واقع إدارة أمن المعلومات للإجراءات والسياسات الرقابية وسبل تطوير إدارة أمن نظم المعلومات في المراكز البحثية

أحمد دخيل[1] ، د. سعد طلحة[2]، د. حنان دوزان[3]

[1]المركز المتقدم للتقنية ، [2]هيئة البحث العلمي والتعليم التقني والفني، [3]المعهد العالي للعلوم والتقنية

dkhel@act1.ly

الملخص

يعتبر أمن المعلومات ضروري لحماية وتأمين الموارد المستخدمة, حيث أنه يعمل على سريتها وسلامتها ففي حالة غياب أمن المعلومات أو نقصه أو عدم الاستفادة منه, يؤدى ذلك إلى وجود ثغرات مثل الوصول أو الاستخدام الغير مصرح به, أو ربما الكشف والتعطيل والتعديل أو التخريب، ولهذا يعد أمن المعلومات من الركائز الضرورية في حماية الأفراد والمؤسسات من الأضرار الناتجة، لضمان أمن المعلومات هناك عدة طرق دقيقة وملائمة وموثوقة تستخدم لعدم إفشاء البيانات والمعلومات المخزنة التي تؤثر على سير أداء المراكز البحثية.

هدفت هذه الدراسة إلى تقييم واقع أمن المعلومات في المراكز البحثية التابعة للهيئة الليبية للبحث العلمي، من خلال التعرف على مدى توافر الاجراءات والسبل الرقابية لآمن المعلومات وكيفية تطوير ادارة امن المعلومات في هذه المراكز البحثية، حيث تم استخدام استبيان كوسيلة لجمع المعلومات ولاختبار فرضيات الدراسة، تم استخدام برنامج التحليل الإحصائي(Statistical Package for Social Science SPSS). للوصول إلى نتائج ومن تم التوصل إلى مجموعة من الاستنتاجات والتوصيات من أهمها تطوير سياسة أمن المعلومات بهذه المراكز وإتخاد كافة التدابير الضرورية لنشر ثقافة أمن المعلومات على مختلف المستويات الإدارية والفنية بالمراكز عن طريق إعداد برامج تدريبية وورش عمل توعوية.

الكلمات الافتتاحية: أمن نظم المعلومات، سياسة إدارة أمن المعلومات، برنامج الحزمة الإحصائية للعلوم الاجتماعية

Abstract

Information security is necessary to protect and secure the resources used, where works on its confidentiality and integrity, in the absence of information security, deficiency or non-utilization of it, this leads to the existence of loopholes such as unauthorized access or use for data. For this reason, information security is one of the necessary pillars in protecting individuals and institutions from the resulting damage. To ensure information security, there are several accurate, appropriate and reliable methods used not to disclose stored data and information that affect the functioning of research centers. This study aimed to assess the reality of information security in the research centers of the Research, Natural Sciences and Technology Authority. By identifying the availability of procedures and control methods for information security and how to develop information security management in these research centers. Where a questionnaire was used as a means to collect information and to test the study's hypotheses, by using SPSS (Statistical Package for Social Science), To reach results for developing the information security policy in these centers and to take all necessary measures to spread the culture of information security at the various administrative and technical levels in the centers.

1. المقدمة

تعد المعلومات في وقتنا الحاضر أحد أهم مقومات إدارة الأعمال في المؤسسات الحكومية والغير الحكومية، ومع إزدياد أهمية المعلومات والإيمان بأهميتها يزداد الاهتمام بكيفية الحفاظ عليها وحمايتها مما أدى إلى ظهور علم مختص يسمى علم أمن المعلومات Information Security، ولا يعد أمن المعلومات عملية تقنية يقوم بها المختصون فقط وإنما هو نتاج تعاون بين جميع العاملين بالمؤسسة, بحيث تتوزع الأدوار والمسؤوليات بما يخدم مصالح المؤسسة وبالتالي فإن أي خطة تضعها المؤسسة بخصوص أمن المعلومات لابد من احتواؤها على عناصر وبنود شاملة لكل العمليات والسياسات المتعلقة بالنواحي التقنية والبشرية.

في العادة يجب **أن** تشتمل خطة أمن المعلومات في الشركات والمؤسسات أو المراكز البحثية على كل الأوجه الحساسة للمعلومات بحيث تضمن سرية وسلامة بياناتها وتوافرها، والتي تعرف بأنها نهج أمني مستمر ومنظم لإدارة حماية معلومات المؤسسة من التعرض للخطر من قبل الأطراف غير المسئولة ولضمان بقاء المعلومات آآمنة [1] ، وذلك بتوعية العاملين بها بالمخاطر والهجمات الممكنة ومسئولياتهم في حفظ المعلومات، كما يجدر التنويه على أن أمن المعلومات يمثل مجموعة من المقاييس المختلفة على كافة المستويات الطبيعية المتعلقة بالأفراد أو المقاييس الإدارية لمستويات نظام المعلومات، وعند وجود أي قصور في أحد المستويات يمكن أن يهدد كل المستويات الأخرى, عليه قامت مجموعة من الهيئات الحكومية وغير الحكومية بإيجاد معايير خاصة بأمن المعلومات للتأكد من وجود مستوى معين من الحماية للمعلومات لكي تضمن أن الموارد الحاسوبية للمؤسسة تستخدم بأسلوب صحيح, ولتبني أفضل الممارسات في أمن المعلومات. ولضمان برنامج ناجح لأمن المعلومات في المؤسسات لابد من إجراء عملية إدارة المخاطر بفاعلية، وأن تكون وظيفية من وظائف الإدارة في المؤسسة[2].

فاليوم باتت الحلول الإدارية وسيلة ناجحة للحماية وتعزيز أمن المعلومات لما يمكن أن تتضمنه من منافع والحد من التكاليف للحلول الفنية والبرمجية.

2. أسباب الدراسة

يتمحور سبب الدراسة في عدم إعطاء الأهمية اللازمة من قبل أغلب المراكز البحثية لاستخدام وتطبيق سياسات أمن المعلومات لحماية مواردها المادية والمعنوية، وحيث انه لا يمكن تحقيق حماية نظام المعلومات إلا من خلال إدارة فعالة لأمن المعلومات وتنفيذ خطة أمنية كاملة عليه يمكن طرح التساؤلات الأتية:

- هل يوجد إدارة لأمن المعلومات بالمراكز البحثية؟
- هل تتأثر هذه المراكز البحثية بوجود أمن المعلومات أو غيابه؟
- ما هي سبل تطوير إدارة أمن المعلومات في المراكز البحثية؟

3. أهمية الدراسة

تنحصر الدراسة على أهمية إدارة أمن وسرية المعلومات وما مدى تأثيرها على أداء هذه المراكز البحثية، كما أنها ستعطي للمراكز البحثية أهمية كبيرة باعتبار بياناتها ومعلوماتها الرقمية متصلة بالعالم الخارجي وذات أهمية حيوية وفعالة في بلادنا.

4. أهداف الدراسة

1- تسليط الضوء على الإجراءات اللازمة لأمن وسرية المعلومات وكيفية الاستفادة منها في المراكز البحثية.

2- حماية وتوفير أمن وسرية لشبكة المعلومات في المراكز البحثية من أي اعتداء أو تطفل أو عبث وكذلك من الحوادث والكوارث الطبيعية.

3- معرفة تأثير أمن وسرية المعلومات على أداء المركز البحثية.
4- نشر الوعي وثقافة أمن المعلومات للعاملين بهذه المراكز.
5- تقديم مقترح لتحسين نظام إدارة أمن المعلومات في المراكز البحثية.

5. منهجية الدراسة

سيتم استخدام أسلوب المنهج الوصفي للإجابة على التساؤلات وإثبات فرضيات الدراسة من خلال :

- المقابلات الشخصية : وذلك بإجراء مقابلات شخصية مع مدراء الإدارات والعاملين بأقسام تقنية المعلومات.
- استمارة الاستبيان : إستخدمت الاستمارة كأداة لجمع البيانات الرئيسية من جميع العاملين بأقسام نظم المعلومات في المراكز البحثية.

6. فرضيات الدراسة

الدلالة الإحصائية هي وصف لنتائج تجارب أجريت على القيمة الاحتمالية (p-value) أقل من مستوى الدلالة، وعند القيام بدراسة علمية فإنه غالبا ما يتم اختبار مستوى الدلالة قبل جمع البيانات وغالبا ما يكون هذا المستوى 0.05، وإسنادا لما سبق وضعت الفرضية الرئيسية الاتية :

- عدم توفر سياسة لأمن المعلومات يؤثر على إدارة أمن ونظم المعلومات في المراكز البحثية بصورة إيجابية عند مستوى الدلالة الإحصائية.
- هل توجد فروق ذات دلالة إحصائية في نتائج عينة الدراسة عند مستوى الدلالة الإحصائية حول واقع إدارة نظم المعلومات في المراكز البحثية؟

7. الدراسة النظرية

يتناول الجانب النظري من الدراسة التعرف على مفهوم وسياسة أمن المعلومات :

7.1 . مفهوم أمن المعلومات

يعرف أمن المعلومات بأنه السياسات والإجراءات والمقاييس التي تتخذها المؤسسات أو المنظمات لتأمين وحماية معلوماتها وأنظمتها من وصول الأفراد الغير مصرح لهم سواء من هم داخل المؤسسة ومن خارجها، وتعتبر هذه العمليات مستمرة وتتطلب استمرارية في التطوير ومتابعة للمستجدات وكذلك مراقبة وافتراض المخاطر وإبتكار الحلول لها[3].

بناءاً على ما سبق فإن المنظمات لا توصف بأن لها نظام معلوماتي أمني حقيقي وفعال حتى يحقق نظام تطوير مستمر للعمليات الأمنية والبشرية والتقنية من أجل تقليل واحتواء المخاطر المفترضة أو المتوقعة.

7.2 . مكونات أمن المعلومات

- السرية: وتعني الحفاظ على سرية المعلومات والمعاملات والإجراءات التي تضمن التأكد من حماية الموارد من الأفراد الغير مخولين بذلك.
- سلامة المحتوى: التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به.
- استمرارية توفر المعلومات: التأكد من استمرار عمل النظام ألمعلوماتي واستمرار القدرة على التفاعل مع المعلومات والمستخدمين لتقديم الخدمة لمواقع المعلوماتية وضمان أن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو الدخول إليها.

- عدم الإنكار: يقصد به ضمان عدم إنكار المستخدم الذي قام بتصرف ما، بحيث تتوفر قدرة الإثبات أن التصرف حدث من مستخدم معين في وقت محدد[4].

7.3 . أسباب حدوث المخاطر

من المهم أن نذكر أن أنظمة المعلومات الالكترونية تتضمن كما هائلاً من البيانات ولذلك فانه يصعب عمل نسخ ورقيه لها, بالإضافة إلى صعوبة اكتشاف الأخطاء الناتجة عن التغير في نظام المعلومات وذلك لأنه لا يمكن التعامل أو قراءة سجلاتها إلا بواسطة الحاسب، هذه الأنظمة قد تتعرض للعديد من المخاطر والتهديد بسبب مجموعة من العوامل منها:

- إحتمال تعرض النظم الآلية إلى حدوث أخطاء أو إساءة عند استخدام النظام أو أثناء تشغيل البيانات أو ربما إساءة استخدامها بواسطة الخبراء غير المنتمين للمؤسسة في حال استدعائهم لتطوير النظم.
- قد تؤذي المخاطر التي تتعرض لها المعلومات إلى تدمير كافة سجلات المؤسسة وبذلك فهي أشد خطورة على النظم الآلية من النظم اليدوية.
- ضعف الرقابة على النظام الآلي بسبب الاتصال المباشر للمستخدم بنظم المعلومات.
- التطور التكنولوجي في الاتصال عن بعد سهل عملية الاتصال بنظم المعلومات من أي مكان في العالم، الأمر الذي قد يسبب إمكانية الوصول الغير المسموح به أو الإساءة لاستخدام نظام المعلومات من قبل العابثين.
- استخدام العديد من التطبيقات من عدة مواقع مختلفة في نفس قاعدة البيانات يؤذي إلى إمكانية اختراقها بفيروسات الحاسب وبالتالي إمكانية تدمير أو تغيير قاعدة البيانات لنظام المعلومات.

7.4 . أنواع المخاطر

أشار الباحثان (Baskerville & Siponen) أن هناك العديد من المخاطر التي من الممكن أن تواجه أنظمة المعلومات، أبرزها[5]:

1. **اختراق الأنظمة:** ويتحقق ذلك بدخول شخص غير مخول بذلك إلى نظام الحاسوب والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير الملفات أو البرمجيات أو النظام ويتم الاختراق بشكل تقليدي من خلال أنشطة التخفي أو من خلال استغلال نقاط الضعف في النظام كتجاوز إجراءات السيطرة والحماية أو من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مادية أو معنوية للحصول على كلمات السر أو معلومات عن النظام أو عن طريق الهندسة الاجتماعية أو المكالمات الهاتفية.
2. **الاعتداء على حق التخويل:** يتم ذلك من خلال قيام الشخص المخول له باستخدام النظام في أغراض دون أن يحصل على تخويل بذلك، وهذا الخطر يعد من الأخطار الداخلية في حقل إساءة استخدام النظام من قبل موظفي المؤسسة وقد يكون أيضاً من الأخطار الخارجية كاستخدام المخترق حساب الشخص المخول باستخدام النظام عن طريق تخمين كلمة السر الخاصة به أو باستغلال نقطة ضعف النظام للدخول إليه بطريق مشروع ومن ثم القيام بأنشطة غير مشروعة.
3. **زراعة نقاط الضعف:** ينتج هذا الخطر من قبل مستخدم غير مخول له بالدخول إلى النظام أو من خلال مستخدم مخول له بالدخول لكنه تجاوز حدود التخويل الممنوح له بحيث يقوم المستخدم بزرع مدخل ما يحقق له الاختراق فيما بعد ومن أشهر زراعة المخاطر (حصان طروادة) وهو عبارة عن برنامج يؤذي غرضاً مشروعاً في الظاهر لكنه يمكن أن يستخدم في الخفاء للقيام بنشاط غير مشروع.

4. **مراقبة الاتصالات:** وهو أن يتمكن المخترق من الحصول على معلومات سرية غالباً ما تكون من المعلومات التي تسهل له من اختراق النظام لاحقا وذلك ببساطة من خلال مراقبة الاتصالات من إحدى نقاط الاتصال أو حلقاتها.

5. **إعتراض الاتصالات:** وهو عبارة عن اعتراض المعلومات خلال عملية الإرسال بدون اختراق النظام وعادة ما تجرى عليها التعديلات التي تتناسب مع غرض الاعتداء ويشمل اعتراض الاتصالات القيام بخلق نظام وسيط وهمي يجبر المستخدم على المرور من خلاله وتزويده بمعلومات حساسة بشكل طوعي.

6. **إنكار وحجب الخدمة:** ويتم ذلك من خلال القيام بأنشطة تمنع المستخدم من سرعة الوصول إلى المعلومات أو الحصول على الخدمة، وابرز طرق إنكار الخدمة إرسال كمية كبيرة من رسائل البريد الالكتروني دفعة واحدة إلى موقع معين بهدف إرهاق النظام لعدم قدرته على احتمالها أو توجيه عدد كبير من عناوين الانترنت على نحو لا يتيح عملية تجزئة حزم البيانات المرسلة الأمر الذي يؤذي إلى اكتظاظ الخادم وعدم قدرته على التعامل مع تلك البيانات.

7. **عدم الإقرار بالقيام بالتصرف** : يتمثل هذا الخطر في عدم إقرار الشخص المرسل أو المرسل إليه بالتصرف الذي صدر عنه، كأن ينكر أنه ليس هو شخصيا الذي قام بإرسال طلب الشراء عبر الانترنت.

8. **مكونات نظام أمن المعلومات**

- العمليات : تعتبر العمليات مهمة وجوهرية لأي نظام فهي عبارة عن مجموعة من المعايير الدولية ذات طبيعة مستمرة للحماية من الأخطاء والمخاطر[6].
- الموظفين : جميع العاملين في مجال تقنية المعلومات والاتصالات ذات الخبرات والمهارات المناسبة, يقومون بإنجاز كل العمليات والخدمات.
- التكنولوجيا : هي جميع الأجهزة الحديثة التي تساعد على توفير وحفظ أمن المعلومات في المؤسسات والجهات العامة ويجب تحديثها حسب المتطلبات.
- الثقافة : ترتبط بطبيعة ثقافة العاملين في المؤسسات والجهات العامة والخاصة ويجب العمل على رفعها باستمرار.

9. **متطلبات حماية أمن المعلومات**

يذكر كل من (تارة، وزبيبي، 2006) بأن مسألة أمن نظم المعلومات من المسائل المهمة والضرورية التي ينبغي على المؤسسة أخذها بعين الاعتبار ووضع خطة حماية شاملة في حدود إمكانياتها التنظيمية والمادية ولذلك فإنه توجد عدة متطلبات لحماية أمن نظم المعلومات[7] تتمثل في:

- وضع سياسة حماية عامة لأمن نظم المعلومات حسب طبيعة عمل وتطبيقات المؤسسة.
- يجب على الإدارة العليا في المؤسسة دعم أمن نظم المعلومات لديها.
- يجب أن توكل مسؤولية أمن نظم المعلومات في المؤسسة لأشخاص محددين .
- تحديد آليات المراقبة والتفتيش لنظم المعلومات وشبكات الحاسوب.
- الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل أمن.
- تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط .
- تأمين استمرارية عمل نظم المعلومات خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات .

10. وسائل حماية أمن المعلومات

أهم وسائل أمن المعلومات تتمثل في:

- الاكتشاف المبكر : يتم ذلك عن طريق ملف تسجيل النظام، الأوامر ونظام التشغيل، مدير المهام الذي يعرض جميع البرامج ويتم التعرف على البرنامج الدخيلة من بينها.
- حماية الشبكة: يتم حماية الشبكة داخليا باتخاذ مجموعة من الإجراءات منها تدريب العاملين في الشبكة على التعامل مع الإجراءات الأمنية المتخذة في المؤسسة.
- التشفير المحكم : لضمان عدم الاستفادة من المعلومات ومعرفة فحواها حتى وان تم الحصول عليها.
- الجدار الناري : هو مجموعة من البرامج والأجهزة تعمل على تصفية البيانات الداخلة إلى قواعد البيانات قبل وصولها للخادم وبذلك يقوم الجدار الناري بحجز ما يصل من الشبكة الخارجية ولا يرغب به في الشبكة الداخلية.
- مضادات الفيروسات : وهي مجموعة من البرامج التي تتصدى للفيروسات الداخلة إلى الجهاز، وتتفاوت مضادات الفيروسات من القوة والفاعلية إلا أنه يمكن لصناع الفيروسات وناشريها تجاوز مفعولها في كثير من الأحيان.
- تعدد الخوادم : يقصد بتعدد الخوادم استخدام خادم لكل نظام أو لكل مجموعة أنظمة تربطها علاقة وظيفية مثل المراسلات الإدارية، اللوائح والقوانين، الأبحاث والمشاريع العلمية، حيث تتواجد جميع هذه الأنظمة في خادم واحد يزيد من احتمال اختراقها وتوزيع جميع الأنظمة وتعددها يؤذي إلى انحصار المشكلة في خادم واحد[8].

11. الدراسات السابقة

ظهرت العديد من الدراسات السابقة التي تناولت موضوع أمن المعلومات ومن بينها:

11.1. الدراسات العربية:

1. دراسة (رؤى يونس، 2017) بعنوان "واقع إدارة أمن المعلومات في المؤسسات السورية"، توصلت الدراسة إلى ضرورة بناء سياسات أمن نظم المعلومات والعمل على نشرها واستخدام الحوافز المادية والمعنوية لتشجيع المبدعين في مجال أمن المعلومات والحرص على استخدام البرمجيات الاصلية، كما أوصت الدراسة إلى الاعتناء بتدريب العاملين وزيادة الموازنات المالية لضمان أمن المعلومات والاهتمام بالبنية التحتية[9].
2. دراسة (رضا ابراهيم، 2020) بعنوان "أثر ادارة امن المعلومات على نجاح برنامج نظم المعلومات"، هدفت هذه الدراسة إلى الحد من المخاطر التي تتعرض لها نظم المعلومات من خلال المعايير الدولية، وتوصلت الدراسة إلى وجود العديد من المخاطر التي تتعرض لها نظم المعلومات وذلك لعدم وجود سياسات وبرامج لأمن المعلومات داخل المؤسسات والمنظمات)[10].
3. دراسة (عرفان وآخرون، 2010) بعنوان "دراسة عملية حول أمن المعلومات في المنظمات السعودية"، هدفت هذه الدراسة إلى تحقيق فهم أكثر حول أمن المعلومات داخل المؤسسات السعودية، وتوصلت الدراسة إلى أهمية تطبيق سياسة أمن المعلومات في المؤسسات العاملة، بالإضافة إلى أن هناك العديد من الحلول التي تمكن المؤسسات من الحفاظ على سرية المعلومات، وإرساء الوعي الأمني بين العاملين داخل المؤسسات من خلال التدريب[11].

11.2. الدراسات الأجنبية :

1. دراسة (Zammani, M and Razali, R, 2016) بعنوان "دراسة تجريبية لعوامل نجاح إدارة أمن المعلومات"، هدفت هذه الدراسة إلى تخفيف التهديدات الأمنية ونقاط الضعف التي تعصف بالعديد من المؤسسات من خلال

وضع مجموعة من العوامل الرئيسية لإدارة أمن المعلومات، توصلت هذه الدراسة إلى مجموعة من النتائج أهمها عدم وجود سياسات وبرامج لأمن المعلومات داخل المؤسسات[12].

2. دراسة (MWITA SIMION MAROA, 2015) بعنوان "العوامل المؤثرة على فاعلية أمن المعلومات في جامعة نيروبي"، عالجت هذه الدراسة العوامل المؤثرة على أمن نظم المعلومات توصلت هذه الدراسة إلى مجموعة من النتائج أهمها دعم الإدارة العليا والسياسات الأمنية لنظم المعلومات، وتدريب المستخدمين وزيادة الوعي[13].

3. دراسة (Huang, et .. al, 2010) بعنوان "العوامل التي تؤثر في مستوى إدراك العاملين لأمن المعلومات "، توصلت الدراسة إلى وجود ستة عوامل رئيسية اعتبرتها تشكل تهديدا من وجهة نظرهم وهي (المعرفة، التأثير، الشدة، التحكم، الإمكانية وأخيراً التوعية)، وإن أهم التهديدات تتمثل في اختراق أجهزة الحاسوب، والديدان، والفيروسات، وأحصنة طروادة وبرامج الباب الخلفي[14].

11.3. التعقيب على الدراسات السابقة

يظهر من الدراسات السابقة تعدد الآراء ووجهات النظر حول أمن المعلومات, لقد ساعدت الدراسات السابقة في إعطاء نظرة عن الجانب النظري لأمن المعلومات، خاصة في تحديد الإشكالية والتساؤلات المطروحة ثم الاستفادة من بياناتها ونتائجها وطريقة تحليلها وأسلوبها العلمي لكي يتم توظيفها حسبما يتناسب مع موضوع الدراسة.

أما في ما يميز الدراسة الحالية عن الدراسات السابقة هي أن الدراسات السابقة أجريت في بيئات مختلفة، في حين تم تطبيق الدراسة الحالية في المراكز البحثية الليبية.

12. مجتمع وعينة الدراسة

اقتصرت هذه الدراسة على الأفراد العاملين ضمن نظم المعلومات في المراكز البحثية، وقد بلغ حجم العينة 70 وتم توزيع الاستبيان على جميع أفراد العينة، حيث تم استرداد 62 استبان، وبعد مراجعة الاستبيانات تم استبعاد 6 منها نظرا لعدم تحقق الشروط المطلوبة للإجابة، وكانت الاستبيانات المستوفاة الشروط 56 استبان، والجدول (1) يوضح مجتمع الدراسة وحجم العينة لكل مركز بحثي.

جدول (1) مجتمع الدراسة وحجم العينة لكل مركز بحثي .

اسم المركز	الموزع	المسترجع	الفاقد	نسبة الاستجابة
المركز المتقدم للتقنية	10	10	0	%100
مركز تقنيات اللحام	10	7	3	%70
مركز اللدائن	10	6	4	%60
مركز البحوث الصناعية	10	9	1	%90
مركز التدريب والإنتاج	10	8	2	%80
مركز المنظومات الالكترونية والبرمجيات	10	10	0	%100
مركز الاستشعار عن بعد	10	6	4	%60

12.1- استبان الدراسة :

يتناول واقع أمن نظم المعلومات في المراكز البحثية وينقسم إلى محورين:

1. **المحور الاول** : الإجراءات والسياسات الرقابية.
2. **المحور الثاني** : سبل تطوير إدارة أمن نظم المعلومات في المراكز البحثية.

13. تحليل ومناقشة نتائج الدراسة

13.1 . المعالجات الإحصائية

لتحقيق أهداف الدراسة وتحليل البيانات التي تم تجميعها، فقد تم استخدام العديد من الأساليب الإحصائية المناسبة باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعية في تحليل البيانات لغرض الوصول إلى دلالات ذات قيم ومؤشرات تدعم موضوع الدراسة:

1- حساب مقياس ليكرث الخماسي (حيث كانت الدرجة "5" تعنى موافق بشدة والدرجة "1" تعنى غير موافق بشدة) ولتحديد طول فترة مقياس ليكرث الخماسي (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم حساب المدى (5-1=4)، ثم تقسيمه على عدد فقرات المقياس الخمسة للحصول على طول الفقرة، بعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس وهى (الواحد الصحيح) وذلك لتحديد الحد الأعلى للفترة الأولى كما هو موضح بالجدول رقم (2).

جدول (2) يبين أطوال الفقرات

الفترة	1.80-1	2.60-1.80	3.40-2.60	4.20-3.40	5.0-4.20
التصنيف	غير موافق تماما	غير موافق	محايد	موافق	موافق تماما
الدرجة	1	2	3	4	5

2- تخدام طريقة ألفا كرونباخ لقياس ثبات الاستبانة لجميع محاور الدراسة.

3- ختبار كولمجروف Kolmogorov-Smirnov Test لاختبار ما كانت البيانات تتبع التوزيع الطبيعي أو لا.

4- حساب المتوسط الحسابي Mean والوزن النسبي لمعرفة ارتفاع أو انخفاض استجابات أفراد الدراسة عن كل فقرة من فقرات الاستبيان.

5- ختبار t.test لمتوسط العينة الواحدة ولمعرفة الفرق بين متوسط الفقرة والمتوسط الحيادي.

13.2 . ثبات الاستبيان

معامل الثبات يأخذ قيما تتراوح ما بين الصفر والواحد الصحيح، فإن لم يكن هناك ثبات في البيانات فإن المعامل يكون مساويا للصفر وإن كان هناك ثبات تكون قيمة المعامل الواحد الصحيح وكلما اقتربت قيمة البيانات من الواحد الصحيح كان الثبات مرتفعا وكلما اقتربت البيانات من الصفر كان الثبات منخفضاً وقد تم استخدام طريقة ألفا كرونباخ لقياس ثبات الاستبانة لجميع محاور الدراسة، ومن الجدول رقم (3) يتضح أن معامل الاستبانة لكل المحاور أكبر من 78% وهى نسبة مرتفعة، مما يدل على درجة عالية من ثبات الاستبانة التي يمكن الاعتماد عليه في الدراسة.

جدول (3) يبين ثبات الاستبانة بطريقة ألفا كرونباخ

رقم	عنوان المحور	عدد الفقرات	معامل الفا كرونباخ
1	الإجراءات والسياسات الرقابية	15	0.918
2	سبل تطوير إدارة أمن نظم المعلومات في المراكز	7	0.789
	جميع الفقرات	22	0.826

13.3 . اختبار التوزيع الطبيعي

تم استخدام اختبار كولمجروف Kolmogorov-Smirnov Test لاختبار ما كانت البيانات تتبع التوزيع الطبيعي من عدمه، ويوضح الجدول رقم (4) نتائج الاختبار حيث كانت القيمة الاحتمالية لكل محور أكبر من 0.05 وهذا يدل على ان البيانات تتبع التوزيع الطبيعي.

جدول (4) يبين اختبار التوزيع الطبيعي بطريقة كولمجروف

رقم	عنوان المحور	عدد	قيمة Z	القيمة
1	الإجراءات والسياسات الرقابية	15	0.926	0.358
2	سبل تطوير إدارة أمن نظم المعلومات	7	0.855	0.344
	جميع الفقرات	22	0.892	0.351

13.4 . تحليل فقرات ومحاور الدراسة

تساؤلات الدراسة : ما هو واقع إدارة أمن المعلومات في المراكز البحثية ؟ وما هي طرق تطويرها ؟

تم استخدام اختبار t.test للعينة الواحدة لتحليل فقرات الاستبانة، حيث تكون الفقرة إيجابية في حالة أفراد العينة يوافقون على محتواها إذا كانت قيمة t المحسوبة أكبر من t الجدولية والتي تساوى 1.98 (أو القيمة الاحتمالية أقل من 0.05 والمتوسط الحسابي النسبي أكبر من 60%)، وتكون الفقرة سلبية في حالة أفراد العينة لا يوافقون على محتواها إذا كانت قيمة t المحسوبة أصغر من t الجدولية والتي تساوى 1.98- (أو القيمة الاحتمالية أقل من 0.05 والمتوسط الحسابي النسبي أقل من 60%)، وتكون أراء العينة في الفقرة محايدة إذا كان مستوى الدلالة لها أكبر من 0.05.

وللإجابة على هذه التساؤلات نختبر الفرضيات التالية :

1. الفرضية الأولي : يؤثر توفر الإجراءات والسياسات الرقابية على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$.

تم استخدام اختبار t.test للعينة الواحدة والذي يبين أراء أفراد عينة الدراسة في فقرات الإجراءات والسياسات الرقابية والنتائج موضحة في جدول رقم (5).

جدول (5) تحليل الفقرات المتعلقة الإجراءات والسياسات الرقابية

	الفقرة	المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	اتجاه الفقرة
1	توجد هناك إدارة/ قسم لنظم المعلومات في الهيكل التنظيمي للمركز	4.10	82.00	1.41	0.114	1
2	يوجد دليل للإجراءات والسياسات المتبعة لأمن المعلومات بالمركز	2.69	53.80	2.98	0.020	موافق
3	توجد صلاحيات واضحة بكل وظيفة من وظائف نظم المعلومات	3.21	64.20	2.78	0.024	محايد
4	توجد صلاحيات للعاملين بالإدارة أو القسم لإصدار الأوامر لتغيير البرامج والصلاحيات والملفات لحماية النظام	2.98	59.60	2.88	0.022	محايد
5	يتم اختيار الكفاءات المؤهلة علميا وعمليا لتوظيفها وتدريبها لحماية النظام	3.32	66.40	3.82	0.009	محايد
6	يمنع مشغلي الأجهزة من الحصول على أية بيانات غير لازمة لتشغيل الجهاز	3.07	61.40	2.52	0.032	محايد
7	تقوم الإدارة العليا بإصدار قرارات خاصة لتجنب مخاطر أمن المعلومات	3.01	60.20	2.80	0.024	محايد

8	تتابع الإدارة الموظفين العاملين بتكنولوجيا المعلومات في تنفيذ الحماية المطلوبة	2.87	57.40	3.90	0.008	محايد
9	تقوم الإدارة دوريا بوضع خطط حماية شاملة تشمل إغلاق منافذ الاختراقات والاحتفاظ بنسخ احتياطية للمعلومات	2.76	55.20	3.72	0.010	محايد
10	تقوم الإدارة بوضع قواعد خاصة لحماية أمن المعلومات ومعاقبة العاملين المخلين بهذه القواعد	2.82	56.40	2.58	0.030	محايد
11	تقوم إدارة المركز بتحليل المخاطر الخاصة بأمن المعلومات فيما يتعلق باختيار التقنية المناسبة والية العمل بها وتحديد طرق الحماية حسب التغيرات في بيئة التكنولوجيا	2.82	56.40	4.51	0.005	محايد
12	تقوم الإدارة بتركيب طرق الحماية التقنية مثل جدران النار ومضادات الفيروسات	3.55	71.00	1.90	0.064	محايد
13	تقوم الإدارة بصد الاختراقات الطارئة عند حدوثها وصلاح الخلل الناتج عنه	3.58	71.60	3.07	0.018	موافق
14	تستفيد الإدارة من خبرة الشركات العالمية في مجال أمن المعلومات والاتصالات	3.10	62.00	4.18	0.006	موافق
15	يوجد دليل متضمنا تحديد الصلاحيات المتعلقة بكل وظيفة من وظائف نظم المعلومات	3.17	63.40	3.18	0.016	محايد
جميع الفقرات		3.13	62.60	3.08	0.026	

نلاحظ من الجدول رقم (5) أن المتوسط الحسابي لجميع فقرات الإجراءات والسياسات الرقابية على إدارة أمن نظم المعلومات يساوى 3.13، وهو متوسط يقع في الفئة الثالثة من مقياس ليكرت الخماسي ويعبر عن الاتجاه (محايد) وهو متوسط أكبر من القيمة المتوسطة المحايدة "3"، ومن ثم فإن هذه الفقرات ذات أثر متوسط في زيادة أمن المعلومات، كما نلاحظ أن المتوسط الحسابي النسبي يساوى 62.60 وهو أكبر من المتوسط الحسابي النسبي المحايد 60% والقيمة t المحسوبة المطلقة تساوى 3.08 وهى أكبر من قيمة t الجدولية والتي تساوى 1.98، والقيمة الاحتمالية (Sig') تساوى 0.026 وهى أصغر من 0.05، مما يدل على صحة الفرضية الفرعية (يؤثر توفر حماية الإجراءات والسياسات الرقابية على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq$ 0.05).

1. الفرضية الثانية : يؤثر توفير طرق تطوير إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq$ 0.05.

تم استخدام اختبار t.test للعينة الواحدة والذي يبين أراء أفراد عينة الدراسة في طرق تطوير إدارة أمن المعلومات والنتائج موضحة في جدول رقم (6).

جدول (6) تحليل الفقرات المتعلقة بطرق لتطوير إدارة أمن نظم المعلومات

الفقرة		المتوسط الحسابي	المتوسط الحسابي النسبي	قيمة t	القيمة الاحتمالية	اتجاه الفقرة
16	تعزيز البنية التحتية لتكنولوجيا المعلومات لضمان أمن نظم المعلومات	4.10	82.00	1.44	0.111	موافق
17	توفير ميزانية مخصصة لأمن المعلومات	3.85	77.00	2.10	0.051	موافق
18	اختبار أنظمة المعلومات للتحقق من الالتزام بمعايير الأداء الأمني	2.82	56.40	2.58	0.030	محايد
19	استخدام برامج حماية فعالة لمنع محاولات الاختراقات والاعتداءات على نظم المعلومات في المراكز البحثية	3.76	75.20	2.31	0.040	موافق
20	دعم الجهات المسئولة العليا لسياسة ناجحة لأمن المعلومات	3.83	76.60	2.06	0.053	موافق
21	استخدام الوسائل البيولوجية (بصمة الإصبع، أو بصمة العين، أو التعرف على الوجه) في تحديد شخصية وصلاحية مستخدمي نظم المعلومات.	3.46	69.20	3.20	0.016	موافق
22	وضع ضوابط لتبادل المعلومات مع الجهات الخارجية	3.50	70.00	3.24	0.015	موافق
جميع الفقرات		3.62	72.34	2.41	0.045	

نلاحظ من الجدول رقم (6) أن المتوسط الحسابي لجميع فقرات المتعلقة بطرق لتطوير إدارة أمن نظم المعلومات يساوى 3.62، وهو متوسط يقع في الفئة الرابعة من مقياس ليكرت الخماسي ويعبر عن الاتجاه (موافق)، ومن ثم فإن هذه الفقرات ذات أثر كبير في زيادة أمن المعلومات، كما أن المتوسط الحسابي النسبي يساوى 72.34 وهو أكبر من المتوسط الحسابي النسبي المحايد 60% والقيمة t المحسوبة المطلقة تساوى 2.41 وهى أكبر من قيمة t الجدولية والتي تساوى 1.98، والقيمة الاحتمالية (Sig') تساوى 0.045 وهى أصغر من 0.05، مما يدل على صحة الفرضية الفرعية, (يؤثر توفير طرق تطوير إدارة أمن نظم المعلومات على إدارة أمن نظم المعلومات بصورة إيجابية عند مستوى الدلالة الإحصائية $\alpha \leq 0.05$).

14 .النتائج

1. لاحظ من خلال نتائج الدراسة عدم توفر حماية لأمن المعلومات في المراكز البحثية بصورة جيدة.
2. معرفة الجهات المسئولة للمراكز البحثية بأهمية سياسات أمن المعلومات، إلا انه لا يوجد في أي من المراكز المذكورة سياسات وإجراءات معمول بها ومطبقة على أسس واضحة.
3. هناك نقص في برامج التوعية والتدريب للعاملين في مجال أمن المعلومات.
4. عدم توفر سياسات أمن المعلومات وعدم توفر الإجراءات الداعمة لها.
5. عدم توفر الكفاءات سواء من جانب مشغلي خدمات أمن المعلومات أو من جانب الجهات المسئولة.
6. غياب الوعي بأمن المعلومات على جميع مستويات المراكز البحثية.
7. اعتقاد أن امن المعلومات يعتمد على بعض التقنيات كجدار الحماية أو مضاد الفيروسات وعدم التفكير في تبنى استراتيجيات لاحتواء الأحداث الأمنية بطرق مناسبة والعمل على معرفة أسباب حدوثها.

15. التوصيات

في ضوء النتائج السابقة نوصى بالتالي :

1. زيادة الاهتمام بتوعية العاملين بالمراكز البحثية بأهمية إستخدام المعايير والسياسات الأمنية وإقامة دورات تدريبية وورش عمل.
2. ضرورة قيام المراكز البحثية ببناء سياسات لأمن نظم المعلومات خاصة بها والعمل على نشرها وتطبيقها، والقيام بتطويرها ومراجعتها وتقييم المخاطر بشكل دوري ووضع خطط لضمان أمن وسرية المعلومات.
3. تطبيق المعايير الدولية لأمن المعلومات يوفر ضمان الحماية لها في جميع المراكز البحثية .
4. التأكد من الالتزام بالسياسات والإجراءات الأمنية.
5. استخدام تقنيات تشفير البيانات والتأكد من أمن كافة الأنظمة بشكل مستمر.
6. حماية شبكات المراكز وكافة الخوادم وأجهزة الحاسوب من خلال التحديث المستمر للبرامج الأصلية.
7. وضع نظام مجدول للنسخ الاحتياطي والعادي خاصة في ظل الظروف الحالية من ناحية التهديدات والانتهاكات اليومية من قبل المحترفين.
8. تحديد المخاطر وتقييم الثغرات الأمنية التي يمكن أن تهدد امن المعلومات في هذه المراكز البحثية.
9. تطوير النظام وصيانته لحماية أصول المراكز البحثية وتحصين مبانيها في كل نواحي أنظمة تكنولوجيا المعلومات والبرامج والبيانات التابعة لها .

16. الخاتمة

إن تطبيق خطة إدارة امن المعلومات في المراكز البحثية يكون على عدة مراحل وتحتاج إلى مراجعة دورية ليتلاءم فعلها مع وجود التحديات والاختراقات الموجودة، لذا يجب على الجهات المختصة إتباع كافة المعايير الأمنية، والاهتمام بكافة السياسات والاجراءات الرقابية لتطوير إدارة امن المعلومات بها، كما يجب نشر الوعي بين العاملين تجاه حماية معلوماتهم ومعلومات الجهات التابعين لها وتحديد الإجراءات والسياسات الأمنية التي تقوم بها الجهة المختصة في حال حدوث خروقات أو انتهاكات، وفي الختام نأمل تطبيق سياسة أمن المعلومات فى جميع المؤسسات الحكومية والغير حكومية.

المراجع

[1] Zammani, M and Razali, R, (2016), "An Empirical Study of Information Security Management Success Factors", International Journal on Advanced Science Engineering information Technology, Vol. 6, No. 6.
[2] BOWEN, Pauline and others, (2006)-Information Security Handbook. A Guide for Managers, Washington:NIST.
[3] Micki Krause ;Harold F. Tipton, Information Security Management Hand book, Sixth Edition, Auerbach Publication , New York , 2008.
[4] Bel G. Raggad. 2010, “Information Security Management: concepts and practice page 23.
[5] Baskerville, Richard, and Mikko Siponen. An information security meta-policy for emergent organizations. Logistics Information Management 15.5/6 (2002) 337-346.
[6] Stair, Ralph M. &George W. Reynolds. (2010).Principles Of Information Systems, Course Technology. 9th Editions. NY: Mc- Graw-Hill Straub, et.al.(1995). Measuring System.

[7] . تارة ، أنس (2006)، أمن المعلومات والنظم

[8] "PROTECT YOUR INFORMATION FROM PHYSICAL THREATS", www.securityinabox.org, 28-6-2018، Retrieved 20-9-2018. Edited.

[9] رؤى بن يونس، "دراسة واقع أمن نظم المعلومات في المؤسسات السورية"، مجلة البعث– المجلد 39 – العدد 31 لسنة 2017.

[10] رضا ابراهيم، أحمد عبد السلام "دراسة أثر ادارة امن المعلومات على نجاح برنامج نظم المعلومات"،مجلة الدراسات التجارية المعاصرة، المجلد السادس، العدد العاشر، 2020.

[11] عرفان نبي، عبد الرحمن مرزا، خالد الغنبر، "دراسة عملية حول أمن المعلومات في المنظمات السعودية"، جامعة الملك سعود، مركز التميز لأمن المعلومات، لسنة 2010.

[12] Zammani, M and Razali, R, (2016), "An Empirical Study of Information Security Management Success Factors", International Journal on Advanced Science Engineering information Technology, Vol. 6, No. 6.

[13] MWITA SIMION MAROA, « Factors affecting information systems security effectiveness in university of Nairobi », Thesis of Master of science degree in information systems, Kenya,2015.

[14]Huang, Ding-Long; Rau, Pei-Luen Patrick & Salvendy, Gavriel, (2010), "Perception of information security",Behaviour & Information Technology, Vol. 29, No. 3, May–June: 221–23.