

تقييم أمن نظم المعلومات في المصارف دراسة مقارنة بين مصرف الجمهورية فرع غريان ومصرف شمال أفريقيا فرع غريان

www.doi.org/10.62341/frec2410

أ. فوزي رجب رمضان مسعود

قسم الحاسب الآلي، كلية التربية غريان، جامعة غريان
fawzi.libya@gmail.com

الملخص

هدفت هذه الدراسة إلى إجراء مقارنة بين مصرفين في مدينة غريان، وذلك من ناحية أمن نظم المعلومات المصرفية، ومعرفة أهم أنواع المخاطر التي تتعرض لها نظم المعلومات في المصارف، وما تأثير هذه المخاطر على المصارف، ولتحقيق أهداف الدراسة استخدم الباحث المنهج الوصفي التحليلي وأستخدم وسيلة الاستبيان والمقابلة الشخصية كأداتين لجمع بيانات المصرفين محل الدراسة وهم المصرف التجاري فرع غريان ومصرف شمال أفريقيا فرع غريان، وقد توصلت الدراسة إلى مجموعة من النتائج ومن أهمها أن أمن نظم المعلومات في المصارف يعتبر أمن إلى حد ما، ومعرفة أنواع المخاطر التي من الممكن أن تحدث في المصارف مثل أصابه أجهزة النظام بالفيروسات والاختراق الداخلي والخارجي لنظام المعلومات في المصارف وحجم تأثير هذه المخاطر، وعلى ذلك توصي الدراسة بمجموعة من الإجراءات التي تساعد على حماية أمن نظم المعلومات في المصارف وأهمها أنه يجب تنفيذ اختبارات دورية للنظام للكشف عن نقاط الضعف والثغرات في النظام ومعالجتها، ويجب تحديث برامج الحماية من الفيروسات، وتنزيل البرامج الموثوق فيها، ويجب توعية وتدريب الموظفين على أمن نظم المعلومات.

الكلمات المفتاحية: نظم المعلومات، أمن نظم المعلومات، أمن نظم المعلومات المصرفية، مخاطر نظم المعلومات المصرفية.

Evaluating the security of information systems in banks

Comparative study between the Jumhouria Bank and North Africa bank in Gharyan city

Fawzi rajab ramadan masoud

Department of computer, College of Education, University of Gharyan,
Libya

fawzi.libya@gmail.com

Abstract

This study aimed to compare the information system security in two banks in Gharyan city and to numerous challenges that face banks, which can severely affect customer trust and financial stability.

In order to achieve the objectives of this study, the researcher used the analytical descriptive method relying on the questionnaire and interviews as main tools to collect banking data collection for the two banks, which they are Jumhouria Bank of Gharyan, and North Africa bank of Gharyan.

This study came up with a series of findings includes the protection the banking information system security is quite safe. As well as recognize the types of risks that may occur in these banks such as infecting the system's devices with viruses also internal and external penetration of banks information system and how these risks impact, as result of that, this study recommends a multi-layered approach including utilize automated tools to continuously scan for known vulnerabilities in applications and systems. This helps in early detection of potential they can be exploited. In addition, banks must effectively update programs that protect against viruses and download only reliable antivirus programs moreover banks must continuous training for employees on security information system.

Keywords: Information systems, Information systems security, Security of banking information systems, Risks of banking information systems.

المقدمة

نظراً للتطور الهائل والسريع في نظم الاتصالات وتكنولوجيا المعلومات وتطبيقاتها والتي أصبحت العنصر الأساسي في أداء معظم الأنشطة المختلفة للمنظمات ومنها القطاع المصرفي، الذي أدى إلى ابتكار أساليب جديدة من عمليات الغش والتزوير تعتمد بشكل أساسي على استخدام تكنولوجيا المعلومات، وفي ظل انتشار هذه المخاطر، أصبح لأمن المعلومات أهمية قصوى لدى المصارف وذلك لتوفير المتطلبات الأمنية لحماية أصوله المعلوماتية والحاجة إلى وجود نظام معلومات محاسبي آمن، ومنه يعتبر أمن نظم المعلومات من المواضيع المهمة التي أثاره اهتمام الباحثين في مجال الاقتصاد وخاصة في المجال المصرفي، ولهذا السبب أتت هذه الدراسة للتعرف على واقع أمن المعلومات في المصرفين محل الدراسة والمخاطر التي من الممكن حدوثها وتأثير هذه المخاطر مع تقييم أمن المعلومات في المصرفين

مشكلة الدراسة:

لقد ساهم استخدام نظم المعلومات الالكترونية في المصارف إلى تحسين جودة العمل، ولكن في نفس الوقت أدى إلى تطور التحديات في العمل في تلك البيئة وخاصة من ناحية زيادة تنوع وتطور المخاطر في المصارف، ومن خلال هذه الدراسة يحاول الباحث تقييم أمن المعلومات في المصارف حالة الدراسة، والتعرف على أنواع المخاطر وما مدى تأثير هذه المخاطر على المصارف.

أهداف الدراسة:

تهدف هذه الدراسة إلى:

1. التعرف على واقع أمن نظم المعلومات في المصارف التجارية في مدينة غريان
2. تقييم أمن نظم المعلومات في المصارف محل الدراسة

3. تحديد أنواع المخاطر التي تؤثر على نظم المعلومات المحاسبية في المصارف

أهمية الدراسة:

تعتبر هذه الدراسة مصدراً مهماً في معرفة أنواع المخاطر في النظام المحاسبي، ومعرفة الواقع الفعلي لأمن نظام المعلومات المحاسبية في المصارف محل الدراسة.

تساؤلات الدراسة:

1. هل يوجد تفاوت في فعالية أمن نظم المعلومات بين المصارف محل الدراسة.
2. ما هي أنواع المخاطر التي يمكن حدوثها على نظام المعلومات في المصارف محل الدراسة وما مدى الاختلاف بينهم.
3. هل يوجد اختلاف في تأثير المخاطر على المصارف.

منهجية البحث:

لقد استخدم الباحث المنهج الوصفي التحليلي لتحقيق أهداف الدراسة، وذلك عن طريق القيام بالخطوات التالية:

1. مراجعة الدراسات السابقة كمصدر ثانوي للبيانات وذلك من خلال الكتب والمجلات المحكمة والرسائل والاطروحات الجامعية.
2. استخدام وسائل جمع البيانات كمصدر أولي للبيانات وتمثلت في الآتي:
 - أ. استخدم الباحث أداة الدراسة الاستبيان لجمع البيانات، ويتكون مجتمع الدراسة من رؤساء الأقسام والموظفين العاملين في المصارف التجارية محل الدراسة والبالغ عددهم 39 من مصرف الجمهورية و 34 من مصرف شمال افريقيا ونظراً لمحدودية حجم مجتمع الدراسة فقد قام الباحث بحصر شامل لجميع مفردات مجتمع الدراسة، وتم توزيع الاستبيان عليهم وبعد المتابعة تم استعادة (36) من مصرف الجمهورية من بينها (3) غير صالحة للتحليل

الاحصائي، وعليه أصبح (33) ورقة صالحة للاستبيان بنسبة 84.6% من حجم العينة، وتم استعادة (31) من مصرف شمال أفريقيا من بينها (1) غير صالحة للتحليل الاحصائي، وعليه أصبح (30) ورقة صالحة للاستبيان بنسبة 88% من حجم العينة

ب. تصميم نموذج للمقابلة الشخصية حيث أجريت المقابلة مع مديري ورؤساء الاقسام وخبراء المصارف ذوي تخصص الحاسب الآلي.

حدود البحث:

بدأ الباحث دراسته في الفترة من 1-1-2023 وأنتهى في تاريخ 01-12-2023 وكانت على بعض المصارف في مدينة غريان وهم مصرف الجمهورية ومصرف شمال أفريقيا

الأدب النظري والدراسات السابقة:

أولاً: الأدب النظري:

تحاول هذه الدراسة التعرف على مفهوم ومكونات أمن نظم المعلومات والأخطار التي يمكن أن تتعرض لها نظم المعلومات والحماية من هذه الأخطار.

1 - مفهوم الأمن المعلوماتي

من الممكن تعريف أمن المعلومات Information Security بأنه مجموعة من الإجراءات والتدابير الوقائية التي تستخدم سواء في المجال التقني أو الوقائي للحفاظ على المعلومات والأجهزة والبرمجيات إضافة إلى الإجراءات المتعلقة بالحفاظ على العاملين في هذا المجال.

حيث يجب استخدام مجموعة من التدابير الوقائية في المجالين الإداري و الفني لحماية مصادر البيانات من أجهزة و برمجيات و بيانات من التجاوزات أو التداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلسل أو الإجراءات الخاطئة المستخدمة من قبل إدارة المصادر المعلوماتية

، فضلا عن إجراءات مواجهة الأخطار الناتجة عن الكوارث الطبيعية المحتملة التي تؤدي إلى فقدان بعض المصادر، و من ثم التأثير على نوع و مستوى الخدمة المقدمة.

2- الأخطار التي يمكن أن تتعرض لها أنظمة المعلومات المعتمدة على الحاسب

لقد أصبح اختراق أنظمة المعلومات و نظم الشبكات و المواقع المعلوماتية خطراً يقلق العديد من المنظمات في السنوات الأخيرة و مع مرور الزمن نجد أن على الرغم من سبل الحماية التي تتبعها المنظمات ، إلى أن هناك ارتفاعا واضحا في معدل الإختراقات مع تنوع الوسائل المستخدمة في الإختراق أما عن طبيعة الأخطار التي يمكن أن تواجهها نظم المعلومات فهي عديدة ، فالبعض منها قد يكون مقصود كسرقة المعلومات أو ادخال الفيروسات و غيرها و هي الأشد ضررا على نظم المعلومات و يكون مصدرها أحيانا من داخل أو خارج المنظمة ، و قد يصعب أحيانا التنبؤ بالدوافع العديدة للأشخاص الذين يقومون بها ، أما البعض الآخر فقد يكون غير مقصود كالأخطاء البشرية و الكوارث الطبيعية و يمكن تصنيف الأخطار المحتملة التي يمكن أن تتعرض لها نظم المعلومات إلى ثلاث فئات :

أ . الأخطاء البشرية Humane Errors

و هي التي يمكن أن تحدث أثناء البرمجة أو تجميع البيانات أو أثناء إدخالها إلى النظام ، أو في عمليات تحديد الصلاحيات للمستخدمين ، و تشكل هذه الأخطاء الغالبية العظمى للمشاكل المتعلقة بأمن و سلامة نظم المعلومات في المنظمات .

ب . الأخطار البيئية Environmental Hazard

و هذه تشمل الزلازل و العواصف و الفيضانات و الأعاصير و المشاكل المتعلقة بأعطال التيار الكهربائي و الحرائق إضافة إلى المشاكل القائمة في تعطل أنظمة التكييف و التبريد و غيرها ، و تؤدي هذه الأخطار إلى تعطل

عمل هذه التجهيزات و توقفها لفترات طويلة نسبيا لإجراء الإصلاحات اللازمة و استرداد البرمجيات و قواعد البيانات .

ج. الجرائم المحوسبة Computer Crime

تمثل هذه تحديا كبيرا لإدارة نظم المعلومات لما تسببه من خسارة كبيرة و بشكل عام يتم التمييز بين ثلاثة مستويات للجرائم المحوسبة و هي:

– سوء الإستخدام لجهاز الحاسوب : و هو الإستخدام المقصود الذي يمكن أن يسبب خسارة للمنظمة.

– الجريمة المحوسبة: و هي عبارة عن سوء استخدام لأجهزة الحاسوب بشكل غير قانوني يؤدي إلى ارتكاب جريمة يعاقب عليها القانون خاصة بجرائم الحاسوب .

– الجرائم المتعلقة بالحواسيب: و هي الجرائم التي تستخدم فيها الحواسيب كأداة لتنفيذ الجريمة.

3- الحماية من الأخطار :

تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة والصعبة و التي تتطلب من إدارة نظم المعلومات الكثير من الوقت و الجهد و الموارد المالية و ذلك للأسباب التالية:

أ. العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات.

ب. توزع الموارد المحوسبة على العديد من المواقع التي يمكن أن تكون أيضا متباعدة.

ج. وجود التجهيزات المحوسبة في عهدة أفراد عديدين في المنظمة وأحيانا خارجها.

د. صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية .

هـ. التقدم التقني السريع يجعل الكثير من وسائل الحماية متقدمة من بعد فترة وجيزة من استخدامها.

و. التأخر في اكتشاف الجرائم المحوسبة مما لا يتيح للمنظمة امكانية التعلم من التجربة و الخبرة المتاحة.
ز. تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها .

هذا و تقع مسؤولية وضع خطة الحماية للأنشطة الرئيسية على مدير نظم المعلومات في المنظمة على أن تتضمن هذه الخطة إدخال وسائل الرقابة التي تضمن تحقيق ما يلي :

- الوقاية من الأخطار غير المتعمدة .
 - إعاقة أو صنع الأعمال التخريبية المتعمدة .
 - اكتشاف المشاكل بشكل مبكر قدر الإمكان .
 - المساعدة في تصحيح الأعطال و استرجاع النظام .
- و يمكن تصميم نظام الرقابة ضمن عملية تطوير نظام المعلومات و يجب أن يركز هذا النظام على مفهوم الوقاية من الأخطار ، و يمكن أن يصمم لحماية جميع مكونات النظام بما فيها التجهيزات و البرمجيات و الشبكات .

ثانياً: الدراسات السابقة:

نظراً لأهمية هذا الموضوع فقد أجريت العديد من الدراسات والبحوث لدراسة هذا الموضوع، وما زالت الدراسات مستمرة حتى الآن للتعرف على المخاطر المتجددة والبحث عن حلول لمعالجة القصور في الأنظمة المصرفية وذلك للتغلب على هذه المخاطر.

ومن أهم هذه الدراسات كانت دراسة سارة رحالي (2017)، بعنوان تقييم الأمان المصرفي من منظور العميل دراسة عينة من البنوك الجزائرية بولاية عين الدفلى وهدفت هذه الدراسة إلى معرفة الأمان المصرفي، وتوضيح العوامل المؤثرة على مدى شعور العميل بالأمان عند اختياره للمصرف، وتوصلت الدراسة إلى أهمية الأمان المصرفي بالنسبة للمصرف والعملاء و تتمثل أهم

العوامل المؤثرة على شعور العميل بالأمان المصرفي في رأس المال، الربحية، السيولة، جودة الخدمات المصرفية، الأداء التسويقي والسياسة الائتمانية. وقدم حسين الشمالي في عام (2017)، دراسة بعنوان أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن هدفت هذه الدراسة إلى تعرف بأمن المعلومات وسريتها وأثرها في الأداء المصرفي في البنوك العاملة في الأردن وأظهرت نتائج الدراسة أن مستوى ممارسة أمن المعلومات وسريتها في البنوك العاملة في الأردن من حيث الأهمية النسبية كانت مرتفعة، ووجود أثر ذي دلالة إحصائية لأمن المعلومات وسريتها (الحماية المادية، حماية الأفراد، الحماية البرمجية) في الأداء المصرفي في البنوك العاملة في الأردن.

وفي عام (2020) قدم كل من فراس شحادة ومحمد رجب، دراسة بعنوان واقع أمن وسرية المعلومات الإلكترونية في بنك فلسطين "دراسة حالة" هدفت هذه الدراسة إلى تقييم واقع أمن وسرية المعلومات الإلكترونية في البنك من خلال التعرف على مدى توافر مقومات حماية البنية التحتية لأمن المعلومات، وتوصلت الدراسة إلى أنه يوجد فروق ذات دلالة إحصائية في استجابات أفراد العينة حول واقع إدارة أمن المعلومات في بنك فلسطين تعزي لمتغير الدورات التدريبية، كما يتوفر لدى بنك فلسطين مقومات بنية تحتية مقبولة بمحاورها الثلاثة (المادية، البرمجية والأفراد) بنسبة متفاوتة.

كما قدم راميار رازكار احمد في عام (2021)، دراسة بعنوان دور نظام المعلومات المحاسبية الإلكترونية في تعزيز أمن المعلومات المالية (دراسة تطبيقية في شركة بردبار للصرافة فرع محافظة أربيل)، هدفت الدراسة إلى تقييم فاعلية نظام المعلومات المحاسبية الإلكترونية في تعزيز أمن ورقابة المعلومات المالية في شركة بردبار للصرافة، وتوصلت الدراسة إلى أهم الاستنتاجات منها أنه لدى الشركة نظام متكامل لأمن المعلومات ونظام متكامل للرقابة لأمن المعلومات.

كما قدم كلاً من نبيلة قرزيز و محمد زيدان عام (2022)، دراسة بعنوان دور أمن المعلومات في تحقيق جودة الخدمات المصرفية- دراسة حالة القرض الشعبي الجزائري بالشلف وهدفت هذه الدراسة إلى إبراز مدى مساهمة أمن المعلومات في تحقيق جودة الخدمات المصرفية بالقرض الشعبي الجزائري على مستوى المديرية الجهوية بالشلف، وتوصلت الدراسة إلى وجود أثر ذو دلالة احصائية بين أمن المعلومات وجودة الخدمات المصرفية، كما أظهرت النتائج عدم وجود فروق ذات دلالة احصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لجودة الخدمات المصرفية تعزى لمتغيرات (العمر، المستوى التعليمي و الخبرة المهنية).

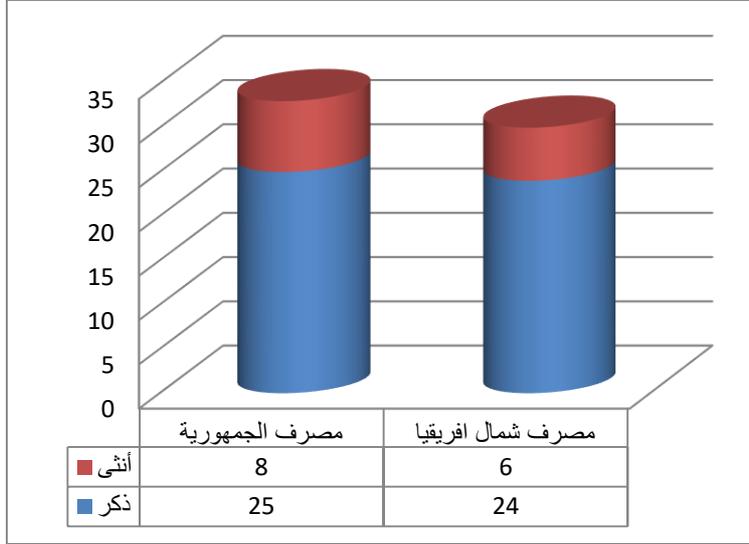
تتشابه هذه الدراسة مع الدراسات السابقة في أنها تدرس أمن نظم المعلومات في المصارف، وتختلف من حيث أنها تعرضت إلى بعض الجوانب التي لم تدرسها الدراسات السابقة مثل مقارنة أمن نظم المعلومات بين المصارف في الليبية وأنواع المخاطر وتأثيرها على المصارف الليبية.

تحليل الدراسة الحالية:

خصائص مفردات عينة الدراسة:

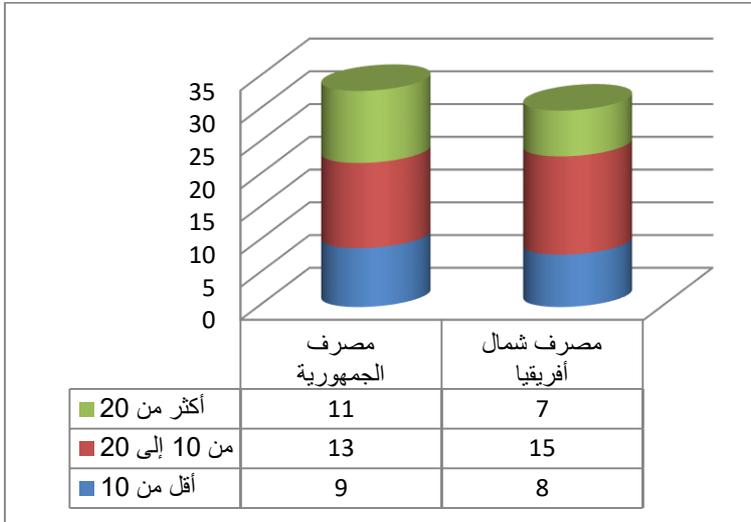
استهدفت الدراسة موظفي مصرف الجمهورية ومصرف شمال أفريقيا والشكل رقم (1) يوضح التمثيل البياني لمفردات عينة الدراسة حسب الجنس.

تم استلام الورقة بتاريخ: / 2024م وتم نشرها على الموقع بتاريخ: / 2024م



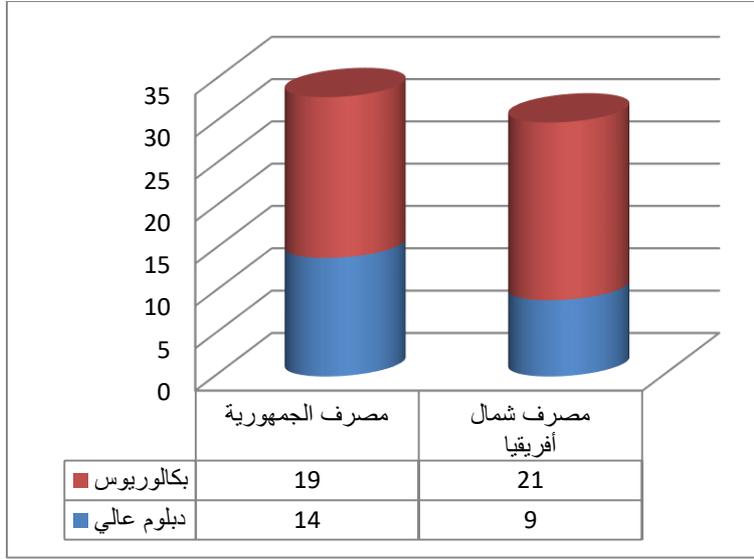
شكل (1) التمثيل البياني لمفردات عينة الدراسة حسب الجنس

والشكل رقم (2) يوضح التمثيل البياني لمفردات عينة الدراسة حسب خبرة سنوات العمل.



شكل (2) التمثيل البياني لمفردات عينة الدراسة حسب خبرة سنوات العمل

والشكل رقم (3) يوضح التمثيل البياني لمفردات عينة الدراسة حسب المؤهل العلمي



شكل (3) التمثيل البياني لمفردات عينة الدراسة حسب المؤهل العلمي

مناقشة تساؤلات الدراسة:

السؤال الأول : هل يوجد تفاوت في فعالية أمن نظم المعلومات بين المصارف محل الدراسة ؟

ويوضح الجدول رقم (1) مقارنة بين نظام الحماية الالكترونية لمصرف الجمهورية فرع غريان ومصرف شمال أفريقيا فرع غريان وذلك بحساب المتوسط الحسابي والانحراف المعياري لإجابات المشاركين في الدراسة.

جدول (1) مقارنة بين نظام الحماية الالكترونية لمصرف الجمهورية فرع غريان ومصرف

شمال أفريقيا فرع غريان

مصرف شمال افريقيا			مصرف الجمهورية			العبارة	م
الانحراف المعياري	المتوسط	الانحراف المعياري	المتوسط	الانحراف المعياري	المتوسط		
3.7		3.7					

تم استلام الورقة بتاريخ: / 2024م وتم نشرها على الموقع بتاريخ: / 2024م

7	.91548	2.1333	8	0.7378	1.9	يوجد في المصرف سياسة و إجراءات مكتوبة لأمن المعلومات	1
14	.83381	1.4667	13	04520.	11.	تحصلت على دورات تدريبية في مجال أمن المعلومات	2
6	.86189	2.2000	9	0.7888	1.8	توجد أنظمة (كاميرات مراقبة، أجهزة إنذار الحرائق ، ... إلخ) لحماية مكونات نظم المعلومات.	3
5	.79881	2.2667	6	0.7888	2.2	يتم استخدام برامج الحماية ضد الفيروسات	4
9	.88372	1.9333	6	0.7888	2.2	يتم تحديث برامج الحماية من الفيروسات دورياً	5
3	.63994	2.5333	5	0.6749	2.3	لا يسمح بتنصيب البرامج الغير أصلية	6
4	.91026	2.4000	1	07830.	3.0	يمنع الدخول لمواقع الأنترنت بالأجهزة المرتبطة بالجهاز الرئيسي (ال خادم المركزي)	7
1	.70373	2.7333	1	07830.	3.0	توجد كلمة مرور لكل مستخدم على حدة	8
2	.72375	2.6667	3	0.6992	2.6	يتم تغيير كلمة المرور باستمرار (حوالي كل 45 يوم)	9
11	.89974	1.6667	11	0.6749	1.3	يوجد شخص آخر يعرف كلمة المرور الخاصة بك	10
13	.91548	1.5333	12	0.6324	1.2	تحتفظ بكلمة المرور الخاصة بك مكتوبة	11

تم استلام الورقة بتاريخ: / 2024م وتم نشرها على الموقع بتاريخ: / 2024م

12	.82808	1.6000	11	0.6749	1.3	تستخدم في كلمة المرور الخاصة بك لأكثر من برنامج	12
14	.73679	1.4000	12	0.6324	1.2	توجد تقنية للدخول إلى النظام غير كلمة المرور	13
5	.88372	2.2667	4	0.6992	2.4	يستطيع الزملاء الموظفون استخدام جهاز الحاسب الآلي الخاص بك في العمل	14
4	.73679	2.4000	3	0.5164	2.6	يستطيع أي موظف الدخول إلى مكتبك	15
9	.88372	1.9333	10	0.6749	1.7	يتم التعامل بالثقة مع باقي الموظفين في إجراءات العمل	16
10	.83381	1.8667	9	0.6324	1.8	يتم عمل صيانة دورية للأجهزة	17
12	.73679	1.6000	7	0.7378	2.1	الصيانة الدورية تتم مرة كل سنة	18
12	.82808	1.6000	6	0.9189	2.2	يقوم بالصيانة الدورية للأجهزة موظف من داخل المصرف	19
9	.96115	1.9333	2	0.6749	2.7	يقوم بالصيانة الطارئة للأجهزة موظف من داخل المصرف	20
5	.88372	2.2667	5	0.6749	2.3	يتم التخلص من الأوراق الغير مرغوب فيها مع القمامة خارج المصرف	21
10	.83381	1.8667	12	0.6324	1.2	توجد أجهزة عدم انقطاع التيار الكهربائي UBS في الأجهزة	22
8	.92582	2.0000	4	0.5164	2.4	يتم معاقبة الموظف الذي ينتهك إجراءات	23

						سياسة أمن المعلومات في المصرف	
	0.2231	2.0116		0.1680	2.017	المتوسط العام للمحور الاول	

وفق الجدول رقم (1) نلاحظ أن المصرفان (مصرف الجمهورية ومصرف شمال أفريقيا) يتفقان على أنه توجد كلمة مرور لكل مستخدم على حدة ولكن يختلفان في العبارة رقم 7 حيث يمنع مصرف الجمهورية الموظفين الدخول إلى مواقع الانترنت باستخدام الاجهزة المرتبطة بالجهاز الرئيسي (الخادم المركزي) أما مصرف شمال أفريقيا فمن الممكن الدخول إلى مواقع الانترنت عبر أجهزة النظام.

أتقنا المصرفان على أنهما لم يتحصل الموظفون على دورات تدريبية في مجال أمن المعلومات.

السؤال الثاني: ما هي أنواع المخاطر التي يمكن حصولها على نظام المعلومات في المصارف محل الدراسة وما مدى الاختلاف بينهم؟

ويوضح الجدول رقم (2) أنواع المخاطر التي يمكن حصولها على نظام المعلومات في المصارف محل الدراسة وما مدى الاختلاف بينهم وذلك بحساب المتوسط الحسابي والانحراف المعياري لإجابات المشاركين في الدراسة.

جدول (2) أنواع المخاطر التي يمكن حصولها على نظام المعلومات في مصرف الجمهورية فرع غريان ومصرف شمال أفريقيا فرع غريان

م	العبارة	مصرف الجمهورية			مصرف شمال افريقيا		
		المتوسط	الانحراف المعياري	المتوسط	الانحراف المعياري	المتوسط	الانحراف المعياري
1	يسمح بتنزيل برامج غير مصرح بها في الأجهزة	1.2	0.4216	1.5333	.91548	5	5

تم استلام الورقة بتاريخ: / 2024م وتم نشرها على الموقع بتاريخ: / 2024م

2	.83381	1.8667	2	0.8432	1.6	يتم توصيل الأجهزة الخاصة (USB) ، الهواتف الذكية ، الأجهزة المحمولة ، الأجهزة اللوحية) بشبكة أو أجهزة المصرف .	2
5	.91548	1.5333	5	0.6324	1.2	سرقة معدات الشبكة و أجهزة الحاسوب ووسائط التخزين	3
1	.77460	2.2000	1	0.5270	2.5	إصابة الأجهزة بالفيروسات	4
5	.91548	1.5333	6	0.3162	1.1	وجود برامج لغرض التجسس في الاجهزة	5
6	.83381	1.4667	2	0.6992	1.6	التعدي و تخريب معدات الشبكة	6
8	.56061	1.2000	4	0.8432	1.4	احترق المكاتب	7
7	.82808	1.4000	3	0.7071	1.5	اختراق الاجهزة من داخل المصرف (من الموظفين)	8
7	.82808	1.4000	6	0.3162	1.1	اختراق الاجهزة من خارج المصرف	9
3	.77460	1.8000	4	0.6992	1.4	التعرض لكوارث طبيعية مثل (الحرائق ، الفيضانات)	10
4	.81650	1.6667	3	0.8498	1.5	التعرض لهجوم إرهابي	11
2	.91548	1.8667	2	0.8432	1.6	تعديل إعدادات أجهزة الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع	12
	0.5038	1.6222		0.3094	1.475	المتوسط العام للمحور الثاني	

أنتقنا المصرفان على أن أكثر المخاطر التي يمكن أن تحدث وهي إصابة الأجهزة بالفيروسات.

كما أنتقنا على أن من المخاطر التي تحدث بكثرة في المصارف هي توصيل الأجهزة الأخرى مثل الهواتف الذكية و USB ... الخ بأجهزة المصرف والشبكة.

وكان الاختلاف بينهم في ارتفاع احتمالية التعدي وتخريب معدات الشبكة في مصرف الجمهورية عكس مصرف شمال أفريقيا الذي كان احتمال حدوثها ضعيف.

السؤال الثالث : هل يوجد أختلاف في تأثير المخاطر على المصارف ؟
ويوضح الجدول رقم (3) وجه الاختلاف في تأثير المخاطر على المصارف محل الدراسة وذلك بحساب المتوسط الحسابي والانحراف المعياري لإجابات المشاركين في الدراسة.

جدول (3) اختلاف تأثير المخاطر على مصرف الجمهورية فرع غريان ومصرف شمال أفريقيا فرع غريان

م	العبارة	مصرف الجمهورية			مصرف شمال افريقيا		
		المتوسط	الانحراف المعياري	الرتبة	المتوسط	الانحراف المعياري	الرتبة
1	يضعف من مستوى التنافس مع المصارف الأخرى	2.5	0.7071	2	2.0667	.79881	2
2	سرقة الأسرار أو المعلومات التجارية في المصرف	1.7	0.8232	5	1.8000	.86189	4
3	صعوبة تحديد مستوى الأثر الذي يمكن أن تحدثه تلك التهديدات	2.7	0.4830	1	1.6667	.61721	6
4	تحقق خسائر مالية في حالة اختراق أنظمة المعلومات	2.4	0.5164	3	2.4667	.74322	1
5	سرقة المعلومات الخاصة بحسابات الزبائن	2.1	0.8756	4	1.7333	.96115	5
6	إتلاف المعلومات الخاصة بحسابات الزبائن	1.4	0.6992	7	1.4667	.83381	7
7	تغيير المعلومات الخاصة بحسابات الزبائن	1.5	0.8498	6	1.3333	.72375	8

3	.84515	2.0000	1	0.4830	2.7	يفقد الزبائن الثقة بالمصرف	8
	41152.	1.8167		0.3726	2.125	المتوسط العام للمحور الثالث	

الاختلاف كان في أن مصرف الجمهورية يرى أن أكبر تأثير لحدوث المخاطر على النظام المصرفي هو أن يفقد الزبائن الثقة بالمصرف مع صعوبة تحديد مستوى التأثير.

بينما مصرف شمال أفريقيا فإنه يرى أن أكثر تأثير لحدوث المخاطر هي تحقيق خسائر مالية وذلك في حالة اختراق نظام المعلومات. وانتقنا المصرفان على أنه لو حدث اختراق في المصرف فإنه لن تتأثر المعلومات الخاصة بحسابات الزبائن سواء بالتغيير أو بالأتلاف.

النتائج والتوصيات:

أولاً نتائج الدراسة:

توصلت هذه الدراسة إلى مجموعة من النتائج والجدول رقم (4) يوضح أوجه التشابه والاختلاف بين المصرفين محل الدراسة من ناحية واقع أمن نظم المعلومات المصرفية.

جدول (4) مقارنة أمن نظم المعلومات بين مصرف الجمهورية فرع غريان ومصرف شمال

أفريقيا فرع غريان

مصرف الجمهورية فرع غريان	مصرف شمال أفريقيا فرع غريان	البيان
أمن إلى حد ما	أمن إلى حد ما	واقع أمن نظم المعلومات في المصرف
توجد ولكن لم يتم اطلاع الموظفين عليها	توجد ولكن لم يتم اطلاع الموظفين عليها	سياسة خاصة بأمن المعلومات في المصرف
ضعيفة	ضعيفة	مستوى كلمة المرور
نعم	نعم	يتم استخدام برامج الحماية ضد الفيروسات
نعم	نعم	يتم تحديث البرامج وأنظمة التشغيل

تخزين البرامج الغير الاصلية في الاجهزة	نعم ولكن برامج غير أساسية	نعم ولكن برامج غير أساسية
استقبال الضيوف والزبائن في المكاتب	حالات قليلة	ممنوع
توصيل النقالات و USB إلى أجهزة الحاسب الخاصة بالمصرف	ممنوع، وتم رصد توصيل حالات قليلة جدا	ممنوع، ولم يرصد أي حالة توصيل للأجهزة
توعية وتدريب الموظفين في المصرف على أمن نظم المعلومات	لا توجد أي دورات	لا توجد أي دورات
الدخول إلى مواقع الانترنت باستخدام الاجهزة المرتبطة بالنظام	مسموح باستخدام جهاز واحد فقط، أما باقي الاجهزة ممنوع	ممنوع
توجد أنظمة (كاميرات مراقبة، أجهزة إنذار الحرائق ، ... إلخ) لحماية مكونات نظم المعلومات.	نعم توجد	نعم توجد
الصيانة الطارئة للأجهزة تتم داخل المصرف	حالات قليلة تتم داخل المصرف	في المتوسط تتم داخل المصرف
يتم تغيير كلمة المرور دورياً	نعم	نعم

ثانياً الخلاصة:

حاول الباحث من خلال هذه الدراسة توضيح مفهوم الأمن المعلوماتي والمخاطر التي يمكن أن تتعرض لها أنظمة المعلومات المعتمدة على الحاسب وحماية أنظمة المعلومات من الأخطار، أما الدراسة الميدانية فحاول الباحث تحليل واقع أمن نظم المعلومات في المصرفين محل الدراسة وتوصل إلى النتائج التالية:

1. أمن نظم المعلومات في المصرفين محل الدراسة يعتبر آمن إلى حد ما.
2. يوجد بعض من الموظفين لم يطلعوا على سياسة أمن المعلومات في كل من المصرفين محل الدراسة، الذي يجعلهم أقل التزام بأمن نظم المعلومات.
3. توجد قواعد خاصة بكلمة المرور في كل من المصرفين محل الدراسة ولكن يوجد بعض من الموظفين في المصرفين يخالفون هذه القواعد مما يعرض المصرفين إلى احتمالية حدوث اختراق داخلي.

4. يوجد بعض من موظفي مصرف شمال افريقيا يوصلون بعض الأجهزة مثل النقالات و USB إلى أجهزة النظام وهذا يزيد من احتمالية أصابه أجهزة النظام بالفيروسات، أما موظفي مصرف الجمهورية فلا يوصلون أي جهاز بأجهزة النظام وهذا الذي يقلل من مخاطر أصابه الأجهزة بالفيروسات.
5. إدارة مصرف الجمهورية تمنع دخول الضيوف إلى المكاتب وهذا يجعل النظام أكثر أماناً، أما مصرف شمال أفريقيا فتوجد به بعض حالات استقبال للضيوف في المكاتب وهذا يزيد من احتمالية حدوث اختراق خارجي للنظام وأن كان هذا الاحتمال ضعيف.

ثالثاً التوصيات:

- 1) يجب تنفيذ اختبارات دورية للنظام للكشف عن نقاط الضعف والثغرات في النظام ومعالجتها.
- 2) يجب تحديث برامج الحماية من الفيروسات.
- 3) يجب تنزيل البرامج الموثوق فيها فقط وعدم تنزيل البرامج الغير أصلية.
- 4) يجب توعية وتدريب الموظفين في المصرفين على أمن نظم المعلومات.
- 5) يجب توثيق سياسة أمن المعلومات في المصرفين واعطائها للموظفين والزام الموظفين بتطبيقها وعدم مخالفتها.
- 6) يجب معاينة من يتخلف عن تنفيذ سياسة أمن المعلومات في المصرف.
- 7) إنشاء إدارة أو مكتب خاص بأمن نظم المعلومات ويكون تخصصهم حاسب آلي في كلا المصرفين.
- 8) يجب أتباع قواعد إنشاء كلمات المرور والتي تكون بالشكل التالي:
 - i. استخدم ستة حروف على الأقل
 - ii. استخدم حروف وأرقام
 - iii. استخدم أحرفا خاصة إذا كان بالإمكان مثل (@#\$%&... الخ)
 - iv. غير كلمة السر بشكل دوري (مثلا مرة كل ثلاث أشهر)
 - v. لا تستخدم الكلمات الشائعة

المراجع:

- حسين علي قاسم الشمالي، (2017)، "أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن"، العدد 7، جامعة القدس المفتوحة، فلسطين.
- ذيب بن عايض الفحطاني، (2015)، "أمن المعلومات"، مدينة الملك عبدالعزيز للعلوم والتقنية، السعودية.
- راميار رازكار احمد، (2021)، "دور نظام المعلومات المحاسبية الالكترونية في تعزيز أمن المعلومات المالية (دراسة تطبيقية في شركة بردبار للصرافة فرع محافظة أربيل)"، المجلة الدولية للعلوم، العدد 24، العراق.
- سارة رحالي، (2017)، "تقييم الأمان المصرفي من منظور العميل دراسة عينة من البنوك الجزائرية بولاية عين الدفلى"، جامعة الجيلالي - عين الدفلى، الجزائر.
- فراس محمد شحادة، محمد رجب بدر، (2020)، " واقع أمن وسرية المعلومات الإلكترونية في بنك فلسطين"، المؤتمر الدولي الاول في تكنولوجيا المعلومات والاعمال، جامعة غزة، فلسطين.
- نبيلة قرزيز، محمد زيدان (2022)، "دور أمن المعلومات في تحقيق جودة الخدمات المصرفية- دراسة حالة القرض الشعبي الجزائري بالشلف"، مجلة الاقتصاد والمالية، المجلد 8، العدد 1، جامعة الشلف، الجزائر.
- ندى اسماعيل جبوري، (2011)، "حماية أمن أنظمة المعلومات دراسة حالة في مصرف الرافدين فرع شارع فلسطين"، مجلة تكريت للعلوم الإدارية والاقتصادية، العدد 21، جامعة تكريت، العراق.