

عنوان البحث

إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية –
بالتطبيق على وزارة الاتصالات وتقنية المعلومات.

Cybersecurity risk management in government institutions in the Kingdom of Saudi Arabia - by
application to the Ministry of Communications and Information Technology

إعداد الطالب/

إشراف/

العام الدراسي:

٢٠٢٤

مقدمة:

إن تنوع وسائل الاتصالات وتفاوت خصائصها وطبيعتها زاد من حجم تبادل المعلومات بين العالم بشكل تسبب في زيادة العبء على الدول التي تسعى إلى تحقيق الأمن المطلوب للفرد والمجتمع في ظل الاستخدام الواسع للحاسب الآلي وتطبيقاته، والأجهزة الذكية، وكذلك ما يندرج تحتها ، ولقد شكل الأمن على مر التاريخ الهاجس الأكبر للدول التي اعتبرت ضمان بقائها واستمرارها من بين أولويات سياستها ، فالأمن هدف تسعى إليه كل الدول كونه أحد أهم مقومات الحياة الإنسانية ، أمام هذا الاحتياج الملح يبرز دور الأفراد والدولة ، المؤسسات و المنظمات الإقليمية والعالمية في العملية الأمنية (الخالدي، ٢٠١٦، ص ٥٢-٥٣).

إن تشريعات الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية تهدف إلى تعزيز وتعزيز أمان البنية التحتية السيبرانية في المملكة وحماية المعلومات الحساسة والتحقق من سلامة البيانات المتداولة. ويتعين على المنظمات تحديد وتحليل المخاطر المحتملة لأمن البيانات والأنظمة السيبرانية الخاصة بها. (الغامدي، ٢٠٢١، ص ١٧).

ويتطلب ذلك تقييم وتحليل التهديدات المحتملة وثرغات الأمان وتأثيرها المحتمل على المنظمة. كما يجب على المنظمات تنفيذ إجراءات أمنية فعالة لحماية الأنظمة والبيانات الحساسة من التهديدات السيبرانية. ويشمل ذلك تطبيق سياسات الأمان والوصول والتحقق من الهوية وتحديث البرامج والأجهزة وتأمين الشبكات والتدريب على الوعي الأمني . ونظرا لأهمية الأمن المعلوماتي في العصر الحديث ، فقد صدر أمر ملكي كريم بإنشاء هيئة باسم الهيئة الوطنية للأمن السيبراني، ترتبط بمقام خادم الحرمين الشريفين، وتضع الهيئة في أولوياتها استقطاب الكوادر الوطنية المؤهلة والطموحة وتأهيلها وتمكينها ، وبناء الشراكات مع الجهات العامة والخاصة، وتحفيز الابتكار والاستثمار في مجال الأمن السيبراني للإسهام في تحقيق نهضة تقنية تخدم مستقبل الاقتصاد الوطني للمملكة. وتهدف الهيئة إلى تعزيز حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات

التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات، وما تحويه من بيانات، مراعية في ذلك الأهمية الحيوية المتزايدة للأمن السيبراني في حياة المجتمعات، ومستهدفة التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال انطلاقاً مما تضمنته رؤية المملكة العربية السعودية ٢٠٣٠ (الهيئة الوطنية للأمن السيبراني ، ٢٠١٨ ، ص٩٦-٩٧).

ويمثل الأمن الوطني أحد المقومات الأساسية لنجاح عملية التنمية، والنمو، والارتقاء بمختلف المجالات؛ حيث يعد الإبداع الفكري، والذهني، والتخطيط المنظم، والسليم، والمثابرة العلمية، من أهم مرتكزات التنمية، ولا يتحقق ازدهار لمشروع التنمية إلا في ظل وجود أمن راسخ يدعم، ويتيح وجود هذه المرتكزات، مما يمكن الإنسان من الاطمئنان على ذاته، وثروته، واستثماراته (الشراري، ٢٠١٧، ص٨٨).

يتضح مما سبق أنه يجب على المنظمات وضع خطط استجابة للحوادث الأمنية وتنفيذها عند حدوث أي انتهاك أمني. ويشمل ذلك التعامل مع الاختراقات والتهديدات المحتملة واستعادة الأنظمة وتحليل الحوادث لتعزيز الأمان في المستقبل. وتشترط تشريعات الهيئة الوطنية للأمن السيبراني الامتثال للمعايير والإرشادات الأمنية المعترف بها عالمياً. يجب على المنظمات مراجعة سياساتها وإجراءاتها للتأكد من الامتثال لهذه المعايير والإشعار بأي انتهاكات أمنية محتملة. ويتناول الباحث في تلك الدراسة موضوع إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات.

مشكلة الدراسة:

تتمثل مشكلة الدراسة الحالية في أنه يجب على المنظمات تعزيز التوعية الأمنية لدى الموظفين وتوفير التدريب المناسب لهم بشأن مخاطر الأمن السيبراني وكيفية التعامل معها. يمكن أن يشمل ذلك التعريف بالتهديدات السيبرانية المحتملة وطرق الوقاية منها والإبلاغ عن أي حالات انتهاك أمني. كما يجب على المنظمات إجراء تقييم دوري لامتثالها لتشريعات

الهيئة الوطنية للأمن السيبراني والمعايير الأمنية المعمول بها. يشمل ذلك تنفيذ عمليات التدقيق الداخلي والتقييم الخارجي للتأكد من مستوى الامتثال وتحديد أي نقاط ضعف تحتاج إلى تحسين.

ولقد أصبح لأمن المعلومات في عصر التكنولوجيا الدور الأكبر في تحقيق التميز المؤسسي من خلال حماية البيانات و صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة، وأيضا حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني (الخالدي، ٢٠١٦، ص ٤١).

وينتهج الأمن السيبراني الناجح نهجا 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 وكذلك التكنولوجيا أن يكملوا بعضهم بعضاً ويتكاتفوا لإنشاء دفاع فعال من الهجمات السيبرانية (عبد ربه ، ٢٠٢٠ ، ص ٦٣).

وقد أكدت نتائج دراسة والدو (Waldo ، ٢٠١٧، ص ١٣) أنه يجب على المستخدمين فهم مبادئ أمن البيانات الأساسية والامتثال لها مثل اختيار كلمات مرور قوية ، والحذر من المرفقات ذات المصدر المجهول في البريد الإلكتروني ، والحرص على عمل النسخ الاحتياطي للبيانات .

يتضح مما سبق أنه من الضروري التعاون مع الهيئة الوطنية للأمن السيبراني ومشاركة المعلومات الأمنية الحيوية معها. يساهم التعاون في تعزيز القدرة على التصدي للتهديدات السيبرانية وتعزيز الأمان السيبراني على المستوى الوطني. وتشجع تشريعات الهيئة الوطنية للأمن السيبراني على التطوير المستمر والابتكار في مجال الأمن السيبراني. ويجب على المنظمات مواكبة التطورات التكنولوجية وتحديث استراتيجياتها وتقنياتها الأمنية لمواجهة التهديدات السيبرانية الجديدة والمتقدمة. ومن هذا المنطلق يمكن تحديد مشكلة الدراسة في

التساؤل الرئيسي التالي: ما سبل إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية ؟

أهمية الدراسة:

الأهمية العلمية:

- يساهم البحث في زيادة المعرفة والفهم المتعمق لمفهوم إدارة مخاطر الأمن السيبراني وتشريعات الهيئة الوطنية للأمن السيبراني. ويمكن أن يوفر البحث نظرة شاملة حول الإطار القانوني والتنظيمي المعمول به في البلد المعين وكيفية تطبيقه لإدارة مخاطر الأمن السيبراني.

- يمكن أن يساهم البحث في تطوير النهج العلمي لإدارة مخاطر الأمن السيبراني. ومن خلال دراسة التشريعات المعمول بها وتحليلها، يمكن أن يتم تحديد الثغرات والتحديات في النهج الحالي واقتراح تحسينات وتوجهات جديدة لتعزيز الأمان السيبراني.

- يمكن أن يكون البحث نقطة انطلاق للبحوث المستقبلية في مجال إدارة مخاطر الأمن السيبراني. وقد يشجع البحث العلماء والباحثين على استكشاف مواضيع ذات صلة وتطوير إطارات ونماذج جديدة لفهم ومعالجة التهديدات السيبرانية.

الأهمية التطبيقية:

- يمكن أن يساهم البحث في تحسين مستوى الأمن السيبراني في المؤسسات والمنظمات والهيئات. وعن طريق فهم تشريعات الهيئة الوطنية للأمن السيبراني وتطبيقها بشكل صحيح، يمكن للمؤسسات تعزيز قدراتها على اكتشاف واحتواء واستجابة للتهديدات السيبرانية.

- يساعد البحث على فهم متطلبات الامتثال لتشريعات الهيئة الوطنية للأمن السيبراني. ويمكن للمؤسسات والشركات أن تستفيد من هذا البحث للامتثال

القانوني وتنفيذ إجراءات وسياسات تعزيز من مستوى الأمن السيبراني وتجنب المخاطر القانونية والعقوبات المحتملة.

- يمكن أن يساهم البحث في تعزيز وعي الفرق العاملة وتعزيز قدراتها في إدارة مخاطر الأمن السيبراني. ومن خلال دراسة التشريعات وتحليلها، يمكن تطوير برامج تدريبية تستهدف توعية الموظفين وتعزيز مهاراتهم في التعامل مع التهديدات السيبرانية.
- يمكن للبحث أن يساعد في توضيح المسؤوليات القانونية للمؤسسات والأفراد فيما يتعلق بالأمن السيبراني. ومن خلال فهم تشريعات الهيئة الوطنية للأمن السيبراني وتطبيقها، يمكن للمؤسسات تحديد مسؤولياتها واتخاذ الإجراءات اللازمة للحماية من التهديدات السيبرانية وتفادي المسائل القانونية.

أهداف الدراسة:

تهدف تلك الدراسة إلى ما يلي:

١. التعرف على مخاطر الأمن السيبراني في وزارة الاتصالات وتقنية المعلومات.
٢. التعرف على مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في وزارة الاتصالات وتقنية المعلومات.
٣. التعرف على سبل تطوير دور إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني في وزارة الاتصالات وتقنية المعلومات.

تساؤلات الدراسة

١. ما مخاطر الأمن السيبراني في وزارة الاتصالات وتقنية المعلومات؟
٢. ما مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في وزارة الاتصالات وتقنية المعلومات؟
٣. ما سبل تطوير دور إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني في وزارة الاتصالات وتقنية المعلومات؟

فروض الدراسة:

١. توجد علاقة ذات دلالة إحصائية بين إدارة مخاطر الأمن السيبراني في وزارة الاتصالات وتقنية المعلومات وتحديد تلك المخاطر.
٢. توجد علاقة ذات دلالة إحصائية بين إدارة مخاطر الأمن السيبراني في وزارة الاتصالات وتقنية المعلومات و مدى الالتزام بتشريعات الهيئة الوطنية للأمن السيبراني في الوزارة.
٣. توجد علاقة ذات دلالة إحصائية بين إدارة مخاطر الأمن السيبراني في وزارة الاتصالات وتقنية المعلومات و تطوير دور إدارة مخاطر الأمن السيبراني وفق تشريعات الهيئة الوطنية للأمن السيبراني

الدراسات السابقة:

يتناول الباحث الدراسات السابقة مرتبة من الأقدم إلى الأحدث ، كما يلي :

دراسة الصيدلاني (٢٠١٧) بعنوان : واقع قرصنة البرمجيات في الأردن ، وسبل مواجهتها. وهدفت الدراسة إلى: التعرف على واقع قرصنة البرمجيات في الأردن ، وسبل مواجهتها . وتم تطبيق الدراسة على عينة مكونة من ١٢٠ من موظفي (١١) شركة خدمية بمدينة عمان العاصمة، وقد استخدمت الدراسة المنهج الوصفي التحليلي ، وتمثلت أداة الدراسة في الإستبانة . وقد توصلت الدراسة إلى عدة نتائج أهمها : إنه في حين تقع مسؤولية توعية الطلبة بحقوق الملكية الفكرية ومخاطر القرصنة على قطاع التعليم فإن توعية عامة الشعب بمختلف مستوياتهم تقع على عاتق الحكومة والقطاع الخاص. والتأكيد بأن زيادة الوعي مفتاح القدرة على الحد من ظاهرة القرصنة.

دراسة ستيفن Stephen (٢٠١٧) بعنوان : أسباب توجه الأفراد والمنظمات إلى انتهاك خصوصية المعلومات ، ودور الأمن السيبراني في مواجهة الظاهرة: هدف البحث إلى التعرف على أسباب توجه الأفراد والمنظمات إلى انتهاك خصوصية المعلومات ودور الأمن السيبراني

في مواجهة الظاهرة. وقد استخدم الباحث المنهج الوصفي المسحي وأداة الإستبانة وطبق دراسته على (١٢٤) من خبراء تكنولوجيا المعلومات بمؤسسة جون بريد بضاحية لندن الغربية بالمملكة المتحدة. وقد توصلت الدراسة إلى نتائج هامة ، ومنها : تقديم اقتراح ببعض الحلول للحد من الظاهرة في المدارس مثل توعية الطلبة والمدرسين بالمسؤوليات والقيود الواجب مراعاتها عند استخدام البرمجيات، إضافة إلى جعل السياسات المتعلقة بقرصنة البرمجيات جزء من سياسات حقوق الطبع لفائدتها على الرغم من كلفتها العالية.

ودراسة والدو (Waldo) (٢٠١٨) بعنوان : التوعية السيبرانية بخصوصية المعلومات والبيانات باستخدام الرحلات المعرفية عبر الويب ، مدخل تعليمي جديد في الاتحاد الأوروبي . هدفت الدراسة إلى توجيه نظر القائمين على السياسة الأمنية في الاتحاد الأوروبي إلى اعتماد استخدام الرحلات المعرفية عبر الويب ، كمدخل تعليمي جديد لاتخاذ القرارات بدلا من استخدامها بشكل فردي من قبل بعض المؤسسات . وقد عرف الباحث الرحلة المعرفية عبر الانترنت بأنها عبارة عن نشاط مبني على رحلة باستخدام الانترنت يتم عرضه مسبقاً، وتعليم الطلبة استخدام المعرفة المراد تعليمها للطلبة وكيفية التعامل معها. وقد استخدم الباحث المنهج المسحي وأداة الإستبانة . وقد طبق الباحث دراسته على (٧) جامعات ومعاهد علمية في بلجيكا وبريطانيا وهولندا . وقد توصلت الدراسة إلى نتائج هامة ومنها : أن إستراتيجية الرحلات المعرفية عبر الويب القائمة على محاكاة خصوصية البيانات تسهل على الجهات الأمنية التوعية بخصوصية المعلومات ومصادر المعرفة المتاحة، على شبكة الإنترنت.

ودراسة الزهراني (٢٠١٨) بعنوان : آثار قرصنة البرمجيات عالميا ، وتمثل هدف الدراسة في التعرف على آثار قرصنة البرمجيات عالميا . وقد استخدمت الدراسة المنهج الوصفي التحليلي . وطبقت الدراسة على (٧٩) من خبراء تكنولوجيا المعلومات بجامعة القاهرة . وتم استخدام الاستبانة في جمع البيانات . و من أهم نتائج الدراسة ما يلي : إن من أسباب

انخفاض نسبة القرصنة في بعض الدول وجود حماية قوية للاختراعات والبرامج وحقوق الملكية الفكرية ، عكس الحال في كثير من الدول النامية .

و دراسة العضياني (٢٠١٨) بعنوان : انتهاك خصوصية البيانات في مؤسسات الأعمال وأثره على أداء المؤسسات . و تمثلت أهداف الدراسة في التعرف على واقع انتهاك خصوصية البيانات في مؤسسات الأعمال وأثره على أداء المؤسسات . وقد استخدمت الدراسة المنهج الوصفي التحليلي . و بلغ حجم عينة الدراسة ١٣٢ من مدراء المؤسسات الخاصة وكبار الموظفين بها في مدينة القاهرة ، وتم جمع البيانات من خلال الاستبانة . و من أبرز النتائج التي توصل إليها الباحث ، ما يلي : إن اختراق أنظمة المعلومات و نظم الشبكات و المواقع المعلوماتية أصبح خطراً يقلق العديد من المنظمات ، إن هناك ارتفاعاً واضحاً في معدل الإختراقات مع تنوع الوسائل المستخدمة في الاختراق على الرغم من سبل الحماية التي تتبعها المنظمات.

و دراسة فايز (٢٠١٩) بعنوان : دور تكنولوجيا المعلومات في تدعيم أداء الموارد البشرية (دراسة ميدانية) : هدفت الدراسة إلى التعرف على دور تكنولوجيا المعلومات في تدعيم أداء الموارد البشرية بالشركات المصرية ، وقد استخدم الباحث المنهج الوصفي وأداة الإستبانة . وتمثلت عينة الدراسة في (١١٨) من العاملين بشركة جهينة بمصر . وقد توصلت الدراسة إلى نتائج هامة ومنها : أن تكنولوجيا المعلومات تعمل على تطوير أداء الموارد البشرية بالشركة ، و أبدى أغلبية عينة الدراسة (٩٨ % منهم) شعورهم الإيجابي بأهمية التدريب .

دراسة إبداح (٢٠١٩) بعنوان : أمن وسرية المعلومات وأثرها على الأداء التنافسي دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية . وقد هدفت الدراسة إلى التعرف على أمن وسرية المعلومات وأثرها على الأداء التنافسي دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية . وطبقت هذه الدراسة في شركة التأمين العراقية العامة وشركة الحمراء للتأمين الأهلية نموذجاً عن شركات التأمين في العراق وباختبار عينة من المديرين والموظفين العاملين في الشركتين وبعدها (٧٠) موظفاً ، وقد

استخدمت تلك البيانات في اختبار الفرضيات. وقد توصلت إلى الدراسة إلى عدد من الاستنتاجات كان أهمها وجود علاقة ارتباط وتأثير بين أمن المعلومات وسريتها والأداء التنافسي لشركات التأمين قيد البحث. وجاءت النتائج متطابقة مع فرضية الدراسة.

ودراسة ليبس Lipps (٢٠٢٠) بعنوان : "الاهتمام بتنظيم دورات تكنولوجيا المعلومات ، مدخل تعليمي جديد في الاتحاد الأوروبي": وهدفت الدراسة إلى توجيه نظر القائمين على السياسة التعليمية في الاتحاد الأوروبي إلى الاهتمام بتنظيم دورات تكنولوجيا المعلومات كمدخل تعليمي جديد بدلا من استخدامها بشكل فردي من قبل المؤسسات بدول الإتحاد . وقد استخدم الباحث المنهج المسحي وأداة الإستبانة . وقد طبق الباحث دراسته على (٧) جامعات ومعاهد علمية في بلجيكا وبريطانيا وهولندا . وقد توصلت الدراسة إلى نتائج هامة ومنها : إن التقنيات الحديثة في تنمية الموارد البشرية تعتبر عصب الحياة العملية فهي ترفع من معنويات الفرد و تزيد فاعليته و ثقته ، وتقلل من ضعفه النفسي أمام الآخرين ، إن استخدام المنظمات لنظم المعلومات ذات الكفاءة والفعالية من شأنه أن يحقق لها أهدافها.

ودراسة حمدان (٢٠٢١) بعنوان: أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن. هدفت هذه الدراسة إلى تعرف أمن المعلومات وسريتها وأثرها في الأداء المصرفي في البنوك العاملة في الأردن، وقد تكون مجتمع الدراسة من البنوك العاملة في الأردن، وأخذت عينة عشوائية طبقية متناسبة بنسبة ٥٠% من مجتمع الدراسة (٦١٥) فرد. و أظهرت نتائج الدراسة أن مستوى ممارسة أمن المعلومات وسريتها في البنوك العاملة في الأردن من حيث الأهمية النسبية كانت مرتفعة، إذ بلغ المتوسط الحسابي (٤.١١). كما تبين أن الأهمية النسبية للأداء المصرفي في البنوك العاملة في الأردن كانت مرتفعة، إذ بلغ المتوسط الحسابي (٤.٠٧) وبينت نتائج الدراسة وجود أثر ذي دلالة إحصائية لأمن المعلومات وسريتها (الحماية المادية، حماية الأفراد، الحماية البرمجية) في الأداء المصرفي في البنوك العاملة في الأردن.

ودراسة لينر Lerner (٢٠٢١) بعنوان : "دور تكنولوجيا المعلومات في إعداد الكفاءات البشرية بمركز (ايزونتي)": هدفت الدراسة إلي عرض تجربة مركز (ايزونتي للصحة النفسية) بمدينة (أنتويرب) بلجيكا في إعداد الكفاءات البشرية. وطبقت الدراسة على عدد (٢٦) من العاملين. وقد توصلت الدراسة إلي نتائج هامة ومنها : إن التخطيط المسبق لإعداد الموارد البشرية يساعد على تلافي السلبيات ، يمكن الاعتماد على تكنولوجيا المعلومات في إعداد الموارد البشرية نظرا لفاعليتها الكبيرة .

التعقيب على الدراسات السابقة:

بعد استعراض الدراسات السابقة تبين ما يلي:

اتفقت الدراسة الحالية مع الدراسات السابقة في التركيز على موضوع الأمن السيبراني ، كما اتفقت الدراسة الحالية مع بعض الدراسات السابقة في استخدام المنهج الوصفي. واختلفت الدراسة الحالية عن الدراسات السابقة لاختلاف الزوايا التي تم تناولها واختلاف الأهداف التي سعت إليها كل دراسة. كما تناولت الدراسات السابقة موضوع الدراسة في بيئات مختلفة عن بيئة الدراسة الحالية وأيضا اختلاف الفترة الزمنية التي سوف تتم فيها الدراسة الحالية عن الفترات الزمنية التي تمت فيها الدراسات السابقة . وسوف نستفيد من الدراسات السابقة فيما يلي :

- التأصيل النظري للدراسة الحالية
- في تحديد مصطلحات الدراسة
- في الاطلاع على دراسات سابقة في موضوع الدراسة الحالية
- في الاستفادة من الدراسات السابقة في تحديد منهج الدراسة
- في بناء أداة الدراسة
- تحديد الأساليب الإحصائية المناسبة
- في تحليل وتفسير النتائج التي توصلت إليها الدراسة.

المنطلقات النظرية للدراسة:

١- مفهوم الأمن السيبراني

الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني. والأمن السيبراني هو سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول. وينتهج الأمن السيبراني الناجح نهجا 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 . وفي عصر التكنولوجيا أصبح لأمن المعلومات الدور الأكبر صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة، وأيضا حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني (الشراري ، ٢٠١٧، ص٣٩-٤٠).

إن هدف الأمن السيبراني هو المساعدة على حماية أصول المنظمات ومواردها من النواحي التنظيمية، والبشرية، والمالية، والتقنية والمعلوماتية بحيث يسمح لها بمواصلة مهمتها. والهدف النهائي هو ضمان عدم تضررها ضرراً دائماً. وهذا يتمثل في تقليل احتمالات تجسد أي تهديد، والحد من الضرر الناجم أو سوء الأداء، وضمان استعادة العمليات العادية لحالتها السابقة خلال إطار زمني مقبول وبتكلفة مقبولة في أعقاب وقوع حادث أمني. وتشمل عملية الأمن السيبراني المجتمع بأسره، من حيث يكون كل فرد فيه معنياً بتنفيذها.

ويمكن دعم ذلك بتطوير مدونة سلوك سيبرانية لأجل الاستخدام السليم لتكنولوجيا المعلومات والاتصالات، وإعلان سياسات أمن واقعية تقنن المعايير التي يكون متوقعاً من مستخدمي الأمن السيبراني (الكيانات والشركاء والموردون) الوفاء بها. ولإنشاء عملية أمن سيبراني، يكون من المهم التحديد الدقيق للأصول والموارد اللازمة للوقاية الفعالة. ويستلزم ذلك نهجاً عالمياً للأمن، نهجاً متعدد التخصصات وشاملاً إذ لا يصلح الأمن السيبراني في عالم يسوده التسبب ويعتق الإباحية. والمطلوب هو مجموعة من المبادئ الأساسية للسلوك الأخلاقي، والمسؤولية والشفافية المتجسدة في إطار قانوني مناسب، ومجموعة عملية من الإجراءات والقواعد. ويجب إنفاذ تلك المبادئ محلياً، بالطبع، ولكن ينبغي أيضاً تطبيقها عبر المجتمع الدولي وأن تكون متوافقة مع التوجهات الدولية القائمة. ولتفادي إتاحة الفرص أمام تنامي الجريمة، يجب على البنى التحتية للاتصالات أن تشمل على تدابير أمن مناسبة ذات طبيعة تقنية وقانونية مناسبة. ويمكن للهجمات عبر الفضاء السيبراني أن تتخذ أشكالاً كثيرة: الاختطاف السري لنظام، رفض تقديم الخدمة، تدمير أو سرقة بيانات حساسة، اقتحام المتسللين للشبكة، كسر حماية البرمجيات، الفركنة أو التنصت الإلكتروني (phreaking) والذي يشمل التخريب واختطاف المبادلات الهاتفية وأكثر من ذلك. وتقع تكلفة ذلك في الغالب الأعم على عاتق الضحايا، أي المنظمات والأفراد المستهدفين (الاتحاد الدولي للاتصالات، ٢٠١٩، ص ١١-١٣).

٢- أهمية الأمن السيبراني

تحدد أهمية الأمن السيبراني، فيما يلي:

١. الحماية من الهجمات السيبرانية: يتعرض الأفراد والشركات والمؤسسات والحكومات للعديد من التهديدات السيبرانية مثل اختراق الأنظمة، والبرمجيات الخبيثة، والاحتياز الإلكتروني، وتسريب المعلومات الحساسة، والإرهاب الإلكتروني، والتجسس السيبراني. ويهدف الأمن السيبراني إلى توفير الحماية اللازمة للأنظمة والبيانات والمعلومات ضد هذه الهجمات.

٢. الحفاظ على الخصوصية: تعتبر الخصوصية أحد جوانب الأمن السيبراني المهمة. ويجب حماية البيانات الشخصية والمعلومات الحساسة للأفراد والمؤسسات من الوصول غير المصرح به والاستخدام غير القانوني. فقد تتضمن هذه المعلومات المالية، والطبية، والتجارية، والحكومية، والخاصة. يتطلب الأمر تنفيذ إجراءات الحماية المناسبة مثل تشفير البيانات وضمان الوصول المحدود للأشخاص المخولين فقط.

٣. الحفاظ على استقرار الأنظمة: يعتمد العديد من الجوانب في حياتنا اليومية على الأنظمة السيبرانية مثل النظام المصرفي والشبكات الاجتماعية والنقل العام والتجارة الإلكترونية. ويهدف الأمن السيبراني إلى ضمان استقرار هذه الأنظمة ومنع تعطّلها أو تعرضها للهجمات التي يمكن أن تتسبب في فوضى وتوقف الخدمات الحيوية (الزهراني، ٢٠١٨، ص ٤٧-٤٩).

٤. الحماية الوطنية والاقتصادية: يعد الأمن السيبراني أحد جوانب الأمن الوطني، حيث يمكن للهجمات السيبرانية المستهدفة للبنى التحتية الحيوية للدولة أن تسبب أضراراً جسيمة على المستوى الاقتصادي والعسكري والسياسي. وتستهدف بعض الهجمات السيبرانية الحكومات والمؤسسات الحكومية والبنى التحتية الحيوية مثل الشبكات الكهربائية والمياه والمواصلات. ويعمل الأمن السيبراني على تعزيز القدرة التنافسية للدول والاقتصادات من خلال حماية المعلومات الاقتصادية والتكنولوجية الحساسة ومنع سرقتها أو تسريبها.

٥. الحماية من التجسس الصناعي: تعاني العديد من الشركات من التجسس الصناعي الذي يستهدف سرقة المعلومات التجارية والتكنولوجية الحساسة. ويتطلب الأمن السيبراني تنفيذ إجراءات لحماية الملكية الفكرية والأسرار التجارية وضمان عدم الوصول غير المصرح به إلى هذه المعلومات.

٦. الحماية الشخصية: يعتبر الأمن السيبراني أيضاً أمراً هاماً للأفراد. ويجب على الأفراد اتخاذ إجراءات الأمان السيبراني لحماية هويتهم الشخصية والمعلومات الشخصية

الحساسة مثل المعلومات المالية والصحية والخصوصية الشخصية على الإنترنت. ويشمل ذلك استخدام كلمات مرور قوية، وتحديث برامج الحماية (الصيدلاني، ٢٠١٧، ص ٩٥-٩٧).

٣- أهداف الأمن السيبراني

تحدد أهداف الأمن السيبراني ، فيما يلي:

١. حماية السرية والخصوصية: يهدف الأمن السيبراني إلى حماية البيانات والمعلومات الحساسة من الوصول غير المصرح به والاستخدام غير القانوني. ويتم تنفيذ تدابير الأمان مثل التشفير وإدارة الوصول للحفاظ على سرية المعلومات وحماية خصوصية الأفراد والمؤسسات.

٢. ضمان توافر الأنظمة: يهدف الأمن السيبراني إلى ضمان توافر الأنظمة والخدمات السيبرانية المهمة. ويتضمن ذلك حماية الأنظمة من الهجمات السيبرانية المتعمدة التي تهدف إلى تعطيلها أو إلحاق أضرار بها. ويتم تطبيق تدابير الأمان مثل إعدادات الحماية والنسخ الاحتياطي والاستعداد للكوارث لضمان استمرارية العمليات.

٣. الوقاية من الهجمات السيبرانية: يشمل الهدف الأساسي للأمن السيبراني الوقاية من الهجمات السيبرانية المحتملة. ويتم تحليل ومراقبة الأنشطة السيبرانية لاكتشاف التهديدات المحتملة والاستجابة لها قبل حدوث الأضرار. ويشمل ذلك استخدام أدوات الكشف عن التسلل وأنظمة الإنذار المبكر والتحليل الأمني للكشف عن الهجمات والتصدي لها.

٤. تعزيز الاستعداد والاستجابة: يهدف الأمن السيبراني إلى تعزيز الاستعداد والاستجابة للهجمات السيبرانية. ويتضمن ذلك وضع خطط الطوارئ والاستجابة للتعامل مع الهجمات واحتواء الأضرار واستعادة النظم إلى حالتها الطبيعية بأقل وقت ممكن. كما يشمل تقييم التهديدات وتحديث السياسات والإجراءات لمواجهة التهديدات المتغيرة.

٥. تعزيز التوعية والتدريب: يهدف الأمن السيبراني إلى تعزيز التوعية والتدريب للأفراد والمؤسسات بشأن التهديدات السيبرانية وأفضل الممارسات للوقاية منها. ويهدف ذلك إلى

زيادة الوعي بأمن المعلومات وتعزيز المهارات الفنية لتأمين الأنظمة والشبكات السيبرانية تتطلب تنفيذ استراتيجيات وتدابير أمنية متعددة لتحقيق هذه الأهداف. ويجب أن تكون هذه التدابير شاملة وتشمل الجوانب التقنية والتنظيمية والتعليمية والقانونية (فايز، ٢٠١٩، ص ٦٣-٦٥).

٤-العناصر الأساسية للأمن السيبراني :

تحدد العناصر الأساسية للأمن السيبراني ، فيما يلي :

أ. منظومة الأجهزة الإلكترونية وملحقاتها :

إن أجهزة الحواسيب تتطور بشكل هائل بالمقابل هناك تطور في مجال السبل المستخدمة لاختراقها مما يتطلب تطوير القابليات و المهارات للعاملين في أقسام المعلومات لكي يستطيعوا مواجهة حالات التلاعب و العبث المقصود في الأجهزة أو غير المقصود .

ب. الأفراد العاملين في أقسام المعلومات :

يلعب الفرد دوراً أساسياً و مهماً في مجال أمن المعلومات و الحواسيب و له تأثير فعال في أداء عمل الحواسيب بجانبه الإيجابي و السلبي ، فهو عامل مؤثر في حماية الحواسيب و المعلومات و لكن في الوقت نفسه فإنه عامل سلبي في مجال تخريب الأجهزة و سرقة المعلومات سواء لمصالح ذاتية أو لمصالح الغير ، إن من متطلبات أمن الحواسيب تحديد مواصفات محددة للعاملين و وضع تعليمات واضحة لاختيارهم و ذلك للتقليل من المخاطر التي يمكن أن يكون مصدرها الأفراد إضافة الى وضع الخطط لزيادة الحس الأمني و الحصانة من التخريب ، كما يتطلب الأمر المراجعة الدورية للتدقيق في الشخصية و السلوكية للأفراد العاملين من وقت لآخر و ربما يتم تغيير مواقع عملهم و محاولة عدم احتكار المهام على موظفين محددين (سكيكر ، ٢٠١٠ ، ص ٤٩-٥١).

ج. البرمجيات المستخدمة في تشغيل النظام :

تعتبر البرمجيات من المكونات غير المادية و عنصر أساس في نجاح استخدام النظام ، لذلك من الأفضل اختيار حواسيب ذات أنظمة تشغيل لها خصائص أمنية و يمكن أن تحقق حماية للبرامج و طرق حفظ كلمات السر و طريقة إدارة نظام التشغيل و أنظمة الاتصالات ، إن أمن البرمجيات يتطلب أن يؤخذ هذا الأمر بعين الاعتبار عند تصميم النظام و كتابة برامجه من خلال وضع عدد من الإجراءات كالمفاتيح و العوائق التي تضمن عدم تمكن المستفيد من التصرف خارج الحدود المخول بها و تمنع أي شخص من إمكانية التلاعب و الدخول إلى النظام و ذلك من خلال أيضا تحديد الصلاحيات في مجال قراءة الملفات أو الكتابة فيها ، و محاولة التمييز بين اللذين يحق لهم الإطلاع و حسب كلمات السر الموضوعة ، وهناك أسلوبان للتمييز إما عن طريق البرمجيات أو استخدام الأجهزة المناسبة (السالي ، ٢٠١٩ ، ص ١٢٥-١٢٧).

د. شبكة تناقل المعلومات :

تعتبر شبكة تناقل المعلومات المحلية أو الدولية ثمرة من ثمرات التطورات في مجالات الاتصالات كما أنها سهلت عملية التراسل بين الحواسيب و تبادل و استخدام الملفات ، و لكن من جهة أخرى إتاحة عملية سرقة المعلومات أو تدميرها سواء من الداخل كاستخدام الفيروسات أو من خلال الدخول عبر منظومات الاتصال المختلفة ، لذلك لا بد من وضع إجراءات حماية و ضمان أمن الشبكات من خلال إجراء الفحوصات المستمرة لهذه المنظومات و توفير الأجهزة الخاصة بالفحص ، كما أن نظم التشغيل المستخدمة و المسؤولة عن إدارة الحواسيب يجب أن تتمتع بكفاءة و قدرة عالية على الكشف عن التسلل إلى الشبكة و ذلك من خلال تصميم نظم محمية بإقفال معقد أو عن طريق المجففات و ربطها بخطوط الاتصال و التي هي عبارة عن استخدام الخوارزميات الرياضية أو أجهزة و معدات لغرض تجفير تناقل المعلومات (عبد ربه ، ٢٠١٣ ، ص ٦٠-٦١).

هـ. مواقع منظومة الأجهزة الإلكترونية وملحقاتها :

يجب أن تعطى أهمية للمواقع و الأبنية التي يحوي أجهزة الحواسيب و ملحقاتها ، و حسب طبيعة المنظومات و التطبيقات المستخدمة يتم اتخاذ الإجراءات الإحترازية لحماية الموقع و تحصينه من أي تخريب أو سطو و حمايته من الحريق أو تسرب المياه و الفيضانات ، و محاولة إدامة مصدر القدرة الكهربائية و انتظامها و تحديد أساليب و إجراءات التفتيش و التحقق من هوية الأفراد الداخلين و الخارجين من الموقع و عمل سجل لذلك (السالمي ، ٢٠١٩ ، ص١٣٣).

إن ثورة المعلومات تحدث تغييرات عميقة في الطريقة التي تتم بها معالجة المعلومات وتخزينها. وهي تغير الطريقة التي تؤدي بها المنظمات، بل المجتمع ككل في حقيقة الأمر، وظائفه. فهي ليست الابتكار التقني الوحيد الذي حدث خلال السنوات الأخيرة، وإنما تبرز بسبب تأثيرها على معالجة المعلومات، ومن ثم على المعارف. ولأن ثورة المعلومات تؤثر في الآليات التي تُخَلَقُ بها المعارف وبها يتم تقاسمها، فيمكن اعتبارها منبعاً للابتكار في المستقبل لا ينبغي استبعاد البلدان النامية عنه. فثورة المعلومات وتكنولوجيات الاتصالات تؤدي إلى ثورة حقيقية في كيفية تفكيرنا في المبادلات الاقتصادية والاجتماعية والثقافية. وهي تزودنا كذلك بنموذج جديد لتكنولوجيا المعلومات يستند إلى الشبكة التي يحتاج أمن انسياب المعلومات عبرها إلى تأمين حتى يمكن تطوير الاستخدامات التطبيقية الجديدة التي ستزيد من فعالية التنظيمات. إذ لا يمكن لأي شكل من أشكال النشاط الاقتصادي أن يبقى بدون المبادلات وبدون التفاعل بين المشاركين فيه، ولا يمكن أن يحدث أي تبادل للمعلومات دون وجود نوع من ضمانات الأمن الأساسية. ولا يمكن تخطيط أي خدمة بدون مراعاة نوعية تلك الخدمة. غير أنه يجب علينا، مع ذلك، أن نضع نصب أعيننا أن نجاح اتصال ما يعتمد على قدرة الأطراف الضالعة فيه على التعامل مع العقبات التقنية وإدارة العادات التي تدخل في أي مبادلة للمعلومات (الهيئة الوطنية للأمن السيبراني، ٢٠١٨، ص٢٥-٢٧).

٥-النظريات المفسرة لإدارة مخاطر الأمن السيبراني

تتمثل النظريات المفسرة لإدارة مخاطر الأمن السيبراني ، فيما يلي :

١-نظرية النموذج الدائري للأمن السيبراني (Cybersecurity Diamond Model):

تعتبر هذه النظرية منهجا شاملا لفهم وتحليل مخاطر الأمن السيبراني. وتتألف النظرية من أربعة عناصر رئيسية هي: المهاجم (Adversary)، والضحية (Victim)، والسلوك (Behavior)، والتهديدات والضعف (Threats and Weaknesses). وتعزز هذه النظرية فهم كيفية تفاعل هذه العناصر وتوفر إطارا لتحليل المخاطر وتصميم استراتيجيات الحماية.

٢-نظرية الانحدار العقدي للأمن السيبراني (Cybersecurity Maturity Model):

تركز هذه النظرية على تقييم مستوى نضج أمان المؤسسة أو المنظمة. وتعتمد النظرية على تقدير القدرة على التحمل والاستجابة والاستعادة بعد وقوع هجمات سيبرانية. وتساعد هذه النظرية المؤسسات على تحديد نقاط الضعف وتحسين قدراتها في مجال الأمان السيبراني.

٣-نظرية السلسلة الإمدادية للأمان السيبراني (Cybersecurity Supply Chain):

تركز هذه النظرية على أهمية حماية سلسلة الإمداد التكنولوجي والتأكد من أمان الموردين والجهات الفاعلة الأخرى في البيئة السيبرانية. وتعتبر هذه النظرية مهمة في تقييم المخاطر المحتملة التي يمكن أن تنشأ عند التعامل مع جهات خارجية (فايز، ٢٠١٩، ص ٤٥-٤٧).

٤-نظرية السلوك البشري في الأمن السيبراني (Human Behavior in Cybersecurity):

تركز هذه النظرية على الجانب البشري في أمن المعلومات والأمان السيبراني. وتهدف النظرية إلى فهم سلوك المستخدمين والعاملين في المؤسسات وكيفية تأثيرهم على مخاطر الأمن السيبراني. وتعتبر التوعية والتدريب السلوكي للمستخدمين جزءا أساسيا من هذه النظرية.

٥-نظرية النموذج العام للتهديدات السيبرانية (General Model of Cyber Threats):

تقدم هذه النظرية نموذجا شاملا لفهم التهديدات السيبرانية وأنماطها. وتعتمد النظرية على تحليل الهجمات السيبرانية السابقة والتعرف على الأنماط المشتركة والعوامل المؤثرة في

تكرارها. ويتيح هذا النموذج للمؤسسات تحديد الثغرات الأمنية المحتملة واتخاذ التدابير الوقائية المناسبة.

٦-نظرية تحليل الأخطار(Risk Analysis Theory):

تركز هذه النظرية على تحليل المخاطر وتقييمها في سياق الأمن السيبراني. وتعتمد النظرية على تحديد وتصنيف المخاطر السيبرانية المحتملة وتقييم مدى تأثيرها واحتمالية حدوثها. ويتيح هذا التحليل للمؤسسات تحديد الأولويات وتخصيص الموارد للتعامل مع المخاطر الأكثر تأثيرا.

٧-نظرية الاستجابة للحوادث السيبرانية (Incident Response Theory):

تهدف هذه النظرية إلى تطوير إطار عمل للاستجابة الفعالة للحوادث السيبرانية. وتشمل هذه النظرية إجراءات وممارسات للكشف عن الاختراقات والتعامل معها واستعادة النظام بعد الحادث. وتوفر هذه النظرية الإرشادات اللازمة للمؤسسات للتعامل مع الحوادث السيبرانية بشكل منهجي وفعال.

٨-نظرية السلوك البشري في الأمن السيبراني (Human Behavior Theory in Cybersecurity):

تركز هذه النظرية على فهم سلوك المستخدمين ودورهم في تعزيز الأمن السيبراني أو تعريضه للمخاطر. وتهدف النظرية إلى تحليل العوامل النفسية والسلوكية التي تؤثر في قرارات المستخدمين المتعلقة بالأمن السيبراني، مثل التصرفات السلوكية الخاطئة أو الاستخدام السليم لكلمات المرور (سكيكر، ٢٠٢٢، ص ١١٣-١١٥).

ويتبنى الباحث في تلك الدراسة نظرية تحليل الأخطار، حيث أن نظرية تحليل الأخطار تعتبر أحد الجوانب الهامة في مجال الأمن السيبراني. ففي سياق الأمن السيبراني، يتعامل المختصون مع الجوانب التقنية والتحديات الفنية، ولكن يجب أيضا أن يأخذوا في الاعتبار الجانب البشري. فالبشر يشكلون جزءا أساسيا في أنظمة الأمان وقد يكونون عرضة للهجمات السيبرانية أو قد يسببون تهديدا غير مقصود للأمن.

المنهجية وطرق البحث:

منهج الدراسة

سوف يتبع الباحث في هذه الدراسة المنهج الوصفي التحليلي ، إذ يختص بوصف الواقع من أجل فهمه وكيفية التعامل معه فهو تمهيد منطقي لوصف واقع الأشياء.

مجتمع وعينة البحث

سوف يتحدد مجتمع الدراسة في منسوبي وزارة الاتصالات وتقنية المعلومات والبالغ عددهم (٥٧٠) موظف وموظفة (الهيئة العامة للإحصاء، ١٤٤٤ ، ص٩٦).

وسوف يتم اختيار نسبة لا تقل عن ٢٠% من منسوبي وزارة الاتصالات وتقنية المعلومات. وسوف يتم اختيار العينة بالطريقة العشوائية عن طريق وضع الأسماء على جهاز الحاسب الآلي والاختيار من بينها.

وسوف تتكون هذه الدراسة، مما يلي:

الفصل الأول: مقدمة البحث.

الفصل الثاني: الإطار النظري والدراسات السابقة.

الفصل الثالث: إجراءات البحث (المنهجية والإجراءات)

الفصل الرابع: الدراسة الميدانية وتحليل ومناقشة النتائج.

الفصل الخامس: خلاصة لأهم نتائج الدراسة وتوصياتها

المصادر والمراجع، ثم الملاحق.

أدوات الدراسة :

أداة البحث

سوف يقوم الباحث بتصميم إستبانه من خلال النظر إلى الأدبيات والدراسات السابقة ، وسوف تتكون أداة الدراسة من قسمين، نوضحها كما يلي:

القسم الأول: البيانات الشخصية.

القسم الثاني: محاور الاستبانه.

وسوف يستخدم الباحث مقياس ليكرت الخماسي للتعرف على إستجابات عينة الدراسة لفقرات الإستبانه، والجدول التالي يوضح بدائل الإستجابات:

جدول رقم (١)

مقياس ليكرت الخماسي

المعيار	موافق بشدة	موافق	إلى حد ما	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1
المتوسط الحسابي	٥.٠٠-٤.٢٠	4.19-3.40	3.39-2.60	2.59-1.80	1.79-1.00
درجة الموافقة	مرتفعة جداً	مرتفعة	متوسطة	منخفضة	منخفضة جداً

حدود الدراسة :

تحدد الدراسة الحالية بالحدود التالية:

■ الحدود الموضوعية:

سوف تركز الدراسة على إدارة مخاطر الأمن السيبراني في المؤسسات الحكومية بالمملكة العربية السعودية – بالتطبيق على وزارة الاتصالات وتقنية المعلومات.

■ الحدود البشرية:

منسوبي وزارة الاتصالات وتقنية المعلومات.

■ الحدود المكانية:

منطقة الرياض.

■ الحدود الزمنية:

سوف تجري الدراسة خلال العام ١٤٤٥هـ/٢٠٢٤م.

المراجع المتوفرة حول البحث:

المراجع العربية :

- الاتحاد الدولي للاتصالات. (٢٠١٩). الأمن السيبراني في المملكة العربية السعودية. بيروت: مطابع الاتحاد الدولي للاتصالات.
- إبداح، باسم محمد. (٢٠١٩). أمن وسرية المعلومات وأثرها على الأداء التنافسي دراسة تطبيقية في شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية. رسالة ماجستير منشورة. كلية إدارة الأعمال، جامعة بغداد. بغداد.
- البار، عدنان مصطفى. (٢٠٢١). أمن المعلومات والأمن السيبراني. جدة: جامعة الملك عبد العزيز.
- حمدان، أحمد عبد الله. (٢٠٢١). أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن. رسالة ماجستير منشورة. كلية السلط التقنية، جامعة البلقاء التطبيقية، البلقاء.
- الخالدي، ساري محمد. (٢٠١٦). اتجاهات في أمن المعلومات وأمانها: أهمية تقنيات التعمية - التشفير. المنامة: أكاديمية الخليج العربي للدراسات.
- درويش، محمود أحمد. (٢٠١٨). مناهج البحث في العلوم الإنسانية. الرياض: مكتبة ابن تيمية للنشر.
- الزهراني، أحمد سعيد. (٢٠١٨). آثار قرصنة البرمجيات عالميا. رسالة ماجستير منشورة. كلية العلوم الإستراتيجية. جامعة نايف العربية للعلوم الأمنية: الرياض.
- السالمي، علاء الكيلاني. (٢٠١٩). أساسيات نظم المعلومات الإدارية. مكتبة وائل: عمان.
- سكيكر، محمد علي. (٢٠٢٢). الجريمة المعلوماتية و كيفية التصدي لها. ط٢. الدار البيضاء: دار النشر المغربية.

- السهلي، فارس بن صالح. (٢٠١٩). نطاق مسؤولية الناقل الجوي للركاب وأساسها في نظام الطيران المدني السعودي. الرياض: مطابع وزارة الداخلية.
- الشراري، خالد جويش. (٢٠١٧): الأمن السيبراني في المملكة العربية السعودية. الرياض: مكتبة دار القلم.
- الصيدلاني، خالد صالح. (٢٠١٧). واقع قرصنة البرمجيات في الأردن وسبل مواجهتها. رسالة ماجستير منشورة. كلية الأعمال : الجامعة الأردنية.
- عبد ربه ، رائد محمد. (٢٠٢٠). مبادئ نظم المعلومات الإدارية. بيروت: مكتبة بيروت الحرة.
- عطوان، أسعد محمد. (٢٠١٦). مناهج البحث العلمي. ط٢. القاهرة: مكتبة دار المعارف.
- العضياني ، ماجد محمد . (٢٠١٨) . انتهاك خصوصية البيانات في مؤسسات الأعمال وأثره على أداء المؤسسات . رسالة ماجستير منشورة .كلية التجارة . القاهرة : جامعة القاهرة .
- الغامدي، محمد حسن. (٢٠٢١) . فرص حلول الأمن السيبراني في المملكة العربية السعودية . الرياض: مطابع فنتك السعودية.
- فايز ، وائل علي. (٢٠١٩) . دور تكنولوجيا المعلومات في تدعيم أداء الموارد البشرية (دراسة ميدانية) .رسالة ماجستير منشورة . كلية التربية. المنصورة: جامعة المنصورة.
- القحطاني ، منصور سعيد. (٢٠١٩) . مهددات الأمن المعلوماتي وسبل مواجهتها. ط٢. الرياض : مكتبة دار القلم .
- الكبيسي، حامد جهاد. (٢٠١٩). مناهج البحث العلمي في العلوم الإدارية. الرياض: مكتبة العبيكان.
- موقع الهيئة العامة للطيران المدني بالمملكة العربية السعودية
<https://www.gaca.gov.sa/web/ar-sa/page/home>
- نوبي ، فاطمة إبراهيم . (٢٠٢١) . أثر كفاءة أداء الموارد البشرية على سلامة الطيران المدني بالتطبيق على قطاع الطيران المدني المصري. القاهرة : أكاديمية السادات.

- الهيئة الوطنية للأمن السيبراني. (٢٠١٨). التعريف بالهيئة الوطنية للأمن السيبراني . الرياض : مطابع وزارة الداخلية.
- الهيئة الوطنية للأمن السيبراني. (٢٠١٨). الضوابط الأساسية للأمن السيبراني في المملكة العربية السعودية . الرياض: مطابع وزارة الإعلام.
- الهيئة العامة للإحصاء. (٢٠١٨). موجز إحصاءات هيئة الطيران المدني بالمملكة العربية السعودية. الرياض: مطابع الهيئة العامة للإحصاء.
- ياغي، محمد. (٢٠١٧). الأمن المعلوماتي وإدارة العلاقات الدولية. عمان: دار وائل للنشر والتوزيع.

المراجع الأجنبية :

- Lipps، k (2020). *Interest in organizing information technology courses, a new educational entrance in the European Union*. Eric Digest. (110). Ed:823493.
- Lerner, G (2021). *The role of information technology in the preparation of human competencies at the Center (Izonti). An Electronic Journal of the U.S. Department of Educational Sciences*. from <http://usinfo.state.gov/journals>.
- Stephen, S. (2018). Reasons for individuals and organizations to violate the privacy of information, and the role of cyber security in the face of the phenomenon. Eric Digest . No.(284) . Ed:536981.
- Waldo, R. (2018). Cyber awareness of the privacy of information and data using web-based knowledge flights, a new educational portal in the European Union. Eric Digest .No.(263) . Ed:598680.