

تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية

Evaluating the level of cyber awareness among employees responsible for accounting information systems in Libyan financial institutions

عبد السلام عطية عبد السلام يوسف

حاصل علي درجة الماجستير في المحاسبة - كلية الاقتصاد والعلوم السياسية - جامعة طرابلس

الملخص:

يهدف هذا البحث إلى تحديد مستوى المعرفة والإدراك العام بمخاطر وتهديدات أمن المعلومات السيبراني لدى الموظفين، وعلي تقييم مدى التزام الموظفين بسياسات وإجراءات أمن المعلومات المتبعة في مؤسساتهم. كما يهدف البحث إلي التعرف على العلاقة بين مستوى الوعي السيبراني وبعض المتغيرات كالمؤهل العلمي وسنوات الخبرة. ويسعي البحث إلي وضع توصيات ومقترحات لتعزيز مستوى الوعي السيبراني وسد الفجوات القائمة لدى الموظفين بهذه المؤسسات.

تم اتباع المنهجية الكمية لهذا البحث باعتبارها المنهجية الأوسع انتشاراً في جمع وتحليل البيانات في العلوم المحاسبية والإدارية وعلوم نظم المعلومات والأمن السيبراني من أجل الوصول إلى النتائج المرجوة. تم إنشاء اسئلة الاستبيان وتوزيعها على مجموعة من الموظفين في المؤسسات المالية في ليبيا لمعرفة لتقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية. لقد عمل إنشاء الاستبيان باستخدام جوجل فورم وتوزيعه على الأشخاص المعنيين بالتجربة، وقد تم تحصيل ٢٠٠ من الردود، وتم استخدام برنامج الحزمة الاحصائية المتكاملة SPSS من أجل تحليل البيانات والتوصل الى النتائج.

وجود علاقة عكسية بين ارتفاع مستوى الوعي السيبراني وحالات التعرض لهجوم سيبراني علي نظم المعلومات المحاسبية يدل عليها معامل بيرسون (٠.٦٩٥)، وذلك عند مستوى دلالة (٠.٠٥). كما أشارت النتائج إلي وجود قيم متوسطات عالية تدل علي تمتع عدد كبير من الموظفين بدرجات عالية من الوعي السيبراني المتعلق بنظم المعلومات المحاسبية في المؤسسات المالية، مثل قدرة الموظفين علي التعرف على محاولات الاختيال الالكتروني أو البريد الإلكتروني الاحتمالي (متوسط ٣.٩٩، وانحراف معياري ٠.٩٠٨)، ومن مظاهر هذا الوعي قيام غالبية الموظفين باتخاذ تدابير وقائية مثل تغيير كلمات المرور الافتراضية باستمرار (متوسط ٣.٩٣، وانحراف معياري ٠.٩٢٩)، وسعيهم نحو تشفير البيانات الحساسة أثناء نقلها أو تخزينها (متوسط ٣.٩٢، وانحراف معياري ٠.٩٢٨). وفي الختام، أوصي البحث بضرورة إجراء دورات تدريبية مكثفة للموظفين حول أفضل الممارسات في مجال الأمن السيبراني، وتطوير آلية لقياس مدى التزام الموظفين بتطبيق سياسات وإجراءات الأمن السيبراني.

الكلمات المفتاحية: الأمن السيبراني، نظم المعلومات المحاسبية، أمن المعلومات، المؤسسات المالية، ليبيا.

Abstract:

This research aims to determine the level of knowledge and public awareness of cyber information security risks and threats among employees, and to evaluate the extent of employees' commitment to the information security policies and procedures followed in their organizations. The research also aims to identify the relationship between the level of cyber awareness and some variables such as academic qualifications and years of experience. The research seeks to develop

recommendations and proposals to enhance the level of cyber awareness and fill the existing gaps among employees in these institutions. The quantitative methodology for this research was followed as it is the most widespread methodology for collecting and analyzing data in accounting and administrative sciences, information systems sciences, and cybersecurity in order to reach the desired results. Survey questions were created and distributed to a group of employees in financial institutions in Libya to assess the level of cyber awareness among employees responsible for accounting information systems in financial institutions. The questionnaire was created using Google Form and distributed to the people involved in the experiment. 200 responses were collected, and SPSS was used to analyze the data and reach results. There is an inverse relationship between the high level of cyber awareness and cases of exposure to cyber-attacks on accounting information systems, as indicated by the Pearson coefficient (0.695), at a significance level (0.05). The results also indicated that there are high average values indicating that a large number of employees have high degrees of cyber awareness related to accounting information systems in financial institutions, such as the ability of employees to recognize electronic fraud attempts or fraudulent e-mail (average 3.99, standard deviation 0.908). One manifestation of this awareness is that the majority of employees take preventive measures such as constantly changing default passwords (average 3.93, standard

deviation 0.929), and striving to encrypt sensitive data during transfer or storage (average 3.92, standard deviation 0.928). In conclusion, the research recommended the necessity of conducting intensive training courses for employees on best practices in the field of cybersecurity. and developing a mechanism to measure the extent of employees' commitment to implementing cybersecurity policies and procedures.

Keywords: cybersecurity, accounting information systems, information security, financial institutions, Libya.

١ - المقدمة:

يُعد أمن المعلومات والأمن السيبراني من الموضوعات الحيوية والمهمة في عصرنا الراهن، وذلك نظراً للتطور الهائل في مجال تكنولوجيا المعلومات والاعتماد الكبير على الإنترنت، حيث أصبحت معظم المصارف والشركات تعتمد بشكل كبير على أنظمة المعلومات في إدارة أعمالها وعملياتها المختلفة (عاطف، ٢٠١٩).

وتُعد المصارف من أكثر القطاعات أهمية في الاقتصاد المعاصر مما دفع الكثيرون إلى الاهتمام بأمن المعلومات لهذا القطاع الحيوي (عبد الواحد، ٢٠٢٣). فالبيانات والمعلومات المالية والمصرفية شديدة الحساسية ويمكن أن يؤدي اختراقها أو سرقتها إلى أضرار فادحة، لذلك، من الضروري توفير مستوى عالٍ من الأمن والحماية لنظم المعلومات المحاسبية في هذه المصارف (سالم، ٢٠٢٣).

وقطاع المصارف في ليبيا يعد أحد القطاعات الحيوية ذات الأهمية البالغة في الاقتصاد الوطني الليبي، ويتعامل مع كميات هائلة من المعلومات المحاسبية والمعاملات الإلكترونية يومياً (عبد السلام، ٢٠١٤). وبالتالي، فإن ضمان جودة

وأمان هذه المعلومات يعد أمراً حيوياً لاستدامة ونجاح العمليات المالية لهذه المؤسسات المالية (عبد السلام، ٢٠٢١).

ويتطلب تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية توفر إطار قوي لاتخاذ القرارات ونظام فعال لإدارة المخاطر وضمان التوازن بين مختلف أصحاب المصالح وتحقيق الأهداف المستهدفة للمنشآت المصرفية (حمودي، ٢٠٢٠) في سياق أمن المعلومات والأمن السيبراني، تتعدد العقبات التي تواجه المؤسسات المصرفية، وتشمل اختراق البيانات وسرقتها والتهديدات السيبرانية المتزايدة (يونس، ٢٠١٥).

وتهدف هذه الدراسة إلى تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية في ليبيا، وتركز بشكل خاص على أقسام المعاملات الإلكترونية وأقسام المحاسبة، وستقوم هذه الدراسة بتحديد مدى فاعلية وكفاءة إجراءات الأمان المعتمدة في هذه الأقسام وتحديد معايير جودة أمن المعلومات. حيث سيتم تحديد المقاييس والمؤشرات الرئيسية لقياس جودة أمن المعلومات ومعايير الجودة للأمن السيبراني (عيسي، ٢٠٢١). كما تهدف الدراسة إلى تحليل المشكلات التي قد تواجه المؤسسات المصرفية في تنفيذ إجراءات أمن المعلومات، وتقديم توصيات عملية لتعزيز جودة أمن المعلومات وتحسين الأداء العام للأقسام المعنية (فرج والوكيل، ٢٠٢٣).

وتسعي هذه الدراسة إلى إثراء المعرفة حول تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية في ليبيا. ومن المتوقع أن تكون نتائج الدراسة وتوصياتها دافعاً للمؤسسات المصرفية في تحسين سياسات وإجراءات الأمان، وتعزيز قدرتها على التصدي للتهديدات السيبرانية وحماية معلوماتها المحاسبية، كما ستسهم الدراسة في توجيه البحوث المستقبلية والجهود العملية المتعلقة بأمن المعلومات والأمن السيبراني في القطاع المصرفي والمؤسسات الأخرى ذات الصلة (حمول، ٢٠١٨).

سيتم اختيار عينة الدراسة من بين الموظفين والمدراء العاملين في أقسام المحاسبة وأقسام المعاملات الإلكترونية في المؤسسات المالية في ليبيا. ستشمل العينة مجموعة متنوعة من الأفراد ذوي الخبرة المهنية في هذه الأقسام، وسيتم جمع البيانات عن طريق استبانة الكترونية، وسيتم معالجة البيانات باستخدام تقنيات إحصائية وتحليلية لتحقيق أهداف الدراسة والاستنتاجات المطلوبة. بالإضافة إلى ذلك، ستقوم الدراسة أيضاً بتسليط الضوء على مفهوم الأمن السيبراني وأهميته لضمان أمن نظم المعلومات المحاسبية في قطاع المصارف التجارية، كما ستستكشف الدراسة تأثير التهديدات السيبرانية المتزايدة على أمن المعلومات في قطاع المصارف التجارية الليبية، وستقوم الدراسة بتحليل الأدوات والتقنيات المتاحة للتصدي لهذه التهديدات وتعزيز الأمان السيبراني.

٢ - مشكلة الدراسة:

تعد المؤسسات المالية من أكثر المؤسسات عرضة للهجمات والتهديدات الإلكترونية، نظراً لاحتوائها على بيانات ومعلومات مالية ومحاسبية سرية وحساسة. وتزداد أهمية الوعي بأمن المعلومات لدى الموظفين صانعي ومشغلي تلك الأنظمة. إلا أن هناك العديد من الدراسات التي تشير إلى التحديات السيبرانية المتزايدة في المؤسسات المالية مما أدى إلى ضرورة تقييم مستويات الوعي لديهم تجاه التهديدات السيبرانية.

ومن هنا تتمثل مشكلة الدراسة في السؤال الرئيسي التالي:

ما مستوى الوعي السيبراني الحالي لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية؟

٣- أهداف الدراسة

- ١- تحديد مستوى المعرفة والإدراك العام بمخاطر وتهديدات أمن المعلومات السيبراني لدى الموظفين.
- ٢- تقييم مدى التزام الموظفين بسياسات وإجراءات أمن المعلومات المتبعة في مؤسساتهم.
- ٣- التعرف على مواطن الضعف والقصور في الوعي السيبراني لدى هؤلاء الموظفين.
- ٤- دراسة العلاقة بين مستوى الوعي السيبراني وبعض المتغيرات كالمؤهل العلمي وسنوات الخبرة.
- ٥- وضع توصيات ومقترحات لتعزيز مستوى الوعي السيبراني وسد الفجوات القائمة لدى الموظفين بهذه المؤسسات.
- ٦- تقديم إطار يمكن أن تسترشد به المؤسسات المالية في تقييم وتطوير الوعي السيبراني لدى موظفيها.

٤- أهمية الدراسة

إن أهمية هذا البحث تكمن في تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية، حيث إن نظم المعلومات المحاسبية تعتبر من العناصر الحيوية في أي مؤسسة مالية. ويأتي هذا البحث في ظل التطور الهائل في تكنولوجيا المعلومات والاتصالات وانتشار الهجمات الإلكترونية، مما يستدعي ضرورة امتلاك الموظفين المسؤولين عن تلك الأنظمة مستوى عالٍ من الوعي بمخاطر الفضاء الإلكتروني.

وسيساعد هذا البحث في تحديد مواطن الضعف والقوة في مستوى الوعي السيبراني لدى تلك الفئة، مما يمكن صانعي القرار من اتخاذ الإجراءات المناسبة لرفع مستوى الوعي وتدريب الموظفين على أفضل الممارسات في الأمن السيبراني. كما أن استخدام المنهج الكمي

والأدوات الإحصائية سيُمكن من الحصول على نتائج دقيقة وموضوعية حول واقع مستوى الوعي، واقتراح التوصيات المناسبة بناءً على البيانات الفعلية.

٥- محتويات الدراسة

تحتوي هذه الدراسة على عدد من الأبواب التي يسعى الباحثون من خلالها إلى تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية:

- ١) ملخص الدراسة باللغتين العربية والإنجليزية.
- ٢) المقدمة.
- ٣) مشكلة الدراسة.
- ٤) أهداف الدراسة.
- ٥) أهمية الدراسة. محتويات الدراسة.
- ٦) الخاتمة. النتائج.
- ٧) التوصيات.
- ٨) المصادر والمراجع.
- ٩) الملاحق.

٦- منهجية البحث

٦.١ منهج البحث

تم اتباع المنهجية الكمية لهذا البحث باعتبارها المنهجية الأوسع انتشاراً في جمع وتحليل البيانات في العلوم المحاسبية والإدارية وعلوم نظم المعلومات والأمن السيبراني من أجل الوصول إلى النتائج المرجوة. وسيتم استخدام الاختبارات التحليلية مثل الوصف الاحصائي واختبارات الترابط بين المتغيرات.

٦.٢ مجتمع البحث

المجتمع: الموظفين في المؤسسات المالية في ليبيا.

تم إنشاء اسئلة الاستبيان وتوزيعها على مجموعة من الموظفين في المؤسسات المالية في ليبيا لمعرفة لتقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية. لقد عمل إنشاء الاستبيان باستخدام جوجل فورم وتوزيعه على الأشخاص المعنيين بالتجربة، وقد تم تحصيل ٢٠٠ من الردود. بالاعتماد على برنامج الحزمة الاحصائية المتكاملة SPSS من أجل تحليل البيانات والتوصل الى النتائج.

٦.٣ أداة البحث

تم الاعتماد على الاستبانة كأداة رئيسية لجمع البيانات من عينة الدراسة، وذلك لملاءمتها لموضوع وأهداف البحث، ولذلك، تم تصميم استبانة إلكترونية تراعي الخصوصية وسهولة الاستجابة، وارسالها لعينة الموظفين عبر البريد الإلكتروني.

تم تقسيم الاستبانة إلى أقسام تغطي: البيانات الشخصية، المعرفة العامة بالأمن السيبراني، اتخاذ إجراءات الحماية، التعامل مع التهديدات والهجمات، السياسات واللوائح ذات الصلة.

تم صياغة أسئلة الاستبانة بدقة بحيث تقيس بشكل موضوعي مستوى الوعي السيبراني لدى المستجيبين.

استخدام مقياس ليكرت الخماسي لتحديد درجة الموافقة على العبارات.

تم التأكد من صدق وثبات أداة الدراسة قبل تطبيقها ميدانياً.

تم جمع البيانات وتفريغها وتحليلها باستخدام برنامج SPSS للحصول على النتائج.

٧- تحليل بيانات ونتائج البحث

سيتم تحليل البيانات على مرحلتين، وهما الوصف الإحصائي وتحليل العلاقة بين المتغيرات باستخدام الاختبارات الإحصائية الملائمة.
الوصف الإحصائي:

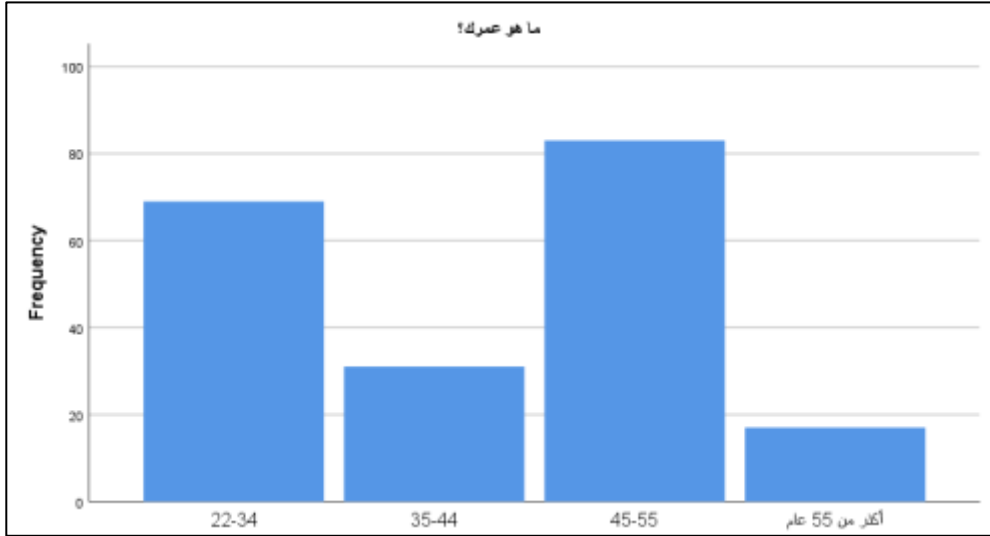
يعتبر الوصف الإحصائي حيز الزاوية في التعرف على حجم ونوعية البيانات، ويمثل تحليل أسئلة الاستبيان خطوة هامة لفهم اتجاهات المستجيبين في التجربة وتفضيلاتهم واتجاهاتهم.
١. كم عمرك؟

بالنظر إلى أعمار المشاركين في التجربة، فقد كان معظم الموظفين ينتمون إلى فئة الشباب (من عمر ٢٢ إلى ٣٤ عام) حيث بلغت نسبتهم ٦٤.٥%، مما يدل على أن هذا القطاع الحيوي يعتمد غالباً على سواعد الشباب ونشاطهم وحيويتهم.

جدول ١: السؤال عن أعمار المشاركين في الاستبيان

ما هو عمرك؟					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	22-34	129	64.5	64.5	64.5
	35-44	31	15.5	15.5	80.0
	45-55	23	11.5	11.5	91.5
	أكثر من ٥٥ عام	17	8.5	8.5	100.0
	Total	200	100.0	100.0	

تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية
 عبد السلام عطية عبد السلام بوسنة



رسم توضيحي ١: السؤال عن أعمار المشاركين في الاستبيان

٢. ما هو جنسك؟

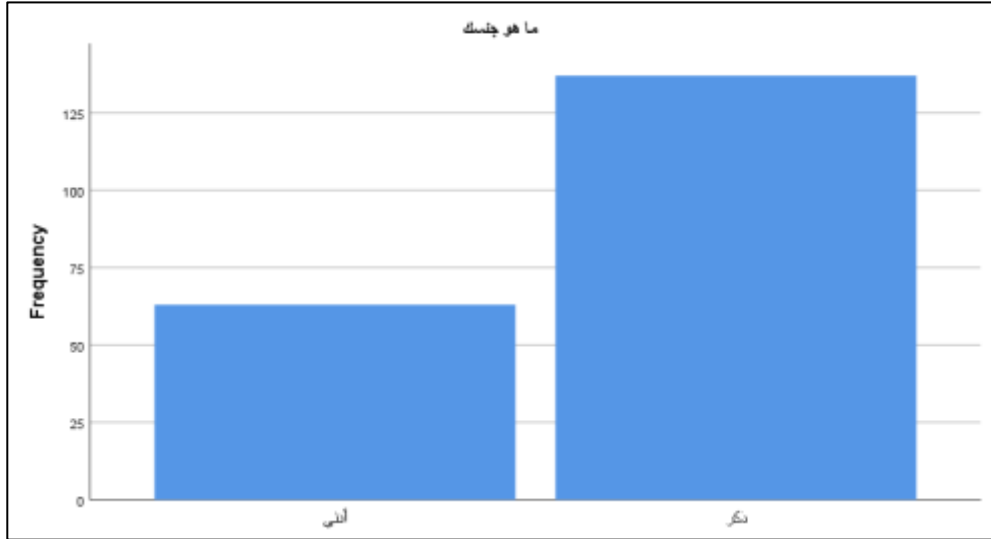
بالنظر إلى جنس المشاركين في التجربة، فقد كان معظم الموظفين من الذكور بنسبة بلغت ٦٨.٥% بينما بلغت نسبة الإناث ٣١.٥%.

جدول ٢: السؤال عن جنس المشاركين في الاستبيان

		ما هو جنسك			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أنثي	63	31.5	31.5	31.5
	ذكر	137	68.5	68.5	100.0
	Total	200	100.0	100.0	

تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية

عبد السلام عطية عبد السلام بوسنة



رسم توضيحي ٢: السؤال عن جنس المشاركين في الاستبيان

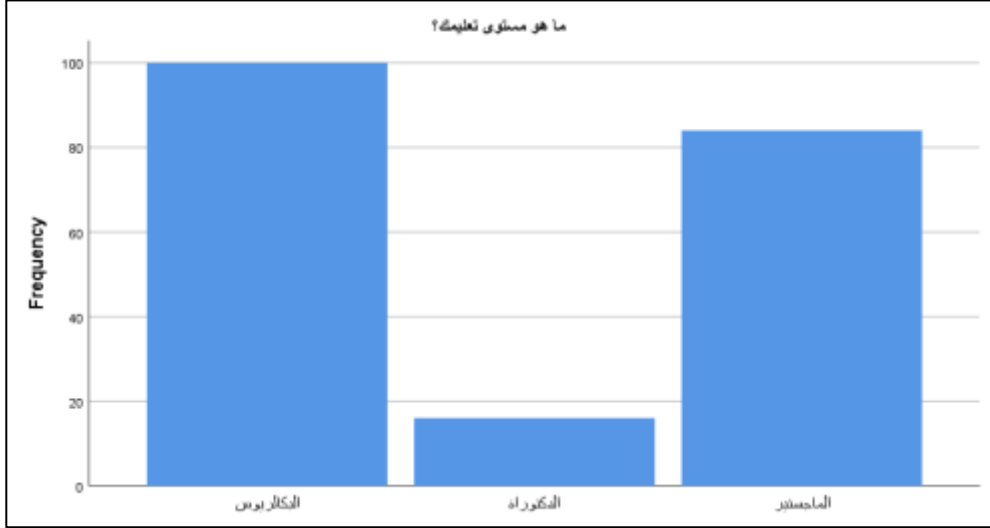
٣. الدرجة العلمية

بالنظر الى الشهادات العلمية للموظفين، فكانت درجة البكالوريوس هي المسيطرة على معظم شهادات الموظفين مع وجود نسبة كبيرة من حملة الماجستير ٤٢%، وبلغت نسبة حملة الدكتوراة ٨%. وكلما ارتفعت درجة الشهادات العلمية للموظفين كلما كان هناك مصداقية في آرائهم.

جدول ٣: السؤال عن الدرجة العلمية للمشاركين في الاستبيان

		ما هو مستوى تعليمك؟			
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	البكالوريوس	100	50.0	50.0	50.0
	الدكتوراة	16	8.0	8.0	58.0
	الماجستير	84	42.0	42.0	100.0
	Total	200	100.0	100.0	

تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية
 عيد السلام عطية عيد السلام بوسنة



رسم توضيحي ٣: السؤال عن الدرجة العلمية للمشاركين في الاستبيان

٤. عدد السنوات الخبرة

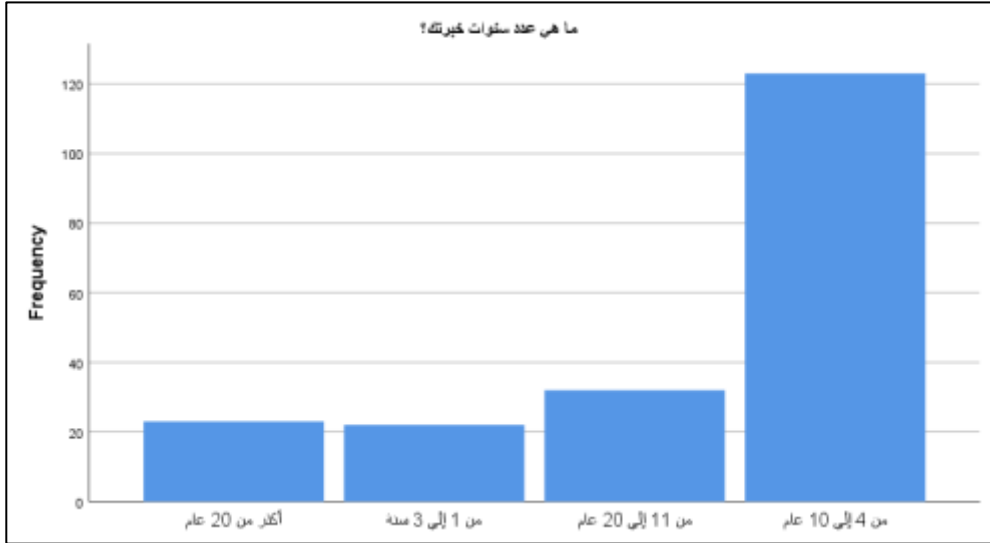
بالنظر الى عدد سنوات الخبرة للمستجيبين في التجربة، فكان معظم الموظفين يتمتعون بـ ٤ سنوات خبرة (من ٤ إلى ١٠ عام) حيث بلغ عددهم ١٢٣ موظف بنسبة ٦١.٥%.

جدول ٤: السؤال عن عدد سنوات الخبرة

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	أكثر من ٢٠ عام	23	11.5	11.5	11.5
	من ١ إلى ٣ سنة	22	11.0	11.0	22.5
	من ١١ إلى ٢٠ عام	32	16.0	16.0	38.5
	من ٤ إلى ١٠ عام	123	61.5	61.5	100.0
	Total	200	100.0	100.0	

تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية

عبد السلام عطية عبد السلام بوسوف



رسم توضيحي ٤: السؤال عن عدد سنوات الخبرة

٥- المتوسط والانحراف المعياري لأسئلة الاستبيان

تم اعتماد قيم عددية من ١ إلى ٥ لتعبر عن مقياس ليكرت الخماسي، بحيث (١=أقل قيمة، و ٥=أكبر قيمة).

جدول ٥: المتوسط والانحراف المعياري لأسئلة الاستبيان

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
هل تعرضت نظم المعلومات المحاسبية في مؤسستك إلى هجوم سيبراني؟	200	1	5	3.37	1.368
هل لديك معرفة جيدة بأنواع التهديدات السيبرانية الشائعة علي نظم المعلومات المحاسبية ؟	200	1	5	3.35	1.307
هل تستطيع تحديد نقاط الضعف في الأنظمة والشبكات التي تتعامل معها؟	200	1	5	3.43	1.505
هل تقوم بتغيير كلمات المرور الافتراضية باستمرار؟	200	1	5	3.93	.929

تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية

عبد السلام عطية عبد السلام بوسوق

هل تحافظ على نسخ احتياطية متقحة للبيانات بانتظام؟	200	1	5	3.88	.982
هل لديك إمام بالإجراءات الواجب اتخاذها عند وقوع هجوم سيبراني؟	200	1	5	3.51	1.349
هل تستطيع التعرف على محاولات الاحتيال الإلكتروني أو البريد الإلكتروني الاحتمالي؟	200	1	5	3.99	.908
هل توجد سياسات واضحة للأمن السيبراني في مؤسستك؟	200	1	5	3.62	1.205
هل يتم مراجعة سياسات وإجراءات الأمن السيبراني بانتظام في مؤسستك؟	200	1	5	3.79	1.068
هل لديك المعرفة الكافية للتعامل مع البيانات المالية والمحاسبية بشكل آمن؟	200	1	5	3.79	.974
هل تحصل دائماً على تشفير البيانات الحساسة أثناء نقلها أو تخزينها؟	200	1	5	3.92	.928
هل تجري فحوصات دورية للتأكد من سلامة أجهزة الكمبيوتر والشبكات من الفيروسات وبرامج التجسس؟	200	1	5	3.57	1.180
هل يوجد لدي مؤسستك فريق متخصص للتعامل مع حوادث الأمن السيبراني؟	200	1	5	2.88	1.403
هل يتم تنظيم برامج وندوات لنشر الوعي بين الموظفين حول مخاطر الأمن السيبراني؟	200	1	5	3.34	1.390
هل يخضع الموظفون في مؤسستك لاختبارات دورية لقياس مدى التزامهم بسياسات وإجراءات الأمن السيبراني؟	200	1	5	3.89	.916
Valid N (listwise)	200				

يُظهر الجدول وجود قيم متوسطات عالية تدل علم تمتع عدد كبير من الموظفين بدرجات عالية من الوعي السيبراني المتعلق بنظم المعلومات المحاسبية في المؤسسات المالية، مثل قدرة الموظفين علي التعرف على محاولات الاحتيال الإلكتروني أو البريد الإلكتروني الاحتمالي (متوسط ٣.٩٩، وانحراف معياري ٠.٩٠٨)، ومن مظاهر هذا الوعي قيام غالبية الموظفين باتخاذ تدابير وقائية مثل تغيير كلمات المرور الافتراضية باستمرار (متوسط ٣.٩٣، وانحراف معياري

تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية
عبد السلام عطية عبد السلام يوسف

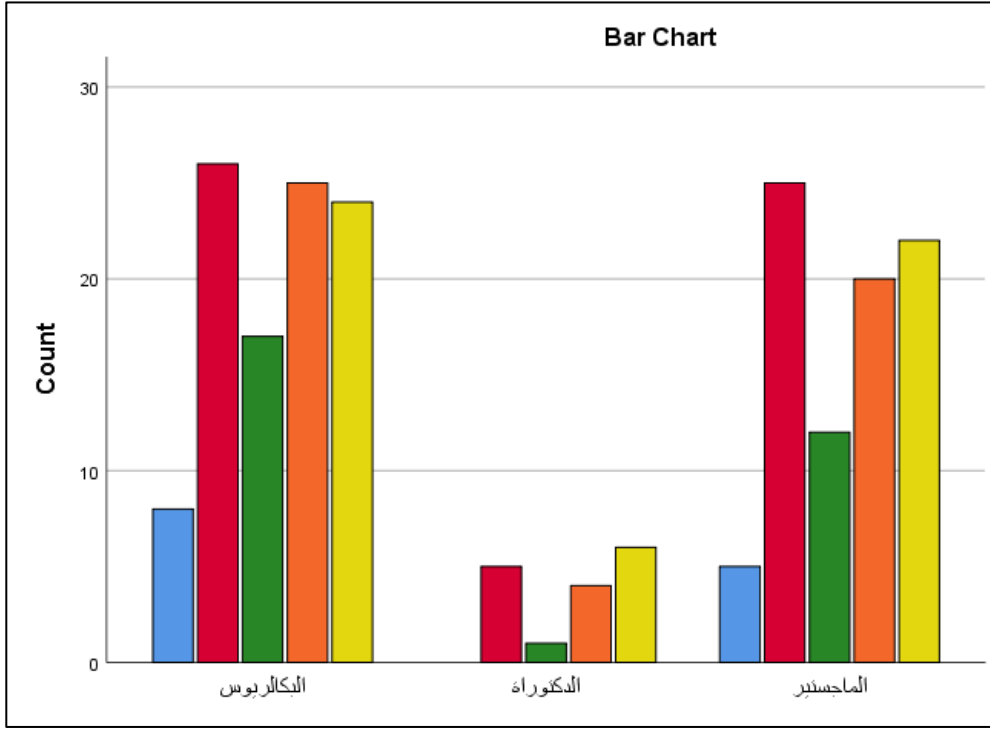
٠.٩٢٩)، وسعيهم نحو تشفير البيانات الحساسة أثناء نقلها أو تخزينها (متوسط ٣.٩٢، وانحراف معياري ٠.٩٢٨).

٦- العلاقة بين مستوى الوعي السيبراني والمؤهل العلمي

توجد علاقة بين مستوى الوعي السيبراني والمؤهل العلمي، ورغم أن معظم المشاركين في التجربة من حملة البكالوريوس، فإن حملة الماجستير (٨٤) والدكتوراة (١٦) يتمتعون أيضاً بوعي مرتفع بأهمية الأمن السيبراني لحماية نظم المعلومات المحاسبية.

جدول ٦: العلاقة بين مستوى الوعي السيبراني والمؤهل العلمي

Crosstabulation مستوى الوعي السيبراني * والمؤهل العلمي							
Count							
		مستوى الوعي السيبراني					Total
		1	2	3	4	5	
المؤهل العلمي	البكالوريوس	8	26	17	25	24	100
	الدكتوراة	0	5	1	4	6	16
	الماجستير	5	25	12	20	22	84
Total		13	56	30	49	52	200



رسم توضيحي ٥: العلاقة بين مستوى الوعي السيبراني والمؤهل العلمي

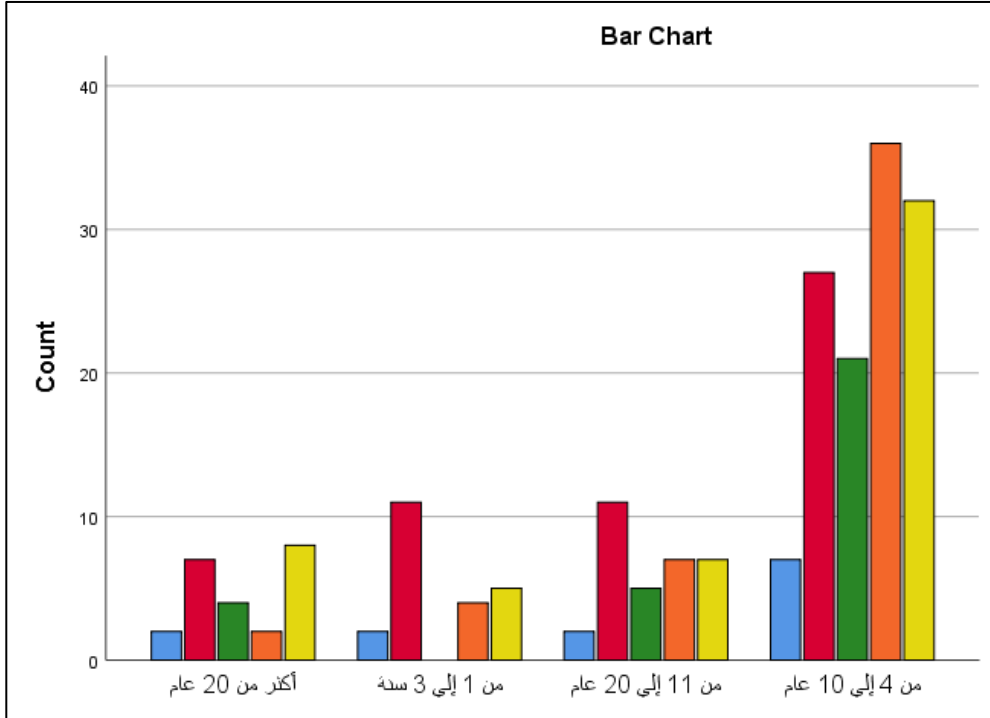
٧- العلاقة بين مستوى الوعي السيبراني وعدد سنوات الخبرة

توجد علاقة بين مستوى الوعي السيبراني وعدد سنوات الخبرة، ورغم أن معظم المشاركين في التجربة من حملة اصحاب الخبرات، ورغم تمتع القطاع بالعديد من الشباب من حديثي التخرج، فإن أصحاب الخبرة الطويلة (من ١١ إلى ٢٠ عام) وأصحاب الخبرات الأعلى (أكثر من ٢٠ عام) يتمتعون بوعي مرتفع بأهمية الأمن السيبراني لحماية نظم المعلومات المحاسبية.

تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية
 عبد السلام عطية عبد السلام بوسنة

جدول ٧: العلاقة بين مستوى الوعي السيبراني وسنوات الخبرة

Crosstabulation عدد سنوات خبرتك * مستوى الوعي السيبراني							
Count		مستوي الوعي السيبراني					Total
		1	2	3	4	5	
عدد سنوات خبرتك	أكثر من ٢٠ عام	2	7	4	2	8	23
	من ١ إلى ٣ سنة	2	11	0	4	5	22
	من ١١ إلى ٢٠ عام	2	11	5	7	7	32
	من ٤ إلى ١٠ عام	7	27	21	36	32	123
Total		13	56	30	49	52	200



رسم توضيحي ٦: العلاقة بين مستوى الوعي السيبراني وسنوات الخبرة

٨- تحليل الارتباطات:

العلاقة بين مستوى الوعي السيبراني والتعرض لهجوم سيبراني علي نظم المعلومات المحاسبية:

تُظهر النتائج وجود علاقة عكسية بين ارتفاع مستوى الوعي السيبراني وحالات التعرض لهجوم سيبراني علي نظم المعلومات المحاسبية يدل عليها معامل بيرسون (٠.٦٩٥)، وذلك عند مستوى دلالة (٠.٠٥).

جدول ٨: العلاقة بين مستوى الوعي السيبراني والتعرض لهجوم سيبراني علي نظم المعلومات المحاسبية

Correlations			
		مستوي الوعي السيبراني	هل تعرضت نظم المعلومات المحاسبية في مؤسستك إلي هجوم سيبراني؟
مستوي الوعي السيبراني	Pearson Correlation	1	.695
	Sig. (2-tailed)		-.028-
	N	200	200
والتعرض لهجوم سيبراني علي نظم المعلومات المحاسبية	Pearson Correlation	.695	1
	Sig. (2-tailed)	-.028-	
	N	200	200

العلاقة بين مستوى الوعي السيبراني واتخاذ اجراءات لضمان تطبيق الأمن السيبراني:

تُظهر النتائج وجود علاقة قوية وطرديّة، يدل عليها معامل بيرسون (٠.٨٣٨)، وذلك عند مستوى دلالة (٠.٠٥) بين مستوى الوعي السيبراني واتخاذ اجراءات لضمان تطبيق الأمن السيبراني مثل فحوصات دورية للتأكد من سلامة أجهزة الكمبيوتر والشبكات من الفيروسات وبرامج التجسس.

جدول ٩: العلاقة بين مستوى الوعي السيبراني والتعرض لهجوم سيبراني علي نظم المعلومات المحاسبية

Correlations			
		اجراء فحوصات دورية للتأكد من سلامة أجهزة الكمبيوتر والشبكات من الفيروسات وبرامج التجسس	مستوي الوعي السيبراني
اجراء فحوصات دورية للتأكد من سلامة أجهزة الكمبيوتر والشبكات من الفيروسات وبرامج التجسس	Pearson Correlation	1	.838
	Sig. (2-tailed)		.015
	N	200	200
مستوي الوعي السيبراني	Pearson Correlation	.838	1
	Sig. (2-tailed)	.015	
	N	200	200

٩- تحليل أنوفا

يتضح من نتائج اختبار أنوفا أن هناك اختلاف دال إحصائياً عند معامل p - ($value = 0.03$)، وذلك عند مستوى دلالة (٠.٠٣) وجوهرياً بين مستويات حدوث مخاطر الأمن السيبراني فيما يتعلق بمستوى الوعي بين موظفي القطاع المصرفي. وهذا يعني أن هناك تأثير يمكن تعزيره لمستوى الوعي على حدوث مخاطر الأمن السيبراني.

جدول ١٠: اختبار أنوفا للعلاقة بين المتغيرات

ANOVA					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	9.159	4	2.290	1.229	.03
Within Groups	363.196	195	1.863		
Total	372.355	199			

قيمة F في المجموعات بين (Between Groups) هي ١.٢٢٩، وهذا يشير إلى وجود فرق دال إحصائياً بين المجموعات المختلفة فيما يتعلق بمستوى حدوث مخاطر الأمن السيبراني. بمعنى آخر، يمكن أن تكون هناك اختلافات واضحة في مستوى حدوث المخاطر بين المجموعات المختلفة من موظفي القطاع المصرفي.

بشكل عام، يمكن استنتاج أن مستوى الوعي بين موظفي القطاع المصرفي يؤثر في حدوث مخاطر الأمن السيبراني في نظم المعلومات المحاسبية. وبالتالي، يمكن أن يكون التركيز على تعزيز الوعي وتعزيز المعرفة بمخاطر الأمن السيبراني بين الموظفين هو أمر ضروري للحد من هذه المخاطر وتعزيز سلامة وأمان البيانات والمعلومات في القطاع المصرفي.

٨- الخاتمة

لقد هدف هذا البحث إلى تقييم مستوى الوعي السيبراني لدى الموظفين المسؤولين عن نظم المعلومات المحاسبية في المؤسسات المالية الليبية، وذلك نظراً لأهمية تلك الأنظمة وحساسية البيانات التي تحتويها. وقد خلصت نتائج الدراسة إلى وجود عدد من الثغرات ونقاط الضعف في مستوى الوعي لدى تلك الفئة من الموظفين، مما يجعل أنظمة المعلومات المحاسبية عرضة بدرجة كبيرة للهجمات والاختراقات الإلكترونية. وفي ضوء ذلك، أوصت الدراسة بضرورة اتخاذ عدد من الإجراءات والتدابير من قبل إدارات المؤسسات المالية، والتي من شأنها رفع مستوى الوعي وتعزيز قدرات الموظفين على التصدي والحد من الهجمات الإلكترونية. ويؤمل أن تشكل نتائج وتوصيات هذا البحث نقطة انطلاق نحو بيئة عمل أكثر أمناً وحماية للأنظمة والبيانات المالية في القطاع المصرفي الليبي.

٨.١ نتائج البحث

- معظم الموظفين ينتمون إلى فئة الشباب (من عمر ٢٢ إلى ٣٤ عام) حيث بلغت نسبتهم ٦٤.٥%، مما يدل على أن هذا القطاع الحيوي يعتمد غالباً على سواعد الشباب ونشاطهم وحيويتهم.
- بالنظر إلى جنس المشاركين في التجربة، فقد كان معظم الموظفين من الذكور بنسبة بلغت ٦٨.٥% بينما بلغت نسبة الإناث ٣١.٥%.
- درجة البكالوريوس هي المسيطرة على معظم شهادات الموظفين مع وجود نسبة كبيرة من حملة الماجستير ٤٢%، وبلغت نسبة حملة الدكتوراة ٨%.
- وكلما ارتفعت درجة الشهادات العلمية للموظفين كلما كان هناك مصداقية في آرائهم.
- بالنظر إلى عدد سنوات الخبرة للمستجيبين في التجربة، فكان معظم الموظفين يتمتعون يتمتعون بخبرات (من ٤ إلى ١٠ عام) حيث بلغ عددهم ١٢٣ موظف بنسبة ٦١.٥%.
- وجود قيم متوسطات عالية تدل على تمتع عدد كبير من الموظفين بدرجات عالية من الوعي السببراني المتعلق بنظم المعلومات المحاسبية في المؤسسات المالية، مثل قدرة الموظفين على التعرف على محاولات الاختيال الإلكتروني أو البريد الإلكتروني الاحتيالي (متوسط ٣.٩٩، وانحراف معياري ٠.٩٠٨)، ومن مظاهر هذا الوعي قيام غالبية الموظفين باتخاذ تدابير وقائية مثل تغيير كلمات المرور الافتراضية باستمرار (متوسط ٣.٩٣، وانحراف معياري ٠.٩٢٩)، وسعيهم نحو تشفير البيانات الحساسة أثناء نقلها أو تخزينها (متوسط ٣.٩٢، وانحراف معياري ٠.٩٢٨).
- توجد علاقة بين مستوي الوعي السببراني والمؤهل العلمي، ورغم أن معظم المشاركين في التجربة من حملة البكالوريوس، فإن حملة الماجستير (٨٤) والدكتوراة (١٦) يتمتعون أيضاً بوعي مرتفع بأهمية الأمن السببراني لحماية نظم المعلومات المحاسبية.

- توجد علاقة بين مستوى الوعي السيبراني وعدد سنوات الخبرة، ورغم أن معظم المشاركين في التجربة من حملة اصحاب الخبرات، ورغم تمتع القطاع بالعديد من الشباب من حديثي التخرج، فإن أصحاب الخبرة الطويلة (من ١١ إلى ٢٠ عام) وأصحاب الخبرات الأعلى (أكثر من ٢٠ عام) يتمتعون بوعي مرتفع بأهمية الأمن السيبراني لحماية نظم المعلومات المحاسبية.
- وجود علاقة عكسية بين ارتفاع مستوى الوعي السيبراني وحالات التعرض لهجوم سيبراني علي نظم المعلومات المحاسبية يدل عليها معامل بيرسون (٠.٦٩٥)، وذلك عند مستوي دلالة (٠.٠٥).
- وجود علاقة قوية وطرديّة، يدل عليها معامل بيرسون (٠.٨٣٨)، وذلك عند مستوي دلالة (٠.٠٥) بين مستوي الوعي السيبراني واتخاذ اجراءات لضمان تطبيق الأمن السيبراني مثل فحوصات دورية للتأكد من سلامة أجهزة الكمبيوتر والشبكات من الفيروسات وبرامج التجسس.
- يتضح من نتائج اختبار أنوفا أن هناك اختلاف دال إحصائيًا عند معامل p - (value = 0.03)، وذلك عند مستوي دلالة (٠.٠٣) وجوهريًا بين مستويات حدوث مخاطر الأمن السيبراني فيما يتعلق بمستوى الوعي بين موظفي القطاع المصرفي. وهذا يعني أن هناك تأثير يمكن تعزيزه لمستوى الوعي على حدوث مخاطر الأمن السيبراني.

٨.٢ التوصيات

- إجراء دورات تدريبية مكثفة للموظفين حول أفضل الممارسات في مجال الأمن السيبراني.
- تطوير آلية لقياس مدى التزام الموظفين بتطبيق سياسات وإجراءات الأمن السيبراني.
- وضع سياسات واضحة ومحدثة بشكل مستمر لحماية أنظمة المعلومات المحاسبية من الهجمات الإلكترونية.

- تعيين فريق متخصص ومدرب للتعامل مع حوادث الأمن السيبراني.
- إجراء تدقيق وتقييم دوري لإجراءات وممارسات الأمن السيبراني المتبعة.
- نشر الوعي بين الموظفين حول أهمية حماية أنظمة المعلومات المحاسبية والبيانات المالية.
- تشجيع الإبلاغ عن أي محاولات اختراق أو هجوم إلكتروني.
- استخدام تقنيات التشفير الحديثة لحماية البيانات الحساسة أثناء نقلها أو تخزينها.
- الاستعانة بخبراء أمن سيبراني مستقلين لتقييم الثغرات الأمنية بشكل دوري.
- تبني ثقافة تنظيمية تؤكد على أهمية اليقظة والانتباه لقضايا الأمن السيبراني.

٩- المصادر والمراجع:

- احمد عبد السلام: مخاطر أمن نظم المعلومات المحاسبية الإلكترونية، معهد الإدارة العامة، السعودية، ٢٠١٤م، مج ٤٤، ع ٣، ص ٥٠٧.
- آلاء عبد الواحد: فاعلية نظم المعلومات المحاسبية في ضوء متطلبات الحوكمة الرقمية: دراسة تحليلية، مجلة اتحاد الجامعات العربية للبحوث في التعليم العالي، اتحاد الجامعات العربية - الأمانة العامة، الأردن، ٢٠٢٣م، مج ٤٣، عدد خاص، ص ٨٦٥.
- بدر الدين فرج، ونادية الوكيل: الإفصاح عن المخاطر المالية والتشغيلية بالمصارف التجارية: دراسة على القطاع المصرفي في ليبيا، مجلة جامعة بنغازي العلمية، ليبيا، ٢٠٢٣م، مج ٣٦، ع ١٤، ص ٤٧.
- تامر عيسى: أثر مقومات الأمن السيبراني في خصائص المعلومات المحاسبية، رسالة دكتوراة، كلية الدراسات العليا، جامعة العلوم الإسلامية العالمية، الأردن، ٢٠٢١م، ص ١٢-١٨.
- طارق حمول، ومعاشو لخضر: استراتيجيات أمن البيانات والمعلومات المصرفية لمواجهة التهديدات ومخاطر الاحتيال، مجلة الدراسات المالية والمصرفية، الاكاديمية العربية للعلوم المالية والمصرفية - مركز البحوث المالية والمصرفية، الأردن، ٢٠١٨م، مج ٢٦، ع ٣٤، ص ٢٦.

- عاليًا يونس: واقع المخاطر المصرفية في ليبيا من منظور الحوكمة المصرفية، جامعة عين شمس - كلية التجارة - قسم المحاسبة والمراجعة، ٢٠١٥م، مج ١٩، ع ٤، ص ٩٦٧.
- عبد الرحمن عاطف: الأمن السيبراني في الوطن العربي، المركز العربي للبحوث والدراسات، ٢٠١٩م، ع ٤٨، ص ٥٥.
- فريدة حمودي: الأمن المعلوماتي في الجزائر بين التطورات التكنولوجية وضعف البيئة الرقمية: المجال المصرفي نموذجًا: دراسة قانونية، مجلة جيل الأبحاث القانونية المعمقة، لبنان، ٢٠٢٠م، ع ٤١، ص ٩١.
- محمد سالم: خصائص نظم المعلومات المحاسبية الإلكترونية الحالية بالبنوك، جامعة عين شمس - كلية التجارة - قسم المحاسبة والمراجعة، ٢٠٢٣م، مج ٢٧، ع ١، ص ٢٠١.
- مختار عبد السلام، العوامل المؤثرة في جودة الخدمة المصرفية بالمصارف التجارية في ليبيا: دراسة ميدانية على مصرف الجمهورية فرع زليتن، مجلة العلوم الاقتصادية والسياسية، الجامعة الأسمرية الإسلامية - كلية الاقتصاد والتجارة، ليبيا، ٢٠٢١م، ع ١٨٤، ص ٥٧.

١٠ - الملحق

أسئلة الاستبيان:

- ١- ما هو عمرك؟
- ٢- ما هو جنسك؟
- ٣- ما هو مستوى تعليمك؟
- ٤- ما هي عدد سنواتك خبرتك؟
- ٥- هل تعرضت نظم المعلومات المحاسبية في مؤسستك إلي هجوم سيبراني؟
- ٦- هل لديك معرفة جيدة بأنواع التهديدات السيبرانية الشائعة علي نظم المعلومات المحاسبية؟
- ٧- هل تستطيع تحديد نقاط الضعف في الأنظمة والشبكات التي تتعامل معها؟
- ٨- هل تقوم بتغيير كلمات المرور الافتراضية باستمرار؟
- ٩- هل تحافظ على نسخ احتياطية منقحة للبيانات بانتظام؟
- ١٠- هل لديك إلمام بالإجراءات الواجب اتخاذها عند وقوع هجوم سيبراني؟

- ١١- هل تستطيع التعرف على محاولات الاحتيال الالكتروني أو البريد الإلكتروني الاحتيالي؟
- ١٢- هل توجد سياسات واضحة للأمن السيبراني في مؤسستك؟
- ١٣- هل يتم مراجعة سياسات وإجراءات الأمن السيبراني بانتظام في مؤسستك؟
- ١٤- هل لديك المعرفة الكافية للتعامل مع البيانات المالية والمحاسبية بشكل آمن؟
- ١٥- هل تحصل دائماً على تشفير البيانات الحساسة أثناء نقلها أو تخزينها؟
- ١٦- هل تجري فحوصات دورية للتأكد من سلامة أجهزة الكمبيوتر والشبكات من الفيروسات وبرامج التجسس؟
- ١٧- هل يوجد لدى مؤسستك فريق متخصص للتعامل مع حوادث الأمن السيبراني؟
- ١٨- هل يتم تنظيم برامج وندوات لنشر الوعي بين الموظفين حول مخاطر الأمن السيبراني؟
- ١٩- هل يخضع الموظفون في مؤسستك لاختبارات دورية لقياس مدى التزامهم بسياسات وإجراءات الأمن السيبراني؟