الجامعة الإسلامية –غزة
عمادة الدراسات العليا
كلية التجارة
قسم المحاسبة والتمويل

مخاطر نظم المعلومات المحاسبية الإلكترونية

"دراسة تطبيقية على المصارف العاملة في قطاع غزة"

إعداد الطالبة

حرية شعبان محمد الشريف

إشراف الدكتور

عصام البحيصي

قدمت هذه الرسالة استكمالا للحصول على درجة الماجستير في المحاسبة والتمويل من كلية التجارة بالجامعة الإسلامية بغزة

1427هـ - 2006م

بسم الله الرحمن الرحيم

"يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ
وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ"

(المجادلة، من الآية ١١)

الإهداء

إلى زهور المستقبل

إلى زهور الغد المشرق

إلى زهور الأمل المتدفق

أحبائي

أسيل ... نور ... أسامة

وإلى زوجي الغالي

عبد الكريم

شكر وتقدير

الشكر والتقدير أولا وأخيرا لله عز وجل ممهد السبل وموفق المساعي ومرشد من يضل .

كما وأتقدم بالشكر والتقدير لكل من مد يد العون لي وساعدني في إنجاز هذا الجهد المتواضع .

وأخص بالشكر والتقدير مشرفي الفاضل ...

الدكتور عصام البحيصي

على ما بذله من جهد طيب من خلال إشرافه على هذه الدراسة والذي لم يبخل عليّ بوقته وعلمه لاتمام هذا الجهد .

كما أتقدم بخالص الشكر والتقدير إلى...

أساتذتي الكرام الأستاذ الدكتور يوسف عاشور والدكتور حمدي زعرب والدكتور علي شاهين

على تفضلهم بقبول مناقشة هذه الرسالة حتى تزدان بآرائهم السديدة وأفكارهم النيرة.

وأتقدم أيضا بالشكر الجزيل لعائلتي الحبيبة زوجي وأطفالي لصبرهم وتعاونهم معي وتشجيعهم المتواصل لي في مسيرة العلم

فجزى الله تعالى الجميع عنّي خير الجزاء، وجعل ذلك في موازين حسناتهم يوم القيامة.

الفهرس

ملخص الدراسة

يهدف هذا البحث إلى التعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، والتعرف على أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر .

حيث استعانت الباحثة بما تناولته الدراسات السابقة والأبحاث التي اهتمت في هذا المجال، كذلك تم التعرف على الإجراءات والوسائل الرقابية المتبعة من قبل المصارف العاملة في قطاع غزة لمواجهة تلك المخاطر التي قد تواجه نظم معلوماتها المحاسبية الالكترونية .

وبناء على ذلك تم استخلاص بعض النتائج التي تسهم في التعرف على أهم المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، وتقديم التوصيات في هذا المجال .

كما استخدمت الدراسة المنهج الوصفي التحليلي في الوصول لنتائج الدراسة، حيث تم توزيع استبانة على المصارف العاملة في قطاع غزة وفروعها .

وقد تم استخدام برنامج التحليل الإحصائي (SPSS) للعلوم الإنسانية والإجتماعية لمعالجة البيانات باستخدام التكرارات والنسب المئوية، والمتوسطات الحسابية، واختبار الإشارة اللامعلمي (Sign Test) .

وقد تم التوصل إلى مجموعة من النتائج أهمها :

١. أوضحت الدراسة قلة عدد موظفي تكنولوجيا المعلومات في المصارف العاملة في قطاع غزة حيث يعتمد الفروع على موظف واحد مهمته تشغيل أنظمة الحاسوب بينما

الموظفين المختصين يكون مكانهم في المراكز الرئيسية للفروع وغالبا ما توجد في الضفة الغربية.

٢. الإدارة الجيدة تستطيع أن تقلل أوتحد من حدوث المخاطر التي تواجه نظم المعلومات المحاسبية لدى المصارف .

٣. تطبيق إجراءات أمن النظم المعلوماتية يقلل من إمكانية حدوث مخاطر نظم المعلومات المحاسبية .

وعلى ضوء نتائج الدراسة تم التوصل إلى مجموعة من التوصيات أهمها :

١. وضع اجراءات تضمن استمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الأزمات من خلال استخدام تجهيزات منيعة أو مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها والحد من وقوعها .

٢. وضع ضوابط أمن ورقابة المعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أو اتصالات سلكية ولاسلكية والإنترنت والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية .

٣. العمل على تطوير شبكة المصارف وربطها بشبكة الإنترنت من أجل تمكين العملاء من تنفيذ الخدمات الخاصة بهم بسهولة وبسرعة دون أي تأخير ولكن مع إحكام الرقابة المصرفية على شبكة المصرف ووضع قيود تحد من محاولة اختراق شبكة المصرف والحصول على أي معلومات غير مرخص لهم بالحصول عليها .

Abstract

The objective of this research is to investigate the threats of electronic accounting information systems in the working banks in the Gaza strip, to investigate the most important reasons that lead to the occurring of these threats, and to investigate the procedures that prevent the occurring of these threats.
The researcher depended on the previous studies concerned in this field, and the procedures and controlling methods that are applied in the banks in the Gaza strip in order to face these threats which may face their electronic accountant information systems, are also investigated.

Some findings that participate in the investigation of the most important threats that face electronic accountant information systems are summarized, in addition to the recommendations in this field.

The study has been used the descriptive analytical curriculum to reach the research findings, so a questionnaire was distributed to the main banks in the Gaza strip and their branches.

Statistical Package for Social Sciences (SPSS) version 11 has been used to analyze data using frequencies, percentages, means and sign test.
And the following findings were reached:

1- The study reported that there is a low number of information technology employees in the banks in the Gaza strip, and the branches depend only on one employee whose job is to keep the operation of information systems, while specialized employees work in the main branch, an these branches are usually found in the West bank.

2- The good management can able to minimize or prevent the occurrence of threats that face accounting information systems in the banks.
3- The implementation of security procedures for information systems will decrease the possibility of the occurring of information security threats.

And upon the findings, a group of recommendations had been reached, and the most important of which are:
1- Write procedures that assure the work continuity and availability of information systems in crisis cases through using immune equipments that can able to explore the threats before their occurrence and prevent their occurrence.
2- write perfect controlling security tools for information into all their shapes including paper form, wire or wireless communications and Internet, and work at making the required laws for information systems security and information networks security.
3- Work at the development of the internal network of the banks, and connect it to the internet to let customers make their private services easy and quickly without delay, but by perfect control and monitor of the bank network, and by putting constraints to prevent the penetration of the bank network or an unauthorized access to any information.

الفصل الأول
خطة الدراسة

الفصل الأول
خطة الدراسة

مقدمة :

يعتبر العصر الحالي هو عصر ثورة المعلومات والاتصالات، وتعد المعلومات هي السمة الأهم للعقود الأخيرة من القرن العشرين، حيث أدى تطور تكنولوجيا المعلومات إلى ازدياد حجم المعلومات التي يجب أن تعالج وتخزن وتقدم للنظام بشكل كبير مما عقد عملية التحكم بها والسيطرة عليها، وقد انتشرت تطبيقات تكنولوجيا المعلومات في شتى المجالات وعلى جميع المستويات، وأصبح استخدام الحاسوب في معالجة المعلومات المحاسبية يعد خطوة ضرورية وهامة جدا لانتاج واستهلاك المعلومات في المنشأة. (قاسم ،١٩٩٨ ،ص٥،٦)

ويعد التطور السريع في تكنولوجيا المعلومات والإنتشار الواسع للنظم والبرامج الصديقة للمستخدم، بالاضافة إلى رغبة المنشآت في إقتناء وتطبيق أحدث النظم والبرامج الإلكترونية دافع أساسي لإستخدام الحاسب الآلي وأداء العديد من المهام والوظائف المحاسبية بصورة أسرع وأدق، ولكن على الجانب الأخر فإن هذا التقدم التكنولوجي الهائل قد يحمل بين طياته العديد من المخاطر الهامة المتعلقة بأمن وتكامل النظم المحاسبية الإلكترونية، نظراً لأن التطور في الحاسبات وتكنولوجيا المعلومات لم يصاحبه تطوراً مماثلاً في الممارسات والضوابط الرقابية، كما لم يواكب ذلك تطوراً مماثلاً في معرفة وخبرات ووعي العاملين بتلك المنشآت.(أبو موسى، ص١، ٢٠٠٤)

ولذلك فإن نظام المعلومات المحاسبي في أي منشأة يجب أن يتضمن وسائل وضوابط رقابية على البيانات حتى يتم تقديم تقارير تحتوي على معلومات موثوق بها من قبل مستخدمي نظام المعلومات .

وللمحاسبين دور هام في تطوير وتقييم مقاييس الرقابة والأمان في نظام المعلومات المحاسبي، فهم يعملون عن قرب مع مصممي النظم أثناء تطوير نظام المعلومات المحاسبي حتى يتم التأكد من أن مقاييس الرقابة والأمان مناسبة وكافية، وإدخال الحاسب الآلي في نظام المعلومات يؤثر على وسائل الرقابة والأمان للبيانات، فرغم المزايا التي يخلقها التشغيل الآلي للبيانات من الدقة والسرعة، فإن المشاكل الخاصة بالرقابة قد تؤدي إلى سهولة التلاعب في البيانات وعدم دقة المخرجات .(الدهراوي ،٢٠٠٣،ص١٥٩)

ومن هنا تظهر مهمة جديدة ومسؤولية كبيرة أمام إدارة نظم المعلومات في المنشأة وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل هذه النظم بشكل صحيح والتخطيط الدقيق لمواجهة جميع الأخطار التي يمكن أن تؤدي إلى تعطلها أوتوقفها عن العمل، وفي حال حدوث ذلك، التمكن من إعادة تشغيلها بأسرع وقت ممكن، وتسمى هذه الوظيفة الهامة والضرورية جدا حماية وأمن نظم المعلومات، وتهدف هذه الوظيفة إلى حماية الموارد المحوسبة من الأخطار والتهديدات المقصودة وغير المقصودة التي يمكن أن تؤدي إلى عمليات غير مسموح بها مثل تعديل أو انكشاف أوتخريب البيانات أو البرامج. (جمعة وآخرون ،ص٣٤٠، ٢٠٠٣)

وبالنظر إلى البيئة الفلسطينية نلاحظ انتقال العمل في المصارف العاملة في قطاع غزة من النظام اليدوي إلى النظام الإلكتروني، وهذا يتطلب من إدارة المصارف العمل على احكام الرقابة على العمل المصرفي من أجل الحفاظ على أمن نظم المعلومات المصرفية .

وعليه تأتي هذه الدراسة للتعرف على المخاطر المختلفة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية والتعرف على أسباب حدوثها وإجراءات الحماية المتبعة لمواجهة تلك المخاطر .

مشكلة الدراسة :

وتتمثل مشكلة الدراسة في الإجابة عن التساؤلات التالية :

١. ما هي المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة ؟
٢. ما هي أهم المخاطر ودرجة تكرارها التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية لدى المصارف العاملة في قطاع غزة ؟
٣. ما هي أسباب حدوث المخاطر المختلفة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية لدى المصارف العاملة في قطاع غزة ؟
٤. ما هي معدلات حدوث المخاطر المختلفة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية لدى المصارف العاملة في قطاع غزة ؟
٥. ماهي اجراءات الحماية التي تتبعها المصارف العاملة في قطاع غزة للحد من المخاطر التي تهدد نظم المعلومات المحاسبية ؟

فرضيات الدراسة :

١. لا تحدث المخاطر التالية بشكل متكرر في المصارف العاملة في قطاع غزة:

- مخاطر تتعلق بادخال البيانات.
- مخاطر تتعلق بالتشغيل
- مخاطر تتعلق بالمخرجات
- مخاطر تتعلق بالبيئة

٢. ترجع اسباب حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة إلى:

- أسباب تتعلق بموظفي البنك نتيجة لقلة الخبرة و الوعي والتدريب .
- اسباب تتعلق بادارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الاجراءات والادوات الرقابية المطبقة .

٣. لا توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة

أهداف الدراسة :

تهدف هذه الدراسة إلى:

١. التعرف على طبيعة المخاطر التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى بيئة المصارف العاملة في قطاع غزة ومعدلات تكرارها .

٢. التعرف على أسباب حدوث المخاطر المختلفة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية لدى المصارف العاملة في قطاع غزة.

٣. التعرف على اجراءات الحماية التي تتبعها المصارف العاملة في قطاع غزة للحد من المخاطر التي تهدد نظم معلومات المحاسبية الإلكترونية .

٤. التمييز بين مخاطر أمن نظم المعلومات وعدم كفاية الضوابط الرقابية لأمن تلك النظم.

٥. التركيز على مخاطر مخرجات الحاسب الآلي وعدم إهمالها.

أهمية الدراسة :

تنبع أهمية هذه الدراسة من أهمية الموضوع ذاته وتتلخص في النقاط التالية:

١. أن نظم المعلومات المحاسبة الإلكترونية قد أصبحت عرضة للعديد من المخاطر التى تهدد صحة وموثوقية ومصداقية وسرية وتكامل ومدى إتاحية البيانات المالية والمحاسبية التى توفرها تلك النظم، مما يؤدي إلى سهولة حدوث تلك المخاطر.

٢. وجود خلط واضح وعدم تمييز بين مخاطر أمن نظم المعلومات وعدم كفاية الضوابط الرقابية لأمن تلك النظم لدى العديد من الباحثين.

٣. أن معظم الدراسات السابقة قد ركزت على مخاطر أمن نظم المعلومات المتعلقة بمرحلتى إدخال وتشغيل البيانات، وأهملت تماماً المخاطر المرتبطة بمرحلة هامة وحيوية من مراحل النظام وهى مخرجات الحاسب الآلى.

٤. حداثة هذه الدراسة حيث تعتبر الأولى من نوعها والتي تطبق على المصارف العاملة في قطاع غزة.

٥. تركز هذه الدراسة على أهمية المخاطر التي تواجه أمن نظم المعلومات المحاسبية لدى القطاع المصرفي وبالتالي تمكن المصارف من الإستفادة من نتائج هذه الدراسة .

٦. سوف تنعكس هذه الددراسة على تطوير أداء المصارف فيما يتعلق بالسيطرة على المخاطر مما يعزز دورها في المجتمع وزيادة الثقة في الجهاز المصرفي بشكل عام .

٧. اعتبار هذه الدراسة نقطة انطلاق لمزيد من الدراسات المستقبلية فيما يتعلق بموضوع الدراسة .

منهجية الدراسة :

يتمثل منهج هذه الدراسة في إجراء دراسة تطبيقية للتعرف على المخاطر التي تهدد أمن نظم المعلومات المحاسبية الالكترونية وأسباب حدوث تلك المخاطر والإجراءات التي يمكن اتباعها لمواجهة المخاطر السابقة في المصارف العاملة في قطاع غزة وقد اعتمدت الباحثة في ذلك على المصادر التالية:

١. المصادر الثانوية :

وتتكون المصادر الثانوية من الكتب والمقالات والأبحاث المنشورة في المجلات العلمية المتخصصة والمحكمة .

٢. المصادر الأولية :

وتتمثل المصادر الأولية في اعتماد الباحثة على الاستبيان[1]، والذي أعد خصيصا لهذه الدراسة ،وتم دراسة قائمة المخاطر التي تم التوصل إليها في الدراسات السابقة، حيث تم توزيع عدد (١٥٩) استبانة على جميع المصارف العاملة في قطاع غزة وفروعها باستثناء المؤسسة المصرفية والبنك العربي وذلك للأسباب التي سيتم ذكرها لاحقا، وبعد المتابعة تم تجميع عدد (١٢٩) استبانة ليصل معدل الردود إلى (٨١%) من إجمالي العينة، حيث تم استخدام ما نسبته (١٠٠%) من إجمالي الردود، وقد قامت الباحثة باجراء التحليل الوصفي Descriptive Analysis (مثل معدل التكرارات والنسب) للبيانات التي تم تجميعها للتعرف على الخصائص الأساسية لعينة ومتغيرات الدراسة، حيث اعتمدت الباحثة على المنهج الوصفي التحليلي، لأنه يعتبر من أنسب المناهج لمثل هذه الدراسة، وتم إجراء بعض الاختبارات اللامعلمية Non-Parametric Tests (مثل إختبارSign Test) لإختبار فرضيات البحث وذلك من خلال استخدام برنامج (SPSS) الاحصائي.

[1] أنظر ملحق رقم (١)

مجتمع الدراسة :

يتكون مجتمع الدراسة من جميع المصارف العاملة في قطاع غزة والبالغ عددها (١٢) مصرفا والتي تضم مدراء المصارف والمحاسبين ورؤساء الأقسام ومراجعو نظم المعلومات الإلكترونية والمراجعين الداخليين والمراقبين في تلك المصارف ومهندسو وموظفو دوائر تكنولوجيا المعلومات وهي موضحة كالتالي :

م.	اسم البنك	العدد
١.	بنك فلسطين المحدود	٥٠
٢.	البنك التجاري الفلسطيني	٦
٣.	بنك الاستثمار الفلسطيني	٦
٤.	البنك الإسلامي العربي	١٢
٥.	بنك القدس للتنمية والاستثمار	٦
٦.	بنك فلسطين الدولي	٣
٧.	البنك الإسلامي الفلسطيني	٢٥
٨.	بنك القاهرة عمان	٢٥
٩.	بنك الأردن	٦
١٠	البنك العقاري المصري العربي	٨
١١	بنك الاسكان للتجارة والتمويل	٦
١٢	البنك الرئيسي للتنمية والائتمان الزراعي	٦

علما بأنه قد تم استبعاد المؤسسة المصرفية الفلسطينية لعدم ملائمة عملها لطبيعة الدراسة، أما البنك العربي فقد تم استبعاده بسبب رفض ادارة البنك للتعامل مع الباحثة أو الافصاح عن أي معلومات قد تساعد الباحثة في دراستها.

عينة الدراسة :

وتتمثل عينة الدراسة في كافة أفراد مجتمع الدراسة ولما كان مجتمع الدراسة محدد فقد تم اختيار العينة لتمثل كافة أفراد المجتمع .

مشكلات واجهت الباحثة :

١. امتناع بعض مدراء المصارف العاملة في قطاع غزة عن التعامل مع الباحثة في تعبئة الاستبانة أو تزويد الباحثة بأي معلومات قد تفيدها في الدراسة .

٢. عدم تمكن الباحثة من تعميم الدراسة على المصارف العاملة في الضفة الغربية وذلك بسبب الظروف السياسية والحصار المفروض على قطاع غزة.

٣. ندرة المصادر العربية المتخصصة في أمن المعلومات .

محددات الدراسة :

١. الحد البشري :

وشمل مدراء ورؤساء الأقسام والمحاسبين والمراجعين الداخليين والمراقب العام في المصارف العاملة في قطاع غزة، بالإضافة إلى موظفي قسم تكنولوجيا المعلومات في المصارف .

٢. الحد المكاني :

اقتصرت الدراسة على المصارف العاملة في قطاع غزة وفروعها، مع استبعاد المؤسسة المصرفية والبنك العربي لما تم ذكره سابقا .

الدراسات السابقة :

يعتبر موضوع أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية من المواضيع الهامة والحديثة نسبيا، حيث أنه من خلال مراجعة الدراسات والأبحاث السابقة والمتعلقة بهذا الموضوع نجد أن هناك ندرة في العالم العربي حول هذا الموضوع مع توفر دراسات قليلة في العالم الغربي وهذا إن دل على شيء فإنما يدل على الحداثة النسبية لهذا الموضوع رغم أهميته الحيوية لكثير من المنشآت والمصارف.

وتجدر الإشارة إلى أن الأبحاث القليلة التى تمت فى هذا الموضوع قد إستهدفت التعرف على المخاطر المحتملة التى قد تواجه أو تهدد أمن تلك النظم والتعرف على أسبابها ومحاولة تطوير قائمة تتضمن أهم المخاطر التى قد تواجه أمن النظم المحاسبية الإلكترونية، ومن ثم محاولة إختبار مدى جوهرية وأهمية تلك المخاطر فى الواقع العملى من خلال مجموعة من الدراسات الميدانية التى تمت فى هذا الشأن، وذلك من خلال التعرف على معدل تكرار حدوثها وحجم الخسائر المالية الناجمة عنها.

(١) وتعد الدراسة التى قام بها Loch وآخرون (١٩٩٢) من أوئل الدراسات فى هذا المجال، حيث قام Loch ورفاقه بعمل دراسة مسحية إستهدفت إستكشاف مدى إدراك مديرى نظم المعلومات الإدارية فيما يتعلق بالمخاطر الأمنية التى تواجه أمن النظم المحاسبية الإلكترونية فى بيئة الحاسبات الشخصية والحاسبات الكبيرة وكذلك شبكة الحاسبات الإلكترونية.

ولقد قام Loch ورفاقه بتطوير قائمة تضمنت إثنتى عشرة من المخاطر المحتملة التى قد تواجه أمن نظم المعلومات المحاسبية الإلكترونية بناءً على الأبحاث النظرية المتاحة وكذلك

محاولة إختبار مدى وجود وأهمية تلك المخاطر عملياً من خلال البحث الميدانى، ولقد تضمنت تلك القائمة المخاطر التالية:-

١. الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة موظفى المنشأة .

٢. الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة موظفى المنشأة .

٣. التدمير غير المتعمد للبيانات بواسطة موظفى المنشأة .

٤. التدمير المتعمد للبيانات بواسطة موظفى المنشأة .

٥. المرور (الوصول) غير المرخص للبيانات/ النظام بواسطة موظفى المنشأة .

٦. الرقابة غير الكفاية على الوسائل Media مثل الأشرطة والأقراص الممغنطة .

٧. الرقابة الضعيفة على المناولة اليدوية لمدخلات ومخرجات الحاسب الألى .

٨. الوصول غير المرخص به للبيانات/ النظام بواسطة أطراف خارجية (قراصنة المعلومات Hackers) .

٩. الوصول غير المرخص به للبيانات/ النظام من قبل المنافسون .

١٠. إدخال فيروسات الكمبيوتر إلى النظام أو البرامج .

١١. الأدوات الرقابية المادية غير الكافية .

١٢. الكوارث الطبيعية مثل الحرائق والفيضانات أو إنقطاع مصدر الطاقة وغيرها .

ولقد قام الباحثون بعمل دراسة مسحية شملت ٦٥٧ من مديرى نظم المعلومات الإدارية فى الولايات المتحدة، ولقد طلب من المشاركين فى الدراسة أن يقوموا بترتيب أهم ثلاث مخاطر فيما يتعلق بأمن نظم المعلومات المحاسبية الإلكترونية من بين بنود القائمة المقترحة للمخاطر،

ولقد أوضحت نتائج تلك الدراسة أن الكوارث الطبيعية والأحداث غير المقصودة لموظفى المنشأة قد تم تصنيفها ضمن الثلاث مخاطر الهامة فى جميع بيئات تكنولوجيا المعلومات، كما أعطى المشاركون فى الدراسة أهمية أكبر للمخاطر الداخلية مقارنة بالمخاطر الخارجية لأمن نظم المعلومات المحاسبية الإلكترونية، كما أظهرت الدراسة أن التدمير غير المتعمد للبيانات والإدخال غير المتعمد لبيانات غير سليمة بواسطة موظفى المنشأة وكذلك الرقابة غير الكافية على الوسائل مثل الأشرطة والأقراص الممغنطة تعد أهم ثلاث مخاطر تواجه أمن نظم المعلومات فيما يتعلق بأجهزة الحاسب الشخصية .

بينما أوضحت الدراسة أن أهم ثلاث مخاطر تتعلق بأجهزة الحاسب الألى الكبيرة تتمثل فى الإدخال غير المتعمد لبيانات غير سليمة من قبل موظفى المنشأة، الكوارث الطبيعية، والتدمير غير المتعمد للبيانات بواسطة موظفى المنشأة، بينما أظهرت الدراسة أن الكوارث الطبيعية والدخول غير المصرح به للبيانات/ النظام من قبل أطراف خارجية (قراصنة المعلومات) وضعف الأدوات الرقابية المادية تعد أهم ثلاث مخاطر تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى بيئة شبكة الحاسب الآلى .

(٢) وفي دراسة للباحث Ryan and Bordoloi (1997) وهي دراسة تطبيقية لتقييم مخاطر أمن نظم المعلومات فى النظم المحاسبية الإلكترونية فى المنشأت التى تحولت من نظام أجهزة الكمبيوتر الكبيرة إلى نظام خدمة العملاء، ولقد قام الباحثان بتطوير قائمة شملت خمسة عشر من المخاطر المحتملة التى قد تهدد أمن نظم المعلومات الإلكترونية بناء على الدرسات السابقة والأبحاث التى تمت فى هذا الشأن، ولقد قام الباحثان بتوزيع قائمة إستقصاء على مائة

وعشرين شركة من الشركات الكبيرة والمتوسطة الحجم فى الولايات المتحدة، وتم الحصول على ردود من ٥٢ شركة بما يعادل ٤٧% من عدد الإستبيانات التى تم توزيعها، ولقد طلب من المشاركين فى الإستبيان أن يقوموا بترتيب مدى خطورة وأهمية المخاطر المحتملة لأمن نظم المعلومات المحاسبية الإلكترونية فى بيئة أجهزة الحاسب الألى الكبيرة وكذلك فى نظام خدمة العملاء مستخدمين فى ذلك 10- Point Scale حيث يشير الرقم ١ إلى أن عنصر المخاطر المقترح غير هام بالنسبة للمنشأة بينما يشير الرقم ١٠ إلى أن عنصر المخاطر يعد ذو أهمية كبيرة ومحل إهتمام بالنسبة للمنشأة .

وتشير نتائج تلك الدراسة إلى وجود فروق جوهرية (عند مستوى معنوية P = 0.05) بين المنشأت التى لديها نظام أجهزة الكمبيوتر الكبيرة وتلك التى تطبق نظام خدمة العملاء فيما يختص بمخاطر أمن نظم المعلومات المحاسبية الإلكترونية التالية : التدمير غير المتعمد للبيانات بواسطة موظفى المنشأة، الإدخال غير المتعمد لبيانات خاطئة بواسطة موظفى المنشأة، التدمير المتعمد للبيانات بواسطة موظفى المنشأة، الإدخال المتعمد لبيانات خاطئة بواسطة موظفى المنشأة، الخسائر الناجمة عن عدم إعداد نسخ إضافية Backups أو الرقابة على ملفات الدخول للنظام Log Files، أو فشل النظام وسقوط الشبكات، وقد أعترف الباحثان أن قائمة المخاطر المقترحة من قبلهم قد تضمنت بعض العناصر التى لايمكن إعتبارها ضمن مخاطر أمن نظم المعلومات بالمعنى الدقيق .

(٣) وفي دراسة قام بها الباحث Dhillon (1999) تتعلق بطبيعة اختراقات أمـــن المعلومات التي حدثت في أماكن مختلفة من العالم، حيث ناقش فيها العديد من خـــسائر

أمن المعلومات التي تنتج من الاحتيال على أنظمة الحاسوب، حيث أنه يمكن تفادي هذه الخسائر إذا تبنت المنظمات نظرة أكثر واقعية في التعامل مع مثل هذه الحوادث بالإضافة إلى تبني نظرة تحكم أمنية تضع تأكيدا متساويا للتدخلات الشكلية والرسمية والتقنية لأنظمتها الإلكترونية، ومن خلال نتائج الدراسة اقترح بأن تطبيق السيطرة، كما هو معرف في سياسة أمن المعلومات، يردع حقيقية سوء استعمال الحاسوب، كما أن ارتكاب الاحتيال على أنظمة الحاسوب من قبل المستخدمين الداخليين، تعرف كمشاكل التخزين، واحتيال أنظمة الحاسوب عالية التقنية يصعب منعها خاصة إذا امتزجت بالمعاملات القانونية .

(٤) وهناك دراسة أخرى للباحث (2000) Siponen قدمت تصورا لبرنامج وعي أمن المعلومات في المؤسسات وذلك لتقليل أخطاء المستخدمين، ولتحسين فعالية سيطرة الأمن المطبقة، وقد توصل (2000) Siponen إلى أن تقنيات أو إجراءات أمن المعلومات تفقد فائدتها الحقيقية إذا تم إساءة استخدامها، أو تم تفسيرها بطريقة خاطئة أو تم تطبيقها بشكل غير صحيح من قبل المستخدمين.

(٥) وفى دراسة أخرى قام (2001) Abu-Musa بعمل دراسة تطبيقية لإستكشاف وإختبار المخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى القطاع المصرفى بجمهورية مصر العربية، حيث قام أبو موسى بعمل دراسة مسحية شملت جميع البنوك الرئيسية العاملة بجمهورية مصر العربية مستخدماً فى ذلك إستمارة إستقصاء للتعرف على أراء كل من رؤساء أقسام الحاسب الألى ورؤساء أقسام المراجعة الداخلية فيما يختص بالمخاطر الهامة التى تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى البنوك التى يعملون

بها، ولقد تم الحصول على ردود تتمثل فى ٧٩ إستمارة إستقصاء من بينها ستة وأربعون إستمارة إستقصاء تم إستيفاء بياناتها من قبل رؤساء أقسام الحاسب الألى، وثلاثة وثلاثون تم ملئ بياناتها بواسطة رؤساء أقسام المراجعة الداخلية، ومن ثم كانت نسبة الردود هى ٧٩% فيما يختص بأقسام الحاسب الألى و ٥٧% فيما يختص بأقسام المراجعة الداخلية.

ومن خلال تلك الدراسة قام أبوموسى بتطوير قائمة شملت تسعة عشر من المخاطر المحتملة لأمن نظم المعلومات المحاسبية الإلكترونية لإختبار مدى تواجدها وأهميتها فى البيئة المصرية. وتضمنت تلك القائمة بعض المخاطر المحتملة التى تم إختبارها لأول مرة فى تلك الدراسة والتى تتعلق بصفة أساسية بمخاطر أمن مخرجات النظام المحاسبى، ولقد تضمنت القائمة المخاطر الأتية:-

١. الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين .
٢. الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين .
٣. التدمير غير المتعمد (غير المقصود) للبيانات بواسطة الموظفين .
٤. التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين .
٥. المرور (الوصول) غير الشرعي (غير المرخص به) للبيانات/ النظام بواسطة الموظفين.
٦. المرور غير الشرعي (غير المرخص به) للبيانات/ النظام بواسطة أشخاص من خارج المنشأة .
٧. اشتراك الموظفين في كلمة السر .

٨. الكوارث الطبيعية مثل الحرائق، الفيضانات أو انقطاع مصدر الطاقة .

٩. الكوارث غير الطبيعية والتي هي من صنع الإنسان مثل الحرائق، أو الفيضانات .

١٠.إدخال فيروس الكمبيوتر للنظام المحاسبي .

١١.طمس أو تدمير بنود معينة من المخرجات .

١٢.خلق مخرجات زائفة/ غير صحيحة .

١٣.سرقة البيانات/ المعلومات .

١٤.عمل نسخ غير مصرح (مرخص) بها من المخرجات .

١٥.الكشف (الإظهار) غير المرخص به للبيانات عن طريق عرضها على شاشات العــرض أو طبعها على الورق .

١٦.طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك .

١٧.المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم / ليس لهم الحق فى استلام نسخة منها .

١٨.المستندات الحساسة يتم تسليمها إلى أشخاص لا تتوافر فيهم الناحية الأمنية وذلك بغرض تمزيقها .

١٩.مقاطعة تحويل البيانات من أماكن بعيدة .

وتشير نتائج الدراسة إلى أن الإدخال غير المتعمد لبيانات غيرصحيحة من قبل موظفى البنوك، التدمير غير المتعمد للبيانات من قبل موظفى البنوك، إدخال فيروس الكمبيوتر إلى النظام، الكوارث الطبيعية والكوارث التى هى من صنع الإنسان، إشتراك بعض الموظفين فى إستخدام نفس كلمة السر، وكذلك توجية البيانات والمعلومات إلى أشخاص غير مخول لهم بإستلامها تعد

من أهم المخاطر التى تواجه أمن نظم المعلومات المحاسبية الإلكترونية فى البنوك المصرية. وتجدر الإشارة إلى أنه فى جميع الحالات فإن رؤساء أقسام المراجعة الداخلية قد أعطوا تقديرات أعلى لمعدلات حدوث تلك المخاطر فى البنوك التى يعملون بها مقارنة بتقديرات رؤساء أقسام الحاسب الألى، وتشير نتائج الدراسة أنه لا توجد إختلافات جوهرية بين أنواع البنوك المختلفة إلا فيما يختص بالمرور غير المرخص به للبيانات/ النظام من قبل أطراف خارجية (قراصنة المعلومات) .

(٦) وهناك دراسة للباحث Michael E. Whitman (٢٠٠٣) ركزت للإجابة على ثلاثة أسئلة، السؤال الأول يتعلق بحصر التهديدات التي تواجه أمن المعلومات، والسؤال الثـــاني يتعلق بدرجة خطورة هذه التهديدات، والسؤال الثالث يتعلق بعدد مرات حدوثها (شهريا)، حيـــث قام الباحث بعمل تقييم لعدد من الأبحاث والمقالات في مجال أمن المعلومات، وحصر التهديـــدات التي تواجه أمن المعلومات لتشمل اثنتي عشرة وهي كالتالي:

١. الخطأ أو الفشل البشري (حوادث،أخطاء المستخدمين)
٢. سرقة الحقوق الذهنية والفكرية (قرصنة، انتهاك حقوق الطبع)
٣. أفعال التجسس المتعمدة (وصول غير مخول)
٤. أفعال متعمدة لإبتزاز المعلومات (ابتزاز كشف المعلومات)
٥. أفعال متعمدة للتخريب أو التدمير (دمار الأنظمة أو المعلومات)
٦. أفعال متعمدة للسرقة (مصادرة غير شرعية من الأجهزة أو المعلومات)
٧. هجوم متعمد للبرمجيات (فيروسات، نكران الخدمة، حصان طروادة)
٨. قوة الطبيعة (نار، فيضان، زلزال، برق)

٩. نوعية انحرافات الخدمة من مجهزو الخدمة (قضايا متعلقة بالشبكة وقوتها)

١٠.حالات فشل أو أخطاء أجهزة تقنية (فشل أجهزة)

١١.حالات فشل أو أخطاء البرامج التقنية (أخطاء برمجية، فجوات مجهولة)

١٢.تقادم تكنولوجي

ثم قام الباحث بعمل دراسة مسحية شملت ١٠٠٠ موظف أغلبهم من مدراء نظم المعلومات، والمدراء و مشرفين، ولقد طلب من المشاركين فى الدراسة أن يقوموا بترتيب أهم ثلاث مخاطر فيما يتعلق بأمن نظم المعلومات من بين بنود القائمة المقترحة للمخاطر، ولقد أوضحت نتائج تلك الدراسة أن الهجوم المتعمد للبرمجيات وحالات فشل أو أخطاء البرامج التقنية والخطأ أو الفشل البشري قد تم تصنيفها ضمن الثلاث مخاطر الهامة فى جميع بيئات تكنولوجيا المعلومات.

وفيما يتعلق بعدد التهديدات الشهرية لأمن المعلومات، أوضحت الدراسة أن بعض التهديدات لم يتم اكتشافها، مثل الأفعال المتعمدة لابتزاز المعلومات، والاستملاك الغير شرعي للمعلومات من المنظمة، نسب معظمهم ذلك إلى الطبيعة الشريرة للدخلاء، لكن بشكل عام معظم المستجيبين أشاروا إلى حدوث معظم التهديدات سواء داخلية أو خارجية .

وأوضحت الدراسة أن التهديد حقيقي، وخطورته عالية، وأن الأنظمة المعرضة للتهديد يصعب حمايتها، وركزت الدراسة على أن الإدارة يجب أن تكون مطلعة أكثر على تهديدات أمن المعلومات، ويجب أن يزداد وعيها في كل المجالات، وأن مستوى فهمهم العام لأمن المعلومات متأصل من علاقتها مع البيئة التي تعمل بها .

(٧) **ولقد قام Abu-Musa (2004) بعمل دراسة تطبيقية للتعرف على المخاطر الهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية فى المنشأت السعودية**، ولقد أظهرت نتائج الدراسة أن نسبة عالية من المنشأت التى شاركت فى الإستقصاء قد عانت من وجود خسائر مالية كبيرة نتيجة بعض التعديات على أمن نظم المعلومات المحاسبية بها سواءً من قبل أطراف داخلية (موظفى المنشأة) أو أطراف خارجية (قراصنة المعلومات)، وأن تلك الخسائر قد تراوحت ما بين ١٠٠,٠٠٠ ريال سعودى و ٢٠٠ مليون ريال سعودى، كما أوضحت الدراسة أن كثيراً من تلك التلاعبات والإختلاسات والتعديات على أمن نظم المعلومات المحاسبية قد تم إكتشافها عن طريق الصدفة نتيجة لعدم كفاية وفعالية الأدوات والضوابط الرقابية المطبقة فى تلك المنشأت، وأن معظم الإختلاسات والتلاعبات التى تم إكتشافها قد تم تسويتها داخلياً ولم يتم الإفصاح أو التقرير عنها للجمهور حفاظاً على سمعة الشركة وتحسين صورتها فى السوق .

أما فيما يختص بمدى إدراك المنشأت السعودية للمخاطر الهامة التى تهدد نظم المعلومات المحاسبية ومعدلات تكرار حدوث تلك المخاطر بها، حيث أشارت نتائج الدراسة إلى أن أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشآت السعودية هي: الإدخال المتعمد وغير المتعمد لبيانات غير صحيحة بواسطة موظفي المنشآت، إدخال فيروسات الكمبيوتر إلى النظام المحاسبي، مشاركة الموظفين في استخدام نفس كلمات السر، طمس أو تدمير مخرجات الحاسب الآلي، الكشف (الإظهار) غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الأوراق، وكذلك توجيه المطبوعات والمعلومات إلى أشخاص غير مخول لهم باستلام تلك المعلومات أو الإطلاع عليها، ولم تظهر

النتائج أي اختلافات جوهرية بين المنشآت المختلفة فيما يختص بتقديرها لأهمية المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في بيئة الأعمال السعودية.

ولكن من خلال ما سبق نجد أن جميع الدراسات السابقة ركزت على أهمية المخاطر التي تواجه أمن نظم المعلومات وأنواع تلك المخاطر، ولكن لم يتم دراسة أسباب حدوث المخاطر أو التعرف على الاجراءات اللازمة من أجل مواجهة تلك المخاطر ومنع حدوثها، ولذلك فإن الباحثة قد ركزت في دراستها على معرفة المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية، إضافة إلى معرفة أسباب حدوث تلك المخاطر وإجرارات الحماية المتبعة ضد مخاطر أمن نظم المعلومات المحاسبية .

الفصل الثاني

نظم المعلومات المحاسبية وعلاقتها بالحاسوب

الفصل الثاني

نظم المعلومات المحاسبية الإلكترونية

تعتبر المحاسبة علم اجتماعي ونشاط خدمي يخدم العديد من الأطراف المهتمة والمستخدمين سواء كانوا من داخل المؤسسة أو من خارجها ولذلك تنبع ضرورة المحاسبة من خلال حاجتها إلى المعلومات التي يمكن أن تساعدها في تلبية احتياجات المهتمين والمستخدمين لمساعدتهم في اتخاذ القرارات الاقتصادية المناسبة.

وتعتبر نظم المعلومات أو تكنولوجيا المعلومات أحد المجالات الهامة التي ينبغي على المحاسبين الإلمام بها والتعرف عليها وذلك نظرا لاعتماد المحاسبين على كم كبير من المعلومات في عملهم والتي يمكن الحصول عليها من خلال نظام المعلومات المحاسبي الذي يعتبر كأداة فعالة لتـــوفير المعلومات اللازمة للإدارة أو المؤسسة .

وقد أصبحت نظم المعلومات عنصرا أساسيا في المنشأة يعتمد عليه في شتى المجـــالات لـــدعم أنشطتها من أجل تحقيق أهدافها المنشودة سواء كانت تلك الأهداف تسعى إلى تحقيق الربح أو لا تسعى إلى تحقيق الربح .

وقبل التطرق إلى تعريف نظم المعلومات المحاسبية لا بد لنا من التعرف على مفهوم النظام والبيانات والمعلومات .

وبالنسبة لتعريف النظام فهناك العديد من التعريفات لهذا المفهوم، حيث تطـــرق الـــبعض إلـــى تعريف النظام حسب مدخلين وهما مدخل النظم والمدخل التحليلي .

فقد عرف سكودربك شارلز وآخرون (١٩٨٠ ،ص١٢) النظام حسب مدخل النظم بأنه :

"مجموعة من الأجزاء التي ترتبط ببعضها ومع البيئة المحيطة وهذه الأجزاء تعمل كمجموعة واحدة من أجل تحقيق أهداف النظام "

"ولكن عرفه حسب المدخل التحليلي بأنه مجموعة من الأجزاء المستقلة عن بعضها البعض"[٢].

ومن خلال ما سبق يتضح لنا أن التعريف الثاني يركز على استقلالية أجزاء النظام عن بعضها البعض وهذا ما يعيب هذا التعريف حيث لا يمكن درسة أي نظام بجزئيات مستقلة دون الربط بين تلك الجزئيات، بل يجب أن تكون تلك الجزئيات مترابطة ولا يمكن فصلها عن بعضها البعض .

ويعرف الدهراوي ومحمد (٢٠٠٢ ، ص١٦) النظام بأنه :

"عبارة عن إطار عام متكامل يحقق عدة أهداف، فهو يقوم بتنسيق الموارد اللازمة لتحويل المدخلات إلى مخرجات، وهذه الموارد تتراوح من المواد إلى الآلات وعناصر الطاقة الإنتاجية وذلك حسب نوع النظام"

وعرفه (Cashing ,B ,1974)[٣] بأنه :

"عبارة عن مجموعة من المركبات والوحدات ذات العلاقة، أو هو مجموعة أغراض ذات علاقة بعضها مع البعض الآخر مع خصائصها"

ولكن هذه التعريفات لم توضح الهدف من النظام، بل ركزت على أجزاء ومكونات النظام دون التطرق إلى الأهداف التي يسعى إليها النظام.

---

[2]- نقلا عن الدهراوي (٢٠٠٣ ،ص٤)

[3]- نقلا عن (الراوي،١٩٩٩ ،ص٢٣)

ولكن جمعة وآخرون (٢٠٠٣،ص١٥) عرفوا النظام بشكل عام بأنه :

"شبكة من الإجراءات ذات العلاقات المترابطة ببعضها البعض، والتي يتم إعـدادها بطريقة متكاملة بغرض أداء نشاط معين، ويحتوي النظام المحاسبي على شبكة مـن التعليمات والإجراءات المحاسبية، والتي تمثل سلسلة من العمليات الكتابية والحسابية والتي يقوم بها عدد من الأفراد المؤهلين، وتتم في عدد من الأقسام داخـل الوحـدة الاقتصادية" .

ويعرف طه(٢٠٠٠ ،ص٢٣) النظام بأنه :

"مجموعة من المكونات ذات علاقات متداخلة مع بعضها تعمل على نحو متكامـل داخل حدود معينة لتحقيق هدف أو أهداف مشتركة في بيئة ما، وفي سبيل ذلك تقبل مدخلات وتقوم بعمليات وتنتج مخرجات، وتسمح باستقبال مدخلات مرتدة (تغذيـة عكسية)" .

كما ويعرف قاسم (٢٠٠٣ ،ص١٧) النظام على أنه :

"مجموعة من العناصر التي ترتبط مع بعضها بسلسلة من العلاقـات بهـدف أداء وظيفة محددة أو مجموعة من الوظائف، فالنظام عبارة عن مجموعة من العناصـر التي تشكل ما يدعى بمكونات النظام التي تكون إما عبارة عن مكونات مادية مثـل الحواسيب أو الشاشات أو خطوط الاتصال أو الورق أدوات الكتابـة والطباعـة أو مكونات معنوية مثل البرامج والملفات والأنظمة والقوانين والتعليمـات والعلاقـات هي كل ما يعمل على ربط مكونات النظام مع بعضها بحيث تشكل هـذه العناصـر منظومة نافعة تؤدي وظيفة معينة أو مجموعة من الوظائف"

ومن خلال ما سبق يمكن أن نعرف النظام بأنه عبارة عن اطار عام وشـامل لمجموعـة مـن العناصر المترابطة مع بعضها البعض ومع البيئة المحيطة بها من أجل تحقيق الأهـداف التـي يسعى هذا النظام إلى تحقيقها، سواء كانت الأهداف رئيسية أو فرعية، وتتحدد تلك الأهداف بنوع النظام الذي نعنيه، فمثلا لوكانت المنشأة صناعية فإن الهدف الرئيسي لها قد يكون تحقيق أقصى

قدر ممكن من الأرباح، ولذلك لا بد لها من تحقيق الأهداف الفرعية وهي زيادة المبيعات وخفض التكاليف، كما أن النظام المحاسبي يسعى إلى توفير المعلومات اللازمة عن طبيعة وأوجه نشاط المنشأة وتوفير معلومات تفيد الفئات المستفيدة في اتخاذ القرارات اللازمة وتوفير المعلومات التي تساعد الإدارة في حماية أموالها وأصولها والمحافظة على أمن معلوماتها للحد من تعرضها للمخاطر التي تعيق تحقيق أهداف النظام .

تعريف البيانات والمعلومات :

تعتبر البيانات هي المواد الخام التي يعتمد عليها النظام، كما أن المعلومات هي المخرجات الرئيسية للنظام (كما سيلي شرحه فيما بعد)، أما من حيث التعريف والمفهوم فتعرف البيانات والمعلومات بأنها :

أولا : البيانات :

"هي حقائق أولية وأرقام إذا ما جمعت معا فإنها تمثل المدخلات لنظام المعلومات" (الدهراوي ومحمد ،٢٠٠٢،ص١٥)

ويعرف تنتوس (١٩٩٨، ص١٢٥) البيانات بأنها عبارة عن :

"حقائق وأرقام مشوشة وغير مرتبة ومزدحمة بحيث لا يمكن استخراج أي حكمة أو قاعدة منها قبل أن يتم معالجتها بالصورة الواردة أعلاه".

وهناك تعريف آخر للبيانات وهو أن :

"البيانات Data هي عبارة عن الأعداد والأحرف الأبجدية والرموز التي تقوم بتمثيل الحقائق والمفاهيم بشكل ملائم يمكن من إيصالها وترجمتها ومعالجتها من قبل الإنسان أو الأجهزة لتتحول إلى النتائج". (قاسم، ٢٠٠٣، ص١٥)

أما الراوي (١٩٩٩ ،ص٤٠) فيعرف :

"البيانات Data كونها الأرقام أو الأعداد غير المفسرة أو المحللـــة أو المعالجـــة أو كونها الأرقام المطلوب معالجتها بواسطة النظام".

ثانيا : المعلومات

والمعلومات هي "عبارة عن بيانات معالجة بصورة أعطتنـــا (معلومـــات) مفيـــدة" (تنتوش،١٩٩٨،ص ١٢٥) .

"كما أن المعلومات تتكون من بيانات تم تحويلها وتشغيلها لتصبح لها قيمة، وبالتالي فإن المعلومات تمثل معرفة لها معنى وتفيد فـــي تحقيـــق الأهـــداف" (الـــدهراوي ومحمد،٢٠٠٢، ص١٥).

أوهي "البيانات التي تعطي معنى وأكثر من ذلك كونها ذات قيمة والتي تحقق هدفا معينا (الراوي،١٩٩٩،ص٤٠) .

و يعرفها (عوض،١٩٨٩، ص٤٠) بأنها :

"عبارة عن مجموعة الحقائق والبيانات المعرفة والمسجلة في صـــورة مفـــردات أو مسموعة بها أو مرئية حيث يمكن اتخاذ القرارات الإدارية عليها".

ويعرفها(قاسم،٢٠٠٣،ص١٥) بشكل أشمل المعلومات بأنها :

"عبارة عن البيانات التي تمت معالجتها بشكل ملائم لتعطي معنى كاملا يمكن مـــن استخدامها في العمليات الجارية والمستقبلية لاتخاذ القرارات".

ومن خلال التعريفات السابقة يمكن إيجاز تعريف للبيانات بأنها عبارة عن حقائق وأرقام خام غير معدة للاستخدام بشكلها الحالي، أما المعلومات فهي عبارة عن بيانات تمت معالجتها وأصبحت جاهزة للاستخدام ويمكن تقديمها للأطراف المهتمة للاستفادة منها.

كما أن البيانات تمثل مرحلة أساسية وهامة من مراحل النظام وهي المدخلات والتي ينبغي أن تكون سليمة وواضحة، فلو كانت البيانات المدخلة إلى النظام غير صحيحة أو غير سليمة فإنها تؤدي للوصول إلى نتائج غير سليمة والتي يعبر عنها بالمعلومات والتي تمثل مرحلة المخرجات بالنسبة للنظام .

وبالتالي فإن ادخال بيانات غير سليمة للنظام يؤدي للوصول لمخرجات زائفة غير صحيحة والتي تعتبر من ضمن المخاطر التي تهدد أمن نظم المعلومات المحاسبية االإلكترونية .

مكونات النظام:

من خلال ما سبق يمكن التوصل إلى أن النظام هو عبارة عن إطار شامل لمجموعة من الأجزاء والعناصر المترابطة والمتصلة بالبيئة المحيطة والتي تتفاعل فيما بينها من أجل تحقيق أهداف معينة تفيد الأطراف المستفيدة.

ولذلك فإن عناصر النظام تتكون من العناصر الأساسية التالية:

- المدخلات Inputs
- التشغيل Processing
- المخرجات Outputs
- التغذية العكسية Feedback

أولا/ المدخلات Inputs

حيث تتمثل المدخلات في المواد والأرقام الخام التي يتم تحديدها وتجميعها وإدخالها إلى النظام ليقوم بعملية معالجتها وتشغيلها من أجل الحصول على المعلومات .

> وتعتبر المدخلات "القوة الدافعة والوقود اللازم لتشغيل النظام وهذه المدخلات ممثلة في مواد أولية، عمالة، رأسمال، معلومات أو أي شيء يحصل عليه النظام من البيئة المحيطة ومن نظم أخرى" (الدهراوي ومحمد،٢٠٠٢، ص٥).

ثانيا/ التشغيل Processing

وهي عملية معالجة البيانات التي تم إدخالها إلى النظام للحصول على المعلومات المفيدة وتتمثل تلك البيانات في المدخلات التي يتم تشغيلها ومعالجتها ليتم تحويلها إلى مخرجات .

وتمثل مرحلة التشغيل "الجانب الفني من النظام والذي يقوم بإجراء العديد من العمليات في نفس المرحلة، والتشغيل بهذا يمثل تفاعل كل العوامل داخل النظام مثل عوامل الإنتاج في الوحدة الاقتصادية في صورة نشاط ينتج عنه عملية تحويل المواد الأولية إلى منتجات نهائية، ويتم تحويل البيانات في نظم المعلومات إلى معلومات بطرق التشغيل المختلفة من تسجيل، تلخيص، حساب، مقارنة.. الخ". (الدهراوي ومحمد، ٢٠٠٢، ص٧).

ثالثا/ المخرجات Outputs

وهي النتيجة النهائية التي يتم التوصل إليها بعد عملية التشغيل على المدخلات للوصول إلى الناتج النهائي وتقديمه للفئات المستفيدة لمساعدتها في اتخاذ القرارات المناسبة سواء كانت تلك الفئات داخلية أو خارجية.

"حيث أن المخرجات وهي الناتج النهائي من النظام والذي يذهب إلى البيئة المحيطة أو إلى نظم أخرى، وقد تكون هذه المخرجات في صورة منتج نهائي أو وسيط، خدمة للمستهلك أو معلومات تستخدم في اتخاذ القرارات الإدارية أو تستخدم كبيانات لنظام معلومات آخر" (الدهراوي ومحمد،٢٠٠٢، ص٧).

رابعا/ التغذية العكسية Feedback

وهي عبارة عن مخرجات يتم ارجاعها لأشخاص مناسبين في المؤسسة لتساعدهم في تقييم وتصحيح مرحلة الإدخال .(Laudon & Laudon, 2006, P19)

أنواع النظم Types of Systems

١. النظام المفتوح Open Systems

٢. النظام المغلق Closed System

النظام المفتوح Open System

ويطلق مصطلح النظام المفتوح على النظام الذي يمكن لأجزائه أن تتفاعل مع بعضها الـــبعض ومع البيئة المحيطة به خارج حدود النظام .

"ويحصل هذا النظام على مدخلاته من البيئة المحيطة به ليقوم بتأدية وظائفه المهمة ومن ثم إمداد البيئة بالمخرجات المطلوبة ليتم الاستفادة منها والتعليق عليها إن لـــزم الأمر، ومن الممكن أن تعود تلك المخرجات لتكون مدخلات مرة أخرى أي حدوث التغذية العكسية . (الراوي،١٩٩٩، ص٨).

ويتضح النظام المفتوح من خلال الشكل رقم (١)

النظام المغلق Closed System

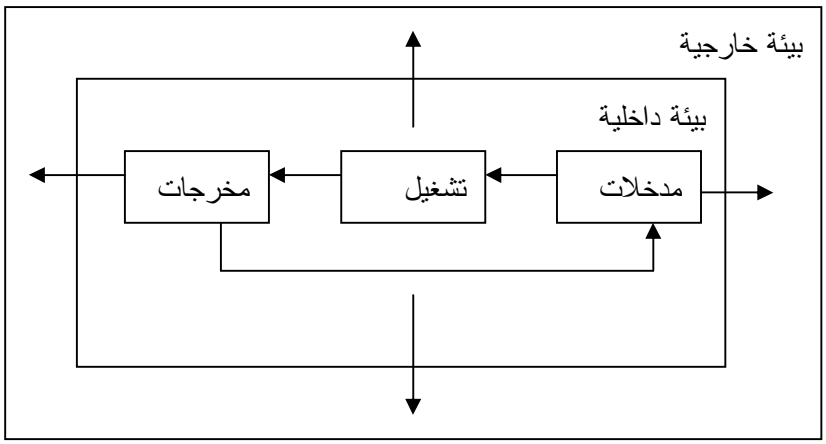
وهذا النوع من الأنظمة لا تتفاعل أجزاؤه مع عناصر البيئة الخارجية المحيطة به وإنما هو مغلق على نفسه حيث أن أجزاؤه الداخلية تتفاعل مع بعضها البعض ،كما أنه لا يستمد أي مدخلات من البيئة الخارجية ولا يقدم لها أي مخرجات يتم التوصل لها وإنما مدخلاته من البيئة الداخلية له .

"حيث أن التغذية العكسية من الممكن أن تحدث داخل النظام نفسه ومتصلة بالرقابـــة ولا يمكن أن تخترق حدود النظام . (طه،٢٠٠٠، ص٣٤)

ويتضح النظام المغلق من خلال الشكل رقم (٢)

ومن خلال ما سبق يمكن اعتبار النظام المحاسبي بأنه نظام مفتوح حيث يتعامل مع البيئة الداخلية والخارجية للنظام وذلك من خلال قيامه بإمداد البيئة الخارجية بالمعلومات التي تتمثل في التقارير والقوائم المالية التي تساعدهم في اتخاذ القرارات المناسبة .

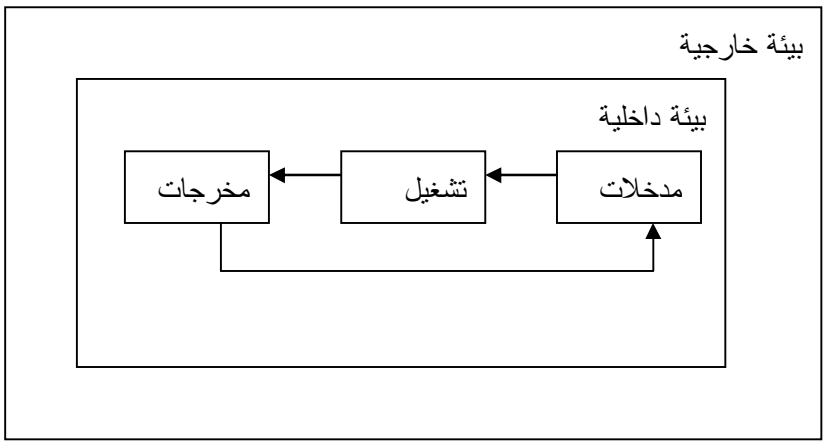
شكل رقم (١)



شكل يوضح النظام المفتوح

(الراوي،١٩٩٩،ص٣٩)

شكل رقم (٢)



شكل يوضح النظام المغلق

(الراوي،١٩٩٩،ص٣٩)

بيئة النظام

من خلال ما سبق تم التوصل إلى أن النظام عبارة عن اطار شـــامل لمجموعـــة مـــن الأجـــزاء والعناصر المترابطة فيما بينها والمتصلة بالبيئة المحيطة بها، ولذلك فإن كل نظـــام لا بـــد وأن يعمل داخل بيئة محيطة به تقع خارج حدوده تؤثر به وتتأثر به وذلك من خلال العمليات التبادلية التي تحدث بينهما.

حيث أن البيئة المحيطة بالنظام تتمثل في جميع المتغيرات التي لا تخضع تماما لسيطرة النظـــام، أي أنها تقع خارج حدود النظام ولا بد للنظام بأن يتفاعل معها ويتكيف مع متغيراتهـــا . (طـــه، ٢٠٠٠،ص٣٥)

ويذكر الدهراوي ومحمد (٢٠٠٢، ص٩) أن :

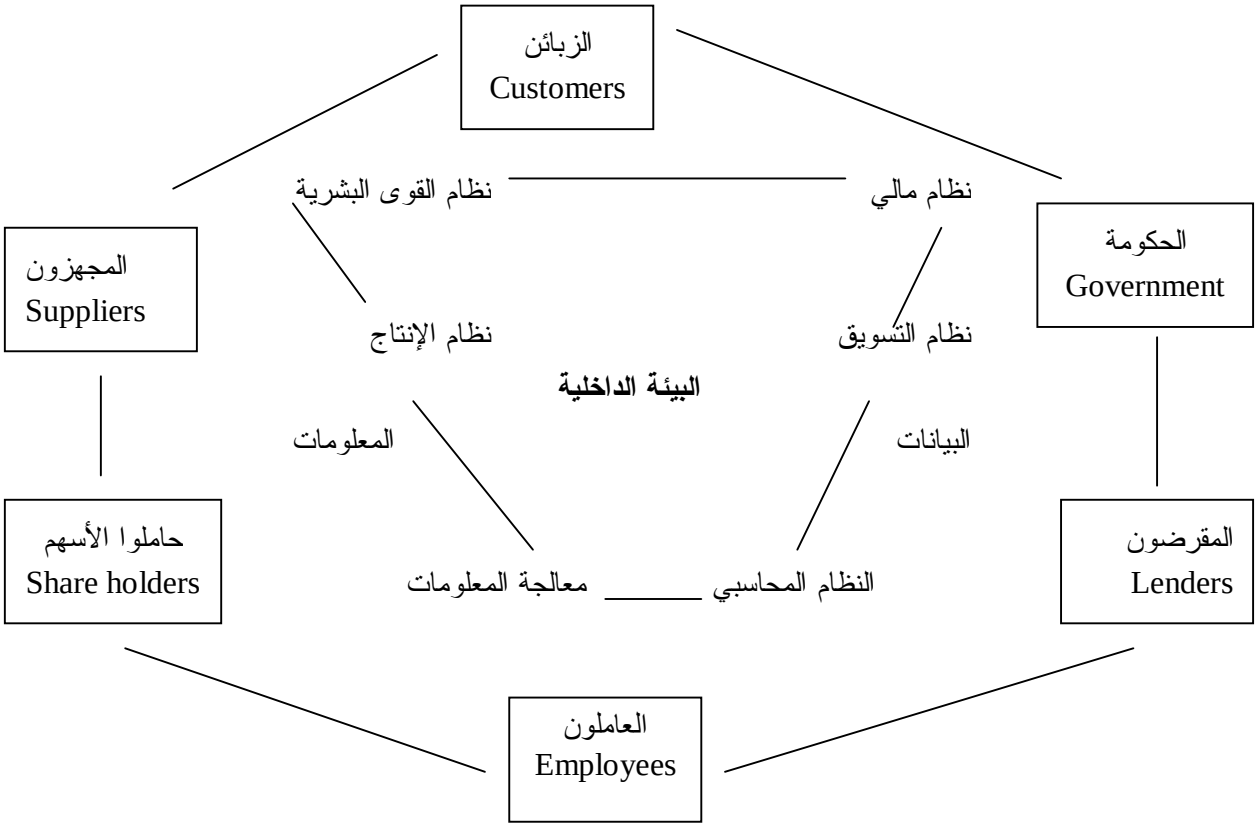
"بيئة النظام تتمثل في كل العناصر والعوامل المؤثرة في النظام والتي لا تخضع لسيطرة أو رقابة النظام" .

وأما الراوي (١٩٩٩، ص٢٥) فقد عرف مفهوم البيئة :

"بأنه مجموعة المحددات أو الإطار المحيط بذلك الشيء ويقسم بيئـــة النظـــام إلـــى قسمين:

- البيئـــة الخارجيـــة للنظـــام External Environment وتتمثـــل فـــي الزبـــائن والمجهزون وحاملو الأسهم والعاملون والمقرضون والحكومة".
- البيئة الداخلية للنظام Internal Environment وتتمثل في مجموعة الإجراءات

شكل رقم (٣)



شكل يوضح بيئة المنشأة وأهم الأنظمة الداخلية والخارجية

المصدر : الراوي (١٩٩٩، ص٢٦)

حدود النظام:

ويتم تحديد حدود النظام حسب الغرض من الدراسة أو البحث حيث أن كل نظام يعمل داخل حدود معينة.

كما ينظر إلى حدود النظام باعتبارها الخط الفاصل عن البيئة المحيطة به وعن الأنظمة الأخرى والذي يضم داخله مكونات النظام ولذلك فإن بيئة النظام تتمثل في جميع الأشياء التي تقع خارج حدود النظام حيث يكون مستوى تبادل العمليات خارج حدود النظام أقل مما يتم تبادله من مكونات النظام داخل حدوده، كما أن حدود النظام تتغير وفقا لنوع النظام حيث أنه في حالة النظم المادية تكون الحدود ثابتة ومميزة، أما في حالة النظم المجردة فيتم رسم الحدود من خلال محلل النظم بطريقة حكمية بناء على المتغيرات الخاضعة للدراسة . (طه، ٢٠٠٠، ص٣٧).

نظام المعلومات

تعتبر نظم المعلومات المصدر الرئيسي للإدارة لتزويدها بالمعلومات اللازمة لاتخـــاذ القـــرارات المناسبة التي تساعدها على أداء وظائفها بالطريقة الصحيحة والمثلى والوصول إلـــى الأهـــداف المطلوبة بأفضل الطرق وأمثلها.

حيث عرف أوبرن نظام المعلومات بأنه :

"مجموعة من الأفراد والإجراءات والبيانات تقوم بجمع وتشغيل (تحويـــل) ونـــشر المعلومات داخل المنظمة".(Obrien, J,.1996)[٤]

ونلاحظ بأن تعريف أوبرن ركز على المكونات البسيطة لنظم المعلوملت ووظيفتها المبدئية والتي تشمل عملية جمع وتشغيل البيانات ونشر للمعلومات .

ولكن الصباغ (٢٠٠٠ ،ص٨) عرف نظام المعلومات بأنه :

"عبارة عن مجموعة من الإجراءات والبرامج والمعدات والأساليب التـــي تعـــالج البيانات وتجعلها متاحة للإدارة لصناعة القرارات".

وبهذا نجد أن الصباغ توسع قليلا في التعريف ليضيف إلى المكونات السابقة لنظم المعلومات مكونات أساسية وهي المعدات والأساليب التي تستخدم في عملية معالجة البيانات .

وتعرف البكري (٢٠٠٤ ،ص١٤) نظام المعلومات بأنه :

"مجموعة من الإجراءات التي تقوم بجمع واسترجاع وتشغيل وتخزين وتوزيع المعلومات لتدعيم اتخاذ القرارات والرقابة في التنظيم".

---

[4]-نقلا عن طه (٢٠٠٠ ،ص٤٨)

ونجد أن البكري أضافت شيئ جديد للتعريفات السابقة وهو توضيح الهدف من نظم المعلومات .

ومع ذلك نجد بأن جميع التعريفات السابقة ركزت على الناحية الفنية لنظم المعلومات

ويعرف لاودن Laudon نظم المعلومات بصورة أدق وأوسع بأنها :

"مجموعة من العناصر المرتبطة مع بعضها البعض والتي تقوم بجمع (أو استرجاع) ومعالجة وتخزين وتوزيع المعلومات بغرض دعم صناعة القرار والتنسيق والتحكم بالمؤسسة، بالإضافة إلى مساعدة المد راء والعاملين في حل المشاكل وتصور الموضوعات الصعبة، وإنشاء أصناف جديدة (Laudon 2006, P13).

ونجد أن تعريف لاودن أشمل من التعريفات السابقة ولكن مع ذلك فإن جميع التعريفات السابقة لم تتطرق إلى الدور التقني لنظم المعلومات ولكن (Jessup & Valacich) عرفوا نظم المعلومات بأنها :

"مجموعة من القطع المادية والبرمجيات وشبكات الاتصال والتي يقوم الناس ببنائها واستخدامها لجمع وخلق وتوزيع البيانات المفيدة عمليا بما يتناسب مع إعدادات المؤسسة" (Jessup & Valacich, 2003, P4)

ويعرف طه (٢٠٠٠، ص٥١) نظم المعلومات المبنية على الحاسبات الآلية بأنها :

"مجموعة مترابطة ومنظمة من المكونات المادية للحاسبات الآلية Hardware وغير المادية Software والأفراد والبيانات والإجراءات التي تعمل بطريقة متكاملة في تجميع وتخزين ثم تحويل (معالجة) البيانات المدخلة لها إلى معلومات قابلة للاستخدام تفيد عملية اتخاذ القرارات في أنشطة الأعمال المختلفة" .

وقد ركزت التعريفات السابقة على نظم المعلومات كونها قطع مادية وبرمجيات وقطع غير مادية وأفراد وبيانات وإجراءات، وتعتبر القطع المادية والبرمجيات من أهم المكونات التي تستخدم في انشاء الجدران النارية والتي تعتبر أحد الوسائل الهامة لمواجهة الاختراقات التي قد تتعرض لها أمن نظم المعلومات المحاسبية .

ومن خلال التعريفات السابقة نصل إلى تعريف شامل لنظم المعلومات بأنه عبارة عن :

إطار شامل لمجموعة من المكونات (سواء كانت مكونات بشرية أو مادية) والتي تشتمل على العناصر والإجراءات التي تعمل مع بعضها البعض بشكل مترابط ومتكامل من خلال تطبيق وظائف النظام من ادخال وتشغيل للبيانات ثم استخراج النتائج وايصالها إلى الفئات المستفيدة لمساعدتها في اتخاذ القرارات اللازمة لأداء وظائفها في الوقت المناسب.

مداخل دراسة نظم المعلومات:

لدراسة نظم المعلومات والتعرف على جوانبها لا بد لنا من التعرف على المداخل الأساسية لدراسة نظم المعلومات وهي:

- المدخل الفني Technical Approach
- المدخل السلوكي Behavioral Approach
- المدخل الاجتماعي الفني Sociotechnical Approach

أولا : المدخل الفني Technical Approach

يركز المدخل الفني على النماذج المبنية على الرياضيات في دراسة نظم المعلومات، وكذلك التقنية المادية لهذه الأنظمة، حيث تشمل المجالات التي تساهم في المدخل الفني على علم الحاسوب والعلم الإداري وبحوث العمليات، كما ويهتم علم الحاسوب بترسيخ نظريات الحوسبة وطرقها وطرق معالجة وتخزين البيانات بطريقة فعالة، ويركز العلم الإداري على تطوير نماذج صناعة القرار وممارسات الإدارة، أما علم بحوث العمليات فيسلط الضوء على التقنيات الرياضية لاختيار المعاملات الأفضل للمؤسسة مثل النقل والتحكم بالمخزون وتكاليف الحركات. (Laudon & Laudon 2006, P26)

ثانيا : المدخل السلوكي Behavioral Approach

لقد اهتمت نظم المعلومات بالقضايا السلوكية والتي تزايدت مع تطور نظم المعلومات وإدارتها على الأمد البعيد، وهذه القضايا كتكامل الأعمال الاستراتيجي والتنظيم والتطبيق والاستخدام والإدارة لا تستطيع أن تتحد بطريقة جيدة مع النماذج المستخدمة في المدخل الفني، أي أنه لا

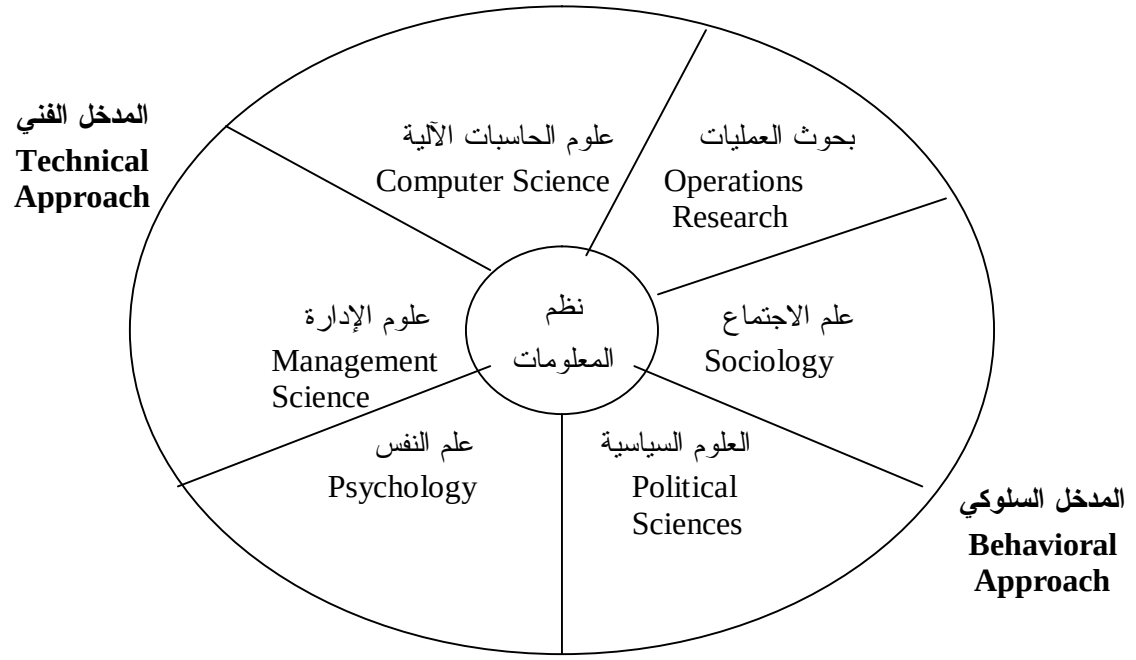
يمكن الاعتماد على المدخل الفني فقط في تفسيرها أو تحليلها، فمثلا علماء الاجتماع اهتموا بدراسة الاستخدام الجماعي لنظم المعلومات وكيفية تأثير استخدام هذه الأنظمة على الأفراد والمجموعات والمؤسسات، بينما اهتمت العلوم السياسية بالآثار المترتبة على توظيف المعلومات في مجال السياسة والاستخبارات، أما علماء النفس قاموا بدراسة نظم المعلومات لمعرفة استجابات الأفراد وردود أفعالهم واتجاهاتهم نحو التعامل مع نظم المعلومات وكيفية استيعابهم للتطورات في تقنية المعلومات ومدى تطبيق تلك المستحدثات في الواقع العملي بمنظماتهم، أما علماء الاقتصاد فيهتمون بدراسة نظم المعلومات لمعرفة الأنظمة التي تؤثر في التحكم والتكاليف داخل المؤسسة والسوق، وتجدر الإشارة إلى أن المدخل السلوكي لا يهمل الجانب التكنولوجي، حيث تعتبر تكنولوجيا نظم المعلومات المؤثر في المشكلة أو القضية السلوكية دائما، وأن التركيز في هذا المدخل ليس دائما على الحلول التكنولوجية فقط، بل الأخذ بعين الاعتبار التغيرات والمواقف والإدارة والسياسة التنظيمية والسلوك . (Laudon & Laudon 2006, P26)

ثالثا : المدخل الاجتماعي الفني Sociotechnical :

تزايدت دراسة نظم المعلومات في الأربعينات وكانت تركز على نظم المعلومات المعتمدة على الحاسوب في مؤسسات الأعمال والوكالات الحكومية، وأصبحت نظم المعلومات تجمع بين العمل في علم الحاسوب والعلم الإداري وبحوث العمليات مع الممارسة العملية تجاه تطوير حلول الأنظمة لمشاكل العالم الحقيقي، وإدارة مصادر تكنولوجيا المعلومات وتهتم أيضا بالقضايا السلوكية والنفسية للأفراد المتعاملين مع تلك الأنظمة. (Laudon & Laudon 2006, P27)

وبناء على فهم المداخل المتعددة لنظم المعلومات فإنه لا يوجد مدخل واحد للتعامل مع نظم المعلومات بشكل فعال، حيث أن نجاح وفشل المعلومات نادرا ما يكون كله فني أو كله سلوكي، لذا يجب فهم المجالات والمداخل المتعددة والمتعلقة بنظم المعلومات، ومن وجهة نظر المدخل الاجتماعي الفني فإن أداء المؤسسة الأمثل يمكن إنجازه بالجمع ما بين النظم الاجتماعية (السلوكية) والنظم الفنية المستخدمة في الإنتاج، كما أن تطبيق المدخل الاجتماعي الفني للنظم يساعد في تجنب المدخل التكنولوجي البحت لتكنولوجيا المعلومات . (Laudon & Laudon 2006, P27)

شكل رقم (٤)



المداخل المعاصرة لدراسة نظم المعلومات IS Approaches :

المصدر (Laudon & Laudon, 2006, P26)

ومن خلال ما سبق نجد أن نظم المعلومات المحاسبية تجمع ما بين المدخلين وهما المدخل الفني والمدخل السلوكي، حيث تقوم نظم المعلومات المحاسبية على أساس الفهم للنظريات والمبادئ والأسس التي بنيت عليها نظرية المحاسبة وتطبيق تلك الأسس فنيا من خلال الحاسوب .

كما أن نظم المعلومات المحاسبية لم تتجاهل الناحية الإدارية والسلوكية لإدارة النظم والتي تفيدها في تطوير وإدارة النظم، ولذلك فإن نظم المعلومات المحاسبية تعتبر ضمن المدخل الاجتماعي الفني، والذي من خلاله يتم التركيز على إدارة تكنولوجيا المعلومات والعمل على دعم تلك الإدارة من أجل المحافظة على أمن وسرية المعلومات، إضافة للإهتمام بالعنصر البشري وتطويره والعمل على توعيته وامداده بالخبرة اللازمة التي تفيده في التعامل مع النظام وعدم الوقوع في أخطاء قد تؤدي إلى حدوث مخاطر تؤثر على أمن نظم المعلومات المحاسبية لدى الشركة .

ويعتبر العنصر البشري من ضمن الأسباب التي تؤدي إلى حدوث مخاطر أمن نظم المعلومات المحاسبية

الأنواع الرئيسية الأربعة لنظم المعلومات

لقد صنف **(Laudon & Laudon, 2006)** نظم المعلومات حسب المستويات الثلاثة للمؤسسة(المستوى التشغيلي والمستوى الإداري والمستوى الاستراتيجي) إلى أربع أنواع أساسية حيث أن نظم المعلومات تخدم المد راء والعاملين في كل هذه المستويات، في وظائف البيع والتسويق والتصنيع والإنتاج، والمحاسبة والتمويل، وإدارة الأفراد .

١. نظم معالجة الحركات

تعتبر نظم معالجة الحركات من أنظمة الأعمال الأساسية، والتي تخدم المستوى التشغيلي لدى المؤسسة، وهو نظام محوسب يقوم بتأدية وتسجيل الحركات اليومية الروتينية، والتي تعتبر ضرورية لأعمال المؤسسة . (Laudon & Laudon 2006, P43)

ويعتبر نظام معالجة الحركات مركزيا لأعمال المؤسسة، وقد يؤدي أي عطل في هذا النوع من الأنظمة ولو لعدة ساعات لانقراض الشركة، ولربما للشركات الأخرى المتعاونة مع هذه الشركة، كما أن المدراء يحتاجون لنظام معالجة الحركات من أجل مراقبة العمليات الداخلية وعلاقات الشركة مع البيئة الخارجية، ويعتبر نظام معالجة الحركات مزودا ومنتجا لأنظمة أخرى فمثلا نظام الرواتب يقوم بتزويد بيانات لنظام حسابات الشركة العام، والذي يعتبر مسئولا عن متابعة مدخلات وتكاليف الشركة، ويقوم بإنتاج التقارير الضرورية كتقارير الميزانية.

(Laudon & Laudon 2006, P44)

٢. *نظم المعلومات الإدارية*

تعرف نظم المعلومات الإدارية بأنها عبارة عن دراسة نظم المعلومات في مجال الأعمال والإدارة، ويعتبر مصطلح نظم المعلومات الإدارية تصنيف محدد لنظم المعلومات والتي تخدم وظائف المستوى الإداري لدى المؤسسة، وتزود المد راء بالتقارير، وفي بعض الحالات بمعالجة

آنية عن طريق الإنترنت لمعالجة سجلات الأداء والسجلات التاريخية ومن ناحية عملية يوجهون عملهم نحو الأحداث الداخلية وليس الخارجية للمؤسسة، حيث تخدم نظم المعلومات الإدارية وظائف التخطيط، والتحكم وصناعة القرار على المستوى الإداري، وبشكل عام تعتمد على البيانات المستخرجة من نظم معالجة الحركات، وتقوم نظم المعلومات الإدارية بتلخيص وإنتاج تقارير عن حركات المؤسسة الأساسية وبيانات الحركات الأساسية المستخرجة من نظم معالجة الحركات، حيث يتم ضغطها وعرضها على شكل تقارير مطولة، وإنتاجها على شكل جداول منتظمة . (Laudon & Laudon 2006, P44)

كما أن نظم المعلومات الإدارية تخدم الإداريين بما يهمهم من نتائج أسبوعية وشهرية وسنوية، وليس عن النشاطات اليومية .

٣. ***نظم دعم القرار***

نظم دعم القرار تخدم أيضا المستوى الإداري للمؤسسة وتساعد المدراء في صناعة القرارات الفريدة والسريعة التغير مقدما بشكل مبسط، كما تقوم بتحديد المشاكل في حال أن إجراءات إيجاد الحلول ليست معرفة بشكل كامل، وعلى الرغم من أن نظم دعم القرار تستخدم المعلومات الداخلية من نظم معالجة الحركات ونظم المعلومات الإدارية فهي دائما تجلب معلومات من مصادر خارجية، مثل أسعار الأسهم الحالية أو أسعار منتجات المنافسين . (Laudon & Laudon 2006, P45)

ومن ناحية التصميم فإن نظم دعم القرار تملك قدرة تحليلية أكبر من أنواع النظم الأخرى، حيث يتم بنائها من نماذج متعددة لتحليل البيانات، وتقوم بتكثيف كميات كبيرة من البيانات بطريقة تمكن صناع القرارات من تحليلها، بحيث يقوم المستخدمون باستخدامها مباشرة، في تكوين

برامج صديقة للمستخدم، كما أن نظم دعم القرار متفاعلة مع المستخدم حيث يقوم بتغيير الافتراضات وعمل أسئلة جديدة وتضمين بيانات جديدة. (Laudon & Laudon 2006, P46)

٤. نظم دعم الإدارة التنفيذية

تخدم نظم دعم الإدارة التنفيذية المستوى الإستراتيجي للمؤسسة، حيث أن المدراء القدامى يستخدمون نظم دعم الإدارة التنفيذية لصناعة القرارات، كما تعالج القرارات الغير روتينية والتي تحتاج تقييم بشري وبصيرة لأنه لا يوجد موافقة على إجراء محدد للوصول لأحد الحلول، كما أن نظم دعم الإدارة التنفيذية تنشئ بيئة محوسبة واتصالات عامة، بدلا من إنتاج تطبيق ثابت أو قدرات محددة، ويتم تصميم نظم دعم الإدارة التنفيذية لتجمع بيانات عن الأحداث الخارجية، مثل قوانين ضريبية جديدة أو منافسين، ولكنها أيضا ترسم ملخصات عن معلومات داخلية من نظم معالجة الحركات ونظم دعم القرارات، وتقوم نظم دعم الإدارة التنفيذية بترشيح وضغط وتتبع بيانات حرجة، مع التركيز على اختصار الوقت والجهد المطلوبين للحصول على معلومات مفيدة للمدراء التنفيذيين، كما تقوم نظم دعم الإدارة التنفيذية بتوظيف برامج الرسومات وعرض رسومات وبيانات من عدة مصادر مباشرة لمكتب المدير التنفيذي، وعلى العكس من أنواع نظم المعلومات الأخرى، فإن نظم دعم الإدارة التنفيذية ليست مصممة أساسا لحل مشاكل محددة بل مزودة بطاقة محوسبة واتصالات عامة يمكن تطبيقها على مصفوفة متغيرة من المشكلات . (Laudon & Laudon 2006, P47)

ومن خلال ما سبق فإن نظام معالجة الحركات يعتبر بمثابة نظام لتشغيل ومعالجة البيانات والذي يعد من المراحل الأساسية للنظام وهي مرحلة معالجة البيانات "التشغيل" وتعتبر هذه المرحلة مهمة جدا وقد تتعرض للعديد من المخاطر التي تهدد أمن نظم المعلومات المحاسبية، ومثال ذلك ادخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام .

ويعد كلا من نظام المعلومات الإداري ونظام المعلومات المحاسبي نظامين متداخلين وبينهما عناصر مشتركة، كما أن نظام المعلومات الإداري يمد الإدارة بالتقارير اللازمة والتي تساعدها في اتخاذ القرارات المناسبة، وقد تكون تلك القرارات إدارية تساعد الإدارة في وضع قواعد وقرارات خاصة لحماية أمن نظم المعلومات المحاسبية ومنع حدوث المخاطر التي تواجه أمن نظم المعلومات المحاسبية .

وأما نظم دعم القرار فهي من النظم التي تساعد المدراء في صناعة القرارات الرشيدة من خلال المعلومات والتقارير التي يتم الحصول عليها من نظم معالجة الحركات ونظم المعلومات الإدارية.

كما أن نظم دعم الإدارة التنفيذية والتي تخدم المستوى الاستراتيجي في صناعة القرارات المناسبة تقوم باصدار قرارات ووضع قواعد ورسم سياسات تحكم عمل نظام المعلومات المحاسبي للمنشأة وتحد من وقوع المخاطر التي تهدد أمن نظام المعلومات المحاسبي، إضافة إلى وضع الإجراءات اللازمة لحماية أمن نظم المعلومات المحاسبية لدى المنشأة .

نظم المعلومات المحاسبية

يعتبر النظام المحاسبي من أقدم نظم المعلومات الذي يعد كمصدر رئيسي يساعد الإدارة في الحصول على المعلومات الاقتصادية التي تساعدها في اتخاذ القرارات المناسبة .

كما أن النظام المحاسبي يتكون من مجموعة من المستندات والـدفاتر والـسجلات التـي تمثـل مدخلات النظام والذي يهتم نظام المعلومات المحاسبي بتحليل كيفية تسجيل وتلخـيص وتقريـر العمليات الواردة بها من أجل الحصول على معلومات تمثل مخرجات النظام والتي تـساعد فـي تحقيق الأهداف المحددة للنظام .

وقد عرف النظام المحاسبي من قبل Kohler بأنه :

"يقوم بتسجيل العمليات المالية وإعداد تقرير عنها"(Kohler, E, 1975, P8.)[5]

وأما جمعة وآخرون (٢٠٠٣، ص١٥) فقد عرفوا النظام المحاسبي بأنه :

"أحد أهم نظم المعلومات في الوقت الحاضر بل يعتبر من أقدم نظم المعلومات التي عرفها الإنسان، حيث يهتم بتسجيل العمليات المالية وإعداد تقرير عنها وتقديمها إلى مختلف الجهات الداخلية والخارجية".

ومن خلال ما سبق نلاحظ أن التعريفات السابقة ركزت على أهداف النظام المحاسبي دون التطرق إلى مكونات النظام المحاسبي .

[5]- نقلا عن الراوي (١٩٩٩، ص٢٤)

وقد عرف الرزق (١٩٩٠ ،ص١٩) النظام المحاسبي بشكل أشمل بأنه :

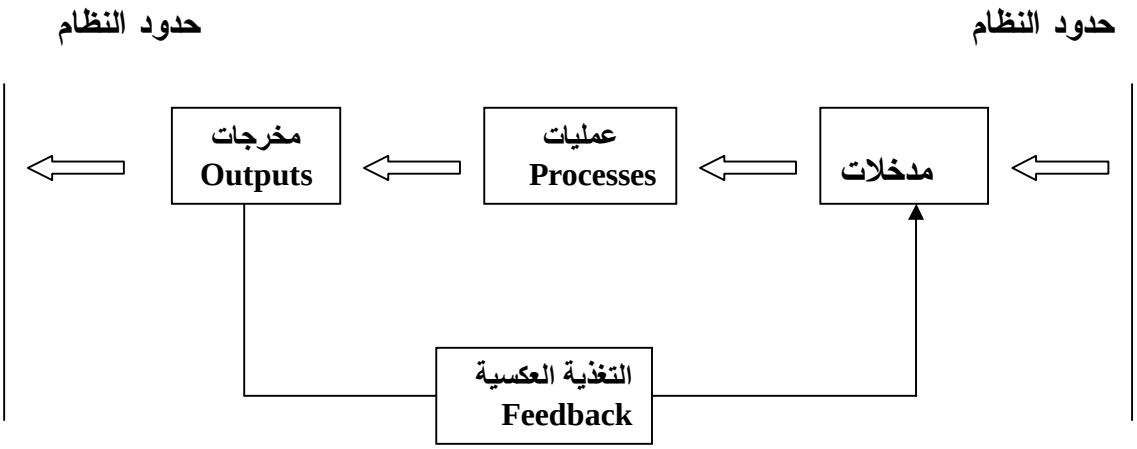
"مجموعة من الأوراق الثبوتية والمستندات والدفاتر المحاسبية والسجلات والإجراءات والوسائل المستخدمة في تسجيل وتلخيص العمليات المالية وتقرير البيانات المالية وعرضها في شكل التقارير المعبرة عن البيانات المطلوبة من قبل الإدارة لتحقيق الرقابة على أنشطة المشروع ولتقديمها إلى الجهات الخارجية المهتمة بأعمال المشروع"

كما ويعرف النظام المحاسبي بأنه:

"أحد مكونات نظام المعلومات الإداري والذي يهتم بجمع وتصنيف ومعالجة العمليات المالية وتحويلها إلى معلومات وتوصيلها إلى الأطراف المختلفة ذات العلاقة من أجل ترشيد قراراتها" (العيسى ،٢٠٠٣ ،ص٢٠) .

ويوضح عيسى مكونات النظام والمراحل التي يمر بها من خلال الشكل رقم (٥)

شكل رقم (٥)



شكل يوضح النظام المحاسبي

المصدر : العيسى (٢٠٠٣، ص٢٠)

ومن خلال ما سبق يمكن تعريف النظام المحاسبي بأنه عبارة عن مجموعة من العناصر والاجراءات والوسائل التي تقوم بعمليات تسجيل وتلخيص وتقرير العمليات المالية بهدف مساعدة الجهات المستفيدة بأداء وظائفها وفي اتخاذ القرارات المناسبة وفي الوقت المناسب .

وقد تتعرض مكونات النظام المحاسبي للعديد من المخاطر التي تهدد أمن نظم معلوماتها المحاسبية والتي سيتم التركيز عليه من خلال هذه الدراسة .

دور المحاسبة كنظام للمعلومات :

تؤدي المحاسبة دورها كنظام للمعلومات في عملية مستمرة ومتكاملة يمكن أن تتحدد معالمها في ثلاث خطوات متتالية هي : (Robinson & Davis,1985,p7)[٦]

١. حصر العمليات المالية المتعلقة بنشاط المنشأة وتمثيلها في صورة بيانات أساسية (خام) تسجل في الدفاتر .
٢. تشغيل أو معالجة البيانات الأساسية وفق مجموعة من الفروض والمبادئ المحاسبية المتعارف عليها لتتحول هذه البيانات بعد تشغيلها في النظام المحاسبي إلى معلومات مالية تخدم أغراض مستخدمي هذه المعلومات .
٣. إيصال المعلومات التي يتم معالجتها إلى الأطراف ذات المصلحة وذلك بواسطة مجموعة من التقارير المالية .

وتعتبر الخطوات السابقة ممثلة للمكونات الأساسية للنظام من حيث ادخال البيانات وتشغيلها ومعالجتها ومن ثم الحصول على المخرجات والممثلة في التقارير المالية .

تعريف نظم المعلومات المحاسبية:

تعتبر دراسة نظم المعلومات الحديثة أمرا هاما وضروريا في العصر الحالي وهو عصر التقنية والكمبيوتر، ولقد كان الاعتماد في السابق في تشغيل النظام المحاسبي على المعالجة اليدوية للبيانات وذلك لعدم توافر التقنيات الحديثة ولكن مع التطور السريع في عالم الكمبيوتر أصبح هناك توجه نحو تشغيل نظام المعلومات المحاسبي من خلال الكمبيوتر .

وتعرف نظم المعلومات المحاسبية بأنها:

"أحد أنظمة المعلومات المحوسبة في منشآت الأعمال، يهدف هذا النظام إلى تخزين المعلومات المحاسبية التي يتم التوصل لها بعد معالجة البيانات المحاسبية التي يتم الحصول عليها من البيئة الداخلية والخارجية" (حفناوي، ٢٠٠١، ص٦٦)

---

[6]-نقلا عن مطر (١٩٩٥،ص٣٥)

كماعرف نظام المعلومات المحاسبية من قبل ماسكوف وآخرون (p299،١٩٩٧):

"بأنه أحد عناصر المنظمة وذلك بجمع وتصنيف ومعالجة وتحليل واتصال مالي موجه، واتخاذ القرارات والمعلومات للجهات الخارجية بالشركة (مثل المستثمرون، الدائنون، وكالات الضريبة) وللجهات الداخلية (للإدارة بشكل أولي)"[٧].

وأوضح دبيان (١٩٩٧ ،ص٢) النقاط التي تهتم نظم المعلومات المحاسبية بدراستها حيث قال بأن:

"دراسة نظم المعلومات المحاسبية تهتم بتحليل كيفية تسجيل وتلخيص وتقرير الأحداث المتباينة التي يمكن أن يكون لها تأثير على مسلك وحياة المنظمة أيا كان نوعها، فهذه الأحداث يتم تسجيلها باستخدام الأساليب والطرق والمبادئ المحاسبية المتعارف عليها، وأخيرا صياغة النتائج النهائية في صورة تقارير معلومات تقدم للمهتمين بالمنظمة سواء كانوا داخل إطار المنظمة أو خارجها"

ومن خلال ما سبق يتضح لنا أن نظم المعلومات المحاسبية تسعى لتحقيق هدف محدد وهو توفير المعلومات اللازمة (مالية وكمية) من أجل إمداد الأطراف المستفيدة (الداخلية والخارجية) لمساعدتهم في اتخاذ القرارات الاقتصادية الرشيدة .

وتعد مرحلة توصيل المعلومات للأطراف المستفيدة من المراحل الهامة بالنسبة لنظم المعلومات المحاسبية الإلكترونية، فقد تتعرض تلك المرحلة للعديد من المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية، والتي من أهمها تدمير تلك المخرجات أو سرقتها أو عمل نسخ غير مصرح بها من تلك المخرجات أو توصيلها إلى أشخاص لا يحق لهم الحصول عليها، وبالتالي تسرب تلك المعلومات يؤثر على أمن نظم المعلومات المحاسبية الإلكترونية للمنشأة .

---

[7]-نقلا عن الراوي (١٩٩٩ ،ص٢٤)

خصائص نظام المعلومات المحاسبي:

لكل نظام خصائص يجب أن يتمتع بها ويسعى إلى تحقيقها وللنظام المحاسبي العديد من الخصائص التي يجب أن يسعى لتحقيقها لكي يكون هذا النظام ناجحا ومن تلك الخصائص (الدلاهمة، ٢٠٠٦، ص٢) :

١. الوضوح وهي تعني أن يكون النظام واضحا متضمنا على التعليمات التوضيحية التي تساعد على فهم النظام وعدم وجود مصطلحات قد تعيق فهم النظام.
٢. السهولة وهي تعني امكانية تطبيق وتنفيذ عمليات النظام بسهولة ودون أي صعوبات.
٣. الدقة ويقصد بها تطبيق وتنفيذ عمليات النظام بشكل صحيح ودون حدوث أخطاء أثناء عملية التنفيذ.
٤. السرعة ويقصد بها قدرة النظام على تقديم المعلومات للجهات المستفيدة في الوقت المناسب حتى تكون مفيدة ومؤثرة في اتخاذ القرار المناسب وفي الوقت المناسب.
٥. المرونة ويقصد بها قدرة النظام على مواجهة أي تغيير في النظام وإمكانية تعديل الاجراءات بما يتناسب وظروف عمل المنشأة.
٦. الملاءمة ويقصد بها أن يكون النظام ذو تكلفة اقتصادية ملائمة تتناسب مع التكلفة المرجوة من النظام بالاضافة إلى ملاءمة المعلومات التي يمكن الحصول عليها من النظام مع الهدف الذي أعدت من أجله.

أهداف نظم المعلومات المحاسبية (د.بيان، ١٩٩٧، ص٢٨٦، ٢٨٧):

١. إنتاج التقارير اللازمة لخدمة أهداف المشروع سواء مالية أو بيانية وإحصائية أو تقارير التشغيل اليومية والأسبوعية.

٢. توفير تقارير تحتوي على درجة من الدقة في الإعداد والنتائج.

٣. تقديم التقارير في الوقت المناسب لتساعد الإدارة في اتخاذ القرارات الملائمة في الوقت المناسب.

٤. تحقيق النظام المحاسبي لشتروط الرقابة الداخلية اللازمة لحماية أصول المشروع ورفع كفاءة أدائها من خلال توفير وسائل الرقابة الداخلية في النظام.

٥. تناسب تكلفة النظام وتكلفة إنتاج بياناته مع الأهداف المطلوبة منها بما يحقق التوازن بين تكلفة النظام وأهدافه.

وبالتالي فإن تحقيق أهداف نظام المعلومات المحاسبي يؤدي إلى تحقيق الأمن لهذا النظام والمحافظة على سرية المعلومات التي يتم الحصول عليها .

مكونات نظام المعلومات المحاسبي (الدهراوي، محمد،٢٠٠٢،ص١٩-٢٢)

١. وحدة تجميع البيانات

وتختص هذه الوحدة بعملية تجميع البيانات اللازمة من البيئة المحيطة بالمشروع أو عن طريق التغذية العكسية وإمداد الإدارة بها وتتحدد طبيعة البيانات المراد الحصول عليها حسب طبيعة أهداف المشروع نفسه وطبيعة المخرجات المطلوب الوصول إليها.

٢. وحدة تشغيل البيانات

ومن خلال هذه الوحدة يتم تشغيل البيانات الأولية التي يتم الحصول عليها إذا كانت في حاجة للتشغيل والمعالجة لتصبح معلومات مفيدة، أما إذا كانت البيانات التي تم الحصول عليها جاهزة للاستخدام بشكلها الحالي فلا داعي لإجراء عملية التشغيل عليها.

٣. وحدة تخزين واسترجاع البيانات

حيث يتم من خلال هذه الوحدة عملية تخزين للبيانات التي لم تتم استخدامها بعد والمحافظة عليها ليتم استرجاعها والاستفادة منها مستقبلا أو يتم إجراء بعض العمليات على البيانات التي تم تشغيلها قبل إرسالها إلى متخذي القرارات.

٤) وحدة توصيل المعلومات

وتعتبر هذه الوحدة كوسيلة اتصال بين وحدات النظام المحاسبي يتم من خلالها نقل وتوصيل البيانات والمعلومات من وحدة إلى أخرى داخل نظام المعلومات المحاسبي حتى تصل إلى متخذي القرارات من خلال قنوات آلية أو يدوية حسب الغرض والإمكانيات المتاحة للمشروع.

٥) وحدة القرارات الإدارية

وتتمثل وظيفة هذه الوحدة باتخاذ القرار المناسب بناء على المعلومات التي تم الحصول عليها والمفاضلة بين مجموعة البدائل المتاحة إليها ودراستها ومقارنتها بأهداف المشروع ومن ثم اختيار البديل الأفضل والذي يحقق أفضل نتائج ممكنة للمشروع في ضوء المحددات والقيود المفروضة.

الوظائف الأساسية لنظام المعلومات المحاسبية: - (سلام وآخرون، ٢٠٠٠،ص٤٩)

١. جمع البيانات وتسجيلها وترميزها وتصنيفها وفحصها والتأكد من دقتها واكتمالها وتحويل البيانات من وسيلة تخزين إلى وسيلة أخرى.

٢. تشغيل البيانات من خلال عملية فرزها وإجراء العمليات الحسابية والمنطقية عليها ثم تلخيص النتائج وجمعها.

٣. إدارة البيانات من خلال تخزينها وتحديثها وصيانتها واسترجاعها وقت الحاجة إليها.

٤. رقابة وحماية البيانات حتى لا يتم التلاعب بها أو اختراقها وتغييرها أو حذفها.

٥. إنتاج وتوصيل المعلومات وإعداد التقارير اللازمة وذلك من خلال عمليات تجميع واسترجاع ونقل المعلومات وتقريرها.

العوامل التي تؤثر على نظم المعلومات المحاسبية

تسعى الإدارة دائما للحصول على المعلومات اللازمة والتي تفيدها في اتخاذ القرارات المناسبة ولذلك ومع التطور التقني الذي تواجهه المؤسسات لا بد للمحاسب من الإلمام بكافة العوامل التي قد تؤثر على المعلومات التي يقدمها للإدارة، وبالتالي تؤثر على نظام المعلومات المحاسبي وهي:-

١) التحليل السلوكي (Behavioral Analysis)

والمقصود بالتحليل السلوكي هو التعرف على العوامل السلوكية والنفسية التي يواجهها الأفراد أثناء قيامهم بأداء واجباتهم المهنية لدى الشركة وذلك لأن الوضع النفسي لدى الموظفين قد يؤثر على أدائهم لواجباتهم وقدرتهم على تحقيق أهداف المؤسسة التي يعملون بها، ولكن ليس هذا معناه أن يكون المحاسب أو المدير محللا نفسيا ولكن يكفي أن يكون ملما بأوضاع الموظفين

وذو قدرة على التأثير عليهم وتشجيعهم على أداء واجباتهم المهنية وتحقيق أهداف المؤسسة. (موسكوف وسيمكن، ١٩٨٩، ص٥٢)

وتعتبر العوامل النفسية والسلوكية لدى الموظفين من العوامل المؤثرة على آدائهم لعملهم، وبالتالي تعد تلك العوامل من ضمن الأسباب التي قد تؤدي إلى حدوث مخاطر نظم المعلومات المحاسبية، حيث يقع إدارة الشركة دراسة تلك المشاكل ومعالجتها حتى لا يؤثر ذلك على أداء الموظفين لعملهم .

كما أنه يجب الأخذ بعين الاعتبار أنه عند القيام بإجراء أي تعديل في عمل النظام المحاسبي لا بد من التأكد من أن تلك التعديلات يمكن تحقيقها من قبل الموظفين ولن تكون متعارضة مع قدرات الموظفين، ويتم ذلك من خلال مشاركة الموظفين في عمليات تطوير وتعديل النظام والمشاركة في تقديم مقترحاتهم فيما يتعلق باختصاصاتهم ومسئوليات عملهم وهذا يؤدي إلى تشجيعهم على تنفيذ خطوات التعديل والتطوير التي قاموا بإعدادها بسهولة ونشاط من أجل إثبات قدراتهم، وتحقيق الأهداف التي يسعون إلى تحقيقها.

٢) الأساليب الكمية (Quantitative methods)

والمقصود بذلك مجموعة الطرق التحليلية التي يمكن أن تستخدمها الإدارة في اتخاذ القرارات المناسبة في عمليات دعم نظام المعلومات المحاسبي ورفع كفاءة المعلومات التي تزودها الإدارة. فقد تسعى الإدارة إلى القيام بمشاريع جديدة أو تطوير المشاريع التي تقوم على إدارتها ولذلك يجب أن يتوفر لها كافة المعلومات اللازمة لمساعدتها في اتخاذ القرار المناسب وهذا يجعلها

تلجأ إلى استخدام العديد من الطرق التحليلية ومنها التحليل الإحصائي والبرمجة الخطية والمحاكاة ونظرية خطوط الانتظار وغيرها . (موسكوف وسيمكن، ١٩٨٩، ص٥٣)

وتعد الخبرة الكافية للموظفين من العوامل التي تساعد الموظفين بدقة وسرعة وكفاءة عالية، وبالتالي التمكن من التغلب على العوامل التي تؤثر على أمن نظم المعلومات المحاسبية الالكترونية .

٣) الكمبيوتر (Computers)

لقد كانت المؤسسات في السابق تقوم بأداء عملها بطريقة يدوية مما يستهلك الوقت والجهد الكبير ولكن مع التطور التكنولوجي الهائل ومواكبة تلك المؤسسات لهذا التطور انتقلت المؤسسات من الأداء اليدوي إلى الأداء التكنولوجي وأصبح الاعتماد بشكل كبير على الكمبيوتر في أداء العديد من مهام المؤسسة وهذا أدى إلى توفير الوقت اللازم لأداء المهمات والواجبات التي تقع على عاتق الموظفين، وقد ساهم هذا التطور في قدرة المؤسسة على الاحتفاظ بسجلاتها المحاسبية من خلال الكمبيوتر، ولذلك لا بد للمحاسب أن يكون ملما بطاقة وإمكانيات الكمبيوتر في معالجة البيانات التي يتم إدخالها بكفاءة وفعالية معقولة . (موسكوف وسيمكن، ١٩٨٩، ص٥٣-٥٤)

ومع التطور التكنولوجي الهائل أصبح الكمبيوتر هو الأساس في شتى المجالات، ولذلك اعتمدت معظم المؤسسات على على الحاسوب في إنجاز العمليات الخاصة بها وهذا يتطلب من الإدارة العمل على احكام الرقابة على الحاسوب وعلى العمليات التي يقوم الأفراد بتأديتها الكترونيا والتي تكون عرضة للمخاطر أكثر من غيرها من العمليات التي يتم معالجتها يدويا .

علاقة نظم المعلومات المحاسبية بالحاسوب

يعتبر استخدام الحاسوب في المحاسبة ذا أثر كبير على شكل وطبيعة ومقومات نظام المعلومات المحاسبي حيث تم الانتقال من الشكل التقليدي اليدوي للنظام إلى الشكل الآلي للنظام، فقد كان الاعتماد في السابق على التسجيل اليدوي في دفاتر اليومية والأستاذ وإعداد تقارير بشكل يدوي ولكن مع تطور الحاسوب تم الانتقال من التسجيل اليدوي إلى التسجيل الآلي وأصبحت البيانات تسجل وتخزن في الكمبيوتر بدلا من تسجيلها في دفاتر وسجلات يدوية مع سرعة الحصول عليها في حالة طلبها.

وتعتبر نظم المعلومات المحاسبية والحاسوب نظامين مكملين لبعضهما البعض حيث أن تطبيق نظم المعلومات المحاسبية يتم من خلال الحاسوب ولذلك فإن هناك علاقة قوية تربط بين هذين النظامين وتتمثل تلك العلاقة في النقاط التالية: (الراوي، ١٩٩٩،ص٨٠)

١. تعتمد فكرة الحاسوب على فكرة نظم المعلومات والتي لا تخرج عن فلسفة النظام.
٢. يتكون النظام من ثلاث أجزاء رئيسية (مدخلات، تشغيل، مخرجات) وهي نفسها الأجزاء المكونة لجهاز الحاسوب.
٣. تعتبر فلسفة النظام المحاسبي أقدم وأشمل من فكرة الحاسوب.
٤. يعتبر الحاسوب أداة تنفيذية وتخطيطية للنظام المحاسبي يقوم بتطبيق فكر نظم المعلومات.

٥. يعتمد تقدم تكنولوجيا الحاسوب على فلسفة النظام والسلوك البشري المساعد في عملية التطور.

٦. الترابط بين النظام المحاسبي والحاسوب أدى إلى التكامل بين فكرة النظام وفكرة الحاسوب.

٧. الحاجة البشرية إلى المعرفة الدقيقة والسريعة والمكونة والمتخصصة والبحث عن الجزئيات.

تأثير استخدام الحاسوب على مقومات نظام المعلومات المحاسبي :

لكل نظام محاسبي مقومات أساسية يعتمد عليها من أجل تحقيق أهدافه المحددة ونستطيع تحديد تلك المقومات من خلال التعريفات السابقة للنظام المحاسبي وتتمثل مقومات نظام المعلومات المحاسبي في:

١. الأوراق الثبوتية والمستندات

٢. الدفاتر والسجلات المحاسبية

٣. دليل الحسابات

٤. التقارير والقوائم المالية

وفيما يلي تأثير استخدام الحاسوب على مقومات نظام المعلومات المحاسبي : (العيسى ،٢٠٠٣،ص٢١٠-٢١٣) :

١. يعتبر استخدام الأوراق الثبوتية والمستندات في النظام اليدوي هي نفسها في النظام الآلي ولكن الفرق بينهما يكمن في اختلاف شكل الأوراق الثبوتية والمستندات في النظام الآلي عن

النظام اليدوي بما يتلاءم مع طبيعة الحاسوب وقدرة الحاسوب على التعامل معها، فالمستندات تمثل وسائط تدخل البيانات من خلالها إلى الحاسوب، وتتمثل تلك الوسائط بالاسطوانات أو الأقراص الممغنطة أو الطرفيات .

وتعد الإسطوانات والأقراص الممغنطة والطرفيات من الوسائل التي يتم من خلالها نقل فيروس الكمبيوتر إلى النظام وبالتالي التأثير على تشغيل بيانات النظام، ويعد فيروس الكمبيوتر من المخاطر التي تتعرض لها نظم المعلومات المحاسبية .

٢. كما أن الدفاتر والسجلات المحاسبية تختلف من النظام اليدوي عن النظام الآلي من حيث الشكل، حيث اعتمد النظام الآلي على أقراص واسطوانات ممغنطة لا تمكن القارئ من معرفة جميع البيانات المسجلة بها بصورة مباشرة .

وبالتالي فإن اشتراك الموظفين في استخدام نفس كلمة السر قد تؤدي إلى كشف تلك البيانات لأشخاص لا يحق لهم الحصول عليها،

٣. يعتبر دليل الحسابات أحد المقومات الأساسية لنظام المعلومات المحاسبي سواء كان النظام يدويا أم آليا ولا يمكن الاستغناء عنه، حيث لا يوجد اختلاف بين النظام الآلي والنظام اليدوي في دليل الحسابات، ولكن إعداد دليل الحسابات في نظام المعلومات المحاسبي المعتمد على الحاسوب يعتبر أسرع وأدق من إعداده في نظام المعلومات المحاسبي اليدوي، كما أن الحاسوب لا يستطيع أن يقوم بتوجيه بيان معين إلى حساب معين إلا إذا كان هناك رموز وأرقام بأسماء الحسابات الإجمالية والفرعية معد مسبقا داخل الحاسوب .

وهذا يحتاج إلى حماية تلك البيانات حتى لا يتم اختراقها من قبل أشخاص لا يحق لهم الوصول إليها ومن ثم تخربها وإفسادها بما يخدم مصلحتهم .

٤. وبالنسبة للتقارير والقوائم المالية فلا توجد اختلافات بين مقومات نظام المعلومات المحاسبي اليدوي ونظام المعلومات المحاسبي الآلي ولكن الاختلاف يكمن في سرعة إعداد تلك التقارير وسرعة عرضها ومراجعتها وتدقيقها وتصحيح الأخطاء إن وجدت بسرعة وكفاءة عالية.

وتعتبر التقارير التي يتم الحصول عليها من خلال النظام الآلي أكثر عرضة للمخاطر من التقارير التي يتم الحصول عليها من خلال النظام اليدوي .

الفصل الثالث

مخاطر نظم المعلومات المحاسبية الإلكترونية

الفصل الثالث

مخاطر نظم المعلومات المحاسبية الإلكترونية

تعتبر نظم المعلومات المحاسبية الإلكترونية من النظم التي تواجه العديد من المخاطر التي قد تؤثر على تحقيق أهداف تلك النظم وذلك نظرا لاعتمادها على الحاسوب، حيث تزامن التطور الكبير للحاسبات وأنظمة المعلومات مع التطور في تكنولوجيا المعلومات وسرعة انتشار هذه المعلومات واستخدامها إلكترونيا، ولقد صاحب هذا التطور في استخدام المعلومات الإلكترونية العديد من المخاطر والمشاكل التي تؤثر على أمن المعلومات سواء كانت تلك المخاطر مقصودة أو غير مقصودة .

ولذلك تزايد الاهتمام الكبير بتوفير الوسائل والأساليب اللازمة لحماية نظم المعلومات والرقابة على عملياتها وضمان استمرارية عمل تلك النظم بشكل صحيح وبالطريقة المطلوبة التي صممت من أجلها .

أمن المعلومات

يعرف أمن المعلومات من زاوية أكاديمية "أنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها"، أما من زاوية تقنية فيعرف أمن المعلومات أنه عبارة عن "الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية"، ومن زاوية قانونية يعرف أمن المعلومات بأنه "محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة" .

www.arablaw.org/information ; p1

ويعتبر التعريف السابق شامل لأمن المعلومات من شتى النواحي العلمية والعملية والقانونية .

أما (ميلاد، ٢٠٠٦،ص١) فيعرف أمن المعلومات من الناحية الأكاديمية بأنه:

"البحث في السياسات والاستراتيجيات التي ينبغي توخيها لحماية المعلومات من مختلف الاعتداءات التي قد تتعرض لها والمخاطر التي يمكن أن تهددها" .
أما من الناحية التقنية فقد عرف أمن المعلومات بأنه: "مجموعة الوسائل والتدابير والإجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر المتأتية سواء من داخل بيئة المعلومات محل الحماية أو من خارجها" .

ومن الملاحظ بأن تعريف ميلاد يتفق مع التعريف السابق في الناحية العلمية (الأكاديمية) باعتباره علم يبحث في سياسات واستراتيجيات أمن المعلومات ومن الناحية العملية (الفنية) باعتباره الجانب التطبيقي لإجراءات وسياسة حماية أمن المعلومات .

كما يعرف أمن المعلومات بأنه "السياسات والإجراءات والمقاييس الفنية والتي تستخدم لتحول دون الوصول غير المتعمد أو السرقة أو التدمير للسجلات" . (سلطان، ٢٠٠٠، ص٣٩٦)

أمن المعلومات "هو عبارة عن السياسات والممارسات والتقنية التي يجب أن تكون داخل المؤسسة لتداول حركات الأعمال إلكترونيا عبر الشبكات بدرجة معقولة ومؤكدة من الأمان، هذا الأمان ينطبق على كل النشاطات والحركات والتخزين الإلكتروني وعلى شركات الأعمال والزبائن والمنظمين والمؤمّنين وأي شخص آخر ممكن أن يكون معرضا لمخاطر الاختراق" . (Linda, Robinson, 2004, p1)

ونلاحظ أن تعريف سلطان و Linda, Robinson يركز على أمن المعلومات من الناحية التقنية والتي تركز على توفير السياسات والإجراءات اللازمة لحماية المعلومات .

وأما جمعة وآخرون فقد عرفوا أمن المعلومات بأنه: "حماية كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين

فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة ويتم ذلك عن طريق اتباع إجراءات ووسائل حماية عديدة تتضمن سلامة وأمن المعلومات" . (٢٠٠٣،ص٣٤٢)

ومن الواضح أن جمعة وآخرون قد ركزوا في هذا التعريف على الناحية القانونية (التشريعية) لأمن المعلومات من حيث التركيز على حماية أمن المعلومات وتوضيح الإجراءات والوسائل الواجب اتباعها لضمان سلامة وأمن المعلومات .

ونستطيع أن نعرف أمن المعلومات بأنه عبارة عن :

العلم الذي يهتم بدراسة النظريات والاستراتيجيات والقوانين التي تهتم بتوفير الحماية لأمن المعلومات من المخاطر التي قد تواجهها والعمل على تطبيق الوسائل والأساليب والإجراءات اللازمة لتوفير تلك الحماية ومواجهة المخاطر والتغلب عليها، وسن القوانين الصارمة لمنع حدوث تلك المخاطر مستقبلا ومعاقبة مرتكبيها .

ويعد تطبيق أمن المعلومات من شتى النواحي العلمية والعملية والقانونية ذا أثر كبير على زيادة الثقة بنظام المعلومات المحاسبي .

استراتيجية أمن المعلومات :

تعرف استراتيجية أمن المعلومات أو سياسة أمن المعلومات بأنها :-

"مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها".

www.arablaw.org/information ; p٢٤

ويعرفها (ميلاد، ٢٠٠٦،ص١) بأنها:

"مجموعة القواعد التي تتعلق بالوصول إلى المعلومات والتصرف فيها ونقلها داخل هيكل يعتمد المعلومة عنصرا أساسيا في تحسين أدائه وبلوغ أهدافه" .

ومن خلال ما سبق نصل إلى أن استراتيجية أمن المعلومات عبارة عن القواعد التي تحدد كيفية الوصول إلى المعلومات والتعامل معها .

وتعد استراتيجية أمن المعلومات مهمة جدا للحفاظ على أمن نظم المعلومات المحاسبية بحيث تمنع الأشخاص الذين لا يحق لهم الوصول إلى المعلومات أن يصلوا إلى تلك المعلومات أو التعامل معها أو التعرف عليها .

أهداف استراتيجية أمن المعلومات :

ولكي تعتبر استراتيجية أمن المعلومات ناجحة وفعالة وقابلة للتطبيق فلا بد أن يشارك في اعدادها وتنفيذها جميع المستويات الوظيفية التي لها علاقة بتلك الاستراتيجية حيث تسعى تلك المستويات إلى انجاح تلك الاستراتيجة من خلال تحقيق أهداف استراتيجية أمن المعلومات والتي تتمثل في : p24 ; www.arablaw.org/information

١. تعريف مستخدمي نظم المعلومات ومختلف الاداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الحاسوب والشبكات والمعلومات بكافة أشكالها وفي مختلف مراحل جمعها وادخالها ومعالجتها ونقلها عبر الشبكات واعادة استرجاعها عند الحاجة .

٢. تحديد وضبط الآليات التي يتم من خلالها تحقيق وتنفيذ الواجبات المحددة لكل من له علاقة بنظم المعلومات ونظمها وتحديد المسؤوليات عند حصول الخطر .

٣. بيان الإجراءات المتبعة لتفادي التهديدات والمخاطر وكيفية التعامل معها عند حصولها والجهات المكلفة بالقيام بذلك .

عناصر أمن المعلومات

من أجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنف (ميلاد، ٢٠٠٦) تلك العناصر إلى خمسة عناصر وهي:

١) السرية أو الموثوقية: (Confidentiality)

وهي تعني التأكد من أن المعلومات لا يمكن الاطلاع عليها أو كشفها من قبل أشخاص غير مصرح لهم بذلك ولتجسيد هذا الأمر يجب على المؤسسة استخدام طرق الحماية المناسبة من خلال استخدام وسائل عديدة مثل عمليات تشفير الرسائل أو منع التعرف على حجم تلك المعلومات أو مسار إرسالها .

٢) التعرف أو التحقق من هوية الشخصية: (Authentication)

وهذا يعني التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم الصحيح لتلك المعلومات أم لا، ويتم ذلك من خلال استخدام كلمات السر

الخاصة بكل مستخدم، وتوضح مؤسسة (RSA) لأمن المعلومات (RSA Security Inc, www.rsasecurity.com) ثلاث طرق للتحقق من الشخصية وهي:

الأولى: عن طريق شيء يعرفه الشخص مثل كلمة المرور، والثانية عن طريق شيء يملكه مثل رسالة الشيفرة (Token) وهي عبارة عن كود يقوم بإدخاله المستخدم للحاسوب للحيازة على صلاحيات التشغيل أو الشهادة الإلكترونية، والثالثة عن طريق شيئ يتصف به الشخص من الصفات الفيزيائية مثل بصمة الإصبع أو المسح الشبكي أو نبرة الصوت، وكل طريقة لها إيجابياتها وسلبياتها، وتنصح مؤسسة (RSA) باستخدام طريقتين مع بعضهما البعض من هذه الطرق الثلاثة .

٣) سلامة المحتوى: (Integrity)

وهي تعني التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل سواء كان التعامل داخليا في المشروع أو خارجيا من قبل أشخاص غير مصرح لهم بذلك ويتم ذلك غالبا بسبب الاختراقات الغير مشروعة مثل الفيروسات حيث لا يمكن لأحد أن يكسر قاعدة بيانات البنك ويقوم بتغيير رصيد حسابه لذلك يقع على عاتق المؤسسة تأمين سلامة المحتوى من خلال اتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات أو الفيروسات .

٤) استمرارية توفر المعلومات أو الخدمة: (Availability)

وهي تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمات لمواقع المعلومات وضمان عدم تعرض مستخدمي تلك

المعلومات إلى منع استخدامها أو الوصول إليها بطرق غير مشروعة يقوم بها أشخاص لإيقاف الخدمة بواسطة كم هائل من الرسائل العبثية عبر الشبكة إلى الأجهزة الخاصة لدى المؤسسة .

٥) عدم الإنكار: (No repudiation)

ويقصد به ضمان عدم إنكار الشخص الذي قام بإجراء معين متصل بالمعلومات لهذا الإجراء، ولذلك لا بد من توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص للشخص الذي قام به في وقت معين، ومثال ذلك للتأكد من وصول بضاعة تم شراؤها عبر شبكة الإنترنت إلى صاحبها، ولإثبات تحويل المبالغ إلكترونيا يتم استخدام عدة رسائل مثل التوقيع الإلكتروني والمصادقة الإلكترونية .

العوامل التي تساعد على اختراق نظام المعلومات المحاسبي: -

تعتبر نظم المعلومات المحاسبية الإلكترونية أقل أماناً من نظم المعلومات اليدوية وذلك نظرا لاعتماد النظم المحاسبية الإلكترونية على حفظ بياناتها في ملفات الكترونية يستطيع عدد كبير من الأشخاص الوصول إليها والاطلاع عليها، ولذلك فإن نظم المعلومات المحاسبية الإلكترونية قد تتعرض للعديد من المخاطر التي قد تهدد أمنها وذلك بسبب مجموعة من العوامل وهي كما يذكرها (سلطان، ٢٠٠٠،ص٣٩٣-٣٩٤):

١. نظم المعلومات الإلكترونية تتضمن كم هائل من البيانات ولذلك فإنه يصعب عمل نسخ ورقية لها .
٢. صعوبة اكتشاف الأخطاء الناتجة عن التغير في نظام المعلومات المحاسبي الإلكتروني وذلك لأنه لا يمكن التعامل أو قراءة سجلاتها إلا بواسطة الحاسب والذي لا يكشف أي تغيير .
٣. صعوبة مراجعة الإجراءات التي تتم من خلال الحاسب وذلك لأنها غير مرئية وغير ظاهرة .
٤. صعوبة تغيير النظم الآلية مقارنة بالنظم اليدوية .
٥. احتمال تعرض النظم الآلية إلى إساءة استخدامها بواسطة الخبراء غير المنتمين للمنظمة في حال استدعائهم لتطوير النظم .
٦. قد تؤدي المخاطر التي تتعرض لها النظم الآلية إلى تدمير كافة سجلات المنظمة وبذلك فهي أشد خطورة على النظم الآلية من النظم اليدوية .

٧. انخفاض المستندات التي يمكن من خلالها مراجعة النظام تؤدي إلـــى انخفـــاض حالة الأمان اليدوية .

٨. احتمال تعرض النظم الآلية إلى حدوث أخطاء أو إساءة اســـتخدام النظـــام فـــي مرحلة تشغيل البيانات وذلك لتعدد عمليات التشغيل في النظام الآلي .

٩. ضعف الرقابة على النظام الآلي بسبب الاتـــصال المباشـــر للمـــستخدم بـــنظم المعلومات .

١٠. التطور التكنولوجي في الاتصال عن بعد سهل عملية الاتصال بنظم المعلومات من أي مكان وبالتالي إمكانية الوصول غير المسموح به أو إساءة استخدام نظـــم المعلومات .

١١. استخدام العديد من التطبيقات في مواقع مختلفة لنفس قاعدة البيانات يؤدي إلـــى إمكانية اختراقها بفيروسات الحاسب وبالتالي امكانية تـــدمير أو تغييـــر قاعـــدة البيانات لنظام المعلومات .

ومن خلال ماسبق نجد أنه ينبغي على إدارة المؤسسة العمل على حماية بياناتها بكافة أشكالها، سواء كانت ورقية أو غير ورقية، كما أن نظام المعلومات المحاسبي الإلكتروني يكون عرضة للمخاطر أكثر من غيره من النظم ولذلك لا بد للإدارة من وضع قيود على المستخدمين تحد من امكانية التلاعب بالبيانات أو العبث بها سواء من أطراف داخل المؤسسة أو خارجها .

المخاطر التي يمكن أن تتعرض لها نظم المعلومات المحاسبية الالكترونية :-

يعتبر موضوع حماية البيانات من الأمور الواجب الاهتمام بها في كافة مراحل إعداد نظم المعلومات المحاسبية حيث أن أمن البيانات والمعلومات أصبح من أهم عناصر الرقابة الواجب تطبيقها على المعلومات من خلال التخطيط المستمر خلال دورة حياة نظم المعلومات المحاسبية المستخدمة .

وتعتبر المخاطر المقصودة أشد خطرا على أداء فعالية النظم وتزداد تلك الخطورة في النظم الإلكترونية .

وتكمن خطورة مشاكل أمن المعلومات في عدة جوانب منها تقليل أداء الأنظمة الحاسوبية، أو تخريبها بالكامل مما يؤدي إلى تعطيل الخدمات الحيوية للمنشأة، أما الجانب الآخر فيشمل سرية وتكامل المعلومات حيث قد يؤدي الاطلاع والتصنت على المعلومات السرية أو تغييرها الى خسائر مادية أو معنوية كبيرة . (www.ksu.edu.sa/security/ahdaf.html)

ويصنف (أبو موسى، ٢٠٠٤، ص٣-ص٩) مخاطر تهديدات أمن نظم المعلومات المحاسبية الإلكترونية من وجهات نظر مختلفة إلى عدة أنواع:-

أولا/ من حيث مصدرها: (The Source of Threats)

أ. مخاطر داخلية (Internal)

ب. مخاطر خارجية (External)

ثانيا/ من حيث المتسبب بها: (The perpetrator)

أ. مخاطر ناتجة عن العنصر البشري (Human Threats)

ب. مخاطر ناتجة عن العنصر الغير بشري (Non-Human)

ثالثا/ من حيث أساس العمدية: (Intention)

أ. مخاطر ناتجة عن تصرفات متعمدة (مقصودة) (Intentional)

ب. مخاطر ناتجة عن تصرفات غير متعمدة (غير مقصودة) (Accidental)

رابعا/ من حيث الآثار الناتجة عنها: (Consequences)

أ. مخاطر ينتج عنها أضرار مادية (Physical Damage)

ب. مخاطر فنية ومنطقية (Technical or Logical)

خامسا/ المخاطر على أساس علاقتها بمراحل النظام

أ. مخاطر المدخلات (Input)

ب. مخاطر التشغيل (Processing)

ت. مخاطر المخرجات (Output)

وفي ما يلي توضيح لتلك المخاطر

أولا/ من حيث مصدرها

أ. مخاطر داخلية (Internal) :

حيث يعتبر موظفي المنشآت هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية وذلك لأن موظفي المنشآت على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق لدى المنشآة، ومعرفة نقاط القوة والضعف ونقاط القصور لهذا النظام ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال

صلاحيات الدخول الممنوحة لهم، ولذلك فإن موظفي الشركة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها . (أبو موسى، ٢٠٠٤، ص٣)

ب. مخاطر خارجية (External):

وتتمثل في أشخاص خارج المنشأة ليس لهم علاقة مباشرة بالمنشأة مثل قراصنة المعلومات والمنافسين الذين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية عن المنشأة أو قد تتمثل في كوارث طبيعية مثل الزلزال والبراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام في المنشاة . (أبو موسى، ٢٠٠٤، ص٤)

ثانيا/ من حيث المتسبب لها :

أ. مخاطر ناتجة عن العنصر البشري:

وتلك الأخطاء قد تحدث من قبل أشخاص بشكل مقصود وبهدف الغش والتلاعب أو بشكل غير مقصود نتيجة الجهل أو السهو أو الخطأ . (أبو موسى، ٢٠٠٤، ص٤)

ب. مخاطر ناتجة عن العنصرغير البشري:

وهي تلك المخاطر التي قد تحدث بسبب كوارث طبيعية ليس للإنسان علاقة بها مثل حدوث الزلازل والبراكين والفيضانات والتي قد تؤدي إلى تلف النظام ككل أو جزء منه . (أبو موسى، ٢٠٠٤، ص٤)

ثالثا/ من حيث العمدية :

أ. مخاطر ناتجة عن تصرفات متعمدة(مقصودة) :

و تتمثل في تصرفات يقوم بها الشخص متعمدا مثل ادخال بيانات خاطئة وهو يعلم ذلك، أو قيامه بتدمير بعض البيانات متعمدا ذلك بهدف الغش والتلاعب والسرقة، وتعتبر هذه المخاطر من المخاطر المؤثرة جدا على النظام . (أبو موسى، ٢٠٠٤، ص٤)

ب. مخاطر ناتجة عن تصرفات غير متعمدة (غير مقصودة) :

وتتمثل في تصرفات يقوم بها الأشخاص نتيجة الجهل وعدم الخبرة الكافية كادخالهم لبيانات بطريقة خاطئة بسبب عدم معرفتهم بطرق ادخالها أو السهو في عملية التسجيل وتعتبر هذه المخاطر أقل ضررا من المخاطر المقصودة وذلك لإمكانية إصلاحها . (أبو موسى، ٢٠٠٤، ص٤)

رابعا/ من حيث الآثار الناتجة عنها :

أ. مخاطر تنتج عنها أضرار مادية:

وهي المخاطر التي تؤدي إلى حدوث أضرار للنظام وأجهزة الكمبيوتر أو تدمير لوسائل تخزين البيانات والتي قد يكون سببها كوارث طبيعية لا علاقة للانسان بها أو قد تكون بسبب البشر بطريقة متعمدة أو عفوية . (أبو موسى، ٢٠٠٤، ص٥)

ب. مخاطر فنية ومنطقية:

وهي المخاطر الناتجة عن أحداث قد تؤثر على البيانات وإمكانية الحصول عليها للأشخاص المخول لهم بذلك عند الحاجة لها أو إفشاء بيانات سرية لأشخاص غير مصرح لهم بمعرفتها

وذلك من خلال تعطيل في ذاكرة الكمبيوتر أو إدخال فيروسات للكمبيوتر قد تفسد البيانات أو جزء منها وتلك المخاطر قد تؤثر على الموقف التنافسي للمنشأة . (أبو موسى، ٢٠٠٤، ص٥)

وقد تحدث المخاطر السابقة من خلال قيام المهاجم بالبحث في مخلفات التقنية الخاصة بالمؤسسة من قمامة وأوراق متروكة بهدف الحصول على أية معلومات قد تساعد على اختراق النظام للحصول على كلمات السر المدونة على الأوراق الملقاة أو الأقراص الصلبة التي يتم استبدالها، أو أي معلومة أخرى تساهم في اختراق النظام والتي تعرف بتقنية القمامة، ونستطيع أن ندرك درجة خطورة تقنية القمامة من خلال معرفة ما حصل مع وزارة العدل الأمريكية .

حيث قامت وزارة العدل الأمريكية ببيع مخلفات أجهزة تقنية بعد أن تقرر اتلافها وكان من ضمن تلك المخلفات جهاز كمبيوتر يحتوي قرصه الصلب على كافة العناوين الخاصة ببرنامج حماية الشهود وخوفا من نشر تلك المعلومات أو استثمارها ضد الوزارة فقد قامت وزارة العدل بنقل كافة الشهود وتغيير مكان اقاماتهم وهوياتهم وهذا تطلب تكلفة مالية ضخمة وذلك بسبب الاخفاق في اتلاف الأقراص بطريقة صحيحة . p11 ; www.arablaw.org/information

خامسا/ المخاطر من حيث علاقتها بمراحل النظام :

أ. مخاطر المدخلات:

وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال.

وتتمثل المخاطر المتعلقة بأمن المدخلات إلى أربعة أقسام أساسية وهي:

١ -خلق بيانات غير سليمة:

ويتم ذلك من خلال خلق بيانات غير حقيقية ولكن بواسطة مستندات صحيحة يتم وضعها داخل مجموعة من العمليات دون أن يتم اكتشافها، ومثال ذلك استخدام أسماء وهمية لموظفين لا يعملون بالشركة وادراج تلك الأسماء ضمن كشوف الرواتب وصرف رواتب شهرية لهم أو ادخال فواتير وهمية باسم أحد الموردين . (أبو موسى، ٢٠٠٤، ص٥)

٢ -تعديل أو تحريف بينات المدخلات:

ويتم ذلك من خلال التلاعب في المدخلات والمستندات الأصلية بعد اعتمادها من قبل المسؤول وقبل ادخالها إلى النظام، وذلك عن طريق تغيير في أرقام مبالغ بعض العمليات لصالح المحرف، أو تغير أسماء بعض العملاء أو معدلات الفائدة . . (أبو موسى، ٢٠٠٤، ص٨)

٣ -حذف بعض المدخلات

ويحدث ذلك من خلال حذف أو استبعاد بعض البيانات قبل ادخالها إلى الحاسب الآلي، وذلك إما بشكل متعمد ومقصود أو بشكل غير متعمد وغير مقصود، ومثال ذلك قيام الموظف المسؤول

عن المرتبات في المنشأة بتدمير مذكرات وتعديلات تفصيلات حساب البنك لحساب آخر خـــاص بالموظف المحرف . (أبو موسى، ٢٠٠٤، ص٨)

٤ - ادخال البيانات أكثر من مرة :

والمقصود بذلك قيام الموظف بتكرار ادخال البيانات إلى الحاسب إما بطريقة مقصودة أو غيـــر مقصودة، ويتم ذلك من خلال إدخال بينات بعض المستندات أكثر من مرة إلى النظام قبل أوامـــر الدفع وذلك إما بعمل نسخ إضافية من المستندات الأصلية وتقديم كل من الـــصورة والأصـــل أو إعادة ادخال البينات مرة أخرى إلى النظام . (أبو موسى، ٢٠٠٤، ص٨)

ب. مخاطر تشغيل البيانات :

ويقصد بها المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقـــوم بتـــشغيل تلك البيانات وتتمثل مخاطر تشغيل البيانات في الاستخدام غير المـــصرح بـــه لنظـــام وبـــرامج التشغيل وتحريف وتعديل البرامج بطريقة غير قانونية أو عمل نسخ غيـــر قانونيـــة أو ســـرقة البيانات الموجودة على الحاسب الآلي، ومثال على ذلك قيام الموظف بإعطاء أوامر للبرنامج بأن لا يسجل أي قيود في السجلات المالية تتعلق بعمليات البيع الخاصة بعميـــل معـــين مـــن أجـــل الاستفادة من مبلغ العملية لصالح المحرف نفسه . (أبو موسى، ٢٠٠٤، ص٩)

ج. مخاطر مخرجات الحاسب :

ويقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عمليـــة تـــشغيل ومعالجة البيانات، وقد تحدث تلك المخاطر من خلال طمس أو تدمير بنود معينة من المخرجات أو خلق مخرجات زائفة وغير صحيحة أو سرقة مخرجات الحاسب أو إساءة استخدامها أو عمل

نسخ غير مصرح بها من المخرجات أو الكشف الغير مسموح به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق أو طبع وتوزيع المعلومات بواسطة أشخاص غير مسموح لهم بذلك، كذلك توجيه تلك المطبوعات والمعلومات خطأ إلى أشخاص ليس لهم الحق في الاطلاع على تلك المعلومات أو تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها مما يؤدي إلى استخدام تلك المعلومات في أمور تسيء إلى المؤسسة وتضر بمصالحها.

مخاطر نظم المعلومات حسب الغرض منها :

تتعرض نظم المعلومات الحاسوبية إلى العديد من الأخطار والمهددات التي قد تهدد أمن نظم معلوماتها، وقد تتنوع مصادر تلك المهددات بحسب الأغراض التي تقوم بها تلك النظم ويمكن تصنيف أنواع التهديدات والأخطار بحسب مصادرها إلى أربعة أنواع رئيسية : (تارة، زبيبي، ٢٠٠٦)

١. خرق النظم الحاسوبية بهدف الاطلاع على المعلومات المخزنة فيها والوصول إلى معلومات شخصية أو أمنية عن شخص ما، أو التجسس الصناعي، أو التجسس المعادي للوصول إلى معلومات عسكرية سرية .
٢. خرق النظم الحاسوبية بهدف التزوير أو الاحتيال (التلاعب بالحسابات في البنوك، التلاعب بفاتورة الهاتف، التلاعب بالضرائب، تغيير بيانات شخصية من السجل المدني أو السجل العام للموظفين، إلخ..) .

٣. خرق النظم الحاسوبية بهدف تعطيل هذه النظم عن العمل لأغراض تخريبية باستخدام ما يسمى البرامج الخبيثة (مثل الفيروسات، الدودة، حصان طروادة، أو القنابل الإلكترونية) إما من قبل الأفراد أو العصابات أو الجهات الأجنبية بغرض شل هذه النظم الحاسوبية (أو المواقع على الانترنت) عن العمل وخاصة في ظروف خاصة أو في أوقات الحرب .

٤. أخطار ناتجة عن فشل التجهيزات في العمل، أعطال كهربائية، حريق، كوارث طبيعية (فيضانات، زلزال) .

وتعتبر التصنيفات السابقة لمخاطر نظم المعلومات المحاسبية الإلكترونية شاملة لجميع المخاطر التي تواجه نظم المعلومات المحاسبية، ومن خلال هذه الدراسة قامت الباحثة بتصنيف المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية بشكل عام إلى أربعة أصناف رئيسية:

أولا: مخاطر المدخلات

وهي المخاطر التي تتعلق بأول مرحلة من مراحل النظام وهي مرحلة ادخال البيانات إلى النظام الآلي وتتمثل تلك المخاطر في البنود التالية:

١. الادخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين .

٢. الادخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين .

٣. التدمير غير المتعمد للبيانات بواسطة الموظفين .

٤. التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين .

ثانيا: مخاطر تشغيل البيانات

وهي المخاطر التي تتعلق بالمرحلة الثانية من مراحل النظام وهي مرحلة تشغيل ومعالجة البيانات المخزنة في ذاكرة الحاسب وتتمثل تلك المخاطر في البنود التالية:

١. المرور (الوصول) غير الشرعي (غير المرخص به) للبيانات والنظام بواسطة الموظفين .

٢. المرور غير الشرعي (غير المرخص به) للبيانات والنظام بواسطة أشخاص من خارج المنشأة .

٣. اشتراك العديد من الموظفين في نفس كلمة السر .

٤. إدخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام .

٥. اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين .

ثالثا: مخاطر مخرجات الحاسب:

وتلك المخاطر تتعلق بمرحلة مخرجات عمليات معالجة وتشغيل البيانات وما يصدر عن هذه المرحلة من قوائم للحسابات أو تقارير وأشرطة ملفات ممغنطة وكيفية استلام تلك المخرجات وتتمثل تلك المخاطر في البنود التالية:

١. طمس أو تدمر بنود معينة من المخرجات .

٢. خلق مخرجات زائفة/ غير صحيحة .

٣. سرقة البيانات/ المعلومات.

٤. عمل نسخ غير مصرح (مرخص) بها من المخرجات .

٥. الكشف غير المرخص به للبيانات عن طريق عرضها علـــى شاشـــات العـــرض أو طبعها على الورق .

٦. طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك .

٧. المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهـــم/ ليس لهم الحق في استلام نسخة منها .

٨. تسليم المستندات الحساسة إلى أشخاص لا تتوافر فـــيهم الناحيـــة الأمنيـــة بغـــرض تمزيقها أو التخلص منها .

رابعا: **مخاطر بيئية**

وهي المخاطر التي تحدث بسبب عوامـــل بيئيـــة، مثـــل الـــزلازل والعواصـــف والفيـــضانات والأعاصير المتعلقة بأعطال التيار الكهربائي والحرائق، وسواء كانت تلك الكوارث طبيعيـــة أو غير طبيعية فإنها قد تؤثر على عمل النظام المحاسبي وقد تؤدي إلى تعطل عمـــل التجهيـــزات وتوقفها لفترات طويلة مما يؤثر على أمن وسلامة نظم المعلومات المحاسبية الالكترونية .

أسباب حدوث المخاطر التي تواجه أمن نظم المعلومات المحاسبية الالكترونية

تتعرض نظم المعلومات المحاسبية الالكترونية للعديد من المخاطر التي تهدد أمنها وقد قمنا بتقسيم تلك المخاطر إلى أربعة أقسام رئيسية تتعلق بمراحل النظام الأساسية من ادخال وتشغيل ومخرجات والقسم الرابع يتعلق بالمخاطر البيئية وقد ترجع أسباب حدوث تلك المخاطر إلى أسباب تتعلق بالمدخلات والمخرجات وأسباب تتعلق بالتشغيل أو قد نعتبرها أسباب إدارية رقابية وأسباب لها علاقة بالموظفين، وتتلخص تلك الأسباب في البنود التالية:[٨]

١. عدم كفاية وفعالية الأدوات الرقابية المطبقة لدى إدارة المنشأة .
٢. ضعف نظم الرقابة الداخلية لدى المنشأة وعدم فعاليتها .
٣. اشتراك بعض الموظفين في استخدام نفس كلمات السر من أجل الدخول إلى النظام والعبث بمحتوياته .
٤. عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات المحاسبية في المنشأة .
٥. عدم وجود سياسات واضحة وبرامج محددة ومكتوبة فيما يختص بأمن نظم المعلومات المحاسبية لدى المنشأة .
٦. عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر .
٧. ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب .
٨. عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات المحاسبية بالبنك .

[8] تم استنباط الأسباب السابقة من خلال الرجوع إلى نتائج دراسة أبوموسى ،٢٠٠٤

٩. عدم التوصيف الدقيق للهيكل الوظيفي والاداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي لدى المنشأة .

١٠.عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي المنشأة .

١١.عدم الزام الموظفين بأخذ إجازاتهم الدورية .

١٢.عدم الاهتمام الكافي بفحص التاريخ الوظيفي المهني للموظفين الجدد مما قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب .

١٣.عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي المنشأة .

١٤.عدم وجود الوعي الكافي لدى الموظفين بضرورة فحص أي البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر .

متطلبات أمن نظم المعلومات المحاسبية

تعتبر مسألة حماية أمن نظم المعلومات المحاسبية من المسائل الهامة والضرورية والتي ينبغي على المؤسسة أخذها بعين الاعتبار ووضع خطة حماية شاملة في حدود امكانياتها التنظيمية والمادية ويجب أن تكون تلك الحماية قوية وليست ضعيفة ولذلك فإنه توجد عدة متطلبات لحماية أمن نظم المعلومات المحاسبية تتمثل في: (تارة، زبيبي، ٢٠٠٦)

١. وضع سياسة حماية عامة لأمن نظم المعلومات المحاسبية تتحدد حسب طبيعة عمل وتطبيقات المنشأة .

٢. يجب على الإدارة العليا في المنشأة دعم أمن نظم المعلومات لديها .

٣. يجب أن توكل مسؤولية أمن نظم المعلومات في المؤسسة لأشخاص محددين .

٤. تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة .

٥. تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية .

٦. الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن .

٧. تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط .

٨. تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات .

أساليب الرقابة على النظم المحاسبية الالكترونية

مع تطور تكنولوجيا المعلومات ومع الانتشار الواسع لتطبيق النظم المحاسبية بطرق إلكترونية أصبحت هناك حاجة ماسة لحماية تلك النظم من المخاطر التي تتعرض لها وتوفير أساليب الرقابة اللازمة لحماية النظم المحاسبية الإلكترونية وضمان إنجاز عملياتها بالشكل الصحيح وفي الوقت المناسب ولذلك فإن الرقابة على النظم المحاسبية الإلكترونية تقسم إلى ثلاث مجموعات رئيسية حسب مراحل النظام وهي:

أ) الرقابة على المدخلات

وهي تهدف إلى التأكد من أن البيانات التي تم إدخالها إلى النظام أدخلت في الوقت المناسب وبشكل صحيح، وضمان سير تلك البيانات خلال خطوط الاتصال وعدم فقدها أو تغييرها واكتشاف أي أخطاء تتعلق بالبيانات قبل عملية تشغيلها وذلك لضمان خلو البيانات المدخلة من أي أخطاء وليتم الحصول على مخرجات سليمة بناء على مدخلات سليمة ولذلك فلا بد من الحصول على مدخلات البيانات في مرحلة مبكرة من مراحل معالجتها في النظام، وذلك للأسباب التالية: (قاسم، ٢٠٠٣، ٣٥٨)

١. امكانية تصحيح الأخطاء التي تم اكتشافها في البيانات التي تم رفضها في بداية ادخالها والرجوع إلى المستندات الخاصة بها وفحص أسباب رفضها .
٢. أن البيانات التي تم ادخالها بشكل صحيح ليس من الضرورة أن تكون بيانات جيدة ولذلك يجب اجراء اختبارات أخرى لفحصها خلال مراحل تداولها ومعالجتها.

٣. خلو نظام المعلومات المحاسبي من بيانات غير دقيقة في المراحل الأخيرة لعمليات المعالجة يمكن من حماية ووقاية الملفات الرئيسية وعمليات المعالجة في خطواتها الأخيرة .

٤. اعتماد نظام المعلومات المحاسبي على مدخلات جيدة يمكنه من الحصول على مخرجات جيدة .

ب) الرقابة على تشغيل البيانات

وهي تهدف إلى التحقق من أن البيانات تم تشغيلها بصورة دقيقة وبشكل صحيح وأنه تم معالجة كافة العمليات المتعلقة بالتشغيل وقد تم استخدام جميع البرامج المناسبة واللازمة لعملية التشغيل ومن أهم الوسائل الرقابية على تشغيل العمليات ما يلي (الدهراوي، ٢٠٠٣، ص١٨٨)

١. تطبيق الاختبارات التي تضمن صحة عمليات التشغيل بحيث يتم رفض التعامل مع المدخلات أو المخرجات غير الصحيحة .

٢. استكمال مسار المراجعة الذي يمكن من تتبع سجل عملية من عمليات التشغيل والمساعدة في اعداد القوائم المالية .

٣. تزويد برامج التشغيل بوظائف ومهام تمكن من تسجيل أي عملية محاولة للتدخل في عمل البرنامج أثناء عملية التشغيل والمعالجة .

ج) الرقابة على المخرجات

وهي تهدف للتأكد من أن نتائج مخرجات عملية التشغيل كاملة وصحيحة وجيدة ودقيقة، وأنه تم تسليمها وتوزيعها للأشخاص المسموح لهم باستلامها والاطلاع عليها، وتستند الرقابة على المخرجات على البند السابق وهو عملية الرقابة على التشغيل، فإذا كانت الرقابة على

المدخلات وعلى عملية التشغيل جيدة ودقيقة فهذا يؤدي إلى الحصول على مخرجات سليمة ودقيقة .

كيف نحمي أمن نظم المعلومات المحاسبية:

لتحقيق متطلبات أمن وحماية نظم المعلومات المحاسبية فلا بد للمؤسسة من اتباع عدة اجراءات للحماية ومنها: (تارة، زبيبي، ٢٠٠٦)

١. اجراءات الحماية الفيزيائية لنظم المعلومات بما فيها الحماية المادية للأجهزة التي تحتوي على نظم المعلومات .
٢. انتقاء العاملين في النظم المعلوماتية بحيث يكونوا ذوي خبرة وثقة وأمانة ويعملون لمصلحة المنشأة وتوعيتهم أمنيا للمحافظة على أمن المعلومات .
٣. إجراءات الحماية الخاصة بنظم تشغيل البيانات والبرامج التطبيقية اللازمة لذلك وضبط الصلاحيات الخاصة بنظم التشغيل .
٤. إجراءات الحماية الخاصة بالشبكات المعلوماتية ومنع اختراقها .
٥. العمل على تشفير المعلومات التي يتم تخزينها ونقلها حتى لا يتم معرفة ماهيتها في حالة الحصول عليها من أشخاص غير مصرح لهم بذلك .
٦. إجراءات حفظ البيانات بصورة عامة وحفظ نسخ منها في مواقع آمنة يمكن الرجوع إليها عند الحاجة لذلك .
٧. إجراءات ضمان استمرارية عمل وجاهزية نظم المعلومات في شتى الظروف التي قد تواجه النظم، مثل تعطل أو توقف النظم المعلوماتية عن العمل .

إجراءات الحماية المتبعة ضد مخاطر أمن نظم المعلومات المحاسبية:

تعتبر قضية تطبيق أمن المعلومات قضية مهمة جدا لدى المؤسسات والشركات التي تعتمد في عملها على تكنولوجيا المعلومات، حيث تسعى المؤسسات إلى حفظ أمن نظمها المعلوماتية من خلال تطبيق شتى وسائل الحماية مثل جدران النار "والذي يعتبر أحد وسائل أمن المعلومات والذي صمم لمنع الوصول الغير مصرح به من وإلى الشبكة الخاصة، ويتم بناؤه من خلال القطع المادية والبرمجيات" (Voloniono,Robinson,2004,p199) إضافة إلى برامج مكافحة الفيروسات وطرق حماية تقنية أخرى، ولكن هذا الأمر يعتبر خطير جدا ولا يمكن أن نضمن نجاحه بدون إدارة ممتازة، وإجراءات تشغيلية جيدة، حيث يقع على عاتق المنشأة إصدار القرارات الإدارية المتعلقة بأمن نظم المعلومات لتجنب المخاطر التي يمكن أن تتعرض لها .

ومع ذلك فإننا نجد أنه مع قيام الشركات بتطبيق وسائل الحماية المطلوبة إلا أن هناك بعض الاقتراحات الناجحة لنظم المعلومات .

كما أن كل كتب أمن الشركات وضحت أن الأمن أساسا قضية إدارية وليست تكنولوجية، فبدون تغيير جوهري في ثقافة أمن الشركات وممارساتها، فإن شراء التكنولوجيا سوف لا يجلب إلا قليلا من الأمن، ولذلك فإن على المنشآت اتباع العديد من الإجراءات لمواجهة مخاطر أمن نظم المعلومات المحاسبية ومن تلك الإجراءات : (Panko, Raymond R,2004)

أولا/ تعهد التزام الإدارة العليا

حيث يقع على عاتق الإدارة العليا للشركة الالتزام بشكل قوي بتطبيق أمن المعلومات، كما أن الإدارة العليا لتكنولوجيا المعلومات تحتاج أيضا إلى التزام قوي بتطبيق أمن المعلومات، فأمن

المعلومات يعتبر دائما سببا غير مرغوبا لأقسام تكنولوجيا المعلومات في الشركة .
(Panko, Raymond R,2004,p31)

"فمثلا في سنة (٢٠٠٢) أوضحت ردود استطلاع (Network World Survey) أن أعلى خمس اهتمامات في تكنولوجيا المعلومات كانت اهتمامات الأمن، وحماية الشبكة، وتحسين أنظمة الاسترجاع من الكوارث، وبناء شبكات افتراضية خاصة"[٩](John cox,2002)

لذلك هذه الردود المتشابهة تقول أيضا أنهم خططوا فقط لزيادة ميزانية أمن المعلومات بمعدل ٥% . (Panko, Raymond R,2004,p32)

ثانيا/ تنفيذ الاجراءات المطلوبة

وهي حرجة أيضا لأفراد تكنولوجيا المعلومات، وموظفي الشركة الآخرين، لتنفيذ مهام أمن المعلومات بشكل مخلص وجيد، فمعظم الهجمات تستفيد من الاختراقات الناتجة من الإعدادات الغير صحيحة لأدوات الأمن، وكذلك بسبب فشل الموظفين التشغيليين في تغطية نقطة ضعف أمن معروفة في البرمجيات . (Panko, Raymond R, 2004, p32)

ولذلك يجب على ادارة الشركة متابعة موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة .

ثالثا/ وضع الاجراءات ومعاقبة الموظفين

ربما الشيء المقيت جدا، أنه من الحرج أن تنفذ إجراءات الأمن من خلال إقرار موظفين يقومون بكسرهذه الاجراءات، فالمبدأ الأساسي للإدارة أن تحصل على ماذا تريد أن تنفذ، حيث

[9] نقلا عن(Panko, Raymond R,2004,p32)

أن كثيرا من موظفي المستوى التشغيلي، وحتى مدراء الادارة العليا سوف يكسرون إجراءات الأمن لكي يجعلوا حياتهم أفضل أو لأسباب أخرى، وما دام المنتهكين لا يعاقبون، فالأمن لا يمكن له أن يزدهر، وبالطبع فإن المعنيين بالأمن يحتاجون للتدريب على وسائل حماية أمن معلوماتهم، ويجب أن يكونوا واقعيين باقتراح العقوبات . (Panko, Raymond R, 2004, p32)

و بشكل عام ينبغي على إدارة الشركة أن تضع قواعد خاصة لحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد .

رابعا/ تطبيق خطة الأمن الشاملة

من الدروس الحرجة الأخرى التي تدرس بواسطة حوادث الأمن المؤلمة، هو أن الشركة يجب أن تملك خطة شاملة لأمن المعلومات، فيجب عليها أن تغلق جميع أبواب الاختراق وبينما تقوم المؤسسة بحماية نفسها من الاختراق يحاول المهاجم اكتشاف نقطة ضعف واحدة لكي يخترق من خلالها الأنظمة، ولذلك فإن إحدى الطرق لتحسين الحماية هو انشائها بشكل معمق، لأن المهاجم يحاول كسرها خلال اجراءات مضادة ومتعددة يقوم بها بشكل متكرر حتى ينجح، فمثلا تقوم الشركة بوضع عدة جدران نارية (Firewalls)، واحد منهم رئيسي والأخرى متفرعة، فيقوم المهاجم بمحاولة اختراقها كلها للوصول إلى النظام المستهدف، ومع أن اجراءات الحماية صعبة الاعداد، فإنه من السهل وجود اختراق، حتى ولو كانت المؤسسة تعتقد أنها تمتلك حماية شاملة إلا أنه من المهم أيضا امتلاك تدقيق الحماية (Security Audit)، حيث أن مجموعة الهجوم قد تُوظف لدى الشركة لكي تحاول اختراق النظام. (Panko, Raymond R, 2004, p33)

ولكي تكون المؤسسة آمنة فلا بد لها من تحقيق الأهداف الجوهرية لأمن المعلومات **وهي** (كما تم ذكرها تحت بند عناصر أمن المعلومات سابقا)، السرية أو الموثوقية (Confidentiality) و التعرف أو التحقق من هوية الشخصية (Authentication) وسلامة المحتوى (Integrity) و استمرارية توفر المعلومات أو الخدمة (Availability)، عدم الإنكار (No repudiation) ، وهي تعتبر أيضا من الدعائم الأساسية لتطبيق أمن المعلومات في أي منشأة . (Panko, Raymond R, 2004, p33)

خامسا/ دورة التخديط-الحماية-الاستجابة (Plan-Protect-Respond PPR)

الشركات المهتمة جدا بالحماية الشاملة يجب أن تمر إجراءات تطبيقها خلال عملية تدعى التخطيط-الحماية-الاستجابة (PPR) .

١. التخطيط

حيث يشمل تخطيط الحماية الشامل كما أوضحنا سابقا، مثل إغلاق جميع الأبواب في وجه المهاجمين، فإذا قمت بعمل حماية لأبواب دخول المبنى الرئيسية، ولكن لم تأخذ بعين الإعتبار حماية الأبواب الفرعية مثل أبواب النار فهذا يعني أنك لم تقم بعمل حماية شاملة، فالمهاجمين يحتاجون نقطة ضعف واحدة للاختراق، لذا يجب وضع السؤال التالي دائما: ماذا نسينا أن نعمل؟

ويندرج تحت هذه المرحلة الأمور التالية: (Panko, Raymond R,2004,p34)

أ. تحليل المخاطر

فيجب على المؤسسة تحليل المخاطر المتعلقة بأمن المعلومات، كما يجب عليها تحديد حجم النفقات التي ستصرفها في سبيل وضع إجراءات الحماية، صحيح أن التهديدات تدمر ولكن الحماية أيضا مكلفة، وتشمل تحليل المخاطر عدة خطوات :

- حصر وتعداد التهديدات، وهو تعريف كل التهديدات المتوقعة .
- تحليل شدة التهديدات، وهو تكلفة كل تهديد واحتمال حدوثة .
- تطبيق الاجراءات المضادة، حيث من الممكن أن يكون التهديد معقولا ولكن إيقافه قد يكون مكلف جدا، فقيمة الحماية هي تكلفة شدة التهديد مطروحا منها تكلفة الإجراءات المضادة، فالمؤسسة غالبا ترفض تطبيق الاجراءات المضادة لأن تكلفتها تزيد عن تكلفة شدة التهديد، أي تبقى على مخاطرته، وهذا منطقيا .
- وضع الأولويات، أي ترتيب الاجراءات المضادة حسب الأهم فالأقل أهمية .

ب. سياسات الحماية

حيث يتم تطبيق هذه السياسات على نطاق واسع داخل المؤسسة، فمثلا تسمح المؤسسة بإجازة لموظفيها لمدة أسبوعين سنويا على أن يكون منها أسبوعا بشكل متتالي، والغرض من ذلك كشف حالات الغش لدى الموظفين خاصة إذا لم يكن حول هذه الحالة من الغش منشغلا في إجازته، ومثال آخر وضع إجراء إداري مركزي لحماية أجهزة الموظفين من الفيروسات . (Panko, Raymond R, 2004, p37)

ج. وضع سياسات إرشاد تشمل الاجراءت والفحص

ويقصد بذلك وضع مجموعة محكمة وشاملة من السياسات التي يجب أن توضع لترشد الأفعال التي تحدث في المستوى الأدنى من المؤسسة، ويشمل ذلك وضع السياسات التي تتحكم بالتكنولوجيا مثل وضع سياسة لربط الشبكة الداخلية للموسسة مع الشبكة العالمية (الانترنت)، تتضمن هذه السياسة احتياج المؤسسة من جدران النار (Firewalls) وأماكن تشغيلها وأن تتحكم السياسات بالاجراءات، فمثلا إذا طلب حماية للرقم الوطني للأفراد في نظام ما، فيجب وضع السياسات اللازمة للتأكد من عدم كسر طرق الحماية لدى الأنظمة واختراقها من قبل المهاجمين، وأخيرا أن تتحكم السياسات بفحص طرق الحماية باستمرار . (Panko, Raymond R, 2004, p37)

٢. الحماية

من الملاحظ دائما أن أمن المعلومات لدى المؤسسة يكون مفتوحا خلال مرحلة الحماية، وأحيانا يقوم المهاجم بكشف نقطة ضعف في هذه المرحلة وربما تكون ناجحة، وتشمل طرق الحماية تركيب الأجهزة الخاصة بالحماية مثل جدران النار (Firewalls) وتنزيل البرامج اللازمة لها، وإعدادها برمجيا بما يتناسب مع سياسات الحماية المطلوبة، وأن يتم تحديث طرق الحماية باستمرار، لأن أدوات الحماية تصبح غير مفيدة مع مرور الوقت، وتشمل أيضا فحص طرق الحماية والإعدادات الخاصة بها باستمرار، وهو ما يسمى بتدقيق أمن المعلومات .

(Panko, Raymond R, 2004, p38)

الاستجابة

يقوم المهاجم باختراق الأنظمة أحيانا وينجح في ذلك حتى مع وجود حماية قوية، فإذا حصل مثل هذا الحادث ولم تكن هناك خطة موضوعة لتقليل مخاطر هذا الحادث، تكون عمليـــة الرجـــوع للأنظمة بوضعها الطبيعي عملية صعبة ومستحيلة، لذلك يجب على المؤسسة أن تضع إجراءات صارمة تشمل انتاج تقارير رسمية لتعريف وتحديد حادث الاختراق وتحديد المهاجمين وإيقـــافهم وإصلاح الدمار الناتج، وفي بعض الحالات معاقبـــة المهـــاجمين . (Panko, Raymond R, 2004, p39)

الفصل الرابع

الجهاز المصرفي الفلسطيني

الفصل الرابع

الجهاز المصرفي الفلسطيني

يعتبر القطاع المصرفي من أهم القطاعات الاقتصادية في فلسطين والتي تقوم بـــدعم الاقتـــصاد الفلسطيني، ويمثل الجهاز المصرفي الفلسطيني حلقة الوصل بين المستثمرين والمودعين ويساعد على تداول المال بسرعة وسهولة، وهذا ما يؤثر على عمل النظام المحاسبي المصرفي والـــذي يجب أن يكون قويا وفعالا حتى يستطيع اسستيعاب حركة العمليات المالية التي يقوم بها النظـــام المصرفي والقدرة على متابعة تلك العمليات بصورة تعكس عمل النظام بكل دقة وثقة .

أهداف النظام المحاسبي المصرفي :

يسعى نظام المعلومات المحاسبي المصرفي إلى تحقيق العديد من الأهداف والتي مـــن أهمهـــا: (كراجة، ٢٠٠٠، ص٢٢)

١. تحقيق الدقة في انجاز العمليات المالية واستخراج النتائج بالشكل الصحيح .

٢. السرعة في تنفيذ العمليات المالية وفي الوقت المناسب .

٣. الاقتصاد في النفقة بما يحقق التوازن بين تكلفة النظام وبين الأهداف المطلوبة .

٤. تحقيق مبدأ الرقابة الداخلية اللازمة لحماية النظام .

٥. انجاز الكشوف والتقارير المالية المطلوبة لغايات البنك وكذلك البنك المركزي .

ومن خلال ماسبق نلاحظ أن أهداف النظام المحاسبي المصرفي هي نفـــسها أهـــداف أي نظـــام معلومات محاسبي، والتي لابد من العمل على تحقيقها من أجل ضمان استمرارية العمـــل لـــدى المصرف وتعزيز الثقة والأمان بالعمل المصرفي .

مشاكل الجهاز المصرفي الفلسطيني

يتعرض الجهاز المصرفي الفلسطيني إلى العديد من المشاكل التي قد تؤثر على العمل المصرفي الفلسطيني ومن أهم تلك المشاكل: (عاشور، ٢٠٠٣، ص٤١٠- ٤١٥)

١. التشريع المصرفي والناتج عن الافتقار لبعض التشريعات التي تحكم العلاقة بين المصرف وعملائه في حالات الاخلال بالالتزامات .

٢. عدم وجود مناخ استثماري ملائم يساعد المستثمر على اتخاذ القرار المناسب للاستثمار بسبب العديد من العوامل الإقتصادية والإجتماعية والثقافية والدينية والقانونية وعوامل الثقة والأمان .

٣. عدم وجود الاستقرار السياسي والاجتماعي .

٤. عدم توافر الكوادر المدربة على الأعمال المصرفية بالرغم من توافر الخريجين في المجالات التي تحتاجها أعمال المصارف .

٥. مشاكل تتعلق بضعف البنية التحتية بسبب الظروف السياسية التي يعيشها المجتمع الفلسطيني .

٦. الضمانات العقارية المتعلقة بالمباني والأراضي والتي تتم بعقود خارج دائرة الطابو والتي من الصعب قبولها لدى المصرف كضمانات مقابل الحصول على قروض صعبة.

٧. ضعف التنظيم المحاسبي في بيئة الأعمال الفسطينية .

٨. افتقار الجهاز المصرفي إلى المؤسسة المصرفية المالية المساندة لعمله .

٩. وجود اختلال وتشوهات هيكلية في الجهاز المصرفي وذلك بسبب عدم التزام المصارف في الهدف الذي أنشئت من أجله حيث أن العديد من المصارف المتخصصة لا تمـــارس عملها كمصارف متخصصة وإنما تمارس عمل المصارف التجارية .

١٠.مشكلة بداية العمل وكيفية تحديد ورسم الأهداف والسياسات القومية .

وقد تؤثر المشاكل السابقة على أداء العمل المصرفي وخاصة الموظفين الذين يتعرضون لمشاكل عدم الاستقرار في الحياة السياسية والاجتماعية والذي يؤدي إلى عدم قيـــام هـــؤلاء المـــوظفين بانجاز أعمالهم بالدقة المطلوبة مما يؤدي إلى عدم الثقة بالنظام المصرفي لدى المصرف .

أمن نظم المعلومات المحاسبية في المصارف الفلسطينية وأثرها على مرونة العمل المصرفي :

تعتبر مسألة توفير الحماية لأمن نظم المعلومات المحاسبية في المصارف الفلسطينية من المسائل الهامة والضرورية وفي غاية الخطورة .

وخاصة فيما يتعلق بالخدمات التي يستطيع العملاء تنفيذها بأنفسهم ومثال ذلك بطاقة الصراف الآلي الذي يستطيع العميل من خلالها الإستعلام عن رصيد حسابه ويتمكن من سحب المبلغ الذي يريده ولكن عليه في نفس الوقت توفير كلمة المرور التي تمكنه من تنفيذ المهمة التي يريدها، كما توفر بعض المصارف خدمة التعامل مع صفحة البنك من خلال الإنترنت والتي توفر للعميل التعرف على رصيد حسابه وتحويل مبلغ معين من رصيده إلى رصيد عميل آخر ولكن ينبغي على العميل الذي يريد تنفيذ عملية التحويل تحديد رقم الحساب وكلمة المرور الخاصة به بالإضافة إلى معلومات أخرى قد تكون ضرورية لتنفيذ المهمة، ولكن يعتبر البنك العربي في قطاع غزة هو البنك الوحيد الذي يوفر خدمة تمكين العملاء من تنفيذ اطلاع العميل على رصيد حسابه وإجراء عملية التحويل المطلوبة من خلال الإنترنت، ولكن هناك قيود محددة تضعها المصارف للحفاظ على أمن معلوماتها التي يتم الوصول إليها من خلال الخدمات التي ينفذها العملاء بأنفسهم مثال ذلك تحديد سقف محدد لعملية السحب أو التحويل .

ولكن السؤال الذي يطرح نفسه هنا هو هل يعتبر أمن المعلومات عدو المرونة؟ أو هل يؤثر أمن المعلومات على تنفيذ الخدمات التي يقدمها المصرف لعملائه؟

والجواب هنا هو أن أمن المعلومات ليس عدو المرونه وإنما قد يؤثر على مرونة تقديم الخدمات نسبيا، ولكن في الوقت نفسه يوفر مرونة وخدمات جديدة، ومثال ذلك ما تم طرحه سابقا في خدمة الصراف الآلي حيث أن أمن المعومات زاد من العقبات وقلل من الخدمة الذاتية فيما يتعلق بالخدمات المصرفية الآلية ولكن في الوقت نفسه قدم للعملاء مرونة في الاستعلام عن الرصيد وتسديد الفواتير والتحويل وغيرها من الخدمات والتي لا يمكن توفيرها دون الاعتماد على أمن المعلومات، ولكي نوازن بين أمن المعلومات من ناحية والخدمات المقدمة والمرونة من ناحية أخرى، فلا بد من دراسة جدوى تطبيق أمن المعلومات قبل تطبيقه وتحديد إيجابيات وسلبيات عملية التطبيق للإستفادة من الإيجابيات ومعالجة السلبيات، حيث أن تطبيق أمن المعلومات يعتبر مهم جدا لثلاثة أطراف وهم المستفيدين من الخدمات المقدمة وموظفي الدعم الفني والعلاقات العامة والإدارة العليا لدى البنك لكسب ثقتهم ودعمهم لتطبيقات أمن المعلومات، حيث أن أهم ما تحتاج إليه الإدارة العليا وبعض إدارات تقنية المعلومات هو إقتناء التقنيات المختلفة في أمن المعلومات واستخدام العوامل المساعدة التكاملية لتحقيق الأمن الشامل والتي كثيرا ما تكون تلك العوامل المساعدة أدوات نجاح لتلك التقنيات مثل الإجراءات المدروسة والجهود البشرية المختلفة . (الغتبر، ٢٠٠٦، ص١)

الفصل الخامس

تحليل الاستبيان واختبار فرضيات الدراسة

الفصل الخامس

تحليل الاستبيان واختبار فرضيات الدراسة

مقدمة :

في هذا الفصل سيتم التطرق إلى التأكد من صدق الاستبانة بالاضافة إلى التحليل الوصفي لعينة الدراسة واختبار الفرضيات باستخدام الأساليب الإحصائية المناسبة وذلك باستخدام برنامج (SPSS) الإحصائي .

أولاً: صدق وثبات استبانة الدراسة:

يقصد بصدق الاستبانة أن تكون استبانه الدراسة قادرة على انجاز قياس ما وضعت لأجله بما يحقق أهداف الدراسة ويجيب على أسئلتها وفرضياتها وقد تم قياس صدق الاستبانة من خلال طريقتين كما يلي:

١. صدق المحتوى (المحكمين)

قامت الباحثة بعرض استبانه الدراسة في صورتها الأولية على مجموعة من الأساتذة الأكاديميين[١٠] ،ومن لهم خبرة في نظم المعلومات المحاسبية الالكترونية في المصارف، من أجل الاسترشاد بآرائهم حول العبارات التي تضمنتها استبانه الدراسة وقد تم الأخذ بآراء المحكمين حيث تم حذف بعض الفقرات التي لا ترتبط بموضوع الاستبانة كما تم تعديل فقرات أخرى وإعادة تصنيف بعض الفقرات في المجالات التي تضمنتها استبانه الدراسة، حتى تم التوصل إلى الصورة النهائية الاستبانة والمتعلقة بمخاطر نظم المعلومات المحاسبية الالكترونية في النظام المصرفي الفلسطيني، بحيث أصبح بمقدور الباحثة توزيع الاستبانة على أفراد عينة الدراسة الذين لهم علاقة و اطلاع على نظام المعلومات المحاسبي في فروع المصارف العاملة

[10] انظر ملحق (٢) ،قائمة بأسماء محكمي استبانة الدراسة.

الذين لهم علاقة و اطلاع على نظام المعلومات المحاسبي في فروع المصارف العاملة في قطاع غزة. و تتكون استبانه الدراسة من جزئين كما يلي:

أ. الجزء الأول:

وهو مكون من عدة أسئلة تتعلق بمعلومات عامة عن أفراد العينة مثل المؤهل العلمي، سنوات الخبرة، المسمى الوظيفي و معلومات أخرى حول النظام المحاسبي المعمول به في المصرف.

ب. الجزء الثاني:-

ويتكون من ثلاثة مجالات كلها تتعلق بمخاطر نظم المعلومات المحاسبية، وهذه المجالات موضحة في الجدول التالي:

جدول رقم (١)

مجالات مخاطر نظم المعلومات المحاسبية الالكترونية

رقم المجال	عنوان المجال	عدد الفقرات
١	المخاطر التي تهدد أمن نظم المعلومات المحاسبية الالكترونية	١٩
٢	أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية	١٤
٣	إجراءات الحماية المتبعة ضد مخاطر أمن نظم المعلومات المحاسبية الالكترونية	١٤

٢. صدق الاتساق الداخلي:

يقصد بصدق الاتساق الداخلي مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي إليه هذه الفقرة، وقد تم التحقق من صدق الاتساق الداخلي من خلال إيجاد معامل الارتباط الخطي لبيرسون بين كل فقرة من فقرات الاستبانة والدرجة الكلية للمجال الذي تنتمي إليه هذه الفقرة، وقد كانت النتائج ايجابية بشكل عام ، حيث دلت معاملات الارتباط المختلفة على أن هناك اتساقا داخلياً للفقرات مع المجالات التي تنتمي إليها وفيما يلي معاملات الارتباط المختلفة لكل فقرة مع المجال الذي تنتمي إليه.

جدول رقم (٢)

معاملات ارتباط بيرسون بين فقرات المجال الأول المتعلق بالمخاطر التي تهدد نظام المعلومات المحاسبي الالكتروني والدرجة الكلية للمجال

رقم العبارة	نص عبارات المجال الأول (المخاطر التي تهدد أمن نظم المعلومات المحاسبية الالكترونية)	معامل ارتباط بيرسون	مستوى الدلالة الإحصائية sig
١	الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.	٠,٤٩٦	٠
٢	الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.	٠,٧٢٩	٠
٣	التدمير غير المتعمد للبيانات بواسطة الموظفين.	٠,٦١٣	٠
٤	التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.	٠,٧٩٨	٠
٥	المرور (الوصول) غير الشرعي (غير المرخص به) للبيانات / النظام بواسطة الموظفين.	٠,٦٨٦	٠
٦	المرور غير الشرعي (غير المرخص به) للبيانات / النظام بواسطة أشخاص من خارج المنشأة.	٠,٦٧٧	٠

تابع جدول رقم (٢)

٧	إشراك الموظفين في كلمة السر .	٠,٥٤٤	٠
٨	إدخال فيروس الكمبيوتر للنظام المحاسبي.	٠,٥٢٣	٠
٩	اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين	٠,٦٥٢	٠
١٠	طمس أو تدمير بنود معينة من المخرجات.	٠,٧٢٦	٠
١١	خلق مخرجات زائفة / غير صحيحة.	٠,٦٥٠	٠
١٢	سرقة البيانات / المعلومات.	٠,٧١٧	٠
١٣	عمل نسخ غير مصرح (مرخص) بها من المخرجات.	٠,٨٤٦	٠
١٤	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.	٠,٦٩٠	٠
١٥	طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.	٠,٦٩٥	٠
١٦	المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم / ليس لهم الحق في استلامها نسخة منها.	٠,٧٤٦	٠
١٦	تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.	٠,٥٨٤	٠
١٨	الكوارث الطبيعية مثل الحرائق، الفيضانات أو انقطاع مصدر الطاقة.	٠,٢٦٨	٠,٠٠٢
١٩	الكوارث غير الطبيعية والتي هي من صنع الإنسان مثل الحرائق، أو الفيضانات.	٠,٥٦٩	٠

مستوى الدلالة الإحصائية حسب عند α = ٠,٠٥

يلاحظ من خلال الجدول السابق أن كافة معاملات ارتباط بيرسون بين كل فقرة من فقرات المجال الأول والبالغة ١٩ فقرة والدرجة الكلية للمجال معنوية إحصائيا عند مستوى دلالة الإحصائية (٠,٠١) وهذا يشير إلى الاتساق الداخلي الكبير لفقرات المجال الأول.

جدول رقم (٣)

معاملات ارتباط بيرسون بين فقرات المجال الثاني المتعلق بأسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية **والدرجة الكلية للمجال**

رقم العبارة	نص فقرات المجال الثاني (أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية)	معامل ارتباط بيرسون	مستوى الدلالة الإحصائية sig
١	عدم كفاية وفعالية الأدوات والضوابط الرقابية المطبقة في البنك.	٠,٨٨٨	٠
٢	ضعف نظم الرقابة الداخلية في البنك وعدم فعاليتها.	٠,٨٩٩	٠
٣	اشتراك بعض الموظفين في استخدام نفس كلمات السر .	٠,٨١٥	٠
٤	عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات.	٠,٩٠٩	٠
٥	عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات المحاسبية بالبنك.	٠,٩٢٤	٠
٦	عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في البنك.	٠,٨٧٧	٠
٧	ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب الآلي.	٠,٨٩٢	٠
٨	عدم وجود سياسات واضحة ومكتوبة فيما يختص بأمن نظم المعلومات المحاسبية في البنك.	٠,٨٨١	٠
٩	عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في البنك.	٠,٩١٣	٠
تابع جدول رقم (٣)			
١٠	عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي البنك.	٠,٨٧٣	٠
١١	عدم إلزام الموظفين بأخذ إجازتهم الدورية.	٠,٨٦٣	٠
١٢	عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد.	٠,٨٤٣	٠
١٣	عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية	٠,٧٤١	٠

	لموظفي البنك.		
١٤	عدم الوعي الكافي لدى الموظفين بضرورة فحص أي البـــرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.	٠,٨٧١	٠

مستوى الدلالة الإحصائية حسب عند α = ٠,٠٥

يلاحظ من خلال الجدول السابق أن كافة معاملات ارتباط بيرسون بين كل فقـــرة مـــن فقـــرات المجال الثاني والبالغة ١٤ فقرة والدرجة الكلية للمجال معنوية إحصائيا عنـــد مـــستوى دلالـــة الإحصائية (٠,٠١) وهذا يشير إلى الاتساق الداخلي الكبير لفقرات المجال الثاني.

جدول رقم (٤)

معاملات ارتباط بيرسون بين فقرات المجال الثالث المتعلق بإجراءات الحماية المتبعة ضد مخاطر نظم المعلومات المحاسبية الالكترونية **والدرجة الكلية للمجال**

رقم العبارة	نص فقرات المجال الثالث (إجراءات الحماية المتبعة ضد مخاطر أمن نظم المعلومات المحاسبية الالكترونية)	معامل ارتباط بيرسون	مستوى الدلالة الإحصائية sig
١	تقوم إدارة البنك بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات.	٠,٨١٨	٠
٢	تتعهد إدارة البنك العليا بتطبيق أمن المعلومات.	٠,٨٢٢	٠
٣	تتابع إدارة البنك موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة.	٠,٧٨٧	٠
٤	تقوم إدارة البنك بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد.	٠,٧٩٢	٠
٥	تقوم إدارة البنك بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن الرجوع إليها عند الضرورة.	٠,٧٩٩	٠
٦	تطبق إدارة البنك أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد.	٠,٧٤٦	٠
٧	تقوم إدارة البنك بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة.	٠,٨٠٠	٠
٨	تقوم إدارة البنك بوضع سياسات خاصة بأمن المعلومات فيما يتعلق باختيار التقنية المناسبة وآلية العمل بها.	٠,٧٩٨	٠

تابع جدول رقم (٤)

٩	تقوم إدارة البنك بتركيب طرق الحماية التقنية مثل جدران النار (Firewalls) ومضادات الفيروسات وغيرها.	٠,٦٥٥	٠
١٠	تقوم إدارة البنك بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا.	٠,٧٦١	٠
١١	تقوم إدارة البنك بفحص طرق الحماية ودراسة مدى فعاليتها.	٠,٨١٧	٠
١٢	تقوم إدارة البنك باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق.	٠,٨٢٣	٠
١٣	تقوم إدارة البنك بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه.	٠,٧١٥	٠
١٤	تستفيد إدارة البنك من خبرة البنوك العالمية في مجال أمن المعلومات.	٠,٧٩٦	٠

مستوى الدلالة الإحصائية حسب عند α = ٠,٠٥

يلاحظ من خلال الجدول السابق أن كافة معاملات ارتباط بيرسون بين كل فقرة من فقرات المجال الثالث والبالغة ١٤ فقرة والدرجة الكلية للمجال معنوية إحصائيا عند مستوى دلالة الإحصائية (٠,٠١) وهذا يشير إلى الاتساق الداخلي الكبير لفقرات المجال الثالث.

بالإضافة إلى ما سبق فقد تم حساب معامل ارتباط بيرسون بين درجة كل مجال من مجالات الاستبانة الثلاثة والدرجة الكلية للاستبانة وذلك كما في الجدول التالي:

جدول رقم (٥)

حساب معامل ارتباط بيرسون بين درجة كل مجال من مجالات الاستبانة الثلاثة والدرجة الكلية للاستبانة

رقم المجال	عنوان المجال	معامل ارتباط بيرسون	مستوى الدلالة الإحصائية sig
١	المخاطر التي تهدد نظام المعلومات المحاسبي الالكتروني	٠,٤٦٧	٠
٢	أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية	٠,٧٨١	٠
٣	إجراءات الحماية المتبعة ضد مخاطر نظم المعلومات المحاسبية الالكترونية	٠,٥٤٠	٠

مستوى الدلالة الإحصائية حسب عند α = ٠,٠٥

يتضح من خلال الجدول السابق أن جميع معاملات الارتباط في جميع مجالات الاستبانة الثلاثة دالة إحصائيا وبدرجة قوية عند مستوى دلالة إحصائية (٠,٠١).

مما يعني أن درجات أفراد العينة في كل مجال من مجالات الاستبانة ترتبط ارتباطاً دالاً إحصائيا بدرجاتهم الكلية في الاستبانة وهذا يشير إلى تحقق صدق الاتساق الداخلي لاستبانه الدراسة وبشكل قوي.

ثبات الاستبانة:

يقصد بثبات الاستبانة أن تعطى هذه الاستبانة نفس النتيجة لو تم إعادة توزيع الاستبانة أكثر من مرة أو بعبارة أخرى ، أن ثبات الاستبانة يعني الاستقرار في نتائج الاستبانة وعدم تغييرها بشكل كبير فيما لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية معينة.

وقد تحققت الباحثة من ثبات استبانة الدراسة من خلال طريقتي التجزئة النصفية ومعامل الفاكرونباخ وذلك كما يلي:

١. **طريقة التجزئة النصفية**:

قامت الباحثة بتقسيم فقرات كل مجال من مجالات الاستبانة الثلاثة وكذلك الاستبانة ككل إلى جزئين بحيث يشمل الجزء الأول العبارات ذات الأرقام الفردية ويشمل الجزء الثاني العبارات ذات الأرقام الزوجية، ثم حسبت درجات الجزء الأول ودرجات الجزء الثاني في كل مجال من مجالات الاستبانة، وبعد ذلك تم حساب معامل ارتباط بيرسون بين الجزئين، ثم تم تعديل معامل الارتباط باستخدام معادلة سيبرمان براون وهذه المعادلة هي:

معامل الثبات: $$R = \frac{2r}{r+1}$$

حيث r = معامل ارتباط بيرسون، وقد كانت النتائج كما يلي:

جدول رقم (٦)

معاملات ارتباط بيرسون والثبات لكل مجال من مجالات الاستبانة وكذلك للاستبانة ككل:

الرقم	مجـــــالات الاستبانة	عدد الفقرات	معامل ارتباط بيرسون	معامل الثبات	مستوى الدلالة الإحصائية sig
	الاستبـــــــانة ككـــــل.	٤٧	٠,٩٤٩	٠,٩٧٣	٠
١	المخاطر التي تهدد نظـــام المعلومـــات المحاســبي الالكتروني	١٩	٠,٨٩٧	٠,٩٤٦	٠
٢	أسباب حدوث مخاطر نظم المعلومات المحاســبية الالكترونية	١٤	٠,٩٥٤	٠,٩٧٦	٠
٣	إجراءات الحماية المتبعــة ضــد مخــاطر نظــم المعلومات المحاسبية الالكترونية	١٤	٠,٩٤١	٠,٩٦٩	٠

مستوى الدلالة الإحصائية حسب عند α = ٠,٠٥

ومن خلال الجدول السابق يلاحظ أن معامل ثبات الاستبانة بلغ ٠,٩٧٣ ، وهــو قيمــة مرتفعــة وجيدة ودالة إحصائيا عند مستوى دلالة α = ٠,٠١، كما أن معاملات الارتباط والثبات لمجالات الاستبانة الثلاثة أيضاً مرتفعة ومعنوية إحصائيا و هــذا يؤكــد ثبــات الاســتبانة وصــلاحيتها للاستخدام.

٢.طريقة معامل ألفا كرونباخ:

قامت الباحثة بحساب معاملات الفاكرونباخ للاستبانة ككل وكذلك لكل مجال من مجالاتها الثلاثة وذلك كما يلي:

جدول رقم (٧)

معاملات الفاكرونباخ للاستبانة ككل وكذلك لكل مجال من مجالاتها الثلاثة

الرقم	مجالات الاستبانة	عدد الفقرات	معامل ثبات الفاكرون باخ
ـــــ	الاستبـــــــانة ككـــــل.	٤٧	٠,٩٢٣
١	المخاطر التي تهدد نظام المعلومات المحاسبي الالكتروني	١٤	٠,٩٠٣
٢	أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية	١٤	٠,٩٧٥
٣	إجراءات الحماية المتبعة ضد مخاطر نظم المعلومات المحاسبية الالكترونية	١٤	٠,٩٤٩

يتضح من خلال الجدول السابق أن معامل ألفا كرونباخ للاستبانة ككل بلغ ٠,٩٢٣، وهي قيمـــة مرتفعة وجيدة من الناحية الإحصائية في مثل هذه الدراسات، كذلك فان قيم معاملات ألفاكرونباخ في جميع المجالات جيدة من الناحية الإحصائية في مثل هذه الدراسات وتتمتع بدرجة عالية مـــن الثبات.

وبذلك تكون الباحثة قد تأكدت من صدق وثبات استبانه الدراسة المتعلقة بمخاطر نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، مما يجعلها على ثقة تامـــة بـــصحة الاستبانة وصلاحيتها لتحليل النتائج والإجابة على أسئلة الدراسة و اختبار فرضياتها.

ثانيا : وصف العينة

جدول رقم (٨)

المؤهل العلمي

المؤهل العلمي	Frequency	Percent	Valid Percent	Cumulative Percent
ثانوية عامة	3	2.3	2.3	٢,٣
دبلوم	11	8.5	8.5	١٠,٨
بكالوريوس	109	84.5	84.5	95.3
ماجستير	6	4.7	4.7	100.0
Total	129	100.0	100.0	

يتضح من خلال الجدول رقم (٨) أن أغلبية المشاركين في الاستقصاء كانوا من حملـــة شـــهادة البكالوريوس وأن عدد قليل منهم كانوا من حملة شهادة الماجستير وهذا يدل علـــى أن مـــوظفي المصارف لا يسعون لإكمال دراستهم العليا وإنما يكتفون بالدرجة التي توصلوا إليها .

جدول رقم (٩)

المسمى الوظيفي

Cumulative Percent	Valid Percent	Percent	Frequency	المسمى الوظيفي	
11.9	11.9	11.6	15	محاسب	Valid
19	7.1	7.0	9	مراجع لنظم المعلومات الالكترونية	
30.1	11.1	10.9	14	مراجع داخلي	
57.9	27.8	27.1	35	رئيس قسم	
٦٤,٣	٦,٤	٦,٢	٨	مدير	
٧٣,٠	٨,٧	٨,٥	١١	مراقب عام	
100.0	٢٧,٠	٢٦,٤	٣٤	غير ذلك	
	100.0	97.7	126	Total	
		2.3	3	System	Missing
		100.0	129		Total

من خلال الجدول رقم (٩) يمكن القول بأن عينة الدراسة تعد عينة ممثلة للهيكل الـــوظيفي فـــي المصارف العاملة في قطاع غزة .

جدول رقم (١٠)

عدد سنوات الخبرة

Cumulative Percent	Valid Percent	Percent	Frequency	عدد سنوات الخبرة	
27.1	27.1	27.1	35	اقل من 3 سنوات	Valid
40.3	13.2	13.2	17	6 - 3سنوات	
65.9	25.6	25.6	33	10 - 7سنوات	
86.8	20.9	20.9	27	من 15 - 11 سنة	
100.0	13.2	13.2	17	اكثر من 15 سنة	
	100.0	100.0	129	Total	

من خلال الجدول رقم (١٠) نلاحظ أن عدد كبير من المشاركين في الإستقصاء تقل خبرته عن ثلاث سنوات، وهذا راجع إلى زيادة افتتاح مصارف جديدة وفروع جديدة لها وبذلك زيادة الطلب على خريجين جدد في مجال تخصص المحاسبة والمصارف للعمل لدى المصارف الفلسطينية، إضافة إلى أن ٧٧ من المشاركين في الإستقصاء (٥٩,٧% من إجمالي العينة) كانت خبرتهم تزيد عن ٧ سنوات، وهذا يعطي دعم وثقة أكبر للعمل المصرفي، حيث أنه مع زيادة الخبرة تزداد قدرة المصرف على مواجهة المخاطر التي قد يتعرض لها .

جدول رقم (١١)

عدد المحاسبين

Cumulative Percent	Valid Percent	Percent	Frequency	عدد المحاسبين	
47.6	47.6	46.5	60	1 - 5	Valid
68.3	20.6	20.2	26	6 -10	
80.2	11.9	11.6	15	11-15	
86.5	6.3	6.2	8	16-20	
100.0	13.5	13.2	17	اكثر من20	
	100.0	97.7	126	Total	
		2.3	3	System	Missing
		100.0	129		Total

من خلال الجدول رقم (١١) يتضح أن أغلبية المشاركين في الاستقصاء متفقين علـــى أن عـــدد المحاسبين لدى المصارف يتراوح من ١-٥ محاسبين، وهذا يدل على قلة عدد المحاسبين الـــذين يعملون لدى المصار ف .

جدول رقم (١٢)

عدد المتخصصين في نظم المعلومات

Cumulative Percent	Valid Percent	Percent	Frequency	عدد المتخصصين في نظم المعلومات	
76.6	76.6	73.6	95	1-5	Valid
93.5	16.9	16.3	21	6-10	
98.4	4.8	4.7	6	11-15	
100.0	1.6	1.6	2	اكثر من20	
	100.0	96.1	124	Total	
		3.9	5	System	Missing
		100.0	129		Total

يتضح من خلال الجدول رقم (١٢) أن حوالي ٩٥ من المشاركين في الإستقصاء يؤكدون على أن عدد المتخصصين في مجال تكنولوجيا المعلومات يتراوح من ١-٥ ، حيث أن أغلب المصارف لا يوجد لديها سوى موظف واحد مختص بتكنولوجيا المعلومات ومهمته تشغيل

النظام فقط، وهذا راجع إلى أن قسم تكنولوجيا المعلومات عادة يكون في المراكز الرئيسية للمصارف وليس الفروع .

جدول رقم (١٣)

النظام المحاسبي بالبنك

Cumulative Percent	Valid Percent	Percent	Frequency	النظام المحاسبي بالبنك	
.8	.8	.8	1	يدوي	Valid
79.7	78.9	78.3	101	شديد الالية	
100.0	20.3	20.2	26	خليط	
	100.0	99.2	128	Total	
		.8	1	System	Missing
		100.0	129		Total

كما أوضحت الدراسة أن العمل في المصارف يعتمد بنسبة كبيرة على العمل الآلي، وهذا يتطلب توفير حماية أكبر لنظام المعلومات لمواجهة المخاطر التي قد تتعرض لها نظم المعلومات .

اختبار الفرضيات:

لاختبار فرضيات الدراسة فقد تم استخدام اختبار الإشارة اللامعلمي (Sign Test) والذي يعتبر أحد بدائل اختبار t لعينة واحدة المعلمي، إذ انه يستخدم للتحقق من مطابقة وسيط عينة مختارة من مجتمع إحصائي مع وسيط ذلك المجتمع، كما أن اختبار الإشارة لا يعتمد على قيمة الفرق بين الدرجات والوسيط العام وإنما يتعامل فقط مع الإشارات من حيث كونها موجبة أو سالبة أو تأخذ صفراً والذي لا يدخل في المعالجة الإحصائية لأنه يعد محايداً، ولذلك فإن اختبار الإشارة يستخدم لتحديد اتجاه الفروق بين آراء أفراد العينة. (عفانة، ١٩٩٨، ص٦٢-٦٣)

وقد تم إستخدام اختبار الإشارة لاختبار فرضيات الدراسة من خلال اختبار ما إذا كان وسيط آراء أفراد العينة على كل عبارة من عبارات الاستبانة، وكذلك على المجالات ككل يختلف إحصائياً عن وسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (٣) والتي تمثل الرأي (متردد) في المجالين الثاني و الثالث، و الصفة (أكثر من مرة شهريا إلى مرة اسبوعيا) في المجال الأول، من أجل معرفة ما إذا كان هناك موافقة جوهرية ومعنوية احصائياً من أفراد العينة على عبارات الاستبانة أم لا.

وقد تم استخدام اختبار الإشارة اللامعلمي نظراً لأن متغيرات الاستبانة (العبارات) هي متغيرات رتبية وبالتالي لا يناسبها الاختبارات المعلمية كاختبار t وإنما تم الاستعاضة عن ذلك بالاختبارات اللامعلمية لعينة واحدة وأفضلها وأكثرها مناسبة لبيانات الدراسة هو اختبار الإشارة.

<u>مقياس الاستبانة:</u>

المقياس المستخدم في استبانة الدراسة هو مقياس ليكرت الخماسي وقد تم ترميز هذا المقياس كما يلي:

موافق بشدة	موافق	متردد	غير موافق	غير موافق بشدة
٥	٤	٣	٢	١

وبالتالي كلما اقتربنا من الدرجة (٥) ازدادت شدة الموافقة على العبارة في حين تزداد شدة المعارضة كلما اقتربنا من الدرجة (١) أما إذا اقتربنا من الدرجة (٣) فإن ذلك يكون في الاتجاه المتردد. و هذا المقياس استخدم في المجالين الثاني و الثالث، اما في المجال الاول فقد كان المقياس المستخدم حول عدد مرات وقوع مخاطر نظم المعلومات كما يلي:

أقل من مرة واحدة سنوياً	من مرة سنوياً إلى مرة شهرياَ	اكثر من مرة شهرياً إلى مرة اسبوعيا	اكثر من مرة أسبوعيا إلى مرة يومياً	اكثر من مرة يومياً أو بصفة متكررة
٥	٤	٣	٢	١

وبالتالي كلما اقتربنا من الدرجة (٥) فان عدد مرات حدوث المخاطر ينخفض الى درجة انعدام حدوث المخاطر عند الدرجة (٥)، ويزداد عدد مرات حدوث هذه المخاطر كلما اقتربنا من الدرجة (١) أما إذا اقتربنا من الدرجة (٣) فإن ذلك يعني ان عدد مرات حدوث مخاطر نظم المعلومات في البنك متوسطا نسبيا.

١. اختبار الفرضية الرئيسية الأولى والتي تنص على أنه:

(لا تحدث المخاطر التالية بشكل متكرر في المصارف العاملة في قطاع غزة:

أ. مخاطر تتعلق بإدخال البيانات.

ب. مخاطر تتعلق بالتشغيل.

ج. مخاطر تتعلق بالمخرجات.

د. مخاطر تتعلق بالبيئة.)

ولاختبار الفرضية السابقة تم استخدام اختبار الاشارة وذلك لاختبار الفرضية الإحصائية الموجهة التالية:

H0: M <= 3

H1: M > 3

وتشير الفرضية الإحصائية العدمية H0 إلى حدوث مخاطر نظم المعلومات بشكل متكرر في المصارف العاملة في قطاع غزة فيما لو كانت آراء أفراد العينة أقل أو تساوي الدرجة ٣ و التي تمثل الخيار **(أكثر من مرة شهرياً إلى مرة أسبوعيا)**. أما الفرضية البديلة H1 فتشير إلى انعدام أو عدم حدوث مخاطر نظم المعلومات بشكل متكرر في المصارف العاملة في قطاع غزة فيما لو كانت آراء أفراد العينة اكبر من الدرجة ٣ و التي تمثل الخيار **(أكثر من مرة شهرياً إلى مرة أسبوعيا)**. وسيتم اجراء الاختبار الاحصائي و تحديد مستوى المعنوية على أساس ذيل واحد و هو الذيل الأعلى كما هو واضح من الفرضية البديلة السابقة، كما سيتم اختبار الفرضية الإحصائية السابقة لكل نوع من أنواع المخاطر الأربعة التي وردت في الفرضية البحثية السابقة لمعرفة مدى تكرار حدوث هذه المخاطر في المصارف العاملة في قطاع غزة وذلك كما يلي:

جدول رقم (١٤)

نتيجة اختبار الإشارة للمجال الأول الخاص بمخاطر نظم المعلومات المحاسبية الإلكترونية

أنواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	الوسيط العام
مخاطر إدخال البيانات	١	١٢٦	٢	١٢٩	-١١,٠٠٣	٠	٥
مخاطر التشغيل	٠	١٢٦	٣	١٢٩	-١١,١٣٦	٠	٥
مخاطر المخرجات	٠	١٢٦	٣	١٢٩	-١١,١٣٦	٠	٥
مخاطر البيئة	٠	١٢٨	١	١٢٩	-١١,٢٢٥	٠	٥

مستوى المعنوية الإحصائية حسب عند α = ٠,٠٥

تم تحديد الإشارات على أساس (وسيط مقياس الاستبانة (٣) – وسيط آراء افراد العينة)

من خلال الجدول السابق يلاحظ أن قيمة اختبار الإشارة (z) معنوية إحصائياً عند مستوى دلالة (0.05) وهذا يعني أن هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على كل نوع من أنواع مخاطر نظم المعلومات المحاسبية في المصارف العاملة في قطاع غزة ، ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (٣) ويعزز هذه النتيجة أن الوسيط العام لآراء أفراد العينة على كل نوع من أنواع المخاطر الأربعة في الجدول بلغ (٥) وهي تمثل انعدام أو ندرة تكرار هذه المخاطر في المصارف العاملة في قطاع غزة حسب المقياس المستخدم في استبانة الدراسة. وبالتالي نستنتج من ذلك أن مخاطر نظم المعلومات المحاسبية الإلكترونية الأربعة لا تحدث بشكل متكرر . وبناء على ذلك نقبل الفرضية البحثية الأولى و التي تنص على أن مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة لا تحدث بشكل متكرر، وبذلك فإن هذه المخاطر على الرغم من عدم حدوثها بشكل

متكرر فإنها قائمة بحكم طبيعة العمل المصرفي الألي والذي يتطلب توفير اجراءات حماية كافية .

وللوقوف على اراء افراد العينة حول مدى حدوث المخاطر التي تتضمنها كل نوع من انواع المخاطر الاربعة فقد تم إيجاد اختبار الإشارة لكل عبارة على حدة من العبارات التي تضمنها المجال الأول و المتعلق بالمخاطر التي تهدد نظم المعلومات المحاسبية وذلك كما يلي:

جدول رقم (١٥)

نتيجة اختبار الإشارة لكل عبارة من عبارات المجال الأول الخاص بمخاطر نظم المعلومات المحاسبية المصارف الوطنية

م	عبارات المجال الأول (مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	قيمة السو سيط
١	الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.	١٥	٩٣	٢١	١٢٩	-٧,٤٠٩	٠	٤
٢	الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.	٢	١٢٦	١	١٢٩	-١٠,٨٧٢	٠	٥
٣	التدمير غير المتعمد للبيانات بواسطة الموظفين.	٠	١٢٦	٣	١٢٩	-١١,١٣٦	٠	٥
٤	التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.	٠	١٢٦	٣	١٢٩	-١١,١٣٦	٠	٥
٥	المرور (الوصول) غير الشرعي (غير المرخص به) للبيانات / النظام بواسطة الموظفين.	١	١٢٥	٣	١٢٩	-١٠,٩٥٨	٠	٥
٦	المرور غير الشرعي (غير المرخص به) للبيانات / النظام بواسطة أشخاص من خارج المنشأة.	١	١٢٧	١	١٢٩	-١١,٠٤٩	٠	٥
٧	إشراك الموظفين في كلمة السر .	١	١١٩	٩	١٢٩	-١٠,٦٨١	٠	٥

تابع جدول رقم (١٥)

م	عبارات المجال الأول (مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	قيمة الوسيط
٨	إدخال فيروس الكمبيوتر للنظام المحاسبي.	٠	١٢٧	٢	١٢٩	-١١,١٨١	٠	٥
٩	اعتراض وصول البيانات من اجهزة الخوادم إلى اجهزة المستخدمين.	١	١٢١	٧	١٢٩	-١٠,٧٧٤	٠	٥
١٠	طمس أو تدمير بنود معينة من المخرجات.	١	١٢٦	٢	١٢٩	-١١,٠٠٣	٠	٥
١١	خلق مخرجات زائفة / غير صحيحة.	٠	١٢٧	٢	١٢٩	-١١,١٨١	٠	٥
١٢	سرقة البيانات / المعلومات.	١	١٢٥	٣	١٢٩	-١٠,٩٥٨	٠	٥
١٣	عمل نسخ غير مصرح (مرخص) بها من المخرجات.	٢	١٢٤	٣	١٢٩	-١٠,٧٨٠	٠	٥
١٤	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.	٥	١٢٢	٢	١٢٩	-١٠,٢٩٣	٠	٥
١٥	طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.	٣	١٢٠	٦	١٢٩	-١٠,٤٥٩	٠	٥
١٦	المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم / ليس لهم الحق في استلام نسخة منها.	٠	١١٩	١٠	١٢٩	-١٠,٨١٧	٠	٥
١٧	تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.	٣	١١٩	٧	١٢٩	-١٠,٤١٢	٠	٥
١٨	الكوارث الطبيعية مثل الحرائق، الفيضانات أو انقطاع مصدر الطاقة.	٠	١٢٦	٣	١٢٩	-١١,١٣٦	٠	٥
١٩	الكوارث غير الطبيعية والتي هي من صنع الإنسان مثل الحرائق، أو الفيضانات.	٠	١٢٦	٣	١٢٩	-١١,١٣٦	٠	٥

مستوى المعنوية الإحصائية حسب عند $\alpha = 0.05$

تم تحديد الإشارات على أساس (وسيط مقياس الاستبانة (٣) – وسيط آراء افراد العينة)

يلاحظ من خلال الجدول السابق أن قيمة اختبار الإشارة (z) معنوية إحصائياً في كافة العبارات وهذا يعني أن هناك فرق معنوي احصائياً بين وسيط آراء أفراد العينة على كل عبارة ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (٣) كما ان وسيط آراء أفراد العينة في جميع العبارات كان ٥ باستثناء العبارة الاولى فقد كان ٤ و هذا يعني ندرة او انعدام حدوث المخاطر التي يتضمنها الجدول السابق.

٢ - اختبار الفرضية الرئيسية الثانية والتي تنص على أنه:

ترجع اسباب حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة إلى:

أ- اسباب تتعلق بموظفي البنك نتيجة لقلة الخبرة و الوعي والتدريب.

ب- اسباب تتعلق بادارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الاجراءات والادوات الرقابية المطبقة.

لاختبار الفرضية السابقة فقد تم استخدام اختبار الإشارة لمعرفة ما إذا كان هناك فروق معنوية إحصائياً بين وسيط آراء أفراد العينة على المجال الثاني والمتعلق باسباب حدوث مخاطر نظم المعلومات المحاسبية ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (٣) والتي تمثل صفة (متردد) وذلك لتحديد ما إذا كان هناك موافقة جوهرية من قبل أفراد العينة على اسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية و التي تضمنها المجال الثاني بشكل عام ام لا. وفيما يلي نتيجة اختبار الإشارة على المجال الثاني ككل مصنفا في فئتين هما اسباب تتعلق بالموظفين و اسباب تتعلق بادارة المصرف:

حيث تم استخدام اختبار الاشارة لاختبار الفرضية الإحصائية الموجهة التالية:

H0: M <= 3

H1: M > 3

وتشير الفرضية الإحصائية العدمية H0 إلى تردد او اعتراض افراد العينة على اسباب حـــدوث مخاطر نظم المعلومات فيما لو كانت آراء أفراد العينة اقل او تساوي الدرجة ٣ و التـــي تمثـــل الخيار **(متردد)** حسب المقياس المستخدم في استبانة الدراسة وفق الترميز الـــسابق ذكـــره، أمـــا الفرضية البديلة H1 فتشير إلى موافقة افراد العينة على اسباب حدوث مخاطر نظم المعلومـــات المحاسبية فيما لو كانت آراء أفراد العينة اكبر من الدرجة ٣ .

وسيتم اجراء الاختبار الاحصائي و تحديد مستوى المعنوية على اساس ذيل واحد و هـــو الـــذيل الاعلى كما هو واضح من الفرضية البديلة السابقة، وفيما يلي نتيجة الاختبار:

جدول رقم (١٦)

نتيجة اختبار الإشارة للمجال الثاني الخاص بأسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية

انواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	الوسيط العام
اسباب تتعلق بالموظفين	٤٢	٦٦	٢١	١٢٩	٢,٢١٣-	٠,٠٢٧	٤
اسباب تتعلق بإدارة المصرف	٤٦	٧٠	١٣	١٢٩	٢,١٣٥-	٠,٠٣٣	٤

مستوى المعنوية الإحصائية حسب عند α = ٠,٠٥

تم تحديد الإشارات على أساس (وسيط مقياس الاستبانة (٣) – وسيط آراء افراد العينة)

من خلال الجدول السابق يلاحظ أن قيمة اختبار الإشارة (z) معنوية إحصائياً عند مستوى دلالة (0.05) وهذا يعني أن هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على كلا النوعين من اسباب حدوث مخاطر نظم المعلومات المحاسبية ، ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (٣) ويعزز هذه النتيجة أن الوسيط العام لآراء أفراد العينة على كلا النوعين من اسباب حدوث مخاطر نظم المعلومات المحاسبية بلغ (٤) وهي تمثل درجة الموافقة حسب المقياس المستخدم في استبانة الدراسة. وبالتالي نستنتج من ذلك ان افراد العينة يرون ان اسباب حدوث مخاطر نظم المعلومات المحاسبية ترجع لاسباب تتعلق بموظفي المصرف و اسباب تتعلق بادارة المصرف بشكل عام . وبناء على ذلك نقبل الفرضية البحثية الثانية و التي تنص على ان اسباب حدوث مخاطر نظم المعلومات المحاسبية يرجع إلى اسباب تتعلق بموظفي البنك نتيجة لقلة الخبرة و الوعي والتدريب، و اسباب تتعلق بادارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الاجراءات والادوات الرقابية المطبقة.

وللوقوف على اراء افراد العينة حول اسباب حدوث المخاطر الواردة في المجال الثـــاني بـــشكل مفصل فقد تم إيجاد اختبار الإشارة لكل عبارة (سبب) على حدة من العبارات (الاســـباب) التـــي تضمنها المجال الثاني و المتعلق باسباب حدوث المخاطر التي تهدد نظم المعلومات المحاســـبية وذلك كما يلي:

جدول رقم (١٧)

نتيجة اختبار الإشارة لكل عبارة من عبارات المجال الثاني الخاص بأسباب حدوث مخـــاطر نظم المعلومات المحاسبية

م	عبارات المجال الثاني (أسباب حدوث مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	قيمة الوسيط
١	عدم كفاية وفعالية الأدوات والضوابط الرقابية المطبقة في البنك.	٤٠	٧٤	١٥	١٢٩	-٣,٠٩١	0.001	٤
٢	ضعف نظم الرقابة الداخلية في البنك وعدم فعاليتها.	٤٦	٦٥	١٨	١٢٩	-١,٧٠٨	0.044	٤
٣	اشتراك بعض الموظفين في استخدام نفس كلمات السر .	٦٢	٥٥	١٢	١٢٩	-٠,٥٥٥	0.2895	٣
٤	عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات.	٤٤	٧٠	١٥	١٢٩	-٢,٣٤١	0.0095	٤
٥	عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات المحاسبية بالبنك.	٤٣	٧٤	١٢	١٢٩	-٢,٧٧٤	0.003	٤
٦	عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في البنك.	٤٧	٦٩	١٣	١٢٩	-١,٩٥٠	0.0255	٤
٧	ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب الآلي.	٥٣	٦٥	١١	١٢٩	-١,٠١٣	0.1555	٣
٨	عدم وجود سياسات واضحة ومكتوبة فيما يختص بأمن نظم	٤٥	٦٨	١٦	١٢٩	-٢,٠٧٠	0.019	٤

تابع جدول رقم (١٧)

م	عبارات المجال الثاني (أسباب حدوث مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	قيمة الوسيط
	المعلومات المحاسبية في البنك.							
٩	عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في البنك.	٥٠	٧١	٨	١٢٩	-١,٨١٨	**0.0345**	٤
١٠	عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي البنك.	٤٧	٦٩	١٣	١٢٩	-١,٩٥٠	**0.0255**	٤
١١	عدم إلزام الموظفين بأخذ إجازتهم الدورية.	٥٣	٥٤	٢٢	١٢٩	٠	**0.5**	٣
١٢	عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد.	٤٤	٦٠	٢٥	١٢٩	-١,٤٧١	**0.0705**	٣
١٣	عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي البنك.	٣١	٧٣	٢٥	١٢٩	-٤,٠٢٠	**0**	٤
١٤	عدم الوعي الكافي لدى الموظفين بضرورة فحص أي البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.	٣٨	٧٠	٢١	١٢٩	-٢,٩٨٣	**0.0015**	٤

مستوى المعنوية الإحصائية حسب عند $\alpha = 0.05$

تم تحديد الإشارات على أساس (وسيط مقياس الاستبانة (٣) – وسيط آراء افراد العينة)

يلاحظ من خلال الجدول السابق أن قيمة اختبار الإشارة (z) معنوية إحصائياً في كافة العبارات باستثناء العبارات (٣، ٧،١١، ١٢) لم يكن هناك فرق معنوي احصائيا بين وسيط اراء افراد العينة على هذه العبارات الاربعة ووسيط المقياس و هو الدرجة (٣) و يعزز ذلك ان وسيط اراء افراد العينة في هذه العبارات الاربعة بلغ ٣ و هو نفس وسيط المقياس، في حين ان وسيط

اراء افراد العينة في باقي العبارات الاخرى بلغ (٤) و هي تمثل صفة الراي (موافــق) حــسب المقياس المستخدم في الاستبانة و هو اكبر من وسيط مقياس الاستبانة و بشكل معنوي احــصائيا كما يتضح من قيمة(sig) و هي اقل من (٠,٠٥). ونستنتج من ذلك انه عند اجــراء التحليــل المفصل لدرجة موافقة افراد العينة على الاسباب التي تضمنها المجال الثــاني تبــين ان هنــاك اختلاف وتباين بين افراد العينة حول الاسباب التالية:

١. اشتراك بعض الموظفين في استخدام نفس كلمات السر .

٢. ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب الآلي

٣. عدم إلزام الموظفين بأخذ إجازتهم الدورية.

٤. عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد.

٣ - اختبار الفرضية الرئيسية الثالثة والتي تنص على أنه:

(لا توجد اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة).

لاختبار الفرضية السابقة فقد تم استخدام اختبار الإشارة لمعرفة ما إذا كان هناك فروق معنوية إحصائياً بين وسيط آراء أفراد العينة على المجال الثالث والمتعلق باجراءات الحماية لمواجهة مخاطر نظم المعلومات المحاسبية ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (٣) والتي تمثل صفة (متردد) وذلك لتحديد ما إذا كان هناك موافقة جوهرية من قبل أفراد العينة على اتباع اجراءات الحماية الواردة في المجال الثالث ام لا. وفيما يلي نتيجة اختبار الإشارة على المجال الثالث ككل.

ويختبر اختبار الإشارة الفرضية الإحصائية الموجهة التالية:

H0: M <= 3

H1: M > 3

وتشير الفرضية الإحصائية العدمية H0 إلى تردد او عدم موافقة افراد العينة على اجراءات الحماية المذكورة، فيما لو كانت آراء أفراد العينة اقل او تساوي الدرجة ٣، وهذا يعني عدم توفر اجراءات الحماية في المصارف. أما الفرضية البديلة H1 فتشير إلى موافقة افراد العينة على وجود اجراءات الحماية في مصارفهم فيما لو كانت آراء أفراد العينة اكبر من الدرجة ٣ .

وسيتم اجراء الاختبار الاحصائي و تحديد مستوى المعنوية على اساس ذيل واحد و هو الذيل الاعلى كما هو واضح من الفرضية البديلة السابقة، وفيما يلي نتيجة الاختبار:

جدول رقم (١٨)

نتيجة اختبار الإشارة للمجال الثالث الخاص باجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة

انواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	الوسيط العام
إجراءات الحماية المتبعة لمواجهة المخاطر التي تهدد نظم المعلومات المحاسبية	٢	١١٩	٨	١٢٩	-١٠,٥٤٥	٠	٥

مستوى المعنوية الإحصائية حسب عند α = ٠,٠٥

تم تحديد الإشارات على أساس (وسيط مقياس الاستبانة (٣) – وسيط آراء افراد العينة)

من خلال الجدول السابق يلاحظ أن قيمة اختبار الإشارة (z) معنوية إحصائياً عند مستوى دلالة (0.05) وهذا يعني أن هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على اجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية ، ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة (٣) ويعزز هذه النتيجة أن الوسيط العام لآراء أفراد العينة بلغ (٥) وهي تمثل درجة الموافقة بشدة حسب المقياس المستخدم في استبانة الدراسة. وبالتالي نستنتج من ذلك ان افراد العينة يرون ان المصارف التي يعملون فيها تتبع اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية.

وبناء على ذلك نرفض الفرضية البحثية الثالثة و التي تنص على انه لا توجد اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة. وللوقوف على اراء افراد العينة حول طبيعة اجراءات الحماية التي تتبعها المصارف

العاملة في قطاع غزة بشكل تفصيلي فقد تم إيجاد اختبار الإشارة لكل عبارة علـــى حـــدة مـــن العبارات التي تضمنها المجال الثالث و المتعلق باجراءات الحماية المتبعة لمواجهـــة المخـــاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية وذلك كما يلي:

جدول رقم (١٩)

نتيجة اختبار الإشارة لكل عبارة من عبارات المجال الثالث الخاص باجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية

م	عبارات المجال الثالث (**اجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية** الإلكترونية)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	قيمة الوسيط
١	تقوم إدارة البنك بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات.	٣	١٢٢	٤	١٢٩	-١٠,٥٥٤	0	٥
٢	تتعهد إدارة البنك العليا لتطبيق أمن المعلومات.	٣	١١٧	٩	١٢٩	-١٠,٣١٥	٠	٥
٣	تتابع إدارة البنك موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة.	٥	١١٦	٨	١٢٩	-١٠	٠	٥
٤	تقوم إدارة البنك بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد.	١	١١٢	١٦	١٢٩	-١٠,٣٤٨	٠	٥
٥	تقوم إدارة البنك بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن الرجوع إليها عند الضرورة.	٣	١٢٠	٦	١٢٩	-١٠,٤٥٩	٠	٥
٦	تطبق إدارة البنك أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد.	٠	١٢٣	٦	١٢٩	-١١	٠	٥
٧	تقوم إدارة البنك بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة.	٥	١٠٥	١٩	١٢٩	-٩,٤٣٩	٠	٤

تابع جدول رقم (١٩)

م	عبارات المجال الثالث (**اجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية** الإلكترونية)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية sig	قيمة الوسيط
٨	تقوم إدارة البنك بوضع سياسات خاصة بأمن المعلومات تشمل اختيار التقنية المناسبة، والإجراءات اللازمة لجعل هذه التقنية فعالة .	١	١١٦	١٢	١٢٩	-١٠,٥٣٩	٠	٥
٩	تقوم إدارة البنك بتركيب طرق الحماية التقنية مثل جدران النار (Firewalls) ومضادات الفيروسات وغيرها.	٥	١١٣	١١	١٢٩	-٩,٨٥٠	٠	٥
١٠	تقوم إدارة البنك بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا.	٥	١١٤	١٠	١٢٩	-٩,٩٠	٠	٥
١١	تقوم إدارة البنك بفحص طرق الحماية.	٣	١١٥	١١	١٢٩	-١٠,٢١٨	٠	٥
١٢	تقوم إدارة البنك باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق.	٥	١٠٠	٢٤	١٢٩	-٩,١٧٣	٠	٤
١٣	تقوم إدارة البنك بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه.	٢	١٠٩	١٨	١٢٩	-١٠,٠٦١	٠	٥
١٤	تستفيد ادارة البنك من خبرة البنوك العالمية في مجال امن المعلومات	٧	١١١	١١	١٢٩	-٩,٤٨٢	٠	٤

مستوى المعنوية الإحصائية حسب عند $\alpha = 0.05$

تم تحديد الإشارات على أساس (وسيط مقياس الاستبانة (٣) – وسيط آراء افراد العينة)

يلاحظ من خلال الجدول السابق أن قيمة اختبار الإشارة (z) معنوية إحصائياً في كافة العبارات وهذا يعني أن هناك فرق معنوي احصائياً بين وسيط آراء أفراد العينة على كل عبارة ووسيط

المقياس المستخدم في استبانة الدراسة وهو الدرجة (٣) كما ان وسيط آراء أفـــراد العينـــة فـــي جميع العبارات كان ٥ باستثناء العبارات (٧، ١٢، ١٤) فقد كان ٤ و هذا يعني ان المـــصارف العاملة في قطاع غزة تتبع اجراءات الحماية الواردة في الجدول السابق حسب اراء افراد العينة.

الفصل السادس
النتائج والتوصيات

الفصل السادس

النتائج والتوصيات

أولا : النتائج

لقد توصلت هذه الدراسة إلى مجموعة من النتائج والتي تعتبر في مجملها خلاصة التحليلات والمناقشات بالإضافة إلى النتائج الخاصة باختبار الفرضيات .

١. أوضحت الدراسة قلة عدد موظفي تكنولوجيا المعلومات في المصارف حيث يعتمد الفروع على موظف واحد مهمته تشغيل أنظمة الحاسوب بينما الموظفين المختصين يكون مكانهم في المراكز الرئيسية للفروع وغالبا ما توجد في الضفة الغربية .

٢. عدم اتصال شبكة المصارف بشبكة الانترنت وبالتالي عدم تمكن العملاء من اجراء بعض الخدمات المصرفية من خلال الانترنت .

٣. الأنظمة المرتبطة مع شبكة الإنترنت أكثر عرضة للفيروسات من الأنظمة غير المرتبطة مع شبكة الإنترنت .

٤. اعتماد المصارف في عملها بشكل كبير على النظام الآلي وبالتالي توفير الوقت والجهد في العمل .

٥. تعتبر مخاطر الإدخال غير المتعمد واشتراك الموظفين في كلمة السر وتوجيه البيانات والمعلومات إلى أشخاص غير مصرح لهم بذلك، قد تحدث أكثر من مرة شهريا إلى مرة أسبوعيا .

٦. الإدارة الجيدة تستطيع أن تقلل أوتحد من حدوث المخاطر التي تواجه نظم المعلومات المحاسبية لدى المصارف .

٧. تطبيق إجراءات أمن النظم المعلوماتية يقلل من إمكانية حدوث مخاطر نظم المعلومات

المحاسبية .

٨. تم قبول الفرضية الأولى وهي عدم حدوث مخاطر نظم المعلومات المحاسبية في المصارف العاملة في قطاع غزة، حيث أوضحت الدراسة أن تلك المخاطر لا تحدث بشكل متكرر في المصارف العاملة في قطاع غزة .

٩. تم قبول الفرضية الثانية وهي أن حدوث مخاطر نظم المعلومات المحاسبية الالكترونية ترجع إلى أسباب تتعلق بموظفي البنك نتيجة قلة الخبرة والوعي والتدريب، اضافة إلى أسباب تتعلق بإدارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الاجراءات والأدوات الرقابية المطبقة لدى المصرف.

١٠. اتضح أيضا أن المصارف العاملة في قطاع غزة تتبع اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية، وبالتالي يتم رفض الفرضية الثالثة والتي تنص على أنه لا توجد اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة.

ثانيا : التوصيات

بعد استعراض نتائج الدراسة فإنه يمكننا الخروج بمجموعة من التوصيات وهي كالتالي :

١. من الضروري أن تدعم الادارة العليا للمصارف أمن المعلومات لديها وتعمل على إنشاء قسم خاص بتكنولوجيا المعلومات في كافة المصارف وتوفير كادر متخصص في تكنولوجيا المعلومات بحيث يكون له مندوبين في الفروع ذوي خبرة وكفاءة عالية من أجل العمل على حماية أمن نظم المعلومات المحاسبية لدى المصارف .

٢. العمل على تطوير شبكة المصارف وربطها بشبكة الانترنت من أجل تمكين العملاء من تنفيذ الخدمات الخاصة بهم بسهولة وبسرعة دون أي تأخير ولكن مع احكام الرقابة المصرفية على شبكة المصرف ووضع قيود تحد من محاولة اختراق شبكة المصرف والحصول على أي معلومات غير مرخص لهم بالحصول عليها.

٣. نوصي المصارف بإنشاء قسم خاص بتكنولوجيا المعلومات في كافة المصارف بحيث يكون له مندوبين في الفروع ذوي خبرة وكفاءة عالية من أجل العمل على حماية أمن معلومات المصرف.

٤. وضع اجراءات تضمن استمرارية عمل وجاهزية نظم المعلومات للعمل في حالة الأزمات من خلال استخدام تجهيزات منيعة أو مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها والحد من وقوعها .

٥. العمل على تعمية أو تشفير المعلومات عند الحفظ والنقل والتخزين على مختلف الوسائط حتى لا يتمكن أحد من اختراقها .

٦. العمل على توعية المؤسسات العامة والخاصة بأهمية أمن النظم المعلوماتية وضرورة

وضع سياسة أمنية لمنظوماتها المعلوماتية .

٧. وضع ضوابط أمن ورقابة المعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أو اتصالات سلكية ولاسلكية والإنترنت والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية .

٨. ضرورة وجود خطة حماية أمنية شاملة والتي تنعكس في انخفاض النفقات الناتجة عن توظيف الحلول الجزئية للأمن

٩. العمل على توضيح كافة الممارسات الأمنية المقبولة في النظم المعلوماتية على كافة مستويات الإدارة، ومن ثم رفع حجم الثقة لدى إدارة المؤسسات بفاعلة إجراءات الحماية وإمكانية قياسها .

١٠. الإشراف على حسن تطبيق إجراءات أمن النظم المعلوماتية .

المراجع

المراجع

أولا/ المراجع العربية

- البكري سونيا، (٢٠٠٤)، "نظم المعلومات الادارية، المفـاهيم الأساسـية"، الـدار الجامعيـة، الاسكندرية.
- تنتوش محمود، (١٩٩٨)، "نظم المعلومات في المحاسبة والمراجعة المهنيـة (دور الحاسـوب في الادارة والتشغيل)، دار الجيل، بيروت، ط١.
- جمعة أحمد، العربيد عصام، الزعبي زياد، (٢٠٠٣)، "نظـم المعلومـات المحاسـبية مـدخل تطبيقي معاصر"، دار المناهج للنشر والتوزيع، ط١.
- حفناوي محمد، (٢٠٠١)، نظم المعلومات المحاسبية، دار وائل للنشر عمان، ط١.
- دبيان عبدالمقصود، (١٩٩٧)، "مدخل إلى نظم المعلومات المحاسبية"، الدار الجامعيـة للنـشر والتوزيع، الاسكندرية.
- الدهراوي كمال الدين، (٢٠٠٣)، "مدخل معاصر في نظـم المعلومـات المحاسـبية"، الـدار الجامعية للنشر والتوزيع، مصر، ط٢.
- الدهراوي كمال الدين، محمد سمير، (٢٠٠٢)، "نظم المعلومـات المحاسـبية"، دار الجامعـة الجديدة، ط٢، الاسكندرية.
- الراوي حكمت، (١٩٩٩)، "نظم المعلومات المحاسبية والمنظمة (نظري مع حالات دراسية)"، مكتبة دار الثقافة للنشر والتوزيع، عمان، ط١.
- الرزق صالح، آل آدم يوحنا، (٢٠٠٠)، "مبادئ المحاسبة (أسس وأصول علمية وعملية)"، دار الحامد للنشر والتوزيع، عمان، ط١.

- سلام حلمي وأبو طالب أحمد وعبده عبدالعاطي، (٢٠٠٠)، "أساسيات نظم المعلومات المحاسبية"، جامعة القاهرة/ ط١.
- سلطان ابراهيم، (٢٠٠٠)، "نظم المعلومات الادارية (مدخل النظم)"، الدار الجامعية للطبع والنشر والتوزيع، الاسكندرية.
- الصباغ عماد، (٢٠٠٠)، مدخل لتحليل وتصميم نظم معلومات الأعمال"، الدار العلمية الدولية ودار الثقافة للنشر والتوزيع، عمان، ط١.
- طه طارق، (٢٠٠٠)، "مقدمة في نظم المعلومات الادارية والحاسبات الآلية"، منشأة المعارف للنشر والتوزيع، الاسكندرية، ط٣.
- عاشور يوسف، (٢٠٠٣)، "آفاق النظام المصرفي الفلسطيني"، مطبعة الرنتيسي للطباعة والنشر، غزة، فلسطين، ط١ .
- عفانة عزو، (١٩٩٨)، "الإحصاء التربوي: الجزء الثاني، الإحصاء الاستدلالي"، غزة، فلسطين، ط١.
- عوض منصور، (١٩٨٩)، "مقدمة في تحليل النظم"، دار الفرقان للنشروالتوزيع، عمان، الأردن .
- العيسى ياسين، (٢٠٠٣)، أصول المحاسبة الحديثة (الجزء الأول)، دار الشروق للنشر والتوزيع، عمان الأردن، ط١.
- قاسم عبدالرزاق، (٢٠٠٣)، "نظم المعلومات المحاسبية الحاسوبية"، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، ط١.
- كراجة عبد الحليم، (٢٠٠٠)، "محاسبة البنوك"، دار صفاء للطباعة والنشر والتوزيع، عمان،

ط١.

- موسكوف ستيفن، سيمكن مارك، (١٩٨٩)، "نظم المعلومات المحاسبية لاتخاذ القرارات (مفاهيم تطبيقات)"، دار المريخ للنشر.

ثانيا/ المراجع الأجنبية

- Abu-Musa, Ahmad A. (2001), "Evaluating The Security of Computerized Accounting Information Systems: An Empirical Study on Egyptian Banking Industry", PhD. Thesis, Aberdeen University, UK.
- Abu-Musa, Ahmad A. (2004), "Important Threats to Computerized Accounting Information Systems: An empirical Study on Saudi Organizations" Pubic Administration, A Professional Quarterly Journal Published by The Institute of Public Administration Riyadh, Saudi Arabia, (Vol. 44, No. 3), pp. 1-65.
- Cashing, B "Accounting Information Systems and Business Organization" Addison, Wesley Publication Co, Call. , 1974)
- Davis, Charles E. (1997), "An Assessment of Accounting Information Security", The CPA Journal, New York (Vol. 67, Iss. 3), pp. 28 - 34.
- Dhillon, G. (1999), "Managing and controlling computer misuse", Information Management & Computer Security, (Vol. 7, Number 4), PP. 171-175.
- Janvrin Diane J., "Using Role Play to Examine Internal Control and Fraud Detection Concepts", Journal of Information Systems,

Vol. 17, No. 2 Fall 2003 pp. 17.39

- Jessup Leonard and Valacich, Joseph (2003), " Information Systems Today", Isted., Prentice hall.
- John Cox, "Survey: Security Remains Job, "Network World, May 20, 2002, www.nwfusion.com /news/2002/0520nw500.htm"
- Kohler, E "A dictionary for Accountants", Englewood Cliff, N.J: Prentice Hall, Inc, 1975 P8.
- Laudon K. C. and Laudon J. P. (2006), "Management Information Systems", 9th ed., Prentice Hall.
- Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding", MIS Quarterly, (June), pp. 173 - 186.
- Mcnurlin B. C. and Sprague R. H. (2006), "Information Systems Management in Prictice:, 7th ed., Prentice Hall.
- Moscovo & et. Al., "Core Concepts of Accounting Information Systems", Johnwiley and sons Inc, 1997.
- Obrien, J, Management Information Systems: Managing Information Technology in the Network Enterprise, Northern Arizona University.
- Panko, Raymond R (2004), Corporate Computer and Network Security, Prentice Hall, Upper Saddle, New Jersey.
- Richard I rwin Ind 1996. Introduction to Information Systems An end user Enterprise Perspective, Northern Arizona University

- Robinson Aleonard and Davis R James "Accounting Information Systems, Acycle Approach Harper and Row Publishers,

Newyourk, 1985.

- Ryan, S. D. and B. Bordoloi (1997), “Evaluating Security Threats in Mainframe and Client / Server Environments”, Information & Management, (Vol. 32, Iss. 3), pp. 137 - 142.
- Schoderbk, charles and other "Management Systems",(Business Publication, Dallas, 1980)
- Siponen, M. T. (2000), “A conceptual Foundation for Organizational Information Security Awareness”, Information Management and Computer Security, Bradford, (Vol. 8, Iss. 8), PP. 31- 44.
- Volonino, Linda and Stephen R. Robinson (2004). "Principles and Practices of Information Security". Upper Saddle River, N.J.: Prentice Hall.
- Whitman Michael E. (2003), "Enemy at the Gate: Threats to Information Security", Communication of the ACM, (Vol. 46, Iss. 8), pp. 91-95.

ثالثا : المواقع الإلكترونية

- Carey Allan (2004), “Information Security Global Workforce Study”, http://www.sis.smu.edu.sg/news_events/news/(ISC)2IDC%20study.pdf, (Accessed, September 2005).
- GAO (United States General Accounting Office) (1999),“Accounting Information Systems Accounting Dissertation:2000”, http://www.gao.gov/special.pubs/ai00033.pdf, (Accessed October 2005).
- RSA Security Inc, "A guide to Security Technologies"., Bedford, MA01730,1999;http://www.rsasecurity.com

- تـــارة أنـــس، زبيبـــي مـــروان، الرقميـــات، "أمـن المعلومـات والـنظم المعلوماتيـة"، (www.alrakameiat.com) ، تم دخول الموقع pm١٢:٠ تاريخ ٢٠٠٦/٦/١ .
- الدلاهمة سليمان، "مبادئ المحاســبة (١)" (www.qudsopenun.com/arabic/sumaries) تم دخول الموقع pm ١:٥ تاريخ ٢٠٠٦/٥/١١
- الشبكة القانونية العربية، أمن المعلومات ماهيتها وعناصرها واستراتيجياتها (www.arablaw.org/information%20security.htm)، تم دخول الموقع ١٢,٥ pm تاريخ ٢٠٠٦/٣/٥ .
- الغتبر خالد، "أمن المعلومات والمرونة"، جريدة العرب الإقتصادية الدولية الإلكترونية، (http://aleqt.com/news.php?do1) تم دخول الموقع pm ١٢:٥ تاريخ ٢٠٠٦/٦/١ .
- ميلاد عبد المجيد، "نشر الطمأنينة وبناء الثقة في العصر الرقمي"، /articles (www.abdelmajid-miled.com) تم دخول الموقع am١١ تاريخ ٢٠٠٦/٥/٨ .
- وحدة أمن المعلومات، "أمن المعلومات"، (www.ksu.edu.sa/security/ahdaf.html)، تـم دخول الموقع am١١:١٠ تاريخ ٢٠٠٦/5/8 .

المـــــلاحــق

ملحق (١)

الاستبيان

مخاطر نظم المعلومات المحاسبية الإلكترونية:
دراسة تطبيقية على المصارف العاملة في قطاع غزة

السيد الفاضل / السيدة الفاضلة

يهدف هذا الاستبيان إلى التعرف عل آرائكم فيما يختص بالمخاطر الهامة التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في المصارف العاملة في قطاع غزة ، لذلك نرجو منكم التكرم بمليء بيانات الاستبيان المرفق ،ونود أن نؤكد على أن البيانات التي سوف يتم تجميعها في هذا الاستبيان سوف تكون سرية ولن تستخدم إلا في أغراض البحث العلمي ، ونظراً لأن إجاباتكم سوف تكون على قدر عالٍ من الأهمية بالنسبة لهذا البحث ،لذا نرجو التكرم بمراعاة الدقة في استيفاء بيانات هذا الاستبيان ونشكر لكم مشاركتكم في هذا الاستبيان .

الباحثة

الطالبة حرية الشريف

ماجستير محاسبة وتمويل

الجامعة الإسلامية - غزة

معلومات عامة

من فضلك ضع علامة " Ö" على المربع الذي تختاره لكل سؤال على حدة

١- ما المؤهل العلمي لك ؟

o ثانوية عامة
o دبلوم
o بكالوريوس
o ماجستير
o دكتوراة

التخصص:.....

٢- هل تعمل حالياً في:-

o بنك تجاري
o بنك إسلامي

٣- ما هو المسمى الوظيفي لعملك الحالي بالبنك؟

o محاسب مالي
o مراجع لنظم المعلومات الإلكترونية
o مراجع داخلي
o رئيس قسم
o مراقب عام
o مدير
o غير ذلك حدد .....

٤- كم عدد سنوات الخبرة التي قضيتها في مزاولة عملك الحالي؟

o أقل من ٣ سنوات
o من ٣ سنوات - ٦
o من ٧ سنوات - ١٠
o من ١١ سنة - ١٥
o أكثر من ١٥ سنة

5- كم عدد المحاسبين الذين يعملون حالياً بالبنك؟

o ١ - ٥
o ٦ - ١٠
o ١١ - ١٥
o ١٦ - ٢٠
o أكثر من ٢٠

6- كم عدد المتخصصين في نظم المعلومات الذين يعملون حالياً بالبنك؟

o ١ - ٥
o ٦ - ١٠

o ١١ - ١٥ o ١٦ - ٢٠

o أكثر من ٢٠

٧- النظام المحاسبي في البنك الذي تعمل فيه:

o يدوي لا يستخدم الحاسبات الآلية.

o يعتمد بدرجة كبيرة على الكمبيوتر (شديد الآلية).

o خليط من العمل اليدوي والتشغيل الإلكتروني.

٨-هل عانى البنك من خسائر مالية نتيجة خلل في أمن المعلومات ؟

o نعم o لا

٩- إذا كانت الإجابة على السؤال السابق بنعم فما هو السبب :

o تصرفات غير أمينة من قبل موظفي البنك

o تصرفات غير أمينة من قبل أطراف خارجية (مثل القرصنة)

o تصرفات غير أمينة سواء داخلية أو خارجية.

١٠- هل شبكة البنك متصلة بشبكة الإنترنت

o نعم o لا

١١- إذا كانت الإجابة على السؤال رقم (١٠) بنعم فهل يستطيع جميع الموظفين الدخول إلى شبكة البنك عبر شبكة الإنترنت خلال فترة الدوام

o جميع الموظفين o بعض الموظفين o لا أحد

١٢- إذا كانت الإجابة على السؤال رقم (١٠) بنعم فهل يستطيع عملاء البنك الدخول إلى موقع البنك من خلال شبكة الإنترنت والاطلاع على كشف

حساباتهم وإجراء بعض العمليات المالية البسيطة مثل تحويل مبلغ حساب إلى آخر خاص بالعميل .

o نعم o لا

إذا كانت الإجابة على السؤال رقم (١٢) بنعم فالرجاء الإجابة على الأسئلة التالية (١٣،١٤)

ما هي نسبة العملاء الذين يدخلون إلى موقع البنك عبر شبكة الإنترنت.

o أقل من ١٠% o من ١٠%-٣٠%

o من ٣١%-٥٠% o من ٥١%-٧٠%

o أكثر من ٧٠%

هل يؤثر دخول هؤلاء العملاء إلى موقع البنك على أمن المعلومات لديكم.

o يؤثر بدرجة كبيرة جدا o يؤثر بدرجة كبيرة

o يؤثر بدرجة متوسطة o يؤثر بدرجة ضعيفة

o يؤثر بدرجة ضعيفة جدا

تهديدات أمن المعلومات

من فضلك ضع علامة " Ö" على المربع الذي تختاره في عمود التكرارات المناسب لكل تهديد على حدة

مخاطر أمن نظام المعلومات المحاسبية الإلكترونية	أقل من مرة واحدة سنوياً	من مرة سنوياً إلى مرة شهرياَ	أكثر من مرة شهرياً إلى مرة أسبوعيا	أكثر من مرة أسبوعيا إلى مرة يومياً	أكثر من مرة يومياً أو بصفة متكررة
١. الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.					
٢. الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.					
٣. التدمير غير المتعمد للبيانات بواسطة الموظفين.					
٤. التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.					
٥. المرور (الوصول) غير الشرعي (غير المرخص به) للبيانات / النظام بواسطة الموظفين.					
٦. المرور غير الشرعي (غير المرخص به) للبيانات / النظام بواسطة أشخاص من خارج المنشأة.					
٧. إشراك الموظفين في كلمة السر .					
٨. إدخال فيروس الكمبيوتر للنظام المحاسبي.					
٩. اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين .					
١٠.طمس أو تدمير بنود معينة من المخرجات.					
١١.خلق مخرجات زائفة / غير صحيحة.					
١٢.سرقة البيانات / المعلومات.					
١٣.عمل نسخ غير مصرح (مرخص) بها من المخرجات.					
١٤.الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على					

الورق.					
١٥.طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.					
١٦.المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم / ليس لهم الحق في استلامها نسخة منها.					
١٧.تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.					
١٨.الكوارث الطبيعية مثل الحرائق، الفيضانات أو انقطاع مصدر الطاقة.					
١٩.الكوارث غير الطبيعية والتي هي من صنع الإنسان مثل الحرائق، أو الفيضانات.					

من فضلك ضع علامة " Ö" على المربع الذي تختاره في العمود المناسب لكل سبب على حدة

أسباب حدوث مخاطر أمن نظم المعلومات المحاسبية	موافق بشدة	موافق	متردد	معارض	معارض بشدة
١. عدم كفاية وفعالية الأدوات والضوابط الرقابية المطبقة في البنك.					
٢. ضعف نظم الرقابة الداخلية في البنك وعدم فعاليتها.					
٣. اشتراك بعض الموظفين في استخدام نفس كلمات السر .					
٤. عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات.					
٥. عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المعلومات المحاسبية بالبنك.					
٦. عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في البنك.					

٧. ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب الآلي.					
٨. عدم وجود سياسات واضحة ومكتوبة فيما يختص بأمن نظم المعلومات المحاسبية في البنك.					
٩. عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في البنك.					
١٠.عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي البنك.					
١١.عدم إلزام الموظفين بأخذ إجازتهم الدورية.					
١٢.عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد.					
١٣.عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي البنك.					
١٤.عدم الوعي الكافي لدى الموظفين بضرورة فحص أي البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.					

من فضلك ضع علامة " Ö" على المربع الذي تختاره في العمود المناسب لكل إجراء على حدة

إجراءات الحماية المتبعة ضد مخاطر أمن نظم المعلومات المحاسبية	موافق بشدة	موافق	متردد	معارض	معارض بشدة
١. تقوم إدارة البنك بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات.					
٢. تتعهد إدارة البنك العليا بتطبيق أمن المعلومات.					
٣. تتابع إدارة البنك موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة.					
٤. تقوم إدارة البنك بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد.					
٥. تقوم إدارة البنك بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات يمكن الرجوع إليها عند الضرورة.					
٦. تطبق إدارة البنك أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد.					
٧. تقوم إدارة البنك بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة.					
٨. تقوم إدارة البنك بوضع سياسات خاصة بأمن المعلومات فيما يتعلق باختيار التقنية المناسبة وآلية العمل بها.					
٩. تقوم إدارة البنك بتركيب طرق الحماية التقنية مثل جدران النار (Firewalls) ومضادات الفيروسات وغيرها.					
١٠.تقوم إدارة البنك بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة التكنولوجيا.					
١١.تقوم إدارة البنك بفحص طرق الحماية ودراسة مدى فعاليتها.					
١٢.تقوم إدارة البنك باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق.					

١٣.تقوم إدارة البنك بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه.					
١٤.تستفيد إدارة البنك من خبرة البنوك العالمية في مجال أمن المعلومات.					

ملحق (٢)

قائمة بأسماء محكمي الاستبانة

الإسم	المسمى الوظيفي
الدكتور علي شاهين	مساعد النائب الإداري للشئون الإدارية والمالية
الدكتور نبيل الحويحي	عميد كلية تكنولوجيا المعلومات
الدكتور أيمن أبوسمرة	أستاذ مساعد في كلية الهندسة/ قسم هندسة الحاسوب
الدكتور نافذ بركات	رئيس قسم وحدة الدراسات التجارية