Millennium Journal of Economic and Administrative Sciences

Journal homepage: http://www.milljournals.org

إدارة مخاطر الأمن السيبراني في البنوك الأردنية

الدكتور احمد محمود الزيود
بنك لبنان والمهجر – المملكة الأردنية الهاشمية
https://doi.org/10.47340/mjeas.v1i1.2020

الملخص:

ناقش البحث مفهوم الأمن السيبراني من كافة الجوانب، إدارة المخاطر السيبرانية، وأنواع التهديدات ومجالاتها. كما ناقش الأدوات المستخدمة في إدارة وتقييم المخاطر في البنوك الأردنية والتي تهدف إلى المحافظة على سلامة البنوك و تدعيم مركزها، والتحقق من سلامة إجراءاتها، والمحافظة على أمن معلوماتها وبياناتها وأجهزة حفظ المعلومات. بيّن البحث أهمية إدارة مخاطر الأمن السيبراني في البنوك الأردنية وضرورة توضيح السياسات المتبعة بخصوص الأمن السيبراني بشكل أدق، بالإضافة إلى نشر مزيد من الإيضاحات في التقارير السنوية بخصوص حجم التهديدات السيبرانية وقدرة البنوك الأردنية على معالجتها.

الكلمات المفتاحية: الأمن السيبراني، البنوك الأردنية، أدوات إدارة وتقييم المخاطر

Managing Cybersecurity Risks in Jordanian Banks

Dr. Ahmed Mahmoud Al-Zyoud
BLOM Bank - The Hashemite Kingdom of Jordan

ABSTRACT

The research discussed the concept of cyber security in all aspects, managing cyber risks, and the types and fields of threats. The research also discussed the tools used in managing and assessing risks in Jordanian banks, which aim to maintain the safety of banks and strengthen their position, verify the integrity of their procedures, and maintain the security of their information, data, and information-storage devices. The research explored the importance of managing cyber security risks in Jordanian banks and the need to clarify the policies followed regarding cyber security more precisely, in addition to publishing more clarifications in the annual reports regarding the size of cyber threats and the ability of Jordanian banks to address them.

Keywords: cyber security, Jordanian banks, risk assessment, management tools

مشكلة الدراسة:

تعالج الدراسة إدارة مخاطر الأمن السيبراني في البنوك الأردنية.

هدف الدراسة:

بيان أهمية الأمن السيبراني في البنوك الأردنية من خلال دراسة إدارة المخاطر التي تعترض أمن المعلومات في البنوك والأدوات المستخدمة في إدارة وتقييم المخاطر.

أهمية الدراسة:

الدراسة تعالج موضوع مهم وحاسم للبنوك من خلال التعرف على أدوات إدارة وتقييم مخاطر الأمن السيبراني في البنوك الأردنية.

منهجية الدراسة:

سيقوم الباحث بإتباع المنهج الوصفي والتحليلي، لوصف أدوات إدارة وتقييم مخاطر الأمن السيبراني في البنوك الأردنية، وبيان مفهوم الأمن السيبراني، وتحليل التقارير السنوية للبنوك الأردنية للتعرف على سياسات إدارة الأمن السيبراني.

مخطط الدراسة:

تم تقسيم الدراسة إلي مبحثين، المبحث الأول يتناول مفهوم الأمن السيبراني بشكل عام، وفي الثاني نستعرض أدوات إدارة وتقييم مخاطر الأمن السيبراني في البنوك الأردنية.

المبحث الأول: مفهوم الأمن السيبراني

مقدمة:

يعتبر الأمن السيبراني من المفاهيم والمصطلحات الجديدة التي ظهرت مع تطور الحياة الاقتصادية والتكنولوجية، وثورة الاتصالات، خاصة خلال العقود الثلاث الماضية حتى يومنا الحاضر. ينتشر استخدام هذا المصطلح في المؤسسات والشركات ذات الكثافة التكنولوجية، كما تبنت كثير من الدول أنظمة وقوانين تتضمن سياسات إدارة مخاطر الأمن السيبراني، وذلك بهدف حماية المعلومات ومنع اختراق الأجهزة الإلكترونية. ولكن ما هو الأمن السيبراني وماذا يتضمن وكيفية إدارة سياسة الأمن السيبراني بشكل عام وفي البنوك بشكل خاص.

مفهوم الأمن السيبراني:

يمكن شرح مفهوم الأمن السيبراني إنه ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. التي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المال من المستخدمين أو مقاطعة العمليات التجارية. تعني كلمة (سيبر) الفضاء المعلوماتي، وبذلك فالأمن السيبراني هو أمن الفضاء المعلوماتي، وهو أعم وأشمل من أمن المعلومات (فاضل، 2014). وهو عبارة عن وسائل تقنية وإدارية يتم استخدامها لمنع الاستخدام الغير مصرح به، وكذلك منع سوء الاستغلال، واستعادة المعلومات الإلكترونية، ونظم الاتصالات والمعلومات التي تحويها، وذلك بهدف ضمان استمرارية وتوافر عمل نظم المعلومات، وتأمين بيانات وخصوصية المواطنين. وهو يشمل أمن المعلومات على أجهزة وشبكات الحاسب الآلي، وبهذا تتضمن سياسات الأمن السيبراني كافة أشكال الأجهزة التكنولوجية المستخدمة في خلق ونقل وحفظ المعلومات. كذلك تتضمن حماية أماكن العمل وخطوط نقل المعلومات وصولا إلى المحافظة على الأقمار الصناعية. وبشكل أوسع نعنى به خلق (نظام بيئي للشبكة، التي تتضمن هاتف وأسلاك وخوادم) (الخملي، 2013).

ويعرف الأمن السيبراني بإنه (مجموعة الأنشطة والتدابير سواء التقنية أو غير التقنية، التي تهدف إلى حماية بيئة الكهرباء الحيوية والبيانات التي يحتوي عليها ومن كل تهديد محتمل) (الهيئة الوطنية للامن السبراني).

كذلك يعرف الأمن السيبراني بأنه (مجموعة من الشبكات والنشاطات والسلوك الإنساني) (Kostopoulo،2013)، ويختلف الأمن السيبراني عن أمن المعلومات من حيث اختصاص الأمن السيبراني بحماية أي جهاز الإلكتروني، بينما يختص أمن المعلومات

بحماية أي معلومة موجودة على الورق أم الكترونيا". كذلك فإن الأمن السيبراني يهتم بأمن الثروة الرقمية والثقافية للناس وللمنظمات وللبلدان، ويتم تنفيذ ذلك من خلال أرادة سياسية تسعى لخلق استراتيجية وطنية وتطوير بنية تحتية لحماية الثروة الرقمية تتصف بالتماسك والفعالية والموضوعية وقابلية الإدارة (الحجو، 2011).

إدارة مخاطر الأمن السيبراني :

يعتبر الأمن السيبراني بمثابة أوكسجين كوكب الأرض، بغياب الأمن السيبراني نتعرض للاختناق (Kostopoulo،2013)، هذا التشبيه يؤكد أهمية الأمن السيبراني والذي يتعرض للمخاطر مثل كافة جوانب حياتنا. وتزداد أهمية إدارة مخاطر الأمن السيبراني بسبب نوعية وقيمة الأجهزة والمعلومات والأنظمة والسياسات، كذلك أهمية استمرارية العمل وضمان تدفق المعلومات وعدم توقفها. فلا يمكن للبنوك والمؤسسات بمختلف أنواعها العمل بدون نظام معلومات أمن، يوفر سهولة الدخول وسرعة الإنجاز وسرية المعلومات وسهولة النقل والحفظ والاسترجاع (الخمعلي،2013).

أنواع التهديدات السيبرانية

تشمل التهديدات ثلاث أنواع من التهديدات السيبرانية التي يمكنها مهاجمة الأجهزة والشبكات؛ وهي الهجمات على السرية، النزاهة، والتوافر (العمراوي، 2016).

- **الهجمات على السرية (Confidentiality)**

تشمل سرقة معلومات التعريف الشخصية، والحسابات المصرفية، أو معلومات بطاقة الائتمان، حيث يقوم العديد من المهاجمين بسرقة المعلومات، ومن ثم بيعها على شبكة الإنترنت المظلمة (Dark Web) لكي يشتريها الآخرون، ويستخدموها بشكل غير شرعي.

- **الهجمات على النزاهة(Integrity)**

تتكون هذه الهجمات من التخريب الشخصي أو المؤسساتي، وغالبًا ما تسمى بالتسريبات؛ إذ يقوم المجرم الإلكتروني بالوصول إلى المعلومات الحساسة، ثم نشرها، بغرض كشف البيانات، والتأثير على الجمهور لإفقاد الثقة في تلك المؤسسة أو الشخصيّة.

- **الهجمات على التوافر(Availability)**

الهدف منها هو منع المستخدمين من الوصول إلى بياناتهم الخاصة إلى أن يدفعوا رسومًا ماليّة، أو فدية معيّنة.

مجالات التهديدات الإلكترونية

هناك العديد من المجالات لحدوث التهديدات الإلكترونية وهي (حازم، 2010):

- **الهندسة الاجتماعية (Social engineering)**

هي نوع من أنواع الهجوم على السرية، وتنطوي على عملية التلاعب النفسي في أداء الأعمال، أو دفع الضحية للتخلي عن معلومات مهمّة.

- **التهديديات المستمرة المتقدّمة (Advanced Persistent Threats)**

تُعرف اختصارًا ب APTs ، وهي نوع من أنواع الهجوم على النزاهة، يتسلل فيها مستخدم غير مصرح به إلى شبكة غير مكتشفة ويبقى فيها لفترة طويلة. والقصد من APT هو سرقة البيانات، مع عدم الإضرار بالشبكة. وتحدث APTs في معظم الأحيان في القطاعات ذات المعلومات عالية القيمة، مثل الدفاع الوطني، ومؤسسات التصنيع، ومنصّات التمويل.

- **البرامج الضارة والتجسّسيّة (Malware)**

هي نوع من أنواع الهجوم على التوافر. تشير إلى برنامج مصمم لانتزاع الوصول، أو إتلاف جهاز الكمبيوتر دون معرفة المالك. تتضمن الأنواع الشائعة من البرامج الضارة برامج التجسس(spyware) ، وkey loggers، والفيروسات، وغيرها.

أهمية الأمن السيبراني

خلال العقود الثلاث الماضية زاد الترابط بواسطة الشبكات داخل الدول وبين دول العالم المختلفة. من هنا فإن الاستفادة من برامج الدفاع السيبراني تشمل الجميع (أفراد ومجتمعات) (العمراوي،2016).

مستوى الأفراد: يتعرض الأفراد إلى عدة أنواع من هجمات الأمن السيبراني مثل سرقة الهوية أو محاولات الابتزاز أو فقدان البيانات المهمة مثل الصور العائلي.

مستوى المجتمع: تتعدد خدمات البنية التحتية الحيوية التي يعتمد أفراد المجتمع عليها، مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية. هذه الخدمات قد تتعرض إلى هجوم الإلكتروني بغية تعطيلها وأحداث بلبة في المجتمع، لذا فإن تأمين هذه المنظمات وغيرها أمر ضروري للحفاظ على عمل مجتمعنا بطريقة آمنة وطبيعية.

شمولية مصطلح الأمن السيبراني

يشمل مصطلح الأمن السيبراني عدة قطاعات، مثل من قطاع الأعمال، وقطاع الحوسبة المتنقلة، وبالعموم تقسم إلى (الشمراني، 2017):

- **أمن الشبكات**:

هو ممارسة تأمين شبكة الكمبيوتر من العناصر المتطفلة والانتهازية، سواء المهاجمين المستهدفين، أو البرامج الضارة.

- **أمان التطبيقات**:

يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات، إذ يمكن أن يوفر التطبيق المخترق الوصول إلى البيانات المصممة للحماية، وإنّ تطبيق مفهوم الأمان الناجح يبدأ في مرحلة التصميم الأوّلي قبل نشر البرنامج أو الجهاز.

- **أمن المعلومات**:

يحمي سلامة وخصوصية البيانات، سواء في مرحلة التخزين أو التناقل.

- **الأمن التشغيلي**:

يشمل العمليات والقرارات التي تتعامل مع أصول البيانات، وتكفل حمايتها. إن الأذونات التي يمتلكها المستخدمون عند الوصول إلى الشبكة، والإجراءات التي تحدد كيف وأين يمكن تخزين البيانات أو مشاركتها، كلّها تقع تحت هذه المظلة.

- **الاسترداد بعد الكوارث واستمرارية الأعمال**:

يحدد كيفية استجابة المؤسسة لحادث أمان إلكتروني، أو أي حدث آخر يتسبب في فقدان البيانات، وهذا ينطوي على آلية عمل المؤسسة في استعادة بياناتها وعملياتها ،للعودة إلى نفس القدرة التشغيلية التي كانت عليها قبل الحادث، وإنّ استمرارية العمل هي الخطة التي تعتمد عليها المنظمة بينما تحاول العمل بدون موارد معينة.

الهدف من إدارة الأمن السيبراني

تنتهج سياسة الأمن السيبراني الناجحة نهجاً معيناً يتكون عادة من طبقات متعددة للحماية تنتشر في أجهزة الكمبيوتر أو الشبكات أو البرامج أو البيانات التي ينوي المرء الحفاظ على سلامتها و في أي منظمة يجب على المستخدمين والعمليات والتكنولوجيا أن يكملوا بعضهم بعضاً ويتكاتفوا لإنشاء دفاع فعال من الهجمات السيبرانية (حازم، 2010).

- **المستخدمين:** يجب على المستخدمين فهم مبادئ أمان البيانات الأساسية والامتثال لها مثل اختيار كلمات مرور قوية، والحذر من المرفقات ذات المصدر المجهول في البريد الإلكتروني، والحرص على عمل النسخ الاحتياطي للبيانات .
- **التكنولوجيا** : تعد التكنولوجيا ضرورة ملحة لمنح المنظمات والأفراد أدوات الحماية اللازمة من الهجمات السيبرانية . ثلاثة كيانات رئيسية يجب أن تتم حمايتها- : أجهزة الكمبيوتر والأجهزة الذكية والراوترات.

وبهدف الحفاظ على مستوى متقدم من الأمن السيبراني تنتهج مختلف البنوك سياسة لإدارة مخاطر الأمن السيبراني. بحيث تتضمن الإجراءات الكفيلة بالمحافظة على مستوى متقدم من أمن المعلومات وتدفقها، وحماية الأجهزة والأنظمة من العبث والاختراق والقرصنة. ويمكن رصد عدة مخاطر تؤثر على الأمن السيبراني في هذا الصدد تتباين في طرق تشكيل التهديد ومقدار التأثير. وعلى الرغم من التباين في شكل ومقدار التهديد تبقى جميع المخاطر ذات أثر سلبي على الأصول (الملموسة وغير الملموسة) للمؤسسات والشركات (عبد الباري، 2012). من خلال الجدول رقم (1) التالي نستعرض أهم المخاطر التي تحتاج إلى إدارة وتعامل سريع لمنع الخسارة.

جدول رقم (1)

نوع الخطر	تعريف الخطر	التاثير على الأصول	طريقة المعالجة
انتحال الشخصية	سرقة مفتاح التشفير السري أو اسم المستخدم والرقم السري	تأكيد هوية المستخدم	أساليب التحقق من الشخصية
التلاعب والتزوير	تعديل المحتوى (بيانات، رموز، عمليات)	الأضرار بسلامة العمليات والرموز والبيانات	تطبيق سياسة وصول المستخدم فعاله
التنصل	أنكار صحة البيانات	التحقق من الأعمال المنتهية	تشفير البيانات
أفشاء المعلومات	الإطلاع على معلومات بدون تصريح	سرية البيانات	منع الدخول غير المصرح به
حجب الخدمات	الحجب الكلي أو الجزئي للخدمات عن العملاء	تأثير أمكانية الوصول للنظام البنكي مثلا"	فلترة الدخول إلى النظام
مراجعة الصلاحيات	منع ترقية صلاحية الدخول	صلاحيات دخول للبيانات غير قانونية	تحديد الصلاحيات والمستويات بدقة
الجدول من أعداد الباحث			

المصدر: الشمراني، عبد الله، الأمن السبراني في القطاع المصرفي السعودي، 2017.

كيفية تحقيق الأمن السيبراني

هناك عدة أساليب وطرق لتحقيق الأمان والسلامة السيبرانية (الجلاب، 2014):

- **الموثوقيّة**

استخدم فقط المواقع الموثوق بها عند تقديم معلوماتك الشخصية، والقاعدة الأساسية الفضلى هنا هي التحقق من عنوان URL. إذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أمّا إذا كان عنوان URL يحتوي على http بدون s ؛ فتجنّب إدخال أيّ معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي.

- **البريد الاحتيالي**

لا تفتح مرفقات البريد الإلكتروني أو تنقر فوق روابط الرسائل من المصادر غير المعروفة، إذ إنّ إحدى الطرق الأكثر شيوعًا التي يتعرض فيها الأشخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها مرسلة من شخص تثق به.

- **التحديثات (Always up-to-date)**

احرص دائمًا على تحديث أجهزتك، فغالبًا ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإنّ هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.

- **النسخ الاحتياطي**

تجهيز نسخ احتياطية من ملفات كافة العمليات التشغيلية والإدارية بانتظام، وذلك لضمان عدم فقدان البيانات بسبب الهجمات من خلال شبكة الإنترنت، وإذا كنت بحاجة إلى تنظيف جهازك (Format) بسبب هجوم إلكتروني سابق، فسيساعدك ذلك على تخزين ملفاتك في مكان آمن ومستقل.

إن مفهوم الأمن السيبراني وعملياته المرتبطة يتطوران باستمرار، مما يجعل من الصعب حقًّا مواكبة كلّ التفاصيل، وعمومًا؛ فإن البقاء على اطلاع، والتحلّي بالحذر على الإنترنت هما خير وسيلة للمساعدة في حماية نفسك وعملك.

المبحث الثاني: أدوات إدارة وتقييم مخاطر الأمن السيبراني في البنوك الأردنية

مقدمة عن البنوك الأردنية:

بلغ عدد البنوك في الأردن حتى نهاية 2018، (24) بنك، منها (13) بنك أردني تجاري، و(3) بنوك إسلامية أردنية، و(8) بنوك أجنبية من بينها بنك إسلامي واحد (الراجحي). بلغ مجموع موجوداتها (48573) مليون دينار أردني، حصة البنوك الثلاثة الأولى (العربي والأسكان والإسلامي الأردني) على التوالي (19.66%) (14.38) (8.57%).

تخضع البنوك الأردنية لقانون البنك المركزي وقانون التجارة الأردني وغيرها من قوانين تنظم عمليات البنوك، والتي تهدف بمجملها دعم العلميات وحماية أموال المودعين وتحقيق الشفافية والعدالة للمتعاملين مع البنوك.

أحد أهم القوانين والأنظمة هو تعليمات التكيف مع المخاطر السيبرانية الصادرة عن البنك المركزي وقانون رقم 2019/16 (قانون الأمن السيبراني) المنشور في الجريدة الرسمية عدد 5143 تاريخ 16-9-2019. وهي تنظم عمل إدارات البنوك والمؤسسات المالية الأردنية فيما يتعلق بإدارة مخاطر الأمن السيبراني.

أهمية الأمن السيبراني في البنوك الأردنية

شرعت البنوك الأردنية في تنظيم برامجها وسياساتها الداخلية المتعلقة بأمان المعلومات وأنظمة الرقابة والمراجعة في اتجاه المحافظة على موجودات البنوك من الأجهزة الإلكترونية ومعلومات بيانات العملاء. كذلك ضمان استمرارية العمل وتقديم الخدمات على مدار الساعة.

حيث طبقت أحدث الوسائل والتقنيات والبرامج في سبيل تحقيق الأهداف القصوى من حماية البيانات وتجنب مخاطر الفضاء السيبراني. ويمكن ملاحظة الاهتمام الكبير الذي تولية البنوك الأردنية لموضوع مخاطر الأمن السيبراني من خلال الجدول رقم (2) الذي يتضمن خلاصة التقارير السنوية لعام 2018 لكافة البنوك في الأردن فيما يتعلق بسياسة أمان المعلومات، يتبين لنا إن هناك ثلاث جوانب مهمة في عملية التزام البنوك بإدارة مخاطر الأمن السيبراني بشكل عام وأمان المعلومات بشكل خاص، وهي كالتالي (الموقع الرسمي للبنك المركزي الأردني):

1. **وجود سياسة أمان معلومات**: بشكل عام فإن جميع البنوك لديها سياسة أمان معلومات يناط بها رسم الخطوط العريضة للمحافظة على درجة مقبولة وكافية من أمان المعلومات.
2. **لجنة حاكمية تكنولوجيا المعلومات**: تتشكل في كل لجنة حاكمية تكنولوجيا المعلومات من أعضاء مجلس الإدارة باستثناء البنوك الأجنبية التي يتواجد مجالس إدارتها خارج الأردن. حيث سمحت تعليمات البنك المركزي تشكيل لجان توجيهية تابعة لإدارة البنك الأجنبي في الأردن لمتابعة تطبيق تعليمات الحاكمية الخاصة بتكنولوجيا المعلومات.
3. **التطبيقات والبرنامج التكنولوجية**: تسعى البنوك في الأردن إلى تطبيق وتبني تطبيقات وبرامج تكنولوجية ذات مستوى عالي من الموثيقية والقدرة على حفظ البيانات واسترجاعها دون التعرض لمخاطر القرصنة والحذف والتزوير. كما تلتزم بتطبيق نظام (COBIT) وتطبيقات نظم المعلومات الإدارية. بالإضافة للعمل على رفع مستوى النضوج في الأمن السيبراني والتصدي للهجمات السيبرانية، والتزام بالمعيار الدولي DSS PCI وهو معيار يختص بحماية بيانات حاملي البطاقات عن طريق توفير ضوابط أمنية خاصة.

جدول رقم (2)

البنك	وجود سياسة أمان معلومات	لجنة حاكمية تكنولوجيا المعلومات	التطبيقات والبرنامج التكنولوجية
البنك العربي ش م ع	*	*	*
المؤسسة العربية المصرفية (الأردن)	*	*	*
بنك الأردن	*	*	*
بنك القاهرة عمان	*	*	*
بنك المال الأردني	*	*	*
البنك التجاري الأردني	*	*	*
البنك الأردني الكويتي		*	*
البنك الأهلي الأردني	*	*	
بنك الإسكان للتجارة والتمويل	*	*	*
بنك الاستثمار العربي الأردني		*	*
البنك الاستثماري	*	*	*
بنك سوسيته جنرال / الأردن	*	*	
بنك الاتحاد	*	*	*
ستاندرد تشارترد		*	*
البنك العقاري المصري العربي		*	*
سيتي بنك إن . إيه	*	*	*
مصرف الرافدين			*
بنك الكويت الوطني			*
بنك لبنان والمهجر	*		*
بنك عوده ش.م.ل	*	*	*
البنك العربي الإسلامي الدولي	*	*	*
البنك الإسلامي الأردني	*	*	*
بنك صفوة الإسلامي	*	*	*
مصرف الراجحي	*		

المصدر: الجدول من إعداد الباحث، المصدر: التقارير السنوية لعام 2018 لكافة البنوك الأردنية

إدارة مخاطر الأمن السيبراني في البنوك الأردنية:

تهدف البنوك الأردنية من إدارة مخاطر الأمن السيبراني إلى تحقيق الحد الأدنى من المتطلبات الأساسية للأمن السيبراني المعتمدة على أفضل الممارسات والمعايير الهادفة لتقليل مخاطر الأمن السيبراني وحماية الأصول المعلوماتية والتقنية من التهديدات الداخلية والخارجية (حافظ، 2018).

ترتكز سياسات إدارة المخاطر على (الشولي، 2018):

1. الإستراتيجية.
2. الأشخاص.
3. الإجراء.
4. التقنية.

وضع السياسات والإجراءات الخاصة بالأمن السيبراني:

1. تحديد سياسات وإجراءات الأمن السيبراني، وضوابط ومتطلبات ذلك، وتوثيقها واعتمادها من مجلس الإدارة.
2. تحميل الإدارة المعنية بالأمن السيبراني مسؤولية ضمان تطبيق سياسات وإجراءات الأمن السيبراني.
3. دعم سياسات وإجراءات الأمن السيبراني بمعايير تقنية أمنية.
4. مراجعة وتحديث سياسات الأمن السيبراني بشكل دوري.

الإجراءات المتبعة من قبل البنوك الأردنية لإدارة مخاطر الأمن السيبراني

1. تحديد وتوثيق واعتماد منهجيات وإجراءات إدارة مخاطر الأمن السيبراني وفق اعتبارات السرية و توافر وسلامة الأصول المعلوماتية والتقنية.
2. متابعة تطبيق الإجراءات في جميع إدارات وفروع البنك.
3. تنفيذ إجراءات تقييم مخاطر الأمن السيبراني خلال تنفيذ المشاريع التقنية وقبل إجراء التغيرات، وعند أدخال طرف خارجي، وعند أطلاق خدمات جديدة.
4. مراجعة منهجية وإجراءات إدارة المخاطر السيبرانية بشكل دوري وتحديثها وتوثيق التغيرات وفق جدول زمني.

النتائج

في نهاية هذه البحث يمكن الوصول للنتائج التالية:

1. تلتزم البنوك الأردنية بالسياسات الخاصة بأمان المعلومات وسياسة الأمن السيبراني.
2. تطبيق ومتابعة جميع التعليمات الصادرة من البنك المركزي الأردني فيما يتعلق بالأمن السيبراني.
3. تقوم البنوك الأردنية بنشر دليل الحاكمية المؤسسية لتكنولوجيا المعلومات ضمن التقارير السنوية أو ضمن تقارير خاصة على مواقعها.

التوصيات

بناء على النتائج السابقة التي تم التوصل إليها يمكن صياغة التوصيات التالية:

1- توضيح السياسات المتبعة بخصوص الأمن السيبراني بشكل أدق.
2- نشر مزيد من الإيضاحات في التقارير السنوية بخصوص حجم التهديدات السيبرانية وقدرة البنوك على معالجتها.

المراجع العربية

[1] التقارير السنوية للبنوك الأردنية.

[2] الحجو، زهير، (2011). *العولمة التكنلوجية وثارها على القطاع المصرفي*، بحث مقدم لمؤتمر القطاع المصرفي ورهانات المستقبل، مركز الشمال للدراسات.

[3] الحميد، محمد دباس، نينو، ماركو إبراهيم، (2007). *حماية أنظمة المعلومات*، دار الحامد للنشر.

[4] الجلاب، عاصم، (2014). *العولمة المصرفية*، بحث مقدم لمؤتمر القطاع المصرفي والعولمة، الطبعة الأولى.

[5] الخمعلي، سليمان، (2013). *الامن السبراني والاقتصاد السعودي*، مكتبة وهبة للنشر والتوزيع.

[6] الرزو، حسن مظفر، (2007). *الفضاء المعلوماتي*، مركز دراسات الوحدة العربية.

[7] الشمراني، عبد الله (2017). *الأمن السبراني في القطاع المصرفي السعودي*، مجلة اقتصاديات السوق، العدد 4، المجلد2.

[8] الشولي، اياس، (2018). *حماية المعلومات المصرفية*، الواقع والتطلعات، مكتبة بشرى للتوزيع، الطبعة الثانية.

[9] العمراوي، هلال، (2016). *مفاهيم حول الأمن السبراني*، دار إشبيلية الحديثة للنشر، الطبعة الأولى.

[10] حازم، محمد، (2010). *الأمن السبراني التحدي الجديد للقطاع المالي*، مكتبة الناشر للتوزيع، الطبعة الثانية.

[11] حافظ، عبد الله، (2018). *امن المعلومات في القطاع المصرفي*، مكتبة الرشد للتوزيع، الطبعة الأولى.

[12] داود، حسن طاهر، (1425). *أمن شبكات المعلومات*، معهد الإدارة العامة.

[13] عبد الباري، سليمان، (2012) ، *الأمن السبراني*، مكتبة البركة للنشر والتوزيع.

[14] فاضل، حفيظ (2014) ، *الامن السبراني وتحديات العولمة*، الرياض للنشر والتوزيع، الطبعة الأولى.

[15] موقع البنك المركزي الأردني.

المراجع الالجنبية

[1] Kostopoulos, G. (2013). *Cyberspace and cybersecurity*. New York, USA: CRC Press.

