Al-Saeeda Journal of Engineering, Technical and Administrative Sciences (SJETAS)
مجلة السعيدة للعلوم الهندسية والتقنية والإدارية
Available Online at: journal.su-edu.net/index.php/su-journal
A peer reviewed journal published by Research Center - Al-Saeeda University, Dhamar, Yemen
SJMS; Volume 1, Issue 1; August: 2023; Page No. 1-8

أمن المعلومات في المؤسسات المصرفية اليمنية

Information Security in Yemeni banking institutions

Ismail Ibrahim Ahmed [1]*, Mahmoud J.M. Hamoudah[2]
[1]Head of Information Technology department- Al-Saeeda University, Yemen Sana'a.
Mob. +967-777158255
E-mail: Ism116620@gmail.com
[2]Master Degree in Cyber Security. Yemen Sana'a
Mob. +967-734033311
E-mail : atair207@hotmail.com

Article Info:

Article Types:
Research article
Received
23 April 2022
Revised
28 May 2023
Accepted
25 June 2023
Corresponding Author:
Ismail Ibrahim Ahmed
Email: Ism116620@gmail.com
Telephone: +967-777158255
Conflict of interest: Nil

To cite this article:
Ismail I. Ahmed &, Mahmoud JM. Hamoudah, Information Security in Yemeni banking institutions. *SJETAS*. 2023; 1(1): 1-8.

الملخص Abstract

تشهد المؤسسات والمنظمات تطويرا مطردا لتطبيق مفاهيم أدوات الحماية والأمن لكافة البيانات والشبكات المعلوماتية وماهي الإجراءات والأدوات التي تتخذها القطاعات أو المنظمات لتأمين وحماية معلوماتها وأنظمتها ووسائطها من الوصول غير المصرح به، سواء من داخل القطاع أو من خارجه.

فجاء هذا البحث لتقييم الاستراتيجيات المستخدمة في المؤسسات المصرفية في الجمهورية اليمنية لما تحويه من إجراءات سرية وأمنية عالية يجب أخذها بعين الاعتبار حساسية البيانات باستخدام كافة الاساليب والخوارزميات والإجراءات والأدوات المتاحة في الشركات العالمية لتطبيق المفهوم الموحد لأمن وحماية البيانات من الفقدان والتسرب.

لقد تم احصاء البيانات الخاصة بالمؤسسات المصرفية وتصنيفها حسب أهميتها وحُددت المخاطر والتهديدات و احتمالية حدوثها وحجم كل خطر ومدى تأثيره كما حُددت الثغرات الأمنية والهجمات المحتملة وأسبابها.

كذلك تم دراسة وتحليل مصادر البيانات في الجهات المعنية وتعريفها وتقييم أهميتها باستخدام معايير أمنية معترف بها.

Abstract: Institutions and organizations have seen a development steadily to apply the concepts of security tools and security for all data and information networks and what are the procedures and tools taken by sectors or organizations to secure and protect their information and systems and its arguments from accessing unauthorized, both from within the industry or outside that. Then came this research to evaluate the strategies used in banking institutions and major academic, technical institutions, because they contain confidential and high security must be taken into account data sensitivity by using all of the methods and algorithms, procedures and tools available in international companies to implement unified concept of security and protection of data against loss and leakage. And they counted and classified data on institutions according to their importance and identified risks and threats and also identified the likelihood of occurrence and magnitude of each risk and its impact and identify security gaps and expected and their possible causes and attacks. The study and understand the data sources in the stakeholders and define and assess their importance using recognized security standards.

Keywords: أمن المعلومات Information-Security، الهجمات الأمنية Security-Attacks، الآليات الأمنية Security Mechanisms.

1. المقدمة Introduction

تعد البيانات لدى المؤسسات والشركات التجارية والمؤسسات الحكومية والعسكرية من أهم العناصر والمكونات لديها، وتم البحث فيها لضمان الحصول على مؤشرات حولها لتساعد في اكتشاف طرق الحماية وامن المعلومات فيها.
كما برزت أهمية تقييم استراتيجية تقنية الأمن المعلوماتي في المؤسسات المصرفية والمؤسسات التجارية في الآونة الأخيرة لكثرة الحوادث الأمنية. وبالنظر إلى دراسة مجموعة من جوانب الحوادث الأمنية للمعلومات والشبكات والبيانات ونوع وحجم الخسائر التي تعرضت لها ومن خلال دراسة مدى إدراك القائمين على أمن البيانات وتبرز أهمية التنقيب والبحث والتطوير لحماية البيانات من الفقدان والتسريب والتلف.
لقد طبق هذا البحث على مجموعة من المؤسسات المصرفية والتقنية في الجمهورية اليمنية باستخدام أساليب الاستبيان وأظهرت النتائج مواطن القوة ومواطن الضعف في استخدام استراتيجيات الأمن المعلوماتي لدى المؤسسات.

2. مشكلة البحث Research Problem

يمكن اختصار مشكلة البحث بانها الحاجة الى تحسين وتطوير الآليات المستخدمة في الامن المعلوماتي للمؤسسات المصرفية من خلال تقييمها و دراسة جوانب الحوادث الامنية، واقتراح الحلول المناسبة لتحاشي حدوث البيانات لهذه المؤسسات.

3. أهداف البحث Research Objectives

a. تقييم أداء الآليات الأمنية في المؤسسات المصرفية.
b. تحديد مواطن القوة لتطويرها، وتحديد مواطن الضعف لمعالجتها.
c. تطوير الآليات الأمنية لتصبح قادرة على مواجهة القرصنة والاختراقات الأمنية للمعلومات.
d. تقليل الخسائر الناجمة عن الهجمات الأمنية على المعلومات ونظمها في المؤسسات المصرفية.
e. زيادة الثقة لدى عملاء المؤسسات المصرفية بها.

4. تساؤلات البحث Research Queries

a. هل تستخدم المؤسسات المصرفية آليات لمواجهة الهجمات الأمنية؟
b. ما هو مستوى حماية المعلومات المستخدم في المؤسسات المصرفية؟
c. هل توجد اختراقات للمعلومات في المؤسسات المصرفية؟
d. ما هي الأنظمة المستخدمة لحماية المعلومات في المؤسسات المصرفية؟
e. هل يمكن البحث في تطوير الآليات الأمنية المستخدمة في المؤسسات المصرفية؟

5. فرضيات البحث Research Hypotheses

a. أنظمة حماية المعلومات في المؤسسات المصرفية غير آمن تماماً.
b. عدم وجود فروق ذات دلالة احصائية بين التدابير اللازمة لحماية المعلومات وبين التدابير المتخذة فعلياً في المؤسسات المصرفية، سواء كماً أو نوعاً.
c. عدم وجود معايير متبعة لحماية الشبكة المعلوماتية من قبل ادارة الشبكة.
d. اختراق معلومات المؤسسات المصرفية قابل للحدوث.
e. الآليات والأنظمة المستخدمة في المؤسسات المصرفية قابلة للتطوير.

6. أهمية البحث Research Importance

نظرا للأخطار المتزايدة التي تستهدف أمن البيانات وحمايتها واستخدام الأساليب المتعددة لاختراقها تبرز أهمية هذا البحث من خلال توفير الإرشادات والتعليمات اللازمة لتطوير إجراءات أمن وحماية البيانات وتتلخص فيما يلي: -

- اثراء المراجع المهمة للعاملين في مختلف القطاعات الأمنية عسكرية أو مدنية والعاملين في المجالات الصناعية والتجارية حكومية كانت أم أهلية في مجال تقنية البيانات بمختلف تخصصاتها كالشبكات وقواعد البيانات فيما يخص موضوع الحماية من زاوية الأمن والاحتياط للحفاظ على سلامة البيانات وتكاملها واعتماديتها والحفاظ على سرية البيانات الموجودة في موارد الشبكات أو المنتقلة لها والتقليل من إصابتها بالفيروسات والبرامج الضارة وتضييق احتمالات اختراق تجهيزاتها وبالتالي قرصنة مواردها وتجنب الوقوع في الأعطال والتوقف عن العمل وتكبد الخسائر الفادحة أو تعريض السمعة الوطنية والتجارية للضرر[4].
- يؤمن هذا البحث مصدرًا مهما للعاملين بمجال التحقيق في الجرائم المستحدثة حيث يستفاد منها في التعرف على عناصر بناء نظم حماية الشبكات وتفاصيل تثبيتها ومخرجات أجهزتها من تسجيلات حركة البيانات اليومية التي تساعد في جمع الأدلة الجنائية في حالات التحقيق والتحري في مجال الجرائم الإلكترونية[3].
- يوفر إرشادات لإعادة النظر في الهيكل التنظيمي المناسب للأعمال الفنية المطلوبة في إطار الهيكل التنظيمي للمنظمة. وكما يحاول التوصل إلى إجراءات مناسبة تتداخل فيها المهام الفنية والأعمال الإدارية في إطار الهيكل التنظيمي لأقسام وإدارات تقنية البيانات.

- يقدم للعاملين في الأجهزة الأمنية مرجعاً أمنياً مهماً للوقاية من الجرائم الالكترونية. [2]
- يقدم هذا البحث معلومات مفيدة للراغبين في تصميم الشبكات ومراكز البيانات آخذين في الاعتبار الاحتياطات الأمنية اللازمة لحماية شبكاتهم مختصرين الجهد والمال والوقت[8].
- يتميز بالجمع ما بين استخدام مفاهيم تقنية البيانات وإدارة الموارد البشرية ليعملا تكاملياً بتناوله موضوع الهيكل التنظيمي والموظفين والإجراءات والتوثيق.

7. الدراسات السابقة Previous Studies

1. العنزي، 2003: أجري هذا البحث حول جرائم نظم المعلومات وتوصلت البحث إلى أن حجم استخدام منفذ شبكة الانترنت وبرامج الاختراق الموجودة بها (4.25%) من مؤسسات عينة البحث كمنفذ خارجي أعلى من المنافذ الداخلية والخارجية الأخرى كإفشاء الرقم السري من قبل الموظفين (4.16%) من مؤسسات عينة البحث.
2. علي سامان توسون(2003 (Ali Saman Tosun ، وهي بعنوان"Mechanisms for Multimedia Networking "Security.
3. عمارة،2007 حيث قام شيخ فاروق عمارة بتقديم دراسة بعنوان " The Control of Firewalls using Active Networks" حول ضبط جدران الحماية باستخدام الشبكات النشطة وتتمحور حول مشكلة تغيير إعدادات أجهزة الشبكة (جدران الحماية والموجهات) المبنية على تصفية حزم البيانات بوضع برامج صغيرة مسبقة التعريف داخل تلك الأجهزة التي تمكِّن من تعديل أو إعادة توجيه حزم البيانات.
4. إدريس، 2007: قام كل من "نور بك باشا إدريس" رئيس شركة سكان الماليزية المتخصصة بأمن المعلومات و"بحراني دهران شانموجان"، بتقديم دراسة بعنوان "Hybrid Intelligent Intrusion Detection" حول نظام هجين للكشف الذكي عن التجسس على شبكات الحاسب، وقد طرح الباحثان مشكلة عدم كفاية نظام كشف التجسس.

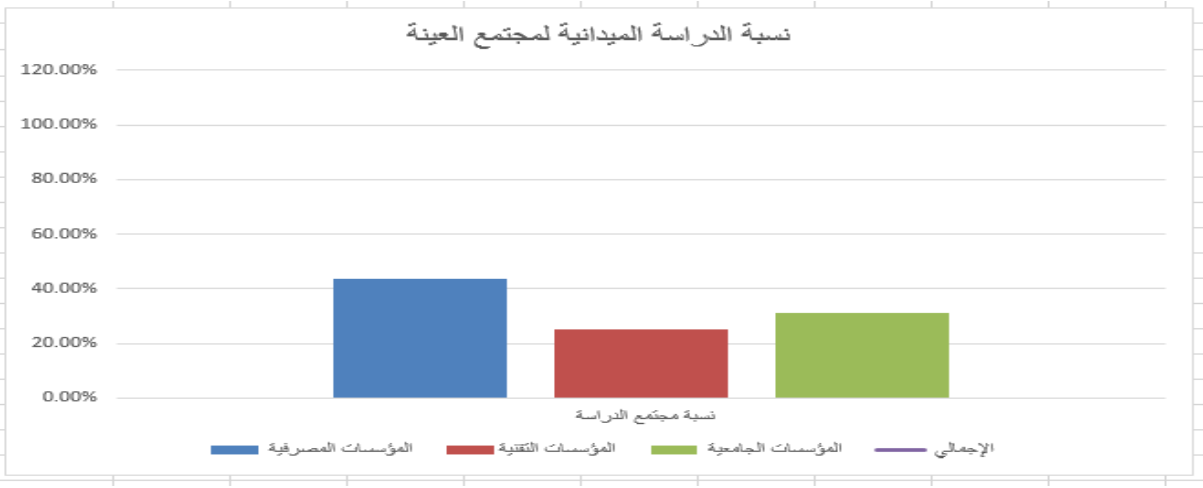
8. مجتمع وعينة الدراسة Society and Study Sample

طبقت أداة البحث على العينة التي تكونت من مجموعة من المؤسسات المصرفية والتقنية والجامعية وكما يوضح الجدول رقم (1) التي تعتمد على تقنيات الحاسب الآلي في تسيير معظم أعمالها المصرفية والإدارية والمالية وقد بلغ عدد تلك المؤسسات التي خضعت لتلك الدراسة 16 مؤسسة مصرفية وتقنية وجامعية أخذت كعينة عشوائية من أصل 17 مؤسسة مصرفية و8 مؤسسات تقنية و18 مؤسسة جامعية في مدينة صنعاء أي بأجمالي 43 مؤسسة ،أي ما نسبته 37.2% من مجتمع البحث وقد بلغ عدد أفراد العينة الذين خضعت استبياناتهم للتحليل 63 فرداً وقد تم الاكتفاء بهذه العينة نظراً لكبر مجتمع البحث وصعوبة الوصول إلى جميع أفراده في الحدود الزمنية للدراسة.

جدول رقم (1): نسبة الدراسة الميدانية لمجتمع العينة.

ذ	المؤسسة	العدد الكلي	عدد العينة	نسبة مجتمع الدراسة
1	المؤسسات المصرفية	17	7	43.75%
2	المؤسسات التقنية	8	4	25.00%
3	المؤسسات الجامعية	18	5	31.25%
	الإجمالي	43	16	100.00%

وكما يوضح الشكل رقم (1) يتبين ان نسبة المؤسسات المصرفية هي أكثر العينات التي تم الاعتماد عليها في مجمع الدراسة.



الشكل رقم (1): نسبة الدراسة الميدانية لمجتمع العينة

9. منهج الدراسة Study Methodology

اعتمد البحث على المنهج الوصفي الذي يناسب دراسة الظاهرة كما توجد في الواقع حيث وضعت تساؤلات تكونت من خمسة محاور وكل محور يحاكي واقع الحماية في المؤسسات المصرفية والجامعات والمؤسسات التقنية الكبرى والصغرى والواقع المعرفي للعاملين في مجال الحماية بتلك المؤسسات، ويتميز المنهج الوصفي بوصف الظاهرة وصفاً دقيقاً ويعبر عنها تعبيراً كمياً أو كيفياً بالإضافة إلى تصنيف المعلومات بطريقة تساهم في ربط العلاقات بين المتغيرات المراد قياسها من خلال البحث.

10. حدود البحث Research Limits

تهتم البحث بالحماية الأمنية للمعلومات وللشبكات الحاسب الآلي العائدة للمؤسسات المصرفية الحكومية والأهلية والجامعات والمؤسسات التقنية الكبرى والصغرى الموجودة في مدينة صنعاء بالجمهورية اليمنية. وفي الفترة من توزيع الاستبيان إلى وقت جمعها، وتبعاً لأهداف البحث والمجتمع الإحصائي المختار فقد وُضعت للبحث الحدود التالية:

- الحدود الموضوعية

ركّز البحث على موضوع محدد هو تقييم استراتيجيات الامن المعلوماتي في المؤسسات المصرفية والجامعات والمؤسسات الكبرى.

- الحدود البشرية

تمثلت الحدود البشرية للبحث على العاملين في مراكز أنظمة المعلومات وحمايتها من حيث الإعداد والتحديث والتطوير. بالإضافة لمدراء أقسام أو مراكز تقنية المعلومات، في المؤسسات المصرفية والجامعات والمؤسسات الكبرى.

- الحدود الزمنية

حُدد المجال الزمني بفترة تطبيق البحث المسحية وهي الأشهر الستة الأخيرة من عام 2016.

- الحدود المكانية

اقتصرت البحث على عينة عشوائية من المؤسسات المصرفية والجامعات والمؤسسات الكبرى الموجودة في مدينة صنعاء بالجمهورية اليمنية.

11. المعالجة الاحصائية Statistical Processing

بعد حساب معامل ارتباط بيرسون لقياس الصدق البنائي وكذلك تحديد معامل ثبات البحث باستخدام معامل كرونباخ ألفا وبعد ذلك تم استخدام المقاييس الإحصائية التالية:

a. التوزيعات التكرارية والنسب المئوية لوصف البيانات.
b. المتوسط الحسابي الموزون، لعبارات المحاور الأول والثالث والرابع ذلك أن لكل عبارة ثلاثة مقاييس، كما تم إيضاحها في الفقرة الخاصة بأداة البحث بحيث تقاس درجات المتوسط كما يلي:
   - المتوسط من (1) إلى أقل من (1.67) يشير إلى (غير موافـــــــق).
   - المتوسط من (2.33) إلى (3) يشير إلى (موافـــــــــــــــــــق).
c. المتوسط الحسابي الموزون، لعبارات المحورين الثاني والخامس ذلك أن لكل عبارة خمسة مقاييس، وهي من رقم (5) إلى رقم (1)، كما تم إيضاحها في الفقرة الخاصة بأداة البحث. هذا يحدد مدى ارتفاع أو انخفاض استجابات مجتمع الدراسة لكل عبارة واردة بهذين المحورين بحيث تقاس درجات المتوسط كما يلي:
   - المتوسط من (1) إلى (1.80) يشير إلى أن موضوع العبارة عديم الأهمية.
   - المتوسط من (1.81) إلى أقل من (2.60) يشير إلى أن موضوع العبارة قليل الأهمية.
   - المتوسط من (2.61) إلى (3.40) يشير إلى أن موضوع العبارة متوسط الأهمية.
   - المتوسط من (3.41) إلى (4.20) يشير إلى أن موضوع العبارة مهم.
   - المتوسط من (4.21) إلى (5) يشير إلى أن موضوع العبارة مهم جداً.
d. الانحراف المعياري لتحديد مقدار التشتت في إجابات مجتمع الدراسة لكل عبارة عن المتوسط والذي يوضح مدى تشتت إجابات مجتمع الدراسة كما يفيد في ترتيب المتوسطات عند تساوي بعضها.
e. معامل ارتباط بيرسون لتوضيح العلاقات بين متغيرات عناصر محاور البحث وذلك على النحو التالي:
   - الارتباط من + 1.00 إلى يشير إلى + 0.7 يشير إلى أن الارتباط عالي.
   - الارتباط أقل من+ 0.7 إلى + 0.4 يشير إلى أن الارتباط متوسط.

بعد حساب معامل ارتباط بيرسون لقياس الصدق البنائي وكذلك تحديد معامل ثبات البحث باستخدام معامل كرونباخ ألفا وبعد ذلك تم استخدام المقاييس الإحصائية التالية:

f. التوزيعات التكرارية والنسب المئوية لوصف البيانات.
g. المتوسط الحسابي الموزون، لعبارات المحاور الأول والثالث والرابع ذلك أن لكل عبارة ثلاثة مقاييس، كما تم إيضاحها في الفقرة الخاصة بأداة البحث بحيث تقاس درجات المتوسط كما يلي:
   - المتوسط من (1) إلى أقل من (1.67) يشير إلى (غير موافـــــــق).

المتوسط من (1.67) إلى أقل من (2.33) يشير إلى (موافق إلى حد ما).

- اختبار (ت) T-test للفرق بين متوسطين. واختبار LSD البُعدي للتعرف على مصادر الفروق الدالة إحصائياً وذلك بين المتغيرات التابعة والمتغيرات المستقلة.

12. نتائج البحث Research Results

نستعرض فيما يلي أهم نتائج البحث الممثلة في تحديد مواطن القوة ومواطن الضعف في استراتيجيات تقنية الأمن المعلوماتي للوصول إلى إجراءات عمل مناسبة لتطوير وتحديد حماية البيانات وحصر وتحديد المخاطر التي تهددها.

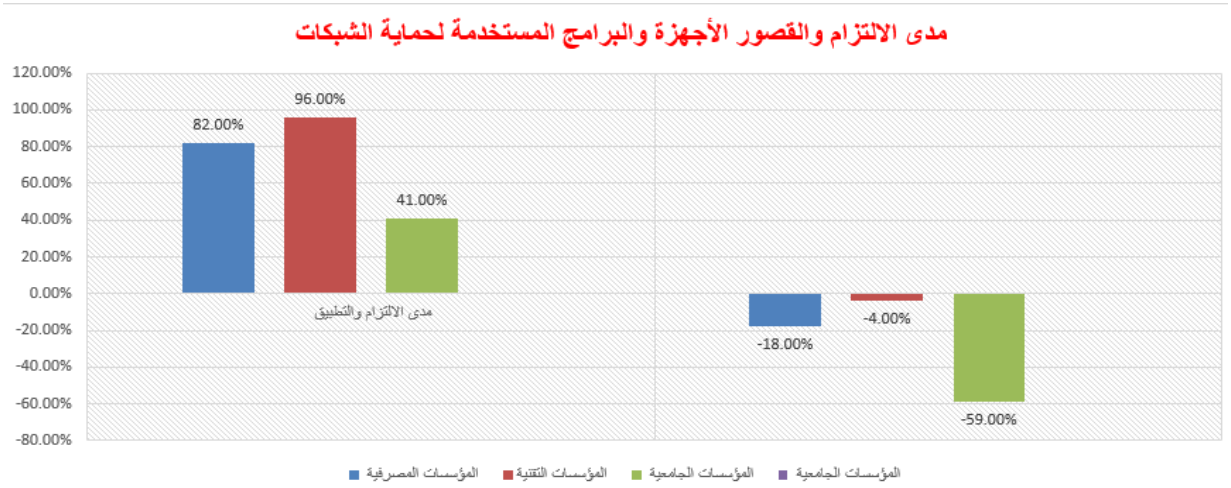
المحور الأول: الأجهزة والبرامج المستخدمة لحماية الشبكات ومدى استخدام تلك الأجهزة والبرامج ومدى إعدادها وتحديثها.

كما يوضح الجدول رقم (2) ان المؤسسات التقنية تحتل المرتبة الأولى في مدى تطبيق المحور الأول من حيث الأجهزة والبرامج المستخدمة لحماية الشبكات ومدى استخدام تلك الأجهزة والبرامج ومدى إعدادها وتحديثها وتأتي بعدها المؤسسات المصرفية والذي يتضح ان المؤسسات الجامعية ذات نقاط الضعف العالية في تطبيق استراتيجيات الحوسبة في إدارة اعمالها.

جدول رقم (2): مدى الالتزام والقصور في الأجهزة والبرامج المستخدمة لحماية الشبكات ومدى استخدام تلك الأجهزة والبرامج ومدى إعدادها وتحديثها.

م	المؤسسة	نقاط الضعف	نقاط القوة	مدى الالتزام والتطبيق	مدى الضعف والصور
1	المؤسسات المصرفية	18.00	82.00	82.00%	-18.00%
2	المؤسسات التقنية	4.00	96.00	96.00%	-4.00%
3	المؤسسات الجامعية	59.00	41.00	41.00%	-59.00%
	الإجمالي	81.00	219.00		

كما نلاحظ من الشكل رقم (2) المنحنيات الزمنية للنقاط القوة والضعف للمحور الأول أن الارتباط أقل من 0.4 + يشير إلى أن الارتباط منخفض أو ضعيف.



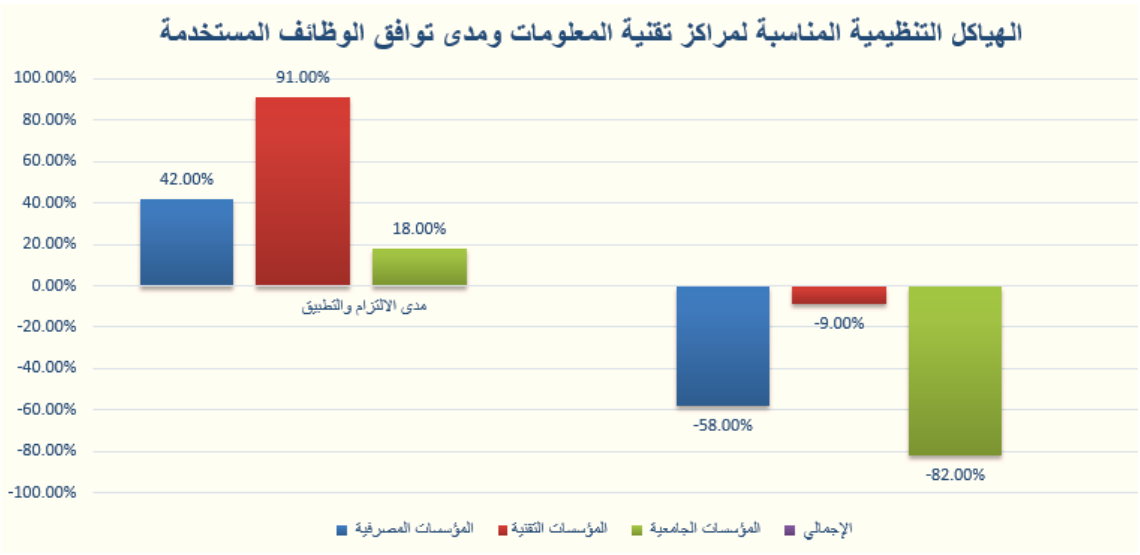
شكل رقم (2): المنحنيات الزمنية للنقاط القوة والضعف للمحور الأول.

المحور الثاني: يتضح أن المؤسسات التقنية كذلك تحتل المرتبة الأولى في مدى تطبيق المحور الثاني من حيث الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات ومدى توافق الوظائف المستخدمة في مجال أمن شبكات المعلومات معها كما يوضح ذلك الجدول رقم (3).

ويأتي بعدها المؤسسات المصرفية والذي يتضح أن المؤسسات الجامعية ذات نقاط الضعف العالية في تطبيق استراتيجيات الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات.

جدول رقم (3): مدى الالتزام والقصور الهياكل التنظيمية المناسبة لمراكز تقنية المعلومات.

المؤسسة	نقاط الضعف	نقاط القوة	مدى الالتزام والتطبيق	مدى الضعف والصور
المؤسسات المصرفية	58.00	42.00	42.00%	-58.00%
المؤسسات التقنية	9.00	91.00	91.00%	-9.00%
المؤسسات الجامعية	82.00	18.00	18.00%	-82.00%
الإجمالي	149.00	151.00		



الشكل رقم (3): يوضح المنحنيات الزمنية للنقاط القوة والضعف للمحور الثاني.

المحور الثالث **:**إجراءات العمل في حماية شبكات المعلومات ومدى تطبيقها والعمل بها.

وبالانتقال إلى المحور الثالث يتضح أن المؤسسات المصرفية تحتل المرتبة الأولى في مدى تطبيق المحور الثالث من حيث إجراءات العمل في حماية شبكات المعلومات ومدى تطبيقها والعمل بها وتأتي بعدها المؤسسات التقنية والذي يتضح ان المؤسسات الجامعية ذات نقاط الضعف العالية في تطبيق إجراءات العمل في حماية شبكات المعلومات ومدى تطبيقها والعمل بها كما يوضح الجدول رقم (4)جدول رقم (4): إجراءات العمل في حماية شبكات المعلومات ومدى تطبيقها والعمل بها**.**

المؤسسة	نقاط الضعف	نقاط القوة	مدى الالتزام والتطبيق	
المؤسسات المصرفية	13.00	87.00	87.00%	-13.00%
المؤسسات التقنية	59.00	41.00	41.00%	-59.00%
المؤسسات الجامعية	98.00	2.00	2.00%	-98.00%
الإجمالي	170.00	130.00		

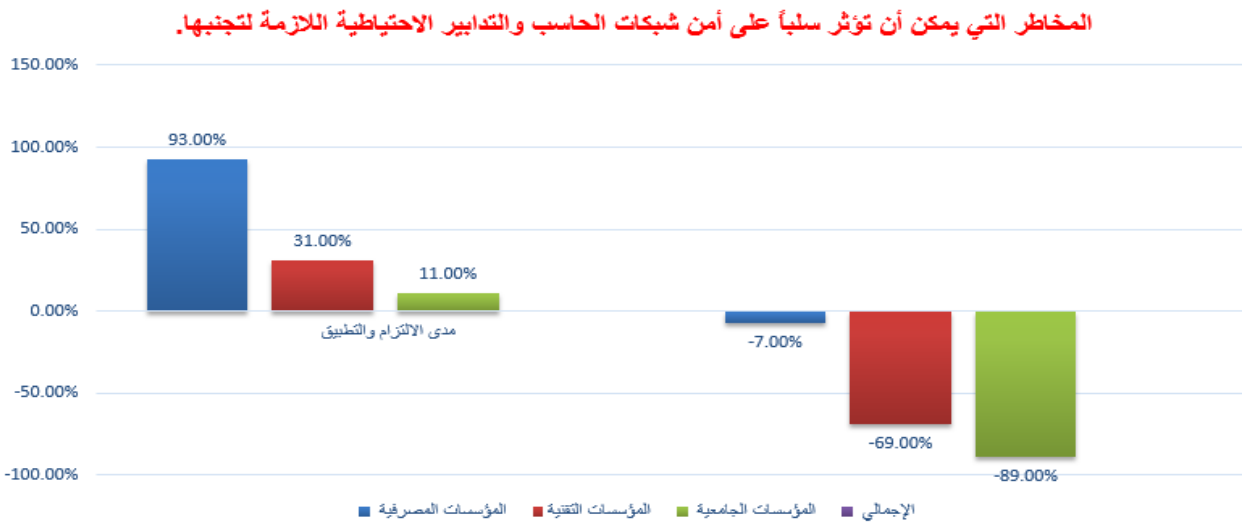
ويوضح الجدول رقم (4) المنحنيات الزمنية للنقاط القوة والضعف للمحور الثالث الجامعية ذات نقاط الضعف العالية في تطبيق استراتيجيات الحوسبة في إدارة أعمالها.

المحور الرابع: المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب والتدابير الاحتياطية اللازمة لتجنب تلك المخاطر .
وبالإشارة إلى المحور الرابع وكما يوضح الجدول رقم (5) أن المؤسسات المصرفية تحتل المرتبة الأولى في مدى تطبيق المحور الرابع من حيث المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب والتدابير الاحتياطية اللازمة لتجنبها ويأتي بعدها المؤسسات التقنية مما يتضح أن المؤسسات الجامعية ذات نقاط الضعف العالية والأخذ بعين الاعتبار التدابير الاحتياطية اللازمة لحماية الأمن.

جدول رقم (5) : المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب والتدابير الاحتياطية اللازمة لتجنبها.

المؤسسة	نقاط الضعف	نقاط القوة	مدى الالتزام والتطبيق	
المؤسسات المصرفية	7.00	93.00	93.00%	-7.00%
المؤسسات التقنية	69.00	31.00	31.00%	-69.00%
المؤسسات الجامعية	89.00	11.00	11.00%	-89.00%
الإجمالي	165.00	135.00		

كما يوضح الشكل رقم (5) المنحنيات الزمنية لنقاط القوة والضعف للمحور الرابع.



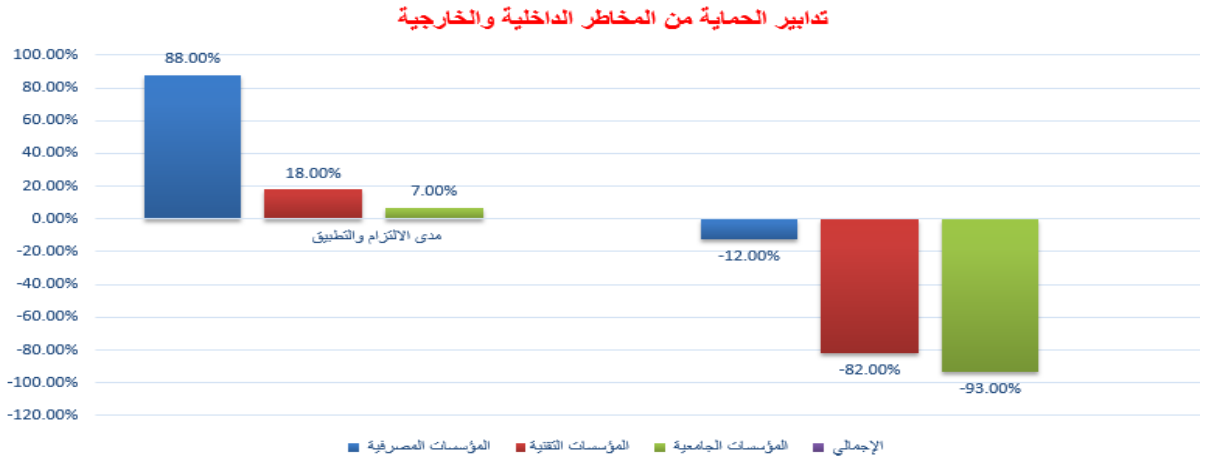
شكل رقم (5): يوضح المنحنيات الزمنية للنقاط القوة والضعف للمحور الرابع.

المحور الخامس والأخير : تدابير الحماية من المخاطر الداخلية والخارجية.

الجدول رقم (6) يبين أن المؤسسات المصرفية تحتل المرتبة الأولى في مدى تطبيق المحور الخامس من حيث تدابير الحماية من المخاطر الداخلية والخارجية ويأتي بعدها المؤسسات التقنية مما يتضح ان المؤسسات الاكاديمية تحتل المرتبة الأخيرة في تطبيق تدابير الحماية من تهديدات المخاطر.

جدول رقم (6): تدابير الحماية من المخاطر الداخلية والخارجية.

المؤسسة	نقاط الضعف	نقاط القوة	مدى الالتزام والتطبيق	
المؤسسات المصرفية	12.00	88.00	88.00%	-12.00%
المؤسسات التقنية	82.00	18.00	18.00%	-82.00%
المؤسسات الجامعية	93.00	7.00	7.00%	-93.00%
الإجمالي	187.00	113.00		



الشكل رقم (6): يوضح المنحنيات الزمنية للنقاط القوة والضعف للمحور الخامس.

13. الاستنتاجات Conclusion

يتضح من تقييم المحاور الخمسة السابقة وجود معدلات فرق إحصائية واضحة بين توفر الأجهزة والبرامج التي تستخدم في حماية الشبكات وبين تطبيق الإعدادات وتثبيت التحديثات لتلك الأجهزة والبرامج، وذلك لصالح توفر الأجهزة والبرامج ويدل ذلك على عدم اكتمال الإعداد والتحديث للأجهزة والبرامج التي توفرها المؤسسات وكما توجد معدلات فرق إحصائية واضحة بين درجة خطورة نقاط الضعف التي يمكن أن تُستغل لاختراق شبكات الحاسب وبين التدابير الوقائية المتخذة لتلافي نقاط الضعف، وذلك لصالح درجة خطورة نقاط الضعف ويدل ذلك على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي نقاط الضعف وأيضا يتضح انه توجد معدلات فرق إحصائية واضحة بين تلك المخاطر، وذلك لصالح المخاطر الداخلية والخارجية ويدل ذلك على

عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتجنب المخاطر الداخلية والمخاطر الخارجية.

14. التوصيات Recommendations

في ضوء نتائج البحث يقترح الباحث مجموعة من التوصيات التي تركز على أن الجهود التي ينبغي إكمالها لتحقيق حماية قصوى لا تكمن في المعدات أو البرمجيات فحسب وإنما تكمن في الجانب الإداري والموارد البشرية كذلك، ومن أهم تلك التوصيات:

1. توفير آليات تنفيذ سياسات العمل.
2. الاهتمام بالعنصر البشري بحيث يتولى إدارة وتشغيل شبكات البيانات عناصر بشرية مدربة ومؤهلة للتعامل مع هذه التكنولوجيا ولا يترك المجال للهواة للعبث بمثل هذه المقدرات الثمينة وخاصة في الأماكن الحكومية والحيوية على مستوى الدول.
3. تغيير الأوضاع الأصلية لمعدات الشبكات. وذلك بأن يتم كل فترة تغيير الأوضاع الأصلية للمعدات Hardware والبرامج Software الخاصة بشبكات البيانات كإجراء احترازي لمنع الاختراقات الخارجية.
4. توفير نوع من المراقبة والمتابعة لأنشطة البيانات على الشبكة بشكل دقيق ودائم وذلك بهدف اكتشاف أي أنشطة مشبوهة أو حركات غير طبيعية ضمن نطاق الشبكة.
5. استخدام بروتوكولات التحقق والتشفير.
6. توفير أخصائيين في أمن البيانات لإنشاء السياسات الأمنية ومراجعة تنفيذها.
7. تقدير أعمال الحماية بتقديم المكافآت و العلاوات و شهادات التقدير.
8. تدريب العاملين في الحماية وفق مسارات تدريبية تخصصية بشكل يكفي لتأدية أعمالهم على الوجه الأكمل.
9. يجب توفير وصف وظيفي للوظائف المتعلقة بالحماية والأمان.
10. تشكيل اللجان والمجالس المطلوبة لتسيير إجراءات العمل في مجال أمن البيانات.
11. العناية الخاصة بالموارد البشرية العاملة في مجال أمن وحماية الشبكات فهي القادرة على التغلب على صعوبات الحماية ومما يقلل من تلك الصعوبات.

15. المراجع References

[1]] فادي حجار، "تشريح الفيروسات"، حلب: شعاع للنشر والعلوم، 2003.

[2]عبد الحميد بسيوني، "الحروب الإلكترونية وقرصنة المعلومات"، القاهرة: دار الكتب العلمية للنشر والتوزيع، 2004م.

[3] عفاف شمدين، "الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات"، دمشق، بدون، 2003م.

4]] محمد أمين البشري، "المبادئ الأساسية لاختصاصي المكتبات والمعلومات"، الرياض، مكتبة الملك فهد الوطنية، 2000م.

[5] مدحت أبو النصر، "أمن المعلومات "، الرياض: مكتبة الملك فهد الوطنية، 2008م.

[6] Chris Brenton, "Cameron Hunt, Network Security", (Marian Village, Alameda: Sybex,2003).

[7] Cisco systems Inc., "Fundamentals of network security", Indiana: Cisco press, 2004.

[8] Cisco systems, Inc., "Indiana, Cisco press", Cisco networking academy program, first year companion guide 2nd ed., 2001.

[9] http://en.wikipedia.org/wiki/Host_computer, HCP: Dynamic Host Configuration Protocol.