A Prospective Vision of the Requirements for Students Based on the Delphi Building a Cybersecurity Culture among Jordanian University Methodology

Muhammad Salim Al-Zboun[(1)*] **Faten Mahmoud Abu Salah**[(2)]

(1) Professor, University of Jordan,Jordan.
(2) Part-time Lecturer, University of Jordan, Jodan.

Received: 10/03/2025
Accepted: 23/04/2025
Published: 13/11/2025

* ***Corresponding Author:***
zboon75@yahoo.com

DOI:https://doi.org/10.59759/educational.v4i3.1444

Abstract

This study aimed to propose a foresight vision of the requirements necessary to build a cybersecurity culture among Jordanian university students, based on the Delphi method. To achieve the study's objectives, the qualitative approach was used with the predictive Delphi methodology (rounds). Information was collected by defining the subject of the study which is the requirements for building a cybersecurity culture among Jordanian university students, for which the possible and probable future is predicted and investigated. A questionnaire was then developed as a data collection tool, and a group of experts was selected to provide their opinions by answering the questionnaire's questions. The study sample consisted of (40) university professors from three universities (University of Jordan, Yarmouk University, Mutah University), who were selected by simple random sampling so that none of them knew each other. Then, the initial measurement of the experts' opinions, which were received when the questionnaire was applied in the first round, was carried out. The data in the questionnaire was then organized and arranged in its initial form, summarized, and its initial results were presented to the group of experts as a form of feedback. The opinions in the experts' responses were remeasured after they made the appropriate changes and modifications in light of their colleagues' responses. The questionnaire was applied over two rounds to ensure the stability of the responses. The results showed that the experts agreed on the necessity of including elements related to the intellectual, technological, theoretical, and legislative aspects in the future requirements for building a cybersecurity culture among students.

Special Issue on Educational Technologies and Future Technology.

رؤية استشرافية للمتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى طلبة الجامعات الأردنية استنادا الى منهجية دلفاي

محمد سليم الزبون[1] فاتن محمود أبو صلاح[2]

(1) أستاذ، الجامعة الأردنية، عمان – الأردن.

(2) محاضر غير متفرغ، الجامعة الأردنية، الأردن.

الملخص

هدفت الدراسة إلى اقتراح رؤية استشرافية للمتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى طلبة الجامعات الأردنية استنادا إلى أسلوب دلفاي، ولتحقيق أهداف الدراسة تم استخدام المنهج النوعي باستخدام منجية دلفاي التنبؤية (الجولات)، وتم جمع المعلومات من خلال تحديد الموضوع محل الدراسة وهو المتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى طلبة الجامعات الأردنية، والذي يتم التنبؤ واستقصاء المستقبل الممكن والمحتمل من أجله، ومن ثم تم تطوير استبانة كأداة لجمع البيانات واختيار مجموعة من الخبراء لكي يدلو بآرائهم من خلال الإجابة عن أسئلة الاستبانة، وتكونت عينة الدراسة من (40) أستاذ جامعي من ثلاث جامعات (الأردنية، اليرموك، مؤتة)، وتم اختيارهم بالطريقة العشوائية البسيطة بحيث لا يعرف أي منهم الآخر، وتم بعد ذلك القيام بالقياس الأولي لآراء الخبراء التي وردت عند تطبيق الاستبانة في الجولة الأولى، ومن ثم تنظيم وترتيب البيانات الواردة في الاستبانة بصورتها الأولية وتلخيصها والقيام بعرض نتائجها الأولية على مجموعة الخبراء كنوع من أنواع التغذية الراجعة. وإعادة قياس الآراء الواردة في استجابات الخبراء بعد أن يقوموا بإجراء التغييرات والتعديلات المناسبة في ضوء استجابات زملائهم، وتم القيام بتطبيق الاستبانة على مدار جولتين لضمان ثبات الإجابات، أظهرت النتائج اتفاق الخبراء على ضرورة أن تتضمن المتطلبات المستقبلية لبناء ثقافة الأمن السيبراني لدى الطلبة عناصر تتعلق بالجانب الفكري والتكنولوجي والنظري والتشريعي.

المقدمة:

ساهم الانفجار المعرفي وظهور العصر الرقمي في القرن الحالي في تطور التكنولوجيا وأدواتها، وقد ساعد ذلك في ظهور العديد من الجرائم السيبرانية والتهديدات التي أصبحت تشكل تحديات كبيرة لدول العالم، خاصة فيما يتصل بالأمن القومي، الأمر الذي دفع العديد من المهتمين والباحثين في ميدان الأمن السيبراني إلى اعتبار الفضاء السيبراني مجالًا خامسًا في الحروب كما سيظهر في متن الدراسة، وهذا ما دفع الدول للبحث عن الوسائل والضمانات التي يمكن من خلالها حماية الفضاء السيبراني من التهديدات المتنوعة.

ولقد تغير مفهوم الأمن السيبراني واكتسب سمات وخصائص عديدة في ظل تدفق المعلومات في العديد من دول العالم، وظهور عصر الإنترنت والعولمة، ووسائل الاتصالات السريعة التي حولت العالم إلى قرية صغيرة يكاد أبعدها يكون أقرب إلى الإنسان من أقرب الأشياء المادية، وأصبح الأمن السيبراني مسألة ذات أهمية عالمية، وما يُظهر ذلك أن أكثر من خمسين دولة نشرت رسميًا شكلاً من أشكال وثيقة الاستراتيجية التي تحدد موقفها الرسمي من الفضاء الإلكتروني و/أو الجريمة الإلكترونية و/أو الأمن السيبراني (Leung, 2018).

ويُمكن التعريف بمفهوم الأمن السيبراني بأنه الأسلوب أو الطريقة التي يحدث من خلالها تقليص الأخطار والتهديدات التي قد يتعرّض لها الفرد والمؤسسة في الفضاء السيبراني، بحيث توفّر شبكة الإنترنت البيئة الواسعة والمناسبة والمحفزة لهذه الهجمات والتهديدات الإلكترونية. ويشمل الأمن السيبراني ضمان سلامة وأمن الأجهزة الحاسوبية، والبرامج والأنظمة التقنية، والاتصالات الإلكترونية، بما تحتويه من معلومات وبيانات سرية وخاصة، من الولوج غير الآمن، والاختراق والاستغلال غير المصرّح به، وحالات التجسس والتخريب، ليُشير بذلك مفهوم الأمن السيبراني إلى العملية التي تحد من الهجمات والتهديدات السيبرانية، بهدف حماية النظام التقني وتأمينه ضمن فضاء سيبراني ممتد ومتنوّع (شلوش، 2018).

ومع زيادة التعامل مع الإنترنت والانفتاح الثقافي على ثقافات متعددة، وسهولة الوصول للمعلومات والأفراد في الفضاء السيبراني، وتعدد منصات التواصل الاجتماعي، أصبح من الضروري إكساب المتعلمين مهارات التعامل مع البيانات في الفضاء السيبراني وتعليمهم أهمية حماية معلوماتهم من الهجمات والاختراقات، وتهذيب سلوكهم في هذا الفضاء وبناء شخصياتهم الوطنية وتعزيز انتمائهم لوطنهم وحماية هويتهم الوطنية في وجود التأثيرات السلبية العابرة للحدود الجغرافية. حيث أشارت كثير من الدراسات مثل دراسة زويلنج وكلين ولِسجاك ووايهتيك وسيتين وباسيم (Zwilling; Klien; Lesjak; Wiechetek, Çetin & Basım, 2022) إلى أن هناك علاقة إيجابية قوية بين الوعي بالأمن السيبراني والقيم الأخلاقية والوطنية والدينية لدى الطلبة، كما أنه يمكن التنبؤ بالقيم الأخلاقية والوطنية والدينية من خلال الوعي بالأمن السيبراني.

لذا فإن تزويد طلبة الجامعات بمعارف ومعلومات حول الأمن السيبراني سيرفع مستوى الوعي بأهمية هذا المفهوم ومجالات الاستفادة منه، كما أن إعطائهم المفاهيم والمبادئ والمهارات والأسس

والأساليب التي يقوم عليها الأمن السيبراني سينعكس على مدى قدرتهم في التكيف والتعامل مع التطورات والمتطلبات المستقبلية المتلاحقة، كما وسيوفر لهم البيئة الآمنة والمحمية لاستخدام البيانات والبرامج والتطبيقات في الفضاء السيبراني.

ومن هذا المنطلق توجد العديد من الأهداف لتحقيق متطلبات الأمن السيبراني في الجامعات أشار لها المنيع (2022)، كالعمل على إيجاد بنية تحتية منسابة لأمن البيانات والمعلومات التي تتعلق بأعضاء هيئة التدريس في الكليات والطلبة، والعمل أيضًا على الحماية لشبكة المعلومات من خلال الكشف عن الأمور التي يمكن من خلالها حدوث الاختراقات والتعديات والعمل على كشفها والتصدي لها، وإيجاد أرقام سرية لجميع المعاملات التي تتم داخل الجامعة بحيث يتم الحماية من أي اختراق، بالإضافة إلى العمل على توفير بيئة آمنة، بعمل واعٍ ومدروس على شبكة الإنترنت، والعمل على تعزيز قدرة الطلبة في مجال أنظمة حماية الشبكات وقواعد البيانات المختلفة، وإكساب الطلبة الأسس والمهارات الضرورية واللازمة في حقول ومواضيع الأمن السيبراني، وأيضًا العمل على إعداد وتجهيز الطلبة بحيث يكونوا كادرًا بشريًا متميزًا ومؤهلًا ومجهزًا بالكفايات النظرية والعملية اللازمة للعمل والتطوير المطلوب في بيئة الفضاء السيبراني المعاصر.

فللأمن السيبراني دور رئيس في تعزيز وتدعيم الأمن الفكري للطلبة بما يقدمه من حماية وأمن للمعلومات الحساسة والتكنولوجيا المستخدمة فيها، وما يوفره من سياق قانوني يشمل التشريعات والقواعد التي تكافح التهديدات والجرائم السيبرانية، حيث يقوم الأمن السيبراني بحماية المواقع والمنصات الإلكترونية المختلفة التي يستخدمها الطلبة من نشر وتداول الأفكار والقيم السلبية والمتطرفة، بالإضافة إلى تفعيل آليات الأمن السيبراني في مراقبة هذا المحتوى الفكري من السلوكيات غير القويمة، ومنع فقدان الملكية الفكرية للطلبة أو التلاعب فيها بهدف تغيير اتجاهاتهم وقيمهم ومعتقداتهم، وضمان استمرار توافقها وانسجامها مع ثقافة ومعايير مجتمعهم وهويتهم الوطنية.

والمؤسسات التعليمية، وعلى رأسها الجامعات، مسؤولة عن تنمية الهوية الوطنية وحمايتها لدى الطلبة، وتعزيز المواطنة الصالحة ورموز الوطن ومعالمه في أفكارهم وممارساتهم، حتى لا تتأثر بالشائعات والقيم المتطرفة والتضليل والتحريض الذي قد يتعرضون له في ضوء الفضاء السيبراني الواسع، وذلك بتفعيل منظومة الأمن السيبراني داخل الحرم الجامعي وتوعية الطلبة بوسائل وآليات هذه المنظومة وكيفية استثمارها في تحقيق أمنهم الفكري وهويتهم الوطنية.

مشكلة الدراسة وأهميتها

شهدت المملكة الأردنية الهاشمية وبحسب المركز الوطني للأمن السيبراني ارتفاعاً في نسبة التهديدات السيبرانية إلى (77%) في الربع الأول من العام (2023)، إذ رصد المركز (63) حادث تجسس، و(563) حادث وتهديد سيبراني في نفس الفترة، والذي استطاع أن يتعامل معها والحدّ من تأثيرها هي وغيرها من التهديدات السيبرانية الأخرى، والتي صُنفت بين المرتفعة والمتوسطة وعادية الخطورة، كما وأظهر تقرير للمركز الوطني السيبراني خلال الربع الثالث من العام (2024) أن عدد الحوادث السيبرانية المكتشفة (1656) حادثاً أي أنه ارتفع بنسبة (4.7%) عن الربع الثاني من نفس العام، كما أن المركز الوطني للأمن السيبراني لم يسجل أي حادث سيبراني مصنف بدرجة شديد الخطورة للربع الثالث على التوالي من العام الحالي، كما وبلغ عدد الحوادث المصنفة خطير (31) جادثاً لتبين انخفاضاً بنسبة (34%) عن الربع الثاني من العام الحالي، بينما أظهر نفس التقرير ارتفاع في الحوادث السيبرانية والمصنفة متوسط الخطورة خلال الربع الثالث وبنسبة (8.9%) أي 1536 حادثاً مقارنةً مع (1411) حادثاً خلال الربع الثاني من العام الحالي، أما الحوادث منخفضة الخطورة وصلت إلى 98 حادثاً في الربع الثالث لتنخفض بنسبة (21%) عن الربع الثاني من نفس العام (المركز الوطني للأمن السيبراني، 2024)، ومن هذا المنطلق ووسط هذه التحديات تتضح أهمية مشكلة الدراسة الحالية.

تكمن أهمية الدراسة في نتائجها المتوقعة، إذ يُؤمل أن يستفيد من نتائج الدراسة الجهات الآتية:

1- **أصحاب القرار والمعنيين في الجامعات الأردنية:** وذلك من خلال الاستفادة من نتائج هذه الدراسة في وضع إجراءات وآليات بناء ثقافة الأمن السيبراني وتعزيزها لدى الطلبة.
2- **واضعو الخطط المستقبلية في وزارة التعليم العالي الأردنية:** وذلك من خلال إلقاء الضوء على دور الجامعات الأردنية في بناء ثقافة الأمن السيبراني وتعزيزها لدى طلبتها، والعمل على تفعيل الوسائل والإجراءات والآليات التي تساعدها في تحقيق هذا الدور.

وتهدف الدراسة الإجابة على السؤال التالي:

- ما الرؤية الاستشرافية للمتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى طلبة الجامعات الأردنية استنادا الى منهجية دلفاي؟

وتأسيساً على ما سبق فإن مشكلة الدراسة تبحث في رؤية استشرافية للمتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى طلبة الجامعات الأردنية استنادا الى منهجية دلفاي.

مصطلحات الدراسة

الأمن السيبراني اصطلاحاً: "هو أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وعليه؛ فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الإلتزام بها لمواجهة التهديدات، ومنع التعديّات، أوللحدّ من آثارها في أقسى وأسوأ الأحوال، ويرتبط هذا الأمن، ارتباطاً وثيقاً بأمن المعلومات، فالوصول إلى هذه الأخيرة، أو بثها أو الإطلاع عليها، والمتاجرة بها، أو تشويهها واستغلالها هو ما يقف غالب الأحيان، وراء عمليات الإعتداء على الشبكات وعلى الإنترنت بشكل أكثر"(العمارات والحمامصة، 2022: 15).

ثقافة الأمن السيبراني اصطلاحاً: "ثقافة حماية البيئة الرقمية الحركية التي يخلقها مستخدمو الانترنت ببرامجهم المتنوعة وهي إعادة تشكيل المجتمع المحلي بواسطة التكنولوجيا المتاحة وتوفير معدات وأدوات تأمين المعلومات " (فرجاني، 2023 :39).

وتعرّف إجرائياً: بأنها جميع الوسائل والأساليب والعمليات والآليات والنشاطات والبرامج والحملات التثقيفية والتوعوية التي تقوم بها الجامعات الأردنية بهدف بناء ثقافة الأمن السيبراني وتعزيزها ورفع مستوى الوعي بأهميتها وضرورة حماية أمن العلومات والبيانات وأجهزتها وقواعدها من الأخطار والتهديدات السيبرانية في الفضاء السيبراني المفتوح، وتم قياسها من خلال إجابات أفراد العينة على الأداة المعدة لهذا الغرض.

الدراسات السابقة

وقد تناول عدد من الدراسات الدراسات السابقة موضوع الأمن السيبراني فقد أجرت القحطاني (2019) دراسة هدفت إلى تعرف درجة توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي، وتم استخدام منهج المسح الاجتماعي بأسلوب العينة، وبلغت عينة الدراسة (486) طالباً وطالبة، واعتمدت الدراسة على الاستمارة الإلكترونية لتجميع البيانات، وقد تمت الدراسة في الجامعات السعودية للعام 1440/1439، وكانت أهم النتائج بأن أقرب مفهوم للأمن السيبراني من وجهة نظر عينة الدراسة هو: استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، في حين جاءت جريمة (الاحتيال الالكتروني/ النصب الالكتروني) كأكثر جريمة يتعامل معها الأمن السيبراني، في حين تعد التوعية الإعلامية للمجتمع حول طرقه هي أهم طرق الوقاية المجتمعية

لمشكلات الفضاء السيبراني، كما جاءت النتائج بوجود معوقات اجتماعية في تحقيق الوقاية للمجتمع السعودي، وأن أهم هذه المعوقات هو التطور الهائل في نظم المعلومات، ووسائل التكنولوجيا التي يتعامل معها أفراد الأسرة دون المعرفة الكاملة لمشكلات هذه الوسائل وكيفية تجنبها.

وأجرت كاعوه (2020) دراسة هدفت إلى تقديم رؤية مقترحة لتضمين سياسات الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي، تم الاستعانة بالمنهج الوصفي لوصف وتحليل المشكلة ووصف التحول الرقمي للجامعات، وأهم متطلبات تطبيقه، ومعرفة وتحديد العلاقات بين مكونات التحول الرقمي، وسياسات الأمن السيبراني، كما استخدمت الدراسة المنهج المستقبلي لرسم تصور مقترح لسياسات الأمن السيبراني، بحيث تستطيع أن تحمي البُنية التكنولوجية الرقمية الداعمة للتحول الرقمي للجامعات المصرية، وأجريت الدراسة على الجامعات المصرية في العام 2020. وتوصلت إلى وضع رؤية مقترحة لسياسات الأمن السيبراني للجامعات المصرية بالاستفادة من الخبرات الدولية.

وأجرى توفيق ومرسي (2023) دراسة هدفت إلى تحديد أهم متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ظل التحول الرقمي وأهم المعوقات التي تحول دون تحقيق هذه المتطلبات من وجهة نظر أعضاءهيئة التدريس بجامعة بنها في مصر، واستخدمت الدراسة المنهج الوصفي لتحقيق هدفها، باستخدام الاستبانة، وقد تكونت عينة الدراسة من (248) عضو هيئة تدريس، وتوصلت نتائج الدراسة إلى اتفاق العينة على متطلبات تحقيق الأمن السيبراني بجامعة بنها في ظل التحول الرقمي، والتي تمثلت مجموعة من المتطلبات التقنية والمادية والبشرية والمعرفية، ومعوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها .

كما أجرى توحيدي و بريدمور (Towhidi & Pridmore ,2023) دراسة هدفت إلى تقديم أنموذج لتصميم دورة للأمن السيبراني تتوافق مع ما تحتاجه مؤسسات الصناعة وذلك للإستجابة لنقص المتخصصين في الأمن السيبراني، واعتمد النموذج المقترح على تصميم الدورة التي تتماشى مع المبادئ التوجيهية من المعهد الوطني للمعايير والتكنولوجيا NICE في إطار الأمن السيبراني، واستخدم الباحثان منهجية لتصميم دورة الأمن السيبراني لتتماشى مع احتياجات الصناعة من إنشاء إطار تعليمي تم تطويره بناءً نموذج يتوافق مع NIST Cybersecurity Framework، وإرشادات المعهد الوطني للمعايير والتكنولوجيا NICE للخطة الإستراتيجية، ورؤى من الصناعة من وجهة نظر المهنيين، وتتضمن نموذج تصميم الدورة ما يلي : تحديد أهداف التعلم المناسبة للدورة التي تتماشى مع احتياجات

الصناعة وتحديد المناهج التعليمية والتربوية المناسبة وطُرق تحديد الأدلة المقبولة ومعايير التقييم وطرق تطوير المحتوى التعليمي، تم تطبيق النموذج في معهد للتعليم العالي في الولايات المتحدة الأمريكية، حيث يشغل خريجو التعليم العالي معظم وظائف الأمن السيبراني، وأشارت النتائج إلى أن التصميم قوبل بمستويات عالية من رضا الطلبة وردود فعل إيجابية من الصناعة ومستويات عالية من نجاح الطلبة، كما أشارات النتائج إلى إمكانية تطبيق النموذج على أي مؤسسة تعليمية وتخصيصه وفقًا للاحتياجات المرغوبة للمعهد الطلبة والصناعة لتوفير التكلفة والوقت.

وأجرى كل من نوجوكو وشيديك نجوكو وتشوكو رافيشدران (Njoku & Chidike Njoku & Chukuw & Ravichandran, 2023) دراسة هدفت إلى تحليل تأثير الأمن السيبراني و التهديدات السيبرانية على المكتبات والمستودعات الجامعية كما ركزت الدراسة على حماية المؤسسات ومستودعات المكتبات الجامعية في نيجيريا، واستخدم الباحثون التقييم اليدوي لجميع مستودعات المكتبات الجامعية في نيجيريا والمسجلة على Opendoar.org باستخدام المنهج الوصفي النوعي، وعلى عينة الدراسة المكوّنة من (88) من أمناء مكتبات ومعلومات واتصالات والعاملين في مجال التكنولوجيا في الجامعات، بتوزيع استبيان حول التهديدات والمخاطر السيبرانية، وأظهرت النتائج أنه من (198) جامعات فيدرالية وحكومية وخاصة، فقط (29) أنشأت مستودعات مؤسسية للأمن السيبراني، وأن تطبيق أنظمة الأمن السيبراني وحراسة الأجهزة والبرامج والبنية التحتية مثل؛ إدارة الهوية الوصول والتشغيل، والتطبيق شبكة آمن والبيانات في مستودعات مكتبات الجامعات يمكن أن تقلل من حوادث الجرائم الإلكترونية.

وقد اعتمدت أغلب الدراسات السابقة على المنهج الوصفي التحليلي في جمع البيانات وتحليلها لتحقيق أهداف الدراسة، وقد استفادت هذه الدراسة من الدراسات السابقة، إذ شكلت لها المصدر الأساسي لكثير من المعلومات المهمة ساهمت في كتابة الأدب النظري، فقد تم الاستفادة من أطرها العامة، وطُرُقها الإجرائية، وهذا بالاضافة إلى أن تلك الدراسات وجهت الباحثين نحو العديد من البحوث والمراجع المناسبة، ومكنتهم من تكوين تصوّر شامل عن الأُطر النظرية التي ينبغي أن تشتملها هذه الدراسة.

كما وتتميز هذه الدراسة عن غيرها من الدراسات السابقة في عدد من الأمور أهمها محاولة تعرف المتطلبات المستقبلية اللازمة لبناء ثقافة الأمن السيبراني لدى الطلبة، باستخدام منهجية دلفاي، وإضافةً إلى أن عينة الدراسة اشتملت جامعات أردنية من مختلف أقاليم المملكة.

الطريقة والإجراءات

مجتمع الدراسة وعينتها

تكون مجتمع الدراسة من جميع أعضاء الهيئة التدريسية في الجامعات الأردنية الرسمية، والبالغ عددهم (8197) حسب إحصائيات وزارة التعليم العالي للعام (2022/ 2023).

وتم اختيار عينة الدراسة على دفعتين، إذ تم أولًا اختيار الجامعة الأردنية لتمثل إقليم الوسط وجامعة اليرموك لتمثل إقليم الشمال وجامعة مؤتة لتمثل إقليم الجنوب، وقد تم اختيار هذه الجامعات قصديًا، ومن ثم تم اختيار (40) عضوًا من أعضاء الهيئة التدريسية في الجامعات الأردنية ليمثلوا الخبراء وتم اختيارهم بالطريقة العشوائية البسيطة.

الإجراءات:

تم البدء بالجولة الأولى حتى يتم التوصل إلى مجموعة من المتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى طلبة الجامعات الأردنية، وذلك من خلال استفتاء آراء مجموعة من الخبراء وأساتذة الجامعة المتخصصين بأصول التربية والحاسوب والأمن السيبراني، وذلك اعتماداً على عدة جولات متتابعة للوصول إلى إجماع في آرائهم، واتفاق حول تلك المتطلبات ومدى مُوافقتهم عليها.

أدوات الدراسة

حيث اعتمدت الدراسة على استخدام منهجية دلفاي، وذلك بهدف إعداد قائمة بأهم المتطلبات المستقبلية اللازمة لبناء ثقافة الأمن السيبراني لدى الطلبة، وذلك من خلال إجماع آراء الخبراء حول بنود الاستبانات المتتابعة. وهذه المتطلبات نابعة من خبرة وممارسة أساتذة متخصصين في تطوير التعليم الجامعي، واشتملت الدراسة الحالية على جولتين، وكل جولة تتضمن استبانة، وتم تطبيق الاستبيانات على مجموعة من الخبراء لتُحقق في مجملها هدف الدراسة، وعلى النحو الآتي:

1- **استبانة الجولة الأولى:**

تم تصميم الأداة الخاص بالجولة الأولى في صورة استبانة استنتاجية مفتوحة تتضمن العنصر الفكري والعنصر النظري والعنصر التكنولوجي. وبعد ذلك تم تنظيم وترتيب البيانات الواردة في الاستبانة وتحليلها إحصائيًا.

بعد ذلك تم عرض نتائج الاستبانة الأولى على مجموعة الخبراء أنفسهم كتغذية راجعة، والطلب من الخبراء مراجعة استجاباتهم في الجولة الأولى بناء على معرفتهم بالنتائج الإحصائية للجولة ككل، وجاءت تعديلات المحكمين بضرورة إضافة العنصر التشريعي.

وبعد إجراء التعديلات السابقة الذكر أصبحت الاستبانة نهائية وجاهزة للتطبيق في الجولة الأولى من جولات دلفاي وتتضمن العنصر الفكري (امتلاك الإدارة الرؤية حول أهمية الثقافة السيبرانية وتوفير الاستراتيجيات والخطط التي تحققها). والعنصر النظري (نظريات التعلّم والتعليم التقني والأساليب التقنية الحديثة). والعنصر التكنولوجي (الأجهزة والمعدات التقنية والحواسيب والمختبرات). والعنصر التشريعي (اللوائح والمعايير والتشريعات المحلية والعالمية في مواضيع الأمن السيبراني).

2- <u>استبانة الجولة الثانية:</u>

تمت صياغة الجولة الثانية من جولات دلفي في ضوء ما أسفرت عنه نتائج الجولة الأولى من معلومات أولية تخص الرؤية الاستشرافية للمتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى الطلبة ، والهدف من هذه الجولة هو الوصول الى اتفاق مبدئي بشأنها من جميع الخبراء، وتُتاح الفرصة لكل خبير للإطلاع على جميع الآراء السابقة، و الإدلاء برأيه حول مدى أهمية إدراج المفردات الخاصة بكل عنصر و ذلك من خلال اختيار أحد الاحتمالات الآتية: (عالية الأهمية- متوسطة الأهمية- منخفضة الأهمية)، و تم عرض الاستبانة على مجموعة من المحكمين لتحكيم استبانة الجولة الثانية، وبناءً على آرائهم تم تعديل صياغة بعض العبارات من الناحية اللغوية وإضافة عناصر فرعية تتبع لكل عنصر رئيسي، وأمكن بذلك صياغة الصورة النهائية لأهم مُفردات الرؤية المستقبلية للمتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى الطلبة.

النتائج

بعد استقصاء آراء الخبراء تم الخروج بالمتطلبات الآتية بعد اتفاقهم عليها.

<u>المتطلبات اللازمة للعنصر الفكري:</u> ويتمثل بالآتي:

- تعزيز ثقافة استخدام التكنولوجيا والتقنية الحديثة بين الطلبة، ومتابعة هذا الاستخدام ضمن ما توفره الجامعة من معدات وأجهزة تقنية وبرامج أمن وحماية لتحصين وحماية هذا الاستخدام من أي تهديد أو اختراق غير مصرّح به.

- دعم دور الجامعات المتمثل في الإدارة العليا وأعضاء هيئة التدريس والقوى العاملة فيها بتفعيل ثقافة الأمن السيبراني وتوضيح آلياته وتعزيز قيم وأفكار الثقافة السيبرانية، وذلك بتنظيم البرامج التدريبية وورش العمل التدريبية المخصصة والمعدّة بتوجيه من خبراء ومختصي المجال السيبراني الواسع ليحقق الدور التربوي أهدافه.
- تشجيع الطلبة على ممارسة التكنولوجيا ضمن مجالات سيبرانية آمنة، باستحداث التخصصات التقنية والسيبرانية والتخصصات العابرة للتعليم التقليدي بحيث تواكب هذه التخصصات متطلبات العصر وتطلعات الطلبة.
- التطوير المستمر للمناهج والمساقات الدراسية على مستوى الكليات جميعها بحيث يتوفر فيها ثقافة التعليم التكنولوجي بجودة تواكب تطورات الميادين التعليمية الحديثة.
- تعزيز دور البحث العلمي بدعم ثقافة الإبداع والابتكار في الميادين التعليمية التقنية الحديثة وربط المؤسسات المجتمعية بالجامعات ومخرجاتها ضمن خطة تنموية تعاونية تجعل المجتمع أيضاً داعم لثقافة التعليم التكنولوجي والتعليم السيبراني.

المتطلبات اللازمة للعنصر التكنولوجي: ويتمثل بالآتي:

- تدعيم البنية التحتية التكنولوجية وذلك بتوفير شبكة انترنت موثوقة وآمنة وذات سرعة عالية في الحرم الجامعي.
- تزويد مختبرات الجامعة وقاعاتها بمعدات وأجهزة تكنولوجية حديثة ومتطورة تخدم الطلبة وأعضاء هيئة التدريس والقوى العاملة بما يلائم متطلباتهم، وتكون قادرة على استيعاب وتفعيل برامج الحماية والآمان التي يتطلبها الأمن السيبراني.
- توطيد التعاون مع منصات تعليمية ذكية وسهلة الفهم والاستخدام بالنسبة للطلبة وتعمل على توفير أنماط متنوعة وحديثة من التعليم في ظل فضاء سيبراني متسع.
- تنمية مهارات وقدرات القوى العاملة في الجامعة، وذلك بتدريب مستمر ومتطور للاستثمار الفعّال في تقنيات وآليات ووسائل التكنولوجيا الحديثة، لمنع أي اختراق أو انتهاك عند استخدامها.
- تحفيز الكوادر البشرية على تفعيل برامج الحماية والآمان على الأجهزة والمعدات المستخدمة داخل الحرم الجامعي لتأمين وحماية البيانات والمعلومات الشخصية والإدارية والعلمية وضمان جودة الممارسات الإلكترونية المتاحة عليها.

- التوعية بمفهوم وأسس وآليات الأمن السيبراني والحرص على تبادل الممارسات والسلوكيات الإلكترونية الأفضل مع مختصي هذا المجال.
- تصميم منصات تعليمية تفاعلية وذكية سهلة الاستخدام، تُلبي تطلعات وحاجات الطلبة وأعضاء هيئة التدريس وتواكب التطور التقني المعاصر.
- تمكين أعضاء هيئة التدريس من دمج الأساليب التكنولوجية الحديثة في المساقات التدريسية ومشاركة الطلبة نماذج التعليم الرقمي الآمن والمحمي لضمان تحقيق هدف الأمن السيبراني في نوعية التعليم وجودته.
- استمرار الرقابة والتقييم للاستراتيجيات والأساليب والوسائل المستخدمة في منظومة الأمن السيبراني في ضوء تطبيق التعليم المعاصر ودمج التقنية بالمساقات الجامعية.
- استمرار التحسين والصيانة للأجهزة والمعدات المستخدمة في منظومة الأمن السيبراني داخل الحرم الجامعي ومختبراته لضمان بيئة سيبرانية آمنة.
- تعزيز مفاهيم التعّلم الذكي والمتقدم في ظل فضاء سيبراني متسع وممتد، وفق بيئة سيبرانية محمية وآمنة من الجرائم والتهديدات الإلكترونية للسعي نحو تحقيق النتائج الأمثل في تعليم جامعي متقدم.

المتطلبات اللازمة للعنصر التشريعي: ويتمثل بالآتي:

- اعتماد سياق أو حقل تشريعي يشتمل مجموعة من اللوائح والقوانين المنظمة والموضحة والداعمة في تفعيل منظومة الأمن السيبراني، وتحديد أشكال وأنماط الولوج للفضاء السيبراني ضمن مرافق ومختبرات الحرم الجامعي يتناعم مع التشريعات والسياسات السيبرانية الوطنية والعالمية.
- توضيح رؤية الجامعة وأهدافها من تعزيز ثقافة الأمن السيبراني والتوعية بها، وانعكاسات هذه الرؤية على جودة ونتاجات التعليم الجامعي.
- توثيق حجم تفعيل الأمن السيبراني في كل مساق أكاديمي من مساقات التعليم الجامعي على أن يُراعى طبيعة التخصص والمساقات والاحتياجات التعليمية والهدف المتوقع منها.
- تحديد أشكال التعلم الجديد وأنماطه في ضوء ثورة معرفية تقنية متسارعة يشملها فضاء سيبراني ممتد، وتوفر منصات تعليمية الكترونية ذكية تتطلب مهارات تقنية تلاءم هذا التعليم وتعزز مفهوم الأمن السيبراني.

- العمل على إعادة الهيكلة للعديد من خطط المواد للمساقات الدراسية والبرامج الأكاديمية المختلفة، بما يتوافق مع نمط التعليم المعاصر وطبيعة التخصص والمتطلبات الإجبارية والاختيارية لكل منها.
- تعزيز أفضل الممارسات الإلكترونية الأخلاقية لدى الطلبة وأعضاء هيئة التدريس والقوى العاملة في منظومة الأمن السيبراني داخل الحرم الجامعي.
- التوعية بالاستخدام الأفضل والمواءم للضوابط والمعايير والتشريعات السيبرانية التي نصت عليها رؤية الجامعة في مجال التعليم الجامعي ضمن منظومة الأمن السيبراني.

المتطلبات اللازمة للعنصر النظري:

- توفير مدخلات قائمة على النظريات المعرفية، والتي تبحث في دمج التقنية بالتعليم الجامعي وفق ما يلاءم كل تخصص ومتطلباته الإجبارية والاختيارية وخطة المواد لكل تخصص، بالإعتماد على المفاهيم والأسس والاثباتات ذات المراجع العلمية.
- تعزيز مصادر التعلّم والتقنيات التي تهدف لتعلّم جامعي تقني آمن، وفق تفعيل أمن سيبراني بالمفاهيم والآليات والوسائل والأدوات التي يعتمد عليها.
- تمكين العنصر البشري من وسائل وأساليب منظومة الأمن السيبراني المفعلّة في الحرم الجامعي، حيث أن العنصر البشري هو الركن الأول في الفضاء السيبراني ومسبب رئيس في التهديدات والهجمات الإلكترونية.
- ضرورة توظيف المعارف والنظريات العلمية والتقنية ودمجها في قطاع التعليم الجامعي بما يتوافق مع مجال الأمن السيبراني.
- تحفيز مهارات التفكير الابداعي والقدرة على تحليل المشكلات وتقديم الحلول الفنية المبتكرة وفق منظومة الأمن السيبراني في قطاع التعليم الجامعي.
- تكييف مفهوم الأمن السيبراني وما يشتمله من وسائل وآليات وأدوات بما يتلاءم مع التعليم الجامعي واستخدام الفهم والمعرفة السيبرانية ومجموعة ممارساتها لتسهيل نقلها للطلبة والقوى البشرية العاملة في الجامعة.

المناقشة والتوصيات

في ضوء نتائج الدراسة يوصي الباحثان بما يلي:

1- تبني المتطلبات اللازمة لبناء ثقافة الأمن السيبراني لدى الطلبة من قبل الجهات الممعنية وذات العلاقة.

2- اعتماد الجامعات الأردنية الحكومية الرسمية والخاصة آليات ووسائل لتفعيل ثقافة الأمن السيبراني والتوعية به، وحماية أنظمة المعلومات فيها من أي انتهاكات أو تهديدات الكترونية.

3- قيام الجامعات الأردنية بعقد الدورات التدريبية لطلبة الجامعات من أجل بناء ثقافة الأمن السيبراني وتوعيتهم بمفهومه ومجالاته.

المراجع

المراجع العربيّة

- توفيق، صلاح ومرسي، شيرين (2023) متطلبات تحقيق الأمن السيبراني بالجامعات المصرية فى ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس (جامعة بنها أنموذجاً)، **المجلة التربوية لكلية التربية** بسوهاج، 2 (105عدد يناير)، 738 – 864.
- شلوش، نوره (2018). القرصنة الالكترونية في الفضاء السيبراني: التهديد المتصاعد بأمن الدول، **مجلة مركز بابل للدراسات الإنسانية**، 8(2)، 185-206.
- العمارات، فارس والحمامصة إبراهيم محمد (2022). **الأمن السيبراني (المفهوم وتحيات العصر)**، دار الخليج للنشر والتوزيع، عمان: الأردن.
- فرجاني، علي. (2023). **اقتصاد الانتباه في عصر المراقبة السيبرانية بالتطبيق على علم النفس الاجتماعي**. الجيزة، مصر: دار بدائل للطبع والنشر والتوزيع.
- القحطاني، نورة (2019). مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي، **مجلة شؤون اجتماعية**، 36 (144)، 85 – 120.
- كاعوه، عبير (2020). سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية، **مجلة دراسات تربوية واجتماعية**، جامعة حلوان، 3 (يونيو 2020)، 134 – 200.
- المركز الوطني للأمن السيبراني، تم استرجاعه من الموقع : https://ncsc.jo/Default/Ar، 2025/2/20.

- المنيع، الجوهرة بنت عبد الرحمن (2022). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030، **المجلة العلمية لكلية التربية**، جامعة أسيوط، 38(1)، 156-194.

ثانياً: المراجع الأجنبيّة

- Leung, R. (2018). **Cyber Security Regulation in the Banking Sector". Global Emerging Themes**. Master's Thesis, The London School of Economic and Political Science.
- Njoku, I & Njoku, B & Chukwu, S & Ravichandran, R. (2023). Fostering Cybersecurity in Institutional Repositories: A Case of Nigerian Universities. **Afr. J. Lib. Arch. & Inf. Sc**. 33(1) .April 2023. 1-21.
- Towhidi, G & Pridmore, J. (2023). Aligning Cybersecurity in Higher Education with Industry Needs. **Journal of Information Systems Education,** 34(1), pp70-83, winter 2023.
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Çetin, F., & Basım, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems. 62(1),82-97.