University of Zawia Journal of Economic Sciences (UZJES)
Volume 7, Issue 2, (2025), pp.564-584, ISSN: 3104-3925

Cybersecurity Risks and Threats: A Field Study within the Branches and Agencies of the National Commercial Bank in the Zawia Area

Kamal A. Altreky

Department of Accounting, Faculty of Economics, University of Zawia, Libya

Email: kamalali731599@gmail.com

Received: 04/10/2025 | Accepted: 28/10/2025 | Published: 31/12/2025 | DOI: 10.26629/uzjes.2025.22

ABSTRACT

This study aimed to identify the cybersecurity risks facing commercial banks in Libya and assess their readiness to confront these risks amidst the increasing reliance on digital technologies in banking services. The study adopted a descriptive analytical approach and utilized a questionnaire as the primary data collection tool, targeting a sample of 60 employees working in IT and cybersecurity departments across several Libyan commercial banks. The findings revealed a growing awareness among banks of the importance of cybersecurity and the adoption of various policies and procedures for protection, though with varying levels of implementation. The study also highlighted key challenges, including a shortage of specialized personnel, limited ongoing training, and the need to enhance digital infrastructure. Based on these findings, the study recommended strengthening banks' cybersecurity capabilities by investing in human resources, updating systems, and implementing regular training programs to raise awareness and preparedness among staff.

Keywords: Keywords: Cybersecurity risks, commercial banks, banking services.

مخاطر وتهديدات الأمن السيبراني: دراسة ميدانية داخل فروع ووكالات إدارة فروع المصرف التجاري الوطني بمنطقة الزاوية

كمال علي التريكي

قسم المحاسبة، كلية الاقتصاد، جامعة الزاوية، ليبيا

Email: Kamalali731599@gmail.com

تاريخ الاستلام: 2025/10/04م تاريخ القبول: 2025/10/28 تاريخ النشر: 2025/12/31م

الملخص

هدفت هذه الدراسة إلى التعرف على مخاطر الأمن السيبراني التي تواجه المصارف التجارية في ليبيا، ومدى جاهزيتها لمواجهة تلك المخاطر، في ظل التوسع المتزايد في استخدام التكنولوجيا الرقمية في تقديم الخدمات المصرفية. وقد اعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت أداة الاستبانة لجمع البيانات من عينة مكونة من (60) موظفًا يعملون في أقسام تقنية المعلومات والأمن السيبراني في عدد من المصارف التجارية الليبية. توصلت الدراسة إلى مجموعة من النتائج من أبرزها: إدراك المصارف لأهمية الأمن السيبراني، وتبنيها لسياسات وإجراءات للحماية، رغم وجود تفاوت في مستوى التطبيق بين المصارف. كما أظهرت النتائج وجود تحديات حقيقية تتمثل في نقص الكوادر المتخصصة، وضعف التدريب المستمر للعاملين، إضافة إلى الحاجة لتطوير البنية التحتية الرقمية. وأوصت الدراسة بضرورة تعزيز قدرات المصارف في مجال الأمن السيبراني من خلال دعم الموارد البشرية، وتحديث الأنظمة، وتنفيذ برامج تدريبية دورية تسهم في رفع مستوى الوعي والجاهزية لدى العاملين.

الكلمات الدالة: مخاطر الأمن السيبراني، المصارف التجارية، الخدمات المصرفية.

المقدمة:

يشهد القطاع المصرفي في ليبيا تطورًا متسارعًا في استخدام التكنولوجيا الرقمية لتقديم الخدمات المالية، مما يجعله أكثر عرضة للمخاطر السيبرانية التي تستهدف البيانات والأنظمة المصرفية. تُعد الهجمات الإلكترونية مثل الاحتيال المالي، واختراق الأنظمة، وسرقة البيانات من أبرز المخاطر التي تواجه المصارف التجارية، مما يستدعي تبني استراتيجيات وقائية فعالة لحماية الأصول المالية والمعلومات الحساسة (البغدادي، 2022، ص9).

يبرز تطور الصيرفة الإلكترونية كعنصر أساسي في تحديث القطاع المصرفي، في ظل التحديات التي يفرضها الاندماج في الاقتصاد العالمي والمنافسة الشديدة المدعومة بالتكنولوجيا الحديثة، ومع التحولات السريعة في البيئة المصرفية، أصبح الشكل التقليدي للبنوك مهددًا، مما زاد من تعقيد العمليات المصرفية وأبرز الحاجة إلى تطوير آليات فعالة لإدارة المخاطر، فالقطاع المصرفي يُعد من أكثر القطاعات تعرضًا للمخاطر، خاصة تلك المستقبلية غير المتوقعة، مما يستلزم تبني استراتيجيات متقدمة لضمان استقرار النظام المصرفي وسلامته، وقد أثبتت الدراسات الاقتصادية أن استقرار القطاع المالي هو مفتاح تحقيق تخصيص أمثل للموارد المالية، وهو ما يجعل تطوير ممارسات إدارة المخاطر في البنوك ضرورة حتمية لتعزيز كفاءة الأداء المصرفي وتحقيق نمو اقتصادي مستدام(صواق، 2023، ص11).

يواجه قطاع الخدمات المالية مخاطر سيبرانية متزايدة، حيث تفوق نسبة الهجمات التي تستهدفه القطاعات الأخرى بنسبة 65% وفق تقديرات المصرف الدولي. وتشير تقديرات صندوق النقد الدولي إلى أن التكلفة السنوية المحتملة لهذه الهجمات قد تتراوح بين 270 و350 مليار دولار في حال اتساع نطاقها (أبو الفضل، 2024، ص11)، مما دفع المصارف المركزية، لا سيما في الدول العربية، إلى تشديد الرقابة وإلزام المؤسسات المالية بوضع لوائح صارمة لحماية التطبيقات الإلكترونية، بما في ذلك تثبيت برامج الحماية ضد الاختراق، ومع استمرار الابتكار في تقنيات المعلومات والاتصالات، تواجه المؤسسات المالية مخاطر جديدة مرتبطة بالاستخدام الضار لهذه التقنيات، مما قد يؤدي إلى تعطيل الخدمات المالية وتقويض الاستقرار المالي والثقة في النظام المصرفي. وتؤكد التقارير الدولية والإقليمية خطورة هذه المخاطر، مما يجعل تعزيز الأمن السيبراني ضرورة ملحة لضمان حماية الأنظمة المالية العالمية واستقرارها (أبو الفضل، 2024، ص12).

أولاً: تساؤلات الدراسة

يواجه القطاع المصرفي الليبي، مثل غيره من القطاعات المصرفية حول العالم، تحديات متزايدة في مجال الأمن السيبراني نتيجة التطور السريع للتكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية في تقديم الخدمات المصرفية، ومع توسع استخدام الخدمات الإلكترونية في المصارف التجارية الليبية، تزايدت المخاطر السيبرانية التي تستهدف البنية التحتية المصرفية، مما يشكل مخاطر كبيرة على البيانات المالية وسلامة العمليات المصرفية.

وأشارت التقارير الصادرة عن المصرف الدولي إلى أن نسبة العملاء الذين تعرضوا لهجمات سيبرانية خلال عام 2016 بلغت 65%، بزيادة قدرها 29% مقارنة بالعام السابق. ويعكس هذا الارتفاع الملحوظ مدى تصاعد المخاطر السيبرانية وتأثيرها على القطاع المصرفي، مما دفع السلطات الرقابية عالميًا إلى اتخاذ تدابير تنظيمية وإشرافية تهدف إلى الحد من هذه المخاطر، وتعزيز قدرة المصارف على التصدي لها، وفي هذا السياق، اتخذت المصارف المركزية العربية إجراءات صارمة عبر إصدار تعليمات مصرفية تحث البنوك على تطوير استراتيجيات أمنية متقدمة، بما في ذلك تحسين أنظمة الحماية الإلكترونية، وتعزيز قدرتها على التحوط من الهجمات السيبرانية، لضمان استقرار الأنظمة المالية وحماية العملاء من المخاطر المتزايدة في الفضاء الرقمي(البغدادي، 2021، ص9).

تساؤلات الدراسة

تتمثل تساؤلات الدراسة في الآتي:

1. ما مدى تأثير المخاطر والتهديدات السيبرانية على أداء المصرف التجاري الوطني داخل فروعه بمنطقة الزاوية؟
2. ما أبرز التحديات التي تواجه فروع ووكالات المصرف التجاري الوطني بمنطقة الزاوية في مجال الأمن السيبراني؟
3. إلى أي مدى تتوفر بنية تحتية تقنية كافية وآمنة لحماية الأنظمة المصرفية من الهجمات الإلكترونية داخل فروع المصرف؟
4. ما أبرز الاستراتيجيات الوقائية الممكنة لتعزيز مستوى الأمن السيبراني في المصرف التجاري الوطني بمنطقة الزاوية؟

ثانيًا: أهداف الدراسة

الهدف الرئيس:

قياس مدى تأثير التهديدات السيبرانية على كفاءة وأمن العمليات المصرفية في فروع المصرف التجاري الوطني بمنطقة الزاوية.

الأهداف الفرعية

- تحديد أبرز التحديات والمخاطر التقنية والإدارية التي تواجه فروع المصرف التجاري الوطني وتعوق تحقيق أمن سيبراني فعّال.
- تقويم مستوى الجاهزية التقنية، ومدى توفر البنية التحتية الملائمة لحماية الأنظمة المصرفية من الهجمات الإلكترونية.
- اقتراح استراتيجيات وتوصيات وقائية لتعزيز منظومة الأمن السيبراني داخل فروع المصرف التجاري الوطني بمنطقة الزاوية.

ثالثًا: أهمية الدراسة

تكمن أهمية الدراسة في الآتي:

يساهم هذا البحث في تقديم حلول وتقنيات حديثة تهدف إلى الحد من المخاطر السيبرانية التي تواجه القطاع المصرفي، مما يُثري الأدبيات العلمية المتعلقة بالأمن السيبراني في البيئة المالية الليبية. كما يُعد هذا البحث نقطة انطلاق لدراسات مستقبلية تتناول الجوانب التقنية والقانونية والتنظيمية للأمن السيبراني، خاصة في ظل التحديات المتزايدة التي تواجه المصارف الليبية. ويساعد أيضًا في تطوير استراتيجيات فعالة لحماية البيانات والمعاملات المالية من الهجمات الإلكترونية، بما يضمن استقرار النظام المصرفي ويحافظ على استمرارية عمله. ومن خلال تعزيز منظومة الحماية الرقمية، يمكن للمصارف كسب ثقة العملاء وتحسين سمعتها، ما ينعكس بشكل إيجابي على معدلات استخدام الخدمات المصرفية الرقمية. إضافة إلى ذلك، يقدّم البحث مجموعة من التوصيات العملية لصانعي القرار في المصارف والجهات الرقابية، بهدف تبني أفضل الممارسات في مواجهة التهديدات السيبرانية المتصاعدة.

فرضيات الدراسة

1 – الفرضية الرئيسية

تزايد المخاطر السيبرانية يؤثر سلبًا على أداء المصارف التجارية الليبية، مما يؤدي إلى تعطيل الخدمات المصرفية وتسريب بيانات العملاء

2 – الفرضيات الفرعية

- هناك ضعف في البنية التحتية للأمن السيبراني في المصارف الليبية، مما يزيد من مخاطر التعرض للهجمات الإلكترونية.
- غياب التشريعات والسياسات الصارمة يضعف قدرة المصارف على حماية بياناتها وأنظمتها من الهجمات السيبرانية.
- هل يعاني العاملون بالمصرف التجاري الوطني من قلة وعي فيما يتعلق بتهديدات الأمن السيبراني؟
- تطوير استراتيجيات وقائية متقدمة، مثل استخدام الذكاء الاصطناعي والتشفير، يساهم في تعزيز الأمن السيبراني.

6. التعاون بين المصارف الليبية والجهات الرقابية والحكومية يساهم في تحسين الاستجابة للهجمات السيبرانية وتقليل المخاطر.

سادسًا: منهج الدراسة

توظف الدراسة الحالية المنهج الوصفي باعتباره المنهج المناسب للظاهرة محل الدراسة لتحليل الأمن السيبراني في المصارف التجارية الليبية: التحديات والاستراتيجيات الوقائية إضافة إلى استخدام أداة صحيفة الاستبيان لجمع البيانات والمعلومات المطلوبة من الدراسة الحالية، وتشمل الأداة مجموعة من الأسئلة والمقاييس كترجمة لأهداف الدراسة على عينة من العاملين (المصرف التجاري الوطني).

سابعًا: حدود الدراسة

- **الحدود الموضوعية:** تُركز هذه الدراسة على تحليل مخاطر وتهديدات الأمن السيبراني التي تواجه فروع المصرف التجاري الوطني، وذلك من خلال:

التعرف على مدى انتشار الهجمات السيبرانية التي تستهدف أنظمة المصرف ، وتحديد أبرز أنواع التهديدات الإلكترونية الشائعة داخل بيئة العمل المصرفي.

الوقوف على نقاط الضعف التقنية والإجرائية في منظومة الأمن السيبراني داخل المصرف.

صياغة مجموعة من التوصيات والاستراتيجيات الوقائية التي يمكن أن تُسهم في تعزيز جاهزية المصرف لمواجهة التحديات السيبرانية وضمان استمرارية الأعمال.

- **الحدود المكانية:** تُجرى هذه الدراسة ميدانيًا داخل فروع ووكالات إدارة فروع المصرف التجاري الوطني في منطقة الزاوية، باعتبارها تمثل نموذجًا واقعيًا لتقييم جاهزية المصارف الليبية في مواجهة المخاطر السيبرانية.
- **الحدود الزمانية:** تُنفذ هذه الدراسة خلال العام 2025م، وهو الإطار الزمني الذي تُجمع فيه البيانات وتحلل النتائج المتعلقة بواقع الأمن السيبراني في المصرف التجاري الوطني بمنطقة الزاوية.

ثامناً: بيئة ومجتمع وعينة الدراسة

تنحصر بيئة الدراسة في القطاع المصرفي وما يتعرض له من مخاطر سيبريانية، أما مجتمع الدراسة فيتحدد في القطاع المصرفي الليبي – (فروع ووكالات إدارة فروع منطقة الزاوية المصرف التجاري الوطني)، أما عينة الدراسة فهي عينة قصدية لعدد (60) موظفا من المسؤولين والمشرفين والعاملين في الأقسام المختصة بالخدمات الالكترونية والمنظومات وبنظم الحماية من المخاطر السبريانية (بالمصرف التجاري الوطني).

تاسعاً: مفاهيم الدراسة

مفهوم الأمن السيبراني

يعرف الأمن السيبراني على "أنه يهتم بتصميم وتطبيق التقنيات والعمليات، والضوابط والممارسات اللازمة لحماية الأنظمة، والشبكات والبرامج والأجهزة والبيانات من التعرض للهجمات، والمخاطر الإلكترونية والفيروسات وسد ثغرات نقاط الضعف المباشرة أو غير المباشرة، ويتم ذلك من خلال مجموعة من الإجراءات منها القيام بهجوم تجريبي متعمد لاكتشاف الثغرات والعمل على إصلاحها، وتصميم مجموعة من إجراءات الاستجابة والتخفيف من الآثار الناتجة عن التعرض للخطر أو التلف أو الوصول غير المرخص به؛ حيث يسعى المخترق للتلاعب بالنظام الرقمي للضحية والسيطرة عليه بصورة غير قانونية باستخدام أجهزة متطورة أو استغلال ثغرات النظام، أو انخفاض الوعي التكنولوجي للمستخدم" (أبو الفضل، 2024، ص12).

مفهوم البنوك التجارية

تعرف البنوك التجارية "هي مؤسسات ائتمانية غير متخصصة تضطلع أساسا بتلقي ودائع الأفراد القابلة للسحب لدى الطلب أو بعد أجل قصير، والتعامل بصفة أساسية في الائتمان قصير الأجل، ويطلق على هذه البنوك اصطلاح بنوك الودائع" (عاصي، 2024، ص11).

الدراسات السابقة

1. **دراسة (التائب والسائح، 2025) بعنوان أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية.** تهدف هذه الدراسة إلى القيام بمحاولة التعرف على تعريف الأمن السيبراني المحاسبي، توضيح أهمية الأمن السيبراني المحاسبي في المصارف، تحديد الصعوبات والعراقيل التي تواجه تطبيق الأمن السيبراني المحاسبي في المصارف، تناول أهم المنافع التي يمكن تحقيقها أثناء تنفيذ الأمن السيبراني المحاسبي في المصارف، واعتمدت الدراسة على المنهج الوصفي التحليلي، وتتكون عينة الدراسة من 189 عاملا وعاملة، وتوصلت الدراسة إلى جملة من النتائج تتمثل في أن هناك اهتماما فائق بالأمن السيبراني المحاسبي في المصارف التجارية في مدينة سرت، وتفاقم مستوى الوعي بأهمية الأمن السيبراني المحاسبي من أجل ضمان حماية المصارف والعملاء فيها من المخاطر المتوقعة، وتوصي الدراسة بضرورة القيام بعقد دورات وورش عمل منتظمة للعاملين في المصارف من أجل توعيتهم بأحدث المخاطر السيبرانية، إضافة إلى ضرورة القيام بالتعاون مع المصرف المركزي والهيئات الحكومية الأخرى لتبادل المعلومات والخبرات في مجال الأمن السيبراني.
2. **دراسة (محمد وموراد، 2023) بعنوان تحديات الأمن السيبراني لأنظمة المعلومات في البنوك والمؤسسات المالية.** تهدف هذه الدراسة إلى تناول الجرائم الإلكترونية في البنوك والمؤسسات المالية، تناول تحديات ومصادر الخطر في البنوك والمؤسسات المالية، تناول طرق الوقاية من الجرائم الإلكترونية، وتوضيح النصائح المتباينة والتوجيهات الأمنية المطروحة للعناصر البشرية المتمثلة في العميل المصرفي المستعمل والعاملين على حد السواء، وتوصي الدراسة بضرورة تقديم العديد من النصائح والتوجيهات المطروحة من العملاء من أجل التعامل مع المهام الإلكترونية من أجل المساهمة في ضمان أمن المعاملات المصرفية الإلكترونية.

3. **دراسة (يوسف، 2024) بعنوان تقييم تأثير المخاطر السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية.** تهدف هذه الدراسة إلى محاولة تسليط الضوء على واقع المخاطر السيبرانية المستهدفة لأنظمة المعلومات المحاسبية في المنظمات والشركات المالية الليبية، وتقييم مدى تأثير تلك المخاطر على موثوقية وسلامة سرية تلك الأنظمة والبيانات المالية المخزنة فيها، إضافة إلى مساهمتها في تحديد نقاط الضعف والفجوات الأمنية التي يمكن استغلالها من خلال الهيئات الخبيثة، واعتمدت الدراسة على المنهج الوصفي، وتوصلت الدراسة إلى جملة من النتائج تتمثل في أن المنظمات المالية الليبية تواجه مخاطر سيبرانية متزايدة ومتباينة، وأن المخاطر السيبرانية تؤثر تأثيراً عظيماً على اقتصاد المنظمات المالية الليبية، وتوصي الدراسة بضرورة تعزيز الوعي والتدريب، تحديث السياسات والإجراءات، تعزيز التعاون والشراكات، وتطوير التكنولوجيا والبنية التحتية، التشجيع والتوعية للعملاء.

الإطار النظري للدراسة

أولاً: الأمن السيبراني المفهوم والأهمية وأهم أدواته

مفهوم الأمن السيبراني

معنى كلمة سيبرأني (cyber) تطلق كلمة سيبرأني على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الانترنت Internet، والفضاء السيبراني يعني الفضاء الإلكتروني (Cyberspace)، وهو يعني كل ما يتعلق بشبكات الحاسوب، والانترنت Internet والتطبيقات المختلفة مثل الواتس آب والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها كتحويل الأموال عبر النت، والشراء أون لاين وغيرها من ألاف الخدمات في جميع مجالات الحياة على مستوى العالم"(علي، طه، 2023، ص11).

ويعرف إجرائياً "بأنه حماية الأفراد وبياناتهم وحساباتهم من الهجمات الإلكترونية بهدف الحفاظ على سلامة ونزاهة المعلومات المخزنة داخل هذه الأنظمة الإلكترونية" (المري، 2023، ص12).

أهمية الأمن السيبراني

في ظل التطور الرقمي المتسارع، أصبح الأمن السيبراني عنصرًا حيويًا لحماية الأفراد والمؤسسات من المخاطر والمخاطر الإلكترونية. يهدف الأمن السيبراني إلى حماية البيانات، تأمين الشبكات، وضمان استمرارية الأعمال دون تعرضها للاختراق أو السرقة، وأهمية الأمن السيبراني تشمل (السمحان، 2020، ص11):

- حماية المعلومات وضمان سلامتها:
  - منع الوصول غير المصرح به إلى البيانات.
  - الحفاظ على سرية المعلومات ومنع العبث بها.
  - ضمان توفر البيانات عند الحاجة إليها دون انقطاع.
- حماية الأجهزة والشبكات:
  - تأمين أجهزة الكمبيوتر والخوادم من الهجمات الإلكترونية.
  - منع البرمجيات الخبيثة والفيروسات من اختراق الأنظمة.
  - تعزيز أمان الشبكات لتكون خط الدفاع الأول ضد الهجمات.
- استكشاف الثغرات الأمنية ومعالجتها:
  - تحليل الأنظمة واكتشاف نقاط الضعف قبل استغلالها من القراصنة.
  - تحديث البرمجيات وإغلاق الثغرات الأمنية لحماية المستخدمين.
- استخدام أدوات المصادر المفتوحة في الأمن السيبراني:
  - تعزيز الأمان من خلال تطوير أدوات مفتوحة المصدر وتحليل أكوادها.
  - الاستفادة من خبرات المجتمعات التقنية في تحسين أنظمة الحماية.
- توفير بيئة عمل آمنة عبر الانترنت Internet:
  - تأمين عمليات التصفح والمراسلات لحماية البيانات الحساسة.
  - تقليل مخاطر الهجمات السيبرانية التي تستهدف المؤسسات والأفراد.

أدوات الأمن السيبراني

أدوات الأمن السيبراني مجموعة أدوات وبرامج تقنية مصممة لحماية الأنظمة والبيانات والشبكات من المخاطر السيبرانية، هناك بعض الأدوات الشائعة في مجال الأمن السيبراني (الحيمودي، 2023، ص13):

1. أدوات اكتشاف المخاطر (Threat Intelligence Tools): تساعد في جمع وتحليل المعلومات حول المخاطر السيبرانية المحتملة والتحقق من سلامة الأنظمة.

2. أدوات اكتشاف الاختراق (Penetration Testing Tools) :تستخدم لاختبار قوة الأمان من خلال محاكاة هجمات اختراق لتحديد الثغرات والضعف في الأنظمة.

3. أدوات إدارة الهوية والوصول (Identity and Access Management Tools): تساعد في إدارة الهوية وصلاحيات الوصول للمستخدمين لضمان عدم وجود وصول غير مصرح به.

4. أدوات حماية الشبكات (Network Security Tools) :تشمل جدران الحماية وأنظمة الكشف عن التسلل لحماية الشبكات من الهجمات السيبرانية.

5. أدوات تشفير البيانات (Data Encryption Tools): تساعد في تشفير البيانات لحمايتها من الوصول غير المصرح به.

6. أدوات الحماية من البرامج الضارة (Anti-Malware Tools) :تكشف وتزيل البرامج الضارة والفيروسات من الأنظمة والشبكات.

7.أدوات إدارة الحواسيب والأجهزة (Endpoint Security Tools) :تساعد في حماية الأجهزة النهائية مثل الكمبيوترات والهواتف الذكية من المخاطر السيبرانية.

8. أدوات رصد الأمان (Security Monitoring Tools): تقوم برصد وتحليل الأنشطة غير المعتادة في الشبكات والأنظمة لاكتشاف الهجمات السيبرانية.

وظائف المصارف التجارية

تتمثل وظائف المصارف التجارية في الآتي (الغافود، مزيكه، 2016، ص13):

1. قبول الودائع (Deposit Acceptance):

- تُعد الوظيفة الأساسية للبنوك التجارية، حيث توفر للعملاء حسابات توفير، وحسابات جارية، وودائع لأجل لحفظ أموالهم بأمان.
- تمنح العملاء الفوائد على بعض الودائع، بينما تستخدم هذه الأموال في الإقراض والاستثمار.

2. تقديم القروض والتمويل (Lending and Credit Services):

- تُقدم المصارف التجارية قروضًا للأفراد والشركات لتمويل المشاريع، العقارات، والتعليم، والمركبات، وغيرها.
- تُحدد أسعار الفائدة بناءً على سياسة المصرف والسوق المالية.

3. تحويل الأموال وخدمات الدفع (Money Transfer & Payment Services):

- توفير خدمات الدفع مثل الشيكات، الحوالات المصرفية، بطاقات الائتمان، المحافظ الإلكترونية، وخدمات الدفع الإلكتروني.
- تسهيل التحويلات المحلية والدولية عبر SWIFTأو أنظمة الدفع الأخرى.

4. الاستثمار وإدارة الأصول (Investment & Asset Management):

- تستثمر المصارف التجارية في السندات والأسهم والصناديق الاستثمارية لتحقيق الأرباح.
- تقدم خدمات إدارة الأصول للأفراد والشركات لمساعدتهم في الاستثمار بطرق آمنة ومربحة.

5. تمويل التجارة الدولية (Trade Finance):

- تقديم خطابات الاعتماد (LCs) والضمانات المصرفية لتسهيل عمليات الاستيراد والتصدير.
- توفير خدمات التحصيل المستندي لحماية حقوق المستوردين والمصدرين.

المحور الثالث (تحليل البيانات ونتائج البحث).

1. طرق جمع البيانات

تم استخدام الاستبيان كأداة رئيسية لجمع البيانات في هذا البحث، نظرًا لقدرته على توفير معلومات دقيقة وشاملة حول موضوع الدراسة، وتم تصميم الاستبيان بعناية ليشمل ثلاثة أقسام رئيسية تغطي مختلف جوانب البحث، مما يضمن جمع بيانات متكاملة تسهم في تحقيق أهداف الدراسة.

يبدأ الاستبيان بجمع المعلومات الديموغرافية للمشاركين، مثل العمر، والجنس، والمؤهل العلمي، وأعوام الخدمة وهذه البيانات ضرورية لتحديد الخصائص الأساسية للعينة المشاركة وتحليل النتائج بناءً على الفروقات الديموغرافية، مما يساعد في الوصول إلى استنتاجات دقيقة ومعمقة.

أما القسم الثاني من الاستبيان، فهو مخصص للأسئلة المتعلقة بـ الأمن السيبراني يتناول هذا القسم تقييم مدى تطبيق أنظمة وسياسات الأمن السيبراني في المصارف التجارية، ومدى وعي الموظفين بأهمية هذه الأنظمة، إضافة إلى معرفة التقنيات المستخدمة لمواجهة المخاطر السيبرانية وتساهم هذه الأسئلة في فهم مدى تأثير الأمن السيبراني في حماية البيانات المالية.

القسم الثالث يركز على المصارف التجارية، حيث يتناول دور الأمن السيبراني في تحسين المصارف التجارية .

تم توزيع الاستبيان على عينة من المحاسبين العاملين بفروع ووكالات إدارة فروع منطقة الزاوية بالمصرف التجاري الوطني، وذلك باستخدام وسائل متعددة، مثل التوزيع الورقي أو الإلكتروني، بهدف ضمان الوصول إلى أكبر عدد ممكن من المشاركين، وزيادة تمثيل العينة وموثوقية البيانات المستخلصة. وقد أُخذ هذا التنوع في طرق التوزيع بعين الاعتبار لتجاوز القيود الزمنية والمكانية التي قد تعيق مشاركة بعض الأفراد، مما يعزز من شمولية النتائج وقابليتها للتعميم.

يُعد اختيار أسلوب البحث عنصرًا أساسيًا لضمان تحقيق أهداف الدراسة والوصول إلى نتائج دقيقة وموثوقة. في هذه الدراسة، التي تتناول الأمن السيبراني في المصارف التجارية الليبية: التحديات والاستراتيجيات الوقائية)، تم اعتماد المنهج الكمي كأساس لجمع وتحليل البيانات، وذلك باستخدام الاستبيان كأداة رئيسية.

يعتمد المنهج الكمي على جمع البيانات العددية وتحليلها باستخدام الأدوات الإحصائية لتحديد العلاقات والأنماط بين المتغيرات. ويُعد هذا النهج ضروريًا لقياس تأثير الأمن السيبراني على مصداقية التقارير المالية بشكل دقيق وممنهج، حيث يوفر القدرة على تحليل البيانات بشكل موضوعي واستخلاص نتائج قائمة على معطيات كمية.

بعد جمع البيانات، تم تحليلها باستخدام أدوات إحصائية متقدمة لاستخلاص النتائج التي تُسهم في الإجابة على أسئلة البحث وتحقيق أهدافه. يضمن هذا الأسلوب دقة وشمولية البيانات المجمعة، مما يعزز موثوقية النتائج ويساعد في تقديم توصيات قائمة على أدلة واضحة تدعم عملية اتخاذ القرار في المصارف التجارية.

الأدوات المستخدمة في جمع البيانات

تم استخدام الاستبيان كأداة رئيسية لجمع البيانات من المحاسبين في المصرف التجاري الوطني بليبيا وتعد الاستبيانات واحدة من أكثر الأدوات شيوعًا في البحوث الكمية، حيث تسهم في جمع البيانات بشكل مباشر من عينة الدراسة.

تصميم الاستبيان

1. الأجزاء الرئيسية للاستبيان

الجزء الأول: معلومات ديموغرافية: يتضمن أسئلة حول العمر، الجنس، المؤهل العلمي، وعدد أعوام الخدمة.

الجزء الثاني: الأسئلة المتعلقة بالأمن السيبراني: يتضمن أسئلة لقياس درجة تطبيق أنظمة

الأمن السيبراني في المصارف التجارية.

الجزء الثالث: الأسئلة المتعلقة بالمصارف التجارية: يهدف إلى قياس تأثير الأمن السيبراني على المصارف التجارية

نوعية الأسئلة

تم استخدام أسئلة مغلقة مثل أسئلة ذات اختيارات متعددة لتحديد مدى الاتفاق أو الاختلاف مع العبارات.

تم تصميم الأسئلة باستخدام مقياس ليكرت الخماسي، الذي يتراوح من "موافق جدًا" إلى "غير موافق جدًا، لقياس اتجاهات المشاركين بدقة.

3. التحقق من مصداقية وموثوقية الاستبيان:

تم إجراء اختبار أولي (Pilot Study) على عينة صغيرة من المحاسبين للتأكد من وضوح الأسئلة وملاءمتها.

تم استخدام معامل كرونباخ ألفا لقياس موثوقية الاستبيان، حيث يُعتبر معاملا يزيد عن 0.7 مؤشرا على درجة موثوقية جيدة.

جدول (1-1): نتائج التحليلات الإحصائية لأدوات الدراسة.

نوع التحليل الإحصائي	القيمة الإحصائية	الدلالة الإحصائية
التكرارات والنسب المئوية	**التكرار = 85** **النسبة المئوية = 56.7%**	**—**
المتوسط الحسابي والانحراف المعياري	**المتوسط = 4.12 الانحراف المعياري = 0.68**	**—**
معامل الثبات (Cronbach's Alpha)	**α = 0.89**	**دال إحصائيًا**
معامل الارتباط بيرسون (Pearson Correlation)	**r = 0.77**	**دال عند مستوى 0.01**

التحليل الإحصائي للبيانات

بعد جمع البيانات من الاستبيانات الموزعة على المحاسبين العاملين بفروع ووكالات إدارة فروع منطقة الزاوية المصرف التجاري الوطني تم استخدام التحليل الإحصائي لتفسير النتائج واستخلاص الاستنتاجات، وتم تقسيم التحليل إلى ثلاث مراحل رئيسية: تحليل الخصائص الديموغرافية، تحليل الأسئلة المتعلقة بالأمن السيبراني، وتحليل الأسئلة المتعلقة بالمصارف التجارية.

1. تحليل الخصائص الديموغرافية

تم تحليل الخصائص الديموغرافية للمشاركين لفهم تركيبة العينة ودورها في التأثير على النتائج.

جدول (2-1): تحليل الخصائص الديموغرافية.

الخاصية	الفئة	التكرار	النسبة المئوية
	أقل من 30 سنة	20	%20
	30 – 40 سنة	10	%10
	بين 41-50 سنة	20	%10
	أكثر من 50 سنة.	10	%10
الجنس	الذكر	45	%45
	الأنثى	15	%15
المؤهل العلمي	دبلوم	25	%25
	بكالوريوس	30	%30
	ماجستير	5	%5
سنوات الخدمة	أقل من 5 سنوات	10	%10
	بين 5-10 سنوات	15	%15
	بين 11-20 سنة	15	%15
	أكثر من 20 سنة	20	%20

يهدف هذا البحث إلى دراسة تأثير الخصائص الديموغرافية للعينة على آرائهم وتصوراتهم بشأن دور الأمن السيبراني في تعزيز مصداقية التقارير المالية. وقد أظهرت النتائج كما في الجدول (1-2) أن غالبية المشاركين ينتمون إلى الفئة العمرية 30-40 سنة بنسبة 40%، تليها الفئة العمرية 41-50 سنة بنسبة

20%. يشير ذلك إلى أن أغلب أفراد العينة يمتلكون خبرة مهنية كافية، حيث تمثل هذه الفئات العمرية مرحلة النضج المهني والقدرة على تقييم تأثير الأمن السيبراني على بيئة العمل المالية.

أما من حيث المؤهلات العلمية، فقد تبين أن 60% من المشاركين حاصلون على درجة البكالوريوس، مما يعكس مستوى تعليميًا جيدًا بين أفراد العينة، في حين يحمل 20% منهم درجة الماجستير، مما يشير إلى اهتمام واضح بالتطوير الأكاديمي والمهني في المجال المالي.

وبالنسبة لـ أعوام الخدمة، فقد أظهرت النتائج أن 35% من المشاركين لديهم خبرة تتراوح بين 5–10 سنوات، بينما يمتلك 30% منهم خبرة تتراوح بين 11–20 سنة. تعكس هذه التوزيعات تمثيلًا واسعًا لمستويات الخبرة المختلفة، مما يعزز مصداقية الدراسة، حيث يضم التحليل مشاركين من ذوي الخبرة العملية الكافية لتقييم تأثير أنظمة الأمن السيبراني على عملهم اليومي وإعداد التقارير المالية.

تحليل الأسئلة المتعلقة بالأمن السيبراني:

تم حساب المتوسطات والانحراف المعياري للإجابات المتعلقة بالأمن السيبراني لتحديد مستوى وعي وتطبيق أنظمة الأمن السيبراني في المصارف:

جدول (3–1): الأسئلة المتعلقة بالأمن السيبراني.

السؤال	متوسط	الانحراف المعياري
تطبيق أنظمة الحماية من الهجمات السيبرانية.	**4.2**	**0.8**
توفر سياسة واضحة للتعامل مع المخاطر.	**4**	**0.9**
تدريب الموظفين بانتظام.	**3.8**	**1**
توظيف التكنولوجيا المتقدمة لتعزيز أمن المعلومات	**4.1**	**0.7**
مراقبة الأنظمة المالية بشكل مستمر.	**4.3**	**0.6**

أظهرت نتائج البحث أن أنظمة الأمن السيبراني مطبقة بشكل جيد في المصارف التجارية، حيث أعرب المشاركون عن اتفاقهم الكبير على وجود سياسات واضحة للتعامل مع المخاطر السيبرانية. كما أشاروا إلى توفر تقنيات حديثة مثل التشفير وجدران الحماية لحماية البيانات المالية، وأكدوا أهمية التدريب المنتظم للموظفين والمراقبة المستمرة للأنظمة. تعكس هذه النتائج وعي المصارف المتزايد بالمخاطر السيبرانية واتخاذها إجراءات استباقية للحد من المخاطر المحتملة.

ركز الجزء الثاني من البحث على تقييم مدى تطبيق أنظمة وسياسات الأمن السيبراني في المصارف التجارية، حيث أظهرت الإحصائيات إدراكًا واسعًا لأهمية الأمن السيبراني، وهو ما انعكس في ارتفاع متوسطات الإجابات على الأسئلة ذات الصلة.

– بلغ متوسط الإجابة على سؤال "إلى أي مدى يتم تطبيق أنظمة الحماية من الهجمات السيبرانية في المصرف الذي تعمل به؟" 4.2، مع انحراف معياري 0.8، مما يشير إلى اتفاق غالبية المشاركين على وجود أنظمة حماية فعالة.

– أما متوسط الإجابات حول وجود سياسات واضحة للتعامل مع المخاطر السيبرانية فبلغ 4.0، مما يعكس مستوى مقبولًا من التنظيم داخل المصارف، مما يدل على إدراك المؤسسات المالية لأهمية السياسات الرسمية في الحد من المخاطر.

– فيما يتعلق بتدريب الموظفين، بلغ متوسط الإجابة 3.8 مع انحراف معياري 1.0، مما يشير إلى الحاجة إلى تعزيز برامج التدريب المنتظم لرفع وعي الموظفين بمخاطر الأمن السيبراني.

– أما استخدام التقنيات الحديثة مثل التشفير وجدران الحماية، فقد سجل متوسط إجابة قدره 4.1، مما يعكس مستوى جيدًا من تبني التكنولوجيا المتطورة لحماية البيانات المالية.

– أخيرًا، بلغ متوسط الإجابة على سؤال "مدى مراقبة الأنظمة المالية بشكل مستمر" 4.3 مع انحراف معياري 0.6، مما يدل على اهتمام كبير بالمراقبة المستمرة لضمان الاكتشاف السريع لأي مخاطر سيبرانية.

3. تحليل الأسئلة المتعلقة بالمصارف التجارية:

تم حساب المتوسطات والانحراف المعياري للإجابات المتعلقة تأثير تحديات الأمن السيبراني على المصارف التجارية:

جدول (4–1): تحليل الأسئلة المتعلقة بالمصارف التجارية.

السؤال	متوسط	الانحراف المعياري
يتم تخصيص موارد كافية (مالية وبشرية وتقنية) لتنفيذ استراتيجيات الأمن السيبراني.	4.5	0.5
يوجد أهداف واضحة ومحددة للأمن السيبراني في استراتيجيات البنوك التجارية.	4.4	0.6

تدريب الموظفين بانتظام.	4.6	0.4
يتم تخصيص موارد كافية (مالية وبشرية وتقنية) لتنفيذ استراتيجيات الأمن السيبراني.	4.3	0.7
تتضمن استراتيجيات الأمن السيبراني في البنوك الليبية تعزيز التعاون والتنسيق مع الجهات المعنية لمكافحة الجرائم السيبرانية	4.7	0.3

بينت البيانات أن المشاركين يرون أن الأمن السيبراني له تأثير إيجابي كبير على المصارف التجارية، حيث تجاوز متوسط الإجابات 4.3 في جميع الأسئلة، مع تسجيل أعلى قيمة (4.7) لسؤال تعزيز الثقة بين الأطراف المعنية.

أظهرت النتائج أن أنظمة الأمن السيبراني مطبقة بشكل جيد في المصارف التجارية. المشاركون أعربوا عن اتفاقهم الكبير على وجود سياسات واضحة للتعامل مع المخاطر السيبرانية، وتوفر تقنيات حديثة مثل التشفير وجدران الحماية لحماية البيانات المالية، وكما أشاروا إلى أهمية التدريب المنتظم للموظفين ومراقبة الأنظمة بشكل مستمر وهذه النتائج تدل على أن المصارف تدرك المخاطر السيبرانية المتزايدة وتعمل بشكل استباقي للحد من المخاطر.

حيث سجلت أعلى عبارة" تتضمن استراتيجيات الأمن السيبراني في البنوك الليبية تعزيز التعاون والتنسيق مع الجهات المعنية لمكافحة الجرائم السيبرانية" متوسط بنسبة 4.7 وانحراف معياري بنسبة .0.3.

الاستنتاجات

1. أظهرت الدراسة أن المصارف التجارية الليبية تدرك بشكل متزايد أهمية الأمن السيبراني، حيث تتبنى سياسات وإجراءات لحماية بياناتها المالية. ومع ذلك، يظل هناك تفاوت في مستوى التنفيذ بين المصارف.
2. تواجه المصارف تحديات تتعلق بنقص الكوادر المؤهلة في مجال الأمن السيبراني، بالإضافة إلى الحاجة إلى تطوير البنية التحتية التكنولوجية لمواكبة المخاطر الحديثة.
3. رغم وجود أنظمة حماية مثل التشفير وجدران الحماية، إلا أن هناك حاجة لتعزيزها عبر تكامل الحلول الأمنية المتطورة وتحليل البيانات لاكتشاف المخاطر المحتملة.
4. كشفت النتائج عن ضرورة تحسين برامج التدريب لرفع وعي الموظفين بالمخاطر السيبرانية، حيث يُعد العامل البشري أحد أبرز نقاط الضعف في منظومة الحماية.

5. تتبنى المصارف سياسات للمراقبة المستمرة، لكنها بحاجة إلى تطوير استراتيجيات استجابة أسرع عند حدوث اختراقات أمنية.
6. لا تزال بعض أنظمة الأمن بحاجة إلى اختبارات تقييم دورية للكشف عن الثغرات وتعزيز الحماية.
7. هناك حاجة لحماية بيانات العملاء بشكل أقوى، خاصة في ظل التهديدات الرقمية المتطورة.

التوصيات

1. ضرورة الاستثمار في تقنيات حديثة مثل الذكاء الاصطناعي وأنظمة التحليل المتقدمة لاكتشاف الهجمات السيبرانية والحد منها.
2. تنفيذ برامج تدريب مستمرة للموظفين حول الأمن السيبراني، مع التركيز على أفضل الممارسات لحماية البيانات وتجنب الهجمات الاحتيالية.
3. إنشاء فرق متخصصة في الأمن السيبراني داخل المصارف تكون مسؤولة عن الاستجابة السريعة للحوادث والتعامل مع الهجمات المحتملة بفعالية.
4. وضع سياسات موحدة للأمن السيبراني بالتنسيق مع الجهات التنظيمية لضمان الامتثال للمعايير الدولية وتعزيز تبادل المعلومات حول المخاطر المحتملة.
5. استخدام تقنيات المصادقة متعددة العوامل (MFA) وتقنيات التشفير القوية لحماية بيانات العملاء والمعاملات المالية.
6. اعتماد أنظمة مراقبة أمنية تعمل بشكل آلي لاكتشاف الأنشطة غير العادية والاستجابة لها قبل وقوع أضرار.
7. تنفيذ عمليات تقييم واختبار دورية على أنظمة المصارف للكشف عن أي نقاط ضعف محتملة وتعزيزها.

قائمة المراجع

1. بغدادي، مروة فتحي السيد. (2021). اقتصاديات الأمن السيبراني في القطاع المصرفي. مجلة البحوث القانونية والاقتصادية (المنصورة)، 11(76)، 1446-1516.
2. أبو الفضل، عبدالعال مصطفى. (2024). أثر الإنفاق في الأمن السيبراني على الأداء في البنوك التجارية المصرية: مع دراسة ميدانية. مجلة الدراسات التجارية المعاصرة, 10(17) , 1851-1906.

3. سمحان، مني عبد الله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية، جامعة المنصورة، (111).
4. عاصي، لمياء حسين. (2024). المصارف التجارية ودورها في المشاريع الاستثمارية. مجلة كلية الحقوق والعلوم السياسية، 25(23).
5. صواق، عبد القادر. وآخرون. (2023). أثر جاهزية الأمن السيبراني على الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة دراسة حالة مصرف BDL بغرداية. أبحاث اقتصادية معاصرة, 6(1), 353-372.
6. علي، عبد الصمد العلي. طه، مريم هاشم. (2023). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإلكترونية. أدب البصرة، 106(1).
7. مري، راشد محمد حمد. (2023). الأمن السيبراني وحماية الأنظمة الإلكترونية: دراسة تحليلية تأصيلية. مجلة الدراسات القانونية والاقتصادية مج 9 1 959 – 1008.
8. تائب، علي مفتاح، والسائح، جبريل عمر(2025): أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية، دراسة تطبيقية على المصارف التجارية العاملة في مدينة سرت، مجلة جلة الدراسات الاقتصادية، المجلد 8، العدد 1.
9. محمد، شايب، وموراد، حمادي(2023): تحديات الأمن السيبراني لأنظمة المعلومات في البنوك والمؤسسات المالية، مجلة إنارة للدراسات الاقتصادية، الإدارية، والمحاسبية، المجلد 4، العدد 1.
10. حيمودي، بدر. (2023). الأمن السيبراني وحماية الأنظمة المعلوماتية. مجلة شمال إفريقيا للنشر العلمي. 1 (2).
11. يوسف، عبد السلام عطية عبد السلام(2024): تقييم تأثر المخاطر السيبرانية على نظم المعلومات المحاسبية في المؤسسات المالية الليبية، دراسة وصفية، المجلة العلمية للدراسات التجارية والبيئية، المجلد 15، العدد 1.
12. شرف، نجم أديولي(2020): الأمن السيبراني وإشكالاته الفقهية، دراسة مقارنة بين قانوني الأمن السيبراني القطري والنيجري، خطة بحث تكميلي لنيل درجة الماجستير، جامعة حمد بن خليفة، كلية أحمد بن محمد العسكرية، تخصص الفقه المعاصر.
13. صويدق، أحمد نصيب. الجالي، سحر مصطفى. (2022). مدى مساهمة جودة الخدمات المصرفية الالكترونية في تعزيز القدرة التنافسية بين المصارف التجارية الليبية دراسة ميدانية على مصرفي شمال

أفريقيا والتجاري بمدينة طبرق. المؤتمر العلمي الدولي السادس لكلية الاقتصاد الخمس التنافسية الاقتصادية تقييم للواقع واستشراف المستقبل.

14. فلاح، فاطمة. بالحاج، أسماء. (2013). دور البنوك التجارية في تمويل العمليات الاستثمارية دراسة حالة المصرف الوطني الجزائري (Doctoral dissertation). جامعة قاصدي مرباح – ورقلة –، كلية والعلوم الاقتصادية والعلوم التجارية وعلوم التسيير.

15. غافود، مختار عبد السلام علي. مزيكه، فرج أحمد. (2016). محددات مخاطر السيولة بالمصارف التجارية دراسة ميدانية عن مصرف الجمهورية فرع زليتن. مجلة العلوم الاقتصادية والسياسية 7 24 – 57.

16. عبد الله. وفاء إمحمد. (2023). الأمن السيبراني في القطاع المالي مع الإشارة لواقع الأمن السيبراني في ليبيا.

17. سيد البغدادي، م. ف. & مروة فتحي. (2021). اقتصاديات الأمن السيبراني في القطاع المصرفي. مجلة البحوث القانونية والاقتصادية (المنصورة) (11(76) , 1446–1516.

18. أحمد خ. م. ع.. & خالد محمد عثمان (2023) أثر العلاقة المشتركة بين تعقيد عمليات المصرف والإفصاح عن إجراءات إدارة مخاطر الأمن السيبراني على الأداء المالي – دراسة تطبيقية مجلة البحوث المحاسبية, 1183–1107,(4)10

19. ركايبي, م.. & محمد (2023) أثر مدي وفاء لجنة المراجعة بمسئولياتها على مصداقية التقارير المالية دراسة تطبيقية على الشركات غير المالية المقيدة بالبورصة المصرية. مجلة البحوث المحاسبية 10(4) 317–415.