البحث الثالث عشر

متطلبات تطبيق الذكاء الاصطناعي من وجهة نظر المعلمين بمنطقة المدينة المنورة التعليمية وفقا لمعايير الأمن السيبراني

إعداد

د./ طلال حمد فرز الاحمدي
استاذ مشارك بقسم تقنيات التعليم
كلية التربية جامعة طيبة

د./ خالد مريع القحطاني
استاذ مساعد بقسم تقنيات التعليم
كلية التربية جامعة طيبة

مستخلص الدراسة:

هدفت الدراسة الحالية إلى التعرف على متطلبات تطبيق الذكاء الاصطناعي من وجهة نظر المعلمين بمنطقة المدينة المنورة التعليمية وفقا لمعايير الأمن السيبراني، واستخدم الباحثان المنهج الوصفي التحليلي معتمداً على الاستبانة التي قام بتصميمها لتحقيق أهداف الدراسة، واشتملت عينة الدراسة على (120) معلم ومعلمة من معلمي اللغة العربية والتربية الإسلامية بمدارس التعليم العام بمنطقة المدينة المنورة، وقد توصلت الدراسة للعديد من النتائج أهمها: أن درجة متطلبات تطبيق الذكاء الاصطناعي من وجهة نظر المعلمين بمنطقة المدينة المنورة التعليمية وفقا لمعايير الأمن السيبراني جاءت بدرجة (عالية) من وجهة نظر أفراد عينة الدراسة، وجاء في الترتيب الأول المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (4.10)، وانحراف معياري بلغ (.719)، يليه في الترتيب الثاني المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (3.48)، وانحراف معياري بلغ (.711)، بينما جاء في الترتيب الأخير المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (3.01)، وانحراف معياري بلغ (.960)، وقد أظهرت النتائج عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول محاور الاستبانة والدرجة الكلية لتوظيف تطبيقات الذكاء الاصطناعي وفق معايير الأمن السيبراني طبقاً إلى اختلاف متغيرات (النوع – عدد سنوات الخبرة – المؤهل العلمي)؛ وأوصى الباحثان بالعديد من التوصيات في ضوء ما توصل إليه من نتائج أهمها: ضرورة تعزيز وحماية البنية التحتية لمدارس التعليم العام؛ بحيث تساعد على تطبيق الذكاء الاصطناعي بالتدريس وفقاً لمعايير الأمن السيبراني، وضرورة شراء البرمجيات والحواسيب وفق أنظمة تحددها إدارة المدرسة لتطبيق الذكاء الاصطناعي في التعليم.

الكلمات المفتاحية: متطلبات – الذكاء الاصطناعي– الأمن السيبراني.

Abstract

The current study aimed to identify the requirements for the application of artificial intelligence from the point of view of teachers in Al-Madinah Al-Munawwarah educational district in accordance with the standards of cybersecurity. Arabic and Islamic education in general education schools in Al-Madinah Al-Munawwarah region. The study reached many results, the most important of which are: The degree of requirements for the application of artificial intelligence from the point of view of teachers in Al-Madinah Al-Munawwarah educational district in accordance with cybersecurity standards came with a (high) degree from the point of view of the study sample. The first rank, the first axis: the (organizational) requirements for employing artificial intelligence applications in teaching according to cybersecurity standards, with an arithmetic mean of (4.10) and a standard deviation of (.719), followed by the second rank, the third axis: (physical) requirements for employing artificial intelligence applications in teaching. Teaching according to cybersecurity standards, with an arithmetic average of (3.48), and a standard deviation of (.711), while the second axis came in the last order: (human) requirements for employing artificial intelligence applications in teaching according to cybersecurity standards, with an arithmetic mean of (3.01), and a deviation of (3.01). Normative reached (.960), and the results showed that there were no statistically significant differences at the level of significance (0.05) in the opinions of the members of the research sample about the questionnaire axes and the total degree of employing artificial intelligence applications according to cyber security standards according to the different variables (type - number of years of experience - Qualification); The two researchers recommended several recommendations in the light of its findings, the most important of which are: the need to strengthen and protect the infrastructure of general education schools; So that it helps to apply artificial intelligence in teaching in accordance with cybersecurity standards, and the need to purchase software and computers according to systems determined by the school administration to apply artificial intelligence in education.

Keywords: Requirements - Artificial Intelligence - Cybersecurity.

مقدمة:

نظرا للتطور الهائل في مجالات البرمجيات والإلكترونيات وتكنولوجيا المعلومات، وما أحدثوه من تطور في كافة المجالات الحياتية، بدءًا من علوم الفضاء ومروراً بمجالات التصنيع ومراقبة الجودة، ووصولا إلى الهواتف المحمولة، فقد ظهر ذلك التطور في مجال الذكاء الصناعي، والذي أحدث بدوره طفرة حقيقية في مجالات عديدة من أهمها: المجالات التعليمية، والرعاية الصحية، والقيادة الذاتية للمركبات، ووسائل التواصل الاجتماعي، والصناعة، وغير ذلك من المجالات الأخرى، الأمر الذي دفع كثير من التخصصات المختلفة إلى محاولة الاستفادة من تقنياته لإثراء عملهم، ولمواكبة التطور والتقدم الحاليين. (حسانين، 2020، ص. 629)

وبالنظر إلى أن المنظومة التعليمية في عصرنا فإنها تحتاج إلى منتجات تعليمية متميزة تعتمد على فكر معرفي متطور، فقد سعت دول العالم إلى تطوير النظم التعليمية من حيث الأهداف والطرق والأدوات، ووسائل التقويم، وكذلك إعداد المعلمين، كما سعت بهذا التطوير إلى مواكبة التغيرات العلمية والتكنولوجية والمعرفية السائدة في الوقت الراهن، وذلك لتهيئة الكوادر البشرية اللازمة للقيام بعملية التنمية، وقد اعتمدت في ذلك على الذكاء الصناعي، وقد أحدثت تقنيات الذكاء الصناعي تغييرات في احتياجات المتعلمين، والخدمات المعلوماتية التي يجب أن تقدم لهم، الأمر الذي دعا بالضرورة إلى تكيف المؤسسات التعليمية مع تلك التكنولوجيا وتعزيز خدماتها لتصبح أكثر مرونة واستجابة، وقد استطاعت المؤسسات التعليمية في الدول المتقدمة إدخال تلك التقنيات وتوظيفها بشكل مبكر نظرا لجاهزيتها العالية، وتوافر كافة المتطلبات والتجهيزات اللازمة لإدخال تلك التقنيات الذكية المتطورة، كما تعمل المؤسسات التعليمية بالمملكة العربية السعودية توظيف تكنولوجيا الذكاء الصناعي فيها، واستثمارها ومواجهة التحديات التي تواجهها. (فرج، 2022، ص. 457)

وقد بدأت المؤسسات في استخدام الذكاء الاصطناعي في الأمن السيبراني لتوفير أمن معلوماتي أفضل ضد المهاجمين ذوي المهارات المتزايدة، حيث يساعد الذكاء الاصطناعي في أتمتة العمليات المعقدة لتحديد الهجمات والرد على انتهاكات نظم المعلومات، وتتطور هذه الأنواع من التطبيقات وتصبح أكثر تقدمًا وشمولية من خلال الاستفادة من الذكاء الاصطناعي (Vähäkainu & Lehto, 2019).

وفي السنوات الأخيرة، كانت هناك محاولات لتصميم حلول قائمة على الذكاء الاصطناعي لمجموعة واسعة من تطبيقات الأمن السيبراني في المدارس والمؤسسات التعليمية، ويرجع ذلك جزئيًا إلى فهم المؤسسات التعليمية المتزايد لأهمية الذكاء الاصطناعي في الحد من التهديدات السيبرانية (Zhang et al., 2022).

ونظرا للأهمية الكبرى التي توليها المملكة للأمن السيبراني الوطني، وإدراكها بأنه هدف ومقوم أساسي لحماية المصالح الحيوية، للوصول إلى فضاء سعودي آمن وموثوق، فقد تم تضمين ثقافة الأمن السيبراني في المؤسسات التعليمية والثقافية، كما تم تأسيس مراكز ومؤسسات معنية بالأمن السيبراني. (فرج، 2022، ص. 515)

ويعد رفع الوعي بالأمن السيبراني عند المعلمين وتبني أسس ومبادئ متنوعة لتنمية مهاراتهم المهنية والمستقبلية أمرا ملحا، نظرا للحاجة لرفع الكفاءات وتنمية القدرات بما يتوافق مع المتغيرات التكنولوجية القائمة والمتسارعة، على أن يتم ذلك في ضوء حاجات المعلمين وخبراتهم لتقليل المخاطر السيبرانية المتوقعة في المؤسسات التعليمية. (السعادات والتميمي، 2022، ص. 257)

ولهذا السبب، يجب أن يأخذ منهج الذكاء الاصطناعي في المدارس في الاعتبار الكفايات الخاصة بطلاب المدارس، فالهدف من التعليم في المدارس هو تزويد الطلاب بفرصة لتقوية الكفايات الأساسية للعمل كعضو في المجتمع بنجاح، ويجب أن تتوجه كفاية المدرسة نحو تعزيز قدرة الطلاب على فهم العالم المتكامل للذكاء الاصطناعي (Kim et al., 2021).

ومن هنا تبرز أهمية توفير مختلف المتطلبات المادية والإدارية والبشرية الضرورية لتطبيق الذكاء الاصطناعي في المدارس. ومن المهم أن يكون ذلك في ظل مراعاة جوانب الأمن السيبراني. فكلما ازداد تعقيد التقنيات التكنولوجية، كلما ازدادت درجة المخاطر المحيطة بها. لذلك فإن تطبيق الذكاء الاصطناعي ومتطلبات الأمن السيبراني في العملية التعليمية ينبغي أن يتم على نحو لا انفصام فيه.

مشكلة الدراسة:

يشهد العالم المعاصر تطوراً متزايدًا لتقنيات الذكاء الاصطناعي في شتى المجالات. ولعل ذلك يرجع إلى الإدراك المتزايد للدور الذي يمكن أن تلعبه الأتمتة في تحسين نتائج العمليات والأنشطة. ومع ذلك، فإن هناك تحديات تكتنف توفير المتطلبات الضرورية لدمج تقنيات الذكاء الاصطناعي في المجالات التعليمية. وقد تناولت الدراسات الحديثة بعضًا من تلك التحديات. فعلى سبيل المثال، دراسة أكجون وغرينهاو (Akgun & Greenhow, 2022) إلى وجود مخاوف أخلاقية واجتماعية محيطة بتوظيف تقنيات الذكاء الاصطناعي في العملية التعليمية.

وتتفق هذه النتائج مع نتائج دراسة تشانغ وأصلان (Zhang & Aslan, 2021)، والتي أشارت إلى وجود إشكاليات أخلاقية محيطة باستخدام الذكاء الاصطناعي في العملية التعليمية. أما دراسة تاهيرو (Tahiru, 2021) فقد سلطت الضوء على عدة تحديات أخرى متنوعة، والتي تتضمن تحديات متعلقة بالأمن السيبراني مثل عدم اكتمال أو دقة البيانات، واستخدام التقنيات غير المناسبة، ومسائل ملكية البيانات والأمن والثقة، ومشكلات الاستعداد التنظيمي. ومن مشكلات الأمن السيبراني الأخرى المحيطة بتطبيق الذكاء الاصطناعي .

ومما يؤسف له أن تطبيق الذكاء الاصطناعي ما يزال في مرحلة غير ناضجة في نظام التعليم العام بالمملكة العربية السعودية. فكما أشارت دراسة التويجري (2022)، فإن تطبيق الذكاء الاصطناعي يعاني من مشكلات مثل الرؤية والفلسفة التي توجه الذكاء الاصطناعي لدعم اتخاذ القرارات الإدارية في وزارة التعليم بالمملكة العربية السعودية، وضعف استقطاب الخبرات التقنية المؤهلة لعملية تطوير الذكاء الصناعي، وضعف البنية التحتية الرقمية.

في هذا الصدد من المهم تسليط الضوء على الدور الذي يمكن أن يلعبه تطبيق الذكاء الاصطناعي في المؤسسات التعليمية وفقا لمعايير الأمن السيبراني، حيث أصبحت جميع المؤسسات التعليمية وغيرها بحاجة إلى تطوير لتحقيق أهدافها ومخرجاتها على أكمل وجه، إلا أن هذا الذكاء لا يمكن تطبيقه أو الاستفادة منه دون رقابة، ومن هنا ينبغي العمل على تطبيق الأمن السيبراني أولا ونشره في جميع المجالات للحفاظ على المعلومات والبيانات المهمة في جميع المؤسسات وضمان حمايتها من أي اعتداء، ثم إدراج الذكاء الصناعي تحت هذا النمط من الحماية للوصول إلى الأهداف المنشودة من تطبيق الذكاء الصناعي داخل المؤسسات بوجه عام والمؤسسات التعليمية على وجه الخصوص.

وتنبثق من مشكلة الدراسة التساؤلات التالية :

1- ما المتطلبات (التنظيمية- البشرية - المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني؟
2- هل توجد فروق حول محاور الاستبانة والدرجة الكلية وفق متغير(النوع) ؟
3- هل توجد فروق حول محاور الاستبانة والدرجة الكلية وفقا لمتغير (عدد سنوات الخبرة) ؟
4- هل توجد فروق حول محاور الاستبانة والدرجة الكلية وفقا لمتغير (المؤهل الدراسي) ؟

أهداف الدراسة:

- التعرف على المتطلبات (التنظيمية– البشرية – المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني.
- التعرف على إمكانية وجود فروق حول محاور الاستبانة والدرجة الكلية وفق متغير (النوع) .
- التعرف على إمكانية وجود فروق حول محاور الاستبانة والدرجة الكلية وفقا لمتغير (عدد سنوات الخبرة) .
- التعرف على إمكانية وجود فروق حول محاور الاستبانة والدرجة الكلية وفقا لمتغير (المؤهل الدراسي).

أهمية الدراسة:

تنبع أهمية الدراسة الحالية من أهمية الموضوع الذي تتناوله وهو تطبيق الذكاء الاصطناعي في التدريس وفقاً لمعايير الامن السيبراني؛ ويمكن إبراز أهمية الدراسة فيما يلي:

أولاً: الأهمية النظرية:

- قد تساعد الدراسة الحالية في التأطير النظري لاهم المتطلبات اللازمة لتطبيق الذكاء الاصطناعي من وجهة نظر المعلمين وفقا لمعايير الأمن السيبراني.
- قد تساهم الدراسة الحالية في لفت انتباه المتخصصين لإقامة المزيد من الدورات التدريبية وورش العمل بهدف توعية المعلمين بمتطلبات تطبيق الذكاء الاصطناعي وفقا لمعايير الأمن السيبراني.
- يأمل الباحثان في إثراء المكتبات العربية بالمزيد من الدراسات والأبحاث حول متطلبات تطبيق الذكاء الاصطناعي من وجهة نظر المعلمين وفقا لمعايير الأمن السيبراني في ظل ندرة الدراسات في هذا السياق –على حد علم الباحث–.

ثانياً: الأهمية التطبيقية:

- قد تساعد نتائج الدراسة الحالية في تعميم الإجراءات التي تهدف إلى تطبيق الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني على كافة مدارس التعليم العام بالمملكة.
- قد تساهم نتائج الدراسة الحالية في طرح التوصيات المناسبة التي تزيد من فرص المدارس في تطبيق الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني.

مصطلحات الدراسة:

- **الذكاء الاصطناعي:**

ما زال الإنسان يعمل جاهدا لتطويع الكون في يديه وجعله تحت إمرته، لذا لا يكف عن التنقيب والاختراع والتجديد كل يوم، وقد كان الذكاء الاصطناعي أحد الاختراعات التي توصل إليها مؤخرا محاولا تطبيق هذا الذكاء على جميع مجالات الحياة بما فيها المجال التربوي والعلمي. وتتعدد تعريفات الذكاء الصناعي والتي ما هو موضح أدناه.

ويعرف الذكاء الاصطناعي بأنه نظام قائم على الآلات يمكنه، لمجموعة معينة من الأهداف التي يحددها الإنسان، وضع تنبؤات أو توصيات أو قرارات تؤثر على البيئات الحقيقية أو الافتراضية (Phillips et al., 2022).

كما يعرف الذكاء الاصطناعي بأنه ذلك النوع الذي يعمل بقدرة مشابهة لقدرة الإنسان، حيث يمكّن الآلة من التفكير والتخطيط بشكل ذاتي مشابها لتفكير البشر، بل إنه يفوق مستوى الذكاء البشري، حيث يؤدي المهام بشكل أفضل من الإنسان المتخصص وذو الخبرة، كما أنه يتميز بالقدرة على التعلم، والتواصل التلقائي، وإصدار الأحكام. (حسانين، 2020، ص. 631)

ويعرف كاسوا وآخرون (Kaswa et al., 2022) الذكاء الاصطناعي بأنه أتمتة الأنشطة المرتبطة بالتفكير البشري مثل اتخاذ القرارات، وحل المشكلات، والتعلم.

ويعرف الباحثان الذكاء الاصطناعي بأنه نوع من أنواع الذكاءات التي تعتمد على الآلة وتحاكي ذكاء الإنسان بل وتفوقه قدرة وتحكم، لمساعدة الإنسان في كافة مجالات الحياة.

- **الأمن السيبراني:**

أصبح الاعتماد على التكنولوجيا مؤخرا شيئا أساسيا في كل مناحي الحياة، إلا أن هذه التكنولوجيا تحاوطها العديد من الأخطار خاصة فيما يتعلق بالمعلومات والبيانات، لذا كان لا بد من وضع حد لتلك المخاطر ومن هنا بدأ سعي الإنسان الحثيث على البحث عن طرق لحماية تلك البيانات والحفاظ عليها من أي انتهاك أو تعدي، ومن هنا تكمن أهمية الأمن السيبراني والذي تتعدد تعريفاته ومنها ما هو موضح أدناه.

ويعرف الأمن السيبراني بأنه كافة الوسائل المتاحة المستخدمة لحماية البريد الإلكتروني والبيانات الرقمية الشخصية والمعلومات والأجهزة المحمولة وتعزيز خصوصيتها وتشفيرها واتخاذ الإجراءات اللازمة لحماية الطلاب من مخاطر الفضاء السيبراني. (فرج، 2022، ص. 521)

كما أن الأمن السيبراني هو مفهوم أمني خاص بحماية المعلومات، وكل ما له صلة بتلك المعلومات من عمليات وخدمات وأجهزة وتقنيات، ضد أي شكل من أشكال الوصول غير المسموح به، أو استخدام تلك المعلومات بشكل سلبي، أو بما يمثل خطرا على الجهات والأفراد ذوي الصلة بتلك المعلومات. (المنتشري، 2020، ص. 463)

ويشير الأمن السيبراني أيضًا إلى القدرة على حماية أو الدفاع عن استخدام الفضاء السيبراني من الهجمات السيبرانية، ويتعامل مع حماية الفضاء السيبراني واستخدامه ضد أي نوع من الجرائم (Hamburg & Grosch, 2017).

ويعرف جوتام (Goutam, 2015) الأمن السيبراني بأنه التقنيات والعمليات التي تم إنشاؤها لحماية أجهزة الحاسوب، ومعدات الحواسيب، والبرامج، والشبكات والبيانات من الوصول غير المصرح به، ونقاط الضعف التي يتم توفيرها عبر الإنترنت من قبل مجرمي الإنترنت والجماعات الإرهابية والمخترقين.

كما يعرف الباحثان الأمن السيبراني إجرائيا بأنه عبارة عن أنظمة حديثة للحفاظ على البيانات والمعلومات التي تتضمنها وتحتويها الأجهزة الإلكترونية الحديثة في كل المؤسسات والمنظمات من أي تعدي أو انتهاك.

الإطار النظري والدراسات السابقة

في عالم لا يسير على وتيرة واحدة، سمته التغير والتطور في كل وقت، لم يعد غريبا أن تكون هناك بعض الأجهزة والآلات التي تحاكي البشر في قدراتهم ومهاراتهم بل وأحيانا تقوم بتخطيها، ولا سيما في مجال التعليم، حيث تسعى جميع الدول مؤخرا إلى مواكبة التطورات الهائلة في هذا المجال، لإخراج جيل قادر على مواكبة تحديات العصر.

وقد تم الإجماع على الاستفادة من الذكاء الاصطناعي في التعليم في خمسة مجالات وهي: الذكاء الاصطناعي لإدارة التعليم وتقديمه، الذكاء الاصطناعي لتمكين التدريس والمعلمين، الذكاء الاصطناعي لتقييم التعلم والتعليم، تنمية القيم والمهارات اللازمة للحياة والعمل في عصر الذكاء الاصطناعي، والذكاء الاصطناعي لتقديم فرص التعلم مدى الحياة للجميع، وتستفيد أنظمة الذكاء الاصطناعي من تخصصات متعددة مثل: علوم التعلم والتعليم، علم النفس، علم الأعصاب، اللغويات، علم الاجتماع، والأنثروبولوجيا، لتعزيز تطوير بيئات التعلم التكيفية وغيرها من أدوات الذكاء الاصطناعي التي تتسم بالمرونة والشمول والشخصية والانخراط، بهدف تطوير برامج ذكية للحاسب الآلي يمكن بنفسها أن تتخذ قرارات في شتى المواضيع المختلفة. (درويش والليثي، 2020، ص. 63- 64)

ونظرا لما يشهده عالمنا من تطورات تقنية متسارعة أحدثت طفرة في شتى المجالات، وتحولات هائلة كان لها دور كبير على الأعمال والمهام وكفاءة العمليات وتنفيذها، ما أسهم في دفع الدول لمسايرة هذا التطور والتغيرات المصاحبة له، كان لا بد من اتخاذ أساليب جديدة في أنظمتها وبيئاتها وتعاملاتها، إلا أن هناك العديد من المشاكل والجرائم السيبرانية التي برزت تبعا للثورة التكنولوجية، وارتبطت في غالبها بالأفراد وممارساتهم خلال تعاملهم الرقمي، لذلك يعد رفع الوعي بالأمن السيبراني عند المعلمين وتبني أسس ومبادئ متنوعة لتنمية مهاراتهم المهنية والمستقبلية أمرا ملحا، نظرا للحاجة لرفع الكفاءات وتنمية القدرات بما يتوافق مع المتغيرات التكنولوجية القائمة والمتسارعة، خاصة في ضوء الذكاء الصناعي، على أن يتم ذلك في ضوء حاجات المعلمين وخبراتهم لتقليل المخاطر السيبرانية المتوقعة في المؤسسات التعليمية (السعادات والتميمي، 2022، ص.257-259)

لذلك فإنه من الأهمية بمكان أن تكون التطبيقات الإلكترونية الحديثة خاصة الذكاء الاصطناعي تحت رقابة الأمن السيبراني حفاظا على الأجهزة والمعلومات الشخصية من أي تعد أو انتهاك للخصوصية؛ وقد أصبحت المؤسسات الأكاديمية أهداف مغرية للهجمات السيبرانية وعانت بالفعل من عدة حوادث شديدة التأثير، فالمؤسسات الأكاديمية تدير كميات كبيرة من الأبحاث القيمة والبيانات الشخصية الحساسة، مما يجعلها هدفًا جذابًا لمجرمي الإنترنت والتجسس ونشطاء القرصنة (Ulven & Wangen, 2021, 1).

ومن هنا تبرز ضرورة توفير متطلبات الأمن السيبراني الضرورية والكافية من أجل تيسير تطبيق تقنيات الذكاء الاصطناعي في العملية التعليمية على نحو فعال؛ وبدون توافر تلك المتطلبات قد يؤدي استخدام تقنيات الذكاء الاصطناعي إلى نشوء العديد من المشكلات والتحديات بالنسبة لمستخدمي هذا التقنيات، سواء أكانوا من الطلاب أم المعلمين.

أهمية تطبيق الذكاء الصناعي في التعليم:

مع تطور تقنيات الحوسبة ومعالجة المعلومات، تم تطبيق الذكاء الاصطناعي (AI) على نطاق واسع في الممارسات التعليمية (الذكاء الاصطناعي في التعليم؛ AIEd)، مثل أنظمة التدريس الذكية، وروبوتات التدريس، ولوحات معلومات تحليلات التعلم، وأنظمة التعلم التكيفية، والتفاعلات بين البشر والحاسوب، وما إلى ذلك، ومنذ ظهور الذكاء الاصطناعي في التعليم منذ عدة ثلاثة عقود، كان الذكاء الاصطناعي يعتبر أداة قوية لتسهيل النماذج الجديدة للتصميم التعليمي، والتطوير التكنولوجي، والبحوث التعليمية التي من المستحيل تطويرها في وضع التعليم التقليدي (Ouyang & Jiao, 2021, 1).

وترجع أهمية تطبيق الذكاء الاصطناعي في مجال التعليم إلى أنه أدّى إلى إحراز تقدم كبير في النظرية والتطبيق في الألفية الجديدة، كما تم استخدام الذكاء الاصطناعي كحل لزيادة الكفاءة في التعلم عبر الإنترنت وإشراك الطلاب وتوصيلهم ببعضهم البعض وبمعلميهم في بيئات غير متزامنة عبر الإنترنت تخترق الحواجز الزمانية والمكانية للتعلم. (شعبان، 2021، ص. 12)

كما يجمع الخبراء على أهمية الذكاء الصناعي في التعليم في القرن الحادي والعشرين لما له من مميزات عديدة منها، القدرة على التعلم (Machine Learning)، والقدرة على تنظيم العلوم وفهمها (Knowledge Representation)، والقدرة على تحليل اللغة (NLP)، والقدرة على فهم الصوت (Speech Recognition)، وفهم وتحليل الصور والفيديو (Computer Vision)، وحل المشاكل، الإبداع، والتعامل العاطفي والمجتمعي، تحريك الروبوتات، والذكاء العام (AGI) ويشمل القيام بكل ما سبق، كما للذكاء الاصطناعي القدرة على شرح المواد الدراسية، وتقديم التغذية الراجعة الفورية على الإجابات، وتقديم النصح والإرشاد الأكاديمي للطلاب حول أفضل قسم في الكلية أو لدراسة مواد دراسية تتلاءم مع قدراتهم العقلية، كما يمكن للذكاء الاصطناعي الوصول لعدد كبير من الطلاب حيث يساعد في جعل الفصول الافتراضية متاحة للجميع، خاصة إذا كانوا يتحدثون بلغات مختلفة أو يعانون من إعاقات سمعية. (رزق، 2021، ص. 574)

وتشهد المنطقة العربية حاليا زيادة في تطبيق التكنولوجيا في مجال التعليم، ومن المتوقع أن تنتقل الفصول الدراسية في منطقة الشرق الأوسط قريبا من الإطار التقليدي للتعلم إلى التعليم الذكي الذي يعد الذكاء الاصطناعي عنصرا محوريا فيه، حيث سيتم استخدام مزيج من الروبوتات والذكاء الاصطناعي المصمم حسب الحاجة والمعلمين، ووفقا للخبراء ستستفيد نسبة كبيرة من الشباب في المنطقة من الروبوتات التي تتسم بالصبر والمرونة، كما سيتحرر معلمو الصفوف من الأمور الإدارية وسيتفرغون للتركيز على الطلاب، فإذا كان للذكاء الاصطناعي دور مهم في كثير من الميادين والمجالات فإن له دورا أكثر أهمية في العملية التعليمية والتربوية الحديثة، حيث يمكن تنفيذ العديد من التطبيقات في العملية التربوية والتي من خلالها يمكن تحقيق عدة مزايا أهمها: تحسين عملية اتخاذ القرار، وتحسين جودة التعليم، وتنمية المهارات الحياتية، وتنمية التحصيل المعرفي لدى المتعلمين، وغيرها من المزايا التي تسهم بشكل كبير في تعزيز تنافسية العملية التربوية، وإنتاج أجيال قادرة على مواجهة تحديات العصر الذي يعيشون فيه. (عبد القادر، 2020، ص. 202)

ومن هنا يتبين بأن الذكاء الاصطناعي قد أصبح إضافة مهمة وقيِّمة في مجال التعليم العام؛ فقد قدّم الذكاء الاصطناعي العديد من الإسهامات في المجال التعليمي، ورفع من مستوى وجودة الصفوف الدراسية؛لذا تسعى جميع الدول المتقدمة والنامية لاعتماده كوسيلة أساسية في العملية التعليمية لما يقدمه من إثراء في هذا المجال؛ ومن المتوقع ازدياد أهمية الذكاء الاصطناعي في التعليم بشكل كبيرة خلال السنوات القادمة.

خصائص الذكاء الاصطناعي :

يتميز الذكاء الاصطناعي بقدرته على أداء عمليات مثل الاستنتاج والتفكير وحل المشكلات (العوامل المجسدة، والشبكات العصبية، والأساليب الإحصائية للذكاء الاصطناعي)؛ وتمثيل المعرفة (الأنطولوجيا)؛ والتخطيط (التخطيط والتعاون متعدد العوامل)؛ والتعلم الآلي؛ ومعالجة اللغة الطبيعية (استرجاع المعلومات – التنقيب عن النصوص، الترجمة الآلية)؛ والذكاء الاجتماعي (محاكاة التعاطف)؛ والإبداع (الحدس الاصطناعي، الخيال الاصطناعي) (Dilek et al., 2015, 23)؛ ويتم أدناه تناول تلك الخصائص.

- **الاستنتاج والتفكير وحل المشكلات (العوامل المجسدة والشبكات العصبية والأساليب الإحصائية للذكاء الاصطناعي):**

إن الشبكات العصبية الاصطناعية هي نموذج رياضي حسابي يحاكي الخصائص السلوكية للشبكات العصبية للحيوان وينفذ معالجة المعلومات المتوازية الموزعة؛ السمة الأساسية لها هي محاولة تقليد نمط نقل المعلومات بين الخلايا العصبية في الدماغ، وبالتفصيل، فإن الشبكة العصبية الاصطناعية هي الحصول على حل مشكلة محددة، وفقًا لفهم آلية الشبكة العصبية البيولوجية، وفقًا للتحكم في الأفكار الهندسية وطريقة الوصف الرياضي، وإنشاء النموذج الرياضي المقابل واستخدام الخوارزميات المناسبة لتحديد معالم النموذج الرياضي للتكنولوجيا (Liu, 2022, 45).

لذلك يساهم الذكاء الاصطناعي في العملية التعليمية بشكل كبير حيث تعتبر المدارس والطلاب مصدر كبير للبيانات، لذلك يمكن عمل أنظمة مدرسية قادرة على إدارة بيانات المدارس والطلاب في آن واحد وحفظها على شكل قواعد بيانات ضخمة، هذه البيانات الضخمة يمكن استخدامها في تدريب شبكات عصبية تستطيع التنبؤ بضعف المستوى الفردي للطالب والنقص في الموارد المادية والبشرية على مستوى المدارس والجامعات قبل حدوثها.

ويعتمد الذكاء الاصطناعي على البيانات ولذلك ستساعد مثل هذه الخوارزميات الوزارات والمدارس على اتخاذ قرارات معلوماتية (informed decisions) بخصوص مؤسساتهم مما سيزيد من جودة المخرجات التعليمية ويقلل من تكاليف هذه المدارس، حيث يمكن على سبيل المثال جمع بيانات إعداد الكتب واستخدامها واسترجاعها وأعداد الطلاب من المدارس على مر سنوات سابقة، ومن ثم تنبؤ الحاجة من الكتب في مختلف المدارس في السنة القادمة بناء على العدد المتوقع للطلاب في كل المدارس، وبذلك يتم إرسال الكمية المثالية للكتب للمدارس بدلا من الزيادة والنقص التي تحصل كل عام، وتتسبب في تأخر استلام الطلاب لكتبهم الدراسية في بعض الأحيان. (رزق، 2021، ص. 577- 578)

- **تمثيل المعرفة (الأنطولوجيا):**

يعد تمثيل المعرفة والاستدلال مجالًا فرعيًا مهمًا في الذكاء الاصطناعي يتعامل مع القضايا المتعلقة بتشكيل المعرفة بطريقة يمكن للآلات أن تقرأها وتفهمها وتستنبطها؛ في الوقت الحاضر، يمتلك تمثيل المعرفة الكثير من التطبيقات داخل، على سبيل المثال، الويب الدلالي، حيث ينشأ الكثير من العمل على منطق الوصف والأنطولوجيا من هذا المجال (Thimm, 2014, 528).

وتبرز أهمية الذكاء الاصطناعي في مجال تمثيل المعرفة (الأنطولوجيا) من خلال تصميم الأنظمة الذكية باستخدام اللغات المنطقية ذات الكفاءة التعبيرية العالية، بالإضافة إلى أن الذكاء الاصطناعي يخدم البرمجة التي يستخدم فيها المنطق بوصفه لغة برمجة تتعامل مع المعارف المطلوبة، وبناء آليات الاستدلال التي يتم تطبيقها لاستنتاج نتائج عند التعامل مع المعلومات المطلوبة، وعلى الرغم من أهمية هذا الدور الذي يلعبه الذكاء الاصطناعي في مجال النظم المنطقية الخبيرة بهدف مساعدة الخبراء البشريين، إلا أنها ليست بديلا عنهم، لأن البشر في النهاية يملكون مرونة في التفكير والاستدلال المنطقي، ما قد تفتقده الآلة في بعض الأحيان، ولهذا تجد علماء الذكاء الاصطناعي في سعي دائم لمحاولة تطوير عملية الاستدلال المنطقي لـ الآلة، وجعلها قادرة على التعلم من التجربة والأخطاء تماما مثل البشر، للحصول على المرونة المطلوبة في التعامل مع كافة المعطيات باستخدام تقنيات الذكاء الاصطناعي المختلفة. (الحصى وآخرون، 2022، ص. 165)

- **التخطيط (التخطيط والتعاون):**

يعد الذكاء الاصطناعي فرعا من فروع علوم الحاسبات Computer Science وإحدى الركائز الأساسية التي تقوم عليها صناعة التكنولوجيا في العصر الحالي، وإحدى الركائز الأساسية التي تقوم عليها صناعة التكنولوجيا في العصر الحالي، والتي تهتم بطرق ووسائل صنع وتصميم أجهزة وآلات ذكية تستطيع التفكير والتصرف مثل البشر، وتقوم بمهام متعددة تتطلب ذكاءً مثل التعلم، والتخطيط، وتمييز الكلام، والتعرف على الوجه، وحل المشكلات، والإدراك، والتفكير العقلي والمنطقي، وبحيث تصبح الآلات تفكر مثل البشر، بما يمكن أن يوصف بأنه "حاسوب له عقل"، وبذلك فإن تطبيقات الذكاء الاصطناعية في التعليم تواكب متطلبات العصر تخطيطا وتنفيذا وتقويما وتطويرا، وتقوم على أسس علمية، ولا تخضع في ذات الوقت لإملاءات معينة، سواء كانت إملاءات تحددها رغبات داخلية أو تحركها ضغوط خارجية، لأن للتعليم متطلباته التي تنبع من طبيعته والتي تحتاج إلى تطبيقات حديثة تدعم كل ما يتم فيه. (المهدي، 2021، ص. 108-133)

ويعد التخطيط من العناصر الأساسية للذكاء الاصطناعي، حيث تعتبر مرحلة التخطيط من أهم المراحل التي يجب الاهتمام بها لتطبيق الذكاء الاصطناعي داخل المؤسسات التعليمية، ويمكن تحديد مراحل التخطيط من خلال: تحديد المبادئ التي ستبنى عليها الرؤية المقترحة لتطبيق الذكاء الاصطناعي، ولا بد أن تتفق تلك الرؤية مع الممارسات العالمية وثوابت العمل في المؤسسات التعليمية، وتحديد القيم التي ستبنى عليها الرؤية، بحيث تتلخص تلك القيم في: الالتزام، والمشاركة، والتعاون، أيضا ينبغي تحديد عناصر الرؤية المقترحة، ووضع نماذج فعلية لممارسات متميزة في هذا المجال، ودراستها بشكل متعمق للاستفادة منها في التعرف على نقاط القوة والضعف فيها، ومن ثم تبني نقاط القوة، ومحاولة إيجاد حلول لنقاط الضعف، وفي الأخير ينبغي تحديد المتطلبات التي على أساسها سوف سيتم تطبيق الرؤية المقترحة في شكل قائمة محددة وواقعية وواضحة يمكن تحقيقها. (الألفي، 2022، ص. 763)

- **التعلم (التعلم الآلي):**

التعلم الآلي هو تخصص فرعي للذكاء الاصطناعي، حيث تتعلم برامج الحاسوب (الخوارزميات) ارتباطات القوة التنبؤية من الأمثلة الموجودة في البيانات، والتعلم الآلي هو ببساطة تطبيق النماذج الإحصائية على البيانات باستخدام أجهزة الحاسوب؛ ويستخدم التعلم الآلي مجموعة واسعة من الأساليب الإحصائية من تلك المستخدمة عادةً في الطب، وتعتمد التقنيات الأحدث مثل التعلم العميق على نماذج ذات افتراضات أقل حول البيانات الأساسية وبالتالي فهي قادرة على التعامل مع بيانات أكثر تعقيدًا (Panch et al., 2018, 2).

وتعتمد تطبيقات التعلم الآلي (تسمى أيضا نماذج التعلم الآلي) على الشبكة العصبية، وهي شبكة من العمليات الحسابية الخوارزمية التي تحاول محاكاة عملية الإدراك والتفكير للعقل البشري، وتتكون الشبكة العصبية في أبسط أمورها من: مستوى المدخلات: حيث تدخل البيانات إلى الشبكة، ومستوى مخفي واحد على الأقل، حيث تقوم خوارزميات التعلم الآلي بمعالجة المدخلات وتطبيق الأوزان والتحيزات والحدود على المدخلات، حيث تدخل البيانات إلى الشبكة، كما تتكون من: طبقة مخرجات: حيث تظهر الاستنتاجات المختلفة التي تتمتع فيها الشبكة بدرجات مختلفة من الثقة، وتعتمد نماذج التعلم الآلي على شبكات عصبية اصطناعية ذات طبقة مخفية واحدة فقط، ويتم تغذية هذه النماذج بالبيانات المصنفة وهي بيانات معززة بعلامات تحدد خصائصها بطريقة تساعد النموذج على تعريف وفهم البيانات، وهي قادرة على التعلم الخاضع للإشراف (أي التعلم الذي يتطلب الإشراف البشري)، مثل التعديل الدوري للخوارزميات في النموذج. (بكاري، 2022، ص. 294- 295)

- **الذكاء الاجتماعي:**

تهدف محاكاة التعاطف إلى المشكلة المزدوجة لتحليل التعاطف، أي التجسيد الاصطناعي وإظهار السلوكيات التعاطفية في العوامل الافتراضية أو الروبوتية، والتي يتصورها المستخدمون البشريون؛ حتى الآن، لا يزال من المستحيل إعادة إنشاء النظام الإدراكي العصبي البشري في الآلات، بحيث يستحيل صنع الصور الرمزية "المتعاطفة بشكل فعلي"، ومع ذلك، فإن محاكاة السلوك الشبيه بالبشر التي تستدعي تصورًا للتعاطف من قبل المستخدم أمر ممكن ومفيد للتجريب والتطبيقات، وتتضمن المنهجية عادةً تصميمًا مستوحى من النظرية أو الممارسة لنظام اصطناعي "مدمج في التعاطف" وتقييم بشري لفعاليته (Xiao et al., 2016, 5).

ومن أهم تقنيات الذكاء الاصطناعي الحوسبة الوجدانية Affective Computing وهي تقنية تهدف إلى تطوير أنظمة وأجهزة يمكنها التعرف على العواطف البشرية وتفسيرها ومحاكاتها، بالإضافة إلى تقنية الذكاء المحيطي Ambient Intelligence وهي تقنية تهدف إلى توفير واجهات ذكية لجميع الأشياء المحيطة بالبشر، مما يمكنها من التعرف والاستجابة للبشر عن طريق الصوت أو الحركة أو الإيماءة، وأيضا تقنية النظام الخبير Expert System وهو نظام أو برنامج كمبيوتر يعتمد على الذكاء الاصطناعي مصمم خصيصا لمحاكاة قدرة الخبير البشري في حل المشكلات واتخاذ القرارات أو أداء مهمة محددة. (حسن، 2022، ص. 215-216)

- **الإبداع (الحدس الاصطناعي والخيال الاصطناعي):**

إن الحدس الاصطناعي هو قدرة أنظمة الذكاء الاصطناعي على اتخاذ خيارات بديهية أو الاستجابة بشكل حدسي للمشكلات؛ وهو أيضًا قدرة النظام على تقييم سياق المشكلة واستخدام التعرف على الأنماط أو الخصائص من مجموعة البيانات لاختيار مسار العمل أو المساعدة في عملية اتخاذ القرار بطريقة تلقائية؛ ويُقارن الحدس الاصطناعي، على سبيل المثال، بالأجهزة العصبية أو التعلم الآلي أو الشبكات العصبية، أكثر في مراحله الأولى؛ وقد يكون تصرف الذكاء الاصطناعي بشكل حدسي ضروريًا في مواقف معينة لأنه يمكن اتخاذ القرارات بشكل أسرع مما هو عليه في الذكاء الاصطناعي المنطقي (Johanssen & Wang, 2021, 175).

والحدس الاصطناعي عملية تلقائية لا تبحث عن بدائل منطقية، وتستبق استجابات مفيدة في فترة قصيرة من الزمن، وتركز بشكل أساسي على تقديم إجابات دون البحث المتكرر عن حلول لمشكلة معينة؛ وعادةً، تحتاج العملية التي تتحكم في جهازٍ ما إلى ملاحظات لمعرفة ما إذا كان التحكم في الإجراء صحيحًا، ولكن مع الحدس الاصطناعي، يُفترض أن الإجابة صحيحة، ولا يتم تنفيذ أي ملاحظات أخرى، بمعنى أنه لا يوجد تقييم ذاتي؛ بشكل أساسي، تعتمد معالجة الحدس الاصطناعي على خوارزميات بسيطة تم إنشاؤها لحل المشكلات الشائعة دون آليات حل المشكلات المعقدة (Diaz-Hernandez & Gonzalez-Vilella, 2015, 27).

ومن خلال ما تم تناوله، يتبين بأن الذكاء الاصطناعي أصبح يتسم بالعديد من الخصائص التي تجعل منه مشابهًا للذكاء البشري؛ فالذكاء الاصطناعي المتطور قادر على التعلم والتكيف وإجراء العمليات المنطقية والتفاعل، لذلك فإن الذكاء الاصطناعي قد يستجيب بطرق ذكية ومختلفة؛ ونظرًا لتكلف وتطور تلك الخصائص، فقد يكون الذكاء الاصطناعي إضافة قيمة إلى السياقات التعليمية.

متطلبات تطبيق الذكاء الاصطناعي بمجال التعليم:

يتم أدناه تناول المتطلبات الرئيسية لتطبيق الذكاء الاصطناعي بمجال التعليم. وتندرج هذه المتطلبات تحت ثلاث فئات، وهي المتطلبات المادية والمتطلبات البشرية (الإدارية) والمتطلبات التقنية.

- **متطلبات مادية:**

لا يعتمد تبني الذكاء الاصطناعي في المؤسسات التعليمية على الثقافة فحسب، بل ينتج أيضًا عن الموارد، والتي يجب تقسيمها بشكل أكبر، وبالمقارنة مع الابتكارات الأخرى، تعد الموارد المالية المتاحة من خلال الميزانية جانبًا مهمًا يحدد بشكل عام تنفيذ التقنيات الجديدة في مشاريع الذكاء الاصطناعي، ويمكن أن تساعد الميزانية المرتفعة في تمكين القدرات، وخلق الحرية المالية والمساعدة في بناء المهارة في الذكاء الاصطناعي (Pumplun et al., 2019, 9).

ومن المتطلبات المادية الرئيسية التي ينبغي توافرها لإدماج الذكاء الاصطناعي في التعليم: ضرورة توفير أدوات مهارات المعلمين والعاملين بالتربية والتعليم، وذلك من خلال برامج التدريب وتوفير منصة إلكترونية باللغة العربية للذكاء الاصطناعي بهدف تنمية مهارات المعلمين في برامج الذكاء الاصطناعي، واستثمار الموارد المحيطة والخارجية لتوفير عملية الإدخال للذكاء الاصطناعي، والعمل على تقليل الهدر من الإمكانيات المادية والبشرية، وتوفير عملية مسح شامل للبيئة الداخلية والخارجية قبل تنفيذ عملية الذكاء الاصطناعي في تعليم قبل الجامعي، وكذلك إشراك القطاع الخاص في عملية الإعداد، والتنفيذ. (تره، 2019، ص. 368– 369)

- **متطلبات بشرية (إدارية):**

من المتطلبات البشرية الضرورية لتطبيق الذكاء الاصطناعي داخل المؤسسات التعليمية: تأهيل وتنمية وتطوير الكفاءات العلمية والقدرات المحلية المتخصصة في مجال الذكاء الاصطناعي، وتدريب العاملين من خلال دورات متخصصة لتنمية المعرفة بكيفية استخدام تقنيات الذكاء الاصطناعي، وتطوير المناهج الدراسية مع تخصيص مادة مستقلة للذكاء الاصطناعي في المدارس والجامعات لترسيخ مفهومه بين الطلاب، وتبني كل ما يسهم في زيادة عدد الطلبة المتفوقين المقبولين بالمدارس وأولئك الذي يملكون الفهم والمهارات اليدوية، كما ينبغي إعداد البرامج التدريبية والتثقيفية بالمؤسسات التعليمية للاستفادة من تقنيات الذكاء الاصطناعي لمواكبة التغير المتوقع حدوثه بالوظائف المستقبلية. (عبد السلام، 2022، ص. 423)

كما ينبغي ضرورة صياغة رؤية واضحة حول إدخال برامج الذكاء الاصطناعي للمعلمين، وأيضا إعداد برامج تدريبية لتعليم الطلاب استخدام وإنشاء برامج الذكاء الاصطناعي في مصر، ووضع استراتيجية عمل يجتمع في إعدادها كل من: وزارة التربية والتعليم، ووزارة الاتصالات ووزارة الاستثمار، بهدف وضع مخطط وقانون عمل يحدد كيفية إدخال الذكاء الاصطناعي في التعليم قبل الجامعي، ووضع نماذج إرشادية للعاملين على إدخال نظام الذكاء الاصطناعي بالتعليم قبل الجامعي، وتحديد أدوار كل المنظمات المشاركة في إعداد الخطة، وتنفيذها، وإشراك القطاع الخاص في عملية الإعداد، والتنفيذ لعملية إدخال الذكاء الاصطناعي في التعليم قبل الجامعي. (تره، 2019، ص. 368)

- **متطلبات تقنية:**

من أهم المتطلبات التقنية لتطبيق الذكاء الاصطناعي في التعليم: توفير البنية التحتية والإمكانات المادية والشبكات اللازمة، والعمل على تطوير استخدام تقنية التعلم بالواقع الافتراضي لتتماشى مع الذكاء الاصطناعي وخاصة مع شيوع وانتشار استخدامها في الفترة الأخيرة، وضرورة التوعية بأهمية التغيير ومواكبة تطورات العصر وتثقيف الجمهور وفئات المجتمع المختلفة بمفهوم وأهمية الذكاء الاصطناعي واستخداماته لتسهيل تبني هذه التقنية في عمل وتطوير الخدمات بالمؤسسات التعليمية وخاصة من الجيل القديم المسيطر، والذي يكون أحيانا غير قابل للتغيير. (عبد السلام، 2021، ص. 423-424)

ومن المتطلبات التقنية التي يتطلبها الذكاء الاصطناعي في المؤسسات التعليمية (المقيطي، 2021، ص. 51-52) :

1. تحديث قاعدة معلومات وبيانات المؤسسات التعليمية كلما دعت الحاجة لذلك.
2. توفير خبراء ومختصين لتطوير الذكاء الاصطناعي المستخدم بالمؤسسات التعليمية.
3. توفير شبكة حاسوبية ذات سرعة معقولة وتكون متاحة لكل منتسبي المؤسسات التعليمية.
4. توفير أنظمة وبرامج تساعد على ربط الوحدات الجامعية المختلفة معا بما يوفر مشاركة المعلومات والبيانات.
5. توفير نظام بريد إلكتروني بما يتناغم مع آخر التطبيقات الذكية لجميع منتسبي المؤسسة التعليمية.
6. توفير أحدث برامج التدريب المختصة بتطبيقات الذكاء الاصطناعي، وتوفير القنوات المختلفة لعقد الاجتماعات الخاصة بالمؤسسة التعليمية.

ومن خلال ما تم استعراضه، يتبين بأن التطبيق الفعال لتقنيات الذكاء الاصطناعي يتطلب توفر العديد من المتطلبات المتنوعة؛ ومن هنا يمكن القول بأن تطبيق الذكاء الاصطناعي ليس مسعى سهل التحقيق؛ لذلك فإن على المؤسسات التربوية على مختلف المستويات توجيه بالغ اهتمامها نحو توفير الموارد والمقومات الكافية لتطبيق نظم الذكاء الاصطناعي ودمجها في العملية التعليمية بصورة فعالة؛ وفي هذا الصدد، من المهم أيضًا رصد أي صور من المعوقات التي قد تعيق توافر المتطلبات الضرورية لاستخدام الذكاء الاصطناعي على النحو المأمول.

معايير الأمن السيبراني:

في عام 2018، قدمت الهيئة الوطنية للأمن السيبراني ضوابط الأمن السيبراني الأساسية لضمان الحد الأدنى من متطلبات الأمن السيبراني للمؤسسات في السعودية، ويتمثل الهدف الرئيسي للضوابط في حماية وفرض السرية والنزاهة وتوافر معلومات المؤسسة وأصولها التكنولوجية، علاوة على ذلك، يتم استخدام الضوابط من قبل الحكومة كطريقة لتقييم الامتثال، وقد تم إنشائها بناءً على أطر ومعايير الأمن السيبراني الوطنية والدولية إلى جانب القوانين الوطنية في السعودية؛ وهي تغطي خمسة مجالات رئيسية: حوكمة الأمن السيبراني، وتعزيز الأمن السيبراني، وصمود الأمن السيبراني، والأمن السيبراني للحوسبة السحابية والأطراف الخارجية، والأمن السيبراني لأنظمة التحكم الصناعي (Almomani et al., 2021, 10). وفيما يلي يتم تناول هذه المعايير بشيء من التفصيل.

- **حوكمة الأمن السيبراني:**

إن حوكمة الأمن السيبراني هي إحدى وسائل إدارة المعلومات وتنظيم الأنظمة الأمنية المطبقة داخل المؤسسات وإعداد الموارد البشرية للحفاظ على سير العمل في إدارة شبكات الحاسوب، وتهدف حوكمة الأمن السيبراني إلى ضمان فاعلية خطط الأمن السيبراني والأهداف والمبادرات داخل المؤسسات التعليمية في تحقيق المتطلبات التشريعية والتنظيمية ذات العلاقة، ولذلك يجب تحديد وتوثيق واعتماد استراتيجيات الأمن السيبراني داخل المؤسسات التعليمية ودعمها من قبل الرؤساء والمديرين، كما لابد أن تتماشى الأهداف الاستراتيجية للأمن السيبراني للمؤسسات التعليمية مع المتطلبات التشريعية والتنظيمية ذات العلاقة، والعمل على تنفيذ خطة عمل لتطبيق استراتيجية الأمن السيبراني بنجاح، ولذلك ينبغي مراجعة استراتيجية الأمن السيبراني على فترات زمنية مخطط لها، والتزام ودعم أصحاب الصلاحية فيما يتعلق بإدارة وتطبيق برامج الأمن السيبراني في تلك المؤسسات التعليمية، ولإدارة ضوابط الأمن السيبراني يجب إنشاء إدارة معينة بالأمن السيبراني في الجهة المستقلة عن إدارة تقنية المعلومات والاتصالات، ويفضل ارتباطها مباشرة بالرؤساء والمدراء. (الهيئة الوطنية للأمن السيبراني، 2018، ص.14-19-26)

وتراعي حوكمة الأمن السيبراني تحديد وتوثيق واعتماد إطار إدارة مخاطر أمن المعلومات، ويتم تنفيذ إجراء إدارة المخاطر في العديد من الحالات، منها ما هو في مرحلة مبكرة للمشاريع الجديدة، ومنها ما يتم قبل إجراء تغييرات جوهرية أو كبيرة في البيئة التقنية، وكذلك قبل التعاقد والاستعانة بمصادر خارجية، وقبل إطلاق خدمات أو تقنيات جديدة أو استخدام تقنيات الحوسبة السحابية، وعند حدوث هجمات أو اختراقات متقدمة وعلى نطاق واسع لجهات أخرى ولأنظمة مشابهة للأنظمة المستخدمة في المؤسسات التعليمية، كما أنه يتم تقييم مخاطر الأمن السيبراني على العمليات والتطبيقات والبنية التحتية. (الإدارة العامة للأمن السيبراني، 2021، ص.11)

- **تعزيز الأمن السيبراني:**

تتضمن المجالات الفرعية لتعزيز الأمن السيبراني: إدارة الأصول؛ وإدارة الهوية والوصول؛ ونظام المعلومات والمعالجة؛ وحماية المنشآت؛ وحماية البريد الإلكتروني؛ وإدارة أمن الشبكات؛ وأمن الأجهزة المحمولة؛ وحماية البيانات والمعلومات؛ والتعمية؛ وإدارة النسخ الاحتياطي والاسترداد؛ وإدارة نقاط الضعف؛ واختبار الاختراق؛ وإدارة سجلات أحداث الأمن السيبراني والمراقبة؛ وإدارة حوادث وتهديدات الأمن السيبراني؛ والأمن المادي؛ وأمن تطبيقات الويب، والهدف من تعزيز الأمن السيبراني هو التأكد من أن المؤسسة التعليمية لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العلاقة لجميع الأصول المعلوماتية والتقنية المتاحة للمؤسسة التعليمية، من أجل دعم العمليات التشغيلية للمؤسسة التعليمية ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية والتقنية ودقتها وتوافرها، ولتعزيز ضوابط الأمن السيبراني لإدارة تلك الأصول المعلوماتية والتقنية للمؤسسة التعليمية. (الهيئة الوطنية للأمن السيبراني، 2018، ص.14-26)

وتسعى المؤسسات التعليمية إلى تعزيز الأمن السيبراني من أجل الحد من التجسس والتخريب الإلكتروني، وتعزيز القدرات الفنية لدى الطلاب للدفاع عن خصوصيتهم ضد التهديدات السيبرانية، بالإضافة إلى حماية الشبكات وأنظمة المعلومات على مستوى القطاعات التعليمية، والتصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة والحواسيب لضمان بيئة آمنة داخل المدارس والمؤسسات التعليمية في ظل مجتمع المعلومات، لذلك تسعى القطاعات التعليمية إلى تعزيز الأمن السيبراني من خلال توظيف نظام شبكي آمن لتبادل المعلومات بين الطلبة، ومعالجة المشكلات الطارئة، وحماية جميع الأجهزة من الاقتحامات والبرمجيات الضارة. (فرج، 2022، ص. 528-529)

- **صمود الأمن السيبراني:**

يتمثل جزء أساسي من برامج الصمود السيبراني في العملية المستمرة لتحديد المخاطر وتقييمها والاستجابة لها حيث يمكن للمؤسسات فهم احتمالية وقوع حدث وتأثيره الناتج، وإن أساس تحقيق مطالب ومجاراة الجرائم السيبرانية هو الصمود، سواء بالنسبة للإدارات الحكومية، والمنظمات التجارية وغير الهادفة للربح، والأفراد، والأسر، والمجموعات، والمناطق، والدول القومية (Dalton et al., 2017, 4)

ويهدف الأمن السيبراني إلى ضمان توافر متطلبات صمود البيانات والمعلومات لاستمرارية أعمال المؤسسات التعليمية، وضمان تقليل الآثار الحرجة المترتبة عن الاضطرابات في الخدمات الإلكترونية، وأنظمة وأجهزة معالجة معلوماتها، جرّاء الكوارث الناتجة عن المخاطر السيبرانية، لذلك يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني ضمن إدارات المؤسسات التعليمية لاستمرارية أعمالها وتحقيق أهدافها.(الهيئة الوطنية للأمن السيبراني، 2018، ص.14-26)

- **الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية:**

يستلزم الأمن المتعلق بالأطراف الخارجية تضمين متطلبات الأمن السيبراني في العقود وإلزام مقدم الخدمة السحابية الذي يتم التعاقد معه بتطبيقها. (هيئة الاتصال والفضاء والتقنية، 2020، ص. 5)

ويهدف الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية إلى ضمان حماية المؤسسات التعليمية من المخاطر المتعلقة بالأطراف الخارجية، بما في ذلك خدمات الإسناد لتقنية المعلومات Outsourcing، والخدمات المدارة Managed Services، وذلك وفقا للسياسات والإجراءات التنظيمية للمؤسسات التعليمية، كما يهدف الأمن السيبراني المتعلق بالحوسبة السحابية والاستضافة إلى: ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية، والاستضافة بشكل ملائم وفعّال، وذلك وفقا للسياسات والإجراءات التنظيمية للمدارس، والمتطلبات التشريعية، والتنظيمية، والأوامر، والقرارات ذات العلاقة، وضمان حماية الأصول المعلوماتية والتقنية للجهة التعليمية، وخدمات الحوسبة السحابية التي تم استضافتها، أو معالجتها، أو إدارتها بواسطة أطراف خارجية. (الهيئة الوطنية للأمن السيبراني، 2019، ص. 14)

- **الأمن السيبراني لأنظمة التحكم الصناعي:**

يهدف الأمن السيبراني لأنظمة التحكم الصناعي إلى ضمان إدارة الأمن السيبراني بشكل صحيح وفعال لحماية توافر أصول جهاز ICS/OT الخاص بالمنشأة وسلامتها وسريتها من الهجمات السيبرانية (مثل الوصول غير المصرح به، والتخريب، والتجسس، والتلاعب)، بالارتباط مع استراتيجية الأمن السيبراني للمنشأة، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات الصلة، فضلاً عن المتطلبات الرقابية الدولية الموضوعة في كيان الأمن السيبراني (Maleh & Maleh, 2022, 17).

كما يهدف الأمن السيبراني لأنظمة التحكم الصناعي إلى: التأكد من أن متطلبات الأمن السيبراني مضمنة في منهجية إدارة مشاريع الجهات التعليمية، وإجراءاتها لحماية السرية، وسلامة الأعمال التشغيلية، ودقتها، وتوافرها لأنظمة التحكم الصناعي، وذلك وفقا للسياسات والإجراءات التنظيمية للمؤسسات التعليمية، والمتطلبات التشريعية والتنظيمية ذات العلاقة، ومن الضوابط الأساسية للأمن السيبراني، أنها يجب أن تغطي متطلبات الأمن السيبراني ضمن إدارة المشاريع أنظمة التحكم الصناعي (OT/ICS) بحد أدنى ما يلي: تضمين متطلبات الأمن السيبراني ضمن اختبارات القبول Acceptance Test، وعمليات التقييمEvaluation Process، مثل اختبارات قبول المصنع Factory Acceptance Tests، واختبارات القبول الميداني Site Acceptance Tests، واختبارات التشغيل Commissioning Tests، واختبارات التغيير Change Tests، واختبارات التكامل Integration Tests، ومراجعة الشفرة المصدرية Source Code Review، بالإضافة إلى تضمين مبدأ الأمن من خلال التصميم Secure-By-Design، بوصفه جزء من الأمن المعماري لتصميم البيئة الخاصة بأنظمة التحكم الصناعي OT/ICS، وحماية الأنظمة في البيئة التطويرية Development Environment، وتشمل بيئات الاختبار Testing Environment، والمنصات التكاملية Integration Platforms، وأخيرا يجب مراجعة متطلبات الأمن السيبراني ضمن إدارة مشاريع أنظمة التحكم الصناعي OT/ICS وقياس فعالية تطبيقها وتقييمها دوريا. (الهيئة الوطنية للأمن السيبراني، 2022، ص. 17)

ومن خلال ما تم تناوله، يمكن القول بأن معايير الأمن السيبراني تهتم بتحديد متطلبات حماية أمان الشبكات الإلكترونية من جميع مصادر التهديد والمخاطر الداخلية والخارجية؛ بالإضافة إلى ذلك، لا تركز معايير الأمن السيبراني على الوقاية من حدوث مخاطر الأمن السيبراني، ولكنها أيضًا تحدد الطرق المثلى للاستجابة لتلك المخاطر في حال حدوثها فعليًا؛ لذلك، يمكن القول بأن اتباع معايير الأمن السيبراني قد يساعد المؤسسات التعليمية على مواجهة التهديدات الأمنية في الفضاء السيبراني على نحو فعال.

المخاطر الأمنية للذكاء الاصطناعي بمجال التعليم:

تتزايد تطبيقات الذكاء الاصطناعي كل يوم بصورة لا يمكن حصرها واستيعابها، حيث أصبح الذكاء الاصطناعي واقعا معاشا بعد أن كان مجرد خيالا علميا، وبناءً عليه فقد انقسمت آراء الخبراء إلى قسمين: قسم ينظر إلى الذكاء الاصطناعي نظرة مستقبلية إيجابية، ويرى أنه يحسّن حياتنا ويجعلها أكثر سرعة وسهولة، وقسم آخر ينظر إلى الذكاء الاصطناعي نظرة تشاؤمية خوفًا من التداعيات السلبية للذكاء الاصطناعي على حياتنا، إلا أنه في الواقع يعد الذكاء الاصطناعي سلاحًا ذا حدّين، حيث يمكن أن يكون تأثيره إيجابيا في كل مناحي الحياة، إلا أن ذلك لا ينفي وجود العديد من الأضرار والآثار السلبية والمخاطر الأمنية التي تنتج عن الذكاء الاصطناعي وخاصة في مجال التعليم. (الفراني والحجيلي، 2020، ص. 217)

وعلى الرغم من الإيجابيات الهائلة التي تحققت بفضل تقنية المعلومات، فإن تلك الثورة المعلوماتية المتصاعدة قد صاحبتها العديد في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام، ومن بين تلك الانعكاسات المستحدثة: ظاهرة الجريمة الرقمية، والتي تصاعدت أخطارها بدورها مما أفرز نوعا جديدا من الجرائم العابرة للقارات، والتي لم تعد أخطارها وآثارها محصورة في نطاق دولة بعينها مما أثار بعض التحديات القانونية أمام الأجهزة بمكافحة الجريمة، وقد زاد اتجاه المملكة العربية السعودية مؤخرا نحو استخدام الذكاء الصناعي وإدماجه في شتى المجالات مما أدّى إلى استخدام الإنترنت والتكنولوجيا والمعاملات الإلكترونية، لذلك زادت الهجمات السيبرانية منذ ذلك الحين، مما دفع المملكة لتخصيص جهد أكبر في هذا المجال، وما زال الميدان يحتاج إلى المزيد من الجهود في هذا الاتجاه للحفاظ على أمن المعلومات بالمملكة. (السمحان، 2020، ص. 5-6)

ومن المخاطر الأمنية الأخرى للذكاء الاصطناعي في مجال التعليم: انعدام الخصوصية الشخصية حيث أن هذه الأدوات التقنية الجديدة تطلب من المستخدم تزويد البيانات حتى تتيح توفير خدمات مقننة، إذا لم يزود العميل بياناته الشخصية فلن يحصل على المميزات التي يحصل عليها العملاء الآخرين، مما يشكل ضغطا من أجل التخلي عن الخصوصية وتزويد بعض المواقع ببيانات شخصية من أجل الراحة، وكثير من الأدوات التي نستخدمها يوميا تنافي الخصوصية الفردية، لكن عادة ما يستغني الناس عن الخصوصية في مقابل التواصل مع الآخرين وجودة الخدمة المقدمة، إلا أن هناك بعض المحاولات لاستخدام تقنية البلوكتيشن من أجل وضع البيانات في محتوى الجميع، وتطوير ذكاء اصطناعي دون منحها للشركات مثل مبادرةOpen Mined إلا أن هذه المبادرة ما زالت في مراحلها الأولية. (رزق، 2021، ص. 584)

ومع أن الذكاء الاصطناعي في التعليم يبشر بالخير على نحو كبير، فمن المهم إدراك المخاطر والتحديات المحتملة التي يمثلها، وأحد هذه المخاطر هو إمكانية استمرار التحيز داخل النظم التعليمية، حيث يتم تدريب خوارزميات الذكاء الاصطناعي على كميات هائلة من البيانات.

وبالنظر إلى ما سبق، يتضح بأن استخدام تقنيات الذكاء الاصطناعي ليس خاليًا من التحديات والمخاطر؛ فعلى الرغم من الإمكانات الهائلة التي تتيحها تلك التقنيات، من المهم عدم إغفال احتمالية حدوث مخاطر الأمن السيبراني خارجية المنشأ، وذلك إلى جانب العديد من المخاطر الداخلية الأخرى المهددة لجودة العملية التعليمية؛ لذلك فإن تبني تقنيات الذكاء الاصطناعي في العملية التعليمية ينبغي أن يصاحبه توافر المتطلبات البشرية من مهارات وكفايات تقنية، وذلك من أجل التمكن من تحقيق أقصى استفادة ممكنة من تلك التقنيات من التقليل من حجم المخاطر إلى أدنى حد ممكن.

أثر الأمن السيبراني في تطبيق الذكاء الاصطناعي في التعليم:

تواجه المؤسسات التعليمية سنويا فيضانا مستمرا من الهجمات الإلكترونية السيبرانية، التي كلفتها خسارات كبيرة مالية وفنية، تبلورت في ضياع المعلومات والبيانات، وتشويهها وتغييرها لتحقيق أهداف خبيثة تصب في مصلحة المهاجمين إضافة إلى سرقة الاختبارات النهائية والفصلية، والنتائج الطلابية، لذا صار هناك حاجة ماسة لتطوير ممارسات الأمن السيبراني بالمؤسسات التعليمية خاصة في ظل التطورات العالمية والمستحدثات التقنية الحديثة. (الألفي، 2022، ص. 713- 715)

ومع التسارع الكبير في تطبيق الذكاء الصناعي في المملكة العربية السعودية وارتفاع معدل الهجمات الإلكترونية ومخاطر اختراق البيانات، فقد حرصت المملكة على توفير بيئة آمنة للبيانات والعمليات الرقمية من خلال نظام أمني متين، ووضعت قوانين ولوائح بأنظمة الأمن السيبراني، وأصدرت الإطار السعودي لكوادر الأمن السيبراني "سيوف" التابع للهيئة الوطنية للأمن السيبراني (2020) كمحرك أساسي ودليل مرجعي لإعداد الكوادر المتخصصة في هذا المجال، كما تنبهت إلى ضرورة رفع مستوى الوعي لدى الأفراد من خلال توفير الإرشادات ونهج التدريب الأمثل والتي تسهم في تأمين أنظمة المعلومات وحمايتها، وبناء على ذلك فإن تطوير أداء المعلمين في هذا الجانب ورفع الوعي لديهم سينعكس على ممارساتهم وممارسات طلابهم، ما سيحقق نموا اقتصاديا ورافدا معرفيا هائلا. (السعادات والتميمي، 2022، ص.260-261)

ويعمل الأمن السيبراني من خلال مجموعة من الإجراءات التقنية والإدارية التي تشمل العمليات والآليات التي يتم اتخاذها في عالم الذكاء الاصطناعي لمنع أي تدخل غير مقصود أو غير مصرح له بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما يعمل الأمن السيبراني على تأمين وحماية وسرية وخصوصية البيانات الشخصية للعاملين داخل القطاعات التعليمية، وحماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف. (السمحان، 2020، ص. 11)

وتوضح دراسة الدمرداش (2022، ص. 1358–1359) أن إدراج الذكاء الاصطناعي في عمليات التدريس والتعلم كإحدى مستحدثات التكنولوجيا في التعليم يعد ثورة صناعية جديدة تفتح آفاقا لمواجهة معظم التحديات في التعليم اليوم، والعمل على ابتكار ممارسات حديثة في عملية التعليم والتعلم بهدف تحقيق التنمية المستدامة في جميع الدول، وتعزيز متخذي القرار وصانعي السياسات للذكاء الاصطناعي في تطوير سياسات التعليم عامة وتكنولوجيا التعليم خاصة والتي أصبحت في الوقت الراهن تتبع منهج محوره الطالب في مجال التعليم بالأجهزة النقالة لضمان تأثير الذكاء الاصطناعي على سد الفجوات التكنولوجية في التعليم والاستفادة منه في الابتكار والمعرفة، من هنا تنبع مدى أهمية تنمية مهارات الأمن السيبراني لدى المتخصصين في المؤسسات التعليمية ولدى الطلاب، وخاصة طلاب الحاسبات والذكاء الاصطناعي، حيث أن هؤلاء الطلاب هم مستقبل أمن المؤسسات الحكومية وغير الحكومية، ويعود ذلك لما توفره مهارات الأمن السيبراني من مهارات فكرية لحل المشكلات ومهارات أدائية لتنفيذ الحلول وصد الهجمات السيبرانية، بما يعود بالإفادة الكبيرة على مجال الذكاء الاصطناعي حيث أن أي تأخير في التفكير في الحلول وتنفيذ الحل الأمثل القابل للتنفيذ فورا قد يؤدي إلى مخاطر وتهديد لأمن الأفراد والمؤسسات.

وبذلك فإن الأمن السيبراني يهدف إلى أن تظل البيانات في المؤسسات التعليمية وغيرها من المؤسسات تحت الرقابة والحماية خاصة في ظل الاعتماد على الذكاء الاصطناعي والوسائل التقنية المتجددة والتي تستخدم كم هائل من البيانات والمعلومات المعرضة إلى السرقة أو التلف في أي وقت، مما يؤدي إلى انهيار المؤسسات أو تكبدها التكاليف المادية الهائلة، بالإضافة إلى انتهاك خصوصية العاملين والمعلمين والطلاب، ولذا يعمل الأمن السيبراني على حماية المؤسسات وأفرادها، وتوفير الأمان داخلها.

الدراسات السابقة:

- **أولا: الدراسات التي تناولت الذكاء الاصطناعي:**

سعت دراسة التويجري (2022) إلى التعرف على متطلبات دعم اتخاذ القرارات الإدارية باستخدام الذكاء الاصطناعي في وزارة التعليم بالمملكة العربية السعودية، وتقديم التوصيات لدعم اتخاذ القرارات الإدارية باستخدام الذكاء الاصطناعي في وزارة التعليم بالمملكة العربية السعودية، وقد تكون مجتمع الدراسة من خبراء القيادات في وزارة التعليم، وأساتذة الجامعات، والمختصين في علوم الحاسب والذكاء الاصطناعي، واشتملت العينة على (17) فرد، وقد اعتمدت الدراسة على المنهج الوصفي المسحي كمنهج لها، واستعانت بالمقابلة كأداة للدراسة، وقد توصلت الدراسة إلى العديد من النتائج أهمها: ضعف الرؤية والفلسفة التي توجه الذكاء الاصطناعي لدعم اتخاذ القرارات الإدارية في وزارة التعليم بالمملكة العربية السعودية، وضعف استقطاب الخبرات التقنية المؤهلة لعملية تطوير الذكاء الصناعي لدعم اتخاذ القرارات الإدارية في وزارة التعليم بالمملكة العربية السعودية، بالإضافة إلى ضعف البنية التحتية الرقمية من أبرز المعوقات التي تواجه تطبيق الذكاء الصناعي لدعم اتخاذ القرارات الإدارية في وزارة التعليم بالمملكة العربية السعودية.

وهدفت دراسة القحطاني (2022) إلى التعرف على واقع استخدام الذكاء الاصطناعي في إدارة الموارد البشرية ومعوقاته ومتطلبات استخدامه من وجهة نظر أعضاء هيئة التدريس العاملين، وقد تكون مجتمع الدراسة من أعضاء هيئة التدريس بجامعة الملك سعود، واشتملت العينة على (54) عضو، وقد اعتمدت الدراسة على المنهج الوصفي المسحي كمنهج لها، واستعانت بالاستبانة كأداة للدراسة، وقد توصلت الدراسة إلى العديد من النتائج أهمها: أن استخدام الذكاء الاصطناعي في إدارة الموارد البشرية بجامعة الملك سعود حصل على متوسط حسابي كلي (2.82) من (5) أي بدرجة متوسطة، كما حصلت متطلبات استخدام الذكاء الاصطناعي في إدارة الموارد البشرية على متوسط حسابي كلي (3.87) أي بدرجة كبيرة، وحصلت معوقات استخدام الذكاء الاصطناعي في إدارة الموارد البشرية بجامعة الملك سعود على متوسط حسابي كلي (3.67) أي بدرجة كبيرة.

وقامت دراسة تشانغ وأصلان (Zhang & Aslan, 2021) بمراجعة الوضع الحالي لأبحاث الذكاء الاصطناعي في التعليم، وإبراز بعض تقنيات الذكاء الاصطناعي المستخدمة في التعليم وفوائدها المؤكدة والمحتملة للتعليم؛ واعتمد الباحثان على المنهج الوثائقي القائم على استعراض عدد من الأدبيات السابقة التي توضح الذكاء الاصطناعي، وتطبيقات تكنولوجيا الذكاء الاصطناعي في التعليم والمزايا التربوية، والآثار المترتبة على استخدام الذكاء الاصطناعي في التعليم؛ وتوصلت الدراسة إلى العديد من النتائج أهمها: أن تقنية الذكاء الاصطناعي تتقدم بسرعة ومن المتوقع أن ينمو تطبيقها في التعليم بسرعة في المستقبل القريب، وأن أبرز فوائد الذكاء

الاصطناعي في التعليم تشمل: تحفيز المحادثات، وزيادة اهتمام ومشاركة الطلاب، وتحسين جودة التفاعلات، وتجارب التعلم المخصصة بناء على الاحتياجات والتفضيلات والمعرفة السابقة، وتوفير التدخلات الوقائية والتكيفية، وتوفير التعلم التشاركي، وبيئات التعلم التفاعلية، وأن إرشادات أخلاقيات الذكاء الاصطناعي الحالية لديها عيوب خطيرة، إضافةً إلى نقص مجموعة من أخلاقيات الذكاء الاصطناعي التي تعد بالغة الأهمية لأبحاث الذكاء الاصطناعي وتطويره وتنفيذه في مثل هذه الإرشادات.

أما دراسة تاهيرو (Tahiru, 2021) فقد قامت بتحليل فرص وفوائد وتحديات الذكاء الاصطناعي في التعليم؛ واعتمد الباحث على المنهج الوثائقي القائم على استعراض عدد من الأدبيات السابقة التي توضح الذكاء الاصطناعي في التعليم، وأنواع الذكاء الاصطناعي في التعليم، وتحديات وفرص الذكاء الاصطناعي في التعليم؛ وأظهرت الدراسة العديد من النتائج أهمها: أن الذكاء الاصطناعي أثبت كونه وسيلة فعالة لإنشاء تجربة تعليمية هادفة ومفيدة للطلاب من خلال توفير تغذية راجعة وتوجيه أفضل للطالب، وتحسين مستوى التدريس، وأن الذكاء الاصطناعي يعزز التعلم التشاركي، ويحسن الدافعية ومستوى التعلم لدى الطالب، وأن أبرز تحديات الذكاء الاصطناعي في التعليم تتضمن: البيانات غير الدقيقة أو غير المكتملة، واستخدام التكنولوجيا الخاطئة في تصميم أنظمة التعلم التكيفية، والمخاوف المتعلقة بملكية البيانات والأمن والثقة، ومشكلات الاستعداد التنظيمي وتوافر البنية التحتية اللازمة لاستخدام الذكاء الاصطناعي، وفقدان الوظائف، وقضية المساءلة.

- **ثانيًا: الدراسات التي تناولت الأمن السيبراني:**

استقصت دراسة الدحياني والصنوي (2021) عن متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر المختصين، وقد تكون مجتمع الدراسة من المختصين ف مجال الحاسوب والتقنيات والذكاء الاصطناعي، واشتملت العينة على (70) فرد، وقد اعتمدت الدراسة على المنهج الوصفي المسحي كمنهج لها، واستعانت بالاستبانة كأداة للدراسة، وقد توصلت الدراسة إلى العديد من النتائج أهمها: أن متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر المختصين كانت عالية جدا، بالإضافة إلى عدم وجود فروق ذات دلالة إحصائية في استجابات أفراد العينة تعزى للمتغيرات الديموغرافية (النوع – الدرجة العلمية– وسنوات الخبرة في هذا التخصص) وذلك على مستوى الدرجة الكلية للأداة وعلى مستوى كل مجال من مجالات البحث.

وقد عملت دراسة المنتشري وحريري (2020) على التعرف على درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، وقد تكون مجتمع الدراسة من معلمات المرحلة المتوسطة بمدينة جدة، واشتملت العينة على (362) معلمة، وقد اعتمدت الدراسة على المنهج الكمي الوصفي التحليلي كمنهج لها، واستعانت بالاستبانة كأداة للدراسة، وقد توصلت الدراسة إلى العديد من النتائج أهمها: أن معلمات المرحلة المتوسطة على درجة متوسطة من الوعي بكل من مفاهيم الأمن السيبراني، مخاطر الأمن السيبراني، وانتهاكات الأمن السيبراني، كما أنه لا يوجد فروق ذات دلالة إحصائية عند مستوى (0.05) تعزى إلى متغيري المؤهل الدراسي، وعدد سنوات الخبرة بين استجابات المعلمات، إلا أن هناك فروق ذات دلالة إحصائية عند مستوى (0.05) تعزى إلى متغير دورات تدريبية في الأمن السيبراني.

واستكشفت دراسة رحمن وآخرين (Rahman et al., 2020) أسباب أهمية تثقيف الطلاب المعاصرين المخاطر المرتبطة بالنشاط في الفضاء السيبراني والاستراتيجيات التي يمكن استخدامها لتعزيز تعليم الأمن السيبراني في المدارس؛ وقد اعتمد الباحثون على المنهج الوثائقي القائم على استعراض عدد من الأدبيات السابقة التي توضح الأمن السيبراني، والحاجة إلى تعليم الأمن السيبراني، وتحديات تعليم الأمن السيبراني؛ وأظهرت الدراسة عدة نتائج، كان أهمها: تأثير تعليم الأمن السيبراني بدرجة (كبيرة) على وعي الطلاب بالمخاطر المحتملة التي تواجههم عند استخدام أدوات التواصل عبر الإنترنت، تعد أفلام الكرتون من الموارد المهمة لاستخدامها عند مناقشة مبادئ الأمن السيبراني مع طلاب المدارس، وتعتبر برامج الوعي الأمني أحد الاستراتيجيات المهمة لتعزيز تعليم الأمن السيبراني في المدارس.

- **ثالثًا: الدراسات التي تناولت الأمن السيبراني والذكاء الاصطناعي:**

هدفت دراسة تريفونوف وآخرين (Trifonov et al., 2020) إلى توضيح محاولات تحسين التعليم من خلال إدخال مبادئ ديناميكية والتخصيص في المناهج الدراسية لتحقيق أنظمة التعلم التكيفية التي تدار بواسطة أساليب الذكاء الاصطناعي، وقد استخدم الباحثون تجربتهم في الجامعة التقنية بصوفيا في تطبيق هذه الأساليب في مجال الأمن السيبراني؛ واعتمد الباحثون على المنهج الوثائقي القائم على استعراض عدد من الأدبيات السابقة التي توضح تجربة كلية نظم وتكنولوجيا الحاسوب في الجامعة التقنية بصوفيا في مجال أبحاث تطبيق أساليب الذكاء الاصطناعي في الأمن السيبراني، والمتطلبات والمعايير والمبادرات الدولية في مجال تعليم الأمن السيبراني، والسمات الخاصة بمنهج تدريب الأمن السيبراني في الجامعة التقنية بصوفيا، والتدريب التكيفي وأساليب الذكاء الاصطناعي؛ وأظهرت الدراسة العديد من النتائج أهمها: بدأت كلية نظم وتكنولوجيا الحاسوب في أبحاث تطبيق أساليب الذكاء الاصطناعي في الأمن السيبراني منذ

2013 للتوصل إلى الاستخدام الفعال لأساليب الذكاء الاصطناعي المختارة نظريًا لاكتشاف الهجمات ومنع الاختراقات والإجراءات الأكثر شيوعًا في الدفاع السيبراني عن نظم المعلومات، وأن أبرز المبادرات الدولية في مجال تعليم الأمن السيبراني في السنوات الأخيرة تشمل: "أداة التقييم الذاتي للأمن السيبراني الوطني وحماية البنية التحتية للمعلومات الحيوية الوطنية" للاتحاد الدولي للاتصالات (ITU)، وتوصيات الشبكة الأوروبية ووكالة أمن المعلومات (ENISA)، ومن أهم المعايير الدولية في تعليم الأمن السيبراني: إطار الشهادة المهنية للمبادرة العالمية لتعليم الأمن السيبراني، ومنهج الأمن السيبراني الذي أعدته مجموعة عمل حلف الناتو للتحديات الأمنية الناشئة (ESCWG)، وتوصيات فريق العمل المشترك CSEC2017 المعني بتعليم الأمن السيبراني (JTF)، وأن هدف الكلية هو تشكيل ثلاثة تخصصات تتعلق بالتدريب في الأمن السيبراني: للبكالوريوس، والماجستير في علوم الحاسوب العامة، والماجستير في الأمن السيبراني.

وتناولت دراسة الخضري وآخرين (2020) التعرف على مفهوم الأمن السيبراني لدى طلاب الجامعات السعودية، والتعرف على أهم الجرائم التي يتعامل معها الأمن السيبراني، وطرق الوقاية من تلك الجرائم، وكذلك التعرف على المعوقات المجتمعية لتحقيق الوقاية من جرائم الفضاء السيبراني، والوصول إلى مقترح يساعد على تفعيل الأمن السيبراني داخل الجامعات السعودية، وقد تكون مجتمع الدراسة من مجموعة من طلاب الجامعات السعودية وأعضاء هيئة التدريس، والإداريين، واشتملت العينة على (300) فرد تم تقسيمهم إلى: (212) طالب، و(52) عضو هيئة تدريس، (36) إداري، وقد اعتمدت الدراسة على المنهج الوصفي التحليلي كمنهج لها، واستعانت بالاستبانة كأداة للدراسة، وقد توصلت الدراسة إلى العديد من النتائج أهمها: ندرة التدريب على برامج الذكاء الاصطناعي بالنسبة للقيادات الجامعية والطلاب، وضعف التكنولوجيا المستخدمة في الذكاء الاصطناعي، بالإضافة إلى قلة خبرة القيادات التربوية في التعامل مع الذكاء الاصطناعي، وتعدد المخاطر التي تتعرض لها الجامعات السعودية متمثلة في البرامج الخبيثة والاختراقات، مما يعد تدمير للبيانات، وعدم وجود سياسات أمنية واضحة وبرامج حماية في الجامعات.

ومن خلال استعراض الباحثان للإطار النظرى والدراسات السابقة تم وضع فرضيات الدراسة التالى :

1- يمكن التعرف على المتطلبات (التنظيمية- البشرية- المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني.

2- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (05..0) حول محاور الاستبانة ودرجتها الكلية وفق متغير (النوع).

3- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) حول محاور الاستبانة والدرجة الكلية وفقا لمتغير وفقا لمتغير (عدد سنوات الخبرة).

4- لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) حول محاور الاستبانة والدرجة الكلية وفقا لمتغير وفقا لمتغير (المؤهل الدراسي).

خصائص عينة البحث:

تم حساب التكرارات والنسب المئوية لأفراد عينة البحث وفقًا (النوع – عدد سنوات الخبرة – المؤهل الدراسي).

4- توزيع أفراد العينة حسب النوع :

جدول رقم (1) توزيع أفراد العينة وفقا للجنس

م	النوع	التكرار	النسبة المئوية
1	ذكر	68	**%56.7**
2	انثى	52	**%43.3**
المجموع		**120**	**%100.0**

يتضح من الجدول رقم (1) أن نسبة (56.7%) من أفراد العينة ذكور، بينما نسبة (43.3%) من أفراد العينة إناث.

5- توزيع أفراد العينة حسب عدد سنوات الخبرة:

جدول رقم (2) توزيع أفراد العينة وفقا لعدد سنوات الخبرة

م	عدد سنوات الخبرة	التكرار	النسبة المئوية
1	أقل من 5 سنوات	9	%7.5
2	من 5 سنوات إلى أقل من 10 سنوات	84	%70.0
3	10 سنوات فأكثر	27	%22.5
المجموع		120	%100.0

يتضح من الجدول رقم (2) أن نسبة (7.5%) من أفراد العينة لديهم خبرة لفترة أقل من (5)سنوات، بينما نسبة (70.0%) من أفراد العينة لديهم خبرة لفترة من 5 إلى أقل من 10 سنوات، بينما نسبة (22.5%) من أفراد العينة لديهم خبرة لفترة من 10 سنوات فأكثر.

6- توزيع أفراد العينة حسب المؤهل الدراسي:

جدول رقم (3) توزيع أفراد العينة وفقا للمؤهل العلمى

م	المؤهل الدراسي	التكرار	النسبة المئوية
1	بكالوريوس	116	%96 .6
2	ماجستير	4	%3.4
المجموع		120	%100.0

يتضح من الجدول رقم (3) أن نسبة (96.6%) من أفراد العينة حاصلين على مؤهل بكالوريوس، بينما نسبة (3.4%) من أفراد العينة حاصلين على مؤهل ماجستير.

صدق أداة الدراسة:

2) صدق الاتساق الداخلي لأداة البحث.

ت) صدق الاتساق الداخلي لمحاور البحث.

تم حساب صدق الاتساق الداخلي وفقًا لاستجابات أفراد العينة الاستطلاعية (ن=30)، وذلك بحساب معامل ارتباط بيرسون بين درجات كل عبارة والدرجة الكلية للمحور الذي تنتمي إليه العبارة من محاور الاستبانة كما يوضح نتائجها جدول رقم (4) التالي:

جدول رقم (4) معاملات ارتباط بيرسون بين درجات كل عبارة والدرجة الكلية للمحور الذي تنتمي إليه العبارة من محاور الاستبانة

المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني					
رقم الفقرة	معامل الارتباط	رقم الفقرة	معامل الارتباط	رقم الفقرة	معامل الارتباط
1	.862**	5	.858**	9	.816**
2	.760**	6	.881**	10	.691**
3	.867**	7	.776**		
4	.776**	8	.703**		
المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني					
1	.860**	5	.856**	9	.786**
2	.748**	6	.880**	10	.685**
3	.890**	7	.776**		
4	.741**	8	.685**		
المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني					
1	.829**	5	.813**	9	.709**
2	.827**	6	.858**	10	.749**
3	.698**	7	.869**		
4	.866**	8	.831**		

**** دال إحصائيًا عند مستوى الدلالة (0.01) * دال إحصائيًا عند مستوى الدلالة (0.05)**

يتبين من جدول (4) السابق أن معاملات ارتباط العبارات بالدرجة الكلية للمحور الذي تنتمي إليه العبارة من محاور الاستبانة جاءت جميعهًا دالة إحصائيًا عند مستوى دلالة (0.01)، وجاءت جميع قيم معاملات الارتباط قيم عالية حيث تراوحت في المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بين (.691**-.881**)، بينما تراوحت معاملات الارتباط في المحور الثاني: المتطلبات

(البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بين (**748.-**890.)، بينما تراوحت في المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بين (**698.-**869.)، مما يدل على توافر درجة عالية من صدق الاتساق الداخلي لعبارات محاور الاستبانة.

ث) الصدق البنائي العام لمحاور الاستبانة":

تم التحقق من الصدق البنائي لمحاور الاستبانة من خلال إيجاد معاملات الارتباط بين الدرجة الكلية لكل محور والمجموع الكلي للاستبانة، ويوضح نتائجها الجدول التالي:

جدول رقم (5) معاملات الارتباط بن الدرجة الكلية لكل محور والدرجة الكلية لمحاور الاستبانة

م	المحور	معامل الارتباط
1	**المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني**	**.998**
2	**المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني**	**.994**
3	**المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني**	**.993**

**** دال إحصائيًا عند مستوى الدلالة (0.01)**

يتبين من الجدول رقم (5) السابق أن قيم معاملات الارتباط لمحاور الاستبانة بالدرجة الكلية للاستبانة جاءت بقيم مرتفعة حيث تراوحت بين (**993.-**998.)، وكانت جميعها دالة إحصائيًا عند مستوى دلالة (0.01)، مما يدل على توافر درجة عالية من الصدق البنائي لمحاور الاستبانة.

جدول رقم (6) معاملات ثبات ألفا كرونباخ لمحاور الاستبانة

م	المحور	عدد الفقرات	معامل ألفا كرونباخ
1	المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	10	.996
2	المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	10	.998
3	المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	10	.998
	المجموع	30	.997

يتضح من الجدول رقم (6) السابق أن قيم معاملات الثبات لمحاور الاستبانة جاءت بقيم عالية حيث تراوحت قيم معاملات الثبات لمحاور الاستبانة بين (.996-.998) وبلغت قيمة معامل الثبات الكلي لمحاور الاستبانة (.997)، وتشير هذه القيم من معاملات الثبات إلى صلاحية الاستبانة للتطبيق وإمكانية الاعتماد على نتائجها والوثوق بها.

عرض ومناقشة نتائج الدراسة :

نتائج الفرض الأول :

لبحث نتيجة **الفرض الأول** والذى ينص على أنه يمكن التعرف على المتطلبات (التنظيمية- البشرية- المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني، تم حساب المتوسط الحسابي والانحراف المعياري لكل محور من محاور الاستبانة، ثم ترتيب تلك المحاور ترتيب تنازلي بناءً على المتوسط الحسابي كما تبين نتائج الجدول (7) التالي:

جدول رقم (7) التكرارات والمتوسطات الحسابية لتوضيح متطلبات تطبيق الذكاء الاصطناعي من وجهة نظر المعلمين بمنطقة المدينة المنورة التعليمية وفقا لمعايير الأمن السيبراني

م	المحور	المتوسط الحسابي	الانحراف المعياري	ترتيب المحور	درجة الاستجابة
1	المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	4.10	.719	1	عالية
3	المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	3.48	.711	3	عالية
2	المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	3.01	.960	2	متوسطة
	الدرجة الكلية للاستبانة	3.53	.620	---	عالية

يتبين من الجدول رقم (7) السابق أن درجة متطلبات تطبيق الذكاء الاصطناعي من وجهة نظر المعلمين بمنطقة المدينة المنورة التعليمية وفقا لمعايير الأمن السيبراني جاءت بدرجة (عالية) من وجهة نظر أفراد عينة الدراسة، حيث جاء المتوسط العام للاستبانة (3.53) بانحراف معياري بلغ (620.)، وبلغت الانحرافات المعيارية لمحاور الاستبانة بين (711.-960.) مما يدل تقارب أراء أفراد عينة الدراسة.

وجاء في الترتيب الأول المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (4.10)، وانحراف معياري بلغ (719.)، يليه في الترتيب الثاني المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (3.48)، وانحراف معياري بلغ (711.)، بينما جاء في الترتيب الأخير المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (3.01)، وانحراف معياري بلغ (960.).

ويرى الباحثان أن حصول المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني على درجة استجابة عالية من وجهة نظر أعضاء هيئة التدريس أفراد العينة قد يعزى إلى اهتمام إدارات المدارس السعودية محل الدراسة بالحفاظ على تطوير الكفايات المهنية لدى المعلمين وزيادة وعيهم بأساليب وطرائق تطبيق الذكاء الاصطناعي في التدريس، وربما كان هذا هو السبب محاولة توفير كافة المتطلبات التنظيمية المطلوبة وبكل الإمكانات المتاحة سواء كانت مادية أو تقنية أو إدارية؛ وقد يكون ذلك أيضًا نتيجة لاهتمام المدارس بحماية ما لديها من موارد ومحتويات التعليمية من مخاطر الهجمات والاختراقات السيبرانية.

وتتفق تلك النتيجة مع ما أشارت إليه دراسة القحطاني (2022) التي أكدت على أن متطلبات استخدام الذكاء الاصطناعي حصلت على متوسط حسابي كلي (3.87) أي بدرجة كبيرة.

كما يرى الباحثان أن حصول المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني على درجة استجابة متوسطة قد يعزي إلى اللوائح الإدارية والقوانين المعمول بها في المدارس محل الدراسة والتي تساعد المعلمين إلى حد ما على تطبيق الذكاء الاصطناعي في التدريس مما يحد من كثرة المعوقات التي تحول دون الحفاظ على الامن السيبراني، وذلك إلى جانب التعقيدات التي قد تكتنف حماية المحتويات التعليمية من الاختراقات غير المصرح بها.

وتتفق تلك النتيجة مع ما توصلت إليه نتيجة دراسة الخضري وآخرين (2020) التي أكدت على وجود قصور في توافر التكنولوجيا المستخدمة في الذكاء الاصطناعي، بالإضافة إلى قلة خبرة القيادات التربوية في التعامل مع الذكاء الاصطناعي مما يجعل المتطلبات التنظيمية أحد أهم المتطلبات الواجب توافرها.

نتائج الفرض الثانى:

لبحث نتيجة **الفرض الثانى** والذى ينص على أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (05..0) حول محاور الاستبانة ودرجتها الكلية وفق متغير (النوع)، تم تطبيق اختبار (ت) "Independent Samples Test" لتوضيح دلالة الفروق في إجابات مفردات عينة الدراسة طبقًا لمتغير النوع كما موضح في الجدول التالي رقم (8)

جدول (8) نتائج " اختبار ت " (Independent Samples Test) للفروق في إجابات مفردات عينة الدراسة حول محاور الاستبانة والدرجة الكلية طبقًا إلى اختلاف متغير النوع

المحور	النوع	ن	المتوسط الحسابي	الانحراف المعياري	درجات الحرية	قيمة "ت"	الدلالة	مستوى الدلالة
المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	ذكر	68	4.0779	.74710	118	-.499	.619	غير دالة عند مستوى > 0.05
	انثى	52	4.1442	.68611				
المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	ذكر	68	2.9529	.88663	118	-.809	.420	غير دالة عند مستوى > 0.05
	انثى	52	3.0962	1.05179				
المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	ذكر	68	3.4485	.61656	118	-.699	.486	غير دالة عند مستوى > 0.05
	انثى	52	3.5404	.82254				
الدرجة الكلية	ذكر	68	3.4931	.55271	118	-.877	.382	غير دالة عند مستوى > 0.05
	انثى	52	3.5936	.70160				

يتضح من خلال النتائج الموضحة بالجدول (8) ما يلي:

- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير النوع .
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير النوع .
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير النوع .
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول محاور الاستبانة والدرجة الكلية طبقًا إلى اختلاف متغير النوع ، مما يدل على صحة الفرضية الأولى.

ويرى الباحثان أن تلك النتيجة قد ترجع إلى أن أفراد العينة من الجنسين سواء الذكور أو الإناث يلمسون حرص الإدارات المدرسية على تطوير الأساليب والاستراتيجيات التدريسية بما يتناغم مع الصحوة التكنولوجية في التعليم رغم المعوقات التي قد تحول دون قدرتها على ذلك في مختلف المدارس التي ينتسب لها أفراد عينة الدراسة، وقناعتهم بأهمية الحفاظ على الامن السيبراني لما له من نفع يعود على الطلاب والمعلمين في مختلف المجالات ويزيد من الاستفادة المُحققة منها مما قارب بين إجاباتهم حول محاور الاستبانة ودرجتها الكلية، وتم التأكيد على عدم وجود فروق دالة إحصائيًا بين أفراد العينة وفقا لمتغير النوع .

نتائج الفرض الثالث:

لبحث نتيجة **الفرض الثالث** والذى ينص على **لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) حول محاور الاستبانة والدرجة الكلية وفقا لمتغير وفقا لمتغير (عدد سنوات الخبرة)**، تم اختبار "تحليل التباين الأحادي"(One Way Anova) لتوضيح دلالة الفروق في إجابات مفردات عينة حول محاور الاستبانة والدرجة الكلية وفقا لمتغير طبقًا (عدد **سنوات الخبرة)**، وكانت نتائج التحليل كما هو موضح بالجدول (9) التالي:

الجدول رقم (9) نتائج " تحليل التباين الأحادي " (One Way Anova) للفروق في إجابات مفردات عينة الدراسة حول محاور الدراسة طبقًا إلى اختلاف متغير عدد سنوات الخبرة

المحور		مجموع المربعات	عدد درجات الحرية	مربع المتوسط	أداة الإحصاء (ف)	الدلالة	مستوي الدلالة
المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	بين المجموعات	.483	2	.241	.463	.631	غير دالة عند مستوى 0.05 >
	داخل المجموعات	61.052	117	.522	---		
	المجموع	61.535	119	---	---		
المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	بين المجموعات	3.350	2	1.675	1.843	.163	غير دالة عند مستوى 0.05 >
	داخل المجموعات	106.343	117	.909	---		
	المجموع	109.693	119	---	---		
المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	بين المجموعات	5.172	2	2.586	5.495	.128	غير دالة عند مستوى 0.05 >
	داخل المجموعات	55.052	117	.471	---		
	المجموع	60.224	119	---	---		
الدرجة الكلية	بين المجموعات	1.967	2	.983	2.620	.097	غير دالة عند مستوى 0.05 >
	داخل المجموعات	43.903	117	.375	---		
	المجموع	45.870	119	---	---		

يتضح من خلال نتائج الجدول رقم (9):

- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير عدد سنوات الخبرة.
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير عدد سنوات الخبرة.
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير عدد سنوات الخبرة.
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول محاور الاستبانة والدرجة الكلية طبقًا إلى اختلاف متغير عدد سنوات الخبرة، مما يدل على صحة الفرضية الثانية.

ويرى الباحثان أن تلك النتيجة قد ترجع إلى كثرة الاحتكاك بين أغلب أفراد العينة أثناء العمل ووعيهم بما يمارسون من أعمال تتعلق بتطبيق الذكاء الاصطناعي في التدريس بمساعدة إدارات المدارس المنتسبين لها، مما قارب بين إجاباتهم حول محاور الاستبانة والدرجة الكلية.

وتتفق تلك النتيجة مع ما أشارت إليه نتيجة دراسة الدحياني والصنوي (2021) التي توصلت إلى عدم وجود فروق ذات دلالة إحصائية في استجابات أفراد العينة تعزى لمتغير سنوات الخبرة وذلك على مستوى الدرجة الكلية للأداة وعلى مستوى كل مجال من مجالات البحث.

نتائج الفرض الرابع:

لبحث نتيجة **الفرض الرابع** والذى ينص على **لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) حول محاور الاستبانة والدرجة الكلية وفقا لمتغير وفقا لمتغير (المؤهل** العلمى)، تم اختبار "تحليل التباين الأحادي"(One Way Anova) لتوضيح دلالة الفروق في إجابات مفردات عينة حول محاور الاستبانة والدرجة الكلية وفقا لمتغير طبقًا (المؤهل العلمى)، وكانت نتائج التحليل كما هو موضح بالجدول (10) التالي:

الجدول رقم (10) نتائج " تحليل التباين الأحادي " (One Way Anova) للفروق في إجابات مفردات عينة الدراسة حول محاور الدراسة طبقًا إلى اختلاف متغير المؤهل العلمى

المحور		مجموع المربعات	عدد درجات الحرية	مربع المتوسط	أداة الإحصاء (ف)	الدلالة	مستوي الدلالة
المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	بين المجموعات	.276	2	.138	.263	.769	غير دالة عند مستوى 0.05 >
	داخل المجموعات	61.259	117	.524	---		
	المجموع	61.535	119	---	---		
المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	بين المجموعات	.143	2	.072	.077	.926	غير دالة عند مستوى 0.05 >
	داخل المجموعات	109.550	117	.936	---		
	المجموع	109.693	119	---	---		
المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني	بين المجموعات	.034	2	.017	.033	.968	غير دالة عند مستوى 0.05 >
	داخل المجموعات	60.190	117	.514	---		
	المجموع	60.224	119	---	---		
الدرجة الكلية	بين المجموعات	.023	2	.011	.029	.971	غير دالة عند مستوى 0.05 >
	داخل المجموعات	45.847	117	.392	---		
	المجموع	45.870	119	---	---		

يتضح من خلال نتائج الجدول رقم (10):

- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير المؤهل العلمى.
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير المؤهل العلمى.
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني وفقًا لمتغير المؤهل العلمى.
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول محاور الاستبانة والدرجة الكلية طبقًا إلى اختلاف متغير المؤهل العلمى ، مما يدل على صحة الفرضية الثالثة.

ويرى الباحثان أن تلك النتيجة قد ترجع إلى أن اختلاف المؤهل الدراسي ليس له أي تأثير في تقييم متطلبات تطبيق الذكاء الاصطناعي في التدريس وفقاً لمعايير الأمن السيبراني، وأن المسؤول الاول عن هذا هو اللوائح الإدارية والقانونية والقدرة المادية والتقنية التي تساعد في تطبيق الذكاء الاصطناعي في التدريس، مما قارب بين إجاباتهم حول محاور الاستبانة والدرجة الكلية.

وتتفق تلك النتيجة مع ما أشارت إليه نتيجة دراسة المنتشري وحريري (2020) التي أكدت على أنه لا يوجد فروق ذات دلالة إحصائية عند مستوى (0.05) تعزى إلى متغيري المؤهل العلمى .

ملخص النتائج:

- أن درجة متطلبات تطبيق الذكاء الاصطناعي من وجهة نظر المعلمين بمنطقة المدينة المنورة التعليمية وفقا لمعايير الأمن السيبراني جاءت بدرجة (عالية) من وجهة نظر أفراد عينة الدراسة.
- جاء في الترتيب الأول المحور الأول: المتطلبات (التنظيمية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (4.10)، وانحراف معياري بلغ (719.)، يليه في الترتيب الثاني المحور الثالث: المتطلبات (المادية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (3.48)، وانحراف معياري بلغ (711.)، بينما جاء في الترتيب الأخير المحور الثاني: المتطلبات (البشرية) لتوظيف تطبيقات الذكاء الاصطناعي في التدريس وفقا لمعايير الأمن السيبراني بمتوسط حسابي بلغ (3.01)، وانحراف معياري بلغ (960.).
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول محاور الاستبانة والدرجة الكلية طبقًا إلى اختلاف متغير النوع ، مما يدل على صحة الفرضية الأولى.
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول محاور الاستبانة والدرجة الكلية طبقًا إلى اختلاف متغير عدد سنوات الخبرة، مما يدل على صحة الفرضية الثانية.
- عدم وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0.05) في آراء أفرد عينة البحث حول محاور الاستبانة والدرجة الكلية طبقًا إلى اختلاف متغير المؤهل العلمى ، مما يدل على صحة الفرضية الثالثة.

توصيات الدراسة:

- ضرورة استفادة الخبراء التربويين من نتائج الدراسة الحالية في تحديد الأنواع المناسبة من الصور التي يجب استخدامها لتطبيق الذكاء الاصطناعي في التدريس وفقاً لمعايير الأمن السيبراني.
- ضرورة إنشاء المدارس لقواعد بيانات لتخزين المحتويات العلمية مع اتخاذ التدابير اللازمة لتقييد وتنظيم عملية الوصول إلى والاستفادة من تلك المحتويات في تطوير أداء المعلمين.
- ضرورة اهتمام إدارات مدارس التعليم العام برصد المعوقات والتحديات المختلفة التي تكتنف التصدي لمخاطر الأمن السيبراني عبر جميع المستويات التنظيمية للمدارس.

- ضرورة تعزيز حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية بالمدارس ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات لتحقيق الأمن السيبراني.
- ضرورة تعزيز وحماية البنية التحتية لمدارس التعليم العام؛ بحيث تساعد على تطبيق الذكاء الاصطناعي بالتدريس وفقاً لمعايير الأمن السيبراني.
- ضرورة شراء البرمجيات والحواسيب وفق أنظمة تحددها إدارة المدرسة لتطبيق الذكاء الاصطناعي في التعليم.
- ضرورة قيام كليات التربية بالمملكة بتصميم المزيد من الدورات وورش عمل تدريبية تستهدف توعية الطلاب المعلمين حول تطبيق الذكاء الاصطناعي في مجال التعليم المعاصر.

قائمة المراجع

أولًا: المراجع العربية:

ابن إبراهيم، منال حسن محمد. (2021). الوعي بجوانب الأمن السيبراني في التعليم عن بعد. *المجلة العلمية لجامعة الملك فيصل- العلوم الإنسانية والإدارية*، 22(2)، 299-307. http://search.mandumah.com/Record/1159533

الإدارة العامة للأمن السيبراني. (2021). سياسة الأمن السيبراني.

الألفي، هاني رزق عبد الجواد. (2022). القيادات الأكاديمية وأدوارها في تعزيز ممارسات الأمن السيبراني بالجامعات الأمريكية وإمكانية الإفادة منها بالجامعات المصرية. *مجلة كلية التربية- جامعة المنصورة*، 119، 709-778.

بكاري، مختار. (2022). تحديات الذكاء الاصطناعي وتطبيقاته في التعليم. *مجلة المنتدى للدراسات والأبحاث الاقتصادية*، *6*(1)، 286-305. http://search.mandumah.com/Record/1278730

تره، مريم شوقي عبد الرحمن. (2019). متطلبات إدخال تكنولوجيا الذكاء الاصطناعي في التعليم قبل الجامعي المصري. *المجلة الجزائرية للدراسات الإنسانية*، *1*(2)، 349-372.

التويجري. فواز بن عبدالله. (2022). متطلبات دعم اتخاذ القرارات الإدارية باستخدام الذكاء الاصطناعي في وزارة التعليم بالمملكة العربية السعودية. *مجلة الفنون والأدب وعلم الإنسانيات والاجتماع*، (85)، 154-171.

حسانين، مجدولين السيد. (2020). عملية التصميم الصناعي في ضوء الذكاء الاصطناعي. *مجلة العمارة والفنون والعلوم الإنسانية*، (عدد خاص)، 628-643. http://search.mandumah.com/Record/1117756

حسن، ياسمين أحمد عامر. (2022). الذكاء الاصطناعي- الأسس ومجالات التطبيق في المكتبات وعلوم المعلومات. *المجلة العربية لتكنولوجيا المعلومات والبيانات*، *2*(2)، 209-218.

الحصى، دينا محمد محمد علي، والنويهي، سهام محمود، وإسماعيل، فاطمة، والسيد، مايسة عبده علي. (2022). تطبيق منطق الارتباط في مجال الذكاء الاصطناعي وتمثيل المعرفة. *مجلة بحوث- جامعة عين شمس*، 2(1)، 140-170. http://search.mandumah.com/Record/1379532

الخشان، خشان بن صالح. (2021). العروض والذكاء الاصطناعي. *مجلة جامعة الطائف للعلوم الإنسانية*، 7(28)، 853-887. http://search.mandumah.com/Record/1197043

الخضري، جيهان سعد محمد، وكليبي، نعمة ناصر مدبش، وسلامي، هدى جبريل علي (2020). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية المقارنة. *مجلة تطوير الأداء الجامعي*، 12 (1)، 217- 233.

الدحياني، ناصر سعيد علي محسن، والصنوي، أمير عبد الوالي حيدر. (2021). متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر الخبراء. *مجلة الجامعة الوطنية*، (18)، 93-126.

درويش، عمرو محمد محمد أحمد، والليثي، أحمد حسن محمد. (2020). أثر استخدام منصات الذكاء الاصطناعي في تنمية عادات العقل ومفهوم الذات الأكاديمي لعينة من طلاب المرحلة الإعدادية منخفضي التحصيل الدراسي. *مجلة كلية التربية- جامعة عين شمس*، *4*(44)، 61-136.

الدمرداش، نانسي صابر. (2022). 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- جامعة المنيا*، 41، 1331-1427.

رزق، هناء رزق محمد. (2021). أنظمة الذكاء الاصطناعي ومستقبل التعليم. *دراسات في التعليم الجامعي*، *52*، 571-587. http://search.mandumah.com/Record/1279733

زمورة، جمال، وبن عيسى، ليلى. (2022). أهمية حوكمة الأمن السيبراني لضمان تحول رقمي آمن للخدمات العمومية في الجزائر. *مجلة البحوث الاقتصادية المتقدمة*، *7*(2)، 414-429.

سراج، شيماء أحمد محمد أحمد.(2022). التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي. *المجلة العربية للعلوم التربوية والنفسية*، (26)، 199-212.

السعادات، خليل بن إبراهيم، والتميمي، ندى بنت عبدالله. (2022). رفع الوعي بالأمن السيبراني لدى المعلمين في ضوء مبادئ تعليم الكبار. *مجلة آفاق جديدة في تعليم الكبار*، *32*، 255-280.

السمحان، منى عبدالله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. *مجلة كلية التربية– جامعة المنصورة، 111*، 3-29.

السيد، إيمان سعيد عبد المنعم. (2020). استخدام طلاب كلية الهندسة بجامعة القاهرة للذكاء الاصطناعي في دعم العملية التعليمية والعوامل المؤثرة في تقبلهم له في ضوء نظرية UTAUT. *العلوم التربوية– جامعة القاهرة*، 28(3)، 493-534.

شعبان، أماني عبد القادر محمد. (2021). الذكاء الاصطناعي وتطبيقاته في التعليم العالي. المجلة التربوية–جامعة سوهاج، *84*، 1-23. http://search.mandumah.com/Record/1141709

عبد السلام، ولاء محمد حسني. (2021). تطبيقات الذكاء الاصطناعي في التعليم: المجالات، المتطلبات، المخاطر الأخلاقية. *مجلة كلية التربية*، *36*(4)، 385-466.

عبد القادر، عبد الرازق مختار محمود. (2020). تطبيقات الذكاء الاصطناعي: مدخل لتطوير التعليم في ظل تحديات جائحة فيروس كورونا (COVID-19). المجلة الدولية للبحوث في العلوم التربوية، *3*(4)، 171-224.

العقلاء، رؤى أحمد صالح، وعلي، نور الدين عيسى آدم. (2022). درجة الوعي بمفاهيم الأمن السيبراني لدى معلمي ومعلمات الحاسب الآلي بمدينة حائل. دراسات عربية في التربية وعلم النفس، (144)، 277-300.

غزال، سارة محمد روحي فتحي. (2022). الأمن السيبراني ودرجة وعي المؤسسات بأهميته. *المجلة العربية للنشر العلمي، 47*، 578-584.

الفراني، لينا بنت أحمد بن خليل، والحجيلي، سمر بنت أحمد بن سليمان. (2020). العوامل المؤثرة على قبول المعلم لاستخدام الذكاء الاصطناعي في التعليم في ضوء النظرية الموحدة لقبول واستخدام التكنولوجيا UTAUT. *المجلة العربية للعلوم التربوية والنفسية، 14*، 215-252. http://search.mandumah.com/Record/1036714

فرج، حنان أحمد إبراهيم. (2022). استثمار الذكاء الصناعي في المكتبات الأكاديمية: الواقع والتحديات. المجلة المصرية لعلوم المعلومات– جامعة بني سويف، *9*(2)، 455-483. http://search.mandumah.com/Record/1336061

فرج، علياء عمر كامل إبراهيم. (2022). دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي: جامعة الأمير سطام بن عبد العزيز نموذجا. *المجلة التربوية–جامعة سوهاج، 94*، 509-537. http://search.mandumah.com/Record/1224961

القحطاني، غادة بنت علي بن سعد. (2022). واقع استخدام الذكاء الاصطناعي في إدارة الموارد البشرية ومعوقاته ومتطلبات تطبيقه بجامعة الملك سعود من وجهة نظر هيئة التدريس بالجامعة. *مجلة العلوم التربوية والنفسية*، 6 (55)، 1-23.

مركز البحوث والمعلومات "المملكة العربية السعودية". (2021). *الذكاء الاصطناعي*.

المزيني، عبد العزيز بن أحمد.(2022). الأمن السيبراني واجب من واجبات الدولة الحديثة ووسائل تحقيقه التنظيمية: دراسة تأصيلية مقارنة. *مجلة قضاء- جامعة الإمام محمد بن سعود الإسلامية*،*29*، 492-542.

المقيطي، سجود أحمد محمود. (2021). *واقع توظيف الذكاء الاصطناعي وعلاقته بجودة أداء الجامعات الأردنية من وجهة نظر أعضاء هيئة التدريس* [رسالة ماجستير غير منشورة]. جامعة الشرق الأوسط.

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

المنتشري، فاطمة يوسف، وحريري، رندة. (2020). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية*، (14)، 95-140.

المهدي، مجدي صلاح طه. (2021). التعليم وتحديات المستقبل في ضوء فلسفة الذكاء الاصطناعي. مجلة تكنولوجيا التعليم والتعلم الرقمي، 2(5)، 97-140. http://search.mandumah.com/Record/1354108

مولاي، أمينة، وطيبي، إكرام، وبن الزرافة، إكرام. (2021). تطبيق الذكاء الاصطناعي والذكاء العاطفي في اتخاذ القرار. *مجلة مجاميع المعرفة*، *7* (1)، 187-205.

هيئة الاتصالات والفضاء والتقنية. (2020). *الإطار التنظيمي للأمن السيبراني لمقدمي الخدمة في قطاع الاتصالات وتقنية المعلومات*.

الهيئة الوطنية للأمن السيبراني. (2018). *الضوابط الأساسية للأمن السيبراني*. المؤلف.

الهيئة الوطنية للأمن السيبراني. (2019). *ضوابط الأمن السيبراني للأنظمة الحساسة*. المؤلف.

الهيئة الوطنية للأمن السيبراني. (2022). *ضوابط الأمن السيبراني للأنظمة التشغيلية*. المؤلف.

ثانيًا: المراجع الأجنبية:

Akgun, S., & Greenhow, C. (2022). Artificial intelligence in education: Addressing ethical challenges in K-12 settings. *AI and Ethics, 2*, 431-440. https://link.springer.com/article/10.1007/s43681-021-00096-7

Almomani I, Ahmed M, & Maglaras L. (2021). Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. *PeerJ Computer Science. 7*, 1-26. DOI 10.7717/peerj-cs.703

Anwar, A., & Hassan, S. I. (2017). Applying Artificial Intelligence Techniques to Prevent Cyber Assaults. *International Journal of Computational Intelligence Research, 13*(5), 883-889. http://www.ripublication.com/ijcir17/ijcirv13n5_19.pdf

Cheatham, B., Javanmardian, K., & Samandari, H. (2019). Confronting the risks of artificial intelligence. *McKinsey Quarterly*, *2*(38), 1-9. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Analytics/Our%20Insights/Confronting%20the%20risks%20of%20artificial%20intelligence/Confronting-the-risks-of-artificial-intelligence-vF.pdf

Dalton, W., van Vuuren, J. J., &Westcott, J. (2017). *Building Cybersecurity Resilience in Africa*. A paper presented at the 12th International Conference on Cyber Warfare and Security (ICCWS), Dayton, Ohio, USA.

Diaz-Hernandez, O., & Gonzalez-Vilella, V. J. (2015). Analysis of Human Intuition towards Artificial Intuition Synthesis for Robotics. *Mechatronics and Applications: An International Journal, 1*(1), 23-39. https://nnandn.net/journal/mechatroj/papers/11mechatroj03.pdf

Dilek, S., Çakır, H., & Aydin, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *International Journal of Artificial Intelligence & Applications, 6*(1), 21-39. DOI : 10.5121/ijaia.2015.6102

Goutam, R. K. (2015). Importance of cyber Security. *International Journal of Computer Applications, 111*(7), 14-17. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5cfb7a5bd2e6c181e8a69ebd49b1dadb795f493b

Hamburg, I., & Grosch, K. R. (2017). Ethical Aspects in Cyber Security. *Archives of Business Research, 5*(10), 199-206. http://dx.doi.org/10.14738/abr.510.3818.

Johanssen, J., & Wang, X. (2021). Artificial Intuition in Tech Journalism on AI: Imagining the Human Subject. *Human-Machine Communication, 2*, 173-190. https://doi.org/10.30658/hmc.2.9

Kaswa, R., Nair, A., Murphy, S., & von Pressentin, K. B. (2022). Artificial intelligence: A strategic opportunity for enhancing primary care in South Africa. *South African Family Practice, 64*(1), 1-2. https://doi.org/10.4102/safp.v64i1.5596

Kim, S., Jang, Y., Kim, W., Choi, S., Jung, H., Kim, S., & Kim, H. (2021, February 2-9). *Why and What to Teach: AI Curriculum for Elementary School*. A paper presented at The Thirty-Fifth AAAI Conference on Artificial Intelligence (AAAI-21), online.

Liu, Y. (2022). Artificial Intelligence and Its Application in Educational Industry. *Frontiers in Educational Research, 5*(6), 44-47. DOI: 10.25236/FER.2022.050608

Maleh, Y., & Maleh, Y. (2022). *Cybersecurity in Morocco*. Springer.

Ouyang, F., & Jiao, P. (2021). Artificial intelligence in education: The three paradigms. *Computers and Education: Artificial Intelligence, 2*, 1-6. https://doi.org/10.1016/j.caeai.2021.100020

Panch, T., Szolovits, P., & Atun, R. (2018). Artificial intelligence, machine learning and health systems. *Journal of Global Health, 8*(2), 1-8. doi: 10.7189/jogh.08.020303

Phillips, S. P., Spithoff, S., & Simpson, A. (2022). Artificial intelligence and predictive algorithms in medicine. *Canadian Family Physician, 68*, 570-572. https://www.cfp.ca/content/cfp/68/8/570.full.pdf

Pumplun, L., Tauchert, C., & Heidt, M. (2019). *A New Organizational Chassis for Artificial Intelligence - Exploring Organizational Readiness Factors*. A paper resented at the Twenty-Seventh European Conference on Information Systems (ECIS2019), Stockholm-Uppsala, Sweden.

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology, 10*(5), 378-382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Tahiru, F. (2021). AI in Education: A Systematic Literature Review. *Journal of Cases on Information Technology, 23*(1), 1-20. https://doi.org/10.4018/jcit.2021010101

Thimm, M. (2014, July 20-24). *Tweety: A Comprehensive Collection of Java Libraries for Logical Aspects of Artificial Intelligence and Knowledge Representation*. A paper presented at the Fourteenth International Conference on Principles of Knowledge Representation and Reasoning, Vienna, Austria.

Trifonov, R., Nakov, O., Tsochev, G., & Pavlova, G. (2020, October 1-3). *Possibilities for Improving the Quality of Cyber Security Education through Application of Artificial Intelligence Methods*. A paper presented at the International Conference Automatics and Informatics (ICAI), Varna, Bulgaria.

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Impact, 13*, 1-40. https://doi.org/10.3390/fi13020039

Vähäkainu, P., & Lehto, M. (2019, February 28 - March 1). *Artificial intelligence in the cyber security environment*. A paper presented at the 14th International Conference on Cyber Warfare and Security (ICCWS), Stellenbosch University, South Africa.

Xiao, B., Imel, Z. E., Georgiou, P., Atkins, D. C., & Narayanan, S. S. (2016). Computational Analysis and Simulation of Emphatic Behaviors: a Survey of Empathy Modeling with Behavioral Signal Processing Framework. *Current psychiatry reports, 18*, 1-11. DOI 10.1007/s11920-016-0682-5

Zhang, K., & Aslan, A. B. (2021). AI technologies for education: Recent research & future directions. *Computers and Education: Artificial Intelligence, 2*, 1-11. https://doi.org/10.1016/j.caeai.2021.100025

Zhang, Z., Ning, H., Shi, F., Farha, f., Xu, Y., Xu, J., Zhang, F., & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review, 55*, 1029-1053. https://doi.org/10.1007/s10462-021-09976-0