IUGJEPS
Vol 29, No 6, 2021, pp 353-372

ISSN 2410-3152

مجلة الجامعة الإسلامية للدراسات التربوية والنفسية

تاريخ الإرسال (02-06-2021)، تاريخ قبول النشر (23-07-2021)

الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة

اسم الباحث: أ. منير عبد الله مفلح البيشي

اسم الجامعة والبلد: المملكة العربية السعودية

* البريد الالكتروني للباحث المرسل:

E-mail address: gheedaan@gmail.com

https://doi.org/10.33976/IUGJEPS.29.6/2021/14

الملخص:

هدفت الدراسة إلى معرفة واقع الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقافة الرقمية من وجهة نظر أعضاء هيئة التدريس، ولتحقيق أهداف الدراسة استُخدم المنهج الوصفي التحليلي، وكانت أداة الدراسة عبارة عن استبانة تنقسم إلى محور للأمن السيبراني ومحور للثقة الرقمية، وطُبقت الاستبانة على عينة اختيرت عشوائياً وبلغت (210) عضو هيئة تدريس، فاستجاب منهم (182) عضواً. وتوصلت الدراسة إلى عدة نتائج جاء أهمها أن واقع الأمن السيبراني بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعاً بنسبة (73.18%)، كما تبين أن مستوى الثقة الرقمية للجامعات السعودية من وجهة نظر أعضاء هيئة التدريس مرتفعاً بنسبة (74.58%)، وتبين أن الأمن السيبراني في الجامعات السعودية يؤثر في تعزيز الثقة الرقمية، حيث بلغت نسبة التأثير (46.70%)، وتبين أنه لا توجد فروق بين استجابات المبحوثين حول الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية تعزى لمتغيري سنوات الخدمة والدرجة العلمية والتفاعل بينهما.

وقدمت الدراسة مجموعة من التوصيات جاء أبرزها تخصيص موازنة لتوفير متطلبات الأمن السيبراني وتطبيقاته، ومزيد من الاهتمام ببرامج حماية وأمن المعلومات لما لها أثر في ثقة المستفيد الرقمية.

كلمات مفتاحية: الأمن السيبراني – الثقة الرقمية – الجامعات السعودية.

Cyber Security in Saudi Universities and its Impact on Enhancing Digital Confidence from Members Point of View: Study at Bisha University

Abstract:

The study aimed to identify the reality of cybersecurity in Bisha University and its impact on promoting digital confidence according to faculty members point of view, to achieve the study objectives, the descriptive and analytical approach have been used. The study tool was a questionnaire include the cybersecurity topic and digital trust topic, and the questionnaire was conducted on a randomly selected sample of (210) faculty members, (182) of them are staff, the study showed several results included the most important point is that the reality of cybersecurity in Saudi universities is high from the point of view of faculty members (73.18%). Also, it was found that the level of digital confidence in Saudi universities from the faculty members' perspective is high as well (74.58%), and the cybersecurity in Saudi universities affects the enhancement of digital confidence, whereas the impact rate has reached (46.70%). It was found that there are no differences between the respondents' responses about cybersecurity in Saudi universities and its impact on enhancing digital confidence due to the years of service variable, academic degree, and the interaction between them. Moreover, the study presented a set of recommendations, most notably a budget was allocated to provide the cybersecurity requirements, their applications, and more attention to information protection and security programs because of its impact on beneficiary's digital trust. The study presented a set of recommendations, the most prominent of which was allocating a budget to provide cybersecurity requirements and its applications, and more attention to information protection and security programs because they have an impact on the digital trust of the beneficiary.

Keywords: Cyber security - Digital confidence - Saudi University.

المقدمة:

وضعت المملكة العربية السعودية رؤية المملكة (2030)، وتتطلع من خلالها إلى تحقيق معدلات تنموية كبيرة، ويتوقع منها مستقبل مشرق للمملكة، حيث اهتمت هذه الرؤية باستثمار الموارد المتاحة ضمن (13) برنامج تنفيذي؛ من أجل تحقيق (96) هدفاً تنموياً واستراتيجياً (دليل رؤية المملكة العربية السعودية، 2030).

وتعد البنية التحتية الرقمية من أبرز أهداف رؤية المملكة (2030)، والتي ترتكز على الاتصالات وتكنولوجيا المعلومات كقواعد رئيسة في تحفيز الصناعة والتجارة والخدمات، واستقطاب المستثمرين ودعم وتعزيز عمليات التحول الرقمي (الشهراني وفلمبان، 2020: 614).

وتتجه كافة المؤسسات بالمملكة العربية السعودية على اختلاف أنواعها نحو الاستفادة من عالم التقنيات والمعارف، حيث أصبحت أنظمة المعلومات أكثر الموضوعات تداولاً وانتشاراً بالمملكة. وكان لهذه الطفرة المعلوماتية التقنية أثر على اعتماد مختلف المؤسسات التعليمية والأكاديمية على الفضاء الإلكتروني، ولتحقيق الاستفادة الجيدة من هذه التقنيات والطفرة، فإنه يجب حماية الأنظمة والمعلومات والشبكات التي تعتمد عليها المؤسسات.

فمسايرة التغيرات لابد أن يتم وفق آليات وإجراءات تحمي الأنظمة والمعلومات، فالأمن في الفضاء السيبراني يعتبر أمراً مهماً بالنسبة للدول، والمؤسسات، والأفراد (العريشي والدوسري، 2018: 302). لذا بدأت كثير من الدول والمؤسسات خاصةً التعليمية منها بتبني وتطبيق أمن المعلومات وممارسة الأمن السيبراني وتوفير متطلباتها (الجندي ومحمد، 2019: 15).

والجامعة كمؤسسة تعليمية اليوم لا تقاس بالأرقام القياسية المتمثلة بأعداد الطلبة، أو أعداد أعضاء هيئة التدريس ورتبهم الأكاديمية، والمباني الفخمة فحسب، إنما تقاس بأعمالها العلمية، ونتائج ومخرجات العمل التعليمي، وهي بذلك أصبحت ذات رسالة علمية وإنسانية وحضارية وثقافية (بركات وحسن، 2009: 113). والجامعات لها وظائف متجددة حسب ما تقتضيه الحاجة، ومع التقدم تتقدم أهدافها، ووظائفها (يونس، 2015: 128)، ومن هذا المنطلق اكتسب التعليم الجامعي اهتماماً خاصاً، وتطلب جهوداً كبيرة للتغلب على مختلف التحديات الزمانية والمكانية والاقتصادية والاجتماعية التي قد تقف حائلاً أمام تحقيق أهدافها.

وعلى اعتبار أن الجامعة صانع وناقل المعرفة فإنها تعتمد على الشبكات والمعلومات بشكل متزايد، خاصةً في بيئة التعليم الإلكتروني التي فرضتها جائحة كورونا، وهذا الاندفاع المتزايد نحو توظيف الانترنت والأجهزة والشبكات في العمل الإداري والأكاديمي يجعل الجامعة عرضة للمخاطر الإلكترونية والجرائم الافتراضية. حيث أشار كل من (الدهشان والسيد، 2020) إلى أن حاجة الجامعات إلى التحول الرقمي أكثر من المؤسسات الأخرى؛ لأنها ترتبط بعالم المعرفة وإنتاجها، وأن الجامعات البوابة الرئيسية إلى رقمنة الحياة اليومية.

وأشارت كثير من الدراسات إلى أن هناك حراك كبير في العالم أجمع نحو أمن المعلومات والشبكات والأمن السيبراني، من خلال الانضمام لاتفاقيات محاربة جرائم الانترنت. كما تركز المؤسسات التعليمية على تحقيق أعلى استفادة من تكنولوجيا المعلومات والاتصالات مع حماية أنظمتها حفاظاً على سرية بياناتها وحماية الشبكات والأنظمة، وتتجه نحو تطويع سياساتها وتوعية وتثقيف العاملين بمتطلبات الأمن السيبراني (القحطاني، 2019؛ والجندي ومحمد، 2019؛ والموجي ومحمود وإمام، 2021).

ويعد الأمن السيبراني الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت، وتطبيقاته وأنظمته المختلفة، للتقليل من المخاطر التي تنشأ من سوء الاستخدام، حيث توجد محتويات غير مشروعة وغير مرغوب بها ذات تأثير سلبي على أخلاقيات وقيم المجتمع، وتؤدي إلى تغيرات في شخصية الأفراد، وتعزز ميلهم للانحراف (الصانع والسواط وأبو عيشة وسليمان وعسران، 2020: 49).

والأمن السيبراني من حيث المفهوم أوسع وأكثر شمولاً من أمن المعلومات، حيث يتضمن تأمين البيانات والمعلومات التي تتداول عبر المؤسسات الداخلية والخارجية، والتي يتم تخزينها في خوادم داخل وخارج الهيئات من الاختراق (الموجي ومحمود وإمام، 2021م، ص 21).

حيث عرف الاتحاد الدولي للاتصالات (2011: 17) الأمن السيبراني بأنه مجموعة من المهمات تتمثل في تجميع الوسائل والسياسات والإجراءات الأمنية والمبادئ التوجيهية والمقاربات لإدارة المخاطر والتدريبات وممارسات آمنة، وتقنيات يمكن استخدامها لحماية البيئة السبرانية وموجودات المؤسسات والمستخدمين.

ورأى جوتام أن الأمن السيبراني مجموعة من التقنيات والعمليات التي تم وضعها لحماية أجهزة الحاسوب والبرمجيات والشبكات والبيانات من الوصول غير المصرح به؛ لمجابهة مواطن الضعف التي تم توفيرها من خلال الانترنت من قبل مجرمي السيبرانية، والجماعات الإرهابية والمتسللين (Goutam & Verma, 2015: 24).

فالأمن السيبراني طريقة مثلى لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، وذلك بهدف الولوج للمعلومات المهمة ومحاولة اتلافها أو الابتزاز من خلالها للمستخدمين (الغامدي، 2018: 7).

كما عرفت القحطاني (2019: 91) الأمن السيبراني على أنه عمليات الحماية التي تقوم بها الدولة أو المؤسسات أو الأفراد؛ لحماية العمليات المرتبطة بتقنيات الاتصالات والمعلومات للحد من الخسائر والأضرار والجرائم المرتبطة بهذه التقنيات.

كما يعرف الأمن السيبراني على أنه مجموعة من التدخلات والتدابير التقنية المتخذة لحماية الأجهزة والشبكات والبيانات والمعلومات من الوصول غير المصرح به؛ بهدف المحافظة على السلامة ونزاهة المعلومات المخزنة بهذه الأجهزة (Richardson, Lemoine, Stephens, & Waller, 2020: 24).

وعُرف الأمن السيبراني بأنه حماية الأفراد وبياناتهم وحساباتهم من الهجمات الإلكترونية (الصانع والسواط وأبو عيشة وسليمان وعسران، 2020: 48).

يتضح من عرض التعريفات المرتبطة بالأمن السيبراني بأنها لا تقف على طريقة أو وسيلة من أجل حماية المعلومات والشبكات، بل تفتح الطريق لأي أسلوب أو إجراء من أجل تحقيق أمن المعلومات والشبكات؛ وقد يرجع ذلك إلى تطور المجرم السيبراني وإمكاناته التقنية.

ولقد تناولت كثير من الدراسات والبحوث أهمية الأمن السيبراني، حيث إن تصعيد الهجمات الاحتيالية يعد مشكلة كبيرة، والأمن السيبراني بمثابة آليات للتصدي لهذه الهجمات والحد من مخاطرها. وأشار الألفي (2010: 86) أن أهمية الأمن السيبراني يعود إلى الحاجة الضرورية إلى تطوير استراتيجية وطنية وحماية البنية التحتية للدولة ومؤسساتها للحفاظ على المعلومات الحساسة، إضافة إلى ردع الجريمة الإلكترونية، كما إن الأمن السيبراني له أبعاد تتعلق بالحماية الفكرية والممتلكات والأسرار والعلامات.

والأمن السيبراني يحافظ على المعلومات وتجانسها وسلامتها، ويكف العابثين عنها، وتجعل أكثر جهوزية عند الحاجة لها، وتحمل الأجهزة والشبكات من الاختراق، ويعد درعاً واقياً لما تحتويه، ويمكن من خلال الأمن السيبراني معرفة الثغرات في الأنظمة ومعالجتها، وتوفر بيئة آمنة للمستخدمين.

وتخلص الباحثة إلى أن قدر وحجم المعلومات التي تتضمنها الجامعات السعودية، وطبيعة تحولها الإلكتروني واعتمادها على الأنظمة التقنية يجعلها من أكثر دول العالم حاجة إلى بناء ثقافة لحماية المعلومات والأنظمة، حتى يتم الحفاظ على الأنظمة والشبكات وزيادة ثقة المستخدمين لهذه الشبكات والمعلومات، والتحقق من أن معلوماتهم وبياناتهم محمية ويمكن الرجوع إليها والاستفادة منها بالوقت المناسب.

وحول أهداف الأمن السيبراني أشارت كل من (السمحان، 2020: 12؛ المنتشري، 2020: 463) أن تطبيق الأمن السيبراني ونشر ثقافته وتوعية الأفراد والمؤسسات به، وجاء للأهداف التالية:

1. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
2. التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

3. توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات، وتوفير بنى تحتية لديها حساسية للهجمات الإلكترونية.
4. توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
5. التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
6. سد الثغرات في أنظمة أمن المعلومات.
7. مقاومة البرمجيات الخبيثة، بما تستهدفه من إحداث أضرار بالغة للمستخدمين.
8. حد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.
9. اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.
10. تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

والثقة الرقمية هي واحدة من عوامل نجاح الجامعات وقدرتها على تأدية رسالتها ورؤيتها، حيث أشارت كليمان (2018) أن الثقة الرقمية تعني أن تقوم المؤسسة على توفير المتطلبات العصرية والرقمية والاتصالية، وتضمن الاستخدام الآمن لها، وأن المستخدم يمكنه الاعتماد على البيانات والمعلومات، وأن ما يحصل عليه هو آمن وصادق.

وأشار كل من نذير ومعمر وريحان وعنكوش (2012: 77 – 82) أن الثقة الرقمية من متطلبات إرساء مجتمع المعرفة، وإدارة المعرفة، وأنها أصبحت جزء من الميزة التنافسية لكثير من المؤسسات خاصة الأكاديمية، وفي ظل بيئة تعلم إلكترونية فإن هناك حاجة لإرساء قواعد ومبادئ الثقة الرقمية، وأن يكون هناك نماذج وبرامج حماية تسهم في تعزيز ثقة المستخدم بالبرامج والتقنيات، وأن يدرك المستخدم أنه في مكان رقمي آمن.

وقد يصعب تحقيق الثقة الرقمية في عصر الجريمة السبرانية دون ارساء قواعد وأنماط من الثقافة السيبرانية التي تعزز قدرة المستخدم على حماية بياناته من التلف أو من الهجمات الرقمية. وترى الباحثة أنه كلما زادت المعلومات أهمية فإنها تتطلب جهوداً أكبر في حمايتها؛ لأنها تصبح أكثر عرضة للجرائم السيبرانية، وبشكل عام فإن أهمية ثقافة الأمن السيبراني تتمثل في أنها جدار حماية للأفراد والمؤسسات، وتسهم في الوصول الآمن للبيانات، والقدرة على استردادها والاستفادة منها بالوقت المناسب. وكلما ضعفت قدرات المجرم على الوصول لبيانات الجامعة فإن ذلك يعزز استعداد المستخدم لمواصلة ومتابعة بياناته بثقة وآمن.

مشكلة الدراسة وأسئلتها:

تتجه معظم الجامعات السعودية إلى الاعتماد على أنظمة تقنية ورقمية في سياساتها وبرامجها الإدارية والأكاديمية في إطار سعيها لمواكبة التطورات وتحقيق رؤية المملكة العربية السعودية (2030)؛ مما أسفر إلى تدفق وتبادل كم هائل من المعلومات والبيانات داخل هذه الجامعات، وفي ظل التطورات العالمية وتنامي الجرائم الإلكترونية فإن الثقة الرقمية بحاجة إلى إجراءات للحماية وجدر أمان، فالأمن السيبراني يتمثل بكافة الإجراءات التي يمكن أن تعزز ثقة المستخدم الرقمية، وتمنحه الراحة والطمأنينة على بياناته وتعامله مع البرمجيات والشبكات ومختلف الأنظمة الرقمية، وحول أهمية الثقافة السيبرانية أشار كل من ريتشاردسون وليموني وستيفينز وولاير (Richardson, Lemoine, Stephens, & Waller, 2020: 23) أن المجرم الإلكتروني يستغل الأفراد والمؤسسات التي لا تتمتع بثقافة الأمن السيبراني، وأشار كل من يان وإكسو ولو (Yan, Xue, & Lou, 2021) أن الاهتمام بالأمن السيبراني أصبح على نطاق واسع؛ لأن المخاطر السيبرانية والجرائم الإلكترونية أصبحت تصل لكل فئات المجتمع ومؤسساته، كما أشارت (فوزي، 2019) أن الجرائم السيبرانية تهدد الأمن والاستقرار والسلم الاجتماعي؛ وأنها بزيادة مستمرة، وأن لها أبعاد متعددة تجعلها من أبرز تهديدات تحقيق التنمية المستدامة، وأشار لوتو (Lehto, 2020) إلى أن الجامعات عليها تطبيق الأمن السيبراني لحماية البيانات والمعلومات والوثائق المهمة التي تخزن في أجهزتها، وأشار إلى أهمية تدريس الأمن السيبراني في

الجامعات لأهميته في حماية الأفراد والمؤسسات، كما أشار كل من ويجناتو وبراباو (Wijayanto, & Prabowo, 2020) أن مستخدمي الانترنت زاد خلال جائحة كورونا، وعدد ساعاتهم زاد بشكل كبير جداً، وأصبحت الحاجة إلى الوعي بالأمن السيبراني وتطبيقاتها وبرامجه أكثر في ظل الظروف التي تواجه العالم بأسره، ومن خلال خبرة الباحثة في العمل الأكاديمي ببعض الجامعات السعودية ترى من الأهمية توعية الطلبة وأعضاء هيئة التدريس بمتطلبات الأمن السيبراني، ونشرها كثقافة حتى يتسنى لكل فرد الحفاظ على بياناته وسريتها، وخصوصيتها، لأن المجرم السيبراني يقتحم الموقع ولا يفرق بين الطالب وعضو هيئة التدريس، وغالباً ما تكون دوافعه غير معروفة بشكل دقيق، إضافة إلى احترافية هذا النوع من المجرمين، كما يتميز المجرم السيبراني بالحنكة والذكاء والقدرات والمهارات الهائلة في مجال التقنيات وتكنولوجيا المعلومات، وبالتالي لا يمكن التصدي لهجماته عبر برامج فقط، بل هناك حاجة لثقافة متكاملة للأمن السيبراني. لذا تنحصر مشكلة الدراسة في السؤال الرئيس التالي: **ما أثر الأمن السيبراني في الجامعات السعودية في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس؟**

وينبثق عن السؤال الرئيس مجموعة الأسئلة الفرعية التالية:

1- ما واقع الأمن السيبراني في الجامعات السعودية من وجهة نظر أعضاء هيئة التدريس؟
2- ما مستوى الثقة الرقمية في الجامعات السعودية من وجهة نظر أعضاء هيئة التدريس؟
3- إلى أي مدى يؤثر الأمن السيبراني في تعزيز الثقة الرقمية بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس؟
4- هل توجد فروق بين استجابات المبحوثين حول الأمن السيبراني في الجامعات السعودية في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس تعزى لاختلاف متغيري سنوات الخدمة والدرجة العلمية والتفاعل بينهما؟

أهداف الدراسة:

تسعى الدراسة إلى تحقيق ما يلي:

1- التعرف إلى واقع الأمن السيبراني في الجامعات السعودية من وجهة نظر أعضاء هيئة التدريس.
2- الكشف عن مستوى الثقة الرقمية في الجامعات السعودية من وجهة نظر أعضاء هيئة التدريس.
3- التحقق من وجود أثر للأمن السيبراني في تعزيز الثقة الرقمية بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس.
4- اختبار الفروق بين استجابات المبحوثين حول الأمن السيبراني في الجامعات السعودية في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس تبعاً لاختلاف متغيري سنوات الخدمة والدرجة العلمية والتفاعل بينهما.

أهمية الدراسة:

تتضح أهمية الدراسة في التالي:

1- الأهمية النظرية:

أ- تعد الدراسات من المحاولات القليلة التي تبحث في ثقافة الأمن السيبراني في البيئة السعودية، كما إنها تربط بين الأمن السيبراني والثقة الرقمية.
ب- تبين الدراسة الإطار الفلسفي للأمن السيبراني والحاجة إليه، وتطبيقاته في الجامعات السعودية.
ت- تقدم الدراسة إطار يثري المكتبة السعودية بموضوعات تزداد أهميتها في ظل التطورات وظهور التقنيات المختلفة، والمخاوف الإلكترونية لدى كثير من الفئات.

2- الأهمية التطبيقية:

أ- تفيد نتائج الدراسة صناع القرار في الجامعات السعودية، حيث تقدم لهم بعض المعلومات والآراء المرتبطة بالأمن السيبراني، وطرق تحقيقه في الجامعات.

ب- تفيد نتائج الدراسة الحالية القائمين على أنظمة وبرمجيات الجامعات السعودية، والعاملين في مجال صناعة وتطوير البرامج حيث توضح لهم سبل حماية هذه الشبكات والبرمجيات وأثر ذلك في رفع مستوى الثقة الرقمية للمستخدمين.

ت- كما تقدم الدراسة نتائج وتوصيات تثري معارف المستخدمين من إداريين وأكاديميين وطلبة حول الأمن السيبراني والثقافة الرقمية وطرق حماية البيانات.

ث- قد تفيد نتائج الدراسة الحالية الباحثين والمختصين؛ حيث تفتح لهم آفاقاً لدراسات مستقبلية تتعلق بالأمن السيبراني والثقة الرقمية وتطبيقاتها في الجامعات.

حدود الدراسة:

تتحدد الدراسة في إطار التالي:

1- **الحدود الموضوعية:** اقتصرت الدراسة على معرفة واقع ثقافة الأمن السيبراني في الجامعات السعودية وأثرها على الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس.

2- **الحدود المكانية:** أجريت الدراسة على جامعة بيشة بمنطقة عسير جنوب المملكة العربية السعودية.

3- **الحدود الزمنية:** طُبقت الدراسة خلال العام (1442هـ/ 2021م).

4- **الحدود البشرية:** أجريت الدراسة من خلال استطلاع آراء عينة من أعضاء هيئة التدريس بجامعة بيشة.

مصطلحات الدراسة الإجرائية

الأمن السيبراني إجرائياً:-

تُعرف الباحثة الأمن السيبراني بأنه الإجراءات والبرامج والتطبيقات التي توفرها الجامعات السعودية لحماية أنظمتها وشبكاتها والمعلومات والبيانات المتوفرة لديها من الجرائم الإلكترونية بشتى أنواعها، ومنع الوصول غير المصرح به لهذه الشبكات والأنظمة.

الثقة الرقمية:-

تُعرف الباحثة الثقة الرقمية بأنها استخدام البيانات والمعلومات والأنظمة والشبكات في إطار من الطمأنينة محفوظة ومحمية من هجمات المجرمين الرقميين، وأنه يمكن استرداد البيانات والمعلومات اللازمة بالوقت المناسب.

الدراسات السابقة:

أجرى كل من يولفين ووانجين (Ulven, & Wangen, 2021) دراسة بهدف مراجعة الأدبيات ذات العلاقة بمخاطر الأمن السيبراني في مؤسسات التعليم العالي، واستخدمت الدراسة الأسلوب المكتبي، حيث تبين أن الأبحاث التجريبية في مجال مخاطر الأمن السيبراني نادرة، وتبين وجود فجوة كبيرة في نتائج الدراسات والبحوث التي تمت مراجعتها على فترة زمنية تجاوزت (12 عام)، لكن تبين وجود اتفاق كبير حول متطلبات ومصادر الأمن السيبراني، وأهمية الأمن السيبراني في حماية وأمن المعلومات، كما تبين أن هناك تسع مخاطر إلكترونية حقيقية بحاجة إلى أمن سيبراني.

كما أجرت **السمحان (2020)** دراسة بهدف معرفة متطلبات الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، حيث تم الاعتماد على المنهج الوصفي، واستخدمت الاستبانة في جمع البيانات، حيث طبقت على عينة بلغت (478)، وقد توصلت الدراسة إلى وجود سياسات أمنية لأنظمة المعلومات الإدارية بالجامعة، وأن هناك تطبيق لإجراءات إدارية من أجل حماية الأنظمة، وتوجد خطط لإدارة المخاطر الإلكترونية، وتقوم الجامعة بتحديث برامج الحماية، كما تطبق متطلبات الأمن السيبراني في تعريف هوية الدخول والصلاحيات، وتوجد بالجامعة أنظمة حماية تقنية وحاسوبية، وتقوم الجامعة بتقديم الدعم الفني اللازم لتطبيق الأمن السيبراني وتقوم بتوعية الموظفين بمتطلبات الأمن السيبراني وتطبيقاته، وتمتلك الجامعة نظام حماية عالي المستوى، ويتوفر الأجهزة التقنية اللازمة لتوفير الحماية.

كما أجرت **المنتشري (2020)** دراسة بهدف توضيح دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، واستخدمت الدراسة المنهج الوصفي التحليلي، وتم اعداد استبانة طبقت على عينة بلغت (420) معلمة، وأظهرت نتائج الدراسة أن دور القيادة المدرسية في تعزيز الأمن السيبراني يتحقق بدرجة موافقة قليلة، وفي ضوء هذه النتيجة تم الوصول إلى تصور مقترح لتطوير دور القيادة المدرسية في تعزيز الأمن السيبراني.

كما حاول كل من ويجناتو وبراباو (Wijayanto, & Prabowo, 2020) قياس سلوك ضعف الأمن السيبراني خلال جائحة كورونا، ولتحقيق الأهداف تم استخدام المنهج الوصفي، وتم استخدام مقياس سلوك الأمن السيبراني للمخاطر، وطبق على إداريين ومدراء يعملون في جامعات وكليات بمنطقة جافا الوسطى في إندونيسيا، وتوصلت الدراسة إلى أن المقياس الذي يتضمن (33) فقرة يتمتع بصدق وثبات مناسب، وأن التنشئة الاجتماعية السوية هي سبيل لتحقيق الأمن السيبراني، وأن هناك حاجة ملحة للأمن السيبراني في ظل متطلبات التحول الرقمي بمختلف المؤسسات التعليمية.

وهدفت دراسة ريدمان وياكسلي وجونيور (Redman, Yaxley, & Joiner, 2020) إلى تحسين التعليم العام للأمن السيبراني، ولتحقيق ذلك تم إعداد مقرر يدرس بالمختبرات العلمية وتم تطبيقه على طلبة البكالوريوس في جامعة نيو ساوث ويلز وكان عنوان المقرر "مقدمة في الأمن السيبراني"، وشملت عينة التجربة (160) طالباً وطالبة، وتم استطلاع آرائهم فتبين وجود قبول واستعداد لدراسة الأمن السيبراني كمقرر ضمن مقررات الجامعة، واختبروا الطلبة فتبين وجود قدرات ومهارات سيبرانية مختلفة اكتسبوها من خلال المقرر، كما تضمنت النتائج بعض جوانب القصور التي تم التوصية بتطويرها وتحسينها في المقرر ليكون جاهزاً للتنفيذ عام (2020).

هدفت دراسة **القحطاني (2019)** إلى تعرف مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية: (جامعة الأمير نايف، وجامعة الأميرة نورة، وجامعة الإمام محمد بن سعود، وجامعة الجوف، وجامعة الملك خالد، وجماعة الملك سعود، وجامعة الملك عبدالعزيز، وجامعة الملك فيصل، وجامعة شقراء)، وتم استخدام منهج المسح الاجتماعي بالعينة، واعتمدت الدراسة على الاستبانة في جمع البيانات، حيث أجريت على (486) طالباً وطالبة، وجاءت أهم النتائج أن أقرب مفهوم للأمن السيبراني من وجهة نظر العينة هو استخدام مجموعة الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، وجاءت أبرز الجرائم الإلكترونية التي يعيها الطلبة الاحتيال الإلكتروني، كما تبين وجود معوقات اجتماعية في تحقيق الوقاية من مشكلات الفضاء السيبراني.

وهدفت دراسة كل من **الجندي ومحمد (2019)** إلى التحقق من دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة، وتم الاعتماد على المنهج التكنولوجي التطويري المنظومي، وتم توظيف المنهج الوصفي وشبه التجريبي، وطبقت الدراسة على (80) طالبة من طالبات قسم الحاسب الآلي بالكلية الجامعية – جامعة أم القرى، وتم تقسيمهن إلى مجموعتين الأولى ضابطة والثانية تجريبية، وأشارت النتائج إلى تفوق طالبات المجموعة التجريبية على طالبات المجموعة الضابطة في المهارات ودقة التطبيق العملي للأمن المعلوماتي، مما يشير إلى وجود دور مهم للممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلومات لدى طالبات الجامعة.

بينما هدفت دراسة **الصبان والحربي (2019)** إلى معرفة علاقة إدمان الطلاب على استخدام مواقع التواصل الاجتماعي والأمن النفسي والتورط في جرائم سيبرانية، وتم استخدام المنهج الارتباطي، وتكونت عينة الدراسة من (252) طالب بجامعة طيبة بالمدينة المنورة، واستخدمت الدراسة مقياس الأمن النفسي والتعرض للتورط بجرائم سيبرانية عبر مواقع التواصل الاجتماعي، ومقياس لاستخدام مواقع التواصل الاجتماعي، فتبين وجود علاقة سالبة بين إدمان الطلاب على استخدام مواقع التواصل الاجتماعي والأمن النفسي، وتبين وجود علاقة موجبة بين استخدام مواقع التواصل الاجتماعي والتورط في الجرائم السيبرانية.

التعقيب على الدراسات السابقة

يتضح من عرض الدراسات السابقة أن تطبيقات الأمن السيبراني ومتطلباته حظيت على اهتمام الباحثين والمختصين، ومن خلال عرض هذه الدراسات يتضح أن الأمن السيبراني يعزز حماية وأمن المعلومات؛ وأن تطبيقه بحاجة إلى متطلبات منها مادية وتقنية وبشرية مثل ما جاء في دراسة (السمحان، 2020)، كما أشارت بعض الدراسات إلى موضوع وعي الطلاب بالأمن السيبراني لبعده الاجتماعي وحماية المجتمع من الانحراف (القحطاني، 2019).

كما تبين الدراسات السابقة أن من يحصل على تدريب في تطبيق الحماية من خلال الأمن السيبراني بطرق عملية أفضل من التدريب بطرق نظرية حسب ما جاء في دراسة (الجندي ومحمد، 2019)، كذلك تناولت دراسة (المنتشري، 2020) دور القيادة المدرسية في تعزيز الأمن السيبراني لدى الطالبات والمعلمات؛ وهذا مؤشر على أن نشر ثقافة الأمن السيبراني يجب أن يتم من مراحل العمر الأولى. وأشارت دراسة (Redman, Yaxley, & Joiner, 2020) إلى أهمية إدراج مقرر للأمن السيبراني لطلبة البكالوريوس. وتناولت دراسة (Ulven, & Wangen, 2021) مراجعة لبحوث الأمن السيبراني ومخاطره وتبين وجود قصور في الدراسات التجريبية بينما تبين أن معظم الدراسات أشارت إلى أهمية الأمن السيبراني في أمن وحماية المعلومات.

ولقد اعتمدت الدراسات السابقة على عدة مناهج لتحقيق أهدافها، حيث إن معظمها استخدم النهج الوصفي التحليلي كما في دراسة (السمحان، 2020؛ والمنتشري، 2020)، بينما استخدمت بعض الدراسات منهج المسح الاجتماعي مثل دراسة (القحطاني، 2019)، واعتمدت دراسة (الجندي ومحمد، 2019) على المنهج الوصفي وشبه التجريبي.

ولقد استفادت الدراسة الحالية من الدراسات السابقة في عدة جوانب أبرزها صياغة استبانة الدراسة، كما استعانت ببعض الدراسات في وصف مشكلة الدراسة، وإثراء الخلفية النظرية، كذلك تضمنت الاستفادة تحليل واقع الأمن السيبراني في المجتمع السعودي وتفسير نتائج الدراسة الحالية بناءً على ذلك.

منهج الدراسة:

اعتمدت الدراسة الحالية على المنهج الوصفي التحليلي؛ لأنه يتناسب مع خصائص الدراسة وأهدافها، حيث يعد المنهج الوصفي مظلة واسعة للبحوث والدراسات الإنسانية، يتم من خلالها تناول موضوع الدراسة بالوصف والتفسير الدقيق، ومن ثم يتم جمع البيانات والمعلومات والتفاعل معها بغرض الوصول إلى نتائج، وتعميمات وعلاقات جديدة تثري المعرفة وتعالج مشكلة الدراسة.

مجتمع الدراسة:

تكون مجتمع الدراسة من جميع أعضاء هيئة التدريس بجامعة بيشة، والبالغ عددهم نحو 980 عضو هيئة تدريس.

عينة الدراسة:

اختارت الباحثة عينة عشوائية بسيطة بلغت (220) عضو هيئة التدريس، أرسلت إليهم أداة الدراسة إلكترونياً عبر البريد الإلكتروني أو مواقع التواصل الاجتماعي؛ فاستجاب منهم (184) عضو بنسبة استجابة بلغت (83.6%)، وتم حذف استبانتين لعدم استيفاء الشروط، وبالتالي كانت عينة الدراسة تساوي (182) عضو، بنسبة (18.8%) من المجتمع الأصلي للدراسة، وجاءت خصائصهم الشخصية كما يوضحها جدول (1) على النحو التالي:

جدول (1) توزيع عينة الدراسة حسب متغيري سنوات الخدمة والدرجة العلمية

البيان		العدد	النسبة المئوية
سنوات الخدمة	7 سنوات فأقل	51	28.02
	من 7 إلى أقل من 15 سنة	106	58.24
	15 سنة فأكثر	25	13.74
المجموع		**182**	**100.0**
الدرجة العلمية	محاضر	15	8.24

	أستاذ مساعد	110	60.44
	أستاذ مشارك	41	22.52
	أستاذ دكتور	16	8.80
المجموع		**182**	**100.0**

أداة الدراسة:

اعتمدت الدراسة على الاستبانة كأداة رئيسة في جمع البيانات حول الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية، حيث تم صياغة الاستبانة في ضوء بعض الأدبيات السابقة خاصةً (المنتشري وحريري، 2020؛ والمنتشري، 2020؛ والقحطاني، 2019)، وكانت الاستبانة عبارة عن:

- محور للبيانات الشخصية، ويتضمن متغيري سنوات الخدمة والدرجة العلمية.
- محور للأمن السيبراني في الجامعات، ويتضمن (16) فقرة.
- محور للثقة الرقمية، ويتضمن (15) فقرة.

ولقد تحققت الباحثة من صدق وثبات الأداة من خلال مجموعة من الإجراءات والخطوات وأبرزها تطبيق الاستبانة بصورتها الأولية على عينة استطلاعية بلغت (30) عضو هيئة تدريس، وكانت خطوات وإجراءات الصدق والثبات على النحو التالي:

صدق الأداة:

يقصد بالصدق أن تقيس الأداة الموضوع الذي تتناولها، وأن تكون الفقرات قادرة على قياس ما وضعت لأجل قياسه، وتم التحقق من صدق الأداة من خلال عرضها على لجنة من أعضاء هيئة التدريس وبعض المختصين، وتقنينها وتعديلها حسب آراء لجنة التحكيم، كما قامت الباحثة بتحليل بيانات العينة الاستطلاعية، ومن ثم حساب معاملات الارتباط بين درجة كل فقرة من فقرات الاستبانة مع الدرجة الكلية للمحور، وفيما يلي توضيح لنتائج صدق الاتساق الداخلي للفقرات:

جدول (2): يوضح نتائج الاتساق الداخلي لفقرات الأمن السيبراني

م.	فقرات الأمن السيبراني	معامل الارتباط	قيمة الاحتمال
.1	تؤمن إدارة الجامعة أن الأمن السيبراني أساس حماية أنظمتها.	**0.847**	**0.000**
.2	يوجد بالجامعة قسم خاص بأمن المعلومات.	**0.702**	**0.000**
.3	تقوم الجامعة بصيانة أنظمتها بشكل مستمر.	**0.770**	**0.000**
.4	توفر برامج الجامعة السرية اللازمة على حسابات المستخدمين.	**0.775**	**0.000**
.5	تعتمد الجامعة على تطبيقات لحماية البيانات الشخصية.	**0.662**	**0.000**
.6	تقاوم برامج الجامعة وأجهزتها البرمجيات الخبيثة.	**0.718**	**0.000**
.7	تعالج الجامعة نقاط الضعف في أجهزتها من خلال سد الثغرات.	**0.841**	**0.000**
.8	تضع الجامعة جدر حماية لمنع حالات الولوج غير المسموح بها.	**0.718**	**0.000**
.9	تحمي الجامعة أنظمتها التشغيلية من خلال برامج متطورة.	**0.575**	**0.001**
.10	تبني الجامعة سياساتها السيبرانية للحد من حالات التجسس والتخريب الرقمي.	**0.734**	**0.000**
.11	توجد آليات تخزين آمنة للوثائق التعليمية والفكرية.	**0.783**	**0.000**
.12	توجه الجامعة المستفيدين من أنظمتها نحو طرق حماية وأمن المعلومات.	**0.849**	**0.000**
.13	تشارك الجامعة في اتفاقيات وندوات الأمن السيبراني.	**0.701**	**0.000**
.14	تنشر الجامعة تعليمات للمستفيدين من أنظمتها لمواجهة الجريمة الإلكترونية.	**0.724**	**0.000**

.15	تقوم الجامعة بمراجعة البيانات والمعلومات المتوفرة على شبكاتها من أجل إصلاحها حال تعرضها للجرائم السيبرانية.	**0.724**	**0.000**
.16	تحذف الجامعة البيانات التالفة التي تعرضت لهجمات سيبرانية.	**0.814**	**0.000**

** ر **الجدولية دالة عند مستوى دلالة** (0.01) * ر **الجدولية دالة عند مستوى دلالة** (0.05)

يبين جدول (2) أن جميع قيم الاحتمال جاءت أقل من مستوى الدلالة (0.05)، وبالتالي فإن معاملات الارتباط دالة إحصائياً، وأن فقرات محور الأمن السيبراني صادقة لما وضعت لأجل قياسه.

جدول (3): يوضح نتائج الاتساق الداخلي لفقرات الثقة الرقمية

م.	فقرات الثقة الرقمية	معامل الارتباط	قيمة الاحتمال
.1	يجد مستخدم البيانات حفاظاً على سرية وخصوصية بياناته.	**0.873**	**0.000**
.2	يعتمد المستخدم على كلمات مرور ورموز سرية من أجل الوصول إلى الشبكة.	**0.578**	**0.001**
.3	يثق المستخدم أن بإمكانه استعادة بياناته بالوقت المناسب.	**0.741**	**0.000**
.4	يؤمن المستخدم بأن الأمن السيبراني كاف لمنحه الأمان في استخدام شبكات الجامعة وبرامجها.	**0.751**	**0.000**
.5	يمنح النظام المتوفر الاستجابة لأي رسالة مجهولة.	**0.514**	**0.003**
.6	يحد النظام المتوفر من وصول الآخرين لمعلومات شخصية للمستخدمين.	**0.883**	**0.000**
.7	يطالب النظام من المستخدمين تغيير كلمات المرور بشكل دوري.	**0.653**	**0.000**
.8	تحمي برامج أمن المعلومات بيانات المستخدمين من التلف.	**0.733**	**0.000**
.9	تحد برامج أمن المعلومات من وصول الفيروسات إلى أجهزة الجامعة.	**0.684**	**0.000**
.10	تعزز برامج أمن وحماية المعلومات ثقة المستخدمين بالنظام.	**0.848**	**0.000**
.11	تعتمد الجامعة على خبراء متخصصين من أجل تطبيق الأمن السيبراني مما يعزز ثقة المستخدمين.	**0.735**	**0.000**
.12	تقدم الجامعة تقارير واضحة وموضوعية حول المخاطر السيبرانية.	**0.635**	**0.000**
.13	تستمع الجامعة لكافة الآراء والأفكار المطروحة حول تعزيز الثقة الرقمية.	**0.539**	**0.000**
.14	تعتمد الجامعة على سياسات وأنظمة مرنة يمكن تغييرها لتعزيز الثقة الرقمية.	**0.617**	**0.000**
.15	تصمم الجامعة سياسات وخطط لتعزيز ثقة المستخدم بأنظمة الجامعة وبرامجها.	**0.598**	**0.000**

** ر **الجدولية دالة عند مستوى دلالة** (0.01) * ر **الجدولية دالة عند مستوى دلالة** (0.05)

يبين جدول (3) أن جميع قيم الاحتمال جاءت أقل من مستوى الدلالة (0.05)، وبالتالي فإن معاملات الارتباط دالة إحصائياً، وأن فقرات الثقة الرقمية صادقة لما وضعت لأجل قياسه.

ثبات الأداة

يدلل ثبات الأداة على استقرار نتائجها، وأنها ستعطي نفس النتائج لو طبقت عدة مرات، وتم التحقق من صدق الأداة من خلال الطرق التالية:

1 – الثبات بطريقة كرونباخ ألفا: تم حساب معاملات كرونباخ ألفا لجميع فقرات المحور الأول والثاني، والجدول (4) يبين النتائج:

جدول (4) معاملات ألفا كرونباخ لمحاور الاستبانة

م.	المحاور	عدد الفقرات	ألفا كرونباخ
1	الأمن السيبراني في الجامعات السعودية	**16**	**0.908**
2	الثقة الرقمية	**15**	**0.894**

يبين جدول (4) أن معامل كرونباخ ألفا لجميع فقرات محور الأمن السيبراني (0.908)، ولفقرات محور الثقة الرقمية (0.894)، وهي مؤشرات على ثبات الاستبانة.

2 – الثبات بطريقة التجزئة النصفية:

هي طريقة لا يتم من خلالها إعادة التطبيق، وتتم من خلال تقسيم أبعاد استبانة الفاعلية الذاتية للعاملين والدرجة الكلية إلى فقرات فردية وأخرى فقرات زوجية رتب، ومن ثم إيجاد العلاقة بينهما، وذلك من أجل تصحيح هذه العلاقة من خلال معادلة سبيرمان براون (Spearman– Brown Coefficient) وذلك حسب المعادلة: $\frac{2R}{R+1}$ في حال تساوي طرفي الارتباط، أو معادلة جتمان في حال عدم تساوي طرفي الارتباط وذلك حسب المعادلة: $2\left(1-\frac{ع_1^2+ع_2^2}{ع^2}\right)$، وكانت النتائج كما في الجدول (5) التالي:

جدول (5) ثبات مقياس دافعية الإنجاز بطريقة التجزئة النصفية

البيان	المحور الأول	المحور الثاني
عدد الفقرات	**16**	**15**
معامل ارتباط الفقرات فردية الرتب مع الدرجة الكلية	**0.889**	**0.755**
معامل ارتباط الفقرات زوجية الرتب مع الدرجة الكلية	**0.870**	**0.832**
معامل الارتباط بين الفقرات فردية الرتب والزوجية	**0.741**	**0.617**
معامل الارتباط المصحح بطريقة سبيرمان بروان	**0.851**	**0.763**
معامل الارتباط المصحح بعد تعديل الطول باستخدام جتمان	**0.849**	**0.757**

يبين جدول (5) أن معامل الارتباط بين الفقرات فردية الرتب والفقرات زوجية الرتب للمحور الأول بلغ (0.741)، وبعد تصحيحه باستخدام سبيرمان بلغ (0.851)، وللمحور الثاني بلغ (0.617)، وبعد تصحيحه باستخدام معادلة جتمان بلغ (0.757)، وهي مؤشرات على ثبات الاستبانة.

تصحيح الاستبانة:

تكونت استبانة الدراسة من (31) فقرة تنقسم إلى محورين؛ الأول لقياس الأمن السيبراني في الجامعات السعودية (16) فقرة، والثاني للثقة الرقمية (15) فقرة، وأعطيت كل فقرة من فقرات الاستبانة سلم استجابة خماسي الترتيب بدرجات موافقة (مرتفعة جداً، مرتفعة، متوسطة، منخفضة، منخفضة جداً)، وتم تصحيح البيانات وترميزها باستخدام المفتاح التالي (5، 4، 3، 2، 1).

الأسلوب والمعالجات الإحصائية:

اعتمدت الدراسة على برنامج رزمة التحليل الإحصائي للعلوم الاجتماعية (Statistical Sciences For Social studies)؛ وتحديداً الاصدار (SPSS IBM– Version 22.0)، حيث تم الاعتماد على مجموعة من الأساليب والمعالجات الاحصائية في تحليل البيانات، واختبار فرضيات الدراسة، وأهمها التكرارات والنسب المئوية والمتوسطات الحسابية والانحرافات المعيارية، كما استخدمت معاملات كرونباخ ألفا، وطريقة التجزئة النصفية، ومعاملات الارتباط، واختبار تحليل الانحدار الخطي البسيط، إضافة إلى اختبار تحليل التباين الأحادي للفروق بين ثلاث مجموعات فأكثر، واختبار تحليل التباين الثنائي لدراسة الفروق تبعاً لتفاعل متغيرين.

اختبار التوزيع الطبيعي للبيانات:

استخدمت الباحثة اختبار اختبار كولمجروف – سمرنوف (1-Sample Kolmogorov-Smirnov) بهدف الكشف عن طبيعة البيانات، والاختبارات الواجب استخدامها، وكانت النتائج كما هو مبين بالجدول (6):

جدول (6) اختبار التوزيع الطبيعي لمتغيرات استبانة الدراسة

م.	الاستبيان	عدد الفقرات	قيمة الاختبار	قيمة (Sig.)
1	محور الأمن السيبراني	**16**	0.966	0.334
2	محور الثقة الرقمية	**15**	0.432	0.666

يوضح الجدول رقم (6) أن جميع قيم (Sig.) الاحتمالية كانت أكبر من مستوى الدلالة 0.05، ($sig. > 0.05$)، وعلية يمكن القول بأن محاور استبانة الدراسة تتبع توزيعاً طبيعياً، وعليه يجب استخدام الاختبارات المعلمية في هذه الدراسة.

النتائج المتعلقة بالسؤال الأول ومناقشتها

للإجابة عن السؤال الأول والذي ينص على "**ما واقع الأمن السيبراني في الجامعات السعودية من وجهة نظر أعضاء هيئة التدريس؟**". تم استخدام الاختبارات الوصفية المناسبة مثل المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية والرتب لفقرات محور الأمن السيبراني ودرجته الكلية:

جدول (7) المتوسط الحسابي والانحراف المعياري والوزن النسبي لفقرات محور الأمن السيبراني

م.	الفقرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الرتبة
.1	تؤمن إدارة الجامعة أن الأمن السيبراني أساس حماية أنظمتها.	3.473	1.070	69.46	15
.2	يوجد بالجامعة قسم خاص بأمن المعلومات.	3.440	0.966	68.80	16
.3	تقوم الجامعة بصيانة أنظمتها بشكل مستمر.	3.626	0.988	72.52	11
.4	توفر برامج الجامعة السرية اللازمة على حسابات المستخدمين.	3.819	0.901	76.38	3
.5	تعتمد الجامعة على تطبيقات لحماية البيانات الشخصية.	3.630	1.042	72.60	10
.6	تقاوم برامج الجامعة وأجهزتها البرمجيات الخبيثة.	3.599	1.035	71.98	12
.7	تعالج الجامعة نقاط الضعف في أجهزتها من خلال سد الثغرات.	3.670	1.025	73.40	8
.8	تضع الجامعة جدر حماية لمنع حالات الولوج غير المسموح بها.	3.742	0.999	74.84	5
.9	تحمي الجامعة أنظمتها التشغيلية من خلال برامج متطورة.	3.687	1.033	73.74	7
.10	تبني الجامعة سياساتها السيبرانية للحد من حالات التجسس والتخريب الرقمي.	3.758	0.984	75.16	4
.11	توجد آليات تخزين آمنة للوثائق التعليمية والفكرية.	3.489	1.071	69.78	14
.12	توجه الجامعة المستفيدين من أنظمتها نحو طرق حماية وأمن المعلومات.	3.582	1.083	71.64	13
.13	تشارك الجامعة في اتفاقيات وندوات الأمن السيبراني.	3.736	0.995	74.72	6
.14	تنشر الجامعة تعليمات للمستفيدين من أنظمتها لمواجهة الجريمة الإلكترونية.	3.654	0.926	73.08	9
.15	تقوم الجامعة بمراجعة البيانات والمعلومات المتوفرة على شبكاتها من أجل إصلاحها حال تعرضها للجرائم السيبرانية.	3.830	0.916	76.60	1
.16	تحذف الجامعة البيانات التالفة التي تعرضت لهجمات سيبرانية.	3.820	0.937	76.40	2
	الأمن السيبراني بالجامعات السعودية	3.659	0.709	73.18	

يبين جدول (7) أن واقع الأمن السيبراني في الجامعات السعودية جاء مرتفعاً، حيث بلغ الوزن النسبي لكافة فقرات المحور الأول (73.18%)، كما يتضح من أعلى الفقرات كانت:

- حصلت الفقرة رقم (15) على المرتبة الأولى والتي تنص على (تقوم الجامعة بمراجعة البيانات والمعلومات المتوفرة على شبكاتها من أجل إصلاحها حال تعرضها للجرائم السيبرانية)، بوزن نسبي (76.60%). ويمكن تفسير ذلك من خلال أهمية البيانات والمعلومات المتوفرة على شبكات الجامعة، وضرورة إصلاحها للاستفادة منها.
- حصلت الفقرة رقم (16) على المرتبة الثانية والتي تنص على (تحذف الجامعة البيانات التالفة التي تعرضت لهجمات سيبرانية)، بوزن نسبي (76.40%). وترى الباحثة أن البيانات التالفة تشكل عبء على الجامعة لأنها تأخذ حيز في برامج وتطبيقات التخزين، ولعدم القدرة على الاستفادة منها لاحقاً، إضافة إلى أن البيانات التالفة قد تشمل محتوى سلبي، أو محتوى يمكنه إتلاف مزيد من البيانات والمعلومات.
- حصلت الفقرة رقم (4) على المرتبة الثالثة والتي تنص على (توفر برامج الجامعة السرية اللازمة على حسابات المستخدمين)، بوزن نسبي (76.38%). وهذا ينبثق عن طبيعة العمل بالمؤسسات الأكاديمية حسابات المستخدمين من أعضاء هيئة تدريس وباحثين وخبراء وطلبة وإداريين لها خصوصية وبيانات مهمة جداً، لذا تسعى الجامعات لحمايتها من الدخول غير المصرح به، أو مداهمتها بالفيروسات.

وكانت أدنى الفقرات ما يلي:

- حصلت الفقرة رقم (1) على المرتبة ما قبل الأخيرة والتي تنص على (تؤمن إدارة الجامعة أن الأمن السيبراني أساس حماية أنظمتها)، بوزن نسبي (69.46%). ورغم أنها بمرتبة متأخرة إلا أنها جاءت بوزن نسبي مرتفع إلى حد ما، وهذا يرجع إلى حداثة الأمن السيبراني وتنوع برامجه وأساليبه.
- حصلت الفقرة رقم (2) على المرتبة الأخيرة وتنص على (يوجد بالجامعة قسم خاص بأمن المعلومات)، بوزن نسبي (68.80%). ومن خلال احتكاك الباحثة بعدد من الجامعات السعودية فإن معظم الجامعات تضع مهام أمن المعلومات على قسم يتعلق بتكنولوجيا الاتصالات والمعلومات وأنظمة المعلومات، ولا يتم تخصيص قسم لأمن المعلومات ذاتها.

بشكل عام يتضح أن هناك اهتمام بالأمن السيبراني من إدارة الجامعات السعودية، ويمكن تفسير ذلك في ضوء التقنيات والتطورات التي طرأت على تكنولوجيا الاتصالات والمعلومات، والحاجة إلى حماية الأنظمة والشبكات والبيانات من التلف ومن الجرائم الإلكترونية.

كذلك يمكن تفسير ذلك في ضوء الاتفاقات التي أبرت في المملكة العربية السعودية والتي تدعم كافة الأطراف بما فيها الجامعات إلى تبني متطلبات الأمن السيبراني والإيمان بأهميتها في حماية المستفيدين والأنظمة المتوفرة.

كذلك جاءت هذه النتائج في ضوء تنامي الاعتماد على تكنولوجيا الاتصالات والمعلومات في الجامعات السعودية، والتحول الرقمي لكافة الأقسام الإدارية والأكاديمية.

وتأتي هذه النتائج في سياق مواجهة الجرائم السيبرانية؛ خاصةً أن القائمين على الجرائم السيبرانية محترفين ولديهم خبرات وقدرات تقنية هائلة حسب ما أشار إليه (مانيطه، 2017)، ويصعب مواجهتهم إلا من خلال سياسات وآليات وبرامج وجدر حماية قوية وفعالة، وصيانتها بشكل دوري لأجل الحفاظ عليها. كما تتفق النتائج المتعلقة بالسؤال الأول مع بعض الدراسات السابقة مثل (Wijayanto, & Prabowo, 2020)، وتتفق أيضاً مع نتائج دراسة (Ulven, & Wangen, 2021).

النتائج المتعلقة بالسؤال الثاني ومناقشتها

للإجابة عن السؤال الثاني الذي ينص على: "**ما مستوى الثقة الرقمية في الجامعات السعودية من وجهة نظر أعضاء هيئة التدريس؟**". تم استخدام المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية والرتب لفقرات محور الثقة الرقمية ودرجته الكلية، وفيما يلي توضيح للنتائج:

جدول (8) المتوسط الحسابي والانحراف المعياري والوزن النسبي لفقرات محور الثقة الرقمية

م.	الفقرات	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	الرتبة
.1	يجد مستخدم البيانات حفاظاً على سرية وخصوصية بياناته.	4.044	0.909	80.88	1
.2	يعتمد المستخدم على كلمات مرور ورموز سرية من أجل الوصول إلى الشبكة.	3.780	1.175	75.60	5
.3	يثق المستخدم أن بإمكانه استعادة بياناته بالوقت المناسب.	3.696	1.049	73.92	9
.4	يؤمن المستخدم بأن الأمن السيبراني كاف لمنحه الأمان في استخدام شبكات الجامعة وبرامجها.	3.852	1.069	77.04	2
.5	يمنح النظام المتوفر الاستجابة لأي رسالة مجهولة.	3.774	0.954	75.48	6
.6	يحد النظام المتوفر من وصول الآخرين لمعلومات شخصية للمستخدمين.	3.560	1.038	71.20	15
.7	يطالب النظام من المستخدمين تغيير كلمات المرور بشكل دوري.	3.613	1.051	72.26	13
.8	تحمي برامج أمن المعلومات بيانات المستخدمين من التلف.	3.758	1.091	75.16	7
.9	تحد برامج أمن المعلومات من وصول الفيروسات إلى أجهزة الجامعة.	3.790	0.990	75.80	4
.10	تعزز برامج أمن وحماية المعلومات ثقة المستخدمين بالنظام.	3.714	0.989	74.28	8
.11	تعتمد الجامعة على خبراء متخصصين من أجل تطبيق الأمن السيبراني مما يعزز ثقة المستخدمين.	3.820	0.925	76.40	3
.12	تقدم الجامعة تقارير واضحة وموضوعية حول المخاطر السيبرانية.	3.670	0.886	73.40	10
.13	تستمع الجامعة لكافة الآراء والأفكار المطروحة حول تعزيز الثقة الرقمية.	3.571	1.031	71.42	14
.14	تعتمد الجامعة على سياسات وأنظمة مرنة يمكن تغييرها لتعزيز الثقة الرقمية.	3.641	0.987	72.82	12
.15	تصمم الجامعة سياسات وخطط لتعزيز ثقة المستخدم بأنظمة الجامعة وبرامجها.	3.659	1.016	73.18	11
	الثقة الرقمية	3.729	0.790	74.58	

يبين جدول (8) أن مستوى الثقة الرقمية في الجامعات السعودية مرتفعاً وبوزن نسبي (74.58%)، حيث يبين الجدول أن أعلى الفقرات من حيث الوزن النسبي جاءت:

- حصلت الفقرة رقم (1) على المرتبة الأولى والتي تنص على (يجد مستخدم البيانات حفاظاً على سرية وخصوصية بياناته)، بوزن نسبي (80.88%). وترى الباحثة أن الحفاظ على سرية وخصوصية بيانات المستخدمين يجعلهم يثقون بالمحتوى والأنظمة لذا تهتم الجامعات السعودية بسرية وخصوصية المستخدم، إضافة إلى أن الحفاظ على سرية وخصوصية المستخدمين يمنح الجامعة سمعة أكاديمية، وهذا يجعلها أكثر اهتماماً بموضوع سرية وخصوصية البيانات والمستخدمين.
- حصلت الفقرة رقم (4) على المرتبة الثانية والتي تنص على (يؤمن المستخدم بأن الأمن السيبراني كاف لمنحه الأمان في استخدام شبكات الجامعة وبرامجها)، بوزن نسبي (77.04%). وهذا يرجع إلى درجة الوعي التي يتمتع بها أعضاء هيئة التدريس وإدراكهم لمبادئ ومتطلبات الأمن السيبراني ودوره في حماية بياناتهم واستخداماتهم للشبكات والبرامج.

- حصلت الفقرة رقم (11) على المرتبة الثالثة ونصها (تعتمد الجامعة على خبراء متخصصين من أجل تطبيق الأمن السيبراني مما يعزز ثقة المستخدمين)، بوزن نسبي (76.40%). ويمكن تفسير ذلك في ضوء أن أساليب وتقنيات الأمن السيبراني بحاجة إلى قدرات فنية وبرمجية ومعرفة عميقة بالجريمة السيبرانية، وهذا يجعل الجامعات تتجه لاستشارة ذوي الخبرة، ويمكن تفسير هذه النتيجة من جهة أخرى حيث إن المملكة العربية السعودية تهتم بالأمن السيبراني وتدعو الجامعات إلى الانتماء للاتفاقات واستشارة المراكز المختصة، مثل: الهيئة الوطنية للأمن السيبراني، والمركز الوطني للعمليات الأمنية في وزارة الداخلية، والمركز الوطني لتقنية أمن المعلومات، والاتحاد السعودي للأمن السيبراني والبرمجة، ومركز التميز لأمن المعلومات بجامعة الملك سعود، ووحدة الأمن السيبراني بجامعة الأمير سلطان.

بينما كانت أدنى الفقرات من حيث الوزن النسبي:

- حصلت الفقرة رقم (13) على المرتبة ما قبل الأخيرة والتي تنص على (تستمع الجامعة لكافة الآراء والأفكار المطروحة حول تعزيز الثقة الرقمية)، بوزن نسبي (71.42%). رغم أنها جاءت بمرتبة متأخرة إلا أنها جاءت بمستوى مرتفع، وهذا يدلل على موافقة العينة على أن الجامعات السعودية تجمع المعلومات والأفكار والآراء حول الثقة الرقمية.
- حصلت الفقرة رقم (6) على المرتبة الأخيرة وتنص على (يحد النظام المتوفر من وصول الآخرين لمعلومات شخصية للمستخدمين)، بوزن نسبي (71.20%). وجاءت بنسبة مرتفعة وبمرتبة أخيرة، بمعنى أن هناك محاولات حثيثة لحماية النظام ومعلومات المستخدمين.

والثقة الرقمية متغير له عوامل مختلفة، ويتأثر بجوانب تتعلق بالمتطلبات المادية والتقنية والفنية المتوفرة بالجامعة، وأن الجامعات السعودية تسعى لتوفير متطلبات الثقة الرقمية، إلا أن جوانب الضعف والقصور فقط ترجع إلى احتراف المجرمين السيبرانيين وتمتعهم بمهارات تقنية مرتفعة، قد تفوق إمكانات الجامعات وبرامج الحماية لديها. وهذه النتائج تتفق بشكل ضمني مع نتائج دراسة (Ulven, & Wangen, 2021)

النتائج المتعلقة بالسؤال الثالث ومناقشتها

للإجابة عن السؤال الثالث الذي نصه: "**إلى أي مدى يؤثر الأمن السيبراني في تعزيز الثقة الرقمية بالجامعات السعودية من وجهة نظر أعضاء هيئة التدريس؟**". تم استخدام اختبار تحليل الانحدار الخطي البسيط، وكانت النتائج على النحو التالي:

جدول (9): العلاقة الخطية بين الأمن السيبراني بالجامعات السعودية والثقة الرقمية

النموذج	قيمة B	قيمة t	قيمة Sig.
الثابت	0.946	4.188	0.000
الأمن السيبراني	0.760	12.55	0.000
قيمة اختبار F	157.43		
قيمة R^2	0.467		

يبين جدول (9) أن قيم الاحتمال جاءت أقل من مستوى الدلالة (0.05)، وهذا يدلل على وجود أثر دال إحصائياً، وأن العلاقة الخطية بين الأمن السيبراني والثقة الرقمية دالة، كما يتضح أن معامل التفسير يساوي (0.467)، وهذا يدلل على أن التغير في الأمن السيبراني يفسر ما نسبته (46.70%) من التباين الحاصل في الثقة الرقمية.

وتفسر الباحثة هذه النتائج من خلال أن تطبيقات الأمن السيبراني تتضمن برامج حماية وأمن المعلومات والبيانات، وهذا يفيد المستفيدين من خلال حماية بياناتهم والمعلومات المتوفرة، وحماية تلك البيانات تجعل المستفيد يلجأ لها عند الحاجة، وتضمن برامج الحماية ومتطلبات الأمن السيبراني هذه البيانات من الاختراق أو التلف، وهذا يعزز ثقة المستفيد بأن الجامعة تحفظ بياناته. كذلك فإن حماية وأمن المعلومات يحافظ على سرية المستفيد وخصوصية بياناته، مما يجعل المجرم السيبراني غير قادر للوصول إليها

واختراقها أو ارسال رسائل تهدد هذه البيانات؛ مما يزيد ثقة المستفيد بأن بياناته والمعلومات المتوفرة والبرامج والشبكات آمنة وغير معرضة للمخاطر، وهذا انعكس على الثقة الرقمية لديه. ولم تتناول الدراسات السابقة تأثير الأمن السيبراني على الثقة الرقيمة، لكن أشارت بعض الدراسات بشكل ضمني إلى هذا التأثير منها (السمحان، 2020؛ المنتشري، 2020). وهذه النتائج تتفق بشكل ضمني مع نتائج دراسة (Ulven, & Wangen, 2021).

النتائج المتعلقة بالسؤال الرابع ومناقشتها:

للإجابة عن السؤال الرابع والذي ينص على: "**هل توجد فروق بين استجابات المبحوثين حول الأمن السيبراني في الجامعات السعودية في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس تعزى لاختلاف متغيري سنوات الخدمة والدرجة العلمية والتفاعل بينهما؟**". تم التحقق من الفروق بين استجابات المبحوثين باختلاف متغيري سنوات الخدمة والدرجة العلمية باستخدام اختبار تحليل التباين الأحادي.

وتم حساب الفروق بين الاستجابات المبحوثين تبعاً لتفاعل متغيري سنوات الخدمة والدرجة الكلية باستخدام اختبار تحليل التباين الثنائي، وفيما يلي توضيح للنتائج:

أولاً – الاختلاف تبعاً لمتغير سنوات الخدمة

جدول (10): اختبار تحليل التباين الأحادي للفروق بين استجابات المبحوثين تبعاً لمتغير سنوات الخدمة

البيان	مصدر التباين	مجموع المتوسطات	درجات الحرية	متوسط المربعات	قيمة (F)	قيمة (Sig.)
الأمن السيبراني	بين المجموعات	0.945	2	0.473	0.937	0.394
	داخل المجموعات	90.262	179	0.504		
	الإجمالي	91.207	181			
الثقة الرقمية	بين المجموعات	0.082	2	0.041	0.065	0.937
	داخل المجموعات	112.960	179	0.631		
	الإجمالي	113.042	181			

يبين جدول (10) أن قيم الاحتمال جاءت أكبر من مستوى الدلالة (0.05)، وهذا يدلل على أنه لا توجد فروق ذات دلالة إحصائية بين استجابات المبحوثين تعزى لمتغير سنوات الخدمة على محورين الأمن السيبراني والثقة الرقمية. وترى الباحثة أنه رغم اختلاف سنوات الخدمة لأفراد العينة إلا أن استجاباتهم جاءت متقاربة ودون فروق، وقد يرجع ذلك إلى أن الجامعات السعودية تشترك بكثير من الاتفاقات ومراكز الأمن السيبراني والتي تمنحها الاستشارات والبرامج وتطبيقات الحماية، فكانت تطبيقات الأمن السيبراني والاهتمام بها لدى معظم الجامعات السعودية، وهذا انعكس على ثقة المستفيد، وبالتالي جاءت الاستجابات دون الفروق لأن البيانات والشبكات المتاحة لكافة العاملين دون استثناء ويمكن لعضو هيئة التدريس الولوج لنفس الشبكات والبرامج دون تمييز من حيث سنوات الخدمة لديهم.

ثانياً – الاختلاف تبعاً لمتغير الدرجة العلمية

جدول (11): اختبار تحليل التباين الأحادي للفروق بين استجابات المبحوثين تبعاً لمتغير الدرجة العلمية

البيان	مصدر التباين	مجموع المتوسطات	درجات الحرية	متوسط المربعات	قيمة (F)	قيمة (Sig.)
الأمن السيبراني	بين المجموعات	2.207	3	0.736	1.471	0.224

	داخل المجموعات	89.00	178	0.500		
	الإجمالي	91.207	181			
الثقة الرقمية	بين المجموعات	2.059	3	0.686	1.101	0.350
	داخل المجموعات	110.983	178	0.623		
	الإجمالي	113.042	181			

يبين جدول (11) أن قيم الاحتمال جاءت أكبر من مستوى الدلالة (0.05)، وهذا يدلل على أنه لا توجد فروق ذات دلالة إحصائية بين استجابات المبحوثين تعزى لمتغير الدرجة العلمية على محورين الأمن السيبراني والثقة الرقمية. وترى الباحثة أن رؤية المملكة (2030) استدعت من كافة العاملين بالجامعات السعودية الاتجاه نحو تكنولوجيا المعلومات والاتصالات، والعمل ضمن فضاء سيبراني، ولقد قامت الجامعات بإنفاق كثير من المال وبذلت كثير من الجهد لتوفير بيئة إلكترونية آمنة لكافة أعضاء هيئة التدريس، وأنه رغم اختلاف هيئة التدريس من حيث الدرجات العلمية إلا أنهم يتعاملون مع أنظمة موحدة حيث تعتمد كثير من الجامعات برامج موحدة في الأمن والحماية لكافة أجهزتها وفق اتفاقات مع شركات وبرامج الحماية، كذلك فإنه يمكن تفسير ذلك في ضوء أن كافة العاملين بالجامعات السعودية وأعضاء هيئة التدريس يواجهون نفس المخاطر والجرائم الإلكترونية وبالتالي جاءت استجاباتهم متقاربة.

ثالثاً: التفاعل بين متغيري سنوات الخدمة والدرجة العلمية

جدول (12): اختبار تحليل التباين الثنائي للفروق بين استجابات المبحوثين تبعاً لمتغيري سنوات الخدمة الدرجة العلمية

المحور	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة (F)	قيمة (Sig.)
الأمن السيبراني	سنوات الخدمة	**0.022**	**2**	**0.011**	**0.022**	**0.978**
	الدرجة العلمية	**1.160**	**3**	**0.387**	**0.761**	**0.517**
	سنوات الخدمة – الدرجة العلمية	**1.900**	**6**	**0.317**	**0.624**	**0.711**
	الخطأ	**86.342**	**170**	**0.508**		
	الكلي	**2528.33**	**182**			
الثقة الرقمية	سنوات الخدمة	**0.078**	**2**	**0.039**	**0.060**	**0.942**
	الدرجة العلمية	**0.937**	**3**	**0.312**	**0.483**	**0.695**
	سنوات الخدمة – الدرجة العلمية	**0.852**	**6**	**0.142**	**0.219**	**0.970**
	الخطأ	**109.99**	**170**	**0.647**		
	الكلي	**2643.39**	**182**			

يبين الجدول (12) أن جميع قيم الاحتمال جاءت أكبر من مستوى الدلالة (0.05)، وهذا يدلل على عدم وجود اختلاف يعزى لاختلاف التفاعلات بين متغيري سنوات الخدمة والدرجة العلمية، بمعنى أن تفاعل متغيري سنوات الخدمة والدرجة العلمية لا تؤثر في استجابات المبحوثين حول الأمن السيبراني والثقة الرقمية. وترى الباحثة أن الجامعات السعودية لديها إيمان بأن الأمن السيبراني يتيح بيئة آمنة لاستخدام الفضاء الإلكتروني، وهذا الإيمان جعلهم يتجهون نحو حماية كافة الأنظمة والشبكات وفق خطط وسياسات واضحة، وشعر بها كافة أعضاء هيئة التدريس كونهم يستخدمون هذه البرامج والأنشطة، فلا يمكن لعضو هيئة تدريس أن يلج لصفحات وبرامج الجامعة دون كلمة مرور وكلمة سر خاصة به، وكثير من الإجراءات يتم تطبيقها لكافة البرامج والأجهزة مما جعل أي اختلاف في خصائصهم الديمغرافية من سنوات خدمة ودرجات علمية أو متغيرات أخرى لا يؤثر في إدراكهم لخطوات وتطبيقات الأمن السيبراني والثقة الرقمية.

التوصيات:

على ضوء ما توصلت إليه الدراسة من نتائج توصي الباحثة بالتالي:

1- الإيمان بأن الأمن السيبراني أفضل وأقصر الطرق لحماية البيانات والأنظمة.
2- تخصيص قسم لأمن وحماية المعلومات مهمته متابعة وتحديث برامج حماية وأمن المعلومات والأنظمة الإدارية والأجهزة التقنية.
3- اعتماد آليات توثيق للوثائق العلمية والمراسلات الإدارية والأكاديمية بالجامعات آمنة ومحمية من الاختراق أو التهديديات الإلكترونية.
4- توعية وتثقيف العاملين بالجامعات السعودية حول سبل حماية بياناتهم وأجهزتهم من الجرائم السيبرانية.
5- الاعتماد على أقوى البرامج لمقاومة البرمجيات الخبيثة والفيروسات التي تتلف البيانات والأجهزة.
6- تطوير أنظمة تقنية تمنع وصول العابثين إلى المعلومات الشخصية للمستخدمين والمستفيدين من أنظمة الجامعة وبرامجها.
7- الاهتمام بآراء وأفكار العاملين حول سبل حماية وأمن المعلومات والأمن السيبراني.
8- الاعتماد على سياسات مرنة يمكن تغييرها وتطويرها لتحقيق الأمن وحماية الأجهزة والتقنيات والشبكات والبرامج مما يسهم في تحقيق الثقة الرقمية.

المقترحات:

1- إجراء مزيد من الدراسات حول واقع الأمن السيبراني من وجهات نظر مختلفة: الإداريين، الطلبة.
2- إجراء دراسات تبحث في واقع الأمن السيبراني في الجامعات كإطار لتحقيق رؤية المملكة (2030).
3- إجراء مزيد من الدراسات حول درجة وعي العاملين في الجامعات السعودية بمتطلبات وتطبيقات الأمن السيبراني.
4- إجراء دراسات حول مخاطر الجرائم السيبرانية في المجتمع السعودي.

قائمة المصادر والمراجع

أولاً: المصادر والمراجع العربية.

الاتحاد الدولي للاتصالات. (2011). *الاتجاهات في مجال الاتصالات: تمكين عالم الغد الرقمي*. (http://www.itu.int)، تاريخ الاسترجاع: 14/ مايو/ 2021م.

الألفي، محمد. (2010). بعض أنماط جرائم الاعتداء على النظم المعلوماتية في المؤسسات. ندوات مكافحة الجريمة عبر الانترنت المنعقدة في المنظمة العربية للتنمية الإدارية، *ورشة عمل بعنوان: "أمن المعلومات والتوقيع الإلكتروني"*، القاهرة: المنظمة العربية للتنمية الإدارية، ص 83 – 100. متوفرة على الرابط الإلكتروني التالي: (https://search.mandumah.com/Record/125053)، تاريخ الاسترجاع: 28/ مايو/ 2021م.

بركات، زياد وحسن، كفاح. (2009). حاجات التنمية المستقبلية لدى طلبة الدراسات العليا تخصص التربية في الجامعات الفلسطينية. المؤتمر الأول لعمادة البحث العلمي في جامعة النجاح الوطنية، المنعقد بجامعة النجاح الوطنية بنابلس.

الجندي، علياء بنت عبدالله ومحمد، نهير طه. (2019). دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلومات لدى طالبات الجامعة. *مجلة عالم التربية – المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية. ع(67)، ج(3)، ص 14 – 84.*

الدهشان، جمال علي والسيد، سماح السيد. (2020). رؤية مقترحة لتحويل الجامعات المصرية الحكومية إلى جامعات ذكية في ضوء مبادرة التحول الرقمي للجامعات. *المجلة التربوية – جامعة سوهاج، م(78)، ع(78)، ص 1249 – 1344.*

دليل رؤية المملكة العربية السعودية (2030). المركز الإعلامي، تم الاسترجاع من الرابط: (https://www.vision2030.gov.sa/ar/)، تاريخ الاسترجاع: 21/ يوليو/ 2021م.

السمحان، منى عبدالله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. *مجلة كلية التربية – جامعة المنصورة. ع(111)، ج(1)، ص 2 – 29.*

الشهراني، بيان ناصر وفلمبان، فدوى ياسين. (2020). أثر برنامج تدريبي قائم على تصميم ألعاب تعليمية إلكترونية باستخدام برنامج (Game Marek) لإكساب مفاهيم الأمن السيبراني لدى طالبات المرحلة المتوسطة. *مجلة البحث العلمي في التربية – جامعة عين شمس. ع(21)، ج(9)، ص 614 – 651.*

الصانع، نورة عمر وسليمان، إيناس السيد محمد وعسران، عواطف سعدالدين والسواط، حمد بن حمود وأبو عميشة، زاهدة جميل. (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. *مجلة كلية التربية – جامعة أسيوط. م(36)، ع(6)، ص 41 – 90.*

الصبان، عبير محمد والحربي، سماح عيد. (2019). إدمان الطلاب على استخدام مواقع التواصل الاجتماعي وعلاقته بالأمن النفسي والتورط في الجرائم السيبرانية. *المجلة الدولية للدراسات التربوية والنفسية. م(6)، ع(2)، ص 267 – 293.*

العريشي، جبريل حسن والدوسري، سلمى بنت عبدالرحمن. (2018). دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع. *مجلة مكتبة الملك فهد الوطنية – مكتبة فهد الوطنية. م(24)، ع(2)، ص 302 – 373.*

الغامدي، سارة أحمد. (أكتوبر/ 2018). مبادرة العطاء الرقمي، تم الاسترجاع من الرابط: (https://attaa.sa/arabic-content/view/20)، بتاريخ: 17/ مايو/ 2021م.

فوزي، إسلام. (2019). الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي. *المجلة الاجتماعية القومية – المركز القومي للبحوث الاجتماعية والجنائية. م(56)، ع(2)، ص 99 – 139.*

القحطاني، نورة بنت ناصر. (2019). مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. *مجلة شؤون اجتماعية – جمعية الاجتماعيين في الشارقة. م(36)، ع(144)، ص 85 – 120.*

كليمان، سارة غران. (2018). *التعلم الرقمي: التربية والمهارات في العصر الرقمي*. الندوة الاستشارية المعنية بالتعلم الرقمي التي عقدت كجزء من برنامج معهد كورشام للقيادة الفكرية: (Corsham Institute Thought Leadership Programme).

مانيطه، يوسف إسماعيل. (2017). نظرة عامة على الجريمة الإلكترونية في الفضاء السيبراني. *المجلة الليبية العالمية – جامعة بنغازي، ع(32)، ص 1 – 10.*

المنتشري، فاطمة يوسف وحريري، رندة. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية. م(4)، ع(13)، ص 95 – 140.*

المنتشري، فاطمة يوسف. (2020). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للعلوم التربوية والنفسية. م(4)، ع(17)، ص 457 – 484.*

الموجي، كوثر السعيد ومحمود، دينا كمال وإمام، أحمد عزمي. (2021). تصور مقترح لتفعيل الأمن السيبراني بوزارة ومديريات الشباب والرياضة بجمهورية مصر العربية. *مجلة بني سويف لعلوم التربية البدنية والرياضية. م(4)، ص (7)، ص 14 – 38.*

نذير، غانم ومعمر، جميلة وريحان، عبدالحميد وعنكوش، نبيل. (نوفمبر/ 2012). الثقة الرقمية ضمن استراتيجية الجزائر الإلكترونية 2013 واقعها ودورها في إرساء مجتمع المعرفة. *أعمال المؤتمر الثالث والعشرون: الحكومة والمجتمع والتكامل في بناء المجتمعات المعرفية العربية. ج(1)، (ص: 76 – 93)*، الدوحة، قطر.

يونس، مجدي محمد. (2015). دور الجامعة في تحقيق مجتمع المعرفة لمواكبة التطور المعلوماتي – دراسة ميدانية بجامعة القصيم. *المجلة العربية لضمان جودة التعليم العالي. م(8)، ع(21)، ص 125 – 156.*

ثانياً: المصادر والمراجع الأجنبية.

Goutam, R. K., & Verma, D. K. (2015). Top Five Cyber Frauds. *International Journal of Computer Applications*, *119*(7), 23 - 25.

Lehto, M. (2020, June). Cyber security capacity building–cyber security education in Finnish universities. In *ECCWS 2020 20th European Conference on Cyber Warfare and Security* (p. 221). Academic Conferences and publishing limited.

Redman, S. M., Yaxley, K. J., & Joiner, K. F. (2020). Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities?. *Creative Education*, *11*(12), 2541 – 2558.

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for Cyber Security in Schools: The Human Factor. *Educational Planning*, *27*(2), 23-39.

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39.

Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, *9*(3), 395-399.

Yan, Z., Xue, Y., & Lou, Y. (2021). Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. *Computers in Human Behavior*, *121*, 106791.