حرجة وتسبب الخسائر أو تتعرض لسوء الاستخدام، ومن الامثلة على هذا النوع من البرمجيات الخبيثة برامج الدعاية والبرمجيات المساعدة Adware و برمجيات التلويث Malware، وبرمجيات رخص الاستخدام Eualware . وهي تختلف عن الديدان والفيروسات كونها لا تنسخ نفسها .

وتستغل برمجيات التجسس الثغرات الأمنية لنظم التشغيل و برامج استعراض الانترنت لأغراض تجارية او تخريبية أو بيع المعلومات لمؤسسات إعلانات أو شركات عن طريق سرقة المعلومات الشخصية للمستخدم، ومراقبة نشاطه أثناء تصفح شبكة الويب(بسيوني،2007،ص193-194).

- مسجلات ضربات المفاتيح : وهي برمجيات صغيرة تقوم بتسجيل ضربات المفاتيح التي يقوم بها المستخدم وذلك سعياً لإلتقاط كلمات المرور وتخزينها، ومعلومات خاصة كأرقام بطاقات الائتمان(الألفي وآخرون،2011،ص581)، وبعض هذه البرمجيات له أهداف حميدة ويقوم المستخدم بتثبته من اجل الحماية الأسرية وخاصة في حال استخدام الاطفال للانترنت وخوفاً عليهم من استغلالهم من قبل مواقع ذات أغراض سيئة .(Janzeweski,2008,p.174)

ثانياً :التنصت

عرف داوود(2004،ص 128) التنصت بأنه قيام المهاجم أو المقتحم (hacker) بمراقبة ما يدور بالشبكة، وما يتم تبادله فيها من رسائل، وذلك بهدف الحصول على معلومات يهتم بها الضحية بإبقائها في طي الكتمان.

ويرى king (2003) أن التنصت لا يحدث إلا في حال تم استخدام الشبكات ذات البنية عامة الوصول، وغير المحمية وكوسيلة لمجابهته يتم بناء شبكات خاصة افتراضية أو شبكات تمرير أمن للبيانات.

وسواء أكان الاتصال عبر الانترنت أو عن طريق الشبكة المحلية، فإن البيانات تسلك طريقها عبر أسلاك أرضية أو عن طريق الاتصالات اللاسلكية، بالتالي فإن الشخص المتطفل الراغب في الحصول على هذه المعطيات بإمكانه أن يتنصت على المعطيات المرسلة التي ترسل عبر هذه الوسائط المختلفة ويتمكن من قراءتها وسرقتها(Garfinkel and et al.,2003,p.253).

وهناك نوعان من التنصت (Garfinkel and et al.,2003,pp.253-255) :

- مراقبة الرسائل : وفيه يهدف المتنصت الحصول على معلومات أو التقاط كلمات السر وقد يتم ذلك حديثاً بشكل آلي بمعنى وجود برامج متخصصة في البحث عن هذه الغايات، وتسمى هذه العملية بالانجليزية (Sniffing) وتعني التشمم تشبيهاً بما يفعله الكلب حين يتشمم لفافة ما ليحاول معرفة ما بداخلها .
- إعادة إرسال الرسائل : حيث يتم تخزين البيانات التي تحملها الرسائل أثناء إرسالها عبر الشبكات، ومن تم يعاد تمريرها إلى وجهتها المقصودة أصلاً وهذا النوع من التنصت يمكن كبحه عبر استخدام بروتوكول يمنع إعادة إرسال الحزم.

ثالثاً: التزوير (Fabrication)

ويسمى هذا الانتهاك إقحام المعلومات وتعديلها (Data Injection and Modification)، حيث يقوم مهاجم نظام المعلومات عبر الشبكة بتغيير، أو تعديل البيانات ومن ثم إعادة إرسالها وهو بذلك قد يلجأ لاستخدام أساليب أخرى كالتنصت أو الاقتحام.

ولحل هذه الإشكالية يلجأ خبراء أمن المعلومات إلى المجموع الاختباري (Checksum) وهو عبارة عن رقم يتم احتسابه بناء على مجموعة من البيانات، ويستخدم للتأكد من سلامة البيانات المنقولة، بحيث يقوم الطرف المرسل باحتسابه قبل إرسال البيانات، ويقوم الطرف المستقبل بالشيء نفسه والغرض من ذلك اكتشاف أي تغيير متعمد للبيانات قد قام به الشخص المهاجم (داوود،2004،ص138).

رابعاً: الاقتحام أو التطفل (Intrusion)

يعد ثاني أكبر التهديدات الأمنية خطورة وانتشاراً، والمقتحم (المتطفل) يستطيع بعد اقتحامه نظام المعلومات وتحديداً أجهزة الحاسوب أو توابعه، أن يستخدم هذا الجهاز كيفما يشاء وبكامل صلاحيات المستخدم الشرعي (المصرح له بالولوج للنظام).

ويرى Mcclure (1999,) أن المقتحم إذا نجح في اقتحام النظام فانه يستطيع ارتكاب جميع أنواع الانتهاك الأخرى كالتنصت أو التزوير أو إقحام الرسائل.

ويعرف كلاً من الحمامي و العاني (2007،ص300) التطفل بأنه أي مجموعة فعاليات تحاول التدخل في سلامة وخصوصية وتوفر الموارد، ويذكرا ثلاثة أصناف من المتطفلين :

1. المتنكر (Masquerader) وهو فرد غير مخول باستخدام الحاسوب ويخترق السيطرة بالوصول للنظام للاطلاع على امتيازات المستفيدين القانونين وهو على الدوام من خارج المؤسسة.
2. الفضولي (Misfeasor) هو مستفيد مخول يصل إلى بيانات وملفات وبرامج أو موارد ليس مخول بالوصول إليها، أو هو مخول بالوصول لكنه يسيء الاستخدام من أجل مصلحته الشخصية، وهو بصورة عامة من داخل المؤسسة.
3. المستخدم السري (Clandestine User) وهو مستخدم يسيطر على سيطرات الإشراف للنظام ويستخدمها من أجل تغيير التدقيق و سيطرات الوصول أو للتهرب من مجموعة التدقيق، وهو يمكن أن يكون من خارج النظام أو جزء منه.

وبصورة عامه يطلق على المتطفل مصطلحات مختلفة مثل Hacker هاكر، أو كاسر الخصوصية Cracker وفي كل الأحوال فإن هدف المهاجم السيطرة على النظام .

ويستخدم المتطفل كلمات المرور للوصول إلى غايته في اقتحام النظام ويمكن أن يستخدم عدة طرق للحصول عليها منها :

- الشم (Sniffing) حيث يلجأ المهاجم إلى مقاطعة البيانات المارة عبر الشبكة المحلية والبحث فيها عن كلمات المرور التي ستتيح له اختراق النظم المحلية أو قواعد بيانات على الانترنت.
- تقنية إعادة الإرسال أو التوجيه (Replay Attack) ويتم باستخدام الحزم المشفرة نفسها.
- سرقة كلمات المرور أو التجربة العشوائية للكلمات الافتراضية والسهلة الخاصة بالمستخدمين
- استخدام الملاحظات المباشرة أثناء قيام المستخدمين الفعليين بتسجيل الدخول للنظام.
- **الهندسة الاجتماعية :**

وتعني حصول الدخلاء على تقليد المستخدمين الشرعيين ليتمكنوا من الدخول غير الشرعي إلى نظم المعلومات عبر إتباع طرق اجتماعية في الحصول على المعلومات بطرق إلتوائية كخداع شخص ما لتقديم معلومات قيمة من أجل الوصول للمعلومات، كمثل استغلال الضعف الإنساني أو أخطاء المستخدم في الحصول على كلمات المرور، أو الاتصال الكاذب بمدير النظام تحت اسم شخص مخول له بالدخول،

طالباً منه ضرورة تغيير كلمة المرور او السماح بصلاحية مضافة معينة (البداينة،2002،ص241).

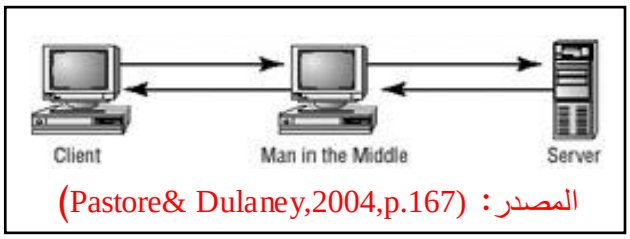
- التفتيش في مخلفات التقنية (Dumpster diving) ويقصد به قيام المهاجم بالبحث في مخلفات المؤسسة من القمامة والمواد المتروكة بحثاً عن أي شيء يساعده على اختراق النظام، كالأوراق المدون عليها كلمات السر، أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة.

خامساً: اعتراض البث (Session Hijacking)

ويقصد به : الاقتحام الذي يكون فيه المهاجم في مكان بين طرفي اتصال (كالخادم Server والمضيف Client) ويسمى هذا النوع من الاقتحام (Man In the Middle) ويشابه اختطاف المواقع.

ويصور الشكل رقم (3-12) بالأسفل عملية اعتراض البث من قبل المهاجم (المتطفل) الذي يكون في وسط عملية الاتصال .

شكل رقم (3-12) يوضح اعتراض البث



المصدر: (Pastore& Dulaney,2004,p.167)

سادساً: عرقلة الخدمة (Denial of Service)

وعرفها داوود(2004،ص148) بأنها منع أجهزة شبكة المعلومات من العمل والتي تؤدي إلى أذى شديد وخسارة كبيرة، وهذا نوع من الهجوم لا يستفيد منه القائم به، ولا يجني من وراءه أي مكسب .

ويضيف أنه يمكن إتمام هذا الانتهاك عن طريق إغراق النظام أو الشبكة بالرسائل أو البرامج أو طلبات المعلومات بحيث يقضي النظام أو الشبكة كل الوقت في محاولة الاستجابة لهذه الرسائل والطلبات دون جدوى ؛ وكثيراً ما يحدث تعاون بين مجموعة من المهاجمين حيث يقومون في توقيت معين بمهاجمة خدمة معينة في وقت معين عن طريق إغراق نظم المعلومات بطلبات مشروعة ومصرح بها ولكنها أكبر من الحجم المسموح.

ويرى الباحث ان هذا النوع من اساليب انتهاك نظم المعلومات إنما يهدف إلى الاخلال بإحدى اهم الاغراض من أمن المعلومات وهو التوفر (Availability) حيث ستمنع نظم المعلومات من القيام بوظائفها في توفير الخدمات للمستخدمين والمستفيدين منها .

المهددات الطبيعية والبيئية والخارجية لنظم المعلومات :

ذكر الزهيري (2008) عدة مهددات، يذكر الباحث ما هو كثير الحدوث في بيئتنا الفلسطينية وخصوصاً في قطاع غزة :

1. الحرارة العالية

الحاسوب الشخصي شأنه شأن الأجهزة الكهربائية الاخرى، فيه الكثير من القطع التي تولد حرارة أثناء عملية التشغيل مما يؤدي إلى ارتفاع درجة الحرارة داخل الحاسوب بمعدلات أعلى من البيئة المحيطة له، لذا يتم تجهيز الحاسوب بمراوح داخلية تعمل مع بداية التشغيل، لغرض تقليل درجة الحرارة للمعدل المقبول، و ارتفاع درجة الحرارة الخارجية إلى أكثر من المعدلات الموصى بها (16–33) درجة مئوية قد يؤدي إلى تضرر الحاسوب.

2. **عوامل التآكل**

يعد الماء والأملاح من المواد الخطرة على الحاسوب ويجب تجنيب الحاسوب الأشياء التالية :

أ. انسكاب الماء او إي سوائل أخرى .

ب. الترشيح الناتج عن تسرب المياه الرطبة إلى داخل الحاسوب .

ت. فيضان المياه ودخول الماء إلى الحاسوب .

ث. نتيجة تراكم الأملاح بسبب تعرق جسم الإنسان .

ج. أكسدة نقاط الدارات وبالتالي تفقد وظيفتها في وصل الدارات مما يعطل الحاسوب .

كما أن هناك عوامل بيئية وخارجية وهي دائمة الحدوث، وتراكمها يؤدي إلى مشاكل لأجهزة الحاسوب و مكونات نظم المعلومات بشكل عام وقد ذكر منها :

1. **الغبار**

حيث يمكن ان يؤدي إلى تشكيل طبقة عازلة حرارياً وهذا يقلل من تبديد الحاسوب للحرارة الناتجة،أو تعطيل مزود الطاقة، أو تعطل الأقراص الصلبة ومحركات الاقراص المضغوطة.

2. **المجال المغناطيسي**

في حال تعرض الحاسوب الشخصي إلى مجال مغناطيسي عالي، فان المكونات الممغنطة فيه مثل القرص الصلب قد تتأثر، ويتم فقد المعلومات المخزنة عليها.

3. **تذبذب الطاقة**

إذ تصنف المشاكل الناتجة عن تأثيرات مصدر الطاقة إلى:

أ– المشاكل الناتجة عن ازدياد الجهد وانخفاض الجهد(تذبذب التيار).

ب– المشاكل الناتجة عن غياب الجهد نهائياً.

ج- المشاكل الناتجة عن العبور، والعبور عبارة عن تغير طفيف في الطاقة لا يمكن أنه يكرر نفسه مرة أخرى ويأتي على شكل انخفاض في الجهد أو ارتفاع في الجهد فإذا امتلك العبور تردداً كافياً عطل مكثفات الحماية و عناصر أخرى لوحدة الإمداد بالطاقة كما أن الجهد يؤدي إلى نفس الأضرار وتعطيل رقائق الحاسوب .

د- المشاكل الناتجة عن عملية تفريغ الكهرباء الساكنة.

تهديدات الأفراد (الموارد البشرية) :

أمن نظم المعلومات يعتمد أولاً وأخيراً على أمانة الأفراد المتعاملين معه فلا يكفي التأكد من أخلاقيات الموظف وأهليته عند تعيينه بل يجب إن تستمر مراقبته لأن التغيير السلوكي متوقع في أي وقت كذلك يجب عدم الإعتماد على موظف واحد بأي حال من الأحوال وإن كان لابد من ذلك فيجب أن يشمل ذلك الموظف إشرافا ومراقبة دقيقة وتوثيقا دقيقا لأعماله وأن يكون هناك تدريب لمساعدين لهم، وعند انتهاء خدمات أي موظف يجب سحب صلاحيته قبل فترة كافية فهناك عدة حوادث انتقام من موظفين أنهيت خدماتهم (حاج علي،2006،ص12).

وتشمل التهديدات التي تصدر من الأفراد المتعاملين مع نظم المعلومات التالي:

أ) التصرفات الخاطئة من قبل المتعاملين

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

- عرض معلومات حساسة
- إدخال بيانات خاطئة
- حذف البيانات أو تعديلها عن طريق الخطأ
- تخزين البيانات في مواقع غير صحيحة مثل سطح المكتب (Desktop)

ب) الأفعال المتعمدة (المدروسة)

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

- أفعال التعدي المقصودة

يمثل هذا النوع فئة واسعة من الأنشطة البشرية والالكترونية التي يمكن أن تؤثر سلباً على السرية وخصوصية المعلومات، عندما يصل أو يطلع أحد الأفراد غير المرخص لهم إلى

معلومات تعمل المنظمة على حمايتها، يعتبر مثل هذا التصرف تعدى مقصود ويعتبر مرتكبيه مثالا لمجرمي هذه التصرفات المتعدية المقصودة.

- أفعال الابتزاز المقصودة

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

- أفعال التخريب المقصودة

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

- أفعال السرقة المقصودة

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

ويؤدي عدم وجود سياسات واضحة لاستخدام نظام المعلومات إلى مشكلات أمن ضخمة يتعرض لها النظام، كما في حالة أعمال الصيانة والسلامة، وعند نقص الأفراد المؤهلين، أو بسبب تغيير ودوران العمالة، أو إدخال تكنولوجيات متقدمة تتطلب مهارات جديدة، أو إبطاء العمل أو توقفه .

وعندما لا توجد سياسة أمن معلومات للمنظمة تتصل بإعداد وحفظ نسخ إضافية مساندة لملفات المعلومات والبرمجيات التي تمتلكها، فإن المنظمة سوف تتحمل نفقات وخسائر واضحة ترتبط بالوقت والجهد والمال الذي ينفق في إعادة إنشائها من جديد.

إن سوء الاستخدام المقصود للنظام والوصول غير المعتمد له بغرض التطفل والنزوع للأذى وتعمد التخريب والتدمير والاحتيال أو السرقة تعتبر مخاطر وتهديدات خطيرة تؤثر سلبيا على قابلية نمو حياة النظام والمنظمة المالكة له بل تؤثر أيضا على القابلية للبقاء والاستمرار.

ومن الملاحظ أن كثيرا من المؤسسات أو المنظمات السياسية والاقتصادية والاجتماعية القائمة حالياً وخاصة في المجتمعات النامية لم تجاري حتى الآن التطور والنمو التكنولوجي المرتبط

باستخدام نظم المعلومات و تأمينها، فلا يزال يوجد قصور واضح ونقص كبير في التقنيين وعدم الأخذ بالمعايير الدولية و استخدام التشفير الخاص بالمزاولة الأحسن، إلى جانب قصور الإرشاد والتوعية والحقوق والالتزامات القانونية، مما يزيد في النفقات ويسبب تأخير الأعمال وعدم تكامل البيانات، و السماح باستمرار الوضع الراهن يحد من النمو المستقبلي ويؤخر اللحاق بعصر المعلومات والمعرفة المستهدف(الشبلي،2009،ص231).

المبحث الخامس

وسائل حماية نظم المعلومات

مقدمة:

في ظل تهديدات ومخاطر أمن نظم المعلومات تسعى الكثير من المؤسسات لإيجاد السبل والوسائل الوقائية والإجرائية التي تمكنها من مواجهة التهديدات الأمنية لكي تتمكن من القيام بوظائف أمن المعلومات ويتزايد الاهتمام بحماية نظم المعلومات سعياً لتقليل التكاليف ولضمان استمرارية العمل وجودة المعلومات المقدمة وهو ما من شأنه تعزيز استقرار المؤسسات للقيام بدورها في تقديم الخدمات والتي أصبح جُلها يقدم بصورة آلية .

وتتزايد الحاجة يوماً بعد يوم لمزيد من الوسائل والحلول لتعزيز حماية النظم، فنجد أن صناعة التعهيد وحلول الحوسبة السحابية آخذة في الاتساع على أساس أنها أحدى الحلول الممكنة (من وجهة نظر البعض) لإدارة مخاطر أمن نظم المعلومات.

ولا تنفك مراكز نظم المعلومات في المؤسسات المختلفة تبحث عن الآليات والوسائل التي تؤهلها لحيازة نظم المعلومات الأمنة، وقلما وجدت نظاماً آمناً بالكامل، بل أن البعض يجزم أن النظام الآمن بالكامل هو مستحيل لأنه من صنع وتنفيذ البشر، بل أن النظم الآمنة هذه اللحظة ربما لا تكون آمنة بعد فترة وجيزة من الزمن .

ويتعاظم دور المختصين في أمن المعلومات في إيجاد الحلول المختلفة لمشاكل أمن المعلومات . وكما ذكر البحيصي والشريف (2008) فالأمن مفهوم شامل يجب أن يشمل الجوانب الإدارية والتقنية ويتخلل إجراءات العمل المختلفة في أجزاء النظام الأربعة : الادخال والمعالجة والمخرجات والرقابة العكسية .

وسيتناول هذا المبحث توضيح سبل ووسائل حماية نظم المعلومات عبر استعراض السبل التي تتضمن الوسائل والإجراءات التنظيمية للحماية مثل تصنيف المعلومات، والتوثيق، والنسخ الاحتياطي، وإعداد البرنامج الأمني والسياسة الأمنية، ويشمل أيضاً استخدام آليات التحكم بالوصول، وكذلك وسائل الحماية التقنية كالتشفير، وجدران الحماية، وبرمجيات مكافحة الفيروسات والاختراق، وبرمجيات الحماية الشاملة، ووسائل التحقق من الشخصية.

الاجراءات التنظيمية لضبط نظم المعلومات

وتشمل عمليات المعلومات الرئيسة المتصلة بأمن المعلومات والتي تتطلب ممارسة وظائف نظم المعلومات ضمن مجموعة من الاجراءات الدقيقة والمناسبة والتي تحقق جودة العمل و تطبيق الاجراءات و آليات العمل الصحيحة والتي ستؤدي إلى ثقة المؤسسات بتسلسل العمليات لديها .

أولاً: / تصنيف المعلومات

تصنف المعلومات حسب أهميتها وحساسيتها وذلك بغرض معرفة درجة الحماية التي تتطلبها، فمن المعلومات ما لا يحتاج إلى حماية بالمطلق ويحصل عليها من يريد ومتى يشاء، ومنها ما يحتاج إلى مستوى من الحماية ويمكن لأشخاص معينين أن يحصلوا عليها، ومنها ما يتطلب حماية قصوى ولا يتوفر إلا لشخص بعينه أو مجموعة يحددها .

ويرى عرب (2002،ص3) أن ضمان غايات أمن المعلومات كلها أو بعضها يعتمد على المعلومات محل الحماية واستخداماتها وعلى الخدمات المتصلة بها، فليس كل المعلومات تتطلب السرية وضمان عدم الافشاء، وليس كل المعلومات في منشأة واحدة بذات الاهمية من حيث الوصول لها أو ضمان عدم العبث بها.

ويرجع الباحث أسباب إختلاف تصنيفات المعلومات إلى أن احتياجات المؤسسات من المعلومات متفاوتة، كما أن احتياجات المستخدم النهائي من المعلومات مختلفة.

و إليه تشير البكري(2001) أن يمكن تصنيف المعلومات حسب درجة الرسمية إلى :

- معلومات رسمية : وهي المعلومات التي تخرجها نظم معلومات المؤسسة
- معلومات غير رسمية : وهي معلومات تأتي من خارج نظم المعلومات .

ويعرف تقرير دائرة المحفوظات بالأمم المتحدة(2006) عملية تصنيف المعلومات بأنها :النظام الذي يوضح كيفية عنونة وإنشاء أنواع حماية المعلومات الحساسة.

كما ويبين التقرير عبر طرحه مجموعة أسئلة في قائمة معايير مرجعية آلية لتقييم حساسية المعلومات، وهي كالتالي :

- هل تتعلق هذه المعلومات بسلامة وأمن الموظفين والمرافق؟
- هل تنطوي هذه المعلومات على احتمالية تعريض الغير للخطر؟
- هل تتعلق هذه المعلومات بأمن المؤسسة أو طبيعة العلاقات الدولية؟
- هل تحتوي هذه المعلومات على بيانات تتعلق بأسرار الميزة التنافسية ؟
- هل تتعلق هذه المعلومات بالعمليات التجارية للمنظمة؟
- هل تتعلق هذه المعلومات بخصوصية الموظفين والعاملين الآخرين؟ .

وتقوم بعض المؤسسات بتصنيف المعلومات من حيث السرية لديها طبقاً لمستويات أربع هي:

- عام(متاح للجميع)
- خاص(متاح عند الولوج للنظام بشكل أمن)
- سري (متاح بكلمة سر لمجموعة محددة)
- سري للغاية (متاح فقط للمستويات العليا، أو لفرد واحد).

ويشير الباحث إلى أنه ومن خلال عمله بأحدى الكليات التقنية محل الدراسة، وخبرته بنظم المعلومات فإن بيئة الكليات التقنية تفرض أخذ الزمن بالاعتبار عند القيام بتصنيف المعلومات، بمعنى أن بعض المعلومات التي تعتبر غير متاحة لفئة معينة ربما تصبح متاحة مع مرور الزمن، والمدة الزمنية هنا غالباً فصل دراسي أو سنة دراسية أو مدة برنامج دراسي (سنتان في حالة برامج الدبلوم، أو أربع سنوات في حال برامج البكالوريوس).

ويجب ملائمة حماية أنظمة المعلومات بنوع المعلومات التي تحتويها هذه النظم، مثلاً تتناسب إجراءات تشفير المعلومات مع درجة السرية التي تحملها الرسائل أو البيانات المنقولة، وحينما تزيد الإجراءات الأمنية دون داعي فإن ضعف وبطء النظام هو ما يحدث نتيجة لذلك مما يجعل المؤسسات تتكلف تكاليف أكبر في غير مكانها دون أن تجني الثمار التي من أجلها استثمرت في تحقيق أمن نظم المعلومات، وعلى النقيض فإن بعض النظم التي تستدعي حماية متقنة وعالية الدرجة قد لا تكون كذلك !، وهو ما قد يكلف المؤسسات الكثير من التكاليف مقابل معالجة المخاطر الناتجة عن عدم الالتفات لتطبيق مستوى عالٍ من الأمان(الشبلي،2009،ص).

ثانياً: / استخدام الوثائق المكتوبة

وتتطلب عمليات المعلومات اتباع نظام توثيق خطي لتوثيق بناء النظام وكافة وسائل المعالجة والتبادل ومكوناتها، وبشكل رئيس فإن التوثيق لازم وضروري لنظام التعريف والتخويل، وتصنيف المعلومات، والأنظمة التطبيقية، وفي إطار الأمن فإن التوثيق يتطلب أن تكون استراتيجية أو سياسة الأمن موثقة ومكتوبة وأن تكون إجراءاتها ومكوناتها كاملة محل توثيق، إضافة إلى خطط التعامل مع المخاطر والحوادث، والجهات المسئولة ومسؤولياتها وخطط التعافي وإدارة الأزمات وخطط الطوارئ المرتبطة بالنظام عند حدوث الخطر(الشبلي،2009،ص215).
والحاجة إلى توثيق نظم المعلومات غايتها الاستفادة من الخبرات السابقة والمدونة وتفيد في التالي:

- ضمان استمرار التشغيل في حالة تعطل الاجهزة او نقل الأفراد.
- تقليل الصعوبات المرتبطة بتعديل أو إصلاح أو تطوير البرامج

- تقليل الأخطاء.
- تحقيق الاتصال بين الاقسام المختلفة.

ثالثاً : / تحديد المهام والواجبات الشخصية

Administration and Personnel Responsibilities

إن مهام المتصلين بنظام أمن المعلومات تبدأ في الأساس من حسن اختيار الأفراد المؤهلين وعمق معارفهم النظرية والعملية، وبشكل رئيسي فان المهام الإدارية أو التنظيمية تتكون من خمسة عناصر أو مجموعات رئيسة :

- تحليل المخاطر.
- وضع السياسة او الإستراتيجية
- وضع خطة الأمن
- توظيف الأجهزة والمعدات والوسائل
- تنفيذ الخطط والسياسات.

ومن المهم إدراك أن نجاح الواجبات الفردية أو الجماعية للمنشأة يتوقف على إدراك كافة المعنيين في الإدارة (بمهامهم التقنية والإدارية والمالية) لإستراتيجية وخطة وواجبات الأمن والتزامات المؤسسة باعتبار مسائل الأمن واحدة من الموضوعات التي يدركها الكافة ويتمكن الكل من التعامل مع ما يخص واجباتهم من بين عناصر الأمن.

وعلى مستوى المستخدمين، فان على المؤسسة ان تضع التوجيهات الكافية لضمان وعي عام ودقيق بمسائل الأمن، بل المطلوب بناء ثقافة الأمن لدى العاملين والتي تتوزع بين وجوب مراعاة أخلاقيات واستخدام التقنية وبين الإجراءات المتطلبة من الكل لدى ملاحظة أي خلل، وعلى المؤسسة أن تحدد للمستخدمين ما يتعين عليهم القيام به والأهم ما يحظر عليهم القيام به في معرض استخدامهم للوسائل التقنية المختلفة(الشبلي،2009،ص217).

ويقلل تقسيم الواجبات والمسئوليات من خطر حدوث اختراق في نظم المعلومات إلى حد كبير(طلبة وآخرون،1997،ص289) وتوزع مسئوليات أمن المعلومات وفق السياسة الأمنية بحيث تكون مسئولية حماية كل أصل من أصول المنظمة والعمليات الأمنية الواجب القيام بها محددة بوضوح، ويمكن للأفراد أصحاب المسئوليات الأمنية تفويض مهام أمنية إلى غيرهم، ولكن تبقى المسئولية على عاتقهم، ويتوجب أن تكون المسئولية المفوضة قد تمت بالطريقة الصحيحة.

رابعاً: / خطط الطوارئ

لابد من وضع الخطط لإستمرارية عمل نظم المعلومات في حالة المشاكل الكبيرة كتعطل أجهزة الحاسوب تعطلاً طويلاً أو غير ذلك من الحالات الطارئة، ولابد من قياس المشاكل التي سيواجهها مستخدم النظام في هذه الحالات ووضع البدائل على ضوء ذلك، وفي بعض الأنظمة يستوجب وجود نظام مساند يعمل بطريقة فورية في حالة الطوارئ في حين أن هناك أنظمة أخرى يمكنها الاستغناء عن الحاسوب عدة أيام دون إن تتأثر تأثراً كبيراً هذا من ناحية الاستمرار التشغيلي المباشر للحواسيب، أما النواحي الأخرى الهامة غير المباشرة أو المساندة كالكهرباء المستمرة والثابتة أو التبريد الموزون المستمر فهي ضرورية للتشغيل الخالي من الأخطاء إذ أن الزيادة الشديدة في التيار الكهربائي والارتفاع غير المحتمل في درجات الحرارة كلها تؤدي إلى أخطاء في تشغيل ومعالجة البيانات كذلك يجب مراعاة إن الانقطاع المفاجئ للتيار والإطفاء المباشر لأجهزة الحاسوب كثيرا ما يؤدي إلى فقد بعض المعلومات أو السجلات(حاج علي،2006،17).

ولكي يكتمل تحقيق المتطلبات الإدارية للحماية يجب مراعاة حزمة من الإجراءات التنظيمية الخاصة بقسم نظم المعلومات مباشرة وهي :

أولاً : تنظيم إدارة خاصة بأمن نظم المعلومات يناط بها تحديد السياسة الأمنية للنظام من حيث الإدخال، التعديل ومن حيث ضمان استمرارية العمل بالكفاءة المطلوبة، وبعد تحديد هذه السياسة يجب توثيقها ودعمها من قبل الإدارة العليا للمؤسسة، والعمل على تعزيز وعي العاملين والمستخدمين.

ثانياً : يحدد مشرفا للأمن بمركز نظم المعلومات تقع على عاتقه التأكد من التزام العاملين بالسياسة الأمنية المرسومة وتنسيق التدريب الفني في هذا المجال والمساعدة في التصميم والبرمجة لتنفيذ المتطلبات الفنية لهذه السياسة.

ثالثاً : يحدد مسئول أمن يمثل المستخدم ويكون مسئولاً لدى الجهة المستخدمة للنظام عن ضمان التزام إدارة نظم المعلومات بالسياسة الأمنية المحددة وتحديد مستوى الصلاحية لكل المتعاملين مع النظام.

رابعاً : مراجعات مجدولة لعمليات إدارة أمن نظم المعلومات، بما يلزمها من تنفيذ نظام دقيق للمخزون يشتمل أجهزة وملحقات وأقراص وتوثيق ومكتبات برمجية وقطع غيار وأوراق طباعة وحبر وغيرها من المستلزمات التشغيلية لنظام المعلومات (حاج علي و حسين،2005،ص19).

وقد وضع العتيبي(2010،ص86) من خلال دراسة أجراها على المنظمات السعودية مجموعة من الضوابط لتنسيق الاجراءات التي تتعلق بالأنشطة داخل المنظمة و ما يتعلق بأنشطة تخص تنسيق العلاقة مع الاطراف الخارجية (المتعهدين)، ويبين الجدول رقم (3-2) هذه الضوابط الاجرائية :

م.	الاجراء	الضابط
1	التزام الإدارة تجاه أمن المعلومات	ستقوم الإدارة وبشكل إيجابي بدعم الأمن داخل المنشأة من خلال التوجيه الواضح وبيان الالتزام بمسئوليات أمن المعلومات.
2	تنسيق أمن المعلومات	يتم تنسيق الأنشطة المتعلقة بأمن المعلومات حسب المسؤوليات من مختلف أجزاء المنشأة ووفقاً للأدوار ومهمات الوظائف ذات العلاقة.
3	تخصيص المسؤوليات	يتم وضع تعاريف محددة لكافة المسؤوليات المتعلقة بأمن المعلومات.
4	عملية إصدار التصاريح لمرافق معالجة المعلومات	يتم تحديد وتنفيذ عمليات إصدار التصاريح الإدارية للمرافق الجديدة الخاصة بمعالجة المعلومات.
5	الاتفاقيات المتعلقة بالسرية	يتم تحديد المراجعة المنتظمة للاتفاقيات الخاصة بمتطلبات اتفاقيات السرية أو عدم الكشف والتي تعكس احتياجات المنشأة لحماية المعلومات.
6	الاتصال بالسلطات	الحرص على إجراء الاتصالات الملائمة مع السلطات ذات العلاقة.
7	الاتصال بالجهات ذات الاهتمامات الخاصة	الحرص على إجراء الاتصالات الملائمة مع الجهات ذات الاهتمامات الخاصة أو الاتحادات والمؤسسات المتخصصة في النواحي الأمنية.
8	المراجعة المستقلة لأمن المعلومات	يتوجب القيام بالمراجعة المستقلة لاتجاه المنشأة نحو إدارة أمن المعلومات وتنفيذها(مثل أهداف وضح الضوابط، الضوابط، السياسات، العمليات والإجراءات المتعلقة بأمن المعلومات) وذلك على فترات محددة، أو عند حدوث تغييرات جوهرية على تنفيذ الخطة الأمنية.
9	تعريف المخاطر ذات العلاقة للجهات الخارجية	يتم تحديد المخاطر التي يمكن أن تهدد أمن معلومات المنشأة ومرافق معالجة المعلومات من العمليات ذات العلاقة بجهات خارجية ووضع الضوابط الملائمة قبل منح تصريح بالدخول.
10	الاهتمام بالنواحي الأمنية عند التعامل مع العملاء	يتم الإهتمام بكافة المتطلبات الأمنية قبل منح العملاء التصريح بالدخول على المعلومات الخاصة بالمنشأة أو الأصول الخاصة بها.
11	الاهتمام بالنواحي الأمنية عند التعامل مع الاتفاقيات المتعلقة بطرف ثالث	الاتفاقيات الموقعة مع أي طرف ثالث والتي تتضمن "الدخول على المعلومات، معالجة المعلومات، الاتصال أو إدارة المعلومات الخاصة بالمنشأة او مرافق معالجة المعلومات بها، أو إضافة منتجات أو خدمات على مرافق معالجة المعلومات"، سوف تغطي كافة المتطلبات الأمنية ذات العلاقة.

التحكم بالوصول لنظم المعلومات Access Control

وقد عرفه الألفي وآخرون (2011،ص18) بأنه منع الاستخدام غير المرخص للموارد، أي ان يتم تحديد من يمكنهم النفاذ إلى مورد معين وتحت أي ظروف يمكن أن يتحقق ذلك، وما هو المسموح به لهؤلاء المرخص لهم باستخدام تلك الموارد.

وسائل التعرف والتحقيق من شخصية المستخدم :

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

والتعرف (Identification) يعتبر أول خطوة في سبيل منح حق الدخول إلى النظام والمقصود به الأسم الذي يعرف به المستخدم، وهذا التعرف لا يكون كافيا لتحقيق أمن البيانات، حيث أنه يتوجب التحقق أو الوثوق من شخصيه المستخدم (Authentication) وهو يعني التأكد من المستخدم بأنه الشخص صاحب الاسم الذي تم إدخاله، والشكل رقم (3-14) يوضح خريطة تدفق البيانات التي تحتوى على وسائل التحقق من شخصية المستخدم، وهذا التحقق عادة يتم مرة واحدة بإستثناء النظم الكبيرة التي تطلب مزيدا من الأمن (طلبة وآخرون،1997،ص231-236).

و هناك ثلاثة وسائل للتحقق من شخصية المستخدم كالآتي:

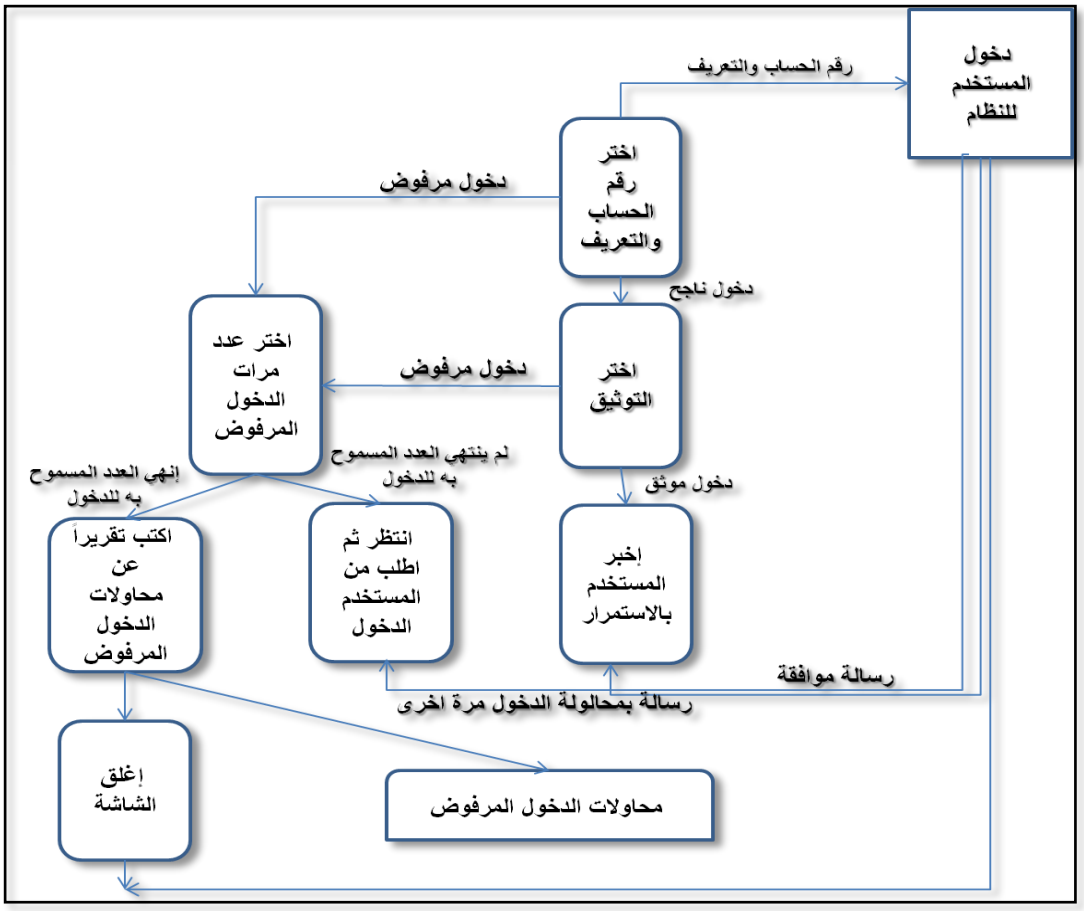
1- استخدام خواص مميزة للمستخدم(في الشخص) مثل الصوت أو بصمات الأصابع أو قياسات الوجه، وهي في الغالب تستخدم مقاييس بيولوجية Biometric، والصورة التالية : توضح أحدى هذه التقنيات صورة رقم (3-13) توضح قيام مستخدم بالدخول إلى نظام المعلومات بواسطة بصمة الاصبع.

2- استخدام أشياء يمتلكها المستخدم مثل المفاتيح أو البطاقات الممغنطة.

3- استخدام أشياء يعرفها المستخدم مثل كلمات المرور (Passwords).

ويرى الباحث أن الوسيلة الأولى هي أكثر الوسائل تأميناً لأنها تعتمد على خصائص بشرية فريدة، ولكنها ليست منتشرة لصعوبة تنفيذها، والوسيلتان الثانية والثالثة هما الشائعتان في معظم النظم، والمفاتيح والبطاقات تستخدمان بصفة خاصة في النظم التي تتطلب درجة عالية من الأمن مثل البنوك والمؤسسات العسكرية وأنظمة التحكم.

شكل رقم (3-14) يوضح خريطة التحقق من شخصية المستخدم.

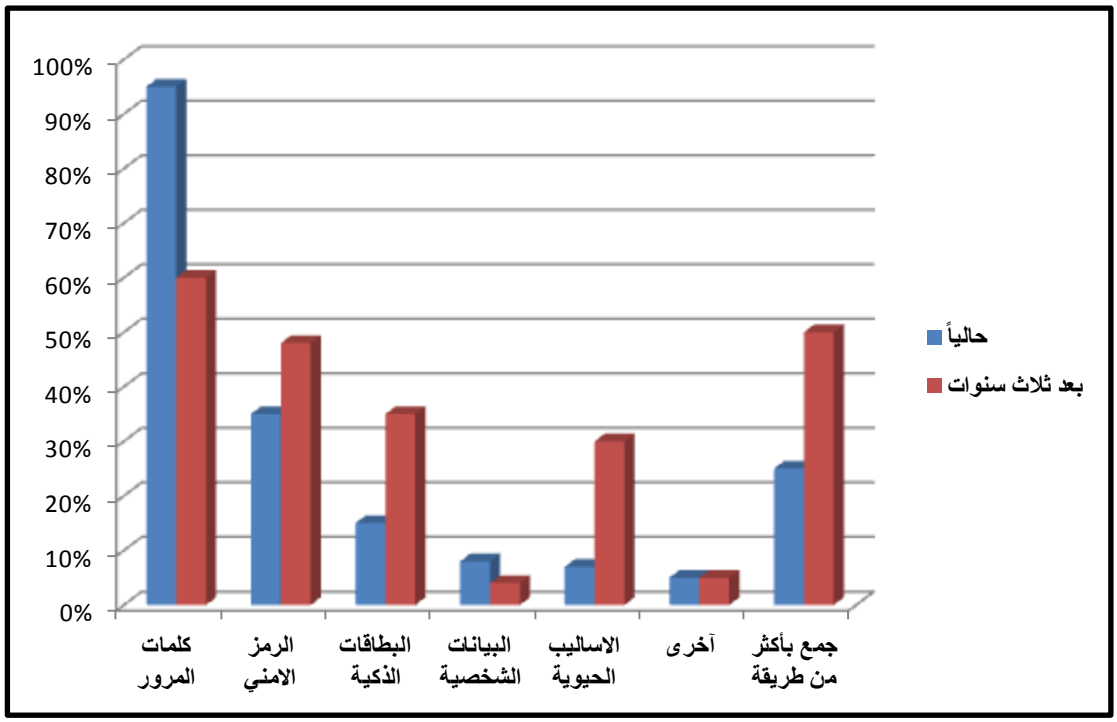


المصدر بتصرف : (طلبة وآخرون،1997،ص233)

وتعد وسائل التعريف والتوثيق الأقوى هي تلك الوسائل التي تجمع بين هذه الوسائل جميعا على نحو لا يؤثر على سهولة التعريف وفعاليته في ذات الوقت(عرب،2002،ص13)، ويوضح الشكل (3-15) مخططاً لأكثر الطرق المستخدمة حالياً في عمليات التحقق من الوصول وما سيكون عليه الحال بعد ثلاث سنوات من وجهة نظر المبحوثين في بحث أجراه David Perry (2006)[6] . ، ويظهر التقرير أن كلمات المرور هي الأكثر استخداماً بينما المقاييس الحيوية ستستمر منخفضة الاستخدام نسبياً.

[6] قام الخبير في أمن المعلومات David Perry باجراء هذه الدراسة في بيئات عدة ومنظمات متعددة وتوصل من خلالها الى العديد من النتائج التي مكنته فيما بعد من وضع تصور لحال Global Security خلال الثلاث سنوات المقبلة في حينه. ،المصدر : http://www.theregister.co.uk/2010/07/12/practicalities_of_provisioning

شكل رقم (3-15): مخطط يبين الطرق التحقق من الوصول حالياً، وبعد 3 سنوات قادمة



المصدر بتصرف : (http://www.theregister.co.uk/2010/07/12/practicalities_of_provisioning)

ومن أشهر وسائل التحقق :

أولاً:/ كلمات المرور (Passwords):

كلمة المرور(السر) هي عبارة عن مجموعة من الحروف و/أو الأرقام المتتالية التي يقوم المستخدم بإدخالها إلى الحاسب، ويقوم الحاسب بفحص هذه الحروف ومطابقتها مع الكلمة المخزونة به، فإذا وجدها مطابقة فأنه يسمح للمستخدم بتنفيذ جميع العمليات المصرح له بها.

وعند اختيار كلمة المرور يراعى أن تكون سهلة التذكر بالنسبة للمستخدم المصرح له بالدخول إلى النظام كما يراعى صعوبة التعرف عليها بواسطة المتطفلين عن طريق التخمين وكلما زاد عدد حروف كلمة المرور كلما فشل احتمال التعرف عليها واكتشافها بالتخمين أو عبر برمجيات كسر كلمات المرور.

وقد حدد Burnett (2006,p.3) الوقت اللازم لاكتشاف كلمة المرور بالمعادلة التالية:

وقت الاكتشاف = (عدد محاولات الوصول إلى كلمة المرور) x (الوقت اللازم لإدخال كل كلمة)

وتجري عملية احتساب محاولات أو احتمالات كسر كلمات السر، على أساس رياضي، فلو افترضنا استخدام الاحرف الانجليزية وهي 26حرفاً، وهي تكون بصورة أحرف صغيرة small letters أو كبيرة Capital letter وتضاف اليها استخدام 10 اشارات ورموز بما فيها الاشارات

الخاصة وهي ((,),*,&,^,%,$,#,@,!,`) بالتالي يصبح أمامنا 36 قيمة ممكنة، ولو أفترضنا كلمة مرور مكونة من 3 خانات، إذن فان عدد الاحتمالات هي كما في الجدول رقم (3-3) التالي :

استخدام حروف فقط (من نوع واحد)	26×26×26
استخدام حروف ورموز	36×36×36
استخدام حروف بنوعيها صغيرة وكبيرة بالاضافة إلى الرموز	62×62×62[7]
استخدام الارقام وحدها	10×10×10
استخدام الارقام والحروف	36×36×36
استخدام الحروف (بنوعيها) والأرقام والرموز	72× 72×72[8]

وتخيل الإحتمالات كيف ستصبح، لو أنك أمام ستة أحرف على الأقل وتستخدم الخليط من الارقام والحروف و الرموز (Ratzan,2004,P.67).

ويذكر الباحث مجموعة من الارشادات والنصائح الخاصة بإنشاء كلمات المرور منها:

- من الافضل أن تتكون كلمة المرور من الأحرف بشكليها والارقام وعلى الأقل أحدى الأحرف الخاصة كـ(!@#$%^&*()_+|)
- أن يكون طول كلمة المرور أو عدد خاناتها يتجاوز 7 أحرف أو خانات .
- عدم استخدام كلمات المرور نفسها لأجهزة متعددة، وعدم استخدام كلمات مرور لتطبيقات وبرامج مختلفة.
- أمثلة لكلمات مرور قوية :

&Ewa037(Sa , 8@ −95Da!zI , 93 −Lkw#-aq

ثانياً:/ المصافحة Handshaking

وتعتبر المصافحة من وسائل التحقق من المستخدم التي توفر درجة عالية من الأمن، حيث يتم إعطاء المستخدم دالة تحويلية معينة Transformation Function بحيث تكون معروفة لنظم الحاسوب، فلو رمزنا للدالة بالرمز د()، وعندما يرغب المستخدم بالدخول إلى النظام، فإن الحاسب يعطيه رقماً عشوائيا(ر) وينتظر إجابته، ويقوم المستخدم بحساب هذه القيمة د(ر)

[7] 62= (2*26)+10، وهي الحروف بنوعيها small letters، و capital letters

[8] 72=(2*26)+10+10، وهي الحروف بنوعيها small letters، و capital letters، بالاضافة الى الارقام من (0 الى 9)

ويدخلها إلى الحاسب، وفي هذه الحالة يصعب على المتطفل الدخول إلى النظام دون معرفة دالة التحويل د.

ومن وسائل التحكم بالوصول :

يستخدم مخططو نظم المعلومات لهدف التحكم في الوصول مصوفة الوصول، وهي تخطيطاً يسبق عمليات الوصول والنفاذ، وتجري فيها معالجات عمليات الولوج بناءاً على مصفوفة من بعدين، بينما تأتي سجلات الأداء للرقابة على الوصول.

أولاً:/مصفوفة الوصول :

ويذكر الالفي وآخرون (2011،ص650-ص652) أن هناك نموذج عام للتحكم في الوصول كالنظام المستعمل من قبل نظم إدارة قواعد البيانات والملفات ألا وهو مصفوفة الوصول (Access Matrix) المبينة بالشكل رقم(3-16)، والعناصر الأساسية لهذا النموذج هي كما يأتي :

- الفاعل : وهو كيان قادر على الوصول إلى الأشياء وعموما، فإن مفهوم الفاعل يكافئ مفهوم العملية. وفي الواقع أي مستخدم أو تطبيق لا يصل إلى كائن ما إلا من خلال العملية التي تمثل ذلك المستخدم أو التطبيق.
- الكائن : أي شئ يتم التحكم في الوصول أو النفاذ إليه : كالملفات أو أجزاء منها، والبرامج، وقطاعات الذاكرة .
- حق الوصول : الطريقة التي يمكن للفاعل النفاذ بها لكائن ما: كالقراءة، والكتابة، والتنفيذ.

شكل (3-16) يوضح مصفوفة الوصول

	البرنامج 1	القطعة (أ)	القطعة (ب)	(البعد الثاني)
العملية 1	قراءة وتنفيذ	قراءة وكتابة		
العملية 2			قراءة	
(البعد الأول)				

المصدر : الالفي وآخرون (2011)

ويبين كل مدخل في المصفوفة حقوق وصول فاعل معين لكائن ما، حيث يمثل أحدى محوري المصفوفة الفاعل الذي قد يحاول الوصول إلى البيانات، والمحور الاخر فيعدد الكائنات التي يمكن الوصول إليها، وقد تكون تلك الكائنات حقولاً للبيانات أو سجلات محددة أو قواعد بيانات بأكملها .

ومتى ما استخدمت وسائل تعريف ملائمة لإتاحة الوصول للنظام، ومتى ما تحققت عملية التوثق والمطابقة والتأكد من صحة التعريف (الهوية) فإن المرحلة التي تلي ذلك هي تحديد نطاق الاستخدام Authorization وهو ما يعرف بالتخويل أو التصريح باستخدام قطاع ما من المعلومات في النظام، وهذه المسألة تتصل بالتحكم بالدخول أو التحكم بالوصول إلى المعلومات أو أجزاء النظام Access Control system.

ويذكر الباحث أن هناك ثلاث تقنيات للدخول للبيانات وهي كالتالي:

أ. هرمية الدخول Access Hierarchies : وتعني منح مستخدمي الإدارات الأعلى سلطات الإدارات الأدنى.

ب. جداول السلطات Authority Lists : وهي قائمة بالمستخدمين مع إمتيازات الدخول لكل مستخدم، تعتبر مثالية لحماية ملفات معينة من النظام والجدول التالي رقم (3-4) يوضح مثالاً لهذه الجداول.

جدول رقم (3-4): يبين جدول السلطات

المستخدم	الامتيازات
رائد	قراءة وكتابة
عمار	قراءة فقط
رشيد	قراءة وكتابة

ج. القدرات Capabilities : وهي إعطاء كل مستخدم حق الدخول إلى أحد المكونات بما يحقق له تنفيذ الوظائف الخاصة به وهذه الوسيلة تحقق مبدأ أقل إمتياز (Least Privilege).

ثانياً:/سجل الأداء :

وتعرف أيضاً بسجلات النفاذ إلى النظام، والمطلوب منها أن تحدد شخص المستخدم ووقت الاستخدام، ومكانه، ومحتوى الاستخدام وأي معلومات إضافية أخرى تبعاً للنشاط ذاته.

وحاليا توظف سجلات الأداء في مختلف أنواع نظم المعلومات حتى تقوم بالكشف وتسجيل ما يتعلق باستخدامات الجهاز وبرمجياته و النفاذ إليه، وتتخذ سجلات الأداء أهمية استثنائية في حال تعدد المستخدمين وتحديداً في حالة شبكات الحاسوب التي يستخدم مكوناتها أكثر من شخص، وفي حالة شبكات المستخدمين فإن هناك أكثر من نوع من أنواع سجلات الأداء وتوثيق الإستخدامات، كما أن سجلات الأداء تتباين من حيث نوعها وطبيعتها وغرضها، فهناك سجلات الأداء التاريخية والسجلات المؤقتة، وسجلات التبادل وسجلات النظام وسجلات الأمن وسجلات قواعد البيانات والتطبيقات وسجلات الصيانة أو ما يعرف بسجلات الأمور التقنية وغيرها.

ويرى الباحث أن تركيز عمل مصفوفة الوصول يأتي في جزئي النظام (الإدخال والمعالجة)، بينما تعتبر سجلات الأداء جزء من إخراجات النظام، أو أقرب ما تكون كعملية للرقابة والتتبع تماثل عملية تنفيذ التغذية الراجعة feed back.

سياسة أمن المعلومات

قال ابن خلدون: "لابد للعمران البشري من سياسة ينتظم بها أمره"[9]

اشتمل عنوان هذه الدراسة على كلمة (إدارة) وتحمل هذه الكلمة معنى ومحتوى وهدف، فالإدارة هي التخطيط والتنظيم والتوجيه والرقابة، وبذلك فإن التخطيط الذي يعتبر المنطلق الأول للعمليات الإدارية يتوجب أن تتضمنه برامج الأمن المعلوماتي لنظم المعلومات، وبالتالي فإن التخطيط هنا هو أبرز الخطوات الأولية التي ينطلق منها أمن نظم المعلومات ، ولا بد من أن تتبعه أنشطة توجيه وتنظيم ورقابة وهذا مكمن نجاح السياسات الأمنية .

ولذلك يرى الباحث في سياسة أمن المعلومات أو كما يسميها البعض السياسة الأمنية أنها البذرة التي ستنتج نظاماً آمناً، إذ ما تم حسن التخطيط لها وإنجازها، وحسن ترتيبها وتوزيعها على أفراد نظام المعلومات، وإدارة تنفيذها وممارستها، وقبل كل هذا رعايتها من قبل الإدارة العليا، ومن ثم عمليات الرقابة لتعديلها وتحسينها.

وعرف Olson and Abrams and Bailey (2001) سياسة أمن المعلومات بأنها مجموعة من القواعد والقوانين والممارسات التي تضبط عمل المؤسسة وتحمي مصادرها لتحقيق غايات أمنية خاصة، ولتكن جدية وممكنة يجب أن تمنح هذه القوانين الأفراد القدرة على تحديد الأفعال الحسنة والأفعال التي تتنافى مع هذه السياسات.

وبحسب الغثبر والقحطاني(2009) فإن سياسة أمن المعلومات تعني مجموعة من التوجيهات واللوائح والقواعد والممارسات التي ترشد إلى كيفية قيام المنظمة بإدارة وحماية وتوزيع المعلومات.

بينما يعرفها Dulany (2002) أنها مجموعة قوانين أمنية تسيطر على نظام المعلومات و تزوده بمستوى حماية موثوق به. و هذه السياسات يجب أن تُوجه الإدارة و سبل الحماية والمصادر المرتبطة بالمعلومات و بنظام المعلومات، ويرتبط مستوى قسوة تلك السياسات عادة بمستوى المخاطر المراد تجنبها .

وبذلك رأى نعيم (2003) أن السياسة الأمنية تغدو فعالة إذا توافقت مع ثقافة المنظمة والبيئة البرمجية المحيطة فليس هناك سياسة أمنية واحدة تناسب الجميع .

ويعرفها الباحث بأنها تطبيق وسائل تقنية وإجراءات إدارية لحيازة مصادر المعلومات (المادية، البرمجية، البيانات) بهدف الحفاظ على نظم المعلومات وأصول المنظمة بشكل عام وضمان خصوصية المؤسسة .

---

[9] (ابن خلدون، الجزء الرابع، الفصل 52،ص277) نقلاً عن العتيبي (2010،ص94)

ويرى الباحث أن السياسة الأمنية تنبثق من قواعد وتوجيهات تضعها إدارة المنظمة وفق الثقافة العامة في المنظمة، لتوضح كيفية قيام الاشخاص بأداء أعمالهم المتعلقة بنظم المعلومات بما يضمن تحقيق الغايات الأمنية (السرية – السلامة – التوفر)، ويوافق الباحث الدراسات السابقة بأن قسوة السياسات الأمنية تزداد باطراد تناغماً مع مستوى المخاطر التي تتعرض لها المؤسسة.

ويذكر طلبة وآخرون (1997،ص) أنه لابدّ من وجود أربعة مراحل تمهيدية لتحقيق السياسات الأمنية في المؤسسات وهي كالتالي:

- مرحلة التقييم: إنّ تقييم المخاطر الممكنة في أفق عمل المؤسسة أمر ضروري وذلك من خلال التقاء العاملين ومعرفة الوضع الأمني والأخذ بتوصياتهم وإرشاداتهم ووضعها بعين الاعتبار.
- مرحلة التصميم: إنّ استخدام أحدث تقنيات الحماية الأمنية كالجدران النارية وأنظمة كشف التطفل لا تحقق الحماية الكاملة، وخاصة عندما لا يتم تحديثها باستمرار، لذلك لابدّ من اعتماد هيكل أمني صلب أثناء تصميم البنية الأساسية للأمن المعلوماتي للمؤسسة.
- مرحلة التنفيذ: يتم تركيب كل الضوابط التقنية كالجدران النارية وأنظمة كشف التطفل وغيرها. مرحلة المراقبة: لابدّ من مراقبة جميع التقنيات والإجراءات الأمنية التي تمّ وضعها في المنشأة للتأكد من استمرارية عملها على الوجه المطلوب و إصلاح الأعطاب حال التعرض لها واستمرار تحديثها عند توفر تحديثات جديدة.

متطلبات السياسة الأمينة :

يرى داوود(2004،ص119–120) أنه على السياسة الأمنية للمؤسسة أن تحقق المتطلبات التالية:

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

ويمكن إجمال بعض من محاذير آليات بناء دليل لسياسة أمن نظم المعلومات وفق المعايير العالمية كما يلي :

- من الضروري أن تتعرف كل منظمة على متطلبات الأمن الخاصة بنظم معلوماتها (ISO/IEC 27002:2008)
- تبنى سياسات أمن المعلومات على عدم ذكر الصفات المجردة والخاصة للاشياء وبدلاً من ذلك توضع تحفظات عامة وذات دلالات دون التخصيص المطلق .
- كأي عملية توثيق موجهة توجد مخاطر في أن تنتج عن إعداد سياسة الأمن المعلوماتي وصيانتها وتوزيعها بيروقراطية في حد ذاتها، لذلك يصبح الحكم الجيد والصائب على الأمور المتضمنة ضرورياً فيما يتصل بالنسب التي يجب تبنيها والأخذ بها، إلى جانب عدم التقليل من الجهد الذي بذل في إعداد هذه السياسة وحفظها وصيانتها (الهادي،2006،ص26).
- تسهم التشريعات و المعايير في توفير بيئة مناسبة لتطبيق السياسات الرصينة الضامنة لحماية المعلومات(العتيبي،2010،ص108).
- توفير حماية رصينة للمستخدم والمستفيد حيث يتوافر مستوى أمن من الاستفادة من نظم المعلومات.

وقد فرق Abrams and Bailey (2001) بين ثلاث مستويات من السياسات الأمنية:

- سياسة أمن معلومات المؤسسة وهي تعكس توجهات إدارة المؤسسة.
- سياسة أمن المعلومات التنظيمية وهي تحدد عمل المستخدم بشكل تفصيلي.
- سياسة أمن المعلومات الفنية وهي تعكس توجهات المختصين في أمن المعلومات ومصممي السياسات.

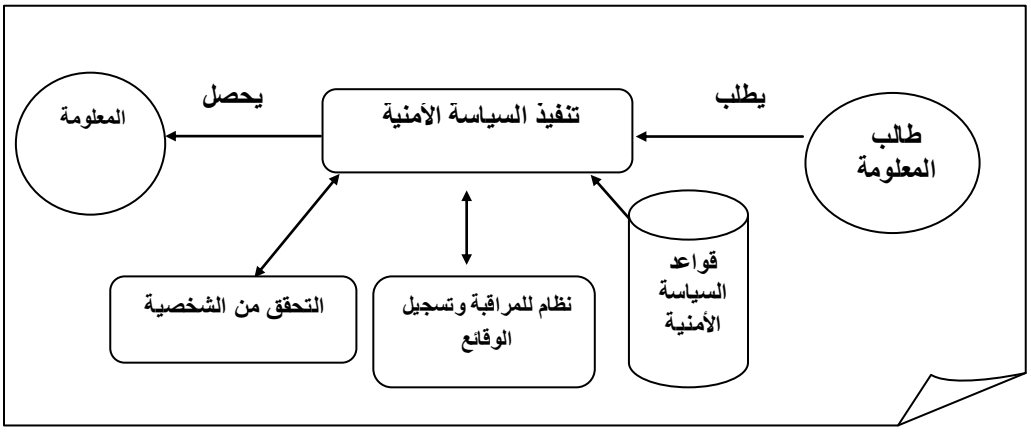
و لما كانت السياسة الأمنية المكتوبة للمؤسسة موجهة بالدرجة الأولى لمستخدمي نظم المعلومات بما فيهم الإدارة العليا كي يسترشد بها كل فرد عند اتخاذه لقرارات العمل، فإن وثيقة السياسة الأمنية الناجحة يجب أن تتسم بالصفات التالية :

- استخدام لغة بسيطة : حيث ان المستخدمين في المؤسسة ليسوا كلهم من خبراء أمن المعلومات، ومن ثم فلابد أن تكون اللغة المكتوبة بها السياسة الأمنية لغة بسيطة لا تحتوي على الكثير من المفردات، وأن يكون هناك شرح واضح لكل مفردة.
- الوضوح الكامل : يجب أن تكون السياسة الأمنية واضحة ومفهومة، وأن تكون مجموعة القيود والإجراءات والقواعد التي تحتويها مبررة ومقنعة، حتى يتبعها الجميع عن اقتناع .

- تحديد مسئوليات كل شخص: يجب أن تحدد السياسة الأمنية بكل وضوح المسئوليات والواجبات الملقاة على عاتق كل موظف وكل مسئول وكل مستفيد، فلا يجب أن تركز على شخص مسئولي أمن المعلومات، فإن ذلك سيعطي انطباعاً بأن هناك من يتولي مسئولية الأمن، وأن دور مستخدم نظم المعلومات هو دور هامشي
- سلطة فرض السياسة : أهم شيء هو فرض تنفيذ السياسة الأمنية وليس فقط كتابتها أو توزيعها، لذلك يجب أن تتضمن وثيقة السياسة الأمنية تحديد من لديهم صلاحية حرمان المستفيد من الخدمة عند المخالفة، وتحديد من لديهم صلاحية إيقاف بعض الخدمات المقدمة إذا كانت تؤثر على أداء الشبكة أو أمن المعلومات فيها .
- إتاحة المجال للحالات الاستثنائية والخاصة: لأنه لا توجد سياسة أمنية تغطي كل احتمالات الحاضر والمستقبل معاً، فيحب تحديد أسلوب تعديلها للسماح بالاستثناءات، عندما تظهر حالات خاصة تستدعي ذلك .
- إتاحة مجال للمراجعة : لا بد من إتاحة المجال لمراجعة السياسة الأمنية وتنقيحها عبر الزمن، كظهور مستجدات جديدة، وتقنيات جديدة (داوود،2004،ص120).

ولتصور كيفية عمل السياسة الأمنية في الحفاظ على أمن نظام المعلومات، نفترض أن هناك مستخدماً للنظام يريد الحصول على معلومات نسميه طالب المعلومة، وهناك معلومات، وهناك سياسة أمنية يتخللها قواعد السياسة الأمنية، وآليات التحقق من الوصول التي تتيح للمستخدم تحقيق وصول في حيز معلومات محدد، نظام رقابي لتسجيل الأداء والوقائع التي يقوم بها مستخدم النظام، فهذه المكونات تجتمع لكي تحقق تنفيذ السياسة الأمنية، ويبين الشكل رقم (3-17) عملية تنفيذ السياسة الأمنية .

الشكل رقم (3-17) يوضح تنفيذ وعمل السياسة الأمنية –



المصدر : (داوود،2004،ص113)

ويوصي الشبلي(2009،ص330) بأنه لضمان نجاح السياسة الأمنية يتعين أن تعمم بشكل كامل على كافة القطاعات داخل المؤسسة وأن تكون مقبولة و واقعية وتتوافر فيها الأدلة التوجيهية والإرشادية لضمان إدامة تنفيذها وعدم التقاعس، كما يرى وجوب أن تبين تصنيفاً واضحاً للمعلومات، وتنظم استراتيجية التعامل مع الأطراف الخارجية (المتعهدين).

ويرى داوود(2004،ص117) بوجوب توافق السياسة الأمنية مع السياسة العامة للمؤسسة، معللاً أنه من الخطأ أن يتم وضع السياسة الأمنية بمعزل عن السياسة العامة للمؤسسة، وإلا فهناك احتمال وقوع التعارض أو التضارب أو عدم التنسيق في أحسن الأحوال، وأي إجراء يتم تصميمه ليتبعه الموظفين لابد أن يتوافق مع باقي الإجراءات التي تتبعها المؤسسة.

وقد وضع الباحث رجوعاً إلى العديد من الدراسات جدولاً بالمبادئ التي من الواجب التنبه لها عند إعداد السياسات الأمنية لنظم المعلومات، ويوضح الجدول التالي رقم (3-5) حزمة من هذه المبادئ ومدى توافق الدراسات المذكورة معها .

جدول رقم (3-5) : يوضح مبادئ سياسة أمن المعلومات وتوافقها مع عدد من الدراسات.

مبادئ سياسة أمن نظم المعلومات	NIST (2006)	الحمامي والعاني (ص41-42)	OCED (2002,P.10-13)	ISO27002 (2005)
1. يجب أن تتكامل سياسة أمن نظم المعلومات مع استراتيجية المؤسسة.	✓		✓	✓
2. أن تكون تكلفة الحصول على المعلومات هي أعلى من تكلفة حمايتها .	✓	✓		
3. تتحصل المؤسسة على متطلبات السياسة الأمنية من خلال معرفتها بالمخاطر على مستوى المؤسسة	✓	✓	✓	✓
4. تنطلق سياسة أمن نظم معلومات المؤسسة من توجسات ومخاوف (هواجس) لدى العاملين على نظم المعلومات	✓	✓		✓
5. يجب أن توفر سياسة أمن نظم المعلومات مستويات متعددة من الحماية، لضمان سريان عمل المؤسسة حال تعرضها لكارثة أمنية .	✓	✓		
6. تتطلب سياسة أمن المعلومات درجة عالية من الإدراك والإلتزام بالتنفيذ .	✓		✓	✓
7. سياسة أمن المعلومات تتطلب تحديثاً مستمراً.	✓	✓	✓	✓

وسائل الحماية البرمجية لنظم المعلومات :

تتعدد أوجه الحفاظ على أمن نظم المعلومات وتختلف أشكالها ومنفذيها، كما أسلفت بذكر العديد من الصور والتوجهات ولابد من فهم أن استراتيجية حماية نظم المعلومات تشكل منظومة متكاملة وبالطبع لا غنى فيها عن استخدام الطرق البرمجية أيضاً .

ويأتي على أجندة هذه الوسائل ذكر: استخدام تقنيات التشفير، وجدران الحماية Firewall، و برمجيات مكافحة الفيروسات، ونظم منع وكشف الاختراقات .

أولاً: التشفير

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

والتشفير أو ما سماه العرب قديماً علم التعمية ليس جديداً بل أستخدمه المصريون القدماء منذ آلاف السنوات، ويعرف KESSLER(2012) التشفير بأنه العلم الذي يحول المعلومة الواضحة إلى معلومة سرية غير قابلة للفهم، ويذكر هنا ضرورة التشفير حال الاتصال عبر وسائط غير موثوقة، وخصوصاً في حالة التراسل من خلال الانترنت.

وتتم عملية التشفير بنقل معلومة من طرف لآخر عبر قناة وسيط، إذن هنالك ثلاث أجزاء هامة لفهم عملية التشفير، ولاستيضاح أكبر يبين الشكل التالي رقم (3-18) تصوراً لعملية التشفير في شكلها العام :

شكل رقم (3-18): طريقة عمل التشفير

المصدر:(مركز التميز لأمن المعلومات)

وقد حدد KESSLER(2012) ثلاث انواع رئيسية للتشفير وهي :

- التشفير المتناظر ويسمى المفتاح الخاص بحيث يعلمه كلا من طرفي الاتصال .
- التشفير غير المتناظر (المفتاح العام) بحيث يستخدم مفتاحاً للتشفير ومفتاحاً آخر لفك التشفير .
- وهناك نظاماً يجمع بين كلاهما، ويسمى (Hash Functions)؛

والجدول التالي رقم (3-6) يبين مقارنة بين هذه الانواع الثلاث للتشفير :

مقارنة بين أنواع بعض أنظمة التشفير.				
نوع التشفير	عدد المفاتيح	السرعة	حجم البيانات	قوة الحماية
المفتاح العام Symmetric key	مفتاح واحد	سريع	تشفير بيانات كبيرة الحجم أكثر من 400كيلوبايت	سرية وحماية محدودة
المفتاح العام Public key	مفتاحين	بطيء	تشفير بيانات محدودة الحجم أقل من 400 كيلوبايت	سرية وحماية أعلى
Hash/Xml Encryption	دمج بين الاثنين	سريع	تشفير بيانات كبيرة الحجم 400 K.B	سرية وحماية أعلى

المصدر : (سفور،2010،ص)

وكما للتشفير منافع كثيرة، ولكن توجد بعض الثغرات ومنها ما ذكره حاج علي(2007،ص12-14) وهي :

أ- اعتماد معظم التطبيقات على طريقة تشفير واحدة لفترة زمنية طويلة يساعد المحلل في أن يركز على هذه الطريقة فقط حتى يتمكن من معرفة المفتاح أو تصميم آلية لمعرفة المفتاح في كل مرة يتم تغييره .

ب-إن عملية تغيير المفتاح تعتبر عملية معقدة نظراً لتداخل عوامل إدارة وتوزيع المفاتيح خاصة عندما يزيد عدد المشتركين ومن ثم تظل بعض الإدارات تستخدم المفتاح لفترة طويلة مما يمكن لمحلل من كشفه .

ج-حتى وأن تم تغيير المفتاح فإن توزيعه خلال شبكات الاتصال يؤدي إلى إعتراضه من قبل الأعداء .

د- كل أنظمة التشفير يزيد ضعفها مع الزمن لتكاثر الهجومات عليها و ثبت من التجارب أن طرق التشفير والتي تقيم في فترة معينة بأنها قوية تكون ضعيفة في فترات لاحقة . فمثلاً الطرق الكلاسيكية كان يعول عليها كثيراً في تشفير المعلومات لكن التقدم في معالجة إستخدام الحواسيب أدى إلى التقليل مكانتها في حماية البيانات .

ثانياً: جدار الحماية Firewall

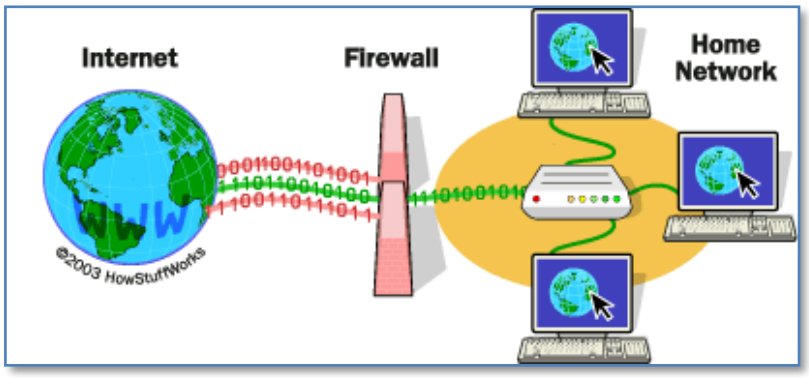
في قديم العصور كانت تبنى القلاع والحصون للدفاع عن المدن ضد المهاجمين، بطريقة مشابهة ولنفس الهدف صممت جدران النار او ما يسمى جدار الحماية .
وتسمى هذه الجدران بالجدران النارية بحيث أن رماة الدفاع من الداخل يستطيعون أن يطلقوا النار إلى الخارج من فتحات بجدران الحصن وهذه الفتحات لا تمكن الغزاة من إرسال نيرانهم إلى الداخل(يحياوي،2011).

وجدار الحماية هو أداة تصفي أو تحجز مرور البيانات بين الشبكة الداخلية المحمية والشبكة الخارجية التي نخشى منها والهدف منه هو حجز المستخدم في حيز سياسة أمنية معينة، وهذه السياسة قد تكون مثلاً منع أي دخول من الخارج مع السماح بالمرور من الداخل إلى الخارج . أو قد تكون هذه السياسة السماح بالدخول من أماكن معينة فقط أو من جانب مستفيدين معينين أو تسمح بدخول لأنشطة معينة دون باقي الأنشطة .

ويعتبر وضع السياسة الأمنية السليمة التي تلبي احتياجات المنظمة هو أحد التحديات الحقيقية التي تواجه المنظمة عندما تقرر حماية شبكتها عن طريق جدار الحماية (داوود،2000،ص159).

ويستطيع المستخدم من خلال الجدار الناري الخروج إلى عالم الانترنت ولكن لا يستطيع من في الخارج الدخول إلى الجهاز من خلاله ويوضح الشكل رقم (3-19) موقع جدار الحماية في بيئة نظم المعلومات وكيفية صده للهجومات من الخارج.

شكل رقم (3-19) يوضح كيفية صد الجدار الناري للهجومات من الخارج



المصدر: Tayson,Jeff(2011).How firewall works?

وهناك عدة أنواع للجدار الناري، يبين الجدول التالي أهمها مع المقارنة .

جدول رقم (3-7) : يوضح مقارنة بين بعض أنواع جدران الحماية

الموجه الحاجب	الوسيط	الحارس
الاكثر بساطة	معقد بعض الشئ	الاشد تعقيداً
لا يرى سوى العناوين ونوع البروتوكول المستخدم	يرى النص الكامل للرسالة	يرى النص الكامل للرسالة
عملية الرقابة على الأنشطة صعبة	يمكن مراقبة الأنشطة	يمكن مراقبة الأنشطة
قرار السماح أو المنع يعتمد على القواعد الموضوعة للاتصال	قرار السماح أو المنع يعتمد على سلوك البرنامج المركب	قرار السماح أو المنع يتوقف على تقسير محتويات الرسالة
إذا كانت قواعد العنونة معقدة يمكن أن يصبح الترتيب صعبا	يمكن أن يكون البديل المناسب في حالة قواعد العنونة المعقدة	الوظائف المعقدة للحارس تقلص من درجة الثقة به

المصدر : (داوود،2000،ص163)

ويذكر الباحث أن جدران الحماية أما أن تكون مادية أو برمجية أو جهاز متكامل يجمع بين النوعين .

ثالثاً : أدوات منع وكشف الاختراقات Intrusion Prevention/Detection Systems

تضاف أدوات صد أو منع الاختراقات إلى مستويات الحماية التي يجب توفيرها للنظم، وتعتبر هذه الإضافات بمثابة حماية مبكرة للنظام ولكن فيما لو تمكن مهاجم أو برنامج محدد من إحداث خلل بالنظام فإن أدوات أخرى يجب استخدامها تسمى أدوات الكشف عن الاختراقات ويجب ان يتم فحص هذه الوسائل من فترة لفترة حتى يتمكن النظام من العمل بفعالية، كما أنها تفيد مسئولي النظم في توظيف التقارير التي تنتجها النظم آلياً في وضع احصائيات محددة ووضع تصورات حول أنشطة النظام وأمنه وتختلف عن الجدران النارية بأنها تحتاج إدارة ومتابعة أكبر من قبل مراقبي نظم المعلومات والقائمين على تتبع أمن نظم المعلومات .(Farmer,2006,P168)

رابعاً : برمجيات مكافحة الفيروسات

البرنامج المضاد للفيروسات هو برنامج يستخدم لمنع واكتشاف فيروسات الحاسوب، والديدان، وأحصنة طروادة، و برامج التجسس، وغيرها من أشكال البرمجيات الخبيثة.

لكن و مهما كانت برامج مكافحة الفيروسات مفيدة، فأنه في بعض الأحيان يمكن أن تكون لها عيوب، فيمكن لبرامج مكافحة الفيروسات أن تقلل أداء الحاسوب إذا لم تكن مصممة بكفاءة وقد يواجه المستخدمين غير الخبراء مشكلة في فهم الأوامر والقرارات التي يقدمها برامج الحماية من الفيروسات وقد يؤدي القرار غير الصحيح إلى الإخلال بالأمن (ويكيبيديا،2009).

وتتواجد في أسواق البرمجيات الجاهزة العديد من البرمجيات المضادة للفيروسات، ويجب معرفة أن هذه البرمجيات تفقد قيمتها في ظل عدم وجود تحديثات مستمرة Updating، للحصول على قاعدة بيانات جديدة حول الفيروسات التي لا تتوقف عن التمحور والظهور بأسماء و أشكال تهديد مختلفة على مدار الوقت.

ويضيف الباحث إن اهم ما يعيب أدوات الحماية البرمجية عموماًعن غيرها من أدوات ووسائل حماية نظم المعلومات هو كونها الأكثر إلتصاقاً بالعامل الزمني، أي أن إستخدام هذه الأدوات دون الالتفات للتحديثات ومراعاة أن تبقى دائماَ محدثة ومتطورة يعني أنها ستكون دون جدوى وفعالية ولن تحقق المستوى الأمني المطلوب.

كما يمكن تصنيف كل نوع من أنواع أدوات الحماية التي تم ذكرها آنفاً طبقاً لزمن تنفيذها إلى :-

- وقائية : حيث تقوم بمحاولة تجنب وقوع الحوادث .
- تفحصية : وتهدف لاكتشاف الحوادث بعد وقوعها .

ويبين الجدول رقم (3-8): يبين أمثلة على الحماية الوقائية والحماية التفحصية.

نوع الحماية	أمثلة على الحماية الوقائية Preventive	أمثلة على الحماية التفحصية Detective
الإدارية (الاجراءات التنظيمية)	• برامج التدريب والتعزيز الأمني • فصل المهام • خطط الطوارئ	• تقييم الأداء • دوران الواجبات والمهام • عمليات المراجعة والتدقيق الأمني
الأدوات الفنية (البرمجية)	• البطاقات الذكية • مكافحات الفيروسات • اجراءات ضبط الوصول • التشفير	• نظم فحص التسلل • تتبع الوصول
الحماية المادية	• اختيار الموقع الفيزيائي • الوسائل الحيوية البيولوجية • مصدر الطاقة البديل	• كاشفات الحريق والدخان • صفارات الانذار والمتحسسات • دوائر الرقابة التلفزيونية

المصدر بتصرف: **(Tibton,2000)**

وتمنع الرقابة الوقائية مستخدمي نظم المعلومات من الاستخدام الحر للموارد الحاسوبية حيث تستخدم بالدرجة التي تتفق مع صلاحيات و حق الوصول المناط بالمستخدم، وتساعد برامج التوعية والتدريب في تعزيز الحماية الوقائية وتزيد من اعتمادية المستخدمين للنظم تحت مبدأ أن الحماية كفيلة بالثقة وقادرة على تحقيق الأمن .

وتوفر أنواع الحماية المختلفة (الادارية والمادية والبرمجية) ضوابط للرقابة تتنوع بين الضوابط الرادعة وضوابط التصحيح والمعالجة وضوابط الإستعادة وربما لا تصنف هذه الضوابط ضمن الرقابة الوقائية أو حتى الرقابة التفحصية فهي تتخلل أنشطة الحماية الادارية التنظمية، والحمايات البرمجية بل و الحماية المادية أيضاً **(Tipton,2000,P10-16)** .

المبحث السادس

الكليات التقنية في قطاع غزة

مقدمة:

ندرك جميعاً أن التعليم هو طريق تقدم الأمم والحضارات عبر العصور، وأنه لابد من الاهتمام به وتنميته وحسن إدارته للوصول للغايات المنشودة منه، ومهما كانت صور هذا التعليم فمن المتوقع أن يسهم في التنمية الاقتصادية المجتمعية الدائمة والتي تعود بالنفع المستمر والطويل الأمد على المجتمع بأسره .

فما من أمة في عصورها القديمة أو الحديثة تقدمت دون نهضة علمية مشهودة، ولنأخذ تجربة كوريا الجنوبية التي كانت ترزخ تحت العزلة والفقر والمجاعات وقلة الحيلة منذ وقت ليس بالبعيد، وما إن وضعت استراتيجية تعليم تقوم على أسس واضحة وبسيطة وتأخذ من البحث العلمي طريقها للابداع والتطوير حتى أصبحت هذه الفقيرة من كبرى ثريات العالم الاقتصادية في أقل من 35 عاماً، .

أن أهم ما أهتمت به كوريا الجنوبية هو التعليم التقني أو التعليم الفني الموجه نحو البحوث الصناعية والزراعية والتقنية البحتة، وكانت تدير هذه الطفرة التعليمية التطويرية بإضافات متتالية ومترابطة مع مجالات التعليم التقني المختلفة مستفيدة من تجارب الآخرين(قناة الجزيرة،2012).

بداية سيلقي الباحث الضوء على التعليم التقني ببيان جهة الاشراف عليه، وماهيته، وتعريفه، وأهدافه، وجوانبه، ومعوقاته، ثم سيضع تعريف للكليات التقنية، وتحديد مجتمع الدراسة المستهدف من الكليات وفق معايير محددة، ثم التوسع بمعرفة طبيعة نظم المعلومات والصورة الأمنية في كل كلية من الكليات مجتمع الدراسة وفق المقابلات التي أجريت معهم وسترتب الكليات حسب تاريخ المقابلة.

لمحة عن التعليم العالي في فلسطين :

نشأت مؤسسات التعليم العالي في ظل الاحتلال الإسرائيلي وبمبادرات محلية وطنية، ونمت وتطورت بسرعة حتى وصل عدد الجامعات على الأرض الفلسطينية عام 2011 (14) جامعة (2 حكومية، 3 خاصة، و 9 عامة) وعدد الكليات الجامعية (15)، والكليات المتوسطة (20)، وبذلك يبلغ عدد مؤسسات التعليم العالي في فلسطين (49) مؤسسة يعمل فيها حوالي (14600) موظف موزعين على كادر أكاديمي وإداري وخدماتي (21% منهم غير متفرغين).

وقد بلغ معدل الالتحاق بالتعليم العالي للفئة العمرية (18– 24) سنة حوالي 30 % (قاعدة بيانات التعليم العالي،2011).

وما يميز مؤسسات التعليم الفسطيني عن غيرها في الدول المجاورة هو وجود مفهوم الجامعة العامة الذي هو ليس حكوميا وليس خاصا، فهي لا تهدف إلى الربح وفي الوقت نفسه تتمتع باستقلالية في الإدارة والتعيين والتوظيف وتتحمل مسؤولية الرواتب والمصاريف التشغيلية الأخرى.

وفي عام 2002 دمجت وزارة التعليم العالي والبحث العلمي مع وزارة التربية والتعليم في وزارة واحدة،وأُعيد فصل وزارة التعليم العالي عن وزارة التربية والتعليم في عام 2012(وزارة التعليم العالي–رام الله،2012).

التعليم التقني في فلسطين :

أن التعليم التقني مثل التعليم الجامعي يعتبر جزء مهم من التعليم العالي ويجب التركيز على هذا النوع من التعليم ليحقق أهدافه في البنية التحتية للدولة الفلسطينية(أبوجراد،1994،ص77).

ويتميز التعليم التقني عن غيره من أنواع التعليم الأخرى بارتباطه المباشر والعضوي بالواقع الاقتصادي والاجتماعي للمجتمع من ناحية، وبالتطور التكنولوجي من ناحية أخرى، باعتباره مصدر إعداد القوى العاملة التي تقع عليها مسئولية تنفيذ وتشغيل وصيانة المشاريع الصناعية والزراعية والصحية والخدماتية (حمدان، 2005، ص13) .

مفهوم التعليم التقني :

يعرفه الاتحاد العربي للتعليم التقني (1979) بأنه ذلك التعليم الذي يهدف إلى إعداد أطر تقنية تقع بين الأخصائيين (الجامعيين) والعمال المهرة في هرم القوى العاملة، ومدة الدراسة فيه من سنتين إلى ثلاث سنوات بعد الثانوية العامة .

أما محمد (2002،ص23) فيرى أنه التعليم المتضمن إعداداً تربوياً وتوجيها سلوكياً، والمصمم لإعداد المهارات الوسطى من العمال التقنيين في الإدارة الوسطى في مؤسسات تعليمية بين سنتين وثلاث سنوات، بعد الدراسة الثانوية ودون مستوى الدراسة الجامعية، ويتضمن منهج التعليم التقني تعليما عاماً ودراسات مكونات هذا النهج تبعا لنوع العمالة والمستوى الذي تهيئه تلك المناهج ويصنف خريجو هذا التعليم في مستوى التقني أو الفني في هرم العمالة.

وبناء على ما سبق من تعريفات فإن التعليم التقني من وجهة نظر الباحث هو :

" التعليم الذي يوفر للطالب الحاصل على الثانوية العامة دراسة فنية تطبيقية تتصل مباشرة بسوق العمل ويحصل من خلالها الطالب بعد دراسته لمدة سنتين على الأقل على شهادة أكاديمية تؤهله للاندماج في سوق العمل، أو إكمال دراسته في الجامعات وفق سياساتها" .

معوقات نظام التعليم التقني في فلسطين:

بينت الدراسات والأبحاث التي أجريت حول نظام التعليم التقني في فلسطين وجود سلسلة من المعيقات والمشاكل التي يواجهها هذا النظام، ومن أهمها:

- صغر حجمه من ناحية العاملين في مؤسساته.
- المستوى الأكاديمي والتعليمي لمجموع الطلبة الذي يستقبلهم.
- تشرذم مؤسساته وتشتت الجهات المسئولة عن اتخاذ القرارات ورسم السياسات والتخطيط.
- ضعف مستوى ونوعية البرامج والخدمات التي توفرها مؤسساته.
- التمييز الطبقي والنوعي الذي يسيطر على كل فعاليات هذا النظام(أبو نحلة،1996).

أنواع التعليم التقني :

وذكر أبو عمر(2008) جانبين من التعليم التقني هما :

أ. التعليم التقني بأغلبيةٍ أكاديمية وهو التعليم الذي يركز على الجانب النظري أكثر منه على الجانب العملي و يمثل هذا النوع من التعليم في فلسطين التعليم الهندسي في الكليات و الجامعات المحلية بمستويي الدبلوم و البكالوريوس، و يؤهل هذا التعليم خريجوه للعمل المهني كخبراء و مشرفين ومصممين، ولا يتوقع أن يعملوا في المجال المهني و الحرفي المباشر كالصيانة مثلاً.

ب. التعليم التقني بأغلبيةٍ مهنية والذي يركز على الجانب العملي أكثر منه على الجانب النظري ويمثل هذا النوع من التعليم في فلسطين التعليم المهني في مراكز التدريب المهني و حديثاً التعليم المهني في المدارس الصناعية ضمن المسار التطبيقي، حيث يعمل خريجو هذا التعليم في سوق العمل في المجال الحرفي المباشر.

ويرى الباحث أن الغالب على الكليات التقنية هو النوع الأول الذي يغلب عليه الجانب النظري الأكاديمي مع التطبيق العملي، أما النوع الثاني فيقع في صلب اختصاص المراكز والمدارس المهنية، ومن ناحية أخرى فإن الدرجة العلمية التي تمنحها المعاهد أو المدارس المهنية لا تتساوى مع الدرجة التي تمنحها الكليات التقنية وذلك بالطبع يعود لكون الطالب عند دخوله الكلية

التقنية ملزم بأن يكون حاملاً لشهادة الثانوية العامة _ وهذا ليس من شروط الالتحاق بمؤسسات التعليم المهني _، وتنطبق عليه صفات طالب الجامعة في بعض التخصصات.

مؤسسات التعليم االتقني (الكليات التقنية):

حدد قانون التعليم العالي رقم 11 لسنة 1998 مؤسسات التعليم العالي في أربعة مستويات:

- الجامعات: لا يقل عدد الكليات أو الدورات عن ثلاثة وتمنح درجة البكالوريوس أو أعلى.
- الكليات الجامعية: توفر برامج أكاديمية وتقنية وفنية وتمنح درجة الدبلوم لسنتين أو ثلاثة وأحيانا تقدم درجة البكالوريوس.
- البولتكنيك: تمنح درجة الدبلوم أو البكالوريوس في الحقول الفنية والتقنية.
- كليات المجتمع: وتمنح البرامج الأكاديمية والفنية والتقنية ولا يقل مدة هذه البرامج عن سنة واحدة وتؤدي إلى درجة الدبلوم في هذه البرامج.

ويرى أبو جراد (1994، ص75) أن الكليات التقنية جزءاً من كليات المجتمع التابعة لوزارة التربية والتعليم العالي في فلسطين والتي أعتبرت مفهوماً جديداً للتعليم الجامعي المتوسط وقد دخل هذا المفهوم إلى فلسطين في بداية العقد السابع من القرن العشرين حيث تطورت دور ومعاهد المعلمين والمعلمات إلى كليات مجتمع، وكان الهدف من هذه الكليات تأهيل المعلمين والمعلمات للتدريس في مرحلة التعليم الأساسي وكان مستوى الدراسة فيها سنتين دراسيتين يدرس الطالب خلالهما مواد تدريسية محددة لجميع الكليات

وهنا يذكر الباحث أنه ووفقاً لما سبق وما جاء في الخطة الخمسية التطويرية الاستراتيجية (2008-2012) المنفذة، فإن الكليات التقنية تقع في ثلاثة أنواع محددة هي: (الكليات الجامعية، البولتكنيك، كليات المجتمع)، وعليه فإن الكليات التقنية هي اسم يجمع في طياته الكليات على اختلاف بنياتها شريطة أن تكون برامجها أو الجزء الغالب من برامجها تقني التوجه.

وتعرف الكليات التقنية بأنها: تلك الكليات التي هي نوع من أنواع كليات المجتمع، ومدة الدراسة فيها سنتان دراسيتان أو أكثر بعد الثانوية العامة وتشمل على واحد أو أكثر من البرامج التقنية المختلفة (تعليمات الدراسة في كليات المجتمع، 1997،ص6).

وبذلك يعرف الباحث إجرائياً الكليات التقنية بأنها : " الكليات التي تهتم بتعليم الطالب الجوانب الفنية والتطبيقية وتطرح برامجها سواء على مستوى الدبلوم أو البكالوريوس، بما يعزز من المهارات الفنية والخبرة التطبيقية لحقل العمل مقروناً باستيعاب السوق "

تحديد مجتمع الدراسة المستهدف:

حسب التعريف الذي تم تقديمه للكليات التقنية فأنه يوجد في قطاع غزة أكثر من (10) عشر كليات، وتقوم جهات متعددة بالاشراف على هذه الكليات منها الحكومية (وزارة التعليم العالي)، ووكالة الغوث الدولية، والعامة(الأهلية سابقا)، والخاصة .

وتشرف وزارة التربية والتعليم العالي من الجانب التربوي على هذه الكليات، وتعترف بالشهادات التي تمنحها، وبحكم تبعية الكليات الحكومية لوزارة التربية والتعليم العالي فإنها تعتبر الجهة المسئولة ايضاً عن التمويل والاشراف الاداري والمالي على الكليات الحكومية .

ولكن الكليات التي ستشملها الدراسة ستخضع لمعايرين أساسين هما:

- استقلالية مباني الكلية[10] .
- أن يكون مر على تأسيسها أكثر من سبع سنوات[11] .

والجدول رقم(3–9) يوضح إحصائية بعدد الكليات التقنية المختارة في قطاع غزة، وسنة التأسيس وموقعها، وجهة الإشراف عليها .

جدول رقم (3–9) : بيانات كليات الدراسة

م.	اسم الكلية	سنة التأسيس	موقعها	جهة الإشراف
.1	كلية تدريب غزة	1989	غزة	وكالة الغوث الدولية
.2	كلية العلوم والتكنولوجيا	1991	خانيونس	حكومية
.3	كلية فلسطين التقنية	1992	دير البلح	حكومية
.4	الكلية الجامعية للعلوم التطبيقية	1998	غزة	عامة
.5	الكلية العربية للعلوم التطبيقية	1999	رفح	خاصة

المصدر: مواقع الويب الخاصة بالكليات المذكورة

[10] حيث توجد بعض الكليات التي تخضع في سياساتها لسياسة الجامعات التي تعمل في كنفها مثل كلية الدراسات المتوسطة التي تخضع لجامعة الازهر وكلية مجتمع الأقصى التي تتبع جامعة الأقصى .

[11] حيث هناك بعض الكليات الناشئة والتي ليس لديها سنوات كافية من الخبرة في مجال نظم المعلومات .

الكليات التقنية مجتمع الدراسة في قطاع غزة :

سيستعرض الباحث هنا الحديث عن الكليات التقنية مجتمع الدراسة، ومراكز نظم المعلومات فيها و سيتناول قضايا أمن نظم المعلومات فيها وهي مرتبة حسب تاريخ المقابلة.

1. كلية فلسطين التقنية – دير البلح

نشأت الكلية عام 1992 م، بإمكانات متواضعة في تجهيزاتها وتخصصاتها إلا أن الحاجة إلى التعليم التقني والتدريب الفني ازدادت لأجل مواكبة هذا التطور الهائل في نظام الحياة والمجتمع الذي صاحبه نقص حاد في المهندسين والفنيين المتخصصين المؤهلين تقنياً . وبدت الحاجة إلى إيجاد كوادر ماهرة وقادرة على القيام بمهام المهندس المتخصص والفني في مختلف التخصصات، واستجابة لتلك العوامل برزت كلية فلسطين التقنية كمؤسسة تقنية تعليمية متخصصة رائدة تعمل عل دمج استخدام الحاسوب والتقنيات المتطورة في الحياة، وصقل العقلية العلمية المبدعة والمبتكرة لمواكبة التطورات العلمية المتسارعة . وتسعى كلية فلسطين التقنية– دير البلح لتطوير وتعزيز مكانتها في خدمة وتنمية المجتمع المحلي.

وتطويراً للسياسات التعليمية فإن الكلية عملت على رفع جودة العملية التعليمية، والتحسين، والتطوير المستمر في مختلف التخصصات التقنية فيها، وأدخلت نظام التعليم الالكتروني كأحد الأنظمة المساندة للدراسة من أجل تطوير تكنولوجيا التعليم بالكلية .

وقد ساهمت النقلة النوعية الملموسة في كافة مناحي العمل في الكلية في بناء شراكات محلية ودولية لدعم التوجه الاستراتيجي في التطوير، وتبادل الخبرات والمنفعة بما يخدم العملية التعليمية في الكلية (دليل كلية فلسطين التقنية، 2012/2011).

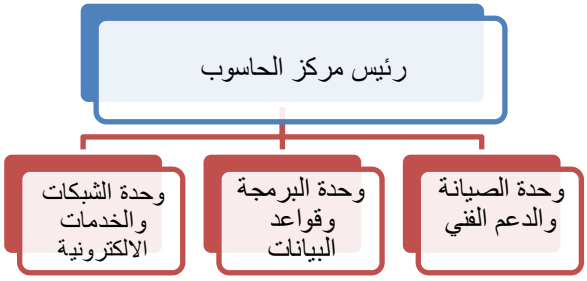
- *مركز الحاسوب / كلية فلسطين التقنية*

تأسس مركز الحاسوب في كلية فلسطين التقنية– دير البلح سنة 2006 تحت مسمى وحدة الحاسوب بهدف إدارة تكنولوجيا المعلومات والإشراف على تطوير التجهيزات المحوسبة في الكلية، وقبل ذلك كان قسم الحاسوب بالاشتراك مع لجان تشكلها إدارة الكلية وبالتنسيق مع قسم التخطيط والتطوير هم من يقومون بعمل وحدة الحاسوب حتى تأسيس مركز الحاسوب . ثم أنتقل القسم إلى مرحلة جديدة ليحصل على اسم مركز الحاسوب بحلول عام 2007، حيث أنيطت له العديد من المهام الأساسية وتشكلت داخله العديد من الوحدات ويبين الشكل رقم (3–20) المخطط التنظيمي لقسم الحاسوب، و حالياً يوجد بالمركز ثلاث وحدات وهي :

- وحدة الشبكات والخدمات الالكترونية.

- وحدة الصيانة والدعم الفني .
- وحدة البرمجة وقواعد البيانات.

شكل رقم (3-20):المخطط التنظيمي لمركز الحاسوب – كلية فلسطين التقنية



المصدر: (مقابلة م.مروان ابو شغيبة،11-11-2012)

ويعمل في مركز الحاسوب (5)خمسة موظفين، وهناك عدداً من اللجان والفرق التي تشارك من خارج مركز الحاسوب .

ومنذ عام 2008 يقوم مركز الحاسوب بحوسبة نظم المعلومات الخاصة بأعمال الأقسام الإدارية المختلفة، ويشرف على جميع خدمات نظم المعلومات المقدمة للموظفين والطلاب، ويدير موقع الانترنت الخاص بالكلية ويشرف على الدورات التدريبية المتعلقة بتطوير نظم المعلومات، وسبق أن أعد حقيبة تدريبية شاملة لتطوير وحوسبة نظم المعلومات في الكلية، شملت العديد من الفرق التي شاركت في وضع اللبنات الأولى لتحليل نظم المعلومات في الأقسام المختلفة، ويعد القسم كل بداية عام دراسي خطة تشغيلية تؤهله لوضع تصوراته حول العام المقبل ومتطلبات الكلية من احتياجات تكنولوجيا المعلومات، كما أن خططاً استراتيجية معدة قد ناقشت عقد ورشات عمل عدة باخصائيين من خارج الكلية لطرح سياسة لأمن المعلومات يتم إعلانها ولكن ظروف حالت دون ذلك، لعل أهمها قلة التمويل (مقابلة مع م./مروان أبو شغيبة،11-11-2012).

ورداً على سؤال الباحث حول وجود موظف متخصص في قضايا أمن المعلومات، تبين عدم وجوده كوظيفة بينما يمكن الحديث عن وجود ممارسة لأمن نظم المعلومات .

- *رؤية كلية فلسطين التقنية – دير البلح تجاه أمن نظم المعلومات*

في مقابلة م./مروان أبو شغيبة(2012) رئيس مركز الحاسوب، ذكر أن أهم ما يميز نظم المعلومات والبرامج التي تقوم الكلية بتطويرها أنها تركز على أن تكون مقدمة عبر الشبكة المحلية فلا هي برامج مثبتة في محطات العمل ولا هي برامج ويب .Web App،

وهي تقع في الوسط للإستفادة من مزايا كلا الطرفين وتجنب عيوب النوعين المذكورين أيضاً، و رأى في ذلك جودة أفضل وكفاءة وفاعلية .

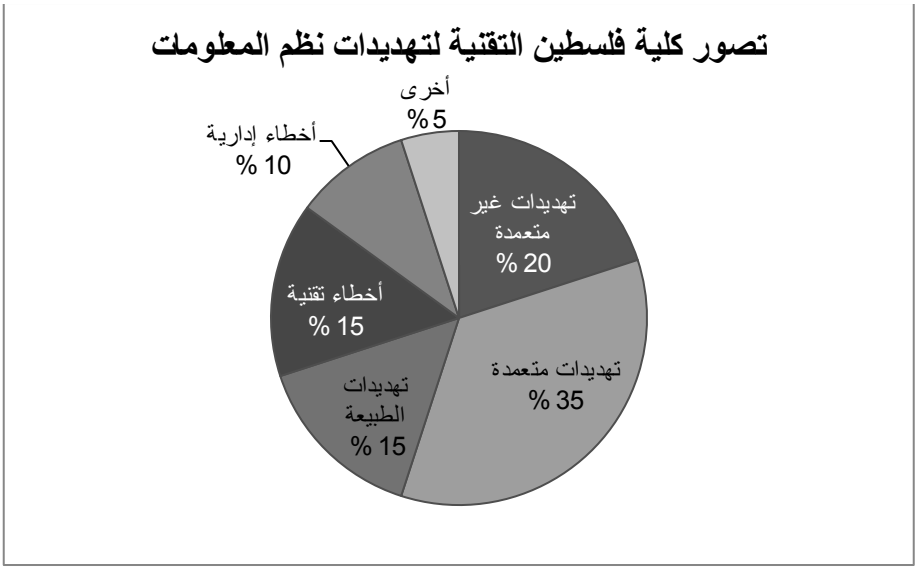
وذكر أن أهمية تحقيق أمن المعلومات هو ضمان لاستمرارية العمل، وأعتقد أن ما يهم الكلية في قضايا أمن المعلومات هو الحفاظ على سلامة المعلومات من التغيير وإبقاء وتوفر هذه المعلومات وسرعة توفيرها لمن يطلبها عبر نظام المعلومات، حيث رأى أن جانب السرية هو أمر محكوم بالزمن، وقد تفقد البيانات سريتها مع مرور الوقت، بينما اعتبر أنه لا حياد عن سلامة المعلومات .

أما عن حصر التهديدات، فبين أن التهديدات قائمة بكافة أنواعها ولو بنسب متفاوتة، وذكر أن الكلية تواجه تهديدات تقع في خانة التهديدات المتعمدة (كمخاوف قصف الاحتلال،الاختراقات)،أو التهديدات غير المتعمدة (كالحرائق، سوء الاستخدام، انقطاع الكهرباء المتكرر)،أو التهديدات الطبيعية (كحدوث زلازل، ارتفاع شديد في درجات الحرارة)، أو التهديدات التي تقع في حيز أخطاء تقنية، أو أخطاء إدارية

وفي جانب هام أعتبر سوء الاستخدام من قبل الموظف ليس مبعثاً للخطر مع علمه الأكيد بأنه أحد المخاطر التي تعرض النظام لفقدان فاعليته، وهدفه من ذلك هو تعزيز المسئولية لدى الموظف، وعدم تحميله ما يمكن أن يجعله ينأى جانباً عن استخدام نظام المعلومات .

ويرى أن توزيع التهديدات نسباً لمخاطرها هي كما المخطط في شكل رقم (3-21).

شكل رقم (3-21) : وجهة نظر كلية فلسطين التقنية لتهديدات نظم المعلومات



المصدر: (مقابلة م.مروان ابو شغيبة، 11-11-2012)

2. الكلية العربية للعلوم التطبيقية ــ رفح

تأسست الكلية العربية للعلوم التطبيقية في محافظة رفح سنة 1999م بترخيص واعتماد من وزارة التربية والتعليم العالي منبثقة عن المعهد العربي الثقافي الذي تأسس سنة 1995 بترخيص واعتماد وزارة الإعلام والذي تخصص في الدراسات الإعلامية، وتمنح الكلية خريجيها درجة الدبلوم المتوسط والبكالوريوس في بعض التخصصات المتميزة حيث تعتمد نظام الساعات المعتمدة موزعة علي فصول دراسية، ومن أهم أهداف وفلسفة الكلية هي المساهمة في دعم المجتمع المحلي بالخبرات المؤهلة والمدربة مهنيا وتقنيا وأكاديمياوتمكين الطالب بالاحتكاك بسوق العمل من خلال التدريب الميداني في المؤسسات المحلية مما يسهل عليه إمكانية الحصول علي فرصة عمل بعد تخرجه(موقع الكلية العربية للعلوم التطبيقية،2012).

- *مركز الحاسوب / الكلية العربية للعلوم التطبيقية*

لا يوجد في الكلية العربية للعلوم التطبيقية مركزاً أو قسماً متخصصاً بإدارة نظم المعلومات وعوضاً عن ذلك تستفيد الكلية من طرف خارجي بالحصول على خدمات وتطبيقات نظم المعلومات فيما يتعلق بتنفيذ الأعمال الإدارية المختلفة، وترى الكلية في ذلك تقليلاً للتكاليف و سرعة في تنفيذ العمل و تسعى الكلية في خطتها الاستراتيجية لإنشاء مركزاً لنظم المعلومات ولكنها تستبعد الاستغناء عن خدمات(التعهيد) الأطراف الخارجية (مقابلة مع أ. أحمد عواجة، 5-1-2013)

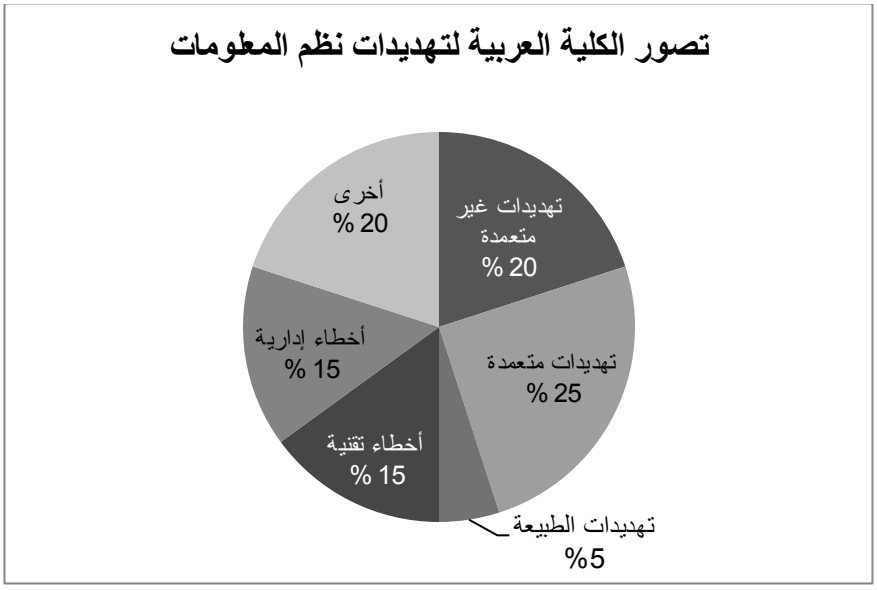
- *رؤية الكلية العربية تجاه أمن نظم المعلومات*

ترى إدارة الكلية أن أمن نظم المعلومات من المواضيع الحساسة وبالغة التعقيد والذي يحتاج الى تطوير دائم و تكاليف كبيرة، وربما هذا يبرر لها ما أقدمت عليه من تعاقد مع أحدى شركات البرمجة وتطوير النظم.

وتسعى الكلية دوماً للحفاظ على أمن معلوماتها، ودراسة البدائل الأقل تكلفة والأكثر فعالية لإدارة نظم معلوماتها، وقد قامت الكلية بتكليف أحد مهندسي نظم المعلومات العاملين في الكلية بمتابعة المشاكل التي تواجه نظم المعلومات التي تقدمها الشركة المتعاقدة والتنسيق معهم لحلها وتقوم الشركة بذلك بما لا يعطل الأعمال المختلفة.

وفيما يخص دراسة التهديدات التي تواجه نظم المعلومات فإدارة الكلية قد حددت نسب الخطورة تجاه المهددات المختلفة كما في الشكل التالي رقم (3-22) .

شكل رقم (3-22): وجهة نظر الكلية العربية لتهديدات نظم المعلومات



المصدر: (مقابلة أ.أحمد عواجة،5-1-2013)

ويرى الباحث أنه تبين عدم وجود متخصص في أمن نظم المعلومات يمارس عمله ضمن نظام المعلومات، وذلك لعدم وجود مركز للحاسوب / نظم المعلومات .

ولا تتخوف الكلية من التهديدات التي تستهدف الكيانات المادية للبنى التحتية لتكنولجيا المعلومات، تبريراً منها بأن برامج ونظم المعلومات تعمل على الويب، ولا يمكن أن يلحق الضرر بالمعلومات التي تخص بيانات الكلية في حال حدث ذلك، حيث أن آليات النسخ الاحتياطي تعمل بشكل آلي لخفظ ما يودع في قواعد البيانات كل ربع ساعة.

3. كلية مجتمع تدريب غزة –الوكالة

في العام 1953 تم تأسيس كلية مجتمع / تدريب غزة تحت اسم "مركز التدريب المهني" تجسيدا لفلسفة وكالة الغوث الدولية لإغاثة اللاجئين الفلسطينيين، حيث هدفت لإعداد خريجين مؤهلين للحصول على فرص عمل تمكنهم من العيش الكريم، وعليه فقد تبلورت رسالة الكلية في إعداد وتنفيذ برامج تقنية و مهنية متنوعة ومتخصصة تلبي حاجات السوق المحلي والإقليمي، وتزويد أبناء اللاجئين الفلسطينيين بالمعارف والمهارات والقيم والاتجاهات المرغوب فيها للحصول على فرص عمل أفضل.

وأخذت الكلية بالتطور إلى أن وصل عدد التخصصات المهنية فيها حالياً إلى أربعة عشر تخصصاً، وبلغ عدد التخصصات الفنية إلى سبعة عشر، وإجمالي قدرتها الاستيعابية يزيد عن ألف طالب وطالبة، وتتبع الكلية من حيث الإشراف والتمويل لوكالة الغوث الدولية لتشغيل اللاجئين الفلسطينيين وذلك من خلال دائرة التربية والتعليم بغزة وقسم التعليم التقني والمهني بمقر

رئاسة الوكالة بعمان، وتم اعتماد كلية تدريب غزة ككلية مجتمع متوسطة من وزارة التربية والتعليم العالي والبحث العلمي في فلسطين وذلك على مستوى الأقسام التقنية بالكلية في العام 1995م(موقع كلية تدريب غزة،2013).

- *مركز الحاسوب*– كلية مجتمع تدريب غزة

لا يوجد في كلية مجتمع تدريب غزة جهة مختصة بشكل مباشر بإدارة نظم المعلومات حيث يتبع ما وجد من نظم للمعلومات لقسم التعليم التقني والمهني بمقر رئاسة الوكالة بعمان، ومع ذلك وبجهد شخصي غير مكلف بشكل رسمي قام م.زكريا بتطوير موقع ويب يخدم الطالب، والمعلم، ورئيس القسم ويتيح الموقع الكثير من الخدمات والميزات التي ربما لا تتوافر في النظم القائمة (مقابلة مع م. زكريا أبو سلمية،6-1-2013)

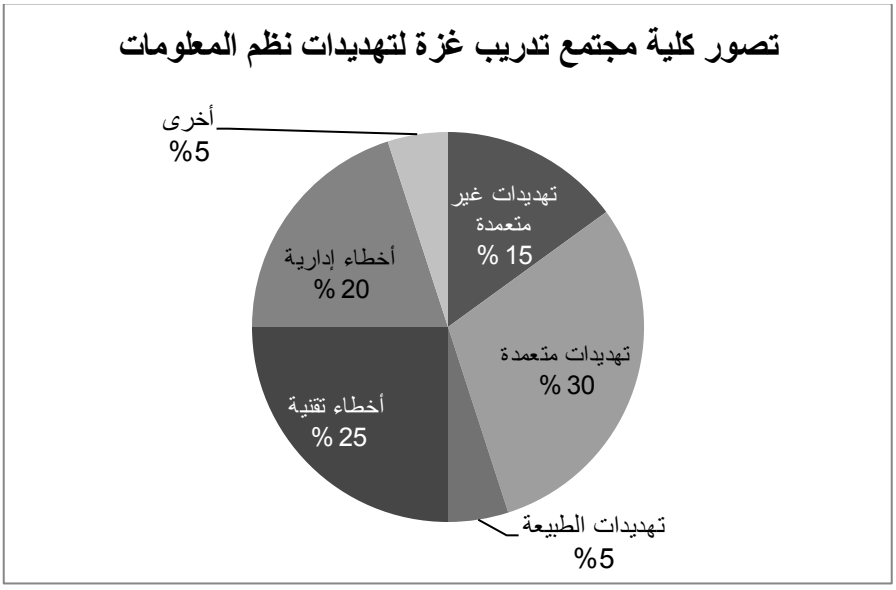
- *رؤية كلية تدريب غزة تجاه أمن نظم المعلومات*

لأن الكلية تتبع الأونروا – وكالة الغوث التي عرف عنها المركزية في إدارة أعمالها فإن أمور نظم المعلومات بكافة جوانبها لا تتيح للكلية الكثير من المرونة، فعلى صعيد تخصيص قسم يهتم بنظم المعلومات، لا يمكن للكلية إتخاذ قرارات بهذا الشأن دون موافقة من إدارتها المركزية، ومع ذلك وفي ظل هذه السياسة، فإن الكلية تطمح وتعمل على إدارة نظم معلوماتها بما يتيح لها تيسير أعمالها الإدارية والأكاديمية في محيط من الأمن والحفاظ على توفير المعلومة للطالب و للمعلم، وربما أحد أهم ما يميز مكونات نظم المعلومات القائمة أنها لا تشتمل إلا على تطبيقات وبرامج مرخصة، ولا يمكن تشغيل أي من البرمجيات على الأجهزة دون ترخيص، وهذا بحد ذاته يعتبر نمطاً سائداً قد يفسر وجود شبه ممارسة لمحتويات سياسة أمن للمعلومات وحتى أن لم يصرح بذلك القائمون على نظم المعلومات الحالية التي ربما لا تلاقي استحساناً عند البعض.

ويقول المعنيون والعاملون على نظم المعلومات بأنهم يراعون بشدة المسألة الأمنية، ويخشون من مخاطر فقدان المعلومات ولذلك فهم يجدون في النسخ الاحتياطية سبيلاً في طريق حماية قواعد البيانات .

وفيما يخص دراسة التهديدات التي تواجه نظم المعلومات فإدارة الكلية قد حددت نسب الخطورة تجاه المهددات المختلفة كما في المخطط شكل رقم (3-23) .

شكل رقم (3-23) : يبين وجهة نظر كلية تدريب غزة /الوكالة لتهديدات نظم المعلومات



المصدر: (مقابلة م.زكريا أبو سلمية،6-1-2013)

وعن سؤالنا حول وجود متخصص في أمن نظم المعلومات يمارس عمله ضمن نظام المعلومات تبين عدم وجوده وذلك لأنه لا يوجد مركزاً لنظم المعلومات أصلاً.

وعن الحماية في شقها المادي فالكلية بحكم تبعيتها لوكالة الغوث الدولية فهي تنتهج نظاماً أمنياً مادياً صارماً، حيث يحظر دخول الكلية لغير الطلاب والمعلمين إلا بإذن ويتطلب ذلك تسليم البطاقة الشخصية وتسجيل بيانات، ويتلقى الشخص بطاقة دخول خاصة لمدة معينة، وربما لا يتواجد هذا في كل الكليات السابقة، مع العلم أن باقي الكليات فيها أمن مادي ولكن في أغلب الأحيان هو شكلي أو أخف من الناحية التنفيذية .

4. الكلية الجامعية للعلوم التطبيقية

الكلية الجامعية للعلوم التطبيقية تعتبر من أكبر الكليات التقنية في فلسطين، أُنشئت بقرار من وزارة التعليم العالي في عام (1998)، تحت مسّمى (كلية مجتمع العلوم المهنية والتطبيقية)، وكان الهدف الرئيسي للكلية هو توفير خدمة التعليم التقني والمهني للمجتمع الفلسطيني خلال ستة وثلاثين اختصاصاً في كافة المجالات، وذلك للمساهمة في إتاحة تخصّصات جديدة، ومُلحة لحاجات سوق العمل، وتطورت النشأة لتصبح عام (2007) من كلية تمنح شهادة الدبلوم المتوسط، إلى كلية جامعية تمنح درجتي البكالوريوس لنحو (7) تخصّصات في مختلف المجالات، وتوفر الكلية الجامعية كادراً إدارياً مؤهلاً في مختلف الوحدات والأقسام بلغ عددهم (250) موظفاً وموظفة .

وفي عام (2009) استحدثت الكلية برامج التطوير حسب الخطّة المرسومة في تحسين مخرجات جودة التعليم، وتعزيز ملاءَمتها وفقاً لاحتياجات المجتمع المحلي والإقليمي فأنشأت الكلية الجامعية مركز لخدمة المجتمع اشتمل المركز على عدة مرافق مهمة خلال تنفيذها برامج التأهيل والتدريب كمركز التعليم المستمر، وعيادة اضطرابات التخاطب، ووحدة العمل عن بُعد، ووحدة الرسوم المتحركة، وحاضنات الأعمال والمشاريع الصغيرة، واستمرار لبرنامج التطور في الكلية أوجدت الضرورة لتحسين الظروف اللوجستية لطلاب الجنوب وذلك خلال افتتاح فرع الكلية الجامعية للعلوم التطبيقية في خانيونس عام (2009)، ولازال العمل على تطوير برامج الدبلوم والبكالوريوس تعزيزاً للاختصاصات والبرامج وفق المعايير والمتطلبات العالمية التي تحقّق وتلبّي احتياجات المجتمع المحلّي والإقليمي(موقع ويب الكلية الجامعية للعلوم التطبيقية،2013) .

- *مركز الحاسوب – الكلية الجامعية للعلوم التطبيقية*

تعتبره الكلية بمثابة العمود الفقري، ويضم المركز ثلاث وحدات أساسية ضمن مخططه التنظيمي كما تظهر في المخطط في شكل رقم (3-24) و هي:

1- وحدة الصيانة والدعم الفني

تهتم الوحدة بمتابعة وحل المشكلات المتعلقة بأجهزة الحاسوب في الكلية التي يزيد عددها عن 1450 جهاز ما بين أجهزة مختبرات وأجهزة موظفين سواء عن طريق توجيهها إلى ورشة الصيانة الخاصة بالمركز أو عن طريق أسلوب الدعم الفني عن بعد، والذي اعتمده مركز الحاسوب حفاظاً للوقت والطاقة وانجازاً للمهام بشكل متطور .

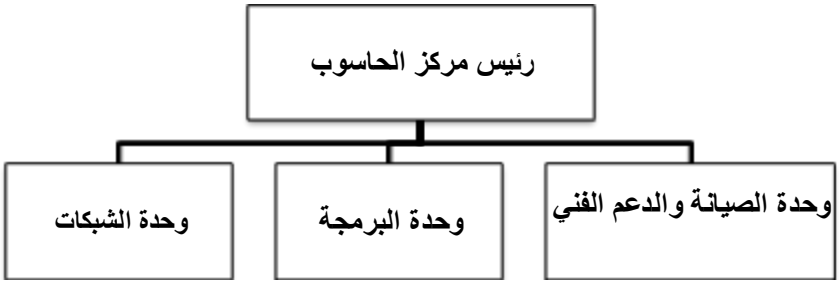
2- وحدة الشبكات :

ومن مسؤوليات الوحدة إدارة حسابات الموظفين والبريد الإلكتروني، وإدارة حسابات الدخول إلى الشبكة وتوصيل أجهزة الحاسوب في الكلية من خلال شبكة مترابطة، وإدارة حسابات البريد الخاصة بالطلاب وتسخير كافة الإمكانيات لتحسين الأداء .

3- وحدة البرمجة :

وهم مسئولون عن تطوير وإنشاء قواعد البيانات الخاصة بالكلية وإعطاء الصلاحيات لكل موظف حسب مجال عمله وأرشفة القضايا وحوسبتها إلكترونياً، وإدارة موقع الكلية وتطويره، وتنفيذ العديد من البرامج التطبيقية وتطوير أنظمة الامتحانات المحوسبة .

شكل رقم (3-24):المخطط التنظيمي لمركز الحاسوب – الكلية الجامعية



المصدر : (مقابلة أ.محمد المدهون،8-1- 2013)

ويزيد عدد الموظفين الاداريين في المركز عن خمسة عشر(15) موظفاً، ويوجد بينهم متخصصون في أمن نظم المعلومات، كما يوجد مدققون في تطوير النظم.

ويرى الباحث أن هذا العدد من العاملين في مركز الحاسوب في الكلية الجامعية للعلوم التطبيقية يعتبر العدد الأكبر بين الكليات التقنية جميعاً، وهذا يميز الكلية الجامعية عن غيرها من الكليات الأخرى.

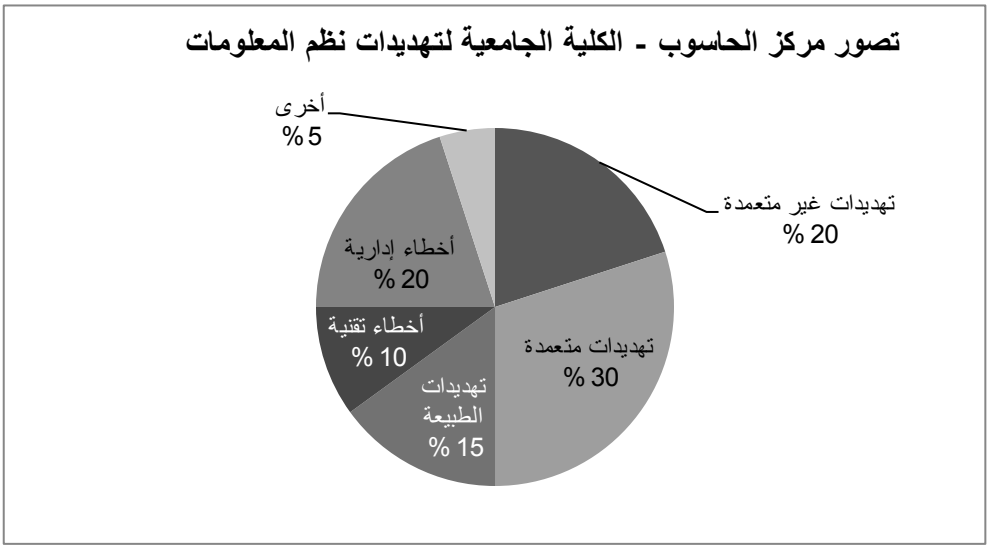
- *رؤية الكلية الجامعية حول أمن نظم المعلومات*

تنطلق الكلية الجامعية في عملها من خلال إستراتيجيات واضحة تنفذ ضمن مخطط زمني على جميع الصعد الإدارية بما فيها أعمال تطوير نظم المعلومات التي يقوم بها مركز الحاسوب؛ وتتوافر لديهم الخبرات في ذلك، ولقد كانت الكلية هي المقر الوحيد الذي كان قادراً على استقبال اختبارات التوظيف الالكترونية بالتنسيق مع ديوان الموظفين، وهذا ينم عن قناعة المجتمع المحلي ودوائر القرار والحكومة بقدرات الكلية الجامعية ومستوى ما تمتلكه من مؤهلات في مجال تقنيات المعلومات و التعليم الالكتروني (مقابلة أ.سامر ياغي، 8-1-2013)

ويرى المدهون (2013) أن جودة البرامج والنظم التي تطورها الكلية الجامعية من حيث مستوى الأمن فيها و سهولتها و مرونتها و الخدمات الواسعة التي تقدمها باتت تتحسن باستمرار.

ورداً على سؤالي في مقابلة مع المدهون(2013) حول التهديدات التي تواجه نظم المعلومات وتوزيعها نسبياً على الأنواع التي ذكرتها ظهرت الاجابة كما في الشكل رقم (3-25).

شكل رقم (3-25) :يبين وجهة نظر الكلية الجامعية تجاه تهديدات نظم المعلومات



المصدر: (مقابلة محمد المدهون،8-1-2013)

وفي ظل المساءلة القانونية والتخوفات الأمنية ومسايرة المقاييس والمعايير الدولية فقد مضت الكلية الجامعية بالإلتزام باستخدام برمجيات ونظم تشغيل أصلية ومرخصة بعيداً عن البرمجيات المزيفة الغير مرخصة والتي توجد فيها الكثير من التهديدات لأمن نظم المعلومات.

ولعل ما يميز الكلية الجامعية عن غيرها من الكليات التقنية محل الدراسة بل الكليات الفلسطينية بشكل عام المستوى الكبير من استخدام تقنية المعلومات في أعمالها، وهذا بدوره يلزم الكلية الجامعية بانتهاج سياسة أمنية للمعلومات وإن لم تكن مكتوبة وهذا ما يلاحظ في ثقافة العاملين وتعاملات الكلية الجامعية مع المجتمع المحلي وخصوصاً فيما يتعلق بقضايا أمن المعلومات ؛ وقد يرجع أحد أهم الأسباب وراء هذا النمو التقني والمعلوماتي الذي تعيشه الكلية الجامعية إلى سياسات الإدارات العليا وما توليه من التفويض والمبادرة للقائمين على بناء نظم المعلومات.

5. كلية العلوم والتكنولوجيا – خانيونس

أُنشِئَت كلية العلوم والتكنولوجيا– بخانيونس عام 1990م كمؤسسةٍ أهلية، تُعنى بتدريس العلوم التقنية، وقد تولي مجلس التعليم العالي بالقدس الإشراف عليها عام 1994م، ثم تولت وزارة التربية والتعليم العالي الإشراف عليها، وأصبحت الكلية مؤسسة حكومية عام 1997.
وتمنح الكلية خريجيها درجتي البكالوريوس والدبلوم المتوسط في أربعةٍ وعشرينَ تخصصاً علمياً تقنياً ضمن برنامج دراسي متميز (موقع ويب – كلية العلوم والتكنولوجيا،2013).

- *مركز الحاسوب – كلية العلوم والتكنولوجيا*

قسم مركز الحاسوب هو قسم تم استحداثه ضمن هيكلية الكلية في العام 2008 وذلك بعد أن لمست إدارة الكلية الحاجة الماسة لحوسبة جميع العمليات الإدارية و الأكاديمية داخل الكلية، حيث يُناط بهذا المركز العمل على إدارة جميع البرامج المحوسبة داخل الكلية وإدارة الشبكات وأجهزة الحاسوب وإدارة عملية التعليم الإلكتروني بالكلية، كما يناط به متابعة موقع الكلية الإلكتروني وتطويره بما يلائم التطورات الحديثة في العالم ويلائم احتياجات الموظفين والطلاب.

ويتألف مركز الحاسوب من ثلاث وحدات يشرف عليها رئيس مركز الحاسوب بشكل مباشر وهذه الوحدات سيتم ذكرها كما في المخطط التنظيمي للقسم وفق الشكل رقم (3–26)، ويعمل في المركز اربعة (4) موظفين من المتخصصين .

شكل رقم (3–26) – المخطط التنظيمي لمركز الحاسوب – كلية العلوم والتكنولوجيا

المصدر : (مقابلة م.أحمد الفرا، 14–1– 2013)

وقد رأى رئيس المركز أن هذا العدد من الموظفين غير كافٍ وهو بحاجة الى المزيد من الموظفين ذوي الخبرات في مجال نظم المعلومات وخصوصاً التطبيقات التي تعمل في بيئة الجامعات والكليات التقنية، وبالتالي فإن حجم الأعباء المتراكمة على المركز تزداد باضطراد وهذا لا يتناسب مع الهيكلية القائمة بالمركز، وربما هذا ما أنعكس على قرار الكلية ومركز المعلومات بتعهيد بعض نظم المعلومات في شقها البرمجي، حيث قامت الكلية بتعهيد (برامج القبول والتسجيل، وشئون الطلبة، والشئون الأكاديمية، والمكتبة) لطرف خارجي مقابل مبالغ مالية يعتبرها مدير المركز كبيرة .

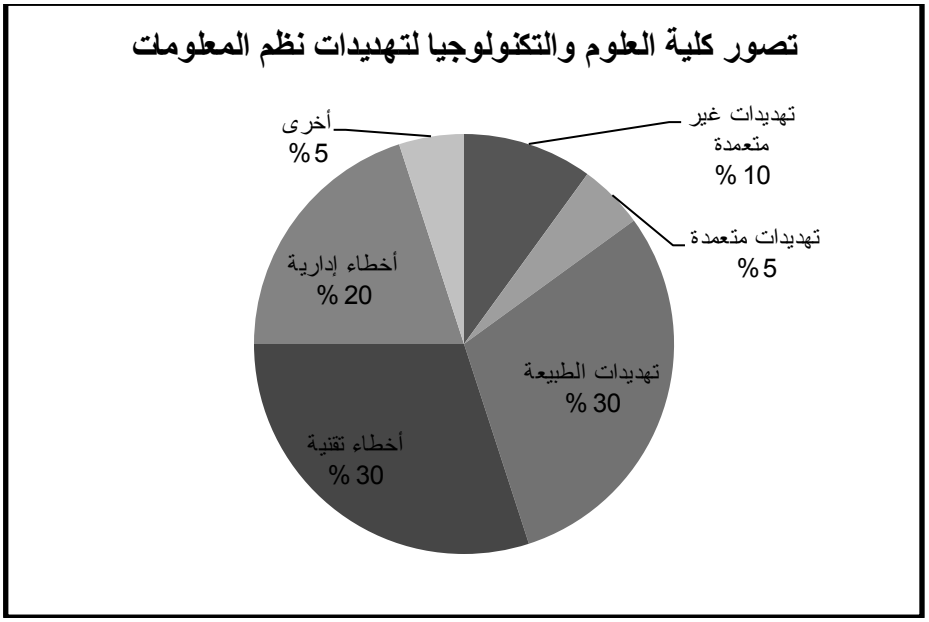
- *رؤية كلية العلوم والتكنولوجيا حول أمن نظم المعلومات*

تدرك الكلية أهمية أمن نظم المعلومات ولكنها في نفس الوقت توازي الاحتياجات السريعة لأداء وظائف نظم المعلومات لتغطية الأعمال الروتينية اليومية، وفي ظل التبعية

الحكومية عبر وزارة التربية والتعليم العالي ربما تعجز الكلية عن تنفيذ ما تطمح له بشكل كامل وتكتفي الوزارة بتغطية جزءاً يسيراً مما تحتاجه الكلية من المتخصصين لذلك لا يتوافر في الكلية متخصصين في أمن نظم المعلومات، أو في تدقيق أمن المعلومات.

وعقب سؤالي عن نقاط الضعف في نظم المعلومات و ماهية التهديدات التي من الممكن أن تستغل هذه النقاط والوهن في النظم، وتوزيعها بنسب حدوثها تبين أن وجهة نظر الكلية تجاه التهديدات كانت على النحو التالي كما في الشكل رقم (3-27)، وقد تبين أن تهديداً داخلياً يتمثل في كون العاملين في المركز أغلبهم من الموظفين الغير مثبتين والذين من الممكن أن تنتهي فترة التعاقد معهم دون إحراز ترتيبات أمنية خاصة بإنهاء الخدمة .

شكل رقم (3-27) :يبين وجهة نظر كلية العلوم والتكنولوجيا لتهديدات نظم المعلومات



المصدر: (مقابلة أحمد الفرا،14-1-2013)

وينظر الى الموقع الفيزيائي لقسم مركز الحاسوب على أنه مكاناً غير مناسب، وذلك لصعوبة التنقل بين غرفة الخوادم والمركز، ويتولد عن ذلك صعوبة إدارة عمليات الدعم الفني السريع، وكذلك توفير الحماية المادية، ويصعب على إدارة قسم مركز الحاسوب إنجاز الكثير من وسائل الحماية البرمجية لقلة الكفاءات.

ويوجد في الكلية حديثاً سياسة مكتوبة لأمن المعلومات ولكنها غير معلنة ولا يعلم فيها الموظفين بشكل عام، ولا حتى العاملين على نظم المعلومات، وقد تبين الباحث أن السياسة مقترحة حديثاً من قبل وزارة الاتصالات وتكنولوجيا المعلومات، ولم تسعى الكلية بعد إلى تخصيصها بما يتلائم بشكل مباشر مع البيئة المستهدفة و ظروفها الخاصة .

تعليق الباحث على المقابلات:

بعد زياراتي التي قمت من خلالها بمقابلة رؤساء أقسام مراكز الحاسوب القائمين بالمسئولية تجاه نظم المعلومات في الكليات التقنية الخمسة:(كلية فلسطين التقنية، كلية العلوم والتكنولوجيا، الكلية الجامعية للعلوم التطبيقية،الكلية العربية للعلوم التطبيقية، كلية تدريب غزة) تبين لي التوجه العام لدى الكليات بحرصها على تنفيذ أعمالها الإدارية اليومية والروتينية بشكل محوسب عبر نظم المعلومات المحوسبة، وبذلك فجميع الكليات وإن أختلفت الوسائل والطرق لاقتناء برامج نظم المعلومات تقوم بهذا العمل .

فبينما وجدت في الكليات التي تشرف عليها الحكومة متمثلة في وزارة التربية والتعليم العالي بشكل مباشر مثل: (كلية العلوم والتكنولوجيا، كلية فلسطين التقنية) توافر مركز للحاسوب في الكليات، وعدم الاكتفاء بما يقدمه مركز الحاسوب الحكومي من خدمات تكنولوجيا المعلومات إن وجدت أحياناً كما اعتاد على تقديمها لبعض الوزارات .

وربما أكتفى مركز الحاسوب الحكومي التابع لوزارة الإتصالات وتكنولوجيا المعلومات بتقديم سياسة أمن للمعلومات كما حدث مع كلية العلوم والتكنولوجيا –خانيونس، وبذلك فإن الكليات تتوجه نحو التخصيص الذاتي في مجال تطوير برامجها .

وإن كانت كلية العلوم والتكنولوجيا قد بادرت بتعهيد بعض من نظم معلوماتها، وفق مبررات لها علاقة مباشرة بصعوبة توظيف كادر برمجي يكون قادر على تطوير نظم تناسب أعمال الكلية، نظراً لأن توظيف موظف حكومي جديد مسألة تحتاج الى وقت وتسويات مالية قد ترجأ تنفيذها الى وقت، وربما أن الوقت ليس في صالح الكلية وبذلك فهي وقعت وهي مرغمة على تعهيد بعض نظم معلوماتها .

بينما في حالة الكلية العربية التي تتبع الإشراف الخاص، فإنها تعتبر التعهيد مسألة مهمة للغاية لتخفيض التكاليف وهي إن تقوم به، فهذه العملية قد جاءت بعد دراسة متأنية وربما تكون من وجهة نظر الباحث هذه الحالة السائدة لدى أغلب الكليات التي تتبع الإشراف الخاص لأنها قليلة التكاليف، حيث ترى في إنشاء مركز حاسوب واستقطاب وتوظيف متخصصي أمن نظم المعلومات هي تكاليف مستمرة وباهظة وربما تكون التكاليف ليست بالقدر الذي تستطيع تلك الكليات الخاصة استيعابه .

ولعل الكلية الجامعية التي تقع تحت إشراف عام إنموذجاً في العمل الإداري المنسق تجاه تطوير نظم المعلومات والعناية بأمن المعلومات حيث تنطلق عبر استراتيجيات موضوعة وفق برامج تنفيذية وتدقيق مستمر وبذلك فالجامعية تسترشد من واقع تحليل أنظمتها و بيئة ترغب بتطويرها

إلى حال أفضل وتتيح الهيكلية التنظيمية الواسعة لقسم الحاسوب الذي يشرف على إدارة نظم المعلومات بلوغ أهدافها.

ورغم أن كلية فلسطين التقنية التي يضم مركز نظم معلوماتها العدد الأقل من الموظفين مقارنة بالكليات الأخرى التي تتوافر فيها مراكز حاسوب، ومع ذلك فإنها تسعى لتطوير نظم معلوماتها ذاتياً بما لديها من إمكانات متواضعة وأقتربت من إنجاز نظم معلومات شاملة متكاملة لجميع أنشطة الكلية الإدارية والأكاديمية، حيث أستفاد مركز الحاسوب في ذلك من تمويل بعض الجهات الخارجية لمشاريع تطوير البنى التحتية في السنوات السابقة ولا تزال الكلية ترى في مسائل التعهيد والإستعانة بالمصادر الخارجية قضية مهددة لأمن المعلومات بشكل كبير.

وفيما يخص كلية تدريب غزة فإنها الحالة الأكثر تساؤلاً من قبل العاملين في الكلية نفسها، حيث يشكو العاملين من عدم وجود مركزاً للحاسوب يتابع ويدير نظم المعلومات، ونيابة عنه يقوم بعض الأفراد المتخصصون من الأكاديمين بأعمال خارج وصفهم الوظيفي وبشكل تطوعي دون تكليف بتطوير برامج وتطبيقات وموقع الويب من أجل تيسير أعمال الأقسام الأكاديمية بالكلية، حيث يرون أن النظم المركزية التي تقدمها رئاسة برنامج التعليم في الوكالة بالأردن لا تفي بالمطلوب، ويرغبون في تخصيص هذه البرامج والتطبيقات بما يتوافق مع بيئة قطاع غزة ومتغيراتها، ويتوقع مطورو البرامج أن تزداد أمنية نظم المعلومات بما يشعرهم بزيادة حجم استخدامهم لتكنولوجيا المعلومات.

وبناءاً على ماسبق يرى الباحث :

- الكليات الحكومية تتجه نحو تنفيذ سياسات أمن معلومات كي تحمي نظم المعلومات وتزيد من أمنها، وتستفيد من خدمات بعض الأطراف الحكومية الأخرى، ونسبة التعهيد في المؤسسات الحكومية بشكل عام ستأخذ بالتراجع نظراً لتوافر كل الميزات الجيدة التي يوفرها التعهيد في الكليات نفسها.
- الكليات العامة أكثر تطوراَ واستجابة للتغيير في الواقع الأمني، والأكثر إنفاقاً على تطوير نظم المعلومات، والحفاظ على أمن النظم الحوسبة.
- الكليات الخاصة تنظر إلى تعهيد نظم المعلومات بأنها الوسيلة لتقليل التكاليف والحصول على أمن نظمها واستقرار وتوافر المعلومات .
- كلية الوكالة (كلية تدريب غزة) تستخدم الإجراءات التنظيمية وسيلة لحماية نظم المعلومات من التهديدات الداخلية بشكل قد يبطئ من زيادة استخدام نظم المعلومات على الصعيد الإداري والخدماتي .

الفصل الرابع

منهجية الدراسة وإجراءاتها

- منهجية الدراسة
- مجتمع وعينة الدراسة
- صدق وثبات الاستبانة
- خصائص وسمات عينة الدراسة
- المعالجات الإحصائية

مقدمة :

يتناول هذا الفصل وصفاً لمنهج الدراسة، والأفراد مجتمع الدراسة وعينتها، وكذلك أداة الدراسة المستخدمة وطرق إعدادها، وصدقها وثباتها، كما يتضمن هذا الفصل وصفا للإجراءات التي قام بها الباحث في تقنين أدوات الدراسة وتطبيقها، وأخيراً المعالجات الإحصائية التي اعتمد الباحث عليها في تحليل الدراسة .

منهجية الدراسة :

يمكن اعتبار منهج البحث بأنه الطريقة التي يتتبع الباحث خطاها، ليصل في النهاية إلى نتائج تتعلق بالموضوع محل الدراسة، وهو الأسلوب المنظم المستخدم لحل مشكلة البحث، إضافة إلى أنه العلم الذي يعنى بكيفية إجراء البحوث العلمية(عبيدات وآخرون،2001).

و هناك عدة مناهج تستخدم في البحث العلمي ويستخدم كل منهج من هذه المناهج حسب الظاهرة التي يتم دراستها وقد يتم استخدام أكثر من منهج لدراسة نفس الظاهرة، وحيث أن الباحث يعرف مسبقاً جوانب وأبعاد الظاهرة موضع الدراسة من خلال إطلاعه على الدراسات السابقة المتعلقة بموضوع البحث، ويسعى الباحث للوصول إلى دراسة "**واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها**"، وهذا يتوافق مع المنهج الوصفي التحليلي الذي يهدف إلى توفير البيانات والحقائق عن المشكلة موضوع البحث لتفسيرها والوقوف على دلالاتها، وحيث أن المنهج الوصفي التحليلي يتم من خلال الرجوع للوثائق المختلفة كالكتب والصحف والمجلات وغيرها من المواد التي يثبت صدقها بهدف تحليلها للوصول إلى أهداف البحث(الآغا،2002،ص2) و الباحث سيعتمد على هذا المنهج للوصول إلى المعرفة الدقيقة والتفصيلية حول مشكلة البحث، ولتحقيق تصور أفضل وأدق للظاهرة موضع الدراسة، كما أنه سيستخدم أسلوب العينة العشوائية الطبقية في اختياره لعينة الدراسة، وسيستخدم الأستبانة في جمع البيانات الأولية كما ستساهم المقابلة في الحصول على البيانات الأساسية الأولية.

طرق جمع البيانات:

اعتمد الباحث على نوعين من البيانات :

1-**البيانات الأولية (من الميدان).**

(1) قام الباحث بتوزيع استبيانات لدراسة بعض مفردات البحث وحصر وتجميع المعلومات اللازمة في موضوع البحث ومن ثم تفريغها وتحليلها باستخدام برنامج SPSS

(Statistical Package for Social Science)الإحصائي واستخدام الاختبارات الإحصائية المناسبة بهدف الوصول لدلالات ذات قيمة ومؤشرات تدعم موضوع الدراسة.

(2) قام الباحث بإجراء مقابلات مع كل مسئول عن نظم المعلومات في الكليات التقنية.

2-البيانات الثانوية:

وتمت مراجعة الكتب والدوريات والمنشورات الخاصة أو المتعلقة بالموضوع قيد الدراسة، والتي تتعلق بدراسة **واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها**، وأي مراجع قد يرى الباحث أنها تسهم في إثراء الدراسة بشكل علمي، وينوي الباحث من خلال اللجوء للمصادر الثانوية في الدراسة، التعرف على الأسس والطرق العلمية السليمة في كتابة الدراسات، وكذلك أخذ تصور عام عن آخر المستجدات التي حدثت و تحدث في مجال الدراسة.

مجتمع وعينة الدراسة:

أولاً: مجتمع الدراسة

يعرف عبيدات وآخرون (2001،ص109) مجتمع الدراسة بأنه جميع مفردات الظاهرة التي يدرسها الباحث، وبذلك فإن مجتمع الدراسة هو جميع الأفراد أو الأشياء الذين يكونون موضوع مشكلة الدراسة .

ويتكون مجتمع الدراسة من جميع العاملين بمراكز/أقسام نظم المعلومات في الكليات التقنية بالإضافة للعاملين بالأقسام المختلفة التي تنفذ أعمالها مستفيدة من خدمات نظم المعلومات التي تخدم أعمال تلك الكليات .

ثانياً: عينة الدراسة

وقد تم اختيار عينة الدراسة باستخدام أسلوب العينة العشوائية الطبقية حسب الكلية، حيث تم حساب حجم العينة وفق معادلة ستيفن ثامبسون:

معادلة ستيفن ثامبون	p	نسبة توفر الخاصية والمحايدة = 0.50	N	حجم المجتمع
$n = \frac{N \times p(1-p)}{\left[\left[N-1\times\left(d^2 \div z^2\right)\right]+ p(1-p)\right]}$	d	نسبة الخطأ وتساوي 0.05	n	حجم العينة

وقد بلغ حجمها 123 موظف وموظفة، وتم توزيع الاستبانة على جميع أفراد عينة الدراسة حسب حصة كل كلية، ويوضح الجدول رقم (4-1) مجتمع الدراسة وحجم العينة لكل كلية من مجتمع الدراسة.

جدول رقم (4-1): يوضح حجم المجتمع والعينة في كل كلية

اسم الكلية	عدد المبحوثين	نسبة العينة للمجتمع * 68.33%[12]
كلية فلسطين التقنية – دير البلح	50	35
الكلية الجامعية للعلوم التطبيقية	55	37
كلية العلوم والتكنولوجيا – خانيونس	45	30
كلية تدريب غزة – الوكالة	16	11
الكلية العربية للعلوم التطبيقية	14	10
حجم المجتمع/العينة الإجمالي	180	123

وقد تم استرداد 103 استبانة أي أن بنسبة استجابة كانت **83.7%**، وبعد تفحص الاستبانات استبعد 6 منها نظرا لعدم تحقق الشروط المطلوبة للإجابة، وعليه يكون ما يصلح منها هو عدد 97 استبانة بواقع نسبة صحة **78.8%** من الحجم الكلي للعينة، وهي نسبة جيدة وفي المستوى الملائم لإجراء الدراسة . والجدول رقم (4-2) يبين توزيع العينة، والمسترجع، والصالح على الكليات مجتمع الدراسة.

جدول رقم (4-2): يبين الكليات مجتمع الدراسة ونسبة استجابة كل كلية:

اسم الكلية	الموزع	المسترجع	الفاقد	الصالح	نسبة الاستجابة
كلية فلسطين التقنية – دير البلح	35	32	1	31	88.57%
الكلية الجامعية للعلوم التطبيقية	37	30	1	29	78.37%
كلية العلوم والتكنولوجيا –	30	22	3	19	63.33%
كلية تدريب غزة – الوكالة	11	10	0	10	90.9%
الكلية العربية للعلوم التطبيقية	10	9	1	8	80%
حجم المجتمع/العينة الإجمالي	**123**	**103**	**6**	**97**	**78.8%**

أجزاء استبانة الدراسة :

- ولقد تم تقسيم الاستبانه إلى جزأين كما يلي:
- **الجزء الأول** : يتكون من البيانات الشخصية لعينة الدراسة ويتكون من 10 فقرات.
- **الجزء الثاني:** يتناول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها وتم تقسيمه إلى ستة محاور كما يلي:

1. المحور الأول : حماية البنية التحتية لنظم المعلومات ويتفرع منه المحاور الفرعية التالية:

(أ) الحماية المادية Hardware Security

[12] وتم إيجاد النسبة من حجم المجتمع ككل _ كالتالي : 180/123= ~0.683

(ب) الحماية البرمجية Software Security

(ج) حماية الأفراد Human Resources Security

2. المحور الثاني : سياسة أمن المعلومات Information Security Policy
3. المحور الثالث : التحكم بالوصول لنظم المعلومات IS Access Control
4. المحور الرابع : الاجراءات التنظيمية Organizational Procedures.
5. المحور الخامس : التعهيد (الاستعانة بالمصادر الخارجية) IT-Outsourcing.
6. المحور السادس : سبل تطوير إدارة أمن نظم المعلومات في الكلية

وقد كانت الإجابات على كل فقرة مكونة من 5 إجابات حيث الدرجة " 5 " تعني موافق بشدة والدرجة "1" تعني غير موافق بشدة كما هو موضح بجدول رقم (4-3).

جدول رقم(4-3):مقياس الإجابات

التصنيف	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
الدرجة	5	4	3	2	1

صدق وثبات الاستبيان:

صدق الاستبانة يعني التأكد من أنها سوف تقيس ما أعدت لقياسه (العساف،1995،ص429)، كما يقصد بالصدق " شمول الاستبانة لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها ومفرداتها من ناحية ثانية، بحيث تكون مفهومة لكل من يستخدمها"(عبيدات وآخرون، 2001،ص179)، وقد قام الباحث بالتأكد من صدق أداة الدراسة كما يلي:

صدق فقرات الاستبيان :

تم التأكد من صدق فقرات الاستبيان بطريقتين:

(1) الصدق الظاهري للأداة (صدق المحكمين)

قام الباحث بعرض أداة الدراسة في صورتها الأولية على مجموعة من المحكمين تألفت من (10) أعضاء من أعضاء الهيئة التدريسية في كلية التجارة بالجامعة الإسلامية وجامعة الأزهر وكلية فلسطين التقنية ووزارة التربية والتعليم العالي ومتخصصين في نظم المعلومات والإدارة والإحصاء. ويوضح الملحق رقم (3) أسماء المحكمين الذين قاموا مشكورين بتحكيم أداة الدراسة. وقد طلب الباحث من المحكمين إبداء آرائهم في مدى ملائمة العبارات لقياس ما وضعت لأجله، ومدى وضوح صياغة العبارات ومدى مناسبة كل عبارة للمحور الذي ينتمي إليه،ومدى كفاية العبارات لتغطية كل محور من محاور متغيرات الدراسة الأساسية هذا بالإضافة إلى اقتراح ما يرونه ضرورياً من تعديل صياغة العبارات أو حذفها، أو إضافة عبارات جديدة لأداة الدراسة، وكذلك إبداء آرائهم فيما يتعلق بالبيانات

الأولية (الخصائص الشخصية والوظيفية المطلوبة من المبحوثين)، إلى جانب مقياس ليكارت المستخدم في الاستبانة، وتركزت توجيهات المحكمين على انتقاد طول الاستبانة حيث كانت تحتوي على بعض العبارات المتكررة، كما أن بعض المحكمين نصحوا بضرورة تقليص بعض العبارات من بعض المحاور وإضافة بعض العبارات إلى محاور أخرى، واستنادا إلى الملاحظات والتوجيهات التي أبداها المحكمون قام الباحث بإجراء التعديلات التي اتفق عليها معظم المحكمين، حيث تم تعديل صياغة العبارات وحذف أو إضافة البعض الآخر منها، والملحق رقم (4) يظهر الاستبانة في صورتها النهائية بعد تحكيمها .

(2) صدق الاتساق الداخلي لفقرات الاستبانة

تم حساب الاتساق الداخلي لفقرات الاستبيان على عينة الدراسة الاستطلاعية البالغ حجمها 25 مفردة، وذلك بحساب معاملات الارتباط بين كل فقرة والدرجة الكلية للمحور التابعة له كما يلي.

- **الصدق الداخلي لفقرات المحور الأول: حماية البنية التحتية لنظم المعلومات**

جدول رقم (4-4) يبين معاملات الارتباط بين كل فقرة من فقرات المحور الأول **(حماية البنية التحتية لنظم المعلومات)** والمعدل الكلي لفقراته، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى دلالة (0.05)،حيث إن القيمة الاحتمالية لكل فقرة اقل من 0.05 وقيمة r المحسوبة أكبر من قيمة r الجدولية والتي تساوي 0.396، وبذلك تعتبر فقرات المحور الأول صادقة لما وضعت لقياسه

جدول رقم (4-4):الصدق الداخلي لفقرات المحور الأول : حماية البنية التحتية لنظم المعلومات

م	الفقرة	معامل الارتباط	القيمة الاحتمالية
Hardware Securityالحماية المادية			
1	تستخدم المحيطات الأمنية (الجدران – الأبواب – الأقفال – بطاقات الدخول) لحماية مكونات نظم المعلومات.	0.601	0.001
2	كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم خدمات نظم المعلومات محمية من العبث بها أو إتلافها.	0.534	0.006
3	يوجد في الكلية مصدر بديل للكهرباء.	0.563	0.003
4	يتم صيانة الأجهزة بشكل سليم لضمان استمرارية عملها وسلامتها.	0.558	0.004
5	يمنع الموظف غير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات	0.603	0.001
6	يتم تأمين شاشة الحاسوب بشكل يدوي عند عدم استخدامها لفترة ما.	0.600	0.002
Software Security الحماية البرمجية			
7	يتم التحقق من صحة البيانات المدخلة.	0.594	0.002

م	الفقرة	معامل الارتباط	القيمة الاحتمالية
8	تستخدم آليات تشفير لحماية البيانات.	0.708	0.000
9	توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي.	0.438	0.028
10	تتم حماية البرامج المصدرية (Source Code) المستخدمة.	0.499	0.011
11	توفر قواعد البيانات المستخدمة مستويات أمنية متعددة.	0.464	0.019
12	يتم وقاية النظام عن طريق برامج مكافحة الفيروسات.	0.785	0.000
13	توجد برامج حماية لتتبع الاختراق والتسلل.	0.694	0.000
14	هناك معايير لقبول أي أنظمة جديدة أو أي تعديلات، ويتم إجراء اختبارات عليها قبل القبول بها.	0.610	0.001
	حماية الأفراد Human Resources Security		
15	يتوفر تدريب للعاملين على النظم المحوسبة بشكل دوري لتطوير مهارتهم المتعلقة بالمستجدات الأمنية.	0.547	0.005
16	تحتوي وثيقة الوصف الوظيفي للموظف على مسؤلياته ومهامه تجاه أمن المعلومات في الكلية	0.825	0.000
17	يطلب من الموظف التوقيع على تعهد بعدم الافصاح عن معلومات حساسة تخص الكلية كجزء من شروط التوظيف.	0.826	0.000
18	يطلب من الموظفين والمتعاقدين الابلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.	0.681	0.000
19	هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.	0.724	0.000
20	يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في الكلية.	0.213	0.306

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية "23" تساوي 0.396

الصدق الداخلي لفقرات المحور الثاني :

سياسة أمن المعلومات Information Security Policy

جدول رقم (4-5) يبين معاملات الارتباط بين كل فقرة من فقرات المحور الثاني (سياسة أمن المعلومات Information Security Policy) والمعدل الكلي لفقراته، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى دلالة (0.05)، حيث إن القيمة الاحتمالية لكل فقرة اقل من 0.05 وقيمة r المحسوبة أكبر من قيمة r الجدولية والتي تساوي 0.396، وبذلك تعتبر فقرات المحور الثاني صادقة لما وضعت لقياسه.

جدول رقم (4-5): الصدق الداخلي لفقرات المحور الثاني/ (سياسة أمن المعلومات)

م.	الفقرة	معامل الارتباط	القيمة الاحتمالية
1	توجد في الكلية سياسة مكتوبة لأمن المعلومات .	0.760	0.000
2	يعرف الموظف بسياسة أمن المعلومات .	0.784	0.000
3	توجد جهة مكلفة بالإشراف على متابعة سياسة أمن المعلومات .	0.803	0.000
4	يتم مراجعة وتطوير سياسة أمن المعلومات بشكل دوري .	0.764	0.000
5	تدرك الإدارة العليا في الكلية أهمية سياسة أمن المعلومات.	0.428	0.033
6	يوجد إجراءات ضبط صارمة مطبقة على تنفيذ أي تغيرات على نظم المعلومات لحمايتها من العطل.	0.660	0.000

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية "23" تساوي 0.396

الصدق الداخلي لفقرات المحور الثالث

(التحكم بالوصول لنظم المعلومات IS Access Control)

جدول رقم (4-6) يبين معاملات الارتباط بين كل فقرة من فقرات المحور الثالث (التحكم بالوصول لنظم المعلومات IS Access Control) والمعدل الكلي لفقراته، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى دلالة (0.05)، حيث إن القيمة الاحتمالية لكل فقرة اقل من 0.05 وقيمة r المحسوبة أكبر من قيمة r الجدولية والتي تساوي 0.396، وبذلك تعتبر فقرات المحور الثالث صادقة لما وضعت لقياسه

جدول رقم (4-6):الصدق الداخلي لفقرات المحور الثالث/(التحكم بالوصول لنظم المعلومات)

م	الفقرة	معامل الارتباط	القيمة الاحتمالية
1	صلاحيات الدخول للمعلومات تعطى حسب المستوى الإداري.	0.478	0.008
2	لكل مستخدم هوية محددة خاصة به، حيث لا توجد حسابات عامة	0.572	0.001
3	توجد مراجعات دورية لصلاحيات المستخدمين في الوصول للأنظمة.	0.570	0.003
4	يُحجب الوصول إلى شبكة الانترنت أحياناً.	0.617	0.001
5	يمنع الوصول لبعض خدمات نظم المعلومات عبر الشبكات اللاسلكية.	0.655	0.000
6	توجد إرشادات لطريقة إنشاء كلمات المرور القوية .	0.660	0.000
7	بعض أنظمة المعلومات الحساسة معزولة في شبكات محلية مستقلة.	0.486	0.014
8	يتم إغلاق صلاحيات المستخدم بعد فترة محددة من انعدام نشاطها.	0.758	0.000
9	تستخدم سجلات الأداء لحفظ أنشطة المستخدم لدواعي متعلقة بأمن المعلومات.	0.704	0.000

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية "23" تساوي 0.396

الصدق الداخلي لفقرات المحور الرابع

(الاجراءات التنظيمية Organizational Procedures)

جدول رقم (4-7) يبين معاملات الارتباط بين كل فقرة من فقرات المحور الرابع (الاجراءات التنظيمية Organizational Procedures) والمعدل الكلي لفقراته، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى دلالة (0.05)، حيث إن القيمة الاحتمالية لكل فقرة اقل من 0.05 وقيمة r المحسوبة أكبر من قيمة r الجدولية والتي تساوي 0.396، وبذلك تعتبر فقرات المحور الرابع صادقة لما وضعت لقياسه

جدول رقم (4-7) : الصدق الداخلي لفقرات المحور الرابع/(الاجراءات التنظيمية)

م.	الفقرة	معامل الارتباط	القيمة الاحتمالية
1	يتم إحاطة الموظف بإجراءات التأمين الوقائية.	0.465	0.019
2	يوجد دليل تصنيف للمعلومات يمكن أن يساعد في تحديد كيفية التعامل مع المعلومات وحمايتها .	0.791	0.000
3	تحتفظ الكلية بسجلات حول الأصول المكونة لكل نظام معلومات.	0.686	0.000
4	يتم تحديد الأحداث التي تؤدي إلى توقف نظم المعلومات في الكلية عن العمل، بهدف تقدير مخاطر تلك الأحداث ووضع خطط طوارئ لإستعادة العمل.	0.692	0.000
5	في حال حدوث إخفاق أو انقطاع في أداء الأعمال توجد خطط لإعادة الأعمال إلى طبيعتها ضمن إطار زمني مخطط .	0.535	0.006
6	يتم تسجيل ما يحدث من أخطاء في نظم المعلومات في تقارير، ويتم ذكر الإجراءات التي اتخذت لتصحيحها.	0.640	0.001
7	يتم عمل نسخ احتياطي للمعلومات بشكل دوري.	0.553	0.004
8	يوجد آليات للإبلاغ عن الحوادث ذات العلاقة بأمن المعلومات.	0.809	0.000
9	يجري منع الموظف من استخدام المعلومات للإغراض غير المصرح بها.	0.798	0.000

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية "23" تساوي 0.396

الصدق الداخلي لفقرات المحور الخامس

IT-Outsourcing التعهيد (الاستعانة بالمصادر الخارجية)

جدول رقم (4-8) يبين معاملات الارتباط بين كل فقرة من فقرات المحور الخامس (التعهيد (الاستعانة بالمصادر الخارجية) IT-Outsourcing) والمعدل الكلي لفقراته، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى دلالة (0.05)، حيث إن القيمة الاحتمالية لكل فقرة اقل من 0.05

وقيمة r المحسوبة أكبر من قيمة r الجدولية والتي تساوي 0.396، وبذلك تعتبر فقرات المحور الخامس صادقة لما وضعت لقياسه

جدول رقم (4-8):الصدق الداخلي لفقرات المحور الخامس /استخدام التعهيد

م.	الفقرة	معامل الارتباط	القيمة الاحتمالية
1	يوجد تعاقد مع أطراف خارجية في مجال تطوير نظم المعلومات في الكلية.	0.786	0.000
2	تقوم الكلية بالاستعانة بخبراء في مجالات نظم المعلومات للحصول على استشارات في أمن المعلومات.	0.715	0.000
3	تتم مراقبة عمليات تطوير البرامج التي تنفذها الأطراف الخارجية .	0.690	0.000
4	يطلب من الجهات الخارجية الإبلاغ عن أي ثغرات أمنية يلاحظونها في الأنظمة.	0.785	0.000
5	يتم التحقق من قيام الأطراف الخارجية المتعاقدة بتنفيذ الضوابط الأمنية المتفق عليها.	0.694	0.000
6	يجري مراقبة أداء الاطراف الخارجية عند إجراء الصيانة .	0.751	0.000

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية "23" تساوي 0.396

الصدق الداخلي لفقرات المحور السادس:

(سبل تطوير إدارة أمن نظم المعلومات في الكلية)

جدول رقم (4-9) يبين معاملات الارتباط بين كل فقرة من فقرات المحور **السادس (سبل تطوير إدارة أمن نظم المعلومات في الكلية)** والمعدل الكلي لفقراته، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى دلالة (0.05)، حيث إن القيمة الاحتمالية لكل فقرة اقل من 0.05 وقيمة r المحسوبة أكبر من قيمة r الجدولية والتي تساوي 0.396، وبذلك تعتبر فقرات المحور السادس صادقة لما وضعت لقياسه

جدول رقم (4-9):الصدق الداخلي لفقرات المحور السادس (سبل تطوير إدارة أمن نظم المعلومات)

م.	الفقرة	معامل الارتباط	القيمة الاحتمالية
1	تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمن نظم المعلومات.	0.718	0.000
2	زيادة الموازنة المخصصة لأمن المعلومات ضمن موازنة تكنولوجيا المعلومات	0.746	0.000
3	فحص أنظمة المعلومات للتحقق من الالتزام بمعايير الأداء الأمني.	0.911	0.000
4	استخدام برامج حماية فعالة لمنع محاولات الاختراق والتعدي على نظم المعلومات في الكليات.	0.781	0.000
5	توفير الحوافز(المادية والمعنوية) المناسبة للمبدعين والمتفوقين في مجال أمن نظم المعلومات.	0.790	0.000
6	استقطاب خبراء حماية نظم المعلومات للعمل بمراكز نظم المعلومات بالكليات التقنية.	0.740	0.000

م.	الفقرة	معامل الارتباط	القيمة الاحتمالية
7	دعم الإدارة العليا لسياسة ناجحة لأمن المعلومات.	0.891	0.000
8	اعتماد استخدام الوسائل البيولوجية في تحديد شخصية وصلاحية مستخدمي نظم المعلومات.	0.758	0.000
9	وضع ضوابط لتبادل المعلومات مع الجهات المعنية خارج الكلية.	0.754	0.000
10	الاستفادة من خدمات الأطراف الخارجية ضمن ضوابط أمنية وشروط جزائية متفق عليها.	0.540	0.005

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية "23" تساوي 0.396

صدق الاتساق البنائي لمحاور الدراسة

جدول رقم (4-10) يبين معاملات الارتباط بين معدل كل محور من محاور الدراسة مع المعدل الكلي لفقرات الاستبانة والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى دلالة 0.05، حيث إن القيمة الاحتمالية لكل فقرة اقل من 0.05 وقيمة r المحسوبة أكبر من قيمة r الجدولية والتي تساوي 0.396.

جدول رقم (4-10):معامل الارتباط بين معدل كل محور من محاور الدراسة مع المعدل الكلي للفقرات

المحور	عنوان المحور	معامل الارتباط	القيمة الاحتمالية
الأول	حماية البنية التحتية لنظم المعلومات	0.528	0.007
الثاني	سياسة أمن المعلومات	0.583	0.002
الثالث	التحكم بالوصول لنظم المعلومات	0.638	0.001
الرابع	الإجراءات التنظيمية	0.877	0.000
الخامس	التعهيد (الاستعانة بالمصادر الخارجية)	0.636	0.001
السادس	سبل تطوير إدارة أمن نظم المعلومات في الكلية	0.829	0.000

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية "23" تساوي 0.396

(3)ثبات فقرات الاستبانة Reliability:

أما ثبات أداة الدراسة فيعني التأكد من أن الإجابة ستكون واحدة تقريباً لو تكرر تطبيقها على الأشخاص ذاتهم في أوقات مختلفة(العساف، 1995،ص430). وقد أجرى الباحث خطوات الثبات على العينة الاستطلاعية نفسها بطريقتين هما طريقة التجزئة النصفية ومعامل ألفا كرونباخ.

1- **طريقة التجزئة النصفية** Split-Half Coefficient:

تم إيجاد معامل ارتباط بيرسون بين معدل الأسئلة الفردية الرتبة ومعدل الأسئلة الزوجية الرتبة لكل بعد وقد تم تصحيح معاملات الارتباط باستخدام معامل ارتباط سبيرمان براون للتصحيح (Spearman-Brown Coefficient) حسب المعادلة التالية:

معامل الثبات = $\frac{2ر}{1+ر}$ حيث ر معامل الارتباط وقد بين جدول رقم (4-11) يبين أن هناك معامل ثبات كبير نسبيا لفقرات الاستبيان مما يطمئن الباحث على استخدام الاستبانة بكل طمأنينة.

جدول رقم (4-11):معامل الثبات (طريقة التجزئة النصفية)

المحور	عنوان المحور	التجزئة النصفية			
		عدد الفقرات	معامل الارتباط	معامل الارتباط المصحح	القيمة الاحتمالية
الأول	حماية البنية التحتية لنظم المعلومات	20	0.7924	0.8842	0.0000
الثاني	سياسة أمن المعلومات	6	0.7625	0.8653	0.0000
الثالث	التحكم بالوصول لنظم المعلومات	9	0.7489	0.8564	0.0000
الرابع	الإجراءات التنظيمية	9	0.8154	0.8983	0.0000
الخامس	التعهيد (الاستعانة بالمصادر الخارجية)	6	0.7126	0.8322	0.0000
السادس	سبل تطوير إدارة أمن نظم المعلومات	10	0.8235	0.9032	0.0000
	جميع المحاور	60	0.7724	0.8716	0.0000

قيمة r الجدولية عند مستوى دلالة 0.05 ودرجة حرية "25" تساوي 0.381

2- طريقة ألفا كرونباخ Cronbach's Alpha:

استخدم الباحث طريقة ألفا كرونباخ لقياس ثبات الاستبانة كطريقة ثانية لقياس الثبات ويبين جدول رقم (4-12) أن معاملات الثبات مرتفعة مما يطمئن الباحث على استخدام الاستبانة بكل طمأنينة.

جدول رقم (4-12):معامل الثبات (طريقة والفا كرونباخ)

المحور	عنوان المحور	عدد الفقرات	معامل ألفا كرونباخ
الأول	حماية البنية التحتية لنظم المعلومات	20	0.8994
الثاني	سياسة أمن المعلومات	6	0.8821
الثالث	التحكم بالوصول لنظم المعلومات	9	0.8795
الرابع	الإجراءات التنظيمية	9	0.9014
الخامس	التعهيد (الاستعانة بالمصادر الخارجية)	6	0.8564
السادس	سبل تطوير إدارة أمن نظم المعلومات في الكلية	10	0.9215
	جميع الفقرات	60	0.8957

خصائص وسمات مجتمع الدراسة :

يتناول هذا الجزء توضيح الخصائص الشخصية لعينة الدراسة بعد إجراء الدراسة الميدانية التي تلت الدراسة الاستطلاعية Pilot study، والخصائص تعود للكليات مجتمع الدراسة ونظرة عينة الدراسة تجاه مواضيع كتوافر نظم المعلومات، حجم الأداء الأمني، والتدريب، والموازنة .

و البيانات والجداول التالية تبين خصائص وسمات عينة الدراسة كما يلي:

1- توزيع المبحوثين حسب الكلية :

ويبين جدول رقم (4-13) أن عينة الدراسة تمثل جميع الكليات بنسب تقترب من النسب الموضوعة سابقاً في جدول توزيع العينة الطبقية العشوائية .

جدول رقم (4-13):توزيع عينة الدراسة حسب متغير الكلية

	التكرار	النسبة المئوية
كلية فلسطين التقنية	31	32.0
كلية العلوم والتكنولوجيا	19	19.6
كلية تدريب غزة	10	10.3
الكلية الجامعية للعلوم التطبيقية	29	29.9
الكلية العربية للعلوم التطبيقية-رفح	8	8.2
المجموع	97	100.0

وبتوزيع المبحوثين بحسب نطاق إشراف الكليات كما في جدول (4-14) يتضح أن أكثر من 51% منهم يتبع الإشراف الحكومي بينما 30% منهم يتبع الإشراف العام فيما الخاص نسبتهم 8.2% والوكالة يسجل حوالي 10.3%، وهذا يعطي مؤشراً عن احتمالية تأثير نطاق الإشراف على إدارة أمن نظم المعلومات في الكليات التقنية.

ويبين الجدول (4-14) توزيع عينة الدراسة حسب جهة الإشراف

جهة الإشراف	حكومية	عامة	خاصة	الوكالة	المجموع
التكررات	50	29	8	10	97
النسبة	%51.5	%30	%8.2	%10.3	%100

2- توزيع المبحوثين حسب الجنس :

جدول رقم (4-15): توزيع عينة الدراسة حسب متغير الجنس

الجنس	التكرار	النسبة المئوية
ذكر	77	79.4
أنثى	20	20.6
المجموع	97	100.0

و ويلاحظ من الجدول (4-15) أن نسبة الذكور إلى الأناث هي 1:4، ويرجع الباحث الزيادة في نسبة الذكور إلى طبيعة نشاطات الكليات التقنية التي تتطلب عملاً فنياً شاقاً، يتفوق فيه الرجال على النساء وخصوصاً في المجتمعات العربية .

3- توزيع المبحوثين حسب العمر:

ويلاحظ من الجدول رقم (4-16) أن قرابة (78.3%) من المبحوثين تتراوح أعمارهم بين 20 إلى أقل من 40 سنة وهو ما يشير إلى أن غالبية العاملين بحقل نظم المعلومات في الكليات التقنية هم من الشباب، وهي نفس نسب مستويات الأعمار في دراسة البحيصي والشريف (2008)، ودراسة القحطاني (2008)، العتيبي(2010).

جدول رقم (4-16):توزيع عينة الدراسة حسب متغير العمر

العمر	التكرار	النسبة المئوية
20 سنة إلى أقل من 30 سنة	30	30.9
30سنة إلى اقل من 40 سنة	46	47.4
40 سنة إلى أقل من 50 سنة	16	16.5
50 سنة فأكثر	5	5.2
المجموع	97	100.0

4- توزيع المبحوثين حسب سنوات الخبرة :

يلاحظ من الجدول رقم (4-17) أن قرابة (70%) من المبحوثين تتراوح سنوات خبراتهم أقل من 10 سنوات وهو ما يشير إلى نضوج اهتمام الكليات التقنية بتطبيق نظم المعلومات المحوسبة في أعمالها، وهو ما يتطلب توظيف طبقة من المتخصصين في نظم المعلومات، وربما أيضاً يعزى السبب بشكل عام إلى أن الكليات التقنية أغلبها حديثة النشأة.

ولعل التنوع العام في الخبرات سيسهم في تعزيز نتائج البحث ويضفي قوة في تصور المبحوثين نحو واقع إدارة أمن نظم المعلومات في الكليات التقنية، وهي نفس نسبة الخبرات في دراسة البحيصي والشريف (2008)، ودراسة القحطاني (2008) .

جدول رقم (4-17): توزيع عينة الدراسة حسب متغير سنوات الخبرة

سنوات الخبرة	التكرار	النسبة المئوية
اقل من 5 سنوات	33	34.0
من 5 إلى اقل من 10سنوات	29	29.9
من 10 إلى اقل من 15 سنة	16	16.5
15 سنة فأكثر	19	19.6
المجموع	97	100.0

5- توزيع المبحوثين حسب المؤهل العلمي:

ويلاحظ من الجدول (4-18) أن قرابة (69%) من المبحوثين يحملون الشهادة الجامعية الأولى أو شهادة الدبلوم المتوسط بينما ثلثهم المتبقي يحمل شهادات جامعية عليا مما يشير إلى تنوع المعارف العلمية وربما سيؤثر ذلك في نظرة المبحوثين نحو واقع إدارة أمن نظم المعلومات في الكليات التقنية، وكانت نفس نسبة حاملي مؤهل البكالوريوس تقريباً قد ظهرت في دراسة العتيبي(2010)، والقحطاني(2008) .

جدول رقم (4-18): توزيع عينة الدراسة حسب متغير المؤهل العلمي

المؤهل العلمي	التكرار	النسبة المئوية
دبلوم متوسط	21	21.6
بكالوريوس	46	47.4
ماجستير	25	25.8
دكتوراه	5	5.2
المجموع	97	100.0

6- توزيع المبحوثين حسب التخصص العلمي :

ويلاحظ من الجدول رقم(4-19) أن ما يقارب من ثلث المبحوثين من تخصصات الحاسوب الذين هم على إدراك مباشر بعمل نظم المعلومات أو ممن يسهمون بشكل أساسي في تطويرها، في حين أن الثلث الآخر هم من أصحاب المعرفة المتصلة مباشرة بنظم المعلومات من تخصصي (الإدارة و المحاسبة) والثلث الآخر من التخصصات الأخرى المتنوعة والتي جميعها ستعزز من فهم وادراك أهمية توجهاتهم وروائهم نحو واقع إدارة أمن نظم المعلومات في الكليات التقنية .

وهي نفس نسب توزيع التخصصات العلمية في دراسة البحيصي والشريف(2008)، ودراسة تايه (2008).

جدول رقم (4-19): توزيع عينة الدراسة حسب متغير التخصص العلمي

التخصص العلمي	التكرار	النسبة المئوية
هندسة حاسوب / علوم حاسوب	29	29.9
إدارة أعمال	25	25.8
محاسبة	9	9.3
غير ذلك	34	35.1
المجموع	97	100.0

7- توزيع المبحوثين حسب تصورهم لمدى استخدام الكلية لنظم المعلومات المحوسبة :

ويلاحظ من الجدول رقم(4-20) أن الكليات التقنية تستخدم نظم المعلومات بمستوى أعلى من المتوسط بنسبة (92.8%) من وجهة نظر المبحوثين، وهو ما يدعم اختيار موضوع البحث وبيئة البحث التي تتصف بالتطور التقني واستخدام جديد تكنولوجيا المعلومات .

جدول رقم (4-20): مدى استخدام الكلية لنظم المعلومات المحوسبة

مدى استخدام الكلية لنظم المعلومات المحوسبة	التكرار	النسبة المئوية
بصورة قليلة جداً	0	0.0
بصورة قليلة	7	7.2
بصورة متوسطة	26	26.8
بصورة مرتفعة	48	49.5
بصورة مرتفعة جداً	16	16.5
المجموع	97	100.0

8- توزيع المبحوثين حسب مدى توافر إدارة لأمن نظم المعلومات في الكلية:

ويلاحظ من الجدول رقم (4-21) أن هناك توافر لإدارة أمن نظم المعلومات في الكليات التقنية بمستوى أقل من المتوسط بنسبة (50.5%) من وجهة نظر المبحوثين، وهو ما يدعم اختيار بيئة البحث.

جدول رقم (4-21): مدى توافر إدارة لأمن نظم المعلومات في الكلية

	التكرار	النسبة المئوية
بصورة قليلة جداً	4	4.1
بصورة قليلة	11	11.3
بصورة متوسطة	34	35.1
بصورة مرتفعة	38	39.2
بصورة مرتفعة جداً	10	10.3
المجموع	97	100.0

9- توزيع المبحوثين حسب استجاباتهم لمستوى التدريب الذي يتلقونه في مجال أمن المعلومات:

ويلاحظ من الجدول رقم (4-22) أن (74.2%) من مستخدمي نظم المعلومات بالكليات التقنية (المبحوثين) يعتقدون بأنهم يتلقون تدريباً في مجال أمن المعلومات بمستوى أقل من المتوسط، وهو ما يدعم باتجاه البحث .

جدول رقم (4-22): مستوى التدريب الذي تتلقونه في مجال أمن المعلومات

مستوى التدريب الذي تتلقونه في مجال أمن المعلومات	التكرار	النسبة المئوية
قليل جداً	21	21.6
قليل	31	32.0
متوسط	20	20.6
مرتفع	14	14.4
مرتفع جداً	11	11.3
المجموع	97	100.0

10- توزيع المبحوثين حسب تقديرهم للنسبة المخصصة لموازنة عمليات أمن المعلومات **من** الموازنة الكلية لمركز/قسم نظم المعلومات:

حيث يلاحظ من الجدول رقم (4-23) أن (71.2%) من مستخدمي نظم المعلومات بالكليات التقنية (المبحوثين) يعتقدون أن النسبة المخصصة لموازنة عمليات أمن المعلومات من الموازنة الكلية لمركز/قسم نظم المعلومات تقع في مستوى أقل من المتوسط، والسبب يرجع لعدم وجود متخصصي أمن المعلومات في غالبية الكليات التقنية وكانت دراسة تايه (2008،ص98) قد رصدت نفس النسب تقريباً.

جدول رقم (4-23): توزيع عينة الدراسة حسب تقديرهم للنسبة المخصصة لموازنة عمليات أمن المعلومات من الموازنة الكلية لمركز/قسم نظم المعلومات

النسبة المخصصة لموازنة عمليات أمن المعلومات من الموازنة الكلية	التكرار	النسبة المئوية
نسبة قليلة جداً	18	18.6
نسبة قليلة	24	24.7
نسبة متوسطة	27	27.8
نسبة مرتفعة	20	20.6
نسبة مرتفعة جداً	8	8.2
المجموع	97	100.0

المعالجات الإحصائية:

لتحقيق أهداف الدراسة وتحليل البيانات التي تم تجميعها، فقد تم استخدام العديد من الأساليب الإحصائية المناسبة باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية وفيما يلي مجموعة من الأساليبى الإحصائية المستخدمة في تحليل البيانات:

1- تم ترميز وإدخال البيانات إلى الحاسب الآلي، حسب مقياس ليكرت الخماسي (1 غير موافق بشدة، 2 غير موافق، 3 محايد، 4 موافق، 5 موافق بشدة)، ولتحديد طول فترة مقياس ليكرت الخماسي (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم حساب المدى(5-1=4)، ثم تقسيمه على عدد فترات المقياس الخمسة للحصول على طول الفقرة أي (4/5=0.08)، بعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس (وهي الواحد الصحيح) وذلك لتحديد الحد الأعلى للفترة الأولى وهكذا وجدول رقم (4-24) يوضح أطوال الفترات كما يلي:

جدول رقم(4-24) لأطوال الفترات

الفترة	1-1.80	1.80-2.60	2.60-3.40	3.40-4.20	4.20-5.0
التصنيف	غير موافق تماماً	غير موافق	محايد	موافق	موافق تماماً
الوزن	**1**	**2**	**3**	**4**	**5**

2- تم حساب التكرارات والنسب المئوية للتعرف على الصفات الشخصية لمفردات الدراسة وتحديد استجابات أفرادها تجاه عبارات المحاور الرئيسية التي تتضمنها أداة الدراسة.

3- المتوسط الحسابي Mean وذلك لمعرفة مدى ارتفاع أو انخفاض استجابات أفراد الدراسة عن كل عبارة من عبارات متغيرات الدراسة الأساسية، مع العلم بأنه يفيد في ترتيب العبارات حسب أعلى متوسط حسابي (كشك،1996،ص89) علما بأن تفسير مدى الاستخدام أو مدى الموافقة على العبارة يتم كما سبق أوضحناه في النقطة الأولى.

4- تم استخدام الانحراف المعياري (Standard Deviation) للتعرف على مدى انحراف استجابات أفراد الدراسة لكل عبارة من عبارات متغيرات الدراسة ولكل محور من المحاور الرئيسية عن متوسطها الحسابي، ويلاحظ أن الانحراف المعياري يوضح التشتت في استجابات أفراد الدراسة لكل عبارة من عبارات متغيرات الدراسة إلى جانب المحاور الرئيسية، فكلما اقتربت قيمته من الصفر كلما تركزت الاستجابات وانخفض تشتتها بين المقياس (إذا كان الانحراف المعياري واحد صحيحا فأعلى فيعني عدم تركز الاستجابات وتشتتها) .

5- اختبار ألفا كرونباخ لمعرفة ثبات فقرات الاستبانة.

6- معامل ارتباط بيرسون لقياس صدق الفقرات .

7- معادلة سبيرمان براون للثبات .

8- اختبار كولومجروف-سمرنوف لمعرفة نوع البيانات هل تتبع التوزيع الطبيعي أم لا (1- Sample K-S) .

9- اختبار t لمتوسط عينة واحدة One sample T test لمعرفة الفرق بين متوسط الفقرة والمتوسط الحيادي "3" .

10- اختبار t للفروق بين متوسطي عينتين مستقلتين.

11- تحليل التباين الأحادي للفروق بين ثلاث متوسطات فأكثر .

12- اختبار شفيه للفروق المتعددة بين المتوسطات .

الفصل الخامس

تحليل نتائج الدراسة وتفسيرها

- اختبار التوزيع الطبيعي
- تحليل وتفسير فقرات وفرضيات الدراسة

أولاً: / اختبار التوزيع الطبيعي

(اختبار كولمجروف– سمرنوف (1- Sample K-S))

سنعرض اختبار كولمجروف– سمرنوف لمعرفة هل البيانات تتبع التوزيع الطبيعي أم لا وهو اختبار ضروري في حالة اختبار الفرضيات لأن معظم الاختبارات المعلمية تشترط أن يكون توزيع البيانات طبيعيا.

ويوضح الجدول رقم (5-1) نتائج الاختبار حيث أن القيمة الاحتمالية لكل محور أكبر من 0.05 ($sig. > 0.05$) وهذا يدل على أن البيانات تتبع التوزيع الطبيعي ويجب استخدام الاختبارات المعلمية.

جدول رقم (5-1) :اختبار التوزيع الطبيعي(1-Sample Kolmogorov-Smirnov)

المحور	عنوان المحور	عدد الفقرات	قيمة Z	القيمة الاحتمالية
الأول	حماية البنية التحتية لنظم المعلومات	20	0.941	0.339
الثاني	سياسة أمن المعلومات	6	1.027	0.242
الثالث	التحكم بالوصول لنظم المعلومات	9	0.932	0.350
الرابع	الإجراءات التنظيمية لضبط نظم المعلومات	9	0.970	0.304
الخامس	التعهيد (الاستعانة بالمصادر الخارجية)	6	0.700	0.711
السادس	سبل تطوير إدارة أمن نظم المعلومات في	10	0.911	0.378
	جميع الفقرات	60	1.077	0.197

ثانياً : / تحليل فقرات الدراسة

تم استخدام اختبار T للعينة الواحدة (One Sample T test) لتحليل فقرات الاستبانة، وتكون الفقرة ايجابية بمعنى أن أفراد العينة يوافقون على محتواها إذا كانت قيمة t المحسوبة أكبر من قيمة t الجدولية والتي تساوي 1.98(أو القيمة الاحتمالية اقل من 0.05 والمتوسط الحسابي النسبي أكبر من 60 %)، وتكون الفقرة سلبية بمعنى أن أفراد العينة لا يوافقون على محتواها إذا كانت قيمة t المحسوبة أصغر من قيمة t الجدولية والتي تساوي -1.98(أو القيمة الاحتمالية اقل من 0.05 والمتوسط الحسابي النسبي اقل من 60 %)، وتكون آراء العينة في الفقرة محايدة إذا كان مستوى الدلالة لها أكبر من 0.05.

تحليل فقرات ومحاور الدراسة :

❖ **تساؤلات الدراسة : (ما هو واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة؟ وما هي سبل تطويرها؟)**

وللإجابة على هذا التساؤلات نختبر الفرضيات التالية:

1. الفرضية الأولى : تؤثر حماية البنية التحتية لنظم المعلومات بصورة ايجابية على إدارة أمن نظم المعلومات عند مستوى دلالة إحصائية $\alpha = 0.05$ وتنبثق عن هذه الفرضية الفروض الفرعية التالية:

1.1 – يؤثر توفر الحماية المادية على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5–2) والذي يبين آراء أفراد عينة الدراسة في فقرات (الحماية المادية Hardware Security) .

جدول رقم (5–2):تحليل الفقرات المتعلقة بالحماية المادية Hardware Security

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
1	تستخدم المحيطات الأمنية (الجدران – الأبواب – الأقفال – بطاقات الدخول) لحماية مكونات نظم المعلومات.	4.06	81.24	13.270	0.000	الرابع
2	كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم خدمات نظم المعلومات محمية من العبث بها أو	4.08	81.65	13.560	0.000	الثالث
3	يوجد في الكلية مصدر بديل للكهرباء.	4.41	88.25	16.588	0.000	الأول
4	يتم صيانة الأجهزة بشكل سليم لضمان استمرارية عملها وسلامتها.	4.05	81.03	10.772	0.000	الخامس
5	يمنع الموظف غير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات	4.26	85.15	14.658	0.000	الثاني
6	يتم تأمين شاشة الحاسوب بشكل يدوي عند عدم استخدامها لفترة ما.	3.68	73.61	5.779	0.000	السادس
	جميع الفقرات	4.09	81.82	19.312	0.000	

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "96" تساوي 1.98

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات (الحماية المادية Hardware Security) تساوي4.09، و المتوسط الحسابي النسبي يساوي 81.82 % وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 19.312 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و والقيمة الاحتمالية تساوي 0.000 وهي اقل من 0.05، مما يدل على صحة الفرضية الفرعية 1.1 : توفر الحماية المادية يؤثر على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

وسيجرى ترتيب فقرات هذا المحور وفقاً لآراء المبحوثين في الكليات مجتمع الدراسة ترتيباً تنازلياً حسب المتوسط الحسابي النسبي لكل فقرة، وسيتم ذكرها وتفسيرها:

1. يرجع الباحث سبب ارتفاع نتيجة الفقرة :" يوجد في الكلية مصدر بديل للكهرباء " إيجابياً إلى حرص الكليات على توفير مصدر بديل للكهرباء في ظل بيئة قطاع غزة التي تعاني من إنقطاع مستمر في التيار الكهربائي، وتتفق بنسبة كبيرة مع نتائج دراسة تايه(2008،ص111)، دراسة (العتيبي،2010،ص170) فيما رأى Kreicberga(2010,P.62) أن الحاجة الى توفير الطاقة البديلة UPS هي ضمن مسئولية المؤسسة التي تتبع من ثقافة التوفر والتي تعتبر أحدى الإعتبارات المركزية لأمن نظم المعلومات.

2. دللت نتيجة الفقرة:" يمنع الموظف غير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات " على إهتمام الكليات بأصولها المعلوماتية على الأقل من الناحية المادية، وربما تميزت هذه الدراسة بطرح هذه الفقرة.

3. أكدت صحة نتائج الفقرة:" كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم خدمات نظم المعلومات محمية من العبث بها أو إتلافها " على إهتمام الكليات بتوفير الحماية لكابلات الكهرباء والاتصالات، وهو ما أتفق مع دراسة العتيبي (2010،ص170) بنسبة كبيرة.

4. ويؤكد ارتفاع نسبة ردود المبحوثين نحو هذه الفقرة:" تستخدم المحيطات الأمنية (الجدران – الأبواب – الأقفال – بطاقات الدخول) لحماية مكونات نظم المعلومات " سعي الكليات المتزايد لتوفير الحمايات المادية المباشرة، ويعتبرها الباحث الأساس المبدأي الأولي الذي تبنى عليه درجات الأمان لنظم المعلومات، وأشارت دراسات (العتيبي،2010؛ البحيصي والشريف،2008؛القحطاني،2008) إلى وجوب استخدام المحيطات الامنية بنسبة كبيرة .

5. يعزو الباحث ارتفاع متوسط هذه الفقرة: " يتم صيانة الأجهزة بشكل سليم لضمان استمرارية عملها وسلامتها " وربما إلى توفر متخصصين في صيانة أجهزة الحاسوب ومرفقاتها في الكليات بنسبة مرتفعة نسبياً، أو نتيجة تعهيد عمليات الصيانة لدى بعض الكليات كما أكدت مقابلة(أحمد عواجه،2013) في الكلية العربية للعلوم التطبيقية حيث يلجأون الى ذلك رؤية منهم في تقليل

التكاليف، بينما ترى الكليات العامة والحكومية في ذلك إنتقاصاً لمستويات الحماية الأمنية للمعلومات.

6. يتبين إنخفاض نتيجة الفقرة "يتم تأمين شاشة الحاسوب بشكل يدوي عند عدم استخدامها لفترة ما " نسبياً مقارنة بالمتوسط العام للمحور الفرعي، حيث يرى الباحث أن نقص برامج التوعية والتدريب الأمني سبباً في عدم إحاطة الموظف بأهمية هذا الجانب .

ومما سبق نخلص إلى القول بأن نتائج عبارات المحور الفرعي (الحماية المادية Hardware Security) تؤكد أن الآراء نحو أهميتها في توفير إدارة أمن نظم المعلومات مرتفعة، وهذا يتلائم مع معايير ضبط نظم المعلومات وتحقيق الأمن المادي.

1.2- يؤثر توفر الحماية البرمجية على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5-3) والذي يبين آراء أفراد عينة الدراسة في فقرات (الحماية البرمجية Software Security) .

جدول رقم (5-3) : تحليل الفقرات المتعلقة بالحماية البرمجية Software Security

م	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
1	يتم التحقق من صحة البيانات المدخلة.	4.29	85.77	19.682	0.000	الأول
2	تستخدم آليات تشفير لحماية البيانات.	3.87	77.32	9.387	0.000	السادس
3	توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي.	4.17	83.33	14.464	0.000	الثاني
4	تتم حماية البرامج المصدرية (SourceCode) المستخدمة.	3.97	79.38	10.663	0.000	الرابع
5	توفر قواعد البيانات المستخدمة مستويات أمنية متعددة.	3.96	79.18	11.961	0.000	الخامس
6	يتم وقاية النظام عن طريق برامج مكافحة الفيروسات.	4.12	82.47	13.939	0.000	الثالث
7	توجد برامج حماية لتتبع الاختراق والتسلل.	3.61	72.16	5.471	0.000	الثامن
8	هناك معايير لقبول أي أنظمة جديدة أو أي تعديلات، ويتم إجراء اختبارات عليها قبل القبول بها.	3.85	76.91	8.212	0.000	السابع
	جميع الفقرات	3.98	79.55	16.162	0.000	

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "96" تساوي 1.98

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات (الحماية البرمجية Software Security) تساوي3.98، و المتوسط الحسابي النسبي يساوي 79.55 % وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 16.162 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و والقيمة الاحتمالية تساوي0.000 وهي أقل من 0.05 مما يدل على أن توفر الحماية البرمجية يؤثر على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

وسيتم تفسير نتيجة كل فقرة من فقرات هذا المحور وفقاً لترتيب آراء المبحوثين في الكليات مجتمع الدراسة ترتيباً تنازلياً حسب المتوسط الحسابي النسبي لكل فقرة كما يلي:

1. يتبين ارتفاع النسبة الايجابية لآراء المبحوثين "يتم التحقق من صحة البيانات المدخلة "، ويعزو الباحث السبب إلى توفر بعض قواعد السلامة للمعلومات في الكليات التقنية و أهمية المعلومات الى توفرها الكليات، وربما تحتاج بعض أقسام الكليات الى مراجعة وتدقيق البيانات أكثر من مرة باختلاف نوع البيانات والجهة المستفيدة منها، كبيانات مالية أو درجات الطلاب ومعدلاتهم الدراسية وبيانات الموظفين و خصوصية الطلاب .

2. تؤكد هذه النسبة المرتفعة نسبياً للفقرة " توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي " توجه ونظرة الموظفين بضرورة توفير خدمات النسخ الاحتياطي مما يستنتج منه تولد شعور لدى العاملين يوحي بحرصهم على توفر وسلامة المعلومات، وتتفق الدراسة مع (تايه،2008 ؛ البحيصي والشريف،2008 ؛ القحطاني،2008؛ ONDER,2007) بنسبة كبيرة نحو أهمية توفير الأنظمة لخدمات النسخ الاحتياطي.

3. تبين نتيجة الفقرة " يتم وقاية النظام عن طريق برامج مكافحة الفيروسات" حرص الموظفين على حماية أجهزة الحاسوب التي يعملون عليها، ولعل مشاهدات الباحث أثناء قيامه بالمقابلات في الكليات التقنية وأسئلته بهذا الخصوص أكدت ذلك، ولكن يجدر القول أنه لا تتوافر في أي من الكليات برامج مرخصة تجارياً للحماية من الفيروسات، وربما على حد علم الباحث يعتبر هذا الأمر مسألة غير قانونية، بحكم أن غالبية منتجي مكافحات الفيروسات لا يوفرون برامج مجانية للمؤسسات، عدا على أن مثل هذه البرامج غير المرخصة قد تضر بأجهزة ونظم الحاسوب أكثر من نفعها .

4. أعطت نتيجة الفقرة "تتم حماية البرامج المصدرية (SourceCode) المستخدمة" دلالة على أن الكليات تقوم بهذا الدور بنسبة متوسطة إلى مرتفعة جزئياً وهذا يتفق مع دراسات (تايه،2008 ؛ العتيبي،2010 ؛ القحطاني،2008؛ Lane,2007) وربما جاءت دراسة ONDER (2007) بالنتيجة نفسها ولكنها لا تعتبر في ذلك عملاً من إختصاص العاملين على الأجهزة الطرفية حيث لا تتوافر أي من البرامج المصدرية على أجزاء النظام لديهم.

ويرى الباحث أن بعض نظم المعلومات في الكليات لا زالت تعمل بطريقة تستوجب من العاملين على هذه النظم، معرفة كيفية التعامل مع حماية البرنامج المصدري، وربما تتولد الحاجة هنا لتطوير هذه النظم في ظل دراسة دراسةONDER (2007) المتخصصة في هذا الجانب.

5. تعطي نتيجة الفقرة " توفر قواعد البيانات المستخدمة مستويات أمنية متعددة " دلالات بأن المبحوثين على علم بآليات الوصول لقواعد البيانات، وتبين النسبة المرضية تقريباً وجود تخوفات من سوء استخدام صلاحيات في مستوى أعلى من صلاحية الموظف نفسه في حال استطاع الحصول على كلمات المرور، وربما يكون تمهيداً لإجراء تهديد داخلي لنظام المعلومات.

6. تعليقاً على المتوسط المنخفض نسبياً لنتيجة الفقرة : " تستخدم آليات تشفير لحماية البيانات " يعزو الباحث سبب ذلك قلة ممارسة التشفير، بينما بينت الدراسة في خصائص وسمات مجتمع الدراسة سابقاً بأن ثلثي العاملين هم من المتخصصين في نظم المعلومات تقريباً، ويعزو الباحث ذلك إلى شعور نسبة غير قليلة من أفراد نظم المعلومات بعدم أهمية التشفير.

7. أتفقت نتيجة الفقرة: " هناك معايير لقبول أي أنظمة جديدة أو أي تعديلات، ويتم إجراء اختبارات عليها قبل القبول بها " جزئياً مع دراسة تايه(2008).

8. تبدو نتيجة الفقرة: " توجد برامج حماية لتتبع الاختراق والتسلل " شبه جيدة، ويربطها الباحث بقلة برامج التوعية الأمنية وهي ما تستوجب النظر إلى وجوب إهتمام إدارات مراكز الحاسوب (نظم المعلومات) في الكليات التقنية بزيادة البرامج والتدريب لتحسين فهم الموظف ومعرفته تجاه المهددات الخارجية لأمن نظم المعلومات.

ومما سبق نخلص إلى القول بأن نتائج عبارات المحور الفرعي (الحماية البرمجية Software Security) تدلل أن الآراء نحو أهميتها في تحسين إدارة أمن نظم المعلومات جيدة نسبياً، وهذا يدعو الكليات إلى توفير المزيد من الحماية البرمجية .

1.3- يؤثر توفر حماية الأفراد على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5-4) والذي يبين آراء أفراد عينة الدراسة في فقرات (حماية الأفراد Human Resources Security)

جدول رقم (5-4):تحليل فقرات المحور الأول/ حماية الأفراد Human Resources Security

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
1	يتوفر تدريب للعاملين على النظم المحوسبة بشكل دوري لتطوير مهارتهم المتعلقة بالمستجدات الأمنية.	3.36	67.22	3.285	0.001	الخامس
2	تحتوي وثيقة الوصف الوظيفي للموظف على مسؤلياته ومهامه تجاه أمن المعلومات في الكلية .	3.39	67.84	3.523	0.001	الرابع
3	يطلب من الموظف التوقيع على تعهد بعدم الافصاح عن معلومات حساسة تخص الكلية كجزء	3.32	66.39	2.509	0.014	السادس
4	يطلب من الموظفين والمتعاقدين الابلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.	3.56	71.13	4.947	0.000	الأول
5	هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.	3.43	68.66	3.817	0.000	الثالث
6	يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في	3.46	69.28	3.955	0.000	الثاني
	جميع الفقرات	3.41	68.25	4.518	0.000	

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "96" تساوي 1.98

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات (حماية الأفراد Human Resources Security) تساوي 3.41، و المتوسط الحسابي النسبي يساوي 68.25% وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 4.518 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و والقيمة الاحتمالية تساوي0.000 وهي اقل من 0.05 مما يدل على أن توفر حماية الأفراد يؤثر على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

وسيجرى ترتيب فقرات هذا المحور وفقاً لآراء المبحوثين في الكليات مجتمع الدراسة ترتيباً تنازلياً حسب المتوسط الحسابي النسبي لكل فقرة، وسيتم ذكرها وتفسيرها:

1. تؤكد نتيجة الفقرة : " يطلب من الموظفين والمتعاقدين الإبلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة " وجود تأثير لأمن الأفراد في واقع إدارة أمن نظم المعلومات.

2. تبين الفقرة : " يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في الكلية " أن هناك دور لتنامي تفعيل هذه الإجراءات في تطوير فاعلية أمن نظم

المعلومات في الكليات التقنية، ولربما ما بينته نتائج هذه الفقرة يتعارض كلياً مع دراسة تايه(2008) التي توصلت الى ان الأمن التنظيمي لا يؤثر في فاعلية أمن المعلومات .

3. يعزو الباحث إنخفاض النتيجة نسبياً في الفقرة " هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات " لعدم توفر وعي كامل لدى معظم إدارات الكليات تجاه قضايا ومتطلبات أمن نظم المعلومات، و تتفق ايجابية الاجابة على هذه الفقرة مع دراسة العتيبي(2010) .

4. يفسر الباحث انخفاض نسبة الاجابة على الفقرة " تحتوي وثيقة الوصف الوظيفي للموظف على مسؤلياته ومهامه تجاه أمن المعلومات في الكلية " بأن الكليات مجتمع الدراسة تختلف في جهات الاشراف عليها، فالحكومية منها تخضع لآليات التوظيف للحكومة ولا دخل مباشر للكليات فيها وربما تتشابه معها الوكالة إلى حد ما في شقها المركزي، بينما في الكليات العامة والخاصة تجد آليات التوظيف تنبع من حاجات الكلية ووفقاً للشروط التي تحددها، وربما أثر ذلك على آراء المبحوثين ونظرتهم تجاه أهمية محتوى وثيقة الوصف الوظيفي في تعزيز أمن نظم المعلومات.

5. تأتي نتيجة الفقرة " يتوفر تدريب للعاملين على النظم المحوسبة بشكل دوري لتطوير مهارتهم المتعلقة بالمستجدات الأمنية " لتضع هذه النسبة إدارات الكليات التقنية في موقف حرج كونها لا توفر أحد أهم مرتكزات نجاح البرامج الأمنية، وبالتالي يعتبر الباحث نقص تدريب العاملين على نظم المعلومات تجاه قضايا أمن المعلومات، هو بمثابة التهديد بل أنه المصدر الأساسي لنقاط ضعف نظم المعلومات.

6. ويعزو الباحث ضعف نتيجة إجابات المبحوثين على الفقرة : " يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص الكلية كجزء من شروط التوظيف" إلى إعتقاد المبحوثين بأن حساسية المعلومات في الكليات التقنية منخفضة كونها تتقضي سريتها بمرور الزمن، ولا يعد التصريح بها إنتقاصاً للخصوصية .

وتكاد تقترب نتيجة هذا المحور الفرعي من حالة شبه مقبولة تقريباً وبذلك ينصح أن تقوم الكليات بالمزيد من الجهد بشأن الإعتناء بالأمن التنظيمي لنظم المعلومات لتجنب ما يمكن أن يسببه الأفراد من تهديد داخلي حاد لنظم المعلومات، وما يميز هذه الدراسة هي كونها تناقش موضوع فني من جانب إداري بامتياز كونها تتلمس أضعف حلقة في نظم المعلومات وهي الأفراد بكافة تشكيلاتهم في تركيبة نظم المعلومات.

اختبار الفرضية الأولى الرئيسية : تؤثر حماية البنية التحتية لنظم المعلومات بصورة ايجابية على إدارة أمن نظم المعلومات عند مستوى دلالة إحصائية $\alpha = 0.05$

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5-5) والذي يبين آراء أفراد عينة الدراسة لجميع المحاور الفرعية للمحور الأول (حماية البنية التحتية لنظم المعلومات) .

جدول رقم (5-5) : تحليل المحاور الفرعية للمحور الأول/حماية البنية التحتية لنظم المعلومات

م.	المحاور الفرعية	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية
1	الحماية المادية Hardware Security	4.09	81.82	19.312	0.000
2	الحماية البرمجية Software Security	3.98	79.55	16.162	0.000
3	حماية الأفراد Human Resources	3.41	68.25	4.518	0.000
	جميع الفقرات	**3.84**	**76.90**	**14.149**	**0.000**

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "96" تساوي 1.98

و يتبين بصفة عامة أن المتوسط الحسابي لجميع المحاور الفرعية للمحور الأول تساوي 3.84، و المتوسط الحسابي النسبي يساوي 76.90 % وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 14.149 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و القيمة الاحتمالية تساوي0.000 وهي اقل من 0.05 مما يدل على أن حماية البنية التحتية تؤثر بصورة ايجابية على إدارة أمن نظم المعلومات عند مستوى دلالة إحصائية $\alpha = 0.05$

ويرى الباحث بأنه يتوفر لدى الكليات التقنية بنى تحتية مقبولة إلى حد ما على الأقل في شقيها (البرمجي، والمادي)، وعلى الرغم من ذلك فهي أيضاً بحاجة إلى تطوير لأن حماية البنية التحتية لنظم المعلومات مسألة في غاية الأهمية، كونها تضع الأساس الذي سيقوم عليه بناء النظام الأمني من الناحية المادية والفنية والبشرية، ويتفق تايه(2008)، Yeo etal(2007)، دراسة Jorro(2011)،دراسة العتيبي(2010)، ودراسة Bjorck(2005)، ودراسة Onder(2007) على أهمية تطوير البنى التحتية بشكل عام للتصدي للمخاطر بينما ركزت دراسة البحيصي والشريف(2008) على ضرورة الاهتمام بالحماية البرمجية .

الفرضية الثانية : يؤثر توفر سياسة لأمن المعلومات على إدارة أمن نظم المعلومات داخل الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5-6) والذي يبين آراء أفراد عينة الدراسة في فقرات المحور الثاني (سياسة أمن المعلومات)

جدول رقم (5-6):تحليل فقرات المحور الثاني/ سياسة أمن المعلومات

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
1	توجد في الكلية سياسة مكتوبة لأمن للمعلومات .	3.22	64.33	1.763	0.081	الخامس
2	يعرف الموظف بسياسة أمن المعلومات .	3.18	63.51	1.461	0.147	السادس
3	توجد جهة مكلفة بالإشراف على متابعة سياسة أمن المعلومات .	3.41	68.25	3.497	0.001	الثالث
4	يتم مراجعة وتطوير سياسة أمن المعلومات بشكل دوري .	3.38	67.63	3.169	0.002	الرابع
5	تدرك الإدارة العليا في الكلية أهمية سياسة أمن المعلومات.	3.86	77.11	8.705	0.000	الأول
6	يوجد إجراءات ضبط صارمة مطبقة على تنفيذ أي تغيرات على نظم المعلومات لحمايتها من العطل.	3.57	71.34	5.221	0.000	الثاني
	جميع الفقرات	3.43	68.69	4.435	0.000	

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "96" تساوي 1.98

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات المحور الثاني (سياسة أمن المعلومات) تساوي 3.43، و المتوسط الحسابي النسبي يساوي 68.69 % وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 4.435 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و والقيمة الاحتمالية تساوي 0.000 وهي أقل من 0.05 مما يدل على أن توفر سياسة لأمن المعلومات يؤثر على إدارة أمن نظم المعلومات داخل الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$

وسيجرى ترتيب فقرات هذا المحور وفقاً لآراء المبحوثين في الكليات مجتمع الدراسة ترتيباً تنازلياً حسب المتوسط الحسابي النسبي لكل فقرة، وسيتم ذكرها وتفسيرها:

1. يعزو الباحث هذه النتيجة المرتفعة نسبياً للفقرة : " الإدارة العليا في الكلية تدرك أهمية سياسة أمن المعلومات " مرتفعة نسبياً، إلى أن هنالك وعياً أمنياً في الكليات التقنية لا سيما التي تتبع الاشراف الحكومي والعام منها بخطورة ما قد يترتب على فقدان المعلومات، خاصة بعد وقوع بعض الأحداث المؤلمة وحوادث الاختراق و التهديدات المادية المباشرة وقضايا سرقة لدى بعض الكليات[13]، كما لاحظ الباحث تأثير التوجيهات التي تصدرها وزارة الاتصالات وتكنولوجيا المعلومات في غزة على بداية إهتمام الكليات بدور سياسة أمن المعلومات، وتتفق النتيجة مع دراسة العتيبي(2010)، و دراسة تايه(2008).

2. أتفقت نتيجة الفقرة :"يوجد إجراءات ضبط صارمة مطبقة على تنفيذ أي تغيرات على نظم المعلومات لحمايتها من العطل " مع دراسة jorro(2011).

3. كشفت نتيجة الفقرة : " توجد جهة مكلفة بالإشراف على متابعة سياسة أمن المعلومات " عن حداثة إدراك الادارات العليا لسياسة أمن المعلومات في الكليات التقنية، وتختلف نتيجة الفقرة مع دراسة العتيبي(2010)، دراسة تايه(2008)، Yeo etal.(2007)

4. بينت النتيجة الضعيفة نسبياً للفقرة: " يتم مراجعة وتطوير سياسة أمن المعلومات بشكل دوري" عجز الكليات عن فعل ذلك، حيث يرى الباحث أن عمليات مراجعة وتطوير سياسة أمن المعلومات تتصدر قائمة موازنة أمن نظم المعلومات لما تتطلبه من حسن معرفة بالأحداث المحيطة بالواقع، والتحليل المستمر لبيئة العمل، البرامج التدريبية والتوعوية لأفراد نظم المعلومات، وبحسب تقديرات الباحث فإن غالبية الكليات تعجز عن فعل ذلك و يرى الباحث ضرورة ملحة لقيام الكليات بالتنسيق مع جهات خارجية للقيام بذلك، وأقترحت دراسة العتيبي(2010) ودراسة القحطاني(2008) حلاً بإنشاء مركزاً عاماً للبحوث الأمنية يهتم بتطوير بيئات نظم معلومات آمنة ومستقرة، وتتفق مع هذا المقترح جزئياً دراسة Yeo etal(2007) ، وكذلك دراسة Lane(2007).

5. دللت سلبية نتيجة الفقرة :" توجد في الكلية سياسة مكتوبة لأمن للمعلومات" على عدم صحة الفقرة أي أنه لا توجد في الكليات سياسة مكتوبة لأمن للمعلومات، و ثبت من خلال المقابلات التي أجراها الباحث عدم إدراك بعض الكليات لأهمية تطبيق سياسة أمن المعلومات وبالتالي عدم وجودها ايضاً، ففي حين أن الكلية الجامعية للعلوم التطبيقية لديها سياسة أمن معلومات مطبقة لا يتوفر لدى الكليات الأخرى أي سياسات مكتوبة أو معلنة، ولهذا فإن الكليات التقنية بحاجة إلى إعادة النظر بوضع سياسات أمنية تمكنها من الحفاظ على أمن نظم المعلومات، لما لسياسة أمن

[13] يتحفظ الباحث على ذكر تفاصيل حول السرقات وقضايا التهديدات المادية، نزولاً عند رغبة الكلية، و يكتفي بذكر سنة الحادثة الأخيرة (2007)..

نظم المعلومات من أثر على فعالية إدارة أمن نظم المعلومات وهذا ما يتفق مع دراسة العتيبي(2010)، ودراسة Lane(2007).

6. تشير سلبية الفقرة : " الموظف يعرف بسياسة أمن المعلومات" على عدم صحة الفقرة أي أن الموظف لا يعرف بسياسة أمن المعلومات ويعزو الباحث سبب ذلك إلى أن أغلب الكليات كما تم ذكره لا يوجد فيها سياسات ناجحة لأمن المعلومات، وكذلك لقلة برامج التوعية الأمنية، ولعل هذا ما يتفق جزئياً مع دراسة Lane(2007).

وعليه يخلص الباحث للقول أن سياسة أمن المعلومات هي مؤثر فاعل في إدارة أمن نظم المعلومات فهي تمثل إطاراً لكل الأفعال المقبولة والممنوعة، وتعتني بضرورات التوفر والسلامة والسرية للمعلومات تبعاً للمعلومات محل الحماية وتبعا للآليات التقنية للعمليات محل الحماية، إلى جانب الأخذ بالاعتبار عناصر تكامل الأداء وعناصر الكلفة المالية وغيرها.

الفرضية الثالثة : يؤثر التحكم بالوصول لنظم المعلومات على إدارة أمن نظم المعلومات في الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5-7) والذي يبين آراء أفراد عينة الدراسة في فقرات المحور الثالث (التحكم بالوصول لنظم المعلومات)

جدول رقم (5-7) : تحليل الفقرات المحور الثالث/التحكم بالوصول لنظم المعلومات

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
1	صلاحيات الدخول للمعلومات تعطى حسب المستوى الإداري.	4.08	81.65	12.544	0.000	الثاني
2	لكل مستخدم هوية محددة خاصة به، حيث لا توجد حسابات عامة يستخدمها عدة أشخاص .	4.15	83.09	12.893	0.000	الأول
3	توجد مراجعات دورية لصلاحيات المستخدمين في الوصول للأنظمة.	3.87	77.32	8.748	0.000	الثالث
4	يُحجب الوصول إلى شبكة الانترنت أحياناً.	3.80	76.04	7.933	0.000	السادس
5	يمنع الوصول لبعض خدمات نظم المعلومات عبر الشبكات اللاسلكية.	3.81	76.29	8.347	0.000	الخامس
6	توجد إرشادات لطريقة إنشاء كلمات المرور القوية .	3.82	76.49	7.803	0.000	الرابع
7	بعض أنظمة المعلومات الحساسة معزولة في شبكات محلية مستقلة.	3.58	71.55	5.010	0.000	السابع

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
8	يتم إغلاق صلاحيات المستخدم بعد فترة محددة من انعدام نشاطها.	3.51	70.10	4.373	0.000	التاسع
9	تستخدم سجلات الأداء لحفظ أنشطة المستخدم لدواعي متعلقة بأمن المعلومات.	3.55	70.93	4.937	0.000	الثامن
	جميع الفقرات	3.80	75.95	11.886	0.000	

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "96" تساوي 1.98

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات المحور الثالث (التحكم بالوصول لنظم المعلومات) تساوي3.80،والمتوسط الحسابي النسبي يساوي 75.95% وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 11.86 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و والقيمة الاحتمالية تساوي 0.000 وهي اقل من 0.05 مما يدل على ان التحكم بالوصول لنظم المعلومات يؤثر على إدارة أمن نظم المعلومات في الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

وسيجرى ترتيب فقرات هذا المحور وفقاً لآراء المبحوثين في الكليات مجتمع الدراسة ترتيباً تنازلياً حسب المتوسط الحسابي النسبي لكل فقرة، وسيتم ذكرها وتفسيرها:

1. يلاحظ من نتيجة الفقرة : " لكل مستخدم هوية محددة خاصة به، حيث لا توجد حسابات عامة يستخدمها عدة أشخاص" أن استجابات المبحوثين نحو هذه الفقرة تشير بتوفر مرتفع نسبياً لعمليات التحقق من مستخدمي نظم المعلومات، ويرى الباحث بأن هوية المستخدم تحدد معالم وجوده ضمن نظم المعلومات، كما تلعب دوراً فاعلاً في كيفية تواصله وعمله في إطار نظام المعلومات، وتتفق نتيجة الفقرة مع دراسة العتيبي(2010) التي ترى في الهوية الخاصة بالمستخدم بمثابة خريطة مسارات يتم إعدادها بعناية ويسر.

2. تعطي نتيجة الفقرة : "صلاحيات الدخول للمعلومات تعطى حسب المستوى الإداري." دلالات حول معرفة المبحوثين بالمستويات الإدارية ومعرفتهم بوظائف وأجزاء نظم المعلومات .

3. تعليقاً على نتيجة الفقرة : " توجد مراجعات دورية لصلاحيات المستخدمين في الوصول للأنظمة" يضيف الباحث بأن عمليات المراجعة تتطلب معرفة المعنيين و اتصالهم بصناع القرار، لمعرفة طبيعة الأدوار والمهام المتغيرة للموظفين، وتتحدد عمليات المراجعة الدورية بقدرة مطوري نظم المعلومات في الكليات المختلفة على فهم الهيكل التنظيمي، و حسن تواصلهم مع إدارة الكلية وفق قواعد تحقق الأمن الفعال، ويرى Lane(2007) والعتيبي(2010) أهمية إجراء هذه المراجعات، في حين أضاف

تايه(2008) ووفق المعيار الأمني ISO17799 ضرورة فعل ذلك بشكل دوري محدد وأحياناً إحترازي طارئ .

4. تؤكد النسبة المرتفعة نسبياً في الفقرة :" توجد إرشادات لطريقة إنشاء كلمات المرور القوية " مدى اهتمام مراكز نظم المعلومات بمراعاة تطوير نظم قادرة على تحقيق خصوصيات أفراد نظم المعلومات، وتتفق نتائج الفقرة مع جاء في دراسة القحطاني(2008)، ودراسة العتيبي (2010)، ودراسة البحيصي والشريف(2008).

5. يتضح من النتيجة الايجابية للفقرة :"يمنع الوصول لبعض خدمات نظم المعلومات عبر الشبكات اللاسلكية " أنه بالرغم من عدم توفر خدمات الشبكات (الانترنت) اللاسلكية في غالبية الكليات مجتمع الدراسة وافق المبحوثون بغالبيتهم على هذه الفقرة ويتفق ذلك مع دراسة القحطاني(2008)، كما يتفق جزئياً مع دراسة عرفان نبي وآخرون(2010) التي أجريت كدراسة عملية حول امن المعلومات في المنظمات السعودية حيث بينت نتائج الدراسة حرص المنظمات على توفير الخدمات اللاسلكية لتسهيل التعاملات وأوصت بضرورة ضبط الوصول للشبكات اللاسلكية بشكل أكبر منه في الشبكات اللاسلكية، ويرى الباحث أن إيقاف الشبكات اللاسلكية بشكل مؤقت في الكليات التقنية مجتمع الدراسة يهدف لمنع الوصول الغير مسموح به و يأتي بعد عمليات من الرصد ومتابعة الشبكة، و يرى بعض رؤساء أقسام مراكز الحاسوب خلال مقابلات أجريت معهم من قبل الباحث أن نقل المعلومات عبر الشبكات اللاسلكية أمر يستوجب آليات معقدة من التشفير وفي غالبية الأوقات لا يسمح به، مع تأكيد البعض بأن نظم المعلومات التي يطورونها لا تحتوي نقاط ضعف تتعلق باستخدام الشبكات اللاسلكية(مقابلة سامر ياغي،2013)و(مقابلة مروان أبو شغيبة،2012).

6. رغم ما بينته عينة الدراسة من رأي مرتفع إلى حد ما نحو هذه الفقرة :" يُحجب الوصول إلى شبكة الانترنت أحياناً " فالكليات تحرص على توفير خدمات الانترنت بشكل آمن، ولكنها تمنع بعض الطرفيات من الإتصال بشبكة الانترنت لدرائع أمنية، واختلفت نتائج دراسة عرفان نبي وآخرون(2010) مع نتيجة هذه الفقرة، فيما يبرر ذلك باختلاف مجتمع الدراسة في كلتا الدراستين، وتوافر سياسة أمنية في غالبية مجتمع دراستهم .

ومن خلال المقابلات التي أجراها الباحث مع رؤساء أقسام مراكز الحاسوب يعتقد الباحث أن حجب الانترنت لن يؤثر على عمل نظم المعلومات في غالبية الكليات مجتمع الدراسة لأن هذه النظم والبرمجيات تعمل على الشبكات المحلية .

7. بينت إيجابية نتيجة هذه الفقرة : " بعض أنظمة المعلومات الحساسة معزولة في شبكات محلية مستقلة" توخي الكليات الحرص في تطبيق تصنيف للمعلومات من خلال هذا العزل، فمثلاً البيانات المالية و سجلات توقيعات الموظفين و أرشيف البرامج المصدرية المكتوبة وتحليلات نظم المعلومات وقاموس النظم، وقواعد بيانات أخرى خاصة تعتبر أمور سرية بدرجة متوسطة، ربما وجودها ضمن

الشبكات العامة يجعلها عرضة للانتهاك، وبذلك يرى الباحث ضرورة فصل وعزل نظم المعلومات الحساسة ، وتتفق مع دراسة Kreicberga(2010) على اهمية عزل نظم المعلومات التي تقدم معلومات حساسة.

8. تتفق نتيجة الفقرة " سجلات الأداء تستخدم لحفظ أنشطة المستخدم لدواعي متعلقة بأمن المعلومات " مع Yeo etal.(2007) .

ويسعى مطورو النظم في الكليات التقنية لتحقيق مزايا جديدة ضمن نظم المعلومات، وإن كانت الإمكانات التقليدية التي تقدمها النظم الحالية كفيلة بذلك مثل "LOG files" سجلات الأداء، ويرى بعض رؤساء أقسام مراكز الحاسوب (مطوري نظم المعلومات) ضرورة التخلي عن تعزيز الموظف المخل بالنظام لضمان استمرارية قبوله للأنظمة (مقابلة مراون أبو شغيبة، 11-2012).

9. يرى الباحث في نتيجة الفقرة : " يتم إغلاق صلاحيات المستخدم بعد فترة محددة من انعدام نشاطها " أمراً مطمئناً بدلالته على توافر الأمن ضمن نطاق صلاحيات المستخدم، ويرى Kreicberga(2010)، القحطاني(2008)، العتيبي(2010) اهمية تطبيق هذه الفقرة.

ويضيف الباحث أنه يمكن الخروج بعدة استنتاجات استناداً لتحليلات هذا المحور الهام، ومستنداً إلى ما جاء في المقابلات، تختلف الكليات التقنية بممارساتها تجاه قضايا التحكم بالوصول لنظم المعلومات، في حين تتفق بنسبة مرتفعة نسبياً برؤيتها نحو تعزيز أمن نظم المعلومات عبر اعتبارا التحكم بالوصول لنظم المعلومات أحدى الزوايا الهامة المؤثرة في تحسين إدارة أمن نظم المعلومات، وعليه يخلص الباحث إلى الأهمية المتزايدة لضبط الوصول لشبكات المعلومات، والوصول للانترنت مع التركيز على ضرورة التوفيق بين أمن النظم كخط أحمر، وضروريات التوفر والحصول على المعلومات للمستخدم والمستفيد، والنظر الى سلامة وسرية وخصوصية بيانات ومعلومات الكليات .

الفرضية الرابعة: يؤثر توفر الإجراءات التنظيمية لضبط نظم المعلومات على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5-8) والذي يبين آراء أفراد عينة الدراسة في فقرات المحور الرابع (الإجراءات التنظيمية) .

جدول رقم (5-8):تحليل الفقرات المحور الرابع: الإجراءات التنظيمية

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
1	يتم إحاطة الموظف بإجراءات التأمين الوقائية.	3.54	70.72	4.643	0.000	الثامن
2	يوجد دليل تصنيف للمعلومات يمكن أن يساعد في تحديد كيفية التعامل مع المعلومات وحمايتها .	3.24	64.74	2.110	0.037	التاسع
3	تحتفظ الكلية بسجلات حول الأصول المكونة لكل نظام معلومات.	3.80	76.08	7.867	0.000	الثالث
4	يتم تحديد الأحداث التي تؤدي إلى توقف نظم المعلومات في الكلية عن العمل، بهدف تقدير مخاطر تلك الأحداث ووضع خطط طوارئ لإستعادة العمل.	3.63	72.58	5.718	0.000	السادس
5	في حال حدوث إخفاق أو انقطاع في أداء الأعمال توجد خطط لإعادة الأعمال إلى طبيعتها ضمن إطار زمني مخطط .	3.65	72.99	6.143	0.000	الخامس
6	يتم تسجيل ما يحدث من أخطاء في نظم المعلومات في تقارير، ويتم ذكر الإجراءات التي اتخذت لتصحيحها.	3.63	72.58	5.769	0.000	السابع
7	يتم عمل نسخ احتياطي للمعلومات بشكل دوري.	4.06	81.24	11.073	0.000	الأول
8	يوجد آليات للإبلاغ عن الحوادث ذات العلاقة بأمن المعلومات.	3.69	73.81	7.328	0.000	الرابع
9	يجري منع الموظف من استخدام المعلومات للإغراض غير المصرح بها.	3.96	79.18	10.916	0.000	الثاني
	جميع الفقرات	3.69	73.77	8.487	0.000	

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "96" تساوي 1.98

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات المحور الرابع (الإجراءات التنظيمية) تساوي 3.69، و المتوسط الحسابي النسبي يساوي 73.77 % وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 8.487 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و والقيمة الاحتمالية تساوي 0.000 وهي اقل من 0.05 مما يدل

على إن توفر الإجراءات التنظيمية لضبط نظم المعلومات يؤثر على إدارة أمن نظم المعلومات بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

وسيجرى ترتيب فقرات هذا المحور وفقاً لآراء المبحوثين في الكليات مجتمع الدراسة ترتيباً تنازلياً حسب المتوسط الحسابي النسبي لكل فقرة، وسيتم ذكرها وتفسيرها:

1. يشير إرتفاع استجابة المبحوثين إيجابياً في الفقرة " يتم عمل نسخ احتياطي للمعلومات بشكل دوري " إلى أن الاجرءات الوقائية لحماية النظم قائمة بنسبة مرتفعة، وهو ما يؤكد وجود حالة من سياسات الإسترداد والإستعادة للنظم، وتتفق نتيجة الفقرة مع دراسة العتيبي(2010) بشكل كبير ويذكر أن عدم وجود نظام موحد وسياسة محددة للقيام بالنسخ الاحتياطي سيؤدي إلى فوضى، وتتفق بدرجة متوسطة مع دراسة القحطاني (2008) وكذلك البحيصي والشريف(2008) .

2. تناولت الفقرة : " يجري منع الموظف من استخدام المعلومات للإغراض غير المصرح بها " جانباً من الصلاحيات، ولعلها بذلك تعطي دلالة على تطبيق أنظمة المعلومات لجوانب الصلاحيات في حيز من الاجراءات التنظيمية، وتتفق النتيجة بنسبة كبيرة مع دراسة القحطاني(2008) كون مجتمع الدراسة يشمل عدداً من المؤسسات العسكرية .

3. تعطي نتيجة الفقرة: " الكلية تحتفظ بسجلات حول الأصول المكونة لكل نظام معلومات " دلالة على تطبيق نظام العهد بنسبة مرتفعة نسبياً، حيث تخضع الأصول المعلوماتية في الكليات التقنية عموماً والحكومية منها بشكل خاص الى نظام العهد ويقوم قسم اللوازم في الكليات بعمليات جرد العهد وتنسب كل عهدة لصاحبها ويكون مسئولاً عنها، ومن شأن هذا الاجراء التنظيمي أن يعزز من موثوقية إتصال الأجهزة بنظام المعلومات، وجاءت دراسة تايه(2008) ودراسة القحطاني(2008) بنفس النتيجة.

4. يعزو الباحث هذه النتيجة المتوسطة للفقرة : "يوجد آليات للإبلاغ عن الحوادث ذات العلاقة بأمن المعلومات " لعدم وجود تنسيق ومتابعة من قبل الادرات العليا مع القائمين على نظم المعلومات بخصوص ضبط الأمن التنظيمي.

5. تدلل نتيجة الفقرة : " في حال حدوث إخفاق أو انقطاع في أداء الأعمال توجد خطط لإعادة الأعمال إلى طبيعتها ضمن إطار زمني مخطط " على حسن ممارسة عمليات الإستعادة وإعادة الأعمال إلى طبيعتها ضمن إطار زمني مخطط و هو ما يؤكد سعي إدارات الكليات لتعزيز الاجراءات التنظيمية المتعلقة بمراجعات وأمن نظم المعلومات، وتتفق النتيجة جزئياً مع دراسة القحطاني(2008)، والعتيبي(2010).

6. تأتي النتيجة في الفقرة : "يتم تحديد الأحداث التي تؤدي إلى توقف نظم المعلومات في الكلية عن العمل، بهدف تقدير مخاطر تلك الأحداث ووضع خطط طوارئ لإستعادة العمل" لتؤكد ما بينته المقابلات من ممارسة القائمين على نظم المعلومات ممثلين (على الأقل فنياً) بأقسام مراكز الحاسوب من أن الكليات التقنية مجتمع الدراسة في مجملها تقوم بعمليات دراسة للمخاطر ولكن ليس بالمستوى المطلوب، ولعل هذا النشاط يعزى لشعور عام لدى الكليات بأهمية المعلومات ومخاطر فقدانها في ضوء تهديدات قد توقع الخطر وربما أشدها التهديد المادي المباشر المقصود كقصف طائرات الاحتلال الاسرئيلي، وبينت دراسة البحيصي والشريف(2008) مقاربة في النتيجة وبنسبة أعلى لكون مجتمع الدراسة من البنوك والمؤسسات المالية التي يوجد لديها متخصصون في إدارة المخاطر أو مؤسسات استشارية لديها علاقات مباشرة معها .

7. ترشد النسبة المقبولة نسبياً " يتم تسجيل ما يحدث من أخطاء في نظم المعلومات في تقارير، ويتم ذكر الإجراءات التي اتخذت لتصحيحها " الباحث لاستنتاج دلالة ولو بقدر متوسط على وجود آليات لتنظيم عمليات أمن المعلومات في سبيل إيجاد طرق للإستعادة عند حدوث مشاكل في النظم، وتقترب نتيجة الفقرة من ما توصلت اليه دراسة تايه(2008).

8. تباينت نتيجة هذه الفقرة : " يتم إحاطة الموظف بإجراءات التأمين الوقائية " في الدراسات السابقة ويرجع ذلك لاختلاف مجتمع الدراسة في الدراسات التي تناولت الفقرة، فدراسة العتيبي (2010) بينت نسبة مرتفعة، بينما دراسة القحطاني(2008) اعتبرته مهدداً للأمن المعلوماتي بنسبة متوسطة.

9. تعطي هذه النتيجة المنخفضة نسبياً للفقرة : " يوجد دليل تصنيف للمعلومات يمكن أن يساعد في تحديد كيفية التعامل مع المعلومات وحمايتها " دلالات واضحة على أن الكليات لا تبلي كثيراً من الأهمية تجاه تصنيف المعلومات، وعلى ذلك أعطت النتيجة دلالة على وجود معوقات في تنظيم الاجراءات الأساسية لأمن المعلومات، ولعل هذا ما تؤكده دراسة تايه(2008) التي جاءت لفحص مدى الفاعلية للتوافق مع المعيار القياسي لأمن المعلومات ISO17799، وكذلك توافقت مع دراسة العتيبي(2010) بنسبة كبيرة حيث طبقت على مجتمع دراسة أكثر التزاماً من الناحية الأمنية مما استوجب وجود تصنيفاً للمعلومات حسب الأهمية، وحسب المستفيدين.

وعليه يخلص الباحث للقول أن توفر الإجراءات التنظيمية لضبط نظم المعلومات هي مؤثر فاعل في إدارة أمن نظم المعلومات فهي بمثابة الراعي والمنظم لعمليات تبادل ونقل المعلومات و مدخل الإدارة العليا للحفاظ على عمل نظم المعلومات، حيث تضع خطط الطوارئ والإستعادة، وتعتني بضرورات التوفر والسلامة والسرية للمعلومات وفق رؤيتها وسلامة مساراتها، ووفق ما لديها من إمكانات مالية وبشرية وفنية.

الفرضية الخامسة : يؤثر استخدام التعهيد في نظم المعلومات IT- Outsourcing على إدارة أمن نظم المعلومات في الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5-9) والذي يبين آراء أفراد عينة الدراسة في فقرات المحور الخامس (التعهيد (الاستعانة بالمصادر الخارجية)) .

جدول رقم (5-9): تحليل الفقرات المحور الخامس/ التعهيد (الاستعانة بالمصادر الخارجية)

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
1	يوجد تعاقد مع أطراف خارجية في مجال تطوير نظم المعلومات في الكلية.	3.62	72.37	5.065	0.000	الأول
2	تقوم الكلية بالاستعانة بخبراء في مجالات نظم المعلومات للحصول على استشارات في أمن المعلومات.	3.49	69.90	4.548	0.000	الرابع
3	تتم مراقبة عمليات تطوير البرامج التي تنفذها الأطراف الخارجية .	3.48	69.69	4.869	0.000	الخامس
4	يطلب من الجهات الخارجية الإبلاغ عن أي ثغرات أمنية يلاحظونها في الأنظمة.	3.52	70.31	4.463	0.000	الثالث
5	يتم التحقق من قيام الأطراف الخارجية المتعاقدة بتنفيذ الضوابط الأمنية المتفق عليها.	3.47	69.48	4.666	0.000	السادس
6	يجري مراقبة أداء الاطراف الخارجية عند إجراء	3.58	71.55	6.491	0.000	الثاني
	جميع الفقرات	3.53	70.55	5.981	0.000	

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "49" تساوي 2.01

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات المحور الخامس تعهيد نظم المعلومات تساوي3.53، و المتوسط الحسابي النسبي يساوي 70.55% وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 5.981 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 و والقيمة الاحتمالية تساوي 0.000 وهي أقل من 0.05 مما يدل على أن استخدام التعهيد في نظم المعلومات IT- Outsourcing يؤثر على إدارة أمن نظم المعلومات في الكليات التقنية بصورة ايجابية عند مستوى دلالة إحصائية $\alpha = 0.05$.

وسيتم تفسير كل فقرة من فقرات هذا المحور وفقاً لترتيب آراء المبحوثين في الكليات مجتمع الدراسة ترتيباً تنازلياً حسب المتوسط الحسابي النسبي لكل فقرة كما يلي:

1. يرى الباحث في نتيجة الفقرة: " يوجد تعاقد مع أطراف خارجية في مجال تطوير نظم المعلومات في الكلية " نسبة واقعية تمثل واقع ما هو ماثل من ممارسات في تطوير نظم المعلومات، فقد بينت المقابلات التي أجراها الباحث مع الكليات التقنية مجتمع الدراسة وجود استخدام للتعهيد بشكله المباشر الكبير في الكلية العربية للعلوم والتكنولوجيا، وبنسبة متوسطة في كلية العلوم والتكنولوجيا، وجزئياً في كلية تدريب غزة بإشراف مركزي من المركز في عمان – الأردن، وهذا بدوره يؤكد أن حاجات الكليات من تطوير نظم المعلومات يحدث تفاوتاً في درجات استخدام التعهيد.

2. قصد الباحث في هذه الفقرة : " يجري مراقبة أداء الأطراف الخارجية عند إجراء الصيانة " استنتاج مدى تعاطي العاملين في نظم المعلومات وإحساسهم تجاه تعهيد بعض أنظمة كليتهم لجهات خارجية، وتبين النتيجة حرصاً بنسبة متوسطة في هذا الجانب وربما لم تتطرق الكثير من الدراسات السابقة للحديث حول دور التعهيد في أمن نظم المعلومات، ولعل الدراسة التي أجراها العتيبي (2010) أفضت إلى نفس النتيجة تقريباً، مع ملاحظة أن قضايا تعهيد نظم المعلومات لم تكن من محاور دراسة العتيبي.

3. تعطي النتيجة في الفقرة : " يطلب من الجهات الخارجية الإبلاغ عن أي ثغرات أمنية يلاحظونها في الأنظمة " دلالات على أن الكليات التقنية تمارس عملياً رقابة بنسبة معقولة على الأنشطة التي تقوم بها جهات خارجية، وأنه يوجد لدى الكليات حرص على قضايا أمن المعلومات، وتسعى للحفاظ على استقرار نظم المعلومات.

4. يعزو الباحث النسبة المنخفضة في الفقرة: "الكلية تقوم بالاستعانة بخبراء في مجالات نظم المعلومات للحصول على استشارات في أمن المعلومات " لربما إلى قلة حدوث قضايا أمنية مربكة، وأن كل ما تواجهه الكليات لا تعجز عن حله، ولكن الباحث يعتقد أنه رغم وجود الكفاءات داخل معظم الكليات، إلا أن الحاجة للاستزادة والمعرفة المتعلقة بالأمن المعلوماتي وإيجاد الحلول تتطلب وجود استشارات ، وقد تعطي هذه النتيجة دلالات على تدني الاستعانة بالمصادر الخارجية بشكل عام.

5. أشارت النتيجة الضعيفة للفقرة :" تتم مراقبة عمليات تطوير البرامج التي تنفذها الأطراف الخارجية " إلى تردي أنشطة الرقابة على عمليات التطوير البرمجي الذي ينفذه المتعهدون.

6. يرى الباحث أن النتيجة المنخفضة نسبياً للفقرة : " يتم التحقق من قيام الأطراف الخارجية المتعاقدة بتنفيذ الضوابط الأمنية المتفق عليها" تفضي إلى استنتاجات أهمها تخوفات لدى الكليات من عمليات التعهيد ونظام التعاقد المعمول به، وقد أكدت نتائج المقابلات التي أجراها الباحث مع

الكليات مجتمع الدراسة إلى وجود حالة من عدم الارتياح تجاه القواعد المعمول بها في حالات التعهيد الموجودة، وأن المتعهدين قليلاً ما يلتزموا بالقواعد الأمنية بما أوكل لهم من برامج لتطويرها، و منهم من أعتبر أن مفهوم التعهيد يتناقض مع الأمن، وربما هذا يلخص انخفاض النتيجة على هذه الفقرة .

وعليه يخلص الباحث للقول أن استخدام تعهيد نظم المعلومات هي ليست حالة عامة كلياً في الكليات، ومن نتائج المقابلات تبين أن الكليات التقنية التي تستخدم التعهيد تسعى إلى الاستغناء عنه، وتبقى فئة الكليات التقنية التي تتبع الاشراف الخاص هي الأكثر اقتناعاً وارتباطاً بمفهوم التعهيد، بينما تتوقع الكليات الحكومية الاستغناء عنه أو إيقاف التعامل به ضمن القواعد الحالية في وقت قريب . ويرى الباحث من منظور التكاليف أن استخدام التعهيد في نظم المعلومات أكثر وفرة وأقل تكلفة، ولكنه من منظور تحقيق الأمن لنظم المعلومات على الوجه الذي يحقق السرية و السلامة والتوفر "CIA– Triangle" يعتبر أحدى الإشكاليات التي تحتاج إلى مزيداً من الضبط والمراجعة من أجل إنتاج نظم أكثر أمناً، وفي دراسة Kazemi etal.(2012) التي ناقشت تقييم عوامل نجاح إدارة أمن نظم المعلومات توصلت بأن استخدام التعهيد(الاستعانة بالمصادر الخارجية) هو العامل الأقل أولوية في إنجاح إدارة أمن نظم المعلومات وهذا يتفق مع نتيجة المحور بشكل عام مقارنة مع ما ذكر من محاور مؤثرة على إدارة أمن نظم المعلومات .

الفرضية السادسة : تتوفر طرق وسبل جيدة لتطوير إدارة أمن نظم المعلومات في الكليات التقنية عند مستوى دلالة إحصائية $\alpha = 0.05$.

تم استخدام اختبار t للعينة الواحدة والنتائج مبينة في جدول رقم (5–10) والذي يبين آراء أفراد عينة الدراسة في فقرات المحور السادس (سبل تطوير إدارة أمن نظم المعلومات في الكلية)

جدول رقم (5–10) :تحليل الفقرات المحور السادس/ سبل تطوير إدارة أمن نظم المعلومات في الكلية

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
1	تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمن نظم المعلومات.	4.28	85.57	19.153	0.000	الثاني
2	زيادة الموازنة المخصصة لأمن المعلومات ضمن موازنة تكنولوجيا المعلومات	4.11	82.27	12.684	0.000	السابع
3	فحص أنظمة المعلومات للتحقق من الالتزام بمعايير الأداء الأمني.	4.23	84.54	16.576	0.000	الثالث
4	استخدام برامج حماية فعالة لمنع محاولات الاختراق والتعدي على نظم المعلومات في الكليات.	4.34	86.80	20.507	0.000	الأول

م.	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	الترتيب
5	توفير الحوافز (المادية والمعنوية) المناسبة للمبدعين والمتفوقين في مجال أمن نظم المعلومات.	4.10	82.06	10.700	0.000	الثامن
6	استقطاب خبراء حماية نظم المعلومات للعمل بمراكز نظم المعلومات بالكليات التقنية.	4.19	83.71	14.453	0.000	الخامس
7	دعم الإدارة العليا لسياسة ناجحة لأمن المعلومات.	4.22	84.33	14.854	0.000	الرابع
8	اعتماد استخدام الوسائل البيولوجية (بصمة الأصبع، أو بصمة العين، أو التعرف على الوجه) في تحديد شخصية وصلاحية مستخدمي نظم المعلومات.	3.59	71.75	4.355	0.000	العاشر
9	وضع ضوابط لتبادل المعلومات مع الجهات المعنية خارج الكلية.	4.18	83.51	14.889	0.000	السادس
10	الاستفادة من خدمات (التعهيد) الأطراف الخارجية ضمن ضوابط أمنية وشروط جزائية متفق عليها.	4.02	80.41	13.408	0.000	التاسع
		4.12	82.49	18.019	0.000	

قيمة t الجدولية عند مستوى دلالة 0.05 ودرجة حرية "49" تساوي 2.01

وبصفة عامة يتبين أن المتوسط الحسابي لجميع فقرات المحور السادس (سبل تطوير إدارة أمن نظم المعلومات في الكلية) تساوي4.12، والمتوسط الحسابي النسبي يساوي82.49% وهي أكبر من المتوسط الحسابي النسبي المحايد " 60% " وقيمة t المحسوبة المطلقة تساوي 18.019 وهي أكبر من قيمة t الجدولية والتي تساوي 1.98 والقيمة الاحتمالية تساوي0.000 وهي اقل من 0.05 مما يدل على أنه : تتوفر طرق وسبل جيدة لتطوير إدارة أمن نظم المعلومات في الكليات التقنية عند مستوى دلالة إحصائية $\alpha = 0.05$.

وسيجرى ترتيب فقرات هذا المحور وفقاً لآراء المبحوثين في الكليات مجتمع الدراسة ترتيباً تنازلياً حسب المتوسط الحسابي النسبي لكل فقرة، وسيتم ذكرها وتفسيرها:

1. تبين النتيجة في الفقرة : " استخدام برامج حماية فعالة لمنع محاولات الاختراق والتعدي على نظم المعلومات في الكليات " ارتفاعاً نسبياً في رأي أفراد نظم المعلومات المبحوثين في الكليات تجاه هذه الفقرة كأحد سبل التطوير، وتتفق النتيجة بنسبة كبيرة مع دراسة القحطاني(2008) وإن جاءت في المرتبة الثانية من بين عشر "10" نقاط طرحها القحطاني.

2. بالربط مع نتيجة الفقرة السابقة أعطت نتيجة هذه الفقرة :" تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمن نظم المعلومات " دلالات بأن رأي المبحوثين قد ركز على تطوير الجانب البرمجي بنسبة أكثر من تطوير الجانب المادي، وربطاً مع ما بينته نتائج المحور

البرمجي كمؤثر فاعل في واقع إدارة أمن نظم المعلومات التي أعطت متوسطاً نسبياً أقل من متوسط المحور المادي مما يدلل على إتزان آراء المبحوثين والصدق النسبي للنتائج.
بينما بينت دراسة القحطاني(2008) أن هذه الفقرة كانت في الترتيب الأول لآراء المبحوثين.
ويرى الباحث أنه أي كانت سبل التطوير برمجية أو مادية فهي في النهاية تطويراً للبنى التحتية لنظم المعلومات وتستوجب وضع خطط واستراتيجيات ربما متصلة أحياناً لأنه لا غنى عن أي منهما حيث تربطهما علاقة تكامل والمستفيد المكون الأساسي لنظام المعلومات إلا وهو الأفراد .

3. لعل آراء المبحوثين العالية تجاه أهمية هذه الفقرة : " فحص أنظمة المعلومات للتحقق من الالتزام بمعايير الأداء الأمني " تشير إلى نظرة أفراد نظم المعلومات إلى تحسين الجودة، حيث يرى Bjorck(2005) أهمية هذه الخطوة في تعزيز جودة نظم المعلومات، وتتفق دراسة العتيبي(2010) جزئياً مع النتيجة، وفي تقرير ISF(2007) ذكرت عدة مجالات أساسية لتطوير وتحسين أمن نظم المعلومات، بينما ISO/IEC20007(2005) حددت 10 مجالات أساسية لقياس مدى فعالية إدارة أمن نظم المعلومات .

4. يعزو الباحث ارتفاع إجابات مجتمع الدراسة في الفقرة : "دعم الإدارة العليا لسياسة ناجحة لأمن المعلومات " لشعور العاملين بأن هناك تقصيراً جزئياً لدى الإدارات العليا تجاه تحسين أمن نظم المعلومات، وأتفقت النسبة جزئياً مع دراسة القحطاني(2008) .

5. يبرر الباحث إعتقاد المبحوثين بأهمية نتيجة إيجابية هذه الفقرة : " استقطاب خبراء حماية نظم المعلومات للعمل بمراكز نظم المعلومات بالكليات التقنية " في ظل آراء المبحوثين في فقرة سابقة حول واقع الاستعانة الخارجية بالاستشارات التي تبين أنها متدنية نسبياً، وظهرت نتيجة هذه الفقرة متوافقة تماماً مع دراسة القحطاني(2008).

6. كشفت نتيجة هذه الفقرة : " وضع ضوابط لتبادل المعلومات مع الجهات المعنية خارج الكلية " بأن المبحوثين يشعرون بإن علاقة الكليات مجتمع الدراسة مع الأطراف ذات الصلة "Stackholders" بحاجة إلى تنظيم، وتتوافق هذه النتيجة مع دراسة عرفان نبي وآخرون(2010) التي أوصت بضرورة وضع ضوابط ضمن سياسة أمن المعلومات للتعامل مع الجهات الخارجية، وأظهرت دراسة Lane(2007) أهمية أن تشمل الثقافة الأمنية من هم خارج المؤسسة من خلال مراجعة سياسات التعامل الخارجي لاسيما وأن نظم المعلومات لا تعرف الحدود وتزداد نقاط الضعف كلما زادت الأدوار واتسعت مساحات عمل المستخدمين، بينما أعتبرت دراسة Kreicberga(2010) أن الثقة الداخلية المفرطة بين زملاء العمل في نظم المعلومات أشد خطراً على النظم من التعاملات الخارجية، ويعزو الباحث ذلك لكون الدراسة ركزت على الجانب السلوكي للتهديدات الداخلية.

7. تتفق آراء المبحوثين ومن أجريت معهم المقابلات على أهمية النتيجة الإيجابية لهذه الفقرة : " زيادة الموازنة المخصصة لأمن المعلومات ضمن موازنة تكنولوجيا المعلومات" في تطوير أمن نظم المعلومات، حيث أنه عند سؤال المبحوثين عن تقديرهم لنسبة الموازنة المالية المخصصة لأمن نظم المعلومات من الموازنة الكلية لنظم المعلومات في فقرة سابقة تبين أن نسبة تتجاوز النصف أبدت تقديراً "بنسبة متوسطة"، وبذلك فإن إحساساً يتولد لدى المبحوثين بضرورة دعم موازنات أمن المعلومات في الكليات التقنية، ويشير الباحث أن نتائج المقابلات التي أجريت مع رؤساء أقسام الحاسوب المُطورة لنظم المعلومات داخل الكليات تمنت زيادة الموازنات أيضاً، وكانت دراسة تايه(2008) قد أشارت إلى تأثير ضعف الموازنات السنوية المخصصة على فاعلية أمن المعلومات .

8. جاءت دراسة القحطاني بنتيجة أعلى نسبياً تجاه هذه الفقرة : " توفير الحوافز (المادية والمعنوية) المناسبة للمبدعين والمتفوقين في مجال أمن نظم المعلومات "، ويعزو الباحث ذلك إلى إختلاف الأنماط الإدارية السائدة في كلا المجتمعين.

وينظر إلى هذه النتيجة من زاوية دعم الإدارة العليا للمتميزين مما يزيد من فعالية وأداء أمن النظم، ويجب الاشارة لأهمية تشجيع المتميزين في أمن المعلومات من خلال توفير الحوافز المادية والمعنوية من أجل حفزهم على زيادة فعاليتهم وإقبالهم على العمل.

9. دللت صحة الفقرة : " الاستفادة من خدمات التعهيد (الأطراف الخارجية) ضمن ضوابط أمنية وشروط جزائية متفق عليها " على أنه لا يمكن إغلاق الباب كلياً أمام خيار تعهيد نظم المعلومات، ففي حين تقدر موازنات بعض الكليات على دفع فاتورة تطوير نظم معلوماتها بذاتها، نجد كليات أخرى تعتقد أن خيار تعهيد نظم معلوماتها بالكامل لأطراف خارجية هو أقل تكلفة وأفضل حالاً من التكاليف التي ستدفعها في حال ذاتية التطوير كرواتب مهندسي النظم و تكلفة أجهزة الخوادم (Servers) وعبء النسخ الاحتياطي الأساسي، وما يلحق بصيانة هذه المرفقات، وألخ..

وربما تجد بعض الكليات التي تشرف عليها جهات خاصة خيار تعهيد نظم المعلومات كلياً أنسب وأقل تكلفة وأكثر مرونة، ولعل الكليات الأخرى تطبق جزئياً بعض خدمات التعهيد التي ترى فيها داعمة لأمن نظم معلوماتها.

10. تدنت نتيجة هذه الفقرة : " اعتماد استخدام الوسائل البيولوجية (بصمة الأصبع، أو بصمة العين، أو التعرف على الوجه) في تحديد شخصية وصلاحية مستخدمي نظم المعلومات " بسب تخوفات المبحوثين من تعقيدات استخدام التقنيات الجديدة في جانبها الحيوي لاعتقاد البعض بأثرها الصحي وربما تأتي مقاومة التغيير عاملاً آخر، كما أن نتائج المقابلات قد قللت من أهمية إستخدام هذه الوسائل لمبررات تكلفتها العالية، وكانت نتيجة دراسة القحطاني(2008) قد أبدت تاييداً أعلى

لاستخدام هذه الوسائل ويعزو الباحث ذلك لمدى اختلاف حساسية المعلومات ، في حين يرى الهادي(2006) أن استخدام هذه التقنيات والوسائل يتزايد باستمرار .

ويضيف الباحث أن السبل والوسائل التي تم ذكرها في محور "سبل ووسائل التطوير" في الاستبانة، تم دراساتها بعناية إستناداً إلى نتائج مجموعة من الدراسات السابقة، وأستفاد الباحث من المقابلة التجريبية (مقابلة مروان أبو شغيبة،2012) في الاعداد الأولي لفقرات المحور، ثم عرضت على مجموعة من المختصين في كلية فلسيطن التقنية، ثم جرى تحكيمها بجانب فقرات المحاور الأخرى، وأتفقت نتائج المحور بنسبة كبيرة مع دراسة القحطاني(2008).

وبذلك يتوصل الباحث إلى تأييد كبير من عينة الدراسة نحو سبل تطوير إدارة أمن نظم المعلومات و إعتبار هذه الوسائل والسبل هي طريقاً مدروساً لتطوير أمن نظم المعلومات في الكليات التقنية، ومن الأهمية هنا أن تستخدم هذه السبل والوسائل كما رتبتها نتائج الدراسة.

الفرضية السابعة: لا توجد فروق ذات دلالة إحصائية في آراء عينة الدراسة عند مستوى دلالة إحصائية $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى للمتغيرات التالية : (الكلية، الموازنة الأمنية لكل كلية، مستوى التدريب، مدى توافر إدارة لأمن نظم المعلومات، العمر، سنوات الخبرة، المؤهل العلمي، التخصص العلمي).

وينبثق من هذه الفرضية الفرضيات الفرعية التالية:

7.1: لا توجد فروق ذات دلالة إحصائية عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى الكلية :

تم استخدام اختبار تحليل التباين الأحادي (One Way ANOVA)لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى الكلية عند مستوى $\alpha = 0.05$. والنتائج مبينة في جدول رقم (5-11).

جدول رقم (5-11): نتائج تحليل التباين الأحادي في رؤية المبحوثين لواقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى متغير "الكلية".

عنوان المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة "F"	القيمة الاحتمالية
واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها	بين المجموعات	6.944	4	1.736	6.606	0.000
	داخل المجموعات	24.177	92	0.263		
	المجموع	31.121	96			

قيمة F الجدولية عند درجة حرية "4، 92" ومستوى دلالة 0.05 تساوي 2.47

ويتبين أن قيمة F المحسوبة لجميع المحاور مجتمعة تساوي 6.606 وهي أكبر من قيمة F الجدولية والتي تساوي 2.47، كما أن القيمة الاحتمالية لجميع المحاور تساوي 0.000 وهي اقل من 0.05 مما يدل على وجود فروق ذات دلالة إحصائية حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى الكلية عند مستوى $\alpha = 0.05$.

ويبين اختبار شفيه جدول رقم (5-12):

- أن هناك فروق بين " الكلية العربية للعلوم التطبيقية " و " كلية فلسطين التقنية " والفروق لصالح " كلية فلسطين التقنية ".
- أن هناك فروق بين " الكلية الجامعية للعلوم التطبيقية " و " كلية فلسطين التقنية " والفروق لصالح " الكلية الجامعية للعلوم التطبيقية ".

تدلل الفروق على وجود تباينات في ممارسة إدارة عمليات أمن نظم المعلومات في الكليات التقنية مجتمع الدراسة ، ويعزو الباحث الفروق الواضحة بين كلية فلسطين التقنية و الكلية العربية للعلوم التطبيقية إلى إختلاف نظرة كلاً من الكليتين تجاه تعهيد نظم المعلومات بشكل كبير، فبينما ترى الكلية العربية أهمية استخدام التعهيد، تظهر آراء كلية فلسطين ضرورة عدم استخدامه وتبني التطوير الذاتي. وفيما يتعلق بالفروق الواضحة بين الكلية الجامعية وكلية فلسطين التقنية يرى الباحث أن السبب يعزى الى إختلاف جهتي الاشراف، ووجود سياسة أمن المعلومات في الكلية الجامعية.

جدول رقم (5-12): اختبار شفيه للفروق بين المتوسطات حسب متغير الكلية

الفرق بين المتوسطات	كلية فلسطين التقنية	كلية العلوم والتكنولوجيا	كلية تدريب غزة	الكلية الجامعية للعلوم التطبيقية	الكلية العربية للعلوم التطبيقية-رفح
كلية فلسطين التقنية		-0.466	-0.141	-0.610*	-0.604
كلية العلوم والتكنولوجيا	0.466		0.324	-0.144	-0.138
كلية تدريب غزة	0.141	-0.324		-0.468	-0.462
الكلية الجامعية للعلوم التطبيقية	0.610*	0.144	0.468		0.006
الكلية العربية للعلوم التطبيقية-رفح	0.604	0.138	0.462	-0.006	

7.2-لا توجد فروق ذات دلالة إحصائية عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى نسبة الموازنة الأمنية لكل كلية .

تم استخدام اختبار تحليل التباين الأحادي لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى الموازنة الأمنية لكل كلية عند

مستوى $\alpha = 0.05$ والنتائج مبينة في جدول رقم (5-13) ويتبين أن قيمة F المحسوبة لجميع المحاور مجتمعة تساوي 14.755 وهي أكبر من قيمة F الجدولية والتي تساوي2.47 ، كما أن القيمة الاحتمالية لجميع المحاور تساوي 0.000 وهي أقل من 0.05 مما يدل على وجود فروق ذات دلالة إحصائية حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى نسبة الموازنة الأمنية لكل كلية عند مستوى $\alpha = 0.05$.

جدول رقم (5-13): نتائج تحليل التباين الأحادي لواقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى الموازنة الأمنية لكل كلية

عنوان المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة " F"	القيمة الاحتمالية
واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها	بين المجموعات	12.162	4	3.041	14.755	0.000
	داخل المجموعات	18.958	92	0.206		
	المجموع	31.121	96			

قيمة F الجدولية عند درجة حرية "4، 92" ومستوى دلالة 0.05 تساوي 2.47

ويبين اختبار شفيه جدول رقم (5-14) أن:

- الفروق بين الفئة " نسبة مرتفعة " و كل من الفئات " نسبة قليلة جداً "، " نسبة قليلة "، " نسبة متوسطة " والفروق لصالح الفئة " نسبة مرتفعة ".
- كما توجد فروق بين الفئة " نسبة مرتفعة جدا " و كل من الفئات " نسبة قليلة جداً "، " نسبة قليلة "، " نسبة متوسطة " والفروق لصالح الفئة " نسبة مرتفعة جدا ".

ويعزو الباحث ذلك لإختلاف جهات الاشراف على الكليات، والنظم التي تعمل عليها الكليات، وحجم أعمال الكليات، و مدى استخدام نظم المعلومات في كل كلية وتختلف النتيجة مع دراسة تايه(2008).

جدول رقم (5-14): اختبار شفيه للفروق بين المتوسطات حسب متغير الموازنة الأمنية لكل كلية

الفرق بين المتوسطات	نسبة قليلة جداً	نسبة قليلة	نسبة متوسطة	نسبة مرتفعة	نسبة مرتفعة جداً
نسبة قليلة جداً		-0.029	-0.372	-0.808*	-0.992*
نسبة قليلة	0.029		-0.342	-0.778*	-0.962*
نسبة متوسطة	0.372	0.342		-0.436*	-0.620*
نسبة مرتفعة	0.808*	0.778*	0.436*		-0.184
نسبة مرتفعة جداً	0.992*	0.962*	0.620*	0.184	

7.3 –لا توجد فروق ذات دلالة إحصائية عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى مستوى التدريب .

تم استخدام اختبار تحليل التباين الأحادي(One Way ANOVA) لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى مستوى التدريب عند مستوى $\alpha = 0.05$. والنتائج مبينة في جدول رقم (5–15) و يتبين أن قيمة F المحسوبة لجميع المحاور مجتمعة تساوي 13.457 وهي أكبر من قيمة F الجدولية والتي تساوي 2.47، كما أن القيمة الاحتمالية لجميع المحاور تساوي 0.000 وهي اقل من 0.05 مما يدل على **وجود فروق** ذات دلالة إحصائية حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى مستوى التدريب عند مستوى $\alpha = 0.05$

جدول رقم (5–15): نتائج تحليل التباين الأحادي واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى مستوى التدريب

عنوان المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة " F"	القيمة الاحتمالية
واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها	بين المجموعات	11.487	4	2.872	13.457	0.000
	داخل المجموعات	19.633	92	0.213		
	المجموع	31.121	96			

قيمة F الجدولية عند درجة حرية "4، 92" ومستوى دلالة 0.05 تساوي 2.47

ويبين اختبار شفيه جدول رقم (5–16) أن:

- الفروق بين فئتي " مرتفع جداً " وكل من " قليل جدا"، " قليل " والفروق لصالح الفئة "مرتفع جداً "
- كما توجد فروق بين الفئة "مرتفع " وكل من الفئات " قليل جداً"،" قليل" والفروق لصالح الفئة "مرتفع

ويعزو الباحث ذلك لاختلاف الموازنات المخصصة لأمن نظم المعلومات في كل كلية .

جدول رقم (5–16): اختبار شفيه للفروق بين المتوسطات حسب متغير مستوى التدريب

الفرق بين المتوسطات	قليل جداً	قليل	متوسط	مرتفع	مرتفع جداً
قليل جداً		−0.274	−0.435	−0.963*	−0.941*
قليل	0.274		−0.161	−0.690*	−0.667*
متوسط	0.435	0.161		−0.529	−0.506
مرتفع	0.963*	0.690*	0.529		0.023
مرتفع جداً	0.941*	0.667*	0.506	−0.023	

7.4-لا توجد فروق ذات دلالة إحصائية عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى مدى توافر إدارة لأمن نظم المعلومات

تم استخدام اختبار تحليل التباين الأحادي لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى مدى توافر إدارة لأمن نظم المعلومات عند مستوى $\alpha = 0.05$. والنتائج مبينة في جدول رقم (5-17) و يتبين أن قيمة F المحسوبة لجميع المحاور مجتمعة تساوي 8.655 وهي أكبر من قيمة F الجدولية والتي تساوي2.47 ، كما أن القيمة الاحتمالية لجميع المحاور تساوي 0.000 وهي اقل من 0.05 مما يدل على **وجود فروق** ذات دلالة إحصائية حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى مدى توافر إدارة لأمن نظم المعلومات عند مستوى $\alpha = 0.05$

جدول رقم (5-17): نتائج تحليل التباين الأحادي لاختبار الفروق في آراء المبحوثين حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة تعزى إلى مدى توافر إدارة لأمن نظم المعلومات

عنوان المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة "F"	القيمة الاحتمالية
واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل	بين المجموعات	8.509	4	2.127	8.655	0.000
	داخل المجموعات	22.612	92	0.246		
	المجموع	31.121	96			

قيمة F الجدولية عند درجة حرية "4، 92" ومستوى دلالة 0.05 تساوي 2.47

ويبين اختبار شفيه جدول رقم (5-18) أن:

- الفروق بين الفئة " بصورة مرتفعة جداً " و كل من الفئات " بصورة قليلة جداً "، " بصورة متوسطة " والفروق لصالح الفئة " بصورة مرتفعة جداً ".

ويعزو الباحث ذلك لأسباب متعلقة باختلاف الهياكل التنظيمية لأقسام الحاسوب/نظم المعلومات في الكليات مجتمع الدراسة.

جدول رقم (5-18): اختبار شفيه للفروق بين المتوسطات حسب مدى توافر إدارة لأمن نظم المعلومات

الفرق بين المتوسطات	بصورة قليلة جداً	بصورة قليلة	بصورة متوسطة	بصورة مرتفعة	بصورة مرتفعة جداً
بصورة قليلة جداً		-0.133	0.046	-0.502	-0.778*
بصورة قليلة	0.133		0.179	-0.369	-0.645
بصورة متوسطة	-0.046	-0.179		-0.548	-0.824
بصورة مرتفعة	0.502	0.369	0.548		-0.276
بصورة مرتفعة جداً	0.778*	0.645	0.824*	0.276	

7.5 –لا توجد فروق ذات دلالة إحصائية عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى العمر.

تم استخدام اختبار تحليل التباين الأحادي (One Way ANOVA) لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى العمر عند مستوى $\alpha = 0.05$. والنتائج مبينة في جدول رقم (5–19) و يتبين أن قيمة F المحسوبة لجميع المحاور مجتمعة تساوي 5.411 وهي أكبر من قيمة F الجدولية والتي تساوي 2.70، كما أن القيمة الاحتمالية لجميع المحاور تساوي 0.002 وهي اقل من 0.05 مما يدل على **وجود فروق** ذات دلالة إحصائية حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى العمر عند مستوى $\alpha = 0.05$.

جدول رقم (5–19): نتائج تحليل التباين الأحادي لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة تعزى إلى العمر.

عنوان المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة"F "	القيمة الاحتمالية
واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها	بين المجموعات	4.625	3	1.542	5.411	0.002
	داخل المجموعات	26.496	93	0.285		
	المجموع	31.121	96			

قيمة F الجدولية عند درجة حرية "3، 93" ومستوى دلالة 0.05 تساوي 2.70

ويبين اختبار شفيه جدول رقم (5–20) أن :

- الفروق بين الفئة " 50 سنة فأكثر " و كل من الفئات "20 سنة إلى أقل من 30 سنة "، "30سنة إلى اقل من 40 سنة "، " 40 سنة إلى أقل من 50 سنة " والفروق لصالح الفئة "50 سنة فأكثر ".

يرى الباحث أن المبحوثين من فئة "50 سنة فأكثر" يعتبرون هم في الغالب من الفئات الوظيفية التي تشغل مناصب إدارية عليا وعلى إطلاع أكثر بالمعلومات الأمنية ويميلون إلى إيجابية المواقف وربما هذا ما يفسر اختلافهم عن الفئات الآخرى، و على النقيض فالفئات الأخرى تتقارب في آرائها نحو واقع إدارة أمن نظم المعلومات في الكليات التقنية في قطاع غزة، وتختلف النتيجة مع دراسة تايه(2008)،العتيبي(2010)، ودراسة القحطاني (2008).

جدول رقم (5–20): اختبار شفيه للفروق بين المتوسطات حسب متغيرالعمر

الفرق بين المتوسطات	20سنة إلى 30 سنة	30سنة إلى 40 سنة	40 سنة إلى 50 سنة	50 سنة فأكثر
20 سنة إلى أقل من 30 سنة		0.214	0.439	-0.546

30سنة إلى اقل من 40 سنة	-0.214		0.225	-0.760*
40 سنة إلى أقل من 50 سنة	-0.439	-0.225		-0.985*
50 سنة فأكثر	0.546	0.760*	0.985*	

7.6-لا توجد فروق ذات دلالة إحصائية عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى سنوات الخبرة.

تم استخدام اختبار تحليل التباين الأحادي(One Way ANOVA) لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى سنوات الخبرة عند مستوى $\alpha = 0.05$. والنتائج مبينة في جدول رقم (5-21) و يتبين أن قيمة F المحسوبة لجميع المحاور مجتمعة تساوي 4.140 وهي أكبر من قيمة F الجدولية والتي تساوي 2.70، كما أن القيمة الاحتمالية لجميع المحاور تساوي0.008 وهي اقل من 0.05 مما يدل على **وجود فروق** ذات دلالة إحصائية حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى سنوات الخبرة عند مستوى $\alpha = 0.05$.

جدول رقم (5-21): نتائج تحليل التباين الأحادي لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية وسبل تطويرها تعزى إلى سنوات الخبرة

عنوان المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة "F"	القيمة الاحتمالية
واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها	**بين المجموعات**	3.690	3	1.230	4.170	0.008
	داخل المجموعات	27.431	93	0.295		
	المجموع	31.121	96			

قيمة F الجدولية عند درجة حرية "3، 93" ومستوى دلالة 0.05 تساوي 2.70

ويبين اختبار شفيه جدول رقم (5-22) أن:

- الفروق بين فئتي " من 10 إلى اقل من 15 سنة " و " اقل من 5 سنوات " والفروق لصالح الفئة " اقل من 5 سنوات ".

ويعزو الباحث ذلك إلى حداثة خبرات أصحاب هذه الفئة وربطها بالواقع العملي والعلمي النظري التي تلقونها عبر مقاعد الدراسة، بالاضافة إلى حاجاتهم العميقة لاثبات قدراتهم وسعيهم لتعزيز مهاراتهم واستفاداتهم من خبرات السابقين، واتفقت نتائج هذه الفرضية مع نتائج دراسة العتيبي(2010)، واختلفت مع دراسة تايه(2008).

جدول رقم (5-22): اختبار شفيه للفروق بين المتوسطات حسب متغير سنوات الخبرة

الفرق بين المتوسطات	اقل من 5 سنوات	من 5 إلى اقل من 10سنوات	من 10 إلى اقل من 15 سنة	15 سنة فأكثر
اقل من 5 سنوات		0.214	0.553*	0.349
من 5 إلى اقل من 10سنوات	-0.214		0.339	0.134
من 10 إلى اقل من 15 سنة	-0.553*	-0.339		-0.205
15 سنة فأكثر	-0.349	-0.134	0.205	

7.7-لا توجد فروق ذات دلالة إحصائية عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى المؤهل العلمي .

تم استخدام اختبار تحليل التباين الأحادي لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى المؤهل العلمي عند مستوى $\alpha = 0.05$. والنتائج مبينة في جدول رقم (5-23) و يتبين أن قيمة F المحسوبة لجميع المحاور مجتمعة تساوي1.457 وهي اقل من قيمة F الجدولية والتي تساوي 2.70، كما أن القيمة الاحتمالية لجميع المحاور تساوي 0.231 وهي أكبر من 0.05 مما يدل على **عدم وجود** فروق ذات دلالة إحصائية حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى المؤهل العلمي عند مستوى $\alpha = 0.05$.

جدول رقم (5-23): نتائج تحليل التباين الأحادي لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية تعزى إلى المؤهل العلمي

عنوان المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة "F"	القيمة الاحتمالية
واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها	بين المجموعات	1.397	3	0.466	1.457	0.231
	داخل المجموعات	29.724	93	0.320		
	المجموع	31.121	96			

قيمة F الجدولية عند درجة حرية "3، 93" ومستوى دلالة 0.05 تساوي 2.70

ويعزو الباحث عدم وجود فروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية تعزى إلى درجة المؤهل العلمي ربما إلى تقارب نسب كل من المؤهلات وتشابه الآراء بين كل فئة وآخرى وهذا يختلف مع نتائج دراسة العتيبي(2010)، بينما إلى حد ما يتفق مع دراسة القحطاني(2008)، ودراسة تايه (2008).

7.8-لا توجد فروق ذات دلالة إحصائية عند مستوى $\alpha = 0.05$ حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى التخصص العلمي.

تم استخدام اختبار تحليل التباين الأحادي (One Way ANOVA) لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى التخصص العلمي عند مستوى $\alpha = 0.05$. والنتائج مبينة في جدول رقم (5-24) و يتبين أن قيمة F المحسوبة لجميع المحاور مجتمعة تساوي 0.316 وهي اقل من قيمة F الجدولية والتي تساوي 2.70، كما أن القيمة الاحتمالية لجميع المحاور تساوي 0.814 وهي أكبر من 0.05 مما يدل على عدم وجود فروق ذات دلالة إحصائية حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها تعزى إلى التخصص العلمي عند مستوى $\alpha = 0.05$.

جدول رقم (5-24): نتائج تحليل التباين لاختبار الفروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية تعزى إلى التخصص العلمي

عنوان المحور	مصدر التباين	مجموع المربعات	درجة الحرية	متوسط المربعات	قيمة "F"	القيمة الاحتمالية
واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها	بين المجموعات	0.314	3	0.105	0.316	0.814
	داخل المجموعات	30.807	93	0.331		
	المجموع	31.121	96			

قيمة F الجدولية عند درجة حرية "3، 93" ومستوى دلالة 0.05 تساوي 2.70

ويعزو الباحث عدم وجود فروق في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية تعزى إلى التخصص العلمي لتقارب تخصصات المبحوثين بنسبة كبيرة وربما تجانسها، وهذه النتيجة تتقارب مع نتيجة دراسة تايه(2008).

الفصل السادس

النتائج والتوصيات

6-1 نتائج الدراسة

6-2 التوصيات

6-3 دراسات مستقبلية مقترحة

6-1 نتائج الدراسة :

توصلت الدراسة إلى مجموعة من النتائج عن خصائص أفراد عينة الدراسة من العاملين في حقل نظم المعلومات في الكليات التقنية بقطاع غزة، إضافة إلى آرائهم حول موضوع الدراسة "**واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها**"، وخلاصة التحليلات والمناقشات ومن أهم النتائج التي تم التوصل إليها ما يلي:

I. **البيانات الأولية لأفراد عينة الدراسة :**

أظهرت النتائج ما يلي :

1. تبين أن 51% من أفراد مجتمع الدراسة يمثلون كليات تتبع الاشراف الحكومي.
2. نحو 80% من أفراد عينة الدراسة تتراوح أعمارهم بين 20-40 عاماً، مما يشير بدلالات واضحة إلى أن مجتمع الدراسة في عمر شاب، مما يدلل على أن قابليته للتغيير والتدريب والتطوير ممكنة وسهلة .
3. قرابة 70% من المبحوثين تتراوح سنوات خبراتهم أقل من 10 سنوات وهو مايشير بوضوح إلى نضوج اهتمام الكليات التقنية بتطبيق نظم المعلومات المحوسبة.
4. تنوعت المؤهلات العلمية لأفراد عينة الدراسة، وإن كان حاملو الشهادة الجامعية الأولى هم الفئة الأكبر.
5. ما يزيد عن 75% من أفراد عينة الدراسة هم من أصحاب التخصصات العلمية المتصلة بنظم المعلومات.

I. **خصائص الكليات وفقاً لآراء أفراد عينة الدراسة :**

أظهرت النتائج ما يلي :

1. ما يزيد عن نصف أفراد عينة الدراسة رأوا أن مدى توفر إدارة أمن نظم المعلومات في كلياتهم أقل من المستوى المتوسط .
2. ما يزيد عن92% من عينة الدراسة رأوا أن الكليات تستخدم نظم معلومات محوسبة بمستوى مرتفع نسبياً.
3. نحو 75% من أفراد عينة الدراسة يعتقدون بأن مدى التدريب التي يتلقونه في مجالات أمن المعلومات هو دون المستوى المتوسط.
4. ما يزيد عن 70% من أفراد عينة الدراسة يقدرون بأن نسبة موازنة عمليات أمن المعلومات من النسبة الاجمالية لنظم المعلومات تقع في مستوى دون المتوسط.

II. النتائج الخاصة بتحليل فقرات محاور الدراسة :

أظهرت النتائج ما يلي :

1. توفر البنى التحتية لنظم المعلومات في الكليات التقنية بدرجة متوسطة حيث :

- أرتفعت آراء أفراد عينة الدراسة إيجابياً نحو توفر الحماية المادية لنظم المعلومات وجاءت درجة الموافقة بمتوسط حسابي (4.09) درجة من (5) درجات.
- تتوفر الحماية البرمجية بنسبة أعلى من متوسطة بمتوسط حسابي(3.98)درجة.
- تتوفر حماية أفراد نظم المعلومات بنسبة مقبولة نسبياً بمتوسط (3.41)درجة.

2. تدرك الإدارات العليا للكليات التقنية أهمية سياسات أمن المعلومات إلا أنه لا يوجد في أي من الكليات سياسات معمول بها ومطبقة على أسس واضحة حيث :

- لا يعرف موظفو الكليات المبحوثين بسياسات أمن المعلومات في كلياتهم .
- تطبق بعض الكليات التقنية، جزء من السياسات غير المكتوبة والتي لا يعلم بها الموظف أو يعي تفاصيلها .

3. مع أن تأثير التحكم بالوصول لنظم المعلومات على واقع إدارة أمن نظم المعلومات حسب آراء المبحوثين لا يعتبر مرتفعاً إلى حد ما إلى أن :

- تعتبر الكليات التقنية التحكم بالوصول لنظم المعلومات أحدى الزوايا الهامة التي تؤثر في تحسين إدارة أمن نظم المعلومات .
- تختلف الكليات التقنية بممارستها تجاه قضايا التحكم بالوصول .
- يظهر لدى الكليات التقنية إهتمام متزايد بضبط الوصول لنظم المعلومات .

2. ظهرت آراء المبحوثين تجاه توفر الاجراءات التنظيمية الضابطة لنظم المعلومات مقبولة نسبياً

<u>حيث أنه من الناحية الايجابية :</u>

- تقوم الكليات بإجراء عمليات النسخ الاحتياطي الاعتيادي المجدول و الطارئ
- تخضع الأصول المعلوماتية في الكليات لنظام العهد الذي يحدد ملكية كل جزء من مكونات نظم المعلومات .

<u>أما في الناحية السلبية :</u>

- فإن الكليات لا تبلي الكثير من الأهمية تجاه تصنيف معلوماتها .
- لا توجد خطط جاهزة لإستعادة العمل في حالات الطوارئ لدى أغلب الكليات.
- تقتصر عمليات دراسة المخاطر التي تواجه أمن المعلومات على التهديدات الخارجية.

3. أظهرت الدراسة النتائج التالية المتعلقة باستخدام الاستعانة بالأطراف الخارجية (التعهيد):

- تتفاوت الكليات التقنية مجتمع الدراسة في درجات إستخدام تعهيد نظم معلوماتها.

- أظهرت نتائج المقابلات الشخصية أن استخدام التعهيد قد يؤثر سلباً في إدارة أمن نظم المعلومات .
- الكليات التقنية التي تشرف عليها جهات خاصة باتت مقتنعة أكثر باستخدام تعهيد نظم معلوماتها .
- تسعى بعض الكليات للاستغناء عن تعهيد نظمها والاتجاه نحو تطويرها ذاتياً.

4. توجد فروق ذات دلالات إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة تعزى للمتغيرات التالية :(العمر،سنوات الخبرة،مستوى التدريب، الكلية،الموازنة الأمنية لكل كلية، مدى توفر إدارة لأمن المعلومات، مستوى استخدام نظم المعلومات).
5. لدى مفردات مجتمع الدراسة من العاملين بنظم المعلومات في الكليات التقنية رؤية متشابهة نحو واقع إدارة أمن نظم المعلومات في كلياتهم مهما اختلفت مؤهلاتهم العلمية أو تخصصاتهم العلمية.
6. تتوفر سبل وطرق جيدة لتطوير أمن نظم المعلومات في الكليات التقنية

6-2 التوصيات :

في ضوء تحقيق أهداف الدراسة وما نتج من تحليل أدوات الدراسة فإنه يمكن للباحث أن يضع مجموعة من التوصيات كالتالي:

1. أطلقت نتائج المقابلات إنذاراً مدوياً بعدم تواجد مختصين بأمن المعلومات في غالبية الكليات التقنية بقطاع غزة، وهذا ما يدعو الجهات المعنية أن تبذل المزيد من الجهد في سبيل استقطاب وتعيين بعض المختصين في هذا الجانب أو على الأقل تحفيز العاملين الحاليين مادياً أو معنوياً ليكونوا أكثر إلماماً بالنواحي الأمنية المستجدة .
2. قيام الكليات التقنية ببناء سياسات أمن المعلومات الخاصة بها، والعمل على نشرها و تطبيقها، والقيام بتطويرها ومراجعتها، لما لهذه السياسات من أثر في تحسين الاجراءات الأمنية، وتوضيح الأطر التي من شأنها أن تشكل موجه لآليات عمل أفراد نظم المعلومات، وزيادة وعي الأفراد نحو الأمن المعلوماتي.

3. أعطت نتائج الدراسة دلالات على توفر حماية البنى التحتية لنظم المعلومات بنسبة جيدة ولكن هذه النتيجة لابد وأن تحث الكليات التقنية على الاستمرار بالاهتمام بالبنى التحتية لنظم المعلومات وتطويرها لتجاري المستحدثات التكنولوجية السريعة .

4. بينت النتائج أن حماية الأفراد (الأمن التنظيمي) مقبولة نسبياً، وهذا ما يدعو الكليات التقنية إلى مزيد من الاعتناء بالترتيبات الخاصة بضبط العاملين في نظم المعلومات واستحداث آليات للرقابة وتعزيز الاجراءات العقابية بحق منتهكي أمن نظم المعلومات من الداخل.

5. ولتعزيز الأمن التنظيمي يجب على الكليات التقنية الاعتناء بدور أكبر بالتدريب الذي من شأنه أن يمكن الأفراد من زيادة معرفتهم بالقضايا المستجدة والنواحي الأمنية، وهنا يقترح الباحث أن تشمل هذه الدورات التدريبية:
   - دورات في تدقيق نظم المعلومات وتحسين كفاءة نظم المعلومات.
   - دورات في بناء خطط الإستعادة وإدارة الأزمات.
   - دورات في أمن الأنظمة المحوسبة، والتشفير، ونظم التشغيل LINUX.
   - دورات في تطبيق المعايير الدولية لأمن المعلومات.

6. دعوة الإدارات العليا في الكليات التقنية لزيادة الموازنات المالية المخصصة لعمليات أمن المعلومات .

7. يرى الباحث ضرورة أن تقوم الإدارات العليا في الكليات التقنية بوضع تصنيفات للمعلومات بالطريقة التي تناسب أعمالها وسرية معلوماتها، مع عزل البيانات والمعلومات التي يشكل عرضها للعامة ضرر لنظم المعلومات .

8. وضع برامج مجدولة للنسخ الاحتياطي الاعتيادي والطارئ والتأكد من صحة عمليات النسخ الاحتياطي و إعتماد النسخ الاحتياطي الخارجي، خاصة أن بيئة قطاع غزة هي بيئة غير آمنة من ناحية التهديد المادي المقصود و المباشر .

9. تحسين آليات ضبط الوصول لنظم المعلومات، ووضع برامج وإجراءات خاصة بالأدوار والصلاحيات ضمن نظم المعلومات والتركيز على ضرورات أمن المعلومات ومرتكزاته الثلاث : (التوفر – السلامة – السرية).

10. تحسين شروط التعاقد مع المتعهدين (الأطراف الخارجية) ووضع ضوابط وإجراءات عقابية لتحسين عمليات تعهيد نظم المعلومات، وإلزام المتعاقد أو المتعهد بالشروط الموضوعة وبسياسات أمن المعلومات الخاصة بالمؤسسة.

11. العمل على تطبيق الجودة في إجراءات العمل وضرورة تنظيم عمليات الرقابة الداخلية بالتنسيق مع القائمين على أمن نظم المعلومات.

12. بينت الدراسة توفر سبل لتطوير واقع إدارة أمن نظم المعلومات بناءاً على ما أقترحه الباحث، **وبذلك يوصي الباحث بتنفيذها، وهي مرتبة حسب أهميتها وفق وجهة نظر المبحوثين:**

م.	وسائل و سبل التطوير المقترحة
1	استخدام برامج حماية فعالة لمنع محاولات الاختراق والتعدي على نظم المعلومات في الكليات.
2	تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمن نظم المعلومات.
3	فحص أنظمة المعلومات للتحقق من الالتزام بمعايير الأداء الأمني.
4	دعم الإدارة العليا لسياسة ناجحة لأمن المعلومات.
5	استقطاب خبراء حماية نظم المعلومات للعمل بمراكز نظم المعلومات بالكليات التقنية.
6	وضع ضوابط لتبادل المعلومات مع الجهات المعنية خارج الكلية.
7	زيادة الموازنة المخصصة لأمن المعلومات ضمن موازنة تكنولوجيا المعلومات
8	توفير الحوافز(المادية والمعنوية) المناسبة للمبدعين والمتفوقين في مجال أمن نظم المعلومات.
9	الاستفادة من خدمات(التعهيد)الأطراف الخارجية ضمن ضوابط أمنية وشروط جزائية متفق عليها.
10	اعتماد استخدام الوسائل البيولوجية في تحديد شخصية وصلاحية مستخدمي نظم المعلومات.

13. تقييم المخاطر بشكل دوري للوقوف على ما يمكن عمله وإيجاد السبل الكفيلة بإستعادة العمل ووضع خطط الطوارئ اللازمة لضمان أمن نظم المعلومات وقد طرح الباحث نموذجاً إجرائياً لتقييم المخاطر في ملحق رقم (6).

14. ضرورة قيام الجهات الحكومية بإنشاء مركز متخصص يعنى بقضايا أمن المعلومات، ويهدف لمساعدة الهيئات والمؤسسات العامة والخاصة والحكومية في تطوير جودة نظمها لمواكبة الأحداث والمستجدات خاصة في مجالات أمن المعلومات .

6-4 دراسات مقترحة مستقبلية:

- تقييم خطط الطوارئ و برامج إستعادة العمل في الوزارات الفلسطينية بقطاع غزة.
- أثر تطبيق سياسات أمن المعلومات على الأمن التنظيمي في الكليات التقنية بقطاع غزة .
- قياس تكلفة تطبيق المعايير الدولية لأمن المعلومات في وزارات الدولة الفلسطينية.

المراجع

أولاً: المصادر و المراجع العربية

- **القرآن الكريم**
- **أبو جراد**،محمد(1994).التعليم المهني والتقني في فلسطين:واقع وطموح، الخليل:رابطة الجامعيين
- **أبو شنب**، د.عماد أحمد محمد(2009). أدارة وتحليل مخاطر أمن المعلومات، مؤتمر أمن المعلومات والحكومة الالكترونية، ماليزيا : كوالالمبور – ابريل 2009
- **أبو نحلة**، لميس(1996).التعليم والتدريب المهني والتقني من منظور تخطيط ودمج النوع الاجتماعي،القدس:مطبعة الرسائل المقدسية.
- **الاتحاد العربي للتعليم التقني**–الأمانة العامة(1979).النظام الأساسي،العراق.
- **الآغا**، إحسان(2000). دور المشرف التربوي في فلسطين في تطوير اداء المعلم، بحث مقدم للمؤتمر العلمي الرابع عشر للجمعية المصرية للمناهج وطرق التدريس، القاهرة: جامعة عين شمس.
- **الامم المتحدة** – قسم إدارة المحفوظات والسجلات (2006). توجيهات حول حساسية المعلومات وتصنيفها وطرق التعامل معها . متاح في : WWW.UN.ORG بتاريخ :16-10-2012
- **البحيصي**،د. عصام محمد، الشريف،حرية (2008). مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة،مجلة الجامعة الإسلامية(سلسلة الدراسات الإنسانية) المجلد السادس عشر،العدد الثاني،ص895-ص923
- **البداينة**، دياب(2002). الأمن و حرب المعلومات، الطبعة الاولى، الأردن، عمان :دار الشروق للنشر والتوزيع.
- **بسيوني**، عبد الحميد(2007). حماية الحاسبات والشبكات من فيروسات الكمبيوتر والتجسس والملوثات، القاهرة : دار الكتب العلمية للنشر والتوزيع،ط1
- **البكري**، سونيا محمد(1999)نظم المعلومات الإدارية، ط1، مص، القاهرة: الدار الجامعية.
- **تايه**، علاء الدين محمد(2008). مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في فلسطين، رسالة ماجستير غير منشورة، غزة : الجامعة الإسلامية.
- **جامعة الدول العربية**، المركز العربي للبحوث القانونية (2012). الاجتماع الثاني لرؤساء الإدارات المختصة بتقنية المعلومات، المنعقد في 5-2012/03/7، بيروت – الجمهورية اللبنانية، ص6، متاح في :http://carjj.org/node/1242 ، بتاريخ 2012/11/15 .

- **حاج علي**،أ.د عوض(**2006**).التعريف بتقنيات التشفير وأمنية المعلومات،جامعة النيلين، متاح على :http://www.profawad.info/7777.doc بتاريخ 2012/11
- **حاج علي**،أ.د عوض(**2008**).مقال بعنوان:أمن المعلومات والمعايير الدولية، مجلة المعرفة العدد 155- فبراير /2008 م .. نقلاً عن : http://www.qedu.gov.sa/articles-action-show-id-49.htm
- **حاج علي**،عوض؛حسين،عبدالأمير(**2005**).أمنية المعلومات وتقنية التشفير،الطبعة الأولى، الأردن،عمان:دار الحامد.
- **الحسنية**،سليم ابراهيم(2002).مبادئ نظم المعلومات الادارية، الطبعة الثانية، الاردن – عمان : مؤسسة الوراق للنشر والتوزيع.
- **حماد** , طارق عبد العال(2008). إدارة المخاطر, الإسكندرية :الدار الجامعية
- **الحمامي**،علاء حسين؛العاني،سعد عبد العزيز(2007). تكنولوجيا أمنية المعلومات وأنظمة الحماية، الطبعة الأولى، عمان:دار وائل للنشر والتوزيع
- **الحمدان**،عبد الرحمن بن عبد العزيز،والقاسم، محمد بن عبد الله (2004).أساسيات أمن المعلومات، الرياض: مطابع الحميضي.
- **حمدان**،عبد الرحيم(**2001**).التعليم التقني في فلسطين ودوره في تحقيق التنمية،مجلة رؤية،الأمانة العامة للاستعلامات،فلسطين،غزة،العدد 11.
- **حمدان**،عبد الرحيم(**2005**).مدى فاعلية التعليم المستمر في تحقيق التنمية بالكليات التقنية في محافظات غزة،مجلة جامعة الاقصى بغزة،العدد(9)،المجلد(1).
- **الحميد**، محمد دباس،ونينو، ماركو ابراهيم(2007).حماية أنظمة المعلومات،الأردن، عمان:دار الحامد للنشر والتوزيع.
- **داوود**، حسن طاهر (2004). أمن شبكات المعلومات، ط1، الرياض : معهد الإدارة العامة، مكتبة الملك فهد الوطنية .
- **داوود**، حسن طاهر(2000). جرائم نظم المعلومات، الرياض: أكاديمية نايف للعلوم الأمنية – مركز الدراسات والبحوث.
- **الزهيري**، د. طلال ناظم(2008). الحاسوب الشخصي ومتطلبات أمن المعلومات، مدونة الدكتور طلال ناظم الزهيري .تاريخ الاسترداد(11-2012)، من http://drtazzuhairi.blogspot.com/2012/04/2.html
- **السالمي**، علاء عبد الرزاق(2000).تكنولوجيا المعلومات، الطبعة الثالثة، الاردن: دار المناهج للتوزيع والنشر
- **السالمي**،علاء عبد الرازق (2008).الإدارة الالكترونية، الأردن- عمان:دار وائل للنشر.

- **سفور**،هيثم(2010). تحسين وقت الاستجابة والأمن باستخدام خدمة الويب بلغة الترميز الممتدة وحفظ مفتاح الجلسة لـ SSL في كائن الكاش (Cache)، مجلة جامعة الملك عبدالعزيز: العلوم، م 22 ع2، ص ص: 251-274
- **سلطان**،إبراهيم(2005). نظم المعلومات الادارية -مدخل النظم، مصر: الدار الجامعية
- سيد **عرفان نبي**، عبد الرحمن مرزا، خالد الغثبر(2010). دراسة عملية حول أمن المعلومات في المنظمات السعودية، المملكة العربية السعودية: جامعة الملك سعود، مركز التميز لأمن المعلومات.
- **الشيخ**، عصمت عبد الله (1998). دور نظم تكنولوجيا المعلومات في تيسير وفاعلية العمل الاداري، القاهرة : دار النهضة العربية للنشر والتوزيع
- **صالح**، حسين محمود(2009) مقال : المعلومات مفهومها وأهميتها، مجلة المعلوماتية، الرياض : وزارة التربية والتعليم ؛ متاح في : www.informtics.gov.sa/modules.php بتاريخ 24-10-2012.
- **طه**، طارق(2000).مقدمة في نظم المعلومات الادارية والحاسبات الآلية، ط3، مصر، الاسكندرية : منشاة المعارف للنشر والتوزيع،
- **عبيد**،أحمد يوسف(2009).مقال بعنوان :إدارة مخاطر أمن المعلومات، متاح على : http://www.secureminds.net/Pages/articleRiskManagement.aspx بتاريخ 26-11-2012
- **عبيدات**، ذوقان، وعدس، عبد الرحمن، وعبد الخالق، كايد(2001) البحث العلمي، مفهومه، أدواته، وأساليبه. عمان: دار الفكر.
- **العتيبي**، عمر بن محمد(2010). الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير المحلية والدولية، رسالة دكتوراة غير منشورة،الرياض:جامعة نايف العربية للعلوم الأمنية.
- **عثمان**، أ.د حسن(2012). التعهيد..صناعة ملحة، مجلة التعليم الالكتروني – دورية تصدر عن جامعة المنصورة، العدد العاشر، 14-10-2012، النسخة الالكترونية متاحة على : http://emag.mans.edu.eg/digitalcopy/10/
- **عرب**، يونس(2002). دليل أمن المعلومات والخصوصية-جرائم الكمبيوتر والانترنت، الطبعة الأولى، منشورات إتحاد المصارف العربية
- **العساف** صالح حمد(1995).المدخل إلى البحث في العلوم السلوكية في العلوم السلوكية، الرياض: مكتبة العبيكان.
- **الغثبر**،خالد سليمان.**القحطاني**، محمد عبدالله (2009).أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، الرياض: جامعة الملك سعود.

- **غيطاس**، جمال محمد(2007).عصر المعلومات :القادم مذهل أكثر، القاهرة: مركز الخبرات المهنية.
- **القاسم**، محمد بن عبدالله (2007). مقال في جريدة الرياض بعنوان: أمن المعلومات لا يعني سريتها فقط، جريدة الرياض، تاريخ النشر 21-4-2007م
- **قاسم**،عبد الرزراق(2003).نظم المعلومات المحاسبية الحاسوبية،الطبعة الأولى،الاردن، عمان : مكتبة دار الثقافة للنشر والتوزيع
- **القحطاني**، منصور بن سعيد(2008). مهددات الأمن المعلوماتي وسبل مواجهتها"دراسة مسحية على منسوبي مركز الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض"،رسالة ماجستير غير منشورة،الرياض:جامعة نايف العربية للعلوم الأمنية.
- **قناة الجزيرة** (2012). كوريا الجنوبية نهضة تحتذى ..، برنامج الشاهد، فيلم وثائقي من انتاج الجزيرة -تاريخ 3-9-2012
- **قنديلجي**، عامر والجنابي، علاء الدين (2008)نظم المعلومات الادارية وتكنولوجيا المعلومات، ط2، الاردن- عمان : دار الميسرة للنشر والتوزيع والطباعة.
- **كشك**، محمد بهجت(1996). مبادئ الإحصاء واستخداماتها في مجالات الخدمة الاجتماعية، مصر، الإسكندرية: دار الطباعة الحرة
- **محفوظ**،علاء الدين(2010) صناعة التعهيد، بحث مقدم لوزارة التجارة والصناعة، مصر متاح على : http://www.mfti.gov.eg/SME/pdf/researchs/7.pdf ، accssed on 6-11-2012
- **محمد**،أحمد علي الحاج(2002)،مسيرة التعليم والتدريب المهني والتقني في اليمن، الطبعة الأولى، الأردن- عمان :دار المناهج للنشر والتوزيع.
- **مركز التميز لأمن المعلومات** (2009). مصطلحات أمن المعلومات، الرياض :جامعة الملك سعود.
- **المشهداني**، سرحان سليمان السرحان محمود(2001). "أمن الحاسوب والمعلومات"، عمان: دار وائل للطابعة والنشر.
- **المصري**،منذر(1990).المعلم المهني، ،عمان: المركز العربي للتدريب المهني وإعداد المدربين.
- **معجم الحاسبات** (1995)، معجم الحاسبات – الطبعة الموسعة، مصر : مجمع اللغة العربية.
- **المغربي**، عبد الحميد عبد الفتاح(2002) نظم المعلومات الادارية – الاسس والمبادئ، الاسكندرية : مجموعة النيل العربية طباعة نشر توزيع
- **موقع موسوعة ويكيبيديا** (2009). مضاد الفيروسات، متاح على http://ar.wikipedia.org بتاريخ 2012/12
- **نزار**، عامر أبو علي (1999). فيروسات الكمبيوتر، الاردن، عمان : دار حنين.
- **نعيم**، مأمون(2003). وجهاً لوجه :الهكرز بلا اقنعة، القاهرة :شعاع للنشر و العلوم.

- **الهادي** محمد محمد(**2006**) .توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية cybrarians journal ع 9 (يونيو 2006) متاح في: 2012-11-20http://www.journal.cybrarians.org
- **الهادي**، محمد محمد(**1994**).نحو توظيف تكنولوجيا المعلومات في تطوير التعليم في مصر، أبحاث المؤتمر العالمي الثاني لنظم المعلومات وتكنولجيا الحاسبات 13-15 ديسمبر 1994، مصر، القاهرة ، المكتبة الاكاديمية،ص153
- **وزارة التعليم العالي** (2012) . موقع وزارة التعليم العالي الفلسطينية على الانترنت، متاح http://www.mohe.pna.ps/Intro.htm، بتاريخ 18-12-2012
- **وزارة التربية والتعليم(1997)**. تعليمات الدراسة في كليات المجتمع لعام1997.
- **وزارة التربية والتعليم**(2008). الخطة الخمسية التطويرية الاستراتيجية {2008-2012}
- **ياسين**، سعد غالب(2009).أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات، عمان: دار المناهج.
- **يحياوي**، محمد (2011). مخاطر القرصنة المعلوماتية على الحكومة الالكترونية، مجلة البحوث والدراسات العلمية: ع:-05، يوليو 2011، ص 280-285

ثانيا:المراجع الأجنبية

- (**NIST**) National Institute of Standard and Technology (**2002**). Risk Management Guide for Information Technology Systems, ,U.S. Departmrent of Commerce – Publication:800-30.
- **Abrams**, M. and Bailey, D.(**2001**), Essay 5: Abstraction and Refinement of Layered Security Policy. Information Security: An Integrated Collection of Essays. USA, California: IEEE Computer Society Press.
- **Australian National Audit Office**(**2006**). IT Security Management Audit Report No.23 2005-2006, www.anao.gov.au/uploads/documents/2005-06_Audit_Report_23.pdf accessed on 10/2012.
- **Al-adaileh**, Raid Moh'd(**2009**). An Evaluation of Information Systems Success: A User Perspective - the Case of Jordan Telecom Group, European Journal of Scientific Research,Vol.37 No.2 (2009), pp.226-239. http://www.eurojournals.com/ejsr.htm
- **Allen**, Julian(**2005**).Governing for Enterprise Security , USA: Carnegie Mellon University, Software Engineering Institute.
- **Amaio**,Tracy(**2009**). Exploring and Examining the Business Value of Information Security,PHD Management Dissertation,Arizona: Northcentral University
- **Bagad**,V.S.(**2008**) Financial & Industrial Management, 1st Edition, India:Technical Publication Pune.
- **Bagad**,V.S.(**2008**)Management Information Systems, 3rd Revised Edition, India :Technical Publication Pune.
- **Barthelemy**, J. (**2001**). The hidden costs of IT outsourcing, Sloan Management Review, 42(3), 60–69.

- **Bjorck**, Fredrik J.(**2005**). Discovering Information Security Management, Unpublished PHD Thesis, Sweden: Stockholm University & Royal Institute of Technology.
- **Bodnar**, Jeorge and William Hopwood(**1995**). Accounting Information System, New Jersy: Prentice-Hall .
- **Bowen**, Pauline and others (**2006**) Information Security Handbook: A Guide for Managers ,Washington :NIST.
- **BS 7799-2**(**1999**)Information Security Management Systems, London:British Standards Institute
- **Burnet**, Mark M.(**2006**). Perfect Passwords: Selection, Protection, Authentication, Canda:Syngress Publishing
- **Cegielski**, C. G. (**2008**). Toward the development of an interdisciplinary information assurance curriculum: Knowledge domains and skill sets required of information assurance professionals. Decision Sciences Journal of Innovative Education, 6(1), 29-49. Retrieved Dec 20, 2012, from ProQuest database.
- **CNCS**, National Security Telecommunication and information Security,National training standard for Information systems Security (infosrc)
- **COBIT**(**1998**)COBIT:Control Objective,ISACA Rolling Meadows,IL
- **Collins**, J., & Millen, R. (1995). Information systems outsourcing by large American industrial firms:Choices and impact, Information Resources Management Journal, 8(1), 5–13.
- **Date**,C. J.(**2000**) An Introduction to Database Systems, Seven Edition, Addison-Wesley publishing Company.
- **Dhillon**, G.(**1995**). Interpreting the management of information system security, unpublished Phd thesis, UK: University of London.
- **Dickie**, J. (**1996**) Improving Your Organisation's Attitude and Commitment to Securit, Computer Audit Update.
- **Drazin**, R. and Van, A.(1985)Alternative forms of fit in Contingency Theory, Adminstrative Science Quarterly,Vol.30,NO.4,PP. 514-539.
- **Dulany**, Kevin M.(**2002**)."Security, It's Not Just Technical " ,GSEC Practical Assignment , v1.3 , 15 January 2002 , SANS Institute , p 4 .
- **Elliot**, J.(2000)Distributed denial of service attacks and the zombie effect, IEEE IT Pro ,USA,55-57.
- **ENISA**(**2006**). "Critical success factors for ISMS", European Network and Information Security Agency.
- **Farmer**,Jakie(**2006**). Information Security: The Nature and Structure of Intrusion Detection Systems, Management Dissertation ,Walden University
- **Flynn**,N.L.(**2001**).The Epolicy HandBook:Desiging and Implementing Effective E-mail,Internet and software policies,New York :American Management Association
- **Fulford**, H. and Doherty, N. (**2003**). The Application of Information Security Policies in Large UK Based Organisations: An Exploratory Investigation, Information Management and Computer Security, Vol. 11, No. 3, pp.106-114.
- **Garfinkel**,S., Spafford,G. ,Schwartz,A.(**2003**). Practical UNIX and Internet Security, Practical Series, O'Reilly Media.

- **General Accounting Office** "Information security risk assessment: Practices of leading organizations," **GAO**, **1999**. [Online]. Available at: http://www.gao.gov/special.pubs/ai00033.pdf accessed on 9/2012.
- **Gerić** Sandro, Hutinski Željko (**2007**). INFORMATION SYSTEM SECURITY THREATS CLASSIFICATIONS, Journal of Information and Organizational Sciences, Vol 31, No 1 (2007),P.60.
- **Gupta**,M.,Charturvedi,A.R.,Metha,S. And Valeri,L.(**2001**)The Experimental Analysis Of Information Security Issues for Online Financial Services,ICIS2000,PP.667-675 .
- **Harms**,Dan(**2006**).Plagirism,Publishing,and the academy.Journal of Scholarly Publishing,Vol38,Issue 1,P1-13.
- **Hazari**, S. (**2002**). Reengineering an information security course for business management focus. Journal of Information Systems Education, 13(3), 197-204. Retrieved Nov 30, 2012, from ProQuest database.
- **Hentea**, M., Dhillon, H. S., & Dhillon, M. (**2006**). Towards changes in information security education. Journal of Information Technology Education, 5, 221-233. Retrieved Oct 12, 2012, from EBSCOhost.
- **Hertig**, C. A. (**2002**). Charting an academic course. Security Management, 46(12), 81-85. Retrieved Nov 20, 2012, from ProQuest database.
- **Hong** ,Kwo-Shing; Chi, Yen-Ping; Chao, Louis R; Tang, Jih-Hsing (**2003**). An integrated system theory of information security management ,Information Management & Computer Security, 11, 5; ABI/INFORM Global ,pg. 243-249
- **Humpert**, Frederik ;Vrielink and Nina Vrielink(**2004**). Ganzheitliches Sicherheitskosten-Controlling. Available at : http://www.kes.info/archiv/online/kostencontrolling.html. accessed on 11-2012
- **Hyatt**, Michael(**2001**)Invasion of Privacy : How to protect yourself in the digital age, USA : Regnery Publishing.
- International Technical Support Organization-**ITSO**(**2010**). Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security, 2nd edition ,ibm.com: Redbooks.
- **ISACA**(**2009**). An Introduction to the Business Model for Information Security, Available at : http://isaca.org accessed on 12-2012.
- **ISACA**. (**2010**). IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals.
- **ISF**: Information Security Forum(**2007**). The standard Of Good Practice for Information Security. UK: Information Security Forum.
- **ISO**.(**2005**). Information technology -- Security Techniques -- Information Security Management Systems – Requirements. [Online]. Available at: http://www.iso.org/ Accessed on 6/2012 .
- **ISO/IEC 17799**(**2000**)Information Technology code of practice for information Services,International Organization for Standarization , Geneva.
- **Janzeweski**,Lech(**2008**) Cyper crime and Cyper Terrorism, USA: IGI Global.
- **Jorro**, YigezuBalcha(**2011**). Information System Security Audit Readiness -Case study: Ethiopian Government Organizations, Unpublished Master Thesis, Sweden: Stockholm University & Royal Institute of Technology.

- **Kabay**,M.E.(**1996**)The NCSA Guide to Enterprise Security,New York:McGraw-Hill.
- **Kaeo**,Merike(**1999**).Designing Network Security : a practical guide to create a secure network infrastructure, USA:Cisco press ,Macmillan Technical Publishing.
- **Kaplan**,A.(**1964**)The Conduct of inquiry ,New York:Chandler Co.
- **Kazemi**,Mehdi, Khajouei,Hamid and Nasrabadi,Hashem(**2012**).Evaluation of information security management system success factors: Case study of Municipal organization, African Journal of Business Management Vol. 6(14), pp. 4982-4989, 11 April, 2012.
- **Khalfan** A.M. (**2004**). Information security considerations in IS/IT outsourcing projects:a descriptive case study of two sectors, International Journal of Information Management 24 (2004) 29–42 .
- **King**, S(**2003**). Threats and Solutions to Web Services Security, Network Security, Volume 2003 ,September 2003.
- **Kowalski**, Stewart. (**1994**). IT Insecurity: A Multi-disciplinary Inquiry, Ph.D. Thesis. Stockholm:Department of Computer and Systems Science, Stochholm University.
- **Kreicbera**, Liene(**2010**). Internal Threat Information Security –Countermeasures and human factor within SME, Master Thesis, Sweden: Luela University Of Technology.
- **Lacity**, M., Hirschheim, R., and Willcocks, L.(**1994**). Realizing outsourcing expectations. Information Systems Management, 11, 7–18.
- **Lane**, Tim(**2007**). Information Security Management In Australian Universities – An Exploratory Analysis, Master Thesis, Australia :Queensland University of Technology QUT.
- **Lee**, M. (**1995**). IT Outsourcing Contracts:Practical Issues for Management, Working Paper # 95/05. Information Systems Department, City University of Hong Kong.
- **Lee**,S.M.,Luthans,F. and Olson,D.L.(**1982**)A Management Science approach to contingency models of organizational structure ,Academy of Management Journal,Vol.25,No.3,PP.53-566.
- **Logan**, P. Y. (**2002**). Crafting an undergraduate information security emphasis within information technology. Journal of Information Systems Education,13(3), 177-182. Retrieved Nov 30, 2012, from ProQuest database.
- **Loudon**, Kenneth , Loudon, Jane(**2010**). Management Information Systems. Managing The Digital Firm , 9th Edition, New Jersey: Prentice- Hall Inc.
- **Luthans**,F.(**1976**)Introudction to Management A Contingency Approach,New York: McGraw-Hill.
- **Mcgraw**, Gray & Greg Morriset(**2000**) Attacking Malicious code : areport to the infosec research council , submitted to IEEE Software and presented to the IRC, USA,may.
- **McMahon**, W.W.(**1993**), An efficiency-based management information system, Fundamentals of educational planning, Unesco: International Institute for Educational Planning.

- **Michael** E. Whitman,Herbert J. Mattord(**2012**)Principles Of Information Security, Fourth Edition, USA: Cengage Learning.
- **Norton** cypercrime report **2012**,Symantic Norton Web Site.
- **ONDER**,HULUSI(**2007**). A SECURITY MANAGEMENT SYSTEM DESIGN,Unpublished Master Thesis ,Turkey: The Middle East Technical University.
- ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT-OECD(**2002**). **OECD** Guidelines for the Security of Information Systems and Networks:Towards a Culture of Security,Paris: OECD PUBLICATIONS,pp.10-13.
- **Panko**, Raymond (**2004**). Corporate Computer and Network Security, New Jersey: Prentice Hall, Upper Saddle.
- **Paquin**, Michel(**1990**) Management of Information Technology, Canada: Agency Editions .
- **Parker**, Donn B. **(1998)** Fighting Computer Crime , New York : John Wiley& sons.
- **Pastore**,Mike;Dulaney, Emmett(**2004**).Security+ study Guides,USA: John Wiley & Sons.
- **Pierce**, C (**1958**).Collected papers of Charles Sanders Pierce, MA:Harvard University Press.
- **Pipkin** ,DL(**2000**). Information Security – Protecting the Global Enterprise, USA: HP Professional Series.
- **Power**, Mark John; Kevin Clyde Desouza and Carlo Bonifazi(**2006**)The outsourcing handbook : how to implement a successful outsourcing process, London : kogan-page.
- **Whitman** Michael, **Mattod** Herberet(**2011**)Principles of Information Security, 4th edition, Boston : Cengage Learning /Course Technology.
- **Rainer** R. Kelly; Cegielski, Casey G(**2011**) Introduction to Information Systems: Enabling and Transforming Business, 3rd edition, New York: john wiely &sons.
- **Ratzan**,Lee(**2004**). Understanding Information Systems :What they do and why we need them, USA: American Library Association.
- **Rico**, David(**2004**)ROI for Software Process Improvement:Metrics for Project Managers and Software Engineers, USA: J Ross Publishing Series.
- **Rittinghouse**, John W., Ransome James(**2005**). Business Continuity and Disaster Recovery for InfoSec Managers, F. Uk : Elsevier Digital Press.
- **Satzinger** John W. , Jackson Robert B. , Burd Stephen D. (**2009**), Systems Analysis and Design in a Changing World, 5th edition, Boston: course technology centage learning .
- **SALVATI**, DOMENICO(**2008**). Management of Information System Risks, Published Dissertation, Switzerland: University of Zurich [Online]. Available at: www.dsv.su.se/eng/publikationer/index.html accessed on 8/2012
- **Schultz**, E.,Proctor,W. And Lien,M.(**2001**).Usability and Security :an appraisal of usability issues in information security methods, Computers&Securiy, Vol.20, No18, PP. 620-634.

- **Sonnenreich,** W. ,Albanese, j. (**2005**).Return on Security Investment (ROSI): A Practical Quantitative Model, Journal of Research and Practice in Information Technology, vol. 38, no.1.
- **Stair**,Relaph; Reynolds,George(**2010**). Principles of Information Systems ,USA: Course Technology Ptr.
- **Tayson**,Jeff(**2011**).How firewall works?, article on web site : www.howstuffworks.com accessed on 12-2012
- **Tipton,** Harold, Krause Micki (**2000**). Information Security Management Handbook, Fourth Edition, Volume II , USA,WA:Auerbach Publications.
- **Tudor**, J.K., (**2001**). Information Security Architecture: An Integrated Approach to Security in the Organization, Florida- Boca Raton: Auerbach Publications.
- **Whitson**, G., (**2003**).Computer security: theory, process and management, The Journal of Computing in Small Colleges, Vol. 18, No. 6, 2003, p.57 – 66.
- **Wood**, C. (**2002**).An Unappreciated Reason Why Information Security Policies Fail. ,Computer Fraud and Security. Vol: 2000, Issue: 10, pp.13-14 .
- **Wright**,M.(**1999**)Third generation risk management practice, Computers&Security, Vol.1999 No.2,PP.9-12.
- **Yeo**, Ai Cheo; Rahim, MdMahbubur; and Miri, Leon(**2007**). "Understanding Factors Affecting Success of Information Security Risk Assessment: The Case of an Australian Higher Educational Institution". PACIS 2007 Proceedings. P74. http://aisel.aisnet.org/pacis2007/74 ACCESSED ON 8/2012.
- **Zeleznikar**, A.P. (**2002**).An Introduction to Artificial Consciousness', The Philosophy OF the Informational, Formalism, and Implementation (Ver. 1.5), Available free in http://www.artifico.org. ACCESSED ON 24-10-2012.

ثالثاً : المقابلات

- مقابلة مع **مروان أبو شغيبة**،رئيس مركز الحاسوب، كلية فلسطين التقنية – دير البلح، 11 نوفمبر 2012.
- مقابلة مع **أحمد عواجة**،نائب العميد للشئون الاكاديمية،الكلية العربية للعلوم التطبيقية–رفح،5 يناير 2013.
- مقابلة مع **زكريا ابو سلمية**،محاضر تقنية معلومات، كلية تدريب غزة – الوكالة، 6 يناير 2013.
- مقابلة مع **محمد المدهون**، رئيس مركز الحاسوب، الكلية الجامعية للعلوم التطبيقية – غزة، 8 يناير 2013.
- مقابلة مع **سامر ياغي**، مساعد نائب الرئيس للشئون الادارية و مدير مركز الحاسوب سابقاً، الكلية الجامعية للعلوم التطبيقية– غزة، 8 يناير 2013.
- مقابلة مع **أحمد الفرا**، رئيس قسم مركز الحاسوب،كلية العلوم والتكنولوجيا –خانيونس،14 يناير 2013

الملاحق

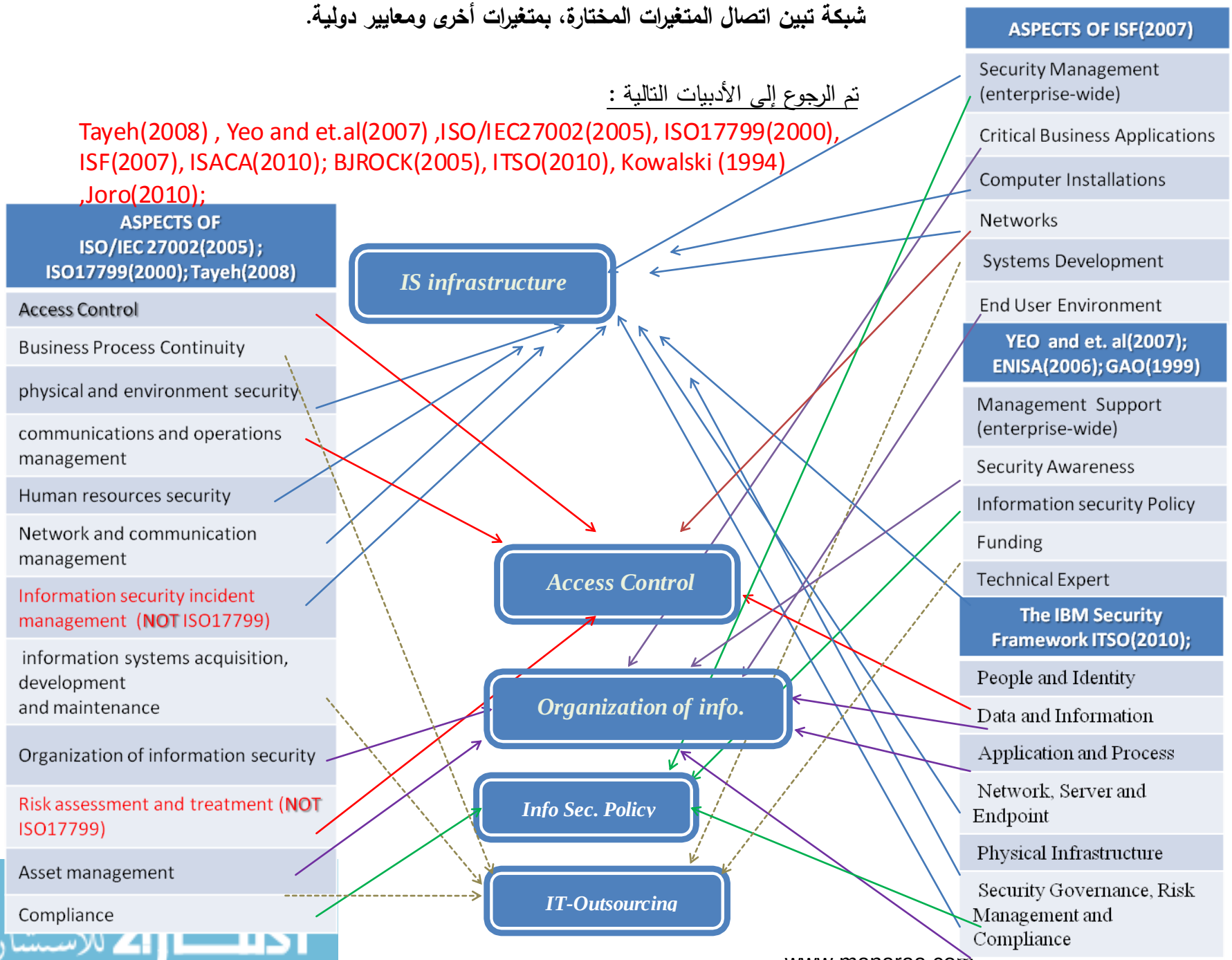
- ❖ ملحق رقم(1): شبكة إشتقاق متغيرات الدراسة و ربطها بالدراسات السابقة
- ❖ ملحق رقم(2):كتاب تسهيل المهمة
- ❖ ملحق رقم(3): بيان بأسماء المحكمين لأداة الدراسة
- ❖ ملحق رقم(4):استبانة الدراسة في صورتها النهائية
- ❖ ملحق رقم(5):أسئلة المقابلات
- ❖ ملحق رقم(6):نموذج إجرائي مقترح لتقييم مخاطر نظم المعلومات في الكليات

ملحق رقم (1):

شبكة تبين اتصال المتغيرات المختارة، بمتغيرات أخرى ومعايير دولية.

تم الرجوع إلى الأدبيات التالية :

Tayeh(2008) , Yeo and et.al(2007) ,ISO/IEC27002(2005), ISO17799(2000), ISF(2007), ISACA(2010); BJROCK(2005), ITSO(2010), Kowalski (1994) ,Joro(2010);



ملحق رقم (2): كتاب تسهيل مهمة باحث

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

كلية التجارة
Faculty of Commerce

الرقم Ref ..... ج س غ/62
التاريخ 19- ذو الحجة 1433 Date
3 تشرين الثاني 2012

من يهمه الأمر

الموضوع: تسهيل مهمة باحث

تهديكم كلية التجارة بالجامعة الإسلامية تحياتها، وترجو التكرم بمساعدة الباحث/ **أيمن محمد الدنف**، برقم جامعي **(120100656)** والملتحق في برنامج ماجستير إدارة الأعمال، في تسهيل مهمته في الحصول على المعلومات والبيانات التي تساعده في عمل رسالة الماجستير بعنوان:

"واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها"

وفى ذلك خدمة للبحث العلمي ودعماً لعملية التنمية الاقتصادية في فلسطين.

وتقبلوا فائق الاحترام والتقدير،،،

عميد كلية التجارة

أ.د. ماجد محمد الفرا

صورة إلى:
*الملف.

P.O. Box 108, Rimal, Gaza, Palestine fax: +970 (8) 286 0800 فاكس Tel: +970 (8) 286 0700 ص.ب 108 الرمال غزة فلسطين هاتف
public@iugaza.edu.ps www.iugaza.edu.ps

ملحق رقم (3)

بيان بأسماء المحكمين لأداة الدراسة

تم تحكيم الاستبانة من الفترة 15..2012/12/27

م.	الاسم	المسمى الوظيفي
1.	أ.د ماجد الفرا	عميد كلية التجارة – الجامعة الإسلامية بغزة
2.	أ.د يوسف عاشور	محاضر ماجستير بالجامعة الإسلامية
3.	د. سامي أبو ناصر	عميد كية الهندسة وتكنولوجيا المعلومات – جامعة الأزهر
4.	د. نبيل البحيصي	محاضر علوم الحاسوب – جامعة الأقصى
5.	د.سمير صافي	رئيس قسم العلوم الاقتصادية والسياسية – الجامعة الإسلامية بغزة
6.	د.نافذ بركات	استاذ الإحصاء وتحليل البيانات – الجامعة الإسلامية
7.	د.هيثم عايش	مدير عام التعليم التقني والمهني – وزارة التربية والتعليم العالي
8.	د.عماد عدوان	عميد كلية فلسطين التقنية.
9.	د.سامي سلامة	محاضر هندسة نظم الحاسوب – كلية فلسطين التقنية
10	م.مروان أبو شغيبة	رئيس مركز الحاسوب ونظم المعلومات – كلية فلسطين التقنية

ملحق رقم (4)

الاستبانة في صورتها النهائية

بسم الله الرحمن الرحيم

الجامعة الإسلامية بغزة
عمادة الدراسات العليا
كلية التجارة – إدارة الأعمال

رقم الاستبانة:.....

الأخ الكريم/ الأخت الكريمة ..... حفظه/ها الله

السلام عليكم ورحمة الله وبركاته

تحية طيبة وبعد:

يتشرف الباحث بأن يضع بين أيديكم استبانة لدراسة "**واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها**" بهدف إستكمال متطلبات الحصول على درجة الماجستير في إدارة الأعمال من الجامعة الإسلامية، وسيشمل مجتمع الدراسة جميع العاملين بمراكز/أقسام نظم المعلومات في الكليات التقنية بالإضافة للعاملين بالأقسام المختلفة التي تنفذ أعمالها مستفيدة من خدمات نظم المعلومات التي تخدم أعمال تلك الكليات، لذا أرجو التكرم من سيادتكم بقراءة كل عبارة من عبارات الاستبيان، ثم وضع علامة (✓) في الخانة التي تمثل وجهة نظركم نحو ما هو قائم بالفعل وفق تدرج خماسي : (أوافق تماماً، أوافق، محايد، لاأوافق، لا أوافق تماماً) . علما بأن إجاباتكم سيتم معالجتها بسرية تامة ولأغراض البحث العلمي فقط.

ونشكر تعاونكم معنا، وتقبلوا فائق الشكر والتقدير .

إذا كنت تريد حضور مناقشة الماجستير

ضع رقم جوالك هنا :..... .....

الباحث

أيمن محمد فارس الدنف

(0599850844)

أولاً: المعلومات العامة

1. الكلية: ☐ كلية فلسطين التقنية ☐ العلوم والتكنولوجيا ☐ كلية تدريب غزة

☐ الكلية الجامعية للعلوم التطبيقية ☐ الكلية العربية للعلوم التطبيقية–رفح

2–الجنس: ☐ ذكر ☐ أنثى

3 – العمر:

☐ 20 سنة إلى أقل من 30 سنة. ☐ 30سنة إلى اقل من 40 سنة.

☐ 40 سنة إلى أقل من 50 سنة. ☐ 50 سنة فأكثر.

4 – سنوات الخبرة:

☐ اقل من 5 سنوات. ☐ من 5 إلى اقل من 10سنوات.

☐ من 10 إلى اقل من 15 سنة. ☐ 15 سنة فاكثر.

5 – المؤهل العلمي:

☐ دبلوم متوسط. ☐ بكالوريوس.

☐ ماجستير. ☐ دكتوراة .

6 – التخصص العلمي:

☐ هندسة حاسوب / علوم حاسوب. ☐ إدارة أعمال.

☐ محاسبة. ☐ غير ذلك، حدد..... .

---

7 – مدى استخدام الكلية لنظم المعلومات المحوسبة (توافر التكنولوجيا – والنظم المحوسبة)

☐ بصورة قليلة جداً ☐ بصورة قليلة ☐ بصورة متوسطة

☐ بصورة مرتفعة ☐ بصورة مرتفعة جداً

8 – مدى توافر إدارة لأمن نظم المعلومات في الكلية:

☐ بصورة قليلة جداً ☐ بصورة قليلة ☐ بصورة متوسطة

☐ بصورة مرتفعة ☐ بصورة مرتفعة جداً

9 – مستوى التدريب الذي تتلقونه في مجال أمن المعلومات:

☐ قليل جداً ☐ قليل ☐ متوسط

☐ مرتفع ☐ مرتفع جداً

10 – النسبة المخصصة لموازنة عمليات أمن المعلومات من الموازنة الكلية لمركز/قسم نظم المعلومات:

☐ نسبة قليلة جداً ☐ نسبة قليلة ☐ نسبة متوسطة

☐ نسبة مرتفعة ☐ نسبة مرتفعة جداً

ثانياً: تساؤلات الدراسة

فيما يلي عبارات متعلقة بموضوع الدراسة يرجى التكرم باختيار درجة موافقتك أو عدم موافقتك عليها حسب واقع توافرها في الكلية التي تعمل بها، وذلك بوضع علامة (✓) أمام الدرجة التي تناسب اختيارك.

المحور الأول :- حماية البنية التحتية لنظم المعلومات

(أ) – الحماية المادية Hardware Security

م	العبارة	أوافق تماماً	أوافق	محايد	لا أوافق	لا أوافق تماماً
.1	تستخدم المحيطات الأمنية (الجدران – الأبواب – الأقفال – بطاقات الدخول) لحماية مكونات نظم المعلومات.					
.2	كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم خدمات نظم المعلومات محمية من العبث بها أو إتلافها.					
.3	يوجد في الكلية مصدر بديل للكهرباء.					
.4	يتم صيانة الأجهزة بشكل سليم لضمان استمرارية عملها وسلامتها.					
.5	يمنع الموظف غير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات					
.6	يتم تأمين شاشة الحاسوب بشكل يدوي عند عدم استخدامها لفترة ما.					

أخرى (من فضلك ذكرها):.....

(ب) – الحماية البرمجية Software Security

م	العبارة	أوافق تماماً	أوافق	محايد	لا أوافق	لا أوافق تماماً
.7	يتم التحقق من صحة البيانات المدخلة.					
.8	تستخدم آليات تشفير لحماية البيانات.					
.9	توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي.					
.10	تتم حماية البرامج المصدرية (Source Code) المستخدمة.					
.11	توفر قواعد البيانات المستخدمة مستويات أمنية متعددة.					
.12	يتم وقاية النظام عن طريق برامج مكافحة الفيروسات.					
.13	توجد برامج حماية لتتبع الاختراق والتسلل.					
.14	هناك معايير لقبول أي أنظمة جديدة أو أي تعديلات، ويتم إجراء اختبارات عليها قبل القبول بها.					

أخرى (من فضلك أذكرها):.....

(ج) – حماية الأفراد Human Resources Security

م	العبارة	أوافق تماماً	أوافق	محايد	لا أوافق	لا أوافق تماماً
.15	يتوفر تدريب للعاملين على النظم المحوسبة بشكل دوري لتطوير مهارتهم المتعلقة بالمستجدات الأمنية.					
.16	تحتوي وثيقة الوصف الوظيفي للموظف على مسؤلياته ومهامه تجاه أمن المعلومات في الكلية .					
.17	يطلب من الموظف التوقيع على تعهد بعدم الافصاح عن معلومات حساسة تخص الكلية كجزء من شروط التوظيف.					
.18	يطلب من الموظفين والمتعاقدين الابلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.					
.19	هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.					
.20	يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في الكلية.					

أخرى (من فضلك أذكرها):.....

المحور الثاني :- سياسة أمن المعلومات Information Security Policy

م.	العبارة	أوافق تماماً	أوافق	محايد	لا أوافق	لا أوافق تماماً
.21	توجد في الكلية سياسة مكتوبة لأمن للمعلومات .					
.22	يعرف الموظف بسياسة أمن المعلومات .					
.23	توجد جهة مكلفة بالإشراف على متابعة سياسة أمن المعلومات .					
.24	يتم مراجعة وتطوير سياسة أمن المعلومات بشكل دوري .					
.25	تدرك الإدارة العليا في الكلية أهمية سياسة أمن المعلومات.					
.26	يوجد إجراءات ضبط صارمة مطبقة على تنفيذ أي تغيرات على نظم المعلومات لحمايتها من العطل.					

أخرى (من فضلك أذكرها):.....

المحور الثالث :- التحكم بالوصول لنظم المعلومات IS Access Control

م	العبارة	أوافق تماماً	أوافق	محايد	لا أوافق	لا أوافق تماماً
.27	صلاحيات الدخول للمعلومات تعطى حسب المستوى الإداري.					
.28	لكل مستخدم هوية محددة خاصة به، حيث لا توجد حسابات عامة يستخدمها عدة أشخاص .					
.29	توجد مراجعات دورية لصلاحيات المستخدمين في الوصول للأنظمة.					
.30	يُحجب الوصول إلى شبكة الانترنت أحياناً.					
.31	يمنع الوصول لبعض خدمات نظم المعلومات عبر الشبكات اللاسلكية.					
.32	توجد إرشادات لطريقة إنشاء كلمات المرور القوية .					
.33	بعض أنظمة المعلومات الحساسة معزولة في شبكات محلية مستقلة.					
.34	يتم إغلاق صلاحيات المستخدم بعد فترة محددة من انعدام نشاطها.					
.35	تستخدم سجلات الأداء لحفظ أنشطة المستخدم لدواعي متعلقة بأمن المعلومات.					

آخرى (من فضلك أذكرها):.....

المحور الرابع :- الاجراءات التنظيمية لضبط نظم المعلومات Organizational Procedures

م	العبارة	أوافق تماماً	أوافق	محايد	لا أوافق	لا أوافق تماماً
.36	يتم إحاطة الموظف بإجراءات التأمين الوقائية.					
.37	يوجد دليل تصنيف للمعلومات يمكن أن يساعد في تحديد كيفية التعامل مع المعلومات وحمايتها .					
.38	تحتفظ الكلية بسجلات حول الأصول المكونة لكل نظام معلومات.					
.39	يتم تحديد الأحداث التي تؤدي إلى توقف نظم المعلومات في الكلية عن العمل، بهدف تقدير مخاطر تلك الأحداث ووضع خطط طوارئ لإستعادة العمل.					
.40	في حال حدوث إخفاق أو انقطاع في أداء الأعمال توجد خطط لإعادة الأعمال إلى طبيعتها ضمن إطار زمني مخطط .					

تابع / المحور الرابع:الاجراءات التنظيمية لضبط نظم المعلومات

	العبارة	أوافق تماماً	أوافق	محايد	لا أوافق	لا أوافق تماماً
.41	يتم تسجيل ما يحدث من أخطاء في نظم المعلومات في تقارير، ويتم ذكر الإجراءات التي اتخذت لتصحيحها.					
.42	يتم عمل نسخ احتياطي للمعلومات بشكل دوري.					
.43	يوجد آليات للإبلاغ عن الحوادث ذات العلاقة بأمن المعلومات.					
.44	يجري منع الموظف من استخدام المعلومات للإغراض غير المصرح بها.					

أخرى (من فضلك أذكرها):.....

.....

المحور الخامس :- استخدام التعهيد (الاستعانة بالمصادر الخارجية) IT-Outsourcing

م	العبارة	أوافق تماماً	أوافق	محايد	لا أوافق	لا أوافق تماماً
.45	يوجد تعاقد مع أطراف خارجية في مجال تطوير نظم المعلومات في الكلية.					
.46	تقوم الكلية بالاستعانة بخبراء في مجالات نظم المعلومات للحصول على استشارات في أمن المعلومات.					
.47	تتم مراقبة عمليات تطوير البرامج التي تنفذها الأطراف الخارجية .					
.48	يطلب من الجهات الخارجية الإبلاغ عن أي ثغرات أمنية يلاحظونها في الأنظمة.					
.49	يتم التحقق من قيام الأطراف الخارجية المتعاقدة بتنفيذ الضوابط الأمنية المتفق عليها.					
.50	يجري مراقبة أداء الاطراف الخارجية عند إجراء الصيانة .					

أخرى (من فضلك أذكرها):.....

.....

ثالثاً :- الرجاء منكم التفضل بالمشاركة بإبداء رأيكم أو تصوركم نحو سبل تطوير إدارة أمن نظم المعلومات في الكلية التي تعملون بها، وذلك بوضع علامة (✓) أمام الدرجة التي تناسب اختيارك، و بإمكانك كتابة أي إقتراحات أخرى أسفل الجدول .

م	العبارة	أوافق بشدة	أوافق	محايد	لا أوافق	لا أوافق بشدة
.51	تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمن نظم المعلومات.					
.52	زيادة الموازنة المخصصة لأمن المعلومات ضمن موازنة تكنولوجيا المعلومات					
.53	فحص أنظمة المعلومات للتحقق من الالتزام بمعايير الأداء الأمني.					
.54	استخدام برامج حماية فعالة لمنع محاولات الاختراق والتعدي على نظم المعلومات في الكليات.					
.55	توفير الحوافز(المادية والمعنوية) المناسبة للمبدعين والمتفوقين في مجال أمن نظم المعلومات.					
.56	استقطاب خبراء حماية نظم المعلومات للعمل بمراكز نظم المعلومات بالكليات التقنية.					
.57	دعم الإدارة العليا لسياسة ناجحة لأمن المعلومات.					
.58	اعتماد استخدام الوسائل البيولوجية (بصمة الأصبع، أو بصمة العين، أو التعرف على الوجه) في تحديد شخصية وصلاحية مستخدمي نظم المعلومات.					
.59	وضع ضوابط لتبادل المعلومات مع الجهات المعنية خارج الكلية.					
.60	الاستفادة من خدمات (التعهيد) الأطراف الخارجية ضمن ضوابط أمنية وشروط جزائية متفق عليها.					

أخرى (من فضلك أذكرها):.....

.....

إنتهى وشكراً

ملحق رقم (5)

أسئلــة المقابلــة

1. ما هو المسمى الفعلي للقسم المسئول المباشر عن نظم المعلومات ؟
2. متى تأسس القسم ؟ وما هي مراحل تطوره ؟ نبذة تاريخية ,,,
3. ماهي الرؤية، الرسالة، والغايات، وماهي الخدمات التي تقدمونها؟
4. وهل هناك خطط استراتيجية للقسم؟
5. كم عدد الموظفين في القسم ؟ وما طبيعة الهيكلية الادارية للقسم ؟ هل من الممكن تزويدنا بها ؟ لضرورات البحث العلمي؟
6. **هل توجد جهة مختصة بأمن المعلومات** ؟ شخص موكل له القيام بقضايا أمن المعلومات ومتابعتها ؟ وما هي المعوقات لفعل ذلك ؟
7. هل يعتبر أمن المعلومات أولوية بالنسبة لكم ؟ وكيف ترون متطلبات الامن (السرية – التوفر – السلامة) بالنسبة لأنشطة المعلومات ؟
8. **هل لديكم سياسة أمن معلومات؟**
9. ماهي البنى التحتية لتكنولوجيا المعلومات، بمعنى ما هوطبيعة نظم المعلومات ككل؟
10. هل تلبي البنى التحتية الحالية لنظم المعلومات احتياجات الاقسام (الكلية):بمعنى هل الشبكة فعالة، هل البرمجيات كفؤة، هل الخوادم تعمل بشكل مناسب، هل يتم مراجعة دورية وفحص وإجراء تقييم للبنى التحتية؟
11. ماذا عن خطط الاستبدال لمكونات نظام المعلومات ؟ تكلم عن كل جزء بشكل منفرد :
    a. المادي H.W.
    b. البرمجي Software
        i. نظم تشغيل
        ii. برامج التطبيقات
    c. الشبكي (وسائط النقل – الشبكة اللاسلكية – الموجهات والمبدلات–تحسين سرعة النقل – الربط بالانترنت)
12. هل يتم إجمال التهديدات التي من الممكن التعرض لها وبدوره السؤال الاشمل هل تقومون بإدارة وتحليل للمخاطر ؟ [أرفق مع الاجابة pie–chart لأنواع ونسب التهديدات من وجهة نظرك]
    a. الثغرات الامنية
    b. التهديدات بأنواعها :
        i. التهديدات الغير متعمدة
        ii. التهديدات المتعمدة

iii. التهديدات الطبيعية

iv. الاخطاء التقنية

v. الاخطاء الادارية

13. هل ترون في الموقع الفيزيائي لقسم الحاسوب /نظم المعلومات موقعاً مناسباً؟

14. ماذا عن وسائل الحماية المتبعة؟

a. وسائل الحماية المادية

b. وسائل الحماية الفنية (التقنية)

i. ضبط الوصول Access Control

ii. Firewall(s/h)

iii. التشفير

c. وسائل الحماية التنظيمية (الادارية)

i. تصنيف المعلومات

ii. التوثيق

iii. النسخ الاحتياطي

iv. خطط الطوارئ والاسترداد الآمن

v. خطط التطوير والتعلم من الاخطاء

15. ماذا عن **التعهيد IT–Outsourcing**؟ وهل ترون فيه حل ؟ وما الفوائد ؟ والمعوقات و العيوب ؟

16. ما هي السبل التي يمكن إتخاذها لحماية المؤسسة من مخاطر قد تتعرض لها سلامة وتوفر المعلومات ؟

مع شكري وتقديري

نموذج مقابلة شخصية

الكلية :..... التاريخ : .....

اسم /أسماء من أجريت معهم المقابلة :

م.	الاسم	الوظيفة	التاريخ والوقت
▪			
▪			
▪	>>		

1- المقابلة التي أجريت مع .....

م	السؤال	الاجابة
.1		
.2	>>	

ملحق رقم (6)

نموذج إجرائي مقترح لتقييم مخاطر نظم المعلومات في الكلية:

اسم الكلية:	مصدر البيانات:	التاريخ:

I. بيانات حول القسم / المركز المشرف على نظم المعلومات

م.	الموظف	الخبرة	الدرجة العلمية	مجال الخبرة
.1				
.2				
.3				
.4				
.5				
.6				
.7	<<<			

II. حصر الاقسام التي تشملها نظم المعلومات

م.	النظام	متوفر	الجهة المنفذة للنظام(الاشراف)	بيانات وتوضيحات آخرى
.1	القبول والتسجيل			
.2	شئون الطلاب			
.3	الشئون الاكاديمية			
.4	شئون الموظفين			
.5	المكتبة			
.6	المحاسبة			
.7	المالية			
.8	اللوازم والمشتريات			
.9	موقع الويب			
.10	التعليم الالكتروني			
.11	<<<[14]			

[14] الإشارة (<<<) تعني : المزيد من البيانات والصفوف المدرجة.

III. بعض الخدمات التي تنفذها أطراف خارجية (IT-Outsourcing)

م.	الخدمة	مدة التعاقد	الجهة المنفذة للنظام	الجهة الممولة	الحالة بعد انتهاء العقد
.1					
.2					
.3	>>>				

IV. البنية المادية والشبكية المتوفرة IT Infrastructure :Hardware/Networks

المستفيدون مباشرة من النظم Clients	الخوادم Servers	Storage Capacity
#	#	#
Internet Service Provider	Network Size (Clients)	Central Wireless Network(y/n)
	#	
معدل صيانة الحواسيب الشهري	فترة الصيانة الوقائية	فترة التوقف عن الخدمة المسموحة
%		

V. بيئة البرامج المستخدمة Software Environment

OS	Windows7☐	WinXP☐	Win☐	Linux☐	others☐
P/L					
DB Platforms	Oracle☐	MySQL☐	Web Enabled☐		
Intrusion Prevention Systems			Intrusion Detection Systems		
Firewall			Anti Virus		Update every

VI. النسخ الاحتياطي Backup

	البيانات	البرامج المصدرية	قواعد البيانات
نسخ احتياطي داخلي			
Off-site نسخ خارجية			
الفترة ?.... Every			

VII. نقاط الضعف :

م.	نقطة ضعف	النوع	التأثير المصاحب	المدة	التهديد المستفيد
.1			.1		
			.2		
			.3 >>>		
.2			.1		
			.2		
			.3 >>>		
.3			.1		
			.2		
			.3 >>>		
.4	>>>		.1		
			.2		
			.3 >>>		

- نقطة ضعف : هي الثغرات التي من الممكن استغلالها لتهديد أمن نظم المعلومات
- النوع: والمقصود هنا تصنيف نوع نقطة الضعف بدقة (برمجي – إداري – داخلي – خارجي)
- التأثير المصاحب : آثار قد تنتج عن الثغرات
- المدة : الزمن الذي يبقى مستمراً معه هذا الأثر.
- التهديد المستفيد : ما هي التهديدات التي ستستغل هذه الثغرة

VIII. التهديدات التي قد تواجه المؤسسة والاجراءات المضادة :

م.	التهديد	نسبة	الاجراءات المضادة	التكلفة	نتيجة الاجراء
.1			.1		
			.2		
			.3 >>>		
.2			.1		
			.2		
			.3 >>>		
.3			.1		
			.2		
			.3 >>>		
.4			.1		
			.2		
			.3 >>>		
.5	>>>		.1		
			.2		
			.3 >>>		

- التهديد: هو كل ما تشعر المؤسسة بشك حول أضرار ممكن أن يسببها في حال تمكن من استغلال الثغرات بالنظام (كالفيروسات – السرقة)
- النسبة : هي نسبة التمكن من الضرر في حال حدث ذلك
- الاجراء المضاد : ما يمكن اقتراحه من حلول لصد التهديد وكبحه
- التكلفة : هي تكلفة تقديرية لكل إجراء مضاد مقترح
- نتيجة الاجراء : هي ما يمكن أن توفره هذه الإجراءات من حالة شعور بالامن،

و تكون الاجابة حول الآلية التي تتوصل بها للنتيجة مثلا : (سريع – مرحلي – مستمر)

IX. الخسائر المتوقعة نتيجة المخاطر التي لازلت قائمة أو التي حدثت بالفعل :

م.	المخاطر	الموارد التي قد تتأثر بالخطر	قيمة المورد	نسبة الأثر	الخسارة المالية المتوقعة
.1		.1			
		.2			
		.3 <<<			
.2		.1			
		.2			
		.3 <<<			
.3		.1			
		.2			
		.3 <<<			
.4	<<<	.1			
		.2			
		.3 <<<			

- المخاطر : هي تهديدات أثرها لازال فعال، أو حدثت بالفعل مستغلة أحدى نقاط الضعف
- الموارد: هي موارد المؤسسة التي تقع تحت الخطر القائم أو الذي حدث فعلاً
- قيمة المورد : هي قيمة المورد المقدرة أو الفعلية حسب نوع المورد
- نسبة الأثر : هي نسبة توقع تأثير الخطر على المورد اذا كان الخطر قائم، ونسبة حقيقية أو مقدرة إذا وقع الخطر .
- الخسارة المتوقعة = قيمة المورد * نسبة الأثر .