مخاطر الأمن المعلوماتي وسبل مواجهتها في المصارف التجارية العاملة في محافظة البلقاء

دكتور/ إبراهيم حربي تادرس (*)
دكتور/ عبدالله رضوان عربيات (*)

الملخص:

تأتي أهمية المحافظة على أمن المعلومات والبيانات الخاصة بالمصارف التجارية الأردنية وحمايتها من احتمال فقدانها، لما لها من تأثير على إستراتيجيتها وخططها المستقبلية وبالتالي نموها وتطورها في القطاع التي تنتمي إليه. ومن هنا هدفت الدراسة إلى الكشف عن مخاطر أمن المعلومات في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها على مختلف مستوياتهم الإدارية، واقتراح أهم السبل لمواجهتها. استخدم المنهج الوصفي التحليلي في هذه الدراسة لاستنباط النتائج باستخدام عينة عشوائية بسيطة مكونة من (٢٢٥) موظفًا، وبعد أن عولجت البيانات التي وردت في الاستبانة باستخدام الأساليب الإحصائية المناسبة، توصلت الدراسة إلى أن الدرجة الكلية لمخاطر أمن المعلومات في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها «متوسطة» بمتوسط حسابي (٣,٤٠). حيث جاء «مخاطر الأفراد» في المرتبة الأولى تلاه في المرتبة الثانية «مخاطر العمليات» بينما جاء «مخاطر البيانات» في المرتبة الأخيرة. وأشارت النتائج أن أهم سبل التغلب على هذه المخاطر هو «تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمان نظام المعلومات». وفي ضوء ذلك تم صياغة مجموعة من

(*) قسم نظم المعلومات الحاسوبية ـ كلية الأمير عبدالله بن غازي لتكنولوجيا المعلومات ـ جامعة البلقاء التطبيقية.

التوصيات المنبثقة من النتائج التي يؤمل أن يستفيد منها المعنيون من الدراسة الحالية.

الكلمات المفتاحية: مخاطر، تهديدات، أمن المعلومات، المصارف التجارية العاملة محافظة البلقاء.

Abstract

The importance of maintaining information on the Jordanian commercial banks and protecting it from possible loss has a significant impact on their strategies and future plans. Moreover, it will considerable affect their growth and development in the sector to which they belong. Therefore, this study aimed to reveal the information security risks in commercial banks operating in Al- Balqa governorate from employees' perspective at various administrative levels and to propose the most important ways to address them.

Descriptive and analytical approach has been used to draw conclusions using a simple random sample consisting of (225) employees. Statistical appropriate methods were used to analyze the data collected by a questionnaire. The study found that the overall degree of information security risks in commercial banks operating in the Balqa governorate as perceived its employees was "medium" with mean of 3.40. The "individuals' risks" came in the first place, followed by "operations risks" and finally "communication networks risks". The results indicated that the most important ways to overcome these risks are to enhance the infrastructure of information technology and to ensure the strengthening of information system security." In light of this, a set of recommendations emanating from the results has been formulated that will hopefully benefit the stakeholders of the current study.

Key words: risks, threats, information security, commercial banks, Balqa governorate

المقدمة

مع بدايات القرن الحادي والعشرين، وظهور الثورة المعلوماتية، وحدوث الطفرة التكنولوجية الهائلة في التقنيات المختلفة، أصبحت تكنولوجيا المعلومات ضرورة من ضروريات عصرنا الحالي وأداة من أدوات العمل الرئيسية؛ بل وأصبحت أداة إستراتيجية تسهل الوصول إلى الميزة التنافسية الدائمة، ونتيجة لهذه الطفرة الكبيرة التي حدثت؛ كان لابد من ظهور مخاطر ومهددات جديدة في الساحة العالمية وهي المسماة بجرائم الحاسوب مما يستدعي أخذ كافة الوسائل المتاحة والممكنة لأمن نظم المعلومات وحمايتها في المجالات كافة (الدنف، ٢٠١٣؛ Turban, et al., 2008).

وتأسيساً على ما سبق ظهر مفهوم أمن المعلومات ليعبر عن درجة الحماية من المخاطر المتصلة والناتجة عن استغلال ثغرات وضعف نظم المعلومات، والتي هدفها حماية نظام المعلومات ومكوناته، مع عدم تعرضها لتلك المخاطر والتهديدات والتعامل معها من خلال أشخاص مصرح لهم بذلك أو لأي أسباب أخرى (Raval & Fichadia, 2007: 21). ومن هنا تظهر مسؤولية جديدة وكبيرة أمام إدارة نظم المعلومات في المنشأة وهي ضرورة توفير الوسائل والأساليب اللازمة لضمان استمرارية عمل تلك النظم بشكل صحيح، مع التخطيط الدقيق لمواجهة جميع الأخطار التي يمكن أن تؤدي إلى تعطلها أو توقفها عن العمل، وفي حال حدوث ذلك، التمكن من إعادة تشغيلها بأسرع وقت ممكن (البحيصي والشريف، ٢٠٠٧).

ومن ناحية أخرى يشكل الجهاز المصرفي مرتكزًا أساسيًا من مرتكزات النظام الاقتصادي الأردني كما في غيره من اقتصاديات الدول عمومًا. وقد أسهم الإبداع التكنولوجي المتواصل والمنافسة المحتدمة بين مكونات القطاع المصرفي في إحداث تطورات متسارعة في الصناعة المصرفية وبرزت أشكالاً جديدة من المنتجات والخدمات المصرفية في مختلف مجالات العمل المصرفي كعمليات الصيرفة

الالكترونية وبطاقات الائتمان المصرفية وخدمات الصراف الآلي **A.T.M** وتقديم الخدمات المصرفية عبر الإنترنت ... وغيرها (القطناني، ٢٠٠٧). لذا يتطلب من إدارة المصارف العمل على أحكام الرقابة على العمل المصرفي لأجل الحفاظ على أمن نظم المعلومات المصرفية. وعليه أتت هذه الدراسة للتعرف إلى المخاطر المختلفة التي تهدد الأمن المعلوماتي مخاطر الأمن المعلوماتي وسبل مواجهتها في المصارف التجارية العاملة في محافظة البلقاء.

مشكلة الدراسة

تتزايد تحديات أمن المعلومات في البيئة الرقمية كلما تبنينا التقنيات والحوسبة الحديثة، ومع اتساع نطاق المؤثرات الداخلية والخارجية تصبح التقنيات وحدها عاجزة عن التغلب على المخاطر الأمنية التي تحدق بهذه النظم. ولعل الحل يكمن بإدارة أفضل لأمن نظم المعلومات عبر ممارسة عملية تقييم وإدارة المخاطر وإيجاد الحلول الأمنية كسياسات أمن المعلومات، ومراجعة أنظمة الرقابة والتحكم والحلول الإستراتيجية الأخرى الممكنة .

ومن هنا تبرز الحاجة للمحافظة على أمن المعلومات في قطاع المصارف الأردنية؛ وذلك لأنه من أهم القطاعات المستخدمة لأنظمة المعلومات، خاصة أن قطاع المصارف يعتمد يوماً بعد يوم بشكل متزايد على نظم المعلومات لنموه السريع المضطرد. وانطلاقاً من تزايد معدلات الاختراقات غير المشروعة، والحاجة لاتخاذ وسائل الحماية اللازمة للبيانات والمعلومات التي تزداد أهميتها في حالة كون البيانات المراد حمايتها تابعة لجهة مصرفية، ومن الصعب إيجاد وسائل حماية دائمة في ظل التطور التقني السريع، وظهور وسائل اختراق ذات قدرات متطورة. وعليه فإن المصارف الأردنية بحاجة إلى حماية أنظمتها عموماً وأمن تلك النظم خصوصاً بشكل خاص لتعزيز دورها في أعمالها. ومن هنا شعر الباحث أهمية دراسة مخاطر الأمن المعلوماتي وسبل مواجهتها في المصارف التجارية العاملة في محافظة البلقاء.

وتتمثل مشكلة الدراسة في الإجابة عن التساؤلات الآتية:

١. ما مخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها.
٢. ما سبل مواجهة مخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها.

أهداف الدراسة

هدفت الدراسة إلى الكشف عن مخاطر أمن المعلومات في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها على مختلف مستوياتهم الإدارية، واقتراح أهم السبل لمواجهتها.

أهمية الدراسة

يمكن تلخيص أهمية الدراسة بما يلي:

– تنبع الأهمية النظرية للدراسة من أهمية المحافظة إلى أمن المعلومات والبيانات الخاصة بالمصارف التجارية الأردنية وحمايتها من احتمال فقدانها، مما لها من تأثير على إستراتيجيتها وخططها المستقبلية وبالتالي نموها وتطورها في القطاع الذي تنتمي إليه.

– تأتي الدراسة مكملة لدراسات سابقة عديدة على الصعيد المحلي والدولي، لكنها تجسد مفاهيم جديدة وبيئة جديدة لم تدرس من قبل وتعتبر ذات أهمية من منطلق تعزيز مفهوم إدارة المخاطر والمنافع وتحقيق إدارة سليمة لأمن المعلومات بما يؤكد استمرارية العمل.

– قد تسهم هذه الدراسة أيضاً في التعرف إلى أهم الآليات والاستراتيجيات المقترحة من خلال نتائج الدراسة، والتي تساعد في تذليل تلك المخاطر والتغلب عليها، والمساهمة في تحقيق أمن المعلومات في المصارف كافة ومصارف محافظة البلقاء خاصة.

- الخروج بالتوصيات حول سبل التغلب على مخاطر أمن المعلومات في المصارف التجارية العاملة في محافظة البلقاء.

حدود الدراسة

- حدود مكانية: تقتصر هذه الدراسة على المصارف التجارية في محافظة البلقاء.
- حدود زمانية: تم إجراء هذه الدراسة في العام ٢٠١٤م.
- حدود بشرية: تقتصر هذه الدراسة على العاملين في المصارف التجارية العاملة في محافظة البلقاء.

التعريفات الاصطلاحية والإجرائية

تحتوي الدراسة مجموعة من المصطلحات تم تعريف أهمها اصطلاحيًا وإجرائيًا على النحو الآتي:

- **أمن المعلومات**: «مجموعة الوسائل والتدابير والإجراءات التي يجب توفيرها لتأمين حماية المعلومات من المخاطر سواء من داخل المعلومات محل الحماية أو من خارجها» (ميلاد، ٢٠٠٦ :١).

- **نظم المعلومات**: «نظم يتم من خلالها تجميع وتسجيل وتخزين ومعالجة البيانات في سبيل الوصول على معلومات لمتخذي القرار، كما يتم من خلال حماية أصول المنشأة بما فيها البيانات».**(Romney & Steinbart, 2012: 21)**

- **المخاطر** «وضع صعب يكتنفه شيء من الغموض يحول دون تحقيق الأهداف بكفاية وفاعلية، ويُمكن النظر إليه على أنها المسبب للفجوة بين مستوى الإنجاز المتوقع والإنجاز الفعلي أو على أنها الانحراف في الأداء عن معيار محدد مسبقًا» (درويش، ٢٠٠٥: ٢٦).

- **وتعرف اجرائيًا**: هو كل الأضرار التي ممكن أن تحدث في حال التمكن من استغلال الثغرات بنظم المعلومات في المصارف التجارية في محافظة البلقاء؛ بحيث كلما زادت تلك التهديدات زادت درجة المتوسط الحسابي حسب تقديرات عينة الدراسة.

- **المصارف التجارية في محافظة البلقاء**: هي جميع المصارف الأردنية التابعة لمحافظة البلقاء والمشرف عليها البنك المركزي الأردني، والتي اختارها الباحث لتطبق عليها الدراسة.

الإطار النظري للدراسة

في هذا الجزء من الدراسة سيتم تناول مفهوم الأمن المعلوماتي، المخاطر التي تواجه الأمن المعلوماتي، مكونات الأمن المعلوماتي.

مفهوم الأمن المعلومات

لقد شاع استعمال مفهوم الأمن المعلوماتي بعد انتشار استخدام الحواسيب والبرمجيات بتطبيقاتها المختلفة وفي المجالات الحياتية والعلمية والثقافية الإدارية المتعددة أيضاً. ومن أبرز التعريفات التي تطرقت إلى مفهوم أمن المعلومات:

إن أمن المعلومات عبارة عن «مجموعة من الإجراءات والتدابير الوقائية التي تستخدم للحماية من جرائم الحاسوب والانترنت» (السالمي، ٢٠٠٨، ٢٨١). ويعرف على أنه «درجة الثقة بالأمن والحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام».(**Raval & Fichadia, 2007**).

ويعرفها الباحث بأنها: مجموعة من الإجراءات التي تتخذ لحماية الأجزاء المادية كمكونات الحاسب الآلي والشبكات، وغير المادية كالبرامج والتطبيقات والبيانات والمعلومات.

المخاطر التي تواجه الأمن المعلوماتي

تنبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة على السواء التي قد ترد من مصادر داخلية أو خارجية. ومن هذه التهديدات والمخاطر الآتي:

- اقتحام الهاكرز **Hackers**: ويعني الدخول غير المصرح به للشبكة أو نظام المعلومات الحاسوبي بهدف تعديل البيانات أو المعلومات أو سرقتها أو تدميرها.

– اقتحام الكراكرز **Crackers**: ويعني الدخول إلى للشبكة مما يؤدي إلى تفشي أسرار العمل والعاملين، أو تخريب البيانات وإتلافها.

– التنصت من خلال تعليق شخص لمعدات معينة على الكابلات .

– مراقبة خطوط الهاتف والتجسس على مستخدمي الشبكة.

– إقحام الفيروسات للشبكة.

– إطلاع الأشخاص المصرح لهم باستخدام الشبكة على معلومات غير مصرح لهم بالاطلاع عليها.

– التشويش على الإشارات المنقولة عبر الكابلات.

– تعطيل أحد الأشخاص لنظام الأمن الخاص بالشبكة أو كشفه لإجراءات الحماية المتبعة (داود،٢٠٠٢؛ **Brock, 2013**).

ولقد أشار رومني وستينبارت **(Romney & Steinbart, 2012)** إلى عدة أساليب تتضمن عدة تهديدات ومخاطر وهي:

- الهندسة الاجتماعية: ويقصد به استدراج المستخدم على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع معلومات دون إثارة أي شبهة.
- البرمجيات الضارة: ويقصد بها برامج متخصصة لتسهيل التسلل إلى النظام أو الشبكة بهدف تدميرها.

ويصنفها البحيصي والشريف (٢٠٠٨) على النحو الأتي:

- مخاطر المدخلات: وهي المخاطر التي تتعلق بأول مرحلة من مراحل النظام وهي مرحلة إدخال البيانات إلى النظام الألي.
- مخاطر تشغيل البيانات: وهي المخاطر التي تتعلق بالمرحلة الثانية من مراحل النظام وهي مرحلة تشغيل ومعالجة البيانات المخزنة في ذاكرة الحاسب.

- مخاطر مخرجات الحاسب: تتعلق تلك المخاطر بمرحلة مخرجات عمليات معالجة البيانات وما يصدر عن هذه المرحلة من قوائم للحسابات أو تقارير وأشرطة ملفات ممغنطة وكيفية استلام تلك المخرجات.
- مخاطر بيئية: وهي المخاطر التي تحدث بسبب عوامل بيئية، مثل: الزلازل والعواصف والفيضانات، والمتعلقة بأعطال التيار الكهربائي والحرائق؛ وسواء كانت تلك الكوارث طبيعية أم غير طبيعية فإنها قد تؤثر على عمل النظام المحاسبي.

يتضح مما سبق أن ما يتعرض له أمن المعلومات من مخاطر قد يكون في الموقع نفسه أو ما يتعرض له من مخاطر عن بعد. وعلى الرغم من ذلك إن إلحاق الأذى بالشبكة عن بعد يعد أكثر سهولة وأكثر خطورة من إلحاق الأذى بها في الموقع نفسه.

مكونات الأمن المعلوماتي

للوصول إلى أمن معلوماتي أشار ويتمان وماتورد (**Whitman & Mattord, 2011**) إلى ضرورة توفر مكونات أساسية داخل المنظمة، ويمكن تحديها بالآتي:

– الأمن المادي: ويتضمن أمن البنية التحتية والمباني بمنع التعدي غير المشروع عليها.

– أمن الأفراد: ويتضمن حماية الأفراد من الوصول إلى معلومات خاصة بهم.

– أمن العمليات: ويتضمن حماية الأنشطة والعمليات التي يقوم بها المعنيين بالقيام بها.

– أمن البيانات: وتتضمن السرية وتوفر وسلامة المعلومات.

– أمن الاتصالات: وتتضمن حماية وسائط الاتصالات التكنولوجيا من حيث المحتوى.

– أمن الشبكات: وتتضمن حماية مكونات الشبكة من حيث المحتوى.

لقد أشار المركز القومي للمعلومات في السودان (٢٠١٤) أن أمن المعلومات يهدف إلى تحقيق أساسيات ثلاثة متمثل في سرية البيانات، وتكاملية البيانات، وتوفر البيانات.

ويرى الباحث على الرغم من أن هناك عدداً من معايير أمن المعلومات المتاح، وهي منظمة بحيث لا يمكن الاستفادة منها إلا إذا تم تنفيذ هذه المعايير بشكل صحيح ومن خلال مشاركة جميع الأطراف سواء من الإدارة العليا والعاملين في أمن المعلومات، والمحترفين في تكنولوجيا المعلومات والمستخدمين والكل منهم له دور يؤديه في تأمين أصول المؤسسة.

الدراسات السابقة

يمثل الحديث عن مخاطر الأمن المعلوماتي وسبل مواجهتها في المصارف التجارية اهتمام كبير لدى العديد من الباحثين في الفكر المعلوماتي حيث أجريت العديد من الدراسات بهذا الخصوص سيقوم الباحث باستعراض بعضها من الأقدم إلى الأحدث فيما يأتي:

هدفت دراسة القطناني (٢٠٠٧) إلى دراسة خصائص البيئة التقنية وتكنولوجيا المعلومات (الخصائص الإدارية، خصائص الملاءمة، خصائص الأمن والسلامة) وقياس مدى توافرها في المصارف الأردنية، بالإضافة إلى تحديد مدى تأثير هذه الخصائص في مخاطر الرقابة التشغيلية في المصارف الأردنية. وقد قام الباحث بتطوير أداة الدراسة (استبانة) استنادًا إلى الإطار النظري والدراسات السابقة. وتم توزيع (٦٤) استبانة على عينة من مجتمع الدراسة الذي يتكون من العاملين في دوائر الرقابة الداخلية في المصارف الأردنية والمدققين الخارجيين. توصل الباحث إلى عدم وجود فروق ذات دلالة إحصائية بين آراء عينتي الدراسة لهذه المصارف بشأن مدى تأثير خصائص البيئة التقنية والتكنولوجية لنظم المعلومات في مخاطر الرقابة التشغيلية في المصارف الأردنية.

هدفت دراسة البحيصي والشريف (٢٠٠٨) إلى التعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، والتعرف إلى أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر. استخدمت الاستبانة لتحقيق أهداف الدراسة على عينة بلغت (١٢٩) موظفاً. تم استخلاص بعض النتائج منها: حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية ترجع إلى أسباب تتعلق بموظفي البنك نتيجة قلة الخبرة، وقلة الوعي بأمن المعلومات، وضعف التدريب، إضافة إلى أسباب تتعلق بإدارة المصرف.

هدفت دراسة الحمادي (٢٠١٠) إلى بناء أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية في شركة صناعة الكيماويات البترولية في الكويت. ولتحقيق أهداف الدراسة تم تصميم استبانة شملت (٤٣) فقرة لجمع المعلومات الأولية من عينة الدراسة المكونة من (٦٠) موظفًا. أظهرت النتائج وجود مخاطر في العمليات تهدد أمن المعلومات والاتصالات، ووجود أثر ذو دلالة احصائية لقلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات.

هدفت دراسة حمادة (٢٠١٠) إلى التعرف على أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية. ولتحقيق أهداف الدراسة طورت استبانة وزعت على (٨٧) مكتبًا، وخلصت الدراسة إلى أن هناك تأثيرًا كبيرًا للضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية في الشركات.

هدفت دراسة موحد وآخرون (**Mohd et al., 2010**) إلى الكشف عن دور تكنولوجيا المعلومات في أمن النظم المطرفي في المصارف الماليزية من خلال تقديم ورقة بحيثة. خلصت الدراسة إلى وجود اقتحام للنظم المصرفية ونقاط الضعف موجود في المؤسسة المالية الماليزية منها: التدخل غير القانوني غير المصرح به للأفراد أو المجموعات، انتهاك النظام الأمني، ووجود تحديات تعترض البيانات

منهـا: خـرق البيانـات، والافتقـار للتوثيـق والترخـيص، وسـرقة وتعـديل وحـذف المعلومات في النظام.

هدفت دراسة كـاظمي وآخـرون (**Kazemi et al., 2012**) إلـى الكشـف عـن عوامل نجاح تطبيـق نظـام إدارة أمـن المعلومـات في المؤسسـات الإيرانيـة. ولتحقيـق هذا الغرض تم تصميم استبانة كأداة لجمـع البيانـات، تـم توزيعهـا علـى عينـة قوامهـا (٣٥) فرداً. جاءت نتائج الدراسة أن مـن أهـم أسـباب تحقيـق نظـام أمـن المعلومـات دعـم الإدارة العليـا، وتـوفير سياسـة أمـن المعلومـات، والـوعي بـأمن المعلومـات، والتدريب على كيفية أمن المعلومات.

هدفت دراسة مونيرول وآخرون (**Munirul et al., 2011**) إلـى الكشـف عـن أصـول المعلومـات والتهديـدات المحتملـة للـنظم المصـرفية في أندونيسـيا، ومقارنـة عناصر أطر حوكمة أمن المعلومات والمعايير وأفضل الممارسات من خلال الإطـار الأولى لتحكم في أمن المعلومات في النظام المصرفي من خلال ثلاثة مستويات: وهي المستوى الاستراتيجي، التكتيكي، والتشغيلي، والفني. أظهرت نتائج الدراسة وجود حاجة إلى مراجعة أمن المعلومـات مـن قبـل أشـخاص متخصصـين، ووجـود حاجـة لتطوير حوكمة أمن المعلومات في البيئة المصرفية ونظم المعلومات.

هـدفت دراسـة صـالحي وعبـد الغفـور (**Salehi & Abdipour, 2011**) إلـى الكشف عن المعوقات التي تحول دون تطبيق نظم المعلومات الحاسوبية في طهران. تكونت عينة الدراسة من (١٠٠) شركة في مختلف القطاعات الصـناعية. اسـتخدمت الاسـتبانة لجمـع البيانـات والمـنهج الوصـفي التحليلـي لتحقيـق أهـداف الدراسـة. أظهرت نتائج الدراسة أن من أهم المعوقات التي تحول دون تطبيق نظم المعلومـات الحاسوبية الموارد البشرية والعوامل البيئية.

هدفت دراسة أكبري (**AKbari, 2012**) إلى التعرف على المخـاطر التشـغيلية المصرفية الإلكترونيـة والعوامـل المـؤثرة في الصـناعة المصـرفية في إيـران. تـم جمـع البيانات من خلال عينة عشوائية عنقودية بلغت (٣٠٠) موظفًا و(٣٨٤) عميلاً. وقـد

تم استخدام المنهج المسحي لتحقيق أهداف الدراسة. أظهرت النتائج أن أهم محاور المخاطر في بنك (ملي كرمنشاه) هي عدم دقة البيانات، وضعف الرقابة الداخلية، وضعف في البنية التحتية التكنوبوجية.

هدفت دراسة عبد الجابر (٢٠١٣) إلى الكشف عن مدى فاعلية إجراءات الرقابة الداخلية في الشركات الصناعية الأردنية المستخدِمة لنظم المعلومات المحاسبية الإلكترونية في تخفيض مخاطر أمن المعلومات لديها. ولتحقيق هذا الغرض تم تصميم استبانة وقد تم توزيعها على عينة الدراسة المكونة من (٣٠) شركة صناعية عاملة في المملكة الأردنية. أظهرت النتائج وجود معوقات وتحديات تواجه تطبيق إجراءات رقابة داخلية فعالة ومنه: عدم مواكبة التطور المتسارع لأساليب الاحتيال الإلكتروني، وعدم دعم الإدارة لأنشطة الرقابة الداخلية المتعلقة بأمن المعلومات.

لقد سلطت الدراسات السابقة الضوء على جملة من أمور أبرزها: خصائص البيئة التقنية وتكنولوجيا المعلومات وخصائص الأمن والسلامة، والمخاطر التشغيلية المصرفية الإلكترونية، وأهمية الرقابة في تحقيق أمن المعلومات، وعوامل نجاح تطبيق نظام إدارة أمن المعلومات. ويلاحظ بصفة عامة أن هذه الدراسة تبحث في مخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء وما سبل مواجهة تلك المخاطر.

ولقد استفادت الدراسة الحالية من الدراسات السابقة: فهم أعمق لموضوع ومشكلة البحث، وصياغة أهداف وأسئلة البحث، واختيار المنهجية وأداة جمع المعلومات المناسبة، وتصور واضح لمحاور ومجالات الدراسة التي تم بناء الاستبيان عليها، ومناقشة النتائج ووضع التوصيات.

منهجية الدراسة

تعتمد منهجية الدراسة على استخدام المنهج الوصفي التحليلي فيما يتعلق بالبيانات الخاصة بالإطار النظري للدراسة لعرض وتحديد المفاهيم الأساسية للدراسة.

أما بيانات الدراسة الميدانية فقد تم جمعها باستخدام أسلوب قائمة الاستقصاء (الاستبانة) التي تم تصميمها لأغراض الدراسة وتوزيعها على عينة من العاملين في مصارف محافظة البلقاء لقياس مدى التوافق أو الاختلاف بين إجابات عينة الدراسة.

أداة الدراسة

قام الباحث باستقصاء البيانات الأولية للدراسة الميدانية مستعيناً بأداة الدراسة الرئيسية (الاستبيان **Questionnaire**)، التي تم تصميمها استناداً إلى الدراسات السابقة والإطار النظري للدراسة. وتتكون الاستبانة من خمسة مجالات على النحو الآتي:

المجال الأول: ويحتوي على الفقرات (١-٨) المتعلقة بمخاطر مادية.

المجال الثاني: ويحتوي على الفقرات (٩-١٦) المتعلقة بمخاطر الأفراد.

المجال الثالث: ويحتوي على الفقرات (١٧-٢٧) المتعلقة بمخاطر العمليات.

المجال الرابع: ويحتوي على الفقرات (٢٨- ٣٧) المتعلقة بمخاطر البيانات.

المجال الخامس: ويحتوي على الفقرات (٣٨- ٤٨) المتعلقة بمخاطر شبكة الاتصال.

وتم الاستعانة بدراسات إسماعيل في تصمم الأداة. وقد تم تدريج الإجابة عن كل فقرات وفق مقياس ليكرت الخماسي، وحددت بخمس إجابات هي)دائماً، غالباً، أحياناً، نادراً، إطلاقاً) وتمثل (١،٢،٣،٤،٥) على التوالي. وقد اعتمدت الدراسة خمسة مستويات وهي: وقد اعتمدت الدراسة ثلاثة مستويات تم تحديدها

وفقاً للمعادلة التالية: (المدى الأعلى ـ المدى الأدنى مقسوماً على ثلاثة مستويات) (٥-١÷٣= ١,٣٣) والمستويات هي:

- من ١ - ٢,٣٣ مستوى ممارسة ضعيف.
- من ٢,٣٤ - ٣,٦٧ مستوى ممارسة متوسط.
- من ٣,٦٨ - ٥ درجة مستوى ممارسة مرتفع.

صدق الأداة

تم التأكد من صدق الأداة (**Validity**) المستخدمة في الدراسة، وذلك من خلال عرضها على مجموعة من المحكمين المتخصصين في تكنولوجيا المعلومات، والبالغ عددهم (٧) محكمين. تم الأخذ بملاحظاتهم فيما يتعلق بالتعديل والحذف والإضافة وإعادة الصياغة.

ثبات الأداة

للتأكد من ثبات أداة الدراسة، فقد تم التحقق بطريقة الاختبار وإعادة الاختبار (**test-retest**) بتطبيق الاختبار، وإعادة تطبيقه بعد أسبوعين على مجموعة من خارج عينة الدراسة مكوّنة من (٢٠) موظفًا، ومن ثم تم حساب معامل ارتباط بيرسون بين تقديراتهم في المرتين على أداة الدراسة ككل.

وتم أيضاً حساب معامل الثبات بطريقة الاتساق الداخلي حسب معادلة كرونباخ ألفا، والجدول رقم (١) يبين معامل الاتساق الداخلي وفق معادلة كرونباخ ألفا وثبات الإعادة للمجالات والأداة ككل واعتبرت هذه القيم ملائمة لغايات هذه الدراسة.

جدول (١): معامل الاتساق الداخلي كرونباخ ألفا وثبات الإعادة للمجالات والدرجة الكلية

المجال	ثبات الإعادة	الاتساق الداخلي
المخاطر المادية	0.87	0.84
مخاطر الأفراد	0.91	0.87
مخاطر العمليات	0.87	0.89
مخاطر البيانات	0.90	0.86
مخاطر شبكة الاتصال	0.88	0.88
الدرجة الكلية	0.90	0.92

مجتمع الدراسة وعينتها

تكوّن مجتمع الدراسة من كافة العاملين في المصارف التجارية في محافظة البلقاء والبالغ عددهم (٢٧٣) موظفًا، ونظرًا لصغر حجم مجتمع الدراسة تم مسحه كاملاً، متضمنًا المصارف العشرة بكافة فروعها في محافظة البلقاء. حيث وزعت (٢٧٣) استبانه على أفراد الدراسة، تم استرداد (٢٣٧) استبانة أي ما نسبته (٨٦,٨٪) من مجتمع الدراسة، تم استبعاد (١٢) استبانة لعدم صلاحيتها، وبذلك أصبح عدد الاستبانات الصالحة للتحليل (٢٢٥) استبانة، مشكلة بذلك ما نسبته (٨٢,٤٪) من مجتمع الدراسة.

المعالجات الإحصائية

تم حساب المتوسطات الحسابية والانحرافات المعيارية لمجالات الدراسة وفقراتها، والتكرارات المئوية.

نتائج السؤال الأول ونصه: «ما مخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها».

للإجابة عن هذا السؤال تم استخراج المتوسطات الحسابية والانحرافات المعيارية لمخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها، والجدول (٢) يوضح ذلك.

جدول (٢): المتوسطات الحسابية والانحرافات المعيارية لمخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها مرتبة تنازليًا حسب المتوسطات الحسابية

الرتبة	الرقم	المجال	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	2	مخاطر الأفراد	3.96	.553	مرتفعة
2	3	مخاطر العمليات	3.73	.567	متوسطة
3	1	المخاطر المادية	3.30	.596	متوسطة
4	5	مخاطر شبكة الاتصال	3.27	.582	متوسطة
5	4	مخاطر البيانات	2.80	.573	متوسطة
الدرجة الكلية			3.40	.421	متوسطة

يبين الجدول (٣) أن المتوسطات الحسابية قد تراوحت ما بين (٢,٨٠- ٣,٩٦)، حيث جاءت المخاطر المتعلقة بالأفراد في المرتبة الأولى بأعلى متوسط حسابي بلغ (٣,٩٦)، بينما جاءت مخاطر البيانات في المرتبة الأخيرة وبمتوسط حسابي بلغ (٢,٨٠)، وبلغ المتوسط الحسابي للأداة ككل (٣,٤٠) وبدرجة «متوسطة».

وقد تم حساب المتوسطات الحسابية والانحرافات المعيارية لتقديرات أفراد عينة الدراسة على فقرات كل مجال على حدة، حيث كانت على النحو التالي:

أولا: المخاطر المادية: اشتمل هذا المجال على ثماني فقرات، ويبين الجدول (٤) نتائجه.

جدول (٤): المتوسطات الحسابية والانحرافات المعيارية لفقرات المخاطر المادية مرتبة تنازليـًا حسب المتوسطات الحسابية

الرتبة	الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	1	وجود ضعف في المحيطات الأمنية (الجدران ـ الأبواب ـ الأقفال ـ بطاقات الدخول).	3.91	1.024	مرتفعة
2	7	البنية التحتية لا تتناسب مع حجم أعمال المصرف مما يؤثر على أمن المعلومات.	3.88	1.079	مرتفعة
3	2	نقص كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم خدمات نظم المعلومات.	3.85	1.102	مرتفعة
4	8	عدم وجود محددات في المباني تمنع دخول الموظفين إلى غرف التحكم.	3.66	1.139	متوسطة
5	4	يتم صيانة الأجهزة بحالات معينة كتعطل الجهاز نهائيـًا أو البرنامج عن العمل.	3.06	1.446	متوسطة
6	5	يسمح للموظف غير المختص من إجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات.	3.03	1.417	متوسطة
7	6	يتم الاحتفاظ بالنسخ الأصلية والاحتياطية من البرامج والملفات في مباني لا تتلاءم مع الظروف والتغيرات الطبيعية.	2.61	1.312	متوسطة
8	3	عدم توفر مصدر بديل للكهرباء في حالة انقطاع التيار الكهربائي.	2.36	1.303	متوسطة
		المخاطر المادية	3.30	.596	متوسطة

يبين الجدول (٤) أن المتوسطات الحسابية قد تراوحت مابين (٢.٣٦-٣.٩١)، حيث جاءت الفقرة رقم (١) والتي تنص على «وجود ضعف في المحيطات الأمنية (الجدران – الأبواب – الأقفال – بطاقات الدخول)» في المرتبة الأولى وبمتوسط حسابي بلغ (٣.٩١) وبدرجة «مرتفعة»، بينما جاءت الفقرة رقم (٣) ونصها «عدم توفر مصدر بديل للكهرباء في حالة انقطاع التيار الكهربائي» بالمرتبة الأخيرة وبمتوسط حسابي بلغ (٢.٣٦) وبدرجة «متوسطة». وبلغ المتوسط الحسابي للمجال ككل (٣.٣٠) وبدرجة «متوسطة» وبالمرتبة الثالثة من بين المخاطر. وقد يرجع السبب في حصول المجال على درجة متوسطة إلى وجود عدة مخاطر تهدد أمن المعلومات في المصارف الأردنية مثل: ضعف المحطات الأمنية المتعلقة بجدران الحماية وبطاقات الدخول وأبواب الحماية. اتفقت نتائج الدراسة مع نتائج دراسة أكبري (**AKbari, 2012**) بأن أهم محاور المخاطر في بنك (ملي كرمنشاه) هي عدم دقة البيانات، وضعف الرقابة الداخلية، وضعف في البنية التحتية التكنولوجية.

ثانيـًا: مخاطر الأفراد: اشتمل هذا المجال على ثماني فقرات، ويبين الجدول (٥) نتائجه.

جدول (٥): المتوسطات الحسابية والانحرافات المعيارية لفقرات مخاطر الأفراد مرتبة تنازليـًا حسب المتوسطات الحسابية

الرتبة	الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	9	قلة البرامج التدريبية لاستخدام تقنيات حماية أمن المعلومات.	**4.11**	**.948**	مرتفعة
2	12	نقص وعي العاملين بمهددات أمن المعلومات.	**4.04**	**.963**	مرتفعة
3	14	عدم وجود عقوبات للعاملين المهملين أو المتسببين في تسرب المعلومات.	**4.00**	**.991**	مرتفعة
4	10	قلة الكفاءة المهنية عند المستفيدين من التعامل مع نظم المعلومات.	**3.96**	**1.089**	مرتفعة
5	11	نقص الحوافز المادية للعاملين على حماية أمن المعلومات.	**3.93**	**1.278**	مرتفعة
6	13	غياب وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات.	**3.89**	**1.114**	مرتفعة

الرتبة	الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
7	15	غياب سياسة تحديد الصلاحيات لمستخدمي النظام يتناسب مع حجم ونوع الأعمال الموكلة لهم.	**3.88**	**1.053**	مرتفعة
8	16	توكيل مسؤولية حفظ قوائم الحسابات وملفات البيانات إلى أشخاص لا تتوفر فيهم الناحية الأمنية.	**3.87**	**1.106**	مرتفعة
مخاطر الأفراد			**3.96**	**.553**	مرتفعة

يبين الجدول (٥) أن المتوسطات الحسابية قد تراوحت مابين (**3.87-4.11**)، حيث جاءت الفقرة رقم (٩) التي تنص على «قلة البرامج التدريبية لاستخدام تقنيات حماية أمن المعلومات» في المرتبة الأولى وبمتوسط حسابي بلغ (**4.11**) وبدرجة «مرتفعة»، بينما جاءت الفقرة رقم (١٦) ونصها «توكيل مسؤولية حفظ قوائم الحسابات وملفات البيانات إلى أشخاص لا تتوفر فيهم الناحية الأمنية» بالمرتبة الأخيرة وبمتوسط حسابي بلغ (**3.87**) وبدرجة «مرتفعة». وبلغ المتوسط الحسابي للمجال ككل (**3.96**) وبدرجة «مرتفعة». وقد يفسَر السبب في حصول المجال على درجة «مرتفعة»، وبالمرتبة الأولى من بين المخاطر، إلى أن الأفراد هم من أهم الأسباب التي تؤدي إلى مخاطر في نظم أمن المعلومات وذلك لما يقوم به الأفراد من سرقة بيانات ومعلومات، وتجسس، وتحريف...وغيرها. ومن ناحية أخرى قد يكون السبب قلة الكفاءة المهنية عند المستفيدين، وقلة البرامج التدريبية لاستخدام تقنيات حماية أمن المعلومات، وتدني وعي العاملين بمهددات أمن المعلومات. اتفقت

نتائج الدراسة مع نتائج دراسة صالحي وعبد الغفور (Salehi & Abdipour, 2011) بأن من أهم المعوقات التي تحول دون تطبيق نظم المعلومات الحاسوبية الموارد البشرية والعوامل البيئية. كما اتفقت نتائج الدراسة مع نتائج دراسة البحيصي والشريف (٢٠٠٨) بحدوث مخاطر نظم المعلومات المحاسبية الإلكترونية ترجع إلى أسباب تتعلق بموظفي البنك نتيجة قلة الخبرة، وقلة الوعي بأمن المعلومات، وضعف التدريب، إضافة إلى أسباب تتعلق بإدارة المصرف. وتناغمت نتائج الدراسة مع نتائج دراسة كاظمي وأخرون (Kazemi et al., 2012) بأن من أهم أسباب تحقيق نظام أمن المعلومات الوعي بأمن المعلومات، والتدريب على كيفية أمن المعلومات. كما اتفقت نتائج الدراسة مع نتائج دراسة الحمادي (٢٠١٠) بوجود مخاطر في العمليات تهدد أمن المعلومات والاتصالات، ووجود أثر ذي دلالة احصائية لقلة الخبرة والتدريب لدى الموظفين على أمن المعلومات والاتصالات.

ثالثًا: مخاطر العمليات: اشتمل هذا المجال على إحدى عشرة فقرة، ويبين الجدول (٦) نتائجه.

جدول (٦): المتوسطات الحسابية والانحرافات المعيارية لفقرات مخاطر العمليات مرتبة تنازليًا حسب المتوسطات الحسابية

الرتبة	الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	**27**	عدم تنفيذ اختبار دوري يكشف نقاط ضعف أمن المعلومات.	**3.95**	**1.254**	مرتفعة
2	**17**	عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم.	**3.90**	**1.127**	مرتفعة
3	**18**	عدم تحديث أنظمة تشغيل جدران الحماية بالنظام.	**3.84**	**.989**	مرتفعة
4	**24**	عدم توفر اختبارات التسلل الفاحص لتحديد النقاط القابلة للاختراق في النظام.	**3.82**	**1.050**	مرتفعة
5	**23**	ضعف تلبية نظم أمن المعلومات المطبقة للاحتياجات التشغيلية رغم تطور حجم العمليات وطبيعتها.	**3.80**	**1.070**	مرتفعة
6	**19**	حجب الخدمة عن المستخدمين الشرعيين.	**3.79**	**1.104**	مرتفعة
6	**21**	عدم توفر سجلات الأداء للحفاظ على أنشطة المستخدم لدواعي متعلقة بأمن المعلومات.	**3.79**	**1.149**	مرتفعة

الرتبة	الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
8	**25**	ضعف نظام تصنيف ملفات البيانات والبرامج إلى عدة مستويات من السرية.	**3.74**	**1.248**	مرتفعة
9	**26**	ضعف نظام الرقابة لمنع مشغلي الجهاز من الحصول على أية بيانات غير لازمة لتشغيل الجهاز.	**3.72**	**1.051**	مرتفعة
10	**22**	متابعة عمليات القيام بتشغيل أوامر لأكثر من مرة بهدف الاختلاس أو التلاعب.	**3.55**	**1.176**	متوسطة
11	**20**	تسليم الوثائق الحسابية إلى أشخاص بغرض تمزيقها أو إتلافها.	**3.15**	**1.296**	متوسطة
		مخاطر العمليات	**3.73**	**.567**	مرتفعة

يبين الجدول (٦) أن المتوسطات الحسابية قد تراوحت مابين (**3.15**-**3.95**)، حيث جاءت الفقرة رقم (٢٧) التي تنص على «عدم تنفيذ اختبار دوري يكشف نقاط ضعف أمن المعلومات» في المرتبة الأولى وبمتوسط حسابي بلغ (**3.95**) وبدرجة «مرتفعة»، بينما جاءت الفقرة رقم (٢٠) ونصها «تسليم الوثائق الحسابية إلى أشخاص بغرض تمزيقها أو إتلافها» بالمرتبة الأخيرة وبمتوسط حسابي بلغ (**3.15**) وبدرجة «متوسطة». وبلغ المتوسط الحسابي للمجال ككل (**3.73**) وبدرجة «متوسطة» وبالمرتبة الثانية من بين المخاطر. وقد يكون السبب في

ذلك وجود خلل في أنظمة العمليات التي يقوم المعنيون في المصارف كضعف نظام الرقابة، وعدم قيام إدارة أمن المعلومات بإجراء اختبار دوري يكشف نقاط الضعف في أمن المعلومات، وعدم تحديث أنظمة تشغيل جدران الحماية في النظام، وضعف نظام تصنيف ملفات البيانات والبرامج إلى عدة مستويات من السرية. اتفقت نتائج الدراسة مع نتائج دراسة حمادة (٢٠١٠) إلى أن هناك تأثيرًا كبيرًا للضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية في الشركات. وتناغمت نتائج الدراسة مع نتائج دراسة كاظمي وأخرون **(Kazemi et al., 2012)** بأن من أهم أسباب تحقيق نظام أمن المعلومات دعم الإدارة العليا، وتوفير سياسة أمن المعلومات.

رابعًا: مخاطر البيانات: اشتمل هذا المجال على عشر فقرات، ويبين الجدول (٧) نتائجه.

جدول (٧): المتوسطات الحسابية والانحرافات المعيارية لفقرات مخاطر البيانات مرتبة تنازليًا حسب المتوسطات الحسابية

الرتبة	الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	33	طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.	3.72	1.097	مرتفعة
2	36	غياب متابعة كلمات السر للموظفين وتغيرها باستمرار.	3.32	1.394	متوسطة
3	32	عدم توفر عدة مستويات أمنية لقواعد البيانات المستخدمة.	3.23	1.402	متوسطة
4	29	عمل نسخ غير مرخص بها من البيانات بهدف سرقتها.	3.15	1.468	متوسطة
5	28	طمس أو تدمير بنود دقيقة من البيانات.	2.53	1.268	متوسطة
6	31	اشراك بعض الموظفين في استخدام كلمة السر نفسها للوصول إلى البيانات.	2.50	1.415	متوسطة
7	34	تحريف البيانات الموجودة كزيادة رقم على الرقم الفعلي.	2.44	1.368	متوسطة
8	35	الادخال المتعمد لبيانات غير سليمة بواسطة (أشخاص أو موظفين).	2.42	1.294	متوسطة
9	30	توليد مخرجات زائفة (غير صحيحة) من البيانات.	2.36	1.288	متوسطة
9	37	اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.	2.36	1.360	متوسطة
		مخاطر البيانات	2.80	.573	متوسطة

يبين الجدول (٧) أن المتوسطات الحسابية قد تراوحت مابين (**2.36**-**3.72**)، حيث جاءت الفقرة رقم (٣٣) التي تنص على «طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك» في المرتبة الأولى وبمتوسط حسابي بلغ (**3.72**) وبدرجة «مرتفعة»، بينما جاءت الفقرتان رقم (٣٠) (٣٧) ونصهما «توليد مخرجات زائفة (غير صحيحة) من البيانات». و«اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين» بالمرتبة الأخيرة وبمتوسط حسابي بلغ (**2.36**) وبدرجة «متوسطة». وبلغ المتوسط الحسابي للمجال ككل (**2.80**) وبدرجة متوسطة وبالمرتبة الأخيرة من بين المخاطر. وقد يعزى السبب في حصول المجال على درجة متوسطة إلى وجود مخاطر تهدد أمن البيانات في المصارف منها مقدرة بعض الأشخاص على تحريف البيانات أو طمسها، أو طبع بعض البيانات بواسطة أشخاص غير مصرح لهم بذلك، أو قد يكون السبب ضعف في الأجهزة المستخدمة مما يؤدي إلى اعتراض وصول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين، وعدم توفر عدة مستويات أمنية لقواعد البيانات المستخدمة. اتفقت نتائج الدراسة مع نتائج دراسة موحد وأخرون (**Mohd et al., 2010**) بوجود تحديات تعترض البيانات منها: خرق البيانات، والافتقار للتوثيق والترخيص، وسرقة وتعديل وحذف المعلومات في النظام.

خامسـاً: مخـاطر شـبكة الاتصـال: اشـتمل هـذا المجـال علـى عشـر فقـرات، ويبـين الجدول (٨) نتائجه.

جدول (٨): المتوسطات الحسابية والانحرافات المعيارية لفقرات مخاطر شبكة الاتصال مرتبة تنازلياً حسب المتوسطات الحسابية

الرتبة	الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
1	**38**	غياب متابعة تحديث مخطط الشبكة الأمنية بشكل دوري.	**3.69**	**1.199**	مرتفعة
2	**42**	عدم وجود خاصية منع التلصص **(IPS)** في جدران حماية شبكة الاتصال.	**3.67**	**1.090**	متوسطة
3	**39**	يستطيع مستخدمو النظام الوصول إلى موارد الشبكة بصعوبة.	**3.66**	**1.272**	متوسطة
4	**45**	عدم توفر خاصية اتصال الشبكة الافتراضية **(VPN)** في معظم جدران الحماية.	**3.47**	**1.261**	متوسطة
5	**43**	عدم تحديث أجهزة الوسيط **(Proxy)** بانتظام.	**3.44**	**1.249**	متوسطة
6	**44**	عدم وضوح مخطط جدران الحماية والخوادم والموجهات المتصلة بالشبكة.	**3.17**	**1.472**	متوسطة

الرتبة	الرقم	الفقرات	المتوسط الحسابي	الانحراف المعياري	الدرجة
7	40	نادراً ما يتم تثبيت تحديثات أجهزة نقاط الشبكة لا سلكي Access (Points) دورياً.	3.15	1.328	متوسطة
8	48	عدم تحديث خاصية تصفية المواقع المرغوبة في جدران حماية الشبكة.	3.03	1.417	متوسطة
9	41	عدم تحديث خاصية الحماية من البريد الدعائي (Spam) في جدران الحماية.	2.72	1.341	متوسطة
10	46	عدم تحديث خاصية الحماية من الفيروسات في جدران حماية الشبكات.	2.69	1.326	متوسطة
مخاطر شبكة الاتصال			3.27	.582	متوسطة

يبين الجدول (٨) أن المتوسطات الحسابية قد تراوحت مابين (2.69-3.69)، حيث جاءت الفقرة رقم (٣٨) التي تنص على «غياب متابعة تحديث مخطط الشبكة الأمني بشكل دوري» في المرتبة الأولى وبمتوسط حسابي بلغ (3.69) وبدرجة «مرتفعة»، بينما جاءت الفقرة رقم (٤٦) ونصها «عدم تحديث خاصية الحماية من الفيروسات في جدران حماية الشبكات» بالمرتبة الأخيرة وبمتوسط حسابي بلغ (2.69) وبدرجة «متوسطة». وبلغ المتوسط الحسابي للمجال ككل (3.27) وبدرجة «متوسطة» وبالمرتبة الرابعة من بين المخاطر. وقد يفسر السبب بغياب متابعة تحديث مخطط الشبكة الأمني بشكل دوري من قبل المعنيين، وضعف

في نظام الشبكة لتخدم كافة العمليات بين مستخدمي الشبكة في ظل التغيرات والتطورات المتسارعة في أنظمة الشبكات. اتفقت نتائج الدراسة مع نتائج دراسة مونيرول وأخرون (**Munirul et al., 2011**) بوجود حاجة إلى مراجعة أمن المعلومات من قبل أشخاص متخصصين، ووجود حاجة لتطوير حوكمة أمن المعلومات في البيئة المصرفية ونظم المعلومات. وتناغمت نتائج الدراسة مع نتائج دراسة عبد الجابر (٢٠١٣) بوجود معوقات وتحديات تواجه تطبيق إجراءات رقابة داخلية فعالة ومنها عدم مواكبة التطور المتسارع لأساليب الاحتيال الإلكتروني، وأيضا عدم دعم الإدارة لأنشطة الرقابة الداخلية المتعلقة بأمن المعلومات.

٣. نتائج السؤال الثاني ونصه: «ما سبل مواجهة مخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها».

للإجابة عن هذا السؤال تم احتساب التكرارات والنسب المئوية لإجابات أفراد عينة الدراسة سبل مواجهة مخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء كما موظفوها، والبالغ عددهم (٢٢٥) مستجيبًا، حيث تم احتساب التكرارات والنسب المئوية من خلال المعادلة التالية: التكرار/ مجموع التكرار ×١٠٠. والجدول (٧) يوضح ذلك.

جدول (٩) التكرارات والنسب المئوية ما سبل مواجهة مخاطر الأمن المعلوماتي في المصارف التجارية العاملة في محافظة البلقاء كما يراها موظفوها مرتبة ترتيباً تنازلياً

الرتبة		التكرار	النسبة من الإجابات	النسبة من العينة
1	تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمان نظام المعلومات.	**64**	**13.6**	**28.4**
2	توفير الحوافز (المادية والمعنوية) المناسبة للمبدعين والمتفوقين في مجال أمن المعلومات.	**63**	**13.3**	**28.0**
3	استقطاب خبراء حماية نظم المعلومات للعمال بمراكز نظام المعلومات.	**52**	**11.0**	**23.1**
4	زيادة الموازنة المخصصة لأمان المعلومات ضمن موازنة تطوير تكنولوجيا المعلومات والاتصالات.	**50**	**10.6**	**22.2**
5	فحص أنظمة المعلومات للتحقق من الالتزام بمعايير الأداء الأمني.	**49**	**10.4**	**21.8**
6	استخدام برامج حماية فعالة لمنع محاولات الاختراق والتعدي على نظم المعلومات.	**43**	**9.1**	**19.1**
7	وضع ضوابط لتبادل المعلومات مع الجهات المعنية خارج المصارف.	**41**	**8.7**	**18.2**
8	وجود فريق استجابة للتهديدات التي تعرض لها النظام.	**36**	**7.6**	**16.0**
9	الاستفادة من خادمات (التعهيد) الأطراف الخارجية ضمن ضوابط أمنية وشروط جزائية متفق عليها.	**32**	**6.8**	**14.2**
10	استخدام وسائل التحقق من الشخصية مثل بصمة العين.	**21**	**4.4**	**9.3**

الرتبة		التكرار	النسبة من الإجابات	النسبة من العينة
10	استخدام برامج مكافحة الفيروسات لحماية الأنظمة.	**21**	**4.4**	**9.3**
المجموع		**472**	**100.0**	**100.0**

يتبين من الجدول (٩) «تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمان نظام المعلومات» جاءت بالمرتبة الأولى بأعلى تكرار بلغ (٦٤)، حيث بلغت النسبة المئوية من مجموع الإجابات (١٣.٦)، وبنسبة مئوية من العينة (٢٨.٤)، وتلاها في المرتبة الثانية " توفير الحوافز (المادية والمعنوية) المناسبة للمبدعين والمتفوقين في مجال أمن المعلومات " بتكرار بلغ (٦٣)، حيث بلغت النسبة المئوية من مجموع الإجابات (١٣.٣)، وبنسبة مئوية من العينة (٢٨.٠)، تلاها المرتبة الثالثة "استقطاب خبراء حماية نظم المعلوماات للعمال بمراكز نظام المعلومات" بتكرار بلغ (٥٢) حيث بلغت النسبة المئوية من مجموع الإجابات (٤.٤)، وبنسبة مئوية من العينة (٢٣.١). بينما جاءت " استخدام برامج مكافحة الفيروسات لحماية الأنظمة " بالمرتبة الأخيرة بتكرار بلغ (٢١) حيث بلغت النسبة المئوية من مجموع الإجابات (٥.٦) وبنسبة مئوية من العينة (٩.٣). وقد يفسر السبب في حصول المقترح تعزيز البنى التحتية لتكنولوجيا المعلومات بما يضمن تعزيز أمان نظام المعلومات " بالمرتبة الأولى إلى وجود حاجة إلى تعزيز البنى التحتية لتكتولوجيا المعلومات بصورة مستمرة وذلك لطبيعة المستجدات الحاصلة في تكنولوجيا المعلومات والاتصالات، أما السبب في حصول المقترح "استخدام برامج مكافحة الفيروسات لحماية الأنظمة " بالمرتبة الأخيرة وذلك لأن من الطبيعي أن يكون على جميع أجهزة الحاسوب برامج لمكافحة الفيروسات والمهم تحديثها بإستمرار. اتفقت نتائج الدراسة مع نتائج دراسة القطناني (٢٠٠٧) بوجود فروق ذات

دلالة إحصائية بين آراء عينتي الدراسة لهذه المصارف بشأن مدى تأثير خصائص البيئة التقنية والتكنولوجية لنظم المعلومات في مخاطر الرقابة التشغيلية في المصارف الأردنية.

التوصيات

في ضوء النتائج السابقة توصي الدراسة بما يأتي:

١. لتعزيز الأمن التنظيمي على إدارة المصارف أن تولي عملية التدريب أهمية أكبر لتمكن الأفراد من زيادة معرفتهم بالقضايا المستجدة والنواحي الأمنية، وهنا يقترح الباحث أن تشمل هذه الدوا رت التدريبية:
- دورات في تدقيق نظم المعلومات وتحسين كفاءة نظم المعلومات.
- دورات في بناء خطط الإستعادة و إدارة الأزمات.
- دورات في أمن الأنظمة المحوسبة، والتشفير، ونظم التشغيل (**LINUX**).
- دورات في تطبيق المعايير الدولية لأمن المعلومات.

٢. تزويد المصارف بالتقنيات المتطورة بشكل مستمر في مجال نظم الحماية المادية من خلال التصميم المناسب لغرف النظام ومراعاة الشروط الأمنية كالدخول ببطاقات ممغنطة، وفي مجال المعلوماتية كالوسائل البيولوجية لتحديد شخصية وصلاحية مستخدم النظام.

٣. اتباع بعض الإجراءات الأمنية اللازمة لإحكام أمن المعلومات خصوصًا في ظل ارتباط الشبكة المحلية بشبكة الإنترنت؛ ومن تلك الإجراءات تقنية الحوائط النارية والتشفير ودعم أجهزة عدم انقطاع التيار الكهربائي.

٤. توفر عدد كافٍ من موظفي الحماية ممن يحملون مؤهلات علمية تتناسب مع متطلبات أعمال الحماية، وتوفر وصف وظيفي للوظائف المتعلقة بالحماية والأمان مع تشكيل اللجان والمجالس المطلوبة لتيسير إجراءات العمل في مجال الأمن المعلوماتي.

٥. توفير الكوادر من ذوي الخبرة في مجال الحماية وتحفيزهم بالمكآفات المالية والمعنوية. وإعطاء السلوك النزيه والتمتع بالأخلاق العالية والصدق

أولوية عالية عند التوظيف، والتأكيد من محافظة الموظفين على مستويات تلك الأخلاقيات.

٦. تحديث جميع البرامج بما في ذلك أحدث نسخة من برامج التشغيل الذي يستخدم عن بعد من خلال تحديث تلقائي بشكل يومي عند بدء تشغيل الجهاز.

٧. مراقبة الحركة المرورية عبر الشبكة باستخدام أحد برامج مراقبة بيانات الشبكة، حيث يتم من خلاله تجميع البيانات الداخلية والخارجية، للكشف عن محاولات التسلل عبر الشبكة وتحليل المشكلات الشبكية، وتصفية وحجب المحتوى غير المرغوب فيه بالدخول إلى الشبكة.

٨. وضع ضوابط أمن ورقابة المعلومات المتداولة بكافة أشكالها، سواء كانت ورقية أم اتصالات سلكية ولاسلكية والإنترنت، والعمل على سن التشريعات اللازمة لأمن المعلومات والنظم والشبكات المعلوماتية. ووجود خطة حماية أمنية شاملة ضرورة وضع اجراءات تضمن استمرارية عمل وجاهزية نظم المعلومات؛ للعمل في حالة الأزمات من خلال استخدام تجهيزات منيعة أو مرتبة بحيث تستطيع اكتشاف المخاطر قبل حدوثها والحد من وقوعها. وكذلك العمل على تعمية أو تشفير المعلومات عند الحفظ والنقل والتخزين على مختلف الوسائط كي لا يتمكن أحد من اختراقها.

٩. تحسين آليات ضبط الوصول لنظم المعلومات، ووضع برامج وإجراءات خاصة بالأدوار والصلاحيات ضمن نظم المعلومات والتركيز على ضرورات أمن المعلومات ومرتكزاته الثلاثة: التوفر، والسلامة، والسرية.

دراسات مستقبلية

- إجراء دراسة مقارنة عن مصادر مخاطر الأمن المعلوماتي بمصارف المملكة الأردنية الهاشمية كافة.
- إجراء دراسة عن دور التقنيات الحديثة في مواجهة مخاطر الأمن المعلوماتي بالمصارف الأرنية كافة.
- إجراء دراسة عن المعوقات التي تحد من فاعلية استخدام التقنية الحديثة في حماية نظم أمن المعلومات.

قائمة المراجع

البحيصي، عصام والشريف، حرية (٢٠٠٨). مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة. **مجلة الجامعة الإسلامية (سلسلة الدراسات الإنسانية)**. ٦(٢)، ٨٩٥- ٩٢٣.

حمادة، رشا (٢٠١٠). أثر الضوابط الرقابية العامة لنظم المعلومات المحاسبية الإلكترونية في زيادة موثوقية المعلومات المحاسبية. **مجلة جامعة دمشق للعلوم الاقتصادية والقانونية**. ٢٦(١): ٣٠٥-٣٣٤.

الحمادي، علي (٢٠١٠). **أنموذج مقترح لإدارة أمن المعلومات والاتصالات في ظل البيئة الشبكية**. رسالة ماجستير غير منشورة. جامعة الشرق الأوسط. الأردن.

داود، حسن طاهر(٢٠٠٢). **الحاسب وأمن المعلومات**. الرياض: معهد الإدارة العامة.

درويش، علي (٢٠٠٥). **تطبيقات الحكومة الإلكترونية ـ دراسة ميدانية على إدارة الجنسية والإقامة بدبي**، رسالة ماجستير غير منشورة - جامعة نايف العربية للعلوم الأمنية.

الدنف، أيمن (٢٠١٣). **واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها**. رسالة ماجستير غير منشورة. الجامعة الإسلامية- غزة.

السالمي، علاء عبد الرازق (٢٠٠٨). **الإدارة الالكترونية**، عمان، الأردن: دار وائل للنشر.

عبد الجابر، يوسف (٢٠١٣). **مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية**. رسالة ماجستير غير منشورة. جامعة الشرق الأوسط. الأردن.

القطناني، خالد (٢٠٠٧). أثر خصائص البيئة التقنية وتكنولوجيا المعلومات في مخاطر الرقابة التشغيلية "دراسة تحليلية في المصارف الأردنية. **مجلة المنارة**. ١٣ (٢). ٩-٣٩.

المركز القومي للمعلومات (٢٠١٠). **مقدمة عن سياسات و معايير أمن المعلومات**. السودان.

ميلاد، عبد المجيد (٢٠٠٦). نشر الطمأنينة وبناء الثقة في العصر الرقمي.استرجع بتاريخ ٢٧/ ٨/ ٢٠١٤ من الموقع **www.abdelmajid-miled.com**

Akbari, P (2012). A Study on Factors Affecting Operational Electronic Banking Risks in Iran Banking Industry (Case Study: Kermanshah Melli Bank). Int. J. Manag. Bus. Res. 2 (2), pp 123- 135.

Brock, Linda (2013). The market value of information system (IS) security for e-banking. Online Journal of Applied Knowledge Management. 1(1), pp 1-17.

Kazemi, M., Khajouei, H and Nasrabadi, H (2012). Evaluation of information security management system success factors: Case study of Municipal organization, African Journal of Business Management. 6(14), pp 4982-4989.

Mohd, A., Rayvieana, R ., Leau, B and Tan, F (2010). Security Issues on Banking Systems. International Journal of Computer Science and Information Technologies. 1 (4), pp 268-272.

Munirul, U., Zuraini, I and Zailani S (2011). A Framework for the Governance of Information Security in Banking System. Journal of Information Assurance & Cyber security. 1(3). pp 0-12

Raval, V and Fichadia, A (2007). Risk, Controls, and Security: Concepts and Applications, England: John Wiley and Sons.

Romney, M and Steinbart, P (2012). Accounting Information Systems", 12th edition, England: Pearson Education.

Salehi, M. & Abdipour, A. (2011). A Study Of The Barriers Of Implementation Of Accounting Information System: Case Of Listed Companies In Tehran Stock Exchange. Journal Of Economics And Behavioral Studies, 2 (2), pp 76-85.

Turban, E., Leidner, D and Wetherb, J (2008). Information Technology for management :transforming organization in the digital economy. Francisco: Efraim Turban. Pp 187-198.

Whitman, M and Mattod, H (2011). Principles of Information Security, 4th edition, Boston: Cengage Learning - Course Technology.