مخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية في المملكة الأردنية الهاشمية

ريم عقاب خصاونة (*)

(*)ريم عقاب خصاونة: مدرس بجامعة البلقاء التطبيقية كلية الحصن ،ومدقق سابق بالبنك الأهلـــى ولهـــا اهتمامات بحثية فى التدقيق ونظم المعلومات.

ملخص

تهدف هذا الدراسة إلى التعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في الوحدات الحكومية الأردنية ،وبناء على ذلك تم استخلاص بعض النتائج التي أسهمت في التعرف على أهم المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في الوحدات الحكومية الأردنية ومن أهمها إن مخاطر نظم المعلومات المحاسبية المحوسبة، و إن كانت تحدث لدى الوحدات الحكومية الأردنية إلا أنها تكرر بشكل غير كبير،حدوث مخاطر نظم المعلومات المحاسبية الالكترونية ترجع إلى أسباب تتعلق بموظفي الوحدات الحكومية الأردنية نتيجة قلة الخبر ة، الوعي والتدريب، إضافة إلى أسباب تتعلق بإدارة الوحدات الحكومية الأردنية ؛ نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى الوحدات الحكومية الأردنية إن الوحدات الحكومية الأردنية تتبع إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية .وعلى ضوء نتائج الدراسة تم التوصل إلى مجموعة من التوصيات من أهمها يجب أن تدعم سياسات أمن معلومات لدى الوحدات الحكومية الأردنية أن تعمل على إنشاء قسم خاص بتكنولوجيا المعلومات في كافة مديرية التابع للوزارات و المؤسسات ،وضرورة وضع إجراءات تضمن استمرارية عمل وجاهزة نظم المعلومات للعمل في حالة الأزمات ،و وضع ضوابط أمن ورقابة للمعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أم اتصالات سلكية ولاسلكية والإنترنت والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية.

Abstrac

This study aimed to identify the risks faced by the accounting information systems, electronic units and the Jordanian government and Aspbha researcher has access to the previous studies and research in this area has, and then prepared a special questionnaire has been distributed to ministries and government institutions and then the data were analyzed that has been collected on the basis of this was to draw some conclusions that have contributed to the identification of the main risks faced by the accounting information systems, electronic units of government of Jordan is the most important of the risks of computerized accounting information systems, and that there were units of the Jordanian government, however, it repeats in a large non - , a risk of electronic accounting information systems due to the reasons of the staff of the Jordanian government units because of lack of added H, awareness and training, in addition to reasons relating to the management of the Jordanian government units; result of the absence of clear policies and written procedures, and the weakness of the regulatory tools applied to government units that the Jordanian government units Jordan procedures adequate protection to counter the risks of electronic accounting information systems. In the light of the results of the study was to produce a set of recommendations, the most important of which must be supported by information security policies of the Jordanian government units to work on the establishment of a special section of information technology in all of the Directorate of the ministries and institutions, and the need to develop procedures to ensure continuity in the work of information systems and ready for action in the case of crises, and controls the security and control of information in circulation in all its forms, whether paper or telecommunications, the Internet and work to enact the legislation necessary to the security of information systems and information network

المقدمة

في السنوات الأخيرة تزايدت أهمية استخدام تقنية المعلومات والاتصالات داخل الجهات الحكومية وبصفة خاصة عقب الاستخدام الموسع للإنترنت والانترنت داخل تلك الجهات والهيئات حيث عملت هذه التقنية على زيادة حجم البيانات والمعلومات التي يجري معالجتها ، كما أنها أثرت بشكل عميق في مجالات الضوابط الرقابية. وتعتبر تقنية المعلومات والاتصالات هي المكون الرئيسي لإستراتيجيات عمل الجهات الحكومية والأنشطة الرئيسة في مجال معالجة البيانات، لذلك فقد ازدادت إدارة مخاطر تقنية المعلومات والاتصالات داخل تلك الجهات وأصبحت تشكل الآن جزءاً هاماً من الإشراف الحكومي . وبالتالي تعتبر الإدارة الفاعلة والمؤثرة لتقنية المعلومات والاتصالات حيوية لنجاح تلك الجهات في تحقيق أهدافها.

ومع تطور تقنية الحاسب الآلي فقد تزايد اعتماد الجهات الحكومية على أنظمة المعلومات التي تستخدم أجهزة الحاسب الآلي لأداء عملياتها التشغيلية وتقديم خدماتها ومعالجة البيانات الهامة وحفظها وإصدار التقارير بشأنها، كما اتسع أيضاً مجال اختراق أنظمة تقنية المعلومات والاتصالات وازدادت التهديدات التي يتعين مواجهتها بفاعلية وكفاءة. وبالنتيجة تعتبر سرية بيانات الحاسب الآلي وموضوعيتها و جاهزيتها ودرجة الاعتماد عليها وعلى الأجهزة التي يتم بها معالجة تلك البيانات وحفظها وإصدار التقارير بشأنها تعتبر من المخاوف الرئيسية التي ينبغي مراعاتها أثناء الرقابة،.

ومن هنا تظهر مسئولية جديدة و كبيرة أمام إدارة نظم المعلومات في الوحدات الحكومية وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل تلك النظم بشكل صحيح، مع التخطيط الدقيق لمواجهة جميع الأخطار التي يمكن أن تؤدي إلى تعطلها أو توقفها عن العمل، وفي حال حدوث ذلك، التمكن من إعادة تشغيلها بأسرع وقت ممكن. وبالنظر إلى البيئة الأردنية نلاحظ انتقال العمل في الوحدات الحكومية من النظام اليدوي إلى النظام الإلكتروني؛ مما يتطلب من إدارة نظم المعلومات العمل على احكام الرقابة على العمل الحكومي الالكتروني لأجل الحفاظ على أمن نظم المعلومات الحكومية. وعليه أتت هذه الدراسة للتعرف على المخاطر المختلفة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في القطاع الحكومي والتعرف على أسباب حدوثها وإجراءات الحماية المتبعة لمواجهة تلك المخاطر

هدف الدراسة

تهدف هذه الدراسة إلى التعرف على المخاطر المختلفة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية الوحدات الحكومية والتعرف على أسباب حدوثها وإجراءات الحماية المتبعة في القطاع الحكومي لمواجهة تلك المخاطر ومدى كفاية ضوابط الرقابة الداخلية تلك الوحدات .

أهمية الدراسة

تنبع أهمية هذه الدراسة من أهمية الموضوع ذاته نظرا لان هنالك تطور كبيرا في تقنيات أنظمة المعلومات و الاتصال وهذا التقدم التقني يرافقه زيادة الخبرة لدى الأفراد في استخدام الحاسبات الآلية ويرافقه مخاطر الاختراق من خلال شبكات المعلومات المحلية و عالمية و التلاعب في البيانات ، حيث أصبحت نظم المعلومات المحاسبة الإلكترونية عرضة للعديد من المخاطر التي تهدد صحة وموثوقية ومصداقية وسرية وتكامل ومدى إتاحة و ملاءمة البيانات المالية والمحاسبية التي توفرها تلك النظم .إضافة إلى انه يوجد خلط واضح وعدم تمييز بين مخاطر أمن نظم المعلومات وعدم كفاية ضوابط رقابة في تلك النظم لدى العديد من الباحثين حيث توضح هذه الدراسة مخاطر أمن المعلومات المتعلقة بمرحلة الإدخال و المعالجة والإخراج.

مشكلة الدراسة وعناصرها:

تتجه الوحدات الحكومية في المملكة الأردنية الهاشمية إلى الاعتماد على تكنولوجيا المعلومات في النواحي عديدة ،حيث تعتمد يوما بعد يوم بشكل متزايد على نظم المعلومات المحوسبة؛ لتغطية جميع جوانب النشاط، ...مة المحاسبي منها الأمر الذي يجعلها عرضة للإخطار التي تتعلق بهذا المجال .و حيث إن النظم المحاسبية الالكترونية تواجه العديد من المخاطر المتعلقة بالمدخلات والمخرجات والتشغيل، فقد جاءت هذه الدراسة كمحاولة للتعرف على أهم المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية في المملكة الأردنية الهاشمية ، ودرجة تكرارها .و أسباب حدوثها، و معدلات حدوثها .و كذلك إجراءات الحماية التي تتبعها إدارة نظم معلومات للحد من المخاطر التي تهدد نظم المعلومات المحاسبية.من هنا يمكن تحديد عناصر مشكلة الدراسة بـ:

هل تواجه الأنظمة المحاسبية الالكترونية في الوحدات الحكومية الأردنية مخاطر تتعلق(بإدخال البيانات ،بتشغيل البيانات ،تتعلق بالمخرجات) ؟

هل ترجع أسباب حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية :(أسباب تتعلق بموظفي الوحدة الحكومية ،أسباب تتعلق بإدارة الوحدة الحكومية نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الإجراءات والأدوات الرقابية المطبقة.)

هل توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية الأردنية ؟

فرضية الدراسة

تقوم الدراسة باختبار الفرضيات التالية :_

- ☒ تواجه الأنظمة المحاسبية الالكترونية في الوحدات الحكومية الأردنية مخاطر تتعلق(بإدخال البيانات ،بتشغيل البيانات ،تتعلق بالمخرجات)
- ☒ ترجع أسباب حدوث المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية :(أسباب تتعلق بموظفي الوحدة الحكومية ،أسباب تتعلق بإدارة الوحدة الحكومية نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الإجراءات والأدوات الرقابية المطبقة.)
- ☒ توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية الأردنية

الطريقة و الإجراءات

مجتمع الدراسة وعينة الدراسة :

تتكون عينة الدراسة من ورؤساء الأقسام و مدققي نظم المعلومات الإلكترونية والمدققين الداخليين في٣٢ وزارة و مؤسسة حكومية ملحق (١) بمعدل ٥ استبيان لكل وحدة حكومية

أما من حيث عينة الدراسة فأنها تتكون من مدراء نظم والمحاسبين ورؤساء الأقسام ومراجعي نظم المعلومات الإلكترونية والمدققين الداخليين في تلك الوحدات الحكومية

ومهندسي وموظفي دوائر تكنولوجيا المعلومات الوحدات الحكومية .و قد تم توزيع عينة شاملة تشمل جميع أعضاء مجتمع العينة .و قد تم توزيع 160 استبيان وقد تم استعادة 130 منها ليصل

معدل الردود إلى 81 % من إجمالي العينة .وقد تم استخدام أسلوب التحليل للبيانات التي تم تجميعها؛ للتعرف على الخصائص الأساسية (Descriptive Analysis) الوصفي لعينة ومتغيرات الدراسة، حيث اعتمد الباحث على المنهج الوصفي التحليلي، لأنه يعتبر من أنسب المناهج لمثل هذه الدراسة، كما تم إجراء بعض الاختبارات اللامعلمية Non-Parametric Tests مثل اختبار(Sign Test) لاختبار فرضيات البحث وذلك من خلال استخدام برنامج الإحصائي(SPSS) .

أداوت الدراسة :

لتحقيق أهداف الدراسة والإجابة عن أسئلتها اعتمد الباحث على المنهج الوصفي التحليلي للبيانات من مصدرين :

مصادر ثانوية و تتمثل في مراجعة الأدبيات المحاسبية المتوفرة حول موضوع الدراسة

مصادر أولية و تتمثل في جمع البيانات الميدانية من خلال:

المقابلات الشخصية مع ورؤساء الأقسام و مدققي نظم المعلومات الإلكترونية والمدققين الداخليين في تلك الوزارات و المؤسسات الحكومية ومهندسي وموظفي دوائر تكنولوجيا المعلومات.

قائمة الاستقصاء : حيث تشتمل الاستبيان على قائمة تضم مجموعة المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة كما استخلصها الباحث من الدراسات السابقة الخاصة بالموضوع .

و قبل توزيع الاستبيان على عينة الدراسة تم اختبار مدى صلاحيتها عبر تنفيذ الإجراءات من خلال اختبار الصدق و الثبات : فقد تم أجراء بعض التحليلات الإحصائية للاستبيان) تحليلات الصدق و الثبات . (أما بالنسبة لتحليل الصدق ، أي مدى اتساق كل فقرة من فقرات الاستبيان مع المجال الذي تنتمي إليه تلك الفقرة، فقد تم التحقق من صدق الاتساق الداخلي من خلال إيجاد معامل الارتباط الخطي لبيرسون بين كل فقرة من فقرات الاستبيان والدرجة الكلية للمجال الذي تنتمي إليه تلك الفقرة، وقد كانت النتائج ايجابية بشكل كبير، حيث دلت معاملات الارتباط المختلفة على أن هناك اتساق داخلياً للفقرات مع المجالات التي تنتمي إليه أما فيما يتعلق بتحليل الثبات فقد تحقق الباحث من ثبات استبيان البحث من خلال طريقتي التجزئة النصفية ومعامل ألفاكرونباخ .وقد تبين لنا من نتائج التحليل التجزئة النصفية ان معامل ثبات الاستبيان بلغ 0.975 ، و أن معامل ألفاكرونباخ للاستبيان ككل بلغ 0.956 وهي قيم جيدة 0.01، كما أن معاملات الارتباط والثبات ومعاملات α = ودالة إحصائيا عند مستوى دلالة ألفاكرونباخ لمجالات الاستبيان الخمس أيضاً مرتفعة ومعنوية إحصائيا؛ مما يؤكد ثبات الاستبيان وصلاحيتها للاستخدام.

الدراسات السابقة و الإطار النظري

تساهم هذه الدراسة في تغطية جانب من الثغرات فيما يتعلق بمخاطر أمن نظم المعلومات فيالوحدات الحكومية الأردنية التي قد تواجه نظم المعلومات المحاسبية الإلكترونية فيها 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 أم غير مقصودة . وتعتبر المخاطر المقصودة أشد خطرا على أداء فعالية النظم .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 الإطلاع والتصنت على المعلومات السرية أو تغييرها إلى خسائر مادية أو معنوية كبيرة. هذا ويعتبر موضوع أهمية مخاطر نظم المعلومات المحاسبية الإلكترونية من المواضيع الهامة والحديثة نسبيا، حيث إنه 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 والبنوك .وتجدر الإشارة إلى أن الأبحاث القليلة التي تمت في هذا الموضوع قد استهدفت التعرف على المخاطر المحتملة التي قد تواجه أو تهدد أمن تلك النظم والتعرف على أسبابها ومحاولة تطوير قائمة تتضمن أهم المخاطر التي قد تواجه أمن النظم المحاسبية الإلكترونية، ومن ثم محاولة اختبار مدى جوهرية وأهمية تلك المخاطر في الواقع العملي من خلال مجموعة من الدراسات الميدانية التي تمت في هذا الشأن، وذلك من خلال التعرف على معدل تكرار حدوثها وحجم الخسائر المالية الناجمة عنها .و من اهم الدراسات في هذا المجال.:

١-دراسة (Siponen 2000) بعنوان هي و " A conceptual Foundation for Organizational Information Security Awareness". و التي قدمت تصورا لبرنامج توعية بخصوص أمن المعلومات في المؤسسات؛ وذلك لتقليل أخطاء المستخدمين؛ ولتحسين فعالية سيطرة الأمن المطبقة، وقد توصل الباحث 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

٢- دراسة(Abu-Musa 2001) وهي بعنوان
" A conceptual Foundation for Organizational "Information Security Awareness .

حيث قام الباحث بعمل دراسة تطبيقية؛ لاستكشاف واختبار المخاطر الهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في القطاع المصرفي بجمهورية مصر العربية، حيث تم عمل دراسة مسحية شملت جميع البنوك الرئيسة العاملة بجمهورية مصر العربية للتعرف على أراء كل من رؤساء أقسام الحاسب الألى ورؤساء أقسام المراجعة الداخلية، فيما يختص بالمخاطر الهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في البنوك التي يعملون بها .وتشير نتائج الدراسة إلى أن الإدخال غير المتعمد لبيانات غير صحيحة من قبل موظفى البنوك، التدمير غير المتعمد للبيانات من قبل موظفى البنوك، إدخال فيروس الكمبيوتر إلى النظام، الكوارث الطبيعية والكوارث التي هي من صنع الإنسان، اشتراك بعض الموظفين في استخدام نفس كلمة السر، وكذلك توجية البيانات والمعلومات إلى أشخاص غير مخول لهم باستلامها تعد من أهم المخاطر التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في البنوك المصرية .وتجدر الإشارة إلى أنه في جميع الحالات فإن رؤساء أقسام المراجعة الداخلية قد أعطوا تقديرات أعلى لمعدلات حدوث تلك المخاطر في البنوك التي يعملون بها مقارنة بتقديرات رؤساء أقسام الحاسب الألى، وتشير نتائج الدراسة أنه لا توجد اختلافات جوهرية بين أنواع البنوك المختلفة إلا فيما يختص بالمرور غير المرخص به للبيانات /النظام من قبل أطراف خارجية (قراصنة المعلومات)

٣- دراسةWhitman (2003) هي بعنوان Enemy at the Gate: Threats to Information Security

و قد ركزت على الإجابة على ثلاثة فقرات، الاولى تتعلق بحصر التهديدات التي تواجه أمن المعلومات، و الثانية تتعلق بدرجة خطورة هذه التهديدات، و الثالثة تتعلق بعدد مرات حدوثها شهريا ، حيث قام الباحث بعمل تقييم لعدد من الأبحاث والمقالات في مجال أمن المعلومات، وحصر التهديدات التي تواجه أمن المعلومات. حيث قام الباحث بعمل دراسة مسحية شملت ألف موظف أغلبهم من مدراء نظم المعلومات، والمدراء و المشرفين. 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 خلال علاقتها مع البيئة التي تعمل به.

٤-دراسة(Podgorsek ٢٠٠٤) بعنوان **Risk Assessment of E-Government projects.**

هدفت هذه الدراسة إلى تعريف القواعد النظرية و المنهجية لإدارة المخاطر في مشاريع الحكومة الإلكترونية، لأن هذه المشاريع ستأخذ حيزاً في الميزانية العامة للدولة، يضاف الى ذلك أنها يجب أن تكون مدعومة بأنظمة و تعليمات حتى يصار إلى التدقيق و الرقابة على أعمالها بشكل سليم .فقد قسم الباحث مخاطر الحكومة الإلكترونية إلى أصناف منها المخاطر الخاصة بأولوية العمل و حافز التغيير، ومخاطر التركيب وإدارة و تطبيق المشروع، ومخاطر التقنيات المستخدمة و مخاطر المستخدمين، وأشار الباحث في دراسته إلى خطوات إدارة المخاطر من تحليل المخاطر و ادارة المخاطر من خلال ووضع الضوابط الرقابية اللازمة والية إدارة المخاطر و أهميته في مشروع الحكومة الإلكترونية .

وقد أشار الباحث في دراسته إلى المخاطر التي تظهر في مراحل تطبيق الحكومة الإلكترونية في مرحلة الإعداد و مراحل التخطيط و مرحلة التنفيذ و مرحلة العمل و التي تتطلب نظاماً مراقباً و تدقيق مستمراً، وقد استخدم الباحث المنهج النظري لدراسة مشاريع الحكومة الإلكترونية و مخاطر المتعلقة بالعمل الحكومي الالكتروني، والضوابط الرقابية اللازمة في مشاريع الحكومة الإلكترونية.

وقد توصل الباحث الى أصناف المخاطر التي قد تتعلق بالخصوصية و السرية و فقدان الأمان و المخاطر المتعلقة بالتركيب و إدارة المشروع .

إن تعزيز الثقة والأمن في استعمال تكنولوجيا المعلومات والاتصالات سوف يعزز إطار الطمأنينة الذي يشمل أمن المعلومات وأمن الشبكات وحماية الخصوصية والسرية وحماية المستخدم مما يعتبر شرطا مسبقا لإنشاء المشروعات الإلكترونية لتنمية مجتمع المعلومات لبناء الثقة بين مستخدمي تكنولوجيا المعلومات والاتصالات ،ويتضمن هذا العمل عدة محاور ترتبط بالتوسع في استخدامات نظم وتطبيقات وخدمات المعلومات الرقمية والتي تتاح علي شبكات المعلومات التي صارت تتسم بالاعتمادية، وقابليتها للتعرض للضرر والخطر، وحاجتها لاكتساب الثقة في التعامل معها من قبل المواطنين؛ وأمن نظم المعلومات وتطبيقاتها وخدماتها في بيئة المصالح والمنظمات الرقمية يجب أن يتم حماية سريتها وسلامتها وتوافرها فيما يتصل بالتهديدات المطلوب مواجهتها والاعتبارات العامة التي تشكل معالم شفافيتها من العمليات والبشر والتكنولوجيا والثقافة المؤسسية المتاحة ،ومن خلال الإطلاع على الدراسات السابقة قام البحث يمكن بتصنيف المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية بشكل عام إلى أربعة أصناف رئيسة:

أولاً :مخاطر المدخلات

وهي المخاطر التي تتعلق بأول مرحلة من مراحل النظام وهي مرحلة إدخال البيانات إلى النظام الآلي وتتمثل تلك المخاطر في البنود التالية :الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين، الإدخال المتعمدة (المقصود)لبيانات غير سليمة بواسطة الموظفين،التدمير غير المتعمد للبيانات بواسطة الموظفين، التدمير المتعمد(المقصود) للبيانات بواسطة الموظفين.

ثانياً :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:الوصول غير الشرعي) غير المرخص به (للبيانات والنظام بواسطة الموظفين ،الوصول غير الشرعي للبيانات والنظام بواسطة أشخاص من خارج المنشأة. ،شتراك العديد من الموظفين في نفس كلمة السر .إدخال فيروس الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام.اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.

ثالثاً :مخاطر مخرجات الحاسب.

تتعلق تلك المخاطر بمرحلة مخرجات عمليات معالجة البيانات وما يصدر عن هذه المرحلة من قوائم للحسابات أو تقارير وأشرطة ملفات ممغنطة وكيفية استلام تلك المخرجات وتتمثل تلك المخاطر في البنود التالية: طمس أو تدمير بنود معينة من المخرجات و خلق مخرجات زائفة /غير صحيح وسرقة البيانات /المعلومات و عمل نسخ غير مصرح) مرخص (بها من المخرجات والكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق .وطبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك والمطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخولين باستلام نسخة منه وتسليم المستندات الحساسة إلى أشخاص لا تتوافر فيه الناحية الأم نية بغرض تمزيقها أوالتخلص منها.

رابعاً :مخاطر بيئية

وهي المخاطر التي تحدث بسبب عوامل بيئية، مثل : الزلازل والعواصف والفيضانات والأعاصير، و المتعلقة بأعطال التيار الكهربائي والحرائق ؛ وسواء كانت تلك الكوارث طبيعية أم غير طبيعية فإنها قد تؤثر على عمل النظام المحاسبي وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة مما يؤثر على أمن وسلامة نظم المعلومات المحاسبية الالكترونية

الدراسة الميدانية ونتائج التحليل الإحصائي

في هذا من البحث نستعرض خصائص عينة البحث و أهم نتائج التحليل الإحصائي التي تم الحصول عليها عبر تحليل البيانات التي شملتها الاستبانة.

خصائص العينة.

وتشمل خصائص العينة ، خصائص الأشخاص الذين قاموا بالإجابة على لاستبيان و يشمل الموضوعات التالية –المؤهل العلمي المسمى الوظيفي و سنوات الخبرة ، و هذه الخصائص موضحة في الجداول(1)

المؤهل العلمي	النسبة المئوية	المسمى الوظيفي	النسبة المئوية	الخبرة	النسبة المئوية
ثانوية عامة	% 2.3	محاسب	% 12	اقل من 3 سنوات	%30
دبلوم	% 8.5	مدقق نظم معلومات الكترونية	%7.	من 3إلى 6سنوات	% 27.
بكالوريوس	% 84.5	مراجع داخلي	% 27.	من7إلى 10سنوات	
ماجستير	% 4.7	مدقق ديوان المحاسبة	% 11	من ١١الى 15سنة	%30
		رئيس قسم	%30	اكثر من 15	%13
		مدير	%13		
الإجمالي	100%	الإجمالي	100%	الإجمالي	100%

يتضح من خلال الجدول رقم (1) أن أغلبية ا لمشاركين في الاستقصاء كانوا من حملة شهادة البكالوريوس وأن عدد ا قليلا منهم كانوا من حملة شهادة الماجستير وهذا يعكس واقع الهيكل الوظيفي لمؤسسات الحكومة التي تتجه نحو تعيين موظفين حملة درجة البكالوريوس مما يعني أن عينة الدراسة تعد عينة ممثلة للهيكل الوظيفي في الوحدات الحكومية الأردنية . كما أن هؤلاء الموظفين هم من مختلف التخصصات ذات العلاقة موضوع البحث . من ناحية أخرى فإننا نلاحظ أن حوالي 60% من المشاركين في الاستقصاء كانت خبرتهم تزيد عن سبع سنوات، مما يعطي دعم ا وثقة أكبر لنتائج الاستبانة نتيجة الخبرة الجيدة التي يتمتع بها هؤلاء الموظفين في العمل الحكومي.

اختبار الفرضيات

لاختبار فرضيات الدراسة فقد تم استخدام اختبار الإشارة اللامعلمي لعينة واحدة المعلمي Sign) (Test، إذ انه يستخدم للتحقق من مطابقة وسيط (t) والذي يعتبر أحد بدائل اختبار عينة مختارة من

مجتمع إحصائي مع وسيط ذلك المجتمع، كما أن اختبار الإ شارة 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 الوقد تم – الإشارة يستخدم لتحديد اتجاه الفروق بين آراء أفراد العينة . استخدام 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 (3) والتي تمثل الرأي (محايد) في المجالين الثاني و الثالث والصفة (أكثر من مرة شهريا إلى مرة أسبوعيا)في المجال الأول، لأجل معرفة ما إذا كانت هناك موافقة جوهرية ومعنوية إحصائيا من أفراد العينة على عبارات الاستبانة أم لا. وقد تم استخدام اختبار الإشارة اللامعلمي؛ نظراً لأن متغيرات الاستبانة (العبارات)هي متغيرات وإنما تم الاستعاضة عن ذلك (t) رتبية وبالتالي لا تناسبها الاختبارات المعلمية كاختبار بالاختبارات اللامعلمية لعينة واحدة وأفضلها وأكثرها مناسبة ل بيانات الدراسة هو اختبار الإشارة و قد تم استخدام مقياس ليكرت الخماسي وقد تم ترميز هذا المقياس كما يلي:

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

وبالتالي كلما اقتربنا من الدرجة(5) ؛ تزداد شدة موافقة عينة الدراسة على العبارة في حين تزداد شدة المعارضة إجابات عينة الدراسة كلما اقتربنا من الدرجة (1) أما إذا اقتربنا من الدرجة (3؛ فإن اتجاه إجابات عينة الدراسة محايد و هذا المقياس استخدم في المجالين الثاني و الثالث لدراسة ، اما في المجال الأول فقد كان المقياس المستخدم حول عدد مرات وقوع مخاطر نظم المعلومات كما يلي:

تكرر أقل من مرة بالسنة	تكرر من مرة بالسنة إلى مرة بالشهر	تحدث أكثر من مرة بالشهر إلى مرة بالأسبوع	أكثر من مرة بالأسبوع إلى مرة باليوم	أكثر من مرة باليوم أو بصفة متكرر
٥	٤	٣	٢	١

وبالتالي كلما اقتربت إجابات عينة الدراسة من الدرجة(5) ؛ فان عدد مرات حدوث المخاطر ينخفض إلى درجة انعدام حدوث المخاطر عند الدرجة(5) ، ويزداد عدد مرات حدوث تلك المخاطر ؛ كلما اقتربت إجابات عينة الدراسة من الدرجة (1) أما إذا إجابات عينة الدراسة قريبة من الدرجة(3) ؛ فإن ذلك يعني ان عدد مرات حدوث مخاطر نظم المعلومات في البنك متوسطا نسبيا.

☒ اختبار الفرضية الرئيسية الأولى والتي تنص على أنه: تحدث المخاطر المتعلقة بإدخال البيانات ، التشغيل، المخرجات و بالبيئة بشكل متكرر الوحدات الحكومية الأردنية .

وتشير الفرضية الإحصائية العدمية(H 0) إلى انعدام حدوث مخاطر نظم المعلومات بشكل متكرر في الوحدات الحكومية الأردنية فيما لو كانت آراء أفراد العينة أقل أو تساوي الدرجة (3) و التي تمثل الخيار) أكثر من مرة شهرياً إلى مر ة أسبوعي او التي تمثل الخيار أكثر من مرة شهرياً إلى مر ة أسبوعيا، يتم إجراء الاختبار الإحصائي 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 لمعرفة مدى تكرار حدوث تلك المخاطر في الوحدات الحكومية الأردنية وذلك كما هو موضح في الجدول رقم(٢)

(جدول رقم 2)

نتيجة اختبار الإشارة للمجال الأول الخاص بمخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية الأردنية

أنواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	الوسيط العام
مخاطر الإدخال	١	126	٣	١٣٠	11.003-	0.000	5
مخاطر التشغيل	٣	١٢٦	١	١٣٠	11.136-	0.000	5
مخاطر المخرجات	٢	١٢٥	٣	١٣٠	11.135-	0.000	5
مخاطر البيئة	٢	١٢٦	٢	١٣٠	11.225-	0.000	5

يلاحظ من خلال ا لجدول رقم (3) أن قيمة اختبار الإشارة معنوية إحصائياً عند(z) مستوى دلالة (0.05)؛ مما يعني أن هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على كل نوع من أنواع مخاطر نظم المعلومات المحاسبية في الوحدات الحكومية الأردنية ،ووسيط المقياس المستخدم في استبيانة الدراسة ، وهو الدرجة (3) ويعزز هذه النتيجة أن الوسيط العام لآراء أفراد العينة على كل نوع من أنواع المخاطر الأربعة في الجدول بلغ (5) وهي تمثل انعدام أو ندرة تكرار تلك المخاطر في الوحدات الحكومية الأردنية حسب المقياس المستخدم في استبيان 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 نصت على أن مخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية الأردنية لا تحدث بشكل متكرر، و بذلك فإن تلك المخاطر على الرغم من عدم حدوثها بشكل متكرر فإنها قائمة بحكم طبيعة العمل الآلي الذي يتطلب

توفير إجراءات حماية كافية. وللوقوف على أراء أفراد العينة حول مدى حدوث المخاطر التي تتضمنها كل نوع من أنواع المخاطر الأربعة ؛ 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 هو موضح الجدول رقم (٣)

جدول رقم (٣)

نتيجة اختبار الإشارة لعبارات المجال الأول الخاص بمخاطر نظم المعلومات المحاسبية في الوحدات الحكومية الأردنية

المجال الأول (مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة	مستوى المعنوية (sig)	الوسيط العام
الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين	١٦	٩٣	٢١	١٣٠	7,409-	0.000	4
الإدخال المتعمدة لبيانات غير سليمة بواسطة الموظفين.	٣	١٢٦	١	١٣٠	10.872-	0.000	5
التدمير غير المتعمد للبيانات بواسطة الموظفين.	١	١٢٦	٣	١٣٠	11.135-	0.000	5
التدمير المتعمد للبيانات بواسطة الموظفين.	١	١٢٦	٣	١٣٠	11.136-	0.000	5
المرور الوصول (غير المرخص به) للبيانات / النظام بواسطة الموظفين	٢	١٢٥	٣	١٣٠	10.958-	0.000	5
المرور (غير المصرح به) للبيانات / النظام بواسطة أشخاص من الخارج	1	١٢٧	٢	١٣٠	11.049-	0.000	5
إشراك الموظفين في كلمة السر	1	١١٩	١٠	١٣٠	10.681-	0.000	5
إدخال فيروس الكمبيوتر للنظام المحاسبي.	١	١٢٧	٢	١٣٠	11.181-	0.000	5
طمس أو تدمير بنود معينة من المخرجات.	٢	١٢٦	٢	١٣٠	11.003-	0.000	5

خلق مخرجات زائفة /غير صحيحة	١	١٢٧	٢	١٣٠	11.181-	0.000	5
سرقة البيانات ألمعلومات	٢	١٢٧	١	١٣٠	10.958-	0.000	5
عمل نسخ غيرمصرح (مرخص) بها من المخرجات.	٢	١٢٧	١	١٣٠	10.780-	0.000	5
الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.	٢	١٢٧	١	١٣٠	10.780-	0.000	5
طبع و توزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.	٣	١٢٦	١	١٣٠	10.459-	0.000	5
المطبوعات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم(ليس لهم الحق) في استلام نسخة منها	٣	١٢٦	١	١٣٠	10.459-	0.000	5
تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقه ا أو التخلص منها	٣	١٢٦	١	١٣٠	10.412-	0.000	5
الكوارث الطبيعية مثل الحرائق،الفيضانات أو انقطاع مصدر الطاقة.	١	١٢٦	٣	١٣٠	11.136-	0.000	5
الكوارث غير الطبيعية والتي هي مثل الحرائق، أو الفيضانات	٠	١٢٦	٤	١٣٠	11.136-	0.000	5

يلاحظ من خلال الجدول رقم (3)أن قيمة اختبار الإشارة معنوية إحصائياً (z) في كافة العبارات؛ ما يعني أن هناك فرق معنوي إحصائيا بين وسيط آراء أ فراد العينة على كـل عبـارة ووسـيط المقياس المستخدم في استبيان الدراسة وهو الدرجة (3) كما أن وسيط آراء أفراد العينة في جميع

العبارات كان 5 باستثناء العبارة الأولى فقد كان(4) ؛ مم ا هذا يعني نـــدرة أو انعـــدام حـــدوث المخاطر

اختبار الفرضية الرئيسة الثانية والتي تنص على أنه:ترجع أسباب حدوث المخاطر التي تهـــدد نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية الأردنية إلى أسباب تتعلق بموظفي الوحدات الحكومية ؛ نتيجة لقلة الخبرة و الوعي والتدريب بموظفي الوحدات الحكومية، أسباب تتعلق بإدارة الوحدة الحكومية ؛ نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الإجراءات والأدوات الرقابية المطبقة.

لاختبار الفرضية السابقة فقد تم استخدام اختبار الإشارة ؛ لمعرفة ما إذا كانت هناك فروقا معنويـــة إحصائياً بين وسيط آراء أفراد العينة على المجال الثاني والمتعلق بأسباب حدوث مخـــاطر نظـــم المعلومات المحاسبية ووسيط المقياس المستخدم في استبيان الدراسة وهو الدرجة (3) والتي تمثل صفة(محايد)وذلك لتحديد ما إذا كانت هناك موافقة جوهرية من قبل أفراد العينة علـــى أســـباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية و التي تضمنها المجال الثاني بشكل عـــام . وفيما يلي نتيجة اختبار الإشارة على المجال الثاني ككل مصنفا في فئتـــين همـــا أســـباب تتعلـــق بالموظفين و أسباب تتعلق بإدارة الوحدة الحكومية . وتشير الفرضية الإحصائية العدمية إلى تردد أو اعتراض أفراد العينة على أسباب حدوث مخاطر نظم المعلومات فيما لو كانت آراء أفراد العينة اقل أو تساوي الدرجة (3) حسب المقياس المستخدم في استبيان الدراسة ، أما الفرضـــية البديلـــة فأشارت إلى موافقة أفراد العينة على أسباب حدوث مخاطر نظم المعلومات المحاسبية فيمـــا لـــو كانت آراء أفراد العينة اكبر من الدرجة(3) ؛ وسيتم إجراء الاختبار الإحصائي و تحديد مستوى المعنوية على أساس ذيل واحد و هو الذيل الأعلى كما هو واضح من الفرضية لبديلة السابقة، وفيما يلي نتيجة الاختبار الفرضية السابقة

جدول رقم(٤)

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

أنواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة	مستوى المعنوية (sig)	الوسيط العام
أسباب تتعلق بالموظفين	43	66	21	**130**	2.213-	0.027	4
أسباب تتعلق بإدارة نظم المعلومات في الوحدة الحكومية	46	70	14	**130**	2.135-	.033	4

من خلال الجدول رقم (٤) يلاحظ أن قيمة اختبار الإشارة معنوية إحصائياً عند(z) مستوى دلالة (0.05؛ هذا يعني أن هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على كلا النوعين من أسباب حدوث مخاطر نظم المعلومات المحاسبية ، ووسيط المقياس المستخدم في استبيان الدراسة وهو الدرجة (3) ويعزز هذه ا لنتيجة أن الوسيط العام لآراء أفراد العينة على كلا النوعين من أسباب حدوث مخاطر نظم المعلومات المحاسبية بلغ (4) وهي تمثل درجة الموافقة حسب المقياس المستخدم في استبيان الدراسة . وبالتالي نستنتج من ذلك أن أفراد العينة يرون أن أسباب حدوث مخاطر نظم المعلومات المحاسبية ترجع لأسباب تتعلق بموظفي الوحدة الحكومية ، و أسباب أخرى تتعلق بإدارة الوحدة الحكومية بشكل عام . وبناء على ذلك نقبل الفرضية البحثية الثانية و التي نصت على ان أسباب حدوث مخاطر نظم المعلومات المحاسبية ترجع إلى أسباب تتعلق بموظفي الوحدة الحكومية ؛ نتيجة لقلة الخبرة و الوعي والتدريب، و أسباب تتعلق بإدارة الوحدة الحكومية نتيجة لعدم وجود سياسات واضحة ومكتوبة، وضعف الإجراءات والأدوات الرقابية المطبقة.وللوقوف على أراء أفراد العينة حول أسباب حدوث المخاطر الواردة في المجال الثاني بشكل مفصل فقد تم إيجاد اختبار الإشارة لكل سبب من الأسباب التي تضمنها المجال الثاني و المتعلقة بحدوث المخاطر التي تهدد نظم المعلومات المحاسبية وذلك كما يظهر في الجدول(٥)

جدول رقم (٥)

نتيجة اختبار الإشارة لكل عبارة من عبارات المجال الثاني الخاص بأسباب حدوث مخاطر نظم المعلومات المحاسبية في الوحدات الحكومية الأردنية

المحال الثاني (أسباب مخاطر نظم المعلومات)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	الوسيط العام
عدم كفاية وفعالية الأدوات والضوابط الرقابية المطبقة الوحدة الحكومية الأردنية	41	74	15	**130**	3.091-	0.001	4
ضعف نظم الرقابة الداخلية في الوحدات الحكومية الأردنية وعدم فعاليتها.	47	65	18	**130**	1.708-	0.044	4
اشتراك بعض الموظفين في استخدام نفس كلمات السر.	62	56	12	**130**	0.555-	0.2895	3
عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظم المعلومات	44	70	15	**130**	2.341-	0.0095	4
عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظم المحاسبية في الوحدات الحكومية	**43**	**74**	**13**	**130**	2.774-	0.003	4

عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر في الوحدات الحكومية	47	69	14	130	1.950-	0.0255	4
ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب الآلي	53	65	12	130	11013-	0.1555	3
عدم وجود سياسات واضحة ومكتوبة فيما يختص بأمن نظم المعلومات المحاسبية في الوحدات الحكومية .	45	68	16	130	2.070-	0.019	4
عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسئوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي في الوحدات الحكومية	50	72	8	130	1.818-	0.0345	
عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الأعمال من قبل الوحدات الحكومية	47	70	13	130	1.950-	0.0255	4
عدم إلزام الموظفين بأخذ إجازتهم الدورية	53	54	23	130	0.15	0.5	3
عدم الاهتمام الكافي بفحص التاريخ الوظيفي والمهني للموظفين الجدد	44	61	25	130	1.471-	0.0705	3
عدم الوعي الكافي لدى الموظفين بضرورة فحص البرامج أو الأقراص الممغنطة الجديدة عند إدخالها إلى أجهزة الكمبيوتر.	38	70	22	130	2.983-	0.0015	4

يلاحظ من خلال الجدول رقم(٥) أن قيمة اختبار الإشارة معنوية إحصائياً في كافة(z) العبارات باستثناء الفقرات (12,11, 7, 3) لم يكن هناك فرقا معنويا إحصائيا بين وسيط أراء أفراد العينة على هذه العبارات الأربع و وسيط المقياس هو الدرجة(3) ، في حين ان وسيط اراء افر اد العينة في باقي العبارات بلغ(4) ، و هي تمثل صفة الرأي (موافق) حسب المقيـــاس المســـتخدم فـــي

الاستبانة و هو اكبر من وسيط مقياس الاستبانة ، و بشكل معنوي احصائيا كما تتضح من قيمة (sigو هي اقل من .(0.05) الأمر الذي يبيني أهمية هذه الأسباب كمسببات للمخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الوحدات الحكومية.

اختبار الفرضية الرئيسة الثالثة والتي نصت على أنه: توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية الأردنية

لاختبار الفرضية السابقة ؛ فقد تم استخدام اختبار الإشارة لمعرفة ما إذا كانت هناك فروقا معنوية إحصائياً بين وسيط آراء أفراد العينة على المجال الثالث والمتعلق بإجراءات الحماية؛ لمواجهة مخاطر نظم المعلومات المحاسبية ووسيط المقياس ا لمستخدم في استبانة الدراسة، وهو الدرجة (3والذي تمثل صفة (محايد) وذلك لتحديد ما إذا كان ت هناك موافقة جوهرية من قبل أفراد العينة على إتباع إجراءات الحماية الواردة في المجال الثالث أم لا. وأشارت الفرضية الإحصائية العدمية إلى تردد أو عدم موافقة أفراد العينة على إجراءات الحماية المذكورة، فيما لو كانت آراء أفراد العينة اقل أو تساوي الدرجة(3) ؛مما يعني عدم موافقة أفراد العينة توفر إجراءات الحماية في الوحدات الحكومية . أما الفرضية البديلة فقد أشارت إلى على وجود إجراءات الحماية في الوحدات الحكومية العاملين بها فيما لو كانت آراء أفر اد العينة اكبر من الدرجة . (3)وسيتم إجراء الاختبار الإحصائي و تحديد مستوى المعنوية على أساس ذيل واحد و الذيل الأعلى كما هو واضح من الفرضية البديلة السابقة.

جدول(6)

نتيجة اختبار الإشارة للمجال الثالث الخاص بإجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية الأردنية

أنواع مخاطر نظم المعلومات	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجمو ع	zقيمة	مستوى المعنوية (sig)	الوسيط العام
إجراءات الحماية المتبعة لمواجهة المخاطر التي تهدد نظم المعلومات المحاسبية	2	120	8	130	10.545-	0.000	5

جدول رقم (7) يوضح نتيجة التحليل الخاص بالمخاطر التي تتعلق بالبيئة . كما يظهر في الجدول معنوية إحصائياً عند مستوى دلالة(0.05) ؛ م ما يعني أن (z) المذكور، فان قيمة اختبار الإشارة هناك فروق معنوية إحصائياً بين وسيط إجابات أفراد العينة على إجراءات الحماية المتبعة ؛ لمواجهة مخاطر نظم المعلومات المحاسبية ، ووسيط المقياس المستخدم في استبانة الدراسة وهو

الدرجة (3) ويعزز هذه النتيجة أن الوسيط العام لآراء أفراد العينة بلغ (5) وهي تمثل درجة الموافقة بشدة حسب المقياس المستخدم في استبانة الدراسة . وبالتالي نستنتج من ذلك أن أفراد العينة يرون ان الوحدات الحكومية التي يعملون فيها تتبع إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية . وبناء على ذلك نرفض الفرضية البحثية الثالثة و التي نصت على انه لا توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية الأردنية .وللوقوف على أراء أفراد العينة حول طبيعة إجراءات الحماية التي تتبعها الوحدات الحكومية الأردنية بشكل تفصيلي ؛ فقد تم إيجاد اختبار الإشارة لكل عبارة على حدة من العبارات التي تضمنها المجال الثالث ، و المتعلق بإجراءات الحماية المتبعة لمواجهة المخاطر التي تهدد نظم المعلومات الم حاسبية الإلكترونية وذلك كما يظهر في الجدول رقم (٧)

جدول رقم(7)

نتيجة اختبار الإشارة لكل عبارة من عبارات المجال الثالث الخاص بإجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في الوحدات الحكومية

المجال الثاني (إجراءات الحماية المتبعة لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية)	عدد الإشارات الموجبة	عدد الإشارات السالبة	عدد الأصفار (الحياد)	المجموع	قيمة z	مستوى المعنوية (sig)	الوسيط العام
تقوم إدارة الوحدة الحكومية بإصدار قرارات إدارية خاصة لتجنب مخاطر أمن المعلومات.	4	122	4	130	10.554-	0.000	5
تتابع إدارة الوحدة الحكومية موظفي تكنولوجيا المعلومات في تنفيذ إجراءات الحماية المطلوبة	6	116	8	130	10.000-	0.000	5
تقوم إدارة الوحدة الحكومية بوضع قواعد خاصة بحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد	2	112	16	130	10.348-	0.000	5

تقوم إدارة الوحدة الحكومية بوضع خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، وتدقيق الإجراءات الداخلية والاحتفاظ بنسخة احتياطية من المعلومات	3	120	7	130	10.459-	0.000	5
تطبيق الوحدة الحكومية أهداف حماية أمن المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح به، وتوفر البيانات في الوقت المحدد	1	123	6	130	11.001-	0.000	5
تقوم إدارة الوحدة الحكومية بتحليل المخاطر الخاصة بأمن المعلومات مثل العائد المتوقع مقابل تكاليف الإجراءات المضادة.	6	105	19	130	9.934-	0.000	4
تقوم إدارة الوحدة الحكومية بوضع سياسات خاصة بأمن المعلومات تشمل اختيار التقنية المناسبة،والإجراءات اللازمة لجعل هذه التقنية فعالة.	2	116	12	130	10.539-	0.000	5
تقوم إدارة الوحدة الحكومية بتركيب طرق الحماية التقنية مثل جدران الحماية ومضادات(Firewalls) الفيروسات وغيرها.	6	113	11	130	9.850-	0.000	5
تقوم إدارة الوحدة الحكومية بتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة	5	115	10	130	9.900-	0.000	5

التكنولوجيا.							
تقوم إدارة الوحدة الحكومية بفحص طرق الحماية	3	115	12	130	10.218-	0.000	5
تقوم إدارة الوحدة الحكومية باكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق.	5	100	24	130	9.173-	0.000	4
تقوم إدارة الوحدة الحكومية بصد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه	2	109	19	130	10.061-	0.000	5

يلاحظ من خلال الجدول رقم ٧ أن قيمة اختبار الإشارة معنوية إحصائياً في كافة(z) العبارات؛مما يعني أن هناك فرق معنوي إحصائيا بين وسيط آراء أفراد العينة على كل عبارة ووسيط المقياس المستخدم في استبانة الدراسة وهو الدرجة(3) ، كما ان وسيط آراء أفراد العينة في جميع العبارات كان(5) باستثناء العبارات 7 ,12 فقد كان (4) و هذا يعني أن الوحدات الحكومية تتبع إجراءات الحماية الواردة في الجدول السابق حسب أراء أفراد العينة.

النتائج و التوصيات

هدفت هذه الدراسة إلى التعرف على المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في القطاع الحكومي الأردني ومعدلات تكرارها، و أسباب حدوثها .وكذلك التعرف على إجراءات الحماية التي تتبعها تلك الوحدات الحكومية للحد من المخاطر التي تهدد نظم معلومات المحاسبية الإلكترونية .وقد توصلت هذه الدراسة إلى مجموعة من النتائج والتي من

أهمها:

١-عدم حدوث مخاطر نظم المعلومات المحاسبية في الوحدات الحكومية الأردنية ، بشكل متكرر، و لكن تعتبر مخاطر الإدخال غير المتعمد واشتراك الموظفين في كلمة السر وتوجيه البيانات

والمعلومات إلى أشخاص غير مصرح لهم بذلك؛ أكثر المخاطر تكرارا حيث قد تحدث أكثر من مرة شهريا إلى مرة أسبوعيا.

٢- حدوث مخاطر نظم المعلومات المحاسبية الالكترونية ترجع إلى أسباب تتعلق بموظفي الوحدات الحكومية نتيجة قلة الخبرة والوعي والتدريب، إضافة إلى أسباب تتعلق بإدارة الوحدة الحكومية نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى الوحدة الحكومية.

٣- الوحدات الحكومية الأردنية تتبع إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية.

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

١. من الضروري أن. زيادة الوعي الحكومي حول أمن المعلومات لديها و أن تعمل على إنشاء قسم خاص بتكنولوجيا المعلومات في كافة الوحدات الحكومية وتوفير كادر متخصص في تكنولوجي المعلومات بحيث يكون له مندوبون في الإدارة الفرعية ذوي خبرة وكفاءة عالية لأجل العمل على حماية أمن نظم المعلومات المحاسبية لدى الوحدة الحكومية و كذلك تطوير قدرات العاملين لديها في مجال امن المعلومات و حمايتها.

٢. ضرورة وضع إجراءات تضمن استمرارية عمل وجاهزة نظم المعلومات في الوحدات الحكومية ؛ للعمل في حالة الأزمات من خلال استخدام تجهيزات منيعة أو مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها والحد من وقوعها .وكذلك العمل على تعمية أو تشفير المعلومات عند الحفظ والنقل والتخزين على مختلف الوسائط كي لا يتمكن أحد من اختراقها.

٣. وضع ضوابط أمن ورقابة المعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أم اتصالات سلكية ولاسلكية والإنترنت والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية .و وجود خطة حماية أمنية شاملة والتي تنعكس في انخفاض النفقات الناتجة عن توظيف الحلول الجزئية للأمن.

المراجع

- أبو موسى , أحمد عبد السلام , "**أهمية مخاطر نظم المعلومات المحاسبية الالكترونية** " المجلة العلمية للتجارة والتمويل , العدد الثاني , كلية التجارة , جامعه طنطا : مصر ٢٠٠٤ ص ١-٤٥
- العطار، حسن ، **نموذج مقترح لتقييم مخاطر بيئة التشغيل الالكتروني مدخل لتدعيم دور مراقب الحسابات في ظل التحديات المعاصرة**،مجلة البحوث التجارية،٢٢-٢-٢٠٠٠ ص٥٣-٩١
- **على ،عبد الوهاب نصر و شحاته، شحاته السيدو نعمة الله نجيب ،عادل،(٢٠٠٣)"، ، " دراسات في : المراجعة المتقدمة"، الدار الجامعية، الإسكندرية.**

- علي، عبد الوهاب نصر (٢٠٠١)، " خدمات مراقب الحسابات لسوق المال – المتطلبات المهنية ومشاكل الممارسة العملية في ضوء معايير المراجعة المصرية والدولية والأمريكية"، كلية التجارة – جامعة الإسكندرية، بدون ناشر،.
- الفيومي , محمد , والدميري , علاء الدين محمد ,وشتيوي , أيمن أحمد (٢٠٠٦), دراسات متقدمة في المراجعة , الإسكندرية , المكتب الجامعي الحديث , .
- القباني ،ثناء علي ،(٢٠٠٣)،الرقابة المحاسبية الداخلية في النظامين اليدوي و الالكتروني ،الدار الجامعية ،القاهرة ،مصر.

-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.
- Dhillon, G. (1999), "Managing and controlling computer misuse", Information Management & Computer Security, (Vol. 7, Number 4), PP.171-175.
- 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.
- 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.
- 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.
- Whitman Michael E. (2003), "Enemy at the Gate: Threats to Information Security", Communication of the ACM, (Vol. 46, Iss. 8), pp. 91-95.