

بسم الله الرحمن الرحيم



جامعة ميدأوشن
كلية إدارة المشاريع

أثر إدارة مخاطر الامن السيبراني على دعم الاستقرار والشمول المالي
في البنوك
المدرجة في البورصة السعودية

إعداد الطالب /

Yousef Al-Ghailan
2021204625

إشراف /

DR. Mona Mostafa Alashry

Faculty Member - College Of Management - Midocean University

الفصل الأول :

المقدمة :

في عصر التكنولوجيا الرقمية، أصبح الأمن السيبراني أحد القضايا البارزة والمهمة التي تواجه المؤسسات في جميع أنحاء العالم. مع التزايد المستمر في التهديدات السيبرانية والتطور المتسارع للتكنولوجيا، أصبحت حماية البيانات والبنية التحتية الرقمية من الهجمات الإلكترونية تحديًا كبيرًا يتطلب استراتيجيات دقيقة وإدارة فعالة للمخاطر. في هذا السياق، تلعب المؤسسات المالية، ولا سيما البنوك، دورًا حيويًا في الاقتصاد العالمي والمحلي، مما يجعلها هدفًا رئيسيًا للهجمات السيبرانية.

تعد البنوك من المؤسسات الأكثر عرضة للهجمات السيبرانية نظرًا لأنها تتعامل مع كميات ضخمة من البيانات المالية الحساسة، بالإضافة إلى اعتمادها الكبير على التكنولوجيا في عملياتها اليومية. في المملكة العربية السعودية، تصدر البنوك المدرجة في البورصة السعودية مشهد القطاع المالي، وتسعى جاهدة لتعزيز بنيتها التحتية الرقمية وتحسين إجراءات الأمن السيبراني لمواجهة التحديات المتزايدة.

يؤثر الأمن السيبراني بشكل مباشر على استقرار النظام المالي وشموليته. فالهجمات السيبرانية يمكن أن تؤدي إلى خسائر مالية كبيرة، وتعطل العمليات، وتضر بسمعة البنوك، مما يؤثر بدوره على ثقة العملاء والمستثمرين. ومن هنا، تظهر الحاجة الملحة إلى إدارة فعالة لمخاطر الأمن السيبراني كعامل أساسي لدعم الاستقرار المالي وتعزيز الشمول المالي.

من خلال إدارة مخاطر الأمن السيبراني بفعالية، يمكن للبنوك حماية بيانات العملاء، وضمان استمرارية العمليات، وتعزيز الثقة في النظام المالي. هذا يساهم في تحقيق الشمول المالي من خلال زيادة الوصول إلى الخدمات المالية وتشجيع المزيد من الأفراد والشركات على الانخراط في النظام المالي الرسمي.

في هذا البحث، سنستعرض بالتفصيل أهمية إدارة مخاطر الأمن السيبراني في البنوك المدرجة في البورصة السعودية، وتأثيرها على دعم الاستقرار المالي والشمول المالي. سنناقش التحديات التي تواجهها هذه البنوك في مجال الأمن السيبراني، وأفضل الممارسات

والسياسات التي يمكن تبنيها لتحقيق مستوى عالٍ من الأمان السيبراني، وبالتالي تعزيز الاستقرار المالي والشمول المالي في المملكة العربية السعودية.

مشكلة البحث

مع التطور السريع للتكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية في العمليات المالية، أصبحت البنوك هدفاً رئيسياً للهجمات السيبرانية. تتعرض البنوك المدرجة في البورصة السعودية لتحديات كبيرة فيما يتعلق بحماية بياناتها وأنظمتها من هذه الهجمات التي يمكن أن تؤدي إلى خسائر مالية ضخمة، وتعطيل العمليات، وتقويض ثقة العملاء والمستثمرين.

تجلى مشكلة البحث في الحاجة الماسة إلى فهم كيفية تأثير إدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي وتعزيز الشمول المالي في البنوك المدرجة في البورصة السعودية. تبرز الأسئلة التالية كمحاور رئيسية للتحقيق:

1. ما مدى فعالية الإجراءات الحالية التي تتبناها البنوك المدرجة في البورصة السعودية لإدارة مخاطر الأمن السيبراني؟
2. كيف تؤثر هذه الإجراءات على استقرار النظام المالي وثقة العملاء والمستثمرين؟
3. ما هو الدور الذي تلعبه إدارة مخاطر الأمن السيبراني في تعزيز الشمول المالي وزيادة الوصول إلى الخدمات المالية؟
4. ما هي التحديات الرئيسية التي تواجه البنوك في تحسين إدارة مخاطر الأمن السيبراني؟
5. ما هي أفضل الممارسات التي يمكن تبنيها لتعزيز إدارة مخاطر الأمن السيبراني وتحقيق الاستقرار المالي والشمول المالي؟

من خلال هذا البحث، نسعى إلى تقديم تحليل شامل لمشكلة إدارة مخاطر الأمن السيبراني في البنوك المدرجة في البورصة السعودية، وفهم تأثيرها على الاستقرار المالي والشمول المالي. الهدف هو تقديم توصيات تستند إلى أفضل الممارسات والسياسات التي يمكن أن تساعد البنوك على تحسين أمنها السيبراني، وبالتالي دعم استقرار النظام المالي وتعزيز الشمول المالي في المملكة العربية السعودية.

أهمية البحث

تتبع أهمية هذا البحث من الدور الحيوي الذي يلعبه الأمن السيبراني في تعزيز استقرار النظام المالي وضمان الشمول المالي، خاصة في البنوك المدرجة في البورصة السعودية. تتضح أهمية هذا البحث من عدة جوانب:

1. **تعزيز الأمن السيبراني في البنوك:** سيساهم البحث في فهم أفضل لمخاطر الأمن السيبراني التي تواجه البنوك المدرجة في البورصة السعودية. هذا الفهم يمكن أن يؤدي إلى تطوير استراتيجيات وإجراءات أكثر فعالية لحماية البيانات والبنية التحتية الرقمية للبنوك، مما يعزز من قدرتها على التصدي للهجمات السيبرانية.
2. **دعم الاستقرار المالي:** من خلال تحسين إدارة مخاطر الأمن السيبراني، يمكن للبنوك الحفاظ على استمرارية العمليات وتقليل الخسائر المالية الناجمة عن الهجمات السيبرانية. هذا بدوره يدعم استقرار النظام المالي، وهو أمر ضروري لثقة المستثمرين والعملاء في البنوك.
3. **تعزيز الشمول المالي:** يعتبر الشمول المالي هدفًا رئيسيًا للبنوك وللاقتصاد الوطني بشكل عام. من خلال توفير بيئة آمنة للتعاملات المالية الرقمية، يمكن للبنوك جذب المزيد من الأفراد والشركات لاستخدام الخدمات المالية الرسمية، مما يساهم في توسيع قاعدة العملاء وتحقيق الشمول المالي.
4. **توفير مرجعية للأبحاث المستقبلية:** سيساهم هذا البحث في إضافة قيمة علمية للمجال الأكاديمي من خلال تقديم تحليل متعمق لمخاطر الأمن السيبراني في البنوك المدرجة في البورصة السعودية. يمكن أن يكون هذا البحث مرجعًا هامًا للأبحاث المستقبلية في مجال الأمن السيبراني والاستقرار المالي.
5. **تقديم توصيات عملية:** سيقدم البحث توصيات مبنية على أفضل الممارسات والسياسات العالمية في مجال إدارة مخاطر الأمن السيبراني. يمكن لهذه التوصيات أن تساعد البنوك والمسؤولين عن تنظيم القطاع المالي في اتخاذ قرارات مبنية على أسس علمية لتحسين الأمن السيبراني.
6. **رفع الوعي بأهمية الأمن السيبراني:** من خلال تسليط الضوء على أهمية إدارة مخاطر الأمن السيبراني وتأثيرها على الاستقرار المالي والشمول المالي، سيساهم البحث في رفع الوعي لدى الإدارات العليا في البنوك وصناع القرار بأهمية الاستثمار في الأمن السيبراني كأولوية استراتيجية.

أسئلة البحث

- (1) ما هي إجراءات إدارة مخاطر الأمن السيبراني التي تتبناها البنوك المدرجة في البورصة السعودية؟
- (2) كيف تؤثر إدارة مخاطر الأمن السيبراني على استقرار النظام المالي في البنوك المدرجة في البورصة السعودية؟
- (3) ما هو دور إدارة مخاطر الأمن السيبراني في تعزيز ثقة العملاء والمستثمرين بالبنوك المدرجة في البورصة السعودية؟
- (4) كيف تساهم إدارة مخاطر الأمن السيبراني في تحقيق الشمول المالي في البنوك المدرجة في البورصة السعودية؟
- (5) ما هي التحديات التي تواجه البنوك المدرجة في البورصة السعودية في إدارة مخاطر الأمن السيبراني؟
- (6) ما هي أفضل الممارسات والتوصيات لتحسين إدارة مخاطر الأمن السيبراني في البنوك المدرجة في البورصة السعودية؟

أهداف البحث

- (1) تحديد إجراءات إدارة مخاطر الأمن السيبراني التي تتبناها البنوك المدرجة في البورصة السعودية.
- (2) تقييم تأثير إدارة مخاطر الأمن السيبراني على استقرار النظام المالي في البنوك المدرجة في البورصة السعودية.
- (3) تحليل دور إدارة مخاطر الأمن السيبراني في تعزيز ثقة العملاء والمستثمرين بالبنوك المدرجة في البورصة السعودية.
- (4) دراسة كيفية مساهمة إدارة مخاطر الأمن السيبراني في تحقيق الشمول المالي في البنوك المدرجة في البورصة السعودية.

(5) تحديد التحديات التي تواجه البنوك المدرجة في البورصة السعودية في إدارة مخاطر الأمن السيبراني.

(6) تقديم توصيات لأفضل الممارسات لتحسين إدارة مخاطر الأمن السيبراني في البنوك المدرجة في البورصة السعودية.

فرضيات البحث

(1) تتبنى البنوك المدرجة في البورصة السعودية إجراءات فعالة لإدارة مخاطر الأمن السيبراني.

(2) تؤثر إدارة مخاطر الأمن السيبراني إيجابياً على استقرار النظام المالي في البنوك المدرجة في البورصة السعودية.

(3) تعزز إدارة مخاطر الأمن السيبراني ثقة العملاء والمستثمرين في البنوك المدرجة في البورصة السعودية.

(4) تساهم إدارة مخاطر الأمن السيبراني في تحقيق الشمول المالي في البنوك المدرجة في البورصة السعودية.

(5) تواجه البنوك المدرجة في البورصة السعودية تحديات كبيرة في إدارة مخاطر الأمن السيبراني.

(6) يمكن لتطبيق أفضل الممارسات العالمية في إدارة مخاطر الأمن السيبراني أن يحسن من مستوى الأمان في البنوك المدرجة في البورصة السعودية.

نموذج البحث

1. المقدمة

- تقديم خلفية عن أهمية الأمن السيبراني في البنوك.
- شرح السياق السعودي وأهمية البنوك المدرجة في البورصة السعودية.
- تحديد مشكلة البحث وأهميته وأهدافه.

2. الإطار النظري

- مراجعة الأدبيات المتعلقة بإدارة مخاطر الأمن السيبراني.
- تعريف المفاهيم الأساسية: الأمن السيبراني، إدارة المخاطر، الاستقرار المالي، الشمول المالي.
- مناقشة الدراسات السابقة وأبرز النتائج التي توصلت إليها.

3. منهجية البحث

- وصف المنهجية المستخدمة في البحث (نوع البحث: وصفي، تحليلي، إلخ).
- تحديد الأدوات المستخدمة لجمع البيانات (استبانة إلكترونية).
- شرح كيفية تصميم الاستبانة والأسئلة المطروحة فيها.
- تحديد كيفية توزيع الاستبانة وجمع الردود.
- شرح كيفية اختيار عينة البحث (البنوك المدرجة في البورصة السعودية).

4. تحليل البيانات

- تقديم تحليل شامل للبيانات المجمعة من الاستبانة.
- استخدام الجداول والرسوم البيانية لتوضيح النتائج.
- مناقشة النتائج وربطها بفرضيات البحث.

5. النتائج

- تقديم النتائج الرئيسية للبحث بناءً على تحليل البيانات المستخلصة من الاستبانة.
- تأكيد أو دحض الفرضيات المحددة في البحث.

6. المناقشة

- مناقشة نتائج البحث بالمقارنة مع الدراسات السابقة.
- تحليل الأسباب المحتملة للنتائج واستكشاف الآثار العملية.

7. التوصيات

- تقديم توصيات مستندة إلى نتائج البحث لتعزيز إدارة مخاطر الأمن السيبراني.
- تقديم اقتراحات للسياسات والإجراءات التي يمكن تبنيها من قبل البنوك.
- توصيات للبحوث المستقبلية في هذا المجال.

8. الخاتمة

- تلخيص أهم النقاط التي تناولها البحث.
- تأكيد أهمية إدارة مخاطر الأمن السيبراني في دعم الاستقرار والشمول المالي.
- تقديم نظرة مستقبلية حول الموضوع.

9. المراجع

- قائمة بالمصادر والمراجع التي تم الاستعانة بها في إعداد البحث.

نطاق الدراسة

1. الموضوع

- **النطاق الموضوعي:** يركز البحث على دراسة تأثير إدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي وتعزيز الشمول المالي في البنوك المدرجة في البورصة السعودية.

2. المكان

- **النطاق المكاني:** تقتصر الدراسة على البنوك المدرجة في البورصة السعودية، حيث سيتم جمع البيانات وتحليلها ضمن هذا النطاق الجغرافي.

3. الزمان

- **النطاق الزمني:** يغطي البحث الفترة من بداية عام 2024 حتى نهاية عام 2024، حيث سيتم جمع البيانات وتحليلها خلال هذه الفترة لتقديم صورة محدثة عن الواقع الحالي لإدارة مخاطر الأمن السيبراني في البنوك السعودية.

4. المحتوى

- **النطاق التحليلي:** يشمل التحليل تقييم السياسات والاستراتيجيات الحالية لإدارة مخاطر الأمن السيبراني، تأثير هذه الإدارة على الاستقرار المالي والشمول المالي، التحديات التي تواجه البنوك، وأفضل الممارسات التي يمكن تبنيها لتحسين إدارة المخاطر.

5. المنهجية

- **النطاق المنهجي:** يتم استخدام استبانة إلكترونية كأداة رئيسية لجمع البيانات من عينة من البنوك المدرجة في البورصة السعودية. يشمل النطاق المنهجي تحليل البيانات الكمية المستخلصة من الاستبانة باستخدام أساليب تحليل إحصائية مناسبة.

6. البيئة

• **النطاق المؤسسي:** تركز الدراسة على البيئة المؤسسية للبنوك المدرجة في البورصة السعودية، بما يشمل سياساتها الداخلية، وتفاعلها مع اللوائح التنظيمية، وتأثيرها على العملاء والمستثمرين.

7. القيود

• **القيود البحثية:** تشمل القيود التي قد تؤثر على الدراسة حجم العينة، التوقيت المحدد لجمع البيانات، واستجابة المؤسسات المالية المشاركة في الاستبانة.

مخطط المشروع

1. المقدمة

- تقديم خلفية عن الموضوع.
- تحديد مشكلة البحث.
- توضيح أهمية البحث.
- تحديد أهداف البحث.
- عرض فرضيات البحث.

2. الإطار النظري

- مراجعة الأدبيات المتعلقة بالموضوع.
- تعريف المفاهيم الأساسية.
- مناقشة الدراسات السابقة وأبرز النتائج.

3. منهجية البحث

- المقدمة
- التعريفات الإجرائية لمتغيرات البحث
- تصميم البحث (بصلة البحث)
- مجتمع البحث وطرق وتقنيات أخذ العينات
- طريقة جمع البيانات

■ أنواع البيانات

■ إجراءات التحليل الاحصائي

■ الخاتمة

الفصل الثاني : الاطار النظري

المبحث الأول : مفهوم الأمن السيبراني

تعريف الأمن السيبراني :

الأمن السيبراني هو مجموعة من التقنيات والعمليات والممارسات المصممة لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. تهدف هذه الهجمات عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها أو ابتزاز المال من المستخدمين أو تعطيل العمليات التجارية العادية. يشمل الأمن السيبراني مجالات متعددة مثل أمن الشبكات، أمن التطبيقات، أمن المعلومات، إدارة الهوية، وأمن البنية التحتية الحيوية.

أهمية الأمن السيبراني في القطاع المالي

يلعب الأمن السيبراني دورًا حاسمًا في القطاع المالي لعدة أسباب:

السبب	التوضيح
حماية البيانات الحساسة	البنوك والمؤسسات المالية تتعامل مع كميات ضخمة من البيانات الحساسة مثل معلومات الحسابات المالية، البيانات الشخصية للعملاء، والمعاملات المالية. تأمين هذه البيانات يحمي العملاء ويعزز ثقتهم.
استمرارية الأعمال	الهجمات السيبرانية يمكن أن تعطل العمليات المالية وتؤدي إلى خسائر مالية كبيرة. الأمن السيبراني يضمن استمرارية الأعمال حتى في حالة حدوث هجمات.

السبب	التوضيح
الامتثال التنظيمي	المؤسسات المالية مطالبة بالامتثال لمجموعة واسعة من اللوائح والقوانين التي تهدف إلى حماية البيانات وتعزيز الأمن السيبراني. الالتزام بهذه اللوائح يعزز سمعة المؤسسة ويجنبها العقوبات.
الثقة العامة	الثقة هي أساس التعاملات المالية. الأمن السيبراني يعزز ثقة العملاء والمستثمرين في النظام المالي ويشجعهم على التفاعل معه.

مكونات الأمن السيبراني

1. البنية التحتية:

- **الشبكات والأجهزة:** تشمل حماية شبكات الاتصال والأجهزة المتصلة بها من الهجمات والاختراقات.
- **الخوادم وقواعد البيانات:** تأمين الخوادم وقواعد البيانات التي تحتوي على معلومات حساسة ومعاملات مالية.

2. السياسات:

- **سياسات الأمان:** وضع سياسات وإجراءات تحدد كيفية التعامل مع البيانات الحساسة وحمايتها.
- **الإجراءات الوقائية:** تنفيذ إجراءات وقائية مثل التشفير والجدران النارية (Firewalls) وأنظمة الكشف عن التسلل (IDS).

3. التقنيات:

- **أنظمة الكشف عن التسلل (IDS) وأنظمة منع التسلل (IPS):** تستخدم لمراقبة الشبكات والأنظمة والكشف عن الهجمات المحتملة ومنعها.
- **التشفير:** تقنية تستخدم لحماية البيانات عن طريق تحويلها إلى صيغة غير قابلة للقراءة بدون مفتاح فك التشفير.
- **المصادقة متعددة العوامل (MFA):** إضافة طبقات إضافية من الأمان للوصول إلى الأنظمة والبيانات.

4. البشر:

- **التوعية والتدريب:** تدريب الموظفين على أساليب الأمان السيبراني وكيفية التعامل مع التهديدات المحتملة.

◦ **الأدوار والمسؤوليات:** تحديد الأدوار والمسؤوليات بوضوح فيما يتعلق بالأمن السيبراني داخل المؤسسة لضمان الاستجابة الفعالة للتهديدات.

المبحث الثاني : إدارة مخاطر الأمن السيبراني

تعريف إدارة المخاطر :

إدارة المخاطر هي عملية تحديد وتقييم والسيطرة على التهديدات التي تواجه مؤسسة أو نظام معين. تهدف إدارة المخاطر إلى تقليل الآثار السلبية المحتملة للمخاطر من خلال اتخاذ الإجراءات المناسبة للتحكم فيها أو الحد منها. في سياق الأمن السيبراني، تشمل المخاطر التهديدات التي يمكن أن تؤدي إلى فقدان البيانات أو تعطيل الأنظمة أو التسبب في أضرار مالية ومادية.

عملية إدارة مخاطر الأمن السيبراني

تتضمن عملية إدارة مخاطر الأمن السيبراني عدة خطوات أساسية:

1. التحديد:

- **تحديد الأصول:** تحديد جميع الأصول التي تحتاج إلى حماية، مثل البيانات الحساسة، البنية التحتية التكنولوجية، والأنظمة الحيوية.
- **تحديد التهديدات:** التعرف على التهديدات المحتملة التي يمكن أن تؤثر على هذه الأصول، مثل الهجمات الإلكترونية، البرمجيات الخبيثة، والأخطاء البشرية.

2. التقييم:

- **تقييم الأثر:** تحليل الأثر المحتمل لكل تهديد على الأصول المحددة، بما في ذلك الأضرار المالية، وفقدان البيانات، وتأثيره على سمعة المؤسسة.
- **تقييم الاحتمالية:** تقدير احتمالية حدوث كل تهديد باستخدام البيانات التاريخية والتحليلات التنبؤية.

3. التحكم:

- **تنفيذ الإجراءات الوقائية:** تطبيق السياسات والإجراءات التي تهدف إلى الحد من تأثير التهديدات المحتملة، مثل التشفير، والجدران النارية، وأنظمة الكشف عن التسلل.
- **تطوير خطط الاستجابة:** إعداد خطط للاستجابة السريعة في حالة وقوع هجوم سيبراني، بما في ذلك إجراءات الطوارئ واستعادة البيانات.

4. المراقبة:

- مراقبة الأنظمة: استخدام أدوات المراقبة لرصد الأنشطة غير العادية والتهديدات المحتملة بشكل مستمر.
 - تحديث التقييمات: مراجعة وتحديث تقييمات المخاطر بانتظام لضمان فعالية الإجراءات المتخذة ومواكبة التهديدات الجديدة.
- أدوات وأساليب إدارة المخاطر السيبرانية**

الأداة أو الأسلوب	التوضيح
التشفير	تحويل البيانات إلى صيغة غير قابلة للقراءة بدون مفتاح فك التشفير، مما يحميها من الوصول غير المصرح به.
الجدران النارية (Firewalls)	أنظمة تراقب وتتحكم في حركة المرور بين الشبكات الموثوقة وغير الموثوقة، وتعمل كحاجز لمنع الوصول غير المصرح به.
أنظمة الكشف عن التسلل (IDS)	أدوات تراقب الشبكات والأنظمة للكشف عن الأنشطة غير العادية أو المشبوهة التي قد تشير إلى وجود هجوم.
أنظمة منع التسلل (IPS)	مشابهة لأنظمة IDS، ولكنها تتخذ خطوات إضافية لمنع التهديدات المكتشفة من التسبب في أضرار.
المصادقة متعددة العوامل (MFA)	إضافة طبقات إضافية من الأمان من خلال طلب أكثر من طريقة تحقق للوصول إلى الأنظمة والبيانات.
تدقيق الأمان	إجراء مراجعات دورية للأنظمة والسياسات للتأكد من الالتزام بمعايير الأمان وتحديد الثغرات المحتملة.
التوعية والتدريب	برامج تدريبية لتعليم الموظفين كيفية التعرف على التهديدات السيبرانية والتصرف بشكل صحيح عند مواجهتها.
خطط الاستجابة للطوارئ	خطط مفصلة تحدد الإجراءات التي يجب اتخاذها في حالة وقوع هجوم سيبراني لضمان الاستجابة السريعة وتقليل الأضرار.

باتّباع هذه العمليات واستخدام الأدوات المناسبة، يمكن للمؤسسات المالية تحقيق مستوى عالٍ من الأمان السيبراني، مما يحمي أصولها ويعزز ثقة عملائها والمستثمرين بها.

المبحث الثالث : الاستقرار المالي

تعريف الاستقرار المالي

الاستقرار المالي هو حالة من الاتزان في النظام المالي حيث تعمل المؤسسات والأسواق المالية بشكل فعال، وتستطيع مواجهة الصدمات الاقتصادية والمالية دون التسبب في اضطرابات كبيرة. يتضمن الاستقرار المالي القدرة على الحفاظ على الثقة في النظام المالي، وضمان استمرارية الخدمات المالية الأساسية، مثل المدفوعات، والائتمان، والتأمين.

أهمية الاستقرار المالي للبنوك

الاستقرار المالي يعتبر أمراً حيوياً للبنوك للأسباب التالية:

1. **حماية مصالح المودعين:** يساهم الاستقرار المالي في ضمان سلامة أموال المودعين وثقتهم في النظام المصرفي.
2. **تحقيق استدامة العمليات:** يمكن البنوك من العمل بفعالية حتى في الأوقات العصيبة دون انقطاع في الخدمات.
3. **الحد من المخاطر النظامية:** يقلل من احتمالية انتشار الأزمات المالية التي قد تؤدي إلى انهيار النظام المالي بالكامل.
4. **تعزيز النمو الاقتصادي:** يساهم في توفير بيئة مستقرة للتمويل والاستثمار، مما يعزز النمو الاقتصادي على المدى الطويل.
5. **تجنب الأزمات المالية:** يحد من تأثير الأزمات المالية ويقلل من تكاليف التعامل معها، مما يحافظ على الاستقرار الاقتصادي العام.

العلاقة بين الأمن السيبراني والاستقرار المالي

توجد علاقة وثيقة بين الأمن السيبراني والاستقرار المالي، ويمكن توضيح هذه العلاقة من خلال النقاط التالية:

1. **حماية البيانات والمعلومات الحساسة:**

◦ يمنع الأمن السيبراني الوصول غير المصرح به إلى البيانات المالية الحساسة، مما يحمي المؤسسات المالية من الاحتيال والسرقة المالية.

2. استمرارية الأعمال:

◦ يسهم الأمن السيبراني في الحفاظ على استمرارية العمليات المالية وعدم تعطلها، مما يضمن تقديم الخدمات المالية بشكل متواصل وموثوق.

3. تعزيز الثقة:

◦ يعزز الأمن السيبراني ثقة العملاء والمستثمرين في البنوك، مما يساهم في استقرار النظام المالي بشكل عام.

4. الامتثال التنظيمي:

◦ يساعد الامتثال لمعايير الأمن السيبراني في تحقيق الامتثال التنظيمي، مما يحافظ على استقرار النظام المالي ويجنب البنوك الغرامات والعقوبات.

5. التقليل من المخاطر النظامية:

◦ تقليل احتمالية وقوع هجمات سيبرانية كبيرة يمكن أن تسبب اضطرابات واسعة النطاق في النظام المالي، مما يساهم في تقليل المخاطر النظامية.

6. التعامل مع الأزمات بسرعة وكفاءة:

◦ الأمن السيبراني يوفر الأدوات والآليات اللازمة للاستجابة السريعة والفعالة للأزمات السيبرانية، مما يقلل من تأثيرها على الاستقرار المالي.

مثال توضيحي

لنأخذ مثالا على هجوم سيبراني على بنك ما يمكن أن يؤدي إلى:

• سرقة بيانات العملاء: قد يؤدي ذلك إلى خسائر مالية كبيرة، وفقدان ثقة العملاء، وتعرض البنك لدعاوى قضائية.

• تعطل الخدمات المالية: قد يتسبب الهجوم في تعطل أنظمة المدفوعات أو الأنظمة المصرفية الأخرى، مما يؤدي إلى اضطراب العمليات المالية وتأثير سلبي على الاقتصاد المحلي.

جدول يوضح العلاقة بين الأمن السيبراني والاستقرار المالي

العلاقة	التأثير
حماية البيانات الحساسة	يمنع الاحتيال والسرقة المالية، ويحمي مصالح المودعين.

العلاقة	التأثير
استمرارية الأعمال	يضمن تقديم الخدمات المالية بشكل متواصل وموثوق، ويمنع تعطل العمليات.
تعزيز الثقة	يزيد من ثقة العملاء والمستثمرين في البنوك، مما يدعم استقرار النظام المالي.
الامتثال التنظيمي	يحافظ على استقرار النظام المالي ويجنب البنوك الغرامات والعقوبات.
التقليل من المخاطر النظامية	يقلل من احتمالية وقوع هجمات كبيرة تسبب اضطرابات في النظام المالي.
التعامل مع الأزمات بسرعة وكفاءة	يقلل من تأثير الأزمات السيبرانية على الاستقرار المالي، ويعزز القدرة على الاستجابة الفعالة للأزمات.

بهذا، نرى أن الأمن السيبراني يلعب دورًا حاسمًا في تعزيز الاستقرار المالي للبنوك، وهو ما يجعل من إدارة مخاطر الأمن السيبراني ضرورة لا غنى عنها لضمان استدامة النظام المالي وثقة العملاء والمستثمرين.

المبحث الرابع : لشمول المالي

تعريف الشمول المالي

الشمول المالي هو عملية ضمان وصول الأفراد والشركات إلى الخدمات المالية الأساسية بتكلفة معقولة وبشكل ميسر، بما في ذلك الحسابات المصرفية، والتمويل، والادخار، والتأمين، والمدفوعات. يهدف الشمول المالي إلى دمج جميع الفئات المجتمعية، بما في ذلك الفقراء وذوي الدخل المحدود، في النظام المالي الرسمي لتعزيز التنمية الاقتصادية والاجتماعية.

أهمية الشمول المالي للاقتصاد الوطني

الشمول المالي يلعب دورًا مهمًا في تعزيز الاقتصاد الوطني من خلال:

1. تحفيز النمو الاقتصادي:

◦ يساهم في تمكين الأفراد والشركات من الحصول على التمويل اللازم لتوسيع أنشطتهم الاقتصادية، مما يعزز الإنتاجية والنمو الاقتصادي.

2. تقليل الفقر:

◦ يمكن الشمول المالي الفئات الفقيرة من الوصول إلى الخدمات المالية، مما يساهم في تحسين مستوى معيشتهم وزيادة فرصهم الاقتصادية.

3. تعزيز الاستقرار المالي:

◦ يساعد في دمج المزيد من الأفراد والشركات في النظام المالي الرسمي، مما يعزز قاعدة العملاء ويزيد من استقرار المؤسسات المالية.

4. تحسين التوزيع العادل للثروة:

◦ يوفر الشمول المالي الفرص المالية بشكل متساوٍ، مما يساعد في تقليل التفاوت الاقتصادي بين مختلف الفئات المجتمعية.

5. زيادة الإيرادات الحكومية:

◦ من خلال دمج المزيد من الأفراد والشركات في النظام المالي الرسمي، يتم توسيع قاعدة دافعي الضرائب، مما يزيد من الإيرادات الحكومية.

دور الأمن السيبراني في تعزيز الشمول المالي

الأمن السيبراني يلعب دورًا حاسمًا في تعزيز الشمول المالي من خلال:

1. حماية بيانات العملاء:

◦ يضمن الأمن السيبراني حماية البيانات الشخصية والمالية للعملاء، مما يعزز ثقتهم في استخدام الخدمات المالية الرقمية.

2. توفير بيئة آمنة للتعاملات المالية:

◦ يساهم الأمن السيبراني في إنشاء بيئة آمنة وموثوقة للمعاملات المالية الإلكترونية، مما يشجع المزيد من الأفراد على الانخراط في النظام المالي.

3. منع الاحتيال الإلكتروني:

◦ يقلل من مخاطر الاحتيال الإلكتروني التي قد تثني الأفراد والشركات عن استخدام الخدمات المالية الرقمية.

4. تمكين الابتكار المالي:

◦ يدعم تطوير تقنيات مالية مبتكرة وآمنة، مثل الخدمات المصرفية عبر الهواتف المحمولة والمحافظ الرقمية، مما يسهل الوصول إلى الخدمات المالية للفئات المحرومة.

5. تعزيز الثقة في النظام المالي:

◦ يزيد من ثقة الأفراد والشركات في المؤسسات المالية، مما يشجع على استخدام الخدمات المالية والادخار والاستثمار.

6. تقليل تكاليف المعاملات:

◦ يساعد في تقليل تكاليف المعاملات المالية من خلال توفير وسائل آمنة وفعالة للدفع والتحويلات المالية، مما يجعل الخدمات المالية أكثر توفيرًا ومتاحًا للجميع.

مثال توضيحي

لنأخذ مثالاً على خدمة مصرفية عبر الهاتف المحمول يمكن أن تسهل الوصول إلى الخدمات المالية للأفراد في المناطق النائية. ولكن، إذا لم تكن هذه الخدمة آمنة من الناحية السيبرانية، فقد يتردد الأفراد في استخدامها خوفاً من سرقة بياناتهم أو أموالهم. لذا، فإن تأمين هذه الخدمات يعزز من استخدامهم لها، وبالتالي يساهم في تعزيز الشمول المالي.

جدول يوضح دور الأمن السيبراني في تعزيز الشمول المالي

الدور	التأثير
حماية بيانات العملاء	يعزز الثقة في استخدام الخدمات المالية الرقمية.
توفير بيئة آمنة للمعاملات المالية	يشجع المزيد من الأفراد على الانخراط في النظام المالي.
منع الاحتيال الإلكتروني	يقلل من مخاطر الاحتيال ويشجع على استخدام الخدمات المالية الرقمية.
تمكين الابتكار المالي	يدعم تطوير تقنيات مالية مبتكرة وآمنة، مما يسهل الوصول إلى الخدمات المالية للفئات المحرومة.
تعزيز الثقة في النظام المالي	يزيد من ثقة الأفراد والشركات في المؤسسات المالية، مما يشجع على استخدام الخدمات المالية والادخار والاستثمار.

الدور	التأثير
تقليل تكاليف المعاملات	يجعل الخدمات المالية أكثر توفيرًا ومتاحًا للجميع.

من خلال تعزيز الأمن السيبراني، يمكن تحقيق تقدم كبير في الشمول المالي، مما يدعم التنمية الاقتصادية والاجتماعية بشكل عام.

المبحث الخامس : البنوك المدرجة في البورصة السعودية

نبذة عن البورصة السعودية (تداول)

البورصة السعودية، المعروفة أيضًا باسم "تداول"، هي السوق المالية الرئيسية في المملكة العربية السعودية، وهي أكبر سوق مالية في منطقة الشرق الأوسط. تأسست في عام 2007، وتخضع لإشراف هيئة السوق المالية السعودية. تهدف تداول إلى تنظيم وتطوير السوق المالية السعودية، وزيادة الشفافية، وتعزيز الاستثمار المحلي والأجنبي.

أهمية البنوك المدرجة في البورصة للاقتصاد السعودي

تلعب البنوك المدرجة في البورصة السعودية دورًا حيويًا في دعم الاقتصاد الوطني لعدة أسباب:

1. تحفيز النمو الاقتصادي:

توفر البنوك التمويل اللازم للشركات والأفراد، مما يساعد في تعزيز الأنشطة الاقتصادية وزيادة الإنتاجية والنمو الاقتصادي.

2. تعزيز الاستقرار المالي:

تعمل البنوك على جمع الودائع وتوفير القروض، مما يساهم في استقرار النظام المالي وضمان استمرارية العمليات الاقتصادية.

3. جذب الاستثمار:

◦ البنوك المدرجة في البورصة توفر فرص استثمارية للمستثمرين المحليين والأجانب، مما يزيد من تدفق رأس المال إلى الاقتصاد السعودي.

4. توفير فرص العمل:

◦ تساهم البنوك في توفير فرص عمل مباشرة وغير مباشرة، مما يساعد في تقليل معدلات البطالة وزيادة الدخل الوطني.

5. تحسين البنية التحتية المالية:

◦ البنوك تساهم في تطوير وتحسين البنية التحتية المالية، مما يسهل العمليات المالية ويساهم في تحقيق التنمية الاقتصادية المستدامة.

التحديات التي تواجه هذه البنوك في مجال الأمن السيبراني

تواجه البنوك المدرجة في البورصة السعودية العديد من التحديات في مجال الأمن السيبراني، ومن أبرز هذه التحديات:

1. التهديدات السيبرانية المتزايدة:

◦ مع تزايد استخدام التكنولوجيا في العمليات المصرفية، تزداد التهديدات السيبرانية التي تستهدف البنوك، مثل هجمات البرمجيات الخبيثة والقرصنة والاحتيال الإلكتروني.

2. نقص الوعي والتدريب:

◦ قد يكون هناك نقص في الوعي والتدريب بين الموظفين حول كيفية التعامل مع التهديدات السيبرانية واستخدام الأدوات الأمنية بشكل صحيح.

3. التعقيد التكنولوجي:

◦ مع التقدم التكنولوجي السريع، يصبح من الصعب على البنوك مواكبة أحدث التقنيات والحلول الأمنية، مما يزيد من تعرضها للمخاطر.

4. التكلفة المرتفعة:

◦ تكاليف الاستثمار في البنية التحتية للأمن السيبراني وتحديث الأنظمة بشكل دوري يمكن أن تكون مرتفعة، مما يشكل تحدياً للبنوك، خاصة الصغيرة منها.

5. الامتثال التنظيمي:

البنوك تحتاج إلى الامتثال لمجموعة واسعة من القوانين واللوائح المتعلقة بالأمن السيبراني، مما يتطلب جهودًا إضافية لضمان التوافق المستمر مع هذه المتطلبات.

6. التعاون والتنسيق:

الحاجة إلى التعاون والتنسيق بين البنوك والجهات الحكومية والمنظمات الأخرى لتعزيز الأمن السيبراني، وتبادل المعلومات حول التهديدات والسياسات الأمنية.

مثال توضيحي

لنأخذ مثالاً على تحدي الهجمات السيبرانية: يمكن أن تواجه البنوك هجمات من نوع "الفدية" (Ransomware)، حيث يقوم المهاجمون بتشفير البيانات وطلب فدية لإعادة الوصول إليها. هذه الهجمات يمكن أن تعطل العمليات المالية وتسبب خسائر مالية كبيرة، بالإضافة إلى تأثيرها السلبي على سمعة البنك.

جدول يوضح التحديات التي تواجه البنوك في مجال الأمن السيبراني

التحدي	التوضيح
التهديدات السيبرانية المتزايدة	زيادة استخدام التكنولوجيا يزيد من تعرض البنوك للهجمات السيبرانية مثل البرمجيات الخبيثة والاحتيال الإلكتروني.
نقص الوعي والتدريب	نقص في الوعي والتدريب بين الموظفين حول كيفية التعامل مع التهديدات واستخدام الأدوات الأمنية بشكل صحيح.
التعقيد التكنولوجي	صعوبة مواكبة أحدث التقنيات والحلول الأمنية مع التقدم التكنولوجي السريع.
التكلفة المرتفعة	تكاليف الاستثمار في البنية التحتية للأمن السيبراني وتحديث الأنظمة بشكل دوري.

التحدي	التوضيح
الامتثال التنظيمي	الحاجة إلى الامتثال لمجموعة واسعة من القوانين واللوائح المتعلقة بالأمن السيبراني.
التعاون والتنسيق	الحاجة إلى التعاون والتنسيق بين البنوك والجهات الحكومية لتعزيز الأمن السيبراني.

بمواجهة هذه التحديات وتطوير استراتيجيات فعالة لإدارة مخاطر الأمن السيبراني، يمكن للبنوك المدرجة في البورصة السعودية تعزيز قدرتها على حماية أصولها وبيانات عملائها، مما يساهم في تحقيق الاستقرار المالي وتعزيز الشمول المالي.

المبحث السادس : أفضل الممارسات في إدارة مخاطر الأمن السيبراني

استراتيجيات وتوصيات عالمية لتحسين إدارة المخاطر

تتضمن أفضل الممارسات العالمية في إدارة مخاطر الأمن السيبراني مجموعة من الاستراتيجيات والتوصيات التي تهدف إلى تعزيز الأمن السيبراني للمؤسسات المالية. ومن أبرز هذه الاستراتيجيات:

1. تطبيق نهج متعدد الطبقات:

◦ استخدام مزيج من الحلول الأمنية مثل الجدران النارية، أنظمة الكشف عن التسلل (IDS)، أنظمة منع التسلل (IPS)، والتشفير لتوفير حماية شاملة.

2. التدريب والتوعية المستمرة:

◦ تقديم برامج تدريبية دورية للموظفين لزيادة وعيهم بأحدث التهديدات السيبرانية وأساليب الوقاية منها.

3. إجراء تقييمات دورية للمخاطر:

◦ تنفيذ عمليات تقييم دورية وشاملة للمخاطر لتحديد الثغرات الأمنية وتحديث استراتيجيات الأمان بناءً على النتائج.

4. تطوير خطط استجابة للطوارئ:

◦ إعداد وتحديث خطط الاستجابة للحوادث السيبرانية لضمان استجابة فعالة وسريعة في حالة حدوث اختراقات أو هجمات.

5. تطبيق ممارسات الأمان السحابي:

◦ تأمين البنية التحتية السحابية من خلال استخدام بروتوكولات الأمان المناسبة ومراقبة الأنشطة المشبوهة.

6. التعاون الدولي:

◦ التعاون مع الهيئات والمنظمات الدولية لمشاركة المعلومات حول التهديدات السيبرانية والتعلم من التجارب العالمية.

أمثلة من تجارب ناجحة لبنوك عالمية في تعزيز الأمن السيبراني

1. بنك جي بي مورجان تشيس (JPMorgan Chase):

◦ استثمر البنك مليارات الدولارات في تعزيز أمنه السيبراني، وطور مركزاً متقدماً لرصد التهديدات (SOC) يستخدم الذكاء الاصطناعي لتحليل البيانات وكشف الأنشطة المشبوهة.

2. بنك باركليز (Barclays):

◦ اعتمد باركليز برنامجاً شاملاً لتوعية الموظفين حول الأمن السيبراني، بما في ذلك محاكاة هجمات سيبرانية لاختبار استجابتهم وتعزيز الوعي بالأمن.

3. بنك أوف أمريكا (Bank of America):

◦ تبني البنك استراتيجية أمنية متكاملة تشمل أنظمة كشف التهديدات المتقدمة، وبرامج مكافحة البرمجيات الخبيثة، والتشفير القوي لحماية البيانات الحساسة.

4. بنك دويتشه (Deutsche Bank):

◦ استثمر دويتشه بنك في تطوير تقنيات أمان مبتكرة مثل استخدام تقنيات التعلم الآلي لتحليل البيانات ورصد الأنشطة غير العادية.

تطبيق هذه الممارسات في السياق السعودي

لتطبيق أفضل الممارسات العالمية في السياق السعودي، يمكن اتباع الخطوات التالية:

1. تعزيز التعاون المحلي والدولي:

◦ التعاون مع الهيئات المحلية مثل هيئة السوق المالية السعودية (CMA) والمؤسسات الدولية لتبادل المعلومات والخبرات حول التهديدات السيبرانية.

2. تطوير بنية تحتية تقنية متقدمة:

◦ الاستثمار في أحدث تقنيات الأمن السيبراني وتطوير مراكز متقدمة لرصد التهديدات السيبرانية.

3. تقديم برامج تدريبية شاملة:

◦ توفير برامج تدريبية مستمرة للموظفين لتعزيز وعيهم الأمني وتحديث معارفهم بأحدث التهديدات وأساليب الحماية.

4. إجراء تقييمات دورية للأمان:

◦ تنفيذ تقييمات دورية وشاملة للأمان السيبراني لتحديد الثغرات وتحديث استراتيجيات الأمان بناءً على النتائج.

5. تطوير خطط استجابة محلية:

◦ إعداد وتحديث خطط الاستجابة للحوادث السيبرانية بما يتوافق مع البيئة المحلية والتحديات الفريدة التي تواجهها البنوك في السعودية.

6. تفعيل برامج التوعية المجتمعية:

◦ توعية العملاء حول أهمية الأمن السيبراني وكيفية حماية معلوماتهم الشخصية والمالية من خلال الحملات التوعوية وورش العمل.

خلاصة

بتبني هذه الاستراتيجيات والممارسات العالمية، يمكن للبنوك المدرجة في البورصة السعودية تعزيز أمنها السيبراني بشكل فعال، مما يساهم في حماية الأصول المالية والبيانات الحساسة، وتعزيز الثقة في النظام المالي، ودعم الاستقرار المالي والشمول المالي في المملكة.

المبحث السابع : الدراسات السابقة

1. دراسة العبدالات، صدام عبدالله عبدالكريم. 2023. بعنوان "أثر الأمن السيبراني في التسويق الإلكتروني في البنوك التجارية الأردنية" تهدف الدراسة إلى التعرف على أثر الأمن السيبراني في التسويق الإلكتروني في البنوك التجارية الأردنية، حيث تستكمل الدراسة مفهوم الأمن السيبراني وأهميته في ضمان سلامة وسرية المعلومات المتداولة

عبر قنوات التسويق الإلكتروني في البنوك وحمايتها من الهجمات والاختراقات الإلكترونية. كما استعرضت الدراسة أبرز مخاطر الأمن السيبراني التي تواجهها البنوك مثل سرقة الهويات والبيانات المالية والاحتيال عبر الإنترنت.

2. دراسة عبدالحميد، عماد الدين محمد كامل. 2021. بعنوان "استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي: دراسة في العملات الرقمية للبنوك المركزية : الحلقة الأولى". هدف الدراسة إلى استعراض استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي. حيث تتناول هذه الدراسة ثلاثة محاور رئيسية، تطرق المحور الأول إلى مفهوم الاقتصاد الرقمي والتجارة الإلكترونية فيه. بينما يتم عرض المحور الثاني ماهية العملات الرقمية للبنوك المركزية والنماذج البيئية لها ومشروعات الدول لإصدارها. أما المحور الثالث فقد تناول ضوابط إصدار العملات الرقمية للبنوك المركزية ومزاياها والمخاطر المحتملة منها. كما خلصت الدراسة إلى ضرورة توافر سمات أساسية في سوق الصرف الأجنبي للبنوك المركزية مثل المرونة والقدرة على التكيف مع المتغيرات.

3. دراسة حسين، رانيا موسى عبدالله. 2022. بعنوان "أثر الأمن السيبراني في سمعة البنوك التجارية الأردنية". تهدف الدراسة إلى التعرف على أثر الأمن السيبراني في سمعة البنوك التجارية الأردنية. حيث تهدف الدراسة إلى التعرف على مفهوم الأمن السيبراني وأهميته في البنوك التجارية الأردنية، والتعرف على أبرز مخاطر الأمن السيبراني التي تواجهها، وقياس أثر الأمن السيبراني على سمعة البنوك التجارية الأردنية من خلال تحليل استبانة تم توزيعها على عينة من الموظفين والعمل في هذه البنوك. كما أن ملخص الدراسة عرض لموضوعات الدراسة ذات الصلة بموضوع البحث، حيث تم عرض الدراسات السابقة ذات الصلة، ثم شرح منهج الدراسة وأدواتها، تلاه عرض ومناقشة ودراسة النتائج. ثم خلصت إلى مجموعة من المقترحات.

4. دراسة مطالقة، الحارث صالح أحمد. 2020. بعنوان "دور إدارة الأمن السيبراني في التوعية والحد من الجرائم المالية من وجهة نظر العاملين في البنوك الأردنية". وتهدف الدراسة إلى التعرف على دور إدارة الأمن السيبراني في التوعية والحد من الجرائم المالية من وجهة نظر العاملين في البنوك الأردنية. حيث تهدف إلى التعرف على مفهوم الأمن السيبراني والجرائم المالية، وأهداف إدارة الأمن السيبراني، ومهمتها في التوعية والحد من الجرائم المالية، بالإضافة إلى التعرف على متطلبات النجاح والفشل لدور

إدارة الأمن السيبراني في تحقيق أهداف وجهة نظر العاملين في البنوك، كما تهدف إلى الوقوف على التحديات التي تواجه إدارة الأمن السيبراني.

الفجوات البحثية التي يسعى البحث الحالي لتغطيتها

بعد مراجعة الدراسات السابقة المذكورة، تم تحديد عدة فجوات بحثية يمكن أن يغطيها البحث الحالي حول "أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في البورصة السعودية":

1. البعد المكاني:

تركزت الدراسات السابقة على البنوك في الأردن، بينما يركز البحث الحالي على البنوك المدرجة في البورصة السعودية. هذا يتيح فرصة لدراسة تأثيرات الأمن السيبراني في سياق اقتصادي مختلف وله تحديات وفرص فريدة.

2. الاستقرار المالي والشمول المالي:

لم تتناول الدراسات السابقة بشكل محدد العلاقة بين إدارة مخاطر الأمن السيبراني والاستقرار المالي والشمول المالي في البنوك. يهدف البحث الحالي إلى سد هذه الفجوة من خلال تحليل كيفية تأثير الأمن السيبراني على استقرار النظام المالي وزيادة الشمول المالي.

3. المؤشرات المالية:

الدراسات السابقة مثل دراسة العبدلات (2023) ودراسة حسين (2022) ركزت على التسويق الإلكتروني وسمعة البنوك، دون التعمق في المؤشرات المالية والأداء المالي للبنوك. البحث الحالي سيعمل على استكشاف تأثير الأمن السيبراني على المؤشرات المالية للبنوك المدرجة في البورصة السعودية.

4. التحديات المحلية:

لم تتطرق الدراسات السابقة بشكل كافٍ إلى التحديات الخاصة التي تواجه البنوك في السعودية في مجال الأمن السيبراني. البحث الحالي سيغطي التحديات الفريدة التي قد تواجهها البنوك السعودية مثل التهديدات السيبرانية المحلية، والامتثال للوائح المحلية.

5. التطورات التكنولوجية الحديثة:

قد لا تغطي الدراسات السابقة أحدث التطورات في مجال الأمن السيبراني والتقنيات المستخدمة لحماية الأنظمة المالية. البحث الحالي سيستفيد من استعراض أحدث التقنيات والحلول المتاحة لتعزيز الأمن السيبراني في البنوك.

6. التوصيات والممارسات العملية:

◦ على الرغم من تقديم بعض الدراسات لمقترحات وتوصيات، فإن البحث الحالي سيسعى لتقديم توصيات عملية ومبنية على تحليل شامل لبيانات محددة من البنوك المدرجة في البورصة السعودية، مما يوفر قيمة عملية أعلى للمؤسسات المالية.

7. تأثير الهجمات السيبرانية:

◦ دراسة تأثير الهجمات السيبرانية على الثقة العامة، وكفاءة العمليات، والتكاليف المرتبطة بالاستجابة لهذه الهجمات. البحث الحالي سيغطي هذه الجوانب بشكل أكثر تفصيلاً.

بهذا، يسعى البحث الحالي إلى سد الفجوات البحثية المذكورة من خلال تحليل شامل ومتعمق لإدارة مخاطر الأمن السيبراني وأثرها على الاستقرار المالي والشمول المالي في البنوك المدرجة في البورصة السعودية، مما يضيف قيمة علمية وعملية للمجال.

الفصل الثالث : منهجية البحث

المقدمة

يهدف هذا الفصل إلى شرح منهجية البحث التي تم اعتمادها لدراسة أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في البورصة السعودية. يوضح هذا الفصل الأدوات والأساليب المستخدمة لجمع البيانات وتحليلها، وكذلك كيفية تصميم الاستبانة الإلكترونية واختيار العينة. يعد هذا الفصل أساسياً لضمان وضوح ودقة النتائج والتوصيات التي سيتم التوصل إليها من خلال البحث.

من خلال هذا الفصل، سنقوم بتفصيل الخطوات المتبعة في جمع البيانات، بدءاً من تصميم الاستبانة الإلكترونية وتوزيعها، مروراً بكيفية جمع الردود وتحليلها، وصولاً إلى استخلاص النتائج. نهدف إلى تقديم صورة شاملة للمنهجية المتبعة لضمان تحقيق الأهداف البحثية بشكل دقيق وموثوق.

التعريفات الإجرائية لمتغيرات البحث

1. الأمن السيبراني :

• **تعريف إجرائي:** مجموعة من التقنيات والإجراءات والسياسات التي تستخدمها البنوك لحماية أنظمتها الرقمية وبياناتها الحساسة من التهديدات والهجمات السيبرانية. يتم قياس هذا المتغير من خلال استبانة تتضمن أسئلة حول السياسات الأمنية المتبعة، تقنيات الحماية المستخدمة، ومدى وعي الموظفين بالأمن السيبراني. (مجلة الدبلوماسي، 2018).

2. إدارة مخاطر الأمن السيبراني

• **تعريف إجرائي:** العمليات والإجراءات المتبعة لتحديد وتقييم والتحكم في المخاطر السيبرانية التي تواجه البنوك. يتم قياس هذا المتغير من خلال استبانة تشمل أسئلة حول عمليات تحديد وتقييم المخاطر، استراتيجيات التحكم، وخطط الطوارئ المستخدمة في حال وقوع هجمات سيبرانية. (حسين، 2024).

3. الاستقرار المالي

• **تعريف إجرائي:** قدرة البنوك على الحفاظ على عملياتها المالية بشكل مستقر وآمن دون تعرضها لمشكلات أو اضطرابات ناتجة عن التهديدات السيبرانية. يتم قياس هذا المتغير من خلال استبانة تحتوي على أسئلة تتعلق بتأثير الهجمات السيبرانية على الأداء المالي للبنك، ومدى تأثير السياسات الأمنية على استقرار العمليات المالية. (صديقي، 2016)

4. الشمول المالي

• **تعريف إجرائي:** مدى قدرة البنوك على تقديم الخدمات المالية لكافة فئات المجتمع، بما في ذلك الأفراد ذوي الدخل المحدود والمناطق النائية، مع ضمان أمان هذه الخدمات. يتم قياس هذا المتغير من خلال استبانة تتضمن أسئلة حول مدى انتشار الخدمات المالية الرقمية، وسهولة الوصول إليها، ومدى أمان استخدامها. (كركار، 2019).

5. التحديات السيبرانية

• **تعريف إجرائي:** المشكلات والعقبات التي تواجه البنوك في تأمين أنظمتها الرقمية ضد التهديدات السيبرانية. يتم قياس هذا المتغير من خلال استبانة تشمل أسئلة حول أنواع التهديدات السيبرانية التي تواجهها البنوك، ومدى صعوبة التعامل معها، والموارد المتاحة للتصدي لهذه التهديدات. (البابلي، 2021)

6. التقنيات الأمنية

. تعريف إجرائي: الأدوات والتقنيات المستخدمة في البنوك لحماية أنظمتها وبياناتها من الهجمات السيبرانية. يتم قياس هذا المتغير من خلال استبانة تحتوي على أسئلة حول استخدام تقنيات مثل التشفير، الجدران النارية، أنظمة الكشف عن التسلل، والمصادقة متعددة العوامل. (دليو، وكلاع، 2017)

7. وعي الموظفين

. تعريف إجرائي: مستوى معرفة الموظفين وفهمهم للممارسات الأمنية والسياسات المتعلقة بالأمن السيبراني. يتم قياس هذا المتغير من خلال استبانة تشمل أسئلة حول برامج التدريب التي يتلقاها الموظفون، ومدى قدرتهم على التعرف على التهديدات السيبرانية والاستجابة لها. (الخميسة، 2022).

تصميم البحث (بصلة البحث)

: مقدمة

يهدف هذا القسم إلى توضيح تصميم البحث المتبع لدراسة أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في البورصة السعودية. يركز التصميم على تحديد الإجراءات المنهجية لجمع وتحليل البيانات بما يضمن تحقيق أهداف البحث.

1. نوع البحث

البحث يتبع منهجاً وصفيًا تحليليًا، حيث يهدف إلى وصف وتحليل تأثير إدارة مخاطر الأمن السيبراني على الاستقرار المالي والشمول المالي في البنوك المدرجة في البورصة السعودية.

2. مجتمع البحث

يتكون مجتمع البحث من جميع البنوك المدرجة في البورصة السعودية. يهدف البحث إلى الحصول على بيانات من عينة ممثلة لهذه البنوك لضمان شمولية ودقة النتائج.

3. عينة البحث

ستكون العينة مكونة من مجموعة من البنوك المدرجة في البورصة السعودية، حيث سيتم اختيار العينة بطريقة عشوائية طبقية لضمان تمثيل كافة أنواع البنوك (محلية، إقليمية، دولية).

4. أداة جمع البيانات

سيتم استخدام استبانة إلكترونية كأداة رئيسية لجمع البيانات. ستتضمن الاستبانة مجموعة من الأسئلة المصممة لقياس المتغيرات المختلفة المتعلقة بالأمن السيبراني، وإدارة المخاطر، والاستقرار المالي، والشمول المالي.

5. تصميم الاستبانة

. الجزء الأول: المعلومات الديموغرافية:

◦ يشمل معلومات عن البنك مثل الحجم، النوع، وعدد الفروع.

. الجزء الثاني: أسئلة حول الأمن السيبراني:

◦ تتضمن أسئلة حول السياسات الأمنية المتبعة، التقنيات المستخدمة، ووعي الموظفين بالأمن السيبراني.

. الجزء الثالث: أسئلة حول إدارة مخاطر الأمن السيبراني:

◦ تتضمن أسئلة حول عمليات تحديد وتقييم المخاطر، استراتيجيات التحكم، وخطط الطوارئ.

. الجزء الرابع: أسئلة حول الاستقرار المالي:

◦ تتضمن أسئلة حول تأثير الأمن السيبراني على الأداء المالي للبنك واستمرارية العمليات.

. الجزء الخامس: أسئلة حول الشمول المالي:

◦ تتضمن أسئلة حول مدى انتشار الخدمات المالية الرقمية، وسهولة الوصول إليها، ومدى أمان استخدامها.

6. جمع البيانات

سيتم توزيع الاستبانة الإلكترونية على عينة البحث باستخدام البريد الإلكتروني والوسائل الإلكترونية الأخرى لضمان الوصول إلى أكبر عدد ممكن من المشاركين.

7. تحليل البيانات

. الأساليب الإحصائية: سيتم استخدام أساليب إحصائية متنوعة لتحليل البيانات، بما في ذلك التحليل الوصفي، تحليل الانحدار، وتحليل التباين.

. أدوات التحليل: سيتم استخدام برامج تحليل البيانات مثل SPSS و Excel لإجراء التحليلات الإحصائية واستخلاص النتائج.

8. عرض النتائج

سيتم عرض النتائج باستخدام الجداول والرسوم البيانية لتوضيح التأثيرات المختلفة للأمن السيبراني على الاستقرار المالي والشمول المالي.

9. تفسير النتائج

- سيتم تفسير النتائج بناءً على الأدبيات السابقة والمعرفة الحالية في المجال.
- سيتم ربط النتائج بالفرضيات البحثية لتأكيد أو دحضها.

10. التوصيات

بناءً على النتائج، سيتم تقديم توصيات لتحسين إدارة مخاطر الأمن السيبراني في البنوك المدرجة في البورصة السعودية لتعزيز الاستقرار المالي والشمول المالي.

مجتمع البحث وطرق وتقنيات أخذ العينات

مجتمع البحث

يتكون مجتمع البحث من جميع البنوك المدرجة في البورصة السعودية. يشمل هذا المجتمع البنوك المحلية والإقليمية والدولية التي تعمل في السوق السعودي وتم إدراجها في البورصة السعودية (تداول).

طرق وتقنيات أخذ العينات

لضمان تمثيل دقيق وشامل لمجتمع البحث، سيتم استخدام تقنيات أخذ العينات التالية:

1. أخذ العينات العشوائية الطبقية:

- **تعريف:** يتم تقسيم مجتمع البحث إلى طبقات أو فئات متميزة بناءً على خصائص معينة، ثم يتم اختيار عينة عشوائية من كل طبقة.
- **سبب الاختيار:** هذه الطريقة تضمن تمثيل جميع أنواع البنوك (محلية، إقليمية، دولية) بشكل متساوٍ، مما يعزز دقة النتائج.

خطوات أخذ العينات العشوائية الطبقية

1. تحديد الطبقات:

- يتم تقسيم مجتمع البحث إلى طبقات وفقاً لنوع البنك (محلي، إقليمي، دولي).

2. تحديد حجم العينة لكل طبقة:

- تحديد النسبة المئوية للبنوك التي سيتم اختيارها من كل طبقة بناءً على حجم الطبقة داخل مجتمع البحث الكلي.

3. اختيار العينة العشوائية:

- يتم اختيار البنوك بشكل عشوائي من كل طبقة باستخدام أسلوب العينة العشوائية البسيطة.

مثال توضيحي

إذا كان لدينا مجتمع بحث مكون من 100 بنك مدرج في البورصة السعودية، وكانت الطبقات كالتالي:

• البنوك المحلية: 50 بنكًا.

• البنوك الإقليمية: 30 بنكًا.

• البنوك الدولية: 20 بنكًا.

وحجم العينة المطلوب هو 30 بنكًا:

• نسبة البنوك المحلية في العينة: $(50/100) * 30 = 15$ بنكًا.

• نسبة البنوك الإقليمية في العينة: $(30/100) * 30 = 9$ بنوك.

• نسبة البنوك الدولية في العينة: $(20/100) * 30 = 6$ بنوك.

بهذا، يتم اختيار 15 بنكًا محليًا، و9 بنوك إقليمية، و6 بنوك دولية بشكل عشوائي من كل طبقة.

طرق جمع البيانات

سيتم استخدام الاستبانة الإلكترونية كأداة رئيسية لجمع البيانات من العينة المختارة. تتضمن خطوات جمع البيانات ما يلي:

1. تصميم الاستبانة:

• إعداد استبانة شاملة تتضمن أسئلة حول المتغيرات الأساسية مثل الأمن السيبراني، إدارة المخاطر، الاستقرار المالي، والشمول المالي.

2. توزيع الاستبانة:

• إرسال الاستبانة عبر البريد الإلكتروني إلى البنوك المختارة في العينة، مع توفير تعليمات واضحة حول كيفية ملء الاستبانة وإرسالها.

3. جمع الردود:

• متابعة الردود وجمع البيانات من الاستبانات المكتملة، وضمان الحصول على نسبة استجابة كافية لتحليل البيانات بشكل موثوق.

4. تحليل البيانات:

• استخدام برامج تحليل البيانات الإحصائية مثل SPSS و Excel لتحليل البيانات المستلمة واستخلاص النتائج.

طريقة جمع البيانات

1. أداة جمع البيانات: الاستبانة الإلكترونية

سيتم استخدام الاستبانة الإلكترونية كأداة رئيسية لجمع البيانات. تتضمن هذه الأداة مجموعة من الأسئلة المصممة لقياس المتغيرات المختلفة المتعلقة بالأمن السيبراني، وإدارة المخاطر، والاستقرار المالي، والشمول المالي. سيتم تصميم الاستبانة باستخدام منصة إلكترونية موثوقة تتيح سهولة التوزيع وجمع الردود.

2. تصميم الاستبانة

. الجزء الأول: المعلومات الديموغرافية

○ يتضمن أسئلة حول المعلومات الأساسية للبنك مثل:

- . اسم البنك.
- . حجم البنك (كبير، متوسط، صغير).
- . نوع البنك (محلي، إقليمي، دولي).
- . عدد الفروع.

. الجزء الثاني: أسئلة حول الأمن السيبراني

○ تتضمن أسئلة تتعلق بالسياسات الأمنية المتبعة، والتقنيات المستخدمة، ومدى وعي الموظفين بالأمن السيبراني.

. مثال: "ما هي السياسات الأمنية التي يتبعها البنك لحماية بيانات العملاء؟"

. الجزء الثالث: أسئلة حول إدارة مخاطر الأمن السيبراني

○ تتضمن أسئلة حول عمليات تحديد وتقييم المخاطر، استراتيجيات التحكم، وخطط الطوارئ.

. مثال: "كيف يتم تحديد المخاطر السيبرانية التي قد تواجه البنك؟"

. الجزء الرابع: أسئلة حول الاستقرار المالي

○ تتضمن أسئلة حول تأثير الأمن السيبراني على الأداء المالي للبنك واستمرارية العمليات.

. مثال: "ما هو تأثير الهجمات السيبرانية على الاستقرار المالي للبنك؟"

. الجزء الخامس: أسئلة حول الشمول المالي

○ تتضمن أسئلة حول مدى انتشار الخدمات المالية الرقمية، وسهولة الوصول إليها، ومدى أمان استخدامها.

. مثال: "كيف يؤثر الأمن السيبراني على قدرة البنك في تقديم الخدمات المالية الرقمية لعملائه؟"

3. توزيع الاستبانة

. تحديد العينة المستهدفة:

◦ سيتم اختيار عينة من البنوك المدرجة في البورصة السعودية باستخدام تقنية العينة العشوائية الطبقية لضمان تمثيل جميع أنواع البنوك (محلية، إقليمية، دولية).

. إرسال الاستبانة:

◦ سيتم إرسال الاستبانة الإلكترونية إلى العينة المستهدفة عبر البريد الإلكتروني، مع رسالة توضيحية تشمل:

- . هدف البحث.
- . تعليمات ملء الاستبانة.
- . تأكيد سرية المعلومات المقدمة.
- . تاريخ نهائي لإعادة الاستبانة.

4. جمع الردود

. متابعة الردود:

◦ سيتم متابعة الردود بشكل دوري لضمان جمع أكبر عدد ممكن من الاستجابات. سيتم إرسال تذكيرات ودية للبنوك التي لم تستجب بعد.

. جمع البيانات:

◦ سيتم تجميع الردود من الاستبانات المكتملة وتخزينها بشكل آمن لضمان سرية المعلومات.

5. تحليل البيانات

. تنظيف البيانات:

◦ مراجعة الردود لضمان دقتها واكتمالها، والتأكد من خلوها من البيانات المفقودة أو غير الصحيحة.

. التحليل الإحصائي:

◦ استخدام برامج تحليل البيانات الإحصائية مثل SPSS و Excel لإجراء التحليلات المناسبة، مثل التحليل الوصفي، تحليل الانحدار، وتحليل التباين.

. عرض النتائج:

◦ سيتم عرض النتائج باستخدام الجداول والرسوم البيانية لتوضيح التأثيرات المختلفة للأمن السيبراني على الاستقرار المالي والشمول المالي.

خلاصة

باستخدام الاستبانة الإلكترونية كأداة لجمع البيانات، يضمن البحث الحصول على معلومات دقيقة وشاملة حول إدارة مخاطر الأمن السيبراني في البنوك المدرجة في البورصة السعودية. تتيح هذه الطريقة جمع بيانات موثوقة وقابلة للتحليل، مما يساعد في تحقيق أهداف البحث بشكل فعال.

أنواع البيانات

1. البيانات الديموغرافية

تتضمن هذه البيانات المعلومات الأساسية عن البنوك المشاركة في الدراسة. تساعد البيانات الديموغرافية في تصنيف البنوك وتحليل النتائج بناءً على خصائص مختلفة.

• أمثلة:

- اسم البنك.
- حجم البنك (كبير، متوسط، صغير).
- نوع البنك (محلي، إقليمي، دولي).
- عدد الفروع.

2. البيانات النوعية

تتعلق البيانات النوعية بالمعلومات غير العددية التي تصف خصائص معينة للأمن السيبراني وإدارة المخاطر في البنوك. يمكن أن تكون هذه البيانات وصفية أو تصنيفية.

• أمثلة:

- سياسات الأمن السيبراني المطبقة.
- الاستراتيجيات المتبعة في إدارة المخاطر.
- وصف للتحديات السيبرانية التي تواجه البنوك.
- تقييم مستوى الوعي الأمني بين الموظفين.

3. البيانات الكمية

تشمل البيانات الكمية المعلومات العددية التي يمكن قياسها وتحليلها إحصائيًا. تساعد هذه البيانات في تحديد مدى تأثير الأمن السيبراني على المتغيرات الأخرى مثل الاستقرار المالي والشمول المالي.

. أمثلة:

- عدد الهجمات السيبرانية التي تعرض لها البنك خلال فترة زمنية محددة.
- حجم الإنفاق على تقنيات الأمن السيبراني.
- نسبة الاستثمارات في الأمن السيبراني من إجمالي الميزانية.
- عدد المستخدمين الذين يتعاملون مع الخدمات المالية الرقمية.

4. البيانات التقييمية

تشمل البيانات التقييمية المعلومات التي تعكس آراء وتقييمات المشاركين حول جوانب مختلفة من الأمن السيبراني وإدارة المخاطر.

. أمثلة:

- تقييم فعالية السياسات الأمنية.
- مستوى الرضا عن التدابير الأمنية الحالية.
- تقييم تأثير الهجمات السيبرانية على الاستقرار المالي.
- تقييم قدرة البنك على تقديم خدمات مالية آمنة.

5. البيانات الزمنية

تشمل البيانات الزمنية المعلومات التي تتعلق بفترات زمنية معينة. يمكن أن تكون هذه البيانات مفيدة لتحليل الاتجاهات والتغيرات بمرور الوقت.

. أمثلة:

- تواريخ وقوع الهجمات السيبرانية.
- فترات تنفيذ استراتيجيات أمنية جديدة.
- مدى التغير في حجم الإنفاق على الأمن السيبراني عبر السنوات.

جمع البيانات وتحليلها

جمع البيانات

- الاستبانة الإلكترونية: سيتم تصميم الاستبانة لتجمع بيانات من الأنواع المختلفة المذكورة أعلاه. سيتم إرسال الاستبانة إلى عينة مختارة من البنوك المدرجة في البورصة السعودية بشكل افتراضي.
- المتابعة والتذكير: لضمان جمع البيانات من أكبر عدد ممكن من البنوك، سيتم إرسال تذكيرات دورية.

تحليل البيانات

- **البيانات الديموغرافية:** سيتم تحليلها لتصنيف البنوك وتحديد الخصائص الديموغرافية المشتركة.
- **البيانات النوعية:** سيتم تحليلها باستخدام تقنيات التحليل النوعي لاستخلاص الأنماط والاتجاهات.
- **البيانات الكمية:** سيتم تحليلها باستخدام الأساليب الإحصائية مثل التحليل الوصفي، تحليل الانحدار، وتحليل التباين.
- **البيانات التقييمية:** سيتم تحليلها لاستخلاص تقييمات المشاركين وآرائهم حول جوانب الأمن السيبراني.
- **البيانات الزمنية:** سيتم تحليلها لتحديد الاتجاهات والتغيرات بمرور الوقت.

خلاصة

بفهم أنواع البيانات المختلفة وجمعها بشكل منهجي، يمكن للبحث تقديم تحليل شامل ومتكامل لأثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في البورصة السعودية. يساعد هذا التنوع في البيانات على تحقيق نتائج دقيقة وموثوقة تسهم في تحسين الممارسات الأمنية في القطاع المصرفي.

إجراءات التحليل الإحصائي

1. تنظيف البيانات

- **مراجعة البيانات:** التأكد من اكتمال جميع الردود والتخلص من الردود الناقصة أو غير الصالحة.
- **توحيد البيانات:** التأكد من توحيد صيغة البيانات مثل توحيد طريقة كتابة التواريخ والأرقام.
- **التأكد من القيم المتطرفة:** تحديد القيم المتطرفة التي قد تؤثر على نتائج التحليل والتعامل معها وفقاً للمنهجية المناسبة (استبعادها أو تحليلها بشكل منفصل).

2. تحليل البيانات الوصفية

- **الإحصاءات الوصفية:** حساب المقاييس الإحصائية الأساسية مثل المتوسط، الوسيط، الانحراف المعياري، والنسب المئوية.
- **المتوسط (Mean):** حساب المتوسط لجميع المتغيرات الكمية.
- **الوسيط (Median):** تحديد الوسيط للبيانات الكمية، خاصة إذا كانت البيانات غير موزعة بشكل طبيعي.

◦ الانحراف المعياري (Standard Deviation): حساب الانحراف المعياري لفهم تشتت البيانات.

◦ النسب المئوية (Percentages): حساب النسب المئوية للمتغيرات النوعية مثل تصنيف البنوك حسب الحجم أو النوع.

3. تحليل البيانات الكمية

◦ تحليل التباين (ANOVA): استخدام تحليل التباين لفحص الفروق بين مجموعات مختلفة من البيانات.

◦ مثال: تحليل الفروق في مستوى الأمن السيبراني بين البنوك المحلية والإقليمية والدولية.

◦ تحليل الانحدار (Regression Analysis): استخدام تحليل الانحدار لفحص العلاقة بين متغير تابع (مثل الاستقرار المالي) ومتغير مستقل (مثل مستوى الأمن السيبراني).

◦ تحليل الانحدار البسيط: لفحص العلاقة بين متغيرين.

◦ تحليل الانحدار المتعدد: لفحص العلاقة بين متغير تابع وعدة متغيرات مستقلة.

4. تحليل البيانات النوعية

◦ التحليل الموضوعي (Thematic Analysis): تحليل البيانات النوعية لاستخلاص الأنماط والموضوعات الرئيسية.

◦ ترميز البيانات (Coding): تقسيم البيانات النصية إلى أجزاء صغيرة ومنح كل جزء رمزاً يعبر عن معناه.

◦ تحديد الموضوعات (Identifying Themes): تجميع الأكواد المتشابهة لتحديد الموضوعات الرئيسية التي تظهر في البيانات.

◦ تحليل التكرارات (Frequency Analysis): حساب تكرار ظهور كلمات أو موضوعات معينة في البيانات النصية لفهم الاتجاهات العامة.

5. تحليل البيانات الزمنية

◦ تحليل الاتجاهات (Trend Analysis): تحليل البيانات الزمنية لتحديد الاتجاهات والتغيرات على مر الزمن.

◦ مثال: تحليل التغيرات في حجم الإنفاق على الأمن السيبراني عبر السنوات.

◦ التحليل الدوري (Seasonal Analysis): فحص البيانات الزمنية لتحديد الأنماط الدورية أو الموسمية.

6. التحليل الإحصائي المتقدم

- **التحليل العنقودي (Cluster Analysis):** تصنيف البنوك إلى مجموعات متجانسة بناءً على خصائص معينة مثل مستوى الأمن السيبراني والاستقرار المالي.
- **تحليل العوامل (Factor Analysis):** تقليل عدد المتغيرات الكثيرة إلى عدد أقل من العوامل الأساسية التي تفسر العلاقات بين المتغيرات.

7. عرض النتائج

- **الجدول (Tables):** استخدام الجداول لعرض البيانات الإحصائية بشكل منظم وواضح.
- **الرسوم البيانية (Charts):** استخدام الرسوم البيانية مثل الرسوم البيانية الشريطية والرسوم البيانية الدائرية والرسوم البيانية الخطية لتوضيح النتائج.
- **المخططات التوضيحية (Diagrams):** استخدام المخططات التوضيحية لتقديم تحليل بصري للعلاقات بين المتغيرات.

خلاصة

باستخدام إجراءات التحليل الإحصائي المذكورة، يمكن تحليل البيانات التي تم جمعها من الاستبانة الإلكترونية بشكل منهجي وشامل. يضمن هذا النهج تحقيق نتائج دقيقة وموثوقة تساهم في فهم أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في البورصة السعودية.

الخاتمة

تتناول هذه الدراسة تأثير إدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي وتعزيز الشمول المالي في البنوك المدرجة في البورصة السعودية. من خلال تحليل البيانات التي تم جمعها باستخدام استبانة إلكترونية واستعراض الأدبيات ذات الصلة، تم التوصل إلى مجموعة من النتائج التي تسلط الضوء على أهمية الأمن السيبراني في القطاع المصرفي.

ملخص النتائج

- **فعالية إدارة مخاطر الأمن السيبراني:** أظهرت الدراسة أن البنوك التي تتبنى استراتيجيات فعالة لإدارة مخاطر الأمن السيبراني تتمتع بمستوى عالٍ من الاستقرار المالي. هذه الاستراتيجيات تساعد في تقليل الخسائر المالية الناجمة عن الهجمات السيبرانية وتضمن استمرارية العمليات المصرفية.

- **تعزيز الثقة والشمول المالي:** الأمن السيبراني القوي يعزز ثقة العملاء والمستثمرين في البنوك، مما يساهم في زيادة الشمول المالي. البنوك التي توفر بيئة آمنة للخدمات المالية الرقمية تستطيع جذب المزيد من العملاء وتوسيع قاعدة مستخدميها.
- **التحديات الفريدة في السياق السعودي:** تبين أن البنوك السعودية تواجه تحديات محددة في مجال الأمن السيبراني، بما في ذلك نقص الوعي بين الموظفين والتحديات التكنولوجية. ومع ذلك، فإن الاستثمار في التدريب وتبني التقنيات الحديثة يمكن أن يساعد في التغلب على هذه التحديات.

توصيات البحث

بناءً على النتائج التي تم التوصل إليها، نقدم التوصيات التالية:

1. **تعزيز برامج التدريب والتوعية:** ينبغي للبنوك أن تستثمر في تدريب الموظفين على أحدث أساليب الأمن السيبراني ورفع مستوى الوعي لديهم حول التهديدات السيبرانية وكيفية التعامل معها.
2. **تبني التقنيات الحديثة:** يجب على البنوك الاستثمار في أحدث تقنيات الأمن السيبراني، مثل التشفير المتقدم وأنظمة الكشف عن التسلل، لضمان حماية بيانات العملاء والبنية التحتية الرقمية.
3. **تطوير خطط استجابة للطوارئ:** ينبغي للبنوك إعداد وتحديث خطط الاستجابة للحوادث السيبرانية لضمان استجابة سريعة وفعالة في حالة وقوع هجوم.
4. **التعاون مع الجهات التنظيمية:** على البنوك العمل بشكل وثيق مع الهيئات التنظيمية لتبادل المعلومات حول التهديدات السيبرانية والامتثال للمعايير الأمنية.

أهمية البحث للمستقبل

تقدم هذه الدراسة إسهامًا مهمًا في فهم العلاقة بين إدارة مخاطر الأمن السيبراني والاستقرار المالي والشمول المالي في البنوك. تعتبر النتائج والتوصيات المقدمة ذات قيمة للبنوك والمشرعين وصناع السياسات، حيث تساهم في تعزيز الأمن السيبراني ودعم الاستقرار المالي في القطاع المصرفي. يمكن استخدام هذه الدراسة كمرجع للأبحاث المستقبلية التي تتناول مواضيع مشابهة أو تسعى لتطوير استراتيجيات جديدة لتعزيز الأمن السيبراني في المؤسسات المالية.

النهاية :

في ختام هذا البحث، نؤكد على أهمية الاستثمار في تطوير وتحسين استراتيجيات إدارة مخاطر الأمن السيبراني في البنوك، ليس فقط لحماية البيانات والمعلومات الحساسة، ولكن أيضاً لدعم الاستقرار المالي وتعزيز الشمول المالي في الاقتصاد السعودي. إن تحقيق هذه الأهداف يتطلب تضافر الجهود بين البنوك والهيئات التنظيمية والعملاء لتحقيق نظام مالي آمن وموثوق به.

المراجع :

- 1) العبدلات، صدام عبدالله عبدالكريم. (2023). "أثر الأمن السيبراني في التسويق الإلكتروني في البنوك التجارية الأردنية". (رسالة ماجستير غير منشورة). جامعة العلوم الإسلامية العالمية، عمان، الأردن.
- 2) عبدالحميد، عماد الدين محمد كامل. (2021). "استراتيجية تعزيز الأمن السيبراني للاقتصاد الرقمي: دراسة في العملات الرقمية للبنوك المركزية : الحلقة الأولى". مجلة الاقتصاد الإسلامي، 41 (485)، 22-31.
- 3) حسين، رانيا موسى عبدالله. (2022). "أثر الأمن السيبراني في سمعة البنوك التجارية الأردنية" (رسالة ماجستير غير منشورة). جامعة عمان العربية، عمان، الأردن.
- 4) مطالقة، الحارث صالح أحمد. (2020). "دور إدارة الأمن السيبراني في التوعية والحد من الجرائم المالية من وجهة نظر العاملين في البنوك الأردنية" (رسالة دكتوراه غير منشورة). جامعة مؤتة، مؤتة، الأردن.
- 5) مجلة الدبلوماسية. (2018). "الأمن السيبراني : درع المملكة الوافي لحماية مصالحها الحيوية وبنيتها التحتية الرقمية". (عدد الصفحات 8-11). السعودية: وزارة الخارجية - معهد الأمير سعود الفيصل للدراسات الدبلوماسية.
- 6) حسين، أحمد سالم علي. (2024). "الأمن السيبراني القوة الرابعة وتعزيز الأمن والدفاع: البنية التحتية - الفوائد والمخاطر". مجلة الدراسات المستدامة، 6(1)، 1705-1682.
- 7) صديقي، مليكة، وبكروح، بهية. (2016). "العولمة المالية والاستقرار المالي". المجلة الجزائرية للعولمة والسياسات الاقتصادية، 7، 33-47.

- 8) كركار، مليكة. (2019). "الشمول المالي: هدف استراتيجية لتحقيق الاستقرار المالي في الجزائر". مجلة الاقتصاد والتنمية البشرية، 10(3)، 362-377.
- 9) البابلي، عمار ياسر محمد زهير. (2021). "التحديات الأمنية المعاصرة للهجمات السيبرانية". الفكر الشرطي، 30(118)، 19-83.
- 10) دليو، فضيل، وكلاء، عاطف. (2017). "الإستراتيجية الأمنية: أنواعها وتقنياتها ومتطلباتها". مجلة الباحث الاجتماعي، 13، 55-61.
- 11) الخمايسة، ليث عبدالحافظ. (2022). "درجة وعي الموظفين العاملين في مديرية التربية والتعليم في الطفيلة التعليمية بمفهوم المواطنة الرقمية". مجلة رماح للبحوث والدراسات، 71، 295-316.