العلاقة بين التمويل الرقمي والأمن السيبراني

دراسة تطبيقية على الإدارة العامة لـ المصرف التجاري الوطني بمدينة البيضاء/ ليبيا

The Relationship Between Digital Finance and Cybersecurity: An Empirical Study on the General Management of the National Commercial Bank in El-Beida City, Libya

أمصورة السنوسي[1]، حمدي حدوث [2]

Amsawrah Alsanousi[1], Hamdi Hadouth[2]

[1] عضو هيئة تدريس بكلية الاقتصاد/جامعة درنة .ليبيا a.alsanousi@uod.edu.ly

[2] عضو هيئة تدريس كلية الاقتصاد/ جامعة طبرق hamdi20203@googlemail.com

تاريخ الاستلام: 07 /2026/05 تاريخ القبول: 25 /2026/06 تاريخ النشر: 30 /2026/06

ملخص:

هدفت هذه الدراسة إلى تحليل أثر التمويل الرقمي في مواجهة المخاطر السيبرانية في الإدارة العامة للمصرف التجاري الوطني في مدينة البيضاء، وذلك من خلال بحث العلاقة بين أبعاد التمويل الرقمي (التمويل الرقمي، أمن المعلومات، إدارة العمليات الرقمية) وتهديدات البيانات والمعلومات، إلى جانب دور وعي الموظفين بالمخاطر السيبرانية. اعتمدت الدراسة المنهج الوصفي التحليلي، واستخدمت الاستبانة كأداة رئيسية لجمع البيانات من عينة قصدية (49) موظفاً من العاملين في مجالات الإدارة، وتقنية المعلومات، وإدارة المخاطر، والعمليات المصرفية، وتم تحليلها عبر برنامج *(SPSS)* ومعامل ارتباط سبيرمان.

أظهرت النتائج وجود ارتباطات إيجابية ذات دلالة إحصائية بين التمويل الرقمي وأمن المعلومات، وبين التمويل الرقمي وإدارة العمليات الرقمية، وكذلك بين أمن المعلومات وإدارة العمليات الرقمية، مما يدل على أن التحول الرقمي يرتبط بتحسين التنظيم التشغيلي وتعزيز البنية الأمنية داخل المصرف في المقابل، لما تُظهر النتائج علاقة ذات دلالة إحصائية بين أبعاد التمويل الرقمي وتهديدات البيانات والمعلومات، ولا بين أمن المعلومات وتهديدات البيانات، ولا بين إدارة العمليات الرقمية وتهديدات البيانات، الأمر الذى يشير إلى أن المخاطر السيبرانية تمثل بُعداً مستقلاً يتأثر بعوامل أخرى، وأوصت الدراسة بدمج الأمن السيبراني ضمن استراتيجيات التحول الرقمي، وتحديث المستمر لأنظمة أمن المعلومات والبنية التحتية الرقمية، وتعزيز برامج التدريب والتوعية الأمنية للموظفين لضمان استدامة الخدمات المصرفية الرقمية.

الكلمات المفتاحية: التمويل الرقمي، تعزيز البيئة الأمنية للمصارف، استراتيجيات التحول الرقمي، الأمن السيبراني، المخاطر السيبرانية في القطاع المصرفي.

Abstract:

This study aimed to analyze the impact of digital finance on addressing cyber risks in the general management of the National Commercial Bank in Al-Bayda city. The study examines the relationship between the main dimensions of digital finance digital finance practices, information security, and digital operations management and data threats, while also exploring the role of employees of cyber risks. The research adopts a descriptive- analytical approach data were collected from a sample of 49 employees through a structured questionnaire. The collected data were analyzed using the statistical package for the social sciences (SPSS), and spearmans correlation coefficient was employed to test the relationships among the study variables. The result reveal statistically significant positive correlations between digital finance and information security, digital finance and digital operations management, as well as between information security and digital operations management. These findings indicate that digital transformation enhances operational efficiency, strengthens internal control systems, and supports the development of a secure digital environment within the bank. However, no statistically significant relationship was found between the dimensions of digital finance and data threats. This suggests that cyber risks may constitute an independent dimension influenced by additional organizational and technological factors. The study recommends integrating cybersecurity into digital transformation strategies, upgrading technological employee training and awareness programs to ensure the sustainability and resilience of digital banking services.

Keywords: Digital finance, cybersecurity, cyber risks in the banking sector.

المؤلف المرسل: أمصورة السنوسي ، الإيميل: a.alsanousi@uod.edu.ly

المقدمة:

شهد القطاع المالي والمصرفي في السنوات الأخيرة تطوراً متسارعاً بفعل التقدم في تكنولوجيا المعلومات والاتصالات، مما أدى إلى بروز مفهوم التمويل الرقمي كأحد المداخل الحديثة لتقديم الخدمات المالية، ويقوم التمويل الرقمي على توظيف الوسائل الإلكترونية والتطبيقات الذكية والتكنولوجيا المالية في تنفيذ المعاملات المصرفية بما، يسهم في تحسين الكفاءة التشغيلية، وخفض التكاليف، وتسهيل وصول العملاء إلى الخدمات المالية المختلفة **(عبدالله، 2021)**

ويعد التمويل الرقمي جزءاً أساسياً من التحول الرقمي الشامل الذي تسعى المؤسسات المصرفية إلى تحقيقه من أجل تعزيز قدرتها التنافسية ومواكبة المتغيرات المالية، وقد ساهم هذا التحول في إعادة تشكيل نماذج الأعمال المصرفية التقليدية، من خلال الاعتماد المتزايد على القنوات الرقمية في تقديم الخدمات، الأمر الذي انعكس إيجابياً على جودة الخدمات وسرعة إنجاز المعاملات**(الطاهر، 2022)**، إلا أن التوسع في استخدام التقنيات الرقمية في القطاع المالي صاحبه ظهور مجموعة من المخاطر، وعلى رأسها المخاطر المرتبطة بأمن المعلومات والبيانات المالية. وقد أدى ذلك إلى تزايد الاهتمام بمفهوم الأمن السيبراني، الذي يُعني بحماية الأنظمة الإلكترونية والشبكات، وقواعد البيانات من التهديدات والهجمات الإلكترونية التي قد تؤثر على سلامة المعاملات المالية**(سالم، 2020)**، ويكتسب الأمن السيبراني أهمية خاصة في القطاع المصرفي نظراً لحساسية البيانات المالية، واعتماد المصارف المتزايد على النظم الرقمية، حيث إن أي اختراق أو خلل أمني قد يؤدي إلى خسائر مالية كبيرة، ويؤثر سلباً على ثقة العملاء واستقرار النظام المالي ككل**(جغل، زقرير، 2023)**، وتشير الدراسات العربية الحديثة إلى أن نجاح التمويل الرقمي واستدامته يرتبطان ارتباطاً وثيقاً بمدى فاعلية نظم الأمن السيبراني المطبقة داخل المؤسسات المالية، إذ تسهم هذه النظم في تعزيز الثقة في الخدمات المصرفية الرقمية، وضمان استمرارية تقديمها بكفاءة وأمان**(بنعايني، سيلكا، 2025)**.

مشكلة الدراسة:

على الرغم من الانتشار المتزايد للخدمات الرقمية في المصرف التجاري الوطني بمدينة البيضاء، إلا أن التحول نحو التمويل الرقمي لم يكن دائماً مصحوباً بمستوى كافٍ من الأمن السيبراني لضمان حماية البيانات والمعاملات المالية، وتظهر الملاحظات الميدانية والدراسات السابقة وجود فجوة بين تطبيق التقنيات الرقمية والإجراءات الأمنية المتبعة، مما يؤدي إلى ضعف كفاءة الخدمات الرقمية وتأثير ثقة العملاء؛ وعليه ومن هذا المنطلق ينبثق التساؤل الرئيسي التالي:

ما أثر التمويل الرقمي على مواجهة المخاطر السيبرانية في الإدارة العامة للمصرف التجاري الوطني بمدينة البيضاء؟

وبناءً على التساؤل الرئيسي أعلاه تنبثق مجموعة من التساؤلات الفرعية التالية:

1. ما مدى تأثير تقنيات التمويل الرقمي المستخدمة في المصرف على مستوى الأمن السيبراني؟
2. ما مدى فعالية حماية البيانات والمعلومات الرقمية في تعزيز الأمن السيبراني للمصرف؟
3. ما مدى مساهمة إدارة العمليات الرقمية وتنظيمها في دعم وتعزيز الأمن السيبراني؟
4. ما دور الأمن السيبراني في تطوير التمويل الرقمي؟
5. ما مدى مستوى الوعي والتدريب الأمني لدى موظفي المصرف في تعزيز وكفاءة التمويل الرقمي؟

أهداف الدراسة:

1. معرفة أثر التمويل الرقمي في مواجهة المخاطر السيبرانية في الإدارة العامة للمصرف التجاري الوطني
2. التعرف على أثر التقنيات الرقمية المستخدمة في المصرف على مستوى الأمن السيبراني
3. تقييم فعالية حماية البيانات والمعلومات الرقمية في تعزيز مستوى الأمن السيبراني
4. دراسة دور إدارة العمليات الرقمية وتنظيمها في دعم وتعزيز الأمن السيبراني
5. بيان أثر مستوى الوعي والتدريب الأمني لدى الموظفين على كفاءة التمويل الرقمي وتحسين الأمن السيبراني.

فرضيات الدراسة:

استنادًا إلى ما تم عرضه في الإطار النظري والدراسات السابقة، تم صياغة فرضيات الدراسة على النحو الآتي:

أولًا: الفرضية الرئيسية:

توجد علاقة ذات دلالة إحصائية بين التمويل الرقمي وأمن المعلومات وإدارة العمليات الرقمية وتهديدات البيانات.

ثانيًا: الفرضيات الفرعية:

1- توجد علاقة ذات دلالة إحصائية بين التمويل الرقمي وأمن المعلومات.
2- توجد علاقة ذات دلالة إحصائية بين التمويل الرقمي وإدارة العمليات الرقمية.
3- توجد علاقة ذات دلالة إحصائية بين التمويل الرقمي وتهديدات البيانات.
4- توجد علاقة ذات دلالة إحصائية بين أمن المعلومات وإدارة العمليات الرقمية.
5- توجد علاقة ذات دلالة إحصائية بين أمن المعلومات وتهديدات البيانات.

أهمية الدراسة:

تنبع أهمية هذه الدراسة من تناولها موضوع التمويل الرقمي في ظل المخاطر السيبرانية في القطاع المصرفي، بوصفه من القضايا المعاصرة ذات الأثر المباشر على كفاءة واستمرارية الخدمات المصرفية. وتسهم هذه الدراسة في تعزيز المعرفة العلمية من خلال تحليل العلاقة بين التمويل الرقمي والمخاطر السيبرانية، بما يدعك الأدبيات ذات الصلة، ويوفر أساساً يمكن البناء عليه في دراسات لاحقة، خاصة في البيئة المصرفية الليبية. كما تبرز أهميتها التطبيقية في إمكانية الاستفادة من نتائجها في تقييم واقع التمويل الرقمي، ودعم متخذي القرار في المصرف التجاري الوطني لتطوير السياسات، والإجراءات اللازمة لتعزيز الأمن السيبراني وتحسين كفاءة الخدمات المصرفية الرقمية.

منهجية الدراسة:

اعتمدت هذه الدراسة على المنهج الوصفي و التحليلي، واستخدمت أداة الاستبانة لجمع البيانات من مدراء الأقسام، وموظفي تقنية المعلومات، والخدمات الإلكترونية، وإدارة المخاطر، وموظفي العمليات المصرفية مع اختيار العينة القصدية لضمان تمثيل المشاركين الأكثر خبرة؛ وتم تحليلها بواسطة برنامج الحزم الاجتماعية (SPSS)

مجتمع وعينة الدراسة:

يشمل مجتمع الدراسة جميع موظفي الإدارة العامة للمصرف التجاري الوطني بمدينة البيضاء المرتبطين بالتمويل الرقمي والأمن السيبراني، وهم مدراء الأقسام، وموظفي تقنية المعلومات والخدمات الإلكترونية، وإدارة المخاطر، وموظفي العمليات المصرفية اما عينة الدراسة تم اختيار العينة القصدية لضمان تمثيل الأشخاص الأكثر حبرة وتأثيراً في مجال الدراسة، مما يساعد على جمع بيانات دقيقة حول تأثير المخاطر السيبرانية على التمويل الرقمي.

حدود الدراسة:

تقتصر الدراسة على:

- **الحدود الموضوعية:** دراسة التمويل الرقمي والأمن السيبراني.
- **الحدود البشرية:** شملت الدراسة مدراء الأقسام، وموظفي تقنية المعلومات، والخدمات الإلكترونية، وإدارة المخاطر، والعمليات المصرفية في الإدارة العامة للمصرف التجاري الوطني.
- **الحدود المكانية:** أجريت الدراسة في الإدارة العامة للمصرف التجاري الوطني بمدينة البيضاء.

الدراسات السابقة:

1. دراسة طاهر فرج(2025) بعنوان تقنيات التحول الرقمي وأثرها علي فعالية نظم المعلومات المحاسبية هدفت هذه الدراسة إلى التعرف على مدى إسهام التحول الرقمي في تحسين كفاءة وفاعلية النظم المحاسبية، وأظهرت نتائج الدراسة وجود أثر إيجابي ذي دلالة إحصائية لتطبيق التحول الرقمي على فعالية نظم المعلومات المحاسبية، وأوصت

الدراسة بضرورة تطوير البنية التحتية الرقمية، وتعزيز نظم الأمن السيبراني، وتكثيف برامج التدريب للعاملين بما يدعم كفاءة الأداء المصرفي.

2. دراسة حسني رمضان**(2024)** بعنوان أثر تطبيق التحول الرقمي في المصارف الإسلامية الليبية علي تطوير مهنة المحاسبة والمراجعة، وهدفت إلى التعرف على مستوى تطبيق التحول الرقمي وابعاده المختلفة داخل المصارف الإسلامية، ومدى انعكاس ذلك علي تطوير الخدمات المصرفية والإدارية، وأظهرت نتائج الدراسة أن التحول الرقمي يُسهم بشكل جزئي في تحسين جودة الخدمات المصرفية والإدارية في المصارف الإسلامية الليبية، كما أكدت النتائج وجود حاجة ملحَة إلى تعزيز البنية التحتية الرقمية، وتطوير الأنظمة التكنولوجية المستخدمة، وأوصت الدراسة بضرورة توفير الإمكانات التكنولوجية اللازمة، ودعم التحول الرقمي داخل المصارف الإسلامية، بما يسهم في تحسين الأداء المصرفي ورفع كفاءة الخدمات المقدمة.
3. دراسة الصديق خنفر، حمزة أكريم**(2022)** بعنوان أثر مخاطر التحول الرقمي في تحسين كفاءة أمن المعلومات هدفت إلى التعرف على مدى إسهام إدارة مخاطر التحول الرقمي في تحسين كفاءة أمن المعلومات بالمصارف التجارية الليبية، وأظهرت نتائج الدراسة وجود أثر إيجابي ذي دلالة إحصائية لإدارة مخاطر التحول الرقمي علي كفاءة أمن المعلومات خاصة فيما يتعلق بإدارة المخاطر الداخلية والخارجية المرتبطة بالأنظمة الرقمية المصرفية. كما بينت النتائج أن الاهتمام بإدارة مخاطر التحول الرقمي يُسهم في حماية البيانات والمعلومات الحساسة من المخاطر السيبرانية، وأوصت الدراسة بضرورة تعزيز تطبيق ممارسات إدارة مخاطر التحول الرقمي داخل المصارف التجارية الليبية، وزيادة الاهتمام بتطوير البنية التكنولوجية، وتحسين كفاءة نظم أمن المعلومات، بما يدعم سلامة العمليات المصرفية في ظل التحول الرقمي المتسارع.
4. دراسة علي التائب، جبريل السائح**(2025)** بعنوان تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية هدفت الدراسة إلى تسليط الضوء علي مستوى تطبيق إجراءات الأمن السيبراني المحاسبي في المصارف التجارية الليبية محل الدراسة، وقياس مدى إدراك العاملين لأهميته في حماية المعلومات المحاسبية من المخاطر والتهديدات الإلكترونية، وأظهرت نتائج الدراسة أن المصارف التجارية في مدينة سبها تطبق إجراءات الأمن السيبراني المحاسبي بدرجات متفاوتة مع وجود إدراك متزايد لدى العاملين بأهمية هذه الإجراءات في حماية المعلومات المحاسبية كما أشارت النتائج إلى وجود عدد من التحديات والمعلومات التي تحد من التطبيق الفعال للأمن السيبراني المحاسبي، ومن أبرزها ضعف البنية التحتية التقنية ونقص الكفاءات المتخصصة، وأوصت الدراسة بضرورة تعزيز الاهتمام بتطبيق معايير الأمن السيبراني المحاسبي، وتكثيف برامج التدريب والتأهيل للعاملين إلى جانب دعم البنية التحتية التكنولوجية، بما يُسهم في تحسين مستوى حماية نظم المعلومات في المصارف التجارية الليبية.

التعليق على الدراسات السابقة:

يتضح من خلال استعراض الدراسات السابقة أنها تناولت موضوع التحول الرقمي والتمويل الرقمي والأمن السيبراني من زوايا متعددة، إلا أنها اختلفت في نطاق التركيز وطبيعة العلاقات المدروسة بين متغيرات البحث.

فقد ركزت دراسة إبراهيم (2025) على أثر التحول الرقمي في فعالية نظم المعلومات المحاسبية، حيث توصلت إلى وجود أثر إيجابي معنوي، وهو ما يتفق مع نتائج الدراسة الحالية التي أظهرت وجود علاقة إيجابية بين التمويل الرقمي وكلٍّ من إدارة العمليات الرقمية وأمن المعلومات. ومع ذلك، لم تتناول تلك الدراسة المخاطر السيبرانية بوصفها متغيرًا مستقلاً ضمن نموذج تحليلي متكامل، وهو ما سعت الدراسة الحالية إلى معالجته.

كما أشارت دراسة الشتيوي (2024) إلى أن التحول الرقمي يسهم جزئيًا في تطوير الخدمات المصرفية، مع استمرار وجود تحديات مرتبطة بالبنية التحتية التقنية، وهو ما يتقاطع مع نتائج الدراسة الحالية التي أكدت أهمية تحديث الأنظمة وتعزيز البنية الرقمية لضمان فاعلية التحول الرقمي.

وتتميز الدراسة الحالية بأنها: قدمت نموذجًا تحليليًا متكاملاً جمع بين أبعاد التمويل الرقمي وأمن المعلومات وإدارة العمليات الرقمية وتهديدات البيانات والمعلومات ضمن إطار واحد، حيث تم تطبيقه ميدانيًا على الإدارة العامة للمصرف التجاري الوطني بمدينة البيضاء، مع اختبار العلاقات بين المتغيرات إحصائيًا وتحليلها تفسيرياً. وقد أظهرت النتائج أن المخاطر السيبرانية قد تمثل بُعدًا مستقلاً نسبيًا لا يرتبط بصورة مباشرة بمستوى تطبيق التمويل الرقمي، وهو ما يمثل إضافة علمية تسهم في إثراء الأدبيات السابقة، ويختلف جزئيًا مع ما طرحته بعض التقارير والدراسات الدولية الصادرة عن البنك الدولي وبنك التسويات الدولية.

الجانب النظري للدراسة:

أولا مفهوم التمويل الرقمي:

هو مجموعة من المنتجات والخدمات المالية التي تمكّن الأفراد والشركات من الوصول إلى المدفوعات والتسهيلات الائتمانية والمدخرات إلكترونياً، دون الحاجة إلى زيارة فروع المصارف، حيث يتم التعامل مباشرة مع مزود الخدمة عبر الإنترنت. ويشمل ذلك الخدمات المقدمة عبر أجهزة الحاسوب الشخصي أو الهاتف المحمول، بالإضافة إلى البطاقات المرتبطة بأنظمة الدفع الرقمي أو بطاقات الإنترنت، بما يضمن سهولة وأمان المعاملات المالية**2017,2018 (Oizli,;Combr& eat,)**

ثانيًا: أهمية التمويل الرقمي:

يعد التمويل الرقمي أداة أساسية لتسهيل الوصول إلى الخدمات المالية بشكل آمن وفعّال ومنخفض التكلفة، مما يعزز الشمول المالي ويوسع نطاق الخدمات للأفراد والقطاعات غير المالية، ويسهم في تحسين الوصول إلى الخدمات المالية الحديثة عالمياً، بما يساهم في الحد من الفقر ودعم النمو الاقتصادي. كما يشجع على استخدام الإنترنت في مختلف الأنشطة اليومية، مثل دفع الفواتير والرواتب وإعادة تعبئة الأرصدة، مما يعزز التفاعل الاجتماعي وتنمية الاقتصاد الرقمي. ويساهم التحول من المعاملات الورقية والنقدية إلى المعاملات الرقمية عبر منصات آمنة في زيادة الكفاءة والشفافية، بينما يمكن للهيئات التنظيمية التحكم بشكل أفضل في العمليات المالية والحد من تداول الأموال المزيفة، وضمان سرعة وسهولة استلام المدفوعات لجميع الأفراد والشركات، بما يعزز الناتج المحلي الإجمالي ويقوي الاقتصاد الرقمي**(جارالله، 2023)**

ثالثًا: خدمات التمويل الرقمي:

- أنظمة التسوية الإلكترونية (الدفع . التحويل): تُعد هذه الأنظمة من الركائز الأساسية لخدمات التمويل الرقمي، إذ تقوم على استخدام دفاتر أستاذ محاسبية رقمية تُسجل من خلالها ملكية الأصول المالية. وتمثل عملية التسوية الإجراء الذي يتم بموجبه تحديث سجلات الملكية للأصول المنقولة، سواء تعلّق الأمر بعمليات الدفع أو تحويل الأموال. وتحقق التسوية من خلال تعديل أرصدة الأطراف المتعاملة، بحيث يُخفض رصيد المرسل ويُزاد رصيد المستلم في دفاتر الأستاذ الإلكترونية، الأمر الذي يسهم في تسوية الالتزامات المالية القائمة بين الطرفين وضمان إتمام المعاملات بكفاءة ودقة**(وليد، 2023)**
- الإقراض ومنصات التمويل الجماعي: يُعد الإقراض عبر المنصات الرقمية أحد أبرز نماذج التمويل الحديثة، إذ يقوم على ربط الممولين بالأفراد أو الجهات التي تحتاج إلى التمويل، ولا سيما المؤسسات الصغيرة والمتوسطة، من خلال منصات إلكترونية متخصصة مثل منصات الإقراض المباشر ومنصات التمويل الجماعي. ويُعرَّف التمويل الجماعي على أنه آلية تمويل تعتمد على جهود رواد الأعمال في جمع الموارد المالية اللازمة لمشروعاتهم عبر منصات إلكترونية تعمل كوسيط بين الممولين والمستثمرين، مقابل تقاضي عمولات أو عوائد تختلف باختلاف نموذج التمويل، سواء على أساس الفائدة أو المشاركة في الأرباح. كما تتيح منصات التمويل الجماعي مجموعة متنوعة من الخدمات المالية التي تسهم في تسهيل الوصول إلى التمويل وتعزيز الابتكار وريادة الأعمال**(لينه، 2023)**
- العملات المشفرة: تمثل العملات المشفرة من بين الأدوات الحديثة المساعدة في إنجاز المدفوعات عبر شبكة الإنترنت، وهي عبارة عن عملات رقمية لا مركزية تعتمد على تقنية الند للند، وتتميز هذه العملات بعدم استنادها إلى اقتصاد أي

دولة أو إلى أصول ملموسة أو أساسيات أي شركة، بل تقوم على خوارزميات رقمية معقدة. وتختلف العملات المشفرة بشكل كبير عن الأدوات المالية التقليدية مثل الأسهم والسندات والسلع وأسواق العملات الأجنبية. ومن أبرز خصائصها أنها تتمتع بتقلبات شديدة في القيمة، ما يعرض المستثمرين لمخاطر مرتفعة، وقد يؤدي ذلك إلى تكبد خسائر كبيرة أو تحقيق أرباح عالية. وبناءً على، ذلك ينبغي على المستثمرين أخذ هذه التقلبات بعين الاعتبار عند التعامل مع هذه الأصول**(جارالله، 2023)**

- التأمين الرقمي: يُعرَف بأنه عملية التحويل الرقمي لكافة خدمات التأمين التي تقدمها شركات التأمين، حيث يتم تحويلها إلى خدمات رقمية بهدف أتمتة استخدام الحواسيب والأجهزة القائمة على المعالجات أو المتحكمات، إلى جانب البرمجيات، في مختلف القطاعات الصناعية والتجارية والخدمية، لضمان سير الإجراءات والأعمال بشكل آلي ودقيق مع الحد من الأخطاء قدر الإمكان**(عبدالسميع وآخرون، 2024).**

رابعًا: الأمن السيبراني:

يعرف الأمن السيبراني بأنه مجموعة من الاستراتيجيات والتقنيات والسياسات والإجراءات التي تهدف إلى حماية الأنظمة الإلكترونية والشبكات وأجهزة الحاسوب وقواعد البيانات من التهديدات والهجمات السيبرانية. ويشمل ذلك الحفاظ على سرية المعلومات وسلامتها وتوافرها، ومنع الوصول غير المصرح به، والكشف عن أي محاولات استغلال غير قانونية للبيانات أو الموارد الرقمية. كما يهدف الأمن السيبراني إلى ضمان استمرارية الأعمال من خلال تطبيق التدابير الوقائية وآليات الاستجابة الفعّالة للحد من آثار المخاطر السيبرانية المتزايدة**(زراق، 2024)**.

خامسًا: أهمية الأمن السيبراني:

يُعدّ الأمن السيبراني أحد العناصر الأساسية في مكافحة الجرائم الإلكترونية التي تنشأ في الفضاء الرقمي أو الافتراضي، والتي تنفذها أفراد أو جماعات تمتلك مهارات تقنية متقدمة، وتترتب عليها أضرار جسيمة تمس الأفراد والمجتمعات. وفي ظل التحول المتسارع نحو الاعتماد على شبكة الأنترنت وتزايد الترابط الرقمي بين مختلف القطاعات، أصبح الأمن السيبراني ضرورة لا غنى عنها في الحياة اليومية على المستويات السياسية والاقتصادية والاجتماعية. كما غدا ركيزة أساسية في إنجاز المعاملات الإلكترونية للأفراد والدول على حد سواء، وعنصراً حيوياً في دعم الأمن القومي وتعزيز الأمن الجماعي وحماية المصالح الاستراتيجية**(حشروف، صديقي، 2025)**

*المخاطر السيبرانية

يُقصد بالخطر السيبراني احتمال تعرض أصول الأعمال، بما في ذلك الإيرادات والسمعة والبيانات والأنظمة، لأضرار أو خسائر ناتجة عن هجمات سيبرانية تنفذها أطراف بشرية تسعى إلى سرقة الأموال أو المعلومات أو التقنيات. وعلى الرغم من أن هذه الهجمات تقع ضمن بيئة تقنية، إلا أن آثارها غالباً ما تمتد لتشمل الكيان المؤسسي بأكمله، مما يجعلها تهديداً استراتيجياً يتجاوز البعد التقني. وبناءً عليه، يتطلب التعامل مع المخاطر السيبرانية مواءمتها ضمن أطر شاملة لإدارة المخاطر تشمل القياس والتقييم والمتابعة والتخفيف من آثارها. ولا تزال العديد من المؤسسات تنظر إلى مخاطر الأمن السيبراني بوصفها مشكلة تقنية بحتة، وهو تصور يؤدي إلى استنتاجات غير دقيقة ويحدّ من فاعلية الاستجابة الاستراتيجية اللازمة للتقليل من تأثيرها على أداء الأعمال واستدامتها**(يحياوي، 2024)**

سادسًا: التحديات التي تواجه المخاطر السيبرانية في القطاع المصرفي:

يواجه القطاع المصرفي، في ظل التوسع المتزايد في تطبيقات التمويل الرقمي، مجموعة من التحديات المرتبطة بالمخاطر السيبرانية، حيث أدى الاعتماد المتزايد على القنوات المصرفية الإلكترونية إلى ارتفاع احتمالية التعرض للهجمات الإلكترونية، مثل الاختراقات وهجمات التصيّد الاحتيالي والبرمجيات الخبيثة، مما يشكل تهديداً مباشراً لأمن وسرية البيانات المالية للعملاء**(World Bank, 2020)**. كما تُعد محدودية كفاءة البنية التحتية التقنية وعدم تحديث الأنظمة المصرفية بما يتلاءم مع

متطلبات الأمن السيبراني الحديثة من أبرز التحديات التي تواجه المؤسسات المصرفية في الدول النامية، الأمر الذي يزيد من قابلية التعرض للمخاطر السيبرانية**(BIS,2018)**. إضافةً إلى ذلك، يُعد ضعف الوعي الأمني لدى بعض الموظفين والعملاء أحد العوامل الرئيسة المساهمة في تفاقم المخاطر السيبرانية، حيث تشير الدراسات إلى أن العنصر البشري يمثل إحدى نقاط الضعف الأساسية في منظومة الأمن السيبراني للمصارف **(ISO/IEC 27001,2013)**. كما تواجه المصارف تحدياً يتمثل في قصور الأطر التشريعية والتنظيمية في مواكبة التطورات المتسارعة في مجال التمويل الرقمي، مما يحدّ من فعالية سياسات إدارة المخاطر السيبرانية، **(OECD,2019)**. وعلاوة على ذلك، تمثل حماية البيانات والمعلومات الحساسة تحدياً جوهرياً في ظل الزيادة الكبيرة في حجم البيانات المتداولة عبر الأنظمة الرقمية، فضلاً عن ارتفاع تكاليف تطبيق أنظمة الأمن السيبراني المتقدمة وخطط الاستجابة للحوادث، الأمر الذي يتطلب من المصرف التجاري الوطني تعزيز استراتيجيات إدارة المخاطر السيبرانية لضمان استمرارية وكفاءة الخدمات المصرفية الرقمية وبناء الثقة لدى العملاء**(NIST,2018)**

الجانب العملي للدراسة:

يتناول هذا الجانب التطبيق العملي للدراسة من خلال عرض منهجية البحث والأدوات المستخدمة في جمع البيانات وتحليلها، حيث اعتمدت الدراسة على المنهج الوصفي والتحليلي لملاءمته لطبيعة موضوع الدراسة. وتم استخدام أداة الاستبانة لجمع البيانات من عدد من مدراء الأقسام وموظفي تقنية المعلومات والخدمات الإلكترونية وإدارة المخاطر والعمليات المصرفية، مع اختيار العينة القصدية لضمان تمثيل المشاركين ذوي الخبرة. وقد تم تحليل البيانات باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية(SPSS) ، تمهيدًا لعرض النتائج وتفسيرها.

أولاً: تحليل البيانات الديموغرافية:

يُظهر جدول الخصائص الديموغرافية أن تركيبة عينة الدراسة في المصرف التجاري الوطني – الإدارة العامة بمدينة البيضاء تتسم بتنوع تخصصي ووظيفي يعزز من موثوقية النتائج التفسيرية المتعلقة بموضوع التمويل الرقمي والمخاطر السيبرانية. فقد تصدّر تخصص إدارة الأعمال المرتبة الأولى بنسبة (36.7%)، يليه تخصص المحاسبة (24.5%) ثم التمويل والمصارف (14.3%)، وهي تخصصات ترتبط مباشرة بطبيعة العمل المصرفي والتحول الرقمي، ما يشير إلى أن غالبية المشاركين يمتلكون خلفية علمية ملائمة لفهم أبعاد الدراسة. في المقابل، بلغت نسبة التخصصات التقنية (تقنية معلومات وعلوم حاسوب) مجتمعة (12.3%)، ورغم أنها نسبة أقل، إلا أنها تمثل شريحة مهمة لأنها تعكس وجهة النظر الفنية المرتبطة بالبنية التحتية الرقمية وأمن المعلومات.

وعلى مستوى الوظائف، يتضح أن العينة تضم مستويات تنظيمية متنوعة؛ حيث جاءت فئة الوظائف الأخرى (مثل إدارة المشتريات والعقود) في المرتبة الأولى بنسبة (30.6%)، تليها وظيفة موظف إدارة مخاطر (24.5%)، ثم مديري الأقسام (16.3%). ويشير هذا التنوع الوظيفي إلى أن البيانات لم تقتصر على مستوى إداري واحد، بل شملت مستويات تشغيلية وإشرافية ورقابية، وهو ما يعزز شمولية الرؤية التحليلية للظاهرة المدروسة، خصوصاً أن إدارة المخاطر والعمليات والتقنية تمثل محاور أساسية في دراسة العلاقة بين التمويل الرقمي والتهديدات السيبرانية.

أما من حيث المستوى التعليمي، فتُظهر النتائج ارتفاع مستوى التأهيل العلمي للعينة؛ إذ يحمل (67.3%) درجة البكالوريوس و(4.1%) درجة الماجستير، ما يعني أن أكثر من ثلثي المشاركين يمتلكون تعليماً جامعياً، وهو مؤشر إيجابي يعكس قدرة المبحوثين على فهم مفاهيم الدراسة والاستجابة على بنود الاستبيان بدقة تحليلية. كما أن وجود نسبة (28.6%) من حملة الدبلوم يوفر تمثيلاً للكوادر الفنية والتطبيقية التي تتعامل مباشرة مع الأنظمة المصرفية الرقمية.

وفيما يتعلق بالخبرة المهنية، تُظهر النتائج توزيعاً متوازناً نسبياً؛ حيث بلغت نسبة من لديهم خبرة تزيد عن عشر سنوات (40.8%)، وهي أعلى فئة، ما يدل على أن جزءاً كبيراً من العينة يمتلك خبرة طويلة في العمل المصرفي قد تمكنه من تقييم التحولات الرقمية والمخاطر المرتبطة بها بصورة واقعية. وفي المقابل، بلغت نسبة من تقل خبرتهم عن خمس سنوات (38.8%)،

وهو ما يعكس وجود جيل وظيفي حديث نسبياً قد يكون أكثر احتكاكاً بالتقنيات الرقمية الحديثة. ويعزز هذا التوازن بين الخبرة الطويلة والحديثة من مصداقية النتائج، لأنه يجمع بين الخبرة التراكمية والرؤية المعاصرة للتكنولوجيا المالية.

بوجه عام، تشير الخصائص الديموغرافية للعينة إلى أنها عينة متنوعة، الأمر الذي يمنح نتائج الدراسة درجة عالية من المصداقية التفسيرية، ويجعل الاستنتاجات المتعلقة بعلاقة التمويل الرقمي بالمخاطر السيبرانية قائمة على آراء تمثل أطيافاً مختلفة من العاملين داخل البيئة المصرفية.

الجدول (1) يبين: الخصائص الديموغرافية للعينة

المتغير	الفئة	التكرار	النسبة المئوية
التخصص	إدارة أعمال	18	36.7
	محاسبة	12	24.5
	تمويل ومصارف	7	14.3
	أخرى (أذكرها)	6	12.2
	تقنية معلومات	4	8.2
	علوم حاسوب	2	4.1
	الإجمالي	**49**	**100**
الوظيفة	أخرى (أذكرها) -إدارة المشتريات -إدارة العقود	15	30.6
	موظف إدارة مخاطر	12	24.5
	مدير قسم	8	16.3
	موظف تقنية معلومات	7	14.3
	العلميات المصرفية	5	10.2
	موظف خدمات الكترونية	2	4.1
	الإجمالي	**49**	**100**
المستوى التعليمي	بكالوريوس	33	67.3
	دبلوم	14	28.6
	ماجستير	2	4.1
	الإجمالي	**49**	**100**
عدد سنوات الخبرة	أكثر من 10 سنوات	20	40.8
	أقل من 5 سنوات	19	38.8
	10-5سنوات	10	20.4
	الإجمالي	**49**	**100**

ثانيًا: اختبار توزيع البيانات:

تشير نتائج اختبار شابيرو–ويلك المعروضة في الجدول إلى أن جميع متغيرات الدراسة لا تتبع التوزيع الطبيعي، حيث جاءت قيم الدلالة الإحصائية لكل من التمويل الرقمي في المصرف (0.003)، وأمن المعلومات (0.023)، وإدارة العمليات الرقمية (0.009)، وتهديدات البيانات والمعلومات (0.002)، ووعي الموظفين بالمخاطر السيبرانية (0.008) أقل من مستوى المعنوية المعتمد

(0.05). وهذا يعني رفض الفرضية الصفرية القائلة بأن البيانات تتبع التوزيع الطبيعي، وقبول الفرضية البديلة التي تفيد بأن توزيع البيانات غير طبيعي إحصائياً. وتعكس هذه النتيجة نمطاً شائعاً في الدراسات الميدانية المعتمدة على بيانات الاستبيانات، خصوصاً في البيئات التنظيمية، حيث تتأثر الاستجابات باتجاهات الإدراك الفردي والخبرة المهنية ومستوى المعرفة التقنية.

ومن الناحية المنهجية، تترتب على هذه النتيجة آثار مباشرة على اختيار الأساليب الإحصائية المناسبة لتحليل البيانات واختبار الفرضيات. أن شرط الطبيعية غير متحقق، فإن استخدام الاختبارات المعلمية يصبح غير ملائم، الأمر الذي يستوجب الاعتماد على الاختبارات اللامعلمية الأكثر توافقاً مع طبيعة البيانات. وعليه، فإن اختيار **معاملات الارتباط الرتبية مثل سبيرمان** يُعد إجراءً منهجياً سليماً لاختبار علاقات الارتباط بين متغيرات الدراسة، لأنه لا يفترض التوزيع الطبيعي ويعتمد على ترتيب القيم بدلاً من قيمها الأصلية، مما يزيد من دقة النتائج وموثوقيتها.

الجدول (2) يبين: اختبار الطبيعي

المتغير	شابيرو-ويلك	التوزيع
التمويل الرقمي في المصرف	.003	**غير طبيعي**
أمن المعلومات	.023	**غير طبيعي**
إدارة العمليات الرقمية	.009	**غير طبيعي**
تهديدات البيانات والمعلومات	.002	**غير طبيعي**
وعي الموظفين بالمخاطر السيبرانية	.008	**غير طبيعي**

ثالثًا: اختبار ثبات وصدق مقاييس الدراسة:

تُظهر نتائج اختبار الصدق والثبات في الجدول أن أداة القياس المستخدمة في الدراسة تتمتع بدرجة جيدة من الاتساق الداخلي والقدرة على قياس المتغيرات المستهدفة بدقة، حيث تراوحت معاملات الثبات بين (0.601–0.939)، وهي قيم تشير إجمالاً إلى مستوى ثبات مقبول إلى مرتفع وفق المعايير الإحصائية المعتمدة في البحوث السلوكية والإدارية. فقد سجل متغير أمن المعلومات أعلى معامل ثبات بلغ (0.939)، ما يدل على تجانس مرتفع بين فقراته وقدرته على قياس المفهوم بصورة مستقرة، يليه متغير تهديدات البيانات والمعلومات (0.861)، ثم إدارة العمليات الرقمية (0.818)، وأخيراً التمويل الرقمي في المصرف (0.798)، وجميعها تقع ضمن نطاق الثبات الجيد الذي يسمح بالاعتماد عليها في التحليل الإحصائي واختبار الفرضيات.

أما متغير وعي الموظفين بالمخاطر السيبرانية فقد بلغ معامل الثبات له (0.601)، وهي قيمة تقع ضمن الحد الأدنى المقبول إحصائياً في الدراسات الاستكشافية، وتشير إلى أن المقياس لا يزال صالحاً للاستخدام لكنه أقل اتساقاً من بقية المقاييس. وقد يعزى ذلك إلى طبيعة هذا المتغير الإدراكية التي تتأثر بعوامل شخصية وخبرات فردية ومستويات معرفة تقنية متفاوتة بين المبحوثين، الأمر الذي يؤدي إلى تباين الاستجابات وانخفاض درجة التجانس بين الفقرات.

وفيما يتعلق بمعاملات الصدق، فقد سجلت جميع المتغيرات قيماً مرتفعة تراوحت بين (0.775–0.969)، وهي مؤشرات قوية على أن الفقرات المستخدمة تقيس فعلاً المفاهيم التي صُممت لقياسها. ويُلاحظ أن أعلى قيمة صدق كانت أيضاً لمتغير أمن المعلومات (0.969)، وهو ما يعكس دقة بناء فقراته ووضوحها المفاهيمي لدى المبحوثين. كما أن جميع معاملات الصدق تجاوزت الحد المقبول علمياً (0.70)، مما يؤكد سلامة البناء المنهجي للأداة البحثية.

وبصورة عامة، يمكن القول إن نتائج الصدق والثبات تدعم صلاحية أداة الدراسة للاستخدام في اختبار العلاقات بين متغيرات التمويل الرقمي والمخاطر السيبرانية، إذ إن ارتفاع معاملات الثبات والصدق لمعظم المتغيرات يشير إلى أن البيانات التي تم جمعها تتمتع بدرجة عالية من الموثوقية، وبالتالي فإن النتائج التحليلية اللاحقة يمكن تفسيرها بثقة علمية معقولة.

الجدول (3) يبين: اختبار الصدق والثبات

المتغير	عدد الفقرات	معامل الثبات	معامل الصدق
التمويل الرقمي في المصرف	5	0.798	**0.893**
أمن المعلومات	5	0.939	**0.969**
إدارة العمليات الرقمية	5	0.818	**0.904**
تهديدات البيانات والمعلومات	5	0.861	**0.927**
وعي الموظفين بالمخاطر السيبرانية	5	0.601	**0.775**

رابعًا: اختبار الفرضيات:

1. توجد علاقة ذات دلالة إحصائية بين التمويل الرقمي في المصرف وأمن المعلومات.
2. توجد علاقة ذات دلالة إحصائية بين التمويل الرقمي في المصرف وإدارة العمليات الرقمية.
3. توجد علاقة ذات دلالة إحصائية بين التمويل الرقمي في المصرف وتهديدات البيانات والمعلومات.
4. توجد علاقة ذات دلالة إحصائية بين أمن المعلومات وإدارة العمليات الرقمية.
5. توجد علاقة ذات دلالة إحصائية بين أمن المعلومات وتهديدات البيانات والمعلومات.

تُظهر نتائج اختبار معاملات الارتباط باستخدام معامل سبيرمان وجود تباين واضح في طبيعة العلاقات بين متغيرات الدراسة، وهو ما يعكس تعقيد التفاعلات بين أبعاد التمويل الرقمي والمخاطر السيبرانية داخل البيئة المصرفية. فقد بينت النتائج وجود علاقة ارتباط موجبة ذات دلالة إحصائية بين التمويل الرقمي وأمن المعلومات، حيث بلغ معامل الارتباط (0.543) عند مستوى دلالة (0.000)، ما يشير إلى أنه كلما ارتفع مستوى تطبيق التمويل الرقمي تحسن مستوى أمن المعلومات. وتدل هذه النتيجة على أن التحول الرقمي المصرفي لا يؤدي بالضرورة إلى زيادة المخاطر كما يُفترض أحياناً، بل قد يرتبط بتعزيز البنية الأمنية نتيجة الاستثمار في الأنظمة والحلول التقنية المصاحبة للتحول الرقمي.

كما أظهرت النتائج وجود علاقة موجبة معنوية بين التمويل الرقمي وإدارة العمليات الرقمية بمعامل ارتباط (0.587)، وهو ارتباط متوسط يميل إلى القوة، مما يعكس أن التوسع في تطبيقات التمويل الرقمي يرتبط بتطور كفاءة إدارة العمليات الرقمية داخل المصرف. ويمكن تفسير ذلك بأن المؤسسات المصرفية التي تتبنى الخدمات الرقمية تضطر بطبيعتها إلى تطوير أنظمة التشغيل، وأتمتة الإجراءات، وتحسين تدفق البيانات، وهو ما ينعكس على مستوى كفاءة العمليات الرقمية. وتدعم هذه النتيجة الطرح النظري الذي يرى أن التحول الرقمي عملية متكاملة تشمل البنية التشغيلية وليس فقط الخدمات المقدمة للعملاء.

في المقابل، لم تظهر النتائج وجود علاقة ذات دلالة إحصائية بين التمويل الرقمي وتهديدات البيانات والمعلومات، إذ بلغ معامل الارتباط (-0.163) بمستوى دلالة (0.264)، وهي قيمة غير معنوية. وتشير هذه النتيجة إلى أن مستوى التهديدات السيبرانية لا يرتبط مباشرة بدرجة تطبيق التمويل الرقمي، ما يعني أن التهديدات قد تكون مرتبطة بعوامل أخرى مثل سياسات الحماية أو مستوى الوعي الأمني أو البنية التقنية، وليس بمجرد وجود أنظمة تمويل رقمية بحد ذاتها. وهذا الاستنتاج مهم لأنه يفصل بين مفهوم التوسع الرقمي ومفهوم التعرض للمخاطر، ويؤكد أن العلاقة ليست حتمية.

ومن جهة أخرى، أظهرت النتائج أقوى علاقة ارتباط في الجدول بين أمن المعلومات وإدارة العمليات الرقمية، حيث بلغ معامل الارتباط (0.692) عند مستوى دلالة (0.000)، وهي علاقة قوية نسبياً. وتعكس هذه النتيجة ترابطاً هيكلياً بين النظام الأمني والنظام التشغيلي، إذ إن كفاءة العمليات الرقمية تعتمد بدرجة كبيرة على قوة أنظمة الحماية وضبط الوصول وإدارة الصلاحيات وسلامة قواعد البيانات. كما يمكن تفسير ذلك بأن المؤسسات التي تمتلك إدارة رقمية منظمة تميل إلى تبني سياسات أمنية أكثر صرامة، مما يخلق علاقة تكاملية بين المتغيرين.

أما فيما يتعلق بالعلاقة بين أمن المعلومات وتهديدات البيانات، فقد تبين عدم وجود علاقة معنوية إحصائياً، حيث بلغ معامل الارتباط (-0.156) ومستوى الدلالة (0.283). وتوحي هذه النتيجة بأن مستوى التهديدات المدركة لا يتأثر مباشرة بمستوى إجراءات الأمن المطبقة، وهو ما قد يعكس وجود فجوة إدراكية لدى الموظفين أو محدودية اطلاعهم على حجم التهديدات الفعلية. وقد يكون السبب أيضاً أن التهديدات السيبرانية ظاهرة ديناميكية متغيرة تتأثر بعوامل خارجية مثل طبيعة الهجمات والتطور التكنولوجي وليس فقط بالإجراءات الداخلية.

وأخيراً، لم تظهر النتائج علاقة ذات دلالة إحصائية بين إدارة العمليات الرقمية وتهديدات البيانات، إذ بلغ معامل الارتباط (0.030) عند مستوى دلالة (0.840)، وهي قيمة شبه معدومة. ويعني ذلك أن مستوى كفاءة العمليات الرقمية لا يرتبط بزيادة أو انخفاض التهديدات، مما يشير إلى أن التهديدات السيبرانية ليست ناتجة عن طبيعة إدارة العمليات بقدر ما هي مرتبطة بعوامل أمنية وتقنية متخصصة. وتؤكد هذه النتيجة أن تحسين الكفاءة التشغيلية لا يؤدي تلقائياً إلى تقليل المخاطر السيبرانية ما لم يصاحبه تطوير موازٍ في منظومة الحماية.

بصورة إجمالية، تكشف نتائج اختبار الفرضيات أن العلاقات المعنوية ظهرت بين المتغيرات التشغيلية والتنظيمية المرتبطة بالتحول الرقمي (التمويل الرقمي، أمن المعلومات، إدارة العمليات)، في حين لم تظهر علاقات معنوية مع متغير التهديدات السيبرانية، وهو ما يشير إلى أن المخاطر السيبرانية تمثل بُعداً مستقلاً نسبياً يتأثر بعوامل مختلفة عن العوامل التنظيمية الداخلية، الأمر الذي يستدعي دراسته ضمن نماذج تفسيرية أوسع تأخذ في الاعتبار المتغيرات التقنية والسلوكية والبيئية.

الجدول (4) يبين: العلاقات الارتباطية بين متغيرات الدراسة

م	الفرضية	معامل الارتباط (Spearman)	مستوى الدلالة (Sig.)	النتيجة
1	توجد علاقة بين التمويل الرقمي وأمن المعلومات	.543**	0.000	علاقة معنوية (موجبة)
2	توجد علاقة بين التمويل الرقمي وإدارة العمليات الرقمية	.587**	0.000	علاقة معنوية (موجبة)
3	توجد علاقة بين التمويل الرقمي وتهديدات البيانات	-.163	0.264	علاقة غير معنوية
4	توجد علاقة بين أمن المعلومات وإدارة العمليات الرقمية	.692**	0.000	علاقة معنوية (موجبة)
5	توجد علاقة بين أمن المعلومات وتهديدات البيانات	-.156	0.283	علاقة غير معنوية
6	توجد علاقة بين إدارة العمليات الرقمية وتهديدات البيانات	.030	0.840	علاقة غير معنوية

****. الارتباط ذو دلالة إحصائية عند مستوى 0.01**

خامسًا: تحليل المضمون لمقترحات المستجيبين

تشير نتائج تحليل المضمون لمقترحات المستجيبين إلى وجود تركيز واضح على تعزيز الأمن السيبراني ودعم التمويل الرقمي بشكل متوازي، وهو ما يعكس وعي الموظفين بأهمية الربط بين حماية البيانات وتطوير الخدمات الرقمية. فقد اقترح المستجيبين وضع استراتيجية شاملة للأمن السيبراني وتحديث أنظمة أمن المعلومات بشكل مستمر، إضافة إلى التطوير المستمر للمنظومة الأمنية، وهو ما يدل على إدراكهم لحساسية البيئة الرقمية المصرفية وضرورة وجود سياسات منهجية للحماية من التهديدات السيبرانية المحتملة.

أما فيما يخص مقترحات تحسين خدمات التمويل الرقمي، فقد ركز المستجيبون على تحسين البنية التحتية الرقمية وتحديث أنظمة الحوسبة، مع أهمية التدريب المستمر والبرامج التأهيلية للموظفين. هذا يشير إلى أن تحسين جودة الخدمات

الرقمية لا يقتصر على الجانب التقني فقط، بل يشمل رفع كفاءة الموظفين وتطوير مهاراتهم لضمان تقديم خدمات تمويلية رقمية آمنة وفعالة، وتعزيز تجربة العملاء في المصرف.

وبشكل عام، يمكن استخلاص أن المستجيبين يرون أن التحول الرقمي الفعّال يعتمد على تكامل الجوانب التقنية والأمنية والتدريبية، حيث يشكل الاستثمار في الأمن السيبراني والتدريب المستمر ركيزة أساسية لدعم تطبيقات التمويل الرقمي، وهو ما يتوافق مع ممارسات أفضل المصارف العالمية في إدارة المخاطر الرقمية. كما تعكس هذه المقترحات فهم الموظفين للعلاقة التكاملية بين الأمن السيبراني وكفاءة العمليات الرقمية، وضرورة اعتماد نهج استباقي لتعزيز الحماية وتقليل المخاطر المرتبطة بالتمويل الرقمي.

الجدول (5) يبين: تحليل المضمون لمقترحات المستجيبين

مقترحات إجراءات تعزيز الامن السيبراني لدعم التمويل	مقترحات تحسين خدمات التمويل الرقمي
وضع استراتيجية للأمن السيبراني	تحسين البنية التحتية والأمن السيبراني
تحديث أمن المعلومات	تحديث أنظمة الحوسبة
التطوير المستمر	الدورات التدريبية
تطوير المنظومة الأمنية	التدريب المستمر

النتائج والتوصيات:

أولاً: نتائج الدراسة

توصلت الدراسة إلى مجموعة من النتائج، أهمها ما يلي:

1- وجود علاقة ارتباط إيجابية ذات دلالة إحصائية بين التمويل الرقمي وأمن المعلومات، مما يدل على أن التوسع في الخدمات الرقمية يسهم في تعزيز الجوانب الأمنية داخل المصرف.

2- وجود علاقة ارتباط ذات دلالة إحصائية بين التمويل الرقمي وإدارة العمليات الرقمية، بما يعكس دور التحول الرقمي في تحسين كفاءة التنظيم والتشغيل المصرفي.

3- وجود علاقة إيجابية ذات دلالة إحصائية بين أمن المعلومات وإدارة العمليات الرقمية، الأمر الذي يشير إلى التكامل بين الجوانب الأمنية والإدارية في دعم الأداء المؤسسي.

4- عدم وجود علاقة ذات دلالة إحصائية بين أبعاد التمويل الرقمي وتهديدات البيانات والمعلومات.

5- عدم وجود علاقة ذات دلالة إحصائية بين أمن المعلومات وتهديدات البيانات.

6- عدم وجود علاقة ذات دلالة إحصائية بين إدارة العمليات الرقمية وتهديدات البيانات، مما يشير إلى أن المخاطر السيبرانية تمثل بُعدًا مستقلاً قد يتأثر بعوامل أخرى خارج نطاق متغيرات الدراسة.

ثانياً: توصيات الدراسة:

في ضوء النتائج التي تم التوصل إليها، توصي الدراسة بما يلي:

1- ضرورة دمج الأمن السيبراني ضمن استراتيجيات التحول الرقمي في المصارف لضمان حماية البيانات والمعاملات الإلكترونية.

2- العمل على التحديث المستمر لأنظمة أمن المعلومات والبنية التحتية الرقمية بما يتواكب مع التطورات التقنية الحديثة.

3- تعزيز برامج التدريب والتأهيل للموظفين في مجال الأمن السيبراني ورفع مستوى الوعي بالمخاطر الرقمية.

4- تطوير سياسات وإجراءات وقائية تسهم في الحد من تهديدات البيانات وتعزيز استدامة الخدمات المصرفية الرقمية.

المراجع

. إبراهيم، طاهر فرج. (2025) تقنيات التحول الرقمي وأثرها على فعالية نظم المعلومات المحاسبية "دراسة ميدانية على المصارف التجارية الليبية". مجلة الدراسات الاقتصادية، 8(2)

. بنعايي، رحيمة، وسيلكا، إبراهيم. (2025) الأمن السيبراني كضرورة لتعزيز الثقة في الخدمات المالية الرقمية. مجلة بحوث الاقتصاد والتسيير، 9(1)، 7255

. التائب، على مفتاح، السائح، جبريل عمر. (2025) أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية" دراسة تطبيقية على المصارف التجارية العاملة في مدينة سرت". مجلة الدراسات الاقتصادية، 8(1)

. جارالله، زهراء حمو. (2023) استخدام التمويل الرقمي في تعزيز الاستقرار المالي" دراسة تحليلية لعينة من المصارف الاهلية في محافظة نينوى". مجلة الريادة للمال والاعمال، 4(3)

. جغل، جميلة، وزقرير، عادل. (2023) الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي. مجلة الاقتصاد والتنمية المستدامة، 7(2)، 150.133

. حدود، امال 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)

. حشروف، فاطمة الزهراء، صديقي، وحيدة. (2025) الأمن السيبراني في البنوك الجزائرية التحديات والاستراتيجيات. مجلة دفاتر اقتصادية، 16(1)

. خنفر، الصديق محمد، اكريم، حمزة محمد. (2022) أثر إدارة محاطر التحول الرقمي في تحسين كفاءة أمن المعلومات "دراسة على المصارف التجارية الليبية". المجلة الافريقية للدراسات المتقدمة في العلوم الإنسانية والاجتماعية، 1(4)

. الشتيوي،حسني رمضان. (2024) أثر تطبيق التحول الرقمي في المصارف الإسلامية الليبية على تطوير مهنة المحاسبة والمراجعة. مجلة دراسات محاسبية، (5)

. رزاق، عبير. (2024) الأمن السيبراني في القطاع الحكومي، المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة

. سالم، فاطمة عبدالرحمن. (2020) الأمن السيبراني وحماية نظم المعلومات في القطاع المالي. مجلة الدراسات الإدارية، 12(3)، 118.101

. الطاهر، على محمود. (2022) التحويل الرقمي في المؤسسات المصرفية وأثرة على الأداء المالي. مجلة البحوث الاقتصادية، 18(1)، 94.77

. عبدالله، محمد أحمد. (2021) التمويل الرقمي ودورة في تطوير الخدمات المصرفية. مجلة العلوم المالية والمصرفية، 13(2)، 6245

. عبدالسميع، بابا عربى، وآخرون. (2024) دور التمويل الرقمي في تنمية التجارة الخارجية(رسالة ماجستير). كلية العلوم الاقتصادية والتجارية وعلوم التسيير، الجزائر

. لينة، الواهم مصابح. (2023) دور تقنيات التمويل الرقمي في تسريع وتيرة التحول إلى الاقتصاد الرقمي(رسالة ماجستير). كلية العلوم الاقتصادية والتجارية وعلوم التسيير، الجزائر

. وليد، كرادم شرة. (2023) أثر التمويل الرقمي على الاستقرار والشمول المالي" دراسة حالة على البنك الوطني الجزائري عين تموشنت(رسالة ماجستير). كلية العلوم الاقتصادية والتجارية وعلوم التسيير، الجزائر

. يحياوي، فطيمة. (2024) المخاطر السيبرانية في شركات التأمين التكافلي وسبل إدارتها. المجلة الجزائرية للعولمة والسياسات الاقتصادية، 15(1)

.Bank for International Settlements (BIS).(2018) Sound practices; implications of fintech developments for bank and bank supervisors.

.Gomber, p ., Koch, J. A., & Siering, M.(2017). Digital Finance and Fintech: Current research and future research directions. Journal of Business Economics, 87, 537-580.

.International Organization for Standardization (ISO/IEC27001).(2013) Information technology – Security techniques Information security management Systems.

.National Institute of Standards and Technology (NIST). (2018) Framework for Improving Critical Infrastructure Cybersecurity.

.Organisation for Economic Co- operation and Development (OECD). (2019) Digital Security Risk Management.

. Ozili, P.k (2018). Impact of digital finance on financial inclusion and Stability. Borsa-Istanbul Review, PP.333-334, April 18.

.World Bank. (2020) Cybersecurity and Financial Consumer Protection in Digital Finance.