أثر الأمن السيبراني في تأمين الأنظمة الرقمية المطبقة بميناء دمياط

إعداد
إيهاب أحمد عبد الباقي السيد حجازي [١]، علاء عبد الباري [٢]، نبيل محمود احمد [٣]
[١] هيئة ميناء دمياط
[٢،٣] الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

DOI NO. https://doi.org/10.59660/527223
Received 05/09/2025, Revised 04/10/2025, Acceptance 19/11/2025, Available online 01/07/2026

Abstract

This study aims to analyze the impact of cybersecurity on enhancing the safety of digital systems applied at Damietta Port by examining the three main dimensions of information security: data confidentiality, data integrity, and data availability. The importance of the study arises from the increasing challenges facing the maritime transport industry regarding the protection of operational systems and the security of sensitive information amid the global rise in cyberattacks. The research problem stems from the high financial costs incurred by maritime institutions in implementing cybersecurity measures, in addition to the scarcity of studies addressing its impact within seaport environments, according to the researcher's review.

The study adopted the descriptive-analytical methodology, collecting data through a questionnaire designed to measure the extent and direction of cybersecurity's influence on maintaining digital operational systems in ports. The sample included no fewer than 250 participants working in the field. The results indicated that implementing cybersecurity policies is a critical factor in ensuring the safety and continuity of digital systems, thereby reducing downtime in automated operational processes. It was also found that employee training and the enhancement of cybersecurity awareness contribute to minimizing human errors and strengthening the stability of the information security system. The study further emphasized the importance of adopting advanced systems for early detection and rapid response to threats, which enhances resilience, reduces losses, and improves the operational efficiency and competitiveness of the port.

المستخلص

يهدف هذا البحث إلى تحليل أثر الأمن السيبراني في تعزيز سلامة الأنظمة الرقمية المطبقة في ميناء دمياط، من خلال دراسة الأبعاد الثلاثة الرئيسة لأمن المعلومات، وهي: سرية البيانات، وسلامة البيانات، وتوافر البيانات. تأتي أهمية الدراسة في ضوء ما تشهده صناعة النقل البحري من تحديات متزايدة تتعلق بحماية الأنظمة التشغيلية وتأمين المعلومات الحساسة في مواجهة تنامي الهجمات السيبرانية عالميًا، انبثقت مشكلة البحث من ارتفاع التكلفة المالية التي تتحملها المؤسسات البحرية مقابل تطبيق تدابير الأمن السيبراني، إضافة إلى ندرة الدراسات التي تناولت أثره في بيئة الموانئ البحرية – وفقًا لمطالعات الباحث.

استخدمت الدراسة المنهج الوصفي التحليلي، حيث جمعت البيانات من خلال استبانة صُممت لقياس درجة واتجاه تأثير الأمن السيبراني في الحفاظ على الأنظمة التشغيلية الرقمية بالموانئ، وشارك فيها ما لا يقل عن (٢٥٠) فردًا من العاملين في المجال، وأظهرت النتائج أن تطبيق سياسات الأمن السيبراني يمثل عاملًا حاسمًا

في ضمان سلامة واستمرارية الأنظمة الرقمية، بما يحد من توقف العمليات التشغيلية المميكنة، كما تبين أن تدريب العاملين ورفع مستوى الوعي السيبراني يسهمان في تقليل الأخطاء البشرية وتعزيز استقرار منظومة أمن المعلومات، وأكدت علي أهمية تبني أنظمة متقدمة للكشف المبكر والاستجابة السريعة للتهديدات، بما يعزز القدرة على المواجهة، ويخفض الخسائر، ويرفع الكفاءة التشغيلية والتنافسية للميناء.

١. المقدمة

الموانئ البحرية أحد الأعمدة الرئيسية في دعم الاقتصاد الوطني والدولي، إذ تمثل شرياناً حيوياً لحركة التجارة العالمية، ومصدراً رئيسياً للإيرادات الاقتصادية، ومحركاً للتنمية المستدامة، ويعد ميناء دمياط نموذجاً متطوراً ضمن منظومة الموانئ المصرية الحديثة، حيث يتميز بموقعه الجغرافي الاستراتيجي على البحر المتوسط، وبنيته التحتية المتقدمة، وتنوع محطاته التشغيلية التي تشمل الحاويات، والصب الجاف والسائل، والبضائع العامة، والبتروكيماويات، مما جعله من الموانئ المحورية في شرق المتوسط (البديوى محمد واخرون، ٢٠٢٤). ومع ذلك، فإن التنافس الإقليمي والدولي المتصاعد بين الموانئ يتطلب مواكبة التطور التقني والتحول الرقمي في إدارة العمليات البحرية واللوجستية لضمان استدامة الأداء التشغيلي وتعزيز الكفاءة التشغيلية. (المطيري، ٢٠٢١)

الرقمنة والتحول الرقمي في الموانئ البحرية أصبحت شرطاً أساسياً لتحقيق الكفاءة التشغيلية، غير أن هذا التحول يقترن بتحديات أمنية معقدة تتعلق بحماية الأنظمة الرقمية من الهجمات السيبرانية التي قد تعطل حركة الملاحة والتجارة، وتبرز من هنا أهمية تطبيق استراتيجيات الأمن السيبراني لضمان سرية البيانات وسلامتها وتوافرها، وهو ما أشار إليه Lehto و Neittaanmäki (2015) باعتباره الإطار الثلاثي الأساسي لحماية المعلومات، كما تشير الدراسات الحديثة إلى أن الاستثمار في الأمن السيبراني يسهم في تعزيز الأداء التشغيلي واستقرار الأنظمة الرقمية في الموانئ (Adabere et al., 2021& Lee, 2021) كما أثبتت تقارير دولية مثل تقرير Cisco (2017) أن المؤسسات التي تطبق سياسات أمنية قوية تحقق مستويات أعلى من الثقة والاستدامة التشغيلية، مما يجعل الأمن السيبراني عنصراً محورياً في نجاح التحول الرقمي بالموانئ الذكية.

٢. مفهوم وأبعاد الأمن السيبراني

يعرف الأمن السيبراني بأنه مجموعة من الإجراءات والاستراتيجيات التقنية والتنظيمية الهادفة إلى حماية الشبكات والأنظمة الرقمية والبيانات من أي وصول أو استخدام أو تعديل أو تدمير غير مصرح به، ويشمل حماية أجهزة الحاسب الآلي والهواتف الذكية والأنظمة الإلكترونية وشبكات الإنترنت من الهجمات الخبيثة والجرائم الإلكترونية. ويعد من أهم متطلبات التحول الرقمي بالمؤسسات الحديثة، إذ يسهم في تحقيق الأمان المعلوماتي وضمان استمرارية الأعمال والحد من المخاطر التشغيلية. ويعتمد الأمن السيبراني على مبادئ أساسية تشمل السرية، السلامة، والتوافر، وهي العناصر التي تشكل الإطار العام لحماية الأصول الرقمية من التهديدات المتزايدة (العمارات والحمامصة، ٢٠٢٢؛ قنديل، ٢٠٢٣؛ Gotam & Verma, 2015)

تستند منظومة الأمن السيبراني إلى أربعة أبعاد رئيسية تتكامل فيما بينها لتحقيق الحماية الشاملة، وتشمل حماية البيانات من خلال التشفير، والنسخ الاحتياطي، وحوكمة البيانات؛ والتحكم في الوصول عبر المصادقة متعددة العوامل وتطبيق أنظمة إدارة الهوية؛ والكشف والاستجابة للتهديدات باستخدام أنظمة كشف ومنع التسلل ومراكز العمليات الأمنية وتقنيات الذكاء الاصطناعي؛ وتدريب وتوعية المستخدمين لضمان رفع الوعي

بالمخاطر الإلكترونية وتقليل الأخطاء البشرية التي تشكل مدخلًا رئيسيًا للهجمات السيبرانية، وتمثل هذه الأبعاد مجتمعة الأساس لبناء منظومة دفاعية فعالة تضمن حماية الأنظمة الرقمية بالمؤسسات الحيوية مثل الموانئ البحرية. (Stallings, 2019 & Cram, 2017)

٣. الهجمات السيبرانية – Cyberattacks

الهجمات السيبرانية من أخطر الظواهر الإجرامية المعاصرة التي نشأت مع التطور التكنولوجي والعولمة، إذ تعتمد على تقنيات رقمية متقدمة لاختراق الأنظمة المعلوماتية واستهداف الشبكات والبيانات، مما يجعلها في حالة تطور مستمر مع تطور التكنولوجيا (نمدلي، ٢٠١٧). وتتعدد أنواعها لتشمل التهديدات الموجهة إلى الشبكات، والحواسيب، والبيانات، والاستغلال غير المشروع للمعلومات (حياة ونسيمة، ٢٠٢٢). وقد أصبحت الجرائم الإلكترونية من أكبر التحديات التي تواجه المؤسسات حول العالم، إذ تُقدّر خسائرها العالمية بنحو 6 تريليونات دولار سنويًا عام ٢٠٢١ مقارنة بـ٣ تريليونات عام ٢٠١٥، وفقًا لتقرير Cybersecurity Ventures.

١.٣ انواع الهجمات السيبرانية

تتنوع الهجمات السيبرانية في أساليبها وأهدافها تبعًا لتقنيات المهاجمين ودرجة الحماية للضحايا (Li et al.,2021) ومن أبرز أنواعها البرمجيات الخبيثة (Malware) التي تشمل الفيروسات وبرامج التجسس والإعلانات القسرية، وتستخدم لاختراق الأنظمة وسرقة البيانات، كما تعد هجمات التصيد (Phishing) من أكثر الأساليب شيوعًا في سرقة المعلومات الحساسة عبر البريد الإلكتروني أو الروابط المزيفة (Oest et al., 2020) ويضاف إليها هجمات الهندسة الاجتماعية (Social Engineering) التي تستغل العامل البشري بالخداع والإقناع لتنفيذ عمليات غير آمنة (Jansen & van Schaik, 2019) .

تأتي هجمات حجب الخدمة (DoS/DDoS) ضمن الهجمات المدمرة التي تعطل البنية التحتية الرقمية بإغراق الخوادم بطلبات وهمية (Mahjabin et al., 2017) ، وتعد برامج الفدية (Ransomware) من أخطر الهجمات، حيث تشفر بيانات الضحايا ويطلب فدية مالية ضخمة لاستعادتها، مما يسبب خسائر مالية وسمعة مؤسسية جسيمة.(Beaman et al., 2021)

٢.٣ إدارة المخاطر السيبرانية – Cyber risk

إدارة المخاطر السيبرانية من الركائز الأساسية لحماية الأنظمة الرقمية وضمان استمرارية الأعمال، إذ تمثل عملية منهجية تتضمن تحديد المخاطر، تحليلها، تقييمها، ومراقبتها بهدف الحد من تأثيرها وتقليل الخسائر المحتملة (الرحماوي، ٢٠٢٤). تعتمد هذه الإدارة على تبني نهج استباقي يسمح للمنظمات بالتعامل مع التهديدات قبل تفاقمها من خلال تطوير خطط استجابة فعّالة وتحديثها بانتظام. كما يمكن تطبيق إدارة المخاطر السيبرانية على المستويين الاستراتيجي والتشغيلي داخل المؤسسات، بما يعزز من قدرة المنظمة على حماية بياناتها وأنظمتها التشغيلية، وتحقيق التوازن بين الكفاءة التقنية والأمان المعلوماتي في مواجهة الهجمات المتزايدة والتطور المستمر في أساليب التهديدات الرقمية.

٣.٣ أثر الهجمات السيبرانية على صناعة النقل البحري

تمتد آثار الهجمات السيبرانية على صناعة النقل البحري لتشمل شبكات سلسلة التوريد البحرية (MSCN) التي تعتمد على ترابط عناصر متعددة تشمل الوكلاء الملاحيين وشركات الشحن والتفريغ وسلطات الموانئ ومقدمي

الخدمات، مما يزيد من احتمالية انتشار نقاط الضعف السيبرانية (Mesa et al., 2024) هذا الترابط بين الأنظمة القديمة والحديثة يؤدي إلى تفاوت في نضج الأمن السيبراني ويضعف من قدرة الشبكة على التصدي للهجمات، وهو ما ظهر في حوادث عالمية مثل هجوم الفدية على ميناء ناغويا (٢٠٢٣) وهجوم NotPetya على شركة ميرسك (٢٠١٧) الذي تسبب في خسائر بملايين الدولارات وتوقف العمليات التشغيلية لعدة أيام.

ورغم اعتماد المؤسسات البحرية على أطر أمنية مثل إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا (NIST) وإرشادات المنظمة البحرية الدولية(IMO) ، إلا أن الحاجة لا تزال قائمة لتعزيز التعاون الدولي وتطوير بروتوكولات موحدة ترفع الوعي السيبراني وتحد من تأثير هذه الهجمات على أمن واستدامة سلاسل التوريد البحرية.

٤. تأمين الأنظمة الـرقمية (أمن المعلومات)

١.٤ مفهوم تأمين الأنظمة الـرقمية (أمن المعلومات)

يمثل مفهوم تأمين الأنظمة الرقمية (أمن المعلومات) أحد الركائز الأساسية لتحقيق التحول الرقمي الآمن في المؤسسات الحيوية، إذ يشير إلى مجموعة الإجراءات الإدارية والفنية الرامية إلى حماية البيانات والأنظمة من الوصول غير المصرح به أو التعديل أو الإتلاف أو السرقة، بما يضمن سرية المعلومات وسلامتها وتوافرها. وقد تنوعت الرؤى الدولية حول أمن المعلومات كما عرضتها الأمم المتحدة، حيث ركزت الولايات المتحدة والمملكة المتحدة على الجانب التقني لحماية البيانات، بينما تناولت الصين وروسيا وأرمينيا وأوكرانيا الأبعاد السياسية والاقتصادية والاجتماعية للأمن المعلوماتي، مما يعكس شمولية المفهوم وارتباطه بالأمن القومي للدول.(Maurer & Morgus, 2022)

٢.٤ أهم الأنظمة الرقمية المطبقة بميناء دمياط:

يمثل ميناء دمياط نموذجًا متقدمًا في مجال التحول الرقمي بالموانئ المصرية، إذ تبنى تطبيق أحدث الأنظمة الرقمية التي تسهم في رفع الكفاءة التشغيلية، وتقليل الأخطاء البشرية، وتحقيق التكامل بين الجهات الحكومية والمجتمع المينائي، فقد تم تطوير البنية التحتية المعلوماتية للميناء لتشمل مراكز بيانات حديثة عالية الكفاءة، وشبكات اتصالات سلكية ولاسلكية مؤمنة بتقنية الألياف الضوئية، بما يضمن استمرارية العمل واستقرار الأنظمة. كما تم تطبيق نظام النافذة الواحدة (PSW) لتسهيل إجراءات تداول البضائع والإفراج الجمركي إلكترونيًا، مدعومًا بتقنية Blockchain لضمان الحماية والشفافية.

تشمل الأنظمة الأخرى منظومة التعرف الآلي (RFID) لتتبع الشاحنات والمعدات، ومنظومة تخطيط الموارد (ERP) التي تدير عمليات الموارد البشرية والمخازن والمشتريات إلكترونيًا، بالإضافة إلى منظومة الربط الحكومي (G2G) التي تتيح تبادل البيانات مع الجهات الرسمية مثل مصلحة الضرائب والجمارك والتموين. كما تم تطبيق أنظمة إدارة الحاويات(NAVIS N4) ، ومنظومة الدفع الإلكتروني والتكامل البنكي لتسريع عمليات السداد والتحصيل، إلى جانب البوابة الرقمية لميناء دمياط التي تتيح للعملاء تنفيذ معاملاتهم إلكترونيًا في بيئة مؤمنة بالكامل.

وبذلك، يُعد ميناء دمياط من أوائل الموانئ التي استطاعت بناء منظومة رقمية متكاملة، تجمع بين الكفاءة التشغيلية العالية ومتطلبات الأمن السيبراني، ما يجعله نموذجًا يحتذى به في تطبيق مفهوم "الميناء الذكي."

٥. مشكلة البحث

تتمثل مشكلة الدراسة في قصور الاهتمام البحثي بتأثير تطبيق استراتيجيات الأمن السيبراني في الموانئ البحرية مقارنةً بالقطاعات المالية والمصرفية التي تناولتها دراسات سابقة مثل السرحان (٢٠٢٠)، والزيود (٢٠٢١)، وحسين (٢٠٢٢)، وعبد القادر وآخرون (٢٠٢٣)، والتي أكدت دور الأمن السيبراني في حماية البيانات وتقليل المخاطر وتعزيز الأداء المؤسسي، ورغم التحول الرقمي الواسع في الموانئ المصرية، لا سيما ميناء دمياط، ما زال تأثير تطبيق الأمن السيبراني على الكفاءة التشغيلية لهذه الموانئ غير مدروس بشكل كافٍ.

٦. أسئلة البحث:

السؤال الرئيسي: ما أثر الأمن السيبراني في تأمين الأنظمة الرقمية المطبقة بميناء دمياط ؟

ويتفرع من هذا السؤال الرئيسي الاسئلة الفرعية الأتية:

السؤال الفرعي الأول: ما أثر الأمن السيبراني في تأمين سرية بيانات الأنظمة الرقمية المطبقة بميناء دمياط؟

السؤال الفرعي الثاني: ما أثر الأمن السيبراني في تأمين سلامة بيانات الأنظمة الرقمية المطبقة بميناء دمياط؟

السؤال الفرعي الثالث: ما أثر الأمن السيبراني في تأمين توافر بيانات الأنظمة الرقمية المطبقة بميناء دمياط؟

٧. أهداف البحث

تحليل أثر تطبيق الأمن السيبراني في تأمين الأنظمة الرقمية المطبقة بميناء دمياط، وذلك من خلال دراسة مدى مساهمته في حماية البيانات وضمان استمرارية التشغيل الآلي وتعزيز الكفاءة التشغيلية في ظل التحول الرقمي للموانئ.

٨. فرضيات البحث

الفرضية الرئيسية: توجد علاقة ارتباط ذات دلالة إحصائية بين الأمن السيبراني وتأمين الأنظمة الرقمية المطبقة بميناء دمياط. وتنبثق منها عدد من الفرضيات الفرعية وهي كالآتي:

الفرضية الفرعية الأولى: توجد علاقة ارتباط ذات دلالة إحصائية بين الأمن السيبراني وتأمين سرية بيانات الأنظمة الرقمية المطبقة بميناء دمياط.

الفرضية الفرعية الثانية: توجد علاقة ارتباط ذات دلالة إحصائية بين الأمن السيبراني وتأمين سلامة بيانات الأنظمة الرقمية المطبقة بميناء دمياط.

الفرضية الفرعية الثالثة: توجد علاقة ارتباط ذات دلالة إحصائية بين الأمن السيبراني وتأمين توافر بيانات الأنظمة الرقمية المطبقة بميناء دمياط.

٩. أهمية البحث

تنبع أهمية هذا البحث من تركيزه على دراسة استراتيجيات الأمن السيبراني ودورها في حماية الأنظمة الرقمية بالموانئ البحرية، خاصة في ظل التحول المتسارع نحو الرقمنة وميكنة الإجراءات التشغيلية.

١٠. حدود البحث

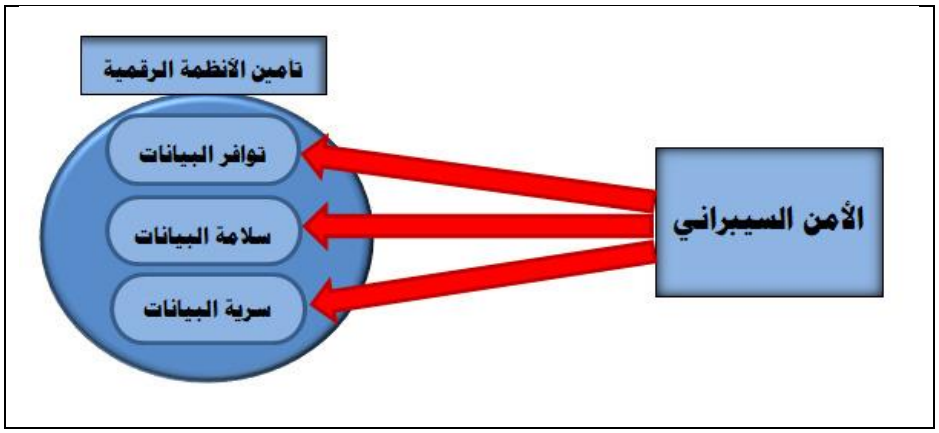
الحدود الموضوعية تشمل: المتغير المستقل "الأمن السيبراني" والمتغير التابع "تأمين الأنظمة الرقمية"

الحدود المكانية: ميناء دمياط البحري.

الحدود الزمنية: خلال النصف الأول من عام ٢٠٢٥.

١١. منهجية البحث

اعتمدت الدراسة على المنهج الوصفي التحليلي، الذي يهدف إلى وصف واقع تطبيق الأمن السيبراني في ميناء دمياط وتحليل مدى تأثيره في تأمين الأنظمة الرقمية المطبقة بالميناء، ويقوم على جمع البيانات الميدانية وتحليلها إحصائيًا لاستخلاص العلاقات بين متغيرات الدراسة وتحديد مستوى التأثير بين الأمن السيبراني وكفاءة الأنظمة الرقمية.



شكل رقم (١): نموذج العلاقة بين متغيرات الدراسة

١٢. عينة البحث

تتكون عينة الدراسة من عينة عشوائية بسيطة تضم مجموعة من العاملين بميناء دمياط في مختلف الإدارات مثل نظم المعلومات، الأمن، الخدمات البحرية، السلامة المهنية، والموارد البشرية، إلى جانب عدد من العملاء والمتعاملين مع الخدمات الإلكترونية التي تقدمها هيئة الميناء بصفة يومية، وذلك بهدف تمثيل مختلف فئات المجتمع المهني المرتبطة بتطبيقات الأنظمة الرقمية داخل الميناء وخارجه.

١٣. ادوات واجراءات البحث

اعتمد البحث على الاستبيان كأداة رئيسية لجمع البيانات من العاملين والعملاء بميناء دمياط لقياس أثر الأمن السيبراني في تأمين الأنظمة الرقمية بالميناء، حيث قام الباحث بمراجعة الدراسات السابقة وإعداد الإطار النظري وتصميم الأداة البحثية وتحكيمها للتأكد من صدقها وثباتها، ثم تطبيقها ميدانيًا وجمع البيانات وتحليلها إحصائيًا وتفسيرها، وصولًا إلى استخلاص النتائج وتقديم التوصيات في ضوء ما توصلت إليه الدراسة.

جدول (١) مجتمع الدراسة والاستمارات الموزعة ونسبة الاستجابة

مجتمع الدراسة	عينة الدراسة	الاستمارات المستردة	الاستمارات غير المستردة والمستبعدة	الاستمارات القابلة للتحليل	نسبة الاستمارات القابلة للتحليل
٢٠٠٠	٣٢٢	٢٦٠	٦٢	٢٢٣	%٦٩.٣

يوضح الجدول أن مجتمع الدراسة بلغ 2000 فرد، وتم اختيار عينة عشوائية من 322 مفردة، استُرد منها 260 استمارة، بينما استبعدت 62 استمارة لعدم صلاحيتها، ليصبح عدد الاستمارات القابلة للتحليل 223 استمارة بنسبة 69.3%، وهي نسبة ملائمة لإجراء التحليل الإحصائي وتمثيل المجتمع الأصلي.

١٤. اختبار صدق وثبات قائمة الاستقصاء

جدول (٢) معاملات ألفا كرونباخ لأبعاد الدراسة

أبعـــــــاد الدراســة	عدد العبارات	معامل ألفا كرونباخ
المتغير المستقل: الأمن السيبراني		
مقياس المتغير المستقل: الأمن السيبراني	١٦	٩٠٨0.
مقياس المتغير التابع: تأمين الأنظمة الرقمية في ميناء دمياط	١٥	٠.٩٢٤
الأثر العام للأمن السيبراني	٦	٠.٨٧٦
المقياس ككل	٣٧	٦٣0.9

يبين الجدول تمتع أدوات الدراسة بدرجة ثبات مرتفعة، حيث بلغت معاملات ألفا كرونباخ لكل من مقياس الأمن السيبراني (٠.٩٠٨) وتأمين الأنظمة الرقمية (٠.٩٢٤) والأثر العام (٠.٨٧٦)، بينما بلغ للمقياس ككل (٠.٩٦٣)، وهي قيم تفوق الحد المقبول إحصائيًا وتؤكد ثبات وموثوقية أدوات القياس.

١٥. نتائج اختبار فروض الدراسة:

جدول (٣) نتائج ملخص نموذج الانحدار المتعدد للفرض الرئيسي والفروض الفرعية

الفرض	المتغير المستقل	معامل B	اختبار t	مستوي المعنوية	F	Sig.
الفرض الرئيسي	ثابت	٢.٣٥٥	٢.٥٥٤	٠.٠١١	F	Sig.
	الأمن السيبراني	٠.٨٤١	٢٥.١٨١	٠.٠٠٠	٦٣٤.٠٨٠	٠٠٠.b
	تأمين الأنظمة الرقمية				R	R Square
					.٨٦٢a	0.٧٤٢
الأثر العام للأمن السيبراني	ثابت	٥.٤٨٤	٦.٣٤٦	0.00٠	F	Sig.
	الأثر العام للأمن السيبراني	١.٩٨٣	٢٣.٤٠٩	0.00٠	٥٤٧.٩٦٦	.٠٠٠b
	تأمين الأنظمة الرقمية				R	R Square
					.٨٤٤a	0.٧١٣

أظهرت نتائج التحليل الإحصائي أن الأمن السيبراني يؤثر بشكل معنوي وقوي على تأمين الأنظمة الرقمية بميناء دمياط، حيث تبين وجود علاقة ارتباط مرتفعة بين الأمن السيبراني وكل من سرية البيانات (R^2 = 0.687)، وسلامة البيانات(R^2 = 0.616) ، وتوافر البيانات .(R^2 = 0.576) كما بينت النتائج أن الأمن السيبراني يفسر نحو ٧٤.٢% من التغيرات في تأمين الأنظمة الرقمية ككل(R = 0.862) ، مما يدل على دوره المحوري في تعزيز الحماية والاستقرار التشغيلي للأنظمة الرقمية بالميناء. كذلك أظهر الأثر العام للأمن السيبراني تأثيرًا جوهريًا بنسبة تفسير بلغت (R^2 = 0.713) 71.3%، وهو ما يؤكد فاعلية تطبيق ممارسات الأمن السيبراني في رفع مستوى أمان الأنظمة الرقمية.

١٦. النتائج العامة للدراسة:

تشير نتائج الدراسة إلى أن الأمن السيبراني يمثل ركيزة استراتيجية لتعزيز تأمين الأنظمة الرقمية بميناء دمياط:

- **الأمن السيبراني يعزز حماية المعلومات الحساسة:** تطبيق ممارسات الأمن السيبراني يرفع من مستوى حماية المعلومات الحساسة ويقلل من المخاطر الناتجة عن الوصول غير المصرح به، ويظهر من الدراسة أن وجود سياسات وإجراءات واضحة للتحكم في استخدام البيانات يعزز قدرة الميناء على منع أي تسرب أو إساءة استخدام للمعلومات.
- **الأمن السيبراني يضمن دقة وصحة المعلومات:** الأمن السيبراني يسهم بشكل فعال في الحفاظ على دقة وسلامة المعلومات المتوفرة داخل الأنظمة الرقمية، ويقلل من احتمالية التلاعب أو الفقدان.
- **الأمن السيبراني يضمن استمرارية الوصول إلى البيانات:** مستوى الأمن السيبراني المطبق يعزز توافر المعلومات بشكل مستمر وبدون انقطاع، مما يدعم العمليات اليومية للميناء ويضمن سرعة التعامل مع المعاملات التشغيلية.
- **الأمن السيبراني يدعم وعي الموظفين وكفاءتهم في التعامل مع التهديدات:** أهمية البعد البشري في منظومة الأمن السيبراني، حيث يسهم التدريب والتوعية المستمرين في رفع وعي العاملين بمخاطر الممارسات غير الآمنة ويحد من الأخطاء البشرية التي قد تهدد النظام الرقمي.
- **التحكم الدقيق في الوصول إلى الأنظمة يعزز الأمان الرقمي:** تطبيق سياسات صارمة للتحكم في الوصول إلى الأنظمة الرقمية يسهم في الحد من المخاطر المرتبطة بالتلاعب أو الدخول غير المصرح به.
- **القدرة على الكشف السريع والاستجابة للتهديدات الرقمية:** وجود أنظمة متقدمة للكشف المبكر عن التهديدات والاستجابة الفورية لها يرفع مستوى الحماية ويقلل من تأثير أي هجمات أو اختراقات محتملة.

١٧. مناقشة نتائج الدراسة

تشير نتائج الدراسة إلى وجود أثر معنوي قوي للأمن السيبراني على تأمين الأنظمة الرقمية في ميناء دمياط، بما يشمل سرية وسلامة وتوافر البيانات، وهو ما يتفق مع نتائج الدراسات السابقة مثل عبد الرازق وفتحي (٢٠٢٤)، والمعايطة (٢٠٢٤)، و(2018) .Von Solms et al، التي أكدت أن تطبيق ممارسات الأمن السيبراني يرفع من مستوى حماية المعلومات من خلال السياسات التقنية وبرامج التوعية والتدريب. كما تتوافق النتائج مع دراسات الخاطري والزيتاوي (٢٠٢٤)، والطراونة (٢٠٢٣)، و Taherdoost (2022)التي أبرزت أهمية التشفير وإجراءات المراقبة والتحديث الدوري للأنظمة. وأظهرت الدراسة أن ارتفاع تطبيق الأمن السيبراني يؤدي إلى تحسين واضح في سلامة وتوافر البيانات، مما يعكس فعالية التدابير التقنية

والمؤسسية بالميناء. وتتميز الدراسة الحالية عن سابقاتها بتركيزها على بيئة تشغيلية بحرية محددة، مع تقديم قياسات كمية دقيقة لقوة التأثير عبر معاملات الانحدار (B = 1.983 و(R^2 = 0.742 ، مما يعزز موثوقية النتائج ويؤكد أهمية دمج السياسات المؤسسية والحوكمة الرقمية في تعزيز أبعاد تأمين الأنظمة الرقمية.

المراجع:

- البديوى السيد مح, سامح فرحات السيد, and مختار حبشي. "أثر تطوير المنظومة اللوجستية علي الميزة التنافسية بالموانئ" مقارنة بين ميناء روتردام و دمياط." AIN Journal ٤٧ (٢٠٢٤). DOI NO. https://doi.org/10.59660/47115

- الخاطري، ميثاء مصبح والزيتاوي، ضياء الدين، (٢٠٢٤) " الأمن السيبراني وحماية خصوصية البيانات الرقمية في الإمارات في عصر التحول الرقمي والذكاء الإصطناعي " الندوة الدولية حول التربية الإسلامية والسلام. الكوفة. العدد٤. ص ص ٦٨٣-٦٩٧.

- الرحماوي، رحاب حسني، (٢٠٢٤) "إدارة المخاطر السيبرانية في المجال الاقتصادي" مجلة الأمن القومى والاستراتيجية. القاهرة.المجلد٢. عدد٤، ص ص١٠٤ -١١٥.

- الزيود، محمود سليمان، (٢٠٢١) " أثر التدقيق الداخلي في الحد من مخاطر السيبرانية في البنوك التجارية الأردنية " رسالة ماجستير غير منشورة. جامعة آل البيت، المفرق.

- السرحان، حنين عبد المهدي، (٢٠٢٠) " أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية " رسالة ماجستير غير منشورة. جامعة آل البيت، المفرق.

- الطروانـــة، خلود خلف، (٢٠٢٣) " المعرفة المعلوماتية بمفهوم الأمن السيبراني بين أفراد المجتمع " دراسة ميدانية في منطقة المزار الجنوبي. مجلة الدراسات الأمنية.الكرك. عدد١٩، ص ص١١٤ -١٥٢.

- العمـارات، فـارس محمد والحمامصـه، إبـراهيم محمد، (٢٠٢٢) " الأمـن السـيبراني المفهـوم وتحـديات العصـر" عمان: دار الخليج للنشر والتوزيع.

- المطيري، أحلام عوض، (٢٠٢١) " الموانئ البحرية وأثرها على الاقتصاد السعودي " مجلة حوليات آدب عين شمس. القاهرة. عدد ابريل. مجلد ٤٩. ص ص ٢٠٣-٢١٥.

- المعايطـة، معـن نايـل، (٢٠٢٤) " اسـتراتيجيات الأمـن السـيبراني ودورهـا فـي تعزيـز حمايـة الشـبكات الإلكترونية في البلديات " الكرك: مجلة العلوم الإنسانية والطبيعية.

- جداوي، أميرة هاتف ومسلم، علي ضرغام ومحمد، صفاء تايه ، (٢٠٢٤) " القيادة الرقمية ودورها في تعزيز سلوك الامن السيبراني في المنظمات دراسة تحليلية لآراء عينة من العاملين في المصارف الأهلية في النجف الاشرف " مجلة العلوم الإنسانية والطبيعية. الكوفة. العدد ١. المجلد ٥. ص ص ٦٨١-٧٠١.

- حياة، حميدي ونسيمة، طايلب، (٢٠٢٢) " مدخل مفاهيمي حول الأمن السيبراني " مدار للدراسات الإتصالية الرقمية. الجزائر. العدد ٢. المجلد ٢. ص ص ١-١٦.

- عبد الرازق، برادة وفتحي، القصير، (٢٠٢٤) " الأمن السيبراني ودوره في الحد من الهجمات الإلكترونية " المركز المغاربي شرق أدنى للدراسات الإستراتيجية . الجزائر. ص ص ٢٣٠-٢٤٢.

- محمد، ملك، (٢٠١٦) " استراتيجية إدارة أمن المعلومات " مقاربة نظمية مع استشراف تطبيقات المعيار الدولي. رسالة دكتوراة غير منشورة. جامعة الجزائر، الجزائر.

- عبد القادر، صواق وبومدين، بوداود وعبد اللطيف، أولاد حيمودة، (٢٠٢٣) " أثر جاهزية الأمن السيبراني على الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة دراسة حالة بنك Bdl بغرداية " مجلة ابحاث اقتصادية معاصرة. الجزائر. العدد ١. المجلد ٦. ص ص ٣٥٣-٣٧٢.

- نمديلي، رحيمة، (٢٠١٧) " خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة " المؤتمر الدولي الرابع عشر حول الجرائم الإلكترونية. طرابلس. ص٥.

- قنديل، اشرف عبدالقادر، (٢٠٢٣) " آليات تحقيق الأمن المعلوماتي في دولة الإمارات العربية المتحدة: مجلة الفكر الشرطى " دبي. العدد ١٢٦. المجلد٣٢. ص ص ١٨٥ -٢٢٩.

- Adabere, S., Kwateng, K. O., Dzidzah, E., & Kamewor, F. T. (2021). Information technologies and seaport operational efficiency. Marine Economics and Management, 4(2), 77–96.

- Beaman, C. P. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. Computers & Security, 109, 102387.

- Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. European Journal of Information Systems, 26(6), 605–641. https://doi.org/10.1057/s41303-017-0059-6

- Goutam, R. K., & Verma, D. K. (2015). Top five cyber frauds. International Journal of Computer Application, 119(7), 23–25.

- Jansen, J., & van Schaik, P. (2019). The effectiveness of fear appeal in strengthening the security behaviour of end users. Computers & Security, 80, 1–11.

- Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. Business Horizons, 64(5), 659–671.

- Lehto, M., & Neittaanmäki, P. (Eds.). (2015). Cyber security: Analytics, technology and automation (Vol. 78). Springer International Publishing. https://doi.org/10.1007/978-3-319-18302-2

- Mahjabin, T., Islam, S., & Rahman, M. (2017). A survey of distributed denial-of-service attack, prevention and mitigation techniques. International Journal of Computer Applications, 168(7), 1–9.

- Maurer, T., & Morgus, R. (2022). Compilation of existing cybersecurity and information security related definitions. New America Foundation. https://www.newamerica.org

- Mesa, M. V. C., Patino-Rodriguez, C. E., & Carazas, F. J. G. (2024). Cybersecurity at sea: A literature review of cyber-attack impacts and defenses. Maritime Safety and Security Journal.

- Oest, A., Safei, Y., Doupé, A., Ahn, G. J., Wardman, B., & Tyers, K. (2020). Phish Time: Continuous longitudinal measurement of the effectiveness of anti-phishing blacklists. Proceedings of the 29th USENIX Security Symposium, 379–396.

- Stallings, W. (2019). Cryptography and network security: Principles and practice (8th ed.). Pearson Education.

- Taherdoost, H. (2022). Cybersecurity vs. information security. Procedia Computer Science, 215, 483–487.

- Von Solms, B., & Von Solms, R. (2018). Cybersecurity and information security – what goes where? Information & Computer Security, 26(1), 2–9.