EISSN: 3105-8019
ISSN: 2663-9610

# تأثير مخاطر أمن السلامة والسرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني*

أ.م.د. فؤاد احمد العفيري - أ.م.د. محمد حمود السمحي

واصل محمد حسن زياد

## المستخلص

هدفت هذه الدراسة إلى استكشاف تأثير مخاطر أمن السلامة والسرية المعلوماتية على النظام المحاسبي في البنك المركزي اليمني. واعتمدت الدراسة المنهج الوصفي التحليلي في جانبيها النظري والميداني، حيث تم تصميم أداة الدراسة، وهي الاستبانة، بالاستناد إلى الإطار النظري المستمد من الدراسات السابقة ذات الصلة. وقد استخدمت الاستبانة لجمع البيانات الأولية من مجتمع الدراسة - البنك المركزي اليمني - حيث تم توزيع (112) استبانة على عينة قصدية شملت المحاسبين والمراجعين الداخليين وموظفي إدارة تقنية المعلومات. أظهرت نتائج الدراسة أن مخاطر أمن السلامة المعلوماتية تؤثر بشكل واضح على النظم المحاسبية للبنك المركزي، نتيجة ضعف تأمين الأنظمة، وغياب إجراءات فعّالة للتحكم بدخول غير المختصين إلى إدارة تقنية المعلومات، خاصة العمال الذين يجب إخضاعهم للتفتيش الدوري، إضافة إلى استخدام برامج حماية غير مرخصة أو مقرصنة، كذلك أن مخاطر أمن السرية المعلوماتية تؤثر على النظم المحاسبية بسبب القصور في تدريب الموظفين بشكل مستمر على أهمية مواجهة مخاطر أمن المعلومات، وغياب تعليمات واضحة لإتلاف التقارير المستخرجة من الأنظمة بعد انتهاء الغرض منها.

الكلمات المفتاحية: مخاطر أمن السلامة، مخاطر أمن السرية، النظم المحاسبية الالكترونية.

* بحث مستل من رسالة ماجستير، محاسبة، الأكاديمية اليمنية للدراسات العليا، الجمهورية اليمنية.

EISSN: 3105-8019
ISSN: 2663-9610

المجلة العلمية للأكاديمية اليمنية للدراسات العليا
المجلد الخامس العدد الأول 2022

# The Impact of Information Security Risks on The Accounting Systems of The Central Bank of Yemen *

**Dr. Fua'ad A. Al-ofairi – Dr. Mohammed H. Al-Samhi**

**Wasel M. H. Ziad**

## Abstract

This study aimed to explore the impact of information security and confidentiality risks on the accounting system at the Central Bank of Yemen. The study adopted a descriptive and analytical approach in both its theoretical and field aspects. The study tool, a questionnaire, was designed based on a theoretical framework derived from previous relevant studies. The questionnaire was used to collect primary data from the study population—the Central Bank of Yemen—with (112) questionnaires distributed to a purposive sample of accountants, internal auditors, and IT department employees.

The study results showed the following:

-Information security risks clearly impact the Central Bank's accounting systems, as a result of weak system security, the absence of effective procedures to control the entry of non-specialists into the IT department, especially employees who must be subject to periodic inspection, and the use of unlicensed or pirated security software.

- Information security risks affect accounting systems due to the lack of continuous employee training on the importance of addressing information security risks, and the absence of clear instructions for destroying reports extracted from systems after their intended purpose has been served.

**Keywords: Safety Security Risks, Confidentiality Security Risks, Electronic Accounting Systems.**

EISSN: 3105-8019
ISSN: 2663-9610

المقدمة:

يشهد قطاع البنوك اليوم تغييرات كبيرة نتيجة التطور التقني السريع والاعتماد المتزايد على الأنظمة الإلكترونية في إدارة العمليات المالية والمحاسبية. ومع هذه التغيرات، ظهرت تحديات جديدة تتعلق بأمن المعلومات وحمايتها، خاصة فيما يخص السلامة والسرية، إذ أصبحت البيانات المحاسبية والمصرفية معرضة لمخاطر مثل الاختراق أو الضياع أو التلاعب، ما يجعل مسألة أمن المعلومات قضية أساسية تواجه المؤسسات المالية في الوقت الحالي.

وتُعد النظم المحاسبية من أكثر النظم حساسية وتأثرًا بهذه التحديات، نظرًا لطبيعة انشطتها المعلوماتية واعتمادها الكبير على البيانات وسريتها واستمرارية تدفقها داخل بيئة التشغيل الإلكتروني. فأي خلل في أمن المعلومات يمكن أن ينعكس بصورة مباشرة على التقارير المحاسبية وما يترتب عليه من انعكاسات في القرارات المالية المبنية عليها. كما أن ضعف ضوابط الحماية أو اختلال السلامة المعلوماتية وسريتها قد يؤدي إلى نتائج مالية وإدارية خطيرة تمس ثقة المتعاملين بالمؤسسة واستقرارها المالي.

وانطلاقًا من هذه المعطيات، يُعد البنك المركزي اليمني نموذجًا مهمًا لدراسة هذه الظاهرة، باعتباره الجهة المسؤولة عن الإشراف على النظام المالي والمصرفي في البلاد، والمعتمد بدرجة كبيرة على الأنظمة الإلكترونية في تسيير أعماله وإعداد تقاريره المالية والرقابية. ومن ثم فإن تعرض هذه الأنظمة لأي مخاطر متعلقة بأمن المعلومات يشكل تهديدًا مباشرًا للثقة في النظام المالي الوطني، الأمر الذي يفرض الحاجة إلى دراسة علمية متعمقة لتحديد حجم هذه المخاطر وآثارها وسبل الحد منها.

ومن هذا المنطلق، جاءت هذه الدراسة للنهوض بالتعرف على أثر مخاطر أمن المعلومات بمكونيها: السلامة والسرية، على النظم المحاسبية في البنك المركزي اليمني.

مشكلة الدراسة

تكمن مشكلة الدراسة في التحديات البنيوية التي تواجه النظم المحاسبية في بيئة التشغيل الإلكتروني بالبنك المركزي اليمني، نتيجة التحولات التقنية المتسارعة والاعتماد المتنامي على الأنظمة الإلكترونية، مما جعلها عرضة لمخاطر متعددة تمس أمن السلامة المعلوماتية وسريتها. وتشكل هذه المخاطر مصدر تهديد مباشر

EISSN: 3105-8019
ISSN: 2663-9610

لعمليات معالجة البيانات وتبادلها، بما يعكس تحديات جوهرية لمكونات النظم المحاسبية الضامنة لموثوقيتها في البنك المركزي اليمني، باعتباره الجهة المسؤولة عن إدارة السياسة النقدية والإشراف على استقرار القطاع المالي.

وتبرز مخاطر أمن السلامة المعلوماتية باعتبارها أحد المكونات الأساسية لضمان امن النظم، إذ تشمل احتمالات فقدان البيانات أو تلفها أو التلاعب بها نتيجة الأعطال الفنية أو الهجمات الإلكترونية أو القصور في إجراءات التشغيل والرقابة الداخلية بما ينعكس في ضعف منظومة السلامة المعلوماتية التي تمثل اساس قدرة البنك على اتخاذ القرارات الاستراتيجية.

وفي المقابل، تمثل مخاطر أمن السرية المعلوماتية بعدًا حاسمًا آخر في حماية النظم المحاسبية، إذ تتعلق بالحفاظ على سرية البيانات المحاسبية الحساسة ومنع الوصول غير المصرح به إليها أو استخدامها بصورة غير قانونية. وتكتسب هذه المخاطر أهمية استثنائية في بيئة البنك المركزي اليمني نظرًا لطبيعة المعلومات التي يتعامل معها، والتي تمس بصورة مباشرة استقرار النظام النقدي والثقة في القطاع المصرفي.

وبناءً على ما تقدم، تتضح إشكالية الدراسة في تحديد مدى تأثير مخاطر أمن السلامة والسرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني. ومن ثمّ، تتلخص مشكلة الدراسة في التساؤل الرئيس الآتي:

ما مدى تأثير مخاطر أمن السلامة والسرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني؟

ويتفرع عن هذا التساؤل الرئيس التساؤلان الفرعيان:

1. ما مدى تأثير مخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي اليمني؟
2. ما مدى تأثير مخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني؟

اهمية الدراسة:

الاهمية العلمية: تنبع من التأصيل العلمي لعلاقة مخاطر أمن المعلومات المتمثلة في السلامة والسرية بالنظم المحاسبية الالكترونية وتكوين الرؤية النظرية من خلال توجه سليم في اختيار المعلومات من المصادر العلمية واستخدامها استخدام أمثل يخدم موضوع الدراسة والدراسات الاخرى في نفس الموضوع.

EISSN: 3105-8019
ISSN: 2663-9610

الاهمية العملية: تنبع الاهمية العملية من خلال مراجعة الادبيات والدراسات الميدانية والتطبيقية في موضوع الدراسة لإضفاء الطابع العملي للدراسة من خلال ما توصلت اليه تلك الدراسات من نتائج تقارن في الوقت نفسه بهذه الدراسة لمعرفة حقيقة التطبيق ونتائجه.

أهداف الدراسة:

- إبراز تأثير مخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي اليمني.
- إظهار تأثير مخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني.

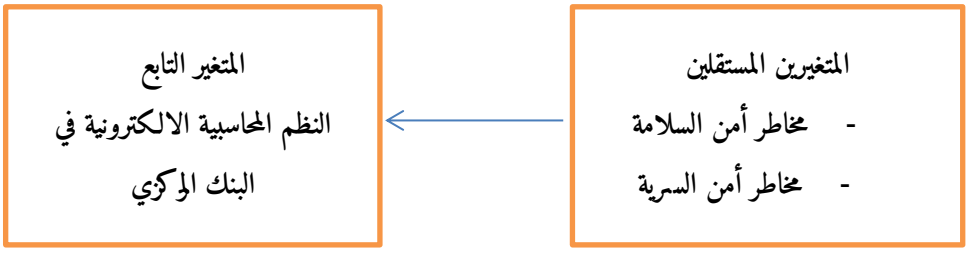
حدود الدراسة:

أولًا: الحدود الموضوعية: تركز الدراسة على تأثير مخاطر أمن المعلومات، خاصة تلك المتعلقة بالسلامة والسرية، على النظم المحاسبية في البنك المركزي اليمني، دون التطرق إلى النظم المصرفية الأخرى أو المؤسسات المالية الأخرى.

ثانيًا: الحدود المكانية والزمانية: تشمل الدراسة الفترة الزمنية التي تم خلالها جمع البيانات الأولية من الدراسة الميدانية التي اجريت في البنك المركزي اليمني والاستفادة من البيانات الثانوية المستمدة من الدراسات السابقة ذات الصلة، وتمتد حتى نهاية العام 2025م.

ثالثًا: الحدود المكانية: اقتصر نطاق الدراسة على البنك المركزي اليمني.

متغيرات الدراسة:



فرضيات الدراسة:

الفرضية الرئيسية لا يوجد تأثير ذو دلالة إحصائية لمخاطر أمن المعلومات على النظم المحاسبية في البنك المركزي اليمني، ومنها تم صياغة فرضيتي الدراسة الفرعيتين على النحو التالي:

- ليس هناك تأثير ذو دلالة إحصائية لمخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي.
- ليس هناك تأثير ذو دلالة إحصائية لمخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي.

تحليل الدراسات السابقة:

من خلال الاطلاع على الدراسات السابقة، أمكن التوصل إلى التحليل الآتي:

تشير دراسة **Abu-Musa (2004)** بعنوان "التعرّف على المخاطر الهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشآت السعودية" إلى أن الهدف الرئيس تمثل في تحديد أبرز المخاطر التي تواجه أمن نظم المعلومات المحاسبية الإلكترونية في تلك المنشآت. وقد أظهرت نتائج الدراسة أن نسبة كبيرة من المنشآت المشاركة في الاستقصاء قد تكبدت خسائر مالية ملموسة نتيجة التعديات على أمن نظم المعلومات المحاسبية، سواء من قبل أطراف داخلية (الموظفين) أو خارجية (قراصنة المعلومات). كما أوضحت الدراسة أن العديد من حالات التلاعب والاختلاس والتعدي على أمن النظم تم اكتشافها مصادفة بسبب ضعف الأدوات والضوابط الرقابية المطبقة. وأشارت كذلك إلى أن غالبية تلك الحالات تمت تسويتها داخليًا دون الإفصاح عنها حفاظًا على سمعة المنشآت وصورتها في السوق. وتوصلت النتائج إلى أن أبرز المخاطر التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية تمثلت في: الإدخال المتعمد أو غير المتعمد لبيانات خاطئة من قبل الموظفين، إدخال فيروسات إلى النظام المحاسبي، مشاركة كلمات المرور بين الموظفين، تدمير أو طمس مخرجات الحاسب الآلي، وتوجيه المعلومات إلى أشخاص غير مخولين بالاطلاع عليها. كما لم تظهر فروق جوهرية بين المنشآت المختلفة في تقديرها لأهمية تلك المخاطر في بيئة الأعمال السعودية.

أما دراسة **Kreicbera (2010)** بعنوان "التهديدات الداخلية لأمن المعلومات: التدابير المضادة والعنصر البشري"، فقد هدفت إلى دراسة دور العامل البشري في أمن نظم المعلومات من خلال التساؤل حول العوامل المؤثرة في السلوك الأمني للموظفين. وتوصلت الدراسة إلى أن رضا الموظفين وقبولهم للتدابير الأمنية يعدّان عنصرين أساسيين لتحقيق سلوك آمن تجاه نظم المعلومات. كما أوضحت أن الموظفين غالبًا ما يواجهون

EISSN: 3105-8019
ISSN: 2663-9610

صعوبة في فهم الوثائق المتعلقة بأمن المعلومات، وأن التطبيق الفعّال لتلك المتطلبات يحتاج إلى رفع مستوى الوعي الأمني. وأكدت أن أمن المعلومات يتأثر بالعادات والسلوكيات التي يتبناها العاملون داخل المؤسسات.

وجاءت دراسة غنية (2013) بعنوان "أمن المعلومات المحاسبية في ظل الأنظمة الإلكترونية"، وهدفت إلى التعرف على المخاطر التي تهدد أمن وسلامة نظم المعلومات المحاسبية الإلكترونية، والسياسات الرقابية وإجراءات الحماية المتبعة لمواجهتها في المؤسسات ذات الأنشطة المختلفة (التجارية، الخدمية، الصناعية). وقد توصلت الدراسة إلى أن الأنظمة المحاسبية الإلكترونية المستخدمة في المؤسسات الليبية تفتقر إلى الإجراءات الرقابية الفعالة، كما أظهرت ضعفًا في تطبيق أساليب الرقابة والحماية على نظم المعلومات.

أما دراسة الذنيبات (2015) بعنوان "مخاطر أمن المعلومات المحتملة في تطبيقات التعاملات الإلكترونية وأثرها في كفاءة نظام المعلومات"، فقد أجريت على موظفي المديرية العامة للجوازات في منطقة الطائف باستخدام استبانة شملت (82) موظفًا. وهدفت الدراسة إلى تحديد طبيعة المخاطر التي تهدد أمن التعاملات الإلكترونية ومدى تكرارها، إضافة إلى تقييم كفاءة نظام المعلومات في تنفيذ المعاملات الإلكترونية. وتوصلت النتائج إلى أن مستوى تكرار المخاطر الأمنية كان منخفضًا، وبالتالي لم يؤثر بشكل جوهري في كفاءة النظام. كما أظهرت النتائج أن الإجراءات الأمنية المتبعة قوية وفعالة، سواء كانت أدوات حماية برمجية أو مادية أو تنظيمية. وبيّنت أن أكثر المخاطر تكرارًا هي المخاطر الطبيعية مثل الانقطاع المفاجئ للكهرباء، بينما تمثل الأعطال الفنية أبرز المعوقات أمام كفاءة النظام. وخلصت الدراسة إلى أن نظام المعلومات يتمتع بمستوى أمني مقبول، وأن إدارة المخاطر تتبنى نهجًا يقوم على تقبّل مستوى المخاطر مع تعزيز وسائل الحماية.

وفي المقابل، جاءت دراسة Hossin & Ayedh (2016) بعنوان "مخاطر نظام المعلومات المحاسبي الإلكتروني في البنك المركزي الليبي"، وهدفت إلى التعرف على طبيعة المخاطر التي تهدد سرية نظم المعلومات ومعدلات تكرارها، وتحديد أسباب تلك المخاطر والأساليب الوقائية المعتمدة في البنوك للحد منها. وقد توصلت الدراسة إلى أن أبرز أسباب المخاطر تتمثل في قلة خبرة موظفي البنوك وضعف وعيهم بأمن المعلومات، إضافة إلى عدم كفاية الإجراءات وأساليب الحماية لمواجهة التهديدات التي تتعرض لها النظم المحاسبية الإلكترونية.

كما تناولت دراسة المحارب وسليمان (2017) بعنوان "واقع مخاطر أمن نظم المعلومات المحاسبية الإلكترونية في المصارف التجارية الليبية"، التعرف على طبيعة تلك المخاطر ومصادرها ومعدل تكرارها، وكذلك الإجراءات الوقائية المتبعة للحد منها. وقد استخدم الباحثان المنهج الوصفي التحليلي، ووزعت الاستبانات على (217) موظفًا في مصارف مدينة البيضاء. وتوصلت النتائج إلى وجود مخاطر متعلقة بعمليات إدخال البيانات وتشغيلها وإخراجها، إضافة إلى مخاطر بيئية متكررة مثل انقطاع التيار الكهربائي. كما أكدت الدراسة أن العاملين يمثلون أحد أهم مصادر المخاطر نتيجة ضعف الوعي أو الإهمال.

وفي دراسة Al-Sharairi et al. (2018) بعنوان "أثر مخاطر مدخلات نظام المعلومات المحاسبي على الرقابة الإدارية والرقابة المحاسبية والرقابة الداخلية في البنوك التجارية الأردنية"، هدفت الدراسة إلى تحديد أثر مخاطر مدخلات نظم المعلومات المحاسبية على أنظمة الرقابة في البنوك التجارية الأردنية. وأظهرت النتائج أن هناك تأثيرًا واضحًا لمخاطر نظم المعلومات الإلكترونية على الرقابة الإدارية والمحاسبية، حيث تبين أن الازدواجية في إدخال البيانات والتلاعب في المدخلات يؤثران سلبًا على توثيق العمليات وصحة القرارات الإدارية، كما أن الاستخدام غير المصرح به للنظام يضعف السيطرة الفعالة على أصول البنك.

أما دراسة Al-Fatlawi et al. (2021) بعنوان "دور تطبيق حوكمة تكنولوجيا المعلومات باستخدام إطار عمل COBIT5 في تحسين أمن أنظمة المعلومات المحاسبية"، فقد تناولت تطبيق مبادئ حوكمة تكنولوجيا المعلومات في مصرف التجارة العراقي (TBI)، وهدفت إلى تقييم مستوى تطبيق الحوكمة عبر أربعة أبعاد (التخطيط والتنظيم، الاستحواذ والتنفيذ، الدعم والتسليم، المراقبة). وتوصلت الدراسة إلى أن تطبيق إطار COBIT5 يسهم في تقليل مخاطر معالجة البيانات وتحسين أمن أنظمة المعلومات المحاسبية، كما أثبتت أن النظام المحاسبي في المصرف يحتوي على خصائص تضمن سرية معلومات العملاء وتمنع اختراق النظام، بما يعزز كفاءة وموثوقية النظم المحاسبية الآلية.

خلاصة التحليل:

يُلاحظ من مجمل الدراسات السابقة أن معظمها ركّز على تحديد طبيعة المخاطر التي تهدد أمن نظم المعلومات المحاسبية وتحليل مسبباتها وآثارها، مع تأكيد واضح على دور العامل البشري وضعف الوعي الأمني بوصفهما من أبرز مسببات تلك المخاطر. كما بينت الدراسات أن ضعف الضوابط الرقابية وعدم تفعيل إجراءات الحماية

EISSN: 3105-8019
ISSN: 2663-9610

المادية والبرمجية يؤديان إلى تهديد سلامة وسرية المعلومات المحاسبية. ويُلاحظ كذلك أن القليل من الدراسات تناولت هذا الموضوع في إطار مؤسسي مركزي كالبنك المركزي، مما يبرز أهمية الدراسة الحالية في سد هذا الفراغ البحثي عبر تحليل تأثير مخاطر أمن السلامة والسرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني.

الإطار المعرفي للدراسة:

أولًا: مخاطر أمن السلامة والسرية المعلوماتية:

ان نظام المعلومات يعاني من مخاطر التعديل في بيانات النظام دون علم المالك أو المستخدم ويمكن أن يكون هذا التعديل عرضياً، أو بفعل فاعل، وكما أن التهديد الآخر يمس سرية البيانات المخزونة على الوسائط المعلوماتية، يأتي من تعدد الحواسيب وارتباطها بالشبكات، والسلامة المعلوماتية تعني اتخاذ التدابير اللازمة لحماية المعلومات من التغير (الغشيرى، القحطاني،2009، صـ26).

وتعني سلامة المعلومات حماية البيانات من عمليات الحذف والتخريب، ويتم تأمين ذلك من خلال مجموعة من الأساليب التي توفرها نظم قواعد البيانات كقوائم الولوج والصلاحيات، بالإضافة إلى علاقات الترابط ما بين البيانات المخزنة فيها، ويتكون عنصر سلامة المعلومة من شقين: أحدهما: هو سلامة المعلومة، ويعني عدم تغيير المعلومات بشكل غير ملائم، سواء عن عمد أو عن غير عمد، والثاني: هو سلامة المصدر، وتعني الحصول على المعلومة من مصدرها الأصلي (الدنف،2013، ص47).

في حين أن سرية المعلومات تعني تأمين سرية البيانات المخزنة في النظام المحاسبي وخصوصيتها، ومنه إتاحة هذه البيانات فقط لأصحابها، إضافة إلى تأمين الطرق المناسبة لحمايتها من القراءة في أثناء نقلها عبر شبكة الاتصال، ويتحقق ذلك من خلال مجموعة من الطرق تقدم مستويات مختلفة من درجات الأمان وسرعة نقل المعلومات.

وقد عرف معهد المدققين الداخليين الأمريكيين" **Institute of Internal Auditor**" المخاطر أنها مفهوم يستخدم لقياس حالات عدم التأكد في عمليات التشغيل التي تؤثر على قدرة الوحدة في تحقيق أهدافها،

ويمكن أن يكون الأثر سلبياً، ويطلق عليه خطر/ تهديد، وإذا كان إيجابياً يطلق عليه فرص ( لظن ، 2016. صـــ42،43).

وفي ضوء المفاهيم السابقة يمكن تصنيف المخاطر في بيئة التشغيل الإلكتروني إلى خمسة أنواع موضحة كما يلي (الجبالي، ايهاب ،2007، ص 110-112): -

1. مخاطر تتعلق باختفاء السجلات، وهنا تصبح مشكلة البيانات المحاسبية غير مرتبة، إضافة إلى مشكلة فقدان تكامل البيانات نتيجة ضعف خطوط الاتصالات، أو وجود خلل في الذاكرة الرئيسة، وهنا يمكن التغلب عليها من خلال وضع الضوابط على صحة البيانات وتضمن عدم تغيير محتويات تلك البيانات.
2. مخاطر دليل سند المراجعة ويشمل عدم وجود المستندات الأصلية بعد الإدخال المبدئي، ودفاتر اليومية، حيث يتم الإدخال مباشرة لدفتر الأستاذ، وعدم إمكانية ملاحظة التتابع والتشغيل، حيث يتم ذلك داخل الحاسب الآلي، ويمكن معالجة هذه المخاطر من خلال المراجعة في ظل الحاسب الآلي والتشغيل الالكتروني للبيانات.
3. مخاطر ارتكاب الغش والسهو والتلاعب، والتي تتمثل في سهولة ارتكاب التلاعب، وذلك لقصور الرقابة على نظم الحاسبات وصعوبة اكتشاف وتتبع التلاعب، حيث يمكن ارتكابه دون ترك أثر ملموس يمكن متابعته، ويمكن التغلب على ذلك من خلال تصميم نظام رقابة جديد في بيئة التشغيل الكتروني.
4. مخاطر فيروسات الحاسبات، وتتمثل: في تدمير جزء من البرامج، بحيث لا يمكن استرداده، كما أن هناك فيروسات الكتابة على الملفات وإخفاء الفيروس ومضاعفتها، ويمكن التغلب على ذلك من خلال البرامج الرقابية للفيروسات.
5. مخاطر العاملين، وتتمثل في نقص الخبرة لدى العاملين في مجال التشغيل الإلكتروني، كما أن معظم مرتكبي حالات التلاعب للحسابات من داخل التنظيم وذلك لسبب ضعف إجراءات أساليب الرقابة الداخلية القائمة، وعدم الأخذ بالأساليب والنظم المتطورة وامكانية وصول بعض العاملين الذين تم استبعادهم من النظام وارتكاب حالات الغش والتلاعب أو نقل البرامج (الفيروسات)، لكونهم يعرفون كلمة السر.

EISSN: 3105-8019
ISSN: 2663-9610

واستناداً الى ما سبق فإنه يمكن القول أن هناك مجموعة من الصعوبات الإجرائية التي تساعد مرتكبي جرائم المعلومات بكل سهولة ويسر ولعل أهمها ما يلي: (حامد،2013، صـ16):

1. صعوبة إثبات وقوع عملية التهكير للمعلومات (السرقة).
2. صعوبة تحديد المسؤول عن هذا الفعل.
3. صعوبة إلحاق عقوبة الهكرز على المقيم في الخارج.
4. تنازع القوانين الجنائية من حيث المكان.
5. صعوبة التوصل إلى الهكرز.
6. القصور في القوانين التشريعية القائمة.
7. افتراض العلم بقوانين جميع دول العالم.

وسائل حماية أمن المعلومات:

1) الحاجز الناري: أحد الاحتياطات الأمنية الذي يحمي المعلومات ويمنع الوصول إليها، أو يضمن عدم إلحاق المستخدمين أي ضرر بنظم التشغيل الخاصة بالمعلومات، وهو نظام أمني لتنظيم حركة المرور عند نقاط الاتصال بين أي شبكتين عامتين، حيث يمنع مرور البيانات، معتمد على القواعد والتدابير التي يضعها مدير الشبكة مثل: كلمة السر، أو رقم المستخدم الذي يسمح للمستخدم بالدخول (عرب،2001، صـ 128، 129).
2) النسخ الاحتياطية: يجب عمل نسخ احتياطية للمعلومات، فحين تعرض النظام للتخريب يكون بالإمكان الرجوع إليها واستخدامها واستعادتها من البيانات الخاصة وغيرها، وتكمن أهمية النسخ الاحتياطية أنها تحمي من التعرض إلى الأخطار الفيزيائية والكوارث الطبيعية (ليان، 2004، صـ17).
3) التشفير: يقصد به استخدام منظومه تقنية وحسابية تستخدم مفاتيح خاصة لتحويل البيانات والمعلومات المقروءة الكترونياً، بحيث لا يمكن استخلاص هذه البيانات أو المعلومات الا عن طريق استخدام مفاتيح الشفرة (منصور، 2007، صـ 38). كما يقصد به أيضاً استخدام خوارزميات رياضية لتحويل البيانات إلى شكل غير مقرو وبشكل مباشر.

4) التوقيع الرقمي: يقصد به أن البيانات يتم الحاقها بوحدة البيانات للسماح لمستقبل وحدة البيانات أن يتأكد من أصل وحدة البيانات وتكاملها لغرض حمايتها من التزوير من قبل المستقبل.

5) التحكم بالوصول ويقصد به مجموعة من الإجراءات والآليات التي تحددها قوانين الوصول إلى الموارد (الناضري، 2005، ص ـ19-21).

ثانيًا النظم المحاسبية الالكترونية:

ينظر لنظام المعلومات المحاسبية أنه أحد النظم الفرعية في الوحدة الاقتصادية، والذي يتكون من عدة نظم فرعية متعددة تعمل مع بعضها البعض بصورة مترابطة ومتناسقة ومتبادلة بهدف توفير المعلومات التاريخية والحالية والمستقبلية، سواء المالية أو غير المالية لجميع الجهات التي يهمها أمر الوحدة الاقتصادية، وبما يخدم تحقيق أهدافها. وفي ضوء ذلك فقد عرفت النظم المحاسبية الالكترونية بأنها عبارة عن " مجموعة المكونات المتداخلة والإجراءات النمطية التي تعمل لتجميع المعلومات التي تحتاجها إليها المنظمة وتخزينها وتوزيعها ونشرها واسترجاعها، بهدف دعم العمليات والإدارة والتحليل والرقابة داخل المنظمة" (loundon, 2008 ,p ,12).

مكونات النظم المحاسبية الالكترونية:

تتكون النظم المحاسبية الرقمية من عدة مكونات رئيسية تعمل معًا لتسهيل إدارة العمليات المالية بشكل آلي وفعّال وهذه المكونات تشمل:( Ali & Muhammad،2021 243-221 pp )

1. وحدات إدخال البيانات: تسمح بإدخال البيانات المالية إلكترونيًا، سواء يدويًا أو من خلال التكامل مع أنظمة أخرى مثل أنظمة المبيعات أو المشتريات.
2. وحدات معالجة البيانات: تقوم بمعالجة البيانات وفقًا للقواعد المحاسبية، مثل تسجيل الإيرادات، المصروفات، والأصول، باستخدام خوارزميات وقواعد بيانات متقدمة.
3. وحدات تخزين البيانات: تخزن البيانات المالية في قواعد بيانات آمنة، سواء محلية أو سحابية، لتسهيل الوصول إليها واسترجاعها عند الحاجة.
4. وحدات إعداد التقارير: تتيح إعداد التقارير المالية مثل قوائم الدخل والميزانيات العمومية بشكل تلقائي، مما يوفر معلومات دقيقة وفي الوقت المناسب.

EISSN: 3105-8019
ISSN: 2663-9610

5. وحدات التحليل والتنبؤ: توفر أدوات تحليلية متقدمة تعتمد على الذكاء الاصطناعي لتحليل البيانات المالية وتوقع الاتجاهات المستقبلية.
6. وحدات الأمان والتحكم: تضمن حماية البيانات من الاختراقات عبر أنظمة التحقق من الهوية، التشفير، والنسخ الاحتياطي.
7. وحدات التكامل: تسمح للنظام بالتكامل مع أنظمة أخرى داخل المؤسسة) مثل إدارة الموارد البشرية أو المخزون (باستخدام واجهات برمجة التطبيقات (Aps).
8. وحدات واجهات المستخدم: توفر واجهات سهلة الاستخدام) مثل لوحات التحكم (وأدوات دعم فني لضمان تفاعل المستخدمين مع النظام بسلاسة.

خصائص النظم المحاسبية الالكترونية:

تتمثل خصائص النظم المحاسبية الالكترونية بالآتي: (Al-Hassani & Al-Jabri، 2021 ,116-97):

- السرعة: معالجة البيانات وإعداد التقارير بسرعة فائقة.
- الدقة: تقليل الأخطاء البشرية عبر التشغيل الآلي.
- المرونة: تكييف النظام مع احتياجات المؤسسات المختلفة.
- التكامل: الربط مع أنظمة أخرى) مثل إدارة المخزون أو الموارد البشرية).
- التقارير التلقائية: توليد تقارير مالية فورية وقابلة للتخصيص.
- الأمان العالي: حماية البيانات عبر التشفير والنسخ الاحتياطي.
- التحليل والتنبؤ: استخدام الذكاء الاصطناعي لتحليل البيانات وتوقع الاتجاهات.
- التخزين السحابي: الوصول إلى البيانات من أي مكان وفي أي وقت.
- خفض التكاليف: تقليل النفقات التشغيلية على المدى الطويل.
- التحديث التلقائي: تحسينات مستمرة دون تدخل يدوي.
- الشفافية: تسهيل تتبع المعاملات والتدقيق المالي.

التطورات التكنولوجية في المصارف:

تعتبر النظم المصرفية الرقمية جزءًا أساسيًا في تطور المصارف الحديثة. مع انتشار التكنولوجيا، تحولت العديد من المصارف إلى استخدام أنظمة محاسبية رقمية ونظم دفع إلكترونية. تتيح هذه الأنظمة للمصارف تحسين الكفاءة التشغيلية، تقليل التكاليف، وتعزيز الأمان المالي. كما سهلت العمليات المصرفية عبر الإنترنت وتحويل الأموال عبر التطبيقات المصرفية.

ولقد أصبحت تكنولوجيا المعلومات ضرورة من ضرورات عصرنا الحالي وأداة من أدوات العمل الرئيسية، بل وأصبحت أداة استراتيجية تسهل الوصول إلى الميزة التنافسية الدائمة، ونتيجة لهذه الطفرة الكبيرة التي حدثت ظهرت تحديات جديدة في وسائل الاتصالات وشبكات المعلومات والدخول في عصر العولمة والانترنت، ومنها مخاطر أمن المعلومات وهو ما يستدعي أخذ كافة الوسائل المتاحة أو الممكنة لتعزيز أمن نظم المعلومات وحمايتها في ظل توجهنا نحو اقتصاد قائم على الاتصال والبيانات الكبيرة وانترنت الأشياء. فالحكومات والشركات الكبيرة وحتى الشركات الصغيرة الحديثة الإنشاء أصبحت غير قادرة على تحمل تكلفة الاستثمار بالحلول غير المجدية لكشف ومعالجة تحديات أمن المعلومات، كما أصبح من الضروري بالنسبة لها أن تعي تأثير أمن المعلومات على استراتيجياتها لذلك فعلى البنك المركزي اليمني استخدام وسائل الحماية المتطورة لضمان أمن سلامة وسرية المعلومات وحمايتها من المخاطر وانعكاساتها على النظم المحاسبية المتمثلة في النظام المحاسبي ونظام الائتمان ونظام السوفت.

الدراسة الميدانية:

نبذة عن البنك المركزي اليمني:

شهد إنشاء البنك المركزي اليمني مراحل متعددة في الشمال والجنوب قبل الوحدة اليمنية عام 1990م. اكتملت التجربة في الشمال عام 1971م مع صدور القانون رقم (4) الذي أسس البنك، تزامنًا مع انضمام اليمن للبنك الدولي وصندوق النقد الدولي وازدهار النشاط الاقتصادي، مما استدعى وجود مؤسسة مصرفية مركزية لتنظيم العمل المصرفي وتحديد صلاحيات البنك ومسؤولياته.

EISSN: 3105-8019
ISSN: 2663-9610

وفي الجنوب، اختلفت التجربة نتيجة الاحتلال البريطاني، ومع رحيله وازدهار النشاط المصرفي في عدن، صدر القانون رقم (36) للعام 1972م لتنظيم النظام المصرفي، وأنشئ مصرف اليمن الجنوبي ليؤدي مهام البنك المركزي.

ومع الوحدة اليمنية في 22 مايو 1990م، تم دمج البنكين تحت اسم البنك المركزي اليمني، وأصدر القانون رقم (21) للعام 1991م، واستمر العمل به حتى صدور القانون رقم (11) للعام 2000م، مواكبًا التطورات الاقتصادية والمالية في البلاد (الجرادي، سلطان، 2000صـ 12-20).

انواع النظم في البنك المركزي:

- النظام المحاسبي
- نظام الائتمان المصرفي
- نظام السوفت

منهجية الدراسة:

اعتمدت الدراسة المنهج الوصفي التحليلي، نظراً لملاءمته لطبيعة البحث في جانبيه النظري والميداني. فقد تم الاستفادة من البيانات الثانوية المستمدة من الدراسات السابقة ذات الصلة بموضوع البحث لتكوين الإطار النظري، والذي شكل الأساس العلمي لتصميم استمارة الاستبيان.

كما تم جمع البيانات الأولية من مجتمع الدراسة الميدانية في البنك المركزي اليمني، وذلك لتحليل تأثير مخاطر أمن السلامة والسرية المعلوماتية على النظم المحاسبية.

مجتمع وعينة الدراسة:

تمثل مجتمع الدراسة في موظفي البنك المركزي اليمني. أما عينة الدراسة فقد تم اختيارها بأسلوب العينة القصدية، واشتملت على مديري النظم والمدققين الداخليين والمراقبين الماليين. وقد تم توزيع 112 استبانة على أفراد العينة، وتم استرجاعها بالكامل، ما يعكس تمثيلاً مناسباً ودقيقًا لمجتمع الدراسة. والجدول رقم (1) ادناه يوضح ذلك.

EISSN: 3105-8019
ISSN: 2663-9610

جدول رقم: (1) توزيع الاستبانات

| الرقم | اسم الفرع | عدد الاستبانات الموزعة | عدد الاستبانات المستردة | عدد الاستبانات الصالحة للتحليل | النسبة المئوية للاستبانات الصالحة للتحليل |
|---|---|---|---|---|---|
| 1 | المركز الرئيس | 72 | 72 | 72 | %100 |
| 2 | فرع ذمار | 20 | 20 | 20 | %100 |
| 3 | فرع البيضاء | 8 | 8 | 8 | %100 |
| 4 | فرع عدن | 12 | 12 | 12 | %100 |

- اساليب جمع المعلومات من مصدرين الاول المصادر الاولية المعتمدة على الاستبيان والذي يتضمن البيانات الديمغرافية لعينة الدراسة والثاني بيانات الدراسة. واما المصادر الثانوية فتم الاعتماد على المصادر والمراجع من المكتبات الالكترونية.
- درجة المقياس المعتمدة في الدراسة

تمثلت في درجات مقياس ليكرت الخماسي والمتوسط والوزن المقابل لكل درجة كما هو موضح في الجدول رقم (2).

الجدول رقم (2) درجات مقياس ليكرت الخماسي والمتوسط والوزن المقابل لكل درجة.

| الاستجابة | عالي جدا | عالي | متوسط | منخفض | منخفض جدا |
|---|---|---|---|---|---|
| الدرجة | 5 | 4 | 3 | 2 | 1 |
| المتوسط الحسابي | 4.2من -إلى5.00 | 3.40-4.19 | 2.60-3.39 | 1.80 2.59- | أقل من 180 |
| الوزن النسبي | %100 -%84 | %83.8-%68 | %67.8-%52 | %51.8 -36 | أقل من36% |

EISSN: 3105-8019
ISSN: 2663-9610

- الصدق الظاهري: خضعت الدراسة الى تحكيم علمي من قبل عشرة محكمين في مجال المحاسبة والاحصاء والاقتصاد.
- صدق الاتساق الداخلي: تم فيه استخدام معامل الارتباط بيرسون وكما يلي:-

جدول رقم (3) يوضح معامل الارتباط يبين درجات الارتباط بين درجات كل محور والدرجة الكلية.

| المحـــــــور | | تأثير مخاطر السلامة المعلوماتية على النظم المحاسبية | تأثير مخاطر السرية المعلوماتية على النظم المحاسبية | اجمالي المحاور |
|---|---|---|---|---|
| المقياس | معامل بيرسون | 0.857** | 0.929** | 0.857** |
| | مستوى الدلالة | 0.000 | 0.000 | 0.000 |

- ثبات اداة الدراسة: تم استخدام معامل الفا كرونباخ وكانت نتائجه في الجدول رقم (4) كما يلي:

جدول (4) معامل الفا كرونباخ.

| م | فقرات المحور | عدد الفقرات | معامل الثبات |
|---|---|---|---|
| 1 | السلامة المعلوماتية وتأثيرها على نظم المعلومات المحاسبية | 12 | 0.691 |
| 2 | السرية المعلوماتية وتأثيرها على نظم المعلومات المحاسبية | 9 | 0.999 |
| * | اجمالي المحاور | 21 | 0.882 |

- نتائج التحليل الوصفي لعينة الدراسة:

اولاً: - تحليل بيانات الدراسة بحسب التغيرات الديمغرافية كما هو موضح بالجدول رقم (5).

EISSN: 3105-8019
ISSN: 2663-9610
المجلة العلمية للأكاديمية اليمنية للدراسات العليا
المجلد الخامس العدد الأول 2022

جدول(5) نتائج تحليل بيانات الدراسة بحسب التغيرات الديمغرافية.

| المتغير | الفئـــــــــــــــــــة | التكرار | النسبة (%) | النسبة الاجمالية (%) |
|---|---|---|---|---|
| القطاع الذي تعمل فيه | قطاع الشئون المالية والإدارية | 30 | 26.8 | 43.8 |
| | قطاع المحاسبة والحاسب الآلي | 23 | 20.5 | 64.3 |
| | قطاع العمليات المصرفية المحلية | 40 | 35.7 | 100 |
| | أخر | 19 | 17 | 17 |
| | إجمالي | 112 | 100 | |
| | بكالوريوس | 72 | 64.3 | 64.3 |
| المستوى التعليمي | دبلوم عالي | 7 | 6.3 | 70.5 |
| | ماجستير | 28 | 25 | 95.5 |
| | أخر | 5 | 4.5 | 100 |
| | إجمالي | 112 | 100 | |
| | محاسبة | 45 | 40.2 | 40.2 |
| التخصص العلمي | إدارة | 16 | 14.3 | 54.5 |
| | تقنية معلومات | 28 | 25 | 79.5 |
| | أخر | 23 | 20.5 | 100 |
| | إجمالي | 112 | 100 | |
| | محاسب | 26 | 23.2 | 23.2 |
| الوظيفة | مراقب حسابات- مراجع | 35 | 31.3 | 54.5 |
| | تقنية حاسوب | 20 | 17.9 | 72.3 |
| | تشغيل | 20 | 17.9 | 72.3 |

EISSN: 3105-8019
ISSN: 2663-9610

| المتغير | الفئـــــــــــــــــــة | التكرار | النسبة (%) | النسبة الاجمالية (%) |
|---|---|---|---|---|
| | أخر | 31 | 27.7 | 27.7 |
| | إجمالي | 112 | 100 | 100 |
| | <5 | 1 | 0.9 | 0.9 |
| سنوات الخبرة | 6-10 | 26 | 23.2 | 24.1 |
| | 10-15 | 38 | 33.9 | 58 |
| | >15 | 47 | 42 | 100 |
| | إجمالي | 112 | 100 | |
| | 0 | 2 | 1.8 | 1.8 |
| الدورات التدريبية | دورة | 15 | 13.4 | 15.2 |
| | دورتين | 9 | 8 | 23.2 |
| | ثلاث فاكثر | 47 | 42 | 65.2 |
| | لاشي | 39 | 34.8 | 100 |
| | إجمالي | 112 | 100 | 100 |

من خلال النتائج الإحصائية الظاهرة في الجدول أعلاه تبين ان المتغيرات الديمغرافية كان لها تأثير كبير في فهم أفراد العينة لأسئلة الاستبيان والإجابة عليها بموضوعية، وذلك من خلال سنوات الخبرة في العمل المالي والمصرفي وكذا المؤهل العلمي، والتخصص العلمي، حيث تبين ان ما نسبته (83%) من أفراد العينة يتركزون في قطاع العمليات المصرفية المحلية واقطاع المحاسبة والحاسب الآلي والشؤون المالية والإدارية، وبينما شكلت ما نسبته (17%) في القطاعات الأخر ، كما انه تبين ان ما نسبته (79%) من أفراد العينة تخصصهم العلمي محاسبه وادره وتقنية معلومات، وبينما شكلت ما نسبته (11%) من التخصصات الأخرى كما انه تبين ان

EISSN: 3105-8019
ISSN: 2663-9610

ما نسبته (95%) من أفراد العينة يحملون مؤهلات بكالوريوس ودبلوم عالي وماجستير وبينما شكلت ما نسبته (5%) من حملة المؤهلات الآخر كما أنه تبين ان ما نسبته(91%) من أفراد العينة خبرتهم بين 6سنوات واكثر من 15 سنه وبينما شكلت ما نسبته (9%) خبرتهم في البنك أقل من 5 سنوات، كما أنه تبين ان ما نسبته (65%) من أفراد العينة لديهم دورات تدريبة بين دوه الي ثلاث دورات في مجال أمن المعلومات وبينما شكلت ما نسبته (35%) من موظفي البنك لا يوجد لديهم اي دورة في مجال أمن المعلومات حسب الجدول الموضحة أدناه:

ثانيًا: التحليل الوصفي لبيانات الدراسة:

1. نتائج تحليل مخاطر أمن السلامة:

جدول رقم(6): تأثير مخاطر أمن السلامة المعلوماتية على النظم المحاسبية

| One-Sample Test | | | | | | | |
|---|---|---|---|---|---|---|---|
| البيـــــــــــــان | Test Value = 3 | | | | | | |
| | t | درجة الحرية | المتوسط | الانحراف المعياري | مستوى الدلالة | الوزن النسبي | الترتيب | الاهمية النسبية |
| يتم القيام بحفظ النسخ الاحتياطية للبيانات المحاسبية في أماكن أمنة وبعيدة عن أماكن العمل وتحت الرقابة الثنائية | 11.638 | 110 | 4.11 | 1.003 | 000 | 0.822 | 1 | مرتفعة |

EISSN: 3105-8019
ISSN: 2663-9610

| One-Sample Test | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| البيـــــــــــــان | Test Value = 3 | | | | | | | |
| | t | درجة الحرية | المتوسط | الانحراف المعياري | مستوى الدلالة | الوزن النسبي | الترتيب | الاهمية النسبية |
| يمتلك البنك وسيلة مؤتمتة لحماية البيانات والبرامج لمحاسبية في الإدارة المعنية على سبيل المثال (برامج مكافحة الفيروسات) للحد من مخارطها | 4.894 | 110 | 3.5 | 1.086 | 0000 | 0.7 | 6 | متوسط |
| تتم متابعة الاصول وتقنية المعلومات المحاسبية للتأكد من سلامتها وجاهزيتها للعمل بصورة صحيحة | 5.296 | 110 | 3.55 | 1.093 | 000 | 0.71 | 5 | عالية |
| يقوم البنك بالتأمين على الانظمة المحاسبية المتوفرة لدية لضمان سلامتها جاهزيتها وعدم تعطيلها | 1.373 | 111 | 3.17 | 1.308 | 0.173 | 0.634 | 9 | متوسط |
| يمتلك البنك إجراءات خاصة تمنع غير المخولين من الدخول للنظم المحاسبية | 8.661 | 111 | 3.88 | 1.08 | 000 | 0.776 | 2 | مرتفع |

EISSN: 3105-8019
ISSN: 2663-9610
المجلة العلمية للأكاديمية اليمنية للدراسات العليا
المجلد الخامس العدد الأول 2022

| One-Sample Test | | | | | | | |
|---|---|---|---|---|---|---|---|
| البيـــــــــــــان | Test Value = 3 | | | | | | |
| | t | درجة الحرية | المتوسط | الانحراف المعياري | مستوى الدلالة | الوزن النسبي | الترتيب | الاهمية النسبية |
| يمتلك البنك تعليمات خاصة للحد من فساد المعلومات أو البرامج المحاسبية ومعالجة مشاكل الفيروسات | 2.594 | 111 | 3.29 | 1.166 | 0.011 | 0.658 | 8 | متوسط |
| يسمح لغير المختصين بالدخول إلى إدارة تقنية المعلومات أو اقسامها. | -1.850- | 111 | 2.79 | 1.226 | 0.067 | 0.558 | 10 | متوسط |
| يسمح فقط بالدخول لغرفة الحاسوب ( مركز البيانات) بعد الحصول على الموافقة المسبقة | 4.305 | 111 | 3.48 | 1.185 | 000 | 0.696 | 7 | عالية |
| يتم إخضاع عمال النظافة في تقنية المعلومات للرقابة المستمرة | -.325- | 110 | 2.96 | 1.167 | 0.746 | 0.592 | 10 | متوسط |

EISSN: 3105-8019
ISSN: 2663-9610

| One-Sample Test | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| البيـــــــــــــان | Test Value = 3 | | | | | | | |
| | t | درجة الحرية | المتوسط | الانحراف المعياري | مستوى الدلالة | الوزن النسبي | الترتيب | الاهمية النسبية |
| يتم إخضاع الانظمة المحاسبية الجديدة للتجربة بهدف التأكد من سلامتها وجاهزيتها ومدى فاعليتها | 6.575 | 111 | 3.68 | 1.092 | 000 | 0.736 | 4 | مرتفعة |
| يتم القيام بالرقابة على مخرجات الانظمة المحاسبية للتأكد من سلامتها ومدى فاعليتها وخلوها من الاخطاء | 7.112 | 110 | 3.7 | 1.041 | 000 | 0.74 | 3 | مرتفعة |
| يسمح بتثبيت البرامج المحاسبية المقرصنة وغير المرخصة | -3.923- | 110 | 2.51 | 1.306 | 000 | 0.502 | 12 | منخفضة |
| الإجمالي | 6.685 | 110 | 3.3851 | .60699 | 000 | .67702 | | متوسط |

يبين الجدول أعلاه تأثير مخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي وبصورة اجمالية حيث تراوحت المتوسطات الحسابية له بين (2.51-4.11) وبالمقارنة مع المتوسط الحسابي العام

للدراسة(افتراضي) وهو(3) لتأثير مخاطر أمن المعلومات على النظم المحاسبية في البنك المركزي حيث بلغ المتوسط الفعلي للدراسة 3.38 حيث جاءت الفقرة التي تنص على انه يتم القيام بحفظ النسخ الاحتياطية للبيانات المحاسبية في أماكن أمنة وبعيدة عن أماكن العمل وتحت الرقابة الثنائية في المرتبة الأولى بمتوسط حسابي (4.11) وانحراف معياري بلغ (1.003)وبوزن نسبي بلغ (0.822 ) وبالمقارنة مع المتوسط الحسابي العام والانحراف المعياري العام والوزن النسبي فقد حصلت الفقرة يسمح بتثبيت البرامج المحاسبية المقرصنة وغير المرخصة على المرتبة الأخيرة بمتوسط حسابي (2.51 ) وانحراف معياري بلغ (1.306) وبوزن نسبي بلغت (0.502) وبالمقارنة مع المتوسط الحسابي العام البالغ (3) والانحراف المعياري العام، حيث يتبين ان الانحراف المعياري والتشتت العالي.

اظهرت نتائج الدراسة أن المتوسطات الحسابية للفقرات رقم (11،10،5،1) ما بين( 3.55،4.11) وكذا الوزن النسبي لها واقع بين ( 0.822 -0.71 ) وكانت قيمة T المحسوبة واقعة بين (11.638-5.296 ) وعند مستوى دلالة بين (0.000-0.000)، وهذا يدل على عدم وجود مخاطر تتعلق بحفظ البيانات والمعلومات في النسخ الاحتياطية كونه يتم حفظها في أماكن آمنة وان هناك إجراءات تمنع غير المختصين من الدخول لنظم المعلومات متمثلة بالتشفير وإجراءات الحماية اللازمة كما انه يتم إخضاع الانظمة المحاسبية للتجربة قبل استخدامها وذلك من خلال بيئة تجريبه يتم عملها في النظم المحاسبية وعلية فلا يوجد مخاطر على النظم المحاسبية في البنك المركزي اليمني.

بينما الاجابة على الفقرات رقم ( 2، 4، 6،7)، والتي كانت متوسطاتها الحسابية واقعة بين ( 3.5-2.96) وبوزن نسبي بين (634-.592 ) وعند مستوى اختبار ل T. بقيمة بلغت ( 4.894-3.25 ) ومستوى دلالة من (0.000-0.746) ، وهذا يشير إلى ان أفراد العينة يميلون إلى الإفصاح عن وجود تأثير لمخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي بينما الاجابة على الفقرة رقم ( 12) والتي بلغ متوسطها الحسابي( 2.51) وبوزن نسبي بلغ ( 0.502) وعند مستوى دلالة ( 0.000) وعند مستوى اختبار T بنسبة ( 6.685) والذي يشير إلى وجود مخاطر عالية كون إدارة البنك تسمح بتثبيت البرامج المقرصنة وغير المرخصة والتي لها آثار على أنظمة المعلومات في البنك المركزي.

2- نتائج تحليل مخاطر أمن السرية:

EISSN: 3105-8019
ISSN: 2663-9610

الجدول (7) نتائج تأثير مخاطر أمن السرية المعلوماتية على النظم المحاسبية

| One-Sample Test | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| البيـــــــان | Test Value = 3 | | | | | | | |
| | t | المتوسط | الانحراف المعيارى | درجة الحرية | مستوى الدلالة | الوزن النسبي | الترتيب | الاهمية النسبية |
| يتم ادخال المعلومات المحاسبية بعد المصادقة عليها من المسؤول المباشر | 12.183 | 4.06 | 0.923 | 111 | 000 | 0.812 | 1 | مرتفعة |
| يتم تدريب الموظفين على مواجهة مخاطر نظم المعلومات بشكل مستمر | -1.690- | 2.81 | 1.174 | 111 | 0.094 | 0.562 | 8 | متوسط |
| يتم تشفير النسخ الاحتياطية للبيانات المحاسبية لتلافي مخاطر سرقتها أو تسريبها | 5.937 | 3.68 | 1.21 | 111 | 000 | 0.736 | 3 | مرتفعة |
| يمتلك البنك وحده مستقله لمتابعة التدابير اللازمة للحد من مخاطر سرية المعلومات المحاسبية | 0.64 | 3.08 | 1.336 | 110 | 0.524 | 0.616 | 7 | متوسط |

EISSN: 3105-8019
ISSN: 2663-9610
المجلة العلمية للأكاديمية اليمنية للدراسات العليا
المجلد الخامس العدد الأول 2022

| One-Sample Test | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| البيـــــــان | Test Value = 3 | | | | | | | |
| | t | المتوسط | الانحراف المعياري | درجة الحرية | مستوى الدلالة | الوزن النسبي | الترتيب | الاهمية النسبية |
| يشترك المختصين في السرية والموثوقية للمعلومات المحاسبية عند تحديث النظام بشكل مستمر | 4.264 | 3.46 | 1.13 | 111 | 000 | 0.692 | 5 | متوسط |
| هنالك مكان مخصص للنظم المحاسبية والشبكة وربط الأجهزة بحيث لا يسمح لغير المختصين للوصول اليها حفاظا على سريتها | 8.754 | 3.9 | 1.09 | 111 | 000 | 0.78 | 2 | مرتفعة |
| توجد تعليمات واضحة لا تلاف التقارير المستخرجة من النظم المحاسبية بعد انتفاء الغرض منها لضمان الحفاظ على سريتها | 1.466 | 3.18 | 1.289 | 111 | 0.145 | 0.636 | 6 | متوسط |

EISSN: 3105-8019
ISSN: 2663-9610

| One-Sample Test | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| البيـــــــان | Test Value = 3 | | | | | | | |
| | t | المتوسط | الانحراف المعيارى | درجة الحرية | مستوى الدلالة | الوزن النسبي | الترتيب | الاهمية النسبية |
| يمتلك البنك إجراءات وصلاحيات محدده لطباعة وتوزيع التقارير المحاسبية بما يضمن سريتها | 5.163 | 3.56 | 1.153 | 111 | 000 | 0.712 | 4 | متوسط |
| يمتلك البنك تعليمات واضحة لصلاحية الوصول للبيانات المحاسبية بحسب الاختصاص | 9.863 | 3.9 | 0.968 | 111 | 000 | 0.78 | 2 | عالية |
| الإجمالي | 6.313 | 3.5105 | .85193 | 111 | 000 | 0.7021 | | عالية |

حيث يشير الجدول أعلاه إلى تأثير مخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني وبصورة اجمالية حيث تراوحت المتوسطات الحسابية بين(2.81-4.06) وبالمقارنة مع المتوسط الحسابي العام لمخاطر السرية المعلوماتية وتأثيرها على النظم المحاسبية في البنك المركزي، حيث جاءت الفقرة التي تنص على انه يتم ادخال المعلومات المحاسبية بعد المصادقة عليها من المسؤول المباشر بالمرتبة الأولى وبمتوسط حسابي بلغ (4.06) وبمعدل انحراف معياري بلغ ( 0.923 ) وبوزن نسبي بلغ (812.) بينما جاءت الفره التي تنص على يتم تدريب الموظفين على مواجهة مخاطر نظم المعلومات بشكل مستمر في المرتبة الأخيرة وبمتوسط بلغ (2.81) وبمعدل انحراف معياري بلغ (1.174) وبوزن نسبي بلغ ( 0.562 ) ، وبالمقارنة

مع المتوسط الحسابي والانحراف المعياري العام والوزن النسبي، فقد تبين ان الانحراف المعياري والتشتت العالي عن الإجابة على تأثير مخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني على الرغم من بلوغه الدرجة العالية الا ان هناك مخاطر يواجهها البنك المركزي. في حين بلغت المتوسطات الحسابية للفقرات رقم (6، 9) ما بين (4.06، 3.9)، وكذا الوزن النسبي لها واقع بين (0.812- 0.78) وكانت قيمة T المحسوبة واقعة بين (8.754-9.863) وعند مستوى دلالة بين (0.000-0.000)، وهذا يدل على ان عدم وجود مخاطر تتعلق بالوصول إلى البيانات والمعلومات المحاسبية من قبل غير المختصين.

بينما الاجابة على الفقرات رقم (2، 4،5، 8،7)والذي كانت متوسطاتها الحسابية واقعة بين (6 3.5- 2.81) وبوزن نسبي بين (5.62.-3.56) وعند مستوى اختبار لT عند نسبة (1.69-8.754.) ومستوى دلالة من (0.524-000.) وهذا يشير إلى أن أفراد العينة يميلون إلى الافصاح عن وجود تأثير لمخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي ؛ لكونه يشترك أكثر من موظف في كلمة السر الواحدة وانه لا يوجد تعليمات لإتلاف التقارير المستخرجة من النظم المحاسبية بعد إنهاء الغرض منها ، وغيرها وهذا فيه مخاطر على أمن سرية المعلومات المحاسبية في البنك المركزي.

## نتائج اختبار الفرضيات:

### الفرضية الاولى الفرعية:

تم استخدام اختبار (T) لعينة واحده للتحقق من تأثير مخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي، وقد كانت نتيجة اختبار (T) للتحقق من انه ليس هناك تأثير لمخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي اليمني" كما في الجدول.

EISSN: 3105-8019
ISSN: 2663-9610

الجدول (8) نتائج اختبار الفرضية الفرعية الاولى

| One-Sample Test 100 | | | | | | | |
|---|---|---|---|---|---|---|---|
| البيان | Test Value = 100 | | | | | | |
| | المتوسط الحسابي | الانحراف المعياري | T المحسوبه | T الجدولية | Df درجة الحرية | Sig. (2-tailed) مستوى الدلالة | الوزن النسبي |
| متوسط المحور الأول | 3.3851 | 0.60699 | 6.685 | 1.645 | 110 | 0.000 | 0.67702 |

يتضح من الجدول رقم (8) ان قيمة (T) المحسوبة بلغت 6.685 وهي دالة عند مستوى (a<=0.05)، وبالمقارنة مع قيمةT الجدولية البالغة 1.645 وهذا يؤكد عدم قبول الفرضية العدمية الأولى وقبول الفرضية البديلة التي تنص على:

"هناك تأثير لمخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي اليمني": يعزى ذلك إلى عدم إخضاع عمال النظافة للتفتيش المستمر، كما انه يسمح بتثبيت البرامج المقرصنة وغير المرخصة؛ التي فيها مخاطر عالية على سلامة المعلومات المحاسبية كما انه يسمح بالدخول إلى مركز تقنية المعلومات.

نتائج اختبار الفرضية الفرعية الثانية

تم استخدام اختبار (T) لعينة واحدة للتحقق من تأثير مخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني، وقد كانت نتيجة اختبار (T) للتحقق من أن ليس هناك تأثير لمخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني"

كما في الجدول التالي.

EISSN: 3105-8019
ISSN: 2663-9610
المجلة العلمية للأكاديمية اليمنية للدراسات العليا
المجلد الخامس العدد الأول 2022

الجدول رقم (9) نتائج اختبار الفرضية الفرعية الثانية

| One-Sample Test 100 | | | | | | | |
|---|---|---|---|---|---|---|---|
| البيان | Test Value = 100 | | | | | | |
| | المتوسط الحسابي | الانحراف المعياري | T المحسوبة | T الجدولية | Df درجة الحرية | Sig. (2-tailed) مستوى الدلالة | الوزن النسبي |
| إجمالي المحور الثاني | 3.510 | 0.85 | 6.313 | 1.645 | 110 | 000 | 0.6021 |

يتضح ن قيمة (T) المحسوبة بلغت ( 6.313 )، وهى دالة عند مستوى (a<=0.05) وبالمقارنة مع قيمة(T)الجدولية البالغة ( 1.645 ) وهذا يؤكد على عدم قبول الفرضية العدمية الأولى وقبول الفرضية البديلة التي تنص على أن: هناك تأثير لمخاطر أمن السرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني؛ ويعزى ذلك الي عدم قيام الإدارة بتدريب الموظفين لديها على اهمية مخاطر أمن المعلومات المحاسبية وكذا عدم امتلاك البنك لوحدة مستقلة لمتابعة التدابير اللازمة للحد من المخاطر سواء في المركز أو الفروع فضلًا عن عدم وجود تعليمات واضحة لإتلاف التقارير بعد إنهاء الغرض منها.

الجدول رقم (10) نتائج اختبار الفرضية الرئيسية

| الفرضية | نتيجة اختبار الفرضيات الاحصائي | | نتيجة الفرضية الصفرية |
|---|---|---|---|
| | المحسوبة T | Tالجدولية | |
| ليس هناك تأثير لمخاطر أمن السلامة المعلوماتية على النظم المحاسبية في البنك المركزي اليمني. | 6.685 | 1.645 | رفض |
| ليس هناك تأثير لمخاطر أمن السرية المعلوماتية | 6.313 | 1.645 | رفض |

EISSN: 3105-8019
ISSN: 2663-9610

| | | | |
|---|---|---|---|
| على النظم المحاسبية في البنك المركزي اليمني. | | | |
| ليس هناك تأثير لمخاطر أمن السلامة والسرية المعلوماتية على النظم المحاسبية في البنك المركزي اليمني. | -- | -- | رفض |

يتضح من الجدول اعلاه ان نتائج الفرضيتين الفرعيتين تؤكدا أن هناك تأثير لمخاطر أمن السلامة والسرية على النظم المحاسبية في البنك المركزي ممثل في مخاطر تواجه البنك المركزي في انظمته المحاسبية المستخدمة ويجب عليه تلافي ذلك من خلال استحداث ادارة المخاطر يتم فيها مراقبة المعلومات وتتبع دورتها للمحافظة على سلامة وسرية المعلومات المستخدمة في النظم المحاسبية.

الاستنتاجات والتوصيات:

أولاً: الاستنتاجات:

- توضح نتائج الدراسة أن مخاطر أمن السلامة تؤثر بشكل واضح على النظم المحاسبية في البنك المركزي اليمني. ويرجع ذلك إلى عدم إخضاع بعض العاملين، مثل عمال النظافة، للتفتيش الدوري، بالإضافة إلى السماح بتثبيت برامج غير مرخصة أو مقرصنة، ما يشكل تهديدًا مباشرًا لسلامة المعلومات المحاسبية. كما أن الدخول غير المنظم وغير المراقب إلى مركز تقنية المعلومات يزيد من حدة هذه المخاطر.
- تشير النتائج أيضًا إلى أن مخاطر أمن السرية تؤثر بشكل ملموس على النظم المحاسبية. ويعود السبب في ذلك إلى نقص التدريب الممنهج للموظفين حول أهمية حماية المعلومات، فضلاً عن غياب وحدة مستقلة لمتابعة التدابير الوقائية للحد من المخاطر، سواء في المركز الرئيس أو الفروع. كما أن عدم وجود تعليمات واضحة لإتلاف التقارير بعد انتهاء الغرض منها يزيد من احتمالية تعرض البيانات للخطر.
- تشير الدراسة إلى أن المخاطر المتعلقة بالسلامة والسرية معًا تشكل تهديدًا على النظم المحاسبية المستخدمة في البنك المركزي. ومن ثم، يتطلب الأمر تطوير آليات لمراقبة المعلومات وتتبع دورة حياتها بهدف الحفاظ على سلامتها وسريتها ضمن العمليات المحاسبية.

ثانياً: التوصيات

- يُوصى بأن يقوم البنك المركزي اليمني بإخضاع جميع العاملين للتفتيش الدوري، ومنع تثبيت أي برامج غير مرخصة أو مقرصنة، وتنظيم الدخول إلى مركز تقنية المعلومات بما يضمن حماية وسلامة البيانات.
- ينبغي على البنك إعداد خطة تدريب شاملة للموظفين حول مخاطر أمن المعلومات المحاسبية، إضافة إلى إنشاء وحدة مستقلة لمتابعة الإجراءات الوقائية للحد من المخاطر، سواء في المركز الرئيس أو الفروع.
- يُنصح باستحداث إدارة متخصصة للمخاطر ضمن هيكل البنك المركزي، تكون مهمتها مراقبة البيانات وتتبع دورة حياتها بالكامل، بما يضمن الحفاظ على سلامة وسرية المعلومات المستخدمة في النظم المحاسبية.

EISSN: 3105-8019
ISSN: 2663-9610

## قائمة المصادر:

### المصادر العربية:

1- الجبالي، محمد، & نظمي، إيهاب. (2007). قياس درجة تطبيق التدقيق الداخلي المستند للمخاطر في الأعمال المصرفية. مجلة العربي للإدارة, 27(2).

2- بالقاسم، أمحارب، & سليمان، حسين. (2017). واقع مخاطر أمن نظم المعلومات المحاسبية الإلكترونية بالمصارف التجارية الليبية. المؤتمر العلمي الدولي الأول التحوط وإدارة الخطر بالصناعة المالية الإسلامية، مركز السنابل للبحث وتطوير الموارد البشرية، الأردن.

3- الدنف، أيمن محمد. (2013). واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها (رسالة ماجستير). الجامعة الإسلامية بغزة، فلسطين.

4- الذنيبات، معاذ يوسف. (2015). مخاطر أمن المعلومات المحتملة في تطبيقات التعاملات الإلكترونية وأثرها في كفاءة نظام المعلومات. مجلة البحوث الأمنية السعودية, 24(60).

5- الربيعي، عبد الكريم، & نهاد، عبد اللطيف، خلود. (2013). أمن وسرية المعلومات وأثرها على الأداء التنافسي: دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية. مجلة دراسات محاسبية ومالية, 8(23).

6- الغثيري، خالد بن سلمان، & القحطاني، محمد عبد الله. (2009). أمن المعلومات. مكتبة الملك فهد الوطنية، السعودية.

7- حامد، فيصل. (2013). الأمن المعلوماتي. جامعة نايف العربية للعلوم الأمنية، السعودية.

8- عرب، يوسف. (2001). قانون الكمبيوتر. اتحاد المصارف العربية.

9- عرب، يوسف. (2002). دليل أمن المعلومات بخصوص جرائم الكمبيوتر والإنترنت. اتحاد المصارف العربية.

10- غنية، حمد الطاهر. (2013). أمن المعلومات المحاسبية في ظل الأنظمة الإلكترونية: دراسة تطبيقية على الشركات المساهمة الليبية. أكاديمية الدراسات العليا، طرابلس، ليبيا.

11- ليان، فادي بغدادي. (2004). الجدار الناري الشخصي لحواسيب المدراء والمستخدمين. شعاع للنشر والتوزيع، حلب، سوريا.

12- منصور، محمد حسين. (2007). المسؤولية الإلكترونية. دار الجامع الجديد للنشر، الإسكندرية، مصر.

13- الناضري، ساند محمود. (2005). العتمية وأمن الشبكات (الجزء الأول). شعاع للنشر والتوزيع، حلب، سوريا.

المصادر الاجنبية:

1. **Abu-Musa, A. A. (2004). Important threats to computerized accounting information systems: An empirical study on Saudi organizations. Public Administration, 44.(3)**
2. **Ali, S.,& Mohammed, A. (2021). The development of accounting information systems using information technology tools: Characteristics, obstacles and risks. Al-Jami' Journal, 33, 221–243.**
3. **Al-Fatlawi, Q. A., Ali, S., Dawood, & Almagtome, A. (2021). Accounting information security and IT governance under COBIT5 framework: A case study. Faculty of Administration and Economics, University of Kufa, Najaf, Iraq, 18, 294–310. Retrieved from https://www.researchgate.net**
4. **Al-Hassani, W. H., & Al-Jabri, A. J. K. (2021). Evaluating the performance of Iraqi banks according to the International Auditing Standard (570, 560): A study of a sample of commercial banks listed on the Iraqi Stock Exchange. Tikrit Journal for Administrative and Economic Sciences, 17(55), 97–116.**
5. **Al-Sharairi, M., Al-Hosban, A., & Thnaibat, H. (2018). The impact of the risks of the input of accounting information system on managerial control,**

EISSN: 3105-8019
ISSN: 2663-9610

**accounting control, and internal control in commercial banks in Jordan. International Journal of Business and Management, 13(2), 1–15.**

6. **Hossin, A. M., & Ayedh, A. M. (2016). The risks of electronic accounting information system in the Central Bank of Libya. South East Asia Journal of Contemporary Business, Economic & Law, 1(1), 45–59.**
7. **Kreicbera, L. (2010). Internal threat information security countermeasures and human factor within SMEs (Master's thesis). Lulea University of Technology, Sweden.**
8. **Laudon, K. C., & Laudon, J. P. (2008). Management information systems: Managing the digital firm (9th ed.). Prentice Hall.**