وزارة التعليم العالي والبحث العلمي
جامعة كربلاء
كلية الادارة والاقتصاد
قسم العلوم المالية والمصرفية

استراتيجية المرونة السيبرانية ودورها في تعزيز ثقة المودعين

دراسة تحليلية لعينة من العاملين والمودعين في المصارف التجارية المدرجة في سوق العراق للاوراق المالية

رسالة مقدمة

إلى مجلس كلية الادارة والاقتصاد جامعة كربلاء

وهي جزء من متطلبات نيل شهادة الماجستير

في العلوم المالية والمصرفية

من قبل الطالب

عمار عبد الحسين شعلان الحسناوي

بإشراف

أ. د كمال كاظم جواد الشمري

أ. د كرار عباس متعب المسعودي

يرفعِ اللهُ الَّذين آمنوا منكم والَّذين أوتوا العِلمَ درجاتٍ. .

صدق الله العظيم

(58 المجادلة آية 11)

إقرار المشرف

اشهد أن إعداد الرسالة الموسومة (**استراتيجية المرونة السيبرانية و دورها في تعزيز ثقة المودعين**) والتي تقدم بها الطالب (**عمار عبد الحسين شعلان**) قد جرت تحت إشرافي في كلية الأدراة والاقتصاد / جامعة كربلاء وهي جزء من متطلبات نيل درجة الماجستير في العلوم المالية والمصرفية.

أ. د. كمال كاظم جواد

/ /٢٠٢٤

أ. د. كرار عباس منعب

/ /٢٠٢٤

توصية رئيس القسم

بناء على توصية الاستاذ المشرف ارشح هذه الرسالة للمناقشة .

أ.د. علي أحمد فارس

رئيس قسم العلوم المالية والمصرفية

/ /٢٠٢٤

اقرار لجنة المناقشة

نشهد بأننا اعضاء لجنة المناقشة، الموقعون أدناه أطلعنا على الرسالة الموسومة ب (**استراتيجية المرونة السيبرانية و دورها في تعزيز ثقة المودعين**) وقد ناقشنا الطالب (**عمار عبد الحسين شعلان**) في محتوياتها وفيما له علاقة بها، وجدنا بأنها جديرة لنيل درجة الماجستير في العلوم المالية والمصرفية بتقدير (جيد جداً)

رئيساً

أ. د. زينب مكي محمود

كلية الادارة والاقتصاد – جامعة كربلا

عضوا

أ.م.د. نور صلاح عبد النبي

كلية الإدارة والاقتصاد – جامعة كربلاء

عضوا

أ.م.د. سجاد محمد عطية

كلية الإدارة والاقتصاد – جامعة الكوفة

عضوا ومشرفا

أ. د. كمال كاظم جواد

كلية الإدارة والاقتصاد – جامعة كربلاء

عضوا ومشرفا

أ.د. كرار عباس متعب

كلية الإدارة والاقتصاد – جامعة كربلاء

اقرار رئيس لجنة الدراسات العليا

بناءا على اقرار المقوم العلمي والخبير اللغوي لرسالة الماجستير / قسم / العلوم المالية والمصرفية للطالب (**عمار عبد الحسين شعلان**) الموسومة ب(**استراتيجية المرونة السيبرانية و دورها في تعزيز ثقة المودعين**) ارشح هذه الرسالة للمناقشة .

أ.د. علي أحمد فارس

رئيس لجنة الدراسات العليا

معاون العميد للشؤون العلمية والدراسات العليا

مصادقة مجلس الكلية

صادق مجلس كلية الأدارة والاقتصاد / جامعة كربلاء على توصية لجنة المناقشة.

أ.م .د. هاشم جبار حسين الحسيني

عميد كلية الأدارة والاقتصاد

الاهداء

بسم الله الرحمن الرحيم

الهي لا يطيب الليل الا بشكرك ولا يطيب النهار الا بطاعتك. ولا تطيب اللحظات الا بذكرك. ولا تطيب الاخرة الا بعفوك. ولا تطيب الجنة الا برؤيتك ...الله جل جلالة

الى من كلله الله بالهيبة والوقار.. علمني العطاء بدون انتظار

احمل اسمه بكل افتخار.. ارجو الله ان يمد في عمرك لترى الثمار قد حان

قطافها بعد طول انتظار وستبقى كلماتك نجوم يهتدي بها اليوم وفي الغد والى الابد.

والدي الحبيب....

الى ملاكي في الحياة.. الى معنى الحب والحنان والتفاني.. بسمة الحياة

وسر الوجود التي كان دعاؤها سر نجاحي وحنانها بلسم جراحي..

امي الحبيبة ....

الى توأم روحي ورفيقة دربي في هذه الحياة، معك أكون انا وبدونك أكون

مثل أي شيء... أرى التفاؤل بعينها والسعادة في محياها..

زوجتي العزيزة ....

الى من رافقاني منذ ان حملنا حقائب صغيرة ومعكم سرت الدرب خطوة

بخطوة ومازلتم ترافقوني حتى الان.. يا شمعة متقدة تنير ظلمة حياتي

اخوتي واخواتي .....

الى فلذات كبدي شموع الامل وقناديل المستقبل..

أطفالي الأعزاء

الى كل من علمني حرفاً، واخذ بيدي في سبيل تحصيل العلم، والمعرفة

إليهم جميعا اهدي ثمرة جهدي، ونتاج بحثي المتواضع.

الباحث

شكر وتقدير

بسم الله نبدأ واليه ننتهي وعليه نعول فيما نرتجي، ونستهل بالحمد لله الذي ليس لقضائه دافع ولا لعطائه مانع ولا كصنعه صانع وهو الجواد الواسع، والسلام على من خصه بالنبوة سيد الأنام أبي القاسم محمد صلى الله عليه وآلة وسلم وعلى آله الطيبين الطاهرين وصحبه المنتجين الأخيار.

أما وقد وفقني الله عز وجل لإنجاز هذه الرسالة فأنه لمن دواعي الوفاء والإقرار بالجميل أن أسجل شكري وعرفاني وعظيم امتناني لاستاذي كل من **أ.د كمال كاظم جواد الشمري** و**أ.د كرار عباس متعب السعودي** الذين اشرفوا على اكمال هذه الرسالة، والذين أغدقوا على الكثير من علمهم ، فما من رأي سديد أبدوه، وملاحظة قيمة أشارو بها إلا وكانت الموجه للباحث في مسار البحث العلمي الصحيح، إن الكلمات لتعجز عن الوفاء بحق المشرفين الافاضل الذين كانت لمساتهم ومنهجيتهم و علميتهم أثر بارز في إخراج هذه الرسالة بهذه الصورة، فجزاهم الله عني خير الجزاء وأطال الله في عمرهم وجعلهم ذخراً.

ويشرفني أن أتقدم بفائق شكري وتقديري إلى السيد عميد كلية الإدارة والاقتصاد جامعة كربلاء **أ.د هاشم الحسيني** لروحه الطيبة وخلقه الرفيع واهتمامه البالغ بطلبة الدراسات العليا، والشكر موصول الى المعاون العلمي ورئيس قسم العلوم المالية والمصرفية **أ.د علي احمد فارس** لرعايتة واهتمامه بطلبة الدراسات العليا، كذلك اتوجه بالشكر الجزيل لرعايته العلمية واهتمامه الكبير بطلبة الدراسات العليا في القسم وتذليله كل الصعاب والمعوقات التي يوجهونها، وفقه الله وجزاه خيراً.

وان واجب العرفان يملي على الباحث ان يتقدم بالشكر والامتنان للسادة رئيس واعضاء لجنة المناقشة المحترمين لقبولهم مناقشة رسالتي فجزاهم الله خير الجزاء.. واتقدم بشكري وتقديري الى المقوم اللغوي والعلمي على جهودهم المبذولة.

واتقدم بالشكر والعرفان الى رئيس قسم مدينة الامام الحسين عليه السلام **السيد صادق سلطان ثامر** والأستاذ **وائل حمزة وحيد** معاون رئيس القسم لرعايتهم واهتمامهم بنا طول مدة الدراسة فلهم منا كل الشكر والتقدير وأقدم شكري وتقديري الى جميع أساتذة قسم العلوم المالية والمصرفية في كلية الإدارة والاقتصاد لما بذلوه من جهد في سبيل الارتقاء بالواقع العلمي للكلية، كما وأقدم شكري وامتناني لزملائي وزميلاتي لتعاونهم الكبير معي خلال مدة الدراسة، وأخيراً أتقدم بجزيل شكري وتقديري لوالديَ العزيزين ولزوجتي ولأخوتي وأخواتي لمساعدتهم لي على الاستمرار والعطاء وتهيئة الظروف المناسبة للمثابرة في إتمام مسيرتي العلمية.

الباحث

المستخلص:

هدفت الدراسة إلى بيان تاثير استراتيجية المرونة السيبرانية بأبعادها الفرعية ودورها في تعزيز ثقة المودعين بأبعادها، ومدى تمتع المصارف عينة الدراسة باستراتيجية المرونة السيبرانية من عدمها ومدى صلة هذه الاستراتيجية بتجاوز المخاطر والتهديدات والتكييف معها لتعزيز ثقة المودعين بالقطاع المصرفي لاسيما التعاملات الالكترونية منها.

وانطلقت هذه الدراسة من ما يعانيه القطاع المصرفي بابتعاده عن تأثيره الحيوي في تحفيز النشاط الاقتصادي باستخدام التكنلوجيا الكترونية في العراق فضلاً عن عدم استجابته للأزمات المالية والاقتصادية الداخلية او الخارجية وهو ما كان واضحا في السنوات الماضية وجاءت مشكلة الدراسة لبيان العلاقة بين استراتيجية المرونة السيبرانية وثقة المودعين في المصارف، ومن هنا استوجب التركيز في مدى تمتع هذه المصارف باستراتيجية ألمرونة السيبرانية من عدمها، وكيف يمكن للمصارف التجارية ان تستفيد من هذه الاستراتيجيات لتعزيز ثقة المودعين في ظل التهديدات السيبرانية المتزايدة.

وتم تحليل هذة الدراسة بأخذ عينة من العاملين والمودعين في ستة مصارف تجارية أذ اختيرت هذه المصارف لاهميتها الكبيرة ولانها تقدم مجموعة من التعاملات والتعاملات الالكترونية، وهي توفرالبيئة الملائمة لمعرفة ودراسة العلاقة بين تطبيق استراتيجية المرونة السيبرانية ودورها في تعزيز ثقة المودعين من خلال العمل المصرفي الالكتروني.

وتوصل الباحث الى ان استراتيجية المرونة السيبرانية تعمل على تعزيز ثقة المودعين عبر توفير السلامة والأمان والاستجابة للتهديدات الإلكترونية والتكيف معها والحد من التعرض للمخاطر او الهجمات السيبرانية من خلال التعاملات الكترونية في القطاع المصرفي، واختتم الباحث الدراسة بمجموعة من التوصيات من اهمها وضع خطة لاستراتيجية المرونة السيبرانية وتنفذ على مراحل الهدف منها الاستمرار بتطوير البنية التحتية للأمن السيبراني وحماية البيانات بمستوياتها كافة على وفق أحدث التقنيات والتكنولوجيا المتطورة والمعتمدة في التعاملات المصرفية الالكترونية.

الكلمات الرئيسية: استراتيجية المرونة السيبرانية، ثقة المودعين، التعاملات المصرفية الكترونية، المصارف التجارية.

قائمة المحتويات

قائمة الجداول

قائمة الاشكال

المقدمة:

يعد القطاع المصرفي والمالي قطاعا كبيراً يضم عدداً كبيراً من الزبائن حول العالم، واستمرت إمكانية وصول التعاملات المصرفيةإلى الفئات الأضعف أو الأكثر ضعفا في المجتمع، ووفقا لقاعدة بيانات فينديكس غلوب لعام 2017 فقد وجد أن هناك 1.2 مليار شخص بالغ لديهم حسابات مصرفية, فضلاً عن ذلك فقد لوحظ أن معظم البلدان التي تتحول إلى النهج الرقمي حوالي 51% يفضلون القنوات المصرفية عبر الإنترنت، بينما 26% يصلون إلى الخدمات من المواقع الإلكترونية للمصارف ويستخدمون التعاملات المصرفيةعبر الهاتف المحمول، ولقد أتاح التطور المذهل الذي شهدته صناعة التقنيات المالية الكثير من الفرص أمام المصارف نحو تعزيز مستوى ثقة المودعين من خلال قنوات جديدة ومبتكرة بعيداً عن القنوات التقليدية التي اعتادت عليها المصارف في التعاملات المصرفية.

ومن هنا جاء دوراستراتيجية المرونة السّيبرانية المتمثل بالاستعداد الوقائي لمواجهة التهديدات ألسيبرانية والتعافي السريع من آثارها ويحضرللهجمات السيبرانية المحتملة عبر التحليل الاستباقي لنقاط الضعف في جميع مستويات البيئة الرقميّة لتعزيز ثقة المودعين، وهذا مايمثل مشكلة الدراسة الذي يساهم في الحد من حجم الأضرار المادية والمعنوية للموسسات المالية المختلفة لاسيما القطاع المصرفي، وبتالي تعمل هذة الاستراتيجيات على تعزيز ثقة المودعين بالقطاع المصرفي في ظل التهديدات السيبرانية المتزايدة.

وقسمت الدراسة الى اربعة فصول تضمن الفصل الاول منهجية الدراسة كمبحث اول فيما خصص المبحث الثاني منه الى بعض الدراسات السابقة العربية والاجنبية الخاصة بمتغيرات الدراسة، اما الفصل الثاني فقد تضمن الاطار النظري للدراسة وقسم الى مبحثين خصص الاول منه الى استراتيجية المرونة السيبرانية فيما اهتم الثاني بثقة المودعين، في حين جاء الجانب العملي للدراسة في الفصل الثالث أذاهتم المبحث الاول بواقع الخدمات الالكترونية في العراق ومؤشراتها، اما المبحث الثاني فقد خصص لاختبار اداة الدراسة وبياناتها بينما خصص المبحث الثالث الى عرض نتائج الدراسة وتحليلها وتفسيرها واخيراً تناول المبحث الرابع اختبار فرضيات الدراسة، واختتمت الدراسة بالفصل الرابع الخاص بالاستنتاجات والتوصيات

الفصل الاول:

المنهجية العلمية للدراسة وبعض الدراسات السابقة

المبحث الاول:
المنهجية العلمية للدراسة

المبحث الثاني:
بعض الدراسات السابقة

"المبحث الاول"
المنهجية العلمية الدراسة

توطئة:

يتناول هذه المبحث منهجية الدراسة الحالية متمثلة بـ (مشكلة الدراسة، اهمية الدراسة، اهداف الدراسة، فرضيات الدراسة، مجتمع وعينة الدراسة، متعيرات الدراسة، وسائل جمع المعلومات والبيانات، الوسائل الاحصائية المستخدمة والمخطط الفرضي للدراسة).

أولاً: – مشكلة الدراسة:

يعاني القطاع المصرفي بابتعاده عن تأثيره الحيوي في تحفيز النشاط الاقتصادي باستخدام التكنلوجيا الكترونية في العراق فضلاً عن عدم استجابته للأزمات المالية والاقتصادية الداخلية او الخارجية وهو ما كان واضحا في السنوات القليلة الماضية خصوصا في ازمة جائحة كوفيد- 19 الذي استوجب التركيز في مدى تمتع هذه المصارف باستراتيجية المرونة السيبرانية من عدمها ومدى صلة هذه المرونة بتجاوزالازمات والتهديدات والتكييف معها لتعزيز ثقة المودعين بالقطاع المصرفي، وهل ان اسباب عدم الاستجابة هوانخفاض في تطبيق استراتيجيات المرونة السيبرانية لتلك المصارف ام عوامل اخرى لها علاقة بحوكمة وأتمتت الانظمة التي تستخدمها المصارف في تعاملاتها الالكترونية او قلة البحوث والدراسات الاكاديمية في هذا المجال.

تتمثل مشكلة الدراسة في طرح السؤال الآتي الذي يمثل اشكالية الدراسة:-

هل هنالك دور لاستراتيجية المرونة السيبرانية في تعزيز ثقة المودعين؟

من الاشكالية الرئيسة هناك مجموعة من التساؤلات الفرعية التي تصاغ على النحو الآتي:-

1. ماهي استراتيجية المرونة السيبرانية وماهي استخداماتها في القطاع المصرفي؟
2. كيف تختلف استراتيجية المرونة السيبرانية عن الامن السيبراني؟
3. ماهي العلاقة بين مستوى استراتيجية المرونة السيبرانية وثقة المودعين في المصارف؟
4. ماهي العوامل والمخاطر التي تؤثر على ثقة المودعين في المصارف ؟
5. كيف يمكن قياس مستوى ثقة المودعين في المصارف ؟
6. ماهي التحديات التي تواجة المصارف في تنفيذ استراتيجية المرونة السيبرانية التي تعزز ثقة المودعين.

ثانياً: – أهمية الدراسة:

تبرز أهمية الدراسة في الجانب النظري والعملي (التطبيقي) من النقاط الاتية:

أ – الأهمية النظرية للدراسة:

1- توسيع آفاق المعرفة: تساهم الدراسة في توسيع نطاق المعرفة النظرية حول العلاقة المعقدة بين الأمن السيبراني، واسترتيجية المرونة السيبرانية، وثقة المودعين، خاصة في سياق المصارف التجارية.

2- بناء النظريات: تساعد في بناء نظريات جديدة أو تطوير النظريات القائمة حول إدارة المخاطر السيبرانية، سلوك المودعين، وتأثير العوامل التنظيمية على المصارف.

3 - توفير إطار تحليلي: تقدم إطارا تحليليا متيناً يمكن للباحثين استخدامه لدراسة ظواهر مشابهة في مجالات أخرى.

4- إثراء المكتبة العلمية: تضيف قيمة مضافة للمكتبة العلمية من خلال تقديم نتائج أصلية وبحثية حديثة وتوفر الدراسة أسئلة بحثية جديدة، منهجيات بحثية متطورة، وقاعدة بيانات غنية يمكن الاستفادة منها في أبحاث مستقبلية.

ب – الأهمية التطبيقية للدراسة:

1- تحسين أداء المصارف: تساعد الدراسة المصارف التجارية على فهم نقاط قوتها وضعفها في مجال الأمن السيبراني من خلال تطبيق استراتيجيات المرونة السيبرانية، مما يتيح لها اتخاذ قرارات استثمارية أفضل وتحسين عملياتها.

2- تعزيز الثقة المودعين: تساهم في تعزيز ثقة المودعين في المصارف التجارية من خلال إظهار التزامها بتطبيق استراتيجيات المرونة السيبرانية.

3- استخدام استراتيجيات جديدة :تساعد المصارف على تطوير استراتيجيات أكثر فعالية لإدارة المخاطر السيبرانية وتعزيزمرونة النظام المعتمد في المصارف التجارية.

4- في ميدان الدراسة: يساهم في تطوير المعرفة في مجال إدارة المخاطر وتطبيق ابعاد استراتيجية المرونة السيبراني ، وسلوك المودعين.

تكتسب هذه الدراسة اهميتها من اهمية وحداثة موضوع الدراسة في المجتمع بشكل عام وفي القطاع المصرفي بشكل خاص بغية الاعتماد على تطبيق استراتيجية المرونة السيبرانية التي يتم من خلالها الاستعداد والتخطيط للأحداث والمخاطر السيبرانية واستيعابها والتعافي منها والتكيف معها بنجاح أكبر في ظل التهديدات السيبرانية المتزايدة.

ثالثاً: – أهداف الدراسة:

تهدف الدراسة بشكل اساسي الى مایاتي:

تهدف الرسالة بشكل أساسي إلى فهم العلاقة والدور بين استراتيجية المرونة السيبرانية وبين مستوى تعزيز ثقة المودعين في المصارف التجارية، و كيف تساهم استراتيجية المرونة السيبرانية في زيادة ثقة المودعين في المصارف التجارية؟

بالاضافة الى هنالك مجموعة من ألأهداف الفرعية التي تتضمنها الدراسة والتي تشمل:

1- تحديد الابعاد الأساسية التي تشكل استراتيجية مرونة سيبرانية فعالة في القطاع المصرفي.

2- قياس تأثير مختلف ابعاد استراتيجية المرونة السيبرانية على مستوى ثقة المودعين.

3- تحديد العوامل الأخرى التي تؤثرعلى ثقة المودعين بالإضافة إلى استراتيجية المرونة السيبرانية.

4- مقارنة مستوى استراتيجية المرونة السيبرانية وثقة المودعين بين مختلف المصارف.

5- تهدف الدراسة ولأول مرة على صعيد الدراسات والبحوث الاكاديمية في العالم العربي والعراق خصوصا الى تبني موضوع جديد وحديث يحد ويعالج المخاطر والتهديدات والجرائم السيبرانية التي تتعرض لها المؤسسات المالية بشكل عام والمصارف بشكل خاص من تطبيق مفاهيم حديثة ومتطورة والتي تتمثل بأستراتيجية المرونة السيبرانية في العمل المصرفي.

رابعاً: – فرضيات الدراسة:

في ضوء مشكلة الدراسة فأن فرضيات الدراسة تتمثل بما يأتي:

الفرضية الرئيسه الأولى: وتنص على أنه (لا توجد علاقة ارتباط ذات دلاله معنوية بين استراتيجية المرونة السيبرانية وثقة المودعين)، ولقد تفرعت عنها خمسة فرضيات فرعية وكما هو مبين: -

1- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الحوكمة وثقة المودعين.

2- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الحماية وثقة المودعين.

3- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الاستكشاف وثقة المودعين.

4- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الاستجابة وثقة المودعين.

5- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الاستعادة والتقييم وثقة المودعين.

الفرضية الرئيسه الثانية: (لا توجد علاقة تاثير ذات دلالة معنوية لاستراتيجية المرونة السيبرانية في ثقة المودعين) ولقد تفرعت عن الفرضية الرئيسية الثانية خمس فرضيات فرعية وهي:

1- لا يوجد تاثير لبعد الحوكمة ذو دلالة معنوية في ثقة المودعين.
2- لا يوجد تاثير لبعد الحماية ذو دلالة معنوية في ثقة المودعين.
3- لا يوجد تاثير لبعد الاستكشاف ذو دلالة معنوية في ثقة المودعين.
4- لا يوجد تاثير لبعد الاستجابة ذو دلالة معنوية في ثقة المودعين.
5- لا يوجد تاثير لبعد الاستعادة والتقييم ذو دلالة في ثقة المودعين.

خامساً: - مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة من مجموعة من العاملين والمودعين لدى مجموعة من المصارف التجارية المدرجة في سوق العراق للأوراق المالية، وتتكون عينة الدراسة من العاملين والمودعين في ستة مصارف تجارية أذ اختيرت هذه المصارف لاهميتها الكبيرة ولانها تقدم مجموعة من التعاملات الالكترونية، وهي توفر البيئة الملائمة لمعرفة ودراسة العلاقة بين تطبيق استراتيجية المرونة السيبرانية وأثرها في تعزيز ثقة المودعين من خلال العمل المصرفي الالكتروني، وفيما يتعلق بمدة الدراسة فقد اعتمدت على عشرة اعوام للمدة (2013- 2022) حسب ما توفر من تقارير سنوية للمصارف عينة الدراسة، وكذلك طول مدة الدراسة من شأنه ان يعطي نتائج افضل حول العلاقة بين المتغيرات والجدول (1) يوضح المصارف عينة الدراسة ورمز كل مصرف.

جدول (1) المصارف التجارية عينة الدراسة ورموزها

ت	اسم المصرف	رمز المصرف
1	مصرف الخليج التجاري	BGUC
2	مصرف المنصور للاستثمار	BMNS
3	مصرف الموصل للتنمية والاستثمار	BMFI
4	مصرف بغداد	BBOB
5	مصرف الاهلي العراقي	BNOI
6	مصرف الشرق الأوسط العراقي للاستثمار	BIME

سادساً: - متغيرات الدراسة:

المتغير المستقل: المتمثل باستراتيجية المرونة السيبرانية والتي تشتمل على الابعاد الاتية (الحوكمة، الحماية، الاكتشاف، الاستجابة، الاستعادة والتقييم).

المتغير التابع: المتمثل بثقة المودعين والتي تشتمل على الابعاد الاتية (الكفاءة والقدرة، المنفعة، الامان).

سابعاً: – وسائل جمع المعلومات والبيانات:

جمعت البيانات والمعلومات المهمة لاتمام هذة الدراسة بطرقتين:-

1- الجانب النظري:

اعتمدت الدراسة على الادبيات من المراجع والكتب العلمية الحديثة والعربية والدولية والرسائل وألاطاريح والمقالات التي تحكم المعلومات اللازمة من الانترنت والمكتبات.

2- الجانب العملي:

اعتمدت الدراسة على الاستبانة التي تعد مصدراً هاماً للحصول على البيانات ذات الصلة بموضوع الدراسة وقد وزعت 67 استبانة على عدد من المدراء ومسؤولي الشعب التنفيذيين ومعاونيهم فضلاً عن عدد من الموظفين في المصارف التجارية عينة الدراسة، كما وزعت 202 استبانة على عدد المودعين المتعاملين مع المصارف التجارية عينة الدراسة.

كما رفدت الدراسة بمجموعة من المؤشرات والتقارير السنوية لكل مصرف من المصارف عينة الدراسة للمقارنة مع نتائج الاستبيان عبر سلسلة زمنية للمدة الممتدة من عام 2013 لغاية عام 2022 لإسناد وتقوية الدراسة كون التعاملات المصرفية الالكترونية تعتبر العمود الفقري للعمليات المصرفية الحديثة، ومن جهة المخاطر تعتبر هدفا رئيسياً للهجمات السيبرانية، اما من جهة الارتباط المباشر بثقة المودعين فأن جودتها وسلامتها بشكل مباشر تؤثر على تعزيز ثقة المودعين، فضلاً عن التطورات التكنولوجية المستمرة وهذا يجعل طبيعة المجال ديناميكيا ويتطلب دراسة مستمرة في ظل التهديدات السيبرانية المتزايدة، بالاضافة الى تطور حجم الودائع ومعرفة سلوك المودعين وثقتهم في تلك المصارف، ولهذا تم اخذ مجموعة من المؤشرات التي تخص التعاملات المصرفية الالكترونية وتمثلت المؤشرات بالاتي:

1- عدد اجهزة الصراف الالي.
2- عدد البطاقات الالكترونية.
3- عدد المصارف المراسلة.
4- حجم الودائع المصرفية .

ثامناً: – الوسائل الاحصائية المستخدمة:

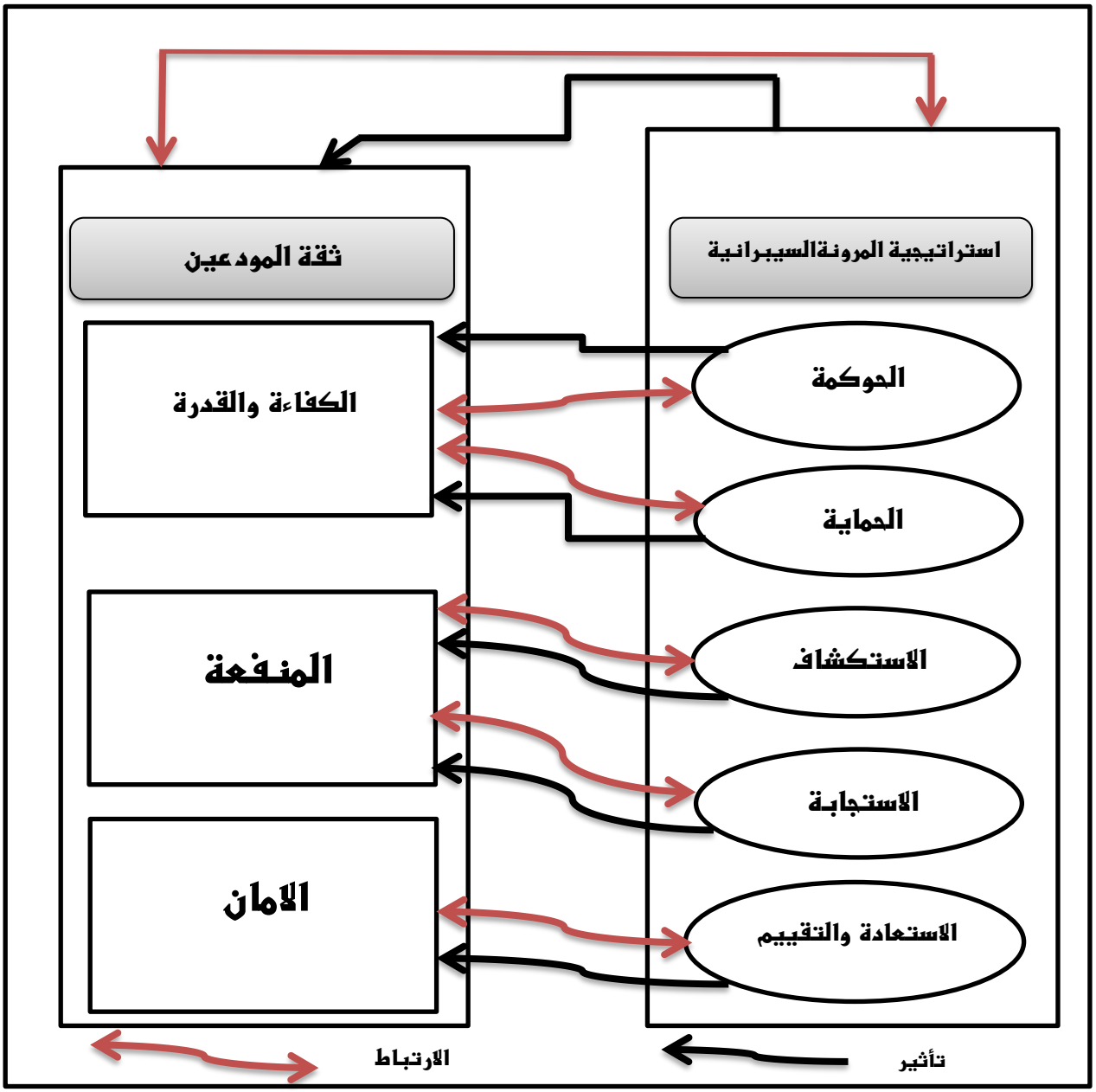
تعتمد منهجية الدراسة المنهج الوصفي والتحليلي كونه أكثر ملائمة لطبيعة الدراسة ومجالها وأهدافها واستعين بعدد من البرامج الإحصائية لاجراء تحليل العلاقة ودورها بين متغيرات الدراسة واختبار الفرضيات: 1- برنامج اوفيس Excel.

1- البرنامج الاحصائي (spss). 3 - البرنامج الاحصائي (AMOS,24).

تاسعاً: – المخطط الفرضي للدراسة

أعد مخطط إجرائي للدراسة يصور حركة متغيرات الدراسة، والشكل (1) يوضح ذلك من خلال المتغير المستقل المتمثل بأستراتيجية المرونة السيبرانية والتي تشتمل على الابعاد الاتية:

(الحوكمة، الحماية، الاكتشاف، الاستجابة، الاستعادة والتقييم)، والمتغير التابع المتمثل بثقة المودعين والذي يشتمل على الابعاد الاتية (الكفاءة والقدرة، المنفعة، الامان) وحسب مامبين من المخطط:



شكل (1) المخطط الفرضي للدراسة

المصدر: من اعداد الباحث بالاعتماد على الادبيات السابقة.

بعض الدراسات السابقة

توطئة:

يهدف هذا المبحث إلى عرض موجز لبعض من الدراسات السابقة التي تناولت متغيرات الدراسة الحالية (استراتيجية المرونة السيبرانية ودورها في تعزيز ثقة المودعين) أذ تعد هذه الدراسات ذات اهمية كبيرة لانها توفر معلومات مهمة حول متغيرات الدراسة، وتعد الدراسات السابقة مصدرا رئيسا يسهم في تطوير الجهود البحثية للدراسات العلمية وبلورتها، لاسيما عندما تنطلق هذه الدراسة من نقطة انتهاء البحوث والدراسات الخاصة بالموضوع في سلسلة تكميلية لها لا تتضمن التكرار، وقد اعتمد الباحث على تلك الدراسات من اجل اثراء الدراسة الحالية بالحقائق العلمية، لاسيما ان هذه الدراسة تعد بهذا العنوان هي من اول الدراسات المتقدمة لبحث استراتيجية المرونة السيبرانية ودورها في تعزيز ثقة المودعين بالقطاع المصرفي و فيما يأتي نستعرض بعض الدراسات السابقة وهي كالاتي :

أولاً: – بعض الدراسات السابقة العربية والاجنبية المتعلقة باستراتيجية المرونة السيبرانية:

1- **دراسة: – عبد القادر واخرون:** 2023	
عنوان الدراسة	أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية بتقليل المخاطر المدركة.
عينة الدراسة	عينة البحث مكونة من 127 من عملاء بنك التنمية المحلية.
هدف الدراسية	تهدف الدراسة إلى تسليط الضوء على أثر جاهزية البيئة المادية والبشرية للأمن السيبراني على استخدام الخدمات المصرفية الإلكترونية بتقليل المخاطر المدركة لدى عينة من عملاء بنك التنمية المحلية.
الاساليب الإحصائية	استخدم نموذج تحليل المسار لاختبار الأثر المباشر وغير المباشر لمتغيرات الدراسة واختبار صلاحية وصدق وثبات نموذج الدراسة باستخدام البرنامج الاحصائي SPSS.
نتائج الدراسة	توصلت الدراسة إلى وجود علاقة تأثير غير مباشرة لبعدي جاهزية البيئة المادية والبشرية للأمن السيبراني في استخدام الخدمات المصرفية الإلكترونية بتقليل المخاطر المدركة للعملاء.

2- **دراسة: –** Melenchuk: 2017	
عنوان الدراسة	Is Ukraine cyber resilient? هل تتمتع أوكرانيا بالمرونة السيبرانية؟
عينة الدراسة	اعتمدت عينة الدراسة على عدد التهديدات والهجوم السيبراني و كانت أوكرانيا هدفًا لـ (7000) هجوم إلكتروني استهدف البنية التحتية الحيوية للدولة
هدف الدراسية	لمعرفة ما إذا كانت السياسة الوطنية لأوكرانيا في المجال السيبراني تتوافق مع مفهوم المرونة السيبرانية وتحديد التحديات الرئيسه التي تواجه توفير المرونة السيبرانية في البلاد.
الاساليب الإحصائية	استخدام نهج قائم على الحالة للاستدلال السببي الذي يركز على استخدام القرائن داخل الحالة (ملاحظات العملية السببية (CPOs).
نتائج الدراسة	توصلت الدراسة الى تحديد أكبر المخاطر والتهديدات التي تواجه المرونة السيبرانية على المستوى الوطني بشكل أفضل.
3- **دراسة: –** Mayunga: 2019	
عنوان الدراسة	Develop and Assessing Cyber Resilience Framework for Kenyan Banks. تطوير وتقييم إطار المرونة السيبرانية للمصارف الكينية.
عينة الدراسة	اختيرت عينة مكونة من أربعين مصرفاً من أصل أربعة وأربعين مصرفاً محتملاً في كينيا باستخدام عينات عشوائية بسيطة.
هدف الدراسية	يتمثل الهدف الرئيسي في جمع مؤشرات قياس أفضل الممارسات ووضع إطار محلي لقياس المرونة السيبرانية في المصارف الكينية، وثم استخدام الإطار لتقييم قوة المرونة السيبرانية لدى المصارف.
الاساليب الإحصائية	استخدمت الننهج الوصفي معززة بالتقنيات الكمية لقياس المتغيرات باستخدام البرنامج الاحصائي SPSS.
نتائج الدراسة	ينبغي لجميع المصارف أن تولي مزيداً من التركيز للمرونة السيبرانية لضمان السلامة السيبرانية على كل مستوى، وان وجود إطار مشترك للمرونة السيبرانية أمرا ضروريا لتنسيق تقييم المرونة السيبرانية.

4- **دراسة:** – Loonam et al : 2020	
عنوان الدراسة	Cyber resilience for digital enterprises: A strategic leadership. المرونة السيبرانية للمؤسسات الرقمية: قيادة استراتيجية.
عينة الدراسة	تم اخذ عينة من (100) شخص لإجراء مقابلات معهم في جميع أنحاء المملكة المتحدة وإيرلندا بالاضافة الى مقابلة (8) من كبار الرؤساء التنفيذيين للمؤسسات الرقمية.
هدف الدراسية	تعزيز ثقافة المرونة السيبرانية للموظفين وتوسيع نطاقها والاهتمام بأصحاب المصلحة التنظيميون بتطوير ثقافتهم بالثقة للتغلب على التهديدات السيبرانية.
الاساليب الإحصائية	المنهج الاستكشافي جمع المعلومات بالمقابلة والملاحظة باستخدام البرنامج الاحصائي SPSS.
نتائج الدراسة	توصلت الدراسة الى اهمية ضمان الاتي: 1- توافق الاستراتيجية السيبرانية مع استراتيجية العمل في المؤسسة مع ضمان وجود الحكومة واعداد التقارير الدورية لرئيس العمل. 2- تعزيز ثقافة الثقة في جميع أنحاء المؤسسة حيث تصبح المرونة السيبرانية جزءاً من سلوك الموظفين والفريق.
5- **دراسة:** – Kasanga: 2021	
عنوان الدراسة	Outcome of techniques Employed for cyber resilience by ommercial banks in Kenya. نتائج التقنيات المستخدمة من أجل المرونة السيبرانية من قبل المصارف التجارية في كينيا.
عينة الدراسة	اخذت عينة من (39) من مدراء المصارف التجارية في كينيا الذين يعملون في اقسام تكنولوجيا المعلومات في المصارف.
هدف الدراسية	اولا: تقييم التقنيات التي تعتمدها المصارف التجارية في كينيا. ثانيا: تقييم العلاقة بين التقنيات المعتمدة ومستوى المرونة السيبرانية في المصارف التجارية في كينيا.

الاساليب الإحصائية	استخدمت المنهج الوصفي التحليلي في الدراسة ومجموعة من الأدوات الرياضية والكمية باستخدام البرنامج الاحصائي SPSS.
نتائج الدراسة	توصلت الدراسة الى ان تقنيات المرونة السيبرانية كان لها الاثر الكبير والايجابي على المرونة السيبرانية في المصارف التجارية الكينية.
6- **دراسة: –** Al-Hidaifi et al: 2024	
عنوان الدراسة	A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions دراسة استقصائية حول المرونة السيبرانية: الاستراتيجيات الرئيسه وتحديات البحث والاتجاهات المستقبلية.
عينة الدراسة	اسكتلندة.
هدف الدراسية	الهدف الرئيسي من هذه الدراسة هو فهم استراتيجيات المرونة السيبرانية والقضايا الحرجة ذات الصلة.
الاساليب الإحصائية	اعتمدت هذه الدراسة على الاسلوب الاستقصائي في مراجعة الأدبيات للأطر والاستراتيجيات والتطبيقات والأدوات والتقنيات الخاصة بتعزيز استراتيجية المرونة السيبرانية.
نتائج الدراسة	سلط الضوء على العديد من التوجهات البحثية المستقبلية والأبحاث والمشاكل لتوجيه دعوة للعمل من أجل تحسين المرونة السيبرانية.

ثانيا: – بعض الدراسات السابقة العربية والاجنبية المتعلقة بثقة المودعين:

1- **دراسة:– ماجدة:** 2021	
عنوان الدراسة	العوامل المؤثرة على ثقة العملاء في التعاملات المصرفية الالكترونية - دراسة حالة المصارف الجزائرية.
عينة الدراسة	تتكون عينة الدراسة من (154) من العملاء في المصارف الجزائرية.
هدف الدراسية	تهدف الدراسة إلى معرفة خصائص التعاملات المصرفية الالكترونية المقدمة من طرف المصرف الوطني الجزائري ومدى تلبيتها لرغبات وتطلعات المستفيدين منها وكذلك معرفة العلاقة الارتباطية والتأثيرية لخصائص التعاملات المصرفية الالكترونية على تعزيز العلاقة مع الزبون.
الاساليب الإحصائية	استخدم المنهج الوصفي التحليلي في الدراسة ومجموعة من الأدوات الرياضية والكمية باستخدام برنامج التحليل الاحصائي (AMOS)،SPSS .
نتائج الدراسة	توصلت الدراسة إلى أن كل من خصائص الخدمة المتمثلة في السرية والأمان وسهولة الاستخدام وخصائص المصرف المتمثلة في الحجم والسمعة وخصائص المستهلك المتمثلة في التجارب السابقة والكفاءة في استخدام الحاسب الآلي تؤثر على ثقة العملاء في التعاملات المصرفية الالكترونية في الجزائر.
2- **دراسة: – عبد العزيز:** 2022	
عنوان الدراسة	دور الموبايل المصرفي في تعزيز مستوى ثقة العملاء في التعاملات المصرفية الالكترونية.
عينة الدراسة	اعتمدت الدراسة على عينة عمدية متاحة من مستخدمي الموبايل المصرفي قوامها 250 من الزبائن.

هدف الدراسية	تهدف هذه الدراسة الى التعرف على دور الموبايل المصرفي في تعزيز ثقة العملاء بالتعاملات المصرفية الالكترونية.
الاساليب الإحصائية	استخدم المنهج الوصفي التحليلي في الدراسة ومجموعة من الأدوات الرياضية والكمية من برنامج التحليل الاحصائي SPSS.
نتائج الدراسة	توصلت الدراسة الى وجود فروق ذات دلالة إحصائية بين الخصائص الديموغرافية للمبحوثين والثقة الإلكترونية في المؤسسات المصرفية.
3- **دراسة: – بسمة وعفاف:** 2023	
عنوان الدراسة	أثر ثقة العملاء على تبني التعاملات المصرفية الالكترونية في المصارف التجارية الجزائرية.
عينة الدراسة	اخذت عينة من الزبائن تبلغ (150) من مصرف الفلاحة والتنمية الريفية في الجزائر.
هدف الدراسية	التعرف على اهم محددات وقنوات الخدمة المصرفية الالكترونية وكذلك معرفة ان كان هنالك أثر لثقة العملاء على تبني التعاملات المصرفية الالكترونية المقدمة من طرف بنك الفلاحة والتنمية الريفية.
الاساليب الإحصائية	استخدم المنهج الوصفي التحليلي في الدراسة ومجموعة من الأدوات الرياضية والكمية من برنامج التحليل الاحصائي SPSS.
نتائج الدراسة	أظهرت نتائج الدراسة صحة وقبول الفرضيات التي تم صيغت، كما توصلئ إلى ان ابعاد الكفاءة والمنفعة والامان لها تأثير على تبني التعاملات المصرفية الالكترونية، مما نستنتج ان هنالك تأثير لثقة العملاء على تبني التعاملات المصرفية الالكترونية في المصارف التجارية الجزائرية.

4- **دراسة: –** Herzallah et al : 2018	
عنوان الدراسة	The Impact of customer Trust and perception of Security and Privacy on The Acceptance of Online Banking: Sstructural Equation Modeling Approach. تأثير ثقة العملاء ومفهوم الأمن والخصوصية على قبول التعاملات المصرفيةعبر الإنترنت: نهج نمذجة المعادلات الهيكلية.
عينة الدراسة	اجري استطلاع على عينة تبلغ (198) عميلاً في المصارف الاردنية.
هدف الدراسية	هدفت الدراسة إلى معرفة تأثير تصورات الأمن والخصوصية على ثقة العملاء في قبول واعتماد التعاملات المصرفيةعبر الإنترنت.
الاساليب الإحصائية	استخدمت الحزمة الاحصائية لبرنامج SPSS.
نتائج الدراسة	أظهرت النتائج ان الثقة لها أثر إيجابا على نية العملاء السلوكية لتبني التعاملات المصرفيةعبر الإنترنت.
5- **دراسة: –** Andersen: 2019	
عنوان الدراسة	Trust in Online financial Services: A Research on the formation of Trust Formation in financial Firms in the Digital Age. الثقة في الخدمات المالية عبر الإنترنت: بحث حول تكوين الثقة في المؤسسات المالية والمصارف في العصر الرقمي.
عينة الدراسة	تم توزيع الاستبيان على (39) من الذين يستخدمون Facebook وLinkedIn وInstagram .
هدف الدراسية	الهدف العام من الأطروحة يشكل استكشاف عوامل بناء الثقة المالية عبر الإنترنت.

الاساليب الإحصائية	اجريت طريقة استكشافية مختلفة تقريباً لدراسة مستهلكي التجزئة المالية باستخدام ثلاث مقابلات مع مجموعات التركيز للوصول إلى النتائج من استبيان عبر الإنترنت.
نتائج الدراسة	تشير النتائج إلى أن الوسائل الأساسية التي حددت يمكن أن تزيد من ثقة المستهلكين بمعتقداتهم اتجاه المؤسسات المالية والمصارف، وعلى هذا الأساس يقترح على المؤسسات المالية والمصارف زيادة ثقة المستهلكين بمعتقداتهم عن طريق باظهار الوسائل الأساسية المكتشفة للسمات المحددة عبر الإنترنت.
6- **دراسة: –** Omkar, et al : 2023	
عنوان الدراسة	Customers Trust in E-payment: The Influence of Security and Privacy. ثقة العملاء في الدفع الإلكتروني: تأثير الأمن والخصوصية.
عينة الدراسة	اعتمدت عينة الدراسة على جمع (327) عينة على أساس البحوث والدراسات التي اجريت في السابق.
هدف الدراسية	تهدف الدراسة الى معرفة تأثير تصورات الأمن والخصوصية على ثقة العملاء بين مستخدمي الدفع الرقمي وكذلك تأثير الفائدة المدركة والاستخدام المتصور على نية العملاء لاستخدام ادوات الدفع الرقمي.
الاساليب الإحصائية	استخدم تحليل المسار لاختبار الفرضيات في الدراسة من برنامج التحليل الاحصائي SPSS.
نتائج الدراسة	توصلت الدراسة الى ان المستهلكين يهتمون بخصوصيتهم أكثر من اهتمامهم بأمنهم ويشير هذا إلى أن الأفراد يشعرون بالقلق إزاء احتمال تسرب المعلومات أثناء استخدام منصة الدفع الإلكتروني، وتوصلت الدراسة الى ان الخصوصية والأمان لهما تأثيرات متطابقة تقرياً على ثقة العملاء.

ثالثاً: – مجالات الإفادة من الدراسات السابقة:

فضلاً عن ما ذكر في جداول الدراسات السابقة هناك بعض الجوانب التي رفدت الدراسة الحالية وهي كالاتي:

1- التعرف على آخر المستجدات العلمية والبحثية في مجال دراستنا الحالية.

2- بلورت الدراسات السابقة أهمية المتغيرات التي تناولتها الدراسة الحالية.

3- التعرف على منهجية الدراسات السابقة والإفادة منها في إعداد منهجية الدراسة الحالية وتصميمها.

4- الإفادة في تحديد وتعريف المفاهيم الفلسفية لمتغيرات الدراسة الحالية، وبما يمكن التأطير لها نظرياً.

5- أخذ الاطر والمعايير للتعرف على مكونات المتغيرات الرئيسة وفقرات الاستبانة.

6- تحديد الأساليب الإحصائية الأكثر ملائمة للدراسة الحالية.

7- الاهتداء إلى بعض المراجع والمصادر والبحوث التي لم يتسن للباحث معرفتها والاطلاع عليها.

رابعاً – مميزات الدراسة الحالية عن الدراسات السابقة:

1- انها جمعت بين متغيرات لم يسبق ان جمع بينها من حيث استراتيجية المرونة السيبرانية وثقة المودعين التي اعتمدت في هذه الدراسة.

2- ما يميز هذه الدراسة عن الدراسات السابقة تعتبر الدراسة هي الأولى من نوعها التي تركز على استراتيجية المرونة السيبرانية ودورها المباشر في تعزيز ثقة المودعين.

3- فتحة الدراسة باباً جديداً للبحث في مجال أمن المعلومات، حيث تربط بشكل مباشر بين الجانب التقني لاستراتيجية المرونة السيبرانية والجانب الاقتصادي والسلوكي ثقة المودعين.

4- الأهمية العملية للدراسة انها تقدم رؤى قيمة للمؤسسات المالية (المصارف) وصناع السياسات حول كيفية بناء ثقة المودعين من خلال تقديم تحليلاً شاملاً للتهديدات السيبرانية وكيفية التصدي لها.

5- تتميز دراسة استراتيجية المرونة السيبرانية في المصارف بتركيزها على التهديدات السيبرانية التي تواجه المصارف في العصر الرقمي.

6- تتميز دراسة استراتيجية المرونة السيبرانية في المصارف باعتمادها على التكنولوجيا والحلول الرقمية لتحقيق الأمان السيبراني، وهذا يمثل تطوراً عن الدراسات السابقة التي لم تولي الاهتمام الكافي لهذه الجوانب التكنولوجية.

7- تتبنى هذة الدراسة موضوع التوجة الحكومي من خلال التحول الرقمي ومواكبة التطور والحداثة في التعاملات والتعاملات الالكترونية وخصوصاً التعاملات المصرفية التي تعزز من ثقة المودعين مجال الدراسة.

الفصل الثاني:

الإطار المفاهيمي لاستراتيجية المرونة السيبرانية وثقة المودعين

المبحث الاول:
استراتيجية المرونة السيبرانية

المبحث الثاني:
ثقة المودعين بالقطاع المصرفي

"المبحث الاول"
استراتيجية المرونة السيبرانية

توطئة:

تعد استراتيجية المرونة السيبرانية أمراً بالغ الأهمية في النظام المصرفي للحماية من التهديدات السيبرانية وضمان استقرار القطاع المالي وتتضمن استراتيجية المرونة السيبرانية القدرة على تحمل الصدمات الخارجية الناجمة عن المخاطر السيبرانية والتعافي منها والتكيف معها، فضلاً عن أنها تتجاوز تدابير الأمن السيبراني التقليدي وتركز على القدرة في الاستمرار بالعمل في ظل الظروف الصعبة.

تؤدي التوقعات التنظيمية والتعاملات الإشرافية دوراً مهماً في تعزيز استراتيجية المرونة السيبرانية بالمصارف ولذلك يعد التحول النموذجي نحو استراتيجية المرونة السيبرانية ضرورياً بسبب الترابط المتزايد للأنظمة ورقمنة التعاملات المصرفية والتهديدات السيبرانية المتطورة.

اولاً – نشأة المرونة السيبرانية وتطورها التاريخي:

The historical development of cyber resilience and its origins

منذ عام 2000 وخلال الوقت الذي ركزت فيه أبحاث الأمن السيبراني على المخاطر والتهديدات التي تفرضها الأنظمة الرقمية، ظهر مفهوم القدرة على الصمود والتعافي من الهجمات السيبرانية، والمعروف أيضا باسم استراتيجية المرونة السيبرانية وفي الآونة الأخيرة اكتسب هذا المفهوم اهتماماً متزايدا بسبب جائحة كوفيد-19 والتسارع السريع للرقمنة، في حين يعترف الخبراء بالتمييز بين الأمن السيبراني والمرونة السيبرانية (Adekiya & Gawuna,2015: 46).

تعود أصول مجال الأمن السيبراني إلى سبعينيات وثمانينيات القرن العشرين، اذ أصبحت تكنولوجيا الحوسبة أكثر انتشاراً في الأعمال التجارية والحكومة والاستخدام الشخصي، وبمرور الوقت نضج هذا المجال وتكيف مع التهديدات الناشئة والتقنيات المتطورة وكان جوهر الأمن السيبراني دائماً هو تأمين الأنظمة والبيانات الرقمية من الوصول غير المصرح به أو الضرر أو التعطيل (Yost, 2015: 46).

لقد اكتسب مصطلح " استراتيجية المرونة السيبرانية" اعترافًا وجاذبية كبيرين في عام 2010 تقريباً مما يمثل نقطة محورية في إنشائه، اذ لم يكن مفهوم المرونة السيبرانية مفهوماً أو مناقشاً على نطاق واسع وكان الأمن السيبراني هو المصطلح السائد المستخدم لوصف التدابير المتخذة للحماية من التهديدات السيبرانية.

ومن التطور التاريخي لمفهوم استراتيجية المرونة السيبرانية كان هناك اعتراف بأنها تشير إلى قدرة النظام أو المصارف على التكيف والاستجابة للهجمات أو التهديدات السيبرانية والحفاظ على العمليات الحيوية في ضوء الأحداث غير المتوقعة، وخلال عام 2010 قدموا Sterbenz وآخرون إطاراً شاملاً للمرونة يدمج التخصصات والاستراتيجيات والمبادئ وتقنيات التحليل المتنوعة، ويوفر الإطار الذي يتكون من ست مراحل وهي الدفاع، الكشف، المعالجة، والاسترداد، التشخيص والتحسين، وهذه المراحل هي عبارة عن مجموعة من المبادئ الخاصة بتصميم البنية للشبكات المرنة، بما في ذلك المتطلبات الأساسية وعوامل التمكين والسلوكيات لتلك الشبكات (Sterbenz et al. ,2020:98).

أن مصطلح المرونة السيبرانية هو تطور جديد ظهر في أوائل العقد الأول من القرن الحادي والعشرين اعترافاً بضرورة إنشاء أنظمة يمكنها الصمود والتعافي من الحوادث السيبرانية.

ومنذ ذلك الحين اكتسب مفهوم المرونة السيبرانية اهتماماً متزايداً في كل من القطاعين العام والخاص حيث أصبحت المؤسسات المالية والمصارف أكثر اعتماداً على التكنولوجيا وتواجه مجموعة متزايدة من التهديدات السيبرانية، وعلية أصبح مفهوم المرونة السيبرانية عنصر أساسي في أي استراتيجية شاملة للأمن السيبراني لأنها تساعد المؤسسات المالية والمصارف على الحد من تأثير الهجمات السيبرانية والحفاظ على استمرارية الأعمال وحماية المعلومات الحساسة في العمل المصرفي ومن مراحل التطور التاريخي يمكن دراسة كيفية تطور مفهوم المرونة السيبرانية مع مرور الوقت ونكتسب رؤى تمهيدية حول الاستراتيجيات والأساليب التي كانت فعالة في الحد من التهديدات السيبرانية اذ تُعلم هذه المعرفة التاريخية استراتيجياتنا في الوقت الحاضر وتساعدنا على اتخاذ قرارات مستنيرة بشأن التطويرالمستقبلي للمرونة السيبرانية، السيبرانية مما يسهل إنشاء فهم موحد ومشترك أكثر للمفهوم (Tzavara & 2023: 2) .Vassiliadis,

ويرى الباحث ان القيمة المضافة للدراسة تكمن في قدرتها على إثراء الممارسات الحالية وتوجيه الاستراتيجيات المستقبلية والمساهمة في الخطاب الأكاديمي الأوسع مما يعزز في نهاية المطاف الفعالية الشاملة والقدرة على التكيف لتدابير الأمن السيبراني في مواجهة التحديات المتطورة، كما تتجلى استراتيجية المرونة السيبرانية من قدرتها ليس على تحصين الدفاعات الحالية فقط ولكن على الاستعداد بشكل استباقي أيضاً لمشهد الأمن السيبراني المتغير باستمرار مما يعزز مستقبل رقمي أكثر مرونة وأماناً.

ثانيا – مفهوم استراتيجية المرونة السيبرانية واهميتها:

The concept of cyber resilience strategy and its importance

1- **مفهوم استراتيجية المرونة السيبرانية:** The concept of cyber resilience strategy

ان أصل كلمة المرونة يأتي من علوم المواد والفيزياء حيث تميز المرونة خاصية أي مادة لامتصاص الطاقة عند تعرضها للإجهاد واستئناف شكلها الأصلي أو الحفاظ عليها بعد ثنيها أو تمددها أو ضغطها وقدم Xiuying (1973) لأول مرة مصطلح "المرونة" في سياق النظم البيئية مشيراً إلى قدرة النظام على استيعاب التغيرات في البيئة المحيطة والبقاء مستمراً (Oxford Brookes,2020:14) .

أن المرونة السيبرانية هي عبارة عن استراتيجية تساعد المصارف على إدراك أن المتسللين يتمتعون بميزة الأدوات المبتكرة وعنصر المفاجأة والهدف ويمكن أن ينجحوا في محاولتهم ويساعد هذا المفهوم المصارف ايضا على الاستعداد والوقاية والاستجابة والتعافي بنجاح إلى الحالة الآمنة المقصودة وهذا تحول ثقافي بالمقارنة مع الأمن السيبراني، اذ تتطلب استراتيجية المرونة السيبرانية من المصارف التفكير بشكل مختلف وأن تكون أكثر مرونة في التعامل مع الهجمات السيبرانية (Ploch,2010:14). ويعرف Cavelty استراتيجية المرونة السيبرانية بأنها قدرة النظام المصرفي على حماية نفسه من الحوادث والهجمات السيبرانية والحفاظ على مستوى مقبول من الأداء والحفاظ على الوظائف الحيوية واستعادة جودة الخدمات في الوقت المناسب إلى المستوى الذي كان موجوداً قبل وقوع الحادث (Cavelty, 2013:17).

تشير استراتيجية المرونة إلى القدرة على الاستعداد للظروف المتغيرة والتكيف معها والصمود والتعافي بسرعة من التهديدات والهجمات المتعمدة أو الحوادث والتهديدات الطبيعية (Buryachok, 2016:22).

وفقًا Accenture تعني استراتيجية المرونة السيبرانية القدرة التي تقلل من التأثير وتستعيد النظام أو البيانات بسرعة عندما يهاجم جهات خارجية غير معروفة النظام في الفضاء الإلكتروني، وبعبارة أخرى تعمل زيادة المرونة على إعادة البيئة الطبيعية في أسرع وقت ممكن واستئناف الوظائف الأساسية للنظام (Accenture, 2018:16).

وتُعرَّف استراتيجية المرونة على نطاق واسع بأنها "قدرة النظام على تجنب الاضطراب وإعادة التنظيم مع الخضوع للتغيير أيضا من أجل الاحتفاظ بوظيفة وشخصية وبنية وردود أفعال مماثلة" (Omar & Kilika,2018:249). وتشير استراتيجية المرونة السيبرانية إلى قدرة المصرف للحفاظ على العمليات على الرغم من الهجوم أو انقطاع الخدمة، إن اختيار مصطلح "المرونة" كان لغاية فالمرونة تعني القدرة على التعافي بسرعة من التهديد والمخاطر السيبرانية التي لحقت في المصارف وإدراك المرء للبيئة المحيطة به وتعزيز مواقفه وخبراته لضمان استمرارية الأعمال (Hayes&Kotwica,2019).كما تشير

استراتيجية المرونة السيبرانية إلى قدرة المصرف على ممارسة اعماله وتحقيق النتائج المرجوة منها على الرغم من الأحداث السيبرانية السلبية التي يواجها (Maziku et al. 2019:11).ويرى Kott استراتيجية المرونة السيبرانية بأنها القدرة على الاستعداد والتخطيط للأحداث السلبية واستيعابها والتعافي منها والتكيف معها بنجاح أكبر خاصة تلك المرتبطة بالهجمات السيبرانية الكبيرة (Kott ,2019:33). وتعرف استراتيجية المرونة السيبرانية على انها قدرة المصرف على "توقع، والصمود، والتعافي من، والتكيف مع التحديات والضغوط على الأنظمة التي تتطلب موارد سيبرانية(Ross et al., 2020:). وتشير استراتيجية المرونة السيبرانية إلى قدرة المصرف على التوقع والمقاومة والتعافي من الهجمات والتكيف معها في مواجهة ظروف الشدائد أو الضغوطات على الموارد السيبرانية التي تحتاجها للعمل". وهذا يعني أنه يجب إنجاز العمل بغض النظر عن كيفية مهاجمة العناصر السيبرانية (Bejarano et al 2021:16).

وتعني استراتيجية المرونة السيبرانية نظاما لديه القدرة على الصمود والتعافي والتكيف بسرعة لتقليل العواقب الضارة الناجمة عن حدث غير مرغوب فيه وقبول الاختراق السيبراني كحدث محتمل، ومعاناة النظام نتيجة لذلك؛ وينصب التركيز على قدرة النظام على التعافي والتكيف وليس مجرد المقاومة" (Kott & Linkov, 2021:56).

ووفقا للمعهد الوطني للمعايير والتكنولوجيا عرفت استراتيجية المرونة السيبرانية على انها القدرة على توقع الظروف المعاكسة والصمود فيها والتعافي منها والتكيف معها بما في ذلك التهديدات أو الهجمات على الأنظمة التي تستخدم أو التي لا تمكن بواسطة الموارد السيبرانية، وتجدر الإشارة أيضاً إلى أن جميع المناقشات المتعلقة بالمرونة السيبرانية تركز على ضمان الانظمة وتستند إلى افتراض أن الخصم سوف يخترق الدفاعات ويؤسس وجوداً طويل الأمد في الأنظمة المصرفية ومن ثم فإنه يؤكد على الفرق بين الأمن السيبراني القياسي واستراتيجيات المرونة السيبرانية التي تتضمن تعليمات للأنظمة مع التركيز على ضمان سرية وسلامة وتوافر أصول المعلومات (NIST, 2021:160).

وتشير المرونة السيبرانية إلى قدرة المصرف على توقع التهديدات أو الاضطرابات أو الهجمات السيبرانية ومواجهتها والتكيف معها والتعافي منها، وتتجاوز هذه المرونة مجرد آليات الدفاع لتشمل استراتيجيات استباقية تهدف إلى الحفاظ على استمرارية الأعمال وحماية الأصول الحيوية والحفاظ على ثقة أصحاب المصلحة في مواجهة المخاطر السيبرانية المتطورة، وفي جوهرها تجسد المرونة السيبرانية نهجًا شاملاً للأمن السيبراني يدمج الأشخاص والعمليات والتقنيات للتخفيف من المخاطر وضمان المرونة التنظيمية في مشهد رقمي مترابط بشكل متزايد (Sophia & Sharif, 2024:5).

2- اهمية ومزايا استراتيجية المرونة السيبرانية:

The importance and advantages of the cyber resilience strategy

أدى التطور السريع للتكنولوجيا على مدى العقود القليلة الماضية إلى تطورات غير مسبوقة، مما أدى إلى تغيير جذري في طريقة عمل المصارف وتفاعلها مع العالم، ومع ذلك فإن هذه الوتيرة السريعة للتطور التكنولوجي لم تأت دون مجموعة من التحديات، وأصبحت القضايا الأمنية سائدة بشكل متزايد حيث تتضاعف التهديدات السيبرانية ونقاط الضعف جنباً إلى جنب مع التقدم التكنولوجي (Aslan, et al ,2023:12).

تتبنى المصارف التكنولوجيا بشكل متزايد لتظل قادرة على المنافسة وذات صلة في هذا العصر الرقمي ومع ذلك فإن الاعتماد المتزايد على التكنولوجيا والاتصال يدل على زيادة التعرض للمخاطر السيبرانية وان الاتصال بالإنترنت يجعل المؤسسات مرئية في عالم معولم حيث يمكن أن يحدث التعطيل بشكل غير متوقع مما يتسبب في أضرار وخسائر مالية كبيرة (Bounaamane, 2023: 8).

فضلاً عن ذلك أدت جائحة كوفيد-19 إلى تسريع التحول نحو العمل الرقمي والعمل عن بعد، مما زاد من تفاقم الوضع وأدى إلى المزيد من نقاط الضعف والخصوم السيبرانيين، ومن هنا جاءت اهمية استراتيجية المرونة السيبرانية في معالجة المخاطر المتعلقة بالتكنولوجيا والتكييف معها، بما في ذلك المخاطر المرتبطة بالإنترنت والتي تعد من أهم المخاطر كما اشار تقرير المخاطر العالمية الأخير لعام 2023 واعدها واحدة من المخاطر الكبرى (Kaplan, et al ,2019:22).

تعتمد استراتيجية المرونة السيبرانية على مفاهيم الدفاع والوقاية، وقد ركزت على الاجراءات الأمنية والوقائية من المخاطر السيبرانية والاختبارات والاستجابة للحوادث وقدرة المصارف على العودة إلى مدة الأزمة لمنع الحوادث الأمنية وإدارتها، كما تعمل استراتيجية المرونة السيبرانية على أهمية إعداد الانظمة الخاصة بالمصارف لمواجهة عواقب الهجوم السيبراني واستعادة القدرة على خلق القيمة بعد وقوعها ضحية لهجوم سيبراني معين (Bounaamane, 2023: 9).

وأصبح لاستراتيجية المرونة السيبرانية دور واهمية كبيرة في المؤسسات المالية لا سيما القطاع المصرفي لأنها أداة واستراتيجية فعالة لمواجهة التهديدات والمخاطر السيبرانية ويتجلى ذلك في قدرتها على الدفاع عن الهجمات السيبرانية عبر الإنترنت والحد من عواقبها والحفاظ على نشاط تشغيلي بإنتاجية مستقرة نسبيا في عالم يشوبه العديد من التهديدات والمخاطر السيبرانية، وان القدرة على البقاء في بيئة تبدو فيها التهديدات السيبرانية أمراً لا مفر منه (Mcquiggan, 2020:36).

ومع ذلك فإن استراتيجية المرونة السيبرانية ليست محدودة في استراتيجياتها ولكنها توفر أيضاً المزايا المهمة للمؤسسات المالية والمصرفية بما في ذلك:

أ- تحسين العمليات الداخلية: يتطلب تنفيذ تدابير المرونة السيبرانية تقييماً وتحسيناً مستمراً للعمليات الداخلية مما يؤدي إلى تحسين كفاءة العمليات وتحسين ادارة الموارد.

ب- منع الخسائر المالية: تهدف استراتيجية المرونة السيبرانية إلى تقليل تكاليف الهجمات السيبرانية مثل الخسائر المالية الناتجة عن حجم البيانات أو تدمير الأنظمة أو اضطراب العمليات التجارية، وهنالك دور وأهمية كبيرة لتدابير استراتيجية المرونة السيبرانية الموجة نحو الاستثمار، إذ يمكن للمؤسسات المالية والمصارف أن تحد من تأثير تمويل الهجمات السيبرانية وفهم التعامل معها في هذا المجال (Bidgoli, 2019:21).

ج- الحفاظ على السمعة: يمكن أن تؤدي الهجمات السيبرانية إلى عواقب سيئة على سمعة المصرف، وتتيح فعالية استراتيجية المرونة السيبرانية الحد من الأضرار التي لحقت بالسمعة من الاستجابة السريعة للهجمات وحماية البيانات الحساسة للجمهور والحفاظ على ثقة المودعين (Bounaamane, 2023: 8).

ان الحفاظ على ثقة المودعين في المصارف التي تكتسب قوة كبيرة من المرونة السيبرانية التي تلهم الثقة من خلال حماية المعلومات السرية وضمان استمرارية العمليات التي تحد من الهجمات السيبرانية، ومن ثم فإنها تعزز العلاقات التجارية وتحافظ على إخلاص مودعيها وزيادة ثقتهم، ومن المؤكد أن الأمن السيبراني هو مكون أساسي لاستراتيجية المرونة السيبرانية كما أن المرونة السيبرانية استراتيجية تشمل التدابير الوقائية والتفاعلية واستمرارية التعاملات التي تهدف إلى ضمان دوام المصارف وازدهارها على المدى الطويل(Davis , 2021: 6).

إن المؤسسات المالية والمصارف التي تبدأ بتطبيق استراتيجية المرونة السيبرانية ترى اهميتها من خلال القدرة على الحفاظ على الوضع الراهن واستيعاب تأثير التهديدات، في المقابل تتبنى المؤسسات المالية والمصارف الأكثر تقدماً وتكيفياً لاستراتيجية المرونة السيبرانية فهماً يعتمد على التنظيم الذاتي واعتماد ممارسات جديدة تتوافق مع متطلبات واستراتيجيات المرونة السيبرانية. (Grøtan, et al.:2022: 205).

ولكل ماسبق يرى الباحث ان استراتيجية المرونة السيبرانية تمثل أولوية واهمية قصوى في صناعة التعاملات المصرفية ومجالاً رئيساً لاهتمام السلطات المالية وهذا ينسجم مع الحوادث السيبرانية التي يتميز بها العصر الرقمي بالقرن الحادي والعشرين بالاستخدام الواعي والواسع النطاق لتكنولوجيا المعلومات مما أدى إلى حاجة المصارف إلى حماية مواردها وتحسين سمعتها وزيادة ثقة مودعيها بخدماتها ومحافظتها على خصوصية بيانات المودعين لديها.

ثالثاً – مفهوم التعاملات السيبرانية والمفاهيم المقاربة لها:

The concept of cyber activities and concepts related to them

هناك مجموعة من المفاهيم التي ترتبط ارتباطاً وثيقاً بمفهوم استراتيجية المرونة السيبرانية والتعاملات السيبرانية المرافقة للعمل المصرفي، وبالنظر لارتباط هذه المفاهيم بمقومات استراتيجية المرونة السيبرانية كان لابد من توضيح هذه المفاهيم وكما يأتي:

1- **مفهوم الأمن السيبراني:** Cyber security concept

تعددت التعاريف المحددة للأمن السيبراني فكان لزاماً علينا الاطلاع على أكبر عدد ممكن من التعاريف وقبل أن نبين مفهوم الامن السيبراني لابد أن نتطرق إلى بعض المفاهيم المرتبطة بالأمن السيبراني بحيث تقارب هذا المفهوم من عدة زوايا:

السيبرانية لغة: وهي مأخوذة من كلمة (سيبر) وهي صفة تقنية لشيء مرتبط بثقافة الحواسيب، أو تقنية المعلومات أوالواقع الافتراضي، فالسيبرانية تعني فضاء الأنترنت وهي كلمة مشتقة من الكلمة اليونانية sybermetes التي وردت بداية في مؤلفات الخيال العلمي وكان يقصد بها قيادة ربان السفينة.

السيبرانية اصطلاحاً: كلمة سيبرانية في مفهومها الحديث استعملت لأول مرة من قبل عالم الرياضيات الأمريكي الأصل Norbert Winer وهو أستاذ الرياضيات في معهد ما ساسوستس التقني الذي أعطاها مفهومها الاصطلاحي الحديث عام 1948 (عطية ,2019 :51).

ولذلك يعد مفهوم الأمن السيبراني: هو عملية الدفاع عن أمن الشبكات والمعلومات والأجهزة والبرامج بطريقة تقنية (تكنولوجية) باتخاد الإجراءات والتدابير والوسائل التكنولوجية الحديثة بهدف الحماية من الهجمات أو التهديدات الإلكترونية لضمان أمن وسلامة وتوافر المعلومات (الشورة, 2022: 8).

2- **الفضاء السيبراني:** Cyberspace

هو ذلك المكان الذي أوجدته تكنولوجيا المعلومات والاتصالات وفي مقدمتها الأنترنت، ويرتبط الفضاء السيبراني ارتباطاً وثيقاً بالعالم المادي عبر البنى التحتية المختلفة للاتصالات والأنظمة المعلوماتية وعبر العديد من الخدمات التي لم يكن بالإمكان الحصول عليها من دونه، كما عرف الفضاء السيبراني بأنه بيئة متعددة الأوجه يتفاعل فيها الأفراد والبرامج والخدمات من خلال الأجهزة التقنية والشبكات المترابطة على الإنترنت (الشورة, 2022: 9).

3- **القوة السيبرانية:** Cyber power

يعد Joseph Nye Say من أبرز المهتمين بالقوة السيبرانية أذ يعرفها على أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا الدولة والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية، واشار الى أن مفهوم القوة السيبرانية يشير إلى مجموعة الموارد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية المعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل (زروقة, 2019: 101).

4- **التهديدات السيبرانية:** Cyber threats

وهي التهديدات التي تستخدم آليات وشبكات الإنترنت وأجهزة الكمبيوتر بهدف الإضرار بالأجهزة الالكترونية والشبكات المتصلة بالإنترنت، كما تعد التهديدات السيبرانية على أنها الفعل الذي يقوض سلامة وأداء شبكة الكمبيوتر لأغراض متعددة باستغلال نقطة ضعف تمكن المهاجم من التلاعب بالنظام وإلحاق الضرر بالأخرين (الجعفري، 2022: 24).

5- **الحرب السيبرانية:** cyber warfare

تعرف الحرب السيبرانية بانها توظيف القدرات السيبرانية اذ يكون الهدف الاساسي هو تحقيق الاهداف والاثار في الفضاء السيبراني او من خلاله وهي كذلك نشاط مماثل او غير مماثل دفاعي كان ام هجومي على الشبكة الرقمية من قبل فواعل دولية او محلية القصد منها هو الحاق الضرر بالبنى التحتية الحيوية والانظمة المصرفية (شنوف ،2020: 91).

6- **التجسس الإلكتروني:** Electronic espionage

يمكن تعريف التجسس الإلكتروني على أنه استراتيجية اقتحام أنظمة وشبكات الكمبيوتر من أجل استخراج معلومات حساسة حكومية أو خاصة بالمؤسسات (Morag, 2014:12). ويعد التجسس الإلكتروني تهديداً منتشراً على نطاق واسع جداً وقد يكون له هدف سياسي أو اقتصادي او لا يكون له هدف، ويجرى التجسس السيبراني عادةً باستخدام ثغرات يوم الصفر جنباً إلى جنب مع التصيد الاحتيالي من أجل التسلل إلى الشبكات والحصول على بيانات حساسة، ويمكن أيضاً استخدام البيانات المجمعة للتحركات الجانبية ايضاً داخل الأنظمة المستهدفة من أجل الحصول على معلومات من مصادر أخرى من المصدر الذي تمكن المهاجمين من اختراقه إلكترونيا، وغالبا ما تستغل هذه الثغرات وحتى تشاركها ما بين القراصنة قبل أن تكتشفها الجهات المطورة للبرمجيات المصابة. (Lillemose, 2015:8).

❖ **يعد يوم الصفر (Zero-day attack) هو هجوم دون انتظار، او هو استغلال نقاط الضعف في البرمجيات وثغراتها الأمنية خاصة غير المعروفة منها للعامة أو حتى مطوريها في شن هجمات.**

7- **الجرائم السيبرانية:** cyber crimes

وهي الأعمال والأفعال والممارسات الإجرامية غير القانونية التي تجرى بواسطة محترفين بصورة فردية أو يتبعون جهات مختلفة بقصد السيطرة على نظام المصرف الالكتروني، وتشمل الجرائم السيبرانية المهاجمين والمخربين السيبرانيين الذين هم أفراد أو كيانات تقوم بأفعال وسلوكيات مخالفة للقوانين وغالباً ما يكونوا على درجة من الاحترافية في التخطيط والتنفيذ للهجمات السيبرانية على المصارف الالكترونية (Catota, etal, 2019:22).

8- **الردع السيبراني:** cyber deterrence

هو عبارة عن إجراءات سريعة وفورية تأتي كرد فعل على المخربين السيبرانيين بحيث تتخذ التدابير اللازمة على منعهم في المستقبل من فعل تلك التهديدات واجراء التعديلات اللازمة على النظام لمنع تكرار تلك الاختراقات مع كيفية اتخاذ التدابير القانونية تجاههم (Ethan, etal,2017:32).

9- **المخاطر السيبرانية:** cyber risks

وهي عبارة عن مجموعة من النشاطات التي تشكل أو تمثل أعمالاً ضارة من قبل بعض الأطراف وتكون غير واضحة لدى مسؤولي المؤسسات والمصارف الأمر الذي يتطلب اتخاذ قرارات فورية لمواجهة هذه النشاطات والقضاء عليها في مهدها (Foua.,2021:15).

10- **مفهوم الارهاب السيبراني:** The concept of cyber terrorism

يعد العثور على ثغرة في برنامج الكمبيوتر أحد أكثر الطرق شيوعاً للمراوغة للوصول إلى النظام المستهدف وإلحاق الضرر به، ويمكن للقراصنة استغلال هذه الثغرة الأمنية للوصول إلى المعلومات المقيدة فضلاً عن إلى إنشاء واستخدام البرامج الضارة وبرامج التجسس، وغالباً ما يهاجم المهاجمين الضحايا باستخدام شكل من أشكال التخريب السيبراني. ان الارهاب السيبراني يمكنه تعطيل العديد من أنظمة المؤسسات والمصارف وكذلك وسائل النقل العالمية والتي يمكن ان تكون على سبيل المثال من خلال تنفيذ هجمات على نحو سرقة البيانات وعمليات الاختراق الأخرى، تعد الفيروسات هي أشهر وأقدم أنواع البرامج الضارة كونها برامج ملحقة بالأجهزة المستخدمة (Unipath,2023,45).

رابعاً – الفرق بين استراتيجية المرونة السيبرانية والامن السيبراني :

ان البحث في قضايا التحديات الامنية و استراتيجية المرونة السيبرانية يقتضي توصيف بيئة هذه التحديات ومعرفة الفروق الاساسية بين مفهوم الفضاء السيبراني و استراتيجية المرونة السيبرانية وهي كالاتي:

ترتبط استراتيجية المرونة السيبرانية والأمن السيبراني ارتباطاً وثيقاً ولكن هناك اختلافات رئيسة بينهما اذ يركز الأمن السيبراني على الإجراءات والممارسات الدفاعية لحماية تكنولوجيا المعلومات وبيئات التكنولوجيا التشغيلية من التهديدات السيبرانية وهي تتضمن تدابير مثل الدفاع عن الشبكة وحماية البنية التحتية الحيوية وضمان المعلومات(Robertson & Rice, 2020:13).

ومن ناحية أخرى تشيراستراتيجية المرونة السيبرانية إلى قدرة النظام على مقاومة الهجمات السيبرانية والتعافي منها واستعادة وظائفه، لذلك فهي لا تنطوي فقط على إجراءات دفاعية فقط ولكن القدرة على التكيف والتعافي من التهديدات السيبرانية ايضاً تؤكد استراتيجية المرونة السيبرانية القدرة على تحمل الصدمات الخارجية التي تسببها المخاطر السيبرانية والتعافي منها والتكيف معها وهذا يتطلب طرقاً وأدوات تجريبية استراتيجية للمرونة السيبرانية، بينما يركز الأمن السيبراني على الوقاية والتخفيف من المخاطر والجرائم السيبرانية، أذ تركز استراتيجية المرونة السيبرانية على التأهب والاستجابة والتكيف لضمان بقاء الأنظمة الحرجة. بينما يعتمد الأمن السيبراني على مبدأ ثنائي وقد تكون البيئة آمنة أو لا تكون كذلك وهو يشمل التدابير المتخذة لحماية نظام المعلومات من التهديدات الرقمية لمنع المتسللين من الوصول إلى الخوادم والبيانات (McQuiggan, 2020:17).

في المقابل، تتضمن استراتيجية المرونة السيبرانية قبول ضعف الفرد والقدرة على الصمود كما ان المرونة السيبرانية تدرك أن الحماية الكاملة لبنيتها التحتية ضد الهجمات وانقطاع الخدمة أمراً صعباً ولكن من المهم أن تكون على دراية بهذه الثغرة الأمنية والمخاطر الموجودة، فضلاً عن انها تتجاوز مفاهيم الدفاع والوقاية وهي تركز على استراتيجيات السياسة الأمنية والوقاية من المخاطر والاختبار والاستجابة للحوادث وقدرة المصرف على التعافي في أوقات الأزمات على عكس الأمن السيبراني الذي يهدف الى منع وإدارة الحوادث الأمنية (Bidgoli, 2019:13).

ويتضح للباحث مما سبق ارتباط المفاهيم السابقة بمفهوم الأمن السيبراني أذ ان مفهوم الأمن السيبراني مفهوم عام وشامل يتضمن كل هذه المفاهيم كما ان الكثير من التهديدات تتعلق بالخلط بين المفاهيم في مجال الأمن السيبراني من عدم التحديد الدقيق لتلك المفاهيم ومن ثم فلابد من توضيحها بشكل دقيق، فضلاً عن المعرفة بتلك المفاهيم سوف تؤثر في اساليب التعامل مع القضايا السيبرانية كافة.

خامساً: – المكونات الرئيسه لاستراتيجية المرونة السيبرانية والتحديات التي تواجهها:

Key components of a cyber resilience strategy and the challenges they face

أ– المكونات الرئيسية لاستراتيجية المرونة السيبرانية:

هناك مجموعة من المكونات الخاصة باستراتيجية المرونة السيبرانية والتي تعد نهجاً متعدد الأوجه للأمن السيبراني وهي كالاتي (Ladoke Akintola,2024:2):

1- الإدارة الاستباقية للمخاطر: Proactive risk management

يتضمن ذلك تحديد وإدارة المخاطر السيبرانية وتقييمها وترتيب أولوياتها، فضلاً عن تنفيذ تدابير وقائية للتخفيف من نقاط الضعف وتعزيز الاستعداد.

2- الاستجابة القوية للحوادث: Strong incident response

تتيح خطة الاستجابة للحوادث السيبرانية المحددة جيداً للمؤسسات اكتشاف الحوادث السيبرانية واحتوائها والتخفيف منها بسرعة مما يقلل من التأثير على العمليات وتسهيل التعافي في الوقت المناسب.

3- التخطيط للاستمرارية والتعافي من الحوداث: Continuity and incident recovery planning

يضمن إنشاء خطط استمرارية قوية وآليات للتعافي من الحوداث السيبرانية إمكانية استدامة وظائف الأعمال الحيوية حتى في حالة حدوث اضطرابات شديدة أو هجمات إلكترونية.

ب– التحديات التي تواجه تحقيق استراتيجية المرونة السيبرانية

على الرغم من أهميتها فإن تحقيق استراتيجية المرونة السيبرانية يمثل تحديات عديدة للمؤسسات المالية بما في ذلك (Ladoke Akintola,2024:2):

1- تعقيد مشهد التهديدات: Complexity of the threat landscape

تشكل الطبيعة المتطورة للتهديدات السيبرانية وتعقيدها تحديات كبيرة أمام المؤسسات والمصارف في تحديد المخاطر الناشئة والتخفيف من حدتها بشكل فعال.

2- قيود الموارد: Resource constraints

قد تعيق الموارد المالية والتكنولوجية والبشرية المحدودة قدرة المؤسسات المالية والمصارف على تنفيذ استراتيجيات شاملة للمرونة السيبرانية والاستثمار في الحلول الأمنية المتقدمة.

3- الامتثال والمتطلبات التنظيمية: Compliance and regulatory requirements

يضيف الامتثال للوائح الصناعة وقوانين حماية البيانات تعقيداً إلى جهود استراتيجية المرونة السيبرانية مما يتطلب من المؤسسات المالية والمصارف التنقل في متاهة من الأطر القانونية والتنظيمية.

سادساً: – أهداف استراتيجية المرونة السيبرانية:

Objectives of the cyber resilience strategy

تعد الأهداف هي تعبيرات عالية المستوى للنتائج المرغوبة والتي تكون مشتركة بين العديد من تعريفات المرونة وتتضمن في إطار بناء استراتيجية المرونة السيبرانية لتوفير رابط بين قرارات إدارة المخاطر على مستوى النظام ومستوى المهمة ومستوى العمليات التجارية وكذلك على المستوى التنظيمي، ويمكن لاستراتيجيات إدارة المخاطر التنظيمية استخدام أهداف استراتيجية المرونة السيبرانية المرتبطة بها لتكاملها ومن ثم لا يمكن احتساب أهداف استراتيجية المرونة السيبرانية أهدافاً نهائية بقدر ما هي مهام استراتيجية حالية واهداف وسيطة تشكل المشهد التشغيلي للمصرف (NIST, 2021:160).

ويمكن القول إنها توفر نهجاً أكثر توحيداً لإدارة المخاطر وسد الفجوات بين المستويات التنظيمية المختلفة وتعزيز ثقافة استراتيجية المرونة السيبرانية الاستباقية، وتتمثل اهداف استراتيجية المرونة السيبرانية بالآتي (NIST, 2021:161)، (Fedir & Korobeynik ,2023:5):

1- **القدرة على التطور:** The ability to develop

أن تحسين القدرات السيبرانية الشاملة للمصرف ذات الصلة ليست صفة ثابتة ولكنها ديناميكية تتطلب التطوير والتحسين المستمر لفهم جوهر استراتيجية المرونة السيبرانية وكيف تختلف عن الأمن السيبراني فضلاً عن الحاجة الماسة لتطوير القدرات والمهارات بما يتناسب مع التطورات الكبيرة في تكنلوجيا المعلومات والاتصالات.

2- **التوقع:** Anticipation

يركز هذا الهدف على التدابير الاستباقية للتنبؤ وتحديد عناصر النظام الأكثر أهمية لعمليات المصرف والتي تكون عرضة للهجمات السيبرانية المعقدة أو الإخفاقات أو الحوادث غير المتوقعة، لذلك جميع المخاطر ذات المستوى الحرج يجب أخذها بالحسبان ومعالجتها بتطبيق حلول استراتيجية المرونة السيبرانية عليها بغض النظر عن احتمالية تحقيقها على افتراض أن التهديد مهما كان غير محتمل ومعقداً في تحقيقه سيكون لا يزال تحقيقه في اي وقت ممكن.

3- **استكشاف التهديدات:** Threat exploration

ينبغي على المصارف أن تتوقع التهديدات وأن تطبق استراتيجيات المرونة السيبرانية الأكثر أهمية في النظام التشغيلي للمصرف، ويدعو المعهد الوطني للمعايير والتكنلوجيا (NIST) إلى اتخاذ موقف استباقي بشأن التهديدات ويتضمن ذلك إجراء عمليات شاملة لاستكشاف أنواع جديدة من التهديدات لتحديد نواقل الهجوم المحتملة والتنبؤ بالتهديدات الجديدة، ويتضمن أيضاً عمليات تدقيق منتظمة للأنظمة التي تساعد على

اكتشاف نقاط الضعف قبل أن تستغل ويجب أن يتخلل هذا التفكير المستقبلي جميع مستويات المصرف مما يشجع اليقظة والتعلم المستمر، ويتضمن هذا الهدف تنمية ثقافة الوعي والتعليم واليقظة الدائمة أيضاً.

4- **القدرة على الصمود:** Ability to withstand

تساعد استراتيجية المرونة السيبرانية على إنشاء إطار وقائي إضافي للمصرف يفعل عندما لا تتمكن عناصر الأمن السيبراني من التعامل مع هجوم أو فشل أو حدث سلبي، إذ إن التحقيق العملي لهذا الهدف يدل على أن الأنظمة المرنة يجب أن تكون قادرة على تحمل الشدائد وضمان الحد الأدنى من الوظائف الضرورية ويمكن اختبار التهديدات السيبرانية الجديدة على نطاق واسع أو في بيئة معزولة بهدف تحديد قدرة النظام على تحمل تلك التهديدات والقدرة على الصمود امامها، وينبغي أيضاً تحقيق المرونةمن خلال اتخاذ تدابير وقائية لمنع التهديدات السيبرانية من أن تصبح هجمات حقيقية.

5- **القدرة على التعافي:** Ability to recover

تعد القدرة على استعادة انظمة التشغيل العادي بسرعة بعد وقوع حادث سيبراني أمراً بالغ الأهمية لاستراتيجية المرونة السيبرانية، ويمكن للتعافي السريع والفعال أن يخفف بشكل كبير من تأثير الحادث على عمليات المصرف وأدائه وسمعته.

ويعد التعافي هو عملية متعددة الأوجه ولا يقتصر الأمر على الجوانب الفنية لاستعادة الأنظمة والبيانات بعد وقوع حادث ما فحسب بل يتضمن إدارة العواقب الأوسع نطاقاً للهجوم السيبراني أيضاً، ويمكن أن يشمل ذلك استراتيجيات الاتصال لإدارة الضرر الذي يلحق بالسمعة أو الاعتبارات القانونية في حالة حدوث خرق للبيانات.

6- **القدرة على التكيف:** Adaptation ability

أن الجانب الأكثر أهمية في المرونة السيبرانية هو القدرة على تجميع المعلومات بشكل مستمر حول الحوادث ونقاط الضعف والتقنيات الجديدة ومن ثم تكييف الاستراتيجيات، ويمكن أن يشمل ذلك مراجعة السياسات الأمنية وتعزيز معلومات التهديدات وإعادة تقييم استراتيجيات إدارة المخاطر والتي يجب أن تحدث بشكل منتظم، فأثناء الهجوم يجب أن يكون النظام المرن قادراً على التكيف بسرعة والعثور على موارد جديدة لأداء مهامه الأساسية وتقليل الضرر الناجم عن التهديدات والهجمات المحتملة.

سابعاً – تقنيات استراتيجية المرونة السيبرانية:

Cyber resilience strategy techniques

تشير تقنيات استراتيجية المرونة السيبرانية في المصارف إلى التدابير والاستراتيجيات المطبقة لضمان قدرة المصرف على الصمود والتعافي من الهجمات والحوادث السيبرانية، وفي القرن الحادي والعشرين تواجه المصارف التقليدية تحديات جراء التحولات الرقمية وتكنولوجيا المعلومات مما أدى إلى زيادة الاعتماد على الأنظمة الإلكترونية المعقدة للعمليات اليومية.

إن أهمية استراتيجية المرونة السيبرانية في القطاع المصرفي معترف بها عالمياً، ولذلك تجرى الأبحاث والدراسات لتطوير تقنيات استراتيجية المرونة السيبرانية في المصارف، أذ تعمل تقنيات المرونة السيبرانية على فهم التهديدات السيبرانية وكذلك العمليات المرتبطة بتعزيز المرونة السيبرانية من أجل معالجة التهديدات التي يواجها النظام المصرفي (Linkov, 2021:58).

وفيما ياتى مجموعة من التقنيات التى تخص عمل استراتيجيات المرونةالسيبرانية وهي كالاتي.

1- **الاستجابة التكيفية:** Adaptive response

تعمل تقنيات الاستجابة التكيفية على تمكين الأنظمة والمصارف من الاستجابة بشكل مناسب وديناميكي لمواقف محددة باستخدام حالات الطوارئ التشغيلية المرنة والبديلة للحفاظ على الحد الأدنى من القدرات التشغيلية من أجل الحد من التهديدات وتجنب زعزعة الاستقرار واتخاذ إجراءات وقائية عند الاقتضاء.

وبشكل أكثر تحديداً تتضمن الاستجابة التكيفية اختيار وتنفيذ ومراقبة فعالية النظام التي تغير مستوى الهجوم بشكل أفضل وتحافظ على القدرات الحيوية وتستعيد القدرات الوظيفية، وتشمل القدرات التي تدعم الاستجابة التكيفية إعادة التكوين الديناميكي والتخصيص الديناميكي للموارد والعمل الوقائي وقدرته التركيب الديناميكي للمصرف (Kott,etal, 2017: 18).

2- **المراقبة التحليلية:** Analytical monitoring

تقوم تقنيات المراقبة التحليلية بجمع البيانات ودمجها وتحليلها بشكل مستمر لاستخدام معلومات التهديد وتحديد نقاط الضعف والعثور على مؤشرات للظروف المعاكسة المحتملة، وتحديد الأضرار المحتملة أو الفعلية وتشمل القدرات التي تدعم المراقبة التحليلية لمراقبة وتقييم الأضرار ودمج أجهزة الاستشعار وتحليلها وتحليل البرامج الضارة بشكل دوري ومستمر (Linkov, 2018:156).

3- **الحماية المنسقة:** Coordinated protection

تقوم تقنيات الحماية المنسقة بتنسيق آليات متعددة ومتميزة لحماية الموارد الحيوية عبر الأنظمة الفرعية للمصارف، ويعد النهج الرئيسي هو الحماية الفنية المتعمقة في حين أن القدرات التي تدعم الحماية المنسقة تشمل التنسيق وتحليل الاتساق والإدارة التكيفية. (Woodard, 2019:74).

4- **تحديد المواقع الديناميكية:** Dynamic positioning

تقوم تقنيات تحديد المواقع الديناميكية بتوزيع الوظائف ونقلها ديناميكياً ومن ثم تغيير مستوى الهجوم وتشمل القدرات النقل الوظيفي والوظائف الموزعة في المصارف (Kitsak & Linkov,2017:12) .

5- **تقييد الامتيازات:** Restricting privileges

تعمل تقنيات تقييد الامتيازات على تقييد الامتيازات المخصصة للمستخدمين والكيانات السيبرانية، وتعيين متطلبات الامتيازعلى الموارد على أساس الأهمية، وتشمل قدرات إدارة الامتيازات وقيود الاستخدام القائمة على الامتيازات على الحد من تأثير واحتمالية الإجراءات غير المقصودة من قبل المودعين المصرح لهم والتي تهدد المعلومات والخدمات لفرض المزيد من الوقت والجهد على الخصم حتى يتمكن من الحصول على أوراق الاعتماد كما أنها تحد من قدرة الخصم على الاستفادة الكاملة من أوراق الاعتماد التي تم الحصول عليها (Connelly & Linkov, 2017:48).

6- **التمثيل الديناميكي:** Dynamic representation

تدعم تقنيات التمثيل الديناميكي الوعي بحالة المهمة والاستجابة لها باستخدام التمثيل الديناميكي للمكونات والأنظمة والخدمات وأنشطة الخصم والمواقف السلبية الأخرى وتأثيرات مسارات العمل البديلة بما في ذلك مسارات استراتيجية المرونة السيبرانية (Ganin & Linkov, 2017:38).

8 – **النزاهة المثبتة:** Proven integrity

توفر تقنيات النزاهة المثبتة آليات للتأكد مما إذا كانت الخدمات الحيوية ومخازن المعلومات وتدفقات المعلومات والمكونات قد تعرضت للتلف، وتشمل فحوصات النزاهة والجودة وتتبع المصدر والتحقق من صحة السلوك، فهي تسهل تحديد النتيجة الصحيحة عندما يكون هناك تعارض بين الخدمات أو المدخلات المختلفة واكتشاف محاولات الخصم لتقديم برامج أو أجهزة أو بيانات مخترقة فضلاً عن التعديل أو التصنيع (Kott & Lange,2017:19).

ثامناً: – مراحل وارشادات لجنة بازل (3) لتحقيق استراتيجية المرونة السيبرانية:

Basel Committee stages and guidelines for achieving a cyber resilience strategy

أ – مراحل لجنة بازل لتحقيق استراتيجية المرونة السيبرانية

يُمكن تحقيق استراتيجية المرونة السيبرانية على سبع مراحل (معاد، 2022 :5):

المرحلة الأولى - قدرات التحديد: تشمل هذه المرحلة الإدارة السيبرانية والهيكلية والقدرة على الاستشعار لتوقع ومعالجة الأعمال السلبية أو الأحداث السيبرانية.

المرحلة الثانية - الصمود: تشمل وضع إطار دفاع إلكتروني متكيّف يُحافظ على المهام، ويُساعد في التصدي للتهديدات التي تتعرض لها المؤسسة.

المرحلة الثالثة - الدفاع: تشمل الدفاع ضد الأحداث السيبرانية التخريبية والتحوّط بمناعة رقمية قوية ذاتية الشفاء ودفاع إلكتروني نشط.

المرحلة الرابعة - الفحص: تشمل مراقبة الشبكات الالكترونية والإنترنت في الوقت الفعلي للكشف عن التهديدات السيبرانية في الوقت الفعلي.

المرحلة الخامسة - الملاحظة: تشمل الاعتماد على الأتمتة والتعلم الآلي لمواجهة التهديدات السيبرانية المستقبلية.

المرحلة السادسة - الاسترداد: تشمل القدرة على استعادة المنصات الرقمية بسرعة، والتكييف، واستعادة الأنظمة ذات المهام الحرجة، لتجنب انقطاع الأعمال في حال حصول أي تهديدات سيبرانية.

❖ المرحلة السابعة - التكيُّيف: وتشمل التقييم الذاتي المستمر وقياس الأداء السيبراني والتحسين المستمر لدعم الأعمال التجارية.

ب – ارشادات لجنة بازل لتحقيق استراتيجية المرونة السيبرانية:

تقترح لجنة « بازل 3 » للرقابة المصرفية مجموعة من الإرشادات تُساعد المصارف في تعزيز قدراتها على الصمود في وجه الهجمات السيبرانية وتتضمن هذه الارشادات البنود الاتية (معاد، 2022 :6):

1- **مواجهة المخاطر السيبرانية:**

ينبغي على المصرف مواجهة المخاطر السيبرانية، سواء على صعيد إدارة المخاطر أو أطر عمل أمن المعلومات، أو على صعيد استراتيجيات الأمن السيبراني الخاصة بها، وتشمل الاستراتيجيات المتطلبات المتعلقة بالحوكمة، والرقابة، والملكية، والمخاطر، والمساءلة، وأمن المعلومات، والتقييم الدوري، ومراقبة ضوابط الأمن السيبراني، والاستجابة للحوادث، واستمرارية الأعمال، والتخطيط للانتعاش من الحوادث. وعلى المصرف الالتزام بالمعايير الدولية استراتيجية للمرونة السيبرانية.

2 – **الاستجابة للحوادث السيبرانية والتعافي منها:**

ينبغي على المصارف أن تضع إطاراً للاستجابة للحوادث والتعافي منها، مما يضمن استمرارية الأعمال والتعافي من الكوارث. ولمساعدة المؤسسات المالية على تعزيز ممارساتها في هذا المجال، أصدر مجلس الاستقرار المالي FSB في العام 2020 تقريراً بعنوان الممارسات الفعَّالة للاستجابة لحوادث الإنترنت والتعافي منها بالتركيز على سبعة بنود هي: الحوكمة - التخطيط والإعداد والتحليل والتخفيف والتعافي والتنسيق والاتصال والتحسين.

3 – **التعامل مع الطرف الثالث:**

يجب على المصرف مراعاة استمرارية الأعمال وسرية المعلومات ونزاهتها عند التعامل مع أطراف ثالثة. ويجب أن تتوافق كيفية التعامل مع الأطراف الثالثة مع احتياجات وسياسات المصرف بما في ذلك سرية المعلومات وسلامتها، ومتطلبات حماية البيانات العامة، ومتطلبات الأمان المحددة لحماية معلومات المصرف والزبائن. وتشمل متطلبات حماية البيانات موقع البيانات، وفصل البيانات، وقيود استخدام البيانات، وأمن البيانات، ومعالجة البيانات في حالة انتهاء العمل مع الطرف الثالث.

4- ترتيبات تبادل المعلومات:

يُحدد تقرير لجنة «بازل3» للرقابة المصرفية خمسة أنواع من الترتيبات لمشاركة المعلومات: المشاركة بين المصارف ومشاركة المصرف مع الجهات الرقابية، فضلاً عن مشاركة المصرف مع الجهات الرقابية وبالعكس مشاركة الجهات الرقابية مع المصرف واخيرا المشاركة مع الأجهزة الأمنية

5- مقاييس استراتيجية المرونة السيبرانية:

لا تزال مقاييس استراتيجية المرونة السيبرانية وجودتها قيد التطوير. وتركز المقاييس السائدة حالياً على استخدام المعلومات، والاستطلاعات، والرقابة إلاّ أن هناك حاجة ملحة إلى تطوير المزيد من مقاييس المرونة السيبرانية والتي تؤثر تأثيراً حيوياً في تأمين المصارف وحماية أنظمتها من التهديدات السيبرانية، ولعل من أهم المقاييس الخاصة بالمرونة السيبرانية في المصارف هي:

(أ) التحصينات الأمنية: تشمل تدابير الأمان والحماية للحد من الهجمات والاختراقات، ويشمل ذلك استخدام جدران الحماية، والتحقق المزود، وتشفير البيانات.

(ب) الكشف المبكر: يتعلق بالقدرة على اكتشاف الهجمات والتهديدات في وقت مبكر، ويتضمن استخدام أنظمة الكشف عن التسلل ومراقبة السجلات.

(ج) التدريب والتوعية: ينبغي توعية الموظفين بأفضل الممارسات الأمنية وتدريبهم على التعامل مع التهديدات السيبرانية.

(د) اختبار الضعف: يتعلق بتقييم نقاط الضعف في الأنظمة وتحسينها، ويشمل اختبار الاختراق والتحقق من الأمان.

تاسعاً – معايير استراتيجية المرونة والامن السيبراني:

Standards and strategic frameworks for external embezzlement

1 – معيار الامن والمرونة السيبرانية (ISO 22316)

قامت المنظمة الدولية للمعايير (ISO) بتطوير معيار (ISO 22316) للأمن والمرونة السيبرانية لتوفير مبادئ وتوجيهات لاستراتيجية المرونة السيبرانية، وفي هذا المعيار تعرف المرونة السيبرانية على أنها قدرة المصرف على استيعاب البيئة المتغيرة والتكيف معها وتمكينها من تحقيق أهدافها والبقاء والازدهار وبنفس الوقت لا يعتمد المعيار بوجود نهج واحد يناسب الجميع لتحقيق استراتيجية المرونة السيبرانية.

يحدد المعيار تسع سمات التي تساهم في بناء القدرة على الصمود، بما في ذلك الرؤية المشتركة ووضوح الهدف والفهم والتأثير والقيادة الفعالة الممكنة والثقافة الداعمة وتبادل المعلومات والمعرفة وتوافر الموارد والتطوير وتنسيق التخصصات الإدارية والتحسين المستمر والقدرة على توقع وإدارة التغيير، وتركز أنشطة المعيار في المقام الأول على الإدارة والتنظيم والتطوير والتنسيق مع التركيز على دعم التحسين المستمر وإدارة التغيير مع وضع المبادئ والتعاملات التي تعزز استراتيجية المرونة السيبرانية (International Organization for Standardization: 2017).

2 – معيار نظام إدارة أمن المعلومات: ISO 27001:2022 ISMS - ISO27001:2013

يُستخدم ISO27001 بشكل عام لتقييم قدرة المصرف على تلبية متطلبات أمن المعلومات وتنفيذ نهج قائم على المخاطر السيبرانية، ويركز معيار ISO27001 على الحفاظ على السرية والنزاهة وتوافر أصول المعلومات من خلال الإدارة المنهجية لثلاثة مكونات رئيسه: الأشخاص والعمليات والتكنولوجيا، باستخدام نهج قائم على المخاطر، ويوفر عناصر التحكم التوجيه في الاستعداد والمقاومة والاستجابة والتعافي. ومن المهم ملاحظة أن الضوابط ليست إلزامية، ويمكن للمؤسسات اختيار تنفيذها بناءً على تقييم المخاطر واحتياجات أمن المعلومات الخاصة بها، وتعتمد قوة أمان المصرف على نهج المخاطر الذي تتبعه المنظمة، على سبيل المثال يحتوي المعيار على عنصر تحكم يوجه المنظمة للتعلم من حادث سابق. ومع ذلك لم يذكر التكيف مع الطبيعة المتغيرة لبيئة المصرف والتي تعد إحدى سمات المرونة السيبرانية، ومع ذلك يمكن استخدام المفاهيم المنصوص عليها في معيار ISO27001 لتقييم وإدارة مخاطر الأمن السيبراني والمساهمة في تعزيز استراتيجية المرونة السيبرانية (International Organization for Standardization: 2017).

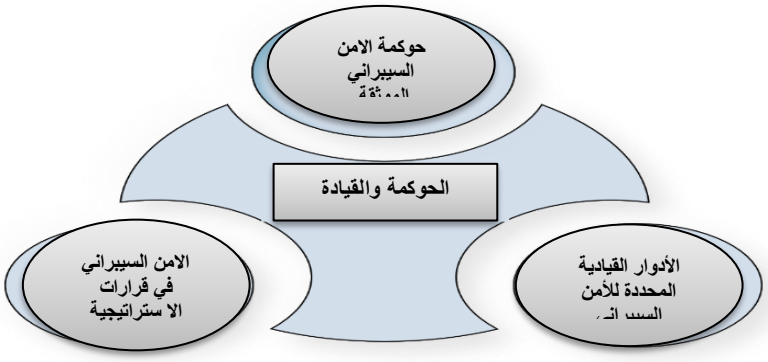
عاشراً: مراحل ومؤشرات استراتيجية المرونة السيبرانية:

Developing a cyber resilience framework and indicators:

في صياغة الإطار الشامل للمرونة السيبرانية اعتمدت مراحل ومؤشرات متميزة ومتعددة وهي كالاتي:

1- **الحوكمة والقيادة:** Governance and Leadership

ينصب التركيز الأساسي للمرحلة الأولية على الحوكمة والقيادة مع الاعتراف بالدور الحاسم الذي تؤديه هياكل الحوكمة التنظيمية وممارسات القيادة في تعزيز استراتيجية المرونة السيبرانية، وتتضمن هذه المرحلة التأسيسية ثلاثة مؤشرات محورية لتوجيه وتقييم إنشاء إطار فعال للمرونة السيبرانية كما هو مبين في الشكل (2).



شكل (2) مؤشرات الحوكمة والقيادة

S. Slapnicar, M. Axelsen, I Bongiovanni, and D. Stockdale,"A pathway model to five lines of accountability in cybersecurity gov- ernance,P:7, 2023.

أ-حوكمة الأمن السيبراني الموثقة: وهي أحد الأمور الأساسية لتنمية استراتيجية المرونة السيبرانية القوية لتطوير وتوثيق سياسات وإجراءات واضحة وشاملة لحوكمة الأمن السيبراني (Slapnicar et al., 2023:51). ويؤكد هذا المؤشر الأول على ضرورة صياغة إطار منظم يحدد المبادئ الشاملة والمبادئ التوجيهية والبروتوكولات الإجرائية التي تحكم الأمن السيبراني ضمن السياق التنظيمي، وإن وجود سياسات موثقة جيداً لا يعد بمثابة نقطة مرجعية أساسية لجميع أصحاب المصلحة فحسب، بل يضمن أيضاً اتباع نهج موحد لإدارة مخاطر وتحديات الأمن السيبراني (Safitra et al., 2023:18).

ب- الأدوار القيادية المحددة للأمن السيبراني: بناءً على وضع سياسات الحوكمة يؤكد المؤشر الثاني على أهمية الأدوار والمسؤوليات المحددة بوضوح لقيادة المرونة السيبرانية، وتتطلب استراتيجية المرونة

السيبرانية استجابة منسقة وفعالة للتهديدات المحتملة، وهذا يتطلب تحديدا واضحا للوظائف والمسؤوليات بين الأفراد أو الفرق المسؤولة عن الأمن السيبراني (Axelsen et al., 2023:51).

ت- الأمن السيبراني في القرارات الاستراتيجية: يضخم المؤشر الثالث البعد الاستراتيجي للمرونة السيبرانية بتسليط الضوء على ضرورة دمج اعتبارات الأمن السيبراني في نسيج قرارات الأعمال الاستراتيجية، بينما تتنقل المؤسسات في مشهد رقمي متزايد، ويصبح مواءمة الأمن السيبراني مع الأهداف الإستراتيجية الأوسع أمرًا بالغ الأهمية، ويؤكد هذا المؤشر على ضرورة قيام المؤسسات المالية بتضمين الأمن السيبراني كعنصر أساسي ومتكامل في عمليات التخطيط الاستراتيجي الخاصة باستراتيجية المرونة السيبرانية (Jaradatet al., 2024:12).

2- **تقييم المخاطر:** Risk Assessment

تركز المرحلة الثانية على تقييم المخاطر، وهو عنصر حاسم يدعم الإدارة الفعالة للأمن السيبراني، وفي هذه المرحلة يركز على تقييم وفهم المشهد الديناميكي للمخاطر السيبرانية بنهج منظم وشامل، وتشمل المرحلة الثانية ثلاثة مؤشرات رئيسه، كل منها مصمم لتعزيز قدرة المنظمة على تقييم وإدارة مخاطر السيبرانية بشكل استباقي، كما هو مبين في الشكل (3).

الشكل (3) مؤشرات تقييم المخاطر

J. Al-Gasawneh, A. AL-Hawamleh, A. Alorfi, and G. Al-Rawashde, "Moderating the role of the perceived security and endorsement on the relationship between per- ceived risk and intention to use the artificial intelligence in financial services , P:12, 2022.

أ- التقييمات المحدثة للمخاطر السيبرانية: ويمثل حجر الزاوية في استراتيجية المرونة السيبرانية الفعالة في إنشاء تقييمات مخاطر السيبرانية المحدثة بانتظام والموثقة جيدًا، ويؤكد هذا المؤشر على الحاجة إلى تقييم مستمر ومنهجي للتهديدات ونقاط الضعف المحتملة التي يمكن أن تؤثر على الأصول الرقمية

للمصرف، وتتضمن التحديثات المنتظمة لتقييمات المخاطر السيبرانية بقاء المصرف على اطلاع دائم بالتهديدات السيبرانية المتطورة والتقدم التكنولوجي والتغيرات في مشهدها التشغيلي (Gasawneh, 2022:751).

ب- تحديد أولويات المخاطر: تتطلب الإدارة الفعالة للمخاطر السيبرانية اتباع نهج استراتيجي لتحديد الأولويات، ويؤكد هذا المؤشر على أهمية تحديد أولويات المخاطر المحددة بشكل منهجي بناءً على تأثيرها المحتمل واحتمالية حدوثها، ومن تصنيف المخاطر وفقا لخطورتها واحتمالاتها يمكن للمصارف تخصيص الموارد بحكمة مع التركيز على تخفيف التهديدات الأكثر أهمية من حيث خطورتها على المصارف (Gasawneh, 2022:751).

ت- التقييم المستمر: ان المخاطر السيبرانية ديناميكية وتتأثر بالعديد من العوامل الداخلية والخارجية، ويؤكد هذا المؤشر على أهمية الدراسة والتحليل المستمر لهذه العوامل للحفاظ على فهم شامل لمشهد المخاطر المتطور، وقد تشمل العوامل الداخلية تغييرات في الهيكل التنظيمي أو البنية التحتية للتكنولوجيا أو ديناميكيات القوى العاملة، في حين يمكن أن تشمل العوامل الخارجية التهديدات السيبرانية الناشئة أو التغييرات التنظيمية، أو التحولات في المشهد الجيوسياسي.

3- **السياسات والإجراءات الأمنية:** Security policies and procedures

ان التركيز الآن على السياسات والإجراءات الأمنية جانب حاسم في تعزيز الثقافة السيبرانية داخل المصارف، و هذه المرحلة مخصصة لصياغة وتوصيل وصيانة سياسات وإجراءات شاملة مصممة للحماية من التهديدات السيبرانية، وتحدد ثلاثة مؤشرات رئيسه لتعزيز قدرة المصرف على إنشاء والحفاظ على سياسات وإجراءات أمنية فعالة، كما هو مبين في الشكل (4).

الشكل (4) مؤشرات السياسات والإجراءات الأمنية

S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D A.Alabbad"Digitaltransformation and cybersecurity challenges for businesses resilience: Issues and recommendations," Sensors, P:5,2023.

أ- إمكانية الوصول والوعي: من الأمور الأساسية لفعالية السياسات الأمنية إمكانية الوصول إلى هذه السياسات والوعي بها بين الموظفين، ويؤكد هذا المؤشر على أهمية التأكد من أن السياسات السيبرانية ليست موثقة جيدا فحسب بل يسهل أيضا الوصول إليها لجميع أعضاء المصارف وتسهل إمكانية الوصول والفهم الجماعي للمبادئ التوجيهية المعمول بها مما يخلق مسؤولية مشتركة عن الأمن السيبراني بين الموظفين (Slapnicar et al., 2023:51).

ب- التواصل المنتظم: بناءً على المؤشر الأول، تتطلب السياسات الأمنية الفعالة مبادرات تواصل وتدريب مستمرة، ويضمن التواصل المنتظم بقاء الموظفين على علم بتحديثات السياسات والتهديدات الناشئة وأفضل الممارسات، ويساعد هذا النهج الاستباقي على دمج عقلية التهديدات السيبرانية في الثقافة التنظيمية مما يعزز الشعور بالمسؤولية المشتركة لحماية الأصول الرقمية (Saeed et al., 2023:15).

ت- تحديثات السياسات المتعلقة بالتكنولوجيا والتهديدات: تتطلب الطبيعة الديناميكية للمشاهد السيبرانية من المصارف الحفاظ على المرونة السيبرانية في الاستجابة للتقدم التكنولوجي والتهديدات الناشئة، ويؤكد هذا المؤشر على الحاجة إلى تحديث السياسات والإجراءات الأمنية في الوقت المناسب لمعالجة المخاطر المتطورة، وينبغي إجراء مراجعات منتظمة لمواءمة السياسات مع أحدث التطورات التكنولوجية ومعايير الصناعة ومشهد التهديدات المتغير باستمرار.

4- **تدريب الموظفين وتوعيتهم:** Employee Training and Awareness

تعترف هذه المرحلة الحاسمة بالدور المحوري الذي يؤديه الموظفون المطلعون واليقظون في تعزيز استراتيجية المرونة السيبرانية الشاملة للمصارف، ولتحقيق ذلك حددت ثلاثة مؤشرات رئيسه يهدف كل منها إلى تنمية قوة عاملة واعية بالتهديدات السيبرانية تكون قادرة على تخفيف المخاطر بشكل فعال، كما هو مبين في الشكل (5)

الشكل (5) مؤشرات تدريب الموظفين وتوعيتهم

M. Hawamleh and A. Ngah, "An adoption model of mobile knowledge sharing based on the theory of planned behavior " P:13,2017.

أ- تكرار الدورات التدريبية والحضور: إن حجر الزاوية في بناء ثقافة واعية بالتهديدات السيبرانية هو توفير دورات تدريبية منتظمة للموظفين، ويؤكد هذا المؤشر على أهمية تكرار وحضور هذه الدورات التدريبية، وتضمن الدورات التدريبية المنتظمة والمتكررة تعرض الموظفين باستمرار لأحدث معلومات الأمن السيبراني والتهديدات وأفضل الممارسات (Hawamleh & Ngah, 2017:43).

ب- الوعي بالتهديدات السيبرانية وأفضل الممارسات: يتمثل الهدف الرئيسي لتدريب الموظفين في تعزيز الوعي بالتهديدات السيبرانية الشائعة وغرس أفضل الممارسات للتخفيف من المخاطر السيبرانية، ويؤكد هذا المؤشر على حاجة الموظفين ليس لحضور الدورات التدريبية فقط ولكن لإظهار فهم شامل للتهديدات السيبرانية السائدة والتدابير الوقائية المقابلة (Safitra, et al., 2023:18).

ت- دليل الإبلاغ عن التعاملات المشبوهة: يمتد تعزيز ثقافة الوعي السيبراني إلى ما هو أبعد من الاحتفاظ بالمعرفة إلى المشاركة النشطة في حماية الأصول التنظيمية، ويقيم هذا المؤشر إنشاء ثقافة يساهم فيها الموظفون بنشاط في جهود المرونة السيبرانية بالابلاغ عن التعاملات المشبوهة أو الحوادث الأمنية المحتملة (Kanaan, et al., 2023:185).

5- **خطة الاستجابة للحوادث السيبرانية:** Incident Response Plan

يتحول التركيز في هذه المرحلة إلى تطوير وتنفيذ خطة الاستجابة للحوادث، وهذه المرحلة مخصصة لإعداد المصارف للاستجابات الفعالة في حالة وقوع حادث سيبراني، وحددت ثلاثة مؤشرات رئيسه لضمان أن المصارف مجهزة تجهيزا جيدًا للكشف عن الحوادث والاستجابة لها والتعافي منها، كما هو موضح في الشكل (6)

الشكل (6) مؤشرات خطة الاستجابة للحوادث السيبرانية

H. M. Melaku, "A dynamic and adaptive cybersecurity governance framework," Journal of Cybersecurity and Privacy, P:8 ,2023.

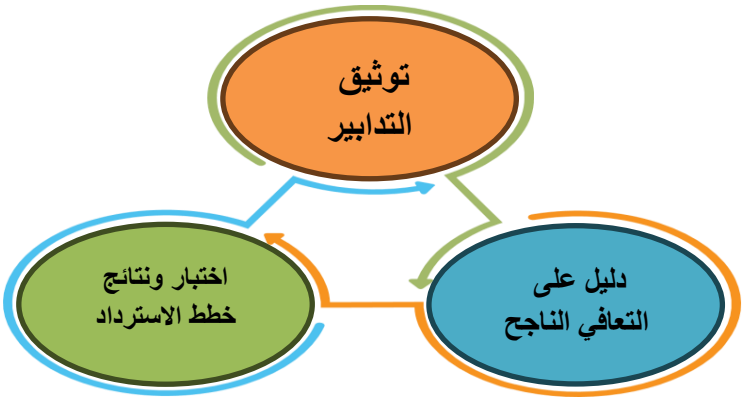
أ- وجود خطة الاستجابة للحوادث وإمكانية الوصول إليها: يكمن أساس القدرة الفعالة على الاستجابة للحوادث في وجود خطة استجابة للحوادث موثقة جيدا، ويؤكد هذا المؤشر على أهمية وجود خطة شاملة تحدد الإجراءات والبروتوكولات الواجب اتباعها في حالة وقوع حادث سيبراني (Saeed et al., 2023:15).

ب- الاختبار والتحديث المنتظم: تتطلب الطبيعة الديناميكية للتهديدات السيبرانية والمشهد التكنولوجي المتطور إجراء اختبار وتحديث منتظمين لخطة الاستجابة للحوادث السيبرانية، ويؤكد هذا المؤشر على أهمية إجراء تمارين واختبارات محاكاة للتحقق من فعالية خطة الاستجابة للحوادث وإمكانية الوصول إليها في سيناريوهات العالم الحقيقي، كما يؤكد على الحاجة إلى إجراء مراجعات وتحديثات دورية للحفاظ على توافق الخطة مع مشهد التهديدات المتغير والتقدم التكنولوجي (Melaku, 2023:350).

ت- التنسيق والتواصل الفعال: إلى جانب وجود واختبار وجود خطة الاستجابة للحوادث وإمكانية الوصول إليها، فإن فعالية الاستجابة للحوادث تتوقف على التنسيق والتواصل، ويؤكد هذا المؤشر على حاجة المصارف إلى إجراء تدريبات محاكاة للاستجابة للحوادث لا تختبر الإجراءات الفنية فحسب، بل تقيم أيضاً التنسيق والتواصل بين فرق الاستجابة للحوادث السيبرانية (Hawamleh et al., 2024:16).

6- **استمرارية الأعمال والتعافي من الحوداث:** Business Continuity and Disaster ecovery

ان استمرارية الأعمال والتعافي من التهديدات هو جانب بالغ الأهمية في استراتيجية المرونة السيبرانية الذي يضمن قدرة المصارف على الحفاظ على الوظائف الأساسية في مواجهة الحوادث، وحددت ثلاثة مؤشرات رئيسه لتحديد وتقييم مدى استعداد المصارف لاستدامة العمليات أثناء وبعد وقوع الحوادثالسيبرانية كما هو مبين في الشكل (7).



الشكل (7) مؤشرات استمرارية الأعمال والتعافي من الكوارث

M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," Sustainability, P:11, 2023.

أ- توثيق التدابير: يقع في صميم استمرارية الأعمال والتعافي من الكوارث توثيق التدابير التي تضمن استمرارية الوظائف الحيوية، ويؤكد هذا المؤشر على ضرورة وجود خطط واستراتيجيات شاملة للحفاظ على العمليات الأساسية أثناء وبعد وقوع حادث سيبراني مدمر (Melaku, 2023:350).

ب- اختبار ونتائج خطط التعافي: أحد العناصر الحاسمة لاستمرارية الأعمال والاستعداد للتعافي من الكوارث هو الاختبار المنتظم لخطط التعافي من الحوادث السيبرانية، ويؤكد هذا المؤشر على أهمية إجراء اختبارات منهجية لتقييم فعالية خطط التعافي، بما في ذلك استعادة أنظمة تكنولوجيا المعلومات والعمليات الحيوية، ويعد تكرار هذه الاختبارات ودقتها بمثابة مقاييس أساسية لتقييم مدى جاهزية المصرف للتعامل مع التهديدات السيبرانية (Safitra, et al., 2023:18).

ت- دليل التعافي الناجح: يأتي التحقق النهائي من إجراءات استمرارية الأعمال والتعافي من الحوادث السيبرانية من دليل التعافي الناجح بعد وقوع حادث حقيقي أو محتمل، ويؤكد هذا المؤشر على أهمية تتبع وتوثيق الحالات التي نجحت فيها المصارف في استعادة وظائفها الحيوية بعد حدوث انقطاع سواء جرت محاكاة الحادث أو حدث في سيناريو من العالم الحقيقي (Hawamleh et al., 2024:16).

7- **الضوابط الأمنية:** Security Controls

يتحول التركيز في هذه المرحلة إلى الضوابط الأمنية وهي عنصر أساسي في حماية الأصول الرقمية للمصارف، وتشمل هذه المرحلة تنفيذ وإدارة التدابير التي تهدف إلى منع التهديدات الأمنية وكشفها والاستجابة لها، وحددت ثلاثة مؤشرات رئيسه لتقييم قدرة المصارف على الحفاظ على ضوابط أمنية فعالة كما هو مبين في الشكل (8)

شكل (8) مؤشرات الضوابط الأمنية

AHawamleh, A. S. M. Alorfi, J. A. Al-Gasawneh, and G. Al- Rawashdeh, "Cyber security and ethical hacking: The importance of protecting user data," Solid State Technology, P:7 2020.

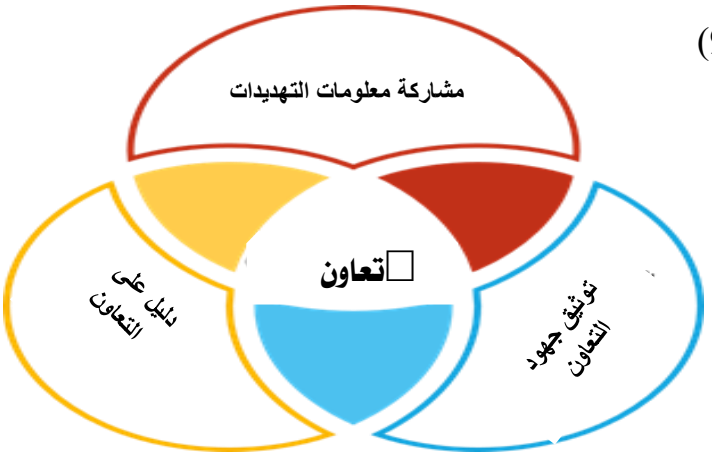
أ- تحديثات منتظمة للتحكم في الأمان: يكمن أساس الضوابط الأمنية القوية في التحديثات المنتظمة وتصحيح الإجراءات الأمنية، ويؤكد هذا المؤشر على أهمية الحفاظ على الضوابط الأمنية الحالية لمعالجة التهديدات الناشئة ونقاط الضعف وتقنيات الاستغلال، وتضمن التحديثات المنتظمة أن آليات الدفاع الخاصة بالمصارف مجهزة لمقاومة التهديدات السيبرانية المتطورة (Saeed et al., 2023:13).

ب- تنفيذ وفعالية المصادقة: أحد الجوانب الأساسية لتعزيز الضوابط الأمنية هو تنفيذ وفعالية المصادقة متعددة العوامل، ويؤكد هذا المؤشر على أهمية استخدام عوامل مصادقة إضافية تتجاوز كلمات المرور لتعزيز أمان الوصول، ويضيف ايظاً طبقة إضافية من الحماية من خلال مطالبة المستخدمين بتقديم أشكال متعددة من التعريف مثل كلمات المرور أو القياسات الحيوية أو رموز الأمان (Hawamleh, 2023:1).

ت- مراقبة سجل التحكم الأمني بحثا عن الحالات الشاذة: يتم تسهيل التحديد الاستباقي للتهديدات الأمنية من خلال المراقبة والتحليل المستمر لسجلات التحكم الأمني بحثا عن الحالات الشاذة، ويؤكد هذا المؤشر على أهمية المراجعة النشطة للسجلات الناتجة عن الضوابط الأمنية (Melaku, 2023:3).

8- **التعاون مع أصحاب المصلحة:** Cooperation with stakeholders

عند الدخول الى المرحلة الثامنة من إطار المرونةالسيبراني، يتوسع التركيز الآن ليشمل التعاون مع أصحاب المصلحة وهو عنصر حاسم في تعزيز القدرة الجماعية على اكتشاف التهديدات السيبرانية ومنعها والاستجابة لها.، تؤكد هذه المرحلة على أهمية إقامة الشراكات وتبادل المعلومات مع الجهات الخارجية لتعزيز المرونة السيبرانية للمصارف، وقد حددت ثلاثة مؤشرات رئيسه لتقييم فعالية جهود التعاون، كما هو مبين في الشكل (9)



الشكل (9) مؤشرات التعاون مع أصحاب المصلحة

S. Pandey, R. K. Singh, and A. Gunasekaran, “Supply chain risks in industry 4.0 environment: review and analysis framework,” Pro- duction Planning & Control, P:5, 2023.

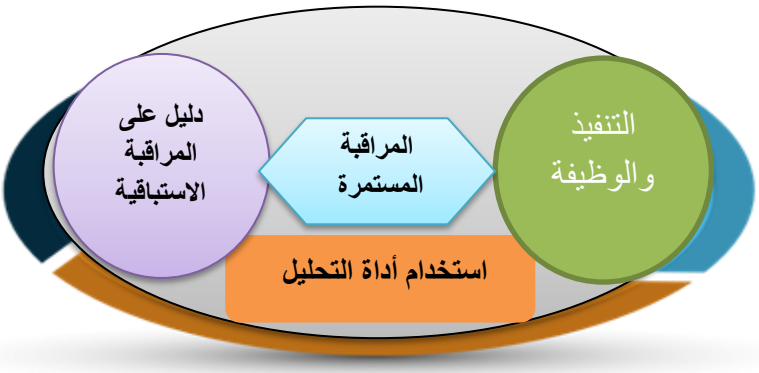
أ- توثيق جهود التعاون: من الأمور المركزية للتعاون الفعال هو توثيق الجهود المبذولة بالشراكة مع أصحاب المصلحة الخارجيين، ويؤكد هذا المؤشر على أهمية الاحتفاظ بسجل للمبادرات التعاونية مع تحديد طبيعة ونطاق الارتباطات مع الكيانات الخارجية، وقد يشمل التوثيق اتفاقيات رسمية أو مشاريع مشتركة أو موارد مشتركة تهدف إلى تعزيز قدرات استراتيجية المرونة السيبرانية (Hawamleh, 2023:12).

ب- مشاركة معلومات التهديدات: ان حجر الزاوية في التعاون الفعال هو مشاركة معلومات التهديدات وأفضل الممارسات مع مجموعات الصناعة المصرفية ويؤكد هذا المؤشر على أهمية المساهمة الفعالة والاستفادة من المعرفة الجماعية داخل الصناعة المصرفية، ومن تبادل المعلومات حول التهديدات الناشئة ونواقل الهجوم السيبراني واستراتيجيات الدفاع الفعالة يمكن للمصارف بشكل جماعي رفع مستوى استراتيجية المرونة السيبرانية لديها (Stojcic, 2021:562).

ت- دليل التعاون: ان أحد الجوانب الأساسية للتعاون من أجل تعزيز استراتيجية المرونة السيبرانية ينطوي على المشاركة مع منظمات إنفاذ القانون، ويؤكد هذا المؤشر على أهمية إنشاء والحفاظ على علاقات تعاونية مع الكيانات التي تعمل على مكافحة الجرائم السيبرانية وتعزيز الأمن السيبراني على نطاق أوسع (Pandey, et al., 2023:1301).

9- **المراقبة المستمرة:** Continuous Monitoring

ومع الشروع في المرحلة التاسعة من إطار استراتيجية المرونة السيبرانية يتقارب التركيز الآن على المراقبة المستمرة وهو عنصر حاسم في الكشف الاستباقي والاستجابة للتهديدات السيبرانية المحتملة، وتؤكد هذه المرحلة على أهمية المراقبة والتحليل المستمر للحفاظ على انظمة المصارف، وحددت ثلاثة مؤشرات رئيسه لتقييم قدرة المصرف على المراقبة المستمرة، كما هو مبين في الشكل (10)



الشكل (10) مؤشرات الرصد المستمر

H. Naseer, K. Desouza, S. B. Maynard, and A. Ahmad, "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics, P:15,2023.

أ- التنفيذ والوظيفة: يقع في قلب المراقبة المستمرة تنفيذ ووظيفة الأنظمة المصممة لتتبع وتحليل البيئة الرقمية للمصارف بشكل مستمر، ويؤكد هذا المؤشر على أهمية وجود حلول قوية وفعالة للرصد المستمر وينبغي أن تشمل هذه الأنظمة مجموعة واسعة من الأصول بما في ذلك صافي الأصول في المصارف (Hawamleh, 2023:1).

ب- استخدام أداة التحليل: إحدى التقنيات الرئيسه في مجال المراقبة المستمرة هي المعلومات الأمنية وإدارة الأحداث ويؤكد هذا المؤشر على أهمية استخدام أدوات التحليل بانتظام لتحليل الأحداث الأمنية في الوقت الفعلي وتقوم الانظمة بتجميع البيانات من مصادر مختلفة وربطها مما يوفر رؤية شاملة للوضع الأمني للمصارف (Stojcic, 2021:252).

ت- دليل على المراقبة الاستباقية: إن استكمال المراقبة المستمرة المعتمدة على التكنولوجيا هو دليل على الجهود الاستباقية التي يقودها الإنسان بما في ذلك عمليات التدقيق المنتظمة ومراجعات السجل، ويؤكد هذا المؤشر على أهمية إنشاء روتين لعمليات الفحص اليدوي للسجلات والتكوينات وضوابط الأمان (Naseer,, et al., 2023:21).

10- **الامتثال التنظيمي:** Regulatory Compliance

تؤكد هذه المرحلة على أهمية موائمة ممارسات استرايجية المرونة السيبرانية مع اللوائح المعمول بها لضمان الوفاء بالالتزامات القانونية والتنظيمية، وحددت ثلاثة مؤشرات رئيسه لتقييم التزام المصرف بالامتثال التنظيمي كما هو مبين في الشكل (11)

الشكل (11) مؤشرات الامتثال التنظيمي

E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rek- eraho, “Enhancing cloud security—proactive threat monitoring and detection using a siem-based approach, P:4 ,2023.

أ- الوعي بلوائح المرونة السيبرانية: يكمن أساس الامتثال التنظيمي في الوعي وفهم لوائح استراتيجية المرونة السيبرانية ذات الصلة، ويؤكد هذا المؤشر على أهمية البقاء على اطلاع بالمشهد التنظيمي المطبق على الصناعة المصرفية وموقعها الجغرافية، ويمتد الوعي إلى ما هو أبعد من مجرد المعرفة إلى الفهم العميق لآثار ومتطلبات هذه الأنظمة (Tuyishime, et al, 2023:1355).

ب- تقييمات الامتثال المنتظمة: الامتثال هو عملية مستمرة تتطلب تقييمات وتوثيق منتظم لحالة امتثال المصرف، ويؤكد هذا المؤشر على أهمية إجراء تقييمات منهجية لقياس مدى الالتزام باستراتيجة المرونة السيبرانية ذات الصلة، وتضمن التقييمات المنتظمة بقاء المصرف في حالة امتثال ويمكنها إثبات التزامها بالمعايير التنظيمية (Safitra, et al., 2023:16).

ت- التعديلات على الممارسات: مع تطور المشهد التنظيمي يجب أن تكون المصارف قابلة للتكيف وإجراء تعديلات على ممارساتها لضمان الامتثال المستمر، ويؤكد هذا المؤشر على حاجة المصارف إلى تحديد وتنفيذ التغييرات بشكل استباقي في ممارسات المرونة السيبرانية الخاصة بها استجابة للمتطلبات التنظيمية المتطورة، وقد تتضمن التعديلات تحديثات للسياسات والإجراءات والضوابط الفنية لتتوافق مع اللوائح الجديدة أو المعدلة (Donalds & Bryson, 2020:51).

11- **التكنولوجيا ومرونة البنية التحتية:** Technology and Infrastructure Resilience

تؤكد هذه المرحلة على أهمية تحصين التكنولوجيا والبنية التحتية لمقاومة التهديدات ونقاط الضعف، وحددت ثلاثة مؤشرات رئيسه لتقييم قدرة المصارف على مرونة التكنولوجيا والبنية التحتية كما هو مبين في الشكل (12).

الشكل (12) مؤشرات مرونة التكنولوجيا والبنية التحتية

Z. Jaradat, A. Al-Hawamleh, M. O. Al Shbail, and A. Hamdan, "Does the adoption of blockchain technology add intangible benefits to the industrial sector, P:3,2023.

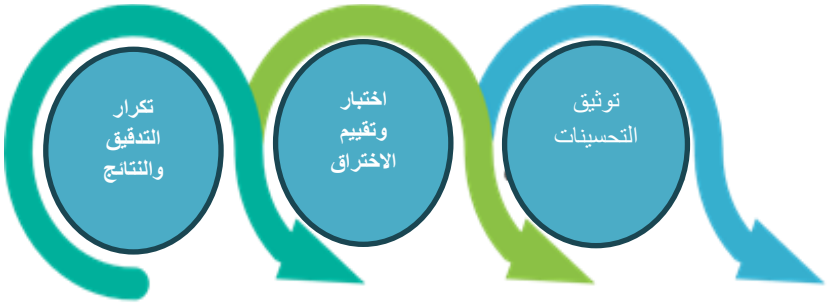
أ- وجود تدابير التكرار: في قلب التكنولوجيا ومرونة البنية التحتية يوجد تدابير التكرار في أنظمة التكنولوجيا الحيوية، ويؤكد هذا المؤشر على أهمية تنفيذ آليات النسخ الاحتياطي وتجاوز الفشل لضمان استمرارية العمليات في حالة حدوث تهديد أو فشل النظام، وتوفر تدابير التكرار شبكة أمان مما يسمح للوظائف الحيوية بالاستمرار حتى لو واجهت مشاكل في الأنظمة الأساسية (Jaradat, et al., 2023:48).

ب- نتائج اختبار البنية التحتية: يتضمن ضمان مرونة البنية التحتية إجراء اختبارات منتظمة لتقييم قدرة المصارف على تحمل مختلف السيناريوهات والتحديات، ويؤكد هذا المؤشر على أهمية إجراء اختبارات منهجية لتقييم مرونة مكونات البنية التحتية بما في ذلك الشبكات والخوادم والأصول الحيوية الأخرى (Hawamleh, 2023:1).

ت- تحديثات الأجهزة والبرامج: تعتمد مرونة التكنولوجيا والبنية التحتية على تحديثات الأجهزة والبرامج في الوقت المناسب لمعالجة نقاط الضعف، ويؤكد هذا المؤشر على أهمية مواكبة التحديثات والتحسينات الأمنية للتخفيف من المخاطر والتهديدات المحتملة (Al Omari, et al., 2023:10).

12- **عمليات التدقيق والتقييمات المنتظمة:** Regular audits and evaluations

وبالدخول إلى المرحلة الأخيرة من إطار المرونة السيبرانية يتقارب التركيز على عمليات التدقيق والتقييمات المنتظمة وهي عنصر أساسي في الحفاظ على وضع قوي للأمن السيبراني، وتؤكد هذه المرحلة على أهمية التقييمات المنهجية وعمليات التدقيق والتقييم لتحديد نقاط الضعف وتقييم الضوابط ودفع التحسين المستمر وحددت ثلاثة مؤشرات رئيسه لتقييم التزام المصارف بعمليات التدقيق والتقييم المنتظمة كما هو مبين في الشكل (13).



الشكل (13) مؤشر عمليات التدقيق والتقييم المنتظمة

H. M. Melaku, "A dynamic and adaptive cybersecurity governance framework," Journal of Cybersecurity and Privacy, P:3, 2023.

أ- تكرار التدقيق ونتائجه: يقع في صميم الحفاظ على وضع مرن للمرونة السيبرانية إجراء عمليات تدقيق التهديدات السيبرانية بشكل منتظم، ويؤكد هذا المؤشر على أهمية عمليات التدقيق المجدولة بشكل منهجي لتقييم مدى التزام المصارف بالسياسات والمتطلبات التنظيمية وأفضل ممارسات للانظمة (Melaku, 2023:3).

ب- تقييمات الضعف واختبار الاختراق: لتحديد ومعالجة نقاط الضعف المحتملة في البنية التحتية للانظمة بشكل استباقي يجب على المصارف إجراء تقييمات الضعف واختبار الاختراق، ويؤكد هذا المؤشر على أهمية البحث النشط عن نقاط الضعف والثغرات في الأنظمة والشبكات والتطبيقات

ت- توثيق التحسينات: لا يكون إجراء عمليات التدقيق والتقييمات ذا قيمة إلا إذا أدت النتائج إلى تحسينات ملموسة، ويؤكد هذا المؤشر على أهمية توثيق الإجراءات المحددة المتخذة لمعالجة نقاط الضعف وتعزيز الضوابط وتنفيذ تدابير العلاج بناءً على نتائج التدقيق والتقييم (Naseer,, et al., 2023:15).

الشكل (14) إطار ومؤشرات المرونة السيبرانية

J. Al-Gasawneh, A. AL-Hawamleh, A. Alorfi, and G. Al-Rawashde, "Moderating the role of the perceived security and endorsement on the relationship between per-ceived risk and intention to use the artificial intelligence in financial services, P:14, 2022.

يقدم إطار المرونة السيبرانية نهجا شاملا ومنهجيا لتعزيز الدفاعات التنظيمية ضد التهديدات السيبرانية المتطورة، ومن خلال اثنتي عشرة مرحلة متميزة كما هو موضح في الشكل (14) وترتكز كل منمؤشرات رئيسه، ويوجه هذا الإطار المؤسسات المالية والمصرفية في رحلة نحو تعزيز استراتيجية المرونة السيبرانية.

الحادي عشر:- ابعاد استراتيجية المرونة السيبرانية:

Dimensions of cyber resilience strategy

اليوم في المشهد الرقمي المترابط تواجه المصارف تهديدا متزايدا من الهجمات الإلكترونية. يمكن لهذه الهجمات، التي تتراوح من برامج الفدية إلى مخططات التصيد الاحتيالي المتطورة، أن تعطل العمليات وتهدد البيانات الحساسة وتقوض الثقة مع أصحاب المصلحة، ولمعالجة هذه التحديات تتجه المصارف بشكل متزايد إلى استراتيجيات المرونة السيبرانية لتحسين قدرتها على تحمل الهجمات الإلكترونية والاستجابة لها والتعافي منها.

تتجاوز المرونة السيبرانية تدابير الأمن السيبراني التقليدية من خلال التركيز على قدرة المصرف على التكيف والاستجابة للتهديدات المتطورة وهي تشمل نهجاً شاملاً يجمع بين التدابير الاستباقية، مثل تقييم المخاطر والتخفيف منها، والاستراتيجيات التفاعلية، مثل الاستجابة للحوادث والتخطيط للتعافي، ومن خلال تبني إطار استراتيجية المرونة السيبرانية، يمكن للمصارف الاستعداد بشكل أفضل للهجمات الإلكترونية والاستجابة لها والتعافي منها، وضمان استمرارية التشغيل وحماية سمعتها.

هناك مجموعة من الابعاد التي ترتبط بالمرونة السيبرانية والتي تعمل على تزويد المصارف وتأهيلها من اجل مواجهة التهديدات والمخاطر السيبرانية وهي كما حددها:

(Tsena et al. 2023:6)، (Dr. Isabella Lee. 2024:6)، (G.A. Hubbard, 2023:6)

: (Nepal Rastra,2023:10)

1 **- الحوكمة:** Strategy and planning

تشمل الحوكمة العملية الكاملة لتطوير استراتيجية المرونة السيبرانية الشاملة من خلال السياسات أو العمليات الخاصة بالمصرف على وجه الخصوص، ويعد هذا البعد ضروريا في دمج استراتيجية المرونة السيبرانية في المصرف من خلال النظر في الأهداف الاستراتيجية والمخاطر الحالية والممارسات الإدارية بالنسبة لجميع هذه الأبعاد، أذ يشار بوضوح إلى الحاجة إلى مراجعة الضوابط وتحسينها (Tsena et al. 2023:6).

كما يشير مصطلح الحوكمة السيبرانية إلى الترتيبات التي وضعتها مؤسسة مالية او مصرف لإنشاء وتنفيذ ومراجعة نهجها في إدارة المخاطر السيبرانية، وينبغي أن تبدأ الحوكمة السيبرانية الفعّالة بإطار عمل واضح وشامل للمرونة السيبرانية يعطي الأولوية لأمن وكفاءة عمليات المصرف، ويدعم أهداف الاستقرار المالي، وينبغي أن يسترشد الإطار بالمرونة السيبرانية ويحدد كيفية تحديد أهداف استراتيجية المرونة السيبرانية، ويحدد متطلباتها من الموظفين والعمليات والتكنولوجيا لإدارة المخاطر السيبرانية والتواصل في

الوقت المناسب من أجل تمكين المصارف من التعاون مع أصحاب المصلحة المعنيين للاستجابة بفعالية للهجمات السيبرانية والتعافي منها. ومن الضروري أن يكون الإطار مدعوما بأدوار ومسؤوليات محددة بوضوح لمجلس إدارة المصارف وإدارتها، ويقع على عاتق مجلس إدارتها وإدارتها خلق ثقافة تعترف بأن الموظفين على جميع المستويات لديهم مسؤوليات مهمة في ضمان المرونة السيبرانية للمصرف.

إن الحوكمة السيبرانية القوية ضرورية لتنفيذ العمل المنهجي واستباقي لإدارة التهديدات السيبرانية السائدة والناشئة التي تواجهاالمصارف، كما أنها تدعم الجهود المبذولة للنظر في المخاطر السيبرانية وإدارتها بشكل مناسب على جميع المستويات داخل المصرف وتوفير الموارد والخبرات المناسبة للتعامل مع هذه المخاطر(NEPAL RASTRA,2023:10) .

2 – **الحماية:** Protection

ويشمل ذلك حماية الأنظمة والتطبيقات والبيانات والتأكد من أن المودعين المصرح لهم هم من يمكنهم الوصول إلى الأنظمة فقط، والمساعدة في تتبع المودعين بمجرد دخولهم إلى الأنظمة والوصول إلى خدماته كما تتعلق الحماية بالضوابط الفنية التي تحمي الوصول إلى أنظمة المصرف وسلسلة التوريد الخاصة بها وتركز وظيفة الحماية على تنفيذ الضمانات لضمان تقديم خدمات البنية التحتية الحيوية. وهذا يشمل تنفيذ الضوابط للحماية من التهديدات، مثل التحكم في الوصول، وأمن البيانات، والتدريب .(Dr. Isabella Lee. 2024:6)

2– **الكشف:** Disclosure

ويشمل ذلك اكتشاف نقاط الضعف في التطبيقات، وإيجاد أي نقاط ضعف يمكن استغلالها في المصرف بأية ضوابط تمكن من اكتشاف الحوادث السيبرانية، تساعد عناصر التحكم هذه المصرف على تطوير عملية الكشف بتحديد ومراقبة السلوك الأساسي ومقارنة السلوك الملحوظ ومراجعة الضوابط، وتركز وظيفة الكشف على تحديد وقوع حدث للأمن السيبراني، ويشمل ذلك تنفيذ عمليات المراقبة والكشف لتحديد أحداث الأمن السيبراني والاستجابة لها في الوقت المناسب (Tsena et al. 2023:6).

3– **الاستجابة:** Response

تتعلق الاستجابة بكيفية تخطيط المصرف للحادث السيبراني والاستجابة له والاسترداد من قبل المصرف فيما يتعلق بالحوادث السيبرانية، كما يشير هذا البعد الى كيفية تخطيط المصرف للحادث السيبراني والاستجابة له فضلاً عن وضع خطة استجابة تتضمن التواصل مع أصحاب المصلحة المعنيين، و تركز وظيفة الاستجابة على اتخاذ إجراءات للتخفيف من تأثير حدث الأمن السيبراني المكتشف. ويشمل ذلك

تطـــوير وتنفيـــذ خطـــط الاســـتجابة لاحتـــواء وتخفيـــف تـــأثير حـــوادث الأمـــن الســـيبراني (Dr. Isabella Lee. 2024:6).

يجب أن يكون لديك استراتيجية مخططة ومختبرة للاستجابة للحوادث، يجب أن تتضمن استراتيجية الاستجابة للحوادث الإجراءات التي ستتخذها المنظمة أثناء الهجوم الإلكتروني، ويجب أن تتضمن هذه الإجراءات تحديد الهجوم وعزل الأنظمة المتأثرة واستعادة الأنظمة والبيانات وإجراء تحقيق لتعزيز الأمن السيبراني، يجب على المنظمات التأكد من امتلاكها لاستراتيجية فعّالة ومختبرة للاستجابة للحوادث، إلى جانب تنفيذ التدابير الوقائية المناسبة (Tsena et al. 2023:6).

ومع ذلك لا تقتصر استراتيجية المرونة السيبرانية على منع الهجمات فحسب؛ بل يتضمن أيضا التعافي السريع للأنظمة والبيانات بعد الهجوم. ولذلك فإن استرنيحية المرونة ذات أهمية قصوى في مواجهة التهديدات الناشئة. ينبغي أن تكون المصارف قادرة على تكييف أنظمة وأساليب الأمن الخاصة بها بمرور الوقت، والتعلم من الحوادث السابقة وتحديد نقاط الضعف الجديدة، والعوامل ذات الصلة الأخرى. من خلال اتخاذ هذه الإجراءات التي تمكن المصارف من تعزيز استعدادها وقدرتها على التكيف في مواجهة الهجمات السيبرانية، وبالتالي تقليل مخاطر مثل هذه الهجمات وحماية نفسها من الخسائر المحتملة (G.A. Hubbard,. 2023:6).

يعد اكتشاف الحوادث وتحليلها (IDA) مرحلة رئيسية في الاستجابة للحوادث لأن الاستجابة لا يمكن أن تتجلى بدون اكتشاف دقيق، على الرغم من أن اكتشاف الحوادث يعتبر نهجا لرد الفعل، إلا أن هناك أحداثًا يمكن اكتشافها تسبق الحادث.

4 – الاسترداد والتقييم : Recovery

يشير بُعد التعافي إلى أي إجراءات يستخدمها المصرف لتمكين استمراره والتشغيل بعد الحادث السيبراني قد تمتد هذه الخطط والإجراءات أيضًا إلى التعلم وإعداد التنظيم للحوادث اللاحقة بتطوير الكفاءات والضوابط، وتتعلق الأبعاد الثلاثة الاتية بشكل مباشر أكثر بالجوانب غير التقنية لاستراتيجية المرونة السيبرانية وتركز وظيفة الاسترداد على استعادة قدرات أو خدمات المصرف التي تضررت بسبب حدث للأمن السيبراني، ويشمل ذلك تطوير وتنفيذ خطط الاسترداد ولاستعادة الأنظمة والبيانات ويرتبط التخطيط للتعافي من الكوارث ارتباطا وثيقا بالتخطيط لاستمرارية الأعمال وينطوي على وضع خطط لكيفية استرداد أنظمة تكنولوجيا المعلومات والبيانات في حالة وقوع هجوم إلكتروني أو كارثة أخرى. ويشمل ذلك تحديد إجراءات النسخ الاحتياطي والاسترداد، فضلاً عن اختبار هذه الإجراءات للتأكد من فعاليتها (Dr. Isabella Lee. 2024:6).

الحادي عشر – أهم التعاملات المصرفية المعرضة للتهديدات السيبرانية:

The most important banking services exposed to cyber threats

تعد التعاملات المصرفية الإلكترونية هدفاً للتهديدات السيبرانية، أذ يستغل المجرمون السيبرانيون التوسع في هذه الخدمات لشن هجمات متقدمة على المصارف والمؤسسات المالية، وسوف نبين أهم التعاملات المصرفية الالكترونية التي يستهدفها المجرمون السيبرانيون هي كالاتي (Kibrom Berhe, 2022:26) :(Kibrom & Berhes,2022:11)

1- **التعاملات المصرفية عبر الإنترنت:** Online banking

تشير التعاملات المصرفية عبر الإنترنت إلى الأنظمة التي تمكن مودعو المصارف من الوصول إلى الحسابات والمعلومات العامة عن خدمات المصارف من خلال جهاز كمبيوتر شخصي أو أي جهاز ذكي آخر.

2- **التعاملات المصرفية عبر الهاتف المحمول:** Mobile banking

وهي الخدمات التي تحدث عندما يصل المودعين إلى شبكة المصرف باستخدام الهواتف المحمولة أو أجهزة الاستدعاء أو المساعد الرقمي الشخصي أو الأجهزة المماثلة من خلال شبكات الاتصال اللاسلكية

3- **أجهزة الصراف الآلي (ATMs):** Automated teller machines ATMs

ماكينة الصراف الآلي هي ماكينة يمكن من خلالها سحب النقود من الآلة دون الدخول إلى قاعة المصرف كما أنها تبيع بطاقات إعادة الشحن وتحويل الأموال، ويمكن تقييمها على مدار 24 ساعة من الاستعلام عن رصيد الحساب (Fenuga, 2010:55).

4- **محطات تحويل نقاط البيع (POS):** Point of sale (POS) transfer stations

يتعامل هذا الجانب من التعاملات المصرفية الالكترونية مع التحقق من الشيكات وتفويض الائتمان والإيداع النقدي والسحب والدفع النقدي، اذ يعزز تحويل الأموال الإلكتروني في نقطة البيع ومن ثم ستخصم تكلفة الشراء على الفور من حساب المودع في أحد منافذ البيع مثل محطة بنزين أو سوبر ماركت ويدل ذلك أن المودعين يمكنهم سداد ثمن السلع والخدمات دون الحاجة بالضرورة إلى التعامل بالنقود المادية أذ سيخصم سعر الشراء من بطاقة المشتري وإيداعه في حساب البائع.

5- **التعاملات المصرفية عبر البريد:** Postal banking services

وهي خدمة مصرفية إلكترونية أخرى تتيح التواصل مع المصرف بالبريد الإلكتروني وتسخدم بشكل متكرر لإرسال كشوفات الحساب المتفق عليها الى صندوق بريد المودعين في المصارف بشكل دوري.

6- **خدمة الرسائل النصية (SMS):** Text messaging service (SMS)

تستخدم التعاملات المصرفية عبر الرسائل النصية القصيرة المرسلة عبر الهاتف المحمول الخاص بالمودعين، ويمكن استخدامها لكل من العمليات النشطة والسلبية بعد إجراء عملية معينة، كما يمكن للمودعين الحصول تلقائياً على معلومات حول رصيد حسابهم ويمكن للمصرف إرسال معلومات حول أسعار الفائدة الحالية وأسعار الصرف بناءً على طلب المودعين.

7- **خدمات بطاقات الائتمان:** Credit card services

تختلف بطاقة الائتمان عن بطاقة الخصم من حيث أنها لا تقوم بإزالة الأموال من حساب المستخدم بعد كل معاملة، وفي حالة بطاقات الائتمان يقوم المصرف بسداد المال للمودعين أو المستخدم ليدفع للتاجر، وتسمح بطاقة الائتمان للمودعين بتدوير رصيدهم على حساب تحصيل الفائدة وتشمل الأطراف المشاركة في معاملة بطاقة الائتمان حامل البطاقة، والمصرف الذي أصدر البطاقة والمصرف المستفيد ومنظمة المبيعات المستقلة وحساب التاجر وجمعية بطاقة الائتمان وشبكة المعاملات.

8- **بطاقات الخصم:** Debit cards

وهي البطاقات المعروفة باسم البطاقة المصرفية أو بطاقة الشيكات هي بطاقة بلاستيكية توفر طريقة دفع بديلة للنقد عند إجراء عملية التبادل.

من الناحية الوظيفية يمكن أن يطلق عليها الشيك الإلكتروني، أذ تسحب الأموال مباشرة من الحساب المصرفي أو من الرصيد المتبقي على البطاقة وفي بعض الحالات تصمم البطاقات حصرياً للاستخدام على الإنترنت، ومن ثم لا توجد بطاقة فعلية.

9- **التعاملات المصرفية بدون بطاقة:** Cardless banking services

تتيح التسهيلات المصرفية بدون بطاقة للمودعين سواء الذين لا يتعاملون مع المصارف أو لديهم حسابات مصرفية تحويل الأموال إلكترونياً باستخدام ماكينة الصراف الآلي أو كشك الخدمة الذاتية أو التعاملات المصرفيةعبر الهاتف المحمول أو الإنترنت.

الثاني عشر – الجرائم السيبرانية التي تهدد التعاملات الالكترونية بالمصارف:

Cybercrimes that threaten electronic transactions in banks

ان الجرائم السيبرانية هي التي تنطوي على استخدام الكمبيوتر والشبكات كوسيلة أو مصدر أو أداة أو هدف أو مكان للجريمة، ومع زيادة جوانب التجارة الإلكترونية والمعاملات الالكترونية تزايدت الجرائم السيبرانية على مستوى العالم ويمكن تصنيف الجرائم السيبرانية التي تتعرض لها المصارف وحسب الاتي :(Maireva, 2022:8)

1- **القرصنة:** Piracy

القرصنة هي جريمة تنطوي على كسر الأنظمة والحصول على وصول غير معتمد إلى المعلومات المخزنة فيها، وأصبح من الواضح مؤخرا ان عمليات القرصنة المرتبطة بواجهات محددة عبر الإنترنت يستحصل عليها من السجلات الخاصة بالبريد الإلكتروني للمودعين، والقراصنة هم الأفراد الذين يحاولون الحصول على دخول غير معتمد إلى أجهزة الكمبيوتر، ويكون ذلك بانتظام باستخدام برنامج الوصول غير المباشر المتوفر على اجهزة المودعين (Stamp, 2011: 12).

2- **انتحال البريد الإلكتروني:** Email spoofing

هو أسلوب لإخفاء المصدر الفعلي للبريد الإلكتروني بتزوير رأس البريد الإلكتروني ليبدو وكأنه مصدر شرعي واحد بدلاً من المصدر الأصلي الفعلي، ويشير الانتحال إلى الموقف الذي يكون جعل جهاز الكمبيوتر الخاص بشخص ما على الشبكة يعمل مثل جهاز كمبيوتر آخر، وعادةً ما يكون جهازاً يتمتع بحقوق وصول استثنائية وذلك للوصول إلى الأنظمة الأخرى الموجودة على شبكة الانظمة المصرفية .(Maireva, 2022:9)

3- **التصيد الاحتيالي:** Phishing

تهدف هجمات التصيد الاحتيالي إلى سرقة معلومات المستخدم مثل بيانات اعتماد المستخدم وأرقام بطاقات الائتمان وأرقام التعريف الشخصية للوصول إلى الحساب البنكي للضحية أو السيطرة على بيانات الشبكة الاجتماعية (Sujata& Joshi,2020:8).

4- **سرقة الهوية:** Identity theft

تعد سرقة الهوية نوع من الجرائم الإلكترونية حيث يحاول المتسللون الحصول على البيانات الشخصية الرئيسة مثل رقم الضمان الاجتماعي أو بطاقة الائتمان أو غيرها من البيانات المتعلقة بانتحال شخصية شخص ما والاستفادة من اسمه (Sujata& Joshi,2020:8)

ان سرقة الهوية هي فعل متعمد لانتحال شخصية شخص حي آخر لارتكاب عمليات احتيال تجارية أو مدنية أو جنائية من أجل الحصول على أموال شخص منتحل أو تعزيز جريمة باسمه أو الوصول بشكل غير مبرر للاستفادة منه (Bounaman & Al-Darisi, 2023:5).

5- **البرمجة النصية عبر المواقع:** Cross-site scripting

تعد البرمجة النصية عبر المواقع نوعا من نقاط الضعف في أمان الكمبيوتر الشخصي والتي يعثرعليها بانتظام في تطبيقات الويب التي تسمح بتسريب التعليمات البرمجية من قبل عملاء الويب الضارين في الصفحات التي يشاهدها عملاء مختلفون، وتشتمل مثيلات هذه التعليمات البرمجية على كود ومحتويات من جانب العميل، ويمكن للمهاجمين الاستفادة من ضعف الترتيب المسبق عبر المواقع لتجاوز ضوابط الوصول (Hasan & Alramadan, 2021:4).

6- **هجمات حجب الخدمة الموزعة:** Distributed DoS attacks

تعد هذه الهجمات نوعا من هجمات الجرائم الإلكترونية التي يستخدمها مخربو الإنترنت لقطع نظام أو تعطيل الخدمات المقدمة، وفي بعض الأحيان، تستخدم أجهزة شبكة الأشياء ذات الصلة لإرسال هجمات حجب الخدمة الموزعة (Thijeel et al., 2018:22).

7- **عمليات الاحتيال المتعلقة بالرسوم المسبقة:** Advance fee scams

عادةً ما تكون عمليات الاحتيال عبر الإنترنت هذه من خلال خطاب أو بريد إلكتروني أو مكالمة هاتفية تعرض مبلغاً كبيراً من المال إذا كان بإمكانك مساعدة شخص ما في تحويل ملايين الدولارات أو أي عملة أخرى خارج بلده، وعند بدء المعاملة يُطلب منك إرسال تفاصيل حسابك المصرفي ورسوم إدارية، ويكون بعد ذلك استخدام هذه التفاصيل المصرفية بشكل احتيالي من قبل المحتالين عبر الإنترنت (Maireva, 2022:8).

8- **مواقع الويب المزيفة والمقلدة:** Fake and imitation websites

هناك اتجاه جديد في الاحتيال عبر الإنترنت وهو ظهور مواقع الويب المزيفة او المقلدة التي تستغل المودعين النهائيين الذين لا يعرفون الإنترنت أو الذين لا يعرفون عنوان الويب الصحيح للمصرف، وعندما يقوم المودع بإدخال تفاصيل ائتمانية في قاعدة البيانات الشخصية من أجل شراء بضائع من الشركة المقصودة ببراءة يقوم بإدخال التفاصيل للمحتال ويتمكن المحتال بعد ذلك من الاستفادة من هذه المعلومات في مرحلة لاحقة إما لأغراضه الخاصة أو لبيعها للآخرين المهتمين بارتكاب الجريمة (Thijeel et al., 2018:22).

9- **المطاردة السيبرانية:** Cyber stalking

المطاردة عبر الإنترنت هي استخدام الإنترنت أو أي غرض إلكتروني آخر لمتابعة شخص ما، ويُستخدم هذا المصطلح بشكل متبادل مع التضليل وسوء المعاملة عبر الإنترنت، وتتضمن المتابعة بشكل عام السلوك المزعج الذي يشترك فيه الفرد بشكل متكرر مثل ملاحقة شخص ما أو الظهور في منزل الفرد أو بيئة عمله، أو اتخاذ قرارات هاتفية مزعجة أو ترك رسائل مكتوبة أو احتجاجات أو تخريب ممتلكات الفرد (Hasan & Alramadan, 2021:2).

10- **أدوات الفدية:** Ransom ware

وهي من أبرز التهديدات التي يواجها الفضاء الإلكتروني، وهذا نوع من البرامج الضارة المصممة لمنع الوصول إلى جهاز كمبيوتر أو مجموعة من أجهزة الكمبيوتر حتى يدفع مبلغ من المال، اذ إنهم يهددون بنشر بيانات حساسة حتى يتم دفع مبلغ من المال للمهاجمين (Bounaman & AlDarisi, 2023:5).

11- **الفيروسات وأحصنة طروادة:** Viruses and Trojans

ان الفيروسات ليست سوى ثمن شيفرات خبيثة تنسخ نفسها كالفيروس البشري دون مساعدة الإنسان، اذ ان الفيروس طفيلي يمكن أن يلوث مجموعة الكمبيوتر وهو مرتبط ببرنامج ما، وهو عرضة لإجراء اضطرابات طبيعية أثناء عمله، ويعد حصان طروادة هو برنامج يبدو شرعياً ولكن عندما يفتح يسمح بإصابة البرنامج أو التحكم في الكمبيوتر، ويمكن أن يسبب الكثير من الأشياء، ويعد نوعا من انواع البرامج الضارة المصممة بشكل أساسي لسرقة المعلومات المالية والمصرفية للمستخدمين من رسائل البريد الإلكتروني العشوائية (Bounaman & Al-Darisi, 2023:5).

" المبحـــــث الثاني "

ثقة المودعين

توطئة:

شهدت التعاملات المصرفية عبر الإنترنت والمعروفة بالتعاملات المصرفية الإلكترونية نمواً هائلاً في السنوات الأخيرة، وتعد ثقة المودعين عاملا مؤثرا في الولاء المصرفي من الناحية النظرية والتجريبية حتى أن مثل هذه الابتكارات التكنولوجية السريعة اخترقت العديد من القطاعات بما في ذلك المصارف.

أدركت المصارف أهمية اعتماد التكنولوجيا كمحرك رئيسي في تعزيز التعاملات والخدمات التي تقدمها ولذلك فإن الحاجة إلى اعتماد التكنولوجيا في أماكن العمل المتنوعة، بما في ذلك التعاملات المصرفية التي تنبع من دور التكنولوجيا في تقديم التعاملات المصرفية المختلفة وتسريع أداء المصارف وتقليل النفقات غير الضرورية وتحقيق كفاءة الإنتاجية كنتيجة مهمة لاعتماد التكنولوجيا في التعاملات المصرفية ومن ثم يؤدي استخدام التكنلوجيا الى سهولة التبادلات المصرفية وهذا ينعكس على رضا المودعين وزيادة ثقتهم.

اولاً – مفهوم ثقة المودعين:

The concept of depositors confidence

وتُعرَّف الثقة بأنها افتراض أو انتظار أو اعتقاد أو رغبة أو سلوك، وتظهر كمفهوم متعدد الأشكال، واستنادا إلى التأملات المبكرة تم تحديد نهجين سائدين في الأدبيات بواسطة Smith and Barclay . في النهج الأول، تُعرَّف الثقة بأنها حالة نفسية تسبق النية السلوكية (اعتقاد انتظار افتراض). وفي النهج الثاني يُنظَر إليها باعتبارها نية أو سلوكا (الاستعداد للاعتماد على سلوكيات الشريك الواثق). وبالتالي فإن التصنيف الذي يمكن تقديمه هو أن الثقة كمتغير نفسي يدمج العمليات المعرفية والعاطفية في مفهوم الثقة كمتغير سلوكي (Smith & Barclay,1997:217).

يمكن التعرف على العديد من مفاهيم ثقة المودعين المختلفة في الأدبيات العلمية، لذلك من الضروري تحليل مفاهيمها والعوامل التي تحددها، اذ قام أكاديميون (اقتصاديون ومديرون، وعلماء نفس، وعلماء اجتماع) من مختلف المجالات بتحليل ثقة المودعين، واصبح من الضروري تعريفها والتحقق منها بشكل مناسب في النظام المصرفي من الجانب النفسي والاقتصادي لأن المودع له دور اساسي في هذه العلاقة التي تنشأ بينه وبين المصارف التي يتعامل معها، ولا تتأثر قراراته فقط من العوامل الاقتصادية فحسب ولكن من الجوانب النفسية، ونتيجة لذلك فإن غالبية تعريفات ثقة المودعين هي عبارة عن تفاعل بين التعبيرات النفسية والاقتصادية للسلوك البشري، وهناك علماء يعرّفون ثقة المودعين بأنها التنبؤ بالسلوك الفردي المستقبلي

وتعتمد على يقين المودعين بأن المديرين الذين يساعدون مودعيهم سيتخذون إجراءات ضرورية لصالح مودعيهم (Gil,etal,2006 :12).

عرفت ثقة المودعين على أنها اعتقاد أو توقع الفرد أن طرف آخر (المصرف) سوف يقوم بعمل معين للحفاظ على امواله في حالة غيابه (Al-Saghi et al, 2009:298).

وتعبر ثقة المودعين عن تصورات المستفيدين من الخدمات تجاه مجموعة من الخصائص التي يتمتع بها مقدمي هذه الخدمات من القدرة والكفاءة والنزاهة والاخلاص والقدرة على الاعتماد على شريك التبادل فى كافة الظروف والاوضاع (Deng, Zhaohua 2010:).

وتعد ثقة المودعين مفهوم ديناميكي متغير يشتمل على مرحلتين مختلفتين، الأولى هي الثقة قبل توظيف التكنولوجيا (ثقة ما قبل الاستخدام) والثانية هي الثقة بعد توظيف التكنولوجيا(ثقة ما بعد الاستخدام)، فكلا النوعين يعدل من سلوك المستخدم للتكنولوجيا ، ففي حالة ثقة المودعين ما قبل الاستخدام تؤثر على نوايا المستخدم نحو تبني التكنولوجيا وقبولها، بينما تقوم ثقة ما بعد الاستخدام بتعديل نوايا المستخدم للإستمرار في استخدام التكنولوجيا(Hernandez, 2011:7).

وعرفت أيضا على أنها رغبة من جانب المودع في إجراء معاملات عبر الأنترنت لتلبية احتياجاته المصرفية مع توقع أن المصرف سيفي بالتزاماته (Qamar, et al., 2012: 82).ويعتبر مفهوم ثقة المودعين تجسيد الأفكار والعواطف والمشاعر والسلوك الذي يحصل عند شعور المودعين بأن مقدم الخدمة يمكن الاعتماد عليه في تحقيق مصالحهم بكفاءة وذلك بتلبية احتياجاتهم وتوفير الخدمات التي تخلق قيمة للمودعين (Vuuren, et al, 2012: 88). كما يمكن تعريفها على أنها درجة إيمان وتقبل المودع للقرارات والسياسات التي يضعها المصرف والتي يقوم بتنفيذها وادارتها بشكل عادل لجميع الأطراف (Yap et al ., 2012 :157).

وتعرف ثقة المودعين على أنها اعتقاد المودع أن جهة أخرى (المصرف) سوف تؤدي بعض الأعمال والخدمات وفق توقعاتهم، وعرفت ايضاً على أنها الشعور بالأمان من شعور أحد الطرفين بأن سلوك الطرف الأخر منقاد بشكل واضح لخدمة مصلحته (Raewf & Thabit, 2017:54). كما عرفت ثقة المودعين على أنها مقدار ومدى ارتياح المودعين أو الأمان الذي يشعرون به عند استخدام التعاملات المصرفية الالكترونية سواء عبر الأنترنت أو بالهاتف المحمول وغيره من قنوات التوزيع الإلكترونية الأخرى (بسمة، عفاف,2022: 49).

ثانياً: – اهمية ثقة المودعين: The importance of depositor confidence

تعد الثقة في النظام المصرفي مسألة مهمة ولذلك ينبغي إعادة بناء ثقة المودعين في المصارف التجارية. قد لا تؤدي مستويات الثقة العالية إلى تقليل التكاليف التعاقدية فحسب بل قد تؤدي أيضاً إلى تقليل التكاليف القانونية بتقليل التقاضي، وتقلل الثقة من تكاليف الوكالة وتكاليف المعاملات في العلاقات المصرفية مما يدل على أن الثقة هي أحد أهم العناصر التي تحدد تطور العلاقات التجارية المستقبلية في النظام المصرفي (Jureviciene & Skvarciany, 2013:1).

كما تعد ثقة المودعين في المصارف أمراً بالغ الأهمية خاصة في الأوقات المضطربة وهي حيوية للحصول على مصالحهم الشخصية من قبل تلك المصارف (Bijlsma & Koldijk, 2022:17).

تعد الثقة أمراً مهماً للعلاقات بين المودعين والمصرف وللعلاقات مع المودعين بشكل عام، اذ يمكن للثقة ان تسهل المعاملات الخاصة بالمودعين ولا داعي للقلق بشأن مصالحهم الشخصية ومدخراتهم لدى المصرف وارصدتهم المالية التي اودعوها أو التي يخططون لإيداعها في المصرف والتي تشمل الاستثمار والودائع والتأمين والرهون العقارية، ومع وجود مستوى عالٍ من الثقة يشعر المودعين بأن المصرف يخدم مصالحهم بشكل جيد إلى حد ما ويعد المستوى العالي من الثقة بمثابة حاجز ضد التجارب السلبية التي يمكن أن تنشأ بين المودعين (Hurle &Wagar 2014:48).

تعد الثقة التي يضعها المودعون في المصارف ضرورية للوصول إلى الخدمات المالية والشمول للأفراد وكذلك لتجميع المدخرات وتوسيع الائتمان من قبل المصارف (Fungacova et al, 2022:94).

يؤدي انخفاض الثقة إلى الحد من الوصول إلى التعاملات المصرفية بالنسبة للمودعين، لذلك يعد المودعين الذين لديهم مستويات منخفضة من الثقة هم أقل عرضة لامتلاك حساب توفير ولديهم تفضيلات سيولة أقوى من المودعين ذوي مستويات أعلى من الثقة (Kruijsen et al., 2021:6).

وأصبحت مسألة ثقة المودعين في النظام المصرفي ذات أهمية كبيرة بين السلطات التنظيمية (Cruijsen, 2022:31). تعد ثقة المودعين في المصارف عاملاً مهماً يضمن نجاح العمليات المصرفية وتطويرها وتوفير تعاون مصرفي استهلاكي وتجاري مستمر وعالي الجودة (Jureviciene & Skvarciany, 2013:1).

عندما تنخفض ثقة المودعين في الصناعة المصرفية، فسيختار المودعون التعامل بشكل أقل مع المصارف الأمر الذي سيؤدي إلى الإضرار بكل من الصناعة المصرفية والاقتصاد بتقليل توافر رأس المال للأغراض الإنتاجية، فضلاًعن ذلك عندما تبدو تفاعلات المودعين ذات مستوى منخفض لا يُنظر إليها على أنها غير

ناجحة فحسب بل تؤدي أيضاً إلى اعتقادات غير مناسبة للثقة من قبل المودعين (Kruijsen et al, 2022:9).

تشير الدراسات المصرفية على نطاق واسع إلى أن الثقة في النظام المصرفي تتطور عندما يرى المودعين بتلبية احتياجاتهم والوفاء بالوعود المقدمة لهم (Tafanish, 2019:17).

وجد Lombard & Petzer أن توجيه المودعين ومشاركة المعلومات وعدالة الخدمة أمر بالغ الأهمية لتعزيز ثقة المودعين، ويمكن أن يؤدي عدم ثقة المودعين إلى قيام عدد كبير من المودعين بسحب أموالهم من المصرف بسبب قلقهم من فشل المصرف وهذا يؤدي إلى تعريض الاستقرار الاقتصادي للخطر من خلال بالتسبب في افلاس المصارف ومن ثم حدوث أزمة مالية أعمق (Lombard & Petzer, 2021:31).

يفتقر المودعون إلى الأمان عندما لا تتحقق الثقة اللازمة للمشاركة الكاملة مع المؤسسة المالية (المصرف) مما قد يعيق قدرتهم على تجربة التعاملات المصرفية، ومع ذلك لمنع هذه الآثار تحتاج المصارف إلى إعطاء الأولوية للشفافية والأمن والسلوك الأخلاقي وخدمة المودعين القوية للحفاظ على الثقة وتعزيزها (Lombard & Petzer, 2021:31).

ويرى Esterik أن للثقة اهمية كبيرة للعلاقة بين المودعين والمصرف وللعلاقات مع المودعين بشكل عام وذلك للأسباب الاتية (Esterik,2017:97):

1- تسهل الثقة المعاملات الإلكترونية والتقليدية مع المودعين، فلا داعي لأن يقلق المودعون بشأن رعاية مصالحهم الشخصية ومدخراتهم لدى المصرف والخدمات المالية التي يقدمها المصرف.

2- ان الثقة تحقق شعورا لدى المودعين بأن المصرف سوف يخدم مصالحهم.

3- يعد المستوى العالي من الثقة بمثابة حاجز ضد التجارب السلبية التي يمكن أن تنشأ بين المودعين اذ يميل المودعين إلى التغاضي عن التجارب السلبية وعدها استثناء إذا كانوا يثقون في المصرف، أما إذا كان مستوى الثقة منخفضا قد يُنظر إلى عدم الوثوق في المصرف.

4- تساعد الثقة في جذب زبائن جدد والاحتفاظ بالمودعين الحاليين.

5- تساهم الثقة في إعطاء استمرارية العلاقة وخلق مشاعر الولاء، ومن ثم كلما زادت ثقة المودع في المصرف والموظفين زادت احتمالية مشاركته في تعاملات مستقبلية والحفاظ على علاقة طويلة الأمد.

ثالثاً – عوامل بناء ثقة المودعين بالمصارف :

Factors for building depositors' confidence in electronic commerce

الثقة مفهوم حظي بالاهتمام في العديد من المجالات المختلفة في العلوم الاجتماعية والأدب وعلم النفس وعلم الاجتماع والعلوم السياسية والاقتصاد والمختارات والتاريخ وعلم الاجتماع الحيوي (Lewicki and) لأنها تنطوي على معلومات شخصية ومالية، والتي تتم في بيئة افتراضية تتميز بعدم اليقين ونقص السيطرة والانتهازية المحتملة، والثقة ضرورية لتبادل العلاقات عبر الإنترنت لأنها تنطوي على معلومات شخصية ومالية، والتي تتم في بيئة افتراضية تتميز بعدم اليقين ونقص السيطرة والانتهازية المحتملة (Hoffman et al, 1999:).

1 – **العوامل الاقتصادية:** Economic factors

تعتمد الثقة في المؤسسات المالية على العوامل الاقتصادية: فهي تتحرك بشكل دوري. وقد أجرى ستيفنسون بحثاً عن الثقة في المصارف والمؤسسات المالية وفي المصرفيين في الولايات المتحدة ووجدا علاقة سلبية قوية مع معدل البطالة، وقد تأكدت هذه العلاقة الدورية من خلال تحليل عبر البلدان لـ 98 دولة: فقد شهدت البلدان التي شهدت أكبر ارتفاع في البطالة أيضاً انخفاضاً حاداً في الثقة في المؤسسات المالية والمصارف وتزداد هذه الصلة قوة في بلدان منظمة التعاون الاقتصادي والتنمية (Stevenson & Wolfers, 2011:52).

وحدد Centeno مجموعة من العوامل المرتبطة ببناء ثقة المودعين في التجارة الإلكترونية وتنقسم إلى عدة عوامل على النحو الاتي (Centeno,2002:2):

1- **عوامل ما قبل التفاعل:** Our factors before interaction

يقوم المودعون ببناء ثقتهم بعد النظر إلى كل من العلامة التجارية والسمعة الحالية للمصارف، ويتعلق الأمر بتجربتهم الخاصة في العالم غير المتصل بالإنترنت وأي نصيحة أو تجربة تلقوها من مصادر المعلومات الموثوقة (الكلام الشفهي ووسائل الإعلام التقليدية).

2- **عوامل واجهة المستخدم:** User interface factors

يتضمن ذلك التصميم والصورة والاحترافية وسهولة الاستخدام والفعالية وسهولة التصفح، وإذا كان الموقع يستخدم لغات أصلية، فإن هذا يجعل الناس يثقون في التجارة الإلكترونية.

3- **عوامل معلومات الموقع:** Location information factors

أن نهج الشفافية في وصف وتحديد موقع ومعلومات المصارف بما في ذلك العنوان الفعلي وبيانات الاتصال وأرقام الاتصال بخدمة الزبائن والارتباط بالشركات الموثوقة فيما يتعلق بأمنها مثل حماية وخصوصية البيانات وبيانات سياسة الأمان كل هذه المعلومات هي عوامل تؤثر على ثقة المودعين باختيار المصرف.

4- **عوامل التفاعل مع الشراء:** Factors of interaction with purchas

ان الثقة في التجارة الإلكترونية تتأثر بعناصر مثل الشروط والأحكام التعاقدية والتسعير الواضح (بما في ذلك تكاليف التسليم والضرائب) وسياسة الإرجاع المحددة بوضوح (الإجراء، والتكاليف، والسداد) والقدرة على التراجع للمعاملة والأختام الأمنية (مثل شعارات بطاقات الائتمان، وعلامات الثقة) وتوفير طرق دفع بديلة بمستويات مخاطر مختلفة للمودعين (الدفع عند التسليم، وبطاقات الائتمان، وما إلى ذلك) واستخدام التكنولوجيا الحديثة (التشفير). وقد أجرى Kolsaker and Payne بحثا حول توليد ثقة المودعين في التجارة الإلكترونية، وقد وجد أن المستجيبين بشكل عام أظهروا قلقا بشأن الأمن وسرية المعلومات والنزاهة الإرجاع والاسترداد في بناء الثقة، ومن حيث الاختلافات بين الجنسين، كشف البحث أيضًا أن الرجال أكثر اهتمامًا بالأمن، خاصة عندما يتعلق الأمر بالمدفوعات الإلكترونية، ومن ناحية أخرى فإن النساء يكن اهتماما خاصا بسرية المعلومات والنزاهة في المصارف(Kolsaker& Payne,2003:78).

وقد حدد باتوكوربي وكيمبا (2006) أن نجاح الثقة عبر الإنترنت هو مزيج من أربعة عناصر أساسية، وهي: السمعة والتكنولوجيا والخبرة والعلاقة.

رابعاً – العناصر المعرفية والعاطفية لثقةالمودعين بالمصارف

Cognitive and emotional elements of depositors' trust in banks

لقد كان مفهوم الثقة محل اهتمام العديد من العلماء في جميع أنحاء العالم وتم البحث فيه على نطاق واسع عبر مختلف التخصصات بما في ذلك الاقتصاد وعلم الاجتماع والعلوم السياسية وتكنولوجيا المعلومات وعلم النفس. على مر السنين، وتعد العناصر المعرفية والعاطفية للثقة هي نوع آخر من الثقة المقترحة، وأن الثقة تسهل الاحتفاظ بالمودعين وولائهم. لذلك يُنظر إليها على أنها متغير مهم للغاية في التفاعلات البشرية ولهذا قسمت الى نوعين من العناصروحسب الاتي:

1- **عناصر الثقة المعرفية:**

تتكون العناصر المعرفية من ثلاثة أنواع هي ثقة النزاهة، وثقة الكفاءة، وثقة حسن النية أو الإحسان"و يُعرَّف عنصر النزاهة في الثقة المعرفية بأنها فعل الوفاء بالوعود، بناءً على القاعدة الأخلاقية للصدق وبالتالي يمكن القول إن "ثقة النزاهة" هي ثقة تعاقدية وثقة التزام وثقة وعد (Albaum&Young ,2002:63).

يعتبر العنصر الثاني للثقة المعرفية هو "ثقة الكفاءة"، والتي تُعرف أيضاً باسم ثقة القدرة وثقة الخبرة ويرى Punyatoya ثقة الكفاءة بأنها المدى الذي يعتقد فيه أحد الطرفين أن شريكه في التبادل لديه الخبرة المهنية المطلوبة والمهارات ذات الصلة والمؤهلات والخبرة لأداء الوظيفة بشكل فعال، اما العنصر المعرفي الثالث للثقة هو "ثقة حسن النية أو الإحسان"، وقد عرّفها Punyatoya بأنها مدى الاعتقاد في شخص أو منظمة بأن مصلحة ما (Punyatoya ,2019 :28).

2- **عناصر الثقة العاطفية:**

تتضمن الثقة القائمة على "العاطفية" الروابط العاطفية والمهارات الاجتماعية المرتبطة بالرعاية والاهتمام بالطرف الآخر (Yang.etal.,2019:). واقترح Yang عنصرين للثقة العاطفية، وهما: "الثقة العلائقية" و"الثقة الحدسية"، الثقة العلائقية هي جانب من جوانب الثقة العاطفية المرتبطة بقاعدة المعاملة بالمثل ولها علاقة بالإيمان بالطرف الآخر، ويرى إنها تشبه إلى حد كبير الاعتقاد الديني، مع الإيمان الملقى على الشريك الآخر بأنه سيتصرف كما ينبغي، بطريقة جديرة بالثقة،وتعد بأنها تقييم غير عقلاني للثقة يعتمد على قاعدة المعاملة بالمثل وليس على المعرفة أو التقييم الفعلي للسلوكيات الماضية

في حين أن "الثقة البديهية" تتعلق بالأحكام المتحيزة القائمة على الحالات المزاجية والمشاعر حول شخصية شخص آخر(Yang et al., 2019:).وهنالك مجموعة من العناصر الخاصة بثقة المودعين بالمصارف الالكترونية والتي هي :

عد Patokorpi and Kimppa أن نجاح ثقة المودعين عبر الإنترنت هو مزيج من أربعة عناصر أساسية، وهي: السمعة والتكنولوجيا والخبرة وبناء العلاقات وهي (Patokorpi& Kimppa ,2006:17):

1- **السمعة:** Reputation

الأولى التي ينبغي على المصارف الإلكترونية أن تأخذ بالحسبان، فمن المفترض أن السمعة هي أهم عامل في خلق الثقة للزبائن الجدد، وتتمتع الأعمال الإلكترونية ذات العلامة التجارية أو السمعة القوية بالسبق مقارنة بالمواقع التجارية الأخرى.

2- **التكنولوجيا:** Technology

وهو احد العناصر الذي يمكن منه تصور مصداقية التكنولوجيا والذي يتغير بمرور الوقت من فرد إلى آخر مما يجعله عنصراً متقلبا لبناء ثقة المودعين، ويُنظر إلى تصميم الويب هنا على أنه جزء من التقنية المنفذة عبر الإنترنت، ويتضمن تصميم الويب مسائل تتعلق بالصورة والإدراك لفهم المودعين للتكنلوجيا.

3- **الخبرة:** Experience

يمكن ربطها بأي من العناصر الثلاثة الأخرى، وإن المنتج والخدمة والمعاملة والتسليم والموقع الإلكتروني المتقن الصنع سوف يغرس الثقة لدى المودعين، وينبغي أن تكون الخدمة والتسليم في الوقت المناسب وأن يكون الوقت نفسه مقبولاً للمستخدم، ويجب أن يزود موقع الويب المودعين بمعلومات دقيقة وفي الوقت المناسب ويجب أن يكون من السهل التنقل فيه لتمكين المودعين من العثور بسهولة وسرعة.

4- **بناء العلاقات:** Building relationships

في التجارة الإلكترونية تكون العلاقة غير واضحة بين المصارف والمودعين وكذلك مع شركاء الأعمال الآخرين، ان العلاقة الوثيقة ليست بالضرورة علاقة جيدة عندما يستخدم المودع غير متصل بالإنترنت لأول مرة خدمات المصرف عبر الإنترنت، يكون لديه فهم المصرف ومنتجاتها والعلاقة بينهما، ويُنظر إلى "الثقة" على أنها سابقة تؤثرعلى تطور العلاقة ومع ذلك فأن العلاقة المستقرة يمكن أن تؤثر على ثقة المودعين أيضا، وأن الثقة تساعد الشركاء على بناء الثقة في العلاقة من الفترة الأولية على مدى فترة طويلة جداً، حتى أن البعض زعموا أنها البناء الرئيسي في عملية تطور العلاقة ،وأن "المودعين الذين يعتمدون على مصرف موثوق قد يقيمو علاقة طويلة الأمد معه وتزيد ثقتهم بالمصرف (Hollebeek & Macky, 2019:55).

رابعاً: – انواع الثقة في المصارف :

Types of trust in electronic banks

تُعَد الثقة الركيزة الأساسية التي تُبنى عليها إدارة التعاملات في أي عمل تجاري. ولا يمكن المبالغة في التأكيد على تأثير الثقة على التعاملات المصرفية. وبالتالي، يُنظر إلى الثقة باعتبارها عاملاً رئيسيًا في تطوير وتعزيز العلاقة بين المصرف والمودعين، وبناءً على ذلك حددت هذه الدراسة جوانب مختلفة للثقة في الصناعة المصرفية. وتشمل هذه: الثقة في موقف السيولة المصرفية، والثقة في الوفاء بوعود البنك، والثقة في أنظمة الاتصالات المصرفية، والثقة في موظفي البنك، والثقة في عمليات تقديم الخدمات المصرفية، والثقة في المعاملات المصرفية عبر الإنترنت، والثقة في أنظمة الأمن المادي والسيبرانية للبنك. يتم تقديم هذه الجوانب أدناه:

هناك عدة انواع من الثقة بالمصارف بشكل خاص وبالنظام المصرفي بشكل عام وعلاقتها بشخصية المودعين والتي تتمثل بالاتي (Rajablina,2011,22)، (Lova Rajabelina,2011:33)

: (Karim Foluhonso et al,2021:8)

1- **الثقة بين المصارف:** Trust between institutions

تنشأ هذه الثقة بين المؤسسات المختلفة التي تربطها علاقات تعامل فيما بينها، وهذا النوع من الثقة هو الاخر يركز على سمعة المصرف وكفاءته، وتشمل التعاملات الالكترونية في اغلب الدراسات التي تطرقت إلى موضوع الثقة بين المصارف ومحدداتها والنتائج المترتبة عليها.

إن الثقة في وعود المصارف هي مجال آخر من مجالات ففي بداية أي علاقة تعاقدية، يكون لدى كل مصرف اتفاقية مستوى خدمة يعد فيها دائما بتقديم الخدمات للمودعين. ومن المؤسف أن البنوك غالباً ما تواجه العديد من التحديات الداخلية والخارجية التي قد تمنعها من الوفاء بوعود مستوى الخدمة المتفق عليها مع المودعين. وقد تكون التحديات الداخلية قرارات إدارية خاطئة، أو تخطيط غير كافٍ للطوارئ، أو عدم الأمانة من جانب إدارة المصرف، أو موقف الموظفين، أو تصميم وعود غير قابلة للتحقيق لكسب ثقة المودعين وما إلى ذلك. وقد تكون التحديات الخارجية هي الوضع الاقتصادي، والسياسات الحكومية، والمتطلبات التنظيمية، والاحتياجات المتغيرة للمودعين بشكل متكرر، وتشير النتائج إلى أن المصارف التي تفي دائماً بوعودها الخدمية ستكسب ثقة المودعين أكثر من المصارف التي تفشل باستمرار في الوفاء بوعودها، لذا عندما يتم الوثوق في المصرف في الوفاء بالوعود، سيكون المودعين على استعداد للحفاظ على علاقة طويلة الأمد مع مثل هذا المصرف (Rajablina,2011,22).

2- الثقة في أنظمة الاتصالات المصرفية:

في عالمنا الرقمي في القرن الحادي والعشرين اليوم، أصبحت المصارف مفتوحة للعديد من وسائل الاتصال للوصول إلى مودعيها, ويمكن للمصارف الوصول إلى مودعيها من خلال مجموعة متنوعة من الوسائط الإلكترونية مثل Facebook وTwitter وInstagram وWhatsApp وLinkedIn والبريد الإلكتروني والرسائل النصية والمكالمات الهاتفية, يعتمد استخدام هذه الوسائط للتواصل بشأن قضايا الخدمات المالية والتسويق للعملاء إلى حد كبير على قدرات الموظفين والمصارف ويختلف هذا الاستخدام من مصرف إلى آخر.

أن قدرة المصرف على استخدام أي من هذه الوسائط بصورة دقيقة تؤثر بشكل إيجابي على ثقة المودعين في المصرف، ويساعد هذا المصارف على تطوير علاقة طويلة الأمد مع المودعين، لذلك فإن المصارف التي تحاول بناء ثقة طويلة الأمد مع مودعيها، ستسعى دائماً إلى إنشاء نظام اتصال موثوق به بين المصارف ومودعيها وهذا ضروري لتسهيل التفاهم والود والاتفاق المتبادل الذي من شأنه أن يدعم هدف تعزيزالثقة للمصرف، على سبيل المثال فإن إبلاغ التغييرات في رسوم المصرف للمودعين قبل تنفيذهاسيعزز ثقة المودعين في المصرف، كما أن استخدام الرسائل القصيرة لإخطار المصارف بمعاملاتها بناءً على طلباتها من شأنه أن يبني الثقة، وبالتالي عندما يتم خصم أو إضافة مبلغ معين من المال إلى حساب المودع، يتم إرسال رسالة قصيرة إليه لتأكيد إتمام المعاملة بنجاح، وهذا النوع من الاتصالات في الوقت الفعلي بين المصارف وعملائها يعززالثقة المصرفية(Karim Foluhonso et al,2021 :8).

3- الثقة في موظفي المصرف:

يلعب موظفو المصرف دوراً رئيسياً تعزيز ثقة المودعين في المصرف، لذا فإن الثقة في قدرة موظفي المصرف على تقديم الخدمات المالية المتوقعة تؤثر بشكل إيجابي على تطوير العلاقة بين الطرفين، وبالتالي، فإن الموظفين الذين يتمتعون بمهارات تفاعل عالية وموقف جيد تجاه المودعين هم أكثر عرضة لكسب ثقة المودعين من أولئك الذين لديهم مهارات تفاعل منخفضة وموقف سيئ تجاه المودعين.

يلعب التزام موظفي المصارف بتقديم الخدمات المالية أيضاً دوراً أساسياً في تطويروتعزيز الثقة عندما يكون موظفو المصارف ملتزمين، فإنهم يميلون إلى إظهار التعاطف وبذل جهد إضافي لإرضاء المودعين، مما يعزز الثقة طويلة الأجل، لذلك، يجب على المسؤولين التنفيذيين في إدارة المصرف مراقبة مهارات موظفي المصرف ومواقفهم والتزاماتهم وتفاعلاتهم مع المودعين باستمرار (Rajablina,2011,22).

4- الثقة في التعاملات المصرفية عبر الإنترنت:

لقد أدى إدخال التكنولوجيا الحديثة المبتكرة إلى إدخال طريقة جديدة لكيفية تقديم المصارف للخدمات المالية للمودعين، وبالتالي كيفية إتمام المعاملات المصرفية عبر الإنترنت تؤثر بشكل كبير على ثقة المودعين بالمصارف، تزاد ثقة المودعين واستعدادهم للمشاركة في المعاملات المالية ذاتية الخدمة عبر الإنترنت إذا كانت منصة المصرف عبر الإنترنت آمنة وموثوقة وأسهل وأسرع وأكثر ملاءمة، ان جودة التعاملات المصرفية عبر الإنترنت والخدمات المصرفية عبر الهاتف المحمول ونقاط البيع (POS) ومعاملات ماكينة الصراف الآلي (ATM) كلها لها تأثيرات على تعزيز ثقة المودعين في المصارف، وبالتالي فإن المصارف التي تقدم خدمات أجهزة الصراف الآلي على مدار الساعة طوال أيام الأسبوع دون انقطاع مع تقليل ازدحام النقد أثناء سحب النقود من أجهزة الصراف الآلي من المرجح أن تكتسب ثقة المودعين التي ستبقيهم لفترة طويلة مع المصرف (Lova Rajabelina,2011:33).

5- الثقة في الأمن المادي والسيبراني للمصرف:

يعتبر الأمن السيبراني مصدر قلق كبير للعديد من مستخدمي الإنترنت في جميع أنحاء العالم، في مجال التعاملات المصرفية، يهتم المودعون أكثر بأمن أنشطتهم المصرفية عبر الإنترنت؛ لتجنب خسارة الأموال وهذا الشعور بالتهديدات السيبرانية يخلق انعدام الثقة ويتجنب معظم المودعين استخدام منصات التطبيقات عبر الإنترنت للمصارف لمعاملاتهم المالية، أن المودعين سيتحققون دائماً من فعالية تدابير الأمن السيبراني لمصارفهم قبل الدخول في علاقات مصرفية عبر الإنترنت تعاقدية. وفقًا لذلك، فإن المصارف التي لديها أقوى تدابير الأمن المعمول بها هي أكثر عرضة لكسب ثقة المودعين من المصارف ذات التدابير الأمنية الضعيفة، وذلك لأن المودعين لن يكونوا على استعداد للمخاطرة بأموالهم ومدخراتهم أثناء إجراء المعاملات على منصة تطبيقات مصرفية عبر الإنترنت غير آمنة، لذلك من الضروري أن توفر المصارف دائماً تدابير أمنية مادية وسيبرانية كافية لحماية الأرواح والممتلكات داخل وخارج مباني المصرف، لتعزيز ثقة المودعين في القطاع المصرفي (Karim Foluhonso et al,2021 :9).

سادساً:- محددات ثقة المودعين بالتعاملات المصرفية:

Determinants of depositors' confidence in electronic banking services

أصبح من الضروري أن تعمل المصارف على زيادة ثقة المودعين بحثهم على الاستثمار والادخار لديها، فكلما زادت المبالغ النقدية المودعة في المصارف زادت سيولة المصرف ومن ثم يؤدي الى زيادة الثقة لدى المودعين، وعلى المصارف أن تنتبه إلى العوامل التي تزيد من ثقة المودعين وتجعلهم يختارون ويفضلون مصرفاً على آخر، وبما أن المصارف هي أيضا تقدم مجموعة متنوعة من الخدمات فقد وضع المودعون معايير معينة لاختيار المصارف التي يضعون فيها أصولهم وأموالهم (Grundke & Kühn, 2020:167).

إن المعلومات المتاحة لكل من المودعين المحتملين والحاليين وتأثير أفراد المجموعة الاجتماعية قد تكون العامل الأكثر أهمية في جذب وزيادة ثقة المودعين في المصارف والاحتفاظ بهم (Adekiya & Gawuna, 2015:154).

ان تصورات المودعين حول نقاط القوة التنظيمية والإدارية للمصرف تعد مؤشرا موثوقاً على المصارف التي سيختارونها لإيداع أموالهم لديها ومن ثم فإن خصائص المصرف وسلوك المودعين تعد من العوامل المهمة عند اختيار المصرف لإيداع الأموال، وقد تختلف المحددات مع تغير تصور المودع من وقت لآخر حسب الظروف الاقتصادية وأداء المصرف (Ferreira & Dickason, 2020:74).

هناك مجموعة من المحددات التي تعتمد على أساس عوامل الثقة للمودعين في اختيار مصرفهم والتي يمكن اختصارها بالآتي:

1- **اختيار المصرف:** Choose the bank

يميل المودعون في سوق اليوم إلى الاختيار بين المصارف المختلفة للموازنة بين العديد من العوامل، بما في ذلك التكلفة والموثوقية وجودة المنتجات والخدمات والفعالية الشاملة (Ghamry & Shamma,2022:688).

ويمكن ان تتحول الممارسات المصرفية التي تركز على المودعين في البلدان النامية والناشئة تدريجياً من مجموعة من المحددات الملموسة والمحددات غيرالملموسة لاختيار المصارف التي تقدم الخدمات التي

تتماشى مع احتياجات المودعين وتوقعاتهم فإن ذلك يؤدي إلى زيادة ثقة المودعين ويؤدي إلى علاقة ممتدة بين مقدم الخدمة والمودعين (Kaur et al., 2021).

أصبح من الضروري للمديرين أن يفهموا تماماً تفضيلات المودعين وعمليات اختيار المنتج، ويمكنهم بعد ذلك استخدام هذه المعلومات للتوصل إلى استراتيجيات عمل من شأنها أن تساعد المصرف على تحقيق المزيد من الثقة لدى المودعين (Mitik et al., 2017 :17).

ان ميل المودعين إلى التعامل مع مؤسسة مالية او مصرف معين يرتبط ارتباطاً مباشراً بمستوى إيمان المودعين وثقتهم في تلك المصارف، اذ ان سمعة المصرف ضعيفة ومعرضة بسهولة للتناقل الشفهي، وقد تنتشر بسرعة إما بشكل إيجابي أو سلبي وهذا يدل على أن العوامل الاجتماعية مثل توصيات الأصدقاء أو العائلة من المرجح أن تؤثر تاثيراً كبيراً في تحديد المودعين الذين يختارون فتح حسابات في مؤسسات مالية ومصارف معينة (Manohar et al., 2019:406).

أن المودعين لديهم قدرة معرفية محدودة في تحديد الحلول المناسبة، وعادة في عملية اتخاذ القرار الاستهلاكي يميلون إلى اتباع عملية التقييم التقليدية المكونة من خمس خطوات تتضمن عملية التعرف على المشكلات والبحث عن المعلومات والتقييم البديل وتقييم الاختيار والنتائج (Bruner & Pomazal, 1988:225).

2- **سلوك المودعين:** Depositors' behavior

يعد السلوك او الاتجاه هو الميل المكتسب للتفاعل باستمرار بشكل إيجابي أو سلبي تجاه شيء معين، اذ تفترض نظرية القيمة المتوقعة التي اقترحها Fishbein & Ajzen أن مواقف الناس تنبثق بشكل طبيعي من الاعتقاد الذي لديهم بالفعل حول شيء ما، فالمعتقدات غالباً ما تطور بربطها بأشياء أو سمات أو تجارب أخرى (Fishbein & Ajzen 1975:205).

عندما يتعلق الأمر بموقف الشخص تجاه السلوك، فإن كل اعتقاد يربط السلوك بنتيجة معينة أو بشيء آخر، مثل خطورة القيام بهذا السلوك (Ighomereho & Sajuyigbe, 2022:181). ومع ذلك فقد أولى الباحثون الذين يدرسون سلوك المودعين وعملاء المصارف وتفاعلهم مع هذه المؤسسات قدراً كبيراً من الاهتمام بالسلوك لأنه أحد الجوانب الأساسية التي تؤثر على سلوك ثقة المودعين في العديد من الدراسات السابقة حول هذا الموضوع وجد الباحثون أن مواقف المودعين أثرت بشكل كبير على نواياهم تجاه المصارف (Kannaiah eta al. ،2017 :175).

3- **المعيار الشخصي للمودعين:** Personal standard for depositors

هو عبارة عن عامل اجتماعي يسمى القاعدة الذاتية والتي هي عبارة عن الضغوط الاجتماعية التي يمارسها الأشخاص المهمون، مثل العائلة والأصدقاء وزملاء العمل، للقيام بسلوك ما أو الامتناع عنه (Aji et al., 2020:180).

أن تصورات المودعين لقيمة الخدمة قد تتأثر بآراء وأفكار الآخرين، بالنسبة للإجراءات ذات العواقب المعيارية الجوهرية، فإن القاعدة الذاتية ستكون أهم مؤشر للتنبؤ بالاستخدام الفعلي عندما يكون التأثير الذاتي أقوى من القاعدة الذاتية (Alhassany, & Faisal, F. 2018:39).

وفقا Ighomereho & Sajuyigbe's أن المعايير الذاتية لها تأثير إيجابي مهم على اعتماد التعاملات المصرفيةهناك مجموعة من الدراسات تتوافق مع نتائج دراسات أخرى والتي وجدت أن المعايير الذاتية تؤثر بقوة على ثقة المودعين في اعتماد الخدمات المصرفية (Ighomereho & Sajuyigbe, 2022:13).

4- **السيطرة على سلوك المودعين:** Controlling the behavior of depositors

إن قرار الفرد هو انعكاس لسيطرته السلوكية المتصورة لقدراته على اداء الأحكام والسلوك فيما يتعلق باستقلاليته في اختيار القيام بالسلوك ، اذ ان السيطرة السلوكية المدركة هي الدرجة التي يعتقد بها الفرد أن لديه القدرة على الامتناع عن الانخراط في سلوك معين (Hamid & Bano, 2021:57)

وفقًا Ajzen ان الأفراد الذين يعتقدون أن لديهم قدراً كبيراً من السيطرة على سلوكهم من المرجح أن تحفزهم للانخراط فعلياً في هذا السلوك وقد تؤثر السيطرة على سلوك المودعين بطريقتين الاولى يمكن ان تغيير النية لقيامهم بسلوك معين، والثانية يمكن أن تؤثر بشكل مباشر على السلوك بطريقة تعتمد على النية المعنية لديهم.

قد يتأثر اتخاذ القرار وسلوك المودع بعوامل الرقابة الداخلية والخارجية اذ تشمل عوامل الرقابة الخارجية أشياء مثل المال والوقت وتعاون الشركاء، في حين تركز عوامل الرقابة الداخلية على المعرفة والخبرة وقدرات الأفراد المعنيين، ونظراً لأن هذه العوامل تؤثر بشكل مباشر على سلوك الفرد فإن الأشخاص الذين لديهم سيطرة سلوكية مرتفعة هم أكثر عرضة للانخراط في سلوك معين أو الامتناع عنه (Ajzen, 2020:314).

سابعاً: تكامل الثقة وعدم الثقة في بالتعاملات المصرفية:

Integrating trust and mistrust in electronic banking

إن طبيعة الثقة وعدم الثقة والعلاقة المتبادلة بينهما لم تحدد بشكل واضح في الأبحاث السابقة، وفي سياق العمل المصرفي اشارة الدراسات الى وجود اتجاهات إيجابية وسلبية متزامنة مع استخدام التقنيات الآلية في الصناعة المصرفية، وجد Smither & Braun على سبيل المثال أن كبار السن الذين يفكرون في استخدام أجهزة الصراف الآلي يعكسون استجابتين عاطفيتين هما الضمان والتخوف واللتان لهما وزن مختلف اعتماداً على ما إذا كان المودع يستخدم أو لم يستخدم أجهزة الصراف الآلي المصرفية، ووجدوا أن غير المستخدمين شعروا بمشاعر أقل من الاطمئنان (مشاعر السيطرة والسلامة والراحة) ومستويات أعلى من التخوف (تعقيد التكنولوجيا وعدم الثقة وانعدام السيطرة والموثوقية) فيما يتعلق باستخدام التكنولوجيا، وكان العكس هو الصحيح بالنسبة لمستخدمي أجهزة الصراف الآلي العاديين بضمان عالي ومخاوف منخفضة (Smither &Braun,1994:381)

يصنف Serva العلاقة التكاملية بين الثقة وعدم الثقة في التعاملات المصرفية الالكترونية إلى أربعة مجموعات وهي حسب الاتي: ((Serva , 2007:6) ، (Yannick, 2021:8):

1- لا ثقة ولا عدم ثقة: العميل المتناقض The contradictory client

آن المودعين الذين لا يشعرون بثقة أو عدم الثقة في التعاملات المصرفيةعبر الإنترنت لديهم آراء متناقضة بشأن استخدام التكنولوجيا عبر الإنترنت، وقد يتجلى هذا التناقض من عدم الاهتمام أو نقص المعرفة، على سبيل المثال قد لا يكون عميل التعاملات المصرفيةعلى علم بوسائل الراحة التي توفر عبر الإنترنت، كما يسعى الأفراد إلى حل تصورات الثقة أو عدم الثقة لتقليل البعد المعرفي، ولهذا السبب من المرجح أن يميز هذا الجانب الزبائن المحتملين أكثر من الزبائن الحاليين، فضلاً عن ذلك فإن الميل إلى الاعتماد على الثقة وعدم الثقة في عالمنا الخاص يوفر فرصة للمصارف.

ان الزبائن المتناقضون لم يشكلو بعد تصورات قوية حول فوائد التعاملات المصرفيةعبر الإنترنت لذلك من المرجح أن يتم إقناعهم بسهولة أكبر بمزايا التعاملات المصرفيةعبر الإنترنت مقارنة بالزبائن الذين كونوا بالفعل تصوراً سلبياً للخدمات المصرفية عبر الإنترنت.

2- **انعدام الثقة وعدم الثقة: الخوف من التكنولوجيا** Fear of technology

توجد هذه الحالة التي تسمى "الشك الأعمى" عندما يكون هناك توقع كبير أوخوف من تصرفات غير مرغوب فيها من قبل المصرف، ونظراً لافتراض دوافع ضارة تدار أي ترابط بعناية ويمكن للمودعين اتخاذ الإجراءات الوقائية في سياق التعاملات المصرفيةعبر الإنترنت، ويتوقع المودع أن استخدام التكنولوجيا لإدارة احتياجاته المصرفية سيؤدي إلى نتائج غيرمرغوب فيها.

أن المودعين الذين لا يثقون في أحد المصارف من المرجح أن ينتقلوا إلى مصرف آخر فسوف يفترض أن التصورات السلبية الموجهة نحو استخدام التعاملات المصرفيةعبر الإنترنت ناتجة عن استخدام التكنولوجيا وليس المصرف، ويمكن للمصارف معالجة مخاوف عدم ثقة المودعين العمل على نقطتين مهمتين هما خدمة المودعين والأمن عبر الإنترنت.

ان حقيقة الاعتماد على الإنترنت مفادها ان الكثيرين لا يشعرون بالارتياح تجاه استخدام الكمبيوتر الشخصي والإنترنت مما يزيد من تفاقم المشاكل ووجود العديد من الروابط الضعيفة في إنشاء حساب مصرفي عبر الإنترنت ،ومن هذه المشاكل (إعدادات الأجهزة غير الصحيحة وأنظمة التشغيل غير المتوافقة ومشاكل مع مزود خدمة الإنترنت وإنشاء معرف وكلمة مرور للخدمات المصرفية عبر الإنترنت). ويتعين على المصارف أن تتوقع هذه الإحباطات إذا أردنا إدارة تصورات عدم الثقة بشكل فعال.

3- **الثقة وعدم الثقة: المتبني المبكر** Early adopter

تتميزالثقة العمياء ان المودعين الذين كونوا تصورات ثقة إيجابية نتيجة لتجاربهم المثمرة مع المصرف بأنهم يتبنون التكنولوجيا بحرية وسهولة ولا يجدون صعوبة كبيرة في دمجها في حياتهم.

قد يفترض هؤلاء المودعين بشكل عام ان المصارف لا ترتكب أخطاء أو إذا ارتكبت أخطاء فإنها تحدث بشكل نادر جداً لدرجة أنه لا يستحق مراقبة سلوك المصرف، وعندما يقوم المودعون الأوائل بدمج التكنولوجيا بسرعة في حياتهم فهم يقومون بسهولة بتكوين درجات عالية من الثقة الضرورية لتطوير علاقة تكاملية عالية مع مصارفهم بسرعة.

اما بالنسبة للمتبنين الأوائل قد تكون الثقة مدفوعة بالعروض التكنولوجية ومن المحتمل أن يطلب المودع القرض من المصرف إذا كان العرض عبر الإنترنت موجوداً ومن ثم فإن المتبنين الأوائل يمكن للمصارف الاستفادة من علاقاتهم بشكل أفضل من توسيع النطاق الترددي لعلاقاتها عبر الإنترنت في حين أن

المستخدمين الأوائل سينتقلون بسرعة إلى الميزات الأساسية (التحقق من أرصدة الحسابات، وتحويل الأموال) فقد يكونون مرشحين رئيسين لمزيد من الخدمات المميزة (على سبيل المثال القروض عبر الإنترنت ودفع الفواتير)، في حين أن الثقة العمياء قد تبدو المجموعة الأكثر جاذبية للخدمات المصرفية عبر الإنترنت.

4- الثقة وعدم الثقة: العميل السليم The healthy client

نحن نسمي هذه الثقة"بالثقة المحدودة لأن الحدود على مستوى الثقة يخفف منها مستوى عدم الثقة ويعد الوجود المتزامن للثقة وعدم الثقة يمثل علاقة أكثر نضجٍ مما ينعكس في الثقة العمياء وعدم الثقة العمياء، وتعكس الثقة المحدودة اعتراف كل من المصرف والمودع بأن لكل منهما أخطاءه ولذلك يوافق كل منهما على مراقبة تصرفات الآخر وقبول نقاط القوة والقيود لدى كل منهما بتسهيل مهام مثل موازنة الحسابات، وتوفر المصارف للمودعين الفرصة لتعزيز تصوراتهم عن الثقة باتخاذ الإجراءات التي تعزز ثقتهم.

ان المصارف التي تسهل على المودعين التحقق من أنهم يتصرفون بطريقة جديرة بالثقة قد تعزز أيضا تصورات ثقة المودع ، وعلى عكس المودع ذو الثقة المحدودة الذي قد يتفاعل بالمفاجأة وردة الفعل عندما يخسر المصرف وديعتة ولهذا فإن الثقة السليمة تتطلب قبول حدوث أخطاء، ومع ذلك لكي يتمكن المودعون من تحقيق ثقة سليمة يجب عليهم أن يفهموا كيف سيكون رد فعل المصرف عند مواجهة أي تحدي.

ان المودعين الذين يعرفون أن المصرف الذي يتعاملون معه سيبذل جهداً صادقاً لحل المشكلة من المرجح أن يحققوا ثقة سليمة، وفي المقابل من المرجح أن ينتقل المودع إلى حالة عدم الثقة العمياء إذا لم تعالج مثل هذه المواقف بشكل مناسب.

إن تطوير ثقة المودعين وتعزيزها وانعدام الثقة في وقت واحد يتطلب من المصارف تغيير الطريقة التي تنظر بها إلى المودع، ويكون عمل المودع بمثابة فحص إضافي للنزاهة والتحقق من صحة المعاملات المنشورة ولهذا يجب على المصارف أن تفهم أنه لا يمكن للمودعين تكوين ثقة سليمة إلا عندما يقوم المصرف بما يحقق مصالحهم عندما يواجهون التهديدات والمخاطر.

ثامناً: – إثر الثقة على نوايا المودعين اتجاه التعاملات المصرفية:

The impact of trust on depositors' intentions in electronic banks

ارتفع معدل اعتماد التعاملات المصرفية الالكترونية من قبل المودعين بشكل ملحوظ في السنوات الأخيرة على سبيل المثال، في الاتحاد الأوروبي وفقًا لبيانات يوروستات، ارتفع معدل الأفراد الذين يستخدمون الإنترنت للخدمات المصرفية عبر الإنترنت بأكثر من 25% بين عامي 2012 و2023 (Eurostat, 2024:3).

يرجع ارتفاع معدل اعتماد التعاملات المصرفية الالكترونية من قبل المودعين إلى عدة عوامل منها تطور التكنولوجيا ومدة جائحة كوفيد-19 والوقت اللازم لإتمام المعاملة وتوافر الخدمات، ومنذ تفشي جائحة كوفيد-19 حدثت تغييرات كبيرة في كل قطاعات النشاط تقريبا حول العالم، وكان أحد هذه التحديات هو التركيز على بيئة الإنترنت، ومع ذلك وفي بعض الحالات لم يكن التغيير مفاجئاً، حيث كانت هناك بالفعل مبادرات في هذا الاتجاه. ومن الأمثلة على ذلك القطاع المصرفي الذي اعتمدت وحداته بقوة وسائل الإنترنت وتكنولوجيا المعلومات في عملها والتعاملات التي تقدمها نظرا لطبيعتها المتمثلة في إدراك كل ما يحدث في السوق (Kumar & Barquissau, 2012:45).

ومن أجل تقييم أثر الثقة وأبعادها على النوايا السلوكية للمودعين في الخدمات الخاصة المصرفية الإلكترونية والذي يتضح من الاتي:

1- **قدرة الوحدات المصرفية:** Capacity of banking units

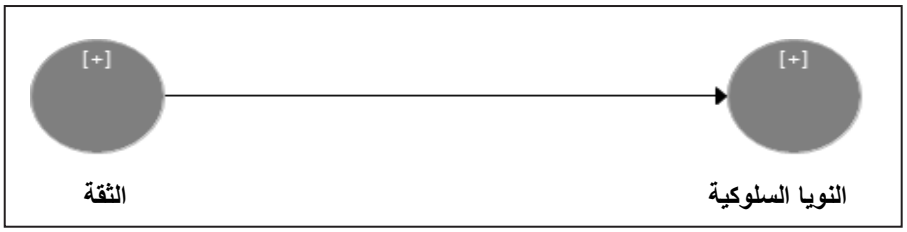
عندما يشير المودعون إلى قدرة الوحدة المصرفية في سياق المعاملات الإلكترونية فإنهم يركزون على اتجاهين وهي كفاءة الوحدة المصرفية في تلبية احتياجات المودعين وحصول الوحدة المصرفية على المعلومات اللازمة لتلبية تلك الاحتياجات (Bhattacherjee, 2002:74).

لذلك يمكن القول إن قدرة الوحدة المصرفية تعتمد على جودة موظفيها، أذ تعد الموارد البشرية أكثر أهمية عندما يتعلق الأمر بالخدمات، ومع التحول من التعاملات المصرفيةالتقليدية إلى التعاملات المصرفيةعبر الإنترنت تكثف أنشطة الوحدات المصرفية باستمرار، مما يزيد الضغط على الموارد البشرية (Chimote, 2019:13).

من المهم جداً أن يستجيب الموظفون لطلبات المودعين بطريقة احترافية، ولهذا السبب تحتاج الوحدات المصرفية إلى أشخاص يتمتعون بمهارات جيدة جداً خاصة في المجال الرقمي

ويمكن ملاحظة ذلك أيضا في طريقة عمل أدوات الوحدة المصرفية والتي تحدد أيضاً من سرعة تحميل صفحات تطبيقات التعاملات المصرفيةعبر الإنترنت، ويتأثر وقت انتظار المودعين مما يولد أيضا مستوى معين من الثقة لديهم اتجاه التعاملات المصرفيةالمقدمة (Nichifor,et al, 2021:26).

إذا واجه الموظفون قيوداً معينة فيما يتعلق بطلبات المودعين فستقلل الثقة في الوحدة المصرفية (Bank Director, 2018:22). وهذا سوف يؤثر على النوايا السلوكية للمودعين وكما موضح بالشكل (15).



شكل (15) التأثير المباشر على ثقة المودعين

Răzvan-Ionuţ, DrugăThe Effect of Trust in Banking Institutions on Behavioural Intentions for E-Services, Ovidius University of Constanta, Romania, p2,2024.

وفي الوقت نفسه من المهم أن يشعر الموظفون بأنهم جزء من ثقافة المصرف، وبدون مستوى عالٍ من رضا الموظفين الناتج عن السياسات الداخلية للوحدة المصرفية لن يتمكن المودعون من الاستفادة من مستوى أعلى من الرضا عند استخدام خدمات المصرف (Allred & Lon Addams, 2000:55).

يؤثر الالتزام التنظيمي تاثيراً مهماً للموظفين للمشاركة قدر الإمكان في عملية التعاون مع المودعين وفي الوقت نفسه سيشارك الموظفون في الابتكار في أنشطتهم وسيبحثون عن حلول جديدة لتقديم خدمات تليق بالوحدة المصرفية اعتماداً على سلوك الموظفين، وقد يكون لدى المودعين نوايا سلوكية مختلفة يمكنهم التأثير على التفاعل مع الموظفين بطريقة أو بأخرى، واعتماداً على هذه الدائرة فإن ربحية الوحدة المصرفية ستكون متناسبة طرديا لأن تحقيق الأداء يعتمد على إنجاز المهام من قبل الموظفين (Lekić et al., 2020:11).

2- **نزاهة الوحدات المصرفية:** Integrity of banking units

وفقا للأدبيات فإن النزاهة في المعاملات الإلكترونية موجودة في ثلاث اتجاهات على الأقل وهي عملية إتمام الصفقة وخدمات ما بعد البيع والمعلومات الشخصية للمودعين (Druga ,2024:2).

ومن أجل الحفاظ على ثقة المودعين تضطر المصارف إلى دعم المعاملات الإلكترونية بطريقة سريعة وآمنة قد تكون هذه هي الأسباب التي تجعل المودعين يفضلون استخدام التعاملات المصرفيةعبر الإنترنت، وخلال هذه العملية يمكن للمؤسسات المصرفية دمج أنظمة معينة للتحقق من أن المعاملة ليست سلبية إذ تنفذ المعاملات بنجاح، ويمكن إنشاء نوايا سلوكية إيجابية جديدة للمودعين وينبغي أن تكون العلاقة بين المؤسسات المصرفية والمودعين على نفس القدر من الأهمية بعد المعاملة الإلكترونية، ويمكن القيام بذلك بدعم من بعض خدمات ما بعد البيع، إذ اخذت هذه الأمور على محمل الجد من قبل موظفي المصرف فيمكنهم ضمان ذلك عند استمرارية المصرف في السوق، وعلى سبيل المثال يمكن تمثيل هذه الخدمة من التعليقات الإيجابية المقدمة من المودعين، وهذا سيعمل على مساعدة الوحدة المصرفية على تحسين خدماتها في المستقبل إذا لزم الأمر(Drugă,2024:2).

يم نشر هذه التعليقات على الموقع الإلكتروني للمصرف أو على مواقع الشبكات الاجتماعية، ويؤدي إلى ردود فعل جديدة من المودعين المحتملين الآخرين، فضلاً عن ذلك يمكن لخدمات ما بعد البيع أن تقدم المزايا الاتية صورة محسنة للعلامة التجارية ودعم مكثف للمودعين فضلاً عن التميز الفعال عن المنافسين مع توفير علاقة مبنية على الثقة مع المودعين (Gallemard, 2022:8).

تتضمن سلامة النظام المصرفي عبر الإنترنت بإدارة البيانات الشخصية للمودعين أهمية كبيرة ولهذا عندما يكون جزء من المودعين مترددين عن استخدام التعاملات المصرفية الالكترونية على وجه التحديد من عدم يقينهم بشأن كيفية جمع بياناتهم الشخصية أو معالجتها أو استخدامها أو تخزينها (منظمة التعاون الاقتصادي والتنمية، 2020). وعلى المستوى العالمي ينبغي للسلطات العامة أن تتخذ التدابير اللازمة لزيادة مستوى ثقة المودعين والجمهور في الجهات التي تتعامل مع بياناتهم الشخصية يمكن أن تكون إحدى المبادرات بهذا المعنى اعتماد اللائحة العامة لحماية البيانات في أوروبا في عام 2018 مما جعل الأمور أكثر استقرارًا قليلاً لمواطني هذه القارة (Forbes, 2021:33).

3- إحسان الوحدات المصرفية: Ihsan banking units

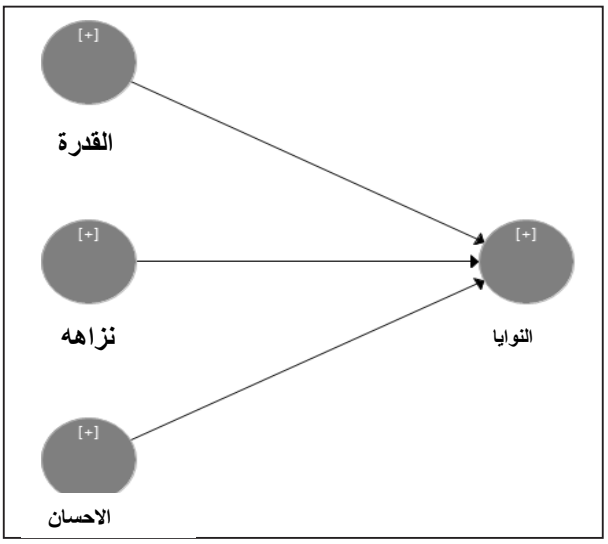
بغض النظر عن ملف تعريف المودعين، يجب أن يكون ممثلو الوحدات المصرفية موجهين نحو احتياجاتهم ويمكن أن يعتمد ذلك على الأعمال الخيرية ومعظمها طوعية التي يقوم بها الموظفون لدعم المودعين، حتى لو كان من الممكن في سياقات أخرى رسم بعض أوجه التشابه بين مفهوم الإحسان ومفهوم الكفاءة (Pivetti, & Berti, 2020:5).

في المؤسسات الائتمانية عند مناقشة التعاملات المصرفية الالكترونية يجب على الموظفين التصرف بما يأتي:

أ. بذل جهود استباقية بحسن نية لحل مخاوف المودعين.

ب. إظهار التقبل والتعاطف تجاه اهتمامات المودع واحتياجاته.

على سبيل المثال خلال جائحة كوفيد-19 حدث تحول تدريجي في استخدام المودعين لمختلف التطبيقات الإلكترونية وفي الوقت نفسه روج ممثلو الوحدات المصرفية لاستخدام بعض الروبوتات في مكاتبهم نظراً لعدم امتلاك جميع المودعين المهارات اللازمة لاستخدام الجهاز، وعرض الموظفون مجموعة من وسائل المساعدة للتعبير عن حسن نيتهم تجاه المودعين، وبهذه الطريقة تمكن المودعين من إتمام معاملاتهم بأمان وصدق، ولم يحصل الموظفون على أي مكافآت إضافية مقابل هذا النشاط، وبناءً على ما تقدم تم اقتراح النموذج الاتي وحسب الشكل (16).



الشكل (16) النموذج المفاهيمي لنوايا المودعين

Răzvan-Ionuţ, DrugăThe Effect of Trust in Banking Institutions on Behavioural Intentions for E-Services, Ovidius University of Constanta, Romania, p2,2024

إذا تلقى المودعين علاجاً مناسباً من مؤسسة مصرفية فإن رضاهم وثقتهم تكون أعلى، ويمكنهم تكوين عدد من النوايا السلوكية الإيجابية مما يدل على الولاء للمصرف، ومن ثم إذا تلقى المودع علاجاً مناسباً من مؤسسة مصرفية وبناء على هذه المعطيات يعد الاحسان إحسان لفروع المصارف وله تأثير مباشر على النوايا السلوكية لمستهلكي التعاملات المصرفيةعن بعد وخصوصاً المودعين (Pandey, & Patwardhan, 2020).

خامساً:- ابعاد ثقة المودعين بالمصارف:

Dimensions of depositors' confidence in electronic banking services

بدأ البحث في مفهوم الثقة في بيئة الأعمال الإلكترونية (e-Trust) في أواخر عام (١٩٩٠)، حيث اختلف الباحثون حول التحديد الدقيق لمفهوم الثقة وخصائصها وأبعادها، أشار (Yaghoubi et al., 2011 :8) إلى ذلك في دراسته التي تهدف إلى عمل مسح شامل للأبعاد الخاصة بالثقة المصرفية وذلك من خلال عرض (١٠) نماذج للثقة الإلكترونية في المصارف، في التحليل المصرفي عبر الإنترنت والحكومة الإلكترونية، وشرحها ومناقشتها ثم عمل تحليل مقارنة بينها على أساس الأبعاد المختلفة النموذج الثقة الإلكترونية الذي قدمه (Kim et al., 2005). والذي اعتبره الباحثون نموذج شامل لكافة الأبعاد الضرورية للثقة الإلكترونية والمتمثلة في الستة أبعاد وهي البعد السلوكي للعميل، البعد المؤسسى بعد محتوي المعلومة، بعد المنتج، بعد العملية، وبعد التكنولوجيا، علق في هذه الدراسة على أنه على الرغم من أهمية الثقة في العديد من المجالات، إلا أنه يوجد عدم اتفاق واسع من جانب الباحثين على المفهوم والخصائص والأسس والنتائج المرتبطة بالثقة، وذلك لكونها مفهوم متعدد الأبعاد وصعب التحديد و مرتبط بالطبيعة البشرية والخبرات المختلفة وتعدد التعبيرات والكلمات الدالة عليه مثل الثقة الجدارة بالثقة

هناك مجموعة من الابعاد الخاصة بثقة المودعين في النظام المصرفي وهي تقسم الى ثلاثة ابعاد:

الكفاءة أوالقدرة والمنفعة والامان وهي كما يأتي (شوابية, عفاف، 2023: 49)، (سناء، 2023: 12):

1- **القدرة أو الكفاءة:** Ability or competence

ويقصد بها أن الفرد يعتقد أن الطرف الآخر لديه القدرة الأداء ما يحتاج إليه والوفاء بالوعود التي قطعها مع عملائه أو تشير إلى إدراك صاحب الثقة لكفاءات ومعارف الموثوق فيه البارزة في سلوكه المتوقع، وهذه المدركات ربما تكون معتمدة على خبرات السابقة أو الشهادات المؤسسية، وفي مجال التجارة الالكترونية وان إدراك قدرة المصرف يعتمد على اعتقادين مترابطين هما: ما إذا كان المصرف كفوء ولديه خبرة ومهارة بدرجة كافية لأداء السلوك المقصود،أو إذا كانت المصارف لديها فرص الحصول على المعرفه اللازمة لأداء السلوك بشكل مناسب أو ملائم ، وان الاهتمام بالقدرة والكفاءة يولدان النفع وان النفع يقدم إيمان في العلاقة ويقلل من عدم التأكد والميل للحذر من السلوك الانتهازي المضاد.

وهي مجموعة المهارات والكفاءات والخصائص التي تمكن طرف ما أن يكون له تأثير داخل مجال معين فمجال القدرة يكون محدداً لأن الموثوق به يمكن أن يكون لديه كفاءة بدرجة عالية في بعض المجالات الفنية وتكفل أن يثق الشخص في المهام المرتبطة بهذه المجالات، وتشير القدرة لإدراك صاحب الثقة لكفاءات

ومعارف الموثوق فيه البارزة في السلوك المتوقع، هذه المدركات ربما تكون معتمدة على الخبرة السابقة الأصلية أو الغير مباشرة أو الشهادات المؤسسية Institutional endorsements وفي مجالات التجارة الإلكترونية، وإدراك قدرة الشركة أو المصرف يعتمد على اعتقادين مرتبطين هما (١) ما إذا كانت الشركة أو المصرف كفء لديها خبره ومهارة بدرجة كافية لأداء السلوك المقصود، و (٢) ما إذا كان المصرف لديه فرص الحصول على المعارف اللازمة لأداء السلوك بشكل مناسب أو ملائم، وبالتالي القدرة تكون محددة المجال، فالموثوق بهم المهرة في مجال معين ينظر إليهم بأنهم لديهم كفاءة أو خبرة في المجالات الاخرى (Bhattacherjee, 2002:241).

2- **المنفعة:** Benefit

ويقصد بها أن الفرد يعتقد أن الطرف الآخر يعتني به ومدفوع بالتصرف وفق مصلحته وفي مجال التجارة الإلكترونية، قد يكون من الصعب توقع حاجات المودعين لكي تصمم الخدمات الجيدة ولذلك يعمل من (1) إداء التعاطف والقدرة نحو اهتمامات وحاجات المودعين (2) عمل جهود بحسن نية لحل مشاكل المودع. ويعني المنفعة مدى إعتقاد أن الموثوق به يريد فعل الخير لصاحب الثقة، بعيداً عن دافع الربح الشخصي فهو يشير إلى أن الموثوق به لديه بعض القيم المحددة المرتبطة بصاحب الثقة وفقاً لمعتقد النفع فإن الموثوق به يكون محسناً لصاحب الثقة، حتى عندما لم يتطلب من الموثوق به أن يكون مساعد أو لم يكافئ لكونه مساعد، فالمنفعة تقدم إيمان وإيثار في العلاقة ويقلل من عدم التأكد والميل للحذر من السلوك الانتهازي المضاد (Mayer et al., 1995).

3- **الامان:** Safety

وتعني أن الفرد يعتقد أن الطرف الآخر يبرم الاتفاقات بحسن نية، يقول الحقيقة يتصرف بخلق، يحقق الوعود ويوفي بالعهود ، وتشير الأمانة إلى إدراك صاحب الثقة أن الموثوق به سيلتزم بمجموعة من مبادئ أو قواعد التبادل المقبولة لدى صاحب الثقة خلال وبعد عملية التبادل فالأمانة المدركة تغرس ثقة صاحب الثقة بالمصرف من خلال التدابير والإجراءات التي تصب في مصلحة المودعين:

أ- إجراء المعاملات على الأنترنت.

ب- سياسات خدمة المودعين بعد الصفقة.

ج- استخدام المصرف للمعلومات الخاصة بالمودعين والمصرف على الأنترنت قد يبني مدركات الأمانة بتوضيح الصريح لقواعدها في التبادل المصرفي.

تاسعاً:- العوامل التي تؤثر على ثقة المودعين بالمصارف:

Factors that affect depositors' confidence in electronic banks

هناك العديد من العوامل التي تم تحديدها في الأدبيات والتي يمكن أن تؤثر على ثقة المودعين من خلال التعاملات المصرفية عبر الإنترنت، وإن تحديد تلك العوامل يمكن أن يكون مفيداً، لذلك تنقسم جميع العوامل التي يمكن أن تؤثر على ثقة المودعين إلى مجموعتين، تتعلق المجموعة الأولى بخصائص الموقع الإلكتروني والمجموعة الأخرى تتعلق بخصائص المودعين (Bhattacherjee ,2002:242).

وجدت إحدى الدراسات التي ركزت على التعاملات المصرفية الإلكترونية أن استعداد المودعين لاستخدام الوسائط المصرفية عبر الإنترنت يتشكل من خلالها تعزيز الثقة (Liu et al ، 2011: 58). بالإضافة إلى ذلك، يمكن أن تتأثر ثقة المودعين بالمعرفة الشخصية أو المعلومات حول الوسائط المصرفية عبر الإنترنت ولهذا يمكن أن تكون الثقة أساساً لعوامل مهمة أخرى والتي سوف نبينها وحسب الاتي : (Shidrokhi et al, 2018: 27)،(Nasrawi et al, 2018: 27) (Jameel&Mohammed,2016:41)

1- **التنبؤ الاستباقي:** Proactive forecasting

من العوامل التي تعزز ثقة المودعين في المصارف هي اعتماد المصارف على استراتيجيات وأساليب تساعد على فهم احتياجات المودعين ورغباتهم والتعرف على المشكلات التي يوجهونها ولذلك يجب على المصارف تقديم منتجات أو خدمات تناسب واحتياجات ومتطلبات المودعين، كما ينبغي عليها التعامل مع التحديات التي تواجه المودعين بتقديم أفضل الخدمات وإيجاد حلول مبتكرة لجميع المشاكل بشكل مبكر واستباقي.

2- **صدق المعاملات:** Verity of transactions

يتعين على موظفي المصارف التعامل مع المودعين بصدق واخلاص، فهذه الصفات تؤدي عملاً مهماً في كسب رضا المودعين وثقتهم على المدى البعيد، كما يجب عليهم الحرص على تقديم خدمة متميزة باستمرار والالتزام بأداء واجباتهم تجاه المودعين بكل شفافية وصدق.

3- **التغذية العكسية:** Reverse feeding

إن تعزيز التغذية العكسية لاحتياجات ورغبات المودعين بالاستماع لملاحظاتهم وشكاويهم يعد أفضل وسيلة لكسب ولائهم وتعزيز ثقتهم على المدى الطويل حيث يجب على موظفي المصارف

الإصغاء جيداً لملاحظات مودعيهم والسعي لتطبيقها عملياً فالموظف المتميز في الوحدة الاقتصادية الناجحة هو الذي يضع نفسه مكان المودعين ويتفهم آرائهم ووجهات نظرهم المختلفة.

4- **التواصل المستمر:** Constant communication

يمكن عد التواصل السيء أحد الأسباب التي تدفع المودعين الى البحث عن مصارف أخرى تبدي اهتماماً أكبر بمودعيها وتلبي احتياجاتهم بفعالية أكبر، لذا يتعين على المصرف الحرص على إنشاء قسم خاص بخدمة المودعين يهدف الى خدمتهم بطريقة سريعة وفعالة ويوظف أشخاص يتمتعون بمهارات تواصل جيدة والحرص على تزويدهم بدورات تدريبية حول كيفية تقديم خدمة متميزة للمودعين.

5- **العلاقات التفاعلية:** Interactive relationships

يتعين على الوحدة الاقتصادية تبني أساليب وسياسات جيدة تهدف للاحتفاظ بالمودعين وتعزيز ولائهم وثقتهم واخلاصهم تجاه مصرفهم، اذ يجب على المصرف اظهار اهتمامه بالمودعين من أنشطته وتواصله الدائم والتفاعل معهم على مواقع التواصل الاجتماعي وفي مناسباتهم الخاصة من أجل بناء علاقات وطيدة معهم لكسب ورفع مستوى ثقتهم ورضاهم عن المصرف وخدماته.

6- **تنفيذ الوعود:** Implementing promises

يعد الاهمال في تنفيذ الوعود التي يقطعها المصرف للمودعين من أخطر السلوكيات التي يجب تجنبها وذلك نظراً لأثرها السلبي على علاقتها بالمودعين، فإن لم يكن المصرف قادرة على حل مشكلة المودعين خلال مدة قصيرة فيجب عليه أن يصارحهم ويشرح لهم طبيعة المشكلة والوقت الفعلي الذي يحتاجه لحلها والحرص على التواصل معهم باستمرار لاطلاعهم على سير العملية داخل المصرف.

7- **سمعة العلامة التجارية:** Brand reputation

تعد سمعة العلامة التجارية عاملاً مهما يمكن أن يؤثر على ثقة المودعين فمن الأرجح أن يثق المودعون في العلامات التجارية التي تتمتع بسمعة طيبة من حيث الجودة والموثوقية وخدمة المودعين.

8- **الوضوح:** Clarity

عامل مهم آخر يمكن أن يؤثر على ثقة المودعين، وينبغي أن يلجأ المودعين إلى المصارف التي تتسم بالانفتاح والشفافية فيما يتعلق بممارساتها وسياساتها وإجراءاتها التجارية.

9- **التخصيص:** Customization

هو عملية تصميم تجربة المودع لتلبية الاحتياجات الفردية وتفضيلاته ويمكن من خلال التخصيص المساعدة في بناء ثقة المودعين وإظهار التزام المصارف بذلك وفهم وتلبية احتياجات مودعيها الأقل معرفة (Hansen, 2014:22).

يكون المودعون ذو المعرفة أكثر قدرة على تقييم المعلومات ومن المرجح أن يتخذوا قرارات أفضل بشأن مزود الخدمة الذي سيختارونه، فضلاً عن ذلك تسهل المعرفة تعلم معلومات جديدة حتى يتمكن المودعون ذوو المعرفة من اكتساب المزيد من المعلومات والاحتفاظ بها مقارنة بالمودعين الأقل معرفة.

وقد تسمح المعرفة أيضا للمودعين بصياغة المزيد من الأسئلة بحيث يكون المودعين ذوو المعرفة أكثر وعيا بما هو ممكن لمقدم الخدمة المالية وهذا قد يسهل فهم المودعين لسلوك مقدم الخدمة المالية مع التركيز على الشباب في اغلب الاوقات (Shim et al,2013:87).

ويرى Anaraki,et al ان هنالك مجموعة من العوامل والمخاطر المؤثرة على ثقة المودعين في استخدام التعاملات المصرفية الإلكترونية والتي حددت لتكون لها تأثير على ثقة المودعين في استخدام التعاملات المصرفية الالكترونية والتي هي كالاتي (Anaraki,et al,2013:5):

أ- المخاطر المصرفية المدركة.

ب- مخاطر الأمن المدرك.

ج- مخاطر السرية المدركة.

د- مخاطر الصدق المتصور.

ه- مخاطر الشعور بالإحسان.

و- مخاطر القدرة على التنبؤ.

ز- مخاطر القدرة المدركة.

ح- مخاطر سمعة المصرف.

ط- مخاطر حجم المصرف.

ي- إن رغبة الأفراد في الحصول على الثقة تؤثر على ثقة المودعين في استخدام الأجهزة الإلكترونية.

الفصل الثالث: الجانب العملي للدراسة

المبحث الاول:
واقـــع التعاملات المصرفـيـــة الإلكترونية فـــي العـــــراق

المبحث الثاني:
أختبار أدوات التحليل وبيانات الدراسة

المبحـــــث الثالث
عرض نتائج الدراسة وتحليلها وتفسيرها

المبحث الرابع
اختبار فرضيات الدراسة

" المبحـــــث الاول "

واقـــع التعاملات المصرفية الإلكترونية فـي العـــــراق

تمهيد:

شهد القطاع المصرفي العراقي بعد عام 2003 انفتاحاً على العالم الخارجي باستخدامه للتقنيات المصرفية الحديثة في تقديم الخدمات للزبائن بهدف مواكبة المستجدات والتطورات الحاصلة في القطاع المصرفي الدولي، وبذلك فقد سعت المصارف العراقية الى تطوير خدماتها باستخدام تقنيات المعلومات و تطبيق انظمة ووسائل الدفع الالكترونية من اجل تنويع التعاملات المصرفيةالتي تقدمها واستحداث خدمات جديدة وكذلك زيادة إنتشار التعاملات المصرفيةفضلاً عن ذلك زيادة كفاءة وفاعلية العمل المصرفي وهذا يؤدي الى زيادة ثقة المودعين، وان الهدف من هذا المبحث هو دعم وتعزيز نتائج الاستبانة.

وينتاول هذا المبحث الجوانب التالية:

أولاً: تطور التعاملات المصرفية الالكترونية في العراق:

ثانياً: مؤشرات تطورالودائع والتعاملات الالكترونية في عينةمن المصارف التجارية العراقية:

أولاً: تطور الودائع والتعاملات المصرفية الالكترونية في العراق:

The development of electronic banking services in Iraq

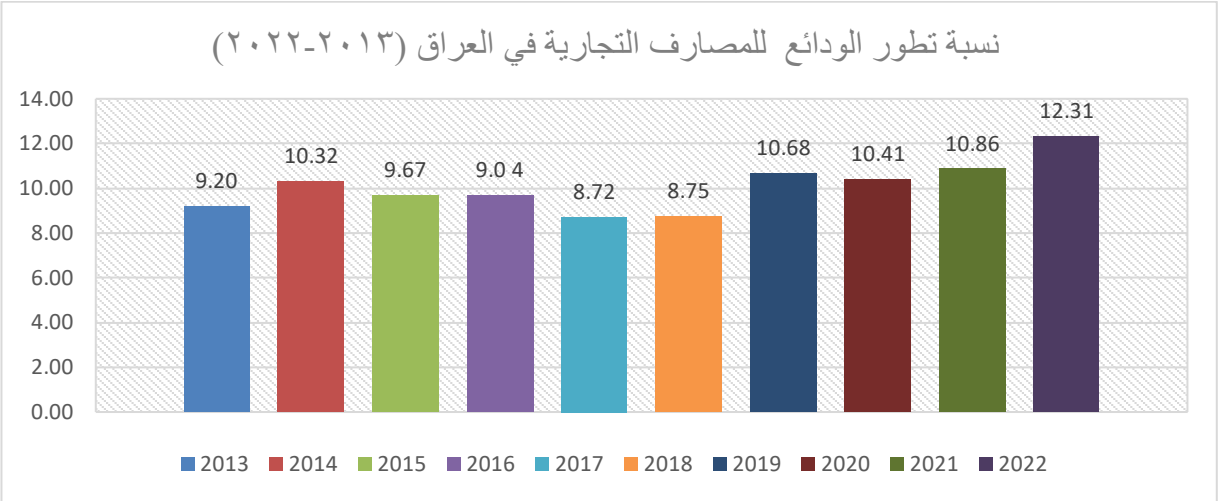
ادى التطور الهائل لتقنية المعلومات الى مساحة واسعة من الابتكار في مختلف المجالات، بما في ذلك الودائع والخدمات المصرفية، فضلاً عن الجمع بين التعاملات المصرفيةوالتقنية عبر الإنترنت، وتوفر الانظمة التقنية للزبائن مجموعة متنوعة من الخدمات بما في ذلك الاستعلام عبر الإنترنت عن حساباتهم ويمكن للزبائن من الوصول إلى النظام الإلكتروني للمصرف ايضاً من خلال كلمات المرور الخاصة بهم للحصول على التعاملات المصرفيةباقل وقت وكلفة (Nazaritehrani & Mashali, 2020: 7).

1- تطور الودائع في المصارف التجارية العراقية:

تعد الودائع المصرفية من أهم مصادر التمويل الخارجية في المصارف الخاصة من جهة ومصدر رئيس لتمويل العمليات الائتمانية الاستثمارية التي تقدمها المصارف على مختلف أنواعها من جهة أخرى، وتعد الودائع من حيث الكم إحدى المؤشرات لقياس مدى ثقة الجمهور في المصرف.

ونظراً لأهمية الودائع للمصارف تتنافس هذه الأخيرة فيما بينها لجذب الزبائن وتحفيزهم على إيداع مدخراتهم اذ تؤدي الفوائد الممنوحة للمتعاملين معها تأثيراً مهماً في عملية كسبهم وتشجيعهم على إيداع مدخراتهم لديها، وشهد حجم الودائع تطوراً ملحوظاً في السنوات الأخيرة وخصوصا بعد تفشي جائحة فايروس كرونا ويُعزى هذا التطور إلى عدة عوامل منها زيادة الثقة والإقبال على التعاملات المصرفيةوزيادة الوعي المالي فضلاً عن جهود المصارف في تحسين وتوسيع خدماتها المصرفية وان هذا التطور يُعد إيجابيا للاقتصاد العراقي، أذ يعكس ثقة الجمهور في النظام المصرفي ويسهم في تمويل الاستثمارات على مستوى التعاملات الداخلية والخارجية ودفع عجلة التنمية الاقتصادية.

اما فيما يخص المصارف التجارية عينة الدراسة فقد لوحظ ان هنالك تطور في نمو الودائع على الرغم من تعرض العراق الى ظروف الحرب على داعش الاجرامية وتفشي وباء فايروس كرونا الا ان هنالك تطور ملحوظ في نمو الودائع في المصارف التجارية العراقية في السنوات الاخيرة من مدة الدراسة وهذا يُعد عاملاً مهماً في تعزيز النظام المالي ودعم التعاملات الاقتصادية في البلاد ومع تزايد حجم الودائع تتاح للمصارف فرص أكبر لتقديم القروض والخدمات المالية للزبائن، وهذا يعزز ثقة المودعين بالنظام المصرفي ويشجع المودعين على إيداع أموالهم في المصارف، حيث يتمكنون من تحقيق عوائد مالية والحفاظ على أموالهم بشكل آمن، ان تعزيز الودائع يمكن المصارف من توسيع نطاق أنشطتها وزيادة قدرتها على تلبية احتياجات السوق ودعم النمو الاقتصادي والشكل (17) يوضح حجم نمو الودائع المصرفية في المصارف التجارية .



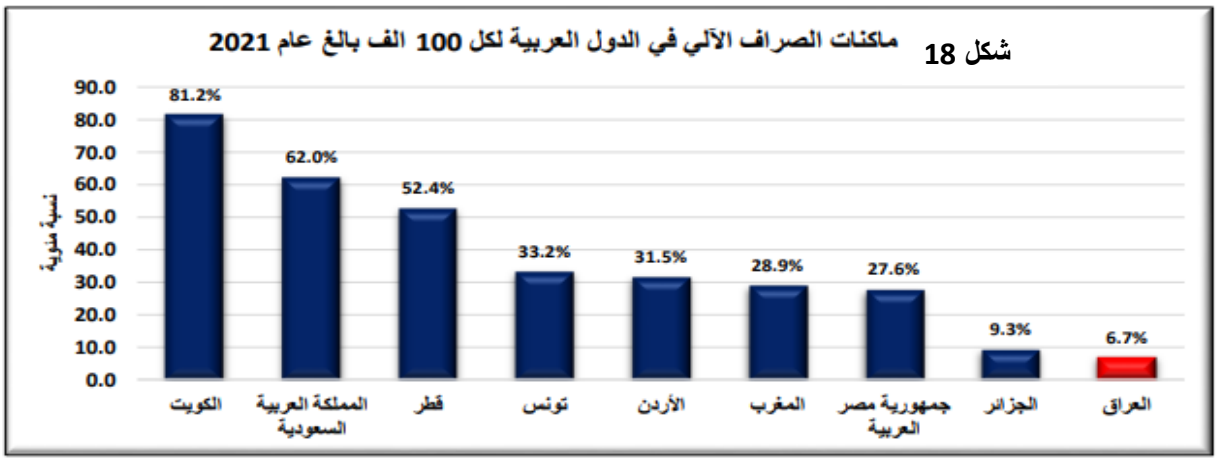
شكل (17) تطور الودائع للمصارف التجارية في العراق
المصدر: البنك المركزي دائرة الاحصاء والابحاث سنوات متفرقة.

يتضح من الشكل (17) ان حجم الودائع المصرفية قد تطور بشكل ملحوظ للسنوات الاخيرة من مدة الدراسة، اذ بلغت نسبة حجم الودائع خلال عام 2013 (9.20) مقارنة بالسنوات اللاحقة، وبعدها لوحظ ارتفاع في حجم الودائع خلال عام 2014 لتصل نسبتها الى (10.32)، وبعدها شهدت الاعوام 2015، 2016، 2017، 2018 انخفاضاً ملحوظاً في معدل حجم الودائع اذ شهد عام 2017 اقل نسبة لحجم الودائع مقارنة مع بقية السنوات اذ بلغت نسبتها (8.72 %) بسبب تأثير حرب داعش الاجرامية على القطاع المصرفي والركود الاقتصادي الذي مر به البلد وفي عام 2019 بدأ حجم الودائع بالنمو اذ بلغت نسبة الودائع (10.68 %) لكن سرعان ما انخفضت النسبة في عام 2020 لتصل الى (10.41 %) لتفشي وباء فايروس كورنا، وبعدها بدأت الودائع بالنمو من جديد مما يشير إلى عودة الثقة في القطاع المصرفي لاسيما المصارف التجارية اذ بلغت اعلى نسبة في عام 2022 اذ بلغت (12.31 %)، ومن هنا نلاحظ ان هناك تطور في التعاملات المصرفيةالمتمثلة بنمو حجم الودائع المصرفية وهذا مؤشر على زيادة الوعي والثقة لدى الجمهور بالمصارف التجارية العراقية.

2- تطور التعاملات المصرفية الالكترونية في العراق:

ان واقع الخدمات الالكترونية في العراق شهد تزايد في انتشار اجهزة الصراف الالي الذي ساهم في تعزيز البنية التحتية المالية وتعزيز استخدام الخدمات المالية الإلكترونية من قبل الزبائن والمؤسسات المالية لاسيما المصارف، ويعد العراق واحد من الدول حديثة النشأة في هذا المجال بسبب تأخر دخول الإنترنت إلى العراق وكذلك ضعف الثقافة المصرفية وتواضع القطاع المصرفي العراقي، ووفقا للشكل (18) لوحظ أن نسبة انتشار أجهزة الصراف الآلي في العراق منخفضة مقارنة ببعض الدول العربية الأخرى وهذا يستدعي

قيام المصارف بزيادة أجهزة الصراف الآلي لإيصال خدماتها للجمهور بسهولة وباقل التكاليف، الأمر الذي يتطلب من المصارف زيادة أعداد هذه الأجهزة لأجل تقديم أفضل الخدمات إلى الجمهور، مما يساعد في زيادة أعداد الزبائن الذين يدخلون في النظام المالي.



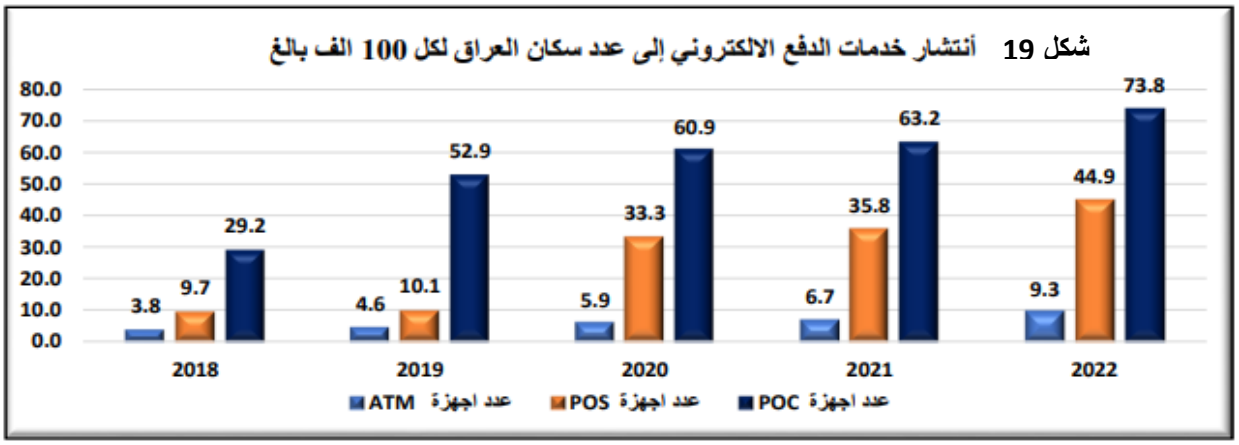
الشكل (18) ماكينات الصراف الالي لكل 100 ألف لعام 2021

المصدر: بيانات البنك الدولي:2021 https://data.albankaldawli.org/indicator/FB.ATM.TOTLview

أن انتشار خدمات الدفع الإلكتروني في العراق بين السكان لا يزال منخفض وكما موضح في الشكل (19) ويعود السبب في ذلك إلى أن معظم الأسواق والمحلات التجارية ما زالت تتعامل بالنقد مع استخدام محدود لأجهزة نقاط البيع الإلكترونية (POS) وهذا لا يقابل حجم الاعمال التجارية الداخلية خاصة في المناطق الشعبية والنائية، بسبب عدم انتشار ثقافة الدفع الإلكتروني بشكل واسع بين فئات المجتمع.

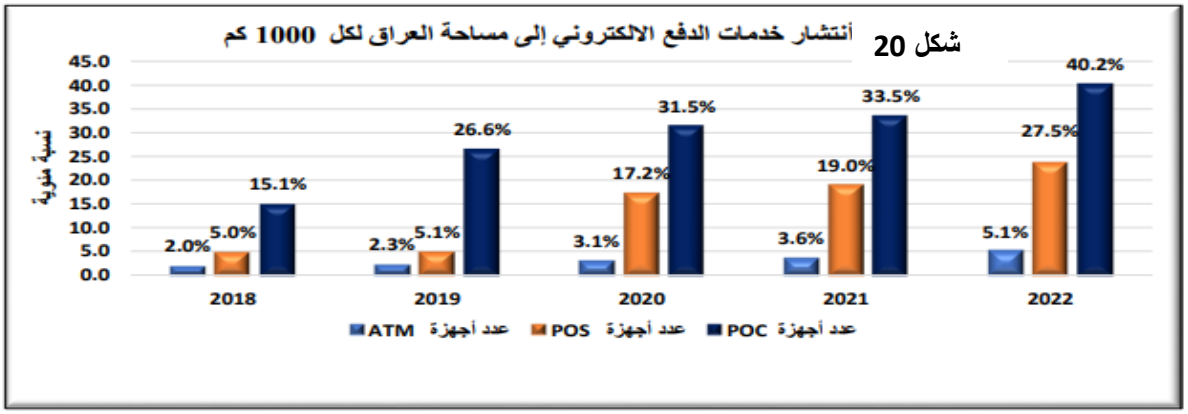
أما بالنسبة لأجهزة الصراف الآلي (ATM) فانتشارها مقتصر على المراكز التجارية والمجمعات التجارية التي تتمتع بدرجة حماية امنية عالية وبعض الدوائر الحكومية والمصارف وفروعها، وتشيرالأرقام المذكورة في الشكل (19) إلى وجود ارتفاع في استخدام خدمات الدفع الإلكتروني في العراق خلال عام 2022 فقد بلغ عدد أجهزة (ATM) إلى عدد السكان لكل 100 ألف بالغ (9.3) جهازمقارنة بـ (6.7) جهاز عام 2021 وارتفع عدد الاهزة حتى وصل إلى (73.8) جهاز في عام 2022.

أما أجهزة نقاط البيع (POS) جهاز، فقد ارتفعت أيضاً إلى (44.9) جهاز في عام 2022، مقارنة بـ (35.8) جهاز في عام 2021 منخفض وكما موضح في الشكل (19)، ولتعزيز انتشار خدمات الدفع الالكترونية في العراق يجب أن تعمل المصارف والشركات التجارية على زيادة عدد أجهزة الصراف الآلي ونقاط البيع وتوفيرها في مواقع عامة ومناطق نائية وكذلك يجب أن تتخذ الحكومة والجهات المعنية إجراءات تعزيز الوعي المالي وزيادة التوعية والتثقيف المالي للأفراد والشركات حول فوائد استخدام التعاملات المصرفية الالكترونية.



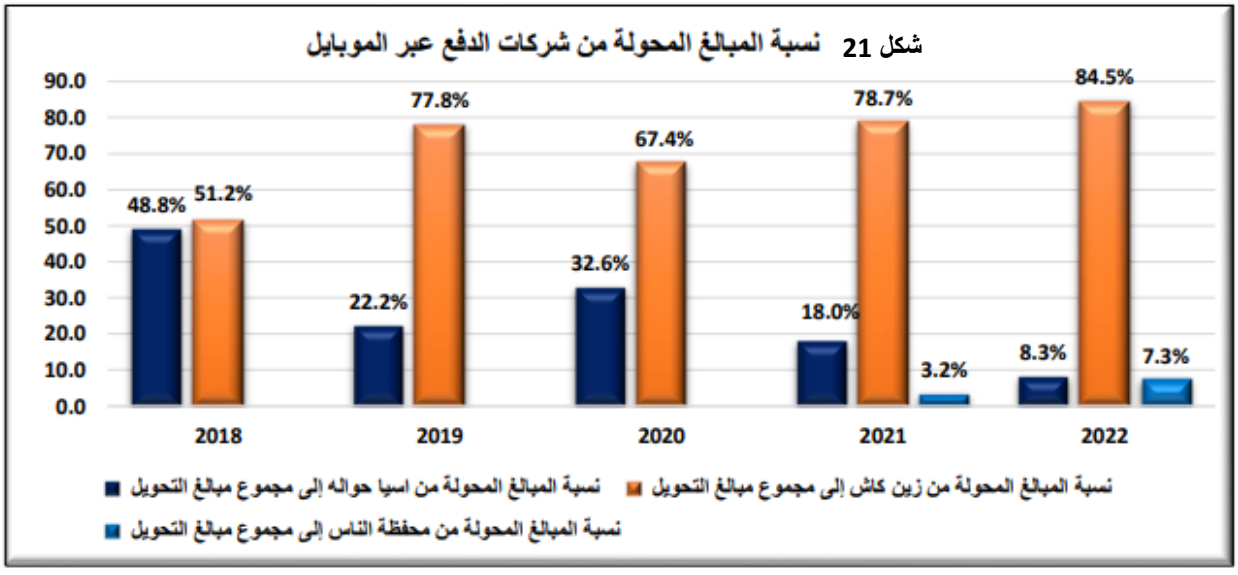
الشكل (19) نسبة انتشار خدمات الدفع الالكتروني الى عدد سكان العراق
المصدر: البنك المركزي العراقي، الموقع الاحصائي، 2022.

تعد خدمات الدفع الإلكتروني وسيلة سريعة وفعالة للوصول إلى الخدمات المالية والمصرفية، كما أنها تساهم في تقليل التكلفة، ويعمل البنك المركزي العراقي على زيادة انتشار هذه الخدمات، ويعد ذلك أحد أهدافه الرئيسه من اجل تحسين أنظمة الدفع الإلكتروني وتسهيل المبادلات الإلكترونية، ويمكن استخدام هذا المؤشر لقياس مستوى انتشار خدمات الدفع الإلكتروني لتقيم وتحليل مدى توافر هذه الخدمات واستخدامها في البلاد ومستوى الوعي والتعليم المالي لدى السكان، ويشهد القطاع المصرفي زيادة في انتشار أجهزة الصراف الآلي وأجهزة نقاط البيع وأجهزة السحب النقدي وذلك وفقا للبيانات المقدمة في الشكل (20) والذي يبين أن نسبة أعداد أجهزة الصراف الآلي إلى مساحة العراق قد زادت من (3.6) في عام 2021 إلى (5.1) في عام 2022، إما بالنسبة الأجهزة نقاط البيع زاد انتشارها من (19) في عام 2021 إلى (27.5) في عام 2022 وأجهزة الدفع فقد زادت أعدادها أيضاً من (33.5) في عام 2021 إلى (40.2) في عام 2022 ومن المتوقع أن تستمر هذه النسب في الارتفاع في المستقبل.



الشكل (20) نسبة انتشار خدمات الدفع الالكتروني الى مساحة العراق
المصدر: البنك المركزي العراقي، دائرة الاحصاء والابحاث، النشرة الاحصائية، 2022

إن التطور في نظام الدفع يُعد من أهم الأساليب التي يمكن بتعزيز الشمول المالي في أي اقتصاد، وإن عمليات الدفع عبر الموبايل تُعد أحد هذه الأساليب، إذ تسهل كثيراً من العمليات المالية وتساعد في إنجازها بسرعة ودقة لذلك فإن الوصول إلى عمليات الدفع عبر الموبايل وإنجاز معاملات مالية أخرى يمثل صورة متقدمة جدا من التطور المالي ويعكس هذا المؤشر مدى انتشار واستخدام التقنيات المتقدمة للدفع التي تعتمد على الهواتف المحمولة، وتشمل هذه التقنيات تطبيقات الدفع الرقمي والمحافظ الإلكترونية التي تسمح للزبائن بإجراء المعاملات المالية وإرسال واستقبال الأموال عبر هواتفهم المحمولة، اذ يسهم في توفير وصول سهل وفعال للخدمات المالية للفئات السكانية المختلفة، ووفقاً للشكل (21) الذي يوضح المبالغ المحولة من شركات الدفع عبر الموبايل، لوحظ أن هناك سيطرة لشركة زين كاش على عمليات التحويل المالي، حيث ارتفعت نسبة المبالغ المحولة منها كجزء من إجمالي المبالغ المحولة شركات الدفع عبر الموبايل من (77.8%) في عام 2019 وصولاً إلى (84.5%) في عام 2022 بالمقابل انخفضت نسبة شركة آسيا حوالة من (22.2%) في عام 2019 إلى (8.3%) في عام 2022. إما شركة محفظة الناس فبدئت عملها في عام 2020، وبسبب حداثة نشاطها كانت نسبة المبالغ المحولة عبرها منخفضة، لكنها ارتفعت من (3.2%) في عام 2021 إلى (7.3%) في عام 2022. ولوحظ أن زيادة المنافسة بين الشركات تسهم في التطور المالي وتعزز تطوير الخدمات المالية التي تقدمها الشركات، وهذا التنافس يحث الشركات على تحسين خدماتها وتوفير عروض أفضل للعملاء، مما يعزز التنمية الاقتصادية.



الشكل (21) نسبة المبالغ المحولة من شركات الدفع عبر الموبايل في العراق

المصدر: البنك المركزي العراقي، دائرة تقنية المعلومات والمدفوعات، 2022.

ثانياً : مؤشرات تطورالودائع والتعاملات الالكترونية في عينة من المصارف التجارية العراقية:

1- مصرف الخليج التجاري:

تأسس مصرف الخليج التجاري كشركه مساهمة خاصه في عام 1999 الصادرة من دائرة تسجيل الشركات وفق قانون الشركات رقم (21))21 لسنة 1997/ المعدل برأسمال قدره (600) مليون دينار، وباشر المصرف ممارسة اعماله عن طريق الفرع الرئيس في عام 2000 بعد حصوله على اجازة ممارسة الصيرفة الصادرة من البنك المركزي العراقي، ويقدم المصرف خدماته المتنوعة من فروعه المتعددة في كل من العاصمة بغداد وعدد من المحافظات العراقية وذلك من (18) فرعاً تضم العاصمة (10) فرعاً والمحافظات تتوزع عليها باقي الفروع وهي (14) فرعاً، وفرع واحد خارج العراق، وبدا في تقديم خدماته الالكترونية منذ عام 2008 وسعى المصرف الى تطبيق التقنيات الحديثة في إنجاز أعماله وإن هدف المصرف من تطبيق هذه التقنيات هو من اجل تطوير عمل المصرف ليتمكن من تقديم افضل التعاملات المصرفيةللزبائن وبذلك بدأ المصرف بإصدار البطاقات الالكترونية بمختلف انواعها، وفيما يتعلق بالصراف الالي فقد قام المصرف بنشر اجهزة الصراف الالي على فروعه لكي يتمكن الزبائن من الحصول على التعاملات المصرفية(التقرير السنوي لمصرف الخليج التجاري، 2022).

جدول (2)

حجم الودائع والتعاملات الالكترونية لمصرف الخليج التجاري للمدة (2013-2022)

السنوات	عدد اجهزة الصراف الالي	عدد البطاقات الالكترونية	عدد البنوك المراسلة	حجم الودائع المصرفية المبالغ (مليون)
2013	25	3510	2	417,143
2014	28	4100	4	455,212
2015	28	6590	6	409,221
2016	32	7290	5	427,201
2017	32	8920	5	256,804
2018	34	8530	6	233,978
2019	36	13820	7	201,579
2020	37	15300	10	180,767
2021	37	19330	12	204,967
2022	39	20330	12	225.447

المصدر :البنك المركزي العراقي النشرات الاحصائية وتقرير مصرف الخليج التجاري لسنوات متفرقة

نلاحظ من الجدول رقم (2) قيام المصرف بنشر اجهزة الصراف الالي على فروعه من اجل استفادة الزبائن من الخدمات التي توفرها هذه الاجهزة، اذ بلغ عدد الاجهزة خلال عام 2013 (25) جهاز موزعة

على فروع المصرف وبعد هذه المدة بدأ عدد الصرافات الالية يزداد الى ان وصل اعلى مستوى له خلال مدة الدراسة في عام 2022 اذ بلغ (39) جهاز، كما يلاحظ من الجدول انف الذكر التزايد في عدد البطاقات الالكترونية المستخدمة من قبل الزبائن بشكل كبير إذ بلغ عدد البطاقات في عام 2013 (3510) بطاقة الى ان وصل اعلى مستوى له خلال مدة الدراسة في عام 2022 اذ بلغ (20330) بطاقة، وفيما يتعلق بعدد عدد المصارف المراسلة اذ كان عدد المصارف المراسلة في عام 2013 مصرفين وبعدها زادت المصارف المراسلة لتصل في عام 2022 الى (12) مصرف، وهذا يشير إلى تطور الخدمات الالكترونية التي يقدمها المصرف من أضافة أجهزة صرافات الالية واصدار بطاقات الكترونية جديدة وزيادة عدد المصارف المراسلة الامر الذي انعكس على حصول زيادة كبيرة نمو الودائع في عام 2014 أذ بلغ نمو الودائع (455,212) مليون وبعدها بدأ بالانخفاض ليصل ادنى مستوياته خلال عام 2020 اذ بلغ (180.767) مليون بسبب الحرب على داعش وتعرض الاقتصاد العراقي لهزات وانتكاسات كبيرة لاسيما بعد ظهور جائحة كورونا وتراجع اسعار النفط وحالة الركود الاقتصادي للعالم اجمع والعراق بشكل خاص، وبعدها بدأ حجم الودائع بالتعافي ليصل في عام 2022 الى (225.447) مليون 8 انخفضت حجم الودائع إلى (233,978) وهذا مؤشر على نمو حجم الودائع خلال مدة الدراسة (التقرير السنوي لمصرف الخليج، 2022).

2- **مصرف بغداد التجاري**:

تأسس مصرف بغداد في 1992 ويعد أول مصرف خاص أسس في العراق وسمح به قانون البنك المركزي العراقي رقم (12) لسنة 1991 المعدل وبدأ المصرف برأس مال وقدرة (100) مليون دينار عراقي، وإتسعت أعمال المصرف الدولية خارج العراق فضلاً عن توسع أعمال المصرف داخل العراق بجذب الزبائن الجدد وتحسين التعاملات المصرفيةوزيادة أجهزة الصراف الالي بشكل ملحوظ وترتبط فروع المصرف بالمركز الرئيسى وكذلك فروع المصرف مع بعضها بنظام الشبكة الكترونية.

يقدم المصرف خدماته من فروعه التي تبلغ (32) فرعاً وهو واحد من أكبر المصارف التجارية الخاصة في العراق، وتطور المصرف من محلي الى عالمي خلال السنوات الماضية وهو يواصل في نموه في تقديم التعاملات المصرفيةللزبائن عبر الانترنيت بتطبيق الموبايل المصرفي الذي يقدم خدمات مصرفية الكترونية متنوعة، وتعد خدمة الصراف الآلي من الخدمات التي يقدمها مصرف بغداد والموجودة في اغلب الفروع (التقرير السنوي لمصرف بغداد، 2022).

جدول (3)
حجم الودائع والتعاملات الالكترونية لمصرف بغداد التجاري للمدة (2013-2022)

السنوات	عدد اجهزة الصراف الالي	عدد البطاقات الالكترونية	عدد البنوك المراسلة	حجم الودائع المصرفية المبالغ (مليار)
2013	50	47930	3	1,393
2014	45	60290	1	1,491
2015	45	72650	4	878
2016	47	85010	3	827
2017	48	97270	2	714
2018	50	109730	2	782
2019	32	122090	1	801
2020	51	134450	1	1,072
2021	52	148810	1	1,158
2022	81	159261	9	1,310

المصدر: المصدر :البنك المركزي العراقي – النشرات الاحصائية وتقرير مصرف بغداد لسنوات متفرقة

نلاحظ من الجدول رقم (3) قيام المصرف بنشر اجهزة الصراف الالي على فروعه من اجل استفادة الزبائن من الخدمات التي توفرها هذه الاجهزة، اذ بلغ عدد الاجهزة خلال عام 2013 (50) جهاز موزعة على فروع المصرف وبعدها لوحظ هنالك تزايد بشكل بسيط ومتذبذب ليصل خلال عام 2022 الى (81) جهازاً، كما يلاحظ من الجدول انف الذكر التزايد في عدد البطاقات الالكترونية المستخدمة من قبل الزبائن بشكل كبير إذ بلغ عدد البطاقات في عام 2013 (47930) بطاقة الى ان وصل خلال مدة الدراسة في عام 2022 اذ بلغ (159261) بطاقة، اما عدد المصارف المراسلة فكان المصرف يعتمد على ثلاثة مصارف في عام 2013 حتى وصل الى (9) مصارف مراسلة ، وكما يلاحظ من الجدول انف الذكر حصول زيادة كبيرة في نمو حجم الودائع اذ بلغت خلال عام 2013 (1,393) مليار واستمرت بالزيادة لتصل في عام 2014 (1,491) مليار، وهذا يشير إلى تطور نمو الودائع في المصرف من خلال أضافة فروع للمصرف، وفي الاعوام 2016- 2019 وبسبب تدهو الاوضاع انخفظت نسبة حجم الودائع وحسب مامبين في الجدول (3) ولكن لوحظ تطور وزيادة في نمو الودائع من عام 2020 وعندها بلغت (1,072) مليار حتى وصلت عام 2022 الى (1,310) مليار, وهذ مؤشر على تطور وزيادة التعاملات المصرفية الالكترونية ويرافقها زيادة في ثقة المودعين بزيادة حجم الودائع خلال مدة الدراسة.

3- مصرف الاهلي العراقي:

ان المصرف الاهلي العراقي هو شركة مساهمة خاصة عراقية تأسس بتاريخ 1995 ومركزه الرئيسى مدينة بغداد، لتبلغ الزيادة في رأسمال الشركة التابعة كما في عام 2013 (250) مليار دينار عراقي، ويقوم المصرف بتقديم جميع التعاملات المصرفيةوالمالية المتعلقة بنشاطه من مركزه الرئيسى في مدينة بغداد وفروعه البالغة (25) فرعاً المنتشرة داخل العراق ويقدم مجموعة من الخدمات الالكترونية سواء فتح الحساب أم الاستفسار عن الحساب أم التسوق الالكتروني أم السحب والتحويل وغيرها من التعاملات المصرفيةعبر الانترنيت (التقرير السنوي لمصرف الاهلي العراقي، 2022).

جدول (4)

حجم الودائع والتعاملات الالكترونية لمصرف الاهلي العراقي التجاري للمدة (2013-2022)

السنوات	عدد اجهزة الصراف الالي	عدد البطاقات الالكترونية	عدد البنوك المراسلة	حجم الودائع المصرفية المبالغ (مليار)
2013	3	7820	7	360
2014	5	8900	9	337
2015	8	11400	10	148
2016	12	12530	12	163
2017	17	14930	16	184
2018	42	18720	21	190
2019	50	23010	19	250
2020	25	30080	18	418
2021	28	39270	19	1,145
2022	140	63887	21	1,539

المصدر :البنك المركزي العراقي – دائرة المدفوعات – قسم العمليات وتقريرمصرف الاهلي العراقي لسنوات متفرقة

يبين الجدول رقم (4) أن أجهزة الصراف الآلي هي الأقل في مصارف العينة على الرغم من تطورها فقد كانت (3) أجهزة في عام 2013 وتزايدت حتى وصلت إلى 140 جهازاً، في المقابل تزايد عدد البطاقات الالكترونية من (7820) في عام 2013 ليصل الى (63887) في عام 2022 وانعكس ذلك التطور على تزايد في نمو حجم الودائع من (360) ملايين دينار إلى (1.539) مليار دينار في عام 2022، كما ان اعداد المصارف المراسلة تزايد بشكل بسيط ومتذبذب اذ بلغت في عام 2013 (7) مصرفا ليصل خلال عام 2022 الى (21) مصرفاً، ونلاحظ هناك تطور كبير وواضح خلال الاعوام الاخير من الدراسة فيما يخص نمو الودائع وباقي الموشرات المتمثلة بالخدمات الالكترونية التي يقدمها المصرف وهذا دليل على زياد الوعي وثقة المودعين والزبائن بشكل عام بالقطاع المصرفي وهذا جهد واضح في توفير خدمات تزيد من اقبال الجمهورعلى التعامل مع المصارف التجارية.

4- مصرف الشرق الاوسط العراقي للاستثمار:

تأسس مصرف الشرق الأوسط العراقي للإستثمار كشركة مساهمة خاصة برأسمال إسمي مقداره (400) مليون دينار عراقي، ويقوم المصرف بتقديم الأعمال المصرفية والمالية الالكترونية المتعلقة بنشاطه من خلال (18) فرعاً تعمل داخل العراق، منها خمسة فروع تعمل داخل بغداد وثلاثة عشر فرعاً خارجها، ويقدم المصرف خدمة الصراف الآلي لتقديم خدمة السحب النقدي السريع والاستعلام عن الرصيد وتقديم بطاقات الماستر كارد فضلاً عن انجاز اغلب معاملاته المصرفية عبر الموقع الالكتروني للمصرف (التقرير السنوي لمصرف الشرق الاوسط العراقي للاستثمار، 2022).

جدول (5)

حجم الودائع والتعاملات الالكترونية لمصرف الشرق الاوسط العراقي للاستثمار للمدة (2013-2022)

السنوات	عدد اجهزة الصراف الالي	عدد البطاقات الالكترونية	عدد البنوك المراسلة	حجم الودائع المصرفية المبالغ (مليون)
2013	6	8720	4	417,143
2014	7	9840	5	358,118
2015	10	12980	6	331,666
2016	11	13420	4	326,517
2017	23	14080	5	332,579
2018	41	14530	6	437,921
2019	51	24170	7	279,215
2020	62	53210	7	276,181
2021	37	64760	7	291,328
2022	78	69312	16	347,495

المصدر :البنك المركزي العراقي – دائرة المدفوعات – قسم العمليات وتقريرمصرف الاهلي العراقي لسنوات متفرقة

يبين الجدول رقم (5) قيام المصرف بنشر اجهزة الصراف الالي على فروعه من اجل استفادة الزبائن من الخدمات التي توفرها هذه الاجهزة، اذ بلغ عدد الاجهزة خلال عام 2013 (6) جهاز ولوحظ ارتفاعها بشكل كبيرومتزايد حتى وصل الى (78) جهاز، وفي المقابل بلغ عدد البطاقات الالكترونية (8720) في عام 2013 ليصل الى (69312) في عام 2022، وانعكس ذلك التطور على تزايد في نمو حجم الودائع من (417,143) مليون دينار وذلك لعد اسباب ذكرت سابقا, حيث بلغ اكبرنمو لحجم الودائع خلال عام 2018 بواقع (437,921) مليون دينار وبعدها بدات ازمة فايروس كرونا وعندها شهد الوضع المالي تدهورا وانعكس على القطاع المصرفي وبدا حجم الودائع المصرفية ينخفظ أذ بلغ في عام 2019 (279,215) مليون دينار واستمر الانخفاظ حتى عام 2020 (276,181) مليون، اما في عام 2021 بدأ تعافي الاقتصاد بشكل عام والقطاع المصرفي بشكل خاص وبلغ حجم الودائع (291,328) مليون مقارنة بالسنة السابقة حتى وصل

الارتفاع الى (347,495) خلال عام 2022 وهذا يشير الى ان هنالك تطور في التعاملات الالكتروني ونمو في حجم الودائع.

5- مصرف المنصور للاستثمار :

بدأ مصرف المنصور للاستثمار أعماله في العراق بداية عام 2006 برأسمال قدره (55) مليار دينار عراقي ليصل وبعد زيادات متتالية إلى 250 مليار دينار عراقي، ويعد مصرف المنصور شركة تابعة لمجموعة شركات بنك قطر الوطني، ويسعى في المصرف إلى التميز والريادة بتقديم مجموعة واسعة من الخدمات عبر (8) أفرع موزعة على أكبر وأهم المحافظات العراقية، وتمكن مصرف المنصور للاستثمار وبمدة قياسية جداً من تحقيق تقدم واضح وملموس في ممارسة أنشطته المصرفية على المستوى المحلي والدولي، وقد شملت خدماته المصرفية ماكينات الصراف الآلي والبطاقات الالكترونية وتحويلات الأموال وقبول الودائع بأنواعها ومنح القروض والسلف وفتح الإعتمادات المستندية وخطابات الضمان وعمليات التحويل المالي محلياً ودولياً (التقرير السنوي لمصرف المنصور للاستثمار ، 2022).

جدول (6)

حجم الودائع والتعاملات الالكترونية لمصرف المنصور للاستثمار للمدة (2013-2022)

السنوات	عدد اجهزة الصراف الالي	عدد البطاقات الالكترونية	عدد البنوك المراسلة	حجم الودائع المصرفية المبالغ (مليار)
2013	6	8720	4	485
2014	7	1295	7	568
2015	9	1420	7	753
2016	12	1659	9	781
2017	13	2081	11	978
2018	16	2317	14	1,215
2019	21	3002	16	1,130
2020	26	4398	19	925
2021	31	5917	21	377
2022	31	6200	21	387

المصدر :البنك المركزي العراقي – دائرة المدفوعات – قسم العمليات وتقرير مصرف المنصور لسنوات متفرقة

نلاحظ من الجدول رقم (6) قيام المصرف بنشر اجهزة الصراف الالي على فروعه التي تؤمن الخدمة على مدار 24 ساعة، اذ بلغ عدد الاجهزة خلال عام 2013 (6) جهاز موزعة على فروع المصرف وبعد هذه المدة بدأ عدد الصرافات الالية يزداد الى ان وصل اعلى مستوى له خلال مدة الدراسة في عام 2022 اذ بلغ (31) جهاز، كما يلاحظ من الجدول انف الذكر التزايد في عدد البطاقات الالكترونية المستخدمة من قبل

الزبائن بشكل كبير إذ بلغ عدد البطاقات في عام 2013 (8720) بطاقة الى ان وصلت خلال مدة الدراسة في عام 2022 (6200) بطاقة، وفيما يتعلق بعدد عدد المصارف المراسلة اذ كان عدد المصارف المراسلة في عام 2013 (4) مصارف وبعدها زادت المصارف المراسلة لتصل في عام 2022 الى (21) مصرف، وهذا يشير إلى تطور الخدمات الالكترونية التي يقدمها المصرف باضافة أجهزة صرافات الالية واصدار بطاقات الكترونية جديدة وزيادة عدد المصارف المراسلة لتدعم النمو في النشاط الاقتصادي عبر تسهيل التجارة الدولية والنشاطات المالية للمصارف العربية، اما بخصوص نمو حجم الودائع المصرفية فقد كان متفاوت في ارتفاع وانخفاض وهذا يعود الى عدة عوامل مرتبطة بالاوضاع التي مر بها العراق.

6- مصرف الموصل للاستثمار:

تأسس مصرف الموصل للتنمية والاستثمار كشركة مساهمة في عام 2001 برأسمال اسمي قدره مليار دينار عراقي، وشهد المصرف تطوراً ملموساً في هيكله التنظيمي ومجالات خدماته المقدمة بدءاً من رأس ماله الاسمي وصولاً إلى تعزيزه إلى (252.500) مليار دينار في عام 2015، وهناك (10) فروع للمصرف يقدم خدماته الالكترونية للزبائن منها خدمة الصراف الآلي اذ تمكن هذه الخدمة حاملي بطاقات من السحب على مدار 24 ساعة وتوفر المرونةفي السحب كونها منتشرة في اماكن متعددة وكذلك خدمة اصدار وتشغيل البطاقات الائتمانية التي توفر سحب النقود من خلال الصراف الآلي او التسوق عبر الانترنت فضلا عن قبول الودائع وغيرها من التعاملات المصرفية الالكترونية.

جدول (7)
حجم الودائع والتعاملات الالكترونية لمصرف الموصل للتنمية والاستثمار للمدة (2013-2022)

السنوات	عدد اجهزة الصراف الالي	عدد البطاقات الالكترونية	عدد البنوك المراسلة	حجم الودائع المصرفية المبالغ (بالمليون)
2013	6	1108	6	269
2014	16	14290	2	71
2015	26	18400	3	86
2016	42	23860	4	61
2017	51	31070	4	87
2018	67	38610	6	82
2019	77	40190	5	78
2020	87	76940	6	77
2021	87	86620	7	359
2022	93	89389	21	211

المصدر :البنك المركزي العراقي - دائرة المدفوعات - قسم العمليات ، مصرف الشرق الاوسط لسنوات متفرقة

نلاحظ من الجدول (7) بدأ المصرف بستة اجهزة خلال عام 2013 وبعدها تتزايد بشكل كبير وسريع خلال هذه مدة الدراسة حتى وصل الى (93) جهاز صراف آلي في عام 2022 مما يوضح ان المصرف يعمل بشكل جيد وينتشر بسرعة كبيرة وهناك عدد كبير من المتعاملين مع المصرف وهذا يرجع للخدمات التي يقدمها المصرف وسمعة المصرف وثقة الجمهور وزيادة الوعي المصرفي، وكان هناك تزايد في عدد البطاقات الالكترونية إذ بلغت (1108) في عام 2013 حتى وصلت في عام 2022 (89389) بطاقة، اما بالنسبة لنمو حجم الودائع فقد كان متفاوت في ارتفاع وانخفاض وكما مبين في الجدول(6) بسبب الحرب على داعش والاوضاع غير المستقرة بسبب الازمة المالية الكبيرة التي يعيشها العراق وهبوط اسعار النفط العالمية وزيادة العجز في موازنة عام 2016 إلى 30% ، وبدأ المصرف بالاعتماد على ستة مصارف مراسلة في عام 2013 حتى وصل الى 21 مصرفاً مراسلاً في عام 2022.

من تحليل وتفسير مؤشرات حجم الودائع والتعاملات المصرفية الالكترونية التي تقدمها المصارف التجارية العراقية للزبائن والمتمثلة بعدد ماكينات الصرافات الالية وعدد البطاقات الالكترونية وعدد المصارف المراسلة، يتضح للباحث منها زيادة في نمو حجم الودائع لاغلب المصارف التجارية العراقية عينة الدراسة فضلاً عن زيادة التعاملات المصرفية الالكترونية التي تقدمها المصارف التجارية للزبائن واعتمادها على التكنولوجيا المتقدمة في تقديم التعاملات المصرفية والتي تزيد فرص التعرض للمخاطر والهجمات السيبرانية الالكترونية ومن ثم لابد من وضع استراتجية شاملة لمواجهة تلك المخاطر والتهديدات السيبرانية الناتجة عن الزيادة الحاصلة في حجم التعاملات المصرفية الالكترونية المقدمة بتطبيق استراتيجية المرونة السيبرانية التي تودي الى حماية مدخرات المودعين ومعلوماتهم الشخصية من الاختراقات السيبرانية والتكيف مع المخاطر والهجمات السيبرانية، ويمكن القول إن زيادة التعاملات المصرفية الالكترونية وتطبيق استراتيجية المرونة السيبرانية تعملان سوياً على تعزيز الثقة لدى المودعين في القطاع المصرفي وتعزيز الاستقرار والنمو في هذا القطاع.

" المبحـــــث الثاني"

اختبار أدوات التحليل وبيانات الدراسة

تمهيد

لضمان صحة اختبارات فرضيات الدراسة، ولضمان دقة اختيار نوعية الاختبارات الإحصائية والنتائج النهائية بغية الوصول الى النتائج الصحيحة، اخضع مقياس الدراسة وبياناتها الى جملة اختبارات:

أولاً– ترميز متغيرات الدراسة وتوصيفها:

الجدول الاتي يبين تفصيلا لمتغيرات الدراسة، حيث ان المتغير المستقل يتمثل في (استراتيجية المرونة السبرانية) وابعادها الفرعية ، والمتغير المعتمد (ثقة المودعين) وابعادها الفرعية، وكما في الجدول الاتي:

الجدول (8) الترميز والتوصيف

المتغير	البعد	الرمز	عدد العبارات	المصدر
استراتيجية المرونة السبرانية	الحوكمة	Gov.	5	(Tsena et al. 2023:6)
	الحماية	Prot.	5	
	الاكتشاف	Disc.	5	
	الاستجابة	Resp.	5	
	الاستعادة والتقييم	Reco.	5	
ثقة المودعين	الكفاءة والقدرة	Comp.	5	(شوابية, عفاف، 2023: 49)
	المنفعة	Ben.	5	
	الامان	Saf.	5	

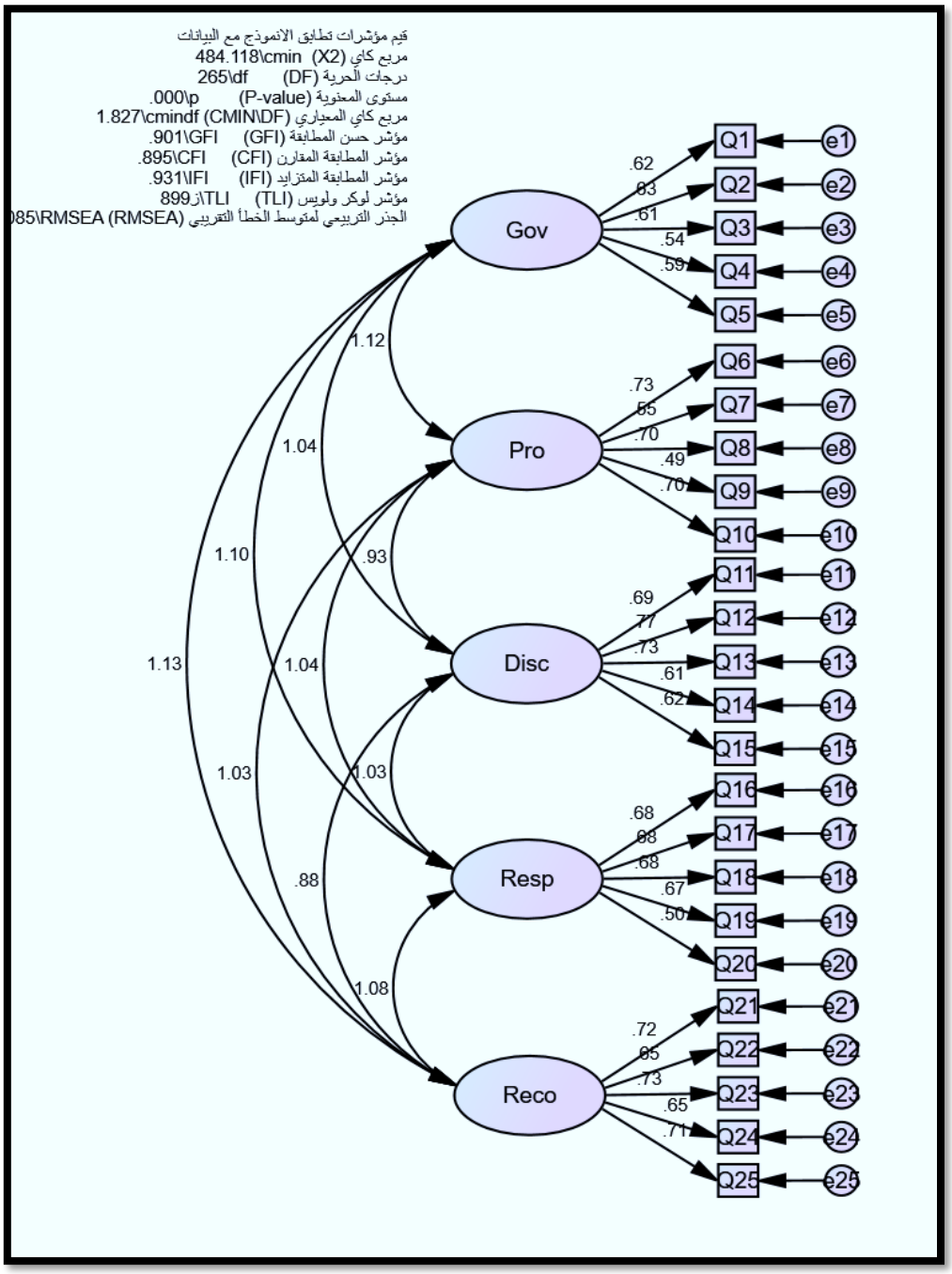
المصدر: إعداد الباحث

ثانياً: اختبار أداة الدراسة:

1- التحليل العاملي التوكيدي لمتغير استراتيجية المرونة السبرانية:

بهدف التحقق من الصدق البنائي لمقياس الدراسة ودقتها ميدانيا، استخدم الباحث التحليل العاملي التوكيدي وبالافادة من البرنامج الاحصائي (AMOS,24)، علما انه اعتمدت مؤشرات مطابقة النموذج التي أوصى بها (Hair etal,2010). ويبين الشكل (22) الاتي ان التحليل العاملي التوكيدي لمتغيراستراتيجية المرونة السبرانية الذي يتكون من خمسة ابعاد فرعية و(25) سؤال، ويلاحظ ان التشبعات

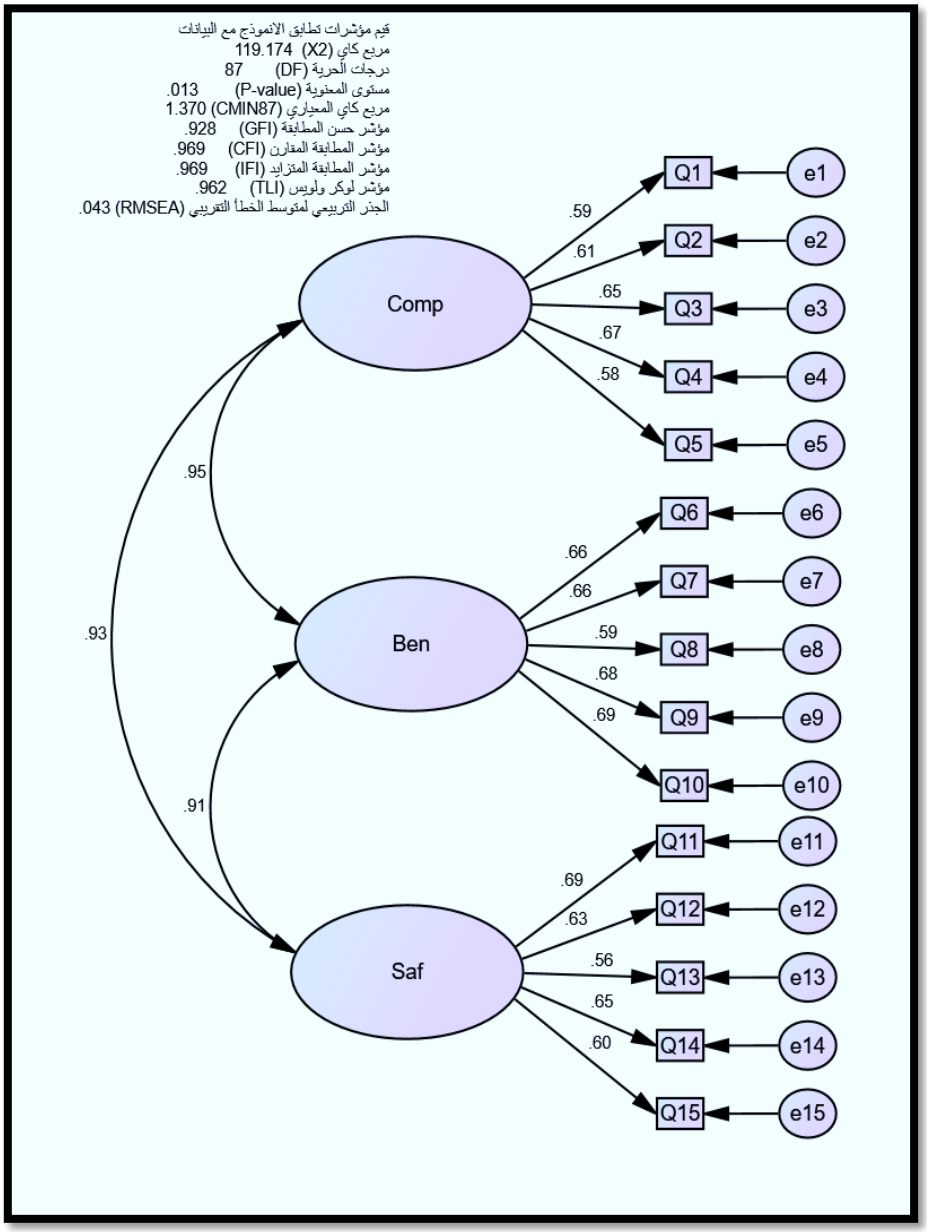
المعيارية (Standardized Estimations) الظاهرة على الأسهم التي تربط المتغيرات الكامنة (Latent variables) مع المتغيرات المقاسة (Observed variables) كانت ضمن النسبة المقبولة البالغة (0.40)، علما ان القيمة الحرجة (Critical ratio) لهذه التشبعات تجاوزت (1.96) مما يدل على معنويتها عند مستوى (5%)، علما ان مؤشرات مطابقة النموذج كانت من الحدود المقبولة.



شكل (22) التحليل العاملي التوكيدي لمتغيراستراتيجية المرونة السبرانية

2- التحليل العاملي التوكيدي لمتغير ثقة المودعين:

يبين الشكل (23) الاتي ان التحليل العاملي التوكيدي لمتغير ثقة المودعين بصفته متغيرا معتمدا، يتكون من ثلاثة ابعاد فرعية و(15) سؤال، ويلاحظ ان التشبعات المعيارية (Standardized Estimations) الظاهرة على الأسهم التي تربط المتغيرات الكامنة (Latent variables) مع المتغيرات المقاسة (Observed variables) لباقي الاسئلة كانت ضمن النسبة المقبولة البالغة (0.40)، علما ان القيمة الحرجة (Critical ratio) لهذه التشبعات تجاوزت (1.96) مما يدل على معنويتها عند مستوى (5%)، علما ان مؤشرات مطابقة النموذج كانت ضمن الحدود المقبولة.



شكل (23) التحليل العاملي التوكيدي لمتغير ثقة المودعين

ثالثا: صدق وثبات واتساق أداة الدراسة:

من اهم المقاييس المستخدمة في قياس ثبات الاستبانة هو مقياس (Cronbach's Alpha)، ويهدف الباحث من استخدام هذا النوع من التحليل التأكد من ان المقياس سيعطي نفس النتائج اذ اعيدت التجربة مرة أخرى على نفس العينة، علما ان (Urasachi etal,2015:681) يشيرون انه في العلوم السلوكية عندما تكون قيمة معامل الثبات (0.60) فانها تعد قيمة مقبولة، ويبين الجدول (9) الاتي قيم اختبار (Alpha Chronbach's) لمتغيرات الدراسة. اما الصدق (Validity) هو ان مقياس الدراسة يقيس فعلا ما وضع لقياسه، بمعنى اخر هل ان المقياس يقيس الظاهرة تحت الدراسة وليس شيء اخر (Sekrana,2003:206)، علما ان استمارة الاستبيان اخضعت للصدق الظاهري بعرضها على مجموعة خبراء (ملحق).

جدول (9) قيم معامل الثبات لأبعاد متغيرات الدراسة

ت	الابعاد	قيم معامل Cronbach's Alpha
1	الحوكمة	0.73
2	الحماية	0.77
3	الاكتشاف	0.81
4	الاستجابة	0.78
5	الاستعادة والتقييم	0.82
	استراتيجية المرونة السبرانية	0.95
1	الكفاءة والقدرة	0.76
2	المنفعة	0.79
3	الامان	0.76
	ثقة المودعين	0.90

المصدر: اعداد الباحث

يتضح من الجدول انف الذكر ان قيم معاملات كافة (Cronbach's Alpha) ضمن الحدود المقبولة احصائيا مما يجعل الباحث مطمئن الى النتائج التي سيتوصل اليها.

كما قام الباحث باحتساب الاتساق الداخلي من معامل ارتباط (Pearson) من اجل التأكد من الاتساق الداخلي بين كل بعد من ابعاد الدراسة والاسئلة المكونة له وعلى النحو الاتي:

1- الاتساق الداخلي لمتغيراستراتيجية المرونة السبرانية: يبين الجدول الاتي قيم علاقات الارتباط بين الأسئلة المكونة لمتغير استراتيجية المرونة السبرانية

جدول(10) احتساب الاتساق الداخلي لمتغير استراتيجية المرونة السبرانية

البعد	السؤال	قيمة علاقة الارتباط
الحوكمة	1	0.68**
	2	0.79**
	3	0.66**
	4	0.72**
	5	0.62**
الحماية	6	0.73**
	7	0.72**
	8	0.78**
	9	0.59**
	10	0.81**
الاكتشاف	11	0.72**
	12	0.84**
	13	0.75**
	14	0.73**
	15	0.75**
الاستجابة	16	0.71**
	17	0.70**
	18	0.78**
	19	0.80**
	20	0.66**
الاستعادة والتقييم	21	0.76**
	22	0.70**
	23	0.81**
	24	0.76**
	25	0.77**

المصدر : من اعداد الباحث

**معنوي بمستوى 1%

يلاحظ من الجدول انف الذكر ان جميع الأسئلة حققت معاملات ارتباط موجبة وذات دلالة إحصائية عند مستوى 1%، الامر الذي يعزز التحليل العاملي التوكيدي، وانه سيأخذ اخذ جميع الاسئلة بالحسبان الاعتبار عند تحليل استجابات افراد العينة لاحقا، علما ان هذا التحليل يدعم نتائج التحليل العاملي التوكيدي، الذي خلص الى عدم حذف اي سؤال من اسئلة المتغير، كذلك عدم وجود أية مؤشرات للتعديل.

2- الاتساق الداخلي لمتغير ثقة المودعين: يبين الجدول الاتي قيم علاقات الارتباط بين الأسئلة المكونة لمتغير ثقة المودعين.

جدول (11) احتساب الاتساق الداخلي لمتغير ثقة المودعين

البعد	السؤال	قيمة علاقة الارتباط
الكفاءة والمقدرة	1	0.69**
	2	0.75**
	3	0.72**
	4	0.76**
	5	0.63**
المنفعة	6	0.73**
	7	0.76**
	8	0.71**
	9	0.76**
	10	0.73**
الامان	11	0.76**
	12	0.72**
	13	0.67**
	14	0.72**
	15	0.70**

المصدر : من اعداد الباحث

**معنوي بمستوى 1%

يلاحظ من الجدول انف الذكر ان جميع الأسئلة حققت معاملات ارتباط موجبة وذات دلالة إحصائية عند مستوى 1%، الامر الذي يعزز التحليل العاملي التوكيدي، وانه سيؤخذ اخذ جميع الاسئلة بالحسبان الاعتبار عند تحليل استجابات افراد العينة لاحقا.

رابعا – اختبار التوزيع الطبيعي للبيانات:

تهدف الدراسة الى معرفة مدى تأثير استراتيجية المرونة السبرانية في ثقة المودعين، مما يدل على ضرورة اعتماد تحليل الانحدار الذي من اهم شروطة هو اعتدالية توزيع بيانات الدارسة، وعلى الرغم من استخدام الباحث لعينة كبيرة، ومن ثم فانه وفقاً لنظرية النهاية المركزية (Central Limit Theorem) ولكون حجم العينة اكبر من (50) مفردة فان التوزيع الاحتمالي لهذه البيانات يقترب من التوزيع الطبيعي (Pituch & Stevens,2016:224). مع ذلك احتسب الباحث قيم معامل(Kolmogorov-Smirnov)

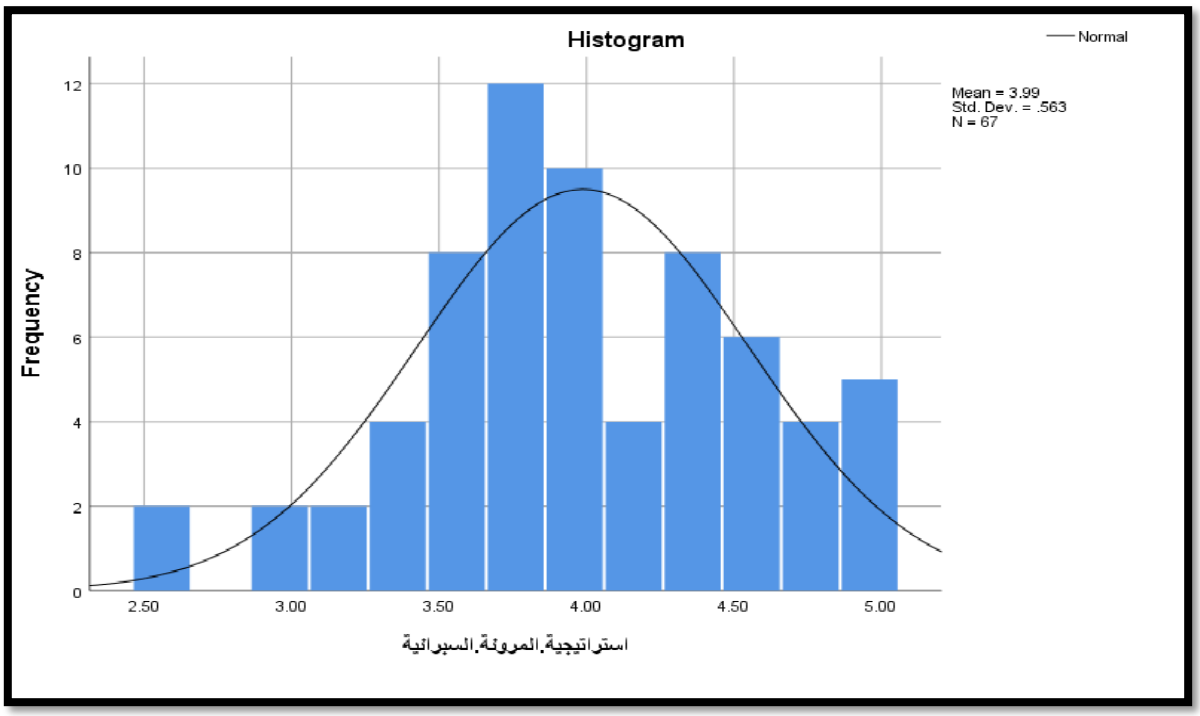
لمتغير استراتيجية المرونة السبرانية لتأكيد من خضوع البيانات للتوزيع الطبيعي،فكانت النتيجة كما يبينها الجدول (12) ادناه

جدول(12) التوزيع الطبيعي لمتغيراستراتيجية المرونة السبرانية

Tests of Normality						
	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	Df	Sig.
استراتيجية المرونة السبرانية	0.070	67	0.200*	0.980	67	0.362

المصدر: اعداد الباحث

تدعم نتائج الجدول انف الذكر الباحث من اجل اجراء الاختبارات المعلمية لاختبار فرضيات الدراسة، ويبن الشكل (24) ادناه المدرج التكراري الخاص بمتغير المرونة السبرانية حيث يتبين خضوع المتغير للتوزيع الطبيعي



المصدر: اعداد الباحث شكل (24) المدرج التكراري الخاص بمتغيراستراتيجية المرونة السيبرانية

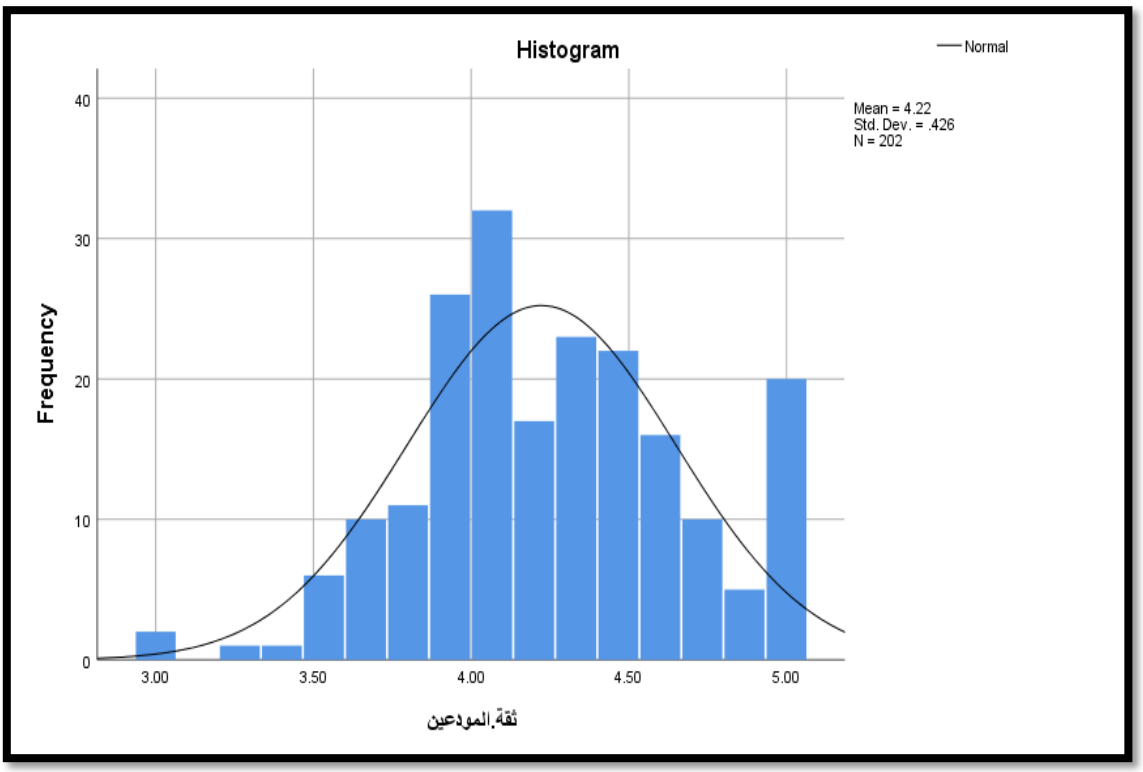
وكذلك احتسب الباحث قيم معامل (Kolmogorov-Smirnov) لمتغير ثقة المودعين السبرانية لتأكد من خضوع البيانات للتوزيع الطبيعي، فكانت النتيجة كما يبينها الجدول (13) ادناه

جدول(13) التوزيع الطبيعي لمتغير ثقة المودعين

Tests of Normality						
	Kolmogorov-Smirnova			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	Df	Sig.
ثقة المودعين	0.080	202	0.200*	0.970	202	0.301

المصدر: اعداد الباحث

تدعم نتائج الجدول أنف الذكر الباحث من اجل اجراء الاختبارات المعلمية لاختبار فرضيات الدراسة، ويبن الشكل (25) ادناه المدرج التكراري الخاص بمتغير ثقة المودعين حيث يتبين خضوع المتغير للتوزيع الطبيعي.



المصدر: اعداد الباحث شكل (25) المدرج التكراري الخاص بمتغير ثقة المودعين

" المبحـــث الثالث"

عرض نتائج الدراسة وتحليلها وتفسيرها

تمهيد

سيقوم الباحث اولا بتحليل الأوساط الحسابية الموزونة والانحرافات المعيارية وشدة الإجابة ومستواها بهدف تكوين تصور عن مدى ادراك مجتمع الدراسة لتوافر المتغيرات المبحوثة فيه. علما ان الباحث اعتمد (Nakapan & Radsiri , 2012 : 573) من اجل الحكم على الوسط الحسابي الموزون، ويبين الجدول الاتي التصنيف المعتمد.

جدول (14) تصنيف الوسط الحسابي الموزون

تدرج الاستبانة	مستوى الاستجابة	الوسط الحسابي الموزون	
		من	الى
لا اتفق تماما	منخفض جدا	1	1.80
لا اتفق	منخفض	1.81	2.60
معتدل	معتدل	2.61	3.40
اتفق	مرتفع	3.41	4.20
اتفق تماما	مرتفع تماما	4.21	5

المصدر: اعداد الباحث بالاعتماد على (Nakapan & Radsiri , 2012 : 573)

أولا: – المتغير المستقل استراتيجية المرونة السبرانية

1- الحوكمة:

الجدول (15) الاتي يتضمن الاوساط الحسابية الموزونة والانحرافات المعيارية ومستوى الإجابة وشدتها لكل سؤال من أسئلة بعد الحوكمة وبشكل اجمالي. أن السؤال (4) حقق أعلى وسط حسابي موزون بلغ(4.09) وبانحراف معياري (0.92) مما يدل على ان المصارف عينة الدراسة يولون اهتمام كبير بالحد من عمليات اختراق انظمة مصارفهم لما لها من تاثير كبير في ثقة المودعين، وحصل السؤال على مستوى إجابة مرتفع، ونال السؤال المذكور شدة إجابة بلغت (81.79%). أما السؤال(1) فقد حقق على أقل الأوساط الحسابية بمقدار (3.97) بانحراف معياري (0.82) وهو من بين الأعلى من الأسئلة الأخرى مما يدل على ضعف انسجام الإجابات تجاه هذا السؤال قياسا بباقي الأسئلة الأخرى التي تشكل منها المتغير . وبلغت شدة الإجابة لها السؤال (79.40%). يتمتع هذا السؤال بمستوى إجابة مرتفع.

حقق بعد الحوكمة وسطاً حسابياً موزوناً عاما بلغ (4.01) وانحراف معياري (0.81)، وبلغت شدة الاجابة (80.30%) وقد حصل هذا البعد على مستوى إجابة (مرتفع)، مما يعني قوة استخدام المصارف عينة الدراسة لبعد الحوكمة من ضمن المتغير استراتيجية المرونة السبرانية.

جدول (15) الإحصاء الوصفي لبعد الحوكمة (n=67)

ت	العبارة	الوسط الحسابي	شدة الإجابة %	الانحراف المعياري	مستوى الاجابة
1	يعتمد المصرف استراتيجية للمرونة السيبرانية ويتم تطويرها والاعتماد عليها ضمن عمله.	3.97	79.40	0.82	مرتفع
2	تؤخذ المعايير الدولية الحديثة (ISO22316) بالحسبان عند تطبيق استراتيجيات العمل المصرفي.	3.97	79.40	0.76	مرتفع
3	يقوم المصرف بمراجعة استراتيجية المرونة السيبرانية كلما حدث تغيير في تكنولوجيا المعلومات في المصرف.	3.99	79.70	0.83	مرتفع
4	تتضمن المرونة السيبرانية عمليات اشعار الجهات المختصة بالمصرف عن أي حالة اختراق لبيانات المودعين والعملاء.	4.09	81.79	0.92	مرتفع
5	تتضمن استراتيجية المرونة السيبرانية إجراءات واضحة (مثل بروتوكولات الاتصال وعمليات اتخاذ القرار) لاتخاذ القرارات في الوقت المناسب في حالة وقوع هجوم سيبراني.	4.06	81.19	0.74	مرتفع
	الحوكمة	4.01	80.30	0.81	مرتفع

المصدر: إعداد الباحث

2- **الحماية:**

يبين الجدول (16) تحليلا وصفيالاسئلة بعد الحماية وبشكل اجمالي. حقق السؤال (6) أعلى وسط حسابي موزون بلغ(4.21)وبانحراف معياري (0.71) مما يدل على قوة اعتماد المصارف عينة الدراسة اتخاذ تدابير الحماية من الهجمات الالكترونية، وحصل السؤال على مستوى إجابة مرتفع جدا، ونال السؤال المذكور شدة إجابة بلغت (84.18%). أما السؤال(9) فقد حقق على أقل الأوساط الحسابية بمقدار (3.94) بانحراف معياري (0.76). وبلغت شدة الإجابة لهذا السؤال (78.81%). يتمتع هذا السؤال بمستوى إجابة مرتفع ولكن مستوى تبنيه من قبل مجتمع الدراسة كان اقل من مستوى تبني الاسئلة الأخرى.

ان بعد الحماية حقق وسطاً حسابياً موزوناً عاما بلغ (4.04) وانحراف معياري (0.81)،وبلغت شدة الاجابة (80.90%) وقد حصل هذا البعد على مستوى إجابة (مرتفع). ان النتائج تدل على ارتفاع مستوى الحماية في التطبيقات الالكترونية المعتمدة من قبل المصارف عينة الدراسة.

جدول (16) الإحصاء الوصفي لبعد الحماية (n=67)

ت	العبارة	الوسط الحسابي	شدة الإجابة %	الانحراف المعياري	مستوى الاجابة
6	تؤخذ التدابير الأمنية لحماية البرامج والشبكات والأجهزة في المصرف من الحوادث السيبرانية.	4.21	84.18	0.71	مرتفع جدا
7	تفحص التقنيات القديمة بانتظام (بشكل دوري) لتحديد نقاط الضعف المحتملة والبحث عن فرص للترقية.	4.07	81.49	0.80	مرتفع
8	هناك ضوابط تمنع الأجهزة غير الخاضعة للرقابة من الاتصال بشبكتها الداخلية (مثل الأجهزة الشخصية) ونقاط النهاية (مثل الوسائط الممكنة للإزالة) من داخل المبنى وخارجه.	4.03	80.60	0.83	مرتفع
9	تكون ملفات تعريف وصول مودعين المصرف محددة وموثقة ويمكنهم الوصول الى ملفات تعريفهم بشكل واضح وسهل وامن.	3.94	78.81	0.76	مرتفع
10	يدرب جميع الموظفين (بشكل دوري) لدعم الامتثال لسياسة أمن المعلومات والإبلاغ عن الحوادث السيبرانية.	3.97	79.40	0.94	مرتفع
	الحماية	4.04	80.90	0.81	مرتفع

المصدر: اعداد الباحث

3- الاكتشاف

الجدول (17) يتضمن الاوساط الحسابية الموزونة والانحرافات المعيارية ومستوى الإجابة وشدتها لكل سؤال من أسئلة بعد الاكتشاف وبشكل اجمالي. حقق السؤال (11) أعلى وسط حسابي موزون بلغ (4.09) وبانحراف معياري (0.81) مما يدل على قوة ادراك اعضاء العينة لوجود عدة مستويات للكشف عن حالات الاختراق التي يمكن ان تتعرض لها المصارف وحصل السؤال على مستوى إجابة مرتفع ، ونال السؤال

المذكور شدة إجابة بلغت (81.79%). أما السؤال (15) فقد حقق على أقل الأوساط الحسابية بمقدار (3.85) بانحراف معياري (0.89) وهو الأعلى من بين الأسئلة الأخرى مما يدل على ضعف انسجام الإجابات تجاه هذا السؤال قياسا بباقي الأسئلة الأخرى التي تشكل منها المتغير، وبلغت شدة الإجابة لهذا السؤال (77.01%) يتمتع هذا السؤال بمستوى إجابة مرتفع.

ان بعد الاكتشاف حقق وسطاً حسابياً موزوناً عاما بلغ (3.96) وانحراف معياري (0.83)،وبلغت شدة الاجابة (79.16%) وقد حصل هذا البعد على مستوى إجابة (مرتفع). ان النتائج تدل على ان المصارف عينة الدراسة تولي اهتمام مضاعف لاكتشاف اية اشارات يمكن ان تدل على خطر يصيب نظامها الالكتروني بهدف المحافظة على ثقة المودعين.

جدول (17) الإحصاء الوصفي لبعد الاكتشاف (n=67)

ت	العبارة	الوسط الحسابي	شدة الإجابة %	الانحراف المعياري	مستوى الاجابة
11	توجد ضوابط كشف متعددة لدى المصرف لإمكانية الكشف المبكر عن الاختراقات التي يتعرض لها .	4.09	81.79	0.81	مرتفع
12	هناك قدرات وبرامج كشف مستمدة من معلومات التهديد أو الضعف العامة وغير المعروفة بعد.	3.94	78.81	0.83	مرتفع
13	هناك حدود تنبيه محددة لأنظمة المراقبة والكشف من أجل تحفيز وتسهيل عملية الاستجابة للحوادث السيبرانية.	3.99	79.70	0.79	مرتفع
14	ان عمليات المصرف الحالية تراقب التعاملات السيبرانية التي لا تتماشى مع السياسة الأمنية.	3.93	78.51	0.84	مرتفع
15	يوجد في المصرف برنامج استخباراتي للتهديدات السيبرانية يفحص بشكل دوري.	3.85	77.01	0.89	مرتفع
	الاكتشاف	3.96	79.16	0.83	مرتفع

المصدر: إعداد الباحث

4- **الاستجابة:**

الجدول (18) يتضمن الاوساط الحسابية الموزونة والانحرافات المعيارية ومستوى الإجابة وشدتها لكل سؤال من أسئلة بعد الاستجابة وبشكل اجمالي. حقق السؤال (16) أعلى وسط حسابي موزون بلغ (4.12) وبانحراف معياري (0.84) مما يدل على وجود خطط بديلة لدى المصارف للتعامل مع الحالات الطارئة وحصل السؤال على مستوى إجابة مرتفع ، ونال السؤال المذكور شدة إجابة بلغت (82.39%).

أما السؤال (19) فقد حقق على أقل الأوساط الحسابية بمقدار (3.85) بانحراف معياري (0.97) وهو الأعلى من بين الأسئلة الأخرى مما يدل على ضعف انسجام الإجابات تجاه هذا السؤال قياسا بباقي الأسئلة الأخرى التي تشكل منها المتغير.وبلغت شدة الإجابة لهذا السؤال (77.01%). يتمتع هذا السؤال بمستوى إجابة مرتفع. ان بعد الاستجابة حقق وسطاً حسابياً موزوناً عاما بلغ (3.98) وانحراف معياري (0.84)، وبلغت شدة الاجابة (79.52%) وقد حصل هذا البعد على مستوى إجابة (مرتفع). ان النتائج تدل على ان المصارف عينة الدراسة لديها وبشكل جيد خطط للاستجابة لاية هجمات وتلافيها يمكن ان يتعرض لها المصرف اثناء تقديم خدماته للزبائن.

جدول (18) الإحصاء الوصفي لبعد الاستجابة (n=67)

ت	العبارة	الوسط الحسابي	شدة الإجابة %	الانحراف المعياري	مستوى الاجابة
16	توجد خطة للاستجابة للحوادث السيبرانية وفريق الاستجابة للحوادث المماثلة في المصرف.	4.12	82.39	0.84	مرتفع
17	تصمم أنظمة وعمليات الوظائف الحيوية في المصرف للحد من تأثير الحوادث السيبرانية.	4.00	80.00	0.78	مرتفع
18	تسمح السياسات والعمليات والإجراءات في المصرف باحتواء الهجوم السيبراني قبل أن يؤدي إلى إتلاف الأنظمة الحيوية أو العمليات التجارية.	3.91	78.21	0.87	مرتفع
19	يمكن أن تتخذ هذه الاستجابات أشكالًا مختلفة اعتمادًا على طبيعة الحوادث السيبرانية.	3.85	77.01	0.97	مرتفع
20	تشتمل عملية المراجعة المستقلة على آليات للاستجابة لطلبات وكالات إنفاذ القانون والمودعين والشركاء والمشاركين في النظام ومقدمي الخدمات.	4.00	80.00	0.74	مرتفع
	الاستجابة	3.98	79.52	0.84	مرتفع

المصدر: إعداد الباحث

5- الاستعادة والتقييم:

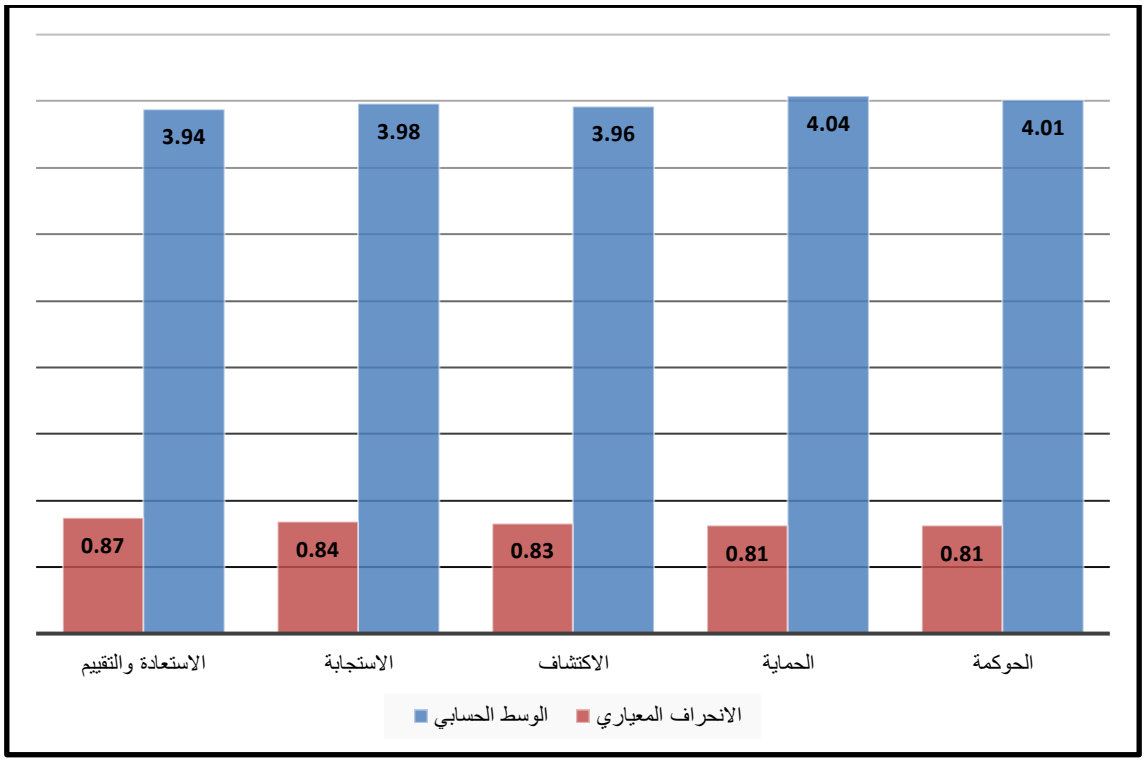
الجدول (19) يتضمن الاوساط الحسابية الموزونة والانحرافات المعيارية ومستوى الإجابة وشدتها لكل سؤال من أسئلة بعد الاستعادة والتقييم وبشكل اجمالي. حقق السؤال (21) أعلى وسط حسابي موزون بلغ(4.21) وبانحراف معياري (0.64) مما يدل على انه يمكن استعادة كل عمليات المصارف في حال تعرضها لهجمات سبرانية، حيث ان هناك نسخ احتياطية منها،وحصل السؤال على مستوى إجابة مرتفع جدا ونال السؤال المذكور شدة إجابة بلغت (84.18%). أما السؤال (22) فقد حقق على أقل الأوساط الحسابية بمقدار (3.67) بانحراف معياري (0.89) وهو الأعلى من بين الأسئلة الأخرى مما يدل على ضعف انسجام الإجابات تجاه هذا السؤال قياسا بباقي الأسئلة الأخرى التي تشكل منها المتغير.وبلغت شدة الإجابة لهذا السؤال (73.43%). يتمتع هذا السؤال بمستوى إجابة مرتفع.

ان بعد الاستجابة حقق وسطاً حسابياً موزوناً عاما بلغ (3.99) وانحراف معياري (0.83)،وبلغت شدة الاجابة (79.75%) وقد حصل هذا البعد على مستوى إجابة (مرتفع). ان النتائج تدل على ان المصارف عينة الدراسة لديها وبشكل جيد القدرة على استعادة نشاطاتها وخدمة زبائنها خلال وقت قياسي، بفضل انظمة الحماية المتاحة لديها. جدول (19) الإحصاء الوصفي لبعد الاستعادة والتقييم (n=67)

ت	العبارة	الوسط الحسابي	شدة الإجابة %	الانحراف المعياري	مستوى الاجابة
20	يضع المصرف خطط لاستعاد نظام العمل بعد تعرضه للهجمات السيبرانية .	4.10	82.09	0.84	مرتفع
21	يمكن استعادة الأنظمة والعمليات والتعاملات المصرفيةفي المصرف من نسخ احتياطية موثوقة.	4.21	84.18	0.64	مرتفع جدا
22	تسمح السياسات والإجراءات والأنظمة في المصرف باستئناف العمليات خلال ساعتين منذ وقوع الحادث السيبراني.	3.67	73.43	0.89	مرتفع
23	تسمح الأنظمة باسترداد البيانات بسرعة بعد اختراقها مما يضمن سلامة تلك البيانات.	3.87	77.31	0.83	مرتفع
24	يكون المصرف قادر على تحديد الأنظمة والبيانات التي تم اختراقها بعد وقوع حادث سيبراني.	3.87	77.31	1.00	مرتفع
25	يضع المصرف خطط لاستعاد نظام العمل بعد تعرضه للهجمات السيبرانية .	3.94	78.87	0.87	مرتفع
	الاستعادة والتقييم	3.99	79.75	0.83	مرتفع
	استراتيجية المرونة السبرانية	4.10	82.09	0.84	مرتفع

المصدر: إعداد الباحث

ومما تنبغي الإشارة أليه هو أن متغير المرونة السبرانية حقق وسطا حسابيا موزونا عاما (4.10)، بانحراف معياري (0.84)، وشدة إجابة بلغت (82.09%). مما يدل بشكل عام على توافر ابعاد المرونة السبرانية في المصارف عينة الدراسة. ويبين الشكل الاتي مقارنة بين ابعاد المرونة السبرانية من حيث اوساطها الحسابية وانحرافاتها المعيارية.



المصدر : اعداد الباحث شكل (26) مقارنة ابعاد استراتيجية المرونة السبرانية

تبين بشكل عام إدراك عينة الدراسة لتوافر ابعاد استراتيجية المرونة السبرانية ، ولقد احتل بعد الحماية المرتبة الأولى، ثم بعد الحوكمة بالمرتبة الثانية، ومن ثم بعد الاستجابة ثالثا. وحل بعد الاكتشاف رابعا، واخيرا حل بعد الاستعادة والتقييم بالمرتبة الخامسة من حيث قوة ادراك توافره . اما من حيث اتساق اجابات افراد العينة،فقد حل بعدي الحوكمة والحماية بالمرتبة الاولى، يليهما بعد الاكتشاف بالمرتبة الثانية،ثم بعد الاستجابة بالمرتبة الرابعة، واخيرا بعد الاستعادة والتقييم.

ثانيا: – المتغير المعتمد ثقة المودعين:

حيث ان الباحث اعتمد عينتين ، الاولى كانت من العاملين لدى المصارف عينة الدراسة وبعدد (67)، واستخدم اجاباتها لغرض قياس مدى تبني المصارف عينة الدراسة لالمرونة السبرانية، اما العينة الثانية فقد تكونت من عدد من المودعين الذين يتعاملون مع المصارف المذكورة، وبعدد (202) مودع. وتبين الفقرات التالية تحليلا وصفيا لاجاباتهم.

1- القدرة والكفاءة

الجدول (20) يتضمن الاوساط الحسابية الموزونة والانحرافات المعيارية ومستوى الإجابة وشدتها لكل سؤال من أسئلة بعد القدرة والكفاءة وبشكل اجمالي. حقق السؤال (5) أعلى وسط حسابي موزون بلغ (4.44) وبانحراف معياري (0.58) مما يدل على قوة ادراك المودعين ان استخدام النت يمكن ان يوفر لهم الخدمة المصرفية بسرعة واقل جهد،وحصل السؤال على مستوى إجابة مرتفع جدا، ونال السؤال المذكور شدة إجابة بلغت (88.71%).

أما السؤال (2) فقد حقق على أقل الأوساط الحسابية بمقدار (4.15) بانحراف معياري (0.69) وهو الأعلى من بين الأسئلة الأخرى مما يدل على ضعف انسجام الإجابات تجاه هذا السؤال قياسا بباقي الأسئلة الأخرى التي تشكل منها المتغير.وبلغت شدة الإجابة لهذا السؤال (82.97%). يتمتع هذا السؤال بمستوى إجابة مرتفع.

ان بعد القدرة والكفاءة حقق وسطاً حسابياً موزوناً عاما بلغ (4.23) وانحراف معياري (0.66) وبلغت شدة الاجابة (84.67%) وقد حصل هذا البعد على مستوى إجابة (مرتفع جدا). ان النتائج تدل على ان المودعين يثقون بكفاءة وقدرة النظام الالكتروني الخاص بالمصارف التي يتعاملون معها.

جدول (20) الإحصاء الوصفي لبعد القدرة والكفاءة (n=202)

ت	العبارة	الوسط الحسابي	شدة الإجابة %	الانحراف المعياري	مستوى الاجابة
1	يمتلك المصرف الكفاءات البشرية القادرة على التعامل الالكتروني.	4.24	84.75	0.66	مرتفع جدا
2	يتمتع المصرف بالقدرة على تلبية معظم الاحتياجات المصرفية الالكترونية للمودعين.	4.15	82.97	0.69	مرتفع
3	المصرف لديه الخبرات اللازمة لإجراء العمليات المصرفية عبر الانترنت كما هو متوقع.	4.17	83.47	0.65	مرتفع
4	يمكن اكمال معاملاتي المصرفية بسرعة عبر الانترنت.	4.17	83.47	0.68	مرتفع
5	استخدام موقع التعاملات المصرفيةيوفر لي الكثير من الجهد والوقت وسرعة الانجاز.	4.44	88.71	0.58	مرتفع جدا
	القدرة والكفاءة	4.23	84.67	0.66	مرتفع جدا

المصدر: إعداد الباحث

2- المنفعة:

الجدول (21) يتضمن الاوساط الحسابية الموزونة والانحرافات المعيارية ومستوى الإجابة وشدتها لكل سؤال من أسئلة بعد المنفعة وبشكل اجمالي. حقق السؤال (8) أعلى وسط حسابي موزون بلغ (4.24) وبانحراف معياري (0.63) مما يدل على قوة ادراك المودعين ان الحصول على المعلومات المطلوبة عن حساباتهم بسرعة وسهولة، وحصل السؤال على مستوى إجابة مرتفع جدا، ونال السؤال المذكور شدة إجابة بلغت (84.75%).أما السؤال (10) فقد حقق على أقل الأوساط الحسابية بمقدار (4.18) بانحراف معياري (0.70) وهو الأعلى من بين الأسئلة الأخرى مما يدل على ضعف انسجام الإجابات تجاه هذا السؤال قياسا بباقي الأسئلة الأخرى التي تشكل منها المتغير.وبلغت شدة الإجابة لهذا السؤال (83.66%). يتمتع هذا السؤال بمستوى إجابة مرتفع.

ان بعد المنفعة حقق وسطاً حسابياً موزوناً عاما بلغ (4.21) وانحراف معياري (0.66)،وبلغت شدة الاجابة (84.16%) وقد حصل هذا البعد على مستوى إجابة (مرتفع جدا). ان النتائج تدل على ان المودعين يحققون منافع من النظام الالكتروني الخاص بالمصارف التي يتعاملون معها.

جدول (21) الإحصاء الوصفي لبعد المنفعة (n=202)

ت	العبارة	الوسط الحسابي	شدة الإجابة %	الانحراف المعياري	مستوى الاجابة
6	توفر الشبكة الالكترونية للمصرف كافة المعلومات للمودعين بشكل امن.	4.22	84.46	0.67	مرتفع جدا
7	يحتفظ موقع التعاملات المصرفية الالكترونية بارشيف سري عن معلوماتي الشخصية وحركة عملياتي المصرفية.	4.20	83.96	0.68	مرتفع
8	بإمكاني الحصول على حركة حسابي المصرفي وتعاملاتي المصرفية بكل سهولة وللمدة التي يحتاجها.	4.24	84.75	0.63	مرتفع جدا
9	يناسب النظام المصرفي الالكتروني الطريقة التي ارغب باستخدامها للحصول على الخدمة المصرفية.	4.20	83.96	0.65	مرتفع
10	يوفر لي المصرف نظام الكتروني يتناسب مع حاجتي وتعاملاتي اليومية.	4.18	83.66	0.70	مرتفع
	المنفعة	4.21	84.16	0.66	مرتفع جدا

المصدر: إعداد الباحث

3- الأمان:

الجدول (21) يتضمن الاوساط الحسابية الموزونة والانحرافات المعيارية ومستوى الإجابة وشدتها لكل سؤال من أسئلة بعد الامان وبشكل اجمالي. حقق السؤال (11) أعلى وسط حسابي موزون بلغ (4.38) وبانحراف معياري (0.62) مما يدل على قوة ادراك المودعين ان تعاملاتهم المصرفية تحافظ على خصوصيتهم ،وحصل السؤال على مستوى إجابة مرتفع جدا، ونال السؤال المذكور شدة إجابة بلغت (87.52%).أما السؤال (14) فقد حقق على أقل الأوساط الحسابية بمقدار (4.11) بانحراف معياري (0.66) وهو الأعلى من بين الأسئلة الأخرى مما يدل على ضعف انسجام الإجابات تجاه هذا السؤال قياسا بباقي الأسئلة الأخرى التي تشكل منها المتغير.وبلغت شدة الإجابة لهذا السؤال (82.28%).يتمتع هذا السؤال بمستوى إجابة مرتفع.

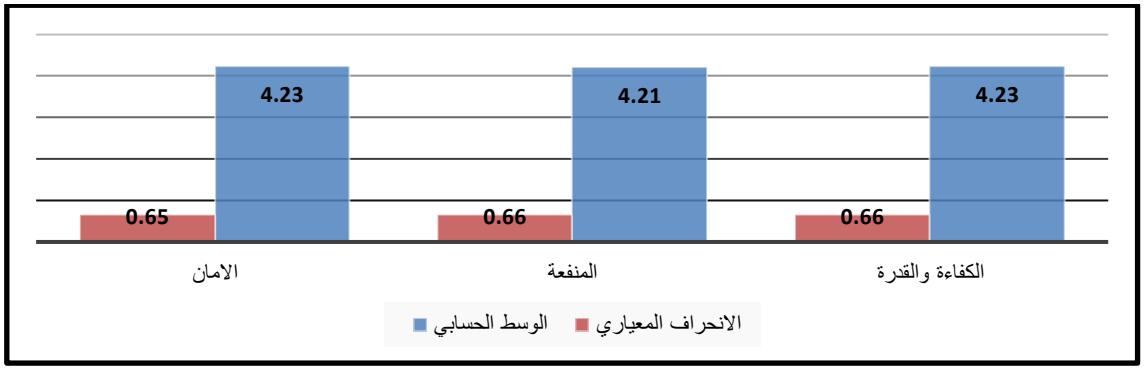
ان بعد الامان حقق وسطاً حسابياً موزوناً عاما بلغ (4.23) وانحراف معياري (0.65)، وبلغت شدة الاجابة (84.55%) وقد حصل هذا البعد على مستوى إجابة (مرتفع جدا). ان النتائج تدل على شعورهم بالامان عند تعاملهم مع المصارف التي يتعاملون معها حاليا.

جدول (22) الإحصاء الوصفي لبعد الامان (n=202)

ت	العبارة	الوسط الحسابي	شدة الإجابة %	الانحراف المعياري	مستوى الاجابة
11	استخدام التعاملات المصرفية الالكترونية يحافظ على الخصوصية.	4.38	87.52	0.62	مرتفع جدا
12	أشعر بالأمان في المصرف الذي اتعامل معه الكترونياً.	4.21	84.26	0.68	مرتفع جدا
13	استخدام خدمات المصرف الالكترونية يساعد في الحد من عمليات الاحتيال والسرقة.	4.21	84.26	0.64	مرتفع جدا
14	في كل مرة أستخدم التعاملات المصرفية الالكترونية احتاج الى تغيير كلمة المرور للحصول على الامان .	4.11	82.28	0.66	مرتفع
15	ان أماكن وجود انظمة الدفع الالكتروني آمنة او متاحة لجميع الزبائن في أي زمان ومكان.	4.22	84.46	0.61	مرتفع جدا
	الامان	4.23	84.55	0.65	مرتفع جدا
	ثقة المودعين	4.22	84.46	0.66	مرتفع جدا

المصدر: إعداد الباحث

ومما ينبغي الإشارة أليه هو أن متغير ثقة المودعين حقق وسطا حسابيا موزونا عاما (4.22)، بانحراف معياري (0.66)، وشدة إجابة بلغت (84.46%). وهذا يدل بشكل عام على تمتع المصارف عينة الدراسة بشكل عام بثقة المودعين . ويبين الشكل ادناه مقارنة بين ابعاد ثقة المودعين من حيث الأوساط الحسابية الموزنة والانحرافات المعيارية



المصدر: اعداد الباحث شكل (27) مقارنة بين ابعاد ثقة المودعين

تبين بشكل عام ان المودعين يشعرون بالامان في التعامل مع المصارف التي يتعاملون معها حاليا ويشعرون بالثقة بكفاءة وقدرة العاملين في المصارف التي يتعاملون معها ، وأخيرا فانهم يحققون منفعة من التعامل مع المصارف التي يتعاملون معها حاليا

"المبحث الرابع"

اختبار فرضيات الدراسة

توطئة

كون الباحث اختار عينتين ، تمثلت العينة الاولى بعدد من المصارف الحكومية، التي مثلها (67) موظفا يمثلون مديرون تلك المصارف ورؤساء الاقسام والشعب فيها، بهدف تكوين صورة واضحة عن المرونة السبرانية، كونهم الاقدر على تحديد مدى تبني المصارف لهذه الاستراتيجية. واختار عينة مكونة من (202) من المودعين الذين يتعاملون مع تلك المصارف بقصد قياس مدى ثقة هؤلاء المودعين باجراءات الحماية السبرانية التي توفرها تلك المصارف لهم من المرونة السبرانية . حولت عينة الدراسة من التجميع بين عدد استمارات الاستبيان الموزعة على العاملين في المصارف المبحوثة والاستمارات الموزعة على عينة من المودعين الذين يتعاملون مع تلك المصارف من برنامج (SPSS V.26) وبأستخدام الامر (Aggregation Data). استخدم الباحث استمارة لاختبار فرضيات علاقات الارتباط بين متغيرات الدراسة مصفوفة الارتباط (معاملات الارتباط البسيط "Pearson"). ولقد استخدمت مصفوفة معاملات الارتباط البسيط للتحقق من قوة واتجاه علاقات الارتباط الموجودة ما بين أبعاد متغيرات الدراسة فيما يخص اختبار فرضيات الارتباط.

اولا :- اختبار علاقات الارتباط بين متغيرات الدراسة:

الفرضية الرئيسة الأولى:

وتنص على أنه (لا توجد علاقة ارتباط ذات دلاله معنوية بين المرونة السبرانية وثقة المودعين). ولقد تفرع عنها خمسة فرضيات فرعية وكما مبين: -

1- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الحوكمة وثقة المودعين.
2- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الحماية وثقة المودعين.
3- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الاستكشاف وثقة المودعين.
4- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الاستجابة وثقة المودعين.
5- لا توجد علاقة ارتباط ذات دلالة معنوية بين بعد الاستعادة والتقييم وثقة المودعين

يظهر الجدول (22) مصفوفة علاقات الارتباط للفرضية الرئيسة الأولى وما تفرع عنها من فرضيات فرعية بأن جميع علاقات الارتباط كانت موجبة وذات دلالة معنوية عند مستوى (1%) بين المرونة السبرانية وثقة المودعين على المستوى الفرعي والاجمالي.فعلى المستوى الفرعي كانت اكبر علاقة ارتباط بين بعد الحماية وثقة المودعين اذ بلغت (0.65)، وهي علاقة معنوية عند مستوى (1%). أما اقل علاقة ارتباط فكانت بين الحوكمة وثقة المودعين اذ بلغت (0.33)، وهي علاقة معنوية عند مستوى (1%). وعلى

المستوى الكلي بلغت قيمة علاقة الارتباط بين المرونة السبرانية وثقة المودعين (0.68)، وهي علاقة معنوية عند مستوى(1%). وتدل النتائج انفة الذكر على قبول الفرضية الرئيسة الاولى وما تفرع عنها من فرضيات فرعية، بمعنى توجد علاقة ارتباط ذات دلالة معنوية بين المرونة السبرانية وثقة المودعين، بمعنى كلما عززت المصارف عينة الدراسة من استخدامها لالمرونة السبرانية ، كلما عزز ذلك من ثقة مودعيها وزبائنها في متانة وسلامة نظامها المصرفي.

جدول (23) اختبار الفرضية الرئيسة الاولى

معتمد / مستقل	ثقة المودعين
الحوكمة	**0.33
الحماية	**0.65
الاستكشاف	**0.57
الاستجابة	**0.40
الاستعادة والتقييم	**0.47
استراتيجية المرونة السبرانية	**0.68

المصدر: اعداد الباحث

ثانيا: – اختبار فرضيات التأثير بين متغيرات الدراسة:

بهدف اختبار علاقات التأثير بين متغيرات الدراسة استخدم الباحث انموذج الانحدار البسيط وعلى النحو الاتي:

الفرضية الرئيسة الثانية:

(لا تؤثر المرونة السبرانية بصورة معنوية في ثقة المودعين).

ولقد تفرعت عن الفرضية خمس فرضيات فرعية وهي:

1- لاتؤثر الحوكمة بصورة معنوية في ثقة المودعين
2- لاتؤثر الحماية بصورة معنوية في ثقة المودعين
3- لايؤثر الاستكشاف بصورة معنوية في ثقة المودعين.
4- لاتؤثر الاستجابة بصورة معنوية في ثقة المودعين
5- لاتؤثر الاستعادة والتقييم في ثقة المودعين

يبين الجدول(24) ادناه اختبار الفرضية الفرعية الاولى المنبثقة عن الرئيسة الثانية وكما يلي:

جدول(24) اختبار الفرضية الفرعية الاولى المنبثقة عن الفرضية الرئيسة الثانية

المتغير المعتمد / المتغير المستقل	ثقة المودعين		t	F	R^2
	α	β			
الحوكمة	1.78	0.32	**6.40	**40.96	0.11

المصدر: اعداد الباحث

**معنوي بمستوى 1%

يتبين من الجدول(24) الاتي:

1- ان بعد الحوكمة يؤثر بصورة ايجابية وبمقدار (0.32) في ثقة المودعين اذا ازداد بمقدار وحدة واحدة.علما ان هذا التاثير كان معنويا عند مستوى 1% لان قيمة t المحسوبة لمعامل الانحدار بلغت (6.40) وهي معنوية عند المستوى المذكور.

2- بلغت قيمة F المحسوبة والتي تقيس معنوية انموذج الانحدار المقدر (40.96) وهي قيمة معنوية عند مستوى (1%) ، مما يعني ثبوت معنوية انموذج الانحدار المقدر عند المستوى المذكور.

3- بلغت قيمة معامل التحديد(R^2) (0.11) ، بمعنى ان بعد الحوكمة تفسر ما نسبته (11%)من التغيرات التي تحصل في ثقة المودعين، اما النسبة المتبقية فتعود لعوامل اخرى غير داخلة في الانموذج. عليه يستدل الباحث على رفض الفرضية الفرعية الاولى بمعنى (تؤثر الحوكمة بصورة معنوية في ثقة المودعين). وستاخذ معادلة الانحدار المقدرة الشكل الاتي:

ثقة المودعين = 1.78 + 0.32 الحكومة

ويبين الجدول (25) اختبار الفرضية الفرعية الثانية المنبثقة عن الفرضية الرئيسة الثانية:

جدول(25) اختبار الفرضية الفرعية الثانية المنبثقة الفرضية الرئيسة الثانية

المتغير المعتمد / المتغير المستقل	ثقة المودعين		t	F	R^2
	α	β			
الحماية	2.98	0.87	**5.80	**33.64	0.42

المصدر: اعداد الباحث

**معنوي بمستوى 1%

يتبين من الجدول(25) الاتي:

1- ان بعد الحماية يؤثر بصورة ايجابية وبمقدار (0.87) في ثقة المودعين اذا ازداد بمقدار وحدة واحدة.علما ان هذا التاثير كان معنويا عند مستوى 1% لان قيمة t المحسوبة لمعامل الانحدار بلغت(5.80) وهي معنوية عند المستوى المذكور.

2- بلغت قيمة F المحسوبة والتي تقيس معنوية انموذج الانحدار المقدر (33.64) وهي قيمة معنوية عند مستوى (1%) ، مما يعني ثبوت معنوية انموذج الانحدار المقدر عند المستوى المذكور.

3- بلغت قيمة معامل التحديد(R^2) (0.42) ، بمعنى ان بعد الحماية يفسر ما نسبته (42%)من التغيرات التي تحصل في ثقة المودعين، اما النسبة المتبقية فتعود لعوامل اخرى غير داخلة في الانموذج. عليه يستدل الباحث على رفض الفرضية الفرعية الثانية بمعنى (تؤثر الحماية بصورة معنوية في ثقة المودعين). وستاخذ معادلة الانحدار المقدرة الشكل الاتي:

ثقة المودعين = 2.98 + 0.87 الحماية

ويبين الجدول (26) اختبار الفرضية الفرعية الثالثة المنبثقة عن الفرضية الرئيسة الثانية

جدول(26) اختبار الفرضية الفرعية الثالثة المنبثقة عن الفرضية الرئيسة الثانية

المتغير المعتمد / المتغير المستقل	ثقة المودعين		t	F	R^2
	α	β			
الاستكشاف	2.09	0.43	**7.17	**51.40	0.32

المصدر: اعداد الباحث

**معنوي بمستوى 1%

يتبين من الجدول اعلاه الاتي:

1- ان بعد الاستكشاف يؤثر بصورة ايجابية وبمقدار(0.43) في ثقة المودعين اذا ازداد بمقدار وحدة واحدة.علما ان هذا التاثير كان معنويا عند مستوى 1% لان قيمة t المحسوبة لمعامل الانحدار بلغت(7.17) وهي معنوية عند المستوى المذكور.

2- بلغت قيمة F المحسوبة والتي تقيس معنوية انموذج الانحدار المقدر (51.40) وهي قيمة معنوية عند مستوى (1%) ، مما يعني ثبوت معنوية انموذج الانحدار المقدر عند المستوى المذكور.

3- بلغت قيمة معامل التحديد(R^2) (0.32)، بمعنى ان بعد الاستكشاف يفسر ما نسبته (32%) من التغيرات التي تحصل في ثقة المودعين، اما النسبة المتبقية فتعود لعوامل اخرى غير داخلة في الانموذج. عليه يستدل

الباحث على رفض الفرضية الفرعية الثالثة بمعنى (يؤثر الاستكشاف بصورة معنوية في ثقة المودعين). وستاخذ معادلة الانحدار المقدرة الشكل الاتي:

ثقة المودعين = 2.09 + 0.43 الاستكشاف

ويبين الجدول (27) اختبار الفرضية الفرعية الرابعة المنبثقة عن الفرضية الرئيسة الثانية

جدول(27) اختبار الفرضية الفرعية الرابعة المنبثقة عن الفرضية الرئيسة الثانية

المتغير المعتمد / المتغير المستقل	ثقة المودعين		t	F	R^2
	α	β			
الاستجابة	1.44	0.66	**6.80	**46.24	0.16

المصدر: اعداد الباحث

**معنوي بمستوى 1%

يتبين من الجدول اعلاه الاتي:

1- ان بعد الاستجابة يؤثر بصورة ايجابية وبمقدار(0.66) في ثقة المودعين اذا ازداد بمقدار وحدة واحدة.علما ان هذا التاثير كان معنويا عند مستوى 1% لان قيمة t المحسوبة لمعامل الانحدار بلغت (6.80) وهي معنوية عند المستوى المذكور.

2- بلغت قيمة F المحسوبة والتي تقيس معنوية انموذج الانحدار المقدر (46.24) وهي قيمة معنوية عند مستوى (1%) ، مما يعني ثبوت معنوية انموذج الانحدار المقدر عند المستوى المذكور.

3- بلغت قيمة معامل التحديد(R^2) (0.16) ، بمعنى ان بعد الاستجابة يفسر ما نسبته (16%)من التغيرات التي تحصل في ثقة المودعين، اما النسبة المتبقية فتعود لعوامل اخرى غير داخلة في الانموذج. عليه يستدل الباحث على رفض الفرضية الفرعية الرابعة بمعنى (تؤثر الاستجابة بصورة معنوية في ثقة المودعين). وستاخذ معادلة الانحدار المقدرة الشكل الاتي:

ثقة المودعين = 1.44 + 0.66 الاستجابة

ويبين الجدول (28) اختبار الفرضية الفرعية الخامسة المنبثقة عن الفرضية الرئيسة الثانية

جدول(28) اختبار الفرضية الفرعية الخامسة المنبثقة عن الفرضية الرئيسة الثانية

المتغير المعتمد / المتغير المستقل	ثقة المودعين		t	F	R^2
	α	β			
الاستعادة والتقييم	2.78	0.86	**5.05	**25.50	0.22

المصدر: اعداد الباحث

**معنوي بمستوى 1%

يتبين من الجدول اعلاه الاتي:

1- ان بعد الاستعادة والتقييم يؤثر بصورة ايجابية وبمقدار(0.86) في ثقة المودعين اذا ازداد بمقدار وحدة واحدة.علما ان هذا التاثير كان معنويا عند مستوى 1% لان قيمة t المحسوبة لمعامل الانحدار بلغت (5.05) وهي معنوية عند المستوى المذكور.

2- بلغت قيمة F المحسوبة والتي تقيس معنوية انموذج الانحدار المقدر (25.50) وهي قيمة معنوية عند مستوى (1%) ، مما يعني ثبوت معنوية انموذج الانحدار المقدر عند المستوى المذكور.

3- بلغت قيمة معامل التحديد(R^2) (0.22) ، بمعنى ان بعد الاستعادة والتقييم يفسر ما نسبته (22%)من التغيرات التي تحصل في ثقة المودعين، اما النسبة المتبقية فتعود لعوامل اخرى غير داخلة في الانموذج. عليه يستدل الباحث على رفض الفرضية الفرعية الخامسة بمعنى (تؤثر الاستعادة والتقييم بصورة معنوية في ثقة المودعين). وستاخذ معادلة الانحدار المقدرة الشكل الاتي:

ثقة المودعين = 2.78 + 0.86 الاستعادة والتقييم

بعد ان اختبر الباحث الفرضيات الفرعية المنبثقة عن الفرضية الرئيسة الثانية ، قرر اختبار الفرضية الرئيسة الثانية وبشكل اجمالي وحسب الجدول (29) الاتي

جدول(29) اختبار الفرضية الفرعية الخامسة المنبثقة عن الفرضية الرئيسة الثانية

المتغير المعتمد / المتغير المستقل	ثقة المودعين		t	F	R^2
	α	β			
استراتيجية المرونة السبرانية	1.89	0.94	**9.40	**88.36	0.46

المصدر: اعداد الباحث

يتبين من الجدول اعلاه الاتي:

**معنوي بمستوى 1%

1- بشكل عام تؤثر المرونة السبرانية بصورة ايجابية وبمقدار(0.94) في ثقة المودعين اذا ازدادت بمقدار وحدة واحدة.علما ان هذا التاثير كان معنويا عند مستوى 1% لان قيمة t المحسوبة لمعامل الانحدار بلغت (9.40)وهي معنوية عند المستوى المذكور.

2- بلغت قيمة F المحسوبة والتي تقيس معنوية انموذج الانحدار المقدر (88.36) وهي قيمة معنوية عند مستوى (1%) ، مما يعني ثبوت معنوية انموذج الانحدار المقدر عند المستوى المذكور.

3- بلغت قيمة معامل التحديد(R^2) (0.22) ، بمعنى ان متغير المرونة السبرانية يفسر ما نسبته (46%)من التغيرات التي تحصل في ثقة المودعين، اما النسبة المتبقية فتعود لعوامل اخرى غير داخلة في الانموذج. عليه يستدل الباحث على رفض الفرضية الرئيسة الخامسة بمعنى (تؤثر المرونة السبرانية بصورة معنوية في ثقة المودعين). وستاخذ معادلة الانحدار المقدرة الشكل الاتي:

ثقة المودعين = 1.89 +0.94 المرونة السبرانية

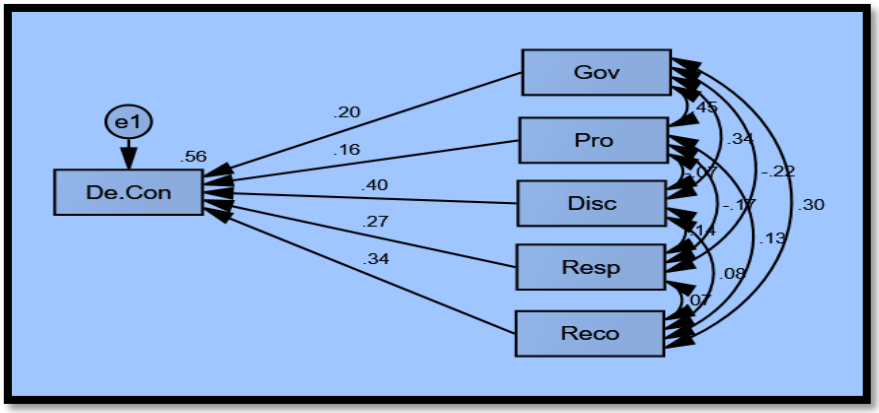
ويبين الجدول (30) ادناه مقارنة بين القوة التاثيرية للابعاد اعلاه منفردة في ثقة المودعين

ت	البعد	القوة التاثيرية	تسلسل القوة التاثيرية
1	الحوكمة	0.32	الخامس
2	الحماية	0.87	الاول
3	الاستكشاف	0.43	الرابع
4	الاستجابة	0.66	الثالث
5	الاستعادة والتقييم	0.86	الثاني

المصدر: اعداد الباحث

يتبين من الجدول اعلاه ان بعد الحماية هو اعلى الابعاد تاثيرا في تحقيق ثقة المودعين، وهذا شيء منطقي حيث ان المودع يتفاعل مع اي تطبيق تزيد من حماية امواله ومذخراته المودعة داخل المصرف، ثم بعد ذلك جاء بعد الاستعادة والتقييم، حيث يلاحظ اهتمام المودعين باستعادة معلوماتهم وتعاملاتهم بسرعة في حال تعرض المصرف الذي يتعاملون معه لخطر القرصنة. ثم جاء بعد الاستجابة بالمرتبة الثالثة وهو ما يعكس اهتمام المودعين بسرعة استجابة المصارف التي يتعاملون معها للمخاطر والتهديدات السبرانية . ثم جاء بعد الاستكشاف بالمرتبة الرابعة من حيث التاثير في ثقة المودعين ، واخيرا جاء بعد الحوكمة بالمرتبة الخامسة والاخيرة، وهذا شيء منطقي حيث ان الحوكمة اجراءات ادارية قد تكون غير منظورة للمودعين، رغم انها تنعكس بصورة نهاية في تحسين اجراءات المصرف لتعزيز ثقة المودعين.

بعد ان اجرى الباحث تحليل الفرضية الرئيسة الثانية باستخدام الانحدار الخطي البسيط ، قرر استخدام المعادلة الهيكلية (SEM) لاختبار الانحدار المتعدد لهذه الفرضية ، وكما في الشكل ادناه



شكل (28) اختبار الانحدار المتعدد للفرضية الرئيسة الثانية

ويبين الجدول ادناه تفصيلا لنتائج الاختبار اعلاه :

جدول(31) اختبار الانحدار الخطي المتعدد للفرضية الرئيسة الثانية

			Estimate	S.E.	C.R.	P
De.Con	<---	Gov	.20	.09	2.22	.006
De.Con	<---	Pro	.16	.05	3.2	.000
De.Con	<---	Disc	.40	.04	10	.000
De.Con	<---	Resp	.27	.07	3.85	.000
De.Con	<---	Reco	.34	.06	5.66	.000

المصدر: اعداد الباحث

يلاحظ من الشكل () والجدول (30) ان جميع ابعاد المرونة السبرانية تؤثر بشكل ايجابي ومعنوي عند مستوى (1%) في ثقة الزبون ، الامر الذي يعزز اهمية اعتماد هذه الاستراتيجية في القطاع المصرفي. ولقد بلغت قيمة معامل التحديد للنموذج R2 (0.65) وهذا يعني ان ابعاد المرونة السبرانية تفسر ما نسبته (65%) من التغيرات التي تطرأ في ثقة المودعين، والنسبة المتبقية تعود لعوامل اخرى غير داخلة في النموذج، الامر الذي يدعم رفض الفرضية الرئيسة ، بمعنى (تؤثر ابعاد استراتيجية المرونة السبرانية مجتمعة بصورة معنوية في تعزيز ثقة المودعين)

الفصل الرابع: الاستنتاجات والتوصيات

المبحث الاول:
الاستنتاجات

المبحث الثاني:
التوصيات

"المبحث الاول"

الاستنتاجات

1- أن مستوى تطبيق استراتيجية المرونة السيبرانية يختلف من مصرف لآخر، فبعض المصارف أكثر تقدما من غيرها في هذا المجال والبعض الاخر تسير في الاتجاه الصحيح فيما يتعلق بتطبيق استراتيجية المرونة السيبرانية، ومع استمرار الجهود المبذولة في هذا المجال من المتوقع أن تصبح التعاملات الإلكترونية في العراق أكثر أمانا وفعالية.

2- لا تزال هناك بعض التحديات التي تواجه المصارف التجارية في تطبيق استراتيجية المرونة السيبرانية ومنها نقص الموارد المادية وانخفاض الوعي لدى الجمهور ولا يزال هناك بعض الموظفين في المصارف غير مدركين لمخاطر الأمن السيبراني وكيفية التعامل معها، كما تعاني بعض المصارف من ضعف في بنيتها التحتية الرقمية، مما يجعلها أكثر عرضة للهجمات السيبرانية.

3- تعمل استراتيجية المرونة السيبرانية على تعزيز ثقة المودعين من عبر توفير السلامة والأمان للودائع، وهذا ما يؤدي إلى زيادة الودائع وتحسين سمعة المصارف، فضلاً عن الاستجابة للتهديدات الإلكترونية والتكيف معها وتحد من التعرض لمخاطر او هجمات سيبرانية مؤكدة تؤدي الى الحاق الضرر وتكبد المصارف خسائر مالية كبيرة.

4- تؤدي استراتيجية المرونة السيبرانية دوراً هاماً في تعزيز وعي الموظفين وتدريبهم على كيفية التعامل مع التهديدات السيبرانية، مما يزيد من قدرتهم على حماية البيانات ومدخرات المودعين وتطبيق إجراءات أمنية مشددة مثل تشفير البيانات واستخدام التوثيق الثنائي لضمان أمان البيانات الشخصية والمالية.

5- ان فعالية وكفاءة المرونة السيبرانية في المصارف التجارية ناجمة عن تحديث نظم الحماية السيبرانية بانتظام لمواجهة التهديدات الجديدة والمتطورة وضمان استمرارية التعاملات المصرفية الالكترونية بفعالية وتقليل التأثير على المودعين وتعزيز ثقتهم في العمليات المصرفية.

6- تقوم استراتيجية المرونة السيبرانية بتحديد وتقييم المخاطر السيبرانية التي تواجهها المصارف التجارية بما في ذلك التهديدات الداخلية والخارجية وتحتم على المصارف وضع خططاً محددة للتعامل مع الهجمات السيبرانية، بما في ذلك خطط استعادة والتقييم والحوكمة للبيانات وخطط استمرارية الأعمال في المصارف.

7- هناك عدد من معايير واطر استراتيجية المرونة السيبرانية التي تمكن المصارف من تحديد المخاطر السيبرانية التي تواجهها وتقييم هذه المخاطر ووضع خطط للتعامل مع هذه المخاطر وكذلك اختبار الخطط وتحسينها بمرور الوقت.

8- تساعد استراتيجية المرونة السيبرانية في تعزيز القدرة على الاستجابة السريعة لأي هجمات سيبرانية، مما يقلل من تأثيرها على الزبائن ويزيد من ثقتهم في المصارف، وبشكل عام يمكن القول إن استراتيجية المرونة السيبرانية تلعب دوراً حيوياً في تعزيز ثقة المودعين في القطاع المصرفي، من خلال تعزيز القدرة على التكيف، وتعزيز الوعي والتدريب، وتعزيز الثقة والشفافية، وتعزيز الاستجابة السريعة للتهديدات السيبرانية.

9- أن استراتيجية المرونة السيبرانية تلعب دوراً هاماً في بناء ثقة المودعين في المصارف الالكترونية فعندما تكون المصارف قادرة على التعامل بشكل فعال مع التهديدات السيبرانية وتتبنى استراتيجيات مرونة تمكنها من التكيف مع التغيرات في البيئة الرقمية، ويمكن أن يزيد ذلك من ثقة المودعين في قدرة المصرف على حماية بياناتهم وتأمين عملياتهم المالية عبر الإنترنت. ومن ثم يمكن القول بأن استراتيجية المرونة السيبرانية تسهم في بناء سمعة إيجابية للمصارف الالكترونية وزيادة الثقة لدى المودعين.

10- أ ن المصارف التجارية التي تظهر قدرة عالية على التعامل مع الهجمات السيبرانية وتحقيق استمرارية أعمالها تحظى بثقة أكبر من قبل المودعين.

11- تعمل الاستراتيجيات القوية للمرونة السيبرانية على تخفيف مخاوف المودعين بشأن فقدان أموالهم نتيجة للاختراقات السيبرانية.

12- يمكن أن تكون الاستراتيجية الفعالة للمرونة السيبرانية عاملاً جاذبًا للمودعين الجدد، خاصة أولئك الذين يبحثون عن مؤسسات مالية (مصارف) آمنة.

13- تساعد الاستراتيجية الفعالة للمرونة السيبرانية في تقليل التكاليف الناجمة عن الحوادث السيبرانية، مما يعود بالنفع على المصارف والمودعين على حد سواء.

"المبحث الثاني"

التوصيات

1- ضرورة وضع خطة لاستراتيجية المرونة السيبرانية تنفذ على مراحل تتضمن مشاريع عدة، والهدف منها الاستمرار بتطوير البنية التحتية للأمن السيبراني وحماية المدخرات والبيانات على وفق أحدث التقنيات والتكنولوجيا المتطورة والمعتمدة في التعامل مع الهجمات الإلكترونية.

2- ينبغي على المصارف إجراء تقييم شامل للمخاطر الإلكترونية لتحديد نقاط الضعف الحالية والمحتملة من خلال الاستفادة من خبرات العديد من الشركات الاستشارية العالمية الرصينة التي تنشط في مجال تقييم المخاطر الإلكترونية ووضع استراتيجيات المرونة السيبرانية.

3- توجيه المصارف بنشر المعرفة وتدريب موظفيهم وتوعية زبائنهم كافة عن طريق تعريفهم بالأنماط الخبيثة والأساليب الخاصة بالتهديدات الإلكترونية وهجمات الاحتيال وطرائق تجنبها وكشفها والإبلاغ عنها من خلال وسائل الاتصال الموثوقة والمنشورات ووسائل التوعية النصية أو المواقع الإلكترونية للمؤسسات الرسمية وإجراء تقييم شامل للمخاطر الإلكترونية لتحديد نقاط الضعف المحتملة.

4- تبني نهج استباقي لإدارة المخاطر السيبرانية وتشكيل فريق الاستجابة للحوادث السيبرانية في المصارف بهدف الامتثال للمفاهيم الأساسية لحكومة أمن المعلومات والصمود السيبراني وتطبيقا أمثل للمعايير القياسية الإدارة مخاطر الأمن المعلوماتي والحماية الرقمية والبنى التحتية التقنية وفقا لأفضل الممارسات.

5- وضع آليات تعاون مستمر بين البنك المركزي العراقي والمصارف التجارية العراقية لتقييم استراتيجية المرونة السيبرانية واستخدام تقنيات ومعايير واطر الأمان ومراقبة شبكاتها باستمرار للكشف عن أي نشاط مشبوه لحماية أنظمتها من الهجمات الإلكترونية.

6- ينبغي على المصارف إجراء اختبارات للاختراق الالكتروني منتظمة لتحديد نقاط الضعف في أنظمتها، فضلا عن ملئ استبانة خاصة بأمن البيانات السيبرانية والأنظمة والتطبيقات ومراكز البيانات لغرض تقييم وتدقيق الإجراءات لتحقيق الأهداف الاستراتيجية والتنظيمية في العمل المصرفي.

7- تعزيز المستوى المعرفي في مجال أمن المعلومات والبيانات وسريتها وتطبيق المعايير الخاصة بها مع بيان ضرورة التزامهم بالتعليمات الواجب اتباعها لتلافي الخروقات والتهديدات والوصول غير المصرح ومنع البرامج الخبيثة والفايروسات وحماية البيانات من التسريب أو السرقة أو الضياع والعمل على تحديد صلاحيات المستخدمين على وفق نطاق عملهم.

8- ينبغي على المصارف مراجعة استراتيجية المرونة السيبرانية بانتظام لتكييفها مع التهديدات الإلكترونية المتطورة ومواكبة التطورات التكنولوجية المصرفية الخاصة وتحديث التعاملات المصرفيةالمقدمة لتعزيز وزيادة ثقة المودعين ومحاولة جذب زبائن جدد من خلال توفير خدمات مصرفية تتناسب مع متطلبات وثقافة كل زبون.

9- الاستثمار في أبحاث وتطوير تقنيات الأمن السيبراني والمرونة السيبرانية الجديدة، وهذا يمكن المصارف التجارية من حماية أنفسها من الخسائر المالية والسمعة، وتعزيز ثقة المودعين، وبناء مستقبل أكثر استدامة وهذا يتوافق مع توجهات الحكومة العراقية في دعم هذا الجانب.

10- تطوير العمل المصرفي وزيادة حجم الودائع وتعزيز ثقة المودعين في الخدمات الالكترونية من خلال نشر أكبر عدد ممكن من اجهزة الصراف الالي والبطاقات الالكترونية فضلاً عن زيادة رقعة التوسع الجغرافي للمصارف على مستوى العراق والعالم الخارجي من خلال تطبيق استراتيجيات بالمرونة السيبرانية.

المصادر

- القران الكريم

اولاً – المصادر العربية:

الرسائل والاطاريح

1. ادريس عطية، مكانة الأمن السيبراني في الجزائر الوطنية الجزائرية، دراسة منشورة جامعة العربي التبسي، الجزائر، 2019.

2. إسماعيل زروقة، الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية السياسية ،جامعة محمد 25 بوضياف، الجزائر، 2019 .

3. إيمان محمد الشورة، السيبراني في البنوك الإسلامية الأردنية، مدير بكالوريوس، كلية الشريعة، الجامعة الأردنية، والسلطة الأمنية،الأردن، 2020.

4. بن صالح, مـــــاجدة، العوامل المؤثرة على ثقة العملاء في التعاملات المصرفية الالكترونية - دراسة حالة المصارف الجزائرية، الجزائر، 2021.

5. زينب شنوف، الحرب في العصر الرقمي: حروب ما بعد كلاوزفيتش، المدرسة الوطنية العلياء للعلوم السياسية، الجزائر، 2020.

6. سارة محمود عبد العزيز، دور الموبايل المصرفي في تعزيز مستوى ثقة العملاء في التعاملات المصرفية الالكترونية، جامعة حلوان،الجزائر، 2022.

7. سها معاد ،المرونة السيبرانية وفق بازل،مجلة اتحاد المصارف العربية ،المجلد (494ع) ،لبنان،2022.

8. شوابية بسمة وعرافة عفاف، أثر ثقة العملاء على تبني التعاملات المصرفية الإلكترونية في البنوك التجارية الجزائرية- دراسة حالة لوكالتي بنك الفلاحة والتنمية الريفية، الجزائر،2023.

9. شوابية بسمة، عرافة عفاف، أثر ثقة العملاء على تبني التعاملات المصرفية الالكترونية في المصارف التجارية الجزائرية،الجزائر، 2023.

10. صواق عبد القادر، بوداود بومدين. أولاد حيمودة عبد اللطيف. أثر جاهزية الأمن السيبراني على التعاملات المصرفية الالكترونية من خلال تقليل المخاطر المدركة دراسة حالة بنك Bdl بغرداية، جامعة غرداية، الجزائر، 2023.

11. عبد الله الجعفري، التهديدات وتأثيرها على الامن القومي الجزائري، جامعة احمد دراية، الجزائر 2022.

12.محمدي سناء، دور جودة الخدمة المصرفية في زيادة ثقة العملاء في البنوك التجارية، جامعة قاصدي مرباح - ورقلة، الجزائر، 2023.

التقاريروالنشرات:

1- البنك المركزي العراقي، دائرة تقنية المعلومات والمدفوعات، 2022.

2- البنك المركزي، تقرير الاستقرار المالي، 2022.

3- المصدر: البنك المركزي العراقي، دائرة الاحصاء والابحاث، النشرة الاحصائية، 2022

4- مصرف الاهلي العراقي، التقرير السنوي لمجلس الادارة والحسابات الختامية للسنة المالية المنتهية 2022.

5- مصرف الخليج التجاري، التقرير السنوي لمجلس الادارة والحسابات الختامية للسنة المالية المنتهية 2022.

6- مصرف الشرق الاوسط للاستثمار، التقرير السنوي لمجلس الادارة والحسابات الختامية للسنة المالية المنتهية 2022.

7- مصرف المنصور للاستثمار، التقرير السنوي لمجلس الادارة والحسابات الختامية للسنة المالية المنتهية 2022.

8- مصرف الموصل للتمنية والاستثمار، التقرير السنوي لمجلس الادارة والحسابات الختامية للسنة المالية المنتهية 2022.

9- مصرف بغداد التجاري، التقرير السنوي لمجلس الادارة والحسابات الختامية للسنة المالية المنتهية 2021.

ثانياً – المصادر الاجنبية_

A- BOOK

1- AccentureThe Nature Of Effective Defense: Shifting from Cybersecurity to Cyber Resilience,2018.

2- Adekiya & Gawuna, M. S. Bank choice determinant factors: A study of university students in metropolitan Kano. International Journal of Management Sciences،2015.

3- Buryachok, V. Technological and anthropogenic impact on security of some countries,2016.

4- Dunn-Cavelty, M A Resilient Europe for an Open, Safe and Secure Cyberspace. Occasional Papers, No.23, The Swedish Institute of International Affairs,2013.

5- Oxford Brookes University, Vikas Kumar Birmingham City University. Cyber resilience for digital enterprises: A strategic leadership Perspective, 2020.

6- Ploch, D. The Information System and the Global Terrorism,2010.

7- Ross, R., Pillitteri, V., Riddle, M., & Guissanie, G Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. National Institute Of Standards and Technology (NIST), 2. U.S Department of Commerce,2020.

Messages and theses

1- AHawamleh, A. S. M. Alorfi, J. A. Al-Gasawneh, and G. Al- Rawashdeh, "Cyber security and ethical hacking: The importance of protecting user data," Solid State Technology, 2020.

2- Ajzen, I.The theory of planned behavior: Frequently asked questions. Human Behavior and Emerging Technologies,2020.

3- Allred, A. T., & Lon Addams, H. Service quality at banks and credit unions: what do their customers say? Managing Service Quality: An International Journal, 2000.

4- Aslan, S. S. Aktugˇ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions, 2023.

5- Axelsen, I Bongiovanni, and D. Stockdale,"A pathway model to five lines of accountability in cybersecurity gov- ernance , 2023.

6- Bank Director. Building Trust with Customers Starts Inside the Bank. Available at: https://www.bankdirector.com/article/building-trust-customers-starts-inside-bank, 2018.

7- Bank Payment, Nepal Rastra Bank Payment Systems Management, Nepal Rastra Bank Cyber Resilience Guidelines, 2023.

8- Bhattacherjee, A Individual trust in online firms: Scale development and initial test. Journal of management information systems, 2002.

9- Bhattacherjee, Individual trust in online firm: Scale development and initial test. Journal of Management Information System, 2002.

10- Bidgoli, H. Building Cyber Resilient Systems: A Comprehensive Guide to Developing Resilient Capabilities for Cyber Threats, 2019.

11- Bounaamane, D.Faculté des Sciences Juridiques, Économiques et Sociales de Fès Université Sidi Mohamed Ben Abdellah de Fès, MarocCybercrime and Cyber Resilience: The Challenges of Digital Security in a Connected World,2023.

12- Bounaman & Al-Darisi, Faculté des Sciences Juridiques, Économiques et Sociales de Fès Université Sidi Mohamed Ben Abdellah de Fès, MarocCybercrime and Cyber Resilience: The Challenges of Digital Security in a Connected World, 2023.

13- Bruner, G. C., & Pomazal, R. J. Problem recognition: the crucial first stage of the consumer decision process. Journal of Services,1988 .

14- Centeno, C. Building security and consumer trust in internet payments. Seville: Institute for Prospective Technological Studies, 2002.

15- Chimote, N. K. Maintaining the Quality of Work-Life Among the Employees of Private Banks.International Journal of Economic Research, 2019.

16- Davis, A. The Cyber Resilient Enterprise : Protecting Your Company from Cyber Threats in the Digital Age, 2021.

17- Deng Zhaohua International,Satisfaction Customer Understanding. Wei Kee Kwok& Lu Yaobin, , China in Messages Instant Mobile of Study Empirical An: Loyalty a, 2010.

18- Donalds and K.-M. Osei-Bryson, "Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents," International Journal of Information Manage- ment, 2020.

19- Dr. Isabella Lee Cyber Resilience Frameworks: Exploring cyber resilience frameworks and strategies for organizations to recover from cyber attacks and maintain operational continuity,2024.

20- Drugă The Effect of Trust in Banking Institutions on Behavioural Intentions for E- Services, Ovidius University of Constanta, Romania, ,2024.

21- ed behavior, 2017.

22- Eurostat. E-banking and e-commerce. Internet use: Internet banking. Available at: https://ec.europa.eu/ eurostat/databrowser/explore/all/all_themes, 2024.

23- Fedir and Korobeynik,ovInstitute for Modelling in Energy, Engineering, Ukraine. UDC 004.056.5 Defining of Goals in the Development, of Cyber Resilient Systems According ,to NIST Ukraine,2023.

24- Ferreira & Dickason-Koekemoer, Z. Analysing the influence of demographics on depositor behaviour. International Journal of Applied Decision Sciences, 2020.

25- Fishbein, M., & Ajzen, I Belief, attitude, intention and behavior reading, MA. Addison- Wesley. Ford, RC & Richardson, WD. Ethical decision making: A review of the empirical literature. Journal of Business Ethics,1975.

26- Forbes. Increase In Digital Banking Raises Consumer Data Privacy Concerns: How To Protect Yourself. Available at: concerns, 2021.

27- G.A. Hubbard, "State-level Cyber Resilience: A Conceptua Framework,"ACIG, vol. 2, no. 1, 2023.

28- Gallemard, J. Customer Service: 4 Tips to Improve Your After-Sales Service. Available ،2022.

29- Ghamry & Shamma, H. M. Factors influencing customer switching behavior in Islamic banks: evidence from Kuwait. Journal of Islamic marketing, 2022.

30- Gill, A.S.; Flaschner, A. B.; Shachar, M. Factors that Affect the Trust of Business Clients in their Banks. International Journal of Bank Marketing, 2006.

31- Grøtan, T.O., Antonsen, S., Haavik, T.K. Cyber resilience: a preunderstanding for an abductive research agenda. In: Matos, F., Selig, P.M., Enriqson, E. (Eds.), Resilience in a Digital Age, 2022.

32- Grundke, P., & Kühn, A. The impact of the Basel III liquidity rat on banks: Evidence from a simulation study. The Quarterly Review ofEconomics and Finance, ،2020.

33- H. M. Melaku, "A dynamic and adaptive cybersecurity governance framework," Journal of Cybersecurity and Privacy, P:8 ,2023.

34- H. Naseer, K. Desouza, S. B. Maynard, and A. Ahmad, "Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics, 2023.

35- Hamid, S., & Bano, N. Behavioral Intention of Traveling in the period of COVID-19: An application of the Theory of Planned Behavior (TPB) and Perceived Risk. International Journal of Tourism Cities, 2021.

36- Hernandez-Ortega, B. "The role of post-use trust in the acceptance of a technology: Drivers and consequences", Tec novation, 2011.

37- Hisham Al-Saghi, Marilyn Ford, Anne Nguyen, Renee Hexel, Conceptualizing Citizen's Trust in E-Government Application of Q Methodology, Journal of e_government, P298, 2009.

38- Hoffman, D. L., Novak, T. P., & Peralta, M. Building consumer trust online, 1999.

39- Hollebeek, L.D. and Macky, K, Digital Content Marketing's Role in Fostering Consumer Engagement, Trust, and Value: Framework, Fundamental Propositions, and Implications. Journal of Interactive Marketing,2019.

40- Hurley, R., Gong, X. & Waqar, A Understanding the loss of trust in large banks. International Journal of Bank MarketingK ,2014.

41- Ighomereho, S., & S. Sajuyigbe, A. Mediating role of perceived service quality between behavioral characteristics, security risk and internet banking usage Banks and Bank Systems,2022.

42- International Organization for Standardization, "ISO 22316:2017 Security and resilience - Organizational resilience - Principles and attributes ،2017.

43- J. Al-Gasawneh, A. AL-Hawamleh, A. Alorfi, and G. Al-Rawashde, "Moderating the role of the perceived security and endorsement on the relationship between per- ceived risk and intention to use the artificial intelligence in financial services , 2022.

44- J. Smither and C. Braun, Technology and older adults: Factors affecting the adoption of , automatic teller machines. The Journal of General Psychology, 1994.

45- Jaradatet, A. AL-Hawamleh, M. Altarawneh, H. Hikal, and A. Elfedawy, "The interplay between intellectual capital, business intelligence adoption, and the decision to innovate: Evidence from jordan," International Journal of Computing and Digital Systems, 2024.

46- Jurevičienė, Viktorija SkvarcianySatisfaction of Small and Medium-sized Companies with the Policy of Mykolas Romeris University, Faculty of Economics and Finance ManagementAteities str. 20, LT-80303, Vilnius, LithuaniaE-daiva.jureviciene@mruni.eu,2013.

47- Karim Foluhonso, Sani Ayantungi, Gbadamuzi Rola Abdulrazaq A Study of the Impact of Trust on Customer Relationship Management in Banks: Evidence from Nigeria University of East London, UK, 2021

48- Kaur, B., Kiran, S., Grima, S., & Rupeika-Apoga, R. Digital banking in Northern India: The risks on customer satisfaction. Risks ,2021.

49- Kibrom Berhe Advisor, Yibeltal Nigussie. Mary Graduate School: Challenges and Opportunities of Electronic Banking in the Ethiopian Banking Industry: The Case of the Central Bank in the Silk Region By, 2022.

Scientific articles

1- Al Omari, N. Mai, H. . Hin, and A. Al Hawamleh, "Enhancing learning process by applying cooperative learning supported with augmented reality environment," International Journal, 2023.

2- Kibrom Berhes, St. Mary's University Graduate School, Studies on the Challenges and Opportunities of E-Banking in the Ethiopian Banking Industry: The Case of the Silk Road Zone at the Central Bank of Ethiopia, NEFA, 2022.

3- Kolsaker, A. & Payne, C. Engendering trust in e-commerce: a study of gender-based concern. Journal Marketing Intelligence & Planning, 2003.

4- Kott, A., Ludwig, J., & Lange, M. Assessing mission impact of cyberattacks: Toward a model-driven paradigm. IEEE Security and Privacy, 2017.

5- Kumar, M., Sareen, M., & Barquissau, E.Relationship between types of trust and level, of adoption of Internet banking. Problems and Perspectives in Management,2012.

6- Ladoke Akintola University of Technology, Strategic Advancements in Cyber Resilience: Harnessing the Power of Cloud Security Solutions, 2024.

7- Lekic, S., Fapa-Tankosic, J., Mandic, S., Rajakovic-Mijalovic, J., Analysis of the Quality of Employee-Bank Relationship in Urban and Rural Areas. Sustainability, 2020.

8- Lillemose, J. The (Re)invention Cyberspace. Kunstkritikk. Available at,2015.

9- Linkov, I., & Kott, A. Fundamental Concepts of Cyber Resilience: Introduction and Overview. In Cyber resilience of systems and Networks. essay, Springer International Publishing,2021.

10- Liu, C.T., Y.M. Gu, and C.H. Lee, The Effects of Relationship Quality and Switching Barriers on Customer Loyalty. International Journal of Information Management, 2011.

11- Lova Rajabelina, D. Origins and consequences of trust. In Management, Université du Québec à Montréal, 2011.

12- Lova Rajablina , les antécédent et les conséquences de la confiance en linge , le cas du secteur financier , these de doctorat an athministration des affaires , souterrue en mivembre , université de quebacaMan –tréal, 2011.

13- M. F. Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," Sustainability, P:11, 2023.

14- M. Hawamleh and A. Ngah, "An adoption model of mobile knowledge sharing based on the theory of planned behavior," Jour- nal of Telecommunication, Electronic and Computer Engineering (JTEC, 2017.

15- M. Hawamleh and A. Ngah, "An adoption model of mobile knowledge sharing based on the theory of plan

16- M. Melaku, "A dynamic and adaptive cybersecurity governance framework," Journal of Cybersecurity and Privacy, 2023.

17- Manohar, S., Mittal, A., & Marwah, Service innovation, corporate reputation and word-of-mouth in the banking sector: A test on multigroup-moderated mediation effect. Benchmarking: An International Journa ,2019.

18- Mayer, R., Davis, J. and Shoorman, F "An integrative model of organizational trust", The Academy of Management Review, 1995.

19- Mcquiggan, J. The Cyber Resilience Handbook: Creating a Secure and Confident Business, 2020.

20- Meriva, University Graduate School, Challenges and Opportunities of E-Banking in the Ethiopian Banking Industry: The Case of the Silk Road Zone at the Central Bank of Ethiopia, by Kibrom Berhe, Advisor: Yibeltal Neguse 2022.

21- Mitik, M., Korkmaz, O., Karagoz, P., Toroslu, I. H., & Yucel, F Data mining approach for direct marketing of banking products with profit/cost analysis. The Review of Socionetwork Strategies, 2017.

22- Mohammed Faez Hasan, Noor Salah Al-Ramadan. Department of Finance and Banking Sciences, Karbala University, Iraq. Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case2021.

23- Morag, Security and Resilience, Resilience: Interdisciplinary Perspectives on Science and Humanitarianism, Volume 2, Vienna,2014.

24- Munish Qamar, Mamta Sareen, EricBarkiso, The relationship between types of trust and the level of adoption of online banking, Problems and Perspectives in Management, 2012.

25- NIST Special Publication 800-160, Volume Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, NIST, 2021.

26- Pandey, N., & Patwardhan, A. Development of conceptual framework for internet banking customer satisfaction index. International Journal of Electronic Banking, 2020.

27- Patokorpi, E. & Kimppa, K. Dynamics of the key elements of consumer trust building online. Journal of Info. Comm. & Ethics in Society, 2006.

28- Pivetti, M., & Berti, C. Competence and Benevolence as Dimensions of Trust: Lecturers' Trustworthiness in the Words of Italian Students. Behavioral Sciences, 2020.

29- Raewf Thabit, Thabit H., and, Manaf B. Applications of Fuzzy Logic in Finance Studies, LAP- Lambert Academic Publisher, Germany2017.

30- Robertson, P & Rice, S.K. Cyber Resilience: Protecting Organizations in the Age of Cyber Threats, 2020.

31- S. Pandey, R. K. Singh, and A. Gunasekaran, "Supply chain risks in industry 4.0 environment: review and analysis framework," Pro- duction Planning & Control, 2023.

32- S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D A.Alabbad"Digitaltransformation and cybersecurity challenges for businesses resilience: Issues and recommendations," Sensors, 2023.

33- Safitra, M. Lubis, and H. Fakhrurroja, "Counterattacking cyber threats: A framework for the future of cybersecurity," Sustainability, 2023.

34- Serva John Benamati Mark A University ofDelaware,Trust and distrust in online banking: Their role in developing countries , 2007.

35- Shidrokh Goudarzi, Mohammad Nazir Ahmad, Seyed Ahmad Soleymani, Nastaran, MohammadhosseiniImpact of Trust on Internet Banking Adoption: A Literature Review,4Universiti Teknologi , Malaysia, 2013.

36- Smith J. B. et Barclay D. W. The effects of organizational differences and trust on the effectiveness of selling partner relationships, Journal of Marketing,1997.

37- Sophia and Sharifuddin Kayodestrategy 13 Advancements in Cyber Resilience: Harnessing the Power of Cloud Security Solutions,2024.

38- Stamp, M. Information security: principles and practice. John Wiley & Sons, 2011.

39- Sterbenz, J., Hutchison, D., Cetinkaya, E., Jabbar, A., Rohrer, J., Schöller, M. Smith, Resilience and survivability in communication networks: strategies, principles, and survey of disciplines, 2010.

40- Stevenson, J. Wolfers, Trust in Public Institutions Over the Business Cycle. American Economic Review, 2011.

41- Stojcˇic´, "Collaborative innovation in emerging innovation sys- tems: Evidence from central and eastern europe," The Journal of Technology Transfer, 2021.

42- Sujata, Suman Acharya, Joshi: Impact Of Cyber-Attacks On Banking Institutions In India: A Study Of Safety Mechanisms And Preventive Measures - Palarch's Journal Of Archaeology Of Egypt/Egyptology, 2020.

43- Thijeel, A. M., Flayyih, H. H., & Talab, H. R. The relationship between audit quality and accounting conservatism in the Iraqi banks. Opcion, 34Special Issue,2018.

44- Tsena, Ryan KL Kobang Serge Slapničara school of Business, University of Queensland, Brisbane, Australia's School of Information Technology and Electrical Engineering, University of Queensland, Brisbane, Australia, 2023.

45- Tzavara, V., Vassiliadis, S.: Industry resilience: before, now, after Covid-19, 2022.

46- Vuuren, T., Lombard, M., and Tonder, E. Customer Satisfaction, Trust and Commitment as Predictors of Customer Loyalty within an Optometric Practice Environment, Southern African Business Review, 2012.

47- Yannick Locle, "Trust-Free Banking Fails to Deliver – The Impact of Banking Mistrust on DeFi Adoption", University of Bayreuth, Germany, 2021.

48- Yap, B., Ramayah, T., and Shahidan, W. Satisfaction and Trust on Customer Loyalty: A PLS Approach, Business Strategy Series, 2012.

49- Yost, J.R The origin and early history of the computer secu-rity software products industry,IEEE Ann Hist, ComputComput, 2015.

50- Z. Jaradat, A. Al-Hawamleh, M. O. Al Shbail, and A. Hamdan, "Does the adoption of blockchain technology add intangible benefits to the industrial sector,2023.

الملاحق

الملحق (1) اسماء المحكمين لاستمارة الاستبانة:

ت	اللقب العلمي	الاسم الثلاثي	الاختصاص	مكان العمل
1	استاذ	علي احمد فارس	ادارة مالية	جامعة كربلاء كلية الادارة والاقتصاد
2	استاذ	احمد كاظم بريس	ادارة استراتيجية	جامعة كربلاء كلية الادارة والاقتصاد
3	استاذ	عادل عباس الجنابي	ادارة استراتيجية وسلوك تنظيمي	جامعة كربلاء كلية الادارة والاقتصاد
4	استاذ مساعد	جنان مهدي شهيد	استراتيجية	جامعة كربلاء كلية الادارة والاقتصاد
5	استاذ مساعد	امير علي خليل	مصارف	جامعة كربلاء كلية الادارة والاقتصاد
6	استاذ مساعد	حامد محسن جداح	مصارف	جامعة كربلاء كلية الادارة والاقتصاد
7	استاذ مساعد	محمد فائز حسن	أدارة مالية	جامعة كربلاء كلية الادارة والاقتصاد
8	استاذ مساعد	حيدر عباس الجنابي	اسواق مالية	جامعة كربلاء كلية الادارة والاقتصاد
9	استاذ مساعد	علي حسين عليوي	ادارة استراتيجية وسلوك تنظيمي	جامعة كربلاء كلية الادارة والاقتصاد

University of Karbala
College of Administration and Economics
Department of Banking and Financial Sciences
Graduate Studies

جامعة كربلاء
كلية الإدارة والاقتصاد
قسم العلوم المالية والمصرفية
الدراسات العليا

م/ استبانة رسالة ماجستير

حضرة السيد / الســـــيدة المحترم:

السلام عليكم ورحمة ..... وبركاته :

نضـــع بـــين ايـــديكم اســـتمارة الاســـتبانة الخاصـــة بدراســـة متغيـــرات رســـالة الماجســـتير الموســـومة **(استراتيجية المرونـة السـيبرانية ودورهـا فـي تعزيـز ثقـة المـودعين)** وهـي جـزء مـن متطلبـات نيـل درجـة الماجستير في العلوم المالية والمصرفية.

نامل تعاونكم معنا في قراءة فقراتها والاجابة عنها، اذ يعتمد نجاح هذه الدراسة على درجة استجابتكم بدقة وموضوعية، وأن تفضلكم بالإجابة المناسبة والصحيحة يسهم في دقة وسلامة النتائج التي يتم التوصل اليها من أجل خدمة المسيرة العلمية، كما ونرجو ملاحظة النقاط المهمة الاتية:

1- أن الاجابات سوف تستخدم لأغراض البحث العلمي فقط لذلك نرجو عدم كتابة الاسم أو التوقيع على الاستمارة.
2- الرجاء وضع علامة (✔) امام الفقرة التي تعكس الواقع الفعلي للمصرف.
3- الرجاء الاجابة على جميع فقرات الاستبانة، لان ترك فقرة واحدة بدون اجابة يؤدي الى اهمال الاستمارة بالكامل.
4- الرجاء ان تكون الاجابة وفقا لما هو موجود فعلا في المصرف وليس لما ترونه مناسبا.

شاكرين جهودكم وحسن تعاونكم مع جزيل الشكر والامتنان...

الباحث
عمار عبد الحسين شعلان
جامعة كربلاء – كلية الادارة والاقتصاد
قسم العلوم المالية والمصرفية

المشرف
الاستاذ الدكتور
كرار عباس متعب
جامعة كربلاء – كلية الادارة والاقتصاد
قسم العلوم المالية والمصرفية

المشرف
الاستاذ الدكتور
كمال كاظم جواد
جامعة كربلاء – كلية الادارة والاقتصاد
قسم العلوم المالية والمصرفية

1445 **2024**

المحور الاول: معلومات عامة

ملاحظة – يرجى وضع اشارة (✔) في المربع الذي تراه مناسباً ولكل فقرة من الفقرات الاتية:

أ- الجنس: ☐ ذكر ☐ انثى

ب- العمر: ☐ 30 فأقل ☐ 31- 40 ☐ 41- 50 ☐ 51- 60 ☐ 61- فأكثر

ت- التحصيل الدراسي: ☐ اعدادية ☐ دبلوم ☐ بكالوريوس ☐ ماجستير ☐ دكتوراه

ث- سنوات الخدمة: ☐ 5 فاقل ☐ 6- 10 ☐ 11- 15 ☐ 21- 25 ☐ 26 فاكثر

المحور الثاني: الاسئلة المتعلقة بالمتغير المستقل (استراتيجية المرونةالسيبرانية)

اولاً- استراتيجية المرونة السيبرانية: هي القدرة على التوقع والمقاومة والتعافي والتكيف مع المخاطر الالكترونية التي يتعرض لها المصرف ومواصلة العمليات المصرفية وتحقيق الاهداف بغض النظر عن الحوادث السيبرانية. وتشتمل المرونة السيبرانية خمسة ابعاد فرعية وهي (الحكومة - الحماية - الكشف - الاستجابة - الاستعادة والتقييم).

أ- الحوكمة : تشمل الحوكمة عملية التطوير الشاملة للمرونة السيبرانية من خلال السياسات والعمليات الخاصة بالمصرف على وجه الخصوص، ويعد هذا البعد ضروري لدمج المرونة السيبرانية في المصرف من خلال النظر في الأهداف الاستراتيجية والمخاطر الحالية والممارسات الإدارية.

ت	الفقرات	1 اتفق تماما	2 اتفق	3 محايد	4 لا اتفق	5 لا اتفق تماما
1	يعتمد المصرف استراتيجية للمرونة السيبرانية ويتم تطويرها والاعتماد عليها ضمن عمله.					
2	يتم اخذ المعايير الدولية الحديثة (ISO 22316)بعين الاعتبار عند تطبيق استراتيجيات العمل المصرفي.					
3	يقوم المصرف بمراجعة استراتيجية المرونة السيبرانية كلما حدث تغيير في تكنولوجيا المعلومات في المصرف.					
4	تتضمن استراتيجية المرونة السيبرانية عمليات اشعار الجهات المختصة بالمصرف عن أي حالة اختراق لبيانات المودعين والعملاء.					
5	تتضمن استراتيجية المرونة السيبرانية إجراءات واضحة (مثل بروتوكولات الاتصال وعمليات اتخاذ القرار) لاتخاذ القرارات في الوقت المناسب في حالة وقوع هجوم سيبراني.					

ب- الحماية: يجب أن تعمل الضوابط الأمنية الفعالة على حماية سرية وسلامة الأصول وخدماتها، كما يجب حماية البيانات أثناء النقل, فضلا عن توازن تدابير الحماية وحجم التهديدات، والحفاظ على سلامة الانظمة الرقمية وبناء حاجز ضد التهديدات السيبرانية المتزايدة من خلال انظمة الابلاغ المبكر في النظام المصرفي.

ت	الفقرات	1 اتفق تماما	2 اتفق	3 محايد	4 لا اتفق	5 لا اتفق تماما
6	يـتم اتخـاذ التـدابير الأمنيـة لحمايـة البـرامج والشـبكات والأجهزة في المصرف من الحوادث السيبرانية.					
7	يتم فحص التقنيات القديمة بانتظام (بشكل دوري) لتحديد نقاط الضعف المحتملة والبحث عن فرص للترقية.					
8	هناك ضوابط تمنع الأجهزة غير الخاضعة للرقابة من الاتصال بشبكتها الداخلية (مثل الأجهزة الشخصية) ونقاط النهاية(مثل الوسائط القابلة للإزالة) من داخل المبنى وخارجه .					
9	تكون ملفات تعريف وصول مودعين المصرف محددة وموثقة ويمكنهم الوصول الى ملفات تعريفهم بشكل واضح وسهل وامن.					
10	يتم تدريب جميع الموظفين (بشكل دوري) لدعم الامتثال لسياسة أمن المعلومات والإبلاغ عن الحوادث					

ج-الاكتشاف: تتطلب المرونة السيبرانية العالية قدرة المصرف على اكتشاف حالات الاختراق والهجمات السيبرانية (محاولة التسلل، حركة المهاجم عبر الأنظمة، استغلال نقاط الضعف) للوصول غير القانوني أو غير المصرح به إلى البيانات وإساءة استخدامها والأحداث التي تشير إلى حادث سيبراني محتمل, كما يسمح هذا الإنذار المبكر للمصارف بتبني إجراءات مضادة ضد أي حادث محتمل والاحتواء الاستباقي للانتهاكات الفعلية.

ت	الفقرات	1 اتفق تماما	2 اتفق	3 محايد	4 لا اتفق	5 لا اتفق تماما
11	توجد ضوابط كشف متعددة لدى المصرف لإمكانية الكشف المبكر عن الاختراقات التي يتعرض لها.					
12	هناك قدرات وبرامج كشف مستمدة من معلومات التهديد أو الضعف العامة وغير المعروفة بعد.					
13	هناك حدود تنبيه محددة لأنظمة المراقبة والكشف من أجل تحفيز وتسهيل عملية الاستجابة للحوادث السيبرانية.					
14	ان عمليات المصرف الحالية تراقب التعاملات السيبرانية التي لا تتماشى مع السياسة الأمنية.					
15	يوجد في المصرف برنامج استخباراتي للتهديدات السيبرانية يفحص بشكل دوري.					

د- الاستجابة : تعرف الاستجابة بأنها التدابير والسياسات التي تحدد إجراءات المصرف فيما يتعلق باكتشاف التناقضات أو الهجمات الإلكترونية, وتضمن الاستجابات بشكل رئيسي الإجراءات الفنية وغير الفنية، بما في ذلك نشر المعلومات إلى أصحاب المصلحة والرد على التهديدات في الوقت المناسب.

ت	الفقرات	1 اتفق تماما	2 اتفق	3 محايد	4 لا اتفق	5 لا اتفق تماما
16	توجد خطة للاستجابة للحوادث السيبرانية وفريق الاستجابة للحوادث المماثلة في المصرف.					
17	يتم تصميم أنظمة وعمليات الوظائف الحيوية في المصرف للحد من تأثير الحوادث السيبرانية.					
18	تسمح السياسات والعمليات والإجراءات في المصرف باحتواء الهجوم السيبراني قبل أن يؤدي إلى إتلاف الأنظمة الحيوية أو العمليات التجارية.					
19	يمكن أن تتخذ هذه الاستجابات أشكالًا مختلفة اعتمادًا على طبيعة الحوادث السيبرانية.					
20	تشتمل عملية المراجعة المستقلة على آليات للاستجابة لطلبات وكالات إنفاذ القانون والمودعين والشركاء والمشاركين في النظام ومقدمي الخدمات.					

هـ - الاستعادة والتقييم: يشير بعد الاستعادة والتقييم الى تلك اجراءات يستخدمها المصرف لتمكين استمراره والتشغيل بعد الحادث السيبراني، فضلاً عن إعادة تقييم مدى ملاءمة الاجراءات لطبيعة للتهديدات السيبرانية المتطورة للحفاظ على سلامة وكفاءة النظام المصرفي.

ت	العبارات	1 اتفق تماما	2 اتفق	3 محايد	4 لا اتفق	5 لا اتفق تماما
21	يضع المصرف خطط لاستعاد نظام العمل بعد تعرضه للهجمات السيبرانية.					
22	يمكن استعادة الأنظمة والعمليات والتعاملات المصرفيةفي المصرف من نسخ احتياطية موثوقة.					
23	تسمح السياسات والإجراءات والأنظمة في المصرف باستئناف العمليات خلال ساعتين منذ وقوع الحادث السيبراني.					
24	تسمح الأنظمة باسترداد البيانات بسرعة بعد اختراقها مما يضمن سلامة تلك البيانات.					
25	يكون المصرف قادر على تحديد الأنظمة والبيانات التي تم اختراقها بعد وقوع حادث سيبراني.					

University of Karbala
College of Administration and Economics
Department of Banking and Financial Sciences
Graduate Studies

جامعة كربلاء
كلية الإدارة والاقتصاد
قسم العلوم المالية والمصرفية
الدراسات العليا

م/ استبانة رسالة ماجستير

حضرة السيد / الســـــيدة المحترم:

السلام عليكم ورحمة ..... وبركاته :

نضـــع بـــين ايـــديكم اســـتمارة الاســـتبانة الخاصـــة بدراســـة متغيـــرات رســـالة الماجســـتير الموســـومة **(استراتيجية المرونـة السـيبرانية ودورهـا فـي تعزيـز ثقـة المـودعين)** وهـي جـزء مـن متطلبـات نيـل درجـة الماجستير في العلوم المالية والمصرفية.

نامل تعاونكم معنا في قراءة فقراتها والاجابة عنها، اذ يعتمد نجاح هذه الدراسة على درجة استجابتكم بدقة وموضوعية، وأن تفضلكم بالإجابة المناسبة والصحيحة يسهم في دقة وسلامة النتائج التي يتم التوصل اليها من أجل خدمة المسيرة العلمية، كما ونرجو ملاحظة النقاط المهمة الاتية:

1- أن الاجابات سوف تستخدم لأغراض البحث العلمي فقط لذلك نرجو عدم كتابة الاسم أو التوقيع على الاستمارة.
2- الرجاء وضع علامة (✔) امام الفقرة التي تعكس الواقع الفعلي للمصرف.
3- الرجاء الاجابة على جميع فقرات الاستبانة، لان ترك فقرة واحدة بدون اجابة يؤدي الى اهمال الاستمارة بالكامل.
4- الرجاء ان تكون الاجابة وفقا لما هو موجود فعلا في المصرف وليس لما ترونه مناسبا.

شاكرين جهودكم وحسن تعاونكم مع جزيل الشكر والامتنان...

الباحث
عمار عبد الحسين شعلان
جامعة كربلاء – كلية الادارة والاقتصاد
قسم العلوم المالية والمصرفية

المشرف
الاستاذ الدكتور
كرار عباس متعب
جامعة كربلاء – كلية الادارة والاقتصاد
قسم العلوم المالية والمصرفية

المشرف
الاستاذ الدكتور
كمال كاظم جواد
جامعة كربلاء – كلية الادارة والاقتصاد
قسم العلوم المالية والمصرفية

1445 **2024**

المحور الاول: معلومات عامة

ملاحظة – يرجى وضع اشارة (✔) في المربع الذي تراه مناسباً ولكل فقرة من الفقرات الاتية:

أ- الجنس: ☐ ذكر ☐ انثى

ب- العمر: ☐ 30 فأقل ☐ 31- 40 ☐ 41- 50 ☐ 51- 60 ☐ 61- فأكثر

ت- التحصيل الدراسي: ☐ اعدادية ☐ دبلوم ☐ بكالوريوس ☐ ماجستير ☐ دكتوراه

ث- سنوات الخدمة: ☐ 5 فاقل ☐ 6- 10 ☐ 11- 15 ☐ 21- 25 ☐ 26 فاكثر

المحور الثاني: الاسئلة المتعلقة بالمتغير التابع (ثقة المودعين)

ثقة المودعين: تعرف ثقة المودعين بأنها التوقعات والمعتقدات لدى المودعين حول تحقيق الخدمات التي وعدت بها المصارف, وفي هذا السياق توفر الثقة شعوراً بالراحة للمودعين والسماح لهم بمعرفة أن أموالهم محمية من قبل المصرف ويخلق شعوراً بالالتزام تجاه المصرف نظراً لوجود عمليات تحمي المودعين من الأخطاء الانتهازية أو سوء السلوك، وتشمل ثقة المودعين على ثلاثة ابعاد فرعية وهي (القدرة والكفاءة- المنفعة- الامان).

أ- الكفاءة والقدرة: وهي مجموعة من المهارات والكفاءات والخصائص التي تمكن طرف ما ان يكون له تأثير داخل مجال معين، فمجال القدرة يكون محدداً لان الموثوق به يمكن ان يكون لديه الكفاءة لدرجة عالية في بعض المجالات الفنية، وتشير القدرة لإدراك صاحب الثقة لكفاءات ومعارف الموثوق فيه البارزة في السلوك المتوقع وهذه المدركات ربما تكون معتمدة على الخبرات السابقة او الاصلية.

ت	الفقرات	1 اتفق تماما	2 اتفق	3 محايد	4 لا اتفق	5 لا اتفق تماما
1	يمتلك المصرف الكفاءات البشرية القادرة على التعامل الالكتروني.					
2	يتمتع المصرف بالقدرة على تلبية معظم الاحتياجات المصرفية الالكترونية للمودعين.					
3	المصرف لديه الخبرات اللازمة لإجراء العمليات المصرفية عبر الانترنت كما هو متوقع.					
4	يمكن اكمال معاملاتي المصرفية بسرعة عبر الانترنت.					
5	استخدام موقع التعاملات المصرفيةيوفر لي الكثير من الجهد والوقت وسرعة الانجاز.					

ب- المنفعة: وتعني مدى اعتقاد ان الموثوق به يريد فعل الخير لصاحب الثقة، بعيداً عن دافع الربح الشخصي، فهو يشير الى ان الموثوق به لديه بعض القيم المحددة المرتبطة بصاحب الثقة وفقاً لمعتقد النفع، ولذلك فان الموثوق به يكون محسناً لصاحب الثقة، حتى عندما يتطلب من الموثوق به ان يكون مساعد فالنفع يقدم ايمان وايثار في العلاقة ويقلل من عدم التأكد والميل للحذر من السلوك الانتهازي المضاد.

ت	الفقرات	1 اتفق تماما	2 اتفق	3 محايد	4 لا اتفق	5 لا اتفق تماما
6	توفر الشبكة الالكترونية للمصرف كافة المعلومات للمودعين بشكل امن.					
7	يحتفظ موقع التعاملات المصرفية الالكترونية بارشيف سري عن معلوماتي الشخصية وحركة عملياتي المصرفية.					
8	بإمكاني الحصول على حركة حسابي المصرفي وتعاملاتي المصرفية بكل سهولة وللمدة التي يحتاجها.					
9	يناسب النظام المصرفي الالكتروني الطريقة التي ارغب باستخدامها للحصول على الخدمة المصرفية.					
10	يوفر لي المصرف نظام الكتروني يتناسب مع حاجتي وتعاملاتي اليومية.					

ج - الامان: يشير الامان الى فهم صاحب الثقة بان المؤتمن سوف سيلتزم بمجوعة من المبادئ او قواعد التبادل المقبولة لدى صاحب الثقة اثناء التبادل وبعده، وان الامان المتصور يلهم الثقة في سلوك الشخص الجدير بالثقة ويقلل من ادراك المخاطر في التعاملات الالكترونية.

ت	الفقرات	1 اتفق تماما	2 اتفق	3 محايد	4 لا اتفق	5 لا اتفق تماما
11	استخدام التعاملات المصرفية الالكترونية يحافظ على الخصوصية.					
12	أشعر بالأمان في المصرف الذي اتعامل معه الكترونياً.					
13	استخدام خدمات المصرف الالكترونية يساعد في الحد من عمليات الاحتيال والسرقة.					
14	في كل مرة أستخدم التعاملات المصرفية الالكترونية احتاج الى تغيير كلمة المرور للحصول على الامان.					
15	ان أماكن تواجد انظمة الدفع الالكتروني آمنة او متاحة لجميع الزبائن في أي زمان ومكان.					

Abstract:

The study aimed to demonstrate the impact of the cyber resilience strategy with its sub-dimensions and its role in enhancing depositors' confidence in its dimensions, and the extent to which the banks in the study sample enjoy a cyber resilience strategy or not, and the extent to which this strategy is relevant to overcoming risks and threats and adapting to them to enhance depositors' confidence in the banking sector, especially electronic transactions.

This study was based on what the banking sector suffers from in terms of its distancing from its vital impact in stimulating economic activity using electronic technology in Iraq, in addition to its lack of response to internal or external financial and economic crises, which was clear in the past years. The problem of the study came to demonstrate the relationship between the cyber resilience strategy and depositors' confidence in banks, and from here it was necessary to focus on the extent to which these banks enjoy a cyber resilience strategy or not, and how commercial banks can benefit from these strategies to enhance depositors' confidence in light of the increasing cyber threats.

This study was analyzed by taking a sample of employees and depositors in six commercial banks. These banks were chosen for their great importance and because they provide a range of electronic transactions and dealings. They provide the appropriate environment to know and study the relationship between the implementation of the cyber resilience strategy and its role in enhancing depositors' confidence through electronic banking. The researcher concluded that the cyber resilience strategy works to enhance depositors' confidence by providing safety and security, responding to electronic threats and adapting to them, and reducing exposure to risks or cyber attacks through electronic transactions in the banking sector. The researcher concluded the study with a set of recommendations, the most important of which is to develop a plan for the cyber resilience strategy and implement it in stages, the aim of which is to continue developing the infrastructure for cyber security and protecting data at all levels according to the latest advanced technologies and technology adopted in electronic banking transactions.

Ministry of Higher Education and
Scientific Research
University of Karbala
Faculty of Administration and
Economics
Department of Banking and Financial
Sciences

Cyber resilience strategy and its role in enhancing depositors' confidence

An analytical study of a sample of employees and depositors in commercial banks listed on the Iraq Stock Exchange

A thesis submitted
to the Council of the College of Administration and Economics
- University of Karbala
as part of the requirements for obtaining a Master's degree
in Financial and Banking Sciences
by the student
Ammar Abdul Hussein Shaalan Al-Hasnawi

Supervised by
Prof . Kamal Kazem Jawad Al-Shammari
prof . Karrar Abbas Miteb Al Masoudi

1446 B.D
2024 A.D