JOURNAL OF ISLAMIC AND RELIGIOUS STUDIES

OPEN ACCESS
ISSN (Online): 2519-7118
ISSN (Print): 2518-5330
www.jirs.uoh.edu.pk

JIRS, Vol.:8, Issue: 1, Jan – June 2023,
DOI: 10.36476/JIRS.8:1.06.2023.05, PP: 77-92

متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية

Requirements for Achieving Cyber Security in Islamic Banks of Jordan

Dr. Abd Al Majeed Ahmad Al Rahamneh
Assistant Professor, Department of Islamic Banks
The World Islamic Sciences and Education University, Jordan

Version of Record Online/Print:
28-06-2023

Accepted:
15-06-2023

Received:
28-05-2023

Abstract

The study aimed to identify the requirements of cyber realization in Jordanian Islamic banks, and the study sample consisted of (35) employees. The analytical descriptive approach was used, and the final scale consisted of (24) items distributed over four dimensions (administrative requirements, financial requirements, technical requirements, and human requirements). The results of the study showed that the requirements of cyber investigation in Jordanian Islamic banks were highly appreciated and that there were no statistically significant differences in the requirements of cyber investigation in the Jordanian Islamic banks due to the variable of gender and job title.

Keywords: *cyber security, Islamic banks.*

متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية

عبدالمجيد أحمد الرحامنة

أستاذ مساعد، قسم المصارف الإسلامية

جامعة العلوم الإسلامية العالمية، الأردن

ملخص البحث

هدفت الدراسة إلى التعرف على متطلبات تحقيق السيبراني في البنوك الإسلامية الاردنية، وتكوّنت عيّنة الدراسة من (35) موظف، واستخدم المنهج الوصفي التحليلي، وتكوّن المقياس بصورته النّهائية من (24) فقرة موزّعة على أربعة أبعاد (المتطلبات الإدارية، المتطلبات المالية، المتطلبات التقنية، المتطلبات البشرية)، وأظهرت نتائج الدراسة أن متطلبات تحقيق السيبراني في البنوك الإسلامية الاردنية جاءت بدرجة تقدير كبيرة، وعدم وجود فروق دالّة إحصائيًا في متطلبات تحقيق السيبراني في البنوك الإسلامية الاردنية تُعزى لمتغير الجنس والمسمى الوظيفي.

الكلمات المفتاحية: الأمن السيبراني، البنوك الإسلامية

المقدمة:

مع انفجار الثورة المعلوماتية ودخول العصر المعرفة الرقمية أصبحت قضية أمن وحماية المعلومات أحد أهم قضايا عصر الثورة الصناعية الرابعة، فنجاح أي مؤسسة يعتمد على ما تمتلكه من معلومات، ويتطلب منها انسيابية المعلومات وأمانها وتكامل أنظمتها، فالعديد من الأنظمة الالكترونية والمعلوماتية والبني التحتية المتعلقة بنظم الشبكات عرضة للخطر بين الحين والآخر، لما تواجهه من شتى أنواع الخروقات للمعلومات والأنشطة الإجرامية (هاكرز) التي تعطل خدماتها وتدمر ممتلكاتها، مما يستوجب المحافظة على الأمن السيبراني للجامعات، وتعزيزه، حماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات والخدمات والأنشطة ذات العلاقة.

ويشهد العالم اليوم حاله من التقدم العلمي والتطورات التقنية والتكنولوجية السريعة في شتى المجالات، إذ تميزت العقود الأخيرة بثورة في مجال تكنولوجيا المعلومات والاتصالات، والتي حولت العالم بأسره إلى مجتمع معلوماتي تتلاشى فيه الحواجز الزمانية والمكانية.[1]

فقد أصبحت دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي الذي نعيشه مؤخرًا في مجال الحوسبة الرقمية، ولكن الجانب المظلم لمثل هذه التطورات الذي نشهدها، يمكن أن تجعل كبرى المؤسسات والشركات التجارية والاقتصادية مهددة بالاختراق، ولعلّ هذا أحد أهم الأسباب لدراسة الأمن السيبراني، والذي يعمل على حماية البيانات والمعلومات والشبكات والأنظمة التقنية والالكترونية من الهجمات والاختراقات التي قد تودي بها وباستقرارها.[2]

يرتبط الأمن السيبيراني ارتباطًا وثيقًا بالاقتصاد وتوسع استخدام التقنيات المتعلقة بنظم المعلومات والاتصالات في تقديم طرق وأساليب جديدة للوصول إلى العملاء، مما يعرضها في الوقت نفسه لمخاطر جديدة، حيث أن الاستخدام

الضار لتقنية المعلومات والاتصالات يمكن أن يؤدي إلى تعطيل الخدمات المتعلقة بالأمور المالية الضرورية للأنظمة المالية، وتعريض الاستقرار المالي للخطر، وتقويض الأمن والثقة، باعتبار أن الهجمات السيبرانية تشكل تهديدًا للنظام المالي بأكمله، وهي حقيقة تؤكدها التقارير الصادرة في هذا الشأن على المستوى الدولي والإقليمي والمحلي.[3]

فالأمن السيبراني هو مجموعة الأنشطة والعمليات التي تؤدي بدورها إلى تأمين الحماية للموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات، ويضمن الحد من حدوث الأضرار والخسائر المترتبة في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه بوقت أسرع، بحيث لا تتوقف عجلة الانتاج، ولا تتحول الأضرار إلى خسائر دائمة.[4]

فمع التطور الهائل والكبير في الوسائل التكنولوجية واستخدام أنظمة التواصل الإلكتروني بحيث أصبح معها اعتماد المؤسسات المالية والبنوك المصرفية في تنفيذ إجراءاتها ومعاملاتها المحلية أو الخارجية عليها، أدى إلى إزدياد الجرائم الإكترونية وعمليات النصب والإحتيال والإختراق المنظم لبيانات هذه المؤسسات في الوقت الذي يزداد فيه حجم وتعقيدات الهجمات السيبرانية في مناطق مختلفة من العالم خاصة منطقتنا العربية كونها مستهلكة للخدمات الإلكترونية وليست منتجة لها وخاصة في قطاع المؤسسات المالية والمصرفية، وهذ يتطلب منها العمل على ضمان سير تعاملاتها الإلكترونية واستمراريتها في بيئة تكنولوجية آمنة، ورفع كفاءتها لمواجهة الأخطار والتحديات التي تواجهها من خلال اعتماد كافة التقنيات الوقائية ووسائل الحماية اللازمة ضدها حفاظًا على االستقرار الأمني المعلوماتي لهذه المؤسسات المتتبع للتحديات والخسائر التي تسببت بها عمليات الإختراق والقرصنة التي تتعرض لها.[5]

كما ويصاحب تقديم العمليات المصرفية في البنوك مخاطر تشغيلية (الكترونية كانت أم تقليدية)، وقد أشارت لجنة بازل للرقابة المصرفية إلى أنه ينبغى قيام البنوك بوضع السياسات والإجراءات التى تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها.[6]

وتتمثل المخاطر السيبرانية في التعرض للهجمات الإلكترونية والتهديدات من قبل المخترقون مما يحد من سلامة أنظمتها والبرامج والمعلومات والبيانات الشخصية، فهي تكون ناتجة عن أعمال قصدية بقصد التخريب والإعتداء، وأعمال غير قصدية نتيجة الإهمال وقلة الوعي والإدراك مما يشكل تهديدًا لأسواق المال والقطاعات المصرفية، أو سرقة البيانات الشخصية والأموال للافراد والإطلاع على المعلومات دون إذن، واختراق أنظمة المعلومات، الإعتداء على الملكية الفكرية نتيجة نقاط ضعف أو ثغرات خاصة بالبرنامج أو استعمال غير سليم من قبل مستخدمي النظام أو البرنامج، أو نتيجة اعتداء جرمي، مما يتطلب تحديد المخاطر وتحليلها ووضع الإجراءات المناسبة لمعالجتها والتي تضمن حماية الأنظمة والبرامج.[7]

فبعد مرور المجتمعات البشرية بتغيرات مختلفة ألق بظلالها الثقيلة على شتى مناحي الحياة، وتأثير ذلك على مدخلاتها الإنتاجية، برزت الحاجة إلى تدريب وتطوير قدرات الأفراد العاملين لتلبية متطلبات العصر من أجل صقل خبراتهم في التعامل مع التطبيقات والبرامج الإلكترونية والتقنية المعاصرة من حيث المعرفة والمهارة اللازمة كسلاح مهم أمام هذا التغير،[8] وتتمثل أنماط وأشكال حماية أمن المعلومات والأنظمة في البنوك بالآتي:

1. الحماية المادية:

ترتبط بالوسائل والأساليب المتبعة في منع الوصول إلى نظم المعلومات وقواعدها كالأقفال والحواجز والغرف

المحصنة وغيرها،[9] مما يتطلب تخصيص غرف مغلقة لحفظ اجهزة خادم الشبكة المركزية، وتركيب تمديدات وكوابل الشبكة في أماكن محمية غير معرضة لوصول غير المتخصصين لها، واستخدام كابلات مغلقة لتقليل الإشعاع الثانوي المنبثق من خلالها، وتأمين النوافذ والفتحات الأخرى الموجودة في غرف الخادم، والأبواب والمنافذ بإستخدام أجهزة إنذار آلية تقوم بقرع أجراس للتنبيه في حالة دخول أشخاص للموقع في غير أوقات العمل، وتوفير وسائل مراقبة للموقع لإتاحة المراقبة بعد ساعات الدوام.[10]

2. حماية الأفراد:

أدركت المؤسسات باختلاف نشاطها وأنواعها أهمية العنصر البشري، وساهمت التطورات العلمية في تطوير وتحديث إدارة الموارد البشرية وذلك بإدخال وظائف ومفاهيم وطرق جديدة من أجل تحقيق الحماية والتنمية والنمو والتطور للوصول إلى المستوى الإداري المطلوب،[11] وهي الحماية التي تتصل بالموظفين العاملين على النظام التقني المعني كتوفير وسائل التعريف الخاصة بكل مفهوم وتحقيق التدريب والتأهيل للمتعاملين بوسائل الأمن إلى جانب الوعي بمسائل الامن ومخاطر الاعتداء على المعلومات،[12] لذا ينبغي تحديد كلمات مرور للموظفين على ان يراعى تحديد صلاحيات كل موظف بما يتناسب مع طبيعة عمله، واختيار الموظفين بعناية تامة خصوصا أولئك الذين يتعاملون مع بيالنات حساسة ويمنحون صلاحيات عالية، تدريب الموظفين بشكل جيد وذلك تجنبًا للعديد من المشكلات التي قد تواجهها الشبكة ومواردها نتيجة لضعف المستوى الفني للعاملين عليها، التأكد من إزالة بياناتالموظفين المنتهية مدة خدمتهم في المؤسسة من قائمة مستخدمي النظام.[13]

ويشير أبو سرحان[14] إلى أنه من مصلحة البنوك أن تبقى أعماله سرية؛ لإرتباط ذلك بمصلحة العملاء الذين يودعون أسرارهم المالية، وعلى ذلك يتوجب على المصرف المحافظة عليها؛ لأن إفشائه لها يهز الثقة به، ويزعزع مبدأ السرّية المصرفية والطمأنينة لدى العميل مما يترتب على ذلك نفور العملاء من التعامل معه، وبالتالي خسارة المصرف على الصعيد المالي والتجاري.

3. الحماية البرمجية:

تعتبر البرمجيات غير المادية عنصرًا رئيسياً في نجاح استخدام النظام، لذلك لابد من حماية البرامج وحفظ كلمات السر وطريقة إدارة نظام التشغيل وأنظمة الإتصالات، وأن أمن البرمجيات يتطلب تصميم النظام وكتابة برامجه من خلال وضع عدد إجراءات كالمفاتيح والعوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخوّل بها وتمنع أي شخص من إمكانية التلاعب والدخول إلى النظام.[15]

ويرى القضاه[16] إلى أنه يتوجب على البنوك الاسلامية أو غيرها إنشاء وحدة مستقلة داخل البنك لمعالجة الشكاوى المقدمة من العملاء ورفدها بكادر مؤهل ومدرب من الموظفين، ووضع إجراءات عمل واضحة للتعامل مع شكاوى العملاء وتصحيح الإجراءات المتبعة إذا ما ثبت مخالفتها للتعليمات النافذة أو سياسات البنك الداخلي وذلك تعزيزا لمبدأ الرقابة وحماية حقوق وأسرار العملاء.

فالمؤسسات المالية المعتمدة على الأنظمة القديمة هي الأكثر عرضة لخطر التهديد بالهجمات السيبرانية، فضلا عن إنخفاض تكلفة شن هذه الهجمات، ويرجع ذلك إلى الأسباب التالية:[17]

1. **استهداف البنية التحتية للمصرف أو تعطيل عملها بحيث تشمل البنية التحتية فى أى قطاع مالي:** أنظمة

الدفع والتسوية، ومنصات التداول، ودائع الأوراق المالية المركزية، والأطراف المقابلة المركزية.

2. **استغلال الثغرات:** ويسمى أيضا بالهجوم دون انتظار Attack Day Zero من خلال إستغلال نقاط الضزيدعف فى برمجيات وثغراتها الأمنية خاصة غير المعروفة.
3. **إختراق البيانات:** من خلال تعرضها لانتهاكات البيانات والمعلومات نظرًا لاعتمادها على بيانات العميل في إدارة الأعمال.
4. **استهداف الهواتف الذكية:** والتى أصبحت وسيلة الإتصال السيبرانى ودخول الكثير من العملاء على حساباتهم المصرفية من خلالها، أو إجراء عمليات البيع والشراء من خلال تلك الهواتف.[18]

كما وأصدرت البنوك المركزية كتيب إرشادات ونشرات لأعضاء مجالس الإدارة في البنوك لأفضل الممارسات الدولية بهدف توفير معايير حاكمية تواكب التطورات التكنولوجية في العمل المؤسسي ولمنع التعارض بين مصالح الإدارة والأطراف الأخرى كالملاك والدائنين والمستثمرين والعاملين، وبما يضمن تطوير المهام والأنشطة التي تنفذها.[19]

ولكي تتحقق متطلبات الأمن السيبراني يجب وضع مجموعة من السياسات والإجراءات الإحترازية لتوفير الحماية الكافية للبيانات والمعلومات لكي لا يتمكن الآخرين الغير مصرح بهم من الإطلاع عليها، كما لا بد من وضع مستويات متعددة للحماية والمرور إذا كانت طبيعة المعلومات والموارد الأخرى المخزونة تتطلب هذا النوع من الحماية أو وضع نظام احتياطي لبعض الملفات المهمة خشية من التدمي أو الفقدان، ووضع مجموعة من الأنظمة والقوانين واللوائح والتعليمات والتوجيهات لتحديد الأدوار الرئيسة المتعلقة بحماية آمن وسلامة مواردها، وتحديد ضوابط أمنها لتقليل المخاطر أو الحد منها، كالبناء السليم لنظام المعلومات، ووضع استراتيجية فاعلة لمراقبة وتقويم النظام، وكذلك وضع برامج تدريبية لمستخدمي نظام وأمن قواعد البيانات والمعلومات وأمن الشبكات.[20]

وتعتبر الصناعة المصرفية صناعة متغيرة ومتطورة وبالتالي تحتاج إلى كوارد مؤهلة للتعامل مع تطوراتها وتكون قادرة على الإرتقاء بها إلى مستويات مرتفعة، وبناء المهارات والقدرات الفنية والتقنية للأفراد العاملين فيها وزيادة الاستثمار في العنصر البشري، والعمل على تطوير مؤشرات السلامة الكلية التي تضمن سلامتها وأمن بياناتها ومعلوماتها وأنظمتها التكنولوجية والتي تساعد على مراقبة أدائها واستقرارها المالي.[21]

فالبحث فى مجال الامن السيبراني للبنوك – فى واقع الأمر – لا يمكن أن ينحصر تحت مظلة واحدة؛ فمنهم من اعتبره علمًا يبحث فى نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التى تهددها، ومنهم من اعتبرها مجموعة الوسائل والأدوات والإجراءات اللازمة لضمان حماية المعلومات من المخاطر، أما الجانب القانوني لها يتمثل بمجموعة التشريعات والقوانين لحماية المعلومات من الأفعال غير القانونية التى تستهدف تلك المعلومات وأنظمتها.[22]

وتتمثل أهداف البنوك الإسلامية في جلب الودائع وتنميتها واستثمار الأموال، وتحقيق الأرباح، وكذلك تقديم الخدمات المصرفية بجودة عالية للمتعاملين، وتوفير التمويل لمستثمرين واستثمارها من خلال شركات تابعة ومتخصصة، وتوفير الأمان للمودعين مما يعزز مدى الثقة للمودعين.[23]

وعليه لا بد من أن يكون هناك مجموعة من الإجراءات والتدابير الوقائية التى تستخدم لحماية المعلومات، والأجهزة، والبرمجيات، بتوفير الأدوات والو سائل اللازمة للحماية من المخاطر، لرفع مستوى الأداء الكلي للبنوك إلى أعلى مستوياته في الحد من المخاطر السيبرانية المتجددة، وأساليب التصيد الإلكتروني ضمن خطط معرفية منظّمة، من

خلال التعرف على متطلبات تحقيق السيبراني في البنوك الإسلامية الأردنية.

ثالثًا: الدراسات السابقة

أجرى الشمالي[24] للتعرف على أمن المعلومات وسريتها في الاداء المصرفي في البنوك العاملة في الاردن، وأخذت عينة طبقية منسبة 50% من مجتمعها، وبينت النتائج أن مستوى ممارسة أمن المعلومات وسريتها في البنوك العاملة في الأردن من حيث الاهمية النسبية كانت مرتفعة، واهمية الاداء المصرفي في البنوك العاملة في الاردن كانت مرتفعة.

وفي دراسة أجراها المعهد العربي للتخطيط[25] حول مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية، واستدراك الثغرات في التخطيط الاقتصادي لمجابهة هذه المخاطر، وتوصلت إلى أنه لا تكفي زيادة الإنفاق بمفردها في مواجهة التهديدات وتحقيق الأمن السيبراني في دول المجلس، بل لابد من تحسين الوعي والحوكمة والعمليات لأن هذه المنطقة هي إحدى أكثر مناطق العالم تقدماً في سرعة تبني واعتماد التكنولوجيا الحديثة.

أجرى أبو زيد[26] دراسة حول الأمن السيبراني في الوطن العربي، والبحث في أثر الهجمات السيبرانية على الوطن العربي ، وأثر الهجمات اليبرانية على السعودية، وأيضا الجهود المبذولة في مجال الأمن السيبراني على الصعيد العربي، وكانت من أهم توصياته إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في الدول العربية، وتشجيع مجالات البحث العلمي والابتكار.

هدفت دراسة البغدادي[27] إلى التعرف على اقتصاديات الأمن السيبراني في القطاع المصرفي، واستخدمت الدراسة المنهج التحليلي والمقارن، وخلصت نتائج الدراسة إلى أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالأنترنت cyber issues يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات.

هدفت دراسة Vucinic[28] إلى دراسة الآثار المحتملة لتطورات التكنولوجيا المالية على الاستقرار المالي، وتأثير التكنولوجيا المالية على هيكل السوق، وتؤكد نتائج الدراسة على أهمية التعاون الدولي للمنظمين من أجل الحفاظ على الاستقرار المالي في العالم الحديث من التغيرات والابتكارات التكنولوجية، وأن التكنولوجيا الجديدة توفر مساحة لتوسيع الخدمات المالية ولكنها تشكل أيضا مخاطر إضافية على النظام المالي من حيث مخاطر التمويل أألصغر والمخاطر المالية الكلية.

قام السمحان[29] بدراسة حول متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، طبقت على عينة قوامها (478) من العاملين في الجامعة، وفق المنهج الوصفي التحليلي، وتوصلت إلى أن جامعة الملك سعود تمتلك أدوات هامة تضمن حماية أنظمة المعلومات الادارية بالجامعة، وأن ن هذه المتطلبات ضرورية بدرجة كبيرة لحماية أنظمة المعلومات فيها.

كما أجرى كل من Khan & Malaika [30] دراسة في التكنولوجيا المالية ومجال الأمن السيبراني ذي الصلة من منظور إدارة مخاطر البنك المركزي، حيث سلطت الدراسة الضوء على ضرورة معالجة المخاطر المتعلقة بالتكنو لوجيا المالية والأمن السيبراني للبنوك المركزية من خلال تفعيل الإدارة السليمة للمخاطر الداخلية من خلال إنشاء وتعزيز نهج متكامل لإدارة المخاطر في جميع أنحاء المنظمة، بما في ذلك وحدة مخصصة إلدارة المخاطر، والتوعية والتدريب المستمر لأعضاء مجلس الإدارة والموظفين، وخطوط إبلا غ واضحة، وتقييم المرونة السيبرانية والوضع الأمني، وربط إدارة المخاطر

بالتخطيط الاستراتيجي.

مشكلة الدراسة وأسئلتها

على الرغم من الإيجابيات الهائلة المتحققة من تقنية المعلومات، إلا أن هذه الثورة المعلوماتية المتصاعدة صاحبها مجموعة من الانعكاسات السلبية الخطيرة الناتجة عن سوء الاستخدام، ومن بينها ظاهرة الجريمة الرقمية، التي لم تعد أخطارها وأثارها محصورة في نطاق دولة بعينها بل شملت أثارها بعض التحديات القانونية أمام الأجهزة المعنية بمكافحة الجريمة، فقد انتشرت كلمة الأمن السيبراني في الآونة الأخيرة، ولاحت في الأفق عدة أبعاد فيما يخص الفضاء السيبراني، مما أدى إلى نمو استخدام الإنترنت والتكنولوجيا والمعاملات الإلكترونية لذلك، وعليه زادت الهجمات السيبرانية والهجمات الارهابية مع تزايد التطور التكنولوجي والثورة المعرفية.

وانطلاقًا من أهمية العصر المعلوماتي الرقمي في تعزيز القدرات التنافسية، لا بد من رسم إستيراتيجيات وتنبي تصورات مقترحة لإدارة البيانات والمعلومات في مختلف المصارف والبنوك وإدارة استخدام تقنيات الاتصال الحديثة مدى الحياه من خلال الاستخدام الواعي لتلك التقنيات ومصادر معلوماتها، لما لها من دور في بناء وتنمية القطاعات الإقتصادية في الأردن.

كما ويعد أمن المعلومات وسريتها من القضايا الرئيسية التي يتطلب أن تعار أهمية كبيرة في المصارف والبنوك على إختلاف أشكالها وأنواعها،فمع زيادة عدد العاملين فيها وزيادة الأرباح التي تحققها وحدة التنافس بينها كل هذا فرض دورًا مهماً عليها في الحفاظ على أمن معلوماتها وسريتها.

وتعتبر البنوك من أكثر المؤسسات المالية التي تولي عناية خاصة وكبيرة لإدارة مخاطر الأمن السيبراني؛ لأن الآثار المحتملة للإختراق السيبراني تنطوي على تعرض البنوك لخسائر مالية مباشرة وغير مباشرة ناجمة عن الهجمات السيبرانية، وتعطيل الأعمال، والضرر على السمعة، وغيرها، ولا يمكن بأي حال من الأحوال إغفال المخاطر المتزايدة للهجمات السيبرانية التي تعتبر البنوك هدفًا جذابًا لها نظرًا للدور الحيوي في الوساطة المالية، مما قد يهدد الإستقرار والشمول المالي، ولهذا تختلف وتتميز هذه الدراسة في أنها تسعى إلى التعرف على متطلبات تحقيق السيبراني في في البنوك الإسلامية الأردنية؛ لمواكبة التطورات والتحديات المعاصرة التكنولوجية والمعرفية، والإرتقاء بالعمليات المصرفية وتجويد مخرجاتها العملية إلى المستوى المطلوب، وذلك من خلال الإجابة عن الأسئلة الآتية:

السؤال الأول: ما متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية؟

السؤال الثاني: هل توجد فروق دالّة إحصائيًا عند مستوى دلالة (α=0.05) في متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية تعزى لمتغيرات (الجنس، المسمى الوظيفي)؟

أهداف الدراسة

هدفت الدراسة إلى التعرف على مفهوم الأمن السيبراني، وتحديد متطلبات تحقيقه في البنوك الإسلامية الأردنية، وقياس الفروق ذات الدلالة الإحصائية في التعرف على متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية تعزى لمتغيرات (الجنس، المسمى الوظيفي).

أهمية الدراسة

1. تنبع أهميتها من كونها تلقي الضوء على قضية الأمن السيبراني للمعلومات ومحاولة الربط بينها وبين أداء البنوك

الإسلامية في الأردن ومدى تأثيرها على أدائها.

2. تعزيز الدور الذي يمثله موضوع الأمن السيبراني كتقنية حديثة في عصرٍ تزداد فيه عدد الأجهزة المتصلة بالإنترنت في الحد من المخاطر السيبرانية المتجددة، وأساليب التصيد الإلكتروني، وحماية البيانات والمعلومات والأنظمة والأصول الإلكترونية الخاصة.
3. تتجلي الأهمية في تطوير البنوك الإسلامية لمنظومتها ماديًا وبشريًا لكبح جماح تطورها والسيطرة عليها بوضع سياسات وأنظمة أمن سيبراني تكنولوجية وتقنية لمعالجة التحديات المستقبلية.
4. إلقاء الضوء على كيفية إدارة وحماية البيانات والمعلومات باعتبارها من المفاهيم الحديثة في تكوين هوية ثقافية سليمة الجذور، والإعداد لمجتمع متوازن قادر على مواجهة المستقبل.

مصطلحات الدراسة

أولًا: الأمن السيبراني: جميع التدابير والإجراءات والتقنيات والأدوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به، ويشمل أيضًا حماية الأجهزة والبيانات،[31] ويعرف **إجرائيًا** بدرجة التقدير التي تم الحصول عليها من خلال اجابات عينة الدراسة على مقياسها الذي قام الباحث بتطويره ليتناسب مع أغراضها.

ثانيًا: البنوك الإسلامية: هي مؤسسات مصرفية هدفها تجميع الأموال والمدخرات من كل من لا يرغب بالتعامل بالربا ثم العمل على توظسفهل في مجالات النشاط الاقتصادي المختلفة، وتوفير الخدمات المصرفية المتنوعة للعملاء والالتزام بما يتفق مع الشريعة الإسلامية ويحقق دعم أهداف التنمية بجوانبها الاقتصادية والاجتماعية في المجتمع.[32]

حدود الدراسة

تتح حدود الدراسة بالآتي:

- ✓ **الحدود البشرية:** الأفراد العاملين في البنوك الإسلامية.
- ✓ **الحدود الزمانية:** العام 2023.
- ✓ **الحدود المكانية:** البنوك الإسلامية الأردنية / محافظة البلقاء/ المملكة الأردنية الهاشمية.

محددات الدراسة

تتحدد نتائج الدراسة الحالية بمدى صدق أداتها وثباتها وخصائصها السيكومترية، إلى جانب صدق استجابة عينتها على فقرات الأداة.

منهج الدراسة

انتهج الباحث المنهج الوصفي التحليلي، لملائمته لطبيعتها وتحقيق أهدافها.

مجتمع وعيّنة الدراسة

تكون مجتمع الدراسة من جميع الافراد العاملين في البنوك الإسلامية الأردنية لمحافظة البلقاء والبالغ عددها (4) بنوك إسلامية، وبلغ الع الإجمالي للأفراد العاملين فيها (88) شخص وفقًا لإحصائيات عام (2022)، وبناء عليه تم إختيار عينة عشوائية بلغت (35) فردًا ليمثلوا أفراد عينة الدراسة والجدول (1) يبيّن ذلك.

جدول (1): توزّع عينة الدراسة ونسبها

المتغير	الفئة	التكرار	النسبة المئوية %
الجنس	ذكر	17	.49
	أنثى	18	.51
المسمى الوظيفي	إداري	9	.28
	مالي	14	.40
	مبرمج	12	.34
المجموع الكلي		**35**	**100%**

أداة الدراسة

تم تطوير مقياس الشمالي[33] والسمحان[34] والمتعلق بمتطلبات تحقيق الأمن السيبراني واستشارة عدد من المتخصصين في مجال الإدارة والمحاسبة والأمن السيبراني، وعليه تكونت أداة الدراسة بصورتهما الأولية من (24) فقرة موزعة على أربعة أبعاد (متطلبات) وهي: (الإدارية، المالية، التقنية، البشرية).

وكمقياس استجابة تم إعتماد مقياس ليكرت Five Likert Scale (1- 5)، وتقسيم مستويات المقياس إلى ثلاثة مستويات (منخفض من 1.00 –2.33، متوسط من 2.34 –3.67، ومرتفع من 3.68 –5.00).

كما وتم التحقّق من دلالات الصدق بعرض الاستبيان على أساتذة وخبراء وأخذ آراءهم حول انتماء الفقرات وسلامة لغتها، وبناءً على آرائهم تم تعديل بعضها من ناحية الصياغة اللغوية لزيادة وضوحها دون حذف أي منها.

كما وتم استخراج معاملات ارتباط الفقرات وبين نتائجها أن المعاملات دالة إحصائيًا عند مستويات الدلالة (0.05) و(0.01)، وتمتع المقياس بصدق عالٍ وملائم لأغراض الدراسة الحالية، والجدول (2) يبين ذلك:

جدول (2): معاملات الارتباط لفقرات مقياس الدراسة

رقم الفقرة	الارتباط بالأداة	الارتباط بالبعد	رقم الفقرة	الارتباط بالأداة	الارتباط بالبعد	رقم الفقرة	الارتباط بالأداة	الارتباط بالبعد
.1	.643**	.718**	**.9**	.806**	.812**	**.17**	.642**	.757**
.2	.681**	.859**	**.10**	.796**	.852**	**.18**	.623**	.752**
.3	.718**	.726**	**.11**	.811**	.867**	**.19**	.718**	.739**
.4	.657**	.804**	**.12**	.807**	.874**	**.20**	.647**	.816**
.5	.671**	.839**	**.13**	.826**	.823**	**.21**	.667**	.842**
.6	.678**	.814**	**.14**	.848**	.826**	**.22**	.687**	.817**
.7	.641**	.788**	**.15**	.826**	.855**	**.23**	.645**	.738**
.8	.616**	.740**	**.16**	.832**	.878**	**.24**	.674**	.744**

***دالة إحصائياً عند مستوى الدلالة (0.05).** ****دالة إحصائياً عند مستوى الدلالة (0.01).**

كما وقام الباحث بحساب معامل الثبات باستخدام معادلة كرونباخ ألفا (Cronbach Alpha) للمقياس الكلي حيث بلغت (.93)، وأظهرت النتائج أن جميع قيم الأبعاد مرتفعة ومقبولة لأغراض الدراسة، والجدول (3) يبين ذلك.

جدول (3): معاملات الثبات لأبعاد المقياس

الرقم	أبعاد المقياس	Cronbach Alpha
.1	المتطلب التقني	4.9
.2	المتطلب البشري	5.9
.3	المتطلب الإداري	3.9
.4	المتطلب المالي	.91
الدرجة الكلية		**.93**

الأساليب الإحصائيّة المستخدمة

1. المتوسطات الحسابية والانحرافات المعيارية ودرجة التقدير للإجابة على السؤال الأول.
2. اختبار تحليل التباين المتعدد (MANOVA) للإجابة على السؤال الثاني.

عرض النتائج ومناقشتها

نتائج السؤال الأول: ما متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية؟

استخراجت الرتب ودرجة التقدير والمتوسطات الحسابية والانحرافات المعيارية على فقرات كل بعد من أبعاد الدراسة وللأداة ككل وذلك على النحو الآتي:

جدول (4): المتوسطات الحسابية والانحرافات المعيارية والرتبة ودرجة التقدير

رقم المجال	البعد	المتوسط الحسابي	الانحراف المعياري	الترتيب	التقدير
.1	المتطلب التقني	4.01	.28	1	كبيرة
.2	المتطلب البشري	3.94	.34	2	كبيرة
.3	المتطلب الإداري	3.89	.39	4	كبيرة
.4	المتطلب المالي	3.92	.37	3	كبيرة
الدرجة الكلية		**3.96**	**.36**	**كبيرة**	

يتضح من الجدول (4) أن متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية جاءت بتقدير كبيرة، إذ بلغ المتوسط الحسابي الكلي للمقياس (3.96) وبانحراف معياري (.36)، وبلغ أعلى متوسط حسابي لبعد المتطلب التقني بمتوسط حسابي (4.01) وبانحراف معياري (.28)، وأدناها لبعد المتطلب الإداري بمتوسط حسابي (3.89) وبانحراف معياري (.39).

وتأتي هذه النتيجة لتبيّن أن موظفوا البنوك لديهم إستراتيجية لإدارة المخاطر المتعلقة بالأمن السيبراني بشكل

واضح وكبير بكافة متطلباتها وجوانبها، تهدف إلى توفير كافة المستلزمات والأجهزة والمعدات والبرانج التقنية الحديثة وكذلك توفير المخصصات المالية اللازمة لتوفيرها وتدريب مواردها البشرية جنبًا إلى جنب مع عمليات البحث والتطوير المستمر للوصول إلى طرق وأساليب إدارة مخاطر الأمن السيبراني الحديثة وتحسين الإنتاج.

كما يتطلب تبنى تعزيز الخصائص الريادية لدى أفرادها، وتدريبهم على ابتكار التقنيات والمنتجات الجديدة لذلك؛ للوصول إلى توطين التقنية وتطبيقات الذكاء الاصطناعي ونقل وتوطين المعرفة التكنولوجية وتفعيلها وتنميتها، ووضع آلية وهيكل تنظيمي يواكب التطورات المعاصرة، والاستفادة من كوادرها الإدارية ذات الكفاءة العالية من مبرمجين وفنيين للعمل على تكييف التقنيات التكنولوجية لتصبح أكثر ملاءمة لحماية البيانات والشبكات والأنظمة الالكترونية من الهجمات والاختراقات التي قد تودي بها وباستقرارها.

فالفرص التي تخلقها تقنيات المعلومات والاتصالات مع استمرارها في الإبداع والابتكار تمثل للمؤسسات المصرفية والبنوك تحدياً كبيرًا في إيجاد وتقديم سبل ووسائل جديدة للوصول للعملاء، فهي تتعرض في الوقت نفسه لمخاطر جديدة، تتطلب منها تدريب كوادرها البشرية لغايات التحسين المستمر والتطوير المهني والوظيفي في شتى المجالات المرتبطة بأنظمتها وبرامجها الفنية والتقنية والتكنولوجية، حيث إن الاستخدام الضار لمثل هذه التقنيات يمكن أن يؤدي إلى تعطيل الخدمات والانظمة المالية.

وقد اتفقت نتائج هذه الدراسة مع نتائج دراسات سابقة مثل دراسة كل من الشمالي،[35] المعهد العربي للتخطيط،[36] أبو زيد،[37] البغدادي[38]، Vucinic [39] و Khan & Malaika.[40]

نتائج السؤال الثاني: هل توجد فروق دالّة إحصائيًا عند مستوى دلالة (α=0.05) في متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية تعزى لمتغيرات (الجنس، المسمى الوظيفي)؟

ولمعرفة أثر متغير الجنس ومتغير المسمى الوظيفي استخرجت المتوسطات الحسابية والانحرافات المعيارية والجدول (5) يوضح النتائج.

جدول (5): المتوسطات الحسابية والانحرافات المعيارية وفقًا لمتغير الجنس والمسمى الوظيفي

المتغيرات	الفئة	المتوسط الحسابي	الانحراف المعياري
الجنس	ذكر	91.3	.34
	أنثى	93.3	.33
المسمى الوظيفي	إداري	87.3	.39
	مالي	92.3	.35
	مبرمج	98.3	.25
الدرجة الكلية		**95.3**	**.28**

يبين الجدول (5) وجود فروق ظاهرية في المتوسطات الحسابية وفقًا لمتغير الجنس، وكان أعلاها لفئة **الإناث** بمتوسط حسابي (3.93)، ووجود فروق ظاهرية في المتوسطات الحسابية وفقًا لمتغير المسمى الوظيفي وكان أعلاها لفئة **المبرمجين** بمتوسط حسابي (3.98)، ولمعرفة دلالة الفروق تم إجراء تحليل التباين المتعدد (MANOVA)، والجدول

(6) يبين النتائج.

جدول (6): نتائج تحليل التباين المتعدد

المصدر	مجموع المربعات	متوسط المربعات	درجات الحرية	قيمة F	الدلالة الإحصائية
الجنس	.521	.174	1	.1121	.097
المسمى الوظيفي	.284	.083	3	.861	.487

يتبين من الجدول (6) عدم وجود فروق ذات دلالة إحصائية عند مستوى دلالة (α=0.05) في متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية على جميع الأبعاد والمقياس الكلي تعزى لمتغير الجنس والمسمى الوظيفي، وقد تعزى هذه النتيجة إلى أن الأفراد العاملين بمختلف مسمياتهم الوظيفية والجنس من فئة الذكور والإناث لديهم وعي واحد ومشترك بأهمية متطلبات تحقيق وتوفير الأمن السيبراني في البنوك الإسلامية سواء على مستوى حماية الأموال والممتلكات المادية والفكرية للأفراد العملاء وحماية البيانات والشبكات والأنظمة الالكترونية في البنك من الهجمات والاختراقات مما يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والاضرار المترتبة من تحقق المخاطر والتهديدات.

كما ويمكن أن تعزو النتيجة إلى مدى إدراك جميع الأطراف العاملة في البنوك بأن الامن السيبراني يعد العمود الفقري لأمن البنوك والمصارف الإسلامية، باعتباره تقنية حديثة من الواجب معرفتها ودراستها ,إدراك وملاحظة التهديدات المتعلقة بأمن المعلومات بالبنوك، ووضع إجراءات وقائية عند استخدامه، وتحليل التحديات التى تواجه أمن المعلومات؛ لمواكبة للعصر وما فيه من تطورات، وبضرورة توحيد الجهود في حماية كافة الأنظمة والشبكات بما تحتويها من بيانات ومعلومات لمواجهة الإختراقات والتهديدات الإلكترونية التي تحصل، وبالأخص المؤسسات المالية والبنوك، لحساسية وسرية المعلومات.

التوصيات

في ضوء نتائج الدراسة يوصي الباحث بالآتي:

1. بناء رؤية مشتركة من شأنها تعزيز متطلبات تحقيق الأمن السيبراني وتقديم الدعم المادي والمعنوي لتوفير أفضل التقنيات والبرامج والدورات التدريبية التكنولوجية الهادفة إلى تحسين الأداء وتطوير الخدمات البنكية إلى أعلى مستوى من الجودة.
2. ضرورة اتخاذ إجراءات توفير الأمن السيبراني لضمان سلامة ومتانة نظم المعلومات المالية والإدارية والحفاظ على الإستقرار والشمول المالي وبما يحقق أهدافها.
3. وضع نماذج فعاله لإدارة المخاطر السيبرانية المصاحبة للتطورات التكنولوجية والتقنية وهو ما يتطلب الرقابة المستمرة على الأنظمة والبرامج التي تستخدمها البنوك الإسلامية لتحديدها.

الهوامش (References)

[1]Na'īmah Al Sa'dīyah and Mubārakah Al Raḥmānī, "Al Ta'allum al Iliktrūnī Lil Lughāt al Ajnabīyah 'Abra al Manaṣṣāt al Ta'Līmīyah al Iliktrūnīyah," *Al Majallah al 'Arabīyah Midād, Jāmi'Ah Muḥammad Khayḍar Baskarah Al Jazā'ir* 4 (2018): 161–82.

السعدية، نعيمة، الرحماني، مباركة، التعلم الالكتروني للغات الأجنبية عبر المنصات التعليمية الالكترونية، المجلة العربية مداد، جامعة محمد خيضر، بسكرة، الجزائر، العدد 4، 2018، ص: 161-182.

[2]Muna 'Abdullāh Al Samḥān, "Mutaṭallabāt Taḥqīq al Amn al Sybrānī li Anẓimah al Ma'lūmāt al Idārīyah bi Jāmi'at al Malik Sa'ūd," *Majallah Kullīyah al Tarbiyah, Mansoura University* 111, no. 1 (2020): 2–29, http://search.mandumah.com/Record/1120017.

السمحان، منى عبدالله، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة، العدد 111، 2020، ص: 1-29.

[3]Marwah Fatḥī Al Baghdādī, "Iqtiṣādīyāt al Amn al Sybrānī fīl Qiṭā' al Maṣrafī," *Majallah al Buḥūth al Qānūnīyah wal Iqtiṣādīyah*, no. 76 (2021): 1446–1513, http://search.mandumah.com/Record/1175084.

البغدادي، مروة فتحي، اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، العدد 76، 2021، ص: 1447-1513.

[4]Muna Al Ashqar Al Jubūr, "Al Sybrāniyah: Hājis al 'Aṣr," *Majallah al Maktabāt wal Ma'lūmāt wal Tawthīq fil 'Ālam al 'Arabī Jāmi'ah al Duwal al 'Arabīyah, Al Markaz al 'Arabī lil Buḥūth al Qānūnīyah wal Qaḍā'īyah*, no. 5 (2016): 262–63, http://search.mandumah.com/Record/854700.

الجبور، منى الأشقر، السيبرانية هاجس العصر، مجلة المكتبات والمعلومات والتوثيق في العالم العربي، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، 2019، ص 262-263.

[5] Ghassān Al Ṭālib, "Ṣyrafah Islāmīyah bi Ri'āyat al Bank al Islāmī al U'rdanī," alrainewspaper, August 6, 2019, https://alrai.com/article/10496854, Accessed on 20/01/2023.

الطالب، غسان، صيرفة اسلامية برعاية البنك الإسلامي الأردني- صحيفة الرأي، عمان، الأردن، 2019، تم الإطلاع 2023/1/20.

[6]Muḥammad Fallāq and Riḍwān Wansā'id, "Al Idārah al Iliktarūnīyah Mafhūmuhā Mutaṭallibātuhā Taṭbīqātuhā Al Multaqa al Duwalī Mutaṭallabāt Irsā' al Ḥukūmah al Iliktrūnīyah Fī Al Jazā'ir Dirāsah Tajārib Ba'ḍ al Duwal" (Al Jazā'ir, Jāmi'ah Sa'ad Daḥl, Al Bulaydah, 2013).

فلاق، محمد، انساعد، رضوان، الإدارة الإلكترونية مفهومها متطلباتها تطبيقاتها، الملتقي الدولي، متطلبات إرساء الحكومة الإلكترونية في الجزائر، دراسة تجارب بعض الدول، جامعة سعد دحل، البليدة، الجزائر، 2013.

[7]Al Jubūr, Al Sybrāniyah: Hājis al 'Aṣr".

الجبور، السيبرانية هاجس العصر.

[8]Rīm Al 'Amūsh and Ḥusayn Al Khuzā'ī, "Barāmij al Tadrīb al Iliktrūnī Fī Tanmiyah al Mahārāt al Raqmīyah Li Mu'allimī al Dirāsāt al Ijtimā'iyyah Fī al Qarn al Ḥādī Wal 'Ishrīn Kamā Yarāhā Mudīrū al Madāris," *Dirāsāt al 'Ulūm al Insānīyah Wal Ijtimā'īyah*

49, no. 5 (2022): 125–46.

العموش، ريم، الخزاعي، حسين، دور برامج التدريب الإلكتروني في تنمية المهارات الرقمية لمعلمي الدراسات الاجتماعية في القرن الحادي والعشرين كما يراها مديرو المدارس، دراسات: العلوم الانسانية والاجتماعية، المجلد 49، العدد 5، 2022، ص 125–146.

[9]Fāyiz Juma'ah Al Najjār, *Naẓm al Ma'lūmāt al Idāriyah Madkhal Mu'āṣir Min Manẓūr Idārī* (Jordan: Dār al Ḥāmid lil Nashr wal Tawzī', 2013).

النجار، فايز جمعة، نظم المعلومات الإدارية مدخل معاصر من منظور إداري، دار الحامد للنشر والتوزيع، الأردن، 2013.

[10]Fātin Sa'īd Bāmflaḥ, *Ḥimāyah Amn al Ma'lūmāt Fī Shabakah al Maktabāt Bi Jāmi'ah Umm al Qurā: Dirāsah Ḥāllah* (KSA: Jāmi'ah Umm al Qurā, 2002).

بامفلح، فاتن سعيد، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى دراسة حالة، جامعة أم القرى، السعودية، 2002.

[11]Samīrah Ṭālib Zawqār, "Taqyīm Adā' al Muwaẓẓafīn Fil Maktabāt al Jāma'īyah al Jazā'irīyah: Wasā'il, Ta'thīr Wa In'ikāsāt," *Majallah Dirāsāt Fil 'Ulūm al Insānīyah Wal Ijtimā'Īyah* 5, no. 1 (2022): 297–327.

زوقار، سميرة طالب، تقييم أداء الموظفين في المكتبات الجامعية الجزائرية: وسائل، تأثير، وانعكاسات، مجلة دراسات في العلوم الإنسانية والإجتماعية، المجلد 5، العدد 1، 2022، ص 297–327.

[12]Al Najjār, *Naẓm al Ma'lūmāt al Idāriyah Madkhal Mu'āṣir Min Manẓūr Idārī*.

النجار، نظم المعلومات الإدارية مدخل معاصر من منظور إداري.

[13]Bāmflaḥ, *Ḥimāyah Amn al Ma'lūmāt Fī Shabakah al Maktabāt Bi Jāmi'ah Umm al Qurā: Dirāsah Ḥāllah*.

بامفلح، حماية أمن المعلومات في شبكة المكتبات بجامعة أم القرى دراسة حالة.

[14]Muḥammad Shiḥdah Abū Sarḥān, "Mabda' al Sirrīyah al Maṣrafīyah Fī Qānūn al Bunūk al Urdunī Wal Sharī'ah al Islāmīyah Dirāsah Muqāranah," *Al Majallah al Urdunīyah Fīl Dirāsāt al Islāmīyah* 15, no. 4 (2018): 109–30, https://search.emarefa.net/ar/detail/BIM-1080206.

أبو سرحان، محمد شحدة، مبدأ السرية المصرفية في قانون البنوك الأردني والشريعة الإسلامية (دراسة مقارنة)، المجلة الأردنية في الدراسات الإسلامية، المجلد 15، العدد 4، 2018، ص 109–130.

[15]Najm Al Ḥumaydī, Salwa Al Sāmrā'ī, and 'Abd al Raḥmān 'Ābīd, *Naẓm al Ma'lūmāt al Idārīyah Madkhal Mu'āṣir* (Jordan: Dār Wā'il lil Nashr, 2005),..

الحميدي، نجم، السامرائي، سلوى، العبيد، عبد الرحمن، نظم المعلومات الإدارية مدخل معاصر، دار وائل للنشر، الأردن، 2005.

[16]Mūsa Al Quḍāh, "Jamī'ah Aṣḥāb Ḥisābāt al Istithmār al Muṭlaqah Fil Bunūk al Islāmīyah (Ka Unmūdhaj Muqtaraḥ Li Tamthīlhm Wa Mumārasah Ḥuqūqihim Wa Ḥimāyatuhā," *Al Majallah al Urdunīyah Fil Dirāsāt al Islāmīyah* 16, no. 4 (2019): 171–95.

القضاه، موسى، جمعية أصحاب حسابات الإستثمار المطلقة في البنوك الإسلامية (كأنموذج مقترح لتمثيلهم وممارسة حقوقهم وحمايتها، المجلة الاردنية في الدراسات الإسلامية، المجلد 16، العدد 4، 2019، ص 171–195.

[17]Sam Friedman, "Taking Cyber Risk Management to the Next Level—Lessons Learned from the Front Lines at Financial Institutions," *Deloitte Insight*, June, 2016.

[18]Maryam Khāliṣ Ḥusayn, "Al Ḥukūmah al Iliktrūnīyah," *Journal of Baghdad College of Economic Sciences University 2013*, no. 4 (2013): 439–60, https://www.iasj.net/iasj/article/72789.

حسين، مريم خالص، الحكومة الإلكترونية، مجلة كلية بغداد للعلوم الاقتصادية، العدد الخاص بالمؤتمر، العراق، 2013، ص

.439-460

[19]Fātin Ḥannā Kyrzān, "Musāhamah al Tadqīq al Dākhilī Fī Taṭbīq al Ḥawkamah Fil Maṣārif al Sūrīyah al 'Āmmah Wal Khāṣṣah (Dirāsah Muqāranah)," *Al Manārah* 19, no. 4 (2013): 85–121.

كيرزان، فاتن حنا، مساهمة التدقيق الداخلي في تطبيق الحوكمة في المصارف السورية العامة والخاصة (دراسة مقارنة)، مجلة المنارة، المجلد 19، العدد 4، 2013، ص 85-121.

[20]Nihād 'Abd al Karīm and Khulūd Al Rabī'ī, "Amn Wa Sryah al Ma'lūmāt Wa Atharuhā 'Ala al Adā' al Tanāfusī: Dirāsah Taṭbīqīyah Fī Shirktay al Ta'mīn al 'Irāqīyah al 'Āmmah Wal Ḥmrā' Lil Ta'Mīn al Ahlīyah," *Majallah Dirāsāt Muḥāsabīyah Wa Mālīyah, Baghdād* 8, no. 23 (2013).

عبد الكريم، نهاد، الربيعي، خلود، أمن وسرية المعلومات وأثرها على الأداء التنافسي: دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية، مجلة دراسات محاسبية ومالية، بغداد، المجلد 8، العدد 23، 2013.

[21]Ibrāhīm Al Karrāsinah, *Al Bunūk al Islāmīyah: Al Iṭār al Mafāhīmī Wal Taḥaddiyāt* (Abu Dhabi: Ma'had al Siyāsāt al Iqtiṣādīyah Ṣundūq al Naqd al Duwalī, 2013).

الكراسنة، إبراهيم، البنوك الإسلامية: الإطار المفاهيمي والتحديات، معهد السياسات الإقتصادية، صندوق النقد الدولي، أبو ظبي، 2013.

[22]Esi Maan Nunoo, "Smartphone Information Security Risks : Portable Devices and Workforce Mobility" (Master's Thesis, Lulea University of Technology, Sweden, 2013).
[23]Ṣāliḥ Kāmil, *Taṭawwur al 'Amal al Maṣrifī al Islāmī, Mashākil Wa Āfāq* (Jeddah: Al Ma'had al Islāmī lil Buḥūth wal Tadrīb, 2005).

كامل، صالح، تطور العمل المصرفي الإسلامي، مشاكل وآفاق، المعهد الإسلامي للبحوث والتدريب، جدة، 2005.

[24]Ḥusayn 'Alī Qāsim Al Shamālī, "Aman Wa Sirriyah al Ma'lūmāt Wa Atharuhā Fil Adā' al Maṣrifī Dirāsah Taṭbīqīyah 'ala al Bunūk al 'Āmilah Fil Urdun," *Al-Quds Open University Journal for Administrative & Economic Research & Studies* 2, no. 7 (2017): 187–200.

الشمالي، حسين علي قاسم، أمن وسرية المعلومات وأثرها في الأداء المصرفي دراسة تطبيقية على البنوك العاملة في الأردن، مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والاقتصادية، المجلد 2، عدد 7، 2017، ص 187-200.

[25]'Alam al Dīn Bānqā, "Makhāṭir al Hajmāt al Iliktrawniyah (Al Sybrāniyah) Wa Athāruhā al Iqtiṣādīyah: Dirāsah Ḥālat Duwal Majlis al Ta'āwun al Khalījī," *Silsilah Dirāsāt Tanmawiyyah Al Ma'had al 'Arabī Lil Takhṭīṭ*, no. 63 (2019): 1–66, https://www.arab-api.org/APIPublicationDetails.aspx?PublicationID=481.

بانقا، د. علم الدين، مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، سلسلة دراسات تنمويه، المعهد العربي للتخطيط، 2019، ص: 1-66.

[26]'Abd al Raḥmān 'Āṭif Abū Zayd, "Al Amn Al Sybrānī fīl Waṭan al 'Arabī, Dirāsah Ḥālah al Mamlikah al 'Arabīyah al Sa'ūdīyah," *Āfāq Siyāsiyyah*, Al Markaz Al 'Arabī lil Buḥūth wal Dirāsāh, no. 48 (2019): 55–61, http://search.mandumah.com/Record/1018657.

أبو زيد، عبد الرحمن عاطف، الأمن السيبراني في الوطن العربي، دراسة حالة المملكة العربية السعودية، المركز العربي للبحوث والدراسات، العدد 48، 2019، ص 55-61.

[27]Al Baghdādī, "Iqtiṣādīyāt al Amn al Sybrānī fīl Qiṭā' al Maṣrafī".

البغدادي، اقتصاديات الأمن السيبراني في القطاع المصرفي .

[28]Milena Vučinić, "Fintech and Financial Stability Potential Influence of Fintech on Financial Stability, Risks and Benefits," *Journal of Central Banking Theory and Practice* 9, no. 2 (May 1, 2020): 43–66, https://doi.org/10.2478/jcbtp-2020-0013.

[29] Al Samḥān, "Mutaṭallabāt Taḥqīq al Amn al Sybrānī li Anẓimah al Ma'lūmāt al Idārīyah bi Jāmi'at al Malik Sa'ūd".

السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود .

[30] Ashraf Khan and Malaika Majid, "Central Bank Risk Management, Fintech, and Cybersecurity," Working Paper (International Monetary Fund, April 23, 2021), https://www.imf.org/en/Publications/WP/Issues/2021/04/23/Central-Bank-Risk-Management-Fintech-and-Cybersecurity-50278.

[31] Al Samḥān, "Mutaṭallabāt Taḥqīq al Amn al Sybrānī li Anẓimah al Ma'lūmāt al Idārīyah bi Jāmi'at al Malik Sa'ūd".

السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود .

[32]'Abd al Mun'im Mubārak and Muḥammad Maḥmūd Yūnus, *Iqtiṣādīyāh al Nuqūd wal Ṣayrafah wal Tijārah al Dawlīyah* (Egypt: Al Dār al Jām'iīyah Al Iskandarīyah, 2006), p: 173.

مبارك، عبد المنعم ويونس، محمد محمود، اقتصاديات النقود والصيرفة والتجارة الدولية، الدار الجامعية، الاسكندرية، مصر، 2006، ص: 173.

[33]Al Shamālī, "Aman Wa Sirriyah al Ma'lūmāt Wa Atharuhā Fil Adā' al Maṣrifī Dirāsah Taṭbīqīyah 'ala al Bunūk al 'Āmilah Fil Urdun".

الشمالي، أمن وسرية المعلومات وأثرها في الأداء المصرفي دراسة تطبيقية على البنوك العاملة في الأردن .

[34] Al Samḥān, "Mutaṭallabāt Taḥqīq al Amn al Sybrānī li Anẓimah al Ma'lūmāt al Idārīyah bi Jāmi'at al Malik Sa'ūd".

السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود .

[35]Al Shamālī, "Aman Wa Sirriyah al Ma'lūmāt Wa Atharuhā Fil Adā' al Maṣrifī Dirāsah Taṭbīqīyah 'ala al Bunūk al 'Āmilah Fil Urdun".

الشمالي، أمن وسرية المعلومات وأثرها في الأداء المصرفي دراسة تطبيقية على البنوك العاملة في الأردن.

[36] Bānqā, "Makhāṭir al Hajmāt al Iliktrawniyah (Al Sybrāniyah) Wa Athāruhā al Iqtiṣādīyah: Dirāsah Ḥālat Duwal Majlis al Ta'āwun al Khalījī".

بانقا، مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي .

[37]Abū Zayd, "Al Amn Al Sybrānī fīl Waṭan al 'Arabī, Dirāsah Ḥālah al Mamlikah al 'Arabīyah al Sa'ūdīyah".

أبو زيد، الأمن السيبراني في الوطن العربي، دراسة حالة المملكة العربية السعودية.

[38]Al Baghdādī, "Iqtiṣādīyāt al Amn al Sybrānī fīl Qiṭā' al Maṣrafī".

البغدادي، اقتصاديات الأمن السيبراني في القطاع المصرفي .

[39]Vučinić, "Fintech and Financial Stability Potential Influence of Fintech on Financial Stability, Risks and Benefits".

[40]Khan and Majid, "Central Bank Risk Management, Fintech, and Cybersecurity".