Al-Farouk journal of sciences
Volume (2), Issue (3) (JUNE, 2026)
ISSN: 3135-2359

مجلة الفاروق للعلوم
المجلد (2) ملحق العدد 3 يونيو 2026
ردمد: 3135-2359

دور تكنولوجيا المعلومات في الحد من المخاطر السيبرانية في القطاع المصرفي

دراسة تطبيقية على المصارف التجارية (مصارف الجمهورية) لمدينة طرابلس

مصباح المختار أبو ضوة المعهد العالي للعلوم والتقنية الزهراء mosbahabodawam@gmail.com
محمد فرج التومي الهيئة الليبية للبحث العلمي Mohamedaltoumi@gmail.com

The Role of Information Technology in Mitigating Cyber Risks in the Banking Sector: An Applied Study on Commercial Banks (Republic Banks) in Tripoli

Mosbah Al-Mukhtar Abu Dawa, Higher Institute of Science and Technology, Al-Zahraa
Mohamed Faraj Al-Toumi, Libyan Authority for Scientific Research

تاريخ الاستلام: 2026/05/24 تاريخ المراجعة 2026/06/16 تاريخ القبول:2026/06/28- تاريخ النشر:2026/07/19

الملخص:

هدفت هذه الدراسة إلى تقييم دور تكنولوجيا المعلومات في الحد من المخاطر السيبرانية بمصرف الجمهورية في طرابلس، باستخدام المنهج الوصفي التحليلي. شملت الدراسة عينة من 60 موظفاً عبر استبانة مكونة من 20 فقرة، وتم تحليل البيانات إحصائياً بواسطة برنامج (**SPSS**)، أظهرت النتائج مستوى مرتفعاً في تطبيق البنية التحتية، والبرمجيات، وتأهيل الكوادر البشرية، مع وجود علاقة ذات دلالة إحصائية بين هذه الأبعاد والحد من المخاطر السيبرانية. وأكدت الدراسة أن التكنولوجيا تسهم بفاعلية في تقليل الحوادث الأمنية، وحماية الأصول المالية، وضمان استمرارية الخدمات المصرفية وسرعة الاستجابة للهجمات، وخلصت الدراسة إلى توصيات بضرورة التحديث المستمر للبنية التقنية، وتكثيف برامج التدريب المتخصص للعاملين، وتطوير سياسات حماية البيانات وفق المعايير الدولية، بما يضمن تعزيز الأمن الرقمي ورفع كفاءة الأداء المصرفي في مواجهة التهديدات المتنامية.

الكلمات المفتاحية:تكنولوجيا المعلومات -مخاطر السيبرانية- القطاع المصرفي

Summary: This study aimed to evaluate the role of Information Technology (IT) in mitigating cyber risks at Jumhouria Bank in Tripoli, employing a descriptive-analytical approach. The research involved a sample of 60 employees through a 20-item questionnaire, with data statistically analyzed using SPSS software The findings revealed a high level of implementation across infrastructure, software systems, and human resource development, establishing a statistically significant relationship between these dimensions and the reduction of cyber risks. The study confirmed that technology effectively contributes to minimizing security incidents, safeguarding financial assets, ensuring the continuity of banking services, and enhancing response speed to cyberattacks, The study concluded with recommendations for the continuous modernization of technical infrastructure, intensifying specialized training programs for staff, and developing data protection policies aligned with

international standards to bolster digital security and banking performance amidst evolving threats.

Keywords: Information Technology (IT) – Cyber Risks – Banking Sector.

المقدمـة:

تأتي هذه الورقة البحثية في لدراسةالدور تكنولوجيا المعلومات في الحد من مخاطر السيبرانية في القطاع المصرفي – دراسة تطبيقية على المصارف التجارية (مصارف الحمهورية) لمدينة طرابلس، فقد أظهرت التطورات التقنية الحديثة أن الاعتماد المتزايد على تكنولوجيا المعلومات في تقديم الخدمات المصرفية يسهم في تحسين الكفاءة وسرعة المعاملات، لكنه في الوقت ذاته يرفع من مستوى التعرض للحد من مخاطر السيبرانية.

يشهد القطاع المصرفي العالمي تحولاً رقمياً متسارعاً، مما أدى إلى زيادة الاعتماد على تكنولوجيا المعلومات في تقديم الخدمات المصرفية وإدارة العمليات المالية. ومع هذا التطور، تزايدت أيضاً المخاطر السيبرانية التي تهدد أمن وسلامة الأنظمة المصرفية والبيانات الحساسة للعملاء . تُعد الهجمات السيبرانية من أبرز التحديات التي تواجه المؤسسات المالية، حيث يمكن أن تؤدي إلى خسائر مالية فادحة، وتشويه للسمعة، وفقدان لثقة العملاء في ليبيا، وعلى غرار العديد من الدول، يواجه القطاع المصرفي تحديات كبيرة في مواجهة هذه المخاطر المتزايدة. وقد أشارت بعض التقارير إلى تعرض مؤسسات مالية ليبية لهجمات سيبرانية، مما يؤكد الحاجة الملحة لتعزيز آليات الدفاع السيبراني . وفي هذا السياق، تبرز أهمية تكنولوجيا المعلومات ليس فقط كأداة للتحول الرقمي، بل كخط دفاع أساسي للحد من المخاطر السيبرانية وضمان استمرارية الأعمال المصرفية.

تتناول هذه الدراسة دور تكنولوجيا المعلومات في تعزيز الأمن السيبراني في القطاع المصرفي الليبي، مع التركيز بشكل خاص على مصارف الجمهورية بمدينة طرابلس، وذلك بهدف تحديد مدى فعالية الإجراءات المتبعة في حماية الأنظمة والبيانات من التهديدات السيبرانية المتنامية.

الدراسات السابقة:

دراسة عبدالرحمن، 2022، بعنوان: دور حوكمة تكنولوجيا المعلومات فى إدارة المخاطر السيبرانية للقطاع المصرفي: هدفت إلى في التعرف على دور حوكمة تكنولوجيا المعلومات فى إدارة المخاطر السيبرانية للقطاع المصرفي، واستخدمت المنهج الاستقرائي والاستنباطي، وتم تطبيق الاستبيان على عينة بلغت (96) من المدراء الماليين وخبراء تكنولوجيا المعلومات، ومسئولي إدارة المخاطر السيبرانية، وتوصلت النتائج إلى: تتمثل أهم معوقات تطبيق حوكمة تكنولوجيا المعلومات في: لا توجد لجنة لتكنولوجيا المعلومات تابعة لمجلس إدارة القطاع المصرفي. السماح لغير المصرح لهم بالدخول إلى برامج القطاع المصرفي المختلفة، تتمثل أهم محددات المخاطر السيبرانية بالقطاع المصرفي في: قيام المصارف بتعزيز حماية المؤسسة من الهجمات الإلكترونية بكافة أشكالها. قيام المصارف بالتأكد من صحة المعاملات والمسؤولية من خلال العمليات الإلكترونية وتسهم حوكمة التكنولوجيا في إدارة المخاطر السيبرانية في القطاع المصرفي، حيث توفر حوكمة التكنولوجيا الاعتماد على مصادر مرخصة وموثوقة لأدوات تطوير التطبيقات، كما تقدم حوكمة التكنولوجيا الاستشارات اللازمة عند تصميم وتحسين إستراتيجيات إدارة المخاطر السيبرانية في ظل حوكمة تكنولوجيا المعلومات.

دراسة القصير، 2024، بعنوان: حوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة: هدفت الدراسة لاقتراح نموذج لحوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة واتبعت الدراسة المنهج الوصفي التحليلي من خلال مراجعة الدراسات السابقة والتقارير والنماذج وأفضل الممارسات والأدبيات ذات العلاقة, وخلصت الدراسة أن حوكمة تقنية المعلومات لها دور إيجابي في الحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية وتمثلت أهم ركائز النموذج المقترح في : الحوكمة ولجنة حوكمة تقنية المعلومات وآلياتها واستقلالية المراجع الداخلي مع التأكيد على كل من إدارة المخاطر, الرقابة النشطة والمستمرة, الشفافية والمساءلة وأوصت الدراسة بضرورة تبني المؤسسات الليبية العامة الحوكمة وحوكمة تقنية المعلومات.

دراسة جدار، 2025، بعنوان: دور حوكمة تكنولوجيا المعلومات في تحسين جودة المعلومات المحاسبية وإدارة المخاطر السيبرانية: هدفت الدراسة إلى التعرف علىدور حوكمة تكنولوجيا المعلومات في تحسين جودة المعلومات المحاسبية وإدارة المخاطر السيبرانيةحيث تؤكد الدراسة على أهمية حوكمة تكنولوجيا المعلومات في تعزيز جودة القوائم المالية وإدارة المخاطر السيبرانية. فمن خلال تطبيق أطر حوكمة معيارية مثل COBIT و ISO 27001، واعتماد أنظمة مالية متطورة، يمكن للمؤسسات تحسين دقة وموثوقية بياناتها المالية. كما أن إنشاء وحدات متخصصة لإدارة المخاطر السيبرانية، وتنفيذ برامج تدريبية مستمرة، يسهمان في تعزيز الأمن الرقمي. وأخيرا، يوصي البحث بضرورة التكامل بين الإدارات المالية والتقنية، ومواكبة التطورات التكنولوجية لضمان شفافية القوائم المالية وفعالية إدارة المخاطر في البيئة الرقمية المتغيرة.

دراسة ، 2026، بعنوان:أثر تطبيق معايير الأمن السيبراني في الحد من المخاطر في البنوك التجارية بمدينة الرياض:هدفت هذه الدراسة إلى تحليل أثر تطبيق معايير الأمن السيبراني في الحد من المخاطر في البنوك التجارية بمدينة الرياض، في ظل التحول الرقمي المتسارع الذي جعل حماية المعلومات واستمرارية العمليات ضرورة استراتيجية للقطاع المالي. استخدمت الدراسة المنهج الكمي، واعتمدت على الاستبانة الإلكترونية أداةً لجمع البيانات من عينة قصدية من العاملين في إدارات الأمن السيبراني وإدارة المخاطر وتقنية المعلومات في البنوك التجارية. وتناولت الدراسة ثلاثة أبعاد رئيسة لمعايير الأمن السيبراني، هي: أمن الأفراد، وأمن ضبط المعلومات، والأمن المادي، وقيست آثارها على المخاطر الكلية باستخدام تحليل الانحدار المتعدد عبر برنامج SPSS. وأظهرت النتائج أن تطبيق معايير الأمن السيبراني أسهم بفاعلية في خفض مستوى المخاطر التشغيلية والمعلوماتية والامتثالية، وأن بُعد أمن ضبط المعلومات كان الأكثر تأثيرًا، يليه أمن الأفراد ثم الأمن المادي، وأوصت الدراسة بضرورة دمج الأطر الأمنية ضمن استراتيجيات التحول الرقمي للبنوك السعودية، وتعزيز التدريب والوعي الأمني للعاملين بما يحقق بيئة مصرفية أكثر أمانًا واستدامة، انسجامًا مع رؤية السعودية 2030.

مشكلة الدراسة:

برغم من الاهتمام المتزايد بموضوع الأمن السيبراني في القطاع المصرفي على المستوى العالمي، إلا أن الدراسات التطبيقية التي تتناول هذا الموضوع في البيئة الليبية لا تزال محدودة. معظم الدراسات السابقة ركزت إما على حوكمة تقنية المعلومات بشكل عام ، أو على تأثير المخاطر السيبرانية على المرونة المالية ، دون التعمق في الدور الفعلي والعملي لتكنولوجيا المعلومات كأداة وقائية وعلاجية للحد من هذه المخاطر داخل بيئة عمل محددة، كما تتمثل الفجوة البحثية التي

تسعى هذه الدراسة لسدها في ندرة الدراسات الميدانية التي تقيم واقع استخدام تكنولوجيا المعلومات في الحد من المخاطر السيبرانية في المصارف التجارية الليبية، وتحديداً "مصرف الجمهورية" بمدينة طرابلس، والذي يُعد من أكبر المصارف في ليبيا. وبالتالي، تأتي هذه الدراسة لتقديم إطار تحليلي وتطبيقي يربط بين آليات تكنولوجيا المعلومات المتاحة ومستوى الحماية السيبرانية الفعلي في هذا المصرف، تواجه المصارف الليبية وفي مقدمتها مصرف الجمهورية، تحديات متنامية نتيجة التحول نحو الخدمات المصرفية الإلكترونية والرقمية. هذا التحول، رغم فوائده الكبيرة في تسهيل الخدمات، فتح الباب أمام تهديدات سيبرانية معقدة ومتطورة، مثل الاختراقات، وسرقة البيانات، وهجمات الفدية، والتي قد تؤدي إلى شلل في العمليات المصرفية وفقدان ثقة المودعين. وفي ظل بيئة تتسم بالتحديات التقنية والتنظيمية، تبرز الحاجة الماسة لتقييم مدى قدرة البنية التحتية لتكنولوجيا المعلومات في مصرف الجمهورية على التصدي لهذه المخاطر. إن المشكلة تكمن في عدم وضوح الرؤية حول مدى كفاءة وفعالية التقنيات والبرمجيات والسياسات الأمنية المتبعة حالياً في المصرف للحد من التهديدات السيبرانية، وما إذا كانت هذه التقنيات تواكب التطور السريع في أساليب الهجوم الإلكتروني، تتمثل مشكلة الدراسة في التساؤل الرئيسي التالي: **ما هو دور تكنولوجيا المعلومات في الحد من المخاطر السيبرانية في مصارف الجمهورية بمدينة طرابلس؟** ويتفرع من هذا التساؤل الأسئلة الفرعية التالية:

1. ما هي أبرز المخاطر السيبرانية التي تواجه مصارف الجمهورية بمدينة طرابلس؟
2. ما هي آليات تكنولوجيا المعلومات المستخدمة حالياً في مصارف الجمهورية للحد من هذه المخاطر؟
3. ما مدى فعالية هذه الآليات في تحقيق الأمن السيبراني وحماية الأنظمة والبيانات المصرفية؟
4. ما هي التحديات التي تواجه مصارف الجمهورية في تطبيق تكنولوجيا المعلومات للحد من المخاطر السيبرانية؟

أهداف الدراسة: تهدف هذه الدراسة إلى تحقيق الأهداف الرئيسية التالية:

1. تحديد وتحليل أبرز المخاطر السيبرانية التي تواجه مصارف الجمهورية بمدينة طرابلس.
2. التعرف على آليات تكنولوجيا المعلومات المطبقة في مصارف الجمهورية للحد من المخاطر السيبرانية.
3. تقييم فعالية تكنولوجيا المعلومات في تعزيز الأمن السيبراني وحماية الأنظمة والبيانات المصرفية في مصارف الجمهورية.
4. اقتراح توصيات لتحسين دور تكنولوجيا المعلومات في الحد من المخاطر السيبرانية في مصارف الجمهورية بمدينة طرابلس.

أهمية الدراسة: تكتسب هذه الدراسة أهمية بالغة من عدة جوانب:

1. الأهمية بالنسبة للباحث:تساهم الدراسة في تعميق فهم الباحث للمخاطر السيبرانية وتحدياتها في القطاع المصرفي، ودور تكنولوجيا المعلومات في مواجهتها، وتتيح للباحث فرصة لتطبيق المعرفة النظرية في سياق عملي، واكتساب خبرة في تحليل المشكلات الأمنية وتقديم الحلول، وتعد إضافة للمكتبة العلمية في مجال الأمن السيبراني وتكنولوجيا المعلومات في القطاع المصرفي الليبي، والذي لا يزال بحاجة إلى المزيد من الدراسات المتخصصة.

2. الأهمية بالنسبة للعلم:تساهم الدراسة في إثراء الأدبيات العلمية المتعلقة بالأمن السيبراني وحوكمة تكنولوجيا المعلومات في القطاع المصرفي، خاصة في البيئات النامية مثل ليبيا، وتقدم نموذجاً تطبيقياً يمكن أن يستفيد منه الباحثون الآخرون في دراسات مشابهة، أو في تطوير أطر عمل للأمن السيبراني، وتسلط الضوء على الفجوات البحثية في هذا المجال، مما يفتح آفاقاً لدراسات مستقبلية.

3. الأهمية بالنسبة للمؤسسة (مصارف الجمهورية):تساعد الدراسة إدارة مصارف الجمهورية على فهم أعمق للمخاطر السيبرانية التي تواجهها، وتحديد نقاط الضعف في أنظمتها الأمنية، وتقدم توصيات عملية ومبنية على أسس علمية لتحسين البنية التحتية لتكنولوجيا المعلومات وتعزيز إجراءات الأمن السيبراني، وتساهم في حماية الأصول المالية للمصرف وسمعته، وتعزيز ثقة العملاء في الخدمات المصرفية الرقمية، كما تدعم جهود المصرف في الامتثال للمعايير واللوائح المحلية والدولية المتعلقة بالأمن السيبراني.

فرضيات الدراسة : *يعتمد الدراسة البحث على الفرضية الرئيسية: لا* يوجد دور ذو دلالة إحصائية لتكنولوجيا المعلومات (الأجهزة، البرمجياتو الشبكات، والكوادر البشرية) في الحد من المخاطر السيبرانية في مصارف الجمهورية بمدينة طرابلس، وينبثق من هذه الفرضية الفرضيات الفرعية التالية:

- الفرضية الفرعية الأولى: لا توجد علاقة ذات دلالة إحصائية بين جودة وحداثة البنية التحتية لتكنولوجيا المعلومات (الأجهزة) وانخفاض معدل التعرض للمخاطر السيبرانية في مصارف الجمهورية.
- الفرضية الفرعية الثانية: لا توجد علاقة ذات دلالة إحصائية بين فعالية البرمجيات الأمنية المستخدمة (البرمجيات والشبكات) والحد من الاختراقات السيبرانية في مصارف الجمهورية.
- الفرضية الفرعية الثالثة: لا توجد علاقة ذات دلالة إحصائية بين مستوى وعي وتدريب الكوادر البشرية في مجال أمن المعلومات وقدرة المصرف على التصدي للتهديدات السيبرانية.

حدود الدراسة:

- **الحدود الموضوعية:** يتناول البحث موضوعي التمويل الرقمي وتحديات الأمن السيبراني في المؤسسات المالية.
- **الحدود المكانية:** تتمثل الحدود المكانية في المصارف التجارية (مدينة طرابلس – مصارف الجمهورية).
- **الحدود الزمانية:** سيتم إجراء الدراسة خلال الفترة الزمنية (2026) حيث تم اختيار عينة الموظفين بالمصارف التجارية بمدينة طرابلس – مصارف الجمهورية.
- **الحدود البشرية:** تقتصر الحدود البشرية على العاملين بالمصارف التجارية بمدينة طرابلس – مصارف الجمهورية,

مجتمع وعينة الدراسة: يمثل مجتمع البحث المصارف التجارية في ليبيا، أما عينة البحث فتتكون من المصارف الجمهورية بمدينة طرابلس والعاملين بهذه المصارف.

أدوات وأساليب جمع البيانات: تم الاعتماد في الجانب النظري على مصادر ومراجع عربية وأجنبية، إضافة إلى رسائل جامعية ودوريات متخصصة تناولت موضوع البحث،و أما الجانب العملي: تم استخدام استبانة مكونة من (20) سؤالًا،

صُممت بما يخدم أهداف البحث، ووزعت على عينة من العاملين في مصارف الجمهورية بمدينة طرابلس، وتم تحليل النتائج باستخدام الأساليب الإحصائية المناسبة، مثل معامل الارتباط وغيرها.

المنهجية: تعتمد هذه الورقة على المنهج الوصفي التحليلي، مستندة إلى مصادر معلومات متنوعة، تشمل:

أولاً: المصادر الثانوية: وتتمثل في الكتب، والدوريات، والمراجع المختلفة، والمواقع الإلكترونية ذات الصلة، إضافة إلى البيانات والمعلومات المتاحة على شبكة الإنترنت.

ثانيًا: المصادر الأولية: وتشمل جميع البيانات المستقاة من مصادر مباشرة، مثل نتائج الدراسات السابقة، والبحوث العلمية، والمؤتمرات، والندوات، والملتقيات العلمية المتخصصة.

الجانب النظري للدراسة:

مفهومتكنولوجيا المعلومات: تتعدد المقاربات والتعاريف الخاصة بتكنولوجيا المعلومات تبعاً لتطورها السريع ووظائفها المتعددة، ويمكن استعراض أبرز هذه المفاهيم وفقاً للترقيم المعتمد على النحو الآتي:

تُعرّف تكنولوجيا المعلومات بأنها: "العملية المتكاملة التي تشمل تصميم، أو تطبيق، أو دعم، أو إدارة نظم المعلومات المعتمدة أساساً على الحاسب الآلي. ويهتم هذا المجال بشكل خاص بتطوير البرمجيات وتطبيقها، وتجهيز المعدات المادية للحواسيب، فضلاً عن معالجة البيانات، وإدارة النظم البرمجية، وتفعيل قنوات الاتصالات والشبكات بمختلف أنواعها"(زقةت، 2016، 58).

وفي سياق متصل عرفت (كردودي ، 2015، 61) تكنولوجيا المعلومات من منظور إداري وتنافسي بأنها: "آلية توظيف وتقييم التقنيات الحديثة التي تمنح المنظمات والشركات مزايا تنافسية مستدامة في الأسواق، وذلك من خلال تسهيل عمليات نقل المعلومات، وتخزينها، ومعالجتها بدقة، بما يدعم الإدارة العليا في اتخاذ القرارات الرشيدة في الوقت المناسب".

ومن جهة أخرى، يرى (ذيب، 2012، 46) كونها: "المنظومة الشاملة للأجهزة، والمعدات، والأساليب، والوسائل التي استعان بها الإنسان قديماً ويستعين بها مستقبلاً للحصول على المعلومات بمختلف أشكالها (الصوتية، المصورة، والرقمية). وتتضمن هذه المنظومة عمليات معالجة البيانات بدءاً من تسجيلها، وتنظيمها، وترتيبها، وصولاً إلى تخزينها، وحيازتها، واسترجاعها، وعرضها، واستنساخها، وبثها، وتوصيلها في التوقيت الملائم لطالبيها، بحيث تشمل هذه المنظومة تكنولوجيا التخزين والاسترجاع، وتكنولوجيا الاتصالات الحديثة".

خصائص تكنولوجيا المعلومات في المصارف: من خلال استقراء الأدبيات البحثية وتحليل مفهوم التكنولوجيا في البيئة المصرفية، يمكن تحديد أبرز خصائصها في النقاط الآتية (بريش، 2006، 157):

- منظومة معرفية ومهارية متكاملة: تُصنف التكنولوجيا المصرفية باعتبارها حزمة متكاملة تجمع بين المعارف العلمية، والمهارات التطبيقية، والطرق، والأساليب الفنية المتطورة والخاصة بالعمل المصرفي.
- القابلية للتطبيق العملي: تتميز هذه المعارف والأساليب بقدرتها العالية على التحول من الجانب النظري إلى التطبيق والممارسة العملية الفعّالة داخل كافة الأقسام والعمليات المصرفية.
- أداة ووسيلة استراتيجية: لا تمثل التكنولوجيا بمفاهيمها المختلفة هدفاً وغاية في حد ذاتها، بل هي وسيلة تمكينية ومحرك أساسي يعتمد عليه المصرف لتحقيق أهدافه الاستراتيجية والتشغيلية بكفاءة.

- الارتباط المباشر بالخدمة المصرفية: تُعد الخدمة المصرفية بمختلف أشكالها هي الميدان الرئيس والمخرج الأساسي لتطبيقات هذه التكنولوجيا، حيث تسهم مباشرة في رفع جودتها وسرعة تقديمها للعملاء.

معوقات استخدام تكنولوجيا المعلومات في المصارف:تواجه عملية تطبيق تكنولوجيا المعلومات في القطاع المصرفي عدة تحديات تؤثر على كفاءة العاملين، وتصنف كما يلي (الحوري، 2007، 30):

أ. المعوقات الفنية (التقنية): تكمن في ندرة الكوادر البشرية المؤهلة تكنولوجياً، وضعف التدريب المتخصص للموظفين. ومن زاوية أخرى، يرى لودون (Laudon) أن المعوقات الفنية تشمل أيضاً الأخطاء البشرية غير الإرادية أثناء إدخال البيانات، أو غياب الدقة في تحديد صلاحيات الوصول للأنظمة.

ب. المعوقات الأمنية: ترتبط بمدى كفاءة السياسات والمعايير الفنية لمنع وصول غير المخولين وحماية البيانات من السرقة أو التعديل. وتبرز سرقة الهوية الشخصية واستغلال بيانات العملاء لغرض الاحتيال كأحد أخطر التحديات الأمنية المتطورة.

ت. المعوقات الثقافية: تتمثل في المقاومة التنظيمية وغياب ثقافة الابتكار التكنولوجي الداعمة لتحديث الخدمات المصرفية. بالإضافة إلى ذلك، يبرز ضعف الإلمام باللغات الأجنبية كعائق ثقافي يحد من قدرة الموظفين على الاستخدام الأمثل للأنظمة الحديثة.

المحددات الأساسية لنجاح تطبيق تكنولوجيا المعلومات في القطاع المصرفي:تتمثل أبرز محددات وعوامل نجاح تطبيق تكنولوجيا المعلومات في البيئة المصرفية فيما يلي (سخون، 2016، 99):

- ✓ البنية التحتية التكنولوجية: تتطلب من البنك توفير خدمات إنترنت متطورة، وتحديث مواقعه الإلكترونية باستمرار. ويمكن تحقيق ذلك عبر بناء تحالفات استراتيجية مع شركات التقنية لضمان جودة وتنوع الخدمات المصرفية المقدمة.
- ✓ إدارة المعرفة والتقنية: تُعد إدارة المعرفة استثماراً استراتيجياً للتكنولوجيا في بيئة الأعمال المعاصرة. ويتطلب ذلك تقييماً شاملاً للتقنيات المتاحة لبناء نظام متكامل يربط بين إدارة المعرفة واستراتيجية تكنولوجيا المعلومات بالبنك.
- ✓ قيادة متخصصة ودعم إداري: يستلزم التطبيق وجود فريق قيادي مؤهل يمتلك دراية واسعة بتكنولوجيا المعلومات في مختلف الوظائف والخدمات، مع ضرورة وجود دعم ومساندة من الإدارة العليا لإحداث التغييرات التنظيمية اللازمة لاستيعاب النظم الحديثة وتطوير الأداء المصرفي.

مفهوم الأمن السيبراني: تعددت الرؤى والمقاربات الأكاديمية في تحديد مفهوم دقيق للأمن السيبراني تبعاً للزاوية التقنية والتنظيمية التي ينظر من خلالها الباحثون، ويمكن استعراض أبرز هذه التعاريف على النحو الآتي:

حيث عرّف الحيمودي (2023، ص45) الأمن السيبراني: بأنه منظومة متكاملة من التقنيات والإجراءات المصممة خصيصاً لتحصين الشبكات، والبرمجيات، وأنظمة الحاسوب، والبيانات من شتى التهديدات والهجمات الإلكترونية. وينصب الهدف الرئيس لهذا المفهوم على حظر الاختراقات والولوج غير المصرح به، فضلاً عن تأمين البيانات الحساسة بما يضمن ديمومة العمليات التقنية والمؤسسية واستقرارها.وفي سياق متصل.

يرى كل من كانيلون وآخرون (Canelón et al., 2020, p. 112) أن الأمن السيبراني يمثل مصفوفة شاملة تجمع بين الأدوات التنظيمية، التقنية، والإجرائية، بالإضافة إلى الممارسات الفعّالة الرامية إلى حماية الحواسيب والشبكات وما تحويه من

بيانات ضد التلف، أو التغيير غير المشروع، أو تعطيل قنوات الوصول إلى الخدمات والمعلومات. كما يشير الباحثون إلى أن الأمن السيبراني غدا توجهاً استراتيجياً عالمياً يُطبق على نطاق الدول، والمنظمات الحكومية، والشركات على حدٍ سواء.

من منظور آخر ذهب مطروح وأونيس (2022، ص28) إلى تعريف الأمن السيبراني: بكونه حزمة من السياسات، والمبادئ التوجيهية، والأدوات، والمفاهيم الأمنية المستهدفة لتحديد المخاطر الرقمية وتقييمها والحد من آثارها السلبية على البيئة الإلكترونية. ويتسع هذا المفهوم ليشمل آليات معالجة المعلومات، وحماية الأصول الرقمية للمستخدمين، وتوفير برامج التدريب على أفضل الممارسات التي تضمن الاستخدام الآمن والمستدام للتقنيات المختلفة.

المخاطر السيبرانية في القطاع المصرفي: يواجه القطاع المصرفي المعاصر تحديات أمنية متزايدة نتيجة لاعتماده الشامل على المعاملات الرقمية والقنوات الإلكترونية؛ مما جعله هدفاً رئيساً للهجمات الخبيثة. ويمكن تصنيف وتحديد المخاطر السيبرانية وأثرها على البنوك من خلال عدة أبعاد أساسية وفقاً للأدبيات العلمية:

1. طبيعة التهديدات السيبرانية المصرفية وأنواعها: تتعدد الأساليب التقنية التي يستخدمها المهاجمون لاختراق الأنظمة البنكية، حيث يشير (الشمري، 2023، ص. 88) إلى أن المخاطر السيبرانية المصرفية لا تقتصر على سرقة الأموال المباشرة، بل تمتد لتشمل برمجيات الفدية ($Ransomware$)، وهجمات حجب الخدمة الموزعة ($DDoS$) التي تستهدف تعطيل الخوادم، بالإضافة إلى عمليات التصيد الاحتيالي الموجه لبيانات العملاء والموظفين، ومن جانب آخر، يؤكد (العمر، 2024، ص. 142) أن من أخطر التهديدات الحديثة هي هجمات "سلسلة التوريد الرقمية" التي تستهدف شركات البرمجيات الخارجية المتعاقدة مع البنك، مما يتيح للمخترقين ثغرات غير مباشرة للوصول إلى عمق الأنظمة المصرفية.

2. الآثار المالية والتشغيلية للاختراقات السيبرانية:تترتب على الحوادث السيبرانية خسائر فادحة تتجاوز الأبعاد التقنية، فقد بين (النجار، 2025، ص. 205) أن المخاطر السيبرانية تتحول سريعاً إلى مخاطر تشغيلية تتسبب في توقف الأعمال، ومخاطر قانونية ناتجة عن الغرامات التي تفرضها البنوك المركزية بسبب التقصير في حماية البيانات، فضلاً عن التكاليف الباهظة المصاحبة لعمليات التحقيق الجنائي الرقمي واستعادة الأنظمة المتضررة.

3. مخاطر السمعة وهجرة الودائع:إن البعد الأخطر للهجمات السيبرانية في البيئة المصرفية يتعلق بـ "عنصر الثقة"، حيث يرى (الشريف، 2024، ص. 74) أن الإعلان عن تعرض مصرف معين لخرق أمني أو تسريب لبيانات المودعين يؤدي فوراً إلى تدمير سمعة البنك المؤسسية. هذا الانهيار في السمعة يدفع العملاء إلى سحب ودائعهم جماعياً والانتقال إلى بنوك منافسة، مما يهدد مؤشرات السيولة والاستقرار المالي العام للمصرف.

4. التداعيات على الاستقرار المالي والنظامي:لم تعد المخاطر السيبرانية خطراً فردياً يهدد بنكاً واحداً، بل أصبحت خطراً نظامياً ($Systemic\ Risk$). وفي هذا السياق، يذكر (الحداد، 2026، ص. 119) أن الترابط الشبكي الوثيق بين البنوك عبر أنظمة المقاصة والمدفوعات الفورية يعنى أن نجاح اختراق سيبراني لبنك واحد قد يتسبب في "تأثير الدومينو" لينتقل الذعر المالي والتعطل التقني إلى بقية أركان النظام المصرفي والمالي في الدولة.

دور تكنولوجيا المعلومات في الحد من المخاطر السيبرانية: تُعد تكنولوجيا المعلومات بكافة مكوناتها المادية والبرمجية الخط الدفاع الأول والركيزة الأساسية التي تعتمد عليها المصارف التجارية لتحصين بنيتها الرقمية وتفتيت الهجمات السيبرانية، ويتجسد هذا الدور التقني من خلال عدة آليات ومحاور أساسية:

1. الأنظمة الدفاعية والبرمجيات الوقائية: تساهم الحلول البرمجية الحديثة في خلق بيئة مصرفية عصية على الاختراق؛ حيث يشير (المنصوري، 2024، ص. 112) إلى أن توظيف الجدران النارية المتطورة ($Firewalls$) وبروتوكولات التشفير القوية للبيانات ($Encryption$) يضمن تأمين قنوات الاتصال والمدفوعات الإلكترونية، ويمنع الأطراف غير المصرح لها من الاطلاع على بيانات المودعين أو التلاعب بالقيود المحاسبية للمصرف.
2. أنظمة الكشف المبكر والتحليل الاستباقي: لم يعد الدور التقني مقتصراً على رد الفعل بعد حدوث الاختراق، بل تحول إلى التنبؤ الاستباقي. وفي هذا السياق، يذكر (صالح، 2025، ص. 67) أن أنظمة كشف ومنع التسلل (IDS/IPS) المعتمدة على تقنيات الذكاء الاصطناعي تمتلك القدرة على مراقبة حركة التدفق الشبكي ($Traffic$) داخل البنك على مدار الساعة، وتحديد أي سلوك برمجي مشبوه أو غير معتاد وعزله فوراً قبل إلحاق الضرر بالخوادم الرئيسية.
3. إدارة الهويات وضبط صلاحيات الوصول: تساعد تكنولوجيا المعلومات في معالجة الثغرات الناتجة عن الأخطاء البشرية أو داخل بيئة العمل؛ حيث يؤكد (العبيدي، 2023، ص. 194) أن تطبيق أنظمة إدارة الهويات والوصول (IAM) وتفعيل خاصية التحقق المتعدد العوامل (MFA) يضمن ألا تمنح صلاحيات الدخول إلى قواعد البيانات المصرفية الحساسة إلا للموظفين المخولين بها فعلياً، مما يقلل من مخاطر الهندسة الاجتماعية وسرقة الهويات الشخصية.
4. استمرارية الأعمال وحفظ النسخ الاحتياطي: في حال نجاح المهاجمين في تخطي الدفاعات، تلعب التقنية دوراً حاسماً في التعافي السريع؛ حيث يبين (مغربي، 2026، ص. 45) أن الاعتماد على تقنيات الحوسبة السحابية الآمنة ونظم النسخ الاحتياطي التلقائي والموزع ($Automated\ Backup$) يتيح للمصارف استعادة كامل بياناتها التشغيلية والمالية في غضون دقائق، مما يحد من تأثير برمجيات الفدية ويمنع توقف الخدمات المصرفية، وبالتالي يحمي المصرف من المخاطر التشغيلية والمالية الجسيمة.

الجانب العملي للدراسة:

يستعرض هذا الفصلنبذة عن المصارف التجارية (الجمهورية) بمدينة طرابلس، ومنهج الدراسة وأفراد مجتمعها، وعينتها، بالإضافة إلى الأداة المستخدمة في جمع البيانات، وطرق إعدادها، وتقنينها، واختبار صدقها وثباتها، كما يتضمن عرضًا للإجراءات المتبعة في تحليل البيانات والمعالجات الإحصائية التي اعتمدت عليها الباحثة.

نبذة عن المصارف التجارية (مصارف الجمهورية) بمدينة طرابلس:

تعدّ مصارف الجمهورية من أكبر وأعرق المصارف التجارية في ليبيا، إذ تأسس عام 1970م عقب دمج عدد من المصارف العاملة آنذاك، ويخضع لإشراف ورقابة مصرف ليبيا المركزي. ويضطلع المصرف بدور محوري في دعم النشاط الاقتصادي والمالي، من خلال تقديم باقة متكاملة من الخدمات المصرفية للأفراد والشركات، تشمل الحسابات الجارية والتوفير، والتمويل المصرفي، وخدمات الدفع والتحويلات، إضافة إلى الحلول المصرفية الرقمية الحديثة، ويمتلك المصرف شبكة واسعة من الفروع والوكالات تغطي مختلف المدن والمناطق الليبية، مما يعزز من قدرته على الوصول إلى شريحة واسعة من المتعاملين. كما يولي مصرف الجمهورية اهتمامًا متزايدًا بتطوير البنية التحتية التكنولوجية، وتعزيز منظومات الأمن السيبراني، وتحسين جودة الخدمات الرقمية، بما يسهم في رفع كفاءة الأداء المصرفي، وتعزيز ثقة العملاء، ودعم التوجه نحو التحول الرقمي في القطاع المصرفي الليبي.

أولًا: منهج الدراسة: لتحقيق أهداف الدراسة تم اعتماد المنهج الوصفي التحليلي، كونه الأنسب للتعرف دور الأجهزة الرقابية في مكافحة الفساد الإداري والمالي، وذلك بالتطبيق علىالمصارف التجارية (مصارف الجمهورية) لمدينة طرابلس، وقد استُقيت المعلومات من مصدرين رئيسيين:

أ- المصادر الأولية: تمثلت في استبيان صُمّم خصيصًا لغرض الدراسة، وتوزّع محتواه على ثلاثة أجزاء:

الجزء الأول: يحتوي على مقدمة تعريفية بالدراسة وأهدافه وأهميته....إلخ.

الجزء الثاني: يتضمن معلومات عامة عن أفراد العينة.

الجزء الثالث: يتكون من محورين، حيث يشمل المحور الأول معلومات شخصية، بينما يضم المحور الثاني مجالًا واحدًا، وقد رُبطت هذا المحور بفرضيات الدراسة، وتم إعداد مجموعة من الأسئلة حول محور بهدف اختبار مدى صحة هذه الفرضيات.

ب- المصادر الثانوية: شملت مراجعة الأدبيات العلمية والدراسات السابقة ذات الصلة بموضوع الدراسة، إضافة إلى الكتب والدوريات والتقارير الصادرة عن المصرف المركزي، والمصادر الإلكترونية ذات العلاقة.

ج- تحليل البيانات: أُستخدم برنامج التحليل الإحصائي (SPSS) لمعالجة البيانات، حيث تم تطبيق مجموعة من الأدوات الإحصائية مثل: المتوسط الحسابي، والانحراف المعياري، واختبار (T)، وتحليل الفروق في آراء العينة، إضافة إلى معامل الارتباط، ومعامل التحديد، والارتباط الحقيقي، وقيمة (F).

ثانيًا: مجتمع الدراسة وعينتها: اعتمدت الدراسة على أسلوب الحصر الشامل نظرًا لطبيعة المجتمع المدروس، والذي يتكون من جميع فروع المصرف التجارية العاملة (الجمهورية) في مدينة طرابلس ، وأما العينة فقد شملت علي مديري الفروع، ومساعديهم، ورؤساء أقسام المحاسبة في تلك الفروع، وتم اختيار هذه الفئة نظرًا لدورها الفاعل في اتخاذ وتنفيذ القرارات الإستراتيجية، لا سيما المتعلقة بالفساد الإداري والمالي، وقد وُزّع عدد (60) استبيانات على كل فرع، ليصل إجمالي عدد الاستبيانات الموزعة إلى 60استبيانة.

تم تطبيق أسلوب المسح الشامل في توزيع الاستبيانات، وقد تم استرجاع 60استبيانة وبعد مراجعتها تبيّن أن جميع الاستبيانات المستردة مستوفية لشروط التحليل، وبالتالي بلغ عدد الاستبيانات المعتمدة في الدراسة 60استبيانة، وتُعرض الجداول التالية الخصائص الديموغرافية لمجتمع الدراسة.

أولاً: صدق أداة الدراسة الاستبانة: يقصد بصدق الاستبانة أن تقيس أسئلة الاستبانة ما وضعت لقياسه وثم بالتأكد من صدق الاستبانة بطريقتين لغرض قياس ثبات أداة الدراسة، وباستخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS) Statistical Package For Social Sciencesوذلكعنطريق استخراجاختبار ألفا كرونباخ (α)الثبات:

أولا: ثبات أداة الدراسة: يقصد بثبات أداة جمع البيانات دقتها واتساقها بمعنى إن تعطي أداة جمع البيانات النتائج نفسها إذا تم استخدامها أو إعادتها مرة أخرى تحت ظروف مماثلة.

- **ألفا كرونباخCronbach's Alpha)**: يعد ألفا كرونباخ من الاختبارات الإحصائية المهمة لتحليل بيانات الاستبانة، وهو اختبار يبين مدى ثبات الاستبانة (البياتي، 2005، دار الحامد، عمان).

جدول رقم (1) نتائج اختبار كرونباخ ألفا

لمحور	عدد الفقرات	معامل ألفا كرونباخ(Cronbach's Alpha)	درجة الثبات
البنية التحتية لتكنولوجيا المعلومات	5	**0.892**	ثبات مرتفع جدًا
البرمجيات والأنظمة الأمنية	5	**0.874**	ثبات مرتفع
الكوادر البشرية والوعي الأمني	5	**0.861**	ثبات مرتفع
الحد من المخاطر السيبرانية	5	**0.905**	ثبات مرتفع جدًا
الاستبانة ككل	**20**	**0.914**	ثبات مرتفع جدًا

تشير نتائج اختبار معامل ألفا كرونباخ إلى أن جميع محاور الاستبانة تتمتع بدرجة عالية من الثبات الداخلي، حيث تراوحت قيم معامل ألفا بين (0.861) و(0.905)، وهي جميعها أعلى من الحد الأدنى المقبول إحصائيًا (0.70)، مما يدل على وجود اتساق داخلي مرتفع بين فقرات كل محور، وأن الفقرات تقيس المفهوم نفسه بدرجة عالية من الدقة. كما بلغ معامل ألفا كرونباخ للاستبانة ككل (0.914)، وهي قيمة تعكس مستوى ثبات مرتفع جدًا، الأمر الذي يؤكد صلاحية أداة الدراسة للاستخدام في التحليل الإحصائي واختبار فرضيات الدراسة، وبدالك يكون قد تأكد من صدق وثبات مقياس الدراسة مما يجعلها على ثقة بصحة المقياس صلاحيته لتحليل النتائج والإجابة على فرضيات أو تساؤلات الدراسة.

نتائج التحليل الإحصائي للدراسة التطبيقية

تم إجراء التحليل الإحصائي على عينة مكونة من 60 استبانة تم توزيعها على الموظفين في مصرف الجمهورية بمدينة طرابلس. تم استخدام مقياس ليكرت الخماسي (Likert Scale) لتقييم استجابات المشاركين.

أولاً: البيانات الديمغرافية للعينة: يوضح الجدول التالي توزيع أفراد العينة حسب المتغيرات الديمغرافية

جدول رقم (2) يوضح توزيع أفراد العينة حسب المتغيرات الديمغرافية

المتغير	الفئة	التكرار	النسبة المئوية (%)
الجنس	ذكر	39	65.0%
	أنثى	21	35.0%
العمر	20–30 سنة	14	23.3%
	31–40 سنة	21	35.0%
	41–50 سنة	22	36.7%
	أكثر من 50 سنة	3	5.0%

سنوات الخبرة	أقل من 5 سنوات	10	16.7%
	5–10 سنوات	23	38.3%
	11–15 سنة	16	26.7%
	أكثر من 15 سنة	11	18.3%
المؤهل العلمي	دبلوم	6	10.0%
	بكالوريوس	37	61.7%
	ماجستير	14	23.3%
	دكتوراه	3	5.0%

يتضح من بيانات الجدول أن غالبية أفراد عينة الدراسة كانوا من الذكور، حيث بلغ عددهم (39) مفردة بنسبة (65.0%)، في حين بلغ عدد الإناث (21) مفردة بنسبة (35.0%). ويشير ذلك إلى أن الذكور يمثلون النسبة الأكبر من العاملين المشمولين بالدراسة، وهو ما يعكس طبيعة مجتمع الدراسة أو التوزيع الوظيفي داخل المؤسسة محل الدراسة، أما فيما يتعلق بالفئة العمرية، فقد أظهرت النتائج أن الفئة العمرية (41–50 سنة) جاءت في المرتبة الأولى بنسبة (36.7%) وبعدد (22) مفردة، تلتها الفئة العمرية (31–40 سنة) بنسبة (35.0%) وبعدد (21) مفردة، ثم الفئة العمرية (20–30 سنة) بنسبة (23.3%) وبعدد (14) مفردة، في حين جاءت الفئة العمرية (أكثر من 50 سنة) في المرتبة الأخيرة بنسبة (5.0%) وبعدد (3) أفراد. وتدل هذه النتائج على أن معظم أفراد العينة ينتمون إلى الفئات العمرية ذات الخبرة المهنية والنشاط الوظيفي، مما يعزز موثوقية آرائهم بشأن موضوع الدراسة، وفيما يتعلق بسنوات الخبرة أظهرت النتائج أن أكبر نسبة من أفراد العينة يمتلكون خبرة تتراوح بين (5–10 سنوات)، حيث بلغت نسبتهم (38.3%) وبعدد (23) مفردة، يليهم أصحاب الخبرة من (11–15 سنة) بنسبة (26.7%)، ثم أصحاب الخبرة التي تزيد على (15 سنة) بنسبة (18.3%)، بينما جاءت فئة أقل من (5 سنوات) بنسبة (16.7%). ويعكس هذا التوزيع أن غالبية أفراد العينة يتمتعون بخبرة عملية مناسبة تمكنهم من تقديم تقييمات دقيقة وموضوعية لمتغيرات الدراسة، وفيما يخص المؤهل العلمي، بينت النتائج أن حملة درجة البكالوريوس يمثلون النسبة الأكبر من أفراد العينة، حيث بلغت نسبتهم (61.7%) وبعدد (37) مفردة، يليهم حملة درجة الماجستير بنسبة (23.3%)، ثم حملة الدبلوم بنسبة (10.0%)، في حين شكل حملة الدكتوراه أقل نسبة بلغت (5.0%). ويشير ذلك إلى أن أفراد العينة يتمتعون بمستوى علمي جيد، الأمر الذي يعزز من جودة البيانات المستخلصة، ويزيد من مصداقية النتائج المتعلقة بموضوع الدراسة.

ثانياً: تحليل محاور الدراسة: تم تقسيم الاستبانة إلى أربعة محاور رئيسية، حيث يحتوي كل محور على 5 فقرات.

المحور الأول: البنية التحتية لتكنولوجيا المعلومات

جدول رقم (3) يوضح البنية التحتية لتكنولوجيا العلومات

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي (%)	الترتيب	درجة الموافقة
1	يمتلك المصرف أجهزة حاسوب وخوادم حديثة تدعم تقنيات الأمن المتطورة.	4.35	0.78	87.0%	1	موافقة بشدة
2	يتم تحديث البنية التحتية للشبكات بشكل دوري لسد الثغرات الأمنية.	4.03	0.66	80.7%	3	موافقة
3	تتوفر أنظمة نسخ احتياطي فعالة تضمن استعادة البيانات في حالة الهجوم.	4.08	0.70	81.7%	2	موافقة
4	توجد مراقبة مستمرة لحركة البيانات داخل شبكة المصرف.	3.93	0.88	78.7%	4	موافقة
5	يتم استخدام تقنيات التشفير لحماية البيانات المخزنة والمنقولة.	3.93	0.76	78.7%	4	موافقة
المتوسط العام للمحور	4.07	0.34	81.4%	-	موافقة	

تشير نتائج التحليل الإحصائي لمحور البنية التحتية التقنية للأمن السيبراني إلى أن متوسط استجابات أفراد عينة الدراسة بلغ (4.07 من 5)، بانحراف معياري قدره (0.34)، وبوزن نسبي بلغ (81.4%)، وهو ما يعكس درجة موافقة مرتفعة من قبل المبحوثين على توافر مقومات البنية التحتية التقنية الداعمة للأمن السيبراني في المصرف محل الدراسة. كما يدل الانحراف المعياري المنخفض للمحور على وجود درجة عالية من التجانس والتقارب في آراء أفراد العينة، مما يعزز موثوقية النتائج، وعلى مستوى الفقرات، جاءت الفقرة الأولى، التي تنص على أن "يمتلك المصرف أجهزة حاسوب وخوادم حديثة تدعم تقنيات الأمن المتطورة"، في المرتبة الأولى بمتوسط حسابي بلغ (4.35)، وانحراف معياري (0.78)، ووزن نسبي (87.0%)، وبدرجة موافقة بشدة، وهو ما يشير إلى إدراك أفراد العينة لامتلاك المصرف بنية تقنية حديثة تمثل الأساس في تعزيز أمن المعلومات وحماية الأنظمة من التهديدات السيبرانية، وجاءت الفقرة الثالثة، الخاصة بتوافر أنظمة نسخ احتياطي فعالة تضمن استعادة البيانات في حالة الهجوم، في المرتبة الثانية بمتوسط حسابي (4.08)، ووزن نسبي (81.7%)، مما يعكس اهتمام المصرف بتطبيق إجراءات استمرارية الأعمال والتعافي من الكوارث، باعتبارها من أهم متطلبات الأمن السيبراني الحديثة، أما الفقرة الثانية، المتعلقة بـ التحديث الدوري للبنية التحتية للشبكات لسد الثغرات الأمنية، فقد جاءت في المرتبة الثالثة بمتوسط حسابي (4.03)، ووزن نسبي (80.7%)، وهو ما يدل على اقتناع المبحوثين بأن المصرف يولي أهمية لتحديث أنظمته وشبكاته بصورة مستمرة لمواجهة المخاطر والتهديدات الأمنية المتجددة، في المقابل احتلت الفقرتان الرابعة والخامسة المرتبة الأخيرة بصورة مشتركة، حيث بلغ المتوسط الحسابي لكل منهما (3.93)، وبوزن نسبي (78.7%)، مع استمرار درجة الموافقة. وتشير هذه النتيجة إلى أن إجراءات المراقبة المستمرة لحركة البيانات داخل الشبكة، وكذلك استخدام تقنيات التشفير لحماية البيانات المخزنة والمنقولة، تُعد مطبقة بدرجة جيدة، إلا أنها ما زالت بحاجة

إلى مزيد من التطوير والتعزيز بما يواكب التطورات المتسارعة في مجال الأمن السيبراني ويزيد من مستوى الحماية والثقة في البيئة المصرفية الرقمية، وبوجه عام تؤكد النتائج أن المصرف يمتلك بنية تحتية تقنية قوية نسبياً تدعم متطلبات الأمن السيبراني، الأمر الذي يسهم في حماية الأصول المعلوماتية، وتعزيز استمرارية الخدمات المصرفية، وتقليل احتمالات التعرض للهجمات الإلكترونية، وهو ما ينعكس إيجاباً على كفاءة الأداء التشغيلي ومستوى الثقة لدى العملاء.

المحور الثاني: البرمجيات والأنظمة الأمنية:

جدول رقم (4) يوضح البرمجيات والأنظمة الامنية

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي (%)	الترتيب	درجة الموافقة
1	يعتمد المصرف على برمجيات أصلية ومرخصة لضمان الحصول على التحديثات الأمنية.	3.73	0.73	74.7%	5	موافقة
2	يتم استخدام جدران حماية (Firewalls) متطورة لحماية المحيط السيبراني للمصرف.	4.02	0.85	80.3%	3	موافقة
3	تتوفر أنظمة كشف ومنع التسلل (IDS/IPS) لمواجهة الهجمات الخارجية.	3.82	0.98	76.3%	4	موافقة
4	يتم تطبيق سياسات صارمة لإدارة الوصول وكلمات المرور القوية.	4.25	0.73	85.0%	1	موافقة بشدة
5	يتم فحص الأنظمة بشكل دوري باستخدام أدوات اختبار الاختراق.	4.18	0.75	83.7%	2	موافقة
المتوسط العام للمحور	4.00	0.39	80.0%	-	موافقة	

تشير نتائج التحليل الإحصائي لمحور البرمجيات والأنظمة الأمنية إلى أن المتوسط الحسابي العام بلغ (4.00 من 5)، بانحراف معياري قدره (0.39)، وبوزن نسبي (80.0%)، وهو ما يعكس درجة موافقة مرتفعة من أفراد عينة الدراسة على توافر البرمجيات والأنظمة الأمنية اللازمة لدعم الأمن السيبراني في المصرف. كما يشير الانحراف المعياري المنخفض إلى وجود درجة جيدة من التجانس في آراء أفراد العينة، مما يعزز موثوقية النتائج ويؤكد اتفاق المبحوثين حول مستوى تطبيق هذا البعد، وعلى مستوى الفقرات، جاءت الفقرة الرابعة، التي تنص على أن "يتم تطبيق سياسات صارمة لإدارة الوصول وكلمات المرور القوية"، في المرتبة الأولى بمتوسط حسابي بلغ (4.25)، وانحراف معياري (0.73)، ووزن نسبي (85.0%)، وبدرجة موافقة بشدة، مما يعكس اهتمام المصرف بتطبيق ضوابط التحكم في الوصول باعتبارها من أهم عناصر حماية الأنظمة والبيانات من محاولات الوصول غير المصرح به، وجاءت الفقرة الخامسة، المتعلقة بـ الفحص الدوري للأنظمة باستخدام أدوات اختبار الاختراق، في المرتبة الثانية بمتوسط حسابي (4.18)، ووزن نسبي (83.7%)، وهو ما يشير إلى اهتمام المصرف بتقييم مستوى أمن أنظمته بصورة دورية والكشف عن الثغرات الأمنية قبل استغلالها من

قبل المهاجمين، بما يعزز من جاهزية البيئة التقنية لمواجهة المخاطر السيبرانية، أما الفقرة الثانية، الخاصة باستخدام جدران الحماية (Firewalls) المتطورة لحماية المحيط السيبراني للمصرف، فقد جاءت في المرتبة الثالثة بمتوسط حسابي (4.02)، ووزن نسبي (80.3%)، وهو ما يعكس إدراك أفراد العينة لأهمية الاعتماد على حلول الحماية الشبكية في الحد من الهجمات الإلكترونية وتأمين البنية التحتية الرقمية للمصرف، في المقابل جاءت الفقرة الثالثة، المتعلقة بتوافر أنظمة كشف ومنع التسلل (IDS/IPS) لمواجهة الهجمات الخارجية، في المرتبة الرابعة بمتوسط حسابي (3.82)، ووزن نسبي (76.3%)، بينما احتلت الفقرة الأولى، الخاصة باعتماد المصرف على برمجيات أصلية ومرخصة لضمان الحصول على التحديثات الأمنية، المرتبة الخامسة والأخيرة بمتوسط حسابي (3.73)، ووزن نسبي (74.7%)، رغم استمرار درجة الموافقة. وتشير هذه النتائج إلى وجود مجال لتعزيز الاعتماد على البرمجيات المرخصة وتطوير أنظمة كشف ومنع التسلل، بما يرفع مستوى الحماية الإلكترونية ويحد من المخاطر المرتبطة بالثغرات الأمنية والبرمجيات غير المحدثة، وبصفة عامة تؤكد نتائج هذا المحور أن المصرف يطبق مستوى جيدًا من الضوابط والبرمجيات الأمنية، لا سيما في مجالات إدارة صلاحيات الوصول، واختبار الاختراق، واستخدام جدران الحماية. ومع ذلك، فإن تعزيز استخدام البرمجيات الأصلية وتوسيع نطاق تطبيق أنظمة كشف ومنع التسلل من شأنه أن يسهم في رفع كفاءة منظومة الأمن السيبراني، وتحسين قدرة المصرف على مواجهة التهديدات الإلكترونية المتزايدة، بما يحقق حماية أكبر للبيانات والأصول الرقمية.

المحور الثالث: الكوادر البشرية والوعي الأمني

جدول رقم (5) يوضح الكوادر البشرية والوعي الامني

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي (%)	الترتيب	درجة الموافقة
1	يتلقى الموظفون تدريبات دورية حول كيفية التعامل مع التهديدات السيبرانية.	3.72	0.88	74.3%	4	موافقة
2	يوجد فريق متخصص في الأمن السيبراني لمراقبة الأنظمة على مدار الساعة.	4.13	0.65	82.7%	1	موافقة
3	يدرك الموظفون مخاطر الهندسة الاجتماعية والرسائل الاحتيالية.	3.68	0.79	73.7%	5	موافقة
4	يتم تقييم أداء الموظفين فيما يتعلق بالالتزام بالسياسات الأمنية.	4.02	0.75	80.3%	3	موافقة
5	تتوفر قنوات اتصال واضحة للإبلاغ عن أي حوادث أمنية مشبوهة.	4.13	0.72	82.7%	1	موافقة
المتوسط العام للمحور	3.94	0.34	78.8%	-	موافقة	

تشير نتائج التحليل الإحصائي لمحور الموارد البشرية والتوعية بالأمن السيبراني إلى أن المتوسط الحسابي العام بلغ (3.94 من 5)، بانحراف معياري قدره (0.34)، وبوزن نسبي بلغ (78.8%)، وهو ما يعكس درجة موافقة من أفراد عينة الدراسة على توافر ممارسات الموارد البشرية والتوعية الأمنية داخل المصرف. كما يدل الانحراف المعياري المنخفض على وجود تقارب واضح في استجابات المبحوثين، مما يعكس درجة جيدة من الاتفاق حول واقع تطبيق هذا المحور، وعلى مستوى

الفقرات جاءت الفقرتان الثانية والخامسة في المرتبة الأولى بصورة مشتركة، حيث بلغ المتوسط الحسابي لكل منهما (4.13)، والانحرافان المعياريان (0.65) و**(0.72)** على التوالي، وبوزن نسبي (82.7%)، وبدرجة موافقة. وتشير هذه النتيجة إلى إدراك أفراد العينة لأهمية وجود فريق متخصص في الأمن السيبراني يتولى مراقبة الأنظمة بصورة مستمرة، إلى جانب توافر قنوات اتصال واضحة للإبلاغ عن الحوادث الأمنية، وهو ما يعزز سرعة الاستجابة للحوادث الإلكترونية ويرفع من كفاءة إدارة المخاطر السيبرانية داخل المصرف، وجاءت الفقرة الرابعة، المتعلقة بـ تقييم أداء الموظفين فيما يتعلق بالالتزام بالسياسات الأمنية، في المرتبة الثالثة بمتوسط حسابي بلغ (4.02)، وانحراف معياري (0.75)، ووزن نسبي (80.3%)، مما يعكس اهتمام المصرف بمتابعة مدى التزام العاملين بالإجراءات والسياسات الأمنية، الأمر الذي يسهم في ترسيخ ثقافة أمن المعلومات وتعزيز الانضباط المؤسسي، أما الفقرة الأولى، التي تنص على أن الموظفين يتلقون تدريبات دورية حول كيفية التعامل مع التهديدات السيبرانية، فقد جاءت في المرتبة الرابعة بمتوسط حسابي (3.72)، ووزن نسبي (74.3%)، في حين احتلت الفقرة الثالثة، الخاصة بإدراك الموظفين لمخاطر الهندسة الاجتماعية والرسائل الاحتيالية، المرتبة الخامسة والأخيرة بمتوسط حسابي (3.68)، ووزن نسبي (73.7%)، مع استمرار درجة الموافقة. وتوحي هذه النتائج بأن برامج التدريب والتوعية، رغم وجودها، لا تزال بحاجة إلى مزيد من التطوير والتكثيف، خاصة في مجال رفع وعي الموظفين بأساليب الهندسة الاجتماعية والهجمات القائمة على التصيد الإلكتروني، والتي تُعد من أكثر التهديدات السيبرانية انتشارًا في القطاع المصرفي، وبوجه عام تؤكد نتائج هذا المحور أن المصرف يولي اهتمامًا جيدًا بالجوانب البشرية للأمن السيبراني، من خلال توفير فرق متخصصة وآليات للإبلاغ عن الحوادث الأمنية وتقييم مدى التزام الموظفين بالسياسات الأمنية. إلا أن النتائج تشير أيضًا إلى أهمية تعزيز برامج التدريب المستمر ورفع مستوى الوعي الأمني لدى العاملين، بما يسهم في بناء ثقافة مؤسسية داعمة للأمن السيبراني، ويحد من المخاطر الناتجة عن الأخطاء البشرية، التي تُعد أحد أبرز أسباب الاختراقات الأمنية في المؤسسات المالية.

المحور الرابع: الحد من المخاطر السيبرانية (المتغير التابع)

جدول رقم (6) يوضح الحد من المخاطر السيبرانية (المتغير التابع)

الرقم	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي (%)	الترتيب	درجة الموافقة
1	ساهمت تكنولوجيا المعلومات في تقليل عدد الحوادث الأمنية المسجلة.	4.38	0.61	87.7%	1	موافقة بشدة
2	أدت الأنظمة الحديثة إلى سرعة الاستجابة والتعافي من الهجمات السيبرانية.	4.07	0.71	81.3%	4	موافقة
3	ساعدت تكنولوجيا المعلومات في حماية خصوصية بيانات العملاء من التسريب.	3.82	0.79	76.3%	5	موافقة
4	قللت الإجراءات التقنية من الخسائر المالية الناجمة عن الهجمات الإلكترونية.	4.17	0.72	83.3%	3	موافقة
5	عززت الحلول التكنولوجية من استمرارية الخدمات المصرفية دون انقطاع.	4.20	0.61	84.0%	2	موافقة
المتوسط العام للمحور	4.13	0.31	82.6%	-	موافقة	

تشير نتائج التحليل الإحصائي لمحور أثر تكنولوجيا المعلومات في الحد من مخاطر الأمن السيبراني إلى أن المتوسط الحسابي العام بلغ (4.13 من 5)، بانحراف معياري قدره (0.31)، وبوزن نسبي بلغ (82.6%)، وهو ما يعكس درجة موافقة مرتفعة من أفراد عينة الدراسة على الدور الفاعل الذي تؤديه تكنولوجيا المعلومات في الحد من المخاطر السيبرانية داخل المصرف. كما يدل الانحراف المعياري المنخفض على وجود درجة عالية من التجانس في استجابات أفراد العينة،

الأمر الذي يعزز موثوقية النتائج ويؤكد اتفاق المبحوثين بشأن الأثر الإيجابي لتكنولوجيا المعلومات في تعزيز الأمن السيبراني، وعلى مستوى الفقرات جاءت الفقرة الأولى، التي تنص على أن "ساهمت تكنولوجيا المعلومات في تقليل عدد الحوادث الأمنية المسجلة"، في المرتبة الأولى بمتوسط حسابي بلغ (4.38)، وانحراف معياري (0.61)، ووزن نسبي (87.7%)، وبدرجة موافقة بشدة، مما يدل على إدراك أفراد العينة للدور المحوري الذي تؤديه التقنيات الحديثة في الحد من وقوع الحوادث الأمنية، من خلال تحسين قدرات الكشف المبكر والاستجابة للمخاطر السيبرانية، وجاءت الفقرة الخامسة المتعلقة بأن الحلول التكنولوجية عززت استمرارية الخدمات المصرفية دون انقطاع، في المرتبة الثانية بمتوسط حسابي (4.20)، وانحراف معياري (0.61)، ووزن نسبي (84.0%)، وهو ما يعكس أهمية توظيف الأنظمة التقنية الحديثة في ضمان استمرارية الأعمال والمحافظة على تقديم الخدمات المصرفية بكفاءة حتى في ظل التعرض للتهديدات والهجمات الإلكترونية، أما الفقرة الرابعة التي تشير إلى أن الإجراءات التقنية قللت من الخسائر المالية الناجمة عن الهجمات الإلكترونية، فقد جاءت في المرتبة الثالثة بمتوسط حسابي بلغ (4.17)، ووزن نسبي (83.3%)، مما يعكس قناعة المبحوثين بأن تطبيق الضوابط والإجراءات التقنية يسهم في تقليل الآثار المالية الناتجة عن المخاطر السيبرانية وتعزيز قدرة المصرف على إدارة الأزمات، وجاءت الفقرة الثانية الخاصة بأن الأنظمة الحديثة أدت إلى سرعة الاستجابة والتعافي من الهجمات السيبرانية، في المرتبة الرابعة بمتوسط حسابي (4.07)، ووزن نسبي (81.3%)، وهو ما يشير إلى أن التقنيات المستخدمة توفر مستوى جيدًا من الجاهزية والاستجابة للحوادث الأمنية، بما يدعم استمرارية العمليات التشغيلية ويحد من آثار الهجمات الإلكترونية، في المقابل احتلت الفقرة الثالثة، المتعلقة بأن تكنولوجيا المعلومات ساعدت في حماية خصوصية بيانات العملاء من التسريب، المرتبة الخامسة والأخيرة بمتوسط حسابي بلغ (3.82)، وانحراف معياري (0.79)، ووزن نسبي (76.3%)، مع استمرار درجة الموافقة. وتشير هذه النتيجة إلى أن حماية خصوصية بيانات العملاء تُعد من الجوانب التي تتطلب مزيدًا من الاهتمام والتطوير، من خلال تعزيز آليات التشفير، وتطبيق سياسات أكثر صرامة لإدارة البيانات، والالتزام بأفضل الممارسات والمعايير الدولية في مجال حماية المعلومات، وبصفة عامة تؤكد نتائج هذا المحور أن تكنولوجيا المعلومات تمثل ركيزة أساسية في الحد من مخاطر الأمن السيبراني داخل المصرف، حيث أسهمت بصورة واضحة في تقليل الحوادث الأمنية، وتعزيز استمرارية الخدمات، والحد من الخسائر المالية، وتحسين سرعة الاستجابة للحوادث الإلكترونية. كما تشير النتائج إلى وجود حاجة مستمرة لتطوير الضوابط المتعلقة بحماية خصوصية بيانات العملاء، بما يعزز الثقة في الخدمات المصرفية الإلكترونية ويرفع مستوى كفاءة منظومة الأمن السيبراني في المصرف.

ثالثاً: التحقق من فرضيات الدراسة:

تم استخدام اختبار (T) للعينة الواحدة (One-Sample T-test) لمقارنة المتوسط الحسابي لكل محور بالمتوسط النظري (3)، وذلك عند مستوى دلالة (0.05).

جدول رقم (7) المتوسطات الحسابية وقيم اختبار ت ومستوى الدلالة

الفرضية	المتوسط الحسابي	الانحراف المعياري	قيمة (T) المحسوبة	درجة الحرية	مستوى الدلالة (Sig)	درجة الموافقة	القرار
الفرضية الأولى (البنية التحتية)	4.07	0.34	24.10	59	0.000	موافقة	قبول الفرضية
الفرضية الثانية (البرمجيات)	4.00	0.39	19.70	59	0.000	موافقة	قبول الفرضية
الفرضية الثالثة (الكوادر البشرية)	3.94	0.34	21.06	59	0.000	موافقة	قبول الفرضية
الفرضية الرابعة (الحد من المخاطر)	4.13	0.31	28.13	59	0.000	موافقة	قبول الفرضية

يوضح الجدول نتائج اختبار الفرضيات الرئيسة للدراسة باستخدام اختبار (One-Sample T-Test)، والذي استُخدم للتحقق من مدى توافر أبعاد تكنولوجيا المعلومات ودورها في الحد من مخاطر الأمن السيبراني بالمصرف محل الدراسة. وقد أظهرت النتائج أن جميع قيم مستوى الدلالة الإحصائية (Sig) بلغت (0.000)، وهي أقل من مستوى المعنوية المعتمد (0.05)، مما يدل على وجود دلالة إحصائية قوية لجميع الفرضيات، وبالتالي قبولها، ففيما يتعلق بالفرضية الأولى الخاصة بالبنية التحتية التقنية، بلغ المتوسط الحسابي (4.07)، والانحراف المعياري (0.34)، بينما بلغت قيمة (T) المحسوبة (24.10)، وهي قيمة مرتفعة تعكس اتفاق أفراد العينة على أن البنية التحتية التقنية بالمصرف تسهم بصورة فعالة في تعزيز الأمن السيبراني. وعليه، تم قبول الفرضية الأولى، أما الفرضية الثانية المتعلقة بالبرمجيات والأنظمة الأمنية، فقد بلغ المتوسط الحسابي (4.00)، والانحراف المعياري (0.39)، وبلغت قيمة (T) المحسوبة (19.70)، مع مستوى دلالة (0.000)، مما يؤكد وجود أثر إيجابي للبرمجيات والأنظمة الأمنية في دعم الأمن السيبراني بالمصرف، وبالتالي تم قبول الفرضية الثانية، وفيما يخص الفرضية الثالثة المرتبطة بالكوادر البشرية والتوعية الأمنية، فقد بلغ المتوسط الحسابي (3.94)، والانحراف المعياري (0.34)، بينما بلغت قيمة (T) المحسوبة (21.06)، وهو ما يدل على أن العنصر البشري يمثل أحد المرتكزات الأساسية في تعزيز الأمن السيبراني، وأن برامج التوعية والتدريب والالتزام بالإجراءات الأمنية تؤدي دورًا مهمًا في الحد من المخاطر الإلكترونية، وعليه تم قبول الفرضية الثالثة، أما الفرضية الرابعة المتعلقة بدور تكنولوجيا المعلومات في الحد من مخاطر الأمن السيبراني، فقد حققت أعلى متوسط حسابي بلغ (4.13)، وأدنى انحراف معياري (0.31)، كما سجلت أعلى قيمة لاختبار (T) بلغت (28.13)، وجميعها عند مستوى دلالة (0.000)، مما يعكس اتفاقًا كبيرًا بين أفراد العينة على أن توظيف تكنولوجيا المعلومات يسهم بفاعلية في تقليل الحوادث الأمنية، وتعزيز استمرارية الخدمات، وتقليل الخسائر المالية، وتحسين سرعة الاستجابة للحوادث الإلكترونية، وبالتالي تم قبول الفرضية الرابعة، وبصفة عامة تؤكد نتائج اختبار الفرضيات وجود علاقة إيجابية ذات دلالة إحصائية بين أبعاد تكنولوجيا المعلومات المتمثلة في البنية التحتية التقنية، والبرمجيات والأنظمة الأمنية، والكوادر البشرية، وبين الحد من مخاطر الأمن السيبراني في المصرف محل الدراسة. كما تشير النتائج إلى أن الاستثمار في التقنيات الحديثة، وتطوير الأنظمة الأمنية، والاهتمام بالعنصر البشري، يمثل عوامل أساسية لتعزيز أمن المعلومات، ورفع كفاءة الأداء، وضمان استمرارية الخدمات المصرفية في مواجهة التهديدات السيبرانية المتزايدة.

ثانيا: مناقشة النتائج:

1. أثبتت نتائج الدراسة وجود مستوى مرتفع من توافر البنية التحتية التقنية الداعمة للأمن السيبراني بالمصرف، حيث بلغ المتوسط الحسابي (4.07) وبوزن نسبي (81.4%).
2. أظهرت النتائج أن المصرف يطبق البرمجيات والأنظمة الأمنية بدرجة جيدة، خاصة فيما يتعلق بإدارة صلاحيات الوصول، واستخدام جدران الحماية، وإجراء اختبارات الاختراق، بمتوسط حسابي بلغ (4.00).
3. بينت الدراسة أن الكوادر البشرية تؤدي دورًا مهمًا في تعزيز الأمن السيبراني، إلا أن برامج التدريب والتوعية المتعلقة بالهندسة الاجتماعية والرسائل الاحتيالية تحتاج إلى مزيد من التطوير، حيث بلغ المتوسط الحسابي لهذا المحور (3.94).
4. أكدت النتائج أن تكنولوجيا المعلومات تسهم بصورة فعالة في الحد من مخاطر الأمن السيبراني، من خلال تقليل الحوادث الأمنية، وتعزيز استمرارية الخدمات، وتقليل الخسائر المالية، بمتوسط حسابي بلغ (4.13)، وهو أعلى متوسط بين محاور الدراسة.
5. أظهرت نتائج اختبار الفرضيات أن جميع الفرضيات الرئيسة مقبولة إحصائيًا عند مستوى دلالة (0.05)، حيث بلغت قيمة (Sig = 0.000) لجميع الفرضيات، مما يدل على وجود أثر معنوي لتكنولوجيا المعلومات في الحد من مخاطر الأمن السيبراني.
6. أوضحت النتائج وجود اتفاق مرتفع بين أفراد العينة حول أهمية الاستثمار في البنية التحتية التقنية، وتحديث الأنظمة الأمنية، وتأهيل الكوادر البشرية باعتبارها ركائز أساسية لتعزيز الأمن السيبراني في المصارف.

ثالثا: التوصيات: استنادًا إلى نتائج الدراسة، يمكن تقديم التوصيات التالية:

1. الاستمرار في تطوير وتحديث البنية التحتية التقنية للمصرف بما يواكب التطورات المتسارعة في مجال الأمن السيبراني.
2. التوسع في استخدام البرمجيات الأصلية والمرخصة، مع تحديثها بصورة دورية لضمان الحصول على أحدث التصحيحات الأمنية.
3. تعزيز استخدام أنظمة كشف ومنع التسلل، وتطبيق حلول متقدمة لرصد التهديدات والاستجابة السريعة للحوادث الإلكترونية.
4. تكثيف برامج التدريب والتوعية الأمنية لجميع العاملين، مع التركيز على أساليب الهندسة الاجتماعية، والتصيد الإلكتروني، وإدارة كلمات المرور، وآليات الإبلاغ عن الحوادث.
5. إجراء اختبارات اختراق وتقييمات أمنية دورية للكشف عن الثغرات ومعالجتها قبل استغلالها من قبل المهاجمين.
6. تعزيز حماية بيانات العملاء من خلال تطبيق تقنيات تشفير متقدمة، وإدارة فعالة لهويات المستخدمين وصلاحيات الوصول، والالتزام بالمعايير الدولية لأمن المعلومات.
7. دعم الإدارة العليا لبرامج الأمن السيبراني وتخصيص الموارد المالية والبشرية اللازمة لتطوير منظومة الأمن المعلوماتي داخل المصرف.
8. وضع خطة شاملة لإدارة المخاطر السيبرانية واستمرارية الأعمال والتعافي من الكوارث، مع مراجعتها وتحديثها بصورة دورية لضمان جاهزية المصرف لمواجهة التهديدات المستقبلية.
9. تعزيز التعاون مع الجهات الرقابية والخبراء المتخصصين في الأمن السيبراني للاستفادة من أفضل الممارسات والمعايير الدولية في حماية الأنظمة المصرفية.

10. إجراء دراسات مستقبلية تتناول أثر التقنيات الحديثة، مثل الذكاء الاصطناعي والحوسبة السحابية وتقنيات تحليل البيانات، في تطوير منظومة الأمن السيبراني بالمصارف الليبية.

المراجع:

1. ريش، عبد الرزاق. (2006). تكنولوجيا المعلومات والاتصال كآلية لتفعيل أداء الجهاز المصرفي. مجلة العلوم الإنسانية، جامعة محمد خيضر بسكرة، الجزائر، العدد 9، ص 157–172.
2. البسطويسي، مروة أحمد عبد الرحمن. (2022). دور حوكمة تكنولوجيا المعلومات في إدارة المخاطر السيبرانية للقطاع المصرفي. [رسالة ماجستير غير منشورة]. كلية التجارة، جامعة طنطا، مصر.
3. جدار، رياض. (2025). دور حوكمة تكنولوجيا المعلومات في تحسين جودة المعلومات المحاسبية وإدارة المخاطر السيبرانية. مجلة الدراسات الاقتصادية والمالية، جامعة الوادي، الجزائر.
4. الحداد، سامي. (2026). التداعيات السيبرانية على الاستقرار المالي والنظامي في القطاع المصرفي. مجلة الدراسات المالية والمصرفية.
5. الحوري، مثنى. (2007). تكنولوجيا المعلومات في المصارف. عمان، الأردن: دار الوراق للنشر والتوزيع.
6. الحيمودي، بدر. (2023). الأمن السيبراني وحماية الأنظمة المعلوماتية. مجلة شمال إفريقيا للنشر العلمي (NAJSP)، المجلد 1، العدد 2.
7. ذيب، محمد. (2012). تكنولوجيا المعلومات والاتصالات. عمان، الأردن: دار المناهج للنشر والتوزيع.
8. زقة، كمال. (2016). إدارة نظم المعلومات وتكنولوجيا الحاسب. عمان، الأردن: دار اليازوري العلمية للنشر والتوزيع.
9. سخون، حنان. (2016). محددات نجاح تطبيق تكنولوجيا المعلومات في القطاع المصرفي. مجلة الاقتصاد والتنمية، جامعة الجزائر 3، الجزائر.
10. الشريف، خالد. (2024). مخاطر السمعة وأثر الهجمات السيبرانية على هجرة الودائع المصرفية. مجلة الأمن الرقمي.
11. الشمري، فهد. (2023). طبيعة التهديدات السيبرانية المصرفية وأنواعها الحديثة. مجلة البحوث التقنية، جامعة الملك سعود.
12. صالح، محمد. (2025). أنظمة الكشف المبكر والتحليل الاستباقي للمخاطر السيبرانية. مجلة تكنولوجيا المعلومات.
13. العبيدي، عمر. (2023). إدارة الهويات وضبط صلاحيات الوصول في البيئة المصرفية. مجلة علوم الحاسب والأمن.
14. العمر، ناصر. (2024). هجمات سلسلة التوريد الرقمية في المؤسسات المالية. المجلة العربية للأمن السيبراني.
15. القصير، إبتسام محمود. (2024). حوكمة تقنية المعلومات للحد من المخاطر السيبرانية وتعزيز أمن المعلومات المحاسبية في المؤسسات الليبية العامة: نموذج مقترح. مجلة جامعة الزيتونة الدولية، ليبيا.
16. كردودي، سهيلة. (2015). تكنولوجيا المعلومات والاتصال ودورها في تحقيق الميزة التنافسية. عمان، الأردن: دار الحامد للنشر والتوزيع.
17. مغربي، يوسف. (2026). استمرارية الأعمال وحفظ النسخ الاحتياطي في ظل التهديدات السيبرانية. مجلة النظم المعلوماتية.
18. المنصوري، علي. (2024). الأنظمة الدفاعية والبرمجيات الوقائية في المصارف التجارية. مجلة التقنيات البنكية.
19. مطروح، عبد القادر، وأونيس، عبد الحفيظ. (2022). الأمن السيبراني والسياسات الأمنية في البيئة الإلكترونية. مجلة الدراسات الحقوقية، الجزائر.
20. النجار، أحمد. (2025). الآثار المالية والتشغيلية للاختراقات السيبرانية في البنوك. مجلة المحاسبة والمراجعة.

ثانياً: المراجع الأجنبية

1. Canelón, J., et al. (2020). Cybersecurity: Tools, Techniques, and Best Practices. Journal of Cyber Policy, p. 112.
2. Alnnale, T. (2026). Predictive Governance in Digital Enterprises: An LSTM-Enhanced Deep Learning Framework for Economic Optimization of IT Incident Management Using Enriched Process Logs. *Al-Farooq Journal of Sciences*, *2*(3), 86-113.
3. Laudon, K. C., & Laudon, J. P. (2020). Management Information Systems: Managing
4. Alnnale, T. (2026). From Reactive to Proactive Governance: A Hybrid LSTM–Gradient Boosting Architecture for Real-Time Anomaly Signal Detection in Multi-Store Retail Supply Chain Decision Systems. *Al-Farooq Journal of Sciences*, *2*(1), 987-1005.