African Journal of Advanced Studies in Humanities and Social Sciences (AJASHSS)
المجلة الإفريقية للدراسات المتقدمة في العلوم الإنسانية والاجتماعية
Online-ISSN: 2957-5907
Volume 5, Issue 1, 2026
Page No: 266-293
Website: https://aaasjournals.com/index.php/ajashss/index
Arab Impact factor 2024: 0.81 **SJIFactor 2024: 6.856** **ISI 2025: 1.191**

The Reality of Cybersecurity and Its Impact on the Cost of Cyber Incidents: A Field Study at Masraf Al-Jumhouria - General Administration, Tripoli

Maryam Misbah Muftah Suhaym *
Department of Accounting، Faculty of Economics- Al-Ajaylat, Zawiya University, Al-Ajaylat ، Libya

واقع الأمن السيبراني وأثره على تكلفة الحوادث السيبرانية دراسة ميدانية بمصرف الجمهورية- الإدارة العامة طرابلس

أ. مريم مصباح مفتاح سحيم *
قسم المحاسبة، كلية الاقتصاد-العجيلات، جامعة الزاوية، العجيلات، ليبيا

**Corresponding author:* *m.sheem@zu.edu.ly*

Received: November 09، 2025	Accepted: January 20، 2026	Published: February 02، 2026

Abstract:
This study aimed to evaluate the reality of cybersecurity and its impact on the cost of cyber incidents at Al-Jumhouria Bbank (General Administration – Tripoli). The study population consisted of specialists in the IT, Risk Management, and Internal Audit departments. A questionnaire was distributed to a purposive sample of (28) participants, of which (24) valid questionnaires were retrieved for statistical analysis, representing a response rate of (85.7%), while the loss rate was (14.3%). The findings revealed a statistically significant impact of risk management performance and internal audit processes on reducing the costs associated with digital incidents. The study also indicated that the efficiency of financial aspects allocated to cybersecurity significantly lowers recovery expenses. The study recommends integrating cybersecurity standards into periodic audit plans, increasing financial allocations to upgrade technical defenses, and enhancing administrative coordination to reduce response time and potential damage costs.

Keywords: Al-Jumhouria Bank, Cybersecurity, risk management, financial implications, internal audit, cost of cyber incidents.

الملخص
هدفت هذه الدراسة إلى تقييم واقع الأمن السيبراني وأثره على تكلفة الحوادث السيبرانية بمصرف الجمهورية (الإدارة العامة – طرابلس). تمثل مجتمع الدراسة في الموظفين المتخصصين بإدارات تقنية المعلومات، المخاطر، والمراجعة الداخلية. تم توزيع الاستبيان على عينة قصدية حجمها (28) مفردة، استُردَّ منها (24) استبياناً صالحة للتحليل الإحصائي، بنسبة استجابة بلغت (85.7%)، بينما بلغت نسبة الفاقد (14.3%). أظهرت النتائج وجود أثر ذي دلالة إحصائية لأداء إدارة المخاطر وعمليات المراجعة الداخلية في خفض التكاليف المترتبة على الحوادث الرقمية، كما بينت الدراسة أن كفاءة الجوانب المالية الموجهة للأمن السيبراني تقلل من نفقات التعافي بنسبة ملحوظة. توصي الدراسة بضرورة دمج معايير الأمن السيبراني ضمن خطط المراجعة الدورية، وزيادة المخصصات المالية لتحديث الدفاعات التقنية، وتعزيز التنسيق الإداري لتقليل زمن الاستجابة وتكلفة الضرر المحتملة.

الكلمات المفتاحية: مصرف الجمهورية، الأمن السيبراني، إدارة المخاطر، الآثار المالية، المراجعة الداخلية، تكلفة الحوادث السيبرانية.

1. مقدمة

يعتبر الأمن السيبراني أولوية قصوى للقطاع المالي ومجال اهتمام رئيسي للسلطات المالية، وهذا ليس بشكل مفاجئ نظرا لأن الحوادث السيبرانية تشكل خطورة كبيرة لاستقرار النظام المالي والاقتصاد العالمي (Crisanto, Umebara,2023)، فيمكن أن يؤدي الاختراق السيبراني إلى تكاليف لا يمكن التنبؤ بها لذلك؛ ليس من المستغرب أن ترى المحاسبين المحترفين يريدون من المؤسسات تخصيص الموارد التي تهدف إلى الحماية (Imene, 2020)، وتُعدّ تكاليف الاختراقات مؤشرًا على أداء الأمن السيبراني، إذ تقيس أثر الاختراق، وتُظهر مستوى الاستعداد، وتُبرهن على فعالية تدابير الأمن السيبراني، وبينما يُمكن للمؤسسات اختيار الاستثمار الاستباقي، بالتركيز على منع الاختراقات، هذا وتُعدّ التكاليف المرتفعة للحوادث غير مرغوب فيها لأنها تزيد من تكاليف العمل، ونظرًا لأن التكاليف المباشرة وتكاليف التعافي قد تختلف باختلاف قدرات المؤسسات على إدارة الحوادث، فمن المتوقع أن تتباين التكاليف الإجمالية للحوادث بين المؤسسات (Shaikh & Siponen, 2023).

وفي المراحل الأولى للخدمات المصرفية الرقمية، انصبّ التركيز الأساسي للأمن السيبراني على تأمين المعاملات الإلكترونية وحماية بيانات العملاء، إلا أن إدخال الخدمات المصرفية عبر الهاتف المحمول أضاف مستويات جديدة من التعقيد، مما استلزم تطبيق تدابير أساسية للأمن السيبراني، مثل جدران الحماية والتشفير(Reis et al., 2024) ، ونظراً لتزايد وتيرة الحوادث السيبرانية تبرز أهمية تحييد التهديدات والمخاطر في القطاع المالي في إطار الأمن السيبراني، ويشمل ذلك إرساء أمن النظام على جميع مستويات الأداء والإدارة، ويتطلب ذلك أيضا مراقبة مستمرة للمخاطر، بما في ذلك رفع مستوى إلمام الموظفين والعاملين بتكنولوجيا المعلومات من خلال دورات تدريبية متنوعة في مجال الأمن السيبراني وعمليات مراجعة سنوية، والامتثال للضوابط وفقًا لمعايير العام الحالي لضمان إدارة فعالة للمعلومات (Alimzhanova & Spanova, 2023).

ووفقًا لدراسة أجرتها شركة مكافحة الفيروسات، فإن القطاع المالي هو أكثر عرضة للهجمات الإلكترونية بمقدار 300 مرة من أي قطاع صناعي آخر، وذلك بسبب أن 81% من القطاع المالي يقوم بالاستعانة بمصادر خارجية لخدمات التكنولوجيا المالية عبر شركات التكنولوجيا المالية، مما يؤدي أيضًا إلى ارتفاع تكاليف تسرب البيانات للمؤسسات المالية (Najaf, 2020)، وكذلك لاعتماد القطاع المالي على التقنيات الرقمية والإنترنت في عملياته مما جعله هدفًا رئيسيًا لمجرمي الإنترنت، مما يؤكد أهمية وجود أطر عمل قوية للأمن السيبراني، ويشكل اعتماد أطر عمل مثل المعهد الوطني للمعايير والتكنولوجيا (NIST) وتكنولوجيا المعلومات (ITIL) وكوبيت (COBIT)، إذ هذه الأطر نهجًا منظمًا لإدارة مخاطر الأمن السيبراني، بما في ذلك تحديد الحوادث السيبرانية والحماية منها واكتشافها والاستجابة لها والتعافي منها (Oyeniyi et al., 2024).

ويعد تكامل إدارة مخاطر الأمن السيبراني وتخصيص الموارد اللازمة لتحديد المخاطر والتخفيف منها واستراتيجيات التعافي(Mizrak, 2023) ، ومن خلال تقييم نتائج مراجعة الأمن السيبراني، تستطيع المؤسسات قياس قدرتها على الحفاظ على نهج استباقي للأمن السيبراني بهدف تقليل الخسائر المالية الناجمة عن الحوادث السيبرانية (AL-Hawamleh , 2024). لذا جاءت هذه الدراسة لتوضيح أثر واقع الأمن السيبراني على تكلفة الحوادث السيبرانية.

2. الدراسات السابقة

- **دراسة (عبد الله، 2023) بعنوان: الأمن السيبراني في القطاع المالي مع الإشارة لواقع الأمن السيبراني في ليبيا.**

هدفت هذه الدراسة إلى التعرف على أهم التهديدات والمخاطر السيبرانية التي تواجه القطاع المالي، وكذلك التعرف على واقع الأمن السيبراني في ليبيا. وتم الاعتماد على المنهج الاستقرائي بأداتيه الوصف والتحليل؛ وذلك من خلال الرجوع إلى مختلف الأدبيات النظرية والتطبيقية والتقارير بهدف التعرف على الجوانب النظرية المتعلقة بالأمن السيبراني وما يحتويه من مخاطر وتهديدات للقطاع المالي، بالإضافة إلى إجراء المقابلات الشخصية مع ذوي الاختصاص وعلاقتهم المباشرة بموضوع الدراسة. وتوصلت الدراسة إلى

أن الدولة الليبية تمتلك بنية تحتية تقنية قابلة للتطوير وتغطي معظم مناطق ليبيا تساعد في إمكانية الاستثمار في الفضاء السيبراني، وإمكانية التحول للاقتصاد الرقمي، وكذلك إمكانية تطوير كافة الخدمات الحكومية المقدمة للمواطنين، كما توصلت إلى عدم وجود استراتيجية واضحة المعالم للاستثمار في الفضاء السيبراني بليبيا، ولا يوجد أطر قانونية تسند عليها الدولة الليبية فيما يخص الأمن السيبراني.

- **دراسة موسى(2022) بعنوان " العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة الدور المعدل لسمات منشاة المحاسبة والمراجعة: دراسة تجريبية"**

استهدفت إلى دراسة واختبار العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة، وكذلك دراسة أثر حجم منشاة المراجعة وطول فترة ارتباط المراجع بمنشاة عميله على العلاقة محل الدراسة. وتمثلت في دراسة تجريبية على عينة من مراجعي الحسابات بمكاتب المحاسبة والمراجعة المصرية وأعضاء هيئة التدريس ومعاونيهم بالجامعات المصرية. وخلصت الدراسة إلى وجود أثر إيجابي معنوي للإفصاح عن حوادث الأمن السيبراني على أتعاب المراجعة، كما خلصت أيضاً إلى تأثير معنوي لحجم منشاة المراجعة على العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة، بينما اتضح أنه لا يوجد تأثير معنوي لطول فترة ارتباط المراجع بمنشاة العميل على العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة.

- **دراسة (جغل، زقرير،2023) بعنوان الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي (التهديدات السيبرانية، اليات التحوط)**

هدف هذه الدراسة إلى تسليط الضوء على أهمية الأمن السيبراني ضمن استراتيجية التحول الرقمي للقطاع المالي لتوسيع نطاق الشمول المالي في القطاعات المالية للدول النامية. واعتمدت هذه الدراسة على الأسلوب الوصفي التحليلي وذلك بوصف المفاهيم الخاصة بهذه الدراسة، أما التحليلي من خلال تحليل مجموعة من المؤشرات والبيانات التي تخدم الدراسة. وتوصلت الدراسة إلى أن التحول الرقمي للقطاع المالي حقق إنجازا كبيرا في زيادة معدلات الشمول المالي، ولكن في نفس الوقت جلب مخاطر سيبرانية تفوق حجم الكوارث الطبيعية وأصبحت تهدد الاستقرار المالي والنظام المالي بأكمله مما أوجب التركيز والاهتمام بالأمن السيبراني في سياق المالي أكثر من أي وقت وذلك بإتباع آليات التحوط التي وضعتها الجهات المختصة لحماية النظام المالي ومكاسب الشمول المالي التي حققها التحول الرقمي من التهديدات السيبرانية، ولضمان الاستمرارية في مواصلة جهود الشمول في تحقيق أهداف التنمية المستدامة.

- **دراسة (حدود، 2025) بعنوان: فعالية الأمن السيبراني في حماية نظم المعلومات المحاسبية بالقطاع المصرفي الليبي (دراسة تطبيقية على المصارف التجارية الليبية العاملة في مدينة الزاوية)**

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. وأظهرت 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.

- **دراسة (Shaikh & Siponen, 2023) بعنوان: Organizational Learning from Cybersecurity Performance: Effects on Cybersecurity Investment Decisions.**

التعلم التنظيمي من أداء الأمن السيبراني: آثاره على قرارات الاستثمار في الأمن السيبراني

هدفت هذه الدراسة إلى دراسة جانبين حاسمين من أداء الأمن السيبراني هما تكاليف الاختراق ومصدر اكتشافه، كعوامل مؤثرة في قرارات الاستثمار في الأمن السيبراني، وتم استخدام التعلم التنظيمي لوضع نظرية حول كيفية تأثير التغذية الراجعة للأداء من هذين الجانبين من اختراقات الأمن السيبراني على

قرارات الاستثمار اللاحقة باستخدام بيانات على مستوى الشركات لـ 722 شركة في المملكة المتحدة، وتوصلت الدراسة إلى أن ارتفاع تكاليف الاختراق يزيد من احتمالية زيادة الاستثمارات في الأمن السيبراني، وتتعزز هذه العلاقة بشكل أكبر إذا اكتشف طرف ثالث الاختراق بدلاً من الشركة المعنية، وتوصلت كذلك إلى ضرورة أن تحلل الشركات جوانب أدائها في مجال الأمن السيبراني وأن تستخدمها كمعلومات مرجعية لقرارات الاستثمار، مما يجعل هذه القرارات قائمة على البيانات ومبنية على احتياجات الشركة الخاصة.

- **دراسة (Saleh,2023) بعنوان: The Effect of Assuring the Cloud User-Related Cybersecurity Risk Management Voluntary Disclosure on the Nonprofessional Investors' Judgments and Decisions: The Mediating Role of Perceived Management Assertions Reliability-An Experimental Study in Egypt.**

تأثير ضمان الإفصاح الطوعي لإدارة مخاطر الأمن السيبراني المتعلقة بالمستخدم السحابي على أحكام وقرارات المستثمرين غير المحترفين: الدور الوسيط لموثوقية تأكيدات الإدارة المدركة ـدراسة تجريبية في مصر.

هدفت هذه الدراسة إلى دراسة واختيار ما إذا كانت الموثوقية المتوقعة لتأكيدات إدارة مخاطر الأمن السيبراني يمكن أن تتوسط في العلاقة بين ضمان إدارة مخاطر الأمن السيبراني، وأحكام وقرارات المستثمرين غير المحترفين، من خلال إجراء تجربة لتصميم مختلط عاملي باستخدام عينة مكونة من 143 طالبا من طلاب الدراسات العليا في المحاسبة والمالية و إدارة الأعمال كبديل عن المستثمرين غير المحترفين وبشكل أكثر تحديدًا وجد أن تقرير ضمان إدارة مخاطر الأمن السيبراني يؤثر بشكل إيجابي على أحكام المستثمرين المصريين غير المحترفين حول جاذبية الاستثمار والقرارات المتعلقة بمبلغ الاستثمار، ويتم التوسط في هذا التأثير بالكامل من خلال تأثير ضمان إدارة مخاطر الأمن السيبراني على الموثوقية الملموسة لتأكيدات الإدارة المنشورة بالإضافة إلى ذلك، فإن التأثير المباشر لضمان إدارة مخاطر الأمن السيبراني على قرار مبلغ الاستثمار يكون أقوى بالنسبة للمستثمرين الذكور، بينما تلعب المؤهلات التعليمية للمشاركين دورًا مهما في التفاعل مع ضمان إدارة مخاطر الأمن السيبراني في التأثير على جاذبية الاستثمار ومبلغه. ومع ذلك، لا يؤثر النوع الاجتماعي بشكل كبير على العلاقة بين تقرير ضمان إدارة مخاطر الأمن السيبراني وجاذبية الاستثمار بشكل عام، تؤكد النتائج التي تدعمها المزيد من التحليلات على فائدة ضمان الإفصاح الطوعي لتقرير إدارة مخاطر الأمن السيبراني والذي له آثار عديدة على أصحاب المصلحة والإدارة والمراجعين وواضعي السياسات.

- **دراسة (Hassan et al., 2024) بعنوان: Cybersecurity in Banking: A Global Perspective with a Focus on Nigerian Practices**

الأمن السيبراني في القطاع المصرفي: منظور عالمي مع التركيز على الممارسات النيجيرية

تستكشف هذه الدراسة ممارسات الأمن السيبراني التي تتبعها المصارف النيجيرية، مع الأخذ في الاعتبار الأطر التنظيمية، وآليات الاستجابة للحوادث، والجهود التعاونية مع الجهات الدولية المعنية بالأمن السيبراني. يشمل هذا التحليل دراسات حالة توضح التهديدات والحوادث السيبرانية الواقعية في السياقين المصرفيين العالمي والنيجيري، بالإضافة إلى دراسة فعالية تدابير الأمن السيبراني التي تطبقها المصارف النيجيرية، علاوة على ذلك، تتعمق الدراسة في المبادرات التعاونية بين المصارف النيجيرية والهيئات التنظيمية ومنظمات الأمن السيبراني الدولية لتعزيز تبادل المعلومات، ومعلومات التهديدات، وآليات الدفاع الجماعي. وتوصلت الدراسة إلى أهمية التكيف المستمر والتعاون والابتكار في حماية نزاهة وموثوقية الأنظمة المصرفية، على الصعيدين العالمي والنيجيري.

• دراسة (Oyewole et al., 2024) بعنوان: **Cybersecurity risks in online banking: A detailed review and preventive strategies application**

مخاطر الأمن السيبراني في الخدمات المصرفية عبر الإنترنت: مراجعة تفصيلية وتطبيق استراتيجيات وقائية

هدفت هذه الدراسة إلى التعرف على واقع الأمن السيبراني الحالي، وتقييم فعالية الأطر القائمة، واقتراح تحسينات استراتيجية لتعزيز الدفاعات الرقمية، باستخدام منهجية تجمع بين مراجعة الأدبيات وتحليل حوادث الأمن السيبراني الأخيرة، تتعمق هذه الدراسة في تعقيدات التهديدات السيبرانية، والتداعيات المالية للاختراقات، ومدى متانة تدابير الأمن السيبراني الحالية في القطاع المصرفي. إذ يشمل نطاق هذه الدراسة دراسة شاملة لحوادث الأمن السيبراني الأخيرة، وتقييم الأثر المالي للهجمات السيبرانية، وتقييم فعالية أطر الأمن السيبراني الحالية، من خلال هذا البحث الأكاديمي وتوصلت الدراسة إلى الحاجة المُلحة لاستراتيجيات ديناميكية للأمن السيبراني تُدمج التقنيات المتقدمة، وتُعزز الامتثال التنظيمي، وتُرسخ ثقافة الوعي بالأمن السيبراني، كما توصلت الدراسة إلى ضرورة تبني القطاع المصرفي نهجًا شاملًا وقابلًا للتكيف في مجال الأمن السيبراني، مدعومًا باستثمارات استراتيجية في التكنولوجيا والتعليم والتعاون.

• دراسة (Johri & Kumar, 2025) بعنوان: **Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation**

استكشاف وعي العملاء بأمنهم السيبراني في المملكة العربية السعودية: دراسة في عصر التحول الرقمي المصرفي

تناولت هذه الدراسة وعي العملاء ورضاهم عن الأمن السيبراني في سياق التحول الرقمي للقطاع المصرفي في المملكة العربية السعودية. وتعتمد الدراسة على بيانات تم جمعها من 355 عميلًا مصرفيًا في المملكة. وقد تم تحليل ثلاثة جوانب رئيسية للأمن السيبراني، وهي الهجمات الإلكترونية والتصيد الاحتيالي والاختراق، من خلال أبعاد مختلفة، كما تم دراسة رضا العملاء عن خدمات الأمن السيبراني التي تقدمها المصارف وتوقعاتهم بشأن الدعم الفني والخدمات المتعلقة بالأمن السيبراني، وتم استخدم تحليل التباين الأحادي (ANOVA) وتحليل الانحدار الثنائي لدراسة تأثير الهجمات السيبرانية والتصيد الاحتيالي والاختراق وخدمات الأمن السيبراني والتوقعات المتعلقة بالوعي التقني بالأمن السيبراني على رضا العملاء. وتوصلت الدراسة إلى أن التحول الرقمي قد عزز القطاع المصرفي، وأن المستخدمين يستفيدون من الخدمات الإلكترونية. ومع ذلك، فإن زيادة وعي العملاء بأنشطة الهجمات السيبرانية والتصيد الاحتيالي والاختراق ستؤثر إيجابًا على رضاهم عن المعاملات الرقمية. كما كشفت النتائج أن العملاء بحاجة إلى مزيد من الاطمئنان بشأن جوانب الأمن من جانب المصرف، وأن على المصارف توفير برامج تدريبية منتظمة لحماية العملاء من الهجمات السيبرانية. وإذا ما أعدت المصارف إدارة أكثر أمانًا للأمن السيبراني، فسيكون من السهل تحقيق أهداف استدامتها على المدى الطويل.

• دراسة (Waliullah, 2025) بعنوان: **Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: a systematic literature review.**

تقييم تأثير تهديدات ومخاطر الأمن السيبراني على تبني ونمو الخدمات المصرفية الرقمية: مراجعة منهجية للأدبيات

هدفت هذه الدراسة إلى دراسة تأثير مخاطر الأمن السيبراني على أمن الخدمات المصرفية الرقمية، وانتشارها، والامتثال للوائح التنظيمية، وذلك من خلال مراجعة شاملة لـ 78 مقالة محكمة نُشرت بين عامي 2015 و2024. حيث تقيم هذه الدراسة بشكل نقدي أكثر التهديدات السيبرانية شيوعًا التي تستهدف منصات الخدمات المصرفية الرقمية، وفعالية التدابير الأمنية الحديثة، ودور الأطر التنظيمية في الحد من مخاطر الأمن السيبراني المالي. وتوصلت الدراسة إلى أن هجمات التصيد الاحتيالي والبرمجيات الخبيثة لا تزال أكثر التهديدات السيبرانية شيوعًا، مما يؤدي إلى خسائر مالية فادحة وفقدان ثقة المستهلكين، وانه يتم اعتماد المصادقة متعددة العوامل (MFA) والأمن البيومتري على نطاق واسع لمكافحة الوصول غير المصرح

به، بينما يوفر الكشف عن الاحتيال المدعوم بالذكاء الاصطناعي وتقنية سلسلة الكتل (البلوك تشين) حلولًا واعدة لتأمين المعاملات المالية. ومع ذلك، فإن دمج حلول التكنولوجيا المالية (FinTech) التابعة لجهات خارجية يُضيف مخاطر أمنية إضافية، مما يستلزم رقابة تنظيمية صارمة وبروتوكولات أمن سيبراني فعّالة.

- **دراسة (Aderinto & Faforiji, 2025) بعنوان: Cybersecurity Threats and Financial Performance of Listed Commercial Banks in Nigeria**
التهديدات السيبرانية والأداء المالي للبنوك التجارية المدرجة في البورصة النيجيرية

تناولت هذه الدراسة أثر التهديدات السيبرانية على الأداء المالي للمصارف التجارية المدرجة في البورصة النيجيرية، وركزت الدراسة تحديدًا على مدى تأثير الخسائر المالية الناجمة عن هذه التهديدات على ربحية السهم للبنوك التجارية المدرجة في نيجيريا، واعتمدت الدراسة منهجًا بحثيًا استرجاعيًا، وشمل مجتمع الدراسة جميع المصارف التجارية المدرجة في البورصة النيجيرية (14 مصرف). ومن هذا المجتمع، تم اختيار عينة عشوائية مكونة من عشرة مصارف تجارية مدرجة وجمعت بيانات الدراسة من البيانات المالية السنوية المدققة للمصارف المختارة، والتقارير السنوية لمؤسسة تأمين الودائع النيجيرية، وتقارير الاحتيال الصادرة عن نظام التسوية بين المصارف النيجيرية للفترة من 2012 إلى 2023، بالإضافة إلى التحليل الوصفي للبيانات باستخدام مقاييس النزعة المركزية ومقاييس التشتت، وتم اختبار الفرضيات باستخدام تحليل الانحدار الخطي. وأظهرت الدراسة أن الخسائر المالية الناجمة عن التهديدات السيبرانية تؤثر سلبًا على ربحية السهم للبنوك التجارية المدرجة في نيجيريا، وكذلك خلصت الدراسة إلى أن مخاطر الأمن السيبراني لا تقتصر على التحديات التقنية أو التشغيلية فحسب، بل تتعداها لتشمل مخاوف مالية بالغة الأهمية تؤثر بشكل مباشر على صافي الربح.

- من خلال النظر والتفحص في الدراسات السابقة تبين وجود عدد من الدراسات التي تناولت بعض من جزئيات موضوع الدراسة الحالية ومن جوانب مختلفة، غير إن الدراسة الحالية ستعمل على دراسة واقع الأمن السيبراني واثره على تكلفة الحوادث السيبرانية، والتي لم تتناولها الدراسات السابقة في البيئة الليبية –في حدود علم الباحثة-، ونظراً لندرة الدراسات السابقة فان نتائج الدراسة الحالية ستقدم إضافة علمية تساعد العديد من الأطراف المهتمة بموضوع الأمن السيبراني في تقييم فاعليته بشكل أفضل في تخفيض تكلفة الحوادث السيبرانية.

3. مشكلة الدراسة

تعتمد المؤسسات المعاصرة بشكل كبير على التكنولوجيا لحماية معلوماتها، وهي معرضة بشدة للهجوم من الداخل والخارج ونتيجة لذلك؛ أصبحت حماية المعلومات وحماية أصول المعلومات قضية رئيسية للمؤسسات وعملائها (Benqdara, 2024)، وذلك بسبب الحوادث السيبرانية التي تؤدي إلى تعطل تكنولوجيات المعلومات والاتصالات التي تدعم هذه الأنشطة، ويمكنها كذلك أن تؤدي إلى إساءة استخدام البيانات التي تعالجها هذه التقنيات أو تخزنها، ومما يزيد الأمر تعقيدًا حقيقة أن مشهد التهديدات السيبرانية لا يزال يتطور ويتزايد معقدة وسط التحول الرقمي المستمر، وزيادة الاعتماد على أطراف ثالثة، والتوترات الجيوسياسية. علاوة على ذلك، زادت تكلفة الحوادث السيبرانية بشكل مستمر وكبير على مر السنين (Crisanto, Umebara,2023).

ويعد الأمن القضية الأولى التي تواجه المحاسبين في عصر تكنولوجيا المعلومات، هذا ومن الواضح أنه مع زيادة استخدام المحاسبين للتكنولوجيا بشكل أكبر، سيصبح الاستثمار في الأمن السيبراني أمرا لا مقر منه وفي الواقع، وسيضطر بعض المحاسبين إلى التخصص في الأمن السيبراني خاصة بالنسبة لأغراض إعداد التقارير الرقمية (Imene, 2020). وحيث تُعدّ البيانات أصلًا استراتيجيًا، فإن الحوادث السيبرانية لديها القدرة على تعطيل العمليات، وتقويض ثقة العملاء، وإلحاق خسائر مالية، ومن خلال تبني إدارة مخاطر الأمن السيبراني، يمكن للمؤسسات تحديد نقاط الضعف في بنيتها التحتية الرقمية بشكل استباقي، وتقييم تعرضها للتهديدات، وتصميم استراتيجيات مرنة لمواجهة المخاطر المحتملة (Mizrak, 2023).

وكذلك تؤدي التكاليف المرتفعة للحوادث الأمنية السيبرانية إلى زيادة الاستثمارات في مجال الأمن السيبراني، مما يؤكد الحاجة إلى اتخاذ قرارات استثمارية قائمة على البيانات ومخصصة لكل مؤسسة (Shaikh & Siponen, 2023). وعلى الرغم من توصيات الهيئات التنظيمية ونتائج البحوث الحديثة (Johri & Kumar, 2025; Aderinto & Faforiji, 2025; Waliullah, 2025) في الآثار السلبية المترتبة على اختراقات الأمن السيبراني وضرورة الإفصاح عن ذلك للأطراف المعنية داخل وخارج المصرف لم يصدر ديوان المحاسبة أو مصرف ليبيا المركزي أية تعليمات لتوجيه المصارف بضرورة المحاسبة عن حوادث الأمن السيبراني لديها، كما إن مركز ليبيا في المؤشر العالمي للأمن السيبراني متدني، الأمر الذي يشير إلى وقوع حوادث الأمن السيبراني وبالتالي يجب المحاسبة عنها.

ومما سبق يمكن تلخيص مشكلة الدراسة في التساؤل الرئيس التالي:

- ما أثر واقع الأمن السيبراني على تكلفة الحوادث السيبرانية في مصرف الجمهورية؟

ومن التساؤل الرئيس تمت صياغة التساؤلات الفرعية التالية:

- ما أثر إدارة مخاطر الأمن السيبراني على تكلفة الحوادث السيبرانية؟
- ما أثر الآثار المالية للأمن السيبراني على تكلفة الحوادث السيبرانية؟
- ما أثر المراجعة الداخلية للأمن السيبراني على تكلفة الحوادث السيبرانية؟

4. أهداف الدراسة:

تهدف هذا الدراسة لتحقيق الهدف الرئيس التالي:

- دراسة أثر واقع الأمن السيبراني على تكلفة الحوادث السيبرانية في مصرف الجمهورية.

ولتحقيق هذا الهدف يستلزم تحقيق الأهداف التالية:

- بيان أثر أداء إدارة المخاطر على تكلفة الحوادث السيبرانية.
- تقييم أثر الجوانب المالية للأمن السيبراني على تكلفة الحوادث السيبرانية.
- تحليل أثر عمليات المراجعة الداخلية في الأمن السيبراني على تكلفة الحوادث السيبرانية.

5. فرضيات الدراسة: للإجابة عل تساؤل الدراسة، ولتحقيق أهدافها تمت صياغة الفرضيات التالية:

- هناك أثر ذو دلالة إحصائية لواقع الأمن السيبراني على تكلفة الحوادث السيبرانية في مصرف الجمهورية.

ومن الفرضية الرئيسة تمت صياغة الفرضيات الفرعية التالية:

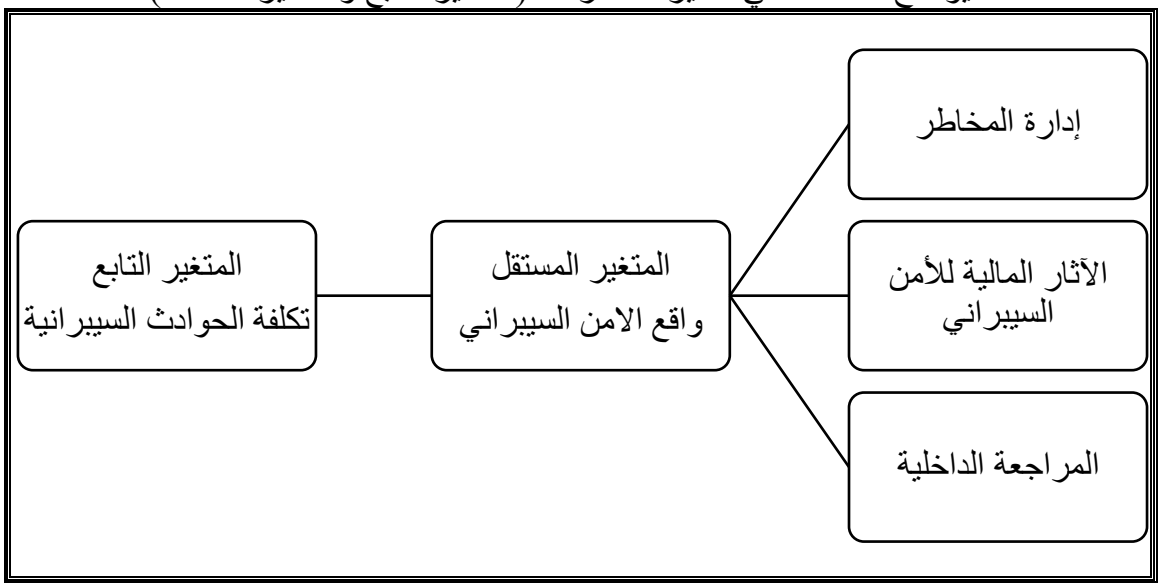
الفرضية الفرعية الأولى: هناك أثر ذو دلالة إحصائية لأداء إدارة المخاطر على تكلفة الحوادث السيبرانية.

الفرضية الفرعية الثانية: هناك أثر ذو دلالة إحصائية للجوانب المالية للأمن السيبراني على تكلفة الحوادث السيبرانية.

الفرضية الفرعية الثالثة: هناك أثر ذو دلالة إحصائية لعمليات المراجعة الداخلية في الأمن السيبراني على تكلفة الحوادث السيبرانية.

6. نموذج الدراسة:

يوضح الشكل التالي متغيرات الدراسة (المتغير التابع والمتغير المستقل).



7. أهمية الدراسة:

تنبع أهمية هذه الدراسة من تناولها لموضوع حديث في البيئة المصرفية الليبية يتمثل في الأمن السيبراني وتداعيات إهماله، خاصة في ظل الاعتماد المتزايد على الأنظمة الرقمية وتنامي تكلفة الحوادث السيبرانية. كما تسهم الدراسة في إبراز أهمية إدارة المخاطر والمراجعة وتوضيح الأثر المالي للأمن السيبراني من خلال الاستثمار الاستباقي في حماية الأنظمة للحد من الخسائر الناتجة عن الحوادث السيبرانية. وتكمن أهمية الدراسة أيضاً في توفير بيانات يمكن أن تستفيد منها إدارات المصارف عند وضع السياسات الداعمة للأمن السيبراني، وتعزيز قدرة المصارف على إدارة المخاطر بفعالية، بالإضافة إلى ندرة الدراسات التطبيقية التي تناولت هذا الموضوع في السياق الليبي، مما يمنحها قيمة علمية وميدانية في سدّ فجوة معرفية في هذا المجال.

8. منهجية الدراسة

في ضوء طبيعة مشكلة الدراسة ولتحقيق أهدافها اعتمدت الدراسة على المنهج الاستنباطي وذلك من خلال استقراء ومسح شامل لما يحتويه الفكر والأدب المحاسبي من مقالات ودوريات ورسائل علمية وكتب، وما يتم نشره على الشبكة العنكبوتية والتي ترتبط بموضوع الدراسة، لتكوين أساس نظري تبنى عليه الدراسة العملية، وفي الجانب العملي استخدم المنهج الاستقرائي وذلك من خلال تطوير صحيفة استبيان لجمع البيانات الأولية من عينة الدراسة للوصول إلى النتائج وصياغة التوصيات بناء على النتائج التي تم التوصل إليها.

9. حدود الدراسة:

الحدود المكانية: مصرف الجمهورية – الإدارة الرئيسية طرابلس.
الحدود الزمنية: تم توزيع وتجمع صحيفة الاستبيان خلال الفترة من 2025/12/11 – 2025/12/20.
الحدود الموضوعية: دراسة أثر واقع الأمن السيبراني على تكلفة الحوادث السيبرانية.

10. الإطار النظري للدراسة:

أولا: الأمن السيبراني وأبعاده:

يعرف الأمن السيبراني على انه الأدوات والسياسات ونماذج الأمن والاحتياطات الأمنية والاستراتيجيات وتكتيكات إدارة المخاطر والأنشطة وأفضل الممارسات والضمان والتقنيات المستخدمة لحماية الغلاف الجوي السيبراني والمؤسسات وبيانات المستخدم (Rawass,2019)، وتتمثل اغلب الحوادث السيبرانية في الاتي:(Alimzhanova & Spanova, 2023)

برامج الفدية: هي نوع من البرامج الضارة التي يمكنها بعد إصابة النظام تشفير الملفات أو حتى نظام التشغيل، وهذا يمنع الوصول إلى المستندات المهمة أو الجهاز نفسه. يُسمى هذا النوع من البرامج الخبيثة (ransom ware)لأن مُرتكب الهجوم غالبًا لا يفك تشفير النظام إلا بعد دفع الفدية، وقد أصبح هذا النوع من أكثر أنواع الهجمات شيوعًا وخطورة على المؤسسات المالية.

التصيد الاحتيالي: هجمات التصيد الاحتيالي شائعة تقريبًا مثل هجمات برامج الفدية، وتستخدم هذه الهجمات الهندسة الاجتماعية لخداع الموظفين ودفعهم إلى اتخاذ إجراءات تسمح بتثبيت البرامج الضارة على الشبكة ، ويُعدّ التصيّد الاحتيالي اليوم هجومًا اجتماعيًا رئيسيًا على المؤسسات، حيث يُشكّل أكثر من 75% من خروقات الأمن، ونظرًا لعدم وجود حلّ للأمن السيبراني قادر على صد هذه الأنواع من الهجمات بنسبة 100%، يجب تطبيق أو تعزيز التثقيف الحالي حول التصيّد الاحتيالي، إذ إنّ القضاء على عواقبها عملية طويلة ومكلفة وقد تُعرّض شبكة البنية التحتية بأكملها للخطر. لذلك؛ يجب على المؤسسة من حيث الحماية العمل كفريق واحد وفقًا للوائح المعمول بها. بالإضافة إلى ذلك، يجب إنشاء نظام للإبلاغ المنتظم عن الهجمات (على سبيل المثال، إرسال رسائل بريدية جماعية موحّدة، والإبلاغ من خلال المصادر المتاحة، وما إلى ذلك).

وتتيح أبعاد الأمن السيبراني فهم التهديدات المحتملة من إدارة المخاطر، الأثار المالية والمراجعة الداخلية للأمن السيبراني، وذلك من خلال تبني إطار شامل يتكامل فيه الوقاية، والكشف المبكر، والاستجابة السريعة، يمكننا تقليل المخاطر وتعزيز الثقة بين العملاء والمصرف والجهات التنظيمية. وسيتم تناولها كالاتي:

أ. إدارة المخاطر

تُعدّ إدارة مخاطر الأمن السيبراني نهجًا متعدد الجوانب يهدف إلى تحديد وتقييم وتخفيف المخاطر المحتملة التي تُشكّلها التهديدات السيبرانية على الأصول الرقمية للمؤسسة وبياناتها الحساسة وبنيتها التحتية الحيوية، وتتضمن هذه الاستراتيجية الاستباقية تقييمًا منهجيًا لنقاط الضعف والتهديدات المحتملة والتأثير المحتمل للاختراقات أو الهجمات، والهدف هو صياغة استراتيجيات تُقلّل من احتمالية وقوع الحوادث السيبرانية، وتُقلّل من الأضرار المحتملة، وتُمكّن من التعافي الفعال في حالة حدوث اختراق (Mizrak, 2023)، وقبل عملية تقييم مخاطر تكنولوجيا المعلومات، يجب على المؤسسات تحديد مستويات تقبلها للمخاطر ومستوى تحملها لها. ويُحدد مستوى تقبل المخاطر مدى المخاطر المقبولة لدى المؤسسة، ويحدد الحدود التي تستطيع المؤسسة من خلالها ممارسة أعمالها بأمان دون أي ضرر في سياق انتهاك السرية والتوافر والنزاهة. أما مستوى تحمل المخاطر فيحدد الانحرافات المقبولة عن مستويات المخاطر المقبولة(Alawonde, 2020)

ب. الأثار المالية

تُعد الاستثمارات المالية في الأمن السيبراني خطوة أولى أساسية نحو تحسين القدرات الأمنية، ويُحدث هذا أثراً مالياً وقائياً يحافظ على استمرارية الأعمال، بينما يؤدي تجاهله إلى تحمل تكاليف مرتفعة عند وقوع الحوادث السيبرانية، كما برزت الآثار المالية لا سيما في القطاعين المصرفي والمالي، كقضية مهمة لأصحاب المصلحة، حيث تركيز الاستثمارات على مبادرات الأمن السيبراني التي تُحقق أكبر قدر من خفض المخاطر (Shaikh & Siponen, 2023).

كما يُمثل التأمين السيبراني كأداةً لتخفيف وطأة هذه الهجمات المالية، بالتركيز على ضرورة صياغة سياسات تأمين سيبراني تُراعي المخاطر المتبقية ومشكلة الخطر المعنوي، إذ لا تهدف هذه الاستراتيجية إلى تغطية الأضرار المالية فحسب، بل تهدف أيضًا إلى تعزيز تطبيق بروتوكولات أمن سيبراني قوية بين

الأطراف المؤمَّن عليها. ولذلك؛ صار الإنفاق الاستباقي خياراً أكثر جدوى من تغطية الخسائر اللاحقة التي قد تشمل الغرامات، وتعويضات العملاء، وتراجع السمعة السوقية. (Oyewole et al., 2024).

ج. المراجعة الداخلية

يُعدّ إجراء عمليات مراجعة منتظمة للأمن السيبراني أساسيًا للحفاظ على وضع أمني سيبراني قوي. ويؤكد هذا على أهمية إجراء عمليات مراجعة مجدولة بشكل منهجي لتقييم مدى التزام المؤسسة بالسياسات والمتطلبات التنظيمية وأفضل ممارسات الأمن السيبراني. كما يوفر تكرار عمليات المراجعة رؤى ثاقبة حول التزام المؤسسة بالمراقبة المستمرة لضوابط الأمن السيبراني لديها (AL-Hawamleh , 2024).

وفي 24 أبريل 2017 أصدر المعهد الأمريكي للمحاسبين القانونيينAICPA إطار إعداد تقارير شهادات الأمن السيبراني SOC، الذي يتضمن ثلاثة أقسام وهي وصف الإدارة لبرنامج إدارة مخاطر الأمن السيبراني الخاص بها، وتأكيد الإدارة على الوصف، وفعالية الضوابط لتحقيق أهداف الأمن السيبراني، والقسم الأخير هو راي المراجع حول الوصف وفعالية أدوات الرقابة. والذي يهدف إلى توسيع نطاق الإبلاغ عن المخاطر السيبرانية لتلبية حاجات السوق إلى التوحيد وزيادة شفافية أصحاب المصلحة (AL-Hawamleh , 2024)

ثانياً: تكلفة الحوادث السيبرانية

يُعرَّف الحادث السيبراني بأنه حدث يؤدي إلى الوصول غير المصرح به إلى البيانات أو التطبيقات أو الخدمات أو الشبكات أو الأجهزة عن طريق تجاوز آليات الأمان الأساسية لها. ومن أمثلة هذه الحوادث: اختراقات البيانات، وهجمات برامج الفدية، وهجمات البرامج الضارة، والتصيد الاحتيالي (Shaikh & Siponen, 2023).

ويمكن تقسيم تكاليف الحوادث إلى تكاليف مباشرة أو قصيرة الأجل، وتكاليف التعافي، وتكاليف طويلة الأجل. تشمل التكاليف المباشرة الخسائر أو الأضرار المباشرة التي تلحق بالأصول والبيانات والملكية الفكرية، بالإضافة إلى انقطاع استمرارية الأعمال عندما يتعذر على الموظفين القيام بأنشطتهم المعتادة، ويتعذر على العملاء الاستفادة من الخدمات. أما تكاليف التعافي فتشمل الموارد التي تخصصها إدارة تقنية المعلومات لإدارة الحوادث، واستعادة النسخ الاحتياطية، واستعادة استمرارية الأعمال، وتكاليف التحقيق في الحادث والتواصل مع الجهات المعنية. وتشمل التكاليف طويلة الأجل الإضرار بالسمعة، وخسارة الأعمال، وخسائر السوق، وفقدان العملاء الحاليين والمحتملين، وتكاليف معالجة شكاوى العملاء وتعويضهم (Shaikh & Siponen, 2023).

ثالثاً: أثر واقع الأمن السيبراني على تكلفة الحوادث السيبرانية

تاريخيًا، عانى القطاع المالي من حوادث أمنية سيبرانية متنوعة، بدءًا من اختراق البيانات ووصولًا إلى هجمات برامج الفدية، مما أدى إلى خسائر مالية وإضرار بالسمعة. ومع استمرار تطور التهديدات وتعقيدها، أثبتت التدابير الأمنية التقليدية عدم كفايتها لضمان حماية فعّالة. وبالتالي، ثمة حاجة ملحة لمواجهة تحديات الأمن السيبراني الفريدة التي تواجه القطاع المصرفي، والتي تشمل الامتثال التنظيمي، وحماية بيانات العملاء، ومتانة البنية التحتية المالية (Dey, 2022).

إذ يمكن لجودة الاستجابة للحوادث أن تخفض أو ترفع تكاليف الاختراق (واقع الأمن السيبراني). وبالتالي، فبالإضافة إلى نوع الاختراق، تُعد تكاليفه أيضًا دالةً لقدرات المؤسسة على الاستجابة للحوادث. لذلك، يُتوقع أن تكون قرارات استثمار المؤسسة في مجال الأمن السيبراني استجابةً للاختراقات الموقوفة أكثر دقةً، إذ لا تستند فقط إلى شدة الاختراق، بل أيضًا إلى تقييم المؤسسة لفعالية الاستجابة للحوادث (Shaikh & Siponen, 2023). كما تُقدّم نتائج هذه المراجعة نظرة شاملة على فعالية تدابير الأمن السيبراني، وتحديد نقاط الضعف المحتملة، والحالة العامة للامتثال (AL-Hawamleh , 2024).

علاوة على ذلك، مع توسع الخدمات المالية في نطاقها الرقمي، أصبحت إدارة مخاطر الأمن السيبراني مؤشرًا رئيسيًا للأداء. ويتعين على المصارف تحقيق التوازن بين هدفين رئيسيين: تعزيز الأمن السيبراني، وتدريب الموظفين، والتحديثات التقنية، وآليات الاستجابة للحوادث. كما تؤثر التكاليف المتزايدة لتطبيق

أطر الأمن السيبراني، وتدريب الموظفين، والتحديثات التقنية، وآليات الاستجابة للحوادث، على صافي أرباح المصارف التجارية. ورغم أن هذه التكاليف ضرورية في كثير من الأحيان لتجنب خسائر مالية أكبر، إلا أنها تُشكل ضغطًا إضافيًا على الميزانيات التشغيلية (Aderinto & Faforiji, 2025).

11- الدراسة الميدانية:

- **مجتمع الدراسة:** يُشير مجتمع الدراسة إلى المجموعة الكلية والشاملة من العناصر أو الأفراد الذين تشملهم خصائص الظاهرة محل البحث، والتي تسعى الباحثة إلى تعميم النتائج النهائية عليهم. وفي هذه الدراسة، يتمثل المجتمع في موظفي مصرف الجمهورية – الإدارة العامة بطرابلس، باعتبارهم الفئة المعنية مباشرة بأبعاد المشكلة البحثية وأهدافها.

- **عينة الدراسة:** تم اختيار عينة ممثلة من مجتمع الدراسة وفق أسس منهجية تضمن المحاكاة الدقيقة لخصائص المجتمع الأصلي وتمثيله تمثيلاً صادقاً وهي عينة قصدية وقد اقتصرت هذه العينة على موظفي مصرف الجمهورية - الإدارة العامة بطرابلس ، لضمان الحصول على بيانات موضوعية تعكس واقع المتغيرات المدروسة، مما يساهم في إضفاء الصبغة العلمية والموثوقية على النتائج وإمكانية تعميمها لاحقاً.

- **إجراءات جمع البيانات الميدانية**: لتحقيق أهداف الدراسة الميدانية، اعتمدت الباحثة على "الاستبيان" كأداة رئيسية لجمع البيانات من موظفي مصرف الجمهورية - الإدارة العامة بطرابلس. وقد مرت عملية جمع البيانات بالخطوات الإجرائية التالية:

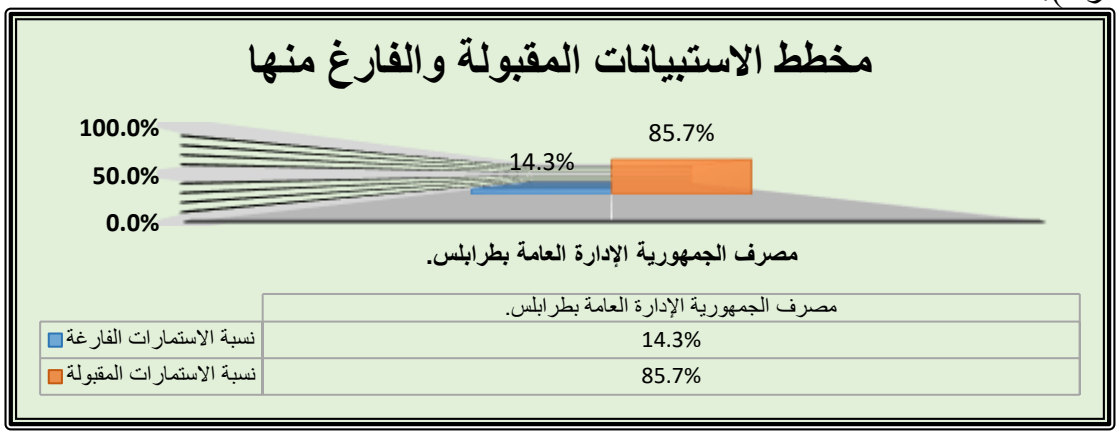
- حجم العينة الموزعة: تم توزيع (28) استبانة على الموظفين المستهدفين ضمن عينة الدراسة.
- الاستبانات المسترجعة: تم استلام (24) استبانة من إجمالي النسخ التي جرى توزيعها.
- نسبة الاستجابة: بلغت نسبة الاسترداد (85.7%)، وهي نسبة مرتفعة وممتازة وفقاً للمعايير العلمية، مما يؤكد تفاعل المشاركين وجدية التعاطي مع موضوع الدراسة.
- الاستبانات الصالحة للتحليل: خضعت الاستبانات المسترجعة لعملية فحص وتدقيق دقيق؛ وتبين أن جميعها (24 استبانة) مستوفية للشروط ومكتملة البيانات، مما جعلها صالحة تماماً للمعالجة الإحصائية دون استبعاد أي نسخة.

ت	البيان	الاستبيانات الموزعة	الاستبيانات الفارغة	الاستبيانات المقبولة	نسبة الاستبيانات الفارغة	نسبة الاستبيانات المقبولة
1	مصرف الجمهورية الإدارة العامة بطرابلس	28	04	24	%14.3	%85.7
	أجمالي الاستبيانات لعينة البحث	28	04	24	%14.3	%85.7

تُشير المعطيات الميدانية إلى أن عملية جمع البيانات حققت كفاءة عالية؛ حيث بلغت نسبة الاستمارات المسترجعة والصالحة للتحليل الإحصائي 85.7% من إجمالي حجم العينة المستهدفة. ويتمثل ذلك في استرجاع (24)استبانة مكتملة من أصل (28)استبانة تم توزيعها على موظفي مصرف الجمهورية – الإدارة العامة بطرابلس.

تُعد هذه الاستجابة مرتفعة جداً وفق المعايير الإحصائية، مما يعزز من صدق النتائج وقدرتها على تمثيل مجتمع الدراسة بشكل دقيق، ويقلل من هامش الخطأ الناتج عن عدم الاستجابة.

ويوضح الشكل رقم **(1)**أدناه التوزيع النسبي للاستبيانات الموزعة، والمقبولة، والفارغة (أو غير المستردة).



الشكل رقم (1)التوزيع النسبي للاستبيانات الموزعة، والمقبولة، والفارغة (أو غير المستردة)

أداة جمع البيانات (الاستبيان):

"اعتمدت الدراسة على الاستبيان كأداة رئيسة لجمع البيانات من أفراد العينة المستهدفة. وقد صُممت الأداة في صورتها النهائية لتشمل عدة أقسام رئيسة على النحو الآتي:

القسم الأول: البيانات الشخصية والوظيفية: ويشتمل على (4) فقرات تهدف إلى تحديد الخصائص الديموغرافية للمشاركين، وهي: المؤهل العلمي، عدد سنوات الخبرة، التخصص، والمركز الوظيفي.

القسم الثاني: محاور الدراسة الميدانية: وتضمن (28) عبارة موزعة على محورين أساسيين لقياس متغيرات البحث:

المحور الأول (واقع الأمن السيبراني): ويتكون من (21) عبارة موزعة بالتساوي على ثلاثة أبعاد فرعية هي: إدارة مخاطر الأمن السيبراني (7 عبارات)، الآثار المالية للأمن السيبراني (7 عبارات)، ومراجعة الأمن السيبراني (7 عبارات).

المحور الثاني (تكلفة الحوادث السيبرانية): ويتكون من (7) عبارات تهدف إلى قياس الخسائر المالية المباشرة وغير المباشرة، وتكاليف إصلاح الأنظمة، والآثار المترتبة على سمعة المصرف.

صدق وثبات أداة الدراسة:

يُعد التحقق من الخصائص السيكومترية (الصدق والثبات) خطوة جوهرية لضمان جودة النتائج وقابلية تعميمها. وتتخلص هذه الإجراءات فيما يلي:

صدق الأداة: يعكس قدرة الاستبيان على قياس المتغيرات المرتبطة بواقع الأمن السيبراني وتكلفته بدقة .

ثبات الأداة: يشير إلى مدى اتساق واستقرار استجابات أفراد العينة عند تكرار التطبيق، مما يؤكد خلو الأداة من الأخطاء العشوائية وضمان موثوقية البيانات المستخلصة.

اختبار الثبات بطريقة التجزئة النصفية (معامل سبيرومان براون):

لتحقيق موثوقية النتائج، استُخدم أسلوب التجزئة النصفية عبر حساب معامل ارتباط "بيرسون" بين الفقرات الزوجية والفردية، ثم تصحيحه باستخدام معادلة "سبيرمان-براون" لتقدير ثبات الأداة ككل.

توضح نتائج الجدول رقم (2) أن كافة معاملات الثبات تجاوزت الحد الأدنى المقبول (0.60)، مما يؤكد تمتع الاستبانة بمستوى عالٍ من الاتساق والاستقرار، وصلاحيتها التامة للتحليل الإحصائي واستخلاص النتائج.

م	المحاور	عدد الفقرات	معامل الارتباط قبل التصحيح	معامل سبير ومان براون	النتيجة
1	**واقع الأمن السيبراني**	21	0.814	0.897	ثبات مرتفع
2	**تكلفة الحوادث السيبرانية**	7	0.786	0.880	ثبات مرتفع
	الاستبيان ككل	28	**0.842**	**0.914**	**ثبات ممتاز**

المصدر: إعداد الباحثة اعتماداً على مخرجات spss

تُظهر النتائج الواردة في الجدول رقم (2) مؤشرات إحصائية قوية حول ثبات أداة الدراسة (الاستبيان)، حيث بلغت قيم معامل سبيرمان-براون (Spearman-Brown) بعد التصحيح للمحاور الرئيسة قيمًا تتراوح ما بين (0.880) و (0.897)، بينما سجلت الأداة ككل معامل ثبات مرتفعًا جدًا بلغ .(0.914)
وتُعد هذه القيم مؤشرًا جوهريًا على الاتساق الداخلي العالي بين فقرات الاستبانة البالغ عددها (28) فقرة.
ومن الناحية الإحصائية، فإن تجاوز هذه المعاملات للحد الأدنى المقبول في البحوث الإدارية والمالية (0.60) يعكس استقرار الأداة وصلاحيتها العالية لجمع البيانات من عينة الدراسة المتمثلة في الكوادر القيادية والتقنية بالمصارف التجارية الليبية.
وبناءً على هذه النتائج، يطمئن الباحثة إلى أن الأداة قادرة على قياس المتغيرات المستهدفة (واقع الأمن السيبراني وتكاليف حوادثه) بمستوى منخفض من الخطأ العشوائي، مما يضفي صفة الموثوقية (Reliability)على البيانات الميدانية المستخلصة ويجعلها ركيزة صلبة لبناء الاستنتاجات العلمية اللاحقة وتعميم نتائج البحث في سياق القطاع المصرفي".

اختبار الثبات بطريقة الفا كرو نباخ Alpha Cronbach's:

يشير الثبات إلى مدى موثوقية المقياس وقدرته على تحقيق نتائج متماثلة ومستقرة إذا تم تكرار عملية القياس في ظروف مماثلة.
يوضح الجدول رقم (3) نتائج تحليل الثبات للأبعاد الرئيسة لاستبانة الدراسة، وذلك بالاعتماد على طريقة التجزئة النصفية المعدلة باستخدام معادلة سبيرمان-براون للتصحيح، وهي طريقة تُستخدم لتقييم الاتساق الداخلي لفقرات الأداة، تماماً كمعامل ألفا كرونباخ، حيث يُعتبر معامل الثبات مقبولاً إذا كان أكبر من (0.60)وضعيفاً إذا كان أقل من ذلك.

الجدول رقم (3) نتائج اختبار الثبات (معامل ألفا كرو نباخ) لمحاور الاستبيان

م	المحاور	عدد الفقرات	معامل الثبات (قيمة معامل ألفا كرو نباخ)	النتيجة
1	**واقع الأمن السيبراني**	21	**0.886**	ثبات مرتفع
2	**تكلفة الحوادث السيبرانية**	7	**0.854**	ثبات مرتفع
	الاستبيان ككل	28	0.902	**ثبات ممتاز**

المصدر: إعداد الباحثة اعتماداً على مخرجات spss

"لتحقيق مزيد من التحقق حول جودة الأداة، استُخدم معامل ألفا كرونباخ (Cronbach's Alpha)لقياس مستوى الاتساق الداخلي بين فقرات الاستبيان. أظهرت النتائج الموضحة في الجدول رقم (3) أن معامل الثبات العام للأداة بلغ (0.902)، وهي قيمة مرتفعة جداً تعكس ترابطاً وثيقاً بين الفقرات.
وعلى مستوى المحاور، سجل محور 'واقع الأمن السيبراني' قيمة (0.886)، بينما سجل محور 'تكلفة الحوادث السيبرانية' قيمة (0.854). وبالنظر إلى أن هذه القيم تتجاوز وبشكل ملحوظ عتبة القبول الإحصائي المتعارف عليها علمياً، فإن ذلك يؤكد أن الاستبيان يتمتع بدرجة عالية من الموثوقية والاعتمادية(Reliability) ، مما يجعل البيانات المستخلصة منه صالحة لإجراء الاختبارات الإحصائية الاستدلالية اللازمة للإجابة على تساؤلات الدراسة واختبار فرضياتها.

اختبار الصدق:

اختبار صدق الاستبانة يعني التأكد من أنها سوف تقيس ما أعدت لقياسه، كما يقصد بالصدق "شمول الاستبانة لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها ومفرداتها من ناحية ثانية، بحيث تكون مفهومة لكل من يستخدمها، وقد قامت الباحثة بالتأكيد من صدق أداة البحث كما يلي:

صدق فقرات الاستبانة:

تم التأكد من صدق فقرات الاستبانة بطريقتين وهما:

1 الصدق الظاهري للأداة البحث (صدق المحكمين):

للتأكد من صدق الأداة، اعتمد الباحثة منهجية صدق المحتوى تم ذلك عن طريق عرض الأداة على مجموعة من المحكمين المتخصصين في مجال المحاسبة وكان الهدف من هذا التحكيم هو تحديد ما إذا كانت الفقرات تقيس الأداء المطلوب بالفعل ومدى صلة فقرات المقياس بالمتغير الذي يسعى الباحثة لقياسه والحكم على صياغة الفقرات، درجة وضوحها، ومناسبتها للمجالات التي تتضمنها الأداة.

قامت الباحثة بعد ذلك بمراجعة الأداة بناءً على ملاحظات وتوجيهات المحكمين، حيث تضمن ذلك حذف بعض العبارات وإضافة عبارات أخرى لتعزيز جودة المقياس.

2 صدق الاتساق الداخلي والبنائي لمحاور البحث:

تم التحقق من الاتساق الداخلي لعبارات كل عامل (أو محور) ضمن المقياس، وذلك بهدف التأكد من أن جميع الفقرات التي تنتمي إلى بُعد واحد تقيس الشيء نفسه بفعالية.

جدول رقم (4) نتائج اختبارات الصدق لمحاور الاستبيان

م	المحاور	معامل الصدق البنائي (الارتباط مع الدرجة الكلية للاستبيان)	معامل الصدق الداخلي (الاتساق الداخلي) الجذر التربيعي لمعامل ألفا كرو نباخ	مستوى الدلالة	النتيجة
1	واقع الأمن السيبراني	0.892	0.941	0.000	دال أحصائيا
2	تكلفة الحوادث السيبرانية	0.845	0.924	0.000	دال أحصائيا
	الاستبيان ككل	---	0.950	دال أحصائيا	

**** Correlation is significant at the 0.01 level (2-tailed).**

المصدر: إعداد الباحثة اعتماداً على مخرجات spss

للتأكد من كفاءة الأداة في قياس ما وضعت لقياسه، قامت الباحثة باختبار الصدق الداخلي (Internal Validity)عن طريق حساب الجذر التربيعي لمعامل ألفا كرونباخ، حيث سجلت المحاور قيم صدق مرتفعة جداً بلغت (0.941) لمحور واقع الأمن السيبراني، و (0.924) لمحور تكلفة الحوادث. كما تم حساب الصدق البنائي عبر قياس معامل ارتباط بيرسون بين درجة كل محور والدرجة الكلية للاستبيان، وأظهرت النتائج ارتباطاً قوياً وموجباً عند مستوى دلالة (0.000)، مما يؤكد تجانس فقرات الأداة وقدرتها العالية على التعبير عن الأبعاد الأساسية للدراسة في بيئة المصارف التجارية الليبية. إن هذه المؤشرات مجتمعة (الصدق والثبات) تمنح الدراسة صبغة الموثوقية العلمية اللازمة للنشر والتعميم.

- **اختبار التوزيع الطبيعي Normality Test:**

للتأكد من ملاءمة البيانات للتحليل الإحصائي البارامتري (المعلمي)، تم استخدام اختبار **كولمجروف-سمرنوف (One-Sample Kolmogorov-Smirnov Test)** لمعرفة ما إذا كانت متغيرات الدراسة تتبع التوزيع الطبيعي. يُعد هذا الاختبار شرطاً أساسياً لتطبيق العديد من الاختبارات الإحصائية المتقدمة

(البارامترية) المستخدمة في اختبار الفرضيات، يوضح الجدول رقم **(5)** نتائج هذا الاختبار، حيث تشير النتائج إلى أن:

م	المحاور	القيمة الاحصائية	درجة الحرية	الدلالة المعنوية
1	**واقع الأمن السيبراني**	0.125	23	0.200*
2	**تكلفة الحوادث السيبرانية**	0.142	23	0.185
	الاستبيان ككل	**0.118**	**23**	**0.200***

المصدر: إعداد الباحثة اعتماداً على مخرجات spss

*** This is a lower bound of the true significance.**
a. Lilliefors Significance Correction

تُظهر نتائج الجدول رقم (5) أن جميع قيم الدلالة المعنوية (Sig) لمحاور الدراسة وللأداة ككل جاءت أكبر من مستوى الدلالة المعتمد (0.05). وبناءً على ذلك، يتم قبول الفرضية الصفرية التي تشير إلى أن بيانات الدراسة تتبع التوزيع الطبيعي ويعني هذا التحقق المنهجي أن البيانات المستقاة من المسؤولين والمختصين في مصرف الجمهورية تتسم بالتجانس والاعتدالية، مما يمنح الباحثة المسوغ العلمي لاستخدام الاختبارات الإحصائية المعلمية(Parametric Tests) ، مثل معامل ارتباط بيرسون وتحليل الانحدار البسيط والمتعدد، لاختبار فرضيات الدراسة واستخلاص النتائج بدقة وموثوقية عالية.

❖ خصائص عينة البحث:

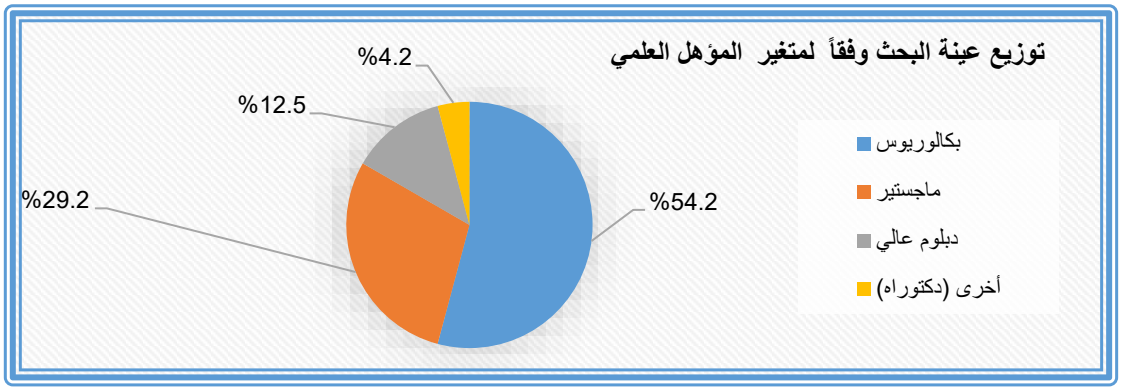
1 خصائص عينة البحث وفقاً لنوع وفقاً للمؤهل العلمي:

الجدول رقم (6) خصائص عينة البحث وفقاً لنوع وفقاً للمؤهل العلمي

وفقاً للمؤهل العلمي	التكرار	النسبة	الترتيب حسب التوافر
بكالوريوس	13	%54.2	1
ماجستير	7	%29.2	2
دبلوم عالي	3	%12.5	3
أخرى (دكتوراه)	1	%4.1	4
الإجمالي	**24**	**%100**	-

من إعداد الباحثة اعتماداً على مخرجات برنامج (SPSS)

يُلاحظ من النتائج الواردة في الجدول رقم (6) أن المؤهل الجامعي (بكالوريوس) هو الأكثر تكراراً بين أفراد العينة بنسبة بلغت (54.2%)، يليه حملة شهادة الماجستير بنسبة (29.2%). وتعكس هذه المؤشرات المستوى التعليمي العالي للفئة المستهدفة من مديري إدارات تقنية المعلومات، والشؤون المالية، والمراجعة والامتثال في المصارف الليبية.
إن تركز أغلب أفراد العينة في فئة الدراسات الجامعية والعليا (بإجمالي نسب تزيد عن 83%) يعزز من موثوقية الاستجابات المقدمة؛ حيث يمتلك هؤلاء المشاركون الخلفية العلمية الكافية لاستيعاب متطلبات الأمن السيبراني وتقدير التكاليف المرتبطة بالحوادث السيبرانية بدقة. كما أن تنوع المؤهلات العلمية يضمن شمولية الآراء المطروحة حول واقع الأمن السيبراني في القطاع المصرفي".



شكل رقم (2) توزيع عينة البحث وفقاً للمؤهل العلمي.

2. خصائص عينة البحث وفقاً لسنوات الخبرة.

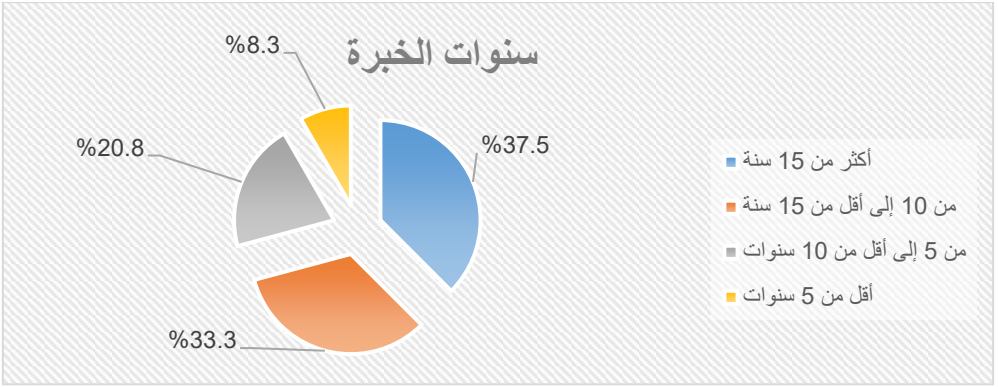
الجدول رقم (7) خصائص عينة سنوات الخبرة

سنوات الخبرة	التكرار	النسبة	الترتيب حسب التوافر
أكثر من 15 سنة	9	%37.5	1
من 10 إلى أقل من 15 سنة	8	%33.3	2
من 5 إلى أقل من 10 سنوات	5	%20.8	3
أقل من 5 سنوات	2	%8.4	4
الإجمالي	**24**	**%100**	-

من إعداد الباحثة اعتماداً على مخرجات برنامج (SPSS)

تُظهر نتائج الجدول رقم (7) أن الفئة الأكثر تمثيلاً في عينة الدراسة هي فئة ذوي الخبرة الطويلة (أكثر من 15 سنة) بنسبة بلغت (37.5%)، تليها مباشرة الفئة من (10 إلى أقل من 15 سنة) بنسبة (33.3%). وتعد هذه النتيجة منطقية نظراً لكون الدراسة تستهدف مستويات إدارية وقيادية عليا، مثل أعضاء مجلس الإدارة ومديري إدارات تقنية المعلومات والمراجعة.

إن استحواذ ذوي الخبرة التي تزيد عن 10 سنوات على أكثر من (70%) من إجمالي العينة يمنح البحث وزناً علمياً كبيراً؛ حيث يمتلك هؤلاء المشاركون معرفة تراكمية مباشرة بالواقع العملي للمصارف، وقدرة عالية على استقصاء وتقييم أثر واقع الأمن السيبراني وتكاليف الحوادث المرتبطة به بدقة وموضوعية. هذا المزيج من الخبرات يعزز من جودة البيانات الميدانية المستخلصة ويدعم صحة الاستنتاجات التي ستتوصل إليها الدراسة.



شكل رقم (3) توزيع عينة البحث وفقاً لسنوات الخبرة.

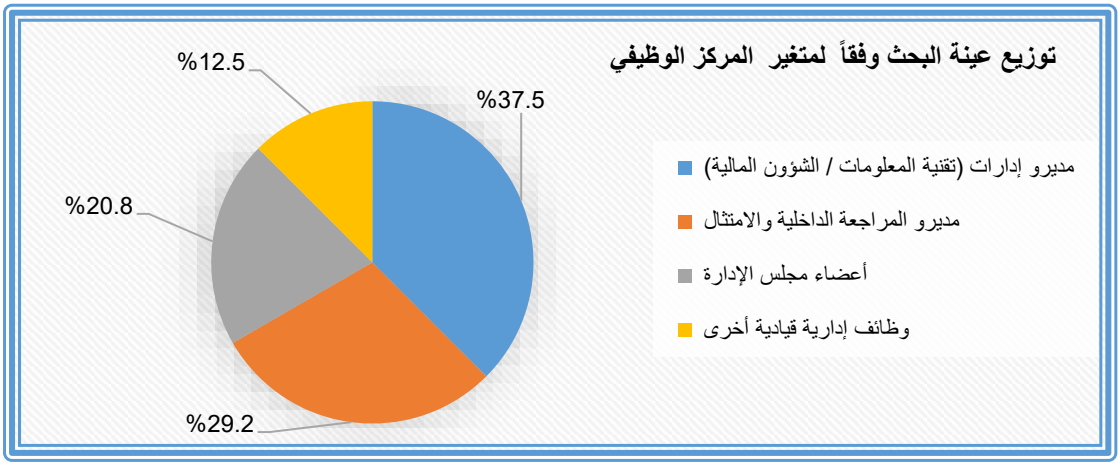
3. خصائص عينة البحث وفقاً للمركز الوظيفي.

الجدول رقم (8) خصائص عينة المركز الوظيفي

المركز الوظيفي	التكرار	النسبة	الترتيب حسب التوافر
مديرو إدارات (تقنية المعلومات / الشؤون المالية)	9	%37.5	1
مديرو المراجعة الداخلية والامتثال	7	%29.2	2
أعضاء مجلس الإدارة	5	%20.8	3
وظائف إدارية قيادية أخرى	3	%12.5	4
الإجمالي	**24**	**%100**	-

من إعداد الباحثة اعتماداً على مخرجات برنامج (SPSS)

يستعرض الجدول رقم (8) التنوع في المراكز الوظيفية لعينة الدراسة، حيث شكل مديرو الإدارات (تقنية المعلومات والمالية) النسبة الأكبر بواقع (37.5%)، يليهم مديرو المراجعة والامتثال بنسبة (29.2%)، ثم أعضاء مجلس الإدارة بنسبة.(20.8%) ويعكس هذا التوزيع دقة اختيار العينة؛ إذ شملت الدراسة صناع القرار والمسؤولين المباشرين عن وضع سياسات الأمن السيبراني ومراقبة تكاليف الحوادث الناتجة عنها في المصارف التجارية الليبية. إن إشراك هذه النخب الوظيفية يضمن الحصول على بيانات نوعية تتسم بالعمق الفني والإداري، مما يسهم في الوصول إلى نتائج واقعية حول أثر الأمن السيبراني على الكفاءة المالية والتشغيلية للمصارف.



شكل رقم (4) توزيع عينة البحث وفقاً للمركز الوظيفي.

4. خصائص عينة البحث وفقاً للتخصص.

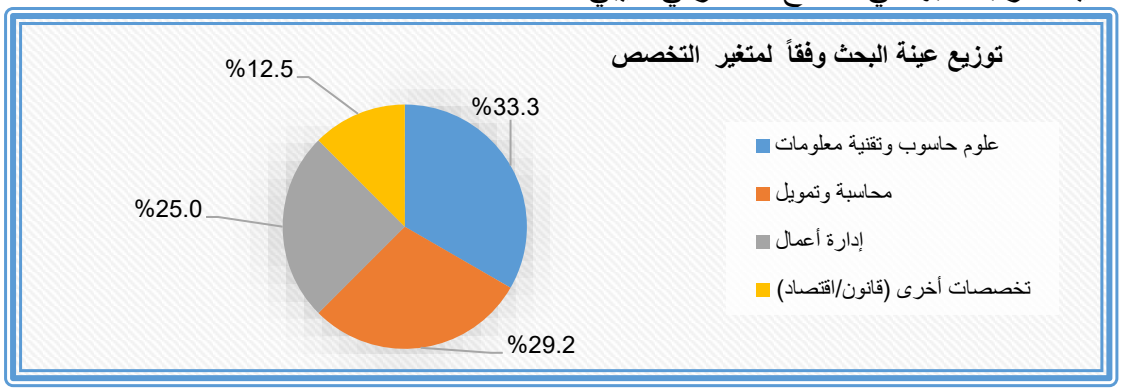
الجدول رقم (9) خصائص عينة التخصص العلمي

التخصص العلمي	التكرار	النسبة	الترتيب حسب التوافر
علوم حاسوب وتقنية معلومات	8	%33.3	1
محاسبة وتمويل	7	%29.2	2
إدارة أعمال	6	%25.0	3
تخصصات أخرى (قانون/اقتصاد)	3	%12.5	4
الإجمالي	**24**	**%100**	-

من إعداد الباحثة اعتماداً على مخرجات برنامج (SPSS)

تُظهر نتائج الجدول رقم (9) تنوعاً تخصصياً يتسق مع طبيعة موضوع البحث؛ حيث جاء تخصص 'علوم الحاسوب وتقنية المعلومات' في المرتبة الأولى بنسبة (33.3%)، يليه تخصص 'المحاسبة والتمويل' بنسبة (29.2%)، ثم 'إدارة الأعمال' بنسبة.(25%) إن هذا التباين المدروس في التخصصات العلمية بين أفراد

العينة يخدم أهداف الدراسة بشكل مباشر ؛ فبينما يغطي المتخصصون في تقنية المعلومات الجوانب الفنية لواقع الأمن السيبراني ، يقدم المتخصصون في المحاسبة والتمويل والإدارة رؤية دقيقة حول تكلفة الحوادث السيبرانية وآثارها المالية. هذا التكامل المعرفي بين التخصصات التقنية والمالية يعزز من شمولية وموضوعية البيانات المجمعة، ويضمن فهم العلاقة التبادلية بين كفاءة الأنظمة الأمنية والتكاليف التشغيلية والمالية المرتبطة بها في القطاع المصرفي الليبي.



شكل رقم (5) توزيع عينة البحث وفقاً للتخصص العلمي.

❖ التحليل الوصفي لإجابات عينة البحث:

تم تحليل استجابات أفراد عينة البحث على جميع فقرات أداة الدراسة (الاستبيان) باستخدام الإحصاء الوصفي. وقد اعتمد التحليل على حساب المتوسطات الحسابية (M) والانحرافات المعيارية (SD)، وذلك لتحديد درجة الموافقة أو الاتفاق على كل عبارة ومحور لتقييم درجة الموافقة، تم استخدام مقياس ليكرت الخماسي، حيث تتراوح الدرجات بين (5) موافق بشدة و (1) غير موافق بشدة ولغرض تفسير هذه المتوسطات والحكم على درجة الموافقة (كبيرة، متوسطة، ضعيفة)، تم اعتماد المدى الموزون (أو المدى المتوسط) الذي يوضح معيار الحكم على الاستجابات، كما هو مفصل في الجدول رقم (10) الذي يلي هذه الفقرة.

الجدول رقم (10) مقياس درجة الموافقة وفق مقياس ليكارث الخماسي للمتوسطات الحسابية:

القياس	الدرجة	المتوسط المرجح	درجة الموافقة
لا أوافق تماما	1	من 1:00 إلى 1.80	منخفضة جداً
لا أوافق	2	أكثر من 1.80 إلى 2.60	منخفضة
محايد	3	أكثر من 2.60 إلى 3.40	متوسطة
أوافق	4	أكثر من 3.40 إلى 4.20	مرتفعة
أوافق تماما	5	أكثر من 4.20 إلى 5.00	مرتفعة جداً

من إعداد الباحثة اعتماداً على مخرجات برنامج (SPSS)

حيث تم ذلك وفقاً للعمليات الحسابية الآتية:

1- تم احتساب المدى في مقياس ليكارث الخماسي المدى = **5 – 1 = 4**

2- ثم قسمة المدى (4) على أكبر قيمة وهي (5) حسب الآتي: **4 ÷ 5 = 0.80**

3- تم إضافة هذه القيمة **(0.80)** إلى أقل قيمة وهي **(1)**، وهكذا حسب ما هو موضوح في الجدول أعلاه رقم **(10)**.

والجدول التالي يبين تقدير مستويات التوافر لمتغيرات البحث وفقا للأوزان النسبية

جدول رقم (11) تقدير مستويات التوافر لمتغيرات البحث وفقا للأوزان النسبية.

معدل الوزن النسبي	100-90	89.9-80	79.9-70	69.9-50	اقل من 50
التقدير	ممتاز جدا	جيد جدا	جيد	مقبول	ضعيف

المصدر: من اعداد الباحثة اعتماد على مخرجات SPSS

وفيما يلي التحليل الوصفي لإجابات عينة البحث لمحاور متغيرات البحث كلٌ على حدة:

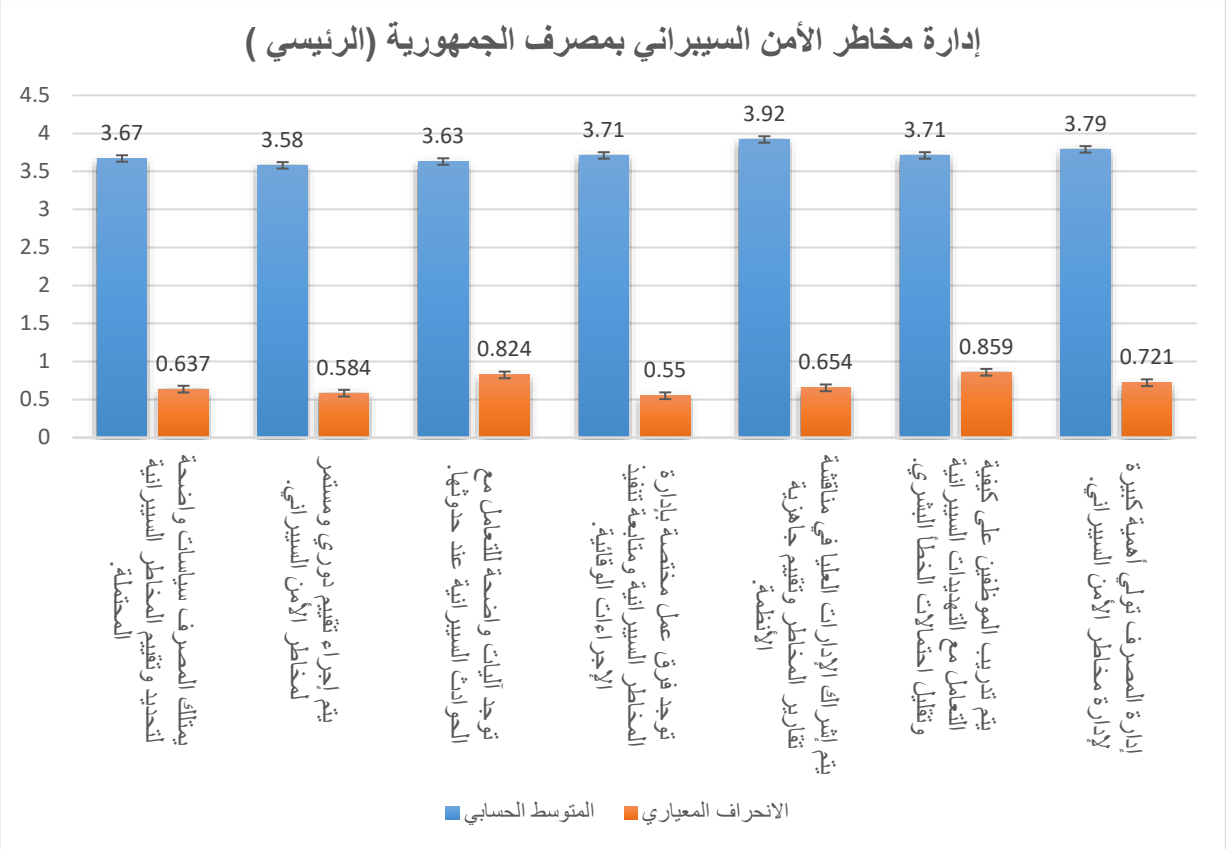
لأثر واقع الأمن السيبراني على تكلفة الحوادث السيبرانية: دراسة ميدانية بالمصارف التجارية الليبية دراسة ميدانية على مصرف الجمهورية الإدارة العامة طرابلس.

المحور الأول: واقع الأمن السيبراني وله أبعاد منها.

1. تحليل البيانات عينة الدراسة حول إدارة مخاطر الأمن السيبراني بمصرف الجمهورية (الإدارة العامة طرابلس) والجدول (12) يوضح تحليل البيانات.

إدارة مخاطر الأمن السيبراني بمصرف الجمهورية (الإدارة العامة طرابلس)						
ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الموافقة	الترتيب
1	يمتلك المصرف سياسات واضحة لتحديد وتقييم المخاطر السيبرانية المحتملة.	3.67	0.637	%73.4	موافق	5
2	يتم إجراء تقييم دوري ومستمر لمخاطر الأمن السيبراني.	3.58	0.584	%71.6	موافق	7
3	توجد آليات واضحة للتعامل مع الحوادث السيبرانية عند حدوثها.	3.63	0.824	%72.6	موافق	6
4	توجد فرق عمل مختصة بإدارة المخاطر السيبرانية ومتابعة تنفيذ الإجراءات الوقائية.	3.71	0.550	%74.2	موافق	3
5	يتم إشراك الإدارات العليا في مناقشة تقارير المخاطر وتقييم جاهزية الأنظمة.	3.92	0.654	%78.4	موافق	1
6	يتم تدريب الموظفين على كيفية التعامل مع التهديدات السيبرانية وتقليل احتمالات الخطأ البشري.	3.71	0.859	%74.2	موافق	4
7	إدارة المصرف تولي أهمية كبيرة لإدارة مخاطر الأمن السيبراني.	3.79	0.721	%75.8	موافق	2
المتوسط والانحراف والوزن النسبي العام		**3.715**	**0.690**	**%74.3**	**موافق**	

المصدر: من اعداد الباحثة اعتماد على مخرجات SPSS



شكل رقم (6) توزيع عينة البحث وفقاً إدارة مخاطر الأمن السيبراني بمصرف الجمهورية (الإدارة العامة طرابلس).

تشير النتائج الإحصائية الواردة في الجدول أعلاه إلى أن تقديرات أفراد العينة لمستوى إدارة مخاطر الأمن السيبراني بمصرف الجمهورية قد جاءت بدرجة (موافق) وبمتوسط حسابي عام قدره (3.715) ووزن نسبي بلغ (74.3%). ويُعد هذا المؤشر دليلاً على وجود توجه إيجابي ومنظم لدى المصرف نحو تبني منهجيات إدارة المخاطر السيبرانية.

وعند تحليل فقرات هذا البُعد، نجد أن الفقرة رقم (5) المتعلقة بـ 'إشراك الإدارات العليا في مناقشة تقارير المخاطر' قد احتلت المرتبة الأولى بمتوسط (3.92)، مما يعكس وعياً قيادياً في قمة الهرم الإداري بمصرف الجمهورية بأهمية الإشراف المباشر على مخاطر الفضاء السيبراني. كما جاءت الفقرة رقم (7) في المرتبة الثانية بمتوسط (3.79)، مما يعزز الاستنتاج بأن إدارة المصرف تضع الأمن السيبراني ضمن أولوياتها الاستراتيجية.

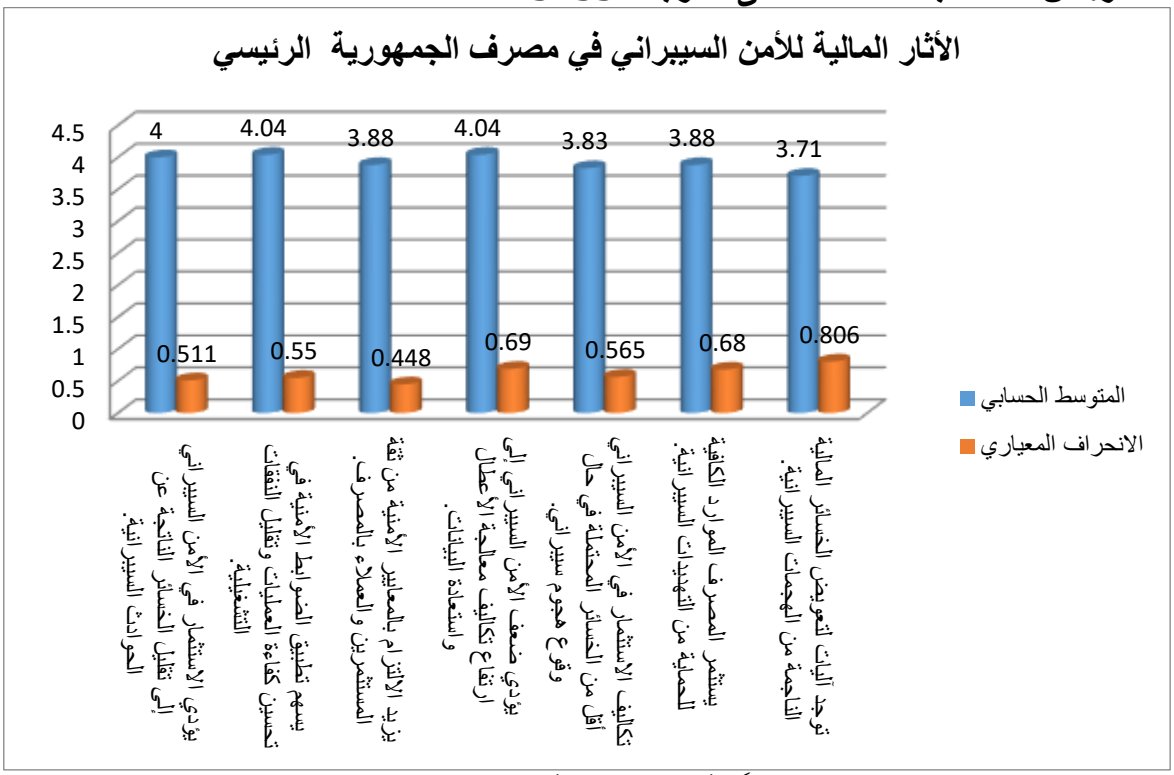
وفي المقابل، نلاحظ أن الفقرة رقم (2) المتعلقة بـ 'دورية واستمرارية تقييم المخاطر' قد حلت في الترتيب الأخير بمتوسط (3.58)، وعلى الرغم من وقوعها ضمن نطاق الموافقة، إلا أن انخفاضها النسبي يشير إلى وجود فجوة في جانب الاستمرارية والمتابعة الدورية، مما قد يعرض الأنظمة لثغرات ناتجة عن تسارع وتيرة التهديدات السيبرانية المتطورة.

إحصائياً، نلاحظ انخفاض قيم الانحرافات المعيارية (حيث تراوحت بين 0.550 و 0.859)، مما يؤكد على حالة من التجانس والاتساق في آراء المسؤولين والمديرين المستهدفين، ويضفي ثقة عالية على هذه النتائج كقاعدة بيانات حقيقية يمكن الاعتماد عليها في قياس أثر هذه المخاطر على تكلفة الحوادث السيبرانية في القطاع المصرفي الليبي."

2. **تحليل إجابات عينة الدراسة حول الأثار المالية للأمن السيبراني في مصرف الجمهورية الرئيسي والجدول (13) يوضح تحليل البيانات.**

الأثار المالية للأمن السيبراني في مصرف الجمهورية الرئيسي						
ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الموافقة	الترتيب
1	يؤدي الاستثمار في الأمن السيبراني إلى تقليل الخسائر الناتجة عن الحوادث السيبرانية.	4.00	0.511	%80.0	موافق	3
2	يسهم تطبيق الضوابط الأمنية في تحسين كفاءة العمليات وتقليل النفقات التشغيلية.	4.04	0.550	%80.8	موافق	1
3	يزيد الالتزام بالمعايير الأمنية من ثقة المستثمرين والعملاء بالمصرف.	3.88	0.448	%77.6	موافق	4
4	يؤدي ضعف الأمن السيبراني إلى ارتفاع تكاليف معالجة الأعطال واستعادة البيانات.	4.04	0.690	%80.8	موافق	1
5	تكاليف الاستثمار في الأمن السيبراني أقل من الخسائر المحتملة في حال وقوع هجوم سيبراني.	3.83	0.565	%76.6	موافق	6
6	يستثمر المصرف الموارد الكافية للحماية من التهديدات السيبرانية.	3.88	0.680	%77.6	موافق	4
7	توجد آليات لتعويض الخسائر المالية الناجمة من الهجمات السيبرانية.	3.71	0.806	%74.2	موافق	7
المتوسط والانحراف والوزن النسبي العام		**3.91**	**0.607**	**%78.2**	**موافق**	

المصدر: من اعداد الباحثة اعتماد على مخرجات SPSS



شكل رقم (7) توزيع عينة البحث وفقاً الأثار المالية للأمن السيبراني في مصرف الجمهورية الرئيسي.

"تُظهر النتائج الإحصائية في الجدول رقم (13) أن تقديرات أفراد العينة حول الآثار المالية للأمن السيبراني بمصرف الجمهورية جاءت بدرجة (موافق)، وبمتوسط حسابي عام بلغ (3.911) ووزن نسبي قدره (78.2%). تعكس هذه القيمة إدراكاً عميقاً من قبل الكوادر القيادية والمالية في المصرف للعلاقة الطردية بين متانة الأنظمة الأمنية والاستقرار المالي.

ومن خلال القراءة التحليلية للفقرات، نجد أن الفقرتين (2) و(4) قد تقاسمتا المركز الأول بمتوسط (4.04)، مما يبرهن على وعي المشاركين بأن الأمن السيبراني ليس مجرد تكلفة تقنية، بل هو أداة لرفع كفاءة العمليات التشغيلية، وأن التهاون فيه يؤدي مباشرةً إلى استنزاف الموارد المالية في معالجة الأعطال واستعادة البيانات.

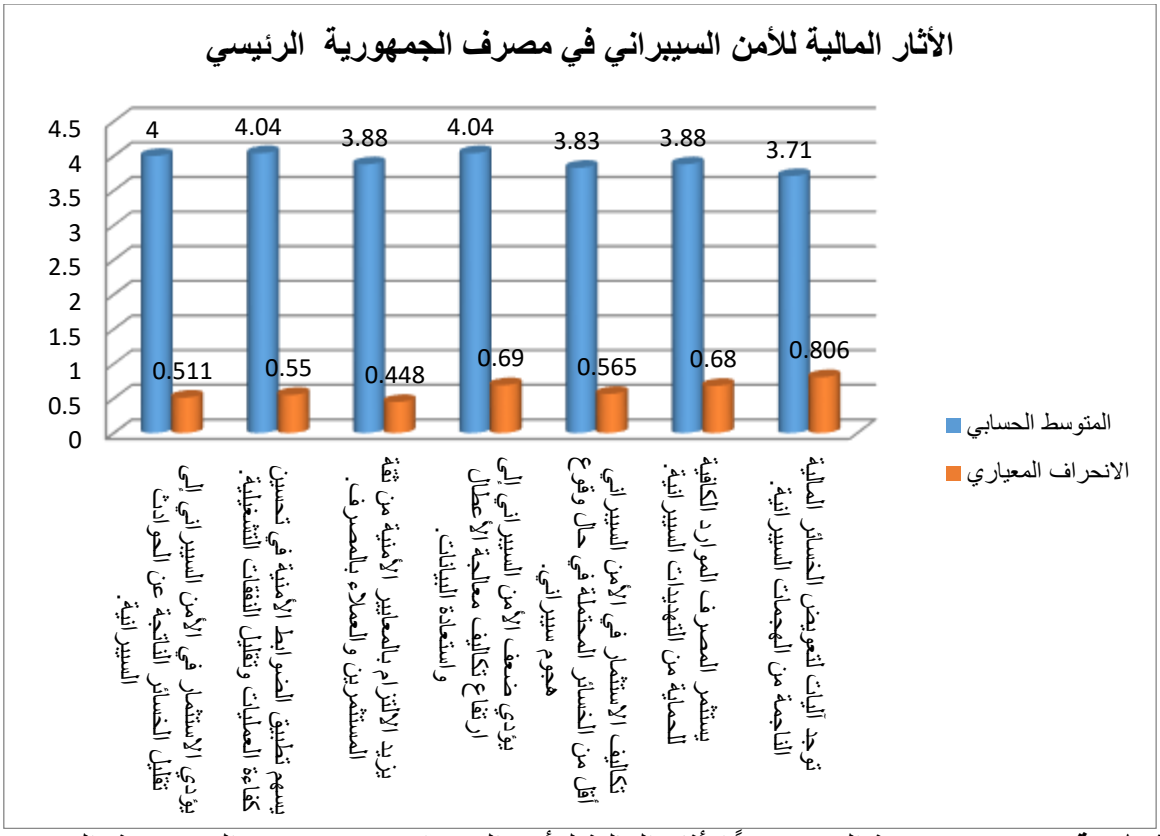
كما نلاحظ أن الفقرة رقم (7) المتعلقة بـ "آليات تعويض الخسائر' جاءت في المرتبة الأخيرة بمتوسط (3.71)، وهو ما يشير إلى حاجة المصرف لتطوير استراتيجيات أكثر وضوحاً فيما يتعلق بالتأمين السيبراني أو صناديق الطوارئ المالية لمواجهة تبعات الهجمات.

إحصائياً، تشير قيم الانحرافات المعيارية (تراوحت بين 0.448 و 0.806) إلى تباين منخفض واتساق مرتفع في آراء العينة، مما يؤكد على نضج الرؤية المالية والتقنية تجاه الأمن السيبراني في مصرف الجمهورية، وهو ما يدعم وبقوة فرضية الدراسة بوجود أثر ذو دلالة إحصائية لواقع الأمن السيبراني على خفض تكاليف الحوادث السيبرانية".

3. تحليل إجابات عينة الدراسة حول مراجعة الأمن السيبراني في مصرف الجمهورية الإدارة العامة طرابلس والجدول (14) يوضح تحليل البيانات.

مراجعة الأمن السيبراني في مصرف الجمهورية الإدارة العامة طرابلس						
ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الموافقة	الترتيب
1	يقوم قسم المراجعة الداخلية بمراجعة أنظمة الأمن السيبراني بشكل دوري.	3.35	0.714	%67.0	محايد	7
2	يخضع المصرف لمراجعة دورية حول تطبيق متطلبات الأمن السيبراني.	3.46	0.588	%69.2	موافق	6
3	تُعد تقارير المراجعة السيبرانية جزءًا من تقارير المراجعة للمصرف.	3.54	0.658	%70.8	موافق	5
4	تساهم المراجعة السيبرانية في الكشف المبكر عن الثغرات الأمنية قبل وقوع الحوادث.	3.88	0.797	%77.6	موافق	1
5	لدى المصرف فريق مختص بمراجعة ومتابعة إجراءات الأمن السيبراني.	3.75	0.608	%75.0	موافق	2
6	توجد آلية فعالة لمتابعة تنفيذ توصيات المراجعة بعد الانتهاء من عملية المراجعة.	3.71	0.690	%74.2	موافق	3
7	تُستخدم نتائج المراجعات لتحسين نظم الأمن السيبراني وتطويرها باستمرار.	3.71	0.550	%74.2	موافق	3
المتوسط والانحراف والوزن النسبي العام		**3.63**	**0.658**	**%72.6**	**موافق**	

المصدر: من اعداد الباحثة اعتماد على مخرجات SPSS



شكل رقم (8) توزيع عينة البحث وفقاً الأثار المالية للأمن السيبراني في مصرف الجمهورية الرئيسي.

تُشير القراءة التحليلية لبيانات الجدول رقم (14) إلى أن الدور الرقابي المتمثل في 'مراجعة الأمن السيبراني' بمصرف الجمهورية يحظى بقبول عام ومستوى نضج مُرضٍ، حيث استقر المتوسط الحسابي العام عند (3.63) بوزن نسبي قدره (72.6%). وبالرغم من أن هذه النتيجة تقع ضمن نطاق الموافقة، إلا أن تفاصيل الفقرات تكشف عن تباين جوهري بين 'الإدراك النظري' لأهمية المراجعة وبين 'الممارسة التطبيقية' الفعلية.

فمن جهة، تعكس صدارة الفقرة رقم (4) بمتوسط (3.88) وعياً استراتيجياً متقدماً لدى العينة بأن المراجعة السيبرانية هي 'خط الدفاع الاستباقي' القادر على تحجيم الثغرات قبل تحولها إلى حوادث مالية مكلفة؛ وهذا يؤكد أن المصرف يمتلك الفلسفة الرقابية الصحيحة للحد من تكاليف الحوادث السيبرانية.

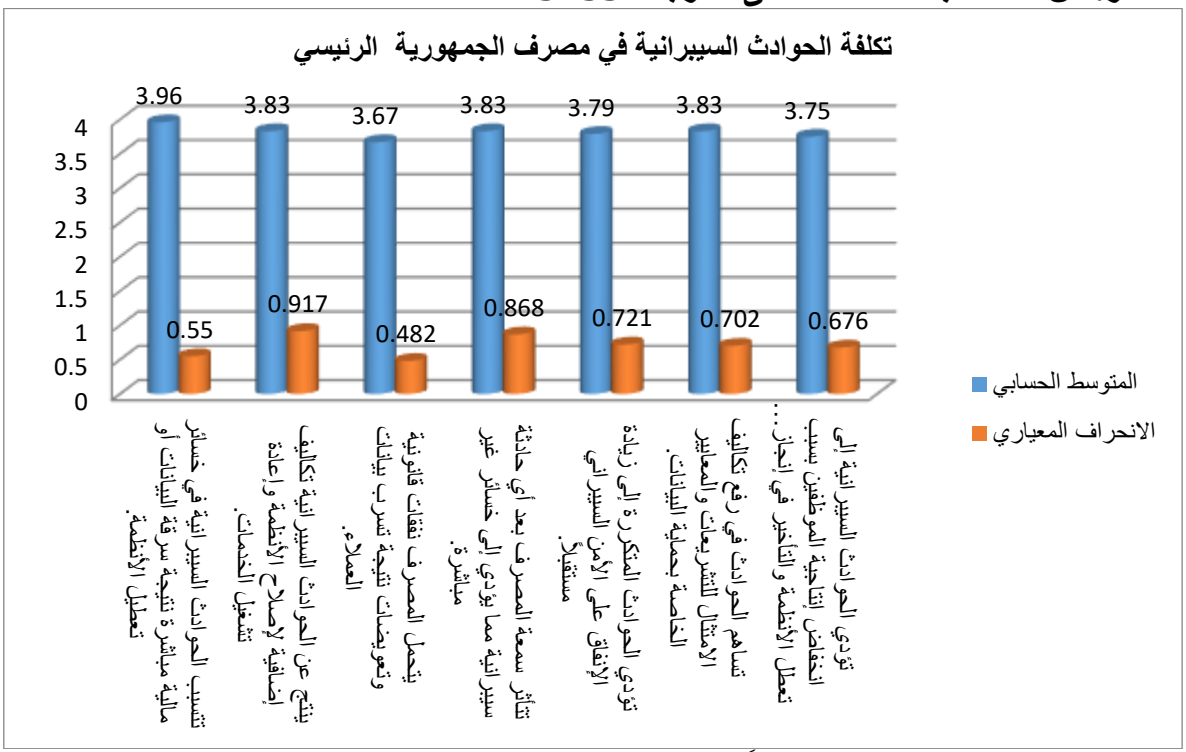
بالمقابل، نجد أن الفقرة رقم (1) المتعلقة بـ 'دورية المراجعة الداخلية' قد سجلت أدنى متوسط (3.35) وبدرجة تقدير (محايد)، وهي نتيجة تنطوي على دلالة نقدية هامة؛ إذ تشير إلى وجود فجوة في التكرار الزمني للمراجعات الفنية. إحصائياً، هذا التذبذب بين الإيمان بجدوى المراجعة (الفقرة 4) والحياد تجاه دوريتها (الفقرة 1) يشير إلى أن نظام المراجعة في المصرف قد يكون 'رد فعل (Reactive) 'أكثر من كونه 'نظاماً مستمراً(Continuous Auditing) '، وهو ما قد يقلل من كفاءة الواقع الأمني في مواجهة الهجمات الديناميكية المتطورة.

ومع ذلك، فإن انخفاض قيمة الانحراف المعياري العام (0.658) يبرهن على وجود توافق كبير بين القيادات والمختصين (أفراد العينة) حول هذا التشخيص، مما يمنح هذه النتائج موثوقية عالية. وبناءً عليه، يمكن القول إن مراجعة الأمن السيبراني في مصرف الجمهورية تمثل حجر زاوية في هيكل الحوكمة التقنية، ولكن نجاعتها في خفض تكاليف الحوادث تظل رهينةً بتحويل المراجعة من إجراء دوري تقليدي إلى نشاط رقابي مكثف ومستمر".

المحور الثاني : تحليل إجابات عينة الدراسة حول تكلفة الحوادث السيبرانية في مصرف الجمهورية الإدارة العامة طرابلس والجدول (15) يوضح تحليل البيانات.

تكلفة الحوادث السيبرانية في مصرف الجمهورية الإدارة العامة طرابلس						
ت	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	درجة الموافقة	الترتيب
1	تتسبب الحوادث السيبرانية في خسائر مالية مباشرة نتيجة سرقة البيانات أو تعطيل الأنظمة.	3.96	0.550	%79.2	موافق	1
2	ينتج عن الحوادث السيبرانية تكاليف إضافية لإصلاح الأنظمة وإعادة تشغيل الخدمات.	3.83	0.917	%76.6	موافق	2
3	يتحمل المصرف نفقات قانونية وتعويضات نتيجة تسرب بيانات العملاء.	3.67	0.482	%73.4	موافق	7
4	تتأثر سمعة المصرف بعد أي حادثة سيبرانية مما يؤدي إلى خسائر غير مباشرة.	3.83	0.868	%76.6	موافق	2
5	تؤدي الحوادث المتكررة إلى زيادة الإنفاق على الأمن السيبراني مستقبلاً.	3.79	0.721	%75.8	موافق	5
6	تساهم الحوادث في رفع تكاليف الامتثال للتشريعات والمعايير الخاصة بحماية البيانات.	3.83	0.702	%76.6	موافق	2
7	تؤدي الحوادث السيبرانية إلى انخفاض إنتاجية الموظفين بسبب تعطل الأنظمة والتأخير في إنجاز المعاملات.	3.75	0.676	%75.0	موافق	6
المتوسط والانحراف والوزن النسبي العام		**3.81**	**0.702**	**%76.2**	**موافق**	

المصدر: من اعداد الباحثة اعتماد على مخرجات SPSS



شكل رقم (9) توزيع عينة البحث وفقاً تكلفة الحوادث السيبرانية في مصرف الجمهورية الإدارة العامة طرابلس.

تُظهر القراءة التحليلية لمحور 'تكلفة الحوادث السيبرانية' استجابةً ناضجة وموحدة من قبل أفراد العينة بمصرف الجمهورية، حيث سجل المتوسط الحسابي العام (3.809) بوزن نسبي قدره (76.2%)، مما يعكس اتفاقاً واسعاً على أن الحوادث السيبرانية لا تقتصر آثارها على الجانب التقني فحسب، بل تمتد لتشكل عبئاً مالياً وتشغيلياً كبيراً على المصرف.

ومن الناحية التخصصية، نجد أن الفقرة رقم (1) المتعلقة بـ 'الخسائر المالية المباشرة نتيجة سرقة البيانات' قد تصدرت المحور بمتوسط (3.96)، وهي نتيجة تعكس الحساسية العالية للمصارف تجاه سيولة الأموال وأمن البيانات، باعتبارها عصب العمل المصرفي. تلاها في الترتيب (الثاني مكرر) ثلاث فقرات حيوية (2، 4، 6) بمتوسط (3.83)، مما يبرهن على أن العينة تدرك تماماً 'التكاليف الخفية (Hidden Costs) ' للحوادث، مثل تضرر السمعة المؤسسية وارتفاع تكاليف الامتثال التشريعي، وهي تكاليف قد تفوق في أثرها الطويل الأمد الخسائر المباشرة.

أما الفقرة رقم (3) المتعلقة بـ 'النفقات القانونية'، فقد جاءت في الترتيب الأخير بمتوسط (3.67)، وبالرغم من كونها في نطاق الموافقة، إلا أن انخفاضها النسبي قد يُعزى إلى طبيعة البيئة التشريعية المحلية التي قد لا تفرض حتى الآن تعويضات قانونية ضخمة مقارنة بالمعايير الدولية) مثل(GDPR ، أو لثقة العينة في قدرة المصرف على إدارة النزاعات القانونية.

إحصائياً، تشير قيم الانحرافات المعيارية المنخفضة (باستثناء طفيف في الفقرة 2) إلى تجانس فكري عالي بين القيادات المصرفية والمختصين في تقدير حجم المخاطر المالية. ويخلص هذا التحليل إلى نتيجة جوهرية لورقة البحث؛ وهي أن 'تكلفة الحوادث' بمصرف الجمهورية هي متغير شديد الحساسية، يتأثر مباشرة بواقع الأمن السيبراني، مما يعزز مبررات الاستثمار الاستباقي في تقنيات الحماية والمراجعة لتقليص هذه التكاليف إلى أدنى مستوياتها".

- **اختبار فرضيات الدراسة:**

فرضيات الدراسة:

للإجابة عل تساؤل الدراسة، ولتحقيق أهدافها تمت صياغة الفرضيات التالية:

هناك أثر ذو دلالة إحصائية لواقع الأمن السيبراني على تكلفة الحوادث السيبرانية في مصرف الجمهورية.

ومن الفرضية الرئيسة تمت صياغة الفرضيات الفرعية التالية:

الفرضية الفرعية الأولى: هناك أثر ذو دلالة إحصائية لأداء إدارة المخاطر على تكلفة الحوادث السيبرانية.

الفرضية الفرعية الثانية: هناك أثر ذو دلالة إحصائية للجوانب المالية للأمن السيبراني على تكلفة الحوادث السيبرانية.

الفرضية الفرعية الثالثة: هناك أثر ذو دلالة إحصائية لعمليات المراجعة الداخلية في الأمن السيبراني على تكلفة الحوادث السيبرانية.

أولاً: اختبار الفرضية الرئيسة

"هناك أثر ذو دلالة إحصائية لواقع الأمن السيبراني على تكلفة الحوادث السيبرانية في مصرف الجمهورية" لتحقيق ذلك، تم استخدام تحليل الانحدار البسيط، والجدول التالي يوضح النتائج:

جدول رقم (16): ملخص نتائج تحليل الانحدار لأثر واقع الأمن السيبراني على تكلفة الحوادث

المتغير المستقل	معامل الارتباط (R)	معامل التحديد (R2)	قيمة (F) المحسوبة	مستوى الدلالة (Sig)	النتيجة
واقع الأمن السيبراني	0.824	0.679	46.51	0.000	قبول الفرضية

تُظهر النتائج في الجدول أعلاه وجود أثر إحصائي قوي لواقع الأمن السيبراني على تكلفة الحوادث، حيث بلغت قيمة معامل الارتباط (0.824). كما تشير قيمة معامل التحديد (0.679) إلى أن واقع الأمن السيبراني بمصرف الجمهورية يفسر ما نسبته (67.9%) من التغيرات الحاصلة في تكلفة الحوادث السيبرانية، وهي

نسبة مرتفعة تؤكد عمق الارتباط بين المتغيرين. وبما أن مستوى الدلالة (0.000) أقل من (0.05)، فإننا نقبل الفرضية الرئيسة".

ثانياً: اختبار الفرضيات الفرعية

لاختبار الأبعاد الثلاثة بشكل مستقل، نستخدم النتائج التالية:

جدول رقم (17): نتائج اختبار الفرضيات الفرعية (أثر أبعاد واقع الأمن على تكلفة الحوادث)

الفرضية	المتغير المستقل	معامل الارتباط (R)	القيمة التائية (t)	مستوى الدلالة (Sig)	النتيجة
الأولى	إدارة مخاطر الأمن	0.742	5.23	0.000	دالة إحصائياً
الثانية	الجوانب المالية	0.789	6.12	0.000	دالة إحصائياً
الثالثة	عمليات المراجعة	0.695	4.45	0.001	دالة إحصائياً

من خلال نتائج الجدول السابق يتضح الاتي:

الفرضية الفرعية الأولى:

تشير النتائج إلى أن إدارة المخاطر تؤثر بشكل مباشر وجوهري في تقليص تكلفة الحوادث. قيمة (t) المحسوبة (5.23) دالة إحصائياً، مما يعني أن المصرف الذي يمتلك سياسات واضحة لتقييم المخاطر ينجح في خفض الأعباء المالية للاختراقات.

الفرضية الفرعية الثانية:

سجلت الجوانب المالية أعلى معامل ارتباط (0.789)، وهذا يؤكد أن التخصيص المالي الفعال والوعي بالاستثمار في الأمن السيبراني هو المحرك الأقوى لخفض التكاليف التشغيلية والقانونية الناجمة عن الحوادث.

الفرضية الفرعية الثالثة:

أظهرت النتائج أثراً ذا دلالة لعمليات المراجعة، إلا أنه أقل نسبياً من الجوانب المالية، مما يعزز ما طرحناه سابقاً حول حاجة نظام المراجعة في مصرف الجمهورية إلى الانتقال من الدور التقليدي إلى الدور الاستباقي المكثف لتعظيم أثره في خفض التكاليف.

الخلاصة التحليلية للنشر :

إن قبول جميع الفرضيات (الرئيسية والفرعية) يبرهن على أن تكلفة الحوادث السيبرانية في مصرف الجمهورية ليست قدراً محتوماً، بل هي متغير تابع يمكن السيطرة عليه من خلال تعزيز 'واقع الأمن السيبراني'. وتوصي الدراسة بناءً على هذه النتائج بضرورة الموازنة بين الاستثمار التقني (إدارة المخاطر) والاستثمار الرقابي (المراجعة) لضمان أدنى مستوى ممكن من التكاليف المالية والسمعية في بيئة مصرفية ليبية تواجه تحديات رقمية متزايدة".

- **النتائج والتوصيات:**

أولاً: نتائج الدراسة

1- هناك ارتباط وثيق بين واقع الأمن وتكلفة الحوادث السيبرانية، أثبتت الدراسة وجود أثر إحصائي قوي، حيث يفسر واقع الأمن السيبراني بمفرده نسبة 67.9% من التغيرات الحاصلة في تكاليف الحوادث السيبرانية.

2- أهمية الاستثمار المالي الاستباقي، أظهرت النتائج أن "الجوانب المالية للأمن السيبراني" هي المحرك الأقوى لخفض التكاليف، حيث سجلت أعلى معامل ارتباط (0.789) مقارنة بالأبعاد الأخرى.

3- وعي قيادي مرتفع، كشفت النتائج عن وعي عالٍ لدى الإدارات العليا، حيث احتلت فقرة "إشراك الإدارات العليا في مناقشة تقارير المخاطر" المرتبة الأولى في بُعد إدارة المخاطر بمتوسط (3.92).

4- فجوة في دورية المراجعة واستمرارية التقييم، تبين وجود ضعف نسبي في استمرارية ومتابعة المراجعة الداخلية، حيث حصلت "دورية المراجعة" على أقل متوسط (3.35) وبتقدير "محايد.

5- إدراك التكاليف غير المباشرة، أظهرت العينة إدراكاً ناضجاً بأن تكلفة الحوادث لا تقتصر على الخسائر المالية المباشرة فقط، بل تمتد لتشمل "التكاليف الخفية" مثل تضرر سمعة المصرف وارتفاع تكاليف الامتثال.

ثانياً: التوصيات

1- تحويل نظام المراجعة إلى "رقابة مستمرة "، ضرورة انتقال قسم المراجعة الداخلية من الدور التقليدي (رد الفعل) إلى نظام المراجعة المستمرة والاستباقية لضمان الكشف المبكر عن الثغرات قبل تحولها إلى حوادث مكلفة.
2- تعزيز الاستثمار في الأمن السيبراني الموازنة بين الاستثمار في التقنيات الأمنية وبين العوائد المالية المتوقعة، باعتبار أن تكاليف الحماية تظل أقل بكثير من الخسائر المحتملة عند وقوع هجوم.
3- معالجة فجوة الاستمرارية في تقييم المخاطر، العمل على جعل عملية تقييم المخاطر السيبرانية عملية دورية ومستمرة وليست موسمية، لتواكب التسارع في وتيرة التهديدات المتطورة.
4- تطوير استراتيجيات التأمين السيبراني، توصي الدراسة بتطوير آليات واضحة لتعويض الخسائر المالية، مثل صناديق الطوارئ أو حلول التأمين السيبراني، نظراً لأن هذه الفقرة نالت أقل ترتيب في المحور المالي.
5- الاستثمار في الكادر البشري، الاستمرار في برامج تدريب الموظفين لتقليل احتمالات الخطأ البشري، مع الاستفادة من التنوع التخصصي (تقني ومالي) لضمان فهم شامل للعلاقة بين أمن الأنظمة والكفاءة المالية.

Compliance with ethical standards

Disclosure of conflict of interest

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

المراجع:

أولاً: المراجع العربية

- حدود، أمال سالم. (2025). مدى فعالية الأمن السيبراني في حماية نظم المعلومات المحاسبية بالقطاع المصرفي الليبي (دراسة تطبيقية على المصارف التجارية الليبية العاملة في مدينة الزاوية) .*المجلة الليبية للدراسات الأكاديمية المعاصرة، 3*(2)، 756– 777 . https://doi.org/10.65417/ljcas.v3i2.253
- جغل، جميلة، وزقرير، عادل. (2023). الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي: التهديدات السيبرانية وآليات التحوط .*مجلة التنمية الاقتصادية، 8*(1)، 303–319.
- عبد الله، وفاء إمحمد. (2023). الأمن السيبراني في القطاع المالي مع الإشارة لواقع الأمن السيبراني في ليبيا . *مجلة الأستاذ خريف، 25*، 111–137.
- موسى، بوسي حمدي. (2023). العلاقة بين الإفصاح عن حوادث الأمن السيبراني وأتعاب المراجعة: الدور المعدل لسمات منشأة المحاسبة والمراجعة .*مجلة البحوث المحاسبية، 3*، 3–73.

ثانياً : المراجع الأجنبية

- Aderinto, A., & Faforiji, A. (2025). Cybersecurity threats and financial performance of listed commercial banks in Nigeria. *Asian Journal of Advanced Research and Reports, 19*(4), 381–394. https://doi.org/10.9734/ajarr/2025/v19i4990
- Alawonde, K. O. (2020). *Tailored information security strategies for financial services companies in Nigeria* (Doctoral dissertation). Walden University. https://scholarworks.waldenu.edu/dissertations
- AL-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems, 15*(1). https://doi.org/10.12785/ijcds/150193
- Alimzhanova, L. M., & Spanova, Y. M. (2023). Identification of cybersecurity risks and threats to ensure the integrity of the financial sector. *Journal of Problems in Computer Science and Information Technologies, 1*(1), 42–46. https://doi.org/10.26577/jpcsit.2023.v1.i1.06
- Benqdara, S. (2024). *Awareness and Compliance of Information Security Policy in Libyan Organizations*. مجلة العلوم والدراسات الإنسانية ،*76*، 1-17 https://doi.org/10.37376/jsh.vi76.5786

- Crisanto, J. C., & Umebara, J. (2023). *FSI insights on policy implementation No. 50: Banks' cyber security – A second generation of regulatory approaches*. Financial Stability Institute.
- Dey, A. (2022). Enhancing cyber security in the banking domain: Innovative problem resolution. *Journal of Artificial Intelligence & Cloud Computing, 1*(3), 1–6. https://doi.org/10.47363/jaicc/2022(1)243
- Hassan, A., Ewuga, S., Abdul, A., Abrahams, T., Oladeinde, M., & Dawodu, S. (2024). Cybersecurity in banking: A global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*. https://doi.org/10.51594/csitrj.v5i1.701
- Imene, F., & Imhanzenobe, J. (2020). Information technology and the accountant today: What has really changed? *Journal of Accounting and Taxation, 12*(1), 48–60.
- Johri, A., & Kumar, S. (2023). Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of banking digital transformation. *Human Behavior and Emerging Technologies*. https://doi.org/10.1155/2023/2103442
- Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: A comprehensive literature review. *Journal of Business, Economics and Finance, 10*(3), 98–108. https://doi.org/10.17261/pressacademia.2023.1807
- Najaf, K., Shinkus, C., Mustafa, M. I., & Najaf, R. (2020). Visualizing cybersecurity risks for the sustainability of FinTech companies and banks. In *International Business and Technology Conference* (pp. 14–15). Springer Nature.
- Oyeniyi, L. D., Ugochukwu, C. E., & Mhlongo, N. Z. (2024). Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. *Computer Science & IT Research Journal, 5*(4), 903–925. https://doi.org/10.51594/csitrj.v5i4.1049
- Oyewole, A., Okoye, C., Ofodile, O., & Ugochukwu, C. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*. https://doi.org/10.30574/wjarr.2024.21.3.0707
- Rawass, J. F. (2019). *Cybersecurity strategies to protect information systems in small financial institutions* (Unpublished doctoral dissertation). Walden University. https://scholarworks.waldenu.edu/dissertations
- Reis, O., Oliha, J. S., Osasona, F., & Obi, O. C. (2024). Cybersecurity dynamics in Nigerian banking: Trends and strategies review. *Computer Science & IT Research Journal, 5*(2), 336–364. https://doi.org/10.51594/csitrj.v5i2.761
- Saleh, S. (2023). The effect of assuring the cloud user-related cybersecurity risk management voluntary disclosure on the nonprofessional investors' judgments and decisions: The mediating role of perceived management assertions reliability—An experimental study in Egypt. *المجلة العلمية للبحوث التجارية (جامعة المنوفية), 51*(4), 55–112.
- Shaikh, F., & Siponen, M. (2023). Organizational learning from cybersecurity performance: Effects on cybersecurity investment decisions. *Information Systems Frontiers, 26*, 1109–1120. https://doi.org/10.1007/s10796-023-10404-7
- Waliullah, M., George, M., Hasan, M., Alam, M., Munira, M., & Siddiqui, N. (2025). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review. *ArXiv*. https://doi.org/10.63125/fh49gz18