معلومات البحث
أستلم: 1-2-2019
المراجعة: 1-3-2019
النشر: 1-4-2019

طبيعة المخاطر التي تهدد امن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الأردن

د. عدنان عواد الشوابكة

جامعة الطائف – قسم نُظم المعلومات الإدارية – كلية إدارة الاعمال

المملكة العربية السعودية

Printed ISSN: 2314-7113

Online ISSN: 5809-2289

الملخص

تهدف هذه الدراسة إلى التعرّف على طبيعة المخاطر التي تهدد امن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن. حيث طبقت الدراسة على عينة عشوائية من مستخدمي النظام بلغ حجمها (58) موظفا من مستخدمي النظام ولتحقيق أغراض الدراسة استخدمت الملاحظة المباشرة والاستبانة لجمع البيانات من مستخدمي النظام. وقد تم استخدام الإحصاءات الوصفية، واختبار (T) للعينة الواحدة في تحليل البيانات واختبار فرضيات الدراسة. وقد توصلت الدراسة إلى العديد من النتائج وأبرزها أن مستوى تكرار منخفض للمخاطر المحتملة، وكذلك أكثر المخاطر تكرارا هي المخاطر الطبيعية مثل (انقطاع التيار الكهربائي عن النظام والأعطال الفنية)، وحيث انها لم تتسبب المخاطر الأمنية التي تهدد النظام في إعاقة أداء نظام المعلومات، وتشير أيضا نتائج الدارسة أن المستوى الأمني للنظام مقبولاً.

وقد اوصت الدراسة بضرورة تحسين وسائل الحماية المستخدمة خصوصاً وسائل إدامة التيار الكهربائي وتحديث المعدات والبرمجيات المرتبطة بالنظام.

Abstract

The nature of the risks that threaten the security of information in the Directorate of Public Passports and Civil Status in Jordan

The purpose of this study is to identify the nature of the threats to information security in the Directorate of Public Passports and Civil Status in Jordan. The study was applied to a random sample of (58) users of the system. The descriptive statistics, and the T sample test, were used to analyze the data and test the hypotheses of the study. The study reached the following results:-

The study found a number of conclusions, the most important ones are:

1. Low level of recurrence of potential risks.
2. Acceptable level of the system performance efficiency in implementation of the Electronic interactions to processing of user requests and provide service to the customers.
3. The most frequent risks are natural risks that are Power System Blackouts and technical malfunctions.
4. the security risks that threaten the Electronic interactions did not cause the obstructing of the information system performance efficiency .
5. The system security level is appropriate to protect the Electronic interactions

The study suggested a number of recommendations, the most important are: improving protection tools that used to provide the perpetuation of power supply tools and updating the hardware and software that associated with the system.

المقدمة :-

نشأت مبادرات الحكومة الالكترونية تمشياً مع توجه العالم نحو اقتصاديات المعرفة والاستثمار في التقنيات الحديثة المختلفة بشكل علمي وعقلاني، خاصة في ظل سهولة الحصول على التقنية واستخدامها واتساع دائرة مستخدميها والمستفيدين من حلولها أفرادا ومؤسسات، لذلك أدركت العديد من المنظمات الحكومية في الدول النامية والمتقدمة على حد سواء، أهمية الاستفادة من التطور الهائل في تكنولوجيا المعلومات والاتصالات، ودورها في تحقيق الكفاءة والفعالية في أداء الأعمال، الأمر الذي دفعها نحو إدخال التكنولوجيا إلى معظم وظائفها وأنشطتها الفنية والإدارية.

ان حكومة المملكة الاردنية الهاشمية كغيرها من الحكومات انتهجت هذا النهج، وعلى وجه الخصوص في المديرية العامة للجوازات والاحوال المدنية، حيث تضمنت الخطة الاستراتيجية لتقنية المعلومات في المديرية تقديم خدماتها الكترونياً إلى المستفيدين وضمن مراحل متعددة، مبدئيا تم توظيف نظام معلومات الكتروني يمكّن من إدخال الطلب المقدم للحصول على الخدمة حاسوبياً، وإدخال كافة الإجراءات التي تتم على الطلب، وصولاً إلى القرار الذي يتم اتخاذه بخصوص ذلك

الطلب، بالإضافة إلى إمكانية الاستفادة من قواعد بيانات خارجية مرتبطة بالنظام وذلك من خلال توفر عنصر التكامل بين نظم الحكومة الإلكترونية للحصول على المعلومات التي تسهل إجراءات تقديم الخدمة، كما تم إنشاء البوابة الإلكترونية للجوازات على الويب بحيث يتم تقديم الخدمات الإلكترونية خلالها.

ومع تطور أدوات معالجة البيانات والمعلومات ووسائل تخزينها وتبادلها بطرق مختلفة، أصبح النظر إلى امن تلك البيانات والمعلومات كأمر مهم للغاية، حيث ساهمت التقنية بشكل ملحوظ في انتهاك حقوق وخصوصيات المستخدمين وتعرضها للخطر، خاصة في ظل التزايد المستمر في كمية البيانات والمعلومات المتبادلة إلكترونيا، مما أثار العديد من التساؤلات عن كيفية حماية تلك المعلومات من الوصول والاستخدام غير المشروع، وكذلك حول الآثار التي تحدثها هذه الأخطار على مخرجات نظم المعلومات (Patriciu, P., & Nicolaescu, 2006).

إن حماية التعاملات الالكترونية في نظم الحكومة الإلكترونية من المخاطر التي تهددها، يعد مطلباً رئيسياً لنجاح تلك النظم، ويأتي ذلك من خلال توفير الأدوات وسبل الحماية اللازمة من المخاطر الداخلية أو الخارجية او الطبيعية، بالإضافة إلى تطبيق المعايير الدولية لأمن المعلومات المتبادلة الكترونياً (مثل المعيار ISO 27006) لمنع الوصول غير المشروع للمعلومات من قبل أشخاص غير مخولين عبر الاتصالات، وكذلك ضمان أصالة وصحة تلك الاتصالات (Kissel, 2013).

ومن المنطلقات السابقة تأتي هذه الدراسة للكشف عن طبيعة المخاطر التي تهدد امن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن وما هو تأثير هذه المخاطر على اداء نظم المعلومات.

مشكلة الدراسة :-

تعتبر بيئة المنظمات الحكومية في المملكة الاردنية الهاشمية بيئة سريعة التطوّر من حيث اعتمادها على تكنولوجيا المعلومات في تقديم الخدمات العامة، فقد أصبحت تعتمد بشكل متزايد على نظم المعلومات الموزعة المبنية على الويب في تنفيذ أعمالها، الأمر الذي يجعلها عرضة للأخطار الأمنية التي تهدد نظامها المعلوماتي.

ومن أجل تقليل حدة هذه الأخطار وأثارها السلبية المحتملة، لا بد من المراجعة المستمرة للمخاطر المحتملة التي تواجه النظام وتحليلها وتقيمها وتحديد احتمال حدوثها، ليتسنى في المقابل تحديد وسائل الحماية اللازمة لتأمين النظام ومصادرة ومكوناته المختلفة، وتحديد التكلفة المقبولة لتلك الوسائل، كما تتضمن أيضاً الاستجابة المقررة للمخاطر التي تقع على النظام، مثل قبول مستوى معين من المخاطر، أو نقل الآثار والخسائر لجهة أخرى من خلال التأمين، أو وقف العمل بالنظام الحالي، والبدء بتطوير نظام جديد أكثر أمناً .....الخ (Elky, 2007).

لما سبق جاءت هذه الدراسة للتعرّف على طبيعة المخاطر التي تهدد امن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن، حيث يعد ذلك مدخلاً يُمكن الاسترشاد بنتائجه لغايات الحكم على المستوى المقبول من المخاطر التي يتعرض لها النظام، وتحديد مدى إعاقة هذه المخاطر على أداء النظام، وبالتالي توفير الاستجابة المناسبة للمخاطر واتخاذ القرار بشأن الإبقاء على النظام الحالي، أو تطوير وسائل الحماية المستخدمة، أو وقف العمل بالنظام الحالي والبدء بتطوير نظام جديد أكثر أمناً.

وتتلخص مشكلة الدراسة في الإجابة على الأسئلة التالية :-

1. ما هي أكثر المخاطر الأمنية التي تهدد امن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن، وما هي درجة تكرارها؟
2. ما هي المخاطر الداخلية التي تهدد امن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن، وما هي درجة تكرارها؟
3. ما هي انواع المخاطر الخارجية التي تهدد امن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن، وما هي درجة تكرارها؟
4. ما هي انواع المخاطر الطبيعية التي تهدد امن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن، وما هي درجة تكرارها؟

أهمية الدراسة :-

تبرز أهمية الدراسة من ما يلي :-

1. أهمية المسائل الأمنية خاصة في بيئة نظم المعلومات الموزعة وذلك بسبب تعدد أوجه الخطر التي تواجهها هذه النظم أثناء تبادل المعلومات خلاله، حيث يمكن معها إلحاق الضرر بالمعلومات والأجهزة عن بعد دون الحاجة إلى التواجد في نفس المكان.
2. أهمية تعريف انواع المخاطر الأمنية التي تهدد نظم معلومات مديرية الجوازات العامة والاحوال المدنية في الاردن، وذلك لمواجهة هذه المخاطر والتقليل من الخسائر الناتجة عنها.
3. تعد هذه الدراسة من أولى الدراسات على حد معرفة الباحث التي تركز على دراسة طبيعة المخاطر الأمنية التي تهدد نظم معلومات مديرية الجوازات العامة في الاردن، بهدف توفير الاستجابة المناسبة للمخاطر التي وقعت على النظام.
4. تعد النتائج التي يؤمل الوصول إليها من خلال هذا البحث إطارا مقترحا لإضافة بعض الإجراءات في الخطة الاستراتيجية لأمن المعلومات في المنظمات الالكترونية يستند إليها عند تصميم النظم الأمنية في نظم المعلومات الموزعة في مديرية الجوازات العامة والاحوال المدنية في الاردن.
5. كما ويؤمل أن يستفيد الباحثون والدارسون في مجال أمن المعلومات من نتائج هذا البحث والتوصيات والمقترحات التي يقدمها حول دراسات مستقبلية ذات أهمية، وكذلك سوف يقدم إطار فكري يساهم في إثراء المكتبة العربية بالأدبيات المتعلقة بمخاطر أمن المعلومات.

أهداف الدراسة :-

يُمكن إجمال الأهداف الرئيسية التي تسعى الدراسة إلى تحقيقها بما يلي :-

1. التعرّف على طبيعة المخاطر التي تهدد أمن المعلومات كواحدة من عمليات الحد من هذه المخاطر في مديرية الجوازات العامة والاحوال المدنية في الاردن.

2. التعرّف على درجة تكرار حدوث المخاطر التي تهدد أمن المعلومات في مديرية الجوازات العامة في الاردن.
3. التوصل الى نتائج يُمكن الاسترشاد بها لقبول هذا المستوى من المخاطر والتوصية بتحسين أدوات وسبل الحماية المتوفرة وإضافة غير المتوفر منها واللازم لحماية التعاملات الإلكترونية، أو وقف العمل بالنظام الحالي والبدء بتطوير نظام أكثر اللازمة لحماية نظام المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن.

فرضيات الدراسة :-

الفرضية الرئيسية الأولى :

لا يوجد فرق بين تقدير مستخدمي نظام المعلومات لمدى حدوث مخاطر داخلية تهدد أمن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن والمتوسط الفرضي (3).

الفرضية الرئيسية الثانية :-

لا يوجد فرق بين تقدير مستخدمي نظام المعلومات لمدى حدوث مخاطر خارجية تهدد أمن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن والمتوسط الفرضي (3).

الفرضية الرئيسية الثالثة :-

لا يوجد فرق بين تقدير مستخدمي نظام المعلومات لمدى حدوث مخاطر طبيعية تهدد أمن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن والمتوسط الفرضي (3).

الإطار النظري والدراسات السابقة :-

مخاطر أمن المعلومات :-

على الرغم من أهمية التعاملات الإلكترونية التي تتم عبر نظم المعلومات وخصوصية المعلومات التي تتضمنها، إلا أنها ما زالت تفتقر إلى الحماية الكاملة ومنع الاعتداء عليها، وما زالت تواجه الكثير من المخاطر الأمنية التي تلحق الضرر والتخريب بتلك التعاملات، فالتهديدات المحيطة بنظم المعلومات على اختلاف مصادرها وأنوعها وانتشار الجرائم

الإلكترونية هي من الأسباب التي تجعل البعض غير مطمئنين على بياناتهم وخصوصياتهم في البيئة الإلكترونية وتَّحِد من انتشارها (Goh , 2003).

قد تكون المخاطر عرضية (غير متعمدة) أو متعمدة وقد يكون لها علاقة باستخدام أو تطبيق نظم المعلومات أو النواحي البيئية والفيزيائية التابعة لنظم المعلومات.

هذا وقد تأخذ المخاطر أي شكل من أشكال سرقة المعلومات أو مخاطر متابعة الأعمال عن طريق الانترنت أو التجسس عن بعد أو سرقة المعدات أو الوثائق، أو فقدان وتدمير البيانات من خلال أي ظاهرة مناخية كالزلازل أو الحرائق أو الفيضانات أو الحوادث الوبائية، أو نتيجة لفقدان إمداد الطاقة أو إخفاق معدات الاتصالات (Whitman, 2003).

كما أنه من الممكن أن يكون مستخدم النظام (المستخدم النهائي، مدير النظام، موظفي الدعم الفني) من المهددات الأمنية للنظام، سواء بشكل متعمد بقصد إلحاق الضرر، أو بشكل غير متعمد بسبب الجهل لدى العاملين وقيامهم بأعمال غير مرخص لهم القيام بها أو غير مدربين على تنفيذها، لذلك يجب ألا يغبن الموظف أو يظلم ويجب أن يتم التأكد من حسن ولائه وحسن خلقه وحسن تدريبه وتأهيله، حيث أشارت بعض الدراسات إلى أن أكثر من % 80 من التهديدات الأمنية لنظم المعلومات مصدرها المستخدمين العاملين بشرعية مع النظام (Lacey, 2001).

تعريف الخطر والمفاهيم ذات العلاقة :-

قبل البدء بشرح أهم المخاطر التي تهدد أمن المعلومات لابد من التمييز بين العديد من المفاهيم المستخدمة في هذا السياق وغالباً ما يتم الخلط بينها، فثمة فرق بين مفاهيم (التهديد، الخطر، نقاط الضعف) بالرغم من التقائها لكونها مضادة للأمنية في بيئة المعلومات وذلك كما يلي :-

1) **التهديد Threats** : يعني احتمال أن يتعرض نظام المعلومات لاعتداء ما وقد يكون مصدر هذا الاحتمال شخصا، كالمتجسسّ أو المجرم المحترف أو المخترق أو المتطفل، أو شيئا يهدد الأجهزة أو البرامج أو المعطيات، أو حدثا كالحريق وانقطاع التيار الكهربائي والكوارث الطبيعية . (Anton and et al, 2003)

2) **الخطر Risk** : يقصد به الأثر الذي يقع نتيجة حدوث فعل التهديد، أي أنه حدث ما يقع نتيجة تهديد ما، والفرق بين الخطر والتهديد هو أن الخطر حدث فعلاً، أم التهديد فيبقى في دائرة الاحتمال (Schechter, 2004).

3) **نقاط الضعف أو الثغرات Vulnerabilities** : تعني جزء من النظام (عنصر أو نقطة أو موقع) يحتمل أن يتحقق بسببه التهديد ليصبح خطراً، أي يعبر من خلاله منفذ التهديد ليقع بعد ذلك الخطر، فمثلا يعد الأشخاص الذين يستخدمون النظام نقطة ضعف إذا لم يكن تدريبهم كافيا لاستخدام النظام وحمايته، وقد يكون الاتصال بالإنترنت نقطة ضعف مثلا إذا لم يكن مشفرا. وقد يكون الموقع المكاني للنظام نقطة ضعف كأن يكون غير مجهز بوسائل الوقاية والحماية، وبالعموم فان نقاط الضعف هي الأسباب المحركة لتحقيق التهديدات وحدوث المخاطر (Anton, 2003).

تصنيف مخاطر أمن المعلومات :-

صنفت مخاطر أمن المعلومات وفقاً لمعايير مختلفة نذكر منها :-

تصنيف المخاطر من حيث المصدر :-

صنفت إلى ثلاثة أصناف هي (مخاطر من الإنترنت، مخاطر من الموظفين، مخاطر طبيعية (Noordegraff,2002) كما وقد صنفت من حيث المصدر إلى أربعة أقسام هي مخاطر (داخلية، خارجية مرتبطة بالأنترنت، مادية، بيئية).

تصنيف المخاطر حسب الهدف :-

حيث صنفت إلى مخاطر متعمدة ومخاطر غير متعمدة (البحيصي، 2011) و (Abu Mousa, 2006).

مصادر المخاطر الأمنية لنظم المعلومات :-

تناولت الأدبيات المتعلقة بأمن المعلومات العديد من المخاطر التي تواجه بيئة نظم المعلومات، وتصنف من حيث المصدر إلى مصادر داخلية ومصادر خارجية ومصادر طبيعية (Warkentin and Willison, 2009) .

أولا : المصادر الداخلية.

وهي التي تحدث بسبب أحد مكونات النظام ونذكر منها :-

1. **المخاطر البشرية** : تعد من أخطر التهديدات وأكثرها تأثيرا المخاطر وتشمل هذه المخاطر الأفعال المقصودة وغير المقصودة من قبل الأشخاص المخولين وغير المخولين باستخدام النظام (Goodhue, 1991).
2. **خلل في المعدات** : يتضمن أعطال أجهزة الحاسوب والطرفيات والتجهيزات الشبكية المرتبطة في النظام سواء كانت هذه الأعطال بسبب التقادم أو بسبب المؤثرات البيئية المحيطة أو بفعل الاستخدام الخاطئ، وهذا النوع من الأعطال يتسبب في توقف النظام عن العمل وحجم الخدمة المقدمة عن المستفيدين (Anton, 2003).
3. **أخطاء البرمجيات** : تعاني كثير من البرمجيات المستخدمة في النظام من احتمال احتوائها على الأخطاء الأمر الذي ينعكس على دقة المخرجات التي يقوم بها النظام، وتكثر أخطاء البرمجيات في البرمجيات غير الأصلية (المنسوخة) أو البرمجيات المستخدمة بطريقة غير شرعية، وكذلك نجد كثير من الأخطاء في البرمجيات مفتوحة المصدر (المجانية) التي توفرها الشركات المطورة للمستخدمين مجاناً بقصد تطويرها وتحسينها (Anton, 2003).
4. **أخطاء البيانات** : يحدث أحيانا أخطاء في عملية إدخال البيانات بحيث يتم ادخال بيانات غير صحيحة مما ينعكس على دقة المخرجات، وقد يكون الخطأ في إدخال البيانات مقصودا أو غير مقصود وفي كلا الحالتين سيزيد حجم الخطر كلما زادت نسبة الخطأ في البيانات المدخلة (Anton, 2003).

ثانيا : المخاطر الخارجية.

هذا النوع من المخاطر يكون مصدره أسباب من خارج النظام أي يمكن أن يكون نتيجة أشخاص غير مخولين باستخدام النظام أو من أسباب بيئية أو طبيعية، ومن أهم هذه المخاطر ما يلي :-

1. **الهجوم الأمني** : يقصد به المحاولات المختلفة التي ينفذها أشخاص من غير المخولين بقصد الوصول غير الشرعي للنظام أو أحد مكوناته وإحداث الخطر، ويقع ضمن الهجوم الأمني عدد من الأخطار من أهمها (البحيصي، 2007) و (Heiser, 2013) :-

- **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 مخوّل لا إلى النظام والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير الملفات أو البرمجيات أو لمجرد الاستخدام غير المشروع (Kissel 2013).
- **الاصطياد الإلكتروني** : يقوم المهاجم بإرسال رسائل بريد إلكترونية خادعة إلى المستخدمين، بحيث تطلب منه معلومات مثل معلومات حسابه البنكي، أو معلومات بطاقته الائتمانية (Litan, 2004).
- **البرامج الخبيثة** : هي عبارة عن برنامج صغير معد لتخريب البيانات يتم إدخاله على نظام الحاسوب من غير علم المستخدم بغرض أن تنسخ أو تزيل البيانات المسجلة عليه، أو تنسخ نفسها إلى حاسوب النظام، ومن الأمثلة عليها الفيروسات الحاسوبية وبرامج الديدان وحصان طروادة والقنابل الموقوتة (Merkow and James, 2005).

ثالثا : المخاطر الطبيعية.

هي المخاطر التي يكون مصدرها الطبيعة التي يعمل بها النظام وتسمى ايضا المخاطر المادية أو الفيزيائية. وهي التي تقع على أي من مكونات النظام مثل أجهزة الحاسب والبرامج والشبكات والبيانات وتسبب خسائر وأضرار للمنظمة وتشمل الحرائق والكوارث الطبيعية والسطو بالإضافة إلى انقطاع التيار الكهربائي (الهادي، 2006).

طبيعة المخاطر في أمن المعلومات :-

تعد المخاطر الأمنية من المؤثرات السلبية في أداء أي نظام معلومات، لذلك لابد من مواجهتها بما ينبغي من إجراءات تختلف من نظام لآخر، ومن هنا لا بد من تعريف المخاطر الأمنية التي قد تؤثر سلباً على سير نظام المعلومات أو على العناصر الأمنية الأساسية فيه (سلامة البيانات، سرية البيانات، استمرارية عمل النظام)، وتقييم هذه المخاطر من حيث احتمال الحدوث مستقبلاً والثغرات الأمنية التي تستغلها وتحديد الأثر الذي تتركه على النظام أو على المعلومات الناتجة

منه، وأخيرا تطوير الاستجابة المناسبة للتحكم بها. وتتضمن هذه الاستجابة ما يلي (Haimes and Chittester, 2005).

1. تجنب المخاطر عن طريق تجنب استخدام تقنيات لا تستطيع المنظمة حماية النظام من المخاطر المحتملة الناتجة عن استخدام هذه التقنية.
2. تقليل المخاطر من خلال تنفيذ ضوابط التخفيف من المخاطر، أي استخدام وسائل حماية قوية والالتزام بمعايير أمن المعلومات العالمية والتوصيات المرتبطة بها عند تطوير نظم المعلومات (ابو شنب، 2009).
3. قبول المخاطر ضمن الحدود المقبولة، فإذا كانت تكلفة التأمين تزيد عن العائد المتوقع، وهذا يتطلب تقييم الأصول المعلوماتية للمنظمة وتحديد قيمتها وتكلفة المخاطر التي قد تتعرض لها، ولا مانع من قبول بعض المخاطر التي تزيد تكلفة تأمينها عن تكلفة تلك المخاطر في حال وقوعها.
4. وقف العمل بالنظام والبدء بتطوير نظام أكثر أمناً وهذا يحدث عندما يتكرر وقوع المخاطر وتفشل سبل الحماية المتبعة من منعها مما يلحق ضرراً كبيراً في نظام المعلومات ومكوناته المختلفة (Conrad, 2005).

أمن المعلومات :-

يقصد به النظم التي تقوم بتجميع وتدقيق وتخزين البيانات الخاصة بالعمليات التشغيلية الروتينية اليومية للمنظمة، ثم تحويلها إلى معلومات، والتي تخدم المستوى التشغيلي في المنظمة. فهي تخدم المستخدمين في المحافظة على أداء الأنشطة والعمليات اليومية الروتينية العادية للمنظمة، حيث يعتبر نظام معلومات مديرية الجوازات شكلاً من أشكال هذه النظم (Rahmatian, 2003).

حيث تعتبر هذه النظم المزود الرئيسي لقواعد البيانات في المنظمة، كما أنها تتكامل مع أنظمة المعلومات الأخرى وتوفر لها الكثير من البيانات التي تحتاجها، لذلك فإن توفير الحماية لهذه الأنظمة وتوفير عناصر امن المعلومات فيها (السرية، السلامة، الاستمرارية) التي تنعكس على جميع نظام المعلومات التي تستخدمها المنظمة (Gupta, Sheetlanim, 2012).

ان معظم نظم الحكومة الإلكترونية تعد نظم تعاملات إلكترونية لإنجاز المعاملات الحكومية وتقديم الخدمة للمواطنين، لذلك فإنها تعتبر من تطبيقات نظم معالجة المعاملات، ويعتبر تأمين هذه النظم والمحافظة عليها مطلباً رئيسياً لنجاح مشاريع الحكومة الإلكترونية، لذلك لابد من البحث المستمر في وسائل وسبل الحماية اللازمة لتأمين هذه النظم خاصة وأنها تقوم بإنجاز معاملات مهمة على مستوى الدول وأي تهديد تتعرض له يعد من مهددات الأمن القومي (Snijder, Kool, 2013).

الدراسات السابقة :-

دراسة (البحيصي، 2011) هدفت هذه الدراسة إلى الكشف عن المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة الفلسطينية في قطاع غزة. وقد تم استخدام استبيان لجمع البيانات من عينة الدراسة المتمثلة في عدد من الشركات الفلسطينية، حيث بلغ حجم العينة 97 شركة وقد توصلت الدراسة إلى مجموعة من النتائج من اهمها أن أهم هذه المخاطر هي :-

1. الإدخال المتعمد للبيانات الخاطئة عن طريق المستخدمين وانقطاع التيار الكهربائي والإتلاف غير المقصود للبيانات من قبل المستخدمين واشتراك العاملين في كلمات الدخول للحاسوب ودخول الفيروسات إلى الأنظمة.
2. أن الشركات الفلسطينية تختلف فيما بينها في درجة تكرار وأهمية المخاطر حسب نوعية نظام المعلومات المستخدم وحسب مدى الارتباط بشبكة الانترنت.
3. ليس هناك ارتباط بين نوع المؤسسة (القطاع الذي تنتمي إليه المؤسسة) ودرجة تكرار وأهمية المخاطر التي تتعرض لها الشركات الفلسطينية.

وقد اوصت الدراسة بضرورة زيادة الاهتمام بأمن المعلومات خاصة لدى الشركات التي تستخدم نظام الشبكات والتي ترتبط بشبكة الانترنت. وتطوير قدرات وكفاءة العاملين في مجال الحاسوب وذلك لضمان عدم إدخال متعمد للبيانات الخاطئة أو إتلاف غير مقصود للبيانات السليمة.

دراسة (أبو شنب، 2009) هدفت هذه الدراسة إلى تحليل المخاطر لمشاريع نظم المعلومات حيث أسهمت الدراسة في توضيح المنطلقات الرئيسية لإدارة المخاطر التي تحيط بمشاريع نظم المعلومات مع التركيز على مشاريع الحكومة الإلكترونية وبينت أنه من أهم الأسباب التي تقف وراء مثل هذه المخاطر، تلك المخاطر التي تهدد أمن وسلامة المعلومات واحتمالية تعرض هذه الأنظمة للاعتداء والتخريب.

وأشارت الدراسة إلى بعض الأساليب التي يُمكن أن تُساعد في معالجة مخاطر مشاريع الحكومة الإلكترونية ومن بينها طريقة (OCTAVE) التي تعتمد على ثلاثة مراحل رئيسية وهي :-

1. بناء تصور للتهديدات المتعلقة بالموجودات والمصادر.
2. التعرُف على وتحديد البنية التحتية القابلة للتعرض للخطر.

وقد توصلت الدراسة إلى مجموعة من النتائج من اهمها أن تنفيذ مشاريع تكنولوجيا المعلومات وخصوصا أنظمة المعلومات محفوف بالمخاطر لأسباب عديدة منها التغير الحاصل بالتكنولوجيا والعناصر الكثيرة والمتداخلة في الأنظمة مثل المستخدمين والشبكات والمزودين، وخصوصا بعد بروز شبكات الإنترنت واتساع نطاق التطبيقات الحديثة، ومع ذلك فإن التخطيط السليم لهذه المشاريع يخفف من التأثيرات الغير مرغوب بها ويزيد من الموثوقية في تحقيق الأهداف.

دراسة (الذنيبات ومبيضين، 2009) هدفت هذه الدراسة إلى اختبار كفاءة الخدمات الإلكترونية المقدمة في مديرية الجنسية وشؤون الأجانب، والتعرّف على أثرها في قبول المستفيدين للخدمات الالكترونية، من خلال إجراء دراسة تحليلية لآراء عينة عشوائية من المستفيدين من هذه الخدمات، ولأغراض هذه الدراسة تم بناء استبانة لقياس المتغيرات المستقلة (أبعاد الكفاءة)، والمتغيرات التابعة عناصر (قبول الخدمة الالكترونية)، وقد أجريت الدراسة على عينة تكونت من (126) فرداً من مراجعي المديرية خلال فترة محددة، ولاختبار الفرضيات استخدم الباحثان الإحصاءات الوصفية، والانحدار المتعدد والبسيط. وقد توصلت الدراسة إلى عدد من النتائج كان من أهمها :-

1. هنالك تقدير متوسط لأبعاد كفاءة الخدمات الإلكترونية، وكان من أكثر الأبعاد تقديرا فعاليّة الخدمة المقدمة حيث كان الوسط الحسابي (3.30).

2. هنالك قبول بمستوى مرتفع للخدمات الإلكترونية المقدمة لدى المستفيدين.

3. هنالك تأثير إيجابي ذو دلالة إحصائية لمجمل أبعاد كفاءة الخدمات الإلكترونية المقدمة على قبول المستفيدين للخدمة الالكترونية، وكان أكثر الأبعاد تأثيراً (جودة الخدمة الالكترونية وفعاليّة الخدمة الالكترونية ثم تكلفة الخدمة الالكترونية).

دراسة (Christopher and Howard, 2007) هدفت هذه الدراسة إلى التعرّف على نظرة مدراء مصادر المعلومات في ولاية تكساس في فعاليّة الحكومة الإلكترونية والعوامل المؤثرة فيها، كما أنها دراسة تجريبية تُركز على ماذا قدمت الإدارات المحلية من مصطلحات ومعلومات وخدمات الحكومة الإلكترونية كحد أدنى من وجهة نظر منفذي القرار.

جاءت هذه الدراسة لتملأ الفراغ من حيث كيف تؤثر الحكومة الإلكترونية في الإدارة في وكالات الحكومة في تكساس؟ كذلك فحصت الدراسة تأثير بعض العوامل على فعاليّة الحكومة الإلكترونية وتمثلت هذه العوامل بـ (حركة إعادة اكتشاف الحكومة، ضغوط البيئة الخارجية، قوة الموارد، العوامل الديموغرافية).

وقد توصلت الدراسة إلى عدد من النتائج كان من أهمها أن عوامل (حركة إعادة اكتشاف الحكومة، ضغوط البيئة الخارجية، قوة الموارد) من أهم العوامل المؤثرة في فعاليّة الحكومة الإلكترونية، وأن حجم الوكالة لا يؤثر في فعاليّة الحكومة الإلكترونية.

دراسة (Patriciu and et al, 2006) هدفت هذه الدراسة إلى وضع مقاييس لتقييم الحالة الراهنة لأمن المعلومات في نظم معلومات المؤسسات والتي تساعد المؤسسة في تحديد أولويات التهديدات الأمنية والثغرات والمخاطر التي تشكلها على أصول المؤسسة. وتعرض هذه الدراسة إطاراً لتقييم الثغرات الأمنية بطريقة متناسقة وبعض المقاييس التشغيلية المستخدمة من قبل المؤسسات الكبيرة في عمليات إدارة أمن نظم المعلومات ومن هذه المقاييس :-

1. قياس ما إذا الثغرات الأمنية استغلت محليا أم عن بعد؟

2. قياس درجة التعقيد في استغلال الثغرة الأمنية مرة واحدة من قبل المستخدم الشرعي، وهل هي مرتفعة أم منخفضة؟

3. قياس ما إذا كان المهاجم يحتاج إلى مصادقة عند استهدافه للنظام عبر الثغرات أو نقاط الضعف؟

4. قياس أثر النجاح في استهداف النظام على مستوى السرية في النظام، وهل هي منعدمة، جزئية، كاملة؟

5. قياس أثر النجاح في استهداف النظام على مستوى سلامة المعلومات في النظام، وهل هي منعدمة، جزئية، كاملة؟

6. قياس أثر النجاح في استهداف النظام على مستوى توفر النظام للمستخدمين الشرعيين، وهل هي منعدمة، جزئية، كاملة؟

وقد اوصت الدراسة انه في حال الحصول على إجابات أو تقييمات لهذه المقاييس يُمكن بعد ذلك تقييم الحالة الأمنية للنظام هل هو (مرتفع الأمن، غير أمن، منخفض الأمن، متوسط الأمن).

دراسة (Anton, et al, 2003) هدفت هذه الدراسة إلى تقييم المخاطر والثغرات الأمنية التي تُواجه نظم المعلومات في المنظمات وكيفية التخفيف من حدتها، بحيث يتم اكتشاف الثغرات الأمنية الجديدة التي لم تستغل في اختراق نظم المعلومات.

أجريت هذه الدراسة بدعم من وكالة البحوث المتقدمة في وزارة الدفاع الأمريكية وقد صُنفت المخاطر التي تهدد أمن نظم المعلومات إلى مخاطر بشرية أو اجتماعية مثل تصرفات المستخدمين الحاقدين بحيث يتعمد الشخص المصرح له دخول النظام إلى التصرُف بحقد مما يدفعه إلى التخريب أو الاعتداء، ومخاطر ذات علاقة ببيئة الإنترنت والشبكات مثل هجمات منع الوصول إلى الخدمة، انتحال الشخصية، عدم القدرة على التمييز بين المستخدم الشرعي والمستخدم غير الشرعي بسبب اللاوعي لدى المستخدمين الشرعيين. كذلك المخاطر المادية المرتبطة بالأجهزة والمعدات المستخدمة بحيث يتم الاعتداء عليها بالتدمير والسرقة، أو تلك المتعلقة بالبرامج المستخدمة مثل استغلال الأخطاء الشائعة وأخطاء التصميم في برامج التطبيقات التجارية من قبل المهاجمين للدخول غير الشرعي للنظام. واخيرا المخاطر البيئية التي يتعرض لها النظام مثل درجة الحرارة والرطوبة والتوقف بسبب انقطاع التيار الكهربائي وغيرها. وقد قدمت هذه الدراسة منهجية تسمى (VAM) لاكتشاف التهديدات الجديدة والتهديدات المعروفة سابقا وأساليب المعالجة المقترحة.

علاقة الدراسة الحالية بالدراسات السابقة :-

فيما يلي ملخصا لمدى استفادة الدراسة الحالية وعلاقتها بالدراسات السابقة، بالإضافة إلى بيان الإضافة العلمية التي تتميز بها الدراسة الحالية عن تلك الدراسات، حيث تُعّد الدراسة الحالية من أولى الدراسات على حد معرفة الباحث والتي تقدم مدخلاً مقترحاً للحد من المخاطر التي تُهدّد نظم المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن.

هدفت دراسة (البحيصي، 2011) الى الكشف عن المخاطر التي تُهدد نظم المعلومات المحاسبية بينما هدفت الدراسة الحالية الى معرفة أهم المخاطر التي تهدد نظم المعلومات، كما هدفت دراسة (أبو شنب، 2009) الى تحليل المخاطر لمشاريع نظم معلومات الحكومة الإلكترونية بينما هدفت الدراسة الحالية الى التعرّف على أهم المخاطر التي تهدد نظم المعلومات، وكذلك الاستفادة من أسلوب تحليل المخاطر الأمنية التي اعتمدته الدراسة، كذلك هدفت دراسة (الذنيبات ومبيضين، 2009) الى اختبار كفاءة الخدمات الإلكترونية المقدمة في مديرية الجنسية وشؤون الأجانب بينما هدفت الدراسة الحالية الى معرفة أهم انواع المخاطر التي تهدد كفاءة نظم المعلومات، كما هدفت دراسة (Christopher and Howard, 2007) الى التعرّف على نظرة مدراء مصادر المعلومات في ولاية تكساس في فعاليّة الحكومة الإلكترونية والعوامل المؤثرة فيها بينما هدفت الدراسة الحالية الى معرفة مستوى المخاطر الأمنية التي تهدد النظام ودرجة تكرارها، كذلك هدفت دراسة (Patriciu and et al, 2006) الى التعرّف على نظرة مدراء مصادر المعلومات في ولاية تكساس في فعاليّة الحكومة الإلكترونية والعوامل المؤثرة فيها بينما هدفت الدراسة الحالية الى التعرّف على طبيعة المخاطر التي تهدد نظم المعلومات، واخيرا هدفت دراسة (Anton, et al, 2003) الى التعرّف على تقييم المخاطر والثغرات الأمنية التي تواجه نظم المعلومات في المنظمات وكيفية التخفيف من حدتها بينما هدفت الدراسة الحالية الى التعرّف أهم المخاطر التي تهدد نظم المعلومات، وكذلك الاستفادة من منهجية اكتشاف التهديدات الأمنية التي اعتمدتها الدراسة.

المنهجية والإجراءات :-

اعتمدت الدراسة على منهج دراسة الحالة حيث يعتبر منهجا مناسبا لمثل هذه الدراسات نظرا لتعمقه في دراسة واقع حالة معينة (مديرية الجوازات العامة والاحوال المدنية في الاردن)، والتعرّف على طبيعة المخاطر التي تهدد أمن معلوماتها، وتمت هذه الدراسة من خلال الإجراءات التالية:-

1. مراجعة الإنتاج الفكري في مجال أمن المعلومات للتعرّف على طبيعة المخاطر التي تواجه نظم المعلومات.
2. إجراء دراسة مسحية لمستخدمي نظام المعلومات للكشف عن تقديرهم لطبيعة المخاطر التي تعرض لها النظام خلال مدة عملهم في مديرية الجوازات العامة والاحوال المدنية في الاردن ومدى تكرار حدوثها، حيث تم استكشاف مدى وقوع مخاطر داخلية ومخاطر خارجية ومخاطر طبيعية ودرجة تكرارها، وتم اختيار هذه المخاطر وفقاً لنتائج الدراسات السابقة.

وبعد تحليل البيانات تم اختبار فرضيات الدراسة بالطرق الإحصائية المناسبة باستخدام البرنامج الإحصائي SPSS.

مجتمع الدراسة وعينتها :-

يتكون مجتمع الدراسة من كافة مستخدمي نظام المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن، (مدير النظام، طاقم الدعم الفني، المستخدم النهائي).

أما عينة الدراسة فقد تم توزيع الاستبانة على أكبر عدد من الموظفين الذين يستخدمون نظام المعلومات وضمن الفئات الرئيسة الثلاثة سابقة الذكر، حيث بلغ عدد الاستبيانات الموزعة 70 استبانة استرجع منها 61 استبانة وتم استبعاد 3 استبانات لعدم صلاحيتها للتحليل الاحصائي وبذلك يكون عدد الاستبانات الصالحة للتحليل الاحصائي 58 استبانة بنسبة بلغت % 82.85 والجدول رقم (1) يبين توزيع عينة الدراسة حسب عدد من المتغيرات التعريفية التي تناولتها الدراسة (خصائص عينة الدراسة).

جدول رقم (1) : يبين التكرارات والنسبة المئوية لأفراد عينة الدراسة

المتغير	الفئة	التكرار	%النسبة المئوية
المؤهل العلمي	ثانوية عامة فما دون	6	10.34 %
	دبلوم متوسط	11	18.97 %
	بكالوريوس	34	58.62 %
	دراسات عليا	7	12.07 %
	المجموع	58	100 %
المستوى الوظيفي	ادارة عليا	1	1.7 %
	ادارة وسطى	17	29.31 %
	ادارة تنفيذية	40	68.97 %
	المجموع	58	100 %
طبيعة العمل مع نظام المعلومات	مدير النظام	1	1.7 %
	طاقم الدعم الفني	7	12.07 %
	المستخدم النهائي	50	86.21 %
	المجموع	58	100 %
مستوى المعرفة في مجال امن المعلومات وطبيعة مخاطر الحاسوب	مرتفعة	12	20.69 %
	متوسطة	27	46.55 %
	منخفضة	17	29.31 %
	ليس لدي أي معرفة	2	3.45 %
	المجموع	58	100 %

تشير النتائج الواردة في الجدول رقم (1) إلى أن خصائص العينة متقاربة مع خصائص المجتمع المبحوث، فمثلا نجد أن غالبية عينة الدراسة من فئة المؤهلين علميا والتي تُمثل الشريحة الأكبر من العاملين في مديرية الجوازات العامة والاحوال المدنية في الاردن، كما أن متغير المستوى الوظيفي قد مثلت فئة (إدارة تنفيذية) 68.97 % من العينة وهي الفئة الأكثر تعاملاً مع نظام المعلومات، وبالنسبة لمتغير التخصص فقد تبين أن معظم العينة مختصة في مجال الحاسب الآلي، أما بالنسبة لمتغير طبيعة العمل مع نظام المعلومات فتبين أن 86.21 % من العينة يعملون كمستخدم نهائي للنظام والذي يقوم بتنفيذ المهام المكلّف بها من خلال نظام المعلومات مثل اصدار جواز سفر واصدار دفتر عائلة وبطاقة شخصية وشهادة ميلاد وشهادة وفاة ومختص في اصدار جواز سفر واصدار وبطاقة شخصية (بعد اتخاذ الاجراءات القانونية).....الخ وهي جميعها مهام تستند إلى مخرجات النظام في اتخاذ القرارات المتعلقة بها، كما أنهم قادرين على اكتشاف المخاطر الأمنية التي يتعرّض لها النظام وذلك من خلال عملهم مع النظام واعتمادهم عليه في تأدية مهامهم. كما بينت النتائج أن نسبة عينة الدراسة ممن يقدرون مستوى معرفتهم في مجال امن المعلومات وطبيعة مخاطر الحاسوب

كانت *20.69 %* بمستوى مرتفع وأن *46.55 %* من العينة بمستوى متوسط وأن *29.31 %* من بمستوى منخفض، وفقط *3.45 %* ليس لديهم أي معرفة بمخاطر أمن المعلومات والحاسوب.

أداة الدراسة :-

اعتمدت الدراسة على الاستبيان بهدف جمع البيانات التي تخدم الدراسة وتُحقق أهدافها حيث تم تصميم استبانة تكونت من قسمين على النحو التالي :-

القسم الأول : يتضمن البيانات التعريفية للعينة مثل المؤهل العلمي والمستوى الوظيفي وطبيعة العمل مع النظام ومستوى المعرفة في مجال امن المعلومات وطبيعة مخاطر الحاسوب.

القسم الثاني : يتعلق بقياس مدى وقوع وتكرار مخاطر أمن المعلومات التي استكشفتها الدراسة حسب تقدير أفراد العينة، ووفقاً للتصنيف الثلاثي للمخاطر (مخاطر داخلية، مخاطر خارجية ، مخاطر طبيعية)، حيث تم استكشاف مدى تعرض النظام للمخاطر الشائعة وفقاً لنتائج الدراسات السابقة، وكانت هذه المخاطر (الاختراق الداخلي، الإدخال الخاطئ للبيانات بشكل متعمد، الإدخال الخاطئ للبيانات بشكل غير متعمد، الاستخدام الخاطئ غير المتعمد للنظام، الإتلاف غير المتعمد لمعدات النظام، أخطاء البرمجيات، الاختراق الخارجي، البرامج الخبيثة، الاصطياد الإلكتروني، الكوارث الطبيعية، انقطاع التيار الكهربائي، الأعطال الفنية). وذلك على مقياس لكرت الخماسي المتدرج من (5-1).

وقد تم تحديد أوزان وفقرات الاستبانة ضمن مقياس لكرت الخماسي للخيارات المتعدّدة الذي يحتسب أوزان تلك الفقرات بطريقة خماسية على النحو التالي :

الخيار (لم تحدث إطلاقا) ويمثل (1) درجة، والخيار (من مرة في السنة إلى مرة كل 6 أشهر) ويمثل (2) درجات، والخيار (أكثر من مرتين في السنة إلى مرة في الشهر) ويمثل (3) درجات، والخيار (مرة في الشهر إلى أكثر من مرتين في السنة) ويمثل (4) درجات، والخيار (أكثر من مرة في الأسبوع) ويمثل (5) درجات.

التحقّق من الصدق والثبات للاستبانة :-

تم إجراء صدق تحكيمي للاستبانة (الصدق الظاهري) للتأكد من أن فقرات الاستبانة تقيس بالفعّل متغيرات الدراسة، حيث تم عرض الاستبانة على عدد من الأساتذة المحكمين لإبداء رأيهم فيها، بالإضافة إلى توزيع الاستبانة على عينة أولية من مستخدمي نظام المعلومات في إدارة أخرى بلغ حجمها (15) فرداً، وذلك للتعرّف على مدى وضوح وسهولة الألفاظ المستخدمة ومدى فهمهم للفقرات الواردة في هذه الاستبانة، ومن ثم تم إجراء التعديلات الضرورية وفقاً لآراء المحكمين ونتائج العينة الاستطلاعية.

كما تم استخدام معامل الاتساق الداخلي كرومباخ ألفا (Cronbach Alpha) بهدف التأكد من مدى اتساق أداة القياس، وكانت النتائج المعالجة بالحاسوب كما هي في الجدول رقم (2)، حيث تشير النتائج إلى أن معامل الثبات لجميع الأبعاد لا يقل عن (0,60)، وأن معامل الثبات لجميع فقرات الاستبانة بلغ (0.78)، وهذا يعني أن أداة الدراسة تتسم بالثبات وصالحة لأغراض التحليل الإحصائي والبحث العلمي (Sekran,2006).

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

التسلسل	المحاور	عدد الفقرات	معامل الثبات (α) Cronbach – Alpha
1	المخاطر الداخلية	*16*	*72 %*
2	المخاطر الخارجية	*10*	*80 %*
3	المخاطر الطبيعية	*7*	*62 %*
	الاستبانة ككل	***33***	***78 % %***

متغيرات الدراسة والتعريفات الإجرائية :-

اشتملت الدراسة على المتغيرات التالية :-

مخاطر أمن المعلومات :-

تُعرّف إجرائيا لغايات هذه الدراسة بأنها عبارة عن حالة الخروج عن الوضع المألوف (الاعتيادي) في سير النظام بكافة عناصره (الإدخال، التشغيل، الإخراج) وكافة مستلزماته (المادية، البرمجية، البشرية) نتيجة حدث غير مشروع من مصدر داخلي أو خارجي أو طبيعي، وسواء كان بشكل متعمد أو غير متعمد، حيث تم استكشاف مدى وقوع المخاطر التالية

والتي بينت الدراسات السابقة شيوعها في أنظمة المعلومات ((البحيصي، 2011) (ابو شنب، 2009) (Anton and et al, 2003))

اولا :– المخاطر الداخلية.

- **الاختراق الداخلي** : وهو أن يقوم أحد الأشخاص العاملين مع النظام (المستخدم الشرعي) باستخدام النظام بشكل غير مصرح والقيام بعمل ينتهك أمن البيانات.
- **الإدخال الخاطئ للبيانات بشكل متعمد** : اي إدخال بيانات مغلوطة للنظام لغايات تحريف المخرجات.
- **إدخال خاطئ غير متعمد** : اي إدخال بيانات خاطئة للنظام بشكل غير مقصود مما يتسبب في تحريف المخرجات.
- **الاستخدام الخاطئ غير المتعمد** : اي استخدام النظام بشكل ينتهك أمنية البيانات من غير قصد مثل نقل فيروس إلى النظام من خلال وحدة تخزين USB أو الكشف عن كلمة السر للغير بشكل غير مقصود.
- **إتلاف غير متعمد لمعدات النظام** : كأن يتم التسبب في قطع سلك الشبكة أو كسر أحد أجهزة النظام بشكل غير مقصود.
- **أخطاء البرامج** : بحيث يتم كتابة تعليمات برمجية خاطئة في النظام بشكل غير مقصود تؤدي إلى انتهاك أمنية النظام وقد ينعكس ذلك على أخطاء في المعالجة وبالتالي الحصول على مخرجات غير صحيحة.

ثانيا :– المخاطر الخارجية.

- **الاختراق الخارجي** : ويقصد به قيام شخص غير مصرح له باستخدام النظام (القراصنة) بالدخول للنظام مستغلا الثغرات الموجودة فيه، والقيام بعمل ينتهك أمنية النظام كالتصنت أو سرقة البيانات أو تخريبها أو تحريفها، أو إيقاف النظام عن العمل.
- **البرامج الخبيثة** : ويقصد بها فيروسات الحاسوب وأشباهها التي تصل إلى النظام ومكوناته البرمجية مما تتسبب بعمل ينتهك أمنية النظام مثل تخريب البيانات أو زرع برامج تجسس أو إيقاف النظام عن العمل.

❖ **الاصطياد الالكتروني** : وهو انتهاك أمنية النظام من خلال رسائل البريد الإلكتروني التي ترسل له بقصد التخريب أو سرقة كلمات المرور أو زرع برامج التجسس.

ثالثا :- المخاطر الطبيعية.

❖ **الكوارث الطبيعية** : وهي الزلازل والبراكين والأعاصير والأمطار والسيول والحرائق التي تنتج عنها .. الخ وفي حال حدوثها قد تنتهك أمنية النظام من خلال إتلاف النظام ومكوناته المادية والبرمجية بشكل كلي أو جزئي.

❖ **انقطاع التيار الكهربائي** : انقطاع التيار الكهربائي عن النظام لأي سبب من الأسباب مما قد يتسبب في انتهاك أمنية النظام في توقفه عن العمل.

❖ **الأعطال الفنية** : وتشمل جميع الأعطال البرمجية والشبكية وأعطال المعدات التابعة للنظام بسبب قدمها أو عدم ملائمتها لأحمال النظام، مما قد يتسبب في انتهاك أمنية النظام إما ببطء المعالجة أو بالتوقف عن العمل.

نتائج التحليل الإحصائي لبيانات الاستبيان :-

فيما يلي عرض لنتائج التحليل الإحصائي الوصفي للبيانات التي تم جمعها بواسطة الاستبيان، وهي قيمة المتوسطات الحسابية والانحرافات المعيارية ومستوى التقدير لجميع متغيرات الدراسة، والفقرات المكونة لكل متغير. ولغايات التقييم فإن قيم المتوسطات الحسابية التي وصلت إليها الدراسة سيتم التعامل معها لتفسير البيانات على النحو التالي :-(3.5) فما فوق يمثل مستوى مرتفعاً و (3.49 – 2.5) يمثل مستوى متوسطاً، بينما أقل من (2.5) يمثل مستوى منخفضاً. وكانت نتائج التحليل على النحو التالي :-

المخاطر الداخلية :-

الجداول رقم (3 – 8) تبين المتوسط الحسابي، الانحراف المعياري، مستوى التقدير، والتكرارات لتقدير أفراد العينة للمخاطر الداخلية والفقرات التي تقيسها، فقد تبين أن المتوسط العام لتقدير أفراد العينة للمخاطر الداخلية كان منخفضاً بمتوسط حسابي بلغ 1.79 فقد كانت معظم إجابات المبحوثين حول الفقرات المتعلقة بهذه المخاطر ضمن عدم الحدوث

مطلقا بشكل يعيق أداء النظام سواء فيما يتعلق بمؤشر السرعة أو الملائمة، أو سلامة البيانات، 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 كيفية استخدام النظام، وكذلك التحقّق من سلامة التعليمات البرمجية من حين لآخر. وتتكون فقرات المخاطر الداخلية من كل مما يلي :-

اولا :- الاختراق الداخلي.

1. تم اختراق النظام من قبل أحد مستخدمي النظام مما تسبب في توقف النظام عن العمل لفترة ما.
2. تم اختراق النظام من قبل أحد مستخدمي النظام مما تسبب في بطء عمل النظام.
3. تم اختراق النظام من قبل أحد مستخدمي النظام مما تسبب في الحصول على مخرجات غير صحيحة.
4. تم اختراق النظام من قبل أحد مستخدمي النظام مما تسبب في تخريب البيانات المخزنة.

جدول رقم (3) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الداخلية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
1	1.65	0.83	0.000	منخفض	31	19	6	2	0
2	1.66	0.81	0.000	منخفض	32	15	9	1	1
3	1.64	0.68	0.000	منخفض	38	16	3	1	0
4	1.98	1.24	0.000	منخفض	29	16	2	9	2
الاختراق الداخلي ككل	1.69	0.54	0.000	منخفض					

ثانيا :- الادخال الخاطئ المتعمد.

5. الإدخال الخاطئ بشكل متعمد للبيانات إلى النظام مما أدى إلى الحصول على مخرجات غير صحيحة.

جدول رقم (4) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الداخلية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
5	1.57	0.66	0.000	منخفض	26	28	4	0	0
الادخال الخاطئ المتعمد	1.57	0.66	0.000	منخفض					

ثالثا :– الادخال الخاطئ غير المتعمد.

6. الإدخال الخاطئ غير المتعمد للبيانات إلى النظام مما تسبب في توقف العمل بالنظام لفترة ما.

7. الإدخال الخاطئ غير المتعمد للبيانات إلى النظام مما أدى إلى الحصول على مخرجات غير صحيحة

جدول رقم (5) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الداخلية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
6	2.0	1.06	0.000	منخفض	23	24	9	0	2
7	1.76	1.17	0.000	منخفض	39	11	3	1	4
الادخال الخاطئ غير المتعمد	1.84	1.02	0.000	منخفض					

رابعا :– الاستخدام الخاطئ غير المتعمد.

8. الاستخدام الخاطئ غير المتعمد للنظام مما يتيح مخرجات غير صحيحة.

9. الاستخدام الخاطئ غير المتعمد للنظام مما يتسبب في توقف العمل بالنظام لفترة ما.

10. الاستخدام الخاطئ غير المتعمد للنظام مما تسبب في تخريب البيانات المخزنة.

جدول رقم (6) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الداخلية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
8	2.06	1,16	0.000	منخفض	27	15	9	4	3
9	2.20	1.23	0.000	منخفض	23	18	8	5	4
10	1.68	0.94	0.000	منخفض	31	17	6	2	2
الاستخدام الخاطئ غير المتعمد :–	1.98	0.92	0.000	منخفض					

خامسا :– الإتلاف غير المتعمد لمعدات النظام.

11. الإتلاف غير المتعمد لمعدات النظام مما يتسبب في توقف عمل النظام لفترة ما.

12. الإتلاف غير المتعمد لمعدات النظام مما يتسبب في تخريب البيانات المخزنة.

جدول رقم (7) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الداخلية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
11	1.73	0.90	0.000	منخفض	29	18	9	1	1
12	1.61	0.91	0.000	منخفض	38	11	6	2	1
الإتلاف غير المتعمد لمعدات النظام	1.67	0.73	0.000	منخفض					

سادسا :– أخطاء البرامج.

13. حدوث أخطاء في التصميم البرمجي للنظام مما أدى إلى بطيء في عمل النظام.

14. حدوث أخطاء في التصميم البرمجي للنظام مما أدى إلى الحصول على مخرجات غير صحيحة.

15. حدوث أخطاء في التصميم البرمجي للنظام مما أدى إلى توقف العمل بالنظام لفترة ما.

16. حدوث أخطاء في التصميم البرمجي للنظام مما أدى إلى تخريب البيانات المخزنة.

جدول رقم (8) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الداخلية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
13	2.0	1.11	0.000	منخفض	27	17	9	3	2
14	2.17	1.15	0.000	منخفض	25	16	12	2	3
15	1.90	0.92	0.000	منخفض	23	19	15	1	0
16	1.86	0.75	0.000	منخفض	29	12	8	5	3
أخطاء البرامج	1.98	0.68	0.000	منخفض					

المخاطر الخارجية :–

الجداول رقم (9 – 11) تبين المتوسط الحسابي، الانحراف المعياري، مستوى التقدير، والتكرارات لتقدير أفراد العينة للمخاطر الخارجية والفقرات التي تقيسها، فقد تبين أن المتوسط العام لتقدير أفراد العينة للمخاطر الخارجية كان منخفضاً، فقد كانت معظم إجابات المبحوثين حول الفقرات المتعلقة بهذه المخاطر ضمن عدم الحدوث مطلقا بشكل يعيق أداء النظام سواء فيما يتعلق بمؤشر السرعة أو الملائمة، أو سلامة البيانات، كما تبين أن أكثر المخاطر تكراراً هي البرامج الخبيثة، بينما كان خطر الاصطياد الإلكتروني أقل هذه المخاطر حدوثاً.

وهذا يعني أن المخاطر الخارجية فقد كانت ضمن المستوى المقبول حيث كان بمتوسط حسابي بلغ 1.88 وأن وسائل الحماية المتبعة مناسبة إلى حد ما، لكن يتطلب الأمر المزيد من التوعية للمستخدمين بخصوص أضرار البرامج الخبيثة وكيفية الوقاية منها، وكذلك استخدام برامج مكافحة الفيروسات القوية والتحديث المستمر لها، بالإضافة إلى استخدام برنامج جدار حماية مناسب لمنع الاختراقات، بالإضافة إلى استخدام تقنيات التشفير لحماية البيانات في حال تعرض النظام للاختراق. وتتكون فقرات المخاطر الخارجية من كل مما يلي :-

اولا :- الاختراق الخارجي.

1. تم اختراق النظام من قبل القراصنة مما تسبب في توقف النظام عن العمل.
2. تم اختراق النظام من قبل القراصنة مما تسبب في بطء عمل النظام.
3. تم اختراق النظام من قبل القراصنة مما تسبب في الحصول على مخرجات غير صحيحة.
4. تم اختراق النظام من قبل القراصنة مما تسبب في تخريب البيانات المخزنة.

جدول رقم (9) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الخارجية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
1	1.84	1.07	0.000	منخفض	27	13	11	4	3
2	2.05	1.26	0.000	منخفض	23	19	9	5	2
3	1.47	0.64	0.000	منخفض	27	21	4	3	3
4	1.48	0.64	0.000	منخفض	36	16	4	2	0
الاختراق الخارجي	1.71	0.58	0.000	منخفض					

ثانيا :- البرامج الخبيثة.

5. توقف النظام عن العمل لفترة ما بسبب تعرضه لهجوم من البرامج الخبيثة (الفيروسات وأشباهها).
6. تعرض النظام لهجوم من البرامج الخبيثة (الفيروسات وأشباهها) مما تسبب في بطء العمل في النظام.
7. تعرض النظام لهجوم من البرامج الخبيثة (الفيروسات وأشباهها) مما تسبب في تعذر الحصول على المخرجات الملائمة

لمتخذ القرار.

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

جدول رقم (10) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الخارجية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
5	1.69	0.97	0.000	منخفض	1	3	11	16	27
6	2.53	1.39	0.000	منخفض	4	6	5	19	24
7	1.78	1.06	0.000	منخفض	2	3	7	17	29
8	2.17	1.15	0.000	منخفض	1	2	5	11	39
الاختراق الخارجي	2.04	0.59	0.000	منخفض					

ثالثا :– الاصطياد الإلكتروني.

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

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

جدول رقم (11) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الخارجية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
9	1.54	0.64	0.000	منخفض	0	3	5	19	31
10	1.56	0.75	0.000	منخفض	0	2	13	14	29
الإتلاف غير المتعمد لمعدات النظام	1.55	0.51	0.000	منخفض					

المخاطر الطبيعية :–

الجداول رقم (12 – 14) تبين المتوسط الحسابي، الانحراف المعياري ،مستوى التقدير، والتكرارات لتقدير أفراد العينة للمخاطر الطبيعية والفقرات التي تقيسها ، فقد تبين أن المتوسط العام لتقدير أفراد العينة للمخاطر الطبيعية كان منخفضاً حيث كان بمتوسط حسابي بلغ 2.09 فقد كانت معظم إجابات المبحوثين حول الفقرات المتعلقة بهذه المخاطر ضمن عدم الحدوث مطلقا بشكل يعيق كفاءة أداء النظام سواء فيما يتعلق مؤشر السرعة أو الملائمة، أو سلامة البيانات، كما تبين أن أكثر المخاطر تكراراً هي انقطاع التيار الكهربائي، ثم الأعطال الفنية، بينما كان خطر الكوارث الطبيعية أقل هذه

المخاطر حدوثاً وإعاقة لكفاءة أداء النظام. وهذا يعني أن المخاطر الطبيعية ضمن المستوى المقبول، وأن وسائل الحماية المتبعة مناسبة إلى حد ما، لكن يتطلب الأمر أن يتم استخدام أجهزة مناسبة للتزويد بالطاقة في حال انقطاعها من المصدر الرئيسي بشكل يضمن عدم توقف النظام عن العمل بسبب انقطاع التيار الكهربائي، كما يجب على المديرية قيد الدراسة أن بالتحديث المستمر لمعدات النظام من أجهزة حاسب طرفية والخادم ومعدات الشبكة، والطابعات المستخدمة، وكذلك التحديث المستمر للبرمجيات بشكل يقلل من الأعطال الفنية الناتجة عنها. وتتكون فقرات المخاطر الداخلية من كل مما يلي :-

اولا:- الأعطال الفنية.

1. توقف العمل بالنظام لفترة ما نتيجة الأعطال الفنية التي تحدث في النظام بشكل اعتيادي.
2. الحصول على مخرجات غير صحيحة من النظام بسبب الأعطال الفنية.
3. فقدان البيانات بسبب أعطال فنية تحدث للنظام.

جدول رقم (12) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الطبيعية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
1	2.48	1.11	0.000	منخفض	2	7	19	31	27
2	2.46	1.20	0.000	منخفض	8	7	9	20	14
3	1.30	0.51	0.000	منخفض	0	0	1	14	43
الأعطال الفنية	2.08	0.96	0.000	منخفض					

ثانيا :- انقطاع التيار الكهربائي.

4. فقدان البيانات بسبب الانقطاع المفاجئ للتيار الكهربائي
5. توقف العمل بالنظام لفترة ما نتيجة انقطاع التيار الكهربائي لسبب ما خارج الدائرة.

جدول رقم (13) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الطبيعية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
4	2.6	1.13	0.000	منخفض	4	1	12	23	18
5	2.48	1.01	0.000	منخفض	9	7	13	19	10
انقطاع التيار الكهربائي	2.27	0.72	0.000	منخفض					

ثالثا :– الكوارث الطبيعية.

6. فقدان البيانات بسبب كوارث طبيعية.

7. توقف العمل بالنظام لفترة ما نتيجة كوارث طبيعية.

جدول رقم (14) : المتوسطات الحسابية والانحرافات المعيارية والتكرارات لتقدير أفراد العينة للمخاطر الطبيعية

فقرات المخاطر	المتوسط الحسابي	الانحراف المعياري	قيمةsig.	مستوى التقدير	التكرارات				
					5	4	3	2	1
6	1.37	0.58	0.000	منخفض	0	0	3	12	43
7	1.72	0.76	0.000	منخفض	3	1	9	16	29
الكوارث الطبيعية	1.54	0.54	0.000	منخفض					

اختبار الفرضيات :–

الفرضية الرئيسية الأولى :-

لا يوجد فرق بين تقدير مستخدمي نظام المعلومات لمدى حدوث مخاطر داخلية تهدد أمن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن والمتوسط الفرضي (3).

لاختبار هذه الفرضية فإننا سوف نستخدم النتائج الواردة في الجداول رقم (3 – 8) التي أشارت إلى أن المتوسط العام لتقدير أفراد العينة للمخاطر الداخلية كان منخفضاً (بدلالة الوسط الحسابي) وبالتالي فإنه يتم رفض الفرضية بشكل مبدئي حيث أن متوسط تقدير أفراد العينة لمستوى المخاطر الداخلية أقل من المستوى الفرضي (3) .

ولاختبار مدى معنوية الفرق بين المتوسط الحقيقي لمتغير المخاطر الداخلية والمتوسط الفرضي (3) سيتم استخدام اختبار (T) لعينة واحدة والجدول رقم (15) يبين النتائج:

جدول رقم (15) : المتوسطات الحسابية والانحرافات المعيارية ونتائج اختبار(T) للعينة الواحدة (One Sample T-Test) لمتغير المخاطر الداخلية

التسلسل	المتغير	المتوسط	الانحراف المعياري	Tقيمة	.sigقيمة	درجات الحرية	القرار
1	الاختراق الداخلي	**1.69**	**0.54**	***-20.604***	**0.000**	**58**	**رفض**
2	الإدخال الخاطئ المتعمد للنظام	**1.57**	**0.66**	***-18.688***	**0.000**	**58**	**رفض**
3	الإدخال الخاطئ غير المتعمد للنظام	**1.84**	**1.02**	***-9.422***	**0.000**	**58**	**رفض**
4	الاستخدام الخاطئ غير المتعمد للنظام	**1.98**	**0.92**	***-9.480***	**0.000**	**58**	**رفض**
5	الإتلاف غير المتعمد لمعدات النظام	**1.67**	**0.73**	***-15.579***	**0.000**	**58**	**رفض**
6	أخطاء البرامج	**1.98**	**0.68**	***-12.855***	**0.000**	**58**	**رفض**
المخاطر الداخلية		**1.79**	**0.61**	***-25.443***	**0.000**		

نلاحظ من النتائج الواردة في الجدول رقم (15) وجود فرقاً معنوياً بين المتوسط الحقيقي لمتغير المخاطر الداخلية والأبعاد المكونة له والمتوسط الفرضي (3)، حيث أن قيمة مستوى الدلالة أقل من (0.05) لجميع الأبعاد وللمتغير ككل وبالتالي يتم رفض الفرضية وقبول الفرضية البديلة التي تعتبر وجود فرق معنوي بين المتوسط الفرضي (3) والمتوسطات الحقيقية لتقدير الأبعاد المكونة للمتغير، وهذا يعني معنوية تقدير الأفراد لكل خطر من المخاطر الداخلية والفقرات المكونة له.

الفرضية الرئيسية الثانية :-

لا يوجد فرق بين تقدير مستخدمي نظام المعلومات لمدى حدوث مخاطر خارجية أمن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن والمتوسط الفرضي (3).

لاختبار هذه الفرضية فإننا سوف نستخدم النتائج الواردة في الجداول رقم (9 - 11) التي أشارت إلى أن المتوسط العام لتقدير أفراد العينة للمخاطر الخارجية كان منخفضاً (بدلالة الوسط الحسابي) وبالتالي فإنه يتم رفض الفرضية بشكل مبدئي حيث أن متوسط تقدير أفراد العينة لمستوى المخاطر الخارجية أقل من المستوى الفرضي (3) .

ولاختبار مدى معنوية الفرق بين المتوسط الحقيقي لمتغير المخاطر الخارجية والمتوسط الفرضي (3) سيتم استخدام اختبار (T) لعينة واحدة والجدول رقم (16) يبين النتائج :-

جدول رقم (16) : المتوسطات الحسابية والانحرافات المعيارية ونتائج اختبار(T) للعينة الواحدة (One Sample T-Test) لمتغير المخاطر الخارجية

التسلسل	المتغير	المتوسط	الانحراف المعياري	Tقيمة	.sigقيمة	درجات الحرية	القرار
1	الاختراق الخارجي	**1.71**	**0.58**	**-19.123**	**0.000**	**58**	**رفض**
2	البرامج الخبيثة	**2.04**	**0.59**	**-13.905**	**0.000**	**58**	**رفض**
3	الاصطياد الإلكتروني	**1.55**	**0.51**	**-24.229**	**0.000**	**58**	**رفض**
4	**المخاطر الخارجية**	**1.88**	**0.55**	**-11.640**	**0.000**	**58**	**رفض**

نلاحظ من النتائج الواردة في الجدول رقم (16) وجود فرقاً معنوياً بين المتوسط الحقيقي لمتغير المخاطر الخارجية والأبعاد المكونة له والمتوسط الفرضي (3)، حيث أن قيمة مستوى الدلالة أقل من (0.05) لجميع الأبعاد وللمتغير ككل وبالتالي يتم رفض الفرضية وقبول الفرضية البديلة التي تعتبر وجود فرق معنوي بين المتوسط الفرضي (3) والمتوسطات الحقيقية لتقدير الأبعاد المكونة للمتغير، وهذا يعني معنوية تقدير الأفراد لكل خطر من المخاطر الخارجية والفقرات المكونة له.

الفرضية الرئيسية الثالثة :-

لا يوجد فرق بين تقدير مستخدمي نظام المعلومات لمدى حدوث مخاطر طبيعية تهدد أمن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن والمتوسط الفرضي (3).

لاختبار هذه الفرضية فإننا سوف نستخدم النتائج الواردة في الجداول رقم (12 - 14) التي أشارت إلى أن المتوسط العام لتقدير أفراد العينة للمخاطر الطبيعية كان منخفضاً (بدلالة الوسط الحسابي) وبالتالي فإنه يتم رفض الفرضية بشكل مبدئي حيث أن متوسط تقدير أفراد العينة لمستوى المخاطر الطبيعية أقل من المستوى الفرضي (3) .

ولاختبار مدى معنوية الفرق بين المتوسط الحقيقي لمتغير المخاطر الطبيعية والمتوسط الفرضي (3) سيتم استخدام اختبار (T) لعينة واحدة والجدول رقم (10) يبين النتائج :-

جدول رقم (18) : المتوسطات الحسابية والانحرافات المعيارية ونتائج اختبار(T) للعينة الواحدة (One Sample T-Test) لمتغير المخاطر الطبيعية

التسلسل	المتغير	المتوسط	الانحراف المعياري	Tقيمة	درجات الحرية	القرار
1	الأعطال الفنية	2.08	0.66	-12.012	58	رفض
2	الانقطاع المفاجئ للتيار الكهربائي	2.27	0.72	-8.708	58	رفض
3	الكوارث الطبيعية	1.54	0.54	-23.303	58	رفض
4	**المخاطر الطبيعية**	1.96	0.40	-22.139	58	رفض

نلاحظ من النتائج الواردة في الجدول رقم (18) وجود فرقاً معنوياً بين المتوسط الحقيقي لمتغير المخاطر الطبيعية والأبعاد المكونة له والمتوسط الفرضي (3)، حيث أن قيمة مستوى الدلالة أقل من (0.05) لجميع الأبعاد وللمتغير ككل وبالتالي يتم رفض الفرضية وقبول الفرضية البديلة التي تعتبر وجود فرق معنوي بين المتوسط الفرضي (3) والمتوسطات الحقيقية لتقدير الأبعاد المكونة للمتغير، وهذا يعني معنوية تقدير الأفراد لكل خطر من المخاطر الطبيعية والفقرات المكونة له.

مناقشة النتائج :-

1. أظهرت الدراسة أن مستوى تكرار المخاطر الأمنية التي تناولتها الدراسة في مديرية الجوازات العامة والاحوال المدنية في الاردن كان منخفضاً، مما يعكس قوة الإجراءات الأمنية المتبعة لتأمين نظام المعلومات سواء كانت أدوات الحماية البرمجية أو المادية أو التنظيمية.
2. بينت الدراسة أن أكثر المخاطر الأمنية تكرارا كانت المخاطر الطبيعية، وكان من أكثر تلك المخاطر تكرارا (الانقطاع المفاجئ للتيار الكهربائي)، وهذا يعكس عدم مناسبة أجهزة تزويد الطاقة التي تدعم النظام، حيث من المفترض أن تقوم هذه الأجهزة بتخزين الطاقة الكهربائية ثم إمداد النظام بالتيار الكهربائي في حال انقطاعه من المصدر الرئيسي.
3. كشفت الدراسة عن وجود بعض الأعطال الفنية التي تسببت إلى حد ما في إعاقة كفاءة أداء النظام، وهذا يعكس الحاجة إلى تحديث مكونات النظام المادية والبرمجية، حيث أن من أكثر الأسباب التي تقف وراء الأعطال الفنية التي

تصيب النظام تعود إلى عدم كفاءة المعدات المستخدمة من أجهزة حاسب ومعدات التشبيك وكذلك الطرفيات التي ترتبط بالنظام، أو أن تكون البرمجيات المستخدمة بحاجة إلى تحديث لتلائم حجم العمل في المديرية.

4. أظهرت النتائج أنه لا يوجد إعاقة لكفاءة أداء النظام في تنفيذ التعاملات الإلكترونية استنادا للمؤشرات التي استخدمتها الدراسة سببها مخاطر أمن نظام المعلومات.

5. استناداً إلى ما سبق، فإن النتيجة الرئيسية للدراسة أن نظام المعلومات المستخدم في مديرية الجوازات العامة والاحوال المدنية في الاردن يتمتع بمستوى أمن مقبول، وأن الاستجابة المناسبة للمخاطر التي تعرض لها النظام وفقاً للمدخل الذي اتبعته الدراسة هي قبول هذا المستوى من المخاطر، مع تحسين وسائل الحماية المادية والبرمجية والتنظيمية التي تعتمدها المديرية قيد الدراسة لحماية وتأمين التعاملات الإلكترونية فيها.

التوصيات :-

استنادا إلى ما سبق تقدم الدراسة التوصيات التالية :-

1. وضع خطة استراتيجية لأمن المعلومات في مديرية الجوازات العامة والاحوال المدنية في الاردن تشتمل على توظيف مدخل إدارة المخاطر الذي يرشد المعنيين بتحديد الاستجابة المناسبة للمخاطر التي تتعرض لها التعاملات الإلكترونية في المديرية محل الدراسة وفقاً للمدخل الذي اقترحته الدراسة.

2. التأكيد على وضع خطة استراتيجية ناجحة من قبل الجهات المعنية تضمن التطوير والتحديث المستمر لإجراءات الحماية التقنية والفيزيائية (المادية) والبشرية والتنظيمية لتأمين التعاملات الإلكترونية في المديرية.

3. التأكيد على وضع خطة استراتيجية لإدارة المخاطر الأمنية لنظام المعلومات بحيث تضمن الاكتشاف المبكر للمخاطر ووضع العلاج الوقائي اللازم.

4. التأكيد على ضرورة استخدام أجهزة تزويد الطاقة التي تناسب النظام وحجم العمل به، حيث تقوم هذه الأجهزة بتخزين الطاقة الكهربائية ثم إمداد النظام بالتيار الكهربائي في حال انقطاعه من المصدر الرئيسي مما يضمن عدم توقف النظام عن العمل بسبب انقطاع التيار الكهربائي.

5. التأكيد على ضرورة تحديث المعدات المرتبطة بالنظام سواء أجهزة الحاسب الصغيرة أو الكبيرة أو معدات الشبكة، أو الطرفيات، وكذلك التحديث والتطوير المستمر للبرمجيات المرتبطة بالنظام سواء كانت برامج تطبيقية، نظام إدارة قاعدة البيانات، واجهات المستخدم، بروتوكولات الشبكة، أو نظام التشغيل، بحيث يتم التقليل من الأعطال الفنية إلى أقل مستوى ممكن.

المراجع :-

البحيصي، عصام محمد (2011م). "استكشاف المخاطر التي تهدد نظم المعلومات المحاسبية المحوسبة في الشركات الفلسطينية العاملة في قطاع غزة : دراسة تطبيقية"، مجلة الجامعة الإسلامية (سلسلة الدراسات الإنسانية). 19 (1) : 1147-1177.

أبو شنب، عماد أحمد محمد (2009م). "تحليل المخاطر لمشاريع أنظمة المعلومات"، مؤتمر أمن المعلومات والحكومة الإلكترونية : ماليزيا كوالمبور ، 12-16 نيسان.

الذنيبات، معاذ، والمبيضيين، باسم (2009م). "اختبار كفاءة الخدمات الإلكترونية المقدمة في مديرية الجنسية وشؤون الأجانب وأثر ذلك في قبول المستفيدين"، المؤتمر الدولي للتنمية الإدارية : نحو أداء متميز في القطاع الحكومي، الرياض، معهد الإدارة العامة ، 14-1430/11/16 هـ ، الموافق 1-11/4/ 2009م.

الهادي، محمد (2006م). "توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية". الدورية الإلكترونية لمنظمة البوابة العربية لمكتبات والمعلومات (cybrarians journal) . متاح في : /http://www.journal.cybrarians.org

الربيحات، أمنة (2004). أثر التهديدات الأمنية في أمن المعلومات في ضوء تطبيق الحكومة الإلكترونية : دراسة ميدانية في الوزارات الأردنية، رسالة ماجستير غير منشورة، الكرك : جامعة مؤته.

Patriciu, V., and Nicolaescu, S. (2006). Security Metrics For Enterprise Information Systems. journal of applied quantitative methods. 1 (2) :151-159

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

Elky, S. (2007) "An Introduction to Information System Risk Management". SANS Institute . As part of the Information Security Reading Room.

Goh ,R. (2003) "Information Security: The Importance of the Human Element", Unpublished PhD dissertation, Singapore Campus: Preston University.

Whitman, M. E (2003) Enemy at the Gate: Threats to Information security. Communication of the ACM. 46(8): 91-95.

Lacey, D.(2011) Managing the Human Factor in Information Security: How to win over staff and influence business managers. :John Wiley & Sons.

Anton, P., and Scheiern, 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 .

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

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

Abu Mousa, A. (2006) "Investigating the perceived threats of computerized accounting information systems in developing countries: An empirical study on Saudi organizations". King Fahd University Journal, Computer and Information Science, 18: 1-26.

Warkentin, M. and Willison, R.(2009) Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems. 18:101–105.

Goodhue, D., (1991) "Security concerns of system users: a study of perceptions of the adequacy of security measures". Information and Management, 20 (1) : 13-27.

Heiser, G.(2013) "Protecting e-Government Against Attacks". In: Proceedings of Security of e-Government Systems Conference. Science and Technology Options Assessment (STOA) European Parliament, Brussels, 19 February.

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

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

Haimes, Y.Y., and Chittester, C.G. (2005) " A Roadmap for Quantifying the Efficacy of Risk Management of Information Security and Interdependent SCADA Systems". Journal of Homeland Security and Emergency Management. 2(2) Article 12.

Conrad, J. R.(2005) "Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations". 4th Annual Workshop on the Economics of Information Security, WEIS, Cambridge: Harvard University, MA, USA, June 1-3.

Rahmatian, S.(2003) Transaction Processing Systems. Encyclopedia of Information Systems. 4 :479 - 488

Gupta, V.K., Sheetlani, J., Gupta, D. and Shukla, B.D. (2012) "Concurrency Control and Security issues of Distributed Databases Transaction". Research Journal of Engineering Sciences.1(2) :70-73.

Snijder, M., and Munnichs, G.(2013) Summary of e-Passport Case Study, .In: Proceedings of Security of E-Government Systems Conference. Science and Technology Options Assessment (STOA) European Parliament, Brussels European Parliament, Brussels, 19 Feb.

Christopher, G., And Howard A. (2007) "E-Government And its Influence on Managerial Effectiveness: A survey Of Florida And Texas City Managers" , Financial Accountability & Management, 23(1):1-26.

Sekaran, U., (2006) "Research Methods for Business : A Skill Building Approach ,4th ed, Singapore : john Wiley and Sons, (Asia) pte Ltd.