مساهمة الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية الرقمية في المصارف الإسلامية

The contribution of cyber security in reducing the risks of electronic accounting information systems in islamic banks

د.براهيمي فائزة [1]، أ د حديدي آدم [2]

Brahimi Faiza [1], Hadidi Adem [2]

[1] جامعة الجلفة، الجزائر، مخبرMQEMADD ، faiza.brahimi@univ-djelfa.dz

[2] جامعة الجلفة، الجزائر، مخبرMQEMADD ، hadidi_adem@yahoo.fr

تاريخ الاستلام: 27-06-2025 تاريخ القبول: 29-06-2025

ملخص :

تهدف هذه الدراسة إلى تحديد مساهمة الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية الرقمية في المصارف الإسلامية ، وتم الاعتماد على الإستبانة كأداة لجمع البيانات حيث تم توزيعها على عدد من موظفي مصرف البركة والسلام، وتم اختبار فرضيات الدراسة عن طريق الإنحدار الخطي البسيط، وذلك بإستخدام البرنامج الإحصائي Spss، وقد توصلت هذه الى وجود علاقة ارتباطية موجبة بين الأمن السيبراني والحد من مخاطر نظم المعلومات المحاسبية الرقمية في المصارف الإسلامية وعليه فإلتزام المصارف الإسلامية بتطبيق معايير و مبادئ الأمن السيبراني من شأنه أن يحد من مخاطر نظم المعلومات المحاسبية الرقمية، وفي الأخير خرجنا بمجموعة من التوصيات.

كلمات مفتاحية: الأمن السيبراني، نظم المعلومات المحاسبية الرقمية، المصارف الإسلامية

تصنيف JEL: G21, H56 , L86 ,M40

Abstract :

This study aims to determine the contribution of cybersecurity in reducing the risks of digital accounting information systems in Islamic banks. The questionnaire was used as a tool for data collection, as it was distributed to a number of employees of Al Baraka and Al Salam Bank. The study hypotheses were tested by simple linear regression, using the statistical program SPSS. This study concluded that there is a positive correlation between cybersecurity and reducing the risks of digital accounting information systems in Islamic banks. Accordingly, the commitment of Islamic banks to implementing cybersecurity standards and principles would reduce the risks of digital accounting information systems. Finally, we came out with a set of recommendations.

Keywords : Cybersecurity, Digital Accounting Information Systems, Islamic Banking.

Jel Classification Codes : G21, H56 , L86 ,M40

المؤلف المرسل: د.براهيمي فائزة ، **الإيميل:** faiza.brahimi@univ-djelfa.dz

1.مقدمة :

1.1.تمهيد:

مع التطور الذي تشهده صناعة الصيرفة الإسلامية، ومع توجهها للتمويل الرقمي، أصبحت هناك الحاجة لحماية الصناعة المصرفية الإسلامية الرقمية، ليس من خلال سلسلة من الإجراءات الفنية فقط، وإنما تقتضي الحاجة إلى إتباع منهج شامل يحمل ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت في شكل أساسي في ظهور الأمن السيبراني Cyber Security.

ولقد شاع إستخدام مصطلح الأمن السيبراني كمرادف لأمن المعلومات، وذلك مع إنتشار مفهوم فضاء الأمن السيبراني، الذي يرتبط بتكنولوجيا المعلومات والإتصالات، عن طريق البنى التحتية المختلفة للإتصالات والأنظمة المعلوماتية، غير أن مفهوم الأمن السيبراني أشمل من مفهوم أمن المعلومات.

وتعتبر نظم المعلومات المحاسبية الرقمية لها أهمية كبيرة في المصارف الإسلامية لما تنتجه من تقارير ومعلومات بدقة وسرعة فائقة، ويرجع الفضل لذلك للثورة الهائلة في قطاع التكنولوجيا.

2.1.الإشكالية:

مع التوجه المستمر نحو رقمنة القطاع المصرف الإسلامي، تعرف المصارف الإسلامية العديد من المخاطر خصوصا مع تواجد نظام معلومات محاسبي رقمي، وبعد معرفة أنواع التهديدات المعلوماتية أصبحت الحاجة للأمن السيبراني ضرورة ملحة.

ولهذا من خلال ما سبق تبرز معالم إشكالية الدراسة كالتالي:

إلى أي مدى يساهم الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية الرقمية في المصارف الإسلامية؟

3.1.فرضيات الدراسة:

لتحقيق أهداف الدراسة ومحاولة الإجابة على الإشكالية المطروحة تم صياغة الفرضيات التالية:

الفرضية 01: لا توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي $0.05 \geq \alpha$ بين الأمن السيبراني و مخاطر مدخلات النظام المحاسبي الرقمي في المصارف الإسلامية؛

الفرضية 02: لا توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي $0.05 \geq \alpha$ بين الأمن السيبراني و مخاطر تشغيل النظام المحاسبي الرقمي في المصارف الإسلامية؛

الفرضية 03: لا توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي $0.05 \geq \alpha$ بين الأمن السيبراني و مخاطر مخرجات النظام المحاسبي الرقمي في المصارف الإسلامية؛

الفرضية 04: لا توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي $0.05 \geq \alpha$ بين الأمن السيبراني و مخاطر بيئة النظام المحاسبي الرقمي في المصارف الإسلامية.

4.1.أهمية وأهداف الدراسة:

تأتي أهمية وأهداف هذه الدراسة من خلال تحليل ودراسة وإلقاء الضوء على النقاط التالية:

- تحديد مفهوم الأمن السيبراني؛
- تناول متطلبات الأمن السيبراني في المصارف الإسلامية؛
- إلقاء الضوء على نظام المعلومات المحاسبة الرقمي في المصارف الإسلامية؛
- تحديد مخاطر نظم المعلومات المحاسبي الرقمي في المصارف الإسلامية؛
- تحديد مدى مساهمة الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبي الرقمي في المصارف الإسلامية.

2.الجانب النظري للدراسة

1.2.مدخل عام حول الأمن السيبراني:

تتزايد أهمية الأمن السيبراني بسبب التطور السريع في مجال الصيرفة الرقمية الذي تشهده المصارف التقليدية أو الإسلامية، وبالتالي تم الإعتماد المتزايد على أنظمة الكمبيوتر والإنترنت.

1.1.2.بناء ثقافة الأمن السيبراني:

الأمن السيبراني هو مجموع الأدوات، السياسات، والوسائل التقنية، التنظيمية والإدارية بالإضافة إلى المبادئ التوجيهية ونهج إدارة المخاطر (زروقة، 2019،ص1017)، حيث يتم من خلال هذه الدوات والإجراءات منع الإستخدام غير المصرح به، وبالتالي منع سوء إستغلال النظم الرقمية من أجل حماية البيئة السيبرانية. (المقصودي، 2017، ص154)

و عن الإتحاد الدولي للإتصالات تم إصدار تقرير يعنى بالإتجاهات المتعلقة بالإصلاح في الإتصالات لسنة 2011/2010 حيث عرف الأمن السيبراني من خالاله بأنه مجموعة من الإجراءات والسياسات الأمنية متعلقة بإدارة المخاطر، ويتعلق الأمن السيبراني بمجموعة من الممارسات والتقنيات المجدية التي يمكن إستخدامها من أجل حماية البيئة السيبرانية المتعلقة بكل من المستخدمين داخل المؤسسة وباقي الموجودات فيها". (ITU، 2010، ص02)

وتم تقديم تعريف للأمن السيبراني من طرف وزارة الدفاع الأمريكية بكونه مجموع الإجراءات التنظيمية التي تعمل وتضمن حماية المعلومات بمختلف أشكالها سواء الإلكترونية أو المادية، من مختلف الجرائم التي تصدر عن الهجمات الإلكترونية، بالإضافة الى مختلف عمليات التجسس (بن سيدهم وعواشرية، 2020، ص236)

وإن أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني تتم من خلال الخطوات التالية (ITU، 2010، ص04-17):

- **وضع إستراتيجية وطنية للأمن السيبراني والحصول على الموافقة عليها:**

يقتضي بناء ثقافة الأمن السيبراني وجود إستراتيجية شاملة تشمل إستعراضا عاما أوليا لمدى كفاية الممارسات الوطنية الحالية (عباس و رياح، 2018،ص1425)، والنظر في دور جميع الأطراف أصحاب المصلحة من الهيئات الحكومية والقطاع الخاص والمواطنين في هذه العملية (العشعاش،

2018، ص179)، وبالتالي عند عملية التخطيط، يمكن لكل من حكومة وقطاع خاص أن يعززا من خبراتهما لمضاعفة الثقة. (مشوش، 2019، ص ص 245-246)

- **ردع الجريمة السيبرانية:**

يمكن تحسين الأمن السيبراني، ضمن جملة أمور أخرى، عن طريق إنشاء وتحديث القوانين والإجراءات والسياسات الجنائية الداعمة لمنع الجريمة السيبرانية وردعها والرد عليها وتقديم مرتكبيها للمحاكمة (المقصودي، 2017، ص157).

- **إنشاء منظمة وطنية لإدارة الحوادث (المراقبة، الإنذار، الإستجابة والإنتعاش):**

من أهم الأدوار الرئيسية للحكومات في معالجة الأمن السيبراني على المستوى الوطني القيام بالترصد وإدارة الحوادث السيبرانية (بارة، 2017،ص276)، والإستجابة لها، وتتطلب الإدارة الفعالة للحوادث النظر في إعتبارات التمويل، والموارد البشرية، والتدريب، والقدرات التكنولوجية، والعلاقات بين الحكومات، والقطاع الخاص، والمتطلبات القانونية. (ITU، 2010، ص26)

- **الترويج لثقافة وطنية للأمن السيبراني:**

مع إستخدام تكنولوجيا المعلومات والإتصالات يتعين على حميع المشاركين نشر ثقافة الأمن السيبراني (مشوش، 2019، ص 248).

2.1.2 الأطر والمعايير الدولية المنظمة للمخاطر السيبرانية في القطاع المصرفي الإسلامي:

وتتكون هذه الأطر والمعايير من العناصر التالية (إسماعيل، 2019، ص ص 44-45):

- **الحوكمة الإلكترونية:** وذلك عبر وضع كل مؤسسة مالية إستراتيجية خاصة بها للأمن السيبراني وذلك بمراجعة هذه الإستراتيجيات من خلال الجهات الرقابية في إطار عملها المتعلق بتقييم ممارسات إدارة المخاطر في المؤسسة.
- **إدارة مخاطر الأمن السيبراني:** ويقصد بها الطرق المتبعة من المصرف للرقابة على الأمن السيبراني، وضوابط أمن المعلومات والطرق المتبعة لإختبارها وضمان إستقلاليتها، بالإضافة إلى مدى الإستجابة لهذه المخاطر عند حدوثها.
- **التواصل وتبادل المعلومات:** وذلك عن طريق مشاركة المعلومات بين المصارف، والمشاركة بين المصرف والجهات الرقابية.
- **تعهيد أمن نظم المعلومات والأنظمة الإلكترونية إلى طرف ثالث:** تقوم العديد من المؤسسات بالإستعانة بمصادر خارجية والمتمثلة في خدمات التعهيد إلى طرف ثالث مثل الحوسبة السحابية، ومختلف خدمات الإتصالات السلكية واللاسلكية...إلخ.
- **الجوانب المتعلقة بالأمن السيبراني في إطار المخاطر التشغيلية:** وتدخل ضمن المخاطر التشغيلية في المصارف سواءا التقليدية أو الإسلامية مجموعة من المخاطر التي علاقة بمخاطر نظم المعلومات وتتمثل هذه الجوانب في العناصر التالية (إسماعيل، 2019، ص ص 46-47):

- الإطار الرقابي العام للمخاطر المرتبطة بالأمن السيبراني؛
- تنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عيبر الإنترنيت؛
- الرقابة على الخدمات الإلكترونية؛
- تقييم نظام الرقابة الداخلي، والذي يعتبر محددا مهما لنوعية التدقيق (مسكين وطلحة، 2019،ص153)؛
- الضوابط والتعليمات الرقابية الخاصة بإدارة كلمة السر ؛
- وضع الضوابط اللازمة والمناسبة على عمليات تحويل الأموال من خلال خدمات الإنترنيت؛
- سرية وسلامة المعلومات؛
- تأمين التطبيقات الإلكترونية.

2.2. نظم المعلومات المحاسبي الرقمي في المصارف الإسلامية و مخاطره:

مع التوجه لرقمنة القطاع المصرفي الإسلامية، لم تستثنى نظم المعلومات المحاسبية من ذلك،غيرأن هذا يتكلله مجموعة من المخاطر التي يجب الحد منها.

*1.2.2.*نظم المعلومات المحاسبي الرقمي في المصارف الإسلامية:

يعرف نظام المعلومات المحاسبي بأنه نظام لتجميع، تسجيل، تخزين، ومعالجة البيانات لإنتاج المعلومات لمتخذي القرارت (مسكين و طلحة، 2019،ص)، ويعد نظام المعلومات المحاسبية أحد مكونات نظام المعلومات الإدارية. (السقا والحبيطي، 2003، ص42)

وتتمثل نظم المعلومات المحاسبية الرقمية في كل من تشغيل البيانات، ومعالجتها، وتخزينها، ونقلها، للمعلومات المالية لصالح المؤسسة عن طريق مجموعة من الحواسيب، ومختلف وسائل الإتصال، وشبكات الربط وباقي المعدات. (علي، 2008، ص18).

ولا يختلف مفهوم نظام المعلومات المحاسبي في المصارف الإسلامية عنه في المصارف التقليدية، من حيث مكوناته التي تعتبر مشتركة بين جميع الأنظمة، والمتمثلة في إدخال البيانات، معالجة البيانات والمخرجات.

وآلية عمل في النظام المحاسبي الرقمي هي نفس طريقة العمل اليدوية، فقط الإختلاف يكمن في قيام المحاسب بأمر البرنامج على الحاسوب بإتباع الأوامر السابقة جميعها لإدخال البيانات إليه، ويقتصر عمل المحاسب بعدها على إدخال المعلومة ليس أكثر، ويقوم الجهاز بباقي العمل (أبو شيبة والفطيمي، 2017، ص83)، ونظام المعلومات المحاسبي الرقمي يشمل العنصر البشري، الأجهزة، البرامج، ومصادر المعلومات. (الدهراوي، 2003، ص98)

ويمكن تقسيم نظم المعلومات المحاسبية الرقمية إلى نظم المعلومات المحاسبية الرقمية الكبيرة ونظم المعلومات المحاسبية الرقمية الصغيرة (Aallah, 2009,p125)، كما توجد نظم المعلومات المحاسبية الرقمية المستأجرة. (أبو شيبة والفطيمي، 2017، ص83).

2.2.2.مخاطر نظم المعلومات المحاسبي الرقمي في المصارف الإسلامية:

تتعدد المخاطر المرتبطة بنظم المعلومات المحاسبي الرقمي في المصرف الإسلامي، وتختلف هذه المخاطر التي تعتبر تهديدات للنظام المحاسبي الرقمي الذي تتنوع باختلاف هياكل الأنظمة المعلوماتية، ومدى تعدد نقاط الضعف فيها، وعليه هذه المخاطر هي: (البحيصي والشريف، 2008، ص ص 89-91)

- **مخاطر المدخلات:**

وتتعلق بالمخاطر المتعلقة بالمرحلة الأولى من مراحل النظام، بحيث نجد مجموعة من المخاطر الممكن حدوثها والتي ترتبط بمدخلات النظام والمتمثلة في قيام الموظفون بشكل غير متعمد أو بصورة متعمدة بإدخال بيانات غير صحيحة، أو قيامهم بتدمير البيانات بشكل متعمد أو غير متعمد.

- **مخاطر معالجة البيانات:**

تعتبر المرحلة الثانية لنظام المعلومات المحاسبي الرقمي هي عملية تشغيل البيانات ومعالجتها، ومنه قد تحتوي هذه المرحلة على مجموعة من المخاطر المتمثلة في الوصول للبيانات داخل النظام من طرف موظفي المصرف بشكل غير شرعي أي الدخول تم دون ترخيص، أو تم الدخول للنظام بصورة غير شرعية كذلك ولكن ليس من طرف موظفي المصرف وإنما من طرف أشخاص خارج المصرف، وكذلك من مخاطر هذه المرحلة هو مشاركة الموظفين لنفس كلمة المرور، أو التسبب في إدخال فيروس للحواسيب مما يؤثر لا محالة على أنظمة المعلومات الرقمية الموجودة بداخله. (كليبات وبنية، 2016، ص24):

- **مخاطر المخرجات:**

المرحلة الثالثة لأي نظام معلومات هي مخرجات النظام والتي قد تعترضها مجموعة من المخاطر والتي تؤثر سلبا على مخرجات النظام المحاسبي الرقمي المتمثلة في التقارير المالية، وتنتج هذه المخاطر من خلال تدمير بعض البنود التي تعتبر من مخرجات هذا النظام، أو القيام بتزييف المخرجات وسرقة المعلومات والبيانات المالية، وتعتبر كذلك من مخاطر هذه المرحلة القيام بنسخ المخرجات بشكل غير شرعي، أو مشاركتها بشكل غير مرخص به من خلال طبع هذه البيانات من طرف أشخاص بشكل غير شرعي، وتعتبر من مخاطر هذه المرحلة القيام بتسليم بيانات ومستندات تحمل معلومات حساسة أو سرية من طرف أشخاص لا تتوفر فيهم الشروط الملائمة.

- **المخاطر البيئية:**

من المخاطر التي قد يتعر لها أي نظام معلومات رقمي ولا سيما نظام المعلومات المحاسبي الرقمي في المصارف الإسلامية هو الكوارث الطبيعية مثل حدوث البراكين والزلازل التي تؤدي الى تعطيل هذا النظام وتخريب البيانات فيه، والملاحظ هنا هو عدم إرتباط الإنسان بهذا النوع من المخاطر لكون الكوارث الطبيعية لا دخل للإنسان فيها.

- **الهجمات الإلكترونية**

تهدف الهجمات الإلكترونية إلى تدمير البيانات والمعلومات الموجودة بالحواسيب من أجل سرقتها او القيام بعملية التجسس أو لمجرد تخريبها ومشكلة هذا النوع من المخاطر هو أنه يصعب إكتشافه وبالتالي يصعب على المؤسسة الوقاية والحذر منه، ومن بين هذه الهجمات هي الهجمات المتعلقة بنقل الفيروسات من خلال البرامج أو الأكواد الخبيثة والهدف منها تخريب البيانات أو سرقتها(عبد الدايم وشعبان، 2017، ص56)، وقد يترك المبرمجون والمصممون طرقا خفية تسمى الأبواب الخلفية من أجل تمكينهم من الوصول للشبكات وأجهزة الحاسوب بغرض إستخدامها في فترة لاحقة عند الحاجة لأعمال الصيانة أو التطوير، غير أن هذا قد يؤدي الى استغلال المهاجمين لذلك وبالتالي يمكنهم الوصول للبيانات من خلال هذه المنافذ؛ (شلوش، 2018، ص200)، وقد يتم الهجوم من خلال تجربة جميع الإحتمالات الممكنة لكلمة المرور وهو ما يسمى بالهجوم الإستقصائي. وقد يتم الهجوم على البيانات وأنظمة المعلومات الرقمية من خلال إلتقاط حزم البيانات المارة عبر الشبكة، وهو ما يسمى بهجوم إختطاف البروتوكول، حيث يتم تعديل البيانات وتخريبها من خلال تغييرها. وقد يتم الوصول إلى الأجهزة بطريقة غير شرعية، وهو ما يسمى بالهجوم الخداع وذلك عن طريق إرسال رسائل خادعة تبدو كأنها قادمة رسائل مرسلة من طرف موثوق، ولهذا يجب الحذر من الرسائل غير المرغوب فيها الواردة عبر البريد الإلكتروني لإمكانية إحتوائها على فيروسات من خلال برامج وأكواد خبيثة. (القحطاني، 1436هـ، ص71)

وتتعد صور الهجمات الإلكترونية إلى إمكانية إطلاع المهاجم على بيانات ومعلومات سرية داخل نظام المعلومات الرقمي من خلال ما يعرف بهجوم التصفح عبر النظر لشاشة المستخدم (عبد الدايم وشعبان، 2017، ص36).

3.الجانب التطبيقي للدراسة

1.3.تقديم أداة الدراسة:

تعد الاستبانة أداة من أدوات جمع المعلومات، وذلك انطلاقا من الرغبة في معرفة الرأي الآخر اتجاه موضوع الدراسة، من خلال توزيع استبانة بها مجموعة من الأسئلة حول موضوع الدراسة على عينة الدراسة والتي تمثل المجتمع الأصلي، من أجل تحقيق أهداف الدراسة واختبار الفرضيات، وتم إنجاز هذه الدراسة باستخدام إحدى الأساليب الإحصائية التي تستعمل لتحليل البيانات والمعالجات الإحصائية المتمثل في برنامج Spss.

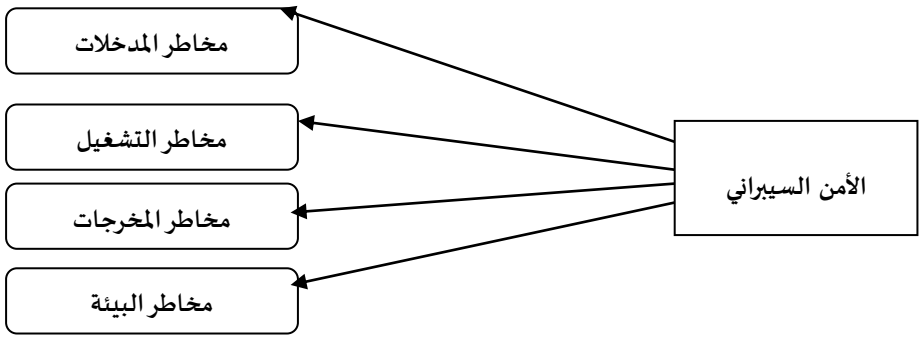
2.3.منهجية الدراسة وأنواع البيانات:

لكي يتحقق الهدف من هذه الدراسة تم الإعتماد على المنهج الوصفي والتحليلي من أجل التعرف على دور ال مبادئ الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية الرقمية في المصارف الإسلامية، حيث تم الإعتماد على نوعين من البيانات المتمثلة في البيانات الأولية من خلال إعداد الإستبانةالملائمة لموضوع الدراسة والقيام بتوزيعها على الموظفين في كل من بنك البركة والسلام لكونها يقدمان منتجات إسلامية، ومنه تم الحصول على المعلومات وتم إفراغها في البرنامج الإحصائيSpss بغرض استخدام الاختبارات الإحصائية التي تتناسب وطبيعة الفرضيات، كما تمت الإستعانة ببيانات ثانوية عن طريق مراجعةالأدبيات النظرية والدراسات السابقة.

- **نموذج الدراسة:** يمكن توضيح نموذج الدراسة من خلال الشكل التالي:

الشكل رقم (01): نموذج الدراسة.

المتغير المستقل (الأمن السيبراني) **الأثر** **المتغير التابع (مخاطر نظم العلومات المعلومات المحاسبية الرقمية)**



المصدر: من إعداد الباحثين.

يمثل الشكل رقم (01) مجموعة من المتغيرات، حيث يتمثل المتغير المستقل في الأمن السيبراني، بينما المتغير التابع هو مخاطر نظم المعلومات المحاسبي في المصارف الإسلامية الذي يتكون من مجموعة أبعاد هي: مخاطر المدخلات، مخاطر التشغيل، مخاطر المخرجات، ومخاطر البيئة.

- **مجتمع وعينة الدراسة:**

يتكون مجتمع الدراسة من مجموع إطارات بنك البركة والسلام، حيث تم استهداف فئة الإطارات، وقد تم توزيع 37 استبانة تجاوبت معنا كلها.

3.3.تفريغ بيانات الاستبيان ومعالجتها إحصائيا.

تم التأكد من صلاحية أداة الدراسة من خلال التأكد صدق فقرات الاستبيان عبر تقديمه للتحكيم من طرف أساتذة متخصصين من جهة، وعن طريق عن طريق الإتساق الداخلي والبنائي من خلال إستخدام

كل من معامل الإرتباط سيبرمان فيما يخص الإتساق الداخلي وكذا معامل الارتباط بيرسون المتعلق بالاتساق البنائي.

وبطريقة معامل الثبات (Cronbach Alpha) تم التحقق من ثبات الدراسة، الذي يشير الى قوة الإرتباط والتماسك بين فقرات الاستبيان عند تجاوز قيمته 0.7 النسبة الملائمة للعلوم الاجتماعية، وتم التأكد من ثبات أداة الدراسة من خلال النتائج المتحصل عليها من الجدول الموالي:

الجدول رقم (01): معاملات الثبات (بطريقة ألفا كرونباخ).

الأبعاد	المحتوى	عدد الفقرات	معامل Cronbach Alpha
البعد1	الأمن السيبراني	19	0.972
البعد2	مخاطر المدخلات	04	0.801
البعد3	مخاطر التشغيل	05	0.868
البعد4	مخاطر المخرجات	05	0.778
البعد5	مخاطر البيئة	03	0.750
	إجمالي فقرات الإستبانة	36	0.980

المصدر: من إعداد الباحثين بالاعتماد على مخرجات البرنامج الإحصائي Spss.

من الجدول السابق نلاحظ أن معامل الثبات لأبعاد الدراسة تتراوح ما بين75% و 98.0% وبالتالي هي أكبر من 70%؛ القيمة المقبولة للثبات في العلوم الإجتماعية، لذلك يمكن القول أن أداة الدراسة ثابتة وبالتالي يمكن استخدامها كأداة للدراسة.

4.3. اختبار الفرضيات وتحليلها.

- **الفرضية الأولى:**

H0: لا توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي 0.05≥ α بين الأمن السيبراني ومخاطر مدخلات النظام المحاسبي الرقمي في المصارف الإسلامية ؛

الجدول الموالي يوضح نتائج الإختبار

الجدول رقم (02): نتائج اختبار الفرضية الأولى

إختبار T	معامل الإرتباط R	معامل التحديد R^2	F المحسوبة	مستوى المعنوية	حجم الأثر
2.945	0.917	0.957	462.301	0.000	0.957

المصدر: من إعداد الباحثين بالاعتماد على مخرجات البرنامج الإحصائي Spss.

بلغ معامل الارتباط R= 0.917 وبمعامل تحديد R^2 بلغ0.957أي أن ما قيمته 95.7% من الحد من مخاطر المدخلات يحققه الأمن السيبراني.

وبما أن قيمة معامل التحديد R^2 أكبر من 0.50 فحسب معيار كوهين فإن حجم أثر مساهمة الأمن السيبراني في الحد من مخاطر المدخلات يعتبر كبيرا.

وكما هو موضح في الجدول السابق بلغت F المحسوبة462.301 وقيمة المستوى المعنوي (Sig) أقل من قيمة (α=0.05) ومنه تعتبر F دالة إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)، ومنه نرفض فرضية العدم ونقبل الفرضية البديلة التي نصها:

توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي ($\alpha \leq 0.05$) بين الأمن السيبراني ومخاطر المدخلات في النظام المحاسبي الرقمي في المصارف الإسلامية.

وهذا ما يمكن التعبير عنها بمعادلة الانحدار البسيط كالآتي:

$$Y_1 = \alpha + (\beta.x) + e_i$$

$$Y_1 = 0.525 + (0.880x)$$

حيث أن:

α: ثابت معادلة الانحدار؛

Y1:مخاطر المدخلات ؛

β : معامل الانحدار لكل متغير؛

e_i: متغير عشوائي أو العوامل الأخرى؛

X:(الأمن السيبراني).

- **الفرضية الثانية:**

H0: لا توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي $0.05 \leq \alpha$ بين الأمن السيبراني ومخاطر تشغيل النظام المحاسبي الرقمي في المصارف الإسلامية ؛

والجدول الموالي يوضح نتائج الإختبار:

الجدول رقم (03): نتائج اختبار الفرضية الثانية.

إختبار T	معامل الإرتباط R	معامل التحديد R^2	F المحسوبة	مستوى المعنوية	حجم الأثر
2.399	0.962	0.981	1056.691	0.000	0.981

المصدر: من إعداد الباحثين بالاعتماد على مخرجات البرنامج الإحصائي Spss.

بلغ معامل الارتباط R= 0.962 وبمعامل تحديد R^2 بلغ0.981أي أن ما قيمته 98.1% من الحد من مخاطر التشغيل يحققه الأمن السيبراني.

وبما أن قيمة معامل التحديد R^2 أكبر من 0.50 فحسب معيار كوهين فإن حجم أثر مساهمة الأمن السيبراني في الحد من مخاطر التشغيل يعتبر كبيرا.

وكما هو موضح في الجدول السابق بلغت F المحسوبة 1056.691 وقيمة المستوى المعنوي (Sig) أقل من قيمة (α=0.05) ومنه تعتبر F دالة إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)، ومنه نرفض فرضية العدم ونقبل الفرضية البديلة التي نصها:

توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي ($\alpha \leq 0.05$)بين الأمن السيبراني و مخاطر التشغيل في النظام المحاسبي الرقمي في المصارف الإسلامية.

وهذا ما يمكن التعبير عنها بمعادلة الانحدار كالآتي:

$$Y_2 = \alpha + (\beta.x) + e_i$$

$$Y_2 = -0.299 + (0.933x)$$

حيث أن:

Y2:مخاطر التشغيل ؛

X: (الأمن السيبراني) .

- **الفرضية الثالثة:**

H0: لا توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي 0.05≤ αبين الأمن السيبراني ومخاطر مخرجات النظام المحاسبي الرقمي في المصارف الإسلامية ؛

والجدول الموالي يوضح نتائج الإختبار:

الجدول رقم (04): نتائج اختبار الفرضية الثالثة.

إختبار T	معامل الإرتباط R	معامل التحديد R^2	F المحسوبة	مستوى المعنوية	حجم الأثر
5.993	0.910	0.954	422.331	0.000	0.954

المصدر: من إعداد الباحثين بالاعتماد على مخرجات البرنامج الإحصائي Spss.

بلغ معامل الارتباط R= 0.910 وبمعامل تحديد R^2 بلغ0.954أي أن ما قيمته 95.4% من الحد من مخاطر المخرجات يحققه الأمن السيبراني.

وبما أن قيمة معامل التحديد R^2 أكبر من 0.50 فحسب معيار كوهين فإن حجم أثر مساهمة الأمن السيبراني في الحد من مخاطر المخرجات يعتبر كبيرا.

وكما هو موضح في الجدول السابق بلغت F المحسوبة 422.331 وقيمة المستوى المعنوي (Sig) أقل من قيمة (α=0.05) ومنه تعتبر F دالة إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)، ومنه نرفض فرضية العدم ونقبل الفرضية البديلة التي نصها:

توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي ($\alpha \leq 0.05$)بين الأمن السيبراني ومخاطر المخرجات في النظام المحاسبي الرقمي في المصارف الإسلامية.

وهذا ما يمكن التعبير عنها بمعادلة الانحدار كالآتي:

$$Y_3=\alpha + (\beta.x) + e_i$$

$$Y_3=-0.997 + (0.788x)$$

حيث أن:

Y3:مخاطر المخرجات ؛

X: (الأمن السيبراني).

- **الفرضية الرابعة:**

H0: لا توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي $0.05 \geq \alpha$ بين الأمن السيبراني و مخاطر بيئة النظام المحاسبي الرقمي في المصارف الإسلامية ؛

والجدول الموالي يوضح نتائج الإختبار:

الجدول رقم (05): نتائج اختبار الفرضية الرابعة.

إختبار T	معامل الإرتباط R	معامل التحديد R^2	F المحسوبة	مستوى المعنوية	حجم الأثر
1.308	0.603	0.777	63.801	0.000	0.777

المصدر: من إعداد الباحثين بالاعتماد على مخرجات البرنامج الإحصائي Spss.

بلغ معامل الارتباط R= 0.603 وبمعامل تحديد R^2 بلغ0.777أي أن ما قيمته 77.7% من الحد من مخاطر البيئة يحققه الأمن السيبراني.

وبما أن قيمة معامل التحديد R^2 أكبر من 0.50 فحسب معيار كوهين فإن حجم أثر مساهمة الأمن السيبراني في الحد من مخاطر البيئة يعتبر كبيرا.

وكما هو موضح في الجدول السابق بلغت F المحسوبة 63.801 وقيمة المستوى المعنوي (Sig) أقل من قيمة (α=0.05) ومنه تعتبر F دالة إحصائيا عند مستوى الدلالة ($\alpha \leq 0.05$)، ومنه نرفض فرضية العدم ونقبل الفرضية البديلة التي نصها:

توجد علاقة ذات دلالة إحصائية عند المستوى المعنوي ($\alpha \leq 0.05$)بين الأمن السيبراني ومخاطر البيئة في النظام المحاسبي الرقمي في المصارف الإسلامية.

وهذا ما يمكن التعبير عنها بمعادلة الانحدار كالآتي:

$$Y_4=\alpha + (\beta.x) + e_i$$

$$Y_4=-0.607 + (0.854x)$$

حيث أن:

Y4:مخاطر البيئة ؛

X: (الأمن السيبراني) .

4.المناقشة:

بعد إختبار الفرضية الأولى تم التوصل أن ما قيمته 95.7% من الحد من مخاطر المدخلات يحققه الأمن السيبراني، وأنه يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$)، كما يعتبر حجم الأثر كبيرا حسب معيار كوهين لكون قيمة معامل التحديد R^2 أكبر من 0.50، ومنه توصلنا إلى نتيجة أن الأمن السيبراني يساهم في الحد من مخاطر المدخلات في نظم المعلومات المحاسبي في المصارف الإسلامية.

وبعد إختبار الفرضية الثانية تم التوصل أن ما قيمته 98.1% من الحد من مخاطر التشغيل يحققه الأمن السيبراني، وأنه يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$)، كما يعتبر حجم الأثر كبيرا حسب معيار كوهين لكون قيمة معامل التحديد R^2 أكبر من 0.50، ومنه توصلنا إلى نتيجة أن الأمن السيبراني يساهم في الحد من مخاطر التشغيل في نظم المعلومات المحاسبي في المصارف الإسلامية.

أما بعد إختبار الفرضية الثالثة تم التوصل أن ما قيمته 95.4% من الحد من مخاطر المخرجات يحققه الأمن السيبراني، وأنه يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$)، كما يعتبر حجم الأثر كبيرا حسب معيار كوهين لكون قيمة معامل التحديد R^2 أكبر من 0.50، ومنه توصلنا إلى نتيجة أن الأمن السيبراني يساهم في الحد من مخاطر المخرجات في نظم المعلومات المحاسبي في المصارف الإسلامية.

وبعد إختبار الفرضية الرابعة تم التوصل أن ما قيمته 77.7% من الحد من مخاطر البيئة يحققه الأمن السيبراني، وأنه يوجد أثر ذو دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$)، كما يعتبر حجم الأثر كبيرا حسب معيار كوهين لكون قيمة معامل التحديد R^2 أكبر من 0.50، ومنه توصلنا إلى نتيجة أن الأمن السيبراني يساهم في الحد من مخاطر البيئة في نظم المعلومات المحاسبي في المصارف الإسلامية.

5. الخلاصة

إنطلاقا من الدراسة النظرية والتطبيقية لموضوع مساهمة الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبية الرقمية في المصارف الإسلامية، وذلك بإستخدام تحليل الإنحدار البسيط وحجم الأثر تم التوصل إلى النتائج التالية:

- ساهمت رقمنة نظم المعلومات المحاسبي في المصرف الإسلامي في مواكبته للتطور في مجال التكنولوجيا، غير أن هذا أدى إلى زيادة المخاطر التي لها علاقة بنظم المعلومات المحاسبي التي تعتبر من أكثرها الهجمات السيبرانية، التي تم تصنيفها ضمن المخاطر التشغيلية؛
- تعتبر عملية تبني ثقافة الأمن السيبراني ضرورة حتمية، لها مجموعة من المتطلبات سواءا على مستوى مؤسسات الدولة الحكومية، أو من خلال القطاع الخاص الذي تعتبر المصارف الإسلامية أحد مكوناته؛

- أكدت جميع الفئات المستهدفة، أن الأمن السيبراني يساهم في الحد من مخاطر المدخلات في نظم المعلومات المحاسبي في المصارف الإسلامية؛
- أكدت جميع الفئات المستهدفة، أن الأمن السيبراني يساهم في الحد من مخاطر التشغيل في نظم المعلومات المحاسبي في المصارف الإسلامية؛
- أكدت جميع الفئات المستهدفة، أن الأمن السيبراني يساهم في الحد من مخاطر المخرجات في نظم المعلومات المحاسبي في المصارف الإسلامية؛
- أكدت جميع الفئات المستهدفة، أن الأمن السيبراني يساهم في الحد من مخاطر البيئة في نظم المعلومات المحاسبي في المصارف الإسلامية؛
- يساهم الأمن السيبراني في الحد من مخاطر نظم المعلومات المحاسبي الرقمي في المصارف الإسلامية.

وفي ظل النتائج المتوصل إليها يمكن تقديم التوصيات التالية:

- على المصارف الإسلامية تبني مفهوم ثقافة الأمن السيبراني، عبر تهيئة البيئة الملائمة له؛
- على الهيئات القائمة على تطوير وتنمية الصناعة المالية الإسلامية بناء إستراتيجية شاملة، وهذا من أجل خلق بيئة آمنة ومرنة في مجال الأمن السيبراني؛
- على المصارف الإسلامية أن تقوم بتدعيم الأمن السيبراني لديها من خلال إنشاء أقسام خاصة تتكفل به؛
- على المصارف الإسلامية أن تقوم بتوعية المستخدمين لديها بالمخاطر السيبرانية، وأن توفر لهم التدريب اللازم.

6.قائمة المراجع:

-ITU. (2010). *تأمين شبكة المعلومات و الإتصالات أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني*. الإتحاد الدولي للإتصالات.

-Saied Aallah .(2009) .*Accouing Information Systems in the Jordanian Banks* .Jordan: Al-Raya for publishing and distribution.

-إبراهيم علي أبو شيبة، و محمد مفتاح الفطيمي. (2017). مخاطر إستخدام نظم المعلومات المحاسبية الإلكترونية. *مجلة دراسات الإقتصاد و الأعمال ، 05* (العدد الخاص)، 80-97.

-إسحاق العشعاش. (2018). الإرهاب السيبراني و تحديات الدول-دراسة مقارنة مع الإتفاقيات الدولية-. *مجلة بحوث* (12)، 173-205.

-إسماعيل زروقة. (2019). الفضاء السيبراني و التحول في مفاهيم القوة و الصراع. *مجلة العلوم القانونية و السياسية ، 10* (01)، 1016-1031.

-الحاج مسكين، و مختار طلحة. (2019). التدقيق الداخلي و نظام الرقابة في المؤسسة الإقتصاديةدراسة تطبيقية بمؤسسة نفطال-وحدة ولاية سعيدة-. *مجلة المالية و الأسواق ، 06* (01)، 146-164.

-حورية بن سيدهم، و رقية عواشرية. (2020). الأمن الفضائي السيبراني-التحديات و الحلول-. *المجلة الجزائرية للأمن الإنساني ، 05* (02)، 125-145.

-ديب بن عياض القحطاني. (1436ه). *أمن المعلومات*. الرياض: مكتبة الملك عبد العزيز للعلوم التقنية.

-زياد يحيى السقا، و قاسم إبراهيم الحبيطي. (2003). *نظام المعلومات المحاسبية*. العراق: وحدة الحدباء للنشر و التوزيع.

-سمير بارة. (2017). الأمن السيبراني في الجزائر-السياسات و المؤسسات-. *المجلة الجزائرية للأمن السيبراني* (04)، 255-280.

-عصام محمد البحيصي، و حرية شعبان الشريف. (جوان, 2008). مخاطر نظم المعلومات المحاسبية الإلكترونية:دراسة تطبيقية في المصارف العاملة في قطاع غزة. *مجلة الجامعة الإسلامية ، 16* (02).

-فريدة صغير عباس، و رضوان رياح. (2018). صراع القيم بين الثقافة المحلية و الثقافة الإفتراضية في ظل الفضاء السيبراني. *مجلة البدر ، 10* (11)، 1420-1431.

-كمال الدين الدهراوي. (2003). *مدخل معاصر في نظم المعلومات المحاسبية* (الإصدار ط2). مصر: الدار الجامعية للنشر و التوزيع.

-محمد إسماعيل. (2019). *الأمن السيبراني في القطاع المصرفي-موجز سياسات-*. صندوق النقد العربي.

-محمد أنيس كليبات، و عمر بنية. (2016). مخاطر إستخدام نظم المعلومات المحاسبية الإلكترونية و أثرها على فاعلية المراجعة في الجزائر. *مجلة جامعة القدس المفتوحة للأبحاث و الدراسات* (40)، 11-40.

-محمد بن احمد علي المقصودي. (2017). الجرائم المعلوماتية-خصائصها و كيفية مواجهتها قانونيا. *المجلة العربية للدراسات الأمنية ، 33* (70).

-مراد مشوش. (2019). الجهود الدولية لمكافحة الإجرام السيبراني. *مجلة الواحات للبحوث و الدراسات ، 12* (02).

-نورة شلوش. (2018). القرصنة الإلكترونية في الفضاء السيبراني:التهديد المتصاعد لأمن الدول. *مجلة مركز بابل للدراسات الإنسانية ، 08* (02)، 185-206.

-هبة أحمد عبد الدايم، و منار محمد شعبان. (جويلية, 2017). الهجمات السيبرانية. *سلسلة دراسات دورية* .