تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية: دراسة وصفية

Evaluating the impact of cyber threats on accounting information systems in Libyan financial institutions: a descriptive study

عبد السلام عطية عبد السلام يوسف
حاصل علي درجة الماجستير في المحاسبة - كلية الاقتصاد والعلوم السياسية - جامعة طرابلس

الملخص:

يهدف هذا البحث إلى تقييم تأثير التهديدات السيبرانية على نُظم المعلومات المحاسبية في المؤسسات المالية الليبية، كما يهدف البحث إلي تحليل الدراسات السابقة التي تناولت تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي وليبيا، وذلك لاستخلاص النتائج والتوصيات المهمة.

تم اعتماد المنهجية الوصفية لهذا البحث، حيث تم اختيار مجموعة من الدراسات السابقة التي بحثت وتعمقت في تقييم تأثير التهديدات السيبرانية على نُظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي بشكل عام وفي ليبيا بشكل خاص. ستشمل العينة مجموعة متنوعة من الدراسات لباحثين من ذوي الخبرة المهنية في هذه التخصص، وسيتم قراءة وتحليل هذه الدراسات للخروج بمجموعة من النتائج والتوصيات.

وتوصل البحث إلي أن المؤسسات المالية الليبية تواجه تهديدات سيبرانية متزايدة ومتنوعة، وتشمل هذه التهديدات الاختراقات الهجمات الإلكترونية، سرقة البيانات المالية، التجسس الصناعي، وتعطيل الخدمات المصرفية عبر الإنترنت. هذه التهديدات تسبب تأثيرًا سلبيًا على نظم المعلومات المحاسبية وتمثل خطرًا على السرية والموثوقية والتوافرية. وتوصل البحث إلي أن هناك عدة نقاط ضعف في نظم

المعلومات المحاسبية في المؤسسات المالية الليبية، وتشمل هذه النقاط ضعف في رصد وكشف هجمات السيبرانية، نقص في التدريب والوعي الأمني للموظفين، ضعف في إجراءات التحقق والتحكم الداخلي، وعدم وجود استراتيجيات شاملة للأمن السيبراني. كما توصل البحث إلي التهديدات السيبرانية تسبب تأثيرًا اقتصاديًا كبيرًا على المؤسسات المالية الليبية، وتشمل هذه التأثيرات تكاليف استعادة البيانات وإصلاح الأضرار، فقدان الثقة لدى العملاء والمستثمرين، توقف الخدمات المصرفية، وتعرض الشركات للمسائل القانونية والتعويضات المالية.وفي الختام، أوصي البحث أن المؤسسات المالية يجب عليها تقييم وتحديث سياسات الأمان والإجراءات المتعلقة بنظم المعلومات المحاسبية لتوفير حماية فعالة ضد التهديدات السيبرانية، كما ينبغي أيضًا تنفيذ نظم رصد وكشف متقدمة للكشف المبكر عن الهجمات السيبرانية والتعامل معها بشكل سريع وفعال. كما ينبغي على المؤسسات المالية تعزيز التعاون مع الهيئات الحكومية ذات الصلة والمؤسسات الأمنية والخبراء في مجال الأمن السيبراني.

الكلمات المفتاحية: التهديدات السيبرانية، نظم المعلومات المحاسبية، المؤسسات المالية، ليبيا، دراسة وصفية.

Abstract:

This research aims to evaluate the impact of cyber threats on accounting information systems in Libyan financial institutions. The research also aims to analyze previous studies that dealt with evaluating the impact of cyber threats on accounting information systems in financial institutions in the Arab world and Libya, in order to extract important results and recommendations. A descriptive methodology was adopted for this research, as a group of previous studies were selected that investigated and delved into the assessment of the impact of

cyber threats on accounting information systems in financial institutions in the Arab world in general and in Libya in particular. The sample will include a variety of studies by researchers with professional experience in this specialty, and these studies will be read and analyzed to come up with a set of results and recommendations. The research found that Libyan financial institutions face increasing and diverse cyber threats, and these threats include hacking, electronic attacks, theft of financial data, industrial espionage, and disruption of online banking services. These threats cause a negative impact on accounting information systems and represent a risk to confidentiality, reliability and availability. The research found that there are several weaknesses in the accounting information systems in Libyan financial institutions. These points include weakness in monitoring and detecting cyber-attacks, a lack of training and security awareness for employees, weakness in internal verification and control procedures, and the lack of comprehensive cyber security strategies. The research also found that cyber threats cause a significant economic impact on Libyan financial institutions. These impacts include the costs of data recovery and damage repair, loss of confidence among customers and investors, cessation of banking services, and exposure of companies to legal issues and financial compensation. In conclusion, the research recommended that financial institutions should It should evaluate and update security policies and

procedures related to accounting information systems to provide effective protection against cyber threats. It should also implement advanced monitoring and detection systems for early detection of cyber-attacks and dealing with them quickly and effectively. Financial institutions should also enhance cooperation with relevant government agencies, security institutions and experts in the field of cybersecurity.

Keywords: cyber threats, accounting information systems, financial institutions, Libya, descriptive study.

1- المقدمة:

تواجه مؤسسات الأعمال والمنظمات في العصر الحديث العديد من التحديات نتيجة التطور الهائل في تكنولوجيا المعلومات والاتصالات، وما رافقه من ظهور العديد من التهديدات الأمنية سواء كانت داخلية أو خارجية، والتي باتت تشكل خطراً حقيقياً على أمن وسرية البيانات والمعلومات (موسي، 2022).

وتعد المؤسسات والشركات المالية من أكثر أنواع المؤسسات عرضة للتهديدات السيبرانية، نظراً لحساسية البيانات المالية التي تتعامل معها، سواءً الخاصة بعملياتها الداخلية أو بيانات العملاء من أفراد وشركات (علي ومفتاح، 2017).

وقد أصبحت ظاهرة الاختراقات الإلكترونية والسرقات المعلوماتية المستهدفة للبنوك وشركات التأمين أمراً شائعاً ومتكرراً، مما قد يتسبب في كوارث مالية وخسائر فادحة لهذه المؤسسات ولعملائها، فضلاً عن تآكل الثقة في موثوقية وأمن هذه المعلومات وخصوصيتها (عبد المجيد واخرون، 2023).

وتأتي ليبيا كغيرها من الدول النامية معرضة بدرجة كبيرة لمخاطر الجرائم السيبرانية المستهدفة للقطاع المصرفي والمالي، نظراً لضعف بنيتها التحتية التقنية

وأنظمتها المعلوماتية، فضلاً عن غياب التشريعات الرادعة وعدم الالتزام بمعايير الأمن السيبراني (عبد المهدي، 2020).

وعليه، تأتي هذه الدراسة لتسليط الضوء على واقع التهديدات السيبرانية المستهدفة لأنظمة المعلومات المحاسبية في المؤسسات والشركات المالية الليبية، وتقييم مدى تأثير تلك التهديدات على موثوقية وسلامة وسرية تلك الأنظمة والبيانات المالية المخزنة فيها. وتكمن أهمية هذه الدراسة في كونها تلقي الضوء على واقع التهديدات الأمنية السيبرانية التي تواجه المؤسسات المالية في ليبيا، والتي قد تتسبب في كوارث مالية واقتصادية في حال تعرض أنظمة المعلومات المحاسبية الحساسة فيها لعمليات اختراق أو سرقة بيانات (فتوح، 2021).

كما أن هذه الدراسة ستساهم في تحديد نقاط الضعف والثغرات الأمنية التي يمكن استغلالها من قبل الجهات الخبيثة لشن هجمات إلكترونية على تلك المؤسسات الحيوية. كما أن الدراسة ستقترح العديد من التوصيات والحلول العملية من شأنها المساهمة في تعزيز مستوى أمن وحماية نظم المعلومات المحاسبية في البنوك وشركات التأمين الليبية، ووضع إطار علمي وعملي يمكن للمسؤولين وصانعي القرار الاستناد إليه في وضع السياسات واتخاذ الإجراءات اللازمة لمواجهة مخاطر التهديدات السيبرانية (كامل، 2014).

وتسعي هذه الدراسة إلي إثراء المعرفة حول تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية. ومن المتوقع أن تكون نتائج الدراسة وتوصياتها دافعاً للمؤسسات المصرفية في تحسين سياسات وإجراءات الأمان، وتعزيز قدرتها على التصدي للتهديدات السيبرانية لنُظم المعلومات وحماية معلوماتها المحاسبية، كما ستسهم الدراسة في توجيه البحوث المستقبلية والجهود العملية المتعلقة بأمن المعلومات والأمن السيبراني في القطاع المصرفي.

سيتم اختيار مجموعة من الدراسات السابقة التي بحثت وتعمقت في تقييم تأثير التهديدات السيبرانية على نُظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي بشكل عام وفي ليبيا بشكل خاص. ستشمل العينة مجموعة متنوعة من الدراسات لباحثين من ذوي الخبرة المهنية في هذه الأقسام، وسيتم قراءة وتحليل هذه الدراسات للخروج بمجموعة من النتائج والتوصيات.

2- مشكلة الدراسة:

تتبلور مشكلة الدراسة حول التحديات والصعوبات التي تواجه أمن وسلامة نُظم المعلومات المحاسبية في المصارف التجارية الليبية في ظل التطور الهائل في التقنيات الرقمية وانتشار التهديدات السيبرانية، حيث تتعرض البيانات والمعلومات المالية والمحاسبية لمخاطر عديدة نتيجة عدم كفاية إجراءات الأمن السيبراني المتبعة، مما يؤدي إلى تعرض المؤسسات المالية والمصرفية لخسائر فادحة. وتمتد المشكلة أيضاً إلى انتشار ظاهرة اختراق بيانات البنوك التجارية وسرقتها، وكذلك تعرض الأنظمة المعلوماتية للابتزاز الإلكتروني، كما ستتناول هذه الدراسة مشكلة ضعف الوعي بأهمية الأمن السيبراني لدى العاملين في المجال المحاسبي والمالي، وعدم وجود سياسات واضحة ومحددة لأمن المعلومات داخل هذه المؤسسات.

3- أهداف الدراسة:

1) تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية.
2) دراسة وصفية للتهديدات السيبرانية التي تواجهها المؤسسات المالية في ليبيا وتأثيرها على نظم المعلومات المحاسبية.
3) تحليل الدراسات السابقة التي تناولت تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي وليبيا، وذلك لاستخلاص النتائج والتوصيات المهمة.

4) توفير أدلة ومعلومات محدثة ومفصلة حول التهديدات السيبرانية المحتملة وتأثيرها على نظم المعلومات المحاسبية في المؤسسات المالية الليبية.

4- أهمية الدراسة:

1) تعزيز الوعي حول أهمية تأمين نظم المعلومات المحاسبية في المؤسسات المالية وحمايتها من التهديدات السيبرانية.
2) توفير معلومات قيمة للمؤسسات المالية الليبية لمساعدتها في تحديد التحديات والمخاطر السيبرانية التي تواجهها واتخاذ الإجراءات اللازمة للحماية.
3) توفير قاعدة معرفية للباحثين والمهتمين بمجال تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي وليبيا.
4) تقديم توصيات فعالة وملموسة تساهم في تعزيز أمان وسلامة نظم المعلومات المحاسبية في المؤسسات المالية الليبية ومنع الاختراقات السيبرانية والتلاعب بالبيانات المالية.

5- محتويات الدراسة:

تحتوي هذه الدراسة على عدد من الأبواب التي يسعي الباحثون من خلالها إلى تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية:

1) ملخص الدراسة باللغتين العربية والإنجليزية.
2) المقدمة.
3) مشكلة الدراسة.
4) أهداف الدراسة.
5) أهمية الدراسة. محتويات الدراسة.
6) الخاتمة. النتائج.
7) التوصيات.
8) المصادر و المراجع.

6- منهجية البحث:

6.1 منهج البحث

تم استخدام المنهج الوصفي لاستعراض الدراسات السابقة من أجل تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية، حيث يتمحور المنهج حول استقراء الدراسات السابقة ومقارنتها مع البحث الحالي لتحديد نقاط التشابه والاختلاف. ويتبع منهج البحث الخطوت التالية:

1- **استعراض الأدبيات:** سيتم إجراء استعراض شامل للأدبيات المتاحة حول تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي وليبيا، وستشمل هذه الأدبيات الدراسات السابقة والأبحاث المنشورة في المجلات العلمية والتقارير المهنية ذات الصلة.
2- **اختيار الدراسات السابقة:** سيتم اختيار مجموعة من الدراسات المتنوعة وذات الصلة التى تعمقت في تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي وليبيا، وسيتم دراسة هذه الدراسات بعناية وفهم نتائجها وتوصياتها.
3- **تحليل الدراسات السابقة:** سيتم تحليل الدراسات المختارة واستقراء النتائج والتوصيات المتعلقة بتأثير التهديدات السيبرانية على نظم المعلومات المحاسبية، وسيتم تحديد نقاط التشابه والاختلاف بين الدراسات السابقة والبحث الحالي وتوضيحها بشكل منهجي.
4- **تحليل البحث الحالي:** سيتم تحليل البحث الحالي وفهم نتائجه وتوصياته بشأن تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية، وسيتم تحديد نقاط التشابه والاختلاف بين البحث الحالي والدراسات السابقة المحددة.
5- **مقارنة النتائج والتوصيات:** سيتم مقارنة نتائج الدراسات السابقة والبحث الحالي لتحديد نقاط التشابه والاختلاف فيما يتعلق بتأثير التهديدات السيبرانية

على نظم المعلومات المحاسبية، ستُوضح المقارنة بشكل مفصل ومنهجي لتحديد النتائج المشتركة والاختلافات الملحوظة.

6- **استنتاج النتائج:** سيتم استنتاج النتائج المستنتجة من تحليل الدراسات السابقة والبحث الحالي، وسيتم تلخيص نقاط التشابه والاختلاف الرئيسية وتوضيح مدى أهميتها وتأثيرها على نظم المعلومات المحاسبية في المؤسسات المالية الليبية.

7- **التوصيات:** سيتم تقديم التوصيات الملائمة استنادًا إلى نتائج المقارنة واستنتاجات الدراسة، وستساهم التوصيات في تعزيز أمان وسلامة نظم المعلومات المحاسبية في المؤسسات المالية الليبية وتوجيه الاهتمام للمسائل الهامة التي تم التوصل إليها من خلال الدراسة.

6.2 مجتمع البحث

سيتم استهداف مجتمع البحث وهو إجمالي الدراسات السابقة في مجال تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية، من إجراء استعراض شامل للأدبيات المتاحة حول تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي وليبيا، وستشمل هذه الأدبيات الدراسات السابقة والأبحاث المنشورة في المجلات العلمية والتقارير المهنية ذات الصلة.

ويعقب ذلك تحديد عينة الدراسة وهي عشرة دراسات سابقة تعمقت في فهم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في ليبيا والوطن العربي.

6.3 أداة البحث

أداة البحث المناسبة لاستخدام المنهج الوصفي هي الدراسة الاستقرائية. ستتطلب الدراسة الاستقرائية تجميع وتحليل المعلومات المتاحة من الدراسات السابقة

والأبحاث والتقارير ذات الصلة لتلخيص النتائج وتحديد نقاط التشابه والاختلاف بين الدراسات المختلفة.

7- تحليل بيانات ونتائج البحث

سيتم استعراض الدراسات السابقة، مع توضيح الهدف من كل دراسة، والمنهجية المستخدمة، والنتائج التي توصلت إليها كل دراسة، بالإضافة إلي التوصيات المقترحة:

هدفت الدراسة التي قام بها (عبد المجيد واخرون، 2023) إلى التعرف على واقع تطبيق نُظم المعلومات المحاسبية وأثره على جودة المعلومات المحاسبية في أقسام المحاسبة وأقسام المعاملات الإلكترونية. وقامت الدراسة بتبني المنهج الوصفي حيث تم تصميم استبانة وتوزيعها على موظفي مكاتب الشؤون المالية، ومكاتب المراجعة الداخلية ومكاتب المراقب المالي في جامعة سرت، وقد تم تطبيق برنامج SPSS لتحليل استبانة من 63 فرداً، وقد تم تحليل البيانات واختبار فرضيات الدراسة عن طريق مجموعة من الاختبارات الإحصائية وعلى رأسها الوسط الحسابي، واختبارات الانحراف المعياري، وتم أيضاً تطبيق اختبار (T)، بالإضافة إلى الانحدار الخطي البسيط. وتوصلت الدراسة إلى وجود أثر إيجابي لاستخدام نُظم المعلومات المحاسبية في أقسام المعاملات الالكترونية واقسام المحاسبة على جودة المعلومات المحاسبية التي يتم الافصاح عنها. كما توصلت الدراسة إلي تطبيق مبادئ امن المعلومات والأمن السيبراني تُسهم بشكل كبير على رفع جودة نُظم المعلومات المحاسبية. وفي الختام، أوصت الدراسة بالأهمية البالغة لتقييم النظام المحاسبي وتأمين نُظم المعلومات المحاسبية والعمل على تطويرها وتحديثها بشكل مستمر.

سلطت دراسة (سلامة، 2022) الضوء على أهم الوسائل لحماية الأمن السيبراني، كما تهدف إلى المساعدة على مكافحة الهجمات الإلكترونية في أقسام المحاسبة وأقسام المعاملات الإلكترونية، ومنع انتهاك البيانات وسرقتها. توصلت الدراسة إلي أن الأمن السيبراني هو وسيلة مهمة لتعزيز أمن المعلومات بأبعادها

المختلفة كالمعلومات المحاسبية، كما توصلت الدراسة إلي الأمن السيبراني ضروري لحماية أقسام المحاسبة وأقسام المعاملات الإلكترونية في المنشآت الحيوية للدولة من أوجه الاستخدام غير القانوني لتكنولوجيا المعلومات.

وأوصت الدراسة بضرورة تبني وسائل تعزيز امن المعلومات والأمن السيبراني فيما يتعلق بأمن المعلومات المحاسبية وغيرها من المعلومات الحيوية، كما أوصت الدراسة بتنمية الوعي المجتمعي حول خطورة الجرائم السيبرانية والتوعية بطرق الوقاية منها عن طريق تفعيل لأمن السيبراني، والتي من أهمها: مواجهة كافة أنواع الجرائم السيبرانية بشكل حاسم، ومعاقبة مرتكبي الجرائم السيبرانية.

سلطت دراسة (فتوح، 2021) الضوء على أنظمة الأمن السيبراني في المنطقة العربية، وقامت الدراسة باستعراض الجهود المبذولة لتوعية المصارف والمؤسسات المالية من أجل إتباع المعايير العالمية لأمن المعلومات في أقسام المحاسبة وأقسام المعاملات الإلكترونية في المصارف التجارية، وأوضحت الدراسة أن الأمن السيبراني ضرورياً لضمان أمن المعلومات المحاسبية، من أجل إدارة أفضل وزيادة إنتاجية هذه الأقسام، وتوصلت الدراسة إلى أن استخدام الأنظمة الرقمية يولد مخاطر، في أقسام المحاسبة وأقسام المعاملات الإلكترونية في المصارف التجارية. كما توصلت الدراسة إلي أت تبادل الخبرات فيما يتعلق بأمن المعلومات وأمن النُظم المحاسبية بين المسؤولين والخبراء في هذا المجال على المستوي العربي والعالمي يؤدي إلى رفع كفاءة المصارف التجارية ومواكبتها للتطورات المتلاحقة على المستوى العالمي.وفي الختام، أوصت الدراسة بتعزيز الأمن السيبراني لنُظم المعلومات المحاسبية وحماية البنى التحتية للمعلومات، ومواجه الحوادث المتعلقة بالأمن السيبراني، كما دعت الدراسة المصارف والمؤسسات المالية العربية إلى تفعيل الأطر القانونية المتعلقة بأقسام المحاسبة وأقسام المعاملات الإلكترونية من أجل ضمان التطبيق الأمثل لمبادئ حوكمة امن المعلومات وتفعيل الأمن السيبراني.

هدفت دراسة (عبد المهدي، 2020) إلى تعقب أثر تطبيق سياسات الأمن السيبراني على جودة نُظم المعلومات المحاسبية في أنشطة البنوك التجارية في

الأردن، تم توزيع الاستبانة على عينة من موظفي البنوك التجارية في الأردن، وتم استخدام برنامج SPSS لتحليل المعلومات، وتوصلت الدراسة إلى وجود علاقة بين إدارة المخاطر السيبرانية وتطبيق مبادئ أمن المعلومات على جودة نُظم المعلومات المحاسبية. كما توصلت الدراسة إلي أن الحفاظ علي خصوصية بيانات العملاء لها تأثير ملموس على جودة نُظم المعلومات المحاسبية.

وأوصت الدراسة بزيادة الاهتمام بمبادئ حوكمة أمن المعلومات لتعزيز جودة المعلومات المحاسبية في الأقسام المحاسبية واقسام التعاملات الالكترونية، وضرورة ان تهتم البنوك بالإفصاح السنوي عن تقارير الأمن السيبراني.

هدفت دراسة (احمد، 2020) إلى التعمق بدراسة التأثير الكبير لحوكمة تكنولوجيا المعلومات في تعزيز أمن نُظم المعلومات المحاسبية في بعض مصارف مدينة دمشق بسوريا، اعتمدت الدراسة على المنهج الوصفي، وضم مجتمع الدراسة 14 مصرفاً خاصاً في سوريا، وقد تم توزيع استبانات على العاملين في القسم المالي في هذه المصارف وبلغ عددهم 100 استبانة، وتوصلت الدراسة إلي وجود تأثير ملموس لأبعاد حوكمة تكنولوجيا المعلومات في أقسام المحاسبة وأقسام المعاملات الإلكترونية على تعزيز أمن المعلومات المحاسبية. كما توصلت الدراسة إلي تعزيز امن نُظم المعلومات المحاسبية يتوقف بشكل أساسي على اعتمام أساليب وقائية لتطبيق مبادئ أمن المعلومات. وقد أوصت الدراسة بضرورة أن تطبق كافة المصارف نموذج فعال لقياس جودة حوكمة تكنولوجيا المعلومات ومساعدة المصارف لتعزيز أمن معلوماتها المحاسبية في أقسام المحاسبة وأقسام المعاملات الإلكترونية.

هدفت دراسة (علي ومفتاح، 2017) إلي التعرف على التحديات في أقسام المحاسبة وأقسام المعاملات الإلكترونية المتعلقة باستخدام نُظم المعلومات المحاسبية في المصارف العاملة في بلدية مصراتة، كما سعت الدراسة إلى التعرف أسباب تلك المخاطر والطرق الواجب اتباعها للحد منها. اطلع الباحثان على الدراسات السابقة في هذا الموضوع، وقام الباحثان بإعداد استبانة يتكون من عينة من موظفي المصارف

ببلدية مصراتة، حيث بلغت العينة (39) فرداً؛ وتوصلت الدراسة إلى أخطار استخدام نُظم المعلومات المحاسبية الإلكترونية في أقسام المحاسبة وأقسام المعاملات الإلكترونية ترجع إلى أسباب متعلقة بموظفي المصرف مثل قلة الوعي وقلة والتدريب. كما توصلت الدراسة إلي أن أخطار استخدام نُظم المعلومات المحاسبية الإلكترونية في أقسام المحاسبة وأقسام المعاملات الإلكترونية تتعلق بأسباب متعلقة بإدارة المصارف؛ مثل عدم وجود سياسات لإدارة تلك المخاطر، وغياب الأدوات الرقابية. وأوصت الدراسة بضرورة أن تقدم الإدارة العليا للمصارف الدعم الكامل لأنظمة أمن المعلومات والأمن السيبراني، كما أوصت الدراسة بأهمية أن تعمل المصارف على إنشاء أقسام خاصة بادراه أخطار تكنولوجيا المعلومات في المصارف، كما وجهت الدراسة المصارف التجارية إلى ضرورة العمل على حماية أمن نظم المعلومات المحاسبية وضرورة قيامهم بتطبيق مبادئ حوكمة أمن المعلومات وتطبيق معايير جودة الأمن السيبراني، وكذلك تطوير وتنمية قدرات العاملين في تلك المصارف في مجالات أمن المعلومات وحمايته.

قامت دراسة (كامل، 2014) بالتعرف على إجراءات أمن المعلومات اللازمة للتعامل مع البيانات المالية في أقسام المحاسبة وأقسام المعاملات الإلكترونية، كما تطرق الدراسة إلى الإجراءات اللازمة لتقليل مخاطر التعامل مع البيانات المالية. أظهرت النتائج أن فهم واستخدام نُظم المعلومات المحاسبية للتعامل مع البيانات والقوائم المالية يمثل ضرورة هامة في الوقت الحاضر، نظرًا لتعدد استخدامات وسائل تقنيات المعلومات في أقسام المحاسبة وأقسام المعاملات الإلكترونية وبصورة خاصة في المصارف التجارية. كما أوضحت النتائج أن استخدام أدوات وبرامج لضمان أمن المعلومات في عمل نُظم المعلومات المحاسبية أصبح ضروري في ظل تنامي المخاطر الالكترونية التي تتعرض لها المصارف التجارية. وتشمل التوصيات توفير التأهيل العلمي للقائمين على أقسام المحاسبة وأقسام المعاملات الإلكترونية في المصارف التجارية على عمل نُظم المعلومات المحاسبية وتقديم التدريب المستمر لهم.

هدفت دراسة (مبروك ومفتاح، 2011) إلي التعرف على مدى ملاءمة المعلومات المحاسبية التي يوفرها النظام المحاسبي في المصرف التجاري الوطني ومدي تطبيق معايير أمن المعلومات لحماية هذه البيانات المحاسبية. ولغرض التوصل إلى هدف الدراسة والإجابة على أسئلتها، سعت الدراسة إلي التعرف على البيانات والمعلومات التي ينتجها النظام المحاسبي للمصرف التجاري الوطني من خلال طرح مجموعة من الأسئلة والاستفسارات علي أعضاء إدارة المحاسبة، وإدارة المعاملات الالكترونية، وإدارة العمليات المصرفية، ولأغراض الدراسة تم إجراء عدداً من المقابلات مع مدراء هذه الإدارات، وتم التوصل إلي تحديد مستوى جودة أمن المعلومات والأمن السيبراني في أنظمة المعلومات المحاسبية في المصارف التجارية. وقد وجدت الدراسة أن الأمن السيبراني في هذه الأقسام يتمتع بمستوى مرتفع من التنفيذ والامتثال لمعايير أمن المعلومات. كما توصلت الدراسة إلي تحديد نقاط الضعف في نظم المعلومات المحاسبية وتحديد التهديدات السيبرانية المحتملة التي قد تؤثر على أمن المعلومات في أقسام المعاملات الإلكترونية وأقسام المحاسبة، وتوصلت الدراسة أن اتخاذ إجراءات لتعزيز أمن المعلومات والتصدي للتهديدات المحتملة يعزز من قدرة نُظم المعلومات المحاسبية من أداء مهامها بنجاح في أقسام المحاسبة وأقسام المعاملات الإلكترونية بالمصارف التجارية. وتم التوصل إلى أن توفير التدريب والتوعية الأمنية المستمرة للموظفين يساهم في تعزيز الوعي بضرورة تطبيق مبادئ أمن المعلومات ومعايير الأمن السيبراني. واخيراً قدمت الدراسة بعض المقترحات، ومنها أهمية الاهتمام بأمن المعلومات في أقسام المحاسبة وأقسام المعاملات الإلكترونية بالبنوك التجارية. كما اوصت الدراسة بضرورة أن تكون مبادئ الجودة فيما يتعلق بأمن المعلومات في بداية اهتمامات المؤسسات المالية والمصرفية.

هدفت دراسة (قاسم واخرون، 2010) إلى تقييم اهتمام البنوك الأردنية بتطبيق إجراءات أمن البيانات ونُظم المعلومات المحاسبية في جميع الأقسام وعلي رأسها أقسام المحاسبة وأقسام المعاملات الالكترونية، تم تحقيق هذا الهدف من خلال استخدام استبانة مؤلفة من ثلاثين فقرة تم توزيعها على الموظفين في البنوك الذين

يشغلون مناصب إدارية في أقسام المحاسبة وأقسام المعاملات الإلكترونية. وأظهر التحليل الاحصائي النتائج أن نسبة الاهتمام بالأمن المادي للمعلومات المحاسبية ولوسائط التخزين وصلت إلى 87.33%. كما بلغت نسبة الاهتمام بأمن الأفراد 91.73%، ونسبة الاهتمام بأمن النظم والتطبيقات والبرمجيات 90.68%. كما توصلت الدراسة إلى أن نسبة الاهتمام بأمن الأجهزة والمعدات 90.94%، ونسبة الاهتمام بأمن طرق الحفظ السليمة وتبادل المعلومات وتخزينها 92.53%. هذه النسب تشير إلى أن الإجراءات المتبعة لحماية البيانات والمعلومات المحاسبية في البنوك الأردنية كافية وشاملة. وتم اختتام الدراسة بالتوصية على ضرورة استمرار في تطوير وتحديث وسائل حماية نُظم المعلومات المحاسبية في أقسام المحاسبة وأقسام المعاملات الإلكترونية. كما تشدد التوصيات على ضرورة المحافظة على المستوى العالي لتطوير إجراءات نُظم أمن المعلومات المحاسبية والاهتمام بتطبيق معايير الجودة لأمن المعلومات وقواعد الأمن السيبراني.

هدفت دراسة (أحمد، 2008) إلى تحديد تحديات نُظم المعلومات المحاسبية الإلكترونية في المصارف التجارية، وخاصة في أقسام المحاسبة وأقسام المعاملات الإلكترونية. كما سعت الدراسة إلى تحديد الأسباب الرئيسية وراء حدوث تلك المخاطر، بالإضافة إلى استعراض الإجراءات التي تساهم في التصدي لتلك المخاطر. تم إعداد استبانة وتوزيعها علي بعض الموظفين في البنوك التجارية في قطاع غزة، وأظهرت النتائج وجود مخاطر نُظم المعلومات المحاسبية تحدث في بعض المصارف العاملة في قطاع غزة وخاصة في أقسام المحاسبة وأقسام المعاملات الإلكترونية، ولكنها ليست متكررة بشكل كبير. كما وضحت النتائج أن عدد الموظفين في اقسام المحاسبة والمعاملات الالكترونية في المصارف التجارية العاملة في قطاع غزة يعد قليلاً. كما أشارت النتائج أيضًا إلى أن التحديات المتعلقة بنظم المعلومات المحاسبية تنجم عن عدة أسباب، بما في ذلك قلة الخبرة والوعي والتدريب لدى الموظفين في المصارف، بالإضافة إلى سوء السياسات والإجراءات ونقص الرقابة في المصارف. بناءً على نتائج الدراسة، تم التوصية بضرورة تعزيز دعم الإدارة العليا للمصارف

لأمن المعلومات وإنشاء قسم متخصص لهذا الغرض وتوفير كادر متخصص ذو خبرة عالية. كما تم التوصية بوضع إجراءات ملائمة تضمن أن يستمر عمل نُظم المعلومات المحاسبية في حالة الأزمات وتعزيز أمان المعلومات من خلال التشفير والحماية الفعالة. وتشدد التوصيات أيضًا على ضرورة وضع ضوابط أمنية ورقابية للمعلومات المتداولة ووضع التشريعات الازمة لتطبيق الأمن السيبراني، والمحافظة على أمن المعلومات والنظم والشبكات المعلوماتية. كما توصي هذه الدارسة أيضًا بضرورة وجود خطة شاملة لحماية المعلومات بشكل جزري، مما يؤدي إلى تقليل التكاليف المرتبطة بتبني حلول أمن مؤقتة أو جزئية.

التعليق علي الدراسات السابقة:

1 -دراسة عبد المجيد وآخرون (2023):

استهدفت هذه الدراسة تقييم أثر نظم المعلومات المحاسبية على جودة المعلومات في أقسام المحاسبة والمعاملات الإلكترونية بجامعة سرت، وقد خلصت إلى وجود أثر إيجابي لنظم المعلومات على جودة المعلومات المحاسبية، كما أكدت على أهمية تطبيق مبادئ أمن المعلومات والأمن السيبراني، وتتفق هذه الدراسة مع الدراسة الحالية في تسليط الضوء على أمن نظم المعلومات المحاسبية.

2 -دراسة سلامة (2022):

ركزت هذه الدراسة على وسائل تعزيز الأمن السيبراني لحماية أمن المعلومات في الأقسام المحاسبية والمعاملات الإلكترونية. وخلصت إلى أهمية الأمن السيبراني في الحماية من التهديدات، وأوصت بضرورة تبني وسائل تعزيز أمن المعلومات. وهو ما تتفق عليه الدراسة الحالية.

3 -دراسة فتوح (2021):

استعرضت أنظمة الأمن السيبراني في المنطقة العربية، ودعت إلى ضرورة الالتزام بمعايير أمن المعلومات لحماية أنظمة المحاسبة والمعاملات الإلكترونية في المصارف. وتتفق مع الدراسة الحالية في تأكيدها على أهمية الأمن السيبراني.

4 -دراسة عبد المهدي (2020):

بحثت هذه الدراسة في أثر تطبيق سياسات الأمن السيبراني على جودة نظم المعلومات المحاسبية في البنوك الأردنية، وخلصت لوجود علاقة إيجابية بينهما.

5 -دراسة أحمد (2020):

سلطت الضوء على أثر حوكمة تكنولوجيا المعلومات في تعزيز أمن نظم المعلومات المحاسبية في المصارف السورية. وخلصت لوجود تأثير إيجابي، وأوصت بضرورة تقييم فاعلية حوكمة تكنولوجيا المعلومات. وهي نتائج مهمة ذات صلة بالدراسة الحالية.

6 -دراسة علي ومفتاح (2017):

هدفت للتعرف على التحديات المتعلقة بأمن نظم المعلومات المحاسبية في مصارف مصراتة الليبية، وخلصت لوجود تحديات تتعلق بنقص الوعي والسياسات الأمنية. وترتبط ارتباطا وثيقا بموضوع الدراسة الحالية.

7 -دراسة كامل (2014):

تناولت إجراءات أمن المعلومات اللازمة للتعامل الآمن مع البيانات المالية في الأقسام المحاسبية والمعاملات الإلكترونية. وأكدت على ضرورة استخدام أدوات أمن المعلومات لحمايتها من التهديدات الإلكترونية. وهو ما يتسق مع أهداف الدراسة الحالية.

8 -دراسة مبروك ومفتاح (2011):

تناولت مستوى أمن المعلومات المحاسبية في المصرف التجاري الوطني الليبي، وخلصت لارتفاعه. كما حددت نقاط الضعف الأمنية، وأوصت بالتدريب والتوعية، وترتبط ارتباطاً وثيقاً بالدراسة الحالية.

9 -دراسة قاسم وآخرون (2010):

قيّمت مستوى الالتزام بإجراءات أمن المعلومات في البنوك الأردنية، وخلصت إلى ارتفاع نسب الالتزام، وأوصت باستمرار التحديث والتطوير، وهي نتائج ذات أهمية بالنسبة للدراسة الحالية.

10 -دراسة أحمد (2008):

تناولت الدراسة تحديات نُظم المعلومات المحاسبية الإلكترونية في المصارف التجارية، وخاصة في أقسام المحاسبة وأقسام المعاملات الإلكترونية، وأوضحت النتائج أن عدد الموظفين في اقسام المحاسبة والمعاملات الالكترونية في المصارف التجارية عندما يكون قليلاً وغير مؤهلاً ينعكس بشكل سلبي علي كفاءة نُظم المعلومات المحاسبية.

التشابه بين الدراسات السابقة والدراسة الحالية:

تشابه الدراسات السابقة والدراسة الحالية يتمثل في التركيز على تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية. كلا الدراسات تسلط الضوء على أهمية الأمن السيبراني وحماية البيانات المحاسبية، بالإضافة إلى تأثير استخدام نظم المعلومات المحاسبية على جودة المعلومات المحاسبية في أقسام المحاسبة والمعاملات الإلكترونية. كما يتم التطرق في الدراسات السابقة والدراسة الحالية إلى تبني مبادئ أمن المعلومات والسيبراني، وأهمية توعية المجتمع وتطبيق الإجراءات القانونية لمكافحة الجرائم السيبرانية. بالإضافة إلى ذلك،

توصي الدراسات السابقة والدراسة الحالية بتعزيز الأمن السيبراني لنظم المعلومات المحاسبية وتحسين البنية التحتية للمعلومات في المؤسسات المالية.

الإختلاف بين الدراسات السابقة والدراسة الحالية:

الدراسة الحالية تختلف عن الدراسات السابقة في عدة نقاط:

موضوع الدراسة:

في الدراسة الحالية، يتم تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية. هذا يركز على التحديات الأمنية المحتملة التي تواجهها المؤسسات المالية نتيجة الهجمات السيبرانية. بينما في الدراسات السابقة، تركزت على جوانب مختلفة مثل جودة المعلومات المحاسبية وتأمين نظم المعلومات المحاسبية بشكل عام.

المؤسسات المستهدفة:

الدراسة الحالية تركز على المؤسسات المالية، وهي تشمل البنوك والشركات المالية الأخرى. تهدف الدراسة إلى فهم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في هذه المؤسسات وتحديد النقاط الضعيفة وتوصيات لتعزيز الأمان والحماية. في حين أن الدراسات السابقة قد تكون تناولت مؤسسات مختلفة مثل الجامعات أو المؤسسات العامة.

باختصار، الدراسة الحالية تركز على تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية، بينما الدراسات السابقة قد تناولت مواضيع مختلفة واستهدفت مؤسسات مختلفة.

8- الخاتمة:

لقد هدف هذا البحث إلى تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية، وذلك نظراً لأهمية تلك الأنظمة وحساسية البيانات التي تحتويها. وبناءً علي استقراء الدراسات السابقة والإطلاع علي نتائجها وتوصياتها، وفهم نقاط التشابه والإختلاف بين الدراسات السابقة والدراسة الحالية، توصل البحث إلي أن المؤسسات المالية الليبية تواجه تهديدات سيبرانية متزايدة ومتنوعة، وتشمل هذه التهديدات الاختراقات الهجمات الإلكترونية، سرقة البيانات المالية، التجسس الصناعي، وتعطيل الخدمات المصرفية عبر الإنترنت. هذه التهديدات تسبب تأثيرًا سلبيًا على نظم المعلومات المحاسبية وتمثل خطرًا على السرية والموثوقية والتوافرية. وتوصل البحث إلي أن هناك عدة نقاط ضعف في نظم المعلومات المحاسبية في المؤسسات المالية الليبية، وتشمل هذه النقاط ضعف في رصد وكشف هجمات السيبرانية، نقص في التدريب والوعي الأمني للموظفين، ضعف في إجراءات التحقق والتحكم الداخلي، وعدم وجود استراتيجيات شاملة للأمن السيبراني.وفي ضوء ذلك، أوصت الدراسة بضرورة اتخاذ عدد من الإجراءات والتدابير من قبل إدارات المؤسسات المالية، والتي من شأنها رفع مستوى الوعي وتعزيز قدرات المؤسسة علي التصدي والحد من الهجمات الإلكترونية. ويؤمل أن تشكل نتائج وتوصيات هذا البحث نقطة انطلاق نحو بيئة عمل أكثر أمناً وحماية للأنظمة والبيانات المالية في القطاعات المصرفية في الوطن العربي.

8.1 نتائج البحث

من خلال استعراض الدراسات السابقة ومعرفة أهدافها والنتائج التي توصلت إليه ومقارنة نقاط التشابه والاختلاف بينهم وبين الدراسة الحالية، وتوصلت الدراسة إلي مجموعة من النتائج:

- توصل البحث إلي أن المؤسسات المالية الليبية تواجه تهديدات سيبرانية متزايدة ومتنوعة، وتشمل هذه التهديدات الاختراقات الهجمات الإلكترونية، سرقة البيانات المالية، التجسس الصناعي، وتعطيل الخدمات المصرفية عبر الإنترنت. هذه التهديدات تسبب تأثيرًا سلبيًا على نظم المعلومات المحاسبية وتمثل خطرًا على السرية والموثوقية والتوافرية.
- توصل البحث إلي أن هناك عدة نقاط ضعف في نظم المعلومات المحاسبية في المؤسسات المالية الليبية، وتشمل هذه النقاط ضعف في رصد وكشف هجمات السيبرانية، نقص في التدريب والوعي الأمني للموظفين، ضعف في إجراءات التحقق والتحكم الداخلي، وعدم وجود استراتيجيات شاملة للأمن السيبراني.
- توصل البحث إلي التهديدات السيبرانية تسبب تأثيرًا اقتصاديًا كبيرًا على المؤسسات المالية الليبية، وتشمل هذه التأثيرات تكاليف استعادة البيانات وإصلاح الأضرار، فقدان الثقة لدى العملاء والمستثمرين، توقف الخدمات المصرفية، وتعرض الشركات للمسائل القانونية والتعويضات المالية.
- توصل البحث إلي أن المؤسسات المالية تواجه تهديدات سيبرانية متزايدة ومتنوعة وتشير إلى وجود نقاط ضعف في نظم المعلومات المحاسبية، وهذه التهديدات تسبب تأثيرًا سلبيًا على السرية والموثوقية والتوافرية للمعلومات المحاسبية. يتضمن التأثير الاقتصادي للتهديدات السيبرانية تكاليف استعادة البيانات وإصلاح الأضرار، فقدان الثقة لدى العملاء والمستثمرين، وتوقف الخدمات المصرفية.

هذه النتائج تلقى الضوء على الحاجة إلى تعزيز أمن المعلومات المحاسبية في المؤسسات المالية الليبية وتطوير استراتيجيات فعالة للتصدي للتهديدات السيبرانية.

8.2 التوصيات

بناءً على تحليل الدراسات السابقة والبحث الحالي حول تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية في الوطن العربي وليبيا، يمكن توجيه التوصيات التالية:

تعزيز الوعي والتدريب: ينبغي على المؤسسات المالية تعزيز وعي الموظفين والعاملين في المجال المحاسبي بشأن التهديدات السيبرانية وأفضل الممارسات الأمنية، كما ينبغي توفير تدريب منتظم حول مخاطر الأمن السيبراني وكيفية التعامل معها والوقاية منها.

تحديث السياسات والإجراءات: يجب على المؤسسات المالية تقييم وتحديث سياسات الأمان والإجراءات المتعلقة بنظم المعلومات المحاسبية لتوفير حماية فعالة ضد التهديدات السيبرانية، كما ينبغي أيضًا تنفيذ نظم رصد وكشف متقدمة للكشف المبكر عن الهجمات السيبرانية والتعامل معها بشكل سريع وفعال.

تعزيز التعاون والشراكات: ينبغي على المؤسسات المالية تعزيز التعاون مع الهيئات الحكومية ذات الصلة والمؤسسات الأمنية والخبراء في مجال الأمن السيبراني، كما يمكن تبادل المعلومات والخبرات والتعاون في تطوير استراتيجيات الأمن السيبراني للحد من التهديدات وتعزيز الاستجابة الفعالة في حالة وقوع هجمات.

تحسين التكنولوجيا والبنية التحتية: ينبغي على المؤسسات المالية الاستثمار في تحسين التكنولوجيا والبنية التحتية لضمان أنظمة المعلومات المحاسبية تكون مقاومة للهجمات السيبرانية، كما يجب تحديث البرامج والأجهزة وتطبيق أحدث التقنيات الأمنية للحد من ثغرات الأمان وتعزيز الحماية.

إجراء تقييم دوري: ينبغي على المؤسسات المالية إجراء تقييم دوري لتقييم فعالية استراتيجيات الأمن السيبراني واتخاذ التحسينات اللازمة، كما ينبغي تحليل الهجمات السابقة والتعلم منها من أجل التكيف والتعزيز المستمر.

توفير الدعم المالي: يجب أن تقوم الحكومات والمؤسسات المالية بتوفير الدعم المالي والموارد اللازمة للمؤسسات الصغيرة والالمتوسطة في المجال المالي لتعزيز قدراتها الأمنية السيبرانية، كما يمكن تقديم المساعدة في تحسين البنية التحتية التقنية وتوفير أحدث التقنيات الأمنية المطلوبة.

التواصل مع المجتمع البحثي: ينبغي على المؤسسات المالية التواصل والتعاون مع المجتمع البحثي والأكاديمي للاستفادة من الأبحاث والدراسات المتاحة وتبادل المعرفة والتجارب، كما يمكن تشجيع تنظيم ورش عمل وندوات لمناقشة التحديات الأمنية والابتكار في مجال الأمن السيبراني.

التحفيز والتوعية للعملاء: يجب على المؤسسات المالية تعزيز التوعية للعملاء بشأن مخاطر الأمن السيبراني وتبعاتها المحتملة، كما يمكن تقديم نصائح وإرشادات للعملاء بشأن كيفية حماية بياناتهم الشخصية والحسابات المالية وتشديد القوانين واللوائح المتعلقة بحماية البيانات المالية.

ويُكمن أن تساعد هذه التوصيات في تعزيز أمان نظم المعلومات المحاسبية في المؤسسات المالية وتقليل التهديدات السيبرانية، ومن المهم مراعاة أن كل مؤسسة قد تحتاج إلى استراتيجيات مختلفة بناءً على احتياجاتها وتحدياتها الفردية.

9- المصادر والمراجع:

- عبد المجيد واخرون: نظم المعلومات المحاسبية وأثره على جودة البيانات والمعلومات المحاسبية: دراسة حالة "جامعة سرت"، مجلة الدراسات الاقتصادية، جامعة سرت - كلية الاقتصاد، ا، 2023م، مج6، ع1، ص 18-25.
- عادل موسي: وسائل حماية الأمن السيبراني، مجلة كلية الشريعة والقانون، جامعة أسيوط، مصر، 2022، مج 3، ص 34، ص 2230-2236.
- حسن فتوح: الأمن السيبراني في المنطقة العربية: توعية المصارف والمؤسسات المالية لإتباع المعايير العالمية، مجلة اتحاد المصارف العربية، مجلة اتحاد المصارف العربية، لبنان، 2021م، ع 490، ص 2-5.
- حنين عبد المهدي: أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية، رسالة ماجستير، كلية الاقتصاد والعلوم الادارية، جامعة آل البيت، الأردن، 2020م، ص 19-26.
- منهل أحمد: أثر حوكمة تكنولوجيا المعلومات في تعزيز أمن المعلومات المحاسبية: دراسة ميدانية، مجلة جامعة البعث سلسلة العلوم الاقتصادية، جامعة البعث، سوريا، 2020م، مج42، ع 30، ص 11-18.
- إبراهيم علي، ومحمد مفتاح: مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية: دراسة ميدانية على المصارف التجارية في بلدية مصراتة، مجلة دراسات الاقتصاد والأعمال، جامعة مصراتة - كلية الاقتصاد والعلوم السياسية، ليبيا، مج 5، عدد خاص، 2017م، ص 80-87.
- إمام كامل: البيانات المالية والمتطلبات اللازمة لتقليل المخاطر المرتبطة بها، مجلة الاقتصاد والمحاسبة، مصر، 2014م، ع 654، ص 14-17.
- أميرة مبروك، وفاخر مفتاح: مدى ملاءمة المعلومات المحاسبية التي توفرها النظم المحاسبية في المصارف التجارية الليبية، رسالة ماجستير، كلية الاقتصاد، جامعة بنغازي، ليبيا، 2011م، ص 5-15.
- قاسم وآخرون: أمن البيانات ونظم المعلومات المحاسبية في بيئة تكنولوجيا المعلومات في البنوك الأردنية: دراسة ميدانية، المجلة العربية للعلوم الاقتصادية والإدارية، لبنان، 2010م، ع 5، ص 90-100.
- عصام وآخرون: مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة، مجلة الجامعة الإسلامية للبحوث الإنسانية، الجامعة الإسلامية بفلسطين - شئون البحث العلمي والدراسات العليا، 2008م، مج 16، ع 2، ص 895-912.