GOIDI AMERICAN JOURNAL

Journal
Goidi American Journal
of Innovation Development and Investment
GOIDI INTERNATIONAL GROUP OF INSTITUTION

The American Journal of Administration and Economics

ISSN: 2837-0287 (Online)

ISSN: 2694-5606 (Print)

Library of Congress*U.S.ISSN

Available Online at: http://www.loc.gov/issn

https://portal.issn.org/resource/ISSN/2694-5606

Research Article :

دور المرأة التربوي في تعزيز الأمن السيبراني في تطبيقات الذكاء الإصطناعي

The educational role of women in enhancing cyber security in artificial intelligence applications

د. متعب بن محمد العتيبي

د. فيصل بن محمد المطيري

ملخص :

يسعى البحث في هدفه الرئيس الى التطرق لبعض القضايا التربوية المعاصرة التي تجسد دور المرأة التربوي واهميتها الفاعلة من خلال نموذجين للقضايا التربوية المستحدثة جداً وهي تطبيقات الذكاء الاصطناعي التي باتت في كل ميدان والتهديد السيبراني الذي تخلفه مثل هذه التطبيقات وكيفية الحماية منها، ويتفرع من هذا الهدف مجموعة من الاهداف الفرعية المتمثلة في التعرض لقضيتين تربويتين تقنيتين بالغة الأهمية، والحديث حول الكفايات بالأمن السيبراني وتطبيقات الذكاء الاصطناعي التعليمية، ويأتي البحث كمحاولة لسد فجوة بحثية ومساهمة علمية جديدة في مجال التعليم وقضايا التعليم المعاصرة المهنية، التي تعتبر حديثة نسبياً في المملكة العربية السعودية والوطن، ثم التطرق بشكل عملي لكيفية توظيف تقنيات الذكاء الاصطناعي لخدمة العملية التعليمية.

أما منهجية البحث التي يتم خلالها اتمام الجانب العملي من البحث وخلاله نجمع البيانات التي توصلنا إلى النتائج التي يتم تفسيرها فيما بعد في ظل أدبيات البحث وتحقيق أهداف البحث والتحقق من هدفه، وفي هذا البحث تم استخدام المنهج الوصفي التحليلي الذي برز من خلال وصف متغيرات الدراسة، وايضاً في تفسير البيانات من أجل الوصول إلى نتائج ذات معنى.

بعد التطرق للأدبيات التربوية السابقة وتحليل البيانات التي تم جمعها حول القضيتين التربويتين توصل البحث الى جملة من النتائج التي كان اهمها عرض بعض المتطلبات اللازمة لتطبيق الأمن السيبراني خاصة في المؤسسات التربوية منها تحديد إجراءات العمل في نطاق شبكة المعلومات بوضوح بما هو مسموح وما هو غير مصرح به، ووضع خطة لآليات تنفيذ العمل ووضع عقوبات في حال كان هناك تجاوز للحدود، ضرورة وجود الكوادر البشرية المدربة للتعامل مع التقنيات التكنولوجية بكفاءة عالية ، تحديث بيانات الخصوصية المتاحة عبر الشبكات بشكل دوري ومستمر منعاً للاختراق.

ونستنتج أن معظم التربويين في الحقل التعليمي يستخدمون نوعاً من الوسائط التعليمية المفتوحة مثل عرض مقاطع فيديو، أو استخدام شبكات التواصل الاجتماعي والعديد من الوسائط، هذا كله بفعل زيادة التعليم عبر الانترنت بسبب التطور التقني الكبير.

وفي ضوء نتائج البحث يوصي الباحث بضرورة توجيه المعلمين في تخطيط وتصميم المواقف التعليمية وتقويمها بالصورة التي تحقق الكفايات المحددة، ورفع كفاءة عمليتي التعليم والتعلم وتحويل بيئة التعلم إلى بيئة فاعلة، وتوفير فرص للتعلم الذاتي.

الكلمات المفتاحية: قضايا تربوية، تعليم تقني، بيئات التعلم الالكترونية، تطبيقات الذكاء الاصطناعي، الأمن السيبراني.

Summary :

The research seeks, in its main objective, to address some contemporary educational issues that embody the educational role of women and their effective importance through the development of 1 gene for very new educational issues, which are the applications of artificial intelligence that have become in every field and the cyber threat left by such applications and how to protect them from them. Among the sub-objectives represented by exposure to two very important technical educational issues, and talking about competencies

in cybersecurity and educational applications of artificial intelligence, the research comes as an attempt to bridge a research gap and a new scientific contribution in the field of education and contemporary professional education issues, which are relatively recent in the Kingdom of Saudi Arabia and the homeland, then Practically addressing how artificial intelligence techniques can be used to serve the educational process.

As for the research methodology, through which the practical side of the research is completed, and during which we collect the data that reached us to the results that are interpreted later in the light of the research literature, achieving the research objectives and verifying its goal, and in this research, the analytical descriptive approach was used, which emerged through the description of the study variables. And also in the interpretation of data in order to reach meaningful results.

After addressing the previous educational literature and analyzing the data collected on the two educational issues, the research reached a number of results, the most important of which was presenting some requirements for the application of cybersecurity, especially in educational institutions, including defining work procedures within the scope of the information network clearly with what is permitted and what is not authorized. Developing a plan for work implementation mechanisms and setting penalties in case there is a violation of the limits, the necessity of having trained human cadres to deal with technological techniques with high efficiency, updating the privacy data available through the networks periodically and continuously to prevent penetration.

And we conclude that most educators in the educational field use some kind of open educational media such as showing video clips, or using social networks and many other media, all of this is due to the increase in online education due to the great technical development.

In the light of the research results, he recommended the need to guide teachers in planning and designing educational situations and evaluating them in a way that achieves the specified competencies, raising the efficiency of the teaching and learning processes, transforming the learning environment into an effective environment, and providing opportunities for self-learning.

GOIDI AMERICAN JOURNAL
Journal
Goidi American Journal
of Innovation Development and Investment
GOIDI INTERNATIONAL GROUP OF INSTITUTION

Keywords: educational issues, technical education, electronic learning environments, artificial intelligence applications, cybersecurity.

مقدمة :

أصبحت الحاجة ملحة للقيام بكافة الأعمال عن طريق الشبكة العنكبوتية، وبات الأمر ضرورة فائقة لا يمكن القيام بدونها، وكان للمرأة اسهام بارز في ذلك، ولها دور فعال لا يمكن إغفاله أو التغافل عنه. فلقد ازداد الاهتمام بالعلاقة التي تربط منظمات الأعمال والبيئة الرقمية خلال القرن العشرين؛ بفعل الحاجة إلى تعزيز التكامل بين المجتمع والمؤسسات فيه وبالتالي تحمل مسار المسؤولية المجتمعية، بفعل هذا كله باتت هناك حاجة لإدارة الموارد البشرية باعتبارها استراتيجية لمواكبة التغيرات نحو الاستدامة والتحول الرقمي مثل الذكاء الاصطناعي وانترنت الأشياء، حيث تساهم ممارسات ادارة الموارد البشرية الرقمية في الوصول إلى الاستدامة وبالتالي تحقيق الرقي الاقتصادي والاجتماعي. (الصاوي والدباغ، ٢٠٢١).

كما وتتصف البيئة الحالية ببيئة اضطراب رقمي كبير حيث تفرض على المؤسسات حتمية مواكبتها من أجل ضمان استمراريتها، حيث تشهد هذه البيئة إقبالاً كبيراً على التحول نحو استخدام التكنولوجيا الرقمية مثل الحوسبة السحابية وانترنت الأشياء، بالتالي أصبحت أصول المنافسة العالمية حديثاً تقوم على قدرة المؤسسات في تطويع التكنولوجيا لصالحها، من أجل مسايرة جملة من التغيرات الاستراتيجية المطروحة مثل التغيرات التنظيمية البشرية. (رابحي و كاريش، ٢٠٢٠).

وأشارت الباحثة إلى قدرة التحول الرقمي على تحسين كفاءة العاملين وتفعيل الابداع وزيادة القدرة التنافسية فهو يعبر عن صورة كيان ما قائم على إحداث تغيرات في خصائص وسمات هذا الكيان عبر مجموعة من وسائل الاتصال وتكنولوجيا المعلومات، والتعامل مع التحديات الرقمية التقنية خلال نماذج الأعمال.

تشير الثقافة الرقمية إلى علاقة الثقافة التنظيمية بتكنولوجيا المعلومات وتقنيات الاتصال كعامل من عوامل نجاحها، حيث يتعلق أي تغير في المؤسسات بإحداث تغيرات جذرية في الثقافة التنظيمية السائدة فيها، فالثقافة الرقمية مظهر من مظاهر توظيف التطبيقات الرقمية في إنجاز المهام والأعمال بفاعلية و كفاءة عالية. (رابحي و كاريش، ٢٠٢٠).

وكما نرى فقد شهدت السنوات القليلة الماضية والحالية تطوراً ملحوظاً في مجال المعرفة وتكنولوجيا المعلومات باعتبار التكنولوجيا عنصراً أساسياً لا يمكن الاستغناء عنه في أي مجال من المجالات، الأمر الذي انعكس جلياً على مسميات العصر مثل عصر الانفجار المعرفي والتكنولوجي.

ونتيجة لهذا التسارع الحاصل فإن العالم يسعى إلى توظيف الجيل الخامس للأنترنت (انترنت الأشياء)، وهو عبارة عن حوسبة كل الأشياء من خلال ربط كل شيء نعرفه من خلال برتوكولات الانترنت هذا التطور أدى إلى ظهور مصطلح معاصر جديد وهو الذكاء الاصطناعي (الأسطل، ٢٠٢٠).

حيث ظهر مصطلح الذكاء الاصطناعي لأول مرة عام ١٩٥٦م باعتباره فرع من فروع علوم الحاسوب من قبل العالم جون مكارثي، وبعد عدة سنوات درس آلان تورينج قدرة الآلات على محاكاة العقل البشري وكان ذلك من خلال اللعب مع الحاسوب في لعبة الشطرنج، وفي منتصف الستينيات أصبحت تلك البحوث تحظى على تمويل من قبل وزارة الدفاع الأمريكية (الفائز، ٢٠٢١).

كما ويعد الذكاء الاصطناعي من الموضوعات بالغة الأهمية التي لفتت انتباه العلماء والباحثين حيث شهد هذا الميدان تطورات مهمة حققت آثاراً مستمرة على جميع الأصعدة العملية والاجتماعية والصحية، ويعبر مصطلح الذكاء الاصطناعي عن علم حديث ومتطور ومتجدد، يسعى إلى تصميم وابتكار أنظمة الحاسوب الذكية التي تُحاكي بطريقة ما أسلوب الذكاء الإنساني، بحيث تستطيع هذه الأنظمة أداء الأعمال بدلاً من الإنسان من خلال محاكاة وظائفه وقدراته (المصري والأغا، ٢٠٢١).

وبناءً عليه تعتقد الباحثة أن العلماء دأبوا بالتأمل في مدى إمكانية جعل الآلة تحاكي العقل البشري قدر الإمكان من خلال التفكر في بعض الطرق وأساليب التفكير التي ينتهجها العقل البشري، وذلك من أجل تسخير تلك البرمجيات لخدمة البشرية في شتى المجالات وعلى رأسها مجال التعليم؛ ليكون عاملاً مساعداً في خدمة الطلاب والمعلمين للمساعدة في تحقيق أهداف النظام التعليمي.

حيث أدت الثورة الرقمية إلى إحداث تطور غير مسبوق في مختلف المجالات شمل جميع أوجه النشاط الإنساني سواء الأنشطة الحياتية اليومية وصولاً إلى المجالات التربوية والتعليمية وغيرها من مجالات، حيث انتشر استخدام وسائل التواصل ووسائل التقنية المتعددة، التي أحدث في المقابل ظهور

الجرائم السيبرانية التي يمكن من خلالها ايقاع خسائر فادحة قد تصل إلى التلاعب بالبيانات والمعلومات أو تغيرها أو سرقتها الأمر الذي حتم وجود ما يعرف بالأمن السيبراني (المنتشري، ٢٠٢٠).

كما يتداخل الأمن السيبراني مع مختلف المجالات سواء السياسية والاقتصادية والاجتماعية والثقافية والتربوية، لأن أي مؤسسة حيوية قائمة اليوم تعتمد بالضرورة على تقنيات المعلومات في مختلف عملياتها الأمر الذي يحتم اعتمادها على الأمن السيبراني (الشمري، ٢٠٢١).

ويعتبر الأمن السيبراني أمثل خيار للتعامل مع الانترنت بكافة تطبيقاته وأنظمته المختلفة والوصول إلى الاستخدام الأمثل والحيلولة دون الوصول إلى المعلومات، لذا بات من الضروري بناء مجتمع واعٍ بأساليب الأمن السيبراني وإعداد الكوادر البشرية المؤهلة لمواجهة التهديدات السيبرانية بكفاءة (كاعوه، ٢٠٢٠).

إن امتلاك كفايات الأمن السيبراني من قبل التربويين من أهم الكفايات التي يتسلح بها في العصر الحالي؛ وذلك لأن نجاح أي مؤسسة تربوية متوقف على ما تمتلكه من معلومات، كما ان أي تربوي تغيرت مهامه تبعاً لتغير الحياة التكنولوجية التي نعيشها اليوم ولأن هناك جانب مظلم لكل هذا التطور وهو تعرض المؤسسات والشركات والمعلومات للخطر تبرز أهمية التسلح بالأمن السيبراني للقضاء على هذا الوجه المظلم (المنيع، ٢٠٢٢) .

ومن وجهة نظرنا ذلك؛ لأن التعليم أصبح معتمداً وبشكل كبير على توظيف التقنيات التكنولوجية وشبكة الانترنت، لذا وجب على المعلمين الانتباه لخطر استخدام شبكة الانترنت التي قد تتسبب في فقدان المعلومات او الاختراقات المتعددة مع تأكيد الباحثة انه لا يمكن القضاء عليها كلياً ولكن يمكن التخفيف من آثارها أو تجنب حدوثها من خلال الدور الفاعل الذي يقوم به المعلم معه ومع طلبته في سبيل تعزيز الأمن السيبراني.

- **مشكلة البحث :**

إن ما نعيشه اليوم مختلف تماماً عما عاصره آباؤنا وأجدادنا وبالطبع لن تكون الأيام كتلك التي سيعيشها أبناؤنا، فالعالم كعجلة تدور بسرعة كبيرة وكل يوجهها نحو الوجهة الأنسب بهذا العصر الذي يتسم بالتطور السريع في مختلف مناحي الحياة، حيث تعايش البشرية تقدماً سريعاً متنامياً في تطور

المعرفة وتسارع المعرفة وكافة المجالات التقنية والتكنولوجية، حيث فرضت التكنولوجيا نفسها في جميع مناحي الحياة وأهمها مجال التربية والتعليم.

حيث تولي الأنظمة التعليمية في جميع البلدان اهتماماً كبيراً في مهنة التعليم ؛ لأن جودة مخرجات التعليم تعتمد بدرجة كبيرة على جودة المؤسسات التعليمية واستثمارها واستهلاكها وتداولها كمصدر رئيس في القرن الحادي والعشرين الذي يحقق النمو، حيث يعتبر في عصرنا الحالي ان المعرفة هي رأس المال الحقيقي؛ لأن عصرنا الراهن يتسم بالتداخل بين العلوم ومنظومات الإنتاج، ويرى ان الفكر البشري هو ذا قيمة أكبر بكثير من المال، وهناك تحول كبير من مرحلة الانتاج الفردي إلى مرحلة الابداع الجماعي التي برزت بفعلها الاختراعات والتي عكست على النمو الاقتصادي والاجتماعي في السعودية.

ولقد حرصت المملكة العربية السعودية على تطوير النظام التعليمي وتحديثه بشكلٍ دوري مستمر؛ لمواكبة القضايا التكنولوجية العالمية المعاصرة، ومنها اطلاق المملكة العربية السعودية لرؤية ٢٠٣٠ لتكون منهج وخارطة طريق لتحقيق التنمية في جميع المجالات في المملكة، ولتحقيق هذه الرؤية قامت بعض الوزارات بإعادة هيكلة نظمها وعلى رأسها وزارة التعليم التي قامت بإعادة هيكلة نظامها بما يتوافق مع متطلبات المرحلة وحتى تحقق الكفاءة والفاعلية في ممارسة مهامها على أكمل وجه، ومن أجل التعامل بفاعلية مع المتغيرات والتحديات التي تعيشها المملكة كانت الرؤية المستقبلية التي ترسم معالم الطريق لتطوير التعليم من خلال منهجية علمية واضحة الأمر الذي يستلزم إعداد استراتيجيات لتطوير نظم التعليم في المملكة العربية السعودية في ضوء رؤية ٢٠٣٠ من خلال مبادرات فعالة. (اليامي، ٢٠١٨) .

كما كان لأزمة كورونا وانتشارها أثر كبير على العملية التعليمية وحفاظاً على حياة الإنسان عُلقت الدراسة وتوقفت العملية التعليمية وبات لا بد من مواجهة هذه الأزمة وتحدياتها والحد من آثارها السلبية بأكبر قدر ممكن، الأمر الذي حتم الاستفادة من التكنولوجيا الحديثة في أقصى مراحلها وكان استخدام تطبيقات الذكاء الاصطناعي على رأسها باعتباره العامل الأكثر تأثيراً في مواجهة تحديات العصر؛ لأنه يمكن أن يفتح آفاقاً جديدة في المناهج الدراسية واستراتيجيات وطرائق التدريس والعديد من المزايا التي توفرها تطبيقات الذكاء الاصطناعي والتي تفعل نجاح البرامج التعليمية.

ويرى العديد من الباحثين أن تطبيقات الذكاء الاصطناعي نعمة كبيرة بينما ينظر إليها آخرون على أنها تحدد وجود الجنس البشري؛ لأنها قد تكون قادرة على التحكم في الإنسان والسيطرة عليه لكن الواقع يعكس أن الذكاء الاصطناعي هو مستقبل الغد، حيث أظهرت بعض الدراسات أن الطلبة بنسبة تزيد عن (٥٠%) يميلون إلى اللجوء إلى الأجهزة الذكية أكثر من المدرس.

وفي ظل هذا التطور التقني الهائل كان هناك وجه آخر وهو التهديد السيبراني لذا فقد أكدت العديد من الدراسات التي تناولت الأمن السيبراني أهمية دور المعلم/ة باعتباره قائدا/ة وموجها وقدوة للطلبة داخل الصف، ومنها دراسة (Pusey & Sadera ٢٠١١)، والتي أشارت إلى أهمية تنمية مفاهيم الأمن السيبراني لدى المعلمين بما يمكنهم من تأهيل طلابهم للتعامل بقدر كبير من الوعي والمسؤولية، والالتزام بالنواحي الأمنية عند تعاملهم مع مصادر المعلومات الرقمية المختلفة، وأكدت الدراسة الصادرة عن التحالف الوطني للأمن السيبراني في الولايات المتحدة (Pruitt-Mentle ٢٠٠٨) على أهمية تعزيز الوعي لدى المعلمين بأهمية دورهم في مجال الأمن السيبراني، وانعكاس هذا الدور على إعداد الطلبة للاستخدام الرشيد لشبكات المعلومات، ومن الدراسات الأخرى التي تناولت دور المعلم وأهميته في هذا المجال دراسة(Black Clark & ٢٠١٥) والتي أكدت على أهمية مشاركة المعلمين لمعارفهم وخبراتهم التقنية، ونقل تلك الخبرات إلى طلابهم، وذلك خلال معمل افتراضي صمم بهدف تنمية الأمن السيبراني، وأظهرت الدراسة الدور الفعال للمعلمين في تنمية الأمن السيبراني لدى الطلبة، وأشارت دراسة (R.Solms & S.Solms، ٢٠١٨) إلى أهمية وعي المعلمين بكافة التطورات المتعلقة بتحديات ومفاهيم الأمن السيبراني، وحيوية هذا الدور بالنسبة لإعداد الطلبة في التعامل مع البيئات السيبرانية في عالم المستقبل.(Bicak, Liu & Murphy ٢٠١٥)

ويساعد المعلمون ذوي الكفاءة في منع التحديات المرتبطة بمخاطر وتهديدات الأمن السيبراني، وأن الأمن السيبراني هو الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته وأنظمته للمحافظة على الأفراد والمجتمع، وبالتالي يحسنون مستويات الطلاب في مجابهة البرامج الضارة التي تعتبر أكثر أشكال مخاطر الأمن السيبراني، وهناك مجموعة من الدراسات التي تدعم العلاقات بين الكفايات بالأمن السيبراني للمعلمين، وقدرتهم على حماية بياناتهم من الهجمات الإلكترونية، كدراسة (القحطاني، ٢٠١٩؛ الجندي ومحمد، ٢٠١٩؛ الموجي ومحمود وإمام،٢٠٢١؛ والصانع والسواط وأبو عيشة وسليمان وعسران،٢٠٢٠).

ويتضح من العرض السابق أهمية تعزيز الأمن السيبراني ودور المرأة في ظل الثورة الرقمية والتكنولوجية المعاصرة، وما اتخذته دول العالم من إجراءات للالتزام بقواعد ومفاهيم الأمن السيبراني، وما أولته تلك الدول من أدوار مهمة للمؤسسات التربوية، وخاصة دور المعلم/ة وأهمية امتلاك الوعي المناسب بالأمن السيبراني، وما أكدت عليه الدراسات السابقة في هذا المجال.

- **أهداف البحث :**

يسعى البحث في هدفه الرئيس إلى التطرق لبعض القضايا التربوية المعاصرة التي تجسد دور المرأة التربوي واهميتها الفاعلة من خلال نموذجين للقضايا التربوية المستحدثة جداً وهي تطبيقات الذكاء الاصطناعي التي باتت في كل ميدان والتهديد السيبراني الذي تخلفه مثل هذه التطبيقات وكيفية الحماية منها، ويتفرع من هذا الهدف مجموعة من الاهداف الفرعية المتمثلة في التالي:

١. ندرة الدراسات –حسب علم الباحث – حول الكفايات بالأمن السيبراني وتطبيقات الذكاء الاصطناعي التعليمية، ويأتي البحث كمحاولة لسد فجوة بحثية ومساهمة علمية جديدة في مجال التعليم وقضايا التعليم المعاصرة المهنية، التي تعتبر حديثة نسبياً في المملكة العربية السعودية والوطن العربي.
٢. التطرق بشكل عملي لكيفية توظيف تقنيات الذكاء الاصطناعي لخدمة العملية التعليمية.
٣. قد تُساعد نتائج البحث في إيجاد حلول عملية من خلال حماية الفرد والمجتمع في ظل ازدياد التهديدات والمخاطر السيبرانية التي تهدد المنظومة التعليمية.

الإطار النظري:

المحور الأول: الذكاء الاصطناعي Intelligence Artificial

مفهوم الذكاء الاصطناعي

يعد الذكاء الاصطناعي أحد فروع علم الحاسوب وأحدى الركائز الأساسية التي تقوم عليها صناعة التكنولوجيا في العصر الحالي، تأسس على افتراض أن ملكة الذكاء يمكن وصفها بدقة لدرجة تمكن الآلة من محاكاتها، وهو علم من علوم الحاسوب يرتبط بأنظمة الحاسوب التي تمتلك الخصائص المرتبطة بالذكاء واتخاذ القرار المحاكي للسلوك البشري (محمود، ٢٠٢٠).

ويرى الباحث أن الذكاء الاصطناعي يقوم على تمثيل برنامج حاسوبي لمجال من المجالات وتطويره ومن ثم مقارنته بمواقف وأحداث ذات المجال للخروج باستنتاجات مفيدة، وأن الفرق بين الذكاء الاصطناعي والذكاء الانساني هو القدرة على استحداث النموذج؛ فالعقل البشري قادر على إبداع وابتكار هذا النموذج، بينما يمثل النموذج الحاسوبي نموذج سبق استحداثه في العقل البشري.

بينما تعرف تطبيقات الذكاء الاصطناعي على أنها مجموعة من التقنيات والأنظمة الحاسوبية والتطبيقات الإلكترونية الذكية التي تتسم بقدرتها على الانخراط في عمليات العقل البشري ولها القدرة على حل المشكلات وتساعد على التعلم بكفاءة (ابراهيم، ٢٠٢٢).

أهداف الذكاء الاصطناعي

يعتبر الذكاء الاصطناعي من أهم نتائج العصر الرقمي وظهور التكنولوجيا الرقمية، فهو ثمرة من ثمار التطور التكنولوجي الذي بذل فيه الإنسان كل امكانياته المعرفية والعملية والمادية من أجل تحقيق الهدف المتمثل في إيجاد عقل اصطناعي يمكنه التفكير معه ومساعدته وتقديم الاشارات الهامة له، وتتلخص أهداف الذكاء الاصطناعي فيما أشار إليه (المصري والأغا، ٢٠٢١) بعد التطرق للعديد من الدراسات وهي:

١. الوصول إلى أنماط معالجة العمليات العقلية العليا الحاصلة داخل العقل الانساني.
٢. تسهيل استخدام فوائد الحاسوب من خلال قدراته على حل المشكلات.
٣. تطوير برامج الحاسوب بحيث تستطيع حل المشكلات.
٤. فهم طبيعة الذكاء الإنساني لعمل برامج حاسوبية قادرة على محاكاة السلوك الإنساني.
٥. تصميم أنظمة ذكية تعطي ذات الخصائص التي يتسم فيها الذكاء البشري.

خصائص الذكاء الاصطناعي

يتمتع الذكاء الاصطناعي بالعديد من الخصائص والمميزات التي أشار إليها (محمود، ٢٠٢٠).

١. توظيف المشاكل في حل المشاكل المعروضة.
٢. خاصية التفكير والإدراك.
٣. اكتساب المعرفة وتطبيقها.
٤. التعلم والفهم والاستجابة من الخبرات السابقة.

٥. توظيف الخبرات السابقة في مواقف جديدة.
٦. الاستجابة السريعة للمواقف والظروف الجديدة.
٧. التعامل مع الحالات الصعبة والمعقدة.
٨. تمييز الأهمية النسبية لعناصر الحالات المعروفة.
٩. التصور والإبداع وفهم الأمور المرئية.
١٠- الافادة من المعلومات المتاحة في اتخاذ القرارات .

ويشير الباحث إلى أن من أهم خواص تطبيقات الذكاء الاصطناعي أنها تعمل التسريع في اكتساب المهارات بصورة متقنة وبكل سهولة، وكذلك سهولة الوصول إلى المحتوى العلمي، ورفع المستوى العلمي، وبناء تمثيل كميات هائلة من المعارف الخاصة بمجال معين بحيث تعالج البيانات الرمزية غير الرقمية من خلال عمليات التحليل والمقارنة المنطقية؛ لمحاكاة الإنسان فكراً وأسلوباً لإثارة أفكار جديدة تؤدي إلى الابتكار.

أهمية الذكاء الاصطناعي في التعليم

تواجه النظم المدرسية عدداً من التحديات مثل نقص المعلمين والافتقار إلى طرق واضحة لتطوير الأداء التدريسي للمعلمين والكفاح المبذول من أجل تلبية الاحتياجات التعليمية وسط ضغوط التعليم، فالذكاء الاصطناعي يوفر خيارات متعددة جديدة لمعالجة العديد من الظروف الصعبة من خلال عدة اساليب منها (ابراهيم، ٢٠٢٢).

١. زيادة فاعلية المعلمين وتفعيل أدوارهم بكفاءة.
٢. توفير العديد من جوانب المحتوى الأساسية ومهارات التدريس ومنح المعلمين المزيد من الوقت والطاقة
٣. حاجة المعلمين إلى مهارات التدريس أكثر من حاجتهم للمحتوى الأكاديمي وللمهارات الحياتية تلعب دوراً مهماً إلى جانب اتقان المحتوى.
٤. يعتبر المعلون الخبراء المورد الأكثر قيمة في النظام التعليمي ومن غير المعقول اعتزال عمل المعلمين إلى اجراءات موحدة أو مهام تلقائية.
٥. انتقال الفصول الدراسية إلى الإطار الملائم للتعلم من خلال استخدام مزيج من الروبوتات والذكاء الاصطناعي المصمم حسب الحاجة.

الذكاء الاصطناعي وسيط جيد للتعليم والتعلم

تساعد تطبيقات الذكاء الاصطناعي على معالجة محتوى التعلم وفقاً لطبيعة الأهداف المرجوة وتحقق مبدأ الفروق الفردية بين المتعلمين من خلال التعامل مع المثيرات والوسائط المتعددة التفاعلية، وهي ميزة خاصة في تعلم البرمجة خاصة من حيث تضمنها عدة خطوات متدرجة من السهولة والصعوبة، كما يمكن النظر إلى البرمجيات المبنية على الذكاء الاصطناعي على أنها نظم خبيرة في مجال التعليم معتمدة بدرجة كبيرة على نمذجة المعرفة الخاصة بالمتعلم ومحاكاة سلوكياته وطريقته في حل المشكلات، يتم ذلك كله من خلال تداخل علوم الحاسوب ونظريات علم النفس المعرفي والتعليم والتدريب على شكل منظومة متفاعلة تشكل نظام تعلم ذكي (شاكر، ٢٠٢٠).

والجدير بذكره إن تطبيقات الذكاء الاصطناعي بمختلف أشكالها ومراحلها مستمرة في التطور والدخول في مجالات حياتنا اليومية وبشكل ملحوظ، وإن حق لي القول أن أقول أنها في طور التقدم والرقي متزامنة من النهضة المعلوماتية، وفي المقابل تحتاج إلى جهد بشري من قبل المعلمات والكادر البشري عموماً لمواكبة ذلكم التقدم والعمل على تفعيله في شتى المجالات، لكن من أجل تحقيق أفضل استخدام لتطبيقات الذكاء الاصطناعي في المؤسسات التعليمية فإن هذه المؤسسات تحتاج الخبرة الكافية في إنشاء منظومة الذكاء الاصطناعي وإدارتها على أوسع نطاق، وتوفير البنية التحتية اللازمة للتنفيذ وكافة الأدوات والاستراتيجيات التي تضمن نجاح تطبيق هذه التطبيقات وتيسير الربط بين المعرفة والخبرة العملية خاصة في المجالات التطبيقية مثل البرمجة.

المحور الثاني: الأمن السيبراني

كانت بدايات تهديدات أمن المعلومات منذ أن كان الهاتف هو وسيلة الاتصال الوحيدة في سبعينيات القرن العشرين، عندما حاول البعض ربط سلك الهاتف بشخص آخر ليتمكنوا من استراق السمع على أحاديثه حتى ظهر اختراع الحاسوب ومن ثم الأنترنت وبدأ ظهور اول فايروس كمبيوتر واختراع أول برنامج لمواجهة الفايروسات، وفي الثمانينيات تطورت الأجهزة المضادة للفيروسات الى تسعينيات القرن حيث ازداد الاتصال بشبكة الانترنت وبذلك ازدادت التهديدات الأمنية للمعلومات واصبح هناك قوانين تحذر الاختراقات المعلوماتية الأمنية، وبدأت التحذيرات بالسجن وتكبده غرامات كبيرة لمن يخترق قانون أمن المعلومات لكن الهجمات لازالت تشتد وتواصل العديد من المنظمات ايجاد حلول للتصدي

لتلك الهجمات أو التخفيف من آثارها مثل برنامج تحليل سلوك الشبكة، وجدران حماية تطبيق ويب، وبالتالي اصبح الأمن السيبراني يزداد قوة (شرف، ٢٠٢٠) .

تعريف الأمن السيبراني

يتكون المصطلح من الكلمة اللاتينية (سايبر) والتي تعني فضاء المعلومات، وبالتالي فهي تعني أمن فضاء المعلومات، ويشير إلى مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها بشكل غير مصرح به، بهدف ضمان استمرارية عمل نظم المعلومات واتخاذ جميع التدابير اللازمة كل من يتعامل مع التقنية والشبكات من التهديدات الأمنية.(Lallie, H2021)

يعرفه (الغامدي والمساندي، ٢٠٢١، ص١٤٨) على أنه "مجموعة من الأدوات التنظيمية والتقنية والاجرائية والممارسات الهادفة إلى حماية أصول المعلومات مثل الحواسيب والشبكات والبرمجيات بما بداخلها من بيانات من التهديدات الداخلية والخارجية، او التلف او التغيير أو التعطيل من الوصول لتلك المعلومات أو الخدمات".

وتعرفه (المنتشري، ٢٠٢٠) بأنه "جميع اجراءات حماية شبكات المعلومات ضد كافة الأعمال والممارسات التي تستهدف التلاعب بتلك المعلومات وإلحاق الأذى بالمستخدمين بما يشمل الحماية ضد الاختراق، وبث البرمجيات الخبيثة والفيروسات والوصول غير المصرح به وغير ذلك من ممارسات،سلبية".

ويمكن تعريف الأمن السيبراني تبعاً لأهدافه على أنه "النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنية الاتصالات والمعلومات ويضمن امكانات الحد من الخسائر والأضرار المترتبة في حال المخاطر والتهديدات، كما ويتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن بحيث لا تتوقف عجلة الانتاج ولا تتحول الأضرار إلى خسائر" (البغدادي، ٢٠٢١).

ويتشابه مفهوم الأمن السيبراني بمفهوم أمن المعلومات إلا أن هناك اختلافات جوهرية بينهما فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما يهتم أمن المعلومات بأمن البيانات الورقية، فمفهوم الأمن السيبراني أوسع من مفهوم أمن المعلومات بحيث يتضمن تأمين البيانات المتداولة عبر الشبكات سواء داخلية أو خارجية، وأمن المعلومات يحافظ على سلامة المعلومات ويبقيها محفوظة كما هي (الصحفي، ٢٠١٩).

ويميل الباحث إلى ما مال له البغدادي؛ لشمولية المفهوم من وجهة نظري. ويتضح لنا مما سبق أن الأمن السيبراني ليس بطريقة محددة او وسيلة لحماية الشبكات، بل هو أسلوب يفتح الطريق أمام كل جديد في سبيل تحقيق أمن المعلومات والشبكات وحماية البيانات المنتقلة عبر الأجهزة الرقمية المختلفة لجميع المستخدمين، وان مختلف الباحثين متفقين على انه يمثل مفهوم أمني بالدرجة الأولى خاص بحماية البيانات وكل ما يتصل بتلك البيانات من ممارسات وخدمات وأجهزة وتقنيات ضد أي شكل من أشكال الوصول غير المسموح به بالشكل الذي قد يشكل خطراً على الأفراد أو المستخدمين.

عناصر الأمن السيبراني

للأمن السيبراني ثلاثة عناصر أساسية يقوم عليها متمثلة في:

١. السرية: أي سرية المعلومات والمحافظة عليها ومنع الوصول اليها الا من المصرح لهم.
٢. تكامل وسلامة المعلومات: أي المحافظة على محتوى البيانات من التعديل أو التغيير أو الحذف أو الإضافة من غير المصرح لهم.
٣. توافر البيانات وإتاحتها: أي توافر المعلومات للأفراد المشرفين عليها واستخدامها في الوقت المناسب لتلبي الغرض منها (المنيع، ٢٠٢٢).

وتضيف (الصانع، ٢٠٢٠) عناصر يجب توافرها للأمن السيبراني لضمان حماية المعلومات وهي:

١. المحافظة على السرية والأمن للمعلومات.
٢. المحافظة على تكاملية المعلومات وسلامتها.
٣. التأكد من استمرارية عمل النظام المعلوماتي وتقديم الخدمات المطلوبة .
٤. عدم إنكار التصرف بالمعلومات او استلامها.

يتضح لنا مما سبق أن عامل السرية والتكاملية والاستمرارية وحسن التصرف للمعلومات هي أهم عناصر الأمن السيبراني التي بتوافرها يتحقق أمن المعلومات ويقلل من أثر الاختراقات.

أهداف الأمن السيبراني :

يحظى الأمن السيبراني بأهمية بالغة؛ لأن مختلف المؤسسات تقوم على قدر ضخم من البيانات على أجهزة الحواسيب وقدر كبير جدا من هذه المعلومات قد تكون على قدر عالٍ من الحساسية خاصة فيما يتعلق بالملكية الفكرية أو المعلومات الأمنية أو البيانات الشخصية والدخول بطريقة غير

مشروعة قد يكون له عواقب وخيمة لذا تجد المؤسسات امام تحدي كبير وهو حماية بياناتها ومعلوماتها، ويمكن إجمال أهم أهداف الأمن السيبراني فيما يشير إليه (الشمري، ٢٠٢١).

١. السرية: السماح للأفراد المصرح لهم فقط يمكنهم الوصول للبيانات.
٢. النزاهة: الأفراد المصرح لهم فقط هم من يمكنهم إجراء أي تغيرات في النظام.
٣. توفر النظام والمعلومات التي يديرها النظام وبالتالي لا يسمح إلا بكيانات مصرح لها يمكنها الوصول إلى البيانات.

ويشير (البيشي، ٢٠٢١) عن عدة دراسات أوردت أهداف الأمن السيبراني، ومنها:

١. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة وباختلاف مكوناتها من أجهوة وبرمجيات وخدمات وما تشمله من بيانات.
٢. التصدي لهجمات أمن المعلومات التي تستهدف مؤسسات القطاعين العام والخاص.
٣. توفر بيئة آمنة تتسم بالثقة في التعاملات في مجتمع المعلومات وتطوير البنى التحتية حساسة لأي هجمات الكترونية.
٤. توفير الحد اللازم من المتطلبات التي تساهم في الحد من المخاطر الالكترونية.
٥. محاولة التخلص من الثغرات ونقاط الضعف في الحواسيب والشبكات والأجهزة المحمولة.
٦. سد الثغرات في أنظمة المعلومات.
٧. مقاومة البرمجيات الضارة والخبيثة والحد من التجسس الالكتروني.
٨. الاهتمام باتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من الاضرار الالكترونية وتدريبهم على آليات مواجهة تلك الاختراقات.

ومن أهداف الأمن السيبراني في المؤسسات التربوية كالجامعات السعودية ما أوردته (المنيع، ٢٠٢٢)

١. حماية البنى التحتية للمعلومات والبيانات الخاصة بالطلاب والمعلمين.
٢. حماية شبكة المعلومات والاتصالات الخاصة بالمؤسسة.
٣. التعرف على أهم التقنيات المرتبطة بأمن المعلومات وكيفيه تطويعها.
٤. تشفير جميع المعاملات الرقمية.
٥. توفير بيئة عمل آمنة عبر الشبكة العنكبوتية.

أهمية الأمن السيبراني

للأمن السيبراني أهمية بالغة ذات علاقة وطيدة بمحيط الإنسان وتعاملاته ونحو ذلك، فقد أوردت الكثير من الدراسات أهمية الأمن السيبراني وتطرقت اليه بدافع الأهمية؛ حيث ان تصعيد الهجمات الاحتيالية يعد المعضلة الكبيرة والامن السيبراني الوسيلة الدفاعية للتصدي لمثل هذه الهجمات، كما ويحافظ الأمن السيبراني على سلامة المعلومات لتكون على جهورية تامة وقت الحاجة وبعيدة عن أيدي الاختراق، كما يمكن خلاله معرفة الثغرات التي تصيب أي نظام ومعالجتها وتوفير بيئة آمنة للمستفيدين (البيشي، ٢٠٢١).

لقد حققت المملكة العربية السعودية إنجازاً عالمياً في مجال الأمن السيبراني، حيث حصلت على المركز الثالث عشر عالمياً والأول عربياً من بين مائة وخمس وسبعين دولة دمعهم المؤتمر العالمي للأمن السيبراني وذلك بعد إنشاء الهيئة الوطنية للأمن السيبراني ٢٠١٧\١٠\٣١، وهي بذلك ترسم خطواتها لتحقق فضاء سيبرانني آمن (المنيع، ٢٠٢٢) .

وقد هدفت دراسة (العتيبي، ٢٠٢٠) إلى التعرف على دور الأمن السيبراني في تحقيق رؤية ٢٠٣٠، وكان من أهم نتائجها : وجود ارتباط بين برامج رؤية المملكة ٢٠٣٠ والمكونات الأساسية للأمن السيبراني.، تتوافر عدة عناصر من متطلبات الأمن السيبراني والضرورية لتعزيز برامج رؤية المملكة ٢٠٣٠، توجد بعض المعوقات التي تحد من تطبيق الأمن السيبراني في رؤية المملكة ٢٠٣٠، وأوصت بتفعيل المكونات الأساسية للأمن السيبراني ومراجعة وتقييم آلياتها ووظائفها وتطبيقها في كافة الأجهزة الحكومية، و مراقبة ومراجعة المكونات الفرعية للأمن السيبراني والتأكد من تطبيقها في كافة الأجهزة الحكومية، و وضع خطط وبرامج وأهداف استراتيجية في الأنظمة الرقمية العاملة في المملكة وتضمينها لخطط وبرامج وأهداف متوافقة مع مكونات الأمن السيبراني في المملكة، و تطبيق حزم التحديثات والإصلاحات الأمنية بشكل دوري ومنتظم وسد الثغرات للحد من انتشار الهجمات الموزعة عبر الفضاء السيبراني.

وفي ذات الصدد هدفت دراسة (الشهري، ٢٠١٩) إلى اقتراح رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية، و تمحورت أهداف الدراسة في: التعرف على طبيعة الجرائم الإلكترونية وأسبابها، والاستبصار للمهددات والمخاطر التي تعترض الأمن

السيبراني في المملكة العربية السعودية للوصول لرؤية استراتيجية تحد من الجرائم الإلكترونية وتعزز الأمن السيبراني، وكان من أهم النتائج التي توصلت اليها: تبين أن الجرائم الإلكترونية لا تعترف بأي حدود زمانية أو مكانية وهذه الخاصية تمثل أهم السمات المميزة لطبيعة الجرائم الإلكترونية. ٢. تبين أن التقنيات الحديثة والانترنت وفرت فرصًا غير مسبوقة لانتشار الجرائم الإلكترونية، كما تبين أن انتهاك السياسات الأمنية الخاصة بالأمن السيبراني تمثل أهم التهديدات التي تواجه الفضاء السيبراني في المملكة العربية السعودية.

فمن خلال ما سبق عرضه يبرز لنا الأهمية التي تحوم حول الأمن السيبراني والضرورة المرتبطة به، التي لا يمكن إغفالها أو تجاهلها أو تجاوزها بشكل من الأشكال.

الأهمية التربوية للأمن السيبراني

لقد ساهم اعتماد العملية التعليمة على الأجهزة الإلكترونية ووسائل الاتصال بفعل جائحة كورونا التي غزت العالم وبفعل التطور الرقمي الهائل في العديد من بلدان العالم، الأمر الذي أدى بوقوع العديد من المعلمين كضحية لأحد الجرائم السيبرانية مما أثر على المعلم والمؤسسة التعليمية والحق الأضرار الأمر الذي يعكس أهمية الأمن السيبراني لكل معلم معاصر اليوم (المنتشري، ٢٠٢٠).

ويشير الباحث أنه تنعكس تلك الأهمية على الطلبة والاداريين حول العالم؛ لأن فرص وقوعهم ضحايا لمثل هذه الجرائم كبيرة ويتضح لنا مما سبق ان جميع أركان العملية التعليمية بحاجة لضمان سرية وخصوصية المعلومات فيها ومتابعة ومراقبة الامن المعلوماتي في كل مدرسة وكل مؤسسة تربوية.

ويُشار إلى أن هناك عدة تهديدات الكترونية تعرض لها قطاع التعليم بشكل خاص في المملكة العربية السعودية وأودت الى الخسارة، حيث بلغت الخسائر في هذا السياق (١٤%) وهي أكبر نسبة لتلك الهجمات بالنظر للقطاعات الأخرى، من هنا تبرز الأهمية الكبرى للأمن السيبراني للمعلمين خاصة في الحقل التربوي (المنتشري، ٢٠٢٠).

كل ذلك ينعكس ببالغ الأهمية على المؤسسات التربوية؛ لما تؤديه من دور مهم في التوعية الحقيقية للأمن السيبراني وإعداد الافراد المؤهلين ويمكن اجمال تلك الاهمية بما يشير اليها (كاعوه، ٢٠٢٠).

١. تضم المؤسسة التعليمية الجيل الرقمي الذي هو أكثر عرضه للمخاطر السيبرانية.

٢. حاجة المعلم لتوافر هذا الأمن بسبب الأضرار النفسية التي يتعرض لها عند تعرضه لتلك الحوادث.

٣. الخسارة الكبيرة للأبحاث والأوراق المنشورة الخاصة بالمؤسسة التعليمية.

كما دعت الدراسات إلى أهمية وعي المعلمين والمعلمات بمفاهيم الأمن السيبراني حيث هدفت دراسة (العقلاء، ٢٠٢٢) إلى الكشف عن درجة الوعي بمفاهيم الأمن السيبراني لدى معلمي ومعلمات الحاسب الآلي بمدينة حائل. واعتمدت الدراسة على المنهج الوصفي المسحي، وتم تطبيق استبانة إلكترونية على عينة عشوائية مكونة من (١٨٤) معلم ومعلمة حاسب آلي بالمرحلتين المتوسطة والثانوية بمدينة حائل. ولمعالجة البيانات استخدمت الباحثة حزمة من الأساليب الإحصائية باستخدام برنامج (SPSS). وأظهرت الدراسة أن درجة وعي معلمي ومعلمات الحاسب الآلي في مدينة حائل بماهية الأمن السيبراني جاءت متوسطة، كما أنها أشارت إلى أن درجة وعيهم بطرق المحافظة على نظام الأمن السيبراني جاءت متوسطة أيضاً، مع وجود فروق ذات دلالة إحصائية في وعي معلمي ومعلمات الحاسب الآلي بالأمن السيبراني تعزى متغيرات للجنس لصالح المعلمات، كما أن معلمي ومعلمات المرحلة المتوسطة لديهم وعي بالأمن السيبراني أعلى من معلمي ومعلمات المرحلة الثانوية وبفارق دال إحصائياً، ولا توجد فروق ذات دلالة إحصائية في وعي معلمي ومعلمات الحاسب الآلي بمفاهيم الأمن السيبراني تعزى لمتغير الخبرة أو المؤهل الأكاديمي، بينما توجد فروق ذات دلالة إحصائية في وعي معلمي ومعلمات الحاسب بمفاهيم الأمن السيبراني تعزى لمتغير الدورات التدريبية، لصالح من تلقى دورة تدريبية واحدة فأكثر. وفي ضوء هذه النتائج قدمت الباحثة جملة من التوصيات والمقترحات لزيادة درجة الوعي بالأمن السيبراني ومفاهيمه لدى معلمي ومعلمات الحاسب الآلي.

فالمعلمة(المرأة) تشعر بذلك الوعي وتلك المسؤولية التي تحيط بها من أجل التكامل في العملية التعليمية والنهوض بها نحو الرقي والتقدم؛ مما جعلها تسهم بدور فعال في ذلك المجال.

دور الأمن السيبراني في المؤسسات التربوية

يبرز دور الأمن السيبراني من خلال رؤية ٢٠٣٠ التي دعت إلى انشاء وحدات الأمن السيبراني داخل تلك المؤسسات، وتقوم بدورها في تقديم الخدمات التوعوية والتعليمية والبحث العلمي عبر جملة من الوسائل اشار اليها (المنيع، ٢٠٢٢) وهي:

١. التوعية بالحاجة الى الأمن وزيادة الثقافة الأمنية للمتعلم.
٢. عقد لقاءات تدريبية للمعلمين والطلبة حول تقنيات الأمن السيبراني.
٣. تقديم خدمات تقنية واستشارية في حال الحاجة حول الأمن الرقمي.
٤. وضع حلول آمنة يتم اللجوء اليها حال تعرض المؤسسة للهجوم او الاختراق.
٥. حفظ حقوق الملكية الفكرية والتشجيع الكبير للبحث في المجال التقني الأمني.

ولسياسات الأمن السيبراني دور في تعزيز التحول الرقمي العالمي الذي تدعو اليه المؤسسات اليوم، ففي دراسة (كاعوه، ٢٠٢٠) هدفت إلى لتقديم رؤية مقترحة لتضمين سياسات الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي، حيث توجهت الحكومه المصرية لتطبيق استراتيجية التحول الرقمي لجميع الهيئات والمؤسسات لرفع مستوى أدائها، وبالتالي تعمل الجامعات المصرية لتطوير أدائها وتوفير متطلبات التحول الرقمي لجميع احتياجاتها ويتم ذلك في ظل بيئة خارجية تتسم تتزايد التغيرات المتسارعة لتكنولوجيا الإتصالات مما يمثل تحديا للتحول الرقمي وتزايد الاعتماد على الخدمات الرقمية في التواصل والعمل من بعد ما يتسبب لتعرض الجامعات للاختراقات المختلفة والمخاطر السيبرانية المتعدده، وعرضت الدراسة مفهوم التحول الرقمي للجامعات ومبررات التحول الرقمي للجامعات، وخطوات ومتتطلبات تطبيق التحول الرقمي، وجهود الجامعات المصرية للتحول الرقمي، ثم تعرف مفهوم الأمن السيبراني، وأهدافه وأهميته، وأهم المخاطر السيبرانية، وكيفية الحماية منها، وعرض لبعض التجارب الدولية لسياسات الأمن السيبراني كمناخ داعم لحماية البنية التحتية الرقمية للجامعات، ما يسهم في دعم أداء الجامعة وبالتالي تحسين تصنيفها عالميا، وتأكيد الدور التكاملي للجامعات مع باقي قطاعات الدولة من اقتصاد وصناعة وتسهيل عملية التنسيق والتواصل بينهم من خلال بنية تكنولوجيا رقمية آمنة.

وفي ذات السياق هدفت دراسة (فرج، ٢٠٢٢) إلى بيان دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبد العزيز، وتحديد الفروق في وجهات نظر أفراد العينة نحو دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي للجامعة تبعاً لمتغيرات: (الكلية، التخصص، سنوات الخبرة)، وتحقيقاً لذلك استخدامت الدراسة المنهج الوصفي، وصممت استبانة تكونت من (٢٦) فقرة توزعت إلى ثلاثة مجالات، وطُبقت على عينة من أعضاء هيئة التدريس بالجامعة بلغت (١٢٥) عضواً، وخلصت الدراسة إلى أن دواعي تعزيز ثقافة الأمن السيبراني في ظل

التحول الرقمي بجامعة الأمير سطام بن عبد العزيز من وجهة نظر أعضاء هيئة التدريس حصل على متوسط عام (٣,٥٥ من ٥) أي بدرجة متوسطة، وبالنسبة للمحاور؛ حصل محور الدواعي المجتمعية لتعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي للجامعة على أعلى متوسط (٣,٧٠)، يليه محور الدواعي المعرفية لتعزيز ثقافة الأمن السيبراني بالجامعة وحصل على متوسط عام (٣,٥١)، وأخيراً محور الدواعي التقنية وحصل على متوسط (٣,٤٦)، كما بينت النتائج عدم وجود فروق ذات دلالة إحصائية تبعاً لمتغير الكلية، والرتبة العلمية، فيما وجدت فروق تعزى لمتغير سنوات الخبرة، وتوصى الدراسة بأهمية إذكاء الوعى بالأمن السيبراني لدى الطلبة، وإدراك منافع البرمجيات المتاحة لمكافحة المخاطر السيبرانية، وتصميم حملات للتوعية بالمخاطر السيبرانية.

منهجية البحث :

إن منهجية الدراسة وإجراءاتها من أهم محاور البحث حيث يتم خلالها اتمام الجانب العملي من البحث وخلاله نجمع البيانات التي توصلنا إلى النتائج التي يتم تفسيرها فيما بعد في ظل أدبيات البحث وتحقيق اهداف البحث والتحقق من هدفه، وفي هذا البحث تم استخدام المنهج الوصفي التحليلي الذي برز من خلال وصف متغيرات الدراسة، وأيضاً في تفسير البيانات من أجل الوصول إلى نتائج ذات معنى.

نتائج البحث :

بعد التطرق للعديد من الدراسات السابقة مثل دراسة (المنيع، ٢٠٢٢)، وغيرها نعرض بعض المتطلبات اللازمة لتطبيق الأمن السيبراني خاصة في المؤسسات التربوية:

١. تحديد إجراءات العمل في نطاق شبكة المعلومات بوضوح بما هو مسموح وما هو غير مصرح به
٢. وضع خطة لآليات تنفيذ العمل ووضع عقوبات في حال كان هناك تجاوز للحدود.
٣. ضرورة وجود الكوادر البشرية المدربة للتعامل مع التقنيات التكنولوجية بكفاءة عالية.
٤. تحديث بيانات الخصوصية المتاحة عبر الشبكات بشكل دوري ومستمر منعاً للاختراق.
٥. المراقبة الحثيثة والدورية والمستمرة لكافة أنشطة المعلومات للكشف عن أي اختراق.

٦. ضرورة اختيار المكان بدقة الانسب للشبكات فلا بد من وجود نقاط اتصال في بيئة آمنة وبعيدة عن اعين الاختراق.
٧. ضرورة تشغيل بروتوكولات التحقق والتشفير والتي حققت تطورا كبيرا اليوم.

ويشير (الجنفاوي، ٢٠٢١) إلى ضرورة توفر عناصر ضرورية لتطبيق الأمن السيبراني ومنها:

١. العناصر المادية المتمثلة بالأجهزة والقطع الإلكترونية والأدوات التي تمثل البنى التحتية.
٢. العناصر البرمجية المتمثلة بالنظم الغير مادية المطلوبة لتشغيل المعلومات.
٣. القوى البشرية الكفر والأفراد المهرة المدربين.
٤. دعم الإدارات العليا لعمليات تطبيق الأمن السيبراني وعدم تعجل النتائج.
٥. إعادة هيكلية الهيكل التنظيم بالصورة التي تخدم متطلبات تكنولوجيا المعلومات.

وفي ذات السياق نشير الى ضرورة أن يهتم الأمن السيبراني بالمحافظة على المعلومات والاجهزة والشبكات بحيث تحمي كل من يتعامل مع الشبكات واجهزة الاتصال، ولتطبيقه في المؤسسات مزايا عدة أهمها:

١. المحافظة على الجدوى الاقتصادية والمالية.
٢. العمل عبر الشاشات بعيداً عن المخاطر والتهديدات.
٣. التعرف على مقدار الانحراف في الأداء من خلال برامج المراقبة المستمرة.

وهناك عدة اجراءات يمكن لمستخدمي الانترنت ولمن يتعامل مع الأجهزة الإلكترونية التعامل معها تعزز من الأمن السيبراني ومنها:

١. الحرص على تحديث بيانات الحماية التي تمثل البنية التحتية للمعلومات.
٢. التأكد بشكل دوري من إعدادات الحاسوب والإنترنت.
٣. التعامل مع كلمات مرور قوية و اتباع عمليات تحقق آمنة لمواقع التواصل والحماية الشخصية للأجهزة الخاصة.
٤. عدم الإفصاح عن أي معلومات شخصية عبر مواقع التواصل سواء لأشخاص مجهولين او معروفين (النمنتشري، ٢٠٢٠).

كما واتجهت الولايات المتحدة الأمريكية في عهد الرئيس باراك اوباما إلى جملة من الاجراءات التي بموجبها يتحقق الأمن السيبراني، ومنها إطلاق المبادرة الوطنية للأمن السيبراني لضمان وجود بنية تحتية للاتصالات على درجة من الموثوقية والتي يمكن الاستفادة منها من خلال:

١. إدارة شبكة المؤسسة الفيدرالية كمؤسسة شبكة الانترنت.
٢. نشر نظام كشف التجسس لأجهزة الاستشعار.
٣. ربط مراكز الأمن السيبراني معاً لتعزيز الوعي الأمني.
٤. تطوير خطط لمواجهة الهجمات السيبرانية على مستوى الحكومات.
٥. توسيع نطاق التعليم السيبراني.
٦. تطوير استراتيجيات وبرامج مواجهة مخاطر الامن السيبراني.

يتضح لنا بناءً على ما سبق إنه بالإمكان تعزيز الأمن السيبراني في المدارس للمعلمين من خلال اتباع عدة سبل تشير الباحثة الى بعض منها:

١. التخطيط الجيد من قبل إدارة المدرسة لتمكين المعلمين من كفايات الأمن السيبراني بجميع التخصصات.
٢. الإشراف على الخطط المتبعة في تنفيذ سياسات الأمن السيبراني المتفق عليها داخل المدرسة أو بين المدارس.
٣. وجود العديد من الاقتراحات والحلول الطارئة عند التعرض لأي من الانتهاكات او الجرائم الالكترونية.
٤. عقد دورات تدريبية وورش عمل لجميع المعلمين حول موضوعات الأمن السيبراني.
٥. نشر الوعي الدائم بأهمية وفاعلية الأمن السيبراني بين المعلمين والطلبة.
٦. إشراك الآباء في تنفيذ سياسات الأمن السيبراني الخاصة بالمؤسسة التعليمية.
٧. التركيز على موضوع الأمن السيبراني ضمن أدلة المعلمين.
٨. طرح قضايا الأمن السيبراني ضمن قضايا الحصص المدرسية وموضوعات المنهاج.

ونستنتج أن معظم التربويين (والمرأة كذلك) في الحقل التعليمي يستخدمون نوعاً من الوسائط التعليمية المفتوحة مثل عرض مقاطع فيديو، أو استخدام شبكات التواصل الاجتماعي والعديد من الوسائط، هذا كله بفعل زيادة التعليم عبر الانترنت بسبب التطور التقني الكبير وبفعل جائحة كورونا التي

غزت العالم وجعلته امام مفترق طرق وكان التعليم الالكتروني المخرج الوحيد الذي يمكن للعملية التعليمية متابعة مسيرها خلالها، بسبب تفشي فايروس كورونا في جميع انحاء العالم والزيادة المتسارعة في أعداد المصابين والاجراءات التي لجأت اليها معظم دول العالم للاحتراز منه والتباعد الاجتماعي الذي بات مفروض وإغلاق العديد من الشركات والمؤسسات خاصة للتعليمية، باتت بيئات التعلم الالكتروني هي البيئة البديلة عن البيئة الصفية للتكيف مع الوضع الراهن واستمرار العملية التعليمية من خلال توظيف التقنيات التكنولوجية المستحدثة.

توصيات البحث :

١. ضرورة توجيه المعلمين في تخطيط وتصميم المواقف التعليمية وتقويمها بالصورة التي تحقق الكفايات المحددة.
٢. رفع كفاءة عمليتي التعليم والتعلم وتحويل بيئة التعلم إلى بيئة فاعلة.
٣. توفير فرص للتعلم الذاتي.
٤. مراعاة الفروق الفردية من خلال التنوع الكبير في أساليب التعلم المستخدمة.
٥. تضمين تعليمه بالأنشطة التي ترفع من مستوى وعي المتعلمين بالأمن السيبراني.
٦. الالتحاق بدورات متخصصة حول مهارات الأمن السيبراني وتنظيم مثلها للمتعلمين.
٧. التنظيم بشكل مستمر بين الجهات المشرفة على الأمن السيبراني.
٨. التخطيط التدريسي لابراز مصطلحات الأمن السيبراني في المقررات المختلفة بصورة تكاملية.
٩. توظيف التكنولوجيا في التدريس وتعريف المتعلمين بآليات الحماية من مخاطرها.

المراجع :

الأسطل، محمود. (٢٠٢٠). تطوير نموذج مقترح قائم على الذكاء الاصطناعي وفاعليته في تنمية مهارات البرمجة لدى طلاب الكلية الجامعية للعلوم والتكنولوجيا. رسالة ماجستير غير منشورة، فلسطين .

المصري، نضال وألاعا، محمد. (٢٠٢١). أثر الذكاء الاصطناعي في مجال تكنولوجيا الاتصال على المناعة التنظيمية في ضوء خصائص الاعلام الرقمي كمتغير وسيط بالجامعات الفلسطينية.

ميرة، أمل و كاطع، تحرير. (٢٠١٩). تطبيقات الذكاء الاصطناعي في التعليم من وجهه نظر تدريسي الجامعةPsychological Science, (22)

محمود، عبد الرازق. (٢٠٢٠). الذكاء الاصطناعي لمدخل نظام التعليم في ظل تحديات جائحة فيروس كورونا ١٩. المجلة الدولية للبحوث في العلوم التربوية (IJRES) 3، (4)

شاكر، صالح. (٢٠٢٠). تأثير استخدام أنظمة التعلم الذكية المستندة الى المعايير القياسية على إتقان مهارات البرمجة وحل المشكلات لدى طلاب شعبة معلم الحاسب بكلية التربية النوعية جامعة المنصورة. المجلة العلمية المحكمة للجمعية المصرية للكمبيوتر التعليمي، ٨(١)، ٤٦٩-٥١٩.

الفائز، عبد العزيز. (٢٠٢١). درجة تضمين مفاهيم وتطبيقات الذكاء في محتوى مناهج الحاسب وتقنية المعلومات بالتعليم العام في المملكة العربية السعودية. المجلة الدولية للبحوث في العلوم التربوية. IJRES) ،4 (4) ،171-214 .

ابراهيم، منال. (٢٠٢٢). مدى تضمين تطبيقات الذكاء الاصطناعي وأخلاقياته بمقررات الفيزياء للمرحلة الثانوية. مجلة العلوم التربوية، ٢(٢٩) .

عبد اللطيف، إبراهيم . (٢٠٢٠). آليات تحقيق التعلم الرقمي باستخدام تطبيقات الذكاء الإصطناعي للطلاب ذوي الإعاقة البصرية المجلة العربية لعلوم الإعاقة والموهبة. مج. ٤، ع. ١٤، نوفمبر ٢٠٢٠.

الغامدي، عهود والمسنادي، ولاء. (٢٠٢١). دور الأمن السيبراني في تحقيق الميزة التنافسية، دراسة ميدانية على موظفي مطار الملك عبد العزيز الدولي بجدة، مجلة العلوم الإقتصادية و الإدارية و القانونية، ٥(٩)، ١٦٤-١٤٤.

الشهري، علي. (٢٠١٩). رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية Doctoral dissertation ، .
جامعة نايف العربية للعلوم الأمنية).

الشمري، مصطفي. (٢٠٢١). الأمن السيبراني وأثره في الأمن الوطني العراقي، مجلة العلوم القانونية والسياسية، المجلد العاشر، العدد الاول .

الاتحاد الدولي للاتصالات. (٢٠١١). الاتجاهات في مجال الاتصالات تمكين عالم الغد الرقمي .

البيشي، منيرة. (٢٠٢١). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة. مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، ٢٩(٦) .

المنيع، الجوهرة. (٢٠٢٢). متطلباتُ تحقيقِ الأَمْن السيبرانيّ في الجَامِعَات السعوديَّة في ضوء رؤية ٢٠٣٠. مجلة كلية التربية (أسيوط)، ٣٨(١)، ١٥٥-١٩٤.

الجنفاوي، خالد. (٢٠٢١). التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت. المجلة العربية للآداب والدراسات الإنسانية، ٥(١٩)، ٧٥-١٢٤.

المنتشري، فاطمة. (٢٠٢٠). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للعلوم التربوية والنفسية، ٤(١٧)، ٤٥٧-٤٨٤.

المنتشري، فاطمة. (٢٠٢٠). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. المجلة العربية للتربية النوعية، ٤(١٤)، ٩٥-١٤٠.

التميمي، دعاء. (٢٠١٩). جريمة الابتزاز الالكتروني: دراسة مقارنة Doctoral dissertation, AL-Quds University.

الصبان، عبير. (٢٠٢٠). التنمر الإلكتروني لدى الطلبة المراهقين في بعض مدارس المرحلة المتوسطة والثانوية في مدينة جدة. Journal of Faculty of Education Assiut University-المجلة العلمية بكلية التربية-جامعة أسيوط، ٣٦(٩)، ٣١٧-٣٥٥.

ربايعة، عبد اللطيف. (٢٠١٦). " الجرائم الالكترونية"(التجريم والملاحقة والإثبات، بحث مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، جامعة النجاح الوطنية.

الصحفي، أحمد (٢٠١٩). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمى فى التربية، ٢٠(الجزء العاشر)، ٤٩٣-٥٣٤.

عوفي ، حبيب. (٢٠٢٢). الفضاء الرقمي ، تحدي أمني جديد واستراتيجيات الدول في تحقيق الأمن السيبراني العالمي. المجلة الجزائرية للعلوم الإنسانية والاجتماعية ، ٦ (١) ، ١٠٢-١٢٣.

بوقرص، ساعد. (٢٠٢٢). الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات واستراتيجيات خاصة.Journal of social protection research, 3(1), 61-76.

شرف، نجم. (٢٠٢٠). الأمن السيبراني وإشكالاته الفقهيّة: دراسة مقارنة بين قانوني الأمن السيبراني القطري والنيجيري (أطروحة دكتوراه ، جامعة حمد بن خليفة (قطر)).

البغدادي، مروة. (٢٠٢١). اقتصاديات الأمن السيبراني في القطاع المصرفي. مجلة البحوث القانونية والإقتصادية (المنصورة)، ١٢(١)، ١٤٤٦-١٥١٦.

الصانع، نورة. (٢٠٢٠). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. مجلة كلية التربية (أسيوط)، ٣٦(٦)، ٤١-٩٠.

السواط، حمد وآخرين. (٢٠٢٠). العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف. مجلة البحث العلمى فى التربية، ٢١(العدد الرابع)، ٢٧٨-٣٠٦.

كاعوه، عبير. (٢٠٢٠). سياسات الأمن السيبراني لتعزيز التحول الرقمي في الجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية. مجلة دراسات تربوية واجتماعية، ٢٥ (يونيو)، ٣٥٣-٤١٩.

العجلان، حياة. (٢٠٢١). درجة تحقيق معلمي الحاسب الآلي لمعايير تكنولوجيا التعليم الدولية ISTE للمعلمين. المجلة السعودية للعلوم التربوية، ١(٨)، ١-٢١.

اليامي، هادية. (٢٠١٨). رؤية مستقبلية لتطوير التعليم في المملكة العربية السعودية في ضوء رؤية المملكة ٢٠٣٠. مجلة العلوم التربوية و النفسية، ٢(٢٦)، ٤٩-٣٢.

الفهمي، مرزوق. (٢٠٢٠). ضبط وضمان الجودة في المؤسسات التعليمية (المعايير والنماذج والأساليب) في ضوء رؤية المملكة العربية السعودية ٢٠٣٠. مجلة العلوم التربوية و النفسية، ٤(١٥)، ١٠٤-٧٩.

الوهابي واخرون. (٢٠٢٠). تطوير إعداد المعلم في المملكة العربية السعودية في ضوء خبرات الولايات المتحدة الامريكية وسنغافورة وماليزيا. مجلة كلية التربية فى العلوم التربوية، ٤٤(٤)، ٢٦٧-٣١٨.

عبد الله، سعدية. (٢٠١٧). الكفايات اللازمة للمعلم لأداء دوره فى التعليم العام فى ضوء معايير جودة التعليم (Doctoral dissertation. جامعة السودان للعلوم والتكنولوجيا) ،

منصور، مصطفى. (٢٠٢٠). درجة توافر الكفايات المهنية لدى أعضاء هيئة التدريس بجامعة غزة من وجهة نظر طلبتهم، مجلة كلية فلسطين التقنية للأبحاث والدراسات، ٧(١)

العالم، تسنيم. (٢٠٢٢). فاعلية بيئة تدريب تكيفية قائمة على التطبيقات السحابية في تحسين الكفايات التكنولوجية والوعي المعلوماتي الرقمي لدى الطالبات المعلمات في الجامعة الاسلامية بغزة. رسالة ماجستير غير منشورة. الجامعة الاسلامية .

الجبوري، حسن. (٢٠١٢). منهجية البحث العلمي مدخل لبناء المهارات البحثية، ط١، دار صفاء للنشر والتوزيع، عمان الأردن .

زكي، الشيماء. (٢٠٢٢). الكفايات التكنولوجية لدى معلمي التربية الرياضية بإدارة الإبراهيمية التعليمية بمحافظة الشرقية. المجلة العلمية للتربية البدنية وعلوم الرياضة، ٢٩(١)، ٤١-٧٤.

هلال، رضا وآخرون. (٢٠٢٠). (٢٠٢٠). الكفايات التكنولوجية لمعلمى التربية الرياضية بالمرحلة الإبتدائية بمركز ومدينة طنطا بمحافظة الغربية. المجلة العلمية للتربية البدنية وعلوم الرياضة، ٢٤(١٠)، ١-١٨.

Doctoralالعتيبي، عبد الرحمن.(٢٠٢٠). دور الأمن السيبراني في تحقيق رؤية ٢٠٣٠ (dissertation ، جامعة نايف العربية للعلوم الأمنية).

محمد، آمنة. (٢٠٢١). الأمن السيبراني في ضوء مقاصد الشريعة. مجلة كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، ٣٧(١)، ٤٤٩-٥٠٥.

العقلاء، رؤى و نور الدين، علي. (٢٠٢٢). درجة الوعي بمفاهيم الأمن السيبراني لدى معلمي ومعلمات الحاسب الآلي بمدينة حائل. دراسات عربية في التربية وعلم النفس، ١٤٤(٢)، ٢٧٧-٣٠٠.

سراج، شيماء. (٢٠٢٢). التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي. المجلة العربية للعلوم التربوية والنفسية، ٦(٢٦)، ١٩٩-٢١٢.

المومني، تمارا. (٢٠٢٢). اتجاهات الطلبة في الجامعات الأردنية نحو دراسة تخصص الأمن السيبراني. مجلة منار الشرق للتربية و تكنولوجيا التعليم، ١(١)، ٦٨-٥٥.

الخضرى، جيهان (٢٠٢٠). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية. مجلة تطوير الأداء الجامعى، ١٢(١)، ٢١٧-٢٣٣.

) في شبكات الشبكات MQQ-ENCمعلا، بشرى واسكندر، خديجة. (٢٠٢٠). تقييم خوارزمية التشفير (اللاسلكية الداعمة للوسائط المتعددة. مجلة جامعة تشرين- سلسلة العلوم الهندسية ،، ٤٣ (٤).

Doctoralالحاج، نادية (٢٠١٧). تحسين خوارزمية تشفير البيانات القياسية بزيادة طول المفتاح (، جامعة الجزيرة).dissertation

فرج، عمر. (٢٠٢٢). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي-جامعة الأمير سطام بن عبد العزيز نموذجاً. المجلة التربوية لكلية التربية بسوهاج، ٩٤(٩٤)، ٥٠٩-٥٣٧.

أبو حجاب سارة. (٢٠٢٢). إجراءات مقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر في ضوء بعض الممارسات الدولية. الإدارة التربوية، ٣٣(٣٣)، ٣٣٣-٥٢٦.

الدمرداش، نانسي. (٢٠٢٢). أثر تفاعل العناصر الافتراضية المدعومة بالذكاء الاصطناعي وأدوات إدارة المعرفة في تنمية مهارات الأمن السيبراني وحل المشكلات لدى طلاب الحاسبات والذكاء الاصطناعي. مجلة البحوث في مجالات التربية النوعية، ٨(٤١)، ١٣٣١-١٤٢٧.

الطيار، حسن (٢٠٢٠). الأمن السيبراني في منظور مقاصد الشارع، دراسة تأصيلية، مجلة جامعة الطائف للعلوم الانسانية، المجلد(٦) ع(٢١) .

لطفى، وفاء. (٢٠٢٢). الجهود الدولية في مجال مكافحة جرائم الارهاب السيبراني: التجربة الماليزية نموذجا. مجلة كلية الاقتصاد والعلوم السياسية، ٢٣(١)، ١٥١-١٧٨.

عبد الوهاب، أحمد. (٢٠٢٠). اشكالية الامن السيبراني العراقي بين التهديدات السيبرانية والتقنين المقيد للحريات.political issues, (60.)

ربايعة،، عبد اللطيف. (٢٠١٦). " الجرائم الالكترونية"(التجريم والملاحقة والإثبات). مقدم إلى المؤتمر الأول للجرائم الالكترونية في فلسطين، جامعة النجاح الوطنية .

العنزي، تهاني، (٢٠٢٢). كفايات الأمن السيبراني لدى معلمي الحاسب الآلي في المرحلة الثانوية بمدينة الرياض. رسالة ماجستير غير منشورة، جامعة الملك سعود.

المراجع الأجنبية :

Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., & Chen, H. (2021). Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. Journal of Cleaner Production, 289, 125834.

Traxler, J., Scott, H., Smith, M., & Hayes, S. (2020). Learning through the crisis: Helping decision-makers around the world use digital technology to combat the educational challenges produced by the current COVID-19 pandemic.

Paszkiewicz, A., Salach, M., Dymora, P., Bolanowski, M., Budzik, G., & Kubiak, P. (2021). Methodology of implementing virtual reality in education for industry 4.0. Sustainability, 13(9), 5049.

Smakman, M. H., Konijn, E. A., Vogt, P., & Pankowska, P. (2021). Attitudes towards social robots in education: enthusiast, practical, troubled, sceptic, and mindfully positive. Robotics, 10(1), 24.

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248.

Yang, S. C. (2019). A curriculum model for cybersecurity m(aster's program: A survey of AACSB-accredited business schools in the United States. Journal of Education for Business, 94(8), 520-530.

BOUKERS, S. (2021). Introduction à la micro-informatique (éd. 1ère édition). Baraki, Alger, Algérie: Mitidja Impression.

Maghfiroh, J. (2022). Pengamanan pesan menggunakan algoritma One Time Pad (OTP) dengan Linear Congruential Generator (LCG) sebagai pembangkit kunci (Doctoral dissertation, Universitas Islam Negeri Maulana Malik Ibrahim.(

Chinese Academy of Cyberspace Studies. (2019). Improving Capacity of Cyber Security Safeguarding. China Internet Development Report 2017: Translated by Peng Ping, 101-130.

GOIDI AMERICAN JOURNAL

Journal
Goidi American Journal
of Innovation Development and Investment
GOIDI INTERNATIONAL GROUP OF INSTITUTION

About Journal

Google scholar

https://scholar.google.com/citations?hl=ar&authuser=4&user=5w_h_4wAAAAJ

Journal Link https://portal.issn.org/resource/ISSN/2694-5606

https://portal.issn.org/resource/ISSN/2694-5460

GOIDI American Journal, Vol 2 Fourth Issue 11 July 2023