Tikrit Journal of Administrative and Economics Sciences
مجلة تكريت للعلوم الإدارية والاقتصادية
EISSN: 3006-9149
PISSN: 1813-1719

The impact of developing accounting education curricula on the labor market in light of the Iraqi cybersecurity strategy: A prospective study of a sample of academics in Iraqi universities

Rafi Nazar Jameel*
College of Administration and Economics/University of Mosul

Keywords:
Development of accounting education curriculum, Iraqi Cyber Security Strategy.

Article history:
Received 10 Dec. 2024
Accepted 19 Jan. 2025
Available online 25 Jun. 2025

*Corresponding author:
Rafi Nazar Jameel
College of Administration and Economics/University of Mosul

Abstract: The research aimed to identify the areas of the Iraqi cybersecurity strategy, which contained (8) areas: (effective governance, legislative and regulatory framework, cybersecurity technology framework, cybersecurity culture and capacity building, research and development towards self-reliance, compliance and implementation, preparedness for cybersecurity incidents, international cooperation) and What is its impact on the labor market in the case of developing accounting education curricula?. From this standpoint, the research problem was to research the type of relationship and impact between developing accounting education curricula according to those areas (8) on the labor market and what are the considerations for developing accounting curricula in Iraq. The general research objective is to present a mechanism for adapting cybersecurity in accounting education, such as protecting financial information and data for entities, individuals and the state, and reducing their exposure to hacking. In this regard, this research focused on shedding light on this objective by taking the opinions of a sample of academics in Iraqi universities specializing in accounting and cybersecurity by designing a questionnaire using (Google Form) and distributing it to the research sample, which numbered (87) respondents. It includes four axes: first one: is specific to the areas of the Iraqi cybersecurity strategy. Second one: is specific to developing accounting education curricula in Iraq. Third one: is specific to the labor market. Fourth one: is specific to considerations for developing accounting curricula according to the Iraqi

	cybersecurity strategy. Then, their answers to those four axes are analyzed after giving weights to the responses according to a five-rank Likert scale to measure the answers to the questions of the questionnaire axes. Using descriptive statistical analysis methods in the answers of the research sample, the research has produced several results, the most important of which are: There is a relationship and a positive impact with statistical significance between the areas of the Iraqi cybersecurity strategy and the labor market. There is a relationship and an impact with a positive statistical significance between the development of accounting education curricula "according to the areas of cybersecurity" and the labor market. There are important considerations that should be taken into account when designing accounting curricula according to the areas of cybersecurity in a series, namely: training and continuous improvement of the teaching staff, including cybersecurity concepts in the curricula, evaluating and analyzing the effectiveness of the curricula, using simulations and media. Multiple, using interactive and applied methods to teach cybersecurity concepts, using self-learning and active learning. The most important recommendations were: including cybersecurity concepts in accounting curricula, such as the need to know networks, artificial intelligence, cloud computing, secure communications and encryption according to an international standard framework to evaluate the outcomes of this development of curricula, strengthening the research community in the field of cybersecurity and its relationship to accounting, especially at the postgraduate level, active participation in all international events, conferences and forums related to cybersecurity and its relationship to accounting, and hosting international and regional conferences and workshops in this field.

انعكاس تطوير مناهج التعليم المحاسبي على سوق العمل في ظل استراتيجية الامن السيبراني العراقي: دراسة استطلاعية لعينة من الأكاديميين في الجامعات العراقية

رافي نزار جميل
كلية الادارة والاقتصاد/جامعة الموصل

المستخلص

هدف البحث إلى التعرف مجالات استراتيجية الأمن السيبراني العراقية التي احتوت على (8) مجالات هي (الحوكمة الفعالة، الاطار التشريعي والتنظيمي، اطار تكنلوجيا الأمن السيبراني، ثقافة الأمن السيبراني وبناء القدرات، البحث والتطوير نحو الاعتماد على الذات، الامتثال والتنفيذ، الجاهزية لحوادث الامن السيبراني، التعاون الدولي) وما هو أثرها في حالة تطوير مناهج التعليم المحاسبي على سوق العمل ؟، ومن هذا المنطلق كانت مشكلة البحث هي البحث في نوع العلاقة والأثر بين تطوير مناهج التعليم المحاسبي وفق تلك المجالات (8)على سوق العمل وماهي اعتبارات تطوري المناهج المحاسبية في العراق، إذ يأتي هدف البحث العام، بعرض الية تكييف الأمن السيبراني في التعليم المحاسبي مثل حماية المعلومات المالية والبيانات للكيانات والأفراد والدولة، والحد من تعرضها للاختراق، وفي هذا الصدد ركز هذا البحث على تسليط الضوء على هذا الهدف من خلال أخذ آراء عينة من الاكاديميين في الجامعات العراقية لتخصص المحاسبة وتخصص الأمن السيبراني من خلال تصميم استمارة استبيان باستخدام Google Form وتوزيعها على عينة البحث البالغ عددهم (87) مبحوث، إذ تضمن أربعة محاور: الأول: خاص بمجالات استراتيجية الأمن السيبراني العراقي والثاني: خاص بتطوير مناهج التعليم المحاسبي في العراق والثالث: خاص بسوق العمل والرابع: خاص باعتبارات تطوير المناهج المحاسبية وفق لاستراتيجية الأمن السيبراني العراقي ومن ثم تحليل اجاباتهم عن تلك المحاور الأربعة بعد اعطاء أوزان للاستجابات وفقا لمقياس (Likert) خماسي الرتب لقياس اجوبة الأسئلة لمحاور الاستبانة وباستخدام أساليب التحليل الاحصائي الوصفية في اجابات عينة البحث، قد خرج البحث بنتائج عدة أهمها: يوجد علاقة وأثر ايجابي ذات دلالة احصائية بين مجالات استراتيجية الأمن السيبراني العراقي وسوق العمل، يوجد علاقة وأثر ذات دالة احصائية ايجابية بين تطوير مناهج التعليم المحاسبي " وفق مجالات الأمن السيبراني " وسوق العمل وهناك اعتبارات مهمة ينبغي أخذها بنظر الاعتبار عند تصميم مناهج محاسبية وفق مجالات الأمن السيبراني متسلسلة وهي: التدريب والتحسين المستمر للكادر التدريسي، تضمين مفاهيم الأمن السيبراني في المقررات الدراسية، تقييم وتحليل فعالية المناهج، استخدام المحاكاة والوسائط المتعددة، استخدام أساليب تفاعلية وتطبيقية لتعليم مفاهيم الأمن السيبراني، استخدام التعلم الذاتي والتعلم النشط أما أهم التوصيات فكانت: تضمين مفاهيم الأمن السيبراني في المقررات الدراسية لتخصص المحاسبة مثل الحاجة إلى معرفة الشبكات والذكاء الاصطناعي والحوسبة السحابية والاتصالات الآمنة والتشفير وفق اطار معياري دولي لتقييم مخرجات هذا التطوير للمناهج، تعزيز مجتمع الأبحاث في مجال الأمن السيبراني وعلاقته في المحاسبة خصوصا على مستوى الدراسات العليا، المشاركة الفعالة في جميع الفعاليات والمؤتمرات والمنتديات الدولية المتعلقة بالأمن السيبراني وعلاقته بالمحاسبة واستضافة مؤتمرات وورش دولية واقليمية في هذا المجال.

الكلمات المفتاحية: تطوير منهاج التعليم المحاسبي، استراتيجية الأمن السيبراني العراقي.

المقدمة

الأمن السيبراني أصبح أمرًا بالغ الأهمية في عالمنا بشكل عام وفي عالم المال والأعمال بشكل خاص وإن المنهاج الدراسية الذي يتم تطويرها في ضوء التغيرات التكنولوجية توفر كفاءة وفاعلية فرعية أساسية ولكنها في الوقت نفسه وظيفية يحتاج الطلاب إلى إظهارها عند استخدام التكنولوجيا وتمكنهم من استخدامها من حيث الاحتياجات الفردية والمؤسسية على المستوى المطلوب. وإن احتواء مجالات الأمن السيبراني العراقي على مجالات تشير أغلبها بطريقة أو بأخرى إلى ضرورة تطوير المناهج الدراسية يعتبر ضرورة لقيام بالبحث في هذه المسالة قدر تعلق الأمر بتطوير مناهج التعليم المحاسبي في ضوء تلك المجالات إذ إن وجود برنامج تعليمي محاسبي أكثر فعالية حول المعرفة التكنولوجيا أصبح الآن جزء لا يتجزأ من المناهج الدراسية في الدول المتقدمة. ومن أجل فحص مستوى منهج تعليم المحاسبة في برامج البكالوريوس وحتى في الدراسات العليا في ضوء الأمن السيبراني في القطاع العام والخاص فهناك ضرورة لتقديم تقييم لمنهج التعليم المحاسبي واكتشاف ما إذا كان متوافقًا مع مسؤوليات القطاع العام والخاص فيما يتعلق باستخدام التكنولوجيا بشكل عام والأمن السيبراني بشكل خاص.إذ إن الهدف من المحاسبة في نهاية المطاف هو قيمة المعلومات، وهنا ينبغي أن يكتسب التعليم المحاسبي عمقًا في مجال الأمن السيبراني، أي السؤال هو ما يجب أن يكون عليه منهج تعليم المحاسبة من أجل الاستجابة لاحتياجات الأمن السيبراني؟ وفي ضوء ذلك جاء هذا البحث في متغيراته الثلاثة وهي مجالات استراتيجية الأمن السيبراني العراقي كمتغير مستقل وتطوير مناهج التعليم المحاسبي كمتغير وسيط وسوق العمل كمتغير تابع، إذ تم تقسيم البحث على خمسة محاور شمل الأول منهجية البحث والثاني شمل استراتيجية الأمن السيبراني العراقي والمحور الثالث شمل على التعليم المحاسبي والأمن السيبراني واتجاهات سوق العمل والمحور الرابع اختص بالدراسة الميدانية والتي في نهاية الأمر ركزت على أهمية وكيفية واعتبارات إضافة تطوير مناهج التعليم المحاسبي في العراق في ظل مجالات الأمن السيبراني ليواكب احتياجات السوق المتغيرة وهذه المسألة تستحق البحث فيها بتكييف التعليم المحاسبي مع التطورات الجديدة واحتياجات السوق. ومع ذلك، فمن الممكن أن يتم تشكيل المناهج وفقًا لمعايير مختلفة لتلبيه هذا المطلب.

المحور الاول
منهجية الدراسة

1-1. مشكلة البحث: جاء هذا البحث كمحاولة للمساهمة في تطوير المناهج التعليمية لتخصص المحاسبة في ظل مجالات استراتيجية الامن السيبراني العراقية عدد (8) وهي: (الحوكمة الفعالة، الإطار التشريعي والتنظيمي، إطار تكنولوجيا الأمن السيبراني، ثقافة الأمن السيبراني وبناء القدرات، البحث والتطوير نحو الاعتماد على الذات، الامتثال والتنفيذ، الجاهزية لحوادث الأمن السيبراني، التعاون الدولي)، وأثر ذلك على سوق العمل في ظل التهديدات التي قد تواجهها الكيانات، ومن هذا المنطلق تكمن مشكلة البحث من خلال طرح الأسئلة الآتية:

السؤال الأول: هل هناك علاقة أثر ذات دلالة احصائية بين مجالات الأمن السيبراني العراقية (الحوكمة الفعالة، الإطار التشريعي والتنظيمي، اطار تكنولوجيا الأمن السيبراني، ثقافة الأمن السيبراني وبناء القدرات، البحث والتطوير نحو الاعتماد على الذات، الامتثال والتنفيذ، الجاهزية لحوادث الأمن السيبراني، التعاون الدولي) وسوق العمل؟

السؤال الثاني: هل هناك علاقة أثر ذات دلالة احصائية بين تطوير مناهج التعليم المحاسبي وفق استراتيجية الأمن السيبراني العراقية على سوق العمل؟

السؤال الثالث: هل هناك اعتبارات يجب اتخاذها عند تطوير المناهج المحاسبية وفقا لاستراتيجية الأمن السيبراني العراقي؟

2-1. أَهداف البحث: إن الخطوة الأولى والأكثر أهمية انطلاقًا من معرفة بأن الأشخاص الذين يتمتعون بخبرة جيدة في مجالات عملهم المختلفة، يمكن تدريبهم لتنمية قدراتهم من الناحية النظرية والتطبيقية، وقدر تعلق الأمر بمهنة وعلم المحاسبة يجب أن يكون موظفو المحاسبة في المستقبل على دراية جيدة ومجهزين فيما يتعلق بأساسيات الأمن السيبراني المطلوبة خصيصًا لمهنتهم، وعلى هذا الأساس فأن هدف هذا البحث يمكن أن يتلخص بالآتي:

1. تقديم مساهمة لأصحاب القرار المعنيين بكيفية تشكيل مناهج التعليم المحاسبي والتعليم السيبراني للمستقبل على شكل هجين بين الاثنين، من حيث الخبراء بالأمن السيبراني الذين لديهم إمكانية رؤية وتقييم العملية بشكل مباشر مع المتخصصين الأكاديميين في المحاسبة والأمن السيبراني.
2. بيان العلاقة والأثر بين مجالات استراتيجية الأمن السيبراني العراقية ومناهج التعليم المحاسبي.
3. بيان مدى ضرورة الوعي بالأمن السيبراني في مجال المحاسبة وأهمية ذلك على سوق العمل.
4. بيان الاعتبارات الواجب اتخاذها عند تطوير مناهج التعليم المحاسبي وفق الأمن السيبراني.

3-1. أَهميَّة البحث: على الرغم من تزايد استخدام التكنولوجيا وضرورتها في مهنة المحاسبة، فأن محتوى الدورات التي يتم تدريسها في التعليم المحاسبي فيما يتعلق بالمخاطر التكنولوجية والأمن السيبراني غير مرضٍ إلى حد ما. ففي الممارسة المحاسبية العملية والتعلمية، يجب القضاء على أوجه القصور في كليهما. ومن هذا المنطلق يمكن تحديد أهمية البحث بالنقاط الآتية:

1. تسليط الضوء على موضوع مهم وهو الربط بين تطوير مناهج التعليم المحاسبي مع مجالات استراتيجية الأمن السيبراني العراقي والتي من ضمن مجالاتها هو التركيز على تطوير المناهج التعليمية.
2. هناك حاجة إلى موارد بشرية مؤهلة لتقييم كيفية استخدام التقنيات الجديدة في سوق العمل. لذلك، وفي ضوء الابتكار التكنولوجي، يُعتقد أنه من الأهمية إعادة تصميم المناهج التعليمية في هذه العملية وتكييفها مع الاحتياجات المتغيرة وخاصة فيما يتعلق بتكييفها مع التعليم المحاسبي.
3. وجود برنامج أكثر ذكاءً وفعالية حول معرفة التكنولوجيا هو الآن جزء لا يتجزأ من المناهج الدراسية العالمية فمن المهم بمكان تقييم لمناهج تعليم المحاسبة في العراق واكتشاف ما إذا كانت متوافقة مع مسؤوليات القطاع العام وحتى الخاص فيما يتعلق باستخدام التكنولوجيا والأمن السيبراني.

4-1. فرضيات البحث: يقوم البحث بإطار ما يقدمه من تفسيرات باختبار الفرضيات الرئيسة الآتية:

الفرضية الأولى: هناك علاقة وأثر ذات دلالة احصائية بين مجالات استراتيجية الأمن السيبراني العراقية (الحوكمة الفعالة، الإطار التشريعي والتنظيمي، إطار تكنولوجيا الأمن السيبراني، ثقافة الأمن السيبراني وبناء القدرات، البحث والتطوير نحو الاعتماد على الذات، الامتثال والتنفيذ، الجاهزية لحوادث الأمن السيبراني، التعاون الدولي) وسوق العمل.

الفرضية الثانية: هناك علاقة أثر ذات دلالة احصائية بين تطوير مناهج التعليم المحاسبي وفق استراتيجية الأمن السيبراني العراقية وسوق العمل.

الفرضية الثالثة: هناك اعتبارات ينبغي مراعاتها عند تطوير المناهج المحاسبية وفق لاستراتيجية الأمن السيبراني العراقي.

1-5. منهج البحث: اعتمد البحث في جانبه النظري على المنهج الوصفي، من خلال الرجوع إلى الوثائق الرسمية (استراتيجية الأمن السيبراني العراقي- 2017) وغيرها والكتب والدوريات والمؤتمرات والرسائل والأطاريح والكتب والدوريات والمؤتمرات والندوات فضلًا عن المواقع الإلكترونية، فضلا عن اعتماد المنهج الاستنباطي من خلال الدراسة الاستطلاعية التي قام بها الباحث والخاصة بتجميع البيانات المتعلقة بموضوع البحث ومن ثم تحليل النتائج التي تم التوصل إليها اعتمادا على استمارة الاستبانة التي تم توزيعها على العينة الخاصة بالبحث.

1-6. مجتمع وعينة البحث: تمثل مجتمع البحث بالأكاديميين في الجامعات والمعاهد العراقية من تخصص المحاسبة والأمن السيبراني وكانت عينة البحث هي اختيار عينة عشوائية من مجتمع الدراسة من بعض الأكاديميين في الجامعات والمعاهد العراقية.

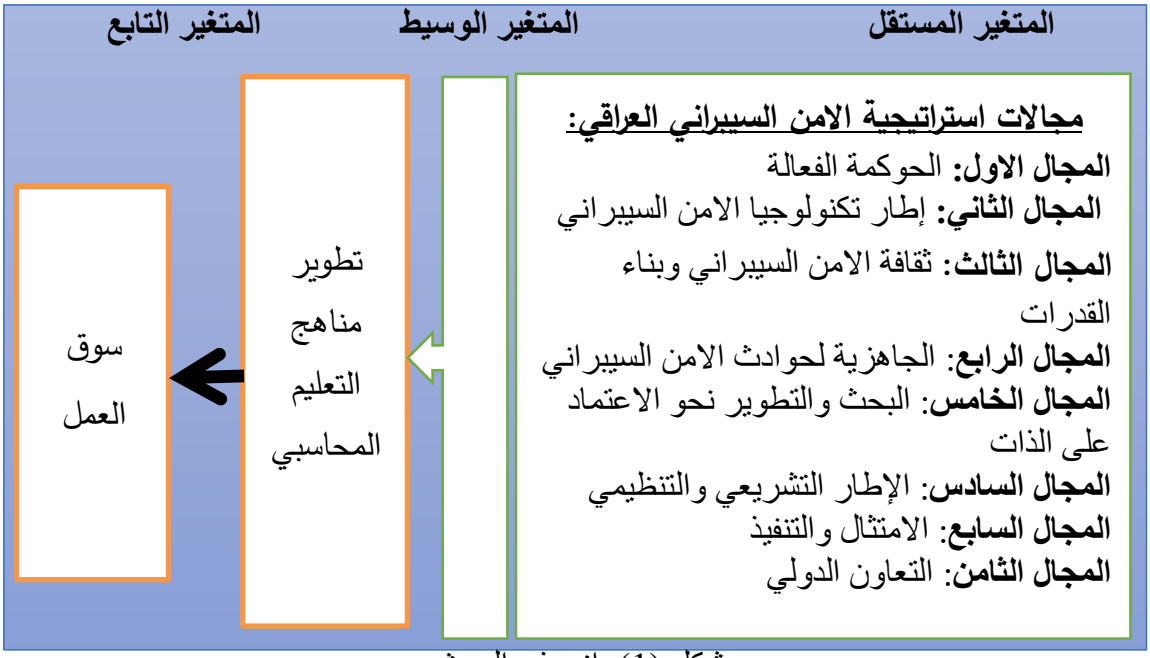
1-7. حدود البحث

1-7-1. الحدود الموضوعية: شملت الحدود الموضوعية للبحث هي التطرق إلى موضوع الأمن السيبراني بالتركيز على استراتجية الأمن السيبراني العراقي، وتطوير مناهج التعليم المحاسبي.

1-7-2. الحدود المكانية والزمانية: تمت الدراسة الميدانية للبحث في العراق (بعض الجامعات العراقية) خلال عام 2023-2024.

1-7-3. الحدود البشرية: تمثلت الحدود البشرية للبحث بعينة من الأكاديميين من تخصص المحاسبة وتخصص الأمن السيبراني العاملين في الجامعات والمعاهد العراقية.

1-8. انموذج البحث: اعتمد هذا البحث على المنهج التحليل الوصفي، كونه يناسب موضوع البحث ومتغيراته بهدف معرفة وجهات النظر لعينة البحث من الأكاديميين وذلك من خلال تحديد ثلاثة متغيرات وكما موضح في الشكل رقم (1) الآتي:



شكل (1): انموذج البحث

المصدر: من اعداد الباحث.

المحور الثاني
استراتيجية الأمن السيبراني

2-1. المفهوم: تتحول العديد من القطاعات الفرعية مثل الكمبيوتر والشبكات والاتصالات والهواتف المحمولة والأنظمة المخصصة وترددات الراديو واللاسلكية وأنظمة الألياف الضوئية وأنظمة شبكات الاتصال المتصلة ببعضها البعض عبر الإنترنت إلى أنظمة سيبرانية. (Apostolou & others, 2020: 4). يشير مفهوم الأدوات الرقمية المستخدمة في أعمال الشركات إلى مجال الأمن السيبراني الذي يتم فيه ضمان سرية البيانات وسلامتها وإمكانية الوصول إليها مع استخدام تقنيات مختلفة للاتصال وتخزين البيانات، ففي اللغة الفنية، يُطلق على الاعتماد على تكنولوجيا المعلومات والاتصالات لمنع وحماية وكشف وإزالة واستعادة أي خرق في البنية التحتية للمعلومات "الأمن السيبراني". (Jha, 2023: 3)، في حين أن مصطلح الأمن السيبراني يكشف عمومًا عن التحكم في التهديدات وحمايتها واكتشافها في مستويات السرية والنزاهة وإمكانية الوصول إلى البيانات والمعلومات، يتم تحديد ثلاثة مفاهيم، وأحيانًا يتم وصفها بأربعة للأمن السيبراني، وهي ضمان المعلومات وأمن المعلومات وأمن البنية التحتية للمعلومات. في هذا السياق، يشتمل نطاق الأمن السيبراني على كل من سرية المعلومات المشتركة في البيئات الآمنة في الفضاء الإلكتروني وأمن البنية التحتية التي تسمح بالوصول إلى هذه المعلومات.(Yee & Zolkipli, 2021: 4) كما عرف الأمن السيبراني من قبل مستشارية الأمن الوطني العراقي بأنه هي استيراتيجة الاستعداد الوطني لتوفير تدابير متماسكة واجراءات استراتيجية لضمان أمن وحماية الوجود العراقي في الفضاء السيبراني، وحماية البنية التحتية الحيوية للمعلومات، وبناء ورعاية مجتمع انترنيت موثوق به (استراتيجية الأمن السيبراني العراقي،1،2017) وعرف أيضا بأنه كافة الاجراءات الادارية والتقنية المتخذة بغرض حماية النظم والشبكات المعلوماتية والبينات والمعلومات من المخاطر الناتجة عن استخدام تقنيات المعلومات (السقا والبرزنجي،2023: 100).

يرى الباحث من خلال ما تقدم أنه يمكن تعريف الأمن السيبراني بأنه كل التدابير التي يجب اتخذاها من قبل الأشخاص والمؤسسات والدولة لمنع حصول أية جرائم إلكترونية ضدهم.

2-2. مخاطر الأمن السيبراني – نظرة عامة: في مجال المال والأعمال، يمكن أن تتسبب مخاطر الأمن السيبراني في أضرار مالية واضرار في سمعة الشركات والمجتمع التي تعمل به أيضا تلك الشركات فضلا عن هناك أيضًا مخاطر سياسية متضمنة بهذا الشان، إذ تتراكم من خسائر وسلبيات عديدة مثل الاحتيال أو الهجمات الإلكترونية. على سبيل المثال، تسبب الهجوم الإلكتروني لعام 2016 بفيروس Petya في تكاليف شحن Maersk Line بقيمة 300 مليون دولار (Tuomala, 2021: 5)، ففي مجال المحاسبة أيضا تشمل اختراق البيانات والاحتيال الإلكتروني واختراق الأنظمة المحاسبية، وهذا يتطلب تطوير برامج عديدة ومنها تركز على حماية المعلومات المالية والتحليل الجنائي الرقمي واعتماد أساليب الوقاية والدفاع السليمة فبالتأكيد أن يكون تهديد الاحتيال الالكتروني مهمًا لمستخدمي البيانات المالية أي ليست خاصة بتخصص المحاسبة فقط، لكنها تحظى بشعبية كبيرة في المجال عليه تبحث العديد من الشركات بالفعل عن موظفين للعمل في مجالات مختلفة من المحاسبة والتمويل متمتعة بمهارات الأمن السيبراني (Yang & Lee, 2022: 5).

يرى الباحث من خلال ما تقدم بأن مخاطر الأمن السيبراني في مجال المحاسبة تكمل في اختراق البيانات والاحتيال الإلكتروني واختراق الأنظمة المحاسبية، وهذا يتطلب تطوير مناهج

تعليمية تركز على حماية البيانات والمعلومات المالية واعتماد أساليب الوقاية والدفاع السليمة هذا من جانب، ومن جانب آخر فضلا وجود نقاط الضعف الشائعة في النظم المحاسبية والرقابية تتضمن قدرة الدخول غير المصرح به إلى النظام، وضعف في إجراءات التحقق من الهوية، ونقص في تحديثات البرامج والأجهزة، مما يتطلب تصميم مناهج تعليمية وانظمة محاسبية تركز على تعزيز الجوانب الأمنية وإجراءات الوقاية والحماية.

2-3. عناصر الأمن السيبراني: يشكّل الأمن السيبراني جزءًا حيويًا من عالم التكنولوجيا الحديثة، إذ يعمل على حماية الأنظمة الإلكترونية والشبكات من التهديدات السيبرانية، وتتضمن عناصر الأمن السيبراني جوانب عدة مختلفة التي يجب مراعاتها. بتصرف من الباحث بالاعتماد على (Ofoegb & Osundare, 2024: 6) (https://www.elnooronline.net)

1. **أمن التطبيقات:** يتعلق أمن التطبيقات بحماية البرامج والتطبيقات الخاصة بالشركة أو المؤسسة، ويجب ضمان أن البرمجيات المستخدمة في الشركة تتوافق مع معايير الأمان المعتمدة وأنها خالية من الثغرات المعروفة. يكون ذلك من خلال إجراء فحوصات أمنية واختبارات التآمن للتأكد من عدم وجود ثغرات قد يستغلها المهاجمون.
2. **أمن الشبكات:** يتعلق أمن الشبكات بحماية البنية التحتية للشبكات والأنظمة المتصلة بها، فبعد أن يتم تأمين نقاط الدخول إلى الشبكة، يصبح بالإمكان حماية المعلومات المخزّنة والمرسلة في طرق مؤمنة.
3. **الأمن التشغيلي:** يتعلق الأمر بضمان استمرار وثبات عمل الأنظمة والخدمات التكنولوجية، ويشمل ذلك تنفيذ احتياطات للتعامل مع أي انقطاعات طارئة أو خلل في العمل، وكذلك تحديث البرمجيات والأجهزة بشكل مستمر لحمايتها من التهديدات الجديدة.
4. **أمن التعافي من الكوارث:** يشير أمن التعافي من الكوارث إلى إجراءات الاحتياطات والاستعداد التي يجب اتخاذها للتعامل مع الحوادث السيبرانية، ويشمل ذلك إنشاء نسخ احتياطية للمعلومات والنظم، وتطوير خطط حماية واستعادة بعد الكوارث.
5. **أمن المعلومات:** يتمثل أمن المعلومات في حماية سرية وسلامة المعلومات الحساسة والهامة للشركة أو المؤسسة، ويجب تنفيذ سياسات صارمة لإدارة وحماية هذه المعلومات، وذلك من خلال تحديد حقوق الوصول وإجراءات الحماية المعتمدة وتشفير البيانات.

2-4. أنواع هجمات الأمن السيبراني: يتعامل الأمن السيبراني مع مستويات مختلفة من الخطر ومنها الآتي (Shruti M., 2024: 1):

1. **البرامج الضارة:** تشير إلى أشكال مختلفة من البرامج التي تغير طريقة عمل الأجهزة، ومجرد تثبيتها، تؤدي مهاما دون علم أو موافقة مستخدمي أجهزة الكمبيوتر أو الهاتف، وذلك للوصول إلى تلك الأجهزة وسرقة البيانات والمعلومات الأخرى بهدف الابتزاز وسرقة الأموال.
2. **برامج الفدية الضارة:** هي نوع من البرامج الضارة التي تصيب أجهزة الكومبيوتر مثلا، وبمجرد دخول هذا البرنامج إلى الجهاز يقوم بتشفير الملفات ويصبح من غير الممكن الوصول إليها، لتطالب بفدية مقابل فك التشفير.
3. **حصان طروادة:** وهو اسم لأكثر البرامج الضارة التي تؤدي إلى خسائر كبيرة مثل سرقة الحسابات المصرفية كونه غير واضح ومن الصعب اكتشافه من قبل المستخدم العادي، إذ يدخل إلى الأنظمة من خلال وسائل يفترض أنها مشروعة.

4. **التصعيد الاحتيالي**: وهو من أشهر الأساليب الهجوم السيبراني حيث يتم من خلالها ارسال رسائل عبر البريد الالكتروني، أو رسائل نصية لخداع المستخدمين للنقر فوق رابط معين أو تنزيل برامج ضارة أو تحويلهم أو نقلهم على مواقع سيئة.
5. **التحايل بالهندسة الاجتماعية:** يمثل شكل من أشكال الهندسة الاجتماعية، يتم من خلالها الحصول على بيانات المستخدمين عبر الاستدراج، من خلال عدد من الخطوات التي قد تؤدي إلى دفع نقدي أو الوصول إلى البيانات السرية عن طريق النقر أيضا على روابط أو تنزيل برامج ضارة.
6. **هجوم التوائم:** يقوم على أساس انشاء نقاط اتصال غير حقيقية من شبكة الواي فاي الأصلية ولكنها تعمل على التنصت على الاتصالات والحصول على معلومات سرية مثل كلمة المرور واسم المرور خاصة بالمستخدمين.
7. **هجوم حجب الخدمة:** يعمل هجوم حجب الخدمة (DoS) على منع المستخدمين من الدخول إلى الموقع الإلكتروني، مما يسبب ضررًا كبيرًا، ويتم ذلك عن طريق توجيه كميات كبيرة من حركة مرور الإنترنت إلى خادم الويب حتى يتم شغلها بالكامل، ليمنع المستخدمين الحقيقيين من الدخول.

2-4. أبعاد الأمن السيبراني: هناك أبعاد عديدة للأمن السيبراني يمكن حصر أهمها بالآتي: (السمحان، 2020: 15)

1. **الأبعاد العسكرية:** تنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجومات السيبرانية وللاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشاة النووية وما قد يحدث عنها من تهديدات لأمن الدول والحكومات مما يؤدي إلى خلل في أنظمتها كافة.
2. **الأبعاد السياسية**: تقوم الأبعاد السياسية للأمن السبراني على أساس أنها جزء مهم من حماية نظام الدولة الساسي وكيانها وخصوصيته، إذ يمكن أن تستخدم التقنيات في بث معلومات أو بيانات قد يحدث من خلالها زعزعة لاستقرار أمن الدولة من خلال وصولها بسرعة إلى عدد كبير من شرائح المجتمع.
3. **الأبعاد الاقتصادية:** يرتبط الأمن السيبراني ارتباطا وثيقا بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد وامن المعلومات فاغلب الدول تعتمد في تعزيز اقتصادها وازدهارها على انتاج وتداول المعرفة والمعلومات على مستويات مختلفة من مفارق الدولة الاقتصادية، مما يبرر الدور المهم للأمن السيبراني في حماية اقتصاد الدولة من الاختراق لأنظمته كافة.
4. **الأبعاد القانونية:** ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقانون، ومع ظهور المجتمع المعلوماتي وتقنياته، ظهرت القوانين الجديدة التي تعد البيئة التنظيمية والتشريعية المنظمة لحماية هذا المجتمع وحفظ التحقيق فيه بأبعاده كافة، إذ يقوم الأمن السيبراني في هذا البعد على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.
5. **البعد الاجتماعي:** هناك من يضيف أيضا البعد الاجتماعي (سالم، 2022: 74) إلى جانب الأبعاد السابقة، إذ تعد الشبكات الدولية للمعلومات مجالا مفتوحا لجميع الاشخاص، إذ يمكن لجميع المتعاملين السيبرانيين أن يستفيدوا من البنى التحية والخدمات المتاحة لهم دون تحمل مخاطر أمنية وهنا يجب معرفة ضرورة الاحساس بأخلاقية الأمن السيبراني. يفوق مستخدمي الانترنيت حاليا أكثر من 4

مليار شخص في العالم منهم 2.6 مليار يستخدمون مواقع التواصل الاجتماعي مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا اتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض اخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنيت، كما يعرض الهويات لعمليات الاختراق الخارجي قد يتسبب بتهديد السلم الاجتماعي للدولة وعليه لابد من العمل على توعية المواطنين بهكذا مخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي.

2-5. استراتيجية الامن السيبراني العراقي – نظرة عامة: نشر مكتب مستشار الأمن القومي استراتيجية الأمن السيبراني العراقي (ICS)، في عام 2017، وكانت هذه الخطوة بمنزلة أول جهد كبير وعام تبذله الدولة العراقية؛ من أجل تحليل مكامن الخلل في السياسة الإلكترونية الوطنية؛ ولرسم خارطة طريق لتأسيس بنية تحتية إلكترونية فوقية للبلاد لوضع العراق على قدم المساواة مع نظرائه الدوليين وحلفائه. شخصت الاستراتيجية السيبرانية العراقية -في خطوة هي الأولى من نوعها- الثغرات في السياسات الإلكترونية للعراق بدقة بوصفها نقطة ضعف هيكلية تتعلَّق بالإهمال البشري، والتدابير غير المدروسة، وتهميش أولوية المجال السيبراني. ومن ثَمَّ، تحدِّد الإستراتيجية جدول أعمال تنفيذية تستند إلى أهداف تنفيذية مدتها عام أو ثلاثة أو خمسة أعوام؛ يشمل تأسيس وكالة إلكترونية فيدرالية، وصياغة القوانين المتعلقة بالفضاء السيبراني إلى «خلق ثقافة الأمن السيبراني»، وشهادات جامعية في الأمن السيبراني. يغطي نطاق الاستيراتيجية الوطنية العراقية للأمن السيبراني **ثمانية مجالات** وطنية عديدة فضلا عن الاطار العام للشراكة والتعاون الدولي بشان الأمن الاسيبراني، إذ تعمل هذه الاستراتيجية على تغطية عدة مجالات خلال السقف الزمني للتنفيذ لهذه الاستراتيجية بثلاث مراحل (المرحلة الأولى خلال سنة واحدة وتشمل معالجة المخاوف الفورية، المرحلة الثانية خلال 3 سنوات وتشمل بناء البنية التحتية، والمرحلة الثالثة خلال 5 سنوات وما بعدها وتشمل تطوير الاعتماد على الذات)، إذ تشمل هذه المجالات الآتي: (استراتيجية الامن السيبراني العراقي، 2017: 8-9)

1. الحوكمة الفعالة
2. الإطار التشريعي والتنظيمي
3. إطار تكنلوجيا الامن السيبراني
4. ثقافة الامن السيبراني وبناء القدرات
5. البحث والتطوير نحو الاعتماد على الذات
6. الامتثال والتنفيذ
7. الجاهزية لحوادث الامن السيبراني
8. التعاون الدولي

فضلا عما تم ذكره سابقا فهناك مؤشرات أخرى للأمن السيبراني عالمية والجدول رقم (1) الآتي يوضح تسلسل العراق عربيا وعالميا ضمن مؤشر الأمن السيبراني (GCI) لغاية عام 2020 ومؤشر الاستعداد التكنلوجي لغاية عام 2023 والمراحل التي وصل اليها في عام ضمن مؤشر (GCI) للعام 2024

جدول (1): مقارنة ترتيب العراق عربيا وعالميا لمؤشر الامن السيبراني ومؤشر الاستعداد التكنلوجي عالميا

ت	الدولة	مؤشر الامن السيبراني (GCI) لغاية عام 2020		مؤشر الاستعداد التكنلوجي عالميا لغاية عام 2023	مؤشر الامن السيبراني (GCI) لغاية عام 2024 عربيا مقسمة على مراحل				
		عربيا	عالميا		مرحلة التأسيس	مرحلة البناء	مرحلة تطوير	مرحلة تقدم	مرحلة تميز
1	المملكة العربية السعودية	1	2	47	اليمن	جزر القمر	الجزائر		البحرين
2	الامارات العربية المتحدة	2	5	37		جيبوتي	الكويت		مصر
3	سلطنة عمان	3	21	64		**العراق**	ليبيا		الاردن
4	مصر	4	23	83		لبنان	تونس		المغرب
5	قطر	5	27	67		موريتانيا			عمان
6	تونس	6	45	66		الصومال			قطر
7	المغرب	7	50	70		فلسطين			السعودية
8	البحرين	8	60	60		السودان			
9	الكويت	9	65	51		سوريا			
10	الاردن	10	71	80					
11	السودان	11	102	163					
12	الجزائر	12	104	97					
13	لبنان	13	109	77					
14	ليبيا	14	113	122					
15	فلسطين	15	112						
16	سوريا	16	126						
17	**العراق**	**17**	**129**	**107**					
18	موريتانيا	18	133	153					
19	الصومال	19	137						
20	جزر القمر	20	174	156					
21	جيبوتي	21	179	150					
22	اليمن	22	182	159					

المصدر: من اعداد الباحث بالاعتماد على(سالم،75،2020)،(Global Cybersecurity Index) (https://cyberspacetrends.com)،2024,27).

يرى الباحث من خلال الجدول السابق رقم (1) أن ترتيب العراق في مؤشر الأمن السيبراني العالمي لسنة 2020 كان 17 عربيا و129 عالميا ونلاحظ أيضا أن ترتيب العراق لمؤشر الاستعداد التكنلوجي عالميا لغاية عام 2023 كان 107، فضلا عن أن العراق في عام 2024 طبقا لمؤشر الأمن السبراني العالمي كان في الترتيب الثالث في مرحلة البناء، وهذا يعد نوعا ما غير جيد بما فيه الكفاية على الأصعدة كافة ومنها التعليمية، إذ جزء من متطلبات تعزيز الأمن السيبراني هو تطوير التعليم والتي منها المناهج الدراسية لتخصص المحاسبة فضلا عن غيرها من التخصصات ذات الصلة.

المحور الثالث

التعليم المحاسبي والأمن السيبراني واتجاهات سوق العمل

3-1. التحولات في سوق العمل والانعكاس على مجال المحاسبة: إن هدف المحاسبة هو توفير المعلومات التي تتمتع بخصائص عديدة ففي النهاية يجب تقديم معلومات مفيدة وفي الوقت نفسه، هناك أيضًا قضية تتعلق بالأمن السيبراني، إذ تكمن أهمية المحاسبة في هذه المواقف في أن يكتسب تعليم المحاسبة عمقًا في مجال الأمن السيبراني (Ramezan, 2023: 4)، وهنا نحتاج إلى معرفة كيف سيتكيف منهج تعليم المحاسبة مع هذه التغييرات وغيرها. إن السؤال حول ما يجب أن يكون عليه منهج تعليم المحاسبة من أجل الاستجابة لاحتياجات السوق هو قضية ذات أهمية (Strang et al., 2020). يغطي تدريب الأمن السيبراني في الغالب علوم الكمبيوتر وأنظمة المعلومات. كيف يجب إضافة عناصر الأمن السيبراني إلى منهج المحاسبة المعد في ضوء احتياجات السوق المتغيرة والتقدم في التخصصات غير المحاسبية؟ ففي الحقيقة هذا سؤال يستحق التحقيق والبحث. أولاً وقبل كل شيء، يجب تكييف تعليم المحاسبة مع التطورات الجديدة واحتياجات السوق. ومع ذلك، فمن الممكن أن يتم تشكيل المناهج الدراسية وفقًا لمعايير مختلفة طبقا لتلك المتغيرات والتي منها الأمن السيبراني (Chowdhury & Gkioulos, 2021: 7).

ذكر الخبير الاقتصادي البريطاني آدم سميث أن الطلب معروف بينما العرض هل موجود بالفعل؟ والمشكلة هي تهيئة جانب العرض لتلبية الطلب. يقدم سميث المشكلة الأساسية لسوق العمل، والتي تتطور على مر القرون حيث تخضع أسواق العمل اليوم لترتيبات مؤسسية لتناسب متطلبات التقدم التكنولوجي السريع وضغوط العولمة. إن انعكاس هذه الضغوط له تأثير على صنع السياسات والمناهج التعليمية قد يؤدي النقص أو الفائض في سوق العمل إلى الكثير من العواقب الاقتصادية للاقتصاد مثل ارتفاع معدلات البطالة، أو ارتفاع معدلات التضخم، أو عدم الكفاءة في عملية الإنتاج. لذلك، فأن توقع التغييرات في سوق العمل أمر بالغ الأهمية. (Lubasz, 2024: 7)

3-2. المحاسبة والامن السيبراني ومتطلبات سوق العمل: المحاسبة ليست مهنة جديدة في سوق العمل فليس من الخطأ القول إنها نشأت بسبب الحاجة في السوق حيث احتاج الناس إلى خبراء وأشخاص مدربين تدريباً جيداً في إدارة الشركات. المحاسبة موجودة منذ أن طورنا مجتمعًا معقدًا وتم تطوير قواعد التجارة فيه من خلال تخصصات عدة والمحاسبة كانت واحدة منها، يرتبط المجتمع بالأشخاص الذين يعملون بشكل مباشر في الأمور المالية أو السلع أو الأموال وإن هؤلاء الأشخاص الذين يدركون أهمية المال ويستخدمونه ويساهمون في التنمية المستدامة للمجتمع. فقد شهد سوق العمل المحاسبي تغييرات جذرية. وفي هذا الصدد، هناك الكثير من المناقشات حول مستقبل توظيف المحاسبة. ويُزعم أن الطلب على خدمات المحاسبة التقليدية ينخفض فيما يتعلق بالزيادات المتوقعة في الاستشارات والتحليل والمعرفة الرقمية والابتكار، وهنا ويُفترض أن التعليم المحاسبي يلعب دورًا

حاسمًا في تزويد الطاقة الشبابية بهذه المتطلبات. ولا ينبغي أن يكون تطوير المناهج المحاسبية خارج ديناميكيات العرض والطلب السريعة هذه، مع الحفاظ على موقفهم المهني تجاه التطوير. والهدف مناقشة الاتجاهات الحديثة في تعليم المحاسبة في ضوء ديناميكيات سوق العمل المتغيرة بسرعة. في مجال الأمن السيبراني، والتي دخلت حياتنا لأسباب مختلفة وأثرت بشكل كبير على خدمات المحاسبة، بإيجاز شديد يفترض تطوير تعليم المحاسبة لمنهج يعالج بشكل صحيح ما يمثله طلب العمالة في ضوء الاتجاهات المذكورة وكيفية تنفيذ ذلك (Tsiligiris & Bowyer, 2021: 2).

وهنا يرى الباحث إنه من الممكن التركيز على أبرز ما يتطلبه سوق العمل من محاسبين يتمتعون بالاتـي (Haapamäki & Sihvonen, 2022: 4-5):

1. **الطلب على المحاسبين المتمرسين في التعامل مع الإنترنت**: لا يمكن التشكيك في أهمية امتلاك المحاسبين المحترفين العاملين في المنظمات للمعرفة بالأمن السيبراني أو تجاهلها وكما ورد في الجمعية الوطنية لمجالس المحاسبة الحكومية (NASBA) ونشرة AICPA "مشروع رؤية المحاسبين القانونيين المعتمدين"، فأن كل نشاط تقريبًا في الكيانات(الشركات) يعتمد على تكنولوجيا المعلومات، وتشمل المسؤوليات المالية والتدقيقية والإدارية لمحترفي المحاسبة استخدام وتطوير ومراقبة تكنولوجيا المعلومات. فضلا عن ذلك، تشكل أنظمة المعلومات المحاسبية جزءًا من منهج الدورات المحاسبية. إذ كان في السابق الامن السيبراني موضوعًا فنيًا والآن أصبح موضوعًا بالغ الأهمية للأعمال، فمن المؤكد أن المحاسبة وأنظمة المعلومات أصبحتا مترابطتين بشكل متزايد بهذا الشأن لذلك، هناك حاجة إلى المعرفة في مجالات مثل الشبكات والذكاء الاصطناعي والحوسبة السحابية والاتصالات الآمنة والتشفير إلى جانب المعرفة المحاسبية التقليدية. مع هذه البيانات ومعلومات الإعداد، فأن المهارات مثل توفير الامتثال للأمن السيبراني في نطاق المحاسبة وإدارة المخاطر السيبرانية وإعادة هيكلة الأمن السيبراني والعمل كمستشار في اختيار تقنيات الأمن السيبراني هي أيضًا مؤهلات إحصائية يسعى إليها المدققون. فضلا عن كل هذا، سيزداد الطلب على المحترفين الذين يفهمون الروابط بين المحاسبة والأمن السيبراني والذين يفكرون بذكاء للتعامل مع اتجاهات المستقبل.
2. **الأدوار والمهارات الوظيفية المطلوبة في المحاسبة**: حتى الآن، لم يعد مصطلح "المحاسبة" يشير فقط إلى التعاملات المالية للشركة وأداء التقارير وفقًا لمعايير المحاسبة المالية الكلاسيكية وإعداد التقارير المالية للشركات، بل بدأ أيضًا في اكتساب معنى يغطي المعاملات ذات المغزى داخل الفضاء الإلكتروني، والتي تتطلب أيضًا معرفة ومهارات محاسبية الكترونية معينة. بالإضافة إلى مهام المحاسبة التقليدية، هناك أيضًا مهام ومسؤوليات محاسبية أخرى مثل إعداد التقارير المالية وإدارة المخاطر، وإعداد التقارير المتعلقة بالامتثال الضريبي، وتطوير التقارير الرقمية التي تعمل على أتمتة العمليات والتطبيقات المحاسبية، وكذلك تقديم المشورة بشأن التطوير التكنولوجي الأساسي فيما يتعلق بالتقنيات المتقدمة باستخدام البيانات الضخمة والبلوك تشين. ومن المتوقع أن تزداد الأدوار الوظيفية بموجب المتطلبات الجديدة، ومتخصص الذكاء الاصطناعي بالتوازي مع توسع المهام والمسؤوليات، من المتوقع أيضًا أن يتمتع الأفراد العاملون في مجال المحاسبة بمجموعة متنوعة من المهارات. ستكون هذه من بين المهارات المتقدمة، ومهارات التكنولوجيا المالية والمعلوماتية الموسعة، وتقنيات تحليل وحماية البيانات المتقدمة، والخبرة في تقييم أنظمة الرقابة الداخلية، والقدرة

على تفسير وفهم العمليات التجارية، والقدرة على فهم المعلومات الأساسية لتطبيقات الذكاء الاصطناعي.

3-3. الاتجاهات المستقبلية للمحاسبة وفق الأمن الاسيبراني

3-3-1. التطورات المتوقعة في التعليم المحاسبي: يبحث المتخصصون الجدد عن محتوى تعليمي يعدهم لتحديات بيئة الأعمال لأنه إذا كانوا غير قادرين على تلبية متطلبات هذه البيئة، فلن يكون لديهم وظيفة مهنية ذات مغزى. في هذا السياق، وبدعم من الإحصائيات لبعض الدراسات، تم تحديد المشاكل التي يمكن أن تحدث في تدفق التعليم المحاسبي من حيث وضع وظائف المحاسبة المتخصصة في بيئة الأعمال، وهنا يجب على المهنيين المحاسبين أن يفهموا البيئات السيبرانية المختلفة التي يمكن أن تؤثر على ممارساتهم، وأن يكونوا على دراية بالسياسات والقوانين ذات الصلة، وأن يكونوا قادرين على معرفة ما يجب عليهم فعله إذا تأثروا. في هذا السياق، ينبغي إصلاح التعليم المحاسبي، وتفترض مراجعة شاملة للمحتوى القديم المعترف به وبعد معالجة تقييم المحاسبة البرمجية من خلال إثراء جزء الممارسة، يتم تقييمه مرة أخرى في نهاية العملية التعليمية. إن توقع المعرفة والمهارات التي ظهرت في الآونة الأخيرة والتي من المتوقع أن تصبح ضرورية للتأثير في مستوى معدلات البطالة إذ ينطوي على تحديث تعليم المحاسبة للقوى العاملة المستقبلية. وينبغي إجراء دراسة استباقية لتحديد المعرفة والمهارات التي تحتاجها القوى العاملة من خلال عكس القطاعات مثل الصناعة والخدمات والقطاع العام والمعلومات والتكنولوجيا التي ستطلب هذه الخدمة. وينبغي تحديد استراتيجيات جديدة نتيجة للدراسة الاستباقية لمنح الطلاب تعليمًا فعالاً ومن ثم فإن تطوير مناهج تعليم المحاسبة سوف يتشكل وفقًا لمتطلبات سوق العمل في المستقبل القريب. وفي إطار توقعات جيدة الإعداد تركز على شرح الميزات المستقبلية، يجب تطوير استراتيجيات خاصة بما في ذلك أهداف القطاع. ويجب تحويل هذه الاستراتيجيات إلى أنشطة تعليمية تحددها المناهج الدراسية. (Alshurafat & others, 2021: 5).

3-3-2. الآثار المترتبة على سوق العمل: من المعروف أن التقدم في التكنولوجيا المدفوعة بالرقمنة قد أدى إلى تقريب الحدود الجغرافية والتشغيلية للعالم. والواقع أن الشركات بدأت تعتمد على محترفي المحاسبة الذين يعرفون التكنولوجيا المتقدمة في مجال الأعمال والذين يتفوقون في هذا الصدد وامنها السيبراني المهم. إن التفاعل بين التعليم الذي يتلقاه المحاسبون في المستقبل والمهارات التي يدركونها ويظهرونها بمثابة مصدر قوة لمجال المحاسبة. لقد أدت وجهات النظر المختلفة للأفراد والكيانات القانونية العاملة، إلى نشوء مشكلة خطيرة في مجال تعليم المحاسبة، وذلك لأن المناهج التدريبية والمحاسبية قد لا تلبي متطلبات التغيرات السريعة عند دخول مجال الخدمة عندما يتخرج الطلاب. ومن ثم، فمن الأهمية بمكان رسم المؤهلات المتوقعة من المحترفين المحاسبين الذين يتعين عليهم مواجهة التغيير السريع والتعقيد وإدارة العملية بذكاء. أن الشركات والكيانات في سوق الأعمال تتوقع من المحاسبين المستقبليين أن يكونوا على دراية بالمحاسبة المالية، والمحاسبة الأولية، والمحاسبة الإدارية، والمحاسبة المالية، واللوائح المحاسبية، وأنظمة المعلومات الإدارية، فضلاً عن المعرفة والتعليقات حول مجالات أخرى. وعلاوة على ذلك، قد ترغب الشركات في الحصول على بعض المؤهلات الأخرى التي تتجاوز المتطلبات المفروضة فضلاً عن توقع أصحاب المصلحة الأكثر مرونة وسلاسة والذين يعرفون الموقف الذي يشغلونه والتوقعات المختلفة لتلك المناصب. (Ebaid, I., 2022: 6).

3-4. تحديات تطوير مناهج التعليم المحاسبي في ظل الامن السيبراني: لقد أدى دمج الذكاء الاصطناعي في المحاسبة إلى تحويل مشهد اكتشاف الاحتيال بشكل كبير. غالبًا ما تكافح الأساليب التقليدية، على الرغم من فعاليتها إلى حد ما، مع التعقيد المتزايد وحجم البيانات المالية. يقدم الذكاء الاصطناعي، بقدراته التحليلية المتقدمة، حلاً واعدًا لهذه التحديات. من خلال التقنيات المستخدمة في اكتشاف الاحتيال المدعوم بالذكاء الاصطناعي في المحاسبة وتسلط الضوء على دراسات الحالة التي توضح التطبيقات العملية وفوائد هذه التقنيات (Adelakun & others, 2024:1) ومن بين التحديات المستقبلية التي تواجه تطوير مناهج التعليم المحاسبي في ظل الأمن السيبراني هي الآتي: (Demirkan & others, 2020: 5).

3-4-1. تكنولوجيا الذكاء الاصطناعي وتأثيرها على تطوير مناهج التعليم المحاسبي: تكنولوجيا الذكاء الاصطناعي من المجالات الناشئة والمتطورة التي من الممكن أن تغير طريقة تعلم وتدريس المحاسبة، إذ يمكن استخدام تقنيات الذكاء الاصطناعي في تحسين مناهج التعليم المحاسبي من خلال توفير أساليب تدريس تفاعلية ومبتكرة، وكذلك تطوير نماذج تعلم ذاتي وتقييم ضروري لتحسين تجربة التعلم للطلاب في هذا المجال خاصة في مجال الاحتيال المالي الالكتروني.

3-4-2. الابتكارات في مجال الأمن السيبراني وتطبيقها في التعليم المحاسبي: الابتكارات في مجال الأمن السيبراني تأتي على رأس الأولويات في تطوير مناهج التعليم المحاسبي. إذ يمكن تطبيق أحدث تقنيات الأمن السيبراني مباشرة في المقررات الدراسية لتأهيل الطلاب بالمعرفة والمهارات الضرورية في هذا المجال، كما يمكن تضمين دروس تفاعلية تعتمد على الابتكارات الحديثة في الأمن السيبراني لتحفيز الطلاب وتعزيز فهمهم لأهميتها في العمل المحاسبي.

3-5. اعتبارات تطوير مناهج التعليم المحاسبي في ظل الأمن السيبراني: يرى الباحث من خلال ما تقدم، أنه من المهم بمكان أخذ بعض الاعتبارات الأساسية عند تصميم أو تطوير مناهج التعليم المحاسبي في ظل الأمن السيبراني والتي تساعد في تطوير المناهج المحاسبية في ظل التحديات والتطورات الخاصة بالأمن السيبراني والتي يمكن حصر أهمها بالآتي: بتصرف من الباحث بالاعتماد على (Byrne, 2022: 7)، (Lubasz, 2024: 6)، (Alahmari & Duncan, 2020: 3):

1. **تضمين مفاهيم الأمن السيبراني في المقررات الدراسية:** ينبغي أن يتم تضمين مفاهيم الأمن السيبراني في المقررات الدراسية بشكل واضح وشامل. يجب أن تشمل هذه المفاهيم موضوعات مثل حماية البيانات المالية، والتصدي لعمليات الاحتيال المحاسبي، وضمان سلامة النظم المحاسبية فضلا عن الحاجة إلى معرفة الشبكات والذكاء الاصطناعي والحوسبة السحابية والاتصالات الآمنة والتشفير إلى جانب المعرفة المحاسبية التقليدية. مع هذه البيانات ومعلومات الإعداد، فأن المهارات مثل توفير الامتثال للأمن السيبراني في نطاق المحاسبة وإدارة المخاطر السيبرانية وإعادة هيكلة الأمن السيبراني والعمل كمستشار في اختيار تقنيات الأمن السيبراني هي أيضًا مؤهلات إحصائية يسعى إليها المدققون وينبغي أيضًا تقديم امثلة عملية توضح كيفية تطبيق مفاهيم الأمن السيبراني في سياق المحاسبة.
2. **استخدام أساليب تفاعلية وتطبيقية لتعليم مفاهيم الأمن السيبراني:** يتعين استخدام أساليب تفاعلية وتطبيقية في تعليم مفاهيم الأمن السيبراني، مثل الدراسات الحالية والنماذج العملية وورش العمل. يساعد ذلك الطلاب على فهم تطبيقات الأمن السيبراني في سياق المحاسبة بشكل أفضل، كما يمكن

للتفاعل والتطبيق العملي أن يسهم في تحفيز الطلاب وزيادة فهمهم لمخاطر الأمن السيبراني وكيفية التعامل معها.

3. **استخدام المحاكاة والوسائط المتعددة:** تعد المحاكاة والوسائط المتعددة أدوات فعالة في عملية تطوير مناهج التعليم المحاسبي بالتركيز على الأمن السيبراني. فالاستخدام السليم للمحاكاة بمختلف أشكالها يساهم في خلق بيئة واقعية لتعلم الطلاب وفهم التهديدات السيبرانية وكيفية التعامل معها. ومن جانبها، تساهم الوسائط المتعددة، مثل الفيديوهات والمحتوى التفاعلي، في تحفيز الطلاب وتوفير تجارب تعلم متنوعة وشيقة تجذب انتباههم وتساعدهم في بناء معرفة قوية حول أمور الأمن السيبراني في المحاسبة.
4. **استخدام التعلم الذاتي والتعلم النشط:** يعد التعلم الذاتي والتعلم النشط أساسيًا في تحسين المناهج التعليمية المحاسبية في مجال الأمن السيبراني. إذ يتيح الاستفادة من تقنيات التعلم الذاتي للطلاب الفرصة لاكتساب المهارات والمعرفة بشكل أكبر من خلال الاستقصاء والبحث الشخصي، وهو ما يساهم في تعزيز تفهمهم الشامل لمفاهيم الأمن السيبراني وتطبيقها على سياقات واقعية. وبالنسبة للتعلم النشط، فإن تشجيع الطلاب على المشاركة الفعّالة في العمليات التعليمية يعزز تفاعلهم مع المحتوى ويساعدهم على تحمل مسؤولية تعلمهم وفهم الأمور المتعلقة بالأمن السيبراني بشكل أكبر.
5. **التدريب والتحسين المستمر للمعلمين والمدربين:** يعد التدريب والتحسين المستمر للمعلمين والمدربين أمرا أساسيا لضمان تحقيق أهداف تطوير مناهج التعليم المحاسبي في ظل الأمن السيبراني. يتطلب ذلك تزويد الكوادر التعليمية بالمهارات والمعرفة اللازمة لتدريس ونقل المفاهيم والتقنيات الحديثة المتعلقة بالأمن السيبراني إلى الطلاب بطرق فعالة ومبتكرة.
6. **تقييم وتحليل فعالية المناهج:** بمجرد تطبيق المناهج التعليمية في مجال المحاسبة، يصبح من الضروري تقييم وتحليل فعاليتها لضمان تحقيق الأهداف المرجوة. يتضمن تقييم فعالية المناهج النظر في تأثيرها على تطوير مهارات الطلاب وزيادة معرفتهم. كما يشمل أيضًا تحليل مدى استجابة المنهج التعليمي لاحتياجات سوق العمل في مجال المحاسبة مع مراعاة الأمن السيبراني.

المحور الرابع
الدراسة الميدانية

4-1. هدف الدراسة الميدانية: هدفت الدراسة الميدانية إلى اختبار فرضيات الدراسة الرئيسة (عدد 3) والفرعية منها، فضلا عن معرفة النتائج التحليلية الخاصة بمفردات استمارة الاستبيان، ومن خلال التحليل الاحصائي باستخدام أسلوب (Likert) خماسي الرتب، إذ شملت الاستمارة من أربعة محاور وكالآتي:

- **المحور الاول**: خاص بمجالات استراتيجية الأمن السيبراني العراقية والتي احتوت على (8) مجالات
- **المحور الثاني**: خاص بتطوير مناهج التعليم المحاسبي وتضمن (8) فقرات أيضا.
- **المحور الثالث**: خاص بسوق العمل وتضمن (7) فقرات.
- **المحور الرابع:** خاص باعتبارات تطوير مناهج التعليم المحاسبي وفق استراتيجية الأمن السيبراني.

4-2. الاجراءات التحليلية الخاصة باستمارة الاستبيان: بهدف التأكد من قدرة استمارة الاستبيان على قياس متغيرات البحث وقدرتها على تعزيز الجانب النظري للبحث والعملي لها، تم اختبار الصدق لفقرات الاستمارة بعد إعدادها من قبل الباحث وعرضها على مجموعة من المحكمين المختصين والمذكورة أسماؤهم في (الملاحق رقم 1) للتأكد من صحة الفقرات ومدى ملائمتها

لفرضيات الدراسة وأهدافها، واستطلاع رأيهم بمدى قدرتها على قياس متغيرات الدراسة وجوانبها النظرية والعملية والمقترحة منها وبما يضمن الوضوح والدقة من الناحية العملية، فقد أضيفت بعض الفقرات وتم استبعاد أخرى أو تعديلها، فضلا عن تصحيح بعض العبارات وصياغة بعضها بشكل أخر أكثر دقة وملائمة مما ساهم في تحقيق الغرض الرئيسي من البحث بشكل أفضل.

فضلا عن ذلك قد خضعت الاستمارة لاختبار المصداقية Reliability لبيان مدى مصداقية نتائج الاستبيان والارتباط بين أسئلتها، إذ تم استخدام تحليل المصداقية Reliability Analysis لحساب معامل ارتباط Corn bach Alpha، ومن ثم تم اجراء اختبار التوزيع الطبيعي باستخدام اختبار Shapiro-Wilk وذلك لمعرفة مدى الموثوقية في استجابة عينة البحث على اسئلة الاستبانة ومدى امكانية تعميم نتائجها على مجتمع الدراسة وكما يأتي:

أ. **الاتساق:** لغرض معرفة مستوى الاتساق قام الباحث بتطبيق اختبار الارتباط المعروف بـــ (Spearman) وذلك لاختبار محتوى أداة البحث (الاستبانة) أي بين متغيراتها وأبعادها، بهدف معرفة مستوى استقلالية كل متغير من متغيرات البحث الثلاثة وبناءً على ما جاء في الجداول أدناه: الجدول رقم (2) الخاص باختبار اتساق فقرات المحور الأول " مجالات استيراتيجية الأمن السبيراني العراقية "والجدول رقم (3) الخاص باختبار اتساق فقرات المحور الثاني" تطوير مناهج التعليم المحاسبي " والجدول رقم (4) الخاص باختبار اتساق فقرات المحور الثالث "سوق العمل"، تبين وجود علاقات ارتباط معنوية ذات اتجاهات ايجابية لمستوى قوة فقرات محاور البحث، مما يؤشر وجود درجة عالية من الاتساق توضح مستوى الصدق لبناء محتويات أداة البحث " الاستبانة ".

جدول (2): اتساق فقرات المحور الأول (مجالات استراتيجية الأمن السيبراني)

t	X8	X7	X6	X5	X4	X3	X2	X1	
0.351	0.309	0.309	0.287	0.272	0.280	0.329	0.243	1	X1
0.633	0.292	0.292	0.333	0.300	0.239	0.491	1		X2
0.670	0.288	0.288	0.350	0.305	0.322	1			X3
0.631	0.578	0.578	0.333	0.350	1				X4
0.500	0.549	0.549	0.405	1					X5
0.543	0.547	0.422	1						X6
0.516	0.439	1							X7
0.665	1								X8
1									t

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

جدول (3): اتساق فقرات المحور الثاني (تطوير مناهج التعليم المحاسبي)

t	X8	X7	X6	X5	X4	X3	X2	X1	
0.521	0.418	0.519	0.203	0.260	0.370	0.295	0.317	1	X1
0.575	0.360	0.572	0.245	0.333	0.228	0.211	1		X2
0.384	0.207	0.338	0.311	0.250	0.324	1			X3
0.637	0.516	0.451	0.562	0.463	1				X4

t	X8	X7	X6	X5	X4	X3	X2	X1	
0.723	0.490	0.346	0.332	1					X5
0.697	0.660	0.480	1						X6
0.683	0.335	1							X7
0.567	1								X8
1									t

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

جدول (4): اتساق فقرات المحور الرابع (سوق العمل)

t	X7	X6	X5	X4	X3	X2	X1	
0.561	0.464	0.363	0.491	0.320	0.407	0.783	1	X1
0.580	0.530	0.324	0.489	0.546	0.400	1		X2
0.453	0.513	0.558	0.575	0.572	1			X3
0.410	0.444	0.448	0.558	1				X4
0.543	0.522	0.579	1					X5
0.501	0.407	1						X6
0.627	1							X7
1								t

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

ب. الثبات: قام الباحث بتطبيق اختبار الثبات بهدف توضيح مستوى امكانية تحقيق النتائج نفسها مرة ثانية في حال تم تطبيق المقياس مرة أخرى للعينة نفسها، فقد تم تطبيق وفقا لمعامل Corn bach Alpha، إذ طبق على المستوى الكلي للعينة المبحوثة التي بلغت (87) استمارة استبيان صالحة للتحليل والتي شملت على (29) سؤالا، إذ تبين وجود قيم مرتفعة لمعاملات Corn bach Alpha إذا بلغت ما قيمته (82%) وتعد هذه النسبة جيدة لهذا النوع من البحث، إذ إن الوصول إلى هذه النتيجة يعد دلالة حول أن جميع الأسئلة تعد ضرورة وتمتلك من الأهمية ما يستوجب استخدامها، وكما موضح في الجدول رقم (5) الآتي:

جدول (5): ثبات متغيرات البحث

المحاور	قيمة الثبات
مجالات استراتيجية الأمن السيبراني العراقي	0.81
تطوير مناهج التعليم المحاسبي	0.78
سوق العمل	0.83
اعتبارات عند تطوير المناهج المحاسبية وفق لاستراتيجية الامن السيبراني العراقي	0.80
الكلي	0.82

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

ج. اختبار التوزيع الطبيعي: قام الباحث بعمل اختبار التوزيع الطبيعي باستخدام اختبار Shapiro-Wilk بغية معرفة مستوى تتبع البيانات المستخدمة للتوزيع الطبيعي، إذ يوضح الجدول رقم (6) الفرضية الصفرية التي تتمحور حول توزيع بيانات المتغيرات طبيعيا وهي مقبولة بسبب تجاز كل القيم مستوى الدلالة المعنوية المتمثل بـ (0.05).

جدول (6): اختبار التوزيع الطبيعي باستخدام اختبار Shapiro-Wilk

المحاور	قيمة الاختبار	مستوى الدلالة
مجالات استراتيجية الأمن السيبراني	1.13	0.82
مناهج التعليم المحاسبي	0.87	0.79
سوق العمل	0.93	0.81
اعتبارات تطوير المناهج المحاسبية وفق لاستراتيجية الامن السيبراني العراقي	1.02	0.93

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

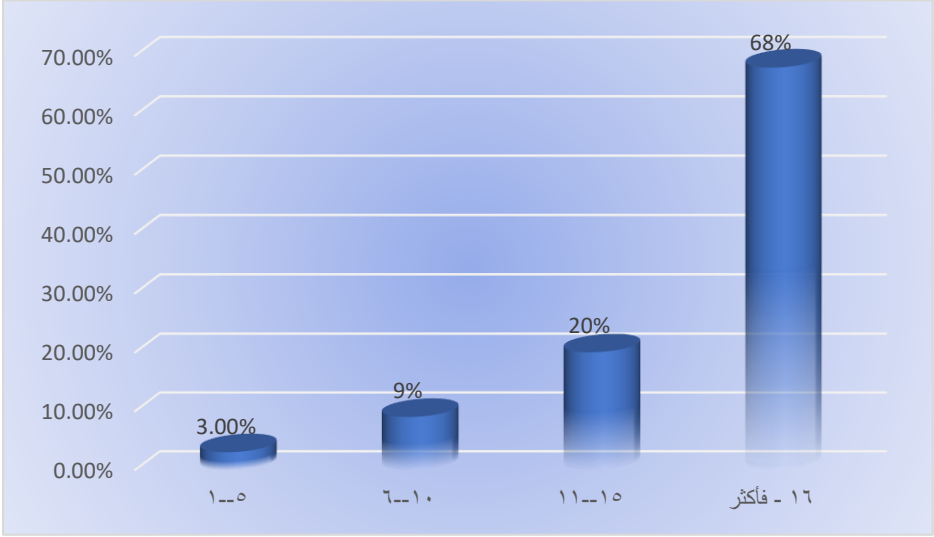
3-4. مجتمع وعينة الدراسة وعينة البحث: تمثل مجتمع البحث بالأكاديميين في الجامعات والمعاهد العراقية من تخصص المحاسبة وأمن سيبراني، أما عينة البحث، وبسبب عدم قدرة الباحث للوصول إلى العدد الكلي لمجتمع البحث، فقد تم اختيار عينة عشوائية من مجتمع البحث والتي تمثلت بـــ (87) استمارة صالحة للتحليل بعد استبعاد غير الصالح منها حول نموذج البحث ووفقا للمحاور الخاصة باستمارة الاستبيان، إذ كانت المعلومات العامة لعينة البحث كما موضحة بالأشكال الآتية:

1. المؤهل العلمي

شكل (2): المؤهل العلمي لعينة البحث

من خلال الشكل رقم (2) يتبين أن المؤهل العلمي لعينة البحث مكون من (دكتوراه عدد 47، ماجستير عدد 40) وهذا يعني أن غالبية الاجابات من عينة البحث جاءت من أشخاص يتمتعون بمؤهلات علمية عالية مما انعكس ايجابا على دقة الاجابات الخاصة بأسئلة الاستبانة.

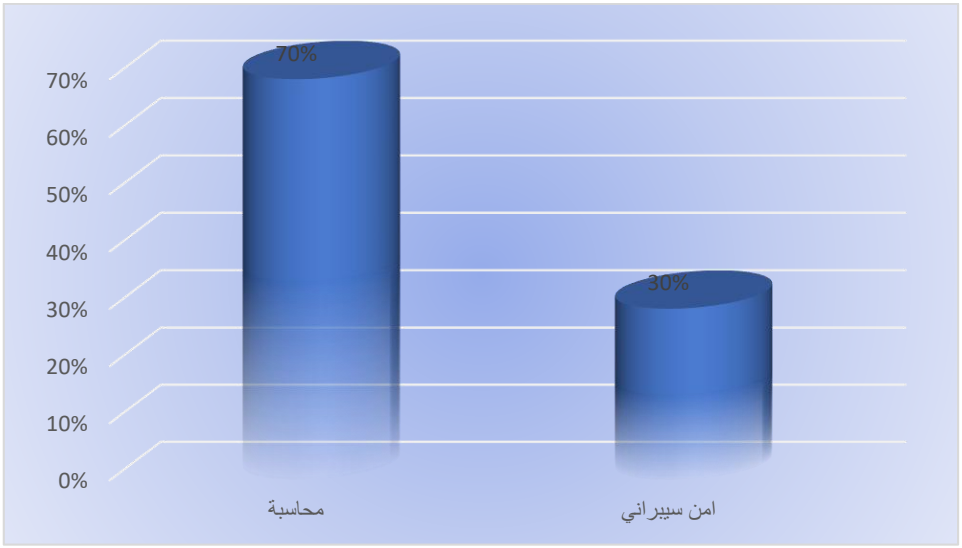
2. عدد سنوات الخبرة في مجال العمل:



شكل (3): عدد سنوات الخبرة في مجال العمل

من خلال الشكل رقم (3) يتبين أن عدد سنوات الخبرة لعينة البحث في مجال العمل (عدد 59 مبحوث 16 سنة خبرة عمل فأكثر، عدد 17 مبحوث ما بين 11-15 سنة خبرة عمل، عدد 8 مبحوث ما بين 6-10 سنة خبرة عمل، عدد 3 مبحوث ما بين 1-5 سنوات خبرة عمل) وهذا يعني أن غالبية الاجابات قد جاءت من اشخاص يتمتعون بخبرة عالية مما انعكس على دقة الاجابات.

3. التخصص لعينة البحث:



شكل (4): تخصص عينة البحث

الشكل رقم (4) يوضح أن مجال عينة البحث كان (لتخصص المحاسبة عدد 61 مبحوث، لتخصص الأمن السيبراني عدد 26 مبحوث) وهذا يدل على تنوع مجالات العمل للمبحوثين مما انعكس ايجابا على دقة الاجابات أسئلة الاسبانة الخاصة والتي تمحورت بالأساس على تطوير مناهج التعليم المحاسبي في العراق وفق استيراتيجية الأمن السيبراني العراقي.

4-4. أسلوب التحليل الاحصائي: تم أسلوب التكرارات في تفريغ الإجابات الخاصة باستمارة الاستبيان من خلال الاستعانة ببرنامج اكسل EXCEL والاستفادة من بعض العلاقات الرياضية والاحصائية المتوافرة في هذا البرنامج الاستخراج بعض النتائج، فضلا عن الاستفادة من البرنامج الإحصائي SPSS في تحليل البيانات المستخرجة والنسب المئوية والمتوسطات الحسابية المرجحة والانحرافات المعيارية في استخراج النتائج الخاصة بإجابات عينة البحث إذ قام الباحث بترميز اسئلة الاستبانة (X1,X2,X3 ....) واعطاء أوزان للاستجابات وفقا لمقياس (Likert) خماسي الرتب لقياس اسئلة محاور الاستبانة إذ تكون المحور الأول " مجالات استراتيجية الأمن السيبراني العراقية " إذا احتوت على 8 اسئلة، والمحور الثاني " تطوير مناهج التعليم المحاسبي " إذا احتوى على 8 أسئلة أيضا، والمجال الثالث: سوق العمل " إذا احتوى على 7 اسئلة، والمجال الرابع " اعتبارات تطوير مناهج التعليم المحاسبي وفق استراتيجية الأمن السيبراني العراقي" إذا احتوى على 6 اسئلة.

4-5. نتائج التحليل الإحصائي لبيانات الدراسة الميدانية

4-5-1. الوصف والتشخيص

4-5-1-1. الوصف والتشخيص الخاص بالمحور الأول "مجالات استراتيجية الأمن السيبراني العراقية" يمثل الجدول رقم (7) الوصف والتشخيص اختبار الفرضية الأولى للبحث وكالآتي:

جدول (7): وصف وتشخيص المحور الأول "مجالات استيراتيجية الأمن السيبراني العراقي"

العبارات	بدائل الاستجابة										الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف	الترتيب الجديد
	أتفق جدا		أتفق		محايد		لا أتفق		لا أتفق تماما						
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%					
X1	50	57%	34	39%	3	3%	0	0%	0	0%	4.5402	0.56660	90.80%	12.48%	1
X2	38	44%	43	49%	6	7%	0	0%	0	0%	4.3908	0.59760	87.82%	13.61%	4
X3	33	38%	48	55%	6	7%	0	0%	0	0%	4.3103	0.59670	86.21%	13.84%	5
X4	46	53%	36	41%	5	6%	0	0%	0	0%	4.4713	0.60692	89.43%	13.57%	3
X5	46	53%	40	46%	1	1%	0	0%	0	0%	4.5172	0.52523	90.34%	11.63%	2
X6	36	41%	46	53%	1	1%	0	0%	4	5%	4.2644	0.88212	85.29%	20.69%	6
X7	31	36%	49	56%	3	3%	0	0%	4	5%	4.1839	0.88303	83.68%	21.11%	8
X8	43	49%	35	40%	3	3%	0	0%	6	7%	4.2529	1.04790	85.06%	24.64%	7
الكلي	81(%93)				4(%5)		2(%2)				4.3664	0.71326	87.33%	16.34%	

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

يتضح من الجدول رقم (7) الذي يختص بـ " مجالات الأمن السيبراني العراقي وعلاقتها بسوق العمل " إذ بلغ المعدل العام لإجابات المبحوثين نسبة (93%) (بين اتفق جدا واتفق) ونسبة (5%) محايد ونسبة (2%) لا اتفق ولا اتفق تماما، حيث بلغت قيمة الوسط الحسابي (4.3664) بانحراف معياري (0.71326) إذا تمثل نسبة استجابة المبحوثين على هذا المحور (87.33%) وبمعامل اختلاف (16.34%). وإن هذه النسب تعد جيدة جدا تجاه الفرضية الأولى للبحث.

4-5-1-2. الوصف والتشخيص الخاص بالمحور الثاني " تطوير مناهج التعليم المحاسبي " يمثل الجدول رقم (9) الوصف والتشخيص اختبار الفرضية الثانية للبحث وكالآتي:

جدول (8): وصف وتشخيص المحور الثاني "تطوير مناهج التعليم المحاسبي"

العبارات	بدائل الاستجابة												الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف	الترتيب الجديد
	أتفق جدا		أتفق		محايد		لا أتفق		لا أتفق تماما								
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%							
X1	39	45%	41	47%	7	8%	0	0%	0	0%			4.3678	0.63089	87.36%	14.44%	1
X2	34	39%	47	54%	6	7%	0	0%	0	0%			4.3218	0.60028	86.44%	13.89%	2
X3	35	40%	47	54%	1	1%	4	5%	0	0%			4.2989	0.71715	85.98%	16.68%	3
X4	32	37%	48	55%	5	6%	2	2%	0	0%			4.2644	0.67272	85.29%	15.78%	5
X5	26	30%	56	64%	5	6%	0	0%	0	0%			4.2414	0.54911	84.83%	12.95%	6
X6	27	31%	58	67%	2	2%	0	0%	0	0%			4.2874	0.50366	85.75%	11.75%	4
X7	26	30%	54	62%	3	3%	4	5%	0	0%			4.1724	0.70227	83.45%	16.83%	8
X8	37	43%	45	52%	4	5%	0	0%	1	1%			4.2069	0.90397	84.14%	21.49%	7
الكلي	82(%94)				4(%5)		1(%1)						4.2701	0.66001	85.40%	15.46%	

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS.

يتضح من الجدول رقم (8) الذي يختص بـ " تطوير مناهج التعليم المحاسبي " إذ بلغ المعدل العام لإجابات المبحوثين نسبة (94%) (بين اتفق جدا واتفق) ونسبة (5%) محايد ونسبة (1%) لا اتفق ولا اتفق تماما، إذ بلغت قيمة الوسط الحسابي (4.2701) بانحراف معياري (0.66001) إذا تمثل نسبة استجابة المبحوثين على هذا المحور (85.40%) وبمعامل اختلاف (15.46%). وإن هذه النسب تعد جيدة جدا تجاه الفرضية الثانية للبحث.

4-5-1-3. الوصف والتشخيص الخاص بالمحور الثالث "سوق العمل" يمثل الجدول رقم (10) الوصف والتشخيص اختبار الفرضية الثالثة للبحث وكالآتي:

جدول (9): وصف وتشخيص المحور الثالث "سوق العمل"

العبارات	بدائل الاستجابة												الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف	الترتيب الجديد
	أتفق جدا		أتفق		محايد		لا أتفق		لا أتفق تماما								
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%							
X1	43	49%	33	38%	7	8%	4	5%	0	0%			4.3218	0.81404	86.44%	18.84%	1
X2	26	30%	48	55%	9	10%	4	5%	0	0%			4.1034	0.76302	82.07%	18.59%	4
X3	26	30%	44	51%	17	20%	0	0%	0	0%			4.1034	0.69941	82.07%	17.04%	5
X4	23	26%	52	60%	5	6%	7	8%	0	0%			4.0460	0.80562	80.92%	19.91%	6
X5	26	30%	43	49%	12	14%	6	7%	0	0%			4.0230	0.84876	80.46%	21.10%	7
X6	32	37%	45	52%	4	5%	6	7%	0	0%			4.1839	0.81453	83.68%	19.47%	3
X7	34	39%	49	56%	0	0%	4	5%	0	0%			4.2989	0.70075	85.98%	16.30%	2
الكلي	75(%86)				8(%9)		4(%5)						4.1544	0.77802	83.09%	18.73%	

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS.

يتضح من الجدول رقم (9) الذي يختص بـ " سوق العمل" إذ بلغ المعدل العام لإجابات المبحوثين نسبة (86%) (بين اتفق جدا واتفق) ونسبة (9%) محايد ونسبة (4%) لا اتفق ولا اتفق تماما،إذ بلغت قيمة الوسط الحسابي (4.1544) بانحراف معياري (0.77802) إذا تمثل نسبة استجابة المبحوثين على هذا المحور(83.09%) وبمعامل اختلاف (18.73%). وإن هذه النسب تعد جيدة جدا تجاه الفرضية الثالثة للبحث.

4-5-2. تحقيق فرضيات البحث: ادناه مناقشة نتائج اختبار فرضيات العلاقة والأثر الخاصة بمتغيرات البحث الثلاثة والتي تم توزيع استمارة الاستبيان على أساسها.

4-5-2-1. الفرضية الأولى: علاقة وأثر بين مجالات استراتيجية الأمن السيبراني ومناهج التعليم المحاسبي

الجدول (10): علاقة وأثر المتغير المستقل مع المتغير التابع "مجالات استراتيجية الأمن السيبراني وسوق العمل"

سوق العمل / مجالات استراتيجية الأمن السيبراني	معامل الارتباط	التأثير β1	R^2	F المحسوبة	F الجدولية	مستوى المعنوية
	0.783 (11.606)*	0.769 (11.604)*	0.613	134.655	3.967	0.000**

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

$P \leq 0.05, N = 87, df = 85$: t (1.991)

$P \leq 0.05, N = 87, df = (1, 85)$: f (3.967)

يتضح من الجدول رقم (10) أعلاه أن هناك علاقة وأثر قوية ودالة بين مجالات استيراتيجية الأمن السيبراني العراقي وسوق العمل، إذ بلغ معامل الارتباط (0.783) وعند اختبارها بالاختبار التائي (T) الخاص بدلالة معامل الارتباط تبين ان القيمة المحسوبة بلغت 11.606 وهي أكثر من القيمة التائية الجدولية البالغة 1.991 عند مستوى معنوية 0.05 ودرجة حرية 85، عليه هناك علاقة وأثر ايجابية لمجالات استراتيجية الأمن السيبراني العراقي عدد (8) في سوق العمل، وإن تسلسل أهمية المجالات (8) والتي تعكس الفرضيات الفرعية للمشكلة الأولى للبحث مبين في الجدول رقم (8) " الوصف والتشخيص " إذ يوضح تسلسل أهمية تلك المجالات الـ 8 من الأكثر أهمية إلى الأقل أهمية، إذ كان المجال الأول هو " مجال الحوكمة الفعالة " بالترتيب الأول ومجال " الجاهزية لحوادث الأمن السيبراني" بالترتيب الثامن أي الأخير. فضلا عن ذلك يتضح أن قيمة معامل التحديد (R^2) البالغة 0.613 تشير إلى أن دلالة علاقة وأثر مجالات استراتيجية الأمن السيبراني (8) وسوق العمل ما نسبته 61.3% وهي تعد نسبة مساهمة جيدة، ويدعم ذلك معنوية قيمة (F) المحسوبة (134.655) وهي أكبر من القيمة الجدولية 3.967 عند مستوى معنوية 0.05 ودرجات حرية (1,85) وكذلك قيمة معامل الانحدار(β1) بلغت 0.769 وعند اختبار دلالتها أظهرت قيمتها (11.604) وهي أكبر من القيمة الجدولية 1.991 وعليه هذه النسب ينتج عنها قبول الفرضية الاولى للبحث (H1) **"هناك**

علاقة وأثر ذات دلالة احصائية بين مجالات استراتيجية الامن السيبراني العراقية (8) وسوق العمل"

4-5-2-2. الفرضية الثانية: علاقة وأثر تطوير مناهج التعليم المحاسبي" وفق مجالات الأمن السيبراني " وسوق العمل.

جدول (11): علاقة وأثر مناهج التعليم المحاسبي "وفق مجالات الأمن السيبراني" وسوق العمل

سوق العمل / مناهج التعليم المحاسبي	معامل الارتباط	التأثير β1	R^2	F المحسوبة	F الجدولية	مستوى المعنوية
	0.803 (12.422)*	0.875 (12.442)*	0.645	154.808	3.967	0.000**

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

$P \leq 0.05$, N =87, df =85 : t (1.991)

$P \leq 0.05$, N =87, df = (1, 85): f (3.967)

يتضح من الجدول رقم (11) أعلاه أن هناك علاقة واثر قوية ودالة بين تطوير مناهج التعليم المحاسبي " وفق مجالات الأمن السيبراني " وسوق العمل، إذ بلغ معمل الارتباط (0.803) وعند اختبارها بالاختبار التائي (T) الخاص بدلالة معامل الارتباط تبين أن القيمة المحسوبة بلغت 12.422 وهي أكثر من القيمة التائية الجدولية البالغة 11.99 عند مستوى معنوية 0.05 ودرجة حرية 85، عليه هناك علاقة واثر لتطوير مناهج التعليم المحاسبي " وفق مجالات الأمن السيبراني " على سوق العمل، وإن تسلسل أهمية الفقرات الخاصة بهذا المحور (8) فقرات مبين في الجدول رقم (9) " الوصف والتشخيص " حيث يوضح تسلسل أهمية تلك المجالات الـــ 8 من الأكثر أهمية إلى الأقل أهمية، حي كانت الفقرة الخاصة بـــ (تعزيز التعاون بين القطاع العام والقطاع الخاص في تطوير مناهج التعليم المحاسبي وفق مجالات الامن السيبراني في العراق وهذا ما يتطابق مع معيار IES5 من معايير التعليم المحاسبي الدولي " متطلبات الخبرة العملية " والمجال الأول لاستراتيجية الأمن السيبراني وهو الحوكمة الفعالة) بالترتيب الأول وفقرة (تعريف الطالب بالتنبيهات الآنية حول ثغرات خاصة بالبيانات والمعلومات المتعلقة بالعمل المحاسبي أو التدقيقي فيما يتعلق بالأمن السيبراني الخاص بها لكي يتم يكون على درجة مقبولة من الجاهزية لتلك الحوادث وهذا يتطابق مع المجال السابع لاستراتيجية الأمن السيبراني وهو الجاهزية لحوادث الأمن السيبراني) بالترتيب الثامن أي الأخير. فضلا عن ذلك يتضح أن قيمة معامل التحديد (R^2) البالغة 0.645 تشير إلى أن دلالة علاقة وأثر تطوير مناهج التعليم المحاسبي " وفق مجالات الأمن السيبراني " وسوق العمل ما نسبته 64.5% وهي تعد نسبة مساهمة جيدة، ويدعم ذلك معنوية قيمة (F) المحسوبة (154.808)وهي أكبر من القيمة الجدولية 3.967 عند مستوى معنوية 0.05 ودرجات حرية (1,85) وكذلك قيمة معامل الانجدار(β1) بلغت 0.875 وعند اختبار دلالتها اظهرت قيمتها (12.442) وهي أكبر من القيمة الجدولية 1.991 وعليه هذه النسب ينتج عنها قبول الفرضية الثانية للبحث (H2) " هناك علاقة

وأثر ذات دلالة احصائية بين تطوير مناهج التعليم المحاسبي وفق استراتيجية الأمن السيبراني العراقية و سوق العمل "

4-5-2-3. الفرضية الثالثة: "هناك اعتبارات ينبغي مراعاتها عند تطوير المناهج المحاسبية وفق لاستراتيجية الأمن السيبراني العراقي".

يمثل الجدول رقم (13) الوصف والتشخيص لاختبار الفرضية الثالثة.

جدول (12): وصف وتشخيص المحور الرابع "اعتبارات تطوير المناهج المحاسبية وفق لاستراتيجية الأمن السيبراني العراقي"

العبارات	بدائل الاستجابة										الوسط الحسابي	الانحراف المعياري	نسبة الاستجابة	معامل الاختلاف	الترتيب الجديد
	أتفق جدا		أتفق		محايد		لا أتفق		لا أتفق تماما						
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%					
X1	39	45%	43	49%	5	6%	0	0%	0	0%	4.3908	0.59760	87.82%	13.61%	2
X2	35	40%	43	49%	5	6%	4	5%	0	0%	4.2529	0.76582	85.06%	18.01%	5
X3	36	41%	44	51%	3	3%	4	5%	0	0%	4.2874	0.74565	85.75%	17.39%	4
X4	30	34%	49	56%	2	2%	6	7%	0	0%	4.1839	0.78546	83.68%	18.77%	6
X5	38	44%	47	54%	2	2%	0	0%	0	0%	4.4138	0.54028	88.28%	12.24%	1
X6	31	36%	54	62%	2	2%	0	0%	0	0%	4.3333	0.52088	86.67%	12.02%	3
الكلي	82(%95)				3(%3)		2(%2)				4.3103	0.65928	86.21%	15.30%	

المصدر: من اعداد الباحث بالاعتماد على مخرجات نظام SPSS

يتضح من الجدول رقم (12) الذي يختص بـ " اعتبارات تطوير المناهج المحاسبية وفق لاستراتيجية الأمن السيبراني العراقي"" إذ بلغ المعدل العام لإجابات المبحوثين نسبة (95%)(بين اتفق جدا واتفق) ونسبة (3%) محايد ونسبة (2%) لا اتفق ولا اتفق تماما، إذ كان ترتيب الاعتبارات من الأكثر أهمية إلى الأقل كالآتي:

1. التدريب والتحسين المستمر للكادر التدريسي.
2. تضمين مفاهيم الأمن السيبراني في المقررات الدراسية.
3. تقييم وتحليل فعالية المناهج.
4. استخدام المحاكاة والوسائط المتعددة.
5. استخدام أساليب تفاعلية وتطبيقية لتعليم مفاهيم الأمن السيبراني.
6. استخدام التعلم الذاتي والتعلم النشط.

حيث بلغت قيمة الوسط الحسابي (4.3103) بانحراف معياري (0.65928) إذا تمثل نسبة استجابة المبحوثين على هذا المحور (86.21%) وبمعامل اختلاف (15.30%) وإن هذه النسب ينتج عنها مؤشرات ايجابية تجاه الفرضية الثالثة مما يعني قبولها.

المحور الخامس
الاستنتاجات والتوصيات

5-1. الاستنتاجات

5-1-1. استنتاجات الجانب النظري:

1. تشمل تطبيقات الأمن السيبراني مجالات مختلفة للمحاسبة مثل حماية البيانات المالية والمعلومات الحساسة من التسرب والاختراق وضمان سلامة العمليات المحاسبية وتأمين البيئة التقنية المستخدمة في مجال المحاسبة لضمان النزاهة والمصداقية.
2. إن الكيانات الدولية من القطاع الخاص وحتى العام، بدأت تعتمد على محترفي المحاسبة الذين يمتلكون مهارات ومعرفة عالية في التكنولوجيا المتقدمة وأمنها السيبراني المهم في مجال أعمالهم.
3. إن التفاعل بين التعليم الذي يتلقاه المحاسبون في المستقبل والمهارات التي يدركونها ويظهرونها، تعد بمثابة مصدر قوة لمجال المحاسبة في سوق العمل.
4. تعد الوظائف المتاحة في مجال التكنولوجيا إلى جانب المعرفة والمهارة المحاسبية من أفضل الوظائف في وقتنا الحالي، والرواتب التنافسية المقدمة فيها من أعلى الرواتب بين قطاعات العمل المتنوعة.
5. إن ترتيب العراق في مؤشر الأمن السيبراني العالمي لسنة 2020 كان 17 عربيا و129 عالميا وهذا يعد نوعا ما غير جيد بما فيه الكفاية على الأصعدة كافة ومنها التعليمية، إذ جزء من متطلبات تعزيز الأمن السيبراني هو تطوير التعليم والتي منها المناهج الدراسية لتخصص المحاسبة.

5-1-2. استنتاجات الجانب العملي:

1. يوجد علاقة وأثر ايجابي ذات دلالة احصائية بين مجالات استراتيجية الأمن السيبراني العراقي (8) وسوق العمل، إذ بلغ معمل الارتباط (0.783) وإن قيمة معامل التحديد (R^2) البالغة 0.613 تشير إلى أن دلالة العلاقة والاثر الايجابية ما نسبته 61.3% وهي تعد نسبة مساهمة جيدة، ويدعم ذلك معنوية قيمة (F) المحسوبة (134.655) وهي أكبر من القيمة الجدولية 3.967 عند مستوى معنوية 0.05.
2. يوجد علاقة وأثر قوية ذات دلالة احصائية ايجابية بين تطوير مناهج التعليم المحاسبي " وفق مجالات الأمن السيبراني " وسوق العمل، إذ بلغ معمل الارتباط (0.803) وإن قيمة معامل التحديد (R^2) البالغة 0.645 تشير إلى أن دلالة علاقة وأثر تطوير مناهج التعليم المحاسبي " وفق مجالات الأمن السيبراني " وسوق العمل ما نسبته 64.5% وهي تعد نسبة مساهمة جيدة.
3. هناك اعتبارات مهمة ينبغي أخذها بنظر الاعتبار عند تصميم مناهج محاسبية وفق مجالات الأمن السيبراني متسلسلة وهي: التدريب والتحسين المستمر للكادر التدريسي، تضمين مفاهيم الأمن السيبراني في المقررات الدراسية، تقييم وتحليل فعالية المناهج، استخدام المحاكاة والوسائط المتعددة، استخدام أساليب تفاعلية وتطبيقية لتعليم مفاهيم الأمن السيبراني، استخدام التعلم الذاتي والتعلم النشط. إذ بلغ المعدل العام لإجابات المبحوثين على هذه الاعتبارات نسبة (95%) (بين اتفق جدا واتفق) وبلغت قيمة الوسط الحسابي (4.3103) بانحراف معياري (0.65928) إذا تمثل نسبة استجابة المبحوثين على هذا المحور (86.21%) وبمعامل اختلاف (15.30%).

5-2. التوصيات:

1. من المهم بمكان أن يتم تعزيز الوعي الثقافي بأهمية الأمن السيبراني في مجال المحاسبة وتقديم تدريب وتحسين مستمر للمعلمين والمدربين.

2. ينبغي تطبيق الأمن السيبراني في مجالات مختلفة للمحاسبة والاستفادة من تقنيات الذكاء الاصطناعي والابتكارات في مجال الأمن السيبراني في تطوير المناهج التعليمية لتخصص المحاسبة.
3. تتضمن توجيهات لتطبيق المناهج المحاسبية وفق مجالات الأمن السيبراني هي تعزيز التعاون بين مؤسسات التعليم والقطاع الخاص لتحقيق الانسجام بين متطلبات سوق العمل والمناهج التعليمية لتخصص المحاسبة وهذا ما يتطابق مع معيار IES5 من معايير التعليم المحاسبي الدولي " متطلبات الخبرة العملية " والمجال الأول لاستيراتيجية الأمن السيبراني (الحوكمة افعالة).
4. العمل على صياغة خطة تعمل على إدماج أساليب وتقنيات الأمن السيبراني الحديثة في المقررات الدراسية لتخصص المحاسبة بهدف تزويد الطلاب بالمهارات والخبرات اللازمة لمواجهة التحديات السيبرانية في سوق العمل.
5. تعزيز مجتمع الأبحاث في مجال الأمن السيبراني وعلاقته في المحاسبة خصوصا على مستوى الدراسات العليا مثال ذلك جرائم الاحتيال الخاصة ببطاقات الائتمان وأثرها المالي على الأفراد والكيانات أو الدولة ما يسمى "Credit Card Fraud Detection" وهذا يتطابق مع المجال الخامس لاستيراتيجية الأمن السيبراني (البحث والتطوير نحو الاعتماد على الذات)
6. تضمين مفاهيم الأمن السيبراني في المقررات الدراسية لتخصص المحاسبة مثل حماية البيانات المالية، والتصدي لعمليات الاحتيال المحاسبي، وضمان سلامة النظم المحاسبية فضلا عن الحاجة إلى معرفة الشبكات والذكاء الاصطناعي والحوسبة السحابية والاتصالات الآمنة والتشفير وفق إطار معياري دولي لتقييم مخرجات هذا التطوير للمناهج وهذا يتطابق مع المجال السادس لاستراتيجية الأمن السيبراني (الامتثال والتنفيذ) المالية.
7. المشاركة الفعالة في جميع الفعاليات والمؤتمرات والمنتديات الدولية المتعلقة بالأمن السيبراني وعلاقته بالمحاسبة واستضافة مؤتمرات وورش دولية واقليمية في هذا المجال يعمل على تطوير مناهج التعليم المحاسبي في هذا المجال.وهذا يتطابق مع المجال الثامن لاستراتيجية الأمن السيبراني "التعاون الدولي"

المصادر

اولاً. المصادر العربية:

1. استراتيجية الامن السيبراني العراقي، (2017)، مستشارية الامن الوطني – امانة سر اللجنة الفنية العليا لأمن الاتصالات والمعلومات.
2. مؤشر الامن السيبراني العالمي 2024 (Global Cybersecurity Index 2024)
3. مؤشر الجاهزية الالكترونية العالمية (https://cyberspacetrends.com)
4. سالم، ماجد صدام، (2022)، الامن السيبراني العراقي وأثره في قوة الدولة، مجلة العلوم التربوية والانسانية، العدد (18)
5. السمحان، منى عبد الله، (2020)، متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية لجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد (111).
6. السقا والبرزنجي، زياد هاشم، سهى يونس، (2023)، متطلبات التدقيق الداخلي لتعزيز الامن السيبراني في الوحدات الاقتصادية في ضوء ارشادات معهد المدققين الداخليين (IIA)، مجلد تكريت للعلوم الادارية والاقتصادية، العدد (63)، مجلد (19)، ص 94-112.

ثانياً. المصادر الأجنبية:

1. Adelakun & others, (2024), Enhancing fraud detection in accounting through AI: Techniques and case studies, Finance & Accounting Research Journal, Volume 6, Issue 6, P.No. 978-999.
2. Alahmari, A., & Duncan, B. (2020, June). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA) (pp. 1-5). IEEE. researchgate.net
3. Alshurafat, H., Al Shbail, M. O., Masadeh, W. M., Dahmash, F., & Al-Msiedeen, J. M. (2021). Factors affecting online accounting education during the COVID-19 pandemic: an integrated perspective of social capital theory, the theory of reasoned action and the technology acceptance model. Education and Information Technologies, 26(6), 6995-7013. springer.com
4. Apostolou, B., Dorminey, J. W., & Hassell, J. M. (2020). Accounting education literature review (2019). Journal of Accounting Education.
5. Byrne, C. (2022). What determines perceived graduate employability? Exploring the effects of personal characteristics, academic achievements and graduate skills in a survey …. Studies in Higher Education. leedsbeckett.ac.uk
6. Chowdhury, N. & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: a systematic literature review. Information & Computer Security. ntnu.no
7. Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189-208. researchgate.net
8. Ebaid, I. E. S. (2022). Sustainability and accounting education: perspectives of undergraduate accounting students in Saudi Arabia. Journal of Applied Research in Higher Education. [HTML]
9. Haapamäki, E. & Sihvonen, J. (2022). Cybersecurity in accounting research. Artificial Intelligence in Accounting. emerald.com
10. Hanfy, F. & Khoja, M. (2023). A critical review of determinants of e-audit risk revolution in KSA. resmilitaris. resmilitaris.net
11. Hirudayaraj, M., Baker, R., Baker, F., & Eastman, M. (2021). Soft skills for entry-level engineers: What employers want. Education Sciences. mdpi.com
12. Jha, R. K. (2023). Cybersecurity and confidentiality in smart grid for enhancing sustainability and reliability. Recent Research Reviews Journal. researchgate.net
13. Lubasz, H. (2024). Adam Smith and the'free market'. Adam Smith's Wealth of Nations. [HTML]
14. Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. researchgate.net
15. Ramezan, C. A. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. Journal of Information Systems

16. Shruti M, (2024) ,Types of Cyber Attacks You Should Be Aware of in 2025, https://www.simplilearn.com/tutorials/cyber-security-tutorial/types-of-cyber-attacks
17. Strang, K. D., Che, F., & Vajjhala, N. R. (2020). Ideologies and issues for teaching blockchain cybersecurity in management and computer science. Innovations in Cybersecurity Education. academia.edu
18. Tsiligiris, V. & Bowyer, D. (2021). Exploring the impact of 4IR on skills and personal qualities for future accountants: a proposed conceptual framework for university accounting education. Accounting Education. tandfonline.com
19. Tuomala, V. (2021). Maritime cybersecurity. Before the risks turn into attacks. theseus.fi
20. Yang, C. H. & Lee, K. C. (2020). Developing a strategy map for forensic accounting with fraud risk management: An integrated balanced scorecard-based decision model. Evaluation and program planning. nscpolteksby.ac.id
21. Yee, C. K. & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. Journal of ICT in Education. upsi.edu.my

الملاحق

ملحق (1): اسماء المحكمين

ت	أسماء المحكمين واللقب العلمي	مكان العمل	التخصص
1	أ. د. زياد هاشم السقا	جامعة الموصل	محاسبة
2	أ. د. لقمان محمد ايوب	جامعة الموصل	محاسبة
3	أ. د. عبد الستار عبدالجبار الكبيسي	الجامعة الاسلامية العالمية – الاردن	محاسبة
4	أ. د. باسمة فالح النعيمي	جامعة كويه	محاسبة
5	أ.م.د. طه احمد حسن اردیني	جامعة الموصل	محاسبة
6	ا.م.د. علي مال الله عبد الله	جامعة الموصل	محاسبة
7	م. د. ابراهيم احمد محمد الحليمة	جامعة الموصل – كلية هندسة الحاسبات	امن سبراني
8	أ.م.د. عدي هاشم	جامعة الموصل – كلية علوم الحاسوب والرياضيات	امن سبراني

المصدر: من اعداد الباحث