مجلة الجامعة الإسلامية

للعلوم التربوية والاجتماعية

مجلة علمية دورية محكمة

تصدر أربع مرات في العام خلال الأشهر:

(مارس، يونيو، سبتمبر، ديسمبر)

العدد الثامن عشر - الجزء الأول

ذو القعدة 1445 هـ - يونيو 2024 م

معلومات الإيداع في مكتبة الملك فهد الوطنية

النسخةالورقية :

رقم الإيداع: 1441/7131

تاريخ الإيداع: 1441/06/18

رقم ردمد : 1658-8509

النسخة الإلكترونية :

رقم الإيداع: 1441/7129

تاريخ الإيداع: 1441/06/18

رقم ردمد : 1658-8495

الموقع الإلكتروني للمجلة :

https://journals.iu.edu.sa/ESS

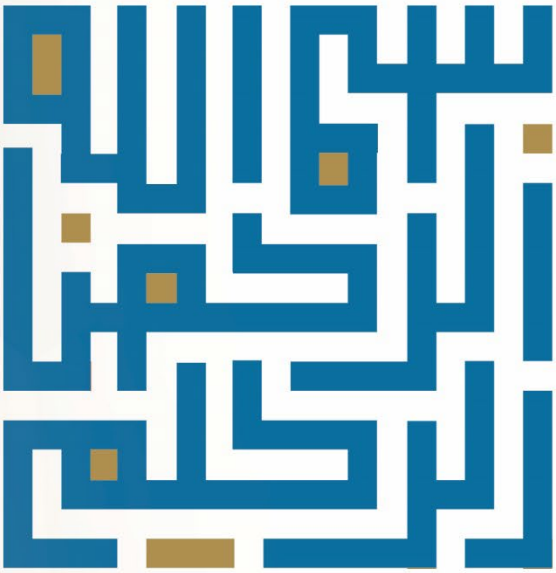
البريد الإلكتروني للمجلة :

ترسل البحوث باسم رئيس تحرير المجلة

iujournal4@iu.edu.sa

الجامعة الإسلامية بالمدينة المنورة
ISLAMIC UNIVERSITY OF MADINAH

البحوث المنشورة في المجلة تعبرعن آراء الباحثـين ولا تعبر بالضرورة عن رأي المجلة



قواعد وضوابط النشر في المجلة

- أن يتسم البحث بالأصالة والجدية والابتكار والإضافة المعرفية في التخصص.
- لم يسبق للباحث نشر بحثه.
- أن لا يكون مستلاً من أطروحة الدكتوراه أو الماجستير سواء بنظام الرسالة أو المشروع البحثي أو المقررات.
- أن يلتزم الباحث بالأمانة العلمية.
- أن تراعى فيه منهجية البحث العلمي وقواعده.
- أن لا تتجاوز نسبة الاقتباس في البحوث التربوية (25%)، وفي غيرها من التخصصات الاجتماعية لا تتجاوز (40%).
- أن لا يتجاوز مجموع كلمات البحث (12000) كلمة بما في ذلك الملخصين العربي والإنجليزي وقائمة المراجع.
- لا يحق للباحث إعادة نشر بحثه المقبول للنشر في المجلة إلا بعد إذن كتابي من رئيس هيئة تحرير المجلة.
- أسلوب التوثيق المعتمد في المجلة هو نظام جمعية علم النفس الأمريكية (APA) الإصدار السابع، وفي الدراسات التاريخية نظام شيكاغو.
- أن يشتمل البحث على : صفحة عنوان البحث، ومستخلص باللغتين العربية والإنجليزية، ومقدمة، وصلب البحث، وخاتمة تتضمن النتائج والتوصيات، وثبت المصادر والمراجع، والملاحق اللازمة مثل: أدوات البحث، والموافقات للتطبيق على العينات وغيرها؛ إن وجدت.
- أن يلتزم الباحث بترجمة المصادر العربية إلى اللغة الإنجليزية.
- يرسل الباحث بحثه إلى المجلة إلكترونيًا ، بصيغة (WORD) وبصيغة (PDF) ويرفق تعهدًا خطيًا بأن البحث لم يسبق نشره ، وأنه غير مقدم للنشر، ولن يقدم للنشر في جهة أخرى حتى تنتهي إجراءات تحكيمه في المجلة.
- المجلة لا تفرض رسوما للنشر.

الهيئة الاستشارية :

هيئة التحرير:

الجامعة الإسلامية بالمدينة المنورة

ISLAMIC UNIVERSITY OF MADINAH

فهرس المحتويات : *

م	عنوان البحث	الصفحة
1	أثر استخدام ChatGPT كدعامة تعليمية في تنمية مهارات إدارة قواعد البيانات لطلاب المرحلة الجامعية د. علي بن سويعد علي القرني	11
2	المتطلبات التنظيمية لإدارة الأمن السيبراني بوزارة التعليم د. عبد الله بن عبد الرحمن الفنتوخ	47
3	صعوبات الإشراف الأكاديمي التي تواجه طالبات الدراسات العليا بكلية التربية بجامعة الملك سعود من وجهة نظرهن د. أمل بنت عبد الله بن راشد الكليب	95
4	The Utilization of ChatGPT in Education: Opportunities and Challenges د. سلطان بن حماد الشمري	143
5	بناء مقياس لتقييم مؤشرات الابتكار المؤسسي في الجامعات السعودية د. منال بنت أحمد عبد الرحمن الغامدي	159
6	التشارك المعرفي لدى طالبات الدراسات العليا بكلية التربية بجامعة الملك سعود من وجهة نظرهن د. ابتسام بنت عبد الكريم العودة	207
7	الكفاءة الذاتية المدركة وعلاقتها بالتنظيم الذاتي والاتزان الانفعالي لدى معلمات المرحلة الابتدائية بمنطقة القصيم د. أمل بنت صالح سليمان الشريدة	255
8	واقع أبعاد التنمية المستدامة في كتاب الدراسات الاجتماعية للصف الثالث المتوسط وتصور مقترح لتضمينها د. محمد بن حارب مليفي الشريف	295
9	الاحتفالات في مكة المكرمة خلال عهد الملك عبد العزيز 1343-1373هـ /1924-1953م دراسة تاريخية حضارية د. سحر بنت علي محمد دعدع	339
10	العلاقات السياسية السعودية العُمانية في عهد الدولة السعودية الثانية 1244-1291هـ/1828-1874م د. أحمد بن عبد الله العرف	379

* ترتيب الأبحاث حسب تاريخ ورودها للمجلة مع مراعاة تنوع التخصصات

الجامعة الإسلامية بالمدينة المنورة

ISLAMIC UNIVERSITY OF MADINAH

المتطلبات التنظيمية لإدارة الأمن السيبراني بوزارة التعليم

Organizational Requirements for Cybersecurity Management in the Ministry of Education

إعداد

د. عبد الله بن عبد الرحمن الفنتوخ

أستاذ الإدارة والتخطيط التربوي المشارك

قسم الإدارة والتخطيط التربوي –كلية التربية

جامعة الإمام محمد بن سعود الإسلامية

Dr. Abdullah bin Abdulrahman Al Fantoukh

Associate Professor of Educational Administration and Planning

Department of Educational Administration and Planning

College of Education - Imam Mohammad Ibn Saud Islamic University (IMSIU)

Email: aafantookh@imamu.edu.sa

DOI:10.36046/2162-000-018-002

المستخلص

هدفت الدراسة التعرف على المتطلبات التنظيمية لإدارة الأمن السيبراني بوزارة التعليم من وجهة نظر مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية، وما إذا كان هناك فروق دالة إحصائيًا باختلاف (العمل الحالي، والخبرة في العمل الحالي، وعدد الدورات في مجال الأمن السيبراني). وقد طبقت على عينة من مجتمع الدراسة المكون من مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة بلغت (٨٨) مشرفًا ومشرفة، واستخدمت الدراسة المنهج الوصفي المسحي، والاستبانة أداةً لها، وتوصلت الدراسة إلى وجود مستوى عالي من الاتفاق بين عينة الدراسة على محور المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم، بمتوسط (٣,٥٠) وأعلى متوسط كان لفقرة "توفير دليل معتمد لسياسات وإجراءات الأمن السيبراني". ووجود مستوى عالي من الاتفاق بين عينة الدراسة على محور المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم، بمتوسط (٤,١٦) وأعلى متوسط كان لفقرة "توفير برامج وقائية باستمرار حمايةً للأجهزة". كما تبين وجود فروق دالة إحصائيًا باختلاف العمل الحالي، والخبرة في العمل الحالي، وعدد الدورات في مجال الأمن السيبراني. وأوصت الدراسة بالقيام بالتطوير الإداري والتقني للبنية التحتية التقنية داخل الوزارة وفي الميدان التعليمي، وإجراء تحديث للسياسات والإجراءات الأمنية متزامنًا مع تدريب وتأهيل الكوادر البشرية تقنيًا.

الكلمات المفتاحية: المتطلبات التنظيمية، إدارة الأمن السيبراني.

Abstract

The study aimed to identify the organizational requirements for cybersecurity management in the Ministry of Education from the perspective of information technology supervisors in the ministry and education departments in the Kingdom of Saudi Arabia, and whether there are statistically significant differences depending on (current work, experience in current work, and the number of courses in the field of cybersecurity). The study was applied to a sample of the study community consisting of information technology supervisors in the ministry and education departments in the Kingdom, totaling (88) supervisors, and the study used the descriptive survey method, and the questionnaire as a tool for it. The study found that there was a high level of agreement between the study sample on the axis of the administrative requirements for cybersecurity management in the Ministry of Education, with an average of (3.50), and the highest average was for the paragraph "Providing an approved guide to cybersecurity policies and procedures." There was also a high level of agreement between the study sample on the axis of the technical requirements for cybersecurity management in the Ministry of Education, with an average of (4.16), and the highest average was for the paragraph "Providing continuous preventive programs to protect devices." It was also found that there were statistically significant differences depending on the current work, the experience in the current work, and the number of courses in the field of cybersecurity. The study recommended that the administrative and technical development of the technical infrastructure within the ministry and in the educational field be carried out, and that the security policies and procedures be updated in conjunction with the training and qualification of human resources technically.

Keywords: Organizational requirements, cybersecurity management.

المقدمة

يعيش العالم اليوم في منظومة حياتية تتحكم فيها متغيرات تختلف جذريًا عما كان في سابق العصور، ومن أبرز المتغيرات المتسارعة تقنية المعلومات وما تحتويه من تفريعات وأجزاء تستلزم مواكبه هذه التقنية من أجل العيش ومسايرة العالم التقني.

وعلى رغم تعدد ايجابيات التقنية الا أن هناك سلبيات نتج عنها ظهور مشكلات أبرزها تهديدات وجرائم واحتيالات. فقد أدت الثورة الرقمية المعاصرة إلى إيجاد آفاق غير مسبوقة لتبادل المعلومات والأفكار بين ملايين المستخدمين لشبكة الإنترنت حول العالم، وانعكس هذا الأمر على كافة المجالات، ومع انتشار الهواتف الذكية والأجهزة الكفية المحمولة، فقد أصبح استخدام شبكة الإنترنت أمراً متاحاً وملحًا لجميع أفراد المجتمع على اختلاف فئاتهم العمرية. ومع التدفق المستمر والهائل للمعلومات، واعتماد الملايين حول العالم من أفراد ومؤسسات خاصة وحكومية على استخدام شبكة الإنترنت للتواصل الاجتماعي أو إنجاز العديد من المعاملات، فقد ظهر تهديدٌ جديد لهؤلاء المستخدمين حيث اتجه البعض إلى اختراق شبكات المعلومات، والتلاعب بالمعلومات وإيذاء المستخدمين بصور وأساليب متعددة، وذلك فيما يعرف بالجريمة السيبرانية Cyber Crime (hang et al., 2013, p.1881).

ومما لا شك فيه أن قضية أمن وحماية المعلومات تُعد من أهم القضايا في العصر الحالي فنجاح أي منظمة يتوقف بشكل كبير وواضح على ما تمتلكه من المعلومات التي تشكل عصب المنظمة، ولابد وضع الاحتمال الكبير بأن تلك المعلومات والأنظمة معرضة للمخاطر بين الحين والآخر. مما يستلزم استخدام نظام أمن للحماية من تلك المخاطر، تبلورت فكرته ومنطلقه في ظهور ما يسمى بالأمن السيبراني (cyber security) كنظام أمني ذو بُعد إداري فني تقني شامل.

ولذا فالأمن السيبراني هو أساسٌ لأي تحول رقمي للمؤسسات، وهو يعتمد على الاستفادة من التكنولوجيات الرقمية دون خوف، وزيادة فرص الابتكار والتطوير، كما يُعد سلاحًا استراتيجيا في أيدي الحكومات والأفراد، بل أصبح يمثل نهجًا استراتيجيًا للتخطيط والتصميم والتشغيل؛ يتضمن جميع الجوانب التعليمية، والاجتماعية، والاقتصادية، والإنسانية، وله تأثير فعال

على المعلومات والحفاظ عليها، كونه يرتبط ارتباطاً وثيقًا بسلامة مصادر الثروة المعلوماتية في عصر التحول الرقمي لكل المؤسسات ومنها الجامعات (الصانع وآخرون، ٢٠٢٠)

إن هذا التحول يتطلب انسيابية المعلومات وأمانها وتكامل أنظمتها، ولذا فقد حرصت المملكة العربية السعودية على منظومة الأمن السيبراني فيها وتعزيزها حمايةً للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات النشطة الحكومية؛ لذلك صدر أمرٌ ملكيٌ برقم (٦٨٠١) بإنشاء هيئة باسم الهيئة الوطنية للأمن السيبراني، في تاريخ (١١) صفر ١٤٣٩هـ ترتبط بمقام خادم الحرمين الشريفين وهي الجهة المختصة بشؤون الأمن السيبراني في المملكة، وتعد مرجع الدولة لحماية أمنها الوطني، ومصالحها الحيوية والبنية التحتية الحساسة فيها، وتوفير خدمات تقنية آمنه وطرق دفاعية لحماية أنظمة المعلومات والاتصالات ضد الهجمات الإلكترونية، والحفاظ على سرية وسلامة المعلومات.(الهيئة الوطنية للأمن السيبراني: المملكة على الموقع https://ega.ee/wp content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf كما أنشئت منصة على الإنترنت خاصة بالأمن السيبراني في المملكة من خلال المنصة الوطنية الموحدة بالرابط التالي:

(https://www.my.gov.sa/wps/portal/snp/content/cybersecurity)

ولأهمية الأمن السيبراني في الميدان التعليمي فقد وقعت وزارة التعليم والهيئة الوطنية للأمن السيبراني اتفاقية لتعزيز التعاون المشترك في مجالات التعليم والبحث العلمي والتدريب والتوعية في مجال الأمن السيبراني، بما يسهم في تأهيل الكوادر الوطنية وبناء القدرات في مجال الأمن السيبراني، تضمنت مجالات التعاون، والدعم المشترك في برامج التعليم والتدريب وبناء القدرات في مجال الأمن السيبراني، ورفع جودة مخرجات البرامج التعليمية في الأمن السيبراني، ورفع مستوى الوعى بالأمن السيبراني في التعليم (وزارة التعليم الهيئة الوطنية للأمن السيبراني، ٢٠٢١)

مشكلة الدراسة:

أدى التسارع الكبير في عمليات التحول الرقمي في كافة المجالات إلى ارتفاع معدلات الهجمات الإلكترونية ومخاطر اختراق البيانات نظرًا لانشغال العالم في البنى التحتية واستغلال الثغرات من قبل ذوي الاحتيالات الإلكترونية، وقد صاحبتها ظاهرة الجريمة الرقمية، التي تصاعدت

أخطارها، محدثةً نوعًا جديدًا من الجرائم العابرة للقارات، التي لم تعُد أخطارها وأثارها محصورةً في نطاق دولة بعينها مما أثار تحديات قانونية أمام الأجهزة المعنية بمكافحة الجريمة في كافة أصقاع المعمورة.

وقد أحدثت الهجمات الإلكترونية أضررًا كبيرةً على البنى التحتية، ففي المملكة العربية السعودية كانت أبرز الحوادث الرئيسة في هذه الهجمات بدايةً استهداف شركة أرامكو السعودية في عام ٢٠١٢ والتي عطلت نشاط الشركة لمدة شهر فيما يشار إليه بأكبر اختراق في التاريخ، وتكرر الخلل مرة أخرى بسبب هذه البرمجيات الخبيثة في نوفمبر ٢٠١٦ ويناير ٢٠١٧م.

ويذكر (أبو زيد، ٢٠١٩) أن تقرير Over Security Advisory Council الصادر في ٢٠١٦، أكد أن الهجوم علي شركة أرامكو السعودية قد كلفها تغيير ٥٠٠٠٠ قرص صلب لأجهزتها الحاسوبية ولم تستطع استخدام الإنترنت لمدة خمسة أشهر تقريبا، وهذا يعتبر زمنًا قياسيًا في الإصلاح، خاصةً إذا ما أخذنا في الاعتبار إمكانات أرامكو المالية والتقنية؛ وفي عام ٢٠١٣، عانت بنوك الإمارات العربية المتحدة وسلطنة عمان من خسارة بلغت أكثر من ٤٥ مليون دولار أمريكي بسبب واحدة من أكبر عمليات سرقة أجهزة الصراف الآلي الإلكترونية في المنطقة. كما هاجم فيروس Mamba Ransomware المملكة العربية السعودية في يوليو ٢٠١٧، وتم استهداف شبكات الشركات داخل المملكة العربية السعودية. ظهرت Mamba Ransomware في عام ٢٠١٦ في الولايات المتحدة الأمريكية وكانت واحدة من الفيروسات الأولى التي لا تشفر الملفات، ولكن الأقراص الصلبة بأكملها. ويستخدم أداة شرعية Disk Cryptor لتشفير القرص بأكمله.

ولذا فالهجمات الإلكترونية تستهدف الثغرات التي تسمح لها بالاختراق في جميع القطاعات تعليميةً كانت أو غيرها، ويكفي في هذا السياق ما أشارت إليه الإحصاءات الصادرة عن هيئة البيانات والذكاء الاصطناعي أنها تعاملت مع كم هائل من التهديدات السيبرانية التي استهدفت منصات مجموعة العشرين أثناء انعقادها افتراضياً في مارس ٢٠٢٠ في الرياض، حيث بلغ عدد الهجمات الإلكترونية التي صُدت على منصة بروق من خلال أنظمة الحماية الخاصة التي طورتها نحو (٢٠٨) مليون هجمة إلكترونية، بينما كان عدد الإنذارات الأمنية التي تم التعامل معها عبر مركز العمليات الأمنية (٢٨) إنذاراً (موقع الهيئة السعودية للبيانات والذكاء الاصطناعي، ٢٠٢١)

وما سبق دعى المملكة إلى تفعيل دور المؤسسات التربوية والتعليمية في مجال الأمن السيبراني، حيث شهد عام (٢٠١٨) توقيع اتفاقية تعاون بين الهيئة الوطنية للأمن السيبراني ووزارة التعليم ممثلة بوكالة الوزارة لشؤون الابتعاث وأسفرت تلك الاتفاقية عن إفساح المجال للابتعاث الخارجي في تخصصات الأمن السيبراني، شبكات الحاسب والذكاء الاصطناعي، وتم تخصيص (١٠٠٠) مقعد لقطاع الأمن السيبراني بواقع (٢٠٠) مبتعث لمدة خمس سنوات، وذلك في أفضل الجامعات الأمريكية والبريطانية والكندية (https://ksp.moe.gov.sa).

كما أطلقت مبادرة حصين من أجل تعزيز الأمن السيبراني على المستوى الوطني وتعنى بحماية البريد الإلكتروني من الانتحال والاستخدام غير المصرح به، وتطبق هذه المبادرة على الجهات الحكومية في المملكة وتشمل الوزارات والهيئات والمؤسسات وغيرها، وجهات القطاع الخاص التي تمتلك بنى تحتية وطنية حساسة، وتشجع الهيئة الجهات الأخرى في المملكة على الاستفادة من تطبيق هذه المبادرة لتحسين الأمن السيبراني وتطويره داخل الجهة (موقع مبادرة حصين، ٢٠٢١م).

ولا يخفى أن التطور التقني في المؤسسات التعليمية يعتريه ما يعتري جميع القطاعات بلا استثناء، فيذكر (الألفي ،٢٠٢٢) أن عددًا من المؤسسات التعليمية اكتفى بشراء بعض البرامج للوقاية من الفيروسات الإلكترونية؛ إلا أن هذه البرامج لم تفلح في وقاية المؤسسات التعليمية من الهجمات الإلكترونية.

ولذا فإن هذه التحديات تستلزم حماية قواعد البيانات من الاختراقات، إلا أن الواقع الحالي في دراسة الخضري وسلامي وكليبي (٢٠٢٠) بينت وجود اتفاق بين عينة البحث حول تعدد أسباب حدوث المخاطر، والسبب في ذلك عدم وجود سياسات أمنية واضحة وبرامج حماية، وكان مما أوصت به الدراسة بناءً على نتائجها العمل على زيادة الاهتمام بتوعية المؤسسات الجامعية السعودية حول تطبيق معايير أمن المعلومات، وتنظيم دورات تدريبية للطلاب وأعضاء هيئة التدريس والإداريين لتدريبهم على تطبيق أمن المعلومات، وتنظيم دورات تدريبية للقيادات التربوية هدفها تنمية الاعتماد على الذكاء الاصطناعي في صنع القرار التعليمي، كذلك دراسة المنتشري (٢٠٢٠) التي أظهرت أن دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات ولدى طالبات المدرسة متحقق بدرجة موافقة قليلة، ودراسة المنيع(٢٠٢٢) ودراسة فرج (٢٠٢٢)

التي بينتا أن واقع تحقيق الأمن السيبراني وثقافته متحقق بدرجة متوسطة، أما دراسة دراسة الشيتي (٢٠١٩) فقد بينت الافتقار لوجود إدارة متخصصة في أمن المعلومات بجامعة القصيم، بالإضافة إلى ضعف اتباع سياسة الهوية الآلية لأمن المعلومات، وضعف سياسات حماية المعلومات.

كل هذا استدعى دراسة المتطلبات التنظيمية بشقيها الإداري والفني للوقوف على أكثرها تلمسًا في الميدان من أجل تسهيل الإجراءات لدى صناع القرار بوزارة التعليم ومن خلال ما يطرحه مشرفي تقنية المعلومات بالوزارة والميدان التعليمي.

أسئلة الدراسة:

١– ما المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم من وجهة نظر مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية؟

٢– ما المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم من وجهة نظر عينة الدراسة؟

٣– هل توجد فروق ذات دلالة إحصائية تجاه المتطلبات الإدارية والفنية باختلاف متغيرات الدراسة (العمل الحالي، والخبرة في العمل الحالي، وعدد الدورات في مجال الأمن السيبراني)؟

أهداف الدراسة:

١– تحديد المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم من وجهة نظر مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية.

٢– تحديد المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم من وجهة عينة الدراسة.

٣– التعرف على الفروق ذات الدلالة الإحصائية تجاه المتطلبات الإدارية والفنية باختلاف متغيرات الدراسة (العمل الحالي، والخبرة في العمل الحالي، وعدد الدورات في مجال الأمن السيبراني).

أهمية الدراسة:

- تتزامن الدراسة الحالية مع رؤية المملكة ٢٠٣٠، والتي تؤكد على دعم استخدام تقنيات المعلومات وتعزيز البنية الرقمية.

- استجابة لمشروع الهيئة الوطنية للأمن السيبراني الذي يركز على تعزيز الأمن السيبراني وحماية الأمن الوطني.
- إطلاع متخذي القرار بوزارة التعليم بأبرز المتطلبات التنظيمية لإدارة الأمن السيبراني بالوزارة.
- دعم الإدارة العامة للأمن السيبراني بوزارة التعليم بأبرز المتطلبات التنظيمية حمايةً لأنظمتها.
- اطلاع متخذي القرار بوزارة التعليم بالواقع الإداري والفني لإدارة الأمن السيبراني وكيفية النهوض به عمليًا.
- الإسهام في حل العقبات التي تعترض الأمن السيبراني على مستوى وزارة التعليم والمنصات لدى الطلاب في منازلهم.

حدود الدراسة:

-الحد الموضوعي: دراسة المتطلبات التنظيمية لإدارة الأمن السيبراني بوزارة التعليم، من خلال التعرف على المتطلبات الإدارية والفنية لإدارة الأمن السيبراني من وجهة نظر مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية.

- الحد المكاني: وزارة التعليم وإدارات التعليم بالمملكة العربية السعودية.

-الحد الزماني: الفصل الدراسي الثالث ١٤٤٤.

- الحد البشري: مشرفي ومشرفات تقنية المعلومات في وزارة التعليم وإداراتها بالمملكة العربية السعودية.

مصطلحات الدراسة:

- إدارة الأمن السيبراني:

يُعد مفهوم الأمن السيبراني من المفاهيم الحديثة، وهو مشتق من لفظة السايبر (Cyber) اللاتينية ومعناها: الفضاء المعلوماتي. والفضاء المعلوماتي (Cyber) هو مفهوم جديد في عالم أمن

المعلومات، ويشير إلى مساحة ضخمة من جميع أشكال الأنشطة الإلكترونية مثل الإنترنت، والهواتف المحمولة، والشبكات السلكية، واللاسلكية. (Otoom & Abu Ali Atoum, 2014).

ويعرفه غسان (٢٠١٩) بأنه " عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الوصول غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين، والمستهلكين في الفضاء السيبراني.

وتذكر وزارة التعليم في سياسة الأمن السيبراني(١٤٤٢) أن إدارة الأمن السيبراني هي" إدارة معنية بحوكمة واستراتيجيات واعتماد الإجراءات والمعايير الداعمة لسياسة الأمن السيبراني، وحماية الشبكات، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها ".

ويعرفها الباحث إجرائيًا بأنها: الإجراءات والاحترازات والتدابير التي تتخذها وزارة التعليم ممثلةً إداريًا في الإدارة العامة للأمن السيبراني، وبشريًا في مشرفي التقنية، وتقنيًا في الأدوات المستخدمة من قبل تقنين الوزارة، لحماية سلامة الشبكات والأجهزة من الهجوم أو الوصول غير المصرح به، وتحديث برامج الحماية باستمرار في ضوء تطبيق إجراءات ومعايير إدارية.

الإطار النظري للدراسة

- مفهوم الأمن السيبراني:

أدت التغيرات المتسارعة إلى نشؤ مصطلحات حديثة تستلزم الوقوف عليها وسبر أغوارها ومن ذلك الأمن السيبراني، والهجمات الإلكترونية، ولذا فقد أشار (Fouad,٢٠٢١) أن السيبرانية تعني الإلكترونية، وقد اتفق علماء المعلوماتية على إطلاق لفظ "سيبراني على ما يتعلق بالشبكات الإلكترونية المرتبطة الإنترنت والتطبيقات المتنوعة مثل (تويتر، فيس بوك، واتس أب.. الخ).

كما أوضحت الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (P262.2018) مفهوم الأمن السيبراني بأنه: "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق، أو تعطيل، أو تعديل، أو دخول استخدام، أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي، ونحو ذلك.

أما خليفة (٢٠١٧، ص ١٣٧) فيعرفه بأنه: جميع الأدوات والسياسات، ومفاهيم الأمن والضمانات الأمنية والمبادئ والتوجيهات ومداخل إدارة المخاطر والإجراءات والتدريب، وأفضل الممارسات والتقنيات التي يمكن استخدامها بهدف حماية الفضاء السيبراني.

ويتقارب قاري، وآخرون (٢٠١٩، ص٧) في التعريف بأنه: "ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف عادةً الوصول إلى المعلومات الحساسة، أو تغييرها، أو إتلافها، أو زيادة المال من المستخدمين أو مقاطعة العمليات التجارية.

وتوسع شكري (٢٠١٩) بأنه مجموعة من الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها من أجل منع الاستخدام غير المصرح به، وكذلك منع سوء الاستغلال، واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها؛ وذلك من أجل ضمان توافر واستمرارية عمل نظم المعلومات والعمل على تعزيز حماية وسرية وخصوصية البيانات الشخصية، واتخاذ جميع التدابير والإجراءات الفنية والعملية اللازمة لحماية المواطنين والمستهلكين من المخاطر القائمة والمحتملة في الفضاء السيبراني.

ولذا فالصانع وآخرون (٢٠٢٠ ، ٤٨) بينوا بأنه "حماية الأفراد وبياناتهم وحساباتهم من الهجمات الإلكترونية، ويقاس بالدرجة التي يحصل عليها المعلم من خلال إجابته على فقرات مقياس الأمن السيبراني.

وتعرفه المنتشري (٢٠٢٠، ٤٦٢) بأنه: "مفهوم أمني خاص بحماية المعلومات وكل ما له صلة بتلك المعلومات من عمليات وخدمات وأجهزة وتقنيات ضد أي شكل من أشكال الوصول غير المسموح به أو استخدام تلك المعلومات بشكل سلبي أو بما يمثل خطراً على المنظمات والأفراد ذوي العلاقة.

كما وضحه Richardson etc al (٢٠٢٠). أنه: "التدخلات التقنية والاحتياطات اللازمة لحماية أجهزة الحاسوب وشبكات الإنترنت والبيانات والمعلومات الشخصية من الوصول غير المصرح به للحفاظ على سلامة ونزاهة البيانات المخزنة في الأجهزة الرقمية.

وجميع ما سبق يدور في فلك إداري يطلق عليه إدارة الأمن السيبراني، ولأهميتها وعظم شأنها وأثرها في الواقع الفعلي فقد أنشئت وزارة التعليم الإدارة العامة للأمن السيبراني تحقيقًا لحوكمة وبناء استراتيجيات ومبادرات الأمن السيبراني في التعليم.

ويعرف الباحث إدارة الأمن السيبراني إجرائيًا بأنها: الإجراءات والاحترازات والتدابير التي تتخذها وزارة التعليم ممثلةً إداريًا في الإدارة العامة للأمن السيبراني، وبشريًا في مشرفي التقنية، وتقنيًا في الأدوات المستخدمة من قبل تقنين الوزارة، لحماية سلامة الشبكات والأجهزة من الهجوم أو الوصول غير المصرح به، وتحديث برامج الحماية باستمرار في ضوء تطبيق إجراءات ومعايير إدارية.

– أهمية إدارة الأمن السيبراني وأهدافه:

تذكر المنتشري (٢٠٢٠، ١٠٣) أهمية الأمن السيبراني في ضمان سرية الوثائق التعليمية وخصوصيتها والحفاظ على سلامتها بشكل مستمر، متابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن في المدرسة، بما يحقق حماية المعلمات والمدرسة من الهجمات السيبرانية في الفضاء السيبراني.

وأضافت السمحان (٢٠٢٠، ١٢) مجموعة نقاط تمثل أهمية الأمن السيبراني:

- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بمنع العبث بها.
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درعًا واقيا للبيانات والمعلومات.
- تحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.

وهذه الأهمية تؤكد على أن الأمن السيبراني منظومة تستدعي تكاتف الجهود والعمل وفق منظومة مجتمعية تحقق أهدافه التي يسعى إليها ومن تلك الأهداف ما ذكره جوهر (٢٠١٦) من تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بالطلاب وأعضاء هيئة التدريس. – حماية شبكة المعلومات والاتصالات من أي اختراق محتمل، وحماية شبكة المعلومات من أي هجوم محتمل؛ وذلك عن طريق معرفة التقنيات المرتبطة بأمن المعلومات ودراستها، وتشفير جميع

المعاملات الرقمية، بحيث يعجز أي مخترق عن مهاجمتها أو العبث بمحتوياتها، وتوفير بيئة العمل الأمنة.

كما يشير الربيعة (٢٠١٧) إلى الأهداف التالية:

- ضمان توافر استمرارية عمل نظم المعلومات.
- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به.
- حماية مصالح المملكة الحيوية وأمنها الوطني، والبني التحتية الحساسة فيها.
- جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة.
- تعزيز حماية الشبكات وأنظمة المعلومات.
- تعزيز حماية وسرية وخصوصية البيانات الشخصية.
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وما تقدمه من خدمات وما تحويه من بيانات.

كما يشير كلاً من صائغ (٢٠١٨، ١٠٣)، والسمحان (٢٠٢٠، ١٢) إلى مجموعة من أهداف الأمن السيبراني، تمثلت في:

١. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات.
٢. التصدي لهجمات أمن المعلومات التي تستهدف الأجهزة الحكومية والقطاع العام والخاص.
٣. توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
٤. صمود البنى التحتية الحساسة للهجمات الإلكترونية.
٥. توفير المتطلبات للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
٦. سد الثغرات في أنظمة أمن المعلومات.
٧. مقاومة البرمجيات الخبيثة، وما تستهدفه من أضرار بالغة بالمستخدمين وأنظمة المعلومات.

٨. الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

٩. تدريب الأفراد على إجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية.

ويتضح مما سبق أن الأهداف والممارسات هي الموجه لإدارة الأمن السيبراني تعليمًا، والتي اتضحت من خلال ما ورد في مكونات سياسة الأمن السيبراني بوزارة التعليم (١٤٤٢) المشتملة على: حوكمة الأمن السيبراني، وأمن الموارد البشرية، وإدارة الأصول المعلوماتية، وإدارة الهوية والوصول، وإدارة البنية التحتية والعمليات الأمنية، وأمن التطبيقات، والتشفير، وإدارة حوادث الأمن السيبراني وعمليات المراقبة، وإدارة استمرارية الأعمال، وأمن الأطراف الخارجية والحوسبة السحابية.

- عناصر الأمن السيبراني:

هناك ثلاثة عناصر أساسية يعتمد عليها الأمن السيبراني، وتتمثل في السرية، وصحة المعلومات وسلامتها التكامل وتوافر البيانات، وتفصيلها كالتالي:(John M & Thomas H. 2019)

١. السرية: الحفاظ على المعلومات من خلال منح الأذن للمخول لهم فقط بالوصول لتلك المعلومات، مع منع الأشخاص غير المخول لهم للمعلومات، مع ضرورة التأكد من عدم الإفصاح عنها أو تسريبها لأشخاص غير متخصصين أو مخول لهم ذلك.

٢. تكامل وسلامة المعلومات وتعني الحفاظ على المحتوي من التعديل، أو التغيير، أو الحذف، أو الإضافة إلا بواسطة الأشخاص المؤهلين والمتخصصين بالإشراف على هذا المحتوى.

٣. توافر المعلومات وإتاحتها من قبل المتخصصين على تقديمها واتاحتها في الوقت المناسب.

ويتبادر إلى الذهن هل الأمن السيبراني هو نفس أمن المعلومات؟ يوضح الجمل(٢٠٢٠، ص٢٥٤) بالتفصيل أن كلا من الأمن السيبراني وأمن المعلومات يعملان على حماية البيانات من الاختراقات والهجمات، إلا أنهما مختلفان ففي الوقت الذي يعمل أحدهما لحماية البيانات في مكان واحد ، يعمل الآخر على حماية البيانات بشكل عام، فالأمن المعلوماتي ينحصر نطاقه في

إطار ومنظور فكرة حماية النظام المعلوماتي، والشبكة المعلوماتية، والبيانات والحاسوب، وبرامجه والموقع الإلكتروني بمفهومها المجرد، من حيث مضمونها ومحتواها كقيمة مادية أو معنوية بالمعنى الضيق، وليست من وجهة أو منظور أمني سيادي ودفاعي يتعلق بمصالح وطنية عليا، والأمن السيبراني أوسع نطاقا وأشمل من الأمن المعلوماتي؛ لأنه يزيد على فكرتي الحماية والتأمين فكرة (الدفاع السيبراني) كأساس وإطار ومبرر لحماية المصالح الحيوية والوطنية ذات الصلة بسيادة الدولة على فضائها الإلكتروني، والتصدي للاعتداءات من خلال مجموعة النظم، والخطط والأدوات ، والإستراتيجيات، والأساليب الضرورية للحفاظ على الأمن الوطني، والنظام العام، وسياسات الدولة في المجال الاقتصادي والاجتماعي، والتقني.

- المتطلبات التنظيمية لإدارة الأمن السيبراني:

تتمثل المتطلبات التنظيمية لإدارة الأمن السيبراني في عددٍ من المتطلبات المتنوعة، وأهمها المتطلبات الإدارية، فقد أشار القحطاني والعنزي (٢٠١١) أن أبرز هذه المتطلبات لتحقيق الأمن السيبراني تمثلت في:

- وضوح تحديد إجراءات العمل في الشبكات المعلوماتية ومدى السماح عليها.
- توفير الآليات اللازمة لتنفيذ سياسات العمل من حيث الوضوح والدقة في التنفيذ لهذه السياسات.
- إسناد إدارة وتشغيل الشبكات المعلوماتية للعناصر البشرية الكفؤ والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة، وعدم إفساح أي مجال للهواة للعبث بمقدرات الهيئات الحكومية بالدولة.
- تحديث الأوضاع الأصلية لمعدات الشبكات كإجراء احترازي، مما يساعد على منع الاختراق
- المراقبة والمتابعة اللازمة والمستمرة للأنشطة المعلوماتية على الشبكة بالشكل الدقيق.
- التنفيذ وحسن اختيار مواقع نقاط الشبكة، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية من الاختراق.

ويضيف توفيق وشيرين (٢٠٢٢) عددًا من المتطلبات الاخرى لتحقيق الأمن السيبراني هي:

(أ) المتطلبات التقنية:

- وجود إدارة مركزية مختصة بأمن المعلومات والأمن السيبراني بين مختلف قطاعات المنظمة.
- التقييم الدوري لمخاطر الأمن السيبراني على أنظمة المعلومات بها.
- الاهتمام بعمل نسخ احتياطية للملفات بشكل دوري.
- فحص الملفات التي يتم تحميلها من المواقع غير المعروفة أو خدمات مشاركة الملفات الواردة عن طريق البريد الإلكتروني الرسمي.
- تجنب إرسال أي معلومات حساسة مثل كلمات المرور وأرقام بطاقات الائتمان عبر البريد الإلكتروني.
- تطبيق التحول الرقمي في كل المدخلات.
- وجود بوابة معلومات إلكترونية ومصادر تعلم ومحتوى رقمي ومنصات تعليمية إلكترونية.
- رفع درجة الحذر لدى الأعضاء عند فتح مرفق في البريد الإلكتروني على صفحاتهم الإلكترونية.
- تطوير البنى التحتية السيبرانية بالجامعة للحد من الاختراق والتجسس والقرصنة الإلكترونية.
- استخدام كلمة مرور معقدة قوية لا يمكن تخمينها، وتغيرها من وقت لآخر.

(ب) المتطلبات المادية:

- توفير برامج لتدريب الهيئة التدريسية على إجراءات لمواجهة التحديات الخاصة بالاختراق.
- توفير الدعم الفني والتقني اللازم لأعضاء هيئة التدريس لمعالجة المشكلات الطارئة.
- توفير بنية تحتية تكنولوجية وأجهزة اتصالات حديثة.
- امتلاك نظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الإلكترونية بين الاعضاء.
- توفير المخصصات المالية اللازمة لتحقيق الأمن السيبراني.

(ت) المتطلبات البشرية:

- عقد لقاءات دورية للمختصين في تطبيق الأمن السيبراني؛ لتعريفهم بالمستجدات في المجال.
- تبادل الخبرات مع الجامعات الأجنبية والعربية في مجال الأمن السيبراني.
- تنظيم حملات توعية لأعضاء هيئة التدريس للتعريف بالأمن السيبراني، ومخاطره، ومتطلباته.
- تعزيز مهارات أعضاء هيئة التدريس في مجال الأمن السيبراني من خلال عقد دورات تدريبية في استخدام الوسائل التقنية بطرق آمنة.
- تفعيل التواصل مع مؤسسات المجتمع المدني لنشر ثقافة الأمن السيبراني.
- إسناد إدارة وتشغيل الشبكات المعلوماتية للعناصر البشرية ذات الكفاءة والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة

(ث) المتطلبات المعرفية:

- توعية أعضاء هيئة التدريس وتثقيفهم بمتطلبات الأمن السيبراني لحماية البريد الإلكتروني.
- مراجعة البيانات والمعلومات المتوفرة على شبكاتها من أجل تحديثها
- تنمية وعي الطلاب بثقافة الأمن السيبراني في ضوء التحول الرقمي للجامعات. ولية.
- إعداد دراسات بحثية حول احتياجات الطلاب من المعلومات وثقافة الأمن السيبراني.
- تطوير الإطار التشريعي الملائم لأمن الفضاء السيبراني، وتشديد العقوبات على جرائم الفضاء السيبراني، وحماية الخصوصية الرقمية.
- الاهتمام بتعريف الطلاب بالاصطياد الإلكتروني وتحديد مصادره.
- تنمية الوعي بمفاهيم انتهاكات الأمن السيبراني ومخاطرها.
- وضع إجراءات وسياسات لحفظ الأمن السيبراني داخل الجامعات، وفقا للضوابط الرسمية.
- نشر ثقافة التعامل مع الأمن السيبراني، هدفها حماية البيانات والمعلومات من الهجمات.

كما تذكر السمحان (٢٠٢٠) نقلاً عن (https://www.arageek.com) عدد من الخطوات البسيطة للحفاظ على مستوى جيد من الأمان والسلامة السيبرانية.

- الموثوقية: وتعني استخدام المواقع الموثوق بها عند تقديم معلومات شخصية، والقاعدة الأساسية هي التحقق من عنوان URL، وإذا كان الموقع يتضمن https في بدايته، فهذا يعني أنه موقع آمن، أما إذا كان عنوان URL يحتوي على http بدون؛ فيجب الحذر من إدخال أي معلومات حساسة مثل بيانات بطاقة الإئتمان أو رقم التأمين الاجتماعي..... الخ.
- البريد الاحتيالي: ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة، إذ إن إحدى الطرق الأكثر شيوعا للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها مرسلة من شخص موثوق به.
- التحديثات up-to-date (Always) وتعني الحرص دائما على تحديث الأجهزة، فغالبا ما تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مشكلات الأمان، وإن هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.
- النسخ الاحتياطي: ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام لمنع هجمات الأمان على الإنترنت.

ويرى الباحث مما سبق تنوع المتطلبات وتعددها وفقًا لطبيعة العمل المؤسسي، ومع تعددها إلا أنها تدور في فلك إدارة المؤسسة التعليمية وكيفية حمايتها وجعلها مصدرًا منيعًا، وقد جمع الباحث أهم هذه المتطلبات وتمت صياغتها في متطلبات تنظيمية لمحورين هامين هما: المتطلبات الإدارية، والمتطلبات الفنية، لإدارة الأمن السيبراني، وتم بناء أداة الدراسة بعدد ٢٠ فقرة.

- أساليب الحماية من المخاطر السيبرانية:

طرح هنت Hunt (٢٠١٥،٨-١٠) مبادرات للحماية من المخاطر السيبرانية فيما يخص الوزارة:

- وضع خطة عمل معلنة تستهدف التعامل مع المخاطر السيبرانية والانتهاكات المختلفة، تشمل التنسيق بين الجامعات المختلفة.

- التعاون بين الوزارة وبعض الجهات التي تستطيع إبراز كيفية التصدي لمواجهة الجرائم السيبرانية.
- متابعة الجامعات للتأكد من التطبيق بالخطة للتعامل الآمن مع التكنولوجيا بما يشمل الأمن السيبراني.
- توفير دورات تدريبية لجميع العاملين بالوزارة على كيفية التوعية بالأمن السيبراني.
- نشر الاهتمام بمفاهيم الأمن السيبراني من خلال عقد الندوات وورش العمل، والتخطيط لأسبوع للأمن السيبراني.
- تحديات الأمن السيبراني ومعوقاته:

كمنظومة جديدة وحديثة فإن الكثير من التحديات تعتري الأمن السيبراني، ولابد من مواجهتها والعمل على حلها حتى يسير في الاتجاه الصحيح، فمن التحديات ماذكره Catota, Frankie B Morgant, M. Granger and Douglas C. Sicker (٢٠١٩):

- الطبيعة المتطورة للمخاطر والتهديدات الأمنية السيبرانية.
- ضمان تحديث جميع عناصر الأمن السيبراني باستمرار للحماية من نقاط الضعف المحتملة.
- تعدد المحاولات والتهديدات نتيجة لكثرة المخربين وسارقي البيانات.
- عدم التزام القيادة بوجود استراتيجية لتطوير الممارسات السيبرانية في الحرم الجامعي، وعدم مشاركتها في وضع خطط إدارة الأزمات السيبرانية.
- نقص في كفاءة الموارد البشرية في تعاملها مع التهديدات السيبرانية؛ وذلك نتيجة قلة البرامج التدريبية، وعدم مسايرتها للاتجاهات الحديثة في مجال الأمن السيبراني.

وهذه التحديات تسير في اتجاه توافقي مع المعوقات التي أوردها توفيق ومرسي (٢٠٢٢) والتي كانت: ضعف القوانين الرادعة، وانتهاك الخصوصية وأمن المعلومات والملكة الفكرية وشخصية المواقع، والإرهاب الإلكتروني السيبراني، واختراق البنى التحتية للاتصالات وتقنية المعلومات، وإخفاء الهويات الرقمية والبيانات الخاصة، والقصور في برامج التوعية الأمنية.

الدراسات السابقة:

قام الباحث بعرض الدراسات السابقة بدءًا بالأقدم فالأحدث، وفق الآتي:

دراسة رحمان وآخرون (Rehman et al .(٢٠١٥ بعنوان Information Security Management in Academic Institutes of Pakistan وهدفت الكشف عن واقع أنظمة إدارة الأمن السيبراني في معاهد التعليم العالي بجامعات باكستان، وقد تألف مجتمع الدراسة من موظفي التقنيات في الجامعات الباكستانية، وقام الباحث باستخدام المنهج الوصفي، وكانت الاستبانة أداة لجمع البيانات. وبينت النتائج أن واقع أنظمة إدارة الأمن السيبراني في معاهد التعليم العالي جاء بدرجة متوسطة. وأوصت الدراسة بضرورة وجود إدارة للمخاطر، كما أوصت بوضع سياسات أمنية هدفها مواجهة هذه المخاطر.

دراسة فينيسا بيرتون (Venessa Burton)٢٠١٨ بعنوان: Protecting small business information from cyber security criminals وهدفت إلى معرفة الصعوبات التي توجه المديرين المتخصصين بأمن المعلومات في حماية المعلومات، بالإضافة إلى مدى حماية الملكية الفكرية من الانتهاكات والاختراقات الأمنية التي يقوم بها القراصنة عبر شبكة الإنترنت، واستخدمت الباحثة المنهج النوعي، من خلال اجراء مقابلات مع مجموعة من (١٠) مديرين متخصصين في أنظمة أمن المعلومات في ولاية واشنطن بأمريكا، وتوصلت إلى عدة نتائج منها : ضعف القوانين المتبعة في حماية البيانات والمعلومات عبر شبكة الإنترنت وذلك بسبب حداثة الجرائم المعلوماتية، وبالتالي ضعف الفاعلية، والافتقار لآلية واضحة للتطبيق تتعلق بالأنظمة الأمنية، ذلك لتنوع وتشعب الجرائم المعلوماتية والاختراقات الأمنية وتطورها باستمرار.

دراسة الشيتي (٢٠١٩) وهدفت التعرف على السياسات والإجراءات الخاصة بأمن نظم المعلومات في المؤسسات التعليمية. وتم استخدام المنهج الوصفي التحليلي، كما تم استخدام الاستبانة، أما عينة الدراسة فتم اختيارها بطريقة عشوائية من الموظفين بإدارة تقنية المعلومات بجامعة القصيم، وتكونت العينة من ٧٠ موظف من أعضاء هيئة التدريس والإداريين. وتوصلت الدراسة إلى الافتقار لوجود إدارة متخصصة في أمن المعلومات بالجامعة، بالإضافة إلى ضعف اتباع سياسة الهوية الآلية لأمن المعلومات، وضعف سياسات حماية المعلومات وعدم مواكبتها للتغيرات

السائدة في مجال الاختراقات والتهديدات الأمنية. وأوصت بضرورة إنشاء إدارة متخصصة بحماية المعلومات مع توافر كوادر وطنية متخصصة ومؤهلة، مع ضرورة تحديثها بصفة مستمرة.

دراسة (٢٠١٩)، Catota,et al وهدفت إلى استكشاف التحديات التي يواجهها نظام التعليم العالي في الإكوادور في النهوض باستراتيجية الأمن السيبراني. استخدمت الدراسة المنهج الوصفي. وتوصلت إلى أن التحديات التي تواجهها استراتيجية الأمن السيبراني تشمل: قلة الموارد البشرية المتخصصة في مجال الأمن السيبراني، ضعف البنية التحتية، قصور في التدريب والتأهيل. وأوصت بتقديم مبادرات لتطوير ممارسات الأمن السيبراني في مؤسسات التعليم العالي تتلخص في مبادرة لتعزيز تدريب الموارد البشرية على كيفية تطبيق إجراءات الأمن السيبراني، ومبادرة دعم قدرات البحث والتطوير والوعي بالأمن السيبراني.

دراسة منى السمحان(٢٠٢٠) هدفت التعرف على متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، واستخدمت المنهج المسحي الوصفي، والاستبانة أداة لها، وطبقت على عينة قدرها(٤٧٨) من جميع العاملين بالجامعة، وتوصلت إلى موافق العينة على المتطلبات الإدارية، وأعلى عبارة" توجد سياسات أمنية لأنظمة المعلومات الإدارية بالجامعة"، كما كانت موافقتهم على المتطلبات الفنية، وأعلى عبارة "تحدث برامج الحماية لأجهزة الحاسب الآلي بالجامعة"، كما كانت موافقتهم على المتطلبات البشرية، وأعلى عبارة "توفير الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات الإدارية"، كما كانت موافقتهم على المتطلبات المادية، وأعلى عبارة " تحدث الجامعة برامج التطبيقات الحاسوبية لمنسوبيها باستمرار".

دراسة المنتشري(٢٠٢٠) وهدفت إلى معرفة دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، واتبعت المنهج الوصفي التحليلي، وتم إعداد استبانة تم تطبيقها على عينة مكونة من ٤٢٠ معلمة في عدد من المدارس الحكومية بمدينة جدة، وأظهرت النتائج أن دور القيادة المدرسية في تعزيز الأمن السيبراني لدى المعلمات ولدى طالبات المدرسة متحقق بدرجة موافقة قليلة ، وفي ضوء تلك النتائج تقدمت الدراسة بتصور مقترح وجاءت آليات تطبيقه عبر التنسيق مع الجهات المختصة المعنية بالأمن السيبراني في المملكة العربية السعودية.

دراسة الخضري وسلامي وكليبي (٢٠٢٠) وهدفت التعرف على طرق وقاية المجتمع السعودي من جرائم الفضاء السيبراني، والتعرف على المعوقات المجتمعية لتحقيق الوقاية من جرائم الفضاء السيبراني، والوصول إلى مقترح يسهم في تفعيل الأمن السيبراني، واستخدمت الدراسة المنهج الوصفي، وكانت الاستبانة أداةً للدراسة، وتألفت عينة الدراسة من طلاب الجامعات السعودية وأعضاء هيئة التدريس والإداريين. وكان مما توصلت إليه الدراسة: وجود اتفاق بين أفراد العينة حول تعدد أسباب حدوث المخاطر، والسبب في ذلك عدم وجود سياسات أمنية واضحة وبرامج حماية، وأوصت بزيادة الاهتمام بتوعية المؤسسات الجامعية حول تطبيق معايير أمن المعلومات، وتنظيم دورات تدريبية للطلاب وأعضاء هيئة التدريس والإداريين لتدريبهم على تطبيق أمن المعلومات، وتنظيم دورات تدريبية للقيادات التربوية هدفها تنمية الاعتماد على الذكاء الاصطناعي في صنع القرار التعليمي.

دراسة البيشي (٢٠٢١) وهدفت إلى توضيح واقع ممارسات الأمن السيبراني في الجامعات بالسعودية وأثر ذلك على تعزيز الثقافة الرقمية، وتم استخدام المنهج الوصفي التحليلي. وتوصلت إلى أن واقع ممارسات الأمن السيبراني في الجامعات السعودية جاء مرتفعًا، كما اتضح أن مستوى الثقة الرقمية جاء أيضاً مرتفعًا، كما أن هناك تأثير للأمن السيبراني في تعزيز وتفعيل الثقة الرقمية، واتضح عدم وجود فروق دالة إحصائياً للأمن السيبراني ترجع لعدد سنوات الخبرة إضافة للدرجات العلمية. وأوصت بضرورة زيادة الميزانية المخصصة للأمن السيبراني بالجامعات، وزيادة الاهتمام بإجراءات أمن المعلومات، والتطوير والتحسين المستمر لقدرات الموارد البشرية بالجامعة خاصة القيادات الأكاديمية تجاه التهديدات السيبرانية.

دراسة Pavel, et al, (٢٠٢١) وهدفت الدراسة الحالية إلى تحليل تحديات الأمن السيبراني لمؤسسات التعليم العالي في دولة مولدوفا (Moldova) لأن مؤسسات التعليم العالي (HEIS) كانت هدفًا للهجمات السيبرانية بسبب أصول المعلومات التي تمتلكها. كما أن الانتقال إلى الدراسة عبر الإنترنت كنتيجة للقيود المفروضة في عام ٢٠٢٠ أدى إلى زيادة تهديدات الأمن السيبراني للأوساط الأكاديمية بسبب نقاط الضعف في منصات التعلم عبر الإنترنت. استخدمت الدراسة المنهج الوصفي، أشارت نتائج الدراسة أن مؤسسات التعليم العالي في مولدوفا مستهدفة من قبل الهجمات الإلكترونية المحلية والدولية، وأن طبيعة التهديدات كانت تتمثل في البرامج

الضارة ضد الملفات الهامة في المجالات البحثية والإدارية. أوصت الدراسة بوضع استراتيجيات لتلك المؤسسات لحمايتها من أخطار التهديدات السيبرانية، إضافةً إلى نشر ثقافة الأمن السيبراني فيها.

دراسة سراج(٢٠٢٢) وهدفت إلى التحليل البعدي لدراسات الأمن السيبراني في المجالات التربوية، استخدمت الدراسة المنهج التحليلي البعدي، وتم اختيار ٢٥ دراسة ما بين(٢٠١٥-٢٠٢١)، وتوصلت الدراسة إلى أن الاتجاهات البحثية في الأمن السيبراني يجب أن تركز على منهجية الأمن السيبراني في مؤسسات التعليم العام والجامعي ، وممارسات الأمن السيبراني، والاتجاهات الحديثة في مجال الأمن السيبراني ، والدراسات المقارنة للمؤسسات الجامعية وممارساتها للأمن السيبراني ، ومشكلات الأمن السيبراني ومقترحات حلها ، وتطوير ممارسات الأمن السيبراني في مؤسسات التعليم ، آليات تفعيل ثقافة الأمن السيبراني في المؤسسات التعليمية ، والمنصات التعليمية والأمن السيبراني ، الأدوار القيادية في مواجهة التهديدات السيبرانية . كما أوصت الدراسة بمزيد من الاهتمام بمجال الأمن السيبراني في المؤسسات التربوية؛ حيث إنه مجال مازال يعاني من الإهمال.

دراسة توفيق ومرسي(٢٠٢٢) وهدفت التعرف على متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس ، وتحديد أهم متطلبات تحقيق الأمن السيبراني بالجامعات المصرية ، وأهم المعوقات التي تحول دول تحقيق هذه المتطلبات، واستخدمت المنهج الوصفي، من خلال استبانة وزعت على عينة(٢٤٨) عضو هيئة تدريس ، وتوصلت إلى اتفاق العينة على متطلبات تحقيق الأمن السيبراني في ظل التحول الرقمي ، والتي تمثلت في مجموعة من المتطلبات التقنية والمادية والبشرية والمعرفية، ومعوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها .

دراسة المنيع (٢٠٢٢) وهدفت التعرف على واقع تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠، واستخدمت المنهج الوصفي التحليلي، وتكون المجتمع من جميع الموظفين التقنيين في (جامعة أم القرى، جامعة الإمام عبد الرحمن بن فيصل، جامعة الإمام محمد بن سعود الإسلامية)، وبلغ عددهم (٤٦٨) موظفا، وقد بلغ عدد العينة (٢١٠) موظفين، كما استخدمت الاستبانة. وتوصلت إلى أن أفراد العينة موافقون بدرجة متوسطة على واقع تحقيق

الأمن السيبراني في الجامعات السعودية، وأن أفراد العينة موافقون بدرجة كبيرة جدًا على معوقات تحقيق الأمن السيبراني في الجامعات السعودية.

دراسة فرج (٢٠٢٢) وهدفت إلى بيان دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبدالعزيز ، استخدمت الدراسة المنهج الوصفي ، وصممت استبانة ، وطُبقت على عينة من أعضاء هيئة التدريس بالجامعة بلغت (١٢٥) عضواً ، وخلصت الدراسة إلى أن دواعي تعزيز ثقافة الأمن السيبراني في ظل التحويل الرقمي حصل على متوسط (٣,٥٥) بدرجة متوسطة ، وبالنسبة للمحاور فكانت أعلى المتوسطات لمحور الدواعي المجتمعية لتعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي ، يليه محور الدواعي المعرفية لتعزيز ثقافة الأمن السيبراني ، وأخيراً محور الدواعي التقنية، كما بينت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير الكلية ، والرتبة العلمية ، فيما وجدت فروق تعزى لمتغير سنوات الخبرة .

التعليق على الدراسات السابقة:

- اتفقت معظم الدراسات السابقة مع الدراسة الحالية في المنهج المستخدم ألا وهو المنهج الوصفي المسحي عدا دراسة (٢٠٢١)، Pavel, et al، ودراسة سراج (٢٠٢٢) فقد كانتا تحليلية.
- اختلفت الدراسة الحالية عن الدراسات السابقة في مجالها فقد كانت معنية بالمتطلبات التنظيمية –الإدارية والفنية– للأمن السيبراني بوزارة التعليم في المملكة العربية السعودية، بينما باقي الدراسات كانت في مؤسسات جامعية أو تعليم عام عدا دراسة (٢٠٢١)، Pavel, et al التي كانت في مؤسسات التعليم العالي في مولدوفا.
- استفادت الدراسة الحالية من الدراسات السابقة في إطارها النظري وبناء أداة الدراسة، وتحليل النتائج.

منهجية الدراسة وإجراءاتها

منهج الدراسة:

اتبعت الدراسة الحالية المنهج الوصفي المسحي لملائمته لطبيعة الدراسة الحالية وأهدافها، بهدف التعرف على المتطلبات التنظيمية لإدارة الأمن السيبراني بوزارة التعليم وذلك من خلال تصميم استبانة لاستطلاع أراء مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية حول المتطلبات الإدارية والفنية لإدارة الأمن السيبراني.

مجتمع الدراسة:

تكون مجتمع الدراسة الحالية من جميع مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية، والبالغ عددهم (١١٧) حسب الإحصائية التي حصل عليها الباحث من الإدارة العامة للتحول الرقمي- إدارة تقنية المعلومات- بوزارة التعليم لعام ١٤٤٤هـ، والجدول رقم (١) يوضح توزيع مجتمع الدراسة وفقا لطبيعة العمل الحالي.

جدول (١) يوضح توزيع مجتمع الدراسة وفقا لطبيعة العمل الحالي

العمل الحالي	العدد
مشرف عموم	١٦
مشرف إدارة تعليم	١٠١
الإجمالي	١١٧

عينة الدراسة:

أولا-العينة الاستطلاعية:

تكونت عينة الدراسة الاستطلاعية من (٣٠) من مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة، حيث تم تطبيق الاستبانة عليهم للتحقق من صدقها وثباتها، ومدى إمكانية تطبيقها والاعتماد على نتائجها في الدراسة الحالية.

ثانيا–العينة الأساسية:

تم اختيار عينة الدراسة النهائية باستخدام جداول مورجان، ومن خلالها تم احتساب حجم العينة الإجمالي (٨٨) مشرفا ومشرفة، منهم (١٢) لوظيفة مشرف عموم، و(٧٦) لوظيفة مشرف إدارة تعليم، حيث تم توزيع استبانة الدراسة على عدد (١٠٠) مشرفا ومشرفة، وبلغ عدد الاستجابات التي حصل عليها الباحث (٩١) فردًا، وتم استبعاد استجابات (٣) من أفراد العينة لعدم اكتمال الاستجابة.

وبذلك تكونت العينة في صورتها النهائية من (٨٨) من مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية، والجدول رقم (٢) يوضح خصائص العينة من حيث العمل الحالي، وسنوات الخبرة في العمل الحالي، وعدد الدورات في الأمن السيبراني:

جدول (٢) يوضح توزيع عينة الدراسة وفقا للعمل الحالي، وسنوات الخبرة في العمل الحالي، وعدد الدورات في الأمن السيبراني

المتغير		العدد	النسبة المئوية
العمل الحالي	مشرف عموم	١٦	٪١٨,٢
	مشرف إدارة تعليم	٧٢	٪٨١,٨
سنوات الخبرة في العمل الحالي	١٠ سنوات وأقل	٢٤	٪٢٧,٣
	أكثر من ١٠ سنوات	٦٤	٪٧٢,٧
عدد الدورات في الأمن السيبراني	لا يوجد	١٢	٪١٣,٦
	١– ٣ دورات	٣٦	٪٤٠,٩
	أكثر من ٣ دورات	٤٠	٪٤٥,٥
الإجمالي		٨٨	٪١٠٠

يتبين من الجدول السابق أن عدد (١٦) من أفراد عينة الدراسة بوظيفة (مشرف عموم)، بنسبة (١٨,٢٪) من إجمالي العينة، وأن عدد (٧٢) من أفراد عينة الدراسة بوظيفة (مشرف إدارة تعليم)، بنسبة (٨١,٨٪) من إجمالي العينة، وهذا مؤشر على تجانس العينة بين الوزارة والميدان بمعدل ١:٤، كما يتبين أن عدد (٢٤) من أفراد عينة الدراسة من ذوي الخبرة (١٠ سنوات وأقل)، بنسبة (٢٧,٣٪) من إجمالي العينة، وأن عدد (٦٤) من أفراد عينة الدراسة من ذوي الخبرة

(أكثر من ١٠ سنوات)، بنسبة (٧٢,٨٪) من إجمالي العينة، وهذا يعطي مؤشرًا لدقة الإجابة نظرًا للخبرة الطويلة في الميدان التربوي، أما بالنسبة لعدد الدورات التدريبية في مجال الأمن السيبراني فلم يحصل (١٢) من أفراد العينة على أي دورات بنسبة (١٣,٦٪) من إجمالي العينة، بينما حصل (٣٦) من أفراد العينة على (١- ٣ دورات) بنسبة (٤٠,٩٪) من إجمالي العينة، في حين حصل (٤٠) من أفراد العينة على (أكثر من ٣ دورات) بنسبة (٤٥,٥٪) من إجمالي العينة.

أداة الدراسة:

أعد الباحث الاستبانة المستخدمة في الدراسة الحالية والتي تكونت من بعض البيانات الديموجرافية لأفراد العينة، والتي تمثلت في (العمل الحالي، وسنوات الخبرة في العمل الحالي، وعدد الدورات في الأمن السيبراني)، إضافةً إلى (٢٠) فقرة موزعة على محورين كما يلي:

المحور الأول: المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم، ويتكون من (١٠) فقرات تعبر عن وجهة نظر مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة.

المحور الثاني: المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم، ويتكون من (١٠) فقرات تعبر عن وجهة نظر مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة.

وكانت جميع فقرات الاستبانة بعد التعديلات التي تمت إيجابية، ولا توجد أي فقرات عكسية.

تصحيح الاستبانة:

يتم الإجابة عن بنود الاستبانة وفقاً لمقياس متدرج من درجة الموافقة التامة إلى عدم الموافقة وفقا للاختيارات التالية (موافق بشدة- موافق- محايد- غير موافق- غير موافق إطلاقا)، وتم تقدير استجابة المفحوص كما يلي (موافق بشدة= ٥ درجات، موافق= ٤ درجات، محايد= ٣ درجات، غير موافق= درجتان، غير موافق إطلاقا= درجة واحدة)، وتشير الدرجة المرتفعة إلى درجة موافقة كبيرة من المشرفين والمشرفات على فقرات الاستبانة، بينما تشير الدرجة المنخفضة إلى عدم الموافقة.

وللحكم على مدى اتفاق عينة الدراسة على متوسطات درجات فقرات الاستبانة ومتوسط كل محور من محاورها تم تقسيم حساب مدى الدرجات (٥-١=٤)، وتقسيمها على خمس فئات

تمثل المستويات التالية (عالي جدا– عالي– متوسط– قليل– قليل جدا)، وبذلك يكون طول كل فئة منها كما يلي:

طول كل فئة = ٠,٨ ثم تم تفسير المتوسطات كما في الدول رقم (٣):

جدول (٣) يوضح فئات المتوسطات وتفسيرها

مدى الدرجات	مستوى التحقق
٤,٢٠– ٥,٠٠	عالي جدا
٣,٤٠– ٤,١٩	عالي
٢,٦٠ – ٣,٣٩	متوسط
١,٨٠– ٢,٥٩	منخفض
١,٠٠– ١,٧٩	منخفض جدا

صدق وثبات استبانة الدراسة الحالية:

أولا – الصدق:

العرض على المحكِّمين:

عرض الباحث الاستبانة في صورتها الأولية والمكوَّنة من (٣٦) فقرة، على عدد من المحكِّمين الأكاديميين ذوي الخبرة والاختصاص من أعضاء هيئة التدريس في الجامعات وقد طُلب منهم إبداء آرائهم في الاستبانة من حيث: مدى وضوح الفقرات، وملاءمة بدائلها، وانتمائها إلى الأبعاد التي تنتمي إليها، للتطبيق على عينة الدراسة الحالية، أو أي ملاحظات أخرى يرون إضافتها. وقد استفاد الباحث من ملاحظات المحكِّمين، واقتراحاتهم، وتم التعديل على صياغة بعض الفقرات لتتناسب مع طبيعة العينة، مع الإبقاء على العبارات التي حازت نسبة قبول (٨٠٪) من آراء المحكِّمين، وبذلك بلغ عدد فقرات الاستبانة في صورتها النهائية بعد تحكيمها (٢٠) فقرة، حيث اتفق المحكمون على الإبقاء على تلك الفقرات بعد تعديل صياغة بعضها.

الاتساق الداخلي:

للتحقق من صدق الاتساق الداخلي للاستبانة قام الباحث بتطبيقها على عينة استطلاعية مكونة من (٣٠) من مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة، ومن

ثم حساب معاملات الارتباط بطريقة بيرسون بين درجة كل فقرة من فقرات الاستبانة، ومجموع درجات المحور الذي تنتمي إليه، والجدول رقم (٤) يتضمن عرضًا للنتائج التي أسفرت عنها المعالجة الإحصائية للاتساق الداخلي:

جدول (٤) يوضح حساب الاتساق الداخلي لفقرات استبانة الدراسة الحالية (ن= ٣٠)

م	الفقرة	معامل الارتباط بدرجة المحور
المحور الأول– المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم		
١	دعم البنية التكنولوجية داخل جهاز الوزارة وإدارات التعليم	٠,٧٦٩**
٢	تطبيق التحول الرقمي في كل مجالات الوزارة	٠,٤٧٤**
٣	تمهير المشرفين من العمليات الإلكترونية (قدرة هجومية /قدرة دفاعية/قدرة استطلاعية)	٠,٨٤٤**
٤	بناء بوابة معلومات ذات استقلالية تقنية بها جميع المحتوى الرقمي والمنصات	٠,٨١٢**
٥	توفير الدعم الإداري والفني اللازم للبنية التكنولوجية	٠,٦٧٠**
٦	التدريب والتوعية من خلال تنظيم لقاءات ومحاضرات وورش عمل في تطبيق الأمن السيبراني	٠,٤٨٣**
٧	تخصيص جهة إدارية تقنية تتولى الخبرات مع الوزارات محليًا وعالميًا في مجال الأمن السيبراني	٠,٦٣٩**
٨	إحلال الشركات المحلية بديلاً عن الأجنبية في مجال العقود المبرمة	٠,٤٢٩*
٩	توفير دليل معتمد لسياسات وإجراءات الأمن السيبراني	٠,٤٨٧**
١٠	وضع خطة للطوارئ للتعامل مع حوادث الأمن السيبراني المحتملة	٠,٦٣٩**
المحور الثاني– المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم		
١١	توفير برامج وقائية باستمرار حمايةً للأجهزة	٠,٨٧٠**
١٢	التقييم الدوري المستمر لمخاطر الأمن السيبراني	٠,٨٢٥**
١٣	وجود ملفات احتياطية تحدث باستمرار	٠,٨٠٩**
١٤	تغيير كلمات المرور بكلمات قوية غير قابلة للحدس والتخمين	٠,٤٩١**
١٥	وضع ممكنات تقنية تحول دون اختراق الأجهزة	٠,٧٧٥**
١٦	تلافي مشاكل ضغط النظام لكثرة المستخدمين في وقت واحد	٠,٨٧١**
١٧	تصميم نظام يمنع الدخول غير الآمن بالإنترنت	٠,٧٨٧**
١٨	معالجة مشكلة الوصول من قبل أطراف إضافية (برامج تطلب الإيميل والرقم السري الخاص)	٠,٧٧٨**

م	الفقرة	معامل الارتباط بدرجة المحور
١٩	التحديث المستمر للأنظمة الحاسوبية وشبكات المؤسسات التعليمية للحصول على أحدث ميزات الأمان	٠,٨٢٩**
٢٠	تحديد الأذونات والصلاحيات لمستخدمي الأنظمة الحاسوبية بشكل دقيق	٠,٦١٩**

** دال عند مستوى (٠,٠١)* دال عند مستوى (٠,٠٥).

يتبين من الجدول السابق أن قيم معاملات الارتباط جميعها دالة إحصائيا عند مستوى دلالة (٠,٠٥) فأقل. بما يشير إلى الاتساق الداخلي لجميع فقرات الاستبانة.

ثانيا– ثبات استبانة الدراسة الحالية:

قام الباحث بالتحقق من ثبات استبانة الدراسة الحالية بحساب معامل ثبات ألفا كرونباخ لكل بعد من محوري الاستبانة، كما قام الباحث بحساب معامل ثبات التجزئة النصفية المصحح بمعادلة سبيرمان براون، وجاءت النتائج كما في الجدول رقم (٥):

جدول (٥) يبين ثبات استبانة الدراسة الحالية باستخدام معامل ألفا كرونباخ والتجزئة النصفية (ن=٣٠)

محوري الاستبانة	عدد الفقرات	طريقة حساب الثبات	
		ألفا كرونباخ	التجزئة النصفية
المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم	١٠	٠,٧٩١	٠,٧٩٧
المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم	١٠	٠,٨٩٦	٠,٩٠٩

أظهرت نتائج الجدول السابق أن قيم معامل الثبات لمحوري الاستبانة قد بلغت (٠,٧٩١)، و (٠,٧٩٧)، كما بلغت قيم معامل الثبات لمحوري الاستبانة باستخدام معامل ثبات التجزئة النصفية المصحح بمعادلة سبيرمان براون (٠,٨٩٦)، و(٠,٩٠٩)، وجميعها قيم مرتفعة تدل على ثبات استبانة الدراسة الحالية.

الأساليب الإحصائية المستخدمة:

بعدما تم جمع البيانات، تم معالجتها باستخدام البرنامج الإحصائي (SPSS) الإصدار الثامن والعشرين، وتم القيام بمجموعة من الأساليب الإحصائية للتحقق من صدق وثبات الاستبانة، والإجابة عن أسئلة الدراسة، هي:

١- التكرارات والنسب المئوية لوصف خصائص العينة وفق المتغيرات الديموغرافية، للإجابة عن الأسئلة الأول والثاني والثالث من أسئلة الدراسة.

٢- معامل الارتباط بطريقة بيرسون للتحقق من الاتساق الداخلي للاستبانة.

٣- معامل ثبات ألفا كرونباخ للتحقق من ثبات الاستبانة.

٤- الثبات بطريقة التجزئة النصفية المصحح بمعادلة (سبيرمان – براون)، للتحقق من ثبات الاستبانة.

٥- المتوسطات، والمتوسطات الموزونة، والانحرافات المعيارية للإجابة عن الأسئلة الأول والثاني من أسئلة الدراسة.

٦- اختبار كولمجروف-سميرنوف (Kolmogorov-Smirnov) للكشف عن اعتدالية توزيع البيانات.

٧- اختبار مان -وتني (Mann-Whitney Test) للفروق بين مجموعتين مستقلتين؛ للإجابة عن السؤال الثالث من أسئلة الدراسة فيما يتعلق بمتغيري العمل الحالي وعدد سنوات الخبرة في العمل الحالي، وكاختبار تتبعي للإجابة عن السؤال الثالث من أسئلة الدراسة فيما يتعلق بمتغير عدد الدورات في الأمن السيبراني.

٨- اختبار كروسكال واليس للفروق المجموعات المستقلة (Independent-Samples Kruskal-Wallis Test) للإجابة عن السؤال الثالث من أسئلة الدراسة فيما يتعلق بمتغير عدد الدورات في الأمن السيبراني.

نتائج الدراسة الميدانية:

نتائج السؤال الأول:

ينص السؤال الأول من أسئلة الدراسة على: "ما المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم؟"

وللإجابة عن هذا السؤال قام الباحث بحساب التكرارات والنسب المئوية والمتوسطات والانحرافات المعيارية لفقرات المحور الأول من محوري الاستبانة، كما في الجدول التالي:

جدول (٦) التكرارات والنسب المئوية والمتوسطات والانحرافات المعيارية لفقرات الاستبانة المتعلقة بالمتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم

م	الفقرة	التكرار والنسبة المئوية	موافق بشدة	موافق	محايد	غير موافق	غير موافق إطلاقا	المتوسط	الانحراف معياري	مستوى الموافقة	الترتيب
٩	توفير دليل معتمد لسياسات وإجراءات الأمن السيبراني	ك	١٣	٩	٧	١	٠	٤,١٣	٠,٩٠٠	عالي	١
		%	٤٣,٣	٣٠,٠	٢٣,٣	٣,٣	٠				
١	دعم البنية التكنولوجية داخل جهاز الوزارة وإدارات التعليم	ك	١٢	٨	٧	١	٢	٣,٩٠	١,١٨٥	عالي	٢
		%	٤٠,٠	٢٦,٧	٢٣,٣	٣,٣	٦,٧				
٨	إحلال الشركات المحلية بديلاً عن الأجنبية في مجال العقود المبرمة	ك	١٣,٣	٢٦,٧	٣٣,٣	٢٣,٣	٣,٣	٣,٧٣	١,٠٤٨	عالي	٣
		%	٩	٨	٩	٤	٠				
٤	بناء بوابة معلومات ذات استقلالية تقنية بها جميع المحتوى الرقمي والمنصات	ك	١٣	٦	٥	١	٥	٣,٧٠	١,٤٨٩	عالي	٤
		%	٤٣,٣	٢٠,٠	١٦,٧	٣,٣	١٦,٧				
١٠	وضع خطة للطوارئ للتعامل مع حوادث الأمن السيبراني المحتملة	ك	٧	٨	١٢	٣	٠	٣,٦٣	٠,٩٦٤	عالي	٥
		%	٢٣,٣	٢٦,٧	٤٠,٠	١٠,٠	٠				
٢	تطبيق التحول الرقمي في كل	ك	٥	١٠	١٢	١	٢	٣,٥٠	١,٠٤٢	عالي	٦

م	الفقرة	التكرار والنسبة المئوية	موافق بشدة	موافق	محايد	غير موافق	غير موافق إطلاقا	المتوسط	الانحراف معياري	مستوى الموافقة	الترتيب
	مجالات الوزارة	%	١٦,٧	٣٣,٣	٤٠,٠	٣,٣	٦,٧				
٣	تمهير المشرفين من العمليات الإلكترونية (قدرة هجومية /قدرة دفاعية/قدرة استطلاعية)	ك	٨	٥	٧	٦	٤	٣,٢٣	١,٤٠٦	متوسط	٧
		%	٢٦,٧	١٦,٧	٢٣,٣	٢٠,٠	١٣,٣				
٧	تخصيص جهة إدارية تقنية تتولى الخبرات مع الوزارات محليًا وعالميًا في مجال الأمن السيبراني	ك	١٣,٣	١٦,٧	٢٠,٠	٣٦,٧	١٣,٣	٣,٢٣	١,٠٧٣	متوسط	٨
		%	٤	٨	١٠	٧	١				
٥	توفير الدعم الإداري والفني اللازم للبنية التكنولوجية	ك	٥	٢	١٤	٩	٠	٣,١٠	١,٠٢٩	متوسط	٩
		%	١٦,٧	٦,٧	٤٦,٧	٣٠,٠	٠				
٦	التدريب والتوعية من خلال تنظيم لقاءات ومحاضرات وورش عمل في تطبيق الأمن السيبراني	ك	٤	٥	٦	١١	٤	٢,٨٠	١,٢٧٠	متوسط	١٠
		%	١٣,٣	٢٦,٧	٣٣,٣	٢٣,٣	٣,٣				
	المتوسط الموزون والانحراف المعياري لدرجة المحور ككل							٣,٥٠	٠,٦٨	عالي	

يتبين من الجدول السابق ما يلي:

- وجود مستوى عالي من الاتفاق بين عينة الدراسة من مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة على محور المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم، حيث بلغ المتوسط العام الموزون للمحور (٣,٥٠)، بانحراف معياري قدره (٠,٦٨)، وهو ما ينتمي إلى فئة الموافقة العالية. وتتفق هذه النتيجة مع دراسة الخضري وسلامي وكليبي (٢٠٢٠) حول تعدد أسباب حدوث المخاطر السيبرانية والتي كان جُلها متطلبات إدارية، كما اتفقت مع دراسة توفيق ومرسي (٢٠٢٢) حول اتفاق العينة على متطلبات تحقيق الأمن السيبراني في ظل التحول الرقمي، واتفقت مع دراسة البيشي (٢٠٢١) التي بينت واقع ممارسات الأمن السيبراني في الجامعات السعودية كان مرتفعًا، واختلفت مع دراسة المنيع (٢٠٢٢) التي توصلت إلى أن

مفردات العينة موافقون بدرجة متوسطة على واقع تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠.

– حازت الفقرات أرقام (٣، ٥، ٦، ٧) على مستوى متوسط من الاتفاق بين عينة الدراسة، بينما جاءت درجة الموافقة عالية على بقية فقرات محور المتطلبات الإدارية لإدارة الأمن السيبراني.

– أكبر متوسط (أكبر درجة اتفاق) لفقرات محور المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم هي الفقرة رقم (٩) التي تنص على "توفير دليل معتمد لسياسات وإجراءات الأمن السيبراني" بمتوسط (٤,١٣) وانحراف معياري (٠,٩٠). واتفقت هذه النتيجة مع دراسة Pavel, et al (٢٠٢١)، التي أوصت بوضع استراتيجيات للمؤسسات لحمايتها من أخطار التهديدات السيبرانية. تليها الفقرة رقم (١) التي تنص على "دعم البنية التكنولوجية داخل جهاز الوزارة وإدارات التعليم" بمتوسط (٣,٩٠) وانحراف معياري (١,١٨٥)، واختلفت مع دراسة فرج (٢٠٢٢) التي بينت أن محور الدواعي التقنية حصل على أقل متوسط. ثم الفقرة رقم (٨) التي تنص على "إحلال الشركات المحلية بديلاً عن الأجنبية في مجال العقود المبرمة" بمتوسط (٣,٧٣) وانحراف معياري (١,٠٤٨).

– بينما كان أدنى متوسط للفقرة رقم (٦) التي تنص على "التدريب والتوعية من خلال تنظيم لقاءات ومحاضرات وورش عمل في تطبيق الأمن السيبراني" بمتوسط (٢,٨٠) وانحراف معياري (١,٢٧٠)، واختلفت هذه النتيجة مع دراسة (٢٠١٩)، Catota,et al التي توصلت إلى أن من التحديات التي تواجهها استراتيجية الأمن السيبراني قصور في التدريب والتأهيل. تليها الفقرة رقم (٥) التي تنص على "توفير الدعم الإداري والفني اللازم للبنية التكنولوجية" بمتوسط (٣,١٠) وانحراف معياري (١,٠٢٩)، واختلفت هذه النتيجة مع دراسة (٢٠١٩)،Catota,et al التي توصلت إلى أن قلة الموارد البشرية المتخصصة في مجال الأمن السيبراني من التحديات التي تواجهها استراتيجية الأمن السيبراني.ثم الفقرة رقم (٧) التي تنص على "تخصيص جهة إدارية تقنية تتولى الخبرات مع الوزارات محليًا وعالميًا في مجال الأمن السيبراني" بمتوسط (٣,٢٣) وانحراف معياري (١,٠٧٣)، واختلفت هذه مع دراسة الشيتي (٢٠١٩) والتي توصلت إلى الافتقار لوجود إدارة متخصصة في أمن المعلومات بجامعة القصيم.

- بشكل عام، أظهرت نتائج البحث أن هناك مستوى عالي من الاتفاق بين عينة الدراسة من مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم على محور المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم. ويمكن تفسير هذه النتائج من خلال عدة عوامل، منها: إدراك مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية بأهمية الأمن السيبراني وضرورة تطويره، ووجود وعي كافٍ لدى مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية بمخاطر الأمن السيبراني وطرق مواجهتها، ووجود اهتمام من قبل وزارة التعليم بتطوير الأمن السيبراني.

- كما أنه لا يزال هناك تحديات تواجه الأمن السيبراني بوزارة التعليم، منها: الحاجة إلى تطوير البنية التحتية التكنولوجية، والحاجة إلى تدريب وتأهيل الكوادر البشرية، والحاجة إلى تحديث السياسات والإجراءات الأمنية.

نتائج السؤال الثاني:

ينص السؤال الثاني من أسئلة الدراسة على: "ما المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم من وجهة نظر مشرفي تقنية المعلومات والأمن السيبراني؟"

وللإجابة عن هذا السؤال قام الباحث بحساب التكرارات والنسب المئوية والمتوسطات والانحرافات المعيارية لفقرات المحور الثاني من محوري الاستبانة، كما في الجدول التالي:

جدول (٧) التكرارات والنسب المئوية والمتوسطات والانحرافات المعيارية لفقرات الاستبانة المتعلقة بالمتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم من وجهة نظر مشرفي تقنية المعلومات والأمن السيبراني.

م	الفقرة	التكرار والنسبة المئوية	موافق بشدة	موافق	محايد	غير موافق	غير موافق إطلاقا	المتوسط	الانحراف معياري	مستوى الموافقة	الترتيب
١	توفير برامج وقائية باستمرار حمايةً للأجهزة.	ك	٢٠	٦	٢	١	١	٤,٤٣	١,٠٠٦	عالي جدا	١
		%	٦٦,٧	٢٠,٠	٦,٧	٣,٣	٣,٣				
٣	وجود ملفات احتياطية تحدث	ك	١٥	١١	٢	٢	٠	٤,٣٠	٠,٨٧٧	عالي جدا	٢

م	الفقرة	التكرار والنسبة المئوية	موافق بشدة	موافق	محايد	غير موافق	غير موافق إطلاقا	المتوسط	الانحراف معياري	مستوى الموافقة	الترتيب
	باستمرار.	%	٥٠,٠	٣٦,٧	٦,٧	٦,٧	٠				
٤	تغيير كلمات المرور بكلمات قوية غير قابلة للحدس والتخمين.	ك	١٧	٩	٢	٠	٢	٤,٣٠	١,٠٨٨	عالي جدا	٣
		%	٥٦,٧	٣٠,٠	٦,٧	٠	٦,٧				
٨	معالجة مشكلة الوصول من قبل أطراف إضافية (برامج تطلب الإيميل والرقم السري الخاص).	ك	١٦	٩	٣	١	١	٤,٢٧	١,٠١٥	عالي جدا	٤
		%	٥٣,٣	٣٠,٠	١٠,٠	٣,٣	٣,٣				
٢	التقييم الدوري المستمر لمخاطر الأمن السيبراني.	ك	١٣	١٢	٢	٣	٠	٤,١٧	٠,٩٥٠	عالي	٥
		%	٤٣,٣	٤٠,٠	٦,٧	١٠,٠	٠				
٦	تلافي مشاكل ضغط النظام لكثرة المستخدمين في وقت واحد.	ك	١٧	٣	٧	٣	٠	٤,١٣	١,١٠٦	عالي	٦
		%	٥٦,٧	١٠,٠	٢٣,٣	١٠,٠	٠				
٥	وضع ممكنات تقنية تحول دون اختراق الأجهزة.	ك	١٠	١٤	٥	١	٠	٤,١٠	٠,٨٠٣	عالي	٧
		%	٣٣,٣	٤٦,٧	١٦,٧	٣,٣	٠				
٩	التحديث المستمر للأنظمة الحاسوبية وشبكات المؤسسات التعليمية للحصول على أحدث ميزات الأمان.	ك	١٥	٨	٢	٥	٠	٤,١٠	١,١٢٥	عالي	٨
		%	٥٠,٠	٢٦,٧	٦,٧	١٦,٧	٠				
١٠	تحديد الأذونات والصلاحيات لمستخدمي الأنظمة الحاسوبية بشكل دقيق.	ك	١٢	٧	٩	٢	٠	٣,٩٧	٠,٩٩٩	عالي	٩
		%	٤٠,٠	٢٣,٣	٣٠,٠	٦,٧	٠				
٧	تصميم نظام يمنع الدخول غير الآمن بالإنترنت.	ك	١٠	٨	٩	٣	٠	٣,٨٣	١,٠٢٠	عالي	١٠
		%	٣٣,٣	٢٦,٧	٣٠,٠	١٠,٠	٠				
المتوسط الموزون والانحراف المعياري لدرجة المحور ككل								٤,١٦	٠,٧٢	عالي	

يتبين من الجدول السابق ما يلي:

- وجود مستوى عالي من الاتفاق بين عينة الدراسة من مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة العربية السعودية على محور المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم، حيث بلغ المتوسط العام الموزون للمحور (٤,١٦)، بانحراف معياري قدره (٠,٧٢)، وهو ما يدل على درجة موافقة عالية على تلك المتطلبات، واتفقت هذه النتيجة مع دراسة توفيق ومرسي(٢٠٢٢) التي توصلت إلى اتفاق العينة على المتطلبات التقنية لتحقيق الأمن السيبراني بجامعة بنها في ظل التحول الرقمي، كما يؤكد ما توصلت إليه دراسة سراج (٢٠٢٢) من أن الاتجاهات البحثية في الأمن السيبراني يجب أن تركز على ممارسات الأمن السيبراني في المؤسسات التعليمية، ومشكلات الأمن السيبراني ومقترحات حلها،كما اختلفت عن أنظمة الأمن السيبراني في معاهد التعليم العالي التي جاءت بدرجة متوسطة في دراسة رحمان وآخرون (٢٠١٥). Rehman et al، كما تؤكد هذه النتيجة العالية واقع تعزيز الأمن السيبراني لدى المعلمات والطالبات المتحقق بدرجة موافقة قليلة التي توصلت إليها دراسة المنتشري(٢٠٢٠).

- حازت الفقرات أرقام (١، ٣، ٤، ٨) على مستوى عالي جدا من الاتفاق بين عينة الدراسة من مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم، بينما جاءت درجة عالية على بقية فقرات المحور الثاني من محوري الاستبانة.

- أكبر متوسط (وبالتالي أكبر درجة اتفاق) لفقرات محور المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم هي الفقرة رقم (١) التي تنص على "توفير برامج وقائية باستمرار حمايةً للأجهزة" بمتوسط (٤,٤٣) وانحراف معياري (١,٠٠٦)، وهذه تتفق مع ما ورد في دراسة فينيسا بيرتون (٢٠١٨)Venessa Burton التي تتطلب لآلية واضحة للتطبيق تتعلق بالأنظمة الأمنية، لتنوع وحداثة وتشعب الجرائم المعلوماتية والاختراقات الأمنية ومراجعتها وتطورها باستمرار، تليها الفقرة رقم (٣) التي تنص على "وجود ملفات احتياطية تحدث باستمرار" بمتوسط (٤,٣٠) وانحراف معياري (٠,٨٧٧)، ثم بنفس المتوسط جاءت الفقرة رقم (٤) التي تنص على "تغيير كلمات المرور بكلمات قوية غير قابلة للحدس والتخمين" بانحراف معياري (١,٠٨٨).

– بينما كان أدنى متوسط للفقرة رقم (٧) التي تنص على "تصميم نظام يمنع الدخول غير الآمن بالإنترنت" بمتوسط (٣,٨٣) وانحراف معياري (١,٠٢٠)، تليها الفقرة رقم (١٠) التي تنص على "تحديد الأذونات والصلاحيات لمستخدمي الأنظمة الحاسوبية بشكل دقيق" بمتوسط (٣,٩٧) وانحراف معياري (٠,٩٩٩)، ثم الفقرة رقم (٩) التي تنص على "التحديث المستمر للأنظمة الحاسوبية وشبكات المؤسسات التعليمية للحصول على أحدث ميزات الأمان" بمتوسط (٤,١٠) وانحراف معياري (١,١٢٥).

– أظهرت نتائج البحث المتعلقة بهذا المحور أن مشرفي ومشرفات تقنية المعلومات في الوزارة وإدارات التعليم بالمملكة لديهم مستوى عالي من الوعي بأهمية الأمن السيبراني وضرورة تطويره. كما أنهم لديهم وعي كافٍ بمخاطر الأمن السيبراني وطرق مواجهتها. ويرجع ذلك إلى اهتمام وزارة التعليم بتطوير الأمن السيبراني، وإلى الجهود التي تبذلها وزارة التعليم لرفع مستوى الوعي لدى الموظفين بمخاطر الأمن السيبراني وطرق مواجهتها. إلا أن هناك العديد من الإجراءات التي ينبغي على المسؤولين عن وزارة التعليم اتخاذها لمعالجة القصور في بعض الجوانب من أهمها: تحديث الأجهزة والبرامج الأمنية، وإنشاء شبكة داخلية آمنة، وعمل نسخ من البيانات في ملفات احتياطية، وتقديم دورات تدريبية حول الأمن السيبراني، ورفع مستوى الوعي بمخاطر الأمن السيبراني، ووضع سياسات وإجراءات أمنية حديثة، ومراجعتها بشكل دوري، والتقييم المستمر لمخاطر الأمن السيبراني، والتعاون مع الجهات الأخرى، من أجل تبادل المعلومات والخبرات في مجال الأمن السيبراني، وتنسيق الجهود لمكافحة الهجمات السيبرانية.

نتائج السؤال الثالث:

ينص السؤال الثالث من أسئلة الدراسة على: "هل توجد فروق ذات دلالة إحصائية في محوري الاستبانة باختلاف متغيرات (العمل الحالي، والخبرة في العمل الحالي، وعدد الدورات في مجال الأمن السيبراني)؟"

وللإجابة عن هذا السؤال قام الباحث أولاً بالكشف عن اعتدالية توزيع بيانات العينة على كل محور من محوري الاستبانة باستخدام اختبار كولمجروف سميرنوف (Kolmogorov-Smirnov) وجاءت النتائج كما يلي:

جدول (٨) يوضح نتائج اعتدالية توزيع بيانات العينة على كل محور من محوري الاستبانة الثلاثة

المحور	قيمة كولمجروف سميرنوف	درجة الحرية	مستوى الدلالة	الحكم على الاعتدالية
المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم	٠,١٤٠	٨٨	٠,٠٠١>	غير اعتدالي
المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم	٠,١٦٠	٨٨	٠,٠٠١>	غير اعتدالي

ويتبين من الجدول السابق أن جميع قيم اختبار كولمجروف سميرنوف دالة إحصائيا، بما يدل على عدم تحقق شرط الاعتدالية لدرجات أفراد العينة على المحاور الثلاثة، ونظرا لأن عدد أفراد أغلب المجموعات الفرعية أقل من (٣٠)، وتفاوت الأعداد بشكل كبير بينها، بالإضافة إلى عدم تحقق شرط الاعتدالية فسوف يستخدم الباحث الإحصاءات اللابارامترية للتحقق من دلالات الفروق بين المجموعات المختلفة.

أولا- الفروق في محوري الاستبانة التي تعزى لمتغير العمل الحالي (مشرف عموم- مشرف إدارة تعليم):

استخدم الباحث اختبار مان ويتني للفروق بين مجموعتين مستقلتين (Mann-Whitney Test) بديلا لابارامتريا عن اختبار ت للفروق بين مجموعتين مستقلتين، وجاءت النتائج كما في الجدول التالي:

جدول (٩) نتائج اختبار مان ويتني للفروق بين متوسطات رتب درجات أفراد العينة على محوري الاستبانة التي تعزى لاختلاف العمل الحالي (مشرف عموم- مشرف إدارة تعليم)

محوري الاستبانة	العمل الحالي	العدد	متوسط الرتب	مجموع الرتب	قيمة Z	مستوى الدلالة
المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم	مشرف عموم	١٦	٦٠,٧٥	٩٧٢,٠	٢,٨٢٧-	٠,٠٠٥
	مشرف إدارة تعليم	٧٢	٤٠,٨٩	٢٩٤٤,٠		
المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم	مشرف عموم	١٦	٥٨,٠٠	٩٢٨,٠	٢,٣٦٠-	٠,٠١٨
	مشرف إدارة تعليم	٧٢	٤١,٥٠	٢٩٨٨,٠		

يتبين من الجدول السابق وجود فروق دالة إحصائيا بين متوسطات رتب درجات أفراد العينة على محوري الاستبانة بين مشرفي العموم، ومشرفي إدارة تعليم، وذلك في اتجاه مشرفي العموم كما يظهر من ارتفاع متوسط الرتب لديهم عن مجموعة مشرفي إدارات التعليم، حيث جاءت قيمة (Z) دالة عند مستوى دلالة (٠,٠١) لمحور المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم، وعند مستوى دلالة (٠,٠٥) لمحور المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم، وهذه النتيجة تختلف عن نتائج دراسة البيشي (٢٠٢١) التي بينت عدم وجود فروق دالة إحصائياً للأمن السيبراني. ويرى الباحث أنه الفروق أتت بسبب أن مشرفي العموم هم أكثر التصاقًا بالأمن السيبراني من مشرفي الميدان الذين هم تنفيذين أكثر من كونهم صانعي قرار.

ثانيا– الفروق في محوري الاستبانة التي تعزى لمتغير سنوات الخبرة في العمل الحالي (١٠ سنوات وأقل– أكثر من ١٠ سنوات):

استخدم الباحث اختبار مان ويتني للفروق بين مجموعتين مستقلتين (Mann-Whitney Test) بديلا لابارامتريا عن اختبار ت للفروق بين مجموعتين مستقلتين، وجاءت النتائج كما في الجدول التالي:

جدول (١٠) نتائج اختبار مان ويتني للفروق بين متوسطات رتب درجات أفراد العينة على محوري الاستبانة التي تعزى لاختلاف سنوات الخبرة في العمل الحالي (١٠ سنوات وأقل– أكثر من ١٠ سنوات)

محوري الاستبانة	العمل الحالي	العدد	متوسط الرتب	مجموع الرتب	قيمة Z	مستوى الدلالة
المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم	١٠ سنوات وأقل	٢٤	٦٧,٣٣	١٦١٦,٠	٥,١٥٩-	٠,٠٠١>
	أكثر من ١٠ سنوات	٦٤	٣٥,٩٤	٢٣٠٠,٠		
المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم	١٠ سنوات وأقل	٢٤	٦٣,٠٨	١٥١٤,٠	٤,٢١٩-	٠,٠٠١>
	أكثر من ١٠ سنوات	٦٤	٣٧,٥٣	٢٤٠٢,٠		

يتبين من الجدول السابق وجود فروق دالة إحصائيا عند مستوى دلالة (٠,٠١) بين متوسطات رتب درجات أفراد العينة على محوري الاستبانة بين مجموعتي (١٠ سنوات وأقل، وأكثر من ١٠ سنوات)، وذلك في اتجاه مجموعة (١٠ سنوات وأقل) كما يظهر من ارتفاع متوسط

الرتب لديهم عن مجموعة (أكثر من ١٠ سنوات). وتختلف هذه النتيجة عن دراسة البيشي (٢٠٢١) التي بينت عدم وجود فروق دالة إحصائياً للأمن السيبراني وأثر ذلك على تعزيز وتفعيل الثقة الرقمية ترجع لعدد سنوات الخبرة.

ثالثا- الفروق في محوري الاستبانة التي تعزى لمتغير عدد الدورات في الأمن السيبراني (لا يوجد- ١- ٣ دورات - أكثر من ٣ دورات):

استخدم الباحث اختبار كروسكال واليس للفروق بين المجموعات المستقلة (Kruskal-Wallis Test) بديلا لابارامتريا عن تحليل التباين أحادي الاتجاه، واختبار مان ويتني (Mann-Whitney Test كاختبار تتبعي، وجاءت النتائج كما يلي:

جدول (١١) نتائج اختبار كروسكال واليس للفروق بين متوسطات رتب أفراد العينة على محوري الاستبانة التي تعزى لاختلاف عدد الدورات في الأمن السيبراني (لا يوجد- ١- ٣ دورات- أكثر من ٣ دورات)

محوري الاستبانة	عدد الدورات في الأمن السيبراني	العدد	متوسط الرتب	قيمة H	مستوى الدلالة
المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم	لا يوجد	١٢	٤٤,٠٠	٢٦,٨٣٠	<٠,٠٠١
	١- ٣ دورات	٣٦	٦٠,٥٠		
	أكثر من ٣ دورات	٤٠	٣٠,٢٥		
المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم	لا يوجد	١٢	٣٨,٠٠	٧,٤٢٩	٠,٠٢٤
	١- ٣ دورات	٣٦	٥٣,٣٣		
	أكثر من ٣ دورات	٤٠	٣٨,٥٠		

يتبين من الجدول السابق ما يلي:

- توجد فروق ذات دلالة إحصائية بين متوسطات رتب درجات جميع المجموعات في محوري (المتطلبات الإدارية، والمتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم) تعزى لاختلاف عدد الدورات في الأمن السيبراني، حيث جاءت قيمة (Z) دالة عند مستوى دلالة (٠,٠١) لمحور

المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم، وعند مستوى دلالة (٠,٠٥) لمحور المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم.

– لمعرفة اتجاهات ودلالات تلك الفروق استخدم الباحث اختبار مان ويتني لدلالة الفروق بين متوسطات الرتب للمقارنة بين كل مجموعتين من المجموعات الفرعية، وجاءت النتائج كما في الجدول التالي:

جدول رقم (١٢) يبين نتائج اختبار مان ويتني لدلالة الفروق بين متوسطات رتب محوري الاستبانة وفق متغير عدد الدورات في الأمن السيبراني

المحور	عدد الدورات في الأمن السيبراني	لا يوجد	١– ٣ دورات	أكثر من ٣ دورات
المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم	لا يوجد	–	١,٣٤٠-	١,١٠٢-
	١– ٣ دورات		–	٥,٤٣٦-**
	أكثر من ٣ دورات			–
المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم	لا يوجد	–	١,١٥٩-	٠,٦٧٤-
	١– ٣ دورات		–	٢,٨٤٦-**
	أكثر من ٣ دورات			–

** دال عند مستوى دلالة ٠,٠١

ويتضح من الجدول السابق وجود فروق ذات دلالة إحصائية عند مستوى (٠,٠١) بين متوسطات رتب درجات مجموعتي و(١– ٣ دورات)، (أكثر من ٣ دورات)، في محوري الاستبانة؛ بينما لا توجد فروق دالة إحصائيا بين باقي متوسطات الرتب.

– ملخص نتائج الدراسة:

- وجود مستوى عالي من الاتفاق بين عينة الدراسة على محور المتطلبات الإدارية لإدارة الأمن السيبراني بوزارة التعليم، بمتوسط (٣,٥٠) وأعلى متوسط كان لفقرة "توفير دليل معتمد لسياسات وإجراءات الأمن السيبراني".

- وجود مستوى عالي من الاتفاق بين عينة الدراسة على محور المتطلبات الفنية لإدارة الأمن السيبراني بوزارة التعليم، بمتوسط (٤,١٦) وأعلى متوسط كان لفقرة "توفير برامج وقائية باستمرار حمايةً للأجهزة".
- وجود فروق دالة إحصائيًا باختلاف العمل الحالي، والخبرة في العمل الحالي، وعدد الدورات في مجال الأمن السيبراني.

- التوصيات:

١- القيام بالتطوير الإداري والتقني للبنية التحتية التقنية داخل الوزارة وفي الميدان التعليمي.

٢- إجراء تحديث للسياسات والإجراءات الأمنية متزامنًا مع تدريب وتأهيل الكوادر البشرية تقنيًا.

٣- تحديث الأجهزة والبرامج الأمنية بالوزارة وإدارات التعليم.

٤- عمل نسخ من البيانات في ملفات احتياطية وتحديثها باستمرار.

٥- وضع خطة إجرائية لرفع مستوى الوعي بمخاطر الأمن السيبراني.

المراجع

المراجع العربية:

الألفي، هاني. (٢٠٢٢). القيادات الأكاديمية وأدوارها في تعزيز ممارسات الأمن السيبراني بالجامعات الأمريكية وإمكانية الإفادة منها بالجامعات المصرية. مجلة كلية التربية بجامعة المنصورة، ع ١١٩، أبريل ٢٠٢٢.

أبو زيد، عبد الرحمن عاطف. (٢٠١٩). الأمن السيبراني في الوطن العربي. دراسة حالة المملكة العربية السعودية. المركز العربي للبحوث والدراسات على الموقع *http://www.acrseg.org/list.aspx*

البيشي، منير. (٢٠٢١). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية – الجامعة الإسلامية بغزة، (١٢٩)، ٣٥٣-٣٧٢

توفيق، صلاح الدين ومرسي، شيرين. (٢٠٢٢). متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس (جامعة بنها أنموذجًا). المجلة التربوية، كلية التربية بجامعة سوهاج. مج ٢. العدد ١٠٥.

الجمل، حازم حسن أحمد. (٢٠٢٠): الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠، مجلة البحوث الأمنية، كلية الملك فهد الأمنية، مركز الدراسات والبحوث، السعودية، مج ع ٧٧، أغسطس، ص ص ٢٤٣-٣٢٨.

جوهر، الجموسي. (٢٠١٦). الافتراض والثورة: مكانة الإنترنت في نشأة مجتمع مدني عربي. المركز العربي للأبحاث ودراسة السياسات.

الخضري، جيهان سعد، سلامي، هدى جبريل، وكليبي، نعمة ناصر. (٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية دراسة مقارنة مجلة تطوير الأداء الجامعي، مج ١٢، (١)، أكتوبر. ٢٧٣٥ – ٣٢٢٢

خليفة، إيهاب. (٢٠١٧). القوى الإلكترونية كيب يُمكن أن تدير الدول شؤونها في عصر الإنترنت. العربي للنشر والتوزيع.

الربيعة، صالح بن عبد الرحمن. (٢٠١٧). الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت. وثيقة هيئة الاتصالات وتقنيه المعلومات بالمملكة العربية السعودية، ص ص ١-٧٩

سراج، شيماء. (٢٠٢٢). التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي. المجلة العربية للعلوم التربوية والنفسية، المؤسسة العربية للتربية والعلوم والآداب، ع٢٦، ١٩٩ – ٢١٢.

السمحان، منى عبد الله. (٢٠٢٠). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية، جامعة المنصورة. ع ١١١، يوليو. ٢-٢٩.

شكري، عمر حامد. (٢٠١٩). المجال الخامس – الفضاء الإلكتروني، المعهد المصري للدراسات القاهرة. متوفر على الموقع *eipss -eg-org.cdn.ampproject.org*

الشيتي، إيناس محمد إبراهيم. (٢٠١٩). تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية في المملكة العربية السعودية: دراسة تطبيقية على جامعة القصيم. الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات بالقاهرة.

الصانع، نوره عمر، عسران، عواطف سعد الدين، السواط، حمد بن حمود، أبو عيشة، زاهد جميل، وسليمان، إيناس السيد. (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم، المجلة العلمية لكلية التربية جامعة أسيوط، ٢٦(٦) يونيو. ٤٢ – ٩٠.

صائغ، وفاء حسن عبد الوهاب. (٢٠١٨). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. المجلة العربية للعلوم الاجتماعية. المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، مج ٣، ع ١٤، يوليو، ٧٠-١٨.

غسان. (٢٠١٩). الأمن السيبراني وإدارة مخاطرة في مجال الأعمال *Retrieved from*، الغد: *http://cutt.lygBTCv7U*

فرج، علياء عمر. (٢٠٢٢). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي: جامعة الأمير سطام بن عبد العزيز نموذجًا. المجلة التربوية كلية التربية بجامعة سوهاج، مج١، ع٩٤،

قاري، ريم عبد الرحيم، الصاني، ريم علوي، وعلام، نوف خالد. (٢٠١٩). مفاتيح الأمن السيبراني في التعليم. مكتبة جرير.

القحطاني، سالم، والعنزي، حمود.(٢٠١١). تبادل المعلومات بين الأجهزة الأمنية في المملكة العربية السعودية: دراسة ميدانية. أطروحة دكتوراه قسم العلوم الشرطية، كلية الدراسات العليا بجامعة نايف العربية للعلوم الأمنية.

المنتشري، فاطمة يوسف. (٢٠٢٠). دور القيادة المدرسية في تعزيز الأمن السيبراني المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للعلوم التربوية والنفسية، ٤(١٧) يوليو، ٢٧٥-٤٨٥

المنتشري، فاطمة يوسف، وحريري، رنده. (٢٠٢٠). درجة وعى معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية، المؤسسة العربية للتربية والعلوم والآداب، ع١٤، ٩٥-١٤٠.

المنيع، الجوهرة عبد الرحمن. (٢٠٢٢). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠. مجلة كلية التربية بجامعة أسيوط، مج ٣٨، ع ١.

الهيئة الوطنية للأمن السيبراني. (٢٠١٨). الضوابط الأساسية للأمن السيبراني. المركز الإعلامي بالهيئة الوطنية للأمن السيبراني.

وزارة التعليم، والهيئة الوطنية للأمن السيبراني. (٢٠٢١). اتفاقية تعاون بين وزارة التعليم والهيئة الوطنية للأمن السيبراني في مجالات البحث العلمي وتأهيل الكوادر الوطنية، الرياض: المركز الإعلامي بوزارة التعليم بالمملكة العربية السعودية.

وزارة التعليم. (١٤٤٢). سياسة الأمن السيبراني. الإدارة العامة للأمن السيبراني.

مبادرة حصين، متاح على: *https://haseen.gov.sa, 16/10/2021*

الهيئة السعودية للبيانات والذكاء الاصطناعي، متاح على : *https://sdaia.gov.sa, 25/10/2021*

الهيئة الوطنية للأمن السيبراني: المملكة على الموقع –*https://ega.ee/wp content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf*

ترجمة المراجع العربية:

AL-Alfi, Hani. (2022). Academic leaders and their roles in promoting cybersecurity practices in American universities and the possibility of benefiting from them in Egyptian universities. Journal of the Faculty of Education, Mansoura University(in Arabic), p. 119, April.

Abu Zeid, Abdel Rahman Atef (2019) Cybersecurity in the Arab World. Case study of the Kingdom of Saudi Arabia Arab Center for Research and Studies on the http://www.acrseg.org/list.aspx website

Al-Bishi, Mounir. (2021). Cybersecurity in Saudi Universities and its Impact on Enhancing Digital Trust from the Point of View of Faculty Members: A Study on the University of Bisha, Journal of the Islamic University for Educational and Psychological Studies - Islamic University of Gaza, (in Arabic) (129), 353-372

Tawfiq, Salah El-Din and Morsi, Sherine. (2022). Requirements for achieving cybersecurity in Egyptian universities in light of digital transformation from the point of view of faculty members (Benha University as a model). Educational Journal, Faculty of Education, Sohag University, (in Arabic),vol. 2. Issue 105.

Al-Jamal, Hazem Hassan Ahmed. (2020). Criminal Protection of Cybersecurity in the Light of the Kingdom's Vision 2030, Journal of Security Research, King Fahd Security College, Center for Studies and Research, Saudi Arabia, (in Arabic), vol. A., August, 243-328.

Johar, Jamoussi .(2016). Assumption and Revolution: The Place of the Internet in the Emergence of an Arab Civil Society, Arab Center for Research and Policy Studies.

Al-Khodari, Jihan Saad Mohammed, Salami Huda Jibril Ali, Kulaibi, Nima Nasser Madbash. (2020). Cybersecurity and Artificial Intelligence in Saudi Universities: A Comparative Study, Journal of University Performance Development, (in Arabic), Volume 12, No. 1, October, 2735-3222

Khalifa, Ehab. (2017). Cape cyber powers can manage states in the cyber age. El Araby for Publishing and Distribution.

Al-Rabiah Saleh bin Abdulrahman. (2017). Digital Security and User Protection from Internet Risks, Communications and Information Technology Commission Document. Saudi Arabia, (in Arabic), pp. 1-79

Siraj, Shaima. (2022). Dimensional Analysis of Cybersecurity Studies in the Educational Field, Arab Journal of Educational and Psychological Sciences, Arab Foundation for Education, Science and Arts, (in Arabic), vol. 26, 199-212.

Al-Samhan Mona Abdullah. (2020). Cybersecurity Requirements for Management Information Systems at King Saud University. Journal of the Faculty of Education, Mansoura University (in Arabic), p., 111, July, pp. 2-29.

Shukri Omar Hamed. (2019). The fifth field - cyberspace, Egyptian Institute for Cairo Studies. Available on eipss -eg-org.cdn.ampproject.org

Al-, Inas Mohamed Ibrahim. (2019). Evaluation of information security and privacy policies in educational institutions in the Kingdom of Saudi Arabia: an applied study on Qassim University, Egyptian Society for Information Systems and Computer Technology, (in Arabic).

Al-Sane, Noura Omar, Asran, Awatef Saad El-Din, Al-Swat, Hamad bin Hammoud, Abu Eisha, Zahid Jameel, Suleiman, Enas Al-Sayed. (2020). Teachers' Awareness of Cybersecurity and Methods of Protecting Students from Internet Risks and Promoting Their National Values and Identity, Scientific Journal of the Faculty of Education, Assiut University, (in Arabic), 26(6) June, 42-90.

Sayegh, Wafaa Hassan Abdel Wahab. (2018). Family members' awareness of the concept of cybersecurity and its relationship to their security precautions from cybercrime, Arab Journal of Social Sciences, Arab Foundation for Scientific Consultations and Human Resources Development, Egypt, (in Arabic), vol. 14, vol. 3, July, pp. 70-18.

Ghassan. (2019). Cybersecurity and Business Risk Management Retrieved from, tomorrow: http://cutt.lygBTCv7U

Farag, Alia Omar .(2022). Reasons for enhancing the culture of cybersecurity in light of digital transformation: Prince Sattam bin Abdulaziz University as a model. Educational Journal, Faculty of Education, Sohag University, (in Arabic),Volume 1, Volume 94,

Qari Reem Abdul Rahim and Al-Sani, Reem Alawi and Allam, Nouf Khalid .(2019). Keys to Cybersecurity in Education, Jeddah.

Al-Qahtani, Salem bin Saeed Al-Anzi Hamoud bin Mohammed. (2011). Information Exchange between Security Services in the Kingdom of Saudi Arabia: A Field Study, PhD thesis, Department of Police Sciences, College of Graduate Studies, Naif Arab University for Security Sciences, Saudi Arabia. (in Arabic)

Al-Muntashari, Fatima Yousef. (2020). The Role of School Leadership in Enhancing Cybersecurity Government Schools for Girls in Jeddah from the Teachers' Point of View Arab. Journal of Educational and Psychological Sciences, (in Arabic), 4(17) July, 275-485

Al-Muntashari, Fatima Youssef Hariri, Randa .(2020). The degree of awareness of middle school teachers of cybersecurity in public schools in Jeddah from the point of view of teachers Arab. Journal of Specific Education, Arab Foundation for Education, Science and Arts, Cairo, (in Arabic), vol. 14, 95-140.

Al-Manea, Al-Jawhara Abdul Rahman. (2022). Requirements for achieving cybersecurity in Saudi universities in light of Vision 2030. Journal of the Faculty of Education, Assiut University, (in Arabic), Volume 38, Volume 1.

National Cybersecurity Authority.(2018). Basic controls for cybersecurity. Riyadh: Media Center of the Authority. (in Arabic)

Ministry of Education and National Cybersecurity Authority .(2021). Cooperation Agreement between the Ministry of Education and the National Cybersecurity Authority in the fields of scientific research and qualifying national cadres, Riyadh: Media Center at the Ministry. (in Arabic)

Ministry of Education. (1442). Cybersecurity Policy. General Administration of Cybersecurity, (in Arabic).

Hussain Initiative, available at: https://haseen.gov.sa, 16/10/2021

Saudi Authority for Data and Artificial Intelligence, available at: https://sdaia.gov.sa, 25/10/2021

National Cybersecurity Authority: Kingdom on website -https://ega.ee/wp content/uploads/2019/03/Essential-Cybersecurity-Controls.pdfreferences

المراجع الأجنبية:

Atoum L. Otoom A. & Abu Ali A. (2014). A holistic Cyber Security Implementation Framework. Information Management & Computer Security 22(3) 251-264.

Catota, Frankie B Morgant, M. Granger and Douglas C. Sicker. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity,1-19 doi: 10.1093/cybsec/ty2001.

Fouad Noran Shafik. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge, Journal of Cyber Policy, 6:2, 137-154, DOI: 10.1080/23738871.2021.1973526.

Hunt. Toni. (2015). Cyber Security Awareness in Higher Education. Central Washington. University. 114.

John M. Broky, Thomas H. Bradley. (T.14) Protecting Information with Cybersecurity, Berlin: Springer International Publishing AG, Pp. 351-350, Available at: http://A1 Yqrxn. 11. y.https.link.springer.com. mplb ci.ekb.eg/content/pdf, Access Date: (10/1/2019).

Pavel Nistiriues Arina Alexei and Alexei Anatolie. (2021). Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions, The 12th International Conference on Electronics, Communications and Computing21-22 October 1-4. Chisinau, Republic of Moldova,

Rehman, H., Masood A.& Cheema A. (2015). Information Security Management in Academic Institutes of Pakistan, Ind. National Conference of Information Assurance (NCIA).

Richardson. M. Lemoine. P. Stephens W. & waller. R. (2020). Planning for Cyber Security in Schools The Human Factor. Educational planning-27(2)- 2339-.

Venessa Burton Howard. (2019). Protecting small business information from cyber security criminals: A qualitative study, United States: Colorado Technical University, Management Dep. (PhD). T.1A, Available at: https://search.proquest.com/docview/2133581243?ac countid-178282.

الجامعة الإسلامية بالمدينة المنورة

ISLAMIC UNIVERSITY OF MADINAH

ISLAMIC UNIVERSITY OF MADINAH

Islamic University Journal For

Educational and Social Sciences

A peer-reviewed scientific journal

Published four times a year in:

(March, June, September and December)