مجلة جلة الدراسات الاقتصادية – كلية الاقتصاد – جامعة سرت المجلد (8) العدد (1)
Economic Studies Journal (ESJ), Faculty of Economics, Sirte University (Vol (8) , No (1))
April 2025
https://doi.org/10.37375/esj.v8i1.3264

أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية: دراسة تطبيقية على المصارف التجارية العاملة في مدينة سرت

د. علي مفتاح التائب، أستاذ مشارك، قسم المحاسبة، كلية الاقتصاد جامعة سرت، سرت، ليبيا
د. جبريل عمر السائح، أستاذ مساعد، قسم المحاسبة، كلية الاقتصاد، جامعة سرت، سرت، ليبيا
j.elsayih78@su.edu.ly

تاريخ وصول البحث :05/مارس/2025 تاريخ الموافقة على البحث:13/مارس/2025

الملخّص

تهدف هذه الدراسة إلى تسليط الضوء على أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية العاملة في مدينة سرت. ولتحقيق أهداف الدراسة، تم اعتماد المنهج الوصفي التحليلي، حيث تم استخدام الاستبانة كأداة رئيسية لجمع البيانات، مع التأكد من صدقها وثباتها. كما تم تحليل البيانات باستخدام برنامج (SPSS) من خلال تطبيق الأساليب الإحصائية الوصفية والاستدلالية. وأظهرت نتائج الدراسة أن موظفي المصارف التجارية في مدينة سرت يرون أن مصارفهم تدرك وتعي أهمية تطبيق الأمن السيبراني المحاسبي. كما أشارت النتائج إلى وجود تحديات وعقبات كبيرة تواجهها هذه المصارف في تطبيق الأمن السيبراني المحاسبي. بالإضافة إلى ذلك، أكدت النتائج أن هناك اهتمامًا كبيرًا من قبل المصرف المركزي والمصارف التجارية في مدينة سرت بتعزيز الأمن السيبراني المحاسبي، حيث يركز هذا الاهتمام على جوانب حيوية مثل: حماية البيانات المالية الحساسة، تعزيز الثقة والمصداقية، تقليل المخاطر، وضمان الامتثال للمعايير الأمنية. وأخيراً قدمت الدراسة مجموعة من التوصيات أهمها: يجب تنظيم دورات وورش عمل دورية لموظفي المصارف لتعزيز وعيهم بأحدث التهديدات السيبرانية وأفضل الممارسات الأمنية. كما ينبغي الاستثمار في تقنيات الأمن السيبراني المتطورة وتحديث الأنظمة بشكل مستمر لمواكبة التطورات التكنولوجية والمخاطر الجديدة. بالإضافة إلى ذلك، من الضروري تعزيز التعاون مع المصرف المركزي والجهات الحكومية لتبادل المعلومات والخبرات في مجال الأمن السيبراني، مما يدعم الجهود المشتركة في هذا المجال..

الكلمات المفتاحية

الأمن السيبراني، الامن السيبراني المحاسبي، المحاسبة، التهديدات السيبرانية، المصارف التجارية.

The importance of accounting cybersecurity in the Libyan commercial banks: empirical study on the commercial banks operating in Sirte City

Ali Muftah Eltaeb, Jibriel Omer Elsayih
j.elsayih78@su.edu.ly

Abstract

This study aims to shed light on the importance of applying accounting cybersecurity in Libyan commercial banks operating in the city of Sirte. To achieve the objectives of the study, the descriptive analytical approach was adopted, where the questionnaire was used as the main tool for collecting data, while ensuring its validity and reliability. The data were also analyzed using the (SPSS) program by applying descriptive and inferential statistical methods. The results of the study showed that employees of commercial banks in the city of Sirte believe that their banks are aware of and conscious of the importance of applying accounting cybersecurity. The results also indicated that there are major challenges and obstacles facing these banks in applying accounting cybersecurity. In addition, the results confirmed that there is great interest by the Central Bank and commercial banks in the city of Sirte in enhancing accounting cybersecurity, as this interest focuses on vital aspects such as: protecting sensitive financial data, enhancing trust and credibility, reducing risks, and ensuring compliance with security standards. Finally, the study presented a set of recommendations, the most important of

Keywords

Cybersecurity, Accounting Cybersecurity, Accounting, Cyber Threats, Commercial Banks

which are: training courses and workshops should be organized for bank employees to enhance their awareness of the latest cyber threats and best security practices. It is also necessary to invest in advanced cybersecurity technologies and continuously update systems to keep pace with technological developments and new risks. In addition, it is necessary to enhance cooperation with the Central Bank and government agencies to exchange information and expertise in the field of cybersecurity, which supports joint efforts in this field.

1- الإطار العام للدراسة

1-1 المقدمة:

في ظل التوسع الكبير في استخدام التقنيات الرقمية، أصبح الأمن السيبراني ضرورة ملحة في جميع قطاعات الاقتصاد، وخاصة في قطاع الخدمات المالية الذي يشمل المصارف وشركات التأمين وشركات الوساطة المالية. يُعد هذا القطاع الأكثر عرضة للاختراقات السيبرانية والهجمات الإلكترونية، نظرًا لاحتوائه على كميات هائلة من البيانات الحساسة، مثل المعلومات الشخصية للعملاء، وتفاصيل الحسابات، وكلمات المرور، وغيرها من البيانات ذات القيمة العالية التي تجعلها هدفًا رئيسيًا لمجرمي الإنترنت (يوسف، 2024).

وأشار تقرير صادر عن صندوق النقد الدولي (IMF) لعام 2024 إلى أن الهجمات الإلكترونية على القطاع المالي تشكل تهديدًا خطيرًا للاستقرار المالي العالمي. على الصعيد الأفريقي، أبرز تقرير موقع "بيزنس إنسايدر" الأمريكي لعام 2023 أن ليبيا تحتل المرتبة الأولى بين الدول الأفريقية الأكثر عرضة لخطر الهجمات السيبرانية، حيث جاءت في المركز الـ 90 عالميًا. وفسر التقرير ذلك بعدم توفر ضمانات كافية ضد الجرائم الإلكترونية في ليبيا، وضعف البنية التحتية المعلوماتية، بالإضافة إلى التشريعات والقوانين الضعيفة أو غير الموجودة لمكافحة التهديدات السيبرانية، مما يعرض المعاملات الحساسة لخطر كبير (عبد الله، 2024؛ وعبد المهدي، 2020).

مع ظهور الخدمات المصرفية الرقمية واعتماد المصارف بشكل متزايد على التكنولوجيا لإدارة معلوماتها المالية، تزايدت المخاطر المرتبطة بالتهديدات والاختراقات السيبرانية. يمكن أن تؤدي هذه الخروقات إلى عواقب مدمرة، بما في ذلك الخسائر المالية، وسرقة البيانات، والإضرار بسمعة المؤسسات، فضلًا عن المسؤولية القانونية (Hasan et al., 2024). كما أصبحت البيانات المحاسبية في المصارف هدفًا رئيسيًا لمجرمي الإنترنت، مما يتطلب تعزيز التدابير الأمنية لحماية معلومات العملاء والمعاملات المالية. لذا، يجب على المتخصصين في المحاسبة إدراك الأهمية الحيوية لتطبيق تدابير أمنية قوية لحماية المعلومات الحساسة، وضمان الامتثال التنظيمي، والحفاظ على سلامة البيانات المالية.

في هذا السياق، تهدف هذه الدراسة إلى دراسة وتحليل أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية، مع تسليط الضوء على أهميته ليس فقط في حماية البيانات المالية، ولكن أيضًا في ضمان الامتثال التنظيمي وتعزيز الحوكمة المؤسسية الشاملة. من خلال تحليل المخاطر الناجمة عن الهجمات السيبرانية وفحص أفضل الممارسات في هذا المجال، يسعى الدراسة إلى التأكيد على ضرورة أن تعطي المؤسسات الأولوية للأمن السيبراني ضمن أطرها المحاسبية، مما يعزز دفاعاتها ضد التهديدات السيبرانية المتطورة بشكل متزايد.

2-1 مشكلة الدراسة وتساؤلاتها:

في الفترة الأخيرة، شهدت المؤسسات المالية زيادة كبيرة في التهديدات السيبرانية، حيث أظهرت تقارير صادرة عن شركة "فورتينت" الأمريكية المتخصصة في الأمن السيبراني أن حوالي 73% من المؤسسات العالمية تعرضت لهجمات سيبرانية خلال عام 2024، مقارنة بنسبة 49% في العام السابق. وأشارت البيانات إلى أن القطاع المصرفي يُعد الأكثر استهدافًا، حيث يمثل ما يقارب 20% من إجمالي الهجمات. وتجدر الإشارة إلى أن الهجمات السيبرانية قد تتسبب في خسائر جسيمة، لا تقتصر على الأفراد فحسب، بل تمتد لتؤثر على النظام المالي بأكمله (العرابي وأبو عنزة، 2024). كما أشارت التقارير إلى أن هجمات الفدية وهجمات "ديدوس" كانت من أبرز التهديدات التي واجهتها المؤسسات الليبية، وخاصة في القطاع المصرفي خلال الفترة الأخيرة. هذه الهجمات لا تشكل خطرًا على الأمان الرقمي فحسب، بل تهدد أيضًا سمعة المؤسسات الوطنية وقدرتها على الحفاظ على ثقة العملاء (يوسف, 2024).

في ضوء هذا التصاعد المستمر في الهجمات السيبرانية، أصبح من الضروري اتخاذ إجراءات استباقية لتعزيز الأمن السيبراني وحماية البيانات الحساسة. وهذا يتطلب تحديث أدوات الأمان في الأنظمة المحاسبية الرقمية، بالإضافة إلى تطوير استراتيجيات أمنية فعالة. لذا، يتعين على المؤسسات المصرفية الاستثمار في تقنيات الأمن السيبراني المتقدمة، وتدريب الكوادر البشرية على كيفية تحديد المخاطر والتعامل معها بكفاءة (عبد الله، 2024).

بناءً على ما سبق، يرى الباحثان أن هناك حاجة ملحة لدراسة وتحليل أهمية تطبيق الأمن السيبراني المحاسبي لضمان حماية البيانات المالية في المصارف التجارية. ويمكن صياغة مشكلة الدراسة من خلال الإجابة على التساؤلات التالية:

1. هل تدرك المصارف التجارية محل الدراسة بأهمية تطبيق الأمن السيبراني المحاسبي؟
2. ما هي المشكلات أو المعوقات التي قد تحول دون تطبيق الأمن السيبراني المحاسبي في المصارف التجارية محل الدراسة؟
3. ما هي الفوائد المتوقعة من تطبيق الأمن السيبراني المحاسبي في المصارف التجارية؟

3-1 اهداف الدراسة:

تسعى هذه الدراسة الى تحقيق مجموعة من الأهداف أهمها:

1. التعرف على مفهوم الأمن السيبراني المحاسبي.
2. بيان أهمية تطبيق الأمن السيبراني المحاسبي في المصارف.
3. تحديد الصعوبات والعوائق التي تواجه تطبيق الأمن السيبراني المحاسبي في المصارف.
4. معرفة أهم المنافع التي من الممكن تحقيقها عند تطبيق الأمن السيبراني المحاسبي في المصارف.

4-1 فرضيات الدراسة:

للإجابة على التساؤلات المطروحة في مشكلة الدراسة لقد قمنا بصياغة الفرضيات التالية:

1. لا يوجد هناك إدراك ووعي لدى المصارف التجارية العاملة في مدينة سرت بأهمية تطبيق الأمن السيبراني المحاسبي.
2. لا تواجه المصارف التجارية العاملة في مدينة سرت تحديات وعقبات كبيرة في تطبيق الأمن السيبراني المحاسبي.

3. لا يوجد هناك اختلاف معنوي بين اراء عينة الدراسة حول المنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي في المصارف التجارية في مدينة سرت.

1-5 أهمية الدراسة:

تكتسب هذه الدراسة أهمية علمية وتطبيقية من عدة جوانب، أبرزها:

1.حداثة الموضوع: تتناول الدراسة موضوعًا حديثًا للغاية، حيث تعد – حسب علم الباحثان –من الدارسات القليلة في بيئة الأعمال الليبية التي تهتم بدراسة مدى تطبيق المصارف التجارية للأمن السيبراني المحاسبي، على الرغم من وجود بعض الأبحاث والدراسات التي تناولت الأمن السيبراني بشكل عام.

2.سد الفجوة العلمية: تساهم هذه الدراسة في سد فجوة علمية واضحة في مجال البحوث المحاسبية، حيث لا يزال موضوع الأمن السيبراني المحاسبي يحتاج إلى مزيد من البحث والدراسة.

3.الكشف عن الواقع والتحديات: تنبع أهمية الدراسة من خلال التعرف على مدى وعي المصارف التجارية في تطبيق الأمن السيبراني المحاسبي، والكشف عن العراقيل التي تحول دون تطبيقه، مما يساعد على فهم أفضل للوضع الحالي والتحديات التي تواجه المصارف في هذا المجال.

4.تقديم معلومات قيمة: يمكن أن تساهم الدراسة في تقديم معلومات قيمة للمؤسسات المالية الليبية، وخاصة القطاع المصرفي، لمساعدتهم في اتخاذ الإجراءات اللازمة لحماية البيانات الحساسة من التهديدات السيبرانية المتزايدة.

5.تطوير الأداء: تهدف الدراسة إلى دراسة وتحليل الأمن السيبراني المحاسبي بشكل يمكن معه الخروج بنتائج ومؤشرات من شأنها الارتقاء بمستوى أداء المصارف التجارية في هذا المجال.

6.مواجهة المخاطر: من المتوقع أن تساهم هذه الدراسة في تعزيز قدرة المصارف التجارية على مواجهة مخاطر الاحتيال والتهديدات السيبرانية، مما يساعدها على تحقيق النمو والاستدامة على المدى الطويل.

7.دعم صانعي القرار: توفر هذه الدراسة بيانات ومعلومات حول أفضل الممارسات في مجال الأمن السيبراني، مما يمكن صناع القرار من اتخاذ قرارات مستنيرة بشأن الاستراتيجيات والتقنيات المناسبة.

8. المساهمات العلمية: تُساهم الدراسة في إثراء المعرفة العلمية في مجال الأمن السيبراني المحاسبي، وتوفر إطارًا علميًا ومنهجيًا لفهم أهمية هذا المفهوم وتطبيقه في المؤسسات المالية.

9.تساعد الدراسة في تحديد الأبعاد المختلفة لأهمية الأمن السيبراني المحاسبي، مثل حماية البيانات المالية، وتعزيز الثقة، وتقليل المخاطر، وضمان الامتثال.

باختصار، تكمن أهمية هذه الدراسة في كونها تتناول موضوعًا حيويًا ومهمًا في العصر الرقمي، وتسعى إلى تقديم مساهمة علمية وعملية من خلال تسليط الضوء على واقع الأمن السيبراني المحاسبي في المصارف التجارية، وتقديم توصيات ومقترحات لتحسينه وتعزيزه.

1-6 الدراسات السابقة:

تؤكد الأدبيات السابقة على الأهمية الحيوية للأمن السيبراني في مهنة المحاسبة، حيث تتناول دراسات عديدة جوانب مختلفة لهذا الموضوع. ومن بين هذه الدراسات، دراسة **بلقاسم وحسين (2017)** هدفت إلى تحليل واقع المخاطر التي تواجه نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية بمدينة البيضاء، بالإضافة إلى تحديد الأسباب الرئيسية التي تؤدي

إلى حدوث هذه المخاطر والتهديدات، والإجراءات التي يمكن اتخاذها لمنعها. شمل مجتمع الدراسة جميع العاملين في المستويات الإدارية المختلفة بفروع المصارف التجارية الليبية العاملة في مدينة البيضاء، والبالغ عددهم (217) عاملاً. ولتحديد حجم العينة، تم الاعتماد على جدول Krejcie and Morgan (1970)، حيث بلغ حجم العينة (136) عاملاً، وتم اختيارها باستخدام الطريقة الطبقية النسبية. توصلت الدراسة إلى عدة نتائج، أهمها: وجود مخاطر مرتبطة بإدخال البيانات، التشغيل، المخرجات، والبيئة، وإن كانت بدرجة ضعيفة في المصارف التجارية الليبية محل الدراسة. كما أظهرت الدراسة أن أكثر المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المصارف قيد الدراسة هي مخاطر التشغيل. كما قدمت الدراسة مجموعة من التوصيات التي يمكن اتباعها لتعزيز أمن نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية، بالإضافة إلى الإجراءات الوقائية التي تساعد في الحد من وقوع هذه المخاطر. اما دراسة **Daoud & Serag (2022)** ركزت على تطوير إطار لدراسة تأثير الأمن السيبراني على البيانات المحاسبية لتعزيز الثقة في التقارير المالية، وذلك في ظل التطورات التكنولوجية مثل البيانات الضخمة، وإنترنت الأشياء، وتكامل أنظمة الحوسبة، وزيادة أتمتة المعاملات، والواقع الافتراضي. كما تناولت الدراسة كيفية تمكين الممارسين من تقييم تهديدات الأمن السيبراني وفهم تأثيرها على استراتيجيات الاستجابة المختلفة، وذلك من خلال الاعتماد على نهج "الحدث والتأثير والاستجابة" لتحليل آثار الأمن السيبراني على البيانات المحاسبية وزيادة الثقة والشفافية في التقارير المالية. توصلت الدراسة إلى أن الأمن السيبراني يلعب دورًا محوريًا في حماية البيانات والمعلومات داخل المؤسسات، إلا أن ذلك يتطلب استجابة فعالة من الإدارة والمستثمرين والمراجعين والجهات التنظيمية. واقترحت الدراسة مجموعة من الاستراتيجيات الفعّالة التي ينبغي على المؤسسات تبنيها لتعزيز الأمن السيبراني، وهي: إجراء تقييم شامل للمخاطر لتحديد التهديدات المحتملة، تعزيز الوعي الأمني من خلال تدريب الموظفين على أفضل ممارسات الأمن السيبراني، تنفيذ تحديثات دورية للبرمجيات وأنظمة التشغيل لتقليل نقاط الضعف، وضع خطط استجابة للحوادث لضمان التعامل السريع والفعال مع أي خروقات أمنية، وتعزيز التعاون بين فرق الأمن السيبراني وفرق المراجعة الداخلية لتحسين فعالية الإجراءات الأمنية.

اما دراسة **Hasan وآخرون (2024)** هدفت إلى اختبار الأهمية الحاسمة للأمن السيبراني في حماية البيانات المالية في مهنة المحاسبة في سياق التهديدات السيبرانية المتزايدة. اعتمدت الدراسة على تحليل نوعي، يشمل دراسات الحالة والمقابلات مع الخبراء، لفحص دمج تقنيات الأمن السيبراني المتقدمة، مثل الذكاء الاصطناعي والبلوك تشين والتشفير، من قبل شركات كبرى مثل Deloitte وPwC وEY. وأظهرت النتائج فعالية استراتيجيات الأمن السيبراني في تعزيز حماية البيانات ومكافحة الاحتيال، على رغم وجود تحديات مستمرة مثل التكاليف المرتفعة والتطور السريع للتهديدات. وخلصت الدراسة إلى توصية بضرورة الابتكار المستمر في مجال الأمن السيبراني لضمان حماية البيانات المالية في العصر الرقمي، وتطرقت دارسة **(Abrahams, et. al, 2024)** إلى استكشاف العلاقة بين المحاسبة والأمن السيبراني، مع التركيز على كيفية تكامل هذين المجالين لتعزيز الامتثال والشفافية داخل المؤسسات. اعتمدت هذه الدراسة على أساليب إحصائية ونماذج تحليلية لتحديد الأنماط والعلاقات بين المحاسبة والأمن السيبراني، بالإضافة إلى تحديد الفجوات البحثية والممارسات الحالية. وأظهرت النتائج أن التكامل الفعّال بين المحاسبة والأمن السيبراني يعزز من حماية البيانات المالية، ويزيد من مستوى

الشفافية، ويقلل من المخاطر القانونية، مما يسهم في تحسين الأداء المؤسسي والامتثال للأنظمة. كما اقترحت الدراسة استراتيجيات شاملة تشمل تعزيز التعاون بين الفرق المختلفة والتحديث المستمر للتقنيات والإجراءات الأمنية، وقد سعت دارسة **النقودي (2024)** إلى فحص أثر الأمن السيبراني نحو تعزيز التحول الرقمي في بيئة الأعمال المحاسبية، مع التركيز على تقنية البلوك تشين كركيزة لقاعدة البيانات في نظام المعلومات المحاسبي. وقد اعتمدت الباحثة منهج البحث الاستكشافي أو النوعي نظراً لحداثة موضوع الدراسة، بالإضافة إلى إجراء مقابلات مع خبراء متخصصين في هذا المجال، وتوصلت الدراسة إلى أن تعزيز الأمن السيبراني يلعب دورًا محوريًا في نجاح التحول الرقمي في رقمنة الأعمال المحاسبية، حيث يعزز الثقة في البيانات المحاسبية ويقلل من مخاطر الاختراق والتلاعب، كما يدعم استمرارية الأعمال من خلال حماية الأنظمة من الهجمات الإلكترونية. وأشارت الدراسة أيضًا إلى أن تقنية البلوك تشين توفر منصة آمنة وشفافة لتبادل المعلومات المالية، مما يسهم في تحسين الكفاءة التشغيلية وخفض التكاليف، أوصت الدراسة بضرورة تعزيز البنية التحتية للأمن السيبراني، إلى جانب تطوير السياسات المحاسبية والإجراءات الأمنية. كما أكدت على أهمية تدريب المحاسبين والمراجعين على أفضل ممارسات الأمن السيبراني، مع التركيز على استخدام تقنيات البلوك تشين بشكل آمن وفعّال. فيما تناولت دراسة **يوسف (2024)** تحليلًا معمقًا لأثر التهديدات السيبرانية على نُظم المعلومات المحاسبية في المؤسسات المالية الليبية، مع التركيز على تحليل الدراسات السابقة التي تناولت هذا الموضوع في كل من ليبيا والعالم العربي. واستندت الدراسة إلى منهجية وصفية لتحليل البيانات، حيث تم اختيار عينة شملت مجموعة من الأبحاث السابقة التي أعدها خبراء متخصصون في هذا المجال. أشارت نتائج الدراسة الى ان المؤسسات المالية الليبية تواجه تهديدات سيبرانية متنوعة، بما في ذلك الاختراقات الإلكترونية، وسرقة البيانات المالية، والتجسس الصناعي، بالإضافة إلى تعطيل الخدمات المصرفية عبر الإنترنت. وقد أوضحت الدراسة أن هذه التهديدات يمكن أن تؤثر سلبًا على المعلومات المحاسبية، مما يشكل خطرًا على سرية البيانات وموثوقيته، كما أوصت الدراسة بأن تقوم المؤسسات المالية بتقييم وتحديث سياسات الأمان والإجراءات المرتبطة بنظم المعلومات المحاسبية، وذلك لضمان توفير حماية فعّالة ضد التهديدات السيبرانية. كما شددت على أهمية تطبيق نظم رصد متطورة لاكتشاف الهجمات السيبرانية في مراحلها المبكرة والاستجابة لها بسرعة وكفاءة، في حين سعت دراسة **عبد الله (2024)** إلى استكشاف طبيعة الأمن السيبراني وأنظمة محاسبة التكاليف الرقمية في شركات القطاع العقاري المصري. اعتمدت الدراسة على منهجية تحليل البيانات باستخدام أدوات إحصائية لفحص العلاقات بين المتغيرات المختلفة. وكشفت النتائج عن وجود علاقة إحصائية ذات دلالة معنوية بين الأمن السيبراني وأنظمة التكاليف الرقمية. كما أوصت الدراسة بضرورة تعزيز الأمان السيبراني على مستوى الشبكات والأنظمة والتطبيقات، مع التركيز على تحسين تقنيات الحماية وتدريب الموظفين على كيفية التعامل مع الهجمات السيبرانية المحتملة، كما ركزت دراسة **Polishchuk et al. (2024)** على تحليل تأثير الأمن السيبراني على استقرار المؤسسات المالية، مع إبراز دور التدابير الأمنية في تعزيز مرونة هذه المؤسسات، خاصة في مواجهة التهديدات السيبرانية. تمثلت منهجية الدراسة في استخدام الأساليب النوعية لاستكشاف تجارب المؤسسات المالية الأوكرانية التي اعتمدت على استراتيجيات دفاعية رقمية متقدمة لضمان استمراريتها، لا سيما في ظل الظروف الصعبة الناتجة عن النزاعات العسكرية العالمية. أظهرت الدراسة أن أنظمة الأمن السيبراني الفعّالة تلعب دورًا محوريًا في ضمان الاستدامة التشغيلية والمالية للمؤسسات المالية. كما أكدت على أهمية

التحديث المستمر للبرامج والأجهزة، بالإضافة إلى تحسين الحلول الإدارية لمواجهة التهديدات السيبرانية المتطورة. وأوصت الدراسة بضرورة تبني الابتكار المستمر كأداة رئيسية لتعزيز الأمن السيبراني وضمان الحماية الفعالة للمؤسسات المالية. وأخيراً دراسة تحليلية أجراها **Morshed and Khrais (2025)** في منطقة دول مجلس التعاون الخليجي، تم التركيز على استكشاف تأثير ممارسات الأمن السيبراني والمساءلة الأخلاقية والأطر التنظيمية، والتقنيات الناشئة على اعتماد أنظمة المحاسبة الرقمية وبناء الثقة بها. اعتمدت الدراسة على منهجية بحثية كمية، حيث تم جمع البيانات من عينة عشوائية مكونة من 324 متخصصًا يمثلون مختلف دول مجلس التعاون الخليجي. ولتحليل البيانات، استخدم الباحثون نمذجة المعادلات الهيكلية الجزئية للمربعات الصغرى (PLS-SEM). أظهرت نتائج الدراسة أن تدابير الأمن السيبراني الفعّالة، وآليات الكشف عن التهديدات المعتمدة على الذكاء الاصطناعي، وبرامج تدريب الموظفين المصممة خصيصًا تسهم بشكل كبير في تسهيل تبني أنظمة المعلومات المحاسبية الرقمية وزيادة الثقة بها. كما أشارت النتائج إلى أن المساءلة الأخلاقية تلعب دورًا وسيطًا في تعزيز هذه التأثيرات، بينما تعمل الأطر التنظيمية الداعمة على تحسين فعالية استراتيجيات الأمن السيبراني. كما قدّمت الدراسة مجموعة من التوصيات الرئيسية، منها ضرورة مواءمة الأطر التنظيمية في دول مجلس التعاون الخليجي مع المعايير الدولية، وتعزيز برامج تدريب القوى العاملة، بالإضافة إلى الاستفادة من التقنيات المعتمدة على الذكاء الاصطناعي لاكتشاف التهديدات السيبرانية وإدارتها بشكل استباقي.

ما يميز الدراسة الحالية عن الدراسات السابقة

لقد تميزت هذه الدراسة عن الدراسات السابقة بعدة جوانب مهمة وهي:

1. تعتبر هذه الدراسة، حسب علم الباحثان، يمكن ان تكون الأولى من نوعها التي تتناول بشكل خاص مدى أهمية تطبيق المصارف التجارية للأمن السيبراني المحاسبي في المصارف التجارية بليبيا، وتحديدًا في مدينة سرت.

2. تسعى الدراسة إلى تقديم رؤى عملية حول مدى وعي المصارف التجارية في تطبيق الأمن السيبراني المحاسبي، والكشف عن العراقيل التي تحول دون تطبيقه، مما يجعلها مرجعًا قيمًا للمؤسسات المالية في المنطقة.

3. تنطلق الدراسة من بيئة بحثية فريدة تختلف عن تلك التي اعتمدت عليها معظم الدراسات السابقة.

4. في حين ركزت الدراسات السابقة التي أُجريت في ليبيا على جوانب أخرى، تركز هذه الدراسة بشكل خاص على مدى قدرة المصارف التجارية على مواجهة مخاطر التهديدات السيبرانية، مما يمنحها أهمية خاصة في فهم التحديات المحلية.

5. الدراسة تركز على مدينة سرت بشكل خاص، مما يعطيها طابع محلي فريد، ويقدم نتائج مميزة تعكس خصوصية هذه المنطقة.

1-7 منهجية الدراسة:

من أجل تحقيق أهداف الدراسة واختبار فرضياتها، اعتمدت هذه الدراسة على المنهج الوصفي التحليلي. حيث تم تغطية الجانب النظري من خلال مراجعة الكتب والدوريات العربية والأجنبية، بالإضافة إلى الأبحاث ذات الصلة بموضوع الدراسة. أما بالنسبة للجزء العملي من الدراسة (الدراسة الميدانية)، فقد

قام الباحثان بإعداد استبانة تم تصميمها بشكل يتوافق مع متطلبات الدراسة، وذلك بهدف جمع البيانات اللازمة وتحليلها باستخدام الأساليب الإحصائية المناسبة، مما يسهم في تحقيق أهداف الدراسة بشكل فعّال.

2- الإطار النظري

2-1 مفهوم واهمية تطبيق الأمن السيبراني

2-1-1 تعريف الأمن السيبراني:

عَرَّف الحيمودي (2023) الأمن السيبراني بأنه "مجموعة من الإجراءات والتقنيات المصمَّمة لحماية أنظمة الحاسوب والشبكات والبرمجيات والبيانات من التهديدات الإلكترونية والهجمات السيبرانية. ويهدف إلى منع الاختراقات والوصول غير المصرح به، وحماية المعلومات الحساسة، وضمان استمرارية العمليات التقنية والمؤسسية بشكل آمن".

في حين يرى Canelón et al., (2020) ان الأمن السيبراني عبارة عن مصفوفة من الأدوات التنظيمية والتقنية والإجرائية، إلى جانب الممارسات التي تهدف إلى حماية الحواسيب والشبكات والبيانات الموجودة داخلها من الاختراقات أو التلف أو التغيير غير المصرح به، أو تعطيل الوصول إلى المعلومات أو الخدمات. ويُعتبر الأمن السيبراني توجهاً عالمياً يُطبق على مستوى الدول، وكذلك في المنظمات الحكومية والشركات.

من جهة أخرى، عَرَّفه مطروح وأونيس (2022) بأنه "مجموعة من الإجراءات والسياسات والأدوات والمفاهيم الأمنية والمبادئ التوجيهية التي تُستخدم لتحديد وتقييم وتقليل المخاطر التي تهدد البيئة الإلكترونية. ويتضمن ذلك معالجة المعلومات، وحماية الموارد الرقمية، وتنظيم أصول المستخدمين. كما تشمل هذه الإجراءات التدريب على أفضل الممارسات وضمان الاستخدام الأمن للتقنيات المختلفة التي تساهم في حماية الأنظمة والشبكات الإلكترونية".

وبناءً على ما سبق، يمكن تعريف "الأمن السيبراني" بأنه مجموعة من الممارسات والتقنيات والعمليات المصمَّمة لحماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية والوصول غير المصرح به أو التلف. ويشمل ذلك تدابير مثل استخدام الجدران النارية، والتشفير، وأنظمة الكشف عن التسلل، بالإضافة إلى إدارة الهويات والوصول

2-1-2 أهمية تطبيق الأمن السيبراني في المحاسبة:

في العصر الرقمي الحالي، أصبحت البيانات المالية والمحاسبية عرضة بشكل متزايد للهجمات السيبرانية، مما يجعل تطبيق الأمن السيبراني المحاسبي أمرًا حيويًا لحماية المؤسسات والشركات من المخاطر والتحديات المتعددة. تتجلى أهمية الأمن السيبراني في المحاسبة في عدة جوانب رئيسية:

حماية البيانات المالية: تحتوي الأنظمة المحاسبية على معلومات حساسة للغاية، مثل البيانات المالية للمؤسسة، وسجلات العملاء، وكشوف الحسابات، والتقارير المالية. أي اختراق قد يؤدي إلى سرقة هذه البيانات أو التلاعب بها، مما قد يتسبب في خسائر مالية كبيرة، وفقدان الميزة التنافسية، والإضرار بسمعة المؤسسة (Abrahams et al, 2024).

الامتثال للقوانين واللوائح: تفرض العديد من القوانين واللوائح الدولية، مثل GDPR في الاتحاد الأوروبي وSOX في الولايات المتحدة، متطلبات صارمة لحماية البيانات المالية والشخصية. عدم الامتثال لهذه القوانين يمكن أن يؤدي إلى

غرامات مالية كبيرة وعقوبات قانونية (Tawalbeh et al, 2023).

منع الاحتيال: يمكن أن تساعد تقنيات الأمن السيبراني في اكتشاف ومنع الأنشطة الاحتيالية، مثل التلاعب في السجلات المالية أو تحويل الأموال بشكل غير قانوني (العرابي وأبو عنزه, 2024).

ضمان استمرارية الأعمال: الهجمات الإلكترونية يمكن أن تعطل العمليات التجارية، مما يؤدي إلى توقف العمل وفقدان الإيرادات. الأمن السيبراني يساعد في ضمان استمرارية الأعمال من خلال حماية الأنظمة الحيوية. (Abrahams et al, 2023).

حماية سمعة المؤسسة: أي خرق أمني يمكن أن يؤثر سلبًا على سمعة المؤسسة، خاصة إذا تم تسريب بيانات العملاء أو الموردين. الأمن السيبراني يساعد في الحفاظ على ثقة العملاء والمستثمرين (موسى وآخرون 2024).

إدارة المخاطر: الأمن السيبراني يساعد في تحديد وتقييم وإدارة المخاطر المرتبطة بالبيانات المالية والأنظمة المحاسبية، مما يقلل من احتمالية حدوث خسائر مالية أو تشويه للبيانات (العرابي وأبو عنزه, 2024).

2-2 نظرة عامة على الاعتماد المتزايد على التكنولوجيا في ممارسات المحاسبة

أدى الاعتماد المتزايد على التكنولوجيا في مجال المحاسبة إلى إحداث تحول جذري في مشهد الإدارة المالية. بفضل ظهور البرامج المتقدمة والحلول السحابية، أصبح المحاسبون قادرين على أتمتة العمليات، وزيادة الدقة، وتسهيل إعداد التقارير في الوقت الفعلي. وقد ساهمت هذه التطورات في تبسيط العمليات المحاسبية، مما يتيح للمؤسسات الوصول السريع إلى البيانات المالية الحيوية، وبالتالي تعزيز قدراتها على اتخاذ القرارات بشكل أكثر فعالية. ومع ذلك، فإن هذا الاعتماد المتزايد على الأدوات التكنولوجية يثير مخاوف كبيرة فيما يتعلق بالأمن السيبراني. فمع تحول البيانات إلى صيغ رقمية بشكل متزايد، تزداد كمية المعلومات الحساسة المعرضة لخطر الاختراقات الإلكترونية. ولتجنب هذه الثغرات الأمنية، يتعين على المنظمات تبني نهج استراتيجي شامل للأمن السيبراني يأخذ في الاعتبار التفاعل المعقد بين التكنولوجيا والنزاهة المالية. بالإضافة إلى ذلك، فإن النظر إلى الأمن السيبراني باعتباره "قضية معرفية" يمكن أن يساعد المؤسسات على تطوير أنظمة قوية تمكنها من التعامل مع التعقيدات الناتجة عن الاعتماد على التكنولوجيا في الممارسات المحاسبية. وهذا يضمن تحقيق الكفاءة التشغيلية مع الحفاظ على حماية البيانات بشكل فعال (Sallos et al. 2019).

3-2 مخاطر التهديدات السيبرانية في المحاسبة

يُشكِّل ظهور التهديدات السيبرانية في قطاع المحاسبة خطراً كبيراً يهدد سلامة المعلومات المالية وموثوقيتها. ومع اعتماد المنظمات بشكل متزايد على المنصات الرقمية لتخزين ومعالجة البيانات المالية الحساسة، يستغل مجرمو الإنترنت نقاط الضعف في الأنظمة لاختراق بروتوكولات الأمان. وتترتب على هذه الاختراقات عواقب وخيمة، مثل الخسائر المالية الكبيرة، والمخاطر القانونية، وتضرر السمعة أمام أصحاب المصلحة. وتشير الأبحاث إلى وجود علاقة إيجابية بين حوادث الأمن السيبراني وزيادة رسوم التدقيق، حيث يقوم المدققون بتعديل رسومهم لتعويض المخاطر المرتبطة بانتهاكات البيانات (Moreira et al.2019). بالإضافة إلى ذلك، تبرز حوكمة رأس المال الفكري، بما في ذلك أمن المعلومات، كأحد

الأولويات الرئيسية لمجالس الإدارة، التي تتحمل مسؤولية حماية الموارد القيمة لمؤسساتها من هذه التهديدات (Renaud et al. 2019). لذلك، يُعد تعزيز تدابير الأمن السيبراني أمراً ضرورياً لضمان دقة العمليات المحاسبية والحفاظ على ثقة أصحاب المصلحة، مما يعزز من قدرة المؤسسات على مواجهة التحديات السيبرانية المتزايدة.

2-4 أنواع التهديدات الإلكترونية التي يواجهها القطاع المصرفي

يواجه القطاع المصرفي في ظل التحول الرقمي تحديات جسيمة ناتجة عن تزايد المخاطر الإلكترونية، التي لا تقتصر تأثيراتها على اختراق البيانات الحساسة فحسب، بل تمتد إلى تعريض أمن الأنظمة المالية للخطر. ومع تطور هذه التهديدات بشكل مستمر، أصبح من الضروري أن تواكب البنوك أحدث أساليب الهجمات الإلكترونية وأن تعزز إجراءاتها الوقائية لضمان حماية فعالة لبنيتها التحتية وبيانات عملائها. فيما يلي أبرز أنواع التهديدات الإلكترونية استناداً لما جاءت به دراسة Unar et al. (2024) ودراسة العرابي وأبو عنزه، (2024).

برامج الفدية: تقوم برامج الفدية بتشفير البيانات أو تعطيل الوصول إليها، ثم يطالب المهاجمون بدفع فدية لإعادة البيانات أو استعادة الوصول إليها. ويمكن أن تتسبب هجمات برامج الفدية في تعطيل العمليات التجارية بشكل كامل، وفقدان بيانات العملاء الهامة، وتشويه سمعة المؤسسة.

التصيد الاحتيالي: يعتمد التصيد الاحتيالي على خداع الموظفين لحملهم على الكشف عن معلومات سرية مثل كلمات المرور أو معلومات الحسابات المصرفية. يتم ذلك غالبًا من خلال رسائل بريد إلكتروني أو مواقع ويب مزيفة تبدو وكأنها من مصادر موثوقة. ويمكن أن يؤدي التصيد الاحتيالي إلى سرقة بيانات العملاء، واختراق الأنظمة الداخلية للشركة، وسرقة الأموال.

التهديدات الداخلية: تأتي التهديدات الداخلية من داخل المؤسسة نفسها، سواء من موظفين ساخطين أو عن طريق الإهمال غير المتعمد من الموظفين. يمكن أن تؤدي هذه التهديدات إلى تسريب المعلومات السرية، تخريب الأنظمة، أو حتى سرقة البيانات، مما يشكل خطراً كبيراً على أمن المنظمة وسلامة عملياتها.

البرامج الضارة: البرامج الضارة هي برامج مصممة لإلحاق الضرر بنظام الكمبيوتر أو سرقة البيانات. يمكن أن تنتشر هذه البرامج عبر رسائل البريد الإلكتروني المخادعة، أو مواقع الويب الملوثة، أو الملفات التي يتم تنزيلها. وتتسبب البرامج الضارة في أضرار جسيمة، مثل تلف الملفات، تعطيل أنظمة التشغيل، سرقة المعلومات الحساسة، وحتى التجسس على أنشطة المستخدمين.

هجمات رفض الخدمة: تهدف هجمات رفض الخدمة إلى إغراق خوادم المؤسسة بكمية كبيرة من حركة المرور، مما يجعلها غير قادرة على الاستجابة للطلبات المشروعة. يمكن أن تؤدي هذه الهجمات إلى تعطيل خدمات المؤسسة وموقعها الإلكتروني بشكل كامل، مما يتسبب في خسائر مالية كبيرة وفقدان العملاء بسبب توقف الخدمات.

2-5 أفضل الممارسات لتعزيز الأمن السيبراني المحاسبي

لضمان أمن المعلومات المالية الحساسة، يجب على المصارف تبني استراتيجية شاملة للأمن السيبراني تتضمن مجموعة من الإجراءات الوقائية والاستباقية. هذه الإجراءات ضرورية لحماية البيانات من التهديدات المتزايدة في العصر الرقمي.

فيما يلي تفصيل لأفضل الممارسات التي يمكن تطبيقها (Torres et al. 2024 , (Shaker et al.2023))

2-5-1 تقييم المخاطر المنتظمة:

الأهمية: يساعد تقييم المخاطر في تحديد نقاط الضعف المحتملة في النظام المحاسبي، مما يسمح باتخاذ إجراءات استباقية لتقليل احتمالية حدوث اختراقات.

الإجراءات: إجراء تقييمات دورية وشاملة للمخاطر لتقييم الثغرات الأمنية تحليل التهديدات المحتملة وتحديد أولويات الإجراءات التصحيحية.

2-5-2 توعية الموظفين وتدريبهم:

الأهمية: يعتبر الموظفون خط الدفاع الأول ضد الهجمات السيبرانية، لذا يجب تزويدهم بالمعرفة اللازمة للتعرف على التهديدات مثل التصيد الاحتيالي (Phishing) والبرمجيات الخبيثة.

الإجراءات: إجراء برامج تدريبية منتظمة وشاملة لرفع مستوى الوعي الأمني لدى الموظفين وتدريبهم على أفضل الممارسات الأمنية.

2-5-3 تشفير البيانات:

الأهمية: يضمن التشفير حماية البيانات من الوصول غير المصرح به حتى في حالة اختراق النظام.

الإجراءات: استخدام تقنيات تشفير قوية لحماية البيانات أثناء التخزين والنقل، والتأكد من أن جميع الأجهزة التي تحتوي على بيانات حساسة مشفرة.

2-5-4 تحديث البرامج بانتظام:

الأهمية: التحديثات الأمنية تسد الثغرات التي يمكن أن يستغلها المهاجمون للوصول إلى النظام.

الإجراءات: تثبيت التحديثات الأمنية والتصحيحات فور صدورها، وكذلك التأكد من أن جميع البرامج وأنظمة التشغيل محدثة إلى آخر إصدار.

2-5-5 مراقبة الأنظمة والكشف عن التهديدات:

الأهمية: المراقبة المستمرة تسمح بالكشف المبكر عن أي نشاط مشبوه، مما يتيح اتخاذ إجراءات سريعة لمنع الهجمات أو تقليل تأثيرها.

الإجراءات: المراقبة المستمرة تسمح بالكشف المبكر عن أي نشاط مشبوه، مما يتيح اتخاذ إجراءات سريعة لمنع الهجمات أو تقليل تأثيرها، وتحليل لأنماط السلوكية لتحديد الأنشطة غير المعتادة التي قد تشير إلى هجوم محتمل.

من خلال مما سبق يمكن القول بان تنفيذ هذه الإجراءات وتكاملها في استراتيجية شاملة للأمن السيبراني، يمكن للمصارف تعزيز دفاعاتها ضد التهديدات السيبرانية وحماية بياناتها المالية وبيانات عملائها بشكل فعال.

3: الجانب العملي للدراسة

3-1 تمهيد

تهدف هذا الدراسة إلى تحديد "أهمية تطبيق الأنظمة السيبرانية المحاسبية في المصارف التجارية الليبية"، مع التركيز على معالجة الموضوع من الناحية العلمية باستخدام أسلوب الاستبيان كأداة رئيسية لجمع البيانات. تم تصميم الاستبيان بناءً على الإطار

النظري للدراسة، واستُخدم برنامج "SPSS" لإجراء التحليل الإحصائي واختبار الفرضيات.

لتحقيق أهداف الدراسة، تم اعتماد منهجية متعددة المداخل، حيث تم استخدام "المنهج الاستقرائي" لاستقراء الظواهر المختلفة المرتبطة بأهداف الدراسة. يعتمد هذا المنهج على دراسة الجزئيات للوصول إلى تعميمات عامة، مما يمهد لتكوين فرضيات تمثل حلولًا محتملة لمشكلة الدراسة. ومع ذلك، نظرًا لأن المنهج الاستقرائي وحده لا يكفي لتلبية جميع متطلبات الدراسة، تم أيضًا استخدام "المنهج الاستنباطي"، الذي يعتمد على تفسير الظواهر من خلال العموميات للوصول إلى الجزئيات. يساعد هذا المنهج في استخلاص النتائج المنطقية التي تدعم الفرضيات وتستبعد تلك التي لا تتوافق مع الحقائق.

من خلال هذه المنهجيات المزدوجة، تم التوصل إلى نتائج وتوصيات الدراسة باستخدام إجراءات البحث العلمي والتحليل الإحصائي للبيانات واختبار الفرضيات.

2-3 مجتمع وعينة الدراسة

تم اختيار مجتمع الدراسة من المصارف التجارية العاملة في مدينة سرت، والتي تضم: مصرف الوحدة (المقر الرئيسي وفرع الجامعة)، المصرف التجاري الوطني فرع سرت، مصرف الجمهورية، مصرف شمال أفريقيا، مصرف التجارة والتنمية، ومصرف الصحاري. ويرجع هذا الاختيار إلى عدة أسباب: أولاً: تُعد هذه المصارف من أكثر القطاعات استخدامًا للتقنيات المالية الحديثة لتحسين خدماتها المقدمة للعملاء. ثانيًا: تتعرض هذه المصارف بشكل كبير للتهديدات الإلكترونية بسبب طبيعة البيانات المالية الحساسة التي تتعامل معها. ثالثًا: تتماشى هذه المصارف مع أهداف الدراسة التي تركّز على أهمية الأمن الإلكتروني المحاسبي في القطاع المصرفي. قد بلغ العدد الكلي المستهدف للاستبانة (189) موظفًا وموظفة، حيث تم توزيع استمارات الاستبيان على جميع المصارف المذكورة. بعد عمليات التوزيع والفحص، تم استبعاد (46) استمارة إما لعدم استرجاعها أو لعدم اكتمال البيانات وعدم صلاحيتها للتحليل، ليتبقى اجمالي الاستمارات الصحيحة القابلة للتحليل الاحصائي (143) استمارة بنسبة استجابة 75.66%. الجدول رقم (1) يوضح عدد استمارة الاستبيان التي تم توزيعه على عينة الدراسة.

جدول (1) يوضح توزيع الاستبيان

ت م	البيان	الاستمارات الموزعة	الاستمارات المستلمة	النسبة %
1	شمال افريقيا	17	15	%88.24
2	الصحاري	24	22	%91.66
3	الجمهورية	23	18	%78.26
4	الوحدة الرئيسي	35	22	%62.86
5	الوحدة الوكالة	30	23	%76.67
6	التجارة والتنمية	25	18	%43
7	التجاري	35	25	%71.43
	الإجمالي	189	143	%75.66
	الاستمارات المستبعدة (المفقودة أو غير صالحة)			46

ملاحظة: يعرض هذا الجدول تفاصيل توزيع استمارات الاستبيان على عينة الدراسة، والتي شملت المصارف التجارية العاملة في مدينة سرت. كما يبين الجدول عدد الاستمارات التي تم توزيعها، وعدد الاستمارات التي تم استلامها، بالإضافة إلى عدد الاستمارات المستبعدة.

3-3 مصادر جمع البيانات:

اعتمدت الدراسة على مصدرين رئيسيين للبيانات، وهما:

1. المصادر الثانوية: تم الاعتماد على البيانات الثانوية لتحديد الإطار النظري للدراسة، حيث تم جمعها من الأدبيات المتعلقة بموضوع الدراسة، بما في ذلك الكتب والأبحاث المنشورة في المجلات العلمية، بالإضافة إلى الدراسات السابقة ذات الصلة.
2. المصادر الأولية: تم تصميم استبيان يتضمن أسئلة مغلقة تعتمد على مقياس ليكرت الخماسي، إلى جانب بعض الأسئلة المفتوحة، وتم توزيعه على عينة الدراسة لجمع البيانات المطلوبة.

3-4 أداة جمع البيانات:

لتحقيق أهداف الدراسة، تم اعتماد استمارة الاستبيان كأداة رئيسية لجمع البيانات والمعلومات من مجتمع الدراسة وعينته. تُعد استمارة الاستبيان وسيلة فعالة للحصول على معلومات من عدد كبير من الأفراد، تفوق القدرة التي تغطيها أدوات جمع البيانات الأخرى مثل المقابلات والملاحظة، بالإضافة إلى ما توفره هذه الأداة من توفير للوقت والجهد.

لذلك، تم تصميم استمارة استبيان شاملة لتغطية جميع جوانب المشكلة ومتغيراتها. تضمنت الاستمارة في مقدمتها رسالة توضح الغرض من الدراسة، مع تأكيدات للمشاركين بخصوص سرية المعلومات وعدم مشاركتها مع أي طرف ثالث.

تألفت الاستبانة من جزأين رئيسيين:

- الجزء الأول: خُصص لدراسة خصائص عينة الدراسة، حيث تضمن معلومات شخصية عن المشاركين. اشتمل هذا الجزء على أربع أسئلة، كل منها يحتوي على مجموعة من الإجابات الاختيارية.
- الجزء الثاني: تم تقسيمه إلى فقرات وفرضيات الدراسة، حيث تم طرح ثلاث فرضيات.

ولقياس واختبار متغيرات الدراسة، تم استخدام "مقياس ليكرت الخماسي" لتقييم الفقرات، كما هو موضح في الجدول رقم (2).

جدول رقم (2) درجات بدائل الإجابة على فقرات الاستبيان

الإجابة	غير موافق بشدة	غير موافق	محايد	موافق	موافق بشدة
الدرجة	1	2	3	4	5

حيث كان الوسط الحسابي الفرضي (لأداة القياس) هو (3)، ويتم استخراجه عن طريق المعادلة الرياضية التالية (1+2+3+4+5) /5=3

3-5 الأساليب الإحصائية المستخدمة:

سيتم الاعتماد على البرنامج الإحصائي SPSS لتحليل بيانات الدراسة، مع استخدام الأساليب الإحصائية التالية:

1. الإحصاء الوصفي: سيتم استخدام الانحراف المعياري والمتوسط الحسابي لوصف البيانات وتحليلها.
2. معامل الصدق والثبات الفاكرونباخ.
3. اختبار T test.

تم استخدام تحليل التباين الأحادي (One – way – ANOVA)

3-6 صدق وثبات الاستبانة

للتأكد من دقة صياغة فقرات الاستبيان وسلامة العبارات المستخدمة، أي لضمان صدق وموثوقية النموذج، تم عرض الاستبيان على مجموعة من المحكمين المكونة من أعضاء هيئة التدريس المتخصصين. واعتُبرت الفقرات صادقة وصالحة للقياس إذا حظيت بموافقة المحكمين. بناءً على آرائهم وملاحظاتهم، تم

تعديل وإعادة صياغة بعض الفقرات لتعزيز مستوى الصلاحية والمصداقية للاستبيان.

أما لاختبار دقة وثبات القياس ومدى الاعتمادية، فقد تم تقييم ثبات الاستبيان باستخدام "**اختبار معامل ألفا كرونباخ**". يعتمد هذا الاختبار على مبدأ أن كلما اقتربت قيمة معامل ألفا كرونباخ من الرقم1، كلما دل ذلك على قوة ثبات أداة الدراسة.

جدول رقم (3) نتائج معامل ألفا كرونباخ لقياس درجة الثبات والاعتمادية

ر. م	محاور الاستبيان	عدد الفقرات	قيمة الفا كرونباخ
1	إدراك ووعي المصرف بأهمية تطبيق الأمن السيبراني المحاسبي	7	**0.830**
2	العقبات التي تواجه المصارف في تطبيق الأمن السيبراني المحاسبي	6	**0.865**
3	المنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي	7	**0.912**
4	تطبيق الأمن السيبراني المحاسبي في المصارف التجارية	11	**0.902**
الاجمالي للمتوسط		**31**	**0.877**

يوضح الجدول رقم (3) أن أداة الدراسة (الاستبيان) تتمتع بثبات عالٍ، حيث تجاوزت قيمة معامل ألفا كرونباخ للفقرات الحد الأدنى المقبول. هذا يشير إلى أنه في حال إعادة توزيع الاستبيان على نفس عينة الدراسة، فإن النتائج ستكون متسقة وبنفس المعدل المحسوب، مما يؤكد موثوقية الأداة وقدرتها على قياس المتغيرات بدقة.

ويوضح الجدول رقم (3) قيمة الثبات في كل فقرة من فقرات الاستبيان حيث ان معدل الفاكرونباخ حيث أن أقل معامل ثبات كان لإدراك ووعي المصرف بأهمية تطبيق الأمن السيبراني المحاسبي والذي بلغ 0.830، بينما أعلى معدل ثبات كان 0.912 والمتعلق بالمنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي. وبشكل عام إن اجمالي قيمة متوسط الفقرات حوالي (0.877) وهي قيمة عالية فيما يتعلق بدرجة الاعتمادية.

3-7 عرض وتحليل البيانات واختبار الفرضيات

3-7-1 عرض النتائج المتعلقة بالمعلومات الشخصية

تناول الجزاء الاول من الاستمارة بعض الاسئلة التي توضح خصائص المشاركين في الدراسة، فيما يلي عرض لنتائج توزيع عينة الدراسة:

3-7-1-1 حسب الجنس.

يوضح الجدول رقم (4) توزيع عينة الدراسة حسب الجنس، والتي شملت (143) فردًا. أظهرت النتائج أن نسبة الذكور بين العاملين في المصارف التجارية كانت أعلى من نسبة الإناث، حيث بلغت نسبة الذكور (71.3%) من إجمالي العينة، بينما كانت نسبة الإناث (28.7%). يعكس هذا التوزيع طبيعة المجتمع الليبي المحافظ، حيث يُتوقع أن تكون نسبة الذكور أعلى في مثل هذه القطاعات.

جدول (4) يوضح توزيع عينة الدراسة حسب الجنس

معلومات الشخصية	البيان	التكرار	النسبة المئوية
الجنس	ذكر	102	%71.3
	انثى	41	%28.7
الإجمالي		143	%100.0

3-7-1-2 حسب المؤهل العلمي

يوضح الجدول رقم (5) توزيع عينة الدراسة حسب المؤهل العلمي، والتي بلغ عددها (143) فردًا من العاملين في المصارف التجارية. أظهرت النتائج أن نسبة حاملي مؤهل الدبلوم بلغت (36.4%)، في حين أن نسبة حاملي مؤهل البكالوريوس كانت الأعلى، حيث وصلت إلى (61.5%). أما نسبة الحاصلين على درجة الماجستير فكانت (2.1%). تشير هذه النتائج إلى أن غالبية المشاركين في الدراسة هم من خريجي البكالوريوس، مما يعكس التركيز الأكاديمي السائد بين العاملين في هذا القطاع.

جدول (5) يوضح توزيع عينة الدراسة حسب المؤهل العلمي

معلومات الشخصية	البيان	التكرار	النسبة المئوية
المؤهل العلمي	دبلوم	52	%36.4
	بكالوريوس	88	%61.5
	ماجستير	3	%2.1
الإجمالي		143	%100.0

3-7-1-3 حسب المركز الوظيفي

يوضح الجدول رقم (6) إلى أن غالبية المشاركين في الاستبيان ينتمون إلى فئة الموظفين المحاسبين في المصارف، حيث بلغت نسبتهم (41.3%)، وذلك نظرًا لخبرتهم الواسعة في هذا المجال. أما نسبة المراجعين فكانت (11.2%)، بينما مثل الموظفون الفنيون (10.5%) من إجمالي عينة الدراسة. أما باقي أفراد العينة، فقد تم توزيعهم كالتالي: مديرو إدارة بنسبة (2.8%)، ونواب مدير بنسبة (2.8%)، في حين شملت الفئة الأخرى (31.5%) من عينة الدراسة.

جدول (6) يوضح توزيع عينة الدراسة حسب المركز الوظيفي

معلومات الشخصية	البيان	التكرار	النسبة المئوية
المركز الوظيفي	مدير إدارة	4	%2.8
	نائب مدير	4	%2.8
	محاسب	59	%41.3
	مراجع	16	%11.2
	فني	15	%10.5
	غير ذلك	45	%31.5

3-7-1-4 حسب سنوات الخبرة

يوضح الجدول رقم (7) توزيع عينة الدراسة، التي بلغ عددها (143) فردًا، فيما يتعلق بأهمية التطبيق السيبراني المحاسبي في المصارف التجارية الليبية. تم تصنيف سنوات الخبرة إلى أربع فئات، تبدأ من أقل من خمس سنوات وتصل إلى خمس عشرة سنة فأكثر. وقد سجلت الفئة ذات الخبرة الأطول (خمس عشرة سنة فأكثر) أعلى نسبة، حيث بلغت (34.3%)، مما يشير إلى أن أفراد عينة الدراسة يتمتعون بخبرة عالية، وهو ما ينعكس إيجابًا على نتائج الدراسة.

جدول (7) يوضح توزيع عينة الدراسة حسب سنوات الخبرة

معلومات الشخصية	البيان	التكرار	النسبة المئوية
سنوات الخبرة	اقل من 5 سنوات	43	%30.1
	من 5 الي اقل من 10سنوات	27	%18.9
	من 10 الي اقل من 15سنة	24	%16.8
	من 15 سنة فأكثر	49	%34.3
الإجمالي		143	%100.0

3-7-2 عرض النتائج المتعلقة بأسئلة الدراسة

أولاً: النتائج المتعلقة بآراء المشاركين حول إدراك ووعي المصرف بأهمية تطبيق الأمن السيبراني المحاسبي: وتتناول السؤال التالي: "هل تدرك المصارف التجارية محل الدراسة بأهمية تطبيق الأمن السيبراني المحاسبي؟ لتحليل هذا السؤال، تم حساب المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات هذا السؤال، بالإضافة إلى المستوى الكلي للاستجابات. يتم عرض هذه النتائج تفصيليًا في الجدول رقم (8).

جدول (8) آراء المشاركين حول إدراك ووعي المصرف بأهمية تطبيق الأمن السيبراني المحاسبي

الفقرات	المتوسط	الانحراف المعياري	ترتيب الاهمية
لا يدرك بعض المديرين والعاملين في المصرف بأهمية الأمن السيبراني المحاسبي وتأثيره على المؤسسة.	3.73	0.905	4
لا يكون الموظفون على دراية كافية بالمخاطر السيبرانية وكيفية التعامل معها.	3.66	0.888	5
شعور بعض الموظفين بالخوف أو القلق من استخدام التقنيات الجديدة في مجال الأمن السيبراني.	3.52	0.999	6
عدم وعي العملاء بأهمية الأمن السيبراني وكيفية حماية حساباتهم.	3.85	0.974	3
عقد ورش عمل ودورات تدريبية للموظفين حول أهمية الأمن السيبراني	4.13	0.804	1
فرض الجهات التنظيمية، مثل المصرف المركزي، معايير أمنية إلزامية يزيد من وعي المصارف بضرورة تطبيق الأمن السيبراني.	4.06	0.846	2
إدراك المصرف لأهمية الأمن السيبراني يساعده على الاستعداد بشكل أفضل لمواجهة التهديدات.	4.13	0.838	1
المتوسط – الإجمالي	3.86	0.893	

يوضح الجدول (8) اتجاهات إجابات أفراد عينة الدراسة حول فقرات إدراك ووعي المصرف بأهمية تطبيق الأمن السيبراني المحاسبي، حيث بلغ المتوسط الإجمالي للإجابات (3.86) بانحراف معياري (0.893). جاءت قيم المتوسطات الحسابية لتلك الفقرات أعلى من المتوسط الفرضي لأداة القياس (3)، مما يعكس مواقف إيجابية نحو الفقرات المطروحة.

يتبين من الجدول رقم (8) أن المتوسط الحسابي لفقرات هذا السؤال يتراوح بين 3.52 و4.13. وقد حصلت الفقرتان التاليتان على أعلى متوسط حسابي، حيث بلغ 4.13 لكل منهما:" **عقد ورش عمل ودورات تدريبية للموظفين حول أهمية الأمن السيبراني** ". والفقرة "**إدراك المصرف لأهمية الأمن السيبراني يساعد على الاستعداد بشكل أفضل لمواجهة التهديدات**"، يشير هذا المتوسط المرتفع إلى أن مستوى تطبيق هذه الفقرات يُعتبر جيدًا، مما يعكس حرص إدارة المصرف على تنظيم ورش العمل والدورات التدريبية لتعزيز وعي الموظفين، ومساعدتهم على الاستعداد بشكل أفضل لمواجهة التهديدات السيبرانية. كما يتبين من الجدول رقم (8) أن الفقرة التالية: "**فرض الجهات التنظيمية مثل المصرف المركزي معايير أمنية إلزامية يزيد من وعي المصارف بضرورة تطبيق الأمن السيبراني** "، جاءت في الترتيب الثاني بمتوسط حسابي بلغ 4.06. يشير هذا المتوسط إلى أن مستوى تطبيق هذه الفقرة يُعتبر جيدًا، مما يعكس دور المصرف المركزي في تعزيز الوعي بأهمية الأمن السيبراني من خلال فرض معايير أمنية إلزامية على المصارف. في المقابل، حصلت الفقرة التالية: " **شعور بعض الموظفين بالخوف أو القلق من استخدام التقنيات الجديدة في مجال الأمن السيبراني** "، على الترتيب الاخير بمتوسط حسابي بلغ 3.85. يشير هذا المتوسط إلى أن مستوى تطبيق هذه الفقرة يُعتبر متوسطًا، مما يعكس أن بعض الموظفين في المصارف يشعرون بالخوف أو القلق من استخدام التقنيات الحديثة في مجال الأمن السيبراني.

كما أظهرت النتائج اتفاقًا واسعًا على ضرورة تعزيز التدريب وزيادة التوعية في هذا المجال. بالإضافة إلى ذلك، هناك إجماع على أن إدراك المصرف لأهمية الأمن السيبراني يُعد عاملاً أساسيًا لتعزيز الاستعداد ومواجهة التهديدات المحتملة بشكل فعال.

ثانياً: النتائج المتعلقة بآراء المشاركين حول العقبات التي تواجه المصارف في تطبيق الأمن السيبراني المحاسبي: وتتناول السؤال التالي:" ما هي المشكلات أو المعوقات التي قد تحول دون تطبيق الأمن السيبراني المحاسبي في المصارف التجارية محل الدراسة؟ " لتحليل هذا السؤال، تم حساب المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات هذا السؤال، بالإضافة إلى المستوى الكلي للاستجابات. يتم عرض هذه النتائج تفصيليًا في الجدول رقم (9).

جدول (9) آراء المشاركين حول العقبات التي تواجه المصارف في تطبيق الأمن السيبراني المحاسبي

الفقرات	المتوسط	الانحراف المعياري	ترتيب الأهمية
يعاني المصرف من محدودية الموارد المالية المتاحة لتطبيق حلول الأمن السيبراني المحاسبي	3.78	1.031	3
يواجه المصرف نقصًا في الموارد البشرية المدربة والمؤهلة في مجال الأمن السيبراني	3.83	1.034	2
قلة الكوادر المؤهلة لإعطاء دورات تدريبية مهنية في الامن السيبراني.	3.85	0.999	1
لا يمتلك المصرف الموارد الكافية لتغطية تكاليف التطبيق.	3.48	0.898	4
صعوبة الالتزام بالتشريعات واللوائح المحلية والدولية المتعلقة بحماية البيانات.	3.48	0.883	4
عدم وجود تنسيق كافي بين إدارات المصرف المختلفة لتنفيذ إجراءات الأمن السيبراني.	3.57	0.873	5
المتوسط – الإجمالي	3.66	0.953	

وضح الجدول (9) اتجاهات إجابات أفراد عينة الدراسة حول العقبات التي تواجه المصارف في تطبيق الأمن السيبراني المحاسبي، حيث بلغ المتوسط الإجمالي للإجابات (3.66) بانحراف معياري (0.953). جاءت قيم المتوسطات الحسابية لتلك الفقرات أعلى من المتوسط الفرضي لأداة القياس (3)، مما يعكس وجود تحديات واضحة في تطبيق الأمن السيبراني.

يتبين من الجدول رقم (9) أن المتوسط الحسابي لفقرات هذا السؤال يتراوح بين 3.48 و3.85. وقد حصلت الفقرة الثالثة على أعلى متوسط حسابي، حيث بلغ 3.85 " **قلة الكوادر المؤهلة لإعطاء دورات تدريبية مهنية في الأمن السيبراني** "، يشير هذا المتوسط المرتفع إلى أن مستوى تطبيق هذه الفقرات يُعتبر جيدًا، مما يعكس وجود نقص في الكوادر المؤهلة لتقديم دورات تدريبية متخصصة في مجال الأمن السيبراني. كما يتضح من الجدول رقم (9) أن الفقرة التالية: " **يواجه المصرف نقصًا في الموارد البشرية المدربة مهنية في الأمن االسيبراني**"، جاءت في الترتيب الثاني بمتوسط حسابي بلغ 3.83. يشير هذا المتوسط إلى أن مستوى تطبيق هذه الفقرة يُعتبر جيدًا، مما يعكس أن المصارف تعاني من نقص في الموارد البشرية المؤهلة والمدربة في مجال الأمن السيبراني. في المقابل، حصلت الفقرة التالية: " **عدم وجود تنسيق كافي بين ادارات المصرف المختلفة لتنفيذ اجراءات الأمن السيبراني** "، على الترتيب الاخير بمتوسط حسابي بلغ 3.57. يشير هذا المتوسط إلى أن مستوى تطبيق هذه الفقرة يُعتبر متوسطًا، مما يعكس وجود ضعف في التنسيق بين إدارات المصرف المختلفة لتنفيذ إجراءات الأمن السيبراني بشكل فعال.

تشير هذه النتائج إلى أن أبرز العقبات التي تواجه المصارف في تطبيق الأمن السيبراني المحاسبي تشمل محدودية الموارد المالية، نقص الكوادر المدربة، وصعوبة الالتزام بالتشريعات المحلية والدولية. كما أظهرت النتائج وجود تحديات تتعلق بالتنسيق بين إدارات المصرف المختلفة.

ثالثاً: النتائج المتعلقة بآراء المشاركين حول المنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي: وتتناول السؤال التالي:" ما هي الفوائد المتوقعة من تطبيق الأمن السيبراني المحاسبي في المصارف التجارية؟ " لتحليل هذا السؤال، تم حساب المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات هذا السؤال، بالإضافة إلى المستوى الكلي للاستجابات. يتم عرض هذه النتائج تفصيليًا في الجدول رقم (10).

جدول (10) آراء المشاركين حول المنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي

الفقرات	المتوسط	الانحراف المعياري	ترتيب الاهمية
ضمان سرية وسلامة البيانات المالية والحسابات المصرفية.	4.13	0.680	1
زيادة ثقة العملاء في المصرف بسبب ضمان أمان معاملاتهم المالية.	4.12	0.655	2
جذب عملاء جدد يبحثون عن مؤسسات مالية ذات معايير أمان عالية.	4.08	0.764	3
الحد من احتمالية التعرض للهجمات الإلكترونية مثل الاختراقات أو سرقة البيانات.	4.02	0.843	5

ضمان سلامة الأصول المالية للمصرف والعملاء.	3.98	0.860	6
توفير بيئة آمنة تمكن المصرف من تبني تقنيات جديدة مثل الخدمات المصرفية الرقمية.	4.03	0.719	4
تحسين إدارة المخاطر واتخاذ القرارات بشكل أكثر فعالية.	4.08	0.783	3
المتوسط – الإجمالي	4.06	0.768	

يوضح الجدول (10) اتجاهات إجابات أفراد عينة الدراسة حول المنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي، حيث بلغ المتوسط الإجمالي للإجابات (4.06) بانحراف معياري (0.768). جاءت قيم المتوسطات الحسابية لتلك الفقرات أعلى من المتوسط الفرضي لأداة القياس (3)، مما يعكس إدراكًا كبيرًا لأهمية وفوائد تطبيق الأمن السيبراني.

يتبين من الجدول رقم (10) أن المتوسط الحسابي لفقرات هذا السؤال يتراوح بين 3.98 و4.13. وقد حصلت الفقرة الأولى على أعلى متوسط حسابي، حيث بلغ 4.13" **ضمان سرية و سلامة البيانات المالية و الحسابات المصرفية**"، يشير هذا المتوسط المرتفع إلى أن مستوى تطبيق هذه الفقرات يُعتبر جيدًا، مما يعكس حرص المصارف على ضمان سرية وسلامة البيانات المالية والحسابات المصرفية. كما يتبين من الجدول رقم (10) أن الفقرة التالية: "**زيادة ثقة العملاء في المصرف بسبب ضمان أمان معاملاتهم المالية**"، جاءت في الترتيب الثاني بمتوسط حسابي بلغ 4.12. يشير هذا المتوسط إلى أن مستوى تطبيق هذه الفقرة يُعتبر جيدًا، مما يعكس أن ضمان أمان المعاملات المالية يساهم بشكل كبير في تعزيز ثقة العملاء في المصرف. في المقابل، حصلت الفقرة التالية: "**ضمان سلامة الأصول المالية للمصرف والعملاء**"، على الترتيب الأخير بمتوسط حسابي بلغ 3.98. يشير هذا المتوسط إلى أن مستوى تطبيق هذه الفقرة يُعتبر متوسطًا، مما يعكس أن سلامة الأصول المالية للمصرف والعملاء تحتاج إلى مزيد من التحسين والاهتمام.

تشير هذه النتائج إلى أن أفراد العينة يرون أن تطبيق الأمن السيبراني المحاسبي يحقق فوائد كبيرة، بما في ذلك ضمان سرية البيانات، زيادة ثقة العملاء، جذب عملاء جدد، والحد من الهجمات الإلكترونية. كما يؤكدون على دور الأمن السيبراني في تحسين إدارة المخاطر وتمكين المصارف من تبني التقنيات الحديثة.

رابعاً: النتائج المتعلقة بآراء المشاركين حول أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية: وتتناول السؤال التالي:" ما أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية؟ " لتحليل هذا السؤال، تم حساب المتوسط الحسابي والانحراف المعياري لكل فقرة من فقرات هذا السؤال، بالإضافة إلى المستوى الكلي للاستجابات. يتم عرض هذه النتائج تفصيليًا في الجدول رقم (11).

جدول (11) آراء المشاركين حول أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية

لفقرات	المتوسط	الانحراف المعياري	ترتيب الاهمية
يحرص المصرف المركزي على تعزيز وتطبيق معايير الأمن السيبراني المحاسبي في المصارف التجارية.	4.10	.664	2
يقوم المصرف المركزي بوضع معايير وضوابط صارمة للأمن السيبراني المحاسبي، وتلزم المصارف التجارية بتطبيقها.	3.94	.700	7
هناك تعاون مع الجهات الحكومية والمؤسسات الأخرى لتبادل المعلومات والخبرات في مجال الأمن السيبراني المحاسبي.	3.90	.776	8
شرع المصرف المركزي في إعادة هيكلة البنية التحتية للمصارف التجارية بهدف تفعيل وتطبيق معايير الأمن السيبراني المحاسبي.	3.94	.739	7
يقوم المصرف المركزي بالإشراف على المصارف التجارية للتأكد من التزامها بمعايير الأمن السيبراني المحاسبي.	4.06	.758	2
يحرص المصرف على الامتثال للوائح والمعايير المتعلقة بأمن البيانات المالية.	3.98	.809	6
يحرص المصرف على الامتثال للوائح والمعايير المتعلقة بأمن البيانات المالية.	3.98	.809	6
يسعى المصرف الى تقليل المخاطر المرتبطة بالاحتيال والأخطاء البشرية عن طريق تطبيق الامن السيبراني.	3.99	.769	5
يعمل المصرف على تحديث أنظمة الأمن السيبراني بشكل دوري.	3.90	.754	8
يعتمد المصرف نهجًا استباقيًا لإدارة المخاطر، من خلال تطبيق استراتيجيات أمنية متطورة.	4.01	.774	4
يمتلك المصرف إجراءات أمن سيبراني كافية لحماية البيانات المالية	3.90	.811	8
المتوسط – الإجمالي	4.53	0.747	

يوضح الجدول (11) اتجاهات إجابات أفراد عينة الدراسة حول تطبيق الأمن السيبراني المحاسبي في المصارف التجارية، حيث بلغ المتوسط الإجمالي للإجابات (4.53) بانحراف معياري (0.747). جاءت قيم المتوسطات الحسابية لتلك الفقرات أعلى من المتوسط الفرضي لأداة القياس (3)، مما يعكس إدراكًا كبيرًا لأهمية تطبيق الأمن السيبراني في القطاع المصرفي.

يظهر من الجدول رقم (11) أن الفقرة السادسة حصلت على أعلى مستوى موافقة، حيث تنص على "**يساعد تطبيق الأمن السيبراني المحاسبي على الحفاظ على ثقة العملاء في المصرف**"، بمتوسط حسابي بلغ 4.14، وهي درجة مرتفعة. هذا المتوسط المرتفع يشير إلى أن مستوى تطبيق هذه الفقرة جيد، مما يعكس دور تطبيق الأمن السيبراني المحاسبي في تعزيز ثقة العملاء في المصرف. من ناحية أخرى، كانت الفقرات الثالثة والتاسعة والحادية عشر هي الأقل موافقةً. الفقرة الثالثة تنص على "**هناك تعاون مع الجهات الحكومية والمؤسسات الأخرى لتبادل المعلومات والخبرات في مجال الأمن السيبراني المحاسبي**"، بينما تنص الفقرة التاسعة على "**يعمل المصرف على تحديث أنظمة الأمن السيبراني بشكل دوري**"، والفقرة الحادية عشر تنص على "**يمتلك المصرف إجراءات أمن سيبراني كافية لحماية البيانات المالية**". بلغ المتوسط الحسابي لكل من هذه الفقرات 3.90، مما يشير إلى أن مستوى تطبيقها يعتبر متوسطًا. هذا يعكس وجود تعاون مع الجهات الحكومية والمؤسسات الأخرى في مجال الأمن السيبراني المحاسبي، بالإضافة إلى قيام المصرف بتحديث أنظمته الأمنية بشكل دوري وامتلاكه إجراءات أمنية كافية لحماية البيانات المالية، ولكن بدرجة أقل مقارنة بالفقرة السادسة.

بشكل عام، تشير هذه النتائج إلى أن أفراد العينة يرون أن تطبيق الأمن السيبراني المحاسبي في المصارف التجارية يحظى باهتمام كبير من قبل المصرف المركزي والمصارف نفسها، مع تركيز على تعزيز الثقة، تقليل المخاطر، وضمان الامتثال للمعايير الأمنية.

3-7-3 عرض النتائج المتعلقة باختبار خضوع البيانات إلى التوزيع الطبيعي

يوضح الجدول التالي نتائج الاختبار الإحصائي الذي تم إجراؤه لتحديد نوع البيانات الأولية المستخدمة في الدراسة. كما يظهر من الجدول رقم (12) ان اتجاه اجابات افراد عينة الدراسة حول فقرات المتعلقة بأهمية التطبيق السيبراني المحاسبي في المصارف التجارية الليبية حيث كانت نتائج الوسط الحسابي كالاتي إدراك ووعي المصرف بإمكانية تطبيق الأمن السيبراني المحاسبي حوالي (3.87)، والعقبات التي تواجه المصارف في تطبيق الأمن السيبراني المحاسبي حوالي (3.66)، والمنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي (4.06) تطبيق الأمن السيبراني المحاسبي في المصارف التجارية (4.53).

جدول (12) التوزيع الطبيعي للمتوسط الحسابي والانحراف المعياري

One-Sample Statistics

البيان	المتوسط	الانحراف المعياري
إدراك ووعي المصرف بأهمية تطبيق الأمن السيبراني المحاسبي	3.87	0.893
العقبات التي تواجه المصارف في تطبيق الأمن السيبراني المحاسبي	3.66	0.953
المنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي	4.06	0.768
تطبيق الأمن السيبراني المحاسبي في المصارف التجارية	4.53	0.747
اجمالي المتوسطات	4.03	0.840

3-7-4 عرض النتائج المتعلقة باختبار الفرضيات

اختبار الفرضية الاولى

الفرضية الصفرية H0: لا يوجد هناك ادراك ووعي لدى المصارف التجارية العاملة في مدينة سرت بأهمية تطبيق الأمن السيبراني المحاسبي.

جدول (13) يوضح نتائج اختبار الفرضية الأولى

One-Sample Test

T الجدولية	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	T المحسوبة	مستوى الدلالة Sig. (2-tailed)	نتيجة الفرضية الصفرية
1.684	3.87	0.893	142	5.222	0.000	رفض

دال احصائيا عند مستوى الدالة ≥ 0.05

يبين الجدول رقم (13) ان الوسط الحسابي المحسوب الاجمالي الفقرات التي تقيس أهمية التطبيق السيبراني المحاسبي في المصارف التجارية الليبية قد بلغ (3.87) وهو يزيد عن الوسط الحسابي الفرضي وهو (3) و الانحراف المعياري (0.893) وان T المحسوبة عند (5.222) وهي اكبر من قيمتها الجدولة (T الجدولة 1.684) كما يلاحظ ان مستوى الدالة الاحصائية قد بلغ (sig.0.000) وهو يقل عن مستوى الدالة الاحصائية المعتمدة بالدراسة (0.05) وبالتالي فان الاختبار الاحصائي (t) يعد دال احصائيا ونستخلص من ذلك ان

نتيجة الاختبار الاحصائي تؤكد رفض الفرض العدمي (HO) وقبول الفرض البديل (H1) الذي يقول أنه يوجد هناك ادراك ووعي لدى المصارف التجارية العاملة في مدينة سرت بأهمية تطبيق الأمن السيبراني المحاسبي .

اختبار الفرضية الثانية

الفرضية الصفرية H0: لا تواجه المصارف التجارية العاملة في مدينة سرت تحديات وعقبات كبيرة في تطبيق الأمن السيبراني المحاسبي.

جدول (14) يوضح نتائج اختبار الفرضية الثانية

One-Sample Test

T الجدولية	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	T المحسوبة	مستوى الدلالة Sig. (2-tailed)	نتيجة الفرضية الصفرية
1.684	3.66	0.953	142	4.636	0.000	رفض

دال احصائيا عند مستوى الدالة ≥ 0.05

يظهر الجدول رقم (14) أن المتوسط الحسابي الإجمالي لفقرات قياس أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية قد بلغ (3.66)، وهو أعلى من المتوسط الحسابي الفرضي البالغ (3)، مع انحراف معياري قدره (0.953). كما بلغت قيمة (T) المحسوبة (4.636)، وهي تفوق القيمة الجدولية المقابلة لها (T الجدولية = 1.684). بالإضافة إلى ذلك، لوحظ أن مستوى الدلالة الإحصائية (sig.) بلغ (0.000)، وهو أقل من مستوى الدلالة الإحصائية المعتمد في الدراسة (0.05). وبالتالي، فإن الاختبار الإحصائي (t) يعتبر ذا دلالة إحصائية. من هذه النتائج، نستنتج أن الاختبار الإحصائي يؤكد رفض الفرضية العدمية (HO) وقبول الفرضية البديلة (H1)، والتي تشير إلى أن المصارف التجارية العاملة في مدينة سرت تواجه تحديات وعقبات كبيرة في تطبيق الأمن السيبراني المحاسبي.

اختبار الفرضية الثالثة

الفرضية الصفرية H0: لا يوجد هناك اختلاف معنوي بين اراء عينة الدراسة حول المنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي لدى المصارف التجارية .

جدول (15) يوضح نتائج اختبار الفرضية الثالثة

One-Sample Test

T الجدولية	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	T المحسوبة	مستوى الدلالة Sig. (2-tailed)	نتيجة الفرضية الصفرية
1.684	4.06	0.768	142	6.391	0.000	رفض

دال احصائيا عند مستوى الدالة ≥ 0.05

يظهر الجدول رقم (15) أن المتوسط الحسابي الإجمالي لفقرات قياس أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية قد بلغ (4.06)، وهو أعلى من المتوسط الحسابي الفرضي البالغ (3)، مع انحراف معياري قدره (0.768). كما بلغت قيمة (T) المحسوبة (6.391)، وهي تفوق القيمة الجدولية المقابلة لها (T الجدولية = 1.684). بالإضافة إلى ذلك، لوحظ أن مستوى الدلالة الإحصائية (sig.) بلغ (0.000)، وهو أقل من مستوى الدلالة الإحصائية المعتمد في الدراسة (0.05). وبالتالي، فإن الاختبار الإحصائي (t) يعتبر ذا دلالة إحصائية. من هذه النتائج، نستنتج أن الاختبار الإحصائي يؤكد رفض الفرضية العدمية (HO) وقبول الفرضية

البديلة (H1)، والتي تشير انه يوجد اختلاف معنوي بين اراء عينة الدراسة حول المنافع المتوقع تحقيقها عند تطبيق الأمن السيبراني المحاسبي لدى المصارف التجارية.

8-3 النتائج والتوصيات

اولاً: النتائج

النتائج التي توصلت إليها الدراسة:

1- أن المتوسط الحسابي لإجابات أفراد العينة حول الفقرات التي تقيس مدى إدراك ووعي المصارف التجارية العاملة في مدينة سرت بإمكانية تطبيق الأمن السيبراني المحاسبي قد بلغ (3.87)، وهو أعلى من المتوسط الحسابي الفرضي البالغ (3). كما بلغت قيمة اختبار (T) (5.222) عند مستوى دلالة إحصائية (sig.0.000). وبالتالي، تؤكد هذه النتيجة إلى أن الموظفين في المصارف التجارية بمدينة سرت يرون أن مصارفهم تدرك وتعي أهمية تطبيق الأمن السيبراني المحاسبي.

2- أظهرت النتائج رفض الفرضية العدمية وقبول الفرضية البديلة التي تفيد بأن المصارف التجارية العاملة في مدينة سرت تواجه تحديات وعقبات كبيرة في تطبيق الأمن السيبراني المحاسبي. حيث بلغ المتوسط الحسابي لإجابات أفراد العينة حول الفقرات المرتبطة بهذه الفرضية (3.66)، وهو أعلى من المتوسط الحسابي الفرضي البالغ (3). كما سجلت قيمة اختبار (T) (4.636) عند مستوى دلالة إحصائية (sig.0.000)، مما يعزز صحة هذه النتيجة.

3- يشير الاختلاف المعنوي في آراء عينة الدراسة حول الفوائد المتوقعة من تطبيق الأمن السيبراني المحاسبي في المصارف التجارية إلى وجود تباين في وجهات نظر الموظفين تجاه هذه الفوائد. وقد يعود هذا التباين إلى عدة عوامل، منها: تفاوت مستوى الوعي بأهمية الأمن السيبراني بين الموظفين، مما يؤثر على تقديرهم للفوائد المتوقعة، واختلاف وجهات النظر بين الموظفين في الإدارات المختلفة، حيث يركز كل منهم على الجوانب التي تتناسب مع طبيعة عمل إدارتهم..

4- أن هناك اهتمامًا كبيرًا بالأمن السيبراني المحاسبي في المصارف التجارية في مدينة سرت، سواء من قبل المصرف المركزي أو المصارف نفسها. وهذا الاهتمام يركز على عدة جوانب حيوية، أهمها: حماية البيانات المالية الحساسة، تعزيز الثقة والمصداقية، تقليل المخاطر، وضمان الامتثال للمعايير الأمنية.

5- تعكس هذه النتائج ارتفاع مستوى الوعي بأهمية الأمن السيبراني في القطاع المصرفي الليبي، كما تُؤكد الحاجة إلى مواصلة تعزيز وتطوير إجراءات الأمن السيبراني المحاسبي لضمان حماية المصارف وعملائها من المخاطر المحتملة.

ثانياً: التوصيات

بناءً على النتائج التي خلصت إليها الدراسة، يقدم الباحثان التوصيات التالية:

1-ضرورة عقد دورات وورش عمل منتظمة للموظفين بالمصارف لتوعيتهم بأحدث التهديدات السيبرانية وأفضل الممارسات الأمنية.

2-ضرورة إطلاق حملات توعية موجهة للعملاء لتعريفهم بأهمية الأمن السيبراني وطرق حماية حساباتهم الشخصية.

3-ينبغي على المصارف الاستثمار في تقنيات الأمن السيبراني الحديثة وتحديث الأنظمة بشكل مستمر.

4-ضرورة تطبيق إجراءات أمنية متقدمة في المصارف لحماية البيانات المالية، مثل أنظمة الكشف عن التسلل، وجدران الحماية، وتقنيات التشفير.

5-ضرورة التعاون مع المصرف المركزي والجهات الحكومية الأخرى لتبادل المعلومات والخبرات في مجال الأمن السيبراني.

6-ينبغي على المصارف توظيف مختصين في مجال الأمن السيبراني وتوفير برامج تدريبية مستمرة لرفع كفاءتهم.

7-يجب على المصارف التجارية العمل على توحيد وجهات نظر الموظفين حول المنافع المتوقعة من تطبيق الأمن السيبراني المحاسبي من خلال توفير التدريب والتوعية اللازمة.

قائمة المراجع:

أولاً: المراجع العربية:

– الحيمودي, بدر. (2023). الأمن السيبراني وحماية الأنظمة المعلوماتية. مجلة شمال إفريقيا للنشر العلمي (NAJSP), 174-189. 189.

– العرابي، ماجد قليل محمد، أبو عنزه، اسماء. (2024). دراسة تطبيقية عن دور إدارة المخاطر في تعزيز الأمن السيبراني للمؤسسات الصغيرة والمتوسطة في المملكة العربية السعودية". المجلة الدولية للعلوم المالية والإدارية والاقتصادية، الإصدار (3)، العدد (10).

– النقودي, سوزي فاروق. (2024). أثر الأمن السيبراني على تعزيز تقنيات التحول الرقمي في بيئة الأعمال المحاسبية. مجلة البحوث المحاسبية, 11(4) , 169-216.

– بالقاسم، أمحارب سعد سليمان، وحسين، أحمد محمد سليم. (2017). واقع مخاطر أمن نظم المعلومات المحاسبية الإلكترونية بالمصارف التجارية الليبية العاملة بمدينة البيضاء. المؤتمر العلمي الدولي الأول: التحوط وإدارة الخطر بالصناعة المالية الإسلامية، عمان: مركز السنابل للبحث وتطوير الموارد البشرية ومركز بيان للهندسة المالية والإسلامية، 25 – 55.

– عبد الله، إيمان السيد محمد (2024). دارسة العلاقة بين تفعيل ادوات الأمن السيبارني وأنظمة محاسبة التكاليف الرقمية: دارسة تطبيقية على شركات القطاع العقاري بمصر، المجلة العلمية للبحوث والدراسات التجارية، المجلد 38 – العدد الأول.

– عبد الله، وليد. (2024). الهجمات السيبرانية المتكررة تقلق المؤسسات المالية في ليبيا. اندبندنت عربية.

– عبد المهدي، حنين (2020). " أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية", رسالة ماجستير غير منشورة، كلية الاقتصاد والعلوم الإدارية، جامعة آل البيت، ص 19-26.

– محيي الدين إبراهيم موسي، مي، بكر عربي الشريف، محمد، & سعيد عبد العظيم أحمد، أحمد. (2024). الآليات المقترحة لتفعيل دور الأمن السيبراني في تحسين أداء المحاسب الإداري وإنعكاسه على الميزة التنافسية للمنشأة. المجلة العلمية للدراسات التجارية والبيئية, 15(3) , 26-52.

– مطروح، وفاء.، وأونيس، ابتسام (2022). تداعيات جائحة كوفيد-19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر. المجلة الدولية للاتصال الاجتماعي, 9(2) , 219-241.

- يوسف، علد السلام عطية عبد السلام (2024). تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية: دراسة وصفية، المجلة العلمية للدراسات التجارية والبيئية، المجلد الخامس عشر، العدد الأول.

ثانياً: المراجع الأجنبية:

- Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). "Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity". Computer Science & IT Research Journal, (5)1, p. 121, 133.
- Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2023). Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security. *World Journal of Advanced Research and Reviews*, *20*(3), 1743-1756.
- Canelón, J., Huerta, E., Leal, N., & Ryan, T. (2020). Unstructured data for cybersecurity and internal control. Proceedings of the 53rd Hawaii International Conference on System Sciences.
- Daoud, M. M., & Serag, A. A. (2022). A proposed Framework for Studying the Impact of Cybersecurity on Accounting Information to Increase Trust in The Financial Reports in the Context of Industry 4.0: An Event, Impact and Response Approach. *Trade and Finance*, 42(1), 20-61
- Hasan, L., Hossain, M. Z., Johora, F. T., & Hasan, M. H. (2024). Cybersecurity in accounting: Protecting financial data in the digital age. *European Journal of Applied Science, Engineering and Technology*, *2*(6), 64-80.
- Moreira, G. P. (2019). Cybersecurity and External Audit: The Disclosure of Risk Factors in Annual Reports (Master's thesis, Universidade Catolica Portuguesa (Portugal)), https://core.ac.uk/download/237231002.pdf
- Morshed, A., & Khrais, L. T. (2025). Cybersecurity in Digital Accounting Systems: Challenges and Solutions in the Arab Gulf Region. *Journal of Risk and Financial Management*, *18*(1), 41.
- Polishchuk, V., Fedirko, N., Grytsyshen, D., Ohdanskyi, K., & Kotkovskyy, V. (2024). Analysis of the Impact of Cybersecurity on The Stability of Financial Institutions. International Journal of Religion, 5(9), 302-309.
- Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security?. Journal of Intellectual Capital, 20(5), 621-641. https://core.ac.uk/download/237029625.pdf.
- Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019).

Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital, 20(4), 581-597.

- Shaker, A. S., Al Shiblawi, G. A. K., Union, A. H., & Hameedi, K. S. (2023). The role of information technology governance on enhancing cybersecurity and its reflection on investor confidence. *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, *8*(6), 7.
- Tawalbeh, L., Tawalbeh, H., Song, H., & Shen, Y. (2023). Cybersecurity challenges and solutions in the era of digital transformation: A review. IEEE Access, 11, 274-293.
- Torres, R. A. G., & Olipas, C. N. P. (2024). Analyzing Student Academic Performance and Cybersecurity Awareness Levels: Basis for Enhancing Instruction.
- Unar, A. A. (2024). Cybersecurity Risks for Professional Services Firms: Assessing Vulnerabilities, Proposing Innovations, and Safeguarding Client Trust. The Repository at St. Cloud State, https://core.ac.uk/download/615522964.pdf