التهديدات السيبرانية في القطاع المصرفي/ دراسة لتجارب عالمية

دعاء علي بدر

أ. د عبد الرحمن نجم المشهداني

الجامعة العراقية/كلية الإدارة والاقتصاد

ECONOMICS AND ADMINISTRATIVE STUDIES JOURNAL (EASJ)
EISSN: 3005-3625, PISSN: 2790-2560, DOI: http://doi.org/10.58564/EASJ/5.2.2026.9

التهديدات السيبرانية في القطاع المصرفي/ دراسة لتجارب عالمية

Cyber threats in the banking sector / a study of global experiences

دعاء علي بدر*
أ. د عبد الرحمن نجم المشهداني
الجامعة العراقية/كلية الإدارة والاقتصاد

Duaa Ali Bader *
Prof. Dr. Abdul Rahman Najm Al-Mashhadani
College of Economic & Administration / Aliraqia University

تاريخ الاستلام: 2025/06/01 تاريخ القبول: 2025/06/23 تاريخ النشر: 2026/06/01
Received: 01/06/2025 Accepted: 23/06/2025 Published: 01/06/2026

المستخلص:

تهدف هذه المقالة الى تسليط الضوء على تجارب البنوك العالمية في مجال الامن السيبراني ومواجهة التهديدات السيبرانية التي تتطور باستمرار مستحدثة أدوات وتقنيات جديدة تحدث اضرارا في استقرار النظام المالي للقطاع المصرفي، وقدمت المقالة ابرز الهجمات السيبرانية التي واجهتها كلا من البنك الاحتياطي الهندي والبنك المركزي للاتحاد الروسي والتي وعلى الرغم من قيام هذه البنوك من اصدار و تحديث استراتيجياتها وتوجيهاتها باستمرار ألا انها تواجه هجمات الكترونية مستمرة ومتطورة مع كل تحديث لهذه التوجيهات، مما يدل على أن مجال الامن السيبراني الذي يتضمن جانبي الحماية السيبرانية والهجمات السيبرانية، سيأخذ حيزا كبير في القضايا المهمة للسنوات القادمة، لذا تركز هذه المقالة على لفت انتباه البنوك والافراد وجميع القطاعات الى أهمية الامن السيبراني ووجوده في أي مؤسسة كانت أصبحت حقيقة ملحة ومهمة جدا.

الكلمات المفتاحية: التهديدات السيبرانية، الاستقرار المالي، الامن السيبراني.

بحث مستل من رسالة ماجستير

*Corresponding Author: doaa.ali.bader@aliraqia.edu.iq

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

Abstract:

This article aims to shed light on the experiences of global banks in the field of cybersecurity and confronting cyber threats that are constantly evolving, developing new tools and techniques that cause damage to the stability of the financial system of the banking sector, and the article presented the most prominent cyber-attacks faced by both the Reserve Bank of India and the Central Bank of the Russian Federation, which despite the fact that these banks issue and update their strategies and directives continuously, but they face continuous and sophisticated cyberattacks with each update of these directives, which It indicates that the field of cybersecurity, which includes the aspects of cyber protection and cyber-attacks, will take a large place in important issues for the coming years, so this article focuses on drawing the attention of banks, individuals and all sectors to the importance of cybersecurity and its presence in any institution has become an urgent and very important reality.

Cyber threats, financial stability, cybersecurity.

المقدمة

تمثل الهجمات السيبرانية على القطاع المصرفي المرتبة الثالثة بعد قطاع الافراد والقطاع العسكري. وتشكل التهديدات السيبرانية تهديدا مستمرا على استقرار النظام المالي والاقتصادي العالمي، حيث يمكن لهجمة سيبرانية أن تعطل نظم تكنلوجيا المعلومات والاتصالات المسؤول عن تقديم الخدمات المصرفية عبر الانترنت لمصرف ما. ويعتبر معظم مسولي المخاطر الرئيسيين ان المخاطر السيبرانية تمثل التهديد الأكبر لصناعة الخدمات المصرفية والأكثر احتمالية في التسبب بأزمات مالية.

أن الهدف الرئيسي للأمن السيبراني في الخدمات المصرفية الرقمية هو تأمين السلامة لحساب المستخدم والأموال الرقمية مثل بطاقات الخصم والائتمان للمعاملات، ولم يكتفي مجرمو الانترنت بسرقة الأموال وسرقة البيانات المهمة بل يهدف بدلا ذلك التسلل إلى المؤسسة المالية مما يهدد مصداقيتها ونزاهتها ويرجع السبب وراء استهداف المؤسسات المالية الى القيمة الهائلة للبيانات شديدة الحساسية وسهولة الوصول اليها حيث كانت الهجمات البارزة في السنوات الأخيرة أكثر استمرارا وتعقيدا وبعيدة المدى وتختلف آثارها حسب هدف المهاجمون فقد يكون هدفهم التسبب بضرر في السمعة او ابتزاز الضحايا والحصول على الأرباح. ان تعزيز قوة الامن السيبراني للمؤسسات المالية يبدأ بالحصول على نظرة ثاقبة حول دوافع المهاجمين ووضع الاستراتيجيات التي تعزز من مرونة الامن السيبراني في المصارف مما يجعلها قادرة على مواجهة هذه الهجمات وتعزيز سبل التعافي منها مما يمنحها القدرة على الاستمرار في تقديم الخدمات المصرفية الرقمية.

المحور الأول: منهجية البحث

أولا: مشكلة البحث

تبرز **مشكلة البحث** في الحاجة الماسة إلى فهم طبيعة وتطور التهديدات السيبرانية التي تواجه القطاع المصرفي، وكيفية استجابة المؤسسات المالية والسلطات الرقابية لها. ورغم وجود دراسات تناولت الأمن السيبراني في القطاع المصرفي، إلا أن هناك فجوة بحثية واضحة في التحليل المقارن للتجارب العالمية الناجحة والفاشلة في مواجهة هذه التحديات، وكيف يمكن الاستفادة من هذه التجارب في تطوير استراتيجيات فعالة.

ثانيا: فرضية البحث

شهدت السنوات القليلة الماضية انتشار للتهديدات السيبرانية على جميع القطاع في العالم لاسيما القطاع المصرفي. يفترض البحث ان هذه التهديدات لها تأثير على استقرار النظام المالي في القطاع المصرفي وذلك من خلال أنظمة المعلومات وشبكات الاتصالات مما يستدعي إدارة هذه الشبكات والسيطرة عليها.

ثالثا: هدف البحث

تركز هذه الدراسة على الأهداف التالية:

1. التعرف على أهم التجارب العالمية في مجال الامن السيبرانية في القطاع المصرفي مما يقدم رؤية واضحة عن كيفية تعزيز قوة المرونة السيبرانية للمصارف.
2. رفع الوعي المصرفي لدى البنوك بأهمية التهديدات السيبرانية وأثرها على الاستقرار المالي للبنك وذلك من خلال توضيح مفاهيم الامن السيبراني واستعراض أشهر انواعه.

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

رابعا: الدراسات السابقة

1. المجلة الدولية للعلوم الإنسانية والاجتماعية، دور محددات الأمن السيبراني في الاشتمال المالي في البنوك الإسلامية العاملة في الأردن، جميل سعيد جميل الشيخ، جامعة العلوم الإسلامية العالمية، الأردن، العدد (52) ديسمبر 2023.

هدفت الدراسة الى التعرف على دور محددات الأمن السيبراني في الاشتمال المالي في المصارف الإسلامية العاملة في الأردن، والتعرف على الأمن السيبراني ومحددات الأمن السيبراني (حوكمة الأمن السيبراني، أمنية البرامج السيبرانية، سياسة الأمن السيبراني والأمن السيبراني في البنوك الإسلامية في الأردن، وكذلك التعرف على الاشتمال المالي في الأردن ودور البنوك الإسلامية في الأردن في تحقيق الاشتمال المالي، وفاعلية الأمن السيبراني على الاشتمال المالي، من خلال خطوات الإستراتيجية الوطنية للاشتمال المالي، وأهدافها، وأدوار المصارف الإسلامية العاملة في الأردن في الاشتمال المالي، وتوصلت الدراسة بشكل عام ، أن إدارة الأمن السيبراني في المصارف الإسلامية العاملة في الأردن يتطلب التركيز على تبني أفضل الممارسات والسياسات والإجراءات الفعالة لحماية البيانات المالية والشخصية للعملاء، وتوفير التدريب والتوعية المستمرة للموظفين والعملاء حول مخاطر الأمن السيبراني وكيفية حماية البيانات المالية والشخصية، نتج عن البحث مجموعة من النتائج أبرزها أن الأمن السيبراني أحد أهم التحديات التي تواجه المصارف الإسلامية في الأردن، و ساهمت المصارف الإسلامية العاملة في الأردن في تعزيز الشمول المالي من خلال تقديم مجموعة متنوعة من المنتجات والخدمات المالية التي تلبي احتياجات مختلف شرائح المجتمع، بما في ذلك الحسابات المصرفية والقروض والتأمينات، كما ساهمت المصارف الإسلامية في الأردن في تنمية الاقتصاد الوطني من خلال تمويل المشاريع الصغيرة والمتوسطة ودعم التجارة والاستثمار والوصول الإلكتروني لأغلب مناطق في الأردن، وبناء على نتائج الدراسة فقد تم صياغة عدد من التوصيات من أهمها : تحديث البرمجيات والأجهزة الخاصة بأدوات الأمن السيبراني في المصرف، وتدريب والتوعية الموظفين والعملاء على كيفية التعامل مع الأمن السيبراني، وتوعيتهم حول أهمية حماية البيانات المالية والشخصية، التنويع في المنتجات المالية، والوصول الجغرافي الواسع.

2. المؤتمر العلمي الدولي الأول، بحث بعنوان (أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك) د. عبد الرحمن محمد سليمان. زينب عبدالحفيظ أحمد قاسم، جامعة عمان 2022

هدفت الدراسة إلى التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، وتقديم تشخيص لواقع إدارة مخاطر الأمن السيبراني من أجل دعم تطبيق الشمول المالي لتعزيز الاستقرار المالي لهذه البنوك، وللإجابة على التساؤلات البحثية واختبار فرضيات الدراسة أعتمد الباحثان على المنهج الوصفي التحليلي، و استخدمت الاستبانة كأداة لجمع المعلومات ووزعت بعد تقيمها وتحكيمها من عدد من المتخصصين على عينة الدراسة والتي بلغت 90 مفردة و المكونة من المدراء العامين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين. وأثبتت نتائج الدراسة أنه يوجد أثر لإدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، كما تقوم البنوك المدرجة في بورصة فلسطين بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة لألمن السيبراني بهدف دعم الشمول المالي. كما أوصت الدراسة بضرورة قيام البنوك المدرجة في بورصة فلسطين باتخاذ إجراءات لألمن السيبراني لضمان سالمة ومتانة نظم المعلومات المالية والإدارية والحفاظ على الاستقرار والشمول المالي وبما يحقق أهدافها، كما ضرورة وضع نماذج فعاله لإدارة المخاطر السيبرانية المصاحبة لتكنولوجيا المعلومات وهو ما يتطلب الرقابة المستمرة لتحديد هذه المخاطر التي قد تهدد الاستقرار المالي في القطاع المصرفي.

3. UDC journal & Filip Jovanović, VARIOUS TYPES OF CYBER THREATS, Ivana Luknar, Institute for Political Studies, Belgrade, vol:83, 1, 2024.

تهدف هذه الدراسة الى فهم السيبرانية وتحليل أنواعها المختلفة لمتطلبات الدفاع السيبراني لكل من الحكومة والقطاع الخاص وتعطي الدراسة الأهمية القصوى لكثرة الوعي بالتهديدات السيبرانية داخل المجتمعات واهمية استخدام المعلومات التكنلوجية بشكل موثوق، وتشير النتائج الى الحاجة الى التحكم بالسيبرانية ووجوب تحليل كل المكونات الأساسية التي تعتمد على التكنلوجيا للوصول الى مستوى قوي لتقليل نقاط الضعف السيبرانية، وتوصي الدراسة الاخذ بعين الاعتبار أدوات الذكاء الاصطناعي في التعامل مع هذه التهديدات.

4. Akhmad Galib& other, Latest Challenges and Trends in Network Security: Facing Cyber Threats in the Digital Era, Journal of Artificial Intelligence and Engineering Applications, Vol. 3. No. 3, 2024.

ركزت هذه الدراسة على التنامي المستمر في العصر الرقمي حيث أصبح أمن الشبكات ذا أهمية متزايدة بالنظر إلى الاعتماد المتزايد لتكنولوجيا المعلومات والإنترنت. تعد التهديدات السيبرانية مثل هجمات القرصنة وسرقة البيانات وبرامج الفدية وسرقة الهوية تهديدات كامنة لكل من الشركات والأفراد. للتغلب على هذه التحديات، هناك حاجة إلى استراتيجيات أمنية فعالة لحماية الشبكات والبيانات من الهجمات الإلكترونية. يستخدم هذا البحث نهجا نوعيا مع دراسات الأدبيات لفهم تصورات وآراء وحلول الخبراء في مجال أمن الشبكات. تظهر نتائج البحث أن التدريب والتعليم واستراتيجيات الأمن السيبراني والتعاون عبر القطاعات هي مفاتيح مواجهة التهديدات السيبرانية والحفاظ على سلامة البيانات في بيئة رقمية دائمة التطور.

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

المحور الثاني: الإطار النظري

اولا. مفهوم التهديدات السيبرانية والاستقرار المالي

نشأ مفهوم التهديدات السيبرانية في القرن الحادي عشر بعد انتشار العديد من الأشظة المشبوهة مثل التصيد الاحتيالي وحوادث برامج الفدية وهجمات الحرمان من الخدمة الموزعة (DDOS)، حينها بدأت الشركات والمؤسسات المالية تدرك خطورة هذه التهديدات وأهمية تغيير النهج المتبع في التعامل مع الامن السيبراني في بيئتها. (Stanclulescu & other, 2024, p:83)

التهديد السيبراني هي عمل إجرامي يستخدم تكنولوجيا الكمبيوتر بشكل فردي أو في مجموعات بهدف مهاجمة أنظمة أمن الكمبيوتر الأخرى لتحقيق فوائد معينة. تعتمد الجرائم الإلكترونية على أشياء مختلفة مثل الحاجة أو لمجرد إرضاء الذات. يمكن أن يتسبب وجود الجرائم الإلكترونية في خسائر لأطراف مختلفة اعتمادا على الطرف الذي تتعرض للهجوم، بدءا من الأفراد أو الجماعات أو السياسة أو البلد. مثال على الجرائم الإلكترونية التي نواجهها غالبا هو ظهور التصيد الاحتيالي باستخدام رسائل الارتباط أو التطبيقات المقنعة المرسلة إلى شخص ما عبر وسائل التواصل الاجتماعي.WhatsApp . (Akhmad G& other, 2024, p:817)

بشكل عام يمكن تعريف التهديد السيبراني على أنه هجوم من جهاز كمبيوتر واحد أو أكثر ضد أجهزة كمبيوتر أو شبكات أخرى بهدف تعطيل أو إدارة الأخيرة الوصول إلى المعلومات، وبالتالي المساس بموثوقيته وسلامته وتوافره. يمثل هذا الخرق الأمني شكلا من أشكال المخاطر السيبرانية، والتي وجد أنها مهمة في حالة القطاع المالي. (Achim, 2023, p:384)

يعرف الاستقرار المالي بأنه حاله تكون فيها المؤسسات المالية مستقرة والتي تتضمن المؤسسات المالية والأسواق المالية والبنية التحتية المالية، ويعرف أيضا بأنه الحالة التي يكون فيها النظام المالي قادر على تسهيل الأنشطة الاقتصادية الحقيقية بسهولة ويكون قادر على كسف الاختلالات المالية الناشئة عن الصدمات. (هاشم، 2025، ص49)

ان بعض الدراسات ترى بأن للاستقرار المالي مفاهيم عديدة تأخذ اتجاهين يذهب الأول في تفسير الاستقرار المالي بأنه مفهوم صعب ومعقد ويصعب تحديد مفهومه لذلك أخذ مفهوم الاتجاه الثاني وهو معاكس للاتجاه الأول وهو عدم الاستقرار المالي والذي عرف بأنه " الوضع الذي تزداد فيه مخاطر حدوث الازمات مما يؤدي الى انهيار القطاع المالي وعدم قدرته على أداء اعماله وتوجيه موارده الاقتصادية الى الفرص الاستثمارية الفعالة والمنتجة". (التميمي، 2022، ص190)

ثانيا: أنواع التهديدات السيبرانية

ان التطور المعزز بالتكنلوجيا يوفر العديد من الفوائد، ألا أنه يسبب العديد من الصعوبات والعديد من التهديدات السيبرانية التي تتوسع باستمرار وتساعدها في ذلك تكنلوجيا المعلومات حيث أصبحت هذه التهديدات عابرة للقارات، ما يلي بعض أنواع التهديدات السيبرانية:

1. البرامج الخبيثة: هي تقنيات تتضمن ارسال برامج ضارة الى أجهزة المستخدمين عبر الانترنت، تستهدف هذه التقنيات أجهزة الكمبيوتر والهواتف المحمولة المربوطة عبر شبكة الانترنت والتي تمثل تهديدا خطيرا على النظام المصرفي، حيث تسمح بتسلل المهاجمين الى النظام وسرقة مبالغ كبيرة من البنوك وبوابات الدفع.

2. الاحتيال: هو انتحال لشخصية العميل يستخدم المهاجمون هذه الطريقة للتظاهر بأنهم مالكو الحساب ويحصلون على معلومات تسجيل الدخول الخاصة بالعميل ومن ثم يقومون بتسجيل دخول غير قانوني وسرقة العميل، ويعتبر هذا النوع أكثر ضررا للفرد من البنوك.

3. خدمات الطرف الثالث: عادة ما تلجأ المصارف الى مزودي الطرف الثالث الذين يقدمون خدمات متطورة لأنظمة الدفع والخدمات المصرفية. يتمثل خطر هذا النوع من التهديدات السيبرانية في حال كان نظام الطرف الثالث مفتوحا للاختراق مما يكون سهل اختراقه والسرقة مما يؤدي الى تدمير سمعة المصرف. (Willims H.& other, 2022, p:2)

4. الحرمان من الخدمة الموزعة (DOSS): يتم تنفيذ هذا النوع من الهجوم على جهاز كمبيوتر مستخدم الشبكة الرئيسي من أجل جعله غير قابل للوصول للمستخدمين الآخرين عن طريق الغرق في رسائل المستخدم من أجل إلحاق الضرر.

5. التصيد الاحتيالي: هو نهج ميسور التكلفة وخالي من المتاعب لإلحاق الضرر بالهدف. في الغالب يقوم المهاجم بإرسال برامج ضارة إلى أجهزة كمبيوتر أخرى عبر رسائل بريد إلكتروني عادية من مصادر حسنة السمعة ومنح المتسللين إمكانية الوصول إليها. مع ظهور خدمات مثل Dropbox و 365 Officeو Salesforce وغيرها من الخدمات، مما يعمل المتسللون على تعزيز قدراتهم بمجموعة متنوعة من الهجمات المزعجة. (Abdul Qarib & Munam, 2021, P:2)

المحور الثالث: تجارب البنوك العالمية في مجال الامن السيبراني والتهديدات السيبرانية

أولا: تجربة البنك الاحتياطي الهندي

أن المصارف الهندية معرضة لأنواع مختلفة من التهديدات السيبرانية حيث يخترع المهاجمون البرامج الضارة ويتزايد نشاط رفض الخدمة الموزعة (DDOS)، وفقا للمعلومات التي جمعها فريق الاستجابة لطوارئ الكمبيوتر في الهند(CERT-in) ، وقع (44,679) و(49,455) و(50,362) حادثا للأمن السيبراني في الهند

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

خلال الأعوام 2014 و2015 و2016 على التوالي. تشمل هذه الحوادث التصيد الاحتيالي، وعمليات اقتحام مواقع الويب وتشويهها، وهجمات الفيروسات والحرمان من الخدمة من بين أمور أخرى.

كما ان هناك زيادة مضاعفة في عمليات الاحتيال على بطاقات الائتمان والخصم بسبب القشط وهجمات البرامج الضارة واختراق بيانات الاعتماد من قبل المطلعين وما إلى ذلك. وتوفر المصارف الهندية أكثر من 40٪ من المعاملات المصرفية من خلال الأجهزة المحمولة. ويتم استغلال نقاط الضعف في البرامج في تطبيقات الهاتف المحمول المصارف، كما ان هناك ارتفاع في إساءة استخدام بيانات اعتماد أنظمة سويفت الخاصة بالبنك لتحويل الأموال من خلال الوصول غير القانوني إلى أنظمة سويفت الخاصة بالبنك للمعاملات عبر الحدود. كما وأصبح البريد الإلكتروني أداة لسرقة بيانات الاعتماد السرية للعملاء مثل تفاصيل تسجيل الدخول. حيث أن عمليات الاحتيال التسوية عبر البريد الإلكتروني للأعمال(BEC) ، تستنزف أموالا ضخمة من حسابات العملاء. (Buchi, 2018, P:27)

وفقا للبنك الاحتياطي الهندي فأن المصارف الهندية خسرت 109.75 روبية بسبب السرقة والاحتيال عبر الانترنت في السنة المالية 2018 تم تسجيل معظمها من خلال بوابات الدفع الرقمية. كما ان الهجمات السيبرانية في الهند ازدادت خلال عام 2020 بنسبة 300% مقارنة بعام 2019 وذلك بسبب جائحة كوفيد-19 ونقص الامن السيبراني والوعي بالتصيد الاحتيالي والهجمات السيبرانية. (KHUSHWANT S.& OTHER, 2023, P:100)

جدول رقم (1): عمليات الاحتيال عبر بوابات الدفع الرقمية المبلغ عنها من قبل البنوك الهندية وحسب السنة

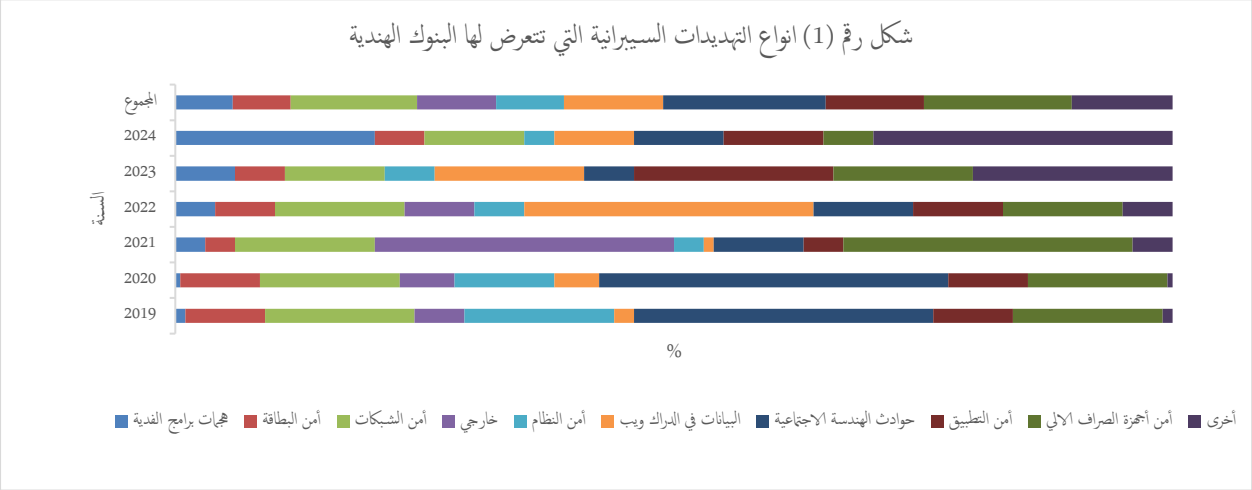
السنة المالية	عدد حالات الاحتيال	مبلغ الخسائر الناتج عنه	السنة المالية	عدد حالات الاحتيال	مبلغ الخسائر الناتج عنه
2004	26	3	2015	1191	40
2005	144	6	2016	1372	42
2005	491	11	2017	2058	102
2007	679	15	2018	1866	71
2008	1036	37	2019	2677	129
2009	1215	35	2020	2545	119
2010	763	21	2021	3596	155
2011	629	23	2022	6699	277
2012	793	49	2023	29082	1457
2013	978	54	2024	13133	514
2014	845	52	المجموع	71818	3212

الجدول من اعداد الباحث بالاعتماد على احصائيات الموقع الرسمي لبنك الاحتياطي الهندي www.rbi.org.in

نلاحظ من الاحصائيات المذكورة في الجدول أعلاه، ان التهديدات السيبرانية في تزايد مستمر من بداية عام 2004 وصولا الى 2024 والتي ارتفعت من 26 في عام 2004 عملية احتيال الى 13133 في سنة 2024 والتي تمثل اعلى عدد احتيال تعرضت له المصارف الهندية، وهذا ما يدل على ان التهديدات السيبرانية مستمرة وتتزايد باستمرار في السنوات القادمة في العالم أجمع، كما ان الأرقام أعلاه تعلنها المصارف والمؤسسات المالية في الهند وتمثل المبالغ ب (الكرو روبية)، أضافة الى ان مبالغ الخسارة هذه لا تعكس الخسارة المتكبدة الاصلية لكون هناك مبالغ استرداد تقلص مبلغ الخسارة المتكبدة. أضافة لعمليات الاحتيال المذكورة أعلاه فأن المصارف الهندية تتعرض الى أنواع أخرى من التهديدات السيبرانية سيتم توضيحها في الشكل ادناه، والذي يمثل أنواع التهديدات السيبرانية المبلغ عنها من الحوادث التي أبلغت عنها REs (SCBs وUCBs وNBFCs) من يناير 2019 إلى مارس 2024.، حيث شكلت حوادث الهندسة الاجتماعية الحصة الأكبر. كما تتزايد الحوادث المتعلقة بتسرب البيانات وأمن التطبيقات وهجمات برامج الفدية بسرعة، وتتضمن معظم هذه الحوادث قيام الجهات الفاعلة بالتهديد بتسريب بيانات المصارف مثل بيانات البطاقة والبيانات الخاصة بالعملاء ومستندات العميل على الويب المظلم أو وسائل التواصل الاجتماعي أو المنصات العامة

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

للبيع. وينشأ مصدر آخر للمخاطر من الاعتماد على مقدمي خدمات تكنولوجيا المعلومات المشتركين بين المحطات المتجددة للمخاطر المعتمدة، كما هو موضح في



الشكل (1).

المصدر/ البنك الاحتياطي الهندي، تقرير الاستقرار المالي، 2024

وعلى الرغم من سعي البنك الاحتياطي الهندي في التحديث المستمر لاستراتيجياته الرسمية في مجال الامن السيبراني ومواجهة التهديدات السيبرانية، ألا ان هذا لا يمنع هذه الهجمات نهائيا وانما يقلل من اثارها على المصارف والاقتصاد الهندي.

ثانيا: البنك المركزي للاتحاد الروسي

يتعرض القطاع المصرفي للعديد من الجرائم الإلكترونية، بما في ذلك انتهاكات البيانات وسرقة الهوية، حيث يستخدم المحتالون أساليب معقدة بشكل متزايد في ظل تأثير التحول الرقمي في حين أن الاخير يعزز الكفاءة ويقلل التكاليف، الا انه يزيد في الوقت نفسه من مخاطر الهجمات الإلكترونية. تعمل المصارف الروسية على تطوير استراتيجيات الامن السيبراني لديها بشكل مستمر لتواكب التطورات المستمرة في هذا المجال ويظهر هذا واضحا من خلال الصد الناجح للتهديدات السيبرانية للمصارف الروسية، حيث تجمع استراتيجياته بين الجهود التعاونية بين المؤسسات المالية والهيئات التنظيمية والمجتمع الدولي لتطوير تدابير حماية شاملة، والإطار التنظيمي والدعم التشريعي الذي تقوم به الحكومة الروسية من خلال وضع أطر قانونية لمكافحة التهديدات السيبرانية مما يعزز من أمن وحماية النظام المالي في القطاع المصرفي الروسي.

أدناه عدد المعاملات غير المصرح بها من قبل العملاء والتي تم الإعلان عنها من قبل الكيانات القانونية في بنوك الاتحاد الروسي، وتتمثل المعاملات غير المصرح بها بأنها حوادث تتعلق بسرقة الأموال من قبل العملاء نتيجة الوصول غير المصرح لأنظمة RBS وأنظمة تحويل الأموال باستخدام حسابات المراسلة القانونية بسبب اختراق تلك الأنظمة واستخدام البرامج الضارة لاختراق الكمبيوتر المكتبية، وكما موضح في الجدول الاتي:

جدول رقم (2): المعاملات غير المصرح بها من قبل العملاء في الاتحاد الروسي

السنة	عدد المعاملات(الالاف)	مبلغ المعاملات (مليون روبية)
2020	773.27	9783.13
2021	1035.01	13582.23
2022	876.59	14165.44
2023	1165.99	15791.41

المصدر/ الموقع الرسمي للبنك المركزي للاتحاد الروسي، قسم أمن المعلومات، التحليلات، 2025/3/10، 3:30م.

في عام 2020، بدأ بنك روسيا مشروعًا تجريبيًا لتبادل المعلومات حول المواقع الاحتيالية مع مكتب المدعي العام للاتحاد الروسي لأغراض حظرها. في عام 2021، تم إضفاء الطابع الرسمي على هذه الآلية في قانون وتم تفويض بنك روسيا بحظر المواقع غير المشروعة بموجب إجراء خارج نطاق القضاء. من خلال هذه الآلية، تم تقييد الوصول إلى 3100 موقع ويب في عام 2020. بالنسبة للموارد عبر الإنترنت المستخدمة لإجراء أنشطة احتيالية في السوق المالية والإعلان عن مخططات هرمية، تم تقليص متوسط الوقت المطلوب للحظر من عدة أسابيع إلى عدة أيام.

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

جدول رقم (3): موارد التصيد الاحتيالي في الاتحاد الروسي				
السنة	الأنشطة غير المرخصة	احتيال	مخططات هرمية	برمجيات خبيثة
2020	1352	6152	28	148
2021	1521	4337	302	53
2022	634	4276	303	4
2023	156	3477	5	1
الموقع الرسمي للبنك المركزي للاتحاد الروسي، قسم أمن المعلومات، التحليلات، 2025/3/10، 10:50م.				

تم استخدام معظم المواقع المحجوبة (حوالي 58%) لإجراء أنشطة غير مرخصة في سوق الأوراق المالية والإعلان عن مخططات هرمية. كان المحتالون يسرقون أموال العملاء تحت ستار الاستثمارات ذات العائد المرتفع في الزراعة والطاقة والعملات المشفرة.

في عام 2021، قام المحتالون في الغالب بإخفاء مواقع التصيد الاحتيالي على أنها مواقع لمؤسسات ائتمانية ومالية حقيقية للحصول على معلومات شخصية للعملاء أو بيانات اعتماد الخدمات المصرفية عبر الإنترنت، بالإضافة إلى معلومات بطاقاتهم المصرفية. بالإضافة إلى ذلك، استخدموا مواقع تحتوي على معلومات كاذبة حول كيفية تلقي المدفوعات المقدمة من الدولة أو كسب المال من خلال إكمال استبيان أو اختبار وما إلى ذلك. كانت طريقة الاحتيال الأخرى المستخدمة على نطاق واسع في عام 2021 هي استنساخ مواقع الويب الخاصة بالأسواق الشعبية وتجار التجزئة عبر الإنترنت الذين يبيعون الإلكترونيات والأجهزة المنزلية وأجهزة الكمبيوتر وما إلى ذلك.

عمل بنك روسيا بشكل نشط على تطوير التعاون مع مكتب المدعي العام للاتحاد الروسي لتقييد الوصول داخل الاتحاد الروسي إلى بعض الموارد عبر الإنترنت المعروفة بتقديم خدمات مالية غير مرخصة والإعلان عن مخططات هرمية.

منذ فبراير 2022، قام بنك روسيا بحظر الصفحات (المجموعات) على وسائل التواصل الاجتماعي وكذلك تطبيقات الكمبيوتر (الجوال) المستضاف في متاجر التطبيقات الرقمية (آب ستور، وجوجل بلاي، وما إلى ذلك) والتي استخدمها المحتالون لنشر معلومات مماثلة. خلال الفترة من 28 فبراير 2022 إلى 31 ديسمبر 2022، بدأ بنك روسيا في حظر الوصول إلى 1942 صفحة (مجموعة) على وسائل التواصل الاجتماعي و23 تطبيقًا. تجدر الإشارة إلى أن غالبية الصفحات (المجموعات) المحظورة على وسائل التواصل الاجتماعي والتطبيقات كانت تستخدم لإجراء أنشطة غير مرخصة.

واصل بنك روسيا التعاون بنشاط مع مكتب المدعي العام للاتحاد الروسي لمنع الوصول في روسيا إلى الموارد عبر الإنترنت التي تنشر معلومات حول تقديم الخدمات المالية غير المرخصة أو الإعلان عن مخططات هرمية. في عام 2023، تم حظر الوصول إلى 34677 موردًا بناءً على معلومات الجهة التنظيمية، وهو ما يزيد عن ثلاثة أضعاف عن العام السابق.

الامن السيبراني والتهديدات السيبرانية على البنوك العراقية

يواجه الامن السيبراني في العراق تحديات هائلة نتيجة التحول الرقمي في مجال الاتصالات والمعلومات مما يعد هدفا للهجمات السيبرانية نتيجة الضعف والهشاشة في الأمان الالكتروني في البنية التحتية كما ان التهديدات السيبرانية تعد تحديات غير مرئية مما يجعلها تؤثر على منظومة الامن الوطني العراقي ومع التطور التكنلوجي الذي يشهده العراق وبالتزامن مع ضعف البنية الأمنية التكنلوجية اصبح العراق منكشفا استراتيجيا لكثير من دول العالم لاختراقه والتجسس على معلوماته الخاصة بكافة المؤسسات، كما ان عدم وجود تشريعات محدده في العراق بمكافحة الهجمات السيبرانية أتاح الفرصة امام المهاجمين لتنفيذ انشطتهم دون عواقب قانونية جادة، الا ان البرلمان العراقي ادرك مؤخرا أهمية الامن السيبراني مما جعله يطرح مشروع قانون جرائم المعلوماتية وذلك في نوفمبر/2023 فقد نصت المادة السادسة من القانون عللا " يعاقب كل من حاول استخدام شبكة المعلومات لتكدير الامن والنظام العام للسجن المؤبد او غرامة تتراوح بين 25-50 مليون دينار عراقي" وتسعى الحكومة الحالية الى تحسين فعاليتها وخدماتها من خلال تبني التقنيات الرقمية، كما انها سعت الى تطوير الحكومة الرقمية من خلال اصدار استراتيجياتها في اطار نظمها السياسية والتي تمثل ب الاتي: (صليبي، 2024، ص517)

1. حماية البنية التحتية للمعلومات الحيوية الوطنية من خلال تقييم المخاطر التي تواجهها البنية التحتية للمعلومات ووضع إطار زمني لإدارة هذه المخاطر.
2. الاستجابة للحوادث والهجمات الالكترونية وحلها والتعافي منها من خلال تداول المعلومات في الوقت المناسب.
3. وضع إطار قانوني وتنظيمي التي تعمل على دعم الاستخدام الامن للفضاء الالكتروني.
3. تطوير الإمكانيات الوطنية للأمن السيبراني.
5. تنمية الوعي بالمخاطر السيبرانية والحلول المتاحة وتعزيز استخدام المنتجات والتكنلوجيا الموثوق بها.

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

أما فيما يخص وضع العراق مقارنة بدول العالم في مجال الامن السيبراني، فأن مؤشر الامن السيبراني العالمي الذي يعمل من خلال جمع 25 معيارا في مقياس واحد لمراقبة التزام 193 دولة عضو في الاتحاد الدولي للاتصالات والأمن السيبراني ومن خلال خمسة ركائز أساسية، حيث اوضح وضع العراق من ضمن هذا المؤشر والجدول ادناه الركائز التي تتعلق بموقف العراق في مجال الامن السيبراني.

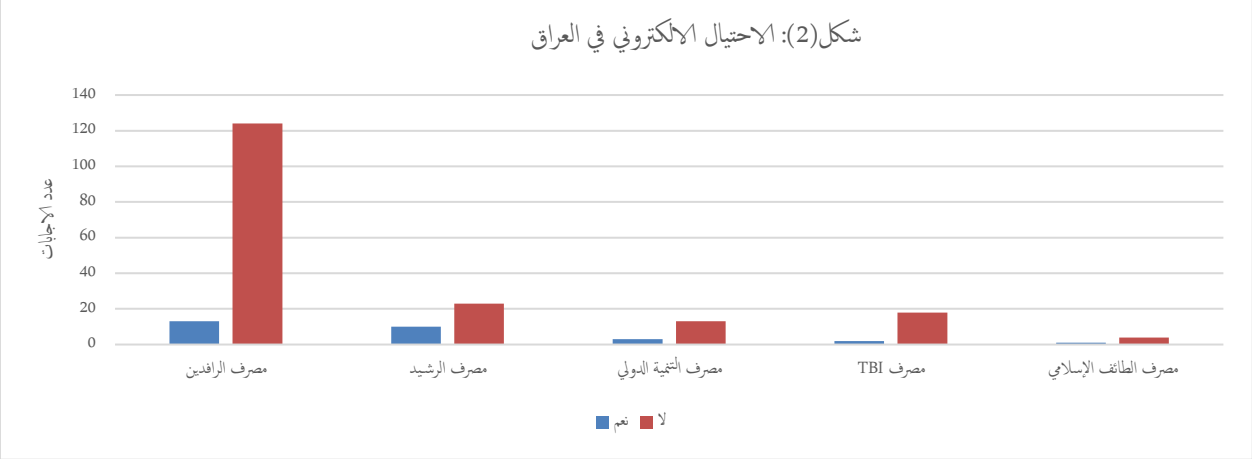
جدول رقم 4: موقف العراق في مؤشر الامن السيبراني العالمي

قانوني	اصطلاحي	تنظيمي	سعة مبنى	تعاون	المجموع
0.000	6.56	7.75	2.14	4.6	20.7

المصدر: أستاذ المساعد سلمان عبود زبار، المتطلبات الازمة لدعم نظام المعلومات الإدارية لمواجهة التهديدات السيبرانية في البنك التجاري العراقي، المجلة القانونية الروسية، مجلد11، عدد3، ص739، 2023.

بحسب النسخة الصادرة عن الاتحاد الدولي للاتصالات لعام 2021 فأن أمريكا تحتل المرتبة الأولى على العالم في مجال الامن السيبراني والسعودية بالمرتبة الثانية ويأتي العراق بالمركز 129 عالميا و17 عربيا.

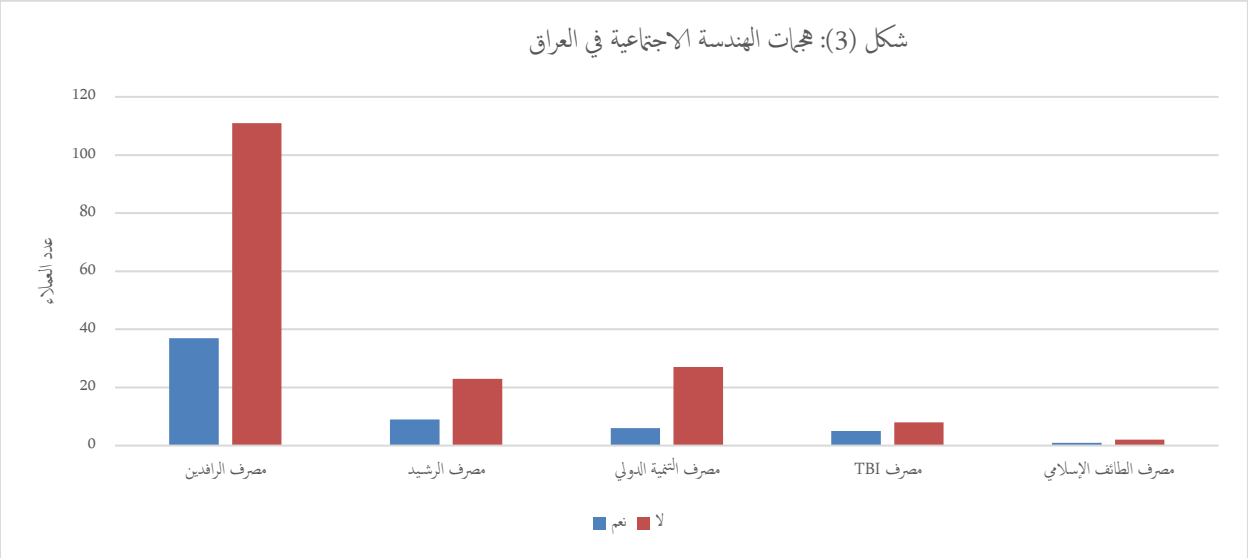
نظرا لانعدام البيانات حول التهديدات السيبرانية على المصارف العراقية لجأت بعض الدراسات الى أسلوب الاستبانة منها دراسة اقيمت في عام 2022 على خمسة مصارف عراقية ضمن القطاع الخاص والتي تضمنت أسئلة مثل (هل كنت ضحية للاحتيال الالكتروني؟) و (هل تعرضت لاحد هجمات الهندسة الاجتماعية؟) وكانت النتائج تتمثل بأن 15% من العملاء تعرضوا الى هجمات الاحتيال الالكتروني والذين أجابوا بجواب (نعم) اما النسبة المتبقية 85% أجابوا ب (لا) أي لم يتعرضوا لمثل هذا النوع من الهجمات، الرسم البياني ادناه يبين بشكل أوضح النتائج.



المصدر/ قصي زهير ومصطفى ضياء، استخدام المستهلك للخدمات المصرفية الالكترونية في العراق: الخروقات الأمنية والعروض، المجلة العراقية للعلوم، مجلد:63، عدد:8، ص3666، 2022.

اما فيما يخص السؤال الثاني توضح النتائج أن 26% من العملاء تعرضوا لهجمات الهندسة الاجتماعية والذي أجابوا ب (نعم)، اما ما نسته 74% أجابوا بكلمة (لا) أي لم يتعرضوا لمثل هذا النوع من الهجمات، والرسم البياني ادناه يبين بشكل أوضح نتائج هجمات الهندسة الاجتماعية.

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9



المصدر/ قصي زهير ومصطفى ضياء، استخدام المستهلك للخدمات المصرفية الالكترونية في العراق: الخروقات الأمنية والعروض، المجلة العراقية للعلوم، مجلد:63، عدد:8، ص3667، 2022.

ومن أجل الاطلاع بشكل اقرب من وضع الامن السيبراني في المصارف العراقية، فقد قمنا بزيارة ميدانية لأحد المصارف العراقية الخاصة (مصرف الناسك الإسلامي) وبناءا على لقائنا مع مسؤول قسم أمن المعلومات في المصرف فقد ذكر لنا بأن المصرف قد تعرض الى هجمات الحرمان من الخدمة وذلك في شهر الثاني والرابع من سنة 2024 وأيضا الالاف من رسائل البريد الالكتروني التي تحمل برامج ضارة، لكن كانت هذه الهجمات فاشلة ولم يستطع المهاجمون من ألحاق الضرر بعمليات المصرف بفضل استثماره ببرامج anti-virus من شركة Trend Micro والتي منعت مثل هذه الرسائل من الوصول الى أجهزة المصرف.

وعلى الرغم من سعي الحكومة العراقية بعمل توازن بين التحول الرقمي الحديث في مؤسساته وبين تعزيز مرونة الامن السيبراني فيها، ألا انها محاولات فقيرة ومازال الامن السيبراني في العراق ضعيف، لذا على البنك المركزي العراقي الاهتمام بتجارب الدول المتقدمة في مجال الامن السيبراني والاستفادة من الاستراتيجيات المتبعة لهذه الدول لضمان سلامة وأمن القطاع المصرفي العراقي.

النتائج

1. توصل البحث الى حقيقة مفادها ان التهديدات السيبرانية بكافة أنواعها لها تأثير مباشر على الاستقرار النظام المالي في القطاع المصرفي.
2. ان المهاجمون السيبرانيون في تحديث مستمر لطرقهم وادواتهم مع كل استحداث لاستراتيجيات المصارف في التصدي لهجماتهم.
3. أن حجم التهديدات السيبرانية يرتبط بحجم العمليات المالية في المصرف، فكلما كان حجم المصرف كبير كلما زادت الهجمات السيبرانية حيث يكون البنك هدفا لأطماع المهاجمين.
4. يقوم البنك الفيدرالي الهندي بالاستفادة من اراء الخبراء في الأسواق المالية الهندية فيما يخص المخاطر السيبرانية وتحليلها والعمل على تفادي وقوعها مستقبلا، الا ان المخاطر السيبرانية في المصارف الهندية غير مستقرة وفي حالة ارتفاع وانخفاض يرجع السبب الى ضخامة حجم المصارف الهندية من ناحية العمليات المالية الالكترونية.

التوصيات

1. جذب نظر البنوك المركزية في دول العالم بصورة عامة والدول النامية بصورة خاص في الاستفادة من هذه التجارب من خلال الاطلاع على اهم الاستراتيجيات المستخدمة من قبل البنك الاحتياطي الهندي والبنك المركزي للاتحاد الروسي وغيرها من البنوك التي استخدمت استراتيجيات قوية قللت من أثر هذه التهديدات على قطاعها المصرفي وتعزيز مرونة الامن السيبراني في بنوكها.
2. ضرورة الإفصاح عما تتعرض له المصارف من تهديدات لرفع الوعي بالأمن السيبراني لدى المصارف والعملاء.
3. وجوب التحديث المستمر للاستراتيجيات وتوجيهات الامن السيبراني بما يتلاءم والتطورات الحاصلة في أدوات المهاجمين.

الخلاصة

أن التطور التكنلوجي في العالم الحديث مستمر وبشكل مخيف وعلى الرغم من هذه التطور له العديد من الفوائد التي تعود على القطاع المصرفي من حيث سرعة انجاز العمل وتقليل التكاليف، ألا انه هناك مضار فعلية ناتجة عن هذه التطورات في التكنلوجيا المصرفية والتي سببت مضار على استقرار النظام المالي في القطاع المصرفي، وبسبب الدور المهم التذي تؤديه المصارف في اقتصاد أي دولة لذلك فانه استقراره قضية مهمة يجب الاهتمام بها، ومع تطور التكنلوجيا المصرفية

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

تتزايد الهجمات السيبرانية على اعمال القطاع المصرفي مع تطور مستمر في أدوات وتقنيات المستخدمة في هذه الهجمات، لذلك فان الهدف الرئيسي من الامن السيبراني او امن المعلومات في الخدمات المصرفية الرقمية له أهمية كبيرة في توفير تدابير السلامة لاستمرار أعمال البنوك وحماية بيانات العملاء من الأموال الرقمية مثل بوابات الدفع الالكتروني كبطاقات الائتمان وبطاقات الخصم.

Funding

None

Acknowledgement

None

Conflicts of Interest

The author declares no conflict of interest.

Arabic References:

التميمي، حيدر كاظم نصر الله التميمي، تأثير جائحة (COVID-9) على الاستقرار المالي وضرائب الدخل في المصارف التجارية، مجلة الدراسات الاقتصادية والإدارية، العدد 27، تموز 2022.

2. هاشم، نورا رعد هاشم، أثر تطبيق ابتكارات التكنلوجيا المالية (FinTech) على تنمية المؤسسات المالية في العراق، مجلة الدراسات الاقتصادية والإدارية، مجلد4، العدد 1، اذار 2025.

3. البنك الاحتياطي الهندي تقارير الاستقرار المالي ,2024. http://www.rbi.org.in/

4. الموقع الرسمي للبنك المركزي للاتحاد الروسي، قسم أمن المعلومات، التحليلات. /https://www.cbr.ru/eng/information_security/analitics

English References:

Abdul-Ridha, Mustafa; Karim, Haider; Harjan, Stan. (2020), Financial Technology and Its Role in Achieving Sustainable Development: A Survey Study of a Sample of Baghdad Commercial Bank Employees, Cihan University Journal, Vol. 4.

Q. Stanikzai and M. A. Shah, "Evaluation of Cyber Security Threats in Banking Systems," 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 2021, pp. 1-4, doi: 10.1109/SSCI50451.2021.9659862.

Abdulbasit. A & Asma A. & Tareq M. & Abdullah M. & Sultan M. & Shouki A, Cyber threats classifications and countermeasures in banking and financial sector, IEEE Access journal, p:18, 2023.

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

Achim, Monica Achim, Economic and Financial Crime, Sustainability and Good Governance, Springer Nature Switzerland, ISBN 978-3-031-34082-6 (eBook), 2023.

Akhmad G. & Muhlies T. & Charlista A. & Sophia A. &Ahmad Z. & Selvira Cahyani, Latest Challenges and Trends in Network Security: Facing Cyber Threats in the Digital Era, Journal of Artificial Intelligence and Engineering Applications, 15th June 2024. Vol. 3. No. 3; e-ISSN: 2808-4519, 2024.

Alexandru & Oros Anu, Cyber: A new challenge of criminality in the digital age, Proceeding of the international conference on cybersecurity and cybercrime, Vol. XI, P:120, 2024.

Aslan, Ö.; Aktu˘ g, S.S.; Ozkan-Okay, M.; Yilmaz, A.A. Akin, E. A Comprehensive Revie of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics 2023, 12, 1333. https://doi.org/10.3390/electronics12061333

Asma A.& Abdullah M. & Abdulbasit A.& Abdullah F. & Rachid Effghi, An Ensemble-based Fraud Detection Model for Financial Transaction Cyber Threat Classification and Countermeasures, Engineering, Technology & Applied Science Research Vol. 13, No. 6, p:12438, 2023.

Burra Buchi, Cyber security in bank, The journal of Indian institute of banking and finance, Vol. 89, No.01, p:30, 2018.

Chandra. S & Manojkumar. K, An overview of cyber security in digital sector, East Asian journal of multidisciplinary Research (EAJMR), Vol.2, No.1, P: 48, 2023.

https://ieeexplore.ieee.org/document/9659862

Juan. C & Jefferson. U & Jemry. P, Banks cyber security second generation of regulatory approaches, Bank for international settlement, p:4, 2023.

KHUSHWANT S.& MISTREAN L.& YUDHVIR S.& DHEERDHWAJ B.& ABHISHEK P., FRAUD PREVENTION IN DIGITAL PAYMENT SYSTEMS AND CYBERSECURITY EDUCATION FOR CUSTOMERS OF NATIONALIZED FINANCIAL INSTITUTIONS, VIRTUAL INTERNATIONAL SCIENTIFIC CONFERENCE "DEVELOPMENT THROUGH RESEARCH AND INNOVATION, h Edition, online conference for young researchers, PhD Students and Post-Doctoral Researchers, Chisinau, Republic of Moldova, 2023.

Md Anwarul & Md Sheam & Rashedul I.& M Shahariar & Muhammad S. & Faysal Hossen, Ai-Powered Cybersecurity in Financial Institutions: Enhancing Resilience Against Emerging Digital Threats, Advanced International Journal of Multidisciplinary Research, Volume 2, Issue 6, November-December 2024.

Mih ret. S & Rajesh. S, Cyber-attack and measuring its risk, Adama science and technology university, IRO journal on sustainable wireless system, Vol.3, No.4, p:222, 2021.

Mohammed Fareed Mahdi, Shared Cybersecurity Responsibilities in the Banking Sector: A Case Study of the Republic of Iraq, Journal of Education for Pure Science- University of Thi-Qar Vol.14, No. 4, P:130, 2024.

Rania Aboalela & Abrar Alsayede, Cyber Security Threats and Protection Technologies for Al Rajhi Bank, King Abdulaziz University, Rabigh, Saudi Arabia, P:33, 2023.

EISSN: 3005-3625, PISSN: 2790-2560, DOI: doi.org/10.58564/EASJ/5.2.2026.9

Tim. M & Arthur. N, Cyber threats to the financial system are Gowing and the global community must cooperate to protect it, finance and development march 2021.

Website: https://ioinformatic.org/

Williams H. & Toyin A. & Ajao Y., Defending against cybersecurity threats to the payment and banking system, Bournemouth university, United Kingdom, 2022.