Journal of Economic, Administrative and Legal Sciences
Volume (5), Issue (14): 30 Jul 2021
P: 1 - 24

AJSRP
ISSN: 2522- 3372

مجلة العلوم الاقتصادية والإدارية والقانونية
المجلد (5)، العدد (14): 30 يوليو 2021 م
ص: 1 - 24

The impact of financial cybercrimes on total quality standards according to Jordanian Islamic banks workers

Ala'a Hashem Tarbeh
University of Banking and Financial Sciences

Abstract: The study aimed to identify the impact of financial cybercrimes on total quality standards according to employees of Islamic banks in Jordan. Adopting the descriptive analysis method, and design a questionnaire was applied to a random sample of (293) employee, and the following results were reached:

1- According to Islamic banks employees, there is a negative impact of financial cybercrimes above mentioned.

2- There is a negative impact of infrastructure's targeting crime with software on the total quality standards.

3- There is a negative impact of the of payment's fraud crime represented by source misuse, and others misuse.

4- The Percentage of the impact of all cybercrime on the total quality standards in the banking sector to those working in Islamic banks in Jordan is medium.

And the study also concluded with several recommendations including work in to set up a banking system aimed at achieving information security in the banking sector to protect it from the risks of these crimes.

Keywords: financial cybercrimes, total quality standards, Jordanian Islamic banks.

أثر الجرائم المالية الإلكترونية على معايير الجودة الشاملة من وجهة نظر العاملين في البنوك الإسلامية الأردنية

آلاء هاشم طربيه
جامعة العلوم المالية والمصرفية|| المملكة الأردنية

المستخلص: هدفت الدراسة إلى تحديد أثر الجرائم المالية الإلكترونية على جودة المعايير الشاملة من وجهة نظر العاملين في البنوك الإسلامية في الأردن، بالاعتماد على المنهج الوصفي التحليلي، وصممت الباحثة استبانة طبقت على عينة عشوائية بلغ عددها (293) من الموظفين العاملين بها، وقد تم التوصل إلى النتائج التالية:

1- هناك تأثير سلبي للجرائم المالية الإلكترونية على معايير الجودة الشاملة من وجهة نظر العاملين في المصارف الإسلامية.

2- هناك تأثير سلبي لجريمة استهداف البنى التحتية بالبرمجيات على معايير الجودة الشاملة.

3- هناك تأثير سلبي لجريمة احتيالات الدفع متمثلة بإساءة استخدام المصدر وإساءة الغير على معايير الجودة الشاملة.

4- نسبة تأثير الجرائم على معايير الجودة الشاملة منخفضة، نسبة خطر الجرائم المالية الإلكترونية على القطاع المصرفي من وجهة نظر العاملين في المصارف الإسلامية في الأردن متوسطة. كما خلصت الدراسة إلى عدة توصيات منها العمل على وضع منظومة مصرفية تهدف إلى تحقيق الأمن المعلوماتي في القطاع المصرفي وحمايته من مخاطر هذه الجرائم.

الكلمات المفتاحية: الجرائم المالية الإلكترونية، معايير الجودة الشاملة، المصارف الإسلامية في الأردن.

مقدمة.

أسهم التطور الهام في مجال التقانة المصرفية في تيسير التعاملات المالية وشكل ركناً هاماً وأساسياً في الأداء المصرفي، وهو ما شجع الأفراد والمؤسسات على الإفادة من تلك الثورة التكنولوجيا مما ساهم في انتشارها عالمياً؛ وقد أفرز هذا الانتشار أنماطاً جديدة من الأخطار؛ فأصبح المتعاملون مع القطاع المصرفي والعاملون به عالمياً عرضة لأنواع مستحدثة من الجرائم المالية إلكترونية وضعتهم أمام تحديات وتهديدات مختلفة، وهو ما دفعهم إلى العمل من أجل المحافظة على معايير الجودة الشاملة وتحقيق أعلى مستوى من الأداء، وتحسين الإنتاجية وزيادة الربحية، للحفاظ على سمعة المؤسسة ومكانتها في ضوء مجموعة من المقومات والمعايير العالمية، ويعد القطاع المصرفي في الأردن كما نظائره عالمياً من المؤسسات المالية المعرضة إلى مخاطر الجرائم الإلكترونية وأثارها على جودة الأداء ومعاييره، ويشكل العاملون في القطاع المصرفي الإسلامي الأردني شريحة هامة لكونهم يعملون في مؤسسات لها معاييرها التي تميزها عن غيرها من المصارف، والتي تجعلها أكثر قدرة على مواجهة تلك الجرائم ذات الطبيعة الإلكترونية، وربما أكثر تعرضاً لتحدياتها، في ظل الانتشار المتزايد لتلك الجرائم وتنوعها وشدة المخاطر الناجمة عنها وتأثيرها على معايير الجودة الشاملة كان البحث الحالي محاولة من أجل تحديد شدة تلك الاخطار الناجمة عن الجرائم المالية الإلكترونية وأثرها على معايير الجودة الشاملة في القطاع المصرفي من وجهة نظر العاملين في النبوك الإسلامية في الأردن.

مشكلة البحث:

ساعدت ثورة الاتصالات والتطور الإلكتروني في تسهيل الخدمات في كافة ميادين الحياة، وقد شكل استخدامها في القطاع المصرفي نقلة نوعية بتوفير أداة الإلكترونية حديثة تسهم في خدمة الزبائن، وتغطي العمليات المصرفية التي تمثل مجموعة متنوعة من الخدمات التي تقدم من قبل النظام المصرفي باستخدام وسائط التكنولوجيا الإلكترونية المتنوعة (Gkoutzinis, 2006: 7). وقد اتسم الأداء المالي الإلكتروني بمزايا عدة جعلته أداة هامة توفر الوقت والجهد والتكلفة للبنوك والعملاء معاً، من خلال استخدام الشبكة العنكبوتية في التسويق والتنفيذ للخدمات البنكية التي تسهم في تحقيق التنافسية وبما يدعم العلاقة مع الزبائن، ويختصر المسافات ويسهم في تعزيز راس المال الفكري، وتوفير المزيد من فرص الاستثمار (بوراس، 2007: 204). ونظراً لكل تلك الميزات دأب القطاع المصرفي إلى اعتماد التقنيات الإلكترونية الحديثة لتوفير الخدمات المتجددة والمبتكرة، وحاول جاهداً مراعاة شروط الأمن والحفاظ على السرية والخصوصية في تعاملاته المالية الإلكترونية، ومع زيادة الاعتماد على الفضاء الإلكتروني في العمليات المالية، وبالرغم من كل المحاولات لضبط خصوصية العمل، فقد تعرض القطاع المصرفي في العديد من دول العالم إلى انتهاكات وجرائم إلكترونية، كجرائم الاختراق والربح غير المشروع والسلب والاحتيال والتي أثرت وبدرجات مختلفة على جودة عمله ونوعيه أداءه (المومني، 2008: 53). وهو ما وضع المصارف أمام تحديات العمل من أجل تقليل تلك المخاطر بكونها أصبحت واقعاً وما فرض عليها من مسؤوليات كبيرة لمواجهته من خلال وسائل الرقابة ووضع السياسات العملية المناسبة وهو ما صدر عام 1988 من توصية في أوروبا حيث نصت المادة 71 على أن العلاقة بين المصدر والمستهلك ترجع المسؤولية إلى البنك عن نتائج عدم التنفيذ والتنفيذ الخاطئ للعمليات المالية إذا تم تنفيذها من خلال جهاز إلكتروني خارج رقابة المصدر بشكل مباشر أو غير مباشر (غنام، 2006: 1010). وهو ودفع المسؤولين على القطاع المصرفي عالمياً إلى بذل المزيد من الجهود لمواكبة التطور التقني من جهة، وحماية سلامه بنيه المصارف الإلكترونية من جهة ثانية، حيث أصبحت البنوك أما تحدي جديد يضعها في حالة متابعة دائمة من أجل لحفاظ على معايير الجودة الشاملة في ضوء انتشار الجرائم المالية الإلكترونية (السلام، 2004: 181).

وتعد البنوك الإسلامية في العالم والأردن خاصةً من أهم بل وأكثر البنوك سعياً إلى المحافظة على معايير الجودة الشاملة، كما يعد العاملون بها من الموظفين ذوي الخبرات والكفاءات الهامة التي يمكن الاعتماد عليها تحديد طبيعة خطر الجرائم المالية الإلكترونية التي قد ترتكب قي القطاع المصرفي عموماً، وتأثيرها على معايير الجودة الشاملة في المصارف الإسلامية، وانطلاقاً مما سبق حددت المشكلة بالسؤال التالي: " ما أثر الجرائم المالية الإلكترونية على معايير الجودة الشاملة من وجهة نظر العاملين في النبوك الإسلامية الأردنية؟. ويتفرع عنه الأسئلة التالية:

1- ما نسبة خطورة الجرائم المالية الإلكترونية على القطاع المصرفي من وجهة نظر العاملين في البنوك الإسلامية في الأردن؟.
2- ما نسبة تأثر معايير الجودة الشاملة بالجرائم المالية الإلكترونية من وجهة نظر العاملين في البنوك الإسلامية في الأردن؟.

فرضيات البحث:

الفرضية الرئيسية: لا يوجد تأثير للجرائم المالية الإلكترونية على جودة المعايير الشاملة في من وجهة نظر العاملين بها في البنوك الإسلامية

يتفرع عنها الفرضيات التالية:

الفرضية الفرعية الأولى: لا يوجد تأثير لجرائم استهداف البنية التحتية على جودة المعايير الشاملة من وجهة نظر العاملين في البنوك الإسلامية.

الفرضية الفرعية الثانية: لا يوجد تأثير لجرائم احتيالات الدفع على جودة المعايير الشاملة من وجهة نظر العاملين بها في البنوك الإسلامية.

أهداف البحث:

1- تحديد نسبة تأثير الجرائم المالية الإلكترونية على معايير الجودة الشاملة في القطاع المصرفي من وجهة نظر العاملين في المصارف الإسلامية في الأردن.
2- تحديد نسبة خطورة الجرائم المالية الإلكترونية على القطاع المصرفي من وجهة نظر العاملين في البنوك الإسلامية في الأردن.
3- دراسة تأثير للجرائم المالية الإلكترونية على جودة المعايير الشاملة من وجهة نظر العاملين في البنوك الإسلامية.

أهمية البحث:

يعد تناول موضوع الجرائم المالية الإلكترونية في القطاع المصرفي من الموضوعات البحثية الجديدة والحديثة نسبياً، وتبرز أهمية الدراسة من تناولها كلاً من متغيري الجرائم المالية الإلكترونية ومعايير الجودة الشاملة، وأهمية تحديد أنواع تلك الجرائم والمخاطر المترتبة عليها وأثرها على معايير الجودة الشاملة من وجهة نظر العاملين في البنوك الإسلامية في الأردن ولاسيما مع تزايد استخدام التقانة في المعاملات المصرفية؛ في ضوء ما تطرّقت إليه الأدبيات حول أثر الجرائم المالية الإلكترونية على أداء القطاع المصرفي عموماً، وتأثر معايير الجودة الشاملة وخصوصية هذه المعايير في البنوك الإسلامية، بالإضافة إلى ندرة الدراسات السابقة التي تناولت كلا المتغيرين معاً سواء محلياً وعربياً وعالمياً، وأهمية النتائج التي يمكن أن يقدمها البحث لكل من العاملين في مجال القطاع المصرفي والمتعاملين معه، فضلاً عن أهمية التوصيات ودورها في تشجيع الباحثين للقيام بالمزيد من الدراسة حول دور معايير الجودة الشاملة في خفض الجرائم المالية الإلكترونية.

2- الإطار النظري والدراسات السابقة

أولاً- الإطار النظري:

معايير الجودة الشاملة:

شكلت نهايات القرن الماضي نقلة نوعية بظهور البنوك الإسلامية العربية والعالمية، ومركزية ودورها في تمويل الأنشطة والمشروعات الاقتصادية القائمة على المشاركة الاستثمارية (الغريب، 2001: 35). وقد تميزت المصارف الإسلامية بالتزامها بكل من المعايير الشرعية والاقتصادية والمالية، انطلاقاً من تعظيم دور الرقابة التشاركية مع الجمهور، حيث وضعت هيئة المحاسبة والمراجعة للمؤسسات المالية الإسلامية مجموعة من المعايير والاخلاقيات والضوابط الشرعية بلغ عددها (89) من معايير المحاسبية والشرعية (هيئة المحاسبة والمراجعة للمؤسسات المالية، 2012: 20). ويوفر المعيار مستوى متفق عليه لجودة الأداء المصرفي، باعتباره هدف أساسي لابد من تحقيقه، وتعد معرفة مدى تحقيق المعيار ومراجعته دليلاً على جودة الأداء، وذلك من أجل تحقيق الجودة الشاملة التي تجمع ما بين الاستراتيجية والتخطيط والأنشطة من خلال الالتزام العاملين بتحقيق رضا المتعاملين والمسؤولين والمشاركين بما يحقق توقعات العميل والمؤسسة معاً، بحيث تقلل الوقت والتكلفة في تلبية احتياجات العملاء، بما يضمن إخلاصهم، وتوفير مناخ يشجع ويدعم العمل بروح الفريق متطور بشكل دائم (الخطيب وغرايبة، 1998: 10).

وقد قدمت دراسة عويضة (2015) دليلاً ضمان جودة الأداء للمصارف الإسلامية " ويشتمل على معايير الجودة ومؤشرات الأداء لكل معيار أساليب تنفيذها، ووضع آلية تمثل انموذجاً لأدوات الرقابة المصرفية، وتزويد المؤسسات المصرفية الإسلامية بدليل يمثل خطة عمل لتطبيق معايير الجودة الشاملة، وقد حدد ضمن عدة مكونات وهي:

أولاً- المجال ويتضمن: (الموارد البشرية، الربحية الاقتصادية، القيادة المصرفية والتخطيط، الربحية الاجتماعية، الاشراف والرقابة).

ثانياً- الجانب ويتضمن: (الجانب الفني، المعتقدات والمهارات الفردية، جودة التفاعل والعلاقات، الانضباط، الاتجاهات نحو التدريب، المواد التدريبية، المؤسسة المصرفية كمؤسسة للتدريب، صيغ التمويل والاستثمارات، عمليات تحسين المؤسسة المصرفية، التسويق والهندسة المالية، كفاءة الأداء المصرفي التمويل الإنتاجي، الزكاة والصدقات والقرض الحسن وتنمية المجتمع المحلي، الدعم الفني من قبل جهات الرقابة، الرقابة الشرعية، صيغ التمويل والاستثمار، علاقات المصرف).

ثالثاً- معايير ضمان الجودة وهي: (معايير تتعلق بالموارد البشرية، معايير الربحية الاقتصادية، معايير الربحية الاجتماعية، معايير تتعلق بالانضباط الشرعي، معايير القيادة والتخطيط).

رابعاً- مؤشرات الأداء وسلوكيات الجودة وقد تكونت من خمسة مؤشرات؛ وقد قامت الباحثة باعتماد الدليل ومعايير للجودة الشاملة في البحث الحالي.

دور التطور التكنولوجي والتقانة في العمل المصرفي:

ساهم التطور التكنولوجي في إحداث تحولات جذرية في نمط وطبيعة العمل المصرفي، ووضعها أمام ضرورة الإفادة من أحدث التقنيات في المعلومات والاتصالات واستخدامها بكفاءة عالية في توفير خدمات مصرفية عالية الجودة ومبتكرة، وقد أوضحت بيرت كينج أن تأثير ودور التكنولوجيا سيظهر واضحاً علي سلوك العملاء ويؤدي إلى إحداث تغيرات جذري في منظومة الخدمات القطاع المصرفي، وإلى أن العقد القادم يتسم بظهور منظومة مختلفة

وجديدة بالكامل بناؤها تكنولوجيا الهاتف المحمول ستوفر خدمات مصرفية كبيرة وتعد الصيرفة الإلكترونية من أهم منتجاتها (فاضل، 2012). وبذلك أصبح ربط العمل المصرفي بشبكة الإنترنت واقعاً يحمل في طياته الكثير من الإيجابيات وينطوي على الكثير من السلبيات، وتعد المصارف الإسلامية من المؤسسات المواكبة لهذا التطور وما يحمله من ميزات تسهم في تحقيق التنافسية من خلال تحسين نوعية الخدمات المصرفية والعلاقة مع العملاء، أصبح تطبيق التكنولوجيا في البنوك الإسلامية ضرورة لتحديد شرائح العملاء وتصنيفهم لتقديم خدمات مصرفية منافسة لكل فئة وفق معايير جودة شاملة تعد الشريعة الإسلامية حد أركانها الأساسية (قاسم والعلي، 2012: 308). وجدير بالذكر أن تطبيق التكنولوجيا في القطاع المصرفي يحمل معه العديد من العوائق المتعلقة بالموارد البشرية والمعرفة ومهارة الاستخدام، وما يتطلبه الربط بين الخدمات المتنوعة التقليدية والإلكترونية وفق معايير العمل الخاصة بها (شايب، 2010: 57- 59). ما يجعلها عرضة كما غيرها من المؤسسات المالية إلى تحديات الأخطار المتعلقة باستخدام التكنولوجيا ومن أهمها الجرائم المالية الإلكترونية.

مخاطر الخدمات المصرفية الإلكترونية:

تواجه الخدمات المصرفية الإلكترونية عددًا من المخاطر تتطلب التعامل معها باهتمام وهي: 1- مخاطر التشغيل التي تتعلق بالاعتماد على التكنولوجيا الجديدة لتقديم الخدمات يجعل الأمن وتوافر النظام من المخاطر التشغيلية المركزية للخدمات المصرفية الإلكترونية. يمكن أن تأتي التهديدات الأمنية من داخل النظام أو خارجه، لذلك يجب على المنظمين والمشرفين المصرفيين التأكد من أن البنوك لديها ممارسات مناسبة مطبقة لضمان سرية البيانات، فضلاً عن سلامة النظام والبيانات (Kiragu, 2017: 20).2- مخاطر السمعة التي يمكن أن تؤدي انتهاكات الأمان وتعطيل توفر النظام إلى الإضرار بسمعة البنك. كلما زاد اعتماد البنك على قنوات التسليم الإلكترونية، زادت احتمالية مخاطر السمعة وهي من المشكلات التي تؤدي إلى فقدان ثقة العملاء في قنوات التسليم الإلكترونية ككل، أو النظر إلى إخفاقات البنوك على أنها أوجه قصور إشرافية على مستوى النظام، فمن المحتمل أن تؤثر هذه المشكلات على مقدمي الخدمات المصرفية الإلكترونية على العملاء الآخرين، ومن أجل إدارة مثل هذه المخاطر، يجب وضع تدابير لإلزام أعضاء مجلس الإدارة والإدارة العليا بتوثيق وشرح القرارات الاستراتيجية المتعلقة بكيفية تطوير البنوك لخدماتهم المصرفية الإلكترونية. ولابد أن يشمل الإشراف الإداري الموافقة على البنية التحتية وتوفير شروط التحكم الأمني المستمر؛ وحماية الأنظمة والبيانات المصرفية الإلكترونية من التهديدات الداخلية والخارجية (Carlson and Lang, 2001: 27). وتعد التحديات الأمنية للخدمات المصرفية الإلكترونية أكبر من تلك التي تواجهها الخدمات المصرفية التقليدية. يمكن معالجة هذه التحديات من خلال إنشاء امتيازات تسمح بإجراءات المتابعة والتدقيق للمعاملات المصرفية الإلكترونية، واتخاذ التدابير اللازمة من أجل الحفاظ على سرية المعلومات المصرفية الإلكترونية (Ombati et al, 2011: 158).

الجرائم المالية الإلكترونية:

يعد القطاع المالي عموماً والمصرفي خصوصاً من أكثر القطاعات تعرضاً لمخاطر الهجمات الإلكترونية على شبكة الإنترنت عالمياً. فقد حقق تقدم تكنولوجيا المعلومات والاتصالات على المستوى العالمي تأثيرًا كبيراً على كافة المجالات بما فيها المصرفية والمالية، ويعد الإنترنت أحد المجالات الأسرع نمواً لاعتماده على بنية تحتية تقنية متطورة. حيث أضحت تكنولوجيا المعلومات والاتصالات منتشرة وموجودة في كل مكان، وازداد الاتجاه نحو الرقمنة (Gercke, 2012: 43). وقد ترافقت هذه الثورة الرقمية مع تغير واضح في الأدوار المحورية للبنوك وأدخلتها إلى عالم جديد يحمل معه الكثير من الأخطار وأشكال محدثة للجرائم، وأصبح من الضروري جدا حماية هذه المؤسسات من تصرفات

المحتالين الغريبة (Okay & Ikechi, 2013: 259).وقد عرفت منظمة التعاون الاقتصادي والتنمية (OCDE) الجريمة المعلوماتية بأنها كل فعل أو امتناع من شأنه أن يشكل اعتداء على أموال مادية أو معنوية تكون نتيجة التدخل التقنية إلكترونية بشكل مباشر أو غير مباشر (رستم، 34: 1992). ويعرف MERWE ميروي الجريمة الإلكترونية بأنها كل فعل غير المشروع يدخل في ارتكابه الحاسب الآلي، وكل فعل إجرامي يركب باستخدام الحاسب الآلي كأداة له، وكل السلوكيات الاجرامية التي ترتكب باستخدام المعالجة الآلية للبيانات (الدسوقي، 2009: 351). والجريمة الإلكترونية هي كل نشاط إجرامي يستخدم جهاز كمبيوتر متصلاً بالشبكة العنكبوتية من قبل مجرمي الإنترنت بهدف جني الأموال ويتم من قبل أفراد مبتدئين أو منظمات احترافية وباستخدام تقنيات متطورة ومهارات فنية عالية (سارة، 2020).

أنواع الجرائم المالية الإلكترونية:

وتتضمن كل أشكال الاحتيال التي تتم عبر الإنترنت من خلال التصيد والهندسة الاجتماعية التي تستهدف المستخدمين من الأفراد والشركات مباشرة، وكما تشمل ما قد يقوم به الموظفون الفاسدون في المؤسسات المالية المختلفة بإدخال بيانات غير صحيحة وخاطئة واستغلال تعليمات أو عمليات غير مصرح بها، أو إجراء تعديلات أو حذف البيانات المحفوظة حول العملاء، أو إساءة المقصودة باستخدام حزم البرامج أو كتابة شفرات برمجية أو غيرها من أدوات النظام من أجل السرقة وبغرض الاحتيال (الخالد، 2018: 44).

التهديدات المتعلقة بالجرائم المالية الإلكترونية في القطاع المصرفي

أولاً- استهداف البنية التحتية ولها عدة أنواع وهي:

1. البرمجيات الخبيثة وتعطيل الخدمة بهدف عرقة لتشغيل الحاسب أو جمع المعلومات أو اقتحام أنظمة كمبيوتر ولها عدة مستويات خطورة تتراوح بين المزعج كما في الاعلانات والمدمر غير قابل للإصلاح كما في الفيروسات الخطيرة تستهدف المؤسسات المصرفية.
2. استغلال الثغرات: من خلال استغلال نقاط الضعف في البرمجيات والثغرات الأمنية المجهولة لمطور او العامة كما في حالات القرصنة بهدف احداث أضرار في الأنظمة البنكية الإلكترونية وهو ما يتطلب المتابعة الدائمة والمتطورة لاكتشاف الثغرات ومنع الهجمات الإلكترونية.
3. استهداف الهواتف الذكية مستغلين عدم معرفة المستخدمين لها للمخاطر الأمنية المتعلقة بها، واعتماد تطبيقات خبيثة أو قرصنة المعلومات المتعلقة بالحسابات الصرفية وتعطيلها، والاستدراج الإلكتروني من خلال الرسائل المزيفة وسرقة هوية الشخص وانتحال الشخصية بهدف السرقة (اللجنة العربية للرقابة المصرفية، 2017: 7-9).

ثانياً- جرائم احتيالات الدفع:

وهي جرائم الأموال الإلكترونية استخدام بطاقات ائتمان منتهية الصلاحية، أو بطاقات ملغاة، أو استخدام بطاقات مزورة أو مسروقة، وجرائم الاعتداء على أموال الغير باستخدام وسائل الإلكترونية، كدخول إلى حسابات العملاء ومواقع البنوك، والعبث بالبيانات من تحريف أو مسح بغرض نقلها أو اتلافها أو ومن أجل اختلاس الأموال، وانتهاكات من قبل أطراف خارجية غير مصرح لها بالدخول واجراء العمليات المصرفية (اللجنة الاقتصادية والاجتماعية لغربي أسيا الإسكوا، 2012: 12). ويمكن تحديدها ضمن أربعة أنواع وهي:

أولاً- إساءة استخدام صاحب العلاقة وذلك بإساءة الاستخدام خلال فترة الصلاحية كأن يتم السحب من رصيد غير موجود أو غير كاف، الوفاء بقيمة البضائع رغم عدم كفاية رصيد، وإساءة الاستخدام بطاقة منتهية الصلاحية في حالتي الوفاء وسحب النقود، إساءة استخدام بطاقة ملغاة في عمليتي السحب والوفاء، والامتناع عن رد البطاقة الملغاة للمصدر.

ثانياً- إساءة استخدام التاجر من خلال استعمال البطاقة الملغاة كما في تجاوزات بواسطة أجهزة دفع يدوية واعتماد ارقام بطاقات مزورة وتزوير توقيع العملاء على سندات المشتريات لم يحصلوا عليها وخصمها من بطاقة العميل، والتجاوزات التي قوم بها التجار بواسطة الجهاز الإلكتروني (P.O.S) بنسخ وطباعة بيانات على بطاقة أخرى والقيام بعمليات بيع وهمية دون علم صاحب البطاقة والاحتيال على البنك من خلال التلاعب بالجهاز الإلكتروني بعمليات البيع والتشغيل لبطاقات تم التبليغ عن سرقتها او ضياعها بعد العب بنظام التشغيل الخاص بها وصرف بطاقات دفع لا تحتوي على رصيد كافي بمبالغ نقدية صغيرة وقبول التعامل ببطاقات دفع مزورة والتلاعب بنظام التشغيل استغلالها لسحب مبالغ كبيرة.

ثالثاً- إساءة الاستخدام من قبل الغير سواء باستخدام غير مشروع لبطاقات مفقودة أو مسروقة كأداة للوفاء والسحب وحالات تزوير البطاقة من قبل الغير كما في تزوير بطاقة الدفع الإلكتروني في حال ضياعها أو سرقتها من قبل الآخرين واستعمال بطاقة الدفع الإلكتروني مزورة من طرف آخر غير معروف وسرقة بطاقة دفع إلكتروني ورقمها السري واستعمال بطاقة دفع إلكتروني مفقودة عثر عليها ولم يتم ارجاعها لصاحبها الشرعي او الجهة المصدرة لها.

رابعاً- إساءة استخدام المصدر كما في حالات تواطؤ موظفي البنك مع العميل كما في استخراج بطاقة ببيانات مزورة، أو مع التاجر والاستيلاء على أموال المعيل، أو تواطؤ موظف البنك مع الغير مع أفراد العصابات وتزويدهم بمعلومات حول حسابات الزبائن (معروف، 2015: 70- 74).

مكافحة الجرائم المالية الإلكترونية في القطاع المصرفي في الأردن:

أظهرت الإحصاءات مديرية الأمن الأردني تسجيل (3649) جريمة تتعلق بتقنية المعلومات في العام 2012م، منها (38) جريمة احتيال مالي إلكتروني ألقى القبض على (32) شخصاً بينهم اثنان من جنسيات اجنبية والباقي أردنيون (الصمادي، 2013: 2). وبعد إنشاء الجمعية الأردني للحد من جرائم المعلوماتية والإنترنت وبما ينسجم مع مبادئ الأمم المتحدة والقيم التي اكدها المؤتمر الثاني في القاهرة 2006، والمؤتمر الدولي لقانون الإنترنت في مصر 2011، (الشوابكة 2014: 143). كما أوضح الأردن في تقرير قدم للجمعية العامة للأمم المتحدة أهم التحديات المتعلقة بمكافحة استخدام تكنولوجيا المعلومات والاتصالات للأغراض الإجرامية متمثلة بوجود برمجيات خبيثة وبرامج مجانية تخفي هويات المستخدمين وتجعل من الصعب تعقبهم وكشفهم؛ وسهولة الحصول على المعلومات وتوفرها وإمكانية اكتساب المعرفة باستخدام الأدوات الإجرامية والخبرة في استخدامها من مواقع مجانية عديدة على مواقع الشبكة العالمية؛ بالإضافة إلى تواجد الشبكة الخفية، التي تشكل مرتعاً للأعمال غير المشروعة بما في ذلك استئجار أشخاص للقيام بعمليات القتل، وتجارة المخدِّرات، والإتجار بالأشخاص، واستغلال الأطفال، الأمر الذي يجعل عملية رصد هذه المواقع ومراقبتها مهمة صعبة، بسبب استخدام التشفير لمنع كشف هوية المستخدمين (الأمم المتحدة الجمعية العامة، 2018: 50). وقد أوضح الفريز محافظ البنك المركزي في الأردن إلى أهمية تفعيل وسائل الحماية من الجرائم الإلكترونية، من خلال إدارة المخاطر وتحديد موارد المعلومات والتهديد السبيراني المحتمل والعمل على توظيف أدوات وتقديم حلول مبتكرة لمواطن الضعف ضمن بيئة العمل. وأشار إلى أنه يتم إعداد فريق استجابة

للأحداث السيبرانية على مستوى القطاعين المالي والمصرفي من أجل تكثيف الجهود والاستثمار الأمثل للطاقات من أجل حماية الجهازين المالي والمصرفي من خلال التشاركية وتبادل المعلومات وتقديم الاستجابة السريعة من أجل كشف واحتواء أي تهديد، ذلك أن استغلال التكنولوجيا لتحقيق غايات جرمية يعد من أكثر الآثار السلبية على سلامة البنى التحتية للاتصالات والمعلومات ولاسيما في القطاع المصرفي (الفريز، 2017).

وتشير المادة رقم (6) من قانون جرائم أنظمة المعلومات الموقت رقم (30) للعام (2010) إلى أن كل من حصل قصدا دون تصريح عن طريق الشبكة المعلوماتية أو أي نظام معلومات على بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد على سنتين أو بغرامة لا تقل عن خمسمائة دينار ولا تزيد على ألفي دينار أو بكلتا هاتين العقوبتين. كما أن كل من استخدم عن طريق الشبكة المعلوماتية أو أي نظام معلومات قصداً دون سبب مشروع بيانات أو معلومات تتعلق ببطاقات الائتمان أو بالبيانات أو المعلومات التي تستخدم في تنفيذ المعاملات المالية أو المصرفية الإلكترونية للحصول لنفسه أو لغيره على بيانات أو معلومات أو أموال أو خدمات تخص الاخرين يعاقب بالحبس مدة لا تقل عن سنة وبغرامة لا تقل عن ألف دينار ولا تزيد على خمسة آلاف دينار (الصمادي، 2013: 7).

حماية أنظمة الدفع الإلكتروني والإجراءات الوقائية المتخذة من قبل البنوك

تسعى البنوك والمؤسسات المصرفية إلى توفير الحماية الكاملة لحسابات عملائهم بما يحقق الأمان ومنع الانتهاكات مما يعزز الثقة بينها وبين عملائها، وذلك باعتماد إجراءات بعضها رقابية وتتضمن الرقابة التوجيهية والداخلية والخارجية التي تحقق جودة العمل المصرفي وحل المشكلات التي تواجه الأداء المالي الإلكتروني والمخاطر المتعلقة به، بالإضافة إلى اتباع مجموعة من الإجراءات الإدارية من خلال تحديد عمليات سحب البطاقة في الوفاء والسحب والعمل على الحفاظ على حقوق العملاء من خلال سحب البطاقة من المصدر أو من التاجر وذلك من أجل مكافحة الجرائم المتعلقة بها، والمعارضة في قبول البطاقة في حال فقدانها أو سرقتها بهدف الحماية من الجرائم الإلكترونية وإساءة الاستخدام. كما تمثل الاجراءات التقنية أحد الوسائل الهامة في ضبط الجرائم المالية الإلكترونية لبطاقات الدفع من خلال من خلال استثمار كل المواصفات التقنية في الحواسيب والبطاقات لتجنب أي احتيالات كما في حالات خدمة الرسائل النصية القصيرة، وتوفير جدار الحماية والكلمات السرية المعقدة وكل ذلك بهدف ضمان حماية أنظمة الدفع الإلكترونية (بوقديرة، 2018: 50- 53).

ثانياً- الدراسات السابقة:

- **دراسة (F.Wada and G.O Odulaja, 2012)** بعنوان: " الأعمال المصرفية الإلكترونية والجرائم الإلكترونية في نيجيريا- منظور سياسي نظري حول الأسباب". بحث منشور في المجلة الافريقية للحوسبة في العام 2012، تناولت مشكلة الجرائم الإلكترونية في القطاع المصرفي النيجيري باعتماد المنهج الوصفي القائم على التحليل النظري للأدبيات والدراسات ذات الصلة منذ العام 1990 حتى العام 2010م، بهدف تقييم الجريمة الإلكترونية وتأثيرها على المؤسسات المصرفية في نيجيريا، وفحصت الأطر السياسية ومدى نجاح المؤسسات في مكافحة جرائم الفضاء الإلكتروني، وتوصلت إلى عدة نتائج أهمها توضيح طبيعة الجرائم الإلكترونية المصرفية في نيجيريا تلك التي تنطوي على أنشطة جنائية كما في حالات الاحتيالات على بطاقات الائتمان وأجهزة الصراف الالي، وسرقة البيانات والهوية الشخصية أو ما يعرف بالاصطياد القائم على الاحتيال وسرقة الهوية باستخدام تقنيات عالية يوجه نحو الافراد أو المؤسسات المشروعات التجارية ضمن ما يعرف بجريمة الهندسة الاجتماعية كما في حالات

الرسائل غير المرغوب بها، والتي تقع بهدف جمع المعلومات الخاصة واستخدامها ضد المؤسسات المالية، وقدمت الدراسة تفسير أسباب هذه الجرائم في ظل عدة توجهات أولها الجريمة كنشاط روتيني يظهر في حال توفر ثلاثة ظروف تسهل حدوثها وهي: وجود هدف مناسب وعدم توفر عنصر الأمن والدافع لارتكاب الجريمة متوفر، نظرية الفرصة التي توضح أن سبب ارتكاب الجريمة الإلكترونية هو توفر الفرصة المناسب لذلك، ثانيها: نظرية التكنولوجيا سبب حدث الجرائم هو ضعف استخدام عمليات الحماية وهندسة البرمجيات التي تحمي من المخاطر، ثالثها: النظرية الاجتماعية التي تتعلق بوعي ومستوى الوعي والرادع الأخلاقي لسلوك المستخدم والتي تسهم التوعية والتثقيف وتوضيح الإجراءات الأمنية دوراً في ضبطه، رابعها: نظرية الشرطة المجتمعية التي تؤكد على دور المواطنين في ردع الجريمة الجزئية والمكتملة من خلال وجود منظومة متكاملة من شرطة دولية متخصصة شرطة الإنترنت، خامسها نظرية انتقال الفضاء وهي تفسر أن ميل الافراد للسلوك الجرمي في الفضاء السبيراني لا يشبه ميلهم في الواقع المادي، وقد لا تظهر عليهم أي علامات إجرامية ولذلك من الصعب امكانية ضبطهم ذلك أنهم في الحياة الواقعية لا يظهرون ذلك (Wada.F and Odulaja.G.O, 2012: 69- 82.).

- **دراسة (Shewangu Dzomira, 2014)** بعنوان: " مخاطر الاحتيال الإلكتروني (الاحتيال السبيراني) على الصناعة المصرفية، زمبابوي"، بحث منشور في مجلة إدارة المخاطر في الأسواق المالية والمؤسسات في العام 2014، وتناولت مشكلة الاحتيال السبيراني ومخاطرة على الصناعة المصرفية في زمباوي، باعتماد المنهج الوصفي التحليلي، وتطبيق مقابلة منظمة على عينة مكونه من 22 من الموظفين في البنوك، وتطبيق استبيان على عينة من 57 من العاملين وذلك بهدف تحديد أشكال الجرائم الإلكترونية التي يتم ارتكابها في الصناعة المصرفية، والتحديات التي يتم مواجهتها لمكافحتها، وقد أظهرت النتائج أن أكثر أنواع الجرائم هي الاحتيال المحاسبي، واحتيالات تحويل الأموال وسرقة الهوية واستهداف الهاتف المحمول، وغسيل الأموال والاختلاس ومن ثم القرصنة والتصيد الاحتيالي وبرامج التجسس الخبيثة، وأكثر التحديات هي الفيروسات ونقص الموارد التكنولوجية التي تمكن من الكشف عنها، وعدم ملاءمة القوانين المتعلقة بالجرائم الإلكترونية، ونقص المعرفة في التعامل مع هذه الجرائم. وقد أوصت الدراسة بأهمية تطبيق الأمن السبيراني واشراك جميع أصحاب المصالح بحيث يتم حمالة الأنظمة التكنولوجية من الهجمات الإلكترونية(Dzomira, 2014: 19- 26).
- **دراسة (إبراهيم رمضان عطايا، 2015)** بعنوان: " الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، بحث منشور في مجلة كلية الشريعة القانون بطنطا في العام 2015م، تناول مشكلة الجريمة الإلكترونية ومواجهتها إسلامياً ودولياً، باعتماد المنهج الوصفي التحليلي والمنهج التاريخي بهدف تسليط الضوء مفهوم وخصائص ومظاهر الجريمة الإلكترونية وتعب مراحل وأساليب مواجهتها في الشريعة الإسلامية والأنظمة الدولية؛ باعتماد كل من المنهج الوصفي التحليلي والمنهج التاريخي. وقد توصل البحث إلى مجموعة من النتائج ومن أهمها، تتفرد الشريعة الإسلامية بمنهجها في مكافحة الجريمة ووسائل استئصالها من جذورها من خلال اتباع الأسلوب الوقائي، والأسلوب العلاجي، وأن من يرتكب الجريمة الإلكترونية قد يكون مكيف اجتماعيا وولديه قدرة مادية، وأن الدافع لارتكاب الجريمة في معظم الأحيان ينبع من رغبته في اثبات قدرته على قهر واختراق النظام، والتي قد تدفعه إلى الرغبة في الحصول على المال، في حين أن مرتكب الجريمة التقليدية غالباً يكون غير متكيف اجتماعيًا، ومحركة الرئيس هو الرغبة في الحصول على المال، وما زالت تتخذ الجرائم الإلكترونية أنماطا جديدة ومتطورة تعكس مستويات من الذكاء الإجرامي ما يجعلها تشك لخطراً وتحدياً حقيقياً، الجريمة الإلكترونية ذات بعد دولي وتتصف بأنها تتجاوز الحدود لكونها تتم عبر الشبكة المعلوماتية، وهو ما يضع عملية مكافحتها أمام تحديات قانونية إدارية فنية بل وسياسية بشأن لاسيما

فيما يتعلق بإجراءات الملاحقة الجنائية، وقدمت الدراسة عدة توصيات بعضها بتعلق باستخدام الإنترنت وتطوير الكفاءات بالتعامل مع مخاطره، وبعضها أسري يتعلق بدور الأسرة في حماية أفرادها من الوقوع بهذه المخاطر، وبعضها في محال التشريع دولياً ومحلياً بهدف مكافحة هذه الجرائم (عطايا، 2015: 361- 403).

- **دراسة (Teju Kujur, Mushtaq Ahmad Shah, 2015)** بعنوان: "الخدمات المصرفية الإلكترونية: قضايا الأثر والمخاطر والأمن". بحث منشور في المجلة الدولية لبحوث الهندسة والإدارة في العام 2015، وتناولت مشكلة مخاطر الخدمات المصرفية الإلكترونية وأثرها على الأمن المصرفي في الهند، باعتماد المنهج الوصفي القائم على تحليل الأدبيات والدراسات التي تناولت الموضوع بهدف تحديد توضيح طبيعة تأثير الخدمات المصرفية الإلكترونية على الأداء المصرفي من حيث المخاطر والتحديات الأمنية التي تجعل منها مصدراً قلق للعملاء، وإجراءات الأمن المصرفي التي تسهم في ثقة العميل بتلم الخدمات وبقاءه وزيادة العملاء المحتملين. وقد توصلت نتائج الدراسة إلى أن اتباع استراتيجية واضحة وشاملة تأخذ الاعتبار فوائد الخدمات المصرفي الإلكترونية ومخاطر استخدامها معاً، إجراء أبحاث تسهم في تبني الأنظمة الفعالية والقادرة على ضمان جودة العمل من خلال حملات التوعية، وأهمية تطوير كفاءة الموظفين والتدريب على إدارة المعلومات وفق صيغ معايير واضحة، واعتماد منهج استراتيجي وقائي لضمان أمن المعلومات من خلال تعزيز الاعتماد على كفاءات من الموارد البشرية الخبيرة والمتطورة، وفق متطلبات العمل من أدوات وأجهزة أمن مصرفي، والتدريب من أجل توفير القدرة على التعامل مع الحوادث المتعلقة بتجاوزات الإنترنت، وقدمت عدة توصيات منها أهمية تعزيز خدمات النبوك المصرفية وتزود العملاء بالكثير من الميزات والفوائد التي تدفعهم إلى التعامل بها في ظل توفر شروط الأمن الإلكتروني المصرفي وبم يضمن حماية مصالح العملاء والبنوك معاً (Kujur and Ahmad Shah, 2015: 207-212)
- **دراسة (خالد ممدوح العزي، 2017)** بعنوان: " الجرائم المالية الإلكترونية الجرائم المصرفية انموذجاً "، ورقة عمل مقدمة إلى مؤتمر الدولي الرابع عشر، طرابلس، لبنان، في العام 2017، تناول مشكلة الجرائم المالية الإلكترونية الدراسة، باعتماد المنهج الوصفي القائم على تحليل الأدبيات والدراسات السابقة، بهدف توضيح معنى الجرائم المالية الإلكترونية وأسبابها وأنواعها وأساليب انتشارها الجرائم المالية الإلكترونية، وتوضيح ما يعانيه القطاع المصرفي نتيجة تطور التقنية والتكنولوجيا، وقد توصلت النتائج إلى معالجة عدة جوانب متعلقة بالجرائم الإلكترونية منها الجرائم المالية وتأثيرها على الاقتصاد العالمي المرتبط بالعولمة، وتطور التقانة الإلكترونية في القطاع المصرفي وما أدت إليه من ظهور مفاهيم القرصنة والهاكر، توضيح الوسائل المتبعة في خرق الخصوصيات العامة والخاصة، والعمل على نشر ثقافة محاربة هذه الجرائم ومن يقوم بها من خلال تطوير برامج وتقنيات إلكترونية التي تحد من انتشارها، وتطبيق القوانين المحلية والدولية التي تسمح بملاحقة المنتهكين للأعمال المالية والاقتصادية، وقدمت عدة توصيات منها أهمية تطوير الأنظمة الأمنية لمراقبة التجاوزات التقنية والتأكيد على أهمية التدريب التأهيل للعاملين في المجال المصرفي لحمايته من تلك الجرائم (العزي، 2017: 1-16).

التعليق على الدراسات السابقة:

من خلال الاطلاع على الدراسات السابقة تبين معظمها اعتمد المنهج الوصفي القائم على تحليل الأدبيات حيث قدمت توضيحاً نظرياً وتاريخياً ومفاهيمياً حول موضوع الجرائم المالية الإلكترونية، في حين اعتمدت إحداها منهجاً وصفياً تحليلياً إجرائياً وقد توصل إلى نتائج هامة لكن على عينة صغيرة تمثل طبيعة وخصائص المجتمع الذي

تمثله، وتناولت متغير الجرائم الإلكترونية فقط وهو ما يتطلب المزيد من الدراسة على عدة ثقافات ومجتمعات، وبذلك اتفقت الدراسة الحالية معها من حيث اتباع المنهج الوصفي التحليلي لوجه نظر عينة ممثلة من العاملين في القطاع المصرفي في البنوك الإسلامية الأردنية، وتميزت بتناولها بالدراسة متغيري الجرائم المالية الإلكترونية لتحديد أكثرها خطورة وأثرها على معايير الجودة الشاملة وهو ما لم تتطرق إليه الدراسات السابقة.

3- منهجية الدراسة وإجراءاتها.

منهج البحث:

قامت الباحثة باعتماد المنهج الوصفيّ التحليليّ لكونه يعتمد على تفسير ووصف الظواهر في الوقت الحاضر، ويمكّن من توصيف معطيات الظروف وتحديد طبيعة ونمط العلاقات بين المتغيّرات المدروسة، واستثمار ما تم جمعه من بيانات وصفيّة حول الظاهرة والقيام بتحليلها وتفسيرها وفقاً لإجراءات القياس من أجل الوصول إلى النتائج المرجوة.

متغيرات البحث:

المتغيّرات المستقلّة: الجرائم المالية الإلكترونية في القطاع المصرفي

المتغيّرات التّابعة: معايير الجودة الشاملة في المصارف الإسلامية

مجتمع البحث وعينته:

حدد المجتمع الكلي للبحث تبعاً لإحصائيّات العام 2019، والمكون من أربعة نبوك الإسلامية موزعة على عشرة فروع. وقد بلغ عدد وإجمالي العاملين في البنوك الإسلامية (4341) ما نسبته (20، 20%) من عدد العاملين في البنوك الأردنية عموماً. (جمعية البنوك في الأردن، 2019). وقد تم سحب عينة عشوائية من البنوك والعاملين فيها بلغ عددها (293). وفيما يأتي عرض مفصّل للمجتمع الإحصائيّ والعينة.

الجدول (1) المجتمع الإحصائي والعينة ونسب التمثيل المئوية

البنوك الإسلامية	عدد الأفرع في الأردن	مجموع العاملين	النسبة الإجمالية لعدد العاملين %	عدد العينة	نسبة العينة إلى المجموع%
البنك الإسلامي الأردني	80	2440	56.20825	92	2.12
البنك العربي الدولي الإسلامي	45	980	22.57544	83	1.912
بنك صفوة الإسلامي	36	612	14.09813	62	1.428
مصرف الراجحي	10	309	7.118176	56	1.29
المجموع	171	4341	100	293	6.75

يتضح أن عدد أفراد المجتمع الإحصائي قد بلغ (4341) وعدد أفراد العينة (293) وبنسبة تمثيل بلغت (6، 75%)، وهي نسبة موثوقة.

خصائص العينة:

حُدّدت خصائص وصفات العينة تبعًا لثلاثة متغيّرات وهي: المؤهّل العلميّ، وسنوات الخبرة، والرّتبة الوظيفيّة، وفيما يأتي عرض لها:

جدول (2) خصائص العينة وفق المؤهل العلمي والرتبة الوظيفية والخبرة

		إدارة عليا	مدير إدارة	مدير مركز	رئيس فريق	موظف	المجموع
الرّتبة الوظيفيّة	العدد	0	20	62	68	143	293
	النسبة%	0	6.8	21.2	23.2	48.8	100
		دكتوراه	ماجستير	دبلوم	بكالوريوس	المجموع	
المؤهّل العلميّ	العدد	1	22	117	153	293	
	النسبة%	0.3	7.5	39.9	52.2	100	
		(1- 5)سنة	(6- 10)سنة	(11- 15)سنة	16 فما فوق سنة	المجموع	
سنوات الخبرة	العدد	54	72	90	77	293	
	النسبة%	18.4	24.6	30.7	26.3	100	

أدوات البحث:

بعد الاطلاع على الأدبيات قامت الباحثة ببناء استبانة لقياس وجهة نظر الأفراد الموظفين في المصارف الإسلامية في الأردن بتأثير الجرائم المالية الإلكترونية في القطاع المصرفي على معايير الجودة الشاملة، مكوّنة من (71) عبارة وتتناول محورين، المحور الأول: الجرائم المالية الإلكترونية الأكثر خطورة على القطاع المصرفي مكونه من (37) عبارة وموزعة على محورين وهما: 1- جائم استهداف البنية التحتية ولها ثلاثة أبعاد فرعية وهي: (1- برمجيات خبيثة، 2- استغلال الثغرات البرمجية، 3- استغلال هواتف ذكية)، 2- جرائم احتيالات الدفع ولها أربعة أباد فرعية وهي (1- إساءة أصحاب العلاقة، 2- إساءة المصدر، إساءة التاجر، إساءة الغير). المحور الثاني: لتحديد تأثير الجرائم المالية الإلكترونية على معايير الجودة الشاملة، وهو مكوّن من (34) عبارة موزعة على ستة أبعاد تمثلا معايير الجودة الشاملة في المصارف الإسلامية وهي: 1- معيار الموارد البشرية، 2- معيار كفاءة الأداء المصرفي، 3- معيار الربحية الاقتصادية، 4- معيار الربحية الاجتماعية، 5- معيار الرقابة والاشراف، 6- عيار الضوابط الشرعية، 7- القيادة المصرفية والتخطيط، وهي وفق ميزان خماسيّ: (كثيرة جداً خمس درجات، كثيرة أربع درجات، متوسطة ثلاث درجات، منخفضة درجتان، منخفضة جداً درجة واحدة). وقد أعدت الباحثة الأداة بعد الاطلاع على عدد من الأدبيات حول المتغيرات، وقد عرضت الاستبانة على محكّمين للتحقق من الصدق المنطقي. وقد انتهت بحذف بعض العبارات وتعديل صياغة بعضها وإضافة عبارات جديدة، ومن ثم طبقت الاستبانة على عدد من العاملين الموظفين في المصارف التجارية في الأردن بلغ عددهم (58) موظفًا؛ بهدف التحقق من الصدق والثبات وفيما يأتي عرض للنتائج:

أولاً- صدق الاستبانة:

أولاً- الصدق الارتباطات الداخلية البنيوي بين أبعاد الاستبانة:

أظهرت النتائج وجود معاملات ارتباط دالة إحصائيًّا بلغت (- 0، 438) بين المحاور المحورين، كما تبين أن قيم معاملات الارتباط بين الأبعاد في كل محور ودرجته الكلية دالة إحصائيًّا وقد تراوحت بين (0، 578 و0، 074) للجرائم المالية الإلكترونية بأبعادها، و (0، 520 و0، 869) لمعايير الجودة الشاملة؛ وبذلك يمكن القول إن الأداة بمحوريها تتمتع بالصدق البنيوي لاستخدامها في قياس المتغيران وهما الجرائم المالية الإلكترونية، ومعايير الجودة الشاملة.

ثانياً- ثبات الاستبانة:

ثانياً- 1- ثبات الاتساق الداخلي (ألفا كرونباخ):

تبين من معامل ألفا كرونباخ لكل من محوري الاستبانة الذي بلغ (0، 863) لمحور الجرائم المالية الإلكترونية، و (0، 941) لمحور معايير الجودو الشاملة أن الاستبانة تتمتع بمؤشرات الثبات لاعتماد نتائجها اللاحقة.

4- نتائج البحث ومناقشتها.

- **إجابة السؤال الأول: ما نسبة تأثر معايير الجودة الشاملة في القطاع المصرفي بالجرائم المالية الإلكترونية من وجهة نظر العاملين في المصارف الإسلامية في الأردن؟**

تم حساب النسبة المئوية لمتوسط درجات أفراد العينة في كل معيار من معايير الجودة الشاملة إلى مجموع المعايير الكلية وكانت النتاج كما يلي:

الجدول (3) النسبة المئوية لتأثير الجرائم المالية الإلكترونية على معايير الجودة الشاملة مرتبة تنازليا

معايير الجودة الشاملة	المتوسط	النسبة%	الوصف	الترتيب
معيار كفاءة الأداء المصرفي	28.24	14.805	منخفض	1
القيادة المصرفية والتخطيط	27.53	14.433	منخفض	2
الاشراف والرقابة	27.31	14.317	منخفض	3
معيار الموارد البشرية	27.24	14.281	منخفض	4
معيار الربحية الاقتصادية	27.15	14.233	منخفض	5
معيار الربحية الاجتماعية	26.95	14.128	منخفض	6
الضوابط الشرعية	26.33	13.803	منخفض	7
مجموع المعايير	190.75	100		

يتضح من الجدول أن النسب المئوية لتأثر معايير الجودة الشاملة بالجرائم المالية الإلكترونية منخفضة وتتراوح بين (14، 81% إلى 13، 80%)، ويمكن ترتيب معايير الجودة الشاملة الأكثر تأثراً بالجرائم الإلكترونية كما هو موضح وعلى التوالي: أعلاها لمعيار كفاءة الأداء المصرفي والذي يعد الأكثر تأثراً بالجرائم المالية الإلكترونية، ومن ثم القيادة المصرفية والتخطيط والاشراف والرقابة، ويليها معيار الموارد البشرية، ومن ثم معيار الربحية الاقتصادية، ومن ثم معيار الربحية الاجتماعية، في حين يعد معيار الضوابط الشرعية الأقل تأثراً بالجرائم المالية الإلكترونية.

- **إجابة السؤال الثاني: ما نسبة خطر الجرائم المالية الإلكترونية على القطاع المصرفي من وجهة نظر العاملين في البنوك الإسلامية في الأردن؟.**

تم حساب النسبة المئوية لخطر الجرائم المالية الإلكترونية على القطاع المصرفي وكانت النتائج كما يلي:

الجدول (4) النسبة المئوية لخطر الجرائم المالية الإلكترونية على القطاع المصرفي

الجرائم المالية الإلكترونية	المتوسط	النسبة%	الترتيب
احتيالات الدفع	30.62	51.08442	1
استهداف البنية التحتية	29.32	48.91558	2
المجموع الكلي	59.94	100	

يتضح من الجدول أن نسبة خطر الجرائم المالية الإلكترونية في القطاع المصرفي من وجهة نظر العاملين في المصارف الإسلامية في الأردن هي متوسطة بلغت (51، 084%) لجرائم احتيالات الدفع، و (48، 915%) لجرائم استهداف البنية التحتية. ولتحديد نسبة خطورة الجرائم المالية الإلكترونية المتعلقة باستهداف البنية التحتية الأكثر انتشاراً في القطاع المصرفي من وجهة نظر العاملين في البنوك الإسلامية أظهرت النتاج ما يلي:

الجدول (5) النسبة المئوية لخطر الجرائم الإلكترونية المتعلقة باستهداف البينة التحتية

جرائم البنية التحتية	المتوسط	النسبة%	الترتيب
برمجيات خبيثة	10.74	36.53	1
استغلال هواتف ذكية	10.6	36.15	2
استغلال ثغرات برمجية	8.04	27.32	3
استهداف البنية التحتية الكلي	29.32	100	

ويتبين أن الجرائم المتعلقة بالبنية التحتية الأكثر خطورة هي البرمجيات الخبيثة ومن ثم استغلال الهواتف الذكية وأقلها هو استغلال الثغرات. وهي نسب منخفضة تراوحت بين (36، 53% إلى 27، 32%). وقد حددت نسبة خطر جرائم احتيالات الدفع في القطاع المصرفي من وجهة نظرا لعملين في النبوك الإسلامية، وقد أظهرت النتاج ما يلي:

جدول (6) النسبة المئوية لخطر جرائم احتيالات الدفع في القطاع المصرفي

احتيالات الدفع	المتوسط	النسبة%	الترتيب
إساءة الغير	9.23	30.1437	1
إساءة استخدم صاحب البطاقة	8.64	28.21685	2
إساءة التاجر	8.24	26.91052	3
إساءة استخدم المصدر	4.51	14.72894	4
احتيالات الدفع	30.62	100	

يتضح أن نسبة خطر الجرائم المالية إلكترونية لأنواع احتيالات الدفع منخفضة فقد تراوحت بين (16، 022% إلى (36، 0414%) وأعلاها تلك الجرائم التي تتعلق بالغير كما في حالات القرصنة والسرقة، ومن ثم جرائم إساءة الاستخدام صاحب العلاقة، ومن ثم إساءة الاستخدام من قبل التاجر، وأقلها جرائم إساءة الاستخدام من المصدر والعاملين في البنوك.

وقد تم تحديد نسبة خطر جرائم احتيالات الدفع المتعلقة بصاحب العلاقة من وجهة نظر لعاملين في المصارف الإسلامية حيث تبين ما يلي:

الجدول (7) النسبة المئوية لخطر الجرائم المتعلقة بإساءة استخدام صاحب البطاقة

إساءة استخدام صاحب البطاقة	المتوسط	النسبة%	الترتيب
خلال فترة الصلاحية	3.41	38.968	1
خارج فترة الصلاحية	3.22	37.268	2
استخدام مقنع	2.01	23.264	3
اساءة استخدم صاحب البطاقة الكلي	8.64	100	

يتضح أن نسبة خطورة الجرائم ذات الصلة بإساءة استخدام صاحب العلاقة منخفضة بلغت (38، 968%) خلال فترة الصلاحية البطاقة، ومن ثم لسوء الاستخدام خارج فترة الصلاحية حيث بلغت (23، 264%)، وأدناها لجرام سوء الاستخدام لاحتيالات الاستخدام المقنع للبطاقة بلغت (37، 263%).

التحقق من فرضيات البحث:

- **الفرضية الرئيسية**: لا يوجد تأثير للجرائم المالية الإلكترونية على جودة المعايير الشاملة في البنوك الإسلامية من وجهة نظر العاملين بها.

من أجل التحقق من الفرضية تم اجراء تحليل الانحدار الخطي المتعدد التدريجي للجرائم المالية الإلكترونية التي تهدد القطاع المصرفي على متغير جودة المعايير الشاملة وقد أظهرت النتاج ما يلي:

الجدول (8) ملائمة نموذج التحليل انحدار المتعدد للجرائم المالية الإلكترونية على متغير معايير الجودة الشاملة

Model Summary [c]										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.196[a]	.038	.035	13.099	.038	11.644	1	291	.001	
2	.257[b]	.066	.060	12.932	.028	8.593	1	290	.004	.258
a. Predictors: (Constant), استهداف البنية. التحتية										
b. Predictors: (Constant), اس استهداف البنية. التحتية، احتيالات. الدفع										
c. Dependent Variable: معايير الجودة الشاملة										

يتضح أن قيم دوربين واتسون للارتباط الذاتي تشير إلى امكانية الثقة بالنموذج، ومعامل التحديد يظهر معنوية نموذج التحليل وأن جرائم استهداف البنى التحتية وجرائم احتيالات الدفع تفسر ما قدره (6، 6%) من التباين في معايير الجودة الشاملة. وقدمت متوسطات البواقي عدم وجود ارتباط فيما بينها وقد بلغت قيمتها الصفر، بالإضافة إلى نتائج تحليل التباين الأحادي والتي يوضحها الجدول التالي:

الجدول (9) تحليل التباين لقيم الجرائم المالية الإلكترونية على معايير الجودة الشاملة

ANOVA [a]								
Model		Sum of Squares	df	Mean Square	F	Sig.	Mean	Std. Deviation
1	Regression	1998.013	1	1998.013	11.644	.001[b]		
	Residual	49932.567	291	171.590			.000	12.832
	Total	51930.580	292				.000	1.000
2	Regression	3435.033	2	1717.517	10.271	.000[c]		
	Residual	48495.547	290	167.226				
	Total	51930.580	292					
3	Regression	1998.013	1	1998.013	11.644	.001[b]		
	Residual	49932.567	291	171.590				
	Total	51930.580	292					
a. Dependent Variable: معايير الجودة الشاملة								
b. Predictors: (Constant), استهداف البنية التحتية								
c. Predictors: (Constant), استهداف البنية التحتية احتيالات الدفع								

ويتضح من قيم F والاحتمال أصغر من 0، 05، إلى وجود تأثير دالّ إحصائيًا لقيم انحدار الجرائم المالية الإلكترونية ممثلة بجرائم البنية التحتية وجرائم احتيالات الدفع على معايير الجودة الشاملة من وجهة نظر العاملين بها في البنوك الإسلامية، وبذلك يمكن الوثوق بنموذج تحليل الانحدار المتعدد التدريجي.

الجدول (10) نتائج نموذج تحليل الانحدار لقيم الجرائم المالية الإلكترونية على معايير الجودة الشاملة

Coefficients [a]								
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	169.982	2.124		80.038	.000		
	استهداف البنية التحتية	-.231-	.068	-.196-	-3.412-	.001	1.000	1.000
2	(Constant)	188.538	6.668		28.274	.000		
	استهداف البنية التحتية	-.223-	.067	-.190-	-3.338-	.001	.998	1.002
	احتيالات الدفع	-.222-	.076	-.166-	-2.931-	.004	.998	1.002
a. Dependent Variable: معايير الجودة الشاملة								

يتضح أن قيم بيتا والقيم البائية وt- test والاحتمال أصغر من 0، 05، جميعها معنوية أي أن هناك تأثير المتغيرات المستقلة على المتغير التابع، وأن قيم الثابت للمتغيّر المستقلّ الجرائم الإلكترونية متمثلة باستهداف البنية التحتية واحتيالات الدفع معنوية ودالة احصائياً، بذلك نرفض الفرضية الصفرية ونقبل البديلة أي أن هناك تأثير سلبي لهذه الجرائم المالية الإلكترونية على معايير الجودة الشاملة من وجهة نظر العاملين في المصارف الإسلامية، أي كلما زادت الجرائم المالية الإلكترونية كلما انخفضت معايير الجودة الشاملة، ومنه يمكن التنبؤ بتأثر الجرائم الإلكترونية المحددة في نموذج الانحدار على معايير الجودة الشاملة وصياغة معادلة الانحدار كما يلي: معايير الجودة الشاملة = [188.538 + (.223- × استهداف البنية التحتية)+ (.222- × احتيالات الدفع)].

وبذلك يتضح أن معايير الجودة الشاملة تنخفض مع زيادة ارتكاب الجرائم المالية الإلكترونية المتعلقة باستهداف البنية التحتية متمثلة بالبرامج الخبيثة واستهداف الهواتف المحمولة واستغلال الثغرات، كما أن معايير الجودة الشاملة تنخفض مع زيادة ارتكاب جرائم الاحتيال متمثلة بإساءة استخدام صاحب العلاقة العميل، وإساءة استخدام المصدر البنك، إساءة استخدام التاجر، وإساءة استخدام الغير من خلال القرصنة والسرقة.

- **الفرضية الفرعية الأولى**: لا يوجد تأثير لأنواع جرائم استهداف البنية التحتية على جودة المعايير الشاملة في البنوك الإسلامية من وجهة نظر العاملين بها.

ومن خلال إجراء تحليل الانحدار المتعدد التدريجي لتحديد أي من الجرائم البنية التحتية هي الأكثر تأثيراً تم التوصل إلى النتائج التالية:

الجدول (11) ملاءمة نموذج التحليل الانحدار لجرائم المالية الإلكترونية على متغير معايير الجودة الشاملة

Model Summary [b]										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.200[a]	.040	.037	13.089	.040	12.138	1	291	.001	.244
a. Predictors: (Constant), البرمجيات خبيثة										
b. Dependent Variable: معايير الجودة الشاملة										

يتضح من الجدول أن أكثر أنواع جرائم استهداف البنى التحتية تأثيراً بجودة المعايير الشاملة هي البرمجيات الخبيثة، وأن قيم الارتباط الذاتي تقع ضمن المدى المقبول، وقيم معامل التحديد والتغيير جميعا دالة احصائياً، وأن ارتكاب جريمة استهداف البنى التحتية من خلال البرمجيات الخبيثة تفسر ما قدره (3، 7%) من التباين في معايير الجودة الشاملة.

كما أظهرت قيم متوسطات البواقي عدم وجود ارتباط فيما بينها وقد بلغت قيمتها الصفر، بالإضافة إلى نتائج تحليل التباين الأحادي والتي يوضحها الجدول التالي:

الجدول (12) يبين نتاج تحليل التباين لقيم جريمة البرمجيات الخبيثة على معايير الجودة الشاملة

ANOVA [a]								
Model		Sum of Squares	df	Mean Square	F	Sig.	Mean	Std. Deviation
1	Regression	2079.405	1	2079.405	12.138	163.22	2.669	
	Residual	49851.175	291	171.310			.000	13.066
	Total	51930.580	292					
a. Dependent Variable: معايير الجودة الشاملة								
b. Predictors: (Constant), برمجيات خبيثة								

تبين قيم F والاحتمال أصغر من 0، 05، وجود تأثير دالّ إحصائيًا لقيم انحدار الجرائم المالية الإلكترونية ممثلة بجريمة البنية التحتية البرمجيات الخبيثة على معايير الجودة الشاملة من وجهة نظر العاملين في البنوك الإسلامية، وبذلك يمكن الوثوق بنموذج تحليل الانحدار المتعدد التدريجي.

الجدول (13) نتائج نموذج تحليل الانحدار لقيم جريمة البرمجيات الخبيثة على معايير الجودة الشاملة

Coefficients [a]								
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	Constant)	170.118	2.122		80.167	.000		
	برمجيات خبيثة	-.650-	.187	-.200-	-3.484-	.001	1.000	1.000
a. Dependent Variable: معايير الجودة الشاملة								

يظهر الجدول أن قيم بيتا والقيم البائية وt- test والاحتمال أصغر من 0، 05، معنوية ودالة احصائياً، وقيم الثابت للمتغيّر المستقلّ جريمة استهداف البنى التحتية البرمجيات الخبيثة معنوية ودالة احصائياً، بذلك نرفض الفرضية الصفرية ونقبل البديلة أي أن هناك تأثير سلبي لهذه الجريمة استهداف البنى التحتية بالبرمجيات على معايير الجودة الشاملة، أي كلما زادت جرائم استهداف البنية التحتية البرمجيات الخبيثة كلما انخفضت معايير الجودة الشاملة، ومنه يمكن التنبؤ بتأثر الجرائم الإلكترونية المحددة في نموذج الانحدار على معايير الجودة الشاملة وصياغة معادلة الانحدار كما يلي: معايير الجودة الشاملة = [170.118 + (650. - × البرمجيات الخبيثة)]. وبذلك يتضح أن معايير الجودة الشاملة تنخفض مع زيادة ارتكاب الجرائم المالية الإلكترونية المتعلقة باستهداف البنية التحتية متمثلة بالبرامج الخبيثة من الفيروسات وأحصنة طروادة التي تخفي هوية المستخدم، وهجمات القرصنة للحرمان من الخدمة، وسرقة معلومات محددة من الحواسب المصرفية والشخصية.

- **الفرضية الفرعية الثانية**: لا يوجد تأثير لأنواع جرائم احتيالات الدفع على جودة المعايير الشاملة في البنوك الإسلامية من وجهة نظر العاملين بها.

ومن خلال اجراء تحليل الانحدار التدريجي المتعدد لتحديد أي من الجرائم احتيالات الدفع هي الأكثر تأثيراً تم التوصل إلى النتائج التالية:

الجدول (14) ملائمة نموذج التحليل الانحدار للجرائم المالية الإلكترونية على متغير معايير الجودة الشاملة

Model Summary[c]										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.146[a]	.021	.018	13.216	.021	6.321	1	291	.012	
2	.190[b]	.036	.029	13.139	.015	4.432	1	290	.036	.218
a. Predictors: (Constant), إساءة المصدر										
b. Predictors: (Constant), إساءة المصدر، إساءة الغير										
c. Dependent Variable: معايير الجودة الشاملة										

يضح من الجدول أن أكثر أنواع جرائم احتيالات الدفع تأثيراً بجودة المعايير الشاملة هي إساءة المصدر، وإساءة الغير وأن قيم الارتباط الذاتي تقع ضمن المدى المقبول، وقيم معامل التحديد والتغيير جميعا دالة احصائياً، وأن ارتكاب جريمة إساءة المصدر وإساءة الغير تفسر ما قدره (2، 9%) من التباين في معايير الجودة الشاملة. كما أظهرت نتائج قيم متوسطات البواقي عدم وجود ارتباط فيما بينها وقد بلغت قيمتها الصفر، بالإضافة إلى نتائج تحليل التباين الأحادي والتي يوضحها الجدول التالي:

الجدول (15) تحليل التباين قيم احتيالات الدفع على معايير الجودة الشاملة

ANOVA[a]								
Model		Sum of Squares	df	Mean Square	F	Sig.	Mean	Std. Deviation
1	Regression	1104.101	1	1104.101	6.321	.012[b]	163.22	2.530
	Residual	50826.480	291	174.661			.000	13.094
	Total	51930.580	292					
2	Regression	1869.120	2	934.560	5.414	.005[c]		
	Residual	50061.460	290	172.626				
	Total	51930.580	292					
a. Dependent Variable معايير الجودة الشاملة								
b. Predictors: (Constant), إساءة استخدام المصدر								
c. Predictors: (Constant), إساءة استخدم المصدر، إساءة الغير								

تبين قيم F والاحتمال أصغر من 0، 05، وجود تأثير دالّ إحصائيًا لقيم انحدار الجرائم المالية الإلكترونية ممثلة احتيالات الدفع متمثلة بإساءة استخدام المصدر وإساءة الغير على معايير الجودة الشاملة لأداء البنوك الإسلامية من وجهة نظر العاملين بها، وبذلك يمكن الوثوق بنموذج تحليل الانحدار المتعدد التدريجي.

الجدول (16) نتائج نموذج تحليل الانحدار لقيم جريمة احتيالات الدفع على معايير الجودة الشاملة

Coefficients [a]								
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	170.291	2.916		58.402	.000		
	إساءة استخدم المصدر	-.942	.375	-.146	-2.514	.012	1.000	1.000
2	(Constant)	178.791	4.970		35.971	.000		
	إساءة استخدم المصدر	-.857	.375	-.133	-2.286	.023	.988	1.012
	إساءة الغير	-.475	.226	-.122	-2.105	.036	.988	1.012
a. Dependent Variable: معايير الجودة الشاملة								

يظهر الجدول أن قيم بيتا والقيم البائية وt- test والاحتمال أصغر من 0، 05، معنوية ودالة احصائياً، وقيم الثابت للمتغيّر المستقلّ جريمة استهداف البنى التحتية البرمجيات الخبيثة معنوية ودالة احصائياً، بذلك نرفض الفرضية الصفرية ونقبل البديلة أي أن هناك تأثير سلبي لجريمة احتيالات الدفع متمثلة بإساءة استخدام المصدر وإساءة الغير على معايير الجودة الشاملة، أي كلما زادت احتيالات الدفع من حلال إساءة المصدر وإساءة الغير كلما انخفضت معايير الجودة الشاملة، ومنه يمكن التنبؤ بتأثر الجرائم الإلكترونية المحددة في نموذج الانحدار على معايير الجودة الشاملة وصياغة معادلة الانحدار كما يلي: معايير الجودة الشاملة = [178.791 + (857. - × إساءة استخدام المصدر) + (475. - × إساءة الغير)]

كما تظهر النتائج أن معايير الجودة الشاملة تنخفض مع زيادة ارتكاب الجرائم المالية الإلكترونية المتعلقة بإساءة استخدام المصدر كما في حالات تواطؤ موظفي البنك مع العميل كما في استخراج بطاقة ببيانات مزورة، تواطؤ موظف البنك مع التاجر والاستيلاء على أموال المعيل، تواطؤ موظف البنك مع الغير مع أفراد العصابات وتزويدهم بمعلومات حول حسابات الزبائن. وهي من أقل الجرائم ارتكاباً من وجهة العاملين في المصارف الإسلامية في الأردن نظراً لكون الأمانة المهنية من أهم شروط العمل فيها. وأن معايير الجودة الشاملة تنخفض مع زيادة ارتكاب الجرائم المالية الإلكترونية المتعلقة بإساءة الغير كما في حالات تزوير بطاقة الدفع الإلكتروني في حال ضياعها أو سرقتها من قبل الآخرين، استعمال بطاقة الدفع الإلكتروني مزورة من طرف آخر غير معروف، سرقة بطاقة دفع إلكتروني ورقمها السري، استعمال بطاقة دفع إلكتروني مفقودة عثر عليها ولم يتم ارجاعها لصاحبها الشرعي او الجهة المصدرة لها.

تفسير النتائج:

1. يوجد تأثير سلبي للجرائم المالية الإلكترونية على معايير الجودة الشاملة من وجهة نظر العاملين في المصارف الإسلامية الأردنية، وكلما زادت الجرائم المالية الإلكترونية كلما انخفضت معايير الجودة الشاملة، والتي يمكن التنبؤ بها، حيث يظهر التأثير السلبي لجريمة استهداف البنى التحتية بالبرمجيات على معايير الجودة الشاملة، وكلما زادت جرائم استهداف البنية التحتية البرمجيات الخبيثة كلما انخفضت معايير الجودة الشاملة، وتتفق هذه النتيجة مع نتائج دراسة العزي (2017) والتي أكدت إلى أن تطور التقانة الإلكترونية في القطاع المصرفي لعب دوراً في تطور مفاهيم القرصنة والهاكر التي ترمي إلى استهداف البنى التحتية، وتأكيد دور توضيح الوسائل المتبعة في ضبط خرق الخصوصيات العامة والخاصة ومكافحتها لخفض آثارها على كل من العملاء والبنوك.

2. هناك تأثير سلبي لجريمة احتيالات الدفع متمثلة بإساءة استخدام المصدر وإساءة الغير على معايير الجودة الشاملة، وكلما زادت احتيالات الدفع من إساءة المصدر وإساءة الغير كلما انخفضت معايير الجودة الشاملة، والتي يمكن التنبؤ بها، وتتفق هذه النتيجة نسبياً مع نتائج دراسة Kujur Ahmad Shah (2015) التي أكدت أهمية اعتماد منهج استراتيجي وقائي لضمان أمن المعلومات واتباع الإجراءات التي تضبط المخاطر والتحديات الأمنية التي تشكل مصدراً لقلق العملاء، وبما يسهم في ثقة العميل بتلك الخدمات واستمرار طلبها.
3. معايير الجودة الشاملة الأكثر تأثراً بالجرائم الإلكترونية هي وعلى التوالي أعلاها لمعيار كفاءة الأداء المصرفي والذي يعد الأكثر تأثراً بالجرائم المالية الإلكترونية، ومن ثم القيادة المصرفية والتخطيط والاشراف والرقابة، ويليها معيار الموارد البشرية، ومن ثم معيار الربحية الاقتصادية، ومن ثم معيار الربحية الاجتماعية، في حين يعد معيار الضوابط الشرعية الأقل تأثراً بالجرائم المالية الإلكترونية. وتتفق هذه النتيجة مع نتائج دراسة عطايا (2015) التي أكدت دور وتفرد الشريعة الإسلامية بمنهجها في مكافحة الجريمة والتزامها باستخدام كافة الوسائل لاستئصالها من جذورها من خلال اتباع الأسلوبين الوقائي والعلاجي وهذا ما يفسر أهمية معيار الضوابط الشعرية وكونه المعيار الأقل تأثراً بالجرائم المالية الإلكترونية والأكثر رسوخاً وثباتاً في العمل المصرفي الإسلامي.
4. نسبة خطر الجرائم المالية الإلكترونية في القطاع المصرفي من وجهة نظر العاملين في المصارف الإسلامية في الأردن هي متوسطة بلغت (51، 084%) لجرائم احتيالات الدفع وأعلاها تلك الجرائم التي تتعلق بالغير كما في حالات القرصنة والسرقة، ومن ثم جرائم إساءة الاستخدام صاحب العلاقة ومن ثم إساءة الاستخدام من قبل التاجر، وأقلها جرائم إساءة الاستخدام من المصدر والعاملين في البنوك، كما بلغت نسبة خطر لجرائم استهداف البنية التحتية (48، 915%)، وأكثر جرائم البنى التحتية خطورة هي الجرائم المتعلقة البرمجيات الخبيثة ومن ثم استغلال الهواتف الذكية واقلها هو استغلال الثغرات. وهي نسب منخفضة تراوحت بين (36، 53% إلى 27، 32%). وتتفق هذه النتيجة نسبياً مع ما ورد في تقرير موقع الأمن العام الاردني حول الجرائم المالية الإلكترونية وبكونها من الجرائم المنخفضة الحدوث وما أوضحه التقرير المقدمة من الأردن للأمم المتحدة حول التحديات في مواجهة هذا النوع من الجرائم بكون أهم تلك التحديات التي تتعلق بالبرمجيات الخبيثة وسهولة توفر الأدوات الاجرامية في شبكة خفية يصعب الوصول إلى المتخفين خلفها. وما أكده الفريز محافظ البنك المركزي إلى أن استغلال التكنولوجيا لتحقيق غايات جرمية يعد من أكثر الآثار السلبية على سلامة البنى التحتية للاتصالات والمعلومات ولاسيما في القطاع المصرفي، وتقترب هذه النتيجة مع نتائج دراسة Odulaja&Wada (2012) إلى أن أكثر الجرائم المالية الإلكترونية انتشاراً في نيجيريا تلك التي تتعلق بحالات الاحتيال الدفع وبطاقات الائتمان وكل ما يتعلق بها من سرقة الهوية الشخصية والهندسة الاجتماعية، وتتفق مع نتائج دراسة Dzomira (2012)التي أوضحت وتبعا لوجهة نظر العالمين في القطاع المصرفي في زمبابوي أن أكثر الجرائم المالية الإلكترونية انتشاراً هي الجرائم المتعلقة بالاحتيال المحاسبي وتحويل الأموال وسرقة الهوية واستهدفا البنى التحتية والهواتف المحمولة.

خاتمه:

ومما سبق وانطلاقاً من نتائج البحث وما عرض في الأدبيات والدراسات السابقة يتأكد أهمية توفر وتطبيق معايير الجودة الشاملة، ودورها في الحفاظ على جودة الأداء في ظل انتشار الجرائم المالية الإلكترونية، والعمل على ترسيخ منظومة حماية مصرفية متينة انطلاقاً من توفر وتطبيق معايير الجودة الأقل تأثراً بتلك الجرائم، وتقوية المعايير الأكثر تأثراً بما يضمن التقليل من آثارها وحماية المعاملات المالية لكل من العملاء والبنوك معاً.

أهم الاستنتاجات:

1. تفرز للجرائم المالية الإلكترونية متمثلة بجرائم استهداف البنى التحتية واحتيالات الدفع أثراً سلبياً واضحاً على معايير الجودة الشاملة من وجهة نظر العاملين في المصارف الإسلامية، وأكثر هذه المعايير تأثراً بالجرائم هي معايير كفاءة الأداء المصرفي.
2. نسبة خطر الجرائم المالية الإلكترونية من وجهة نظر العاملين في المصارف الإسلامية في الأردن متوسطة لكل من الجرائم استهداف البنى التحتية وجرائم احتيالات الدفع.
3. يشكل تطور تقانة المعلومات حاجة ضرورية لتحقيق تنافسية البنوك ورفع كفاءة أدائها مع توفر شروط الأمن المعلوماتي لضمان حماية أصحاب المصالح من العملاء والبنوك من أخطار الجرائم المالية الإلكترونية وآثارها المختلفة.

التوصيات والمقترحات.

بناء على نتائج البحث توصي الباحثة وتقترح ما يلي:

1- تأكيد دور العمل على معرفة وفهم آليات التخطيط والتنفيذ لمعايير الجودة الشاملة ودورها في ضبط عمليات الاحتيال المالي الإلكتروني.
2- تزويد العاملين في القطاع المصرفي بالمهارات اللازمة لمواجهة أي شكل من جرائم المالية الإلكترونية ولاسيما جرائم إساءة المصدر.
3- تطوير نظام أمن معلوماتي قادر على مكافحة الجرائم التي تستهدف البنية التحتية في البنوك وتحديداً الإسلامية.
4- التوعية المجتمعية بخطورة الجرائم المالية الإلكترونية على أصحاب العلاقة من الزبائن والبنوك وعامة المجتمع.
5- ترسيخ منظومة لحماية خصوصية البيانات المتداولة في المعاملات المالية الإلكترونية.
6- التأكيد على دور الأمن إلكتروني الدولي والعربي أو ما يسمى بشرطة الإنترنت، في متابعة التجاوزات المتعلقة بمنظومة المعاملات المالية وردعها وصولاً إلى منع حدوثها.

قائمة المراجع

أولاً- المراجع بالعربية

- أبو قديرة، خولة (2018). الجرائم الواقعة على بطاقات الدفع الإلكتروني، مذكرة مكملة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي أن البواقي كلية الحقوق والعلوم السياسية، الجزائر.
- بوراس، أحمد (2007). العمليات المصرفية الإلكترونية، بحث منشور في مجلة العلوم الإنسانية، العدد الحادي عشر، جامعة محمد خضير بسكيرة، الجزائر.
- الخالد، ساري محمد (2018). اتجاهات في أمن المعلومات وأمانها: أهمية تقنيات التعمية التشفير، كتاب، الطبعة الأولى، شركة العبيكان للتعليم، مكتبة الملك فهد الوطنية، المملكة العربية السعودية.
- الخطيب، فوزي وغرايبة، هشام (1998). جودة الخدمات المصرفي: توقعات عملاء البنوك في الأردن، بحث منشور في مجلة دراسات الأردنية للعلوم الإدارية، المجلد25، العدد1، المملكة الأردنية الهاشمية.

- الدسوقي، عطيه طارق إبراهيم (2009). الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، كتاب، الطبعة الأولى دار الجامعة الجديدة، الاسكندرية، مصر.
- رستم، هشام محمد فريد (1992). قانون العقوبات ومخاطر تقنية المعلومات، كتاب الطبعة الأولى، المجلد 1، مكتبة الآلات الكاتبة أسيوط، مصر.
- سارة، سمير (2020). كل ما تريد معرفته حول الجرائم الإلكترونية أو الجرائم المعلوماتية، موقع رؤية الإلكتروني، تكنولوجيا وتقنيات، 23 ديسمبر2020. تاريخ الاسترداد 2021/5/17. https: //www.alroeya.com
- الشايب، محمد (2010). المصارف الإسلامية وحتمية تبني التكنولوجيات الحديثة مقارنة بنظيرتها التقليدية، بحث منشور في مركز أبحاث فقه المعاملات الإسلامية، الثقافة الاقتصادية، العدد 28. تم الاسترداد بتاريخ 2021/5/20. https: //kantakji.com/tag/
- الشوابكة، محمد أمين أحمد (2014). جرائم الحاسوب والإنترنت /الجريمة المعلوماتية، كتاب، الطبعة الأولى، دار العلم للنشر والثقافة والتوزيع، عمان: الأردن.
- الصمادي، حازم (2013). الجرائم الإلكترونية في التشريع الأردني، النشرة القضائية الصادرة عن مجلس القضائي الأردني، المملكة الأردنية الهاشمية.
- عبد السلام، رضا (2004). اقتصاديات الجريمة – المحددات الاقتصادية للجريمة، بحث منشور في مجلة الحقوق، المجلد الأول، البحرين.
- العزي، خالد ممدوح (2017). الجرائم المالية الإلكترونية الجرائم المصرفية انموذجاً، ورقة عمل مقدمة إلى أعمال مؤتمر الدولي الرابع عشر، طرابلس: لبنان.
- عطايا، إبراهيم رمضان إبراهيم (2015). الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، مجلة كلية الشريعة القانون بطنطا، العدد 30، المجلد 3، طنطا: مصر.
- عويضة عدنان عبد الله محمد (2015). دليل ضمان جودة الأداء للمصارف الإسلامية، بحث منشور في مجلة جامعة الملك عبد العزيز: الاقتصاد الإسلامي، المجلد 28، العدد 3، المملكة العربية السعودية.
- الغريب، ناصر (2001). أصول المصرفية الإسلامية وقضايا التشغيل، كتاب، الطبعة الثانية، دار أبوللو للطباعة النشر، القاهرة.
- غنام، شريف محمد (2006). مسؤولية البنك عن أخطاء الكمبيوتر في النقل الإلكتروني للنقود، كتاب، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية: مصر.
- فاضل، جمل (2012). معامل التكنولوجيا تحصن البنوك في عصر اختفاء الديناصورات الصرفية، مقال منشور في جريدة الاهرام الاقتصادي، العدد 6، فبراير 2021. تم الاسترداد بتاريخ 2021/5/15. http: //digital.ahram.org.eg/articles.aspx?Serial=794598&eid=186
- الفريز، زياد (2017). توظيف أدوات وحلول الكشف المبكر للجريمة المالية في القطاع المصرفي العربي، مقال في منتدى الأمن السبيراني، عمان، اتحاد المصارف العربية. تم الاسترداد بتاريخ 2021/5/18. https: ///uabonline.org
- قاسم، عبد الرازق والعلي، أحمد (2012). أثر تقانة المعلومات في تطوير نظم عمليات المصارف العامة في سورية، بحث منشور في مجلة جامعة دمشق للعلوم الاقتصادية والقانونية – المجلد- 28 العدد الأول 2012، جامعة دمشق: سوريا.

- اللجنة الاقتصادية والاجتماعية بغربي أسيا الاسكوا (2012). بعض أنماط الجرائم المالية عبر الإنترنت، نشرة تكنولوجيا المعلومات والاتصالات للتنمية في المنطقة العربية الجرائم الإلكترونية، العدد 18، الأمم المتحدة نيويورك.
- اللجنة العربية للرقابة المصرفية (2017). سلامة وأمن المعلومات المصرفية الإلكترونية، أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية، تقرير، العدد رقم 72، صندوق النقد العربي أبو ظبي، الامارات العربية المتحدة.
- معروف، منية (2015). جرائم بطاقات الائتمان الإلكترونية، مذكرة تكميلية لنيل درجة الماستر شعبة الحقوق تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهدي أم البواقي، الجزائر.
- المومني، نهلا عبد القادر (2008). الجرائم الإلكترونية، كتاب، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن.
- هيئة المحاسبة والمراجعة للمؤسسات المالية (2012). معايير هيئة المراجعة والمحاسبة للمؤسسات المصرفية الإسلامية، تقرير، البحرين.

ثانياً- المراجع بالإنجليزية:

- Carlson, R. & Lang, E.E. (2001). Internet Banking: E- Banking Expansion and Regulatory Issues. Paper Research in Society of Government economists. Washington D.C
- Dzomira. Shewangu (2012). ELECTRONIC FRAUD (CYBER FRAUD) RISK IN THE BANKING INDUSTRY, Paper Research in ZIMBABWE, Risk governance & control: financial markets & institutions / Volume 4, Issue 2: 16- 26.
- Gercke, M. (2011), Understanding Cybercrime: A Guide for Developing Countries. ICT Applications and Cybersecurity Division. Policies and Strategies Department. ITU Telecommunications Development Sector 2nd Edition. www.itu.int/ITUD/cyb/cybersecurity/legislation.html
- Gkoutzinis, Apostolos (2006). Internet Banking and the Law in Europe, Cambridge University Press, UK.
- Ikechi, K.S. and Okay O.E. (2013), The Nature, Extent and Economic Impact of Fraud on Bank Deposits in Nigeria, Paper Research in Interdisciplinary Journal of Contemporary Research in Business, Vol. 4 No. 9, pp. 253- 265.
- Kiragu, Michael (2017). Effects of E- BANKING on the financial performance of Kenyan Banks, Unpublished master's thesis in the university of applied sciences Bachelor of Business Administration – International Business: 2- 60.
- Kujur, Teju and Ahmad Sha, Mushtaq (2015). Electronic Banking: Impact, Risk and Security Issues, Paper Research in International Journal of Engineering and Management Research, Volume- 5, Issue- 5: 207- 212.
- Ombati, R.B., Magutu, S.M., Nyamwange, N.K. & Nyaoga, P.O. (2011). Technology and Service Quality in the Banking Industry: Importance and performance of various factors considered in

Electronic Banking services. Paper Research in African Journal of Business & Management.1, 151 – 164.

- Wada.F and Odulaja.G.O (2012). Electronic Banking and Cyber Crime In Nigeria, Paper Research in A Theoretical Policy Perspective on Causation, . Afr J. of Comp & ICTs. Vol 5. No. 1. pp 69- 82.