المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثلاثون شهر(11) 2020

دور إدارة الجامعات السعودية الحكومية في تحقيق الأمن السيبراني
بحث مستل من رسالة دكتوراه

إعداد:
د. فاطمة بنت عبد الله الشبانات
دكتوراه إدارة التعليم العالي من كلية التربية بجامعة الملك سعود بالمملكة العربية السعودية
معلمة بوزارة التعليم بالمملكة العربية السعودية
falshabanat@gmail.com

The role of administration of Saudi government universities in achieving cyber security
Research extracted from a PhD thesis

by
Fatimah Abdullah Alshabanat
PhD in Higher Education administration from College of Education in King Saud University in Saudi Arabia
Teacher in Ministry of Education in Saudi Arabia

المجلة الإلكترونية الشاملة متعددة التخصصات
العدد الثلاثون شهر(11) 2020

المستخلص: هدفت هذه الدراسة إلى تحديد واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، من خلال المجالات التالية (التخطيط، التنظيم، التوجيه، التقويم)، وتحديد معوقات تحقيقها للأمن السيبراني، والكشف عن المخاطر المحتملة لانتهاك الأمن السيبراني التي يمكن أن تواجهها، وتم استخدام المنهج المزجي، وتوصلت الدراسة إلى عدة نتائج، من أهمها ما يلي:

- جاءت موافقة عينة الدراسة على واقع ممارسة إدارة الجامعات السعودية الحكومية لدورها في تحقيق الأمن السيبراني بدرجة عالية، حيث أتى مجال التنظيم بالمرتبة الأولى، يليه مجال التقويم بالمرتبة الثانية، وبالمرتبة الثالثة مجال التخطيط، وفي الأخير جاء مجال التوجيه كأقل المجالات من حيث ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني.
- جاءت موافقة أفراد الدراسة المستهدفون بالمقابلة على واقع ممارسة إدارة الجامعات السعودية الحكومية لدورها في تحقيق الأمن السيبراني بدرجة عالية، حيث أتى مجال التقويم أولًا، ثم مجالي التخطيط والتنظيم ثانيًا، ثم مجال التوجيه ثالثًا.

المصطلحات الأساسية: الإدارة التربوية، إدارة الجامعات، إدارة التعليم العالي، الأمن السيبراني، الأمن الإلكتروني.

Abstract: This study aimed to identify the practice reality of universities administration for its role in achieving cybersecurity, through the following fields (planning, organizing, directing, evaluating, and identifying obstacles to achieving cybersecurity, and discovering potential risks of cybersecurity violations that may be faced, the mixed method is used, and the study reached several results, the most important of which are the following:

- The approval of the study sample on practice reality of universities administration for its role in achieving cybersecurity came with a high degree, where the field of organization came first, followed by the field of evaluation at the second place, and the third place in the field of planning, and in the last came the field of guidance as the least areas in terms of the practice of universities administration for its role in achieving cyber security.
- The approval of the targeted study individuals in the first interview on the practice reality of university administration for its role in achieving cybersecurity came with a high degree, where the field of evaluation came first, followed by the fields of planning and organization at the second place, and the third place in the field of guidance.

Keywords: Educational Administration, Universities Administration, Higher Educational Administration, Cyber Security, Electronic Security.

المقدمة

إن التقدم التقني الذي يعيشه العالمُ اليومَ من خلال الثورة التقنيةِ في مختلف المجالات يعد ذا أهمية فائقة في دفع عجلة اقتصادات الدول، لتحقيق موقع مرموق في المشهد العالمي؛ إذ تنطلق الاتجاهات العالمية المعاصرة إلى زيادة الاعتماد على التقنيات الحديثة في كافة نواحي الحياة، وهو ما يُشار إليه بـ "التحول الرقمي".

وفي الوقت الراهن، يعدُّ التحولُ الرقمي ضرورةً لا خيارًا أمام إدارة الجامعات الطامحة للتطوير وتحقيق الجودة؛ عن طريق تبسيط أسلوب العمل، وتقديم الخدمات بصورة سريعة، وجودة عالية، وتكلفة منخفضة في جميع تعاملاتها الداخلية والخارجية؛ لتحقيق رسالتها ورؤيتها بصورة سلسة تتلاءم مع متطلبات العصر، ودواعيه.

ورغم الفوائد الكبيرة للتحول الرقمي للجامعات في تعاملاتها الإدارية والأكاديمية، إلا أنها قد تنطوي على مخاطر عديدة، ومخاوف حقيقية؛ مما يزيد من عبء المسؤولية على إدارة الجامعات في المحافظة على هذه

المعلومات الرقمية، بما يحقق لها البيئة الملائمة للإنتاج والعمل؛ فالموازنة بين عمليات التحول الرقمي وعمليات الأمن السيبراني، يسهم في الحفاظ على بياناتها ومعلوماتها الرقمية، من العبث أو التلف.

وقد تم استخدام مصطلح "الأمن السيبراني" منذ أكثر من ثلاثة عقود مضت، ويعني العمليات التي تختص بحماية أنظمة المعلومات والاتصالات، والمعلومات المتضمنة فيها، والدفاع عنها ضد التلف، أو الاستخدام، أو التعديل، أو الاستغلال غير المصرح به (National Initiative for Cyber Security Careers and Studies, 2018)، وتبرز العلاقة بين الأمن السيبراني وإدارة الجامعات في كونها تواجه تحديًا متناميًا من التهديدات الأمنية السيبرانية المتقدمة، والمستمرة، والمستهدفة؛ نظرًا لتنوع الأنشطة الإلكترونية التي تقدمها الجامعات، الأمر الذي قد يُعيقُ مساهمةَ هذه المؤسسات في الابتكار، والتنمية الاقتصادية، لذا فإن الإدارة الفعّالة لهذه التهديدات المختلفة أصبحت أساسية بشكل متزايدٍ لنجاح مؤسسات التعليم العالي (Universities UK, 2013).

وقد نصت مبادرات برنامج التحول الوطني 2020 الخاصة بوزارة التعليم في المملكة العربية السعودية على عدة مبادرات تخدم هدف التحول الرقمي (مبادرة رقم 2 و25، و33)، وهي على التوالي: التحول نحو التعليم الرقمي لدعم تقدم الطالب والمعلم، إنشاء وتطوير نظام خدمات المعلومات الرقمية، منظومة الخدمات الإلكترونية الجامعية «جامعة» (برنامج التحول الوطني 2020، 2016، ص ص 104-105) مما يجعل من التهديدات السيبرانية المرافقة لهذا التحول الرقمي تحديًا متقدمًا، ومعقدًا ومستمراً في النمو؛ يتزايد مع نمو معلوماتها الرقمية، ودرجة اعتمادها على التقنيات الحديثة في الإدارة، والبحث، والتدريس.

أما الخطة المستقبلية للتعليم الجامعي في المملكة «آفاق»، والتي تمتدُّ حتى عام 1450هـ-2029م، فقد نصّت على العديد من الأهداف الداعمة لتقنية المعلومات، وتشمل الأهداف (17، 18، 19)، وهي على التوالي: توفير شبكة اتصال فائقة السرعة ومنخفضة التكلفة بين مؤسسات التعليم الجامعي مرتبطة بالشبكة العالمية، المواءمة والتكامل بين إستراتيجيات تقنية المعلومات والأنظمة والتطبيقات التعليمية والبحثية والإدارية في مؤسسات التعليم الجامعي، إنتاج ونشر محتوًى معرفيٍّ رقميٍّ في كافة المجالات متاحًا لمنسوبي التعليم العالي والمجتمع (وزارة التعليم العالي، 2011، ص ص 22-23). وهذه الأهداف تؤكد على ضرورة التحول الرقمي وفق مؤشرات أداء دقيقة، مما يزيد العبء على إدارة الجامعات في تحقيق الأمن السيبراني في جميع عملياتها الإدارية، بِناءً على هذه المتغيرات التقنية المتسارعة.

ونظراً لتوجه الجامعات السعودية الحكومية للتحول نحو بيئات التعلم المفتوحة، والتي تستلزم توفير المعلومات للباحثين والطلاب، وإتاحة مصادر التعلم المختلفة، والتحول الرقمي في المعاملات الإدارية، فإن هذا التوجُّه سيُشكّل تحديًا أمنيًا كبيرًا في المحافظة على هذه المعلومات الرقمية، بما يحقق المبادئ الثلاثة التي ذكرها هندرسون (Henderson, 2019): "سرية المعلومة (Confidentiality)، ونزاهة المعلومة (Integrity)، وتوفّر المعلومة (Availability)".

وانطلاقًا من أهمية التحول الرقمي للجامعات، وفق رؤية المملكة 2030، وما يستلزم من ضرورة توفير بيئة إلكترونية آمنة ومستدامة، داعمة للابتكار والتطوير، جاءت هذه الدراسة؛ للكشف عن دور إدارة الجامعات السعودية الحكومية في تحقيق الأمن السيبراني.

مشكلة الدراسة

رغم أهمية التحول الرقمي، واستخدام تقنيات الاتصالات والمعلومات في الجامعات السعودية الحكومية، والتي نصّت رؤية المملكة العربية السعودية 2030 على تعزيزه، من خلال "حوكمة التحول الرقمي عبر مجلس وطني يُشْرفُ على هذا المسار، مع دعم هذا التحول على مستوى الحكومة، وتهيئة الآلية التنظيمية، والدعم المناسب، وبناء الشراكات الفاعلة لذلك" (رؤية المملكة العربية السعودية 2030، 2016، ص 53)، إلا أن هذا الهدف لا يُعدُّ هدفًا نهائيًا يمكن التوقفُ عنده؛ إذ إن المحافظة على هذه المعلومات الرقمية من التهديدات الداخلية والخارجية هو الهدف الأكبر، وهو ما يمكن أن يُسمَّى بـ"الأمن السيبراني".

لذا، فقد تلا ذلك صدور أمر ملكي بتاريخ 1439/2/11هـ، بإنشاء "الهيئة الوطنية للأمن السيبراني" كجهة مختصة، تَهدِفُ إلى تعزيز الأمن السيبراني لمؤسسات الدولة، وحماية مصالحها الحيوية، وأمنها الوطني، والبُنى التحتية الحساسة فيها، الذي يمكن اعتباره مرتكزًا أساسيًا لهذه الدراسة.

وفي مؤتمر عُقِد في جامعة الملك سعود تحت مسمى (حلول القيادة والسيطرة) لعامين متتاليين 2016-2017، هدف إلى تجسير العلاقة بين صُنّاع المعرفة في الجامعات، والمراكز البحثية، ومراكز التميز، وبين صُنّاع

القرار في القطاعات العسكرية والمدنية، والقطاع الخاص، والمؤسسات الحكومية، وقام على بَحْث التوجّهات والتطورات الحديثة في عدة مجالات؛ منها: القيادة، والأمن السيبراني، وخَلُص إلى عدة توصيات؛ من أهمها: دعوة مؤسسات المجتمع المدني إلى تبني وتكريس مفاهيم الصمود السيبراني ضمن الجهود الاستباقية، ودعم جهود البحث العلمي للأمن السيبراني، مع ضرورة العمل على إدخال مفاهيم الأمن السيبراني في المناهج الأكاديمية والتعليمية، والتأسيس لمراكز بحثية متخصصة، ومراكز تدريب المحاكاة للواقع، مع ضرورة تقديم الدعم الحكومي المستمر للمؤسسات؛ بما يُمكّنها من مواكبة التطورات التقنية الحديثة، وتوطين أنظمة حلول القيادة والسيطرة، مع إبقاء الأمن السيبراني بمنأى عن خطوات التقشف (مؤتمر حلول القيادة والسيطرة، 2016). مما يؤكد على ضرورة اتخاذ إجراءات دقيقة وسريعة من قِبَلِ إدارة الجامعات تتلاءم مع متطلبات المرحلة الحالية.

كما أوصى المنتدى الدولي للأمن السيبراني في بيان الرياض للأمن السيبراني (2020) بتحفيز صناعة مزدهرة للأمن السيبراني من خلال الابتكار، والاستثمار من أجل مواجهة المخاطر السيبرانية المتجددة، ودَعْمِ تطوير كوادر عالمية مؤهلة في الأمن السيبراني تواكب متطلبات الاقتصاد العالمي المرتكز على التقنية، مع أهمية تعزيز مشاركة المرأة ضمن تلك الكوادر في مجال الأمن السيبراني، وتثقيف المجتمعات لتكون واعية ومسؤولة سيبرانيًا من خلال تمكين مختلف الأطراف ذات التأثير في المجتمع لتحقيق ذلك، والتعاون والعمل المشترك لمكافحة الجرائم السيبرانية بكافة أنواعها، مع التركيز على وسائل لتثقيف وحماية الأطفال في الفضاء السيبراني، وتطوير الصمود السيبراني على المستوى الدولي من خلال تسخير التقنيات الناشئة والشراكات بين القطاعين العام والخاص للحد من المخاطر السيبرانية، وتعزيز قدرات سيبرانية عالمية وشاملة من خلال التعاون الدولي، مع التركيز على دعم الاقتصادات الناشئة في ذلك.

وقد توصلت دراسة الردفاني (2014) إلى وجود انفلات أمني في مجال الفضاء السيبراني، حيث شكل منظومة تهديدات ومخاطر ومعوقات تجاه تحقيق الأمن، كما تعد الجرائم السيبرانية ذات خطر يؤدي إلى تفاقم الفساد وتقويض سيادة القانون والعمليات الديموقراطية وتهديد أمن المجتمع والدول. كما أشارت دراسة أبو زيد (2019) إلى أثر الهجمات السيبرانية على المملكة العربية السعودية، التي كان أبرزها الهجمات التي استهدفت شركة أرامكو السعودية في عام 2012 وأدت إلى تعطيل نشاط الشركة لمدة شهر، كما تسببت هذه البرمجيات الخبيثة في حدوث خلل مرة أخرى في نوفمبر 2016 ويناير 2017. كما توصلت دراسة الشمري (2015) إلى أن الإجراءات التي اتخذتها المملكة العربية السعودية لحماية فضائها الإلكتروني من خطر التعرّض للهجمات الإلكترونية ليست كافية، وليست فعّالة. إلا أن هذه الدراسة لم تُطبّق في قطاع التعليم العالي؛ مما يستلزم إجراء المزيد من الدراسات في قطاع التعليم العالي؛ لتحديد أوجه القصور بشكل دقيق، والمسارعة في معالجتها؛ فعلى حدّ علم الباحثة لا توجد دراسات عربية سابقة حول إدارة الأمن السيبراني في الجامعات، ويُؤمَّل أن تكون هذه الدراسة رائدةً في هذا المجال.

وفي دراسة استطلاعية قامت بها الباحثة من خلال مقابلة (17) فردًا من العاملين في مجال تقنية المعلومات بالجامعات -موضع الدراسة- ومسح المواقع الإلكترونية للجامعات السعودية الحكومية؛ كان من أبرز نتائجها: وجود بعض المؤشرات التي تدل على قصور العمليات الإدارية التي تسهم في تحقيق الأمن السيبراني بالجامعات، كالنقص الحاد في الكوادر البشرية المتخصصة في مجال الأمن السيبراني، وعدم وجود إدارة مختصة بالأمن السيبراني ضمن هيكلة العمادة/المركز المختص بتقنية المعلومات، وضعف البرامج التوعوية بالأمن السيبراني لمنسوبي الجامعات، وعدم وجود قنوات رسمية للإبلاغ عن التهديدات السيبرانية، وضعف البرامج التدريبية المتخصصة في الأمن السيبراني.

وارتكازًا على توصيات المؤتمرات والمنتدى الدولي، ونتائج الدراسات السابقة، ونتائج المسح الأوليّ، واهتمام الجامعات المتقدمة بتحقيق الأمن السيبراني في ضوء ضرورة التحول الرقمي، فإن مشكلة الدراسة تتلخص في ضرورة الكشف عن دور إدارة الجامعات السعودية الحكومية في تحقيق الأمن السيبراني؛ نظرًا لحداثة الموضوع، وندرة الدراسات السابقة في هذا المجال.

أهداف الدراسة

سعت هذه الدراسة لتحقيق الأهداف التالية:

1. تحديد واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط.
2. تحديد واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم.
3. تحديد واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه.
4. تحديد واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم.

أهمية الدراسة

تلخصت أهمية الدراسة في الجانبين التاليين:

أولًا: الأهمية النظرية

اكتسبت الدراسة الحالية أهميتها النظرية من خلال ما يلي:

1. تنطوي هذه الدراسة على أهمية تتعلق بضرورة توفير السرية والنزاهة والإتاحة؛ للمعلومات الإلكترونية المضافة على الشبكة العالمية من قبل منسوبي الجامعات.
2. يعد هذا الموضوع من الموضوعات المهمة والمستجدة في ساحة التعليم العالي، خصوصًا في ظِلّ اهتمام الدولة بدعم الأمن السيبراني عبر هيئة مختصة باسم (الهيئة الوطنية للأمن السيبراني)، بهدف تعزيز الأمن الإلكتروني لمنظمات الدولة؛ لارتباطه بقضية التحول الرقمي، الذي تهدف إليه رؤية المملكة 2030 وما يترتب على ذلك من ضرورة توفير الضمانات الأمنية لحماية وتنظيم البيئة السيبرانية.

ثانيًا: الأهمية العملية

اكتسبت الدراسة الحالية أهميتها العملية من خلال ما يلي:

1. يُؤمَّل أن تسهم هذه الدراسة في تقصي واقع ممارسة إدارة الجامعات؛ لدورها في تحقيق الأمن السيبراني، مما يوفر أساسًا لمعرفة جوانب القصور والخلل، ومن ثم الإسهام في تحسينها وتطويرها.
2. يُؤمَّل أن تسهم هذه الدراسة في التعرف على وجهات النظر المختلفة للقيادات ذات الاختصاص والعاملين في مجال أمن تقنية المعلومات بالجامعات السعودية الحكومية موضع الدراسة؛ مما يثري الدراسة بآليات للعمل ناتجة عن ممارسة حقيقية تُسهم في مساعدة أصحاب القرار في إدارة الجامعات السعودية لتحقيق الأمن السيبراني.

أسئلة الدراسة

سعت هذه الدراسة للإجابة عن الأسئلة التالية:

1. ما واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط.
2. ما واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم.
3. ما واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه.
4. ما واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم.

حدود الدراسة

تمثلت حدود الدراسة في الآتي:

أولًا: الحدود المكانية

تم تطبيق هذه الدراسة على الجامعات السعودية الحكومية التالية: جامعة الملك سعود، جامعة الملك عبد العزيز، جامعة الملك فهد للبترول والمعادن.

ثانيًا: الحدود الزمانية

تم تطبيق هذه الدراسة خلال العام الدراسي 1439-1440هـ.

أدبيات الدراسة

1. مفهوم الأمن السيبراني

السيبرانية مأخوذة من كلمة (Cyber)، وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسيبرانية تعني: فضاء الإنترنت (الربيعة، 2018).

ويأتي مصطلح الأمن السيبراني من كلمتي (Cyber Security)، وكلمة (سايبر) لاتينية الأصل، ومعناها الفضاء المعلوماتي، فيصبح المقصود بالأمن السيبراني أمن الفضاء المعلوماتي، الذي أصبح ركيزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول لمواجهة الحروب الإلكترونية (البار والمرحبي، 2018).

ويستخدم مصطلح الأمن السيبراني على نطاق واسع، وتعاريفه شديدة التباين، وغالبًا ما تكون لا موضوعية، وأحيانًا مبهمة، إذ إن عدم وجود تعريف موجز ومقبول على نطاق واسع يجسد تعدد أبعاد الأمن السيبراني، ويعرقل التقدم التقني والعلمي من خلال تعزيز النظرة الفنية السائدة للأمن السيبراني، مع فصل التخصصات التي ينبغي أن تعمل في تناسق لحل تحديات الأمن السيبراني المعقدة، لذا فإنه يمكن تعريف الأمن السيبراني بأنه: جمع وتنظيم الموارد والعمليات والبُنى المستخدمة لحماية الفضاء الإلكتروني وأنظمة تمكينه من الحوادث التي تسيء- بحكم القانون- إلى حقوق الملكية الفعلية (Craigen, Diakun-Thibault, & Purse, 2014).

كما يمكن تعريفه بأنه "وصف مجموعة الأدوات والسياسات والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات وآليات الضمان والتقنيات التي يمكن استخدامها في حماية توفر وسلامة وسرية الأصول في البنى التحتية الموصولة التابعة للحكومة والمنظمات الخاصة والمواطنين، وتشمل هذه الأصول أجهزة الحوسبة الموصولة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات والبيانات في البيئة السيبرانية" (The International Telecommunication Union, The World Bank, Commonwealth Secretariat, The Commonwealth Telecommunications Organisation, & NATO Cooperative Cyber Defence Centre of Excellence, 2018, p. 13).

ولقد عرّف تنظيم الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية الأمن السيبراني على أنه: "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحوها" (الهيئة الوطنية للأمن السيبراني، 2020).

2. أهمية الأمن السيبراني

يعد موضوع إدارة الأمن السيبراني من الموضوعات المعقدة، التي تتطلب اهتمامًا مؤسسيًا كبيرًا لكي تكون ذات فاعلية عالية، إذ لا تقتصر مسؤولية الأمن السيبراني على قسم تكنولوجيا المعلومات، وإنما من خلال العمل بشكل تعاوني عبر كامل المؤسسة (Bakertilly, 2018).

وتبين البحوث أنه ما بين عامي 2005 و2014، تم الإبلاغ عن وقوع 562 انتهاكًا للبيانات في 324 مؤسسة من مؤسسات التعليم العالي الأمريكية، وكانت الغالبية بنسبة (63 %) هي المؤسسات التي تمنح درجة الدكتوراه من مجموع المؤسسات المبلغ عنها (Grama, 2014)، وكانت القرصنة والبرامج الضارة والإفصاح غير المقصود أكثر أنواع الانتهاكات التي تم الإبلاغ عنها (U.S. Department of Homeland Security, 2015)، وعندما يتم تهديد مؤسسات التعليم العالي من قبل الهجمات أو التهديدات السيبرانية، فإن التأثير يتجاوز فقدان الطالب أو الموظف للمعلومات الشخصية، إذ يمكن أن تكون هناك آثار تشغيلية، أو تأثير على السمعة، أو على النواحي المالية، فضلًا عن الأمن القومي والمخاوف المتعلقة بالخصوصية، وهذا هو السبب في أن التخطيط للأمن السيبراني والتعليم والتدريب في غاية الأهمية ضمن الإطار العام للإدارة العليا لحالات الطوارئ، ومن حيث ضمان الامتثال للقوانين المحلية والفدرالية (Readiness and Emergency Management for Schools Technical Assistance Center, 2018).

3. أهداف الأمن السيبراني

يسعى الأمن السيبراني إلى ضمان تحقيق وصيانة الخصائص الأمنية للمنظمة وأصول المستخدمين ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية. تشتمل الأهداف الأمنية العامة على تحقيق السرية، والنزاهة، والتوفر للمعلومات والأنظمة الرقمية، ويمكن إيضاح ذلك كما يلي: (Farooq, Waseem, Khairi, &

Mazhar, 2015; Henderson, 2019; InfoSec Institute, 2018; Miorandi, Sicari, De (Pellegrini, & Chlamtac, 2012

- السرية: وهي القدرة على توفير الثقة للمستخدم حول خصوصية المعلومات الحساسة؛ باستخدام آليات مختلفة بحيث يتم منع الإفصاح عنها إلى الطرف غير المصرح به، ويمكن الوصول إليها من قبل المستخدمين المسموح بهم فقط.
- النزاهة: تحقق النزاهة التأكد من عدم العبث بالمعلومات عندما تنتقل من المصدر إلى الوجهة أو حتى عند تخزينها، إذ يجب حماية المعلومات المخزنة في النظم الأساسية، وقواعد البيانات، وما إلى ذلك، من خلال ضوابط النفاذ، وذلك للاحتفاظ بالمعلومات دقيقة ومتسقة ما لم يتم إجراء تغييرات مأذون بها.
- التوفر: ويقصد بها الحالة التي تكون فيها المعلومات متاحة في الوقت والمكان المناسبين، أي أن المعلومات يجب أن تكون متاحة عندما يحتاج المستخدمون المصرح لهم الوصول إليها. يتم الحفاظ على التوفر عندما تعمل جميع مكونات نظام المعلومات بشكل صحيح.

الدراسات السابقة

على حد علم الباحثة، لا تتوفر دراسات عربية حول إدارة الأمن السيبراني في مؤسسات التعليم العالي، لذا فإنه سيتم الاقتصار في ذلك على الدراسات الأجنبية، والتي يمكن تناولها من خلال مجالات الإدارة الأربعة: وهي (التخطيط والتنظيم والتوجيه والتقويم) في إدارة الأمن السيبراني، ويمكن تناول هذه المجالات الأربعة كما يلي:

1. الدراسات التي اهتمت بمجال التخطيط في إدارة الأمن السيبراني:

تناولت دراسة دياز وأندرسون، وولاك، وأوبدربيك (Diaz, Anderson, Wolak, & Opderbeck, 2017) الإجراءات والممارسات الواجب على مجلس الإدارة في مؤسسات التعليم العالي -بالولايات المتحدة الأمريكية- الالتزام بها؛ للتخفيف من المخاطر والتهديدات السيبرانية المتعلقة بإمكانية انتهاك البيانات، واستخدمت الدراسة المنهج الوصفي الوثائقي، وتوصَّلت -من خلال الأدب النظري- إلى أنه يجب على المؤسسات التعليمية في التعليم العالي اتخاذ خطوات استباقية لحماية معلوماتها الرقمية؛ نتيجة للتوسع في استخدام البدائل المستندة إلى التخزين السحابي للبيانات، الأمر الذي يتطلَّب التزامًا كبيرًا من الموارد؛ لتحقيق الإعداد، والتحليل، وصنع القرار في مجال الأمن السيبراني بشكل مدروس.

من جانب آخر اهتمت دراسة مالافت (Malavet, 2017)، بالتعرُّف على التهديدات السيبرانية الحالية، أو المحتملة، التي تواجه مؤسسات التعليم العالي، وأبرز التحديات التي تواجهها، وطرح الحلول للتخفيف من حدوث التهديدات المستقبلية، واستخدمت المنهج الوصفي بأسلوب دراسة الحالة، وطُبّقت على جامعة تكساس، وتوصلت إلى أن الموارد المستخدمة لمنع انتهاك البيانات ليست دقيقة، والتي أدّت إلى العديد من الانتهاكات السيبرانية، وأن أبرز التحديات التي تواجهها تمثلت في قِلَّة الموارد الماليّة لإضافة التدابير الوقائية، وضعف برامج توعية منسوبي الجامعة بأهمية الأمن السيبراني، وكيفية التعامل مع التهديدات المحتملة.

2. الدراسات التي اهتمت بمجال التنظيم في إدارة الأمن السيبراني:

هدفت دراسة ديفيدسون وهاسليدالين (Davidson & Hasledalen, 2014) إلى فهم أفضل للتهديدات السيبرانية التي تواجهها برامج التعلم عبر الإنترنت ووضع استراتيجيات التي يمكن أن تستخدم من قبل المؤسسات التعليم العالي بالولايات المتحدة الأمريكية؛ لحماية بيئة الإنترنت، واستخدمت الدراسة المنهج الوصفي المسحي بأسلوب دلفي، وتكونت العينة من مجموعة من الخبراء (دون تحديد عددهم) من ثلاث جولات، وتوصلت إلى عدة نتائج من أهمها نقص ممارسات التوثيق الصارمة، إذ إن معظم البيئات على الإنترنت ببساطه تطلب اسم المستخدم وكلمة المرور، والتي تعتبر نموذجًا واحدًا للمصادقة، إلا أن مؤسسات التعليم العالي تحجم عن المطالبة بالمزيد من التوثيق الشاق (المتعدد العوامل) خوفًا من فقدان الطلاب، ويلزم أن يكون هناك فهم من جانب القيادة بإضافة خطوات إضافية للمصادقة بدلًا من المخاطر المستمرة التي تواجهها المؤسسة.

وركزت دراسة لي وآخرون (Li et al., 2019) على اقتراح واختبار إطار عمل مفاهيمي لدوافع الحماية الشاملة من خلال دمج جهود الأمن السيبراني التنظيمية، واستخدمت الدراسة المنهج الوصفي المسحي، من خلال مسح آراء (579) من مديري الأعمال والمهنيين في مؤسسات مختلفة بالولايات المتحدة الأمريكية، منها (165) مؤسسة في قطاع التعليم -دون تحديد نوعها- وتمثل 28.5% من إجمالي المؤسسات موضع الدراسة، وأظهرت النتائج أنه عندما يكون الموظفون على دراية بسياسة وإجراءات الأمن السيبراني الخاصة بمؤسستهم، فإنهم يكونون أكثر كفاءة لإدارة مهام الأمن السيبراني من أولئك الذين ليسوا على علم بها.

3. **الدراسات التي اهتمت بمجال التوجيه في إدارة الأمن السيبراني:**

كما سعت دراسة راميرز (Ramirez, 2017) إلى وضع مقترح للمهنيين العاملين في مجال الأمن السيبراني للتعامل مع الأمن السيبراني كمجال متعدد التخصصات، وقد استخدمت الدراسة المنهج الوصفي الوثائقي من خلال مسح المقالات التي نشرت في الفترة بين (2010-2015) في مَجلّات متعددة التخصصات، وتوصلت إلى عدة نتائج من أهمها أن الأمن السيبراني كحقل يضم أربع تخصصات فرعية مختلفة: السياسة، وعلوم الكمبيوتر، والإدارة، والعلوم الاجتماعية. إلا أنه لا يوجد تعاون وتواصل بين هذه التخصصات، كما يتضح أن هناك اختلاف في استخدام المصطلحات الخاصة بالأمن السيبراني، مما يسبب صعوبة التواصل بين المتخصصين في هذه المجالات، ولذلك تم تطوير مقترح للمنهج الدراسي لمعهد ماساتشوستس للتكنولوجيا، مع مناقشة كيفية تطبيقه على الجامعات الأخرى.

كما كان الغرض من دراسة سعيد (Said, 2018) اختبار أفضل الممارسات البيداغوجية لإتقان الطلاب لكفاءات الأمن السيبراني، بالإضافة إلى استكشاف العوامل، التي قد تعزّز أو تَعوقُ تعلُّم الطلاب للأمن السيبراني، واستخدمت الدراسة المنهج الوصفي المسحي، من خلال المقابلة شبه المقننة لعدد من التربويين (دون تحديد عددهم) في الأمن السيبراني في ثماني كليات وجامعات من ولاية تينيسي، وولاية ألاباما، من الذين اجتازوا شرط التميز الأكاديمي، أو مراكز الدفاع السيبراني للتميز الأكاديمي، التي أصبحت مُكلَّفة ببرامج الأمن السيبراني، وتوصَّلت الدراسة إلى عدد من النتائج، كان من أهمها أن أكثر العوامل التي تعزّز أو تَعوقُ تعلّم الطلاب للأمن السيبراني هي كفاية الميزانية، وكفاية عدد الموظفين لمعالجة المخاوف الأمنية، وأن المتخصصين في الأمن السيبراني يجب أن تُدفع لهم رواتبٌ عالية، بينما تتوقَّع هذه المؤسسات أن تَدفع لهم مبالغ زهيدة.

4. الدراسات التي اهتمت بمجال التقويم في إدارة الأمن السيبراني:

سعت دراسة ماك كلارغ (McClurg, 2015) إلى قياس درجة المخاطر السيبرانية بمؤسسات التعليم العالي، ومدى توفر ضوابط العناية الواجبة في مجال الأمن السيبراني، واستخدمت الدراسة المنهج الوصفي المسحي، وطُبّقت على أصحاب المصلحة الرئيسيين من قادة أمن المعلومات بجامعتين أمريكيتين -دون إظهار هويتهما- وتوصَّلت الدراسة إلى أن الجامعتين -موضع الدراسة- تعرضتَا لانتهاك البيانات خلال العامين الماضيين، وأن أهمّ ضوابط العناية الواجبة تمثلت في تطبيق إدارة التصحيح المركزية، وتعزيز السياسات والإجراءات لخطط الاستجابة للحوادث، وتكثيف المراقبة المستمرة.

كما هدفت دراسة بجركن (Bjerken, 2017) إلى تحديد درجة ممارسة قيادة أمن المعلومات التأثير على اعتماد المنظمة لإستراتيجيات الأمن السيبراني النشطة، وتحديد العوامل التي تسبب إخفاقَ المنظمات في تبني إستراتيجيات الأمن السيبراني النشطة، واستخدمت الدراسة المنهج الكمّي الوصفي الارتباطي، وشملت العينة (93) من مديري أمن المعلومات بمؤسسات التعليم العالي الذين هم أعضاء في مركز (REN-ISAC) المتخصص في تبادل معلومات وتحليل شبكات البحث والتعليم لأكثر من 650 مؤسسة من مؤسسات مجتمع التعليم العالي والبحثي، وتوصَّلت الدراسة إلى أن من أهم أسباب فشل المنظمات في تبني الإستراتيجيات النشطة للأمن السيبراني عدم توظيف العاملين ذوي الخبرة الطويلة في مجال الأمن السيبراني؛ إذ إن استخدام الأفراد ذوي الخبرة الطويلة مع الاعتماد على تقنيات محدودة أفضلُ من توظيف أفرادٍ ذوي خبرةٍ قليلةٍ مع الاعتماد على التقنيات المتقدمة.

التعليق على الدراسات السابقة:

اتفقت الدراسة الحالية مع جميع الدراسات السابقة في تركيزها على أهمية الأمن السيبراني في قطاع التعليم العالي، إذ هدفت جميعها إلى ضرورة تطوير الأمن السيبراني بناءً على متطلبات التحول الرقمي للمراحل القادمة في ظلّ الاستخدام المتزايد للتقنيات الحديثة.

وقد اختلفت هذه الدراسة مع جميع الدراسات السابقة في المنهجية المستخدمة، فقد استخدمت جميعها المنهج الوصفي، وتفردت هذه الدراسة في استخدام المنهج المزجي بالتصميم المتوازي المتقارب، كما اختلفت الدراسة الحالية مع جميع الدراسات السابقة في أسلوب المعاينة، فقد استخدمت جميع الدراسات السابقة أحد أسلوبي المعاينة إما القصدية أو العشوائية، وتميزت هذه الدراسة في جمعها بين أسلوبي المعاينة العشوائية والقصدية على حد سواء.

كما تميزت الدراسة الحالية عن الدراسات السابقة جميعها في كونها الدراسة الوحيدة- على حد علم الباحثة- التي تطبق على الجامعات السعودية في مجال الأمن السيبراني، كما تنفرد بتناولها لدور إدارة الجامعات

السعودية الحكومية في تحقيق الأمن السيبراني، من ناحية إدارية شاملة لجميع مجالات الإدارة من تخطيط وتنظيم وتوجيه وتقويم، إذ إن الدراسات السابقة قد ركّزت على تناول مجال واحد من مجالات الإدارة.

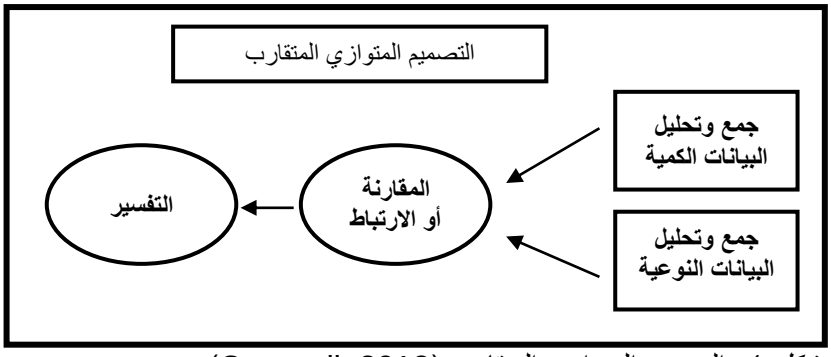
منهج الدراسة

اعتمدت الدراسة على استخدام المنهج المزجي، الذي يقوم على جمع وتحليل و "مزج" كل من الأساليب الكمية والنوعية في دراسة واحدة، أو في سلسلة من الدراسات لفهم مشكلة بحثية (Creswell & Plano Clark, 2011). والافتراض الأساسي هو أن استخدامات الأساليب الكمية والنوعية على السواء، مجتمعة، توفر فهمًا أفضل لمشكلة وأسئلة البحث مقارنة باستخدام من أي من الأسلوبين بشكل منفصل (Creswell, 2012).

ولتحقيق أغراض الدراسة، تم اختيار التصميم المتوازي المتقارب (Convergent Parallel Design)، والذي يعد أحد التصميمات الأساسية للمنهج المزجي (Creswell & Plano Clark, 2011)، وكان الغرض من اختيار هذا التصميم هو: جمع البيانات الكمية والنوعية في وقت واحد، ثم دمج البيانات، واستخدام النتائج لفهم المشكلة البحثية، إذ إن الأساس المنطقي الأساسي لهذا التصميم هو أن أحد أشكال جمع البيانات يوفر نقاط القوة لتعويض نقاط الضعف في الشكل الآخر، وأن الفهم الكامل لمشكلة البحوث ينتج عن جمع البيانات الكمية والنوعية على السواء. فعلى سبيل المثال، توفر الدرجات الكمية لأداة تطبق على العديد من الأفراد نقاط القوة لتعويض نقاط الضعف في الوثائق النوعية التي تطبق على عدد قليل من الناس. وكبديل لذلك، فإن الأساليب النوعية والمتعمقة لعدد قليل من الناس توفر قوة للبيانات الكمية التي لا توفر معلومات مفصلة على نحو كافٍ عن السياق الذي يقدم فيه الأفراد المعلومات (Creswell, 2012).

وفي هذا التصميم يجمع الباحث البيانات الكمية والنوعية على حد سواء، ويحلل مجموعتي البيانات بشكل منفصل، ويقارن النتائج من تحليل مجموعتي البيانات، ويجعل تفسيرًا عما إذا كانت النتائج تدعم بعضها البعض أو تتعارض معها، وتوفر المقارنة المباشرة بين مجموعتي البيانات من قبل الباحث "تقاربًا" بين مصادر البيانات (Creswell, 2012). كما هو مبين في شكل 1:

وقد تحدث هذه المقارنة بعدة طرق، إلا أن النهج الأكثر انتشارًا هو وصف النتائج الكمية والنوعية جنبًا



شكل 1: التصميم المتوازي المتقارب (Creswell, 2012)

إلى جنب في قسم المناقشة من الدراسة. فعلى سبيل المثال، يقدم الباحث أولًا النتائج الإحصائية الكمية ثم يقدم اقتباسات نوعية لتأكيد النتائج الإحصائية أو عدم تأكيدها (Creswell, 2012).

مجتمع الدراسة

تكوّن مجتمع الدراسة من القيادات بجامعة الملك سعود، وجامعة الملك عبد العزيز، وجامعة الملك فهد للبترول والمعادن المسؤولين عن العمادة/المركز المختص بتقنية المعلومات، وجميع الإداريين العاملين في تلك العمادة/ المركز، وبلغ عددهم 623 مفردة.

عينة وأفراد الدراسة

يرى الباحثون في الأساليب المزجية أن أحجام العينة غير المتكافئة لا يمثل إشكالًا في الدراسة، ويقولون إن القصد من إجراء البحث النوعي والكمي يختلف في هدفه، فالكمي للتعميم على المجتمع، والنوعي لاكتساب منظور متعمق، وأن كلاً منهما يوفر إحصاءً كافياً (Creswell, 2014)، ويؤكد كريسول (Creswell, 2012) على أن أحجام العينة الكمية والنوعية قد تكون مختلفة في التصميم المتوازي المتقارب، لذا يجب توخي الحذر بعدم التقليل من أهمية العينة بسبب حجمها، وبناء على ما سبق تم اختيار عينة وأفراد الدراسة كما يلي:

أولاً: عينة الدراسة

لتطبيق الأداة الأولى (الاستبانة) تم سحب عينة عشوائية بسيطة من مجتمع الدراسة، باستخدام معادلة ريتشارد جيجر التالية لتحديد العينة الممثلة لمجتمع الدراسة:

$$n = \frac{\left(\frac{z}{d}\right)^2 \times (0.50)^2}{1 + \frac{1}{N}\left[\left(\frac{z}{d}\right)^2 \times (0.50)^2 - 1\right]}$$

حيث تشير N إلى حجم المجتمع، وz إلى الدرجة المعيارية المقابلة لمستوى الدلالة 0.95 وتساوي 1.96، وd إلى نسبة الخطأ، وبذلك تكونت عينة الدراسة من 238 مفردة من مجموع مجتمع الدراسة، ويوضح جدول 2 توزيعها على العمادتين والمركز في الجامعات -موضع الدراسة- بحسب النسبة المئوية لمجموع منسوبي تلك العمادة/المركز، كما يلي في جدول 1:

جدول 1
عينة الدراسة

م	مسمى العمادة/المركز المختص بتقنية المعلومات	مجموع منسوبي العمادة/المركز	النسبة المئوية لمنسوبي العمادة/المركز من المجموع الكلي	عدد العينة بعد سحبها بحسب النسبة المئوية
1	عمادة التعاملات الإلكترونية والاتصالات بجامعة الملك سعود	343	%55	131
2	عمادة تقنية المعلومات بجامعة الملك عبد العزيز	200	%32	76
3	مركز تقنية المعلومات والاتصالات بجامعة الملك فهد للبترول والمعادن	80	%13	31
	المجموع الكلي	623	%100	238

خصائص عينة الدراسة:

تتصف عينة الدراسة بعدد من الخصائص الاجتماعية والوظيفية تتمثل في: جهة العمل، النوع الاجتماعي، مسمى الوظيفية، عدد سنوات الخبرة، وذلك وفق جدول 2 التالي:

جدول 2
خصائص عينة الدراسة

المتغير	التوزيع	التكرارات	النسبة المئوية
جهة العمل	عمادة التعاملات الإلكترونية والاتصالات بجامعة الملك سعود	131	%55.0
	عمادة تقنية المعلومات بجامعة الملك عبد العزيز	76	%31.9
	مركز تقنية المعلومات والاتصالات بجامعة الملك فهد للبترول والمعادن	31	%13.0
النوع الاجتماعي	ذكر	133	%55.9
	أنثى	105	%44.1
	عميد/ مدير؛ للعمادة/أو المركز	1	%0.4

	وكيل للعمادة/ أو المركز	7	%2.9
	مدير إدارة أو وحدة أو قسم بالعمادة/أو المركز	54	%22.8
	إداري بالعمادة/ أو المركز	176	%73.9
عدد سنوات الخبرة	أقل من 5 سنوات	35	%14.7
	5 إلى 10 سنوات	126	%52.9
	11 إلى 15 سنه	29	%12.2
	أكثر من 15 سنه	48	%20.2

ثانيًا: أفراد الدراسة

لتطبيق الأداة الثانية وهي (المقابلة) -التي هدفت إلى الوصول لفهم أعمق وتفسير أوضح لواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، من خلال المجالات (التخطيط، التنظيم، التوجيه، التقويم) - تم تحديد عينة قصدية قوامها (3) من قادة أمن المعلومات بالجامعات موضع الدراسة وهم رؤساء كل من (إدارة المخاطر وأمن المعلومات بجامعة الملك سعود، وإدارة المخاطر الرقمية وأمن المعلومات بجامعة الملك فهد للبترول والمعادن، وإدارة أمن المعلومات والجودة بجامعة الملك عبد العزيز)، لكونهم في موضع اتخاذ القرار وتوجيه عمليات الأمن السيبراني بالجامعة بشكل مباشر، وقد وافق جميعهم على إجراء المقابلة.

خصائص أفراد الدراسة المستهدفون بالمقابلة:

يتصف أفراد الدراسة المستهدفون بالمقابلة بكونهم جميعا من الذكور وتراوحت سنوات خبرتهم من 5 إلى أكثر من 15 سنة.

أدوات الدراسة

تم استخدام أداتين؛ لتحقيق أهداف الدراسة كما يلي:

الأداة الأولى: الاستبانة

تم إعداد الاستبانة في صورتها الأولية بالاعتماد على أدب المجال، وعلى أدبيات القواعد المنهجية لإعداد الاستبانة، ثم عُرضتْ على 13 محكمًا من ذوي الاختصاص في الميدان الأكاديمي في مجالي الإدارة التربوية والأمن السيبراني لتحكيمها، ومن ثم تعديلها في صورتها النهائية، وقد أجابت هذه الأداة عن أسئلة الدراسة بصورة كمية، وتم تطبيقُها على عينة الدراسة، وهم وكلاء الجامعات المسؤولون عن عمادة/مركز تقنية المعلومات، وجميع القيادات بتلك العمادة/المركز، وجميع الإداريين العاملين في عمادة/مركز تقنية المعلومات بالجامعات السعودية الحكومية موضع الدراسة.

وتضمنت الاستبانة الإجابة عن عبارات الاستبانة وفق تدرج ليكرت الخماسي لدرجة الموافقة (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة)، وتم التوضيح لعينة الدراسة على غلاف الاستبانة إلى أنه يمكن استخدام خيار (محايد) عند عدم التأكد من الإجابة، ولتحديد طول خلايا المقياس الخماسي (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم حساب المدى (5-1=4)، ثم تقسيمه على عدد خلايا المقياس للحصول على طول الخلية الصحيح أي (4/5= 0.80) بعد ذلك تم إضافة هذه القيمة إلى أقل قيمة في المقياس (أو بداية المقياس وهي الواحد الصحيح) وذلك لتحديد الحد الأعلى لهذه الخلية، وهكذا أصبح طول الخلايا كما يتضح في جدول 3:

جدول 3

تحديد فئات مقياس ليكرت الخماسي

موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
5.0 – 4.21	4.20 – 3.41	3.40 – 2.61	2.60 – 1.81	1.80 – 1

صدق أداة الدراسة (الاستبانة)

تم التحقق من صدق أداة الدراسة (الاستبانة) عن طريق:

أ. صدق المحكمين: وذلك بعرض الاستبانة في صورتها الأولية على ثلاثة عشر محكمًا من أعضاء هيئة التدريس والخبراء في مجالي الإدارة التربوية والأمن السيبراني؛ للتأكد من وضوح عبارات الاستبانة، ودقة صياغتها، ومدى أهميتها، وملاءمتها للمحور الذي تنتمي إليه، لبناء الاستبانة في صورتها النهائية.

ب. الاتساق الداخلي: بعد التأكد من الصدق الظاهري لأداة الدراسة تم تطبيق الاستبانة ميدانياً على عينة استطلاعية مكونة من (50) موظفًا من العاملين في العمادة/المركز المختص بتقنية المعلومات بالجامعات المشمولة بالدراسة، وعلى بيانات هذه العينة تم حساب معامل الارتباط بيرسون لمعرفة الصدق الداخلي للاستبانة، بحساب معامل الارتباط بين درجة كل عبارة من عبارات أداة الدراسة بالدرجة الكلية للمحور الذي تنتمي إليه العبارة كما يتضح ذلك من جدولي 4 و 5 فيما يلي:

جدول 4

معاملات ارتباط بيرسون لقياس العلاقة بين عبارات مجالات محور (واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني) بالدرجة الكلية للمجال المنتمية إليه

التخطيط		التنظيم		التوجيه		التقويم	
العبارة	معامل الارتباط	العبارة	معامل الارتباط	العبارة	معامل الارتباط	العبارة	معامل الارتباط
1	**0.611	11	**0.623	18	**0.569	24	**0.784
2	**0.583	12	**0.735	19	**0.789	25	**0.839
3	**0.671	13	**0.759	20	**0.691	26	**0.806
4	**0.649	14	**0.628	21	**0.818	27	**0.703
5	**0.718	15	**0.719	22	**0.778	28	**0.787
6	**0.689	16	**0.766	23	**0.803	29	**0.775
7	**0.699	17	**0.630	-	-	30	**0.850
8	**0.736	-	-	-	-	31	**0.792
9	**0.813	-	-	-	-	-	-
10	**0.700	-	-	-	-	-	-

** دال عند مستوى (0.01)

جدول 5

معاملات ارتباط بيرسون لقياس العلاقة بين مجالات محور (واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني) بالدرجة الكلية للمحور

المجال	معامل الارتباط	المجال	معامل الارتباط
التخطيط	**0.859	التوجيه	**0.896
التنظيم	**0.858	التقويم	**0.882

** دال عند مستوى (0.01)

ثبات أداة الدراسة (الاستبانة)

لقياس مدى ثبات أداة الدراسة (الاستبانة) تم استخدم (معادلة ألفا كرونباخ) (Cronbach's Alpha (α، وذلك وفق جدول 6 كما يلي:

جدول 6

معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

م	المحور	عدد العبارات	معامل الثبات
1	واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط	10	0.876
2	واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم	7	0.815
3	واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه	6	0.840
4	واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم	8	0.901
5	الدرجة الكلية لواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني	31	0.905

الأداة الثانية: المقابلة

تم تصميم استمارة المقابلة في صورتها الأولية بالاستفادة من عبارات الاستبانة، نظرًا لاستخدام الدراسة المنهج المزجي بالتصميم المتوازي المتقارب والذي يقتضي تطابق محاور ومجالات الاستبانة مع محاور ومجالات المقابلة، لتحقيق المقارنة بين النتائج الكمية والنوعية، بالإضافة إلى مراجعة أدب المجال والدراسات السابقة، والأدبيات المتعلقة بالقواعد المنهجية لبناء المقابلة. ثم عرضت على اثنين من المحكمين من ذوي الاختصاص لتحكيمها، والتأكد من وضوح صياغة الأسئلة، وإخراجها في صورتها النهائية، وقد أجابت هذه الأداة عن أسئلة الدراسة بصورة نوعية، من وجهة نظر قادة أمن المعلومات بالجامعات موضع الدراسة للوصول لفهم أعمق، وتفسير أوضح لمشكلة الدراسة الحالية.
وقد تم ترميز المشاركين من أفراد الدراسة المستهدفين بالمقابلة حفاظًا على سرية البيانات (بناء على طلبهم) لحساسية قضايا الأمن السيبراني وفق التالي: (مشارك أ، مشارك ب، مشارك ج).

صدق أداة الدراسة (المقابلة)

تم التحقق من صدق الأداة باستخدام صدق المحكمين، وذلك بالاعتماد أولًا على صدق الأداة الأولى الاستبانة، والتي تم اشتقاق أسئلة المقابلة منها بشكل كامل، وثانيًا بعرضها في صورتها الأولية على اثنين من المحكمين من أعضاء هيئة التدريس في مجال الإدارة التربوية؛ للتأكد من وضوح الأسئلة، ودقة صياغتها، لبناء استمارة المقابلة في صورتها النهائية.

الأساليب الإحصائية

تم استخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) في المعالجة الإحصائية للبيانات المتعلقة باستجابات عينة وأفراد الدراسة بغرض فهمها، وتفسيرها، وتضمنت المعالجة الإحصائية الأساليب الآتية:

- **معامل ارتباط بيرسون (Pearson correlation)**: لحساب الاتساق الداخلي لعبارات الاستبانة.
- **معامل ثبات معادلة ألفا كرونباخ (Cronbach's Alphaα)**: للتحقق من معامل ثبات المحاور المختلفة لأداة الدراسة (الاستبانة).
- **التكرارات، والنسب المئوية، والمتوسطات الحسابية، والرتب:** لوصف عينة الدراسة، وتحديد نسبة الاستجابة، ولترتيب استجاباتهم تجاه محاور الاستبانة، ومجالاتها.
- **الانحرافات المعيارية:** للتعرّف إلى درجة انحراف استجابات عينة الدراسة لكل عبارة من العبارات ولكل محور عن متوسطها الحسابي.
- **التكرارات، والنسب المئوية**: المستخلصة من تفريغ إجابات أفراد الدراسة عن أسئلة المقابلة.
-

عرض نتائج الدراسة ومناقشتها

أولًا: عرض وتحليل نتائج أسئلة الدراسة ومناقشتها

السؤال الأول: ما واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط؟

1. **نتائج الاستبانة:**

للتعرف على واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتخطيط؛ تم حساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري لاستجابات عينة الدراسة، كما تم ترتيب هذه العبارات حسب المتوسط الحسابي لكلاً منها، وذلك وفق جدول 7:

جدول 7

التكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري ودرجة الموافقة والرتبة لواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط

م	العبارات		درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الرتبة
			موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة				
1	تحديد الأصول الإلكترونية المستهدفة بالهجمات السيبرانية؛ بالتنسيق مع الجهات ذات العلاقة في الجامعة.	ك	124	97	15	2	-	4.44	0.65	موافق بشدة	1
		٪	52.1	40.8	6.3	0.8	-				
2	تصنيف الأصول الإلكترونية المستهدفة بالهجمات السيبرانية إلى فئات رئيسية بحسب نوعها.	ك	109	106	18	5	-	4.34	0.71	موافق بشدة	2
		٪	45.8	44.5	7.6	2.1	-				
10	وضع خطة للاستجابة والتعافي، حال تعرض الجامعة لهجمات سيبرانية مؤثرة.	ك	118	82	26	10	2	4.28	0.88	موافق بشدة	3
		٪	49.6	34.5	10.9	4.2	0.8				
5	تعيين الموظفين الأكثر كفاءة في مجال الأمن السيبراني ضمن فريق التخطيط الإستراتيجي.	ك	106	98	20	12	2	4.24	0.87	موافق بشدة	4
		٪	44.5	41.2	8.4	5.0	0.8				
4	اتخاذ القرار بشأن قبول المخاطر أو تخفيفها أو نقلها لجهات أخرى بالتنسيق مع القيادة العليا بالجامعة.	ك	90	104	39	5	-	4.17	0.77	موافق	5
		٪	37.8	43.7	16.4	2.1	-				
9	وضع خطة استراتيجية لإدارة الأمن السيبراني بالجامعة.	ك	100	92	33	12	1	4.17	0.88	موافق	6
		٪	42.0	38.7	13.9	5.0	0.4				
7	تحديد العدد اللازم من الموظفين المؤهلين في التخصصات الدقيقة لإدارة أمن الأنظمة الإلكترونية بالجامعة.	ك	77	102	35	21	3	3.96	0.97	موافق	7
		٪	32.4	42.9	14.7	8.8	1.3				
3	تعيين قيمة للأصول الإلكترونية المستهدفة	ك	73	90	65	10	-	3.95	0.87	موافق	8
		٪	30.7	37.8	27.3	4.2	-				

م	العبارات		درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الرتبة
			موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة				
8	تحديد الموارد المالية اللازمة لتحقيق الأهداف الإستراتيجية.	ك	71	97	56	10	4	3.93	0.92	موافق	9
		٪	29.8	40.8	23.5	4.2	1.7				
6	الاستعانة بالخبراء الخارجيين المختصين في مجال الأمن السيبراني للمشاركة في التخطيط الإستراتيجي.	ك	74	91	56	13	4	3.92	0.96	موافق	10
		٪	31.1	38.2	23.5	5.5	1.7				
المتوسط الحسابي العام للمحور								**4.14**	**0.59**	**موافق**	**-**

يتضح من جدول 7 أن المتوسط الحسابي العام لعبارات المحور بلغ (4.14) بانحراف معياري (0.59)، وهذا يدل على أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط جاء بدرجة عالية.

2. نتائج المقابلة:

أسفرت نتائج المقابلة مع أفراد الدراسة (وهم قادة أمن المعلومات بكل جامعة من الجامعات المشمولة بالدراسة وعددهم ثلاثة) حول واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، في مجال التخطيط، بعد حساب التكرارات والنسبة المئوية لاستجابات أفراد الدراسة، وتوضيح الإجابات -من خلال جدول 8 - عما يلي:

جدول 8

الإجابات الكمية (المحولة) والنوعية لأفراد الدراسة المستهدفين بالمقابلة في مجال التخطيط

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة
		ك	%	ك	%	

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية					الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة	
		ك	%	ك	%		
(1،1)	هل تم تحديد الأصول الإلكترونية المستهدفة بالهجمات السيبرانية؛ بالتنسيق مع الجهات ذات العلاقة في الجامعة؟	3	100	0	0	موافق	أفاد (مشارك أ، مشارك ب، مشارك ج) بأنهم يعملون على تحديد وتصنيف الأصول الإلكترونية وتعيين قيمة لها في الوقت الحالي -تطبيقًا لمتطلبات الهيئة الوطنية للأمن السيبراني- ولكنهم يواجهون بعض الصعوبات بسبب التراكمات الطويلة لهذه الأصول خلال السنوات الماضية، كما أضاف (مشارك ج) بأن الصعوبة تكمن أيضًا في عدم وجود نظام الكتروني خاص بإدارة الأصول الإلكترونية الخاصة بالجامعة، بالإضافة إلى عدم وجود إدارة في العمادة/المركز تختص بإدارة الأصول الإلكترونية ضمن إدارات العمادة/المركز.
(1،2)	هل تم تصنيف الأصول الإلكترونية المستهدفة بالهجمات السيبرانية؛ إلى فئات رئيسية بحسب نوعها؟	3	100	0	0	موافق	
(1،3)	هل تم تعيين قيمة للأصول الإلكترونية المستهدفة بالهجمات السيبرانية؛ لتحديد مقدار الانفاق عليها لحمايتها؟	3	100	0	0	موافق	
(1،4)	هل يتم اتخاذ القرار بشأن قبول المخاطر أو تخفيفها أو نقلها لجهات أخرى؛ بالتنسيق مع القيادة العليا بالجامعة؟	3	100	0	0	موافق	أفاد (مشارك أ، مشارك ب، مشارك ج) بأنهم يعملون بمساندة القيادة العليا بالجامعة على دراسة جميع التقنيات الجديدة التي تستهدف إدارة الجامعة إدخالها ضمن أنظمتها الإلكترونية، لتحديد درجة المخاطر المتوقعة منها، ومن ثم تحديد قبولها أو تخفيفها أو نقلها لجهات أخرى.
(1،5)	هل تم تعيين الموظفين الأكثر كفاءة في مجال الأمن السيبراني، ضمن فريق التخطيط الإستراتيجي؟	3	100	0	0	موافق	أفاد (مشارك أ، مشارك ب، مشارك ج) بأنه يتم تعيين الموظفين الأكثر كفاءة والأقدم في سنوات العمل في العمادة/المركز، ضمن فريق التخطيط الإستراتيجي للخطة السنوية للعمادة/المركز، وخاصة من لهم إلمام بأطر العمل المعتمدة مثل ISO/IEC27001، على أن يكون فريق التخطيط من كافة الإدارات والتخصصات، إلا أنهم بحاجة إلى مزيد من التأهيل المستمر على المستجدات في مجال الأمن السيبراني واستقطاب المتخصصين في هذا المجال ضمن فريق العمل.

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				درجة الموافقة	الإجابة النوعية
		نعم، موافق		لا، غير موافق			
		ك	%	ك	%		
(1،6)	هل تم الاستعانة بالخبراء الخارجيين المختصين في مجال الأمن السيبراني؛ للمشاركة في التخطيط الإستراتيجي؟	0	0	3	100	غير موافق	أفاد (مشارك أ، مشارك ب، مشارك ج) بأنه لا يتم الاستعانة بأي خبراء في مجال الأمن السيبراني من خارج الجامعة للمشاركة في التخطيط الإستراتيجي للعمادة/المركز، وأن العمادة/المركز يعتمد على موظفيه في ذلك اعتمادًا تامًا، وأضاف (مشارك ب ومشارك ج) بأنه يمكن الاستعانة بشكل ودي بالجهات الأخرى المتخصصة عند الحاجة لذلك، بينما أشار (مشارك أ) بأنه لا يوجد أي استعانة بخبراء من خارج الجامعة، وإنما يستعينون بخبيرين من خارج العمادة ولكنهم من منسوبي الجامعة.
(1،7)	هل تم تحديد العدد اللازم من الموظفين المؤهلين في التخصصات الدقيقة لإدارة أمن الأنظمة الإلكترونية بالجامعة؟	3	100	0	0	موافق	أفاد (مشارك أ، مشارك ب، مشارك ج) بأنهم يعملون في العمادة/المركز بشكل دوري على تحديد الأعداد اللازمة من الموظفين، وحصر النقص في الوظائف الإدارية والفنية والتقنية، ولا يعني هذا الحصر توفير هذه الأعداد من الموظفين دائمًا، بسبب عدد من التحديات الإدارية والمالية التي تواجههم.
(1،8)	هل تم تحديد الموارد المالية اللازمة لتحقيق الأهداف الإستراتيجية؟	0	0	3	100	غير موافق	أفاد (مشارك أ، مشارك ب، مشارك ج) بأنه لا يتم تحديد الموارد المالية اللازمة لتحقيق الأهداف الإستراتيجية الخاصة بالأمن السيبراني بشكل سنوي ضمن الخطة الإستراتيجية السنوية للعمادة/ المركز، ويعود ذلك إلى شح الموارد المالية، والتسارع التقني الذي يصعب هذه المهمة، وعدم وجود إدارة مختصة بإدارة الأمن السيبراني ضمن إدارات العمادة/المركز، وأضاف (مشارك ج) بأنه مع إنشاء إدارة خاصة بالأمن السيبراني ضمن هيكلة العمادة/المركز مستقبلًا، سيكون ضمن مهامها وضع خطة مالية وتحديد النفقات والرواتب في كل ما يختص بمجال الأمن السيبراني.
(1،9)	هل تم وضع خطة استراتيجية لإدارة الأمن السيبراني بالجامعة؟	0	0	3	100	غير موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنه لا توجد حاليًا خطة استراتيجية مستقلة خاصة بالأمن السيبراني في الجامعة، وأضاف (مشارك أ، ومشارك ب) بأنهم في مرحلة تطوير خطة استراتيجية للجامعة، بينما نوّه (مشارك ج) بأنه من ضوابط الهيئة الوطنية للأمن السيبراني وجود خطة استراتيجية خاصة بالأمن السيبراني في الجامعة، لذا تم العمل عليها وهي في طور المراجعة لتقديمها للاعتماد النهائي

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة
		ك	%	ك	%	
						من قبل القيادة العليا بالجامعة.
(1،10)	هل تم وضع خطة للاستجابة والتعافي، حال تعرض الجامعة لهجمات سيبرانية مؤثرة؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنه توجد خطة للطوارئ تضعها الإدارة المختصة بإدارة المخاطر الإلكترونية، وأضاف (مشارك ج) بأن الخطة مازالت بحاجة إلى تطوير حتى تحقق نتائج نوعية على مستوى الجامعة.

يتضح من جدول 8 أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط يتضمن (10) أسئلة، جاءت (7) أسئلة منها باستجابة (نعم، موافق) وهو ما يمثل 70% من مجموع أسئلة مجال التخطيط، في حين جاءت الأسئلة الثلاثة الأخرى باستجابة (لا، غير موافق)، وهو ما يمثل 30% من مجموع أسئلة مجال التخطيط، وتشير النتيجة السابقة إلى أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط جاء بدرجة عالية.

وتناقش العبارات التالية أعلى ثلاث عبارات ترتبط بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التخطيط، والتي حصلت على درجة موافق بشدة من قبل عينة الدراسة، وهي مرتبة تنازليًا وفقاً للمتوسط الحسابي لها، وذلك على النحو التالي:

- جاءت العبارة رقم (1) وهي (تحديد الأصول الإلكترونية المستهدفة بالهجمات السيبرانية؛ بالتنسيق مع الجهات ذات العلاقة في الجامعة) بالمرتبة الأولى بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتخطيط بمتوسط حسابي (4.44) وانحراف معياري (0.65)، وهذا يدل على أن هناك موافقة بشدة بين عينة الدراسة على هذه العبارة.
- جاءت العبارة رقم (2) وهي (تصنيف الأصول الإلكترونية المستهدفة بالهجمات السيبرانية إلى فئات رئيسية بحسب نوعها) بالمرتبة الثانية بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتخطيط بمتوسط حسابي (4.34) وانحراف معياري (0.71)، وهذا يدل على أن هناك موافقة بشدة بين عينة الدراسة على هذه العبارة.

وتتفق هاتان النتيجتان مع ما أشار إليه أفراد الدراسة المستهدفون بالمقابلة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤالين (1،1) و(1،2) من أسئلة المقابلة بأنهم يعملون على تحديد وتصنيف الأصول الإلكترونية وتعيين قيمة لها في الوقت الحالي. وقد يُعزى اهتمام العمادة/المركز بـ (تحديد الأصول الإلكترونية المستهدفة بالهجمات السيبرانية؛ بالتنسيق مع الجهات ذات العلاقة في الجامعة) و(تصنيف الأصول الإلكترونية المستهدفة بالهجمات السيبرانية إلى فئات رئيسية بحسب نوعها) إلى أن الجامعات -موضع الدراسة- تتميز بوجود أصول قيمة جدًا على رأسها الإنتاج الفكري لهذه الجامعات وبراءات الاختراع، بالإضافة إلى الكم الضخم من بيانات منسوبي هذه الجامعات، والتي تعد هدفًا ذو أولوية عالية، بالإضافة إلى سمعة الجامعات المتميزة كونها صنفت من بين أفضل الجامعات العالمية، الأمر الذي يجعلها هدفًا سياسيًا بحتًا.

- جاءت العبارة رقم (10) وهي (وضع خطة للاستجابة والتعافي، حال تعرض الجامعة لهجمات سيبرانية مؤثرة) بالمرتبة الثالثة بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتخطيط بمتوسط حسابي (4.28) وانحراف معياري (0.88)، وهذا يدل على أن هناك موافقة بشدة بين أفراد الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (1،10) من أسئلة المقابلة بأنه توجد خطة للطوارئ تضعها الإدارة المختصة بإدارة المخاطر الإلكترونية. وتعكس النتيجتان السابقتان (الكمية والنوعية) اهتمام إدارة العمادة/المركز بوضع خطة للاستجابة والتعافي، حال تعرض الجامعة لهجمات سيبرانية مؤثرة؛ الذي قد يعزى إلى صعوبة تجنب الهجمات السيبرانية بشكل تام، إذ إن

هذا الأمر يؤدي إلى إيقاف العمليات الإلكترونية بشكل تام، مما يستلزم ضرورة إيجاد البدائل -حال الانتهاك السيبراني- وفق خططٍ مدروسة.

وتتفق هاتان النتيجتان مع نتيجة دراسة دياز وآخرون (Diaz et al., 2017) التي أكدت على ضرورة أهمية الخطوات الاستباقية لحماية المعلومات الرقمية؛ نتيجة لتوسع مؤسسات التعليم العالي في استخدام البدائل المستندة إلى التخزين السحابي للبيانات، كما تتفق مع نتيجة ماك كلارغ (McClurg, 2015) التي أكدت على أن أهمّ ضوابط العناية الواجبة تمثلت في تعزيز السياسات والإجراءات لخطط الاستجابة للحوادث.

- جاءت العبارة رقم (5) وهي (تعيين الموظفين الأكثر كفاءة في مجال الأمن السيبراني ضمن فريق التخطيط الإستراتيجي) بالمرتبة الرابعة بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتخطيط بمتوسط حسابي (4.24) وانحراف معياري (0.87)، وهذا يدل على أن هناك موافقة بشدة بين أفراد الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (1،5) من أسئلة المقابلة، بأنهم موافقون على تعيين الموظفين الأكثر كفاءة -في العمادة/المركز- ضمن فريق التخطيط الإستراتيجي للخطة السنوية للعمادة/المركز. وتعكس هاتان النتيجتان (الكمية والنوعية) اهتمام إدارة العمادة/المركز بذلك، الذي قد يعزى إلى أن العمادة/المركز لديهم متخصصين ذوي خبرة طويلة في هذا المجال، إذ يمتلك 20% من عينة الدراسة خبرة تتجاوز 15 عامًا، في ظل حرص العمادة على تقديم التدريب التخصصي لهم بشكل مستمر.

السؤال الثاني: ما واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم؟

1. نتائج الاستبانة:

للتعرف على واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم؛ تم حساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري لاستجابات عينة الدراسة، كما تم ترتيب هذه العبارات حسب المتوسط الحسابي لكلاً منها، وذلك وفق جدول 9:

جدول 9

التكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري ودرجة الموافقة والرتبة لواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم

م	العبارات		درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الرتبة
			موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة				
11	تحديد إدارة أو وحدة تختص بتحقيق الأمن السيبراني بالجامعة.	ك	139	83	12	3	1	4.50	0.69	موافق بشدة	1
		٪	58.4	34.9	5.0	1.3	0.4				
12	اعتماد سياسات الاستخدام الآمن لحماية الأصول الإلكترونية بشكل رسمي.	ك	132	87	12	7	-	4.45	0.73	موافق بشدة	2
		٪	55.5	36.6	5.0	2.9	-				
13	وضع القوانين المنظمة للنشاطات الإلكترونية المختلفة في الجامعة.	ك	104	109	19	6	-	4.31	0.73	موافق بشدة	3
		٪	43.7	45.8	8.0	2.5	-				
14	تحديد إطار عمل ملائم لتحقيق الأمن السيبراني وفقًا لأفضل الممارسات العالمية، مثل: NIST 800-53,	ك	106	89	40	3	-	4.25	0.78	موافق بشدة	4
		٪	44.5	37.4	16.8	1.3	-				

م	العبارات		درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الرتبة
			موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة				
	ISO 27001.										
16	الإشراف على الأنظمة الإلكترونية بالجامعة وفق نظام مركزي.	ك	89	118	20	6	5	4.18	0.85	موافق	5
		٪	37.4	49.6	8.4	2.5	2.1				
15	تشكيل فرق الاستجابة للحوادث السيبرانية وفقًا لأفضل الممارسات العالمية.	ك	89	100	35	12	2	4.10	0.89	موافق	6
		٪	37.4	42.0	14.7	5.0	0.8				
17	الاستعانة بالخبراء غير المتفرغين من المتخصصين في مجال الأمن السيبراني؛ لمساندة العمادة/ المركز.	ك	49	77	88	18	6	3.61	0.98	موافق	7
		٪	20.6	32.4	37.0	7.6	2.5				
المتوسط الحسابي العام للمحور								**4.20**	**0.56**	**موافق**	**-**

يتضح من جدول 9 أن المتوسط الحسابي العام لعبارات المحور بلغ (4.20) بانحراف معياري (0.56)، وهذا يدل على أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتنظيم جاء بدرجة عالية.

2. نتائج المقابلة:

أسفرت نتائج المقابلة حول واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، في مجال التنظيم، بعد حساب التكرارات والنسبة المئوية، وتوضيح الإجابات- كما يوضحها جدول 10 -عما يلي:

جدول 10

الإجابات الكمية (المحولة) والنوعية لأفراد الدراسة المستهدفين بالمقابلة في مجال التنظيم

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة
		ك	%	ك	%	
(2،1)	هل تم تحديد إدارة أو وحدة تختص بتحقيق الأمن السيبراني بالجامعة؟	0	0	3	100	غير موافق

أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنه لا توجد حاليًا إدارة مختصة بتحقيق الأمن السيبراني في الجامعة، ولكن توجد إدارة تقوم بهذا العمل في الوقت الحالي ولها مسمياتٌ مختلفةٌ مثل (إدارة المخاطر وأمن المعلومات، أو إدارة المخاطر الرقمية وأمن المعلومات، أو إدارة أمن المعلومات والجودة)، وأشار (مشارك أ، ومشارك ج) بأنه لا يُمكن الاعتمادُ على هذه الإدارات في تحقيق الأمن السيبراني نظرًا للأدوار المختلفة التي تتطلبها المرحلة الحالية والمرحلة المستقبلية، وأضاف (مشارك أ) بأنهم في المراحل النهائية لإنشاء

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة
		ك	%	ك	%	
						إدارتين تختصان بتحقيق الأمن السيبراني في الجامعة إحداهما تُعنى بالحوكمة، والأخرى بالتنفيذ، ولكن لم يُعتمد الهيكل التنظيمي الجديد من قبل مدير الجامعة بعد، كما ذكر (مشارك ج) بأنه صَدَرت توجيهات قبل فترة قصيرة من القيادة العليا بالجامعة بإنشاء إدارة باسم (إدارة الأمن السيبراني) ويتم العمل على إنشائها ووضع الأسس التنظيمية لها في الوقت الحالي.
(2،2)	هل تم اعتماد سياسات الاستخدام الآمن لحماية الأصول الإلكترونية بشكل رسمي؟	3	100	0	0	موافق	أفاد (مشارك أ، ومشارك ب) بأن سياسات الاستخدام الآمن لحماية الأصول الإلكترونية معتمدة بشكل رسمي من قبل القيادة العليا بالجامعة، بينما أشار (مشارك ج) بأن هذه السياسات معتمدة من قبل مدير العمادة/المركز، ولم تعتمد من قبل القيادة العليا بالجامعة.
(2،3)	هل تم وضع القوانين المنظمة للنشاطات الإلكترونية المختلفة في الجامعة؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنهم يسعون وبشكل مستمر لوضع القوانين المنظمة للنشاطات الإلكترونية المختلفة في الجامعة، وذلك وفق المستجدات التقنية، وأنهم جادون في ذلك رغم مقاومة بعض منسوبي الجامعة لبعض القوانين المستجدة التي تستدعيها المصلحة العامة.
(2،4)	هل تم تحديد إطار عمل ملائم وفقًا لأفضل الممارسات العالمية، مثل: NIST 800-53, ISO 27001؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأن العمادة/المركز يعمل وفقًا لمتطلبات نظام إدارة أمن المعلومات (ISO/IEC 27001)، كما ذكر (مشارك ج) بأنهم يعملون أيضًا وفقًا لبعض معايير منظمة (NIST)، وأنهم في المرحلة الحالية ملتزمون بالعمل على تحقيق الضوابط المطلوبة من الهيئة الوطنية للأمن السيبراني.
(2،5)	هل تم تشكيل فرق الاستجابة للحوادث السيبرانية وفقًا لأفضل الممارسات العالمية؟	3	100	0	0	موافق	أفاد (مشارك أ، ومشارك ب، ومشارك ج) بأن العمادة/المركز لديهم فريق للاستجابة للحوادث السيبرانية وفقًا لمعيار (ISO/IEC 27001)، يكون من مهام هذا الفريق احتواء الحوادث السيبرانية والتعافي منها، عن طريق التكاتف بين كافة التخصصات التقنية، إذ يتم ترشيح عدد من موظفي كل قسم بالعمادة/المركز لتكوين هذا الفريق، وأضاف (مشارك ج) بأن فريقهم مكون من 14 من منسوبي العمادة/المركز في كافة التخصصات التقنية والفنية.
(2،6)	هل يتم الإشراف على الأنظمة	3	100	0	0	موافق	أفاد (مشارك أ، ومشارك ب) بأن العمادة/المركز يتوجه نحو الإشراف على أنظمة العمادة/المركز وفق نظام مركزي بشكل عام،

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				الإجابة النوعية
		نعم، موافق		لا، غير موافق	درجة الموافقة	
		ك	%	ك	%	
	الإلكترونية بالجامعة وفق نظام مركزي؟					إلا أنه توجد بعض الجهات التابعة للجامعة ما زالت تدير أنظمتها الإلكترونية بشكل مستقل ولكن وفق الضوابط المعتمدة من العمادة/المركز، إذ إن هذه الجهات تكون الخوادم الخاصة بها مستضافة لدى العمادة/المركز، بينما أكد (مشارك ج) بأن الإشراف على البنية التحتية لجميع الأنظمة الإلكترونية الخاصة بالجامعة يكون تحت مسؤوليتهم المباشرة، ولابد من رجوع جميع الإدارات لهم في جميع العمليات الإلكترونية، كما أنهم يقومون بتقييم سنوي لجميع الإدارات لمعرفة درجة التزامهم بالضوابط التقنية المعطاة لهم.
(2،7)	هل يتم الاستعانة بالخبراء غير المتفرغين من المتخصصين في مجال الأمن السيبراني؛ لمساندة العمادة/ المركز؟	0	0	3	100	غير موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنه لا يوجد عقود رسمية من قبل العمادة/المركز مع خبراء غير متفرغين من المتخصصين في مجال الأمن السيبراني لمساندة العمادة/المركز، ولكن يمكن أن تتم الاستعانة بالخبراء غير المتفرغين من المتخصصين في مجال الأمن السيبراني؛ لمساندة العمادة/ المركز بشكل ودي وتعاوني ودون مقابل، كاستشارة الخبراء في شركة أرامكو، وفي مدينة الملك عبدالعزيز للعلوم والتقنية، وفي مركز سلطان بن عبدالعزيز للعلوم والتقنية، وفي وزارة الاتصالات وتقنية المعلومات، وحدد (مشارك ج) إجابته بأنهم غالبا ما يستشيرونهم عند الرغبة في البدء بالمشاريع التقنية الجديدة، وفيما عدا ذلك فإن العمادة/المركز يعتمد على خبرة موظفيه بشكل أساسي في إدارة أنظمته الإلكترونية.

يتضح من جدول 10 أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم يتضمن (7) أسئلة، جاءت (5) أسئلة منها باستجابة (نعم، موافق) وهو ما يمثل 71% من مجموع أسئلة مجال التنظيم، في حين جاء اثنان من الأسئلة باستجابة (لا، غير موافق)، وهو ما يمثل 29% من مجموع أسئلة مجال التنظيم، وتشير النتيجة السابقة إلى أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم جاء بدرجة عالية.

وتناقش العبارات التالية أعلى ثلاث عبارات ترتبط بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التنظيم، والتي حصلت على درجة موافق بشدة من قبل عينة الدراسة، مرتبة تنازلياً وفقاً للمتوسط الحسابي لها، وذلك على النحو التالي:

- جاءت العبارة رقم (11) وهي (تحديد إدارة أو وحدة تختص بتحقيق الأمن السيبراني بالجامعة) بالمرتبة الأولى بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتنظيم بمتوسط حسابي (4.50) وانحراف معياري (0.69)، وهذا يدل على أن هناك موافقة بشدة بين أفراد الدراسة على هذه العبارة.

وتختلف هذه النتيجة مع ما أشار إليه أفراد الدراسة في المقابلة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (2،1)، بأنهم غير موافقون على أن إدارة العمادة/المركز قد حددت إدارة أو وحدة تختص بتحقيق الأمن السيبراني بالجامعة.

وقد يعزى الاختلاف بين النتيجتين إلى إفادة جميع المشاركين من أفراد الدراسة في المقابلة (مشارك أ، ومشارك ب، ومشارك ج) بأنه لا توجد حاليًا إدارة مختصة بتحقيق الأمن السيبراني في الجامعة، ولكن توجد إدارة تقوم بهذا العمل في الوقت الحالي ولها مسمياتٌ مختلفةٌ في كل جامعة مثل (إدارة المخاطر وأمن المعلومات، أو إدارة المخاطر الرقمية وأمن المعلومات، أو إدارة أمن المعلومات والجودة)، وأشار (مشارك أ) و(مشارك ج) بأنه لا يُمكن الاعتمادُ على هذه الإدارات في تحقيق الأمن السيبراني نظرًا للأدوار المختلفة التي تتطلبها المرحلة الحالية والمرحلة المستقبلية، وأضاف (مشارك أ) بأنهم في المراحل النهائية لإنشاء إدارتين تختصان بتحقيق الأمن السيبراني في الجامعة إحداهما تُعنى بالحوكمة، والأخرى بالتنفيذ، ولكن لم يُعتمد الهيكل التنظيمي الجديد من قبل مدير الجامعة بعد، كما ذكر (مشارك ج) بأنه صَدَرت توجيهات قبل فترة قصيرة من القيادة العليا بالجامعة بإنشاء إدارةٍ باسم (إدارة الأمن السيبراني) ويتم العمل على إنشائها ووضع الأسس التنظيمية لها في الوقت الحالي.

- جاءت العبارة رقم (12) وهي (اعتماد سياسات الاستخدام الآمن لحماية الأصول الإلكترونية بشكل رسمي) بالمرتبة الثانية بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتنظيم بمتوسط حسابي (4.45) وانحراف معياري (0.73)، وهذا يدل على أن هناك موافقة بشدة بين أفراد الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (2،2) من أسئلة المقابلة، بأنهم موافقون على أن إدارة العمادة/المركز اعتمدت سياسات الاستخدام الآمن لحماية الأصول الإلكترونية بشكل رسمي، وتعكس هاتان النتيجتان اهتمام إدارة العمادة/المركز باعتماد سياسات الاستخدام الآمن لحماية الأصول الإلكترونية بشكل رسمي، وقد يعزى ذلك إلى أن هذه السياسات تسهم بشكل كبير في التعرف على واجبات الموظفين ومسؤولياتهم تجاه أنظمة الجامعة وقوانينها التي تسهم في تحقيق الأمن السيبراني.

وتتفق هاتان النتيجتان مع نتيجة دراسة لي وآخرون (Li et al., 2019) التي توصلت إلى أن الموظفين عندما يكونون على دراية بسياسة وإجراءات الأمن السيبراني الخاصة بمؤسستهم فإنهم يكونون أكثر كفاءة لإدارة مهام الأمن السيبراني من أولئك الذين ليسوا على علم بها. ومن هذا المنطلق فإن اعتماد سياسات الاستخدام الآمن من قبل القيادة العليا في الجامعة بشكل رسمي يسهم في تعميمها على جميع الموظفين، وإلزامهم بها بشكل رسمي، مما يسهم في تحقيق الامتثال للضوابط والقوانين دون إهمال أو تهاون.

- جاءت العبارة رقم (13) وهي (وضع القوانين المنظمة للنشاطات الإلكترونية المختلفة في الجامعة) بالمرتبة الثالثة بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتنظيم بمتوسط حسابي (4.31) وانحراف معياري (0.73)، وهذا يدل على أن هناك موافقة بشدة بين أفراد الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (2،3) من أسئلة المقابلة، بأنهم موافقون على أن إدارة العمادة/المركز تضع القوانين المنظمة للنشاطات الإلكترونية المختلفة في الجامعة، وتعكس النتيجتان السابقتان اهتمام العمادة/المركز بوضع القوانين المنظمة للنشاطات الإلكترونية المختلفة في الجامعة، وقد يعزى ذلك إلى حرص إدارة العمادة/المركز على تنظيم العمل وفق قوانين المملكة العربية السعودية، إذ تعمل الهيئة الوطنية للأمن السيبراني على رصد التهديدات المتجددة، وتوجيه القطاعات الحكومية إلى ضرورة اتخاذ الحيطة والحذر من هذه التهديدات، وبالتالي تقوم العمادة/المركز بسن قوانين تحد من هذه التهديدات السيبرانية.

وتختلف هذه النتيجة مع نتيجة دراسة ديفيدسون وهاسليدالين (Davidson & Hasledalen, 2014) التي توصلت إلى نقص ممارسات التوثيق الصارمة، إذ أن مؤسسات التعليم العالي تحجم عن المطالبة بالمزيد من التوثيق الشاق المتعدد العوامل خوفًا من فقدان الطلاب، وقد يعزى هذا الاختلاف إلى طبيعة الاختلاف بين الجامعات موضع الدراسة في كل من الدراستين كون دراسة ديفيدسون وهاسليدالين طبقت على مؤسسات خاصة للتعليم العالي، بينما طبقت هذه الدراسة على الجامعات الحكومية.

السؤال الثالث: ما واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه؟

1. نتائج الاستبانة:

للتعرف على واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه؛ تم حساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري لاستجابات عينة الدراسة، كما تم ترتيب هذه العبارات حسب المتوسط الحسابي لكلاً منها، وذلك وفق جدول 11:

جدول 11

التكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري ودرجة الموافقة والرتبة لواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه

م	العبارات		درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الرتبة
			موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة				
20	نشر التوعية بأهمية الأمن السيبراني بين منسوبي الجامعة.	ك	126	92	6	14		4.39	0.80	موافق بشدة	1
		٪	52.9	38.7	2.5	5.9					
18	تطبيق معايير الجودة سعياً لحصول الجامعة على الاعتمادات الداعمة للأمن السيبراني من المنظمات الدولية المتخصصة مثل منظمة ISO ومنظمة NIST.	ك	114	96	26	2	-	4.35	0.71	موافق بشدة	2
		٪	47.9	40.3	10.9	0.8	-				
19	إعداد الخطط التدريبية لتأهيل موظفي العمادة/المركز في المجالات المختلفة للأمن السيبراني.	ك	80	95	32	23	8	3.91	1.08	موافق	3
		٪	33.6	39.9	13.4	9.7	3.4				
23	مشاركة المعنيين من منسوبي العمادة/المركز في المنصات أو المحافل الدولية للأمن السيبراني.	ك	74	89	50	20	5	3.87	1.02	موافق	4
		٪	31.1	37.4	21.0	8.4	2.1				
22	الشراكة مع مؤسسات القطاع الخاص ذات الصلة لدعم الجهود الاستباقية المحققة للأمن السيبراني.	ك	56	98	63	18	3	3.78	0.93	موافق	5
		٪	23.5	41.2	26.5	7.6	1.3				
21	الشراكة مع مؤسسات المجتمع المدني لتحقيق التكامل في جهود الصمود السيبراني.	ك	65	87	60	21	5	3.78	1.01	موافق	6
		٪	27.3	36.6	25.2	8.8	2.1				
	المتوسط الحسابي العام للمحور							**4.01**	**0.70**	**موافق**	-

يتضح من خلال جدول 11 أن المتوسط الحسابي العام لعبارات المحور بلغ (4.01) بانحراف معياري (0.70)، وهذا يدل على أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه جاء بدرجة عالية.

2. نتائج المقابلة:

أسفرت نتائج المقابلة حول واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، في مجال التوجيه، بعد حساب التكرارات والنسبة المئوية، وتوضيح الإجابات- كما يوضحها جدول 12- عما يلي:

جدول 12

الإجابات الكمية (المحولة) والنوعية لأفراد الدراسة المستهدفين بالمقابلة في مجال التوجيه

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة
		ك	%	ك	%	
(3،1)	هل تم تطبيق معايير الجودة سعياً لحصول الجامعة على الاعتمادات الداعمة للأمن السيبراني من المنظمات الدولية المتخصصة مثل منظمة ISO ومنظمة NIST؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) أن العمادة/المركز حاصل على الاعتماد الدولي لنظام إدارة أمن المعلومات (ISO/IEC 27001) حاليًا، والذي يتضمن تفاصيل عن الوثائق ومسؤولية الإدارة، والتدقيق الداخلي، والتحسين المستمر، والإجراءات التصحيحية والوقائية لإدارة ومراقبة ومراجعة وصيانة وتحسين نظام إدارة أمن المعلومات، ويأتي ذلك استمرارًا للأعوام السابقة التي حصلت فيها العمادة/ المركز على هذا الاعتماد، وأضاف (مشارك أ) بأنهم قد حصلوا أيضًا على الاعتماد لنظام إدارة استمرارية الأعمال (ISO 22301)، والذي يسهم في التنبؤ بالمخاطر والتخطيط لتفاديها.
(3،2)	هل تم إعداد الخطط التدريبية لتأهيل موظفي العمادة/المركز في المجالات المختلفة للأمن السيبراني؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأن العمادة/المركز تعمل بشكل مستمر على تطوير الخطط التدريبية في المجالات المختلفة للأمن السيبراني، وبين كل من (مشارك أ، ومشارك ب) أن هذه الدورات هي دورات من داخل العمادة أو خارجية من جهات أخرى داخل المملكة من خلال ترشيح بعض الموظفين لها، الذين يعودون لتدريب زملائهم بعد ذلك، وأضاف (مشارك أ) بأن أكثر المعوقات التي تواجههم في مجال التدريب هي قلة الموارد في ظل التكلفة الباهظة لدورات الامن السيبراني المتخصصة، وخالفه في ذلك (مشارك ج) بأنهم يقدمون دورات تدريبية عالية المستوى من داخل المملكة أو خارجها كتدريب الموظفين في معاهد متخصصة بالولايات المتحدة الأمريكية أو المملكة المتحدة، وبعض الدورات التدريبية تبلغ مدتها ثلاث سنوات، كما أن المتدربين دخلوا الاختبارات التخصصية بعد هذه الدورات وحصلوا على شهادات اجتياز، وليس فقط كشهادات حضور، ومن ثم يقومون بنقل الأثر لزملائهم داخل مجتمع العمادة/المركز.
(3،3)	هل تم نشر التوعية بأهمية الأمن السيبراني بين منسوبي الجامعة؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأن العمادة/ المركز تسهم في نشر التوعية بأهمية الأمن السيبراني بين منسوبي الجامعة، وذلك بعدة وسائل، وكانت أهم الوسائل التي ذكرت في إجابتهم هي:

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				الإجابة النوعية
		نعم، موافق		لا، غير موافق	درجة الموافقة	
		ك	%	ك	%	
						الحملات التوعوية في كليات الجامعة، عبارات التوعية على الشاشات الإلكترونية داخل مرافق الجامعة، رسائل التوعية عبر الايميل الإلكتروني لمنسوبي الجامعة، المحاضرات، الندوات، رسائل التوعية على شاشات التوقف على أجهزة الحاسب الآلي، الرسائل النصية القصيرة، المنشورات الإلكترونية والورقية، وأضاف (مشارك ج) بأن وسائل التوعية تكون موجهة باللغتين العربية والانجليزية.
(3،4)	هل توجد برامج للشراكة مع مؤسسات المجتمع المدني؛ لتحقيق التكامل في جهود الصمود السيبراني؟	0	0	3	100	غير موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنه لا توجد برامج شراكة بعقود رسمية وموقعة مع أي من مؤسسات المجتمع المدني تحقق التكامل في جهود الصمود السيبراني، وإنما جميع البرامج الحالية _ إن وجدت _ فهي برامج تعاونية وغير رسمية، وأضاف (مشارك ج) بأنه لديهم عقد شراكة مع جامعة ناشئة إلا أنه لم يتم فيه تبادل الخبرات الأمنية وإنما للاستعانة بخبرتهم في عمل مقابلات التوظيف في عدة مجالات تقنية ومنها وظائف الأمن السيبراني، إلا أن هذا العقد كان مقابل مبلغ زهيد جدًا، الأمر الذي يمكن تصنيفه ضمن وظيفة خدمة المجتمع.
(3،5)	هل توجد برامج للشراكة مع مؤسسات القطاع الخاص ذات الصلة؛ لدعم الجهود الاستباقية المحققة للأمن السيبراني؟	0	0	3	100	غير موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنه لا توجد برامج شراكة بعقود رسمية وموقعة مع أي من مؤسسات القطاع الخاص ذات الصلة؛ التي يمكن أن تدعم الجهود الاستباقية المحققة للأمن السيبراني، وإنما جميع البرامج الحالية _ إن وجدت _ فهي برامج تعاونية وغير رسمية.
(3،6)	هل شارك المعنيين من منسوبي العمادة/المركز في المنصات أو المحافل الدولية للأمن السيبراني؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنه يوجد مشاركة لبعض منسوبي العمادة/المركز في المنصات أو المحافل الدولية للأمن السيبراني ولكنها محدودة جدًا وعلى نطاق ضيق، وأضاف (مشارك ج) بأنهم شاركوا في مؤتمر عام 2018 من تنظيم شركة (Palo Alto Networks) حول الجدران النارية.

يتضح من جدول 12 أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه يتضمن (6) أسئلة، جاءت (4) أسئلة منها باستجابة (نعم، موافق) وهو ما يمثل 67% من مجموع أسئلة مجال التوجيه، في حين جاء اثنان من الأسئلة باستجابة (لا، غير موافق)، وهو ما يمثل 33% من مجموع أسئلة مجال التوجيه، وتشير النتيجة السابقة إلى أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه جاءت بدرجة عالية.

وتناقش العبارات التالية أعلى ثلاث عبارات ترتبط بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التوجيه، والتي حصلت على درجة (موافق بشدة) من قبل عينة الدراسة، مرتبة تنازليًا وفقاً للمتوسط الحسابي لها، وذلك على النحو التالي:

- جاءت العبارة رقم (20) وهي (نشر التوعية بأهمية الأمن السيبراني بين منسوبي الجامعة) بالمرتبة الأولى بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتوجيه بمتوسط حسابي (4.39) وانحراف معياري (0.80)، وهذا يدل على أن هناك موافقة بشدة بين عينة الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (3،3) من أسئلة المقابلة، بأنهم موافقون على أن إدارة العمادة/المركز تسهم بنشر التوعية بأهمية الأمن السيبراني بين منسوبي الجامعة، وقد تعزى النتيجتان السابقتان إلى كثرة التهديدات السيبرانية، وتسارع تطورها نتيجة للتحول الرقمي في إدارة أنظمة الجامعات على الصعيدين الإداري والأكاديمي.

وتختلف هاتان النتيجتان مع نتيجة دراسة مالافت (Malavet, 2017) التي أشارت إلى ضعف برامج التوعية بالأمن السيبراني، وضرورة العناية بها، لما يترتب عليها من تحقيق الامتثال لضوابط الأمن السيبراني بشكل مباشر، وقد يعزى هذا الاختلاف إلى أن الجامعات موضع الدراسة هي من الجامعات المصنفة عالميًا، وذات سمعة عالية، مما يجعلها تحرص على توعية منسوبيها بطرق مختلفة حول التهديدات السيبرانية المحتملة بشكل مستمر.

- جاءت العبارة رقم (18) وهي (تطبيق معايير الجودة سعياً لحصول الجامعة على الاعتمادات الداعمة للأمن السيبراني من المنظمات الدولية المتخصصة مثل منظمة ISO ومنظمة NIST) بالمرتبة الثانية بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتوجيه بمتوسط حسابي (4.35) وانحراف معياري (0.71)، وهذا يدل على أن هناك موافقة بشدة بين عينة الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (1،3) من أسئلة المقابلة، بأنهم موافقون على أن إدارة العمادة/المركز تطبق معايير الجودة سعيًا لحصول الجامعة على الاعتمادات الداعمة للأمن السيبراني من المنظمات الدولية المتخصصة، وقد تعزى النتيجتان السابقتان إلى أن الحصول على الاعتمادات الدولية الداعمة للأمن السيبراني يسهم في حصول المؤسسة على التميز المؤسسي وتحقيق التنافسية، كما يزيد من مستوى الثقة لدى أفراد المجتمع بقدرة الجامعة على الدفاع عن أنظمتها الإلكترونية، ويحميها من المطالبات القانونية حال الانتهاكات السيبرانية لا سمح الله.

أما العبارات التالية فقد حصلت على درجة (موافق) من قبل عينة الدراسة، وقد تم ترتيبها تصاعديًا وفقًا للمتوسط الحسابي لها، وذلك على النحو التالي:

- جاءت العبارة رقم (21) وهي (الشراكة مع مؤسسات المجتمع المدني لتحقيق التكامل في جهود الصمود السيبراني) بالمرتبة السادسة بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتوجيه بمتوسط حسابي (3.78) وانحراف معياري (1.01)، وهذا يدل على أن هناك موافقة بين عينة الدراسة على هذه العبارة.

وتختلف هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (4،3) من أسئلة المقابلة، بأنهم غير موافقون على أن إدارة العمادة/المركز لديها برامج للشراكة مع مؤسسات المجتمع المدني؛ لتحقيق التكامل في جهود الصمود السيبراني.

وقد يعزى الاختلاف بين نتيجتي الدراسة الكمية في العبارة رقم (21) ونتيجتي الدراسة النوعية في السؤال (4،3)؛ إلى الخلط بين مفهومي (الشراكة المجتمعية) و(خدمة المجتمع) لدى عينة الدراسة، إذ إن خدمة المجتمع تعني: الخدمات التي يتطوع بها الأفراد أو المنظمات لصالح المجتمع أو مؤسساته (Houghton Mifflin Harcourt Publishing, 2016)، بينما تشير الشراكة إلى أنها: عقد بين اثنين أو أكثر للقيام بعمل مشترك (سليم, 2005)، وبناء على ذلك فإن جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) من أفراد الدراسة في المقابلة أكدوا عدم وجود برامج شراكة رسمية بعقود موقعة بين طرفين فيما يختص بمجال الأمن السيبراني، وأن جميع البرامج الحالية مع القطاع الحكومي _إن وجدت_ فهي برامج تطوعية تعاونية وغير رسمية ودون توقيع ملزم بين الطرفين.

وقد يعزى عدم اهتمام إدارة العمادة/المركز بإيجاد برامج للشراكة مع مؤسسات المجتمع المدني إلى حداثة الاهتمام بالأمن السيبراني في المملكة العربية السعودية، إذ من المتوقع أن تشهد السنوات القادمة المزيد من الاهتمام في عقد برامج الشراكة مع القطاع العام لتحقيق التكامل في جهود الصمود السيبراني، خصوصًا بعد إنشاء الهيئة الوطنية للأمن السيبراني التي يؤمل أن تسهم بشكل بارز في تنسيق جهود الشراكة بين القطاعات.

السؤال الرابع: ما واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم؟

1. نتائج الاستبانة:

للتعرف على واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم؛ تم حساب التكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري لاستجابات عينة الدراسة، كما تم ترتيب هذه العبارات حسب المتوسط الحسابي لكلاً منها، وذلك وفق جدول 13:

جدول 13

التكرارات والنسب المئوية والمتوسطات الحسابية والانحراف المعياري ودرجة الموافقة والرتبة لواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم

م	العبارات		درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الرتبة
			موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة				
27	تحديث برمجيات الأصول الإلكترونية بشكل دوري.	ك	137	85	8	5	3	4.46	0.77	موافق بشدة	1
		٪	57.6	35.7	3.4	2.1	1.3				
28	تحديث السياسات الأمنية بما يحقق الأمن السيبراني في الجامعة.	ك	116	94	22	3	3	4.33	0.80	موافق بشدة	2
		٪	48.7	39.5	9.2	1.3	1.3				
26	استخدام الأنظمة التقنية؛ للكشف عن نقاط الضعف السيبراني.	ك	102	103	28	4	1	4.26	0.76	موافق بشدة	3
		٪	42.9	43.3	11.8	1.7	0.4				
25	حصر جميع الأضرار المترتبة على انتهاك الأصول الإلكترونية.	ك	87	99	47	4	1	4.12	0.81	موافق	4
		٪	36.6	41.6	19.7	1.7	0.4				
24	تحليل سجلات الهجمات السيبرانية السابقة التي تعرضت لها الجامعة.	ك	91	94	44	6	3	4.11	0.88	موافق	5
		٪	38.2	39.5	18.5	2.5	1.3				
31	مراجعة خطط الاستجابة والتعافي من الهجمات السيبرانية بشكل دوري للتأكد من جاهزيتها.	ك	80	103	45	7	3	4.05	0.87	موافق	6
		٪	33.6	43.3	18.9	2.9	1.3				
30	فحص المقاييس الأمنية بانتظام للتحقق من	ك	82	95	48	11	2	4.03	0.90	موافق	7
		٪	34.5	39.9	20.2	4.6	0.8				

م	العبارات		درجة الموافقة					المتوسط الحسابي	الانحراف المعياري	درجة الموافقة	الرتبة
	مستوى السلامة السيبرانية.		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة				
29	إجراء اختبارات الاختراق بشكل دوري للتحقق من مستوى النضج السيبراني.	ك	86	83	53	14	2	4.00	0.95	موافق	8
		٪	36.1	34.9	22.3	5.9	0.8				
المتوسط الحسابي العام للمحور								**4.17**	**0.67**	**موافق**	**-**

يتضح من خلال جدول 13 أن المتوسط الحسابي العام لعبارات المحور بلغ (4.17) بانحراف معياري (0.67)، وهذا يدل على أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم جاء بدرجة عالية.

1. نتائج المقابلة:

أسفرت نتائج المقابلة حول واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، في مجال التقويم، بعد حساب التكرارات والنسبة المئوية، وتوضيح الإجابات- كما يوضحها جدول 14- عما يلي:

جدول 14

الإجابات الكمية (المحولة) والنوعية لأفراد الدراسة المستهدفين بالمقابلة في مجال التقويم

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية					الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة	
		ك	%	ك	%		
(4،1)	هل يتم تحليل جميع سجلات الهجمات السيبرانية التي تعرضت لها الجامعة بشكل دوري؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنه يتم تحليل جميع سجلات الهجمات السيبرانية التي تعرضت لها الجامعة -إن وجدت- بشكل دوري وفق عدد من المؤشرات مثل النسبة المئوية لعدد الهجمات السيبرانية، ومصادرها، ونوع البيانات المستهدفة.
(4،2)	هل يتم حصر جميع الأضرار المترتبة على انتهاك الأصول الإلكترونية؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنهم يقومون بحصر الاضرار المترتبة على انتهاك الأصول الإلكترونية -إن وجدت فور وقوعها، عن طريق فريق الاستجابة للحوادث السيبرانية، الذي من مهامه رفع تقرير لعميد/مدير العمادة/المركز حول الأضرار المترتبة على الانتهاك السيبراني.
(4،3)	هل يتم استخدام الأنظمة التقنية؛ للكشف عن نقاط الضعف السيبراني؟	3	100	0	0	موافق	أفاد (مشارك أ، ومشارك ب) بأنهم يعتمدون على أدوات وبرامج مخصصة للكشف عن نقاط الضعف السيبراني -دون الإفصاح عن مسمياتها-، وأضاف (مشارك أ) بأنه توجد

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية					الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة	
		ك	%	ك	%		
							أنظمة تقنية متقدمة (SIEM Solution) تقدم تحليلًا في الوقت الحقيقي للتنبيهات الأمنية التي يتم إنشاؤها بواسطة التطبيقات وأجهزه الشبكة، إلا أن ميزانية العمادة/المركز تحول دون توفيرها بسبب ارتفاع تكلفتها السنوية، بينما أكد (مشارك ج) بأن العمادة/المركز تعتمد على نظام (SIEM Solution) متقدم جدًا، وأنه تم توفيره للعمادة/المركز منذ ستة أشهر بدعم من إدارة الجامعة، وقد استغرقت عملية اعتماد هذا النظام مدة سنة ونصف نظرًا لتكاليفه الباهظة جدًا.
(4،4)	هل يتم تحديث برمجيات الأصول الإلكترونية؛ بشكل دوري؟	3	100	0	0	موافق	أفاد جميع المشاركين (مشارك أ، ومشارك ب، ومشارك ج) بأنهم يعملون على تحديث برمجيات الأصول الإلكترونية، ولكن جاءت الإجابات متغايرة حول كيفية التحديث، فقد جاءت إجابة (مشارك أ) بأن التحديث الدوري يكون فقط لبرامج الحماية وأنظمة التشغيل وبرامج الأوفيس، وما عدا ذلك يتم تحديثه بين وقت وآخر ولكن ليس بصفة دورية، أما (مشارك ب) فأشار إلى وجود نظام أمني ترتبط به أجهزة الحاسب الموجودة بالجامعة ويتم تحديث برامج التشغيل مركزيًا دون الرجوع لخوادم الشركة المنتجة، وأي جهاز لا يقبل التحديث يتم استبعاده بشكل تلقائي من هذا النظام مما يُبقي هذا الجهاز دون تحديث حتى يتم تحديثه يدويا، أما (مشارك ج) فقد أشار إلى أن أنظمة التحديث والسياسات موجودة ولكن يوجد خلل في الإجراءات الخاصة بتحديث البرمجيات وغالبًا ما تكون عشوائية، إذ إن آلية عمل التحديثات غير متوافقة مع سياسة العمادة/المركز ويجب إنشاء فريق مختص بعمل التحديثات بصورة منتظمة ومهنية.
(4،5)	هل يتم تحديث السياسات الأمنية؛ بما يحقق الأمن السيبراني في الجامعة؟	3	100	0	0	موافق	أفاد (مشارك أ ومشارك ب ومشارك ج) بأن السياسات الأمنية الخاصة بتحقيق الأمن السيبراني في الجامعة يتم تحديثها بشكل دوري لسد الثغرات الأمنية، كما يتم دراسة درجة تطبيقها بين منسوبي الجامعة بشكل دوري.
(4،6)	هل يتم إجراء اختبارات الاختراق بشكل دوري؛ للتحقق من مستوى النضج السيبراني؟	2	67	1	33	موافق	أفاد (مشارك أ ومشارك ب) بأن العمادة/المركز يُجري اختبارات الاختراق بشكل دوري؛ للتحقق من مستوى النضج السيبراني، بينما أشار (مشارك ج) بأنه لا يوجد اختبارات للاختراق، ولكن يوجد تقييم لنقاط الضعف بشكل دوري بحكم امتلاك العمادة/المركز لنظام (SIEM Solution)

رقم السؤال	السؤال	الإجابة بعد تحويلها من نوعية إلى كمية				الإجابة النوعية
		نعم، موافق		لا، غير موافق		درجة الموافقة
		ك	%	ك	%	
						الذي يقدم تحليلاً في الوقت الحقيقي للتنبيهات الأمنية التي يتم إنشاؤها بواسطة التطبيقات وأجهزه الشبكة، والذي يمكن الاعتماد عليه كبديل عن إجراء اختبارات الاختراق بشكل دوري.
(4،7)	هل يتم فحص المقاييس الأمنية بانتظام؛ للتحقق من مستوى السلامة السيبرانية؟	3	100	0	0	أفاد (مشارك أ ومشارك ب ومشارك ج) بأنه يتم بانتظام فحص المقاييس الأمنية؛ للتحقق من مستوى السلامة السيبرانية، وذلك عن طريق برامج وأدوات كشف نقاط الضعف السيبراني، إذ تقدم هذه البرامج والأدوات تقريرًا مفصلًا يمكن استخدامه كمقياس أمني يسهم في التحقق من مستوى السلامة السيبرانية، وتُعنى إدارة العمادة/المركز بهذه المقاييس لاستنتاج وتقييم نقاط القوة الضعف في أنظمتها الإلكترونية.	موافق
(4،8)	هل يتم مراجعة خطط الاستجابة والتعافي من الهجمات السيبرانية بشكل دوري؛ للتأكد من جاهزيتها؟	3	100	0	0	أفاد (مشارك أ ومشارك ب ومشارك ج) بأنه يتم مراجعة خطط الاستجابة والتعافي من الهجمات السيبرانية بشكل دوري؛ للتأكد من جاهزيتها وفقًا لمستجدات المرحلة الحالية، وحدد (مشارك أ) عمليات التحديث بأنها ربع سنوية.	موافق

يتضح من جدول 14 أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم يتضمن (8) أسئلة، جاءت (7) أسئلة منها باستجابة (نعم، موافق) وهو ما يمثل 87.5% من مجموع أسئلة مجال التقويم، في حين اختلفت إجابة سؤال واحد بين استجابة (نعم، موافق) و(لا، غير موافق)، وهو ما يمثل 12.5% من مجموع أسئلة مجال التقويم، وتشير النتيجة السابقة إلى أن واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم جاء بدرجة عالية.

ومما سبق يمكن ملاحظة أن واقع ممارسة إدارة الجامعات السعودية الحكومية لدورها في تحقيق الأمن السيبراني بشكل عام جاء بدرجة عالية، حيث بلغ مجموع الاستجابات التي حملت إجابة (نعم، موافق) من قبل أفراد الدراسة (23) استجابة من مجموع (31) استجابة، وهو ما يمثل نسبة 74% من مجموع استجابات واقع ممارسة إدارة الجامعات السعودية الحكومية لدورها في تحقيق الأمن السيبراني، بينما بلغ مجموع الاستجابات التي حملت إجابة (لا، غير موافق) من قبل أفراد الدراسة (7) استجابات من مجموع (31) استجابة، وهو ما يمثل نسبة 23% من مجموع استجابات واقع ممارسة إدارة الجامعات السعودية الحكومية لدورها في تحقيق الأمن السيبراني، واختلف أفراد الدراسة في (استجابة واحدة) من مجموع (31) استجابة، وهو ما يمثل نسبة 3% من مجموع استجابات واقع ممارسة إدارة الجامعات السعودية الحكومية لدورها في تحقيق الأمن السيبراني، حيث أتى مجال التقويم أولًا بنسبة موافقة (87,5%)، ثم مجالي التخطيط والتنظيم ثانيًا بنسبة موافقة (71%)، ثم مجال التوجيه ثالثًا بنسبة موافقة (67%) وقد جاءت جميع المجالات (التخطيط، التنظيم، التوجيه، التقويم)، بدرجة استجابة موافق.

وتختلف نتائج الدراسة الكمية عن نتائج الدراسة النوعية في ترتيب المجالات الخاصة بمحور واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، إلا أنها اتفقت على أن مجال التوجيه هو أقل المجالات من حيث ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، مما يستدعي ضرورة المبادرة من قبل إدارة الجامعات للاهتمام بهذا المجال بشكل مكثف.

وتناقش العبارات التالية أعلى ثلاث عبارات ترتبط بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني في مجال التقويم، والتي حصلت على درجة (موافق بشدة) من قبل عينة الدراسة، مرتبة تنازليًا وفقاً للمتوسط الحسابي لها، وذلك على النحو التالي:

- جاءت العبارة رقم (27) وهي (تحديث برمجيات الأصول الإلكترونية بشكل دوري) بالمرتبة الأولى بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتقويم بمتوسط حسابي (4.46) وانحراف معياري (0.77)، وهذا يدل على أن هناك موافقة بشدة بين عينة الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (4،4) من أسئلة المقابلة، بأنهم موافقون على أن إدارة العمادة/المركز تعمل على تحديث برمجيات الأصول الإلكترونية؛ بشكل دوري، وتعكس هاتان النتيجتان اهتمام إدارة العمادة/المركز بتحديث برمجيات الأصول الالكترونية بشكل دوري، وقد يعزى هذا الاهتمام إلى سهولة اختراق الأنظمة والأجهزة والشبكات عند عدم تحديث هذه البرامج، بسبب الإعلان عن وجود الثغرات، مما يسهل من اقتناص المخترقين لهذه الفرص.

- جاءت العبارة رقم (28) وهي (تحديث السياسات الأمنية بما يحقق الأمن السيبراني في الجامعة) بالمرتبة الثانية بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتقويم بمتوسط حسابي (4.33) وانحراف معياري (0.80)، وهذا يدل على أن هناك موافقة بشدة بين عينة الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (5،4) من أسئلة المقابلة، بأنهم موافقون على أن إدارة العمادة/المركز تعمل على تحديث السياسات الأمنية؛ بما يحقق الأمن السيبراني في الجامعة، وتعكس النتيجتان السابقتان اهتمام إدارة العمادة/المركز بتحديث السياسات الأمنية بما يحق الأمن السيبراني في الجامعة، وقد يعزى هذا الاهتمام إلى أن هذا التحديث يسهم في مواكبة المستجدات، كما يسهم في اختبار فاعلية هذه السياسة بشكل مستمر.

- جاءت العبارة رقم (26) وهي (استخدام الأنظمة التقنية؛ للكشف عن نقاط الضعف السيبراني) بالمرتبة الثالثة بين العبارات الخاصة بواقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني فيما يتعلق بالتقويم بمتوسط حسابي (4.26) وانحراف معياري (0.76)، وهذا يدل على أن هناك موافقة بشدة بين عينة الدراسة على هذه العبارة.

وتتفق هذه النتيجة مع ما أشار إليه أفراد الدراسة (مشارك أ، مشارك ب، مشارك ج) في إجابتهم عن السؤال (4،3) من أسئلة المقابلة، بأنهم موافقون على أن إدارة العمادة/المركز تستخدم الأنظمة التقنية؛ للكشف عن نقاط الضعف السيبراني، وقد تعزى النتيجتان السابقتان إلى صعوبة الاعتماد على القدرات البشرية في عمليات المراقبة والتحليل، للكشف عن نقاط الضعف السيبراني، في ظل اتساع هيكلة الجامعات -موضع الدراسة- وضخامة أعداد منسوبيها، بينما توفر هذه الأنظمة السرعة والكفاءة في عمليات التحليل وبشكل مستمر، إلا أن تكلفتها الباهظة تحول دون اقتنائها أحيانًا، مما يستلزم الاستعانة بمصادر خارجية لتوفير الدعم والمساندة.

أبرز نتائج الدراسة وتوصياتها

أولًا: خلاصة نتائج الدراسة

1. النتائج المستخلصة من الاستبانة

جاءت موافقة عينة الدراسة على واقع ممارسة إدارة الجامعات السعودية الحكومية لدورها في تحقيق الأمن السيبراني بدرجة عالية، حيث أتى مجال التنظيم بالمرتبة الأولى، يليه مجال التقويم بالمرتبة الثانية، وبالمرتبة الثالثة يأتي مجال التخطيط، وفي الأخير جاء مجال التوجيه كأقل المجالات من حيث ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، وقد جاءت جميعها بدرجة استجابة (موافق).

تمثلت أعلى العبارات موافقة في مجال التخطيط بما يلي:

- تحديد الأصول الإلكترونية المستهدفة بالهجمات السيبرانية؛ بالتنسيق مع الجهات ذات العلاقة في الجامعة.
- تصنيف الأصول الإلكترونية المستهدفة بالهجمات السيبرانية إلى فئات رئيسية بحسب نوعها.
- وضع خطة للاستجابة والتعافي، حال تعرض الجامعة لهجمات سيبرانية مؤثرة.

وتمثلت أعلى العبارات موافقة في مجال التنظيم بما يلي:

- تحديد إدارة أو وحدة تختص بتحقيق الأمن السيبراني بالجامعة.
- اعتماد سياسات الاستخدام الآمن لحماية الأصول الإلكترونية بشكل رسمي.
- وضع القوانين المنظمة للنشاطات الإلكترونية المختلفة في الجامعة.

وتمثلت أعلى العبارات موافقة في مجال التوجيه بما يلي:

- نشر التوعية بأهمية الأمن السيبراني بين منسوبي الجامعة.
- تطبيق معايير الجودة سعياً لحصول الجامعة على الاعتمادات الداعمة للأمن السيبراني من المنظمات الدولية المتخصصة مثل منظمة ISO ومنظمة NIST.
- إعداد الخطط التدريبية لتأهيل موظفي العمادة/المركز في المجالات المختلفة للأمن السيبراني.

وتمثلت أعلى العبارات موافقة في مجال التقويم بما يلي:

- تحديث برمجيات الأصول الإلكترونية بشكل دوري.
- تحديث السياسات الأمنية بما يحقق الأمن السيبراني في الجامعة.
- استخدام الأنظمة التقنية؛ للكشف عن نقاط الضعف السيبراني.

2. النتائج المستخلصة من المقابلة:

جاءت موافقة أفراد الدراسة المستهدفون بالمقابلة على واقع ممارسة إدارة الجامعات السعودية الحكومية لدورها في تحقيق الأمن السيبراني في جميع المجالات الأربعة بدرجة عالية، حيث أتى مجال التقويم أولًا، ثم مجالي التخطيط والتنظيم ثانيًا، ثم مجال التوجيه ثالثًا، وقد جاءت جميع المجالات (التخطيط، التنظيم، التوجيه، التقويم)، بدرجة استجابة (موافق).

توصيات الدراسة

توصي هذه الدراسة في ضوء نتائج الدراسة بما يلي:

جاءت العبارات (17،21،22،23) كأقل العبارات موافقة في واقع ممارسة إدارة الجامعات لدورها في تحقيق الأمن السيبراني، من خلال المجالات التالية (مجال التخطيط، مجال التنظيم، مجال التوجيه، مجال التقويم)، لذلك توصي هذه الدراسة بما يلي:

- الاستعانة بالخبراء غير المتفرغين من المتخصصين في مجال الأمن السيبراني؛ لمساندة العمادة/ المركز المختص بتقنية المعلومات بالجامعة، من خلال العقود الرسمية.
- مساندة المعنيين من منسوبي العمادة/المركز لإشراكهم في المنصات أو المحافل الدولية للأمن السيبراني.
- إيجاد برامج للشراكة مع مؤسسات القطاع الخاص ذات الصلة؛ تدعم الجهود الاستباقية المحققة للأمن السيبراني.
- إيجاد برامج للشراكة مع مؤسسات المجتمع المدني، تحقق التكامل في جهود الصمود السيبراني.

المراجع:

أولًا: المراجع العربية

أبو زيد، عبد الرحمن عاطف. (2019). الأمن السيبراني الوطن العربي: دراسة حالة المملكة العربية السعودية .*آفاق سياسية: المركز العربي للبحوث والدراسات*، ع48، 55-61.

البار، عدنان والمرحبي، خالد. (2018). أمن المعلومات والأمن السيبراني. مسترجع بتاريخ 2020/2/19 على الرابط https://bit.ly/2P1zPt6

برنامج التحول الوطني 2020. (2016). مسترجع بتاريخ 2020/2/19 على الرابط https://www.yesser.gov.sa/ar/Documents/NTP_ar-2.pdf.

الربيعة، صالح. (2018). الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت. ورقة عمل منشورة في الملتقى الأول لتقنية المعلومات، جدة. مسترجع بتاريخ 2020/2/19 على الرابط https://bit.ly/2KxYhSw

الردفاني، محمد قاسم أسعد. (2014). تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية. *المجلة العربية للدراسات الأمنية: جامعة نايف العربية للعلوم الأمنية*، مج30, ع61، 157 - 192.

رؤية المملكة العربية السعودية 2030. (2016). مسترجع بتاريخ 2020/2/19 على الرابط https://vision2030.gov.sa/download/file/fid/422

الشمري، حامد. (2015). *رؤية إستراتيجية لحماية الفضاء الإلكتروني للمملكة العربية السعودية*. رسالة ماجستير غير منشورة، قسم الدراسات الإستراتيجية، كلية العلوم الإستراتيجية، جامعة نايف العربية للعلوم الأمنية.

المنتدى الدولي للأمن السيبراني. (2020). *بيان الرياض للأمن السيبراني*. مسترجع بتاريخ 2020/2/19 على الرابط https://globalcybersecurityforum.com/ar/declaration

مؤتمر حلول القيادة والسيطرة. (2016). جامعة الملك سعود، الرياض. مسترجع بتاريخ 2020/2/19 على الرابط https://bit.ly/2y5bFJ1

الهيئة الوطنية للأمن السيبراني. (2020). عن الهيئة الوطنية للأمن السيبراني. مسترجع بتاريخ 2020/2/19 على الرابط https://nca.gov.sa/pages/about.html

وزارة التعليم العالي. (2011). الخطة المستقبلية للتعليم الجامعي في المملكة العربية السعودية (آفاق). مسترجع بتاريخ 2020/2/19 على الرابط http://stp.kku.edu.sa/ar/content/1101

ثانيًا: المراجع الأجنبية

Bakertilly. (2018). *Higher education roadmap to building a sustainable cybersecurity management program*. In. Retrieved Feb 19,2020 from https://bakertilly.com/insights/cybersecurity-management-in-higher-education/

Bjerken, A. (2017). *Identifying Why Organizations Fail to Adopt Active Cyber-Security Strategies Assessed using the Unified Theory of Acceptance and Use of Technology Survey (UTAUT-S).* (D.B.A.), Northcentral University, Ann Arbor. Retrieved Feb 19,2020 from https://search.proquest.com/docview/1904975357?accountid=142908

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10).

Creswell, J. W. (2012). *Educational research : planning, conducting, and evaluating quantitative and qualitative research*. 4th ed. Boston: Pearson Education.

Creswell, J. W. (2014). Research design : qualitative, quantitative, and mixed methods approaches. 4th ed. SAGE Publications: Los Angeles.

Creswell, J. W., & Plano Clark, V. L. (2011). *Designing and Conducting Mixed Methods Research* (2nd Edition ed.). Los Angeles: Sage Publications.

Davidson, P., & Hasledalen, K. (2014). Cyber Threats to Online Education: A Delphi Study. *Proceedings of the International Conference on Management, Leadership & Governance*, 68-77.

Diaz, L. J., Anderson, M. C., Wolak, J. T., & Opderbeck, D. (2017). The Risks and Liability of Governing Board Members to Address Cyber Security Risks in Higher Education. *Journal of College and University Law, 40*(6), 43-49.

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(7).

Grama, J. (2014). *Just in Time Research: Data Breaches in Higher Education.* Retrieved Feb 19,2020 from https://bit.ly/2QvWxfO

Henderson, A. (2019). The CIA Triad: Confidentiality, integrity, availability. Retrieved Feb 19,2020 from https://goo.gl/UNiHpL

InfoSec Institute. (2018). The Security CIA Triad. Retrieved Feb 19,2020 from https://bit.ly/2ErZ8AL

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. doi:https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Malavet, J. N. (2017). *Cyber Security in Higher Education: Accuracy of Resources Utilized by Information Technology Departments to Prevent Data Breaches.* (10682256 M.S.), Utica College, Ann Arbor. Retrieved Feb 19,2020 from https://search.proquest.com/docview/1973587134?accountid=142908

McClurg, J. D. (2015). *Cybersecurity in Higher Education: Oversight and Due Diligence.* (Ed.D.), Aspen University, Ann Arbor. Retrieved Feb 19,2020 from https://search.proquest.com/docview/1846958719?accountid=142908 ProQuest Dissertations & Theses Global database. (10291072)

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516. doi:10.1016/j.adhoc.2012.02.016

National Initiative for Cyber Security Careers and Studies. (2018). *A Glossary of Common Cyber security Terminology.* Retrieved Feb 19,2020 from https://goo.gl/9Xq4B5

Ramirez, R. B. (2017). Making cyber security interdisciplinary : recommendations for a novel curriculum and terminology harmonization

Readiness and Emergency Management for Schools Technical Assistance Center. (2018). *Cybersecurity Considerations for Institutions of Higher Education*. Retrieved Feb 19,2020 from https://bit.ly/2SNfxTt

Said, S. E. (2018). *Pedagogical Best Practices in Higher Education National Centers of Academic Excellence / Cyber Defense Centers of Academic Excellence in Cyber Defense.* (10748708 Ed.D.Ed.Lead.), Union University, Ann Arbor. Retrieved Feb 19,2020 from https://goo.gl/4bDVF3

The International Telecommunication Union, The World Bank, Commonwealth Secretariat, The Commonwealth Telecommunications Organisation, & NATO Cooperative Cyber Defence Centre of Excellence. (2018). *Guide to Developing*

a National Cybersecurity Strategy – Strategic engagement in cybersecurity. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

U.S. Department of Homeland Security. (2015). *Malicious Cyber Actors Target US Universities and Colleges.* Retrieved Feb 19,2020 from https://bit.ly/2Ehy9qN

Universities UK. (2013). *Cyber Security and Universities; Managing the Risk.* Retrieved Feb 19,2020 from https://goo.gl/yw1w64