Al-Mohameed, Basem. (2023). The role of university administration in achieving cybersecurity requirements at Prince Sultan Private University, *Journal of Educational Science 9* (4), 83 - 116

The role of university administration in achieving cybersecurity requirements at Prince Sultan Private University

Dr. Basem bin Ibrahim Al-Mohameed
Assistant Professor, Educational Administration and Planning Department
College of Education - Imam Muhammad bin Saud Islamic University
bimohameed@imamu.edu.sa

Abstract:

The study aimed to identify the role of university management in achieving cybersecurity requirements, and to detect the difficulties of achieving cybersecurity, to submit proposals to help meet the requirements of cybersecurity at prince sultan private university, used the descriptive curriculum, and resolution a tool for collecting data, and formed the sample of the study of (212) of faculty members, the reached a number of results including: the role of the university administration in achieving cybersecurity requirements came highly, the most important role was to urge university staff to register out of all electronic accounts before departure, and the difficulties of achieving cybersecurity at the university came to an average degree, the most important of which was the lack of qualified human resources to provide the necessary technical support. The approval of the study members for proposals to contribute to achieving cybersecurity requirements to an average degree, one of the most prominent proposals was to prevent the use of unauthorized software on computers at the university. The study concluded with several recommendations, including: the importance of providing and developing qualified human resources, and the need to improve the infrastructure needed to implement cybersecurity requirements at the university.

Keywords: The role – University administration – Cybersecurity.

المحيميد، باسم. (٢٠٢٣). دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية. *مجلة العلوم التربوية ، ٩* (٤) ، ٨٣ - ١١٦

دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية

د. باسم بن إبراهيم المحيميد[١]

المستخلص:

هدفت الدراسة إلى التعرف على دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني ، والكشف عن صعوبات تحقيق الأمن السيبراني ، وصولًا إلى تقديم مقترحات تساعد على تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية ، واستخدمت المنهج الوصفي ، والاستبانة أداةً لجمع البيانات ، وتكونت عينة الدراسة من (٢١٢) من أعضاء هيئة التدريس ، وتوصلت إلى عددٍ من النتائج منها: أن دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني جاء بدرجة مرتفعة ، وتمثلت أهم الأدوار في حثٍّ منسوبي الجامعة على ضرورة تسجيل الخروج من جميع الحسابات الإلكترونية قبل المغادرة ، كما أن صعوبات تحقيق الأمن السيبراني في الجامعة جاءت بدرجة متوسطة ، وتمثلت أهم الصعوبات في نقص الكوادر البشرية المؤهلة لتقديم الدعم الفني اللازم. وجاءت موافقة أفراد الدراسة على المقترحات المساهمة في تحقيق متطلبات الأمن السيبراني بدرجة متوسطة ، ومن أبرز المقترحات منع استخدام البرامج غير المرخصة على أجهزة الحاسب في الجامعة. وخلُصت الدراسة إلى توصيات عديدة منها: أهمية توفير الكوادر البشرية المؤهلة وتطويرها ، وضرورة تحسين البنية التحتية اللازمة لتطبيق متطلبات الأمن السيبراني في الجامعة.

الكلمات المفتاحية: الدور- الإدارة الجامعية - الأمن السيبراني.

(١) الأستاذ مساعد بقسم الإدارة والتخطيط التربوي - كلية التربية - جامعة الإمام محمد بن سعود الإسلامية
bimohameed@imamu.edu.sa

المقدمة:

يشهد العالم اليوم تطورات سريعة في المجال المعلوماتي والمعرفي، ونموًا هائلًا في استخدام التقنية والتكنولوجيا في جميع الميادين، وازدياد تنوع وسائل الاتصال وتفاوت خصائصها، وطبيعة حجم تبادل المعلومات والمعارف بين دول العالم، أدى ذلك إلى زيادة العبء المالي والإداري والأمني على الدول التي تسعى إلى تحقيق الأمن المطلوب للفرد والمجتمع.

ويعد الميدان التعليمي، أحد أهم الميادين التي ركبت موجة التطور التقني والتكنولوجي، يأتي ذلك تزامنًا مع ما تشهده المؤسسات التعليمية من تغييرات سريعة ومتتابعة؛ نتيجة الانفجار المعرفي، والتقدم التكنولوجي، والتنافسية العالمية القائمة على أساس جودة المنتج التعليمي من حيثُ هو ركيزة أساسية للتنمية المستدامة.

لذا أدى التقدم التقني والتكنولوجي، والتحول إلى العصر الرقمي في المؤسسات التعليمية إلى تفعيل أنظمة المعلومات الإلكترونية، التي تديرها وتتحكم بها وتشغلها شبكات الحاسوب وأجهزته، مما يجعلها عرضة للاختراقات والهجمات الإلكترونية المختلفة، الأمر الذي يكوّن تحديًا أمام المؤسسات التعليمية، المتمثّلة في مدى قدرتها على توفير جميع الوسائل التقنية والإدارية؛ المتضمّنة توفير عمل نظم المعلومات واستمراريته، وتعزز حماية البيانات وخصوصيتها، وهو ما يعرف بالأمن السيبراني (البار والسميري، ٢٠١٩، ص١٠).

يذكر العتيبي (٢٠١٧) في دراسته بأن الأمن السيبراني أصبح حديث العالم بأسره، بل أصبح جزءًا أساسيًا من أي سياسات أمنية، أو اقتصادية، أو سياسات أخرى، حيث أصبح صُناع القرار في مختلف الدول يضعون مسائل الأمن السيبراني أولوية في سياستهم.

وفي ظل الحاجة الملحّة التي زادت مع ازدياد التهديدات والمخاطر الأمنية في الفضاء السيبراني أكثر من أي وقت مضى، وتحقيقًا للأهداف الطموحة التي استهدفتها رؤية المملكة ٢٠٣٠؛ لتعزيز الأمن السيبراني في جميع قطاعات الدولة، بما يضمن انسيابية المعلومات وأمانها وتكامل أنظمتها، جاء تأسيس الهيئة الوطنية للأمن السيبراني، والموافقة على تنظيمها في عام ١٤٣٩هـ، وجعلها المرجع الوطني والجهة المختصة بالأمن السيبراني، التي تعمل على سن الأنظمة والتشريعات، وتوحيد الممارسات، وتطوير الضوابط الأساسية للأمن السيبراني، ومتابعة تنفيذها، والالتزام بها في جميع القطاعات والجهات الحكومية والخاصة (الهيئة الوطنية للأمن السيبراني، ٢٠٢٠، ص٦).

مشكلة الدراسة:

تسعى وزارة التعليم في المملكة العربية السعودية إلى تحقيق أهداف رؤية المملكة ٢٠٣٠ بإحداث تحول مدروس في برامجها ، وأنشطتها ، وأنظمتها ، وإجراءاتها ، لفكر يؤمن بالفرد ومعارفه وقدراته ومهاراته ، بما يسهم في تحقيق الاقتصاد المبني على المعرفة ، وذلك ببناء منهجية لتطويع المعرفة ، وإحداث التطور التعليمي والتقني والاقتصادي للمجتمع (وزارة التعليم ،٢٠١٩).

وقد أصبحت المؤسسات التعليمية عامة والجامعات خاصة تواجه موجة من التحولات والتغيرات المتسارعة في مجال الثورة المعلوماتية ، التي تعتمد على تدفق المعلومات والمعرفة العلمية المتقدمة ، والتي تُمثل مصدرًا أكثر أهمية في بناء الميزة التنافسية بين الجامعات ، لذا تسعى الجامعات السعودية إلى تحقيق متطلبات الأمن السيبراني؛ استجابة للنمو المتسارع للمعلومات والمعارف ، ومع التحول في الخدمات إلى تعاملات إلكترونية ، والتعليم عن بعد في المرحلة الحالية بواسطة المنصات الإلكترونية ، واستخدام الأجهزة المتصلة بالشبكة المعلوماتية الإنترنت ، وتشعب طبيعة الأجهزة والتطبيقات الذكية ، ازداد خطر الهجمات السيبرانية التي تؤدي إلى تعطيل الخدمات الإلكترونية وإتلاف البيانات أو تعديلها ، والتجسس عليها ، وتدمير المعلومات والأصول (البار والسميري ، ٢٠١٩ ، ص١٩).

الأمر الذي يوضح الضرورة الملحة لإدراك أهمية تطبيق الأمن السيبراني في الجامعات السعودية ببذل مزيدٍ من الجهود؛ كون الجامعة تعد الركيزة الأساسية للتنمية المستدامة للمجتمع ، حيث تؤكد ذلك نتائج وتوصيات العديد من الدراسات ، فقد توصلت دراسة العريشي (٢٠١٨) إلى ضعف الوعي بالأمن المعلوماتي في الجامعات السعودية ، وأظهرت دراسة الصحفي (٢٠١٩) أن هناك متطلبات للأمن السيبراني غير مطبقة داخل الجامعات السعودية ، مثل المتطلبات المتعلقة باستخدام الحاسب والهاتف المحمول داخل الجامعة ، كما توصلت دراسة الشوابكة (٢٠١٩) إلى أن الإجراءات الأمنية لمنع الاختراق في جامعة الطائف كانت دون المستوى المطلوب ، وتوصلت دراسة خوجة (٢٠٢٠) إلى وجود تهديدات تؤثر في الأمن السيبراني لإدارات التعليم في المملكة العربية السعودية ، وتؤدي إلى تعطل العمل في الأنظمة الإلكترونية مثل: نظام نور ، ونظام فارس ، ونظم المراسلات الإلكترونية ، وبرامج الإشراف الإلكتروني.

وفي هذا السياق نصّت أهداف رؤية المملكة العربية السعودية ٢٠٣٠ (٢٠١٦) على الوصول إلى المراكز الخمس الأولى في مؤشر الحكومات الإلكترونية عن طريق توسيع نطاق الخدمات المقدمة للمستفيدين على شبكة الإنترنت (ص٦٣) ، ونظرًا لما تحتوي عليه الأنظمة الإلكترونية في الجامعات

من بيانات ومعلومات مهمة تسعى للمحافظة على سريتها وخصوصيتها ، ولأهمية الاستثمار الأمثل للموارد التقنية ، والمحافظة عليها من التعطل وتوقف العمل ، فإنّ أنظمة الجامعة عرضة لجميع أنواع الهجمات السيبرانية التخريبية منها والتجسسية؛ كونها تتعامل مع مجموعة كبيرة من المعلومات والمعارف بواسطة شبكة الإنترنت ، وتقدم خدمات الكترونية ، لذا فإنه يجب على الإدارة الجامعية السعي الحثيث؛ لرفع قدرتها الفنية والتنظيمية للتعامل مع الهجمات السيبرانية المحتملة ، كما تكمن أهمية دور الإدارة الجامعة في تحسين البيئة التنظيمية والتقنية ونشر الوعي بأهمية الأمن السيبراني بين منسوبيها والتشجيع على الالتزام بتنفيذ التعليمات والأنظمة الخاصة بالأمن السيبراني.

يتّضح من المؤشرات السابقة أن تطبيق الأمن السيبراني في الجامعات السعودية لم يصل بعد إلى المستوى المأمول ، كما أنه لا توجد دراسات - بحسب معرفة وجهد الباحث - تكشف عن متطلبات تحقيق الأمن السيبراني في الجامعات الأهلية. واستنادًا إلى ما سبق تتلخص مشكلة الدراسة في التعرف على دور الإدارة الجامعة في تحقيق متطلبات تحقيق الأمن السيبراني في جامعة الأمير سلطان الأهلية من وجهة نظر أعضاء هيئة التدريس فيها.

أسئلة الدراسة:

١. ما دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية من وجهة نظر أعضاء هيئة التدريس فيها؟

٢. ما الصعوبات التي تواجه تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية من وجهة نظر أعضاء هيئة التدريس فيها؟

٣. ما المقترحات التي يمكن أن تسهم في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية من وجهة نظر أعضاء هيئة التدريس فيها؟

أهداف الدراسة:

تسعى الدراسة إلى تحقيق الأهداف الآتية:

١. التعرف على دور الإدارة الجامعية في تحقيق الأمن السيبراني في جامعة الأمير سلطان الأهلية.

٢. التعرف على الصعوبات التي تواجه تحقيق الأمن السيبراني في جامعة الأمير سلطان الأهلية.

٣. تقديم مقترحات قد تساعد في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية.

أهمية الدراسة:

الأهمية نظرية:

- تنبع أهمية هذه الدراسة من أهمية موضوع الأمن السيبراني في ضوء التحديات الأمنية والهجمات السيبرانية المصاحبة لاستخدام التقنية وخطرها على الأنظمة ، والأجهزة في المؤسسات التعليمية ، ومدى وعي الإدارة الجامعية في تحقيق متطلباته والإلمام به.
- تُثري هذ الدراسة الأدب النظري المتعلق بموضوع الأمن السيبراني ، حيث يؤمل أن تكون إضافة أدبية ناجحة في رصيد الدراسات العربية.
- جاءت هذه الدراسة تلبيةً لتوصية العديد من الدراسات التي حثت على الاهتمام بالأمن السيبراني لدى منسوبي الجامعات.
- يؤمل أن تسهم هذه الدراسة في فتح المجال للباحثين بإجراء المزيد من الدراسات في مجال الأمن السيبراني في مؤسسات تعليمية أخرى.

الأهمية التطبيقية:

- توجيه أنظار منسوبي العليم الجامعي إلى أهمية الأمن السيبراني باعتباره أحد أهم مجالات العصر الحاضر ، لاتخاذ ما يلزم لضمان تحقيقه في الجامعات السعودية.
- يؤمل أن تسهم هذه الدراسة مع غيرها من الدراسات العلمية في تحقيق أهداف رؤية المملكة ٢٠٣٠.
- يؤمل أن تقديم نتائج هذه الدراسة تغذية راجعة للمسؤولين ومتخذي القرار عن مستوى تحقيق الأمن السيبراني في الجامعات السعودية.
- يؤمل أن تسهم هذه الدراسة في رفع مستوى الوعي بأهمية الأمن السيبراني داخل مؤسسات التعليم الجامعي.

حدود الدراسة:

- **الحدود الموضوعية:** تتمثل في التعرف على دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية من وجهة نظر أعضاء هيئة التدريس فيها.
- **الحدود المكانية:** اقتصرت الدراسة الحالية على جامعة الأمير سلطان الأهلية بمدينة الرياض.

- **الحدود الزمنية:** طبقت الدراسة الحالية أثناء الفصل الدراسي الأول من العام الجامعي ١٤٤٣هـ.
- **الحدود البشرية:** طبقت الدراسة الحالية على جميع أعضاء هيئة التدريس ومن في حكمهم ممن هم على رتبة أستاذ ، وأستاذ مشارك ، وأستاذ مساعد ، ومحاضر.

مصطلحات الدراسة:

الدور:

هو الوظيفة أو المركز الإداري في المنظمة الذي يقوم به الفرد ، ويحمل معه توقعات معينة لسلوكه كما يراها الآخرون (نشوان ، ١٩٥٨ ، ص١٠٩).

الإدارة الجامعية:

تبنى الباحث التعريف الإجرائي للإدارة الجامعية في أنها: العمليات والبرامج والأنشطة التي يقوم بها العاملون في الجامعة من القيادات الأكاديمية ، وأعضاء هيئة التدريس والإداريين ، بحيث تُنسّق جهودهم وتُوجّه لتقديم العطاءات المتميزة ، تحقيقًا لأهداف الجامعة ، والرقي بمكانتها العملية والعلمية (عبدالحي ، ٢٠٠٧ ، ص٣١).

الأمن السيبراني:

يقصد بالأمن السيبراني في هذه الدراسة: التنظيمات الإدارية ، والممارسات التقنية ، التي تطبق في جامعة الأمير سلطان الأهلية؛ بهدف حماية الحاسبات ، ونظم المعلومات ، والبيانات ، والشبكات من المخاطر والتهديدات السيبرانية.

أولًا: الإطار النظري:

الأمن السيبراني:

تسعى المؤسسات المختلفة في العصر الحالي إلى رفع كفاءة الأداء ، وتحسين مستوى الخدمات المقدمة ، وتحقيق رضا المستفيدين منها ، وذلك بتحويل معظم الخدمات التي تقدمها إلى خدمات الكترونية ، لذا أصبحت البيانات والمعلومات أكثر عرضة للفقد أو التعطل؛ لوجودها في الفضاء الإلكتروني والموسوم بـ(الفضاء السيبراني).

ووجود الخدمات الإلكترونية في الفضاء السيبراني قد يؤدي إلى تعرضها لعدد من الهجمات السيبرانية ، مثل: تعطل الأجهزة ، أو اختراقها ، والوصول غير المشروع إلى بياناتها ، وإتلافها أو نشرها ، وتعطل الاتصال الشبكي فيها ، ومن هنا يأتي دور المؤسسات في توفير الحماية بكافة أشكالها ، وأخذ الحيطة والحذر عند استخدام البيانات والمعلومات في الفضاء السيبراني (شلوش ، ٢٠١٨م ، ص٢٠٢) ، وكون الجامعات أحد أهم المؤسسات التعليمية التي تستوجب المحافظة على بياناتها ، ومعلوماتها ، ومعارفها التي قامت بتوليدها وتخزينها من الفقد أو الاستخدام غير المشروع ، لذا يتعين عليها العمل على تفعيل دور الأمن السيبراني في حماية أنظمتها وبياناتها.

مفهوم الأمن السيبراني:

مصطلح السيبراني: مشتق من السايبر (Cyber) ، وهو مرتبط بثقافة الحاسب ونظم المعلومات ، ويعني هذا أن الأمن السيبراني يختص الأمن الإلكتروني. ويعرف الاتحاد الدولي للاتصالات (ITU , 2020): بأنه مجموعة من السياسات ، والمبادئ ، والأدوات ، والإجراءات ، والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية ، وأصول المؤسسة المتمثلة في أجهزة الحاسب المتصلة ، والتطبيقات ، والخدمات ، وأنظمة الاتصالات والمعلومات في المؤسسة.

كما يعرف الأمن السيبراني: بأنه حماية الشبكات وأنظمة تقنية المعلومات ، ومكوناتها من أجهزة وبرمجيات ، وخدمات ، وبيانات ، من أي اختراق ، أو تعطيل ، أو استغلال غير مشروع (الهيئة الوطنية للأمن السيبراني ،٢٠٢٠ ، ص٣٢).

يتضح من التعاريف السابقة أن الأمن السيبراني عبارة عن مجموعة من الوسائل التقنية التي تحقق أمن المعلومات الإلكترونية ، وأمن الحاسبات ، وأمن الأنظمة الإدارية والبرامج ، وأمن الشبكات ، وبناءً على ذلك يعد مفهوم الأمن السيبراني أوسع وأشمل من مفهوم أمن المعلومات الإلكترونية ، إذ يعد أمن المعلومات الإلكترونية جزءًا من الأمن السيبراني.

أهمية الأمن السيبراني:

تعد البيانات والمعلومات والمعارف والأنظمة في المؤسسات من الأصول الهامة ، وهي مكاسب تنموية وتمكنها من التطور والاستمرار ، فقد أصبح السعي للمحافظة عليها أمر مهم وذلك بتحقيق الأمن السيبراني.

وتكمن أهمية الأمن السيبراني في استمرارية وحماية نظم المعلومات ويذكر الشايع (٢٠١٩) بأنه يساعد في مكافحة الجريمة السيبرانية وزيادة الوعي العام بها (ص٥٩). كما يضيف البار والسميري (٢٠١٩) بأنه يحقق الحماية للبيانات، وأنظمة المعلومات من سرقتها، والبرمجيات الخبيثة، أو الاختراقات، أو استخدامها بطريقة غير مشروعة (ص١٢).

لذا أصبح من الضرورات الهامة لدى جامعة الأمير سلطان الاهتمام بتحقيق متطلبات الأمن السيبراني في ظل تطور التقنيات المستخدمة فيها، لأهميته في الحفاظ على الموارد التقنية، وتحقيق الاستثمار الأمثل لها، والتقليل من تعطلها أو تلفها، فيؤدي إلى تجنب الهدر ورفع كفاءة الأداء، بالإضافة إلى حماية المعلومات الخاصة بكافة أنظمة الجامعة.

الهجمات السيبرانية:

الهجمات السيبرانية هي فعل يضعف من قدرات وظائف الموارد التقنية المتمثلة في أجهزة الحاسب الآلي وأنظمتها، وبياناتها، والشبكات المتصلة بها، عن طريق استغلال ثغرة أو نقطة ضعف ما، تُمكن المهاجم من استغلال الموارد التقنية بطريقة غير مسموح بها (شلوش، ٢٠١٨، ص٢٠٢). وهذه الهجمات تتميز بالديناميكية والتغيير، مما يؤدى إلى صعوبة التنبؤ بها والتصدي لها، ويمكن تصنيف الهجمات السيبرانية عامّة إلى نوعين رئيسين، هما: هجمات التجسس: وهي الوصول إلى بيانات الحساسة والهامة. وهجمات التخريب: وهي إحداث الأعطال في النظام. كما أن هناك أنوعًا متعددة للهجمات السيبرانية، يسعى المهاجمون بواسطتها إلى تحقيق عدد من الأهداف، من أبرزها ما يلي: تعطيل نظم المعلومات، وتعديل أو تدمير البيانات، أو التجسس على أجهزة وأنظمة المعلومات والبيانات.

أبعاد الأمن السيبراني:

يمثل الأمن السيبراني مظلة تتضمن أبعادًا متعددة، يذكر منها الشايع (٢٠١٩) ما يأتي:

١. **البُعد القانوني:** ويقتضي قيام الإدارة العليا بصياغة وثيقة تتضمن الأهداف الهامة والمبادئ والخطط في مجال الأمن السيبراني، والمتوافقة مع القوانين الدولية والمحلية المنظمة للأمن السيبراني؛ لضمان تحقيق الأمن السيبراني في المؤسسة، واتخاذ الإجراءات اللازمة لغير الملتزمين بها.

٢. **البُعد التنظيمي:** ويتضمن تحديد الإجراءات بخطة تشغيلية للتنفيذ والعمل والقياس، ومتابعة تطبيق الإجراءات المحددة.

٣. **البعد الاجتماعي:** عن طريق تعزيز الأمن السيبراني من حيث هو مفهوم مهم بين العاملين في المؤسسة ، وتوضيح المهام والمسؤوليات والواجبات لكل منهم ، وبناء قدراتهم لتحقيق الأمن السيبراني في المؤسسة (ص٣٣).

ويضيف البار والسميري (٢٠١٩) الأبعاد الآتية:

١. **البعد الاقتصادي:** بالمحافظة على مستوى الإنفاق ، وخفض التكاليف المترتبة على التهديدات والهجمات السيبرانية ، التي تؤدي إلى تعطل الأجهزة وفقدان البيانات.

٢. **البعد السياسي:** بمحافظة الدول أو المؤسسات على وثائقها الحساسة والسرية ، التي قد تتسبب في مشكلات حال التجسس عليها أو تسريبها (ص٢٠-٢١).

يتضح من الأبعاد السابقة الأدوار الرئيسة لتحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية ، وهي: تحديد الضوابط العامة اللازمة لتحقيق الأمن السيبراني ، وتحديد الواجبات والمسؤوليات المناطة بمنسوبيها ، وبناء قدراتهم في مجال الأمن السيبراني ، وتوضيح الإجراءات والممارسات التي تؤدي إلى ضمان تحقيق الأمن السيبراني فيها؛ مما يضمن تقليل الهدر الذي قد تسببه الهجمات السيبرانية ، بالإضافة إلى العمل على توفير المتطلبات اللازمة لتحقيق الأمن السيبراني.

متطلبات تحقيق الأمن السيبراني:

تعددت متطلبات تحقيق الأمن السيبراني في الأدبيات ، ويمكن تصنيف هذه المتطلبات كما يأتي:

أولًا: المتطلبات الإدارية:

يرى زيك وكاجتازي (Zec & Kajtazi, 2015) ضرورة تحديد المؤسسة للإجراءات التنفيذية اللازمة؛ لتحقيق الأمن السيبراني حسب طبيعتها (ص٢٣١) ، وتشير جبور (٢٠١٦) إلى أن أولى خطوات تحقيق الأمن السيبراني في المؤسسات ، هي تحديد المبادئ والقواعد اللازمة لتحقيق الأمن السيبراني ، وتحديد الصلاحيات ، وعدم السماح باستخدام النظام ، إلا فيما هو معد لأجله ، وفي الإطار المسموح به (ص٣٠).

ويؤكد البار والسميري (٢٠١٩) على ضرورة تعزيز إدارة المخاطر لتحقيق الأمن السيبراني في المؤسسات بتقييم المخاطر التي تتعرض لها أنظمة المؤسسات، ووضع استراتيجيات محددة لمواجهة أي خطر، والتصدي للبرامج الضارة، وعدم التعامل مع أي محتوى ضار قد يؤثر في أنظمة المؤسسة، وأيضًا تدريب العاملين على كيفية حماية البيانات وأنظمة المعلومات، وتوعيتهم بمدى الخطر الذي قد تتعرض له المؤسسة (ص١٤). كما يرى حمودة (٢٠١٤) ضرورة إنشاء وحدة إدارية خاصة بالأمن السيبراني تعنى بمتابعة تحقيقه في المؤسسة، وتوفير الموارد المادية والبشرية اللازمة للحماية من الهجمات السيبرانية، وإعداد وثيقة تتضمن مجموعة من التعليمات والقوانين التي تتوافق مع سياسات الإدارة العليا، ومتابعة تطبيقها (ص٦٠).

كما أن من أبرز المتطلبات الإدارية لتحقيق الأمن السيبراني تحديد الأهداف وتشخيص الواقع؛ ووضع خطة للدفاع السيبراني من أجل التغلب على الصعوبات، كما أن المقارنة المرجعية والاستفادة من الخبرات والممارسات المتميزة، والتجارب الناجحة لها أثر بارز لتحقيق متطلبات الأمن السيبراني في الجامعة.

ثانيًا: المتطلبات التقنية:

يذكر زيك وكاجتازي (Zec & Kajtazi, 2015) أن متطلبات تحقيق الأمن السيبراني في الجانب التقني تركز على ما يلي:

١. توفير جدار حماية على شبكة الإنترنت، وتوفير برامج مكافحة الفيروسات.
٢. رفع مستوى أمان كلمات المرور بتطبيق شروط كلمات المرور الأمنة.
٣. تحديث البرامج وأنظمة التشغيل؛ لسد الثغرات ومعالجة المشكلات المتعلقة بها.
٤. عمل النسخ الاحتياطي للبيانات دوريًا؛ لاسترجاعها في حال فقدان البيانات وتعطل الأجهزة عن العمل (ص٢٣١).

ويتفق موبري (Mowbray, 2014) مع ما سبق ويضيف أنه لا يكتفى بتثبيت برنامج الحماية من البرامج الضارة على أجهزة الحاسب في المؤسسات، وإنما يتوجب تفعيل التحديث التلقائي لها، والحفاظ على تحديث نظم التشغيل، وتأمين جميع الحسابات باستخدام كلمات المرور العالية الأمان (ص٢٣٩). ويذكر مظلوم (٢٠١٨) أنه يمكن الاستعانة بالأفراد والشركات المتخصصة؛ لتطوير قدرات المؤسسة واختبار مدى جاهزيتها لمواجهة الهجمات السيبرانية، مع الإشارة إلى أهمية توفير الميزانيات المخصصة لتحقيق ذلك (ص٨٩).

وفي ضوء ما سبق يمكن تلخيص أبرز المتطلبات الفنية لتحقيق للأمن السيبراني في توعية منسوبي الجامعة بمفهوم وأهمية الأمن السيبراني ، ونشر تعليمات تحقيق الأمن السيبراني للعمل بها ، وتنظيم دورات تدريبية لإكساب المنسوبين مهارات تحقيق الأمن السيبراني ، وتوفير الدعم الفني للمشاكل المرتبطة بتقنية المعلومات ، ومتابعة تطبيق ذلك باستمرار.

دور إدارة الجامعات في تحقيق الأمن السيبراني:

مع تزايد التحديات التي تواجه المرحلة الحالية من تغييرات مستمرة في الميدان التعليمي ، والحاجة إلى مزيد من المعارف تجاه التحول الإلكتروني في التعليم عن بعد ، وتوفير بيئة الكترونية آمنة تضمن استمرارية هذا النوع من التعليم.

ويأتي دور وزارة التعليم بصفتها أحد شركاء تحقيق الأمن السيبراني؛ بتوعية منسوبيها بمهام الهيئة الوطنية للأمن السيبراني ومراكزها ، وطلب المساعدة منها في حال احتياجها خصوصًا في رفع مستوى الأمن السيبراني في الجامعات الحكومية والأهلية السعودية ، والاطلاع على ما يصدر من المركز الوطني الإرشادي للأمن السيبراني من أدلة ولوائح ، كمراجع عند تنفيذ البرامج التوعوية الخاصة بالأمن السيبراني فيها ، وتفعيل خدمة الإبلاغ عن الحوادث الأمنية التي أتاحتها الهيئة عند الحاجة.

ويتمثل دور الإدارة الجامعية كما أشار إليه كلًا من Mowbray (2014) وجبور (٢٠١٦) والشوابكة (٢٠١٩) في ترشيح منسوبيها ممن تتوافر فيهم الشروط؛ للحصول على البرامج التدريبية التي تعقدها الأكاديمية الوطنية للأمن السيبراني ، وتوفير بيئة إلكترونية آمنة للتواصل ، ويبرز دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني من خلا جهود القيادات الأكاديمية؛ وحثهم على تحسين البيئة الثقافية ، والتنظيمية ، والتقيد بضوابط الأمن السيبراني الصادرة عن الهيئة الوطنية للأمن السيبراني ، والعمل على تحقيق ما جاء فيها ، بالإضافة إلى توعية منسوبي الجامعة بمضمونها والالتزام بما ورد فيها.

ثانيًا: الدراسات السابقة:

تضّمن هذا الجزء عرضًا للدراسات السابقة ذات الصلة بموضوع الدراسة الحالية ، وعُرضت وفق منهجية علمية محددة ، ووفق تسلسل زمني من الأقدم إلى الأحدث جاءت في الفترة الزمنية بين (٢٠١٥) و (٢٠٢٠) ، وقد تم استعراضها من خلال العناصر التالية (اسم الباحث ، عام

النشر ، هدف الدراسة ، وأبرز النتائج ذات الصلة بموضوع الدراسة). ومن ثم التعليق عليها من خلال بيان أوجه الاتفاق والاختلاف بينها وبين الدراسة الحالية ، وعرض جوانب الاستفادة منها ، وأبرز ما يميّز الدراسة الحالية عنها.

دراسة عبد الواحد (٢٠١٥) هدفت إلى التعرف على سياسات أمن المعلومات وعلاقتها بفاعلية نظم المعلومات الإدارية في الجامعات الفلسطينية بقطاع غزة ، وكان من أبرز النتائج التي توصلت إليها الدراسة أن تحقيق سياسات أمن المعلومات في الجامعات الفلسطينية بقطاع غزة جاءت بدرجة مرتفعة ، وأن معرفة الموظف بالإجراءات التي يتبعها لتفادي مخاطر أمن المعلومات جاءت بدرجة مرتفعة ، وأن اهتمام الإدارة العليا بتوزيع سياسات أمن المعلومات على العاملين جاء بدرجة متوسطة ، كما أن تنفيذ الجامعات لبرامج تدريب والتوعية الالزامية للعاملين في مجال أمن المعلومات جاء بدرجة مرتفعة.

دراسة القحطاني (٢٠١٧) هدفت إلى تحديد دور إدارة أمن المعلومات في الحد من الإرهاب الإلكتروني في كلية الحاسبات وتقنية المعلومات بجامعة الملك عبد العزيز بجدة ، وكان من أبرز النتائج التي توصلت إليها الدراسة أن مستوى أمن المعلومات في الكلية جاء بدرجة مرتفعة ، وأن حفظ النسخ الاحتياطية الإلكترونية جاء بدرجة مرتفعة ، كما أن توافر سياسات خاصة شاملة لأمن المعلومات جاء بدرجة مرتفعة.

دراسة ماهنو Mahno (2017) هدفت إلى تحديد الحاجة إلى برنامج التوعية بالأمن السيبراني لطلاب جامعات جمهورية أستونيا غير المتخصصين في تكنولوجيا المعلومات ، وتصميم برنامج للتوعية الأمنية السيبرانية لهم ، وكان من أبرز النتائج التي توصلت إليها الدراسة أن تنظيم دورات تدريبية في الأمن السيبراني لطلاب السنة الأولى غير المتخصصين في تكنولوجيا المعلومات بجمهورية أستونيا جاء بدرجة منخفضة جدًا ، كما أن تسجيل الخروج من الأجهزة عند عدم العمل عليها جاء بدرجة متوسطة.

دراسة إبراهيم (٢٠١٨) هدفت إلى التعرف على مستوى نظم أمن المعلومات وأثرها على قدرات التعلم التنظيمية في الجامعات الأردنية ، وكان من أبرز النتائج التي توصلت إليها الدراسة أن مستوى نظم أمن المعلومات من وجهة نظر العاملين مستخدمي تكنولوجيا المعلومات في الجامعات الأردنية جاء بدرجة مرتفعة ، وأن توفر سياسات خاصة شاملة لأمن المعلومات في الجامعات الأردنية جاء بدرجة مرتفعة ، كما أن تطبيق إدارة الجامعات الأردنية لإجراءات عقابية على الموظف الذي ينتهك إجراءات أمن المعلومات وسياستها جاء بدرجة مرتفعة.

دراسة الصحفي (٢٠١٩) هدفت إلى تحديد متطلبات تحقيق الأمن السيبراني اللازمة لأنظمة المعلومات الإدارية بالجامعات الحكومية السعودية في مدينة الرياض ، ومن أبرز النتائج التي توصلت إليها الدراسة أن أفراد عينة الدراسة موافقون على المتطلبات الإدارية والمتطلبات المادية للأمن السيبراني ، وغير متأكدون من المتطلبات التقنية والمتطلبات البشرية للأمن السيبراني ، بالإضافة إلى عدم وجود فروق ذات دلالة إحصائية بين أفراد عينة الدراسة ، نحو متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بالجامعات الحكومية السعودية تُعزى لمتغيري المؤهل العلمي وسنوات الخبرة.

دراسة الشوابكة (٢٠١٩) هدفت إلى التعرف على دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف ، وكان من أبرز النتائج التي توصلت إليها الدراسة أن مستوى الإجراءات الأمنية في جامعة الطائف جاء بدرجة عالية ، كما أن إجراءات الأمن المعلوماتي لمنع الاختراق عن طريق كل من الشبكة الحاسوبية والهندسة الاجتماعية والبرمجيات الضارة جاءت بدرجة عالية ، بالإضافة إلى أن توعية مستخدمي النظام في جامعة الطائف بالسياسات المتعلقة بالأمن المعلوماتي جاءت بدرجة متوسطة.

دراسة خوجة (٢٠٢٠) هدفت إلى التعرف على المتطلبات الإدارية الداعمة للأمن السيبراني في إدارات التعليم بالمملكة العربية السعودية ، وكان من أبرز النتائج التي توصلت إليها الدراسة موافقة أفراد الدراسة على المتطلبات الإدارية الداعمة للأمن السيبراني في إدارات التعليم بدرجة عالية ، كما أن المحافظة على سرية المعلومات والوثائق الهامة جاءت بدرجة مرتفعة ، والتحكم في اتصال العاملين بالإنترنت جاء بدرجة مرتفعة ، كما أن منع استخدام البرامج غير المرخصة جاء بدرجة مرتفعة ، بالإضافة إلى أن توفر إدارة التقنية لتحقيق الأمن السيبراني في إدارات التعليم جاء بدرجة متوسطة.

التعليق على الدراسات السابقة:

في ضوء الاستعراض للدراسات السابقة ، يمكن تحديد أوجه الاتفاق والاختلاف بينها وبين الدراسة الحالية؛ من حيث: هدف الدراسة ، ومنهجها ، ومجالها ، أداتها ، وأوجه الاستفادة منها:

أوجه الاتفاق والاختلاف بين الدراسة الحالية والدراسات السابقة:

أولًا: الهدف من الدراسة:

هدفت الدراسة الحالية إلى التعرف على دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية، واتفقت جزئيًا في بعض أهدافها مع عدد من الدراسات؛ كدراسة الصحفي (٢٠١٩) التي هدفت إلى تحديد متطلبات تحقيق الأمن السيبراني بالجامعات الحكومية السعودية، وكذلك اتفقت جزئيًا في هدف تحديد مستوى تحقيق الأمن السيبراني مع دراسة كلٍ من: خوجة (٢٠٢٠)، ماهنو Mahno (2017)، القحطاني (٢٠١٧)، الشوابكة (٢٠١٩)، عبد الواحد (٢٠١٥)، إبراهيم (٢٠١٨).

ثانيًا: منهج الدراسة:

واتفقت مع جميع الدراسات حيث استخدمت جميعها المنهج الوصفي.

ثالثًا: مجال الدراسة:

اتفقت الدراسة الحالية مع معظم الدراسات السابقة في مجال مؤسسات التعليم الجامعي، واختلفت مع دراسة خوجة (٢٠٢٠) التي كان مجالها مؤسسات التعليم العام.

رابعًا: أداة الدراسة:

اتفقت الدراسة الحالية مع جميع الدراسات السابقة في استخدام أداة الدراسة (الاستبانة)، باستثناء دراسة خوجة (٢٠٢٠) التي استخدمت أداتين هما: الاستبانة والمقابلة؛ والتي اتفقت معها الدراسة الحالية جزئيًا.

خامسًا: أوجه الاستفادة من الدراسات السابقة:

يمكن إيجاز أبرز نقاط الاستفادة العلمية من الدراسات السابقة فيما يلي:

- الوصول إلى تشخيص دقيق للمشكلة وصياغة دقيقة لعنوان الدراسة.
- توظيف توصيات ومقترحات الدراسات السابقة في دعم مشكلة الدراسة وأهميتها إثراء الإطار النظري، خصوصًا دراسة كل من القحطاني (٢٠١٧)، إبراهيم (٢٠١٨)، الصحفي (٢٠١٩م)، الشوابكة (٢٠١٩م)، خوجة (٢٠٢٠).

- بناء أداة الدراسة ، حيث استفادت الدراسة الحالية في صياغة عباراتها من دراسة كلٍ من عبد الواحد (٢٠١٥) ، إبراهيم (٢٠١٧) ، ماهنو (Mahno(2017) ، الصحفي (٢٠١٩م) ، الشوابكة (٢٠١٩م) ، خوجة (٢٠٢٠م).
- تفسير نتائج الدراسة الحالية ، ومقارنة النتائج التي توصلت إليها بنتائج الدراسات السابقة ، من حيث أوجه الاتفاق والاختلاف ، مما يعزز نتائج الدراسة الحالية.
- التوصل إلى أبرز المراجع لموضوع الدراسة.

منهجية الدراسة وإجراءاتها:

أولًا: المنهج:

استخدم الباحث المنهج الوصفي المسحي ، وذلك بتوزيع الاستبانة على جميع أفراد مجتمع الدراسة؛ بهدف التعرف على دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية.

ثانيًا: مجتمع وعينة الدراسة:

تكون مجتمع الدراسة من جميع أعضاء هيئة التدريس في جامعة الأمير سلطان الأهلية ، والبالغ عددهم (٤٦٦) عضوًا ، ولمحدودية المجتمع طبق أسلوب الحصر الشامل لجميع أفراد مجتمع الدراسة ، وكان العائد (٢١٢) استبانة ، وبذلك بلغت نسبة الاستجابات (٤٦ ٪) من المجتمع الأصلي ، ويعدّ هذا العدد مناسبًا وفقًا لما حدد كرجسي ومرجان (Krejcie and morgan , 1970 , P. 609) في جدول تحديد العينة ، وفيما يأتي خصائص أفراد الدراسة:

جدول (١)

يوضح توزيع خصائص أفراد الدراسة

المتغيرات	الفئات	التكرار	النسبة
الكلية	العلوم الإنسانية	٢٢	١٠,٤
	القانون	٢٥	١١,٨
	الهندسة	٥٩	٢٧,٨
	إدارة الأعمال	٥٨	٢٧,٤

المتغيرات	الفئات	التكرار	النسبة
الكلية	علوم الحاسب والمعلومات	٤٨	٢٢,٦
	المجموع	٢١٢	٪١٠٠
الرتبة العلمية	أستاذ	١٨	٨,٥
	أستاذ مشارك	١٦	٧,٥
	أستاذ مساعد	١٦١	٧٥,٩
	محاضر	١٧	٨,٠
	المجموع	٢١٢	٪١٠٠
الجنس	ذكر	١٠٢	٤٨,١
	أنثى	١١٠	٥١,٩
	المجموع	٢١٢	٪١٠٠

يتضح من الجدول السابق ما يأتي:

١. **بالنسبة للكلية:** اتضح أن (٢٧,٨٪) من إجمالي أفراد الدراسة ينتمون إلى كلية الهندسة ، في حين أن (٢٧,٤٪) من إجمالي أفراد الدراسة ينتمون إلى كلية إدارة الأعمال ، بينما (٢٢,٦٪) من إجمالي أفراد الدراسة ينتمون إلى كلية علوم الحاسب والمعلومات ، كما أن (١١,٨٪) من إجمالي أفراد الدراسة ينتمون إلى كلية القانون ، بينما اتضح أن (١٠,٤٪) من إجمالي أفراد الدراسة ينتمون إلى كلية العلوم الإنسانية.

٢. **بالنسبة للرتبة العلمية:** اتضح أن (٧٥,٩٪) من إجمالي أفراد الدراسة أساتذة مساعدين ، وهي أكبر الفئات ، بينما (٨,٥٪) من إجمالي أفراد الدراسة أساتذة ، كما أن (٨,٠٪) من إجمالي أفراد الدراسة محاضرين ، بينما اتضح أن (٧,٥٪) من إجمالي أفراد الدراسة أساتذة مشاركين.

٣. **بالنسبة للجنس:** اتضح أن (٥١,٩٪) من إجمالي أفراد الدراسة من الإناث ، بينما اتضح أن (٤٨,١٪) من إجمالي أفراد الدراسة من الذكور.

ثالثًا: أداة الدراسة:

تعدّ الاستبانة من أكثر أدوات جمع البيانات استخدامًا؛ وذلك نظرًا لإمكانية تطبيقها على نطاق واسع وعلى عينة كبيرة من الأفراد ، كما تضمن عدم تحيز الباحث ، وتقلل الوقت

والجهد في جمع البيانات ، وتضمن خصوصيتها وسريتها ، وبناءً على ذلك استُخدمت الاستبانة أداةً لجمع البيانات من أفراد الدراسة الحالية؛ لمناسبتها طبيعة الدراسة ، وأهدافها ، ومنهجها ، والإجابة عن تساؤلاتها ، بالإضافة لمناسبتها لحجم العينة ، وتكونت الاستبانة من قسمين:

- **القسم الأول:** البيانات الوظيفية لأفراد عينة الدراسة وتشمل: (الكلية- الرتبة العلمية- الجنس).
- **القسم الثاني:** محاور الدراسة وتتمثل في المحاور الآتية: الأول: دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في الجامعة وتكون من (١٢) عبارة ، والثاني: صعوبات تحقيق متطلبات الأمن السيبراني في الجامعة وتكون من (١٠) عبارة ، والثالث: المقترحات التي قد تساعد في تحقيق متطلبات الأمن السيبراني في الجامعة وتكون من (١٠) عبارة. ويقابل كل عبارة من عبارات هذه المحاور قائمة تحمل العبارات وأُعطيت كل عبارة درجة لتُعالج إحصائيًا على النحو الآتي: مرتفعة جد(٥) ، مرتفعة(٤) ، متوسطة(٣) ، منخفضة(٢) ، منخفضة جدًا(١).

رابعًا: صدق أداة الدراسة:

يهدف قياس صدق أداة الدراسة إلى التأكد من مدى مناسبتها لقياس ما أعدت لقياسه ، وقد تحقق من صدق أداة الدراسة الحالية ، وهي الاستبانة باستخدام كلٍ من:

١. الصدق الظاهري للأداة:

عُرضت الاستبانة بصورتها الأولية على المحكمين ، وعددهم (٢٢) محكم من ذوي الاختصاص والخبرة الإدارية من أعضاء هيئة التدريس في الجامعات السعودية ، المهتمين بموضوع الدراسة الحالية؛ لتجويد الاستبانة بالحكم على وضوح عباراتها ، وجودة صياغتها ، ومدى مناسبتها لمجالات الاستبانة ، وطلب منهم أي تعديل ، أو حذف ، أو إضافة ما يرون مناسبته ، وقد أُخذ بآراء المحكمين ، وأُجريت التعديلات المطلوبة سواءً كانت حذفًا ، أو إضافة ، أو إعادة صياغة.

٢. الاتساق الداخلي للأداة:

تم التأكد من صدق الاتساق الداخلي للاستبانة بحساب معامل الارتباط بيرسون؛ للتعرف على مدى ارتباط كل عبارة من عبارات الاستبانة بالدرجة الكلية للمحور الذي تنتمي إليه ، ويمكن إيضاح ذلك في الجداول الآتية:

جدول (٢)

معاملات الارتباط بين درجة كل فقرة من فقرات محور "دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية" والدرجة الكلية للمحور

رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط
١	٠,٤٢٥**	٧	٠,٤٩٦**
٢	٠,٥٢٤**	٨	٠,٦٠٣**
٣	٠,٦٤٧**	٩	٠,٧٦٥**
٤	٠,٧٤٧**	١٠	٠,٦٤٠**
٥	٠,٤٢١**	١١	٠,٧٨٥**
٦	٠,٦٣٨**	١٢	٠,٣٨٠**

** دالة عند مستوى الدلالة ٠,٠١ فأقل.

جدول (٣)

معاملات الارتباط بين درجة كل فقرة من فقرات محور "صعوبات تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية" والدرجة الكلية للمحور

رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط
١	٠,٦٤٣**	٦	٠,٧١٥**
٢	٠,٥٥٠**	٧	٠,٥٧٦**
٣	٠,٥٨٤**	٨	٠,٦٦٠**
٤	٠,٦٨٣**	٩	٠,٤٩٧**
٥	٠,٦٠٦**	١٠	٠,٤٧٠**

** دالة عند مستوى الدلالة ٠,٠١ فأقل.

جدول (٤)

معاملات الارتباط بين درجة كل فقرة من فقرات محور "المقترحات التي يمكن أن تساهم في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية" والدرجة الكلية للمحور

رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط
١	٠,٤١٧**	٦	٠,٧٤٣**
٢	٠,٤٥٠**	٧	٠,٦٤٠**

رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط
٣	٠,٥٢١**	٨	٠,٥٢٨**
٤	٠,٧٨٦**	٩	٠,٦٩٧**
٥	٠,٧١٤**	١٠	٠,٣٣٩**

** دالة عند مستوى الدلالة ٠,٠١ فأقل.

يتضح من الجداول السابقة أن قيم معاملات الارتباط بين درجة الفقرة والدرجة الكلية للمحور الذي تنتمي إليه هي قيم عالية ، وجميعها موجبة ، ودالة إحصائيًا عند مستوى الدلالة (٠,٠١) ، مما يعني وجود درجة عالية من الاتساق الداخلي بما يعكس درجة عالية من الصدق لفقرات أو مؤشرات الاستبانة.

ثبات أداة الدراسة:

تم حساب ثبات الأداة باستخدام معادلة ألفا كرونباخ ، ويوضح الجدول الآتي قيمة معامل الثبات لكل محور من محاور الاستبانة كما يأتي:

جدول (٥)

معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

المحاور	عدد الفقرات	معامل الثبات
دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية.	١٢	٠,٨٢٦
صعوبات تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية.	١٠	٠,٧٩٦
المقترحات التي يمكن أن تسهم في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية.	١٠	٠,٧٥٢
الثبات الكلي للاستبانة.	٣٢	٠,٨٢٣

يتضح في النتائج الموضحة في جدول أعلاه أن معامل الثبات لأبعاد الدراسة ومحاورها عالي ، حيث يتراوح ما بين (٠,٧٥٢-٠,٨٢٦) ، وبلغت قيمة معامل الثبات العام (٠,٨٢٣) ، وهي قيمة ثبات مرتفعة توضح صلاحية أداة الدراسة للتطبيق الميداني.

أساليب المعالجة الإحصائية:

لتحقيق أهداف الدراسة وتحليل البيانات التي ستُجمع باستخدام الحزم الإحصائية للعلوم الاجتماعية ، والتي يرمز لها اختصارًا بالرمز (SPSS) ، وذلك بعد ترميز البيانات وإدخالها إلى

الحاسب الآلي ، ومن ثم قام الباحث بحساب الوسط الحسابي لإجابات أفراد الدراسة ، ولتحديد طول خلايا المقياس الخماسي(الحدود الدنيا والعليا) المستخدم في محاور الدراسة ، تم حساب المدى(٥-١=٤) ، ثم تقسيمه على عدد خلايا المقياس؛ للحصول على طول الخلية الصحيح أي (٤/٥= ٠,٨٠) بعد ذلك أُضيفت هذه القيمة إلى أقل قيمة في المقياس؛ لتحديد الحد الأعلى لهذه الخلية ، وهكذا أصبح طول الخلايا كما يوضحها الجدول الآتي:

جدول (٦)

مقياس ليكرت الخماسي لقياس درجة الموافقة ومدى الموافقة

درجة الموافقة	الترميز	مدى الموافقة
منخفضة جدًا	١	من ١,٠ إلى ١٨٠
منخفضة	٢	من ١,٨١ إلى ٢,٦٠
متوسطة	٣	من ٢,٦١ إلى ٣,٤٠
مرتفعة	٤	من ٣,٤١ إلى ٤,٢٠
مرتفعة جدًا	٥	من ٤,٢١ إلى ٥,٠

ولخدمة أغراض الدراسة وتحليل البيانات التي جُمعت بواسطة أداة الدراسة في الجانب الميداني ، استُخدم عدد من الأساليب الإحصائية لمعرفة اتجاهات أفراد مجتمع الدراسة حول التساؤلات المطروحة ، وذلك باستخدام أساليب المعالجة الإحصائية الآتية:

١. التكرارات والنسب المئوية؛ للتعرف على الخصائص الشخصية والوظيفية لأفراد عينة الدراسة ، وتحديد استجابات أفرادها تجاه عبارات المحاور الرئيسة التي تتضمنها أداة الدراسة.

٢. المتوسط الحسابي "Mean"؛ لمعرفة مدى ارتفاع أو انخفاض استجابات أفراد عينة الدراسة عن المحاور الرئيسة (متوسط العبارات) ، مع العلم بأنه يفيد في ترتيب المحاور حسب أعلى متوسط حسابي.

٣. الانحراف المعياري "Standard Deviation"؛ للتعرف على مدى انحراف استجابات أفراد عينة الدراسة لكل عبارة من عبارات متغيرات الدراسة ، ولكل محور من المحاور الرئيسة عن متوسطها الحسابي.

٤. معامل الارتباط بيرسون person Correlation""؛ لمعرفة درجة الارتباط بين عبارات الاستبانة والمحور الذي تنتمي إليه كل عبارة من عباراتها.

٥. معامل ألفا كرونباخ (Cronch›lph): لاختبار مدى ثبات أداة الدراسة.

تحليل نتائج الدراسة ومناقشتها وتفسيرها:

عرض ومناقشة أسئلة الدراسة:

عرض ومناقشة نتائج السؤال الأول: ما دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية من وجهة نظر أعضاء هيئة التدريس فيها؟

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية ، والانحرافات المعيارية ، والرتب لاستجابات أفراد عينة الدراسة من أعضاء هيئة التدريس في جامعة الأمير سلطان على محور "دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية" والجدول التالي يوضح النتائج المتصلة بهذا المحور.

جدول (٧)

استجابات أفراد الدراسة على محور "دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية "

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
٩	تؤكد الجامعة على منسوبيها ضرورة تسجيل الخروج من جميع الحسابات الإلكترونية قبل المغادرة.	٤,١٥	٠,٩٢	١	مرتفعة
١١	تطبق الجامعة أنظمة الأمن السيبراني للنسخ الاحتياطي للبيانات والمعلومات الإدارية.	٣,٨٠	١,١٨	٢	مرتفعة
٧	تمنع الجامعة استخدام البرامج غير المرخصة على أجهزة الحاسب.	٣,٦٢	١,٢٧	٣	مرتفعة
١	تعمل الجامعة على توعية منسوبيها بمفهوم الأمن السيبراني وأهدافه.	٣,٥٤	٠,٨٥	٤	مرتفعة
٨	تحرص الجامعة على ضرورة محافظة منسوبيها على سرية كلمات المرور، وعدم الإفصاح عنها.	٣,٤٨	٠,٧٤	٥	مرتفعة
٥	توجد سياسات أمنية لأنظمة المعلومات الإدارية والأكاديمية في الجامعة.	٣,٤٨	٠,٩٥	٦	مرتفعة
٣	تسعى الجامعة إلى نشر ضوابط تحقيق الأمن السيبراني بين منسوبيها.	٣,٤٠	٠,٩٨	٧	متوسطة
٤	يتوفر في الجامعة خطة لإدارة مخاطر الأمن السيبراني داخل الأنظمة الإدارية والأكاديمية.	٣,٣٢	١,٣٠	٨	متوسطة

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
٦	تهتم الجامعة بمتابعة تحديث أنظمة التشغيل لأجهزة الحاسب الآلي دوريًا.	٣,٢٩	١,١٦	٩	متوسطة
١٠	تلتزم الوحدات الإدارية والأكاديمية بالجامعة بتطبيق أنظمة تحقيق الأمن السيبراني.	٣,٢٦	١,١١	١٠	متوسطة
٢	يوجد في الجامعة إدارة خاصة بالأمن السيبراني.	٣,٠٦	٠,٧٢	١١	متوسطة
١٢	تطبق الجامعة متطلبات الأمن السيبراني لحماية أنظمة المعلومات والاتصالات الإدارية.	٣,٠٥	١,١٣	١٢	متوسطة
المتوسط الحسابي العام		٣,٤٥	٠,٦١	مرتفع	

يتضح من الجدول السابق أن هناك تفاوت في درجة موافقة أفراد الدراسة على عبارات محور (دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية) ، حيث يشمل المحور (١٢) فقرة ، وجاءت استجابات أفراد الدراسة على فقرات المحور بدرجات موافقة تتراوح ما بين (متوسطة/ مرتفعة) على أداة الدراسة ، حيث تراوحت المتوسطات الحسابية من (٣,٠٥ إلى ٤,١٥) ، وهذه المتوسطات تشير إلى درجة موافقة (متوسطة/ مرتفعة) بالنسبة إلى أداة الدراسة.

ومن النتائج الموضحة في الجدول أظهرت نتائج المتوسطات الحسابية لعبارات المحور أن أعلى فقرة من حيث المتوسط الحسابي هي العبارة رقم (٩) ، ونصّها: "تؤكد الجامعة على منسوبيها ضرورة تسجيل الخروج من جميع الحسابات الإلكترونية قبل المغادرة" بالمرتبة الأولى وبدرجة موافقة (مرتفعة) ، بمتوسط حسابي(٤,١٥) وانحراف معياري (٠,٩٢) ، تليها في المرتبة الثانية العبارة رقم (١١) ، ونصّها: "تطبق الجامعة أنظمة الأمن السيبراني للنسخ الاحتياطي للبيانات والمعلومات الإدارية" بدرجة موافقة (مرتفعة) ، بمتوسط حسابي(٣,٨٠) وانحراف معياري (١,١٨).

بينما جاءت العبارة رقم (٢) ونصّها: "يوجد في الجامعة إدارة خاصة بالأمن السيبراني" بالمرتبة الحادية عشرة وبدرجة موافقة (متوسطة) ، بمتوسط حسابي (٣,٠٦) وانحراف معياري (٠,٧٢) ، وفي المرتبة الأخيرة جاءت العبارة رقم (١٢) ونصّها: "تطبق الجامعة متطلبات الأمن السيبراني لحماية أنظمة المعلومات والاتصالات الإدارية" وبدرجة موافقة (متوسطة) ، بمتوسط حسابي (٣,٠٥) ، وانحراف معياري (١,١٣).

نستخلص مما سبق أن المتوسط العام لاستجابات أفراد الدراسة على عبارات محور(دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية) بلغ (٣,٤٥ درجة من ٥) ، وهذا المتوسط يشير إلى درجة موافقة (مرتفعة) بالنسبة لأداة الدراسة ، وهكذا يتضح أن أفراد الدراسة يرون أن أهم أدوار الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية تتمثل في: (تأكيد الجامعة على منسوبيها ضرورة تسجيل الخروج من جميع الحسابات الإلكترونية قبل المغادرة ، وتطبق أنظمة الأمن السيبراني للنسخ الاحتياطي للبيانات والمعلومات الإدارية ، ومنع استخدام البرامج غير المرخصة على أجهزة الحاسب ، وتوعية منسوبي الجامعة بمفهوم الأمن السيبراني وأهدافه).

ويتضح مما سبق أن الإدارة الجامعية حريصة على تطبيق مفهوم الأمن السيبراني بجميع مقوماته وعناصره وأساليبه ، من خلال توجيه المنسوبين للالتزام بها ، كما تتخذ إجراءات عملية لضمان الأمن والحفاظ على المعلومات والبيانات الخاصة بها بأعلى وسائل وأساليب الحماية ، سواء بتوفير نسخ احتياطية لأهم البيانات والمعلومات الخاصة بها ، والتنبيه الشديد على جميع منسوبي الجامعة بعدم المجازفة باستعمال أي برنامج غير مرخص من شأنه إتلاف أو الإضرار بالبيانات الموجودة على أجهزة الحاسوب ، كما أن الإدارة الجامعية سعت لابتكار سياسات خاصة بها مبنية على خطة استراتيجية هدفها على توعية منسوبيها بمفهوم الأمن السيبراني وأهدافه.

وتتفق هذه النتائج مع دراسة القحطاني (٢٠١٧م) التي توصلت إلى أن مستوى أمن المعلومات في كلية الحاسبات وتقنية المعلومات بجامعة الملك عبد العزيز بجدة جاء بدرجة مرتفعة ، وأن حفظ النسخ الاحتياطية الإلكترونية يأتي بدرجة مرتفعة ، كما أن توافر سياسات خاصة شاملة لأمن المعلومات جاء بدرجة مرتفعة ، كما تتفق مع دراسة الشوابكة (٢٠١٩م) حيث توصلت إلى أن مستوى الإجراءات الأمنية في جامعة الطائف جاء بدرجة عالية ، كما أن إجراءات الأمن المعلوماتي لمنع الاختراق عن طريق كل من الشبكة الحاسوبية والهندسة الاجتماعية ، والبرمجيات الضارة جاءت بدرجة عالية ، وأن توافر آلية مناسبة للتوثق من شخصية الداخلين إلى النظام والشبكة في جامعة الطائف جاء بدرجة مرتفعة ، وتتفق مع نتائج دراسة خوجة (٢٠٢٠م) التي توصلت إلى أن المحافظة على سرية المعلومات والوثائق الهامة في إدارات التعليم في المملكة جاءت بدرجة مرتفعة ، وأن التحكم في اتصال العاملين بالإنترنت جاء بدرجة مرتفعة.

عرض ومناقشة نتائج السؤال الثاني: ما الصعوبات التي تواجه تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية من وجهة نظر أعضاء هيئة التدريس فيها؟

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية ، والانحرافات المعيارية ، والرتب لاستجابات أفراد عينة الدراسة من أعضاء هيئة التدريس في جامعة الأمير سلطان على محور "صعوبات تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية" والجدول الآتي يوضح النتائج المتصلة بهذا المحور.

جدول (٨)

استجابات أفراد الدراسة على محور "صعوبات تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية"

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
٤	نقص الكوادر البشرية المؤهلة لتقديم الدعم الفني اللازم.	٣,٦٩	١,٠٠	١	مرتفعة
٦	ضعف البنية التحتية اللازمة لتطبيق تقنية الأمن السيبراني في الجامعة.	٣,٥٤	١,٣٢	٢	مرتفعة
٣	قلة البرامج التدريبية لمنسوبي الجامعة في مجال الأمن السيبراني.	٣,٥٢	١,٠٠	٣	مرتفعة
٢	قلة الصلاحيات الممنوحة لمنسوبي الجامعة للوصول إلى المعلومات السرية بما يتناسب مع مهامهم.	٣,٤٧	٠,٨٢	٤	مرتفعة
٨	قلة معرفة منسوبي الجامعة بأهمية الأمن السيبراني وآليات تعزيزه في الجامعة.	٣,٤٥	٠,٩٧	٥	مرتفعة
٩	ضعف تطبيق تبعات عدم التزام منسوبي الجامعة بضوابط الأمن السيبراني.	٣,٤٠	٠,٩٢	٦	متوسطة
٥	ضعف البرامج المستخدمة لحماية البيانات والمعلومات في الجامعة.	٣,٣٣	١,٠٤	٧	متوسطة
١٠	ضعف النظام الشبكي الآمن لتبادل المعلومات الإدارية داخل الجامعة.	٣,٢٧	١,٢٣	٨	متوسطة
٧	ضعف الميزانية المخصصة لشراء برامج حماية المعلومات في الجامعة.	٣,١٧	١,٢٠	٩	متوسطة
١	ضعف الدعم الفني للمشاكل المرتبطة بتقنية المعلومات.	٣,١١	١,٤٠	١٠	متوسطة
المتوسط الحسابي العام		٣,٤٠	٠,٦٦	متوسط	

يتضح من الجدول السابق أن هناك تفاوت في درجة موافقة أفراد الدراسة على عبارات محور (صعوبات تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية) ، حيث يشمل المحور (١٠) فقرات ، وجاءت استجابات أفراد الدراسة على فقرات المحور بدرجات موافقة تتراوح ما بين (متوسطة/ مرتفعة) على أداة الدراسة ، حيث تراوحت المتوسطات الحسابية من (٣,١١ إلى ٣,٦٩) ، وهذه المتوسطات تشير إلى درجة موافقة (متوسطة/ مرتفعة) بالنسبة إلى أداة الدراسة.

ومن النتائج الموضحة في الجدول أظهرت نتائج المتوسطات الحسابية لعبارات المحور أن أعلى فقرة من حيث المتوسط الحسابي هي العبارة رقم (٤) ، ونصّها: "نقص الكوادر البشرية المؤهلة لتقديم الدعم الفني اللازم" بالمرتبة الأولى ، وبدرجة موافقة (مرتفعة) ، بمتوسط حسابي (٣,٦٩) وانحراف معياري (١,٠) ، تليها في المرتبة الثانية العبارة رقم (٦) ، ونصّها: "ضعف البنية التحتية اللازمة لتطبيق تقنية الأمن السيبراني في الجامعة" بدرجة موافقة (مرتفعة) ، بمتوسط حسابي (٣,٥٤) وانحراف معياري (١,٣٢).

بينما جاءت العبارة رقم (٧) ، ونصّها: "ضعف الميزانية المخصصة لشراء برامج حماية المعلومات في الجامعة" بالمرتبة التاسعة وبدرجة موافقة (متوسطة) ، بمتوسط حسابي (٣,١٧) وانحراف معياري (١,٢٠) ، وفي المرتبة الأخيرة جاءت العبارة رقم (١) ، ونصّها: "ضعف الدعم الفني للمشاكل المرتبطة بتقنية المعلومات" بدرجة موافقة (متوسطة) ، بمتوسط حسابي (٣,١١) وانحراف معياري (١,٤٠).

ونستخلص مما سبق أن المتوسط العام لاستجابات أفراد الدراسة على عبارات محور (صعوبات تحقيق الأمن السيبراني في جامعة الأمير سلطان الأهلية) قد بلغ (٣,٤٠ درجة من ٥) ، وهذا المتوسط يشير إلى درجة موافقة (متوسطة) بالنسبة لأداة الدراسة ، وهكذا يتضح أن أفراد الدراسة يرون أن أبرز صعوبات تحقيق الأمن السيبراني في جامعة الأمير سلطان الأهلية تتمثل في: (نقص الكوادر البشرية المؤهلة لتقديم الدعم الفني اللازم ، بالإضافة إلى ضعف البنية التحتية اللازمة لتطبيق تقنية الأمن السيبراني في الجامعة ، وقلة البرامج التدريبية لمنسوبي الجامعة في مجال الأمن السيبراني ، وقلة الصلاحيات الممنوحة لمنسوبي الجامعة للوصول إلى المعلومات السرية بما يتناسب مع مهامهم).

يتضح مما سبق أن هناك صعوبات تقف أمام الإدارة الجامعية في سبيل تحقيقها لمتطلبات الأمن السيبراني نظرًا لظروف وتحديات في بيئة العمل عديدة ولعل أبرزها: عدم قدرة الإدارة الجامعية على استقطاب كفاءة بشرية مؤهلين لدعم بيئة الأمن السيبراني ، خاصة في ظل نقص الأدوات التقنية الحديثة اللازمة لتفعيل بيئة أمنية مثالية للمعلومات ، كما أن الإدارة الجامعية لا تستطيع توفير برامج تدريبية حديثة متطورة لارتفاع تكلفة إعدادها وعدم وجود متخصصين لإدارتها ، كما أن الإدارة الجامعية لا تمنح الصلاحيات المناسبة إلا لعدد محدد من المنسوبين للوصول إلى المعلومات السرية المتعلقة بأنشطة ومهام الجامعة ، ولعل أكبر تحدى يواجه الإدارة

الجامعية هو ضعف نشر ثقافة الأمن السيبراني بين المنسوبين ، وقلة المعرفة بالآليات اللازمة لتفعيل الأمن السيبراني ، كما أن الإدارة الجامعية لا تستطيع توطين برامج حديثة لحماية بيناتها ومعلوماتها لرفع تكلفتها ، وضعف ميزانيات المخصصة لتطوير المستمر.

وتتفق هذه النتائج مع دراسة Mahno (2017) التي توصلت إلى أن تنظيم دورات تدريبية في الأمن السيبراني لطلاب السنة الأولى غير المتخصصين في تكنولوجيا المعلومات بجمهورية أستونيا جاء بدرجة منخفضة جدًا.

عرض نتائج السؤال الثالث ومناقشته: ما المقترحات التي يمكن أن تسهم في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية من وجهة نظر أعضاء هيئة التدريس فيها؟

للإجابة عن هذا السؤال تم حساب المتوسطات الحسابية ، والانحرافات المعيارية ، والرتب لاستجابات أفراد عينة الدراسة من أعضاء هيئة التدريس في جامعة الأمير سلطان على محور "المقترحات التي يمكن أن تسهم في تحقيق الأمن السيبراني في جامعة الأمير سلطان الأهلية" والجدول الآتي يوضح النتائج المتصلة بهذا المحور.

جدول (٩)

استجابات أفراد الدراسة على محور "المقترحات التي يمكن أن تسهم في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية"

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
٩	منع استخدام البرامج غير المرخصة على أجهزة الحاسب في الجامعة.	٤,١٧	٠,٩٦	١	مرتفعة
١٠	متابعة تحديث برامج الحماية لأجهزة الحاسب الآلي دوريًا في الجامعة.	٣,٨٥	٠,٧٢	٢	مرتفعة
١	متابعة تغيير كلمات المرور بضوابط ذات مستوى عالٍ من الأمان.	٣,٧٧	١,٠١	٣	مرتفعة
٢	السماح لمنسوبي الجامعة فقط بالوصول إلى شبكة الإنترنت الخاصة من خلال حمايتها بكلمة مرور.	٣,٧٥	١,٠٤	٤	مرتفعة
٨	متابعة تحديث أنظمة التشغيل لأجهزة الحاسب الآلي دوريًا في الجامعة.	٣,٦١	٠,٨٦	٥	مرتفعة
٣	تقييد الوصول إلى المواقع غير الموثوقة على شبكة الإنترنت.	٣,٥٨	١,٠٤	٦	مرتفعة
٦	تكوين لجنة خاصة على مستوى الوحدات الإدارية والأكاديمية لمتابعة التزام منسوبي الجامعة بتحقيق ضوابط الأمن السيبراني في الجامعة.	٣,٥٤	١,٢٥	٧	مرتفعة
٤	التأكيد على عمل نسخ إلكترونية احتياطية للبيانات وكافة المعلومات التي تُخزّن دوريًا.	٣,٤٢	١,٠١	٨	مرتفعة

م	العبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
٥	نشر واجبات منسوبي الجامعة في تحقيق الأمن السيبراني ومسؤولياتهم.	٣,٤٢	١,١٨	٩	مرتفعة
٧	تنظيم دورات تدريبية لإكساب منسوبي الجامعة مهارات تحقيق الأمن السيبراني.	٣,٣٥	١,٢٦	١٠	متوسطة
المتوسط الحسابي العام		٣,٦٥	٠,٨٥	مرتفع	

يتضح من الجدول السابق أن هناك تقارب في درجة موافقة أفراد الدراسة على عبارات محور (المقترحات التي يمكن أن تسهم في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية) ، حيث يشمل المحور (١٠) فقرات وجاءت استجابات أفراد الدراسة على فقرات المحور بدرجات موافقة تتراوح ما بين (متوسطة/ مرتفعة) على أداة الدراسة ، حيث تراوحت المتوسطات الحسابية من (٣,٣٥ إلى ٤,١٧) ، وهذه المتوسطات تشير إلى درجة موافقة (متوسطة/ مرتفعة) بالنسبة لأداة الدراسة.

ومن النتائج الموضحة في الجدول أظهرت نتائج المتوسطات الحسابية لعبارات المحور أن أعلى فقرة من حيث المتوسط الحسابي هي العبارة رقم (٩) ، التي تنصّ على: "منع استخدام البرامج غير المرخصة على أجهزة الحاسب في الجامعة" بالمرتبة الأولى وبدرجة موافقة (مرتفعة) ، بمتوسط حسابي (٤,١٧) وانحراف معياري (٠,٩٦) ، تليها في المرتبة الثانية العبارة رقم (١٠) التي تنصّ على: "متابعة تحديث برامج الحماية لأجهزة الحاسب الآلي دوريًا في الجامعة" بدرجة موافقة (مرتفعة) ، بمتوسط حسابي (٣,٨٥) وانحراف معياري (٠,٧٢).

بينما جاءت العبارة رقم (٥) التي تنصّ على: "نشر واجبات منسوبي الجامعة في تحقيق الأمن السيبراني ومسؤولياتهم" في المرتبة التاسعة وبدرجة موافقة (مرتفعة) ، بمتوسط حسابي (٣,٤٢) وانحراف معياري (١,١٨) ، وفي المرتبة الأخيرة جاءت العبارة رقم (٧) التي تنصّ على: "تنظيم دورات تدريبية لإكساب منسوبي الجامعة مهارات تحقيق الأمن السيبراني" بدرجة موافقة (متوسطة) ، بمتوسط حسابي (٣,٣٥) وانحراف معياري (١,٢٦).

ونستخلص مما سبق أن المتوسط العام لاستجابات أفراد الدراسة على عبارات محور (المقترحات التي يمكن أن تسهم في تحقيق الأمن السيبراني في جامعة الأمير سلطان الأهلية) قد بلغ (٣,٦٥ درجة من ٥) ، وهذا المتوسط يشير إلى درجة موافقة (مرتفعة) بالنسبة لأداة الدراسة. وهكذا يتضح أن أفراد الدراسة يرون أن أبرز المقترحات التي يمكن أن تسهم في تحقيق الأمن

السيبراني في جامعة الأمير سلطان الأهلية تتمثل في: (منع استخدام البرامج غير المرخصة على أجهزة الحاسب في الجامعة ، ومتابعة تحديث برامج الحماية لأجهزة الحاسب الآلي دوريًا في الجامعة ، ومتابعة تغيير كلمات المرور بضوابط ذات مستوى عالٍ من الأمان).

ويتضح مما سبق أنه على الإدارة الجامعية في سبيل التغلب على صعوبات تطبيق الأمن السيبراني بشكل جيد ، يجب أن تتخذ المزيد من الإجراءات والفاعليات والأنشطة الضرورية للحصول على الأمن المعلوماتي الذي يضمن الحفاظ على سرية معلوماتها وبياناتها من الاختراق من أي مصدر خارجي مجهول يؤدى إلى الإضرار بأنظمتها الإدارية والتعليمية والمالية؛ ولعل أبرزها: وضع أنظمة ولوائح مشددة لمنع أي منسوبيها من استخدام البرامج غير المسموح له باستخدامها على أجهزة الجامعة الخاصة لعدم انتشار الفيروسات المدمرة لملفات البيانات والمعلومات الأساسية ، كما يتطلب ذلك توفير ميزانية مناسبة خاصة بتطوير وتحديث برامج الحماية بشكل دوري حسب التطور التقني الحديث ، وتفعيل نظم لكلمات المرور معقدة يصعب اختراقها من متسللين ، وايضًا فرض قيود على المنسوبين في دخول مواقع الإنترنت مجهولة المصدر أو غير معتمدة للحفاظ على قواعد البيانات الخاصة بالجامعة.

التوصيات والمقترحات:

قدّم الباحث أثناء نتائج بحثه مجموعة من التوصيات الآتية:

- تكثيف البرامج التدريبية لتطوير الكوادر البشرية المؤهلة؛ لتقديم الدعم الفني اللازم في مجال الإدارة الإلكترونية والأمن السيبراني.
- زيادة الصلاحيات الممنوحة لمنسوبي الجامعة للوصول إلى المعلومات السرية بما يتناسب مع مهامهم.
- تقديم ورش عمل وندوات ومحاضرات على نحوٍ مكثّف ومستمر ، وتستهدف منسوبي الجامعة والمستفيدين من خدماتها؛ لزيادة الوعي بأهمية الأمن السيبراني وآليات تعزيزه.
- تكليف فريق عمل ذي مهارات عالية يعمل دوريًا على تحديث برامج الحماية وأنظمة التشغيل لأجهزة الحاسب الآلي في الجامعة.
- حث منسوبي الجامعة على تغيير كلمات المرور بضوابط ذات مستوى عالٍ من الأمان.
- استخدام آلية فعالة لعمل نسخ إلكترونية احتياطية للبيانات ، وكافة المعلومات التي تُخزّن بصورة دورية.

قائمة المصادر و المراجع

المراجع العربية:

إبراهيم ، صديق. (٢٠١٨م). أثر خصائص نظم أمن المعلومات على قدرات التعلم التنظيمية في الجامعات الأردني. *مجلة العلوم الاقتصادية والإدارية والقانونية* ، ٢ (١٢) ، ١-٢٥.

البار ، عدنان ، والسميري ، عيسى. (٢٠١٩م). *أساسيات الأمن السيبراني*. الرياض: دار كنترول بي للنشر.

جبور ، منى. (٢٠١٦م). *السيبرانية هاجس العصر*. بيروت: المركز العربي للبحوث القانونية والقضائية.

حمودة ، بهاء. (٢٠١٤م). سياسة أمن المعلومات في شبكة المكتبات بجامعة النيلين. *المجلة العربية الدولية المعلوماتية* ، ٣ (٥) ، ٥٥-٦٢.

خوجة ، هيفاء. (٢٠٢٠م). *التطوير التنظيمي في إدارات التعليم بالمملكة العربية السعودية تحقيق المتطلبات الإدارية الداعمة للأمن السيبراني:* استراتيجية مقترحة. رسالة دكتوراه غير منشورة ، جامعة الملك سعود ، الرياض.

الشايع ، خالد. (٢٠١٩م). *الأمن السيبراني مفهومه وخصائصه وسياساته*. القاهرة: الدار العالمية للنشر والتوزيع.

شلوش ، نورة. (٢٠١٨م). القرصنة الإلكترونية في الفضاء السيبراني: التهديد المتصاعد لأمن الدول ، *مجلة مركز بابل للدراسات إنسانية* ، ٨(٢) ، ١٨٥-٢٠٦.

الشوابكة ، عدنان. (٢٠١٩م). دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف ، *مجلة دراسات وأبحاث* ، ١١(٤) ،١٦٤-١٨٧.

الصحفي ، تهاني. (٢٠١٩م). *متطلبات تحقيق الأمن السيبراني للازمة لأنظمة المعلومات الإدارية بالجامعات الحكومية السعودية في مدينة الرياض*. رسالة ماجستير غير منشورة ، كليات الشرق العربي ، الرياض.

عبد الواحد ، آن. (٢٠١٥م). *سياسات أمن المعلومات وعلاقتها بفاعلية نظم المعلومات الإدارية في الجامعات الفلسطينية قطاع غزة*. رسالة ماجستير غير منشورة ، كليات الشرق العربي ، الرياض.

عبدالحي ، رمزي. (٢٠٠٧م). *تقييم أداء الإدارة الجامعية في ضوء إدارة الجودة الشاملة*. الإسكندرية: دار الوفاء للطباعة والنشر.

العريشي ، جبريل. (٢٠١٨م). دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع. مجلة مكتبة الملك فهد الوطنية ، ٢٤(٢) ، ٣٠٢-٣٧٢.

القحطاني ، عبد الله. (٢٠١٧م). إدارة أمن المعلومات ودورها في الحد من الإرهاب الإلكتروني بكلية الحاسبات وتقنية المعلومات بجامعة الملك عبد العزيز بجدة. رسالة ماجستير غير منشورة ، جامعة نايف للعلوم الأمنية ، الرياض.

مظلوم ،محمد. (٢٠١٨م). مفهوم القوة السيبرانية ،*مجلة كلية الملك خالد العسكرية* ، ١(١٣٣) ، ٨٤-٨٩.

المملكة العربية السعودية. (٢٠١٦م). *رؤية المملكة العربية السعودية ٢٠٣٠* . تم الاسترجاع من موقع: https://vision2030.gov.sa/download/file/fid/422

نشوان ، يعقوب. (١٩٨٥م). *الإدارة والإشراف التربوي*. دار الفرقان للنشر والتوزيع ، الأردن.

الهيئة الوطنية للأمن السيبراني. (٢٠٢٠م). *الضوابط الأساسية للأمن السيبراني* ، تم الاسترجاع من موقع: https://nca.gov.sa/files/ecc-ar.pdf

وزارة التعليم. (٢٠١٩م). *التعليم ورؤية ٢٠٣٠* . تم الاسترجاع من موقع: https://www.moe.gov.sa/ar/pages/vision2030.aspx

المراجع العربية المترجمة: (Arabic references in English)

Abdulhai , R. (2007). *Evaluating The Performance of University Management in The Light of Comprehensive Quality Management.* Alexandria: Alwafa Printing and Publishing.

Abdulwahid , A. (2015). *Information Security Policies and Their Relationship to The Effectiveness of Administrative Information Systems in Palestinian Universities in The Gaza Strip.* Unpublished Master's , Arab East Colleges , Riyadh.

Alarishi, J. (2018). The Role of Higher Education Institutions in Promoting a Culture of Information Security in Society. *Journal King Fahd National Library*, (2)24, 302-372.

Albar, A. & Alsamiri, I. (2019). *Cybersecurity Essentials*, Control P Publisers.

Alqahtani, A. (2017). *The Department of Information Security and Its Role in Reducing Cyberterrration at The Faculty of Computers and Information Technology at King Abdul-Aziz University.* Unpublished Masters, Nayef University of Security Sciences, Riyadh.

Alsahfey, T. (2019). *Requirements for Achieving Cybersecurity Crisis for Management Information Systems at Saudi Government Universities in Riyadh.* Unpublished Masters, Arab East Colleges, Riyadh.

Alshaya, K. (2019). *Cybersecurity Concept, Characteristics and Policies.* Cairo: Global Publishing and Distribution.

Alshuwabakia, A. (2019). The Role of Information Security Measures in Reducing Information Security Risks at Taif University. *Journal of Studies and Research*, 11(4), 164-187.

Hamouda, B. (2014). Information Security Policy in The Library Network at Nilen University. *Arab International Journal of Informatics*, 3(5).55-62.

Ibrahim, F. (2018). The Impact of the Characteristics of Information Security Systems on Organizational Learning Capabilities in Jordanian Universities. *Journal of Economic, Administrative and Legal Sciences*, 2(12), 1-25.

Jabbour, M. (2016). *Cyber Obsession of the Times*. Arab Center for Legal and Judicial Research.

Khoja, H. (2020). *Organizational Development in Education Departments in Saudi Arabia to Meet the Administrative Requirements Supporting Cybersecurity: Proposed Strategy*, Unpublished PhD Thesis, King Saud University, Riyadh.

Mathlaoum, M. (2018), Concept of Cyber Power, *Journal of King Khalid Military College*,1(133),84-89.

Ministry of Education. (2019). *Education and Vision 2030*. Retrieved From: Https://Www.Moe.Gov.Sa/Ar/Pages/Vision2030.Aspx

Nashwan, Y. (1985) *Department and Educational Supervision.* Jordan: Alfurqan Publishing and Distribution.

National Cybersecurity Authority. (2020). *Basic Cybersecurity Controls.* Retrieved From: Https://Nca.Gov.Sa/Files/Ecc-Ar.Pdf

Saudi Arabia, (2016). *Saudi Arabia Vision 2030*. Retrieved From Https://Vision2030.Gov.Sa/Download/File/Fid/422

Shaloush, N. (2018). Cyber Piracy: The Escalating Threat to State Security. *Babel Center for Humanities Journal*, 82,185-206.

المراجع الأجنبية: References

I.T.U. (The International Telecommunication Union). (2020). *Definition Of Cybersecurity*. Retrieved From: Https://Www.Itu.Int/En/ITU-T/StudYgroups/Com17/Pages/Cybersecurity.Aspx

Krejcie, R. & Morgan, D. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, (30),607-610.

Mahono D. (2017). *Design of The Cyber Security Awareness Program for First-Year Students Who Are Not IT Professionals in The Republic of Estonia*, Master's Thesis, Tallinn University of Technology Faculty of Information Technology.

Mowbray, T. (2014). *Cybersecurity Managing Systems, Conducting Testing, And Investigating Intrusions.* Indiana: John Wiley & Sons, Inc. Retrieved From:Https://Books.Google.Com.Sa/Books?Id=Gxhbaqaaqbaj&printsec

=Frontcover&Dq=Cybersecurity+Managing+Systems,+Conduction+Testing,+And+Intrusions&Hl=Ar&Sa=X&Ved=2ahukewisspdy8czqahuh8hqkhbauclkq6aewahoecaiqag#V=Onepage&Q=Cybersecurity%20Managing%20Systems%2C%20Conducting%20Testing%2C%20and%20Investigating%20Intrusions&F=False

Zec, M. & Kajtazi, M. (2015). Examining How IT Professionals in Smes Take Decisions About Implementing Cyber Security Strategy. *Paper Presented at Ecime 2015 - 9th European Conference*, UK, September 2122 ,2015. Retrieved from: Https://Www.Researchgate.Net/ Publication/ 338149057_Examining_How_IT_Professionals_In_Smes_Take_Decisions_About_Implementing_Cyber_Security_Strategy.