طبيعة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية -دراسة تطبيقية على شركات التأمين الأردنية-

د. إنعام محسن حسن زويلف *

ملخص

يهدف هذا البحث إلى تسليط 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 الشركات المذكورة.

وقد أجريت الدراسة على عينة عشوائية من شركات التأمين الأردنية، حيث تم تطوير استبانة لجمع البيانات والمعلومات لهذه الغاية. وقد أظهرت الدراسة نتائج من أبرزها أن أهم تهديدات أمن نظم المعلومات المحاسبية الإلكترونية في شركات التأمين الأردنية تتمثل في: الإدخال غير المتعمد لبيانات خاطئة من قبل الموظفين، وسرقة وقت الحاسوب واستخدامه في الأغراض الشخصية، والاشتراك في كلمة المرور (السر)، والقيام بتدمير غير متعمد للبيانات من قبل الموظفين، وتوصل موظفون 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.

* أستاذ مساعد، قسم المحاسبة، جامعة الإسراء الخاصة.

The Nature of the Computerized Accounting Information Systems Security Threats: An Applied Study on Jordanian Insurance Companies

Dr. Enaam Mohsen Zuelf *

Abstract

This study aims at highlighting the threats facing the computerized accounting information systems' security, and knowing the extent to which these threats exist in Jordanian insurance companies as well as determining the important threats these companies are exposed to.

Data was collected from a random sample of Jordanian insurance companies through a questionnaire specially designed for that purpose.

The study revealed that the important security threats to computerized accounting information systems in Jordanian insurance companies are: accidental entry of bad data by employees, theft of computer time by using it for personal purposes, employees' sharing of passwords, accidental destruction of data by employees, unauthorized access to the data and system by employees, introduction (entry) of computer viruses to the system, misdirecting output to people not entitled to receive them, and unauthorized document visibility by displaying it on monitors or printed on paper.

* **Assistant Prof., Isra Private University.**

المقدمة

أدى التطور والانتشار الواسع لتكنولوجيا المعلومات والاتصالات إلى حدوث تغيرات كبيرة في الكثير من ميادين النشاط، وأصبحت وسائلها أداة أساسية في جميع المجالات. ونظراً للفوائد التي يمكن أن تصاحب استخدام هذه التكنولوجيا في العمل المحاسبي، أخذت المنظمات في التوسع بالاستعانة بها سعياً وراء مزيد من الفاعلية والكفاءة في تحقيق أهداف الوظيفة المحاسبية وتحسين مستوى أداءها.

ونتيجة لهذا الاستخدام ظهرت مخاطر وأعباء جديدة، إذ واجه أمن نظم المعلومات المحاسبية الإلكترونية العديد من التهديدات ذات الخطورة على ملاءمة وموثوقية وسلامة محتوى وتكامل وسرية المعلومات المحاسبية والتي قد ينجم عنها أضرار تتسبب في خسائر جوهرية وهامة خاصة وأن أساليب الرقابة المطبقة في المنظمات على تلك النظم لم تشهد تطوراً مماثلاً. لذا أصبحت قضية أمن نظم المعلومات المحاسبية الإلكترونية أحد الهواجس التي تؤرق مختلف المنظمات.

ولتوفير الأمن والحماية للنظم المذكورة لا بد لهذه المنظمات من اكتشاف التهديدات الأمنية التي تواجه هذه النظم وتحديد درجة أهميتها، ومن هنا غدت دراسة تهديدات أمن نظم المعلومات المحاسبية الإلكترونية مطلباً ملحاً وحاجة أساسية.

مشكلة الدراسة

لا جدل في أن استخدام وسائل تكنولوجيا المعلومات* والاتصالات في العمل المحاسبي يتيح إمكانيات وفرصاً كبيرة لخدمة المنظمة. ولكن يرافق هذا الاستخدام العديد من المخاطر، إذ يتعرض أمن وتكامل نظم المعلومات المحاسبية نتيجة استخدام تلك الوسائل العديد من التهديدات (Threats).

ويؤدي عدم تحديد هذه التهديدات وإدراك درجة أهميتها إلى حدوث مشكلات عديدة للمنظمات كإساءة استخدام المعلومات، والتعرض للابتزاز، ومواجهة الخسائر المادية والمعنوية، إضافة إلى عدم تمكنها من إيجاد الوسائل الفاعلة لحماية هذه النظم ووقايتها من التهديدات والمخاطر وتلافي ما قد ينجم عنها من أضرار جسيمة.

---

* تتمثل تكنولوجيا المعلومات (IT) Information Technology بالحاسوب الإلكتروني الذي يتم استخدامه لإنجاز المهام ذات العلاقة بالمعلومات، وتدعيم المعلومات واحتياجات تشغيلها في المنظمة، فتكنولوجيا المعلومات تشمل المكونات الصلبة للحاسوب إضافة إلى برمجيات العمل وبرمجيات أنظمة التشغيل (Haag et al.، 2000: 17).

أهمية الدراسة

تنبع أهمية هذه الدراسة من الأهمية التي تستأثر بها قضية أمن نظم المعلومات المحاسبية الإلكترونية، حيث أمست هذه القضية أحد الهواجس التي تؤرق مختلف المنظمات. فتطور وسائل تكنولوجيا المعلومات والاتصالات وتزايد استخدامها في نظم المعلومات المحاسبية، يسّر بشكل كبير خزن واسترجاع وتعديل ونسخ المعلومات والوصول إليها، مما جعل هذه النظم عرضة للعديد من المخاطر الداخلية والخارجية التي تهدد ملاءمة وموثوقية وسلامة محتوى وتكامل وسرية المعلومات المحاسبية، خاصة وأن أساليب الرقابة المطبقة في المنظمات على النظم المذكورة لم تشهد تطوراً مماثلاً. ولتوفير الحماية لنظم المعلومات المحاسبية الإلكترونية ووقايتها لا بد من اكتشاف المخاطر التي تهدد أمن هذه النظم وتحديد أهميتها النسبية، إذ يعد ذلك خطوة ضرورية لوضع الأساليب الرقابية المناسبة.

كما تنبثق أهمية هذه الدراسة من أنها من أوائل الدراسات التي حاولت التعرف على التهديدات التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في بيئة الأعمال الأردنية ولفت النظر إليها، مما ينعكس في أساليب حماية ورقابة أكثر كفاءة وفاعلية تساهم في تجنب الخسائر المحتملة المترتبة على تهديدات أمن هذه النظم في البيئة المذكورة.

أهداف الدراسة

تهدف هذه الدراسة إلى:

1. بيان التهديدات والمخاطر المحتملة التي يمكن أن يتعرض لها أمن نظم المعلومات المحاسبية الإلكترونية وما قد ينجم عن ذلك من أضرار وخسائر جسيمة، و ذلك استنادا الى الادبيات ذات العلاقة.
2. معرفة مدى وجود تهديدات تواجه أمن نظم المعلومات المحاسبية الإلكترونية في شركات التأمين الأردنية، مع تحديد اهم هذه التهديدات، و ترتيبها حسب سُلم الاهمية.
3. إظهار أهمية تحديد التهديدات ذات العلاقة بأمن نظم المعلومات المحاسبية الإلكترونية كخطوة تمهيدية ضرورية لتشخيص نقاط الضعف في أنظمة الرقابة والحماية الخاصة بتلك النظم ومعالجتها.

الإطار النظري والدراسات السابقة

الإطار النظري

مفهوم أمن المعلومات

إن استخدام مصطلح أمن المعلومات ليس جديداً فهو موجود قبل ظهور وسائل تكنولوجيا المعلومات والاتصالات، إلا أنه أصبح شائعاً ومتداولاً بكثرة بعد ولادة تلك الوسائل واستخدامها في معالجة ونقل وخزن البيانات وتداولها.

وتوجد العديد من التعاريف لمصطلح أمن المعلومات، فقد عُرف بأنه "حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنظمة نفسها والأفراد العاملين فيها وأجهزة الحاسوب المستخدمة فيها ووسائل المعلومات التي تحتوي على بيانات المنظمة، ويتم ذلك عن طريق إتباع إجراءات ووسائل حماية عدة تضمن في النهاية سلامة المعلومات" (داوود، 2000: 23).

كما عرفه (حفناوي) بأنه "علم يدعو لوضع إجراءات كافية لضمان أمن المعلومات المركزية وقواعد البيانات الموزعة" (حفناوي، 2001: 315).

أما عرب فقد عرفه من عدة زوايا "فمن زاوية أكاديمية، هو العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية، هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية، ومن زاوية قانونية، هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها أي جرائم الحاسوب" (عرب، 2002: 67).

أهمية أمن نظم المعلومات المحاسبية الإلكترونية

أصبحت نظم المعلومات المحاسبية تتطور بشكل سريع وتزداد تعقيداً مع زيادة اعتماد المجتمع عليها لتتمكن من تلبية الاحتياجات المختلفة لمستخدمي المعلومات، وبالمقابل شهدت المنظمات نمواً مطرداً في المخاطر التي تتعرض لها نظم معلوماتها المحاسبية. فقد أشار المعهد القومي الأمريكي للمعايير والتكنولوجيا بأن النظم الإلكترونية عرضه للعديد من التهديدات والمخاطر التي من الممكن أن تسبب للمنشأة العديد

من الأضرار وتؤدي إلى خسائر جوهرية جسيمة (National Institute of Standards and Technology، 1995) ، الأمر الذي يهدد صحة وموثوقية وتكامل البيانات والمعلومات، كما بينت إحدى الدراسات المسحية الحديثة على سبيل المثال حصول اختراقات أمنية في أنظمة المعلومات المحاسبية في 67 % من الشركات الأمريكية في السنة الأخيرة، كما أظهرت التقارير المالية لـ 60 % من هذه الشركات بأنها تكبدت خسائر مالية نتيجة ذلك. (Romney & Steinbart، 2006: 144)

وعليه فهناك حاجة ماسة لحماية البيانات والمعلومات التي قد يؤدي فقدانها أو تغيرها أو مجرد الإطلاع عليها إلى حدوث العديد من المشاكل مثل التعرض للتهديد وإساءة الاستعمال ومواجهة الخسائر المادية والمعنوية، ومن هنا أصبحت مسألة أمن نظم المعلومات المحاسبية الإلكترونية أحد الهواجس التي تؤرق المنظمات المستخدمة لهذه النظم.

تهديدات أمن نظم المعلومات المحاسبية الإلكترونية

تواجه نظم المعلومات المحاسبية الإلكترونية في المنظمات العديد من التهديدات الأمنية. وقبل الخوض في أنواع التهديدات، لا بد من توضيح بعض المصطلحات المستخدمة في هذا المجال. فمصطلح التهديد (Threat) يشير إلى أي حدث معادي مقصود أو أي حدث غير مقصود يمكن أن يتسبب في أضرار لنظام المعلومات المحاسبي أو للمنشأة. أما أثر التهديد (Impact or Exposure) فيعني الخسائر المادية التي تحدث نتيجة حصول التهديد. كما يشير مصطلح الاحتمال الأرجح (Likelihood) إلى قوة احتمال حدوث التهديد (Romney & Steinbart، 2006: 191).

وتصنف التهديدات التي يتعرض لها أمن النظم المذكورة وفقاً للعديد من الأسس، إذ يمكن تصنيفها:

- حسب المصدر (Source): إلى تهديدات داخلية وتهديدات خارجية.
- حسب المسبب فيها (Perpetrator): إلى تهديدات ناتجة عن العنصر البشري وتهديدات ناتجة عن العنصر غير البشري.
- حسب العمدية أو القصدية (Intention): إلى تهديدات ناتجة عن تصرفات متعمدة وتهديدات ناتجة عن تصرفات غير متعمدة.
- حسب علاقتها بمراحل النظام إلى تهديدات المدخلات (Input) و تهديدات المعالجة (Processing) وتهديدات المخرجات (Out put)، كما هو موضح في الشكل رقم (1).

وبصفة عامة تواجه نظم المعلومات المحاسبية الإلكترونية في المنظمات التهديدات الأمنية الآتية:

- التهديد الأول:

الكوارث الطبيعية والسياسية مثل الحرائق،والفيضانات والزلازل، والبراكين، والحروب، وهجمات

الإرهابيين. فالكوارث التي لا يمكن التنبؤ بها تستطيع تدمير نظام المعلومات المحاسبي بشكل كامل وتتسبب في فشل المنظمة، ويمكن أن يؤثر حدوث هذه الكوارث في العديد من المنظمات في آن واحد.

- التهديد الثاني:

أخطاء البرمجيات وفشل وظائف المعدات (Equipment functions) مثل فشل المكونات الصلبة للحاسوب (Hardware Failures)، وعطل البرمجيات (Software bugs)، وانهيار نظام التشغيل، وانقطاع وتقلب التيار الكهربائي، وأخطاء إرسال البيانات التي لم يتم الكشف عنها.

- التهديد الثالث:

التصرفات غير المقصودة مثل الحذف والأخطاء غير المقصودة والتي تُعرّض نظم المعلومات لمخاطر جسيمة وخسائر فادحة. فقد قدرت جمعية أمن نظم المعلومات المحاسبية (The Information Systems Security Association) أن 65 % من المشاكل ذات العلاقة بأمن هذه النظم سببها أخطاء العنصر البشري، وأن التصرفات غير العمدية للعنصر البشري تنتج عن الإهمال، والإخفاق في إتباع الإجراءات المرسومة، وضعف تدريب الأفراد والإشراف عليهم. فالمستخدمين للنظام غالباً ما يخسرون البيانات أو يضعونها في الأماكن غير الصحيحة ويمحون أو يبدلون الملفات والبيانات والبرامج بشكل غير مقصود. كما أن مشغلي الحاسوب والمستخدمين يمكن أن يقوموا بإدخال خاطئ أو إدخال مدخلات غير صحيحة، واستخدام نسخة خاطئة من البرنامج والتعامل مع الملفات غير الصحيحة للبيانات أو وضعها في الأماكن غير الصحيحة. أما محللي الأنظمة والمبرمجين فيمكن أن يقوموا بعمل أخطاء منطقية وتطوير أنظمة لا تفي باحتياجات المنظمة وغير قادرة على التعامل مع المهام المستهدفة لها، أو ممكن اختراقها بسهولة من قبل المهاجمين.

- التهديد الرابع:

التصرفات العمدية أو المقصودة والتي يشار إليها عادة كجرائم للحاسوب، وأغلب أنواع جرائم الحاسوب هو ما يعرف بالخداع أو الحيلة (Fraud) وفيه تكون النية موجهة نحو سرقة شيء ذو قيمة، ومن الأمثلة على جرائم الحاسوب: الكشف غير المصرح به عن البيانات، والعرض غير الصحيح للمعلومات، وتخصيص الموجودات لأغراض غير مصرح بها. ويمكن أن يتخذ هذا النوع من التهديد أيضاً شكل التخريب (Sabotage) وتكون النية فيه تحطيم أو إلحاق الأذى بالنظام أو بعض مكوناته.

وتتعرض أنظمة المعلومات بشكل متزايد للتهديد المتمثل بالتصرفات العمدية، فعلى مدار السنوات الثلاث الأخيرة أرتفعت نسبة شبكات نظم المعلومات التي تتعرض لهذا الخطر إلى 700 %، ولكن هذا هو الجزء الظاهر من جبل الجليد فقط، فكما يعتقد الخبراء أن العدد الحقيقي للحوادث هو أكثر من (6) مرات عما هو مقدر نظراً لعدم قيام غالبية المنظمات بالتقرير عن الاختراقات الأمنية لنظم معلوماتها

المحاسبية (Romney & Steinbart، 2006: 144-146).

وفي دراسة أجراها معهد أمن الحاسوب (CSI) بين أن حوالي ثلثي المنظمات في الولايات المتحدة الأمريكية على الأقل تعاني من جرائم الحاسوب كل عام، ومن المحتمل أن يزداد هذا المقدار ليصل إلى 90 % من السنوات القادمة لجميع المنظمات الأمريكية. ويرجع سبب الارتفاع المستمر في معدل جرائم الحاسوب إلى نمو وتطور وسائل تكنولوجيا المعلومات والاتصالات، وزيادة معرفة الأفراد بشكل عام في استخدام الحواسيب وبالشكل الذي جعل الأنظمة الإلكترونية عرضة للتهديد والمخاطر، وضخامة حجم الإنفاق السنوي على الحواسيب مقارنة مع الإنفاق على وسائل الرقابة عليها إذ أن هناك فجوة واسعة بين الاثنين (Moscove et al.، 1999: 270)

وتجدر الإشارة إلى أن أكثر مواطن (Area) بيئة نظم المعلومات المحاسبية الإلكترونية عرضة للتهديد هي: نظام التشغيل، وإدارة البيانات، والهيكل التنظيمي للوظائف ذات العلاقة بخدمات الحاسوب، وتطوير الأنظمة، وصيانة الأنظمة، ومركز الحاسوب (Hall، 2004: 77).

لماذا تتزايد تهديدات أمن نظم المعلومات المحاسبية الإلكترونية؟ (Romney & Steinbart, 2006: 190-191)

يشكل تكامل النظم الإلكترونية والرقابة عليها قضية هامة في عالم اليوم، فلقد ازدادت الدراسات التي تتناول رقابة المخاطر ذات الصلة بهذه النظم في السنوات القليلة الماضية، وكشفت هذه الدراسات عن أن 60 % من المنظمات تعاني من إخفاقات هامة في مجال الرقابة على هذه النظم في الآونة الأخيرة. ومن أهم الأسباب التي أدت إلى تزايد المشاكل الأمنية المتصلة بهذه النظم هي:

1. زيادة عدد أنظمة المعلومات في المنشأة، وبالشكل الذي أدى إلى إتاحة المعلومات لعدد كبير من العاملين دون تحديد أولويات للحصول عليها.
2. صعوبة الرقابة على شبكات الحاسوب الموزعة (Distributed computer Networks)، مقارنة مع الحواسيب الكبيرة المركزية (Centralized mainframe).
3. تُمكّن الشبكات التي تغطي مساحة واسعة العملاء والمجهزين من الدخول إلى أنظمة وبيانات بعضهم البعض، الأمر الذي جعل من الثقة محل قلق واهتمام المنظمات المستخدمة لهذه النظم.

وتاريخياً، نجد أن العديد من المنظمات لم تقم بتوفير الحماية الكافية لبياناتها نتيجة لـ:

- عدم التقدير الكافي لأهمية مشاكل الرقابة ذات العلاقة بالحاسوب والنتائج السلبية المترتبة عليها، إذ تنظر المنظمات إلى خسارة المعلومات الحساسة كتهديد بعيد الحدوث وضعيف الاحتمال، فالمشاركين في دراسة (Ernst & Young) الذين يعتقدون بأهمية قضية أمن الحاسوب قد انخفض من 35 % إلى 25 % على مدى سنة واحدة.

- عدم الفهم الكامل لتطبيقات الرقابة على التحول من أنظمة الحاسوب القائمة على أساس مركزي إلى أنظمة الحاسوب القائمة على أساس الشبكات والإنترنت.
- عدم إدراك العديد من المنظمات أن أمن البيانات وهو أمر حاسم للبقاء، فالمعلومات هي أحد الموارد الإستراتيجية وتُعد حمايتها أحد المتطلبات الإستراتيجية.
- الضغط باتجاه زيادة الإنتاجية وتخفيض التكاليف حثَّ الإدارة على تجاهل الإجراءات الرقابية في هذا المجال.

وتجدر الإشارة إلى أن تعرف المنظمة على التهديدات التي تواجه أمن نظم معلوماتها المحاسبية الإلكترونية وتحديد درجة أهميتها هو أمراً ضرورياً لتشخيص نقاط الضعف في نظام الرقابة الداخلية المتعلقة بهذه التهديدات، من أجل تطبيق الأساليب والإجراءات الرقابية المناسبة لحماية هذه النظم من الاعتداءات وتلافي ما قد ينجم عنها من مشكلات وخسائر جسيمة.

الدراسات السابقة

على الرغم من أهمية وحيوية موضوع التهديدات التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في بيئة تشهد تطورات متسارعة في تكنولوجيا المعلومات والاتصالات، إلا أننا نجد شحة في الدراسات التي تناولت هذا الموضوع بشكل خاص، وقد تم الحصول على القليل من الدراسات ذات الصلة المباشرة بموضوع البحث، إضافة إلى بعض الدراسات حول أمن المعلومات بشكل عام.

فقد قام الهيتي والربحيات (2005) بدراسة هدفت إلى التعرف على أثر التهديات الأمنية بمصادرها الداخلية والخارجية في أمن المعلومات بنتائجها المباشرة وغير المباشرة في ضوء تطبيق الحكومة الإلكترونية، حيث تم إجراء دراسة ميدانية في عدد من الوزارات الأردنية وأمانة عمان الكبرى. وخلصت الدراسة إلى ضرورة التنبه إلى خطورة التهديدات الداخلية على أمن المعلومات وتوفير سياسة أمنية تحافظ على الموثوقية والخصوصية والتكاملية لكل منظمة تسعى إلى المحافظة على النظام المعلوماتي بأكمله لدعم نجاح الحكومة الإلكترونية.

واختبر أبو موسى (2004) المخاطر الرئيسة والهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشآت السعودية، وأشارت الدراسة إلى أن هناك العديد من المخاطر التي يتعرض لها أمن هذه النظم في المنشآت السعودية، من أبرزها الإدخال غير المتعمد والمتعمد للبيانات من قبل موظفي المنشأة، والتدمير غير المتعمد والمتعمد للبيانات من قبل موظفي المنشأة، واشتراك الموظفين في استخدام نفس كلمات السر، وإدخال فيروسات إلى النظام.

وسعى Kankanhalli وزملاؤه (2003) إلى تطوير نموذج متكامل للفاعلية الأمنية لنظام المعلومات واختباره عملياً. وأهم ما توصلوا إليه أن المنظمات الصغيرة والمتوسطة الحجم تمارس نشاطات رادعة أقل من المنظمات الكبيرة الحجم لضمان أمن نظام المعلومات، وتزداد الإجراءات الوقائية في المنظمات التي تدعم إدارتها العليا نظام المعلومات مقارنة مع المنظمات التي لا تدعم إدارتها العليا النظام المذكور، وتطبق المنظمات المالية إجراءات مشددة على أمن المعلومات أكثر من بقية المنظمات، وأن الجهود الرادعة والوقائية لحماية المعلومات تعزز الفاعلية الأمنية لنظام المعلومات.

كما ناقش أبو موسى (2002) المخاطر الرئيسة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية وكفاية أنظمة الحماية المطبقة في البنوك المصرية. وبينت نتائج الدراسة أن الإدخال غير المتعمد لبيانات غير صحيحة من قبل موظفي البنوك، والتدمير غير المتعمد للبيانات من قبل الموظفين، وإدخال فيروس الحاسوب إلى النظام، والكوارث الطبيعية، والكوارث من صنع الإنسان، واشتراك الموظفين في استخدام نفس كلمة السر، وتوجيه البيانات والمعلومات إلى أشخاص غير مخول لهم باستلامها، تُعد من أهم المخاطر التي تواجه أمن النظم المذكورة. كما قدمت الدراسة بعض المقترحات لتلافي نقاط ضعف أنظمة الحماية في قطاع البنوك المصري.

وقيّم Ryan & Bordoloi (1997) تهديدات أمن نظم المعلومات المحاسبية الإلكترونية في المنظمات التي تحولت من نظام الحواسيب الكبيرة Main Frames إلى نظام خدمة العملاء Client-Server. وأظهرت نتائج الدراسة أن هناك فروق جوهرية بين المنشآت التي تطبق نظام الحواسيب الكبيرة وتلك التي تطبق نظام خدمة العملاء بالنسبة لتهديدات التدمير المتعمد وغير المعتمد للبيانات من قبل موظفي المنظمة، والإدخال المتعمد وغير المتعمد لبيانات خاطئة بوساطة الموظفين، وكذلك الخسائر الناتجة عن عدم إعداد نسخ إضافية Backups، والرقابة على ملفات الدخول للنظام Log Files، وفشل النظام.

وركز Henry (1997) على مدى تطابق النظرية مع الممارسات العملية، إذ توصل من خلال مسح ميداني شمل 261 شركة بولاية فرجينيا الأمريكية إلى طبيعة وخصائص أمن نظم المعلومات المحاسبية الإلكترونية المطبقة في تلك الشركات، حيث بينت الدراسة مدى قيام الشركات عينة البحث بعمل نسخ إضافية للبيانات والنظام المحاسبي، واستخدام كلمات السر لحماية هذا النظام، وتوفير الحماية الكافية للنظام ضد تهديدات فيروسات الحاسوب، وتوفير الحماية المادية اللازمة للنظم المحاسبية وفيما يتعلق بتوثيق ومشروعية التغييرات في تلك النظم، وتشفير البيانات، ومراجعة البيانات والبرامج المحاسبية الإلكترونية بوساطة برامج للمراجعة.

وفحص Davis (1996 and 1997) حالة أمن نظم المعلومات المحاسبية الإلكترونية في الواقع العملي بوساطة دراسة تطبيقية شملت عينة من جمعية مراقبة ومراجعة نظم المعلومات

Information Systems Audit and control Association (ISACA)، وأعضاء مجمع المحاسبين القانونيين الأمريكي American Institute of Certified Accountants (AICPA). وأظهرت نتائج الدراسة أهم التهديدات التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في كل من بيئة الحواسيب الشخصية (Micro computer)، وبيئة الحواسيب الصغيرة Mini Computer، وبيئة الحواسيب الكبيرة Main Frames، وبيئة الشبكات Networks كما تبيّن أن موقف الإدارة تجاه الرقابة الداخلية يُعد أحد المكونات الهامة للبيئة الرقابية، حيث أن وجود سياسات خاصة بأمن أنظمة المعلومات ووضعها موضع التنفيذ يشير إلى تعهد الإدارة بحماية أمن المعلومات.

وتناول البياتي (1996) تحديد عناصر أمن الحواسيب وأسس التصنيف لتحديد مستوى الأمنية والوسائل الفنية وغير الفنية لحماية الحواسيب، إذ قام بإجراء مسح على عدد من المنظمات العراقية للتعرف على نسبة المنظمات التي تعتمد أنظمة أمنية وخطط وسياسات أمن وحماية، فضلاً عن معرفة أكثر التهديدات أهمية وإثارة لاهتمام المستخدمين. وخلصت الدراسة إلى أن الحاجة الأمنية معترف بها رسمياً في معظم المنظمات التي شاركت في الدراسة، وأن على كل دولة إصدار تشريع دقيق وواضح لمعالجة الاعتداء على المال المعلوماتي.

ومن الدراسات الأولى والرائدة التي تناولت موضوع تهديدات أمن نظم المعلومات المحاسبية الإلكترونية الدراسة التي قدمها Loch و آخرون (1992)، وتطرقت إلى مدى إدراك مديري نظم المعلومات الإدارية في الولايات المتحدة الأمريكية للتهديدات الأمنية التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في بيئة الحواسيب الشخصية والحواسيب الكبيرة والشبكات، حيث طُلب من المدراء المشاركين في الدراسة ترتيب أهم ثلاث تهديدات تتعرض لها النظم المذكورة من بين قائمة تضم عدة تهديدات محتملة. وأشارت نتائج الدراسة إلى أن الكوارث الطبيعية والأحداث غير المقصودة للموظفين قد تم تصنيفها ضمن التهديدات الهامة في جميع بيئات تكنولوجيا المعلومات، كما تم إعطاء أهمية أكبر للتهديدات الداخلية مقارنة بالتهديدات الخارجية لأمن أنظمة المعلومات المحاسبية الإلكترونية.

يتضح مما تقدم، أن أغلب الدراسات التي تم استعراضها والمتعلقة بأمن نظم المعلومات المحاسبية الإلكترونية قد تمت في بيئة الدول المتقدمة. كما يلاحظ أن بعض البنود التي تضمنتها قوائم استبانة تلك الدراسات (عدا دراستي أبو موسى) صنفت كتهديدات لأمن نظم المعلومات المحاسبية الإلكترونية، في حين أنها لا تُعد من ضمن هذه التهديدات إذ تمثل في حقيقتها ضعف وسائل الحماية وعدم كفاية الضوابط الرقابية ذات العلاقة بأمن النظم المذكورة مثل ضعف الرقابة على وسائل حفظ وتخزين المخرجات، وعدم الفصل الجيد بين الوظائف المتعارضة في أقسام المحاسبة والحاسوب، وضعف الرقابة المادية على النظام.

منهجية الدراسة

فرضيات الدراسة

بناء على الإطار النظري للدراسة والدراسات السابقة يمكن صياغة فرضيات الدراسة على النحو الآتي:

1. HO1: "توجد تهديدات تواجه أمن نظم المعلومات المحاسبية الإلكترونية في شركات التأمين الأردنية".
2. HO2: "تدرك شركات التأمين الأردنية أهم التهديدات التي تواجه أمن نظم معلوماتها المحاسبية الإلكترونية".

مجتمع الدراسة وعينتها

تكتسب قضية أمن نظم المعلومات المحاسبية الإلكترونية أهمية خاصة في المنشآت المالية، نظراً لتعامل هذه المنشآت بشكل رئيس بأصول عالية السيولة والتي تكون أكثر عرضة للسرقة والاختلاس، فضلاً عن كثرة استخدامها لوسائل تكنولوجيا المعلومات. ويكشف تاريخ جرائم الكمبيوتر عن أن النسبة العظمى من الجرائم المشهورة في هذا المجال قد تم تنفيذها في منشآت مالية. ومن هنا جاء اختيار قطاع التأمين الأردني لتطبيق هذه الدراسة.

يبلغ عدد شركات التأمين العاملة في السوق الأردني (26) شركة (الاتحاد الأردني لشركات التأمين، 2006). تم اختيار 14 شركة منها عشوائيا، وتمثل الشركات الخاضعة للدراسة (54 %) تقريباً من مجموع شركات التأمين الأردنية. ويتضمن الملحق رقم (2) اسماء هذه الشركات.

أما بالنسبة لأفراد عينة البحث، فقد توزعوا على ثلاث فئات هم العاملين من قسم المحاسبة والتدقيق الداخلي والحاسوب. وقد تم إطلاق تسمية العاملين في مجال المحاسبة على منتسبي قسم المحاسبة وبغض النظر عن عناوينهم الوظيفية، وتسمية العاملين في مجال التدقيق الداخلي على منتسبي قسم التدقيق الداخلي وبغض النظر عن عناوينهم الوظيفية، وتسمية العاملين في مجال الحاسوب على منتسبي قسم الحاسوب وبغض النظر عن عناوينهم الوظيفية. وقد تم توزيع الاستمارات عليهم بشكل متساوي تقريباً، وبلغ عدد الاستمارات الموزعة (216) استمارة استرد منها (136) استمارة واستبعد منها (16) استمارة لعدم صلاحيتها للتحليل، وبذلك خضعت للتحليل (120) استمارة.

أسلوب جمع البيانات

اعتمدت الدراسة على مجموعة من المراجع والدراسات المنشورة ذات الصلة بموضوع البحث لبناء الإطار النظري. وفي الجانب الميداني استخدم أسلوب قائمة الاستبانة في جمع البيانات، إذ تم تطوير قائمة اشتملت على (21) بنداً من التهديدات المحتملة لأمن نظم المعلومات المحاسبية الإلكتروني بالاعتماد على الأدبيات ذات العلاقة وقوائم الاستبانة الواردة في الدراسات السابقة ذات العلاقة المباشرة بموضوع البحث التي تم استعراضها. وقد تضمنت القائمة الحالية بعض التهديدات التي يتم اختبارها ميدانياً للمرة الأولى.

وتكونت الاستبانة من قسمين، هدف الأول إلى الحصول على معلومات عامة عن الشركات محل البحث وأفراد العينة. إما القسم الثاني فقد هدف إلى التعرف على أهم التهديدات التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في الشركات الخاضعة للدراسة، وبيان مدى إدراك هذه الشركات لدرجة أهمية أو خطورة هذه التهديدات من خلال تحديد معدلات تكرار حدوثها في بيئة العمل وهو نفس الأسلوب الذي استخدم في دراستي (أبو موسى، 2002 و 2004).

وللتثبت من دقة صياغة الاستبانة ودرجة تطابق ما تقصده الدراسة مع ما يفهمه المستقصي منها تم القيام بالتطبيق الاستطلاعي على عينة تكونت من 24 شخصاً من العاملين في أقسام المحاسبة والتدقيق الداخلي والحاسوب في بعض الشركات الخاضعة للدراسة، حيث عرضت الاستبانة عليهم وتم الأخذ بملاحظاتهم عند صياغة الاستمارة بشكلها النهائي.

وللتحقق من مصداقية الاستبانة تم عرضها على هيئة من المحكمين ذوي التخصص لإبداء آرائهم بهذا الخصوص وقد جرى الأخذ بملاحظاتهم كما تم اختبار ثبات أداة الدراسة باستخدام اختبار الفاكرونباخ (Cronbch Alpha)، وقد بلغت قيمة معامل الثبات 93 %.

الأساليب الإحصائية المستخدمة في البحث

تم استخدام حزم البرامج الإحصائية (SPSS) لإجراء التحليلات الإحصائية للبيانات والوصول إلى النتائج، ومن الأساليب التي تم تطبيقها:

1. مقاييس الإحصاء الوصفي كالتكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية لوصف عينة البحث وتحليل البيانات المتعلقة بها.
2. تحليل التباين باتجاه واحد (One Way Anova) لاختبار مدى تجانس مجتمعات فئات عينة البحث توطئة للجمع بينها في عينة واحدة أو فصلها إلى ثلاث عينات متمايزة.
3. اختبار (ت) لعينة واحدة (One Sample T Test).

4. اختبار إشارة الرتب (ولكوكسون) (Wilcoxcon Signed Ranked Test) الذي يستخدم لاختبار الفرضيات ذات الإحصاءات اللامعلمية (Bouverman & Oconnell، 2001، Ch: 9; Conver، 1980: 28).

حدود الدراسة

لا تتناول هذه الدراسة أساليب الرقابة على نظم المعلومات المحاسبية الإلكترونية ووسائل الحماية الخاصة بها. كما لا تتطرق إلى التشخيص الدقيق لأسباب حدوث التهديدات التي يتعرض لها نظام المعلومات المحاسبية الإلكترونية في الشركات عينة البحث ووسائل معالجتها.

تحليل بيانات الدراسة واختبار الفرضيات

لغرض استخراج وتحليل النتائج الإحصائية الخاصة بأسئلة الاستبانة، تم التعامل مع فئات عينة البحث (العاملين في مجال المحاسبة، والعاملين في مجال التدقيق الداخلي، والعاملين في مجال الحاسوب) على أنها تمثل عينة واحدة متجانسة تنتمي إلى مجتمع طبيعي واحد. وذلك استناداً إلى نتائج تحليل التباين لاستجابات هذه الفئات على أسئلة الاستبانة، إذ كانت F المحسوبة (0.049) وهي أقل من الجدولية البالغة (4.605) وبمستوى معنوية (0.01)، مما يدل على عدم وجود فروق جوهرية ذات دلالة إحصائية بين استجابات الفئات الثلاث، وعليه تُعد العينة المختلطة المكونة من الفئات المذكورة عينة واحدة متجانسة.

خصائص أفراد عينة الدراسة:

يبين الجدول (1) أن العاملين في مجال المحاسبة قد شكلوا أعلى نسبة من أفراد العينة إذ بلغت (40 %)، تلاها العاملون في مجال الحاسوب حيث كانت نسبتهم (33.3 %)، أما أقل نسبة فكانت للعاملين في مجال التدقيق الداخلي إذ بلغت (26.7 %).

وفيما يتعلق بمتغير المؤهل العلمي، يظهر الجدول رقم (2) ان فئة حملة البكالوريوس مثلت الفئة الأعلى بنسبة (85 %). وهذا يشير إلى تفضيل الشركات محل الدراسة توظيف ذوي المؤهلات العلمية.

إما بالنسبة لمتغير الخبرة، فان الجدول رقم (3) يشير الى ان أعلى نسبة كانت فئة (5 سنوات فأقل) إذ بلغت (49.2 %)، تليها فئة (10 سنوات فأكثر) بنسبة (30 %)، فالفئة (6-10 سنوات) بنسبة (20.8 %). ويمكن القول أن العاملين في المجالات المذكورة لا يمتلكون الخبرة الطويلة، إذ أن نصف أفراد العينة تقريباً لديهم خبرة 5 سنوات أو أقل.

وفيما يخص متغير الدورات التدريبية في مجال الحاسوب والخدمات الإلكترونية، يوضح الجدول رقم (4) أن أعلى نسبة من أفراد العينة تركزت في فئة (3 فأقل) إذ بلغت (75.8 %)، تلتها فئة (4-7) بنسبة (16.7 %)، ثم فئة (7 فأكثر) بنسبة (7.5 %). وهذا يعكس قلة اهتمام الشركات المبحوثة بتطوير كوادرها في هذا المجال.

تحليل إجابات الأسئلة العامة

اشتمل هذا المحور على أربعة أسئلة عرضت الثلاثة الاولى منها في الجدول رقم (5) ، فيما تضمن الجدول رقم(6) السؤال الرابع، وتشير إجابات أفراد العينة الملخصة نتائجها في الجدول رقم (5) إلى أن جميع الشركات المبحوثة تطبق نظام محاسبي إلكتروني، حيث يُعتمد الحاسوب في العمل المحاسبي لهذه الشركات. كما أن (75 %) من المستجيبين يؤكدون استخدام شبكة الإنترنت في إنجاز الأعمال وتقديم الخدمات، أي أنها تستخدم بدرجة كبيرة في الشركات المذكورة. وتؤكد إجابات (65 %) من أفراد العينة أن الشركات محل الدراسة لا تقوم بتطوير الممارسات والضوابط الرقابية باستمرار لكي تتناسب مع التطورات في تكنولوجيا المعلومات والاتصالات المستخدمة في أعمالها، وهذا يعني أنها تقوم بهذا التطوير بدرجة ضعيفة نسبياً.

كما يوضح الجدول رقم (6) أن (25.8 %) من الإجابات تفيد بحدوث خسائر مالية في الشركات محل البحث نتيجة لتصرفات داخلية لخرق أمن نظام المعلومات المحاسبين، بينما تشير (9.2 %) من الإجابات إلى حدوث الخسائر المالية نتيجة لتصرفات خارجية لخرق أمن النظام المذكور. إما الإجابات التي أيدت حدوث تلك الخسائر نتيجة لتصرفات داخلية وخارجية فكانت نسبتها ضعيفة إذ بلغت 1.7 %. وبناء على ما تقدم فإن نسبة الإجابات التي تؤكد حدوث الخسائر المالية نتيجة حصول الخروقات في أمن نظام المعلومات المحاسبي وبغض النظر عن مصادرها هي (36.7 %). أما الإجابات التي أفادت بعدم حدوث خسائر مالية نتيجة التصرفات الداخلية أو الخارجية لخرق أمن هذا النظام، فبلغت نسبتها 63.3 %.

وتجدر الإشارة إلى أن المنظمات بصفة عامة لا تقوم بالإفصاح عن خسائرها المالية بسبب خروقات أمن أنظمة معلوماتها المحاسبية خوفاً من التأثير السلبي لهذا الإفصاح على سمعتها ومركزها التنافسي.

اختبار الفرضيات

اختبار الفرضية الأولى:

HO1: "توجد تهديدات تواجه أمن نظم المعلومات المحاسبية الإلكترونية في شركات التامين الأردنية".

تهدف الأسئلة الواردة في الجدول رقم (7) إلى بيان مدى وجود تهديدات تواجه أمن نظام المعلومات المحاسبية الإلكترونية في الشركات المبحوثة. ويلاحظ أن لدى أفراد العينة قناعة كافية بوجود تلك التهديدات، حيث جاء المتوسط الحسابي الكلي للإجابات عن هذه الأسئلة مرتفعاً فقد بلغ (3.933) أو بنسبة (79.32 %)، كما كانت الإجابات منسجمة مع بعضها إذ تراوحت قيم الانحرافات المعيارية لها بين (0.631-0.462).

وللتحقق من الدلالة الإحصائية للنتائج أعلاه، ولاختبار الفرضية الأولى تم استخدام اختبار (Wilcoxcon)، وتبين نتائج الاختبار الموضحة في الجدول رقم (8) بأن قيمة (Wα) أكبر من قيمة (T+) بمستوى معنوية (0.05)، وهذا يعني قبول الفرضية الأولى بدرجة ثقة (95 %). مما يدل على وجود تهديدات تواجه أمن النظم المذكورة.

الفرضية الثانية:

HO2: "تدرك شركات التامين الأردنية أهم التهديدات التي تواجه أمن نظم معلوماتها المحاسبية الإلكترونية".

تقيس الأسئلة الواردة في الجدول رقم (9) درجة أهمية التهديدات التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في الشركات المبحوثة، وذلك من خلال سؤال أفراد العينة عن تكرار حدوث هذه التهديدات.

ويتضح من إجابات أفراد العينة أن الإدخال غير المتعمد لبيانات خاطئة من قبل الموظفين، وسرقة وقت الحاسوب واستخدامه في الأغراض الشخصية، والاشتراك في كلمة المرور، والتدمير غير المتعمد للبيانات، والتوصل غير المصرح به للبيانات والنظام من قبل الموظفين، وإدخال فيروسات الحاسوب للنظام، وتوجيه المخرجات عن طريق الخطأ إلى أشخاص غير مصرح لهم باستلامها، والكشف غير المرخص عن البيانات والمعلومات بعرضها على شاشة الحاسوب أو طباعتها على الورق، هي من أهم التهديدات فهي ذات معدلات حدوث مرتفعة. فقد بلغت المتوسطات الحسابية لها على التوالي (3.70، 3.61، 3.59، 3.57، 3.55، 3.53، 3.52، 3.51) وبأهمية نسبية (74 %، 72.20 %، 71.80 %، 71.40 %، 71 %، 70.60 %، 70.40 %، 70.20 %).

كما يرى المشاركون في الدراسة أن القيام بطباعة وتوزيع المعلومات من قبل موظفين غير مصرح لهم، وطمس أو تدمير بنود معينة من المخرجات، والنسخ غير المصرح به للمخرجات، هي تهديدات ذات معدلات تكرار متوسطة حيث كانت المتوسطات الحسابية لها (2.61، 2.59، 2.55) وأهميتها النسبية (52.20 %، 51.80 %، 51 %) على التوالي.

ويمكن أن يعود سبب تعرض نظام المعلومات المحاسبية الإلكترونية في الشركات محل البحث للتهديدات المذكورة إلى الأخطاء الناتجة عن قلة الخبرة والمهارة لدى هؤلاء الموظفين، إضافة إلى ضعف اهتمام الشركات قيد الدراسة بالتدريب وتطوير كوادرها في هذا المجال. فقد بينت الدراسة أن أفراد العينة الذين يقعون ضمن فئة الخبرة (5 سنوات فأقل) يشكلون أعلى نسبة منها، إذ بلغت 49.2 %. كما أن (75.8 %) من المبحوثين قد حصلوا فقط على (3 دورات تدريبية أو أقل) من مجال الحاسوب والخدمات الإلكترونية. كما يمكن أن يرجع ذلك إلى ضعف أساليب الرقابة على التطبيقات ذات العلاقة بالعمليات المحاسبية (الرقابة على المدخلات وعمليات المعالجة والمخرجات) وكذلك أساليب الرقابة على التطبيقات الأخرى والتي يطلق عليها في بعض الأحيان أساليب الرقابة العامة كأساليب الرقابة على العاملين مثل الفصل بين الوظائف المتعارضة والإصرار على منح الموظف إجازة سنوية... الخ[×].

وتؤكد آراء أفراد العينة ندرة حدوث التهديدات الآتية: توصل أشخاص غير مصرح لهم من خارج الشركة (قراصنة المعلومات) إلى البيانات والنظام، والقيام بإدخال متعمد لبيانات غير سليمة من قبل الموظفين، وخلق مخرجات غير صحيحة للنظام، ومقاطعة تحويل البيانات من أماكن متباعدة، والتدمير المتعمد للبيانات من قبل الموظفين، و منع أشخاص لهم حق الدخول إلى النظام من ممارسة هذا الحق، وسرقة البيانات والمعلومات، والكوارث غير الطبيعية، والكوارث الطبيعية، وإسناد مهمة إتلاف المخرجات الحساسة التي لم يعد بحاجة إليها إلى أشخاص لا تتوافر فيهم الأمانة.

ويمكن تفسير انخفاض معدل تكرار حدوث تهديد مقاطعة تحويل البيانات المتراسلة عبر شبكات الاتصال السلكية واللاسلكية بعدم حاجة الشركات عينة البحث إلى الاتصال عن بعد بشكل كبير، حيث لا يوجد لدى أغلبها فروع في أماكن متباعدة أما قلة حدوث تهديد الكوارث الطبيعية فيمكن أن يعود إلى كون الأردن من المناطق غير المعرضة بدرجة كبيرة لتلك الكوارث. ولعل أحد التفسيرات المحتملة لانخفاض معدل تكرار حدوث التهديدات الأخرى المذكورة هو عدم قدرة أنظمة الرقابة الداخلية في الشركات محل البحث على اكتشاف هذه التهديدات في حالة حدوثها.

وبهدف التحقق من الدلالة الإحصائية للنتائج السابقة ولاختبار الفرضية الثانية تم استخدام اختبار (t) لعينة واحدة (One Sample Test) ، ويبين الجدول رقم (10) نتائج اختبار هذه الفرضية، إذ كانت قيم (t) المحسوبة لكل إجابات هذا المحور أكبر من القيمة الجدولية البالغة (1.645) على أساس مستوى دلالة (0.05)، مما يفيد بقبول الفرضية الثانية بدرجة ثقة (95 %) أي تدرك شركات التأمين الأردنية درجة أهمية التهديدات التي تواجه أمن نظم معلوماتها المحاسبية الإلكترونية.

نتائج الدراسة والتوصيات

نتائج الدراسة

من خلال عرض وتحليل بيانات الدراسة، تم التوصل إلى النتائج الآتية:

1. لا يمتلك العاملون في المجالات ذات العلاقة بنظام المعلومات المحاسبية الإلكترونية في الشركات محل البحث الخبرة والمهارة الكافية، فقد كان نصف أفراد العينة تقريباً يقعون ضمن فئة الخبرة (5 سنوات فأقل) رغم تفضيل هذه الشركات توظيف ذوي المؤهلات العلمية، إذ يشكل حملة شهادة البكالوريوس نسبة (85 %) من مجموع أفراد العينة.
2. ضعف اهتمام الشركات قيد الدراسة بتدريب وتطوير كوادرها العاملة في الميادين ذات الصلة بنظام المعلومات المحاسبية الإلكترونية، فقد تبين أن نسبة (75.8 %) من المبحوثين قد حصلوا على (3 دورات تدريبية أو أقل) فقط في مجال الحاسوب والخدمات الإلكترونية.
3. يُعتمد الحاسوب في العمل المحاسبي في الشركات عينة البحث، حيث تطبق جميع هذه الشركات نظام محاسبي إلكتروني. كما أنها تستخدم شبكة الإنترنت في إنجاز الأعمال وتقديم الخدمات، فقد بلغت نسبة إجابات أفراد العينة التي أكدت هذا الاستخدام (75 %).
4. لا تقوم الشركات عينة البحث بتطوير الممارسات والضوابط الرقابية فيها باستمرار لتتناسب مع التطورات الحاصلة في تكنولوجيا المعلومات والاتصالات المستخدمة في أعمالها، حيث أنها تقوم بهذا التطوير بدرجة ضعيفة. فقد أفاد (65 %) من أفراد العينة بعدم قيام شركاتهم بهذا التطوير بصورة مستمرة، مما يشير الى عدم كفاية و فعالية الادوات و الضوابط الرقابية المطبقة. و تتفق هذه النتيجة مع نتائج بعض الدراسات السابقة و منها على سبيل المثال:
(أبو موسى 2002؛ Davis 1997 & 1996 , Ryan & Brodoloi 1997؛ البياتي 1996 ؛ Loch et al 1992)
5. وضحت الدراسة بأن (36.7 %) من أفراد العينة أكدوا حدوث خسائر مالية في شركاتهم نتيجة خرق أمن نظام المعلومات المحاسبية الإلكترونية، فيما بلغت نسبة الإجابات التي أفادت بعكس ذلك (63.3 %). وترى الباحثة أنه ينبغي النظر إلى هذه النتيجة بشيء من التحفظ، فمن المعروف تردد المنظمات عادة في الإفصاح عن خسائرها المالية الناجمة عن خروقات أمن نظام المعلومات حفاظاً على سمعتها ومركزها التنافسي.
6. بينت الدراسة وجود تهديدات تواجه أمن نظام المعلومات المحاسبية الإلكترونية في الشركات محل البحث، إذ هناك قناعة كافية لدى أفراد العينة بتعرض النظام المذكور لتهديدات أمنية، فقد جاء المتوسط الحسابي الكلي للإجابات حول وجود هذه التهديدات مرتفعاً إذ بلغ (3.933) أو بنسبة

(72.32 %)، وبانحراف معياري متدن (0.487). و تتفق هذه النتيجة مع نتائج الدراسات السابقة ذات العلاقة المشار اليها في هذا البحث.

7. أظهرت الدراسة أن أهم ثلاث تهديدات تواجه أمن نظام المعلومات المحاسبية الإلكترونية في الشركات محل البحث هي: الإدخال غير المتعمد لبيانات خاطئة من قبل الموظفين، وسرقة وقت الحاسوب واستخدامه في الأغراض الشخصية، والاشتراك في كلمة المرور (السر)، فقد كان المتوسط الحسابي للإجابات التي أيدت هذا الترتيب للتهديدات الثلاث السابقة الذكر مرتفعاً، فقد بلغ على التوالي (3.70، 3.61، 3.59) وبأهمية بنسبة (74 %، 72.20 %، 71.80 %). كما سجلت التهديدات التالية معدلات تكرار حدوث مرتفعة أيضاً: القيام بتدمير غير متعمد للبيانات من قبل الموظفين، وتوصل موظفون 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، فقد بلغ المتوسط الحسابي للإجابات ذات العلاقة بهذا الجانب (3.57، 3.55، 3.53، 3.52، 3.51) وبأهمية نسبية (71.40 %، 71 %، 70.60 %، 70.40 %، 70.20 %) على التوالي. و فيما عدا سرقة وقت الحاسوب و استخدامة في الاغراض الشخصية، فأن تصنيف التهديدات المذكورة ضمن قائمة أهم التهديدات التي تواجه نظم المعلومات المحاسبية الإلكترونية يتفق بشكل عام مع نتائج بعض الدراسات السابقة مثل: (أبو موسى 2004؛ Henry 1997 ; Ryan & Brodoloi 1997 ; Davis 1996)

التوصيات

بناءً على النتائج السابقة التي تم التوصل إليها، يخلص البحث إلى التوصيات الآتية:

1. زيادة الوعي فيما يتعلق بأمن نظم المعلومات المحاسبية الإلكترونية وخطورة التهديدات الأمنية التي قد تواجهها، نظراً لجسامة الخسائر المادية والمعنوية التي تخلفها هذه التهديدات.
2. العناية بتحديد مواصفات واختيار شاغلي الوظائف في المجالات ذات العلاقة بنظام المعلومات المحاسبية الإلكترونية (خبرة، مهارة، تأهيل علمي، أخلاقيات وظيفية رفيعة)، نظراً لحساسية هذه الوظائف وخطورتها.
3. ضرورة اهتمام الشركات محل البحث بالبرامج والدورات التدريبية ذات الصلة بوسائل تكنولوجيا المعلومات والاتصالات المستخدمة في مجال أنظمة المعلومات المحاسبية الإلكترونية، من أجل تنمية وتطوير معارف ومهارات العاملين لديها، فضلاً عن أهمية تشجيعهم على مواكبة التطورات في هذا الميدان بشكل ذاتي وذلك بمنح الحوافز المادية والمعنوية للمبدعين منهم.

4. ضرورة تركيز الشركات محل البحث على التهديدات الأمنية التي تواجه نظم معلوماتها المحاسبية الإلكترونية، وبالأخص ذات معدلات التكرار المرتفعة وتشخيص أسبابها والعمل على تطوير وسائل أمن وحماية لتلافيها وسد الثغرات الأمنية في تلك النظم.
5. ضرورة استمرار مواكبة الممارسات والأساليب الرقابية المطبقة في شركات التأمين عينة البحث للتطورات الحاصلة في وسائل تكنولوجيا المعلومات والاتصالات المستخدمة في أعمال هذه الشركات.
6. أهمية تقويم أنظمة الرقابة الداخلية وأنظمة حماية المعلومات المطبقة في الشركات محل البحث، لتطوير وكشف نقاط الضعف في هذه الأنظمة ومعالجتها، لتوفير الحماية ضد المخاطر الحالية والمحتملة.
7. هناك مجالات متعددة في موضوع البحث ما زالت بحاجة إلى جهود الباحثين، بما يسمح بمقارنة النتائج وتعديلها، ويمكن أن توجه هذه الجهود لدراسة أساليب الرقابة المطبقة على أنظمة المعلومات المحاسبية الإلكترونية ووسائل حمايتها في بيئة الأعمال الأردنية، وتكرار هذا البحث على قطاعات اقتصادية أخرى في البيئة المذكورة.

المراجع العربية

أبو موسى، أحمد عبد السلام، جرائم الكمبيوتر: هل يمكنك حماية نظام المعلومات المحاسبية الخاصة بك؟ ، بحوث مؤتمر الاقتصاد والعلوم الإدارية، جامعة الزيتونة الأردنية، عمان، الأردن، 2002، ص ص 609-625.

أبو موسى، أحمد عبد السلام، "أهمية مخاطر المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المنشآت السعودية"، المجلة العلمية للتجارة والتمويل، كلية التجارة، جامعة طنطا، العدد الثاني، (2004)، ص ص 6-54.

الاتحاد الأردني لشركات التأمين. شركات التأمين، 2006. .http:/ www.joif.or/

البياتي، هلال عبود، "الوسائل الفنية لحماية البرامج ودور التشريع في حماية المعلومات"، مجلة أبحاث الحاسوب، المجلد الأول، العدد صفر، (1996)، ص ص 37-46.

حفناوي، محمد يوسف، نظم المعلومات المحاسبية الإلكترونية، ط1، عمان، الأردن، دار وائل للنشر، 2001.

داوود، حسن طاهر، الحاسب وأمن المعلومات، ط1، الرياض، معهد الإدارة العامة، 2000.

عرب، يونس، جرائم الكمبيوتر والإنترنت، ط1، منشورات اتحاد المصادر العربية، موسوعة القانون وتقنية المعلومات، 2002.

الهيتي، صلاح الدين و الربيحات، أمنة ماجد، "أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية: دراسة ميدانية في عدد من الوزارات الأردنية وأمانة عمان الكبرى"، مجلة المحاسبة والإدارة والتأمين، جهاز الدراسات العليا والبحوث، كلية التجارة، جامعة القاهرة، العدد 65، (2005)، ص ص 309-378.

المراجع اللاإنجليزية

Bouverman, B. L. & O'Connell, R. T., Business Statistics in Practice, 2nd ed., New York: McGraw-Hill, Inc., 2001.

Conver, W. J., Practical Nonparametric Statistics, New York: John Wiley & Sons, Inc., 1980.

Davis, Charles E., "Perceived Security Threats to Today's Accounting Information Systems: A Survey of CISAs", IS Audit & Control Journal, Vol.3, (1996), PP. 3841-.

Davis, Charles E., "An Assessment of Accounting Information Security", The CPA Journal, New York, Vol.67, Iss.3, (1997), PP. 2834-.

Haag, Stephen et al., Management Information Systems for The Information Age, 2nd ed., Irwin McGraw-Hill, Inc., 2000.

Hall, James A., Accounting Information Systems, 4th ed., Thomson. South – Western, 2004.

Henry Laurie. "A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia", The Mid-Atlantic Journal of Business, Vol. 33, Iss. 63, (1997), PP. 171-189.

Kankanhalli, Atreyi et al., "An Integrative Study of Information Systems Security effectiveness," International Journal of Information Management, Vol. 23, (2003) PP. 139154-.

Loch, Karen D. et al., "Threats to Information Systems: Today's Reality, Yesterday's Understanding", MIS Quarterly, (June, 1992), PP. 173186-.

Moscove, Stephen A. et al., Core Concepts of Accounting Information Systems, 6th ed., John Wiley & Sons, Inc., 1999.

National Institute of Standards and Technology, Technology Administration, U.S. Department of commerce, An Introduction to computer Security: The NIST Handbook, Special Publication, October 1995.

Ryan, S. D. & Bordoloi, B., "Evaluating Security Threats in Mainframe and Client Server Environments", Information & Management, Vol. 32, Iss. 3, (1997), PP. 137142-.

Romney, Marshall B. & Steinbart, Paul John, Accounting Information Systems, 10th ed., Pearson Prentice Hall, 2006.

الملاحق

الملحق رقم (1)
قائمة إستبانه

الوظيفة الحالية: المؤهل العلمي:

عدد سنوات الخبرة في الوظيفة الحالية:

عدد الدورات التدريبية ذات العلاقة بالحاسوب والخدمات الإلكترونية:

يرجى وضع إشارة (X) للإجابة المختارة عن الأسئلة الآتية:

أولاً: الأسئلة العامة

1. يتم اعتماد نظام محاسبي إلكتروني في الشركة

☐ نعم ☐ لا

2. تستخدم الشركة شبكة الإنترنت في إنجاز الأعمال وتقديم الخدمات

☐ نعم ☐ لا

3. يتم تطوير الممارسات والضوابط الرقابية في الشركة باستمرار لتتلائم مع التطورات في أساليب تكنولوجيا المعلومات والاتصالات المستخدمة في العمل:

☐ نعم ☐ لا

4. عانت الشركة من خسائر مالية نتيجة:

☐ تصرفات داخلية لخرق أمن نظام المعلومات المحاسبية

☐ تصرفات خارجية لخرق أمن نظام المعلومات المحاسبية

☐ تصرفات داخلية وخارجية لخرق أمن نظام المعلومات المحاسبية

☐ لم لم تعاني الشركة من خسائر مالية نتيجة تصرفات داخلية أو خارجية

☐ لخرق أمن نظام المعلومات المحاسبية

ثانياً: الأسئلة ذات العلاقة بأمن نظام المعلومات المحاسبية الإلكترونية

التسلسل	الأسئلة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1 -	يواجه النظام* العديد من التحديات نتيجة التهديدات الأمنية التي يتعرض لها.					
2 -	تحصل خروقات لأمن النظام باستمرار.					
3 -	يتم القيام بإجراءات من شأنها التقليل من الاعتداءات على أمن النظام.					
4 -	يقوم الموظفون بإدخال غير متعمد (غير مقصود) لبيانات غير سليمة.	يحدث يومياً أو بصفة متكررة (دائماً)	يحدث من مرة أسبوعياً إلى يومياً (غالباً)	يحدث من مرة شهرياً إلى أسبوعياً (أحياناً)	يحدث من مرة سنوياً إلى شهرياً (نادراً)	لا يحدث إطلاقاً
5 -	يقوم الموظفون بإدخال متعمد لبيانات غير سليمة.					
6 -	يقوم الموظفون بتدمير غير متعمد للبيانات.					
7 -	يقوم الموظفون بتدمير متعمد للبيانات.					

* يقصد بالنظام في هذه الإستبانة نظام المعلومات المحاسبية الإلكترونية.

8 -	يتوصل موظفون غير مصرح لهم (غير مرخصين) للبيانات والنظام.					
9 -	يتوصل أشخاص غير مصرح لهم من خارج الشركة (قراصنة المعلومات) إلى البيانات والنظام.					
10 -	يشترك الموظفون في كلمة المرور (السر).					
11 -	تحدث كوارث غير طبيعية (من صنع الإنسان) مثل الحرائق، قطع التيار الكهربائي بشكل متعمد... الخ.					
12-	تحدث كوارث طبيعية مثل انقطاع مصدر الطاقة، الزلازل... الخ.					
13 -	يتم إدخال فيروس الحاسوب للنظام.					
14 -	يتم سرقة وقت الحاسوب واستخدامه في الأغراض الشخصية.					
15 -	يتم سرقة البيانات والمعلومات.					
16 -	يُمنع أشخاص لهم حق الدخول إلى النظام من ممارسة هذا الحق.					

17 -	يتم طمس أو تدمير بنود معينة من المخرجات.					
18 -	يتم خلق مخرجات غير صحيحة (مزيفة) للنظام.					
19 -	تُعد نسخ غير مصرح بها للمخرجات.					
20 -	يتم الكشف بشكل غير شرعي (غير مصرح به) عن البيانات والمعلومات بعرضها على شاشة الحاسوب أو طباعتها على الورق.					
21 -	يقوم موظفون غير مرخص لهم بطباعة وتوزيع المعلومات.					
22 -	توجه المخرجات عن طريق الخطأ إلى أشخاص غير مصرح لهم باستلام نسخة منها.					
23 -	تُسند مهمة أتلاف مخرجات حساسة لم يعد بحاجة إليها إلى أشخاص لا تتوافر فيهم الأمانة.					
24 -	تتم مقاطعة تحويل البيانات من أماكن متباعدة.					

الملحق رقم (2)

أسماء الشركات قيد البحث

1 – شركة التأمين الأردنية
2 – شركة التأمين الوطنية الأهلية
3 – شركة البحار العربية للتأمين
4 – شركة القدس للتأمين
5 – شركة الاردن الدولية للتأمين
6 – شركة دلتا للتأمين
7 – شركة الواحة للتأمين
8 – شركة الأراضي المقدسة للتأمين
9 – شركة فيلادلفيا للتأمين
10 – شركة جراسا للتأمين
11 – شركة العرب للتأمين على الحياة والحوادث
12 – شركة التأمين الإسلامية
13 – شركة الضامنون العرب
14 – شركة الشرق العربي للتأمين

الملحق رقم (3)

جدول رقم (1)

توزيع أفراد العينة حسب مجال العمل

مجال العمل	العدد	النسبة المئوية
العاملون في مجال المحاسبة	48	% 40
العاملون في مجال التدقيق الداخلي	32	% 26.7
العاملون في مجال الحاسوب	40	% 33.3
المجموع	120	% 100

جدول رقم (2)

توزيع أفراد العينة حسب المؤهل العلمي

المؤهل العلمي	العدد	النسبة المئوية
ثانوية عامة	3	% 2.5
دبلوم	10	% 8.3
بكالوريوس	102	% 85
دراسات عليا	5	% 4.2
المجموع	120	% 100

جدول رقم (3)

توزيع أفراد العينة حسب الخبرة الوظيفية

الخبرة في الوظيفة الحالية	العدد	النسبة المئوية
5 سنوات فأقل	59	% 49.2
6-10 سنوات	25	% 20.8
10 سنوات فأكثر	36	% 30
المجموع	120	% 100

جدول رقم (4)

توزيع أفراد العينة حسب الدورات التدريبية ذات العلاقة بالحاسوب والخدمات الإلكترونية

الدورات التدريبية ذات العلاقة بالحاسوب والخدمات الإلكترونية	العدد	النسبة المئوية
3 فأقل	91	% 75.8
7-4	20	% 16.7
7 فأكثر	19	% 7.5
المجموع	120	% 100

جدول رقم (5)

التكرارات والنسب المئوية لإجابات أفراد العينة على الأسئلة العامة (الاسئلة من رقم 1الى رقم 3)*

الأسئلة	نعم		لا		المجموع	
	التكرار	النسبة المئوية	التكرار	النسبة المئوية	التكرار	النسبة المئوية
- يتم اعتماد نظام محاسبي إلكتروني في الشركة.	120	% 100	-	-	120	% 100
- تستخدم الشركة شبكة الإنترنت في إنجاز الأعمال وتقديم الخدمات.	90	% 75	30	% 25	120	% 100
- يتم تطوير الممارسات والضوابط الرقابية في الشركة باستمرار لتتلائم مع التطورات في أساليب تكنولوجيا المعلومات والاتصالات المستخدمة في العمل.	42	% 35	78	% 65	120	% 100

* وفقا لتسلسل الاسئلة الوارد في استمارة الاستبانة في الملحق رقم (1).

جدول رقم (6)

التكرارات والنسب المئوية لإجابات أفراد العينة على الأسئلة العامة (السؤال رقم 4)

السؤال	التكرار	النسبة المئوية
- عانت الشركة من خسائر مالية نتيجة:		
× تصرفات داخلية لخرق أمن نظام المعلومات المحاسبي.	31	% 25.8
× تصرفات خارجية لخرق أمن نظام المعلومات المحاسبي.	11	% 9.2
× تصرفات داخلية وخارجية لخرق أمن نظام المعلومات المحاسبي.	2	% 1.7
× لم تعاني الشركة من خسائر مالية نتيجة تصرفات داخلية أو خارجية لخرق أمن نظام المعلومات المحاسبي.	76	% 63.3
المجموع	120	% 100

جدول رقم (7)

المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لإجابات أفراد العينة

حول مدى وجود تهديدات لأمن نظم المعلومات المحاسبية الإلكترونية

الأسئلة	المتوسط الحسابي (على مقياس خماسي)	النسبة المئوية*	الانحراف المعياري
- يواجه النظام العديد من التحديات نتيجة التهديدات الأمنية التي يتعرض لها.	3.952	% 79.04	0.462
- تحصل خروقات لأمن النظام باستمرار.	4.011	% 80.22	0.631
- يتم القيام بإجراءات من شأنها التقليل من الاعتداءات على أمن النظام.	3.936	% 78.72	0.581
إجمالي	3.933	% 79.32	0.487

* تمثل هذه النسبة قيمة المتوسط الحسابي (المرجح) بالنسبة للقيمة القصوى في المقياس المستخدم والمكون من خمس درجات.

جدول رقم (8)

نتائج اختبار الفرضية الأولى

n	W	Wα	+T
120	1840	92	88

جدول رقم (9)

المتوسطات الحسابية، والانحرافات المعيارية، والأهمية النسبية

لإجابات أفراد العينة عن تهديدات أمن نظام المعلومات المحاسبية الإلكترونية

رقم السؤال	تهديدات أمن نظام المعلومات المحاسبية الإلكترونية	المتوسط الحسابي (على مقياس خماسي)	الانحراف المعياري	الأهمية النسبية (%)	الترتيب حسب الأهمية النسبية	مستوى معدل تكرار الحدوث بالنسبة للمتوسط*
1	- يقوم الموظفون بإدخال غير متعمد (غير مقصود) لبيانات غير سليمة.	3.70	1.16	% 74	1	مرتفع
2	- يقوم الموظفون بإدخال متعمد لبيانات غير سليمة.	1.20	1.19	% 24	13	ضعيف
3	- يقوم الموظفون بتدمير غير متعمد للبيانات.	3.57	1.09	% 71.40	4	مرتفع
4	- يقوم الموظفون بتدمير متعمد للبيانات.	1.12	1.15	% 22.40	16	ضعيف
5	- يتوصل موظفون غير مصرح لهم (غير مرخصين) للبيانات والنظام.	3.55	1.9	% 71	5	مرتفع
6	- يتوصل أشخاص غير مصرح لهم من خارج الشركة (قراصنة المعلومات) إلى البيانات والنظام.	1.30	1.02	% 26	12	ضعيف
7	- يشترك الموظفون في كلمة المرور (السر).	3.59	1.18	% 71.80	3	مرتفع
8	- تحدث كوارث غير طبيعية (من صنع الإنسان) مثل الحرائق، قطع التيار الكهربائي بشكل متعمد... الخ.	1.09	1.17	% 21.80	19	ضعيف

* تم تحديد مستوى معدل تكرار الحدوث وفقاً لقيمة المتوسطات الحسابية والأهمية النسبية لإجابات الاستبانة وعلى النحو الآتي: (5-3.5 مرتفع)، (3.49-2.5 متوسط)، (2.49-1 فأقل ضعيف).

جدول رقم (10)

نتائج اختبار الفرضية الثانية

رقم السؤال*	t المحسوبة	درجات الحرية	مستوى المعنوية
1	34.940	119	0.000
2	11.136	119	0.000
3	35.878	119	0.000
4	10.758	119	0.000
5	35.587	119	0.000
6	13.961	119	0.000
7	33.427	119	0.000
8	10.205	119	0.000
9	11.496	119	0.000
10	35.914	119	0.000
11	36.958	119	0.000
12	10.758	119	0.000
13	11.471	119	0.000
14	27.545	119	0.000
15	11.957	119	0.000
16	26.106	119	0.000
17	35.934	119	0.000
18	25.757	119	0.000
19	33.531	119	0.000
20	10.263	119	0.000
21	12.458	119	0.000

* تمت الإشارة إلى أرقام الأسئلة حسب التسلسل الوارد في الجدول رقم (9)، حيث لم تذكر تجنباً للتكرار.

الملحق رقم (4)

شكل رقم (1)

تهديدات أمن نظم المعلومات المحاسبية الإلكترونية طبقاً لمراحل النظام