AL KUT JOURNAL OF ECONOMIC AND ADMINISTRATIVE SCIENCES
Publisher: College of Economics and Management - Wasit University

اثر التحول الرقمي للمصارف التجارية العراقية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني

م.م شمران عبيد خليف الأمير

مديرية تربية واسط

(بحث مراجعة)

(Review article)

الملخص:

يهدف البحث عموماً إلى مراجعة نظرية حول التحول الرقمي المصرفي وأثر الإفصاح المحاسبي عن الأمن السيبراني ودور المصارف في الإفصاح عن الإجراءات المتعلقة بالأمن السيبراني من خلال التقارير المحاسبية والرقابية وتقارير الإدارة وهل هناك معايير تحدد النوعية والكمية التي تحتويها تلك التقارير المتعلقة بالأمن السيبراني، وهل أن نفعها أكبر من ضررها ولإعطاء إشارات إيجابية لأصحاب المصالح، أو أن هنالك أثراً سلبياً على الوحدة الاقتصادية ومدى كمية وقيمة المعلومات المفصح عنها، حاولت الدراسة الإحاطة بمفهوم التحول الرقمي في القطاع المصرفي وتبيان التجارب التكنولوجية المعاصرة حيث إنها عبارة عن تحد وفرصة في الوقت، نفسه يتمثل التحدي في قدرة القطاع المصرفي على التكيف مع المتطلبات المتمثلة بالتحول الرقمي للسوق، بالمقابل هذا التحول يعد فرصة للتنافس مع القطاع المصرفي في بيئة رقمية، ويُنظر إلى رقمنة المصارف على أنها التحدي الدائم الذي تواجهه الصناعة المصرفية حَالِيًّا ففي عملية التغيير الرقمي هذه يرتبط التحول الرقمي في الصناعة المالية بالعقبات التي يبدو أنها تعيق التنفيذ السلس لِلنَّهْجِ الرقمية ومن أبرز التحديات التي تواجه التحول الرقمي تحديات المحافظة على سرية المعلومة ومن يتعامل معها و مخاطر الافصاح المحاسبي عن مخاطر الأمن السيبراني ، لم تتناول الأدبيات المحاسبية الأكاديمية المحلية مَوْضُوعَة التحول الرقمي المصرفي وتأثير مخاطر الإفصاح المحاسبي عن الأمن السيبراني بشكل كاف على المستوى المحلي والعربي جاءت هذه الدراسة لتكن رائدة في هذا المجال. إن الغرض الرئيس من هذه الدراسة الاستكشافية النوعية هو طرح مفهوم التحول الرقمي المصرفي والإفصاح عن مخاطر إجراءات الأمن السيبراني والآثار المتوقعة من هذه العلاقة. وذلك بالاعتماد على المنهج الوصفي الوثائقي بسبب عدم وجود تطبيق عملي لهذه التقنية فاعتمدت الوثائق المتوفرة من بحوث ومؤلفات وإصدارات وتحليلها واستخلاص الاستنتاجات التي تجيب عن تساؤلات البحث. لقد اعتمد الباحث على التوجه العالمي في التحول المصرفي الرقمي في القطاع المصرفي وتحديات الأمن السيبراني في هذا القطاع الحيوي من خلال الاطلاع على البحوث العالمية في هذا المجال وتوجه الدولة العراقية فقد نشر مكتب مستشار الأمن القومي استراتيجية الأمن السيبراني العراقي(ICS) ، في عام 2017، وكانت هذه الخطوة بمنزلة أول جهد كبير وعام تبذله الدولة العراقية؛

من أجل تحليل مكامن الخلل في السياسة الإلكترونية الوطنية؛ ولرسم خارطة طريق لتأسيس بنية تحتية إلكترونية فوقية للبلاد لوضع العراق على قدم المساواة مع نظرائه الدوليين وحلفائه.

الكلمات الرئيسية: التحول الرقمي. الأمن السيبراني. الإفصاح .

Abstract

The research aims in general to review a theoretical review about banking digital transformation and the impact of accounting disclosure on cybersecurity and the role of banks in disclosing procedures related to cybersecurity through accounting and control reports and management reports. In order to give positive signals to stakeholders, or that there is a negative impact on the economic unit and the extent of the amount and value of the information disclosed, the study attempted to encompass the concept of digital transformation in the banking sector and to show contemporary technological experiences as it is a challenge and an opportunity at the same time. The challenge is the sector's ability On the other hand, this transformation is an opportunity to compete with the banking sector in a digital environment. The digitization of banks is seen as the permanent challenge facing the banking industry currently. In this process of digital change, digital transformation in the financial industry is linked to the obstacles that seem to hinder The smooth implementation of the digital approach is one of the main challenges facing Digital transformation: The challenges of maintaining the confidentiality of information and those who deal with it and the risks of accounting disclosure of cybersecurity risks. The local academic accounting literature did not adequately address the topic of banking digital transformation and the impact of accounting disclosure risks on cybersecurity at the local and Arab levels. This study came to be a pioneer in this field. The main purpose of this qualitative exploratory study is to introduce the concept of banking digital transformation and disclose the risks of cybersecurity procedures and the expected effects of this relationship. By relying on the documentary descriptive approach due to the lack of a practical application of this technique, it relied on the available documents of research, literature and publications, analysing them and drawing conclusions that answer the research questions. The researcher has relied on the global trend in digital banking transformation in the banking sector and cybersecurity challenges in this vital sector by reviewing global research in this field and the direction of the Iraqi state. The Office of the National Security Adviser published the Iraqi Cybersecurity Strategy (ICS), in 2017, This step was the first major and public effort by the Iraqi state; In order to analyse the kinks of the national electronic policy; To draw a

roadmap for the establishment of the country's superstructure electronic infrastructure to put Iraq on an equal footing with its international peers and allies

Keywords: digital transformation. Cybersecurity. disclosure.

- المقدمة:

يُعد القطاع المصرفي أحد أهم القطاعات الأساسية في الاقتصاد العراقي، ليس فقط لِدَوْرِهِ المهم في تنظيم وتمويل المشاريع ومختلف أنواع الائتمان للمشاريع الاستثمارية وغيرها والذي يمثل توجه النشاط الاقتصادي في العراق، في حالة تحول الرقمي سيواجه هذا القطاع تحديات كبيرة فمنها ما يندرج تحت بند التغير الاستراتيجي للعمل المصرفي ومنها ما ينصب على سلامة وأمن المعاملات الرقمية والإفصاح عنها. هنا يجب على المصارف توفير بنية تحتية تكنولوجية قوية ومرنة تضمن تقديم خدمات آمنة تتسم بالجودة والكفاءة. ستكون المصارف في وضع لا يسمح لها بإجراء تغييرات سريعة على البنية التحتية لتكنولوجيا المعلومات أو البنية التي تعلوها أن قرار المصارف بإضافة المزيد من الحلول الرقمية على جميع المستويات التشغيلية وسيكون له تأثير كبير على استقرارها المالي. في حين أن المصارف جميعها ليست في وضع يسمح لها بإجراء تغييرات سريعة على البنية التحتية لتكنولوجيا المعلومات أو البنية التي تعلوها، بالمقابل تأخذ مسألة الإفصاح وسلامة وأمن المعلومات الرقمية حيزاً كبيرا عند عملية التحول الرقمي للمصارف فالهجمات السيبرانية تشكل تهديدًا للأنظمة المرتبطة بالشبكة العالمية وخصوصاً في القطاع المصرفي، ثم إن هنالك مسألة الإفصاح عن إجراءات الأمن السيبراني وهل هنالك معايير تحدد ما يمكن الإفصاح عنه ومدى ملاءمة المعلومات التي يمكن أن تكون متاحة للأخريين، أن التقارير الصادرة في هذا الشأن على أن الفرص التي تخلقها تقنيات المعلومات والاتصالات تمثل للمؤسسات المصرفية، مع استمرارها في الابتكار تحدياً خاصاً في إيجاد وتقديم طرق جديدة للوصول إلى الزبائن، فإن تلك المؤسسات تتعرض في الوقت نفسه لمخاطر جديدة. حيث إن الاستخدام الضار لتقنية المعلومات والاتصالات يمكن أن يؤدي إلى تعطيل الخدمات المالية الضرورية للأنظمة المالية الوطنية والدولية، وتقويض الأمن والثقة، وتعريض الاستقرار المالي للخطر.

المبحث الأول : منهجية البحث ودراسات سابقة

اولاً : مشكلة البحث

تتمحور مشكلة البحث في الأثر الذي يخلفه التحول الرقمي في قطاع التجارية العراقية على الإفصاح المحاسبي والتحديات والصعوبات التي تتمثل بمخاطر الأمن السيبراني وكذلك الإجراءات التي ترافق عمل التحول لذلك يبدو أن التحول الرقمي المصرفي ليس فقط عملية تغير أسلوب خدمات إنما هنالك مخاطر يحتويها هذا الأسلوب بما فيها تحديات الأمن السيبراني وما يتطلب من عمليات إفصاح عن مخاطر إجراءاته. لذا يمكن صياغة المشكلة بما يلي:

هناك أثار وتحديات للتحول الرقمي فيما يخص الإفصاح المحاسبي عن مخاطر الأمن السيبراني في المصارف التجارية العراقية .

ثانياً: فرضيات الدراسة

الفرضية الأولى: هنالك أثر سلبي للإفصاح المحاسبي للمصارف التجارية العراقية في ظل التحول الرقمي

الفرضية الثانية: مستوى الإفصاح المحاسبي مرتبط بقدرة المصارف التجارية العراقية على مواجهة تهديدات الأمن السيبراني.

ثالثاً :أهمية البحث

تأتي أهمية البحث من كون التحول الرقمي في القطاع المصرفي بات ضرورة ملحة لا بد منها في ظل التحول العالمي من الخدمات التقليدية إلى تقديم خدمات رقمية تتسم بالسرعة والكفاءة، أن هذا التحول يواجه بعقبات وتحديات أهمها الإفصاح المحاسبي في ظل بيئة رقمية تختلف كلياً عن تلك البيئة التقليدية فالخدمات المصرفية المقدمة للزبائن تغيرت فالإفصاح المحاسبي هنا لابد من أن يكون مختلفا عن الإفصاح المحاسبي في ظل العمل التقليدي بل يجب أن يفصح عن محتوى مالي وكمي عن كل ما يتعلق بالإفصاح في ظل تحديات الأمن السيبراني وبذلك يشكل البحث منطلقاً جديداً عن الإفصاح واتساع مداه في ظل مخاطر الأمن السيبراني .

رابعاً :هدف البحث: البحث عموماً يهدف إلى مراجعة نظرية للبحوث حول أهمية التحول الرقمي المصرفي والتوصل للنتائج لأثر الإفصاح المحاسبي عن المخاطر التي يتضمنها الأمن السيبراني والتعريف بمفهوم الأمن السيبراني ودور المصارف في الإفصاح عن الإجراءات المتعلقة به من خلال التقارير المحاسبية والرقابية وتقارير الإدارة في ظل غياب معايير تحدد النوعية والكمية لذلك الإفصاح الذي تحتويها تلك التقارير المتعلقة بالأمن السيبراني

خاساً :تحليل الأدبيات السابقة ذات الصلة بالدراسة

في السنوات الأخيرة ، قام البنك المركزي العراقي بكثير من الاجراءات لتحسين جودة ونطاق الخدمات المصرفية. ومع ذلك ، فإن التغيرات في العالم ، وعملية العولمة ، والتطور المفرط للقدرة التنافسية ، والحاجة إلى زيادة تكثيف عملية تحول البنوك التجارية ، والحاجة إلى نقل الخدمات المصرفية إلى مستوى جديد

- دراسات تتعلق بالتحول الرقمي في القطاع المصرفي العراقي:

1. دراسة (عباس ، 2016) " Reliable, fast and accurate banking transactions using the electronic bank "(معاملات مصرفية موثوقة وسريعة ودقيقة باستخدام المصرف الإلكتروني) هدف الدراسة الى اقتراح نظام مصرفي يحول المعاملات اليدوية الى معاملات تعتمد على الحوسبة من اهم النتائج أنه يفتح نافذة الخدمات المصرفية الإلكترونية والتسوق عبر الإنترنت فضلاً عن دفع الفواتير دون أي جهد.
2. دراسة (بريس وجبر،2020)" تكنولوجيا التحول الرقمي وتأثيرها في تحسين الأداء الاستراتيجي للمصرف "هدف البحث إلى دراسة تأثير تكنولوجيا التحول الرقمي في تحسين الأداء الاستراتيجي للمصرف، وأهم النتائج حيث توصلت إلى أن التكنولوجية الرقمية الجديدة أدت إلى زيادة توسع أسواق المصارف وذلك عن طريق تغيير أنموذج الأعمال الذي يمكن المصارف من توسيع نطاقها للوصول إلى الزبائن، وكان من أهم التوصيات ضرورة الإفادة من تجارب المصارف العالمية في هذا المجال.

3. دراسة (عبد علي ،خضير 2020) " التحول الرقمي للعمليات المصرفية كأداة لتطوير الأداء المالي الاستراتيجي لمصرف بغداد نموذجا "هدفت هذه الدراسة إلى التعرف على طبيعة التحول الرقمي للعمليات المصرفية، واختبار تأثير التحول الرقمي للعمليات المصرفية من خلال أبعاده نظام التسوية الآنية إلى الدفع الإلكتروني، المقاصة الإلكترونية. أهم النتائج كانت تتركز على أن التحول الرقمي للعمليات المصرفية له دور مهم في تحقيق العالقة والتأثير على الأداء المالي الاستراتيجي.

- دراسات تتعلق بالأمن السيبراني في العراق :

1. دراسة (الزبيدي والتميمي،2022)" العراق والأمن السيبراني ..الفرص والتحديات" هدفت الدراسة الى التعريف بدور الأمن السيبراني في إدارة ملفات النظام الأمني في العراق وتقديم حلول ممكنة لتعزيز مفهوم الأمن السيبراني ، وتعميق المفهوم العلمي في الميادين الأمنية والسياسية والعسكرية والاقتصادية . ابرز النتائج في ان تقنية المعلومات في مقدمة المطالب الأولى والضرورية لبناء دول آمنة في منطقة لطالما كانت مفتقدة للأمن والأمان

- دراسات سابقة عربية :

1. دراسة (الشمالي،2017)" أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على المصارف العاملة في الأردن "هدفت هذه الدراسة إلى التعريف بأمن المعلومات وأثرها في الأداء المصرفي بالأردن
2. دراسة (السيد البغدادي،2021)" اقتصاديات الأمن السيبراني في القطاع المصرفي" هدفت الدراسة إلى إبراز التحديات التي تواجه المجتمع لغرض تحقيق الأمن السيبراني ومن أهم النتائج أن التطور المستمر في المخاطر السيبرانية يحفز المصارف على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر .

- دراسات اجنبية :

1. دراسة (More et al.2015)"Online Banking and Cyber Attacks: The Current Scenario" الخدمات المصرفية عبر الإنترنت والهجمات الإلكترونية: السيناريو الحالي هدفت الدراسة إلى تحليل فئات الجرائم الإلكترونية في القطاع المصرفي ومراجعة الحيل أو التقنيات المستخدمة من قبل مجرمي الإنترنت وكذلك مراجعة السيناريو الحالي للجرائم الإلكترونية. وأيضا اقتراح الإجراءات الوقائية ونصائح السلامة للسيطرة على الجرائم الإلكترونية والوقاية منها. أهم النتائج تتزايد الجرائم الإلكترونية في الهند بشكل ملحوظ. (وسائل التواصل الاجتماعي، والاحتيال على بطاقات الائتمان،، والفيروسات، والبرامج الضارة، ورفض الخدمات، والمقامرة، وخرق البيانات الشخصية، وخرق بيانات الشركة)
2. دراسة (Ali et al . 2017) " The effects of cyber threats on customer's behavior in e-Banking services") آثار التهديدات الإلكترونية على سلوك العميل في الخدمات المصرفية الإلكترونية) تهدف هذه الدراسة إلى تحليل بشكل نقدي ويناقش آثار التهديدات الإلكترونية عند التعامل مع الخدمات المصرفية عبر الإنترنت. أهم النتائج أن هناك حاجة إلى زيادة وعي الزبائن بشأن الجرائم الإلكترونية المتاحة عند التعامل مع الخدمات المصرفية عبر الإنترنت والبيانات المالية الحساسة.
3. دراسة(Maharjan & Chatterjee. 2019) "Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal (إطار عمل لتقليل مشكلات الأمن السيبراني في المصارف قطاع نيبال هدفت الدراسة لتحليل قضايا الأمن السيبراني المتعلقة بالقطاع المصرفي في النيبال واقتراح إطار عمل جديد للحد من التهديد السيبراني.
4. دراسة (Kitsios et al2021) بعنوان " Digital Transformation and Strategy in the Banking Sector: Evaluating the Acceptance Rate of E-Services"(التحول الرقمي والاستراتيجية في القطاع المصرفي: تقييم

معدل قبول الخدمات الإلكترونية) هدفت هذه الدراسة في مقبولية التحول الرقمي لموظفي القطاع المصرفي في اليونان ومن ابرز النتائج ان المخاطر السيبرانية تمثل تحديًا كبيرًا يجب أن يؤخذ بنظر الاعتبار من قبل الموظفين والمديرين التنفيذيين وقد يؤثر على رغبتهم في استخدام التقنيات الرقمية وجدت الدراسة أن الموظفين يتجاهلون العواقب السلبية للهجمات الإلكترونية.

ما يميز الدراسة الحالية عن الدراسات السابقة بأنها اعتمدت على ثلاثة متغيرات وربطت بعضها ببعضها الاخر وهذه المتغيرات كانت بينهما علاقة ارتباط قوية من حيث التأثير فهناك تأثير قوي بين التحول الرقمي والإفصاح المحاسبي فضلاً عن العلاقة بين الإفصاح المحاسبي ومخاطر الأمن السيبراني

المبحث الثاني

الإطار المفاهيمي للتحول الرقمي المصرفي

1. الإطار المفاهيمي لنماذج الأعمال المصرفية الأساسية:

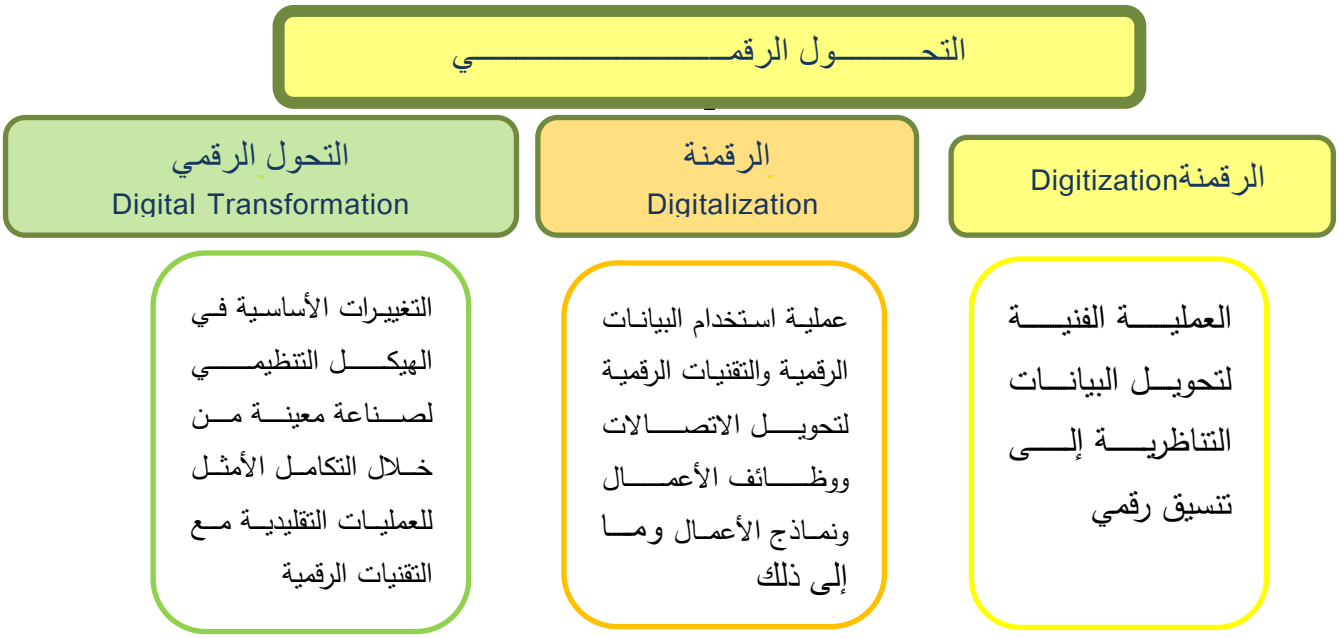
فضلاً عن أن معظمها يؤدي الوظائف الموضحة أعلاه جميعها، إلا أن المصارف تعمل بنماذج أعمال مختلفة بناءً على تفضيلات المخاطر الخاصة بها ومكانتها السوقية والمزايا النسبية. يركز كل نموذج عمل مصرفي على بعض الأنشطة بدلاً من الأخرى (Carletti et al.2020:28) لقد شهدت الصناعة المصرفية تطوير نماذج أعمال مختلفة تهدف إلى إرضاء أسواق معينة. ومع ذلك ، فقد بدأت نماذج الأعمال المصرفية في التغيير ليس فقط تحت تأثير الزبائن ولكن أيضًا تحت تأثير التطورات التكنولوجية. بدلاً من ذلك ، تواجه أنواعًا جديدة من المنافسة من خلال إنشاء نماذج أعمال مصرفية جديدة. بصرف النظر عن النماذج التقليدية ، قد تندرج المؤسسات التي تقدم الخدمات المالية باستخدام تطورات التكنولوجيا المالية في نموذجين تجاريين عريضين مثل نموذج المصرف الرقمي أو نموذج المصرف الجديد.(Temelkov.2020:10)

1.1 نموذج الأعمال المصرفية التقليدية Traditional bank business model: تواجه المصارف التقليدية إجراءات الإصلاح الضرورية وربما التحدي الأكبر الذي تواجهه حتى الآن قدرتها على الاستمرار بالمنافسة وهي تتمتع الآن بفرصة تحويل نموذج أعمالها إلى منصة أو نظام مصرفي رقمي. وهذا سيمكنهم من تلبية متطلبات العصر الرقمي بأسرع طريقة ممكنة (Dapp & Hoffmann. 2015:16) فالتقدم التكنولوجي قد يؤدي إلى التفكك الرأسي والأفقي لنمط العمل المصرفي التقليدي فالتطورات الجديدة مستمرة قدماً في اتجاه تمكين التعلم الآلي والذكاء الاصطناعي من خلال وفرة البيانات (غير المالية)، وهيمنة المنصات الرقمية والهواتف الذكية (Boot et al. 2020:5).

2.1نموذج الاعمال المصرفية الرقمية Digital bank business model :يمكن أن تكون الخدمات المصرفية الرقمية بديلاً جيدًا للبنوك في البلدان الأقل تقدمًا لتقديم الخدمات المصرفية لمحدودي الدخل لأنها تساهم في تجاوز مشكلات البنية التحتية المتخلفة وتكلفة السفر. (Yip & Bocken.2018:156).وتواجه المصارف التقليدية إجراءات الإصلاح الضرورية وربما التحدي الأكبر الذي تواجهه حتى الآن قدرتها على الاستمرار بالمنافسة وهي تتمتع الآن بفرصة تحويل نموذج أعمالها إلى منصة أو نظام مصرفي رقمي. وهذا سيمكنهم من تلبية متطلبات العصر الرقمي بأسرع طريقة ممكنة (Dapp &Hoffmann.2015:16)

3.1**مراحل التحول الرقمي**: تُعرف الرقمنة أيضًا باسم التحول الرقمي وهي مزيج من كل من إجراءات الرقمنة والابتكار الرقمي بهدف تحسين المنتجات الحالية بقدرات متقدمة ،وهي تقوم بتزامن الأعمال واستراتيجية تكنولوجيا المعلومات لوحدة اقتصادية ما وإدماج تكنولوجيا المعلومات في استراتيجية الأعمال(Udovita.2020:522) و بصورة عامة تشمل مراحل التحول الرقمي ثلاث مراحل بصورة عامة ففي العام 1937 ، اخترع المهندس الألماني (Konrad Zuse) آلة (Z1)هذه الآلة تقوم بأجراء العمليات الحسابية على أساس الأرقام الثنائية والأصفار والآحاد، (Zuse) وهذا الاختراع الثوري الذي اصبح أساسًا لجميع التقنيات المحوسبة تقريبًا التي نعرفها ونستخدمها في حياتنا اليومية. لم يؤثر اختراع (Zuse)على عالم التكنولوجيا فقط (جميع أنظمة الكمبيوتر الرقمية الرئيسية التي اتبعت (Z1)كانت تستند إلى مبدأ(نظام Zuse الثنائي) ولكنها كانت بمثابة أصل الصياغة لظاهرة نسميها الرقمنة وهذه المراحل هي :

شكل رقم (1)



المصدر:من اعداد الباحث بالاعتماد على (Morze&Strutynska.2021:5)

1. مَرْحَلَة اَلرَّقْمَنَة (Digitization): مهمتها تحويل أصول مادية كالبيانات إلى بيانات رقمية أو كائنات رقمية عن طريق ماسح ضوئي أو كاميرا أو أي جهاز إلكتروني آخر لغرض معالجتها بواسطة الحاسوب. (Manžuch. 2017:2)

2. مرحلة الرقمنة (Digitalization) : ليس للرقمنة (digitalization) تعريف واحد واضح كالرقمنة (digitization). يوضح كلا من (J. Scott Brnnen)، مرشح الدكتوراه في الاتصال، و (Daniel Kreiss)، على أنها الطريقة التي يتم بها إعادة هيكلة العديد من مجالات الحياة الاجتماعية حول الاتصالات الرقمية والبنى التحتية لوسائل الإعلام، ومن ثم فإن (Brnnen & Kreiss) يبنيان تعريفهما للرقمنة على الحياة الاجتماعية- وبعبارة أخرى، كيف يتفاعل الناس مع انتقال هذه التفاعلات بعيدًا عن التقنيات التناظرية (البريد العادي والمكالمات الهاتفية) إلى التقنيات الرقمية (البريد الإلكتروني والدردشة والوسائط الاجتماعية)، تصبح مجالات العمل والترفيه على حدٍّ سواء رقمية. (Bloomberg. 2018:3)

3. التحول الرقمي (Digital Transformation): التحول الرقمي يشمل الاتصال ما بين الجهات الفاعلة، مثل الشركات والزبائن، عبر قطاعات سلسلة القيمة المضافة جميعها وتطبيق التقنيات الجديدة على هذا النحو ويتطلب التحول الرقمي مهارات تتضمن استخراج البيانات وتبادلها وكذلك تحليل تلك البيانات وتحويلها إلى معلومات قابلة للتنفيذ وتقيم هذه المعلومات لغرض استخدامها في عدة خيارات في اتخاذ القرارات أو أنشطة التي ترفع من أداء ونطاق الشركة ونطاق ويشمل التحول الرقمي الشركات ونماذج الأعمال والعمليات والعلاقات والمنتجات وما إلى ذلك (Schallmo & Daniel. 2018:11) إن الرقمنة التي تُعرف أيضًا باسم التحول الرقمي هي مزيج من كل من إجراءات الرقمنة والابتكار الرقمي بهدف تحسين المنتجات الحالية بقدرات متقدمة، وهي تقوم بتزامن الأعمال واستراتيجية تكنولوجيا المعلومات لوحدة اقتصادية ما وإدماج تكنولوجيا المعلومات في استراتيجية الأعمال (Udovita. 2020:522)

4.1المراحل الرئيسية للتحول الرقمي في القطاع المصرفي :

مفهوم الرقمنة في القطاع المصرفي (Digitization in banking sector) يعني الأداء السلس وتجربة خالية من المتاعب للعملاء, وتقدم الرقمنة خدمات جديدة قائمة على التكنولوجيا لعملائه مثل أجهزة الصراف الآلي ، وبطاقات الائتمان ، والتسوية الإجمالية في الوقت الحقيقي ، والتحويل الإلكتروني للأموال ، والخدمات المصرفية عبر الإنترنت ، والخدمات المصرفية عبر الهاتف النقال.(Shetty &Joishy.2021:126) ، وفقًا للخبراء ، في القطاع المصرفي ، يمكن أن يحدث التحول الرقمي في خمس مراحل رئيسية (Galazova &Maomeva.2019:48-49) .

1. اعتماد القنوات الرقمية: شبكات الصراف الآلي ، الخدمات المصرفية عبر الإنترنت ، الخدمات المصرفية عبر الهاتف المحمول ، روبوتات الدردشة. يبدأ التغيير الرقمي في الأعمال التجارية. المستخدم الذي يريد التفاعل مع المصرف من خلال أي قنوات متاحة في وقت مناسب يكون في قلب النظام البيئي.
2. ظهور المنتجات الرقمية: البيانات الضخمة ، والمدفوعات غير التلامسية ، والبطاقات الافتراضية ، والذكاء الاصطناعي ، والآلات. بمساعدة البرامج الحديثة المتقدمة ، يتم إنشاء منتجات E2E ((end to end) ، مصممة لتلبية الاحتياجات المالية للعملاء على مدار 24 ساعة
3. اعتماد دورة كاملة من الخدمات الرقمية: لا تضيف المصارف فقط الخدمات الرقمية إلى منتجاتها التقليدية ، بل تنشئ أعمالًا رقمية جديدة ، وتغير نماذج الأعمال تمامًا ، وتوسع حدود أعمالها. يتيح استخدام الأدوات الرقمية لها أن تصبح عالمية.
4. خلق ذكاء رقمي. يدرس "العقل الرقمي" البيانات بشكل تلقائي في قطاعات الأعمال جميعها والأقسام وخطوط الإنتاج والخدمات بشكل مستمر ، مما يمنح المؤسسة معرفة أعلى بقدراتها
5. المرحلة الخامسة. إنشاء "DNA رقمي" - نظام إحداثيات جديد لاتخاذ القرارات الاستراتيجية طوال دورة حياة المصرف.

6.1 مزايا وعيوب المصارف الرقمية:

يمكن التنبؤ برقمنة القطاع المصرفي لمواكبة التوقعات المتزايدة للعالم وأن الاستخدام المتزايد للهواتف الذكية قلل من الأخطاء البشرية وزاد من الراحة. أما التهديدات السيبرانية آخذة في الازدياد، ومن ثم، يجب أن تكون المصارف يقظة للغاية ويجب أن تكون مستعدة للتعامل مع الهجمات الإلكترونية وتعتبر الرقمنة ذات أهمية حيوية لمعالجة البيانات وتخزينها ونقلها، لأنها "تسمح بنقل المعلومات من جميع الأنواع بجميع الأشكال بنفس الكفاءة. (Harchekar.

2018:103) من أهم الخدمات التي تقدمها المصارف الرقمية هي الاستثمارات وحسابات التداول عبر الإنترنت وتحويل الأموال الإلكتروني وخدمات المقاصة وشبكات الفروع وتطبيقات الهاتف المحمول والمحفظة هي بعض المنتجات والخدمات الحديثة التي تعمل كمحرك لنمو القطاع المصرفي فتحقق المصارف الرقمية الكثير من المزايا ومنها: (NAVEENA.2018:487) و(Harchekar.2018:104)

1. خفض التكاليف للمصارف والزبائن من خلال استخدام أجهزة الصراف الآلي والمعاملات غير النقدية وما إلى ذلك.
2. إدارة المصارف الرقمية يتيح لها توفر المزيد من البيانات الرقمية تمكنها من اتخاذ قرارات مرنة سريعة من خلال استخدام التحليلات الرقمية وهذا بدوره ينعكس على كل من الزبائن والمصارف.
3. تتصف التكنولوجيا بأنها غير تمييزية لذلك سيتم التعامل مع الجميع بنفس الطريقة في المصارف.
4. سيزداد عدد الزبائن بالنسبة للبنوك بسبب زيادة ملاءمة العمل المصرفي لهم .
5. تقلل الرقمنة من الخطأ البشري.
6. تحسين خبرة الزبائن
7. ستقل الحاجة إلى التعامل مع مبالغ نقدية كبيرة.
8. .تسهل الرقمنة المصرفية من فتح الحسابات المصرفية.
9. بالاعتماد الأتمتة سيتم التخلص من المهام المتكررة.
10. سيتم القضاء على الفجوة الريفية والحضرية.

أما عيوب المصارف الرقمية فتتمثل بالآتي:

1. تقلل الرقمنة من جهد الموظفين ومن ثم تؤدي إلى فقدان الوظائف.
2. قد تتوقف بعض فروع المصارف عن الوجود مع تزايد استخدام الخدمات المصرفية عبر الإنترنت
3. ستكون المصارف أكثر عرضة للهجمات الإلكترونية.
4. انعدام الخصوصية، إذ لا يستطيع أحد إخفاء أي مبلغ في المصارف
5. ارتفاع معدلات البطالة

المبحث الثالث

الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني

1. الافصاح المحاسبي في البيئة الرقمية :

ظهر في نهاية القرن العشرين تقدم وتطور أنظمة (تكنولوجيا المعلومات والاتصالات وتقنية المعلومات). وقد ترافق ذلك مع نمو كبير في استخدام الإنترنت في عالم الأعمال. اتجهت الشركات والأسواق العالمية إلى استخدام الإنترنت والمواقع الإلكترونية لنشر تقاريرها المالية وتقديم المعلومات المالية لأصحاب المصلحة، حيث توفر العديد من المزايا مثل السرعة العالية في إيصال المعلومات، وسهولة الوصول إليها وانخفاض تكلفة الحصول عليها، وهو ما يسمى التقارير المالية عبر الإنترنت (IFR) أو الإفصاح الإلكتروني. (Syaeid. 2019:17)تمتلك الشركات حافزًا لإدارة الإفصاح عن الأمن السيبراني بشكل استراتيجي، تمامًا كما تفعل مع الإفصاح الطوعي الآخر مثل تلك التي تنطوي على مخاطر الأعمال وبعض المعلومات المالية والأداء البيئي والاجتماعي حيث تدفع القوى التنظيمية الشركات إلى الكشف عن المزيد من معلومات الأمن السيبراني والقيام بذلك في الوقت المناسب. من ناحية أخرى، قد يساعد الكشف عن

معلومات الأمن السيبراني المتسللين في مهاجمة الشركة بنجاح، مما يضعف حوافز الكشف. وبالمثل، (D 'Arcy & Basoglu. 2022:780)يعد الإفصاح عن المخاطر جانبًا مهمًا من جوانب حوكمة المخاطر ،فهنالك مخاوف بشأن جودة وكفاية عمليات الكشف عن المخاطر حيث قد يكون لدى المديرين التنفيذيين حوافز لتقليل التعرض للمخاطر الإلكترونية والمبالغة في الدفاعات ضدها، وقد يؤدي الكشف عن المعلومات السلبية حول الأمن السيبراني إلى زيادة تكلفة رأس المال وكشف المعلومات السرية لكل من المنافسين والمهاجمين. من ناحية أخرى ، قد يؤدي الإفصاح غير الكافي إلى ترك الشركة عرضة للتقاضي وفقدان السمعة (McGrath et al.2022:8). فقد اكدت عدد من الدراسات فوائد الإفصاح في سوق رأس المال على سبيل المثال (Healy و Hutton و 1999 Palepu ؛ Leuz and Verrecchia 2000 ؛ Botosan and Plumlee 2002 ؛ Leuz and Schrand 2011 ؛ Balakrishnan و Billings و Kelly و 2014 Ljungqvist). وبالمثل ، فإن الإفصاح عن الأخبار السيئة في الوقت المناسب يمكن أن يحمي الشركات من مخاطر التقاضي.(Ashraf.2020:18)وهنا يجب على الشركات الإفصاح عن طبيعة الهجوم وحدوثه وتكلفته وعواقبه بالإضافة إلى الكشف عن تكاليف الهجمات الفعلية ، يجب على الشركات أيضًا الكشف عن تكاليف الهجمات المحتملة ، والتي قد يكون من الصعب تقديرها ،.(Jin.2015:18) لقد أصبح الأمن السيبراني أيضًا مسألة محاسبة ومراجعة إدارية إلى حد كبير ،فهي تخضع لتحليل التكلفة والعائد ، وتقييم الرقابة الداخلية واعتبارات سياسة الإفصاح. وفقًا لـ(Gordon and Loeb 2006) ، يمكن تقسيم أهداف الأمن السيبراني إلى ثلاث فئات رئيسة: (Haapamäki, & Sihvonen.2019: 809)

- يقوم الأمن السيبراني بحماية سرية المعلومات الخاصة
- يضمن أن المستخدمين المصرح لهم يمكنهم الوصول إلى المعلومات في الوقت المناسب
- يقوم الأمن السيبراني بحماية دقة المعلومات وموثوقيتها وصحتها.

1.1 مفهوم الأمن السيبراني : تناولت عدد من الأوراق البحثية. مثل (Rossouw von Solms، Johan van Niekerk. 2013) مصطلح الأمن السيبراني حيث عرّف على أنه حماية المستخدم وأصوله من أي تهديدات عبر الإنترنت، أما في الوقت الحاضر، فقد أصبح مفهوم الأمن السيبراني أكثر بكثير من مجرد انعدام الأمن ليصبح مشكلة حقيقية تتطلب الاهتمام واتخاذ التدابير المناسبة لضمان سلامة مستخدمي الإنترنت وتجاوز الأمن السيبراني المشكلات التقنية وأصبح سببًا للعديد من المشكلات الاجتماعية فيمكن القول إن الأمن السيبراني يعبر عن الإجراءات والموارد المستخدمة جميعها لضمان سلامة الفضاء السيبراني والأنظمة المتصلة بالفضاء السيبراني من الحوادث غير القانونية والتي تعتبر مخالفة للقانون (Al shamsi. 2019:9). وهناك تعريف الأمن السيبراني استنادا لأهدافه بأنه "النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج ومن ثم لا تتحول الأضرار إلى خسائر دائمة (السيد البغدادي، 2021: 1453). لقد كشفت دراسة استقصائية في عام 2016 حول تكلفة الجرائم الإلكترونية في الاقتصاد العالمي حيث بلغت حوالي 450 مليار دولار أمريكي. ومن هذه الجرائم هجمات رفض الخدمة والبنية التحتية والقضايا الأخرى المتعلقة بحماية البيانات حيث تعد جزءًا رَئِيسِيًّا من الهجمات الإلكترونية عالية التنميط وكذلك ما يقرب من 70٪ من الرؤساء التنفيذيين لسوق رأس المال والمصارف يعتبرون الأمن السيبراني تهديدًا لتطورهم. (Soni. 2019:2) تعتبر المؤسسات المالية المعتمدة على النظم القديمة هي الأكثر عرضة من غيرها لخطر تهديدات بالهجمات السيبرانية، بالإضافة إلى ذلك انخفاض تكلفة شن هذه

الهجمات، وكذلك فإن آثار تلك الهجمات مؤثرة جداً في تلك المؤسسات التي تعتمد النظم الإلكترونية بسبب أنشطتها غير الملموسة بسبب اعتمادها بشكل كبير على التكنولوجيا. ويرجع ذلك إلى الأسباب الآتية. (السيد البغدادي، 2021: 1473).

1.1 البنية التحتية للمصارف الرقمية: يمكن القول ان المصارف التي تستخدم الخدمات المصرفية الرقمية تصنف على أنها "مبتكرة" وتكاليفها أقل مقارنة بالمصارف الاخرى في نفس القطاع لذلك ، فإن أهمية البنية التحتية الإلكترونية التي تستخدمها المصارف تتمثل في انخفاض تكلفة كل معاملة إلى جانب البنية التحتية المتطورة من نظم الدفع والتسوية، ومنصات التداول ، وودائع الأوراق المالية المركزية ، والأطراف المقابلة المركزية. ومع ذلك يمثل مستوى تعليم العميل بما في ذلك وظائف موقع المصرف على شبكة الإنترنت هي أساس العوامل التي تساهم في نجاح الخدمات المصرفية عبر الإنترنت. (Suleymanov et al.2019:19) ان تطوير البنية التحتية المصرفية الإلكترونية بالطريقة الصحيحة يزيد من المسؤولية وأقصى قدر من المشاركة فتجارة الموارد المصرفية سيؤدي إلى رفاهية اقتصادية واجتماعية في المجتمع ، ومن ناحية أخرى ، فإن دورة الإنتاج من خلال تخصيص الموارد المصرفية في مختلف القطاعات و أدت البنى التحتية للمجتمع مثل الصناعة والزراعة والتجارة والصحة والتعليم وريادة الأعمال وما إلى ذلك إلى انخفاض في البطالة وامتصاص العمالة وزيادة نصيب الفرد. ونتيجة لذلك ، سوف يترافق مع تحسين نوعية الحياة والصحة الاجتماعية للمجتمع والحد من الفقر ، والتي تعتبر من مؤشرات التنمية الاقتصادية والاجتماعية.(Mohammadi.2020:94).

3.1 التهديدات المحتملة في قطاع المصارف الرقمية :

1 سرقة الهوية: سرقة الهوية في الخدمات المصرفية الإلكترونية هي الاستيلاء على المعلومات الشخصية لبعض الأفراد لارتكاب الاحتيال من أجل الفوائد المالية. ينتج عنه خسائر مالية فادحة للضحايا وكذلك المصارف.

2 التصيد الاحتيالي: Phishing هو إحدى أكثر الطرق شيوعًا التي يمكن من خلالها سرقة الهوية في الخدمات المصرفية الإلكترونية، ويستخدم عناوين بريد إلكتروني مزيفة ومواقع إنترنت زائفة تحرض الزبائن الساذجين على الكشف عن معلومات شخصية مثل معرف المستخدم وكلمات المرور وأرقام بطاقات الائتمان وأكواد PIN والعناوين، وأرقام الحسابات المصرفية، وما إلى ذلك. (Sah. 2020:2)

3 التصيد Vishing: يحدث عندما يتصل المهاجم بالضحية ويستخدم الهندسة الاجتماعية لخداع الضحية للكشف عن بعض المعلومات السرية.

4 أنظمة الخدمات المصرفية الصوتية المستنسخة Cloned voice- banking systems: يحدث هذا عندما تقوم العديد من هجمات التصيد الإلكتروني باستنساخ أنظمة الخدمات المصرفية الصوتية بحيث تبدو مثل الأنظمة الرسمية. تُستخدم رسائل البريد الإلكتروني المزيفة لحث الزبائن على الاتصال برقم يزعم أنه بنكهم. (Abu & Matalqa. 2015:181).

5 البرامج الضارة (الشفرة الخبيثة) (Malicious) Malware: تُعْرَف الشفرة الخبيثة (أو البرامج الضارة) على أنها برامج تحقق نية المهاجم لإحداث ضرر عمدًا. ويمكن استخدام الفيروسات لإلحاق الضرر بأجهزة الكمبيوتر والشبكات المتصلة، وسرقة المعلومات، وإنشاء شبكات الروبوت، وتقديم الإعلانات، وسرقة الأموال (Moser et al. 2009:1)

6 القرصنة أو الاختراق (Hacking/ Cracking): اقتحام أجهزة وشبكات الكمبيوتر الطرف الآخر لغرض الربح أو حذف البيانات أو ملفات البرامج واختراق خادم الويب وتخريب صفحات الويب أما اختراق أنظمة الكمبيوتر لإحداث ضرر. (Pathak. 2016:48)

7 أتمتة الاحتيال على الخدمات المصرفية عبر الإنترنت Automating Online Banking Fraud: في الوقت الحاضر تقدم مجرمو الإنترنت والمحتالون على الكمبيوتر خطوة إلى الأمام من خلال الاعتماد على أنظمة التحويل الآلي (ATSs). حيث بدأ نظام جديد لنظام احتيال الخدمات المصرفية عبر الإنترنت الآلي الذي يستخدم بالاقتران مع متغيرات البرامج الضارة (Spy Eye) و (Zeus) كجزء من ملفات (Web Inject) وهو ملف نصي يحتوي على الكثير من أكواد JavaScript و HTML. (Ali et al. 2017:73)

8 . الثغرات الأمنية :Zero Day Attack يعتبر Zero Day Attack ثغرة أمنية يستغلها مستخدمو الإنترنت وهو أحد الأدوات الفعالة التي يستخدمها المهاجمون الآن ، لأن بيانات Zero Day Attackغير متاحة الا بعد اكتشاف الهجوم(Adil et al.2020:3) بشكل عام يتم تعريف Zero Day Attack على أنه الموقف الذي يستغل فيه المهاجم ثغرة أمنية لا يلاحظها المسؤول أو المطور ويعد ضمن سياق التصيد الاحتيالي وتتمثل الطريقة المباشرة لمعالجة هذه المشكلة في تنفيذ آلية تحد من هذه الثغرة (Haruta.2019:2463) يخلص نظام التحديث التلقائي Hue Signature القائم على التشابه البصري لكشفZero Day Attack

9 اختراق البيانات: يؤدي خرق البيانات إلى فقدان المعلومات الآمنة أو الشخصية بشكل متعمد أو غير مقصود. يمكن أن تتضمن خروقات البيانات أي نوع من البيانات: المعلومات المالية ، معلومات الهوية الفردية بما في ذلك محركات الأقراص الثابتة أو معلومات قاعدة البيانات التي قد يتم تخزينها دون تشفير(Alliance.2015:5) فيما عرف (Rosati et al.2019:2) اختراق البيانات بأنه حادثة تنطوي على وصول غير مصرح به إلى بيانات حساسة أو محمية أو سرية مما يؤدي إلى اختراق أو احتمال المساس بالسرية أو السلامة أو توافر أصل المعلومات على أنه الاستحواذ غير المصرح به

10 هجمات الهندسة الاجتماعية social engineering attacks: تعد من أخطر التهديدات حَالِيًّا، تمثل أكبر التهديدات التي تواجه الأمن السيبراني. ويمكن اكتشافها ولكن لا يمكن إيقافها. يستغل المهندسون الاجتماعيون الضحايا للحصول على معلومات حساسة، والتي يمكن استخدامها لأغراض محددة أو بيعها في السوق السوداء. (Luo et al 2011:1-2). أصبح الأمن السيبراني أيضًا مسألة محاسبة ومراجعة إدارية إلى حد كبير، تخضع لتحليل التكلفة والعائد، وتقييم الرقابة الداخلية واعتبارات سياسة الإفصاح. وفقًا ل) Gordon and Loeb 2006)، يمكن تقسيم أهداف الأمن السيبراني إلى ثلاث فئات رئيسة: Haapamäki، 2019:809 .& Sihvonen)

- يقوم الأمن السيبراني بحماية سرية المعلومات الخاصة
- يضمن أن المستخدمين المصرح لهم يمكنهم الوصول إلى المعلومات في الوقت المناسب
- يقوم الأمن السيبراني بحماية دقة المعلومات وموثوقيتها وصحتها

المبحث الرابع

جدول (1)

الجانب التطبيقي من خلال المقارنة ما بين الدراسات السابقة والحالية التي تم تناولها

عنوان الدراسة	تناولت الدراسة التحول الرقمي	تناولت الدراسة الأمن السيبراني	دراسات متعلقة بالإفصاح المحاسبي
دراسة (عباس ، 2016) "	نعم تناولت الدراسة التحول الرقمي	لم تتناول الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة (بريس وجبر،2020)"	نعم تناولت الدراسة التحول الرقمي	لم تتناول الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة (عبد علي ،خضير 2020)	نعم تناولت الدراسة التحول الرقمي	لم تتناول الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة (قنديل،2022)" "	لم تتناول التحول الرقمي	نعم تناولت الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة (الزبيدي والتميمي،2022)"	لم تتناول التحول الرقمي	نعم تناولت الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة (الشمالي،2017)"	لم تتناول التحول الرقمي	نعم تناولت الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة (السيد البغدادي،2021)	لم تتناول التحول الرقمي	نعم تناولت الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة (More et	نعم تناولت الدراسة	لم تتناول الأمن السيبراني	لم تتناول الإفصاح

(al.2015	التحول الرقمي		المحاسبي
دراسة (Ali et al2017)	نعم تناولت الدراسة التحول الرقمي	لم تتناول الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة(2019. (Maharjan	نعم تناولت الدراسة التحول الرقمي	نعم تناولت الأمن السيبراني	لم تتناول الإفصاح المحاسبي
دراسة (Kitsios et (al2021	نعم تناولت الدراسة التحول الرقمي	نعم تناولت الأمن السيبراني	لم تتناول الإفصاح المحاسبي
الدراسة الحالية (2022) اثر التحول الرقمي للمصارف التجارية العراقية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني	الدراسة الحالية تطرقت بشكل مباشر إلى أثر التحول الرقمي للمصارف التجارية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني وما ينطوي على هذا الأثر في حين أن الدراسات السابقة لم تتطرق إلى تلك العلاقة ما بين الإفصاح المحاسبي والمخاطر التي تنتج عن مخاطر الأمن السيبراني. لم تكن الدراسات السابقة تتصف بالقصور من ناحية عدم تناول الأمن السيبراني او الإفصاح المحاسبي ، أنما القصور كان في المجال الذي ينتمي الإفصاح المحاسبي لذا تعد الدراسة رائدة في هذا المجال من وجهة نظر الباحث		

الاستنتاجات:

1. اهم نتائج الدراسة الحالية أنها تطرقت بشكل مباشر إلى أثر التحول الرقمي للمصارف التجارية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني وما ينطوي عليه هذا الأثر في حين أن الدراسات السابقة لم تتطرق إلى تلك العلاقة ما بين الإفصاح المحاسبي والمخاطر التي تنتج عن مخاطر الأمن السيبراني.

2. إنّ عملية التحول الرقمي في المصارف التجارية تتطلب اجراءات جدية لعملية التحول من المصارف نفسها وكذلك الجهات المسؤولة عن ادارة المصارف .

3. إنّ عملية التحول الرقمي في المصارف التجارية تؤدي الى زيادة الوصول إلى الزبائن حيث تستفيد المصارف والمؤسسات المالية الأخرى من التكنولوجيا الرقمية لزيادة انتشارها بشكل كبير. تؤدي الى انخفاض تكاليف التوظيف بسبب الاعتماد على التشغيل الآلي لتقديم الخدمات

4. إنّ عملية التحول الرقمي في المصارف التجارية تؤدي الى سيطرة أفضل على المعلومات تفيد باتخاذ قرارات أكثر ذكاءً في الوقت المناسب والمزيد من التحكم في المعلومات وعدم تكرار أخطاء المعلومات

5. يمثل الإفصاح المحاسبي في ظل عملية التحول الرقمي في المصارف التجارية تحدياً كبيراً بسبب البيئة المحلية المتأخرة في هذا المجال

التوصيات:

1. إن على الوحدة الاقتصادية العمل على اتباع سياسة توازن كفتي القبان في الإفصاح السيبراني فعليها أن تحدد من خلال هذه السياسة درجة الإفصاح أو مواطن الإفصاح
2. يجب الافادة من تجارب المصارف الرائدة في مجال توظيف تكنولوجيا الرقمية الجديدة وإدارتها بما يحسن من أداء المصارف للقيام بعملها بشكل مناسب
3. على كليات الإدارة والاقتصادية ولا سيما أقسام المحاسبة والمالية المصرفية إضافة مادة الأمن السيبراني للمناهج الدراسية في هذه الأقسام وكذلك تشجيع الأبحاث العلمية في هذا المجال.
4. يمكن التعاون ما بين المصارف الإقليمية والدولية في مجال التحول الرقمي والأمن السيبراني لتنفيذ عملية التحول
5. على المؤسسات الحكومية ومنها وزارة التعليم العالي تعزيز الخطوات التي قامت بها الجهات الحكومية في مجال الأمن السيبراني بشكل عام .

المصادر:

1. الزبيدي ،زهير خضير عباس , التميمي ،ظفر عبد مطر. (2022). العراق والأمن السيبراني.. الفرص والتحديات .مجلة واسط للعلوم الانسانية ,المجلد 18 العدد51
2. الشمالي، حسين علي قاسم (2017) أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن، مجلة جامعة القدس المفتوحة للأبحاث والدراسات الادارية و الاقتصادية مجلد 2 عدد 7
3. بريس، احمد كاظم ،جبر ، ورود قاسم (2020). تكنولوجيا التحول الرقمي وتأثيرها في تحسين الأداء الاستراتيجي للمصرف (بحث تحليلي لوجهات نظر عينة من المديرين العاملين في القطاع المصرفي التجاري الخاص في كربلاء ، المجلة العراقية للعلوم الإدارية ، المجلد 16 ، العدد65
4. علي ، شروق عبد، خضير، اردان حاتم (2020) " التحول الرقمي للعمليات المصرفية كأداة لتطوير الأداء المالي الاستراتيجي لمصرف بغداد نموذجا، مجلة الادارة والاقتصاد العدد126
5. السيد البغدادي، مروة فتحي. (2021). اقتصاديات الأمن السيبراني في القطاع المصرفي .مجلة البحوث القانونية والاقتصادية (المنصورة مجلد 2 العدد11
6. Abbas, K. I. (2016). Reliable, Rapid, Accurate Banking Transactions using e-Bank. *International Journal of Computer Applications*, *155*(13).
7. Abu-Shanab, E., & Matalqa, S. (2015). Security and Fraud Issues of E-banking. *International Journal of Computer Networks and Applications*, *2*(4), 179-188.

8. Adil, M., Khan, R., & Ghani, M. A. N. U. (2020, February). Preventive techniques of phishing attacks in networks. In *2020 3rd International Conference on Advancements in Computational Sciences (ICACS)* (pp. 1-8). IEEE.
9. Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, *3*(2), 8-29.
10. Alliance, S. C. (2015). *The true cost of data breaches in the payments industry*. Technical report, March 2015. 29, 47.
11. Bloomberg, J. (2018). Digitization, digitalization, and digital transformation: confuse them at your peril. Forbes. Retrieved on August, 28, 2019.
12. Boot, A. W., Hoffmann, P., Laeven, L., & Ratnovski, L. (2020). Financial intermediation and technology: What's old, what's new?.
13. Carletti, E., Claessens, S., Fatás, A., & Vives, X. (2020). Barcelona Report 2-The Bank Business Model in the Post-Covid-19 World. Centre for Economic Policy Research.
14. Shetty, A., & Joishy, S.(2021) DIGITALISATION-OPPORTUNITIES AND CHALLENGES TO BANKING SECTOR. EDITORIAL BOARD, 125.
15. Dapp, T., Slomka, L., AG, D. B., & Hoffmann, R. (2015). Fintech reloaded–Traditional banks as digital ecosystems. *Publication of the German original*, 261-274.
16. D'Arcy, J., & Basoglu, A. (2022). The Influences of Public and Institutional Pressure on Firms' Cybersecurity Disclosures. *Journal of the Association for Information Systems*, *23*(3), 779-805.
17. Galazova, S. S., & Magomaeva, L. R. (2019). The transformation of traditional banking activity in digital.
18. Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. *Managerial Auditing Journal*, *34*(7), 808-834.
19. Harchekar, J. S. (2018). Digitalization in banking sector. (IJTSRD).ISSN.2456-6470
20. Haruta, S., Asahina, H., Yamazaki, F., & Sasase, I. (2019). Hue Signature Auto Update System for Visual Similarity-Based Phishing Detection with Tolerance to Zero-Day Attack. IEICE TRANSACTIONS on Information and Systems, 102(12), 2461-2471.
21. Kitsios, F., Giatsidis, I., & Kamariotou, M. (2021). Digital Transformation and Strategy in the Banking Sector: Evaluating the Acceptance Rate of E-Services. Journal of Open Innovation: Technology, Market, and Complexity, 7(3), 204.
22. Luo, X., Brody, R., Seazzu, A., & Burd, S. (2011). Social engineering: The neglected human factor for information security management. Information Resources Management Journal (IRMJ), 24(3), 1-8.

23. Manžuch, Z. (2017). Ethical issues in digitization of cultural heritage. Journal of Contemporary Archival Studies, 4(2), 4.
24. Mohammadi Raisi, M. Z., Fathi, S., & Karimian, H. (2020). The Developments of the Electronic Banking (E-banking) Industry, A Step towards Achieving Sustainable Development. *IAU International Journal of Social Sciences*, *10*(4), 85-95
25. Morze, N. V., & Strutynska, O. V. (2021, June). Digital transformation in society: key aspects for model development. In Journal of Physics: Conference Series (Vol. 1946, No. 1, p. 012021). IOP Publishing.
26. Moser, A., Kruegel, C., & Kirda, E. (2007, May). Exploring multiple execution paths for malware analysis. In *2007 IEEE Symposium on Security and Privacy (SP'07)* (pp. 231-245). IEEE.
27. NAVEENA, M. S. S. M. (2018)A STUDY ON DIGITAL REVOLUTION IN INDIAN BANKING SECTOR. PRINCIPAL'S MESSAGE, 486.
28. Pathak, P. B. (2016). Cybercrime: A global threat to cyber community. *Incest. Com*, *7*(03), 46-49.
29. Sah, A., Gokare, A. R., & Mounika, U. (2020). IDENTITY THEFT: A BYPRODUCT OF DYNAMIC TRENDS IN E-BANKING. *SUPREMO AMICUS ISSN 2456-9704*, 1.
30. Schallmo, A., & Daniel, R. (2018). Digital Transformation Now! Guiding the Successful Digitalization of Your Business Model. Springer Science+ Business Media, LLC.
31. Soni, V. D. (2019). Role of Artificial Intelligence in Combating Cyber Threats in Banking. International Engineering Journal For Research & Development, 4(1), 7-7.
32. Suleymanov, Q., Farzaliyev, M., & Nagiyev, M. (2019). The Effects of Innovations on Bank Performance: The Case of Electronic Banking Services. Recent Trends in Science and Technology Management, (2), 20-29.
33. Syaeid, T. A. (2019). The Effect of the Reliability of Accounting Information Systems on Electronic Disclosures on the Stock Prices: Applied Study on Industrial Companies Listed on Amman Stock Exchange. International Journal of Economics and Finance, 11(8), 1-14.)
34. Temelkov, Z. (2020). Differences between traditional bank model and fintech based digital bank and neobanks models. SocioBrains, International scientific refereed online journal with impact factor, (74), 8-15.
35. Udovita, P. V. M. V. D. (2020). Conceptual review on dimensions of digital transformation in modern era. *International Journal of Scientific and Research Publications*, *10*(2), 520-529.

36. Yip, A. W., & Bocken, N. M. (2018). Sustainable business model archetypes for the banking industry. *Journal of cleaner production*, *174*, 150-169.
37. McGrath, V., Sheedy, E., & Yu, F. (2022). Governance of cyber security.
38. Ashraf, M. (2020). *The role of market forces and regulation in disclosure: Evidence from cyber risk factors* (Doctoral dissertation, The University of Arizona).
39. Jin, J. (2015). Cybersecurity disclosure effectiveness on public companies.
40. More, D. M. M., & Nalawade, M. P. J. D. K. (2015). Online banking and cyber-attacks: the current scenario. *International Journal of Advanced Research in Computer Science and Software Engineering Research Paper*.
41. Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behaviour in e-Banking services. *International Journal of e-Education, e-Business, e-Management and e-Learning*, *7*(1), 70-78.
42. Maharjan, R., & Chatterjee, J. M. (2019). Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. *LBEF Research Journal of Science, Technology and Management*, *1*(1), 82-98.