استكشاف مخاطر نظم المعلومات المحاسبية الالكترونية في المصارف التجارية الليبية

«دراسة تطبيقية على المصارف التجارية العاملة في ليبيا»

■ د. الصديق عثمان الساعدي

● أستاذ مشارك - كلية المحاسبة - جامعة غريان

■ أ. رباب حسين علي بلحوق

● محاضر مساعد - كلية المحاسبة - جامعة الزنتان

ملخص

هدفت الدراسة إلى التعرف على أنواع مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية، وأيضاً التعرف على الإجراءات المطبقة بالمصارف التجارية الليبية للحماية من المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية، أجريت الدراسة على عينة من المصارف التجارية العاملة في ليبيا، حيث تم تصميم صحيفة استبيان لجمع البيانات الأولية، وزع عدد 100 صحيفة على مديري المصارف ومديري الفروع والمحاسبين والمراجعين والموظفين العاملين بالمصارف التجارية العاملة في ليبيا التي شملتها الدراسة، واستخدام برنامج التحليل الإحصائي (SPSS) Package Statistical for Social Science في تحليل البيانات واختبار الفرضيات، وعلى الرغم من أن معظم اجابات المشاركين في الدراسة أوضحت قلة حدوث الكثير من المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية، إلا أن بعض الاجابات بينت حدوث بعض المخاطر المتعلقة بإدخال البيانات وبعض المخاطر المتعلقة بالبيئة كما أشارت بعض اجابات المشاركين في الدراسة إلى وجود اجراءات حماية إلا أنها غير كافية لمواجهة المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية، وتوصي الدراسة بضرورة الاهتمام بإدخال البيانات والمعلومات المحاسبية في

نظم المعلومات المحاسبية الإلكترونية بشكل سليم وأمن، وبضرورة إنشاء قسم خاص بتكنولوجيا المعلومات في كافة المصارف لحماية أمن المعلومات، وضرورة وضع اجراءات تضمن استمرارية عمل نظم المعلومات المحاسبية الإلكترونية وذلك للعمل في الأزمات والكوارث الطبيعية وغير الطبيعية.

1. مقدمة:

إن التطور السريع في تقنية المعلومات والاتصالات وازدياد حجم المنافسة بين منظمات الاعمال في مجال استخدام تكنولوجيا المعلومات أدى إلى حدوث تغييرات كبيرة في العديد من المجالات وعلى جميع المستويات، وكانت المحاسبة من أهم المجالات التي تأثرت بهذا التغيير، حيث شهد العصر الحالي تحولاً سريعاً نحو استخدام نظم المعلومات المحاسبية الإلكترونية، وبالنظر إلى البيئة الليبية نلاحظ انتقال العمل في النظام المحاسبي في العديد من القطاعات والمؤسسات من النظام اليدوي إلى النظام الإلكتروني وخاصة في المصارف التجارية، لما يتميز به من سرعة ودقة وتنوع في التطبيقات وإنجاز الأعمال، وفي المقابل فإن هذا التقدم التكنولوجي لم يصاحبه تطوراً مماثلاً في القدرات والكفاءات البشرية من مستخدمي هذه التكنولوجيا، وكذلك الإجراءات والضوابط الرقابية الأمر الذي أدى إلى ظهور مخاطر تحد من فاعلية وكفاءة استخدام نظم المعلومات المحاسبية الإلكترونية، وعلى هذا الأساس فإن نظام المعلومات المحاسبي الإلكتروني يجب أن يتضمن وسائل وضوابط رقابية دقيقة، وبالتالي على إدارة نظم المعلومات في المنظمة أو المنشأة ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل تلك النظم بشكل صحيح، مع التخطيط الدقيق لمواجهة جميع المخاطر التي يمكن أن تؤدي إلى تعطلها أو توقفها عن العمل، وبناء على ما سبق نرى أن هناك حاجة للتعرف على المخاطر المختلفة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية، لذلك جاءت هذه الدراسة مستهدفة التعرف على أهم المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية في البيئة المصرفية الليبية ومدى توفر إجراءات حماية كافية لمواجهة هذه المخاطر.

2. مشكلة الدراسة:

استخدمت تكنولوجيا نظم المعلومات في العمل المصرفي منذ أوائل الستينيات من القرن الماضي، وقد غيرت الكثير من أساليب إنتاج وتقديم الخدمات المصرفية، وتعددت استخدامات تكنولوجيا المعلومات في المصارف، مثل تبادل البيانات إلكترونياً، ومعالجة صور الوثائق، والقيام بالعمل المصرفي عن بعد، ونظم التحويل الإلكترونية للأموال من نقطة الشراء، وكان ذلك منذ بداية الثمانينيات من القرن الماضي حيث يشهد القطاع المصرفي يومياً تطور الوسائل التكنولوجية نتيجة احتدام المنافسة، ودخول منافسين جدد إلى القطاع المصرفي (جل، 2010، ص14)، إلَا أن كثيراً ما يرافق هذا الاستخدام العديد من المخاطر، ولتوفر الأمن والحماية لنظم المعلومات المحاسبية الإلكترونية لابد من اكتشاف المخاطر التي تواجه هذه النظم، لذلك فإن استكشاف مخاطر نظم المعلومات المحاسبية الإلكترونية أصبحت مطلبا ملحاً وحاجة أساسية، ونظراً للتطور السريع في استخدام وسائل التكنولوجيا الحديثة في البيئة التجارية الليبية، وخاصة قطاع المصارف الذي يعتمد بشكل متزايد على نظم المعلومات الإلكترونية، لتغطية جميع مجالات نشاطه، خاصة المحاسبي منها الأمر الذى يجعلها عرضة للكثير من المخاطر التي تتعلق بهذا المجال، لذلك جاءت هذه الدراسة كمحاولة للتعرف على المخاطر التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية العاملة في ليبيا، ومن ذلك يمكن صياغة مشكلة الدراسة في التساؤلين الآتيين:

1 – ماهي المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية؟

2 – هل هناك اجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية؟

3. أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق الأهداف الآتية:

1 – التعرف على أنواع مخاطر نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية.

2 – التعرف على إجراءات الحماية المطبقة في المصارف التجارية الليبية للحماية من المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية.

4. فرضيات الدراسة:

استناداً إلى تساؤلات الدراسة وأهدافها، تم صياغة فرضيات الدراسة، على النحو الآتي:

الفرضية الأساسية الاولى: لا توجد مخاطر تهدد أمن نظم المعلومات المحاسبية الإلكترونية المستخدمة في المصارف التجارية الليبية محل الدراسة.

وتندرج تحت هذه الفرضية الأساسية الاولى الفرضيات الفرعية الآتية:

الفرضية الفرعية الأولى: لا توجد مخاطر تتعلق بإدخال البيانات تهدد أمن نظم المعلومات المحاسبية الإلكترونية المستخدمة في المصارف التجارية الليبية محل الدراسة.

الفرضية الفرعية الثانية: لا توجد مخاطر تتعلق بالتشغيل تهدد أمن نظم المعلومات المحاسبية الإلكترونية المستخدمة في المصارف التجارية الليبية محل الدراسة.

الفرضية الفرعية الثالثة: لا توجد مخاطر تتعلق بالمخرجات تهدد أمن نظم المعلومات المحاسبية الإلكترونية المستخدمة في المصارف التجارية الليبية محل الدراسة.

الفرضية الفرعية الرابعة: لا توجد مخاطر تتعلق بالبيئة تهدد أمن نظم المعلومات المحاسبية الإلكترونية المستخدمة في المصارف التجارية الليبية محل الدراسة.

الفرضية الاساسية الثانية: لا توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الإلكترونية المستخدمة في المصارف التجارية الليبية محل الدراسة.

5. أهمية الدراسة:

يمكن تحديد أهمية الدراسة في النقاط الآتية:

1 – الاستخدام المتزايد لنظم المعلومات المحاسبية الإلكترونية في قطاع المصارف في ليبيا وندرة الأبحاث والدراسات التي تتطرق لهذا الموضوع بشكل عام وفي ليبيا بشكل خاص.

2 – إن نتائج هذه الدراسة سوف تمكن مستخدمي نظم المعلومات المحاسبية

الإلكترونية من فهم وتقييم حالة أمن نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية، والتعرف على نواحي القصور بها، ومن ثم إمكانية اتخاذ القرارات التصحيحية المناسبة لتلافي أوجه القصور المختلفة، وتعزيز الضوابط الرقابية الأمنية لتلك النظم بما يحقق الاستفادة المثلي من تكنولوجيا المعلومات في المصارف التجارية الليبية.

3 – كما تبرز أهمية الدراسة فيما يمكن أن تسهم به في إثراء المكتبة العلمية حول أهم المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية.

6. حدود الدراسة:

تحاول الدراسة التعرف على المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية المستخدمة بقطاع المصارف الحكومية وفروعها الواقعة في نطاق منطقة الجبل الغربي وطرابلس وهي (المصرف التجاري الوطني وفروعه منها فرع حي الأندلس وفرع أبو سليم وفرع سوق الثلاثاء، ومصرف الجمهورية وفروعه منها فرع الرجبان وفرع الرحيبات وفرع جادو، ومصرف الصحارى وفروعه منها فرع حي الأندلس وفرع حي الأكواخ وفرع سوق الجمعة، ومصرف الوحدة وفروعه منها فرع السواني وفرع الزنتان وفرع جادو، ومصرف شمال أفريقيا وفروعه منها فرع جادو وفرع قرجي) فقط، ولا تتطرق إلى المصارف الخاصة والمتخصصة ولا المنشآت الأخرى كالشركات التجارية أو الصناعية الحديثة وغيرها وذلك باعتبار أن قطاع المصارف الحكومية يعتبر أن النظام المحاسبي بها يغلب عليه الطابع الآلي وهذا النظام مستخدم منذ سنوات، كما تقتصر الدراسة على استكشاف مخاطر نظم المعلومات المحاسبية للتعرف على أنواعها وأسباب حدوثها وكذلك التعرف على إجراءات الحماية المتخذة في المصارف التجارية الليبية خلال فترة اجراء الدراسة (2016 – 2018) فقط.

7. الادب المحاسبي والدراسات السابقة

1.7 المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية

فيما يلي أهم المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية، حيث تُقسم هذه المخاطر كالآتي:

أولا: مخاطر تتعلق بالموارد البشرية:

وتحدث هذه المخاطر عادة أثناء تصميم التجهيزات أو نظم المعلومات أو خلال عمليات البرمجة أو الاختبار أو التجميع للبيانات أو أثناء إدخالها إلى النظام، أو في عمليات تحديد الصلاحيات للمستخدمين، وتشكل هذه الأخطاء الغالبية العظمى للمشكلات المتعلقة بأمن وسلامة نظم المعلومات في المنشآت (الحميدي وآخرون، 2004، ص267)، وعلى الرغم من أن أجهزة الحاسب نفسها هي أجهزة دقيقة، ويمكن الاعتماد عليها إلى درجة عالية، إلا أن ذلك لا يعني أن النظام محصناً من المخاطر والأخطاء، فالبيانات يتم إدخالها إلى الحاسب من قبل أفراد، والبرامج التي تُشغل الحاسب يتم تصميمها من قبل أفراد أيضاً، وعليه فإن وجود العنصر البشري لابد وأن يعِرض النظام إلى بعض المخاطر الناتجة عن التصرفات غير الصحيحة، أو تعطل الأجهزة عن العمل لأي سبب من الأسباب (العيسى، 2003، ص220).

وتشمل هذه المخاطر أو الأخطاء أخطاء اخصائي التشغيل مثل أخطاء الحذف، أو التكرار غير المقصود، بسبب إهمال العاملين في اتباع الإجراءات المرسومة، أو بسبب سوء التدريب، والذي قد يترتب عليه فقدان البيانات، أو إدخالها بطريقة غير سليمة، مما يؤدي إلى تغيير البيانات، أو الملفات (أرحيم، 2006، ص101)، اشار حسين (2006، ص371) إلى أن أحد المبرمجين في نظام المصارف استطاع أن يعدل من برنامج احتساب الفائدة لكي يقوم البرنامج بإضافة فروق الكسور العشرية إلى الحساب الشخصي لهذا المبرمج، واتضح أنه من الصعب جداً اكتشاف مثل هذا التلاعب نظراً لعدم توقع أن يشتكي العميل لمجرد اختلاف لا يتجاوز 10 أو 20 قرش في حساب الفائدة الخاص به.

ثانيا: مخاطر الشبكات:

تعتبر المخاطر المتعلقة بشبكات الأعمال من المخاطر التي يصعب تقييمها، لأن لها متطلبات كثيرة للحماية وعلى مستويات مختلفة داخل النظام، وكذلك بالنسبة للخدمات الخارجية التي تتفاعل مع النظام (هاشم، 2005، ص174)، أيضاً أصبحت حماية شبكات الحاسب من الاختراق مشكلة معقدة تتزايد بتقدم تكنولوجيا الحاسبات، أن تتوقف

الشبكة عن العمل نتيجة عطل الأجهزة، أو فقد البيانات أو البرامج بسبب حادث أو غيره، ولا يغيب عن الذهن ما يترتب على ذلك من تكاليف، ومصاريف إضافية، كما قد يحدث عرقلة لخدمة الشبكة، والمقصود بعرقلة الخدمة هو حدوث انقطاع في خدمة الاتصال بالشبكة، أو بالخدمات التي تقدم للمستفيدين داخل الشبكة، وتتعدد الوسائل التي قد تسبب هذا الخطر، من هذه الوسائل إرسال حزم وهمية تملأ مساحات الذاكرة الوسطية وتمنع الشبكة من مواصلة العمل، ومن هذه الوسائل أيضاً تخريب معلومات تجزئة الرسائل بحيث إذا حاول النظام مستقبلا إعادة تركيبها عند الوصول، فإن هذه المحاولة تتسبب في تخريب النظام، وهنا تتضح أهمية سرعة التوجه نحو اكتشاف وعلاج نقاط الضعف في الشبكات، لأن استمراريتها لها أثار خطيرة على جودة مخرجات نظم المعلومات المحاسبية الإلكترونية.

ثالثا: مخاطر متعلقة بالأجهزة ووسائط التخزين والبرامج:

قد يكون تلف الأجهزة ووسائط التخزين والبرامج نتيجة لتصرفات من داخل المنشأة، أو نتيجة لمؤثرات من خارجها، وقد اشار هاشم (2005،ص175)، إلى تعرض الأجهزة والمعدات لهذا الخطر إما بالتقادم التكنولوجي أو نتيجة لتعرضها لحوادث مختلفة مثل التخريب المتعمد، أو العنف في التعامل مع الأجهزة، أو سرقة أجزاء منها، أو تغير تردد التيار الكهربائي، أو انقطاعه، أو تلف أو توقف أجهزة التكييف، أو التدفئة، كما أن مشكلات البيئة المحيطة بالحاسب تعتبر من الأخطار التي تعمل على تدمير الوجود المادي للأجزاء المادية للحاسب والتجهيزات الخاصة به، لذا من المعتاد أن نرى مواسير المياه أو البخار تمر داخل غرفة الحاسب، وقد يؤدي التسرب من هذه المواسير أو انفجارها إلى خسائر ضخمة، وفي العديد من الحالات يحدث حريق بغرفة الحاسب المضادة للحريق، نتيجة حدوث حريق بغرفة مجاورة، أو بالطابق الأعلى.

وقد توصل الفيومي، (1993،ص273 - 274) إلى أن وسائط التخزين من المحتمل فسادها نتيجة تعرضها لإشعاعات خارجية، حيث أشار أن أحد المراكز واجه مشكلة حدوث أضرار بالأشرطة الممغنطة ولم يتمكن مدير المركز من معرفة السبب المباشر، وبالملاحظة اكتشف أن الأشرطة التالفة كانت تخزن في قاع دولاب حفظ الأشرطة

وبالمصادفة تم اكتشاف أن هذه المشكلات تنتج من استخدام مكنسة كهربائية لتلميع الأرضية والتي تؤدي إلى توليد مجال مغناطيسي يفسد نمط التسجيل المغناطيسي على الأشرطة الموجودة بالرف الأسفل من الدولاب، لذلك فإن ضرورة التأكد من مستويات الأمن المتعلقة بهذا الخطر تعتبر مهمة، بالإضافة إلى تقديم التقارير الدورية التي توضح مستويات الالتزام بالأمن.

رابعا: مخاطر الفيروسات والبرامج الضارة:

انتشرت في عالم الحاسبات الإلكترونية نوعية من البرامج أطلق عليها اسم برامج الفيروسات، وهي برامج غير مشروعة تتمثل في مجموعة كودية من التعليمات التي يمكن أن تنتشر في النظام وقت تشغيل البيانات لأداء مهام غير مشروعة دون ترك أي أثر إلكتروني يفيد في ملاحظة هذه البرامج وتقييم نظم الرقابة الداخلية، كذلك يمكن استخدام هذه البرامج غير المشروعة لإحباط عمل المراجع عن طريق التعرف على العمليات الاختبارية الفجائية التي يقوم بها المراجع دون علم المنشأة، حيث يتعامل معها هذا الفيروس ويوهمها بصحة نقاط الرقابة داخل نظام المعلومات المحاسبي للشركة (البحيصي والشريف، 2008)، كما بإمكان الفيروسات استنساخ نفسها بعدة نسخ في الذاكرة الداخلية أو الخارجية، مما يتسبب في استغلال المساحات التخزينية المتوفرة بهدف منع المستفيدين من استثمار هذه المواقع التخزينية في خزن بياناتهم وبرامجهم، ايضا بإمكان بعض الفيروسات اتلاف المسارات التي تحوي برامج التحميل والتشغيل التي يفترض أن تستقر في ذاكرة الحاسب عند بدء تشغيله لتقديم الخدمة لمستخدمي هذا الحاسب، لذلك فإن سرعة التوجه نحو التحديث المستمر لبرامج كشف الفيروسات يعتبر أمر في غاية الأهمية، وذلك لتفادي المخاطر التي يمكن أن تحدثها الفيروسات وما لها من آثار خطيرة على جودة مخرجات نظم المعلومات المحاسبية الإلكترونية.

خامسا: المخاطر البيئية:

تتعرض نظم المعلومات إلى تهديد طبيعي ناتج عن الكوارث الطبيعية (الحرائق، والبراكين، والزلازل، والفيضانات) وتهديدات طبيعية ذات صبغة بيئية (الكهرباء، والحرارة، وأنظمة التبريد، والمشكلات الناتجة عن الانفجارات)، ولقد اشار بعض

الكُتاب منهم على سبيل المثال (الفيومي، 1993، دواد، 2000، الهيثي والربيحات، 2005)، إلى أن الحرائق تؤدي إلى تدمير أجهزة الحاسب، وتلف البرامج والبيانات والتي قد يستلزم إعادة تجميعها تكاليف أكبر من تكلفة الحاسب نفسه، وقد يستغرق الأمر عدة سنوات حتى يستطيع المشروع استرداد مكانته، كما أن الزلازل والأعاصير والفيضانات (زلزال سان فرانسيسكو - فيضانات بنجلادش - إعصار أندرو)، على الرغم من ضعف احتمالاتها وندرة حدوثها، إلا أنها تكون عادة مدمرة وأضرارها خطيرة على مكونات الحاسب وبرمجياته، انقطاع أو تذبذب التيار الكهربائي يؤدي إلى تسجيل غير صحيح بالمخزن الداخلي للحاسب نتيجة حدوث قراءة خاطئة من وحدة الاسطوانات المغنطة، كما اشار كل من (هاشم، 2005، الفيومي، 1993)، أن توقف لمورد المنتج عن ممارسة النشاط بصفة عامة، أو توقفه عن التعامل مع المنشأة بصفة خاصة، وعدم توفر قطع غيار بالسوق المحلي قد يؤدي إلى ضياع أسابيع من زمن الحاسب إلى أن يتم استيراد هذه القطع، لذا فإن ضرورة تلافي ذلك الخطر تكمن في التعامل مع مورد له شهرة لضمان استمراريته مع الاتصال المستمر به لمتابعة عمليات الصيانة والتحديث.

سادسا: اجراءات الحماية من المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية:

تعتبر قضية تطبيق أمن المعلومات قضية مهمة جداً لدى المنشآت التي تعتمد في عملها على تكنولوجيا المعلومات، وتحقيق أمن المعلومات لا يكون إلا بإدارة رشيدة، وإجراءات تشغيلية جيدة، لذلك أصبحت قضية أمن المعلومات أساساً إدارية وليست تكنولوجية، لذلك فإنه على المنشآت اتباع العديد من الإجراءات وأساليب الحماية من المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية، حيث يقع على عاتق الإدارة العليا للمنشاة الالتزام بشكل قوي بتطبيق أمن المعلومات، كما أن الإدارة العليا لتكنولوجيا المعلومات تحتاج أيضاً إلى التزام قوي لتطبيق أمن المعلومات، لذا يجب على إدارة المنشأة متابعة موظفي تكنولوجيا المعلومات في تنفيذ اجراءات الحماية المطلوبة، ايضا ينبغي على إدارة المنشأة أن تضع قواعد خاصة لحماية أمن المعلومات ومعاقبة الموظفين المخلين بهذه القواعد، ولكي تكون المنشأة آمنة فلا بد لها من تحقيق الأهداف الجوهرية لأمن المعلومات وهي السرية، والموثوقية والتعرف أو التحقق من

هوية الشخصية وسلامة المحتوى واستمرارية توفر المعلومات أو الخدمة، عدم الإنكار وهي تعتبر أيضاً من الدعائم الأساسية لتطبيق أمن المعلومات في أي منشأة.

ان المنشآت المهتمة جداً بالحماية الشاملة يجب أن تمر إجراءات تطبيقها خلال عملية تدعى التخطيط – الحماية – الاستجابة، يشمل التخطيط الحماية الشاملة، ويندرج تحت هذه المرحلة تحليل المخاطر المتعلقة بأمن المعلومات، وذلك من خلال حصر التهديدات، وهو تعريف كل التهديدات المتوقعة، وتحليل شدة التهديدات، وتطبيق الاجراءات المضادة، ووضع الاولويات، أي تعريف الاجراءات المضادة حسب الأهم فالأقل أهمية، حيث يتم تطبيق هذه السياسات على نطاق واسع داخل المنشأة، فمثلاً تسمح المنشأة بإجازة لموظفيها، والغرض من ذلك كشف حالات الغش لدى الموظفين، ووضع إجراء إداري مركزي لحماية أجهزة الموظفين من الفيروسات، وتشمل طرق الحماية تركيب الأجهزة الخاصة بالحماية مثل جدران النار وتنزيل البرامج اللازمة لها، وإعدادها برمجياً بما يتناسب مع سياسات الحماية المطلوبة، وأن يتم تحديث طرق الحماية باستمرار، لأن أدوات الحماية تصبح غير مفيدة مع الوقت، وتشمل أيضاً فحص طرق الحماية والإعدادات الخاصة بها باستمرار، وهو ما يسمى بتدقيق أمن المعلومات، وضع إجراءات صارمة تشمل انتاج تقارير رسمية لتعريف وتحديد حادث الاختراق وتحديد المهاجمين وإيقافهم وإصلاح الدمار الناتج، وفي بعض الحالات معاقبة المهاجمين.

2.7 الدراسات السابقة:

يعتبر موضوع نظم المعلومات المحاسبية الإلكترونية من الموضوعات الهامة والحديثة نسبيا، ونظراً لقلة الدراسات والبحوث المنشورة في ليبيا حسب علم الباحثين حول موضوع مخاطر نظم المعلومات المحاسبية الإلكترونية، فيما يلى بعض الدراسات التي تناولت هذا الموضوع في بعض الدول التي تتشابه ظروفها الى حد كبير مع ظروف البيئة الليبية للاستفادة منها في إجراء هذه الدراسة.

دراسة البحيصي والشريف (2008)، استكشفت المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في بيئة المصارف العاملة في قطاع غزة ومعدلات تكرارها،

وأسباب حدوثها، وكذلك التعرف على اجراءات الحماية التي تتبعها تلك المصارف للحد من المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية، وخلصت إلى اعتماد المصارف العاملة في قطاع غزة في عملها بشكل كبير على النظام الآلي، وكذلك قلة حدوث مخاطر نظم المعلومات المحاسبية بشكل متكرر، إلا أن مخاطر الإدخال غير المتعمد واشتراك الموظفين في كلمة السر وتوجيه البيانات والمعلومات إلى أشخاص غير مصرح لهم بذلك، أكثر المخاطر تكراراً ، وأن حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية ترجع إلى أسباب تتعلق بموظفي المصرف نتيجة قلة الخبرة والوعي والتدريب، إضافة إلى أسباب تتعلق بإدارة المصرف نتيجة لعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى المصرف، وأخيراً أظهرت نتائج الدراسة أن المصارف التي شملتها الدراسة تتبع إجراءات حماية كافية لمواجهة نظم المعلومات المحاسبية الإلكترونية.

دراسة زويلف (2009)، قامت بتسليط الضوء على التهديدات التي قد تواجه أمن نظم المعلومات المحاسبية الإلكترونية، والتعرف على مدى وجودها في شركات التأمين الأردنية، وتحديد أهم التهديدات التي يتعرض لها أمن هذه النظم في تلك الشركات، وقد أظهرت النتائج أن أهم تهديدات أمن نظم المعلومات المحاسبية الإلكترونية في شركات التأمين الأردنية تتمثل في: الادخال غير المتعمد لبيانات خاطئة من قبل الموظفين، وسرقة وقت الحاسوب واستخدامه في الأغراض الشخصية، والاشتراك في كلمة المرور(كلمة السر)، والقيام بتدمير غير متعمد للبيانات من قبل الموظفين، وتوصل موظفين غير مصرح لهم للبيانات والنظام، وإدخال فيروس الحاسوب للنظام، وتوجيه المخرجات عن طريق الخطأ لأشخاص غير مصرح لهم باستلامها، والكشف بشكل غير شرعي عن البيانات والمعلومات بعرضها على شاشة الحاسوب أو طباعتها على الورق.

دراسة الصلاح (2009)، هدفت إلى التعرف على مخاطر أمن نظم المعلومات المحاسبية الإلكترونية وأثرها على صحة ومصداقية القوائم المالية في المصارف التجارية الأردنية، وقد خلصت إلى نتائج من أهمها أن المصارف التجارية الأردنية

تتعرض إلى عدة مخاطر تهدد امن نظم المعلومات المحاسبية الالكترونية، وتعتبر مخاطر أمن نظم المعلومات المحاسبية الالكترونية مؤثرة على صحة ومصداقية القوائم المالية وأن الاجراءات الرقابية التي تضعها المصارف التجارية الأردنية تحد من مخاطر نظم المعلومات المحاسبية الالكترونية وأثرها على صحة ومصداقية القوائم المالية.

دراسة البحيصي (2011)، ناقشت المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في الشركات الفلسطينية العاملة في قطاع غزة، وقد أظهرت النتائج أن من أهم مخاطر نظم المعلومات المحاسبية الإلكترونية مخاطر الادخال المتعمد للبيانات الخاطئة عن طريق المستخدمين، وانقطاع التيار الكهربائي، والإتلاف غير المقصود للبيانات من قبل المستخدمين، واشتراك العاملين في كلمات المرور، ودخول الفيروسات إلى الأنظمة، والكوارث غير الطبيعية، كما أوضحت أن المخاطر التي تتعرض لها الشركات الفلسطينية تختلف فيما بينها في درجة تكرار وأهمية المخاطر حسب نوعية نظام المعلومات المستخدم وحسب مدى الارتباط بشبكة الأنترنت، إلا أنه ليس هناك ارتباط بين نوع المؤسسة (القطاع الذي تنتمي إليه المؤسسة) ودرجة تكرار وأهمية المخاطر التي تتعرض لها الشركات في الدول الأخرى، خاصة النامية منها.

دراسة العبيدي (2012)، هدفت إلى التعرف على مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية وأثرها على فاعلية عملية التدقيق في الشركات المساهمة العامة المدرجة في بورصة عمان، وتكون مجتمع الدراسة من ثلاثة فئات (المديرون الماليون، والمدققون الداخليون، والمدققون الخارجيون)، وتوصلت إلى نتائج من أهمها وجود أثر للمخاطر البيئية الخاصة بنظم المعلومات المحاسبية الالكترونية على فاعلية عملية التدقيق في الشركات المساهمة العامة الأردنية، كما كشفت عن وجود أثر لمخاطر إدخال نظم المعلومات، تشغيل البيانات، ومخرجات نظم المعلومات المحاسبية الالكترونية على فاعلية عملية التدقيق في الشركات المساهمة العامة الأردنية، وأن معظم هذه المخاطر تتعلق بعدم اخضاع البرامج الإلكترونية للتحديث والتطوير المستمرين، ووجود خلل في الحواسيب المستخدمة في تطبيق النظام، وافتقار المكلفين بتطبيق النظام إلى المؤهلات العلمية والخبرة العملية اللازمة.

دراسة الدلاهمة (2013)، هدفت إلى تقصي أثر مخاطر استخدام تكنولوجيا

المعلومات على أداء نظم المعلومات المحاسبية من وجهة نظر مراجعي الحسابات في المملكة العربية السعودية، وقد أظهرت النتائج وجود أثر لمخاطر استخدام تكنولوجيا المعلومات على أداء نظم المعلومات المحاسبية بدرجة كبيرة، والتي تمثلت بمخاطر عدم تحديد صلاحيات الدخول على النظم المحاسبية، ومخاطر أعطال الملفات، ومخاطر التشغيل، كما أكدت على ضرورة تبنى ضوابط الرقابة العامة لنظم المعلومات المحاسبية الإلكترونية لحمايتها من مخاطر استخدام تكنولوجيا المعلومات.

دراسة الساعدي واقجام (2014)، تناولت دور المراجع الداخلي في مواجهة أخطار نظم المعلومات المحاسبية الالكترونية من خلال دراسة حالة شركة الزاوية لتكرير النفط، وأشارت إلى أن الإدخال المتعمد أو غير المتعمد لبيانات غير سليمة من قبل موظفي الشركة، وإدخال فيروس الكمبيوتر إلى النظام، والكوارث الطبيعية وغير الطبيعية كانقطاع التيار الكهربائي، واشتراك بعض الموظفين في استخدام نفس كلمة السر تعد من أهم المخاطر التي تواجه أمن نظم المعلومات المحاسبية الالكترونية بالشركة، كما أشارت النتائج إلى وجود إجراءات حماية كافية لمواجهة المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية بالشركة.

دراسة زهيري (2015)، ناقشت المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في سورية، وأهم أسباب حدوثها، واجراءات مواجهتها، وأفضت نتائج الدراسة إلى أن أهم المخاطر التي تواجه المصارف السورية تتمثل في الادخال العرضي للبيانات الخاطئة من قبل الموظفين والمشاركة في كلمات المرور، والتدمير غير المتعمد للبيانات من قبل موظفي المصارف، وتوجيه البيانات والمعلومات إلى أشخاص غير مصرح لهم بذلك، وإدخال فيروس الكمبيوتر إلى النظام، والكوارث الطبيعية وغير الطبيعية، تعد من أهم المخاطر التي تواجه أمن نظم المعلومات المحاسبية الالكترونية في المصارف السورية.

دراسة أبو شيبة والفطيمي (2017)، هدفت إلى التعرف على مخاطر استخدام نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في بلدية مصراته، والتعرف على أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر، وقد أظهرت النتائج أن حدوث مخاطر استخدام نظم المعلومات

المحاسبة الإلكترونية ترجع إلى أسباب تتعلق بموظفي المصرف نتيجة قلة الخبرة والوعي والتدريب، إضافة إلى أسباب تتعلق بإدارة المصرف لعدم وجود سياسات واضحة ومكتوبة وضعف الإجراءات والأدوات الرقابية المطبقة لدى المصرف.

من خلال العرض السابق لأهم الدراسات التي تناولت موضوع مخاطر نظم المعلومات المحاسبية الالكترونية تبين للباحثين أنها تناولت الموضوع من وجهات نظر مختلفة وركزت على واقع نظم المعلومات المحاسبية الالكترونية في بعض البلدان العربية وحاجتها الى الاهتمام والتطوير، ومعالجة المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية والتي حددتها نتائج معظم الدراسات السابقة في مجموعات مختلفة أهمها مخاطر متعلقة بإدخال البيانات ومخاطر متعلقة بتشغيل البيانات ومخاطر متعلقة بالمخرجات والمخاطر البيئيةبم وعلى الرغم من تشابه نتائج هذه الدراسات إلا أنها أجريت في بيئات ومجتمعات مختلفة ولاشك أن لكل بيئة أو مجتمع خصوصيات وظروف تميزه عن غيره من المجتمعات مما يعني حاجة كل مجتمع إلى إجراء الدراسات والأبحاث الخاصة بواقعه وظروفه، وبذلك تحاول هذه الدراسة إضافة الجديد للبيئة المحلية وستسهم في ملء جزء في هذا المجال، لذلك تم اجراء هذه الدراسة للوقوف على مزيد من الآراء للتعرف على أنواع المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية وتختلف هذه الدراسة عن الدراسات السابقة في كونها دراسة استكشافية لمخاطر نظم المعلومات المحاسبية الإلكترونية وتحديد مدى اتخاذ اجراءات الحماية الكافية لمواجهة هذه المخاطر في المصارف التجارية في ليبيا وهو ما يميزها تحديداً عن دراسة (الساعدي واقجام، 2014)، وكذلك أنها استهدفت عينة من المصارف لم تستهدفها الدراسات السابقة وهو ما يميزها عن دراسة (أبو شيبة والفطيمي، 2017).

8. الإطار العام للمنهجية المتبعة في الدراسة الميدانية:

يهدف هذا الجزء إلى معرفة المنهجية التي اتبعها الباحثان في إجراء الدراسة الميدانية، وهي على النحو الآتي:

1.8 مجتمع الدراسة وعينتها:

يتكون مجتمع الدراسة من مديري المصارف ومديري الفروع والمحاسبين والمراجعين والموظفين العاملين بالمصارف التجارية العاملة في ليبيا والتي استهدفتها الدراسة

المتمثلة في (المصرف التجاري الوطني وفروعه منها فرع حي الأندلس وفرع أبو سليم وفرع سوق الثلاثاء، ومصرف الجمهورية وفروعه منها فرع الرجبان وفرع الرحيبات وفرع جادو، ومصرف الصحارى وفروعه منها فرع حي الأندلس وفرع حي الأكواخ وفرع سوق الجمعة، ومصرف الوحدة وفروعه منها فرع السواني وفرع الزنتان وفرع جادو، ومصرف شمال أفريقيا وفروعه منها فرع جادو وفرع قرجي)، ونظراً لصعوبة استخدام طريقة الحصر الشامل لجمع البيانات لاعتبارات الوقت والتكلفة والجهد، لذلك سوف يستخدم في هذه الدراسة أسلوب المعاينة.

1.8 أداة جمع البيانات:

ولتحقيق أهداف الدراسة تم تصميم استمارة استبيان، لجمع البيانات والمعلومات، قسم إلى ستة أجزاء، الجزء الأول خاص بمجموعة من الفقرات تتعلق بخصائص المشاركين في الدراسة، أما الجزء الثاني يهدف إلى التعرف على مدى حدوث مخاطر متعلقة بإدخال البيانات، أما الجزء الثالث يهدف إلى التعرف على مدى حدوث مخاطر تشغيل البيانات، أما الجزء الرابع يهدف إلى التعرف على مدى حدوث مخاطر المخرجات، أما الجزء الخامس يهدف إلى التعرف على مدى حدوث المخاطر البيئية، أما الجزء السادس يهدف إلى التعرف على مدى وجود إجراءات للحماية من المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية بالمصارف التجارية العاملة في ليبيا.

1.8 تحكيم استمارة الاستبيان:

وللتحقق من صدق استمارة الاستبيان تم عرضها على مجموعة من المحكّمين من أعضاء هيئة التدريس بالجامعات الليبية، وذوي الخبرة والمتخصصين في مجالات نظم المعلومات الالكترونية والمحاسبة والإحصاء، وكذلك على بعض ممارسي نظم المعلومات المحاسبية الالكترونية، وذلك لمراجعتها والتأكد من مدى صلاحيتها للدراسة، كذلك التأكد من مدى تغطية فقرات الاستبيان لمختلف جوانب مشكلة الدراسة وفرضياتها وأهدافها، وقد تم الأخذ بآراء ونصائح المحكمين في تعديل بعض الفقرات واستبعاد البعض الأخر وإضافة فقرات جديدة، وبعد عملية التحكيم تم توزيع (100) استمارة استبيان على المشاركين في الدراسة، تم استرداد عدد (88) استمارة صالحة للتحليل.

9. تحليل البيانات واختبار فرضيات الدراسة:

بعد تجميع استمارات الاستبيان استخدمت الطريقة الرقمية في ترميز إجابات المشاركين في الدراسة وفق مقياس لكرت الخماسي كما هو موضح بالجدول رقم (1):

الجدول رقم (1) ترميز الاجابات بمقياس لكرت الخماسي

الاجابة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
الرمز	1	2	3	4	5

من خلال الجدول السابق نلاحظ أن متوسط الدرجات (3)، لذا سوف يتم اختيار ما اذا كان متوسط اجابات المشاركين في الدراسة يختلف عن (3) ام لا، لذلك تم استخدام حزمة البرمجيات الجاهزة (SPSS) Statistical Package for Social Science في تحليل البيانات واختبار الفرضيات كما يلي:

1.9 خصائص المشاركين في الدراسة:

الجدول رقم (2) يبين التوزيع التكراري والنسبي للمشاركين في الدراسة حسب مؤهلاتهم وتخصصاتهم العلمية والوظائف التي يشغلونها وخبراتهم العملية، كذلك إجاباتهم حول نوع النظام المحاسبي المطبق بالمصرف الذي يعملون فيه.

الجدول رقم (2) خصائص المشاركين في الدراسة

المؤهل العلمي:	العدد	النسبة ٪
تعليم متوسط	10	٪ 11
دبلوم عالي	29	٪ 34
بكالوريوس	44	٪ 50
ماجستير	5	٪ 5
المجموع	88	٪ 100
التخصص العلمي:		
محاسبة	53	٪ 60
إدارة أعمال	13	٪ 15

المؤهل العلمي:	العدد	النسبة ٪
اقتصاد	3	٪ 3
حاسوب	14	٪ 16
تمويل ومصارف	5	٪ 6
المجموع	88	٪ 100
الوظيفة:		
محاسب	37	٪ 42
مبرمج نظم	8	٪ 9
رئيس قسم	30	٪ 34
مدير ادارة	11	٪ 13
مدير عام	2	٪ 2
المجموع	88	٪ 100
الخبرة العملية:		
أقل من 5 سنوات	13	٪ 15
من 5 سنوات إلى أقل من 10 سنوات	22	٪ 25
من 10 سنوات فأكثر	53	٪ 60
المجموع	88	٪ 100
طبيعة النظام المحاسبي بالمصرف:		
يدوي	4	٪ 5
آلي	24	٪ 27
خليط	60	٪ 68
المجموع	88	٪ 100

يتضح من الجدول السابق أن اغلبية المشاركين في الدراسة من حملة شهادات التعليم العالي حيث بلغت نسبتهم 89 ٪ من اجمالي المشاركين، وأن أغلب المشاركين أيضا من المتخصصين في المحاسبة حيث بلغت نسبتهم 60 ٪ من اجمالي المشاركين، كما يتضح من الجدول السابق أن هناك تنوع في وظائف المشاركين في الدراسة حيث من ضمنهم محاسبين ومبرمجين نظم بالإضافة إلى وظائف ادارية من رئيس قسم إلى مدير إدارة ومدير عام، وأن 85 ٪ من المشاركين خبرتهم العملية تتجاوز 5 سنوات، وأن 95 ٪ من المشاركين أجابوا انهم يستخدمون النظم الالكترونية في النظام المحاسبي بمصارفهم، وهذا يدل على ان المشاركين في الدراسة على مستوى علمي عالي وخبرة عملية جيدة ولديهم المعلومات والدراية الكافية للتعامل مع أداة الدراسة (الاستبيان) والاجابة على الاسئلة بدقة وموضوعية، كما أن تنوع وظائف المشاركين يؤدي إلى التنوع في البيانات المتحصل عليها كل حسب وظيفته، بالإضافة إلى أن استخدام المشاركين للحاسب الآلي في النظام المحاسبي مؤشر جيد على إمكانية تعرضهم لمخاطر نظم المعلومات المحاسبية الالكترونية المقترحة للدراسة وتحديد انواعها وإجراءات الحماية منها، كل ذلك يمكن الباحثان من الاعتماد على اجابات المشاركين وزيادة الثقة في معلومات ونتائج الدراسة.

2.9 التحليل الاحصائي للبيانات:

يهدف هذا الجزء إلى عرض نتائج التحليل الاحصائي لبيانات الدراسة واختبار فرضياتها باستخدام اختبار (One Sample T – Test) على النحو الآتي:

أولا: فيما يتعلق بمدى حدوث المخاطر المتعلقة بإدخال البيانات:

لمعرفة مدى حدوث المخاطر المتعلقة بإدخال البيانات بالمصارف التجارية محل الدراسة اقترحت مجموعة من المخاطر على المشاركين في الدراسة للإجابة بمدى موافقتهم على حدوث هذه المخاطر، حيث يوضح الجدول رقم (3) المتوسط الحسابي والانحراف المعياري وقيمة t وقيمة الدلالة الاحصائية (P – value)، لكل خطر من المخاطر المقترحة بالجدول رقم (3).

الجدول رقم (3) نتائج الاختبار الاحصائي للمخاطر المتعلقة بإدخال البيانات

م	المخاطـــــــــر	المتوسط	الانحراف المعياري	قيمة t	P-value
1	الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين.	3.295	1.252	2.21	0.015
2	الإدخـال المتعمد لبيانات غير سليمة بواسطة الموظفين.	2.818	1.601	- 1.07	0.885
3	التدمير غير المتعمد للبيانات بواسطة الموظفين.	3.091	1.238	0.690	0.246
4	التدمير المتعمد للبيانات بواسطة الموظفين.	2.773	1.603	- 1.33	0.907
5	التأخير غير المتعمد لإدخال بعض البيانات والمعلومات.	3.477	1.072	4.18	0.000
6	التأخير المتعمد لإدخـال بعض البيانات والمعلومات.	2.932	1.552	- 0.41	0.659
7	إدخال البيانات أكثر من مرة.	2.989	1.273	- 0.08	0.533
8	ضيـاع أو تحـريـف في قـاعـدة البيانات الموجودة.	2.716	1.304	- 2.04	0.978
9	حذف بعض البيانات الصحيحة.	2.750	1.333	- 1.76	0.959
10	إدخـال فـيـروس الكمبيوتر إلى النظام المحاسبي.	2.534	1.430	- 3.06	0.999

من خلال الجدول السابق رقم (3) نلاحظ أن النتائج أشارت إلى أن المشاركين أجابوا بعدم الموافقة على حدوث مخاطر الادخال المتعمد لبيانات غير سليمة بواسطة الموظفين ومخاطر التدمير المتعمد والتدمير غير المتعمد للبيانات بواسطة موظفي

المصرف، والتأخير المتعمد لإدخال بعض البيانات والمعلومات، إدخال البيانات أكثر من مرة، وضياع أو تحريف في قاعدة البيانات الموجودة، وحذف بعض البيانات الصحيحة، وإدخال فيروس الكمبيوتر إلى النظام المحاسبي، كما اشارت النتائج بالجدول السابق ان المشاركين في الدراسة اجابوا بالموافقة على حدوث مخاطر الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين، والتأخير غير المتعمد لإدخال بعض البيانات والمعلومات.

ثانيا: فيما يتعلق بمدى حدوث المخاطر المتعلقة بتشغيل البيانات:

لمعرفة مدى حدوث المخاطر المتعلقة بتشغيل البيانات بالمصارف التجارية محل الدراسة اقترحت مجموعة من المخاطر على المشاركين في الدراسة للإجابة بمدى موافقتهم على حدوث هذه المخاطر، حيث يوضح الجدول رقم (4) المتوسط الحسابي والانحراف المعياري وقيمة t وقيمة الدلالة الاحصائية (P – value)، لكل خطر من المخاطر المقترحة بالجدول رقم (4).

الجدول رقم (4)نتائج الاختبار الاحصائي للمخاطر المتعلقة بتشغيل البيانات

م	المخاطـــــــــر	المتوسط	الانحراف المعياري	قيمة t	P-value
1	الوصول غير الشرعي للبيانات والنظام بواسطة الموظفين.	2.557	1.221	- 3.40	0.999
2	الوصول للبيانات والنظام بواسطة أشخاص من خارج المصرف.	2.443	1.294	- 4بم04	0.998
3	اشتراك الموظفين في كلمة المرور.	2.568	1.329	- 3.05	0.998
4	عدم التغيير المنتظم لكلمات المرور.	2.648	1.398	- 2.38	0.990
5	الاستخدام غير المصرح به لنظم المعالجة.	2.614	1.179	- 3.08	0.870
6	سرقة وقت الحاسوب واستخدامه في الأغراض الشخصية.	2.443	1.153	- 4.53	0.867
7	استخدام البرامج بطريقة غير مرخص بها.	2.477	1.222	- 4.01	0.998

م	المخاطـــــــــر	المتوسط	الانحراف المعياري	قيمة t	P - value
8	عمل نسخ إضافية غير قانونية من البرنامج.	2.545	1.259	- 3.39	0.977
9	اعـتـراض وصـول الـبـيـانـات من الخوادم إلى أجهزة المستخدمين.	2.750	147بم1	- 2.04	0.978
10	الاحـتـفـاظ بنسخة احتياطية للبيانات والمعلومات من قبل الموظفين غير مرخصة (غير مصرح بها) من قبل الإدارة.	2.557	1.321	- 3.15	0.999

من خلال الجدول السابق رقم (4) نلاحظ أن النتائج أشارت إلى أن المشاركين أجابوا بعدم الموافقة على حدوث المخاطر المقترحة بالجدول السابق والمتعلقة بتشغيل البيانات، حيث أجابوا بعدم الموافقة على الوصول غير الشرعي للبيانات والنظام بواسطة الموظفين، ولا الوصول للبيانات والنظام بواسطة أشخاص من خارج المصرف، وعدم اشتراك الموظفين في كلمة المرور، وعدم التغيير المنتظم لكلمات المرور، ولا الاستخدام غير المصرح به لنظم المعالجة. سرقة وقت الحاسوب واستخدامه في الأغراض الشخصية، وكذلك عدم استخدام البرامج بطريقة غير مرخص بها، وعمل نسخ إضافية غير قانونية من البرنامج، وعدم اعتراض وصول البيانات من الخوادم إلى أجهزة المستخدمين، ولا الاحتفاظ بنسخة احتياطية للبيانات والمعلومات من قبل الموظفين غير مرخصة (غير مصرح بها) من قبل الإدارة.

ثالثا: فيما يتعلق بمدى حدوث المخاطر المتعلقة المخرجات:

لمعرفة مدى حدوث المخاطر المتعلقة بالمخرجات بالمصارف التجارية محل الدراسة اقترحت مجموعة من المخاطر على المشاركين في الدراسة للإجابة بمدى موافقتهم على حدوث هذه المخاطر، حيث يوضح الجدول رقم (5) المتوسط الحسابي والانحراف المعياري وقيمة t وقيمة الدلالة الاحصائية (P - value)، لكل خطر من المخاطر المقترحة بالجدول رقم (5).

الجدول رقم (5) نتائج الاختبار الاحصائي للمخاطر المتعلقة بالمخرجات

م	المخاطر	المتوسط	الانحراف المعياري	قيمة t	P - value
1	طمس أو تدمير بنود معينة من المخرجات.	2.750	1.289	- 1.82	0.964
2	خلق مخرجات زائفة/غير صحيحة.	2.557	1.388	- 2.99	0.988
3	سرقة البيانات / المعلومات.	2.557	1.421	- 2.93	0.988
4	عمل نسخ غير مصرح بها من المخرجات.	2.511	1.194	- 3.84	0.999
5	الكشف غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الورق.	2.511	1.135	- 4.04	0.997
6	طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.	2.420	1.275	- 4.26	0.994
7	المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم باستلامها.	2.420	1.172	- 4.95	0.993
8	تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.	2.318	1.291	- 4.95	0.994
9	مراجعة وتصحيح غير مناسب للبيانات بعد ترميزها.	2.443	1.153	- 4.53	0.988
10	الاحتفاظ بنسخة احتياطية بالمخرجات من قبل الموظفين (غير مصرح بها) من قبل الإدارة.	2.443	1.338	- 3.90	0.977

توضح النتائج بالجدول رقم (5) ان المشاركين في الدراسة أجابوا بعدم الموافقة على

حدوث المخاطر المتعلقة بالمخرجات والمقترحة بالجدول السابق، حيث اجابوا بعدم طمس أو تدمير بنود معينة من المخرجات، وعدم خلق مخرجات زائفة/غير صحيحة، سرقة البيانات/المعلومات، وعدم عمل نسخ غير مصرح بها من المخرجات، والكشف غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الورق، وعدم طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك، والمطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم باستلامها، وعدم تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها، وعدم مراجعة وتصحيح غير مناسب للبيانات بعد ترميزها، وعدم الاحتفاظ بنسخة احتياطية بالمخرجات من قبل الموظفين غير مرخصة (غير مصرح بها) من قبل الإدارة.

رابعا: فيما يتعلق بمدى حدوث المخاطر المتعلقة بالبيئة:

لمعرفة مدى حدوث المخاطر المتعلقة بالبيئة بالمصارف التجارية محل الدراسة اقترحت مجموعة من المخاطر على المشاركين في الدراسة للإجابة بمدى موافقتهم على حدوث هذه المخاطر، حيث يوضح الجدول رقم (6) المتوسط الحسابي والانحراف المعياري وقيمة t وقيمة الدلالة الاحصائية (P - value)، لكل خطر من المخاطر المقترحة بالجدول رقم (6).

الجدول رقم (6) نتائج الاختبار الاحصائي للمخاطر المتعلقة بالبيئة

م	المخاطـــــــر	المتوسط	الانحراف المعياري	قيمة t	P - value
1	الكوارث الطبيعية مثل (الحرائق والزلازل والأعاصير،.....).	3.420	1.142	3.45	0.000
2	الكوارث غير الطبيعية مثل (انقطاع التيار الكهربائي،.....).	3.375	1.472	2.39	0.010
3	توصل أشخاص غير مصرح لهم إلى البيانات والنظام.	2.693	1.449	- 1.99	0.975
4	الفيروسات الرقمية المعروفة.	3.057	1.188	0.45	0.327

م	المخاطـــــــــر	المتوسط	الانحراف المعياري	قيمة t	P - value
5	التطور التكنولوجي السريع.	3.636	1.074	5.56	0.000
6	المخاطر القانونية (مكافحة غسيل الأموال،.....).	3.432	1.112	3.64	0.000
7	الحرارة والرطوبة العالية	3.341	0.993	3.22	0.001
8	عدم كفاية الأدوات والضوابط الرقابية المطبقة.	3.250	1.137	2.06	0.021
9	المجال المغناطيسي العالي.	2.931	0.932	- 0.69	0.753
10	عوامل التأكل.	2.955	1.222	- 0.35	0.636
11	مشاكل التيار الكهربائي	3.830	1.280	6.08	0.000
12	عدم التأمين الكافي للنظم	3.193	1.221	1.48	0.007

توضح النتائج بالجدول رقم (6) ان المشاركين في الدراسة أجابوا بعدم الموافقة على حدوث مجموعة من المخاطر المتعلقة بالبيئة والمقترحة بالجدول السابق، حيث اجابوا بعدم توصل أشخاص غير مصرح لهم من خارج المصرف (قراصنة المعلومات) إلى البيانات والنظام، وعدم وجود الفيروسات الرقمية المعروفة، وقلة حدوث المجال المغناطيسي العالي، وعدم وجود خطر عوامل التأكل، كما تبين النتائج بالجدول رقم (6) ان المشاركين أجابوا بالموافقة على حدوث مجموعة من المخاطر المتعلقة بالبيئة، حيث أجابوا بحدوث مخاطر الكوارث الطبيعية مثل (الحرائق والزلازل والبراكين والأعاصير والفيضانات)، والكوارث غير الطبيعية (من صنع الأنسان) تتمثل في الحرائق المفتعلة والانفجارات وانقطاع التيار الكهربائي، والتطور التكنولوجي السريع، والمخاطر القانونية (مكافحة غسيل الأموال - مخالفة الاتفاقيات – عدم التحديد الواضح للحقوق والالتزامات)، والحرارة والرطوبة العالية، وعدم كفاية الأدوات والضوابط الرقابية المطبقة، ومشاكل التيار الكهربائي، وعدم التأمين الكافي للنظم.

خامساً: فيما يتعلق بمدى وجود إجراءات للحماية من المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية.

لمعرفة مدى وجود إجراءات للحماية من المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية بالمصارف التجارية محل الدراسة اقترحت مجموعة من إجراءات الحماية من تلك المخاطر على المشاركين في الدراسة للإجابة بمدى موافقتهم على وجود هذه الاجراءات، حيث يوضح الجدول رقم (7) المتوسط الحسابي والانحراف المعياري وقيمة t وقيمة الدلالة الاحصائية (P – value))، لكل خطر من المخاطر المقترحة بالجدول رقم (7).

الجدول رقم (7) نتائج الاختبار الاحصائي المتعلقة باجراءات الحماية

م	الإجراءات	المتوسط	الانحراف المعياري	قيمة t	P - value
1	تقوم الإدارة بإصدار قرارات لتجنب مخاطر أمن المعلومات.	3.613	0.877	6.57	0.000
2	تهتم إدارة المصرف بتطبيق أمن المعلومات.	3.716	0.958	7.01	0.000
3	تتابع الإدارة موظفي نظم المعلومات في تنفيذ إجراءات الحماية.	3.761	0.897	7.96	0.000
4	وضع قواعد لحماية المعلومات ومعاقبة الموظفين المخلين.	3.591	1.079	5.14	0.000
5	توجد خطة حماية شاملة والتدقيق في الإجراءات الداخلية.	3.261	1.255	1.95	0.027
6	تطبق إدارة المصرف أهداف حماية المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح بها.	3.398	1.180	3.16	0.001
7	تحليل المخاطر الخاصة بالمعلومات مثل اختيار التقنية المناسبة، والإجراءات اللازمة لجعل هذه التقنية فعالة.	3.125	1.081	1.08	0.140

م	الإجراءات	المتوسط	الانحراف المعياري	قيمة t	P - value
8	تركيب طرق الحماية مثل جدران الحماية ومضادات الفيروسات.	3.068	1.230	0.52	0.303
9	تحديث طرق الحماية حسب تغيرات بيئة تكنولوجيا المعلومات.	3.148	1.218	1.14	0.129
10	توجد استراتيجية لتطوير برامج الأمن لنظم المعلومات المحاسبية الإلكترونية.	3.068	1.070	0.60	0.276
11	اكتشاف الاختراق، وتحديد ووصف نوع الاختراق.	2.909	1.274	- 0.67	0.747
12	تستخدم وسائل حماية من الكوارث الطبيعية/غير طبيعية.	2.625	1.359	- 2.59	0.994
13	توجد وسائل بديلة لتقديم الخدمة الإلكترونية في حال التعرض إلى كارثة طبيعية/غير طبيعية.	2.500	1.241	- 3.78	0.999

توضح النتائج بالجدول رقم (7) ان المشاركين في الدراسة أجابوا بالموافقة على عدم وجود مجموعة من اجراءات الحماية المقترحة بالجدول السابق والتي تشير إليها الفقرات من 7 إلى 13 حيث أجابوا بعدم وجود تحليل المخاطر الخاصة بالمعلومات مثل اختيار التقنية المناسبة، والإجراءات اللازمة لجعل هذه التقنية فعالة، وعدم تركيب طرق الحماية مثل جدران الحماية ومضادات الفيروسات، وعدم تحديث طرق الحماية حسب التغيرات الحاصلة في بيئة تطور تكنولوجيا المعلومات، ولا توجد استراتيجية لتطوير برامج الأمن لنظم المعلومات المحاسبية الإلكترونية اكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق، ولا يستخدم المصرف في منظومته الإلكترونية وسائل حماية من الكوارث الطبيعية/غير طبيعية، ولا توجد وسائل بديلة لتقديم الخدمة الإلكترونية في حال التعرض إلى كارثة طبيعية/غير طبيعية.

كما تبين النتائج بالجدول السابق ان المشاركين في الدراسة أجابوا بالموافقة على وجود مجموعة من إجراءات الحماية والتي تشير إليها الفقرات من 1 إلى 6، حيث أجابوا بان إدارة

المصرف تقوم بإصدار قرارات لتجنب مخاطر أمن المعلومات، وتهتم بتطبيق أمن المعلومات، كما تتابع الإدارة موظفي نظم المعلومات في تنفيذ إجراءات الحماية، وتقوم بوضع قواعد خاصة بحماية المعلومات ومعاقبة الموظفين المخلين بهذه القواعد، كما توجد خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية، وإدارة المصرف ايضا تطبق أهداف حماية المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح بها.

9.1 اختبار فرضيات الدراسة:

■ الجدول رقم (8) يوضح نتائج اختبار فرضيات الدراسة:

الجدول رق (8) نتائج اختبار فرضيات الدراسة

الفرضية	المتوسط	الانحراف المعياري	قيمة t	P-value
الفرضية الفرعية الأولى: لا توجد مخاطر متعلقة بإدخال البيانات تهدد نظم المعلومات المحاسبية الالكترونية.	2.9375	1.3954	1.330 -	0.905
الفرضية الفرعية الثانية: لا توجد مخاطر متعلقة بتشغيل البيانات تهدد نظم المعلومات المحاسبية الالكترونية.	2.5602	1.2506	10.43 -	0.980
الفرضية الفرعية الثالثة: لا توجد مخاطر متعلقة بالمخرجات تهدد نظم المعلومات المحاسبية الالكترونية.	2.8932	1.2674	11.86 -	0.875
الفرضية الفرعية الرابعة: لا توجد مخاطر متعلقة بالبيئة تهدد نظم المعلومات المحاسبية الالكترونية.	3.2595	1.2272	6.87	0.000
الفرضية الأساسية الأولى: لا توجد مخاطر تهدد نظم المعلومات المحاسبية الالكترونية بالمصارف التجارية العاملة في ليبيا.	2.9238	1.3036	4.07 -	0.998
الفرضية الأساسية الثانية: لا توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية في المصارف التجارية العاملة في ليبيا.	3.2134	1.1980	6.05	0.000

أظهرت النتائج بالجدول السابق بالنسبة للفرضية الفرضية الاولى أن قيمة الدلالة الاحصائية (P – value) تساوي 0.905 وهي أكبر من مستوى المعنوية 0.05 وهذا يعني قبول الفرضية التي تنص على أنه لا توجد مخاطر تتعلق بإدخال البيانات تهدد نظم المعلومات المحاسبية الالكترونية بالمصارف التجارية في ليبيا، أما بالنسبة للفرضية الفرعية الثانية أظهرت النتائج أن قيمة الدلالة الاحصائية (P – value) تساوي 0.980 وهي أكبر من مستوى المعنوية 0.05 وهذا يعني قبول الفرضية التي تنص على انه لا توجد مخاطر متعلقة بتشغيل البيانات تهدد نظم المعلومات المحاسبية الالكترونية في المصارف التجارية في ليبيا، أما بالنسبة للفرضية الفرعية الثالثة يوضح الجدول السابق أن قيمة الدلالة الاحصائية (P – value) تساوي 0.875 وهي أكبر من مستوى المعنوية 0.05 لذلك يعني قبول الفرضية التي تنص على أنه لا توجد مخاطر متعلقة بالمخرجات تهدد نظم المعلومات المحاسبية الالكترونية في المصارف التجارية في ليبيا، كما أظهرت النتائج بالجدول السابق بالنسبة للفرضية الفرعية الرابعة أن قيمة الدلالة الاحصائية (P – value) تساوي 0.000 وهي اقل من مستوى المعنوية 0.05 وهذا يعني رفض الفرضية التي تنص على أنه لا توجد مخاطر متعلقة بالبيئة تهدد نظم المعلومات المحاسبية الالكترونية في المصارف التجارية العاملة في ليبيا، كما يتضح من الجدول السابق ومن خلال نتائج الاختبار للفرضيات الفرعية أن نتائج الاختبار بالنسبة للفرضية الاساسية الاولى أظهرت ان قيمة الدلالة الاحصائية (P – value) تساوي 0.998 وهي أكبر من مستوى المعنوية 0.05 وهذا يعني قبول الفرضية الأساسية الأولى والتي تنص على أنه لا توجد مخاطر تهدد نظم المعلومات المحاسبية الالكترونية في المصارف التجارية العاملة في ليبيا، أما بالنسبة للفرضية الاساسية الثانية أظهرت النتائج أن قيمة الدلالة الاحصائية (P – value) تساوي 0.000 وهي أقل من مستوى المعنوية 0.05 وهذا يعني رفض الفرضية الاساسية الثانية والتي تنص على أنه لا توجد إجراءات حماية كافية لمواجهة مخاطر نظم المعلومات المحاسبية الالكترونية في المصارف التجارية العاملة في ليبيا.

10. النتائج والتوصيات:

أولا: النتائج:

1. عدم الموافقة على حدوث مخاطر الادخال المتعمد لبيانات غير سليمة بواسطة الموظفين ومخاطر التدمير المتعمد والتدمير غير المتعمد للبيانات بواسطة موظفي المصرف، والتأخير المتعمد لإدخال بعض البيانات والمعلومات، إدخال البيانات أكثر من مرة، وضياع أو تحريف في قاعدة البيانات الموجودة، وحذف بعض البيانات الصحيحة، وإدخال فيروس الكمبيوتر إلى النظام المحاسبي.
2. حدوث مخاطر الإدخال غير المتعمد لبيانات غير سليمة بواسطة الموظفين، والتأخير غير المتعمد لإدخال بعض البيانات والمعلومات.
3. عدم الموافقة على حدوث المخاطر المقترحة بالجدول السابق والمتعلقة بتشغيل البيانات، حيث أجابوا بعدم الموافقة على الوصول غير الشرعي للبيانات والنظام بواسطة الموظفين، ولا الوصول للبيانات والنظام بواسطة أشخاص من خارج المصرف، وعدم اشتراك الموظفين في كلمة المرور.
4. عدم التغيير المنتظم لكلمات المرور، ولا الاستخدام غير المصرح به لنظم المعالجة. سرقة وقت الحاسوب واستخدامه في الأغراض الشخصية، وكذلك عدم استخدام البرامج بطريقة غير مرخص بها، وعمل نسخ إضافية غير قانونية من البرنامج، وعدم اعتراض وصول البيانات من الخوادم إلى أجهزة المستخدمين، ولا الاحتفاظ بنسخة احتياطية للبيانات والمعلومات من قبل الموظفين غير مرخصة (غير مصرح بها) من قبل الإدارة.
5. عدم الموافقة على حدوث المخاطر المتعلقة بالمخرجات والمقترحة بالجدول السابق، حيث اجابوا بعدم طمس أو تدمير بنود معينة من المخرجات، وعدم خلق مخرجات زائفة/غير صحيحة، سرقة البيانات/المعلومات، وعدم عمل نسخ غير مصرح بها من المخرجات، والكشف غير المرخص به للبيانات والمعلومات عن طريق عرضها على شاشات العرض أو طبعها على الورق، وعدم طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك، والمطبوعات والمعلومات

الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم باستلامها.

6. عدم الموافقة على حدوث مجموعة من المخاطر المتعلقة بالبيئة والمقترحة بالجدول السابق، حيث اجابوا بعدم توصل أشخاص غير مصرح لهم من خارج المصرف (قراصنة المعلومات) إلى البيانات والنظام، وعدم وجود الفيروسات الرقمية المعروفة، قلة حدوث المجال المغناطيسي العالي، وعدم وجود خطر عوامل التأكل.

7. حدوث مجموعة من المخاطر المتعلقة بالبيئة، حيث أجابوا بحدوث مخاطر الكوارث الطبيعية مثل (الحرائق والزلازل والبراكين والأعاصير والفيضانات)، والكوارث غير الطبيعية (من صنع الأنسان) تتمثل في الحرائق المفتعلة والانفجارات وانقطاع التيار الكهربائي، والتطور التكنولوجي السريع، والمخاطر القانونية (مكافحة غسيل الأموال - مخالفة الاتفاقيات – عدم التحديد الواضح للحقوق والالتزامات)، والحرارة والرطوبة العالية، وعدم كفاية الأدوات والضوابط الرقابية المطبقة، ومشاكل التيار الكهربائي، وعدم التأمين الكافي للنظم.

8. عدم وجود تحليل المخاطر الخاصة بالمعلومات مثل اختيار التقنية المناسبة، والإجراءات اللازمة لجعل هذه التقنية فعالة، وعدم تركيب طرق الحماية مثل جدران الحماية ومضادات الفيروسات، وعدم تحديث طرق الحماية حسب التغيرات الحاصلة في بيئة تطور تكنولوجيا المعلومات، ولا توجد استراتيجية لتطوير برامج الأمن لنظم المعلومات المحاسبية الإلكترونية اكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق، ولا يستخدم المصرف في منظومته الإلكترونية وسائل حماية من الكوارث الطبيعية/غير طبيعية، ولا توجد وسائل بديلة لتقديم الخدمة الإلكترونية في حال التعرض إلى كارثة طبيعية/غير طبيعية.

9. ان إدارات المصارف تقوم بإصدار قرارات لتجنب مخاطر أمن المعلومات، وتهتم بتطبيق أمن المعلومات، كما تتابع الإدارة موظفي نظم المعلومات في تنفيذ إجراءات

الحماية، وتقوم بوضع قواعد خاصة بحماية المعلومات ومعاقبة الموظفين المخلين بهذه القواعد، كما توجد خطة حماية شاملة ومعمقة تشمل إغلاق منافذ الاختراق، والتدقيق في الإجراءات الداخلية، وإدارة المصرف ايضا تطبق أهداف حماية المعلومات مثل الخصوصية، وتجنب تغيير البيانات غير المصرح بها.

ثانيا: التوصيات:

1. الرفع من كفاءة مشغلي النظم المحاسبية الالكترونية بإلحاقهم في دورات تدريبية مكثفة على استخدامات ومهارات الحاسب الآلي لتجنب مخاطر الادخال غير المعتمد لبيانات غير سليمة من قبل الموظفين.
2. توعية الموظفين بضرورة إدخال البيانات في الوقت المناسب وعدم التأخير في إنجاز العمليات لتجنب مخاطر التأخير غير المتعمد في إدخال البيانات.
3. المحافظة على بيئة التشغيل الالكترونية والرفع من كفاءة وقدرة الوسائل اللازمة لتجنب مخاطر الكوارث الطبيعية كالحرائق والـزلازل والفيضانات وغيرها وكذلك توفير وسائل الحماية من الكوارث الغير طبيعية الحرائق المفتعلة والانفجارات وانقطاع التيار الكهربائي، والتطور التكنولوجي السريع وغيرها.
4. تحليل المخاطر الخاصة بالمعلومات مثل اختيار التقنية المناسبة، والإجراءات اللازمة لجعل هذه التقنية فعالة، وتركيب طرق الحماية مثل جدران الحماية ومضادات الفيروسات، وتحديث طرق الحماية حسب التغيرات الحاصلة في بيئة تطور تكنولوجيا المعلومات.
5. ضرورة وجود استراتيجية لتطوير برامج الأمن لنظم المعلومات المحاسبية الإلكترونية واكتشاف حوادث الاختراق من خلال التقارير، وتحديد ووصف نوع الاختراق، واستخدام وسائل حماية من الكوارث، وتوفير وسائل بديلة لتقديم الخدمة الإلكترونية في حال التعرض إلى كارثة طبيعية أو غير طبيعية.
6. حث الباحثين والمهتمين بنظم المعلومات المحاسبية الالكترونية على إجراء المزيد من الدراسات حول استكشاف مخاطر نظم المعلومات الالكترونية والتعرف على انواعها وتحديد اسبابها ووضع وسائل وإجراءات الحماية اللازمة لمواجهتها.

المراجع:

1. أبوشيبة، ابراهيم علي، الفطيمي، محمد مفتاح، (2017)، «مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية – دراسة ميدانية على المصارف التجارية في بلدية مصراته»، مجلة دراسات الاقتصاد والأعمال، المجلد الخامس، العدد: الأول.

2. ارحيم، علي أبو النور، (2006)، "دور التطورات المهنية الحديثة للمراجعة في تقويم نظام الرقابة الداخلية – دراسة تحليلية تطبيقية"، رسالة ماجستير غير منشورة، كلية التجارة والدراسات الاقتصادية والاجتماعية، جامعة النيليين.

3. البحيصي، عصام محمد، (2011)، "استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية الإلكترونية في الشركات الفلسطينية العاملة بقطاع غزة دراسة تطبيقية"، مجلة الجامعة الإسلامية، العدد الأول.

4. البحيصي، عصام محمد، حرية الشريف، (2008)، "مخاطر نظم المعلومات المحاسبية الإلكترونية، دراسة تطبيقية على المصارف العاملة في قطاع غزة "، مجلة الجامعة الإسلامية، العدد الثاني.

5. الحميدي، نجم عبدالله، عبدالرحمن الأحمد العبيد، سلوى أمين السامرائي، (2004)، "نظم المعلومات الإدارية – مدخل معاصر"، عمّان، الأردن، دار وائل للنشر والتوزيع.

6. الدلاهمة، سليمان مصطفى، (2013)، "أثر مخاطر استخدام تكنولوجيا المعلومات على أداء نظم المعلومات المحاسبية من وجهة نظر مراجعي الحسابات في المملكة العربية السعودية"، مجلة جامعة القدس المفتوحة للأبحاث والدراسات، العدد الثلاثون.

7. الساعدي، الصديق عثمان، كوثر إقجام، (2014)، " دور المراجع الداخلي في مواجهة أخطار نظم المعلومات المحاسبية الإلكترونية، دراسة حالة شركة الزاوية لتكرير النفط"، المجلة الوطنية للإدارة، العدد 13.

8. الصلاح، عماد محمد، (2009)، "مخاطر أمن نظم المعلومات المحاسبية الإلكترونية وأثرها على صحة ومصداقية القوائم المالية في البنوك التجارية"، دراسة ميدانية، جامعة آل البيت، كلية إدارة المال والأعمال.

9. العبيدي، فاطمة ناجي، (2012)، "مخاطر استخدام نظم المعلومات المحاسبية المحوسبة وأثرها على فاعلية عملية التدقيق في الأردن"، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، كلية الأعمال، قسم المحاسبة.

10. العيسى، ياسين أحمد، (2003)، "أصول المحاسبة الحديثة – الجزء الأول"، عمان: الأردن، دار الشروق للنشر والتوزيع.

11. الفيومي، محمد، (1993)، "مراجعة النظم المحاسبية المستخدمة للحاسب"، EDP AUDITNG، دار الاشعاع للنشر.

12. الهيتي، صلاح الدين، أمنة ماجد الربيحات، (2005)، "أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية، دراسة ميدانية في عدد من الوزارات الأردنية وأمانة عمّان الكبرى"، مجلة المحاسبة والإدارة والتأمين، كلية التجارة، جامعة القاهرة، العدد الخامس والستون، ص220.

13. جل، إدمون طارق، (2010)، "مدى فاعلية نظم المعلومات المحاسبية في المصارف التجارية العراقية الأهلية من وجهة نظر الإدارة"، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، قسم المحاسبة، كلية الأعمال.

14. حسين، أحمد حسين علي، (2006)، "دليلك في: تحليل وتصميم النظم، الدار الجامعية.

15. داود، حسن طاهر، (2004)، "أمن شبكات المعلومات"، الرياض، المملكة العربية السعودية، مكتبة الملك فهد، الوطنية.

16. زهيري، ماهر فؤاد، (2015)، "مخاطر أمن نظم المعلومات المحاسبية الإلكترونية واستراتيجيات مواجهتها": دراسة وصفية في المصارف السورية، رسالة ماجستير غير منشورة، جامعة تشرين، كلية الاقتصاد الثانية، قسم المحاسبة.

17. زويلف، أنعام محسن، (2009)، "طبيعة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية"، دراسة تطبيقية على شركات التأمين الاردنية، المجلة العربية للمحاسبة.

18. هاشم، أماني هاشم السيد، (2005)، "تفعيل دور المراجع في مواجهة أخطار نظم المعلومات المحاسبية الإلكترونية"، المجلة العلمية للاقتصاد والتجارة، كلية التجارة، جامعة عين شمس، القاهرة، العدد الأول.