Dirassat & Abhath
The Arabic Journal of Human and Social Sciences

مجلة دراسات وأبحاث
المجلة العربية في العلوم الإنسانية والاجتماعية

EISSN: 2253-0363
ISSN : 1112-9751

دور إجراءات الأمن المعلوماتي في الحد من مخاطر امن المعلومات في جامعة الطائف

The role of information security measures in reducing the risks of information security at Taif University

عدنان عواد الشوابكة Adnan Awad AL-Shawabkeh
جامعة الطائف Taif University
a_shawabkeh@yahoo.com

تاريخ الاستلام : 2018-09-02 تاريخ القبول : 2019-09-19

ملخص:

هدفت الدراسة الى التعرّف على دور اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلوماتفي جامعة الطائف. ولتحقيق ذلك تم تصميم استبانة مكونة من (52) فقرة، تم توزيعها على عينة الدراسة المكونة من (129) عاملا، وقد توصلت الدراسة الى ان الاجراءات الامنية في الحد من مخاطر امن المعلوماتفي الجامعة عالية. والاجراءات الامنية لمنع الاختراق عن طريق الشبكة الحاسوبية Network Hackingجاءت بمستوى مرتفع بينما الاجراءات الامنية لمنع الاختراق عن طريق الهندسة الاجتماعية Social Engineeringجاءت بمستوى متوسط. والاجراءات الامنية لمنع الاختراق عن طريق البرمجيات الضارة Malwareجاءت بمستوى متوسط. وتُساهم اجراءات الامن المعلوماتي في الحد من المخاطر الداخلية والخارجية والطبيعية التي يتعرض لها النظام.

وقد اوصت الدراسة بضرورة قيام ادارة الجامعة بوضع تصنيفات للمعلومات بالطريقة التي تناسب اعمالها وسرية معلوماتها مع عزل البيانات والمعلومات التي يشكل عرضها للعامة ضرر للنظام. وتقييم المخاطر التي يتعرض اليها النظام بشكل دوري للوقوف على ما يُمكن عمله وايجاد السبل الكفيلة باستعادة العمل، ووضع خطط الطوارئ اللازمة لضمان امن النظام في الجامعة.

الكلمات المفتاحية : اجراءات الامن المعلوماتي، مخاطر اختراق الشبكات، مخاطر الهندسة الاجتماعية،مخاطر البرمجيات الضارة، امن المعلومات.

Abstract

The study aimed to identify the role of information security measures in reducing the risks of information security at Taif University. To achieve this, a questionnaire consisting of (52) items was designed to be distributed to the study sample of (129) workers. The study concluded that the security measures in reducing the risks of information security at the university are high. The security measures to prevent network hacking came at a high level while security measures to prevent penetration through social engineering came at an average level. Malware security measures came at an average level. Information security measures reduce internal, external and natural risks to the system.

The study recommended that the university administration develop classifications of information in a way that suits its work and confidentiality of its information, while isolating the data and information that are presented to the public as damage to the system. And assess the risks to which the system is exposed periodically to find out what can be done and find ways to restore work, and develop contingency plans to ensure the security of the system at the university.

Key Words : Information security measures, network penetration risks, social engineering risks, malware risks, information security.

1. مقدمة.

لقد اصبحت الجرائم المعلوماتية ظاهرة خطيرة لها تأثيراتها السلبية في المجالات الاقتصادية والسياسية والامنية وازداد خطرها بعد تطور تقنيات الاتصال وزيادة قدرات وسائط التخزين ونقل المعلومات من مكان لآخر ومن بلد لآخر بسرعة فائقة جعلت المواجهة امرا في غاية الاهمية، ولذلك لا بد من وضع اجراءات تعمل على الحد من المخاطر التي يتعرض لها الامن المعلوماتي في المنظمة. ولذا فأن امن المعلومات يمثل حماية وتامين كافة الموارد المستخدمة والعمل على سريتها وسلامتها، وفي غياب امن المعلومات او توقفه وعدم الاستفادة منه يؤدي الى فقدان الثقة مما يجعله عبئا على المنظمة، وعلى هذا الاساس يجب حماية معلومات المنظمة والحد من الاضرار التي قد تؤدي الى المخاطر التي قد يواجها النظام.

ولضمان امن المعلومات وسريتها هناك طرق دقيقة وملائمة وموثوق بها مثل الجدران النارية وكلمة السر والتشفير وغيرها من الطرق التي تُستخدم لعدم افشاء المعلومات المخزّنة والتي قد تؤثر على الاصول المعلوماتية للمنظمة.

ومن اساليب مواجهة مخاطر الامن المعلوماتي في المنظمة العنصر المادي الذي يعمل على توفير الحماية المادية لنظم المعلومات، والعنصر التقني الذي يعمل على دعم وحماية امن المعلومات من خلال استخدام التطبيقات الحديثة، والعنصر البشري الذي يعمل على رفع قدرات وتنمية مهارات العاملين في هذا المجال (عبدالكريم، 2013). وفي هذه الدراسة سنحاول التعرّف على دور اجراءات الامن المعلوماتي واثرها في الحد من مخاطر امن المعلوماتفي جامعة الطائف.

2. مشكلةالدراسة.

نتيجة الانتشار الواسع لتطبيقات تكنولوجيا المعلومات فقد ظهرت الكثير من مخاطر امن المعلومات التي تهدد الاصول المعلوماتية للمنظمة، حيث اصبحت المعلومات عرضة للسرقة والتغيير والكشف من غير المصرح له بالاطلاع عليها. ونتيجة لأهمية هذه المعلومات وارتفاع قيمتها لدى الكثير من المنظمات فانه لا بد من اتخاذ الاجراءات والتدابير المناسبة لحماية المصادر المعلوماتية من المخاطر، ومن بين تلك الاجراءات "اجراءات الامن المعلوماتيفي المنظمة" والتي تهدف الى التحقق من سلامة اداء المنظمة واداء كل نشاط من نشاطاتها. ومن هنا يمكن بلورة مشكلة الدراسة في التساؤل الرئيس التالي :-التعرّف على دور اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلوماتفي جامعة الطائف.

1.2 اسئلة الدراسة.

1) ما هي إجراءات الامن المعلوماتي في جامعة الطائف؟
2) ما هي طبيعة مخاطر امن المعلومات الداخلية ؟
3) ما هي طبيعة مخاطر امن المعلومات الخارجية ؟
4) ما هي طبيعة المخاطر الطبيعية ؟

3. اهداف الدراسة.

تهدف هذه الدراسة إلى تحقيق الامن المعلوماتي من خلال ما يلي:-

1) التعرف على اهم إجراءات الامن المعلوماتي التي تضعها الجامعة على نظم المعلومات للحد من المخاطر التي تتعرض لها هذه النظم.
2) التعرف على اهم المخاطر الداخلية التي تهدد نظم المعلومات.
3) التعرف على اهم المخاطر الخارجية التي تهدد نظم المعلومات.
4) التعرف على اهم المخاطر الطبيعية التي تهدد نظم المعلومات.

4. أهميةالدراسة.

تأتي اهمية هذه الدراسة نتيجة لما تتعرض له نظم المعلومات من مخاطر والتي تهدد امن وموثوقية ومصداقية البيانات التي توفرها تلك النظم، وتأتي الاهمية نتيجة التطور الكبير في تقنية المعلومات وصناعة الحواسيب والذي ادى الى سهولة نسخ وتعديل وتغيير البيانات والملفات المخزنة بذاكرة الحاسوب، وهذا الشيء لم يصاحبه تطور مماثل في اجراءات الامن المعلوماتي المطبقة في الجامعة. ولذلك تبرز أهمية الدراسة من خلال ما يلي :-

1) توفير متطلبات الامن المعلوماتي في الجامعة.
2) المحافظة على أمن المعلومات والبيانات الخاصة بالجامعة وحمايتها من احتمال فقدانها، مما لها من تأثير على استراتيجية الجامعة وخططها المستقبلية.
3) حماية النظام الامني للمعلومات في الجامعة يعمل على منع اختراق بياناتها أو تعديلها او إتلافها.
4) محاولة الربط بين دور اجراءات الامن المعلوماتي واثرها في الحد من مخاطر امن المعلومات
5) قلة الدراسات التي تبحث في المخاطر التي تتعرض لها نظم المعلومات في الجامعات السعودية بشكل عام وفي جامعة الطائف بشكل خاص.
6) تُساهم بصورة ايجابية الى وضع اجراءات امنية على انظمة المعلومات للحد من المخاطر التي تعترض هذه النظم.
7) تقديم نتائج وتوصيات تُساهم في تحديد نقاط الضعف ضمن مكونات نظم الامن المعلوماتي للمحافظة على أمن معلومات الجامعة والمحافظة على سريتها في مختلف المستويات الادارية عن طريق اعداد البرامج التدريبية التوعوية للمستخدمين.

5 فرضيات الدراسة.

1.5 الفرضية الرئيسية الأولى.

تُساهم اجراءات الامن المعلوماتي (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الداخلية.

2.5 الفرضية الرئيسية الثانية.

تُساهم اجراءات الامن المعلوماتي (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الخارجية.

3.5 الفرضية الرئيسية الثالثة.

تُساهم اجراءات الامن المعلوماتي (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الطبيعية.

6. الاطار النظري.

1.6 المقدمة.

تعتبر اجراءات الامن المعلوماتي نقطة الانطلاق التي ترتكز عليها المنظمة في جميع عملياتها ولذلك عندما نتحدث عن امن المعلومات كمفهوم فإننا نجد عدة مفاهيم لها، إلا أن هذه المفاهيم تشترك في مجملها وإن اختلفت نصوصها وصياغتها، فهي عملية متكاملة يتم تصميمها بقصد منع المخاطر التي تهدد امن المنظمة وتوفير درجة الامان لمنع اختراق الاجهزة والبرمجيات والشبكة الحاسوبية وتوفير الامن المعلوماتي في المنظمة.حيث تعمل هذه الاجراءات على حماية بيانات المنظمة والمخزنة على اجهزة الحواسيب والخوادم المتصلة بالشبكة، وقد تكون هذه الشبكات عرضة للاختراق مما يؤدي الى تلف البيانات وتدميرها (عبدالكريم، 2013) .

حيث يؤدي نظام الرقابة الداخلية الضعيف إلى وضع نظام معلومات المنظمة في مخاطر عديدة منها إتاحة الفرصة لسرقة الأصول من قبل الموظفين، واحتمالية فقدان المعلومات المتعلقة بالعمليات، وغيرها من المخاطر والتهديدات التي قد تؤدي إلى فشل منظمات الأعمال في تحقيق أهدافها.

2.6 مفهوم اجراءاتالامن المعلوماتي.

هي مجموعة العمليات التي يتم تصميمها لتحقيق مجموعة من الاهداف تتعلق بإمكانية الاعتماد على فاعليّة العمليات في المنظمة والالتزام بالقوانين واللوائح من اجل التحكم في جميع العمليات داخل المنظمة والحد من المخاطر التي يتعرض لها امن المعلومات في المنظمة(Porter, et al., 2008).

3.6 اجراءاتالامن المعلوماتي.

تعتبر اجراءات الامن المعلوماتي من المواضيع الهامة التي يجب الاهتمام بها من قبل الإدارة العليا نظرا للأهمية الاستراتيجية التي تتمتع بها لعدة اسباب منها ما يلي (Raval& Fichadia 2007) :-

1) احتمالية اختراق الأنظمة وسرقة المعلومات والبيانات أو تعديلها بشكل غير مرغوب أو أن يتم تعديلها من قبل مستخدمي النظام بشكل مقصود أو غير مقصود.
2) الامتثال لمتطلبات قوانين الحماية والخصوصية مثل خصوصية المعلومات المتعلقة بالموظفين والزبائن والموردين.

7 امن المعلومات.

يُعرّف امن المعلومات بانه :- العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. والمعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات والحماية من المخاطر المحتملة والناتجة عن استغلال ثغرات وضعف النظام (Raval& Fichadia, 2007).

1.7 اهمية امن المعلومات.

تنبع اهمية امن المعلومات من انها تستخدم من قبل جميع المستخدمين في المنظمة حيث هناك امكانية الاختراق من قبل المستخدمين العاملين في المنظمة انفسهم. ولذلك يعتبر امن المعلومات من اهم القضايا التي يتم مناقشتها في مجال الشبكات وامن وسرية المعلومات، ونتيجة لكثرة برامج الفيروسات وبرامج التجسس وسرعة انتشارها اقتصر دور الكثير من المختصين في تقنية المعلومات على التعامل مع المنظمة لوضع البرامج المضادة للفيروسات وبرامج الاختراق والتسلل والتركيز على مستوى الاهتمام بتنفيذ الاجراءات الامنية كما اوردها (السالمي، 2001) وتنبع اهمية امن المعلومات منكل مما يلي (Merkowand James., 2005) :-

1) اجراءات للسيطرة تحول دون الوصول للبرمجيات مع اجراءات تمنع او تكشف المتطفل من الدخول للنظام.
2) معدات وبرمجيات مضادة للفيروسات.
3) تغيير مستمر لكلمات السر والتشفير.
4) خطط استرجاع سريعة في حالة الكوارث الطبيعية والبيئية.

ولذلك فان وضع سياسة لأمن المعلومات تُعَد من اكثر الامور صعوبة وحساسية، ومن اولويات الجهة المعنية بتقنية المعلومات في أي منظمة، بحيث تكون هذه السياسة واضحة المعالم لجميع المستخدمين في المنظمة ويكون معروف مسبقا فيها وواجبات كل مستخدم ومستفيد من تقنية المعلومات (Raval& Fichadia, 2007) ومن هذه الاهداف ما يلي (Merkowand James, 2005) :-

1) نزاهة المعلومات Information Integrity وهي دقة وموثوقية المعلومات المستخرجة من النظام.
2) السرية Confidentialityأي الاحتفاظ بالمعلومات السرية بعيدا عن الأشخاص غير المصرح لهم.
3) التحقق من المستخدم User Authenticationأي المصادقة على هوية الأشخاص المصرح لهم.
4) دقة وسلامة امن العمليات ومصادر نظام المعلومات.
5) تقليل الاخطاء والمخاطر التي تعتري النظام.
6) حماية ممتلكات المنظمة من التلف والضياع وسوء الاستخدام.
7) زيادة الملاءمة والموثوقية للمعلومات المستخدمة لاتخاذ القرار.

2.7 مخاطر امن المعلومات.

لا بد من تعريف الخطر والتمييز بين المفاهيم ذات العلاقة وذلك على النحو التالي :-

1) **التهديد Threats:-** يقصد به احتمال تعرض النظام في المنظمة لاعتداء ما يكون مصدره شخصا ما كالمتجسس او المخترق او المتطفل او أي شيء يهدد الاجهزة والمعدات او الكوارث الطبيعية (Anton, 2003).
2) **الخطر Risk:-** يقصد به الاثر الذي يقع نتيجة حدوث فعل التهديد، أي انه حدث ما يقع نتيجة تهديد ما والفرق بين الخطر والتهديد هو ان الخطر حدث فعلا، اما التهديد فيبقى في دائرة الاحتمال(Schchter, 2004).
3) **نقاط الضعف او الثغراتVulnerabilities :-** تعني جزء من النظام يحتمل ان يتحقق بسببه التهديد ليصبح خطرا، أي يعبر من خلاله منفذ التهديد ليقع بعد ذلك الخطر مثل عدم تدريب المستخدمين على النظام وحمايته او الاتصال بالإنترنت اذا لم يكن مشفرا او موقع خوادم النظام في المنظمة اذا لم يكن مجهز بوسائل الحماية. وعموما فان الثغرات هي الاسباب المحركة لتحقيق التهديدات وحدوث المخاطر. وهناك نوعين من الثغرات وهما :-

- **الثغرات التقنية Technical Vulnerabilities** :-ويقصد بها الاخطاء عند تصميم النظام مما يجعل من السهل وقوع الاخطاء من خلالها.
- **الثغرات الادارية Administrative Vulnerabilities**:-وهي الثغرات التي تتمثل بضعف التجهيزات الادارية واماكن تخزين المعلومات مما يتيح تعرضها لبعض المخاطر(Marianne, 2009).

3.7 تصنيف مخاطر امن المعلومات.

صنفت مخاطر امن المعلومات وفقا لمعايير مختلفة منها الاتي :-

1) **تصنيف المخاطر من حيث المصدر ,Noordegraff) (2002** :-صنفت المخاطر الى ثلاثة اصناف هي مخاطر من الانترنت ومخاطر الموظفين والمخاطر الطبيعية، كما صنفت الى اربعة اقسام وهي مخاطر داخلية ومخاطر خارجية مرتبطة بالأنترنت ومخاطر مادية ومخاطر بيئية.
2) **تصنيف المخاطر حسب الهدف (البحيصي، 2011)** :- صنفت المخاطر الى مخاطر متعمدة ومخاطر غير متعمدة.

4.7 مصادر المخاطر الامنية.

تناولت الادبيات المتعلقة بأمن المعلومات العديد من المخاطر التي تواجه بيئة نظم المعلومات، وصنفت من حيث المصدر الى مصادر داخلية ومصادر خارجية (Warkentin, andWillison, 2009) وذلك على النحو التالي :-

1.4.7 المصادر الداخلية.

هي المصادر التي تحدث بسبب احد مكونات النظام ومنها ما يلي :-

1) **المخاطر البشرية** :- تُعّد المخاطر التي يتسبب بها الافراد العاملون في النظام من اخطر التهديدات واكثرها تأثيرا وتشمل الافعال المقصودة والغير مقصودة من قبل الاشخاص المسموح لهم وغير المسموح لهمباستخدام النظام (Goodhue and Straub, 2001) .
2) **الخلل في المعدات** :- يتضمن اعطال اجهزة الحاسوب والطرفيات والتجهيزات الشبكية المرتبطة بالنظام، وهذاالنوع من الاعطال يتسبب في توقف النظام عن العمل وحجب الخدمة عن المستفيدين (Schechter, 2004).
3) **اخطاء البرمجيات** :- تعاني الكثير من البرمجيات المستخدمة في النظام من احتوائها على الاخطاء، الامر الذي ينعكس على دقة المخرجات وصحة المعالجة التي يقوم بها النظام (Robert, 2010).
4) **اخطاء البيانات** :- هي الاخطاء الناشئة عن عملية ادخال البيانات، بحيث يتم ادخال بيانات غير صحيحة مما ينعكس على دقة المخرجات، وكلما زادت نسبة الخطأ في البيانات المدخلة كلما زاد حجم الخطر (Marianne, 2009).

2.4.7 المخاطر الخارجية.

هذا النوع من المخاطر يكون مصدره اسباب من خارج النظام، أي يمكن ان يكون نتيجة اشخاص غير مخولين باستخدام النظام، او من اسباب بيئية او طبيعية، ومن هذه المخاطر ما يلي :-

1) **الهجوم الامني** :- يقصد به المحاولات المختلفة التي ينفذها الاشخاص غير المخولين بقصد الوصول غير الشرعي للنظام، او احد مكوناته واحداث الخطر فيه (Heiser, 2013).
2) **خطر الاختراق** :- يقصد به القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف، ويتحقق ذلك بدخول شخص غير مصرح له الى النظام، والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية او تدمير الملفات او البرمجيات (Kissel, 2013).
3) **الاصطياد الالكتروني** :- يقصد به قيام المهاجمبإرسال رسائل بريد الكترونية خادعة الى المستخدمين تتضمن روابط الكترونية مزيفة تشابه الموقع الالكتروني للمنظمة، او تكون مواقع الكترونية مزيفة تدعي انها بنوك وتقدم خدمات بنكية، وعند دخول المستخدم لهذه المواقع فأنها تطلب منه معلومات، كمعلومات حسابه البنكي او معلومات بطاقته الائتمانية وهذه المواقع تكون مصممة بطريقة تشبه فيها المواقع الالكترونية الحقيقية (Litan, 2004).

4) **البرامج الخبيثة :-** عبارة عن برنامج صغير مُعدّ لتخريب البيانات، يتم ادخاله الى الحاسوب من غير علم المستخدم بغرض نسخ او ازالة البيانات المسجلة عليه ومن الامثلة عليه الفيروسات الحاسوبية وبرامج الديدان وحصان طروادة والقنابل الموقوتة (Merkowand James, 2005).

3.4.7 المخاطر الطبيعية او البيئية.

هي المخاطر التي يكون مصدرها البيئة او الطبيعة التي يعمل بها النظام وهي المخاطر التي تقع على مكونات النظام كالأجهزة والبرمجيات والشبكة الحاسوبية. ويشمل الحرائق والكوارث الطبيعية وانقطاع الكهرباء (الهادي، 2006).

8 التهديدات التي تواجه أمن المعلومات.

تتزايد التهديدات التي تتعرض لها المنظمات نتيجة التطوّر المتسارع في الأساليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية خاصة بالمنظمة بشكل غير مصرح به بهدف تعديلها أو سرقتها أو حتى تدمرها. ويمكن تصنيف أساليب التهديد بهدف الحصول على المعلومات بأسلوب غير مصرح به (Romney & Steinbart 2012) الى ما يلي :-

1) **اختراق الشبكات Hacking :-**تتم عملية الاختراق من خلال سرقة كلمة السر Password cracking او التعرض للاختراق أثناء محاولة معالجة اختراق سابق Zero-day- attack او هجمات حقن قواعد البيانات او Structured Query Language Injection Attack).

2) **الهندسة الاجتماعية Social Engineering:-**يقصد بها تحفيز المستخدم على الإفصاح عن بيانات سريتها من خلال طرح أسئلة بهدف جمع معلومات دون إثارة أي شبهة، ويحتوي هذا الأسلوب على عدة تقنيات منها ما يلي:-

- **التوأمة الشريرةEvil Twin:-**أي ادعاء جهة معينة بأنها جهة موثوق منها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضارا به.
- **سرقة الهوية Identity Theft :-** أي ادعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر.
- **التصيّد Phishing:-** ويقصد منها وصول رسالة مزيفة منجهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة.

3) **البرمجيات الضارة Malware :-**تتم عملية الاختراق من خلال برامج متخصصة لتسهيل التسلل إلى النظام أو الشبكة بهدف تدمير البيانات، وما أن يتم تثبيت البرمجية الضارة فإنه من الصعب جداً إزالتها، ويحتوي هذا الأسلوب على عدة تقنيات منهاما يلي :-

- **حصان طروادة Trojan Horse**:- برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم.
- **الفيروساتViruses**:- برامج تدخل إلى الحاسوب وتتصل بالملفات المخزنة به ثم يكرر نفسه بحيث يتم تدمير هذه الملفات.
- **برامج التجسس Spyware**:- برمجيات تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب وغالبا ما يتم تنزيلها بشكل سري تكون مرافقة لتنزيل برمجيات أو ملفات مجانبة من الإنترنت.

9 الدراسات السابقة.

دراسة (أبو حجر واخرون، 2014) دور اليات حوكمة تكنولوجيا المعلومات في تخفيض مخاطر امن المعلومات في الوحدات الحكومية في ظل الحكومة الالكترونية. تهدف هذه الدراسة الى توضيح دور حوكمة تكنولوجيا المعلومات في الحد من هذه المخاطر للحد من التلاعب المالي الالكتروني في ظل تطبيق الوحدات الحكومية لنظام الحكومة الالكترونية من الناحية النظرية، وقد توصلت الدراسة الى مجموعة من النتائج من اهمها :-

1) يواجه تطبيق نظام الحكومة الالكترونية بعض الصعوبات والمخاطر التي تهدد امن المعلومات الحكومية وتجعله عرضة لفقد ثقة المتعاملين به والمستفيدين منه فيه والتي من اهمها التلاعب المالي الالكتروني.
2) تُساهم اليات حوكمة تكنولوجيا المعلومات في تحقيق متطلبات امن المعلومات والحد من المخاطر التي يتعرض لها.

وقد اوصت الدراسة بتطوير اجراءات نظام الرقابة الداخلية في الحد من التلاعب المالي الالكتروني.

دراسة (الدنف، 2013) واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها. هدفت الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة، واستخدم الباحث المنهج البحثي الوصفي التحليلي، وتكون مجتمع الدراسة من العاملين على نظم المعلومات في الكليات التقنية وجمعت أدوات الدراسة بين الاستبانة والمقابلة، وقد توصلت الدراسة إلى مجموعة من النتائج أهمها :-

1) تتوفر البنى التحتية لنظم المعلومات في الكليات التقنية بدرجة متوسطة.
2) تدرك الإدارات العليا للكليات التقنية أهمية سياسات أمن المعلومات الا أنه لا يوجد في أي من الكليات سياسات معمول بها ومطبقة على أسس واضحة.
3) تتفاوت الكليات التقنية مجتمع الدراسة في درجات استخدام نظم معلوماتها.
4) توجد فروق ذات دلالة إحصائية في آراء عينة الدراسة حول واقع إدارة أمن نظم المعلومات في الكليات التقنية.

وقد اوصت الدراسة بضرورة بناء سياسات أمن نظم المعلومات الخاصة بها، والعمل على نشرها وتطبيقها والقيام بتطويرها ومراجعتها وتقييم المخاطر بشكل دوري للوقوف على ما يمكن ايجاد السبل الكفيلة باستعادة العمل ووضع خطط الطوارئ اللازمة لضمان أمن نظم المعلومات، وكذلك ضرورة إنشاء مركز متخصص يعنى بقضايا أمن المعلومات.

دراسة (عواد، 2012) بعنوان مدى فعاليّة اجراءاتنظام الرقابة الداخلية في ظل نظم المعلومات المحاسبية الإلكترونية - دراسة تطبيقية على البنوك العاملة في قطاع غزة. هدفت الدراسة الى التعرف مدى فعاليّة اجراءات نظام الرقابة الداخلية في ظل نظم المعلومات المحاسبية الإلكترونية على البنوك العاملة في قطاع غزة، وقد تم الاعتماد على استبانة صممت لهذا الغرض حيث تم توزيع 48 استبانة استراد منها 43 استبانة، وقد شملت الدراسة جميع المصارف الاسلامية وعددها 3 مصارف، وقد توصلت الدراسة الى مجموعة من النتائج اهمها :-

1) فعاليّة اجراءات نظام الرقابة على دراسة المخاطر التي تهدد امن المعلومات في النظام.
2) فعاليّة اجراءات نظام الرقابة الداخلية وقدرتها على اكتشاف الاخطاء والغش والتلاعب.

وقد اوصت الدراسة بان تدرس الرقابة الداخلية المخاطر الناتجة عن تطبيق انظمة المعلومات المحوسبة والمخاطر الناتجة عن الموظفين، وكذلك بضرورة حماية الموجودات والملفات والاجهزة من سوء الاستخدام وفرض عقوبات من قبل الادارة عند اكتشاف مخالفات تدل على عدم الامانة.

دراسة (عرفان وآخرون، 2010) بعنوان أمن المعلومات في المنظمات السعودية. هدفت الدراسة إلى استكشاف حالة أمن المعلومات والعمل على تحقيق فهم أفضل للحقائق السائدة في هذا المجال داخل المملكة العربية السعودية، واستخدمت الدراسة المنهج الاستقصائي حيث جرى انتقاء مسبق لمجموعة من 280 منظمة سعودية مثلت المساهمين من أربع قطاعات رئيسية، وقام الباحثون بتنظيم ورشة عمل لممثلين عن تلك المنظمات المختلفة، كما أعد الباحثون استبانة تم توزيعها على المشاركين وكانت نسبة الاستجابة 75.5 %، وقد توصلت الدراسة الى مجموعة من النتائج اهمها :-

1) اهمية سياسة أمن المعلومات في ضمان اتخاذ عوامل تحكم مناسبة حيث بينت الدراسة أن أكثر من نصف المنظمات يمتلك سياسة أمن المعلومات وغالبيتها يميل إلى تطبيقها و 89 %يعمد لمراجعة دورية لتلك السياسة.
2) اعتبار التحكم في الوصول الى الشبكة Control Access امرا حاسماً لأمن المعلومات.
3) تتسم معالجة قضايا أمن المعلومات بالتمييز بين حساسية المعلومات.

وقد أوصت الدراسة بأهمية إرساء الوعي الأمني داخل المؤسسات من خلال التدريب المتخصص والمعرفي.

دراسة (العتيبي، 2010) بعنوان الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية.هدفت الدراسة إلى التعرف على مدى توافق الأمن المعلوماتي للمواقع الإلكترونية للأجهزة الأمنية والمدنية في الرياض في المملكة العربية السعودية مع المعايير المحلية والدولية، واستخدمت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة للدراسة وتكون مجتمع الدراسة من جميع العاملين بالمواقع الإلكترونية، وتم أخذ عينة عشوائية طبقية تكونت من 195 وزع منها 111 للأجهزة الامنية و84 للأجهزة المدنية، وقد توصلت الدراسة الى مجموعة من النتائج اهمها :-

1) درجة توافق اجراءات الأمن المعلوماتي وتنظيم الأمن المعلوماتي في المواقع الإلكترونية للقطاع المدني والأمني مع المعايير الأمنية والمدنية متوسطة.
2) درجة توافق تقنيات الأمن المعلوماتي وبيئة الأمن المعلوماتي والأمن المعلوماتي للعنصر البشري في المواقع الإلكترونية للقطاعين مع المعايير الدولية والمحلية مرتفعة.

وقد اوصت الدراسة إلى حاجة الجهات الحكومية لتطبيق جزء لا بأس به من المعيار الدولي لأمن المعلومات وكذلك توحيد الجهات المسئولة عن تطبيق ومتابعة الأمن المعلوماتي الحكومي لتكون عبر هيئة تديرها الحكومة.

دراسة (الصلاح، 2009) مخاطر امن نظم المعلومات المحاسبية الالكترونية واثرها على صحة ومصداقية القوائم المالية في البنوك التجارية الاردنية. هدفت الدراسة إلى التعرف على هذه المخاطر ولتحقيق اهداف الدراسة فقد تم استخدام اسلوب التحليل الوصفي والاستقرائي من خلال جمع المعلومات من الكتب والدوريات والمقالات العربية والاجنبية اضافة الى الدراسة الميدانية المعتمدة على توزيع الاستبانة، وقد تكونت عينة الدراسة من 85 استبانة بواقع 5 استبانات لكل بنك وتم توزيعها على 16 بنك اردني، وكانت نسبة الاستجابة % 92 وبيان مخاطر امن نظم المعلومات المحاسبية الالكترونية رها على صحة ومصداقية القوائم المالية في البنوك التجارية الاردنية. وقد توصلت الدراسة الى النتائج من أهمها :-

1) تتعرض البنوك التجارية الى عدة مخاطر تهدد امن نظم المعلومات المحاسبية الالكترونية لديها.
2) ان الاجراءات الامنية التي تضعها البنوك التجارية الاردنية تحد من مخاطر امن المعلومات المحاسبية الالكترونية.

وقد اوصت الدراسة بضرورة قيام البنوك التجارية بمراقبة مدى تطبيق الضوابط الرقابية التي تضعها للحد من المخاطر التي يتعرض اليها البنك مع تقييم الاجراءات الرقابية ومدى ملائمة هذه الاجراءات للحد من مخاطر امن المعلومات.

دراسة (Zuhairi, 2015)The Risks Facing The Security of Computerized Accounting Information Systems and The Applicable Strategies in Syrian Banks. بعنوان مخاطر امن المعلومات المحاسبية واستراتيجيات مواجهتها في البنوك السعودية. هدفت الدراسة إلى التعرف على المخاطر التي تواجه نظم المعلومات واهم الاسباب التي تؤدي الى حدوثها واستراتيجيات مواجهتها. حيث تم تصميم استبانة وزعت على مجموعة من الموظفين العاملين في المصارف السورية المتواجدة في الساحل السوري، وقد توصلت الدراسة الى النتائج التالية :-

1) توجد اجراءات لمواجهة المخاطر التي تواجه نظم المعلومات.
2) عدم حدوث مخاطر لنظم المعلومات المحاسبية الإلكترونية بشكل متكرر في المصارف السورية.
3) يوجد اجراءات حماية كافية لمواجهة مخاطر أمن نظم المعلومات المحاسبية الإلكترونية.

وقد اوصت الدراسة بضرورة تحري الدقة عند ادخال البيانات من قبل الموظفين وعدم افشاء كلمات المرور.

دراسة (Al Hanini, 2012)The Risks of Using Computerized Accounting Information Systemsin the Jordanian banks -their reasons and ways of prevention. هدفت هذه الدراسة إلى التعرف على مخاطر نظم المعلومات المحاسبية المحوسبة في المصارف الأردنية والأسباب وطرق الوقاية.

ولتحقيق ذلك، تم تصميم استبيان وتوزيعه على عينة الدراسة والتي تكونت من 63 من المشاركين الذين يعملون كمساعدين من المديرين العامين، ومديري الإدارات ومديري الفروع ومساعديهم، والعاملين في المصارف الأردنية. بعد تحليل البيانات باستخدام برنامج SPSS وقد توصلت الدراسة الى النتائج التالية :-

1) من اهم المخاطر التي يواجهها البنك عدم وجود خبرة لدى الموظفين في الحفاظ على أمن المعلومات.
2) من المخاطر التي تهدد أمن نظم المعلومات في البنوك ما يتعلق بإدخال البيانات من قبل الموظفين.
3) هناك مخاطر داخلية تهدد النظام منها الادخال الخاطئ للبيانات.
4) هناك مخاطر خارجية تهدد النظام منها الفيروسات.
5) هناك مخاطر طبيعية وغير طبيعية يقوم بها الموظفين.

وقد اوصت الدراسة بضرورة ان يضع البنك اجراءات رقابية للحد من اثار مخاطر النظم وتحديث وسائل الحماية وفقا للتطور التكنولوجي وعقد دورات للعاملين وتدريبهم على هذه الاجراءات.

دراسة **(Kreicbera, 2010)Internal Threats to Information Security - Countermeasures andHumanFactor within SME**بعنوان التهديدات الداخلية لأمن المعلومات- التدابير المضادة والعنصر البشري.هدفت الدراسة الى التعرّف على دور العنصر البشري في حقل أمن نظم المعلومات وتساءلت حول العوامل التي تؤثر على السلوك الأمني للموظفينوكيف ينظروا تجاه التدابير الأمنية المضادة للتهديدات الداخلية. وقد استخدم المنهج الكيفي (النوعي) وكانت أدواته المقابلات التي اجريت مع مسؤولي أمن المعلومات والمستخدمين بالإضافة لمراجعة وتحليل الوثائق والمستندات، والملاحظة المباشرة لسلوك المستخدمين، وقد توصلت الدراسة الى النتائج التالية :-

1) رضا وقبول الموظفين و التدابير الأمنية عناصر مهمة في تحقيق السلوك الامني تجاه أمن نظم المعلومات.
2) يواجه الموظفون صعوبة ومقدار من التعقيد في فهم الوثائق المتعلقة بالأمن المعلوماتي.
3) تطبيق المتطلبات البشرية لأمن المعلومات يحتاج إلى حالة وعي بأهمية الأمن المعلوماتي.

وقد اوصت الدراسة بأنه لتحسين أمن المعلومات يجب تقييم لسلوك الموظفين تجاه القضايا الأمنية المختلفة، وأن يتم إعلامهم بالمنافع التي ستتحقق من تطبيق التدابير المضادة للحد من المخاطر التي يتعرض اليها نظم المعلومات بالمنظمة.

10 المنهجية والاجراءات.

لغايات تحقيق الاهداف المرجوة من الدراسة فقد تبنت الدراسة منهجية البحث الوصفي، والميداني التحليلي، فعى صعيد البحث الوصفي تم اجراء المسح المكتبي والاطلاع على الدراسات والبحوث النظرية والميدانية في مجال امن المعلومات، لأجل بلورة الاسس والمنطلقات التي يقوم عليها الاطار النظري حيث تم توضيح مفهوم اجراءات الامن المعلوماتي ومخاطر امن المعلومات ومصادرها الداخلية والخارجية والطبيعية وكذلك التهديدات التي تواجه أمنالمعلومات في المنظمة، والوقوف عند اهم الدراسات السابقة التي تُشكل رافدا حيويا في الدراسة وما تتضمنه من محاور معرفية تخدم الدراسة. اما على سعيد البحث الميداني التحليلي، فقد تم اجراء المسح الاستطلاعي لعينة من اعضاء هيئة التدريس في الجامعات السعودية والطلب منهم الاجابة على فقرات الاستبانة المصممة لهذه الدراسة ومن ثم تحليل البيانات المجمّعة من خلال الاستبانات بالطرق الاحصائية المناسبة باستخدام برمجية الرزمة الاحصائية للعلوم الاجتماعية (SPSS). وبعد تحليل البيانات واستخلاص النتائج الاولية تم اختبار فرضيات الدراسة بالطرق الاحصائية المناسبة واستخلاص النتائج.

1.10 مجتمع الدراسة وعينتها.

تكون مجتمع الدراسة من كافة العاملين في ادارة الجامعة ممن يستخدمون النظام ويتعاملون معه يوميا سواء الاداريين او الفنيين، اضافة الى موظفي تكنولوجيا المعلومات في عمادة تقنية المعلومات والدعم الفني وكلية الحاسبات ذات العلاقة.

اما عينة الدراسة فقد تم اختيار عينة عشوائية طبقية تشمل كافة الفئات المشار اليها اعلاه، وذلك من خلال الموقع الالكتروني للجامعة. وقد تم توزيع الاستبانات من خلال البريد الالكتروني وبلغ عدد الاستبانات المرسلة (160) استبانة، استرجع منها (138) استبانة وقد استبعد (9) استبانات لعدم الجدية عند تعبئته

وبذلك يكون عدد الاستبانات الصالحة للتحليل الاحصائي (129) بنسبة بلغت (80.6 %).

2.10 خصائص عينة الدراسة.

يبين الجدول التالي توزيع افراد عينة الدراسة حسب المتغيرات الشخصية والوظيفية.

جدول رقم (1) : التكرار والنسبة المئوية حسب المتغيرات الشخصية والوظيفية (العمر والدور الوظيفي والمؤهل العلمي والرتبة الوظيفية والخبرة الوظيفية والدورات التدريبية في مجال تكنولوجيا المعلومات)

العمر	30 سنة فاقل	31- 40 سنة	41- 50 سنة	51 سنة فأكثر	المجموع
التكرار	19	49	34	27	129
النسبة المئوية %	14.7 %	38.0 %	26.4 %	20.9 %	100 %
المؤهل العلمي	دبلوم متوسط فما دون	بكالوريوس	ماجستير / دبلوم عالي	دكتوراه	
التكرار	9	78	23	19	129
النسبة المئوية %	6.8 %	60.6 %	17.9 %	14.7 %	100 %
طبيعة العمل	اداري	مالي	تكنولوجيا المعلومات	نظم المعلومات	
التكرار	23	32	53	21	129
النسبة المئوية %	17.8 %	24.8 %	41.1 %	16.3 %	100 %
الرتبة الوظيفية	مدير	رئيس قسم	موظف رئيسي	موظف مبتدئ	
التكرار	9	18	73	29	129
النسبة المئوية %	6.8 %	13.9 %	56.7 %	22.6 %	100 %
الخبرة الوظيفية	5 سنوات فاقل	6 - 10 سنوات	11 - 15 سنة	16 سنة فأكثر	
التكرار	13	25	33	58	129
النسبة المئوية %	10.1 %	19.4 %	25.6 %	44.9 %	100 %
الدورات التدريبة في تكنولوجيا المعلومات	لا شيء	ا - 5 دورات	6 - 10 دورات	11 دورة فاكثر	
التكرار	18	29	39	43	129
النسبة المئوية %	13.9 %	22.6 %	30.2 %	33.3 %	100 %

تشير النتائج الواردة في الجدول رقم (1) بان خصائص افراد عينة البحث متقاربة ومتجانسة مع جميع الخصائص الشخصية والوظيفية، حيث تبين بان غالبية الفئة العمرية ممن تقع ضمن الفئة الشابة (31- 40 سنة) بلغت نسبتها % 38 والحاصلة على المؤهل العلمي (البكالوريوس) بنسبة % 60.6 ونجد ان هذه الفئة مؤهلة في تخصص تكنولوجيا المعلومات والمتخصصة في وسائل الحماية لأمن المعلومات والتعامل معه بشكل جيد والحد من المخاطر التي يتعرض لها النظام حيث بلغت % 41.1 وهم الموظفون العاملون كموظفين تنفيذيين بنسبة % 56.7 من افراد عينة الدراسة ولهم خبرة وظيفية اكثر من 16 سنة بنسبة بلغت % 44.9 وهم ممن حضروا دورات تدريبية متخصصه اكثر من 11 دورات في مجال التخصص.

3.10 اداة الدراسة .

اعتمدت الدراسة على الاستبيان بهدف جمع البيانات حيث تم تصميم استبانة لخدمة اغراض الدراسة تكونت من ثلاثة اجزاء على النحو التالي :-

الجزء الاول : تضمن البيانات الشخصية والوظيفية لأفراد عينة الدراسة.

الجزء الثاني :وتكون من ثلاثة ابعاد وهي :-

البعد الاول :منع الاختراق عن طريق الشبكة الحاسوبية Network Hacking(سرقة كلمة السر ومعالجة التعرض للاختراق اثناء محاولة معالجة سابقة

وهجمات حقن قواعد البيانات) الفقرات (1 - 7).

البعدالثاني : منع الاختراق عن طريق الهندسة الاجتماعية Social Engineeringالفقرات (8 - 13).

البعدالثالث : منع الاختراق عن طريق البرمجيات الضارة Malware(حصان طروادة والفيروسات) الفقرات (14 - 19).

الجزء الثالث : مخاطر امن المعلومات (الداخلية والخارجية والطبيعية) الفقرات (20 - 52).

وقد تم تحديد اوزان فقرات الاستبانة ضمن مقياس ليكرت Lickert للخيرات المتعددة الذي يحتسب اوزان تلك الفقرات بطريقة خماسية على النحو التالي الخيار (موافق بشدة) يمثل (5) درجات، الخيار (موافق) يمثل (4) درجات، الخيار(محايد) يمثل (3) درجات، الخيار(غير موافق) يمثل (2) درجات، الخيار (غير موافق بشدة) يمثل (1) درجة واحدة.

10. 4صدق اداة الدراسة وثباتها.

تم اجراء صدق تحكيمي للاستبانة (الصدق الظاهري) Face Validityللتأكد من ان فقرات الاستبانة تقيس بالفعّل متغيرات الدراسة التي حددت لقياسها اثناء مراحل بناء الاستبانة، حيث تم عرضها على عدد من الأساتذة المحكمين لإبداء رايهم فيها، بالإضافة الى توزيع الاستبانة على عينة تجريبية من اعضاء هيئة التدريس بلغ حجمها (20) فردا للتعرّف على مدى وضوح وسهولة الالفاظ المستخدمة ومدى فهمهم للمفاهيم الواردة في هذه الاستبانة ومن ثم القيام بالتعديلات الضرورية.

كما تم استخدام معامل الاتساق الداخلي كرومباخ الفا Cornbach Alpha بهدف التأكد من مدى اتساق اداة القياس وكانت النتائج المعالجة بالحاسوب كما هي واردة في الجدول رقم (2) حيث تشير النتائج الى ان معامل الثبات لجميع الابعاد لا يقل عن % 60 كما ان معامل الثبات لجميع فقرات الاستبانة بلغ % 83.8 وهذا يعني ان اداة الدراسة تتسم بالثبات وصالحة للتحليل الاحصائي والبحث العلمي (Sekaran, 2006).

جدول رقم (2) : نتائج كرومباخ الفا Cornbach Alpha(α)لمتغيرات الدراسة

المتغيرات	المحاور	عدد الفقرات	معامل الثبات Cronbach – Alpha (α)
المتغير المستقل (بأبعاده الثلاث)	**اجراءات الامن المعلوماتي**		
	الاختراق عن طريق الشبكةالحاسوبية	6	83.2 %
	الاختراق عن طريق الهندسة الاجتماعية	6	76.5 %
	الاختراق عن طريق البرمجيات الضارة	6	85.3 %
المتغير التابع (بأبعاده الثلاث)	**مخاطر امن المعلومات**		
	المخاطر الداخلية	16	90.9 %
	المخاطر الخارجية	10	81.6 %
	المخاطر الطبيعية	7	85.3 %
الاستبانة ككل		52	83.8 % %

.5

10 متغيرات الدراسة والتعريفاتالإجرائية.

1.5.10 المتغير المستقل :-اجراءات الامن المعلوماتي Information Security Procedures:-هي الاجراءات التي تعمل على توفير الحماية للمعلومات من المخاطر التي تهددها، ومنع الاعتداء عليها، وذلك من خلال توفير الادوات والوسائل اللازمة لحماية المعلومات من المخاطر الداخلية او الخارجية او الطبيعية والناتجة عن استغلال ثغرات وضعف في النظام (Ravel & Fichadia, 2007) ومنها ما يلي :-

- **اختراق الشبكة الحاسوبيةHacking**:- الوصول غير المصرح به للنظام او للشبكة الحاسوبية بهدف تعديل البيانات والمعلومات أو سرقتها أوتدميرها (Romney & Steinhart, 2012).
- **الهندسة الاجتماعية Social Engineering**:- تحفيز مستخدم الحاسوب على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع معلومات دون إثارة أي شبهة(Romney & Steinbart,). (2012 .
- **البرمجيات الضارة Malware**:- البرامج المتخصصة بتسهيل التسلل إلى النظام أو الشبكة الحاسوبية بهدف تدميره، مثل حصان طروادةTrojan Horsesوالفيروسات Viruses(Romney & Steinhart, 2012).

2.5.10 المتغير التابع :-مخاطر امن المعلومات Risks Information Security:- هي درجة الثقة بالأمن والحماية من المخاطر المحتملة الناتجة عن استغلال ثغرات وضعف في النظام، وهي حالة الخروج عن الوضع المألوف في سير النظام بكافة عناصره ومستلزماته نتيجة حدث غير مشروع من مصادر داخلية او خارجية او طبيعية (البحيصي، 2011) وهي :-

- **المخاطر الداخلية** :- هي المخاطر التي يتعرض الها النظام بشكل غير مصرح، والقيام بعمل ينتهك امن البيانات ومن مخاطر الاختراق الداخلي "الادخال الخاطئ للبيانات بشكل متعمد والادخال والاستخدام والاتلاف الغير متعمد لمعدات النظام واخطاء كتابة البرامج بشكل غير خاطئ وغير مقصود".
- **المخاطر الخارجية** :-هي المخاطر التي يتعرض الها النظام بشكل غير مصرح، والقيام بعمل ينتهك امن البيانات ومن مخاطر الاختراق الخارجي "قيام شخص غير مصرح له باستخدام النظام كالقراصنة بالدخول للنظام مستغلين الثغرات الموجودة فيه والبرامج الخبيثة مثل فيروسات الحاسوب التي تصل الى النظام ومكوناته البرمجية والاصطياد الالكتروني وهو انتهاك امنية النظام من خلال رسائل البريد الالكتروني التي ترسل له بقصد التخريب او سرقة كلمة المرور او زرع برامج التجسس".
- **المخاطر الطبيعية** :-هي المخاطر التي يتعرض الها النظام بشكل طبيعي مثل الكوارث الطبيعية وانقطاع التيار الكهربائي والاعطال الفنية في المعدات المادية والبرمجية والشبكة الحاسوبية، مما تسبب في انتهاك امنية النظام اما ببطء المعالجة او بالتوقف عن العمل.

11 المعالجة الإحصائية.

لغرض الإجابة عن أسئلة الدراسة ولاختبار فرضياتها، فقد اعتمدت الدراسة على الحزمة الإحصائية (*SPSS*) في التحليلمن خلال الأساليب الإحصائية التالية وهي مقاييس الإحصاء الوصفي، ومعامل كورنباخ الفا *Alpha (α)*معادلة الهدف منها التأكد من ثبات فقرات الاستبانة،وتحليل الانحدار المتعدد Multi Regression Analysisلاختبار صلاحية نموذج الدراسة واختبار تأثير كل متغير مستقل وأبعاده على المتغير التابع،واختبار (*F*) للتحقق من معنوية العلاقة بين متغيرات الدراسة.

1.11 نتائج التحليل الاحصائي.

فيما يلي عرض لنتائج التحليل الاحصائي الوصفي للبيانات، وهي قيم المتوسطات الحسابية والانحرافات المعيارية والاهمية الترتيبية لجميع متغيرات الدراسة، والفقرات المكونة لكل متغير، مع الاخذ بعين الاعتبار ان تدرج المقياس المستخدم في الدراسة كان (موافق بشدة) يمثل (5) درجات، الخيار (موافق) يمثل (4) درجات، الخيار(محايد) يمثل (3) درجات، الخيار(غير موافق) يمثل (2) درجات، الخيار (غير موافق بشدة) يمثل (1) درجة واحدة.

واستنادا الى ذلك فان فيم المتوسطات الحسابية التي وصلت اليها الدراسة، سيتم التعامل معها لتفسير البيانات على النحو التالي الفقرات التي تقع ما بين (*1.00 - 2.33*) فذلك يدل على إن مستوى تصورات أفراد عينة الدراسة متدني، أما إذا كانت قيمة المتوسط الحسابي للفقرات تقع ما بين (*2.34 - 3.66*) فذلك يدل على إن تصورات أفراد عينة الدراسة متوسط، بينما إذا كانت قيمة المتوسط الحسابي للفقرات من (*3.67 - 5.00*) فذلك يدل على إن مستوى تصورات أفراد عينة الدراسة مرتفع. وقد كانت نتائج التحليل الاحصائي على النحو التالي :-

المتغير المستقل :- إجراءات الامن المعلوماتي وتم تقسيمة الى محورين وثلاثة ابعاد والموضحة كالتالي :-

أولا :- تقدير افراد عينة الدراسة لإجراءات الامن المعلوماتي لمنع الاختراق عن طريق الشبكة الحاسوبية *NetworkHacking*من خلال (سرقة كلمة السر ومعالجة التعرض للاختراق اثناء محاولة معالجة سابقة وهجمات حقن قواعد البيانات) وتم قياسها من خلال الفقرات (1 - 7) :-

1) توعية مستخدمي النظام بالسياسات المتعلقة بالأمن المعلوماتي المتبعة داخل الجامعة.
2) يوفر النظام الامني الية مناسبة للتوثق من شخصية الداخلين الى النظام والشبكة والمصرح لهم بذلك وتسجيل تصرفاتهم.
3) تحديد صلاحيات مستخدمي النظام كل حسب صلاحياته.
4) يوجد سجل دخول للنظام *Log File*.
5) يوجد قيود للدخول الى النظام والشبكة للأشخاص المصرح لهم بذلك.
6) يتم اختبار النظام والتدقيق عليه بشكل دوري.
7) يتم استخدام برمجيات تُساعد على زيادة ضبط الدخول الى الشبكة مثل الجدار الناري *Firewall*وبرنامج *Proxy*.

جدول رقم (3) : المتوسط الحسابي والانحراف المعياري وقيمة t المحسوبة والأهمية النسبية لتقدير أفراد العينة

رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	قيمة *t* المحسوبة	مستوى التقدير	الترتيب	التكرارات				
						5	4	3	2	1
1	3.62	1.019	6.65	متوسط	5	26	50	28	0	25
2	3.77	1.163	7.49	عالي	1	49	26	26	2	26
3	3.72	1.142	7.02	عالي	3	43	32	27	0	27
4	3.73	1.210	6.84	عالي	2	49	27	27	0	26
5	3.72	1.135	7.06	عالي	4	41	36	26	1	25
6	3.61	1.162	5.91	متوسط	6	36	38	26	3	26
7	3.60	1.155	5.94	متوسط	7	36	37	28	3	25
بشكل عام	3.67	0.329	23.19	عالي						

يتبين من الجدول رقم (3) ان المتوسط العام لتقدير افراد عينة الدراسة لإجراءات الامن المعلوماتي لمنع الاختراق عن طريق الشبكة الحاسوبية *Network Hacking*من خلال (سرقة كلمة السر ومعالجة التعرض للاختراق اثناء محاولة معالجة سابقة وهجمات حقن قواعد البيانات) كان عاليا فقد بلغ المتوسط الحسابي *3.67* والانحراف المعياري *0.329*وقد حققت الفقرة *2*اعلى وسط حسابي قدره *3.77*وبانحراف معياري قدره *1.163* فقد كانت معظم اجابات المبحوثين حول الفقرات المتعلقة بهذا البعد ضمن الموافقة أي ان الجامعة توفر نظام امني مناسب للتوثق من شخصية الداخلين الى النظام والشبكة والمصرح لهم بذلك وتسجيل تصرفاتهم. وللتحقق من دقة تقدير أفراد عينة البحث تم استخدام اختبار *t* ومستوى الدلالة المرافق له حيث تبين بان قيمة *t* المحسوبة*23.19*ومستوى دلالتها (*0.000*) وهو دال إحصائيا عند دلالة ($\alpha \leq 0.05$)مما يشير إلى معنوية التقدير استنادا للوسط الحسابي.

ثانيا :- تقدير افراد عينة الدراسة لإجراءات الامن المعلوماتي لمنع الاختراق عن طريق الهندسة الاجتماعية*SocialEngineering*وتم قياسها من خلال الفقرات (8 - 13) :-

8) تعرضت بطلب مباشرة من قبل شخص قريب او زميل او صديق عن معلومات دخول النظام.
9) تقوم بكتابة معلومات الدخول الى النظام في اماكن يسهل كشفها من قبل الاخرين.

10) تعرضت للابتزاز من شخص معين بتقديم معلومات الدخول الى النظام.

11) تصلك رسائل تحتوي على ملفات مرفقة من مصدر مجهول.

12) تحتوي الرسائل التي تصلك على رابط مزيف لجهة معروفة.

13) تعرض جهازك للعبث من اشخاص ومحاولة فتحه بطريقة غير قانونية.

جدول رقم (4) : المتوسط الحسابي والانحراف المعياري وقيمة t المحسوبة والأهمية النسبية لتقدير أفراد العينة

رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	قيمة *t* المحسوبة	مستوى التقدير	الترتيب	التكرارات				
						5	4	3	2	1
8	*3.72*	*1.104*	*7.42*	عالي	1	40	38	26	0	25
9	*3.56*	*1.205*	*5.26*	متوسط	6	36	36	26	5	26
10	*3.67*	*1.113*	*6.80*	عالي	2	37	39	27	1	25
11	*3.65*	*1.164*	*6.36*	متوسط	4	38	37	26	2	26
12	*3.58*	*1.164*	*5.67*	متوسط	5	36	35	29	3	26
13	*3.65*	*1.130*	*6.55*	متوسط	3	38	36	28	1	26
بشكل عام	*3.64*	*0.524*	**13.84**							

من الجدول رقم (4) ان المتوسط يتبين
العام لتقدير افراد عينة الدراسة

لإجراءات الامن المعلوماتي لمنع الاختراق عن طريق الهندسة الاجتماعية *Social Engineering*كان متوسط فقد بلغ المتوسط الحسابي *3.64* والانحراف المعياري *0.524*وقد حققت الفقرة *8* أعلى وسط حسابي قدره *3.72*وبانحراف معياري قدره *1.104* فقد كانت معظم اجابات المبحوثين حول الفقرات المتعلقة بهذا البعد ضمن الموافقة حيث تبين بان هناك تعرض من قبل مجموعة من الاشخاص بطلب معلومات دخول للنظام.وللتحقق من دقة تقدير أفراد عينة البحث تم استخدام اختبار *t* ومستوى الدلالة له حيث تبين بان قيمة *t* المحسوبة*13.84*ومستوى دلالتها (*0.000*) وهو دال إحصائيا عند دلالة ($\alpha \leq 0.05$)مما يشير إلى معنوية التقدير للوسط الحسابي.

ثالثا :- تقدير افراد عينة الدراسة لإجراءات الامن المعلوماتي لمنع الاختراق عن طريق البرمجيات الضارة*Malware* من خلال (حصان طروادة والفيروسات) وتم قياسها من خلال الفقرات (14 - 19) :-

14) توجد رقابة شديدة تعمل على منع تنزيل الملفات من شبكة الانترنت.

15) توجد برمجيات سرية تعمل على منع التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب.

16) يتم تحديث البرمجيات بشكل دوري ومستمر.

17) تُستخدم البرمجيات التي تُساعد على زيادة الرقابة في الدخول الى الشبكة مثل مقاوم الفيروسات وتحديثها باستمرار.

18) استخدام برمجيات حديثة ومتطورة تُساعد على زيادة الرقابة في الدخول الى النظام.

19) توجد قيود تمنع من استخدام ذواكر *UBS* والاقراص المدمجة *CD*.

جدول رقم (5) : المتوسط الحسابي والانحراف المعياري وقيمة t المحسوبة والأهمية النسبية لتقدير أفراد العينة

رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	قيمة *t* المحسوبة	مستوى التقدير	الترتيب	التكرارات				
						5	4	3	2	1
14	*3.69*	*1.110*	*7.06*	عالي	1	39	37	27	0	26
15	*3.65*	*1.101*	*6.71*	متوسط	2	37	36	30	5	26
16	*3.60*	*1.156*	*5.87*	متوسط	5	36	36	29	3	25
17	*3.58*	*1.102*	*5.99*	متوسط	6	31	42	29	2	25
18	*3.63*	*1.104*	*6.46*	متوسط	4	34	41	27	1	26
19	*3.64*	*1.117*	*6.54*	متوسط	3	36	39	27	1	26

بشكل عام	3.63	0.612	11.73	متوسط		

يتبين من الجدول رقم (5)

ان المتوسط العام لتقدير افراد عينة الدراسة لإجراءات الامن المعلوماتي لمنع الاختراق عن طريق البرمجيات الضارة Malwareمن خلال (حصان طروادة والفيروسات) كان عاليا فقد بلغ المتوسط الحسابي *3.63* والانحراف المعياري *0.612*وقد حققت الفقرة *14* أعلى وسط حسابي قدره *3.69*وبانحراف معياري قدره *1.110* فقد كانت معظم اجابات المبحوثين حول الفقرات المتعلقة بهذا البعد ضمن الموافقة أي ان الجامعة توفر رقابة شديدة تعمل على منع تنزيل الملفات من شبكة الانترنت. وللتحقق من دقة تقدير أفراد عينة البحث تم استخدام اختبار *t* ومستوى الدلالة المرافق له حيث تبين بان قيمة *t* المحسوبة*11.73*ومستوى دلالتها (*0.000*) وهو دال إحصائيا عند دلالة ($\alpha \leq 0.05$) مما يشير إلى معنوية التقدير استنادا للوسط الحسابي.

المتغير التابع : المتغير المستقل :- مخاطر امن المعلومات وتم تقسيمة الى ثلاثة ابعاد والموضحة كالتالي :-

اولا : المخاطر الداخلية التي يتعرض الها امن المعلومات وتم قياسها من خلال الفقرات (20 - 35) :-

20) تم اختراق النظام من قبل احد مستخدمي النظام مما تسبب فيتوقف النظام عن العمل لفترة ما.

21) تم اختراق النظام من قبل احد مستخدمي النظام مما تسبب في بطيء عمل النظام.

22) تم اختراق النظام من قبل احد مستخدمي النظام مما تسبب في الحصول على مخرجات غير صحيحة.

23) تم اختراق النظام من قبل احد مستخدمي النظام مما تسبب في تخريب البيانات المخزنة.

24) الادخال الخاطئ بشكل متعمد للبيانات الى النظام ادى الى الحصول على مخرجات غير صحيحة.

25) الادخال الخاطئ غير المتعمد للبيانات الى النظام ادى الى توقف النظام عن العمل لفترة ما.

26) الادخال الخاطئ غير المتعمد للبيانات الى النظام ادى الى على مخرجات غير صحيحة.

27) الادخال الخاطئ غير المتعمد للبيانات يتيح مخرجات غير صحيحة.

28) الاستخدام الخاطئ غير المتعمد للنظام يتسبب في توقف العمل بالنظام لفترة ما.

29) الاستخدام الخاطئ المتعمد للنظام تسبب في تخريب البيانات المخزن.

30) الاتلاف غير المتعمد لمعدات النظام يتسبب في توقف عمل النظام لفترة ما.

31) الاتلاف غير المتعمد لمعدات النظام يتسبب في تخريب البيانات المخزنة.

32) حدوث اخطاء في التصميم البرمجي للنظام ادى البطيء عمل النظام.

33) حدوث اخطاء في التصميم البرمجي للنظام ادى الى الحصول على مخرجات غير صحيحة.

34) حدوث اخطاء في التصميم البرمجي للنظام ادى الى توقف النظام عن العمل لفترة ما.

35) حدوث اخطاء في التصميم البرمجي للنظام ادى التخريب البيانات المخزنة.

جدول رقم (6) : المتوسط الحسابي والانحراف المعياري وقيمة t المحسوبة والأهمية النسبية لتقدير أفراد العينة

فقرات المخاطر	رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	قيمة*t* المحسوبة	مستوى التقدير	التكرارات				
						5	4	3	2	1
الاختراق الداخلي	20	3.11	1.376	0.89	متوسط	26	30	26	21	26
	21	3.15	1.381	1.21	متوسط	28	29	26	20	26
	22	3.09	1.366	0.78	متوسط	25	30	27	21	26
	23	3.11	1.376	0.89	متوسط	26	30	26	21	26
بشكل عام	20 - 23	3.12	1.364	0.94	متوسط					
الادخال الخاطئ المتعمد	24	3.23	1.343	1.97	متوسط	28	33	26	17	25
بشكل عام	24	3.23	1.343	1.97	متوسط					

الادخال الخاطئ غير المتعمد	25	3.22	1.334	1.85	متوسط	27	33	27	17	25
	26	3.20	1.337	1.71	متوسط	27	32	27	17	26
بشكل عام	26 - 25	3.21	1.353	1.78	متوسط					
الاستخدام الخاطئ غير المتعمد	27	3.20	1.348	1.69	متوسط	27	33	26	18	25
	28	3.19	1.351	1.56	متوسط	27	32	26	18	26
	29	3.17	1.353	1.43	متوسط	27	31	26	18	27
بشكل عام	29 - 27	3.19	1.351	1.45	متوسط					
الاتلاف غير المتعمد لمعدات النظام	30	3.18	1.349	1.50	متوسط	27	31	27	18	26
	31	3.19	1.333	1.59	متوسط	27	30	29	17	26
بشكل عام	31 - 30	3.19	1.341	1.55	متوسط					
اخطاء البرنامج	32	3.26	1.365	2.13	متوسط	31	30	26	17	25
	33	3.23	1.349	1.96	متوسط	29	31	27	17	25
	34	3.21	1.339	1.78	متوسط	29	28	29	16	27
	35	3.21	1.339	1.78	متوسط	27	33	27	17	26
بشكل عام		3.23	1.318	1.912	متوسط					
المخاطر الداخلية ككل	بشكل عام	3.18	0.878	2.38	متوسط					

يبين الجدول رقم (6) المتوسط الحسابي والانحراف المعياري ومستوى التقدير والتكرارات لتقدير أفراد العينة للمخاطر الداخلية والفقرات التي تقيسها، فقد تبين أن المتوسط العام لتقدير أفراد العينة للمخاطر الداخلية كان متوسط، فقد كانت معظم إجابات المبحوثين حول الفقرات المتعلقة بهذه المخاطر ضمن الموافقة بشكل يحد من مخاطر امن المعلومات، كما تبين أن أكثر المخاطر تكراراً هما الادخال الخاطئ غير المتعمد والاستخدام الخاطئ غير المتعمد والاتلاف غير المتعمد، بينما كان خطر الإدخال الخاطئ المتعمد واخطاء البرنامج أقل هذه المخاطر حدوثاً.وهذا يعني أن المخاطر الداخلية ضمن المستوى المقبول، وأن وسائل الحماية المتبعة مناسبة إلى حد ما، لكن يتطلب الأمر المزيد من الرقابة من قبل مدير النظام على اجراءات الامن المعلوماتي، وكذلك التحقق من سلامة التعليمات البرمجية من حين لآخر.

ثانيا : المخاطر الخارجية التي يتعرض اليها امن المعلومات وتم قياسها من خلال الفقرات (36 - 45):-

36) تم اختراق النظام من قبل القراصنة مما تسبب في توقف النظام عن العمل.

37) تم اختراق النظام من قبل القراصنة مما تسبب في بطء عمل النظام.

38) تم اختراق النظام من قبل القراصنة مما تسبب في الحصول على مخرجات غير صحيحة.

39) تم اختراق النظام من قبل القراصنة مما تسبب في تخريب البيانات المخزنة.

40) توقف النظام عن العمل لفترة ما بسبب تعرضه لهجوم من البرامج الخبيثة (الفيروسات وأشباهها).

41) تعرض النظام لهجوم من البرامج الخبيثة (الفيروسات وأشباهها) مما تسبب في بطء العمل في النظام.

42) تعرض النظام لهجوم من البرامج الخبيثة (الفيروسات) مما تسبب في تعذر الحصول على المخرجات الملائمة لمتخذ القرار.

43) تعرض النظام لهجوم من البرامج الخبيثة (الفيروسات وأشباهها) مما تسبب في تخريب البيانات المخزنة.

44) تعرض النظام لهجوم من رسائل البريد الالكتروني مما تسبب في توقف العمل في النظام لفترة ما.

45) تعرض النظام لهجوم من رسائل البريد الالكتروني مما تسبب في تخريب البيانات المخزنة.

جدول رقم (7) : المتوسط الحسابي والانحراف المعياري وقيمة t المحسوبة والأهمية النسبية لتقدير أفراد العينة

فقرات المخاطر	رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	قيمة t المحسوبة	مستوى التقدير	التكرارات				
						5	4	3	2	1
الاختراق الخارجي	36	3.22	1.346	1.83	متوسط	28	32	26	17	26

	37	3.24	1.368	1.99	متوسط	31	29	26	17	26
	38	3.22	1.352	1.82	متوسط	29	30	27	17	26
	39	3.26	1.355	2.21	متوسط	31	30	26	16	26
بشكل عام	39 - 36	3.24	1.355	1.96	متوسط					
البرامج الخبيثة	40	3.25	1.358	2.08	متوسط	30	31	26	17	25
	41	3.26	1.355	2.21	متوسط	31	30	26	16	26
	42	3.25	1.358	2.08	متوسط	31	29	26	16	27
	43	3.19	1.392	1.58	متوسط	31	27	26	19	26
بشكل عام	43 - 40	3.24	1.366	1.99	متوسط					
الاصطياد الالكتروني	44	3.21	1.373	1.73	متوسط	30	29	26	18	26
	45	3.26	1.348	2.16	متوسط	30	31	26	16	26
بشكل عام	45 - 44	3.24	1.361	1.95	متوسط					
المخاطر الخارجية ككل	بشكل عام	3.26	1.348	2.16	متوسط					

يبين الجدول رقم (7) المتوسط الحسابي والانحراف المعياري ومستوى التقدير والتكرارات لتقدير أفراد العينة للمخاطر الخارجية والفقرات التي تقيسها، فقد تبين أن المتوسط العام لتقدير أفراد العينة للمخاطر الداخلية كان متوسط، فقد كانت معظم إجابات المبحوثين حول الفقرات المتعلقة بهذه المخاطر ضمن الموافقة والموافقة بشدة بشكل يحد من مخاطر امن المعلومات، كما تبين أن أكثر المخاطر تكراراً هما الاستخدام الخاطئ غير المتعمد وأخطاء البرامج، بينما كان خطر الإدخال الخاطئ المتعمد أقل هذه المخاطر حدوثاً.وهذا يعني أن المخاطر الداخلية ضمن المستوى المقبول، وأن وسائل الحماية المتبعة مناسبة إلى حد ما، لكن يتطلب الأمر المزيد من الرقابة من قبل مدير النظام على اجراءات الامن المعلوماتي، وكذلك التحقق من سلامة التعليمات البرمجية من حين لآخر.

ثالثا : المخاطر الطبيعية التي يتعرض اليها امن المعلومات وتم قياسها من خلال الفقرات (46 - 52):-

46) فقدان البيانات بسبب كوارث طبيعية.

47) توقف العمل بالنظام لفترة ما نتيجة كوارث طبيعية.

48) فقدان البيانات بسبب الانقطاع المفاجئ للتيار الكهربائي.

49) توقف العمل بالنظام لفترة ما نتيجة انقطاع التيار الكهربائي لسبب خارج المديرية.

50) توقف العمل بالنظام لفترة ما نتيجة الأعطال الفنية التي تحدث في النظام بشكل اعتيادي.

51) الحصول على مخرجات غير صحيحة من النظام بسبب الأعطال الفنية.

52) فقدان البيانات بسبب أعطال فنية تحدث للنظام.

جدول رقم (8) : المتوسط الحسابي والانحراف المعياري وقيمة t المحسوبة والأهمية النسبية لتقدير أفراد العينة

فقرات المخاطر	رقم الفقرة	المتوسط الحسابي	الانحراف المعياري	قيمة t المحسوبة	مستوى التقدير	التكرارات				
						5	4	3	2	1
الكوارث الطبيعية	46	3.19	1.364	1.64	متوسط	29	29	27	18	26
	47	3.28	1.352	2.34	متوسط	31	31	26	16	25
بشكل عام	47 - 46	3.24	1.358	1.99	متوسط					
انقطاع التيار الكهربائي	48	3.24	1.351	2.02	متوسط	29	32	26	17	25
	49	3.28	1.352	3.34	متوسط	31	31	26	16	25
بشكل عام	49 - 48	3.26	1.352	2.18	متوسط					
الاعطال الفنية	50	3.22	1.371	1.86	متوسط	31	28	26	17	27
	51	3.20	1.366	1.68	متوسط	29	30	26	18	26
	52	3.23	1.361	1.94	متوسط	30	30	26	17	26
بشكل عام	52 - 50	3.15	1.366	1.83	متوسط					
المخاطر الطبيعية ككل	بشكل عام	3.23	0.863	3.10	متوسط					

يبين الجدول رقم (8) المتوسط الحسابي والانحراف المعياري ومستوى التقدير والتكرارات لتقدير أفراد العينة للمخاطر الطبيعية والفقرات التي تقيسها، فقد تبين أن المتوسط العام لتقدير أفراد العينة للمخاطر الداخلية كان متوسط، فقد كانت معظم إجابات المبحوثين حول الفقرات المتعلقة بهذه المخاطر ضمن الموافقة والموافقة بشدة بشكل يحد من مخاطر امن المعلومات، كما تبين أن أكثر المخاطر تكراراً هما الاستخدام الخاطئ غير المتعمد وأخطاء البرامج، بينما كان خطر الإدخال الخاطئ المتعمد أقل هذه المخاطر حدوثاً.وهذا يعني أن المخاطر الداخلية ضمن المستوى المقبول، وأن وسائل الحماية المتبعة مناسبة إلى حد ما، لكن يتطلب الأمر المزيد من الرقابة من قبل مدير النظام على اجراءات الامن المعلوماتي، وكذلك التحقق من سلامة التعليمات البرمجية من حين لآخر.

2.11 اختبار الفرضيات.

1.2.11 الفرضية الرئيسية الأولى.

تُساهم اجراءات الامن المعلوماتي (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الداخلية.

جدول رقم (9) : نتائج اختبار تحليل الانحدار البسيط لتأثير اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات الداخلية

Dependent Variable المتغير التابع	R معامل الارتباط	R Square معامل التحديد	F قيمة المحسوبة	Df درجات الحرية		Sig.* مستوى الدلالة	Decision القرار
مخاطر امن المعلومات الداخلية	0.661[a]	0.437	32.386	3	الانحدار	قبول الفرضية	قبول الفرضية
				125	البواقي		
				128	المجموع		

a. Predictors: (Constant) :- منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة

*الارتباط ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)

القوة التفسيرية للنموذج :-

اظهرت نتائج التحليل الاحصائي وجود اثر ذو دلالة احصائية لأبعاد المتغير المستقل (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الداخلية. اذ بلغ معامل الارتباط البسيط R = 0.661 عند مستوى دلالة($\alpha \leq 0.05$) ومعامل التحديد $R^2 = 0.437$ أي ان ابعاد المتغير المستقل استطاعت ان تفسر % 43.7 من التغير الحاصل في مخاطر امن المعلومات الداخلية والباقي يرجع الى عوامل اخرى من منها الخطأ العشوائي. كما بلغت قيمة P = Value للإحصائي F(0.000) مما يشير الى وجود اثر ذو دلالة احصائية لأبعاد المتغير المستقل ككل على بعد المتغير التابع مخاطر امن المعلومات الداخلية وان النموذج صالح للاختبار.

جدول رقم (10) : يبين قيم T وقيم β وقيم .sig لتأثير اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات الداخلية

Model	Standardized Coefficients	t	Sig.
	Beta β		
Constant	1.047	1.312	0.192
اجراءات منع الاختراق عن طريق الشبكة الحاسوبية	0.113	2.071	0.049
اجراءات منع الاختراق عن طريق الهندسة الاجتماعية	0.515	3.938	0.000
اجراءات منع الاختراق عن طريق البرمجيات الضارة	0.663	5.954	0.000

a. Dependent Variable :- مخاطر امن المعلومات الداخلية

المعنوية الكلية للنموذج :-

وللتعرف على معنوية معاملات الانحدار المعنوية سوف نستخدم قيمة P = Value للإحصائي T حيث تشير البيانات الواردة في الجدول السابق ان جميع ابعاد المتغير المستقل تؤثر بشكل معنوي في بعد المتغير التابع مخاطر امن المعلومات الداخلية بالاستناد الى قيمة T ومستوى دلالتها وهي دالة احصائيا عند مستوى ($\alpha \leq 0.05$).

كما بلغت درجة التأثير لإجراءات منع الاختراق عن طريق البرمجيات الضارة $\beta = 0.663$ يليه إجراءات منع الاختراق عن طريق الهندسة الاجتماعية اذ بلغت قيمة التأثير $\beta = 0.515$ يليه اجراءات منع الاختراق عن طريق الشبكة الحاسوبية حيث بلغت قيمة التأثير $\beta = 0.113$ وهذا يعني ان الزيادة بدرجة واحدة في مستوى الاهتمام بإجراءات الامن المعلوماتي يؤدي الى زيادة في الحد من مخاطر امن المعلومات الداخلية بقيمة (66.3 %, 51.5 %, 11.3 %) على التوالي.

وان قيمsig. بلغت على التوالي (0.000, 0.000, 0.049) ويؤكد معنوية هذا التأثير قيمة F المحسوبة والتي بلغت 32.386 وهي دالة احصائيا عند مستوى ($\alpha \leq 0.05$) وهذا يؤكد عدم صحة الفرضية الرئيسية الاولى.

القرار:- قبول الفرضية بصورتها الحالية.

2.2.11 الفرضية الرئيسية الثانية.

تُساهم اجراءات الامن المعلوماتي (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الخارجية.

جدول رقم (11) : نتائج اختبار تحليل الانحدار البسيط لتأثير اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات الخارجية

Dependent Variable المتغير التابع	R معامل الارتباط	R Square معامل التحديد	F قيمة المحسوبة	df درجات الحرية		*Sig. مستوى الدلالة	Decision القرار
مخاطر امن المعلومات الخارجية	0.596[a]	0.355	22.934	3	الانحدار	قبول الفرضية	قبول الفرضية
				125	البواقي		
				128	المجموع		

a. Predictors: (Constant) :- منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة

*الارتباط ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)

القوة التفسيرية للنموذج :-

اظهرت نتائج التحليل الاحصائي وجود اثر ذو دلالة احصائية لأبعاد المتغير المستقل (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الخارجية. اذ بلغ معامل الارتباط البسيط R = 0.596 عند مستوى دلالة($\alpha \leq 0.05$) ومعامل التحديد $R^2 = 0.355$ أي ان ابعاد المتغير المستقل استطاعت ان تفسر 35.5 % من التغير الحاصل في مخاطر امن المعلومات الخارجية والباقي يرجع الى عوامل اخرى من منها الخطأ العشوائي. كما بلغت قيمة P = Value للإحصائي F(0.000) مما يشير الى وجود اثر ذو دلالة احصائية لأبعاد المتغير المستقل ككل على بعد المتغير التابع مخاطر امن المعلومات الداخلية وان النموذج صالح للاختبار.

جدول رقم (12) : يبين قيم T وقيم β وقيم sig. لتأثير اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات الخارجية

Model	Standardized Coefficients Beta β	t	Sig.
Constant	0.425	0.565	0.573
منع الاختراق عن طريق الشبكة الحاسوبية	0.349	2.279	0.038
منع الاختراق عن طريق الهندسة الاجتماعية	0.549	4.464	0.000
منع الاختراق عن طريق البرمجيات الضارة	0.408	3.897	0.000

a. Dependent Variable :- مخاطر امن المعلومات الخارجية

المعنوية الكلية للنموذج :-

وللتعرف على معنوية معاملات الانحدار المعنوية سوف نستخدم قيمة P = Value للإحصائي T حيث تشير البيانات الواردة في الجدول السابق ان جميع ابعاد المتغير المستقل تؤثر بشكل معنوي في بعد المتغير التابع مخاطر امن المعلومات الخارجية بالاستناد الى قيمة T ومستوى دلالتها وهي دالة احصائيا عند مستوى ($\alpha \leq 0.05$).

كما بلغت درجة التأثير لإجراءات منع الاختراق عن طريق الهندسة الاجتماعية $\beta = 0.549$ يليه إجراءات منع الاختراق عن طريق البرمجيات الضارة اذ بلغت قيمة التأثير $\beta = 0.408$ يليه اجراءات منع الاختراق عن طريق الشبكة الحاسوبية حيث بلغت قيمة التأثير $\beta = 0.349$ وهذا يعني ان الزيادة بدرجة واحدة في مستوى الاهتمام بإجراءات الامن المعلوماتي يؤدي الى زيادة في الحد من مخاطر امن المعلومات الداخلية بقيمة (54.9 %, 40.8 %, 34.9 % على التوالي).

وان قيمsig بلغت على التوالي (0.000, 0.000, 0.038) ويؤكد معنوية هذا التأثير قيمة F المحسوبة والتي بلغت 22.934 وهي دالة احصائيا عند مستوى ($\alpha \leq 0.05$) وهذا يؤكد عدم صحة الفرضية الرئيسية الثانية.

القرار:- قبول الفرضية بصورتها الحالية.

3.2.11 الفرضية الرئيسية الثالثة.

تُساهم اجراءات الامن المعلوماتي (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الطبيعية.

جدول رقم (13) : نتائج اختبار تحليل الانحدار البسيط لتأثير اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات الطبيعية

Dependent Variable المتغير التابع	R معامل الارتباط	R Square معامل التحديد	F قيمة المحسوبة	df درجات الحرية		*Sig. مستوى الدلالة	Decision القرار
مخاطر امن المعلومات الطبيعية	0639[a]	0.408	28.697	3	الانحدار	0.000[b]	قبول الفرضية
				125	البواقي		
				128	المجموع		

a. Predictors: (Constant) :- منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة

*الارتباط ذو دلالة إحصائية عند مستوى ($\alpha \leq 0.05$)

القوة التفسيرية للنموذج :-

اظهرت نتائج التحليل الاحصائي وجود اثر ذو دلالة احصائية لأبعاد المتغير المستقل (منع الاختراق عن طريق الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة) في الحد من مخاطر امن المعلومات الطبيعية. اذ بلغ معامل الارتباط البسيط R = 0.639 عند مستوى دلالة($\alpha \leq 0.05$) ومعامل التحديد $R^2 = 0.408$ أي ان ابعاد المتغير المستقل استطاعت ان تفسر % 40.8 من التغير الحاصل في مخاطر امن المعلومات الطبيعية والباقي يرجع الى عوامل اخرى من منها الخطأ العشوائي. كما بلغت قيمة P = Value للإحصائي F(0.000) مما يشير الى وجود اثر ذو دلالة احصائية لأبعاد المتغير المستقل ككل على بعد المتغير التابع مخاطر امن المعلومات الطبيعية وان النموذج صالح للاختبار.

جدول رقم (14) : يبين قيم T وقيم β وقيم .sig لتأثير اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات الداخلية

Model	Standardized Coefficients Beta β	t	Sig.
Constant	1.185	1.473	0.143
منع الاختراق عن طريق الشبكة الحاسوبية	0.491	2.488	0.026
منع الاختراق عن طريق الهندسة الاجتماعية	0.519	3.938	0.000
منع الاختراق عن طريق البرمجيات الضارة	0.605	5.392	0.000

a. Dependent Variable :- مخاطر امن المعلومات الطبيعية

المعنوية الكلية للنموذج :-

وللتعرف على معنوية معاملات الانحدار المعنوية سوف نستخدم قيمة P = Value للإحصائي T حيث تشير البيانات الواردة في الجدول السابق ان جميع ابعاد المتغير المستقل تؤثر بشكل معنوي في بعد المتغير التابع مخاطر امن المعلومات الطبيعية بالاستناد الى قيمة T ومستوى دلالتها وهي دالة احصائيا عند مستوى ($\alpha \leq 0.05$).

كما بلغت درجة التأثير لإجراءات منع الاختراق عن طريق البرمجيات الضارة $\beta = 0.605$ يليه إجراءات منع الاختراق عن طريق الهندسة الاجتماعية اذ بلغت قيمة التأثير $\beta = 0.519$ يليه اجراءات منع الاختراق عن طريق الشبكة الحاسوبية حيث بلغت قيمة التأثير $\beta = 0.491$ وهذا يعني ان الزيادة بدرجة واحدة في مستوى الاهتمام بإجراءات الامن المعلوماتي يؤدي الى زيادة في الحد من مخاطر امن المعلومات الداخلية بقيمة (60.5 %, 51.9 %, 49.1 %) على التوالي.

وان قيم sig. بلغت على التوالي (0.026, 0.000, 0.000) ويؤكد معنوية هذا التأثير قيمة F المحسوبة والتي بلغت 28.697 وهي دالة احصائيا عند مستوى ($\alpha \leq 0.05$) وهذا يؤكد عدم صحة الفرضية الرئيسية الثالثة.

القرار:- قبول الفرضية بصورتها الحالية.

12 النتائج.

توصلت الدراسة الى النتائج التالية :-

1) كانت الاجراءات الامنية في الحد من المخاطر التي يتعرض اليها نظم المعلومات في الجامعة عالية.
2) ان الاجراءات الامنية لمنع الاختراق عن طريق الشبكة الحاسوبية Network Hacking جاءت بمستوى مرتفع وبمتوسط حسابي قدره 3.67
3) ان الاجراءات الامنية لمنع الاختراق عن طريق الهندسة الاجتماعية Social Engineering جاءت بمستوى متوسط وبمتوسط حسابي قدره 3.64
4) ان الاجراءات الامنية لمنع الاختراق عن طريق البرمجيات الضارة Malware جاءت بمستوى متوسط وبمتوسط حسابي قدره 3.63
5) تم التحقق من دقة تقدير افراد عينة الدراسة باستخدام اختبار t ومستوى دلالتها وتبين بانها دال احصائيا مما يشير الى معنوية التقدير.
6) تُساهم اجراءات الامن المعلوماتي في الحد من (المخاطر الداخلية والخارجية والطبيعية التي يتعرض لها النظام.

13التوصيات.

توصي الدراسة بما يلي :-

1) ضرورة قيام ادارة الجامعة بوضع تصنيفات للمعلومات بالطريقة التي تناسب اعمالها وسرية معلوماتها مع عزل البيانات والمعلومات التي يشكل عرضها للعامة ضرر للنظام.
2) تحسين اليات ضبط الوصول للنظام ووضع برامج واجراءات خاصة بالمستويات الادارية والصلاحيات ضمن النظام والتركيز على ضرورات امن المعلومات ومرتكزاته (التوفر والسلامة والسرية).
3) زيادة الموازنات المالية المخصصة لعمليات امن المعلومات في الجامعة.
4) ضرورة توفر التدريب والتوعية للعاملين بأهمية الاصول المعلوماتية للنظام واساليب المحافظة عليها مع التركيز على العاملين الاقل خبرة حسب نتائج الدراسة.
5) وضع خطة استراتيجية لإدارة المخاطر الامنية لنظم المعلومات، بحيث تضمن الاكتشاف المبكر للمخاطر ووضع العلاج الوقائي اللازم.
6) تقييم المخاطر التي يتعرض اليها النظام بشكل دوري للوقوف على ما يُمكن عمله وايجاد السبل الكفيلة باستعادة العمل، ووضع خطط الطوارئ اللازمة لضمان امن النظام في الجامعة.

14 قائمة المراجع.

1) عبد الكريم، نهاد : امن وسرية المعلومات واثرها على الاداء التنافسي دراسة تطبيقية في شركتي التامين العراقية العامة والحمراء للتامين الاهلية. مجلة دراسات محاسبية ومالية، مج (8)، ع (23)، 2013.

2) السالمي، علاء عبد الرازق : تقنيات المعلومات الادارية. ط1، داروائل للنشر، عمان، 2001.

3) البحيصي، عصام الشريف، حرية : مخاطر نظم المعلومات المحاسبية الإلكترونية :دراسة تطبيقية على المصارف العاملة في قطاع غزة.، مجلة الجامعة الإسلامية، سلسلة الدراسات الإنسانية، 2011.

4) الهادي، محمد محمود : توجهات وامن وشفافية امن المعلومات في ظل الحكومة الالكترونية. الدورية الالكترونية لمنظمة البوابة العربية للمكتبات والمعلومات Cybrarians Journalhttp://journal.cybrarans.org 2006.

5) ابو حجر، سامح رفعت، عابدين، امينة : دور اليات حوكمة تكنولوجيا المعلومات في تخفيض مخاطر امن المعلومات في الوحدات الحكومية في ظل الحكومة الالكترونية. بحث مقدم للمؤتمر السنوي الخامس، جامعة القاهرة، 2014.

6) الدنف،ايمن محمد : واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها. رسالة ماجستير منشورة، الجامعة الاسلامية، غزة، 2013.

7) عواد، ناريمان طعمه : مدى فعالية إجراءات نظام الرقابة الداخلية في ظل نظم المعلومات الإلكترونية - دراسة تطبيقية على البنوك العاملة في قطاع غزة. رسالة ماجستير منشوره، الجامعة الاسلامية، قطاع غزة، 2012.

8) عرفان،سيد نبي، عبد الرحمن مارزا، خالد، الغثبر :امن المعلومات في المنظمات السعودية. جامعة الملك سعود، مركز التميز لأمن المعلومات، 2010.

9) العتيبي، عمار محمد :الأمن المعلوماتي في المواقع الإلكترونية ومدى توافقه مع المعايير المحلية والدولية. رسالة دكتوراه غير منشورة، الرياض، جامعة نايف العربية للعلوم الامنية، 2010.

10) الصلاح، عماد : مخاطر امن نظم المعلومات المحاسبية الالكترونية واثرها على صحة ومصداقية القوائم المالية في البنوك التجارية الاردنية. رسالة ماجستير منشورة، الجامعة الاردنية، عمان، 2009.

11) Porter, B., Simon, J &Hathrly, D, (2008) : Principles of External Auditing, 3rd. edition, England.

12) Raval, V & Fichadia, A, (2007) : Risk, Controls, and Security : Concepts, Applications, England: John Wiley and Sons.

13) Merkow B. and James, (2005) : Information Security : Principles and Practices, Prentice Hall .

14) Anton, R., Mesic, R, M (2003) : Finding and Fixing Vulnerabilities in Information Systems :The Vulnerabilities Assessment and Mitigation Methodology. Prepared for the Defense Advanced Research Projects Agency; National Defense Research Institute .

15) Schechter, S.(2004) : Computer Security Strength & Risk : A Quantitative Approach. PhD. dissertation, Computer Science, Cambridge: Harvard University.

16) Marianne, S. (2009) : Security According to Buzan : A Comprehensive Security Analysis, security discussion. papers series 1. http://geest.msh-paris.

17) Noordegraff, A. (2002) : How Hackers Do it : Tricks ,Tools , and Techniques. U.S.A,CA : sun Microsystems ,INC.

18) Warkentin, and Willison, R.(2009) : Behavioral and policy issues in information systems security , the insider threat. European Journal of Information Systems.

19) Goodhue, D. and Straub, D.,(2001) : Security concerns of system users - A study of perceptions of the adequacy of security measures". Information and Management.

20) Heiser, G.(2013) : Protecting e-Government Against Attacks. In : Proceedings of Security of e - Government Systems Conference. 19 February.

21) Kissel, R. (2013) : Glossary of Key Information Security Terms. NISTIR 7298 Revision 2, : National Institute of Standards and Technology (NIST).

22) Litan, A(2004) : Phishing Attack Victims Likely Targets for Identity Theft. Gartner Research, Gartner, Inc. | FT-22-8873. USA

23) Romney, M. & Steinbart, P, (2012) : Accounting Information Systems", 12th. edition, England : Pearson Education.

24) Zuhairi, M., f., (2015) : The Risks Facing The Security of Computerized Accounting Information Systems - A descriptive Study in Syrian Banks. master degree in Accounting.

25) Al Hanini, E., (2012) : The Risks of Using Computerized Accounting Information Systems in the Jordanian banks -their reasons and ways of prevention. European Journal of Business and Management www.iiste.org. Vol . 4, No.20.

26) Kreicbera, Liene (2010) : Internal Threat Information Security – Countermeasures and human factor within SME, Master Thesis, Sweden : Luela University Of Technology.

27) Sekaran, U., (2006) : Research Methods for Business : A Skill Building Approach, 4th. Ed, Singapore : John Wily and Sons, (Asia) pte, Ltd.