المجلة الليبية للدراسات الأكاديمية المعاصرة (Libyan Journal of Contemporary Academic Studies)
LJCAS, eISSN: 5970-3005
Volume 3, Issue 2 (Part II), 2025, Pages: 756-777

The Effectiveness of Cybersecurity in Protecting Accounting Information Systems in the Libyan Banking Sector (An Applied Study on Commercial Banks Operating in Zawiya)

Amal Salem Hadoud *
Department of Accounting, Faculty of Economics, University of Zawiya, Zawiya, Libya
*Corresponding author: a.hadoud@zu.edu.ly

مدى فعالية الأمن السيبراني في حماية نظم المعلومات المحاسبية بالقطاع المصرفي الليبي (دراسة تطبيقية على المصارف التجارية الليبية العاملة في مدينة الزاوية)

امال سالم حدود *
قسم المحاسبة، كلية الاقتصاد، جامعة الزاوية، الزاوية، ليبيا

Received: 29-09-2025; **Accepted:** 09-12-2025; **Published:** 20-12-2025

Abstract:
This study aimed to measure the effectiveness of cybersecurity (in its dimensions: technical practices, human resource efficiency, and organizational structure) in protecting accounting information systems in Libyan commercial banks operating in the city of Zawiya. To achieve this, a descriptive-analytical approach was adopted, and a questionnaire was used to collect data. The valid sample size for analysis was (70) respondents. The data were analyzed using descriptive analysis and multiple regression analysis. The results showed a statistically significant positive effect of the overall effectiveness of cybersecurity on the protection of accounting systems, with the model explaining 55% of the variance. However, the core finding revealed that this impact is unbalanced, stemming exclusively from technical and organizational practices (which demonstrated a positive effect), while human efficiency and organizational structure showed no statistically significant impact. The level of human efficiency and training was found to be very low compared to the high level of technical engagement.
The study also recommended that banks immediately invest in human capital through intensive training and talent recruitment to bridge the gap between technical strength and human resource weaknesses, thus ensuring comprehensive accounting protection.

Keywords: Cybersecurity, Accounting Information Systems, Commercial Banks, Technical Practices, Human Resource Efficiency.

الملخص :
هدفت هذه الدراسة إلى قياس مدى فعالية الأمن السيبراني (بأبعاده: الممارسات التقنية، الكفاءة البشرية، والهيكل التنظيمي) في حماية نظم المعلومات المحاسبية بالمصارف التجارية الليبية العاملة في مدينة الزاوية. لتحقيق ذلك، تم اعتماد المنهج الوصفي التحليلي، واستُخدمت استبانة لجمع البيانات، حيث بلغت العينة الصالحة للتحليل (70) مستجيباً. وتم تحليل البيانات باستخدام الإحصاء الوصفي وتحليل الانحدار المتعدد.
أظهرت النتائج وجود تأثير إيجابي ذي دلالة إحصائية لفعالية الأمن السيبراني ككل على حماية النظم المحاسبية، حيث فسر النموذج 55% من التباين. إلا أن النتيجة الجوهرية كشفت أن هذا التأثير غير متوازن؛ فهو ناتج بشكل حصري عن الممارسات التقنية (التي أظهرت تأثيراً قوياً)، بينما لم يظهر بُعدا الكفاءة البشرية والهيكل التنظيمي أي تأثير دال إحصائياً. وجاء مستوى الكفاءة البشرية والتدريب منخفضاً جداً مقارنة بالمستوى المرتفع للممارسات التقنية.
كما أوصت الدراسة بضرورة استثمار المصارف الفوري في رأس المال البشري، عبر التدريب المكثف واستقطاب الكوادر، لسد الفجوة بين القوة التقنية والضعف البشري لضمان حماية محاسبية متكاملة.

الكلمات المفتاحية: الأمن السيبراني، نظم المعلومات المحاسبية، المصارف التجارية، الممارسات التقنية، الكفاءة البشرية.

1. المقدمة

في العصر الرقمي الحالي، أصبحت المصارف تعتمد بشكل متزايد على نظم المعلومات المحاسبية الإلكترونية لجمع وتخزين ومعالجة البيانات المالية والمحاسبية. ومع هذا الاعتماد، تنفتح النظم على مجموعة من المخاطر السيبرانية مثل الاختراق، سرقة البيانات، التلاعب المالي، أو تعطيل الخدمات المحاسبية. تعتبر سلامة هذه النظم جزءًا أساسيًا من موثوقية التقارير المالية وهذه بدوره يؤثر في ثقة العملاء والمستثمرين وسمعة المصارف.

في ليبيا، تواجه المصارف عدة تحديات تقنية وبشرية وتنظيمية، من ضعف البنية التحتية التكنولوجية إلى نقص الأطر التشريعية والتوعية الأمنية. ورغم بعض الجهود مثل سياسة الأمن المعلوماتي لدى مصرف ليبيا المركزي، يُلاحظ أن الأبحاث المنشورة في ليبيا حول تفاعل الأمن السيبراني مع نظم المعلومات المحاسبية ما تزال قليلة ومجزأة. من هذا المنطلق، فإن دراسة واقعية توضح كيف يُطبّق الأمن السيبراني لحماية نظم المعلومات المحاسبية في المصارف، وتحديد التحديات التي تواجه ذلك، ستُسهم في سد فجوة معرفية مهمة، وتقديم توصيات عملية لتعزيز الأمان والمصداقية في البيئة المصرفية الليبية.

2. مشكلة الدراسة

رغم أهمية نظم المعلومات المحاسبية في المصارف ودورها في الأداء المالي والشفافية، فإن وجود التهديدات السيبرانية يشكل خطرًا على سرية وسلامة وتوافر البيانات المالية، في ليبيا لا توجد دراسات كافية تبين مدى تطبيق المصارف لآليات الأمن السيبراني لحماية نظم المعلومات المحاسبية، وأنواع التهديدات التي تتعرض لها هذه النظم فعلًا، والتأثيرات المترتبة على جودة البيانات الموثوقة، الثقة، والسمعة المصرفية، والعوائق التقنية والتنظيمية والبشرية التي تعيق تطبيق الأمان السيبراني. بالتالي، السؤال الرئيسي للدراسة: **ما مدى فعالية الأمن السيبراني في حماية نظم المعلومات المحاسبية في المصارف التجارية الليبية؟**

أسئلة فرعية للدراسة:

1. ما هو مستوى تطبيق الممارسات التقنية للأمن السيبراني (كالتحديث والمراقبة) في المصارف التجارية الليبية؟
2. إلى أي درجة تتوفر الكفاءة البشرية والتنظيمية (من حيث التدريب والسياسات) اللازمة لدعم الأمن السيبراني في هذه المصارف؟
3. ما هو واقع الهيكل التنظيمي المتخصص (كوجود فرق أمنية والتكامل مع المحاسبة) في هذه المصارف؟
4. ما هو مستوى حماية نظم المعلومات المحاسبية (من حيث جودة البيانات وموثوقيتها) في المصارف قيد الدراسة؟
5. ما هو مدى التأثير الإيجابي لفعالية الأمن السيبراني (بأبعاده المختلفة) على حماية نظم المعلومات المحاسبية؟

3. أهمية الدراسة

1-أهمية أكاديمية: الإضافة إلى الأدبيات المحلية والعربية في مواضيع الأمن السيبراني والمحاسبة؛ دراسة تربط بين النظم المحاسبية وجودتها من جهة وبين الأمان السيبراني من جهة أخرى، وهو تداخل يحتاج إلى مزيد من البحث.

2-أهمية مهنية للمصارف: توضيح النقاط الضعيفة وإعطاء توصيات لتعزيز الأمان مما يمكن أن يقلل من المخاطر المالية والتشغيلية.

3-أهمية لعملاء المصارف والمجتمع: تحسين الثقة في المصارف حيث أن الأمان السيبراني يُعتبر جزءًا من سمعة المصرف والمصداقية.

4-أهمية تنظيمية تشريعية: دعم صناع القرار في الجهات التنظيمية والمصارف المركزية لوضع أو تحسين السياسات التي تفرض معايير أمنية لنظم المعلومات المحاسبية.

4. أهداف الدراسة

بناءً على مشكلة الدراسة وتساؤلاتها، تسعى هذه الدراسة إلى تحقيق مجموعة من الأهداف المحددة التالية:

1. تقييم مستوى تطبيق الممارسات التقنية والكفاءة البشرية والهيكل التنظيمي للأمن السيبراني في المصارف التجارية الليبية.
2. قياس مستوى حماية نظم المعلومات المحاسبية في العينة محل الدراسة.
3. تحليل مدى التأثير الإيجابي لكل بعد من أبعاد الأمن السيبراني على حماية نظم المعلومات المحاسبية.

4. تقديم توصيات ومقترحات عملية لتعزيز فعالية الأمن السيبراني لتحسين حماية النظم المحاسبية في المصارف الليبية.

5. فرضيات الدراسة

الفرضية الرئيسية:

يوجد تأثير ذو دلالة إحصائية إيجابي لفعالية الأمن السيبراني على حماية نظم المعلومات المحاسبية في المصارف التجارية الليبية عند مستوى المعنوية 5%.

الفرضيات الفرعية:

1. يوجد تأثير ذو دلالة إحصائية إيجابي لمستوى تطبيق الممارسات التقنية للأمن السيبراني على مستوى حماية نظم المعلومات المحاسبية عند مستوى المعنوية 5%.
2. يوجد تأثير ذو دلالة إحصائية إيجابي لمستوى الكفاءة البشرية والتنظيمية على مستوى حماية نظم المعلومات المحاسبية عند مستوى المعنوية 5%.
3. يوجد تأثير ذو دلالة إحصائية إيجابي لوجود هيكل تنظيمي متخصص على مستوى حماية نظم المعلومات المحاسبية عند مستوى المعنوية 5%.

6- المتغيرات الدراسية:

المتغير المستقل :- الأمن السيبراني((بأبعاده: الممارسات التقنية، الكفاءة البشرية، والهيكل التنظيمي)

المتغير التابع:- حماية نظم المعلومات المحاسبية.

7- حدود الدراسة:

لضمان دقة النتائج، تحددت معالم هذه الدراسة بالحدود التالية:

الحدود الموضوعية: اقتصرت الدراسة على قياس أثر فعالية الأمن السيبراني بأبعادها الثلاثة (الممارسات التقنية، الكفاءة البشرية والتنظيمية، الهيكل التنظيمي المتخصص) على حماية نظم المعلومات المحاسبية.

الحدود المكانية: تم تطبيق هذه الدراسة على المصارف التجارية العاملة في مدينة الزاوية، ليبيا.

الحدود البشرية: شملت عينة البحث العاملين في الوظائف ذات الصلة المباشرة بموضوع البحث (كالإدارة المالية، المحاسبة، المراجعة الداخلية، والإدارة العليا).

الحدود الزمنية: تم جمع البيانات الميدانية اللازمة للبحث خلال الربع الأخير من العام 2025.

الدراسات السابقة :

أولا: الدراسات العربية

1- **دراسة زعابطة عبد اللطيف (2022)بعنوان(اثر مخاطر تكنولوجيا المعلومات على نظم المعلومات المحاسبي** دراسة حالة- الجزائر هدفت الدراسة الى معرفة اهم انواع المخاطر التي تواجه المؤسسات الاقتصادية عند استخدامها لتكنولوجيا المعلومات في نظام المعلومات المحاسبي وما الحلول الممكنة لمواجهة هذه المخاطر ثم تم التطرق الى مختلف الاجراءات والممارسات التي من شانها الحد من ذلك الاثر سعيا نحو الاستخدام الامثل لتكنولوجيا المعلومات في نظام المعلومات المحاسبي وخلصت الدراسة الى ان شركة الاتصالات الجزائر تولي اهتماما واضحا بخصوص الحد من مخاطر التكنولوجيا المعلومات وهذا عبر الوسائل البشرية والتقنية وكذا الضوابط الرقابية والامنية المرتبطة بنظم المعلومات الا انه لايزال هنالك بعض الثغرات التي ينبغي تداركها .

2- **دراسة عبد المهدي،(2020) اثر تطبيق سياسات الامن السيبراني على جودة نظم المعلومات المحاسبية** هدفت الدراسة الى تعقب اثر تطبيق سياسات الامن السيبراني على جودة المعلومات المحاسبية في انشطة المصارف التجارية في الاردن وتوصلت الدراسة الى وجود علاقة بين ادارة المخاطر السيبرانية وتطبيق مبادئ امن المعلومات على جودة نظم المعلومات المحاسبية كما توصلت الى ان الحفاظ على خصوصية بيانات العملاء لها تأثير ملموس على جودة نظم المعلومات المحاسبية .واوصت الدراسة بزيادة الاهتمام

بمبادئ حوكمة امن المعلومات الالكترونية وضرورة ان تهتم المصارف بالإفصاح السنوي عن تقارير الامن السيبراني .

3- **دراسة يوسف ,(2024) بعنوان تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية** هدفت الدراسة الى تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية وتوصلت الدراسة الى ان المؤسسات الليبية تواجه تهديدات سيبرانية متزايدة ومتنوعة وتشمل هذه التهديدات الاختراقات الهجمات الالكترونية سرقة البيانات التجسس الصناعي وتعطيل الخدمات المصرفية عبر الانترنت هذه التهديدات تسبب تأثيرا سلبيا على نظم المعلومات المحاسبية وتمثل خطرا على السرية والموثوقية والتوافرية وتوصل البحث الى ان هناك عدة نقاط ضعف في نظم المعلومات المحاسبية في المؤسسات المالية تشمل هذه النقاط الضعف في رصد وكشف هجمات السيبرانية نقص في التدريب والوعي الامني للموظفين

4- **دراسة التائب،السائح (2025) بعنوان أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية: دراسة تطبيقية** على المصارف التجارية العاملة في مدينة سرت 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.

ثانيا: الدراسات الاجنبية :

1-Ai-powered (Dasgupta,et aI (2023) cybersecurity:Identifying Threats in digtal Banking
هدف هذا البحث إلى تسليط الضوء على فوائد استخدام الامن السيبراني المدعوم بالذكاء الاصطناعي لدعم كفاءة الاعمال وزيادة الوعي حول الحاجة الى التغلب على الخوف من تجربة التقنيات الجديدة واظهار كيفية الاستفادة مثل ادارة المخاطر في مالطا على تجارب الشركات التي نفذت انظمة الامن السيبراني التي تعمل بالذكاء الاصطناعي في مالطا ونتج البحث في توفر رؤى للشركات التي تتطلع الى تنفيذ انظمة الامن السيبراني التي تعمل بالذكاء الاصطناعي ادى ظهور الذكاء الاصطناعي الى تغييرات كبيرة في كيفية عمل الشركات وخاصة الامن السيبراني ادى الاعتماد المتزايد على التكنولوجيا في العمليات التجارية وتخزين البيانات الى جعل الشركات عرضة للهجمات الالكترونية ويوصي الباحث الى ضرورة دمج انظمة الامن السيبراني التي تعمل بالذكاء الاصطناعي لحماية عملياتها ومع ذلك على الرغم من الفوائد العديدة لاستخدام الذكاء الاصطناعي في الامن السيبراني لاتزال هناك مخاوف بشان امان التكنولوجيا وفعاليتها.

2-Daoud ,serag:2022 (Aproposed framework for studying the impact of cybersecurity on accounting information to increase trust in the financial reports in the context of industry :an event impact and response approach
هدف هذا البحث إلى التعرف على اطار مقترح لدراسة تأثير الامن السيبراني على المعلومات المحاسبية لزيادة الثقة في التقارير المالية في سياق الصناعة وتشمل تقنيات الصناعة البيانات الضخمة وانترنت الاشياء وتكامل النظام والحوسبة السحابية وزيادة الاتمتة والواقع الافتراضي وتوصل البحث الى أنه يمكن للشركات

المصنعة ان تظل امنه ومزدهرة من خلال حماية جميع الاجهزة والبرامج والمعلومات من التهديدات الداخلية والخارجية هذه الانتهاكات لها اثار على المؤسسات الاعمال لأنها قد تؤدي الى انخفاض الاداء والقيمة السوقية ويوصى البحث بضرورة توفير المعلومات والوقت الذي يقضيه الموظف في ضمان الامتثال للوائح الخصوصية والسرية المناسبة

3-Al-Okaily ,et al (2022)the effect of digital accounting systems on the decision –making quality in the banking industry sector :a mediated-moderated

يهدف البحث الى تقييم تأثير عوامل النجاح انظمة المحاسبة الرقمية على الارتقاء بجودة صنع القرار في البنوك الاردنية وكشفت النتائج ان جودة البيانات والمعلومات كان لها تأثير كبير على جودة اتخاذ القرار بشكل عام مع انظمة المحاسبة الرقمية في حين ان جودة النظام لم يكن لها تأثير كبير عليها ويوصي بضرورة نشر ثقافة صنع القرار التحليلي الى تعديل العلاقة بين جودة المعلومات وجودة صنع القرار.

الاطار النظري للدراسة:-

الامن السيبراني لحماية الانظمة المحاسبية:

1- **مفهوم الامن السيبراني:** يشير مصطلح الامن السيبراني او ما يطلق عليه بأمن نظم المعلومات الى انه عبارة عن مجموعة من الاجراءات والسياسات والادوات والمفاهيم الامنية والمبادئ التوجيهية التي تستخدم لتحديد وتقييم وتقليل المخاطر التي تهدد البيئة الالكترونية، والتي تتضمن معالجة المعلومات وحماية الموارد الرقمية وتنظيم اصول المستخدمين وتتضمن هذه الاجراءات ايضا التدريب على افضل الممارسات وضمان الاستخدام الامن للتقنية المختلفة التي تساعد على حماية الانظمة والشبكات الالكترونية (وفاء ,2022:ص222)

2- **وعرفه martti lehto** على انه (عبارة عن مجموعه من الاجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة.(lehto,martti,2015:25)

اهمية الامن السيبراني :تتمثل اهميته في:(وفاء,224:2022)

1-يهدف الحفاظ على البيانات الى ضمان سلامتها وتكاملها ومنع التلاعب بها.
2-تحقيق وفرة البيانات وجاهزيتها عند الحاجه .
3-حماية الاجهزة والشبكات والحفاظ عليها من الاختراقات والتجاوزات .
4-استكشاف نقاط الضعف والثغرات في الانظمة ومعالجتها.
5-توفير بيئة عمل امنة جدا خلال العمل عبر الشبكة العنكبوتية
6-حماية الشبكات من الولوج غير المصرح به.
7-تحسين مستوى حماية المعلومات وضمان استمرارية الاعمال.
8-في حالة حدوث خرق للنظام الامني السيبراني يتم استيراد البيانات المسربة في اسرع وقت ممكن.

عناصر الامن السيبراني :

وهي ثلاثة عناصر اساسية اتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار اليها بثلاثي CIAوهي: (بن علية ,304:2022)

- السرية :هي عبارة على حماية خصوصية المعلومات المتداولة عبر الانترنت وضمان عدم كشفها لاي طرف غير مخول بها , مما يعزز السرية والامان لهذه المعلومات .
- السلامة هي عملية عدم التلاعب بالمعلومات، وعدم حذفها او تعديلها خلال عملية النقل او التخزين او تدخل او تعديل غير مصرح به .
- التوافر :يقصد بها استمرار توفير المعلومة للشخص او الجهة التي يسمح لها المستخدم بالاطلاع عليها عند الحاجة وبشكل مستمر ومنتظم وذلك لضمان توافر المعلومات للأطراف المعنية في الوقت المناسب وبشكل دقيق، مما يساعد على اتخاذ القرارات الصحيحة والمناسبة.

اجراءات ووسائل الامن السيبراني في ظل انظمة المعلومات المحاسبية: (امجد,34:2011)

1- **ادارة كلمة السر**: تستخدم كوسيلة للتحقق من هوية المستخدمين وتعريفه، وذلك بهدف السماح له بالوصول الى النظام وتحديد البرامج والملفات التي يسمح له بالوصول اليها والقيام بالعمل من خلالها .

2- **تشفير البيانات** :تقنية التشفير تعد واحدة من اهم تقنيات الحماية التي اهتماما كبيرا في مجال سرية وموثوقية وسلامة البيانات المتبادلة تعتمد هذه التقنية على تعديل محتوى الرسالة باستخدام مفتاح التشفير قبل ارسالها ويكون بامكان المستقبل استعادة المحتوى الاصلي للرسالة باستخدام مفتاح فك الشفرة .

3- **برمجيات المضادة للاعتداءات الالكترونية**: تعتبر برامج الحماية اكثر البرامج شهرة وانتشارا بين مستخدمي الحواسيب والشبكات حيث يقوم بالكشف عن البرامج الخبيثة الموجودة في ذاكرة الحواسيب وتحطيمها منع الهجمات الاخرى .ويمكن ان تكون هذه البرامج مخصصة لتحديد تهديد واحد, مثل برنامج (SPYBOT SEARCH AND DESTROY) الذي يهدف الى القضاء على برامج التجسس او برنامج (COFFRE FORT)الذي يساعد على انشاء مساحة امنه للبيانات الحساسة على الحاسوب .كما يمكن ان تكون هذه البرامج متكاملة ,حيث تقوم بمجموعة من المهام التي تهدف الى حماية الحاسوب والمعلومات المخزنة به من التهديدات المختلفة مثل برنامج KASPERSKY INTERNET SECURITY))الروسي برنامج(SECURE ANYWHERE WEBROOT)(زعابطة,140:2022)

4- **النسخ الاحتياطي** :تلجا ادارة النظم المعلومات لعمل الملفات الاحتياطية لحفظ الملفات حيث يتم اعداد نسخ احتياطية من البيانات والبرامج لمواجهة احتمال فقدان او تخريب البيانات او البرامج نتيجة اخطاء التشغيل او نتيجة اختراق نظام المعلومات (زين عبد المالك,83:2024)

5- **الجدران النارية**:-هي برامج خاصة تعمل على حماية الشبكات التي تكون مرتبطة بشبكة الانترنت ,حيث توضع مع خادم الشبكة ,وبالتالي فهي تؤمن الحماية لكل الحاسبات المرتبطة بالشبكة وليس الحاسب واحد فقط, تعمل بمبدأ ترشيح البيانات وعدم السماح للأشخاص غير المخول لهم بالدخول الى الشبكة ويمكن لها حتى التحكم في مستخدمي هذه الشبكة بمنعهم من الدخول الى بعض الملفات دون غيرها .

6- **فحص الاختراقات**: يتم استئجار خدمات شركات متخصصة في الامن السيبراني لتمثيل دور المهاجمين والاختراق الى النظام بهدف تحديد نقاط الضعف التي يمكن اختراقها في نظام الامن ,ثم يتم اخطار ادارة الشركة بتلك النقاط لإصلاحها .وهذا يساعد الشركة في تقييم قدراتها على منع وكشف الوصول غير المصرح به الى النظام ,وتحسين دفاعات الشبكة .

7- **تقنيات الاشعار بالاستلام الرسالة (اختبار الصدى):**هي عبارة عن تقنيات برمجية تستخدم للتحقق من استلام البيانات بشكل كامل من قبل الوحدة المتلقة ,وذلك من خلال عملية المصادقة التلقائية .

8- **الاجراءات التنظيمية** :وهي تعني ان يتم تنظيم ومراقبة الوصول الى البرامج والبيانات المخزنة في نظم المعلومات بعناية (السيطرة على الوصول)ويم ذلك من خلال تحديد سياسات واجراءات الامان وتطبيقها ,وتحديد مستويات الصلاحية للمستخدمين والمسؤولين في نظام ,وتطبيق تقنيات الحماية المناسبة للموارد المختلفة .ويتم ذلك عن طريق الهيكل التنظيمي لدائرة نظم المعلومات والفصل بين الوظائف المختلفة المسؤولة عن تطبيق سياسات الامان والسيطرة على الوصول .

9- **السياسات والاجراءات** :هي عبارة على تطوير تنفيذ سياسات واجراءات للتعامل مع اخطاء النظام في مجال البرامج والبيانات وانظمة التشغيل وتوضيحها للعاملين بحيث يمكن معالجتها من خلال انظمة الامان لاستعادة النظام واتاحته للمستخدمين .

متطلبات تحقيق الامن السيبراني لدى المؤسسات :

تعد مسالة حماية امن نظم المعلومات المحاسبية من اهم القضايا التي يجب ان تولي المؤسسات اهتماما كبيرا بها

وتطبيق خطط حماية شاملة تتماشى مع امكانياتها التنظيمية والمادية يجب ان تكون هذه الحماية قوية وفعالة ولذلك يتطلب الامر توفر عدة متطلبات لحماية امن نظم المعلومات المحاسبية ,وتشمل :(الشريف ,85,2006)

1- ينبغي وضع سياسة حماية شاملة لأمن نظم المعلومات المحاسبية تتناسب مع طبيعة عمل وتطبيقات المؤسسة .
2- يتعين على الادارة العليا في المؤسسات دعم جهود نظم المعلومات المحاسبية والاهتمام بها لضمان سلامتها وعدم تعرضها للتهديدات الامنية .
3- يجب تعيين اشخاص مختصين مسؤولين عن امن نظم المعلومات في المؤسسات .
4- يجب تحديد متطلبات الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة .

علاقة الامن السيبراني مع انظمة المعلومات المحاسبية :

يرتبط الامن السيبراني ارتباطا وطيدا بأنظمة المعلومات ,فمهمة حماية الانظمة والبيانات المخزنة والمعلومات الحساسة في الفضاء السيبراني من اي شكل من اشكال التهديدات والجرائم السيبرانية المختلفة فأنظمة المعلومات المحاسبية تشكل جزء رئيسيا في الحياة اليومية للمؤسسات والهيئات الحكومية وهي مستخدمة جل الاعمال التجارية والمالية الحقيقية على الواقع او الاعمال الافتراضية كتجارة الالكترونية الادارة الالكترونية والخدمات المصرفية وغيرها لذلك فان اي اختراق او تجاوز لأمن تظم المعلومات سوف يسبب بخسارة كبيرة مما يعطل الانشطة ويفقد البيانات ويخرب البنية التحتية الحيوية الحساسة .

الذكاء الاصطناعي وعلاقته مع انظمة المعلومات المحاسبية :

يتزايد استخدام الذكاء الاصطناعي (AI) في الامن السيبراني لتحسين سرعة ودقة اكتشاف التهديدات والاستجابة لها. بحيث ان كبرى الشركات والمؤسسات في العالم اتجهت للبحث في دمج وادخال الذكاء الاصطناعي والعلاقة التي تجمعه معا لأمن السيبراني :

يعرف الذكاء الاصطناعي على انه :علم يبحث في مفهوم الذكاء البشري وخصائصه وتحديد جوانبه ومن ثم محاكاة سلوكياته كما تشمل مجالات متنوعة حيث ان الجانب المشترك بين مجالات الذكاء الاصطناعي هو القدرة على اختراع الآلات حاسوبية تحاكي خصائص الذكاء البشري .(النعانعة:685,2023)

ويعرف انه عملية حاسوبية تستند الى الابداع والاستيعاب لكافة الامور والسلوكيات ,وتهدف الى معالجة المواقف والمشكلات وايجاد حلول ذكية وفعالة باستخدام تقنيات الحوسبة والتعلم الالي.(جهني:39,2023)

نظام المعلومات المحاسبي :

يعرف النظام المحاسبي انه مجموعة من المكونات التي تشكل وسائل الية ووثائق ومستندات وسجلات وتقارير واجراءات واشخاص ومعدات وادوات تكنولوجيا المعلومات والاتصالات والتي تتكامل وتتفاعل مع بعضها البعض لتحقيق هدف معالجة البيانات المحاسبية يتم ذلك من خلال تسجيل وتجميع وتبويب وتلخيص البيانات المحاسبية ثم تحويلها الى معلومات محاسبية يتم تمثيلها في شكل قوائم مالية .(زعابطة :50,2022)

كما يعرف على انه عبارة عن مجموعه من المعدات والبرمجيات القادرة على تحويل المدخلات الى المخرجات اي تحويل البيانات المحاسبية الى معلومات محاسبية من خلال تلخيص واسترجاع واختبار وتلبية محتاجي المعلومات .(السعيد,خالد,9:2023)

اهداف نظام المعلومات المحاسبي :

1- تزويد بالمعلومات اللازمة لتوجيه الموارد البشرية والمادية بشكل فعال والمساهمة في زيادة كفاءتها في مجالات متعددة.
2- تزويد بالمعلومات التي تساعد الادارة في اداء دورها كوكيل لملاك الموارد المتاحة وتقديم التقارير اللازمة للأطراف المعنية لتمكينهم من اتخاذ القرارات المناسبة بشان الاستمرار او عدم الاستمرار في النشاط بشكل مستمر
3- يهدف النظام الى تحقيق الحماية الكافية لأموال المنشاة ومراقبتها وذلك من خلال اتباع الاجراءات والتعليمات المتعلقة بتسجيل ومعالجة بيانات وفقا للقواعد المحاسبية.

اسباب ظهور المخاطر التي تواجه نظام المعلومات المحاسبية :

المخاطر : هي التأثير وعدم اليقين او عدم التأكد على الاهداف وهذا التأثير هو الانحراف ايجابي او سلبي عن المتوقع بمعنى اخر هو حادث احتمالي غير مؤكد الوقوع ينتج عن وقوعه نتائج غير مرغوب فيها.(السعيد,خالد,11:2023)

اما مفهوم مخاطر انظمة المعلومات المحاسبية :هي عبارة عن مجموعة متنوعة من التهديدات والمخاطر ابتداء من المدخلات الخاطئة للمعاملات ووصولا الى اشخاص الذين يمتلكون امكانيات الوصول الى شريط النسخ الاحتياطي الذي يحتوي على جميع البيانات المالية والهامة للمنشاة.

هناك اسباب متعلقة بالمخاطر تتلخص هذه الاسباب في العناصر التالية :(الشريف,84:2006)

1- عدم كفاية وفعالية الاساليب والادوات الرقابية المطبقة من ادارة الشركة.
2- ضعف انظمة الرقابة الداخلية لدى المنشاة وعدم فعاليتها.
3- تشارك بعض الموظفين في استخدام نفس كلمة السر من اجل الدخول الى النظام والعبث بمحتوياته.
4- عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظام المعلومات المحاسبية للمنشاة.
5- عدم توفر الحماية اللازمة لمخاطر الفيروسات الحواسيب.
6- عدم وجود الوعي الكافي لدى موظفين بضرورة فحص اي برامج او روابط خارجية او اقراص ممغنطة جديدة قبل ادخالها الى جهاز الحاسوب.

الاطار العملي للدراسة:

منهج الدراسة: لتحقيق أهداف البحث والإجابة على تساؤلاته، اعتمدت الباحثة على المنهج الوصفي التحليلي(Descriptive-Analytical Approach) ، ويُعد هذا المنهج هو الأنسب لطبيعة هذه الدراسة حيث تم استخدام الجانب الوصفي في توصيف خصائص عينة الدراسة (من خلال الإحصاء الوصفي)، وفي قياس مستوى متغيرات الدراسة (الممارسات التقنية، الكفاءة البشرية، الهيكل التنظيمي، وحماية النظم) وتحديد درجة توافرها في المصارف محل الدراسة.

بينما تم استخدام الجانب التحليلي في قياس واختبار الفرضيات، وتحديداً تحليل طبيعة العلاقة السببية (الأثر) بين أبعاد فعالية الأمن السيبراني (كمتغيرات مستقلة) وحماية نظم المعلومات المحاسبية (كمتغير تابع)، وذلك باستخدام نموذج الانحدار الخطي المتعدد.

أداة الدراسة: تم جمع المعلومات والبيانات وتحليلها، من خلال استمارة استبيان ورقية لجمع البيانات من العينة المستهدفة، والتي تم تصميمها وبناؤها بعد مراجعة الأدبيات النظرية والدراسات السابقة ذات الصلة.

قُسمت الاستبانة إلى ثلاثة أجزاء:

1. **الجزء الأول :**خُصص للبيانات الأساسية والديموغرافية لأفراد العينة (العمر، المؤهل العلمي، الخبرة، المسمى الوظيفي، التخصص).
2. **الجزء الثاني :**خُصص لقياس المتغير المستقل (فعالية الأمن السيبراني) بأبعاده الثلاثة:

المحور الأول: الممارسات التقنية (4 فقرات).
المحور الثاني: الكفاءة البشرية والتنظيمية (5 فقرات).
المحور الثالث: الهيكل التنظيمي المتخصص (2 فقرة).

3. **الجزء الثالث :**خُصص لقياس المتغير التابع (حماية نظم المعلومات المحاسبية) (4 فقرات).

وقد تم استخدام **مقياس ليكرت الخماسي (Five-point Likert Scale)** لقياس استجابات أفراد العينة، (حيث 1 = غير موافق بشدة، و5 = موافق بشدة). وتم تحليل البيانات المجمعة باستخدام برنامج SPSS. V27لاختبار فرضيات الدراسة والوصول إلى النتائج والاستنتاجات.

مجتمع وعينة الدراسة:

تألف مجتمع الدراسة من جميع العاملين في الوظائف ذات الصلة في المصارف التجارية العاملة بمدينة الزاوية. ونظراً لطبيعة المجتمع، تم اللجوء إلى أسلوب العينات لجمع البيانات.

(مصرف الجمهورية (الميدان و الجامعة), مصرف التجاري(الميدان وصرمان والمصفاة) ,مصرف الصحاري ,مصرف الوحدة)

حيث تم استخدام العينة العشوائية البسيطة **(Simple Random Sample)** لضمان حيادية الاختيار وإمكانية تعميم النتائج على مجتمع الدراسة. تم توزيع (80) استبانة بشكل عشوائي، استُرجعت منها (73) استبانة. وبعد المراجعة والفحص، تم استبعاد (3) استبانات لعدم اكتمالها، ليصبح حجم العينة الصالحة للتحليل (70) مستجيباً.

وبهذا، تبلغ نسبة الاسترداد الصالحة للتحليل (87.5%) من إجمالي الاستبانات الموزعة، وهي نسبة ممتازة ومناسبة لأغراض التحليل الإحصائي وتمثيل مجتمع الدراسة.

أساليب التحليل الإحصائي

لتحليل البيانات التي تم جمعها واختبار فرضيات البحث بعد إدخال البيانات في برنامج SPSS v.27 والتحقق من تجانسها وتحرير القيم المفقودة (أقل من 2%)، تم استخدام الأساليب التالية:

1. **تحليل الموثوقية :(Reliability Analysis)** تم استخدام معامل ألفا كرونباخ (Cronbach's Alpha)لقياس درجة الاتساق الداخلي والموثوقية لكل محور من محاور الدراسة.
2. **الإحصاء الوصفي :(Descriptive Statistics)** تم استخدام التكرارات والنسب المئوية لتوصيف خصائص العينة. كما تم استخدام المتوسطات الحسابية والانحرافات المعيارية للإجابة على أسئلة البحث الوصفية وتحديد مستوى تطبيق كل متغير.
3. **اختبار العينة الواحدة :(One-Sample T-Test)** استُخدم هذا الاختبار لمقارنة المتوسط الحسابي لإجابات العينة على كل محور بـالقيمة المفترضة للمقياس (3)، وذلك لتحديد ما إذا كان المستوى (مرتفعاً أو منخفضاً) بشكل ذي دلالة إحصائية.
4. **معامل ارتباط بيرسون (Pearson)** لقياس العلاقة بين متغيرات الامن السيبراني وحماية نظام المعلومات المحاسبية.
5. **تحليل الانحدار الخطي المتعدد :(Multiple Linear Regression)** استُخدم هذا التحليل كأداة إحصائية رئيسية للإجابة على السؤال البحثي رقم (5) واختبار صحة الفرضيات، وذلك لقياس أثر الأبعاد المستقلة الثلاثة مجتمعة ومنفردة على المتغير التابع.

- **صدق وثبات الأداة (Validity and Reliability)**

لضمان صلاحية الأداة لقياس ما وُضعت لقياسه، تم اتخاذ الإجراءات التالية:

أولاً: الصدق الظاهري (Face Validity) تم عرض الأداة بصورتها الأولية (المكونة من 17 فقرة) على مجموعة من المحكمين الأكاديميين والخبراء في مجال المحاسبة وأمن المعلومات وتحليل البيانات، وبناءً على ملاحظاتهم تم تعديل صياغة بعض الفقرات.

ثانياً: تحليل الموثوقية وتنقية المقياس (Reliability Analysis and Scale Purification) بعد التأكد من الصدق الظاهري، تم إجراء تحليل الموثوقية (ألفا كرونباخ) بهدف قياس الاتساق الداخلي لفقرات كل محور. وهو اختبار إحصائي يحدد فيما إذا كانت أسئلة الاستبانة صحيحة على أثر أجوبة مفردات العينة، حيث كلما كانت قيم معامل كرونباخ ألفا كبيرة أكبر من (0.60) فيدل على توفر درجة عالية من الثبات الداخلي في الإجابات مما يمكننا من الاعتماد على هذه الإجابات في تحقيق أهداف الدراسة وتحليل نتائجها. (البياتي: 2005، 49).

ولضمان الحصول على أعلى درجة ثبات ممكنة، تم فحص معاملات الارتباط بين كل فقرة والمحور الذي تنتمي إليه (Item-Total Correlation) وتأثير حذف الفقرة على معامل ألفا.

وبناءً على هذا التحليل، تم إجراء التنقيحات التالية:

1. **المحور الثاني (الكفاءة البشرية والتنظيمية) :**كان هذا المحور يتكون في صورته الأولية من (6) فقرات. أظهر التحليل الإحصائي أن إحدى الفقرات [يتمتع المصرف بالقدرة على الاستجابة بفعالية للحوادث السيبرانية] كانت ذات معامل ارتباط ضعيف، وأن حذفها سيؤدي إلى رفع قيمة معامل الثبات الكلي للمحور. وعليه، تم استبعاد تلك الفقرة ليصبح المحور في صورته النهائية مكوناً من **(5)فقرات**، وبمعامل ثبات (ألفا كرونباخ) بلغ **(0.653)**، وهي قيمة مقبولة إحصائياً.

2. **المحور الثالث (الهيكل التنظيمي المتخصص) :**كان المحور يتكون مبدئياً من (3) فقرات. وتبين أن حذف فقرة واحدة منها [توجد قنوات اتصال رسمية وسريعة للإبلاغ عن الحوادث الأمنية بين قسم المحاسبة والامن السيبراني] يعزز الاتساق الداخلي للمحور بشكل ملحوظ. وعليه، تم اعتماد المحور في صورته النهائية بـ **(2)فقرة**، وبمعامل ثبات ممتاز بلغ **(0.808)**

أما بقية محاور الدراسة، فقد أظهرت معاملات ثبات مرتفعة وممتازة كما يوضح الجدول رقم(1) ، وبذلك أصبحت الأداة في صورتها النهائية مكونة من **(15)** فقرة تتمتع بالثبات والموثوقية اللازمة لأغراض التحليل الإحصائي.

وبلغ معامل الثبات الكلي لجميع فقرات الاستبيان (15 فقرة) مجتمعة، 0.759 وهي قيمة مقبولة إحصائياً وتفي بأغراض البحث العلمي .بصورة عامة يتضح أن أداة الدراسة (الاستبانة) تتمتع بمعاملات ثبات (موثوقية) ومعاملات صدق (صلاحية) مرتفعة ومقبولة إحصائياً، مما يجعل البيانات التي تم جمعها صالحة للاعتماد عليها في التحليلات الإحصائية اللاحقة واختبار فرضيات الدراسة. والجدول التالي يوضح قيم هذه المعاملات.

جدول رقم (1): معاملات ثبات وصدق محاور الدراسة (ألفا كرونباخ)

اسم المحور	عدد العبارات (النهائي)	معامل ألفا كرونباخ	معامل الصدق (الجذر التربيعي لألفا)
الممارسات التقنية للأمن السيبراني	**4**	**0.895**	**0.946**
الكفاءة البشرية والتنظيمية	**5**	**0.653**	**0.808**
الهيكل التنظيمي المتخصص	**2**	**0.808**	**0.899**
حماية نظم المعلومات المحاسبية	**4**	**0.682**	**0.826**
المقياس الكلي	**15**	**0.759**	**0.871**

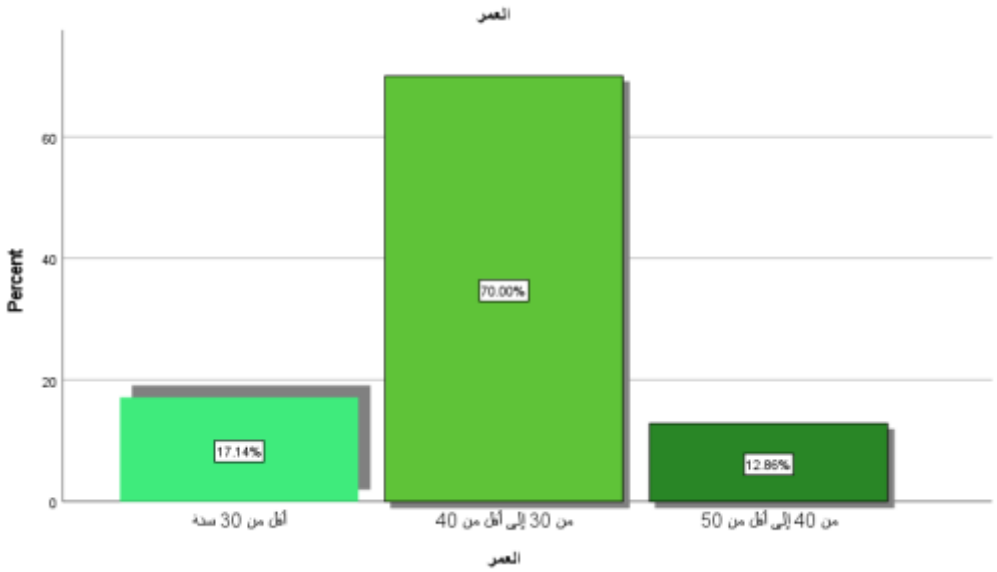
المصدر : من إعداد الباحثة استنادا على مخرجات برنامج SPSS

عرض وتحليل البيانات

أولا : التحليل الوصفي لعينة الدراسة

تحليل خصائص أفراد عينة الدراسة:

1 الفئة العمرية:

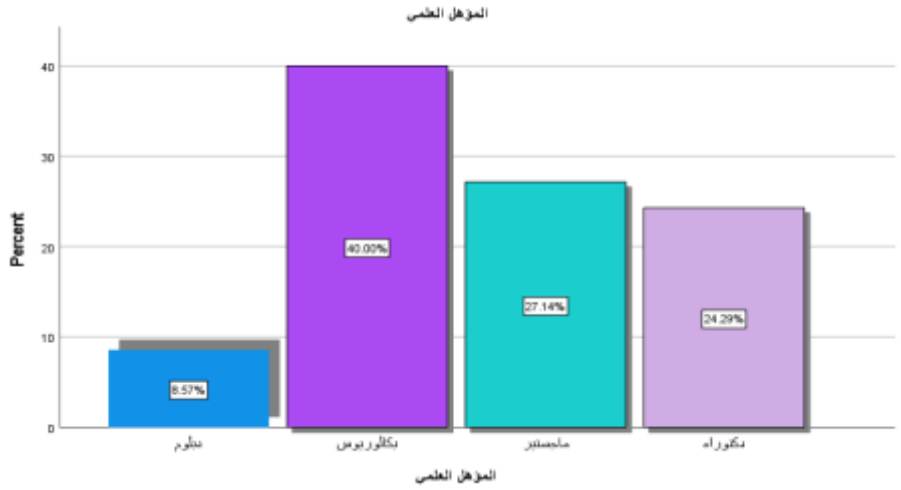


الشكل رقم (1) يمثل التوزيع النسبي لمتغير المؤهل العلمي

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

من خلال الشكل رقم (1) نلاحظ أن 70% من العينة تتراوح أعمارهم بين 30 سنة إلى أقل من 40 سنة، يليهم 17.1%أعمارهم أقل من 30 سنة، والباقي 12.9% أعمارهم بين 40 سنة إلى أقل من 50 سنة، هذا المؤشر إيجابي جداً، ويدل على أن الإجابات جاءت من فئة الموظفين الذين يمثلون عصب العمل في المصارف، فهم ليسوا حديثي التخرج (الأقل من 30) وليسوا في الفئات العمرية المتقدمة، بل هم في قمة عطائهم المهني، مما يضفي مصداقية وفهماً عميقاً على إجاباتهم.

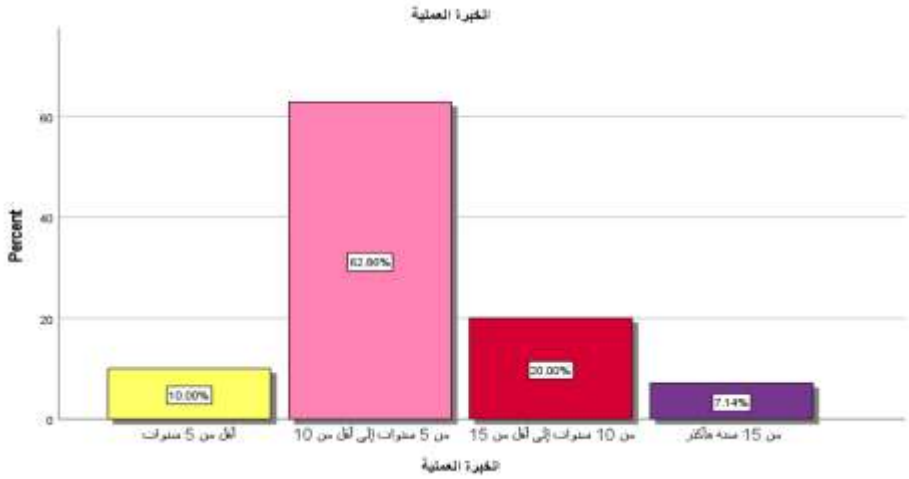
2 المؤهل العلمي:



الشكل رقم (2) يمثل التوزيع النسبي لمتغير المؤهل العلمي
المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

من خلال الشكل رقم (2) تشير النتائج إلى تنوع الخلفيات التعليمية لأفراد العينة. حيث شكلت الفئة الأكبر الحاصلون على درجة البكالوريوس بنسبة 40%، تليها فئة الحاصلين على الماجستير بنسبة 27.14%، ثم الدكتوراه بنسبة 24.29% والباقي متحصلون على مؤهل دبلوم بنسبة 8.57%. ويدل هذا التوزيع على أن غالبية القوى العاملة ضمن العينة تتمتع بمستوى تعليمي جامعي أو أكثر. مما يعكس أن المستجيبين لديهم نضج أكاديمي وعلمي كافٍ لفهم الأبعاد الدقيقة لمتغيرات البحث (كالأمن السيبراني والنظم المحاسبية)، مما يعزز الثقة في دقة البيانات المجمعة.

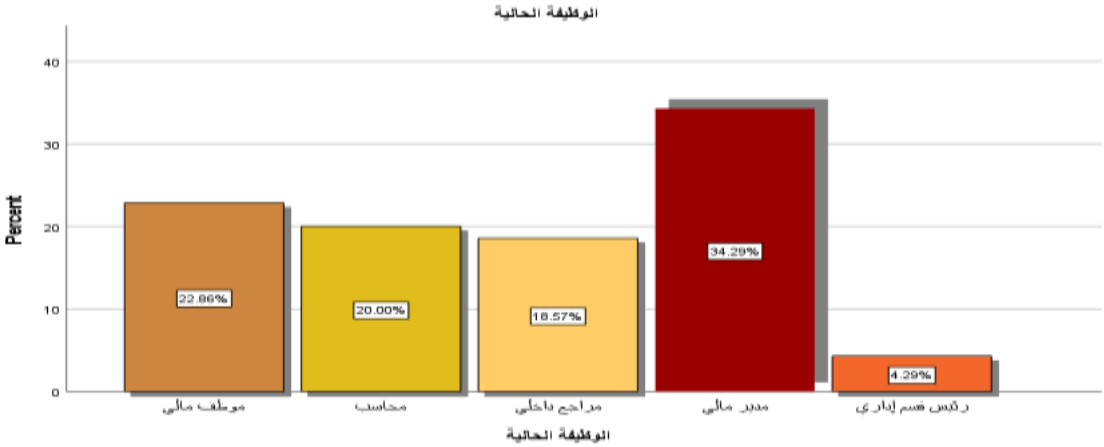
3 سنوات الخبرة:



الشكل رقم (3) يمثل التوزيع النسبي لمتغير سنوات الخبرة الوظيفية
المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

من خلال الشكل رقم (3) أظهرت النتائج أن العينة تتكون في معظمها من موظفين ذوي خبرة متوسطة. حيث شكّلت الفئة الأكبر التي تمثل 62.86% من أفراد العينة من يملكون خبرة تتراوح بين 5 سنوات إلى أقل من 10 سنوات. كما يمتلك 20% من العينة خبرة من 10 سنوات إلى أقل من 15 سنة. ثم تليه الفئة التي تقل خبرتها عن 5 سنوات حيث شكلت 10% فقط من العينة، والباقي ما يمثلون 7.14% من العينة خبرتهم من 15سنة فأكثر. وهذا يعني أن نتائج الدراسة تستند بشكل أساسي إلى رؤى أفراد يتمتعون بخبرة طويلة وممتدة داخل المؤسسة.

4 الوظيفة الحالية:

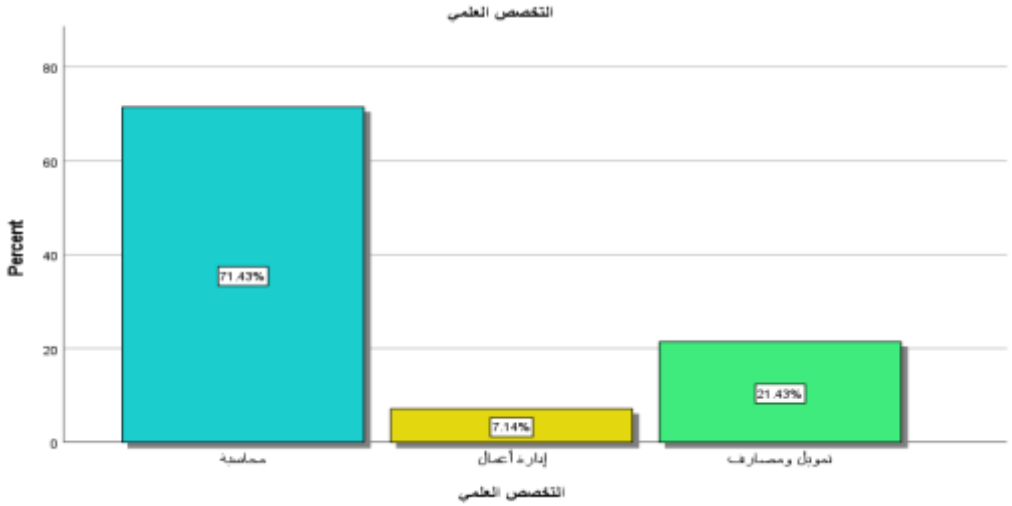


الشكل رقم (4) يمثل التوزيع النسبي لمتغير الوظيفة الحالية

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

من خلال الشكل رقم (4) يتبين أن العينة مسحوبة من مختلف الأقسام لضمان التمثيل الشامل. وقد سجلت وظيفة المدير المالي أعلى نسبة من المشاركين ما يمثل 34.29% من إجمالي العينة. وهو منصب إشرافي وقراراته مؤثرة، تلتها وظيفة موظف مالي بنسبة 22.86%، ثم وظيفة محاسب بنسبة 20%. ثم وظيفة مراجع داخلي بنسبة 18.57% أما بقية أفراد العينة فوظيفتهم رئيس قسم إداري بنسبة 4.29%. هذا التنوع في الوظائف المالية والرقابية (من محاسب وموظف، إلى مراجع، إلى مدير مالي) يضمن للبحث الحصول على آراء من مختلف زوايا العمل المحاسبي والرقابي، وهو ما يثري التحليل.

5التخصص العلمي:



الشكل رقم (5) يمثل التوزيع النسبي لمتغير التخصص العلمي

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

من خلال الشكل رقم (5) يتبين أن العينة متنوعة التخصصات. فقد سجل تخصص المحاسبة أعلى نسبة من المشاركين ما يمثل 71.43% من إجمالي العينة. يليه تخصص التمويل والمصارف بنسبة 21.43%، أما بقية أفراد العينة فتخصصهم إدارة أعمال بنسبة 7.14%. ويعكس هذا التوزيع توافقا للتخصص مع طبيعة الدراسة. هذه النسب تؤكد بأن البيانات تم جمعها من مصدرها الصحيح، وهم الأفراد المتخصصون أكاديمياً ومهنياً في المحاسبة والعمل المصرفي، مما يعطي ثقلاً كبيراً للنتائج التي سيتم التوصل إليها.

وبصورة عامة يمكن القول إن المستجيب النموذجي في هذه الدراسة هو (مدير مالي أو محاسب، متخصص في المحاسبة، ذو مؤهل جامعي عالٍ، وعمره في الثلاثينيات، ويمتلك خبرة عملية تتراوح بين 5 إلى 10 سنوات). وهي خصائص مثالية تخدم أهداف البحث بدقة عالية.

ثانيا: تحليل أسئلة استمارة الاستبيان

تحليل محاور البحث وعبارات الاستبيان

1- التحليل الوصفي لمتغيرات الدراسة (Descriptive Statistics)

يهدف هذا الجزء إلى وصف وتحليل اتجاهات إجابات أفراد عينة الدراسة نحو كل عبارة من عبارات الاستبيان، بالإضافة إلى تحديد المستوى العام لكل محور من محاور الدراسة. ولتحقيق ذلك، تم حساب المتوسطات الحسابية والانحرافات المعيارية، وترتيب العبارات حسب أهميتها النسبية داخل كل محور، وذلك على النحو التالي:

الجدول رقم (2) نتائج تحليل عبارات محاور الاستبيان

ت	المتغير	العبارة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية	قيمة t	مستوى الدلالة sig
1	المتغير المستقل	يطبق المصرف إجراءات أمن سيبراني متقدمة لحماية النظم المحاسبية	4.10	0.617	4	4.36	0.000
2		يتم إجراء اختبارات دورية لاكتشاف الثغرات الأمنية في نظام المعلومات المحاسبية	4.26	0.582	1	4.30	0.000
3		يوجد نظام مراقبة مستمر للأنظمة المحاسبية للكشف عن التهديدات الأمنية.	4.24	0.464	2	4.36	0.000
4		يلتزم المصرف بتحديث أنظمة الأمن السيبراني بشكل منتظم	4.20	0.604	3	4.30	0.000
		المحور الأول: الممارسات التقنية للأمن السيبراني	**4.20**	**0.497**	**2**	**20.182**	**0.000**
1		توجد سياسات أمن معلومات مكتوبة ومعتمدة في المصرف.	2.87	1.115	3	-0.838-	0.402
2		يتم تنفيذ السياسات الأمنية بشكل فعال ودقيق.	2.92	1.194	1	-0.486-	0.627
3		يتم مراجعة وتحديث السياسات الأمنية بشكل دوري.	2.90	1.206	2	-0.363-	0.717
4		يوجد عدد كاف من الكوادر البشرية المؤهلة في مجال الأمن السيبراني داخل المصرف.	1.87	0.536	4	-7.418-	0.000
5		يحصل الموظفون على تدريبات كافية للتعامل مع التهديدات الأمنية.	1.83	0.510	5	-7.484-	0.000
		المحور الثاني: الكفاءة البشرية والتنظيمية	**2.47**	**0.625**	**3**	**7.035-**	**0.000**
1		يوجد فريق متخصص بالأمن السيبراني في المصرف.	4.36	0.483	1	7.565	0.000
2		هناك تكامل وتعاون بين وحدات الأمن السيبراني ووحدات المحاسبة.	4.30	0.622	2	7.195	0.000
		المحور الثالث: الهيكل التنظيمي المتخصص	**4.33**	**0.509**	**1**	**21.798**	**0.000**
		محور المتغير المستقل الكلي (الأمن السيبراني)	**3.67**	**0.353**		**15.827**	**0.000**

ت	المتغير	العبارة	المتوسط الحسابي	الانحراف المعياري	الأهمية النسبية	قيمة t	مستوى الدلالة sig
	المتغير التابع	تظل البيانات المحاسبية محمية من الضياع أو التعديل غير المصرح به.	4.06	0.611	4	7.157	0.000
2		تساهم إجراءات الأمن في تحسين كفاءة ودقة نظام المعلومات المحاسبي.	4.31	0.553	1	7.389	0.000
3		تساهم إجراءات الأمن في تعزيز ثقة العملاء وسمعة المصرف.	4.16	0.581	3	7.292	0.000
4		تضمن إجراءات الأمن جودة وموثوقية التقارير المالية.	4.24	0.600	2	7.279	0.000
المحور الرابع: المتغير التابع (حماية نظم المعلومات المحاسبية)			**4.19**	**0.419**		**23.787**	**0.000**

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

يوضح الجدول (2) نتائج الإحصاء الوصفي (المتوسطات الحسابية والانحرافات المعيارية) والأهمية النسبية، بالإضافة إلى نتائج اختبار T للعينة الواحدة (One-Sample T-Test)، وذلك لوصف اتجاهات إجابات عينة الدراسة حول محاور الدراسة. تم استخدام اختبار T لمقارنة المتوسط الحسابي لكل عبارة وكل محور بالقيمة المفترضة (3)، والتي تمثل متوسط المقياس في مقياس ليكرت الخماسي.
فإذا كان مستوى الدلالة (Sig.) أقل من (0.05) والمتوسط الحسابي أكبر من (3)، يعتبر المستوى مرتفعاً.
وإذا كان مستوى الدلالة (Sig.) أقل من (0.05) والمتوسط الحسابي أقل من (3)، يعتبر المستوى منخفضاً.
وإذا كان مستوى الدلالة (Sig.) أكبر من (0.05)، يعتبر المستوى متوسطاً (محايداً)، أي أنه لا يختلف جوهرياً عن(3) .

أ- مستوى الممارسات التقنية للأمن السيبراني (الإجابة على السؤال الأول)
يُظهر الجدول أن المستوى العام لتطبيق الممارسات التقنية للأمن السيبراني في المصارف قيد الدراسة كان مرتفعاً؛ حيث بلغ المتوسط الحسابي الإجمالي للمحور (4.20) بانحراف معياري (0.497). وهذه القيمة أعلى من المتوسط الفرضي (3) وهو دال إحصائياً، حيث بلغت قيمة T (20.182) بمستوى دلالة (Sig. = 0.000)، وهو ما يؤكد أن هذا الارتفاع جوهري وحقيقي.
وعلى مستوى العبارات، جاءت جميعها بمستوى مرتفع وبدلالة إحصائية(Sig. = 0.000) أقل من 0.05. جاءت العبارة (يتم إجراء اختبارات دورية لاكتشاف الثغرات الأمنية) في المرتبة الأولى كأكثر الممارسات تطبيقاً بمتوسط حسابي.(4.26) ، تليها (يوجد نظام مراقبة مستمر للأنظمة المحاسبية) بمتوسط.(4.24) بينما جاءت عبارة (يطبق المصرف إجراءات أمن سيبراني متقدمة) في المرتبة الأخيرة، وإن كانت لا تزال بمستوى مرتفع جداً (بمتوسط 4.10).
تشير قيم الانحراف المعياري المنخفضة (أقل من 1) لجميع العبارات إلى درجة عالية من التجانس وتقارب آراء أفراد العينة حول ارتفاع مستوى تطبيق هذه الممارسات.

ب- مستوى الكفاءة البشرية والتنظيمية (الإجابة على السؤال الثاني)
بينت النتائج عن وجود انخفاض واضح في المستوى العام لـ الكفاءة البشرية والتنظيمية، حيث بلغ المتوسط الحسابي الإجمالي للمحور (2.47) بانحراف معياري (0.625). وهذا الانخفاض يُعد ذا دلالة إحصائية، حيث بلغت قيمة T (-7.035) بمستوى دلالة.(Sig. = 0.000)
ويُظهر تحليل العبارات انقساماً واضحاً داخل هذا المحور حيث أظهر الجانب التنظيمي (السياسات): العبارات الثلاث الأولى المتعلقة بـ (وجود السياسات، تفعيلها، ومراجعتها) جاءت جميعها بمتوسط (محايد). فمتوسطاتها الحسابية (2.87, 2.92, 2.90) لا تختلف جوهرياً عن القيمة (3)، حيث كانت مستويات الدلالة لها (0.402, 0.627, 0.717) على التوالي، وهي قيم غير دالة إحصائياً (أكبر من 0.05).
أما الجانب البشري (الكفاءة): العبارتان (4 و5) المتعلقتان بـ (وجود كوادر بشرية مؤهلة) و (الحصول على تدريب كافٍ) جاءتا بمستوى منخفض جداً وبدلالة إحصائية واضحة .(Sig. = 0.000) حيث بلغ متوسطهما (1.87) و (1.83) على التوالي، وهما العبارتان الأقل تقييماً في الاستبانة بأكملها.

يمكن الاستنتاج أن الضعف الجوهري في هذا البُعد لا يكمن في وجود السياسات بقدر ما يكمن في النقص الحاد في الكوادر البشرية المؤهلة والتدريب الكافي، وهو ما سحب المتوسط العام للمحور نحو الانخفاض.

ج- واقع الهيكل التنظيمي المتخصص (الإجابة على السؤال الثالث)

أظهرت النتائج أن واقع (الهيكل التنظيمي المتخصص) جاء بمستوى مرتفع جداً، حيث بلغ المتوسط الحسابي الإجمالي للمحور (4.33)، وهو الأعلى بين جميع أبعاد المتغير المستقل. وهذا الارتفاع ذو دلالة إحصائية عالية قيمة(Sig. = 0.000). ، T = 21.798

وجاءت كلتا العبارتين المكونتين للمحور بمستوى مرتفع وبدلالة إحصائية (Sig. = 0.000)

جاءت عبارة (يوجد فريق متخصص بالأمن السيبراني في المصرف) في المرتبة الأولى بمتوسط.(4.36)

تلتها عبارة (هناك تكامل وتعاون بين وحدات الأمن السيبراني ووحدات المحاسبة) بمتوسط (4.30) يشير هذا إلى أن المصارف تولي اهتماماً كبيراً لوجود فرق متخصصة وتدعم التكامل بينها وبين المحاسبة.

د- المستوى الإجمالي لفعالية الأمن السيبراني (المتغير المستقل)

بلغ المتوسط الحسابي الإجمالي لـ فعالية الأمن السيبراني (بأبعاده الثلاثة مجتمعة) (3.67) بانحراف معياري (0.353). وهي قيمة مرتفعة وذات دلالة إحصائية) قيمة(Sig. = 0.000). ، T = 15.827

يشير هذا إلى أن تصورات العينة لفعالية الأمن السيبراني إيجابية بشكل عام. ومع ذلك، يجب تفسير هذا المتوسط المرتفع بحذر، حيث إنه ناتج عن مستوى مرتفع جداً في الممارسات التقنية والهيكل التنظيمي، ولكنه يخفي ضعفاً جوهرياً ومنخفضاً في بُعد الكفاءة البشرية والتدريب.

هـ - مستوى حماية نظم المعلومات المحاسبية (الإجابة على السؤال الرابع)

أظهرت النتائج أن مستوى حماية نظم المعلومات المحاسبية كان مرتفعاً من وجهة نظر عينة الدراسة. حيث بلغ المتوسط الحسي الإجمالي للمحور (4.19) بانحراف معياري (0.419)، وهو ارتفاع جوهري ودال إحصائياً قيمة (Sig. = 0.000) ،T = 23.787

وعلى مستوى العبارات، جاءت جميعها بمستوى مرتفع وبدلالة إحصائية (Sig. = 0.000)

جاءت عبارة (تساهم إجراءات الأمن في تحسين كفاءة ودقة نظام المعلومات المحاسبي) في المرتبة الأولى بمتوسط.(4.31) تلتها عبارة (تضمن إجراءات الأمن جودة وموثوقية التقارير المالية) بمتوسط (4.24).

بينما جاءت عبارة (تظل البيانات المحاسبية محمية من الضياع أو التعديل) في المرتبة الأخيرة، ولكنها لا تزال بمستوى مرتفع جداً (بمتوسط 4.06).

يشير هذا إلى رضا عام لدى العينة عن قدرة الإجراءات الحالية على حماية النظم المحاسبية وضمان جودة مخرجاتها.

2- تحليل الارتباط بين المتغيرات (Correlation Analysis)

لمعرفة طبيعة العلاقة بين الابتكار الإداري كمتغير مستقل بأبعاده المختلفة (الهيكلي، القيادي، التقني)، والمرونة المؤسسية كمتغير تابع، تم استخدام معامل ارتباط بيرسون.

جدول رقم (3) يمثل مصفوفة الارتباط بين متغيرات الدراسة

المتغير	(1)	(2)	(3)	(4)
(1) الممارسات التقنية للأمن السيبراني	1			
(2) الكفاءة البشرية والتنظيمية	0.021	1		
(3) الهيكل التنظيمي المتخصص	0.430**	- 0.014	1	
(4) حماية نظم المعلومات المحاسبية	0.733**	0.132	0.436**	1
الأمن السيبراني بأبعاده مجتمعة	0.690**	0.594**	0.675**	0.632**

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

ملاحظة: ** تعني أن مستوى الدلالة (P-value) هو أقل من 0.01.

يوضح الجدول رقم (3) نتائج تحليل الارتباط نتائج تحليل معامل ارتباط بيرسون (Pearson Correlation)، والذي تم إجراؤه بهدف قياس طبيعة وقوة واتجاه العلاقة الخطية بين متغيرات الدراسة المستقلة (الممارسات التقنية، الكفاءة البشرية والتنظيمية، الهيكل التنظيمي المتخصص)، والمتغير التابع (حماية نظم المعلومات المحاسبية)، وذلك عند مستوى دلالة (0.05). وتُظهر النتائج ما يلي:

أ- العلاقة بين أبعاد الأمن السيبراني وحماية نظم المعلومات المحاسبية

1. **الممارسات التقنية :**أظهرت النتائج وجود علاقة ارتباط **طردية قوية وذات دلالة إحصائية عالية** بين الممارسات التقنية وحماية نظم المعلومات المحاسبية، حيث بلغ معامل الارتباط (r = 0.733) ، وبمستوى دلالة (Sig. < 0.001) وهي قيمة دالة إحصائياً لأنها أقل من (0.05). يشير هذا إلى أنه كلما زاد مستوى تطبيق الممارسات التقنية في المصارف، ارتفع مستوى حماية نظمها المحاسبية.
2. **الكفاءة البشرية والتنظيمية :**بينت النتائج عن عدم وجود علاقة ارتباط ذات دلالة إحصائية بين الكفاءة البشرية والتنظيمية وحماية نظم المعلومات المحاسبية. فعلى الرغم من أن العلاقة إيجابية، إلا أنها ضعيفة جداً(r = 0.132) ، وبمستوى دلالة (Sig. = 0.274)، وهي قيمة غير دالة إحصائياً لأنها أكبر من (0.05).
3. **الهيكل التنظيمي المتخصص :**تبين وجود علاقة ارتباط **طردية متوسطة القوة وذات دلالة إحصائية عالية** بين الهيكل التنظيمي المتخصص وحماية نظم المعلومات المحاسبية، حيث بلغ معامل الارتباط (r = 0.436)، وبمستوى دلالة (Sig. < 0.001)، وهي دالة إحصائياً.

ب- العلاقة الإجمالية (الفرضية الرئيسية)

يُظهر التحليل وجود علاقة ارتباط **طردية قوية وذات دلالة إحصائية عالية** بين أبعاد فعالية الأمن السيبراني مجتمعة وحماية نظم المعلومات المحاسبية، حيث بلغ معامل الارتباط(r = 0.632) ، وبمستوى دلالة (Sig. < 0.001)

ج- فحص الارتباط المتعدد (Multicollinearity) بين الأبعاد المستقلة

- لضمان صلاحية نموذج الانحدار، تم فحص العلاقات البينية بين الأبعاد المستقلة.
- يلاحظ وجود علاقة ارتباط متوسطة ودالة إحصائياً بين الممارسات التقنية والهيكل التنظيمي (r = 0.430).
- بينما لا توجد علاقة دالة إحصائياً بين الكفاءة البشرية وكل من الممارسات التقنية والهيكل التنظيمي.
- نظراً لأن جميع معاملات الارتباط البينية بين الأبعاد المستقلة جاءت أقل من الحد الحرج (0.80)، فإن هذا يشير إلى **غياب مشكلة الارتباط الخطي المتعدد** (Multicollinearity)، مما يؤكد صلاحية المتغيرات المستقلة للدخول في نموذج تحليل الانحدار.

3- اختبار فرضيات الدراسة

لاختبار فرضيات الدراسة، تم تطبيق نموذج الانحدار الخطي المتعدد (Multiple Regression Analysis) حيث يمثل متغير حماية نظم المعلومات المحاسبية المتغير التابع، وتمثل الأبعاد الثلاثة لفعالية الأمن السيبراني المتغيرات المستقلة.

تم فحص صلاحية النموذج للتحليل، حيث أظهرت مصفوفة الارتباط) جدول 3 سابقاً (عدم وجود مشكلة الارتباط الخطي المتعدد (Multicollinearity) بين المتغيرات المستقلة (حيث كانت جميع معاملات الارتباط أقل من 0.80). وتوضح الجداول التالية نتائج التحليل.

اختبار الفرضية الرئيسية

الفرضية الرئيسية تنص على أنه يوجد تأثير ذو دلالة إحصائية إيجابي لفعالية الأمن السيبراني (بأبعاده مجتمعة) على حماية نظم المعلومات المحاسبية عند مستوى المعنوية 5%.

وتهدف هذه الخطوة إلى تحديد مدى قدرة المتغير المستقل على تفسير التغيرات في المتغير التابع، وتحديد أي من أبعاده كان له الأثر الأكبر.

جدول رقم (4) يوضح ملخص نموذج الانحدار (Model Summary)

R	R Square	Adjusted R Square	F	.Sig
0.754	0.569	0.550	29.062	0.000 دال معنويا

تُظهر نتائج تحليل الانحدار الموضحة في الجدول (4) ما يلي:

1. **اختبار جودة التوفيق (Goodness of Fit):** يُظهر الجدول أن النموذج ككل (الأبعاد الثلاثة للأمن السيبراني مجتمعة) ذو دلالة إحصائية عالية في تفسير المتغير التابع (حماية نظم المعلومات المحاسبية). حيث بلغت قيمة (F) المحسوبة (29.062)، وهي دالة إحصائياً عند مستوى دلالة (Sig. = <.001) وهو أقل من 0.05. بناءً على هذه النتيجة، يتم **قبول الفرضية الرئيسية للدراسة**، والتي تنص على: يوجد تأثير ذو دلالة إحصائية إيجابي لفعالية الأمن السيبراني (مجتمعة) على حماية نظم المعلومات المحاسبية.
2. **القوة التفسيرية للنموذج :**يُظهر الجدول أن قيمة معامل الارتباط المتعدد (R) بلغت (0.754)، مما يشير إلى وجود علاقة ارتباط **طردية قوية** بين متغيرات الأمن السيبراني مجتمعة وبين حماية النظم المحاسبية. كما بلغت قيمة **معامل التحديد المعدل (Adjusted R Square)** (0.550). هذا يعني أن **55%** من التغيرات (التباين) الحاصلة في مستوى حماية نظم المعلومات المحاسبية المتغير التابع في المصارف قيد الدراسة، يمكن تفسيرها من خلال المتغيرات المستقلة الثلاثة مجتمعة (الممارسات التقنية، الكفاءة البشرية، والهيكل التنظيمي). وتُعد هذه القوة التفسيرية مرتفعة وذات أهمية عملية. أما النسبة المتبقية (45%) فتعود إلى متغيرات أخرى لم يتضمنها نموذج الدراسة.

اختبار الفرضيات الفرعية (تأثير كل بُعد على حدة)
للتحقق من الفرضيات الفرعية، تم تحليل تأثير كل بُعد على حدى لتحديد الأهمية النسبية لكل بعد من أبعاد المتغير المستقل، كما يوضحه تحليل جدول المعاملات (Coefficients).

جدول رقم (5) يوضح معاملات الانحدار (Coefficients)

المتغير (الأبعاد)	B	Beta	T	.Sig
(Constant)	1.097		2.997	0.004
الممارسات التقنية للأمن السيبراني	0.561	0.665	7.423	0.000 دال معنويا
الكفاءة البشرية والتنظيمية	0.081	0.120	1.488	0.141 غير دال معنويا
الهيكل التنظيمي المتخصص	0.125	0.152	1.700	0.094 غير دال معنويا

المصدر: من إعداد الباحثة بالاعتماد على مخرجات برنامج SPSS

تُظهر نتائج تحليل معاملات الانحدار الموضحة في الجدول (5) الأثر النسبي لكل بُعد من أبعاد الأمن السيبراني كما يلي:

1-الفرضية الفرعية الأولى (أثر الممارسات التقنية): تنص الفرضية على: يوجد تأثير ذو دلالة إحصائية إيجابي لمستوى تطبيق الممارسات التقنية على مستوى حماية نظم المعلومات المحاسبية.
أظهر الجدول أن قيمة (Sig.) لمتغير الممارسات التقنية بلغت (0.000)، وهي قيمة أقل من مستوى المعنوية (0.05). كما جاءت قيمة معامل (B) إيجابية (0.561). بالتالي يتم **قبول الفرضية الفرعية الأولى**. أي يوجد تأثير إيجابي ومعنوي إحصائياً للممارسات التقنية على حماية النظم المحاسبية.

2-**الفرضية الفرعية الثانية (أثر الكفاءة البشرية):** تنص الفرضية على: يوجد تأثير ذو دلالة إحصائية إيجابي لمستوى الكفاءة البشرية والتنظيمية على مستوى حماية نظم المعلومات المحاسبية.
أظهر الجدول أن قيمة (Sig.) لمتغير الكفاءة البشرية بلغت (0.141)، وهي قيمة أكبر من مستوى المعنوية (0.05). بالتالي يتم **رفض الفرضية الفرعية الثانية**. أي لا يوجد تأثير ذو دلالة إحصائية للكفاءة البشرية والتنظيمية على حماية النظم المحاسبية (عند أخذ المتغيرات الأخرى في الاعتبار).

3-الفرضية الفرعية الثالثة (أثر الهيكل التنظيمي): تنص الفرضية على: يوجد تأثير ذو دلالة إحصائية إيجابي لوجود هيكل تنظيمي متخصص على مستوى حماية نظم المعلومات المحاسبية.
أظهر الجدول أن قيمة (Sig.) لمتغير الهيكل التنظيمي بلغت (0.094)، وهي قيمة أكبر من مستوى المعنوية (0.05). بالتالي يتم **رفض الفرضية الفرعية الثالثة**. أي لا يوجد تأثير ذو دلالة إحصائية للهيكل التنظيمي المتخصص على حماية النظم المحاسبية.

الأهمية النسبية للمتغيرات ومعادلة الانحدار

الأهمية النسبية: لتحديد أي أبعاد الأمن السيبراني كان له التأثير الأكبر، ننظر إلى قيم بيتا المعيارية (Standardized Coefficients Beta). يتضح أن متغير الممارسات التقنية هو المتغير الأكثر تأثيراً وأهمية في حماية النظم المحاسبية (قيمة Beta = 0.665). يأتي الهيكل التنظيمي في المرتبة الثانية (Beta = 0.152)، والكفاءة البشرية في المرتبة الأخيرة (Beta = 0.120)، ولكن تأثيرهما كان غير دال إحصائياً.

معادلة الانحدار:
معادلة الانحدار لتأثير الأبعاد الثلاثة للأمن السيبراني على حماية نظم المعلومات المحاسبية:

$$Y=\beta_0+\beta_1X_1+\beta_2X_2+\beta_3X_3+\varepsilon$$

حيث:
Y: حماية نظم المعلومات المحاسبية (المتغير التابع)
X_1: الممارسات التقنية للأمن السيبرانية
X_2: الكفاءة البشرية والتنظيمية
X_3: الهيكل التنظيمي المتخصص.
β_0: الثابت.
β_1 ,β_2 ,β_3 , : معاملات الانحدار الموضحة في الجدول.
ε : الخطأ العشوائي. (العوامل غير المدرجة في النموذج).
ومن خلال القيم المستخلصة من الجدول نحصل على معادلة الانحدار المتعدد

$$Y = 1.097+0.561X_1+ 0.081X_2 +0.125X_3 +\varepsilon$$

التفسير:
قيمة الثابت (1.097) تشير إلى المستوى الأساسي لحماية النظم المحاسبية في حال انعدام المتغيرات المستقلة. أما قيمة (B_1=0.561) تعني أن كل زيادة بمقدار وحدة واحدة في الممارسات التقنية، تؤدي إلى زيادة في حماية النظم المحاسبية بمقدار (0.561) وحدة، مع بقاء المتغيرات الأخرى ثابتة.
بصورة عامة أثبت التحليل أن نموذج الأمن السيبراني ككل له تأثير جوهري على حماية نظم المعلومات المحاسبية ويفسر 55% من التغير فيه. ولكن، هذا التأثير الإيجابي نابع بشكل شبه حصري من بُعد واحد فقط وهو الممارسات التقنية، بينما لم يظهر البُعد البشري (الكفاءة والتدريب) والبُعد الهيكلي (الفريق المتخصص) تأثيراً ذا دلالة إحصائية في هذا النموذج، وهو ما يتسق مع نتائج التحليل الوصفي التي أظهرت انخفاضاً واضحاً في مستوى الكفاءة البشرية والتدريب.

المناقشة والنتائج والتوصيات

مناقشة وتفسير النتائج

يُعَد هذا الجزء الركيزة الأساسية في الدراسة، حيث يتم فيه تجاوز العرض الوصفي للنتائج إلى مرحلة التفسير والتحليل العميق. سيتم في هذا الجزء مناقشة النتائج الرئيسية وربطها بالإطار النظري والدراسات السابقة، وصولًا إلى إبراز المساهمة العلمية التي يقدمها هذا البحث.

1. مناقشة الفرضية الرئيسية (تأثير الأمن السيبراني ككل)

أظهرت نتائج تحليل الانحدار وجود تأثير إيجابي ذي دلالة إحصائية لفعالية الأمن السيبراني (بأبعاده الثلاثة مجتمعة) على حماية نظم المعلومات المحاسبية. حيث نجح النموذج في تفسير 55% (Adjusted R Square = 0.550) من التباين الحاصل في المتغير التابع، وهي نسبة تفسيرية مرتفعة وجوهرية.

الاتفاق مع الدراسات السابقة:

تتفق هذه النتيجة بشكل عام مع الإطار النظري ومعظم الدراسات التي أكدت على وجود علاقة إيجابية بين الأمن السيبراني وحماية النظم المحاسبية.

تتفق مع دراسة عبد المهدي (2020) التي توصلت إلى وجود علاقة بين إدارة المخاطر السيبرانية وجودة نظم المعلومات المحاسبية.

وتتفق مع دراسة يوسف (2024) التي أكدت أن التهديدات السيبرانية تؤثر سلباً على نظم المعلومات المحاسبية في ليبيا.

كما تتفق مع دراسة Daoud & Serag (2022) التي هدفت إلى زيادة الثقة في التقارير المالية عبر الأمن السيبراني.

الإضافة العلمية (R مقابل r): يكشف هذا البحث عن نتيجة دقيقة؛ فعلى الرغم من أن معامل الارتباط البسيط (Pearson r) بين متوسط الأمن السيبراني والحماية كان (0.632) (كما في جدول الارتباط)، إلا أن معامل الارتباط المتعدد (Multiple R) في نموذج الانحدار كان أعلى بكثير (0.754). هذا يشير إلى أن تأثير الأمن السيبراني ليس تأثيراً بسيطاً ناجماً عن متوسط أبعاده، بل هو تأثير موزون. حيث اكتشف نموذج الانحدار توليفة مثلى تمنح وزناً أكبر بكثير للبُعد الأقوى (الممارسات التقنية)، وهذا ما يفسر ارتفاع القوة التفسيرية للنموذج.

2. مناقشة الفرضيات الفرعية (الأهمية النسبية للأبعاد)

بين تحليل الانحدار (جدول Coefficients) التأثير الإيجابي الكلي نابع بشكل شبه حصري من بُعد واحد فقط.

أ) الممارسات التقنية: أظهرت النتائج قبول الفرضية الفرعية الأولى؛ حيث كان لـ الممارسات التقنية تأثير إيجابي قوي جداً (Beta = 0.665) وذو دلالة إحصائية عالية (.Sig=0.000) على حماية النظم المحاسبية.

الاتفاق مع الدراسات: هذه النتيجة منطقية وتتفق مع دراسة Dasgupta et al. (2023) التي ركزت على أهمية الأنظمة المتقدمة (كالذكاء الاصطناعي) في الأمن السيبراني البنكي. كما تتماشى مع توصيات دراسة التائب والسائح (2025) بضرورة الاستثمار في تقنيات الأمن السيبراني المتطورة وتحديث الأنظمة.

يُفسر هذا بأن المصارف التجارية في مدينة الزاوية تعتمد بشكل تقني على حماية أنظمتها. فالإجراءات الملموسة (كالتحديثات، المراقبة، الاختبارات)، والتي أظهر التحليل الوصفي أن مستواها مرتفع فعلاً (بمتوسط 4.20)، هي التي تُحدث الأثر الفعلي في الحماية من وجهة نظر العينة.

ب) الكفاءة البشرية والتنظيمية: تم رفض الفرضية الفرعية الثانية. لم يُظهر متغير الكفاءة البشرية والتنظيمية أي تأثير ذي دلالة إحصائية على حماية النظم (Sig. = 0.141). **هذه النتيجة لا تعني أن الكفاءة البشرية غير مهمة**، بل تفسرها نتائج التحليل الوصفي حيث أن مستوى هذا البُعد كان منخفضاً جداً (بمتوسط 2.47)، خاصة في فقرتي وجود كوادر مؤهلة (1.87) والتدريب الكافي (1.83). بالتالي فإن هذا البُعد لا يساهم في تعزيز الحماية.

الاتفاق مع الدراسات: هذه النتيجة هي جوهر ما يميز هذا البحث وتتفق بشكل مباشر ودقيق مع دراستين في البيئة الليبية: حيث تتطابق تماماً مع دراسة يوسف (2024) التي شخصت نقص في التدريب والوعي الأمني للموظفين كأحد أهم نقاط الضعف في المؤسسات المالية الليبية.

كما تؤكد بشكل قاطع على صحة توصيات دراسة التائب والسائح (2025) التي طالبت بـ تنظيم دورات وورش عمل دورية لموظفي المصارف.

وهي تختلف عن دراسة زعابطة (2022) في الجزائر، التي وجدت أن المؤسسة محل الدراسة تولي اهتماماً بالوسائل البشرية والتقنية معاً، مما يبرز أن النقص في الجانب البشري قد يكون سمة أكثر وضوحاً في المجتمع الليبي.

ج) الهيكل التنظيمي المتخصص: تم رفض الفرضية الفرعية الثالثة. لم يُظهر الهيكل التنظيمي المتخصص تأثيراً ذا دلالة إحصائية (Sig. = 0.094). هنا يكمن تناقض ظاهري مهم. التحليل الوصفي أظهر أن مستوى هذا البُعد مرتفع جداً (بمتوسط 4.33)، حيث أجابت العينة بـ وجود فريق متخصص ووجود تكامل وتعاون.

(الإضافة العلمية): يحلل نموذج الانحدار هذا التناقض. فهو يوضح أن الوجود الشكلي للهيكل التنظيمي (أي وجود فريق على الورق) لا يعني بالضرورة الفعالية التأثيرية لهذا الهيكل. طالما أن هذا الهيكل يعاني من نقص في الكفاءة البشرية والتدريب، فإن تأثيره الإيجابي يصبح هامشياً (Sig. 0.094) ويطغى عليه التأثير القوي للممارسات التقنية.

3. مناقشة مستوى المتغير التابع (حماية نظم المعلومات المحاسبية)

أظهرت النتائج أن مستوى حماية نظم المعلومات المحاسبية كان مرتفعاً (بمتوسط 4.19).

هذا الارتفاع في المتغير التابع يبدو متسقاً مع الارتفاع في المتغير المستقل، أي أن العينة تشعر أن النظم محمية (مرتفع) لأنها ترى الإجراءات التقنية مطبقة (مرتفع)، حتى لو كانوا يدركون النقص في التدريب (منخفض).

الاتفاق مع الدراسات: يتفق هذا مع هدف دراسة Daoud & Serag (2022) حول تعزيز الثقة، ومع نتائج دراسة Al-Okaily et al. (2022) التي ركزت على جودة البيانات والمعلومات كمقياس للنجاح (والتي تضمنتها فقرات المتغير التابع في هذه الدراسة).

أهم النتائج

بناءً على التحليل الإحصائي الوصفي والاستدلالي لبيانات الدراسة، تم التوصل إلى النتائج الرئيسية التالية، والتي تجيب على أسئلة البحث وتحقق أهدافه:

1. أظهرت النتائج أن مستوى تطبيق الممارسات التقنية (كالتحديث والمراقبة) في المصارف قيد الدراسة جاء بمستوى مرتفع وبدلالة إحصائية.
2. كشفت النتائج عن مستوى منخفض وبدلالة إحصائية لـ الكفاءة البشرية والتنظيمية، ويُعزى هذا الانخفاض بشكل جوهري إلى النقص الحاد في الكوادر المؤهلة والتدريب الكافي.
3. تبين أن واقع الهيكل التنظيمي المتخصص (من حيث وجود الفرق والتكامل) جاء بمستوى مرتفع وبدلالة إحصائية.
4. أظهرت النتائج أن المستوى العام لـ حماية نظم المعلومات المحاسبية في المصارف قيد الدراسة كان مرتفعاً من وجهة نظر العينة.
5. تم قبول الفرضية الرئيسية، حيث أثبتت النتائج وجود تأثير إيجابي ذي دلالة إحصائية لـ فعالية الأمن السيبراني (بأبعاده مجتمعة) على حماية نظم المعلومات المحاسبية. ونجح النموذج في تفسير 55% من التغيرات في مستوى الحماية.
6. أظهر التحليل أن هذا التأثير الإيجابي غير متوازن وناتج بشكل شبه حصري عن بُعد واحد حيث:

أ- تم قبول الفرضية الفرعية الأولى: يوجد تأثير إيجابي قوي جداً وذو دلالة إحصائية لـ الممارسات التقنية على حماية النظم.

ب- تم رفض الفرضية الفرعية الثانية: لا يوجد تأثير ذو دلالة إحصائية لـ الكفاءة البشرية والتنظيمية على حماية النظم.

ت- تم رفض الفرضية الفرعية الثالثة: لا يوجد تأثير ذو دلالة إحصائية لـ الهيكل التنظيمي المتخصص على حماية النظم.

الخلاصة :

حققت الدراسة أهدافها الرئيسية، وكشفت أن المصارف التجارية في العينة تعتمد بشكل حاسم على الرادع التقني لحماية نظمها، بينما تعاني من فجوة بشرية وتنظيمية واضحة. فعلى الرغم من وجود هياكل تنظيمية، إلا أن نقص الكفاءة والتدريب جعلها غير مؤثرة، وهو ما يمثل نقطة الضعف الأخطر التي يجب معالجتها.

التوصيات (Recommendations)

بناءً على النتائج التي توصلت إليها الدراسة، توصي الدراسة بما يلي:

1-ضرورة التحول من الأمن السيبراني المعتمد على التكنولوجيا إلى الأمن السيبراني المتكامل (بشري-تقني).

2-العمل على استقطاب وتوظيف كوادر بشرية مؤهلة ومتخصصة في مجال الأمن السيبراني المحاسبي، لسد النقص الحاد الذي أظهرته نتائج التحليل الوصفي.

3-يجب ألا يقتصر دور (الفريق المتخصص بالأمن السيبراني) على الوجود الشكلي (الذي أثبتت الدراسة عدم تأثيره)، بل يجب منحه الصلاحيات والموارد اللازمة لتفعيل دوره الرقابي والتنفيذي.

4- توصي الدراسة بضرورة مراجعة السياسات الأمنية المكتوبة والتأكد من وضوحها، والأهم إنفاذها بشكل صارم ومحاسبة المخالفين.

5-يُقترح أن يضع مصرف ليبيا المركزي حداً أدنى إلزامياً من برامج التدريب المتخصص كشرط لتجديد التراخيص المصرفية.

المقترحات لبحوث مستقبلية (Future Research)

بناءً على النتائج التي تم التوصل إليها، والقيود التي واجهت الدراسة الحالية، يمكن اقتراح المسارات البحثية التالية:

1. يُقترح إجراء دراسة كيفية (Qualitative Study) باستخدام المقابلات المعمقة مع مديري المصارف ومديري الأمن السيبراني، للبحث في الأسباب الجذرية التي تمنع المصارف من الاستثمار الكافي في الكفاءة البشرية (مثل قيود الميزانية، نقص الوعي الإداري، أو صعوبة العثور على كوادر).
2. يُقترح تكرار نموذج الدراسة وتطبيقه على مصارف تجارية في مدن ليبية أخرى (مثل طرابلس، بنغازي، مصراتة)، أو إجراء دراسة مقارنة بين المصارف التجارية والمصارف المتخصصة.
3. يُقترح إجراء دراسة مستقبلية تختبر دور الهيكل التنظيمي كمتغير معدل للعلاقة بين الممارسات التقنية وحماية النظم.

Compliance with ethical standards

Disclosure of conflict of interest

The author(s) declare that they have no conflict of interest.

المراجع:

1- البياتي، محمود مهدي .(2005) .تحليل البيانات الإحصائية باستخدام البرنامج الإحصائي .SPSS دار الحامد.
2- مطروح, وفاء, تداعيات جائحة كوفيد وتأثيرها على تحقيق الامن السيبراني في الجزائر ,المجلة الدولية للاتصال الاجتماعي ,المجلد9,عدد2,مستغانم,2022
3- بن جدو,بنعلية (تحديات الامن السيبراني لمواجهة الجريمة الالكترونية ,المجلة الجزائرية للأمن الانساني ,مجلد 7عدد2, 2022
4- اسماعيل امجد يوسف(مخاطر نظم المعلومات المحاسبية الالكترونية في الشركات المالية الاردنية ,رسالة ماجستير في محاسبة التمويل ,الاردن ,2011
5- عبد اللطيف ,زعابطة (اثر تكنولوجيا المعلومات على نظام المعلومات المحاسبية دراسة حالة شركات الاتصالات الجزائر,اطروحة دكتوراة ,كلية العلوم الاقتصادية والتجارية التسيير, جامعة غرداية جزائر,2022
6- الشريف,حرية شعبان,(مخاطر نظم المعلومات المحاسبية الالكترونية ,رسالة ماجستير,غزة,2006
7- النعانعة, بيان فراس(الصعوبات التي تواجه مديري المكتبات الجامعة الاردنية نحو استخدام تطبيقات الذكاء الاصطناعي ,مؤتمر بعنوان التقنيات الناشئة وتطبيقاتها في المكتبات ومؤسسات المعلومات ,كويت,2023
8- دهني ,روان بنت مفلح, استخدام تقنية الذكاء الاصطناعي لتقديم الخدمات المعلومات في المكتبات الجامعية في المملكة العربية السعودية ,مؤتمر بعنوان التقنيات الناشئة وتطبيقاتها في المكتبات كويت 2023
9- سعيد ,طاهر محمد, خالد سليمان(متطلبات تطبيق الامن السيبراني لأنظمة المعلومات في المؤسسات الاقتصادية الجزائرية ,رسالة ماجستير,2023,جامعة غرداية, كلية العلوم الاقتصادية/الجزائر.
10- عبد المهدي ,حنين بعنوان اثر تطبيق سياسات الامن السيبراني على جودة نظم المعلومات المحاسبية ,رسالة ماجستير, كلية الاقتصاد, الاردن 2020.

11- يوسف عبد السلام، عبد السلام عطية بعنوان تقييم تأثير التهديدات السيبرانية على نظم المعلومات المحاسبية في المؤسسات الليبية، المجلة العلمية للدراسات التجارية والبيئة، مجلد خامس عشر ,2024ع1.
12- التائب، على مفتاح، السائح، جبريل، عمر(2025)بعنوان اهمية تطبيق الامن السيبراني المحاسبي في المصارف التجارية الليبية, مجلة الدراسات الاقتصادية /جامعة سرت مجلد 8,ع1.
13-Iethto,Martti,andothers cyber security :Analytics Technology and Autmation. springer. switzerlan d,2015
14-Daoud ,M.M,Serag ,A,A(2022).Aproposed Framework for studying the impact of Cybersecurity on accounting information to increase trust in the financial reportse approach trade and finance ,42(1).
15-Al-okaily,M.ALGHAZZAWI,Ralkhwaldi,A,f(2022).the effect of digital accounting systems on the decision-making quality in the banking industry sector :a mediated moderated model global knowledge,memory and communication,
16-Dasgupta,s.yelikar,B.v,naredla,s.ibrahim, R.k,alazzam, M,B (2023) AL-POWERED CYBERSECURITY: identifying threats in digital banking in 2023 3rd international conference on advance computing and innovative technologies in engineering.