NTU Journal for Administrative and Human Sciences (2025) 5 (2) : 132-160
DOI: https://doi.org/10.56286/ntujahs.v5i2

IRAQI Academic Scientific Journals

JAHS NTU

P-ISSN: 2789-1240 E-ISSN:2789-1259
NTU Journal for Administrative and Human Sciences
Available online at: https://journals.ntu.edu.iq/index.php/NTU-JMS/index

The Readiness of Organizations for Cyber security Dimensions / An analytical study of the opinions of a sample of employees at the Central Bank of Iraq .. Mosul branch

1 st. Dr. Raafat Assi Hussein Al-Obaidi [1], 2 nd Raghad Khairuldeen Sabri [2]

1- Northern Technical University / Administrative Technical College / Mosul / Department of Business Administration Technologies

2- Northern Technical University / Administrative Technical College / Mosul / Department of Business Administration Technologies

Article Information

Received: 09. 09. 2024
Accepted: 26. 09. 2024
Published online: 01. 06. 2025

Corresponding author:
Name: Raafat Assi Hussei
Affiliation: Northern Technical University
Email: rafat_asai@ntu.edu.iq

Keywords: Cybersecurity . dimensions, confidentiality of data and information, availability .of data and information

A B S T R A C T

The current research aims to evaluate the level of readiness of the Central Bank of Iraq / Mosul Branch to establish cybersecurity through its dimensions represented by (confidentiality of data and information, availability of data and information, integrity of data and information), as the study relied on the descriptive analytical approach, by constructing a questionnaire to analyze the current capabilities and available infrastructure, through which data was collected from the research sample, which amounted to (199) individuals, who are employees of the Central Bank / Mosul Branch, using the questionnaire, which is the main tool for collecting data, and analyzing it based on the statistical program (SPSS), as descriptive statistics were relied upon (arithmetic mean, standard deviation, relative importance), and the One-Sample test was relied upon to test which dimensions are more available in the field under study, and one of the most prominent results that were reached is that there is a need to enhance the dimensions of cybersecurity (confidentiality of data and information, availability of data and information, integrity of data and information) in the field under study to reach the required level.

©2023 NTU JOURNAL FOR ADMINISTRATIVE AND HUMAN SCIENCES, NORTHERN TECHNICAL UNIVERSITY.
THIS IS AN OPEN ACCESS ARTICLE UNDER THE CC BY LICENSE: **https://creativecommons.org/licenses/by/4.0/**

مدى جاهزية المنظمات لإقامة أبعاد الامن السيبراني / دراسة تحليلية لآراء عينة من العاملين في البنك المركزي العراقي .. فرع الموصل

أ . م . د رأفت عاصي حسين العبيدي
الكلية التقنية الإدارية / موصل
الجامعة التقنية الشمالية
rafat_asai@ntu.edu.iq

الباحثة: رغد خيرالدين صبري
الكلية التقنية الإدارية / موصل
الجامعة التقنية الشمالية
ragad_sabri@ntu.edu.iq

المستخلص

يهدف البحث الحالي الى تقييم مستوى جاهزية البنك المركزي العراقي / فرع الموصل لإقامة الأمن السيبراني من خلال ابعاده المتمثلة بـ (سرية البيانات والمعلومات، توافر البيانات والمعلومات، نزاهة البيانات والمعلومات)، إذ اعتمدت الدراسة على المنهج الوصفي التحليلي، من خلال بناء استبانة لتحليل القدرات الحالية والبنية التحتية المتوفرة، اذ تم من خلاله جمع بيانات من العينة البحثية والتي بلغت (199) فرد وهم العاملين في البنك المركزي / فرع الموصل باستخدام الاستبانة والتي تعّد الاداة الرئيسة لجمع البيانات، وتحليلها بالاعتماد على البرنامج الاحصائي (spss)، إذ تم الاعتماد على الإحصاءات الوصفية (الوسط الحسابي، الانحراف المعياري، الأهمية النسبية)، كما تم الاعتماد على اختبار One-Sample test لاختبار أي الابعاد اكثر توافرا في الميدان المبحوث، ومن ابرز النتائج التي تم التوصل ان هناك حاجة لتعزيز ابعاد الامن السيبراني (سرية البيانات والمعلومات، توافر البيانات والمعلومات، نزاهة البيانات والمعلومات) في الميدان المبحوث للوصول إلى المستوى المطلوب.

الكلمات المفتاحية: ابعاد الامن السيبراني، سرية البيانات والمعلومات، توافر البيانات والمعلومات، نزاهة البيانات والمعلومات.

مقدمة البحث:

في ظل التطور التكنولوجي المتسارع وتنامي الاعتماد على الأنظمة الرقمية في إدارة العمليات المصرفية والمالية، أصبح الأمن السيبراني واحدًا من أهم التحديات التي تواجه المؤسسات المالية على مستوى العالم، ويزداد هذا التحدي تعقيدًا مع تزايد التهديدات والهجمات السيبرانية التي تستهدف نظم المعلومات والبيانات الحساسة في البنوك والمصارف، مما يتطلب من هذه المؤسسات تعزيز قدراتها لمواجهة هذه المخاطر وتأمين معلوماتها بشكل فعال، ويُعد البنك المركزي العراقي واحدًا من

الركائز الأساسية في النظام المالي الوطني، ومن ثم تأتي مسؤولية حماية بنيته التحتية الرقمية في غاية الأهمية للحفاظ على استقرار النظام المالي والاقتصادي للبلاد، وبناءً على ذلك، أصبحت دراسة مدى جاهزية المؤسسات المالية لإقامة الأمن السيبراني أمرًا ضروريًا لقياس قدرتها على مواجهة التهديدات الإلكترونية وضمان استمرارية أعمالها.

اولا: مشكلة البحث:

تكمن مشكلة البحث في التساؤلات الاتية:

1. ما مدى جاهزية البنك المركزي العراقي / فرع الموصل لإقامة ابعاد الامن السيبراني؟

ثانيا: أهمية البحث:

يستمد البحث أهميته من خلال:

2. الاسهام في تعزيز فهم أهمية تطبيق أبعاد الأمن السيبراني في المؤسسات المالية، مما يساعد في حماية البيانات الحساسة ومنع التهديدات السيبرانية التي قد تؤثر على استقرار النظام المالي.
3. التحليل المعمق لجاهزية البنك المركزي العراقي / فرع الموصل، مما يمكن إدارة البنك من اتخاذ قرارات مستنيرة بشأن الاستثمارات والتطويرات اللازمة لتعزيز البنية التحتية للأمن السيبراني.

ثالثا: اهداف البحث:

يهدف البحث الى التالي:

1. تحديد وتحليل المتطلبات التي ينبغي مراعاتها لتطبيق أبعاد الأمن السيبراني في البنك المركزي العراقي / فرع الموصل.
2. تقييم مستوى جاهزية البنك المركزي العراقي / فرع الموصل لتطبيق أبعاد الأمن السيبراني من خلال تحليل القدرات الحالية والبنية التحتية المتوفرة.
3. السعي نحو تشخيص اهم الابعاد المعبرة عن الامن السيبراني والتي من الممكن اعتمادها في البنك المركزي العراقي/ فرع الموصل).
4. تقديم توصيات عملية تهدف إلى تعزيز جاهزية البنك المركزي العراقي / فرع الموصل لتطبيق أبعاد الأمن السيبراني، بناءً على نتائج التحليل والتقييم.

رابعا: فرضية البحث:

يبنى البحث على الفرضيات الاتية:

1. يتوفر في البنك المركزي العراقي / فرع الموصل مكونات اقامة ابعاد الامن السيبراني.

خامسا: أساليب جمع البيانات والمعلومات

من أجل تحقيق أهداف الدراسة بالشكل الصحيح والعمل على حل المشكلة التي عمدت الدراسة إلى معالجتها اعتمدت على مجموعة من الأساليب في جانبيها النظري والميداني، إذ اعتمدت في الجانب النظري من هذه الدراسة على مجموعة من المراجع والأدبيات العربية والأجنبية من كتب ودوريات ورسائل و أطاريح ، إضافة إلى عما هو متوفر على شبكة الانترنت من مصادر بالشكل الذي يسهم في تغطية جميع مفردات الدراسة، بينما اعتمدت الباحثة في الجانب الميداني على عدة أدوات بحثية هي:

1. **الزيارات الميدانية:** إستهدفت جمع البيانات والمعلومات التعريفية الخاصة بالبنك المركزي العراقي فرع / الموصل وبناء تصور متكامل عن أنشطته وواقع حاله قدر تعلق الأمر بموضوع الدراسة، من خلال الزيارات المتكررة التي قامت بها الباحثة للمدة من (2024/3/1م) ولغاية (2024/6/1م) للبنك لغرض التعرف على الواقع الفعلي لطبيعة الأنشطة التي يمارسها للبنك والإجراءات التي يتخذها بصدد الامن السيبراني.

2. **إستمارة الإستبانة:** أعتمدنا على إستمارة الإستبانة بوصفها أداةً رئيسة لجمع البيانات والمعلومات وقياس أبعاد متغيرات الدراسة ، وتم تصميمها على نحو يتلاءم مع عينة الدراسة، و سعت الباحثة إلى إنشاء مقياس يتلاءم مع طبيعة المتغيرات بما ينسجم مع بيئة الميدان المبحوث وذلك عن طريق الزيارات الميدانية التي قامت بها الباحثة أولاً وعرضها على عدد من الخبراء ثانياً، ويرجع اعتماد الباحثة على هذا الأسلوب نتيجة لعدم القدرة على استحصال جميع أنواع البيانات من سجلات البنك لأنّ عدداً منها تعد بيانات سرية، إعتمدت الباحثة في قياس استجابة المبحوثين على مدرج (ليكرت) الخماسي الذي يعد ذو مرونة في اختيار مدى الاتفاق مع العبارات أو عدمها على مستوى جميع فقرات الإستبانة والمرتبة من عبارة (أتفق بشدة ، أتفق ، محايد ، لا أتفق ، لا أتفق بشدة) والتي حصلت على الأوزان الآتية (5 ، 4 ، 3 ، 2 ، 1) على التوالي.

سادسا: منهج الدراسة

تعتمد الدراسة الحالية على المنهج الوصفي التحليلي من خلال تركيزها على تشخيص الواقع وتحليله بشكل مفصل، وذلك بهدف التوصل إلى نتائج دقيقة تخدم البنك المركزي قيد الدراسة عن طريق التحليل الشامل للمشكلة ، فقد جرى دراسة وتحليل متغيرات مخطط الدراسة وبناء الفرضيات واختبارها بالاعتماد على استمارة استبانة قامت الباحثة بإعدادها لغرض معرفة وقياس آراء الأفراد عينة الدراسة في الميدان المبحوث حول دور المنظمة الحرباء في تحقيق ابعاد الأمن السيبراني.

سابعا: اختبار صدق الإستبانة وثباتها : لغرض قياس صدق الإستبانة وثباتها تم إخضاع الإستبانة لعدد من الاختبارات ، وذلك قبل البدء بتوزيعها على الأفراد المبحوثين في البنك المركزي ، إذ تمثلت هذه الاختبارات بالآتي :

1.الاختبارات قبل توزيع الإستبانة :

أ. قياس الصدق الظاهري :

بغية التأكد من قدرة الاستمارة على قياس متغيراتها أجريَ اختبار الصدق الظاهري لفقرات الإستبانة بعد الانتهاء من إعدادها وذلك من خلال عرضها على مجموعة من الخبراء المتخصصين في العلوم الإدارية للتأكد من صحة الفقرات ومدى ملاءمتها لفرضيات الدراسة وأهدافها إذ جرى استطلاع آراءهم بشأن قدراتها على قياس متغيرات الدراسة والتأكد من مدى وضوح فقراتها وسهولة فهمها من قبل المجيب ودقتها من الناحية العلمية ونوقشت الملاحظات وتم إجراء التعديلات اللازمة على الإستبانة حسب رأي الأغلبية.

2.الاختبارات بعد توزيع الإستبانة :

أ. اختبار ثبات المصداقية ألفا :

لقياس ثبات أداة القياس للأبعاد مجتمعة قمنا باستخدام معامل الفا الطبقي الذي أشار اليه (Feldt & Brennan,1989) والذي صنف قيم معامل الثبات الى مستويين، فالقيم الأكثر من (70%) تعتبر عالية المستوى، في حين تكون منخفضة إذا قلت قيمة معامل الثبات عن (70%)، ويبين الجدول (1) نتائج اختبار معامل كرونباخ الفا لكل بعد ومعامل الفا الطبقي للأبعاد مجتمعة،

$$\alpha_{st.} = 1 - [\frac{\sum_{i=1}^{m} \sigma_i^2 (1 - \alpha_i)}{\sigma_c^2}]$$

حيث تشير النتائج الى ان قيمة معامل ألفا الطبقي بلغت قيمته (0.95) وهي أكبر من (0.70)، وهذا يدل على قوة ثبات الاستمارة بوجة عام.

اذ ان:

σ_i^2 : تباين كل بعد (تباين مركبة مجموع الأسئلة لكل بعد).

σ_c^2 : تباين مركبة مجموع الابعاد.

α_i : معامل كرومباخ الفا لكل بعد.

m : عدد الابعاد.

الجدول (1) قياس الثبات لأبعاد الدراسة منفردة وبشكل كلي

المتغير	الابعاد	العبارات	معامل كرونباخ الفا لكل بعد α_i	معامل الفا الطبقي للأبعاد مجتمعة $\alpha_{st.}$
الأمن السيبراني	نزاهة البيانات والمعلومات	Y11-Y17	0.81	0.95
	توافر البيانات والمعلومات	Y21-Y27	0.86	
	سرية البيانات والمعلومات	Y31-Y37	0.83	

المصدر: إعداد الباحثة بالاستناد إلى مخرجات برنامج (SPSS V.26) n=199

***Source** :Feldt، L. S.، & Brennan، R. L. (1989). Reliability. In R. L. Linn (Ed.)، Educational measurement. Macmillan Publishing Co، Inc; American Council on Education. (pp. 105–146).*

ب. الاتساق الداخلي :

يعرف الاتساق الداخلي (Internal Consistency) بانه الترابط بين الاسئلة داخل البُعد الواحد، اذا اردنا قياس الاتساق الداخلي على مستوى البُعد ، كذلك يبين لنا مدى الترابط بين الاسئلة

جميعها داخل المتغير الواحد ، ويتم قياس الاتساق الداخلي من خلال متوسط (Mean) معاملات الارتباط (المطلقة) بين ازواج الارتباطات للأسئلة داخل البُعد او المتغير الواحد، وتشير المصادر انه إذا كانت قيمة هذا المتوسط أكبر من او يساوي (0.3) فهذا يدل على وجود اتساق داخلي، وتشير نتائج الجدول (2) الى وجود اتساق داخلي على مستوى كل متغير مع ابعاده، وذلك بدلالة القيمة المطلقة للوسط الحسابي للارتباطات (Mean) والتي ظهرت جميعها أكبر من (0.3).

جدول (2) قيم الاتساق الداخلي على مستوى المتغيرات والابعاد الفرعية التابعة لها

Inter-Item Correlations						
No of Items	Variance	Maximum	Minimum	Mean	الابعاد الفرعية	المتغيرات
7	110.0	5170.	1620.	3750.	نزاهة البيانات والمعلومات	الأمن السيبراني
7	400.0	5930.	3630.	0.470	توافر البيانات والمعلومات	
7	0140.	6050.	1880.	4110.	سرية البيانات والمعلومات	
21	0090.	6050.	0690.	3650.	الأمن السيبراني	

المصدر: إعداد الباحثة بالاستناد إلى مخرجات برنامج (SPSS V.26) n=199

M. et al. (2016). Educational measurement for applied researchers. Singapore: ،Wu
DOI: 10.1007/978-981-10-3302-5_2،Springer Nature Singapore Ltd.

ت. اختبار التوزيع الطبيعي

يعد اختبار التوزيع الاحتمالي للمتغيرات المدروسة من الشروط الاساسية في اي تحليل احصائي اذ تتطلب اغلب طرق التقدير واختبار الفرضيات شرطاً اساسياً، وهو في ان تمتك المتغيرات المدروسة توزيعاً احتمالياً وعادةً ما يكون هذا التوزيع هو التوزيع الطبيعي، وان عدم تحقق هذا الشرط يستوجب منا استخدام طرائق بديلة عن طريقة المربعات الصغرى في تقدير معلمات نموذج الانحدار مثل (طريقة المربعات الصغرى العمومية او طريقة التوزيع الحر او طريقة المربعات

الصغرى غير الموزونة ،... الخ) كذلك يتوجب علينا الاعتماد على الاختبارات اللامعلمية (التي لا تشترط التوزيع الطبيعي للمتغيرات) في تطبيق اختبار الفرضيات الاحصائية، ويعد معيار (Kolmogorov-Smirnov) احد اهم المعايير الاحصائية المستخدمة لاختبار التوزيع الطبيعي ويمتاز بملائمته لحجوم العينات الكبيرة، وتشير نتائج الاختبار الموضح في الجدول (3) الى ان نجد ان جميع القيم الاحتمالية (P-value) ظهرت اقل من (0.05) وهذا دليل على ان المتغيرات الاثنين بأبعادها لا تتبع التوزيع الاحتمالي الطبيعي.

جدول (3) قيم معيار (Kolmogorov-Smirnov) لفحص التوزيع الطبيعي لمتغيرات وابعاد الدراسة

Tests of Normality				
Kolmogorov-Smirnov				
النوع	الوصف	Statistic	N	P-value
الابعاد	نزاهة البيانات والمعلومات	.171	199	.000
	توافر البيانات والمعلومات	.175	199	.000
	سرية البيانات والمعلومات	.196	199	.000
	الأمن السيبراني	.158	199	.000

المصدر: إعداد الباحثة بالاستناد إلى مخرجات برنامج (SPSS V.26) n=199

ث. أساليب التحليل الإحصائي:

من أجل التوصل إلى مؤشرات دقيقة ، واستناداً إلى طبيعة توجهات الدراسة الحالية وأهدافها وآليات اختبار فرضياتها ، فقد اعتمد على البرنامج الاحصائي **(SPSS Statistics v.26, Amos)** لإجراء التحليل الاحصائي المطلوب ، وتتمثل هذه الأساليب بالآتي:

أ. **التكرارات** : لاستعراض الإجابات الخاصة بالمبحوثين .

ب. **النسب المئوية** : لبيان نسبة إجابة المبحوثين عن متغير معين من مجموع الإجابات .

ت. **الوسط الحسابي** : لعرض متوسط إجابات المبحوثين عن متغير معين .

ث. **الانحراف المعياري** : لتحديد تشتت إجابات المبحوثين عن وسطها الحسابي .

ج. **نسبة الاستجابة** : تحديد إستجابة المبحوثين ومواقفهم إزاء متغيرات الدراسة ، وتحسب وفق الصيغة الآتية (الطالبي،91،2015):

$$\text{نسبة الاستجابة إلى مساحة القياس} = \frac{\text{الوسط الحسابي لأجابات المبحوثين}}{\text{مساحة المقياس}} \times 100$$

ح. **اختبار (One-Sample test)** : لاختبار أي الابعاد اكثر توفراً.

ثامنا: مجتمع وعينة الدراسة

تمثل مجتمع الدراسة بالعاملين في البنك المركزي العراقي/ فرع الموصل، وإعتمدت الباحثة في اختيارها لعينة قصدية تمثلت بالأفراد المبحوثين ممن لديهم الخبرة والدراية وعلى علم بنشاط البنك المركزي ومهامه ضمانا لتحقيق الاستفادة من المعلومات الدقيقة والمفيدة المقدمة من قبلهم، إضافة إلى إمكانية الحصول على الأفكار والمقترحات التي تعزز من أهمية الدراسة، وانسجاما مع ذلك شرعت الباحثه بتوزيع (205) إستمارة شملت العاملين في البنك المركزي فرع الموصل، وتم الحصول على (199) إستمارة صالحة للتحليل، ويوضح الجدول (4) تفاصيل توزيع هذه الاستمارات:

الجدول (4) عدد الاستمارات الموزعة والمستلمة ونتيجة الاستجابة

عدد الإستمارات الموزعة	عدد الإستمارات المستلمة	نسبة الاستجابة	عدد الإستمارات المستبعدة	عدد الإستمارات الصالحة	نسبة الاستجابة
205	199	97.07%	6	199	100%

المصدر: إعداد الباحثة بالاعتماد على نتائج الاستمارة

المبحث الأول

الاطار النظري

اولاً: مفهوم الامن السيبراني

يمكن التركيز على مفهوم الأمن السيبراني من خلال الاستفادة من الابتكارات التقنية الحديثة والتقنيات المتقدمة في جميع جوانب الحياة اليومية لتغيير المفاهيم التقليدية لحماية المعلومات. في ظل الثورة التقنية الهائلة التي أدت إلى ظهور تحدي جديد يواجه المجتمع، وهي التهديدات الإلكترونية مثل الابتزاز والاحتيال. بالنظر إلى أن الأمن السيبراني هو قضية ذات أولوية بالنسبة للعديد من الدول، خاصة بعد ظهور الحروب الإلكترونية في بعض الدول الكبرى، فإنها تشير إلى نهاية الحروب التقليدية وبداية حروب جديدة، وهي الحروب الإلكترونية. ومن ثم، يتطلب الأمر وجود سياسة وتنسيق دقيق على مستوى عالٍ، مما يتطلب تطوير مفاهيم واستراتيجيات جديدة تتماشى مع مفاهيم الأمن السيبراني.

ويوضح (*Haaga, 2021, 9*) أن الاختلاف بين أمن المعلومات والأمن السيبراني يكمن في الانتقال من التركيز على حماية المعلومات إلى حماية المستخدمين أنفسهم الذي يستخدمون أنظمة المعلومات. ويروي (*Steiger, 2022, 2*) أن الفضاء السيبراني ليس مستقلاً بذاته، ولكنه يتعلق بشكل وثيق بأنظمة أخرى مثل شبكة الطاقة، والتي تعتمد على البنية التحتية للاتصالات في الواقع. وهذا يؤدي إلى تبعيات مشتركة لضمان أداء المجتمع على أرض الواقع.

وفيما يلي الجدول (5) يوضح أهم المفاهيم التي تعالجها الأمن السيبراني وفقًا لآراء عدد من الكتاب والباحثين.

الجدول (5) مفاهيم الأمن السيبراني بناءً على آراء بعض الباحثين

ت	الباحث، السنة، رقم الصفحة	التعريف
2	***Onumo, 2020,*** ***(22***)	هو عملية تتطلب مجموعة من الأدوات والتقنيات التي يطبقها الأفراد والمنظمات لحماية أصول تقانة المعلومات والحفاظ على المبادئ الأمنية للمعلومات الواردة والمنقولة عبر شبكات مترابطة.
3	***Aljohni et al,*** ***(2021, 276***)	استراتيجية أمنية ضد لهجمات الخبيئة المصممة للوصول إلى أو تعديل أو حذف أو تدمير أو ابتزاز الأنظمة الالكترونية المتصلة بالشبكة العنكبوتية
4	**(*Aksoy, 2023, 52*)**	مجموعة من التدابير المتخذة لضمان أمن أنظمة الحاسوب والشبكات والبرامج والبيئات الرقمية الأخرى، فهو وسيلة يتم استخدامها لمكافحة التهديدات مثل الجرائم السيبرانية والهجمات السيبرانية والإرهاب السيبراني والتجسس السيبراني.
5	**(*BUTEL, 2023, 3*)**	تطبيق التقنيات لضمان سرية وسلامة وتوافر معلومات المنظمة والبنية التحتية من قبل الباحثين ومتخصصي تقانة المعلومات.

المصدر : الجدول من إعداد الباحثة بالاعتماد على المصادر الواردة فيه.

وبناءً على ما سبق، ترى الباحثة أن مفهوم الأمن السيبراني يتألف من مجموعة من السياسات والتقنيات والإجراءات التي تهدف إلى حماية البيانات والمعلومات الإلكترونية من التجسس أو الاختراق غير المصرح به. ويشمل ذلك استخدام التقنيات الأمنية ووضع السياسات الداعمة وتنفيذ الإجراءات الوقائية والتصحيحية لمنع واكتشاف والاستجابة لأي هجوم أو تهديد على أنظمة الاتصالات والمعلومات الحيوية.

ثانيا: ضوابط الامن السيبراني

تمثل ضوابط الأمن السيبراني الإجراءات والسياسات والتقنيات التي تهدف إلى حماية الأنظمة والبيانات الإلكترونية من الهجمات والتهديدات السيبرانية كونها تعد أساسية في العالم الرقمي، حيث تتزايد الاعتمادات على التقانة وتبادل البيانات عبر الإنترنت، بهدف الحفاظ على سلامة البيانات والأنظمة الرقمية وضمان استمرارية العمليات بشكل آمن وموثوق به، حيث يرى

(*Creese et al., 2021, 1*) ان هناك خمسة ضوابط ضرورية لتحسين الأمن السيبراني في المنظمات تمثلت في:

1. استخدام جدار حماية لتأمين الانتماء الخاص بالفرد.
2. اختيار الإعدادات الأكثر أمانا للأجهزة والبرامج الشخصية.
3. التحكم في مَن يمكنه الوصول إلى البيانات والخدمات (الشخصية) ذات العلاقة بالفرد نفسه.
4. توعية الفرد بحماية نفسه من الفيروسات والبرامج الضارة الاخرى.
5. الاحتفاظ بعمليات تحديث الأجهزة والبرامج.

ثالثا: التهديدات السيبرانية

أشار الباحثين الى خمسة أنواع أساسية من التهديدات السيبرانية، والتي يمكن للمنظمة تحقيق أهدافها الامنية فيما لو تم تجاوزها او تلافيها، وتتمثل هذه التهديدات في القرصنة والجريمة السيبرانية والتجسس السيبراني والإرهاب السيبراني والحرب الإلكترونية (*Ahokas et al., 2017, 348*)، والجدول (6) يبين أنواع التهديدات السيبرانية والسمات الفردية للجهات الفاعلة

الجدول (6) أنواع التهديدات السيبرانية والسمات الفردية للجهات الفاعلة

التهديدات السيبرانية	تتمثل بالمتعاملين بالتهدين	الدوافع	الأهداف
القرصنة	المتسللون الهاكرز من الافراد	السمعة والأنانية السياسية	احداث الاضطرابات و لفت الانتباه
الجريمة السيبرانية	الجواسيس صناع الجريمة المنظمة من الافراد	المعلومات الاقتصادية	البيانات التنظيمية للأصول الرقمية
التجسس الالكتروني	الجواسيس صناع الجريمة الحكومية المنظمة	الإيديولوجية الإعلامية والسياسية	البيانات التنظيمية المعرفية للأصول الرقمية
الإرهاب الالكتروني	الحكومات الإرهابية	الإيديولوجية السياسية والدينية والاجتماعية	اضطرابات المنظمات الوطنية والبنى التحتية الحرجة
الحرب الالكترونية	الحكومات الإرهابية	الانانية السياسية والدينية والاجتماعية	اهداف عسكرية وطنية نافذة

المصدر: من اعداد الباحث بالرجوع الى Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L ،M ،(2017)، rsecurity in ports: a conceptual approach ،In Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment، Proceedings of the Hamburg International Conference of Logistics (HICL), Vol 23، p349.

رابعا: عوامل نجاح الامن السيبراني:

نظراً لأن المنظمات المختلفة تواجه تحديات عديدة في مجال الأمن السيبراني، كانت الفكرة هي التماس وفهم المتطلبات الأساسية لنجاح تنفيذ الأمن السيبراني، ويرى (*Choejey et al, 2016, 55*) و (*Yeoh et al., 2022, 12-13*) و (*Atkins & Lawson, 2021, 6*) أن أهم خمسة عوامل نجاح للأمن السيبراني للمنظمات هي:

1. التوعية والتدريب والتعليم

يعد التدريب والتعليم الخاصين بالعاملين أمراً ضرورياً لمكافحة التهديدات الأمنية في مجال تقنية المعلومات، حيث أن تعزيز الوعي الأمني لدى الموظفين العاديين يمكن أن يحول دون تعرضهم ليصبحوا النقطة الضعيفة في أي منظمة، أو هدفاً سهلاً للمجرمين على الإنترنت. بالإضافة إلى ذلك، يعد الوعي والتدريب أمراً هاماً أيضاً بالنسبة للموظفين العاملين في المستويات العليا للمنظمة، حيث أن الأفراد الذين يمتلكون امتيازات وحقوق وصول ذات صلاحيات تفوق قواعد الأمان قد يتخذون قرارات جانحة للمصلحة، بهدف تحقيق أكبر قدر من الفوائد بغض النظر عن التكلفة أو الأثر السلبي لهذا القرار.

2. السياسة والمعايير والإجراءات الأمنية للمنظمة

تعد السياسة الأمنية أساسية في تخطيط وإدارة وصيانة الأمن السيبراني. تهدف السياسة إلى تنفيذ المعايير التي تعزز تطبيق الممارسات والإجراءات والمبادئ التوجيهية بشكل فعّال. لذلك، يجب أن تكون السياسة الأمنية في المؤسسة مرنة وقابلة للتكيف والمراجعة باستمرار لتعكس تغيرات البيئة المحيطة. ويعد تخصيص الميزانية الأمنية أساسيًا لأي مبادرات أمنية قد تتخذها أي مؤسسة. فدون

الميزانية والموارد المالية، ستكون من المستحيل بدء أو تنفيذ هذه المبادرات والأنشطة بنجاح. فالميزانية هي العنصر المركزي في دعم التدريب والتوعية والسياسة الأمنية والبنية التحتية الأمنية. ودون الالتزام بالميزانية والموارد المالية، لا يمكن تنفيذ أي من هذه العوامل ومن ثم لا يمكن تحقيق الأمن السيبراني بنجاح.

3. تمويل موارد الأمن السيبراني

في ظل التقدم السريع للتقانة وزيادة التهديدات السيبرانية، أصبحت استراتيجيات الأمان السيبراني ضرورية وحيوية للمؤسسات في جميع القطاعات. الآن، التحديات الرئيسية التي تواجه المؤسسات تتعلق بتمويل وتوفير الموارد لضمان الأمان السيبراني. يجب على المؤسسات الاستثمار في البنية التحتية السيبرانية القوية وفرق الخبراء والتقنيات الحديثة لمكافحة التهديدات المتزايدة. البنية التحتية الأمنية، مثل الأجهزة والبرامج، تعد ذات أهمية كبيرة لتلبية متطلبات أمان المؤسسة. الأمن السيبراني ليس مجرد مشكلة إدارية، بل هو مشكلة تقنية أيضًا. بالتالي، يتم استخدام آليات أمنية مثل جدران الحماية وحلول مكافحة الفيروسات على نطاق واسع لحماية موارد المعلومات من انتهاكات الأمان.

4. دعم الإدارة العليا للأمن السيبراني

ان نجاح جهود الأمن السيبراني يعتمد إلى حد كبير على التزام ودعم الإدارة العليا، إذ تعد القضايا الإدارية من أهم القضايا الأمنية وتتطلب مشاركة الإدارة لحلها، كما ان دعم الإدارة العليا والتزامها ليس مهماً فقط لتخطيط القرارات الأمنية وتنفيذها وإدارتها، بل انه مهم أيضاً لتثبت لأصحاب المصلحة أن استثماراتهم في امان، لذلك من المهم لأي منظمة أن يكون لديها مديرين أمنيين أكفاء وقادرين على قيادة الحوكمة الأمنية.

5. التدقيق والامتثال للأمن السيبراني

يمثل تدقيق الأمن السيبراني والامتثال نقطة انطلاق حيوية لفهم أهمية هذا المجال المتزايد في عالم التقانة الحديثة، إذ يعد تدقيق الأمن السيبراني والامتثال جانبان حيويان يتعلقان بحماية البيانات وضمان امتثال المنظمات للمعايير والقوانين الصارمة المتعلقة بالخصوصية والأمان، وتتزايد

المخاطر السيبرانية باستمرار، وتتطور بسرعة مع تقدم التقنية، مما يجعل ضرورة فحص ومراجعة النظم والسياسات المتعلقة بالأمان والامتثال أمراً لا غنى عنه.

خامسا: ابعاد الامن السيبراني

لقد اختلف الباحثون والدارسون في تحديد أبعاد الأمن السيبراني سواء ما يتعلق بعددها أو تسميتها ويمكن ارجاع ذلك إلى حيوية هذه الأبعاد وتجددها برغم حداثتها، وقد تناول البحث الابعاد التالية لكونها اكثر الابعاد توافقاً مع الميدان المبحوث كونها واحدة من المنظمات الخدمية التي تعتمد تلك الابعاد في تنفيذ مهام عملها الرسمي ما يتوفر في عينة الدراسة:

1. نزاهة البيانات والمعلومات:

يعد مفهوم النزاهة من المفاهيم الاساسية في الحياة العلمية والعملية، حيث يمكن استخدام هذا المصطلح في عدة مواضع مثل الحديث عن نزاهة منظمة او المورد البشري او أداء الاعمال وغيرها التي تدخل في صلب عمل المنظمة (*Erhard et al., 2009, 14*)، ففي كثير من الأحيان يشار إلى النزاهة بمبدأ أو قيمة معينة مثل الصدق أو الموضوعية أو الاستقامة أو الالتزام بالقواعد أو الاتساق بين القول والفعل في حين وصفت في مواضع أخرى بأنها سمعة لا تشوبها شائبة وترتبط في معظم الأحيان بالثقة بالنفس باعتبارها شكلًا من أشكال الوضوح المطلق ، في حين يراها اخرون كالضمير أو مسألة أخلاقية أو التزامًا أخلاقيًا (*wisesa, 2016, 53*)، ومن ثم فان مصطلح النزاهة يعد الركيزة الأساسية التي يركز عليها اغلب الباحثين وان اختلفوا او اتفقوا في تحديد هذه المفاهيم سواء كانت من منظور اخلاقي او سلوكي او بشكلها العام.

وأوضح (*الحسناوي والفتلاوي، 2016، 195*) بان النزاهة في مجال الأمن السيبراني تضمن بقاء البيانات التي يتم إرسالها أو تخزينها ثابتة، اي عدم إمكانية تعديل الرسائل المرسلة دون علم القائمين عليها ، وأن البيانات التي يتم إرسالها إلى طرف ثاني هي البيانات نفسها التي يتلقاها الطرف الثالث داخل النظام (*Yurkovich, 2022, 10*)، وهنالك العديد من الأسباب التي تؤدي لحدوث مشاكل تؤثر على موثوقية البيانات، ويمكن ايجازها في(*Koumandaros, 2021, 42-43*):

- نسخ البيانات الموجودة كبيانات جديدة.

- الاحتفاظ بمجموعات مكررة من السجلات.
- مراجعة العمل والموافقة عليه دون مراجعة البيانات.
- عدم كفاية التحقيقات لتقييم وتنفيذ الإجراءات التصحيحية لممارسات سلامة البيانات الضعيفة.
- إعداد النظام للتخلص تلقائياً من النتائج السلبية، ومعالجة البيانات للحصول على نتائج إيجابية.
- عدم التحقق من صحة الطرق التحليلية.
- عدم التحقق من صحة الأنظمة المحوسبة.

2. توافر البيانات والمعلومات

تشير خاصية التوافر في مجال الأمن السيبراني إلى ضمان إمكانية الوصول إلى البيانات والموارد للمستخدمين المصرح لهم عند الحاجة، وهي إحدى الركائز الثلاث لأمن المعلومات إلى جانب السرية والنزاهة، والتي تشكل معاً ثالوث مبادئ أمن المعلومات، ويعد توافر البيانات أمراً بالغ الأهمية لأنه يمكّن المنظمات من مراقبة بيئاتها بحثاً عن التهديدات المحتملة، والاستجابة للحوادث على الفور، واتخاذ قرارات مستنيرة لتعزيز الوضع الأمني العام، إذ ان النظام الآمن يؤمن استمرارية وصول المستخدمين إلى المعلومات الخاصة بهم دون أي تأخير، ولهذه الخاصية عدد من الخصائص المتمثلة في (*البحيصي، 2013، 46*):

- **المقاومة:** وهي قدرة النظام للحفاظ على نفسه من عمليات الاختراق التي تجعله غير متاح للمستخدمين المخولين باستخدامه، (على سبيل المثال أن يكون النظام قادرا على منع تنفيذ استعلامات تتطلب حجز حيز كبير من ذاكرة الخادم).
- **سهولة الاستخدام:** يؤدي دورا توافر البيانات دورا حاسما في تسهيل استخدام التقانة وتطوير الحلول الذكية في مختلف المجالات، إذ انه يسهم في تحسين دقة النماذج والخوارزميات، وتحسين تجربة المستخدم، فضلا عن تحسين الأمان والخصوصية، حيث يمثل هذا توافر أساسا لتقديم حلول فعّالة ومستدامة، ويسهم بشكل كبير في تسهيل استخدام التقانة وتقديم تجارب مستخدم محسنة.
- **المرونة:** تكمن في توفر الإمكانيات والأدوات التي تمكن من إدارة النظام بالشكل السليم دون أن يستدعي ذلك إلى توقفه.

3. سرية البيانات والمعلومات

تختلف أهمية المعلومات ومدى السرية المطلوبة للحفاظ عليها، ومن ثم يصعب وضع نظام قياسي لتصنيف المعلومات يغطي جميع الأغراض المطلوبة ويكون مناسبًا لجميع الحالات، فليست جميع المعلومات بحاجة إلى درجة الحمادية نفسها، على سبيل المثال، المعلومات الخاصة بالمنظمات الكبيرة التي يترصد منافسوها التأثير على عمليات الإنتاج، فهؤلاء يبذلون كل الجهود للوصول إلى المعلومات الهامة واستخدامها في مصلحتهم (*Lane, 2007, 171*)، لذا أشار (*أبو نبيب، 2019، 9-10*) إلى المعلومات التي تتطلب توافر حماية فائقة بالشكل الذي يسهم في انجاز المهام والاعمال بالشكل السليم والناجح تتمثل في (الأسرار الداخلية للمنظمة، المعلومات المالية، معلومات تخص الموارد البشرية، الأسرار التجارية، المعلومات المؤقتة، المعلومات التقنية، معلومات الزبائن، المعلومات الأمنية، سلعة المعلومات)، لذا فإن هناك مجموعة من الوسائل والإجراءات الواجب إتباعها لضمان امن وحماية المعلومات تتمثل في (*أبو حجر وآخرون، 2014، 27-28*):

- **ضمان امن وحماية كلمة السر**: وهذه الوسيلة تعد من الوسائل التي يجب أن تضمن الحفاظ على كلمات السر للميولة دون الوصول غير المشروع إليها فبعض كلمات السر يسهل تخمينها، وهنا يجب اختيار كلمات سر تميل إلى التعقيد وان تكون طويلة نوعا ما ويجب التأكيد على ضرورة عدم الاحتفاظ بكلمات السر في أماكن يسهل الوصول.
- **ضمان التوثيق:** وتتم هذه الوسيلة من خلال تحديد المهام المسندة الى الموظفين ومعرفة كل موظف وطبيعة المهام المسندة اليه حتى لا تتداخل المهام ومن ثم صعوبة رصد مراكز الخلل مع وضع نظم التشغيل تحت الرقابة وذلك من خلال مراقبة القائمين عليها.
- **ضمان سلامة الوسائل والإجراءات المتبعة في ضمان امن وحماية المعلومات:** ويتم ذلك من خلال تفعيل نظام رقابة وتحديد المخولين بالدخول الأمن للمعلومات والتعامل معها ويجب التركيز هنا على الآليات المتبعة من قبل الموظفين عند حدوث خلل ما أو مواجهة ما يطرأ على المعلومات من مخاطر وما يستوجب على الموظف من تصرفات لحفظ امن وسرية المعلومات.

- **ضمان معرفة الموظفين بالسياسات والمعايير:** حيث تحفظ امن وحماية المعلومات وتقييم مدى انعكاس ذلك على الأمن الكامل للمعلومات ومتابعة مصادر المخاطر والخلل بشكل دوري ليتم التأكد من تأثيرها على امن وحماية المعلومات، وتجنبا للوصول غير المشروع لأمن المعلومات تم الاستناد إلى بعض الوسائل الكافية أمام الزبائن من الاستخدام الأمن للدخول إلى مواقعهم دون معيقات.

المبحث الثاني

الاطار الميداني

أولا: وصف وتشخيص اجابات المبحوثين عن متغير الأمن السيبراني.

يشير مضمون هذه الفقرة إلى وصف متغير الأمن السيبراني وتشخيصه بدلالة الابعاد المعبرة عنه في ضوء اجابات المبحوثين عن الفقرات المجسدة لكل منها وعلى النحو الآتي:

1. نزاهة البيانات والمعلومات

تؤشر معطيات الجدول (7) وجود اتفاق بين آراء الأفراد المبحوثين بشأن فقرات بُعد **نزاهة البيانات والمعلومات** للعبارات (Y11-Y17)، اذ بلغ معدل الاتفاق العام لإجابات الأفراد المبحوثين بالاتفاق (أتفق بشدة، أتفق) (77.67%) وهذا يدل على ان هناك درجة اتفاق لإجابات الأفراد المبحوثين على فقرات بُعد **نزاهة البيانات والمعلومات**، أي ان آراء الأفراد المبحوثين تتجه نحو الإيجاب بالاعتماد على مقياس (ليكرت) الخماسي، في حين بلغت درجة عدم الاتفاق العام (لا أتفق بشدة، لا أتفق) لإجابات الأفراد المبحوثين على فقرات بُعد **نزاهة البيانات والمعلومات** (5.24%)، أما عن نسبة الإجابات محايدين فهي (17.09%)، وكان الوسط الحسابي (3.94) والانحراف المعياري (0.81)، وبلغ معدل الاهمية النسبية لبُعد **نزاهة البيانات والمعلومات** (78.81%)، وهي أهمية نسبية جيدة، مما يعني اتفاق الأفراد المبحوثين وبدرجة واضحة حول هذه الفقرات وفقا لوجهة نظرهم الشخصية.

اما على المستوى الجزئي فأن فقرة (Y15) والتي تُمثل **ادارة المنظمة تتحقق من سلامة وصحة الأنظمة المحوسبة لديها بشكل مستمر**، حصلت على أعلى اهمية نسبية بلغت (81.31%) وبوسط حسابي (4.07) وانحراف معياري قدرهُ (0.68)، في حين أن فقرة (Y12) حققت أقل اهمية نسبية

ما قدره (76.78%) والذي يُمثل **ادارة المنظمة تتجنب الاحتفاظ بمجموعات مكررة من السجلات،** وذلك باتفاق عينة الدراسة بنسبة (74.37%) وبوسط حسابي (3.84) وانحراف معياري (0.84). تشير نتائج قيمة One-Sample test البالغة 24.057 مع درجة حرية 198 = (df) والقيمة الاحتمالية 0.000 = (sig) إلى أن هناك فرقًا كبيرًا بين المتوسط الفعلي لاستجابات العينة على بُعد "نزاهة البيانات والمعلومات" والقيمة المرجعية المفترضة، أي أن المتوسط الفعلي لبُعد نزاهة البيانات والمعلومات أقل بشكل ملحوظ من القيمة المرجعية التي تم افتراضها، كما ان الدلالة الإحصائية العالية (p-value = 0.000) تعني أن هذا الفرق ذو دلالة إحصائية قوية، مما يشير إلى أن الفروق الملحوظة ليست ناتجة عن الصدفة وإنما تعكس حقيقة إحصائية يمكن الاعتماد عليها، بالتالي فإن بُعد "نزاهة البيانات والمعلومات" موجود في الميدان المبحوث، ولكنه لا يصل إلى المستوى المرجعي المتوقع، إذ ان الفرق الكبير والسالب يشير إلى أن هناك حاجة لتعزيز نزاهة البيانات والمعلومات في الميدان المبحوث للوصول إلى المستوى المرجعي المرغوب.

الجدول (7) التوزيعات التكرارية والاوساط الحسابية والانحرافات المعيارية والأهمية النسبية لبُعد نزاهة البيانات والمعلومات

الفقرات	مقياس الاستجابة										الوسط الحسابي	الانحراف المعياري	الاهمية النسبية%	ترتيب الفقرات
	أتفق بشدة (5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق بشدة (1)					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
Y11	41	20.60	110	55.28	36	18.09	8	4.02	4	2.01	3.88	0.85	77.69	6
Y12	36	18.09	112	56.28	37	18.59	11	5.53	3	1.51	3.84	0.84	76.78	7
Y13	41	20.60	108	54.27	39	19.60	10	5.03	1	0.50	3.89	0.80	77.89	5
Y14	47	23.62	112	56.28	29	14.57	10	5.03	1	0.50	3.97	0.79	79.50	2
Y15	49	24.62	118	59.30	28	14.07	4	2.01	0	0.00	4.07	0.68	81.31	1
Y16	48	24.12	107	53.77	34	17.09	6	3.02	4	2.01	3.95	0.85	78.99	4

Y17	55	27.64	98	49.25	35	17.59	8	4.02	3	1.51	3.97	0.87	79.50	3
المعدل العام		22.76		54.92		17.09		4.09		1.15	3.94	0.81	78.81	
المجموع	77.67				17.09		5.24							
قيمة t-test					24.057		df				198	sig	0.000	

المصدر: إعداد الباحثة بالاستناد إلى مخرجات برنامج (SPSS V.26) n=199

2. توافر البيانات والمعلومات

تشير معطيات الجدول (8) الى وجود اتفاق بين آراء الأفراد المبحوثين بشأن فقرات بُعد **توافر البيانات والمعلومات** للعبارات (Y21-Y27)، اذ بلغ معدل الاتفاق العام لإجابات الأفراد المبحوثين بالاتفاق (أتفق بشدة، أتفق) (80.98%) وهذا يدل على ان هناك درجة اتفاق لإجابات الأفراد المبحوثين على فقرات بُعد **توافر البيانات والمعلومات**، أي ان آراء الأفراد المبحوثين تتجه نحو الإيجاب بالاعتماد على مقياس (ليكرت) الخماسي، في حين بلغت درجة عدم الاتفاق العام (لا أتفق بشدة، لا أتفق) لإجابات الأفراد المبحوثين على فقرات بُعد **توافر البيانات والمعلومات** (3.23%)، أما عن نسبة الإجابات محايدين فهي (15.79%)، وكان الوسط الحسابي (4.03) والانحراف المعياري (0.76)، وبلغ معدل الاهمية النسبية لبُعد **توافر البيانات والمعلومات** (80.66%)، وهي أهمية نسبية جيدة، مما يعني اتفاق الأفراد المبحوثين وبدرجة واضحة حول هذه الفقرات وفقا لوجهة نظرهم الشخصية.

اما على المستوى الجزئي فأن فقرة (Y22) والتي تُمثل **ادارة المنظمة تحسن تجارب المستخدمين وتحسين الأمن والخصوصية**، حصلت على أعلى اهمية نسبية بلغت (81.61%) وبوسط حسابي (4.08) وانحراف معياري قدرهُ (0.74)، في حين أن فقرة (Y24) حققت أقل اهمية نسبية ما قدره (79.30%) والذي يُمثل **ادارة المنظمة تلجأ الى التوسع في المعلومات من حيث الكم والنوع وبما يضمن توفيرها للمستفيدين**، وذلك باتفاق عينة الدراسة بنسبة (78.39%) وبوسط حسابي (3.96) وانحراف معياري (0.82). كما تشير نتائج قيمة One-Sample test البالغة 26.077 مع درجة حرية 198 = (df) والقيمة الاحتمالية 0.000 = (sig) إلى أن هناك فرقًا كبيرًا بين المتوسط

الفعلي لدرجات استجابة عينة الدراسة على بُعد "توافر البيانات والمعلومات" وبين القيمة المرجعية المفترضة، أي أن المتوسط الفعلي أقل بشكل ملحوظ من القيمة المرجعية، كما ان الدلالة الإحصائية العالية (p−value = 0.000) تشير إلى أن هذا الفرق ذو دلالة إحصائية قوية، ما يعني أن الفروق ليست ناتجة عن الصدفة، بل إنها تعكس حقيقة إحصائية يمكن الاعتماد عليها، بالتالي فإن بُعد "توافر البيانات والمعلومات" موجود بشكل كبير في الميدان المدروس، ولكن ليس بالقدر المتوقع وفقًا للقيمة المرجعية التي تم الافتراض بها.

الجدول (8) التوزيعات التكرارية والاوساط الحسابية والانحرافات المعيارية والأهمية النسبية لبُعد توافر البيانات والمعلومات

الفقرات	مقياس الاستجابة										الوسط الحسابي	الانحراف المعياري	الاهمية النسبية%	ترتيب الفقرات
	أتفق بشدة (5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق بشدة (1)					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
Y21	58	29.15	104	52.26	31	15.58	6	3.02	0	0.00	4.08	0.75	81.51	2
Y22	54	27.14	115	57.79	23	11.56	6	3.02	1	0.50	4.08	0.74	81.61	1
Y23	48	24.12	111	55.78	36	18.09	4	2.01	0	0.00	4.02	0.71	80.40	5
Y24	48	24.12	108	54.27	34	17.09	6	3.02	3	1.51	3.96	0.82	79.30	7
Y25	57	28.64	97	48.74	36	18.09	8	4.02	1	0.50	4.01	0.82	80.20	6
Y26	47	23.62	117	58.79	31	15.58	4	2.01	0	0.00	4.04	0.69	80.80	3
Y27	51	25.63	113	56.78	29	14.57	4	2.01	2	1.01	4.04	0.76	80.80	4
المعدل العام		26.06		54.92		15.79		2.73		0.50	4.03	0.76	80.66	
المجموع	80.98				15.79		3.23							
قيمة t-test					26.077		df				198	sig	0.000	

المصدر: إعداد الباحثة بالاستناد إلى مخرجات برنامج (SPSS V.26) n=199

3. سرية البيانات والمعلومات

يتبيَن من معطيات الجدول (9) وجود اتفاق بين آراء الأفراد المبحوثين بشأن فقرات بُعد **سرية البيانات والمعلومات** للعبارات (Y31-Y37)، اذ بلغ معدل الاتفاق العام لإجابات الأفراد المبحوثين بالاتفاق (أتفق بشدة، أتفق) (84.78%) وهذا يدل على ان هناك درجة اتفاق لإجابات الأفراد المبحوثين على فقرات بُعد **سرية البيانات والمعلومات،** أي ان آراء الأفراد المبحوثين تتجه نحو الإيجاب بالاعتماد على مقياس (ليكرت) الخماسي، في حين بلغت درجة عدم الاتفاق العام (لا أتفق بشدة، لا أتفق) لإجابات الأفراد المبحوثين على فقرات بُعد **سرية البيانات والمعلومات** (4.09%)، أما عن نسبة الإجابات محايدين فهي (11.13%)، وكان الوسط الحسابي (4.11) والانحراف المعياري (0.80)، وبلغ معدل الاهمية النسبية لبُعد **سرية البيانات والمعلومات** (82.20%)، وهي أهمية نسبية جيدة، مما يعني اتفاق الأفراد المبحوثين وبدرجة واضحة حول هذه الفقرات وفقا لوجهة نظرهم الشخصية.

اما على المستوى الجزئي فأن فقرة (Y34) والتي تُمثل **توجه ادارة المنظمة جميع مستخدمي الحاسوب في المنظمة إلى عدم ترك الأجهزة مفتوحة دون استخدام،** حصلت على أعلى اهمية نسبية بلغت (83.41%) وبوسط حسابي (4.17) وانحراف معياري قدرهُ (0.77)، في حين أن فقرة (Y31) حققت أقل اهمية نسبية ما قدره (81.01%) والذي يُمثل **ادارة المنظمة تنظم دورات تدريبية لتوعية العاملين لديها،** وذلك باتفاق عينة الدراسة بنسبة (83.42%) وبوسط حسابي (4.05) وانحراف معياري (0.79). تشير نتائج قيمة One-Sample test البالغة 27.917 مع درجة حرية 198 = (df) والقيمة الاحتمالية 0.000 = (sig) إلى أن هناك فرقًا كبيرًا بين المتوسط الفعلي لاستجابات العينة حول بُعد "سرية البيانات والمعلومات" والقيمة المرجعية المفترضة، وهذا يشير إلى أن المتوسط الفعلي أقل من القيمة المرجعية التي تم افتراضها، كما ان الدلالة الإحصائية العالية (p-value = 0.000) تعني أن هذا الفرق ليس صدفة بل هو ذو دلالة إحصائية قوية، مما يشير إلى أن الفروق الملحوظة هي نتيجة لاتجاه حقيقي في البيانات، بالتالي فإن بُعد "سرية البيانات

والمعلومات" كما تم قياسه في هذه الدراسة موجود بشكل كبير، ولكنه لا يصل إلى المستوى المتوقع أو المرجعي، وان الفرق بين القيمة الفعلية والمرجعية ذو دلالة إحصائية كبيرة، مما يعني أن هناك مجالًا لتحسين مستوى سرية البيانات والمعلومات في الميدان المبحوث.

الجدول (9) التوزيعات التكرارية والاوساط الحسابية والانحرافات المعيارية والأهمية النسبية لبُعد سرية البيانات والمعلومات

الفقرات	مقياس الاستجابة										الوسط الحسابي	الانحراف المعياري	الاهمية النسبية%	ترتيب الفقرات
	أتفق بشدة (5)		أتفق (4)		محايد (3)		لا أتفق (2)		لا أتفق بشدة (1)					
	عدد	%	عدد	%	عدد	%	عدد	%	عدد	%				
Y31	54	27.14	112	56.28	24	12.06	7	3.52	2	1.01	4.05	0.79	81.01	7
Y32	55	27.64	114	57.29	25	12.56	3	1.51	2	1.01	4.09	0.74	81.81	5
Y33	62	31.16	104	52.26	24	12.06	7	3.52	2	1.01	4.09	0.81	81.81	6
Y34	70	35.18	101	50.75	21	10.55	6	3.02	1	0.50	4.17	0.77	83.42	1
Y35	70	35.18	99	49.75	23	11.56	7	3.52	0	0.00	4.17	0.76	83.32	2
Y36	62	31.16	106	53.27	22	11.06	6	3.02	3	1.51	4.10	0.82	81.91	4
Y37	66	33.17	106	53.27	16	8.04	4	2.01	7	3.52	4.11	0.90	82.11	3
المعدل العام		31.51		53.27		11.13		2.87		1.22	4.11	0.80	82.20	
المجموع	84.78				11.13		4.09							
قيمة t-test					27.917		df				198	sig	0.000	

المصدر: إعداد الباحثة بالاستناد إلى مخرجات برنامج (SPSS V.26) n=199

4. خلاصة وصف متغير ابعاد الأمن السيبراني.

تأسيسا على ما تقدم يمكن القول ان جميع الإجابات ولكل بعد من ابعاد متغير **الأمن السيبراني** كانت اعلى من الوسط الحسابي الفرضي البالغ (3)، وان الجدول (10) يوضح الأهمية النسبية لأبعاد **الأمن السيبراني** من وجهة نظر عينة من الملاكات في البنك المركزي العراقي فرع /الموصل عن طريق قيم الوسط الحسابي والانحراف المعياري والاهمية النسبية حيث تبين لنا ان اهم الابعاد لمتغير **الأمن السيبراني** نسبيا هو بُعد **سرية البيانات والمعلومات** وذلك بدلالة قيمة الوسط الحسابي البالغ (4.11) والانحراف المعياري (0.80) وبأهمية نسبية بلغت (82.20%)، في حين ان بُعد **نزاهة البيانات والمعلومات** تبين ان اقل الابعاد أهمية وذلك بدلالة قيمة الوسط الحسابي التي بلغت (3.94) والانحراف المعياري (0.81) وبأهمية نسبية قدرها (78.81%). اما فيما يخص توافر ابعاد الامن السيبراني فمن خلال النظر إلى نتائج تحليل (T.Test) المعروضة في الجدول (3)، يمكن تحديد البعد الأكثر توافرًا في الميدان المبحوث بناءً على قيمة t–test، إذ ان البعد ذو القيمة الأقل يمثل البعد الأكثر توافرًا في الميدان المبحوث، حيث أن الفرق بين المتوسط والقيمة المرجعية يكون أقل النتائج، وتشير النتائج الى البعد الأكثر توافرا هو بعد نزاهة البيانات والمعلومات فقد بلغت قيمة (t–test = 24.057)،)، حيث أن قيمة t–test لهذا البعد هي الأعلى مقارنة بالأبعاد الأخرى، مما يعني أن هناك أقل فرق بين متوسط هذا البعد والقيمة المرجعية، وبالتالي هو الأكثر توافرًا في الميدان، ثم جاء بعده بعد توافر البيانات والمعلومات بقيمة (t–test = 26.077)، وجاء في المرتبة الأخيرة بعد سرية البيانات والمعلومات بقيمة (t–test = 27.917) وهو الأقل توافرا بين الابعاد الثلاثة في الميدان المبحوث. تشير النتائج الموضحة في الجداول السابقة والملخصة في الجدول (10) الى توافر مكونات ابعاد الامن السيبراني في البنك المركزي العراقي / فرع الموصل، وان البنك يستجيب لإقامة مكونات ابعاد الامن السيبراني، بالتالي يمكن قبول فرضية الدراسة.

الجدول (10) ترتيب أبعاد الأمن السيبراني

ت	الأبعاد	الوسط الحسابي	لانحراف المعياري	الاهمية النسبية%	t-te قيمة	df	sig	الترتيب

1	سرية البيانات والمعلومات	4.11	0.80	82.20	27.917	198	0.000	الثالث
2	توافر البيانات والمعلومات	4.03	0.76	80.66	26.077	198	0.000	الثاني
3	نزاهة البيانات والمعلومات	3.94	0.81	78.81	24.057	198	0.000	الاول

المصدر: إعداد الباحثة بالاستناد إلى مخرجات برنامج (SPSS V.26) n=199

المبحث الثالث: الاستنتاجات والتوصيات:

4-1 : الاستنتاجات:

1. ان ادارة المنظمة تلجأ الى التوسع في المعلومات من حيث الكم والنوع وبما يضمن توفيرها للمستفيدين إن بُعد توافر البيانات والمعلومات موجود بشكل كبير في الميدان المدروس، ولكن ليس بالقدر المتوقع
2. إن بُعد سرية البيانات والمعلومات موجود بشكل كبير، ولكنه لا يصل إلى المستوى المتوقع، مما يعني أن هناك مجالًا لتحسين مستوى سرية البيانات والمعلومات في الميدان المبحوث
3. إن بُعد نزاهة البيانات والمعلومات موجود في الميدان المبحوث، ولكنه لا يصل إلى المستوى المتوقع، مما يشير إلى أن هناك حاجة لتعزيز نزاهة البيانات والمعلومات في الميدان المبحوث للوصول إلى المستوى المطلوب.

4-2 التوصيات:

بناءً على الاستنتاجات حول الأبعاد المختلفة للأمن السيبراني في الميدان المبحوث، يمكن تقديم التوصيات التالية:

1. ينبغي تحسين الإجراءات الحالية لمراجعة وتدقيق البيانات لضمان صحتها ودقتها. يمكن تطوير نظام مركزي لمراجعة البيانات بشكل دوري والتحقق من نزاهتها.

2. يتوجب استخدام تقنيات متقدمة للتحقق من البيانات، مثل التشفير والتوقيع الرقمي، لضمان عدم التلاعب أو التغيير غير المصرح به.
3. السعي لزيادة حجم ونوعية المعلومات المقدمة للمستفيدين، إذ يمكن تحقيق ذلك من خلال تحسين نظم إدارة المعلومات وتطوير سياسات لتوسيع نطاق المعلومات المتاحة بما يتماشى مع الاحتياجات الفعلية للمستفيدين.
4. تحسين طرق توفير المعلومات لضمان سهولة الوصول إليها وتلبية احتياجات المستفيدين بشكل أفضل.
5. مراجعة وتحديث استراتيجيات حماية سرية البيانات والمعلومات، بما في ذلك تنفيذ سياسات تشفير قوية وتطوير نظم تحكم صارمة للوصول إلى البيانات الحساسة.
6. تنظيم دورات تدريبية منتظمة للموظفين لزيادة وعيهم بممارسات حماية سرية البيانات وتعليمهم كيفية التعامل مع المعلومات الحساسة بشكل آمن.
7. تحديث سياسات إدارة البيانات لضمان الالتزام بمعايير النزاهة المطلوبة، بما في ذلك تطبيق إجراءات تحقق ورقابة دورية على البيانات.
8. تعزيز ثقافة النزاهة داخل المنظمة من خلال نشر الوعي حول أهمية الحفاظ على نزاهة البيانات وتعزيز ممارسات الالتزام بأعلى معايير النزاهة.

المصادر

أولا: المصادر العربية

1. الحسناوي، حسين حريجة غالي، الفتلاوي علي عبد الحسين عباس، 2016، **التأثير الوسيط لنزاهة السلوكية للقائد في العلاقة ما بين روحانية مكان العمل والالتزام التنظيمي**، مجلة جامعة كربلاء العلمية المجد 14، العدد ا
2. البحيصي، عصام محمد، 2013، **واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها**، رسالة ماجستير، الجامعة الاسلامية بغزة.

3. ابو ذيب، قتيبة عاهد مسلم، 2019، **مدى الالتزام بسياسات امن وحماية المعلومات المحاسبية في البنوك التجارية الأردنية**، رسالة ماجستير، جامعة آل البيت.

4. ابو حجر، سامح، عابدين، أمينه محمد، 2014، **دور آليات الحوكمة تقانة المعلومات في تخفيض مخاطر امن المعلومات للحد من التلاعب المالي الالكتروني في الوحدات الحكومية في ظل نظام الحوكمة الالكترونية**، بحث مقدم في جامعه القاهرة.

ثانيا: المصادر الاجنبية

1. Aljohni,Wejdan., Mohamed, Nazar Elfadil., Jarajreh, Mutsam and Gasmelsied, Mwahib (2021) ***Cybersecurity Awareness Level: The Case of Saudi Arabia University Students***, International Journal of Advanced Computer Science and Applications 12(3)
2. Onumo, A ،O ،(2020) ،***A Behavioural Compliance Framework for Effective Cybersecurity Governance and Practice ،Examining the interaction of cultural characteristics and cybersecurity governance in fostering organisational compliance using case studies*** (Doctoral dissertation, University of Bradford).
3. Aksoy, Cenk, 2023, ***CRITICAL SUCCESS FACTORS FOR CYBERSECURITY JUST TECHNICAL? EXPLORING THE ROLE OF HUMAN FACTORS IN CYBERSECURITY MANAGEMENT***, Research Journal of Business and Management (RJBM), 10(2)
4. Butel, J. (2023). ***Impact of organizational security certification on operational security: Examining the red tape*** (Doctoral dissertation, Georgia State University).
5. Haaga, J ،(2021) ،***National cybersecurity Strategies: Review and Analysis of Evaluation Frameworks***

6. Steiger, S. (2022). ***Cyber securities and cyber security politics. Cyber Security Politics***, 141, 0224-12.

7. Creese, S., Dutton, W. H., & Esteve-González, P. (2021). ***The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions***. Personal and Ubiquitous Computing, 25(5), 941-955.

8. Atkins, Sean and Lawson, Chappell. 2021. "***An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure***." Public Administration Review, 81 (5).

9. Yeoh, W., Wang, S., Popovič, A., & Chowdhury, N. H. (2022). ***A Systematic Synthesis of Critical Success Factors for Cybersecurity***. Computers and Security, 118(July), 1-17

10. Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L ،M ،(2017) ،***rsecurity in ports: a conceptual approach ،In Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment*** ،Proceedings of the Hamburg International Conference of Logistics (HICL), Vol 23 ،

11. Choejey, P., Murray, D., & Fung, C. C. (2016, December). ***Exploring critical success factors for Cybersecurity in Bhutan's Government Organizations***. In Eighth International Conference on Networks & Communications (pp. 49-61).

12. Erhard, Werner, Michael C, Jensen, and Steve Zaffron, (2009), ***Integrity: A Positive Model that Incorporates the Normative Phenomena of Morality, Ethics and Legality*** (March 23, 2009), Harvard Business School NOM Working Paper No, 06-11, No, 06-03

13. Wisesa, Anggara, (2016), ***Cognitive Moral Development and Its Relevance in Establishing Moral Integrity in Organization***, Sains Humanika 8,1-2, PP 53-57

14. Yurkovich, P ،J ،(2022) ،***RSU-Based Intrusion Detection and Autonomous Intersection Response Systems*** (Doctoral dissertation, Virginia Tech).

15. Koumandaros, A. (2021). ***THE PREVENTION OF DATA INTEGRITY FAILURES IN PHARMACEUTICAL MANUFACTURING THROUGH RISK-BASED VALIDATION OF COMPUTERIZED SYSTEMS*** _ (Doctoral dissertation, California State University, Dominguez Hills).

16. LANE, Tim (2007), ***Information Security Management in Australian Universities – an Exploratory analysis***, degree of Master, Queen sland university of technology QUT.