



دور تدابير الامن السيبراني في حماية نظم المعلومات المحاسبية دراسة استطلاعية في عينة من المصارف

م.م. أياد سالم خضر^٢

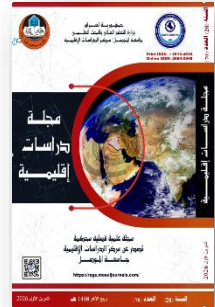
harth_rashd2007@uomosul.edu.iq

ayad.salem@uomosul.edu.iq

د. حارث راشد حمدون^١

^١ كلية الإدارة والاقتصاد/ جامعة الموصل/ العراق.

^٢ كلية الإدارة والاقتصاد/ جامعة الموصل/ العراق.



المخلص

فكرة البحث: يتناول البحث أثر تدابير الأمن السيبراني على حماية نظم المعلومات المحاسبية من منظور عدد من المحاسبين العاملين في مصرف عراقية مختارة بمدينة الموصل. ويستعرض الجانب النظري أهم المفاهيم المتعلقة بالأمن السيبراني ودوره في حماية نظم المعلومات المحاسبية.

الهدف: يهدف البحث إلى تقييم تأثير تدابير الأمن السيبراني على حماية نظم المعلومات المحاسبية في المصارف العراقية.

المنهجية: تم تصميم استمارة استبيان وتوزيعها على عينة البحث لغرض جمع البيانات، حيث بلغ عدد الاستمارات الصالحة للتحليل (١٠٧) استمارة. وقد قاس الاستبيان أربعة أبعاد تمثل متغير تدابير الأمن السيبراني وهي: التدابير القانونية، التدابير التكنولوجية، التدابير التنظيمية، والتدابير المتعلقة بالموظفين ومزودي الخدمات، بالإضافة إلى بُعد واحد يمثل متغير حماية نظم المعلومات المحاسبية.

النتائج: أشارت النتائج إلى وجود تأثير معنوي إحصائي لتدابير الأمن السيبراني على حماية نظم المعلومات المحاسبية.

الاستنتاج: خلص البحث إلى أن تحسين تدابير الأمن السيبراني - ولا سيما التدابير التكنولوجية وتلك المتعلقة بالموظفين ومزودي الخدمات - يسهم بشكل كبير في تعزيز حماية نظم المعلومات المحاسبية في المصارف.

معلومات الأرشفة

الاستلام: ٢٠٢٦/٧/٣١

المراجعة: ٢٠٢٦/٩/٧

القبول: ٢٠٢٦/٩/٢٠

النشر الإلكتروني: ٢٠٢٦/١/١٠

المراسلة

حارث راشد حمدون

الكلمات المفتاحية

الأمن السيبراني؛ تدابير؛ حماية؛ نظم المعلومات.

الاقتباس

حمدون، حارث. ر.، وخضر، أياد، س. (٢٠٢٦). دور تدابير الامن السيبراني في حماية نظم المعلومات المحاسبية دراسة استطلاعية في عينة من المصارف. مجلة دراسات إقليمية. ٢٠ (٧٠). ٤٩٧-٥٢٦.

<https://doi.org/10.33899/rsj.v20i69.62907>



© Authors, 2026, Regional Studies Center, University of Mosul. This is an open access article under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>)



The Role of Cybersecurity Measures in Protecting Accounting Information Systems: An Exploratory Study of a Sample of Banks

Harith R. Hamdoon¹

Eyad S. Khudher²

¹ Lect./ College of Administration and Economics/ University of Mosul/ Iraq.

harth_rashd2007@uomosul.edu.iq

² Assist. Lect./ College of Administration and Economics/ University of Mosul/ Iraq.

ayad.salem@uomosul.edu.iq

Article Information

Received: 31/7/2026

Revised: 7/9/2026

Accepted: 20/9/2026

Published: 1/10/2026

Corresponding

Harith R. Hamdoon

Keywords

Cyber security; measures; protection; information systems.

Citation

Hamdoon, H. R., & Khudher, O. H. S. (2027). The Role of Cybersecurity Measures in Protecting Accounting Information Systems: An Exploratory Study of a Sample of Banks. *Regional Studies Journal*. 20(70).497-526.

<https://doi.org/10.33899/r.sj.v20i69.62907>

Abstract

Research Idea: The research examines the impact of cybersecurity measures on the protection of accounting information systems from the perspective of accountants working in selected Iraqi banks in Mosul. The theoretical part reviews key concepts related to cybersecurity and its role in protecting accounting information systems.

Objective: The research aims to assess the effect of cybersecurity measures on the protection of accounting information systems in Iraqi banks.

Methodology: A questionnaire was designed and distributed to the research sample for data collection, yielding 107 valid questionnaires for analysis. The questionnaire measured four dimensions of cybersecurity measures: legal, technological, organizational, and employee and service-provider measures, as well as one dimension measuring the protection of accounting information systems.

Results: The results indicate a statistically significant effect of cybersecurity measures on the protection of accounting information systems.

Conclusion: The research concludes that improving cybersecurity measures, particularly technological measures and those related to employees and service providers, significantly contributes to strengthening the protection of accounting information systems in banks.



© Authors, 2026, Regional Studies Center, University of Mosul. This is an open access article under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>)

لقد أصبحت دراسة الأمن السيبراني واحدة من نتائج التطور التكنولوجي والرقمي الذي نعيش فيه حالياً، حيث يشهد العالم المتقدم في جميع أنحائه تطوراً كبيراً لا يمكننا تجاهله، لذا أصبحت هذه الدراسات التكنولوجية في مجال الحوسبة الرقمية وجهة للكثير من الباحثين المميزين حول العالم، لكن هناك جانب مظلم آخر لذلك التطور الرقمي الذي نلاحظه، يمكن أن يجعل الدول الكبرى والشركات والمؤسسات التجارية والاقتصادية معرضة للاختراق، ولعل هذا أحد أسباب أهمية دراسة الأمن السيبراني، الذي يعمل على حماية البيانات والشبكات والأنظمة الإلكترونية من الهجمات والاختراقات التي قد تؤدي إلى تهديدها واستقرارها. ومن هنا تبرز الحاجة إلى فهم ماهية الأمن السيبراني ودراسته دراسة علمية شاملة من جوانب مختلفة بعمق كمغير جديد في العلاقات الدولية.

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن الحادي والعشرون وما نتج عنه من تأثيرات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني (Cybersecurity) كبعد جديد ضمن أجندة حقل الدراسات الأمنية، وقد حصل الاهتمام من العديد من الباحثين في هذا المجال. وقد ظهر في الأفق عدة جوانب تتعلق بالفضاء السيبراني، الجانب الأول هو الاقتصادي، حيث ينقسم اقتصاد الإنترنت إلى مجالين أساسيين، الأول يتعلق بصناعة تكنولوجيا المعلومات ويشمل تطوير وإنتاج الأجهزة والبرمجيات وخدمات أخرى، بينما الثاني هو مجال الاتصالات (ICT) المتعلق بالتجارة الإلكترونية من خلال فتح سوق حر عبر الإنترنت. أما الجانب الثاني فيتعلق بأمن المعلومات، حيث تخصص العديد من الدول نسبة كبيرة من ميزانيتها لمواجهة الهجمات السيبرانية وتحديث وتطوير أنظمة الأمان لديها. وأما الجانب الثالث (CTIIC) فهو البعد الأمني، وأفضل مثال على ذلك هو مركز تكامل استخبارات التهديد السيبراني في الولايات المتحدة الأمريكية الذي يعمل على التنسيق بين مختلف أجهزة الأمن الأمريكية مثل: مكتب التحقيقات الفيدرالي، وكالة الاستخبارات المركزية، ووكالة الأمن القومي. وكذلك المثال العربي يتمثل في الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (أبو زيد، ٢٠١٩).

هدف البحث: يهدف البحث بصورة رئيسية إلى التعرف على دور تدابير الأمن السيبراني في حماية نظم المعلومات المحاسبية في المصارف محل الدراسة، وبيان مدى فاعلية هذه التدابير في الحد من المخاطر والتهديدات السيبرانية التي قد تؤثر في أمن وموثوقية المعلومات المحاسبية.

أهمية البحث: تتبع أهمية هذا البحث من تزايد اعتماد المصارف على نظم المعلومات المحاسبية الإلكترونية في تنفيذ العمليات المالية والمصرفية، وما يرافق ذلك من تزايد المخاطر والتهديدات السيبرانية التي قد تؤثر في أمن المعلومات المحاسبية وموثوقيتها. ويمكن توضيح أهمية البحث من خلال الجانبين الآتيين:

أولاً: الأهمية العلمية

١. يسهم البحث في إثراء الأدبيات المحاسبية المتعلقة بالأمن السيبراني ونظم المعلومات المحاسبية، ولا سيما في البيئة المصرفية .
٢. يوضح العلاقة بين تدابير الأمن السيبراني ومستوى حماية نظم المعلومات المحاسبية .
٣. يوفر إطاراً مفاهيمياً يمكن أن يستفيد منه الباحثون في إجراء دراسات مستقبلية تتناول أمن المعلومات المحاسبية والمخاطر السيبرانية .

ثانياً: الأهمية العملية

١. يساعد البحث إدارات المصارف في التعرف على مستوى فاعلية تدابير الأمن السيبراني المطبقة لحماية نظم المعلومات المحاسبية .
٢. يساهم في تحديد أبرز المخاطر والتهديدات السيبرانية التي يمكن أن تتعرض لها البيانات والمعلومات المحاسبية .
٣. يساعد في تعزيز سرية البيانات المحاسبية وسلامتها وتوافرها، بما يدعم موثوقية المعلومات المستخدمة في اتخاذ القرارات .
٤. يساهم في الحد من الآثار المحتملة للهجمات السيبرانية، مثل فقدان البيانات أو التلاعب بها أو الوصول غير المصرح به إليها .

مشكلة البحث: على الرغم من المزايا التي توفرها هذه النظم من حيث السرعة والدقة وتوفير المعلومات اللازمة لاتخاذ القرارات، فإن الاعتماد المتزايد عليها أدى في المقابل إلى ظهور العديد من المخاطر والتهديدات السيبرانية، مثل الاختراقات الإلكترونية، والبرمجيات الخبيثة، وسرقة البيانات، والوصول غير المصرح به، والتلاعب بالمعلومات المحاسبية أو إتلافها. وتزداد خطورة هذه التهديدات في البيئة المصرفية لما تتميز به من حساسية البيانات المالية والمعلومات المصرفية، الأمر الذي يتطلب وجود تدابير فعالة للأمن السيبراني تساهم في المحافظة على سرية المعلومات المحاسبية وسلامتها وتوافرها، والحد من احتمالية تعرضها للسرقة أو التعديل أو فقدان. كما أن ضعف تلك التدابير قد ينعكس سلباً على موثوقية نظم المعلومات المحاسبية وجودة المعلومات التي توفرها للإدارة والأطراف ذات العلاقة. ومن هنا تتمثل مشكلة البحث في التساؤل الرئيس الآتي:

ما دور تدابير الأمن السيبراني في حماية نظم المعلومات المحاسبية في المصارف محل الدراسة؟

ويتفرع عن هذا التساؤل الرئيس مجموعة من التساؤلات، أهمها:

١. ما مستوى تطبيق تدابير الأمن السيبراني في المصارف محل الدراسة؟
 ٢. ما مستوى حماية نظم المعلومات المحاسبية في المصارف محل الدراسة؟
 ٣. هل تسهم تدابير الأمن السيبراني في تعزيز سرية وسلامة وتوافر المعلومات المحاسبية؟
- فرضيات البحث:** بناءً على أهداف ومشكلة البحث تضمن البحث ثلاث فرضيات رئيسية هي:
- الفرضية الأولى: (H1) توجد علاقة ذات دلالة إحصائية بين تدابير الأمن السيبراني وحماية نظم المعلومات المحاسبية في المصارف عينة البحث.
- الفرضية الثانية: (H2) يوجد أثر ذو دلالة إحصائية لكل بعد من أبعاد تدابير الأمن السيبراني على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.
- الفرضية الثالثة: (H3) : يوجد أثر ذو دلالة إحصائية لتدابير الأمن السيبراني إجمالاً على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

المحور الأول: الجانب النظري

١- الأمن السيبراني: (Cybersecurity)

أولاً : مفهوم الامن السيبراني: الأمن السيبراني هو مجموعة من الطرق، والأساليب، والخطوات، والقواعد التي تهدف إلى حماية الأنظمة الحاسوبية، والشبكات، والبرامج، والبيانات من المخاطر الرقمية، والهجمات الإلكترونية، والوصول غير المسموح به، والضرر، أو التعديل غير المسموح به. يشمل الأمن السيبراني حماية سرية البيانات، وسلامتها، وتوفرها (الهيئة الوطنية للأمن السيبراني ٢٠١٨)

عند مراجعة الأدبيات المتعلقة بموضوع الأمن السيبراني، فعرفته الهيئة الأوراق المالية والبورصات (SEC) بأنه "مجموعة من التكنولوجيا والعمليات والممارسات المخصصة لحماية الشبكات والأنظمة وأجهزة الحاسوب والبرامج والبيانات من الهجمات أو الضرر أو الوصول غير المصرح به، (Heroux & Fortin, 2020: 76) ويُعرّف الأمن السيبراني بأنه "النشاط أو العملية أو القدرة على حماية أنظمة المعلومات والاتصالات - وما تحتويه من معلومات - والدفاع عنها ضد الضرر أو الاستخدام غير المصرح به أو التعديل أو الاستغلال. (Gao, et al. , 2020: 3) "

كما يُعرّف بأنه "مجموعة من التكنولوجيا والعمليات والضوابط المخصصة لحماية الأنظمة والشبكات والبيانات من الهجمات السيبرانية، وتقليل مخاطر هذه الهجمات، وحماية المجتمعات والشركات

والأفراد من الاستغلال غير المصرح به للأنظمة والشبكات والتكنولوجيا" (Haapamäki and Sihvonen, 2019: 812).

وللأمن السيبراني أنواع كثيرة تشمل جوانب متنوعة، ومن بين هذه الأنواع أمن الشبكات وأمن التطبيقات وأمن إنترنت الأشياء وأمن المستخدم النهائي وأمن البنية التحتية، ويمكن تقسيم الأمن السيبراني إلى ثلاث فئات رئيسية: أولاً، حماية سرية المعلومات الخاصة، وثانياً، ضمان وصول المستخدمين المصرح لهم إلى المعلومات في الوقت المناسب، وثالثاً، يحمي دقة المعلومات وموثوقيتها وصحتها (Haapamäki and Sihvonen, 2019: 809).

والقول بالأمن السيبراني يشير إلى اتخاذ الخطوات الضرورية لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الأدوات المستخدمة تقنياً وتنظيمياً وإدارياً لمنع الوصول غير المصرح به للمعلومات الإلكترونية ومنع استخدامها بطرق غير قانونية وقانونية، وبالتالي فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات الموجودة بها، وحمايتها بكل خصوصية وسرية من خلال تطبيق الخطوات والإجراءات الضرورية لحماية البيانات.

ثانياً: الأهداف الرئيسية للأمن السيبراني: يرتبط مفهوم الأمن السيبراني بعدة أهداف للأمن السيبراني، يمكن توضيحها كما يلي: (شلوش، ٢٠١٨، ١٤)

١. حماية البيانات : ويعني الحفاظ على سرية وسلامة البيانات، بهدف منع الوصول غير المصرح به والسرقة والتلاعب بالبيانات.
٢. ضمان التوافر : ويعني التأكد من أن الأنظمة الرقمية متاحة للاستخدام عند الحاجة دون انقطاع.
٣. الكشف عن التهديدات : ويتمثل في القدرة على اكتشاف الأنشطة الضارة والهجمات بسرعة وفعالية.
٤. الاستجابة للهجمات : يتعامل هذا الهدف مع الرد السريع على الهجمات السيبرانية للحد من الأضرار واستعادة السيطرة.
٥. الوقاية والتعزيز : الهدف هو تحسين الأمان السيبراني من خلال تحديث وتعزيز أنظمة المعلومات وتنفيذ ممارسات أمان جيدة.
٦. الامتثال والتشريعات : ويعني مطابقة المؤسسات للقوانين واللوائح المتعلقة بالأمن السيبراني.
٧. التعاون والتحالفات : يشير هذا الهدف إلى أهمية التعاون بين الدول والمؤسسات لمواجهة التهديدات السيبرانية.
٨. توعية المستخدمين : يهدف إلى زيادة وعي المستخدمين بمخاطر الأمان السيبراني وتعليمهم كيفية حماية أنفسهم، وعدم تداول كلمات المرور بين الموظفين لتجنب حدوث اختراقات لأنظمة المعلومات المحاسبية (سليمان، ٢٠٢٢)

وهناك من يرى ان اهداف الامن السيبراني : (السحان، ٢٠٢٠، ١٢)

- ١- تعزيز أمان النظم التقنية التشغيلية في جميع الجوانب ومكونات الأجهزة والبرامج، بالإضافة إلى الخدمات المقدمة والبيانات المخزنة.
 - ٢- مواجهة الاعتداءات والحوادث الأمنية المتعلقة بالمعلومات التي تستهدف الأجهزة الحكومية والهيئات في القطاعين العام والخاص.
 - ٣- تقليل عمليات التجسس والتخريب الإلكتروني بالنسبة للحكومة والأفراد.
 - ٤- تلبية الاحتياجات الأساسية للحد من المخاطر والجرائم الإلكترونية التي تواجه المستخدمين.
 - ٥- إنشاء بيئة آمنة وموثوقة للتعاملات في مجتمع المعلومات.
 - ٦- إصلاح الثغرات الموجودة في أنظمة الحواسيب والأجهزة المحمولة بمختلف أنواعها.
 - ٧- اتخاذ كافة الخطوات اللازمة لحماية المستهلكين من المخاطر المحتملة في استخدام الإنترنت.
 - ٨- مكافحة البرمجيات الضارة التي تلحق أضراراً جسيمة بالمستخدمين.
 - ٩- تعزيز البنية التحتية الحساسة ضد الهجمات الإلكترونية.
 - ١٠- معالجة الثغرات الموجودة في أنظمة الأمن المعلوماتي.
 - ١١- تدريب الأشخاص على أساليب وإجراءات جديدة للتصدي لتحديات اختراق أجهزتهم التقنية بهدف الإضرار بمعلوماتهم الشخصية سواء بالتخريب أو السرقة.
- ثالثاً: أهمية الأمن السيبراني: نظراً لأهمية الأمن السيبراني في واقع المجتمعات المعاصرة، فقد وضعته العديد من الدول على قمة اهتماماتها، خاصة مع ظهور دلائل الحروب السيبرانية، حيث تشير بعض الدول الكبرى بشكل واضح إلى انتهاء عصر الحروب التقليدية التي استخدمت فيها الأسلحة الثقيلة، وبداية حقبة جديدة تمثل الحروب السيبرانية، ويكمن أهمية الأمن السيبراني الفعال في الحد من مخاطر الاختراقات الأمنية، إذ يهدف هذا الأمن إلى حماية المجتمع والأفراد والشركات من الاستخدام غير المصرح به للأنظمة والشبكات والتقنيات (Asiri, 2021: 110). ويُعتبر برنامج الأمن السيبراني فعالاً إذا نجح في تقليل مخاطر الهجمات والحوادث السيبرانية وحماية الجميع من سوء الاستخدام أو الاستخدام غير المصرح به للأنظمة والشبكات والتقنيات ذات الصلة (Badawy, 2021: 6). كما يتضمن الأمن السيبراني القدرة على مقاومة التهديدات -سواء كانت متعمدة أو غير متعمدة- والاستجابة لها والتعافي من أثارها، مما يضمن السلامة من المخاطر أو الأضرار الناتجة عن تعطل تقنيات المعلومات والاتصالات أو تلفها أو سوء استخدامها، ويستلزم ذلك حماية الشبكات وأجهزة الحاسوب والبرمجيات والبيانات من الهجمات أو التلف أو الوصول غير المصرح به. ونظراً لأهمية الأمن السيبراني في واقع المجتمعات المعاصرة، فقد وضعته العديد من

الدول على قمة اهتماماتها، خاصة مع ظهور دلائل الحروب السيبرانية، حيث تشير بعض الدول الكبرى بشكل واضح إلى انتهاء عصر الحروب التقليدية التي استخدمت فيها الأسلحة الثقيلة، وبداية حقبة جديدة تمثل الحروب السيبرانية (Al-Zubaidi & Al-Tamimi, 2022: 8). ويمكن القول إن أهمية الأمن السيبراني تكمن في الجوانب التالية (Kaao, 2020: 171):

١. الحفاظ على سرية وخصوصية جميع الوثائق والبيانات الرقمية
٢. ضمان استمرارية عمل الأنظمة الرقمية
٣. توفير الحماية اللازمة للمواطنين وللبنية التحتية المهمة للدولة
٤. حماية المعلومات وسلامتها وانتظامها، من خلال منع تدخل الآخرين فيها
٥. ضمان توفر البيانات وجاهزيتها عند الحاجة إليها
٦. حماية الأجهزة والشبكات بشكل كامل من الاختراقات لتكون درعاً للبيانات والمعلومات
٧. تحديد نقاط الضعف والثغرات في الأنظمة ومعالجتها
٨. استخدام أدوات المصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن الإلكتروني
٩. خلق بيئة عمل آمنة جداً أثناء العمل عبر الإنترنت

رابعاً: عناصر الأمن السيبراني: (<https://www.mah6at.net/>)

حتى يتحقق الهدف من الأمن السيبراني، لابد من توفر مجموعة من العناصر مع بعضها البعض لتكتمل الدور في ذلك، ومن أهم أبعاد وعناصر الأمن السيبراني:

-التقنية: (technology) تلعب التكنولوجيا والتقنية دوراً مهماً في حياة الأفراد والمنظمات، حيث توفر حماية فعالة لهم ضد الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

-الأشخاص: (People) يُطلب من الأشخاص الذين يستخدمون البيانات والأنظمة في أي منشأة استخدام مبادئ حماية البيانات الأساسية مثل تحديد كلمة مرور قوية، وتجنب فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانب القيام بنسخ احتياطية للبيانات.

- الأنشطة والعمليات (Process): يتم استخدام الأشخاص والتقنيات لأداء العديد من العمليات والأنشطة وإدارتها بما يتوافق مع تطبيق أسس الأمن السيبراني ومواجهة هجماته بكل كفاءة.

خامساً: أبعاد الأمن السيبراني: (<https://ab7as.net/>)

أولاً: الأبعاد العسكرية: تبرز أهمية الأمن السيبراني في هذا المجال بسبب خطورة الهجمات السيبرانية والاختراقات التي قد تؤدي إلى الحروب والصراعات المسلحة، واختراقات الأنظمة النووية، وما يمكن أن يؤدي إليه ذلك من تهديدات لأمن الدول والحكومات ويؤدي إلى كوارث.

ثانياً: الأبعاد السياسية: تستند الأبعاد السياسية للأمن السيبراني إلى حماية النظام السياسي للدولة وكيانها، حيث يمكن استخدام التقنيات لنشر معلومات وبيانات قد تؤدي إلى زعزعة استقرار أمن الدول والحكومات، مما يصل بسرعة كبيرة إلى شريحة واسعة من المواطنين بغض النظر عن صحة البيانات والمعلومات التي تُنشر.

ثالثاً: الأبعاد الاقتصادية: يتعلق الأمن السيبراني ارتباطاً وثيقاً بالحفاظ على المصالح الاقتصادية لجميع الدول، فهناك ترابط كبير بين الاقتصاد والمعرفة، حيث تعتمد معظم الدول في تعزيز اقتصادها وازدهارها على إنتاج وتداول المعرفة والمعلومات على جميع المستويات، مما يبرز الدور الهام للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية.

رابعاً: الأبعاد القانونية: ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومن ظهور المجتمع المعلوماتي ظهرت قوانين جديدة تعتبر البيئة التنظيمية التشريعية التي تحمي هذا المجتمع وتحفظ حقوقه في جميع أبعاده، ويعمل الأمن السيبراني في هذا السياق على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.

سادساً: خصائص الأمن السيبراني: (السمحان، ٢٠٢٠، ١٢)

١. السرية: توفير ضمان بأن المعلومات لا تكون متاحة ولا يمكن الوصول إليها إلا للأشخاص أو الأنظمة المصرح لهم، من خلال استخدام أنظمة التشفير، والتحكم في الوصول، وجدران الحماية، مثل تشفير البريد الإلكتروني الحساس ليبقى محصوفاً على المرسل إليهم فقط.

٢. السلامة: يعمل على الحفاظ على دقة البيانات ومنع تعديلها أو تضررها من قبل جهات غير موثوقة، وذلك عبر التوقيعات الرقمية وتقنيات التحقق من التغييرات. على سبيل المثال، استخدام الهاش لاكتشاف أي تغيير في الملفات بعد تنزيلها.

٣. التوافر: يضمن الوصول المستمر إلى الخدمات والبيانات عند الحاجة، مثل حماية من هجمات (DDoS) وإنشاء نسخ احتياطية، مثل إعداد خوادم احتياطية لمواقع الإنترنت لضمان استمرار عملها.

٤. المصادقة والترخيص: تحقق من هوية المستخدم من خلال استخدام كلمات المرور، والبصمات، ويحدد الحقوق الممنوحة له.

٥. إدارة المخاطر والقدرة على التعافي: تهتم بتحديد التهديدات وتقييمها وتخفيفها مثل إصلاح الثغرات. كما تشير إلى القدرة على التعافي السريع بعد الهجمات، مثل استعادة البيانات من النسخ الاحتياطية.

فيما يرى آخرون بأن خصائص الأمن السيبراني تتكون مما يلي: (سمير، ٢٠١٧، ٢٨٥)

- التوسع: بهذا المجال له عدة أبعاد هي: (اقتصادية، ثقافية، قانونية، سياسية، عسكرية)

- الاستمرارية: الاستمرار في تقديم الخدمات دون انقطاع
 - الترابط: درجة عالية من التغير والترابط وسرعة التفاعل
 - النسبية: عدم وجود ام سيبراني مطلق لذلك فهو يتصف بالنسبية
 - المرونة: بحيث يتكيف مع التطورات والهجمات السيبرانية
 - الدفاع: يعتبر وسيلة دفاعية ضد الهجمات وعمليات القرصنة على نظم المعلومات
- سابعاً: الجريمة السيبرانية:** إن المخاطر السيبرانية تزداد كلما زادت سيطرة تكنولوجيا المعلومات والاتصال على مجرى الحياة، فأصبحنا أمام جرائم واقعية ومتكاملة الأركان، تتم عبر الإنترنت بأشكال مختلفة مثل سرقة الأموال والنصب والاحتيال والتخطيط للعمليات الإرهابية، بالإضافة إلى نشر الأخبار المضللة والقرصنة التي تعتبر الجريمة الأكثر شيوعاً في العالم الرقمي. في هذا السياق، فإن البحث في مكونات الأمن السيبراني والتحديات الأمنية في العصر الرقمي يحتاج إلى التعمق فيه من أجل توضيح بيئة التهديدات، خاصة أن الإنترنت يوفر لحوالي مليار ونصف من المواقع الإلكترونية وصفحات لا حصر لها، خاصة مع الانتشار الواسع بعد العام ٢٠١٨. وبالتعلق بموضوع التهديدات السيبرانية، تشير عدة تقارير وإحصائيات إلى أن نحو ٩٥ % من الشركات الكبرى متعددة الجنسيات تعترف بتعرضها للقرصنة، حيث اتخذت أكثر من حوالي ١٣٥ حكومة في العالم إجراءات صارمة تخص العالم الافتراضي والأمن الإلكتروني، خاصة مع كثرة الاعتداءات الإلكترونية بين الدول. (العمارات، ٢٠٢٢، ٤٢) وتقسيم الجرائم السيبرانية: (مناصرة، ٢٠١٨، ص ٤٨)
- صور الجرائم التقليدية مثل الاحتيال والتزوير المعلوماتي
 - نشر المحتوى غير القانوني بالوسائل الإلكترونية مثل المتعلقة بالعنف وانتهاك حقوق الملكية الفكرية
 - الاعتداءات على الشبكات الإلكترونية مثل القرصنة
- ثامناً: التدابير اللازمة لتوفير الامن السيبراني: (علي، ٢٠٢٠، ١٢٤)**
- ضرورة توفير التكنولوجيا الحديثة لمنح المنظمات والافراد أدوات الأمن السيبراني اللازمة لمواجهة الهجمات السيبرانية والاعتماد على الذكاء الاصطناعي مع متابعة التطور
 - توعية الأفراد بخطورة الهجمات السيبرانية، بأهمية الأمن السيبراني لمواجهة هذه المخاطر
 - تدريب الأفراد على كيفية التعامل مع المخاطر السيبرانية، لتقليل حجم الأضرار المترتبة عليها
 - عدم تثبيت البرامج والتطبيقات من مواقع غير موثوقة
 - يجب أن تكون كلمة السر قوية ومعقدة لا يستطيع الآخرون معرفتها
 - استخدام الجدران النارية التي تمنع التسلل والاختحام وهجوم الفيروسات الموجهة من خارج النظام عبر شبكة الإنترنت

- سن تشريعات قانونية صارمة تعمل على ردع الجرائم السيبرانية
- ضرورة التنسيق والتعاون الدولي أمنياً وإجرائياً وقضائياً
- ضرورة وجود هيئة متخصصة ذات كفاءة عالية في مواجهة الجرائم السيبرانية
- تمكين السلطات المسؤولة عن الضبط والتحقيق والملاحقة القانونية في مجال الأمن السيبراني مع تزويدهم بآليات تقنية متطورة لكشف مختلف الجرائم
- ٢- نظم المعلومات المحاسبية وخصائصها:

تعتبر نظم المعلومات من أهم موارد المنظمات، ومع التقدم التكنولوجي زادت هذه الأهمية مما جعل العديد من المنظمات الصناعية والخدمية تعتبر نظم المعلومات هي المورد الرئيسي لها وخاصة المنظمات التي تعتمد في تشغيلها على التطبيقات الإلكترونية، إن المحاسبة كنظام للمعلومات تعمل على جمع وترتيب وتحليل البيانات ومعالجتها إلى معلومات وتوصيلها للأطراف المختلفة المعنية لمساعدتهم في اتخاذ القرارات، ونظم المعلومات المحاسبية هي من مكونات نظام المعلومات الإدارية. (عيسى، ٢٠٠٣، ٢٠).

أولاً: مفهوم نظم المعلومات المحاسبية: عرفت نظم المعلومات المحاسبية بأنها "نظام يختص بجمع وترتيب ومعالجة وتخزين وتوصيل المعلومات القيمة حول الأحداث الاقتصادية في الماضي والحاضر والمستقبل إلى الأطراف المختلفة المستفيدة لمساعدتهم في اتخاذ القرار" (قاسم، ١٩٩٨، ١٤٧).

وعرفها آخر بأنها "أحد مكونات نظام المعلومات المحاسبية والتي تهتم بجمع وتصنيف ومعالجة العمليات المالية وتحويلها إلى معلومات وتوصيلها إلى الأطراف المختلفة ذات العلاقة لمساعدتهم في اتخاذ قرارات مناسبة ويتكون هذا النظام من الأشخاص والإجراءات وتكنولوجيا المعلومات" (عيسى، ٢٠٠٣، ٢٠).

يرى الباحثان أن المفاهيم أعلاه لنظم المعلومات المحاسبية تناولت تعريف نظم المعلومات المحاسبية من ناحية المهام التي تقوم بها هذه النظم، ولهذا يعرف الباحثان نظم المعلومات المحاسبية بأنها: "عبارة عن مجموعة من النظم الفرعية التي تعمل معاً بتناسق تام من خلال استقبال مدخلات البيانات المالية وغير المالية، والعمل على معالجتها بدقة عالية عن طريق التسجيل والترتيب والتلخيص وعرضها كمعلومات في شكل مخرجات محاسبية كتقارير وقوائم مالية وتعمل على تحقيق الرقابة الداخلية وتخدم الأطراف المعنية في اتخاذ القرارات الصائبة لتحقيق أهداف المنظمة".

من التعريف أعلاه يمكن استنتاج مكونات نظم المعلومات المحاسبية في الآتي:

- ١- مجموعة دفترية ومستندات تدعم العمليات المالية.

- ٢- يتكون نظم المعلومات المحاسبية من مجموعة من النظم الفرعية التي تعمل بتناسق كامل.
- ٣- الموارد البشرية والأشخاص الذين يقومون بتشغيل هذه النظم الفرعية.
- ٤- التعليمات والإجراءات اليدوية والآلية التي تستخدم في تجميع وتحليل ومعالجة البيانات.
- ٥- الأجهزة والحاسبات الآلية وملحقاتها ووسائط حفظ المعلومات.
- ٦- البرامج التي تعمل على هذه الحاسبات الآلية، والتي تهدف إلى تحقيق أهداف نظم المعلومات المحاسبية والتي تتمثل في الآتي:

- إنتاج التقارير والقوائم المالية مثل قائمة الدخل وقائمة المركز المالي والتدفقات النقدية وقائمة الأرباح المحتجزة والمعلومات المالية وغير المالية
- توفير تقارير بدقة عالية وفائدة للمستخدمين المختلفين.
- تقديم التقارير في الوقت المناسب للمساعدة في اتخاذ القرار.
- تحقيق الرقابة الداخلية للنظام المحاسبي.
- المساعدة في اتخاذ القرارات الصائبة لتحقيق أهداف المنظمة.

ثانياً: خصائص المعلومات المحاسبية:

الخصائص الأساسية:

أ- خاصية الملاءمة: تعتبر الملاءمة واحدة من الخصائص الأساسية للمعلومات المحاسبية، وسنستعرضها في دراستنا كما يلي:

الملاءمة من الناحية اللغوية: تعني التطابق، التناسب، والانسجام. ويُقال عن الشيء إنه غير ملائم إذا كان غير مناسب للظروف بطريقة غير لائقة أو غير ملائمة.

أما من الناحية العملية، فنقصد بها أن العمل الذي نريد تحديد مدى ملاءمته، يجب أن يتصف بخصائص تمنحه هذه الصفة.

فيما يتعلق بالملاءمة كمفهوم يتعلق بالمعلومات المحاسبية، فقد تناولها الباحثون في ميدان نظم المعلومات من خلال إعطائها عدة تعريفات، من أبرزها:

المعلومات الملائمة هي "تلك المعلومات التي تحتوي على الأقل على ثلاثة أبعاد، وهي: التأثير في الأهداف وتُسمى الملاءمة للأهداف، التأثير في الفهم وتُسمى الملاءمة الدلالية، والتأثير في اتخاذ القرارات وتُسمى الملاءمة للقرارات". (إسماعيل ونعوم، ٢٠١٢ ص ٢٩٠).

ب- خاصية الموثوقية: تعد الموثوقية ثاني الخصائص الأساسية للمعلومات المحاسبية بعد خاصية الملاءمة، وهي تتعلق بإمكانية الاعتماد على هذه المعلومات في العمل.

من الناحية اللغوية، يُقال "وثق" أي تأكد، والموثوقية مشتقة من هذا الفعل، وتعتبر عن مدى صدق ودقة المعلومات المحاسبية في تصوير الأحداث المالية، وحيادها في التعبير عن مقاييس تلك الأحداث. أما من الناحية العملية، لكي تكون المعلومات مفيدة، يجب أن تكون موثوقة. وتتحقق الموثوقية عندما تكون المعلومات:

- ١- خالية من الأخطاء الجوهرية
 - ٢- غير متحيزة
 - ٣- قابلة للاعتماد من قبل المستخدمين، أي أن المعلومات الموثوقة هي تلك التي تعبر بصدق عما يُفترض أن تعبر عنه، أو ما يُتوقع أن تعبر عنه بشكل معقول، (أحمد حلمي جمعة، ٢٠١٠، ص ٤).
- الخصائص المعززة
- ١- القابلية للمقارنة (Comparability) تُسهل على المستخدمين مقارنة المعلومات بين فترات مختلفة أو بين كيانات مختلفة
 - ٢- القابلية للفهم (Understandability) يجب عرض المعلومات بوضوح ومنطقية، بحيث يستطيع المستخدم العادي فهمها بسهولة
 - ٣- التحقق (Verifiability) تعني أن عدة مستخدمين مستقلين يمكن أن يصلوا إلى نفس النتائج عند استخدام نفس البيانات.
 - ٤- الملاءمة الزمنية (Timeliness) يجب تقديم المعلومات في الوقت المناسب لكي تكون مفيدة في اتخاذ القرار (اسماعيل ونعوم ٢٠١٢ ص ٢٩٠)

ثالثاً: تقييم مخاطر نظم المعلومات المحاسبية:

تعد نظم المعلومات المحاسبية من النظم التي تواجه العديد من المخاطر التي قد تؤثر على تحقيق أهداف تلك النظم وذلك نظراً لاعتمادها على الحاسوب، حيث تزامن التطور الكبير للحاسبات وأنظمة المعلومات مع التطور في تكنولوجيا المعلومات وسرعة انتشار هذه المعلومات واستخدامها إلكترونياً، ولقد صاحب هذا التطور في استخدام المعلومات الإلكترونية العديد من المخاطر والمشاكل التي تؤثر على أمن المعلومات سواء كانت تلك المخاطر مقصودة أو غير مقصودة، ولذلك تزايد الاهتمام الكبير بتوفير الوسائل والأساليب اللازمة لحماية نظم المعلومات والرقابة على عملياتها وضمان استمرارية عمل تلك النظم بشكل صحيح (أنيس وبنية، ٢٠١٨). وتقسم المخاطر من حيث الأثر إلى ما يلي: (أحمد، ٢٠٢٢، ١٢)

- ١- مخاطر شديدة الأثر وهي المخاطر التي تكون آثارها كبيرة وينتج عنها خسائر كبيرة قد تفوق قدرة المنشأة على التحمل مما قد يؤدي إلى الانهيار

٢- مخاطر متوسطة الأثر.

٣- مخاطر قليلة الأثر

ينطبق هذا التصنيف على احتمالية وقوع الخطر وتقييم آثاره عند وقوعه. هذا وتنقسم المخاطر أيضاً، من الناحية الكمية وذلك بقياس آثارها كمياً سواء من حيث نسبة حدوثها أو حجم الخسائر المترتبة عليها ويعتمد ذلك على فرضيات وإحصاءات رقمية تاريخية تبني عليها التوقعات وعادة ما تستخدم هذه الأساليب في القطاعات الحكومية والمؤسسات المالية كالبنوك وشركات التأمين أكثر من غيرها

رابعاً: كفاءة الكوادر البشرية وأهميتها للنظم المحاسبية

ان كفاءة الكوادر البشرية تلعب دوراً محورياً في نظم المعلومات المحاسبية، كما ان ضعف هذه الكوادر يمكن أن يؤدي إلى اتخاذ قرارات خاطئة وبالتالي التأثير سلباً على أدائها المؤسسي. وبشكل عام، يمكن ارجاع التحديات والمشكلات في نظم المعلومات المحاسبية إلى عدة عوامل، تشمل الممارسات السيئة والتحديات التقنية، والتي بدورها تؤثر على الثقة والمصادقية. هذه النتائج تؤكد أهمية وجود إرشادات وضوابط قوية لضمان جودة المعلومات المحاسبية واستخدام التكنولوجيا بفعالية لتحسين أنظمة المعلومات المحاسبية. (عيسى، ٢٠٠٣، ٢٢).

خامساً: دور الامن السيبراني في حماية النظم المحاسبية

يمتد نشاط الامن السيبراني ليشمل ما يلي: (Whitman & Mattord, 2018)

- ١- حماية البيانات والمعلومات المالية: حيث يمنع الامن السيبراني الوصول الى البيانات المالية غير المصرح به ويساعد على حماية وسرية وسلامة كافة المعاملات، مع حماية النظم المحاسبية من الاختراقات والتلاعب التي تؤدي الى الخسائر المالية وضبابية التقارير
- ٢- الحد من المخاطر التقنية والبشرية: يتيح الامن السيبراني للمؤسسات ان تتعرف على نقاط الضعف التقنية منها والبشرية مع تطبيق إجراءات وقائية كبرامج مكافحة الفيروسات وجدران الحماية والتشفير. الخ وذلك لضمان منع حدوث مشاكل واختراقات ذات تأثير علة استقرار النشاط
- ٣- استمرارية العمل: تدعم استراتيجيات الامن السيبراني خطط الإجابة على الطوارئ والتعافي من اية هجمات الكترونية، وهذا يضمن التعافي السريع والتقليل بالخسائر المالية يضمن الاستمرارية بالعمل دون توقفات.

المحور الثاني: الدراسة المسحية

أولاً: مجتمع وعينة البحث: شملت الدراسة المسحية عدد من المصارف الحكومية ومصارف القطاع الخاص العراقية، وتحديد المصارف العاملة في مدينة الموصل، وتمثل مجتمع البحث بالمحاسبين والعاملين في

الوظائف ذات الصلة بموضوع البحث في تلك المصارف. ولغرض تحديد حجم العينة تم الاسترشاد بقاعدة (Green, 1991). وفقاً لهذه القاعدة فإن الحد الأدنى لحجم العينة يمكن تحديده كما يأتي:

$$n \geq 50 + 8m$$

حيث ان:

n = الحد الأدنى لحجم العينة.

m = عدد المتغيرات المستقلة في نموذج الانحدار.

وبما ان نموذج الانحدار الخطي البسيط يتضمن متغير مستقل واحد، عليه فإن الحد الأدنى لحجم العينة:

$$n \geq 50 + 8(1) = 58$$

تم توزيع استمارة الاستبيان الخاصة بهذه الدراسة على عدد المصارف العاملة في مدينة الموصل خلال شهر تموز ٢٠٢٦، وقد بلغ عدد استمارات الاستبيان الصالحة للتحليل ١٠٧ استمارة، لذا فإن حجم العينة يُعد كافياً لإجراء تحليل الانحدار الخطي البسيط واختبار فرضيات الدراسة. ويوضح الجدول الآتي الهيكلية الخاصة باستمارة الاستبيان المستخدمة في هذه الدراسة، علماً بأنه تم تكميم اجابات افراد العينة باستخدام مقياس ليكرت الخماسي.

جدول رقم (١) هيكلية استمارة الاستبيان

ترتيب العبارات	رمز المتغير	المتغير	القسم
	D1	العمر	القسم الأول: المعلومات الديمغرافية
	D2	الجنس	
	D3	التحصيل العلمي	
	D4	الاختصاص العلمي	
	D5	عدد سنوات الخبرة	
X1 – X7	XX1	التدابير القانونية	القسم الثاني: تدابير الامن السيبراني
X8 – X18	XX2	التدابير التكنولوجية	
X19 – X25	XX3	التدابير التنظيمية	
X26 – X32	XX4	التدابير المتعلقة بالموظفين ومزودي الخدمات	
Y1 – Y14	Y	حماية نظم المعلومات الحاسبية	القسم الثالث: حماية نظم المعلومات الحاسبية

المصدر: الجدول من اعداد الباحثين

ثانياً: الخصائص العامة لأفراد العينة

يبين الجدول التالي الخصائص العامة لأفراد العينة (المستجيبين) وفقاً لخمس صفات هي (الجنس، العمر، المؤهل العلمي، الاختصاص العلمي وعدد سنوات الخبرة) وموزعة حسب التكرارات والنسبة المئوية الخاصة بكل فئة.

جدول رقم (٢) الخصائص العامة لأفراد العينة

النسبة المئوية	التكرار	الفئات	
58.9	٦٣	ذكر	الجنس
41.1	٤٤	انثى	
<u>%100</u>	<u>107</u>	المجموع	
5.6	6	20-29	العمر
40.2	43	30-39	
45.8	49	40-49	
8.4	9	50-59	
0.0	٠	٦٠ فأكثر	
<u>%100</u>	<u>107</u>	المجموع	
0.0	٠	دبلوم	المؤهل العلمي
80.4	86	بكالوريوس	
6.5	7	دبلوم عالي	
10.3	11	ماجستير او ما يعادلها	
2.8	3	دكتوراه او ما يعادلها	
<u>%100</u>	<u>107</u>	المجموع	
60.7	65	محاسبة	الاختصاص العلمي
20.6	22	علوم مالية ومصرفية	
5.6	6	نظم معلومات	
13.1	14	علوم حاسوب	
<u>%100</u>	<u>107</u>	المجموع	
8.4	9	أقل من ٥ سنوات	سنوات الخبرة
12.1	13	6-10	
50.5	54	11-15	
17.8	19	16-20	
11.2	12	أكثر من ٢٠	

المجموع	107	%100
---------	-----	------

المصدر: الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

يلاحظ من الجدول رقم (٢) في اعلاه ان الدراسة شملت (١٠٧) مستجيب من العاملين في عدد من المصارف في مدينة الموصل، شكل الذكور منهم (٥٨.٩%) والإناث (٤١.١%). ومن حيث العمر، تركزت غالبية أفراد العينة ضمن الفئتين العمريتين (٣٠-٣٩ سنة) و(٤٠-٤٩ سنة)، ونسب بلغت (٤٠.٢%) و (٤٥.٨%) على التوالي. وفيما يتعلق بالمؤهل العلمي، تمثل نسبة الحاصلين على شهادة البكالوريوس النسبة الأكبر من أفراد العينة (٨٠.٤%)، يليهم الحاصلين على شهادة الماجستير أو ما يعادلها (١٠.٣%)، ثم الدبلوم العالي (٦.٥%)، وحملة الدكتوراه أو ما يعادلها بنسبة (٢.٨%). أما من حيث التخصص العلمي، فقد استحوذ تخصص المحاسبة على النسبة الأعلى من افراد العينة بنسبة (٦٠.٧%)، يليه تخصص العلوم المالية والمصرفية (٢٠.٦%)، ثم التخصصات الأخرى وهي علوم الحاسوب ونظم المعلومات بنسبة (١٣.١%) و (5.6%) على التوالي.

وفيما يخص سنوات الخبرة، يبين الجدول ان نصف أفراد العينة تقريباً (٥٠.٥%) لديهم خبرة تتراوح بين (١١-١٥) سنة، تلتها فئة (١٦-٢٠) سنة بنسبة (١٧.٨%)، ثم فئة (٦-١٠) سنوات بنسبة (١٢.١%)، في حين بلغت نسبة الذين لديهم خبرة عملية تزيد على (٢٠) سنة (١١.٢%).

وتعكس هذه الخصائص ان العينة تضم مشاركين ذوي خلفيات علمية وخبرات مهنية متنوعة ملائمة لطبيعة الدراسة، حيث أن تركز العينة في الفئات العمرية (٣٠ - ٤٩) سنة بنسبة بلغت (٨٦%)، وحملة شهادة البكالوريوس وما فوق بنسبة (١٠٠%)، والذين يمتلكون خبرة أكثر من ١٠ سنوات بنسبة تتجاوز (٧٩.٥%)، يعطي موثوقية عالية للبيانات المجمعة، نظراً لأن أفراد العينة يمتلكون الخبرة المهنية والمؤهلات العلمية الكافية لإدراك مخاطر التهديدات السيبرانية على نظم المعلومات المحاسبية في المصارف.

ثالثاً: اختبار الثبات

تم اختبار وقياس ثبات الاستبيان المستخدم في هذه الدراسة من خلال معامل ألفا كرونباخ، وهو مقياس لموثوقية الاتساق الداخلي تتراوح قيمته من ٠ الى ١ ، ويعتبر المقياس الأكثر استخداماً، ومن المتفق عليه عموماً أن الحد الأدنى المقبول لمعامل ألفا كرونباخ هو ٠.٧٠ (Hair et al, 2019) وتشير نتائج اختبار الثبات المبينة في الجدول رقم (٣) إلى ان جميع معاملات ألفا كرونباخ قد تجاوزت الحد المقبول (٠.٧٠)، مما يؤكد ان جميع المقاييس تتمتع بدرجة جيدة من الاتساق الداخلي. حيث بلغ معامل الاتساق للمتغير المستقل ككل "تدابير الأمن السيبراني" (٠.٩٤٥)، بينما بلغ للمتغير التابع

"حماية نظم المعلومات المحاسبية" (٠.٩١٤)، وهي قيم تعكس ثبات مرتفع ، بما يدعم امكانية الاعتماد على هذه المقاييس في اختبار فرضيات الدراسة.

جدول رقم (٣) اختبار الثبات

المتغير	الرمز	عدد العبارات	معامل ألفا كرونباخ
التدابير القانونية	XX1	7	0.832
التدابير التكنولوجية	XX2	11	0.830
التدابير التنظيمية	XX3	7	0.799
التدابير المتعلقة بالموظفين ومزودي الخدمات	XX4	7	0.808
تدابير الأمن السيبراني	X	32	0.945
حماية نظم المعلومات المحاسبية	Y	14	٠.914
الإجمالي	-	46	٠.963

المصدر: الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

رابعاً: الاحصاءات الوصفية لمتغيرات وابعاد الدراسة

يوضح الجدول التالي بعض الاحصاءات الوصفية مثل الوسط الحسابي والانحراف المعياري المتعلقة بمتغيرات البحث الرئيسة والفرعية:

جدول رقم (٤) الإحصاءات الوصفية لمتغيرات وابعاد الدراسة

الترتيب	الأهمية النسبية (%)	الانحراف المعياري	الوسط الحسابي	الرمز	المتغير / البعد
4	84.64	0.39	4.23	X	تدابير الأمن السيبراني
6	83.50	0.50	4.18	XX1	التدابير القانونية
2	84.92	0.41	4.25	XX2	التدابير التكنولوجية
5	84.60	0.38	4.23	XX3	التدابير التنظيمية
1	85.36	0.42	4.27	XX4	التدابير المتعلقة بالموظفين ومزودي الخدمات
3	84.74	0.43	4.24	Y	حماية نظم المعلومات المحاسبية

المصدر: الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

يلاحظ من الجدول رقم (٤) ان المتوسطات الحسابية لمتغيرات الدراسة تراوحت بين (٤.١٨) و(٤.٢٧)، مما يشير إلى ميل استجابات أفراد العينة نحو الموافقة على عبارات الدراسة، ويعكس ارتفاعاً

في مستوى إدراك أفراد العينة لمتغيرات الدراسة. وقد احتل بعد "التدابير المتعلقة بالموظفين ومزودي الخدمات" المرتبة الأولى بمتوسط حسابي بلغ (٤.٢٧)، وانحراف معياري (٠.٤٢)، وأهمية نسبية (٨٥.٣٦٪)، يليه بعد "التدابير التكنولوجية" بمتوسط حسابي (٤.٢٥) وأهمية نسبية (٨٤.٩٢٪). بينما احتل بعد "التدابير القانونية" المرتبة الأخيرة بمتوسط حسابي (٤.١٨)، وانحراف معياري (٠.٥٠)، وأهمية نسبية (٨٣.٥٠٪)، كما بلغ المتوسط الحسابي للمتغير المستقل الكلي "تدابير الأمن السيبراني" (٤.٢٣) بانحراف معياري (٠.٣٩) وأهمية نسبية (٨٤.٦٤٪)، في حين بلغ المتوسط الحسابي للمتغير التابع "حماية نظم المعلومات المحاسبية" (٤.٢٤) بانحراف معياري (٠.٤٣) وأهمية نسبية (٨٤.٧٤٪). وبشكل عام، تشير الانحرافات المعيارية المنخفضة نسبياً والتي تراوحت بين (٠.٣٨) و (٠.٥٠)، إلى تقارب استجابات أفراد العينة وارتفاع درجة الاتفاق على عبارات الاستبيان.

خامساً: اختبار فرضيات الدراسة

١) اختبار الفرضية الرئيسية الأولى (H1): توجد علاقة ذات دلالة إحصائية بين تدابير الأمن السيبراني وحماية نظم المعلومات المحاسبية. ولغرض اختبار هذه الفرضية تم حساب معامل الارتباط بيرسون (Pearson) لتحديد معنوية وقوة واتجاه العلاقة بين المتغيرات، ويظهر الجدول التالي قيمة معامل الارتباط بين المتغير المستقل والمتغير التابع وكذلك بين كل بعد من ابعاد المتغير المستقل والمتغير التابع.

جدول رقم (٥) العلاقة بين تدابير الأمن السيبراني وحماية نظم المعلومات المحاسبية

المتغيرات والابعاد	الرمز	حماية نظم المعلومات المحاسبية Y	
التدابير القانونية	XX1	Pearson	0.775**
		Sig.	0.000
التدابير التكنولوجية	XX2	Pearson	0.826**
		Sig.	0.000
التدابير التنظيمية	XX3	Pearson	0.776**
		Sig.	0.000
التدابير المتعلقة بالموظفين	XX4	Pearson	0.870**
		Sig.	0.000
تدابير الأمن السيبراني	X	Pearson	0.878**
		Sig.	0.000

المصدر: الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

** الارتباط دال معنوياً عند مستوى دلالة ٠.٠١

أظهرت نتائج تحليل الارتباط وجود ارتباطات موجبة وقوية بين جميع أبعاد المتغير المستقل (تدابير الأمن السيبراني) والمتغير التابع (حماية نظم المعلومات المحاسبية) ، ويلاحظ ان أعلى ارتباط ($r = 0.870$) هو بين بعد (التدابير المتعلقة بالموظفين ومزودي الخدمات) والمتغير التابع (حماية نظم المعلومات المحاسبية)، يليه البعد الثاني (التدابير التكنولوجية) حيث بلغت قيمة معامل الارتباط ($r = 0.826$)، كما بلغت قيمة معامل الارتباط ($r = 0.878$) بين المتغير المستقل الكلي (تدابير الأمن السيبراني) والمتغير التابع (حماية نظم المعلومات المحاسبية)، مما يدل على وجود علاقة ارتباط معنوية وموجبة تدعم قبول الفرضية الرئيسية الأولى للبحث (H1) والانتقال إلى تحليل الانحدار لاختبار فرضيات الدراسة الأخرى. وتنعكس النتائج في أعلاه ان ارتفاع مستوى حماية نظم المعلومات المحاسبية في المصارف يرتبط بدرجة عالية بالزيادة أو الارتفاع في تدابير الأمن السيبراني، ولا سيما التدابير المتعلقة بالموظفين ومزودي الخدمات و التدابير التكنولوجية، مما يشير الى الدور المحوري للعنصر البشري في المحافظة على سرية المعلومات المحاسبية وسلامة السجلات والحد من مخاطر الوصول غير المصرح به أو إساءة استخدام البيانات من جهة، وإلى أهمية الوسائل والضوابط التكنولوجية المستخدمة في دعم حماية نظم المعلومات المحاسبية من التهديدات السيبرانية من جهة أخرى.

(٢) اختبار الفرضية الرئيسية الثانية (H2): يوجد أثر ذو دلالة إحصائية لكل بعد من أبعاد تدابير الأمن السيبراني على حماية نظم المعلومات المحاسبية في المصارف عينة البحث. ولغرض اختبار الفرضية الرئيسية الثانية في أعلاه تم تجزئتها الى أربع فرضيات فرعية وإجراء تحليل انحدار خطي بسيط بين كل بعد من ابعاد المتغير المستقل والمتغير التابع وكما يأتي:

الفرضية الفرعية الأولى H2a : يوجد أثر ذو دلالة إحصائية لبعد التدابير القانونية على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

يبين الجدول الآتي نتائج تحليل الانحدار الخطي البسيط بين بعد التدابير القانونية وحماية نظم المعلومات المحاسبية:

جدول رقم (٦) تأثير بعد التدابير القانونية على حماية نظم المعلومات المحاسبية

المتغير المستقل	B	β	T	Sig.	R^2	Adjusted R^2	F	Sig. (F)
XX1	0.660	0.775	12.549	<0.001	0.600	0.596	157.485	<0.001

المصدر : الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

يلاحظ من الجدول رقم (٦) في أعلاه وجود تأثير إيجابي ودال إحصائياً للبعد الأول (التدابير القانونية) في المتغير التابع (حماية نظم المعلومات المحاسبية)، وذلك حسب إدراك أفراد العينة، حيث تشير قيمة معامل الانحدار المعياري ($\beta = 0.775$) الى قوة واتجاه التأثير، بينما تؤكد قيمة ($t = 12.549$) عند مستوى دلالة إحصائية ($\text{Sig.} < 0.001$) معنوية معامل الانحدار. وبلغت قيمة معامل التحديد ($R^2 = 0.600$)، وهو ما يعني أن البعد الأول (التدابير القانونية) يفسر نسبة (٦٠٪) من التباين في المتغير التابع (حماية نظم المعلومات المحاسبية)، في حين تعزى النسبة المتبقية (٤٠٪) إلى عوامل أخرى لم يتضمنها النموذج. كما تؤكد نتائج اختبار تحليل التباين ($\text{Sig.} < 0.001, F = 157.485$) معنوية نموذج الانحدار ككل، مما يدعم قبول الفرضية الفرعية الأولى (H2a) والتي تنص على وجود أثر ذو دلالة إحصائية لبعـد التدابير القانونية على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

وتشير هذه النتائج إلى أهمية وجود إجراءات وتدابير قانونية واضحة وفعالة في المصارف تنظم حماية البيانات والمعلومات المحاسبية وتحدد المسؤوليات والالتزامات المرتبطة باستخدام نظم المعلومات المحاسبية. حيث ان وضوح المتطلبات القانونية ذات الصلة بأمن المعلومات والبيانات يسهم في تعزيز الالتزام بالضوابط والإجراءات التي تحد من مخاطر الوصول غير المصرح به أو إساءة استخدام المعلومات أو التلاعب بالبيانات المحاسبية. وعليه، فإن التدابير القانونية – بوصفها جزءاً من تدابير الأمن السيبراني – يمكن أن تشكل إطاراً داعماً لحماية نظام المعلومات المحاسبية وتعزيز الوثوقية في مخرجاته.

الفرضية الفرعية الثانية H2b: يوجد أثر ذو دلالة إحصائية لبعـد التدابير التكنولوجية على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

يبين الجدول التالي نتائج تحليل الانحدار الخطي البسيط بين بعـد التدابير التكنولوجية وحماية نظم المعلومات المحاسبية:

جدول رقم (٧) تأثير بعـد التدابير التكنولوجية على حماية نظم المعلومات المحاسبية

المتغير المستقل	B	β	T	Sig.	R^2	Adjusted R^2	F	Sig. (F)
XX2	0.866	0.826	14.997	<0.001	0.682	0.679	224.906	<0.001

المصدر: الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

يلاحظ من الجدول رقم (٧) في أعلاه وجود تأثير إيجابي ودال إحصائياً للبعد الثاني (التدابير التكنولوجية) في المتغير التابع (حماية نظم المعلومات المحاسبية)، وذلك حسب إدراك افراد العينة، حيث تشير قيمة معامل الانحدار المعياري ($\beta = 0.826$) الى قوة واتجاه التأثير، بينما تؤكد قيمة ($t = 14.997$) عند مستوى دلالة إحصائية ($\text{Sig.} < 0.001$) معنوية معامل الانحدار. وبلغت قيمة معامل التحديد ($R^2 = 0.682$)، وهو ما يعني أن البعد الثاني (التدابير التكنولوجية) يفسر نسبة (٦٨.٢٪) من التباين في المتغير التابع (حماية نظم المعلومات المحاسبية)، في حين تعزى النسبة المتبقية (٣١.٨٪) إلى عوامل أخرى لم يتضمنها النموذج. كما تؤكد نتائج اختبار تحليل التباين ($\text{Sig.} < 0.001, F = 224.906$) معنوية نموذج الانحدار ككل، وبناءً على ما سبق يتم قبول الفرضية الفرعية الثانية (H2b) التي تنص على وجود أثر ذو دلالة إحصائية لبعد التدابير التكنولوجية على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

وتعكس هذه النتائج أهمية البنية التكنولوجية في المحافظة على سلامة نظم المعلومات المحاسبية والبيانات التي تتضمنها. حيث تعتمد نظم المعلومات المحاسبية بصورة متزايدة على تقنيات تخزين ومعالجة ونقل البيانات إلكترونياً وعبر الخدمات والبرامج المستندة الى الحوسبة السحابية، الأمر الذي يجعل كفاءة الوسائل التكنولوجية المستخدمة عاملاً مهماً في الحد من مخاطر الوصول غير المصرح به، أو التعديل غير المشروع، أو فقدان البيانات، أو تعطيل عملية معالجة البيانات المحاسبية. وبالتالي، فإن تعزيز التدابير التكنولوجية في المصارف يمكن أن يدعم سلامة البيانات المحاسبية، بما ينعكس على موثوقية المعلومات التي ينتجها نظام المعلومات المحاسبية.

الفرضية الفرعية الثالثة H2c : يوجد أثر ذو دلالة إحصائية لبعد التدابير التنظيمية على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

يبين الجدول التالي نتائج تحليل الانحدار الخطي البسيط بين بعد التدابير التنظيمية وحماية نظم المعلومات المحاسبية:

جدول رقم (٨) تأثير بعد التدابير التنظيمية على حماية نظم المعلومات المحاسبية

المتغير المستقل	B	β	T	Sig.	R ²	Adjusted R ²	F	Sig. (F)
XX3	.870٠	.776٠	12.614	<0.001	0.602	0.599	159.102	<0.001

المصدر: الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

يلاحظ من الجدول رقم (٨) في أعلاه وجود تأثير إيجابي ودال إحصائياً للبعد الثالث (التدابير التنظيمية) في المتغير التابع (حماية نظم المعلومات المحاسبية)، وذلك حسب إدراك افراد العينة، حيث تشير قيمة معامل الانحدار المعياري ($\beta = 0.776$) الى قوة واتجاه التأثير، بينما تؤكد قيمة ($t = 12.614$) عند مستوى دلالة إحصائية ($\text{Sig.} < 0.001$) معنوية معامل الانحدار. وبلغت قيمة معامل التحديد ($R^2 = 0.602$)، وهو ما يعني أن البعد الثالث (التدابير التكنولوجية) يفسر نسبة (٦٠.٢٪) من التباين في المتغير التابع (حماية نظم المعلومات المحاسبية)، في حين تعزى النسبة المتبقية (٣٩.٨٪) إلى عوامل أخرى لم يتضمنها النموذج. كما تؤكد نتائج اختبار تحليل التباين ($\text{Sig.} < 0.001, F = 159.102$) معنوية نموذج الانحدار ككل، وبناءً على ذلك يتم قبول الفرضية الفرعية الثالثة (H2c) والتي تنص على وجود أثر ذو دلالة إحصائية لبعـد التدابير التنظيمية على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

وتشير هذه النتائج الى ان التدابير التنظيمية مثل (انشاء وحدة مختصة بالأمن السيبراني، ووجود سياسات واضحة للأمن السيبراني، ووضوح قنوات الاتصال والأدوار والمسؤوليات ذات الصلة، وإجراء عمليات تقييم منتظمة لفعالية ضوابط الأمن السيبراني، فضلاً عن تعزيز ثقافة الأمن السيبراني داخل المؤسسة) يمكن ان تساهم بشكل كبير في تعزيز حماية نظم المعلومات المحاسبية والبيانات المحاسبية من المخاطر السيبرانية.

الفرضية الفرعية الرابعة H2d : يوجد أثر ذو دلالة إحصائية لبعـد التدابير المتعلقة بالموظفين ومزودي الخدمات على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

يبين الجدول التالي نتائج تحليل الانحدار الخطي البسيط بين بعد التدابير المتعلقة بالموظفين و حماية نظم المعلومات المحاسبية:

جدول رقم (٩) تأثير بعد التدابير المتعلقة بالموظفين ومزودي الخدمات على حماية نظم المعلومات المحاسبية

المتغير المستقل	B	β	T	Sig.	R^2	Adjusted R^2	F	Sig. (F)
XX	0.894	0.870	18.097	<0.001	.757	.755	327.512	<0.001

المصدر: الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

يلاحظ من الجدول رقم (٩) في أعلاه وجود تأثير إيجابي ودال إحصائياً للبعد الرابع من ابعاد المتغير المستقل (التدابير المتعلقة بالموظفين ومزودي الخدمات) في المتغير التابع (حماية نظم المعلومات المحاسبية)، وذلك حسب إدراك افراد العينة، حيث تدل قيمة معامل الانحدار المعياري ($\beta = 0.870$) على قوة واتجاه التأثير، بينما تؤكد قيمة ($t = 18.097$) عند مستوى دلالة إحصائية ($\text{Sig.} < 0.001$) معنوية معامل الانحدار. وبلغت قيمة معامل التحديد ($R^2 = 0.757$)، وهو ما يعني أن هذا البعد يفسر نسبة (٧٥.٧٪) من التباين في المتغير التابع (حماية نظم المعلومات المحاسبية)، في حين تعزى النسبة المتبقية (٢٤.٣٪) إلى عوامل أخرى لم يتضمنها النموذج. كما تؤكد نتائج اختبار تحليل التباين ($\text{Sig.} < 0.001$)، ($F = 327.512$) معنوية نموذج الانحدار ككل، مما يدعم قبول الفرضية الفرعية الرابعة (H2d) والتي تنص على وجود أثر ذو دلالة إحصائية لبعـد التدابير المتعلقة بالموظفين على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

أظهرت نتائج الانحدار البسيط أن جميع الأبعاد الأربعة للمتغير المستقل (تدابير الأمن السيبراني) تؤثر تأثيراً معنوياً في المتغير التابع (حماية نظم المعلومات المحاسبية) عند اختبار كل بعد على حدة، إلا أن قوة التأثير تختلف فيما بينها. فقد جاء بعد (التدابير المتعلقة بالموظفين ومزودي الخدمات) في المرتبة الأولى من حيث القدرة التفسيرية، يليه بعد التدابير التكنولوجية، ثم بعد التدابير التنظيمية وبعد التدابير القانونية. مما يشير الى ضرورة الاهتمام بتحسين وتعزيز التدابير المتعلقة بالموظفين ومزودي الخدمات وكذلك التدابير التكنولوجية في المصارف لأنها قد تكون التدابير الأكثر إسهاماً في تعزيز حماية نظم المعلومات المحاسبية وذلك من منظور افراد عينة البحث.

ويمكن تفسير ارتفاع تأثير بعد (التدابير المتعلقة بالموظفين ومزودي الخدمات) مقارنة مع الابعاد الأخرى لتدابير الأمن السيبراني، بأن المورد البشري يمثل خط الدفاع الأول في حماية نظم المعلومات المحاسبية، إذ يتعامل الموظفون بصورة مباشرة مع البيانات والسجلات المحاسبية، ويمارسون عمليات إدخالها ومعالجتها وتعديلها واسترجاعها، كما أن سلوكهم والتزامهم بإجراءات الأمن السيبراني يؤثران بصورة

مباشرة في مستوى حماية المعلومات. وتزداد أهمية هذا البعد مع وجود أطراف ومزودي خدمات خارجيين قد يمتلكون صلاحيات الوصول إلى الأنظمة والبيانات المحاسبية، مما يجعل التحقق من موثوقيتهم عنصراً أساسياً في الحد من مخاطر الوصول غير المصرح به أو إساءة استخدام المعلومات.

(٣) اختبار الفرضية الرئيسية الثالثة (H3): يوجد أثر ذو دلالة إحصائية لتدابير الأمن السيبراني إجمالاً على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

يبين الجدول التالي نتائج تحليل الانحدار الخطي البسيط بين متغير تدابير الأمن السيبراني وحماية نظم المعلومات المحاسبية:

جدول رقم (١٠) تأثير تدابير الامن السيبراني على حماية نظم المعلومات المحاسبية

المتغير المستند	B	β	T	Sig.	R ²	Adjusted R ²	F	Sig. (F)
X	0.956	0.878	18.811	<0.001	0.771	0.769	353.856	<0.001

المصدر: الجدول من اعداد الباحثين بالاعتماد على مخرجات برنامج SPSS23

يلاحظ من الجدول رقم (١٠) في أعلاه وجود تأثير إيجابي ودال إحصائياً لمتغير (تدابير الأمن السيبراني) على المتغير التابع (حماية نظم المعلومات المحاسبية)، وذلك حسب إدراك افراد العينة، حيث تشير قيمة معامل الانحدار المعياري ($\beta = 0.878$) الى قوة واتجاه التأثير، بينما تؤكد قيمة ($t = 18.811$) عند مستوى دلالة إحصائية ($\text{Sig.} < 0.001$) معنوية معامل الانحدار. وبلغت قيمة معامل التحديد ($R^2 = 0.771$)، مما يعني أن متغير تدابير الأمن السيبراني يفسر ما نسبته (٧٧.١٪) من التباين في المتغير التابع (حماية نظم المعلومات المحاسبية)، في حين تعزى النسبة المتبقية (٢٢.٩٪) إلى عوامل أخرى لم يتضمنها النموذج. كما تؤكد نتائج اختبار تحليل التباين ($\text{Sig.} < 0.001, F = 353.856$) معنوية نموذج الانحدار ككل، مما يدعم قبول الفرضية الرئيسية الثالثة (H3) والتي تنص على وجود أثر ذو دلالة إحصائية لتدابير الامن السيبراني على حماية نظم المعلومات المحاسبية في المصارف عينة البحث.

تشير هذه النتائج بصورة عامة إلى أن حماية نظم المعلومات المحاسبية ترتبط بدرجة كبيرة بمدى شمولية وتكامل تدابير الأمن السيبراني المتنوعة، وليس بفعالية أحد أبعادها بصورة منفردة. حيث أن حماية نظم المعلومات المحاسبية تتطلب منظومة متكاملة من التدابير القانونية والتكنولوجية والتنظيمية والتدابير

ذات الصلة بالموظفين ومزودي الخدمات، لأن البيانات والمعلومات المحاسبية تمر بمراحل متعددة من الإدخال والمعالجة والتخزين والاسترجاع والتبادل، مما يجعلها عرضة لمخاطر الوصول غير المصرح به، أو التعديل، أو فقدان، أو التعطيل. وبالتالي، فإن تكامل هذه التدابير يساهم في المحافظة على سرية البيانات المحاسبية وسلامتها وتوافرها في الوقت المناسب، وهي متطلبات أساسية لضمان موثوقية المعلومات المحاسبية وجودة التقارير المالية.

وبالعودة الى الجدول رقم (٥) السابق نجد ان معاملات الارتباط المرتفعة تتسق مع نتائج تحليل الانحدار، إذ تؤكد وجود علاقات إيجابية قوية بين كل بعد من أبعاد المتغير المستقل والمتغير التابع، وكذلك بين المتغير المستقل إجمالاً والمتغير التابع، كما تدعم معاملات الثبات المرتفعة موثوقية أدوات القياس، مما يعزز الثقة في النتائج المستخلصة.

تتفق نتائج الدراسة الحالية مع ما توصلت إليه دراسة (Mariyoush & Wathiq, 2024)، التي أكدت أن الأمن السيبراني يؤثر بصورة مباشرة في نظم المعلومات المحاسبية، وأشارت الدراسة إلى أن تعزيز متطلبات وممارسات الأمن السيبراني يساهم في الحد من المخاطر والتهديدات السيبرانية التي قد تؤثر في كفاءة نظم المعلومات المحاسبية وموثوقيتها.

كما تتفق نتائج الدراسة الحالية جزئياً مع دراسة (AlHyasat & Falahat, 2026)، والتي أظهرت وجود تأثير إيجابي ودال إحصائياً لاستراتيجية الأمن السيبراني في فعالية نظم المعلومات في مؤسسات التعليم العالي الأردنية. وتتفق نتائج الدراسة جزئياً كذلك مع دراسة (Al-Mohammed et al., 2026) التي توصلت الى ان الوعي بالأمن السيبراني كان له تأثير إيجابي ودال إحصائياً على أمن المعلومات المحاسبية في بيئة المصارف الحكومية العراقية. مما يؤكد أهمية الممارسات والوعي المرتبطين بالأمن السيبراني في تعزيز حماية البيانات والمعلومات ضمن نظم المعلومات المحاسبية.

الاستنتاجات والتوصيات

في ظل المفاهيم النظرية التي تم تناولها في هذا البحث والنتائج التي تم التوصل إليها تم استنباط بعض الاستنتاجات واقتراح عدد من التوصيات أهمها:

أولاً: الاستنتاجات

١. ان تعزيز تدابير ومتطلبات الأمن السيبراني بجوانبها المتعددة يسهم في زيادة مستوى حماية نظم المعلومات الحاسوبية وتحسين كفاءتها وموثوقيتها.
٢. أظهرت نتائج تحليل الانحدار وجود تأثير قوي لتدابير الأمن السيبراني المتعلقة بالموظفين ومزودي الخدمات، وهو ما يدل على أهمية هذه التدابير في حماية نظم المعلومات الحاسوبية في المصارف وفقاً لإدراك أفراد العينة.
٣. ان تدابير الأمن السيبراني لا تمثل جانباً تقنياً منفصلاً عن نظم المعلومات الحاسوبية، وإنما تعد أحد العوامل الداعمة لكفاءتها وموثوقيتها، نظراً لما توفره من حماية للبيانات والمعلومات الحاسوبية والحد من المخاطر والتهديدات السيبرانية التي قد تؤثر عليها بصورة سلبية.
٤. تعكس النتائج أهمية تبني الشركات بما في ذلك المصارف لنظرة متكاملة إلى أمن نظم المعلومات الحاسوبية، بحيث لا تقتصر إجراءات الحماية على الجوانب التقنية فقط، وإنما تمتد لتشمل السياسات والإجراءات التنظيمية، وتعزيز الوعي لدى العاملين، وآليات الرقابة والمتابعة والاستجابة للمخاطر السيبرانية.
٥. يمكن الاستنتاج أن رفع مستوى تدابير الأمن السيبراني يمثل عاملاً مهماً في تعزيز الثقة في مخرجات نظم المعلومات الحاسوبية، بما يساعد على توفير معلومات أكثر موثوقية يمكن الاعتماد عليها في اتخاذ القرارات المالية والإدارية المختلفة.

ثانياً: التوصيات

١. تعزيز الاستثمار في متطلبات الأمن السيبراني داخل المصارف العراقية، من خلال توفير التقنيات والأنظمة الأمنية المناسبة وتحديثها بصورة مستمرة بما يتلاءم مع التطورات المتسارعة في طبيعة التهديدات السيبرانية.
٢. تطوير سياسات وإجراءات أمنية واضحة لحماية نظم المعلومات الحاسوبية، مع تحديد المسؤوليات والصلاحيات المتعلقة بالوصول إلى البيانات والأنظمة، ومراجعتها بصورة دورية للتأكد من فاعليتها.
٣. زيادة برامج التدريب والتوعية للعاملين في المجالين الحاسوبي وتقنية المعلومات، بهدف تعزيز قدرتهم على اكتشاف المخاطر والتهديدات السيبرانية والتعامل معها بصورة صحيحة.



٤. تعزيز إجراءات الرقابة على الوصول إلى نظم المعلومات المحاسبية من خلال تطبيق آليات مناسبة لإدارة صلاحيات المستخدمين، والتأكد من منح الصلاحيات وفقاً لطبيعة المهام والمسؤوليات الوظيفية.
٥. إجراء اختبارات وتقييمات دورية لمستوى الأمن السيبراني في نظم المعلومات المحاسبية، بهدف الكشف المبكر عن نقاط الضعف ومعالجتها قبل أن تتحول إلى مخاطر فعلية تؤثر في سرية البيانات وسلامتها وتوافرها.
٦. اعتماد الأمن السيبراني كأحد المعايير الأساسية عند تطوير أو تحديث نظم المعلومات المحاسبية، وعدم التعامل معه بوصفه إجراء لاحق، بما يضمن إدماج متطلبات حماية نظام المعلومات المحاسبية منذ مراحل تصميم النظام وتشغيله.

المصادر والمراجع

- أبو زيد، ع. ع. (٢٠١٩). الأمن السيبراني في الوطن العربي: دراسة حالة المملكة العربية السعودية. المركز العربي للبحوث والدراسات. <https://www.acrseg.org/41356>
- أحمد، س. (٢٠٢٢). إدارة المخاطر بشركات التأمين على الممتلكات والمسئولية المسجلة بالبورصة المصرية باستخدام اختبارات الضغوط. *المجلة العلمية للاقتصاد والتجارة*، ٥٢ (٤)، ٢٧١-٢٩٨. <https://search.emarefa.net/detail/BIM-1426278>
- إسماعيل، خ. إ.، وريان، ن. (٢٠١٢). الخصائص النوعية للمعلومات المحاسبية بين النظرية والتطبيق. *المحاسبان*، م. ع. ب. ص. (٢٠٢٠). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود *مجلة كلية التربية بالمنصورة*، ١١١ (١)، ٢٩-٢٠. <https://search.emarefa.net/detail/BIM-1101516>
- العمارات، ف.، والحامصة، إ. م. (٢٠٢٢). الأمن السيبراني لأنظمة المعلومات: المفهوم وتحديات العصر. دار الخليج للنشر والتوزيع، الأردن.
- أنيس، ك. م. أ.، وعمر، ب. (٢٠١٧). مخاطر استخدام نظم المعلومات المحاسبية الإلكترونية وأثرها على فاعلية المراجعة في الجزائر. *مجلة جامعة القدس المفتوحة للبحوث الإنسانية والاجتماعية*، ١١ (٤٠)، ٤٠-١١. <https://journals.gou.edu/index.php/jresstudy/article/view/566>
- بارة، س. (٢٠١٧). الأمن السيبراني في الجزائر (Cyber Security): السياسات والمؤسسات. *المجلة الجزائرية للأمن الإنساني*، ٢ (٢)، ٢٥٥-٢٨٠. <https://asjp.cerist.dz/en/article/66092>
- جمعة، أ. ح. (٢٠١٠). نظرية المحاسبة المالية: النموذج الدولي الجديد. دار صفاء للنشر والتوزيع، عمان.
- سليمان، م. (٢٠٢٢). نظرية الأنشطة الروتينية: نظرية جديدة لفهم الجرائم السيبرانية. *المجلة المصرية للعلوم الاجتماعية والسلوكية*، ٦ (٦)، ١١٤-١٣٠. <https://doi.org/10.21608/ejsbs.2022.129409.1005>
- شلوش، ن. (٢٠١٨). القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول. *مجلة مركز بابل للدراسات الإنسانية*، ٨ (٢)، ١٨٥-٢٠٦. <https://bcchj.uobabylon.edu.iq/index.php/bcchj/ar/article/view/438>
- عبد الرزاق، م. ق. (١٩٩٨). نظم المعلومات المحاسبية. دار الثقافة للنشر والتوزيع، عمان، الأردن.
- علي، ز. ع. (٢٠٢٠). الصراع والأمن الجيوسياسي في الساحة الدولية: دراسة في استراتيجيات الاشتباك الرقمي. دار أمجد للنشر والتوزيع، عمان.
- مناصرة، ي. (٢٠١٨). جرائم المساس بأنظمة المعالجة الآلية للمعطيات.
- الهيئة الوطنية للأمن السيبراني. (٢٠١٨). الضوابط الأساسية للأمن السيبراني الإصدار ١٠٠. الرياض: الهيئة الوطنية للأمن السيبراني. <https://ega.ce/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf>

٢. ترجمة المصادر العربية إلى الإنكليزية

- Abu Zaid, A. A. (2019). *Cybersecurity in the Arab World: A Case Study of the Kingdom of Saudi Arabia*. Arab Center for Research and Studies. <https://www.acrseg.org/41356>
- Ahmed, S. (2022). *Risk management in property and liability insurance companies listed on the Egyptian Stock Exchange using stress tests*. Scientific Journal of Economics and Commerce, 52(4), 271-298. <https://search.emarefa.net/detail/BIM-1426278>
- Ismail, K. I., & Ryan, N. (2012). *Qualitative characteristics of accounting information between theory and practice*.

- Al-Samhan, M. A. (2020). *Requirements for achieving cybersecurity for administrative information systems at King Saud University*. Faculty of Education, Mansoura University. <https://search.emarefa.net/detail/BIM-1101516>
- Al-Amarat, F., & Al-Hamamsa, I. M. (2022). *Cybersecurity of information systems: Concept and contemporary challenges*. Dar Al-Khaleej Publishing and Distribution, Jordan.
- Anis, A. K. M., & Omar, D. B. (2017). *Risks of using electronic accounting information systems and their impact on audit effectiveness in Algeria*. General framework of the accounting information system, pp. 27–29. <https://journals.qou.edu/index.php/jresstudy/article/view/566>
- Bara, S. (2017). *Cybersecurity in Algeria: Policies and Institutions*. Algerian Journal of Human Security, 2(2). <https://asjp.cerist.dz/en/article/66092>
- Jumaa, A. H. (2010). *Theory of Financial Accounting: The New International Model*. Safaa Publishing and Distribution, Amman.
- Suleiman, M. (2022). Routine Activity Theory: A New Theory for Understanding Cybercrime. *Egyptian Journal of Social and Behavioral Sciences*, 6(6), 114–130. <https://doi.org/10.21608/ejsbs.2022.129409.1005>
- Shalosh, N. (2018). *Electronic piracy in cyberspace: The escalating threat to state security*. Journal of Babylon Center for Human Studies, 8(2), 185–206. <https://bcchj.uobabylon.edu.iq/index.php/bcchj/ar/article/view/438>
- Abdul Razzaq, M. Q. (1998). *Accounting Information Systems*. Dar Al-Thaqafa Publishing and Distribution, Amman, Jordan.
- Ali, Z. A. (2020). *Conflict and Geo-Cybersecurity in the International Arena: A Study in Digital Engagement Strategies*. Amjad Publishing and Distribution, Amman.
- Manasrah, Y. (2018). *Crimes against automated data processing systems*. National Cybersecurity Authority. (2018). *Essential Cybersecurity Controls, Version 1.0*. Riyadh: National Cybersecurity Authority. <https://ega.ec/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf>

٣. المصادر الإنكليزية

- Asiri, M. (2021). *Three essays in investment efficiency, accounting reporting complexity, and cyber security breaches: Evidence from corporate tax avoidance* (Doctoral dissertation). School of Accounting, Curtin University.
- Badawy, H. A. E. S. (2021). *The impact of assurance quality and level on cyber security risk management program on non-professional Egyptian investors' decisions: An experimental study*. *Alexandria Journal of Accounting Research*, 5.
- Gao, L., Calderon, T. G., & Tang, F. (2020). *Public companies' cyber security risk disclosures*. *International Journal of Accounting Information Systems*, 38.