Journal of Risk & Crisis Management (JRCM) • Vol 6, Issue 1 (2025) • P: 25 – 1
https://journals.ajsrp.com/index.php/jrcm
ISSN: 2664-6285 (Online) • ISSN: 2664-6293 (Print)

The Impact of the National Strategy for Cybersecurity in Reducing the Risks of Accounting Information Systems - An Empirical Study on thy Saudi Governmental Sector

Ms. Nahed Abdullah Barasheed *, Dr. Rawya Reda Obaid

King Abdulaziz University | KSA

Received: 23/02/2025

Revised: 08/03/2025

Accepted: 16/03/2025

Published: 30/03/2025

* Corresponding author: nahed.barashed@gmail.com

Citation: Barasheed, N. A., & Obaid, R. R. (2025). The Impact of the National Strategy for Cybersecurity in Reducing the Risks of Accounting Information Systems - An Empirical Study on thy Saudi Governmental Sector. *Journal of Risk and Crisis Management, 6*(1), 1 – 25. https://doi.org/10.26389/AJSRP.B260225

Abstract: The primary objective of this study is to assess the impact of implementing the National Cybersecurity Strategy on reducing the risks associated with accounting information systems (AIS) within government sectors in Saudi Arabia. The study focuses on key aspects of this strategy, including protecting AIS, managing, and evaluating their risks, assessing the quality of their outputs, and determining the availability of qualified personnel to apply cybersecurity strategies to AIS in the Saudi government sector. The study relied on the inductive approach in preparing the theoretical part, where topics and studies related to the research topic were reviewed and analyzed to form the theoretical framework. Meanwhile, the descriptive analytical approach was adopted in the practical aspect. The study population included (300) participants from accountants, financial analysts, internal and external auditors, and specialists in the field of information technology and cybersecurity in a number of government sectors in Saudi Arabia. The results indicated a statistically significant relationship between the studied elements, demonstrating a positive effect of the National Cybersecurity Strategy on protecting accounting information, managing, and assessing risks, and improving the quality of accounting information outputs, contingent upon the availability of qualified personnel to implement the strategy. Consequently, the study confirms that the impact of the National Cybersecurity Strategy on reducing AIS-related risks is a pivotal aspect in Saudi government sectors, given the critical role of accounting information in governance and effective management. The study recommends several measures, including regular training sessions for government employees on the importance of cybersecurity and risk management, investment in the latest cybersecurity technologies to protect AIS from attacks, the establishment of strict and clear security policies that are regularly reviewed to keep pace with cybersecurity developments, and leveraging international expertise and knowledge exchange to adopt best practices in cybersecurity.

Keywords: Cyber Security, Accounting Information Systems, Information Protection, Risk

أثر الاستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية – دراسة ميدانية على القطاعات الحكومية السعودية

أ. ناهد عبد الله بارشيد*، الدكتورة / راوية رضا عبيد

جامعة الملك عبد العزيز | المملكة العربية السعودية

المستخلص: إن الهدف الرئيسي من هذه الدراسة الحالية هو تقييم أثر تطبيق الاستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية في دراسة ميدانية على القطاعات الحكومية في المملكة العربية السعودية. وتتضمن أهم محاور هذه الاستراتيجية حماية نظم المعلومات المحاسبية وتقييم جودة مخرجاتها ومعرفة مدى توفر الكوادر البشرية المؤهلة لتطبيق الاستراتيجية الوطنية للأمن السيبراني على نظم المعلومات المحاسبية في القطاع الحكومي في المملكة العربية السعودية. اعتمدت الدراسة على المنهج الاستقرائي في إعداد الجزء النظري، حيث تم استعراض وتحليل المواضيع والدراسات المتعلقة بموضوع البحث لتكوين الإطار النظري. في حين، اعتمدت المنهج الوصفي التحليلي في الجانب العملي. وقد شمل مجتمع الدراسة (300) مشاركاً من محاسبي ومراقبي الحسابات والمراجعين الداخليين والخارجيين والمختصون في مجال تقنية المعلومات والأمن السيبراني في عدد من القطاعات الحكومية في المملكة العربية السعودية. وقد أظهرت النتائج وجود علاقة إحصائية بين العناصر المدروسة وتبين أن هناك تأثيراً إيجابياً للاستراتيجية الوطنية للأمن السيبراني على حماية المعلومات المحاسبية وجودة مخرجات المعلومات المحاسبية في ظل توافر الكوادر البشرية المؤهلة لتنفيذ هذه الاستراتيجية. وبالتالي، تؤكد هذه الدراسة أن تأثير الاستراتيجية الوطنية للأمن السيبراني على التقليل من المخاطر المتعلقة بنظم المعلومات المحاسبية يعتبر جانباً محوريًا في القطاعات الحكومية السعودية نظرًا للدور الحيوي الذي تلعبه المعلومات المحاسبية في الحوكمة والإدارة الفعالة. وقد اوصت الدراسة بعدد من التوصيات تتمثل في إجراء دورات تدريبية دورية لموظفي القطاع الحكومي حول أهمية الأمن السيبراني وكيفية التعامل مع المخاطر والاستثمار في أحدث تقنيات الأمن السيبراني لحماية نظم المعلومات المحاسبية من الهجمات ووضع سياسات أمنية صارمة وواضحة ومراجعتها بانتظام لمواكبة التطورات في مجال الأمن السيبراني والاستفادة من الخبرات الدولية وتبادل المعرفة وأفضل الممارسات في مجال الأمن السيبراني.

الكلمات المفتاحية: الامن السيبراني، نظم المعلومات المحاسبية، حماية المعلومات، المخاطر.

1-1 المقدمة

لقد أحدثت التطورات الحديثة في تقنية المعلومات تغيرات مطردة في العديد من القطاعات المالية والإدارية، وأصبح توظيف التقنية في العديد من المنظمات والقطاعات الحكومية جانباً هاماً في إنجاز المهام والأعمال الموكلة إليها. كما أصبح استخدام تقنية المعلومات في العديد من القطاعات مؤشراً رئيسياً على التحول الرقمي، والذي يهدف إلى تحسين الكفاءة وتقليل التكاليف وتطوير أساليب الإنتاج والتوزيع (Cascio & Montealegre, 2016). ورغم الفوائد العديدة لهذه التطورات، إلا أنها تحمل في طياتها العديد من المخاطر والتهديدات، لا سيما المخاطر الأمنية التي تهدد المعلومات والنظم المعلوماتية وبشكل خاص نظم المعلومات المحاسبية. وقد أدت هذه التطورات الى ظهور مفاهيم جديدة لا غنى عنها في تحسين جودة الخدمات والأعمال، من بينها مفهوم الأمن السيبراني الذي يلعب دوراً حيوياً في حماية البيانات والأصول الإلكترونية، وحماية الأنظمة المالية من الهجمات الإلكترونية والقرصنة والتعطيل (بوقرة، 2104). ونظراً لتطور تقنيات الاختراق والتعرض المتواصل للهجمات الإلكترونية، وعدم مواكبة الممارسات والضوابط الرقابية لهذه التطورات، وافتقار الكوادر العاملة للمعرفة والخبرة الكافية، فقد أدت هذه العوامل الى ضرورة وجود نظام متكامل يعمل على حماية هذه الأنظمة ويحافظ على سرية معلوماتها (Samimi, 2020). لذا، تعمل العديد من القطاعات الحكومية في المملكة العربية السعودية على تطوير وتوظيف النظم والبرامج المحاسبية الحديثة التي تتناسب مع أعمالها، وتطبيق استراتيجية الأمن السيبراني في قطاعاتها الإدارية، وتحديداً في إداراتها المالية والمحاسبية، بما يتوافق مع رؤية المملكة 2030، بهدف حماية البيانات والحد من المخاطر التي تتعرض لها الأنظمة المحاسبية المستخدمة في هذه الإدارات (العلمي، 2015). ويمكن ربط الأمن السيبراني بنظم المعلومات المحاسبية من خلال مجموعة من الوسائل والآليات التي تندرج تحت مظلة استراتيجية الأمن السيبراني، ويمكن الاستعانة بها لتعزيز أمن المعلومات المحاسبية، حيث يمكن تحديد هذه الوسائل والآليات ضمن إطار استراتيجي شامل يتضمن معايير وعمليات وضوابط ومسؤوليات محددة. ويهدف هذا الإطار الاستراتيجي إلى إنشاء وتنظيم وتخزين وصيانة واستخدام وحذف المعلومات بطريقة تتوافق مع الأهداف التنظيمية العامة. كما تجسد هذه الاستراتيجية الاستفادة الفعّالة والمؤثرة للمعلومات لمساعدة المنظمة في تحقيق أهدافها (المري ،2023).

2-1 مشكلة الدراسة

في ظل النمو المتسارع في مجال تقنية المعلومات واعتماد اغلب القطاعات الحكومية على النظم المعلوماتية الحديثة، وتحديداً نظم المعلومات المحاسبية، وحماية هذه الأنظمة من الهجمات الالكترونية وعمليات الاختراق المتواصلة (سامح واخرون،2014)، والتي من شأنها أن تسهم اسهاماً مؤثراً في التنمية والتطوير وفي تعزيز جودة الخدمات، وتعزيز مبدأ التكامل في الخدمات المالية والمحاسبية، وترفع من الكفاءة التطويرية لمنسوبي القطاعات الحكومية. وكذلك دورها البارز في معالجة العديد من التحديات التي تواجه هذه القطاعات، وفي إدارة الأزمات، وحل الإشكاليات المتعلقة بالقصور في إيصال الخدمات الحكومية للعديد من المستفيدين، أصبح تعزيز الإجراءات الرقابية وتطبيق الاستراتيجية الوطنية للأمن السيبراني ضرورة ملحة لتعزيز كفاءة الأداء الحكومي في حماية البيانات الحكومية (كمال، 2021). لذا، ستتناول هذه الدراسة جانباً هاماً من جوانب تطبيق الاستراتيجية الوطنية للأمن السيبراني ومدى أهميتها في الحد من مخاطر نظم المعلومات المحاسبية، في محاولة للإجابة على التساؤل التالي: ما أثر الاستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية؟

3-1 أهداف الدراسة

تهدف الدراسة الحالية الى تقييم أثر تطبيق الاستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية في دراسة ميدانية على القطاعات الحكومية في المملكة العربية السعودية، والذي سيتم تحقيقه من خلال الأهداف الفرعية التالية:

- تحديد أثر تطبيق الاستراتيجية الوطنية للأمن السيبراني في حماية نظم المعلومات المحاسبية في القطاع الحكومي في المملكة العربية السعودية.
- تقييم مدى أثر تطبيق الاستراتيجية الوطنية للأمن السيبراني في جودة مخرجات نظم المعلومات المحاسبية المقدمة في القطاع الحكومي في المملكة العربية السعودية.
- معرفة مدى توفر الكوادر البشرية المؤهلة لتطبيق الاستراتيجية الوطنية للأمن السيبراني على نظم المعلومات المحاسبية في القطاع الحكومي في المملكة العربية السعودية.

4-1 فروض الدراسة

في ضوء مشكلة الدراسة وأهدافها تم صياغة الفرض الرئيس التالي:

- توجد علاقة ذات دلالة إحصائية بين تطبيق الاستراتيجية الوطنية للأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية.

ويندرج تحت هذا الفرض مجموعة من الفروض الفرعية التالية:

1. توجد علاقة ذات دلالة إحصائية بين حماية المعلومات المحاسبي والحد من مخاطر نظم المعلومات المحاسبية.
2. توجد علاقة ذات دلالة إحصائية بين جودة مخرجات نظم المعلومات المحاسبة والحد من مخاطر نظم المعلومات المحاسبية.
3. توجد فروق ذات دلالة إحصائية بين كفاءة الكوادر البشرية في تطبيق الاستراتيجية الوطنية للأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية وفقاً لمتغير (الخبرة).

2- الإطار النظري للدراسة

2-1-1الأمن السيبراني

يعتبر الأمن السيبراني عنصرًا حيويًا في حماية البيانات والأنظمة الرقمية وضمان استدامة الأعمال والخدمات الحيوية. يجب على الشركات والأفراد الاستثمار في استراتيجيات الأمن السيبراني للحفاظ على سلامة معلوماتهم ومصالحهم. إن الأمن السيبراني ليس مجرد تحديات فقط، بل هو أيضًا استراتيجية لمواجهة أنواع مختلفة من الجرائم السيبرانية، وهو يشمل تنفيذ استراتيجيات وتدابير للحماية من هذه الجرائم السيبرانية ومنعها (المنيع،2022). وهناك العديد من التعاريف للأمن السيبراني، فقد عرفه Amoroso (2006)، بأنه "وسيلة للحد من مخاطر الهجوم على البرامج أو أجهزة الكمبيوتر أو الشبكات، بما في ذلك الأدوات المستخدمة لمكافحة القرصنة، واكتشاف الفيروسات وحظرها، وتوفير اتصالات مشفرة." كما يُعرف الأمن السيبراني بأنه حماية الأنظمة والشبكات والبرامج وأصول المنشأة من الهجمات والحوادث الإلكترونية التي يمكن أن تؤثر على أداء عملها بشكل فعال وكفء وذلك من أجل تحقيق أهداف الحفاظ على سرية المعلومات وسلامتها وتوافرها (محمود على وآخرون، 2022م)، ويعرفه التيماني (2021) بأنه الحماية الشاملة للأشياء من خلال أمن المعلومات والتكنولوجيا حيث يركز على الحماية والاستخدام غير القانوني وغير المنظم للمعلومات الإلكترونية.

وللأمن السيبراني العديد من الأنواع حيث تشمل مجموعة واسعة من الجوانب المختلفة، ومن بين هذه الأنواع امن الشبكات وامن التطبيقات وامن انترنت الأشياء وامن المستخدم النهائي وامن البنية التحتية.

ويرتبط مفهوم الأمن السيبراني بعدة أهداف للأمن السيبراني، يمكن توضيحها كما يلي: (شلوش، 2018).

1. حماية البيانات :ويعني حفظ سرية وسلامة البيانات، بهدف منع الوصول غير المصرح به والسرقة والتلاعب بالبيانات.
2. ضمان التوافر :ويعني ضمان أن الأنظمة الرقمية متاحة للاستخدام عند الحاجة دون تعطل.
3. الكشف عن التهديدات :ويتمثل في القدرة على اكتشاف الأنشطة الضارة والهجمات بسرعة وفعالية.
4. الاستجابة للهجمات :يتعامل هذا الهدف مع الاستجابة السريعة للهجمات السيبرانية للحد من التأثيرات واستعادة السيطرة.
5. الوقاية والتعزيز :الهدف هو تحسين الأمان السيبراني من خلال تحديث وتعزيز أنظمة المعلومات وتنفيذ ممارسات أمان جيدة.
6. الامتثال والتشريعات :ويعني امتثال المؤسسات للقوانين واللوائح المتعلقة بالأمن السيبراني.
7. التعاون والتحالفات :يشير هذا الهدف إلى أهمية التعاون بين الدول والمؤسسات لمواجهة التهديدات السيبرانية.
8. توعية المستخدمين :وبهدف الى التركيز على توعية المستخدمين بمخاطر الأمان السيبراني وتعليمهم كيفية حماية أنفسهم، وعدم تداول كلمات المرور بين الموظفين حتى لا تحدث اختراقات لنظم المعلومات المحاسبية (سليمان, 2022).

2-1-2 نظم المعلومات المحاسبية

يعرف نظام المعلومات المحاسبية بأنه: عبارة عن مجموعة من المكونات المادية والبشرية المترابطة التي تعمل على جمع ومعالجة وإدارة ومراقبة البيانات المحاسبية المتعلقة بالتعاملات المالية الداخلية والخارجية وفقًا لقواعد وإجراءات محددة تمكن مستخدميها من اتخاذ القرارات والخطط والضوابط المناسبة (الخميني ،2014). ومما سبق يمكن القول وبالاتفاق مع أهداف الدراسة الحالية، ان نظام المعلومات المحاسبية هو نظام متكامل يستخدم في مجال المحاسبة وإدارة الأعمال لجمع وتخزين ومعالجة وتقديم المعلومات المالية والمحاسبية التي تساعد في اتخاذ القرارات وإدارة الموارد المالية بكفاءة. يعتمد هذا النظام على مجموعة من البرامج والإجراءات التقنية والإدارية التي تمكن الشركات والمؤسسات من تنظيم وتسجيل أنشطتها المالية وإنشاء تقارير مالية دقيقة ومفهومة.

2-1-3 المخاطر التي تواجه نظم المعلومات المحاسبية وأسباب حدوثها

لقد تم تحديد أهم هذه المخاطر وتصنيفها حسب التالي (البحيصي والشريف،2008)، الكوارث الطبيعية، والاختراقات البشرية المقصودة، والأعطال والمشاكل الفنية في البرامج والأجهزة، وخطر إتلاف وسائط التخزين أو فقدان البرامج، وخطر الإصابة بالفيروسات او تهكير النظام، أو حدوث أخطاء من المستخدمين.

4-1-2 تقييم مخاطر نظم المعلومات المحاسبية

تعتبر نظم المعلومات المحاسبية من النظم التي تواجه العديد من المخاطر التي قد تؤثر على تحقيق أهداف تلك النظم وذلك نظرا لاعتمادها على الحاسوب، حيث تزامن التطور الكبير للحاسبات وأنظمة المعلومات مع التطور في تكنولوجيا المعلومات وسرعة انتشار هذه المعلومات واستخدامها إلكترونيا، 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. 2018).. وتقسم المخاطر من حيث الأثر إلى ما يلي: (احمد، 2022).

1. مخاطر شديدة الأثر وهي المخاطر التي تكون آثارها كبيرة وينتج عنها خسائر كبيرة قد تفوق قدرة المنشأة على التحمل مما قد يؤدي إلى الانهيار.
2. مخاطر متوسطة الأثر.
3. مخاطر قليلة الأثر

ينطبق هذا التصنيف على احتمالية وقوع الخطر وتقييم آثاره عند وقوعه. هذا وتقسم 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 تبنى عليها التوقعات وعادة ما تستخدم هذه الأساليب في القطاعات الحكومية والمؤسسات المالية كالبنوك وشركات التأمين أكثر من غيرها (لبحيصي،2016).

5-1-2 حماية نظم المعلومات المحاسبية

تبرز أهمية أمن نظم المعلومات المحاسبية في القطاع الحكومي في العديد من الدول، نظرًا للدور الحيوي الذي تلعبه في تقديم خدمات عامة عالية الجودة للمستفيدين، واسهامها في توفير معلومات دقيقة لمتخذي القرار وتحسين أداء هذه الخدمات وتطويرها وزيادة فعاليتها وكفايتها في القطاع الحكومي. وعلى الرغم من أهميتها، فقد لجأت العديد من هذه القطاعات الحكومية الى تطبيق آليات الحماية بهدف تعزيز أمن أنظمته المحاسبية (القرشي، 2019). تشمل هذه الجهود التحديث الدائم والمستمر من خلال ابتكار او تطوير بعض الإجراءات وربطها باستراتيجيات الأمن السيبراني. كذلك توضيح أهم المهام والمسؤوليات ذات العلاقة بأمن أنظمة المعلومات المحاسبية، إضافة الى انشاء الإدارات المسؤولة عن إدارة المخاطر المرتبطة بأمن المعلومات، حيث يمكن لهذه الوحدات اتخاذ الإجراءات اللازمة لمواجهة تلك المخاطر (Al-Fatlawi et al., 2021).

6-1-2 جودة مخرجات نظم المعلومات المحاسبية

ان مفهوم جودة المعلومات يختلف باختلاف وجهات نظر واهداف منتجي ومستخدمي المعلومات، ففي حين يركز منتج المعلومات عل الدقة كمقياس للجودة يركز مستخدم اخر على المنفعة والفعالية والتنبؤ كمقياس لهذه الجودة مع اغفال التكلفة، ومنه يمكن تعريف جودة المعلومات المحاسبية أنها المعلومات التي تتوفر على خصائص الدقة والكمال، والصحة، والترابط، والانتظام. (قراطم، واخرون، 2022). ولمعرفة مستوى الجودة في المعلومات المحاسبية يمكن التحقق من وجود الخصائص التالية في مخرجات المعلومات المحاسبية: (العطار، 2018).

- القابلية للفهم: اي قابلية البيانات المالية للفهم من قبل المستخدمين وذلك مع افتراض ان لدى المستخدمين مستوى معقول من المعرفة والرغبة في دراسة المعلومات بقدر معقول من العناية، ويجب عدم استبعاد المعلومات حول المسائل المعقدة لملاءمتها لاتخاذ القرارات من قبل المستخدمين المختلفين.
- الملائمة: اي ملائمة البيانات المالية لحاجات متخذي القرارات من خلال أثرها على قرارات المستخدمين، والتنبؤ بقدرة الشركة على استغلال الفرص ومقاومة الأوضاع النسبية المعاكسة، وتتأثر الملائمة بطبيعة المعلومات وأهميتها.
- الموثوقية (المصداقية): اي يجب ان تكون المعلومات دقيقة وخالية من الاخطاء والتحيز، ويمكن ان تكون المعلومات ملائمة، ولكن غير موثوقة، وذلك يعود الى درجة دقة تلك المعلومات وتوقيت اصدارها وتتكون خاصية الموثوقية من عدة خصائص منها: التمثيل الصادق، الحياد، الحذر، الاكتمال.
- القابلية للمقارنة: اي قابلية مقارنة القوائم المالية للشركة مع مرور الزمن لتحديد الاتجاهات في مركزها المالي وفي الاداء، ومقارنة القوائم المالية للشركات المختلفة من اجل اجراء التقييم النسبي لمركزها المالي (إسماعيل ونعوم،2012). وبتوفر الخصائص السابقة، تمتلك المعلومات المحاسبية في النظم المعلومات الجودة والقدرة على تحقيق اهدافها، لكن عدم توفرها يؤدي الى انخفاض تلك الجودة وبالتالي الحد من الاهداف المنتظرة منها وخاصة اتخاذ القرارات.

2-1-7 كفاءة الكوادر البشرية وأهميتها للنظم المحاسبية

ان كفاءة الكوادر البشرية تلعب دورًا محوريًا 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 والمصداقية. هذه النتائج تؤكد أهمية وجود إرشادات وضوابط قوية لضمان جودة المعلومات المحاسبية واستخدام التكنولوجيا بفعالية لتحسين أنظمة المعلومات المحاسبية.

2-1-8 الاستراتيجية الوطنية للأمن السيبراني ودورها في الحد من مخاطر نظم المعلومات المحاسبية

تُعرف إستراتيجية الأمن السيبراني بأنها مجموعة من الخطط والإجراءات والسياسات المصممة لحماية المعلومات والأنظمة الرقمية من التهديدات السيبرانية والهجمات الإلكترونية. والهدف الرئيسي لهذه الاستراتيجية ضمان سرية البيانات، وسلامتها، وتوفير إمكانية الوصول إليها بشكل آمن ومواجهة التهديدات السيبرانية بفعالية. وتعتمد استراتيجية الأمن السيبراني على تحليل البيئة الخاصة بالمؤسسة أو الجهة التي تنفذها. كما تشمل هذه الاستراتيجية تحديد المخاطر المحتملة، وتصميم وتنفيذ سياسات وإجراءات الأمن، وتطوير التكنولوجيا السيبرانية، وتدريب الموظفين، وإدارة الحوادث والتعامل معها، وتقييم الأمان بشكل دوري (الهيئة الوطنية للأمن السيبراني، 2019).

وتتضمن أهم ضوابط استراتيجية الأمن السيبراني تحديد وتوثيق واعتماد إستراتيجية الأمن السيبراني للجهة ودعمها من قبل رئيس الجهة أو من ينيبه، ويشار له في هذه الضوابط باسم (صاحب الصلاحية) وأن تتماشى الاهداف الإستراتيجية للأمن السيبراني للجهة المناط بها تطبيق استراتيجية الأمن السيبراني مع المتطلبات التشريعية والتنظيمية ذات العلاقة. والعمل على تنفيذ خطة عمل لتطبيق إستراتيجية الأمن السيبراني من قبل الجهة .كما يجب مراجعة إستراتيجية الأمن السيبراني على فترات زمنية مخطط لها أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية ذات العلاقة. بالإضافة الى عمل تقييم متكامل للأمن السيبراني، وإدارة فعالة للمخاطر السيبرانية على المستوى الوطني، وحماية الفضاء السيبراني وتعزيز القدرات الوطنية في الدفاع ضد التهديدات السيبرانية، وكذلك تعزيز الشراكات والتعاون في الأمن السيبراني، وبناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة العربية السعودية (الهيئة الوطنية للأمن السيبراني، 2019).

2-1-9 آليات حماية نظم المعلومات المحاسبية وفقاً لاستراتيجية الأمن السيبراني

هناك العديد من الآليات والوسائل التي يمكن الاعتماد عليها في عملية حماية نظم المعلومات المحاسبية ، تعتمد هذه الوسائل على استراتيجية الأمن السيبراني في عملياته، يمكن للقطاعات الحكومية تطبيق واعتماد اجراءاته من خلال استخدام الأجهزة المتطورة والحديثة وتأهيل القوى العاملة في نظم المعلومات المحاسبية من الكوادر الوطنية من ذوي الخبرة والاختصاص، ايضاً ينبغي الفصل بين المهام الإدارية والوظائف المحاسبية بما يسهم في زيادة فعالية أمن المعلومات مع التزام الأقسام المالية والمحاسبية بالمتطلبات التنظيمية لتحقيق الأمن السيبراني الذي من شأنه زيادة كفاءة وجودة مخرجات نظم المعلومات المحاسبية (حمود،2023). اضافةً الى تعزيز ثبات الأساليب والإجراءات المتبعة بالقياس والافصاح عن المعلومات المحاسبية. وكذلك تعزيز مستوى الأمن للمحافظة على امن المعلومات وذلك من خلال تقييم المخاطر بشكل دوري وتحديد مستواها واتخاذ الإجراءات الاستباقية للحيلولة دون حدوث اختراقات (البابلي، 2021). كما ينبغي الاعتماد على البرامج التشغيلية والتطبيقات المحمية التي تمكن المستخدم من تبادل المعلومات المحاسبية مع الجهات الأخرى بطريقة أسرع وأكثر اماناً وتحسين وضبط مستوى الصلاحية للمستخدمين في مثل هذه البرامج بالإضافة الى تعزيز إجراءات الحماية لشبكات المعلومات في الإدارات المختلفة للقطاع.

2-2 الدراسات السابقة

لقد سعت الباحثة جاهدة الى انتقاء الدراسات التي تناولت متغيري الدراسة الحالية، حيث لوحظ قيام العديد من الباحثين بقياس أثر الأمن السيبراني على نوعين من المعلومات، النوع الأول معلومات عامة غير مالية والنوع الثاني المعلومات المالية يتضمن البعض منها نظم معلومات محاسبية. وقد تضمنت أهم هذه الدراسات من الأقدم إلى الأحدث ما يلي:

1. **دراسة (Thuneibat & Kasasbeh , 2018)** ، وهدفت هذه الدراسة الى إيضاح تاريخ الهجمات الإلكترونية التي تعرضت لها المنظمات السعودية وخاصة الجامعات والجاهزية الإلكترونية العامة لهذه المؤسسات. اعتمدت الدراسة على المنهج الوصفي التحليلي، وقد شملت الدراسة 486 مشاركا من ثلاث جامعات مختلفة في المملكة العربية السعودية. وقد أظهرت النتائج أن لعملية التحكم في الولوج للنظام تأثير متوسط الى عالي في العلاقة بين الهجوم من البرامج الضارة وقدرة النظام على صد تلك الهجمات. وقد اوصت الدراسة بضرورة تعزيز قدرات هذه الجامعات تقنياً وبشرياً لمنع مثل هذه الهجمات مستقبلاً، وتوظيف أكبر قدر ممكن من التقنيات التي يتم تطويرها بصورة دورية.

2. **دراسة (Rawas, 2019)** ، وهدفت هذه الدراسة الى الكشف عن الاستراتيجيات السيبرانية المستخدمة لحماية أنظمة المعلومات في المنشآت المالية من التهديدات السيبرانية. وقد اعتمدت الدراسة المنهج الوصفي التحليلي حيث تم جمع البيانات من خلال مقابلات شخصية شبه منظمة مع خمسة قادة من العاملين في منشآت مالية صغيرة في قطر. وتشير نتائج هذه الدراسة إلى أن قادة المؤسسات المالية يحمون أنظمة معلوماتهم من التهديدات السيبرانية من خلال إدارة فعالة لممارسات أمان المعلومات، ووضع سياسات أمان سيبراني قوية، وتحديد، وتقييم، وتخفيف مخاطر الأمان السيبراني، وتنفيذ استراتيجية تنظيمية شاملة. واوصت الدراسة بإجراء المزيد من الدراسات حول عدد من المتغيرات أهمها التهديدات لأمن المعلومات وتكلفة أمن المعلومات، وثقة المستهلك في النظام المالي، وحلول الشبكات الفعالة للحد من التهديدات السيبرانية.
3. **دراسة (Ali, Matarneh, Almalkawi, & Mohamed, 2020)**، وهدفت الدراسة الى تقييم مدى تأثير الحوكمة السيبرانية في تقليل مخاطر المحاسبة السحابية في البنوك التجارية الأردنية. اعتمدت الدراسة على المنهج الوصفي والتحليلي، حيث شمل مجتمع الدراسة (213) مشارك من المحاسبين القانونيين والمدققين العاملين في عدد من البنوك الأردنية. وتوصلت الدراسة إلى عدة نتائج كان أهمها وجود تأثير ذو دلالة إحصائية لحوكمة الأمن السيبراني (متطلبات حوكمة الأمن السيبراني، برنامج الأمن السيبراني، سياسة الأمن السيبراني، إدارة المعلومات السيبرانية، تقييم وإدارة المخاطر السيبرانية) في الحد من مخاطر المحاسبة السحابية في البنوك التجارية الأردنية. واوصت بضرورة قيام البنوك التجارية الأردنية باعتماد الحوكمة السيبرانية كمرجع أساسي لسياستها المصرفية لمواجهة المخاطر المرتبطة باستخدام المحاسبة السحابية.
4. **دراسة (السرحان، واخرون، 2020)**، وهدفت هذه الدراسة إلى معرفة أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية، كدراسة تطبيقية على عدد من البنوك التجارية الأردنية، حيث اعتمد الباحث على المنهج الوصفي التحليلي واستخدم الاستبانة كأداة لجمع البيانات. وقد تم توزيع هذه الاستبانة على 130 مشاركاً من المدققين الداخليين ومدققي ومحللي الأنظمة وامن المعلومات العاملين في تلك البنوك. وقد خلصت الدراسة الى وجود أثر لخصوصية بيانات العملاء وإدارة المخاطر السيبرانية وتحديد الجهة المالكة ونطاق التطبيق والصلاحيات على جودة المعلومات المحاسبية. وأوصت الدراسة بضرورة زيادة الاهتمام بالحفاظ على خصوصية بيانات العملاء لتعزيز جودة المعلومات المحاسبية.
5. **دراسة (Almomani, et al, 2021)**، وهدفت هذه الدراسة إلى التحقق من مدى تأثير كفاءة وفعالية الأمن السيبراني على المعلومات المحاسبية السحابية في الشركات الأردنية المساهمة العامة من وجهة نظر الأساتذة والمديرين في مجال أمن المعلومات. اعتمدت الدراسة على المنهج الوصفي التحليلي في إتمام إجراءات الدراسة، وكانت الاستبانة هي أداة الدراسة. وقد تم توزيع هذه الاستبانة على 125 أستاذاً و75 مديراً لأمن المعلومات. توصلت الدراسة الى عدد من النتائج أهمها وجود تأثير كبير لفعالية وكفاءة الأمن السيبراني على المعلومات المحاسبية السحابية. وقد اوصت الدراسة بضرورة تعزيز دور الأمن السيبراني في معظم الشركات من أجل الحفاظ على المعلومات المحاسبية السحابية. كما اوصت بضرورة معالجة المخاطر المتعلقة بالتكنو لوجيا المالية والأمن السيبراني من خلال الإدارة السليمة للمخاطر الداخلية.
6. **دراسة (Ehioghiren,et al., 2021)**، وهدفت هذه الدراسة الى تقييم أثر الأمن السيبراني، من وجهة نظر مختصي المحاسبة في نيجيريا. اعتمدت هذه الدراسة على المنهج الوصفي التحليلي حيث شملت عينة الدراسة 160 مشاركًا من مديري التدقيق، ومديري الضرائب، ومساعدي الممارسين، والمحاسبين الماليين الممارسين، والمحاسبين الإداريين، والمدققين الداخليين العاملين في الشركات النيجيرية. وقد أظهرت الدراسة أن محترفي المحاسبة في نيجيريا يمتلكون معرفة عالية في مجال الأمن السيبراني والحوادث المتعلقة به. وأوصت الدراسة بأن يعمل جميع أصحاب المصلحة على وضع المزيد من السياسات المتعلقة بإطار الأمن السيبراني لحماية وتنظيم الأنشطة في الفضاء السيبراني.
7. **دراسة (خليفات والقضاة ،2021)** ، وهدفت الدراسة للتعرف إلى أثر سياسات تدقيق أمن المعلومات بأبعادها (صلاحية النظام، وواجبات فريق التدقيق، وتقارير نظام التدقيق الداخلي، والتوثيق والأدلة، وميثاق السلوك الخاص بتدقيق أمن المعلومات (في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية بأبعادها (مخاطر الإدخال، ومخاطر التشغيل، ومخاطر المخرجات، ومخاطر بيئية (في المؤسسات الحكومية المستقلة الأردنية. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي. حيث تكون مجتمع الدراسة من جميع المؤسسات الحكومية المستقلة الأردنية والبالغ عددها (28) مؤسسة حكومية، وبلغ عدد العينة (297) مشارك. وقد توصلت الدراسة إلى وجود أثر ذو دلالة إحصائية عند مستوى الدالة ($\alpha \leq 0.05$)، لإتباع سياسات تدقيق أمن المعلومات بأبعادها في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية في المؤسسات الحكومية المستقلة الأردنية، واوصت الدراسة بضرورة إخضاع مستخدمي نظم المعلومات المحاسبية الإلكترونية إلى محاضرات إرشادية وبشكل مستمر حول كيفية استخدام النظام والمحافظة على صلاحيته.

8. **دراسة (العوامري، واخرون 2022)**، وهدفت الدراسة إلى استكشاف أثر تكامل الأمن السيبراني وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية؛ وذلك بغرض زيادة الموثوقية، والمصداقية في نظم المعلومات المحاسبية الإلكترونية ومخرجاته. واعتمد البحث على المنهج الوصفي التحليلي. وشملت عينة الدراسة 52 مفردة من أعضاء هيئة التدريس تخصص المحاسبة والمراجعة ببعض كليات التجارة بالجامعات المصرية. وخلصت الدراسة الى تعرض نظم المعلومات المحاسبية للعديد من المخاطر يتمثل أهمها في المخاطر الداخلية. وأوصى الباحث بضرورة اهتمام المنظمات والهيئات المهنية المعنية بالمواكبة مع التطور التكنولوجي بعقد الدورات التدريبية لرفع ثقافة إدارة المخاطر، والتدريب على أحدث الممارسات العلمية والعملية المطبقة في هذا المجال.

2-2-1التعقيب على الدراسات السابقة

لقد أسهمت مراجعة الدراسات السابقة بشكل كبير في تمكين الباحثة من تحديد وصياغة أهداف الدراسة ومشكلتها وفرضياتها. كما ساعدت في تحديد المنهجية والأدوات المناسبة لجمع البيانات، وبناء الإطار النظري، وتحليل وتفسير نتائج الدراسة. بالإضافة إلى ذلك، ساعدت في إعداد أداة الدراسة (الاستبيان) وتقديم التوصيات . ويمكن القول انه اتفقت الدراسة الحالية ومعظم الدراسات السابقة، على أهمية تطبيق الأمن السيبراني ومدى تأثيره على كفاءة وفعالية أمن المعلومات. وتشير معظم هذه الدراسات، إن لم يكن جميعها، إلى الحاجة الماسة لوجود خدمات جديدة تساهم في تقييم الضوابط المتعلقة بالأمن، والتوافر، وتكامل وسلامة التشغيل، وسرية وخصوصية المعلومات المالية والمحاسبية. كما تتفق الدراسات أيضاً على أهمية نظم المعلومات المحاسبية الإلكترونية والحاجة إليها، خاصة فيما يتعلق بضرورة تطوير منهج متكامل لإدارة أمن المعلومات من خلال تقييم التكنولوجيا المستخدمة، وتقييم سلوكيات الأفراد، والاهتمام بالجوانب التنظيمية، وهو ما يمثل أحد أهم أبعاد المشكلة..

ومع ذلك، تتجلى أوجه الاختلاف بين الدراسة الحالية والدراسات السابقة في مجال التطبيق، حيث سيتم تطبيق هذه الدراسة على عدد من القطاعات الحكومية في المملكة العربية السعودية في حين طبقت معظم الدراسات السابقة على القطاع المصرفي (كدراسة (Ali, Matarneh, Almalkawi, & Mohamed, 2020)، باستثناء دراسة (خليفات والقضاة ،2021)، التي طبقت على المؤسسات الحكومية الأردنية. كما ستقوم هذه الدراسة بتقييم أثر تطبيق استراتيجية الأمن السيبراني في الحد من المخاطر التي تهدد أنظمة المعلومات المحاسبية في عدد من القطاعات الحكومية، من حيث طرق تعزيز حماية المعلومات، وتقييم وإدارة مخاطر نظم المعلومات المحاسبية، وجودة مخرجات نظم المعلومات المحاسبية، ومدى توفر الكوادر البشرية المؤهلة لتطبيق وتنفيذ استراتيجية الأمن السيبراني.

وقد لوحظ من خلال استعراض الدراسات السابقة - حسب علم الباحثة- ندرة في الدراسات التي تناولت تقييم أثر الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية في القطاعات العامة، رغم اتفاق بعضها من حيث الهدف والمنهجية إلا أن هذه الدراسات كانت في دول أخرى باستثناء دراسة (Kasasbeh & Thuneibat 2018) التي طبقت على الجامعات السعودية، وعلى فترات زمنية مختلفة. وتعتبر هذه الدراسة إلى حد ما الدراسة الأولى التي سيتم تطبيقها بالمملكة العربية السعودية، وتحديداً على القطاع الحكومي، وهي امتداداً للجهود السابقة المقدمة من المهتمين والباحثين في هذا المجال، ومع ذلك، هناك حاجة الى اجراء المزيد من الابحاث والدراسات بهدف إحداث نوع من التكامل بين هذه الدراسات، والتركيز على استراتيجية الأمن السيبراني ودورها في الحد من مخاطر نظم المعلومات المحاسبية في ظل مساعي الحكومة لتعزيز الأمن السيبراني في قطاعاتها المختلفة.

3- منهجية الدراسة وإجراءاتها

1-3 منهج الدراسة

اتبعت الدراسة المنهج الاستقرائي حيث تم استعراض وتحليل المواضيع والدراسات المتعلقة بموضوع البحث لتكوين الإطار النظري. في حين، اعتمدت المنهج الوصفي التحليلي في الجانب العملي، وقد تم جمع كافة البيانات اللازمة لتحقيق أهداف الدراسة من خلال مصادر ثانوية متمثلة في المراجع والدوريات العلمية والبحوث والدراسات السابقة ومصادر أولية من خلال الاستعانة بالاستبانة لجمع البيانات وذلك لمناسبته لأغراض هذه الدراسة.

2-3 مجتمع وعينة الدراسة

اشتمل مجتمع الدراسة على جميع القطاعات الحكومية في المملكة العربية السعودية، وتم اختيار العينة عشوائياً وذلك من توزيع الاستبانة على (300) مشارك من محاسبي ومراقبي الحسابات والمراجعين الداخليين والخارجيين والمختصين في مجال تقنية المعلومات والأمن السيبراني في عدد من القطاعات الحكومية في المملكة العربية السعودية، حيث تم اختيارهم بناء على اختصاصهم في مجال المحاسبة وتقنية المعلومات بالإضافة الى عملهم في القطاع الحكومي.

3-3 أدوات الدراسة

اعتمدت الباحثة على الاستبانة كأداة أساسية في عملية جمع البيانات المطلوبة ودعم الدراسة النظرية بالجانب التطبيقي، حيث تعد الاستبانة من أكثر الوسائل استخداما للحصول على المعلومات والبيانات من افراد الدراسة (سعد، 2018). وقد قامت الباحثة ببناء الاستبانة وتطويرها وذلك بعد الاطلاع على الدراسات السابقة المتعلقة بموضوع الدراسة ذلك لتشمل محوريين أساسيين:

- المحور الأول: تطبيق الاستراتيجية الوطنية للأمن السيبراني
  - البعد الأول: أثر الاستراتيجية الوطنية للأمن السيبراني في تعزيز حماية المعلومات في نظم المعلومات المحاسبية.
  - البعد الثاني: أثر الاستراتيجية الوطنية للأمن السيبراني في رفع مستوى جودة مخرجات نظم المعلومات المحاسبية:
  - البعد الثالث: مدى توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني على نظم المعلومات المحاسبية.
- المحور الثاني: الحد من مخاطر نظم المعلومات المحاسبية

3-3-1صدق أداة الدراسة

للتأكد من صدق أداة الدراسة، اعتمدت الباحثة على طريقتين رئيسيتين. الأولى هي الصدق الظاهري، حيث تم عرض الأداة (الاستبانة) على مجموعة من الخبراء والمختصين في المجال للحصول على آرائهم حول ملاءمة وموثوقية الأسئلة. أما الطريقة الثانية فهي صدق الاتساق الداخلي، والذي يتم تقييمه من خلال حساب معامل الارتباط بين كل وحدة من وحدات الأداء والأداء الكلي للأداة. هذه الخطوات ضرورية لضمان أن الأداة المستخدمة في الدراسة تتمتع بدرجة عالية من الصدق والموثوقية (حسين، 2020).

جدول (1) قيم معاملات الارتباط (بيرسون) لعبارات المحاور الأساسية

المحور الأول: تطبيق الاستراتيجية الوطنية للأمن السيبراني						المحور الثاني: الحد من مخاطر نظم المعلومات المحاسبية:	
البعد الأول: تعزيز حماية المعلومات في نظم المعلومات المحاسبية		البعد الثاني: جودة مخرجات نظم المعلومات المحاسبية:		البعد الثالث: توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني على نظم المعلومات المحاسبية			
تسلسل	بيرسون	تسلسل	بيرسون	تسلسل	بيرسون	تسلسل	بيرسون
1	0.815**	11	0.359*	21	0.288*	31	0.728**
2	0.748**	12	0.428**	22	0.525**	32	0.635**
3	0.636**	13	0.396**	23	0.599**	33	0.468**
4	0.567**	14	0.597**	24	0.469**	34	0.723**
5	0.596**	15	0.736**	25	0.713**	35	0.630**
6	0.570**	16	0.763**	26	0.900**	36	0.607**
7	0.846**	17	0.749**	27	0.773**	37	0.665**
8	0.822**	18	0.728**	28	0.533**	38	0.477**
9	0.797**	19	0.865**	29	0.567**	39	0.426**
10	0.900**	20	0.701**	30	0.728**	40	0.426**
** دالة عند مستوى دلالة 0.001							

يتضح من نتائج اختبار قيم ارتباط بيرسون (جدول1) ما يلي:

أن معاملات ارتباط بيرسون بين عبارات الابعاد والدرجة الكلية موجبة تراوحت بين (0359: 0,900) وهي قيم مرتفعة وأكبر من القيم الجدولية عند مستوى دلالة (0.001)، مما يدل على درجة عالية من الاتساق الداخلي للاستبانة.

بمعنى آخر، يشير الاتساق الداخلي العالي إلى أن عناصر الاستبيان المختلفة مرتبطة ارتباطاً وثيقاً ببعضها البعض، مما يؤكد موثوقية الاستبيان وصلاحيته من حيث جمع البيانات وتحليلها.

كما تم احتساب معاملات الارتباط بين درجة كل محور والدرجة الكلية للاستبانة كما ورد في الجدول ادناه:

جدول (2) قيم معاملات الارتباط (بيرسون) بين درجات المحاوردرجة الاستبانة الإجمالية

البعد	عدد الفقرات	معامل ارتباط بيرسون
البعد الأول: تعزيز حماية المعلومات في نظم المعلومات المحاسبية	10	0.881**
البعد الثاني: جودة مخرجات نظم المعلومات المحاسبية:	10	0.757**
البعد الثالث: توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني على نظم المعلومات المحاسبية	10	0.488**
المحور الثاني: الحد من مخاطر نظم المعلومات المحاسبية	10	**0.875
** دالة عند مستوى دلالة 0.001		

يتضح من نتائج اختبار قيم ارتباط بيرسون (جدول2) أن معاملات ارتباط بيرسون بين درجات المحاور ودرجة الاستبانة الإجمالية موجبة تراوحت بين (0,488: 0,881) وهي قيم مرتفعة وأكبر من القيم الجدولية عند مستوى دلالة (0.001)، مما يدل على درجة عالية من الاتساق الداخلي بين عبارات محاور الدراسة مع الدرجة الكلية.

3-3-2 ثبات أداة الدراسة

يعتبر ثبات الأداة من العوامل الأساسية والضرورية في البحث العلمي، حيث يؤثر بشكل كبير على نتائج الدراسة وصحة الاستنتاجات. فإذا كانت الأداة غير ثابتة، فإنه من المحتمل أن يؤدي ذلك إلى تشوه في البيانات وتداخل في النتائج. وبالتالي، فإن تحقيق الهدف الرئيسي للبحث العلمي يعتمد بشكل كبير على ثبات الأداة. وللتحقق من ثبات أداة الاستبانة، تم استخدام اختبار ألفا كرونباخ، وذلك لقياس قيمة معاملات الثبات لكل جزء من أجزاء الاستبانة (زارع، 2021).

جدول (3) نتائج اختبار معامل الثبات ألفا كرونباخ

المحور	عدد العبارات	معامل الثبات
المحور الأول: تطبيق الاستراتيجية الوطنية للأمن السيبراني البعد الأول: تعزيز حماية المعلومات في نظم المعلومات المحاسبية	10	0.841
البعد الثاني: جودة مخرجات نظم المعلومات المحاسبية	10	0.962
البعد الثالث: توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني	10	0.891
المحور الثاني: الحد من مخاطر نظم المعلومات المحاسبية	10	0.881
معامل الثبات للدراسة ككل	40	0.893

يتضح من نتائج اختبار معامل الثبات ألفا كرونباخ (جدول3) أن قيم معاملات الثبات لمحاور الاستبانة جاءت جميعها بقيم مرتفعة حيث تتراوح بين (0.841-0.962)، إذ بلغ معامل الثبات الكلي للاستبانة (0.893) مما يعني أن الاستبانة بكافة محاورها تحقق درجة كبيرة من الثبات. وفي ضوء ما تقدم يتضح أن هذه القيم العالية من معاملات الثبات إلى كون الاستبانة تتمتع بدرجة عالية من الصدق والثبات، ومن ثم صلاحيتها للتطبيق الميداني، وإمكانية الاعتماد على نتائجها والوثوق بها.

3-4 الأساليب الاحصائية المستخدمة

اعتمدت الدراسة على الأساليب الإحصائية بناءً على طبيعة الدراسة، والأهداف التي سعت إلى تحقيقها وتم تحليل البيانات من خلال أداة الدراسة (الاستبانة). وتم الاستعانة ببرنامج الحزم الإحصائية للعلوم الاجتماعية(SPSS) ، حيث تم استخراج النتائج وفقا للأساليب الإحصائية، المتوسط الحسابي، والانحراف المعياري، والتكرارات والنسب المئوية، ومعامل ارتباط بيرسون، ومعامل ألفا كرونباخ، وتحليل مربع كاي، وأسلوب الانحدار الخطي البسيط، أسلوب الانحدار الخطي المتعدد، ومقياس ليكرت الخماسي.

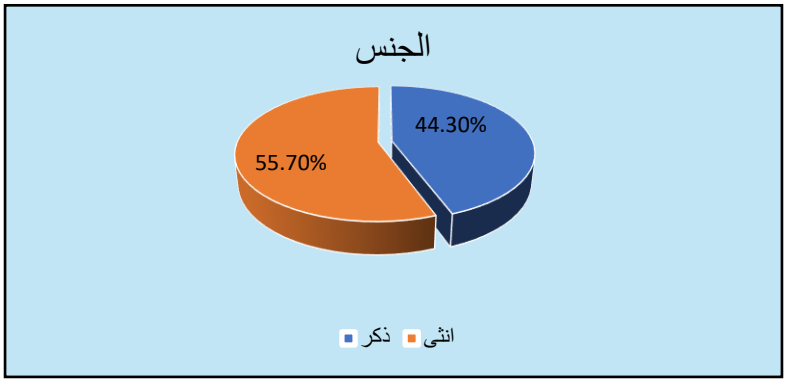
3-5 نتائج الإحصاء الوصفي للدراسة الميدانية

سيتم تحليل البيانات باستخدام أدوات إحصائية وبرامج تحليل البيانات لاستخلاص النتائج الكمية والنوعية. سنركز على تحليل المتغيرات المختلفة المتعلقة بالأمن السيبراني ومخاطر النظم المحاسبية وتفسير العلاقات بينها بشكل دقيق ومنطقي.

3-5-1نتائج الإحصاء الوصفي المتعلقة بالبيانات الأولية

بعد تفريغ البيانات الواردة، تم تحديد خصائص أفراد عينة الدراسة باستخدام النسب المئوية، وكانت النتائج كالتالي:

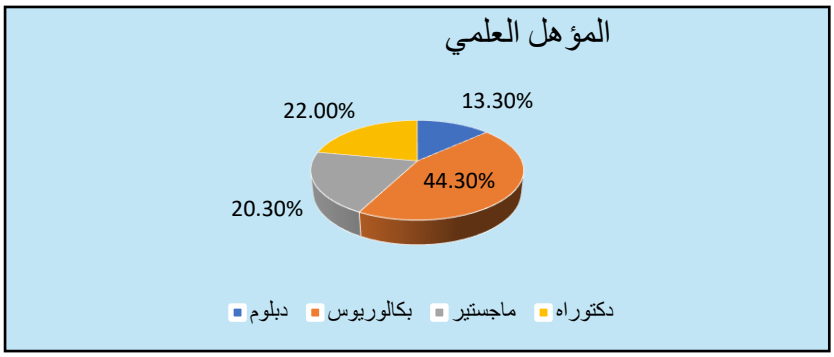
1- توزيع افراد عينة الدراسة وفقاً للجنس



شكل (1) توزيع أفراد عينة الدراسة وفقً للجنس

يتبين من (شكل 3) أن نسبة " الذكور " المشاركين في الدراسة بلغت 44.3% في حين بلغت نسبة "الإناث " 55.7%، ويشير هذا التوزيع إلى وجود تقارب نسبي بين الجنسين، ويساعد على ضمان التمثيل المناسب لكلا الجنسين، مما يساعد على جعل النتائج أكثر تعميمًا واستنتاجًا.

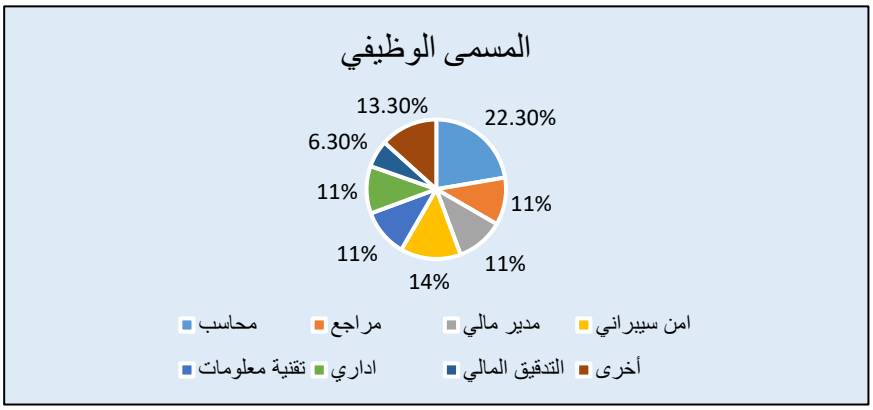
2- توزيع افراد عينة الدراسة وفقاً للمؤهل العلمي



شكل (2) يوضح توزيع عينة الدراسة وفقا للمؤهل العلمي

يتبين من (شكل2) أن نسبة درجة" الدبلوم بلغت " 13.3%، ونسبة درجة "البكالوريوس" 44.3%، في حين بلغت نسبة درجة " الماجستير" 20.3%، ودرجة "الدكتوراه " 22.0%. ويشير هذا الى أن غالبية أفراد العينة من حملة الشهادات الجامعية. وهذا يساعد على فهم أفراد العينة لتساؤلات الدراسة واستيعاب وتحليل المعلومات والحصول على إجابات أكثر دقة.

3- توزيع افراد عينة الدراسة وفقاً للمسمى الوظيفي

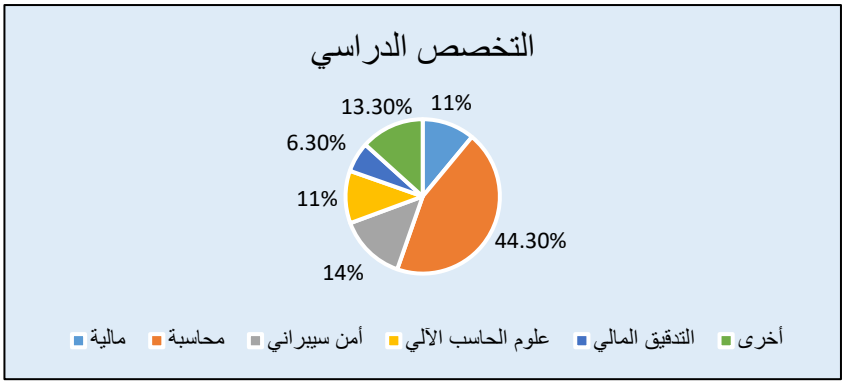


شكل (3) يوضح توزيع عينة الدراسة وفقا للمسمى الوظيفي

من (شكل3) يتبين ان المسمى الوظيفي "محاسب" قد جاء بنسبة مئوية بلغت 22.3%، كما جاء " المدير المالي " بنسبة مئوية بلغت 11.0%، و" الأمن السيبراني " 14.0%، وجاءت " تقنية معلومات " بنسبة مئوية بلغت 11.0%، في حين جاءت الفئات " الأخرى " بنسبة مئوية

بلغت 13.3%. ويضمن هذا التنوع في المسميات الوظيفية تمثيلًا جيدًا للمهن المتعلقة بموضوع الدراسة، وبالتالي، يساعد التوزيع المتنوع للمهن على تغطية جميع جوانب تساؤلات الدراسة بشكل دقيق.

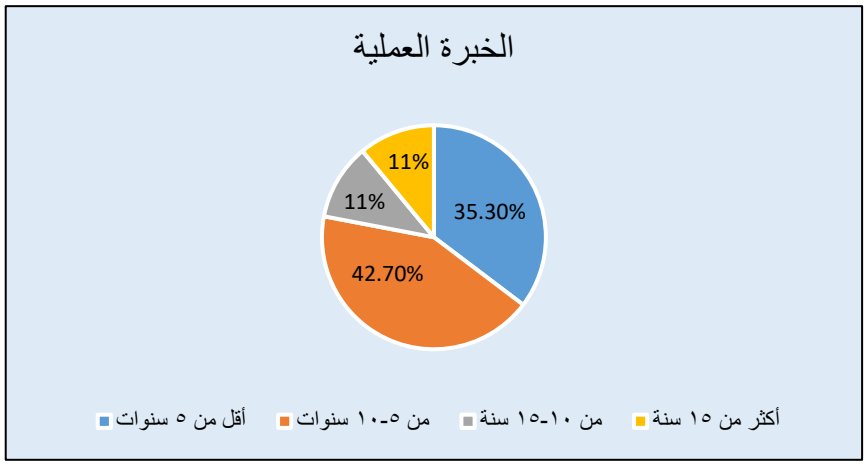
4- توزيع افراد عينة الدراسة وفقاً للتخصص الدراسي



شكل (4) يوضح توزيع عينة الدراسة وفقا للتخصص الدراسي

يتبين من (شكل4) أن تخصص "محاسبة " جاء بأعلى نسبة مئوية بلغت 44.3%، في حين جاء تخصص " الأمن السيبراني " بنسبة مئوية بلغت 14.0%، وجاء تخصص" علوم الحاسب الآلي " بنسبة مئوية بلغت 11.0%. ويمكن القول إن غالبية أفراد عينة الدراسة يحملون تخصص المحاسبة، يليها تخصصات الأمن السيبراني والمالية وعلوم الحاسب الآلي. ويعكس هذا التنوع في التخصصات تنوعًا مهمًا في خلفيات المشاركين، مما يسهم في تحقيق دقة أكبر في النتائج وتحليل البيانات بشكل أفضل.

5- توزيع افراد عينة الدراسة وفقاً للخبرة العملية



شكل (5) يوضح توزيع عينة الدراسة وفقاً للخبرة العملية

يتبين من (شكل5) أن الخبرة العملية للفترة " أقل من 5 سنوات" قد جاءت بنسبة مئوية بلغت 35.3%، وجاءت الخبرة العملية للفترة " من 5-10 سنوات " بأعلى نسبة مئوية بلغت 42.7%، وهذا يدل على أن معظم أفراد العينة يتمتعون بخبرة جيدة. وهذا يساعد في توجيه البحث للحصول على فهم أعمق وبيانات أكثر دقة بناءً على الخبرات العملية العالية.

6- توزيع افراد عينة الدراسة وفقاً للجهة أو القطاع الحكومي

جدول (4) يوضح توزيع عينة الدراسة وفقا للجهة أو القطاع الحكومي

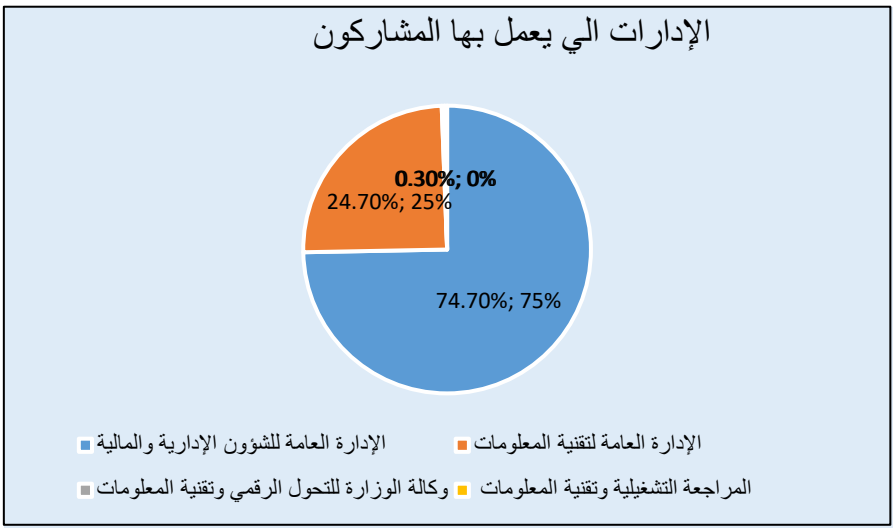
الجهة او القطاع	التكرار	النسبة المئوية
وزارة الاستثمار	10	%3.3
وزارة الشؤون البلدية والقروية	10	%3
وزارة الحرس الوطني	8	%2.7
وزارة الثقافة السعودية	9	%3
وزارة الاتصالات وتقنية المعلومات	23	%7.7

الجهة او القطاع	التكرار	النسبة المئوية
وزارة الكهرباء والماء	8	%2.7
الهيئة السعودية للبيانات والذكاء الاصطناعي	6	%2
الهيئة السعودية للمدن الاقتصادية (مدن)	13	%4.3
الهيئة العامة للطيران المدني	11	%3.7
وزارة الصحة	12	%4
وزارة الاقتصاد والتخطيط	32	%10.7
الهيئة العامة للموانئ	23	%7.7
وزارة المالية	33	%11
وزارة التجارة	32	%10.7
الهيئة العامة للترفيه	8	%2.7
وزارة النقل	8	%2.7
وزارة السياحة	11	%3.7
وكالة الشؤون المالية للإيرادات	32	%10.7
وزارة الحج	11	%3.7
الإجمالي	300	%100

تشير النتائج الإحصائية في (الجدول4) بالنسبة لمتغير الجهة أو القطاع الحكومي الذي يعمل به المشاركون، جاءت الفئة العاملة في " وزارة المالية " بأعلى نسبة مئوية بلغت 11%، ويليها " وزارة التجارة" " وزارة الاقتصاد والتخطيط " وكالة الشؤون المالية للإيرادات " بنسبة مئوية بلغت 10.7%، في حين جاء في المرتبة الثالثة " وزارة الاتصالات وتقنية المعلومات " و"الهيئة العامة للموانئ "بنسبة مئوية بلغت7.7%. وهذا يدل على أن النسب الأكبر من أفراد العينة هي وزارة المالية والتجارة، ووزارة الاقتصاد، ووزارة الاتصالات وتكنولوجيا المعلومات، وديوان الضرائب والمالية. ويشير التوزيع إلى توزيع المشاركين في الدراسة على مختلف الجهات الحكومية، حيث يظهر تركيزا عاليا للمشاركين في وزارة المالية، ووزارة التجارة، ووزارة الاقتصاد، ووزارة الاتصالات وتقنية المعلومات، وكالة الشؤون المالية للإيرادات. ويعتبر هذا التخصيص المتوازن بين الوكالات الحكومية المختلفة مهمًا للدراسة الحالية، ويسمح هذا التوزيع بفهم أعمق وتحليل أفضل للبيانات، مما يؤدي إلى استنتاجات أكثر دقة وشمولاً.

7- توزيع افراد عينة الدراسة وفقاً للإدارة التي يعمل بها المشاركون

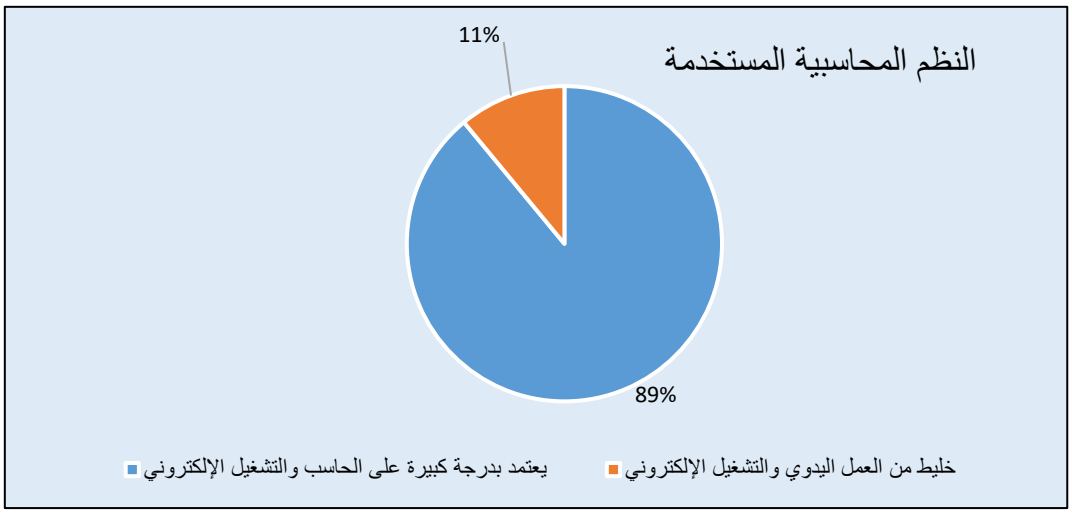
لقد تم حساب النسب المئوية لأفراد عينة الدراسة وفقاً للإدارة التي يعمل بها المشاركون، كما هو محدد في الشكل (6) ادناه، وتتضمن ما يلي:



شكل (6) يوضح توزيع عينة الدراسة وفقاً للإدارات التي يعمل بها المشاركون

يتبين من (شكل6) أن نسبة الفئة العاملة في" الإدارة العامة للشؤون الإدارية والمالية " بلغت 74.7%، ونسبة الفئة العاملة في " الإدارة العامة لتقنية المعلومات بلغت " 24.7%. ويشير هذا التوزيع إلى أن غالبية المشاركين يعملون في الأقسام والإدارات التابعة للإدارة العامة للشؤون الإدارية والمالية، مما يعكس تركيزًا قويًا على هذه الإدارات داخل الهيئات أو القطاعات الحكومية المدروسة.

8- توزيع افراد عينة الدراسة وفقاً للنظم المحاسبية المستخدمة في القطاع الحكومي



شكل (7) يوضح توزيع أفراد عينة الدراسة وفقاً للنظم المحاسبية المستخدمة في القطاع الحكومي

يتبين من (شكل7) أن النسبة المئوية للفئة التي اشارت الى الاعتماد بدرجة كبيرة على الحاسب والتشغيل الإلكتروني " 89.0%، في حين بلغت النسبة المئوية للفئة التي اشارت الى الاعتماد على خليط من العمل اليدوي والتشغيل الإلكتروني. " 11.0%. مما يدل أن النظم المحاسبية المستخدمة في القطاعات الحكومية تعتمد على الحاسب والتشغيل الإلكتروني في نظمها المحاسبية. هذا الاعتماد الكبير على التكنولوجيا يعكس تطور القطاع الحكومي نحو التحديث والتطوير التكنولوجي في عملياته المحاسبية.

2-5-3 نتائج الإحصاء الوصفي لمحاور الدراسة

سيتم في هذا الجزء تنفيذ التحليل الاحصائي الوصفي لمحاور الدراسة وذلك من خلال استخراج المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية واجراء اختبار مربع كاي (Chi-Square).

3-2-5-1 نتائج الإجابة عن أسئلة المحور الأول "تطبيق الاستراتيجية الوطنية للأمن السيبراني"

1- نتائج الإجابة عن أسئلة البعد الأول:

يوضح جدول (5) أثر استراتيجية الامن السيبراني (تعزيز حماية المعلومات) في الحد من مخاطر نظم المعلومات المحاسبية، وللتعرف على هذا البعد قامت الباحثة بتخصيص (10) عبارات لقياس أثر استراتيجية الامن السيبراني (تعزيز حماية المعلومات) في الحد من مخاطر نظم المعلومات المحاسبية، وجاءت النتائج كما يلي:

جدول (5) نتائج الإحصاء الوصفي للبعد الأول للمحور الأول

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة المو افقة	الترتيب
1	يتم تطبيق متطلبات استر اتيجية الأمن السيبر اني التي تضعها الهيئة لحماية بيانات ومعلومات القطاعات الحكومية	4.33	0.472	86.7%	عالية جداً	5
2	تطوير السياسات والإجراءات في القطاعات الحكومية بما يتو افق مع متطلبات استر اتيجية الأمن السيبر اني	4.09	0.753	81.7%	عالية	6

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة	الترتيب
3	وجود تشريعات قانونية تلزم القطاعات الحكومية بتطبيق الأهداف والمبادئ الخاصة بالأمن السيبراني وتضمينها داخل استراتيجيتها المستقبلية	4.53	0.719	90.6%	عالية جداً	3
4	تلتزم الأقسام المالية والمحاسبية بالمتطلبات التنظيمية لتحقيق الأمن السيبراني في القطاعات الحكومية	3.96	0.817	79.2%	عالية	8
5	يساعد الأمن السيبراني في وجود بيئة رقابية مناسبة وملاءمة للحفاظ على سرية وسلامة ونزاهة المعلومات المحاسبية	4.54	0.955	90.7%	عالية جداً	1
6	يطبق القطاع الحكومي متطلبات الأمن السيبراني لإدارة أمن الشبكات والتطبيقات وحمايتها من الاختراق	3.88	1.359	77.5%	عالية	10
7	يتم تطبيق متطلبات الأمن السيبراني لإدارة النسخ الاحتياطية للبيانات والمعلومات المحاسبية	4.42	0.716	88.4%	عالية جداً	4
8	يطبق القطاع الحكومي متطلبات الأمن السيبراني لحماية البريد الالكتروني	3.96	1.245	79.2%	عالية	9
9	هناك تبادل وربط الكتروني آمن بين مختلف الإدارات والأقسام داخل القطاع الحكومي	4.06	0.929	81.3%	عالية	7
10	وجود نظام حماية عالي يساعد على تبادل المعلومات المحاسبية مع الجهات الاخرى بطريقة أسرع وأكثر اماناً	4.54	0.498	90.6%	عالية جداً	2
	البعد الأول: تعزيز حماية المعلومات في نظم المعلومات المحاسبية	4.23	0.572	84.6%	عالية جداً	

تم استخراج المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة وترتيبها تنازلياً حسب النسب المئوية لكل فقرة في الجدول (5)، حيث استخلصت الباحثة مدى التزام القطاع الحكومي بمتطلبات استراتيجية الأمن السيبراني في حماية سرية البيانات والحفاظ عليها وتبدلها بشكل أمن، مما كان له أثر كبير في الحد من مخاطر نظم المعلومات المحاسبية. وبشكل عام فقد أظهرت نتائج الإحصاء الوصفي للبعد الأول جدول (5) أن المتوسط الحسابي لجميع فقرات البعد الأول تعزيز حماية المعلومات تساوي 4.23 وانحراف معياري بلغ (0.572)، أي انه هناك اجماع وموافقة بنسبة84.6% حول أثر البعد الأول (تعزيز حماية المعلومات) لاستراتيجية الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية. وللتأكد من معنوية البعد وتحديد العلاقة بين فقرات البعد الأول، تم اجراء اختبار مربع كاي (Chi-Square)، حيث جاءت النتائج على النحو التالي:

جدول (6) اختبار مربع كاي (Chi-Square) للبعد الأول

م	الفقرات	مربع كاي	مستوى الدلالة
1	يتم تطبيق متطلبات استراتيجية الأمن السيبراني التي تضعها الهيئة لحماية بيانات ومعلومات القطاعات الحكومية	33.333	0.001
2	تطوير السياسات والإجراءات في القطاعات الحكومية بما يتوافق مع متطلبات استراتيجية الأمن السيبراني	79.920	0.001
3	وجود تشريعات قانونية تلزم القطاعات الحكومية بتطبيق الأهداف والمبادئ الخاصة بالأمن السيبراني وتضمينها داخل استراتيجيتها المستقبلية	149.220	0.001
4	تلتزم الأقسام المالية والمحاسبية بالمتطلبات التنظيمية لتحقيق الأمن السيبراني في القطاعات الحكومية	136.160	0.001

م	الفقرات	مربع كاي	مستوى الدلالة
5	يساعد الأمن السيبر اني في وجود بيئة رقابية مناسبة وملاءمة للحفاظ على سرية وسلامة ونزاهة المعلومات المحاسبية	242.180	0.001
6	يطبق القطاع الحكومي متطلبات الأمن السيبر اني لإدارة أمن الشبكات والتطبيقات وحمايتها من الاختراق	73.220	0.001
7	يتم تطبيق متطلبات الأمن السيبر اني لإدارة النسخ الاحتياطية للبيانات والمعلومات المحاسبية	.720	0.001
8	يطبق القطاع الحكومي متطلبات الأمن السيبر اني لحماية البريد الالكتروني	15.140	0.001
9	هناك تبادل وربط الكتروني آمن بين مختلف الإدارات والأقسام داخل القطاع الحكومي	73.220	0.001
10	وجود نظام حماية عالي يساعد على تبادل المعلومات المحاسبية مع الجهات الاخرى بطريقة أسرع وأكثر اماناً	1.613	0.204
	البعد الأول: تعزيز حماية المعلومات في نظم المعلومات المحاسبية	17.920	0.012

من خلال القيم أعلاه، وجدت الباحثة ان هناك أهمية كبيرة لتطبيق متطلبات الأمن السيبراني في القطاعات الحكومية، حيث أن معظم الفقرات تشير إلى وجود علاقة قوية مع تعزيز حماية المعلومات، مع ضرورة التركيز على تحسين إدارة النسخ الاحتياطية وحماية المعلومات عند تبادلها مع الجهات الأخرى، حيث أن هذه الجوانب تحتاج إلى مزيد من الاهتمام، وضرورة وجود تشريعات واضحة وسياسات فعالة لضمان تطبيق الأمن السيبراني بشكل شامل في جميع القطاعات الحكومية . لذا يتبين من خلال تحليل البيانات الواردة في الجدول (6)، أن هناك دلالة إحصائية عند مستوى معنوية أقل من 0.05 لجميع العبارات المدروسة، وكذلك للدرجة الكلية، باستثناء العبارة المتعلقة بـ "وجود نظام حماية عالي يساعد على تبادل المعلومات المحاسبية مع الجهات الأخرى بطريقة أسرع وأكثر أماناً". هذا الاستثناء لا ينتقص من النتيجة العامة التي تشير إلى وجود علاقة ذات دلالة إحصائية بين تعزيز حماية المعلومات والحد من مخاطر نظم المعلومات المحاسبية في القطاع الحكومي.

2- نتائج الإجابة عن أسئلة البعد الثاني

يوضح جدول (7) أثر استراتيجية الامن السيبراني (جودة مخرجات نظم المعلومات المحاسبية) في الحد من مخاطر نظم المعلومات المحاسبية، وللتعرف على هذا البعد قامت الباحثة بتخصيص (10) عبارات لقياس أثر البعد الثاني لإستراتيجية الامن السيبراني (جودة مخرجات نظم المعلومات المحاسبية) في الحد من مخاطر نظم المعلومات المحاسبية، وجاءت النتائج كما يلي:

جدول (7) نتائج الإحصاء الوصفي للبعد الثاني

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة المو افقة	الترتيب
1	تساهم استر اتيجية الأمن السيبر اني في زيادة وكفاءة وجودة مخرجات نظام المعلومات المحاسبية	4.62	0.710	92.4%	عالية جداً	1
2	يدعم الأمن السيبر اني نظم المعلومات المحاسبية في الحصول على المعلومات الملائمة التي تساعد في اتخاذ القرارات	4.53	0.500	90.7%	عالية جداً	2
3	يسهم الأمن السيبر اني في الحصول على معلومات صحيحة وموثوق بها بدرجة مقبولة	4.33	0.471	86.6%	عالية جداً	3
4	تسهم نظم المعلومات المحاسبية في تقليل نسبة الأخطاء بالمعلومات المحاسبية	4.09	0.753	81.7%	عالية	4
5	يدعم الأمن السيبر اني نظم المعلومات المحاسبية في انتاج معلومات محاسبية محدثة وآمنه	4.00	0.814	80.0%	عالية	5
6	قد يتسبب ضعف امن المعلومات في وجود خلل في مخرجات نظم المعلومات المحاسبية	3.98	0.952	79.5%	عالية	6

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة	الترتيب
7	يعزز الأمن السيبراني من ثبات الأساليب والإجراءات المتبعة بالقياس والإفصاح عن المعلومات المحاسبية	3.91	0.726	78.1%	عالية	7
8	توجد سياسات للقطاع الحكومي خاصة بحماية نظامها المحاسبي تساهم في زيادة مستويات الحياد وعدم التحيز بالمعلومات المحاسبية	3.59	1.405	71.9%	عالية	8
9	تغطي المعلومات التي ينتجها نظام المعلومات المحاسبي كل أوجه النشاط المتعلقة بالقطاع	3.58	1.161	71.5%	عالية	9
10	يحتفظ القطاع الحكومي بنسخة من برامج المعالجة في مكان مناسب وتسجل مخرجات النظام كوسيلة رقابية	3.46	1.048	69.1%	عالية	10
	البعد الثاني: جودة مخرجات نظم المعلومات المحاسبية	4.01	0.568	80.2%	عالية	

وقد تم استخراج المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة وترتيبها تنازلياً حسب النسب المئوية لكل فقرة في الجدول ر (7)، استخلصت الباحثة أن استراتيجية الامن السيبراني تسهم في زيادة كفاءة وجودة مخرجات نظم المعلومات المحاسبية، كما تسهم في الحصول على معلومات صحيحة وأكثر موثوقية، كما تقلل من نسب الأخطاء، مما يعكس أثره في الحد من مخاطر نظم المعلومات المحاسبية. وبشكل عام فقد أظهرت نتائج الإحصاء الوصفي للبعد الثاني جدول (7) أن المتوسط الحسابي لجميع فقرات البعد الثاني جودة مخرجات نظم المعلومات المحاسبية تساوي (4.01) وانحراف معياري بلغ (0.568)، أي انه هناك اجماع وموافقة بنسبة 80.2% حول أثر البعد الثاني (جودة مخرجات نظم المعلومات المحاسبية) لاستراتيجية الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية. وللتأكد من معنوية البعد وتحديد العلاقة بين فقرات البعد الثاني، تم اجراء اختبار مربع كاي (Chi-Square)، حيث جاءت النتائج على النحو التالي:

جدول (8) اختبار مربع كاي (Chi-Square) للبعد الثاني

م	الفقرات	مربع كاي	مستوى الدلالة
1	تساهم استراتيجية الأمن السيبراني في زيادة وكفاءة وجودة مخرجات نظام المعلومات المحاسبية	1.333[a]	0.248
2	يدعم الأمن السيبراني نظم المعلومات المحاسبية في الحصول على المعلومات الملائمة التي تساعد في اتخاذ القرارات	238.320	0.001
3	يسهم الأمن السيبراني في الحصول على معلومات صحيحة وموثوق بها بدرجة مقبولة	34.680	0.001
4	تسهم نظم المعلومات المحاسبية في تقليل نسبة الأخطاء في المعلومات لمحاسبية	158.460	0.001
5	يدعم الأمن السيبراني نظم المعلومات المحاسبية في انتاج معلومات محاسبية محدثة وآمنه	84.987	0.001
6	قد يتسبب ضعف امن المعلومات في وجود خلل في مخرجات نظم المعلومات المحاسبية	27.920	0.001
7	يعزز الأمن السيبراني من ثبات الأساليب والإجراءات المتبعة بالقياس والإفصاح عن المعلومات المحاسبية	43.067	0.001
8	توجد سياسات للقطاع الحكومي خاصة بحماية نظامها المحاسبي تساهم في زيادة مستويات الحياد وعدم التحيز بالمعلومات المحاسبية	47.467	0.001
9	تغطي المعلومات التي ينتجها نظام المعلومات المحاسبي كل أوجه النشاط المتعلقة بالقطاع	18.427	0.001
10	يحتفظ القطاع الحكومي بنسخة من برامج المعالجة في مكان مناسب وتسجل مخرجات النظام كوسيلة رقابية	15.140	0.001
	البعد الثاني: جودة مخرجات نظم المعلومات المحاسبية	92.047	0.001

ومن خلال القيم أعلاه، وجدت الباحثة ان الأمن السيبراني له تأثيرات إيجابية قوية على جودة مخرجات نظم المعلومات المحاسبية، وان هناك حاجة لتعزيز استراتيجيات الأمن السيبراني لضمان موثوقية المعلومات وتقليل الأخطاء وان السياسات الحكومية تلعب دورًا مهمًا في حماية المعلومات المحاسبية وزيادة الحياد. وبشكل عام، النتائج تدل على أهمية الأمن السيبراني في تحسين جودة المعلومات المحاسبية وضمان دقتها وموثوقيتها. لذا يتبين من خلال بيانات الجدول (8) ان هناك دلالة احصائية عند مستوى معنوية اقل من 0.05 لجميع العبارات، وكذلك للدرجة الكلية، - عدا العبارة " تساهم استراتيجية الأمن السيبراني في زيادة وكفاءة وجودة مخرجات نظام المعلومات المحاسبية "، مما يشير على ان هناك علاقة ذات دلالة إحصائية بين جودة المخرجات والحد من مخاطر نظم المعلومات المحاسبية في القطاع الحكومي في المملكة العربية السعودية.

3- نتائج الإجابة عن أسئلة البعد الثالث

يوضح جدول (9) مدى توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية، وللتعرف على هذا البعد قامت الباحثة بتخصيص (10) عبارات لقياس أثر البعد الثالث مدى توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية، وجاءت النتائج كما يلي:

جدول (9) نتائج الإحصاء الوصفي للبعد الثالث

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة	الترتيب
1	يقدم القطاع الحكومي الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية	4.31	0.465	86.3%	عالية جداً	2
2	يقوم القطاع الحكومي بتوعية الموظفين والإداريين بأهمية تطبيق الأمن السيبراني	4.02	0.952	80.5%	عالية	6
3	يقوم القطاع الحكومي باستقطاب الكوادر الوطنية المؤهلة من ذوي الخبرة والاختصاص لتطبيق استراتيجيات الأمن السيبراني وتدريب العاملين عليها	3.98	0.931	79.7%	عالية	7
4	ينظم القطاع الحكومي اللقاءات الدورية للمختصين بتطبيق الأمن السيبراني لتعريفهم بالمستجدات في المجال	4.09	0.984	81.9%	عالية	4
5	يقوم القطاع الحكومي بتوفير الدورات التدريبية اللازمة للعاملين على الأنظمة المحاسبية لتطبيق استراتيجيات الأمن السيبراني	4.07	0.999	81.5%	عالية	5
6	يحدد القطاع الحكومي المهام والمسؤوليات ذات العلاقة بأمن أنظمة المعلومات المحاسبية	4.34	1.052	86.7%	عالية جداً	1
7	توجد ضوابط واضحة لإدارة الأصول المحاسبية التي بعهدة الموظف كأجهزة الحاسب	4.22	0.627	84.4%	عالية جداً	3
8	عدم توفر التدريب والتأهيل اللازم لإدارة عمليات نظم المعلومات المحاسبية	3.31	1.243	66.2%	متوسطة	8
9	عدم الوعي الكافي بين موظفي الإدارة المحاسبية حول ضرورة فحص أي برامج يتم استخدامها او أجهزة تخزين خارجية قبل إدخالها في الأجهزة	3.22	1.395	64.5%	متوسطة	9
10	عدم وجود مقاييس مناسبة لقياس أداء الموظف كقياس مؤشرات الأداء الرئيسية	3.20	1.309	64.0%	متوسطة	10
	البعد الثالث: توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني	3.88	0.635	77.6%	عالية	

لقد تم استخراج المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة وترتيبها تنازلياً حسب النسب المئوية لكل فقرة في الجدول (9)، واستخلصت الباحثة مما سبق أن القطاع الحكومي يوفر الدعم الفني اللازم لتطبيق استراتيجية الأمن السيبراني، ويحدد المهام للموظفين ويوفر التدريب اللازم للموظفين، كما يستقطب الكوادر البشرية المؤهلة للعمل على هذه الأنظمة، مما يسهم في الحد من مخاطر أنظمة المعلومات المحاسبية. وبشكل عام فقد أظهرت نتائج الإحصاء الوصفي للبعد الثاني جدول (9) أن المتوسط الحسابي لجميع فقرات البعد الثالث مدى توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني تساوي (3.88) وانحراف معياري بلغ

(0.635)، أي انه هناك اجماع وموافقة بنسبة 77.6% حول أثر البعد الثالث مدى توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية. وللتأكد من معنوية البعد وتحديد العلاقة بين فقرات البعد الثالث، تم اجراء اختبار مربع كاي (Chi-Square)، حيث جاءت النتائج على النحو التالي:

جدول (10) اختبار مربع كاي (Chi-Square) للبعد الثالث

م	الفقرات	مربع كاي	مستوى الدلالة
1	يقدم القطاع الحكومي الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية	41.813[a]	0.001
2	يقوم القطاع الحكومي بتوعية الموظفين والإداريين بأهمية تطبيق الأمن السيبراني	84.987[c]	0.001
3	يقوم القطاع الحكومي باستقطاب الكوادر الوطنية المؤهلة من ذوي الخبرة والاختصاص لتطبيق استراتيجيات الأمن السيبراني وتدريب العاملين عليها	108.187[c]	0.001
4	ينظم القطاع الحكومي اللقاءات الدورية للمختصين بتطبيق الأمن السيبراني لتعريفهم بالمستجدات في المجال	96.747[c]	0.001
5	يقوم القطاع الحكومي بتوفير الدورات التدريبية اللازمة للعاملين على الأنظمة المحاسبية لتطبيق استراتيجيات الأمن السيبراني	97.307[c]	0.001
6	يحدد القطاع الحكومي المهام والمسؤوليات ذات العلاقة بأمن أنظمة المعلومات المحاسبية	277.787[c]	0.001
7	توجد ضوابط واضحة لإدارة الأصول المحاسبية التي بعهدة الموظف كأجهزة الحاسب	91.140[b]	0.001
8	عدم توفر التدريب والتأهيل اللازم لإدارة عمليات نظم المعلومات المحاسبية	59.300f	0.001
9	عدم الوعي الكافي بين موظفي الإدارة المحاسبية حول ضرورة فحص أي برامج يتم استخدامها او أجهزة تخزين خارجية قبل إدخالها في الأجهزة	16.400f	0.001
10	عدم وجود مقاييس مناسبة لقياس أداء الموظف كقياس مؤشرات الأداء الرئيسية	41.947c	0.001
	البعد الثالث: توفر الكوادر البشرية المؤهلة لتطبيق استراتيجية الأمن السيبراني	72.120e	0.001

ومن خلال القيم أعلاه، وجدت الباحثة ان لتوافر الكوادر البشرية المؤهلة تأثيرات إيجابية قوية على تطبيق الاستراتيجية الوطنية للأمن السيبراني على نظم المعلومات المحاسبية، ومن المهم تعزيز استراتيجيات الأمن السيبراني وتوفير التدريب والوعي اللازم لضمان فعالية نظم المعلومات المحاسبية. لذا يتبين من خلال بيانات الجدول (10) ان هناك دلالة احصائية عند مستوى معنوية اقل من 0.05 لجميع العبارات، وكذلك للدرجة الكلية، مما يؤكد على ان هناك توافر للكوادر البشرية المؤهلة لتطبيق الاستراتيجية الوطنية للأمن السيبراني على نظم المعلومات المحاسبية.

3-5-2-2 نتائج الإجابة عن أسئلة المحور الثاني "الحد من مخاطر نظم المعلومات المحاسبية"

يوضح جدول (11) مدى إدارة المخاطر المتعلقة بنظم المعلومات المحاسبية وأثر تطبيق استراتيجية الأمن السيبراني في الحد منها، وللتعرف على هذا المحور قامت الباحثة بتخصيص (10) عبارات للقياس وجاءت النتائج كما يلي:

جدول (11) نتائج الإحصاء الوصفي للمحور الثاني

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة	الترتيب
1	يقوم القطاع الحكومي بتوفير الأجهزة الرقابية اللازمة للتأكد من تطبيق الضوابط وسياسات اللازمة لتحقيق الأمن السيبراني	4.42	0.495	88.5%	عالية جداً	1
2	وجود إدارة في القطاعات الحكومية مسؤولة عن إدارة المخاطر وتقييم هذه المخاطر السيبرانية على نظم المعلومات بشكل دوري	4.31	0.693	86.1%	عالية جداً	2
3	وجود سياسات ولوائح واضحة متعلقة بأمن نظم المعلومات المحاسبية وآليات لتنظيمها	4.22	0.415	84.4%	عالية جداً	3
4	تقوم إدارة المخاطر في القطاعات الحكومية بتحديد مستوى هذه المخاطر المحتملة و اتخاذ الإجراءات اللازمة لمواجهتها	3.78	0.627	75.6%	عالية	8

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة	الترتيب
5	عدم الفصل بين المهام الإدارية والمهام والوظائف المحاسبية يساهم بشكل كبير في الحد من فعالية امن المعلومات وبالتالي التأثير سلباً على استراتيجيات الأمن السيبراني	4.06	1.109	81.3%	عالية	5
6	وجود هيكل تنظيمي واضح يحدد صلاحيات كل شخص في نظم المعلومات المحاسبية	3.91	0.984	78.1%	عالية	6
7	تعد الفيروسات وغيرها من البرامج الضارة أحد أخطر التهديدات لنظم المعلومات المحاسبية في الوقت الحاضر	3.80	0.908	75.9%	عالية	7
8	يواكب القطاع الحكومي التطورات التكنولوجية التقنيات المتقدمة في مجالات برامج حماية أنظمة المعلومات مثل برامج التشفير والتوثيق للمخرجات في الحد من مخاطر نظم المعلومات المحاسبية	3.80	0.908	75.9%	عالية	7
9	يمتلك القطاع الحكومي الأنظمة القادرة على صد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه وفقاً لتعليمات الهيئة الوطنية للأمن السيبراني	4.18	1.038	83.6%	عالية	4
10	هناك عجز في الموارد المادية كالأجهزة او البرامج المناسبة لتنفيذ عمليات نظم المعلومات المحاسبية	3.20	0.933	64.0%	متوسطة	9
	المحور الثاني: الحد من مخاطر نظم المعلومات المحاسبية	3.97	0.456	79.3%	عالية	

تم استخراج المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة وترتيبها تنازلياً حسب النسب المئوية لكل فقرة في الجدول (11)، استخلصت الباحثة مما سبق أن القطاع الحكومي يطبق استراتيجية الأمن السيبراني وذلك من خلال توفير الأجهزة الرقابية الملائمة ووضع السياسات واللوائح المتعلقة بأمن نظم المعلومات المحاسبية، ووجود إدارة لتقييم وإدارة مخاطر هذه النظم مما يحد من مخاطر نظم المعلومات المحاسبية. وبشكل عام فقد أظهرت نتائج الإحصاء الوصفي للبعد الثاني جدول رقم (11) أن المتوسط الحسابي لجميع فقرات المحور الثاني وهو الحد من مخاطر نظم المعلومات المحاسبية تساوي (3.97) وانحراف معياري بلغ (0.456)، أي انه هناك اجماع وموافقة بنسبة 79.3 % حول أثر تطبيق استراتيجية الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية.وللتأكد من معنوية البعد وتحديد العلاقة بين فقرات المحور الثاني، تم اجراء اختبار مربع كاي (Chi-Square)، حيث جاءت النتائج على النحو التالي:

جدول (12) اختبار مربع كاي (Chi-Square) للمحور الثاني

م	الفقرات	مربع كاي	مستوى الدلالة
1	وجود سياسات ولوائح واضحة متعلقة بأمن نظم المعلومات المحاسبية وآليات لتنظيمها	94.080	0.001
2	يقوم القطاع الحكومي بتوفير الأجهزة الرقابية اللازمة للتأكد من تطبيق الضوابط وسياسات اللازمة لتحقيق الأمن السيبراني	7.053	0.001
3	وجود إدارة في القطاعات الحكومية مسؤولة عن إدارة المخاطر وتقييم هذه المخاطر السيبرانية على نظم المعلومات بشكل دوري	54.080	0.001
4	تقوم إدارة المخاطر في القطاعات الحكومية بتحديد مستوى هذه المخاطر المحتملة و اتخاذ الإجراءات اللازمة لمواجهتها	137.040	0.001
5	عدم الفصل بين المهام الإدارية والمهام والوظائف المحاسبية يساهم بشكل كبير في الحد من فعالية امن المعلومات وبالتالي التأثير سلباً على استراتيجيات الأمن السيبراني	142.320	0.001
6	وجود هيكل تنظيمي واضح يحدد صلاحيات كل شخص في نظم المعلومات المحاسبية	47.467	0.001
7	هناك عجز في الموارد المادية كالأجهزة او البرامج المناسبة لتنفيذ عمليات نظم المعلومات المحاسبية	60.480	0.001
8	يمتلك القطاع الحكومي الأنظمة القادرة على صد الاختراق عند حدوثه وإصلاح الخلل الناتج عنه وفقاً لتعليمات الهيئة الوطنية للأمن السيبراني	91.140	0.001

م	الفقرات	مربع كاي	مستوى الدلالة
9	تعد الفيروسات وغيرها من البرامج الضارة أحد أخطر التهديدات لنظم المعلومات المحاسبية في الوقت الحاضر	83.547	0.001
10	يواكب القطاع الحكومي التطورات التكنولوجية التقنيات المتقدمة في مجالات برامج حماية أنظمة المعلومات مثل برامج التشفيروالتوثيق للمخرجات في الحد من مخاطر نظم المعلومات المحاسبية	83.544	0.001
	المحور الثاني: الحد من مخاطر نظم المعلومات المحاسبية	30.540	0.001

وقد أظهرت نتائج اختبار مربع كاي (Chi-Square) للمحور الثاني أن هناك علاقة قوية بين تطبيق الاستراتيجية الوطنية للأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية. وقد وجدت الباحثة ان لتطبيق الاستراتيجية الوطنية للأمن السيبراني تأثيرات إيجابية قوية في الحد من مخاطر نظم المعلومات المحاسبية، ومن المهم أيضا تعزيز فعالية وسائل حماية النظم المحاسبية والاهتمام بجودة مخرجات هذه النظم وتعزيز كفاءة الموارد البشرية العاملة على هذه النظم في القطاعات الحكومية المختلفة في المملكة العربية السعودية. لذا يتبين من خلال بيانات الجدول (12)، أن هناك دلالة احصائية عند مستوى معنوية اقل من 0.05 لجميع العبارات، وكذلك للدرجة الكلية، وهو ما يؤكد ان هناك علاقة ذات دلالة إحصائية بين تطبيق الاستراتيجية الوطنية للأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية في القطاع الحكومي في المملكة العربية السعودية.

6-3 نتائج اختبار فرضيات الدراسة

سيتم في هذه الفقرة استعراض نتائج اختبار الفرضيات من خلال أولا اختبار الانحدار الخطي والذي سيوضح القدرة المعنوية للمتغير المستقل على تفسير المتغير التابع، وبالتالي قبول أو رفض الفرضية بشكل عام.

3-6-1 الفرضية الرئيسة الأولى: توجد علاقة ذات دلالة إحصائية بين تطبيق الاستراتيجية الوطنية للأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية.

وتندرج تحتها الفرضيات الفرعية التالية

3-6-1-1الفرضية الفرعية الأولى

تمثلت الفرضية الفرعية الأولى في أنه توجد علاقة ذات دلالة إحصائية بين حماية المعلومات المحاسبية والحد من مخاطر نظم المعلومات المحاسبية. حيث يوضح جدول (13) نتائج تحليل التباين للانحدار للفرضية الفرعية الأولى، كما يلي:

جدول (13) نتائج تحليل التباين للانحدار للفرضية الفرعية الأولى

النموذج	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى الدلالة F	Adjusted R^2	معامل التحديد R^2	معامل الارتباط R
الانحدار	25.389	25.389	205.868	0.000	0.70	0.704	0.839
الخطأ المتبقي	36.751	.123					
المجموع	62.140						

وتوضح نتائج تحليل التباين للانحدار (الجدول13) من خلال مجموع المربعات أن مجموع المربعات الكلي الذي يساوي 62.14. يمثل التباين الكلي في البيانات. وكان مجموع المربعات للانحدار (Regression Sum of Squares) يساوي 25.389، وهو يمثل التباين المفسر بواسطة النموذج. ويشير هذا إلى أن النموذج يفسر جزءًا من التباين الكلي. كما ان مجموع المربعات للخطأ المتبقي (Residual Sum of Squares) يساوي 36.751، وهو يمثل التباين غير المفسر بواسطة النموذج. كلما كان هذا الرقم أقل، كان النموذج أفضل في التنبؤ بالنتائج. وكان متوسط المربعات ومتوسط المربعات للانحدار (Mean Square for Regression) يساوي 25.389، وهو مجموع المربعات للانحدار مقسومًا على درجات الحرية الخاصة بالانحدار. ومتوسط المربعات للخطأ المتبقي (Mean Square for Residuals) يساوي 0.123، وهو مجموع المربعات للخطأ المتبقي مقسومًا على درجات الحرية الخاصة بالخطأ. كما ان قيمة F المحسوبة :تساوي 205.868، وهي تستخدم لاختبار فرضية أن النموذج لا يفسر أي تباين. قيمة F العالية تشير إلى أن النموذج ذو دلالة إحصائية قوية. ومستوى الدلالة :(Significance Level) يساوي 0، مما يعني أن النتائج ذات دلالة إحصائية عالية، حيث أن القيمة أقل من 0.05 تشير إلى أن هناك علاقة قوية بين المتغيرات. كما ان معامل الانحدار Adjusted R^2يساوي 0.7، مما يعني أن 70% من التباين في المتغير التابع يمكن تفسيره بواسطة المتغيرات المستقلة في النموذج. وكان معامل الارتباط يساوي 0.704، وهو يشير إلى أن النموذج يفسر 70.4% من التباين في البيانات. ومعامل الارتباط (Correlation Coefficient) يساوي

0.839، مما يدل على وجود علاقة إيجابية قوية بين المتغيرات. لذا تشير النتائج إلى أن النموذج المستخدم في التحليل يفسر جزءًا كبيرًا من التباين في البيانات، مع وجود دلالة إحصائية قوية. القيم العالية لكل من F و R^2تدل على فعالية النموذج في التنبؤ بالنتائج . وبالتالي، فإنه توجد علاقة ذات دلالة إحصائية بين حماية المعلومات المحاسبية والحد من مخاطر نظم المعلومات المحاسبية. ويشير هذا إلى أن تحسين حماية المعلومات المحاسبية يمكن أن يسهم بشكل كبير في تقليل مخاطر نظم المعلومات المحاسبية.

3-1-6-2الفرضية الفرعية الثانية:

تمثلت الفرضية الفرعية الثانية في أنه **توجد علاقة ذات دلالة إحصائية بين جودة مخرجات نظم المعلومات المحاسبية والحد من مخاطرنظم المعلومات المحاسبية**. حيث يوضح جدول (14) نتائج تحليل التباين للانحدار للفرضية الفرعية الثانية. كما يلي:

جدول (14) نتائج تحليل التباين للانحدارللفرضية الفرعية الثانية

النموذج	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى الدلالة F	Adjusted R^2	معامل التحديد R^2	معامل الارتباط R
الانحدار	34.379	34.379	369.052	0.000	0.80	0.562	0.750
الخطأ المتبقي	27.760	.093					
المجموع	62.140						

يعرض جدول تحليل التباين (الجدول14) نتائج الانحدار وتحليل البيانات المتعلقة بتطبيق الاستراتيجية الوطنية للأمن السيبراني. حيث يشير مجموع المربعات إلى مجموع التباين في البيانات. في هذا الجدول، مجموع المربعات للانحدار هو 34.379، بينما مجموع المربعات للخطأ المتبقي هو 27.76، مما يدل على أن هناك تباينًا ملحوظًا يمكن تفسيره بواسطة النموذج. كما يمثل متوسط المربعات متوسط المربعات لكل من الانحدار والخطأ المتبقي. متوسط المربعات للانحدار هو 34.379، مما يشير إلى أن النموذج يفسر جزءًا كبيرًا من التباين. وقد بلغت قيمة F المحسوبة 369.052، وهي قيمة مرتفعة جدًا، مما يدل على أن النموذج العام له دلالة إحصائية قوية. هذا يعني أن هناك علاقة ذات دلالة بين المتغيرات المستقلة والتابعة. وكان مستوى الدلالة 0.00 مما يعني أن النتائج ذات دلالة إحصائية قوية، حيث أن القيم أقل من 0.05 تشير إلى أن النتائج ليست ناتجة عن الصدفة. وتشير قيمة Adjusted R^2 إلى أن 80% من التباين في البيانات يمكن تفسيره بواسطة النموذج، مما يدل على قوة النموذج في تفسير البيانات. كما تشير قيمة معامل الارتباط R القيمة 0.75 إلى وجود علاقة إيجابية قوية بين المتغيرات، مما يعزز من مصداقية النموذج. وبشكل عام، تشير النتائج إلى أن النموذج المستخدم في تحليل التباين يفسر بشكل جيد العلاقة بين جودة مخرجات نظم المعلومات المحاسبة والحد من مخاطر نظم المعلومات المحاسبية، مما يعكس فعالية هذه الاستراتيجية في حماية البيانات والمعلومات المحاسبية. وبالتالي، هناك علاقة ذات دلالة إحصائية بين جودة مخرجات نظم المعلومات المحاسبية والحد من مخاطر نظم المعلومات المحاسبية. كما يشير إلى أن تحسين جودة مخرجات نظم المعلومات المحاسبية يمكن أن يسهم بشكل كبير في تقليل المخاطر المرتبطة بنظم المعلومات المحاسبية.

3-1-6-3 الفرضية الفرعية الثالثة:

تمثلت الفرضية الفرعية الثالثة في أنه توجد فروق ذات دلالة إحصائية بين كفاءة الكوادر البشرية في تطبيق استراتيجية الأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية وفقاً لمتغير (الخبرة). حيث يوضح جدول (15) نتائج تحليل التباين للانحدار للفرضية الفرعية الثالثة. كما يلي:

جدول (15) نتائج تحليل التباين للانحدارللفرضية الفرعية الثالثة

النموذج	مجموع المربعات	متوسط المربعات	قيمة F المحسوبة	مستوى الدلالة F	Adjusted R^2	معامل التحديد R^2	معامل الارتباط R
الانحدار	26.049	5.210	42.440	0.000	0.82	0.135	0.368
الخطأ المتبقي	36.091	.123					
المجموع	62.140						

تشير نتائج جدول تحليل التباين (جدول 15) الى نتائج الانحدار ويظهر العلاقة بين المتغيرات المستقلة والتابعة حيث يشير مجموع المربعات إلى التباين الكلي في البيانات. في الجدول، مجموع المربعات للانحدار هو 34.379، بينما مجموع المربعات للخطأ المتبقي هو 27.76. هذا يدل على أن النموذج يفسر جزءًا كبيرًا من التباين في البيانات. كما يعكس متوسط المربعات كفاءة النموذج. متوسط المربعات للانحدار هو 34.379، مما يشير إلى أن النموذج فعال في تفسير البيانات. بينما متوسط المربعات للخطأ المتبقي هو 0.093، مما يدل على أن الخطأ في النموذج

منخفض. وتبلغ قيمة F المحسوبة 369.052، وهي قيمة مرتفعة جدًا، مما يدل على أن النموذج العام له دلالة إحصائية قوية. هذا يعني أن هناك علاقة ذات دلالة بين المتغيرات المستقلة والتابعة. كما ان مستوى الدلالة هو 0، مما يعني أن النتائج ذات دلالة إحصائية قوية، حيث أن القيم أقل من 0.05 تشير إلى أن النتائج ليست ناتجة عن الصدفة. وتشير نتائج قيمة R^2 Adjusted 0.8 إلى أن 80% من التباين في البيانات يمكن تفسيره بواسطة النموذج، مما يدل على فعالية النموذج في تفسير البيانات. كمان ان قيمة معامل الارتباط R هي 0.75 وتشير إلى وجود علاقة إيجابية قوية بين المتغيرات، مما يعزز من مصداقية النموذج. **وبالتالي، هناك فروق ذات دلالة إحصائية بين كفاءة الكوادر البشرية في تطبيق استراتيجية الأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية وفقاً لمتغير الخبرة.** كما يشير إلى أن خبرة الكوادر البشرية تلعب دوراً هاماً في كفاءة تطبيق استراتيجية الأمن السيبراني.

4- النتائج

من خلال تحليل البيانات، يمكن تلخيص النتائج المتعلقة بأثر تطبيق الاستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية في القطاع الحكومي في المملكة العربية السعودية، على النحو التالي:

1. **حماية المعلومات في النظم المعلومات المحاسبية:**

- أظهرت النتائج وجود علاقة قوية وذات دلالة إحصائية بين تطبيق الاستراتيجية الوطنية للأمن السيبراني وحماية المعلومات في نظم المعلومات المحاسبية في القطاع الحكومي. وهذا يدل على أن اعتماد هذه الاستراتيجية يلعب دوراً محورياً في ضمان أمن المعلومات المحاسبية. ويرجع ذلك إلى التوافر العالي للتقنيات الأمنية الملائمة والتشريعات القانونية التي تدعم هذه الاستراتيجية. ويعزز هذا التأكيد على أهمية الأمن السيبراني في حماية البيانات الحساسة ويقلل من المخاطر التي قد تواجهها نظم المعلومات المحاسبية. وتتوافق هذه الدراسة مع دراسة (Kasasbeh & Thuneibat , 2018) التي اشارت إلى أن التحكم في الولوج للنظام يؤثر بشكل إيجابي على قدرة نظم المعلومات المحاسبية على مواجهة التهديدات السيبرانية، ودراسة(Ali; et al., 2020) التي وجدت أن حوكمة الأمن السيبراني تؤثر بشكل كبير في تقليل مخاطر المحاسبة السحابية. ودراسة (Almomani, et al , 2021) التي أكدت على أن فعالية وكفاءة الأمن السيبراني تزيد من موثوقية المعلومات المحاسبية السحابية ودراسة العموش والخزعلي (2023) التي أشارت إلى أن ممارسات الحوكمة السيبرانية القوية تقلل من احتمالية حدوث اختراقات للبيانات وتعزز الوضع الأمني العام لأنظمة المحاسبة السحابية.

2. **جودة مخرجات نظم المعلومات المحاسبية:**

- هناك علاقة واضحة بين تطبيق الاستراتيجية الوطنية للأمن السيبراني وتحسين جودة وكفاءة مخرجات نظم المعلومات المحاسبية في القطاع الحكومي، حيث يقدم دعم الأمن السيبراني إطارًا يعزز من دقة وموثوقية المعلومات المحاسبية، مما يتيح للقطاعات الحكومية إمكانية اتخاذ قرارات مبنية على معلومات موثوقة وملائمة. هذا التحسين في جودة المعلومات يؤدي إلى قرارات أكثر استنارة، مما ينعكس إيجابياً على أداء القطاع الحكومي ككل. وتتفق الدراسة الحالية مع الدراسات السابقة حيث تؤكد هذه الدراسة أن تطبيق الاستراتيجية الوطنية للأمن السيبراني يحسن من جودة وكفاءة مخرجات نظم المعلومات المحاسبية في القطاع الحكومي. وتتفق في ذلك مع دراسة (السرحان وآخرون، 2020) التي وجدت أن خصوصية بيانات العملاء وإدارة المخاطر السيبرانية تؤثر بشكل كبير على جودة المعلومات المحاسبية، ودراسة (العوامري وآخرون، 2022) التي أكدت على أن تكامل الأمن السيبراني وخدمات تأكيد الثقة يزيد من موثوقية ومصداقية نظم المعلومات المحاسبية.

3. **تو افر الكوادر البشرية المؤهلة:**

- أكدت النتائج على توافر الكوادر البشرية المؤهلة لتطبيق الاستراتيجية الوطنية للأمن السيبراني على نظم المعلومات المحاسبية. هذا يشير إلى أن القطاعات الحكومية مستعدة لتطبيق هذه الاستراتيجية بفعالية، وذلك من خلال الاستثمار في تطوير وتدريب الكوادر البشرية. وجود دعم فني وتحديد واضح للمهام والمسؤوليات المتعلقة بالأمن السيبراني يعزز من كفاءة وفعالية تنفيذ هذه الاستراتيجيات، مما يساهم في تحسين الأمن السيبراني بشكل عام. وقد اتفقت الدراسة الحالية مع عدد من الدراسات السابقة حيث أكدت على أهمية توافر الكوادر البشرية المؤهلة لتطبيق الاستراتيجية الوطنية للأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية. وقد اتفقت في ذلك مع دراسة (Ehioghiren, et al. 2021) التي أكدت على أهمية تدريب وتطوير الكوادر البشرية في مجال الأمن السيبراني ودراسة (العموش والخزعلي، 2023) التي أشارت إلى أن الخبرة تلعب دورًا محوريًا في فعالية تطبيق استراتيجيات الأمن السيبراني.

بشكل عام، تتوافق نتائج الدراسة الحالية مع العديد من الدراسات السابقة في التأكيد على أهمية الأمن السيبراني، في تقليل المخاطر المرتبطة بنظم المعلومات المحاسبية. كما تبرز هذه النتائج أهمية كل من التكنولوجيا المتقدمة والتشريعات الملائمة، بالإضافة إلى الإدارة الفعالة

للمخاطر وتطوير الكوادر البشرية، في تعزيز تطبيق الاستراتيجية الوطنية للأمن السيبراني في القطاع الحكومي، مما يحقق حماية أفضل للمعلومات المحاسبية ويعزز من جودة صنع القرار.

كما تمت مناقشة فرضيات الدراسة، ووجد أن هناك علاقات ذات دلالة إحصائية بين مجموعة من العوامل والحد من مخاطر نظم المعلومات المحاسبية في القطاع الحكومي. ويمكن تفسير هذه النتائج على النحو التالي:

1. **العلاقة مع حماية المعلومات المحاسبية:**
   - تشير النتائج إلى وجود علاقة ذات دلالة إحصائية بين حماية المعلومات المحاسبية والحد من مخاطر نظم المعلومات المحاسبية. هذا يعني أن الجهود المبذولة لحماية المعلومات المحاسبية تسهم بشكل مباشر في تقليل المخاطر المرتبطة بهذه النظم. فعند تعزيز إجراءات الأمن والحماية، يتم تقليل فرص حدوث اختراقات أو تسريبات للبيانات، مما يقلل من المخاطر المحتملة ويزيد من استقرار نظم المعلومات المحاسبية.

2. **جودة مخرجات نظم المعلومات المحاسبية:**
   - العلاقة ذات الدلالة الإحصائية بين جودة مخرجات نظم المعلومات المحاسبية والحد من المخاطر تشير إلى أن تحسين جودة المعلومات المحاسبية يلعب دورًا هامًا في تقليل المخاطر. مخرجات ذات جودة عالية تعني بيانات موثوقة ودقيقة، مما يقلل من الأخطاء والتناقضات التي قد تؤدي إلى مخاطر تشغيلية أو قرارات خاطئة. تحسين جودة المخرجات يسهم في بناء نظام معلومات محاسبية أكثر استقرارًا وفعالية.

3. **كفاءة الكوادر البشرية ومتغير الخبرة:**
   - وجود فروق ذات دلالة إحصائية بين كفاءة الكوادر البشرية في تطبيق استراتيجية الأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية وفقًا لمتغير الخبرة يشير إلى أن الخبرة تلعب دورًا محوريًا في فعالية تطبيق استراتيجيات الأمن السيبراني. الكوادر الأكثر خبرة تكون عادةً أكثر كفاءة في التعرف على المخاطر ومعالجتها، مما يساهم في تقليل المخاطر بشكل أكثر فعالية. هذا يبرز أهمية الاستثمار في تدريب وتطوير الكوادر البشرية لضمان قدرتهم على تطبيق الاستراتيجيات الأمنية بما يقلل من المخاطر إلى أدنى حد ممكن.

الخاتمة

لقد تم في هذه الدراسة تقييم أثر تطبيق الاستراتيجية الوطنية للأمن السيبراني للحد من مخاطر نظم المعلومات المحاسبية في القطاع الحكومي بالمملكة العربية السعودية، حيث تبين أن هناك تأثيراً إيجابياً للاستراتيجية الوطنية للأمن السيبراني في حماية المعلومات المحاسبية وجودة مخرجات المعلومات المحاسبية في ظل توافر الكوادر البشرية المؤهلة لتنفيذ هذه الاستراتيجية. وبالتالي، تؤكد هذه الدراسة أن تأثير تطبيق الاستراتيجية الوطنية للأمن السيبراني في التقليل من المخاطر المتعلقة بنظم المعلومات المحاسبية يعتبر جانباً محوريًا في القطاعات الحكومية السعودية نظرًا للدور الحيوي الذي تلعبه المعلومات المحاسبية في الإدارة.

توصيات الدراسة

في ضو ء ما توصلت إليه الدراسة من نتائج يمكن التوصية بما يلي:

1. تطوير وتعزيز السياسات والإجراءات الأمنية في القطاعات الحكومية ومراجعتها بانتظام لمواكبة التطورات في مجال الأمن السيبراني وبما يتوافق مع متطلبات الاستراتيجية الوطنية للأمن السيبراني، والتحقق الدوري والتقييم الشامل للنظم المحاسبية وتحديد الثغرات.
2. الاهتمام بتدريب الكوار البشرية على السلوكيات الأمنية الجيدة وإجراء دورات تدريبية دورية لموظفي القطاعات الحكومية حول أهمية الأمن السيبراني وكيفية التعامل مع المخاطر.
3. تعزيز التوعية بأهمية الأمن المعلوماتي والمخاطر المحتملة لنظم المعلومات المحاسبية من خلال تنظيم عدد من الحملات التوعوية الدورية.
4. الاستثمار في أحدث تقنيات الأمن السيبراني لحماية نظم المعلومات المحاسبية من الهجمات، وضمان تطبيق تقنيات التحليل والكشف المتقدم عن الاختراقات والتهديدات الأمنية والتعامل معها بشكل فوري وفعال.
5. الاستفادة من الخبرات الدولية وتبادل المعرفة وأفضل الممارسات في مجال الأمن السيبراني.

الدراسات المستقبلية

1. دراسات مقارنة: إجراء دراسات مقارنة مع دول أخرى للتعرف على أفضل الممارسات في تطبيق استراتيجيات الأمن السيبراني.
2. تحليل البيانات الضخمة: استخدام تقنيات البيانات الضخمة لتحليل الحوادث الأمنية وتطوير استراتيجيات استباقية للحماية من الهجمات المستقبلية.
3. تقييم الأثر الاقتصادي: دراسة الأثر الاقتصادي للهجمات السيبرانية على القطاعات الحكومية وكيفية تحسين الاستراتيجية لتقليل هذه التكاليف.
4. التكامل مع الذكاء الاصطناعي: بحث دور الذكاء الاصطناعي في تعزيز الأمن السيبراني لنظم المعلومات المحاسبية وتطوير أنظمة أمنية تعلمية وتكيفية.

المراجع

المراجع العربية

- احمد، سهير. (2022). إدارة المخاطر بشركات التأمين على الممتلكات والمسئولية المسجلة بالبورصة المصرية باستخدام اختبارات الضغوط .*المجلة العلمية للاقتصاد والتجارة*، 52(4)، 271-298.
- الاستراتيجية الوطنية للأمن السيبراني – ٢٠١٧-٢٠٢١م.
- إسماعيل، خليل ونعوم، ريان (2012). الخصائص النوعية للمعلومات المحاسبية بين النظرية والتطبيق. مجلة كلية بغداد للعلوم الاقتصادية، (30)
- أنيس، أ. كليبات محمد، عمر و د. بنية. (2018). مخاطر استخدام نظم المعلومات المحاسبية الالكترونية وأثرها على فاعلية المراجعة في الجزائر. الإطار العام لنظام المعلومات المحاسبية، نظم المعلومات المحاسبية (1) – المستوى الثاني – الفصل الدراسي الأول (كود 136)، صفحة 27-29.
- البابلي، عمار ياسر محمد زهير. (2021). التحديات الأمنية المعاصرة للهجمات السيبرانية. الفكر الشرطي، مج30, ع118، 19 – 83.
- بوقرة، سامية. (2014)، تطور استخدام تكنولوجيا المعلومات والاتصال والأمن المعلوماتي في المؤسسة دراسة ميدانية بمؤسسة مطاحن سيبوس -عنابة، *مجلة علوم الإنسان والمجتمع*، المجلد (3)، العدد (4)، ص 555-579.
- التيماني، مداخل زيد عبد الرحيم. (2021). واقع الوعي المعلوماتي بالأمن السيبراني لدى الأفراد في المجتمع السعودي كما يدركها الخبراء المختصين بالأمن السيبراني. مجلة الخدمة الاجتماعية، ع67ج، 1 – 23.
- حسين، محمود محمد عبد الرحيم. (2020). الدور التأثيري لحوكمة تكنولوجيا المعلومات كمتغير وسيط في العلاقة بين المراجعة الداخلية كنشاط مضيف للقيمة والحد من مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة ميدانية. *مجلة الدراسات والبحوث المحاسبية*، ع2، 19 - 93.
- حمد، معاذ أحمد عبد الرازق، وأحمد، نصر الدين حسن. (2016). أمن المعلومات ودوره في الحد من القرصنة الإلكترونية المركز القومي للمعلومات: دراسة حالة (رسالة ماجستير غير منشورة). جامعة أم درمان، السودان.
- حمود، لبنى (2023). إدارة المخاطر في المؤسسات الحكومية: الدليل الشامل. مجموعة ريناد المجد لتقنية المعلومات .RMG https://www.rmg-sa.com/
- خليفات، شهناز والقضاة، ليث (2021). أثر سياسات تدقيق أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية في المؤسسات الحكومية المستقلة الأردنية. مجلة العلوم الإدارية والاقتصادية، 14(2)، 21–53.
- سامح، رفعت. وأبو حجر، أمينة. ومحمد، عبد العزيز. (2014)، آليات حوكمة تكنولوجيا المعلومات في تخفيض مخاطر أمن المعلومات للحد من التلاعب المالي الالكتروني في الوحدات الحكومية في ظل الحوكمة الإلكترونية، المؤتمر الخامس حول المحاسبة في مواجهة التغيرات السياسية والاقتصادية المعاصرة.
- السرحان، حنين عبد المهدي سالم، والمشاقبة، محمد ناصر موسى حمدان. (2020). أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية (رسالة ماجستير غير منشورة). جامعة آل البيت، المفرق.
- سليمان، م. (2022). نظرية الأنشطة الروتينية: نظرية جديدة لفهم الجرائم السيبرانية. المجلة المصرية للعلوم الاجتماعية والسلوكية, 6(6) , 114-130.
- شلوش، نورة. (2018). القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول. مجلة مركز بابل للدراسات الإنسانية، مج8, ع2، 185 – 206.

- العطار، حيدر (2018). فعالية المعلومات المحاسبية والشفافية للقوائم في تفعيل المحتوى الإعلامي للتقارير المالية الشركات دراسة تطبيقية لعينة من الشركات في سوق العراق لأوراق المالية. مجلة المثنى للعلوم الإدارية والاقتصادية، 8(3).
- العلمي، حسام. (2015). دور نظم المعلومات المحاسبية المحوسبة في كفاءة وفعالية التدقيق الخارجي، دراسة تطبيقية على مكاتب تدقيق الحسابات العاملة في المحافظات الجنوبية، رسالة ماجستير، كلية التجارة، جامعة غزة، فلسطين.
- العوامري، عبير والملاح شيرين وخليل علي (2022). أثر تكامل حوكمة أمن المعلومات وخدمات تأكيد الثقة على الحد من مخاطر نظم المعلومات المحاسبية الالكترونية. رسالة للماجستير، جامعة بنها.
- العويمر, محمد حمد ومشرف ،طارق محمد.(2018). دور تقييم المخاطر في أمن المعلومات (رسالة دكتوراة)، جامعة نايف العربية للعلوم الأمنية.
- قراطم، خالد وعون، محمد وفرحات محمد (2022). أثر جودة المعلومات المحاسبية التي يقدمها النظام المحاسبي على اتخاذ القرارات بمصنع إسمنت زليتن. مجلة العلوم الإنسانية والطبيعية، العدد 9 المجلد 3.
- القرشي، محمد. (2019)، تحليل مخاطر أمن نظم المعلومات المحاسبية المحوسبة في شركات الاتصالات المسأهم ة السعودية: دراسة ميدانية، رسالة ماجستير، جامعة الملك عبد العزيز، المملكة العربية السعودية.
- كمال، اكرم. (2021). مدى تطابق إجراءات الرقابة المالية في النظام المحاسبي الحكومي بمصر لمبادئ الأجهزة العليا للرقابة المالية. مجلة البحوث المالية والتجارية, 22(العدد الأول-الجزء الثاني)، 62-81.
- محمود، لمى عبد الباقي، وكيطان، إسراء نادر. (2021). المسؤولة الدولية عن الأضرار التي تحدثها الهجمات الإلكترونية. مجلة العلوم القانونية، مج36, عدد خاص، 336 – 362.
- المري، محمد. (2023). أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية. *مجلة البحوث الفقهية والقانونية*، (40)40، 1303-1373.
- الهيئة الوطنية للأمن السيبراني (2019). الضوابط الأساسية للأمن السيبراني. مسترجع من https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf?fbclid=IwAR1Iw1iiLHkVbe3XXB7WsTV9pLnoZhgMmTbN5WQIwxMas3OokzpI23OZEHs

المراجع الأجنبية

- Ali, O. A. M., Matarneh, A. J., Almalkawi, A., & Mohamed, H. (2020). The impact of cyber governance in reducing the risk of cloud accounting in Jordanian commercial banks from the perspective of Jordanian auditing firms. *Modern Applied Science*, 14(3), 75-89.
- Almomani, S. N., Shehab, M., Al Ebbini, M. M., & Shami, A. A. (2021). The efficiency and effectiveness of cyber security in maintaining the cloud accounting information. *Academy of Strategic Management Journal*, 20, 1-11.
- Cascio, W. & Montealegre, R. (2016). How Technology Is Changing Work and Organizations. Annual Review of Organizational Psychology and Organizational Behavior. 3. 349-375. 10.1146/annurev-org psych-041015-062352.
- Ehioghiren, E., Ojeaga, J., and Eneh, O. (2021). Cyber security: the perspective of accounting professionals in Nigeria. In: Accounting and taxation review 5 (2), S. 15 – 29.
- Kasasbeh, F. I. O., & Thuneibat, N. S. M. (2018). The Ability of Computerized Accounting Information Systems in Saudi Public Universities to Face Cyber Threats. International Review of Management and Marketing, 8(3), 19.
- Li, H., No, W. and Wang, T. (2018), "SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors", International Journal of Accounting Information Systems, Vol. 30, pp. 40-55.
- Lin, Z., Sapp, T. R., Ulmer, J. R., & Parsa, R. (2019). Insider Trading Ahead of Cyber Breach Announcements. Journal of Financial Markets, 100527.
- Samimi, A. (2020). Risk Management in Information Technology. *Progress in Chemical and Biochemical Research*, 3(2), 130-134.