تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية (تصور مقترح)

إعداد

د/أسماء مراد صالح مراد زيدان

أستاذ مساعد بقسم أصول التربية كلية الدراسات العليا للتربية – جامعة القاهرة

ملخص الدراسة باللغة العربية:

هدفت الدراسة إلى الوقوف على الإطار المفاهيمي للتربية الاعلامية الرقمية بالجامعات، وتحديد أهم كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الأمن السيبراني، والكشف عن الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية، وأساليب تنميتها. ووضع تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية. اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات. تكونت عينة الدراسة من (٣٤٧) طالبًا من كليات (التربية، التجارة وإدارة الأعمال، السياحة والفنادق) جامعة حلوان، وتوصلت الدراسة إلى عدة نتائج من أهمها:

- ضعف تركيز اللوائح والقوانين الجامعية على قضايا وممارسات الأمن السيبراني بالجامعات، مما يعرض الأنظمة والشبكات الجامعية لخطر الاختراق والهجمات السيبرانية.
- نقص المتخصصين في مجال الأمن السيبراني في الجامعات، مما يصعب تنفيذ استراتيجيات الأمن السيبراني بشكل فعال.
- ضعف وعي الطلاب بكيفية استخدام شبكات الإنترنت العامة بشكل آمن ومشفر لحماية بياناتهم الحساسة من الاختراق والسرقة، مما يعرضهم لخطر سرقة الهوية الرقمية واختراق حسابات البريد الإلكتروني والشبكات الاجتماعية والاحتيال الإلكتروني.
- نقص البرامج التعليمية والتدريبية المتخصصة في مجال الأمن السيبراني، مما يؤثر سلبًا على قدرة الطلاب على اكتساب المهارات والممارسات الآمنة في استخدام التكنولوجيا الرقمية.
- ضعف وعي الطلاب بأهمية استخدام كلمات مرور قوية وتغييرها بشكل منتظم لتأمين حساباتهم الشخصية والبيانات الحساسة من التهديدات السيبرانية والاختراقات.
- إغفال بعض الطلاب إجراءات تحديث البرامج والتطبيقات الضرورية لمعالجة الثغرات الأمنية، مما يجعلهم عرضة للهجمات الالكترونية التي تستهدف النسخ غير المحدثة.

الكلمات المفتاحية: الأمن السيبراني، كفايات، التربية الإعلامية الرقمية.

Developing Cybersecurity Culture for Helwan University Students in Light of Digital Media Education Competencies

(A Suggested Proposal)

Dr. Asmaa Mourad Saleh Mourad Zeidan

Assistant Professor at Foundations of Education Department

Faculty of Graduate Studies for Education - Cairo University

Abstract

The study aimed to identify the conceptual framework of digital media education in universities, identify the most important digital media education competencies necessary for university students to develop cybersecurity culture, and reveal the current reality of cybersecurity culture for Helwan University students in light of digital media education competencies and their development methods. Also, a suggested proposal was provided to develop cybersecurity culture for Helwan University students in light of digital media education competencies. The study followed the descriptive approach and used a questionnaire as a tool for collecting data. The study sample consisted of (347) students from the faculties of (Education, Commerce and Business Administration, Tourism and Hotels) at Helwan University. The study revealed several results, perhaps the most important of which were:

- Weak focus of university regulations and laws on cybersecurity issues and practices at universities, which exposes university systems and networks to the risk of hacking and cyberattacks.`

- Lack of specialists in the field of cybersecurity in universities, which makes it difficult to implement cybersecurity strategies effectively.
- Students' poor awareness of how to use public Internet networks in a secure and encrypted manner to protect their sensitive data from hacking and theft, which exposes them to the risk of digital identity theft, hacking of email accounts and social networks, and electronic fraud.
- Lack of specialized educational and training programs in the field of cybersecurity, which negatively affects students' ability to acquire skills and safe practices in using digital technology.
- Students' poor awareness of the importance of using strong passwords and changing them regularly to secure their personal accounts and sensitive data from cyber threats and hacks.
- Some students neglect the procedures for updating programs and applications necessary to address security vulnerabilities. This makes them vulnerable to electronic attacks targeting out-of-date versions.

Key words: Cybersecurity - Competencies- Digital Media Education

تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية (تصور مقترح)

أحدثت الثورة التكنولوجية تحولًا جذريًا في كافة مجالات الاتصالات والمعلومات، مما أدى إلى تغيرات هائلة في تفاعل الجمهور مع المضامين الإعلامية. بات الجمهور اليوم أكثر تفاعلًا وتشاركًا، حيث يمتلك القدرة على الوصول إلى مجموعة ضخمة من المعلومات والتواصل مع الآخرين بسهولة وسرعة. ومع هذا التفاعل المتزايد، تنبعث إشكالية جديدة تواجه المهتمين بالشأن الاجتماعي والتربوي تتمثل في كيفية التعامل مع هذا الواقع الجديد. فعلى الرغم من المزايا التي توفرها التكنولوجيا، إلا أنها تأتي أيضًا بتحديات جديدة تتطلب مهارات ومعرفة للتعامل معها بطريقة بناءة.

انتشرت مؤخرًا نوعية خطيرة من الهجمات والجرائم السيبرانية تعتمد علي تقنيات متقدمة كالحوسبة السحابية والذكاء الاصطناعي وانترنت الاشياء، وبرمجيات لفك شفرة ولاختراق لأنظمة الشبكات والحاسبات وقواعد البيانات، وبرمجيات لتشفير العمليات المشبوهة، وبرمجيات خبيثة لاختراق أنظمة أمن الشبكات والحاسبات لتسخيرها في القيام بعمليات اجرامية وتعاملات مشبوهة دون علم أصحابها فيما يسمي بالشبكات الآلية، حيث يمكن أن تضم شبكة آلية واحدة عشرات أو مئات الألاف أو ملايين من الحواسب أو الأجهزة المتصلة بالإنترنت (انترنت الأشياء) التي يمكن استخدامها لشن هجمات متنوعة، مثل الهجمات الموزعة لإعاقة الخدمات علي شبكات ومواقع مستهدفة لأغراض اجرامية كالتخريب والإرهاب والتهديد والترهيب والابتزاز (المجلس الأعلى للأمن السيبراني،٢٠١٧، ٥).

إن استخدام التقنية دون وعيٍ بشكلٍ غير آمنٍ في ظل غياب المسؤولية تجاه الآخرين، ومع غياب القوانين والعقوبات الرادعة وانتشار ضعاف النفوس يؤدي إلى التزايد المستمر في نسب الجريمة الإلكترونية، والتي تشكَّل خطرًا حقيقيًا على المجتمعات وتهدد أفراده؛ حيث ظهر تهديدٌ جديدٌ لمستخدمي شبكة الإنترنت، واتجه بعض الأشخاص لاختراق شبكة الإنترنت والتلاعب بالمعلومات وإيذاء المستخدمين بصور وأساليب متعددة، وذلك فيما يُعرف بالجريمة السيبرانيّة (الشهري، ٢٠٢١، ٨٤).

وانطلاقًا من الدور الاكبر الذي يقع على إدارة الجامعة في استيعابها لآليات العصر وتقنياته وقدرتها على مواجهة التحديات والمُتغيرات وتطويعها، وأن الطلاب هم أهم مكون مستهدفٍ داخل المؤسسة الجامعية والأكثر إقبالًا على استخدام التقنيات الحديثة، كانت الحاجة ملحةً لتعزيز الأمن السيبرانيّ لدى الطلاب، وتوعيتهم بالتعامل الآمن مع العالم الرقمي؛ لضمان ممارسات رقمية وفكرية سليمة، فضلًا عن منحهم أعلى الدرجات العلمية والأكاديمية.

وإذا كان للإعلام الرقمي الفضل في التنوير ونشر الحقائق والمعلومات من خلال إيصال المعلومة والخبر للجماهير في وقت قياسي عندما يتعلق الأمر بما ينفع الطلاب، فإن التحدي الأساسي يكمن في التضليل الذي يخلقه الاعلام الرقمي غير المسؤول، وفي المعلومات المضللة التي ينشرها وتخلق كثيرًا من التفاعل السلبي مع المنشورات المكتوبة أو الفيديوهات السمعية البصرية (سهمي، ٢٠٢٠، ١٢٨).

ونتيجة لتلك المخاطر المرتبطة بعمليات نشر وتداول المحتوى الرقمي الزائف، سعت بعض الدول لفرض عدة قوانين تسهم في الحد من انتشار هذا المحتوى، والذي قد يتسبب في إثارة الفتن وزعزعة الاستقرار الداخلي وتهديد الأمن الاقتصادي، إلا أن السياق الكبير لوسائل التواصل الاجتماعي، وعدم قدرة الدول على محاصرة ما بهذه الوسائل من محتوى رقمي زائف؛ نتيجة لتوظيف خوارزميات الذكاء الاصطناعي في بث آلاف الأخبار عبر الحسابات الوهمية والدعاية المبرمجة، جعل من الخيار القانوني المُشار إليه أداة يصعب تطبيقها لحل تلك المشكلة الشائكة. (مكاوي، وآخرون، ٢٠٢١، ٥٢٩).

إن خط الدفاع الأمثل ضد الغزو الاعلامي الرقمي هو تنمية المهارات المناسبة للطلاب من أجل فهم آليات عمل الاعلام التقليدي (الاذاعة والتلفزيون) والحديث (الهاتف المحمول، الاجهزة اللوحية وشبكات التواصل الاجتماعي) وتمكين الطلاب من التعامل معها بشكل يستخلص الجوانب الايجابية ويتجنب تأثيراتها السلبية، وهذه الأدوات والمهارات هي ما اصطلح عليه التربية الاعلامية الرقمية حيث يرتبط مسارها بشكل وثيق ومباشر بمسارات وسائل الاتصال والاعلام ذاتها (الطعاني، ٢٠٢٠، ١١)

وتأسيسًا على التطورات الجديدة في العالم الرقمي، فإن التربية الاعلامية تجد نفسها اليوم مطالبة بتطوير أدائها التربوي في هذا الفضاء الرقمي الجديد، وقد ترتب عليها في هذا المسار تضمين المهارات الجديدة، والمعارف النوعية المتطورة، في مناهجها والقيام بدمج مختلف أشكال التكنولوجيا الرقمية الجديدة في فعالياتها التربوية ضمن الفضاء الإعلامي الرقمي اللامتناهي (وطفة، ٢٠١٩، ١١١).

وأشارت دراسة موتونهو، وآخرون Mutunhu, et al., (٢٠٢٢) إلى أن طلاب الجامعات هدفًا لهجمات التصيد الاحتيالي بمعدلات عالية بشكل متزايد بسبب مقدار الوقت الذي يقضونه على الإنترنت. حيث يقضي الطلاب الكثير من الوقت في استخدام الإنترنت للبحث والتواصل مع الطلاب الآخرين والمشاركة في الأنشطة التدريسية. وأكدت دراسة القحطاني Alqahtani (٢٠٢٢) أن إعداد برامج للتوعية الأمنية يُعد إحدى المراحل الأساسية في زيادة الأمن السيبراني.

في ضوء العرض السابق يتضح أن التطور التكنولوجي الهائل يشكل آفاقًا جديدة للثغرات الأمنية والتهديدات السيبرانية الأمر الذي يتطلب تعزيز ثقافة الأمن السيبراني

وزيادة الوعي بالمخاطر السيبرانية لطلاب الجامعات في ضوء كفايات التربية الإعلامية الرقمية وذلك ما تسعى الدراسة إلى تحقيقه.

الدراسات السابقة

يتناول الجزء التالي عرض وتحليل بعض الدراسات السابقة من الأحدث للأقدم ويتم تصنيفها إلى محورين على النحو التالي:

١. الدراسات المرتبطة بالأمن السيبراني والجامعات

٢. الدراسات المرتبطة بالتربية الإعلامية الرقمية والجامعات

المحور الأول: الدراسات المرتبطة بالأمن السيبراني والجامعات

هدفت دراسة **(المحيميد، ٢٠٢٣)** تعرف دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية بالمملكة العربية السعودية، والكشف عن صعوبات تحقيقه. اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات. وتوصلت إلى أن دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبرانيِّ جاء بدرجة مرتفعة، وتمثلت أهم الأدوار في حث منسوبي الجامعة على ضرورة تسجيل الخروج من جميع الحسابات الإلكترونية قبل المغادرة، كما أن صعوبات تحقيق الأمن السيبراني في الجامعة جاءت بدرجة متوسطة، نظرًا للتحديات المتعددة التي تواجهها في بيئة العمل. ومن أبرز تلك الصعوبات ما يلي: ضعف قدرتها على استقطاب كفاءة بشرية مؤهلة لدعم بيئة الأمن السيبراني؛ خاصة في ظل نقص الأدوات التقنية الحديثة اللازمة لتوفير بيئة أمنية مثالية للمعلومات، ضعف نشر ثقافة الأمن السيبراني بين المنسوبين، وقلة المعرفة بالآليات اللازمة لتفعيل الأمن السيبراني. بالإضافة إلى صعوبة توفير برامج تدريبية حديثة ومتطورة نظرًا لارتفاع تكلفتها وعدم وجود متخصصين لإدارتها. كما أن الصلاحيات المناسبة للوصول إلى المعلومات السرية المتعلقة بأنشطة الجامعة غير متاحة إلا لعدد محدود من المنسوبين.

وفي نفس الصدد جاءت دراسة **(الركبان، ٢٠٢٣)** بهدف تعرف واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام حمد بن سعود الإسلامية بالمملكة العربية السعودية، والكشف عن المعوقات التي تحد من تحقيقه، اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات. وتوصلت إلى عدة نتائج منها: قلة الدورات التدريبية لتوعية منسوبي الجامعة بضرورة تحقيق الأمن السيبراني، ضعف إدراك بعض منسوبي الجامعة أهمية اختيار كلمات مرور قوية لحساباتهم الرسمية، بحيث يصعب اختراقها والوصول إليها على الرغم من توجيه الجامعة باستمرار منسوبيها إلى

اختيار كلمات مرور قوية. تدني مستوى الخبرة لدى الموظفين، واستخدام الأجهزة الشخصية لنقل أو تخزين معلومات سرية خاصة بالجامعة.

وللكشف عن معوقات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي جاءت دراسة **(توفيق ومرسي، ٢٠٢٣)** اتبعت الدراسة المنهج الوصفي. وتوصلت إلى عدة نتائج منها: غياب التطبيق الفعلي للتشريعات والقوانين الرادعة لمرتكبي الجرائم الإلكترونية، ضعف الوعي بقانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م والذي يعد من أحدث التشريعات الوطنية المصرية في حماية جرائم تقنيات المعلومات، وذلك لاشتماله على العديد من صور الجرائم التي تتم في بيئة الإنترنت والنص على العقوبات التي تقع على مرتكبي مثل هذه الجرائم، تدني مستوى الخبرة لدى الموظفين، واستخدام الأجهزة الشخصية مثل الهاتف المحمول لتخزين أو نقل معلومات سرية خاصة بالجامعة، قلة الدورات التدريبية المنعقدة لأعضاء هيئة التدريس في مجال الأمن السيبراني، ضعف استخدام برامج حماية أصلية موثوقة والاعتماد على استخدام البرامج غير الأصلية.

هدفت دراسة **(Mutunhu, et al.,2022)** إلى تحديد المستويات الحالية للوعي بالأمن السيبراني بين الطلاب والموظفين بالجامعة الوطنية للعلوم والتكنولوجيا في زيمبابوي، واقتراح إطار عمل لإجراء برامج التوعية والتثقيف في مجال الأمن السيبراني. اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات، وتوصلت الدراسة إلى أن الطلاب والموظفين في الجامعات لديهم نقص في المعرفة والفهم المطلوبين لأهمية مبادئ الأمن السيبراني، وتطبيقها العملي في أنشطتهم اليومية، وليس لديهم دراية كافية بها وبكيفية حماية بياناتهم.

أما دراسة (Azzeh, et al., 2022) فهدفت إلى الوقوف على تأثير تبني مفاهيم الأمن السيبراني على منهج تكنولوجيا المعلومات وتحدد التأثير المحتمل على معرفة طلاب جامعة العلوم التطبيقية الخاصة في الأردن بممارسات الأمن السيبراني ومستوى الوعي لديهم، أجريت دراسة تجريبية أولًا لقياس المستوى الحالي للوعي بالأمن السيبراني وما يفعلونه لحماية أنفسهم من الهجمات الإلكترونية. أشارت النتائج إلى أن الطلاب ليس لديهم معرفة كبيرة بالأمن السيبراني وأن المؤسسات التعليمية لا تتعامل بنشاط مع الوعي بالأمن السيبراني بين الطلاب، وأن تضمين موضوعات الأمن السيبراني المهمة في دورات علوم الكمبيوتر الأخرى يمكن أن يزيد وعي الطلاب ومعرفتهم فيما يتعلق بمفاهيم الأمن السيبراني.

وجاءت **دراسة (Alzahrani, 2022)** بهدف فحص وتحليل قضايا الأمن السيبراني، بما في ذلك المخاطر الإلكترونية، والأمن السيبراني، والوعي بالأمن السيبراني، والثقة

الإلكترونية بين طلاب التعليم العالي في المملكة العربية السعودية. اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات، وتوصلت الدراسة إلى عدة نتائج لعل من أهمها: نقص الوعي بالمعلومات الأساسية المتعلقة بالأمن السيبراني بين الطلاب السعوديين.

ولتحديد مستوى الوعى بالأمن السيبراني للطلاب في شمال شرق نيجيريا **جاءت دراسة (Adamu, et al.,2022)** اتبعت الدراسة المنهج الوصفي لجمع البيانات حول العناصر المطلوبة لتحديد مستوى الوعي بالأمن السيبراني وهي التنمر الإلكتروني والمعلومات الشخصية والخدمات المصرفية عبر الإنترنت وإدمان الإنترنت والحماية الذاتية واستخدمت الاستبانة كأداة لجمع البيانات. وتوصلت الدراسة إلى أن الطلاب الذين شملهم الاستطلاع أظهروا مستوى عالٍ من الوعي بالأمن السيبراني لبعض العناصر، وتشمل هذه العناصر الخدمات المصرفية عبر الإنترنت، في حين أن العناصر الأخرى مثل التنمر الإلكتروني والحماية الذاتية وإدمان الإنترنت جاءت بدرجه متوسطة مما يعكس وجود حاجة ملحة لتنفيذ خطة جيدة لبرامج التوعية بالأمن السيبراني لمعالجة هذه المشكلات حتى لا يقع الطلاب ضحية للهجمات الإلكترونية خاصة الطالبات.

وجاءت دراسة **(الحبيب، ٢٠٢٢)** بهدف تعرف درجة الوعي بمفاهيم الأمن السيبراني لدى طلاب وطالبات الدراسات العليا بكلية التربية بجامعة الامام محمد بن سعود الإسلامية بالمملكة العربية السعودية، اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات، وتوصلت الدراسة إلى عدة نتائج لعل من أبرزها نقص وعي الطلاب بجرائم الأمن السيبراني، مما يشير لأهمية الاطلاع الواسع على جرائم الأمن السيبراني بأنواعه المتعددة وأشكاله المتجددة لعدم الوقوع ضحية لتلك الجرائم.

وهدفت **دراسة (Onyema, et al., 2021)** إلى الوقوف على مستوى الوعي بالأمن السيبراني بين طلاب المرحلة الجامعية الأولى من أربع مؤسسات جامعية مختارة في إينوجو، نيجيريا. اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات. وتوصلت الدراسة إلى أن مشاركة الطلاب العالية تزيد من اهتمام الطلاب بالأمن السيبراني. ومن ثم، فإن زيادة مشاركة الطلاب في قضايا الأمن السيبراني من شأنها أن تعزز مهاراتهم الإلكترونية حول الحواجز التي تعيق الوعي بالأمن السيبراني أو التعليم بين الطلاب الجامعيين، نقص الموظفين المدربين (المواهب الإلكترونية)، ونقص البنى التحتية الداعمة، والقيود الزمنية، واستبعاد الأمن السيبراني في الدورات غير الحاسوبية، وضعف المعرفة بمجالات الحوسبة الأساسية، ونقص الموجهين ذوي الخبرة العملية، ونقص التدريب السيبراني.

هدفت **دراسة (الشهري، ٢٠٢١)** إلى تعرف دور إدارة الجامعة في تعزيزِ الوعي بالأمنِ السيبرانيّ لدى طلبةِ كليةِ التربية بجامعة الإمَام محمد بن سعود الإسلامية بالمملكة العربية السعودية، والكشف عن درجة معرفة طلاب كلية التربية في جامعة الإمَام محمد بن سعود الإسلامية بالأمن السيبرانيّ، اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات، وأشارت نتائج الدِّرَاسَة إلى أن معرفة طلبة كلية التربية في جَامِعَة الإمَام محمد بن سعود الإسلامية بالأمن السيبرانيّ جاءت بدرجة متوسطة، وأن ممارسة إدارة الجامعة لدورها في تعزيز الوعي بالأمن السيبرانيّ لدى هؤلاء الطلاب جاءت بدرجةٍ متوسطة.

وجاءت دراسة (الكردي، ٢٠٢١) للوقوف على واقع الأمن السيبراني والتعليم الإلكتروني في جامعات فلسطين من وجهة نظر أعضاء الهيئات التدريسية – جامعة النجاح الوطنية انموذجًا، وتحديد التحديات المحتملة التي يمكن أن تواجه أعضاء هيئات التدريس في هذا السياق، اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات، وتوصلت الدراسة إلى عدة نتائج لعل من أهمها: وجود فروق دالة إحصائيا في استخدام التعليم الإلكتروني في كليات التربية الرياضية مما يشير إلى اختلافات ملحوظة في التطبيق واستخدام للتكنولوجيا في عملية التعليم الإلكتروني. وفيما يتعلق بتحديات استخدام التعليم الإلكتروني تم تحديد صعوبة التكيف مع منصات التعليم الإلكتروني، بالإضافة إلى نقص المهارات التقنية اللازمة لتنفيذ التعليم الإلكتروني بكفاءة، ضعف جودة التعليم وفعاليته في البيئة الافتراضية، وتحديات تنظيم الوقت والإدارة الفعالة للموارد التعليمية الإلكترونية.

المحور الثاني: الدراسات المرتبطة بالتربية الإعلامية الرقمية والجامعات

جاءت دراسة (رجب وآخرون، ٢٠٢٣) بهدف تعرف فعالية برنامج مقترح في التربية الإعلامية الرقمية لتنمية الوعي المعرفي بالخصوصية الرقمية لطلاب جامعة المنيا. اتبعت الدراسة المنهج شبة التجريبي. وتوصلت إلى عدة نتائج منها: برنامج التربية الإعلامية الرقمية المقترح كان فعالًا في زيادة مستوى الوعي المعرفي بالخصوصية الرقمية لدى طلبة الجامعة، وتجلى ذلك في زيادة المعرفة بالمفاهيم والمخاطر المرتبطة بالخصوصية الرقمية وتطوير مهارات الحماية الشخصية.

وجاءت دراسة **(غندر، ٢٠٢٣)** بهدف الكشف عن استجابة طلاب الإعلام التربوي بكليات التربية النوعية بجامعات (بورسعيد، القاهرة، عين شمس، المنصورة) للأخبار الزائفة بمواقع التواصل الاجتماعي وعلاقتها بمهارات التربية الإعلامية الرقمية لديهم، اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات. وتوصلت إلى عده نتائج من أهمها: تمثلت أهم الأنشطة التفاعلية في مواجهة الأخبار الزائفة على مواقع

التواصل الاجتماعي في البحث عن معلومات ذات صلة بالأخبار على محركات البحث في المقدمة، ثم قراءة الخبر الزائف فقط حيث يتبع الطلاب نهجًا نشطًا في التعامل مع الأخبار الزائفة، حيث يبحثون عن مصادر موثوقة للتحقق من صحة الأخبار قبل اتخاذ أي قرارات أو نشر المعلومات، علاوة على وجود علاقة إيجابية بين مهارات التربية الإعلامية الرقمية لدى الطلاب وقدرتهم على استجابة الأخبار الزائفة. وبالتالي، كان الطلاب الذين يمتلكون مهارات تربية إعلامية رقمية أفضل أكثر قدرة على التعرف على الأخبار الزائفة والتعامل معها بشكل فعال.

أما دراسة **(إبراهيم وآخرون، ٢٠٢٣)** فهدفت إلى إعداد برنامج في التربية الإعلامية الرقمية في ضوء بعض مهارات القرن الحادي والعشرين، استخدمت الدراسة كل من المنهج الوصفي والمنهج شبه التجريبي حيث تم إعداد مقياس لمهارات القرن الحادي والعشرين، وبرنامج في التربية الإعلامية الرقمية وتدريسه لمجموعه من طلاب الفرقة الأولى بقسم الاعلام التربوي بكلية التربية النوعية جامعة دمياط بلغ عددها (٦٠) طالبًا وطالبة، وتوصلت الدراسة إلى فاعلية برنامج التربية الإعلامية الرقمية في تنمية بعض مهارات القرن الحادي والعشرين لدى مجموعة البحث.

هدفت **دراسة (محمود، الشهري،٢٠٢١)** تعرف التربية الإعلامية الرقمية وأثرها في إشباع الاحتياجات التربوية والصحية للطلاب الصم في ظل التحديات التي تفرضها جائحة كورونا، اتبعت الدراسة المنهج الوصفي واستخدمت الاستبانة كأداة لجمع البيانات، وتوصلت إلى أن الإعاقة السمعية التي يعانى منها التلاميذ الصم لا تقف عائقًا أمام تعاملهم مع أدوات التكنولوجيا الحديثة، كما أن الطلاب الصم لديهم شغف كبير للتعامل مع التكنولوجيا الحديثة فمعظم الطلاب الصم لديهم صفحات على مواقع التواصل الاجتماعي مما يسهل عملية تدريبهم على مهارات التربية الإعلامية الرقمية.

أما دراسة (يوسف، ٢٠١٩) فهدفت إلى الوقوف على مهارات وسمات التربية الإعلامية الرقمية لدى طلاب الجامعات والعوامل التي ساعدت على اكتسابها، وأهم مقترحات الطلاب لتطوير قدراتهم الانتاجية كإحدى المهارات الأساسية للتربية الإعلامية الرقمية. استخدمت الدراسة مجموعات النقاش المركز مع عينة من طلاب كلية الاعلام بجامعة أكتوبر للعلوم الحديثة والآداب، وتوصلت إلى عدة نتائج لعل من أبرزها: أن من أهم مهارات التربية الاعلامية الرقمية: الوصول، التحليل والتقييم، الخلق للمحتوى، الانعكاس وتطبيق المسئولية الاجتماعية ثم التصرف والمبادرات.

ولتحديد الكفايات الواجب توافرها في منهج التربية الإعلامية الرقمية لتنمية مهارات النقد وتحليل المضامين الإعلامية لدى الطلاب من وجهة نظر أساتذة الجامعات العراقيين **جاءت دراسة (سالم، وحسن،٢٠١٨)**. اتبعت الدراسة المنهج الوصفي، واستخدمت

الاستبانة كأداة لجمع البيانات. وتوصلت إلى عدة نتائج لعل من أبرزها: أن تحديد الكفايات التربوية في منهج التربية الإعلامية الرقمية يتم عن طريق تعلم مهارات الاتصال وتنشيط عمليات الإبداع في الفنون الصحفية وتعلم مهارات الرصد الإعلامي، فضلًا عن ترسيخ روح المواطنة الفاعلة، وتنمية الدافع الأخلاقي الذي يعمل على تكوين طالب مثقف يستطيع التعامل مع وسائل الإعلام المختلفة.

التعقيب على الدراسات السابقة

يركز الجزء التالي على عرض لأوجه الشبه والاختلاف بين الدراسة الحالية والدراسات السابقة، وأوجه الاستفادة منها وذلك على النحو التالي:

أ- أوجه الشبه

- تتشابه الدراسة الحالية مع دراسة (Mutunhu, et al.,2022)، ودراسة (Alzahrani, 2022)، دراسة (Onyema, et al., 2021)، دراسة (الكردي، ٢٠٢١)، دراسة (الشهري، ٢٠٢١)، دراسة (محمود، الشهري،٢٠٢١) في اتباعها المنهج الوصفي واستخدامها الاستبانة كأداة لجمع البيانات.
- تتشابه الدراسة الحالية مع دراسة (Mutunhu, et al.,2022)، دراسة (Onyema, et al., 2021)، في تناولها الأمن السيبراني لطلاب الجامعات.

ب- أوجه الاختلاف

- تناولت بعض الدراسات السابقة الأمن السيبراني لطلاب الجامعات من زوايا مختلفة فركزت دراسة (Mutunhu, et al.,2022) على تحديد المستويات الحالية للوعي بالأمن السيبراني بين الطلاب والموظفين في الجامعات، أما دراسة (Alzahrani, 2022) فهدفت إلى تحليل قضايا الأمن السيبراني، بما في ذلك المخاطر الإلكترونية، والأمن السيبراني، والوعي بالأمن السيبراني، والثقة الإلكترونية بين طلاب التعليم العالي في المملكة العربية السعودية، وجاءت دراسة Adamu, et al., (٢٠٢٢) لتحديد مستوى الوعي بالأمن السيبراني للطلاب في شمال شرق نيجيريا وتختلف الدراسة الحالية مع الدراسات السابقة في تناولها تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية.
- تناولت بعض الدراسات السابقة التربية الإعلامية الرقمية في الجامعات من زوايا مختلفة فبعضها تناول مهارات وسمات التربية الإعلامية الرقمية لدى طلاب الجامعات والعوامل الى ساعدت على اكتسابها كدراسة (يوسف، ٢٠١٩)، وجاءت دراسة (سالم، وحسن،٢٠١٨) لتحديد الكفايات الواجب

توافرها في منهج التربية الإعلامية الرقمية لتنمية مهارات النقد وتحليل المضامين الإعلامية لدى الطلاب وتختلف الدراسة الحالية عن الدراسات السابقة في استخدامها كفايات التربية الإعلامية الرقمية لتنمية ثقافة الأمن السيبراني لطلاب الجامعات.

ج – أوجه الاستفادة من الدراسات السابقة:

تمثلت الاستفادة من الدراسات السابقة فيما يلي: –

- إثراء الدراسة في الإطار النظري.
- استخدام منهج الدراسة الحالية.
- تصميم وتطوير أداة الدراسة (الاستبانة).
- استخدام الأساليب الإحصائية المناسبة.
- المساعدة في تحليل وتفسير نتائج الدراسة الحالية.

مشكلة الدراسة

تعد مشكلة الجرائم الرقمية من أبرز المشكلات التي تواجه طلاب الجامعة عند تعاملهم مع معطيات العصر الرّقمي، فقد أشارت المعلومات الصادرة عن الاستراتيجية الوطنية للأمن السيبراني أنها تعاملت مع كم هائل من التحديات والأخطار السيبرانية التي تمثلت في خطر الإرهاب والحرب السيبرانية، وخطر اختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات وخطر سرق الهوية الرقمية والبيانات الخاصة (الاستراتيجية الوطنية للأمن السيبراني٢٠١٦/٢٠١٧، ٦).

وأشارت دراسة (الألفي، ٢٠٢٢) أن الجامعات المصرية تواجه تحديات سيبرانية متزايدة في الوقت الحالي، حيث يتعرض العديد من طلابها وموظفيها للهجمات السيبرانية التي تستهدف بياناتهم الشخصية والحساسة. وتشمل هذه الهجمات سرقة الهوية الرقمية، اختراق حسابات البريد الإلكتروني والشبكات الاجتماعية، والاحتيال الإلكتروني، إلى جانب الهجمات التي تستهدف الأنظمة الأساسية للجامعات مثل نظم الإدارة والتعليم الإلكتروني والمواقع الإلكترونية الرسمية.

كما أكدت نتائج دراسة على (٢٠٢٠) أن من أكثر المخاطر تتمثل في التعامل غير الواعي للطلاب مع وسائل الاعلام، انعزال الطلاب عن قضايا المجتمع، وتحفيز الميول العدوانية، وتحفيز الغرائز الجنسية، واللامبالاة السلبية، وهدم القيم الاجتماعية والدينية.

وأضافت نتائج دراسة (الألفي،٢٠٢٢)، (السيد، ٢٠٢١) مايلي:

- ممارسات الأمن السيبراني في الجامعات المصرية مازالت محدودة للغاية وقاصرة على تحقيق درجة الوقاية من الهجمات السيبرانية، وتكاد تقتصر على بعض برامج حماية البيانات والدورات التدريبية للمستفيدين.
- نقص البرامج التدريبية في مجالات الأمن السيبراني الموجهة للقيادات خاصة والموارد البشرية الجامعية عامة.
- ضعف تركيز اللوائح والقوانين الجامعية على قضايا وممارسات الأمن السيبراني بالجامعات.
- نقص عدد المتخصصين في مجال الأمن السيبراني في الجامعات، وصعوبة توفير الخبرة اللازمة لتنفيذ استراتيجيات الأمن السيبراني بشكل فعال.

وعلى الرغم من تشكيل المجلس الأعلى للأمن السيبراني بقرار من رئيس مجلس الوزراء بالعام ٢٠١٤ برئاسة وزير الاتصالات، وعضوية ممثلين عن كل من وزارات البترول، الدفاع، الداخلية، الكهرباء، الخارجية، الصحة، التموين، الموارد المائية، البنك المركزي، جهاز المخابرات العامة، إضافة إلى (٣) أعضاء من ذوي الكفاءة والخبرة (قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤). إلا أنه أغفل تمثيل وزارة التعليم العالي بممثل لها يقدم مقترحات ويبادر بالنقاشات، ويوضح ما تعانيه الجامعات من مشكلات ومعوقات تتعلق بالأمن السيبراني وممارساته بداخلها؛ مما يشير إلى مواصلة إغفال جوانب الأمن السيبراني بالجامعات على المستوى الحكومي؛ وإلى الآن مازال تشكيل هذا المجلس كما هو دون تغيير.

في ضوء العرض السابق يتبين أن الجرائم الرقمية تعد من أبرز المشكلات التي تواجه طلاب الجامعات، ومن ثم تسعى الدراسة الحالية لتنمية ثقافة الأمن السيبراني للطلاب في ضوء كفايات التربية الإعلامية الرقمية.

وتتحدد مشكلة الدراسة في السؤال الرئيس التالي: -

كيف يمكن تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية؟

ويتفرع من السؤال الرئيس الأسئلة الفرعية التالية:

١. ماهية الأمن السيبراني بالجامعات، أهدافه، أبعاده؟

٢. ما الإطار المفاهيمي للتربية الاعلامية الرقمية بالجامعات؟

٣. ما كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الأمن السيبراني، وأساليب تنميتها؟

٤. ما الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية، وأساليب تنميتها؟

٥. ما التصور المقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية؟

أهداف الدراسة

تتمثل أهداف الدراسة فيما يلي:

١. تعرف ماهية الأمن السيبراني بالجامعات، أهدافه، أبعاده.

٢. الوقوف على الإطار المفاهيمي للتربية الاعلامية الرقمية بالجامعات.

٣. تحديد كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الأمن السيبراني، وأساليب تنميتها.

٤. الكشف عن الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية، وأساليب تنميتها.

٥. وضع تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية.

أهمية الدراسة

تتمثل أهمية الدراسة في أهميتها النظرية والتطبيقية على النحو التالي: –

الأهمية النظرية

تتمثل أهمية الدراسة النظرية فيما يلي: –

١. الدور الحيويُّ للجامعات في تعزيز الوعي بالأمن السيبرانيّ، من خلال دورها في إعداد الطلاب فكريّا وعمليّا في شتى مناحي الحياة، وتزويده بالقيم والاتجاهات والمعارف والأفكار السليمة التي تمكنهم من الابتكار والتجديد ومن المساهمة في صنع المستقبل.

٢. أهمية الأمن السيبراني باعتباره يشمل جميع الجوانب التعليمية، والاجتماعية، والاقتصادية، وباعتباره ممثلًا لقدرة الدولة على حماية مصالحها في مختلف مجالات الحياة.

٣. يمكن أن تسهم الدراسة في تزويد المكتبة العربية بالمعلومات النظرية عن الامن السيبراني وكفايات التربية الإعلامية الرقمية.

الأهمية التطبيقية

تتمثل أهمية الدراسة التطبيقية فيما يلي: –

١. يمكن أن تسهم الدراسة في توعية الطلاب بأخلاقيات وقواعد السلوك الآمن على الشبكة وفى استخدام وسائل التواصل الاجتماعي.

٢. تُساعد نتائج هذه الدراسة المسئولين وأصحاب القرار في الحد من التهديدات السيبرانية التي تتعرض لها الجامعة والطلاب والمؤسسات الرقمية المختلفة، والتي تمثل خطرًا على الأمن القومي والاقتصادي للدولة.

٣. يمكن أن تسهم نتائج هذه الدراسة في عدة نواحي تطبيقية تهم المسئولين في وزارة التعليم العالي والبحث العلمي لتنمية مهارات الطلاب الفكرية والتحليلية والإبداعية للاستجابة لمختلف التحديات الأمنية السيبرانية، وتطوير القدرات اللازمة للتعامل معها.

منهج الدراسة وأداته

تفرض طبيعة الدراسة الحالية استخدام المنهج الوصفي باعتباره أحد مناهج البحث العلمي التي تهدف إلى جمع معلومات وحقائق مفصلة تصف الظاهرة بغرض تعرف الحالة الراهنة لمجتمع الدراسة والوصول الى استنتاجات تسهم في فهم الواقع وتطويره (درويش، ٢٠١٨، ١١٨)، واستخدمت الاستبانة كأداة لجمع البيانات، وتم تطبيقها على عينة من الطلاب بكليات (التربية، التجارة وإدارة الأعمال، السياحة والفنادق) بجامعة حلوان، سعيًا نحو وضع تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية.

حدود الدراسة

تتحدد حدود الدراسة فيما يلي:

الحدود الموضوعية: اقتصرت الدراسة الميدانية في حدها الموضوعي على الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية وأساليب تنميتها. وتمثلت مبررات اختيار جامعة حلوان فيما يلي:

تعد أحد الجامعات الرائدة في مجال تكنولوجيا المعلومات والاتصالات، وتتميز بخبرتها ومؤهلاتها المتميزة في هذا المجال.

قامت بمبادرات مهمة لتعزيز الأمن السيبراني في مصر، منها تقديم جامعة حلوان مقترح للمجلس الأعلى للجامعات بشأن إدراج موضوع التربية الإعلامية الرقمية كفصل ضمن محتويات مقرر القضايا المجتمعية على طلاب الكليات بالجامعات وتم الموافقة على المقترح لأهمية دور الجامعات في تحسين جودة التعليم وتنمية مهارات الطلاب، وتعزيز الوعي السيبراني والأمن الإلكتروني.

الحدود الزمانية: تم تطبيق أداة الدراسة الميدانية خلال الفصل الدراسي الأول للعام الدراسي ٢٠٢٣/٢٠٢٤ م.

الحدود البشرية: اقتصر تطبيق أداة الدراسة على عينة من الطلاب بكليات (التربية، التجارة وإدارة الأعمال، السياحة والفنادق) بجامعة حلوان. وتمثلت مبررات اختيار كلية (التربية، التجارة وإدارة الأعمال، السياحة والفنادق) بجامعة حلوان فيما يلي:

- **كلية التربية:** يعد التعليم الإلكتروني والتعلم عن بعد من أهم التحديات التي تواجهها المؤسسات التعليمية في الوقت الحالي، ويحتاج الطلاب في هذه الكلية إلى فهم الأسس الأساسية للأمن السيبراني في التعليم الإلكتروني وطرق حماية البيانات والمعلومات التعليمية الحساسة.
- **كلية التجارة وإدارة الأعمال:** يعد قطاع التجارة وإدارة الأعمال هدفًا رئيسيًا للاختراقات السيبرانية، وبالتالي يحتاج الطلاب في هذه الكلية إلى فهم الأسس الأساسية للأمن السيبراني في الشركات والأعمال التجارية، وكذلك طرق الوقاية والحماية من الهجمات الإلكترونية والاحتيال الإلكتروني.
- **كلية السياحة والفنادق:** يعتمد قطاع السياحة والفنادق على التكنولوجيا والإنترنت في إدارة الحجوزات والتسويق وتقديم الخدمات الإلكترونية. ومن خلال استخدام هذه التقنيات، يصبحون أكثر عرضة للهجمات السيبرانية والاختراقات، كما تتعرض قواعد بيانات الفنادق والشركات السياحية لهجمات سيبرانية متكررة تهدف لسرقة بيانات العملاء مثل بطاقات الائتمان ومعلومات الهوية. لذا يحتاج طلاب كلية السياحة والفنادق إلى تنمية ثقافة الأمن السيبراني للحفاظ على سرية المعلومات الحساسة للعملاء وتجنب الاختراقات والاحتيال الإلكتروني.

مصطلحات الدراسة

تتحدد مصطلحات الدراسة فيما يلي: -

الأمن السيبراني: Cybersecurity

تعرف الدراسة الحالية الآمن السيبراني بأنه: مجموعة من الإجراءات والتدابير والتقنيات والأنشطة التي تهدف إلى حماية المعلومات والأجهزة الرقمية والشبكات والفضاء السيبراني بصفة عامة من الوصول غير المصرح به والتدخلات والاختراقات والتهديدات غير المشروعة.

التربية الاعلامية الرقمية Digital Media Education

تعرف الدراسة الحالية التربية الإعلامية الرقمية بأنها: العملية التي يتم من خلالها تطوير مهارات وقدرات الطلاب على استخدام التقنيات الرقمية والوسائط الإعلامية الحديثة بشكل فعال وآمن.

خطوات السير في الدراسة

سعيًا نحو الإجابة عن أسئلة الدراسة وتحقيقا للأهداف التي تم تحديدها، يمكن تحديد خطوات السير في الدراسة في خمسة محاور رئيسة يتم عرضها على النحو التالي:

المحور الأول: ماهية الأمن السيبراني بالجامعات، أهدافه، أبعاده

المحور الثاني: الإطار المفاهيمي للتربية الاعلامية الرقمية بالجامعات

المحور الثالث: كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الأمن السيبراني، وأساليب تنميتها.

المحور الرابع: إجراءات الدراسة الميدانية وتحليل وتفسير نتائجها

المحور الخامس: تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية

المحور الأول: ماهية الأمن السيبراني بالجامعات، أهدافه، أبعاده

يتناول المحور التالي عرضًا لمفهوم الأمن السيبراني، أهدافه، عناصره، أهميته، أبعاده.

أولًا: مفهوم الأمن السيبراني وأهدافه

تعددت تعريفات الباحثين للأمن السيبراني، ومن أبرز تلك التعريفات ما يلي:

عرف بونيف (٢٠١٩، ١٢٤) الأمن السيبراني بأنه: القدرة على مجابهة الهجمات الالكترونية ومختلف التهديدات ذات الصلة والتي تقوم بها جماعات أو دول أو أفراد.

وحدد همايون وآخرون Humayun, et al., (٢٠٢٠، ٣١٧٣) الأمن السيبراني بأنه: آلية لحماية أصول الأفراد والمنظمات من الوصول غير المصرح به.

ويرى الجهني والفاضل Aljohani & Elfadil (٢٠٢٠، ١٤١) الأمن السيبراني بأنه: أمن المعلومات أو البيانات الذي يعتبر الأجهزة الرقمية / الحاسوبية مثل الهواتف الذكية وأجهزة الكمبيوتر والخوادم والإنترنت. ويشمل جميع عناصر أمن الكمبيوتر / الشبكة التي تؤمن الأجهزة من الوصول غير المصرح به والتغييرات وتدمير أنظمة المعلومات، مع انتشار استخدام الكمبيوتر والاعتماد على الإنترنت، يعد الأمن السيبراني جزءًا مهمًا من أي نظام معلومات.

عرف شوكت وآخرون.Shaukat., et al (٢٠٢٠، ٢٢٢٣١٠) الأمن السيبراني بأنه: مجموعة الإجراءات الأمنية التي يمكن اتخاذها لحماية أصول المستخدم والفضاء الإلكتروني ضد الوصول غير المصرح به والهجمات، فالهدف الرئيس لنظام الدفاع السيبراني هو ذلك يجب أن تكون البيانات سرية ومتكاملة ومتاحة.

وأشار كافاك وآخرون Kavak, et al., (٢٠٢١، ٢) للأمن السيبراني بأنه: مجموعة من الأدوات والسياسات ومفاهيم الأمان وضمانات الأمان والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية وأصول المنظمة والمستخدم.

أشار جاب الله (٢٠٢٢، ٢٢٤٤) الأمن السيبراني بأنه: مجموعة من الإجراءات التي يتم اتخاذها للحد أو الدفاع ضد مخاطر الهجمات السيبرانية، من خلال الوسائل والأدوات المستخدمة في مواجهة تلك المخاطر.

وأضاف سليمان، وعبدالحليم (٢٠٢٢، ٤٢– ٤٣) الأمن السيبراني بأنه: مجموع القوانين والأدوات والنصوص والمفاهيم وأساليب إدارة المخاطر والممارسات الفنية المتعمقة بتكنولوجيا المعلومات والاتصالات المستخدمة لحماية المصالح والدول والأشخاص.

عرف ناصف (٢٠٢٢، ٤٩) الأمن السيبراني بأنه: حماية الشبكات وأنظمة وتقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات من أي اختراق أو تعطيل أو استخدام غير مشروع.

كما عرفا العمارات، والحمامصة (٢٠٢٢، ١٩) الأمن السيبراني بأنه: مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر الفضاء السيبراني بصفة عامة من مختلف الهجمات والاختراقات والتهديدات السيبرانية التي قد تهدد الأمن القومي للدول.

وأضاف الركبان (٢٠٢٢، ١٦٧) الأمن السيبراني بأنه: مجموعة الإجراءات والأنشطة الهادفة إلى حماية جميع الأصول الالكترونية الخاصة بالجامعات، من بيانات،

أو أجهزة، أو أنظمة الكترونية من استغلالها أو الاضرار بها بأي شكل من الأشكال ومعالجة الحاصل بأسرع وقت وأقل تكلفة.

عرف توفيق ومرسي (٢٠٢٣، ٧٥٢) الأمن السيبراني بأنه: جميع الإجراءات والوسائل التقنية والتدابير والجهود التي ينبغي أن توفرها الجامعة، بهدف حماية المصادر المختلفة من (البرمجيات، والأجهزة المحمولة، والبيانات الرقمية الشخصية) من التجاوزات والتداخلات غير المشروعة أو سوء الاستغلال، ومقاومة محاولات الاختراق أو الحوادث غير المتوقعة، وتعزيز خصوصيتها وتشفيرها، واتخاذ إجراءات حماية أعضاء هيئة التدريس من مخاطر الفضاء السيبراني.

وأشار البحيري (٢٠٢٣، ٦٤-٦٥) للأمن السيبراني بأنه: جميع الإجراءات الخاصة بحماية الأنظمة الإلكترونية والشبكات والبنية التحتية الرقمية والمعلومات من الاختراقات والهجمات الإلكترونية والتهديدات السيبرانية.

وأشار بانسال، وآخرون Bansal, et al., (٢٠٢٤، ٩٩) الأمن السيبراني بأنه: الإجراءات والتقنيات والأفكار المرتبطة ارتباطًا وثيقًا بأمن المعلومات والبيانات التشغيلية.

باستقراء ما سبق تعرف الدراسة الحالية الآمن السيبراني بأنه: مجموعة من الإجراءات والتدابير والتقنيات والأنشطة التي تهدف إلى حماية المعلومات والأجهزة الرقمية والشبكات والفضاء السيبراني بصفة عامة من الوصول غير المصرح به والتدخلات والاختراقات والتهديدات غير المشروعة.

إن الأمن السيبراني وأمن المعلومات مصطلحان متشابهان، لكنهما ليسا متطابقين، لذا وجب التفرقة بين الأمن السيبراني وأمن المعلومات (ناصف، ٢٠٢٢، ٥١)، (ساعد بوقرص، ٢٠٢٢، ٦٧):

- الأمن المعلوماتي (Information Security) يشير إلى حماية المعلومات والبيانات الحساسة، بما في ذلك الحفاظ على سرية المعلومات والحماية من الاختراق والتدمير والتلاعب. وتشمل الحماية في الأمن المعلوماتي جميع الأصول الرقمية، مثل الأنظمة والشبكات والتطبيقات والبيانات.
- أما الأمن السيبراني (Cyber Security) فيشير إلى حماية الأصول الرقمية، بما في ذلك الأجهزة الإلكترونية والشبكات والأنظمة والبيانات، ويتم التركيز بشكل خاص على الهجمات والتهديدات المتعلقة بالإنترنت والشبكات العامة. ويتطلب الأمن السيبراني فهمًا عميقًا للتهديدات الرقمية والهجمات المحتملة، وتطوير استراتيجيات لمنعها والتعامل معها.

باستقراء ماسبق يتبين أن الأمن المعلوماتي يشير إلى حماية البيانات والمعلومات الحساسة، بينما الأمن السيبراني يركز على حماية الأصول الرقمية من الهجمات والتهديدات السيبرانية.

ويرتبط الأمن السيبراني بعدة مفاهيم اخرى ذات صلة به وضرورية لوجوده أهمها:

- **الفضاء السيبراني: Cyper Space**

عرف همايون وآخرون Humayun, et al., (٢٠٢٠، ٣١٧٣) الفضاء السيبراني بأنه: مجال عالمي داخل عالم المعلومات، يتميز بخصائص فريدة تتمثل في استخدام الطيف الكهرومغناطيسي والإلكتروني لإنشاء وتحديث وتخزين ومشاركة واستغلال المعلومات. ويتم ذلك من خلال استخدام الشبكات المترابطة وتقنيات المعلومات والاتصالات الحديثة.

ويتفق كل من رادونيفيتش Radoniewicz (٢٠٢٢، ٣٣) ومصطفى (٢٠٢٢، ٧٢٤) للفضاء السيبراني بأنه: بيئة تفاعلية رقمية تشمل عناصر مادية وغير مادية مكونة من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مشتغلين أو مستعملين.

وفي ضوء ماسبق الفضاء السيبراني يشير إلى المجموعة الشاملة للأنظمة والشبكات الإلكترونية والمعلوماتية والتي يتم استخدامها للتواصل وتبادل المعلومات عبر الإنترنت.

- **الردع السيبراني: Cyber Deterrence**

عرف بونيف (٢٠١٩، ١٢٩) الردع السيبراني بأنه: استخدام القوة الرقمية لتحقيق أهداف سياسية أو عسكرية عن طريق تهديد المهاجمين المحتملين بالرد بقوة في حالة تنفيذهم لأي عملية هجومية عبر الإنترنت.

ويتفق كل من كينونين Keinonen (٢٠٢٣، ٥٦٧)، ومصطفى (٢٠٢٢، ٧٢٥) على أن الردع السيبراني يقصد به: منع الأعمال الضارة ضد الأصول الوطنية في الفضاء الرقمي والأصول التي تدعم العمليات الفضائية، ويرتكز الردع السيبراني على ثلاث ركائز استراتيجية في الدفاع تتمثل في: مصداقية الدفاع، والقدرة على الانتقام، والرغبة في الانتقام.

باستقراء ماسبق فإن الردع السيبراني يشير إلى الإجراءات والسياسات والتقنيات التي تستخدم لردع عمليات الهجوم السيبراني وحماية الأنظمة الإلكترونية والمعلوماتية من الاختراق.

- **الجريمة السيبرانية: Cyber Crime**

أشار بوقرص (٢٠٢٢، ٦٥) للجريمة السيبرانية بأنها: كل عمل ضار يحدث في الفضاء السيبراني كالاحتيال ونشر محتويات غير قانونية والهجمات التي تستهدف منظومات الإعلام للمؤسسات أو للأفراد بغرض التجسس أو التخريب أو الابتزاز أو التأثير السلبي على الرأي العام.

وعرفها شفيق Shafik (٢٠٢٤، ٧٩) بأنها: مجموعة الأعمال غير القانونية التي تتم عبر أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها.

باستقراء ماسبق تشير الجريمة السيبرانية إلى الأنشطة غير القانونية التي تتم باستخدام تقنيات الحوسبة والإنترنت والتكنولوجيا الحديثة، وتشمل هذه الأنشطة الاختراقات الإلكترونية والاحتيال والتجسس والقرصنة الإلكترونية والتعدي على الخصوصية والتشويش والتهديدات الإلكترونية الأخرى.

وينطلق مفهوم الأمن السيبراني من حاجة المؤسسات والمنظمات والأفراد إلى حماية أنظمتهم وبياناتهم من الهجمات الإلكترونية والتهديدات السيبرانية المختلفة، ويشمل الأمن السيبراني الممارسات والإجراءات والقياسات التي تحمي البيئة السيبرانية وأصول المنظمات والمستخدمين من الهجمات الخبيثة التي تهدف إلى تقويض سرية وسلامة وتوافر المعلومات أو البيانات تشمل الأصول، على سبيل المثال لا الحصر، أجهزة الحوسبة المتصلة والبنية التحتية الحيوية والخوادم والشبكات والمعلومات المخزنة أو المنقولة في البيئة السيبرانية(Anjani,2021, 2).

وتهدف الجامعات إلى تحقيق الأهداف التالية في مجال الأمن السيبراني (Schmeelk,2021, 86)، (Kavak, et al.,2021,2)، (Bhatnagar& Pry,2020, 51-53) :

- تأمين البني التحتية لأمن المعلومات والبيانات الخاصة بالطلاب وأعضاء هيئة التدريس، والحفاظ على خصوصيتها وسريتها وعدم السماح بالوصول إليها من قبل الغير.
- توفير الحماية اللازمة للشبكات والأنظمة والتطبيقات والخوادم من الهجمات السيبرانية المختلفة، والحد من هذه التهديدات بأفضل السبل الممكنة.
- تعزيز الوعي السيبراني لدى الطلاب والعاملين في الجامعة، وتوفير التدريبات اللازمة لهم بشأن كيفية التعامل مع التهديدات السيبرانية المختلفة، والتأكد من أنهم يفهمون أهمية الحفاظ على الأمن السيبراني.

- الامتثال للمعايير والتشريعات السيبرانية المحلية والدولية، وتطبيق الممارسات الأفضل في مجال الأمن السيبراني.

باستقراء ماسبق فالأمن السيبراني في الجامعات يهدف إلى حماية الأنظمة والشبكات الإلكترونية والبيانات الحساسة والمعلومات الشخصية للطلاب والموظفين والأعضاء الآخرين في المؤسسة الجامعية، وذلك عن طريق حماية الأنظمة الحيوية والبيانات الحساسة، وتوفير الحماية للمعلومات الشخصية، وتحسين الوعي الأمني لدى المستخدمين وتأمين السلامة الرقمية للأعضاء والطلاب، إضافة إلى إدارة التهديدات الأمنية بشكل فعال والتعامل مع الهجمات السيبرانية بطريقة سريعة وفعالة.

ثانيًا: عناصر الأمن السيبراني وأهميته

حتى يتحقق الهدف من الأمن السيبراني، لابد من توفر مجموعة عناصر تعمل مع بعضها البعض لتكمل الدور في ذلك، ومن أهم عناصر الأمن السيبراني ما يلي (Miranda-García, et al., 2024, 563)، (العمارات، والحمامصة، ٢٠٢٢،٣٦)، (Wang & Sbeit,2020, 18-20):

- باستمرار لتقليل فرص الهجمات السيبرانية المحتملة. علاوة على ذلك ويجب أن تتضمن هذه التقنيات خاصية الحماية الإضافية مثل تقنيات التشفير وأنظمة الوصول **التقنية:** تتضمن الأجهزة والبرمجيات والتقنيات الأخرى التي تستخدمها الجامعة لإدارة وتخزين ومعالجة المعلومات، ويجب أن تكون هذه التقنيات محمية بشكل جيد ومحدثة ومكافحة الفيروسات والجدران النارية والتطبيقات الأخرى التي تساعد في حماية المعلومات والحفاظ على سرية وسلامة البيانات.
- **الأشخاص:** يشمل هذا العنصر جميع الأفراد الذين يتعاملون مع نظام الحاسوب في الجامعة، مثل الطلاب والموظفين وأعضاء هيئة التدريس والعاملين، ويستوجب الأمر على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسة كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانب القيام بعمل نسخ احتياطية للبيانات.
- **الأنشطة والعمليات:** يتم توظيف الأشخاص، والتقنيات للقيام بالعديد من العمليات مثل إدارة الأنظمة والشبكات والتطبيقات والبيانات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني، والتصدي لهجماته بكل كفاءة. يجب تأمين هذه العمليات والأنشطة لمنع الاختراقات والتسلل من قبل المهاجمين، وذلك بتطبيق ممارسات الأمن السيبراني القياسية

واستخدام التقنيات الأمنية المتطورة، مثل جدران الحماية وبرامج مكافحة الفيروسات والتشفير.

باستقراء ماسبق، يتألف الأمن السيبراني في الجامعات من ثلاثة عناصر رئيسة: الأشخاص، الأنشطة والعمليات، والتقنية. ويقصد بالأشخاص الطلاب والموظفين والمستخدمين الآخرين في الجامعة، حيث يجب توعيتهم وتدريبهم على مخاطر الأمن السيبراني وكيفية تجنبها. أما الأنشطة والعمليات فتشمل جميع العمليات الإلكترونية والأنشطة التي تتم داخل الجامعة، مثل البريد الإلكتروني والتسجيل والمنصات الإلكترونية الأخرى. يجب تأمين هذه العمليات والأنشطة لمنع الاختراقات والتسلل من قبل المهاجمين. أما التقنية فتتضمن جميع الأدوات والتقنيات المستخدمة في الجامعة لحماية نظامها السيبراني، مثل برامج مكافحة الفيروسات وجدران الحماية والتشفير. يجب أن تتم مراقبة وتحديث هذه التقنيات بشكل دوري للحفاظ على أمن النظام السيبراني للجامعة.

وحدد كل من (Alhaif, 2023,40-42)، (سراج،٢٠٢٢، ٢٠٤)، (Ulven & Wangen, 2021,39)، (Matyokurehwa, et al., 2021, 4-6) أهمية الأمن السيبراني بالجامعات على النحو التالي:

- **حماية البيانات الحساسة:** يتم تخزين العديد من المعلومات الحساسة في الجامعات، مثل السجلات الطبية ومعلومات الهوية والمعلومات المالية والأكاديمية. مما يتطلب توفير الحماية الفائقة لخصوصية المعلومات والإبقاء على سريتها، وعدم السماح لغير المخولين بالوصول إليها واستخدامها.
- **الحفاظ على سلامة الأنظمة الأكاديمية:** تعتمد الجامعات على أنظمة حاسوبية معقدة تتيح الوصول إلى معلومات وموارد أكاديمية متنوعة، ويجب حماية هذه الأنظمة من الهجمات السيبرانية التي يمكن أن تتسبب في توقف الخدمات الأكاديمية وتعطيل العملية التعليمية.
- **الحفاظ على سمعة الجامعة:** يمكن للهجمات السيبرانية أن تؤدي إلى تسريب المعلومات الحساسة، مما يؤثر على سمعة الجامعة ويضر بسمعتها واعتماديتها.
- **حماية الأبحاث العلمية:** تعد الجامعات مراكز رئيسة للأبحاث العلمية، ويتم تخزين العديد من البيانات الحساسة والنتائج البحثية في الأنظمة الحاسوبية للجامعات. ويجب حماية هذه الأنظمة من الاختراقات السيبرانية التي تهدد سلامة الأبحاث والنتائج العلمية.

- **تعزيز الثقة والاعتمادية:** يمكن للجامعات التي تتبع إجراءات وأساليب الأمن السيبراني الجيدة أن تتمتع بثقة واعتمادية أكبر من الطلاب والأعضاء التابعين لها، مما يساعد على جذب المزيد من الأعضاء والطلاب وتعزيز مكانة الجامعة في المجتمع الأكاديمي والصناعي.
- **الحد من التكاليف والخسائر:** يمكن للهجمات السيبرانية أن تؤدي إلى خسائر مالية كبيرة، سواء من خلال تعطيل الخدمات الأكاديمية أو تسريب المعلومات الحساسة، ويمكن للأمن السيبراني الجيد أن يحد من هذه التكاليف والخسائر.

باستقراء ماسبق يتبين أن الأمن السيبراني في الجامعات يمثل عاملًا حاسمًا للحفاظ على سمعة الجامعة وجودة التعليم العالي التي تقدمها، حيث يساعد في حماية الأبحاث والأفكار الجديدة والملكية الفكرية وتعزيز الثقة بين الطلاب والموظفين والشركاء. كما يحمي الأمن السيبراني البيانات الحساسة والشخصية ويحد من التكاليف المالية الناتجة عن الاختراقات السيبرانية والتسريبات والتي من شأنها أن تؤدي إلى خسائر كبيرة للجامعة وتؤثر على سمعتها وتنعكس سلبًا على سمعة الطلاب والموظفين والخريجين المرتبطين بها. لذا، فالحفاظ على الأمن السيبراني في الجامعات يمثل أهمية كبيرة لحماية البيانات والمعلومات الحيوية وتحقيق الأهداف الأكاديمية والبحثية والتطويرية.

ثالثًا: أبعاد الأمن السيبراني بالجامعات

يمتد الأمن السيبراني ليشمل جميع المجالات الاقتصادية، والاجتماعية، والسياسية، والقانونية لكافة المجتمعات المعاصرة، واستنادًا لما سبق فإن الأمن السيبراني يرتبط ارتباطا وثيقًا بسلامة مصادر الثروة والتقدم في الوقت الراهن والتي تتضمن: القدرة على اتصال والتواصل، والبيانات والمعلومات التي يستند عليها الإنتاج، والابداع، والقدرة على المنافسة، ومن ثم يمكن عرض أبعاد الأمن السيبراني بالجامعات على النحو التالي:

١-الأبعاد السياسية:

تتعلق بالتأثير الذي يمكن أن تحدثه الهجمات السيبرانية على العلاقات السياسية للمؤسسة ومهمة، ويمكن استخدام هذه المعلومات في العديد من الأغراض، بما في ذلك التأثير التعليمية. وتشمل هذه الأبعاد مسائل مثل التجسس والتلاعب والتأثير على العمليات السياسية. فعلى سبيل المثال، يمكن للهجمات السيبرانية أن تستخدم كأداة للتجسس على الأبحاث والتقنيات التي تنتجها الجامعة، مما يمكن أن يؤدي إلى الحصول

على معلومات حساسة على العلاقات الدولية للجامعة وعلى سمعتها (Pop & Ermicioi, 2021, 171).

ويمكن أن تؤدي الهجمات السيبرانية أيضًا إلى التلاعب بالعمليات السياسية في المؤسسة التعليمية، حيث يمكن للمهاجمين استغلال الثغرات الأمنية لتحريف البيانات أو تزوير الأرقام أو النتائج، وهذا يمكن أن يؤدي إلى تغيير القرارات السياسية التي تتخذها الجامعة وتأثيرها على العلاقات السياسية للجامعة. وتشمل الأبعاد السياسية أيضًا تأثير الهجمات السيبرانية على الأمن القومي والدفاع الوطني، حيث يمكن أن تستخدم الهجمات السيبرانية كأداة في الحرب الإلكترونية، وهذا يمكن أن يؤدي إلى تأثير سلبي على الأمن القومي والدفاع الوطني للدولة(Ceko, 2021, 61).

باستقراء ماسبق يتبين أن الهجمات السيبرانية يمكن أن تؤثر على العلاقات السياسية للمؤسسة التعليمية بعدة طرق، بما في ذلك التجسس على الأبحاث والتقنيات التي تنتجها الجامعة، والتلاعب بالعمليات السياسية في المؤسسة، وتشمل هذه الأبعاد أيضًا تأثير الهجمات السيبرانية على الأمن القومي والدفاع الوطني، حيث يمكن استخدامها كأداة في الحرب الإلكترونية. لذا فعلى المؤسسات التعليمية اتخاذ تدابير أمنية لحماية بياناتها وعملياتها السياسية، بما في ذلك تطوير استراتيجيات أمنية متكاملة وتحديث أنظمة الحماية السيبرانية، وتوعية الموظفين والطلاب حول مخاطر الهجمات السيبرانية وكيفية التعامل معها. كما يجب على المؤسسات التعليمية العمل مع الجهات المختصة في مجال الأمن السيبراني لتحديد وتقييم المخاطر وتحديد الخطط الاستباقية للتعامل معها. وبهذه الطريقة، يمكن للمؤسسات التعليمية الحفاظ على سمعتها وضمان سلامة بياناتها وعملياتها السياسية، وتفادي التأثيرات السلبية التي يمكن أن تسببها الهجمات السيبرانية على علاقاتها السياسية والأمن القومي والدفاع الوطني.

٢-الأبعاد الاقتصادية:

تتعلق بالتأثير الذي يمكن أن تحدثه الهجمات السيبرانية على الجوانب الاقتصادية للمؤسسة التعليمية. وتشمل هذه الأبعاد مسائل مثل تكاليف الهجمات وخسائر الأعمال وتكلفة استعادة البيانات والإنتاجية. فعلى سبيل المثال، يمكن للهجمات السيبرانية أن تؤدي إلى تعطيل خدمات الجامعة مما يؤدي إلى تأثير سلبي على سير العمليات التعليمية والإدارية وبالتالي يمكن أن يؤدي إلى فقدان الإنتاجية وخسائر الأعمال . (Bannister,2022,5)

كما يمكن أن تؤدي الهجمات السيبرانية إلى خسارة البيانات والمعلومات الحيوية التي تكلف الجامعة ملايين الدولارات، حيث يمكن للمهاجمين الوصول إلى المعلومات الحساسة والمالية والشخصية وتدميرها أو سرقتها أو تشفيرها ومنع الجامعة من الوصول

إليها، وبالتالي يمكن أن تؤدي الهجمات السيبرانية إلى تكاليف باهظة لاستعادة البيانات والمعلومات المفقودة (Maulani, et al., 2021, 136).

وتشمل الأبعاد الاقتصادية أيضًا تأثير الهجمات السيبرانية على سمعة الجامعة والتي يمكن أن تؤدي إلى تأثير سلبي على الحصول على التمويل والتبرعات والتعاون الاقتصادي والتعاون مع الشركاء التجاريين والمانحين، وهذا يمكن أن يؤدي إلى خسارة الفرص الاقتصادية والتعليمية والبحثية. لذا، يتعين على المؤسسات التعليمية تحسين الوعي الأمني لدى العاملين والطلاب والمستخدمين، وتوفير التدريب اللازم والأدوات الفعالة للوقاية من الهجمات السيبرانية والتعامل معها، وذلك لتقليل التكاليف الاقتصادية والحفاظ على السمعة والفرص الاقتصادية والتعليمية للجامعة. كما يتعين على المؤسسات التعليمية تطوير استراتيجيات الأمن السيبراني وتنفيذها بشكل فعال ومستمر، وتحديث البرامج والأنظمة والتقنيات الأمنية بشكل دوري، وتوفير الموارد اللازمة للحفاظ على أمن الحوسبة والوقاية من الهجمات السيبرانية، وبالتالي تحقيق الاستقرار الاقتصادي والتعليمي للجامعة (Aborujilah,et al., 2022, 441-442).

في ضوء العرض السابق يتبين أن الأبعاد الاقتصادية للأمن السيبراني في الجامعات تتضمن تكاليف الهجمات وخسائر الأعمال وتكلفة استعادة البيانات والإنتاجية، بالإضافة إلى تأثير الهجمات على سمعة الجامعة وفرص الحصول على التمويل والتعاون الاقتصادي، ويتعين على المؤسسات التعليمية تحسين الوعي الأمني وتطوير استراتيجيات الأمن السيبراني وتنفيذها بشكل فعال ومستمر وتوفير الموارد اللازمة للحفاظ على أمن الحوسبة والوقاية من الهجمات السيبرانية لتحقيق الاستقرار الاقتصادي والتعليمي للجامعة.

٣ -الابعاد الاجتماعية:

تسمح طبيعة الفضاء السيبراني المفتوحة عبر وسائل التواصل الاجتماعية لكل فرد بالتعبير عن تطلعاته السياسة وطموحاته الاجتماعية. كذلك تعتبر فرص ميسرة للاطلاع على الافكار والمعلومات المتباينة، مما يسمح بتبادل الخبرات، وتحقيق التعاون والتقارب بين المجتمعات المختلفة. كما أنه لايمكن تجاهل دور الفضاء السيبراني في تبادل المعلومات في المجالات العلمية والثقافية والخدمية، وفي أوقات الأزمات والكوارث إذ لاتقف الأبعاد الاجتماعية عند هذه الحدود فقط بل تتعداها الي صيانه القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات، إضافة إلى العادات والتقاليد(البغدادي،٢٠٢١، ١٤٥٥).

تتعلق الأبعاد الاجتماعية بالتأثير الذي يمكن أن تحدثه الهجمات السيبرانية على الجوانب الاجتماعية للمؤسسة التعليمية. وتشمل هذه الأبعاد مسائل مثل الخصوصية والأمان والثقة والتعاطف. فعلى سبيل المثال، يمكن للهجمات السيبرانية أن تؤدي إلى

تسريب بيانات الطلاب والموظفين والأساتذة والباحثين وتعريضها للخطر، مما يؤدي إلى الانتهاكات الخصوصية والأمان (Pinchot, et al., 2020, 45-47).

ويمكن للهجمات السيبرانية أيضًا أن تؤثر على الثقة في الجامعة والتي يمكن أن تؤدي إلى خسارة الثقة والاحترام من قبل الطلاب وأولياء الأمور والمانحين والحكومات، كما يمكن أن تؤدي إلى خسارة الثقة في الأنظمة الإلكترونية والتكنولوجيا في المؤسسة التعليمية، وتشمل الأبعاد الاجتماعية أيضًا تأثير الهجمات السيبرانية على الصحة النفسية والاجتماعية للطلاب والعاملين في الجامعة، حيث يمكن أن تؤدي الهجمات السيبرانية إلى التأثير على الحالة النفسية للأفراد وخاصة الطلاب الذين يمكن أن يشعروا بالذعر والقلق حول خصوصيتهم وأمانهم، كما يمكن أن تؤدي إلى تعطيل العمليات التعليمية والإدارية، مما يؤثر على الجو الاجتماعي ويؤدي إلى الإرهاق والتعب والإحباط (Carley, 2020,367).

لذا أشار وانغ Wang (٢٠٢١، ٢١٤) إلى ضرورة أن يتضمن تعليم الأمن السيبراني أنشطة تعليمية وتعلمية متعددة التخصصات حيث يحتاج المتخصصون في الإنترنت إلى تطوير وامتلاك كفاءات فنية وغير تقنية ومعارف ومهارات وقدرات، مثل التفكير النقدي والتحليلي وحل المشكلات والتواصل والعمل الجماعي والمهارات القيادية المتوقعة للقوى العاملة الإلكترونية في المستقبل .

باستقراء ماسبق، تتضمن أبعاد الأمن السيبراني في الجامعات جوانب مختلفة. فمن الناحية السياسية، تتعلق الأمور بحماية البيانات الحساسة والمعلومات الأكاديمية والبحثية من الاختراقات والاستيلاء غير المصرح به عليها. ومن الناحية الاقتصادية، يجب حماية الأنظمة الإلكترونية والإنترنت والموارد المادية والمعلوماتية للجامعات من الهجمات الإلكترونية التي قد تتسبب في خسائر مالية كبيرة. وأخيرًا، الأبعاد الاجتماعية وتتعلق بحماية خصوصية الطلاب والعاملين في الجامعة وضمان عدم تعرضهم للاختراقات السيبرانية والاستغلال غير المصرح به للبيانات الشخصية. لذا، فإن تأمين الأبعاد السيبرانية في الجامعات يعد أمرًا حيويًا للحفاظ على سلامة وأمان الجامعات والمجتمعات التي تخدمها.

المحور الثاني: الإطار المفاهيمي للتربية الاعلامية الرقمية بالجامعات

يتناول المحور الحالي عرضًا لمفهوم التربية الاعلامية الرقمية وأهدافها، ومهاراتها وذلك على النحو التالي:

أولًا: مفهوم التربية الاعلامية الرقمية وأهدافها

قبل التطرق إلى مفهوم التربية الإعلامية الرقمية وجب الإشارة إلى مفهوم التربية الإعلامية وذلك على النحو التالي:

عرف ضيف (٢٠١٧، ٤٤٥) للتربية الإعلامية بأنها: عملية تدريب الأفراد على كيفية التعامل مع وسائل الإعلام المختلفة من خلال إكسابهم معلومات ومعارف ومهارات تساعدهم على الاستخدام المنظم لهذه الوسائط متفادين انعكاساتها السلبية.

وأضاف الجعد، والاسمري (٢٠١٨، ٢٠٠) للتربية الإعلامية بأنها: عملية يتم من خلالها الطالب متلقيًا ايجابيًا للرسالة الاعلامية، بحيث تكسبه القدرة على الدخول للرسائل الاعلامية، باستخدام وسائل الاعلام المناسبة وانتقاء المحتوى الجيد من الوسائل الاعلامية، سواء المقروءة أو المسموعة أو المرئية، وتنمية المهارات النقدية كالاستنتاج والتفسير والتقويم والتشجيع على الحوار وابداء الآراء، وكتابة الرسائل الاعلامية ومشاركتها.

أما فايز، وأبو العز (٢٠٢١، ٦٣٩) فعرف التربية الاعلامية بأنها: عملية توظيف وسائل الاتصال بطريقة مثلى بغرض تحقيق أهداف تربوية مرسومة في إطار سياسة اعلامية/ تعليمية للدولة القائمة عليها.

وعرف إسماعيل وآخرون (٢٠٢٢، ٤٨٢) التربية الاعلامية بأنها: جميع المفاهيم والمعايير والمهارات التي تمكن الطلاب من التعامل الواعي مع وسائل الاعلام.

وإجمالًا فقد ركزت تعريفات التربية الإعلامية على مهارات التعرض النقدية لوسائل الإعلام، وفهم المكونات الفنية والجمالية للرسائل الإعلامية، والقدرة على التفاعل مع وسائل الإعلام في إعداد مواد مسموعة ومرئية، والتأثير على متخذي القرارات في وسائل الإعلام.

وتباينت الأدبيات التي تناولت مفهوم التربية الإعلامية الرقمية وأبعادها خلال العقدين الماضيين؛ نظرًا لاختلاف السياقات الاجتماعية والثقافية والتكنولوجية والاقتصادية لهذا المفهوم من ناحية، ولتطور وسائل الاتصال وتنوع تخصصات باحثيها من ناحية أخرى ولعل من أبرز تلك التعريفات ما يلي:

ويرى سالم، وحسن (٢٠١٨، ٤٤) التربية الاعلامية الرقمية بأنها: تعميق وعي الأفراد تجاه ما يتعرضون له من وسائل الإعلام التقليدية والرقمية وتمكنهم من الفهم والحكم الصحيح على مضامينها ويتم ذلك عن طريق تعلمهم المهارات المعرفية والتقنية اللازمة لذلك.

وأشار الخنيني، وآخرون (٢٠١٩، ١١٩) التربية الاعلامية الرقمية بأنها: امتلاك المبادئ والأحكام والمعارف والمهارات الأساسية والسلوكيات للتعامل مع الآلات والأجهزة

والمخترعات الحديثة وفي مقدمتها الكمبيوتر والانترنت وبناء الامكانيات والقدرات لفهم وتحليل وتقييم وتوصيل والتفاعل مع وسائل الاعلام الالكترونية بعقلية ديناميكية قادرة على فهم المتغيرات الجديدة واكتشاف المعلومات عند الحاجة اليها وتحديد مكانها وكيفية الوصول اليها وتقييمها واستعمالها بشكل فعال، كما تشعل الوعي بالمخاطر المحتملة عبر الانترنت من أجل تعزيز الأمن والسلامة الالكترونية.

وأضاف مكاوي، وآخرون (٢٠٢١، ٥٣٢) التربية الاعلامية الرقمية بأنها: القدرة على الوصول إلى الرسائل الإعلامية وتحليليها وتقييمها وإنتاجها بأشكال متنوعة.

وأشار عوف (٢٠٢١، ٢١٨) للتربية الاعلامية الرقمية بأنها: مناهج تعليمية مخططة لجميع المراحل ومعدة من قبل متخصصين وخبراء في التربية وعلوم الاعلام يتم تطويرها بما يتناسب مع مخرجات وسائل الاعلام الجديدة الناتجة عن التحول الرقمي لتكفل تمكين النشء والشباب من المهارات اللازمة للوصول الى الرسائل الاعلامية بكافة أشكالها، والقدرة على تحليلها وتقييمها وانتاجها، ومواجهة التحديات التي يفرضها المجتمع الرقمي وتتفق في الهدف مع مفاهيم ذات صلة كالإعلام والمعلوماتية الرقمية، أو محو الأمية الرقمية، أو المواطنة الرقمية للقرن الحادي والعشرين.

أما عقيلة (٢٠٢١، ٣٥٧) فعرف التربية الاعلامية الرقمية بأنها: مزيج من التربية الاعلامية والتربية الرقمية تركز على مهارات استخدام وسائل الاعلام الرقمي، وتهدف إلى الحق في التواصل وحرية التعبير وعديد من المهام التي يمارسها الفرد عندما يستخدم وسائل الاعلام الرقمية.

وأضاف راشد وزريزب Rashid & Zreyazb (٢٠٢١، ١٠٢-١١٣) أن التربية الاعلامية الرقمية عملية بناء الإنسان والمساعدة في الاستفادة من وسائل الإعلام وتطويرها بشكل هادف وواعي. يعني استخدام وسائل الإعلام بطريقة نشطة وحيوية بهدف المشاركة الاجتماعية الفعالة.

وأشار الزعبي (٢٠٢٢، ٣٣٢) التربية الاعلامية الرقمية بأنها: تثقيف الطلاب وتعليمهم رقميًا لما يحتاجونه من التكنولوجيا، واستعمالها بالشكل الأنسب والاستفادة من ايجابيات تكنولوجيا الاعلام والاتصال الالكتروني الرقمي وتجنب سلبياتها، وإكسابهم مهارات محو الأمية المعلوماتية.

وأضاف رجب وآخرون (٢٠٢٣، ٢٤١٠) التربية الإعلامية الرقمية بأنها: العملية التي يتم من خلالها تزويد الطلاب بطريقة الاستخدام الصحيحة والواعية لوسائل العالم الجديدة مثل طريقة الوصول والنقد والتقويم والتحليل والمهارات الاجتماعية التي تساعدهم على الاتصال الفعال وتمكنهم من استيعاب احترام الخصوصية الرقمية للأفراد.

باستقراء ما سبق تعرف الدراسة الحالية التربية الإعلامية الرقمية بأنها: العملية التي يتم من خلالها تطوير مهارات وقدرات الطلاب على استخدام التقنيات الرقمية والوسائط الإعلامية الحديثة بشكل فعال وآمن.

وتهدف التربية الإعلامية الرقمية أيضًا إلى تعزيز الوعي والحرص على الخصوصية والأمان الرقمي، مثل حماية البيانات الشخصية والتعرف على المخاطر الأمنية على الإنترنت، وتعزيز السلوكيات الإيجابية عند استخدام وسائل التواصل الاجتماعي والإنترنت.

وحدد كل من (سالم، وحسن، ٢٠١٨، ٤٥)، (العقباوى، ٢٠٢٢، ٣٣٥)، (مهني،٧٤١،٢٠٢٢– ٧٤٢) أهداف التربية الاعلامية الرقمية فيما يلي:

- تنمية مهارات التفكير الناقد والمشاهدة الواعية واكتساب المبادئ الأساسية لتحليل وتفسير ونقد كل ما يُقدم من مضامين إعلامية ذات أهداف مقصودة وغير مقصودة.
- دعم الهوية الثقافية وتكوين جيل قوي منتج ومبدع يُساهم في تنمية بلاده، عبر إمداده بالمعارف لفهم الأيدولوجيات الخاصة بوسائل الإعلام، وتزويده بالثقافة الإعلامية الهادفة لحصر ونقد ما يُشاهد ويتلقى.
- تعليم الأفراد تقييم وتقويم مضامين الإعلام والقائمين على إنتاجها، أي القدرة على تحليل ونقد مضامين الأفلام، كما تعلمهم كيفية انتاج المضامين ومشاركتها حيث أن الهدف الانتاجي هنا هدف تعليمي وليس هدفًا تجاريًا.
- تحويل الطلاب من الاستهلاك السلبي لوسائل الإعلام الى الاستهلاك الايجابي والانتاج الواعي بحيث يكونوا قادرين على التعبير عن افكارهم بواسطة وسائل الاعلام.
- تهيئة الطلاب لفهم وتحليل وتقييم وإنتاج الرسائل الإعلامية.

تأسيسًا على ما سبق فإن التربية الإعلامية الرقمية في الجامعات تهدف إلى تطوير مهارات وقدرات الطلاب في التعامل مع وسائل الإعلام الرقمية وتقنيات الاتصال الحديثة، وذلك لتمكينهم من مواكبة التطورات الحديثة في المجال الإعلامي والتكنولوجي، وتنمية القدرة على التفكير النقدي والتحليلي واتخاذ القرارات المناسبة في ظل هذه التحديات الجديدة، وتحسين قدرات الطلاب على التواصل الفعال والتعاون المثمر في بيئة إعلامية رقمية، وتوفير المهارات اللازمة للطلاب لتطوير أنشطتهم الأكاديمية والمهنية في المستقبل، وتعزيز الوعي والمسؤولية الاجتماعية والأخلاقية في استخدام وسائل الإعلام الرقمي.

ثانيًا: مهارات التربية الاعلامية الرقمية

يرتبط مفهوم التربية الاعلامية الرقمية عمليًا بتحصيل المهارات والمعارف الضرورية التي تفرض نفسها في مختلف أوجه التفاعل بن المتعلمين والميديا. وتشمل مهارات التربية الإعلامية الرقمية (Digital Media Literacy Skills) ما يلي: مهارة الوصول، مهارة التحليل، مهارة التقييم، مهارة إنتاج المحتوى:

أ- مهارة الوصول (Access Skills)

تعد تلك المهارة أولى مهارات التربية الإعلامية الرقمية، وتتمثل في القدرة على استخدام التكنولوجيا الرقمية ومواقع التواصل الاجتماعي، حيث يشير مفهوم الوصول إلى نجاح المستخدم في الحصول على المحتوى الرقمي المرغوب بأقل جهد ممكن أثناء استخدام الوسائط الإلكترونية، ويعني ذلك ارتباط مهارة الوصول بتلك العلاقة المركبة بين امتلاك القدرة على تحقيق أفضل استخدام ممكن للأدوات المتاحة عبر البيئة الرقمية من ناحية، والوصول المباشر للمحتوى المرغوب من ناحية أخرى (مكاوي، وآخرون، ٢٠٢١، ٥٣٣).

فالوصول للرسالة الإعلامية؛ يعني قراءتها وتفكيك رموزها سواء كانت رموزًا كتابية، أو صوتية، كالتأثيرات الصوتية الموسيقية ونحوها، أو مصورة، ترتبط بحركات الكاميرا وزوايا الإضاءة وغيرها مما يرتبط بالحركة على الشاشة، والرموز من خلال التركيب تتحول إلى نماذج مختلفة يمكن تمييزها من خلال تفسير طريقة الارتباطات بين الرموز فعندما يستطيع الطالب الوصول إلى الرسائل الإعلامية، فسيكون بمقدوره جمع المعلومات المطلوبة وفهم معناها بشكل أفضل، وعندئذ يكون قادرًا على أن (حسن،٢٠١٥، ١٣٦):

- التمييز والفهم لكم كبير من المفردات والرموز وأساليب الاتصال.
- تطوير استراتيجيات لتحديد مكان المعلومة وسط مجموعة واسعة من المصادر.
- اختيار مجموعة منوعة من نماذج المعلومات المتصلة بموضوع المهمة التي هم بصدد تنفيذها.

وفي هذا الإطار ينبثق عن مهارة الوصول عدة مهارات فرعية أخرى تتمثل في(مكاوي، وآخرون، ٢٠٢١، ٥٣٣):

- **مهارة التعرض:** وترتبط بقدرة الفرد على استخدام الوسيلة من حيث الانتقاء والاختيار والتخصيص.

- **مهارة معرفة الرموز:** وتعني قدرة المستخدم على إدراك ماهية المحتوى كونه رسالة اتصالية.
- **مهارة توفيق المعنى:** وترتبط بالقدرة على استكشاف الأبعاد المختلفة للمحتوى، ويكتسب المستخدم هذه المهارات الفرعية من خلال التدريب والخبرة

وبوجه عام تتمثل الأبعاد الاجتماعية والتكنولوجية والثقافية لمهارة الوصول في: امتلاك الحق في استخدام المحتوى الرقمي، وتوافر المعرفة اللازمة لاستخدام البرمجيات التي تقدم هذا المحتوى، والقدرة على ملاحظة سلوك وممارسات مستخدمي وسائل الإعلام الجديدة.

باستقراء ما سبق يتبين أن مهارة الوصول إلى المعلومات والمصادر الرقمية أحد المهارات الأساسية في التربية الإعلامية الرقمية بالجامعات، حيث تتطلب هذه المهارة اكتساب المعرفة اللازمة لتحليل البيانات والمعلومات المتاحة عبر الإنترنت وتحديد مدى صحتها وموثوقيتها. كما تتطلب تلك المهارة المعرفة الجيدة بأدوات البحث المتاحة ومصادر البيانات المختلفة، والقدرة على تقييم المصادر والمنابع الرقمية وتحديد مدى موثوقيتها.

ب- مهارة التحليل (Analytical Skills):

وتشير إلى القدرة على تحليل المعلومات والبيانات المتاحة بطريقة فعالة وفهمها وتفسيرها. وترتكز مهارة التحليل على افتراض عدم ارتباط عمليتي فهم المحتوى الرقمي وتقييمه بمجرد الوصول إلى الوسيلة التي تقدمه؛ إذ يتطلب امتلاك مهارة التحليل الإجابة على أسئلة تتعلق (بمصدر المحتوى، وتوجهات الوسيلة، وخصائصها، وطبيعة الخطاب المقدم عبرها، والجمهور المستهدف منها)، وتمثل هذه العناصر الستة محددات أساسية وضرورية لتحقيق الاستخدام الأمثل لوسائل الإعلام الجديدة، وتحليله والتأكد من مصداقيته (مكاوي، وآخرون، ٢٠٢١، ٥٣٣).

وتتطلب مهارة تحليل الرسالة الاعلامية عدد من الكفايات كاستنتاج الأحداث مما يقرأ أو يسمع أو يشاهد في الرسائل الاعلامية وبهذا يستطيع معرفة الأفكار الرئيسة، والمقارنة بين معلومات موضوع ما في وسائل اعلامية مختلفة، والتمييز بين الرأي والحقيقة، ومعرفة المقصود بالصور أو الرسوم، ويدرك التناقض في جوانب المادة الاعلامية، ويستخلص وجهة نظر الكاتب أو المتحدث حول موضوع ما، ويحلل أنواع الحجج المستخدمة ويفسرها، ويبدي رأيه ويكشف مصداقيتها ويقومها في ضوء معايير مجتمعه وثقافته (الجعد، والاسمري، ٢٠١٨، ٢٠٤).

تأسيسًا على ما سبق فإن مهارة التحليل تعني القدرة على تحليل البيانات والمعلومات المتاحة عبر الإنترنت بشكل فعال، وفهم مدى صحتها وموثوقيتها وتحليلها بطريقة فعالة. تتضمن هذه المهارة القدرة على فهم وتفسير المعلومات والبيانات المتاحة وإعداد تقارير وتحليلات مفصلة. وتتطلب هذه المهارة تطوير مهارات التفكير النقدي والتحليلي، وتعلم كيفية استخدام الأدوات الرقمية المختلفة.

ج- مهارة التقييم (Evaluation Skills):

وتشير إلى القدرة على تقييم المصادر الرقمية وتحديد مدى موثوقيتها وصحتها وتمييز الأخبار الزائفة (Fake News) والمعلومات الخاطئة. وترتبط مهارة التقييم بالتفكير النقدي، الذي يتطلب استخدام المستويات المعرفية العليا التي أشار إليها تصنيف بلوم، وهي مستويات: التحليل والتركيب والتقويم؛ فالأفراد الذين لديهم تلك المهارة أكثر قدرة على التمييز بين الحقائق التي يمكن إثباتها، والمزاعم غير الحقيقية، وكذلك التمييز بين المعلومات والادعاءات والأسباب المرتبطة بالموضوع، وغير المرتبطة به؛ كما أنهم يتمتعون بالقدرة على تحديد مصداقية مصدر المعلومات؛ وتحري التحيز؛ واتخاذ قرار بشأن المحتوى الرقمي (مكاوي، وآخرون، ٢٠٢١،٥٣٣).

وتوصلت نتائج دراسة يوسف (٢٠١٩، ٢٠٥-٢٠٧) أن طلاب الجامعات يمارسون مهارة التحليل والتقييم من خلال عدة وسائل ومنها:

- **مصدر الخبر:** فهناك العديد من المصادر والصفحات الى لا يثقون فيها، وهناك مصادر وصفحات أخرى يثقون فيها مثل صفحة BBC أو صفحات الجهات الرسمية او الحكومية. وبالتالي ينتبه الشباب الى مصدر الخبر كوسيلة للتحقق منه.
- **البحث عن مصادر أخرى للخبر عبر الإنترنت:** للتأكد منه وذلك إذا كان الخبر مهم بالنسبة لهم، أو الدخول على صفحات الجهات الرسمية أو صفحات الشخص صاحب البوست أو صاحب الخبر.
- **عدد متابعى الصفحة:** ومن الوسائل الأخرى للتحقق من صحة الخبر فإذا كان عدد كبر دل ذلك على أنها من الصفحات الموثوق فيها « أنظر الى عدد متابعي الصفحة، فإن كان كبرًا دل ذلك على مصداقية الصفحة».
- **الخبرات السابقة مع الصفحات أو المواقع:** فكلما كان الفرد لديه خبرات سيئة مع أحد المواقع او الصفحات كلما قلت ثقته في هذه الصفحة أو الموقع.

باستقراء ما سبق فإن تعني القدرة على تقييم المصادر والمنابع الرقمية وتحديد مدى موثوقيتها وصحتها. تتضمن هذه المهارة القدرة على التمييز بين المصادر الموثوقة وغير الموثوقة، وتحديد ما إذا كانت المصادر تعتمد على حقائق أو آراء أو تشكيلات معينة.

د- مهارة انتاج المحتوى (Content Production Skills):

وتشير إلى القدرة على إنتاج المحتوى الإعلامي الرقمي بطريقة مبتكرة وجذابة، واستخدام الأدوات الرقمية المختلفة لإنشاء وتصميم المحتوى الرقمي. حيث أنتجت البيئة الرقمية لمستخدمي وسائل الإعلام الجديدة فرصًا متنوعة ليشاركوا في صناعة المحتوى الرقمي بمختلف أنواعه؛ حيث انتقل هؤلاء المستخدمين من كونهم مستهلكين للمحتوى إلى منتجين له، ومؤثرين في صناعته، وبوجه عام يرتبط مفهوم إنتاج المحتوى الرقمي بامتلاك الحق في التعبير عن الرأي في سياق ثقافي يسمح بالتعددية، وليس بمجرد امتلاك وسائل وأدوات الاتصال فحسب (مكاوي، وآخرون، ٢٠٢١، ٥٣٤)

تأسيسًا على ماسبق فإن مهارة إنتاج المحتوى تعني القدرة على إنشاء المحتوى الإعلامي الرقمي بطريقة مبتكرة وجذابة، وتحتاج هذه المهارة إلى القدرة على استخدام الأدوات الرقمية اللازمة لإنشاء وتصميم المحتوى، وضبط النصوص والصور والفيديو والصوت بشكل مبتكر وجذاب، تتضمن هذه المهارة القدرة على تحليل الجمهور المستهدف وتحديد أفضل الأساليب للتواصل معهم، والقدرة على إنشاء محتوى يتناسب مع احتياجات الجمهور، يمكن تحقيق هذه المهارة من خلال تعلم برامج الإنتاج والتصميم والتحرير، وتطوير مهارات الكتابة والتواصل والإبداع.

باستقراء ما سبق يتبين أن مهارات التربية الإعلامية الرقمية تتضمن مهارة الوصول، ومهارة التحليل، ومهارة التقييم، ومهارة إنتاج المحتوى الإعلامي الرقمي بطريقة مبتكرة وجذابة. وترتبط مهارة الوصول بالقدرة على البحث والوصول إلى المعلومات والمصادر الرقمية المتاحة عبر الإنترنت. وتتعلق مهارة التحليل بالقدرة على تحليل المعلومات والبيانات المتاحة بطريقة فعالة وفهمها وتفسيرها. وتتمثل مهارة التقييم في القدرة على تقييم المصادر الرقمية وتحديد مدى موثوقيتها وصحتها وتمييز الأخبار الزائفة والمعلومات الخاطئة. أما مهارة إنتاج المحتوى الإعلامي الرقمي، فتتعلق بالقدرة على إنتاج محتوى إعلامي رقمي جذاب وذو جودة عالية واستخدام الأدوات الرقمية المختلفة لإنشاء وتصميم المحتوى الرقمي بطريقة احترافية. ويمكن للطلاب في الجامعات تحقيق هذه المهارات من خلال تعلم كيفية استخدام الأدوات الرقمية المختلفة وتحليل البيانات والمصادر المتاحة بشكل فعال، مما يؤدي إلى تنمية الحس النقدي والإبداع والتفكير المستقل في إنتاج المحتوى الإعلامي الرقمي، وتحسين الإدارة الرقمية والتواصل المؤثر عبر الإنترنت. وتعد هذه المهارات حاسمة لنجاح الطلاب في الحياة الأكاديمية والمهنية في عالم اليوم الرقمي

المتطـور، وتسـاعدهم علـى فهـم مصـادر المعلومـات الرقميـة وتحديـد مـدى صـحتها وموثوقيتهـا، وإنتـاج محتـوى إعلامـي رقمـي جـذاب وذو جـودة عاليـة، وتحقيـق التواصـل الفعال مع الآخرين عبر الإنترنت.

المحور الثالث: كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الأمن السيبراني وأساليب تنميتها

يهدف المحور الحالي إلى تحديد كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الأمن السيبراني، وأساليب تنميتها وتحقيقًا لهذا الهدف يتناول المحور عرضًا لمفهوم الكفايات ومكوناتها، وأهم كفايات التربية الإعلامية الرقمية الواجب توافرها لطلاب الجامعات لتنمية ثقافة الامن السيبراني وأساليب تنميتها.

وتعرض الدراسة مفهوم الكفاية لغة ثم اصطلاحا للوصول إلى المقصود بكفايات التربية الإعلامية الرقمية في هذه الدراسة، فالكفاية لغة تعنى (كفى) الشيء يكفى كفاية، فهو كاف إذا حصل به الاستغناء عن غيره، واكتفيت بالشيء أي استغنيت عنه (ابن منظور، ٢٠٠٨).

أما الكفاية اصطلاحًا فقد اختلف الباحثون في تعريفهم للكفاية، فالبعض يرى أنها مجموعة من القدرات وآخرين يرون بأنها تتمثل في المهارات التي يتقنها الفرد وجاءت أبرز تلك التعريفات على النحو التالي:

عرف السيد (٢٠٢١، ١٥٢) الكفاية بأنها: امتلاك المعارف والمهارات التي تساعد الفرد على أداء الأعمال بالشكل المطلوب وتحقيق الأهداف والدوافع.

وأضاف خير الله وجعفر(٢٠٢١، ١٣) للكفاية بأنها: مجموعة المعارف والمهارات والقدرات التي يجب أن يتمتع بها الفرد لأداء مهمته بشكل فعال، سواء كانت هذه المهمة في المجال العملي أو الأكاديمي.

وعرف الرفيعي، والشمري (٢٠٢١، ٤٦٣) الكفاية بأنها: القدرة على أداء العمل بكفاءة وفاعلية.

وأشار ملجا (٢٠٢٢، ٣٥) للكفاية بأنها: إتقان الفرد للمعارف والقدرات والمهارات والاتجاهات بفعالية وكفاءة في الأداء.

وفي ضوء العرض السابق تعرف كفايات التربية الإعلامية الرقمية بأنها: مجموعة المهارات والمعرفة الضرورية التي يحتاجها الطلاب للتعامل بشكل فعال وآمن مع وسائل الإعلام الرقمية وتكنولوجيا المعلومات والاتصالات.

إن ما يميز الكفاية عن القدرة هو كون الكفاية هي التي تحمل المعنى للقدرة، وما يميز القدرة عن الكفاية هو كونها موردًا أساسيًا من بين الموارد الأخرى التي تجعلها تفضي إلى المعالجة المقبولة والفعالة للوضعية. فالكفاية تعطي المعنى للقدرة، والقدرة مؤسسة للكفاية. لذلك لا تكتسب القدرة معنى إلا حين تستدعيها الكفاية مع موارد أخرى لمعالجة الوضعية في سياق اجتماعي غير سياق التعلم، غير أنها تظل خاضعة وتابعة للقدرة باعتبارها موردًا مؤسسًا لها، وتختلف القدرات نفسها عن المهارات، بحيث تستخدم هذه الأخيرة لوصف الأفعال البيداغوجية التي سيقوم بها المتعلم إزاء المضامين المدرسية قصد إنتاج وبناء معارفه الخاصة. وتعتبر بدورها مؤسسة للقدرة، وغالبا غير سياقية، ولا يصبح لها معنى إلا من خلال القدرة التي تشغلها حين بدء الكفاية في معالجة الوضعية (كوجيل، العسري،٢٠٢٠، ٢٣٣).

وتتشكل الكفايات من ثلاثة مكونات أساسية (سالم، وحسن، ٢٠١٨، ٤٢-٤٣):

- **المكونات المعرفية:** وتتضمن المعرفة النظرية والفهم العميق للمفاهيم والمعلومات المتعلقة بالمجال المستهدف، وتشمل القدرة على استخدام اللغة والحساب والعلوم وغيرها من المهارات الأساسية.
- **المكونات الوجدانية:** وتشير إلى الاتجاهات والقيم والمبادئ الأخلاقية والمواقف الإيجابية التي تتصل بالمهام المطلوبة لتحقيق الكفاية، وتشمل الالتزام والثقة بالنفس والأمانة والعواطف الإيجابية التي تشجع على العمل الجاد والمثابرة.
- **المكونات المهارية:** وتتضمن القدرة على تطبيق المعرفة النظرية والمهارات الأساسية بشكل فعال في العمل العملي، وتشمل المهارات اليدوية واللفظية والغير لفظية والاجتماعية والفنية، وتتطلب التدريب والتطوير الدائم لتحسين الأداء.

وعلى ضوء تلك المكونات ووضح برادي (٢٠٢١، ٩٥) أن التربية الاعلامية الرقمية تسعى لتنمية الثلاث مستويات على النحو التالي:

- المجال العقلي: الذي يتجلى في العمليات العقلية مثل المعرفة والفهم والتذكر لمساعدة الفرد في فهم طبيعة البيئة الاعلامية وتحليل مضامينها والحكم عليها.
- المجال الوجداني: حيث يتعلم المتلقي تذوق المادة الاعلامية متجاوزًا الفهم المجرد، وتلمس اتجاهها والقدرة على الاحساس بالقيم المرتبطة بها.

- المجال السلوكي: يرتبط بالممارسة والاتقان والابداع حينئذ يصبح المتلقي فاعلًا في الاعلام عبر الحوار والتعبير عن الذات وانتاج المواد الاعلامية.

في ضوء العرض السابق يتبين أن الكفايات تتكون من ثلاثة مكونات رئيسة هي: المكون المعرفي والمكون الوجداني والمكون المهاري، وتسعى التربية الإعلامية الرقمية لتنمية هذه المكونات لدى الأفراد من خلال: المجال المعرفي الذي يشمل عمليات المعرفة والفهم والتذكر؛ والمجال الوجداني الذي يشمل تذوق المادة الإعلامية واتجاهاتها والقدرة على إدراك قيمها؛ والمجال السلوكي الذي يشمل الممارسة والإتقان والإبداع من خلال التعبير والحوار وإنتاج المواد الإعلامية.

وتعد التربية الإعلامية الرقمية ضرورة ملحة في عصر المعلوماتية، حيث تساعد الأفراد على امتلاك المهارات والكفايات اللازمة للتعامل الفعال والآمن مع وسائل التكنولوجيا الحديثة. وأشار حسن (٢٠١٥، ١١٨-١٢٠) إلى كفايات التربية الإعلامية على النحو التالي:

- الوعي بوسائل الإعلام: حيث يصبح الفرد قادرا على أن يتعرف على قُدرة وسائل الإعلام في حياة الأفراد.
- القدرة على الوصول إلى وسائل الإعلام: وفيه يصبح الفرد قادرًا على الوصول إلى وسائل الإعلام المختلفة، من اجل نشر الرسائل الخاصة به، وهو ما يؤدي لزيادة الوعي بوسائل الإعلام وأسلوب انتشارها مما يودي لقدرة أعمق على التحليل والفهم.
- القدرة على صياغة الرسائل الإعلامية: حيث يتعلم الفرد كيف يتعامل مع وسائل الإعلام وكيفية استخدامها، وكيفية تشارك الرسائل الهادفة والتي غالبًا ما يتم تجاهلها من قبل المجتمع.
- القدرة على تكوين الآراء الخاصة: وذلك فيما يتعلق بالتأثيرات الإيجابية والسلبية الناتجة عن وسائل الإعلام، وقد يتمثل ذلك في: صورة تأييد لوسائل الإعلام التي تُقدم مضامين هادفة، أو الاعتراض على وسائل الإعلام التي تُقدم مضامين غير هادفة، والقدرة على إعداد حملات للتربية الإعلامية تتعلق بمضامين وسائل الإعلام المختلفة، والقدرة على تغيير الرسائل الإعلامية غير المرغوبة.
- القدرة على تحليل الرسائل الإعلامية: وفيه يصبح الفرد قادرًا على مناقشة الأنماط المختلفة والمضامين المتعددة للرسائل الإعلامية، بالإضافة إلى الوعي بنية وسائل الإعلام لإقناع المتلقي.

كما حدد عوف (٢٠٢١، ٢٢٧) أهم مهارات التربية الاعلامية الرقمية على النحو التالي:

مهارة الهوية الرقمية: القدرة على بناء هوية صحيحة وإدارتها عبر الانترنت.

مهارة إدارة وقت الشاشة: القدرة على ادارة وقت الشاشة، وتعدد المهام، وعدم الانخراط في الألعاب عبر الانترنت وسوء استخدام مواقع التواصل الاجتماعي.

مهارة حل المشكلات عبر الانترنت: القدرة على اكتشاف حالات التسلط عبر الانترنت والتعامل معها بحكمة.

مهارات التفكير الناقد: القدرة على التمييز بين المعلومات الحقيقية والخطأ والاتصالات الموثقة والغير آمنة عبر الانترنت.

مهارة التعاطف الرقمي: القدرة على اظهار التعاطف تجاه احتياجات ومشاعر الآخرين على الانترنت.

باستقراء ما سبق فإن التربية الإعلامية الرقمية تُعد ضرورة ملحة في عصر المعلوماتية، حيث تُساعد الأفراد على امتلاك المهارات والكفايات اللازمة للتعامل الفعال والآمن مع وسائل التكنولوجيا الحديثة. وتتضمن هذه التربية العديد من الكفايات التعلمية المهمة مثل الوعي بوسائل الإعلام والقدرة على الوصول إلى وسائل الإعلام وصياغة الرسائل الإعلامية وتكوين الآراء الخاصة وتحليل الرسائل الإعلامية. وتشمل أيضًا مهارات مثل الهوية الرقمية وإدارة وقت الشاشة وحل المشكلات عبر الإنترنت والتفكير الناقد والتعاطف الرقمي.

وتسهم التربية الإعلامية الرقمية في تطوير عديد من الكفايات التعليمية فمن خلالها يمكن للطلاب امتلاك العديد من المهارات والقدرات التي تساعدهم على التعامل مع الوسائل الإعلامية الرقمية بشكل فعال وآمن. ولعل أبرز تلك الكفايات التعليمية مايلي (اتباتو، ٢٠١٩، ١٣٢-١٣٣)، (الشميمري، ٢٠١٠، ٢٦):

- البحث والوصول إلى المعلومات والمصادر الرقمية المتاحة بسهولة.
- فهم الوسائل الاعلامية وتفسيرها، واكتشاف ما تحمله مضامينها من قيم.
- تحليل المعلومات والبيانات بطريقة فعالة وفهمها وتفسيرها بشكل نقدي.
- تقييم المصادر الرقمية وتحديد مدى موثوقيتها وصحتها وتمييز الأخبار الزائفة والمعلومات الخاطئة.
- إنتاج المحتوى الإعلامي الرقمي بطريقة مبتكرة وجذابة واستخدام الأدوات الرقمية المختلفة لإنشاء وتصميم المحتوى الرقمي بطريقة احترافية.

- النشر والتوزيع الفعال للمحتوى الإعلامي الرقمي على الشبكات الاجتماعية والمواقع الإلكترونية المختلفة.
- التواصل بشكل فعال مع الآخرين عبر الإنترنت والعمل بشكل مشترك على تحقيق أهداف محددة.
- حماية البيانات الشخصية والمعلومات الحساسة عبر الإنترنت وتطبيق أفضل الممارسات لتأمين الحسابات الرقمية.
- التفكير النقدي وتقييم المعلومات والبيانات المتاحة، وفهم مصداقية المصادر وتمييز الحقائق من الأخبار الزائفة والإعلام المضلل.
- الإبداع والتفكير بشكل مبتكر لإنشاء المحتوى الإعلامي الرقمي الجذاب والمميز.
- إدارة الوقت والموارد الرقمية بشكل فعال، وتنظيم المحتوى الرقمي والحفاظ على الترتيب والتنظيم الجيد للبيانات والملفات الرقمية.

وفي السياق ذاته أشار (Haque,et al.,2023)، (Al-Abdullatif & Gameil,2020)، (Park, et al., 2020)، (Tetep, 2019) إلى أن كفايات التربية الإعلامية الرقمية لطلاب الجامعات تمثل مجموعة من المهارات والمعرفة التي يحتاجها الطلاب لفهم وتطبيق التكنولوجيا الحديثة والإعلام الرقمي في الحياة اليومية، وتتضمن ما يلي:

- فهم أساسيات تكنولوجيا المعلومات والاتصالات واستخدامها بشكل فعال وآمن.
- قدرة على التعامل مع البيانات الرقمية والتفاعل معها وإدارتها بشكل صحيح.
- القدرة على تقييم جودة المعلومات المتاحة عبر الإنترنت والتحقق من صحتها.
- فهم الأخلاقيات الرقمية وتطبيقها في السلوك الإلكتروني.
- القدرة على العمل الجماعي والتواصل الفعال مع الآخرين عبر وسائل التواصل الاجتماعي والبريد الإلكتروني وغيرها.
- فهم أساسيات الأمن السيبراني والحماية من الهجمات الإلكترونية.

- قدرة على استخدام تقنيات التعلم الإلكتروني والتعليم عن بعد والتعامل مع المنصات الإلكترونية للتعليم.
- القدرة على استخدام البرامج والتطبيقات الرقمية لإنتاج وتعديل ومشاركة المحتوى الرقمي بشكل فعال.

باستقراء ماسبق يتبين أن التربية الإعلامية الرقمية تسعى لتنمية العديد من الكفايات الهامة لدى الطلاب، منها: البحث والوصول إلى المصادر الرقمية، وفهم وتفسير الوسائل الإعلامية واكتشاف القيم المتضمنة في مضامينها، وتحليل البيانات والمعلومات بطريقة نقدية، وتقييم مصادر المعلومات الرقمية ومدى مصداقيتها، وإنتاج المحتوى الرقمي بطريقة مبتكرة، ونشر المحتوى الإعلامي على مختلف المنصات، والتواصل الفعال مع الآخرين عبر الإنترنت، وحماية البيانات الشخصية والحسابات الرقمية، والتفكير النقدي في تقييم المصادر والتمييز بين الحقائق والأخبار الزائفة، والإبداع في إنتاج المحتوى الرقمي، وإدارة الوقت والموارد الرقمية بكفاءة، وتنظيم المحتوى الرقمي.

وترتبط كفايات التربية الإعلامية الرقمية بشكل كبير بالأمن السيبراني، حيث تهدف هذه الكفايات إلى تمكين الطلاب من فهم كيفية استخدام التكنولوجيا بشكل آمن وفعال. ومن خلال تعليم الطلاب كيفية الاستفادة من المصادر الرقمية بشكل صحيح، يمكنهم تجنب الوقوع ضحية للاحتيال الإلكتروني والهجمات السيبرانية. وبالإضافة إلى ذلك، فإن تعزيز الوعي السيبراني يساعد الطلاب على حماية بياناتهم الشخصية وتجنب الوقوع في فخ التصيد الاحتيالي والهجمات الإلكترونية.

وأشار كل من (Alharbi & Tassaddiq, 2021)، (Kori & Naik, 2023) إلى مهارات الأمن السيبراني اللازمة لطلاب الجامعات على النحو التالي:

- الوعي بالأخطار والتهديدات الإلكترونية والمخاطر المحتملة.
- أخلاقيات السلوك الآمن على الشبكة والحفاظ على الخصوصية.
- استخدام كلمات السر وعبارات أمنية قوية وتغييرها دوريا.
- عدم فتح الروابط المشبوهة أو المرفقات غير المطلوبة.
- تثبيت برامج الأمن والحماية وتحديثها دوريا.
- فحص الأجهزة بشكل دوري للكشف عن البرامج والفيروسات الضارة.
- استخدام شبكات VPN للوصول إلى شبكات غير آمنة.
- إبلاغ إدارة الجامعة فورًا عن المخاطر والهجمات الإلكترونية.

- التدريب المستمر للوقوف على آخر التطورات والتقنيات في مجال الأمن السيبراني.
- وفي نفس الصدد أضاف نوردان Nordan (٢٠٢٣، ٣٧-٤٠) كفايات الأمن السيبراني اللازمة لطلاب الجامعات على النحو التالي:
- القدرة على الكشف المبكر عن الهجمات الإلكترونية والتصدي لها.
- فهم أساليب القرصنة الإلكترونية وكيفية تجنبها.
- التعرف على التقنيات السحابية الآمنة وكيفية استخدامها.
- القدرة على إجراء تحليل أمني للأنظمة والشبكات، واقتراح حلول لتعزيز الأمان.
- التدريب على كيفية الاستجابة لحوادث الأمن السيبراني وإدارتها.
- توظيف مهارات التفكير الناقد وحل المشكلات للتعامل مع التحديات الأمنية.
- وحدد كل من (Alharbi & Tassaddiq, 2021)، (Mai & Tick,2021)، (Alqahtani,2022) أساليب تنمية ثقافة الأمن السيبراني لطلاب الجامعات ويمكن تلخيصها في الشكل التالي:

شكل (1)

أساليب تنمية ثقافة الأمن السيبراني لطلاب الجامعات

المصدر: اعداد الباحثة

- **التوعيــة والتثقيــف:** يتمثل هذا الأسلوب في تنظيم حملات توعية وإطلاق مبادرات تثقيفية للطلاب حول المخاطر الإلكترونية وكيفية حماية البيانات الشخصية على الإنترنت، وذلك عن طريق إجراء ندوات وورش عمل ومحاضرات توعوية للطلاب حول أهمية الحفاظ على الخصوصية والأمن الإلكتروني.
- **البرامج التدريبيــة:** يتمثل هذا الأسلوب في تصميم برامج تدريبية لتعريف الطلاب بالمخاطر والتهديدات الإلكترونية وكيفية الوقاية منها، وتوفير منصات تعليم إلكترونية متاحة للطلاب لتعلم مهارات الأمن السيبراني.
- **التوجيه والإرشاد:** يتمثل هذا الأسلوب في توجيه الطلاب في حال وقوع أي انتهاك للبيانات الشخصية إلى الجهات المختصة للتحقيق في مثل هذه الانتهاكات، وتوفير دليل إرشادي للطلاب حول كيفية التعامل مع الخروقات الأمنية.
- **استخدام منصات التعلم الإلكتروني:** يتمثل هذا الأسلوب في استخدام منصات التعلم الإلكتروني لتوفير مقررات إلكترونية تتضمن معلومات عن كيفية بناء سلوكيات آمنة على الشبكة، وتوفير الدعم الفني للطلاب في حال وجود مشاكل أمنية.
- **نشر الوعي:** يتمثل هذا الأسلوب في نشر الوعي بأهمية اتباع سلوكيات آمنة على الإنترنت، مثل اختيار كلمات مرور قوية وتغييرها بشكل مستمر وتجنب فتح الروابط المشبوهة، وذلك عن طريق توفير مواد تثقيفية متاحة للطلاب.
- **تزويد الطلاب بالمعرفة والمهارات التقنية:** يتمثل هذا الأسلوب في تزويد الطلاب بالمعرفة والمهارات التقنية اللازمة لمواجهة تهديدات الفضاء الإلكتروني، بما في ذلك مهارات استخدام أدوات حماية الخصوصية وبرامج مكافحة الفيروسات

وتأسيسًا على ما سبق تصنف الدراسة الحالية أهم كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الأمن السيبراني إلى عدة مجالات، وذلك على النحو التالي:

شكل (2)

كفايات التربية الإعلامية الرقمية اللازمة لطلاب الجامعات لتنمية ثقافة الامن السيبراني

المصدر: اعداد الباحثة

وفيما يلي العرض بالتفصيل:

١. **كفايات البحث الرقمي:** وتشمل القدرة على الوصول إلى المعلومات الرقمية الصحيحة والموثوقة، واستخدام الأدوات الرقمية للوصول إليها بطريقة فعالة ومناسبة، وتقييم جودة المصادر وموثوقيتها. وتتضمن أيضًا استخدام محركات البحث بشكل فعال وتحديد المصادر الرقمية الموثوقة، وتطوير مهارات البحث الفعال على الإنترنت وتحليل المعلومات والبيانات المتاحة، وتحديد المصادر الموثوقة والمفيدة وتجنب الأخبار الزائفة والمعلومات الخاطئة.

٢. **كفايات تحليل المعلومات والبيانات الرقمية:** تتضمن القدرة على فهم وتحليل البيانات والمعلومات الرقمية بطريقة فعالة وإعداد تقارير مفصلة. وتشمل هذه الكفاية أيضًا استخدام البرامج والأدوات الرقمية المختلفة لتحليل البيانات والمعلومات، فضلًا عن التحليل النقدي للمعلومات والبيانات المتاحة وتقييم مدى صحتها وموثوقيتها.

٣. **كفايات إنتاج المحتوى الإعلامي الرقمي:** وتعني القدرة على إنتاج وإدارة المحتوى الرقمي بطريقة فعالة وجذابة واستخدام أدوات الإنتاج الرقمية المختلفة لإنتاج المحتوى الإعلامي المتنوع بما في ذلك الصوتي والمرئي والنصي. تشمل هذه الكفاية استخدام الأدوات والبرامج الرقمية المختلفة لإنتاج المحتوى الإعلامي الرقمي، وتحسين مهارات الكتابة وتصميم الصور والفيديو وإنتاج المحتوى الإعلامي الجذاب والفعال. كما تشمل هذه الكفاية فهم مبادئ التسويق الرقمي واستخدامها لجذب المستخدمين وزيادة الوعي

بالعلامة التجارية، وتحديد الجمهور المستهدف وإنتاج المحتوى المناسب لهذا الجمهور، وإدارة المحتوى الرقمي بشكل فعال.

٤. **كفايات التواصل الالكتروني:** تعني القدرة على التواصل والتفاعل بشكل فعال مع الآخرين عبر الوسائط الرقمية، وتشمل القدرة على استخدام وسائل التواصل الاجتماعي والبريد الإلكتروني والدردشة الصوتية والمرئية وغيرها من الوسائل الرقمية للتواصل والتفاعل بشكل فعال.

٥. **كفايات الأمان الالكتروني والخصوصية:** تعني القدرة على حماية البيانات الشخصية والخصوصية على الإنترنت والتعرف على المخاطر الرقمية المختلفة والقدرة على تفاديها. تشمل هذه الكفاية فهم مخاطر الأمن الإلكتروني والخطوات الوقائية لتجنبها، مثل استخدام كلمات المرور الآمنة والتحقق من صحة الروابط والمرفقات وتحديث البرامج الأمنية بشكل منتظم. كما تتضمن هذه الكفاية استخدام أدوات الأمان الرقمية المختلفة لحماية البيانات الشخصية وتأمين الحسابات الرقمية، مثل استخدام برامج مكافحة الفيروسات والبرامج الحماية والتحقق من صحة شهادات الأمان عند إجراء المعاملات الحساسة على الإنترنت. ويشمل ذلك أيضًا التعامل مع المعلومات الحساسة بحذر والابتعاد عن المواقع والتطبيقات غير الموثوق بها، وتأمين النسخ الاحتياطي من البيانات الحساسة لتجنب فقدانها.

٦. **كفايات التعلم الرقمي:** وتعني القدرة على التعلم والتطور في بيئة رقمية واستخدام التقنيات الرقمية المختلفة لتعلم مواضيع جديدة وتنمية المهارات والمعرفة. وتشمل هذه الكفاية استخدام التقنيات المتاحة للتعلم عن بعد والتعلم الإلكتروني بشكل فعال، وتحسين مهارات التعلم الإلكتروني والتعامل مع منصات التعليم الإلكتروني. كما تشمل هذه الكفاية فهم مفهوم التعليم الإلكتروني وتطبيق أفضل الممارسات والأساليب الفعالة لتحقيق النتائج المرجوة، مثل تحديد الأهداف وتنظيم الوقت وتنظيم المواد الدراسية وتفاعل مع المحتوى الرقمي بشكل فعال.

٧. **كفايات التفكير النقدي والانتاج الإبداعي:** وتعني القدرة على التفكير بطريقة إبداعية وإنتاج المحتوى الرقمي بطريقة فريدة ومبتكرة واستخدام الأدوات الرقمية المختلفة لإنتاج المحتوى الإبداعي بما في ذلك الصوتي والمرئي والنصي. تشمل هذه الكفاية تحسين مهارات التفكير النقدي والتقييم النقدي للمعلومات والبيانات المتاحة، وتطوير القدرة على التفكير الإبداعي والإنتاج الإبداعي للمحتوى الإعلامي الرقمي، وتطوير مهارات التحليل

النقدي والتفكير النقدي والتعلم الذاتي. وتتضمن هذه الكفاية أيضًا القدرة على استخدام الأدوات الرقمية المختلفة لإنتاج المحتوى الإبداعي، مثل برامج التحرير الصوتي والفيديو والتصميم الجرافيكي والتصوير الفوتوغرافي والرسوم البيانية.

في ضوء العرض السابق فإن هذه الكفايات تتيح للطلاب الاستفادة من الفرص التعليمية والمهنية المتاحة في عالم اليوم الرقمي المتطور، وتمكنهم من التعامل بشكل فعال مع التقنيات والأدوات الرقمية المتنوعة والتفاعل مع الآخرين عبر الإنترنت بطريقة آمنة ومسؤولة. كما تساعد هذه الكفايات على تحسين مستوى الإبداع والتفكير المستقل وتنمية الحس النقدي والقدرة على تحليل المعلومات والبيانات بطريقة فعالة. وتعتبر هذه الكفايات أساسية للنجاح في سوق العمل المتنافس في العصر الحديث، حيث يتطلب العمل في مجالات مختلفة القدرة على التعامل مع التقنيات الحديثة وإنتاج المحتوى الإعلامي الرقمي بشكل جذاب وفعال، وتواصل فعال مع الآخرين عبر الإنترنت، وتحقيق التحليل النقدي وتقييم المصادر المتاحة. لذلك، فإن تعلم هذه الكفايات يعد أمرًا حيويًا لنجاح الطلاب في مختلف المجالات الأكاديمية والمهنية في العالم الرقمي المتطور.

المحور الرابع: إجراءات الدراسة الميدانية وتحليل وتفسير نتائجها

تناول الإطار النظري للدراسة عرضًا لماهية الأمن السيبراني بالجامعات، والإطار المفاهيمي للتربية الاعلامية الرقمية بالجامعات، وحدد العلاقة بين الأمن السيبراني لطلاب الجامعات المصرية والتربية الإعلامية الرقمية، وللوقوف على الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية وأساليب تنميتها، الأمر الذي يتطلب النزول إلى أرض الواقع وإجراء دراسة ميدانية تتضمن أهداف، وأداة يتم حساب صدقها وثباتها، ثم تطبيقها على عينة الدراسة، وأخيرًا التوصل إلى نتائج وتفسيرها وتحليلها، ويمكن عرض ذلك بالتفصيل كما يأتي:

أولًا: إجراءات الدراسة الميدانية:

أهداف الدراسة الميدانية:

- تعرف الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية.
- الوقوف على أساليب تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية.

واستخدمت الباحثة الاستبانة كأداة لجمع البيانات، وفيما يلي الأسس التي بنيت عليها:

- الرجوع إلى الدراسات العربية والأجنبية التي تناولت الأمن السيبراني والجامعات، والدراسات التي تناولت التربية الاعلامية الرقمية والجامعات، للاستفادة منها في تحديد المجالات والبنود المختلفة.
- الوقوف على ماهية الأمن السيبراني بالجامعات، وهذا ما تناوله المحور الأول من الدراسة.
- تعرف الإطار المفاهيمي للتربية الاعلامية الرقمية بالجامعات، وهذا ما تناوله المحور الثاني من الدراسة.
- تحديد مؤشرات العلاقة بين الأمن السيبراني لطلاب الجامعات المصرية والتربية الإعلامية الرقمية، وهذا ما تناوله المحور الثالث من الدراسة.
- آراء الخبراء في مجال التربية حول استبانة عن الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية وأساليب تنميتها، وهذا ما تناوله المحور الرابع من الدراسة.
- آراء عينة من الطلاب بكليات (التربية، التجارة وإدارة الأعمال، السياحة والفنادق) جامعة حلوان، حول مدى توافر كل عبارة تضمنها الاستبانة، وهذا ما تناوله المحور الرابع من الدراسة.

- أداة الدراسة:

الاستبانة:

استخدمت الدراسة الاستبانة على النحو التالي:

لتحقيق أهداف الدراسة الميدانية وجهت استبانة إلى عينة من طلاب جامعة حلوان وتتكون الاستبانة من محورين هما:

- المحور الأول: الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية.
- المحور الثاني: أساليب تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية.

ويندرج تحت كل محور عدة عبارات فرعية وفي نهاية كل محور سؤال مفتوح عن أي ملاحظات أخرى يمكن إضافتها، وروعي أن تكون الإجابة عن عبارات الاستبانة بوضع علامة (✓) أمام كل عبارة في المستوى المناسب من مستويات الإجابة.

وتم استخدام مقياس تقدير من ثلاثة مستويات (متوفر بدرجة كبيرة، متوفر بدرجة متوسطة، غير متوفر).

صدق الاستبانة

يقصد بالصدق أن تقيس الأداة ما وضعت لقياسه فلا تقيس شيئا غيره أو بالإضافة إليه (حمود، ٢٠٢٣)، لذا قامت الباحثة بعرض الاستبانة على السادة المحكمين من الخبراء والمتخصصين في مجال التربية والإدارة التعليمية (انظر ملحق (١))، للتأكد من مدى ملائمة الاستبانة للغرض التي وضعت من اجله، ومدى وضوح العبارات وسلامة صياغتها، ومدى انتمائها لمحاور الاستبانة، وإبداء الرأي بالتعديل أو الحذف أو الإضافة.

وبعد إجراء التعديلات المقترحة من السادة المحكمين بتعديل بعض العبارات، وإضافة بعضها وحذف أخرى أصبحت الاستبانة في صورتها النهائية (انظر ملحق (٢)) واشتملت على محورين على النحو التالي:

المحور الأول: الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية. ويتضمن (٧) كفايات تشمل (٤٦) عبارة فرعية على النحو التالي:

- كفايات البحث الرقمي وتتضمن (٥) عبارات فرعية.
- كفايات تحليل المعلومات والبيانات الرقمية وتشمل (٥) عبارات فرعية.
- كفايات إنتاج المحتوى الإعلامي الرقمي وتتضمن (٧) عبارات فرعية.
- كفايات التواصل الالكتروني وتتضمن (٧) عبارات فرعية.
- كفايات الأمان الالكتروني والخصوصية وتشمل (١٠) عبارات فرعية.
- كفايات التعلم الرقمي وتشمل (٦) عبارات فرعية.
- كفايات التفكير النقدي والانتاج الإبداعي وتتضمن (٦) عبارات فرعية.

المحور الثاني: أساليب تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية. وتتضمن (٦) عبارات فرعية.

ثبات الاستبانة:

تم حساب معامل ثبات الاستبانة من خلال استخدام معامل ألفا كرونباخ على برنامج SPSS، حيث بلغ معامل ثبات الاستبانة الخاصة بالواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية وأساليب

تنميتها (٠,٩٦) مما يشير إلى تمتع الأداة بمعامل ثبات عالي مما يطمئن إلى استخدام أداة الدراسة.

عينة الدراسة:

بعد الحصول على التصريحات والموافقات الإدارية الخاصة بتطبيق الاستبانة من الجهات المعنية (انظر ملحق (٣)). تم تطبيق الاستبانة على (٤٠٠) طالبًا من كليات (التربية، التجارة وإدارة الأعمال، السياحة والفنادق) جامعة حلوان، حيث تم استبعاد (٥٣) استبانة لأن بياناتها غير مكتملة ليصبح إجمالي الاستبانات الصحيحة (٣٤٧) استبانة.

المعالجة الإحصائية:

قامت الباحثة بإجراء المعالجة الإحصائية للبيانات من خلال استخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS)، واستخدمت الدراسة أساليب المعالجة الإحصائية الآتية:

- **التكرارات والنسب المئوية:** بهدف تحديد استجاباتهم حول مدى أهمية كل عبارة من عبارات الاستبانة والنسبة المئوية لتلك التكرارات.
- **المتوسط المرجح:** لتعرف ترتيب العبارات وفقا لأهميتها.
- **الانحراف المعياري:** لقياس مدى التشتت في إجابات العينة إزاء كل عبارة من عبارات الاستبانة.

ثانياً: **تحليل النتائج وتفسيرها**

نتائج المحور الأول: الواقع الحالي لثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية. ويتضمن (٧) كفايات تشمل (٤٦) عبارة فرعية على النحو التالي:

١-كفايات البحث الرقمي:

جدول (١)

استجابات أفراد عينة الدراسة المتعلقة بكفايات البحث الرقمي

م	العبارة	درجة التوافر						المتوسط	الانحراف	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
١	أتجنب تنزيل الملفات والبرامج غير الموثوق بها عبر الإنترنت.	٨١	٢٣,٣٤	١٧٩	٥١,٥٨	٨٧	٢٥,٠٧	١,٩٨	٠,٦٩٦	٤
٢	أتوخى الحذر عند تبادل الملفات والصور مع الآخرين عبر الإنترنت.	١١٣	٣٢,٥٦	١٦٦	٤٧,٨٣	٦٨	١٩,٥٩	٢,١٢	٠,٧١١	٣
٣	استخدم المصادر الموثوقة في البحث عن المعلومات	١٩٤	٥٥,٩٠	٩٧	٢٧,٩٥	٥٦	١٦,١٣	٢,٣٩	٠,٧٥٠	١

م	العبارة	درجة التوافر						المتوسط	الانحراف	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	المهمة.									
٤	أميز بين مواقع الويب الموثوقة وغير الموثوقة.	١٣٥	٣٨,٩٠	١٦٤	٤٧,٢٦	٤٨	١٣,٨٣	٢,٢٥	٠,٦٨٢	٢
٥	أتعرف على هجمات الخداع وتقنيات الاحتيال الإلكتروني الشائعة.	٥٢	١٤,٩٨	٢٣١	٦٦,٥٧	٦٤	١٨,٤٤	١,٩٦	.٥٧٧	٥

يتضح من الجدول السابق أن المتوسطات المرجحة لاستجابات أفراد العينة تراوحت ما بين (١,٩٦-٢,٣٩) وبانحراف معياري ما بين (٠,٥٧٧-٠,٧٥٠)

تصدرت العبارة (٣) والتي تنص على "**استخدم المصادر الموثوقة في البحث عن المعلومات المهمة**" المرتبة الأولي بمتوسط مرجح قدره (٢,٣٩) وقد يعزي ذلك إلى أن البحث الأكاديمي يتطلب استخدام مصادر موثوقة للحصول على معلومات دقيقة وصحيحة، وهذا يعد أمرًا حيويًا لإتمام عملهم الأكاديمي (الأبحاث، المشاريع، والمقالات الأكاديمية) بنجاح. كما أن استخدام مصادر غير موثوقة يمكن أن يؤدي إلى تضخم المعلومات والبيانات الخاطئة، ومن ثم يؤثر على المصداقية وجودة العمل الأكاديمي.

وجاءت العبارة (٥) والتي تنص على "**أتعرف على هجمات الخداع وتقنيات الاحتيال الإلكتروني الشائعة**" بمتوسط مرجح قدره (١,٩٦) في المرتبة الأخيرة وربما يعزى ذلك إلى

ضعف الوعي الكافي للطلاب بأهمية هذه المهارات ومخاطر الهجمات الالكترونية، بالإضافة إلى ضعف تضمين هذه المهارات ضمن برامج المناهج الدراسية بشكل كاف. **وتتفق هذه النتيجة مع دراسة الحبيب (٢٠٢٢)** نقص وعي الطلاب بجرائم الأمن السيبراني، مما يشير لأهمية الاطلاع الواسع على جرائم الأمن السيبراني بأنواعه المتعددة وأشكاله المتجددة لعدة الوقوع ضحية لتلك الجرائم.

٢-كفايات تحليل المعلومات والبيانات الرقمية:

جدول (٢)

استجابات أفراد عينة الدراسة المتعلقة بكفايات تحليل المعلومات والبيانات الرقمية

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
١	أحلل البيانات والمعلومات الرقمية بدقة.	١١١	٣١,٩٨	١٥٣	٤٤,٠٩	٨٣	٢٣,٩١	٢,٠٨	٠,٧٤٤	٤
٢	أعد تقارير مفصلة عن البيانات والمعلومات المحللة.	٩٦	٢٧,٦٦	٢٢٣	٦٤,٢٦	٢٨	٨,٠٦	٢,١٩	٠,٥٦٥	٣
٣	أصمم استبيانات واستطلاعات لجمع البيانات	١٧٢	٤٩,٥٦	١١٧	٣٣,٧١	٥٨	١٦,٧١	٢,٣٢	٠,٧٤٥	١

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	وتحليلها.									
٤	استخلص المعاني الصحيحة والاستنتاجات السليمة من البيانات.	٦٥	١٨,٧٣	١٨٧	٥٣,٨٩	٩٥	٢٧,٣٧	١,٩١	٠,٦٧٤	٥
٥	استخدم البرامج والأدوات الرقمية المختلفة لتحليل البيانات والمعلومات	١٣٦	٣٩,١٩	١٥٨	٤٥,٥٣	٥٣	١٥,٢٧	٢,٢٣	٠,٦٩٩	٢

يتضح من الجدول السابق أن المتوسطات المرجحة لاستجابات أفراد العينة تراوحت ما بين (١,٩١-٢,٣٢) وبانحراف معياري ما بين (٠,٥٦٥-٠,٧٤٥)

تصدرت العبارة (٣) والتي تنص على "**أصمم استبيانات واستطلاعات لجمع البيانات وتحليلها**" المرتبة الأولى بمتوسط مرجح قدره (٢,٣٢) وربما يعزى ذلك إلى أن الاستبيانات والاستطلاعات يمكن تصميمها بسهولة باستخدام العديد من الأدوات المجانية المتاحة عبر الإنترنت، ويعكس تصدرها المرتبة الأولى استخدام الطلاب لها بشكل واسع في مشاريع التخرج والأبحاث الأكاديمية.

أما العبارة (٤) والتي تنص على "**استخلص المعاني الصحيحة والاستنتاجات السليمة من البيانات**" فجاءت في المرتبة الأخيرة بمتوسط مرجح قدره (١,٩١) وربما

يعزى ذلك إلى أنها تتطلب مهارات تحليلية عالية وفهمًا عميقًا للبيانات والمعلومات المتاحة، وقد يكون هذا صعبًا بعض الشيء للطلاب المبتدئين أو الذين لا يمتلكون خبرة كافية في مجال التحليل الإحصائي. كما أن استخلاص المعاني الصحيحة والاستنتاجات السليمة يتطلب عادةً دراسة أكثر تفصيلًا وتحليل أكثر دقة، وقد يتطلب الاستعانة بمهنيين أو خبراء في هذا المجال. وتتفق هذه النتيجة مع دراسة **(Onyema, et al., 2021)** التي توصلت إلى ضعف المعرفة بمجالات الحوسبة الأساسية، ونقص الموجهين ذوي الخبرة العملية، ونقص التدريب السيبراني.

٣-كفايات إنتاج المحتوى الإعلامي الرقمي:

جدول (3)

استجابات أفراد عينة الدراسة المتعلقة كفايات إنتاج المحتوى الإعلامي الرقمي

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
١	**أتجنب نشر المحتوى الذي يحض على الكراهية وأي شكل من أشكال التمييز الاجتماعي.**	١٣١	٣٧,٧٥	١٥٨	٤٥,٥٣	٥٨	١٦,٧١	٢,٢١	٠,٧٠٨	١
٢	أتحقق من مصداق	١٤٩	٤٢,٩٣	٨٧	٢٥,٠٧	١١١	٣١,٩٨	٢,١٠	٠,٨٥٩	٣

	ية المحتوى الرقمي قبل مشاركته مع الآخرين .								
٣	**أتابع إرشادات وسائل التواصل الاجتماعي والقوانين المتعلقة بنشر المحتوى الرقمي.**	١١٩	٣٤,٢٩	١٥٥	٤٤,٦٦	٧٣	٢١,٠٣	٢,١٣	٠,٧٣٣	٢
٤	**أحرص على تحليل احتياجات الجمهور المستهدف لإنتاج المحتوى الإعلامي الملائم**	٤٦	١٣,٢٥	٢٧٦	٧٩,٥٣	٢٥	٧,٢٠	٢,٠٦	٠,٤٤٨	٥

	لها.								
٥	يمكنني إنشاء صفحة وادارتها على مواقع التواصل الاجتماعي بفاعلية.	١٠٥	٣٠,٢٥	١٥١	٤٣,٥١	٩١	٢٦,٢٢	٢,٠٤	٠,٧٥١	٦
٦	استخدم الأدوات والبرامج الرقمية المختلفة لإنتاج محتوى إعلامي رقمي متنوع.	٩٦	٢٧,٦٦	١٦٣	٤٦,٩٧	٨٨	٢٥,٣٦	٢,٠٢	٠,٧٢٨	٧
٧	التزم بالمعايير الأخلاقية التي تنظم نشر المحتوى على مواقع	٧٢	٢٠,٧٤	٢٣١	٦٦,٥٧	٤٤	١٢,٦٨	٢,٠٨	٠,٥٧٣	٤

	التواصل الاجتماعي.									

يتضح من الجدول السابق أن المتوسطات المرجحة لاستجابات أفراد العينة تراوحت ما بين (٢,٠٢-٢,٢١) وبانحراف معياري ما بين (٠,٤٤٨-٠,٨٥٩)

تصدرت العبارة (١) والتي تنص على "**أتجنب نشر المحتوى الذي يحض على الكراهية أي شكل من أشكال التمييز الاجتماعي**" المرتبة الأولى بمتوسط مرجح قدره (٢,٢١) وربما يعزى ذلك إلى الوعي الأخلاقي والقانوني للطلاب، والتزامهم بالقيم الإنسانية والاجتماعية المتعارف عليها، وكذلك احترامهم للسياسات والقواعد التي تفرضها وسائل التواصل الاجتماعي، والتي تحظر نشر المحتوى الذي يحض على الكراهية والتمييز الاجتماعي. بالإضافة إلى الوعي بأهمية الحوار والاحترام المتبادل بين الأفراد في المجتمع، وتأثير الكراهية والتمييز الاجتماعي على النسيج الاجتماعي والاقتصادي والسياسي للمجتمع.

وجاءت العبارة (٦) والتي تنص على "**استخدم الأدوات والبرامج الرقمية المختلفة لإنتاج محتوى إعلامي رقمي متنوع**" المرتبة الأخيرة بمتوسط مرجح قدره (٢,٠٢) وربما يعزى ذلك إلى قلة الاهتمام بتدريب الطلاب على استخدام الأدوات والبرامج الرقمية المختلفة لإنتاج المحتوى الإعلامي الرقمي، مما يؤدي إلى قلة الخبرة والمهارات اللازمة لإنتاج محتوى إعلامي رقمي عال الجودة. بالإضافة إلى ضعف توافر الدعم الفني والتقني الكافي للطلاب لحل المشاكل والصعوبات التي يمكن أن تواجههم أثناء استخدام الأدوات والبرامج الرقمية المختلفة. الأمر الذي يعكس الحاجة للتركيز على توفير الأدوات والبرامج الرقمية المناسبة للطلاب وتدريبهم على استخدامها بشكل فعال، وتوفير الدعم الفني والتقني الكافي لهم. **وتتفق هذه النتيجة مع دراسة (كردي، ٢٠٢١)** والتي توصلت إلى نقص المهارات التقنية اللازمة لتنفيذ التعليم الإلكتروني بكفاءة، ضعف جودة التعليم وفعاليته في البيئة الافتراضية.

٤- كفايات التواصل الالكتروني:

جدول (٤)

استجابات أفراد عينة الدراسة المتعلقة كفايات التواصل الالكتروني

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
١	أعبر عن أفكاري وآرائي بوضوح في مواقع التواصل الاجتماعي.	٥٨	١٦,٧١	٢٣٥	٦٧,٧٢	٥٤	١٥,٥٦	٢,٠١	٠,٥٦٨	٧
٢	استخدم التطبيقات المختلفة للتواصل مع الزملاء والأساتذة في الجامعة بشكل فعال.	١٤٤	٤١,٤٩	١١٦	٣٣,٤٢	٨٧	٢٥,٠٧	٢,١٦	٠,٨٠٠	٣
٣	أتبادل الأفكار والمعلوما ت مع الآخرين عن بُعد باستخدام التقنيات الحديثة.	٤٧	١٣,٥٤	٢٨٢	٨١,٢٦	١٨	٥,١٨	٢,٠٨	٠,٤٢٥	٥

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
٤	استخدم اللغة اللائقة في التواصل الإلكتروني مع الآخرين.	١٢١	٣٤,٨٧	١٥٢	٤٣,٨٠	٧٤	٢١,٣٢	٢,١٣	٠,٧٣٨	٤
٥	أخصص وقت مناسب للتفاعل مع مواقع التواصل الاجتماعي .	٧٧	٢٢,١٩	٢٠٢	٥٨,٢١	٦٨	١٩,٥٩	٢,٠٢	٠,٦٤٦	٦
٦	أحرص على عدم مشاركة أي معلومات شخصية مع أشخاص غير معروفين على	١٥٣	٤٤,٠٩	١٤٢	٤٠,٩٢	٥٢	١٤,٩٨	٢,٩١	٠,٧١٢	١

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	الإنترنت.									
٧	**أتجنب الرد على الرسائل غير المرغوب فيها في البريد الالكتروني**	١٤٨	٤٢,٦٥	١٥١	٤٣,٥١	٤٨	١٣,٨٣	٢,٢٨	٠,٦٩٥	٢

يتضح من الجدول السابق أن المتوسطات المرجحة لاستجابات أفراد العينة تراوحت ما بين (٢,٠١-٢,٩١) وبانحراف معياري ما بين (٠,٤٢٥-٠,٨٠٠)

تصدرت العبارة (٦) والتي تنص على "**أحرص على عدم مشاركة أي معلومات شخصية مع أشخاص غير معروفين على الإنترنت**" المرتبة الأولى بمتوسط مرجح قدره (٢,٩١) وربما يعزى ذلك إلى الوعي المتزايد لدى طلاب الجامعة حول أهمية الحفاظ على الخصوصية الشخصية عند استخدام الإنترنت والتواصل مع الآخرين عبر الشبكة. فالعديد من الأشخاص يدركون الآن خطورة مشاركة المعلومات الشخصية مع الغرباء، مثل الاسم الكامل وتاريخ الميلاد ورقم الهاتف والعنوان ومعلومات الحسابات المصرفية، حيث يمكن استخدام هذه المعلومات في الاحتيال على المستخدمين أو الاستيلاء على هويتهم الشخصية. وبالتالي، يحرص الطلاب على توخي الحذر وعدم مشاركة أي معلومات شخصية مع الأشخاص غير المعروفين على الإنترنت.

جاءت العبارة (١) والتي تنص على "**أعبر عن أفكاري وآرائي بوضوح في مواقع التواصل الاجتماعي**" المرتبة السابعة بمتوسط مرجح قدره (٢,٠١) وربما يعزى ذلك إلى أنه قد يشعر الطلاب بالحذر في التعبير عن آرائهم وأفكارهم بشكل واضح عبر مواقع التواصل الاجتماعي، حيث يمكن أن يواجهوا انتقادات أو ردود فعل سلبية من قبل المستخدمين الآخرين. كما يمكن أن يكون هناك خوف من التعرض للتنمر أو الهجوم الشخصي. بالإضافة إلى ذلك، قد يشعر الطلاب بالقلق بشأن تأثير تعبيرهم وآرائهم على

مستقبلهم الوظيفي أو الأكاديمي، ولذلك فإنهم يفضلون تجنب التعبير عن آرائهم بشكل واضح على مواقع التواصل الاجتماعي.

٥- كفايات الأمان الالكتروني والخصوصية:

جدول (٥)

استجابات أفراد عينة الدراسة المتعلقة بكفايات الأمان الالكتروني والخصوصية

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
١	أفحص جهاز الكمبيوتر بشكل دوري للتخلص من الفيروسات والبرامج الضارة.	١٧٩	٥١,٥٨	١٣١	٣٧,٧٥	٣٧	١٠,٦٦	٢,٤٠	٠,٦٧٥	١
٢	أتوخى الحذر عند تحميل وتنزيل البرامج والتطبيقات من مصادر غير موثوقة.	٨٧	٢٥,٠٧	٢٣١	٦٦,٥٧	٢٩	٨,٣٥	٢,١٦	٠,٥٥٤	٧

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
٣	استخدم برامج مكافحة الفيروسات والبرامج الضارة لحماية أجهزتي الخاصة من الهجمات والاختراقات على مواقع التواصل الاجتماعي.	١٥٥	٤٤,٦٦	١٤٣	٤١,٢١	٤٩	١٤,١٢	٢,٣٠	٠,٧٠٤	٣
٤	احرص على استخدام كلمات مرور قوية وتغييرها بشكل دوري.	٦٢	١٧,٨٦	١٨١	٥٢,١٦	١٠٤	٢٩,٩٧	١,٨٧	٠,٦٨١	١٠
٥	أقوم	١١	٣٣,٧	٢٠	٥٩,٣	٢٤	٦,٩١	٢,٢٦	٠,٥٧٩	٤

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	بالإبلاغ عن المضامين الرقمية التي تهدد أمن الوطن واستقراره.	٧	١	٦	٦					
٦	أحرص على الالتزام بالقوانين والأنظمة المعمول بها في استخدام مواقع التواصل الاجتماعي.	٩٨	٢٨,٢٤	١٩٤	٥٥,٩٠	٥٥	١٥,٨٥	٢,١٢	٠,٦٥٣	٨
٧	استخدم ميزات الحماية المتوفرة مثل المصادقة الثنائية والإشعارا	١٣٨	٣٩,٧٦	١٣٥	٣٨,٩٠	٧٤	٢١,٣٢	٢,١٨	٠,٧٦٠	٦

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	ت عند تسجيل الدخول من أجهزة غير معروفة.									
٨	استخدم شبكات الإنترنت العامة الآمنة والمشفرة عند الاتصال بالإنترنت في الأماكن العامة.	٦٥	١٨,٧٣	٢١٩	٦٣,١١	٦٣	١٨,١٥	٢	٠,٦٠٨	٩
٩	أبلغ عن أي محتوى رقمي مسيء أو غير لائق.	١٥٦	٤٤,٩٥	١٢٤	٣٥,٧٣	٦٧	١٩,٣٠	٢,٢٥	٠,٧٦٠	٥
١٠	أحرص على حماية	١٦٢	٤٦,٦٨	١٤٩	٤٢,٩٣	٣٦	١٠,٣٧	٢,٣٦	٠,٦٦٣	٢

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	بياناتي الشخصية وعدم مشاركتها مع أي شخص غير موثوق به.									

يتضح من الجدول السابق أن المتوسطات المرجحة لاستجابات أفراد العينة تراوحت ما بين (١,٨٧-٢,٤٠) وبانحراف معياري ما بين (٠,٥٥٤-٠,٧٦٠)

تصدرت العبارة (١) والتي تنص على "**أفحص جهاز الكمبيوتر بشكل دوري للتخلص من الفيروسات والبرامج الضارة**" المرتبة الأولى بمتوسط مرجح قدره (٢,٤٠) وربما يعزى ذلك إلى أن حماية الأجهزة الإلكترونية من الفيروسات والبرامج الضارة أمرًا ضروريًا للحفاظ على سلامة المعلومات الشخصية والمهنية، ولتجنب فقدان البيانات والملفات المهمة. بالإضافة إلى زيادة الوعي الإعلامي لدى الطلاب بشأن أهمية الحفاظ على أمان الأجهزة الإلكترونية وتطبيق الممارسات الآمنة في استخدام الإنترنت.

أما العبارة (٨) والتي تنص على "**استخدم شبكات الإنترنت العامة الآمنة والمشفرة عند الاتصال بالإنترنت في الأماكن العامة**" فحصلت على المرتبة التاسعة بمتوسط مرجح قدره (٢) وربما يعزى ذلك إلى ضعف وعي الطلاب بأهمية استخدام شبكات الإنترنت العامة الآمنة والمشفرة لحماية معلوماتهم الحساسة من الاختراق والسرقة. صعوبة العثور على شبكات الإنترنت العامة الآمنة والمشفرة، خاصة في الأماكن العامة التي يوجد فيها العديد من شبكات الإنترنت. علاوة على ذلك، قد يحاول الأفراد الاتصال بالإنترنت بسرعة دون الانتظار للعثور على شبكات الإنترنت الآمنة، الأمر الذي قد يؤدي إلى تعريض معلوماتهم الحساسة للخطر، والتي قد تؤدي إلى فقدان البيانات الحساسة والمعلومات الشخصية والمالية، وتأثيرات أخرى سلبية. **وتتفق هذه النتيجة مع دراسة Azzeh, et al., 2022)** أشارت النتائج إلى أن الطلاب ليس لديهم معرفة كبيرة بالأمن السيبراني وأن

المؤسسات التعليمية لا تتعامل بنشاط مع الوعي بالأمن السيبراني بين الطلاب، وأن إشراك موضوعات الأمن السيبراني المهمة في دورات علوم الكمبيوتر الأخرى يمكن أن يزيد وعي الطلاب ومعرفتهم فيما يتعلق بمفاهيم الأمن السيبراني.

وجاءت العبارة (٤) والتي تنص على "**احرص على استخدام كلمات مرور قوية وتغييرها بشكل دوري**" في المرتبة الأخيرة بمتوسط مرجح قدره (١,٨٧) وربما يعزى ذلك إلى عدة أمور لعل من أهمها:

- ضعف وعي الطلاب بأهمية استخدام كلمات مرور قوية وتغييرها بشكل منتظم لتأمين حساباتهم الشخصية والبيانات الحساسة من التهديدات السيبرانية والاختراقات.
- صعوبة اختيار كلمات مرور قوية وتذكرها خاصة إذا كان لدى الطلاب العديد من الحسابات المختلفة التي يجب عليهم تسجيل الدخول إليها.

وتتفق هذه النتيجة مع دراسة (الركبان، ٢٠٢٣) والتي توصلت إلى ضعف إدراك بعض منسوبي الجامعة أهمية اختيار كلمات مرور قوية لحساباتهم الرسمية، بحيث يصعب اختراقها والوصول إليها على الرغم من توجيه الجامعة باستمرار منسوبيها إلى اختيار كلمات مرور قوية.

٦-كفايات التعلم الرقمي:

جدول (٦)

استجابات أفراد عينة الدراسة المتعلقة بكفايات التعلم الرقمي

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
١	استخدم التطبيقات المختلفة لتحسين مهاراتي في مجال اللغات	١٤٤	٤١,٤٩	١٥١	٤٣,٥١	٥٢	١٤,٩٨	٢,٢٦	٠,٧٠٤	٢

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	وتعلم لغات جديدة بشكل فعال.									
٢	أنظم وقتي على مواقع التواصل الاجتماعي لتفادي الإدمان عليها.	٧٨	٢٢,٤٧	٢٣٢	٦٦,٨٥	٣٧	١٠,٦٦	٢,١١	٠,٥٦٤	٥
٣	استخدم التطبيقات المختلفة لتعلم البرمجة.	١٢٧	٣٦,٥٩	١٤٥	٤١,٧٨	٧٥	٢١,٦١	٢,١٤	٠,٧٤٩	٤
٤	أحرص على متابعة المضامين الرقمية الهادفة	١٧١	٤٩,٢٧	١٣٢	٣٨,٠٤	٤٤	١٢,٦٨	٢,٣٦	٠,٦٩٧	١

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	المنشورة على الانترنت.									
٥	أحرص على الاحتفاظ بنسخ احتياطية من الملفات الهامة وتخزينها على أجهزة تخزين خارجية أو في الحوسبة السحابية .	٨٤	٢٤,٢٠	٢٠٦	٥٩,٣٦	٥٧	١٦,٤٢	٢,٠٧	٠,٦٣٣	٦
٦	استخدم التطبيقات المختلفة لتحسين مهاراتي في	١٤٩	٤٢,٩٣	١٢٤	٣٥,٧٣	٧٤	٢١,٣٢	٢,٢١	٠,٧٧٣	٣

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	الكتابة والتحرير والتعبير عن الأفكار بشكل فعال.									

يتضح من الجدول السابق أن المتوسطات المرجحة لاستجابات أفراد العينة تراوحت ما بين (٢,٠٧-٢,٣٦) وبانحراف معياري ما بين (٠,٥٦٤-٠,٧٧٣)

حصلت العبارة (٤) والتي تنص على "**أحرص على متابعة المضامين الرقمية الهادفة المنشورة على الانترنت**" على المرتبة الأولى بمتوسط مرجح قدره (٢,٣٦) وربما يعزى ذلك إلى حرص الطلاب على استخدام الإنترنت ووسائل التواصل الاجتماعي بطريقة فعالة وذلك عن طريق البحث عن محتوى هادف ومفيد يساعد في تطوير الذات والتعلم.

وجاءت العبارة (٥) والتي تنص على "**أحرص على الاحتفاظ بنسخ احتياطية من الملفات الهامة وتخزينها على أجهزة تخزين خارجية أو في الحوسبة السحابية**" في المرتبة السادسة والأخيرة بمتوسط مرجح قدره (٢,٠٧) وربما يعزى ذلك إلى ضعف وعي بعض الطلاب بأهمية الاحتفاظ بنسخ احتياطية من الملفات الهامة وتخزينها بشكل آمن، كما أن بعض الطلاب قد يستخدمون خدمات التخزين السحابية المجانية التي توفرها بعض الشركات ولا يرون الحاجة للدفع مقابل خدمات التخزين السحابية الأكثر أمانًا وموثوقية، مما يزيد من احتمالية فقدان الملفات الهامة في حال حدوث مشاكل تقنية. وتتفق هذه النتيجة مع دراسة **(توفيق ومرسي، ٢٠٢٣)** والتي توصلت إلى استخدام الأجهزة الشخصية مثل الهاتف المحمول لتخزين أو نقل معلومات، وضعف استخدام برامج حماية أصلية موثوقة والاعتماد على استخدام البرامج غير الأصلية.

٧-كفايات التفكير النقدي والانتاج الإبداعي

جدول (٧)

استجابات أفراد عينة الدراسة المتعلقة بكفايات التفكير النقدي والانتاج الإبداعي

م	العبارة	درجة التوافر						المتوسط المرجح	الإنحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
١	استخدم الأدوات المختلفة لإنشاء المخططات والرسومات التوضيحية والعروض التقديمية بشكل احترافي وجذاب.	١٢٩	٣٧,١٧	١٨١	٥٢,١٦	٣٧	١٠,٦٦	٢,٢٦	٠,٦٣٩	٦
٢	انشر المضامين الرقمية التي تعبر عن أهدافي	٢٤١	٦٩,٤٥	٨٥	٢٤,٤٩	٢١	٦,٥	٢,٦٣	٠,٥٩٥	١

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	واتجاهاتي									
٣	لدي القدرة على تحرير الصور وإضافة التأثيرات والتعديلات اللازمة لتحسين جودتها وجعلها أكثر جاذبية.	٢١٢	٦١,٠٩	١٠٨	٣١,١٢	٢٧	٧,٧٨	٢,٥٣	٠,٦٣٦	٤
٤	لدي القدرة على انتاج المواد الإعلامية التي تعبر عن وجهة نظري.	٢٢٧	٦٥,٤١	١٠١	٢٩,١	١٩	٥,٤٧	٢,٥٩	٠,٥٩٢	٣

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
٥	استخدم التقنيات الحديثة مثل الواقع الافتراضي والواقع المعزز لتصميم تجارب تفاعلية مبتكرة وجذابة للمستخدمين.	٢٣١	٦٦,٥٧	٩٩	٢٨,٥٣	١٧	٤,٨٩	٢,٦١	٠,٥٧٩	٢
٦	استخدم التقنيات المتعلقة بالتشفير والأمان الإلكتروني للحفاظ على سرية وأمان	١٨٧	٥٣,٨٩	١٣١	٣٧,٧٥	٢٩	٨,٣٥	٢,٤٥	٠,٦٤٥	٥

م	العبارة	درجة التوافر						المتوسط المرجح	الانحراف المعياري	الترتيب
		متوفر بدرجة كبيرة		متوفر بدرجة متوسطة		غير متوفر				
		ك	%	ك	%	ك	%			
	المعلومات والبيانات الحساسة.									

يتضح من الجدول السابق أن المتوسطات المرجحة لاستجابات أفراد العينة تراوحت ما بين(٢,٢٦-٢,٦١) وبانحراف معياري ما بين (٠,٥٧٩-٠,٦٤٥)

جاءت العبارة (٢) والتي تنص على "**انشر المضامين الرقمية التي تعبر عن أهدافي واتجاهاتي**" في المرتبة الأولى بمتوسط مرجح قدره (٢,٦٣) وربما يعزى ذلك إلى عدة أمور لعل من أهمها:

- انتشار وسائل التواصل الاجتماعي والتقنيات الحديثة التي تتيح للفرد نشر محتوى رقمي بسهولة وفاعلية.
- حرص الطلاب على التعبير عن أنفسهم ووجهات نظرهم وبثها على نطاق واسع من خلال وسائل التواصل الاجتماعي وغيرها من الوسائل الرقمية.
- رغبة الطلاب في التواصل مع الآخرين ومشاركة أفكارهم وآرائهم وتوجهاتهم الشخصية، وهذا يمكن تحقيقه عن طريق نشر المضامين الرقمية التي تعبر عن أهدافهم واتجاهاتهم.

أما العبارة (١) والتي تنص على "**استخدم الأدوات المختلفة لإنشاء المخططات والرسومات التوضيحية والعروض التقديمية بشكل احترافي وجذاب**" في المرتبة الأخيرة بمتوسط مرجح قدره (٢,٢٦) وربما يعزى ذلك إلى قلة التركيز على تعليم مهارات الحاسوب والتصميم الجرافيكي في مناهج الجامعات المصرية، قلة التدريبات وورش العمل العملية في هذه المهارات داخل الجامعات، نقص توفر برامج تدريبية متخصصة في هذه المهارات لطلاب الجامعات المصرية، ضعف توافر البنية التحتية والأجهزة الرقمية اللازمة لتعلم هذه المهارات في الجامعات.

المحور الثاني: أساليب تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية

جدول (٨)

استجابات أفراد عينة الدراسة المتعلقة بأساليب تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية

م	العبارة	درجة الأهمية						المتوسط المرجح	الانحراف المعياري	الترتيب
		مهمة بدرجة كبيرة		مهمة بدرجة متوسطة		غير مهمة				
		ك	%	ك	%	ك	%			
١	تنظيم حملات توعية حول المخاطر الإلكترونية وكيفية حماية البيانات الشخصية على الإنترنت.	٢٢٢	٦٣,٩٧	١٢٥	٣٦,٠٢	–	–	٢,٦٣	٠,٤٨٠	٥
٢	تصميم برامج تدريبية لتعريف الطلاب بالمخاطر والتهديدات الإلكترونية وكيفية	٢٦٣	٧٥,٧٩	٨٤	٢٤,٢٠	–	–	٢,٧٥	٠,٤٢٨	١

م	العبارة	درجة الأهمية						المتوسط المرجح	الانحراف المعياري	الترتيب
		مهمة بدرجة كبيرة		مهمة بدرجة متوسطة		غير مهمة				
		ك	%	ك	%	ك	%			
	الوقاية منها.									
٣	توجيه الطلاب في حال وقوع أي انتهاك للبيانات الشخصية إلى الجهات المختصة للتحقيق في مثل هذه الانتهاكات .	٢٣٢	٦٦,٨٥	٩٧	٢٧,٩٥	١٨	٥,١٨	٢,٦١	٠,٥٨٤	٦
٤	استخدام منصات التعلم الإلكتروني لتوفير مقررات إلكترونية تتضمن معلومات عن كيفية بناء سلوكيات	٢٥٥	٧٣,٤٨	٩٢	٢٦,٥١	–	–	٢,٧٣	٠,٤٤٢	٢

م	العبارة	درجة الأهمية						المتوسط المرجح	الانحراف المعياري	الترتيب
		مهمة بدرجة كبيرة		مهمة بدرجة متوسطة		غير مهمة				
		ك	%	ك	%	ك	%			
	آمنة على الشبكة.									
٥	نشر الوعي بأهمية اتباع سلوكيات آمنة على الإنترنت، مثل اختيار كلمات مرور قوية وتغييرها بشكل مستمر وتجنب فتح الروابط المشبوهة.	٢٤٨	٧١,٤٦	٩٩	٢٨,٥٣	–	–	٢,٧١	٠,٤٥٢	٣
٦	تزويد الطلاب بالمعرفة والمهارات التقنية لمواجهة	٢٢٥	٦٤,٨٤	١٢٢	٣٥,١٥	–	–	٢,٦٤	٠,٤٧٨	٤

م	العبارة	درجة الأهمية						المتوسط المرجح	الانحراف المعياري	الترتيب
		مهمة بدرجة كبيرة		مهمة بدرجة متوسطة		غير مهمة				
		ك	%	ك	%	ك	%			
	تهديدات الفضاء الإلكتروني ، بما في ذلك مهارات استخدام أدوات حماية الخصوصية وبرمجيات مكافحة الفيروسات									

يتضح من الجدول السابق أن المتوسطات المرجحة لاستجابات أفراد العينة تراوحت ما بين (٢,٦١-٢,٧٥) وبانحراف معياري ما بين (٠,٤٢٨-٠,٥٨٤)

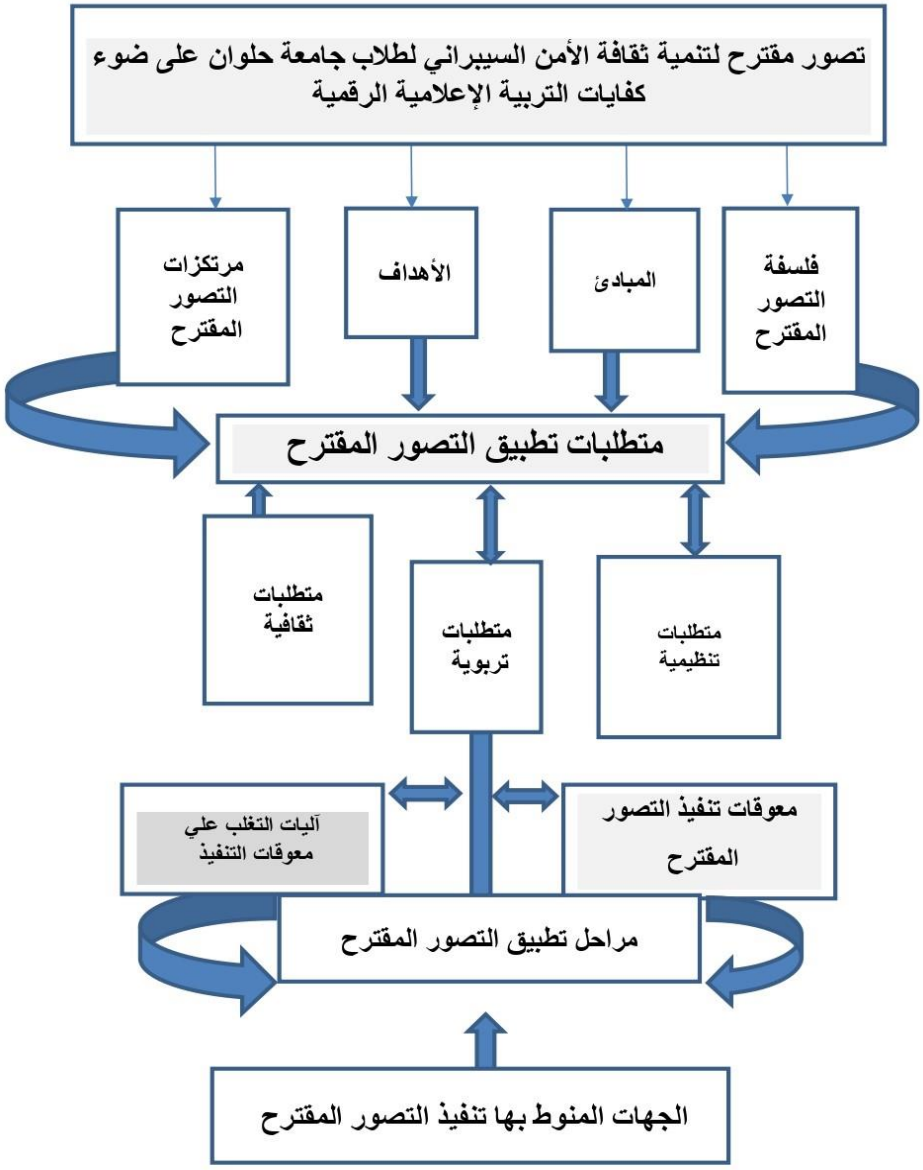
تصدرت العبارة (٢) والتي تنص على "**تصميم برامج تدريبية لتعريف الطلاب بالمخاطر والتهديدات الإلكترونية وكيفية الوقاية منها**" المرتبة الأولى بمتوسط مرجح قدره (٢,٧٥) وربما يعزى ذلك إلى أن طلاب الجامعات يتعرضون بشكل متزايد للتهديدات الإلكترونية، ويعد توفير برامج تدريبية لهم لتعريفهم بأنواع التهديدات الإلكترونية وكيفية الوقاية منها أمرًا مهمًا للغاية، حيث يمكن أن تساعد هذه البرامج في تحسين الوعي الأمني لدى الطلاب وتمكينهم من اتخاذ إجراءات وقائية لضمان سلامة بياناتهم الشخصية وأجهزتهم الإلكترونية من الهجمات السيبرانية. وتتفق هذه النتيجة مع دراسة موتونهو وآخرون **(Mutunhu, et al.,2022)** والتي توصلت إلى أن الطلاب في الجامعات لديهم نقص في المعرفة والفهم المطلوبين لأهمية مبادئ الأمن السيبراني، وتطبيقها العملي في أنشطتهم اليومية، وليس لديهم دراية كافية بها وبكيفية حماية بياناتهم.

وجاءت العبارة (٤) والتي تنص على "**استخدام منصات التعلم الإلكتروني لتوفير مقررات إلكترونية تتضمن معلومات عن كيفية بناء سلوكيات آمنة على الشبكة**" في المرتبة الثانية بمتوسط مرجح قدره (٢,٧٣) وربما يعزى ذلك إلى أن الجامعات تستخدم عادة منصات التعلم الإلكتروني لتوفير المقررات الدراسية للطلاب، ويمكن للجامعات تضمين معلومات حول كيفية بناء سلوكيات آمنة على الإنترنت في هذه المقررات الإلكترونية، حيث يمكن أن تساعد هذه المعلومات في تحسين الوعي الأمني لدى الطلاب.

أما العبارة (٣) والتي تنص على "**توجيه الطلاب في حال وقوع أي انتهاك للبيانات الشخصية إلى الجهات المختصة للتحقيق في مثل هذه الانتهاكات**" فجاءت في المرتبة السادسة وعلى الرغم من حصولها على المرتبة الأخيرة إلا أنها حصلت على متوسط مرجح مرتفع (٢,٦١) وربما يعزى ذلك إلى أهمية الجهات المختصة في تقديم المساعدة اللازمة للطلاب والحيلولة دون حدوث المزيد من الانتهاكات للبيانات الشخصية.

المحور الخامس: تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية

يهدف المحور الحالي إلى وضع تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية، وتحقيقًا لهذا الهدف فإنه ينبغي التعرض لفلسفة التصور المقترح، والمبادئ التي يستند إليها، أهدافه، مرتكزاته، ومراحل ومتطلبات تطبيقه، ومعوقاته وآليات التغلب عليها، وأخيرًا الجهات المنوط بها تنفيذ التصور.



شكل (3)
مخطط لأنموذج التصور المقترح لتنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان على ضوء كفايات التربية الإعلامية الرقمية

المصدر: إعداد الباحثة

أولًا: فلسفة التصور المقترح

تتمحور فلسفة التصور المقترح حول تزويد الطلاب بالمعرفة والكفايات اللازمة لتطوير ثقافتهم الأمنية السيبرانية وفق متطلبات العصر الرقمي، بهدف حمايتهم من المخاطر الإلكترونية والتهديدات السيبرانية، بالاعتماد على تفعيل دور التربية الإعلامية الرقمية في تنمية قدراتهم على التعامل الآمن والواعي مع تقنيات المعلومات والاتصالات، بالإضافة إلى تبني الجامعات للسياسات والأنظمة التي تشجع على استخدام آمن لتكنولوجيا المعلومات.

وتستند هذه الفلسفة إلى ضرورة زيادة الوعي بأهمية الأمن السيبراني لدى طلاب الجامعات وتزويدهم بالمعارف والمهارات واتجاهات السلوك الإيجابية اللازمة للتعامل الآمن مع التكنولوجيا وتطبيقاتها، وتطوير بيئة تشجع على تبادل الخبرات في هذا المجال، وتنمي لديهم مهارات التفكير الناقد لتقييم التكنولوجيات بموضوعية، وتحفزهم على ابتكار حلول لتعزيز الأمن السيبراني بهدف إعداد جيل واع بأهمية حماية الفضاء السيبراني وقادر على التعامل مع تحدياته بكفاءة وأمان.

ثانيًا: مبادئ التصور المقترح

يستند التصور المقترح على مجموعة من المبادئ الأساسية، وهي:

- **المبدأ الأول: دمج التربية الإعلامية الرقمية في مناهج التعليم الجامعي:** يهدف هذا المبدأ إلى دمج التربية الإعلامية الرقمية في مناهج التعليم الجامعي لتنمية مهارات التعامل الآمن مع التقنيات الحديثة وشبكة الإنترنت، وتحديث وتطوير المقاربة التعليمية باستمرار لتتناسب مع المتغيرات والتطورات الحديثة في مجال الأمن السيبراني، وذلك من خلال الاستفادة من التجارب السابقة والمعرفة الحديثة المتاحة في هذا المجال، والتركيز على كفايات التربية الإعلامية الرقمية كأساس لتنمية ثقافة الأمن السيبراني لدى الطلاب. ويمكن تحقيق هذا المبدأ من خلال تطوير المناهج الدراسية وتضمين مواد تعليمية تتعلق بالأمن السيبراني والتربية الإعلامية الرقمية، وتوفير الإمكانيات والموارد اللازمة لتنفيذها.
- **المبدأ الثاني: تطوير البرامج التعليمية:** يهدف هذا المبدأ إلى تطوير برامج تعليمية وورش عمل ودورات تدريبية متخصصة لتعزيز الوعي والمعرفة الخاصة بالأمن السيبراني، وتزويد الطلاب بالمهارات اللازمة لحماية أنفسهم وأجهزتهم الإلكترونية. وتشجيع الطلاب على المشاركة في المسابقات والفعاليات المتعلقة بمجال الأمن السيبراني والتحديات الإلكترونية لتحفيزهم على تطبيق المفاهيم والمهارات التي يتعلمونها في بيئة تحفيزية وممتعة. ويمكن تنفيذ هذا المبدأ من

خلال توفير الموارد اللازمة لإنشاء برامج تعليمية مخصصة للطلاب والمتخصصين في مجال الأمن السيبراني وتنفيذ ورش عمل ودورات تدريبية.

- **المبدأ الثالث: تبني السلوكيات الآمنة:** يهدف هذا المبدأ إلى تبني الجامعات للسياسات والأنظمة واللوائح التي تشجع على السلوكيات الآمنة تكنولوجيًا داخل الحرم الجامعي، وتعزيز الشفافية والمساءلة في مجال الأمن السيبراني من خلال توعية الطلاب بأهمية الالتزام بمعايير الأمان والتدابير الوقائية، وتعزيز المساءلة والمحاسبة في حالة انتهاك أي معايير أمنية. ويمكن تحقيق هذا المبدأ من خلال تطبيق السياسات والأنظمة الأمنية والتقنيات الحديثة لحماية البيانات الحساسة وتوفير الأمن السيبراني داخل الحرم الجامعي، كما يمكن إصدار موجهات وإرشادات للطلاب والعاملين في الجامعة لتحقيق سلوكيات آمنة تكنولوجيًا.
- **المبدأ الرابع: التعاون والشراكة:** يهدف هذا المبدأ إلى التعاون والشراكة مع الجهات الحكومية والخاصة المعنية بالأمن السيبراني لتحقيق التوافق والتكامل في المبادرات والخطط المتعلقة بتنمية ثقافة الأمن السيبراني لدى الطلاب، وتبادل الخبرات والمعرفة والتقنيات الحديثة. علاوة على تطوير شراكات مع الصناعة والقطاع الخاص لتوفير فرص العمل والتدريب للطلاب الذين يتمتعون بمهارات في مجال الأمن السيبراني، وذلك لتشجيع الطلاب على الاستمرار في تعلم هذا المجال وتطوير مهاراتهم، وتوفير فرص العمل المناسبة لهم في سوق العمل.
- **المبدأ الخامس: توفير الموارد والدعم اللازم:** يهدف هذا المبدأ إلى توفير الموارد والدعم اللازم لتطبيق تصور المقترح، بما في ذلك الموارد المالية والتقنية والبشرية، وتعزيز الشراكات والتعاون مع المؤسسات الأخرى لتحقيق هذه الأهداف. ومن شأن هذا المبدأ أن يساعد في تحسين جودة البرامج التعليمية والمبادرات الأخرى المتعلقة بالأمن السيبراني وتوفير الموارد اللازمة لتنفيذها.
- **المبدأ السادس: تقييم وتحسين الجهود:** يهدف هذا المبدأ إلى تقييم الجهود المبذولة لتنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية وتحسينها بما يتناسب مع التطورات السريعة في مجال التكنولوجيا والأمن السيبراني. يمكن تحقيق هذا المبدأ من خلال إجراء تقييم دوري للبرامج التعليمية والتدريبية والسياسات والأنظمة الأمنية في الجامعات وتحسينها بناءً على نتائج التقييم،

كما يمكن توفير آليات لجمع الملاحظات والاقتراحات من الطلاب والعاملين في الجامعات.

- **المبدأ السابع: توعية الجمهور:** يهدف هذا المبدأ إلى توعية الجمهور بشكل عام بأهمية الأمن السيبراني والتحديات التي تواجهها الجامعات والطلاب، وتشجيعهم على تبني السلوكيات الآمنة والإبلاغ عن أي نشاط مشبوه على الإنترنت. ويمكن تحقيق هذا المبدأ من خلال تنظيم حملات توعية وحملات إعلامية للجمهور، وتوفير المعلومات الصحيحة والدقيقة حول التهديدات السيبرانية وطرق الوقاية منها، كما يمكن تحفيز الجمهور على المشاركة في الحملات الإعلامية والتوعوية ونشر الوعي بشكل أكبر.
- **المبدأ الثامن: تشجيع البحث العلمي:** يهدف هذا المبدأ إلى تشجيع البحث العلمي في مجال الأمن السيبراني وتعزيز التعاون بين الجامعات والمؤسسات الحكومية والخاصة المعنية بالأمن السيبراني، وتحفيز الطلاب على المشاركة في الأبحاث العلمية المتعلقة بمجال الأمن السيبراني لتطوير المعرفة والتفاعل مع الموضوع بشكل أكبر، وتحفيزهم على تطوير الحلول الإبداعية والمبتكرة لمواجهة التحديات السيبرانية المختلفة.

ثالثًا: أهداف التصور المقترح

الهدف العام: تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية. ويندرج تحت هذا الهدف عده أهداف فرعية:

- التركيز على كفايات التربية الإعلامية الرقمية كأساس لتنمية ثقافة الأمن السيبراني لدى الطلاب.
- توعية الطلاب بأهمية الأمن السيبراني وأساليب الحماية اللازمة للحفاظ على سلامة بياناتهم الشخصية والمعلوماتية
- تعزيز الوعي بأنشطة الاحتيال الإلكتروني والتهديدات السيبرانية المختلفة وكيفية التعامل معها
- تعزيز القدرات الفنية والتقنية للطلاب في مجال الأمن السيبراني وتوفير الدورات التدريبية اللازمة لتحسين مهاراتهم .
- تعزيز التعاون بين الجامعات والمؤسسات الحكومية والخاصة المعنية بالأمن السيبراني لتبادل الخبرات والمعرفة وتطوير الحلول الفنية والتقنية .

- تشجيع الطلاب على البحث والتطوير في مجال الأمن السيبراني وتوفير الدعم اللازم لتحقيق ذلك.
- تطوير سياسات وإجراءات الأمن السيبراني في الجامعة وتحديثها بشكل دوري لمواكبة التطورات التقنية والتهديدات السيبرانية المتغيرة.
- توعية الطلاب والموظفين بأهمية الأمن السيبراني وتعزيز الوعي بالتهديدات السيبرانية وكيفية التعامل معها
- تطوير وتنفيذ برامج تدريبية وتعليمية للطلاب والموظفين حول الأمن السيبراني والتقنيات الحديثة المستخدمة في هذا المجال .
- تحسين الإجراءات الأمنية للحماية من الهجمات السيبرانية والتأكد من توافر الأدوات والتقنيات اللازمة لذلك .
- استخدام الأدوات التعليمية الحديثة مثل برامج الواقع الافتراضي والمحاكاة السيبرانية لتعزيز تجربة التعلم والتفاعل مع الموضوع.
- تدريب الطلاب على الكفايات والمهارات الأساسية للتعامل الآمن مع تكنولوجيا المعلومات وشبكة الإنترنت.
- تشجيع الطلاب على التفكير النقدي والإبداعي وتنمية مهارات حل المشكلات واتخاذ القرارات الصائبة في مواجهة التحديات السيبرانية.
- تأمين التواصل الفعال والمتواصل بين الطلاب والمدرسين والمسؤولين المعنيين بتنمية ثقافة الأمن السيبراني، وذلك لتحقيق التكامل والتنسيق في الجهود المبذولة في هذا المجال ولتبادل الخبرات والمعرفة.
- توظيف تقنيات التعلم الذكي وتحليل البيانات لتحسين عملية التعليم وتوفير تجربة تعليمية مخصصة ومتكيفة مع احتياجات كل طالب.
- إدماج التعليم السيبراني في المناهج الدراسية لجميع التخصصات الأكاديمية لتعزيز ثقافة الأمن السيبراني لدى الطلاب بشكل شامل.
- توفير دعم فني وفعاليات توعوية للطلاب لتأمين الدعم الفني المستمر والمتخصص لحل المشاكل والأسئلة المتعلقة بالأمن السيبراني، كما يتم توفير فعاليات توعوية مثل الندوات وورش العمل لتبادل الخبرات والمعلومات المتعلقة بمجال الأمن السيبراني.

رابعًا: مرتكزات التصور المقترح

من خلال الدراسة التحليلية النظرية للأدبيات والدراسات السابقة المرتبطة بالموضوع ونتائج الدراسة الميدانية، وجب وضع تصور مقترح ليكون دافعًا لتنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية على النحو التالي:

٧-كفايات البحث الرقمي:

يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية على ضوء كفايات البحث الرقمي من خلال مايلي

- توفير دورات تدريبية وورش عمل للطلاب حول كيفية البحث الرقمي بأمان وحماية البيانات الشخصية أثناء التصفح على الإنترنت.
- توفير موارد تعليمية عبر الإنترنت لتعزيز الوعي بخطر الاحتيال الإلكتروني والبرمجيات الخبيثة والهجمات السيبرانية الأخرى.
- توفير موارد تعليمية حول كيفية استخدام أدوات الأمان السيبراني، مثل برامج مكافحة الفيروسات وجدران الحماية وأدوات إدارة كلمات المرور، وشرح طريقة استخدامها بشكل صحيح وفعال.
- تشجيع الطلاب على استخدام مصادر موثوقة ومواقع آمنة عند البحث على الإنترنت، وتوفير نصائح لتقييم مصداقية المعلومات المتاحة عبر الإنترنت.
- تعزيز الوعي بأهمية الخصوصية الإلكترونية وتوفير نصائح حول طرق الحفاظ على الخصوصية الشخصية والبيانات الحساسة عبر الإنترنت، مثل تجنب مشاركة المعلومات الشخصية مع أي جهة غير موثوقة.
- تعزيز الوعي بأنواع الهجمات السيبرانية وكيفية التعامل معها، وتوفير نصائح حول كيفية التعرف على الرسائل الاحتيالية والرسائل الإلكترونية الغير مرغوب فيها (Spam)، وطرق الإبلاغ عنها وتجنب فتح المرفقات أو الروابط الغير معروفة.
- تشجيع الطلاب على تحديث البرامج والتطبيقات المثبتة على أجهزتهم بشكل دوري، وتفعيل خيارات التحديث التلقائي إن وجدت، للحفاظ على أمان أجهزتهم وحماية بياناتهم الشخصية.
- توفير نصائح حول كيفية إنشاء كلمات مرور قوية ومتعددة وتغييرها بشكل دوري، وتشجيع الطلاب على عدم مشاركة كلمات المرور مع أي شخص آخر.

- تحفيز الطلاب على إجراء عمليات النسخ الاحتياطي الدورية للبيانات الشخصية والملفات المهمة، وتوفير نصائح حول كيفية الحفاظ على نسخ احتياطية آمنة للبيانات.

- توفير نصائح حول السلوكيات الآمنة عند استخدام وسائل التواصل الاجتماعية الرقمية، مثل عدم مشاركة المعلومات الشخصية عبر مواقع التواصل الاجتماعي مع أي شخص غير موثوق به، وعدم الرد على الرسائل الإلكترونية الغير معروفة، وعدم تحميل الملفات من مصادر غير موثوقة.

- تعزيز الوعي بأهمية إعلام الجامعة عن أي حالات اختراق أمني أو احتيال إلكتروني، وتوفير نصائح حول كيفية التعامل مع هذه الحالات والإبلاغ عنها.

٨-كفايات تحليل المعلومات والبيانات الرقمية:

يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية على ضوء كفايات تحليل المعلومات والبيانات الرقمية من خلال مايلي

- توفير دورات تدريبية وورش عمل للطلاب حول كيفية تحليل المعلومات والبيانات الرقمية بأمان، وتعزيز الوعي بأهمية تحليل البيانات الرقمية لتحديد السلوكيات الغير طبيعية والمشبوهة التي يمكن أن تشكل خطرًا على الأمن السيبراني.

- تعزيز الوعي بأهمية تحليل سجلات النشاط على الإنترنت والبيانات الرقمية الأخرى للكشف عن الهجمات السيبرانية والأنشطة الغير مشروعة، وتوفير التدريب على كيفية تحليل هذه البيانات واستخراج المعلومات المفيدة منها.

- تشجيع الطلاب على تطوير مهارات التحليل الرقمي والتعلم الآلي وتطبيقها في مجال الأمن السيبراني، وتوفير الدعم الفني والإرشادات اللازمة لتطوير هذه المهارات.

- تشجيع الطلاب على المشاركة في مسابقات وتحديات تتعلق بالأمن السيبراني والتحليل الرقمي، وتوفير الموارد التعليمية والتدريبية اللازمة للمشاركة في هذه المسابقات.

- توفير فرص التطوع للطلاب في مشاريع الأمن السيبراني والتحليل الرقمي في الجامعة أو في مؤسسات أخرى، وتشجيع الطلاب على المشاركة في هذه المشاريع لتطوير مهاراتهم وخبراتهم في هذا المجال الحيوي.

- توفير موارد تعليمية حول كيفية استخدام الأدوات المتاحة لتحليل المعلومات والبيانات الرقمية، مثل برامج تحليل البيانات وتقنيات التعلم الآلي، وشرح طريقة استخدامها بشكل صحيح وفعال.
- توفير موارد تعليمية حول أبرز التهديدات السيبرانية المتعلقة بالطلاب، والطرق الفعالة للحماية من هذه التهديدات، مثل الهجمات الاحتيالية والتصيد الالكتروني والبرامج الخبيثة.
- تشجيع الطلاب على استخدام برامج مضادة للفيروسات وتطبيقات الأمان الأخرى على أجهزتهم الشخصية، وتوفير التدريب على كيفية استخدام هذه الأدوات بشكل صحيح وفعال.
- توفير الدعم الفني والإرشادات اللازمة للطلاب في حالة وجود أي مشكلة أمنية في أجهزتهم الشخصية أو حساباتهم على الإنترنت، وتوفير قنوات اتصال مباشرة مع فرق دعم الأمن السيبراني في الجامعة للإبلاغ عن أي مشكلة تتعلق بالأمن السيبراني.
- تعزيز الوعي بأهمية الخصوصية الرقمية وأهمية حماية المعلومات الشخصية، وتوفير الموارد التعليمية والتدريبية حول كيفية الحفاظ على الخصوصية الرقمية، والطرق الفعالة لحماية المعلومات الشخصية من الاختراق والسرقة.
- تعزيز الوعي بأهمية إنشاء كلمات مرور قوية وآمنة، وتوفير التدريب والإرشادات حول كيفية إنشاء كلمات مرور آمنة وتغييرها بشكل دوري، وتجنب استخدام كلمات المرور الضعيفة أو السهلة التخمين.
- توفير التدريب على كيفية التعامل مع البريد الإلكتروني بأمان، وتحديد البريد الإلكتروني المشبوه والتعرف على رسائل البريد الإلكتروني الاحتيالية، وتوفير الإرشادات حول كيفية تجنب الوقوع في فخ التصيد الالكتروني.
- تعزيز الوعي بأهمية النسخ الاحتياطي للبيانات وتوفير الدعم الفني والإرشادات اللازمة للطلاب حول كيفية إنشاء نسخ احتياطية للبيانات بشكل دوري وتخزينها بأمان، وتوفير الموارد التعليمية حول كيفية استخدام أدوات النسخ الاحتياطي وتحديد البيانات الحساسة التي يجب حفظها بشكل خاص.
- تشجيع الطلاب على مشاركة المعرفة والخبرات في مجال الأمن السيبراني مع زملائهم الطلاب والمجتمع بشكل عام، وتوفير الدعم لإنشاء مجتمعات للطلاب المهتمين بالأمن السيبراني للتبادل بالمعرفة والخبرات.

- توفير الدعم لإنشاء فرق عمل للأمن السيبراني في الجامعة، وتوفير التدريب اللازم لأعضاء هذه الفرق على كيفية مراقبة وتحليل ومعالجة الأحداث الأمنية السيبرانية في الجامعة.

- توفير الدعم لإنشاء فرق عمل للأمن السيبراني في الجامعة، وتوفير التدريب اللازم لأعضاء هذه الفرق على كيفية مراقبة وتحليل ومعالجة الأحداث الأمنية السيبرانية في الجامعة.

- توفير الدعم لتطوير برامج الحماية السيبرانية في الجامعة، وتحديث هذه البرامج بشكل دوري لتوفير حماية أفضل للأجهزة والبيانات والشبكات السيبرانية في الجامعة.

كفايات تحليل المعلومات والبيانات الرقمية:

يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية على ضوء كفايات تحليل المعلومات والبيانات الرقمية من خلال مايلي

- توفير التدريب اللازم للطلاب على كيفية تحليل البيانات الرقمية المتعلقة بالأمن السيبراني، مثل معلومات تسجيل الدخول وسجلات التصفح والحركة على الشبكة، وتوفير الأدوات اللازمة لجمع وتحليل هذه البيانات.

- تعزيز الوعي بأهمية تحليل البيانات الرقمية للكشف عن التهديدات السيبرانية وتحديد نقاط الضعف في الأنظمة السيبرانية، وتوفير الموارد التعليمية حول أساسيات تحليل البيانات والتقنيات والأدوات المستخدمة في هذا المجال.

- توفير الدعم الفني والإرشادات اللازمة للطلاب حول كيفية استخدام الأدوات والتقنيات المختلفة لتحليل البيانات الرقمية بشكل صحيح وفعال، وتوفير التدريب على كيفية تفسير النتائج واستخلاص القرارات اللازمة.

- تعزيز الوعي بأهمية حماية البيانات الرقمية والخصوصية الرقمية، وتوفير الموارد التعليمية حول كيفية حماية البيانات الرقمية وتحليل البيانات بشكل آمن ومسؤول.

- تشجيع الطلاب على مشاركة الخبرات والمعرفة في مجال تحليل البيانات الرقمية والأمن السيبراني مع زملائهم الطلاب والمجتمع بشكل عام، وتوفير المنصات اللازمة للتواصل والتعاون وتبادل المعرفة والخبرات في هذا المجال.

- توفير الدعم الفني والإرشادات اللازمة للطلاب حول كيفية استخدام تقنيات تحليل البيانات الرقمية لتحسين الأمن السيبراني في الجامعات وخارجها، وتوفير التدريب

على كيفية استخدام هذه التقنيات في تحليل البيانات السيبرانية وتحديد النماذج الاحتمالية للهجمات السيبرانية المستقبلية.

- تشجيع الطلاب على الابتكار والتفكير الإبداعي في مجال تحليل البيانات الرقمية والأمن السيبراني، وتوفير الدعم لهم في تحقيق أفكارهم وتطبيقها بشكل عملي.
- توفير الموارد التعليمية حول أساليب تحليل البيانات الرقمية المتقدمة، مثل تقنيات التعلم الآلي والذكاء الاصطناعي والتحليل الإحصائي، وتوفير التدريب اللازم للطلاب على استخدام هذه التقنيات بشكل فعال في تحليل البيانات السيبرانية.
- تشجيع الطلاب على المشاركة في مسابقات وفعاليات تحليل البيانات الرقمية والأمن السيبراني، وتوفير الدعم اللازم لهم للتحضير لهذه المسابقات والفعاليات وتطوير مهاراتهم في هذا المجال.
- تعزيز الشراكات بين الجامعات والشركات والمؤسسات المختلفة في مجال تحليل البيانات الرقمية والأمن السيبراني، وتوفير فرص للطلاب للتعرف على تجارب عملية ومشاريع حقيقية في هذا المجال، وتوفير التدريب والتوجيه اللازم لهم لتطوير مهاراتهم وتحسين فرصهم في سوق العمل.
- توفير الدعم الفني والإرشادات اللازمة للطلاب حول كيفية استخدام أدوات الحماية السيبرانية المختلفة، مثل برامج مكافحة الفيروسات وبرامج الحماية من البرمجيات الخبيثة والحماية من الاختراقات، وتوفير التدريب على كيفية استخدام هذه الأدوات بشكل صحيح وفعال.
- تعزيز الوعي بأخلاقيات استخدام البيانات الرقمية وضرورة الالتزام بالقوانين واللوائح المتعلقة بالأمن السيبراني، وتوفير الموارد التعليمية حول المخاطر القانونية المترتبة على استخدام البيانات الرقمية بشكل غير قانوني.
- توفير الموارد التعليمية حول أنواع الهجمات السيبرانية المختلفة، مثل هجمات الفيشينج والتصيد الالكتروني والهجمات بواسطة البرمجيات الخبيثة والاختراقات، وتوفير التدريب اللازم للطلاب على كيفية التعرف على هذه الهجمات والتصدي لها.
- تشجيع الطلاب على تطوير مهاراتهم في التحليل الإحصائي والرياضيات وعلوم الحاسوب وتطبيقها في تحليل البيانات الرقمية والأمن السيبراني.
- إنشاء مراكز للأمن السيبراني في الجامعات المصرية لتوفير الدعم الفني والتدريب والإرشادات اللازمة للطلاب والباحثين والأعضاء الأكاديميين في مجال الأمن

السيبراني، وتوفير فرص للتعاون والتبادل المعرفي والتقني بين الجامعات والمؤسسات والشركات المختلفة في مجال الأمن السيبراني.

- توفير فرص للطلاب للمشاركة في مشاريع أبحاث متعلقة بالأمن السيبراني وتحليل البيانات الرقمية وتوفير الدعم اللازم لهم في هذا الصدد، وتشجيعهم على نشر النتائج والمساهمة في تطوير حلول وتقنيات جديدة في مجال الأمن السيبراني.
- تشجيع الطلاب على المشاركة في فعاليات ومسابقات ومؤتمرات علمية متعلقة بالأمن السيبراني وتحليل البيانات الرقمية، وتوفير الدعم اللازم لهم في هذا الصدد، وتشجيعهم على اكتساب الخبرات والمهارات اللازمة في هذا المجال والتعرف على أحدث التقنيات والأدوات المستخدمة فيه.
- توفير الدعم اللازم للطلاب الذين يرغبون في مواصلة دراساتهم العليا في مجال الأمن السيبراني وتحليل البيانات الرقمية، وتوفير الفرص المناسبة لهم للحصول على المنح الدراسية والتدريبات والتدريس في هذا المجال.
- تعزيز التعاون بين الجامعات والمؤسسات الحكومية والشركات والمنظمات ذات الصلة في مجال الأمن السيبراني، وتوفير فرص للطلاب للتعرف على أحدث التقنيات والمنتجات المتعلقة بالأمن السيبراني وتحليل البيانات الرقمية.
- توفير الدعم اللازم للطلاب لتطوير مهاراتهم في التواصل والتعاون والقيادة وإدارة المشاريع، وتوفير الفرص المناسبة لهم للعمل في فرق العمل المتخصصة في مجال الأمن السيبراني وتحليل البيانات الرقمية.

باستقراء ماسبق، يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية على ضوء كفايات تحليل المعلومات والبيانات الرقمية وتطوير مهاراتهم في استخدام أدوات الحماية السيبرانية والتعرف على أنواع الهجمات السيبرانية المختلفة وكيفية التصدي لها، إلى جانب تعزيز الوعي بأخلاقيات استخدام البيانات الرقمية وضرورة الالتزام بالقوانين واللوائح المتعلقة بالأمن السيبراني. ويمكن تحقيق ذلك من خلال توفير الموارد التعليمية والدعم الفني وتشجيع الطلاب على المشاركة في مشاريع البحث والفعاليات العلمية والمسابقات المتعلقة بالأمن السيبراني وتحليل البيانات الرقمية، وتعزيز التعاون بين الجامعات، وتشجيع الطلاب على مشاركة المعرفة والخبرات في هذا المجال وتطبيقها عمليًا في الحياة العملية.

٩-كفايات التواصل الالكتروني:

يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية على ضوء كفايات التواصل الالكتروني من خلال مايلي

- توفير الموارد التعليمية حول أساسيات الاتصالات الالكترونية والتواصل عبر الإنترنت، وتوضيح أهمية حماية المعلومات الشخصية والمهنية والتعرف على أنواع الهجمات السيبرانية المختلفة.

- توفير الدعم الفني والتوجيهات اللازمة حول استخدام البريد الإلكتروني والشبكات الاجتماعية والتطبيقات الرقمية بشكل آمن وفعال.

- تعزيز الوعي بأخلاقيات استخدام ونشر المعلومات عبر الإنترنت، وضرورة الالتزام بالقوانين واللوائح المتعلقة بالأمن السيبراني، وتوفير الموارد التعليمية حول المخاطر القانونية المترتبة على استخدام البيانات الرقمية بشكل غير قانوني.

- توفير التدريب على كيفية التعامل مع رسائل البريد الإلكتروني المشبوهة والتصيد الالكتروني والتهديدات السيبرانية الأخرى، وتوفير الأدوات اللازمة لتحديد ومنع الملفات الخبيثة والبرمجيات الضارة.

- تعزيز الوعي بأهمية استخدام كلمات المرور الآمنة والتحقق الثنائي للهوية وتطبيق تقنيات التشفير والتوقيع الرقمي للحفاظ على الأمان السيبراني.

- توفير الموارد التعليمية حول أنواع الهجمات السيبرانية المختلفة التي تتعرض لها الجامعات والطلاب بشكل خاص، وتوفير التدريب اللازم للطلاب على كيفية التعرف على هذه الهجمات والتصدي لها.

- تشجيع الطلاب على المشاركة في فعاليات ومسابقات ومؤتمرات علمية متعلقة بالأمن السيبراني والتواصل الالكتروني، وتوفير الدعم اللازم لهم في هذا الصدد، وتشجيعهم على اكتساب الخبرات والمهارات اللازمة في هذا المجال.

- إنشاء مراكز للأمن السيبراني في الجامعات المصرية لتوفير الدعم الفني والتدريب والإرشادات اللازمة للطلاب والباحثين والأعضاء الأكاديميين في مجال الأمن السيبراني والتواصل الالكتروني، وتوفير فرص للتعاون والتبادل المعرفي والتقني بين الجامعات والمؤسسات والشركات المختلفة في مجال الأمن السيبراني.

- توفير فرص للطلاب للمشاركة في مشاريع أبحاث متعلقة بالأمن السيبراني والتواصل الالكتروني وتوفير الدعم اللازم لهم في هذا الصدد، وتشجيعهم على نشر النتائج المتعلقة بأبحاثهم في المجلات العلمية المرموقة والمشاركة في المؤتمرات الدولية المختلفة.

- التعاون مع الجهات المعنية في مجال الأمن السيبراني في مصر وخارجها، وتوفير الدعم اللازم للطلاب للمشاركة في البرامج الدولية المختلفة في مجال الأمن السيبراني والتواصل الالكتروني.

في ضوء ماسبق، يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية من خلال توفير الموارد التعليمية اللازمة والدعم الفني والتدريب والإرشادات اللازمة، بالإضافة إلى تشجيع المشاركة في فعاليات ومسابقات ومؤتمرات علمية متعلقة بالأمن السيبراني والتواصل الالكتروني، وتوفير الفرص للتعاون والتبادل المعرفي والتقني بين الجامعات والمؤسسات والشركات المختلفة في هذا المجال. كما يمكن تشجيع الطلاب على المشاركة في مشاريع أبحاث متعلقة بالأمن السيبراني وتوفير الدعم اللازم لهم في هذا الصدد، والتعاون مع الجهات المعنية في مجال الأمن السيبراني في مصر وخارجها. بناءً على ذلك، يمكن تحقيق زيادة في الوعي بأهمية الأمن السيبراني وتعزيز ثقافة الأمن السيبراني لدى طلاب الجامعات المصرية وتحقيق زيادة في مستوى الحماية السيبرانية والأمن الرقمي.

١٠-كفايات الأمان الالكتروني والخصوصية:

يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية على ضوء كفايات الأمان الالكتروني والخصوصية من خلال مايلي:

- توفير التدريب اللازم للطلاب حول كيفية الحفاظ على سلامة الأجهزة والتطبيقات الإلكترونية الخاصة بهم، وذلك من خلال تعزيز الوعي بأساليب الهجوم السيبراني والطرق التي يمكن استخدامها للتغلب على هذه الهجمات.
- تشجيع الطلاب على استخدام برامج الحماية السيبرانية وتطبيق المعايير الأمنية المناسبة لتحسين مستوى الحماية السيبرانية للأجهزة الإلكترونية الخاصة بهم، والحد من تعرضهم للاختراقات السيبرانية.
- تعزيز الوعي بأهمية حماية الخصوصية على الإنترنت، وتوفير التدريب اللازم للطلاب حول كيفية التعامل مع المعلومات الشخصية والبيانات الحساسة على الإنترنت.
- تشجيع الطلاب على استخدام كلمات مرور قوية وتغييرها بشكل دوري، وعدم مشاركتها مع أي شخص آخر.
- التأكد من تحديث البرامج والأنظمة الخاصة بالأجهزة الإلكترونية بشكل دوري، وذلك للحد من احتمالية الاختراق السيبراني.
- توفير التدريبات اللازم للطلاب حول كيفية التعامل مع الرسائل الإلكترونية المشبوهة والرسائل النصية والمكالمات الهاتفية الاحتيالية.
- تشجيع الطلاب على استخدام شبكات الواي فاي الآمنة وتطبيق المعايير الأمنية المناسبة عند استخدام شبكات الإنترنت العامة.

- تعزيز الوعي بأهمية الحفاظ على الأمن السيبراني في المنزل وفي المجتمع، وتوفير التدريب اللازم للطلاب حول كيفية حماية الأجهزة الإلكترونية في المنزل.
- توفير الدعم الفني والأمني اللازم للطلاب في حال واجهوا أي مشاكل أمنية سيبرانية، وذلك لتعزيز الثقة والشعور بالأمان لدى الطلاب.
- توفير المزيد من الفرص للطلاب للمشاركة في المبادرات والفعاليات التي تركز على تعزيز الأمن السيبراني والخصوصية، وذلك لتشجيع الطلاب على التعلم وتطبيق المفاهيم الأمنية الحديثة.
- تعزيز الوعي بأهمية عمليات النسخ الاحتياطي للملفات والبيانات الحساسة، وتوفير الأدوات اللازمة لتنفيذ عمليات النسخ الاحتياطي بشكل منتظم.
- تشجيع الطلاب على التواصل مع الجهات الأمنية المختلفة في حالة وجود أي شبهة أمنية سيبرانية أو توفير وسائل للإبلاغ عن الهجمات السيبرانية والتهديدات الأمنية المحتملة.
- توفير نظام لتقييم مستوى الأمان السيبراني للطلاب ومعرفة مدى الوعي لديهم بأمان الإنترنت، وذلك من خلال إجراء استبيانات دورية لتحديد المستوى الحالي للأمان السيبراني في الجامعة.
- تشجيع الطلاب على استخدام برامج إدارة كلمات المرور لتسهيل عملية تذكر كلمات المرور القوية وتغييرها بانتظام.
- التأكد من تطبيق الإجراءات الأمنية المناسبة عند إجراء الدفع الإلكتروني والتسوق عبر الإنترنت، وتوفير التدريب اللازم للطلاب حول كيفية التعامل مع المعاملات المالية الإلكترونية بأمان.
- توفير الدعم الفني والأمني اللازم للطلاب في حال واجهوا أي مشاكل أمنية سيبرانية، وذلك عبر توفير قنوات اتصال سهلة وفعالة للتواصل مع فريق الدعم الفني والأمني في الجامعة.
- تعزيز الوعي بأهمية تحديث وتطوير البرامج والأنظمة الخاصة بالأجهزة الإلكترونية بشكل دوري، وذلك لتحسين أمن الأجهزة وتقليل فرص التعرض للهجمات السيبرانية.
- توفير التدريب اللازم للطلاب حول كيفية التعامل مع الحسابات الإلكترونية الخاصة بهم بأمان، وذلك من خلال تعزيز الوعي بأساليب الاحتيال وحماية الحسابات الإلكترونية وتطبيق إجراءات الأمان المناسبة لتحسين أمان الحسابات

- تشجيع الطلاب على استخدام برامج إضافية لمكافحة البرامج الضارة والتطبيقات الخبيثة، وتوفير التدريب اللازم للطلاب حول كيفية تحديد البرامج الضارة والتعامل معها.
- توفير التدريب اللازم للطلاب حول كيفية التعامل مع الروابط الاحتيالية والتحذيرات الوهمية التي تظهر على الإنترنت، وذلك للحد من تعرضهم للهجوم السيبراني.
- تعزيز الوعي بأهمية حفظ الملفات والبيانات الحساسة بطريقة آمنة وتشفيرها إذا لزم الأمر، وتوفير التدريب اللازم للطلاب حول كيفية استخدام برامج التشفير وتشفير الملفات الحساسة بشكل صحيح.
- توفير التدريب اللازم للطلاب حول كيفية التعامل مع الهجمات السيبرانية المختلفة مثل الـPhishing والـSpoofing والـMalware، وذلك لتمكين الطلاب من تحديد والتعامل مع هذه الهجمات بشكل فعال.
- تعزيز الوعي بأهمية استخدام برامج الحماية السيبرانية المجانية والمدفوعة، وتوفير التدريب اللازم للطلاب حول كيفية اختيار البرامج المناسبة لحماية أجهزتهم الإلكترونية تشجيع الطلاب على استخدام الحسابات الإلكترونية الآمنة والتحقق من صحة المواقع الإلكترونية المستخدمة لتجنب الوقوع في الفخاخ الإلكترونية والتهديدات الأمنية.
- تعزيز الوعي بأهمية الحفاظ على الأمان السيبراني للأجهزة الذكية، وتوفير التدريب اللازم للطلاب حول كيفية حماية الهواتف الذكية والحواسيب اللوحية والأجهزة الإلكترونية الأخرى من الاختراقات السيبرانية.
- توفير التدريب اللازم للطلاب حول كيفية التعامل مع الهجمات السيبرانية عبر البريد الإلكتروني والرسائل النصية القصيرة والتطبيقات المشبوهة، وتوفير المعلومات التي تساعد الطلاب في التعرف على الرسائل الاحتيالية والبريد الإلكتروني المزيف.
- تشجيع الطلاب على تطوير مهارات البحث وتحليل المعلومات السيبرانية، وذلك لتمكينهم من تحديد التهديدات السيبرانية والتعامل معها بشكل فعال.
- توفير التدريب اللازم للطلاب حول كيفية إجراء عمليات النسخ الاحتياطي للملفات والبيانات، وذلك لتأمين المعلومات وحمايتها من خسارة البيانات أو الاختراق السيبراني.

١١- كفايات التعلم الرقمي:

يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية على ضوء كفايات التعلم الرقمي من خلال مايلي:

- تعزيز الوعي بأهمية الحفاظ على الخصوصية الرقمية، وتوفير التدريب اللازم للطلاب حول كيفية الحفاظ على الخصوصية الرقمية للمعلومات الشخصية والمهنية، وذلك بتطبيق سياسات الخصوصية والحماية القوية والتحقق من مصادر البرامج والتطبيقات المستخدمة.
- تشجيع الطلاب على التحقق من صحة البريد الإلكتروني الوارد قبل النقر على الروابط المرفقة به، وتوفير التدريب اللازم حول كيفية التحقق من المرسلين والمحتويات والروابط المرفقة لتجنب الوقوع في الرسائل الاحتيالية.
- تشجيع الطلاب على استخدام الشبكات الافتراضية الخاصة (VPN) لتأمين اتصالاتهم الإلكترونية والحفاظ على الخصوصية، وتوفير التدريب اللازم حول كيفية استخدام VPN بشكل صحيح وآمن.
- تعزيز الوعي بأهمية الحفاظ على الأمان السيبراني عند استخدام الأجهزة الذكية المتصلة بالإنترنت، مثل الأجهزة المحمولة والأجهزة المنزلية الذكية، وتوفير التدريب اللازم حول كيفية تأمين هذه الأجهزة وتجنب الهجمات السيبرانية التي يمكن أن تستهدفها.
- توفير التدريب اللازم للطلاب حول كيفية التعامل مع الهجمات السيبرانية المعقدة، مثل الهجمات الإلكترونية المتقدمة (APT) والهجمات الداخلية، وذلك لتمكينهم من الكشف عن هذه الهجمات والتعامل معها بشكل فعال.
- تشجيع الطلاب على استخدام الأدوات الأمنية المتقدمة، مثل برامج الكشف عن الفيروسات وأدوات الحماية من البرمجيات الخبيثة والتهديدات الأخرى، وتوفير التدريب اللازم حول كيفية استخدام هذه الأدوات بشكل صحيح وفعال.
- تشجيع الطلاب على تطوير مهاراتهم في مجال الأمن السيبراني، وذلك عبر توفير فرص التدريب والتعلم العملي والمشاركة في المسابقات والأنشطة الخاصة بالأمن السيبراني.
- توفير الدعم الفني والأمني للطلاب الذين يعانون من مشاكل أمنية سيبرانية، وذلك عبر توفير قنوات اتصال سهلة وفعالة للتواصل مع فريق الدعم الفني والأمني في الجامعة.

- تشجيع الطلاب على الإبلاغ عن أي نشاط غير قانوني أو انتهاك للأمن السيبراني الذي يحدث داخل الجامعة، وتوفير التدريب اللازم حول كيفية الإبلاغ عن هذه الأنشطة بشكل آمن وسليم.
- تشجيع الطلاب على الاستثمار في تطوير مهاراتهم الإبداعية والابتكارية في مجال الأمن السيبراني، وذلك عبر توفير فرص التعلم العملي والتدريب الخاصة بهذا المجال، وتحفيزهم على تطوير مشاريعهم وأفكارهم الابتكارية في مجال الأمن السيبراني.
- تعزيز الوعي بأهمية الحفاظ على الأمن السيبراني في الحياة اليومية، وتوفير التدريب اللازم حول كيفية الحفاظ على الأمان السيبراني في استخدام الإنترنت ووسائل التواصل الاجتماعي والتسوق عبر الإنترنت والمصرفية الإلكترونية وغيرها من الأنشطة اليومية التي تتطلب توخي الحذر والتحلي بالحكمة في استخدامها.
- توفير الدعم الفني والأمني للطلاب الذين يرغبون في تطوير مشاريعهم الخاصة في مجال الأمن السيبراني، وذلك عبر توفير قوائم المصادر والأدوات المتاحة على الإنترنت والتي يمكن استخدامها في تطوير المشاريع الخاصة، وتوفير الدعم الفني والأمني للطلاب الذين يحتاجون إلى المساعدة في تشغيل تلك الأدوات والمصادر.
- توفير مساحات ومنصات للتواصل والتفاعل والتبادل الفعال بين الطلاب والخبراء والمتخصصين في مجال الأمن السيبراني، وذلك عبر إقامة فعاليات ومؤتمرات وندوات وورش عمل ومسابقات وأنشطة أخرى تهدف إلى تعزيز الوعي والمعرفة وتبادل الخبرات والمعلومات في هذا المجال.
- تطوير برامج تدريبية وتعليمية في مجال الأمن السيبراني يتم تقديمها بشكل متخصص ومناسب لطلاب الجامعات المصرية، وذلك بالتعاون مع الخبراء والمتخصصين في هذا المجال، ويمكن تنفيذ هذه البرامج بطرق متعددة، مثل التدريب الحضوري والتدريب عن بعد والتدريب الذاتي وغيرها.
- إنشاء مراكز أمنية سيبرانية في الجامعات المصرية، وذلك لتوفير الدعم الفني والأمني للطلاب والموظفين والباحثين والزوار، وتوفير خدمات الحماية والأمان السيبراني والتدريب والتعليم والتوعية المتخصصة في هذا المجال.
- تشجيع الطلاب على المشاركة في مجال الأبحاث العلمية والتطوير التكنولوجي في مجال الأمن السيبراني، وذلك بتوفير الدعم والموارد اللازمة لهم لتطوير

أفكارهم ومشاريعهم في هذا المجال، وتوفير المنصات والفرص اللازمة لعرض أعمالهم ومشاركتها مع الجمهور.

- تعزيز الوعي بأهمية الأمان السيبراني في المجتمع المصري بشكل عام، وذلك عبر توفير التدريب والتوعية اللازمة للجمهور حول الأخطار السيبرانية والطرق الآمنة للاستخدام الإنترنت والتكنولوجيا، ويمكن تحقيق ذلك بالتعاون مع الجهات المعنية والمؤسسات المجتمع المدني والشركاء الآخرين.
- دمج مفاهيم الأمن السيبراني في المناهج الدراسية في الجامعات المصرية، وذلك لتعزيز الوعي والمعرفة لدى الطلاب حول هذا الموضوع الهام، وتمكينهم من التعامل بشكل آمن وفعال مع التكنولوجيا والإنترنت في مساراتهم المهنية والحياتية.
- تشجيع الطلاب على الابتكار والتفكير الإبداعي في مجال الأمن السيبراني، وذلك عبر توفير الدعم والموارد اللازمة لتطوير أفكارهم ومشاريعهم الابتكارية والتنفيذية في هذا المجال، وتوفير المساحات للتعبير عن هذه الأفكار والمشاركة في المسابقات والفعاليات المتخصصة في هذا المجال.
- تعزيز التعاون والتنسيق المحلي والدولي في مجال الأمن السيبراني، وذلك عبر التعاون مع الشركاء المحليين والدوليين في هذا المجال، وتبادل الخبرات والمعلومات والتجارب والتقنيات الحديثة في هذا المجال، والعمل معًا لتطوير وتحسين الأمن السيبراني في البلاد وفي المستوى الدولي.
- تنفيذ الإجراءات القانونية اللازمة لمكافحة الجرائم السيبرانية، وذلك عبر تعزيز التشريعات والقوانين الخاصة بالأمن السيبراني وتطبيقها بشكل فعال، وتعزيز قدرات الجهات المعنية في مكافحة هذه الجرائم، وتوفير الدعم الفني والتقني والتدريب اللازم لهم لتحقيق ذلك، وذلك لضمان حماية البيانات والمعلومات والأنظمة الحيوية والحفاظ على الأمن السيبراني للمجتمع المصري.

١٢-كفايات التفكير النقدي والانتاج الإبداعي:

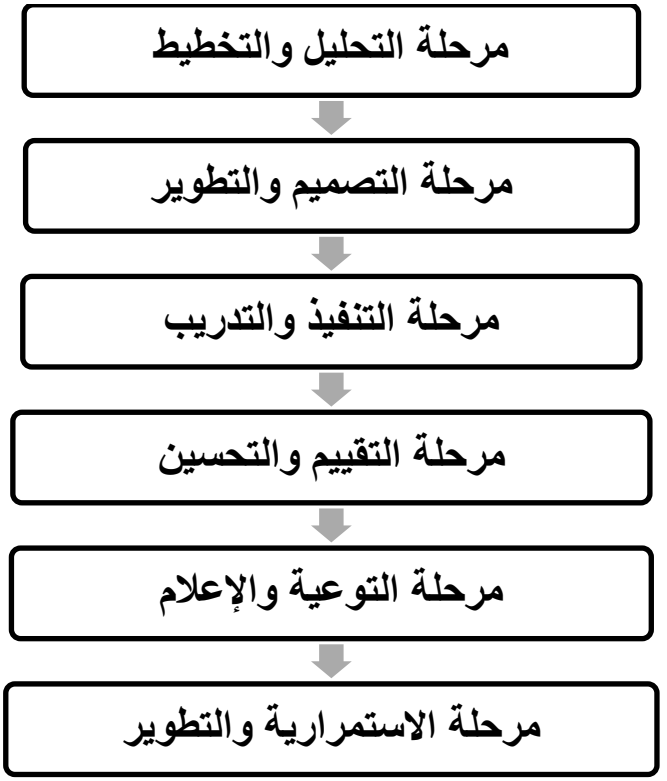
يمكن تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية على ضوء كفايات التفكير النقدي والانتاج الإبداعي من خلال مايلي:

- تطوير برامج تعليمية تشجع التفكير النقدي وتمكنهم من التحليل العميق للمعلومات ذات الصلة بالأمن السيبراني، ويمكن تضمين تدريبات تفكيرية تشجع الطلاب على تحليل الأدلة والبراهين وتقييمها واتخاذ القرارات المناسبة.

- تصميم برامج تعليمية تشجع الطلاب على التفكير خارج الصندوق والابتكار في إيجاد حلول إبداعية لمشاكل الأمن السيبراني. ويمكن تضمين تدريبات تفكيرية تشجع الطلاب على إنتاج أفكار جديدة وتصميم حلول إبداعية لحماية الأجهزة والبيانات الحساسة.
- توفير المصادر التعليمية المناسبة لتنمية ثقافة الأمن السيبراني لدى الطلاب، مثل الكتب والمقالات والدورات التدريبية، والتي يمكن أن تساعد الطلاب على فهم مفاهيم الأمن السيبراني بشكل أفضل وتعزيز قدراتهم في الحماية السيبرانية.
- تنظيم ورش عمل ومسابقات تشجع الطلاب على الإبداع والتفكير النقدي وتعزيز قدراتهم في الحماية السيبرانية. ويمكن تصميم هذه الورش والمسابقات بشكل يشجع المشاركين على تطوير مهاراتهم في الحماية السيبرانية، ويمكن أن تشمل هذه الفعاليات تدريبات وتحديات عملية تعزز قدراتهم في التعامل مع التهديدات السيبرانية وحماية الأجهزة والبيانات الحساسة.
- تعزيز الوعي بأهمية الأمن السيبراني بين الطلاب والمجتمع بشكل عام. يمكن تصميم حملات توعية تشمل إعلانات ومنشورات تعليمية تشرح أهمية الأمن السيبراني وتشجع الأشخاص على اتخاذ الإجراءات اللازمة لحماية أجهزتهم وبياناتهم الحساسة. ويمكن تضمين هذه الحملات في البرامج التعليمية والمشاريع الاجتماعية والثقافية التي يتم تنظيمها في الجامعات والمجتمعات المحلية.

خامسًا: مراحل تطبيق التصور المقترح

يتطلب تنفيذ تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية في عدة مراحل رئيسة وتتضمن كل مرحلة العديد من الأنشطة والاجراءات والأدوات المختلفة التي يجب اتخاذها وتطبيقها لضمان تنفيذ المرحلة بنجاح، ويمكن تلخيص تلك المراحل في الشكل التالي:



شكل (٤)

مراحل تطبيق تصور مقترح لتنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية

إعداد: الباحثة

- **مرحلة التحليل والتخطيط:** تشمل هذه المرحلة تحديد الهدف العام للبرنامج التدريبي والأهداف الفرعية، وتقييم الاحتياجات التدريبية للطلاب الجامعات المصرية وتحديد مستوى الثقافة السيبرانية لديهم، وذلك بإجراء استبيانات ومقابلات شخصية. كما يتم تحديد المواد التعليمية والمنهج والتقنيات المناسبة للبرنامج التدريبي، وتحديد المصادر التعليمية والجهات المشاركة والمسؤوليات والأدوار المطلوبة في عملية التنفيذ.
- **مرحلة التصميم والتطوير:** تتضمن هذه المرحلة تصميم برنامج التدريب والمنهج والمحتويات التعليمية والأنشطة التدريبية بناءً على نتائج مرحلة التحليل والتخطيط. كما يتم تطوير المواد التعليمية والتقنيات الحديثة المطلوبة، واختبار وتحسين المواد التعليمية وتطويرها حسب الحاجة. يتم تصميم الأنشطة التدريبية

بشكل يتناسب مع الأهداف المحددة، ويتم توفير جميع الأدوات والموارد اللازمة للمشاركين في البرنامج.

- **مرحلة التنفيذ والتدريب:** يتم في هذه المرحلة تنفيذ برنامج التدريب وتوفير الموارد التعليمية اللازمة. يتم إدارة الأنشطة التدريبية وتوفير الدعم الفني للطلاب والمشاركين، ويتم تقييم النتائج وتحليلها وتحديد مدى تحقيق الأهداف المحددة والتأكد على الجوانب التي يمكن تحسينها. يجب أيضًا تحديث المحتوى التعليمي والأنشطة التدريبية بناءً على تقييم النتائج وتحديد النقاط القوية والضعيفة.
- **مرحلة التقييم والتحسين:** وتتمثل في تقييم النتائج النهائية لبرنامج التدريب وتحديد مدى تحقيق الأهداف المحددة، وتحليل البيانات وتحديد النقاط القوية والضعيفة، وتحديد المساهمات والتحسينات المطلوبة. يجب أن يكون هناك تحديث دوري للبرنامج التدريبي والمحتوى التعليمي والأنشطة التدريبية بناءً على تقييم النتائج وتحديثها وتحسينها بشكل مستمر.
- **مرحلة التوعية والإعلام:** وتتضمن هذه المرحلة توعية الطلاب والمشاركين بأهمية الأمن السيبراني وكيفية الحفاظ على سلامة البيانات والمعلومات الشخصية، وذلك من خلال الإعلانات والنشرات الإخبارية وورش العمل والمنتديات والمواقع الإلكترونية والتواصل الاجتماعي. يجب أيضًا توفير دعم فني وتقني للطلاب والمشاركين في حالة الاحتياج.
- **مرحلة الاستمرارية والتطوير:** يتطلب برنامج تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية الاستمرارية والتطوير المستمر، وذلك بتقييم النتائج وتحليل البيانات وتحديد المساهمات والتحسينات المطلوبة، وتحديث المحتوى التعليمي والأنشطة التدريبية بشكل دوري ومستمر. يجب أن يكون هناك تواصل مستمر وشراكة بين الجامعات والمؤسسات الحكومية والخاصة والمنظمات المختلفة لتبادل الخبرات والمعرفة وتطوير البرامج التدريبية بشكل مستمر وفعال.

بشكل عام، يجب أن يتم تنفيذ كل مرحلة بعناية ودقة لضمان تحقيق الأهداف المحددة وتنمية ثقافة الأمن السيبراني لدى الطلاب بشكل فعال ومستدام. وعلاوة على ذلك، يجب أن يتم توفير الدعم الفني والتقني المطلوب للطلاب والمشاركين وتحديد المسؤوليات والأدوار المطلوبة لتنفيذ كل مرحلة بنجاح. وبالتالي، يمكن تنفيذ برنامج تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية بنجاح وتحقيق الأهداف المحددة بشكل فعال.

سادسًا: متطلبات تطبيق التصور المقترح

يقترح لنجاح التصور المقترح عدة متطلبات تتمثل في متطلبات تنظيمية، متطلبات تربوية، متطلبات ثقافية يمكن عرضها على النحو التالي:

١- المتطلبات التنظيمية:

تتضمن هذه المتطلبات إجراءات تنظيمية وإدارية للجامعات لضمان تحقيق أهداف وأولويات الأمن السيبراني، والتي تشمل:

- وضع سياسات وإجراءات أمنية محدثة وفعالة للحفاظ على أمن الأنظمة والبيانات المصرفية والطبية والحكومية والأكاديمية، وتحديثها بشكل دوري.
- تحديد الأهداف والأولويات الأمنية للجامعة، وتخصيص الموارد اللازمة لتحقيق هذه الأهداف.
- إنشاء فريق عمل متخصص في الأمن السيبراني للعمل على تنفيذ السياسات والإجراءات الأمنية، وتطوير استراتيجيات الأمنية اللازمة للحفاظ على أمن الأنظمة والبيانات.
- توفير التدريب والتعليم المتخصص للموظفين والطلاب حول مخاطر الأمن السيبراني والإجراءات الأمنية اللازمة للحفاظ على الأمن السيبراني.
- تحديد المسؤوليات الأمنية للجامعة وللأفراد داخلها، وضمان توفير الموارد والدعم اللازمة لتحقيق هذه المسؤوليات.

٢- المتطلبات التربوية:

تتضمن هذه المتطلبات إجراءات تربوية وتعليمية لتطوير ثقافة الأمن السيبراني لدى طلاب الجامعات المصرية، والتي تشمل:

- تطوير برامج تعليمية مخصصة لتعليم الطلاب حول مخاطر الأمن السيبراني والطرق الأمنية اللازمة للحفاظ على الأنظمة والبيانات.
- توفير موارد تعليمية متنوعة (مثل الفيديوهات التعليمية والدروس المصورة والمقالات الإلكترونية) لتعليم الطلاب حول الأمان السيبراني.
- تنظيم ورش عمل ونشاطات تفاعلية لتعليم الطلاب المهارات الأساسية المتعلقة بالأمن السيبراني، وتشجيعهم على تطبيق هذه المهارات في المشاريع الأكاديمية والابتكارية.
- تشجيع الطلاب على المشاركة في فرق الأمن السيبراني والمسابقات والأنشطة ذات الصلة، وتوفير الدعم اللازم لإنشاء وتطوير هذه الفرق والأنشطة.

- تطوير القدرات الفنية والتقنية للطلاب في مجال الأمن السيبراني، وتوفير البرامج الحديثة والأجهزة والتطبيقات التي تعزز الأمن السيبراني.
- تشجيع الطلاب على تحليل الهجمات السيبرانية والاستجابة لها، وتطوير الحلول الإبداعية لمواجهة التحديات المتعلقة بالأمن السيبراني.
- تشجيع الطلاب على التواصل والتعاون مع أفراد الجامعة والمجتمع المحلي والصناعات المختلفة لتبادل الخبرات والمعلومات حول الأمن السيبراني وتحسين مستوى الحماية.
- توفير الدعم والتشجيع للبحوث والمشاريع الابتكارية في مجال الأمن السيبراني، وتحفيز الطلاب على تطبيق الأفكار المبتكرة والحلول الإبداعية لمواجهة التحديات المتعلقة بالأمن السيبراني.

٣ – المتطلبات الثقافية:

تتضمن هذه المتطلبات إجراءات للتركيز على تحسين الوعي الثقافي لدى الطلاب حول مفهوم الأمن السيبراني وأهميته، وتشمل:

- تعزيز ثقافة الأمن السيبراني لدى الطلاب وتحفيزهم على اتخاذ الخطوات الوقائية اللازمة لحماية الأنظمة الإلكترونية والبيانات الحساسة.
- تعزيز الوعي الثقافي لدى الطلاب حول أنواع الهجمات السيبرانية المختلفة والأساليب المستخدمة فيها، وتوضيح المخاطر التي يمكن أن تترتب على عدم اتخاذ الإجراءات الوقائية اللازمة.
- تدعيم ثقافة الحفاظ على الخصوصية والسرية للبيانات الخاصة بالطلاب والموظفين والجامعة، وتوعية الطلاب حول أهمية حماية بياناتهم الشخصية.
- تعزيز الوعي الثقافي لدى الطلاب حول أهمية استخدام كلمات المرور الآمنة والتحقق بصحة المواقع والرسائل الإلكترونية والمرفقات قبل الحفاظ على الأمان السيبراني.
- توفير الدعم والتشجيع للحملات التوعوية حول الأمن السيبراني، وتشجيع الطلاب على المشاركة في هذه الحملات والأنشطة ذات الصلة.
- توفير الموارد اللازمة لإنشاء صفحات ومنتديات إلكترونية للتوعية والتثقيف حول الأمن السيبراني والتواصل مع الطلاب والموظفين والمجتمع المحلي.

- تنظيم ورش عمل ونشاطات تفاعلية للتوعية الطلاب حول الأمن السيبراني وتعزيز الوعي الثقافي لديهم حول مخاطر الهجمات السيبرانية وكيفية الوقاية منها.
- تنظيم محاضرات وندوات حول الأمن السيبراني ودعوة خبراء في هذا المجال لتقديم المحاضرات والإجابة على أسئلة الطلاب وتبادل الخبرات والمعرفة في هذا المجال.
- تشجيع الطلاب على المشاركة في المسابقات والأنشطة ذات الصلة بالأمن السيبراني، وتوفير الدعم والتشجيع اللازم لهم للمشاركة في هذه الأنشطة.
- توفير الموارد اللازمة لإنشاء وتطوير البرامج التعليمية والمواد التوعوية للطلاب حول الأمن السيبراني، وتحديثها باستمرار لمواكبة التطورات السريعة في هذا المجال.

ولتحقيق هذه المتطلبات، يجب اتخاذ عدة إجراءات، منها:

- تدريب أعضاء هيئة التدريس على الكفايات الإعلامية الرقمية وتزويدهم بالموارد اللازمة لتطبيقها في برامج التعليم السيبراني.
- توفير الأدوات والتقنيات الرقمية اللازمة لتطبيق الكفايات الإعلامية الرقمية في برامج التعليم السيبراني.
- تشجيع الطلاب على المشاركة في دورات تدريبية وورش عمل تعليمية لتطوير مهاراتهم الرقمية الأمنية.
- توفير الموارد الإعلامية الرقمية المناسبة للطلاب، مثل الدروس المصورة والنصوص الإلكترونية والفيديوهات التعليمية التي تعزز الثقافة الأمنية.
- تشجيع الطلاب على المشاركة في الفرق والأنشطة المتعلقة بالأمن السيبراني وتوفير الموارد اللازمة لإنشاء وتطوير هذه الفرق والأنشطة.
- تطوير برامج التعليم السيبراني والتأكد من تكييفها مع التحديات الأمنية الحديثة والتطورات التقنية.
- إجراء تقييم دوري للأنظمة والإجراءات الأمنية والتدريبية المتعلقة بالأمن السيبراني للتأكد من فعاليته
- توفير الموارد المالية والبشرية اللازمة لتنفيذ الخطط والبرامج والأنشطة التوعوية والثقافية.

- تحديد الجهات المسؤولة عن تطبيق هذه الخطط والبرامج والأنشطة وضمان تنسيقها وتكاملها.
- تشجيع التعاون والتنسيق بين الجامعات والمؤسسات الحكومية والخاصة المعنية بالأمن السيبراني لتحقيق الأهداف المشتركة.
- تحديد المعايير اللازمة لتقييم أداء الخطط والبرامج والأنشطة وضمان تحقيق الأهداف المرجوة.
- توفير الدعم اللازم للطلاب والموظفين في حالة وجود أي مشكلات أو استفسارات ذات صلة بالأمن السيبراني.
- تطوير قواعد السلوك الإلكتروني والسياسات المتعلقة بالأمن السيبراني والتأكد من تطبيقها بشكل صارم.
- توفير التدريب اللازم للموظفين والأساتذة والمدربين حول الأمن السيبراني وكيفية تطبيق الخطط والبرامج والأنشطة التوعوية والثقافية بشكل فعال.
- تحديد المؤشرات اللازمة لقياس تأثير الخطط والبرامج والأنشطة المتعلقة بالأمن السيبراني وتقييمها بانتظام للتأكد من تحقيق الأهداف المرجوة وإجراء التعديلات اللازمة.

سابعًا: معوقات تنفيذ التصور المقترح وآليات التغلب عليها

لا يخلو أي تصور مقترح من معوقات قد تواجه تنفيذه وفيما يلي عرض لأهم العقبات المتوقعة، وآليات التغلب عليها.

أ-المعوقات الإدارية

تتعدد المعوقات الإدارية التي تعوق تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية، ومن ثم تعرض الدراسة لأبرز المعوقات وكيفية التغلب عليها:

- قلة الخطط والسياسات التي تستهدف التعليم والتدريب على مهارات الأمن السيبراني، وضعف التعاون بين الجامعات والجهات الحكومية ذات الصلة في هذا المجال.
- نقص الموارد المالية والبشرية الكافية لتنفيذ برامج تعليمية وتدريبية حول الأمن السيبراني للطلاب.

- قلة الوعي بأهمية الأمن السيبراني لدى العديد من الطلاب، ونقص اهتمامهم بحماية معلوماتهم الشخصية والأكاديمية.
- نقص وجود سياسات وإجراءات واضحة للتعامل مع حوادث الأمن السيبراني، ونقص توفير الدعم الفني الكافي للطلاب في حال حدوث مشاكل في الأمان السيبراني.

ويمكن التغلب على هذه المعوقات، من خلال اتباع الإجراءات التالية:

- تطوير خطط وبرامج واضحة لتنمية ثقافة الأمن السيبراني في الجامعات المصرية، وتعزيز التعاون بين الجامعات والجهات الحكومية ذات الصلة في هذا المجال.
- توفير الموارد المالية والبشرية الكافية لتنفيذ برامج تعليمية وتدريبية حول الأمن السيبراني للطلاب، والتأكد من توفير الأجهزة والبرامج اللازمة لتطوير هذه المهارات.
- إعطاء الأولوية لتنمية وعي الطلاب بأهمية الأمن السيبراني، وتشجيعهم على حماية معلوماتهم الشخصية والأكاديمية.
- تطوير سياسات وإجراءات واضحة للتعامل مع حوادث الأمن السيبراني، وتوفير الدعم الفني الكافي للطلاب في حال حدوث مشاكل في الأمان السيبراني، مثل إنشاء فريق خاص للتحقق من الهجمات السيبرانية والاستجابة لها.

ب-المعوقات الثقافية

تتعدد المعوقات الثقافية التي تعوق تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية، ومن ثم تعرض الدراسة لأبرز المعوقات وكيفية التغلب عليها:

- قلة الوعي بأهمية الأمن السيبراني وتهديداته، ويمكن التغلب على ذلك من خلال زيادة التوعية بأهمية الأمن السيبراني والتهديدات الناتجة عن انتهاكه من خلال ورش عمل ومحاضرات وحملات توعية.
- ضعف اكتراث الطلاب بقضايا الأمن السيبراني، ويمكن التغلب على ذلك من خلال إثارة اهتمام الطلاب بقضايا الأمن السيبراني من خلال عقد مسابقات وتقديم حوافز لهم.

- ضعف الاهتمام بتنمية الثقافة السيبرانية من قبل الجامعات والمؤسسات التعليمية وعدم إعطائه الأولوية اللازمة، ويمكن التغلب على ذلك من خلال تحفيز الجامعات والمؤسسات التعليمية على إعطاء الأولوية اللازمة لتنمية الثقافة السيبرانية، وتوفير الموارد اللازمة لتحقيق هذا الهدف.
- قلة تضمين مقررات الأمن السيبراني في المناهج التعليمية ويمكن التغلب على ذلك من خلال تضمين مفاهيم ومبادئ الأمن السيبراني في المقررات التعليمية بالجامعات، وتدريب الطلاب على الممارسات الآمنة في استخدام تكنولوجيا المعلومات.

ج-المعوقات التكنولوجية

تتعدد المعوقات التكنولوجية التي تعوق تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية، ومن ثم تعرض الدراسة لأبرز المعوقات وكيفية التغلب عليها:

- ضعف البنية التحتية الرقمية في الجامعات، وبالتالي فإنها غالبًا ما تواجه صعوبات في توفير الأدوات والبرامج الضرورية لتعزيز الثقافة السيبرانية. ويمكن التغلب على ذلك من خلال تطوير البنية التحتية الرقمية في الجامعات وتوفير الأدوات والبرامج الضرورية لتنمية الثقافة السيبرانية.
- نقص البرامج التدريبية المتخصصة في الأمن السيبراني: حيث يواجه الطلاب صعوبات في الحصول على التدريب اللازم لتطوير مهاراتهم في هذا المجال. ويمكن التغلب على ذلك من خلال توفير برامج تدريبية متخصصة في الأمن السيبراني للطلاب والموظفين في الجامعات، وذلك لتعزيز مهاراتهم في هذا المجال.

ثامنًا: الجهات المنوط بها تنفيذ التصور

أ- وزارة الاتصالات وتكنولوجيا المعلومات

يمكن لوزارة الاتصالات وتكنولوجيا المعلومات القيام بالعديد من الأدوار المختلفة لتنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية، ولعل منها:

- توفير البيانات والإحصائيات المتعلقة بالتهديدات السيبرانية ومخاطرها والحوادث الأمنية السيبرانية التي تم التعامل معها، وذلك لمساعدة الجامعات والطلاب وأعضاء هيئة التدريس على فهم الوضع الحالي للأمن السيبراني

وتطوير استراتيجيات وحلول عملية للتعامل مع التحديات الحالية والمستقبلية.

- يمكن لوزارة الاتصالات وتكنولوجيا المعلومات المساهمة في تطوير المناهج الدراسية للجامعات المصرية لتضمن مفاهيم الأمن السيبراني، وتطوير برامج تدريبية وتعليمية تساعد الطلاب على فهم تهديدات الأمن السيبراني وتعزيز مهاراتهم في مجال الحماية.
- توفير الدورات التدريبية المتخصصة في مجال الأمن السيبراني للطلاب وأعضاء هيئة التدريس، والتي تغطي مجموعة واسعة من المواضيع المتعلقة بالأمن السيبراني، مثل الحماية من البرامج الضارة والاختراقات والهجمات الإلكترونية والتشفير والتحقق من الهوية.
- توفير الدعم الفني والتقني للجامعات والطلاب في مجال الأمن السيبراني، وذلك من خلال توفير الأدوات والتقنيات الحديثة والمعدات اللازمة للحماية الإلكترونية، والإرشادات والنصائح المتخصصة حول كيفية الحماية من التهديدات السيبرانية.
- تنظيم حملات توعوية وتثقيفية حول الأمن السيبراني للطلاب، وذلك من خلال إطلاق الحملات الترويجية والإعلانية والمواد التثقيفية والإعلامية التي تشرح مفاهيم الأمن السيبراني بطريقة سهلة ومبسطة.

ب–وزارة التعليم العالي والبحث العلمي:

يمكن لوزارة التعليم العالي والبحث العلمي القيام بالعديد من الأدوار المختلفة لتنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية في ضوء كفايات التربية الإعلامية الرقمية، ولعل منها:

- تطوير برامج تدريبية خاصة بالطلاب لتوعيتهم بأهمية الأمن السيبراني وتعريفهم بأساليب الحماية من الهجمات السيبرانية.
- توفير الموارد اللازمة لتعزيز ثقافة الأمن السيبراني، مثل المنشورات الإرشادية والمواد التعليمية المتخصصة في هذا المجال، والتي يمكن للطلاب الاستفادة منها.
- إنشاء وتعزيز الشراكات مع الجهات المعنية بالأمن السيبراني، مثل الشرطة الإلكترونية والمؤسسات الحكومية والخاصة، لتوفير دعم ومساندة للطلاب في هذا المجال.

- تحفيز الأبحاث العلمية المتعلقة بالأمن السيبراني وتشجيع الطلاب على البحث والاهتمام بهذا المجال.
- تنظيم الفعاليات والندوات المتخصصة بالأمن السيبراني، والتي تمكن الطلاب من التعرف على التحديات والمخاطر المتعلقة بالأمن السيبراني، وتعرض الأساليب الحديثة والفعالة لمواجهة تلك التحديات.
- تطوير سياسات وإجراءات تتعلق بالأمن السيبراني وتطبيقها على مستوى الجامعات، وذلك لتعزيز الوعي والحد من التهديدات السيبرانية.
- توفير الدعم الفني للطلاب في مجال الأمن السيبراني، مثل توفير البرامج والأدوات اللازمة للحماية من الهجمات السيبرانية، وتوفير الدعم الفني المتخصص لحل المشاكل الفنية وتقديم الاستشارات اللازمة في هذا المجال.
- تكثيف التوعية والحملات الإعلامية عن أهمية الأمن السيبراني والتحديات التي يواجهها الطلاب في هذا المجال، وذلك لتعزيز الوعي والحد من التهديدات السيبرانية.

باستقراء ماسبق، يمكن لوزارة التعليم العالي والبحث العلمي أن تؤدي دورًا فعالًا في تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية من خلال تطوير البرامج التدريبية وتوفير الموارد اللازمة وإنشاء الشراكات وتحفيز الأبحاث العلمية وتنظيم الفعاليات والندوات وتطوير السياسات والإجراءات وتوفير الدعم الفني وتكثيف التوعية والحملات الإعلامية. هذه الجهود ستساعد على تحسين الوعي لدى الطلاب فيما يتعلق بالأمن السيبراني وتعزيز مهاراتهم في الحماية والتصدي للتهديدات السيبرانية المختلفة.

ج- وزارة الإعلام :

يمكن لوزارة الإعلام القيام بالعديد من الأدوار المختلفة لتنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية. ومن بين هذه الأدوار:

- بث حملات إعلامية متخصصة للتوعية بأهمية الأمن السيبراني وتعريفهم بأساليب الحماية من الهجمات السيبرانية.
- تحفيز الإعلام المحلي لتغطية الحوادث السيبرانية وتوفير التقارير والأخبار المتعلقة بالأمن السيبراني، وذلك لتوعية الجمهور بالمخاطر المتعلقة بالأمن السيبراني وتعزيز الوعي والحذر.

- تنظيم الفعاليات والندوات المتخصصة بالأمن السيبراني ودعوة خبراء ومتخصصين لتقديم المحاضرات والندوات والورش التدريبية، وذلك لتعزيز ثقافة الأمن السيبراني وتعليم الطلاب الأساليب الحديثة والفعالة للحماية من الهجمات السيبرانية.
- تشجيع الأبحاث العلمية المتعلقة بالأمن السيبراني وتقديم الدعم المالي والفني للطلاب والباحثين الذين يعملون في هذا المجال، وذلك لتطوير الحلول الجديدة والفعالة لمكافحة التهديدات السيبرانية.
- إنتاج المحتوى التعليمي المتخصص في مجال الأمن السيبراني وتوفيره للطلاب والمهتمين بشكل مجاني، وذلك لتعزيز الوعي وتوسيع المعرفة حول هذا الموضوع.
- إنشاء المراكز المتخصصة في مجال الأمن السيبراني وتوفير الموارد اللازمة والدعم الفني للطلاب والمهتمين بالمجال، وذلك لتوفير بيئة تعليمية وبحثية متخصصة تساعد على تطوير الحلول والتقنيات المتعلقة بالأمن السيبراني.
- التعاون مع القطاع الخاص لتوفير البرامج والأدوات اللازمة للحماية من الهجمات السيبرانية، وتقديم الدعم الفني المتخصص لحل المشاكل الفنية وتقديم الاستشارات اللازمة في هذا المجال.
- توفير الدعم الفني للطلاب والمهتمين في مجال الأمن السيبراني، مثل توفير البرامج والأدوات اللازمة للحماية من الهجمات السيبرانية، وتوفير الدعم الفني المتخصص لحل المشاكل الفنية وتقديم الاستشارات اللازمة في هذا المجال.

في ضوء ماسبق، يمكن لوزارة الإعلام أن تؤدي دورًا فعالًا في تنمية ثقافة الأمن السيبراني لطلاب الجامعات المصرية من خلال توعية الجمهور، وتحفيز الإعلام المحلي وتنظيم الفعاليات والندوات وتشجيع الأبحاث العلمية وإنتاج المحتوى التعليمي وإنشاء المراكز المتخصصة والتعاون مع القطاع الخاص وتوفير الدعم الفني للطلاب والمهتمين بمجال الأمن السيبراني. هذه الجهود ستساعد على تعزيز الوعي لدى الطلاب حول أهمية الأمن السيبراني وتعزيز مهاراتهم في الحماية والتصدي للتهديدات السيبرانية المختلفة.

المراجع

المراجع العربية

إبراهيم، محمد معوض، غلاب، شيرين محمد محمد، الدقناوي، شادية محمد جابر، أحمد، سحر حسني غريب (٢٠٢٣). برنامج في التربية الاعلامية الرقمية في ضوء بعض مهارات القرن الحادي والعشرين، المجلة العلمية لكلية التربية النوعية جامعة دمياط، ع٧، ٢٣٤-٢٧٩.

ابن منظور، جمال الدين محمد بن مكرم (٢٠٠٨). لسان العرب، ط٦، مج٣، دار صادر، بيروت.

اتباتو، وليد (٢٠١٩). دور التربية الإعلامية في تنمية الكفايات الإعلامية لدي المراهق المتمدرس، المجلة المغربية للعلوم الاجتماعية والانسانية، ع ٨، ١٥١- ١٦٠.

إسماعيل، أسماء حسين على، أمين، حنفي حيدر، خليفة، محمد أحمد، عطا، أشرف رجب (٢٠٢٢). اثر برنامج مقترح في التربية الإعلامية على تنمية مهارات انتاج الفيديو الرقمي لدى طلاب المرحلة الثانوية: دراسة شبه تجريبية، مجلة البحوث في مجالات التربية النوعية، كلية التربية النوعية – جامعة المنيا، ع ٣٨، ٤٦٣ – ٤٩٠.

الألفي، هاني رزق عبدالجواد (٢٠٢٢). القيادات الأكاديمية وأدوارها في تعزيز ممارسات الأمن السيبراني بالجامعات الأمريكية وإمكانية الإفادة منها بالجامعات المصرية، مجلة كلية التربية جامعة المنصورة، ع١١٩، ٧٠٩-٧٧٨.

البحيري، شيرين (٢٠٢٣). دور الإعلام الرقمي في تعزيز الامن السيبراني ومكافحة التهديدات والجرائم السيبرانية، المجلة العلمية لبحوث العلاقات العامة والإعلان، كلية الإعلام، جامعة القاهرة، ع ٢٥، ٤٧-٨٥.

برادي، نعيمة (٢٠٢١). اشكالية التربية الاعلامية في المجتمع العربي وتحدياتها، المجلة العلمية للتكنولوجيا وعلوم الإعاقة، المؤسسة العلمية للعلوم التربوية والتكنولوجية والتربية الخاصة، مج٣، ع ٣، ٩١ – ١٠١.

البغدادي، مروة فتحي السيد (٢٠٢١). اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق- جامعة المنصورة، ع ٧٦، ١٤٤٦- ١٥١٣.

بوقرص، ساعد (٢٠٢٢). الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة، مجلة الأبحاث في الحماية الاجتماعية، مج ٣، ع ١، ٦١ – ٧٧.

بونيف، سامي محمد (٢٠١٩). دور الاستراتيجيات الإستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني أنموذجا، المجلة الجزائرية للحقوق والعلوم السياسية، مج٤، ع١٢١،٧ – ١٣٥

توفيق، صلاح الدين محمد، ومرسي، شيرين عيد(٢٠٢٣). متطلبات تحقيق الأمن السيبراني بالجامعات المصرية فى ضوء التحول الرقمية من وجهة نظر أعضاء هيئة التدريس: جامعة بنها أنموذجا، المجلة التربوية لكلية التربية بسوهاج، ج ١٠٥، ٧٣٧ – ٨٦١.

جاب الله، عادل موسى عوض. (٢٠٢٢). وسائل حماية الأمن السيبراني: دراسة فقهية تأصيلية مقارنة بالنظم المعاصرة، مجلة كلية الشريعة والقانون بأسيوط، ع٣٤، ج٣،٢٢٩٦- ٢٢٣٠.

الجعد، نوال حمد محمد، الاسمري، فاطمة عبدالرحمن (٢٠١٨). واقع إسهام معلمات المرحلة المتوسطة في التربية الإعلامية للطالبات، مجلة جامعة الملك عبدالعزيز: الآداب والعلوم الانسانية، مج ٢٦، ع ٢، ١٩٥–٢٢٥.

الحبيب، ماجد بن عبد الله (٢٠٢٢). درجة الوعي بالأمن السيبراني لدى طالب وطالبات الدراسات العليا بكلية التربية بجامعة الإمام محمد بن سعود الإسلامية وسبل تعزيزه من وجهة نظرهم، مجلة العلوم التربوية، جامعة الإمام محمد بن سعود الإسلامية، مج١، ع ٣٠، ٢٧١ – ٣٢٦.

حسن، أحمد جمال (٢٠١٥). التربية الاعلامية، دار المعرفة للطباعة والنشر، المنيا.

الخضري، جيهان سعد محمد، سلامي، هدى جبريل علي، كليبي، نعمه ناصر مدبش (٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية دراسة مقارنة، مجلة تطوير الأداء الجامعي، مركز تطوير الأداء الجامعي – جامعة المنصورة، مج ١٢، ع ١، ٢١٧ – ٢٣٣.

الخنيني، محمد رمضان، وهدان، محمد شعبان، حامد، ايناس محمود (٢٠١٩). اثر التربية الاعلامية الرقمية على التصفح الآمن للإنترنت لدى المراهقين، مجلة دراسات الطفولة، كلية الدراسات العليا للطفولة، جامعة عين شمس، مج ٢٢، ع ٨٥، ١١٧–١٢٣.

خير الله، منى عبداللطيف العوض، و جعفر، سالي معاوية فتحي .(2021) .مستوى تحقق كفايات التعليم الإلكتروني لأعضاء هيئة التدريس بكلية التربية بالدلم وقت جائحة كورونا، المجلة العربية للتربية النوعية، المؤسسة العربية للتربية والعلوم والآداب، ع١٧، ٣٠٩-٣٣٢.

رجب، صفاء أحمد محمود، على، وائل صلاح نجيب، و محمود، هاني نادي عبدالمقصود .(2023) . برنامج مقترح في التربية الإعلامية الرقمية لتنمية الوعي المعرفي بالخصوصية الرقمية لدى طلبة الجامعة، مجلة البحوث في مجالات التربية النوعية، كلية التربية – جامعة المنيا، ع٤٤، ٢٣٨٩-٢٤٢٩.

الرفيعي، أحمد فرحان ريس، و الشمري، نبيل كاظم نهير. (٢٠٢١). كفايات التعليم الإلكتروني لدى أعضاء الهيئة التدريسية في كليات التربية.مجلة أبحاث البصرة للعلوم الإنسانية، كلية التربية للعلوم الإنسانية- جامعة البصرة، مج٤٦، ع ٤، ٤٥٨-٤٧٧.

الركبان، الجوهرة بنت عثمان بن علي. (٢٠٢٣). تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقويمية، المجلة العربية للدراسات التربوية والاجتماعية، معهد الملك سلمان للدراسات والخدمات الاستشارية، ع١٥٩،٢٠ - ٢٠٩.

الزعبي، لؤي (٢٠٢٢). علاقة جمهور وسائل الاعلام والاتصال الرقمي بمعايير وأبعاد التربية الاعلامية الرقمية (دراسة مسحية على طلاب المرحلة الثانوية في دمشق)، مجلة جامعة دمشق للآداب والعلوم الانسانية، مج٣٨، ع ١، ٣١٩-٣٨١.

سالم، سحر خليفة، حسن، راضي رشيد (٢٠١٨). كفايات منهج التربية الإعلامية الرقمية من وجهة نظر أساتذة الجامعات العراقيين- دراسة ميدانية، مجلة الباحث العلمي، ع ٤٠، ٣٥-٥٦.

سراج، شيماء أحمد محمد أحمد (٢٠٢٢). التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي، المجلة العربية للعلوم التربوية والنفسية، المؤسسة العربية للتربية والعلوم والآداب، مج ٦، ع ٢٦، ١٩٩ - ٢١٢.

سليمان، ايناس ممدوح محمد محمد (٢٠٢٢). دور الأمن السيبراني فى مواجهة الإرهاب الإلكتروني .مجلة العلوم القانونية والاقتصادية، كلية الحقوق – جامعة عين شمس، مج ٦٤، ع ١، ١٧٣ -٢٢٥.

سليمان، قطاف، وعبدالحليم، بوقرين (٢٠٢٢). الأمن السيبراني والمضامين المفاهيمية المرتبطة به.مجلة طبنة للدراسات العلمية الأكاديمية، المركز الجامعي سي الحواس بريكة، مج٥، ع٢، ٣٧-٥٦.

سهمي، سعيد (٢٠٢٠). الاعلام الرقمي والإشاعة كيف تسهم الشائعات في التضليل وصناعة الشخصية الأسطورية، مركز عبد الرحمن السديري الثقافي،ع ٦٦، ١٢٨-١٣٢.

السيد، سماح السيد محمد. (٢٠٢١). كفايات التعليم الهجين المتطلب توافرها لدى أعضاء هيئة التدريس بالجامعات المصرية من وجهة نظر بعض خبراء التربية، العلوم التربوية، كلية الدراسات العليا للتربية- جامعة القاهرة،مج٢٩، ع١، ١٣٩ - ٢٣٧.

السيد، نهى مجدي محمد. (٢٠٢١). الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر ٢٠٣٠ .المجلة العربية لبحوث الإعلام والاتصال، جامعة الأهرام الكندية، ع ٣٥، ٤٨٤-٥١٤.

الشميمري، فهد بن عبد الرحمن (٢٠١٠). التربية الاعلامية كيف نتعامل مع الاعلام؟، مكتبة الملك فهد الوطنية للنشر والتوزيع، الرياض.

الشهري، مريم بنت محمد فضل (٢٠٢١). دَورُ إدارة الجامعة في تعزيز الوعيِ بالأمن السيبرانيّ لدى طلبة كلية التربية بجامعة الإمَام محمد بن سعود الإسلاميّة، مجلة العلوم الإنسانية والإدارية، مركز النشر والترجمة_ جامعة المجمعة، ع ٢٥، ٨٣- ١٠٤.

ضيف، لينده (٢٠١٧). التربية الإعلامية في ظل الإعلام الجديد شبكات التواصل الاجتماعي أنموذجا، مجلة المعيار جامعة الأمير عبد القادر للعلوم الاسلامية، ع ٤٢، ٤٤٣ – ٤٦٤.

الطعاني، سليمان (٢٠٢٠). الوجيز في التربية الاعلامية، دار الخليج للنشر والتوزيع، عمان، الأردن.

العقباوى، بسنت عبد المحسن (٢٠٢٢). العلاقة بين الوعي بالتربية الاعلامية الرقمية والسمات الشخصية لدى الطالبات المعلمات بكلية التربية للطفولة المبكرة، مجلة كلية التربية جامعة المنوفية، ع ١، الجزء (٤، ٣٣٠-٣٩٢.

عقيلة، عبد المحسن حامد أحمد (٢٠٢١). مؤشرات التحليل البعدي لاستخدام الاعلام الرقمي في بحوث التربية الاعلامية رؤية تحليلية نقدية، المجلة المصرية لبحوث الاعلام، كلية الإعلام – جامعة القاهرة، ع ٧٧، ج ٢، ٣٥٣- ٤٠١.

على، ايمان سيد (٢٠٢٠). اتجاهات النخبة الأكاديمية نحو تفعيل مبادئ التربية الاعلامية لدى طلاب الجامعات، مجلة البحوث الإعلامية، كلية الاعلام – جامعة الأزهر، ع ٥٥، ج٦، ٣٩١٧-٣٩٦٤.

العمارات، فارس محمد، الحمامصة، إبراهيم (٢٠٢٢). الامن السيبراني (المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، عمان، الأردن.

عوف، مروه محمد أحمد (٢٠٢١). التحديات التي تواجه التربية الاعلامية الرقمية في مجال التعليم في ضوء التحول الرقمي، المجلة المصرية لبحوث الرأى العام، كلية الاعلام – جامعة القاهرة، مج ٢٠، ع ٢، ٢٠٣-٢٦٠.

غندر، بوسي فاروق محمود (٢٠٢٣). تفاعلية طلاب الإعلام التربوي في مواجهة الأخبار الزائفة بمواقع التواصل الاجتماعي وعلاقتها بمهارات التربية الإعلامية الرقمية لديهم، مجلة البحوث الإعلامية، كلية الاعلام، جامعة الأزهر، مج٦٦، ع٣، ١٦١٣-١٧١٨.

فايز، فاطمة، أبو العز، إنجي عباس (٢٠٢١). تصور مقترح لبرنامج تدريبي لنشر التربية الاعلامية والرقمية بين الشباب الجامعي في صعيد مصر دراسة طولية شبه تجريبية، مجلة البحوث الإعلامية، كلية الاعلام، جامعة الأزهر، ع ٥٩، ج٢، ٦٣٧- ٦٩٠.

الكردي، مجدي كاظم (٢٠٢١). الأمن السيبراني والتعليم الإلكتروني في جامعات فلسطين من وجهة نظر أعضاء الهيئات التدريسية – جامعة النجاح الوطنية انموذجًا، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، مصر، مج ٢، ع ٥، ١٠٣ – ١٢٤.

كوجيل، رشيدة، العسري، أشرف (٢٠٢٠). المقاربة بالكفايات مدخل نظري تطبيقي، مجلة ابن منظور لعلوم اللغة العربية، الجمعية الليبية لعلوم اللغة العربية، ع ١، ٢٢٥-٢٣٩.

المجلس الأعلى للأمن السيبراني. استراتيجية الوطنية للأمن السيبراني ٢٠١٧ – ٢٠٢١، رئاسة مجلس الوزراء، جمهورية مصر العربية.

مجلس الوزراء، المجلس الأعلى للأمن السيبراني، قرار رئيس مجلس الوزارة رقم ٢٢٥٩ لسنة ٢٠١٤، متاح على: https://www.escc.gov.eg/page1_1.html

محمود، أحمد محمود أحمد، الشهري، فاطمة سعيد محمد (٢٠٢١). التربية الإعلامية الرقمية وأثرها في إشباع الاحتياجات التربوية والصحية للطلاب الصم لمواجهة

التحديات التي تفرضها انتشار فيرس كورونا المستجد (Covid-19) دراسة ميدانية، مجلة علوم الإنسان والمجتمع، مج ١٠، ع ٣، ٤٣٥-٤٧٧.

المحيميد، باسم بن إبراهيم. (٢٠٢٣). دور الإدارة الجامعية في تحقيق متطلبات الأمن السيبراني في جامعة الأمير سلطان الأهلية، مجلة العلوم التربوية، جامعة الأمير سطام بن عبدالعزيز، مج٩، ع٤، ٨٣-١١٦.

مصطفى، إسلام مصطفى جمعة (٢٠٢٢). جريمة اختراق الأمن السيبراني وحماية استخدام البيانات والمعلومات في القانون المصري، المجلة القانونية، كية الحقوق -جامعة القاهرة فرع الخرطوم، مج ١٢،ع ٣، ٧١٧- ٧٥٤.

مكاوي، ممدوح عبدالله، مؤيد، هيثم جوده، عثمان، إسلام أحمد (٢٠٢١). آليات تداول الشباب العربي للمحتوى الرقمي الزائف عبر وسائل التواصل الاجتماعي: نموذج مقترح في إطار مدخل التربية الإعلامية الرقمية، مجلة البحوث الاعلامية، كلية الاعلام_ جامعة الأزهر، ع ٥٦، ج٢، ٥٢٧- ٥٨٤.

ملجا، يس شريف بري. (٢٠٢٢). الكفايات التقنية لأعضاء هيئة التدريس بكليتي التربية: جامعة كردفان وجامعة الدلنج: دراسة مقارنة "٢٠٢٠-٢٠٢١ م، مجلة القلزم للدراسات التربوية والنفسية واللغوية، مركز بحوث ودراسات دول حوض البحر الأحمر وجامعة بخت الرضا، ع١٠، ٣١ - ٥٨.

مهني، محسن يوسف (٢٠٢٢). فاعلية برنامج مقترح في التربية الإعلامية لتنمية المسئولية الاجتماعية لدى طلاب الجامعة، مجلة البحوث في مجالات التربية النوعية، كلية التربية النوعية – جامعة المنيا، ع ٤٠، ٧٣١- ٧٦٥.

ناصف، أحمد مصطفى. (٢٠٢٢). دمج الأمن السيبراني في منظومة الأمن القومي: الأمن السيبراني والأمن القومي، مجلة إدارة الاعمال، جمعية إدارة الاعمال العربية، ع٤٨،١٧٨ - ٥٥.

وطفة، على أسعد (٢٠١٩). التربية الإعلامية في العصر الرقمي: البحث عن هوية في زمن افتراضي، مجلة الطفولة العربية، الجمعية الكويتية لتقدم الطفولة العربية، مج ٢٠، ع ٧٩، ١٠١-١١٦.

يوسف، ريهام سامي حسين (٢٠١٩). مهارات التربية الاعلامية الرقمية لدي طلاب الجامعات: دراسة كيفية، المجلة العربية لبحوث الاعلام والاتصال، جامعة الأهرام الكندية، ع ٢٦، ١٩٦- ٢١٥.

المراجع الأجنبية

Aborujilah, A., Al-Othmani, A. Z., Hussien, N. S., Mokhtar, S. A., Long, Z. A., & Nizam, M. (2022, March). Cybersecurity Risk Assessment Approach for Malaysian Organizations: Malaysian Universities as Case Study. In 2022 9th International Conference on Electrical and Electronics Engineering (ICEEE) (pp. 440-450). IEEE.

Adamu, A. G., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. International Journal of Electrical and Computer Engineering, 12(1), 572-584.

Al-Abdullatif, A., & Gameil, A. (2020). Exploring students' knowledge and practice of digital citizenship in higher education. International Journal of Emerging Technologies in Learning (iJET), 15(19), 122-142.

Alhaif, A. M. (2023). Training Needs of Information Specialists at Saudi Universities Libraries to Achieve Cybersecurity Requirements. International Journal of Education and Information Technologies, 17, 38-50.

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. Big Data and Cognitive Computing, 5(2), 1-15.

Aljohani, W., & Elfadil, N. (2020). Measuring Cybersecurity Awareness of Students: A Case Study at Fahad Bin Sultan University. International Journal of Computer Science and Mobile Computing, 9(6), 141-155.

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences, 12(5), 2589.

Alzahrani, L. (2021). Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes. International Journal of Advanced Computer Science and Applications, 12(11), 630 – 637.

Anjani, N. H. (2021). Cybersecurity protection in Indonesia (No. 9). Policy Brief.

Azzeh, M., Altamimi, A. M., Albashayreh, M., & AL-Oudat, M. A. (2022). Adopting the Cybersecurity Concepts into Curriculum: The Potential Effects on Students Cybersecurity Knowledge. Indonesian Journal of Electrical Engineering and Computer Science, 25(3), 1-11.

Bannister, M. (2022). Collaboration and advance planning across campus create more cybersecure colleges, universities. Campus Legal Advisor, 22(6), 4-6.

Bansal, D., Bhatia, M., Atrey, A., & Yadav, A. K. (2024). Perspective of Cybersecurity and Ethical Hacking with Vulnerability Assessment and Exploitation Tools. In Big Data Analytics Framework for Smart Grids (pp. 98-111). CRC Press.

Bhatnagar, N., & Pry, M. (2020). Student Attitudes, Awareness, and Perceptions of Personal Privacy and Cybersecurity in the Use of Social Media: An Initial Study. Information Systems Education Journal, 18(1), 48-58.

Carley, K. M. (2020). Social cybersecurity: an emerging science. Computational and mathematical organization theory, 26(4), 365-381.

Ceko, E. Cyber Security Issues in ALBANIAN HIGHER EDUCATION INSTITUTIONS CURRICULA, 56-65.

Haque, M. A., Haque, S., Zeba, S., Kumar, K., Ahmad, S., Rahman, M., ... & Ahmed, L. (2023). Sustainable and efficient E-

learning internet of things system through blockchain technology. E-Learning and Digital Media, 20427530231156711.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.

Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity, 7(1), 1-13, doi: 10.1093/cybsec/tyab005

Keinonen, M. (2023, June). The Concept of Comprehensive Security as a Tool for Cyber Deterrence. In European Conference on Cyber Warfare and Security (pp. 567-XVIII). Academic Conferences International Limited.

Kori, D., & Naik, R. (2023). Information Security Awareness Among Postgraduate Students: A Study of Mangalore University. In Handbook of Research on Technological Advances of Library and Information Science in Industry 5.0 (pp. 270-286). IGI Global.

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. Acta Polytechnica Hungarica, 18(8), 67-89.

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (2021). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. Security and Privacy, 4(2), e141. 1 – 11.

Maulani, G., Gunawan, G., Leli, L., Nabila, E. A., & Sari, W. Y. (2021). Digital Certificate Authority with Blockchain

Cybersecurity in Education. Int. J. Cyber IT Serv. Manag, 1(1), 136-150.

Miranda-García, A., Rego, A. Z., Pastor-López, I., Sanz, B., Tellaeche, A., Gaviria, J., & Bringas, P. G. (2024). Deep learning applications on cybersecurity: A practical approach. Neurocomputing, 563, 126904.

Mutunhu, B., Dube, S., Ncube, N., & Sibanda, S (2022). Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology.

Nordan, R. G. (2023). Cyberscience Undergraduate Faculty and School Official Perspectives of the Innovation and Implementation of Curriculum for Inclusion (Doctoral dissertation, Walden University).

Onyema, E. M., Edeh, C. D., Gregory, U. S., Edmond, V. U., Charles, A. C., & Richard-Nnabu, N. E. (2021). Cybersecurity Awareness Among Undergraduate Students in Enugu Nigeria. International Journal of Information Security, Privacy and Digital Forensic, 5(1), 34-42.

Park, H., Kim, H. S., & Park, H. W. (2020). A scientometric study of digital literacy, ICT literacy, information literacy, and media literacy. Journal of Data and Information Science, 6(2), 116-138.

Pinchot, J., Cellante, D., Mishra, S., & Paullet, K. (2020). Student Perceptions of Challenges and Role of Mentorship in Cybersecurity Careers: Addressing the Gender Gap. Information Systems Education Journal, 18(3), 44-53.

Pop, D., & Ermicioi, N. (2021). How can Romania leverage education to become a regional cybersecurity leader? student

paper abstract. Journal of Computing Sciences in Colleges, 37(3), 167-١٨١.

Radoniewicz, F. (2022). Cyberspace, Cybercrime, Cyberterrorism. Cybersecurity in Poland, 33-

Rashid, T. I., & Zreyazb, A. K. (2021). Relationship Between Digital Media Education, the Communication Content Industry and Community Participation: Empirical Study. Utopía y praxis latinoamericana: revista internacional de filosofía iberoamericana y teoría social, (1), 102-113.

Schmeelk, S. (2021). Perspectives on Directing a Graduate Cybersecurity Program. Computer, 54(12), 84-87.

Shafik, W. (2024). Predicting Future Cybercrime Trends in the Metaverse Era. In Forecasting Cyber Crimes in the Age of the Metaverse (pp. 78-113). IGI Global.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE Access, 8, 222310-222354.

Tetep, A. S. (2019). Students' digital media literacy: Effects on social character. International Journal of Recent Technology and Engineering (IJRTE) ISSN, 8(2), 2277-3878.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), 39.

Wang, P. (2021). Cybersecurity student talent recruitment and development: A case study. Issues Inf. Syst, 22(2), 210-222.

Wang, P., & Sbeit, R. (2020). A comprehensive mentoring model for cybersecurity education. In 17th International Conference on Information Technology–New Generations (ITNG 2020) (pp. 17-23).