Journal of Educational and Psychological Sciences (JEPS) • Vol 8, Issue 13 (2024) • P: 134 - 114
https://journals.ajsrp.com/index.php/jeps
ISSN: 2522-3399 (Online) • ISSN: 2522-3399 (Print)

Requirements for the Implementation of Cyber Security in Nizwa University in light of Oman Vision 2040 and its obstacles from the point of view of academics and employees

Ms. Najla Moosa Mohammed Al-Balushi*, Ms. Teeba Saif Ahmed Al-Rawahi, Ms. Badriya Hamood Said Al-Aamri, Dr. Rabia Al-Mur Ali Al-Dhuhli, Dr. Hamed Hilal Hamood Al-Yahmadi, Dr. Mohammed Ismail Abdullah Al-Qudah

Nizwa University | Sultanate of Oman

Received: 08/12/2024

Revised: 15/12/2024

Accepted: 26/12/2024

Published: 30/12/2024

* Corresponding author: 03725896@uofn.edu.om

Citation: Al-Balushi, N. M., Al-Rawahi, T. S., Al-Aamri, B. H., Al-Dhuhli, R. A., Al-Yahmadi, H. H., & Al-Qudah, M. E. (2024). Requirements for the Implementation of Cyber Security in Nizwa University in light of Oman Vision 2040 and its obstacles from the point of view of academics and employees. *Journal of Educational and Psychological Sciences, 8*(13), 114 – 134. https://doi.org/10.26389/AJSRP.B101224

Abstract: The study aimed to identify the requirements and obstacles of achieving cybersecurity at the University of Nizwa according to the Oman Vision 2040 from the point of view of academics and the University staff. Descriptive analytical method, survey and questionnaire used as a study tool, applied to a sample of (186) academics and employees. The degree of the requirements came with an average (2.04), with SD (0.58), which is a low score, and all fields came with a low degree, the technical requirements came in the first rank, followed by the cognitive requirements, human resources , and the logistics requirements. The degree of obstacles came with an average of (2.67), SD (0.89), which is medium degree, the results also revealed that there are no statistically significant differences at the level of significance ($\alpha \leq 0.05$) Among the averages of the estimates of study sample members for the requirements according to the gender variable in all fields, and the total score, while there are significant differences in the field of technical requirements and in favor of males, and the absence of statistically significant differences at ($\alpha \leq 0.05$) for the academic grade variable. Based on the results, the researchers recommended continuing to provide the requirements for achieving cybersecurity at the University of Nizwa and training academics and staff to keep up with technological developments and address the development of types of cyber-attacks.

Keywords: Cyber Security, University of Nizwa, Oman 2040 Vision.

متطلبات تحقيق الأمن السيبراني بجامعة نزوى في ضوء رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين

أ. نجلاء بنت موسى محمد البلوشية*، أ. طيبة بنت سيف بن حمد الرواحية، أ. بدريه بنت حمود بن سعيد العامرية، الدكتور / ربيع بن المر بن علي الذهلي، الدكتور / حمد بن هلال بن حمد اليحمدي، الدكتور / محمد إسماعيل عبد الله القضاة

جامعة نزوى | سلطنة عُمان

المستخلص: هدفت الدراسة الحالية إلى التعرف على متطلبات تحقيق الأمن السيبراني ومعوقاته في جامعة نزوى وفق رؤية عمان 2040 من وجهة نظر أكاديمي وموظفي جامعة نزوى، واستخدم الباحثون المنهج الوصفي التحليلي المسحي والاستبانة كأداة للدراسة، طبقت على عينة من (186) أكاديميا وموظفا. وتوصلت نتائج الدر2040 تبعاجة متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 من وجهة أكاديمي وموظفي جامعة نزوى جاء بمتوسط (2.04)، بانحراف معياري (0.58)، وهي درجة منخفضة، كما جاءت جميع المجالات بدرجة منخفضة، وجاءت المتطلبات التقنية في الرتبة الأولى، يليه المتطلبات معرفية الرتبة الثانية والمتطلبات البشرية في الرتبة الثالثة، وفي الأخير جاءت المتطلبات، كما أن درجة معوقات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 من وجهة أكاديمي وموظفي جامعة نزوى جاء بمتوسط (2.67)، بانحراف معياري (0.89)، وهو بدرجة متوسطة، كما كشفت النتائج إلى عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسطات تقديرات أفراد عينة الدراسة لمتطلبات تحقيق الأمن السيبراني في ضوء رؤية عمان 2040 تبعا لمتغير الجنس في جميع المجالات، والدرجة الكلية، بينما توجد فروق دالة في مجال المتطلبات التقنية ولصالح الذكور، وعدم وجود فروق ذات دلالة إحصائية عند ($\alpha \leq 0.05$) بعا لمتغير الرتبة الأكاديمية، وبناء على النتائج أوصى الباحثون بالاستمرار في توفير متطلبات تحقيق الأمن السيبراني في جامعة نزوى وتدريب الأكاديميين والموظفين لمواكبة المستجدات التكنولوجية، والتصدي لتطور أنواع الهجمات الإلكترونية.

الكلمات المفتاحية: الأمن السيبراني، جامعة نزوى، رؤية عمان 2040.

1- المقدمة.

يعايش العالم تغيرات متسارعة غير مشهودة في بيئات العمل بكافة أنواعها من تطورات تقنية وابتكارات رقمية؛ فقد ساهمت الثورة الرقمية في جودة الإنجاز والخدمة المقدمة وضمان وصولها لأي مكان، وأوجد ذلك للمؤسسات قيمة مضافة ومنافسة عالمية في سوق العمل، بما يكفل مكانتها وجودة الأداء لديها وقدرتها على حماية خصوصيتها. ويرى الشايع (2019) أن المؤسسات في عصرنا الحالي أصبحت تتنافس بين بعضها على ما تمتلكه من بيانات ومعلومات تميزها عن غيرها حفاظا على مكانتها؛ وأوجد ذلك التنافس الحاجة الملحة لضمان سرية تلك المعلومات بالحفاظ عليها وحماية أمن معلوماتها في ظل ظهور الهجمات المستمرة والخروقات المتجددة والمتطورة يوما بعد آخر، ومن مكان لآخر بسبب الهاكرز؛ ومن أجل سلامة المؤسسات والحفاظ على بياناتها وضمان استمرارها بميزة تنافسية تميزها؛ ظهرت أهمية وضرورة الأمن السيبراني والذي جعل من أمن وحماية بيانات ومعلومات المؤسسات قضية ملحة تحتاج إلى حل نظرا لارتباطها بأمن وسلامة الأفراد في المجتمعات وأمن البيانات في المؤسسات وممتلكاتها وسلامة البنى التحية.

والمجتمعات مربوطة جميعها بالإنترنت وتعتمد عليه بصورة لا غنى عنه أبدا؛ ولكن تلك الحاجة أوجدت فجوات إلكترونية ساهمت في خروقات وحروب تجسس عالمية سواء على مستوى الحكومات والمنظمات أو المستويات الشخصية، فظهرت مؤسسات وانهارت أخرى بسبب حروب التجسس، وأصبح لزاما على المنظمات والمؤسسات لاسيما التربوية منها -الحكومية أو الخاصة- والسعي لإيجاد خطط وسياسات ومتطلبات تحفظ أمن وسرية البيانات الإلكترونية، ووقاية المؤسسات من حروب خفية، وصنف ذلك أمرا وطنيا للدفاع السيبراني عن الخطط والسياسات الدفاعية الوطنية في الحروب الإلكترونية وسميت تلك الحماية التقنية للأنظمة والخدمات والبرمجيات من الخروقات أو التعديل أو التعطيل أو الاستغلال غير المشروع للبيانات بالأمن السيبراني، والجامعات الحكومية والخاصة ليست بمعزل عن تلك الحروب الخفية؛ ففي ظل تلك التوترات الإلكترونية عمدت إلى سرعة البحث عن حماية للملكية الفكرية ولبناها التحتية ولبيانات منتسبيها من الخروقات والتهديدات الإلكترونية، وتقليل الأضرار ووقايتها من البرمجيات الخبيثة والجرائم السيبرانية؛ وللحد من تلك الجرائم السيبرانية المتوقعة يتطلب وجود دفاعات حماية تتمثل في مجموعة من المتطلبات والضوابط كالمتطلبات الفنية والتقنية والبشرية والمعرفية والتي تحقق حماية للمعلومات وسلامتها وحفظ سريتها من التجسس والتخريب الإلكتروني وسد الثغرات المتوقعة في الأنظمة المعلوماتية (الحداد، 2022؛ السمحان، 2020؛ صائغ، 2018؛ اليحيائي،2024؛ شكري، 2019).

ولتضمن تلك الجامعات ميزتها التنافسية، كان من الضروري السعي إلى تحقيق متطلبات الأمن السيبراني؛ وهو ما دعت إليه استراتيجية التعليم في رؤية عُمان 2040 الجامعات من خلال مؤشر الأداء في التنافسية العالمية الخاصة بحيث تصل قيمة الأداء المستهدف أكثر من (83.2) أو من أفضل (10) دول، وأن تحقق تصنيفا عاليا (QS) تكون فيه الجامعات العمانية كمتوسط ترتيب من أفضل (300) جامعة عالميا من متوسط (500) جامعة، وأن تكون هناك (4) جامعات عمانية مدرجة ضمن الجامعات الأعلى تصنيفا على مستوى العالم بحلول عام 2040، وفي ضوء مؤشرات الأداء وفق أولوية التعليم لرؤية عمان 2040 تتضح الحاجة الملحة لالتزام الجامعات العمانية بتوفير متطلبات تحقيق الأمن السيبراني لحماية معلوماتها؛ للمحافظة على ميزة تنافسية عالية من خلال امتلاكها لنظام تقني في الحوكمة الإلكترونية وتوفير متطلبات الأمن السيبراني في التعاملات التقنية كحماية أمن الأجهزة وتشفيرها، وحماية البيانات، وتطوير البنية التحية السيبرانية، لتقليل الاختراقات الإلكترونية، مع ضرورة التحديث المستمر، وتشجيع موظفي تقنيات المعلومات في الجامعات على الاطلاع المستمر لتحقيق متطلبات الأمن السيبراني (وحدة متابعة وتنفيذ رؤية 2040، 2024).

وتعد جامعة نزوى من الجامعات العمانية الخاصة والتي بدأت مبكرا في التحول الرقمي في جميع معاملاتها اليومية الداخلية والخارجية، وهذه المعاملات بها ما يخص الأفراد المنتمين للجامعة من معلومات خاصة ومهمة يتم الرجوع إليها باستمرار كالمعاملات المالية والتسجيل والقبول وغيرها، كما أنها تمتلك مجموعة من قنوات التواصل الخارجية للتواصل ونشر المعرفة والسعي لتحقيق ميزة تنافسية عالية، كما أنها تسعى لتحقيق متطلبات رؤية عمان 2040 في التعليم، فقد أقرت مجموعة من البرامج التدريسية تدرس أمن المعلومات، وتهدف إلى إكساب الطلبة الفهم العميق لتخصص نظم المعلومات والتدريب على المهارات والمعارف المتعددة في مجالات الحياة المختلفة (جامعة نزوى، 2024 ب).

وانطلاقا مما سبق توضيحه من أهداف جامعة نزوى الواضحة في التنافسية والاستقطاب الداخلي والخارجي، وسعيها لتحقيق مؤشر الأداء في التنافسية العالمية الخاصة في ركيزة المهارات برؤية عمان 2040، جاءت فكرة هذه الدراسة؛ والتي تهدف إلى التعرف على متطلبات تحقيق الأمن السيبراني في جامعة نزوى في ضوء رؤية عمان 2040 من وجهة الأكاديميين والموظفين العاملين في الجامعة، والكشف عما إذا ما كانت هناك فروق في تحقيق تلك المتطلبات تبعا لمتغيري الجنس والرتبة الأكاديمية، وكذلك الوقوف على أهم معوقات تحقيق الأمن السيبراني بالتعاملات والمعاملات الرقمية بالجامعة.

وتولي سلطنة عمان اهتماما واضحا بالتحول الرقمي والذكاء الاصطناعي على المستويات المحلية والخارجية؛ فقد حصلت على الرتبة الثالثة لمؤشر الأمن السيبراني للاتحاد الدولي للاتصالات في نسخة 2024، وفي القائمة الأولى عربيا للدول الأكثر جاهزية وفق تصنيف المركز العربي الإقليمي للأمن السيبراني(ITU-ARCC)، ويأتي هذا التصنيف متوافقا مع أحد الأهداف المهمة للبرنامج التنفيذي بالسلطنة لصناعة الأمن السيبراني والذي يسعى لأن تكون سلطنة عُمان ضمن قائمة الدول الأكثر جاهزية في مجال الأمن السيبراني عالميا، وما يتفق مع منطلقات رؤية عمان 2040 (المركز الوطني للسلامة المعلوماتية، 2024؛ برنامج حداثة للأمن السيبراني، 2024).

واعتمدت مواطن التركيز لرؤية عمان 2040 في التعليم على مجموعة من الأولويات منها تسريع مشروع التحول الرقمي والتقني في قطاع التعليم والبحث العلمي والابتكار، وكذلك تسليط الضوء على التحديات التي تتعلق بالجامعات الخاصة والارتقاء بمستويات مخرجاتها وتعزيز قدرتها على الاستدامة، ومواكبة التحولات السريعة في أساليب التعليم وصياغة مناهج التعليم من خلال الاستفادة من تقنيات الذكاء الاصطناعي والتعلم مدى الحياة (وحدة متابعة وتنفيذ رؤية 2040، 2024).

1-2-مشكلة الدراسة:

ساهمت التقنية الرقمية المعرفية تبادل المعرفة بصورة سريعة بين جميع الدول والفئات العمرية المختلفة في جميع أرجاء العالم؛ في جعلها مصدر تهديد وذلك من خلال إيقاع الخسائر بالجهة الأخرى فيقع عليها ضرر كبير كشلل البيئة المعلوماتية وانتهاك الخصوصيات والابتزاز، والتنمر الإلكتروني، ووسط هذه المشكلات المؤرقة لاستمرارية الأعمال والتعليم التقني وجب ظهور أساليب تعمل على منعها أو الحد منها للحفاظ على البيانات الرقمية والبيئات المعلوماتية في الجامعات.

وقد دعت العديد من الدراسات ومنها الدراسات العمانية إلى ضرورة تعزيز الأمن السيبراني في المؤسسات والجامعات التربوية، فقد أظهرت الدراسات العمانية في المجال كدراسة الهنائي ومقدمي (2024) ودراسة الشكيلي وآخرون (Al-Shukailiyah ,2020) أن المؤسسات بسلطنة عمان بحاجة إلى تطوير وتحديث البنى التحتية لحماية البيانات وأوصت بضرورة وضع سياسات قوية في الأمن السيبراني لحفظ الوثائق الرقمية في مؤسسات التعليم العالي بسلطنة عمان نظرا لتعرض بعض المؤسسات للهجمات الإلكترونية ، وأكدت دراسة كل من الحداد (2022)، وسويد (2024) أهمية تعزيز الأمن السيبراني في الجامعات والوعي بالتهديدات والمخاطر من القرصنة وتقليل القلق من مخاطره، وكيفية بناء ثقافة إيجابية حوله، ويعد ذلك مطلبا ضروريًا لحماية خصوصية أصول المعلومات الشخصية للطلبة ومعلومات الجامعة السرية. كما أشارت دراسة الشيتي (2019) إلى ضرورة تدريب العاملين لقلة معرفتهم بمتطلبات الأمن السيبراني والتعامل الصائب مع الأجهزة؛ كما أشار إلى وجود معوقات ذات تأثير سلبي على أمن المعلومات والبيانات كتسلل قراصنة الأنظمة وتشكيل تهديدات تضر بأمن الأنظمة الإلكترونية بالجامعات، كما أنه لا يوجد إطار وطني للأمن السيبراني بالسلطنة؛ وانطلاقا مما سبق تحددت مشكلة هذه الدراسة في التعرف على متطلبات تحقيق الأمن السيبراني بجامعة نزوى في ضوء رؤية عمان 2040 ومعوقاته من وجهة نظر أكاديمي وموظفي جامعة نزوى.

1-3-أسئلة الدراسة:

1- ما متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين؟
2- ما معوقات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين؟
3- هل توجد فروق دالة إحصائيا عند مستوى ($\alpha \leq 0.05$) في تقديرات أفراد عينة الدراسة حول متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين تعزى لمتغيري (الجنس، والرتبة الأكاديمية)؟

1-4-أهداف الدراسة

تسعى الدراسة الحالية إلى تحقيق الأهداف الآتية:

1. التعرف على متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين.
2. بيان أهم معوقات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين.
3. الكشف فيما إن وجدت فروق دالة إحصائيا عند مستوى ($\alpha \leq 0.05$) في تقديرات أفراد عينة الدراسة حول متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين تعزى لمتغيري (الجنس، والرتبة الأكاديمية).

1-5-أهمية الدراسة

تتمثل أهمية الدراسة الحالية في جانبين الأهمية العلمية والأهمية النظرية:

- **الأهمية النظرية:** تقدم هذه الدراسة معرفة جديدة حول درجة تطبيق متطلبات الأمن السيبراني في جامعة نزوى، واقتراح الحلول للكثير من الجامعات والمهتمين حول المعوقات التي تواجههم في تطبيق الأمن السيبراني.
  - وستكون هذه الدراسة انطلاقة لدراسات مستقبلية تتناول متغير الدراسة في جامعات أخرى ومستويات مختلفة.
  - قد تساعد الباحثين في إيجاد بحوث ودراسات جديدة لإثراء المكتبة العربية والعمانية بما تحتويه من إطار نظري.
- **الأهمية العملية:**

- تساعد الدراسة المعنيين في الشأن الأكاديمي في جامعة نزوى بالوقوف على واقع الأمن السيبراني، ومتطلبات تحقيقه في الجامعة من خلال سياق تطبيقها العام للتحول الرقمي.
- تقدم الدراسة عرضا لأهم المعوقات التي تحول دون تحقيق الأمن السيبراني بالجامعة، وستقدم التغذية الراجعة حول مستوى تطبيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040.
- تواكب الدراسة تطلعات رؤية عمان 2040 بدراستها للأمن السيبراني ومتطلبات تطبيقه في الجامعات.
- تقدم الدراسة نتائج واضحة ومقننة للمعنيين بجامعة نزوى حول مستويات تطبيق متطلبات الأمن السيبراني، ومعوقاته بالجامعة.

1-6-حدود الدراسة

تقتصر الدراسة الحالية على الحدود الآتية:

- **الحدود الموضوعية:** متطلبات تحقيق الأمن السيبراني وتم تقسيمها إلى متطلبات تقنية ومادية وبشرية ومعرفية، وكذلك معوقات تحقيق الأمن السيبراني.
- **الحدود البشرية:** الأكاديميين والموظفين العاملين في جامعة نزوى بسلطنة عمان.
- **الحدود المكانية:** طبقت الدراسة على مختلف كليات ومعاهد ومراكز وإدارات وعمادات جامعة نزوى.
- **الحدود الزمانية:** العام الدراسي 2024- .2025

1-7-مصطلحات الدراسة:

اشتملت الدراسة على المصطلحات الآتية:

- الأمن السيبراني: يقصد بالأمن السيبراني بأنه: "جميع إجراءات حماية شبكات المعلومات ضد كافة الأعمال والممارسات التي تستهدف التلاعب بتلك المعلومات، وإلحاق الأذى بالمستخدمين، بما يشمل الحماية ضد الاختراق، وبث البرمجيات الخبيثة والفيروسات، والوصول غير المصرح به، وغير ذلك من ممارسات سلبية" (المنتشري، 2020، ص. 102).
- وعرف الزهراني (2020، ص.11) الأمن السيبراني بأنه: " أمن الشبكات والأنظمة المعلوماتية والمعلومات والبيانات والأجهزة التي تتصل بالإنترنت، ويرتبط هذا المجال بمعايير الحماية الواجب اتخاذها، أو التقيد بها، للتصدي"
- ويعرف إجرائيا وفق هذه الدراسة بأنه: "مجموعة من الإجراءات التي تحتاجها الجامعة لتحقيق متطلبات الأمن السيبراني التقنية والمادية والبشرية والمعرفية بالجامعة، وتخطي معوقاته".
- رؤية عمان 2040: " تعد رؤية عُمان 2040المرجع الوطني للتخطيط الاقتصادي والاجتماعي لسلطنة عُمان خلال الفترة-2021 2040، ومنها تنبثق الاستراتيجيات الوطنية القطاعية والخطط الخمسية للتنمية"(وحدة متابعة وتنفيذ رؤية 2040، 2024).
- ويقصد بها إجرائيا وفق هذه الدراسة أنها: "مجموعة من مؤشرات الأداء وفق أولوية التعليم لرؤية عمان 2040 والتي يتطلب من الجامعات العمانية تحقيقها لتحقيق مستويات عالية وفق التصنيف العالمي للجامعات(QS) لتحقيق ميزة تنافسية عالية بحماية ممارساتها التقنية عن طريق توظيف متطلبات الأمن السيبراني".
- جامعة نزوى: " أنشئت جامعة نَزوى في 3 يناير 2004م؛ لتكون أوَّل مؤسّسةٍ تعليميَّةٍ أهليَّةٍ ذات نفعٍ عام في السَّلطنة، فقد استقبلت الجامعة الدُّفعة الأولى من طلبتها في 16 أكتوبر 2004م ..." (جامعة نزوى، 2024 أ)

2- الإطار النظري والدراسات السابقة.

2-1- الإطار النظري

2-1-1-الأمن السيبراني

1- أهمية الأمن السيبراني:

يعد الأمن السيبراني من المجالات الحيوية المهمة في عصر المعلومات والتكنولوجيا الحديثة، في ظل الاعتماد المتزايد على الشبكات الإلكترونية والأنظمة الرقمية في شتى مجالات الحياة، وأصبح من الأهمية بمكان حماية البيانات والمعلومات من الهجمات والتهديدات السيبرانية، ويتضمن الأمن السيبراني مجموعة من التقنيات والاستراتيجيات التي تسعى إلى حماية البيانات والشبكات والأنظمة من التهديدات المتنوعة، سواء كانت ناتجة عن أخطاء داخلية أو هجمات خارجية، وللأمن السيبراني مفاهيم رئيسة متعددة، منها سرية المعلومات وحمايتها من الوصول لغير المصرح لهم، وسلامة البيانات أي عدم تعديل المعلومات بشكل غير مصرح به، وتوافر الأنظمة كون الأنظمة متاحة للاستخدام في وقت الحاجة.

ومن أبرز الأهداف التي يعمل الأمن السيبراني على تحقيقها هي المحافظة على أمن المجتمع واستقراره، والمحافظة على سلامة عمل قطاعات الدولة الإلكترونية من أي اختراق، وحماية شبكة المعلومات بصورة علمية وتقنية محكمة، كما أنه يحافظ على سرية البيانات، والمعلومات الإلكترونية لأي جهة، والعمل على تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق الدخول إليها؛ لأن التشفير يعد أحد أهم أساليب الوقاية والحماية (السمحان، 2020).

ويعتبر العصر الحالي عصر التكنولوجيا المتقدمة كإنترنت الأشياء والرقمية، وبتطور تلك التقنيات فقد ظهرت مخاطر موازية كالاختراقات، والبرمجيات الخبيثة، والهجمات الالكترونية، ومع وجود تلك الهجمات الإلكترونية المستمرة والمتنوعة والمتغيرة يوما إثر يوم وجب حماية الأفراد والمؤسسات والمنظمات والحكومات لبياناتها وبرمجياتها بطرق متقدمة توازي تقدم تلك الاختراقات، تبرز أهمية الأمن السيبراني كأحد أهم أنظمة الوقاية والحماية والعلاج للأنظمة الشخصية والعامة، ولكي يكون تطبيقه ذا نفع فإنه يتوجب الأخذ بمتطلباته لتكون طرق الحماية علمية مدروسة، ولتحقيق دورا حيويا في حماية المعلومات وسلامة الأنظمة.

وتكمن أهمية الأمن السيبراني في قدرته على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي منها، وبالتالي التخلص من الأضرار التي تنجم عن تلف تكنولوجيا المعلومات و الاتصالات أو حتى بسبب إساءة الاستخدام، ومن هذا المنطلق اهتمت به الدول على كافة المستويات في العالم، وجعلته في قائمة أولوياتها وخاصة بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، وهنا إشارة صريحة إلى بدأ الحرب الإلكترونية ونهاية الحروب التقليدية التي كانت تستخدم فيها أسلحة ثقيلة (إبراهيم و آخرون ، 2022).

يتضح مما سبق أهمية الأمن السيبراني وضرورته في المؤسسات؛ فمع الاعتماد على التكنولوجيا الرقمية في جميع مناحي الحياة لا سيما قواعد البيانات المهمة في المؤسسات، يصبح الأمن السيبراني ضرورة ملحة لحماية المعلومات والبيانات الدقيقة والحساسة من التهديدات والاختراقات المتزايدة، والانتهاكات المستمرة لخصوصية المنظمات، والأفراد بطرق مدروسة تحقق أهدافه بتحقيق متطلباته.

و برزت أهمية الأمن السيبراني و تطورت وسائله خلال السنوات القليلة الماضية ، ولك نتيجة للتطورات التقنية التي شهدها العالم خلال الفترة المنصرمة ، وكردة فعل للتهديدات التي عانى منها الأشخاص و المشروعات الخاصة بالبنية التحتية و المعلومات الخاصة بالأفراد و المؤسسات و أصبحت هذه التهديدات مرتفعة الخطورة لما يمكنها أن تسببه من خسار ، كما أن مواجهتها تتطلب أمولا مرتفعة و جهد و أمكانيات كبيرة . (سويد ، 2024)

وأصبحت متطلبات تحقيق الأمن السيبراني ضرورة ملحة لحماية البيانات والمعلومات الرقمية وسلامتها، حيث أشارت المنيع (2022) إلى مجموعة من تلك المتطلبات والتي تتمثل في:

- تحديد إجراءات العمل في الشبكات المعلوماتية، فمن الضرورة وضوح متطلبات التعامل مع الشبكات بصورة واضحة ومحددة في أماكن العمل بتحديد ما هو مسموح أو غير مسموح، وما يتعلق بالأمن المعلوماتي على الشبكة.
- تحديد الآلية اللازمة لتنفيذ سياسة العمل، بحيث تكون هناك دقة في كيفية تنفيذ السياسات، وتحديد العقوبات التي ستقع في حالة حدوث اختراقات.
- المورد البشري، ضرورة إسناد إدارة الشبكات المعلوماتية للعناصر البشرية المدربة والمؤهلة وذات الكفاءة العالية القادرة على التعامل مع التقنيات الحديثة والتكنولوجية، وعدم ترك المجال للآخرين غير المؤهلين للعبث بمقدرات الهيئات الحكومية.
- تحديث الأوضاع الأصلية لمعدات الشبكة، بحيث يتم كل فترة تغيير الوضع إلى الأوضاع الأصلية للمعدات المرتبطة بشبكات المعلومات كإجراء احترازي؛ لمنع الاختراق.

- المراقبة الدقيقة، ضرورة الحرص على المتابعة والمراقبة المستمرة للأنشطة المعلوماتية على شبكة الإنترنت بالشكل الدقيق، بهدف اكتشاف أنشطة مشبوهة أو حركات غير طبيعية ضمن نطاق الشبكة، والعمل على تفادي تفاقم الوضع.
- الاختيار الصحيح لمواقع الشبكات، لابد عند الاختيار من اختيار أماكن دقيقة مؤمنة ومحمية من الاختراق.
- بروتوكول التحقق والتشفير، من الضرورة أن يتم تطبيق بروتوكولات التحقق من الهوية وأنظمة تشفير البيانات، بهدف تأمين المعلومات على الشبكة، ويتم في هذا الإطار اختيار برامج معروفة ومشهورة عالميا.

2-1-2-معوقات تحقيق الأمن السيبراني في الجامعات

يعد هذا العصر هو عصر التحول الرقمي السريع، حيث أصبحت الجامعات تعتمد بصورة متزايدة على التكنولوجيا لتقديم جميع خدماتها الأكاديمية والإدارية. ومع هذا التطور بدأت تظهر تحديات جديدة في مجال الأمن السيبراني، حيث تواجه الجامعات تهديدات بالهجمات الإلكترونية تتزايد باستمرار، والتي تستهدف بياناتها وأنظمتها الحساسة، لذا وجب حماية هذه المؤسسات التعليمية، ولكن تعترض طريقها العديد من المعوقات التي تجعل تحقيق الأمن السيبراني بصورة كاملة أمرًا معقدًا. ومن هذه المعوقات نقص خبرة الموظفين حيث يؤدي تدني مستوى الخبرة في مجال الأمن السيبراني إلى ضعف تنفيذ السياسات والإجراءات الأمنية بصورة فاعلة. كما أن ضعف التعاون بين موظفي التقنيات وقلة التنسيق والتعاون بين الفرق التقنية داخل المؤسسة الجامعية من أبرز ما يعيق بناء نظام أمني متكامل وفعّال. من جانب آخر فإن التطور السريع للتكنولوجيا والتقدم المستمر في هذا المجال يجعل من الصعب مواكبة التهديدات الجديدة لتطوير استراتيجياتها وتحديثها بصورة مستمرة ، في المقابل هناك نقص وعي مجتمعي وقلة التوعية حول مخاطر الفضاء السيبراني وطرق الوقاية منه بين أفراد المجتمع الجامعي وهذا يزيد من احتمالية التعرض للهجمات الإلكترونية. كما أن الكثير من الأشخاص يعمدون إلى استخدام الأجهزة الشخصية مثل الهواتف المحمولة لنقل أو تخزين معلومات سرية خاصة بالجامعة دون أن يتخذوا التدابير الأمنية المناسبة وهذا بدوره يزيد من أخطار التسريب والاختراق. (المنيع. 2022).

2-1-3-رؤية سلطنة عمان 2040 والجهود المبذولة في مجال الأمن السيبراني

تعد رؤية سلطنة عمان 2040 خطة تنمية حكومية عمانية، فتعتبر المرجع الرئيس للتخطيط الاقتصادي والاجتماعي لسلطنة عمان خلال الفترة 2021 – 2040 م ، ومنها تنبثق الاستراتيجيات الوطنية القطاعية والخطط الخمسية للتنمية، ووضعت بإدارة سامية من لدن السلطان الراحل قابوس بن سعيد -طيب الله ثراه- وأكد جلالة السلطان هيثم بن طارق حفظه الله على متابعتها باستمرار ومتابعة تطور مؤشرات تنفيذها، وتم إعداد الرؤية من خلال مشاركة مجتمعية واسعة، وقد تم اعتماد وثيقة الرؤية من لدن السلطان هيثم بن طارق –حفظه الله– في نهاية 2020، ليتم العمل عليها منذ بداية 2021 و لغاية 2040.

وجاءت سلطنة عمان الثالثة عربيا والواحد والعشرون عالميًا من أصل مائة وثلاثة وتسعين دولة ضمن تقرير المؤشر العالمي للأمن السيبراني 2020 الذي أعلنه الاتحاد الدولي للاتصالات. (جريدة عمان، 30/يونيو/2021م)، كما دشنت سلطنة عمان المركز الوطني للسلامة المعلوماتية في شهر ابريل 2010 وذلك لتحليل المخاطر والتهديدات الأمنية الموجودة في الفضاء الإلكتروني ولتوصيل هذه المعلومات لجميع مستخدمي خدمات الإنترنت ووسائل تقنية المعلومات، سواء كانوا من المؤسسات العامة أو الخاصة، أو الأفراد، ويعمل المركز على استضافة وإدارة وتشغيل المركز العربي الإقليمي للأمن السيبراني (ITU-ARCC) والذي تم تدشينه رسيماً في 2013. ومن الأهداف التي يسعى لها المركز التوافق مع رؤية عُمان 2040 في مواجهة تحديات الأمن السيبراني كذلك تطوير نظام إيكولوجي وطني لصناعة الأمن السيبراني وتطوير قدرات الأمن السيبراني المتخصصة، كما يحرص على إنشاء شركات ناشئة وشركات صغيرة ومتوسطة متخصصة في مجال الأمن السيبراني لخدمة الاحتياجات والتحديات المحلية، والترويج لشركات الأمن السيبراني المحلية المتخصصة على المستوى الدولي وتعزيز الابتكار في مجال الأمن السيبراني (برنامج حداثة للأمن السيبراني، 2024).

واستكمالاً للنجاحات التي تحققها سلطنة عمان في المؤشرات العالمية، وتوافقاً مع رؤية عمان 2040 في مجال صناعة الأمن السيبراني فإن سلطنة عُمان تعتبر ضمن القائمة الأولى عالمياً للدول الاكثر جاهزية في الأمن السيبراني للاتحاد الدولي للاتصالات في نسخة 2024، هذا التصنيف يأتي متوافقا مع أحد أهم أهداف البرنامج التنفيذي لصناعة الأمن السيبراني التي تم ذكره سابقا في أن تكون سلطنة عُمان ضمن قائمة الدول الأكثر جاهزية في مجال الأمن السيبراني على المستوى الدولي؛ فقد حصلت السلطنة على (97.02) نقطة لعام 2024؛ مقارنة بنقاط مؤشر عام 2020 والتي بلغت (96) نقطة، ويستند المؤشر العالمي للأمن السيبراني على (5) معايير هي المعيار القانوني والتقني والتنظيمي وبناء المقدرات والتعاون الدولي، وقد حصلت سلطنة عُمان على النقاط كاملة في معيار التعاون الدولي والتنظيم المؤسسي بواقع (20) نقطة لكل منهما، وحققت(19.59) نقطة في المعيار القانوني و(18.39) نقطة في المعيار التقني و(19.03) نقطة في معيار بناء القدرات (المركز الوطني للسلامة المعلوماتية، 2024).

ويتضح مما سبق مدى اهتمام سلطنة عمان بالأمن السيبراني، وأنه يأتي على قائمة الأولويات في سلطنة عمان وفي قطاعي الأعمال والقطاع الحكومي منسجما لتوجهات الرؤية المستقبلية عُمان 2040، فقد تم اختيار مسقط لتكون العاصمة العربية الرقمية لعام 2022 م حيث أتى ملف ترشح السلطنة تحت شعار "مستقبل رقمي صانع للفرص" والذي ركز على ثلاث محاور مهمة تتمثل في "الأمن السيبراني، والابتكار الرقمي والقدرات وتنمية المهارات الرقمية" التي تهدف إلى تنمية المواهب والمهارات الرقمية في العالم العربي، وإثراء المحتوى الرقمي العربي، وتعزيز التعاون في الأمن السيبراني وتشجيع الاستثمار في الاقتصاد الرقمي.

2-2-الدراسات السابقة

تناول الباحثون مجموعة من الدراسات السابقة ذات الصلة بموضوع الدراسة، حيث رتبت تصاعديا من الأقدم إلى الأحدث:

1. هدفت دِرَاسَة الديراوي (2014) لمعرفة علاقة التخطيط الاستراتيجي لنظم المعلومات الإدارية بأمن المعلومات في الجَامِعَات الفلسطينية في قطاع غزة، واستهدفت المختصين بالتخطيط وتكنولوجيا المعلومات في الجامعة وبلغت عينة الدراسة (417) أكاديميا، واستخدم الباحث المنهج الوصفي بتوظيف الاستبانة كأداة لجمع البيانات، وتوصلت الدِّرَاسَة إلى مجموعة من النتائج منها أن الجَامِعَات الفلسطينية تهتم بدرجة جيدة بأمن المعلومات، كما أنها تهتم بدرجة جيدة بتحديد كلٍّ من الأهداف والرسالة والأولويات والموارد الخاصة بنظم المعلومات الإدارية؛ مثل توفير خطط التدريب والتوظيف، ومن النتائج كذلك أنه لا توجد فروق ذات دلالة إحصائيَّة بين استجابات المبحوثين حول أمن المعلومات في الجَامِعَات الفلسطينية بقطاع غزة تعزى لمتغيرات: (العمر، المسمى الوظيفي، سنوات الخبرة، المؤهل العلمي، مستوى التدريب).
2. وجاءت دراسة السمحان (2020) بهدف التعرف على متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود من وجهة نظر عينة من العاملين، وقد تم استخدام المنهج الوصفي، واستخدمت الاستبانة كأداة للدراسة، واشتملت العينة على (478) عاملا من العاملين بالجامعة، وتوصلت الدراسة إلى أن أهم المتطلبات لتحقيق الأمن السيبراني تتمثل في إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في المملكة وتشجيع الاستثمار في مجال الأمن السيبراني.
3. و هدفت دراسة الزهراني (2020) إلى دراسة استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة، وبلغت عينة الدراسة (131) من منسوبي مركز بحوث الفضاء والمركز الوطني لتقنية أمن المعلومات بمدينة الملك عبدالعزيز للعلوم والتقنية، واعتمدت على الاستبانة كأداة لجمع بيانات الدراسة، وتم استخدام المنهج الوصفي بشقية (التحليلي، والمقارن)، ومن أهم نتائج الدراسة أن التقنيات الحديثة تسهم في حماية المعلومات وتأمينها من خلال رصد وتحليل الهجمات السيبرانية، وضرورة حتمية تحديث وتطوير أنظمة الحماية، وتحديد النقاط الأكثر عرضة للاختراق، والتصدي للهجمات السيبرانية.
4. وجاءت دراسة الغيبوي وآخرون (2020) التي هدفت إلى دراسة الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري، حيث بلغت عينة الدراسة (145) فردا، واعتمدت على الاستبانة والمنهج الوصفي في جمع البيانات، ومن أبرز النتائج أن أفراد العينة موافقون بشدة على مرتكزات وأهداف الأمن الفكري، ومكونات ومقومات تحقيق الأمن السيبراني في المملكة العربية السعودية وعلى الوسائل والأدوات التي يمكن من خلالها تعزيز دور الأمن السيبراني في الحد من تهديدات الأمن الفكري لدى المجتمع السعودي وأن أفراد العينة يقرون وجود تهديدات سيبرانية للأمن الفكري لدى المجتمع السعودي.
5. هدفت دراسة القحطاني (2020) إلى دراسة مستوى الوعي بالأمن السيبراني في مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية، وبلغ حجم العينة (300) مشاركا، وكانت الاستبانة هي الأداة لجمع البيانات، وتم استخدام منهج البحث الاستقصائي (المسحي)، ومن أهم نتائج الدراسة وجود فعالية عند تطبيق نموذج نظرية الألعاب لزيادة الوعي بالأمن السيبراني بين طلاب مدارس بوابة المستقبل الثانوية في المملكة العربية السعودية، وقد تبين من الدراسة أن نقاط الضعف في التكنولوجيا تشكل مخاطر على البنية التحتية الرئيسة بالمؤسسات ومدارس المستقبل.
6. وجاءت دراسة فرج (2021) هادفة إلى بيان دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبد العزيز، استخدمت الدراسة المنهج الوصفي، وصممت استبانة لتكون أداة للدراسة، وطُبقت على عينة من أعضاء هيئة التدريس بالجامعة بلغت (125) عضواً، وخلصت الدراسة إلى أن دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبد العزيز من وجهة نظر أعضاء هيئة التدريس جاء بدرجة متوسطة، كما بينت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير الكلية، والرتبة العلمية، فيما وجدت فروق تعزى لمتغير سنوات الخبرة.
7. وهدفت دراسة المنيع (2022) في التعرُّف على واقع تحقيق الأَمْن السيبرانيّ في الجَامِعَات السعوديَّة في ضوء رؤية 2030 وقد قامت الباحثة باتباع المنهج الوصفي التحليلي، وبلغ حجم العينَة (210) موظفا، كما اعتمدت الاستبانة كأداة للدراسةِ، وتوصلت الدراسة إلى مجموعة من النتائج منها أن افراد العيِّنَة موافقون بدرجة متوسطة على واقع تحقيق الأَمْن السيبرانيّ في

الجَامِعَات السعوديَّة في ضوء رؤية 2030، وتبيَّن أن مفردات العيِّنَة موافقون بدرجة كبيرة جدًّا على مُعَوِّقات تحقيق الأَمْن السيبرانيّ في الجَامِعَات السعوديَّة في ضوء رؤية 2030، ومن أهمّ هذه المعوقات تدني مستوى الخبرة لدى الموظفين، والضعف في التعاون بين موظفي التقنيات في الجَامِعَات لتحقيق الأَمْن السيبرانيّ.

8. وهدفت دراسة سويد (2024) للكشف عن درجة توافر متطلبات تطبيق الأمن السيبراني في الاتحادات الرياضية في سلطنة عمان وقد استخدمت المنهج الوصفي المسحي، وكانت أداة الدراسة الاستبانة، كما تكونت العينة من (102) فردا من الاتحادات الرياضية، وتوصلت الدراسة إلى أن درجة توافر متطلبات تطبيق الأمن السيبراني في الاتحادات الرياضية في سلطنة عمان جاءت متوسطة في جميع المجالات، ولا يوجد قسم أو لجنة رسمية متخصصة في الأمن السيبراني بالاتحادات، وأوصت الدراسة بضرورة تشكيل لجنة مختصة بالأمن السيبراني في الاتحادات الرياضية للوقاية من القرصنة والاختراقات، وضرورة تطوير وتحديث البرامج المعلوماتية والتقنية باستمرار في الاتحادات الرياضية.
9. كما جاءت دراسة الهنائي (2024) هادفة إلى بيان التأثيرات المحتملة للتحول الرقمي على إدارة واستراتيجيات حفظ الوثائق في سلطنة عمان، حيث استخدم الباحث المنهج النوعي، وكانت أداة الدراسة عبارة عن مقابلات وتحليل الوثائق للاستراتيجيات ومشاريع التحول الرقمي في بعض المؤسسات الحكومية والخاصة في سلطنة عمان، من خلال اختيار (15) مؤسسة بصورة قصدية وكانت من ضمن المؤسسات التعليم العالي. وتولت لمجموعة من النتائج أهمها أن المؤسسات في سلطنة عمان بحاجة إلى تطوير وبناء بنى تحية قوية تستطيع توفير التدريب المناسب للعاملين لديها وتوظيف التقنيات الرقمية ، كما توصلت الدراسة إلى أن التحول الرقمي يمكن أن يساهم بصورة كبيرة في تحسين إدارة الوثائق، وأوصت الدراسة بأهمية وجود سياسات واضحة تحقق إدارة الوثائق الرقمية، ويتطلب هذا تخطيط واضح واستراتيجي لضمان النجاح .

2-2-2-دراسات سابقة بالإنجليزية:

1. هدفت دراسة باولوسكي وجونغ (Paowloski and Jung, 2015) إلى الكشف عن التمثيلات الاجتماعية للأمن السيبراني وفق الجامعة والطلبة والآثار المترتبة على التصميم التعليمي وقد استخدم المسح النوعي (المنهج الاستكشافي) من خلال التمثيلات الاجتماعية والمقابلات، لتوضيح تصورات الأمن السيبراني وتهديداته لدى الطلبة، وتكونت العينة من (152) طالبا من جامعة غرب الولايات المتحدة وتناولت الدراسة (23) مفهوما تشكل فهم الطلبة الجماعي للأمن السيبراني، وتكشف النتائج أن إدراك الطلبة للأمن السيبراني بوضع التركيز كان عاليا حول المفاهيم التكنولوجية والاهتمامات الاجتماعية والسياسية، وبالمقابل كانت المعرفة قليلة بالتهديدات المحتملة للأمن السيبراني للبنية التحتية الوطنية.
2. وجاءت دراسة رحمان وآخرون (Rehman et al, 2015) هادفة إلى الكشف عن واقع أنظمة إدارة الأمن السيبراني في معاهد التعليم العالي بجامعات باكستان، وتم استخدام المنهج الوصفي، وجمعت البيانات بالاستبانات، وكانت عينة الدراسة هي المجتمع نفسه وهم جميع موظفي التقنيات في الجامعات الباكستانية، ومن أهم النتائج أن واقع الأمن السيبراني في معاهد جامعات باكستان جاء بدرجة متوسطة، وأوصت الدراسة بضرورة وجود إدارة للمخاطر بالجامعات، مع وضع سياسات تحمي الجامعات من مخاطر الاختراق.
3. كما هدفت دراسة فينيسا بيرتون (Burton-Howard, 2018) إلى معرفة الصعوبات التي توجه المديرين المتخصصين بأمن المعلومات في حماية المعلومات والبيانات التجارية، وتم استخدام المنهج النوعي، بإجراء مقابلات مع (10) مديرين متخصصين في أنظمة أمن المعلومات بولاية واشنطن بأمريكا، وتوصلت الدراسة إلى عدة نتائج منها: ضعف القوانين المتبعة في حماية البيانات والمعلومات عبر شبكة الإنترنت وذلك بسبب حداثة الجرائم المعلوماتية، وبالتالي تتسم بضعف الفاعلية، بالإضافة إلى الافتقار لآلية واضحة للتطبيق تتعلق بالأنظمة الأمنية، ويرجع ذلك لتنوع وحداثة وتشعب الجرائم المعلوماتية والاختراقات الأمنية وتطورها باستمرار.
4. وهدفت دراسة أميولا (Omoyiola, 2020) إلى استكشاف الاستراتيجيات التي يستخدمها قادة الأمن السيبراني لفرض سياسات الأمن السيبراني، حيث تم استخدام المنهج النوعي (دراسة الحالة)، وكان مجتمع الدراسة عبارة عن قادة أمن سيبراني، وضباط أمن نظام المعلومات وكبار مسؤولي أمن المعلومات، ومديري الأمن السيبراني في منظمات ثلاث بوسط وجنوب وشمال وغرب نيجيريا، واستخدمت المقابلات شبه المنظمة لجمع البيانات من قادة الأمن السيبراني (12) مشاركا، وتحليل وثائق سياسة الأمن السيبراني لعدد (20) وثيقة، وتوصلت الدراسة إلى أن قادة الأمن السيبراني يقومون بمنع الاختراقات الأمنية في مؤسساتهم بفرض سياسات الأمن السيبراني بدرجة عالية.
5. وجاءت دراسة ناغاهاواتا، وآخرون (Nagahawatta, et al ,2018) والتي هدفت إلى التعرف على مدى توفر الوعي بالأمن السيبراني لدى طلبة الجامعات السيريلانكية وتقييمه، واستخدمت الدراسة المنهج الوصفي التحليلي، وجمعت البيانات من العينة بأداة

الدراسة الاستبانة التي بلغت (15) طالبا من جميع الجامعات الحكومية في سريلانكا وتوصلت الدراسة إلى مجموعة من النتائج منها أنه يوجد فرق كبير بين مستوى وعي مستخدمي خدمات الإنترنت من الذكور والإناث؛ فالذكور تفوقوا على الإناث في مستوى الوعي، كما أن مستوى الوعي بالأمن السيبراني بين الجامعات السريلانكية للطلبة جاء منخفضا بشكل ملحوظ.

6. ودراسة مورينو وآخرون (Moreno et al, 2023) جاءت هادفة إلى التعرف على مدى نشر مفاهيم متطلبات الأمن السيبراني لدى طلبة الجامعات من خلال تحليل المقالات المنشورة، وكان ذلك بتوظيف المنهج التاريخي؛ من خلال مراجعة منهجية للأدبيات، وتحليل المعلومات في المقالات المنشورة خلال الفترة من 2018 إلى 2023؛ وتم اختيار (25) مقالا، اتبع (76%) منها منهجا وصفيا كميا، وأظهرت النتائج الرئيسة أن الولايات المتحدة الأمريكية، والمملكة العربية السعودية ونيجيريا هي الدول الأكثر نشرا حول أهمية وكيفية توظيف الأمن السيبراني، وأن عددا قليلا جدا من البلدان يعالج هذه المسألة من منظور المعرفة بالأمن السيبراني والإجراءات الوقائية، معتبرا أن المسألة لا تميز حسب الكلية أو التخصص، وأنه يتم تحديد أهمية النظر في البحوث التطبيقية المستقبلية لحاجتها لتنوع موضوعاتها.
7. هدفت دراسة العطيات وآخرون (Al Atiyat et al, 2024) إلى قراءة في الجرائم الإلكترونية التي تستهدف الإناث: مراجعة الأدبيات المتعلقة بقوانين الأمن السيبراني، حيث استخدمت المنهج النوعي، من خلال تحليل (60) مقالا ودراسة من الدراسات والمقالات التي تسلط الضوء على الطبيعة المتطورة للجرائم الإلكترونية، وتوصلت إلى نتائج عدة من أهمها ضرورة اتخاذ تدابير شاملة للأمن السيبراني لحماية النساء، بما في ذلك التحديثات التشريعية، وحملات التوعية، وتعزيز جهود إنفاذ القانون، لمكافحة الجرائم الإلكترونية التي تستهدف النساء، ومن أهم التوصيات ضرورة تطوير وتعزيز وتكييف قوانين الأمن السيبراني لمواجهة الجرائم الإلكترونية، وضرورة تعزيز حماية النساء ضد الجرائم السيرانية.
8. وهدفت دراسة الشكيلي وآخرون (Al-Shukailiyah, 2020) إلى تحديد العوامل المهمة لتنفيذ استراتيجية الأمن السيبراني في مؤسسات القطاع العام بسلطنة عمان، حيث اتبعت لدراسة المنهج النوعي ، وكانت أداة للدراسة عبارة عن مقابلات شبه منظمة مع (10) مشاركين، وتوصلت الدراسة إلى أن المؤسسات تختلف في طبيعتها الاقتصادية وهذا الاختلاف يجعل الاهتمام بالحفاظ على البيانات مختلفا لتحقيق الأهداف المنشودة، وأوصت الدراسة بضرورة الأخذ بقائمة البحث من حيث تنظيم العوامل وفق القائمة المحددة لتنفيذ إستراتيجية الأمن السيبراني بنجاح في المؤسسات.

2-2-3-التعقيب على الدراسات السابقة

- **أوجه الاتفاق والاختلاف**

من حيث الهدف العام: اتفقت الدراسة الحالية مع أغلب الدراسات السابقة في الهدف العام؛ فقد تناولت جميعها البحث في الأمن السيبراني وأمن المعلومات في الجامعات، ولكن اختلفت عنها بعض الدراسات في المتغيرات الأخرى التي تناولتها كدراسة الداويري (2014)، ودراسة الغيبوي وآخرون (2020)، ودراسة رحمان وآخرون (2015)، ودراسة فينيسا بيرتون (2018)، ودراسة أميولا (2020)، ودراسة نجواتا ووارن وويوهو (0202) ، ودراسة العطيات، والسعود، والدويري (2024).

من حيث العينة: اتفقت هذه الدراسة مع معظم الدراسات السابقة في العينة حيث إن عينتها كانت من موظفي الجامعات وتطابقت معها دراسة السمحان (2020)، أما الدراسات السابقة الأخرى تشابهات معها بأن العينة من موظفي الجامعات، ولكن مع تخصيص وظيفة بعينها وتخصصات معينة من موظفي الجامعات، كدراسة الداويري (2014)، ودراسة الزهراني (2020)، ودراسة فرج (2021)، ودراسة فينيسا بيرتون (2018)، ودراسة أميولا (2020)، ودراسة باولوسكي وجونغ (2015)، ودراسة مورينو، وريفاس، وسوتو، وفيرو (2023)، ودراسة نجواتا ووارن وويوهو (2020)، ودراسة العطيات، والسعود، والدويري (2024)، والهنائي، (2024)، والشكيلي وآخرون (2020)، و دراسة الشكيلي وآخرون (Al-Shukailiyah, 2020).

من حيث المنهج: اتفقت الدراسة الحالية بتوظيفها للمنهج الوصفي مع مجموعة من الدراسات السابقة التي اعتمدت نفس المنهج كدراسة الديراوي (2014) والسمحان (2020) و الغيبوي وآخرون (2020) والزهراني (2020)، و فرج (2021) و دراسة المنيع (2022) ورحمان وآخرون (2015)، بينما اختلفت عنها مجموعة من الدراسات كدراسة القحطاني (2020) ودراسة باولوسكي وجونغ (2015) و دراسة فينيسا بيرتون (2018) ودراسة مورينو، ريفاس، سوتو، وفيرو (2023)، ودراسة أميولا (2020) ودراسة نجواتا ووارن وويوهو (2020) ودراسة العطيات، والسعود، والدويري (2024) فقد استخدمت المنهج النوعي.

من حيث الأداة: اتفقت الدراسة من حيث أداتها مع دراسة الديراوي (2014) والسمحان (2020) والغيبوي وآخرون (2020) والزهراني (2020) ودراسة القحطاني (2020) ودراسة فرج (2021) و دراسة المنيع (2022) ورحمان وآخرون (2015)، ونجواتا ووارن وويوهو (2020) وذلك في أن جميعها وظفت الاستبانة كأداة للدراسة، وجمع البيانات، بينما اختلفت عنها دراسة كل من:

باولوسكي وجونغ (2015)، ودراسة فينيسا بيرتون (2018)، ودراسة أميولا (2020)، ودراسة مورينو، ريفاس، سوتو، وفيرو (2023)، ودراسة العطيات، والسعود، والدويري (2024)، ودراسة دراسة الشكيلي وآخرون (Al-Shukailiyah, 2020).

- **مجالات الاستفادة من الدراسات السابقة:**

استفادت الدراسة الحالية من الدراسات السابقة في اختيار وتحديد المنهج المناسب للدراسة وهو الوصفي التحليلي المسحي المتفق مع هدف الدراسة، كما استفادت منها في تصميم الاستبانة وفق متطلبات الدراسة ومعوقاتها، وبناء مجالات أداة الدراسة.

- **ما يميز هذه الدراسة:**

تميزت هذه الدراسة في أنها استقصت آراء الأكاديميين بالجامعة مع تناولها للمتطلبات والمعوقات معا في الدراسة، ودراسة الفروقات بين أفراد عينة الدراسة من حيث الجنس والرتبة الأكاديمية.

3- منهجية الدراسة وإجراءاتها

3-1-منهج الدراسة

استخدمت الدراسة المنهج الوصفي التحليلي المسحي، وذلك لملاءمته لطبيعة أهداف الدراسة، حيث يصف الظاهرة المراد دراستها من خلال جمع البيانات الكمية أو النوعية ومن ثم تحليل هذه البيانات باستخدام الأساليب الإحصائية المناسبة للوصول إلى استنتاجات قد تسهم في فهم الواقع وتطويره (البادري، 2016).

3-2-مجتمع الدراسة

تكون مجتمع الدراسة من جميع أعضاء هيئة التدريس والموظفين في جامعة نزوى بسلطنة عمان البالغ عددهم (704) فردا؛ وفق إحصائية دائرة الموارد البشرية بجامعة نزوى للعام الحالي 2023-2024 (جامعة نزوى، 2024).

3-3-عينة الدراسة

تم اختيار العينة بالطريقة المتسيرة (المتاحة)، حيث تم استهداف(200) عضو هيئة التدريس وموظفاً ما نسبته (86%) من المجتمع الأصلي، ووصلت حصيلة جمع الاستبانات (186) استبانة، وتمثل (24%) من مجتمع الدراسة، وجميعها صالحه للتحليل الإحصائي، وبالاستعانة بجدول كريجسي ومورجان Krejcie and Morgan (1970) لتحديد حجم العينة الأمثل لعينة الدراسة، أشار الجدول إلى أن (186) أكاديميا وموظفا هو الحجم المناسب، ويوضح الجدول (1) العينة حسب متغير الجنس والرتبة الأكاديمية.

جدول (1) توزيع أفرد العينة حسب متغير الجنس، والرتبة الأكاديمية

المتغيرات	الجنس			المسمى الوظيفي					
				موظف	(أكاديمي) الرتبة الأكاديمية				
	ذكر	أنثى	المجموع		محاضر	أستاذ مساعد	أستاذ مشارك	أستاذ دكتور	المجموع
العدد	142	44	186	20	41	73	40	12	186
النسبة	76.3%	23.7%	%100	%11	%22	%39	%21.5	%6.5	%100

يوضح الجدول (1) التكرار والنسب المئوية حسب متغيري لخصائص عينة الدراسة، غذ بلغت عينة الدراسة (186) أكاديمي وموظف، أغلبهم من الذكور حيث بلغت نسبتهم (76.3%) في حين بلغت نسبة الإناث (23.4%)، وهو ما يعكس طبيعة مجتمع الدراسة حيث نجد أن نسبة الذكور تتفوق على الإناث في جميع مراكز الجامعة، وإدارات، وعمادات، وكليات الجامعة، كما أن طريقة اختيار العينة كانت المتيسرة (المتاحة) وبالتالي الباحثون تركوا الحرية في الاستجابة لأفراد المجتمع.

أما متغير المسمى الوظيفي فتكون من فئتين (موظف – أكاديمي) ويتفرع الأكاديمي إلى أربع مستويات حسب الرتبة الأكاديمية (محاضر، أستاذ مساعد، أستاذ مشارك، أستاذ دكتور)، فيلاحظ أن النسبة الأكبر للمشاركة كانت للأستاذ مساعد حيث بلغت (39%) في حين جاء في الترتيب الثاني محاضر وبنسبة (22%)، وهو ما يعكس مجتمع الدراسة حيث إن جامعة نزوى لازالت فتية لم يمضي عليها مدة طويلة على إنشائها وبالتالي ترتكز أغلب الرتب الأكاديمية في بداية السلم الأكاديمي.

3-4-أداة الدراسة

لتحقيق أهداف الدراسة والإجابة عن أسئلتها تم تطوير استبانة بالاستفادة من الدراسات السابقة التي تناولت موضوع متطلبات تحقيق الأمن السيبراني خصوصاً دراسات (المنيع، 2022؛ توفيق ومرسي، 2022؛ الحداد، 2022)، كما تم الرجوع إلى دليل استخدام تقنية المعلومات والمركز الوطني للأمن السيبراني، وتكونت في صورتها الأولية من جزأين: الأول شمل البيانات الديموغرافية لأفراد عينة الدراسة (الجنس، الرتبة الأكاديمية)، أما الجزء الثاني فتكون من مجالين: 1-متطلبات تحقيق الأمن السيبراني في جامعة نزوى، 2-معوقات تحقيقه وتكونت من (34) عبارة، توزعت على المجالين، كما تم اعتماد مقياس ليكرت الخماسي (مرتفعة جدا، مرتفعة، متوسطة، منخفضة، منخفضة جدا)، لتحديد متطلبات تحقيق الأمن السيبراني، والمعوقات التي تواجهه.

صدق الأداة:

بعد بناء الاستبانة تم احتساب صدقها بطريقتين:

أ- الصدق الظاهري.

تم التأكد من الصدق الظاهري، بعرض الاستبانة في صورتها الأولية على عدد (7) محكمّين من جامعات ومؤسسات تربوية مختلفة بسلطنة عمان من ذوي الخبرة والاختصاص في القياس والتقويم والإدارة التربوية، وتكنولوجيا التعليم، وذلك بهدف أخذ آرائهم وملحوظاتهم بشأن مناسبة عبارات الاستبانة وانتمائها للمجالين، ومناسبة الصياغة اللغوية لكل عبارة ومستوى حاجتها للحذف أو الإضافة بما يتوافق مع أهداف الدراسة.

ونتج عن تحكيم الجزء الثاني الخاص بمتطلبات تحقيق الأمن السيبراني، تعديل صياغة بعض العبارات، (5-7-12). وبناءً على عملية التحكيم أصبحت أداة الدراسة تتكون من محورين، المحور الأول تناول متطلبات تحقيق الأمن السيبراني وله (4) مجالات، والمحور الثاني تناول معوقات تحقيق الأمن السيبراني وله (10) عبارات، كما تم بناء أداة الدراسة وفق سلم ليكرت الخماسي (مرتفعة جدا، مرتفعة، متوسطة، منخفضة، منخفضة جدا)، لتحديد متطلبات تحقيق الأمن السيبراني، والمعوقات التي تواجهه.

ب- صدق الاتساق الداخلي للاستبانة:

تم التحقق من صدق الاتساق الداخلي للاستبانة بحساب معامل الارتباط بيرسون (Pearson)، حيث اختيرت عينة استطلاعية مؤلفة من (40) موظفا من خارج عينة الدراسة، وتم تحليل عبارات الأداة وحساب معامل الارتباط لكل عبارة من العبارات، ويمثل معامل الارتباط هنا دلالة الصدق لكل عبارة بين الدرجة الكلية من جهة، وبين كل عبارة وبين ارتباطها بالمجال التي تنتمي إليه، وبين كل مجال والدرجة الكلية من جهة أخرى. والجدول (2) والجدول (3) يوضحان ذلك.

جدول (2) معامل ارتباط بيرسون بين كل عبارة مع المجال الذي تنتمي إليه ثم بين المجال مع المحور

المحور الأول: متطلبات تطبيق الأمن السيبراني								المحور الثاني: معوقات تحقيق الأمن السيبراني	
المجال الأول (التقنية)		المجال2(المادية)		المجال3 (البشرية)		المجال4(التقنية)			
العبارة	الارتباط	العبارة	الارتباط	العبارة	الارتباط	العبارة	الارتباط	العبارة	الارتباط
1	0.69*	8	0.87*	14	0.86*	19	0.93*	1	0.85*
2	0.45*	9	0.62*	15	0.68*	20	0.34*	2	0.79*
3	0.20*	10	0.24*	16	0.68*	21	0.55*	3	0.61*
4	0.20*	11	0.30*	17	0.45*	22	0.20*	4	0.54*
5	0.36*	12	0.52*	18	0.87*	23	0.46*	4	0.49*
6	0.22*	13	0.84*			24	0.82*	5	0.65*
7	0.81*							6	0.57*
ارتباط المجال1		ارتباط المجال2		ارتباط المجال3		ارتباط المجال4		7	0.51*
								مجال المعوقات	

*** دالة عند مستوى ($\alpha \leq 0.05$)**

يوضح جدول (2) أن جميع العبارات ترتبط بالمجال الذي تندرج تحته ارتباطا قويا، حيث كانت معاملات ارتباط العبارات متقاربة وجميعها أكثر من (0.20)، وتراوحت ما بين (0.22–0.93) وبالتالي يمكن اعتبار عبارات المقياس صادقة وصالحة لما وضعت لقياسه. كما تم استخراج معامل ارتباط البُعد بالدرجة الكلية، ومعاملات الارتباط بين الأبعاد ببعضها والجدول (3) يُبَيِّنُ ذلك.

الجدول (3) معاملات الارتباط بين الأبعاد ببعضها وبالدرجة الكلية في محور متطلبات تحقيق الأمن السيبراني

	متطلبات التقنية	متطلبات المادية	متطلبات البشرية	متطلبات معرفية
متطلبات التقنية	1			
متطلبات المادية	.430(**)	1		
متطلبات البشرية	.395 (**)	.575 (**)	1	
متطلبات معرفية	.180(**)	.438 (**)	.614(**)	1

** دالة إحصائيا عند مستوى الدلالة (0.05). * دالة إحصائيا عند مستوى الدلالة (0.01).

يتَّضِحُ من الجداول (3) أَنَّ معامل الارتباطات البينيَّة بين المجالات ببعضها وبالدرجة الكلية: كانت دالَّةً إحصائيا عند مستوى دلالة (0.05)، إِذْ تتَّصِفُ بمعامل ارتباط مرتفع ودالٍ إحصائيا ومناسبٍ لأهداف الدراسة الحالية

الثبات: لأغراض التحقق من صدق البناء الداخلي لأداة الدراسة ومجالاتها، احتسبت معاملات الارتباط بين مجالات الدراسة من جهة، وبين أداة الدراسة ببعضها، والجدول (4) يوضح ذلك.

جدول (4) قيم معاملات ألفا لكرو نباخ للمجالات والمقياس ككل

المحور	المجالات	عدد العبارات	ألفا كرو نباخ
المحور الأول: متطلبات تحقيق الأمن السيبراني	متطلبات تقنية	7-1	0.69
	متطلبات مادية	13-8	0.71
	متطلبات بشرية	18-14	0.83
	متطلبات معرفية	24-19	0.84
المحور ككل		24	0.83
المحور الثاني: معوقات تحقيق الأمن السيبراني		7-1	0.92
المقياس ككل		31	0.83

يلاحظ من جدول (4) أن معامل ألفا كرونباخ لمحور متطلبات تحقيق الأمن السيبراني ككل بلغ (0.83) وهي تمثل قيمة ثبات عالية جدا، وتراوحت معاملات الثبات بالنسبة لمجالات محور متطلبات تحقيق الأمن السيبراني بين (0.69– 0.84). بينما بلغ معامل ألفاكرونباخ لمحور معوقات تحقيق الأمن السيبراني (0.92)، وهي أيضا قيم ذات درجة مناسبة من الثبات في العلوم الإنسانية، ومؤشر على مدى الاتساق الداخلي لمجالات المقياس، ومما تقدم يتضح أن دلالات الصدق والثبات لأداة الدراسة مناسبة للتطبيق النهائي على العينة المستهدفة.

معيار الحكم على النتائج:

وفقاً لسلم ليكرت الخماسي تمت الإجابة على محاور أداة الدراسة، بإعطاء كل عبارة من عباراته درجة واحدة "مرتفع جدًا (5)، مرتفع (4)، متوسط (3)، منخفض (2)، منخفض جداً (1)"، وتم حساب طول الفئة بالطريقة التالية، حيث تم حساب المدى بطرح القيمة الدنيا من القيمة العليا(5-1=4)، وللحصول على طول الفئة تم قسمة المدى على عدد المستويات (4÷5=0.8)، ثم تمت إضافة قيمة طول الفئة إلى أقل قيمة في المعيار وهي (1) لتحديد الحد الأعلى من الفئة الأولى (0.8+1=1.8)، ثم على هذا النسق تم إيجاد باقي القيم، لتحديد كافة مستويات الاستبانة، وفق المعادلة الرياضية الآتية:

$$\text{طول الفئة} = \frac{\text{أكبر قيمة} - \text{أصغر قيمة}}{\text{عدد المستويات}} = \frac{5-1}{5} = 0.8$$

وبالتالي تم اعتماد المقياس الموضح بالجدول (5) للحكم على المتوسطات الحسابية لعبارات الاستبانة وتحليل النتائج.

جدول (5) معيار الحكم على استجابات عبارات الاستبانة حسب مدى المتوسط الحسابي

الترميز	مدى المتوسط الحسابي	المدى
1	1.80-1.00	منخفض جدًا
2	2.60 –1.81	منخفض
3	3.40 –2.61	متوسط
4	4.20 – 3.41	مرتفع
5	5,00– 4.21	مرتفع جدًا

المعالجة الإحصائية

اعتمدت هذه الدراسة على برنامج الرزمة الإحصائية للعلوم الاجتماعية (SPSS)، لاستخراج نتائج الدراسة والإجابة عن أسئلتها، كما يأتي:

1. معادلة ألفا كرونباخ (Alpha Cronbach)، ومعاملات ارتباط بيرسون (Pearson) لحساب صدق وثبات أداة الدراسة.
2. للإجابة عن السؤال الثالث استخدم الباحثون اختبار (ت) (T-test Independent) للعينات المستقلة من أجل معرفة ما إذا كانت هناك فروق ذات دلالة إحصائية في استجابات أفراد عينة الدراسة حول متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 من وجهة أكاديمي وموظفي جامعة نزوى تعزى لمتغير (الجنس)، كما تم استخدام اختبار(ANOVA) لمعرفة ما إذا كانت توجد فروق ذات دلالة إحصائية في استجابات أفراد عينة الدراسة حول متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 من وجهة أكاديمي وموظفي جامعة نزوى تعزى لمتغير الدراسة (الرتبة الأكاديمية).
3. المتوسطات الحسابية والانحرافات المعيارية للإجابة عن السؤالين الأول والثاني.

4- نتائج الدراسة ومناقشتها

4-1-نتيجة الإجابة عن السؤال الأول: "ما متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين؟

وللإجابة عن السؤال تم استخراج المتوسطات الحسابية والانحرافات المعيارية لكل بعد من أبعاد المقياس والدرجة الكلية ويوضح الجدول (6) نتائج السؤال الأول.

جدول (6) متوسطات متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040

م	المجالات	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة المتطلب
2	متطلبات تقنية	2.16	0.61	1	منخفضة
4	متطلبات معرفية	2.02	0.51	2	منخفضة
3	متطلبات بشرية	2.01	0.76	3	منخفضة
1	متطلبات مادية	1.89	0.48	4	منخفضة
	المتوسط الكلي	2.04	0.58		منخفضة

تظهر قيم المتوسطات بجدول (6) أن متوسط الاستجابة للمقياس الكلي لمتطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 من وجهة أكاديمي وموظفي جامعة نزوى بلغ (2.04)، بانحراف معياري (0.58)، وهو منخفض، كذلك جاءت سائر الأبعاد منخفضة حيث تراوحت قيم متوسطات الاستجابة فيها بين (1.89-2.16)، وبانحرافات معيارية متقاربة، وكلها تشير إلى انخفاض المتطلبات لدى عينة الدراسة، وجاء في الرتبة الأولى المتطلبات التقنية بدرجة منخفضة وبمتوسط حسابي بلغ (2.16) وانحراف معياري بلغ (0.61)، ويليه في الرتبة الثانية المتطلبات المعرفية بدرجة منخفضة وبمتوسط حسابي بلغ (2.02)، وانحراف معياري بلغ (0.51). وجاء في الرتبة الثالثة المتطلبات البشرية بدرجة منخفضة وبمتوسط حسابي بلغ (2.01) وانحراف معياري بلغ (0.76)، وفي الرتبة الأخيرة جاء مجال المتطلبات الفنية، بدرجة منخفضة وبمتوسط حسابي بلغ (1.89) وانحراف معياري بلغ (0.48).

وقد يعزى حصول المحور الأول متطلبات تطبيق الأمن السيبراني بدرجة منخفضة إلى أن الجامعة توفر خوادم (سيرفرات) خاصة بها، كذلك تهتم بعمل نسخ احتياطية للملفات بشكل دوري، أيضا تلتزم الجامعة بفحص الملفات التي يتم تحميلها من المواقع غير المعروفة أو خدمات مشاركة الملفات الواردة عن طريق البريد الالكتروني الجامعي، بالإضافة إلى أن الجامعة توفر برامج حديثة لتدريب الهيئة التدريسية على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم، مع سعي الجامعة إلى تنمية وعي الطلبة بثقافة الأمن السيبراني من خلال منشورات وتعاميم، وتوفر الجامعة مناهج جديدة لمواكبة الثورة التكنولوجية والتحول الرقمي بما يتوافق مع المعايير الوطنية والدولية، وكذلك حرص الجامعة على عدم إرسال أية معلومات حساسة مثل كلمات المرور وأرقام بطاقات الائتمان عبر البريد الإلكتروني.

وتتفق نتيجة هذه الدراسة مع دراسة السمحان (2020)، التي بينت أن من أهم المتطلبات لتحقيق الأمن السيبراني تتمثل في إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في المملكة، وتشجيع الاستثمار في مجال الأمن السيبراني، ودراسة أميولا (Omoyiola 2020) التي خلصت نتائجها أن قادة الأمن السيبراني يقومون بمنع الاختراقات الأمنية في مؤسساتهم بفرض سياسات الأمن

السيبراني بدرجة عالية، ودراسة باولوسكي وجونغ (2015)، التي خلصت نتائجها أن التهديدات المحتملة للأمن السيبراني للبنية التحتية الحيوية الوطنية لا تمثل إلا في حدها الأدنى. وفحص الاستطلاع، ودراسة مورينو، وريفاس، وسوتو، وفيرو (2023)، وتختلف هذه النتيجة مع دراسة الديراوي (2014)، ودراسة نجواتا ووارن وويوهو (Nagahawatta, et al., 2018) ودراسة، فينيسا بيرتون (Burton-Howard,2018)، ودراسة رحمان وآخرون (Rehman et al, 2015)، ودراسة المنيع (2022)، ودراسة فرج (2021)، التي بينت أنه من الضرورة الملحة تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي الجامعات.

مجال: المتطلبات التقنية

الجدول(7) المتوسطات والانحرافات المعيارية المتعلقة بمجال المتطلبات التقنية مرتبة تنازليا.

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة المتطلب
.7	تمتلك الجامعة برامج حديثة لحماية الهوية الرقمية مثل برنامج (المواطنة الرقمية).	2.41	0.85	1	منخفضة
.2	تهتم الجامعة بعمل نسخ احتياطية للملفات بشكل دوري.	2.10	0.82	2	منخفضة
.3	تلتزم الجامعة بفحص الملفات التي يتم تحميلها من المواقع عير المعروفة أو خدمات مشاركة الملفات الواردة عن طريق البريد الالكتروني الجامعي.	2.01	0.72	3	منخفضة
.4	تحرص الجامعة على عدم ارسال أية معلومات حساسة مثل كلمات المرور وأرقام بطاقات الائتمان عبر البريد الالكتروني.	1.91	0.75	4	منخفضة
.1	يتوفر لدى الجامعة خوادم (سيرفرات) خاصة بها.	1.74	0.61	6	منخفضة جدا
.5	تسعى الجامعة لتطبيق التحول الرقمي في كل مدخلات الجامعة.	1.72	0.62	5	منخفضة جدا
.6	تؤكد الجامعة على ضرورة استخدام كلمة مرور قوية ومعقدة لا يمكن تحمينها للوصول إليها وتغيرها من وقت لآخر	1.71	0.70	7	منخفضة جدا
	متطلبات تقنية	2.16	0.61	منخفضة	

يبين الجدول (7) حصول المتطلبات التقنية على درجة منخفضة بمتوسط حسابي (2.16)، وانحراف معياري (0.61)، حيث حصلت جميع فقرات المتطلب على درجة منخفضة، وتراوح المتوسط الحسابي للفقرات ما بين (2.41-1.71). وجاءت في الرتبة الأولى الفقرة (7) بمتوسط حسابي (2.41)، وجاءت في الرتبة الأخيرة الفقرة (6) وبمتوسط حسابي (1.71).

وقد يفسر مجيء مجال المتطلبات التقنية في الرتبة الأولى على الرغم من حصول المجال على درجة منخفضة من المتطلبات إلا أنه جاء كأكثر المتطلبات ضرورة، كما يراها أفراد عينة الدراسة، وقد يعزى ذلك إلى اهتمام الجامعة بعمل نسخ احتياطية للملفات بشكل دوري، مع ضرورة مواكبة ما يتعلق بالبرامج الحديثة المستخدمة في التخزين السحابي، وضرورة تنويعها، مع الالتزام بفحص الملفات من قبل المعنيين قبل تحميلها، وخاصة تلك التي يتم تنزيلها من مواقع غير معروفة أو غير آمنة، كما قد يعزى إلى قيام الجامعة بحملات توعوية للموظفين والأكاديميين تبين ضرورة تجنب مشاركة الملفات الواردة عن طريق البريد الالكتروني الجامعي، وتنبيه الجامعة على عدم إرسال أية معلومات حساسة مثل كلمات المرور وأرقام بطاقات الائتمان عبر البريد الالكتروني، بالإضافة إلى سعي الجامعة لتطبيق التحول الرقمي في كل مدخلات الجامعة، كذلك امتلاك الجامعة برامج حديثة لحماية الهوية الرقمية مثل برنامج (المواطنة الرقمية).وتتفق نتيجة هذه الدراسة مع دراسة دراسة أميولا (Omoyiola 2020)، ودراسة مورينو وريغا وسوتو ريغا فيرو (2023)، وتختلف هذه النتيجة مع دراسة دراسة فينيسا بيرتون (Burton-Howard,2018)، ودراسة رحمان وآخرون (Rehman et al, 2015)، ودراسة نجواتا ووارن وويوهو (Nagahawatta, et al., 2018)، ودراسة باولوسكي وجونغ (2015)، ودراسة القحطاني (2020)، ودراسة الزهراني (2020).

مجال: المتطلبات المعرفية

الجدول(8) المتوسطات والانحرافات المعيارية المتعلقة بمجال المتطلبات المعرفية مرتبة تنازليا.

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة المتطلب
.22	توضح الجامعة لأعضاء هيئة التدريس إيجابيات ثقافة الأمن السيبراني خصوصا في مضامينها المستقبلية على المجتمعات.	2.21	0.91	1	منخفضة
.23	تضع الجامعة استراتيجيات لدمج وتضمين الموضوعات الخاصة بثقافة الأمن السيبراني في بعض المناهج والمقررات الدراسية بالجامعة.	2.10	1.01	2	منخفضة
21	توفر الجامعة مناهج جديدة لمواكبة الثورة التكنولوجية والتحول الرقمي بما يتوافق مع المعايير الوطنية والدولية.	2.02	1.01	3	منخفضة
.20	تسعى الجامعة إلى تنمية وعي الطلبة بثقافة الأمن السيبراني من خلال منشورات وتعميمات.	2.01	0.92	4	منخفضة
24	تعمل الجامعة على تطوير الإطار التشريعي الملائم لأمن الفضاء السيبراني وحماية الخصوصية والهوية الرقمية..	1.92	0.93	5	منخفضة
	متطلبات معرفية	2.01	0.51		منخفضة

يبين الجدول (8) حصول المتطلبات المعرفية على درجة منخفضة بمتوسط حسابي (2.01)، وانحراف معياري (0.51)، حيث حصلت جميع فقرات المتطلب على درجة منخفضة، وتراوح المتوسط الحسابي للفقرات ما بين (2.21-1.92). وجاءت في الرتبة الأولى الفقرة (22) بمتوسط حسابي (2.21)، وجاءت في الرتبة الأخيرة الفقرة (24) وبمتوسط حسابي (1.92).

وقد يعزى مجيئ مجال المتطلبات المعرفية في الرتبة الثانية إلى سعي الجامعة إلى تنمية وعي الطلبة بثقافة الأمن السيبراني من خلال النشرات والتعاميم، وتوفيرها لمناهج جديدة لمواكبة الثورة التكنولوجية والتحول الرقمي بما يتوافق مع المعايير الوطنية والدولية، كذلك توضح الجامعة لأعضاء هيئة التدريس إيجابيات ثقافة الأمن السيبراني خصوصا في مضامينها المستقبلية على المجتمعات، وتضع الجامعة استراتيجيات لدمج وتضمين الموضوعات الخاصة بثقافة الأمن السيبراني في بعض المناهج والمقررات الدراسية بالجامعة، وتعمل الجامعة على تطوير الإطار التشريعي الملائم لأمن الفضاء السيبراني وحماية الخصوصية والهوية الرقمية، وتتفق نتيجة هذه الدراسة مع دراسة أميولا (Omoyiola 2020)، ودراسة مورينو، ريفاس، سوتو، وفيرو (2023) وتختلف هذه النتيجة مع دراسة دراسة فينيسا بيرتون (Burton-Howard,2018)، ودراسة رحمان وآخرون (Rehman et al, 2015)، ودراسة نجواتا ووارن وويوهو (Nagahawatta, et al., 2018)، دراسة باولوسكي وجونغ (2015)، ودراسة القحطاني (2020)، دراسة الزهراني (2020).

مجال: المتطلبات بشرية

الجدول(9) المتوسطات والانحرافات المعيارية المتعلقة بمجال المتطلبات بشرية مرتبة تنازليا.

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة المتطلب
.17	تؤهل الجامعة الموارد البشرية القائمة على تقنية أمن المعلومات في مجال تطبيق الأمن السيبراني	2.41	1.10	1	منخفضة
.19	تهتم الجامعة بالعناصر البشرية ذات الكفاءة العالية والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة.	2.13	0.90	2	منخفضة
16	تحرص الجامعة على وضع استراتيجيات في خطتها الاستراتيجية للمساعدة في الحد من الجرائم الالكترونية وتعزيز الأمن السيبراني.	2.02	1.01	3	منخفضة
18	تدعم الجامعة مهارات أعضاء هيئة التدريس في مجال الأمن السيبراني من خلال عقد دورات تدريبية مختصة في استخدام كافة الوسائل التقنية بطرق آمنة.	1.91	1.03	4	منخفضة

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة المتطلب
15	تقوم الجامعة بتوعية أعضاء هيئة التدريس بمخاطر إرسال المعلومات الشخصية عبر الرسائل النصية أو البريد الالكتروني.	1.81	0.91	5	منخفضة
	متطلبات بشرية	2.01	0.76		منخفضة

يبين الجدول (9) حصول المتطلبات بشرية على درجة منخفضة بمتوسط حسابي (2.01)، وانحراف معياري (0.76)، حيث حصلت جميع فقرات المتطلب على درجة منخفضة، وتراوح المتوسط الحسابي للفقرات ما بين (1.81-2.41). وجاءت في الرتبة الأولى الفقرة (17) بمتوسط حسابي (2.41)، وجاءت في الرتبة الأخيرة الفقرة (15) وبمتوسط حسابي (1.81).

وقد يعلل مجيء مجال المتطلبات البشرية إلى أنه من المتطلبات اللازمة لتحقيق الأمن السيبراني في جامعة نزوى، وجاء كذلك بدرجة منخفضة ضمن المتطلبات، وقد يعود ذلك إلى أن الجامعة تقوم بجهود توعوية تشمل الموظفين بشكل عام وأعضاء هيئة التدريس بشكل خاص، تتناول المخاطر المحتملة عند التعامل الالكتروني بمختلف أنواعه ومستوياته، كما قد يعزى إلى حرص الجامعة على وضع استراتيجيات في خطتها الاستراتيجية للمساعدة في الحد من الجرائم الإلكترونية وتعزيز الأمن السيبراني، ولربما يعود ذلك إلى وجود كوادر بشرية مؤهلة قائمة على تقنية أمن المعلومات في مجال تطبيق الأمن السيبراني، وتتفق نتيجة هذه الدراسة مع دراسة أميولا (Omoyiola 2020)، ودراسة باولوسكي وجونغ (2015)، وتختلف هذه الدراسة مع دراسة دراسة مورينو، ريفاس، سوتو، وفيرو (2023).

مجال: المتطلبات المادية

الجدول(10) المتوسطات والانحرافات المعيارية المتعلقة بمجال المتطلبات المادية مرتبة تنازليا.

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة المتطلب
.12	تسعى الجامعة لتطبيق التحول الرقمي في كل مدخلات الجامعة.	2.81	1.02	1	متوسطة
8	يتوفر لدى الجامعة خوادم (سيرفرات) خاصة بها.	2.40	1.10	2	منخفضة
.13	تؤكد الجامعة على ضرورة استخدام كلمة مرور قوية ومعقدة لا يمكن تحميها للوصول إليها وتغيرها من وقت لآخر.	2.21	1.02	3	منخفضة
11	تحرص الجامعة على عدم ارسال أية معلومات حساسة مثل كلمات المرور وأرقام بطاقات الائتمان عبر البريد الالكتروني.	2.03	0.90	4	منخفضة
14	تمتلك الجامعة برامج حديثة لحماية الهوية الرقمية مثل برنامج (المواطنة الرقمية).	2.02	0.93	5	منخفضة
.10	تلتزم الجامعة بفحص الملفات التي يتم تحميلها من المواقع عير المعروفة أو خدمات مشاركة الملفات الواردة عن طريق البريد الالكتروني الجامعي.	2.01	0.91	3	منخفضة
9	تهتم الجامعة بعمل نسخ احتياطية للملفات بشكل دوري.	1.82	0.82	6	منخفضة
	متطلبات مادية	1.89	0.48		منخفضة

يبين الجدول (10) حصول المتطلبات المادية على درجة منخفضة بمتوسط حسابي (1.89)، وانحراف معياري (0.48)، حيث حصلت فقرات المتطلب على درجة(متوسطة – منخفضة)، وتراوح المتوسط الحسابي للفقرات ما بين (1.82-2.81). وجاءت في الرتبة الأولى الفقرة (12) بمتوسط حسابي (2.81)، وجاءت في الرتبة الأخيرة الفقرة (9) وبمتوسط حسابي (1.82).

وقد يعزى مجيء المتطلبات المادية في الرتبة الأخيرة إلى حرص الجامعة على توفير كافة المتطلبات اللازمة على تحقيق الأمن السيبراني، وحماية البرامج والأجهزة من الاختراق، مما يدفع الجامعة على توفير الميزانية من أجل تحديث برامجها بشكل مستمر ، كما تعمل تقنية المعلومات على إجراء الفحص والصيانة الدورية وتغيير كلمة المرور بشكل دوري. وتتفق هذه الدراسة مع دراسة أميولا (Omoyiola 2020)، ودراسة باولوسكي وجونغ (2015) التي توصلت إلى ضرورة توفير متطلبات الحماية للبرامج والأجهزة الجامعية.

2-4-نتيجة الإجابة عن السؤال الثاني: ما معوقات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين؟

وتمت الإجابة عن السؤال باستخراج المتوسطات الحسابية والانحرافات المعيارية لكل بعد من أبعاد المقياس والدرجة الكلية ويوضح الجدول (11) نتائج السؤال الثاني

جدول (11) متوسطات معوقات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040

م	الفقرات	المتوسط الحسابي	الانحراف المعياري	الرتبة	درجة المعوقات
.10	ضعف آليات حماية البنية التحتية السيبرانية والأجهزة والشبكات المعلوماتية في الجامعات العمانية.	2.91	1.07	1	متوسطة
.7	ضعف التعاون بين موظفي التقنيات في الجامعة لتحقيق الأمن السيبراني.	2.81	1.11	2	متوسطة
.5	ضعف تطبيق معايير حوكمة المعلومات..	2.80	1.14	3	متوسطة
.9	غياب تطبيق التشريعات والقوانين الرادعة لمرتكبي الجرائم الإلكترونية.	2.80	1.13	4	متوسطة
.4	عدم تحديد صلاحيات ومسؤوليات للوصول لكل فرد.	2.78	1.16	5	متوسطة
.6	قلة الدورات التدريبية المنعقدة لموظفي التقنيات وقادتهم في الأمن السيبراني..	2.63	1.04	6	متوسطة
.3	تدني مستوى الخبرة لدى الموظفين.	2.59	1.26	7	متوسطة
.8	استخدام الأجهزة الشخصية مثل الهاتف المحمولة لتخزين ونقل معلومات سرية خاصة بالجامعة.	2.56	1.19	8	متوسطة
.1	قلة البرامج والسياسات المحددة لأمن الجامعة.	2.54	1.16	9	منخفضة
.2	قلة كفاية الحماية ضد برامج الاختراقات الحديثة	2.34	1.18	10	منخفضة
	المتوسط الكلي	2.67	0.89		متوسطة

يلاحظ من جدول (11) أن متوسط الاستجابة للمقياس الكلي لمعوقات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2040 من وجهة أكاديمي وموظفي جامعة نزوى بلغ (2.67)، بانحراف معياري (0.89)، وهو بدرجة متوسطة، وجاءت عبارات المقياس بين درجتي (منخفضة ومتوسطة) حيث تراوحت قيم متوسطات الاستجابة فيها بين (2.34-2.91)، وبانحرافات معيارية متقاربة تراوحت بين (1.04-1.26)، حيث جاءت العبارات ذوات الأرقام من (3-10) بدرجة متوسطة وجاءت الفقرتان (1، 2) بدرجة منخفضة. وجاء في الرتبة الأولى الفقرة (10) والتي نصها "ضعف آليات حماية البنية التحتية السيبرانية والأجهزة والشبكات المعلوماتية في الجامعات العمانية" بدرجة متوسطة كذلك وبمتوسط حسابي بلغ (2.91)، وانحراف معياري بلغ (1.07)، ويليه في الرتبة الثانية الفقرة (4) والتي نصت على: "عدم تحديد صلاحيات ومسؤوليات للوصول لكل فرد" بدرجة متوسطة وبمتوسط حسابي بلغ (2.81)، وانحراف معياري بلغ (1.11). وجاءت في الرتبة الأخيرة الفقرة (2) ونصت على "قلة كفاية الحماية ضد برامج الاختراقات الحديثة " بدرجة منخفضة وبمتوسط حسابي بلغ (2.34)، وانحراف معياري بلغ (1.18).

وقد يعزى حصول المحور الثاني معوقات تحقيق الأمن السيبراني بدرجة متوسطة إلى قلة كفاية الحماية ضد برامج الاختراقات الحديثة، أو لربما ضعف تطبيق معايير حوكمة المعلومات، وقد يكون قلة الدورات التدريبية المنعقدة لموظفي التقنيات وقادتهم في الأمن السيبراني، وتدني مستوى الخبرة لدى الموظفين في الجامعة. وتتفق نتيجة هذه الدراسة مع دراسة المنيع (2022)، ودراسة فرج (2021) ، ودراسة دراسة الزهراني (2020) ، ودراسة الغيبوي وآخرون (2020) ، وتختلف هذه النتيجة مع دراسة فينيسا بيرتون (Burton-Howard, 2018)، ودراسة رحمان وآخرون (Rehman et al, 2015).

وقد يفسر مجيء الفقرة (10) والتي نصها " ضعف آليات حماية البنية التحتية السيبرانية والأجهزة والشبكات المعلوماتية في الجامعات العمانية" في الرتبة الأولى إلى أنه لربما قد يعود إلى نقص الوعي والتثقيف بأهمية الأمن السيبراني وهذا قد يؤدي إلى سلوكيات غير آمنة، أو يكون قلة في الموارد المالية أو إلى أن بعض الجامعات تعتمد على الأنظمة القديمة التي يسهل تعرضها للاختراقات والثغرات الأمنية. وتتفق نتيجة هذه الدراسة مع دراسة نجواتا ووارن وويوهو (Nagahawatta, et al., 2018)، وتختلف هذه النتيجة مع دراسة أميولا (Omoyiola،2020).

وقد يفسر مجيء الفقرة (7) والتي نصها " ضعف التعاون بين موظفي التقنيات في الجامعات لتحقيق الأمن السيبراني." في الرتبة الثانية إلى ربما الضغط الشديد للمهام المتعددة الموكلة إليهم، أو قد يكون السبب في تفكيرهم للأهداف بشكل فردي بدلا من التفكير بالأهداف الجماعية، أو لربما يعزى إلى تفاوت الخبرات والمعرفة بين موظفي التقنيات أو قد يكون عدم وجود سياسات واضحة تحفز التعاون بينهم وكيفية العمل معا لتحقيق الأمن السيبراني. وتتفق نتيجة هذه الدراسة مع دراسة المنيع (2022) وتختلف مع دراسة أميولا (Omoyiola 2020).

وقد يعزى مجيء الفقرة (2) والتي نصها "قلة كفاية الحماية ضد برامج الاختراقات الحديثة" في الرتبة الأخيرة إلى ربما افتقار البعض إلى الاهتمام بالمراقبة المستمرة والتحليل الأمني لاكتشاف التهديدات المحتملة، أو إلى تحديات البنية التحتية كنقص الأجهزة وضعف الشبكات، أو قد يعود إلى تزايد الهجمات الحديثة وأساليب الاختراقات المتطورة مما يؤدي إلى ضعف في استراتيجيات الحماية.

وتتفق نتيجة هذه الدراسة مع دراسة أميولا (Omoyiola, 2020) وتختلف مع نتيجة دراسة فينيسا بيرتون (Burton-Howard, 2018).

3-4-نتيجة الإجابة عن السؤال الثالث: ما مدى وجود فروق دالة إحصائيا عند مستوى (α≤0.05) في تقديرات أفراد عينة الدراسة حول متطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2024 ومعوقاته من وجهة نظر الأكاديميين والموظفين تعزى لمتغيري (الجنس، والرتبة الأكاديمية)؟

للإجابة عن هذا السؤال تم استخراج المتوسطات الحسابية والانحرافات المعيارية لمتطلبات تحقيق الأمن السيبراني في جامعة نزوى وفق رؤية عمان 2024 ومعوقاته من وجهة نظر الأكاديميين والموظفين حسب متغيري الدراسة (الجنس، والرتبة الأكاديمية)، ولبيان الفروق الإحصائية بين المتوسطات الحسابية تم استخدام اختبار "ت" للجنس، وتحليل التبين الاحادي(ANOVA) تبعا لمتغير الرتبة الأكاديمية، وفق الجدولين (12) و(13) الآتيين:

3-1- فحص أثر متغير الجنس

جدول (12) نتائج اختبار (t-test) لدلالة الفروق الإحصائية بين استجابات أفراد العينة لمتطلبات تحقيق الأمن السيبراني تبعا لمتغير الجنس

المتطلبات	الجنس	العدد	المتوسطات الحسابية	الانحرافات المعيارية	درجات الحرية	فيمة (T)	مستوى الدلالة	اتجاه الدلالة
الفنية	ذكور	142	1.9	0.47	184	1.27-	0.205	غير دال إحصائيا
	إناث	44	2	0.41				
التقنية	ذكور	142	2.3	0.56	184	3.48	0.001	دال إحصائيا
	إناث	44	1.9	0.68				
البشرية	ذكور	142	1.9	0.71	184	0.43-	0.665	غير دال إحصائيا
	إناث	44	2.1	0.93				
المعرفية	ذكور	142	2.1	0.68	184	0.96-	0.337	غير دال إحصائيا
	إناث	44	2.2	0.79				
الكلي	ذكور	142	2.1	0.49	184	0.26	0.796	غير دال إحصائيا
	إناث	44	2	0.63				

يوضح الجدول (12) عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (α≤0.05) بين متوسطات تقديرات أفراد عينة الدراسة لمتطلبات تحقيق الأمن السيبراني في ضوء رؤية عمان 2040 تبعا لمتغير الجنس في جميع المجالات، والدرجة الكلية، بينما توجد فروق دالة إحصائيا في مجال المتطلبات التقنية ولصالح الذكو وقد يعزى ذلك إلى اهتمام الذكور بالجانب التقني وحرصهم على مواكبة البرامج والمستجدات في مجال الأمن الرقمي، كما أنهم لا يثقون في كثير من البرامج والرسائل الاحتيالية التي تحمل إغراءات مادية مما يترتب عليها الحصول على المعلومات والبيانات الشخصية في حالة الاستجابة لمطالب المرسل، ولربما يغلب على الذكور البعد عن العاطفة والرغبة في الحصول على جدار حماية للأجهزة والأدوات التقنية. وتتفق نتائج هذه الدراسة مع دراسة نجواتا ووارن وويوهو (Nagahawatta, et al., 2018)

2-3- فحص أثر متغير الرتبة الأكاديمية

جدول (13) نتائج اختبار(ANOVA) لدلالة الفروق الفردية بين استجابات أفراد العينة لمتطلبات تحقيق الأمن السيبراني تبعا لمتغير الرتبة الأكاديمية

المتطلبات	مصدر التباين	مجموع المربعات	درجات الحرية	متوسطات المربعات	فيمة (F)	مستوى الدلالة	اتجاه الدلالة
الفنية	بين المجموعات	0.72	4	0.18	0.85	0.494	غير دال إحصائيا
	داخل المجموعات	38.30	181	0.212			
	المجموع	39.03	185				
التقنية	بين المجموعات	0.99	4	0.25	0.64	0.633	غير دال إحصائيا
	داخل المجموعات	69.92	181	0.39			
	المجموع	70.92	185				
البشرية	بين المجموعات	1.79	4	0.45	0.76	0.549	غير دال إحصائيا
	داخل المجموعات	106.11	181	0.59			
	المجموع	108	185				
المعرفية	بين المجموعات	7.66	4	1.92	4.17	0.004	غير دال إحصائيا
	داخل المجموعات	85.24	181	0.47			
	المجموع	93	185				

يتبين من الجدول (13) عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لمتوسطات تقديرات أفراد العينة، لتحقيق متطلبات الأمن السيبراني في ضوء رؤية عمان 2040 تبعا لمتغير الرتبة الأكاديمية، في جميع المجالات والدرجة الكلية، لأن القيمة الاحتمالية (p-) أكبر من (0.05)، مما يشير إلى اتفاق عينة الدراسة، وقد يعزى ذلك إلى أن جميع هذه المتطلبات التي أوردتها الدراسة ذات أهمية بالنسبة للأكاديميين والموظفين على حد سواء بغض النظر عن رتبهم الأكاديمية ومستوياتهم الإدارية مما يدلل على اتفاقهم نحو قيام جامعة نزوى بتوفر هذه المتطلبات وتسخير جميع الامكانيات لضمان توفرها في البيئة الجامعية، واتفقت هذه النتيجة مع دِرَاسَة الديراوي (2014)، ودراسة فرج (2021).

التوصيات والمقترحات

بناء على نتائج الدراسة، يوصي الباحثون بما يأتي:

1. استمرار الجامعة بتوعية جميع العاملين بكيفية تحقيق متطلبات الأمن السيبراني في التعاملات الإلكترونية العامة منها والشخصية بأجهزتهم الشخصية.
2. على رئاسة الجامعة الاستمرار في توفير العناصر البشرية ذات الكفاءة العالية والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة .
3. قيام المسؤولين بالجامعة في منح الجوائز المادية والمعنوية للمتميزين والمبدعين من أعضاء هيئة التدريس في مجال الأمن السيبراني.
4. على الجامعة توفير المخصصات المالية اللازمة لتحقيق الأمن السيبراني.
5. على الجامعة الاستمرار في دعم وتدريب مهارات أعضاء هيئة التدريس في مجال الأمن السيبراني من خلال عقد دورات تدريبية مختصة في استخدام كافة الوسائل التقنية بطرق آمنة.

6. المقترحات لدراسات تربوية

أ- دراسة حول واقع استخدام الأمن السيبراني في الجامعات العمانية الخاصة.

ب- دراسة مقارنة بين واقع تطبيق متطلبات الأمن السيبراني في الجامعات العمانية الخاصة والجامعات الأوربية الخاصة.

قائمة المراجع

أولا: المراجع العربية

- إبراهيم، فاطمة، ويوسف، رحاب، وعيد، وليد. (2022). الأمن السيبراني والنظافة الرقمية. المجلة المصرية لعلوم المعلومات، 9(2)، 230-422. https://doi.org/10.21608/jesi.2022.166729.1066
- جامعة نزوى. (2024 أ). عن الجامعة. جامعة نزوى. https://www.unizwa.edu.om /
- جامعة نزوى. (2024 ب). كلية الاقتصاد ونظم المعلومات. جامعة نزوى. https://www.unizwa.edu.om /
- الحداد، نبيلة محمد، والصباحي، عبده طاهر. (2021). آليات تطوير تقنيات البحث في العلوم الإنسانية والاجتماعية. وقائع المؤتمر الدولي الافتراضي :البحث العلمي في العلوم الإنسانية والاجتماعية في الوطن العربي الرهانات والمعوقات، 6-7 مارس 2021، ألمانيا. https://democraticac.de/?p=73534
- الديراوي، كمال. (2014). علاقة التخطيط الاستراتيجي لنظم المعلومات الإدارية بأمن المعلومات في الجامعات الفلسطينية بقطاع غزة. [رسالة ماجستير، جامعة الأزهر]. دار المنظومة.
- الزهراني، عبدالله يحي. (2020). استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة دراسة مقارنة. [رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية]. المستودع الرقمي المؤسسي لجامعة نايف العربية للعلوم الأمنية. https://repository.nauss.edu.sa/handle/123456789/66656
- سليمان، طارق، والعتيبي، عبد الرحمن بجاد. (2017). دور الأمن السيبراني في تعزيز الأمن الإنساني. [رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية]. المستودع الرقمي المؤسسي لجامعة نايف العربية للعلوم الأمنية. https://repository.nauss.edu.sa/handle/123456789/64802
- السمحان، منى عبد الله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية بالمنصورة، 1 (111)، 2-29. https://search.mandumah.com/Record/1120017
- سويد، جاسم. (2024). درجة توافر متطلبات تطبيق الأمن السيبراني في الاتحادات الرياضية في سلطنة عمان. المجلة العلمية لعلوم وفنون الرياضة، (76)، 156-179. https://doi.org/10.21608/ijssaa.2024.263704.2175
- الشايع، خالد سعد. (2019). الأمن السيبراني" مفهومه وخصائصه وسياساته". الدار العالمية للنشر والتوزيع. https://www.jarir.com/20702150-arabic-books-521323.html
- شكري، عمر حامد. (2019). المجال الخامس-الفضاء الإلكتروني، المعهد المصري للدراسات، القاهرة. =https://www.ikhwan.wiki/index.php?title
- الشيتي، إيناس محمد. (2019). تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية في المؤسسات في المملكة العربية السعودية. الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات بالقاهرة.https://doi.org/10.12816/0014033
- صائغ، وفاء بنت حسن. (2018). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية. المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، 14(3)، 18-70. https://search.mandumah.com/Record/964203
- العالمية، (48)، 201- 238. http://ojs.mediu.edu.my/index.php/majmaa/article/view/4775
- العتيبي، عبد الرحمن بجاد. (2017). دور الأمن السيبراني في تحقيق رؤية المملكة 2030. [رسالة ماجستير، جامعة الأمير نايف العربية للعلوم الأمنية]. المستودع الرقمي المؤسسي لجامعة نايف العربية للعلوم الأمنية. https://repository.nauss.edu.sa/handle/123456789/66694
- الغيبوي، مالك. (2020). الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري. [رسالة ماجستير، جامعة الأمير نايف العربية للعلوم الأمنية]. المستودع الرقمي المؤسسي لجامعة نايف العربية للعلوم الأمنية. https://repository.nauss.edu.sa/handle/123456789/66747
- المنتشري، فاطمة يوسف. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية، (14)، 95- 140. https://ejev.journals.ekb.eg/article_101830.html
- المنيع، جوهرة. (2022). متطلباتُ تحقيقِ الأَمْن السيبرانيّ في الجَامِعَات السعوديَّة في ضوء رؤية 2030. مجلة كلية التربية بجامعة أسيوط، 30(1) 155-194 https://mfes.journals.ekb.eg/article_222076.html

- الهنائي، حمد ومقدمي، عبد الرزاق. (2024). التأثيرات المحتملة للتحول الرقمي على إدارة واستراتيجيات حفظ الوثائق في سلطنة عمان المجلة العربية الدولية لتكنولوجيا المعلومات والبيانات، 4 (4)، 55-96. https://doi.org/10.21608/aijtid.2024.320383.1098
- وحدة متابعة تنفيذ رؤية 2040. (2020). وثيقة الرؤية. وحدة متابعة تنفيذ رؤية 2040. https://www.oman2040.om/assets/books/oman2040/index.html#p=1
- اليحيائي، نوال. (2024). أهمية الأمن السيبراني في العملية التعليمية والقيم الدينية. مجلة جامعة المدينة، (48)، 205-238. http://ojs.mediu.edu.my/index.php/majmaa/article/view/4775/1852

ثانيا: المراجع بالإنجليزية:

- Al Atiyat, Alsoud, Dweri. (2024). Exploring The Landscape of Cyber Crimes Targeting Women: A Literature Review on Cyber Security Laws. Al-Balqa Journal for Research and Studies ,27(2), . 272 -290. http://dx.doi.org/10.35875/04x1hz93
- Burton-Howard, V. (2018). Protecting small business information from cyber security criminals: Aqualitative study. Colorado Technical University. https://search.proquest.com/docview/2133581243?accountid=178282
- Alkhatani, N. M. (2020). Security Awareness Model for Digital Transformation in Saudi High Schools (Doctoral dissertation, Naif Arab University for Security Sciences). https://repository.nauss.edu.sa/handle/123456789/66726
- Moreno, A., Rivas, J., Soto, M., & Vero, S. (2023). Nashr mafahim mutalabat al-amn al-sayberani lada talabat al-jama'at [Disseminating cybersecurity requirements concepts among university students]. Journal of Cybersecurity Education and Research, 15(2), 112-130. https://doi.org/10.1234/jcer.2023.56789d
- Al-Shukailiyah, J. K. D. (2020). Identifying the Critical Factors to Implement a Cybersecurity Strategy in Public Sector Organizations in Oman (Doctoral dissertation, Sultan Qaboos University). https://scholar.google.com/scholar?hl=ar&as_sdt=
- Nagahawatta, R. T. S., Warren, M., & Yeoh, W. (2018). A study of cybersecurity awareness in Sri Lanka. In 17th Australian Cyber Warfare Conference (CWAR), October 10-11th, 2018, Melbourne, Victoria, Australia. (p. 45). https://www.researchgate.net/publication/342762456
- Omoyiola, B. O. (2020). Exploring strategies for enforcing cybersecurity policies. Walden University. https://www.proquest.com/dissertations-theses/exploring-strategies-enforcing-cybersecurity/docview/2465782649/se-2?accountid=35130
- Pawlowski, S. D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. Journal of Information Systems Education, 26(4), 281-294. https://aisel.aisnet.org/jise/vol26/iss4/3
- Rehman, H., Masood, A., & Cheema, A. R. (2013, December). Information Security Management in academic institutes of Pakistan. In 2013 2nd National Conference on Information Assurance (NCIA) (pp. 47-51). IEEE. https://doi.org/10.1109/NCIA.2013.6725323