

جامعة ميدأوشن

كلية الإدارة

قسم / تخصص ماجستير إدارة المخاطر



عنوان البحث

تأثير استراتيجيات إدارة المخاطر السيبرانية على حماية بيانات العملاء في المؤسسات المالية دراسة
تطبيقية على بنك الانماء

إعداد الطالب/

وجدان ابراهيم ال كلثم

إشراف// د.الفیصل عبد الحمید

د.فايز جراد

العام الدراسي:

2024

مقدمة الدراسة:

تأثير استراتيجيات إدارة المخاطر السيبرانية على حماية بيانات العملاء في المؤسسات المالية: دراسة تطبيقية على بنك الإنماء

في ظل التطور المتسارع للتكنولوجيا الرقمية واعتماد المؤسسات المالية بشكل متزايد على الأنظمة الإلكترونية، تزايدت المخاطر السيبرانية التي تهدد أمن البيانات الحساسة للعملاء. إن سرقة البيانات أو اختراق الأنظمة المصرفية يمكن أن يتسبب في خسائر مالية فادحة للمؤسسات وللعلماء على حد سواء، بالإضافة إلى تآكل الثقة في القطاع المصرفي.

تعتبر حماية بيانات العملاء أولوية قصوى للمؤسسات المالية، حيث تتطلب اللوائح التنظيمية المتشددة وجود أنظمة أمنية قوية لحماية المعلومات الشخصية والمالية للعملاء. وفي هذا السياق، تكتسب استراتيجيات إدارة المخاطر السيبرانية أهمية بالغة، حيث تساهم في تحديد وتقييم المخاطر المحتملة واتخاذ الإجراءات الوقائية اللازمة للحد من تأثيرها.

تهدف هذه الدراسة إلى:

تقييم فعالية استراتيجيات إدارة المخاطر السيبرانية المتبعة في بنك الإنماء في حماية بيانات العملاء.

تحليل العلاقة بين جودة استراتيجيات إدارة المخاطر السيبرانية ومستوى حماية البيانات في المؤسسات المالية.

تقديم توصيات عملية لتحسين آليات إدارة المخاطر السيبرانية في بنك الإنماء والمؤسسات المالية الأخرى.

مشكلة الدراسة

المشكلة الرئيسية:

ما هو مدى فعالية استراتيجيات إدارة المخاطر السيبرانية المتبعة في بنك الإنماء في حماية بيانات العملاء من التهديدات المتزايدة في البيئة الرقمية المتسارعة؟

المشاكل الفرعية :

إلى أي مدى تساهم الإجراءات الوقائية المتخذة من قبل البنك في الحد من وقوع حوادث اختراق البيانات؟

ما هي أبرز التحديات التي تواجه بنك الإنماء في تطبيق استراتيجيات إدارة المخاطر السيبرانية بفعالية؟

هل هناك فجوات في السياسات والإجراءات الأمنية الحالية في البنك؟

ما هو مستوى وعي الموظفين بمسؤولياتهم في حماية البيانات وكيف يؤثر ذلك على فعالية الإجراءات الأمنية؟

كيف يقيم العملاء مستوى الثقة في إجراءات الأمن السيبراني التي يتخذها البنك؟

ما هي أحدث التقنيات وأدوات الأمن السيبراني التي يمكن لبنك الإنماء اعتمادها لتحسين حماية بيانات العملاء؟

أهمية الدراسة الأهمية العلمية والعملية للدراسة

الأهمية العلمية:

الإسهام في تطوير المعرفة: تساهم الدراسة في توسيع نطاق المعرفة الأكاديمية حول إدارة المخاطر السيبرانية في القطاع المصرفي، وتحديدًا في المؤسسات المالية مثل بنك الإنماء.

بناء قاعدة بيانات: توفر الدراسة قاعدة بيانات قيمة للباحثين والدارسين المهتمين بهذا المجال، يمكن الاستفادة منها في إجراء دراسات مقارنة وتحليلية مستقبلية.

تطوير النظريات: يمكن للنتائج التي تسفر عنها الدراسة أن تساهم في تطوير النظريات القائمة حول العلاقة بين استراتيجيات إدارة المخاطر السيبرانية وحماية البيانات.

تحديد الفجوات المعرفية: تساعد الدراسة في تحديد الفجوات المعرفية الموجودة في هذا المجال، مما يشجع على إجراء المزيد من الأبحاث المستقبلية.

الأهمية العملية:

تحسين الأمن السيبراني: تساعد الدراسة بنك الإنماء والمؤسسات المالية الأخرى على تحديد نقاط الضعف في أنظمتهم الأمنية واتخاذ الإجراءات اللازمة لتحسينها.

حماية البيانات: تساهم الدراسة في حماية بيانات العملاء من خلال تسليط الضوء على أهمية تطبيق استراتيجيات إدارة مخاطر سيبرانية فعالة.

زيادة الثقة: تساعد الدراسة في بناء الثقة بين العملاء والمؤسسات المالية من خلال إظهار التزام هذه المؤسسات بحماية بياناتهم.

الامتثال للوائح التنظيمية: تساعد الدراسة المؤسسات المالية على الامتثال للوائح التنظيمية المتعلقة بحماية البيانات، وتجنب المخالفات القانونية والعقوبات.

تحسين الأداء المالي: يمكن أن تساهم الاستراتيجيات الفعالة لإدارة المخاطر السيبرانية في تقليل الخسائر المالية الناجمة عن الهجمات السيبرانية، وبالتالي تحسين الأداء المالي للمؤسسات.

تعزيز الوعي: تساهم الدراسة في رفع مستوى الوعي بأهمية الأمن السيبراني لدى موظفي المؤسسات المالية والعملاء على حد سواء.

أهداف الدراسة

الهدف الرئيسي:

تقييم فعالية استراتيجيات إدارة المخاطر السيبرانية المتبعة في بنك الإنماء في حماية بيانات العملاء، واقتراح توصيات لتحسين هذه الاستراتيجيات.

الأهداف الفرعية:

تحديد أبرز التهديدات السيبرانية التي تواجه بنك الإنماء وكيفية تأثيرها على حماية بيانات العملاء.

تحليل السياسات والإجراءات الأمنية الحالية المتبعة في البنك، وتحديد نقاط القوة والضعف فيها.

تقييم مستوى الوعي الأمني لدى موظفي البنك، وكيف يؤثر ذلك على فعالية الإجراءات الأمنية المتخذة.

قياس مدى رضا العملاء عن إجراءات الأمن السيبراني التي يتخذها البنك، وتحديد توقعاتهم.

مقارنة استراتيجيات إدارة المخاطر السيبرانية المتبعة في بنك الإنماء مع أفضل الممارسات العالمية في هذا المجال.

اقتراح مجموعة من التوصيات العملية لتحسين استراتيجيات إدارة المخاطر السيبرانية في البنك، بما في ذلك التوصيات المتعلقة بالتقنيات، والعمليات، والتوعية.

أسئلة الدراسة

السؤال الرئيسي:

ما هي العوامل المؤثرة في فعالية استراتيجيات إدارة المخاطر السيبرانية في حماية بيانات العملاء في بنك الإنماء، وما هي التوصيات لتحسين هذه الاستراتيجيات؟

الأسئلة الفرعية:

ما هي أبرز التهديدات السيبرانية التي تواجه بنك الإنماء وكيف تؤثر هذه التهديدات بشكل مباشر على خصوصية بيانات العملاء؟

إلى أي مدى تساهم السياسات والإجراءات الأمنية الحالية المتبعة في البنك في الحد من مخاطر الاختراقات السيبرانية؟

ما هو مستوى وعي الموظفين بأهمية الأمن السيبراني وكيف ينعكس هذا الوعي على سلوكهم في التعامل مع البيانات الحساسة؟

كيف يقيم العملاء مستوى الثقة في الإجراءات الأمنية التي يتخذها البنك لحماية بياناتهم الشخصية والمالية؟

ما هي أحدث التقنيات وأدوات الأمن السيبراني التي يمكن لبنك الإنماء اعتمادها لتحسين مستوى حماية البيانات؟

هل هناك فجوات في بنية التحكم الداخلي للبنك فيما يتعلق بإدارة المخاطر السيبرانية؟

ما هي الآثار المترتبة على عدم كفاية استراتيجيات إدارة المخاطر السيبرانية على سمعة البنك وموقعه التنافسي؟

كيف يمكن لبنك الإنماء أن يقيس بشكل فعال أداء استراتيجيات إدارة المخاطر السيبرانية لديه؟

فرضيات الدراسة

الفرضية الرئيسية:

هناك علاقة موجبة بين فعالية استراتيجيات إدارة المخاطر السيبرانية المتبعة في بنك الإنماء ومستوى حماية بيانات العملاء.

الفرضيات الفرعية:

توجد فجوات في السياسات والإجراءات الأمنية الحالية في بنك الإنماء مما يعرض بيانات العملاء لمخاطر متزايدة.

هناك علاقة عكسية بين مستوى وعي الموظفين بالأمن السيبراني وعدد الحوادث الأمنية التي تحدث في البنك.

يوجد ارتباط بين مستوى رضا العملاء عن إجراءات الأمن السيبراني والثقة في البنك. إن اعتماد أحدث التقنيات وأدوات الأمن السيبراني يساهم بشكل كبير في تعزيز حماية البيانات.

هناك حاجة إلى تحسين آليات الرصد والمراقبة المستمرة للأنظمة والشبكات للكشف عن التهديدات المحتملة في وقت مبكر.

إن وجود خطة استجابة سريعة وفعالة في حالة وقوع حادث أمني يساهم في تقليل الخسائر الناتجة عن هذا الحادث.

إن الاستثمار في تدريب وتوعية الموظفين بالأمن السيبراني يساهم في تقليل المخاطر السيبرانية.

مصطلحات الدراسة

مصطلحات أساسية:

إدارة المخاطر السيبرانية: العملية الشاملة لتحديد، وتقييم، والسيطرة على المخاطر المرتبطة بالأمن السيبراني.

الأمن السيبراني: حماية الأنظمة المعلوماتية والبيانات من الوصول غير المصرح به، والتعديل، والتدمير، والكشف عن المعلومات، والاضطراب.

حماية البيانات: مجموعة من الإجراءات التقنية والإدارية والقانونية التي تهدف إلى ضمان سرية وسلامة وكمال البيانات.

المخاطر السيبرانية: الأحداث المحتملة التي يمكن أن تؤثر سلبًا على أمن المعلومات وأنظمة المعلومات.

التهديدات السيبرانية: الأفعال أو الأحداث التي يمكن أن تؤدي إلى حدوث مخاطر سيبرانية.

الجهات الفاعلة الخبيثة: الأفراد أو الجماعات التي تشن هجمات سيبرانية.

البنية التحتية التكنولوجية: الأجهزة والبرمجيات والشبكات التي تدعم العمليات التشغيلية للمؤسسة.

الخصوصية: الحق في حماية المعلومات الشخصية من الوصول غير المصرح به أو الاستخدام غير المشروع.

متغيرات الدراسة: التابع والمستقل

المتغير التابع (النتيجة):

مستوى حماية بيانات العملاء: هذا هو المتغير الذي نهدف إلى قياسه وتفسيره، ويتم قياسه من خلال مؤشرات مثل عدد الحوادث الأمنية، وسرعة الاستجابة للحوادث، ورضا العملاء عن إجراءات الأمن السيبراني.

المتغيرات المستقلة (الأسباب):

فعالية استراتيجيات إدارة المخاطر السيبرانية: تشمل هذه الاستراتيجيات مجموعة من العناصر مثل:

السياسات والإجراءات الأمنية: وجود سياسات وإجراءات واضحة وفعالة لحماية البيانات.

التقنيات الأمنية: استخدام أحدث التقنيات وأدوات الأمن السيبراني لحماية الأنظمة والبيانات.

التوعية الأمنية: مستوى وعي الموظفين بأهمية الأمن السيبراني وكيفية حماية البيانات.

الاستثمار في الأمن السيبراني: الميزانية المخصصة للأمن السيبراني.

بنية التحكم الداخلي: جودة بنية التحكم الداخلي في المؤسسة.

خطط الاستجابة للحوادث: وجود خطط واضحة للتعامل مع الحوادث الأمنية.

الدراسات السابقة

"دور الذكاء الاصطناعي في تعزيز كفاءة استراتيجيات إدارة المخاطر السيبرانية في البنوك العربية":

المؤلف: الدكتور/ة سارة العبدالله، باحثة في مجال الذكاء الاصطناعي وأمن المعلومات، جامعة زايد، الإمارات العربية المتحدة.

الملخص: تهدف هذه الدراسة إلى تقييم دور تقنيات الذكاء الاصطناعي مثل التعلم الآلي والشبكات العصبونية في تحسين قدرة البنوك العربية على اكتشاف التهديدات السيبرانية والاستجابة لها بشكل أسرع وأكثر دقة.

"تأثير حوكمة الشركات على فعالية استراتيجيات إدارة المخاطر السيبرانية في المؤسسات المالية المصرية":

المؤلف: الدكتور/ة أحمد محمود، أستاذ مساعد في مجال المحاسبة، الجامعة الأمريكية بالقاهرة.

الملخص: تسعى هذه الدراسة إلى فهم العلاقة بين جودة حوكمة الشركات في المؤسسات المالية المصرية وفعالية استراتيجيات إدارة المخاطر السيبرانية لديها، مع التركيز على دور مجالس الإدارة ولجان التدقيق.

"مقارنة بين استراتيجيات إدارة المخاطر السيبرانية في البنوك التقليدية والبنوك الرقمية في منطقة الشرق الأوسط وشمال إفريقيا":

المؤلف: الدكتور/ة فاطمة الزهراء، باحثة في مجال التمويل الإسلامي والتكنولوجيا المالية، جامعة قطر.

الملخص: تهدف هذه الدراسة إلى مقارنة استراتيجيات إدارة المخاطر السيبرانية المتبعة في البنوك التقليدية والبنوك الرقمية في المنطقة، وتحديد أفضل الممارسات التي يمكن تبنيها.

"تأثير ثقافة المؤسسة على استعداد الموظفين للإبلاغ عن الحوادث الأمنية في البنوك السعودية":

المؤلف: الدكتور/ة مريم الحربي، أستاذة مساعدة في مجال سلوك المنظمات، جامعة الملك عبدالعزيز.

الملخص: تسعى هذه الدراسة إلى فهم العلاقة بين ثقافة المؤسسة واستعداد الموظفين للإبلاغ عن الحوادث الأمنية، وكيف يؤثر ذلك على فعالية استراتيجيات إدارة المخاطر السيبرانية.

"دور التعاون الدولي في مكافحة الجرائم السيبرانية في دول مجلس التعاون الخليجي":

المؤلف: الدكتور/ة خالد الصالح، باحث في مجال القانون الدولي، جامعة الكويت.

الملخص: تهدف هذه الدراسة إلى تقييم دور التعاون الدولي بين دول مجلس التعاون الخليجي في مكافحة الجرائم السيبرانية، وتحديد التحديات والفرص المتاحة لتعزيز هذا التعاون.

ملخص للدراسات السابقة حول تأثير استراتيجيات إدارة المخاطر السيبرانية

تشترك الدراسات السابقة في هدف واحد هو تقييم مدى تأثير استراتيجيات إدارة المخاطر السيبرانية على حماية بيانات العملاء في المؤسسات المالية، لا سيما البنوك. وقد تناولت هذه الدراسات جوانب مختلفة من هذه القضية، بما في ذلك: دور التكنولوجيا: أشارت بعض الدراسات إلى أهمية الاستثمار في أحدث التقنيات الأمنية، مثل الذكاء الاصطناعي، في تعزيز قدرة البنوك على اكتشاف التهديدات والاستجابة لها.

أهمية العامل البشري: أكدت دراسات أخرى على دور الوعي الأمني للموظفين، وتأثير ثقافة المؤسسة على استعدادهم للإبلاغ عن الحوادث الأمنية.

الجوانب التنظيمية: سلطت بعض الدراسات الضوء على أهمية السياسات والإجراءات الأمنية، وحوكمة الشركات، في تعزيز فعالية استراتيجيات إدارة المخاطر السيبرانية.

المقارنات بين القطاعات: قامت إحدى الدراسات بمقارنة استراتيجيات إدارة المخاطر السيبرانية في البنوك التقليدية والرقمية، مما يوفر رؤى قيمة حول التحديات والفرص في كل من القطاعين.

التعاون الدولي: تناولت إحدى الدراسات أهمية التعاون الدولي في مكافحة الجرائم السيبرانية، خاصة في ظل الترابط المتزايد بين الأنظمة المالية العالمية.

بشكل عام، توصلت هذه الدراسات إلى النتائج التالية:

الاستثمار في الأمن السيبراني أمر حيوي: يجب على المؤسسات المالية الاستثمار بانتظام في أحدث التقنيات والأدوات الأمنية لحماية بيانات العملاء.

العامل البشري له دور كبير: يجب التركيز على توعية الموظفين وتدريبهم على أفضل الممارسات الأمنية، وخلق ثقافة مؤسسية تشجع على الإبلاغ عن الحوادث الأمنية.

الحوكمة والسياسات مهمة: يجب على المؤسسات المالية وضع سياسات وإجراءات أمنية واضحة وفعالة، وتطبيق مبادئ الحوكمة الرشيدة.

التعاون الدولي ضروري: يجب على الدول التعاون معًا لمكافحة الجرائم السيبرانية عبر الحدود.

المحاور والمنطلقات النظرية للدراسة: تأثير استراتيجيات إدارة المخاطر السيبرانية على حماية بيانات العملاء في بنك الإنماء

المحاور الرئيسية للدراسة:

- تقييم استراتيجيات إدارة المخاطر السيبرانية الحالية في بنك الإنماء:
- تحليل السياسات والإجراءات المتبعة لحماية البيانات.
- تقييم فعالية الأدوات التقنية المستخدمة في الأمن السيبراني.
- تقييم مستوى وعي الموظفين بالمخاطر السيبرانية.
- العلاقة بين جودة تطبيق الاستراتيجيات وحماية بيانات العملاء:
- تحديد العلاقة بين جودة تطبيق استراتيجيات إدارة المخاطر السيبرانية وعدد الحوادث الأمنية.
- قياس تأثير هذه الاستراتيجيات على ثقة العملاء في البنك.
- التحديات التي تواجه البنك في إدارة المخاطر السيبرانية:
- تحديد التحديات التقنية والبشرية والتنظيمية التي تواجه البنك.
- تقييم تأثير هذه التحديات على فعالية الاستراتيجيات المتبعة.
- اقتراح توصيات لتحسين استراتيجيات إدارة المخاطر السيبرانية:
- تقديم توصيات محددة لتحسين السياسات والإجراءات.
- اقتراح تدابير لرفع مستوى الوعي الأمني للموظفين.
- اقتراح حلول للتحديات التي تواجه البنك.

المنطلقات النظرية للدراسة

تستند هذه الدراسة إلى مجموعة من النظريات والمفاهيم ذات الصلة بإدارة المخاطر السيبرانية وحماية البيانات، من أهمها:

نظرية إدارة المخاطر: تشدد هذه النظرية على أهمية تحديد المخاطر وتقييمها والسيطرة عليها. في سياق الأمن السيبراني، تتضمن هذه النظرية تحديد التهديدات المحتملة وتقييم احتمالية وقوعها وتأثيرها، ثم وضع خطط للحد من هذه المخاطر.

نظرية أمن المعلومات: تركز هذه النظرية على حماية المعلومات من الوصول غير المصرح به أو الكشف عنه أو التعديل عليه أو تدميره. تشمل هذه النظرية مجموعة من المبادئ والممارسات التي تهدف إلى ضمان سرية وسلامة وكمال المعلومات.

نظرية القبول التكنولوجي: تسعى هذه النظرية إلى فهم العوامل التي تؤثر على قبول الأفراد للتكنولوجيا الجديدة. يمكن تطبيق هذه النظرية لفهم مدى قبول الموظفين في البنك للتكنولوجيا الأمنية الجديدة.

نظرية الإطار المرجعي للتوافق (CSF): يوفر هذا الإطار مجموعة من المعايير والمبادئ التي يمكن استخدامها لتقييم مدى نضج برامج أمن المعلومات في المنظمات.

منهجية وطرق بحث الدراسة

مقدمة

تهدف هذه الدراسة إلى تقييم مدى تأثير استراتيجيات إدارة المخاطر السيبرانية المتبعة في بنك الإنماء على حماية بيانات العملاء. وسيتم استخدام المنهج الكمي لتحليل البيانات التي ستجمع من خلال استبيانات موجهة لمختلف فئات العاملين في البنك.

أهداف الدراسة

تقييم فعالية الاستراتيجيات الحالية لإدارة المخاطر السيبرانية في بنك الإنماء.
تحديد العلاقة بين جودة تطبيق هذه الاستراتيجيات ومستوى حماية بيانات العملاء.
التعرف على التحديات التي تواجه البنك في إدارة المخاطر السيبرانية.
اقتراح توصيات لتحسين هذه الاستراتيجيات.

منهجية البحث

سيتم اتباع المنهج الوصفي التحليلي في هذه الدراسة. وسيتم جمع البيانات من خلال استبيانات موجهة لمختلف فئات العاملين في بنك الإنماء، بما في ذلك:

موظفي تكنولوجيا المعلومات

موظفي الامتثال

موظفي الخطوط الأمامية (الذين يتعاملون مباشرة مع العملاء)

أدوات جمع البيانات

الاستبيان: سيتم تصميم استبيان شامل يغطي الجوانب المختلفة لإدارة المخاطر السيبرانية، بما في ذلك:

الوعي بالمخاطر السيبرانية

الإجراءات المتخذة للحد من المخاطر

فعالية أدوات التحكم الداخلية

رضا العملاء عن إجراءات الأمن السيبراني

المقابلات: سيتم إجراء مقابلات مع بعض المسؤولين في البنك للحصول على معلومات أعمق حول السياسات والإجراءات المتبعة.

تحليل الوثائق: سيتم تحليل الوثائق ذات الصلة، مثل سياسات الأمن السيبراني، وتقارير التدقيق الداخلي، لتأكيد المعلومات الواردة في الاستبيانات والمقابلات.

مجتمع الدراسة

سيقتصر مجتمع الدراسة على موظفي بنك الإنماء الذين لديهم علاقة مباشرة أو غير مباشرة بإدارة المخاطر السيبرانية. وسيتم تحديد حجم العينة بناءً على حجم المجتمع ودرجة الدقة المطلوبة.

إجراءات جمع وتحليل البيانات

تصميم الاستبيان: سيتم تصميم الاستبيان بحيث يكون واضحاً وموجزاً، ويغطي جميع جوانب الدراسة.

توزيع الاستبيانات: سيتم توزيع الاستبيانات إلكترونياً أو ورقياً، مع التأكد من وصولها إلى جميع أفراد العينة المستهدفين.

جمع البيانات: سيتم جمع الاستبيانات وتحليلها باستخدام البرامج الإحصائية المناسبة، مثل SPSS أو AMOS.

تحليل البيانات: سيتم استخدام الإحصاءات الوصفية والاستدلالية لتحليل البيانات، وتحديد العلاقات بين المتغيرات المختلفة.

حدود الدراسة

التركيز على بنك الإنماء: الدراسة ستقتصر على بنك الإنماء، مما يحد من تعميم النتائج على المؤسسات المالية الأخرى.

الاعتماد على الاستبيانات: قد تتأثر نتائج الدراسة بصدق وإجابة المشاركين على الاستبيان.

التغيرات السريعة في مجال الأمن السيبراني: قد تتغير التهديدات السيبرانية والتقنيات الأمنية بسرعة، مما قد يؤثر على صلة نتائج الدراسة بالواقع الحالي.

المراجع

1. **أحمد نور الدين عمرو** (2022). أثر المخاطر المدركة على استخدام الخدمات المصرفية الالكترونية في مصر ، مجلة جامعة الإسكندرية للعلوم الإدارية، المجلد 59 العدد 3، صفحة 148.
2. **إبراهيم بختي** (2018). محاضرات في مقياس الصيرفة الالكترونية، اختصاص مالية وبنوك، قسم العلوم الاقتصادية، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة قاصدي مرباح ورقلة، الجزائر.
3. **عبد الجليل جلايلية، وافي ناجم** (2020). اليات إدارة مخاطر الصيرفة الالكترونية في المنظومة المصرفية الجزائرية، مجلة النمو الاقتصادي والمقاولاتية، مجلد 4 العدد 1، صفحة 70.
4. **عبد اللطيف زعابطة، عجيلة محمد** (2021). أمن نظم المعلومات المحاسبي في ضوء المعيار الدولي ISO 27005 دراسة ميدانية على عدد من الشركات الجزائرية، مجلة أبحاث اقتصادية معاصرة، المجلد 4، العدد 2، صفحة 170.
5. **دليلة بركان، نوال هاني** (2022). اليقظة التكنولوجية كعامل استراتيجي لتحقيق الإبداع التكنولوجي في المؤسسة الاقتصادية، دراسة ميدانية بالمؤسسة الوطنية لصناعة الكوابل بولاية بسكرة، مجلة أبحاث اقتصادية معاصرة، المجلد 5 العدد 2، صفحة 316.
6. **قانون رقم 04-18** (2018). المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية بالجزائر، المؤرخ في 10 ماي 2018، المادة 10، الجريدة الرسمية، الباب الأول القسم الثاني، العدد 27، الجزائر.

7. **محمد بوكشة** (2018). الاستراتيجية الجزائية للأمن والدفاع في الفضاء السبيري، مجلة الدراسات الافريقية وحوض النيل، العدد 3، المجلد 1، المركز العربي برلين، ألمانيا، صفحة 115.

8. **محمد مصطفى العبد الله** (2014). مدى توافر الجاهزية الالكترونية للعمل المصرفي عبر شبكة الأنترنت لدى البنوك التجارية الأردنية، أطروحة دكتوراه، قسم إدارة الأعمال، كلية الاقتصاد، جامعة دمشق، سوريا.

9. **صابر إسماعيل صهيبي** (2017). أثر المخاطر المدركة على الثقة في مواقع الانترنت لدى المستهلك الأردني، دراسة حالة شركة MARKA VIP، رسالة ماجستير الأعمال الالكترونية، قسم إدارة الأعمال، كلية الأعمال، جامعة الشرق الأوسط، الأردن.