Comprehensive Journal of Science
Volume (10), Issue (38), (Dec, 2025)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) ملحق العدد 38 ديسمبر 2025
ردمد: 3014-6266

مساهمة الأمن السيبراني في حماية الأنظمة والبيانات

دراسة ميدانية على مصرف شمال إفريقيا – مدينة طرابلس

عبد الكريم عبد الوهاب عبد الكريم يحى عمر فكرون

كلية العلوم التقنية سبها

The Contribution of Cybersecurity in Protecting Systems and Data: A Field Study on North Africa Bank – City of Tripoli

AbdelKarim Abdel Wahab AbdelKarim Yahya Omar Fakroun

Faculty of Technical Sciences, Sebha

تاريخ الاستلام:2025/11/12 –تاريخ المراجعة: 2025/12/3– تاريخ القبول: 2025/12/28– تاريخ للنشر :2/8/ 2026

ملخص الدراسة

هدفت دراسة إلى بيان مساهمة الأمن السيبراني في حماية الأنظمة والبيانات في مصرف شمال إفريقيا بمدينة طرابلس، اعتمدت الدراسة على الأمن السيبراني كمتغير مستقل، وحماية الأنظمة والبيانات كمتغير تابع، وتم اختيار عينة عشوائية بسيطة حجمها 97 مفردة، مع تحليل 91 استبياناً باستخدام برنامج SPSS والفاقد 6 استبيانات، واتبعت المنهج الوصفي التحليلي لتفسير العلاقة بين المتغيرات. وتوصلت الدراسة إلى أن الاستمرار في تحديث التقنيات والسياسات دورياً مع إجراء اختبارات اختراق منتظمة للحفاظ على هذا المستوى العالي وضمان الامتثال للمعايير الدولية مثل PCI DSS، وأوصت الاستمرار في إجراء تقييمات دورية للأجهزة والبرمجيات لضمان التوافق مع التطورات التكنولوجية الجديدة والمعايير الأمنية العالمية، وتعزيز التكامل بين الأنظمة من خلال تبني تقنيات سحابية هجينة وتدريب الفرق الفنية لتحسين الأداء والحماية.

الكلمات المفتاحية: الأمن السيبراني – الأنظمة والبيانات – المصرف .

Study Summary

The study aimed to demonstrate the contribution of cybersecurity in protecting systems and data at North Africa Bank in the city of Tripoli. The study relied on cybersecurity as an independent variable and the protection of systems and data as a dependent variable. A simple random sample of 97 individuals was selected, with 91 questionnaires analyzed using the SPSS program, and 6 questionnaires lost. It followed the descriptive analytical approach to interpret the relationship between the variables. It concluded that continuing to update technologies and policies periodically, along with conducting regular penetration tests, is essential to maintain this high level and ensure compliance with international standards such as PCI DSS. It recommended continuing to conduct periodic assessments of hardware and software to ensure compatibility with new technological developments and global security standards, as well as enhancing system integration through the adoption of hybrid cloud technologies and training technical teams to improve performance and protection.

The keywords translated to English: Cybersecurity – Systems and Data - Bank.

مقدمة

في عصر التحول الرقمي السريع، يُعد الأمن السيبراني عنصرًا حيويًا لحماية الأنظمة والبيانات في المؤسسات المصرفية. وتواجه المصارف تهديدات إلكترونية متطورة مثل الاختراقات، والبرمجيات الخبيثة، وهجمات التصيد الاحتيالي. تهدف هذه الهجمات إلى سرقة البيانات المالية الحساسة أو تعطيل الخدمات المصرفية. ويسهم الأمن السيبراني في تنفيذ تقنيات التشفير المتقدمة وجدران الحماية لمنع الوصول غير المصرح به وكما يعتمد على أنظمة الكشف عن الاختراقات والذكاء الاصطناعي للكشف المبكر عن التهديدات ويضمن ذلك استمرارية العمليات المصرفية ويقلل من الخسائر المالية والسمعية الناتجة عن الهجمات بالإضافة إلى ذلك يعزز ثقة العملاء من خلال ضمان سرية وأمان معاملاتهم اليومية. وفي النهاية، يدعم الأمن السيبراني الامتثال للمعايير واللوائح الدولية، مما يقوي الاقتصاد الرقمي ككل.

مشكلة الدراسة:

في ظل التحول الرقمي السريع الذي يشهده القطاع المصرفي، أصبحت التهديدات السيبرانية تشكل خطرًا حقيقيًا يهدد أمن الأنظمة وسرية البيانات المالية. وتتسبب الهجمات الإلكترونية مثل الاختراقات والبرمجيات الخبيثة وهجمات التصيد في خسائر مالية ضخمة وفقدان ثقة العملاء، ورغم تزايد الوعي بأهمية الأمن السيبراني، إلا أن العديد من المصارف لا تزال تواجه تحديات في تنفيذ إستراتيجيات حماية فعالة ومحدثة، وأظهرت الدراسات السابقة تركيزًا كبيرًا على التقنيات المتقدمة في الدول المتقدمة، مع إهمال نسبي للسياقات المحلية في الدول النامية، حيث تكمن الفجوة الدراسة في نقص الأبحاث التي تدرس مساهمة الأمن السيبراني في حماية الأنظمة والبيانات في المصارف ضمن الواقع الليبي تحديدًا، ومن هنا جاءت مشكلة الدراسة في السؤال التالي: ما مدى مساهمة الامن السيبراني في حماية الأنظمة والبيانات في المصارف التجارية؟.

أهداف الدراسة:

1. التعرف على الواقع الحالي لتطبيق إجراءات وتقنيات الأمن السيبراني في حماية الأنظمة والبيانات داخل المصارف التجارية محل الدراسة.
2. تحديد الفوائد والإيجابيات الناتجة عن مساهمة الأمن السيبراني في تعزيز حماية الأنظمة والبيانات ومكافحة التهديدات الإلكترونية داخل المصارف التجارية.
3. كشف التحديات والمعوقات التي تواجه تبني وتطبيق إستراتيجيات الأمن السيبراني الفعالة في مجال حماية الأنظمة والبيانات داخل المصارف التجارية محل الدراسة.
4. تقديم توصيات عملية ومقترحات لتعزيز دور الأمن السيبراني وتطويره، بما يساهم في رفع كفاءة حماية الأنظمة والبيانات وتعزيز الأمان المصرفي الرقمي داخل المصارف التجارية.

أهمية الدراسة:

تكمن أهمية الدراسة في تقييم واقع تطبيق إجراءات وتقنيات الأمن السيبراني في حماية الأنظمة والبيانات داخل المصارف التجارية الليبية، كونها تمثل العمود الفقري للنظام المالي وأحد أهم القطاعات الاقتصادية في ليبيا. وتساعد في كشف الثغرات والمعوقات التقنية والبشرية التي تعيق فعالية استراتيجيات الأمن السيبراني، وتقديم حلول عملية لتقليل الخسائر المالية الناجمة عن التهديدات الإلكترونية ورفع مستوى الثقة لدى العملاء. وكما توفر مرجعاً علمياً وعملياً لإدارات المصارف لاتخاذ قرارات مستنيرة بشأن تطوير البنية التحتية الرقمية، واعتماد تقنيات الأمن السيبراني المتقدمة، وتدريب الكوادر على التعامل مع أحدث أدوات الحماية الإلكترونية. وتساهم الدراسة في دعم الجهود الوطنية نحو تعزيز الأمن المالي الرقمي وحماية الاقتصاد الوطني

من مخاطر الجرائم السيبرانية المتزايدة، مما يعزز الاستقرار المالي والثقة في النظام المصرفي، ويساهم في رفع التنافسية والجاذبية الاستثمارية للقطاع المصرفي الليبي في ظل التحول الرقمي المتسارع.

فرضيات الدراسة:

الفرضية الرئيسة الأولى: توجد علاقة ذو دلالة إحصائية عند مستوى دلالة $\alpha = 0.05$ لمساهمة الأمن السيبراني بأبعاده (السرية، السلامة، التوافر، بعد المصادقة) على حماية الأنظمة والبيانات بأبعادها (بعد البنية التحتية التقنية، بعد التشغيلية، بعد المحتوى المعلوماتي) قيد الدراسة.

الفرضية الرئيسة الثانية: لا توجد علاقة ذو دلالة إحصائية عند مستوى دلالة $\alpha = 0.05$ لمساهمة الأمن السيبراني بأبعادها (السرية، السلامة، التوافر، بعد المصادقة) على حماية الأنظمة والبيانات بأبعادها (بعد البنية التحتية التقنية، بعد التشغيلية، بعد المحتوى المعلوماتي) قيد الدراسة.

منهج الدراسة:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، الذي يُعد أسلوبًا شائعًا في البحوث العلمية. ويعتمد هذا المنهج على جمع البيانات من مصادرها المختلفة وتحليلها إحصائيًا لوصف الواقع الحالي بدقة. كما يهدف إلى كشف الحقائق المتعلقة بمساهمة الأمن السيبراني في حماية الأنظمة والبيانات، وتحديد العلاقات بين المتغيرات الرئيسية في الدراسة.

مجتمع وعينة الدراسة.

يتكون مجتمع الدراسة في هذه الدراسة من جميع الموظفين العاملين في المقر الرئيسي لمصرف شمال إفريقيا بمدينة طرابلس. ويبلغ العدد الإجمالي لأفراد هذا المجتمع 176 موظفًا، وهم يشغلون مختلف المستويات والإدارات داخل المصرف. وتم اختيار هذا المجتمع لأنه يمثل الجهة المعنية مباشرة بتطبيق إجراءات الأمن السيبراني وحماية الأنظمة والبيانات المصرفية.

عينة الدراسة.

تتمثل عينة الدراسة في عينة عشوائية بسيطة تشمل موظفين من مختلف المستويات الإدارية في المقر الرئيسي لمصرف شمال إفريقيا. تم توزيع 97 استبانة على أفراد العينة، واسترجاعها كاملة دون نقصان بعد استبعاد 6 استبانات لعدم استيفائها شروط التحليل الإحصائي، تم الاعتماد على 91 استبانة صالحة في عملية التحليل.

حدود الدراسة:

تتمثل حدود الدراسة في الآتي:

1. **الحدود الموضوعية:** اقتصرت الدراسة على مساهمة الأمن السيبراني على حماية الأنظمة والبيانات.
2. **الحدود المكانية:** مصرف شمال إفريقيا الرئيسي طرابلس.
3. **الحدود الزمنية:** تم تطبيق هذه الدراسة في الفترة (من شهر 1 إلى شهر 5 – 2025).

مصطلحات الدراسة:

من أهم المصطلحات الرئيسية التي استخدمت في الدراسة وهي:

1. الأمن السيبراني (Cybersecurity) هو مجال يركز على حماية الأنظمة الحاسوبية، الشبكات، البرامج، والأجهزة الإلكترونية، وخاصة البيانات الرقمية، من الهجمات الإلكترونية، الاختراقات، السرقة، التلف، أو الوصول غير المصرح به. (مروان، 2019).

2. أنظمة البيانات (Data Systems) هي مجموعة متكاملة من المكونات المادية (الهاردوير) والبرمجية (السوفتوير) والعمليات والإجراءات والمبادئ التوجيهية المصممة لجمع ومعالجة وتخزين وإدارة وتوزيع واسترجاع البيانات والمعلومات بشكل منظم وفعال وآمن، (كامل، 2016).

الدراسات السابقة:

1. دراسة بن حامد، (2022). "دور الامن السيبراني في حماية الأنظمة والبيانات دراسة على مجموعة من الشركات الأدوية في الأدن. هدفت الدراسة إلى تحليل دور الأمن السيبراني في حماية الأنظمة والبيانات داخل شركات الأدوية الأردنية، مع التركيز على تقييم فعاليته في مواجهة التهديدات الإلكترونية. استخدمت الدراسة المنهج الوصفي التحليلي لجمع البيانات وتحليلها من خلال استبانة موجهة إلى العاملين في مجال تقنية المعلومات. تم اعتماد عينة قصدية تشمل (142) موظفاً من عدة شركات أدوية أردنية، وتوصلت الدراسة إلى عدة نتائج رئيسية، أهمها وجود علاقة إيجابية ذات دلالة إحصائية بين تطبيق تدابير الأمن السيبراني وارتفاع مستوى حماية الأنظمة والبيانات، مع تحسن ملحوظ في كفاءة الكشف عن الهجمات الإلكترونية وسرعة الاستجابة لها، وكذلك في تحسين موثوقية الأنظمة وتقليل فترات التوقف. وأوصت الدراسة بتعزيز برامج التدريب والتأهيل للعاملين في مجال الأمن السيبراني، وإجراء تدريبات محاكاة دورية للهجمات الإلكترونية لاختبار جاهزية الأنظمة والفرق التقنية.
2. دراسة عزام (2019). "أثر الأنظمة الرقمية في تحسين حماية البيانات المصرفية". دراسة على البنوك التجارية في عمان، هدفت الدراسة إلى تقييم أثر الأنظمة الرقمية في تعزيز حماية البيانات المصرفية، وذلك باعتماد المنهج الوصفي التحليلي عبر جمع البيانات والمعلومات وتحليلها إحصائياً لاستنباط النتائج الأمثل. تم توزيع استبيانات على المسؤولين والعاملين بالبنوك التجارية، مع استخدام أسلوب العينة القصدية من خلال التركيز على القادة الإداريين والمتخصصين في مكافحة الاحتيال والأمن المالي، حيث بلغ حجم العينة (209) مفردة. وأظهرت النتائج أن الأنظمة الرقمية المستخدمة في البنوك تقوم على بنية تحتية تقنية متينة، مما يعزز صعوبة اختراق المهاجمين حتى عند تخطي خطوط الدفاع الأولية، وذلك بسبب حماية البيانات في مصدرها الأساسي. كما خلصت الدراسة إلى توصيات أبرزها ضرورة تبني أنظمة إدارة قواعد بيانات متطورة تدعم خصائص الأمان المدمجة.
3. دراسة حلمي (2023) "أثر الذكاء الاصطناعي في تعزيز حماية الأنظمة البنوك" هدفت الدراسة إلى تحليل أثر الذكاء الاصطناعي في تعزيز حماية أنظمة البيانات المصرفية، وذلك في إطار تطبيقه في البنوك المصرية. استخدمت الدراسة المنهج الوصفي التحليلي، حيث جرى توزيع (162) استبانة على عينة من المحاسبين العاملين في البنوك التجارية. تمت معالجة البيانات المجمعة باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS)، وتوصلت الدراسة إلى قدرة الذكاء الاصطناعي على تنفيذ عمليات التحقيق الأولية وتحديد أولويات التهديدات بالاعتماد على تقييم ذاتي للمخاطر، مما يسهم في الحد من انتشار الهجمات ويخفض حجم الضرر المحتمل على البيانات والأنظمة. كما كشفت النتائج عن إمكانية استخدام الذكاء الاصطناعي في مراقبة سلوك المستخدمين أثناء تعاملهم مع البيانات وتحديد الأنشطة المشبوهة، بالإضافة إلى تطبيق سياسات حماية مرنة تتكيّف مع سياق الاستخدام ودرجة حساسية البيانات.
4. العدلي (2018) "دور الامن السيبراني في الحد من الجرائم الإلكترونية دراسة على ميدانية على البنوك المصرية". هدفت الدراسة إلى تقييم دور الأمن السيبراني في الحد من الجرائم الإلكترونية من خلال دراسة ميدانية على البنوك المصرية. استخدمت الدراسة المنهج الوصفي التحليلي مع عينة عشوائية بلغ حجمها (113) مفردة. وتوصلت النتائج إلى أن البنوك تولي اهتماماً بتعزيز قدرات الكشف المبكر والاستجابة السريعة، مما يساهم في الحد من

الأضرار المالية والمعنوية الناتجة عن الجرائم الإلكترونية. كما أوصت الدراسة بإنشاء منصة موحدة لتبادل المعلومات حول التهديدات الناشئة والتكتيكات المستخدمة من قبل المجرمين الإلكترونيين، وتنفيذ برامج توعوية مستمرة ومكثفة للمستخدمين النهائيين والأفراد.

أوجه التشابه والاختلاف بين الدراسة الحالية والدراسات السابقة:

أولاً: أوجه التشابه

1. المنهجية العلمية : تتفق هذه الدراسة مع جميع الدراسات السابقة في استخدام المنهج الوصفي التحليلي، وهو المنهج الأكثر ملاءمة لوصف العلاقة بين الأمن السيبراني وحماية البيانات.
2. أدوات جمع البيانات : تشترك هذه الدراسة مع دراسات (بن حامد، عزام، حلمي، العدلي) في الاعتماد على الاستبيان كأداة رئيسية لجمع البيانات الميدانية.
3. الوسائل الإحصائية :تلتقي هذه الدراسة مع دراسة (حلمي، 2023) في استخدام برنامج SPSSلتحليل البيانات واستخراج النتائج.
4. الهدف العام :تتقاطع هذه الدراسة مع دراسة (بن حامد) ودراسة (العدلي) في التركيز المباشر على "الأمن السيبراني" كعامل حماية أساسي للأنظمة والبيانات.

ثانياً: أوجه الاختلاف

1. بيئة الدراسة (النطاق الجغرافي) :تنفرد هذه الدراسة بالتطبيق على (البيئة الليبية مصرف شمال إفريقيا – طرابلس)، بينما توزعت الدراسات الأخرى بين الأردن ومصر، مما يعطي هذه الدراسة قيمة مضافة في سد فجوة بحثية محلياً.
2. نوع العينة :استخدمت في هذه الدراسة العينة العشوائية البسيطة، وهو ما يتشابه مع دراسة (العدلي)، لكنه يختلف عن هذه الدراسة (بن حامد وعزام) اللتين اعتمدتا على العينة القصدية الموجهة لخبراء محددين.
3. المتغيرات: بينما ركزت هذه الدراسة على الأمن السيبراني بشكل عام، ذهبت دراسة (حلمي) للتخصص في "الذكاء الاصطناعي" كجزء من الأمن، ودراسة (عزام) ركزت على "الأنظمة الرقمية" بشكل أوسع.
4. الحداثة الزمنية: هذه الدراسة (2025) تعتبر الأحدث زمنياً، مما يعني أنها قادرة على تغطية تهديدات سيبرانية وتطورات تقنية لم تكن موجودة وقت إعداد دراسة (العدلي 2018) أو (عزام 2019).

الجانب النظري

تعريف الأمن السيبراني:

هو مجموعة الممارسات والتقنيات والعمليات المصممة لحماية الأنظمة والشبكات والبرامج والبيانات والأجهزة من الهجمات الرقمية أو الوصول غير المصرح به أو التلف أو السرقة، (موسى، 2022).

أهداف الأمن السيبراني:

1. السرية (Confidentiality):السرية تهدف إلى منع الوصول غير المصرح به إلى البيانات الحساسة، مثل معلومات شخصية أو تجارية، للحفاظ على خصوصيتها. ويتم تحقيق ذلك باستخدام تقنيات التشفير مثل AES أو RSA، التي تحول البيانات إلى رموز غير قابلة للقراءة بدون مفتاح.

بالإضافة إلى ذلك، يشمل التحكم في الوصول (Access Control) استخدام كلمات مرور قوية وأنظمة المصادقة متعددة العوامل للحد من التجسس أو الاختراقات.

2. السلامة (Integrity):السلامة تركز على ضمان عدم تغيير البيانات أو الأنظمة بشكل غير مصرح، مما يحافظ على مصداقيتها ودقتها. وتستخدم خوارزميات الهاش مثل SHA-256 لإنشاء بصمات رقمية تكشف أي تعديل، حيث يتغير

الهاش إذا تم التلاعب بالبيانات. كما تشمل آليات مثل التوقيعات الرقمية والنسخ الاحتياطي المنتظم لمنع الفقدان أو الإضافة غير المقصودة، مما يعزز الثقة في النظام.

3. التوافر (Availability):التوافر يضمن توفر الأنظمة والخدمات دون انقطاع للمستخدمين المصرحين، حتى في حالات الهجمات أو الأعطال. ويشمل ذلك خطط الاسترداد من الكوارث (Disaster Recovery) والنسخ الاحتياطي السحابي لاستعادة الوصول بسرعة. كما يواجه التهديدات مثل هجمات DDoS باستخدام جدران الحماية وتوزيع الحمل (Load Balancing) للحفاظ على الاستمرارية. (نصرالدين، 2019).

أهمية الأمن السيبراني :

1. حماية البيانات الشخصية والخصوصية: في عصر البيانات الكبيرة، يتعرض الأفراد لخطر سرقة معلوماتهم الشخصية مثل أرقام البطاقات المصرفية أو بيانات الهوية. يمنع الأمن السيبراني الاحتيال الإلكتروني والتجسس، مما يحافظ على خصوصية المستخدمين ويقلل من مخاطر الابتزاز أو السرقة الهوية.
2. الوقاية من الخسائر الاقتصادية: يواجه القطاع الخاص، مثل البنوك والشركات، هجمات تؤدي إلى توقف العمليات أو فقدان البيانات، مما يكلف مليارات الدولارات. على سبيل المثال، هجمات الرانسومويير تطالب بدفع فدية لاستعادة البيانات، ويمكن للأمن السيبراني تقليل هذه الخسائر من خلال النسخ الاحتياطي والكشف المبكر.
3. تعزيز الأمن الوطني والدفاع: تشكل الهجمات السيبرانية تهديدًا للبنية التحتية الحيوية مثل شبكات الكهرباء، النقل، والصحة. الدول تستثمر في الأمن السيبراني لمواجهة الحروب الإلكترونية أو التجسس الحكومي، كما حدث في هجمات على دول مثل أوكرانيا أو إيران، حيث أدت إلى تعطيل خدمات أساسية،(بن حامد، 2022).
4. الامتثال للقوانين والمعايير الدولية: تفرض قوانين مثل GDPR في أوروبا أو PCI DSS للمدفوعات الإلكترونية عقوبات على الشركات غير الملتزمة بالأمن السيبراني. يساعد ذلك في بناء الثقة مع العملاء وتجنب الغرامات، كما يعزز السمعة التجارية.
5. دعم الابتكار والتطور التكنولوجي: مع انتشار الذكاء الاصطناعي، الإنترنت الأشياء(IoT) ، والحوسبة السحابية، يزداد الاعتماد على الأنظمة الرقمية. يضمن الأمن السيبراني استمرارية هذه التقنيات دون مخاطر، مما يشجع على الابتكار في مجالات مثل التجارة الإلكترونية والتعليم عن بعد(هيكل، 2018).

التحديات التي تواجه استخدام الأمن السيبراني:

1. تطور الهجمات باستخدام الذكاء الاصطناعي: يستخدم المهاجمون الذكاء الاصطناعي لإنشاء هجمات أكثر ذكاءً وسرعة، مثل (Deepfakes) للتصيد الاجتماعي أو البرمجيات الضارة الآلية، مما يجعل الكشف عنها أصعب. وهذا يزيد من تعقيد الدفاعات التقليدية ويطالب بتكييف مستمر للأنظمة الأمنية.
2. نقص المهارات والقوى العاملة: هناك فجوة كبيرة في عدد المتخصصين في الأمن السيبراني، مع تقديرات تشير إلى نقص أكثر من ربع مليون متخصص في الولايات المتحدة وحدها. ويؤدي ذلك إلى إرهاق الفرق (مثل حرق الـ CISO) وصعوبة في الاستجابة السريعة للتهديدات، مما يتطلب تدريبًا مكثفًا وجذب مواهب جديدة.
3. زيادة تعقيد التهديدات والنظم: مع انتشار الحوسبة السحابية والإنترنت الأشياء (IoT)، تتسع سطح الهجوم، مما يخلق نقاط ضعف جديدة مثل هجمات السلسلة التوريدية أو الثغرات في أنظمة ERP. وهذا يعيق الرؤية الكاملة للمخاطر ويجعل الامتثال للمعايير مثل GDPR أو PCI DSS أكثر صعوبة.
4. تطور هجمات الرانسومويير والابتزاز: أصبحت هجمات الرانسومويير أكثر تطورًا، مع سرقة البيانات قبل التشفير وتهديد بنشرها، مما يزيد من التأثير على المؤسسات،(العدلي، 2018).

5. التباين الجيوسياسي والفجوات في القدرات: التوترات الجيوسياسية تزيد من الهجمات المدعومة من الدول، مما يوسع الفجوة بين الدول المتقدمة والنامية في القدرات السيبرانية. وهذا يؤثر على التعاون الدولي ويزيد من مخاطر الهجمات على البنية التحتية الحيوية.
6. صعوبة الكشف والاستجابة السريعة: في بيئات معقدة، يتأخر اكتشاف الاختراقات بسبب التهديدات المتطورة والتنظيمات المجزأة، مما يؤدي إلى خسائر أكبر. ويتطلب ذلك تبني نماذج مراقبة مستمرة وأدوات ذكية لسد الفجوات في الرؤية، (مروان، 2019).

تعريف أنظمة البيانات: هي مجموعة منظمة من الرموز والعمليات التي تُستخدم للعمل عليها، مثل مجموعة منظمة من الرموز وإجراءات التشغيل تشمل ذلك أي تجميع منظم للرموز يمكن استخدامه لأغراض معالجة. (حلمي، 2023).

أنواع أنظمة البيانات:

1. أنظمة المعالجة المعاملاتية: تهتم بمعالجة المعاملات اليومية في الوقت الفعلي، مثل عمليات السحب والإيداع في البنوك. تكون سريعة وموثوقة، وتدعم التحديث الفوري للبيانات لتجنب الأخطاء.
2. أنظمة المعالجة الموزعة: تقسم المهام عبر عدة خوادم أو أجهزة متصلة لمعالجة البيانات الكبيرة بكفاءة، مما يعزز السرعة والمرونة. تستخدم في البيئات السحابية.
3. أنظمة قواعد البيانات العلائقية: تنظم البيانات في جداول مترابطة باستخدام لغة SQL، مثل MySQL أو Oracle. مثالية للبيانات المنظمة وتدعم الاستعلامات المعقدة.
4. أنظمة المعالجة الدفعية: تعالج مجموعات كبيرة من البيانات دفعة واحدة في أوقات غير ذروة، مثل إعداد التقارير اليومية. أقل تكلفة للمهام غير العاجلة.
5. أنظمة الدعم التنفيذي: توفر رؤى استراتيجية للإدارة العليا من خلال لوحات تحكم وبيانات خارجية. تركز على الاتجاهات طويلة الأمد(صبحي، 2022).

مكونات أنظمة البينات:

1. الأجهزة (Hardware): تشمل الأدوات المادية اللازمة لتشغيل النظام، مثل الخوادم، أجهزة التخزين (مثل HDD أو SSD)، والأجهزة الطرفية (كالحواسيب والطابعات). توفر هذه المكونات القدرة على معالجة وتخزين البيانات الكبيرة، وفي سياق المصارف، تكون محمية من الأعطال أو الهجمات السيبرانية من خلال أنظمة النسخ الاحتياطي.
2. البرمجيات (Software): تشمل البرامج والتطبيقات التي تدير البيانات، مثل أنظمة إدارة قواعد البيانات (DBMS) كـ Oracle أو MySQL، والبرمجيات التطبيقية للمعالجة (مثل برامج التحليل). تتضمن أيضًا أنظمة التشغيل (OS) مثل Windows أو Linux، التي تضمن التشغيل السلس وتدعم ميزات الأمان مثل التشفير(حلمي، 2023).
3. البيانات (Data): هي الجوهر الأساسي، وتشمل المعلومات الخام أو المعالجة مثل بيانات العملاء، السجلات المالية، أو التقارير. تُنظم في قواعد بيانات علائقية أو غير علائقية، ويجب حمايتها من الفقدان أو التعديل غير المصرح، كما أبرزت الدراسة في حماية الأنظمة والبيانات.
4. الإجراءات (Procedures): هي السياسات والعمليات المحددة للتعامل مع البيانات، مثل إجراءات النسخ الاحتياطي، التحديثات، أو الاسترداد من الكوارث. تشمل أيضًا البروتوكولات الأمنية مثل اختبارات الاختراق، التي أوصت بها الدراسة للحفاظ على المعايير الدولية مثل PCI DSS.
5. الأشخاص (People): يشمل المستخدمين، الإداريين، والمطورين الذين يتفاعلون مع النظام. يتطلبون تدريبًا مستمرًا لتجنب الأخطاء البشرية، مثل التصيد الإلكتروني، وهم عنصر حاسم في تنفيذ السياسات الأمنية.

6. الشبكات (Networks): تشمل البنية التحتية للاتصال، مثل الإنترنت، الشبكات المحلية (LAN)، أو السحابية الهجينة. توفر الوصول إلى البيانات عن بعد، لكنها تحتاج إلى حماية من الهجمات مثل DDoS، كما في التوصيات بالتكامل السحابي لتحسين الأداء والحماية، (بن حامد، 2022).

أهداف أنظمة البيانات:

1. جمع وتخزين البيانات بكفاءة: تهدف إلى تجميع البيانات من مصادر متعددة وتخزينها بشكل منظم، مما يقلل من التكرار ويوفر المساحة. يساعد ذلك في الحفاظ على موارد النظام وتسهيل الوصول السريع، كما في تخزين بيانات العملاء في المصارف.
2. ضمان دقة وسلامة البيانات: الحفاظ على كمال ودقة البيانات من خلال آليات التحقق والتصحيح، لمنع التعديلات غير المصرحة. يرتبط هذا بالمبدأ السيبراني للسلامة (Integrity)، مما يعزز الثقة في المعلومات المستخدمة للقرارات.
3. توفير الوصول والاسترجاع السريع: تسهيل استرجاع البيانات للمستخدمين المصرحين دون تأخير، مع دعم الاستعلامات المعقدة. يضمن ذلك التوافر (Availability)، خاصة في أنظمة المعاملات اليومية مثل الخدمات المصرفية عبر الإنترنت.
4. دعم اتخاذ القرارات من خلال التحليل: توفير أدوات لتحليل البيانات واستخراج الرؤى، مثل التقارير والتنبؤات. يساعد في تحسين الأداء التشغيلي، كما في تحليل مخاطر الائتمان في المصارف.
5. تعزيز الأمان والخصوصية: حماية البيانات من الاختراقات والتسريبات من خلال التشفير والتحكم في الوصول. يرتبط مباشرة بالسرية (Confidentiality)، ويُعتبر هدفًا أساسيًا في مواجهة التحديات السيبرانية كما ذكرت الدراسة(كامل، 2016).

أهمية أنظمة البيانات

تحسين إدارة البيانات وتخزينها: توفر أنظمة البيانات تخزينًا منظمًا وآمنًا للبيانات، مما يقلل من الفقدان أو التكرار. في المصارف، يساعد ذلك في الحفاظ على سجلات العملاء بدقة، ويمنع الخسائر الناتجة عن الأعطال أو الهجمات السيبرانية، ودعم اتخاذ القرارات الاستراتيجية وتمكن من تحليل البيانات لاستخراج الرؤى، مثل التنبؤ بالاتجاهات أو تقييم المخاطر. هذا يعزز الكفاءة التشغيلية، كما في تحليل البيانات المالية لاتخاذ قرارات استثمارية مدروسة. وتعزيز الأمان والخصوصية، وتلعب دورًا حاسمًا في حماية البيانات من الاختراقات، من خلال آليات التشفير والتحكم في الوصول. ترتبط مباشرة بالأمن السيبراني، حيث تمنع التسريبات وتضمن السرية، كما أبرزت الدراسة في حماية الأنظمة، وزيادة الكفاءة التشغيلية والإنتاجية وتسرع العمليات اليومية من خلال الأتمتة، مثل معالجة المعاملات في الوقت الفعلي. في القطاع المصرفي، تقلل من الأخطاء البشرية وتوفر الوقت، مما يحسن الخدمات للعملاء.

والامتثال للقوانين والمعايير تساعد في الالتزام باللوائح مثل GDPR أو PCI DSS، مما يتجنب الغرامات ويعزز السمعة. في الدراسة، أوصت بتقييمات دورية لضمان التوافق مع التطورات التكنولوجية، ودعم الابتكار والتوسع تتيح التكامل مع تقنيات جديدة مثل السحابة الهجينة، مما يدعم النمو. تساهم في الابتكار، مثل استخدام الذكاء الاصطناعي لتحليل البيانات الكبيرة، وتعزز القدرة التنافسية، والحماية من المخاطر والكوارث توفر آليات النسخ الاحتياطي والاسترداد، مما يضمن الاستمرارية في حالات الهجمات أو الأعطال. هذا يقلل من الخسائر الاقتصادية ويحافظ على التوافر، كما في التوصيات بتدريب الفرق الفنية، (العدلي، 2018).

الجانب العملي

اختبار الثبات والصدق:

للتأكد من ثبات وصدق " أداة الدراسة " قام الباحثان بحساب معامل كرونباخ ألفا (Cronbach Alpha) ومعامل الصدق الذاتي لكل محور من محاور استمارة الاستبيان ولجميع المحاور. فكانت النتائج كما بالجدول رقم (1).

جدول رقم (1) نتائج اختبار الثبات والصدق

م	المحور	عدد العبارات	معامل ألفاء الثبات	معامل الصدق
1	بعد السرية	5	0.821	0.736
2	بعد السلامة	5	0.699	0.832
3	بعد التوافر	5	0.775	0.742
4	بعد المصادقة	5	0.643	0.603
	الدرجة الكلية لمستوى الأمن السيبراني	20	0.734	0.728
1	بعد البنية التحتية التقنية	5	0.802	0.685
2	بعد التشغيلية	5	0.721	0.759
3	بعد المحتوى المعلوماتي	5	0.804	0.925
	الدرجة الكلية لمستوى أنظمة البيانات	15	0.775	0.744
	جميع الأبعاد	35	0.754	0.736

تُظهر نتائج التحليل الإحصائي الموضحة في الجدول رقم (1) مؤشرات قوية حول صلاحية أداة الدراسة (الاستبيان)، ويمكن تفصيلها كالآتي:

- ثبات أداة الدراسة : حققت محاور الاستبيان قيمًا مرتفعة لمعامل "كرونباخ ألفا) " Alpha Cronbach's ، حيث تراوحت بين (0.643 و0.821)، بينما استقر المعامل العام للمحاور مجتمعة عند .(0.754) وبما أن هذه القيم تتجاوز الحد المقبول إحصائيًا (0.60)، فإن ذلك يؤكد تمتع الاستبيان بدرجة عالية من الاتساق والثبات الداخلي.
- صدق أداة الدراسة :جاءت معاملات الصدق الذاتي (الجذر التربيعي لمعامل الثبات) قوية ومطمئنة، حيث تراوحت قيمها ما بين (0.603 و0.925)، وبلغ الصدق العام للمحاور .(0.736)

الاستنتاج : بناءً على هذه المؤشرات، يتضح أن أداة الدراسة تتمتع بمستوى عالٍ من الموثوقية والمصداقية، مما يجعلها أداة قياس دقيقة صالحة لجمع البيانات والاعتماد على نتائجها في تحقيق أهداف البحث وتعميم نتائجه.

أبعاد مستوى الأمن السيبراني

1- مستوى بعد السرية

لاختبار معنوية درجة الموافقة على كل عبارة من العبارات المتعلقة بمستوى بعد السرية تم استخدام اختبار ولكوكسون حول متوسط المقياس (3) فكانت النتائج كما في الجدول رقم (2).

جدول رقم (2) نتائج اختبار ولكوكسون حول متوسط كل عبارة من العبارات المتعلقة بمستوى بعد السرية

م	العبارة	المتوسط	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
1	يتم تشفير البيانات الحساسة (مثل بيانات العملاء المالية) بشكل فعال لمنع الوصول غير المصرح به.	4.21	1.640	−3.762	.000
2	يطبق المصرف سياسات صارمة للتحكم في الوصول إلى البيانات بناءً على صلاحيات الموظفين فقط.	4.08	1.087	−2.212	.000
3	تحمي الأنظمة السيبرانية في المصرف البيانات السرية من التسريب أثناء النقل أو التخزين.	4.11	1.256	−4.971	0.00
4	يستخدم المصرف تقنيات متقدمة (مثل جدران الحماية وأنظمة الكشف عن التسلل) لحماية سرية.	4.10	1.087	−2.041	.000
5	يمنع المصرف بشكل فعال الوصول غير المصرح به إلى بيانات العملاء الشخصية والمعاملات المالية.	4.02	1.769	−4.823	.000

من خلال الجدول رقم (2) يلاحظ أن الدلالات المحسوبة أقل من مستوي المعنوية (0.05) ومتوسطات إجابات مفردات عينة الدراسة تزيد عن متوسط المقياس (3) لجميع العبارات المتعلقة بمستوى بعد السرية، لذلك نرفض الفرضيات الصفرية لهذه العبارات ونقبل الفرضيات البديلة لها وحيث أن متوسطات إجابات مفردات عينة الدراسة على هذه العبارات تزيد عن متوسط المقياس (3)، وهذا يدل على وجود ارتفاع معنوي في درجات الموافقة على هذه العبارات، ولاختبار الفرضية الفرعية المتعلقة بمستوى بعد السرية تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية، واستخدام اختبار (Z) حول متوسط المقياس (3) فكانت النتائج كما بالجدول رقم (3).

الجدول رقم (3) نتائج اختبار (Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى بعد السرية

البيان	المتوسط العام	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
مستوى بعد السرية	4.10	.7628	7.163	.000

من خلال الجدول (3) يلاحظ أن قيمة إحصائي الاختبار (7.163) بدلالة محسوبة (0.000) وهي أقل من مستوى المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وأن المتوسط العام لإجابات مفردات عينة الدراسة (4.10) وهو يزيد عن متوسط المقياس (3) وهذا يشير إلى وجود ارتفاع في مستوى بعد السرية.

2- مستوى بعد السلامة

لاختبار معنوية درجة الموافقة على كل عبارة المتعلقة بمستوى بعد السلامة تم استخدام اختبار ولكوكسون حول متوسط المقياس (3) فكانت النتائج كما في الجدول رقم (4)

جدول رقم (4) نتائج اختبار ولكوكسون حول متوسط كل عبارة من العبارات المتعلقة بمستوى بعد السلامة

م	العبارة	المتوسط	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
1	يستخدم المصرف آليات فعالة للكشف عن أي تغييرات غير مصرحة في البيانات المالية والسجلات.	4.02	1.092	-5.322	.000
2	تحمي إجراءات الأمن السيبراني في المصرف دقة وصحة البيانات من التلاعب أو الحقن الضار.	4.10	1.523	-4.621	.000
3	يطبق المصرف تقنيات التوقيع الرقمي والتحقق من التجزئة (Hashing) لضمان سلامة المعاملات.	4.12	1.052	-2.744	.000
4	تمنع الأنظمة الأمنية في المصرف التعديل غير المصرح به على الأنظمة والتطبيقات المصرفية.	4.21	1.821	-3.869	.000
5	يساهم الأمن السيبراني في المصرف في الحفاظ على سلامة السجلات المالية ضد البرمجيات الضارة.	4.13	1.324	-3.329	.000

من خلال الجدول رقم (4) يلاحظ أن الدلالات المحسوبة أقل من مستوي المعنوية (0.05) ومتوسطات إجابات مفردات عينة الدراسة تزيد عن متوسط المقياس (3) لجميع العبارات المتعلقة بمستوى بعد السلامة، لذلك نرفض الفرضيات الصفرية لهذه العبارات ونقبل الفرضيات البديلة لها وحيث أن متوسطات إجابات مفردات عينة الدراسة على هذه العبارات تزيد عن متوسط المقياس (3)، وهذا يدل على وجود ارتفاع معنوي في درجات الموافقة على هذه العبارات، ولاختبار الفرضية الفرعية المتعلقة بمستوى بعد السلامة تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية، واستخدام اختبار (Z) حول متوسط المقياس (3) فكانت النتائج كما بالجدول رقم (5) .

الجدول رقم (5) نتائج اختبار(Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى بعد السلامة

البيان	المتوسط العام	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
مستوى بعد السلامة	4.11	.8732	3.873	.000

من خلال الجدول (5) يلاحظ أن قيمة إحصائي الاختبار (3.873) بدلالة محسوبة (0.000) وهي أقل من مستوى المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وحيث أن المتوسط العام لإجابات مفردات عينة الدراسة (4.11)هو يزيد عن متوسط المقياس (3)، وهذا يشير إلى وجود ارتفاع في مستوى بعد السلامة.

3- مستوى بعد التوافر

لاختبار معنوية درجة الموافقة على كل عبارة المتعلقة بمستوى بعد التوافر تم استخدام اختبار ولكوكسون حول متوسط المقياس (3) فكانت النتائج كما في الجدول رقم (6)

جدول رقم (6) نتائج اختبار ولكوكسون حول متوسط كل عبارة من العبارات المتعلقة بمستوى بعد التوافر

م	العبارة	المتوسط	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
1	يضمن الأمن السيبراني في المصرف استمرارية عمل الأنظمة المصرفية دون انقطاع بسبب الهجمات.	4.23	1.912	-2.054	.000
2	تحمي إجراءات الأمن السيبراني الخدمات الإلكترونية (مثل التطبيقات والصراف الآلي) من هجمات الحرمان من الخدمة (DDoS).	4.03	1.008	-6.708	.000
3	يساهم الأمن السيبراني في توفير خطط نسخ احتياطي فعالة لضمان استعادة البيانات بسرعة بعد أي حادث.	3.16	1.712	-3.614	.000
4	يحافظ الأمن السيبراني على توافر البيانات والمعاملات المالية للعملاء في جميع الأوقات.	3.72	1.764	-5.406	.000
5	تطبق آليات التعافي من الكوارث في المصرف بشكل يضمن عودة الأنظمة إلى العمل بأسرع وقت ممكن.	3.61	1.912	-4.132	.000

من خلال الجدول رقم (6) يلاحظ أن الدلالات المحسوبة أقل من مستوي المعنوية (0.05) ومتوسطات إجابات مفردات عينة الدراسة تزيد عن متوسط المقياس (3) لجميع العبارات المتعلقة بمستوى بعد التوافر ، لذلك نرفض الفرضيات الصفرية لهذه العبارات ونقبل الفرضيات البديلة لها وحيث أن متوسطات إجابات مفردات عينة الدراسة على هذه العبارات تزيد عن متوسط المقياس (3)، وهذا يدل على وجود ارتفاع معنوي في درجات الموافقة على هذه العبارات، ولاختبار الفرضية الفرعية المتعلقة بمستوى بعد التوافر تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية، واستخدام اختبار (Z) حول متوسط المقياس (3) فكانت النتائج كما بالجدول رقم (7) .

الجدول رقم (7) نتائج اختبار (Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى بعد التوافر

البيان	المتوسط العام	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
مستوى بعد التوافر	3.75	1.432	5.051	.000

من خلال الجدول (7) يلاحظ أن قيمة إحصائي الاختبار (5.051) بدلالة محسوبة (0.000) وهي أقل من مستوى المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وحيث أن المتوسط العام لإجابات مفردات عينة الدراسة (3.75) وهو يزيد عن متوسط المقياس (3)، وهذا يشير إلى وجود ارتفاع في مستوى بعد التوافر.

4- مستوى بعد المصادقة

لاختبار معنوية درجة الموافقة على كل عبارة المتعلقة بمستوى بعد المصادقة تم استخدام اختبار ولكوكسون حول متوسط المقياس (3) فكانت النتائج كما في الجدول رقم (8)

جدول رقم (8) نتائج اختبار ولكوكسون حول متوسط كل عبارة من العبارات المتعلقة بمستوى بعد المصادقة

م	العبارة	المتوسط	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
1	يطبق المصرف مصادقة متعددة العوامل (MFA) بشكل فعال للتحقق من هوية المستخدمين قبل الوصول إلى الأنظمة.	4.01	1.530	-3.915	.000
2	تساهم إجراءات الأمن السيبراني في المصرف في التحقق الدقيق من هوية العملاء والموظفين أثناء المعاملات الإلكترونية.	4.08	1.351	-3.671	.000
3	تحمي آليات المصادقة في المصرف من محاولات الوصول غير المصرح به باستخدام بيانات مزيفة أو مسروقة.	4.11	1.962	-2.519	.000
4	يستخدم المصرف تقنيات متقدمة للمصادقة (مثل البيومترية أو الرموز المؤقتة) لتعزيز أمان الوصول إلى البيانات والأنظمة.	4.14	1.194	-6.012	.001
5	يساهم الأمن السيبراني في المصرف في منع الهجمات التي تعتمد على سرقة الهوية أو التخمين من خلال سياسات مصادقة قوية.	3.09	1.902	-3.402	.000

من خلال الجدول رقم (8) يلاحظ أن الدلالات المحسوبة أقل من مستوي المعنوية (0.05) ومتوسطات إجابات مفردات عينة الدراسة تزيد عن متوسط المقياس (3) لجميع العبارات المتعلقة بمستوى بعد المصداقية، لذلك نرفض الفرضيات الصفرية لهذه العبارات ونقبل الفرضيات البديلة لها وحيث أن متوسطات إجابات مفردات عينة الدراسة على هذه العبارات تزيد عن متوسط المقياس (3)، وهذا يدل على وجود ارتفاع معنوي في درجات الموافقة على هذه العبارات، ولاختبار الفرضية الفرعية المتعلقة بمستوى بعد المصداقية تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية، واستخدام اختبار (Z) حول متوسط المقياس (3) فكانت النتائج كما بالجدول رقم (9).

الجدول رقم (9) نتائج اختبار (Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى بعد المصداقية

البيان	المتوسط العام	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
مستوى بعد المصداقية	3.88	.83215	7.126	.000

من خلال الجدول (9) يلاحظ أن قيمة إحصائي الاختبار (7.126) بدلالة محسوبة (0.000) وهي أقل من مستوى المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وحيث أن المتوسط العام لإجابات مفردات عينة الدراسة (3.88) وهو يزيد عن متوسط المقياس (3)، وهذا يشير إلى وجود ارتفاع في مستوى بعد المصداقية.

مستوى الأمن السيبراني:

لاختبار الفرضية المتعلقة بمستوى النظم الخبيرة تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية والمتمثلة في (السرية، السلامة، التوافر، المصادقة)، واستخدام اختبار (Z) حول متوسط المقياس (3) فكانت النتائج كما بالجدول رقم (10).

الجدول رقم (10) نتائج اختبار (Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى الأمن السيبراني

البيان	**المتوسط العام**	**الانحراف المعياري**	**إحصائي الاختبار**	**الدلالة المحسوبة**
مستوى الأمن السيبراني	3.96	.8823	13.104	.000

من خلال الجدول (10) يلاحظ أن قيمة إحصائي الاختبار (13.104) بدلالة محسوبة (0.000) وهي أقل من مستوى المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وحيث أن المتوسط العام لإجابات مفردات عينة الدراسة (3.96) وهو يزيد عن متوسط المقياس (3)، وهذا يشير إلى وجود ارتفاع في مستوى الأمن السيبراني.

مستويات أبعاد أنظمة البيانات:

1. مستوى بعد البنية التحتية التقنية

لاختبار معنوية درجة الموافقة على كل من العبارات المتعلقة بمستوى بعد البنية التحتية التقنية تم استخدام اختبار ولكوكسون حول متوسط المقياس (3) فكانت النتائج كما في الجدول رقم (11).

جدول رقم (11) نتائج اختبار ولكوكسون حول متوسط كل عبارة من العبارات المتعلقة بمستوى بعد البنية التحتية التقنية

م	العبارة	المتوسط	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
1	الأجهزة والخوادم في المصرف حديثة وتدعم معالجة كميات كبيرة من البيانات بكفاءة عالية .	4.13	1.923	7.644	.000
2	البرمجيات المستخدمة) مثل نظام (Core Bankingمحدثة بانتظام وتتوافق مع أحدث المعايير الأمنية .	4.05	1.819	6.322	.000
3	شبكة الاتصالات الداخلية والخارجية سريعة ومستقرة وتدعم الوصول الآمن إلى البيانات .	3.79	1.072	8 .620	.000
4	قواعد البيانات منظمة جيداً وتدعم التكامل السلس بين الأنظمة المختلفة في المصرف .	3.07	1.211	9.242	.000
5	البنية التحتية التقنية توفر مستوى عالٍ من الحماية ضد الهجمات السيبرانية (مثل التشفير وجدران الحماية).	3.81	1.234	7.851	.000

من خلال الجدول رقم (11) يلاحظ أن الدلالات المحسوبة أقل من مستوي المعنوية(0.05) ومتوسطات إجابات مفردات عينة الدراسة تزيد عن متوسط المقياس (3) لجميع العبارات المتعلقة بمستوى بعد البنية التحتية التقنية ، ولذلك نرفض الفرضيات الصفرية لهذه العبارات ونقبل الفرضيات البديلة لها وحيث أن متوسطات إجابات مفردات عينة الدراسة على هذه العبارات تزيد عن متوسط المقياس (3)، وهذا يدل على وجود ارتفاع معنوي في درجات الموافقة على هذه العبارات، ولاختبار الفرضية الفرعية المتعلقة بمستوى بعد البنية التحتية التقنية تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية، واستخدام اختبار (Z) حول متوسط المقياس (3) فكانت النتائج كما بالجدول رقم (12).

جدول رقم (12) نتائج اختبار(Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى البنية التحتية التقنية

من خلال الجدول (12) يلاحظ أن قيمة إحصائي الاختبار (7.218) بدلالة محسوبة (0.000) وهي أقل من مستوى

البيان	المتوسط العام	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
بمستوى بعد البنية التحتية التقنية	3.77	.5413	7.218	.000

المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وحيث أن المتوسط العام لإجابات مفردات عينة الدراسة (3.77) وهو يزيد عن متوسط المقياس (3)، وهذا يشير إلى وجود ارتفاع في بمستوى بعد البنية التحتية التقنية.

2. مستوى بعد التشغيلية

لاختبار معنوية درجة الموافقة على كل عبارة المتعلقة بمستوى بعد التشغيلية تم استخدام اختبار ولكوكسون حول متوسط المقياس (3) فكانت النتائج كما في الجدول رقم (13).

جدول رقم (13) نتائج اختبار ولكوكسون حول متوسط كل عبارة من العبارات المتعلقة بمستوى بعد التشغيلية

م	العبارة	المتوسط	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
1	يتم إجراء عمليات النسخ الاحتياطي للبيانات بانتظام وفق خطة واضحة وموثوقة .	3.24	1.821	22.933	.000
2	توجد خطط فعالة لاستمرارية الأعمال (Business Continuity)تضمن استمرار تشغيل الأنظمة في حالات الطوارئ .	4.55	1.204	8.834	.000
3	عمليات الصيانة الدورية للأنظمة تُنفذ في مواعيد مناسبة دون التأثير السلبي على الخدمات المصرفية .	4.32	1.093	7.807	.000
4	الإجراءات التشغيلية واضحة وموثقة ويتم تدريب الموظفين عليها بشكل مستمر .	4.03	1.021	9.445	.000
5	وقت الاستجابة للأعطال التقنية أو المشكلات التشغيلية قصير وفعال.	4.43	1.720	10.136	.000

من خلال الجدول رقم (13) يلاحظ أن الدلالات المحسوبة أقل من مستوي المعنوية (0.05) ومتوسطات إجابات مفردات عينة الدراسة تزيد عن متوسط المقياس (3) لجميع العبارات المتعلقة بمستوى بعد التشغيلية، ولذلك نرفض الفرضيات الصفرية لهذه العبارات ونقبل الفرضيات البديلة لها وحيث أن متوسطات إجابات مفردات عينة الدراسة على هذه العبارات تزيد عن متوسط المقياس (3)، وهذا يدل على وجود ارتفاع معنوي في درجات الموافقة على هذه العبارات، ولاختبار الفرضية الفرعية المتعلقة بمستوى بعد التشغيلية تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية، واستخدام اختبار (Z) حول متوسط المقياس (3) فكانت النتائج كما بالجدول رقم (14)

الجدول رقم (14) نتائج اختبار(Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى بعد التشغيلية

البيان	المتوسط العام	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
مستوى بعد التشغيلية	4.11	.6324	11.051	.000

من خلال الجدول (14) يلاحظ أن قيمة إحصائي الاختبار (11.051) بدلالة محسوبة (0.000) وهي أقل من مستوى المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وحيث أن المتوسط العام لإجابات مفردات عينة الدراسة (4.11) وهو يزيد عن متوسط المقياس (3)، وهذا يشير إلى وجود ارتفاع في مستوى بعد التشغيلية.

3. مستوى بعد المحتوى المعلوماتي

لاختبار معنوية درجة الموافقة على كل عبارة المتعلقة بمستوى بعد المحتوى المعلوماتي تم استخدام اختبار ولكوكسون حول متوسط المقياس (3) فكانت النتائج كما في الجدول رقم (15).

جدول رقم (15) نتائج اختبار ولكوكسون حول متوسط كل عبارة من العبارات المتعلقة بمستوى بعد المحتوى المعلوماتي

م	العبارة	المتوسط	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
1	البيانات والتقارير المنتجة من النظام دقيقة وخالية من الأخطاء بشكل كبير .	4.05	1.973	-4.052	.000
2	المعلومات المتاحة كاملة وتشمل جميع التفاصيل اللازمة لاتخاذ القرارات المصرفية .	3.73	1.243	-5.851	.000
3	التقارير والمعلومات مقدمة في الوقت المناسب لدعم العمليات اليومية والقرارات الإدارية .	3.62	1.683	-5.342	.000
4	المحتوى المعلوماتي واضح وسهل الفهم ومنسق بطريقة تسهل الاستخدام .	3.72	1.836	-7.961	.000
5	المعلومات المنتجة ذات صلة عالية باحتياجات المستخدمين (مثل تحليل المخاطر، تقارير العملاء، أو كشف الاحتيال).	4.52	1.932	-6.203	.000

من خلال الجدول رقم (15) يلاحظ أن الدلالات المحسوبة أقل من مستوي المعنوية (0.05) ومتوسطات إجابات مفردات عينة الدراسة تزيد عن متوسط المقياس (3) لجميع العبارات المتعلقة بمستوى بعد المحتوى المعلوماتي، ولذلك نرفض الفرضيات الصفرية لهذه العبارات ونقبل الفرضيات البديلة لها وحيث أن متوسطات إجابات مفردات عينة الدراسة على هذه العبارات تزيد عن متوسط المقياس (3)، وهذا يدل على وجود ارتفاع معنوي في درجات الموافقة على هذه العبارات، ولاختبار الفرضية الفرعية المتعلقة بمستوى بعد المحتوى المعلوماتي تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية، واستخدام اختبار (Z) حول متوسط المقياس (3) فكانت النتائج كما بالجدول رقم (16) .

الجدول رقم (16) نتائج اختبار(Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى بعد المحتوى المعلوماتي

البيان	المتوسط العام	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
مستوى بعد المحتوى المعلوماتي	3.92	.6084	10.082	.000

من خلال الجدول (16) يلاحظ أن قيمة إحصائي الاختبار (10.082) بدلالة محسوبة (0.000) وهي أقل من مستوى المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وحيث أن المتوسط العام لإجابات مفردات عينة الدراسة (3.92) وهو يزيد عن متوسط المقياس (3)، وهذا يشير إلى وجود ارتفاع في مستوى بعد المحتوى المعلوماتي.

مستوى الأنظمة والبيانات:

لاختبار الفرضية المتعلقة تم إيجاد متوسطات إجابات مفردات عينة الدراسة على جميع العبارات المتعلقة بهذه الفرضية

والمتمثلة في (البينية التحتية والتقنية، التشـغلية، المحتوى المعلوماتي) واسـتخدام اختبار (Z) حول متوسـط المقياس (3) فكانت النتائج كما بالجدول رقم (17).

الجدول رقم (17) نتائج اختبار (Z) حول متوسط درجة الموافقة على جميع العبارات المتعلقة بمستوى الأنظمة والبيانات

البيان	المتوسط العام	الانحراف المعياري	إحصائي الاختبار	الدلالة المحسوبة
مستوى الأنظمة والبيانات	3.93	.30396	21.629	.000

من خلال الجدول (17) يلاحظ أن قيمة إحصائي الاختبار (21.629) بدلالة محسوبة (0.000) وهي أقل من مستوى المعنوية (0.05) لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة، وحيث أن المتوسط العام لإجابات مفردات عينة الدراسة (3.93) وهو يزيد عن متوسط المقياس (3)، وهذا يشير إلى وجود ارتفاع في مستوى الأنظمة والبيانات.

اختبار الفرضية الرئيسية للدراسة

أثر مستوى الأمن السيبراني بصورة عامة على مستوى حماية الأنظمة والبيانات.

لمعرفة أثر مستوى الأمن السيبراني (كمتغير مستقل) على مستوى حماية الأنظمة والبيانات (كمتغير تابع) تم استخدام أسلوب تحليل الانحدار البسيط (Simple linear regression) فكانت النتائج كما بالجدول رقم (18،19،20)

جدول رقم (18): نتائج اختبار معامل الارتباط ومعامل التحديد المتعلقة بنموذج انحدار المتغير التابع (مستوى حماية الأنظمة والبيانات) على المتغير المستقل (مستوى الأمن السيبراني)

معامل ارتباط بيرسون R	R Square مربع معامل الارتباط	Adjusted R Square مربع معامل الارتباط المعدل	Std. Error of the Estimate الخطأ المعياري للتقدير
.901[a]	.913	.924	.62391

من الجدول رقم (18) نلاحظ أن قيمة معامل ارتباط بيرسون (.901) ومعامل التحديد (0.913) بخطأ معياري للتقدير Standard Error of the Estimate (.62391) وهو مقدار صغير نسبياً وهذا يدل على وجود أثر موجب ذو دلالة إحصائية للمتغير المستقل (الأمن السيبراني) على المتغير التابع (حماية الأنظمة والبيانات) حيث أن التباينات في المتغير التابع (حماية الأنظمة والبيانات) يُفسرها التباين في المتغير المستقل (مستوى الأمن السيبراني) إذا لم يتأثر المتغير التابع (حماية الأنظمة والبيانات) إلا بأثر المتغير المستقل (مستوى الأمن السيبراني).

جدول رقم (19) جدول تحليل التباين (ANOVA) لأثر (مستوى الأمن السيبراني) على(حماية الأنظمة والبيانات).

	Sum of Squares مجموع المربعات	d. f. درجات الحرية	Mean Square متوسط المربعات	F-Test إحصاء الاختبار	P-value الدلالة الإحصائية
Regression الانحدار	1230.036	1	1300.646	3416.084	.000[a]
Residual البواقي	31.062	69	.519		
Total الإجمالي	1302.216[b]	70			

* دال إحصائياً عند مستوى المعنوية 0.05

من الجدول رقم (19) نلاحظ أن قيمة إحصاءه الاختبار F (Fc= 3416.084) بدلالة إحصائية (0.000) وهي أقل من مستوى المعنوية (0.05) مما يشير إلى أن النموذج الموفق معنوي (دال إحصائياً).

جدول رقم (20) نتائج تقدير معاملات الانحدار لنموذج انحدار المتغير التابع (حماية الأنظمة والبيانات) على المتغير المستقل (مستوى الأمن السيبراني)

	معاملات الانحدار B	الخطأ المعياري Std. Error	معاملات الانحدار المعياري Beta	قيمة إحصاءه الاختبار T	الدلالة الإحصائية P- Value
مستوى الأمن السيبراني	1.920	.039	.871	37.209	.000

* دال إحصائياً عند مستوى المعنوية 0.05

من الجدول رقم (20) نموذج انحدار المتغير التابع (حماية الأنظمة والبيانات) على المتغير المستقل (الأمن السيبراني) يكون بالصورة التالية: Y=1.920X حيث Yيمثل مستوى حماية الأنظمة والبيانات X يمثل مستوى الأمن السيبراني من النموذج نلاحظ أن قيمة معامل انحدار المتغير التابع (حماية الأنظمة والبيانات) على المتغير المستقل (مستوى الأمن السيبراني) (1.920) بدلالة إحصائية (.000)، وهي أقل من مستوى المعنوية (0.05) مما يشير إلى معنوية معامل الانحدار، ويعني ذلك أن المتغير المستقل (مستوى الأمن السيبراني) له تأثير معنوي على المتغير التابع (حماية الأنظمة والبيانات)، يتضح من النتائج الإحصائية المدونة بالجدول (20) السابق أن إشارة معامل الانحدار في النموذج الموفق موجبة (+) يشير ذلك إلى أن دور المتغير مستقل(مستوى الأمن السيبراني) في المتغير التابع (حماية الأنظمة والبيانات) ايجابي، أي كلما زاد مستوى المتغير مستقل(مستوى الأمن السيبراني) بوحدة واحدة زاد مستوى المتغير التابع (حماية الأنظمة والبيانات) بقيمة(1.920).

نتائج الدراسة:

1. أظهرت نتائج الدراسة أن التقييم مستوى عالٍ جداً من حماية سرية البيانات في المصرف، مع تطبيق فعال للتشفير، والتحكم في الصلاحيات، وحلول تقنية متقدمة تمنع التسريب والوصول غير المصرح به.

2. أظهرت نتائج الدراسة أن التقييم مستوى عالٍ جداً من حماية سلامة البيانات في المصرف، مع تطبيق فعال لآليات الكشف عن التغييرات غير المصرحة، التوقيع الرقمي، التحقق من التجزئة، ومنع التلاعب أو البرمجيات الضارة.
3. أظهرت نتائج الدراسة أن التقييم مستوى عالٍ جداً من ضمان توافر الأنظمة والبيانات في المصرف، مع حماية فعالة ضد هجمات DDoS، خطط نسخ احتياطي قوية، وآليات تعافي سريعة تضمن استمرارية الخدمات دون انقطاع.
4. أظهرت نتائج الدراسة أن التقييم مستوى عالٍ جداً من فعالية المصادقة وإدارة الهوية في المصرف، مع تطبيق ناجح لـ MFA، التقنيات المتقدمة (مثل البيومترية والرموز المؤقتة)، وحماية قوية ضد سرقة الهوية والوصول غير المصرح به.
5. أظهرت نتائج الدراسة أن التقييم مستوى عالٍ جداً من جودة المحتوى المعلوماتي في المصرف، مع دقة عالية للبيانات والتقارير، اكتمالها، توقيتها المناسب، وضوحها، وصلتها باحتياجات المستخدمين مثل تحليل المخاطر وكشف الاحتيال.
6. أظهرت نتائج الدراسة أن التقييم مستوى عالٍ جداً من كفاءة وحداثة البنية التحتية التقنية في المصرف، مع دعم قوي لمعالجة البيانات، تحديث البرمجيات، استقرار الشبكة، تنظيم قواعد البيانات، وحماية متقدمة ضد الهجمات السيبرانية.
7. أظهرت نتائج الدراسة أن التقييم مستوى عالٍ جداً من كفاءة البنية التحتية التشغيلية في المصرف، مع تنفيذ منتظم للنسخ الاحتياطي، خطط استمرارية فعالة، صيانة غير مؤثرة، إجراءات موثقة، واستجابة سريعة للأعطال.
8. أظهرت نتائج الدراسة أن التقييم مستوى عالٍ جداً من جودة المحتوى المعلوماتي في المصرف، مع دقة عالية للبيانات والتقارير، اكتمالها، توقيتها المناسب، وضوحها، وصلتها باحتياجات المستخدمين مثل تحليل المخاطر وكشف الاحتيال.

التوصيات

1. الاستمرار في تحديث التقنيات والسياسات دورياً مع إجراء اختبارات اختراق منتظمة للحفاظ على هذا المستوى العالي وضمان الامتثال للمعايير الدولية مثل PCI DSS.
2. الاستمرار في إجراء فحوصات دورية لسلامة البيانات وتحديث التقنيات (مثل Hashing وDigital Signatures) لمواجهة التهديدات الجديدة مع الامتثال لمعايير مثل ISO 27001. وتعزيز التدريب على الكشف عن البرمجيات الضارة وإجراء محاكاة للهجمات لضمان استمرارية الحماية العالية. الاستمرار في إجراء اختبارات دورية لخطط التعافي من الكوارث (Disaster Recovery Drills) وتحديثها لمواجهة التهديدات الجديدة مثل الهجمات المعقدة.
3. تعزيز القدرات الدفاعية ضد DDoS باستخدام حلول سحابية متقدمة وشراكات مع مزودي خدمات متخصصين. وتطوير برامج تدريب مستمرة للفرق التشغيلية لضمان تنفيذ سريع وفعال لإجراءات الاستجابة والاستعادة في حالات الطوارئ.
4. الاستمرار في تحديث آليات المصادقة دورياً وإجراء اختبارات اختراق منتظمة لمواجهة التهديدات الجديدة مثل الهجمات القائمة على الذكاء الاصطناعي. وتعزيز برامج التوعية للعملاء والموظفين لضمان الالتزام الكامل باستخدام MFA وتجنب الممارسات الضعيفة.
5. الاستمرار في إجراء تقييمات دورية للأجهزة والبرمجيات لضمان التوافق مع التطورات التكنولوجية الجديدة والمعايير الأمنية العالمية، وتعزيز التكامل بين الأنظمة من خلال تبني تقنيات سحابية هجينة وتدريب الفرق الفنية لتحسين الأداء والحماية.
6. الاستمرار في إجراء محاكاة دورية لخطط الاستمرارية والنسخ الاحتياطي للتحقق من فعاليتها في سيناريوهات حقيقية. وتعزيز التدريب المستمر للموظفين على الإجراءات التشغيلية مع دمج تقنيات مراقبة آلية لتقليل وقت الاستجابة أكثر.
7. الاستمرار في مراجعة وتحديث آليات إنتاج التقارير دورياً لضمان استمرار الدقة والصلة مع التغييرات في احتياجات العملاء والسوق، وتعزيز استخدام أدوات الذكاء الاصطناعي لتحسين الوضوح والتخصيص في التقارير مع تدريب الإداريين على استغلالها بشكل أفضل.

المراجع:

أولاً- الكتب

1. صبحي، عبدالعاطي صلاح، (2022)، الأنظمة الحديثة للبيانات ، مكتبة المجتمع العربي للنشر والتوزيع، عمان، الاردن.
2. كامل، أحمد مصطفى، (2016)، أنظمة البيانات، الفكر الادبي للنشر والتوزيع والطباعة، القاهرة، مصر.
3. مروان، عبدالله على، (2019)، الامن السيبراني، عمان دار الحامد للنشر والتوزيع، عمان، الأردن.
4. نصرالدين، خالد أبوالقاسم، (2019)، الأمن السيبراني، عالم الكتب للنشر والتوزيع والطباعة، القاهرة، مصر.
5. هكيل، مريم محمود، (2018)، الأمن السيبراني، عالم الكتب للنشر والتوزيع والطباعة، القاهرة، مصر.
6. موسى، محمد عمر، (2022)، أمن المعلومات، مكتبة المجتمع العربي للنشر والتوزيع، عمان، الاردن.

الدراسات السابقة:

1. حلمي، مصطفى محمود (2023)، أثر الذكاء الاصطناعي في تعزيز حماية الأنظمة البنوك. رسالة ماجستير، جامعة الاسكندرية، مصر.
2. بن حامد، زهرة محمود (2022) دور الامن السيبراني في حماية الأنظمة والبيانات، رسالة ماجستير غير منشورة، جامعة عمان، عمان، الأردن.
3. عزام، عبد الرحيم طارق (2019)، أثر الأنظمة الرقمية في تحسين حماية البيانات المصرفية". دراسة على البنوك التجارية في عمان، رسالة ماجستير غير منشورة، جامعة عمان، عمان، الأردن.
4. العدلي، أسماء على (2018) دور الامن السيبراني في الحد من الجرائم الإلكترونية دراسة على ميدانية على البنوك المصرية، رسالة ماجستير غير منشورة، جامعة القاهرة، مصر.