Spectrum Journal of Innovation, Reforms and Development
Volume 43, September 2025 | ISSN (E): 2751-1731
WEBSITE: WWW.SJIRD.JOURNALSPARK.ORG

CYBERSECURITY SKILLS AT THE PERSONAL AND INSTITUTIONAL DOMAINS IN PROTECTING MANAGEMENT INFORMATION SYSTEMS: AN APPLIED STUDY

Assistant Lecturer Zahraa falih oudah
Ministry of Higher Education and Scientific Research
Department of Construction and Projects
Email : zahraa.f@mohesr.edu.iq

Abstract

The research aimed to identify the cybersecurity skills necessary for protecting management information systems among students of Management Information Systems faculties at both the personal and institutional domains, and to assess the students' proficiency in these skills, identify the major challenges impeding their development, and suggest appropriate strategies for their enhancement, The research sample consisted of (32) male and female students from the fourth year at a Management Information Systems college in one of the Iraqi universities, The research tool was a questionnaire designed to measure cybersecurity skills at both the personal and institutional domains, The statistical analysis revealed a relative deficiency in some cybersecurity skills compared to the assumed average (4) on the five-point Likert scale, with major challenges identified, including lack of technical expertise and limited practical training opportunities, The research recommended the integration of cybersecurity skills into academic curricula and the design of continuous training programs to enhance students' cybersecurity awareness and skills.

Keywords: Cybersecurity; Cybersecurity skills; Management Information Systems.

Introduction

Protecting information has become a fundamental challenge for organizations, especially administrative ones, given their increasing reliance on digital systems. This makes cybersecurity skills essential for building digital resilience to counter cyber threats targeting sensitive data and systems.

The rise in threats and the sophistication of attacks necessitates the development of advanced cybersecurity skills that combine theory and practice (Alhogail, 2022; Alshaikh, 2023). This is especially true with the average cost of a data breach reaching $4.88 million, exceeding $6.08 million in vital sectors, resulting in financial and reputational losses (IBM, 2024). In light of this growing threat, a significant professional gap is evident in the field of cybersecurity, with approximately 4.8 million unfilled jobs globally in 2024, reflecting a severe shortage of skilled professionals (ISC², 2024). The need is not limited to technical specializations, but also includes

administrative fields that require skills that support decision-making, risk analysis, and information infrastructure protection.

In this context, cybersecurity is no longer merely a limited field of expertise. It has become a strategic necessity at the institutional and national levels, especially in light of the global digital transformation, which has made data and information protection a pillar of national, economic, and social security. Countries with a strong cyber infrastructure are able to protect their national capabilities and provide a secure environment for growth, investment, and sustainable development. Cybersecurity has become a strategic necessity for countries and institutions in light of the digital transformation, given its role in protecting national security and promoting growth and investment (Alshehri, 2023.(

Universities are among the most targeted targets, with more than 65% of them being subjected to attacks in recent years (Cybersecurity Ventures, 2023). Meanwhile, training students in cybersecurity skills can reduce these attacks by 45% and improve institutional response (Ponemon Institute, 2023; Cybersecurity and Higher Education Report, 2024). The importance of integrating cybersecurity skills into management information systems programs is highlighted to prepare cadres capable of protecting academic and administrative systems from hacking, especially with the widespread reliance on digital platforms. The need lies in integrating administrative technology concepts with digital security through curriculum development and practical training. Hence, the study aims to analyze the reality of these skills, identify challenges, and propose a practical vision for enhancing cybersecurity in the university environment in general, and specifically in the College of Administrative Systems, the subject of the current research.

مستخلص البحث:

العنوان: مهارات الأمن السيبراني على المستويين الشخصي والمؤسسي في حماية نظم المعلومات الإدارية: دراسة تطبيقية

هدف البحث إلى الكشف عن مهارات الأمن السيبراني اللازمة لحماية نظم المعلومات الإدارية لدى طلاب كليات نظم المعلومات الإدارية على المستويين الشخصي والمؤسسي، والتعرف على مستوى توافر هذه المهارات لديهم، والكشف عن أبرز التحديات التي تعوق تنميتها، مع اقتراح السبل المناسبة لتعزيزها. تكونت عينة البحث من (32) طالبًا وطالبة من طلاب الفرقة الرابعة بكلية نظم المعلومات الإدارية بإحدى الجامعات العراقية، وتمثلت أداة البحث في استبانة معدة لقياس مهارات الأمن السيبراني الشخصية والمؤسسية. وقد أسفرت نتائج المعالجة الإحصائية عن وجود قصور نسبي في بعض المهارات السيبرانية مقارنة بالمتوسط الافتراضي (4) على مقياس ليكرت الخماسي، مع بروز تحديات أساسية أبرزها ضعف الخبرة التقنية وقلة فرص التدريب العملي، وأوصى البحث بضرورة دمج مهارات الأمن السيبراني ضمن المناهج الدراسية، وتصميم برامج تدريبية مستمرة لتعزيز الوعي الأمني والمهارات السيبرانية لدى الطلاب.

الكلمات المفتاحية: الأمن السيبراني؛ مهارات الأمن السيبراني؛ نظم المعلومات الإدارية.

الفصل الأول (الإطار العام للبحث):

مقدمة:

أصبحت حماية المعلومات تحديًا جوهريًا للمؤسسات، خاصة الإدارية منها، في ظل اعتمادها المتزايد على الأنظمة الرقمية، مما يجعل مهارات الأمن السيبراني ضرورة لبناء حصانة رقمية تُمكّن من التصدي للتهديدات الإلكترونية الموجهة للبيانات والأنظمة الحساسة.

إنَ تزايد التهديدات وتعقيد الهجمات يفرض تأهيل الكوادر بمهارات سيبرانية متقدمة تمزج بين النظرية والتطبيق(Alhogail, 2022; Alshaikh, 2023) ، خاصة مع بلوغ متوسط تكلفة اختراق البيانات 4.88 مليون دولار، وتجاوزها 6.08 مليون دولار في القطاعات الحيوية، نتيجة الخسائر المالية والسمعة المؤسسية (IBM, 2024)، وفي ظل هذا التهديد المتصاعد، يُلاحظ وجود فجوة مهنية كبيرة في مجال الأمن السيبراني، حيث بلغ عدد الوظائف الشاغرة عالميًا نحو 4.8 مليون وظيفة في عام 2024، مما يعكس عجزًا حادًا في الكفاءات المتخصصة بهذا المجال(ISC², 2024) .

ولا تقتصر الحاجة على التخصصات التقنية، بل تشمل المجالات الإدارية التي تتطلب مهارات تدعم اتخاذ القرار وتحليل المخاطر وحماية البنية المعلوماتية.

وفي هذا السياق، لم يعد الأمن السيبراني مجرد مجال تخصصي محدود، بل تحول إلى ضرورة استراتيجية على مستوى المؤسسات والدول، خصوصًا في ظل التحول الرقمي العالمي، الذي جعل من حماية البيانات والمعلومات أحد أعمدة الأمن القومي والاقتصادي والاجتماعي؛ فالدول التي تمتلك بنية سيبرانية قوية قادرة على حماية مقدراتها الوطنية، وتوفير بيئة آمنة للنمو والاستثمار والتنمية المستدامة، وأصبح الأمن السيبراني ضرورة استراتيجية للدول والمؤسسات في ظل التحول الرقمي، لما له من دور في حماية الأمن القومي وتعزيز النمو والاستثمار(Alshehri, 2023) .

وتُعد الجامعات من أكثر الأهداف استهدافًا، إذ تعرض أكثر من 65% منها لهجمات خلال السنوات الأخيرة(Cybersecurity Ventures, 2023) ، في حين يساهم تدريب الطلاب على المهارات السيبرانية في تقليل هذه الهجمات بنسبة 45% وتحسين استجابة المؤسسات (Ponemon Institute, 2023; Cybersecurity and Higher Education Report, 2024).

وتبرز أهمية دمج مهارات الأمن السيبراني في برامج نظم المعلومات الإدارية لإعداد كوادر قادرة على حماية النظم الأكاديمية والإدارية من الاختراق، خاصة مع الاعتماد الواسع على المنصات الرقمية.

وتكمن الحاجة في تكامل مفاهيم التقنية الإدارية مع الحماية الرقمية، عبر تطوير المناهج والتدريب العملي، ومن هنا تهدف الدراسة إلى تحليل واقع تلك المهارات، وتشخيص التحديات، واقتراح تصور تطبيقي لتعزيز الأمن السيبراني في البيئة الجامعية بصفة عامة وبالتطبيق علي كلية النظم الإدارية محل البحث الحالي بصفة خاصة

(1-1) الإحساس بالمشكلة:

أولًا: أكدت الدراسات الحديثة أهمية تنمية مهارات الأمن السيبراني لدى طلاب الجامعات، خاصة في التخصصات الإدارية، لدورها في حماية نظم المعلومات، مثل دراسات(2023) Abuhussein ، Alhogail (2022)، و(2024) Alotaibi & Alshammari، والتي أوصت بإدماج الأمن السيبراني في البرامج الجامعية. كما أشارت مؤتمرات مثل *Cybersecurity and Privacy Professionals Conference (2023)*و *Inscrypt 2024*إلى ضرورة تأهيل الطلاب بمهارات سيبرانية أساسية.

ثانيًا: تصاعدت التهديدات السيبرانية في العالم العربي، وخصوصًا العراق، مما يكشف ضعف البنية الرقمية؛ حيث أشار تقرير ITU (2024) إلى احتلال العراق المرتبة 127 عالميًا في مؤشر الأمن السيبراني بدرجة 53.07، ما يدل على فجوة تنظيمية وتشريعية واضحة.

ثالثًا: من واقع خبرة الباحث وملاحظاته المباشرة، تبيّن وجود ضعف ملحوظ لدى الطلاب في ممارسات الحماية الرقمية، خاصة في إدارة الحسابات وتأمين البيانات الأكاديمية.

رابعًا: تشير الاتجاهات العالمية إلى أن الأمن السيبراني لم يعد تخصصًا تقنيًا فقط، بل أصبح جزءًا من الكفاءة المهنية في تخصصات نظم المعلومات الإدارية، مما يستدعي دراسة هذا المجال في السياق الجامعي العراقي.

(2-1) **مشكلة البحث:**

يتضح مما سبق تدني مستوى مهارات الأمن السيبراني، وانخفاض مستوى الوعي تجاهه لدى الطلاب الجامعيين بصفة عامة، ولدى طلاب كليات نظم المعلومات الإدارية بصفة خاصة.

وتتحدد مشكلة البحث في السؤال الرئيس التالي:

ما مهارات الأمن السيبراني على المستويين الشخصي والمؤسسي اللازمة لحماية نظم المعلومات الإدارية؟

ويتفرع من هذا السؤال الرئيس الأسئلة الفرعية الآتية:

1. ما مهارات الأمن السيبراني اللازم توافرها لدى طلاب نظم المعلومات الإدارية على المستوى الشخصي؟
2. ما مهارات الأمن السيبراني اللازم توافرها لدى طلاب نظم المعلومات الإدارية على المستوى المؤسسي؟
3. ما مستوى طلاب نظم المعلومات الإدارية في مهارات الأمن السيبراني على المستوى الشخصي مقارنة بالمتوسط الافتراضي (4)؟
4. ما مستوى طلاب نظم المعلومات الإدارية في مهارات الأمن السيبراني على المستوى المؤسسي مقارنة بالمتوسط الافتراضي (4)؟
5. ما أبرز التحديات التي تعوق تنمية مهارات الأمن السيبراني لدى طلاب نظم المعلومات الإدارية ؟
6. ما السبل المقترحة لتعزيز المهارات السيبرانية لطلاب الجامعات بما يدعم حماية نظم المعلومات الإدارية؟

(3-1) **أهداف البحث:**

1. التعرف علي مهارات الأمن السيبراني اللازم توافرها لدى طلاب نظم المعلومات الإدارية على المستوى الشخصي.
2. التعرف علي مهارات الأمن السيبراني اللازم توافرها لدى طلاب نظم المعلومات الإدارية على المستوى المؤسسي.
3. التعرف على مستوى طلاب نظم المعلومات الإدارية في مهارات الأمن السيبراني على المستوى الشخصي.
4. التعرف على مستوى طلاب نظم المعلومات الإدارية في مهارات الأمن السيبراني على المستوى المؤسسي.
5. التعرف علي أبرز التحديات التي تعوق تنمية مهارات الأمن السيبراني لدى طلاب التعليم الجامعي.
6. التعرف علي السبل المقترحة لتعزيز المهارات السيبرانية لطلاب الجامعات بما يدعم حماية نظم المعلومات الإدارية.

(4-1) **أهمية البحث:** تبرز أهمية البحث من خلال:

- مواكبته لتوجهات تطوير المناهج الجامعية بإدماج أمن المعلومات ضمن المحتوى التعليمي.
- دعم صناع القرار في وزارتي التعليم العالي والبحث العلمي في تعزيز الأمن السيبراني أكاديميًا.

- التركيز على دمج المهارات السيبرانية في برامج كليات نظم المعلومات الإدارية للحد من التهديدات المؤسسية.
- رفع وعي الطلاب بدور الأمن السيبراني كمهارة عملية أساسية.
- تنمية المهارات الرقمية للطلاب بما يعزز ثقافة الحماية المجتمعية.
- تقديم قائمة مفاهيم ومهارات مرجعية لتخطيط المناهج.
- اقتراح أدوات قياس علمية لتقييم الجوانب المعرفية والمهارية.
- توفير إطار لتصميم برامج تدريبية موجهة للطلاب وأعضاء هيئة التدريس.
- طرح توصيات قابلة للتطبيق تسهم في فتح آفاق لبحوث مستقبلية في المجال.

(5-1) **محددات البحث:** اقتصر البحث الحالي على الحدود التالية:

- حدود موضوعية :تناول المهارات الأساسية في الأمن السيبراني على المستويين الشخصي والمؤسسي، المتعلقة بحماية نظم المعلومات الإدارية في بيئات التعليم الجامعي.
- حدود بشرية :عينة عشوائية مكونة من (32) طالبًا وطالبة من طلاب الفرقة الرابعة بكليات نظم المعلومات الإدارية بإحدى الجامعات العراقية.
- حدود زمنية: الفصل الدراسي الثاني من العام الجامعي 2025/2024م.
- حدود مكانية: إحدى كليات نظم المعلومات الإدارية في الجامعات العراقية.

(6-1) **مجتمع وعينة البحث:**

شمل مجتمع البحث طلاب كلية النظم الإدارية بإحدى الجامعات العراقية، وتم اختيار عينة عشوائية من طلاب الفرقة الرابعة (32 طالبًا وطالبة) خلال الفصل الثاني للعام الجامعي 2025/2024م.

(7-1) **منهج البحث:**

اعتمد الباحث المنهج التطبيقي لدراسة واقع مهارات الأمن السيبراني لدى طلاب النظم الإدارية، بهدف الوصول إلى نتائج قابلة للتطبيق في البيئة الجامعية.

(8-1) **أدوات ومواد البحث:**

1. قائمة بمهارات الأمن السيبراني علي المستويين الشخصي، والمؤسسي.
2. استبانة لقياس مهارات الأمن السيبراني علي المستويين الشخصي، والمؤسسي لدي طلاب كلية النظم الإدارية.

(9-1) **مصطلحات البحث اجرائيًا:**

1- الأمن السيبراني Cybersecurity:

هو الإجراءات والآليات المستخدمة لحماية الشبكات والأجهزة والبيانات من التهديدات على المستوى الشخصي والمؤسسي.

2- مهارات الأمن السيبرانيCybersecurity skills :

المعارف والقدرات التي تُمكّن الطلاب من حماية أنفسهم ومؤسساتهم من المخاطر السيبرانية.

3- نظم المعلومات الإدارية:

أنظمة رقمية تُستخدم في إدارة ومعالجة البيانات الخاصة بالعمليات الإدارية داخل المؤسسات.

(10-1) **اجراءات البحث:**

1. إعداد الإطار النظري: مراجعة الأدبيات والدراسات السابقة ذات الصلة بمهارات الأمن السيبراني وحماية نظم المعلومات الإدارية.
2. بناء أدوات البحث: إعداد قائمة مهارات الأمن السيبراني علي المستويين الشخصي، والمؤسسي، واستبيان لقياس مدى توافر هذه المهارات عند طلاب نظم المعلومات الإدارية، والتحديات التي تعوق سبب ضعف المهارات وسبل مواجهتها.
3. تحكيم أدوات البحث: عرض الأدوات على مجموعة من المحكّمين من المتخصصين في مجالي الأمن السيبراني والعلوم الإدارية للتأكد من صدقها ومناسبتها لعينة البحث.
4. تطبيق أدوات البحث: تطبيق الاستبيان على عينة البحث المكونة من طلاب الفرقة الرابعة بكلية نظم المعلومات الإدارية.
5. جمع البيانات: جمع استجابات الطلاب وتحليل نتائج تطبيق الأدوات.
6. معالجة البيانات إحصائيًا: استخدام الأساليب الإحصائية المناسبة لتحليل النتائج والإجابة عن أسئلة البحث.
7. تفسير النتائج: تفسير النتائج في ضوء أهداف البحث وأسئلته.
8. صياغة التوصيات والمقترحات:بناءً على النتائج المتحصل عليها.

(11-1) **المعالجة الإحصائية:**

:اعتمد الباحث على مجموعة من الأساليب الإحصائية المناسبة لطبيعة البحث، وهي

(One-Sample T-Test) المتوسطات الحسابية والانحرافات المعيارية لقياس مستويات الأداء، اختبار "ت" لعينة واحدة ؛ لقياس مدى دلالة الفروق بين المتوسطات المفترضة والواقعية، تحليل الارتباط (Pearson Correlation) لقياس العلاقة بين مهارات الأمن السيبراني ومستوى الوعي الأمني لديهم.

الفصل الثاني: الإطار النظري والدراسات السابقة:

(2-1) أساسيات الأمن السيبراني:

(2-1-1) مفهوم الأمن السيبراني: يعود أصل مصطلح "سايبر" إلى "Cybernetics" الذي طرحه فينر (Wiener, 1948) ، في إشارة إلى النظم القائمة على التغذية الراجعة في التحكم والتواصل، وقد امتد الأمن (U.S. DoD, 2018) المفهوم ليشمل النظم الرقمية الحديثة؛ حيث عرّفت وزارة الدفاع الأمريكية السيبراني بأنه إجراءات تنظيمية لحماية المعلومات من التخريب والتجسس، مما يبرز الجانب الوقائي على كفاءة المستخدم داخل المؤسسات، موضحة أن Nilsen et al. (2017) للمجال، وركّزت دراسة نقص المعرفة والمهارات والقدرات يشكل ثغرة خطيرة، ويُنظر إلى الأمن السيبراني عمومًا كإجراءات تقنية وإدارية لضمان حماية وسرية وسلامة البيانات، وهو ما يتفق مع التعريف الإجرائي المعتمد في هذا البحث.

(2-1-2) نشأة الأمن السيبراني: برزت الحاجة للأمن السيبراني نتيجة توسع استخدام الأنظمة الرقمية في مجالات حيوية، وما صاحب ذلك من تهديدات متزايدة للخصوصية والبيانات (Cameron & Marcum, 2019) وساهم ضعف البنية التحتية ونقص المهارات في تفاقم المخاطر، مما دفع المؤسسات لاعتماد برامج وقائية ، وتدريبية (Ramezan, 2023) ، كما طورت الحكومات استراتيجيات وطنية لمواجهة تحديات التحول الرقمي أن تعدد مجالات Ramezan (2023) ، وقد أوضحت دراسة (Alotaibi & Alshammari, 2024) الأمن السيبراني يتطلب تطويرًا مستمرًا للمهارات، إذ يشكل ضعف كفاءة المستخدمين تهديدًا حقيقيًا رغم وجود أدوات حماية متقدمة، وهو ما يستدعي تدريبًا وتقييماً عمليًا دوريًا

تاريخيًا، مر الأمن السيبراني بمراحل تطور بدأت من الأربعينيات مع ظهور الحاسوب، وبرزت التهديدات تدريجيًا مع تطور الفيروسات وبرامج الاختراق، حتى وصلت إلى ذروتها في القرن الحالي مع اعتماد الذكاء الاصطناعي في الحماية (الزهراني، 2020؛ الجبوري، 2021؛ العزاوي، 2020؛ الدوسري، 2021؛ عبد الرحيم، 2022)، وهذا يؤكد ما ورد في المقدمة حول الحاجة العاجلة لتأهيل الكوادر البشرية ومواجهة ضعف ممارسات الحماية الرقمية.

(3-1-2) أهمية وأهداف الأمن السيبراني:

يمثل الأمن السيبراني ركيزة أساسية لحماية المصالح الحيوية للأفراد والمؤسسات والدول، ويعكس قدرة الدولة على حماية أمنها وبيئتها الرقمية (راشد المري، 2023).

- فرديًا: يضمن حماية البيانات الشخصية من السرقة والاحتيال، ويعتمد على ممارسات كإدارة كلمات المرور والتحديثات المستمرة.

- مؤسسيًا: يحمي الأنظمة من الهجمات والفيروسات، ويُعد الاستثمار في التقنيات الحديثة وتدريب الموظفين أمرًا ضروريًا (Agrawal et al., 2020).

- حكوميًا: يعزز حماية البنية التحتية الحساسة، ويتطلب سياسات تنظيمية وجهودًا تشاركية مع القطاع الخاص.

- دوليًا: نظراً لطبيعة الهجمات العابرة للحدود، أصبح التعاون الدولي في الأمن السيبراني ضروريًا لمواجهة الحروب السيبرانية المتزايدة (Taha, 2022) .

أن الذكاء الاصطناعي يسهم في أتمتة الحماية، واكتشاف Dambe et al. (2023) كما بيّنت دراسة التهديدات، وتحليل الثغرات، وتحسين عمليات التدقيق، مما يجعله أداة فعالة لضمان الأمن والامتثال التنظيمي.

(2-2) مهارات الأمن السيبراني:

استند تصنيف المهارات السيبرانية إلى تقارير دولية متخصصة مثل NICE Framework (Petersen et al., ، التي ركزت على تطوير القوى العاملة وتأهيلها في المجال(ISC)²و ENISAو 2020؛ ENISA, 2023).

ا) حسب مستوى المهارة:

- **الأساسية**: تشمل إدارة كلمات المرور، التعرف على التهديدات، وتطبيق إجراءات الأمان اليومية.
- **المتوسطة**: تتضمن تحليل المخاطر، إدارة الأنظمة، والاستجابة للحوادث.
- **المتقدمة**: تشمل اختبار الاختراق، التحليل الجنائي، وتطوير البرمجيات الآمنة.

ب) حسب التخصص:

- **المتخصصون**: مطلوب منهم مهارات تقنية عميقة وتحليل متقدم واستجابة فورية.
- **غير المتخصصين**: يكتفى بالوعي العام، استخدام المصادقة، والتبليغ عن التهديدات.
- **المستخدمون العاديون**: يجب عليهم التصفح الآمن وتأمين المعاملات والإبلاغ عن التسلط الإلكتروني.

ج) حسب الوظيفة الإدارية:

- موظفو الموارد البشرية والمالية: حماية البيانات وتطبيق السياسات.
- الدعم الإداري: التحقق من الهوية، النزاهة، والتبليغ.
- دعم مؤسسي عام: الالتزام والتعاون والتدريب.

المهارات الأساسيةالتي يجب أن يتقنها الموظفين الاداريين هي: حماية الشبكات، ومما سبق نخلص أن الأجهزة، الأنظمة، الحسابات، واستخدام أدوات الحماية.

لتقييم الكفاءة (MyCyberKSAs™) نموذجًا تطبيقيًا Nilsen et al. (2017) وقد طوّرت دراسة السيبرانية، تضمن 90 مؤشرًا عبر 23 وحدة معرفية و22 مهارة عملية، وحدد معيارًا للنجاح بنسبة 80%. أظهرت النتائج أن التدريب المنتظم وطبيعة الوظيفة يؤثران بوضوح على الكفاءة، مما يبرز أهمية الدمج بين النظرية والتطبيق، ويدعم مشكلة البحث حول القصور في مهارات طلاب نظم المعلومات الإدارية.

(2-3) التكامل بين الأمن السيبراني والمستحدثات التكنولوجية:

في ظل التطور السريع في التقنيات الحديثة كـ"البيانات الضخمة"، و"إنترنت الأشياء"، و"الذكاء الاصطناعي"، أصبح تكامل الأمن السيبراني معها ضرورة لتعزيز حماية الأنظمة الإدارية (Choucri et al., 2013؛ Hoffman & Friedman, 2014؛ Carr, 2016).

- **البيانات الضخمة:** تسهم في تحليل التهديدات وتوقّعها باستخدام الذكاء الاصطناعي، رغم التحديات المرتبطة بضخامة حجمها وتنوع مصادرها، ويمكن التغلب على هذه التحديات بالتشفير والمراقبة الذكية والتدريب المستمر.

- **إنترنت الأشياء:** حسّن الكفاءة الإدارية، لكنه أوجد ثغرات أمنية بسبب تعدد الأجهزة، ويتطلب الحماية عبر المصادقة المتعددة، والتشفير، والإدارة الفعالة للأجهزة.

- **الذكاء الاصطناعي:** أصبح أداة رئيسية في كشف الهجمات وتحليل البرمجيات الضارة، لكنه معرض لهجمات تضليلية عبر التعلم المعاكس، مما يستدعي تطوير أنظمة ذكية للكشف والاستجابة.

وفي الإدارة، يدعم هذا التكامل التحول الرقمي الآمن، ويعزز حماية البيانات التشغيلية، خصوصًا مع الاعتماد على الأجهزة الذكية والخوارزميات التحليلية لرصد السلوكيات المشبوهة، ودمج هذه الابتكارات مع الأمن السيبراني يضمن بيئات مؤسسية أكثر أمانًا، ويستوجب سياسات مرنة، ونماذج حوكمة حديثة، وتدريب الكوادر الإدارية، وهو ما ينسجم مع هدف البحث في إعداد طلاب نظم المعلومات الإدارية لمواجهة تعقيدات البيئة الرقمية بأدوات أمنية متكاملة.

(2-4) الوعي تجاه الأمن السيبراني:

(2-4-1) أهمية الوعي السيبراني لطلاب النظم الإدارية:

في بيئات التعلم الرقمي، يمثل نقص الوعي بالأمن السيبراني ثغرة خطيرة تُعرّض الطلاب لهجمات تصيد وسرقة بيانات، وقد دعت Bellevue University (2018) إلى إدماج الأمن السيبراني في التعليم المبكر لتعزيز الحصانة الرقمية، وأكد Wilshusen (2012) و Crumpler & Lewis (2019) أهمية التوعية المبكرة لمواجهة الفجوة المهارية وضمان الجاهزية لمواجهة التهديدات، بما يتماشى مع مشكلة البحث.

(2-4-2) التحديات الرئيسية:

تواجه الكليات فجوة بين المهارات المطلوبة والمحتوى الأكاديمي، مع نقص التدريب العملي وضعف الشراكات مع القطاعات التكنولوجية(Ramezan, 2023) ، كما أظهر تقرير Cybersecurity and Higher Education (2024) أن 65% من الهجمات استهدفت مؤسسات تعليمية بسبب ضعف الوعي، وأكدت دراسة عبد الله (2023) أن أبرز المعوقات تشمل نقص الدورات والخبرة والتنسيق، مما يستلزم إصلاحًا مزدوجًا في التدريب والمناهج.

(2-4-3) دور كليات النظم الإدارية:

تؤدي الكليات دورًا محوريًا من خلال التعليم النظري والتطبيقي، والتوعية المؤسسية، والتعاون مع القطاع الصناعي، وقد بينت دراسات العتيبي (2022) ، المحمدي (2023) ، القحطاني (2022) ، والحربي (2021) أن البرامج الحالية بحاجة لتحديث، وأن المعلمين بحاجة لتأهيل تخصصي في الأمن السيبراني. وأكدت Khamzina et al. (2022) أهمية الشراكة بين التعليم والصناعة لمعالجة نقص الوعي.

الاستراتيجية المقترحة للكليات تشمل:

1. دمج الأمن السيبراني بالمناهج وتقديم تدريبات تطبيقية.
2. دعم البحث العلمي والمشاريع الميدانية.
3. تنظيم فعاليات توعوية مستمرة.
4. إنشاء مختبرات محاكاة للهجمات.
5. تطوير سياسات حماية مؤسسية.
6. تعزيز الشراكات مع مؤسسات الأمن السيبراني.

وتتماشى هذه الجهود مع أهداف البحث في إعداد طلاب مؤهلين سيبرانيًا لخوض بيئة العمل بأمان رقمي

(5-2): أمثلة لاختراقات الأمن السيبراني في المؤسسات التعليمية (2020-2024)

: هجوم فدية استهدف أبحاث كوفيد-19، أجبر الجامعة على **(2020) جامعة كاليفورنيا - سان فرانسيسكو** دفع 1.14 مليون دولار (BBC, 2020) .

من المؤسسات التعليمية تعرضت لهجمات تصيد، أدت أحيانًا إلى سرقة 76%: **(2020) التصيد الاحتيالي** هوية (Proofpoint, 2021) .

(2021): كلية لينكولن هجوم فدية تسبب في إغلاق الكلية بعد 157 عامًا من العمل (Schellman, 2024) .

عطّل أنظمة التدريس والإدارة BlackCat **:** هجوم فدية من مجموعة**(2022) جامعة ولاية كارولينا الشمالية** (Security Intelligence, 2024) .

،جامعة Azure (Schellman, 2024) **:** تسريب بيانات 250 ألف طالب عبر**(2023) جامعة إنديانا** أدى إلى تسريب معلومات حساسة عن الطلاب MOVEit اختراق منصة **: (2023) تكساس التقنية** والموظفين (Security Affairs, 2023) .

أكدت هذه الحوادث الحاجة إلى تعزيز الأمن السيبراني في الجامعات من خلال تحديث الأنظمة، تأمين أدوات نقل البيانات، ورفع وعي المستخدمين، كما أوضحت الدراسات (ابن إبراهيم، 2021؛ خضر، 2021) أهمية التدريب والتكامل المؤسسي في تقليل المخاطر، مما يعكس ضرورة تطوير سياسات أمنية شاملة تنطلق من الوعي الفردي وتنتهي بالحماية المؤسسية المستدامة.

(6-2): تخصصات ووظائف الأمن السيبراني المرتبطة بخريجي نظم المعلومات الإدارية

إلى أن خريجي نظم المعلومات الإدارية مؤهلون للعمل في عدة Ramezan (2023) تشير دراسة ، التدقيق، التحليل، والعمليات الأمنية، وبيّنت (GRC) مجالات من الأمن السيبراني، مثل: الحوكمة والمخاطر .يُطلب في أكثر من ربع إعلانات الوظائف السيبرانية، ما يؤكد أهمية هذا التخصص MIS أن تخصص

- **ملاءمة خريجي نظم المعلومات الإدارية للأمن السيبراني:**

يمتلك خريجو هذا التخصص مزيجًا من المهارات الإدارية والتقنية، مما يؤهلهم لمسارات مثل تحليل السياسات، الامتثال، التدقيق، وأمن قواعد البيانات. ويتطلب ذلك تطوير المناهج لتشمل مقررات مهنية، وتوسيع فرص التدريب وربطها بسوق العمل السيبراني.

- **تكامل الأمن السيبراني مع التخصصات الإدارية:**

- **المحاسبة :** أدرج معيار A7 من AACSB الأمن السيبراني ضمن مخرجات التعلّم، مع التأكيد على تأمين البيانات وتحليلها(Cameron & Marcum, 2019) .
- **الموارد البشرية :** تُعد من أكثر الأقسام عرضة للهجمات، ويجب على موظفيها إدراك أساليب التصيد والتهديدات الداخلية.

- **التمويل :** يرى Camillo (2017) أن حماية المؤسسات المالية تستلزم استراتيجيات شاملة تمزج بين الأمن، الأخلاقيات، وإدارة المخاطر.

وعلي ذلك يجب دمج الأمن السيبراني في مناهج الإدارة كمكوّن أساسي عبر مقررات تطبيقية ومشروعات تحاكي الواقع، لتهيئة الطلاب لمتطلبات بيئات العمل الرقمية الحديثة.

(7-2): فروض البحث

1. لا توجد فروق ذات دلالة إحصائية عند مستوى (0.05) بين المتوسط الحسابي لمهارات الأمن السيبراني الشخصي لدى طلاب كليات النظم الإدارية والمتوسط الافتراضي(4) .
2. لا توجد فروق ذات دلالة إحصائية عند مستوى (0.05) بين المتوسط الحسابي لمهارات الأمن السيبراني المؤسسي لدى طلاب كليات النظم الإدارية والمتوسط الافتراضي(4) .

الفصل الثالث: الإطار التجريبي:

اعداد وضبط قائمة مهارات الأمن السيبراني: (3-1)

تم اعداد القائمة في صورتها المبدئية، ثم عرضها على مجموعة من الخبراء المتخصصين في مجال الأمن السيبراني، ونظم المعلومات الإدارية، لإبداء الرأي حول وضوح الصياغة اللغوية لكل مهارة، ملاءمة المهارات للمستوى التعليمي والمرحلة الدراسية، مدى ارتباط كل مهارة بأهداف البحث، وبناءً على آراء المحكمين، تم إجراء التعديلات اللازمة بحذف وإضافة وإعادة صياغة بعض المهارات، لتصبح القائمة في صورتها النهائية القابلة للتطبيق على عينة البحث..... ملحق رقم (1).

إعداد وضبط استبانة مهارات الأمن السيبراني: (3-2)

قام الباحث بإعداد استبانة لقياس مهارات الأمن السيبراني لدى طلاب نظم المعلومات الإدارية، مستندًا إلى الإطار النظري والدراسات السابقة ذات الصلة، بهدف قياس مدى امتلاكهم لهذه المهارات، والتعرف على التحديات التي تواجههم، والمقترحات الممكنة لتعزيزها، كالتالي:

أولًا: إعداد الصورة الأولية للاستبانة:

المهارات على المستوى :تضمنت الاستبانة في صورتها الأولية (40) بندًا موزعة على أربعة محاور رئيسية الشخصي، المهارات على المستوى المؤسسي، التحديات التي تواجه الطلاب، المقترحات لتعزيز المهارات.

ثانيًا: ضبط الاستبانة والتأكد من صدقها وثباتها

1- اختبار الصدق

أ)الصدق الظاهري (Face Validity): عُرضت الاستبانة على مجموعة من الخبراء في الأمن السيبراني ونظم المعلومات والقياس، لتقييم وضوح العبارات ودقتها، وأُجريت تعديلات وفق ملاحظاتهم، ليتم اعتماد الصيغة النهائية القابلة للتطبيق (ملحق 2).

ب) صدق الاتساق الداخلي(Internal Consistency Validity) : طُبّقت الاستبانة على عينة استطلاعية (20 طالبًا) من خارج العينة الأساسية، وحُسبت معاملات الارتباط بين البنود ومحاورها، وجاءت جميعها موجبة ودالة إحصائيًا عند (0.005) أو أقل، مما يدل على اتساق داخلي قوي للبنود والمحاور، كما أظهرت المعاملات بين المحاور والدرجة الكلية دلالة إحصائية، مما يعكس اتساقًا داخليًا جيدًا بين المحاور والاستبانة ككل، ويوضح جدول (3-1) معاملات الارتباط بين كل بند والدرجة الكلية لمحوره.

جدول (3-1): معامل ارتباط بيرسون بين درجة كل بند ومجموع درجات المحور الذي ينتمي إليه.

رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط	رقم العبارة	معامل الارتباط
1	0.3358[1]*	8	0.3335*	15	0.6789**	22	0.5784**	29	0.5798**	36	0.5392**
2	0.6275**	9	0.5238**	16	0.4123*	23	0.6432**	30	0.4897*	37	0.7231**
3	0.6768**	10	0.7143**	17	0.5256*	24	0.7231**	31	0.5392**	38	0.7143**
4	0.3503*	11	0.3333*	18	0.5378**	25	0.5362**	32	0.6174**	39	0.4983*
5	0.5486*	12	0.4567*	19	0.6521**	26	0.4983*	33	0.7298**	40	0.6432**
6	0.3533*	13	0.5892**	20	0.4923*	27	0.5897**	34	0.8123**		
7	0.7231**	14	0.7231**	21	0.5897**	28	0.6174**	35	0.7143**		

كما تم حساب معامل الارتباط بين كل محور والاستبانة ككل وذلك كما يوضحه جدول (3-2)

جدول (3-2): معامل الارتباط بيرسون بين كل محور والاستبانة ككل

رقم المحور	المحور	معامل الارتباط
الأول	مهارات الأمن السيبراني على المستوى المؤسسي	0.6789**
الثاني	مهارات الأمن السيبراني على المستوى الشخصي	0.7123*
الثالث	التحديات التي تواجه التمكين من هذه المهارات	0.7923*
الرابع	المقترحات لتعزيز مهارات الأمن السيبراني	0.6378**

2- اختبار الثبات:

كرونباخ (Cronbach's Alpha)لضمان استقرار نتائج الاستبانة، تم حساب معامل الثبات باستخدام معامل ألفا ، وذلك كما يوضحه جدول (3-3)

جدول (3-3): معامل الثبات للاستبانة باستخدام ألفا كرونباخ

رقم المحور	المحور	معامل ألفا كرونباخ
الأول	مهارات الأمن السيبراني على المستوى المؤسسي	0.764
الثاني	مهارات الأمن السيبراني على المستوى الشخصي	0.869
الثالث	التحديات التي تواجه التمكين من هذه المهارات	0.792
الرابع	المقترحات لتعزيز مهارات الأمن السيبراني	0.637
كل المحاور	الاستبانة ككل	0.790

من الجدول السابق نلاحظ أنه: تراوحت قيم معامل كرونباخ ألفا لكل محور بين (0.637 – 0.869) ، مما يشير إلى مستوى ثبات مقبول إلى مرتفع في جميع المحاور، وبلغت قيمة الثبات الكلي للاستبانة (0.790) ، مما يدل على مستوى ثبات عالٍ، ويؤكد أن الاستبانة قادرة على إعطاء نتائج متسقة عند إعادة تطبيقها في نفس الظروف، مما يعني أن الاستبانة ثابتة إلى حد كبير، وأنها سوف تعطى نفس النتائج إذا أعيد تطبيقها على نفس المجموعة التجريبية في نفس الظروف.

المعالجة التجريبية بالبحث: (3-3)

تم توزيع الاستبانة على عينة البحث المكونة من عدد 32 من طلاب كلية النظم الإدارية .

- [1] (**) يشير إلى أن معامل الارتباط دال إحصائيًا عند مستوى الدلالة.(0.01)
- (*)يشير إلى أن معامل الارتباط دال إحصائيًا عند مستوى الدلالة.(0.05)

التحقق من صحة الفروض الإحصائية: (3-4)

أنه: " لا توجد فروق ذات دلالة إحصائية أولا:للتحقق من صحة الفرض الإحصائي الأول، والذي ينص على عند مستوى (0.05) بين المتوسط الحسابي لمهارات الأمن السيبراني على المستوي: الشخصي لدى طلاب للمجموعات المستقلة "T-Test" . "، استخدم الباحث اختبار(4) كليات النظم الإدارية والمتوسط الافتراضي لقياس دلالة الفرق بين متوسطي درجات طلاب كليات النظم الإدارية في لمهارات الأمن السيبراني على المستوي: الشخصي، كما هو موضح في جدول (4-3)

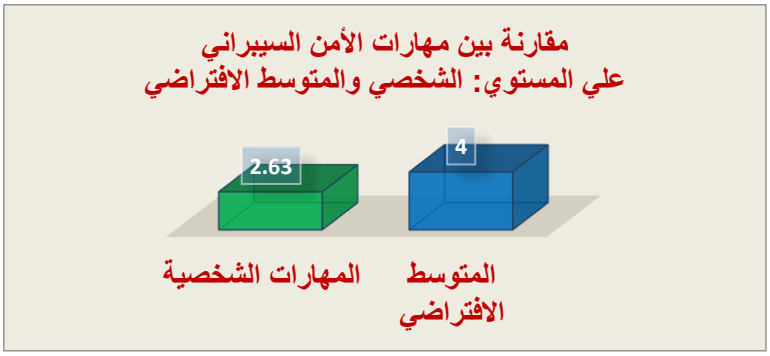
" لدلالة الفرق بين متوسطي درجات مهارات الأمن السيبراني علي Test -tجدول (4-3): نتائج اختبار " المستوي الشخصي والمتوسط الافتراضي (4).

البعـــــد	العينة	المتوسط	الانحراف المعياري	درجات الحرية	معدل الارتباط	قيمة "ت"	مستوى الدلالة
الكفايات الأساسية	32	2.63	1.28	31	0.75	-59.949	0.000

ويمكن التعبير عن ذلك بيانيًا كما بالشكل (3-1) التالي:

شكل (3-1):

التمثيل البياني للفرق بين متوسطي درجات مهارات الأمن السيبراني على المستوي: الشخصي والمتوسط الافتراضي



يوضح التمثيل البياني أن المتوسط الحسابي أقل من المتوسط الافتراضي (4)، مما يشير إلى أن الطلاب يمتلكون مهارات الأمن السيبراني علي المستوي الشخصي بمستوى أقل من المطلوب.

أنه: " لا توجد فروق ذات دلالة إحصائية ثانيًا: للتحقق من صحة الفرض الإحصائي الثاني، والذي ينص على عند مستوى (0.05) بين المتوسط الحسابي لمهارات الأمن السيبراني علي المستوي: المؤسسي لدى طلاب للمجموعات المستقلة "T-Test" كليات النظم الإدارية والمتوسط الافتراضي (4)."، استخدم الباحث اختبار لقياس دلالة الفرق بين متوسطي درجات طلاب كليات النظم الإدارية في لمهارات الأمن السيبراني على المستوي: المؤسسي، كما هو موضح في جدول (5-3).

" لدلالة الفرق بين متوسطي درجات مهارات الأمن السيبراني على Test -tجدول (5-3): نتائج اختبار " المستوي: المؤسسي والمتوسط الافتراضي.

البعد	العينة	المتوسط	الانحراف المعياري	درجات الحرية	معدل الارتباط	قيمة "ت"	مستوى الدلالة
الكفايات الأساسية	32	2.54	1.38	31	0.75	-59.949	0.000

ويمكن التعبير عن ذلك بيانيًا كما بالشكل (3-2) التالي:

شكل (3-2):

التمثيل البياني للفرق بين متوسطي درجات مهارات الأمن السيبراني على المستوي: المؤسسي والمتوسط الافتراضي

يوضح التمثيل البياني أن المتوسط الحسابي أقل من المتوسط الافتراضي (4)، مما يشير إلى أن الطلاب يمتلكون مهارات الأمن السيبراني على المستوي: المؤسسي بمستوى أقل من المطلوب.

الفصل الرابع: نتائج البحث:

بعد أن تم عرض الإطار النظري للدراسة، وبناء أدوات البحث، واختبار صحة فروضه، يأتي هذا الفصل للإجابة عن أسئلة البحث الرئيسية والفرعية؛ وذلك من خلال تحليل البيانات المستخلصة من أدوات الدراسة الميدانية، وربطها بالإطار النظري، بهدف الوصول إلى تفسير علمي للنتائج التي تحقق أهداف البحث وتدعم بناء تصور واضح لتنمية مهارات الأمن السيبراني لدى طلاب نظم المعلومات الإدارية.

وقد جاءت الإجابة عن الأسئلة وفق ما يلي:

السؤال الأول: ما مهارات الأمن السيبراني اللازم توافرها لدى طلاب نظم المعلومات الإدارية على المستوى الشخصي؟

أوضحت النتائج أن المهارات الشخصية تشمل: إنشاء كلمات مرور قوية، تحديث الأنظمة، استخدام وتحديث برامج الحماية، تأمين الشبكات اللاسلكية، الحذر من الروابط المشبوهة، حماية البيانات على وسائل التواصل، وتفعيل التحقق الثنائي. وقد وردت هذه المهارات في الجزء الأول من قائمة المهارات (ملحق1- الجزء الأول)، ما يؤكد دورها في تعزيز وعي الطلاب الرقمي.

السؤال الثاني: ما مهارات الأمن السيبراني اللازم توافرها لدى طلاب نظم المعلومات الإدارية على المستوى المؤسسي؟

أظهرت النتائج أن المهارات المؤسسية المطلوبة تشمل: التعامل مع Firewalls، إدارة الحسابات، وتطبيق معايير حماية Bitlocker، تشفير البيانات بـVPN الإدارية، إعداد سياسات أمن الشبكات، فهم ، بالإضافة إلى إدارة حقوق الوصول ورصد الأنشطة المشبوهة، كما ورد في الجزء الثاني من قائمة البيانات، المهارات (ملحق1-الجزء الثاني).

السؤال الثالث: ما مستوى طلاب نظم المعلومات الإدارية في مهارات الأمن السيبراني على المستوى الشخصي مقارنة بالمتوسط الافتراضي (4)؟

بيّنت النتائج أن متوسط المهارات الشخصية للطلاب جاء أقل من المتوسط الافتراضي (4)، مما يدل على ضعف نسبي، وأظهر اختبار "ت" فرقًا دالًا إحصائيًا لصالح المتوسط الافتراضي، مما يؤكد الحاجة إلى تعزيز المهارات السيبرانية الشخصية لدى الطلاب.

السؤال الرابع: ما مستوى طلاب نظم المعلومات الإدارية في مهارات الأمن السيبراني على المستوى المؤسسي مقارنة بالمتوسط الافتراضي (4)؟

أظهرت النتائج أن متوسط المهارات المؤسسية للطلاب أيضًا أقل من المتوسط الافتراضي، مع دلالة إحصائية تؤكد ضعفهم في إدارة أمن الشبكات والأنظمة، مما يبرز الحاجة لتدريب عملي مكثف ضمن البرامج الأكاديمية.

السؤال الخامس: ما أبرز التحديات التي تعوق تنمية مهارات الأمن السيبراني لدى طلاب نظم المعلومات الإدارية؟

أبرزت نتائج الدراسة أن التحديات تتلخص في ضعف الوعي السيبراني لدى الطلاب للأسباب التالية:

- قلة البرامج التدريبية التطبيقية، ضعف البنية التحتية التقنية في المؤسسات التعليمية.
- نقص الكوادر المتخصصة في التدريب على الأمن السيبراني.
- الاعتماد المفرط على المعلومات النظرية دون ممارسة عملية كافية.
- بالإضافة إلى سرعة تطور التهديدات الإلكترونية التي تتطلب تحديثًا مستمرًا للمناهج والمهارات.

السؤال السادس: ما السبل المقترحة لتعزيز المهارات السيبرانية لطلاب الجامعات بما يدعم حماية نظم المعلومات الإدارية؟

توصي الدراسة بمجموعة من الإجراءات لتعزيز مهارات الأمن السيبراني لدى الطلاب، منها:

- إدخال مقررات دراسية متخصصة في الأمن السيبراني ضمن برامج نظم المعلومات الإدارية.
- تنظيم دورات تدريبية عملية مستمرة.
- توفير بيئة تقنية آمنة ومتطورة داخل الكليات.
- عقد شراكات مع مؤسسات تقنية متخصصة لتقديم برامج تدريبية معتمدة.
- تطوير مهارات أعضاء هيئة التدريس في المجال السيبراني.
- التأكيد على نشر ثقافة الأمن السيبراني بين الطلاب عبر الحملات التوعوية وورش العمل.

بعد الإجابة عن الأسئلة الفرعية تكون تمت الإجابة على السؤال الرئيسي للبحث؛ حيث أظهرت النتائج أن مهارات الأمن السيبراني اللازمة لحماية نظم المعلومات الإدارية تشمل الجوانب الشخصية والمؤسسية، في ظل وعي متفاوت بين الطلاب ناتج عن نقص التدريب، وضعف المناهج والتوعية، مما يستلزم لتعزيز هذه المهارات تدخلًا منهجيًا يشمل تطوير التعليم، وتوفير تدريب فعلي، وبناء شراكات مهنية لضمان تأهيل كوادر قادرة على التصدي للتهديدات الرقمية.

(2-4) توصيات البحث:

في ضوء نتائج البحث، يوصي الباحث بما يلي:

1. إدماج مهارات الأمن السيبراني في مقررات نظم المعلومات الإدارية، خصوصًا في المحاسبة والموارد البشرية والتمويل.
2. إعداد برامج تدريبية دورية وتقييم أثرها على الأداء العملي للطلاب.
3. إطلاق حملات توعوية منتظمة بمشاركة الطلاب والمعلمين.
4. إنشاء مختبرات سيبرانية للتدريب العملي على الهجمات الافتراضية.
5. تحديث البنية التقنية بالكليات بما يتوافق مع معايير الأمن الحديثة.
6. بناء شراكات مع مؤسسات متخصصة لتوفير تدريب وتوظيف في مجالات مثل التدقيق وتحليل الامتثال.
7. تدريب أعضاء هيئة التدريس على دمج مفاهيم الأمن السيبراني وتبسيطها للطلاب.

المراجع العربية:

ابن إبراهيم، م. ح. (2021). *الوعي بجوانب الأمن السيبراني في التعليم عن بعد*. *المجلة العلمية لجامعة الملك فيصل للعلوم الإنسانية والإدارية*، *22*(2)، 299–307.

الجبوري، مروان عبد الله. (2021). *إدارة المعرفة في ظل تطبيقات التقنية الإدارية الحديثة*. *مجلة التنمية الإدارية*.

الحربي، عبد الرحمن. (2019). *التعليم الإلكتروني وأثره في تطوير مهارات الأمن السيبراني*. *مجلة التربية الإلكترونية*.

الدوسري، ناصر بن عبد الرحمن. (2021). *أثر نظم المعلومات الإدارية على اتخاذ القرارات الإدارية*. *مجلة الاقتصاد والإدارة، جامعة الملك عبد العزيز*.

راشد محمد المري. (2023). *الأمن السيبراني وحماية الأنظمة الإلكترونية: دراسة تحليلية تأصيلية*. *المجلة المصرية لبحوث الإعلام*، *9*(1)، 959–1008.

الزهراني، عبد العزيز بن محمد. (2020). *تطبيقات التقنية الإدارية الحديثة في تحسين الأداء المؤسسي*. *مجلة الإدارة العامة*.

عبد الرحيم، مصطفى عبد الجليل. (2022). *استراتيجية تطوير المهارات السيبرانية في بيئة العمل الرقمية*. *مجلة البحوث الإدارية*.

عبد الله، ن. (2023). *متطلبات وضوابط الأمن السيبراني لحماية البيانات في جامعة الأميرة نورة من وجهة نظر أعضاء هيئة التدريس ومن في حكمهم*. *المجلة التربوية، جامعة سوهاج*، *91*(91)، 387–428.

العتيبي، أ. م. (2022). *مستوى الوعي تجاه الأمن السيبراني لدى المتدربين في المؤسسة العامة للتدريب التقني والمهني*. *مجلة البحوث الأمنية، مركز البحوث والدراسات، كلية الملك فهد الأمنية*، *31*(82)، 167–206.

العزاوي، علي عبد الرحمن. (2020). *التقنية الإدارية الحديثة وأثرها في كفاءة المنظمات العراقية*. *المجلة العراقية للعلوم الإدارية*.

القحطاني، م. س. (2022). *تصميم وحدة تعليمية لزيادة الوعي بالأمن السيبراني لدى طلاب جامعة الإمام عبد الرحمن بن فيصل*. *المجلة الدولية التربوية المتخصصة، الجمعية العراقية للعلوم التربوية والنفسية*، *11*(130)، 245–278.

المحمدي، غ. س. (2023). *فاعلية وحدة إلكترونية تفاعلية لتوظيف مهارات الأمن السيبراني في ضوء محددات المواطنة الرقمية لدى طلاب جامعة أم القرى*. *مجلة العلوم التربوية والنفسية، جامعة القصيم*، *7*(12)، 305–338.

المراجع الأجنبية:

(ISC)². (2022). Cybersecurity workforce study: A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution.

87, A. (2023). Cybersecurity practices in higher education institutions. Journal of Information Security, 12(3), 145–158.

Agrawal, N., Zhu, F., & Carpenter, S. (2020). Do you see the warning? Cybersecurity warnings via nonconscious processing. In Proceedings of the 2020 ACM Southeast Conference (ACMSE '20) (pp. 260–263). Association for Computing Machinery.

Alhammadi, S. (2022). Information security in academic management systems. Arab Journal of Information Technology, 18(2), 111–127.

Alhogail, A. (2022). Cybersecurity awareness and practices among university students. International Journal of Cyber Studies, 9(1), 25–41.
Alotaibi, F., & Alshammari, A. (2024). Integrating cybersecurity in management information systems programs. Journal of Cyber Education, 10(2), 90–103.
Alshaikh, M. (2023). Bridging the cybersecurity skills gap in Arab universities. Middle East Journal of Educational Technology, 6(4), 50–67.
Alshammari, H. (2023). Digital safety practices and student awareness. Cyber Education Review, 5(1), 72–85.
Alshehri, N. (2023). Cybersecurity and national digital transformation strategies. Saudi Journal of Digital Governance, 7(2), 33–49.
Althunibat, A. (2023). The role of digital culture in cybersecurity awareness. Arab Journal of Cyber Behavior, 3(1), 55–68.
BBC News. (2020). University of California pays $1.14m ransom to restore COVID-19 research data.
Bellevue University. (2018). First Year Seminar on Cybersecurity. https://www.bellevue.edu
Cameron, E. A., & Marcum, T. M. (2019). Why business schools must incorporate cybersecurity into the business curriculum: Preparing the next generation for success. MBAA International Conference. https://mbaasais.net/2019_proceedings/PDFs/MBAA-2019_Cameron_Marcum_Paper.pdf
Camillo, M. (2017). Cybersecurity strategies to protect information systems in small financial institutions. Journal of Financial Regulation and Compliance, 25(3), 325–336.
Carr, M. (2016). Public-private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.
Choucri, N., Madnick, S., & Ferwerda, J. (2013). Institutions for cybersecurity: International responses and global imperatives. Information Technology for Development, 20, 96–121.
Crumpler, W., & Lewis, J. A. (2019). The cybersecurity workforce gap. Center for Strategic and International Studies.
Cybersecurity and Higher Education Report. (2024). Global impact of cyber threats on academic institutions.
Cybersecurity Ventures. (2023). Cybercrime statistics and trends. https://cybersecurityventures.com/cybercrime-report-2023/
Dambe, S., Gochhait, S., & Ray, S. (2023, November). The role of artificial intelligence in enhancing cybersecurity and internal audit. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE) (pp. 88–93). IEEE.
EDUCAUSE. (2023). Cybersecurity and Privacy Professionals Conference 2023. https://events.educause.edu/cybersecurity-and-privacy-professionals-conference/2023
ENISA. (2021). Principles of cyber hygiene. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/principlesofcyberhygiene
European Centre for Counterterrorism and Intelligence Studies. (2024). Cybersecurity – Risks, Measures, and European Policies. https://www.europarabct.com/
Hoffman, L. J., & Friedman, A. (2014). The internet of (whose) things: Business models, computer architectures, and privacy. Cybersecurity Policy and Research Institute, The George Washington U.

IBM. (2024). Cost of a data breach report 2024. https://www.ibm.com/reports/data-breach

ISC². (2024). Cybersecurity workforce study 2024. https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

ITU. (2024). Global Cybersecurity Index 2024. International Telecommunication Union. https://ispar.unescwa.org/country-index.aspx?Country=81

Khamzina, B., Roza, N., Zhussupbekova, G., Shaizhanova, K., Aten, A., & Meirkhanovna, A. (2022). A systematic review of cybersecurity awareness among university students. International Journal of Emerging Technologies in Learning, 17(18), 177–190.

Khidr, M. (2021). Developing a framework to enhance cybersecurity awareness in academic institutions. Journal of Academic Security, 12(1), 35–49.

Nilsen, R., Levy, Y., Terrell, S., & Beyer, D. (2017). A developmental study on assessing the cybersecurity competency of organizational information system users. KSU Proceedings on Cybersecurity Education, Research and Practice.

Office of the National Cyber Director. (2023). National cyber workforce and education strategy: Unleashing America's cyber talent. Executive Office of the President of the United States.

Petersen, R., Santos, D., Smith, M. C., Witte, G., & Wetzel, K. (2020). Workforce framework for cybersecurity (NICE Framework) (Rev. 1).

Ponemon Institute. (2023). The impact of cybersecurity education on incident reduction in universities. https://www.ponemon.org/cyber-edu-impact-2023

Proofpoint. (2021). The Human Factor Report. https://www.proofpoint.com/us/resources/threat-reports/human-factor

Ramezan, C. A. (2023). Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field. Journal of Information Systems Education, 34(1), 94–105.

Schellman. (2024). A recap of recent cybersecurity incidents at universities. https://www.schellman.com/blog/cybersecurity/cybersecurity-incidents-at-universities-2023

Security Affairs. (2023, August 8). Texas Tech University data breach: Hackers exploited MOVEit file transfer vulnerability. https://securityaffairs.com/172085/data-breach/texas-tech-university-data-breach.html

SecurityWeek. (2025, April 5). University of Manchester hit by cyberattack, data stolen. https://www.securityweek.com/university-of-manchester-hit-by-cyberattack-data-stolen/

State Key Laboratory of Information Security. (2024). Inscrypt 2024 – International Conference on Information Security and Cryptology. https://inscrypt2024.github.io/

Taha, N. (2022). Evaluating the effectiveness of practical cybersecurity practices in developing information security skills among female students at Umm University College. Journal of Cybersecurity and Information Management, 9(1), 85–100.

U.S. Department of Defense. (2018). Department of Defense Dictionary of Military and Associated Terms.

Wiener, N. (1948). Cybernetics: Or control and communication in the animal and the machine. MIT Press.

Wilshusen, G. C. (2012). Cyber threats facilitate ability to commit economic espionage. U.S. Government Accountability Office.

ملاحق البحث:

ملحق رقم (1) قائمة مهارات الأمن السيبراني اللازمة لدى طلاب نظم المعلومات الإدارية

أولاً: مهارات الأمن السيبراني على المستوى الشخصي:

مهارات التعامل الآمن مع الشبكات (1-1):

1. تغيير اسم وكلمة مرور الشبكة بشكل دوري.
2. إعداد مفتاح أمان الشبكة.(Network Security Key)
3. إنشاء ملف تعريف VPN واستخدامه.
4. تجنب استخدام وسائط التخزين الخارجية (USB) غير الموثوقة.

مهارات التعامل الآمن مع الأجهزة (1-2):

5. تشفير البيانات باستخدام خاصية BitLocker.
6. إنشاء حساب مسئول (Administrator) وتحديد صلاحياته بدقة.
7. إجراء النسخ الاحتياطي (Backup) واستعادته.
8. تحديث الأجهزة وبرامجها بشكل دوري.

مهارات التعامل الآمن مع أنظمة التشغيل والبرامج (1-3):

9. تحديث نظام التشغيل Windows بانتظام.
10. التعامل مع مركز الصيانة.(Action Center)
11. استخدام برامج الحماية مثل Windows Defender وتحديثها دوريًا.
12. استخدام مضادات الفيروسات وإجراء الفحص الدوري.

مهارات التعامل الآمن مع المتصفحات ووسائل التواصل الاجتماعي (1-4):

13. إنشاء واستخدام كلمات مرور قوية ومختلفة لكل حساب.
14. تفعيل المصادقة الثنائية.(Two-factor authentication)
15. ضبط إعدادات الخصوصية والأمان في المتصفحات.
16. الحذر من مشاركة المعلومات الشخصية والصور على مواقع التواصل الاجتماعي.

ثانيًا: مهارات الأمن السيبراني على المستوى المؤسسي:

مهارات حماية الشبكات المؤسسية (2-1):

1. تفعيل وتكوين جدران الحماية.(Firewalls)
2. استخدام أنظمة كشف ومنع التسلل.(IDS/IPS)
3. إدارة صلاحيات الوصول واستخدام شبكات VPN المؤسسية.

مهارات إدارة المخاطر والاستجابة للحوادث (2-2):

4. تحليل المخاطر السيبرانية وتطوير استراتيجيات للحد منها.
5. بناء وتنفيذ خطط الاستجابة لحوادث الأمن السيبراني.
6. إجراء تدريبات منتظمة للاستجابة للحوادث.

مهارات حماية البيانات المؤسسية (2-3):

7. تشفير المعلومات الحساسة.
8. تطبيق سياسات النسخ الاحتياطي للبيانات.
9. التحكم في الوصول للبيانات وفقًا للسياسات المؤسسية.

مهارات التعامل مع التهديدات والبرمجيات الضارة (2-4):

10. إجراء اختبارات الاختراق.(Penetration Testing)
11. تحليل الأدلة الرقمية في حالات الاختراق.(Digital Forensics)
12. تطوير البرمجيات بشكل آمن وخالٍ من الثغرات.

مهارات تعزيز ثقافة الأمن السيبراني المؤسسي (2-5):

13. تدريب العاملين دوريًا على أحدث التهديدات وأساليب الوقاية.
14. تعزيز الوعي بسياسات الأمن السيبراني وتطبيقها.
15. توفير آليات واضحة وسهلة للإبلاغ عن الحوادث السيبرانية.

ملحق رقم (2): استبانة مهارات الأمن السيبراني لدى طلاب نظم المعلومات الإدارية

تهدف هذه الاستبانة إلى التعرف على مدى امتلاكك لمهارات الأمن السيبراني، وتحديد التحديات التي تواجهك في التمكُّن منها، بالإضافة إلى اقتراح الحلول الممكنة. يُرجى وضع علامة (✓) أمام الخيار المناسب لك: موافق جدًا – موافق – محايد – غير موافق – غير موافق إطلاقًا

أولاً: مهارات الأمن السيبراني على المستوى الشخصي

1. أستطيع تغيير اسم وكلمة مرور الشبكة الخاصة بي بشكل دوري.
2. أستطيع إعداد مفتاح أمان الشبكة.(Network Security Key)
3. أقوم بإنشاء واستخدام ملف تعريف.VPN
4. أتجنب استخدام وسائط التخزين الخارجية (USB) غير الموثوقة.
5. أستخدم خاصية تشفير البيانات.BitLocker
6. لديَّ القدرة على إنشاء حساب مسئول (Administrator) وتحديد صلاحياته.
7. أقوم بإجراء نسخ احتياطي (Backup) دوري واستعادته.
8. أقوم بتحديث نظام التشغيل Windows بشكل دوري.
9. أستخدم مركز الصيانة (Action Center) لمعالجة المشكلات.
10. أستخدم برامج الحماية مثل Windows Defender وأحدثها باستمرار.
11. أقوم بفحص دوري باستخدام برامج مكافحة الفيروسات.
12. لديَّ القدرة على إنشاء كلمات مرور قوية ومختلفة لحساباتي.
13. أستخدم المصادقة الثنائية.(Two-factor authentication)
14. أقوم بضبط إعدادات الخصوصية في المتصفحات ووسائل التواصل.
15. أتجنب مشاركة معلوماتي الشخصية بشكل غير آمن على الإنترنت.

ثانيًا: مهارات الأمن السيبراني على المستوى المؤسسي

16. أعرف كيفية تفعيل وتكوين جدران الحماية.(Firewalls)
17. لديَّ معرفة بكيفية استخدام أنظمة كشف ومنع التسلل.(IDS/IPS)
18. أستطيع إدارة صلاحيات الوصول واستخدام الشبكات المؤسسية بشكل آمن.
19. لديَّ معرفة بكيفية تحليل المخاطر السيبرانية.
20. أستطيع المساهمة في بناء وتنفيذ خطط الاستجابة لحوادث الأمن السيبراني.
21. أحرص على تشفير المعلومات الحساسة على مستوى المؤسسة.
22. أتبع سياسات النسخ الاحتياطي للبيانات المؤسسية.
23. ألتزم بسياسات الوصول الآمن إلى البيانات المؤسسية.
24. لديَّ القدرة على إجراء اختبارات اختراق مبدئية.
25. أعرف كيف أتعامل مع الأدلة الرقمية في حالات الاختراق.
26. أهتم بتطوير برمجيات خالية من الثغرات الأمنية.
27. أشارك بفاعلية في التدريبات الدورية حول الأمن السيبراني.
28. أحرص على تعزيز الوعي بسياسات الأمن السيبراني في المؤسسة.
29. أعرف آليات الإبلاغ عن الحوادث السيبرانية داخل المؤسسة.

ثالثًا: التحديات التي تواجهني في التمكين من هذه المهارات

30. عدم توافر بنية تحتية تقنية مناسبة بالكلية.
31. نقص الأجهزة الحديثة التي تساعد على التدريب العملي.
32. قلة الوعي لدى الطلاب بأهمية الأمن السيبراني.
33. صعوبة الوصول إلى البرمجيات والتطبيقات الأصلية.
34. عدم توفر كورسات تدريبية متخصصة في الأمن السيبراني.

رابعًا: المقترحات لتعزيز مهارات الأمن السيبراني

35. توفير معامل مجهزة بأجهزة حديثة خاصة بالأمن السيبراني.

36. تطوير البنية التحتية التقنية في الكلية.
37. تقديم كورسات وورش عمل متخصصة بانتظام.
38. توفير وصول مجاني إلى برمجيات وتطبيقات الأمن السيبراني.
39. إجراء حملات توعية مستمرة حول أهمية الأمن السيبراني.
40. دمج مهارات الأمن السيبراني بشكل أكبر في المناهج الدراسية.

شكرًا لتعاونكم.