Sana'a University Journal of Human Sciences
مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 4 | No. 9 | Page 487 – 527 |2025 |
https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

Present a proposed vision for establishing postgraduate programs in the field of cybersecurity and artificial intelligence in Yemeni universities – Sana'a University as a model

Sufian Ali Al-Azab [1,*], Khalid Ali Shania i[1]
[1] Department of Basic Education - Faculty of Education - Sana'a University, Sana'a, Yemen.

***Corresponding author:** *k.shakes@su.edu.ye*

Keywords

1. Proposed concept
2. cyber security
3. artificial intelligence

Abstract:

The research aimed to present a proposed vision for establishing postgraduate programs in the field of Cyber Security and Artificial Intelligence in Yemeni universities - Sana'a University as a mode. The research used the descriptive approach, and a questionnaire consisting of (28) paragraphs distributed over four fields: Financial requirements, Technical requirements, Legislative requirements, and Human requirements. The research sample consisted of (18) experts specialized in the field of cyber security and artificial intelligence, who were chosen intentionally. The most important results were reached as follows: There is a great consensus of the opinions of experts (sample members) on the requirements for establishing postgraduate programs in the field of cyber security and artificial intelligence, as the consensus rate was high and reached 97% at the level of the fields as a whole, and at the level of each field as follows: (Financial requirements 98%, Technical requirements 97%, Legislative requirements 96% Human requirements 94%. The researcher concluded with a proposed vision, and to ensure the achievement of the desired results of the current research, the researcher recommends the necessity of adopting and implementing the proposed vision. Keywords: Proposed concept, cyber security, artificial intelligence.

Sana'a University Journal of Human Sciences
مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 4 | No. 9 | Page 488 – 527 | 2025
https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

تصور مقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية جامعة صنعاء أنموذجًا

سفيان علي العزب [1،*] , خالد علي شانع [2]

[1]قسم التعليم الأساسي ، كلية التربية - جامعة صنعاء ، صنعاء ، اليمن.

*المؤلف: k.shakes@su.edu.ye

الكلمات المفتاحية

1. تصور مقترح
2. الأمن السيبراني
3. الذكاء الاصطناعي.

الملخص:

هدف البحث إلى تقديم تصور مقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية، واتخذ جامعة صنعاء أنموذجًا، واتبع المنهج الوصفي التحليلي، واستخدم استبانة مكونة من (28) فقرة موزعة على (4) مجالات، هي: المتطلبات المالية، والمتطلبات التقنية، والمتطلبات التشريعية، والمتطلبات البشرية، وتكونت عينة البحث من (18) خبيرًا من الخبراء المختصين في مجال الأمن السيبراني والذكاء الاصطناعي من الجامعات اليمنية الحكومية والأهلية، اختيروا بالطريقة القصدية.

وتوصل البحث إلى نتائج عديدة، أهمها: وجود توافق كبير لآراء الخبراء (أفراد العينة) حول متطلبات إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي، حيث بلغت نسبة التوافق (97%)، وهي نسبة مرتفعة على مستوى المجالات ككل، وبلغت نسبة التوافق على مستوى كل مجال كما يلي: بلغت للمتطلبات المالية (98%)، وبلغت للمتطلبات التقنية (97%)، وبلغت للمتطلبات التشريعية (96%)، وبلغت للمتطلبات البشرية (94%)، وخلص البحث إلى وضع تصور مقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية، ومنها جامعة صنعاء، ولضمان تحقيق النتائج المرجوة من البحث يوصي الباحثان بضرورة تبني وتطبيق التصور المقترح.

المقدمة:

يشهد العالم اليوم تحولات وتغيرات هائلة في مجالات الحياة كافة، بما فيها مجال المعلومات والتقنيات الحديثة، مما يفرض على مؤسسات التعليم، لا سيما مؤسسات التعليم العالي، تغييرات جذرية للحفاظ على التعليم الجيد وتوفيره، مثل: تجويد خدماتها ومخرجاتها، ورفد سوق العمل بكوادر بشرية متخصصة ومبدعة وقادرة على الاستجابة للتطورات الحاصلة، ومواكبة متطلبات عصر الثورة الذكية لتعزيز مكانتها التنافسية بين المؤسسات العالمية.

ويعد الذكاء الاصطناعي Artificial Intelligence (AI) وتقنياته من الاتجاهات التكنولوجية الحديثة، ومن أهم روافد الثورة الصناعية الرابعة، وهذه التقنية ستغير شكل التعليم في المستقبل، وقد ظهرت بشكل بارز كتطورات مهمة في تكنولوجيا التعليم (Educause, 2018)، إضافة إلى أنها ترتبط ارتباطًا وثيقًا بمستقبل التعليم العالي (Contact North, 2018, 5)، كما تعد من التقنيات التي حظيت مؤخرًا باهتمام كبير وواسع، حيث أصبحت جزءًا من نسيج الجامعات، وستؤثر موجة الاهتمام الحالية لتقنيَّات الذكاء الاصطناعي تأثيرًا كبيرًا على مؤسسات التعليم العالي (Popenici & Kerr,2017)؛ لذلك أصبحت تقنيات الذكاء الاصطناعي ميدانًا للتنافس لدى العديد من الجامعات العلمية والشركات التكنولوجية، التي تعمل على تنميتها والاستثمار في إمكاناتها.

وعلى نحو متصل يرتبط الأمن السيبراني Cyber Security (CS) بشكل كلي بالذكاء الاصطناعي، فاستخدام التقنيات الذكية الناشئة كالذكاء الاصطناعي في المؤسسات المختلفة، ومنها المؤسسات التعليمية، يتطلب أن تأخذ أمن المعلومات والأمن السيبراني بعين الاعتبار؛ لأن الأمن السيبراني يمثل الحصن الدفاعي الذي لا غنى عنه لحماية البنية التحتية الرقمية من الهجمات الإلكترونية المتطورة، وبذلك أصبح الأمن من أهم الخدمات التي تمثل ركيزة أساسية وقيمة مضافة للأنشطة الحكومية على مستوى المؤسسات والأفراد (كليبي، 2020)؛ لذلك تولي العديد من دول العالم اهتمامًا خاصًا بمفهوم الأمن السيبراني وتجعله كأولوية مهمة لصناع القرار في سياساتهم الأمنية والوطنية، حيث أعلنت أكثر من 130 دولة حول العالم عن سيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني، وخُصصت أقسام لها (البار والمرحبي، 2020، صـ2).

وانطلاقًا من أن التعليم الجامعي بجميع مستوياته ومجالاته يلعب دورًا حاسمًا في تطوير وتقدم المجتمع، كونه يسهم من خلال مؤسساته في ارتقاء الإنسان بفكره وقيمه ومهاراته ليصبح موردًا بشريًا مبدعًا، ومفكرًا، ومنتجًا لخدمة المجتمع والارتقاء به حضاريًا، مما يتطلب ضرورة تطويره بصفة مستمرة في ظل ما يشهده المجتمع من تحولات تكنولوجية رقمية (الدهشان، 2019)، كما تعد الدراسات العليا أحد مجالات وعناصر النظام الجامعي الأساسية، وجزءًا مهمًا يكمل رسالة الجامعة في أي مجتمع، ويمنحها تميزها وعراقتها في جميع الأوساط العلمية، من خلال إعداد كوادر من الأكاديميين والمتخصصين في مجالاتهم الدقيقة على وفق المعطيات الحديثة (الهاشمي، 2006).

ومع تزايد الطلب على الخبراء والمختصين في مجالي الأمن السيبراني والذكاء الاصطناعي للمساعدة في حماية المعلومات الحساسة وتطوير تقنيات متطورة، فقد سارعت العديد من الجامعات في معظم دول العالم، العربية منها والأجنبية، إلى تبني تلك التقنيات الحديثة وتوظيفها، والاستفادة من إمكاناتها، وأنشأت في سبيل ذلك برامج دراسات عليا متخصصة في تلك المجالات، سواء على مستوى الماجستير أو الدكتوراه، من منطلق أن إنشاء أو استحداث برامج دراسات عليا متخصصة أو تطويرها في تلك المجالات أصبح من المواضيع الغاية في الأهمية في العصر الحالي والمستقبلي.

وعلى المستوى المحلي، تبذل الجامعات اليمنية ولا سيما جامعة صنعاء جهودًا حثيثة لمواكبة التطورات التكنولوجية وتبني التقنيات المتطورة، فقد استحدثت في سبيل ذلك تخصصات في مجالات الأمن السيبراني والذكاء الاصطناعي على مستوى الدراسات الأولية (البكالوريوس)، إيمانًا منها بأهمية تلك التخصصات في مواجهة التهديدات الرقمية وتحقيق التقدم في القطاعات المختلفة.

وعلى الرغم من أهمية تلك الخطوات، فإن المراجعة الأولية لبرامج الدراسات العليا في الجامعات اليمنية ومنها جامعة صنعاء، تشير إلى أن برامج الذكاء الاصطناعي والأمن السيبراني لا تزال غائبة في تلك الجامعات، ولذلك فإن النقص في البرامج الأكاديمية المتخصصة في تلك المجالات سيؤدي حتمًا إلى ضعف إعداد الكوادر اليمنية المؤهلة والمتخصصة للعمل في هذه المجالات التقنية المتقدمة، مما سيؤثر سلبًا على قدرة اليمن على التعامل مع التحديات السيبرانية ودمج الذكاء الاصطناعي في القطاعات الاقتصادية والصناعية.

وعليه فإن إنشاء برامج دراسات عليا متخصصة في تلك المجالات أصبح أمرًا حيويًا وضروريًا لضمان إعداد كوادر علمية قادرة على مواجهة التحديات الحالية والمستقبلية، وتتماشى مع احتياجات سوق العمل المحلي والدولي، وتواكب التطورات التكنولوجية العالمية في هذه المجالات، ولذا برزت للباحثين فكرة البحث الحالي من خلال تقديم تصور مقترح لإنشاء برامج دراسات عليا في الجامعات اليمنية، يجمع بين الذكاء الاصطناعي والأمن السيبراني، من خلال تحديد التطورات التكنولوجية في AI والتهديدات السيبرانية، وتقديم برامج ومقررات أكاديمية تلبي احتياجات سوق العمل وتعزز الأبحاث التطبيقية.

وقد حرص الباحثان على إنشاء البرنامج الحالي بما يتوافق مع الخطة الاستراتيجية لجامعة صنعاء وخطط التنمية للدولة، ولوائح الدراسات العليا المعمول بها في الجامعة، إضافة إلى الإمكانات المادية والبشرية للجامعة، وبما يضمن مساهمته في تحسين مخرجات الجامعة، ومواكبة متطلبات واحتياجات سوق العمل الحالية والمستقبلية، مما يجعلها مؤهلة للاعتماد وإثراء المجتمع بالبرامج النوعية.

ويعد البحث الحالي الأول من نوعه على مستوى الجمهورية اليمنية على حد علم الباحثين، كما يأتي التصور المقترح الحالي كتجسيد لالتزام جامعة صنعاء المستمر بتحقيق التميز والابتكار في العملية التعليمية، وتعزيز جودة مخرجاتها التعليمية، والمؤمل أن يسهم في حال تبنيه من قبل الجهات المختصة في إنتاج خبراء ومختصين يجمعون بين المهارات التقنية

المتقدمة والفهم الاستراتيجي للتفاعل بين مجالي الأمن السيبراني والذكاء الاصطناعي.

مشكلة البحث وأسئلته:

في ضوء ما سبق، يمكن بلورة مشكلة البحث بالسؤال الرئيس الآتي: "**ما التصور المقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية –جامعة صنعاء أنموذجًا**"؟ وتنبثق منه الأسئلة الآتية:

[1] ما متطلبات إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية –جامعة صنعاء أنموذجًا؟

[2] ما التصور المقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية –جامعة صنعاء أنموذجًا؟

أهداف البحث:

سعى البحث إلى تحقيق الآتي:

[1] التعرف على متطلبات إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية –جامعة صنعاء أنموذجًا.

[2] إعداد تصور مقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية –جامعة صنعاء أنموذجًا.

أهمية البحث:

تتضح أهمية البحث في النقاط الآتية:

[1] يعد موضوع البحث من المواضيع البالغة الأهمية، لا سيما مع التطورات التكنولوجية المتسارعة وزيادة التهديدات الإلكترونية.

[2] الإضافة المعرفية التي يهدف هذا البحث إلى إضافتها إلى سلسلة الدراسات التي تلقي الضوء على الذكاء الاصطناعي واستراتيجيات الأمن السيبراني.

[3] يقدم هذا البحث برنامجًا مقترحًا قابلًا للتطبيق في البيئات الأكاديمية العربية، مع مراعاة السياق الثقافي والاقتصادي لليمن.

[4] قد يسهم هذا البحث في سد الفجوة بين مخرجات التعليم في جامعة صنعاء ومتطلبات الثورة الصناعية الرابعة، مما يعزز من مكانة الجامعة كمركز إقليمي للتميز في المجالات التقنية.

[5] البرنامج المقترح يركز على إضافة قيمة تكنولوجية وتنافسية لجامعة صنعاء محليًا وعالميًا.

[6] قد يسهم التصور المقترح في حال تبنيه من الجهات ذات العلاقة في رفد الجامعة والمجتمع وسوق العمل بكوادر أكاديمية متخصصة، تملك المهارات التي تحتاجها لمواجهة تحديات المستقبل.

[7] ندرة الدراسات والأبحاث العربية التي تناولت تقديم تصور مقترح لإنشاء برامج دراسات عليا تدمج بين الذكاء الاصطناعي والأمن السيبراني.

[8] يعد هذا البحث الأول من نوعه على مستوى الجمهورية اليمنية، بحسب علم الباحثين.

حدود البحث ومحدداته:

تتمثل إجراءات البحث ونتائجه في إطار الحدود الآتية:

[1] الموضوعية: إعداد تصور مقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.

[2] الزمانية والمكانية: طُبق هذا البحث في شهر نوفمبر من العام 2024م بجامعة صنعاء.

[3] البشرية: هم الخبراء المختصون في مجال الأمن السيبراني والذكاء الاصطناعي من الجامعات اليمنية الحكومية والأهلية.

التعريفات الاصطلاحية والإجرائية:

اشتمل البحث على المصطلحات الآتية:

- **التصور المقترح:** يعُرف أنه فكرة رائدة تهدف إلى قطف نتائج البحث الذي تم في الماضي والحاضر بتصور وضع جديد في المستقبل، فهو تخطيط مستقبلي بني على نتائج فعلية ميدانية، مرتكزًا على نتائج البحث، وتلافي أخطاء الواقع الذي تم البحث فيه، وقد يختلف من بحث إلى آخر بحسب الظاهرة المدروسة والهدف إلى رسمه الباحث لبحثة (العريفي، 2024، صـ250).

ويُعرف إجرائيًا أنه وضع تصور مستقبلي لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمينة.

- **الأمن السيبراني:** يُعرف أنه مجموعة من المهمات تتمثل في تجميع الوسائل والسياسات والإجراءات الأمنية والمبادئ التوجيهية والمقاربات لإدارة المخاطر والتدريبات والممارسات الآمنة، والتقنيات التي يمكن استخدامها في حماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين (Goutam & Verma, 2015, p24).

ويعرف إجرائيًا أنه الإجراءات والبرامج والتطبيقات التي توفرها الجامعات اليمنية لحماية أنظمتها وشبكاتها والمعلومات والبيانات المتوفرة لديها من الجرائم الإلكترونية بشتى أنواعها، ومنع الوصول غير المصرح به إلى هذه الشبكات والأنظمة.

- **الذكاء الاصطناعي:** هو أحد علوم الحاسب الآلي الحديثة التي تبحث عن أساليب متطورة للقيام بأعمال واستنتاجات تشابه ولو في حدود ضيقة تلك الأسباب، التي تنسب لذكاء الإنسان (مازن، 2009، صـ17).

ويعرف إجرائيًا أنه تطوير الآلات والحواسيب الرقميّة؛ بحيث تصبح لديها القدرة على القيام بمهمات تتطلب عمليات ذهنية تشابه وتحاكي تلك التي تقوم بها الكائنات الذكيّة، مثل: المقدرة على التفكير أو التعلُم.

الإطار النظري والدراسات السابقة

أولًا: الإطار النظري:

أ) السياق العالمي وأهمية التخصصات الرقمية الذكية:

أصبح الذكاء الاصطناعي (AI) والأمن السيبراني محورين رئيسيين في التحول الرقمي العالمي، حيث يعد الذكاء الاصطناعي جزءًا أساسيًا من العديد من التطبيقات والصناعات والقطاعات المختلفة، مثل: التعليم والرعاية الصحية والتمويل والتصنيع وغيرها، ومن ناحية أخرى، أصبح الأمن السيبراني ضروريًا لحماية الأنظمة والبيانات من الهجمات السيبرانية.

وتشير منظمة اليونسكو إلى أن 70% من الوظائف المستقبلية ستعتمد على المهارات الرقمية المتقدمة، وسيصل سوق الذكاء الاصطناعي إلى 190 مليار

دولار بحلول عام 2025 (Markets and Markets, 2020)، ومع ذلك تُشير البيانات والتقارير حول فجوة الكوادر في الأمن السيبراني الصادرة عن منظمة ISC² (2023) إلى وجود فجوة عالمية تقدر بـ3.4 مليون متخصص في الأمن السيبراني، كما تُظهر تقارير المنتدى الاقتصادي العالمي (World Economic Forum, 2023) أن الهجمات الإلكترونية تكلف العالم ما يقارب 8 تريليونات دولار سنويًا، مع توقعات بارتفاع هذا الرقم إلى 13 تريليون دولار بحلول 2030، مما يخلق حاجة ملحة إلى تأهيل كوادر قادرة على توظيف AI في تعزيز الأمن السيبراني، والعكس.

ب) دور الجامعات في تبني التقنيات الحديثة وتعزيز الأمن الرقمي:

تسعى المؤسسات التعليمية بجميع مستوياتها إلى تطبيق المبادئ والنظريات والابتكارات الجديدة في المجالات التعليمية والبحثية، سعيًا منها لرفع جودة مخرجاتها بما يتوافق ومتطلبات عصر الثورة الذكية وتعزيز مكانتها التنافسية بين المؤسسات العالمية.

وتعتبر الجامعات حجر الزاوية في بناء الكوادر المؤهلة لمواجهة التحديات التكنولوجية، من خلال تبني التقنيات والوسائل الحديثة ودمجها في عمليات التعلم والتعليم الجامعي، ومع الانتشار الواسع للتقنيات الحديثة، وما ترتب عليه من ظهور وانتشار كبير لاستخدام تطبيقات الذكاء الاصطناعي، وظهور التهديدات السيبرانية، سارعت العديد من الجامعات في معظم دول العالم إلى إحداث تغيرات جوهرية في برامجها ووظائفها وأساليب تقويمها، وإعادة النظر في سياسات التعليم وأنظمته واستراتيجياته ليواكب متطلبات العصر الحديث والتقنيات المتاحة، والحاجة إلى مهارات ومؤهلات جديدة في مخرجاته لتلبية احتياجات سوق العمل والاقتصاد الجديد (عباس، 2020؛ البشر، 2020).

وفي ظل الثورة التقنية الذكية تحرص الجامعات على حجز مكانها بين المؤسسات والأنظمة التعليمية الذكية، ومواكبة تحديات تقنية المعلومات واستثمارها بالشكل الأمثل لبناء مجتمع جامعي يتناسب ومجتمع المعرفة، والتحول إلى صيغ ونماذج جامعية حديثة أبرزها الجامعات الذكية، وتلبية متطلباتها ومقوماتها، من بنية تحتية مادية وتقنية، وكوادر بشرية ذكية، وبيئات تعلم وأبحاث علمية ذكية، وشبكة معرفة واسعة مع توافر خطط واستراتيجيات واضحة (بكرو، 2017).

ج) برامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي:

هي برامج أكاديمية تخصصية تدمج بين تقنيات الذكاء الاصطناعي والأمن السيبراني لتأهيل الطلبة بمهارات متقدمة تمكنهم من مواجهة التحديات الرقمية وتطوير حلول ذكية ومبتكرة، وتعتبر هذه البرامج من برامج الدراسات العليا الحديثة والضرورية لتلبية احتياجات السوق المتزايدة للمهارات التقنية المتقدمة، عن طريق توفير تعليم شامل ومتكامل، للمساهمة في إعداد خريجين مؤهلين لمواجهة التحديات المستقبلية في مجالاتهم، وتطوير حلول مبتكرة لمواجهة التهديدات المتزايدة في هذا المجال (جامعة الدوحة للعلوم والتكنولوجيا، https://www.udst.edu.qa).

1) أهداف برامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي:

تهدف برامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي في عدد من الجامعات، سواء العربية منها أو الأجنبية، إلى إكساب الطلبة المعرفة بأحدث الاتجاهات والتقنيات الناشئة، والمهارات اللازمة لمواجهة تحديات البيئة الرقمية وقيادة الأمن في المستقبل، وتزويدهم بالمهارات المعرفية والعملية والتقنية المتقدمة التي تؤهلهم للعمل في بيئات عمل تنافسية، وتأهيلهم ليصبحوا باحثين ذوي كفاءات عالية، قادرين على قيادة البحوث والتطوير والابتكار في هذا المجال، كما تهدف هذه البرامج إلى تلبية احتياجات سوق العمل من المتخصصين الذين يجمعون بين مهارات الذكاء الاصطناعي والأمن السيبراني، للإسهام في تطوير تقنيات جديدة تعزز من أمان المعلومات والأنظمة للمؤسسات ذات العلاقة في هذا المجال وخدمة المجتمع المحلي والإنسانية بوجه عام (جامعة الدوحة للعلوم والتكنولوجيا، https://www.udst.edu.qa؛ MIT University https://ocw.mit.edu؛ جامعة مؤتة، https://www.mutah.edu.jo)

2) أهمية برامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي:

تنبع أهمية برامج الدراسات العليا في الذكاء الاصطناعي والأمن السيبراني من أهمية التكامل بين هذين المجالين، كون ذلك يعد ضروريًا لتحقيق أقصى استفادة من هذه التقنيات، فالذكاء الاصطناعي والأمن السيبراني يشكلان تحدياتٍ وفرصًا متنوعة، حيث ترتبط القدرات المتزايدة للذكاء الاصطناعي بضرورة تعزيز الأمن السيبراني، كما يعتبر الحفاظ على البيانات والأنظمة الحيوية أمرًا أساسيًا لاستدامة التطور التكنولوجي، ومع الفوائد الكبيرة التي يقدمها الذكاء الاصطناعي، فإن التحديات المتعلقة بالأمن السيبراني تتطلب استراتيجيات متطورة لضمان استخدام تكنولوجيا الذكاء الاصطناعي بطريقة آمنة ومسؤولة في جميع القطاعات والمجتمعات، مما يظهر أن للذكاء الاصطناعي والأمن السيبراني العديد من التفاعلات المختلفة متعددة التخصصات.

ويمكن تطبيق تكنولوجيا الذكاء الاصطناعي كالتعلم العميق على الأمن السيبراني لبناء نماذج ذكية لتصنيف البرامج الضارة، واكتشاف التسلل، واستشعار التهديدات الذكية، وفي الوقت نفسه ستواجه نماذج الذكاء الاصطناعي مجموعة متنوعة من التهديدات السيبرانية، مما سيعطل عملية التعلم وصنع القرار وأخذ العينات.

ولمنع التهديدات والهجمات المضادة، والحفاظ على خصوصية التعلم الآلي، والتعلم الموحد الآمن، وغيرها، يتطلب تحليل سمات تلك الهجمات العدائية، وتصنيف استراتيجيات وتقنيات متخصصة في الدفاع والحماية في مجال الأمن السيبراني باستخدام الذكاء الاصطناعي، وحلول التعلم العميق الراسخة، وتقنيات التعلم الآلي التقليدية، لتطوير أنظمة الذكاء الاصطناعي الآمنة، والتركيز على جوانب بناء شبكات عصبية مشفرة وتنفيذ التعلم العميق الموحد الآمن (Li, 2018).

وبناء على تلك الأهمية، نجد أن العديد من الجامعات في دول العالم المختلفة قد سارعت إلى العمل على تطوير أو استحداث برامج دراسات عليا متخصصة تدمج بين الذكاء الاصطناعي كأداة للابتكار والأمن

السيبراني كضرورة لحماية البنى التحتية الرقمية، ولتزويد الأجيال القادمة من المهنيين والعلماء بالمعرفة المتعمقة والمهارات المتقدمة التي تواكب التطورات الحاصلة في هذه المجالات، فالحاجة إلى هذه البرامج لا تقتصر على جانب الأمان فحسب، بل تمتد لتشمل تطوير تقنيات ذكاء اصطناعي مبتكرة وآمنة، تسهم في تعزيز الابتكار، إضافة إلى إسهام هذه البرامج في إعداد خريجين مؤهلين لمواجهة التحديات المستقبلية وتلبية احتياجات السوق المتزايدة للمهارات التقنية المتقدمة، وتحقيق التنمية المستدامة في مختلف الصناعات.

3) نماذج عالمية وعربية لبرامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي:

جدول (1): نماذج برامج الدراسات العليا في الأمن السيبراني:

الجامعةUniversity	وصف البرنامج
Carnegie Mellon (U.S)	يركز البرنامج على عدة مقررات، مثل: أمن أنظمة الذكاء الاصطناعي، وأمن الشبكات المتقدمة، ومنهج يركز على التدريب العملي من خلال مختبرات محاكاة الهجمات الإلكترونية. https://www.ri.cmu.ed
Stanford (U.S)	برنامج يقدم من خلاله مقررات في علوم الحاسوب مع التركيز على الذكاء الاصطناعي والرؤية الحاسوبية. https://www.stanford.edu
George Washington (أمريكا)	يتضمن البرنامج مقررات في أمن الشبكات، التشفير، والأمن السيبراني المادي. https://www.gwu.edu
الأمير سطام بن عبد العزيز (السعودية)	يشمل البرنامج دراسة لمفاهيم التهديدات السيبرانية وتقنيات الاختراق والدفاع السيبراني، وتأمين الشبكات والأنظمة، وإدارة الحوادث السيبرانية، وحماية البيانات والخصوصية، واستراتيجيات التحليل والتحقق الرقمي، كما يتضمن دروسًا نظرية وتجارب عملية ومشاريع بحثية. https://www.psau.edu.sa
الأميرة سمية للتكنولوجيا (الأردن)	يشمل البرنامج مقررات في التشفير المتقدم، وتحقيقات الأدلة الجنائية، وأمن الشبكات المتقدم، والقدرات والمهارات العلمية والنظرية والفنية للتعامل مع المخاطر التي تواجهها المؤسسات والشركات بسرية وأمن أنظمة المعلومات الخاصة بها، وشبكات المعلومات وما يواجهها من جرائم معلوماتية. https://www.psut.edu.jo
حمد بن خليفة (قطر)	يركز البرنامج على القضايا المتعلقة بأمان الشبكات وأنظمة الحوسبة، ويشمل مقررات متقدمة في التشفير والتحقيقات الرقمية. https://www.hbku.edu.qa

جدول (2): نماذج برامج الدراسات العليا في الذكاء الاصطناعي:

الجامعةUniversity	وصف البرنامج
Texas at Austin (U.S)	يغطي البرنامج عدة مواضيع، مثل: الأخلاقيات في الذكاء الاصطناعي، والتعلم العميق، ونماذج البيانات، ويتطلب إكمال 30 ساعة معتمدة. https://www.utexas.edu

Duke (U.S)	يتضمن البرنامج مقررات أساسية في الذكاء الاصطناعي، والتعلم الآلي، والرؤية الحاسوبية، إضافة إلى خيارات تخصصية في بعض المجالات، مثل: الروبوتات والتفاعل الذكي. https://www.duke.edu
Purdue (U.S)	يوفر البرنامج معرفة أساسية بالذكاء الاصطناعي، قابلة للتطبيق في العديد من المسارات المهنية المختلفة كالهندسة والأعمال والاتصالات وغيرها، كما يقدم أساسيات الذكاء الاصطناعي متعدد التخصصات، وسياسة الذكاء الاصطناعي والحوكمة والأخلاقيات، والتأثيرات المجتمعية للذكاء الاصطناعي، وأساسيات الذكاء الاصطناعي: مقدمة غير تقنية. https://www.purdue.edu
الإمام محمد بن سعود (السعودية)	برنامج أكاديمي يركز على تقديم عدة المقررات، مثل: التعلم الآلي، والتعلم العميق، ومعالجة اللغة الطبيعية، وتحليل ومعالجة البيانات الضخمة. ccis@imamu.edu.sa
اليرموك (الأردن)	يركّز البرنامج على عدة حقول نشطة، مثل: تعلم الآلة، ومعالجة اللغات الطبيعية، والخوارزميات، والذكاء الحسابي، والتعرف على الكلام، والواجهات الذكية، والروبوتات. it.fac@yu.edu.jo

جدول (3): نماذج برامج الدراسات العليا تدمج بين الأمن السيبراني والذكاء الاصطناعي:

الجامعةUniversity	وصف البرنامج
MIT Stephen A. Schwarzman (U.S)	يوفر البرنامج عدة مقررات، مثل: الذكاء الاصطناعي التطبيقي، وأمن الأنظمة الموزعة، والتعلم العميق. https://ocw.mit.edu
الدوحة للعلوم والتكنولوجيا (قطر)	برنامج يمزج بين الدورات الأساسية في الذكاء الاصطناعي والأمن السيبراني والحوسبة المعرفية، مما يوفر فهمًا شاملًا وتكامليًا لهذه المجالات المهمة، ويكتسب الطلبة القدرة على مواجهة المخاطر والتهديدات السيبرانية المعقدة من خلال الفهم العميق لنظريات الذكاء الاصطناعي ومبادئ الأمان المتقدمة والممارسات المبتكرة. https://www.udst.edu.qa
مؤتة (الأردن)	برنامج يدمج بين تقنيات الذكاء الاصطناعي والأمن السيبراني لتأهيل الطلاب بمهارات متقدمة تمكنهم من مواجهة التحديات الرقمية وتطوير حلول مبتكرة. https://www.mutah.edu.jo
الخليج العربي (البحرين)	يقدم البرنامج أحدث التقنيات والأساليب التي تمكّن من التأكد من عدم وجود ثغرات أمنية في العديد من المنظومات الحيويّة الحسّاسة، وبناء أنظمة وبروتوكولات اتصالات عالية الأمان، وبحث سبل توظيف آخر تقنيات الذكاء الاصطناعي التي تمكّن من فهم وتعلّم طريقة تفكير قراصنة الإنترنت، واكتشاف ما يهدّد الأمن السيبراني بصورة استباقية مع التقليص بصفة كبيرة من إنذارات الاقتحام الكاذبة. agu_aru@agu.edu.bh
الجامعة التكنولوجية tech	يوفر البرنامج منهجًا لقيادة تخطيط وتنفيذ ومراقبة الاستراتيجيات الأمنية، وتخفيف المخاطر والاستجابة بفعالية للهجمات والحوادث الإلكترونية، وتصميم السياسات

	الأمنية وإدارة المخاطر التكنولوجية وقيادة الفرق المتخصصة في مواجهة التحديات الناشئة عن التقدم التكنولوجي والرقمنة. https://www.techtitute.com

ثانيًا: الدراسات السابقة:

-دراسة (الرمبيان، 2024): هدفت إلى مقارنة توظيف الذكاء الاصطناعي في برامج الدراسات العليا في كل من الولايات المتحدة الأمريكية والصين، ومدى إمكانية الإفادة منها في المملكة العربية السعودية من خلال التعرف على الأطر النظرية لتوظيف الذكاء الاصطناعي في برامج الدراسات العليا في تلك الدول في ضوء القوى والعوامل المؤثرة فيها، والإفادة منها في المملكة، واتبعت المنهج التحليلي المقارن "لجورج بيردي" ذا الخطوات الأربع، وهي: الوصف والتفسير والموازنة والمقارنة، لدراسة توظيف الذكاء الاصطناعي في برامج الدراسات العليا في الولايات المتحدة الأمريكية والصين في ضوء عوامل عديدة، منها: العوامل السياسية، والعوامل الاقتصادية، والعوامل الاجتماعية، والعوامل الثقافية، والعوامل الجغرافية، وتحديد أوجه التشابه والاختلاف في توظيف الذكاء الاصطناعي بين دول المقارنة، وقد قدمت الدراسة مقترحات وتوصيات يمكن الإفادة من خبرات الولايات المتحدة الأمريكية والصين وتجربتهما في توظيف الذكاء الاصطناعي في المملكة العربية السعودية.

-دراسة (قصقصي، 2024): هدفت إلى التعرف على مقترحات تفعيل الذكاء الاصطناعي في الجامعات داخل الخط الأخضر من وجهة نظر أعضاء هيئة التدريس، واتبعت المنهج النوعي، وتكونت العينة من (20) عضو هيئة تدريس من الجامعات داخل الخط الأخضر، واعتمدت على المقابلات في جمع البيانات، وأظهرت نتائج هذه المقابلات أن أعضاء هيئة التدريس قدموا خمسة مقترحات شملت ما يلي: الاهتمام بتدريب الطلبة على إعداد الأبحاث والمشاريع القائمة على مشكلات المجتمع كل بحسب مرحلته الأكاديمية، وحث العاملين في الجامعات على تقبل التغيير التقني وتفعيله في وظائفهم الإدارية والأكاديمية، وتعزيز الجامعات للدور الذي يقوم به عضو هيئة التدريس المناسب للإنجاز الذي يحققه أثناء تحقيق الأهداف، وقيام الجامعات بالتواصل بشكل فعال مع الطلبة والعاملين ذوي الصلة ضمن المنصات الإلكترونية الفعالة التي من السهولة استخدامها وتداولها.

-دراسة (حربا وشعبان، 2024): هدفت إلى تقديم تصور مقترح لاستخدام تطبيقات الذكاء الاصطناعي في التعليم العالي، واتبعت المنهج الوصفي، وتكونت العينة من (25) عضوًا من أعضاء هيئة التدريس، و(15) طالبًا من طلبة الدراسات العليا بكلية التربية بجامعة حماة، واعتمدت على الاستبانة في جمع البيانات، وتوصلت إلى أن هناك حاجة إلى استخدام تطبيقات الذكاء الاصطناعي بدرجة كبيرة جدًا بوزن نسبي (84%)، وهذه الحاجة تتمحور حول خمسة مجالات هي: التقويم، ودراسة نظرية حول الذكاء الاصطناعي، والتعليم الجامعي، والبحث العلمي، والمشاركة المجتمعية، وفي ضوء ذلك قدمت الدراسة تصورًا مقترحًا لاستخدام تطبيقات الذكاء الاصطناعي في التعليم العالي في ظل تلك الاحتياجات.

-دراسة (البلوشية وآخرون، 2024): هدفت إلى التعرف على متطلبات تحقيق الأمن السيبراني بجامعة نزوى في ضوء رؤية عمان 2040 وعوائقه من وجهة نظر أكاديمي الجامعة وموظفيها، واتبعت المنهج الوصفي التحليلي المسحي، وتكونت العينة من (186) أكاديميًا وموظفًا، واعتمدت على الاستبانة في جمع البيانات، وأظهرت النتائج أن درجة متطلبات تحقيق الأمن السيبراني في جامعة نزوى من وجهة أكاديمي الجامعة وموظفيها جاءت منخفضة، حيث جاءت المتطلبات التقنية في المرتبة الأولى، وجاءت المتطلبات المعرفية في المرتبة الثانية، وجاءت المتطلبات البشرية في المرتبة الثالثة، وفي الأخير جاءت المتطلبات المادية، كما أن درجة عوائق تحقيق الأمن السيبراني في جامعة نزوى على وفق رؤية عمان 2040 من وجهة أكاديمي جامعة نزوى وموظفيها جاءت متوسطة، وأوصت الدراسة بالاستمرار في توفير متطلبات تحقيق الأمن السيبراني في جامعة نزوى وتدريب الأكاديميين والموظفين لمواكبة المستجدات التكنولوجية، والتصدي لتطور أنواع الهجمات الإلكترونية.

- دراسة (جبران والمساجدي، 2023): هدفت إلى تقديم تصور مقترح لتطبيق الذكاء الاصطناعي في الجامعات اليمنية من وجهة نظر الخبراء المختصين، واتبعت المنهج الوصفي التحليلي، وتكونت العينة من (32) خبيرًا من الجامعات اليمنية الحكومية والأهلية، اختيروا بطريقة العينة القصدية، واعتمدت على الاستبانة لمعرفة آراء الخبراء وجمع البيانات، وأظهرت النتائج أن هناك توافقًا لآراء الخبراء حول تطبيق متطلبات أبعاد الذكاء الاصطناعي (المتطلبات التشريعية والتنظيمية، المتطلبات البشرية، المتطلبات التقنية، المتطلبات المالية، المتطلبات الأخلاقية)، حيث بلغت نسبة التوافق (96%)، وهي نسبة مرتفعة، وبلغت نسبة التوافق على مستوى كل بعد كما يلي: بلغت نسبة بعد "المتطلبات الأخلاقية" (99%)، وبلغت نسبة بعد "المتطلبات التقنية" (97%)، وبلغت نسبة بعد "المتطلبات البشرية" وبعد "المتطلبات المالية" (96%) لكل منهما، وبلغت نسبة بعد "المتطلبات التشريعية والتنظيمية" (94%)، وأوصت الدراسة بضرورة تبني وتطبيق التصور المقترح لتطبيق الذكاء الاصطناعي في الجامعات اليمنية.

- دراسة (الخميسي والحاوري، 2023): هدفت إلى معرفة متطلبات الثورة الصناعية الرابعة ومواكبتها، والاستفادة من كل ذلك في بناء تصور مقترح لإنشاء مركز للذكاء الاصطناعي بوزارة التربية والتعليم بالجمهورية اليمنية، واتبعت المنهج الوصفي التحليلي، وتكونت العينة من (19) خبيرًا في مجال الدراسة من أصل (37) خبيرًا من مجتمع الدراسة، واعتمدت على الاستبانة في جمع البيانات والمعلومات، وتوصلت إلى مدى أهمية إنشاء مركز للذكاء الاصطناعي لنقل العملية التعليمية إلى ما يواكب الثورة الصناعية الرابعة، لا سيما أنه لا يوجد مركز تابع لوزارة التربية والتعليم في اليمن، كما خلصت إلى تقديم تصور مقترح لإنشاء مركز للذكاء الاصطناعي بوزارة التربية والتعليم يتضمن الرؤية، والرسالة، والأهداف، والمهام، والهيكل التنظيمي، وكذا مهام كل وحدة داخل المركز، وذلك في ضوء متطلبات الثورة الصناعية الرابعة.

-دراسة (زقوت والسائح والعطاب، 2022): هدفت إلى معرفة درجة وعي أعضاء هيئة التدريس

بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي، وتحديدًا في جامعة الزاوية، واتبعت المنهج الوصفي التحليلي، وتكونت العينة من (138) عضوًا من هيئة التدريس بالجامعة، واعتمدت على الاستبانة أداة في جمع البيانات، وأظهرت النتائج وجود وعي بنسبة كبيرة من قبل أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي، وقدمت الدراسة مجموعة من التوصيات، أبرزها: عقد دورات تدريبية لأعضاء هيئة التدريس في الأمن السيبراني وإدراج مجال الأمن السيبراني ضمن مناهج التعليم في المدارس والجامعات، إضافة إلى تشجيع أبحاث ودراسات الأمن السيبراني في الدراسات العليا.

-**دراسة (السمحان، 2022):** هدفت إلى معرفة متطلبات الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، واتبعت المنهج الوصفي، وتكونت العينة (478) فردًا، واعتمدت على الاستبانة في جمع البيانات، وأظهرت النتائج أن هناك سياسات أمنية لأنظمة المعلومات الإدارية بالجامعة، وأن هناك تطبيقًا لإجراءات إدارية من أجل حماية الأنظمة، وأن هناك خططًا لإدارة المخاطر الإلكترونية، وأن الجامعة تحدث برامج الحماية وتطبق متطلبات الأمن السيبراني في تعريف هوية الدخول والصلاحيات، وأن هناك أنظمة حماية تقنية وحاسوبية بالجامعة، وأن الجامعة تقدم الدعم الفني اللازم لتطبيق الأمن السيبراني وتقوم بتوعية الموظفين بمتطلبات الأمن السيبراني وتطبيقاته، وأن الجامعة تمتلك نظام حماية عالي المستوى وتتوفر الأجهزة التقنية اللازمة لتوفير الحماية.

-**دراسة (الدحياني والصنوي، 2021):** هدفت إلى التعرف على متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر المختصين، واتبعت المنهج الوصفي المسحي، وتكونت العينة من (70) مختصًا في مجال الحاسوب والتقنيات والذكاء الاصطناعي، واعتمدت على الاستبانة في جمع البيانات، وأظهرت النتائج أن درجة الموافقة على متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر المختصين كانت عالية جدًا، على مستوى الأداة ككل وعلى مستوى كل مجال من مجالات الدراسة.

-**دراسة (Ocaña et al. 2019):** هدفت إلى التعرف على الذكاء الاصطناعي وآثاره على التعليم العالي في دولة البيرو، واتبعت المنهج الوصفي التحليلي، واعتمدت على الاستبانة في جمع البيانات، وتوصلت إلى عدد من النتائج، أهمها: أن التقنيات المختلفة القائمة على الذكاء الاصطناعي لها دور كبير وإيجابي في عملية تحسين تعلم الطلاب في المستويات التعليمية كافة، ولا سيما إذا زُود المتعلمون بالدعم الدقيق والمخصص بحسب احتياجاتهم التعليمية، كما أظهرت أن من أبرز التحديات التي تواجهها الجامعات في العصر الحالي هو حاجتها إلى تخطيط وتطوير المهارات الرقمية لتمكين وتدريب مهنيين قادرين على استيعاب متطلبات البيئة الرقمية وتطويرها طبقًا لمتطلباتهم.

التعقيب على الدراسات السابقة:

من خلال الاطلاع على الدراسات السابقة الواردة في البحث الحالي، يمكن القول بأن الذكاء الاصطناعي والأمن السيبراني يعدان القاسم المشترك الأبرز بين

البحث الحالي وتلك الدراسات، وتعد دراسة (الرمبيان، 2024)، ودراسة (حربا وشعبان، 2024) ودراسة (جبران والمساجدي، 2023) الدراسات الأقرب إلى موضوع البحث الحالي، وذلك أن كل واحدة منها حاولت إعداد تصور أو سبل مقترحة لتوظيف الذكاء الاصطناعي وتطوير أداء مؤسسات التعليم العالي، ولذلك يتشابه البحث الحالي أو يختلف عنها وعن بقية الدراسات في عدد من النقاط، نوضحها فيما يلي:

- **من حيث الهدف العام:** يتفق البحث الحالي مع أغلب الدراسات السابقة في الهدف العام، من حيث تناوله للأمن السيبراني والذكاء الاصطناعي، ولكنه يختلف مع تلك الدراسات السابقة، في كونه جمع بين متغيري الأمن السيبراني والذكاء الاصطناعي في الوقت نفسه.
- **من حيث المنهج:** يتفق البحث الحالي مع أغلب الدراسات السابقة في توظيفه للمنهج الوصفي المسحي التحليلي، كدراسات (البلوشية وآخرون، 2024؛ جبران والمساجدي، 2023؛ زقوت وآخرون، 2022؛ الخميسي والحاوري، 2023؛ الدحياني والصنوي، 2021؛ Ocaña et al. 2019)، ولكنه يختلف مع دراسة (الرمبيان، 2024) التي استخدمت المنهج التحليلي المقارن، ودراسة (قصقصي، 2024) التي استخدمت المنهج النوعي، ودراستي (السمحان، 2022؛ الدحياني والصنوي، 2021) اللتين استخدمتا المنهج الوصفي.
- **من حيث نوع العينة:** يتفق البحث الحالي مع معظم الدراسات السابقة في نوع العينة التي تمثلت في أعضاء هيئة التدريس بالجامعة، ولكنه يختلف مع دراسة (البلوشية وآخرون، 2024؛ السمحان، 2022) في إضافة الموظفين والإداريين بالجامعة إلى عينتها، ودراسة (حربا وشعبان، 2024) التي جمعت أعضاء هيئة التدريس والطلبة.
- **من حيث أداة الدراسة:** يتفق البحث الحالي مع أغلب الدراسات السابقة في اعتماده على الاستبانة أداة رئيسة في جمع البيانات، ولكنه يختلف مع دراسة (قصقصي، 2024) التي اعتمدت على المقابلة.
- **من حيث المرحلة التعليمية:** يتفق البحث الحالي مع جميع الدراسات السابقة في التطبيق على المؤسسات التعليمية في التعليم الجامعي.
- **أوجه الاستفادة:** بوجه عام يمكن إيجاز الفوائد التي قدمتها الدراسات السابقة على النحو الآتي:

- قدمت دراسات (حربا وشعبان، 2024؛ جبران والمساجدي، 2023؛ الخميسي والحاوري، 2023؛) للبحث الحالي فوائد عديدة تتعلق بكيفية إعداد وبناء التصورات المقترحة.

- ساعدت دراسة (الرمبيان، 2024؛ البلوشية وآخرين، 2024؛ جبران والمساجدي، 2023؛ السمحان، 2022؛ الدحياني والصنوي، 2021) الباحثين في إعداد استبانة بحثهما الحالي، فقد اعتمدا على تلك الدراسات في كتابة بنود الاستبانة ومحاورها.

- ركزت الدراسات السابقة على تحليل مضمون نتائج الأدب التربوي والمقالات النظرية المنشورة، مثل: (الرمبيان، 2024؛ قصقصي، 2024؛ Ocaña et al. 2019؛ زقوت وآخرون، 2022)، الأمر الذي وفر للباحثين قاعدة معرفية يمكن البناء عليها، وتوظيفها في البحث الحالي.

- سلطت معظم الدراسات السابقة الضوء على مخاطر الذكاء الاصطناعي أو الأمن السيبراني وعوائقهما

وصعوبات تطبيقهما، مما ساعد على الإفادة من هذه الأفكار وتوظيفها وإعادة صياغتها في البحث الحالي.

- استفاد البحث الحالي بشكل كبير من أغلب الدراسات السابقة في الإطار المنهجي للبحث، إضافة إلى الاستفادة منها في استخدام المعالجات الإحصائية المناسبة.

وما يميز البحث الحالي عن الدراسات السابقة هو أنه ركز على إنشاء برامج دراسات عليا في الجامعات، وجمع بين متغيري الأمن السيبراني والذكاء الاصطناعي، وهو ما لم يتوفر في تلك الدراسات، إضافة إلى أنه يعد الأول من نوعه –بحسب علم الباحثين– على مستوى الجمهورية اليمنية.

منهجية البحث وإجراءاته

منهج البحث:

استخدم البحث المنهج الوصفي بشقيه التحليلي والمسحي، كونه المنهج المناسب لهذا الغرض، فهو يعتمد على جمع البيانات عن واقع الظاهرة المراد دراستها وتحليلها وتنظيمها بصورة كمية ونوعية، واستخراج الاستنتاجات والتعميمات التي تساعد على فهم الظاهرة المطروحة للبحث، وذلك من خلال مراجعة الأدب النظري والدراسات السابقة ذات الصلة بالبحث والدراسة الميدانية (الاستبانة)، لمعرفة متطلبات إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية من وجهة نظر الخبراء، واستطلاع آراء بعض الطلبة المحتملين حول احتياجاتهم وتوقعاتهم، واستشارة خبراء في المجال الأكاديمي والمختصين في الذكاء الاصطناعي والأمن السيبراني، وتحليل برامج الدراسات العليا المناظرة، وتحليل البيانات الثانوية (تقارير دولية عن اتجاهات الذكاء الاصطناعي والأمن السيبراني)، وتحليل إحصائيات عن فجوة المهارات في سوق العمل العالمي، وحاجة السوق المحلية.

مجتمع البحث وعينته:

تكون مجتمع البحث وعينته من الخبراء المختصين ذوي الخبرة الطويلة والمعرفة الاختصاصية العميقة، من ذوي الدرجة العلمية (أستاذ – أستاذ مشارك)، ومن الأكاديميين المهتمين بتطوير التعليم الجامعي، والمختصين في الذكاء الاصطناعي ونظم المعلومات الذكية، وبرمجة الحاسوب، وتكنولوجيا المعلومات، وتقنية المعلومات IT، والإدارة والتخطيط، واختيرت عينة قصدية من الجامعات اليمنية الحكومية والأهلية، حيث بلغت عينة الخبراء (18) خبيرًا.

أداة البحث:

من أجل تحقيق أهداف البحث، أعد الباحثان استبانة بالاستفادة من أدبيات الدراسة والدراسات السابقة، لمعرفة آراء الخبراء، وقد تضمنت أداة البحث أربعة مجالات هي: (المتطلبات التشريعية والتنظيمية، والمتطلبات البشرية، والمتطلبات التقنية، والمتطلبات المالية)، وقد أُعطيت كل فقرة من فقرات الاستبانة وزنًا متدرجًا طبقًا لسلم ليكرت الثلاثي، حيث أُعطي الوزن (3) للاستجابة "موافق"، والوزن (2) للاستجابة "موافق إلى حدٍ ما"، والوزن (1) للاستجابة "غير موافق"، ولغرض بناء البرنامج الحالي أجرى الباحثان استطلاعًا أوليًا لآراء الطلبة المحتمل التحاقهم بالبرنامج، والوقوف على احتياجات الأطراف ذات العلاقة، وتحليل البرامج المناظرة من جامعات عربية

وعالمية، واستشارة بعض الخبراء والمختصين حول البرنامج ومكوناته.

صدق أداة البحث وثباتها:

أ) صدق الأداة:

- **الصدق الظاهري:** تحقق الباحثان من الصدق الظاهري للأداة بعرضها على مجموعة من ذوي الخبرة والكفاءة من المختصين، حيث طُلب منهم إبداء الرأي حول فقرات الاستبانة من حيث مدى وضوحها، وسلامتها، ودقة صياغتها اللغوية، إضافة إلى مدى ملاءمتها للمجال الذي تندرج تحته، وقد أُخذت جميع ملاحظات المحكمين لإعداد الاستبانة في صيغتها النهائية.
- **صدق الاتساق الداخلي:** حسب الباحثان معاملات ارتباط بيرسون بين درجة كل فقرة والدرجة الكلية للمحور الذي تنتمي إليه ودرجة أداة البحث ككل، والجدول (4) يوضح ذلك.

جدول (4): معامل ارتباط بيرسون لمجالات الأداة والدرجة الكلية:

المجال	الفقرات	معامل الارتباط
المتطلبات التشريعية لتطبيق الأمن السيبراني والذكاء الاصطناعي	7	0.89
المتطلبات البشرية لتطبيق الأمن السيبراني والذكاء الاصطناعي	6	0.88
المتطلبات التقنية لتطبيق الأمن السيبراني والذكاء الاصطناعي	7	0.84
المتطلبات المالية لتطبيق الأمن السيبراني والذكاء الاصطناعي	8	0.86
الأداة ككل	**28**	**86**

يلاحظ من الجدول (4) أن قيمة معامل الارتباط تتراوح بين (0.84) و(0.89)، وهي دالة إحصائيًا عند مستوى (0.05)، مما يشير إلى قوة الارتباط الداخلي لجميع فقرات الاستبانة، وهذا مؤشر على صلاحية الاستبانة للتطبيق.

ب) الثبات: استخرج الباحثان معامل الثبات للأداة ككل ومحاورها باستخدام معادلة ألفا كرونباخ، حيث تراوحت معاملات الثبات بين (−0.84) و(0.96)، وهي قيم مرتفعة ومناسبة لغايات البحث، والجدول (5) يوضح ذلك.

جدول (5): معامل الثبات باستخدام ألفا كرونباخ لمحاور الأداة والدرجة الكلية:

م	المحاور	درجة الثبات
1	المتطلبات التشريعية لتطبيق الأمن السيبراني والذكاء الاصطناعي	0.84
2	المتطلبات البشرية لتطبيق الأمن السيبراني والذكاء الاصطناعي	0.95
3	المتطلبات التقنية لتطبيق الأمن السيبراني والذكاء الاصطناعي	0.94
4	المتطلبات المالية لتطبيق الأمن السيبراني والذكاء الاصطناعي	0.92
	الاستبانة ككل	0.96

المعالجات الإحصائية:

فُرغت استجابات أفراد العينة ورُمزت وعُولجت بالطرق الإحصائية المناسبة باستخدام برنامج الرزمة الإحصائية للعلوم الاجتماعية (SPSS)، حيث

استخدمت التكرارات (Frequencies)، والنسب المئوية (Valid Percent)، ومعامل ارتباط بيرسون (Pearson)، ومعامل ألفا كرونباخ (Cronbach's Alpha)، والمتوسطات الحسابية (Mean)، والانحرافات المعيارية (Standard Deviation).

إجراءات التصحيح:

لتحديد معيار الاستجابة، حُسب المدى بين الدرجات على النحو الآتي:

المدى= الفرق بين أعلى درجة وأقل درجة=3-1=2، وقُسم المدى على المقياس الثلاثي بالطريقة الآتية: **طول الفئة = المدى ÷ عدد الفئات=2÷3= 0.66**، وبعد ذلك أضيفت هذه القيمة إلى أقل قيمة في المقياس (الواحد الصحيح)، وهكذا أصبح طول الخلايا/المستويات (الحدود الحقيقية لقياس المتوسط الحسابي) على النحو المبين في الجدول (6).

جدول (6): الحدود الحقيقية لقياس المتوسط الحسابي لمجالات الأداة:

الدرجة	الحدود الحقيقية	الوزن النسبي	التقدير اللفظي
1	1.66-1	%55.5 >	غير موافق
2	2.33-1.67	%78-55.5	موافق إلى حد ما
3	3-2.34	%78 <	موافق

نتائج البحث ومناقشتها

هدف البحث الحالي إلى تقديم تصور مقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي بجامعة صنعاء، ولتحقيق أهداف البحث والإجابة عن أسئلته، طور الباحثان استبانة وتأكدا من صدقها وثباتها، وبعد عملية جمع الاستبانات رُمزت وأُدخلت للحاسوب وعُولجت إحصائيًا باستخدام الرزمة الإحصائية للعلوم الاجتماعية (SPSS)، وفيما يلي نتائج البحث تبعًا لتسلسل أسئلته:

[1] النتائج المتعلقة بسؤال البحث الأول الذي ينص على الآتي: "ما متطلبات إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية"؟

أُجيب عن هذا السؤال من خلال حساب المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لتقديرات آراء الخبراء، ورُتبت المجالات والفقرات بحسب كل بُعد، كما هو موضح في الجدول (7).

جدول (7): المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لمعرفة آراء أفراد العينة على مستوى مجالات متطلبات الأمن السيبراني والذكاء الاصطناعي ككل:

المجال	المتوسط الحسابي	الانحراف المعياري	الترتيب	الوزن النسبي
المتطلبات المالية لتطبيق الأمن السيبراني والذكاء الاصطناعي	2.85	0.43	1	0.98
المتطلبات التقنية لتطبيق الأمن السيبراني والذكاء الاصطناعي	2.84	0.46	2	0.97

المتطلبات التشريعية لتطبيق الأمن السيبراني والذكاء الاصطناعي	2.83	0.54	3	0.96
المتطلبات البشرية لتطبيق الأمن السيبراني والذكاء الاصطناعي	2.81	0.61	4	0.94
ككل	2.83	0.51	-	0.97

يتضح من الجدول (7) أن المتوسط العام لجميع مجالات متطلبات الأمن السيبراني والذكاء الاصطناعي بلغ (2.83)، والانحراف المعياري بلغ (0.51)، والوزن النسبي بلغ (97%)، وهذا يدل على توافق آراء أفراد العينة على مجالات متطلبات الذكاء الاصطناعي، وقبول كل المجالات كمتطلبات لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في جامعة صنعاء، حيث حصل مجال (المتطلبات المالية لتطبيق الأمن السيبراني والذكاء الاصطناعي) على أعلى متوسط حسابي بلغ (2.85)، وانحراف معياري بلغ (0.43)، في حين حصل مجال (المتطلبات التقنية لتطبيق الأمن السيبراني والذكاء الاصطناعي) على المرتبة الثانية بمتوسط حسابي بلغ (2.84)، وانحراف معياري بلغ (6)، ويرى الباحثان أن هذه النتيجة طبيعية؛ نظرًا لأن إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي، يحتاج إلى إمكانات وتوفير موارد مالية، وفي حال توفر ذلك يمكن توفير المتطلبات التقنية، وحصل مجال (المتطلبات التشريعية لتطبيق الأمن السيبراني والذكاء الاصطناعي) على المرتبة الثالثة بمتوسط حسابي بلغ (2.83)، وانحراف معياري بلغ (0.54)، في حين حصل مجال (المتطلبات البشرية لتطبيق الأمن السيبراني والذكاء الاصطناعي) على أدنى متوسط حسابي بلغ (2.81)، وانحراف معياري بلغ (0.61)، ويرى الباحثان أن هذه النتيجة طبيعية؛ نظرًا لتوفر العنصر البشري والكوادر الأكاديمية المؤهلة والقادرة على العمل في مجال الأمن السيبراني والذكاء الاصطناعي بجامعة صنعاء.

ويمكن القول بأن هذه النتيجة تشير إلى وعي الخبراء بأهمية إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في جامعة صنعاء؛ إذ أصبح مطلبًا مهمًا وأساسيًا، كونه يُسهم في تطوير العملية التعليمية في الجامعة، ويحقق التنافسية للجامعات ومواكبة تقنية العصر، وتتفق هذه النتيجة مع دراسة (حربا وشعبان، 2024) التي أظهرت الحاجة الكبيرة إلى دمج تطبيقات الذكاء الاصطناعي في التعليم الجامعي، ودراسة (زقوت وآخرون، 2022) التي أظهرت أهمية كبيرة لمتطلبات الأمن السيبراني في الجامعة، ودراسة (الدحياني والصنوي، 2021) التي أظهرت أن درجة الموافقة على متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر المختصين كانت عالية جدًا، على مستوى الأداة ككل وعلى مستوى كل مجال من مجالات الدراسة، ولكنها تختلف مع دراسة (البلوشية وآخرون، 2024) التي أظهرت أن درجة متطلبات تحقيق الأمن السيبراني في

جامعة نزوى من وجهة أكاديمي الجامعة وموظفيها جاءت منخفضة، على مستوى الأداة ككل وعلى مستوى جميع المجالات.

كما حُسبت المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي لاستجابات أفراد عينة البحث لكل مجال على حدة ولجميع فقراته، ويمكن توضيح ذلك على النحو الآتي:

- **المجال الأول: المتطلبات المالية لإنشاء برنامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي:**

جدول (8): المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي على مستوى مجال المتطلبات المالية لإنشاء برامج الأمن السيبراني والذكاء الاصطناعي:

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	الوزن النسبي
1	توفير ميزانية كافية لتغطية تكاليف البرامج بما في ذلك المعدات ورواتب الأساتذة والبحث.	2.92	0.43	1	0.99
2	توفير المخصصات المالية اللازمة للربط الشبكي في الجامعات اليمنية.	2.83	0.56	6	0.97
3	زيادة تمويل المشاريع التحتية في الجامعات في مجال الأمن السيبراني والذكاء الاصطناعي.	2.88	0.37	3	0.98
4	توفير ميزانية لصيانة الأجهزة وشبكات الاتصال المرتبطة بالإنترنت.	2.85	0.35	4	0.98
5	عقد شراكات مع القطاع الخاص بالأمن السيبراني والذكاء الاصطناعي لضمان وجود داعم لإنشاء البرنامج.	2.89	0.64	2	0.99
6	توفير ميزانية كافية لشراء البرمجيات اللازمة لإنشاء برامج الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.	2.84	0.33	5	0.98
7	رصد مبالغ مالية للاستعانة بخبراء في مجال الأمن السيبراني والذكاء الاصطناعي.	2.80	0.45	8	0.97

8	توفير المخصصات المالية اللازمة لبرامج تدريب وتأهيل الموظفين داخليًا وخارجيًا.	2.81	0.36	7	0.98
المجال ككل:		2.85	0.43	-	0.98

يتضح من الجدول (8) موافقة أفراد عينة البحث من الخبراء على مجال المتطلبات المالية، حيث تراوحت قيمة المتوسطات لدرجات فقرات هذا المجال بين (2.80) و(2.92) بتقدير "موافق" على مستوى المجال والفقرات ككل، في حين بلغ المتوسط الحسابي العام (2.85) والانحراف المعياري (0.43) والوزن النسبي (98%)، وقد جاءت الفقرة رقم (1): "توفير ميزانية كافية لتغطية تكاليف البرامج بما في ذلك المعدات ورواتب الأساتذة والبحث"، في المرتبة الأولى بمتوسط حسابي (2.92) وانحراف معياري (0.43) ووزن نسبي (99%)، وهذا يدل على موافقة أفراد العينة من الخبراء والمختصين على أهمية وجود موازنة محددة لإنشاء برنامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي، فبدون هذه الموازنة لا يمكن للجامعات البدء في إجراءات الإنشاء، وجاءت الفقرة رقم (5): "عقد شراكات مع القطاع الخاص بالأمن السيبراني والذكاء الاصطناعي لضمان وجود داعم لإنشاء البرنامج"، في المرتبة الثانية بمتوسط حسابي (2.89) وانحراف معياري (0.64) ووزن نسبي (99%)، وهذا يدل على موافقة الخبراء على أن عقد شراكات مع القطاع الخاص في مجال الأمن السيبراني والذكاء الاصطناعي لضمان وجود داعم لتطبيقه يُعد من أهم المتطلبات المالية لإنشاء البرنامج، في حين جاءت الفقرة رقم (7): "رصد مبالغ مالية للاستعانة بخبراء في مجال الأمن السيبراني والذكاء الاصطناعي"، في المرتبة الأخيرة بمتوسط حسابي (2.80) وانحراف معياري (0.45)، ويعزو الباحثان هذه النتيجة إلى عدم قناعة بعض أفراد عينة البحث بأهمية رصد مبالغ مالية للاستعانة بخبراء في مجال الأمن السيبراني والذكاء الاصطناعي، وقد يعود ذلك إلى امتلاك الجامعات اليمنية العديد من الكفاءات والخبراء في هذا المجال.

كما نلاحظ توافق آراء أفراد العينة على زيادة تمويل المشاريع التحتية في الجامعات في مجال الأمن السيبراني والذكاء الاصطناعي، وتوفير ميزانية لصيانة الأجهزة وشبكات الاتصال المرتبطة بالإنترنت، وعقد شراكات مع القطاع الخاص بالأمن السيبراني والذكاء الاصطناعي، وتوفير ميزانية كافية لشراء البرمجيات اللازمة لإنشاء برامج الأمن السيبراني والذكاء الاصطناعي، وتوفير المخصصات المالية اللازمة لبرامج تدريب وتأهيل الموظفين داخليًا وخارجيًا.

- **المجال الثاني: المتطلبات التقنية لإنشاء برنامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي:**

جدول (9): المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي على مستوى مجال المتطلبات التقنية لإنشاء برامج الأمن السيبراني والذكاء الاصطناعي:

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	الوزن النسبي
1	توفير شبكة إنترنت عالية السرعة.	2.85	0.53	4	0.98
2	تشجيع الابتكارات التقنية في مجالات تقنيات الأمن السيبراني والذكاء الاصطناعي.	2.83	0.55	6	0.98
3	تطوير مختبرات محاكاة وهياكل تدريب متقدمة لتمكين الطلاب من تطبيق ما تعلموه.	2.87	0.47	2	0.99
4	توفير أنظمة التدريب المختصة بتطبيقات الأمن السيبراني والذكاء الاصطناعي.	2.85	0.39	5	0.97
5	توفير أنظمة حماية آلية متطورة لحماية البيانات في جميع الجامعات.	2.86	0.44	3	0.97
6	عمل دراسة لاحتياجات الجامعات من الأجهزة والمعدات والبرامج والمستلزمات اللازمة لإنشاء برامج الأمن السيبراني والذكاء الاصطناعي.	2.88	0.42	1	0.99
7	توفير الفنيين المختصين بالصيانة والتشغيل لتقنيات الأمن السيبراني والذكاء الاصطناعي.	2.81	0.49	7	0.97
	المجال ككل:	2.84	0.46	-	0.97

يتضح من الجدول (9) موافقة أفراد عينة البحث على مجال المتطلبات التقنية، حيث تراوحت المتوسطات لدرجات فقرات هذا المجال بين (2.81) و(2.88) بتقدير "موافق" على مستوى المجال والفقرات ككل، في حين بلغ المتوسط الحسابي العام (2.84) والانحراف المعياري (0.46) والوزن النسبي (97%) بتقدير "موافق" على مستوى المجال والفقرات ككل، وقد جاءت الفقرة رقم (6): "عمل دراسة لاحتياجات

الجامعات من الأجهزة والمعدات والبرامج والمستلزمات اللازمة لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي"، في المرتبة الأولى بمتوسط حسابي (2.88) وانحراف معياري (0.42) ووزن نسبي (99%)، ويرى الباحثان أن هذه النتيجة منطقية؛ لأن ضمان نجاح أي مشروع أو برنامج لا بد أن يسبق بدراسة الاحتياجات وتحديدها، وجاءت الفقرة رقم (3): "تطوير مختبرات محاكاة وهياكل تدريب متقدمة لتمكين الطلاب من تطبيق ما تعلموه"، في المرتبة الثانية بمتوسط حسابي (2.87) وانحراف معياري (0.47) ووزن نسبي (99%)، وهذا يدل على موافقة الخبراء على أهمية توفير البنية التحتية اللازمة لإنشاء البرنامج، في حين جاءت الفقرة رقم (7): "توفير الفنيين المختصين بالصيانة والتشغيل لتقنيات الأمن السيبراني والذكاء الاصطناعي"، في المرتبة الأخيرة بمتوسط حسابي (2.81) وانحراف معياري (0.49) ووزن نسبي (96%)، ويعزو الباحثان هذه النتيجة إلى عدم قناعة بعض أفراد عينة البحث بأهمية الفنيين المختصين بالصيانة والتشغيل، والاعتماد على المعيدين في تشغيل المعامل والمختبرات.

- **المجال الثالث: المتطلبات التشريعية لإنشاء برنامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي:**

جدول (10): المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي على مستوى مجال المتطلبات التشريعية لإنشاء برامج الأمن السيبراني والذكاء الاصطناعي:

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	الوزن النسبي
1	تغيير الثقافة السائدة في الجامعة من خلال نشر ثقافة استخدام الأمن السيبراني والذكاء الاصطناعي.	2.81	0.63	6	0.96
2	وضع التشريعات اللازمة لضمان إنشاء برامج الأمن السيبراني والذكاء الاصطناعي.	2.84	0.59	3	0.97
3	توافر القناعة لدى القيادات الجامعية وأصحاب القرار بأهمية إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي.	2.86	0.47	1	0.98
4	وضع خطة استراتيجية لتحقيق الرؤية والأهداف المرغوبة.	2.85	0.49	2	0.97
5	يجب أن تكون البرامج معتمدة من قبل هيئات تعليمية معترف بها لضمان جودتها.	2.83	0.70	4	0.97
6	إصدار اللوائح التي تضمن سرية تبادل المعلومات في الجامعات.	2.80	0.42	7	0.96

7	تحديد رؤية الجامعة المستقبلية في ضوء الأمن السيبراني والذكاء الاصطناعي.	2.82	0.49	5	0.97
المجال ككل:		2.83	0.54	-	0.96

يتضح من الجدول (10) موافقة أفراد عينة البحث على مجال المتطلبات التشريعية والتنظيمية، حيث تراوحت متوسطات درجات فقرات هذا المجال بين (2.80) و(2.86) بتقدير "موافق" على مستوى المجال والفقرات ككل، في حين بلغ المتوسط الحسابي العام (2.83) والانحراف المعياري (0.54) والوزن النسبي (96%) بتقدير "موافق" على مستوى المجال والفقرات ككل، وقد جاءت الفقرة رقم (3): "توافر القناعة لدى القيادات الجامعية وأصحاب القرار بأهمية إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي"، في المرتبة الأولى بمتوسط حسابي (2.86) وانحراف معياري (0.47) ووزن نسبي (98%)، ويرى الباحثان أن هذه النتيجة منطقية؛ لأن توافر القناعة لدى القيادات الجامعية وأصحاب القرار، تمثل نقطة الانطلاق نحو إنشاء البرنامج، وجاءت الفقرة رقم (4): "وضع خطة استراتيجية لتحقيق الرؤية والأهداف المرغوبة"، في المرتبة الثانية بمتوسط حسابي (2.85) وانحراف معياري (0.49) ووزن نسبي (97%)، وهذا يدل على موافقة الخبراء على أهمية وضع خطة استراتيجية لتحقيق الرؤية والأهداف المرغوبة لإنشاء البرنامج، في حين جاءت الفقرة رقم (6): "إصدار اللوائح التي تضمن سرية تبادل المعلومات في الجامعات"، في المرتبة الأخيرة بمتوسط حسابي (2.80) وانحراف معياري (0.42) ووزن نسبي (96%)، ويعزو الباحثان هذه النتيجة إلى أن هذه اللوائح والتعميمات تأتي في نهاية استكمال البرنامج.

- **المجال الرابع: المتطلبات البشرية لإنشاء برنامج الدراسات العليا في الأمن السيبراني والذكاء الاصطناعي:**

جدول (11): المتوسطات الحسابية والانحرافات المعيارية والوزن النسبي على مستوى مجال المتطلبات البشرية لإنشاء برامج الأمن السيبراني والذكاء الاصطناعي:

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الترتيب	الوزن النسبي
1	ربط الممارسات الإدارية والأكاديمية في الجامعة بالذكاء الاصطناعي والأمن السيبراني.	2.80	0.65	5	0.92
2	استقطاب كفاءات وخبرات في برامج الأمن السيبراني والذكاء الاصطناعي.	2.81	0.57	3	0.94

3	تنمية القيم والأخلاق المهنية لدى القائمين على برامج الأمن السيبراني والذكاء الاصطناعي في الجامعات.	2.80	0.67	6	0.91
4	تدريب الكوادر القيادية والإدارية والتدريسية في الجامعات اليمنية على توظيف تقنيات الأمن السيبراني والذكاء الاصطناعي في أعمالهم المختلفة.	2.83	0.59	2	0.96
5	وضع خطة لتطوير العنصر البشري في الجامعة في ضوء متطلبات الأمن السيبراني والذكاء الاصطناعي.	2.81	0.74	4	0.95
6	الاستعانة بخبراء محليين في إعداد برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي.	2.85	0.45	1	0.97
المجال ككل:		2.81	0.61	-	0.94

يتضح من الجدول (11) موافقة أفراد عينة البحث على مجال المتطلبات البشرية، حيث تراوحت متوسطات درجات فقرات هذا المجال بين (2.80) و(2.85)، في حين بلغ المتوسط الحسابي العام (2.81) والانحراف المعياري (0.61) والوزن النسبي (0.94) بتقدير "موافق" على مستوى المجال والفقرات ككل، وقد جاءت الفقرة رقم (6): "الاستعانة بخبراء محليين في إعداد برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي"، في المرتبة الأولى بمتوسط حسابي (2.85) وانحراف معياري (0.45) ووزن نسبي (97%)، ويرى الباحثان أن هذه النتيجة منطقية؛ لأن وجود الخبراء يُعتبر مطلبًا أساسيًا من متطلبات بناء البرنامج، وجاءت الفقرة رقم (4): "تدريب الكوادر القيادية والإدارية والتدريسية في الجامعات اليمنية على توظيف تقنيات الأمن السيبراني والذكاء الاصطناعي في أعمالهم المختلفة"، في المرتبة الثانية بمتوسط حسابي (2.83) وانحراف معياري (0.59) ووزن نسبي (96%)، وهذا يدل على أهمية التدريب المستمر في التأهيل المهني والأكاديمي، في حين جاءت الفقرة رقم (3): "تنمية القيم والأخلاق المهنية لدى القائمين على برامج الأمن السيبراني والذكاء الاصطناعي في الجامعات"، في المرتبة الأخيرة بمتوسط حسابي (2.80) وانحراف معياري (0.67) ووزن نسبي (91%)، ويعزو الباحثان هذه النتيجة إلى أن هذا المجال يمكن تحقيقه مستقبلًا ضمن الدورات التدريبية وورش العمل.

[2] النتائج المتعلقة بسؤال البحث الثاني الذي ينص على الآتي: "ما التصور المقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية"؟

من خلال العرض السابق للإطار النظري للبحث، ونتائج البحث الميدانية من وجهة نظر الخبراء والمختصين في الأمن السيبراني والذكاء الاصطناعي، ومسح وتحليل البرامج المناظرة في جامعات عربية وأجنبية، واستطلاع أولي لآراء بعض الطلبة المحتملين، وحاجة سوق العمل، واستشارة الخبراء والمختصين في هذا المجال، والاستناد إلى لوائح الدراسات العليا المعمول بها في الجامعات اليمنية ومنها جامعة صنعاء، خرج الباحثان برؤية واضحة للتصور المقترح، متضمنة صورة البرنامج المقترح.

ولذلك فإن هذا التصور المقترح وما يشمله من البرنامج المقترح لم يأت من فراغ، بل جاء نتيجة لما توصل إليه البحث الميداني، وبهذا فهو يعد نقطة تحول مهمة وجوهرية في سبيل توضيح المبادئ والمنطلقات والمتطلبات والآلية والمراحل المهمة لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية، لا سيما جامعة صنعاء، إلى جانب توضيح أهم التحديات والعوائق المحتملة التي من شأنها أن تقف عائقًا أمام تطبيق هذا المقترح.

ويمثل الشكل الآتي الطريقة التي بُني من خلالها التصور المقترح:

شكل (1): يوضح آلية بناء التصور المقترح.

وفيما يلي توضيح آلية وخطوات بناء التصور المقترح:

أولًا: منطلقات وأسس التصور المقترح:

انطلق التصور المقترح من جملة من المسوغات، ويمكن تلخيصها في الآتي:

[1] الرؤية الوطنية لبناء الدولة اليمنية الحديثة 2019م التي أكدت ضرورة تطوير البنية التحتية والتقنية للتعليم بأنواعه، من خلال توفير الربط الشبكي وأجهزة تقنية المعلومات والاتصالات للمؤسسات التعليمية.

[2] اهتمام وزارة التربية والتعليم والبحث العلمي بتطبيق متطلبات الذكاء الاصطناعي والأمن السيبراني في الجامعات بما يحقق جودة أداء مؤسسات التعليم العالي.

[3] توصيات المؤتمر الأول للتحول الرقمي في اليمن المنعقد في 14-16 ربيع الأول لعام 1444هـ، الموافق 10-12 أكتوبر لعام 2022م صنعاء.

[4] توصيات مؤتمر المعرفة التكنولوجية والتحول الرقمي في مؤسسات التعليم العالي 21-22 ديسمبر 2022م صنعاء.

[5] حاجة الجامعات اليمنية إلى إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في ضوء المتطلبات، وذلك لتحقيق مستوى عالٍ من الأداء وتحقيق الميزة التنافسية بين الجامعات، وهذا ما أكده توافق آراء الخبراء حول مجالات الذكاء الاصطناعي والأمن السيبراني ومتطلباتهم، ما يستدعي ضرورة إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية ولا سيما جامعة صنعاء.

ثانيًا: أهداف التصور المقترح:

يهدف التصور المقترح إلى تقديم رؤية مقترحة لإنشاء برامج دراسات عليا (ماجستير) في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية، من خلال تحقيق الأهداف الآتية:

[1] تحديد آليات وإجراءات تسهم في إنشاء برامج دراسات عليا (ماجستير) في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.

[2] مساعدة القائمين على مؤسسات التعليم العالي في وضع رؤية واضحة ومحددة لإنشاء برنامج دراسات عليا (ماجستير) في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية، بما يتناسب مع ظروف البيئة المحلية وطبيعتها.

[3] وضع خطة لتطوير الكفاءات والقدرات البشرية داخل الجامعات وتنميتها لتطبيق متطلبات الأمن السيبراني والذكاء الاصطناعي، من خلال الاستعانة بالكفاءات والخبرات في برنامج الأمن السيبراني والذكاء الاصطناعي.

[4] تحديد إجراءات إنشاء برامج دراسات عليا (ماجستير) في مجال الأمن السيبراني والذكاء الاصطناعي باستخدام منظومة من الأجهزة والبيانات والتخزين، وتضمن توفير البنية التقنية في الجامعات.

ثالثًا: مجالات التصور المقترح:

من خلال ما توصل إليه البحث من نتائج ميدانية على وفق آراء الخبراء، اقترحت مجالات التصور الآتية:

جدول (12): مجالات التصور المقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية:

المجال	المؤشرات
المتطلبات المالية	توفير ميزانية كافية لتغطية تكاليف البرامج بما في ذلك المعدات ورواتب الأساتذة والبحث.
	توفير المخصصات المالية اللازمة للربط الشبكي في الجامعات اليمنية.
	زيادة تمويل المشاريع التحتية في الجامعات في مجال الأمن السيبراني والذكاء الاصطناعي.
	توفير ميزانية لصيانة الأجهزة وشبكات الاتصال المرتبطة بالإنترنت.
	عقد شراكات مع القطاع الخاص بالأمن السيبراني والذكاء الاصطناعي لضمان وجود داعم لإنشاء البرنامج.
	توفير ميزانية كافية لشراء البرمجيات لإنشاء برامج الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.
	رصد مبالغ مالية للاستعانة بخبراء في مجال الأمن السيبراني والذكاء الاصطناعي.
	توفير المخصصات المالية اللازمة لبرامج تدريب وتأهيل الموظفين داخليًا وخارجيًا.
المتطلبات التقنية	توفير شبكة إنترنت عالية السرعة.
	تشجيع الابتكارات التقنية في مجالات تقنيات الأمن السيبراني والذكاء الاصطناعي.
	تطوير مختبرات محاكاة وهياكل تدريب متقدمة لتمكين الطلبة من تطبيق ما تعلموه.
	توفير أنظمة التدريب المختصة بتطبيقات الأمن السيبراني والذكاء الاصطناعي.
	توفير أنظمة حماية آلية متطورة لحماية البيانات في جميع الجامعات اليمنية.
	عمل دراسة لاحتياجات الجامعات من الأجهزة والمعدات اللازمة لإنشاء البرنامج.

	توفير الفنيين المختصين بالصيانة والتشغيل لتقنيات الأمن السيبراني والذكاء الاصطناعي.
المتطلبات التشريعية والتنظيمية	تغيير الثقافة السائدة في الجامعة من خلال نشر ثقافة استخدام الأمن السيبراني والذكاء الاصطناعي.
	وضع التشريعات اللازمة لضمان إنشاء برامج الأمن السيبراني والذكاء الاصطناعي.
	توافر القناعة لدى القيادات الجامعية وأصحاب القرار بأهمية إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي.
	وضع خطة استراتيجية لتحقيق الرؤية والأهداف المرغوبة.
	يجب أن تكون البرامج معتمدة من قبل هيئات تعليمية معترف بها لضمان جودتها.
	إصدار اللوائح التي تضمن سرية تبادل المعلومات في الجامعات اليمنية.
	تحديد رؤية الجامعة المستقبلية في ضوء الأمن السيبراني والذكاء الاصطناعي.
المتطلبات البشرية	ربط الممارسات الإدارية والأكاديمية في الجامعة بالذكاء الاصطناعي والأمن السيبراني.
	استقطاب كفاءات وخبرات في برامج الأمن السيبراني والذكاء الاصطناعي.
	تنمية القيم والأخلاق المهنية لدى القائمين على برامج الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.
	تدريب الكوادر القيادية والإدارية والتدريسية في الجامعات اليمنية على توظيف تقنيات الأمن السيبراني والذكاء الاصطناعي في أعمالهم المختلفة.
	وضع خطة لتطوير العنصر البشري في الجامعات اليمنية في ضوء متطلبات الأمن السيبراني والذكاء الاصطناعي.
	الاستعانة بخبراء محليين في إعداد برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.

رابعًا: متطلبات تطبيق التصور المقترح:

لضمان تطبيق التصور المقترح يجب توفير المتطلبات الآتية:

1. وضع التشريعات والقوانين واللوائح التي تدعم تطبيق متطلبات إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.
2. نشر ثقافة تطبيق الأمن السيبراني والذكاء الاصطناعي في مؤسسات التعليم العالي لزيادة وعي القيادات الأكاديمية في الجامعات اليمنية.
3. التزام ودعم الإدارة العليا (وزارة التعليم العالي، القيادات الأكاديمية في الجامعات اليمنية) واقتناعها بأهمية تطبيق التصور المقترح وتبنيه.
4. وضع خطة استراتيجية لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية، والتهيئة والتطوير للبنية التحتية التقنية.
5. توفير موارد مالية كافية لتطبيق التصور المقترح.
6. التأهيل والتدريب للكوادر البشرية في الجامعات اليمنية على استخدام التكنولوجيا الذكية.

خامسًا: مراحل تطبيق التصور المقترح:

تمر عملية تطبيق متطلبات إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية بالمراحل والخطوات الآتية:

أ) تهيئة الجامعات: إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي يتطلب تهيئة المجتمع الجامعي وتوعيته، وتوافر أسس ومعايير الاستعداد الرقمي والتكنولوجيا للجامعات اليمنية، ويكون ذلك من خلال الآتي:

1. توفير الإطار التشريعي من خلال وضع الإجراءات التشريعية والقانونية لتطبيق الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.
2. تكوين قناعات لدى الإدارة العليا (القيادات الأكاديمية في الجامعات اليمنية) لتبني التصور المقترح، من خلال بيان أهمية البرنامج وسماته وفوائده لمختلف الأطراف ذات العلاقة.
3. توافر بنية تحتية للتكنولوجيا الذكية من خلال توافر وإتاحة الشبكات، والحاسبات، ونظم المعلومات، والبرمجيات، والتأكد من إمكانية الوصول إليها واستخدامها بسهولة، وزيادة قدرتها على تبادل المعلومات، وتوفير قنوات اتصال قوية وفعالة.
4. توفير الموارد البشرية المؤهلة والمدربة على تكنولوجيا المعلومات والاتصالات، للقيام بتقديم الخدمات التكنولوجية وتطبيقاتها التقنية.
5. تحديد مدى زمني لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.
6. اختيار التوقيت المناسب للبدء بالتنفيذ.

7. توفير الاحتياجات المالية والمادية اللازمة لتطبيق التصور المقترح.
8. عمل الورش والدورات التدريبية اللازمة لتطبيق التصور

ب) التطبيق التجريبي للتصور:

في هذه المرحلة تقوم الإدارة العليا للجامعات اليمنية بتبني فكرة التصور المقترح والشروع في تطبيقه على نطاق محدود وطبقًا لبرنامج زمني محدد ومعلوم من خلال الإجراءات الآتية:

1. تحديد جامعات محددة للتطبيق التجريبي.
2. تهيئة الجامعات المختارة، وتوفير المتطلبات والاحتياجات اللازمة للتطبيق.

ج) تقييم ومتابعة التنفيذ:

تأتي هذه الخطوة أثناء وبعد تنفيذ التطبيق التجريبي للتصور المقترح، وتعد عملية التقييم ومتابعة مراحل التنفيذ والتغذية الراجعة أهم الخطوات التي تضمن معالجة أوجه القصور، والتغلب على الصعوبات أولا بأول، ويفترض أن تحدث عملية التقييم والمتابعة في ضوء رسالة الجامعة وأهدافها، واستنادًا إلى المعايير التي أخذت في الاعتبار كأساس لقياس مدى التقدم في تطبيق التصور.

د) التطبيق الكامل للتصور المقترح:

في ضوء ما تسفر عنه عملية المتابعة والتقييم والتغذية الراجعة، ومع تزايد نجاح التطبيق الشامل، يمكن تعميم التصور بعد ضمان ما يلي:

1. نجاح التجربة المصغرة للتصور المقترح في بعض الجامعات اليمنية.
2. وجود فريق من الخبراء والمتخصصين يشرف على عملية تطبيق التصور المقترح.
3. توفير الاحتياجات اللازمة كافة لتطبيق التصور المقترح.
4. توفير الرقابة الداخلية والخارجية لتطبيق الأمن السيبراني والذكاء الاصطناعي، من خلال توفير أدوات الرقابة الداخلية والخارجية لحماية عمليات وبيانات الجامعة داخليًا وخارجيًا.
5. الاستفادة من الأخطاء التي قد تحدث أثناء التطبيق المرحلي، والعمل على تفادي تكرار حدوثها مستقبلًا.

سادسًا: العوائق المحتملة أمام تطبيق التصور المقترح:

من العوائق التي يمكن أن تحد من فاعلية التصور المقترح وتعوق تطبيقه، ما يلي:

1. ضعف الاهتمام والقناعة من قبل الإدارة العليا بالجامعات اليمنية بأهمية التصور المقترح.
2. ندرة توفير مصادر التمويل اللازمة لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي بالجامعات اليمنية.
3. الافتقار إلى وجود استراتيجيات تطبيق التكنولوجيا الذكية.
4. الافتقار إلى خطة واضحة لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي على أرض الواقع.
5. السياسات التقليدية، وضعف فاعلية التشريعات والإجراءات، والهياكل التنظيمية، كلها يمكن أن تكون عائقًا أمام تطبيق التصور المقترح للتحول الرقمي في الجامعات اليمنية.

6. قلة توفير الكوادر البشرية المؤهلة والمدربة، والقادرة على تطبيق التصور المقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي بالجامعات اليمنية.

سابعًا: طرق التغلب على عوائق التصور المقترح:

يمكن التغلب على تلك العوائق من خلال توفير متطلبات تطبيق التصور المقترح والعمل الجاد على تطبيقه، كما يمكن التغلب عليها باتباع ما يلي:

7. نشر ثقافة التكنولوجيا الذكية من خلال عقد الندوات والورش التوعوية حول أهمية تطبيق الأمن السيبراني والذكاء الاصطناعي بالجامعات اليمنية.
8. حث الجامعات على إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي بالجامعات اليمنية.
9. توفير الكوادر البشرية المؤهلة والمدربة والقادرة على تطبيق التكنولوجيا الذكية.
10. تفعيل وتعزيز الشراكة والعلاقات مع جميع الجهات ذات العلاقة بالجامعات اليمنية في المجتمع والدولة والقطاعات المختلفة الخاصة والعامة داخل البلد.
11. ضرورة تبادل الخبرات بين الجامعات اليمنية في تطبيق برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي والاستفادة من تجارب الجامعات العربية والأجنبية في هذا المجال.

ثامنا: البرنامج المقترح:

جدول (13): وصف البرنامج المقترح:

المعلومات الأساسية للبرنامج
● **اسم البرنامج: برنامج ماجستير في الذكاء الاصطناعي والأمن السيبراني.** ● **مسار البرنامج: مقررات دراسية ورسالة.** ● **الدرجة التي يمنحها: ماجستير.** ● **اسم الدرجة العلمية: ماجستير في الذكاء الاصطناعي والأمن السيبراني.** ● **نوع البرنامج: أكاديمي.** ● **لغة البرنامج: العربية.** ● **نقاط الخروج: بحسب اللائحة.** ● **مدة البرنامج: سنة.** ● **عدد مستويات البرنامج: مستويان.** ● **الساعات المعتمدة: 36 ساعة.**
نبذة عن البرنامج
برنامج دراسات عليا يدمج بين تقنيات الذكاء الاصطناعي (AI) والأمن السيبراني (CS)، لتوفير فهم شامل وتكاملي لهذه المجالات المهمة، وتأهيل الطلبة وتزويدهم بالمعرفة والمهارات الأساسية لمهنة ناجحة في هذه المجالات سريعة التطور، وإكسابهم مهارات متقدمة تمكنهم من مواجهة التحديات الرقمية والمخاطر والتهديدات السيبرانية المعقدة وتطوير حلول مبتكرة، من خلال الفهم العميق لنظريات الذكاء الاصطناعي ومبادئ الأمان المتقدمة والممارسات المبتكرة، ويتضمن البرنامج مقررات تغطي الأسس النظرية والممارسة لتصميم وبناء أنظمة آمنة، والتشفير وأمن الشبكة والبرمجة الآمنة والهاكر الأخلاقي، ومجموعة متنوعة من الموضوعات

كتعلم الآلة، ومعالجة اللغة الطبيعية، والأمن السيبراني مع الذكاء الاصطناعي، ومن ثم تمكين الطلبة المحترفين في مجال الذكاء الاصطناعي والأمن السيبراني وخدمة المجتمع من خلال تطوير تطبيقات ذكية تلبي احتياجات السوق وتعزز التنمية التكنولوجية.

أهمية البرنامج

تتمثل أهمية البرنامج فيما يمكن أن يسهم به من إعداد كوادر مؤهلة لاستقبال العالم الذكي في المجالات المهنية المختلفة، وتزويد سوق العمل على المستوى المحلي والإقليمي بكفاءات في مجال الذكاء الاصطناعي والأمن السيبراني مؤهلين لشغل وظائف البحث والتطوير أو المناصب الإدارية وخلق فرص في ريادة الأعمال، إلى جانب دعم وتعزيز مساهمة جامعة صنعاء في تحقيق الرؤية الوطنية، ودعم خطتها الاستراتيجية ودورها في توفير التعليم المتميز، وإنتاج البحوث العلمية القيمة والمبتكرة في تقنيات وتطبيقات الذكاء الاصطناعي والأمن السيبراني.

سمات البرنامج

تشمل السمات الرئيسة للبرنامج منهجًا أساسيًا متعدد التخصصات، ومسارات التخصص والتطبيق العملي والنظرية والتطوير المهني والتحضير للمستقبل، ومن خلاله سيمتلك الخريجون مجموعة فريدة من المهارات، ويكونون على استعداد لمواجهة تحديات الذكاء الاصطناعي والأمن السيبراني في أدوار مختلفة من خلال التعليم والبحث والصناعات المختلفة، ولذلك فإن هذا البرنامج ليس مجرد طريق إلى الحياة المهنية، بل إنه بوابة ليصبح الخريجون روادًا في مجال يقع في طليعة التقدم التكنولوجي وضروري للأمن السيبراني في العالم الرقمي اليوم.

رؤية البرنامج

الريادة والتميز علميًا وبحثيًا في مجال الأمن السيبراني والذكاء الاصطناعي محليًا وإقليميًا وصولًا إلى العالمية بما يتوافق مع المستويات المعيارية العالمية.

رسالة البرنامج

إعداد خريجين متميزين ومؤهلين بالمعرفة والمهارات لمواكبة التطور الهائل في مجال الأمن السيبراني والذكاء الاصطناعي وتأهيلهم للنجاح في سوق العمل، وتنمية قدراتهم لتقديم بحوث مبتكرة لمواجهة التحديات المستقبلية في هذه المجالات الحيوية.

أهداف البرنامج

يهدف البرنامج بصورة رئيسة إلى تمكين الطلبة من الآتي:

- الاستفادة من التطورات الحالية والناشئة في مجال الذكاء الاصطناعي وتوظيفها لتصميم ونشر استراتيجية أمنية مرنة ومستدامة قادرة على الاستجابة بفعالية للظروف السياقية المتغيرة، بما في ذلك التهديدات والمخاطر الحالية والتحديات الناشئة.
- اكتساب المهارات اللازمة للعمل كمختصين في الذكاء الاصطناعي والأمن السيبراني أو لمواصلة دراساتهم العليا في مختلف مجالات الذكاء الاصطناعي والأمن السيبراني.
- إجراء البحوث التطبيقية المبتكرة في مجال الأمن السيبراني لتلبية احتياجات اليمن ومتطلبات سوق العمل، وتقديم الحلول المناسبة للمؤسسات الخاصة والعامة في البلد.
- تطبيق أعلى المعايير الأخلاقية والقانونية في الذكاء الاصطناعي والأمن السيبراني، لاتخاذ قرارات مستنيرة تأخذ في الاعتبار الآثار الواسعة على الاقتصاد والبيئة والمجتمع.
- إظهار مهارات القيادة والتعاون في فرق متعددة التخصصات، ودفع الابتكار والتعلم المستمر في مبادرات الذكاء الاصطناعي والأمن السيبراني.
- تقييم أفضل الممارسات الحالية والناشئة في مجال الذكاء الاصطناعي والأمن السيبراني لضمان الكفاءة والأمن والاستدامة والنمو واستمرارية العمليات داخل المؤسسة، ولا سيما في البيئات التي تتميز بمخاطر وتهديدات متنوعة.

– الانخراط في التعلم مدى الحياة والتطوير المهني والممارسات الأخلاقية ضمن تخصصات الذكاء الاصطناعي والأمن السيبراني.
مخرجات البرنامج
● المعرفة والفهم: عند استكمال متطلبات البرنامج، سيكون الخريج قادرًا على الآتي: 1–معرفة وفهم الحقائق والمفاهيم والمبادئ والنظريات والممارسات والعمليات الأساسية المتعلقة بالأمن السيبراني والذكاء الاصطناعي وتطبيقها على الحالات المختلفة. 2–تصنيف بروتوكولات أمن المعلومات، وتحليل وبناء وإعداد شبكات اتصال آمنة. 3–تحديد المتطلبات والمسؤوليات المهنية واتخاذ القرارات التي تتعلق بالجوانب الحاسوبية وأخلاقيات استخدام البيانات والمعلومات بحسب المعايير الأخلاقية والقانونية. 4–استنتاج الفجوات في أمن المعلومات مع الأخذ بعين الاعتبار التقنيات الحالية والناشئة والاتجاهات السائدة في أمن المعلومات. ● المهارات الذهنية والعملية: عند استكمال متطلبات البرنامج، سيكون الخريج قادرًا على الآتي: 1–برمجة وتنفيذ أحدث تقنيات الذكاء الاصطناعي. 2–تصميم وتطوير وتقييم حلول وأنظمة ذكية لتلبية احتياجات قائمة. 3–تحديث وتصميم وبناء أنظمة حاسوبية وشبكات آمنة، باستخدام الأدوات المناسبة، وتوثيق جميع مراحل هذه العملية. 4–تقييم نظرية الذكاء الاصطناعي وتقنياته لاستخدامها في تصميم وتنفيذ ونشر الحلول للمشكلات المعقدة. 5–تطبيق الحلول المتقدمة القائمة على الذكاء الاصطناعي لتعزيز أمن المعلومات والأنظمة المتصلة داخل المؤسسة في ظل وجود مخاطر وتهديدات معقدة. ● المهارات العامة والانتقالية: عند استكمال متطلبات البرنامج، سيكون الخريج قادرًا على الآتي: 1–إدارة مشاريع البحث والتطوير والابتكار التعاونية المعقدة في مجالات الذكاء الاصطناعي والتكنولوجيا المتقدمة. 2–العمل بفعالية بشكل مستقل وكعضو فعال في الفريق في مشروع تقني أو برمجي أو لتحقيق هدف مشترك. 3–التخطيط لمشاريع مستقبلية في مجالات الذكاء الصناعي والأمن السيبراني. 4–تقييم الاعتبارات الأخلاقية والمجتمعية والقانونية المتعلقة بتكنولوجيا الذكاء الاصطناعي والأمن السيبراني. 5–الانخراط في التطوير المهني المستمر عن طريق تكنولوجيا المعلومات بشكل مستقل.
الآفاق المهنية والفرص المستقبلية
يمكن للخريجين بعد الانتهاء من دراسة البرنامج الاختيار بين مسارات أكاديمية ومهنية متنوعة، ومنها: 1–الانخراط في البحث والتطوير المتقدم من خلال درجة الدكتوراه في مجال تخصصهم. 2–العمل في المؤسسات الخاصة والعامة لتطوير حلول في مجال الأمن السيبراني باستخدام تقنيات الذكاء الاصطناعي. 3–الالتحاق بالحياة الأكاديمية والبحثية أو المختبرات الصناعية في الجامعات ومراكز البحث على المستوى المحلي وغير ذلك من الجامعات والمراكز البحثية العربية والعالمية. –العمل في مجال التعليم والتدريب والإشراف كمهندس برمجيات ومصمم ومحلل نظم ذكية، ومهندس بيانات. –العمل في المؤسسات العامة والخاصة كمستشار واختصاصي في الذكاء الاصطناعي والأمن السيبراني في مجالات متعددة، مثل: الاستجابة للحوادث وتحليل المخاطر وإدارتها، ومدير أمني للمعلومات، واستخبارات التهديدات أو التشفير، وضمان حماية الأصول الرقمية، وتطوير ونشر أنظمة وتطبيقات الذكاء الاصطناعي.

لوائح الدراسات العليا للبرنامج		
● متطلبات الالتحاق بالبرنامج/القبول: إضافة إلى شروط القبول الواردة في المادة رقم (12) من قرار رئيس مجلس الوزراء رقم (40) لسنة (2008) بشأن نظام الدراسات العليا في الجامعات اليمنية واللائحة الموحدة للدراسات العليا في الجامعات اليمنية والقواعد والإجراءات التنظيمية والتنفيذية للدراسات العليا في جامعة صنعاء، يمكن إضافة الشروط الآتية للالتحاق بالبرنامج: 1-حصول المتقدم على درجة البكالوريوس في المجالات التالية: علوم الحاسب، الذكاء الاصطناعي، الأمن السيبراني، علوم البيانات من جامعة صنعاء أو إحدى الجامعات المعتمدة من المجلس الأعلى للجامعات اليمنية بنظام (الانتظام الكلي) أو ما يعادلها بتقدير لا يقل عن (جيد مرتفع). 2-يجوز قبول غير المتخصصين في علوم الحاسوب من التخصصات التالية: هندسة الحاسوب، نظم المعلومات، هندسة البرمجيات، تقنية المعلومات، تخصصات حاسوبية تربوية، الهندسة الكهربائية، هندسة الاتصالات، هندسة الشبكات، هندسة الإلكترونيات، هندسة الميكاترونكس، الرياضيات التطبيقية، الإحصاء وبحوث العمليات، أو علوم الكمبيوتر من برنامج معترف به من مركز الجودة في المستوى الجامعي بنظام الانتظام الكلي من جامعة صنعاء أو أي جامعة أخرى موصى بها من وزارة التربية والتعليم العالي والبحث العلمي بتقدير لا يقل عن (جيد مرتفع). 3-اجتياز امتحان اللغة العربية المعد لهذا الغرض، والحصول على درجة (450) في اختبار اللغة الإنجليزية STEP أو ما يعادلها في اختبار TOFEL – IELTS، واجتياز مهارات استخدام الكمبيوتر. ● متطلبات التخرج: إضافة إلى شروط القبول الواردة في المادة رقم (13) من اللائحة الموحدة للدراسات العليا في الجامعات اليمنية والقواعد والإجراءات التنظيمية والتنفيذية للدراسات العليا في جامعة صنعاء، يمكن إضافة الشروط الآتية للتخرج من البرنامج: 1-مدة الدراسة: سنة مقسمة على فصلين دراسيين من المقررات كحد أدنى (30 ساعة معتمدة). 2-النجاح في جميع المقررات بمعدل لا يقل عن (75%) من العلامات. 3-إلزامية المشاركة في مؤتمرات أو ورش عمل مرتبطة بالتخصص. 4-توفير مرشد أكاديمي لكل طالب لمتابعة التقدم البحثي. 5-النجاح في رسالة الماجستير، ويحسب لها (6 ساعات معتمدة).		
هيكل البرنامج		
مدة البرنامج	**عدد المستويات الدراسية**	**الساعات المعتمدة**
سنتان	**أربعة فصول دراسية**	**36 ساعة**
المقررات الدراسية		**10 مقررات**
الساعات المعتمدة للمقررات الدراسية		**30 ساعة**
رسالة الماجستير		**6 ساعات**
مجموع الساعات المعتمدة		**36 ساعة**
الخطة الدراسية: انظر ملحق (1)		
توصيف المقررات: انظر ملحق (2)		

الخاتمة

تشمل على استنتاجات البحث وتوصياته ومقترحاته

استنتاجات البحث:

في ضوء ما توصل إليه البحث يمكن استنتاج الآتي:

كما يلي:

1. وجود موافقة بدرجة كبيرة لآراء الخبراء والمختصين حول متطلبات إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.
2. إمكانية تبني وتطبيق التصور المقترح لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.

التوصيات:

3. نشر ثقافة الأمن السيبراني والذكاء الاصطناعي بين العاملين في الجامعات اليمنية وجميع أفراد المجتمع.
4. توفير الكوادر البشرية المؤهلة والمدربة من أجل تطبيق ناجح لبرنامج الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.
5. أهمية توفير البنية التحتية لإنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي.
6. إنشاء مركز للأمن السيبراني والذكاء الاصطناعي تشارك فيه كل مؤسسات التعليم العالي الحكومية والأهلية.
7. على وزارة التربية والتعليم والبحث العلمي والقيادة الأكاديمية في الجامعات اليمنية تطبيق التصور المقترح ودراسة جدوى فاعليته.

المقترحات:

8. إجراء دراسة لوضع استراتيجية لتطبيق برامج الدراسات العليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.
9. إجراء دراسة لكيفية تمويل إنشاء برامج دراسات عليا في مجال الأمن السيبراني والذكاء الاصطناعي في الجامعات اليمنية.

المراجع

أولًا: المراجع العربية:

[1] البار، عدنان مصطفى؛ خالد، المرحبي. (2020). أمن المعلومات والأمن السيبراني. **ورقة علمية**، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، السعودية.

[2] البشر، منى بنت عبد الله بن محمد. (2020). متطلبات توظيف تطبيقات الذكاء الاصطناعي في تدريس طلاب وطالبات الجامعات السعودية من وجهة نظر الخبراء. مجلة كلية التربية: جامعة كفر الشيخ، مج20، ع2، 27-92.

[3] البلوشية، نجلاء موسى؛ الرواحية، طيبة؛ العامرية، بدرية؛ الذهلي، ربيع؛ اليحمدي، حمد؛ القضاة، محمد. (2024). متطلبات تحقيق الأمن السيبراني بجامعة نزوى في ضوء رؤية عمان 2040 ومعوقاته من وجهة نظر الأكاديميين والموظفين. **مجلة التربية والعلوم الاجتماعية**، مج8، ع13، 114-134.

[4] الخميسي، عبد السلام حسين؛ الحاوري، عبد الغني. (2023). تصور مقترح لإنشاء مركز للذكاء الاصطناعي بوزارة التربية والتعليم بالجمهورية اليمنية في ضوء متطلبات الثورة الصناعية الرابعة. **مجلة جامعة صنعاء للعلوم الإنسانية**، مج4، ع2، 579-605.

[5] الدحياني، ناصر سعيد؛ الصنوي، أمير. (2021). متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر الخبراء. **مجلة الجامعة الوطنية**، ع18، 93-126.

[6] الدهشان، جمال علي خليل. (2019). برامج إعداد المعلم لمواكبة متطلبات الثورة الصناعية الرابعة.

المجلة التربوية، كلية التربية، جامعة سوهاج، ع68، 3153=3199.

[7] الرمبيان، هند سليمان صالح. (2024). دراسة مقارنة في توظيف الذكاء الاصطناعي في برامج الدراسات العليا في كل من الولايات المتحدة الأمريكية والصين ومدى إمكانية الإفادة منها في المملكة العربية السعودية. **مستقبل التربية العربية**، مج31، ع143.

[8] السمحان، منى عبد الله. (2020). متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. **مجلة كلية التربية**، جامعة المنصورة، ع111، جزء1، 2-29.

[9] العريفي، نورة سعد. (2024). تصور مقترح لتوظيف تطبيقات الذكاء الاصطناعي في التعليم المستمر. **مجلة الجامعة العراقية**، مج66، ع2.

[10] الهاشمي، سعيد محمد. (2006). اللوائح التنظيمية للقبول والإشراف لكلية الدراسات العليا بجامعة السلطان قابوس، ندوة الدراسات العليا بجامعات دول مجلس التعاون لدول الخليج العربي. **ملخصات بحوث جامعة الملك فيصل**، 2006.

[11] بكرو، خالد. (2017). أهمية البنية التحتية التقنية في التحول إلى الجامعة الذكية. المجلة الدولية المحكمة للعلوم الهندسية وتقنية المعلومات، مج4، ع1، 1-5.

[12] جبران، عامر سعد أحمد؛ المساجدي، خالد. (2023). تصور مقترح لتطبيق الذكاء الاصطناعي في الجامعات اليمنية. **مجلة العلوم الهندسية والتقنية**، مج2، ع1، 71-91.

[13] حربا، علي منير؛ شعبان، أريج. (2024). تصور مقترح لاستخدام تطبيقات الذكاء الاصطناعي في التعليم العالي. **مجلة جامعة البعث**، مج46، ع16، 11-56.

[14] زقوت، نشوة إسماعيل؛ السائح، سناء؛ العطاب، الصديق. (2022). مدى وعي أعضاء هيئة التدريس بالجامعات الليبية بأهمية الأمن السيبراني في ظل التحول الرقمي: دراسة تطبيقية بجامعة الزاوية. **المجلة الدولية للعلوم والتقنية، المؤتمر العلمي الأول لتقنية المعلومات وعلوم الحاسوب**، 21-2022/2/22.

[15]عباس، رياض عزيز. (2020). اتجاه طلبة الجامعة نحو الذكاء الاصطناعي وعلاقته بالتوجه نحو المستقبل لدى طلبة الجامعة. **مجلة الآداب**، ع135.

[16] قرار رئيس مجلس الوزراء رقم (40) لسنة (2008) **بشأن نظام الدراسات العليا في الجامعات اليمنية**، المادة (12) و(13).

[17] قصقصي، حلوة جبر. (2024). مقترحات تفعيل الذكاء الاصطناعي في الجامعات داخل الخط الأخضر من وجهة نظر أعضاء هيئة التدريس. **مجلة الشرق الأوسط للعلوم التربوية والنفسية**، مج4، ع1.

[18] كليبي، نعمة ناصر؛ سلامي، هدى جبريل. (2020). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة. مجلة تطوير الأداء الجامعي، جامعة المنصورة، مج12، ع1، 217-233.

[19] قتيبة، مازن عبد المجيد. (2009). **استخدامات الذكاء الصناعي في تطبيقات الهندسة الكهربائية**. رسالة ماجستير غير منشورة، الدنمارك.

ثانيًا: المراجع الأجنبية:

[1] Contact North. (2018). Ten facts about artificial intelligence in teaching and learning.**https://teachonline.ca/sites/default/files/toolstrends/downloads/ten_facts_about_artificial_intelligence**.

[2] EDUCAUSE. (2018). Horizon report: 2018 higher education edition. Retrieved from EDUCAUSE Learning Initiative and The New Media Consortium website: **https://library.educause.edu/~/media**

/files/library/2018/8/2018horizonreport.

[3] Goutam, R. K., & Verma, D. K. (2015). Top Five Cyber Frauds. **International Journal of Computer Applications**, 119(7), p23 - 25.

[4] Li, J. H. (2018). Cyber security meets artificial intelligence: a survey. **Frontiers of Information Technology & Electronic Engineering**, 19(12), 1462-1474.

[5] MarketsandMarkets. (2020). **Artificial Intelligence Market by Offering, Technology, Deployment Mode, Organization Size**, Industry Vertical, and Region - Global Forecast to 2025.

[6] Ocaña-Fernandez, Y., Valenzuela-Fernandez, L., & Garro- Aburto, L. (2019). Artificial Intelligence and its Implications in Higher Education. Propósitos y Representations. 7(2), 536-568. **http://dx.doi.org/10.20511/pyr2019.v7n2.274.**

[7] Popenici, S. A., & Kerr, S. (2017). Exploring the impact of artificial intelligence on teaching and learning in higher education. **Research and Practice in Technology Enhanced Learning**, 12(1), 22.

التقارير الدولية:

1. (ISC², 2023). تقرير فجوة الكوادر في الأمن السيبراني، **https://www.isc2.org**.
2. (World Economic Forum, 2023). تقرير المخاطر السيبرانية، **https://www.weforum.org**.

الملاحق

ملحق رقم (1): الخطة الدراسية لبرنامج ماجستير "أمن سيبراني وذكاء اصطناعي" بالجامعات اليمنية:

الفصل الدراسي الأول							
م	اسم المقرر	طبيعة المقرر	رمز المقرر	الساعات المعتمدة			إجمالي الساعات المعتمدة
				نظري	عملي	تمارين/ سمنار	
1	تعلم الآلة والتعلم العميق	-	-	2	1	-	3
2	طرق البحث المتقدم	-	-	2	-	1	3
3	مواضيع متقدمة في القرصنة الأخلاقية	-	-	2		1	3
4	أمن الأنظمة الذكية	-	-	2	1	-	3
5	معالجة اللغة الطبيعية (NLP)	-	-	2	1	-	3
إجمالي عدد المقررات والساعات		5	-	10	3	2	15
الفصل الدراسي الثاني							
م	اسم المقرر	طبيعة المقرر	رمز المقرر	الساعات المعتمدة			إجمالي الساعات المعتمدة
				نظري	عملي	تمارين/ سمنار	
1	التشفير المتقدم (Advanced Cryptography)	-	-	2	1	-	3
2	أمن إنترنت الأشياء (IoT Security)	-	-	2	1	-	3
3	الذكاء الاصطناعي في الأمن السيبراني	-	-	2		1	3
4	الذكاء الاصطناعي التطبيقي (Applied AI)	-	-	2	1	-	3
5	أمن الشبكات المتقدمة	-	-	2	1	-	3
إجمالي عدد المقررات والساعات		5	-	10	4	1	15
رسالة الماجستير							6
إجمالي عدد الساعات المعتمدة للبرنامج							36

ملحق رقم (2): توصيف مختصر للمقررات الدراسية لبرنامج ماجستير "أمن سيبراني وذكاء اصطناعي" بالجامعات اليمنية:

م	اسم المقرر	وصف المقرر	عدد الساعات
1	**تعلم الآلة والتعلم العميق** **Machine Learning & Deep Learning**	يهدف هذا المقرر إلى تزويد الطلبة بالمفاهيم والمهارات لتعلم الآلة التطبيقي واستخراج البيانات، ويركز على تطبيق أحدث خوارزميات الذكاء الاصطناعي والتعلم الآلي لحل مشكلات العالم الحقيقية لاكتشاف الأنماط المخفية أو تحديد الحالات الشاذة في البيانات المتولدة في شبكات تكنولوجيا المعلومات الحديثة، وتطبيق نماذج التعلم العميق على عدة مشكلات حقيقية، مثل: معالجة الصور واللغة، وتشمل الموضوعات إعداد البيانات، والتدريب، والتقييم، والمعايير، والتعلم الخاضع للإشراف (الانحدار، والتصنيف، والشبكات العصبية، والتعلم العميق، والشبكات العصبية التلافيفية (CNNs)، والشبكات العصبية المتكررة (RNNs)، وأساسيات التعلم غير الخاضع للإشراف والتعلم المعزز، وأنظمة التوصية، وأساسيات TensorFlow وPyTorch، ونماذج توليدية (GANs)، ونماذج Transformers، ودراسة حالات من أبحاث حديثة في المجال. (جامعة الدوحة للعلوم والتكنولوجيا https://www.udst.edu.qa)	3
2	**طرق البحث المتقدم** **Advance Research Method**	يهدف هذا المقرر إلى تطوير مهارات الطلبة في مناهج البحث العلمي والأبحاث المتعلقة بالأمن السيبراني والذكاء الاصطناعي، وتقليل الفجوة بين النظريات العلمية التي اكتسبها الطلبة من خلال المقررات السابقة والمجال البحثي للعملية المطلوبة، ويتضمن المقرر التقنيات النظرية والمهارات المتقدمة لتحديد وتقديم الحل لمشكلات البحث النوعي والكمي، والحاجة إلى تحليل البيانات العددية وغير العددية، وكيف يمكن أن يسمح جزء من المنهجية بتحليل متعمق للمسائل والعلاقات المعقدة، ويتم تغطية استخدام التحليل العددي للبيانات النوعية لإيجاد حلول وتوصيات ذات دلالة، كما يتضمن المقرر التصميم التجريبي وأخذ العينات، والقياس، والتحليل، وأخلاقيات البحث العلمي، وكيفية كتابة البحوث العلمية والنشر في المجلات العلمية، ومكونات الورقة البحثية، ويقدم هذا المساق تفصيلًا عن كيفية كتابة الرسائل الجامعية وإجراء التجارب وكتابة النتائج والتقارير. (جامعة الدوحة للعلوم والتكنولوجيا https://www.udst.edu.qa)	3
3	**مواضيع متقدمة في القرصنة الأخلاقية**	يهدف هذا المقرر إلى تطوير فهم الطلبة لأدوات القرصنة الأخلاقية لتطوير المهارات والتقنيات لتحديد نقاط ضعف المضيف والشبكة، كما يوفر للطلبة الفهم لنطاق اختبارات الاختراق ومسؤوليات إجراء هذه الاختبارات باتباع مدونة أخلاقية صارمة، إضافة إلى استخدام مجموعة من أدوات البرمجيات الحديثة لأداء مهام اختبار الاختراق المختلفة على مزودات الخدمة، وكيفية تنفيذ آليات دفاع مناسبة للتخفيف من المشكلات المحددة ومعالجتها. (جامعة الزرقاء https://www.zu.edu.jo)	3

م	اسم المقرر	وصف المقرر	عدد الساعات
4	**أمن الأنظمة الذكية (Intelligent Systems)**	يهدف هذا المقرر إلى تطوير قدرات ومهارات الطلبة على تصميم أنظمة ذكية آمنة متكاملة (الروبوتات، أنظمة التوصية)، ودمج تقنيات الذكاء الاصطناعي مع أنظمة صنع القرار، ويتضمن خوارزميات البحث (Search Algorithms)، ونظم الخبراء (Expert Systems)، والتخطيط الآلي (Automated Planning)، كما يركز على تحليل الثغرات الأمنية في نماذج الذكاء الاصطناعي، وتصميم آليات دفاع ضد الهجمات الخبيثة (Adversarial Attacks)، وهجمات التزييف (Model Poisoning)، وحماية بيانات التدريب، وبعض الأدوات، مثل: IBM Adversarial Robustness Toolbox. (جامعة الملك عبدالله KAUST https://cemse.kaust.edu.sa)	3
5	**معالجة اللغة الطبيعية (NLP)**	يهدف هذا المقرر إلى تعزيز فهم الطلبة لتقنيات وتحليل النصوص، والخصائص والتقنيات الكمية الحديثة في معالجة اللغات الطبيعية، والإجابة عن الأسئلة، ونماذج الشبكات العصبية لمهام فهم اللغة، وتوليد اللغة الطبيعية، وتطبيقات في Chatbots، والترجمة الآلية، ونماذج Transformer (مثل BERT, GPT)، وتحليل المشاعر (Sentiment Analysis) باستخدام Python وNLTK. (جامعة أكسفورد University of Oxford: NLP Course) https://www.cs.ox.ac.uk)	3

	اسم المقرر	وصف المقرر	عدد الساعات
1	**التشفير المتقدم (Advanced Cryptography)**	يهدف هذا المقرر إلى توفير نظرة عامة وشاملة للطلبة حول طرق وتقنيات التشفير وفك التشفير، وسيتعلّم الطلبة من خلاله مبادئ نظرية الأعداد، ومبادئ الاحتمالات والإحصاء، ومبادئ الجبر الخطي، والتشفير بالمنحنيات الإهليلجية RSA وAES، وحزمة الخوارزميات غير العسكرية وغير السرية Suite B، وأنواع الهجمات التي يتعرض لها التشفير، مثل: التحليل التفاضلي للتشفير، وهجوم الرجل في الوسط، والتحليل الخطي، وتجزئة التوقيعات الرقمية، وإدارة المفاتيح، والتحليل التقليدي والكلاسيكي للتشفير، والهجمات الجانبية، مثل: هجمات التوقيت وهجمات استهلاك الطاقة، والهجمات عن طريق تحليل اختلاف الأخطاء، والتشفير المستند إلى الهوية، والتوقيع الرقمي، والشبكات الافتراضية الخاصة، والحوسبة الكمومية والتشفير، إضافة إلى المفاتيح العامة والخاصة، والبروتوكولات، ومولدات الأرقام، والتوقيعات الرقمية. (جامعة الأميرة سمية للتكنولوجيا https://www.psut.edu)	3
2	**أمن إنترنت الأشياء (IoT Security)**	يهدف هذا المقرر إلى توفير المعرفة وتطوير الفهم لدى الطلبة لكيفية تأمين الأجهزة المتصلة بالإنترنت (مثل: الكاميرات الذكية، أجهزة المنزل الذكي)، وتحليل الثغرات	3

	اسم المقرر	وصف المقرر	عدد الساعات
		في بروتوكولات الاتصال (مثل: MQTT)، وهجمات IoT الشائعة (مثل: Mirai Botnet)، وتقنيات التشفير لأجهزة IoT محدودة الموارد. (جامعة الخليج العربي agu_aru@agu.edu.bh)	
3	**الذكاء الاصطناعي في الأمن السيبراني**	يهدف هذا المقرر إلى تطوير فهم ومهارات الطلبة لكيفية استخدام تقنيات الذكاء الاصطناعي في اكتشاف الهجمات الإلكترونية، وتطوير أنظمة IDS/IPS ذكية، ويتضمن المقرر تدريب الطلبة على خوارزميات التعلم غير الخاضع للإشراف (Unsupervised Learning) لكشف الشذوذ، وأيضًا تدريبهم على بعض الأدوات، مثل: TensorFlow، لبناء نماذج كشف التهديدات. (جامعة IBM SkillsBuild https://skillsbuild.org)	**3**
4	**الذكاء الاصطناعي التطبيقي Applied AI**	يهدف هذا المقرر إلى تزويد الطلبة بالمفاهيم المتقدمة في مجال الذكاء الاصطناعي وتطبيقاته المتقدمة، ويغطي المقرر الموضوعات التالية: النواحي النظرية في هندسة المعرفة، الاستنباط، السببية الرمزية، البحث، التصنيف الإحصائي للأنماط، النمذجة الإدراكية، الواجهات التحاورية المتقدمة، التخطيط، معالجة الصور بالحاسوب، البرمجة التلقائية، تعلم الآلة، الخوارزميات التطورية، الذكاء الاصطناعي الموزع والمتوازي، تطبيق خوارزميات الذكاء الاصطناعي في بعض المجالات، مثل: الطاقة والبيئة، استخدام بعض الأدوات (مثل: MATLAB وPython) في نمذجة المشكلات. (جامعة الملك عبدالله للعلوم والتقنية https://www.kaust.edu.sa) (KAUST)	**3**
5	**أمن الشبكات المتقدمة**	يهدف هذا المقرر إلى تطوير فهم ومهارات الطلبة في مجالات أمن الشبكات المتقدمة، حيث يتناول المقرر القضايا الرئيسة في اتصالات البيانات وأمن الشبكات وكيفية الوصول إلى المعلومات، وأهم المواضيع التي سيتم تغطيتها في هذا المساق هي: تعريف الأمان وأمن الشبكة والتوقيعات الرقمية وأمان IP وطبقة المقبس الآمن، وكشف التسلل، والمصادقة، وجدران الحماية، ورفض الخدمة، والبريد العشوائي، وفيروسات البريد الإلكتروني، والتصيد الاحتيالي، ونظرة عامة حول العديد من الهجمات التي تتعرض لها الشبكات والطرق المتناسبة للتعامل معها ومنعها، وتصميم شبكات مقاومة للاختراقات باستخدام تقنيات حديثة، وتحليل حركة المرور الشبكية لاكتشاف الهجمات، وبروتوكولات التشفير (IPSec, SSL/TLS)، وبعض الأدوات (مثل: Wireshark) لتحليل الحزم. (جامعة Carnegie Mellon University https://www.sei.cmu.edu)	**3**
	رسالة الماجستير		**6**