Dirasat: Human and Social Sciences, Volume 53, No. 9, 2026, 10921

Deanship of Scientific Research

Jordanian Specialists' Attitudes Towards Employing Artificial Intelligence Applications in Combating Cybercrimes and Enhancing Cybersecurity

***Ibrahim Fuad Al-Khasawneh*[1]*, *Aya Ahmad Rebhi Ali Saleem*[2]**

[1] Department of Radio and Television, Faculty of Mass Communication, University of Petra, Amman, Jordan.

[2] Faculty of Mass Communication, University of Petra, Amman, Jordan.

Received: 24/2/2025
Revised: 5/4/2025
Accepted: 22/4/2025
Published online: 24/6/2026

* *Corresponding author:*
ibrfk200@hotmail.com

Citation: Al-Khasawneh, I. F., & Saleem, A. A. R. A. (2026). Jordanian Specialists' Attitudes Towards Employing Artificial Intelligence Applications in Combating Cybercrimes and Enhancing Cybersecurity. *Dirasat: Human and Social Sciences*, *53*(9), 10921..
https://doi.org/10.35516/Hum.2026.10921

© 2026 DSR Publishers/ The University of Jordan.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license https://creativecommons.org/licenses/by-nc/4.0/

Abstract

Objectives: The study aimed to identify Jordanian specialists' attitudes towards employing artificial intelligence applications in combating cybercrimes and enhancing cybersecurity. It also explored the fields in which these applications are employed, their success factors, and the types of cybercrimes and threats that necessitate the use of AI technologies.

Methods: The study adopted a descriptive survey-based approach in its quantitative dimension, using a questionnaire as the primary tool for data collection. The sample included 100 Jordanian specialists working at the National Center for Cybersecurity.

Results: The findings revealed the most prominent fields of AI application in combating cybercrime: drones (2.93), IP cameras and social analysis applications (2.92), and dynamic GPS tracking (2.86). Key challenges include a weak legislative framework, insufficient financial support, and a shortage of qualified human resources to manage AI technologies. Common cyber threats identified include blackmail, extortion, and data or account hacking. The study also found that Jordanian specialists hold generally positive attitudes toward the use of AI in cybersecurity efforts.

Conclusions: The study concludes that there is strong support among specialists for employing AI in cybercrime prevention. Drones emerged as the most significant application area, while legislative inadequacies were identified as the most critical challenge.

Keywords: Attitudes, AI applications, Cybercrime, Cybersecurity.

اتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني

***إبراهيم فؤاد الخصاونة**، آية أحمد ربحي علي سليم**

قسم الإذاعة والتلفزيون، كلية الإعلام، جامعة البترا، عمان، الأردن.

ملخّص

الأهداف: هدفت الدراسة إلى الكشف عن اتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني، والتعرف إلى مجالات توظيف هذه التطبيقات، ومقومات نجاحه، وكذلك أشكال الجرائم الإلكترونية والتهديدات السيبرانية التي تقتضي توظيف التطبيقات الذكية لمكافحتها.

المنهجية: اعتمدت الدراسة الوصفية منهج المسح بشقه الكمي، وباستخدام "الاستبانة" أداة منهجية لجمع البيانات من عينة قصدية بلغ قوامها (100) مفردة من المختصين الأردنيين العاملين في المركز الوطني للأمن السيبراني.

النتائج: كشفت النتائج عن أبرز مجالات توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وهي على التوالي: "الطائرة دون طيار (Drones)" بنسبة (2.93)، و"كاميرات (آي بي)" و"تطبيقات التحليل الاجتماعي التي تحلل بيانات شبكات التواصل الاجتماعي" بالنسبة ذاتها (2.92)، و"تطبيق التتبع الديناميكي (GPS)" بنسبة (2.86)، وكشفت عن التحديات المصاحبة لتوظيف هذه التطبيقات، والمتمثلة بضعف البيئة القانونية والتشريعية، وغياب الدعم المادي المناسب، وغياب تدريب وتأهيل الموارد البشرية الأمنية للتعامل مع تطبيقات الذكاء الاصطناعي، وكذلك عن أشكال الجرائم الالكترونية والتهديدات السيبرانية التي تقتضي توظيف تطبيقات الذكاء الاصطناعي لمكافحتها، وعلى رأسها جريمتي التهديد والابتزاز، وقرصنة البيانات والحسابات، كما وأسفرت النتائج عن إيجابية اتجاهات العينة نحو موضوع الدراسة.

الخلاصة: تتلخص النتائج في إيجابية اتجاهات العينة، كما وتمثل "الطائرة دون طيار (Drones)" أبرز مجالات توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية، وكذلك يمثل ضعف البيئة القانونية والتشريعية أبرز التحديات المصاحبة لعملية التوظيف.

الكلمات الدالة: الاتجاهات، المختصّون الأردنيون، تطبيقات الذكاء الاصطناعي، مكافحة الجرائم الإلكترونية، الأمن السيبراني.

مقدمة

إن الجرائم السيبرانية امتداد طبيعي لتطور الحواسيب الرقمية وشبكات الخلايا العصبية الاصطناعية، كما أن تداول المعلومات الرقمية المتمثلة بالمستندات والوثائق الشخصية والعقود والبيانات المالية، والسجلات في الفضاء الإلكتروني قد عرضها للأنشطة الإجرامية التي تهدد أمنها.

وحظي أمن المعلومات باهتمام واضعي السياسات العامة الإقليمية والمحلية في ضوء تراجع المنظومة الأخلاقية، وضعف البيئات القانونية المنظمة للمجال الافتراضي، وتنامي الجريمة السيبرانية خلال العقدين الماضيين؛ إذ أصبحت ظاهرة عالمية تقع البنى التحتية للدول ضحيتها، الأمر الذي يضر بالاقتصاد العالمي (المري، 2023).

وعرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة، ومعاقبة المجرمين الجرائم المعلوماتية؛ بأنها الجرائم التي يتم ارتكابها داخل نظام الحاسب الآلي، أو من خلال شبكة حاسوبية (الدسوقي، 2022)، وكذلك وصفت منظمة التعاون الاقتصادي والتنمية هذا الممارسات بالأفعال الجنائية التي تعتدي على الأموال المادية أو المعنوية، ويتم هذا التعدي بشكل مباشر أو غير مباشر بواسطة تدخل تقني معلوماتي (Geisel, 2018).

وكما ساهمت تطبيقات الذكاء الاصطناعي في طرح أفكار تقنية للسلوك الإجرامي، فإنها في الوقت ذاته أدت دورا حيويا في رصد تبعات الظواهر الاجتماعية التي تندرج الجريمة الإلكترونية تحتها، أي أنها طرحت الفكرة الإجرامية من حدها السلبي، وطرحت تطبيقات مكافحتها من حدها الإيجابي، ومن هنا جاءت الدراسة الحالية لإثارة قضية بحثية أمنية تستند إلى تحليل واقع توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية، ومن ثم تعزيز الأمن السيبراني، فالمقدمات تقود إلى نتيجة واحدة مفادها تحصين المعلومات الرقمية للحد من الجرائم التي تتخذ من الفضاء السيبراني ووسائل الاتصال والإعلام الرقمي مجالا لها.

مشكلة الدراسة

انتفع السلوك الإجرامي بالتقدم التكنولوجي الذكي الذي شهدته الحواسيب الرقمية، وشبكات الخلايا العصبية الاصطناعية، ووظفه لتهديد أمن المعلومات المرتبط عضويا بالأمن القومي، وقد أفرز التقدم التكنولوجي في المقابل تطبيقات ذكية تواجه الجرائم السيبرانية التي تقوض الصناعة المعلوماتية، إلا أنها تطبيقات أمنية تقتضي تدخلا حكوميا وإجراءات قانونية لاستخدامها، لذا جاءت الدراسة الحالية لإثارة قضية بحثية أمنية تستند إلى تحليل واقع توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية، ومن ثم تعزيز الأمن السيبراني، ومن هنا تتلخص مشكلة الدراسة في الإجابة عن التساؤل الرئيس الآتي: **ما اتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني؟**

أهداف الدراسة

1. التعرف إلى اتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني.
2. الكشف عن مجالات توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين، وكذلك مقومات نجاح توظيف هذه التطبيقات.
3. الكشف عن أشكال الجرائم الإلكترونية والتهديدات السيبرانية التي تقتضي توظيف تطبيقات الذكاء الاصطناعي لمكافحتها.
4. التعرف إلى مقومات نجاح توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين.
5. الكشف عن التحديات المصاحبة لتوظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني.

أهمية الدراسة

تتجلى **الأهمية النظرية** للدراسة في ارتباطها بالأمن الوطني، وأهمية إثراء الدراسات والبحوث العلمية التي تعنى بالكشف عن مجالات توظيف تطبيقات الذكاء الاصطناعي في تعزيز ثقة الجهات الوطنية، ومؤسسات المجتمع والمستثمرين في الفضاء السيبراني الأردني. أما **الأهمية التطبيقية**: فتتمثل برصد واقع استخدام تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية داخل المركز الوطني للأمن السيبراني في المملكة الأردنية الهاشمية، مما يفسح المجال أمام التقييم العملي، والتطوير الاستشرافي المستند إلى أسس تحليلية لتأصيل تطبيقات الذكاء الاصطناعي في المركز.

تساؤلات الدراسة

1. ما اتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني؟
2. ما مجالات توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين؟
3. ما أشكال الجرائم الإلكترونية والتهديدات السيبرانية التي تقتضي توظيف تطبيقات الذكاء الاصطناعي لمكافحتها من وجهة نظر المختصين الأردنيين؟

4. ما مقومات نجاح توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين؟
5. ما التحديات المصاحبة لتوظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين؟
6. هل توجد فروقات ذات دلالة إحصائية في اتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني تعزى للمتغيرات الديموغرافية لعينة الدراسة؟

مصطلحات الدراسة

الاتجاهات: تعرف بأنها "حالة التأهب العصبي والنفسي ذات التأثير الدينامي على استجابة الفرد، ويحكم متغير الخبرة هذا الاستعداد" (Allport, 1954, 45). وتعرف **إجرائيا**؛ بأنها طبيعة تصرف المختصين الأردنيين بشكل إيجابي أو سلبي نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية، وتعزيز الأمن السيبراني.

تطبيقات الذكاء الاصطناعي: تعرف بأنها "البرامج المغذية بعمليات استدلالية تعبر عن أدوار السلوك البشري بلغة رقمية، وتؤديها من خلال عمليات حاسوبية، قائمة على وصف المشكلات وتحليلها، واتخاذ القرارات المناسبة بشأنها" (سليم، 2024، 50). وتعرف **إجرائيا**؛ بأنها المستحدثات التقنية من تطبيقات الذكاء الاصطناعي الموظفة في مكافحة الجرائم الإلكترونية وتعزيز أمن المعلومات الرقمية.

الجرائم الالكترونية: تعرف بأنها "حصيلة السلوكيات المنظمة، وغير المنظمة لاستخدام التقنيات الرقمية المختلفة في ارتكاب الجرائم المخالفة للقانون، والعرف المجتمعي" (قاسم، 2024، 99). وتعرف **إجرائيا**؛ بأنها الإخلال بقواعد القانون الجنائي الأردني من خلال استخدام الشبكة المعلوماتية، أو ملفات البيانات، أو تقنيات المعلومات، أو المنصات الرقمية والصحافة الرقمية، أو شبكات التواصل الاجتماعي بطريقة غير مصرح بها وفقا للمواد التي نص عليها قانون الجرائم الإلكترونية الأردني رقم (17) لعام (2023).

الأمن السيبراني: عرفته الوكالة الفرنسية لأمن أنظمة الإعلام بأنه "المعدات المعالجة للمعطيات الرقمية بشكل آلي" (المري، 2023، 965). ويعرف **إجرائيا**؛ بأنه ممارسات المختصين الأردنيين لحماية بيانات الفضاء الالكتروني من الهجمات الالكترونية وأخطارها.

حدود الدراسة

الحدود البشرية: اقتصرت الدراسة على المختصين الأردنيين العاملين في المركز الوطني للأمن السيبراني في الأردن.

الحدود الزمانية: خلال الفترة الممتدة بين 2024/11/1 لغاية 2025/1/31.

الحدود المكانية: تم توزيع الاستبانة رقميا على العاملين في المركز الوطني للأمن السيبراني من خلال البريد الإلكتروني، وتطبيق(WhatsApp).

الإطار النظري والدراسات السابقة

نظرية انتشار المبتكرات

استندت الدراسة في إطارها النظري إلى نظرية انتشار المبتكرات المختصة بدراسة ظاهرة تبني المجتمعات للجديد، وتفترض النظرية أن المبتكرات المتمثلة بالمستحدثات والأفكار والأنماط الجديدة تتسرب إلى النظام الاجتماعي وتحظى بالقبول بشكل تدريجي تبعا للمتغيرات والظروف التي تحكم تلك البيئة الاجتماعية التي تتسرب إليها (الحديدي واللبان، 2009). وتفسر النظرية الانتشار الاجتماعي للأفكار والممارسات الجديدة سوسيولوجيا، وكذلك التبني الفردي لها انطلاقا من طبيعة عملية التغيير الاجتماعي، التي تربط الفرد بالجماعة تحت مسمى النسق الاجتماعي، ويعرف بأنه المعايير والأنماط السلوكية السائدة بين أفراد تنظيم اجتماعي، وهو أحد عناصر العميلة بالإضافة إلى عنصر المستحدث المتمثل بكل ما يتم إدراكه على أنه جديد، وعنصر قنوات الاتصال الجماهيري والشخصي، وكذلك عنصر المدة الزمنية اللازمة للانتشار والتبني التي تتسم بالتباين من فرد لآخر داخل التنظيم الاجتماعي ذاته (العلاق، 2010). وأشار روجرز إلى المحطات الأساسية لعملية تبني المستحدثات؛ حيث تتمحور المحطة الأولى حول الوعي بالفكرة الجديدة الذي قد يتشكل بمحض الصدفة وبطريقة عفوية، أو بطريقة عمدية مقصودة للتعرف إلى الفكرة، أما المحطة الثانية؛ فهي محطة الاهتمام بمعرفة الجوانب التفصيلية للفكرة، وفي هذه المحطة يصبح السلوك هادفا، وتليها محطة التقييم التي يتم فيها حصر المنافع المدركة من إخضاع الفكرة للتجريب العملي، ثم تأتي محطة التجريب لفحص الفكرة على نطاق ضيق واختبارها لفترة قصيرة المدى، وتختتم العملية بمحطة التبني التي تستند إلى اقتناع الفرد بنتائج المحطة السابقة؛ فإذا كانت النتائج التجريبية مرضية، يتم تبني الفكرة وتطبيقها على نطاق واسع، فيما إذا كانت غير مرضية، يتم رفضها والعزوف عن تبنها (الداغر، 2021).

ويمكن تطبيق نظرية انتشار المبتكرات في إطار الدراسة الحالية من خلال الكشف عن مجالات توظيف تطبيقات الذكاء الاصطناعي باعتبارها ظاهرة مستحدثة في تعزيز تشييد حاجز يفصل بين الأنظمة الأمنية والتهديدات في الفضاء السيبراني، وكذلك التحديات المصاحبة لتوظيفها، وذلك

لمساعدة المركز الوطني للأمن السيبراني على تحقيق هدفه الاستراتيجي المتمثل بتطوير منظومة مستدامة للعمليات السيبرانية. وبالإشارة لإحصائيات المركز الوطني للأمن السيبراني الفصل رقم (3210)، البرنامج رقم (6663)؛ فقد تبين ازدياد الحوادث الأمنية الوطنية المستهدف تعامل المركز معها من (1500) حادثة لعام (2023) إلى (2000) حادثة لعام (2024)، كما وتبين ازدياد عدد التهديدات المتطورة المستهدف التصدي لها من (45) تهديدا لعام (2023) إلى (50) تهديدا لعام (2024) (دائرة الموازنة العامة، 2023)، الأمر الذي يستدعي تسليط الضوء على توجه المركز المستقبلي لتوظيف تطبيقات الذكاء الاصطناعي في تحديد أشكال الجرائم الالكترونية والتهديدات السيبرانية المحتملة، وسبل مواجهتها.

الأمن السيبراني

أفرز ميدان التكنولوجيا الحيوية تقدما ذكيا في صناعة المعلومات وتحليل البيانات؛ إذ يعد الذكاء الاصطناعي ركيزة صناعة التكنولوجيا في العصر الحالي، وتعرفه منظمة اليونسكو بأنه حقن الآلات بقدرات تفوق قدرات العنصر البشري الإدراكية والحسية، إلا أنها تحاكي عملياته الذهنية الشائكة، مثل الاستقراء والاستنتاج، وتترجمها إلى ما يوازيها من عمليات منطقية (Villasenor, 2019).

ويهدف الذكاء الاصطناعي استراتيجيا إلى تطوير نظام مناعي يتناسب والشبكة العصبية، ويؤدي دور الخلايا البيضاء المتمثل بالتصدي للظواهر السلبية والتهديدات الأمنية المتنوعة، وفي هذا السياق اتجهت الولايات المتحدة والصين للاستثمار في المجال الذكي؛ إذ قامت الولايات المتحدة بتطوير علم الخوارزميات ليتكمن من تحديد الاستجابات الملائمة، واستحدثت تطبيقا يتنبأ بسلوك مرتكبي القضايا الجنائية بعد انقضاء سنوات سجنهم، وطورت الصين إنسانا آليا يصدر الأحكام النهائية في القضايا الصغيرة، وكذلك أولت الشركات الكبرى مثل؛ جوجل وأمازون ومايكروسوفت وأبل اهتماما بأبحاث الذكاء الاصطناعي، وقامت بتحصين قواعد بياناتها، وتأمين سرية المعلومات (الداغر، 2021).

كما وتسعى الدول العظمى والنامية في ظل هذا الصخب اللاأخلاقي والتطور المتلاحق للأنماط الإجرامية إلى الحفاظ على سلامة مجالها الأمني من الجرائم الإلكترونية العابرة للحدود الجغرافية، والتي أشار المشرع الأمريكي إلى أنها جناية ذات طابع تقني تتراوح بين الدرجتين الثانية والثالثة، وترتبط باستخدام الأنظمة والبيانات بطريقة غير قانونية، أو إلحاق الضرر المتعمد بها (صبرة، 2020).

وتختلف دوافع ارتكاب هذه الجنايات ذات الطابع التقني تبعا للأهداف؛ إذ قد يكون الدافع تجاريا بغية قرصنة وتخريب أعمال شركة تجارية معينة أو التجسس على صناعاتها وخدماتها، مثل الهجمة التي استهدفت ثغرات أنظمة التشغيل في شركة "مايكروسوفت" عام (2017)، وأسفرت عن تعطيل أعمال ما لا يقل عن (81) منظمة صحية، وقد يكون سياسيا بهدف الحصول على معلومات سياسية أو عسكرية تخص دولة معينة، وينشط هذا النوع عند نشوب الصراعات والتصعيدات، كما وقد يكون الدافع فرديا بغية ابتزاز أطراف معينة أو التعدي على معلومات حساباتهم الشخصية (Bhavani, 2020).

وأثبت الأمن السيبراني بشكل عام، والأمن متعدد الطبقات بشكل خاص قدرته على إحباط الهجمات الإلكترونية، وعرف الاتحاد الدولي للاتصالات الأمن السيبراني بأنه الممارسات والمهمات التقنية ومقاربات إدارة المخاطر الموظفة لحماية البيئة السيبرانية ومستخدمها والدفاع عنها ضد الهجمات الإلكترونية (Ramirez, Ariza & Miranda, 2022)، ويشير البحث في ضوء ذلك إلى الأمن السيبراني متعدد الطبقات، والمتمثل بالممارسات الأمنية التي تحيط المعلومات بطبقات دفاعية متداخلة وعدة برامج، وتحصن نقاط مرورها بعدد من ضوابط الأمان.

وكذلك أسهم المركز الوطني للأمن السيبراني منذ نشأته بموجب قانون الأمن السيبراني رقم (16) لعام (2019) ببناء منظومة فعالة للأمن السيبراني على المستوى الوطني، وتحصين الفضاء الأردني السيبراني من التهديدات والحوادث الإلكترونية من خلال تعزيز بنى المؤسسات الوطنية التحتية، وتأمين الخدمات الرقمية، وتطوير آليات الاستجابة للتهديدات (دائرة الموازنة العامة، 2023).

تطبيقات الذكاء الاصطناعي الموظفة لمكافحة الجريمة الإلكترونية

تسهم تطبيقات الذكاء الاصطناعي في تجميع الاستدلالات الجنائية؛ فلكل تطبيق وظيفة، منها ما هو على سبيل المثال لتوفير البيانات الجغرافية، ومنها ما هو لإنشاء تمثيل رياضي لملامح الجناة، الأمر الذي يقدم أدلة مادية شاهدة على وقوع جريمة فعلية أو أدلة منطقية تتنبأ بوقوع جريمة محتملة، والآتي يعرض أبرز تطبيقات الذكاء الاصطناعي الموظفة لمكافحة الجريمة الإلكترونية:

- طائرات الدرون (الطائرات دون طيار): يحتضن هذا النوع من الطائرات أجهزة استشعار حساسة، وكاميرات فائقة الدقة، الأمر الذي يمكنها من مراقبة الأمن المادي لبنية الشبكة بشكل تفصيلي، وتقديم تغذية بصرية فورية للبيانات التي تلتقطها أجهزتها، والكشف المبكر عن الخروقات المشبوهة، وكذلك فحص الأضرار المادية التي تصيب نقاطا يصعب الوصول إليها في الهوائيات أو في أطباق الأقمار الاصطناعية (Zhang et al., 2022).

- أنظمة جي بي أس: وهي أنظمة تتبع ديناميكي تنقل بيانات الموقع الجغرافي الذي ترسله الأقمار الاصطناعية إلى الهاتف المحمول ثم إلى هوائي الترحيل المسؤول عن إعادة إرسالها إلى مشغلي الاتصالات، ويتمثل مشغلو الاتصالات بشركات خطوط المحمول، والتي بدورها تنقل البيانات إلى خادم الشرطة (الدسوقي، 2022).

تطبيقات الذكاء الاصطناعي الموظفة لتعزيز الأمن السيبراني

لعبت تطبيقات الذكاء الاصطناعي وخوارزمياتها الدور التحليلي المتمثل بتجميع بيانات الخبرات السابقة، وإعادة تشكيلها للكشف عن أنماط الممارسات الإجرامية في الفضاء السيبراني، الأمر الذي عزز أمن هذا الفضاء، والآتي يعرض عددا من هذه التطبيقات:

- الأنظمة الكاشفة للتهديدات: وهي الأنظمة التي تستند إلى الذكاء الاصطناعي لتحليل قواعد البيانات بشكل دقيق، واستبعاد البيانات المزيفة، وكذلك الكشف عن الممارسات المشبوهة وتحليل مصادرها، مثل: أنظمة (IBM QRadar) ونظام (Csonka, 2020).(IDS/IPS)
- ملفات تعريف أمان وتحليل سلوك المستخدم: وهي النماذج التي تنشئ ملفات مخصصة لمستخدمي الشبكة من خلال التعلم الآلي لسلوكياتهم على الشبكة وتحليلها، الأمر الذي يمكنها من تحديد السلوكيات التي قد تبدو مغايرة لسلوك المستخدم المخزن في الملف؛ حيث إن الضربات على لوحة المفاتيح قد تمثل تهديدا تنبؤيا بأن المستخدم الذي يقوم بهذه الضربات غير مخول، وتتنبأ بالتهديدات بالوصول إلى الشبكة، مثل أداة (Darktrace)التي تتعلم سلوك الشبكة آليا (Reddt & Reddy, 2020).
- تطبيقات حظر روبوتات الويب أو ما يعرف باسم (Bots): وهي الحسابات المبرمجة التي تديرها برامج ضارة بهدف التلاعب بالبيانات والمعلومات، ونشر المضامين المضللة، لكنها تبدو وكأنها حسابات أفراد واقعيين؛ حيث تقوم هذه التطبيقات بحظر شبكة هذه الحسابات الآلية من خلال أدوات أمان التعلم الآلي التي تحلل نقاط البيانات السلوكية، وتشكل نماذج تنبؤية، وتحظر عناوين الويب بطريقة استباقية (عميره، 2019).
- أنظمة المنطق الغامض التي تثبت الحوادث استنادا إلى الخوارزمية الجينية والمنطق الضبابي: وهي أنظمة ذات قواعد غامضة توظف لتصنيف بيانات الهجوم على الشبكة؛ حيث إنها تثبت الهجمة خلال (2-3) ثوان من وصول البيانات إلى نظام الإثبات، وبمعدل يتجاوز ما نسبته (97.5%) (النيادي، 2022).
- العميل المحقق الذكي: وهي قوى متداخلة تحمي نظام التشغيل، وتتداول البيانات فيما بينها، وتقرر نمط الاستجابة المناسب في حال وقوع هجمة طارئة، بما فيها جرائم هجمات التطفل وعدوى الفيروسات (النيادي، 2022).
- تطبيق أمان (Wi-Fi): وهو تطبيق يوظف شبكة افتراضية خاصة تعمل على تشفير البيانات والمعلومات المرسلة من الشبكة، وكذلك الواردة إليها (Twaig, 2019).

وبالانتقال من البعد الوصفي إلى التأملي النقدي من خلال ربط التطبيقات الذكية بالإشكاليات الفلسفية والأخلاقية يتضح أن مجال الأمن القومي بشكل عام والأمن الإلكتروني بشكل خاص مجال خصب لمواطن الضعف الناتجة عن توظيف تطبيقات الذكاء الاصطناعي في اتخاذ القرارات الأمنية، الأمر الذي يثير تساؤلاً متعلقاً بالمسؤولية الأخلاقية في حال حدوث أخطاء.

وفي هذا الصدد أوضحت محكمة استئناف باريس أن فكرة تشخيص الروبوت قانونياً على سبيل المثال تنقل الخطأ ولا تسهم في معالجته؛ فالعنصر البشري المساهم في تغذية الذمة المالية للروبوت لتعويض ضحايا خطؤه هو العنصر البشري ذاته الذي ستنعقد مسؤوليته في حال تطبيق القواعد العامة للمسؤولية، وذلك إذا تبين إهماله للروبوت، أو التسبب في خلل برمجته (محروس، 2024).

كما ويمكن استشراف مسؤولية أخطاء التطبيقات الذكية بالقياس على مسؤولية حوادث الطائرات؛ فالحوادث الناتجة عن الأعطال الميكانيكية المتمثلة بأعطال المحرك أو أعطال النظام الهيدروليكي المُتحكم بالفرامل أو تلوث الوقود تقع مسؤوليتها على الكادر البشري الفني المنوط بمهمة الصيانة، وحوادث الاصطدامات الناتجة عن تقارب المسافات بين الطائرات تقع مسؤوليتها على المراقب الجوي، ومن هنا يرى الباحثان أن العناصر البشرية القائمة على صيانة التطبيق الذكي أو توجيهه أو التحقق من صحة معلوماته هي المسؤولة عن الثغرات الأخلاقية، وبهذا ينفي هذا التأمل الفلسفي إمكانية الاستغناء عن العنصر البشري في الحقل الأمني واستبداله بالعنصر الذكي اصطناعياً.

ويشير الباحثان إلى الإشكاليات الناتجة عن تغير سياقات العمل الأمني، والمسؤوليات الموكلة إليه في ضوء توظيف التطبيقات الذكية؛ حيث أثار ظهور الوكلاء الجُدد في الأدوار الأمنية العلامات الاستفهامية حول استبدال الحدس والخبرة البشرية بالتطبيقات الذكية في التعامل مع الجرائم الإلكترونية، لذا وجبت الإشارة إلى أن خوارزميات التطبيقات تتحرك داخل الإطار المفاهيمي الذي صممه العنصر البشري لها، مما يجعلها عاجزة عن القيام بالممارسات التحليلية والتحقيقية والاستقصائية، وكذلك عن بلوغ الإبداع الذي يقتضي العبور العقلي إلى أطر مفاهيمية جديدة، كما ولا يُتوقع منها مراقبة وتتبع الإنذارات غير المتوقعة، والتي يتتبعها العنصر البشري ويُجري اتصالاته للتحقق من عناصرها، وهذا ينفي قدرتها على أن تحل محل القرار الأمني، ويوضح أنها أدوات مكملة له.

الدراسات السابقة

تعرض الدراسة عددا من الدراسات العربية والأجنبية التي أجريت في المجال على النحو المدرج أدناه:

- هدفت دراسة **(الهنائي، 2024) بعنوان: "تطبيقات الذكاء الاصطناعي في المجال الأمني: دراسة مطبقة على دول مجلس التعاون لدول**

الخليج العربية" الكشف عن واقع تطبيق الذكاء الاصطناعي في المجال الأمني في دول مجلس التعاون الخليجي، واستندت الدراسة إلى المنهج الوصفي التحليلي، واستخدمت الاستبانة لجمع البيانات، وبلغ قوام العينة (150) مفردة من القانونيين، والأمنيين، والتقنيين. أوضحت النتائج أهمية توظيف الذكاء الاصطناعي في الهوية الرقمية، والاستعانة بنظام (جي بي اس) لرصد النقاط السوداء، كما وكشفت عن أبرز التحديات المترتبة على تطبيق الذكاء الاصطناعي في المجال الأمني، وهي على التوالي: ارتفاع تكلفة الأجهزة والتقنيات، وقدرة الذكاء الاصطناعي على تهديد الأمن المعلوماتي من خلال اختراق الشبكات، وصعوبة التعامل مع التقنيات، وكذلك أشارت النتائج إلى المقترحات التي من شأنها تنظيم تطبيق الذكاء الاصطناعي في المجال الأمني، والمتمثلة بتكاتف الرؤى لاعتماد استراتيجية خليجية موحدة للذكاء الاصطناعي، وإقرار مشروع قانوني شامل، وكذلك عقد الدورات التدريبية في القطاعات الأمنية.

- هدفت دراسة **(قاسم، 2024) بعنوان: "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية"** التعرف إلى دور الذكاء الاصطناعي في مكافحة الجريمة الالكترونية وموقف التشريعات القانونية العربية منه، واعتمدت الدراسة المنهج الوصفي التحليلي والمنهج المقارن، وخلصت الدراسة إلى إمكانية توظيف تطبيقات الذكاء الاصطناعي المتمثلة بالشبكات العصبية والخوارزميات لمجابهة الجرائم الإلكترونية والكشف عن هوية مرتكبيها، كما وأشارت إلى تصدر الأنظمة السعودية والإماراتية قائمة الدول العربية الأكثر مواكبة لتطورات علم الذكاء الاصطناعي بفرعيه الصناعي والقانوني من خلال استحداث تشريعات مستقلة، وكذلك تطوير أداء الأجهزة الأمنية على نحو يمكنها من توظيف التطبيقات الاصطناعية لمكافحة هذا النوع من الجرائم.

- هدفت دراسة **(سالم وأبو الجدايل، 2023) بعنوان: "فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي"** الكشف عن التوجه المستقبلي لتوظيف تقنيات الذكاء الاصطناعي من قبل الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية، وتعد من الدراسات الاستكشافية، واعتمدت منهج المسح بفرعه الكمي، وأداة الاستبانة لجمع البيانات من عينة قوامها (106) مفردة من العاملين في الهيئة الوطنية للأمن السيبراني في السعودية. بينت النتائج قدرة تقنيات الذكاء الاصطناعي على التعامل مع الكم الهائل من البيانات، الأمر الذي عدته العينة دافعا لتوظيفها في المستقبل، كما وجاءت جريمة التلاعب في المعلومات بقصد إتلافها في مقدمة الجرائم الإلكترونية التي ينبغي توظيف تقنيات الذكاء الاصطناعي للحد منها.

- هدفت دراسة **(أبو علان، 2022) بعنوان: "معوقات تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونية من وجهة نظر العاملين في وزارة الاتصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة"** التعرف إلى تحديات تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الالكترونية، واعتمدت الدراسة المنهج الوصفي بفرعه الكيفي، واستخدمت المقابلة المتعمقة لجمع البيانات من مجتمع الدراسة المتمثل بالعاملين في وزارتي الاتصالات وتكنولوجيا المعلومات في مدينتي رام الله والبيرة في فلسطين، والبالغ عددهم (50) مفردة وفقا لإحصائيات وزارة الاتصالات وتكنولوجيا المعلومات لعام (2021). أشارت نتائج الدراسة إلى دور الذكاء الاصطناعي الفعال في الكشف عن الجرائم الالكترونية، وبعد المجتمع الفلسطيني عن سلسلة التطورات التكنولوجية نتيجة لتحديات مختلفة مرتبطة بالبنية التحتية، والموازنات المالية، وكذلك الكادر البشري.

- هدفت دراسة **(الداغر، 2021) بعنوان: "اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر"** الكشف عن اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وانعكاساته على دعم الأمن السيبراني في جمهورية مصر العربية، وهي دراسة وصفية، اعتمدت منهج المسح الإعلامي وأسلوب المقارنة المنهجية على عينة قوامها (106) مفردة من النخبة الأمنية والإعلامية والأكاديمية المصرية، كما واستندت إلى أداة الاستبانة لجمع البيانات. أشارت نتائج الدراسة إلى إيجابية اتجاهات العينة نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية، والحد من انتشارها، وكذلك التنبؤ بالكوارث المحتمل حدوثها، كما وأسفرت في المقابل عن وجود بعض التهديدات المصاحبة لتوظيف الذكاء الاصطناعي في الإعلام الأمني، والمتمثلة بالمعالجة السطحية للأحداث، واحتمالية تدمير بنى الدول التحتية.

- هدفت دراسة **(Shetty, Choi & Park, 2024) بعنوان: "Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures"** التحقيق في التقاطع بين تطبيقات الذكاء الاصطناعي والجرائم الإلكترونية من حيث الاتجاهات والمخاطر والتدابير المضادة، واعتمدت الدراسة على المنهج الوصفي بفرعيه الكمي والكيفي؛ إذ تم جمع بيانات التحليل الكمي من خلال (102) مطالبة تفيد بتوظيف تطبيقات الذكاء الاصطناعي في الأنشطة الضارة، وجاءت هذه المطالبات في ثمانية منتديات كانت بمثابة منصات لإيصال مطالبات أفراد من خلفيات لغوية وثقافية مختلفة، كما وتم جمع البيانات النوعية من خلال إجراء المقابلات المتعمقة مع (6) خبراء في مجال الجرائم الاكترونية، والأمن السيبراني، والعدالة الجنائية. أظهرت نتائج الدراسة تزايد سبل الاستخدام غير الأخلاقي مع تزايد توظيف تطبيقات الذكاء الاصطناعي في مجالات الحياة المختلفة، الأمر الذي يتطلب تضافر الجهود لتطوير أطر فعالة أكثر مسؤولية وعدالة لحماية البيئات الرقمية من الجرائم.

- هدفت دراسة **(Umair, Letchmunan, Fadratul & Tieng, 2024) بعنوان: "Leveraging transfer learning with deep learning for crime prediction"** تطوير نموذج ذكاء اصطناعي للتنبؤ بالجرائم من خلال الاستعانة بشبكة عصبية تكرارية تستخدم اللغة الطبيعية لمعالجة

معلومات النصوص تدعى " ذاكرة ثنائية الاتجاه طويلة المدى"، وذلك لاختبار دقة التنبؤ؛ إذ رصدت الدراسة بيانات الجريمة التجريبية الزمانية والمكانية، وقسمتها إلى مجموعتين؛ تدريبية واختبارية، ثم دربت الذاكرة على المجموعة الأولى، وقيمت أداءها على المجموعة الثانية، وأظهرت النتائج قدرة الذاكرة على فهم التداخلات بين الكلمات المكونة للنص بشكل أفضل، كما وكشفت في المقابل عن ظهور بعض المشكلات المتعلقة بالدقة رغم توظيف تقنيات التعلم الآلي والتعلم العميق.

- هدفت دراسة **(Al-Marghilani, 2022) بعنوان: "Target detection algorithm in crime recognition using artificial intelligence"** تطوير نموذج ذكاء اصطناعي لتجويد عملية تحديد هوية مرتكبي الجرائم المالية؛ حيث استند نموذج الدراسة إلى تقنيات التعلم العميق لتوليف رسم الوجه للمشتبه به، ويمر النموذج المقترح بثلاث محطات، وهي على التوالي: محطة المعالجة السابقة لفحص جودة الصورة، وتليها محطة استنباط العلامات الفارقة، ثم محطة توظيف الخوارزمية لتوليف رسم الوجه. أسفرت نتائج الدراسة عن دقة تمثيل النموذج المقترح للبيانات وبسرعة استجابة عالية؛ إذ بلغ متوسط الدقة (93.4%)، وبلغ متوسط وقت الاستجابة (0.002) ثانية، كما وأسفرت عن تمتع الصور المنتجة بواسطته بجودة عالية.

التعقيب على الدراسات السابقة

تشابهت الدراسات السابقة إلى حد كبير في **الأهداف**؛ حيث ابتغت رصد الأدوار التي تؤديها تطبيقات الذكاء الاصطناعي في الحقل الأمني بشكل عام، ومكافحة الجرائم الإلكترونية بشكل خاص، كما وطورت بعض الدراسات نماذج ذكية لمكافحة الجريمة الالكترونية بطريقة استباقية تتنبأ بحدوثها، وتمحورت **المناهج المعتمدة** في الدراسات السابقة حول المنهج الوصفي المسحي بشقه الكمي، والمنهج الوصفي المسحي بشقيه الكمي والكيفي، والمنهج المقارن، وكذلك المنهج التجريبي، كما واعتمدت الدراسات السابقة على عدد من **الأدوات البحثية**، مثل: الاستبانة، والمقابلة المتعمقة، وتراوحت **العينة** في الدراسات السابقة بين القانونيين، والخبراء في مجال الجرائم الإلكترونية والأمن السيبراني والعدالة الجنائية، وكذلك العاملين في المجال الأمني، والإعلاميين، والأكاديميين. كما وأظهر العرض السابق عدم تطرق الدراسات السابقة لاتجاهات عينة الدراسة، والمتمثلة بالمختصين الأردنيين العاملين في المركز الوطني للأمن السيبراني، ومن مختلف المسميات الوظيفية في المركز، مثل: قانوني رئيسي، ومبرمج مساعد، ومحلل شبكات، ومحلل نظم، ومدرب أمن سيبراني، وكذلك مهندس شبكات **وهذا ما يميز الدراسة الحالية**.

نوع الدراسة ومنهجها

تنتمي الدراسة الحالية إلى الدراسات الوصفية التي تهدف الكشف عن الأوصاف الدقيقة للظاهرة موضوع البحث؛ حيث إن هذا الوصف الدقيق يصب اهتمامه على طبيعة الظاهرة، وماهيتها، وشبكة العلاقات والتداخلات والعوامل المؤثرة فيها، واستندت الدراسة في ضوء ذلك إلى منهج المسح بشقه الكمي.

مجتمع الدراسة

تمثل مجتمع الدراسة بالعاملين في المركز الوطني للأمن السيبراني، والبالغ عددهم (349) مفردة وفقا لإحصائيات المركز الوطني للأمن السيبراني لعام (2023) الفصل (3210).

عينة الدراسة

بلغ قوام العينة (100) مفردة من المختصين الأردنيين العاملين في المركز الوطني للأمن السيبراني، وباستخدام العينة القصدية، كما وتمثلت أبرز الأسباب التي دفعت لاعتماد حجم العينة بقدرتها على تمثيل المجتمع المدروس بوصفها دراسة وصفية تؤثر مشكلتها ومتغيراتها وخصائصها على حجم العينة، وبالنظر إلى صغر حجم مجتمع الدراسة يتضح دقة تمثيل العينة للمجتمع غير المتجانس، الأمر الذي أتاح تعميم نتائجها، وتوضح بيانات الجدول (1) توزيع أفراد عينة الدراسة تبعا لمتغيراتها الديموغرافية.

الجدول رقم (1) الوسط الحسابي والانحراف المعياري للمتغيرات الديموغرافية

المتغير	الفئات	التكرار	النسبة المئوية	الوسط الحسابي	الانحراف المعياري
النوع الاجتماعي	ذكر	54	54	1.46	0.501
	أنثى	46	46		
	المجموع	100	%100		
الفئة العمرية	25 - 35	14	14	2.25	0.687
	36 - 45	47	47		
	46 فأكثر	39	39		
	المجموع	100	%100		
الدرجة العلمية	بكالوريوس	76	76	3.24	0.429
	دراسات عليا	24	24		
	المجموع	100	%100		
المسمى الوظيفي	IT	8	8	-	-
	باحث أمن سيبراني	12	12	-	-
	ضابط تخطيط استراتيجي	14	14	-	-
	قانوني رئيسي	7	7	-	-
	مبرمج مساعد	12	12	-	-
	محلل شبكات	8	8	-	-
	محلل نظم	8	8	-	-
	مدرب أمن سيبراني	18	18	-	-
	مهندس شبكات	13	13	-	-
المجموع		**100**	**%100**		

وتشير بيانات الجدول (1) إلى النتائج الآتية:

- **متغير النوع الاجتماعي:** جاءت فئة الذكور بأعلى تكرار، وبنسبة مئوية بلغت (54%)، في حين جاءت فئة الإناث بأقل تكرار، وبنسبة مئوية بلغت (46%)، وبلغ الوسط الحسابي للنوع الاجتماعي (1.46).

- **متغير الفئة العمرية:** جاءت الفئة من "36-45" بأعلى تكرار، وبنسبة مئوية بلغت (47%)، وتليها فئة "46 سنة فأكثر" بنسبة (39%)، بينما جاءت الفئة من "25-35" بأقل تكرار، وبنسبة مئوية بلغت (14%)، وبلغ الوسط الحسابي للفئة العمرية (2.25).

- **متغير الدرجة العلمية:** إن معظم المستجيبين ممن شملتهم عينة الدراسة من حملة شهادة البكالوريوس؛ حيث بلغت النسبة المئوية (76%)، وما نسبتهم (24%) من حملة شهادة الدراسات العليا، وبلغ الوسط الحسابي للمستوى العلمي (3.24).

- **متغير المسمى الوظيفي:** جاء المسمى الوظيفي "مدرب أمن سيبراني" بأعلى تكرار، وبنسبة مئوية بلغت (18%)، بينما جاء المسمى "قانوني رئيسي" بأقل تكرار، وبنسبة مئوية بلغت (7%).

أداة جمع البيانات

اعتمدت الدراسة على "الاستبانة" لجمع البيانات، كما وتم تصحيح أداة الدراسة من خلال منح درجة موافق (3)، ودرجة محايد (2)، ودرجة غير موافق (1)، والاعتماد على التصنيف الآتي للحكم على المتوسطات الحسابية: (أعلى قيمة – أقل قيمة)/ 3 وتساوي: (3-1) / 3 = 0.66 طول الفئة، كما واعتمد الباحثان المقياس الآتي لوصف الوسط الحسابي: من (1- 1.66) منخفضة، من (1.67 - 2.33) متوسطة، من (2.34 – 3) مرتفعة.

صدق الأداة (الاستبانة) وثباتها

تم التحقق من الصدق الظاهري لأداة الدراسة من خلال عرضها على مجموعة من المحكمين تألفت من (9) من أعضاء الهيئات التدريسية في الجامعات الأردنية، والمتخصصين في المجالات الآتية: القانون، والأمن السيبراني، وكذلك الإعلام الرقمي. وتم التحقق من ثبات أداة الدراسة من خلال حساب معاملات

الارتباط بين كل فقرة من الفقرات في الاستبانة عن طريق استخدام معادلة كرونباخ ألفا على عينة الدراسة الأصلية، وذلك لمعرفة ثبات الاتساق الداخلي لفقرات أداة القياس لكل محور من محاور أداة القياس، وتشير بيانات الجدول رقم (2) أدناه إلى نتائج تحليل الاعتمادية (Analysis Reliability).

الجدول رقم (2) قيم معامل كرونباخ ألفا لمحاور أداة القياس وللأداة ككل

الرقم	محاور أداة الدراسة	قيمة معامل كرونباخ ألفا
1	المحور الأول: توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني	0.925
2	المحور الثاني: أشكال الجرائم الالكترونية والتهديدات السيبرانية	0.901
3	المحور الثالث: مقومات نجاح توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية	0.914
جميع محاور الدراسة مجتمعة		**0.913**

توضح بيانات الجدول رقم (2) أن قيمة معامل كرونباخ ألفا لكل محور من محاور الدراسة قد جاءت أعلى من (70%)، كما بلغت قيمة معامل كرونباخ ألفا لجميع فقرات أداة القياس في جميع المحاور (91.3%)، وهي نسبة تدل على ثبات الاتساق الداخلي لفقرات كل محور، وعلى وضوح الفقرات ومفرداتها للعينة التي شملتها الدراسة، وكذلك جاهزيتها للتحليل الإحصائي؛ فإذا بلغت قيمة معامل كرونباخ ألفا (70%) أو أكثر، فإن أداة القياس تعتبر مقبولة في معظم الدراسات الاجتماعية، وتتمتع بموثوقية كافية لاستنباط النتائج (Nunnally, 1978, P245).

نتائج الدراسة ومناقشتها

فيما يأتي عرض للنتائج التي خلصت إليها الدراسة، ومناقشتها في ضوء تساؤلاتها وفروضها:

نتائج التساؤل الأول: اتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني.

الجدول رقم (3) الوسط الحسابي، الانحراف المعياري والنسب والتكرارات لاتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
1	اتجاهاتي إيجابية؛ كون تطبيقات الذكاء الاصطناعي تخدم العمل الأمني، وتحد من الانتهاكات والتهديدات	2.94	0.239	98%	**مرتفع**	**1**
2	سيبقى العمل الأمني كما هو، ولن يتغير بتوظيف هذه التطبيقات	1.14	0.349	38%	**منخفض**	**2**
3	اتجاهاتي سلبية؛ كون تطبيقات الذكاء الاصطناعي تعرقل العمل الأمني وتخدم مرتكبي الجرائم، وتعيق السيطرة على الفوضى الرقمية	1.09	0.288	36.3%	**منخفض**	**3**
	الوسط الحسابي للفقرات جميعها	**1.723**	**0.292**	**%57.4**	**متوسط**	

تشير بيانات الجدول (3) إلى المتوسطات الحسابية والانحرافات المعيارية ومؤشرات الوسط الحسابي لاتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني؛ حيث جاءت الفقرة رقم (1) التي تنص على "اتجاهاتي إيجابية؛ كون تطبيقات الذكاء الاصطناعي تخدم العمل الأمني، وتحد من الانتهاكات والتهديدات" في المرتبة الأولى، وسجلت أعلى مؤشر للوسط الحسابي، كما وبلغ الوسط الحسابي (2.94)، وهذا يدل على أن مؤشر الموافقة على هذه الفقرة مرتفع جدا، في حين جاءت الفقرة رقم (2) والتي تنص على "سيبقى العمل الأمني كما هو، ولن يتغير بتوظيف هذه التطبيقات" في المرتبة الثانية وبوسط حسابي (1.14)، وهذا يدل على قابلية العمل الأمني للتغير بتوظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني، أما الفقرة رقم (3) والتي تنص على "اتجاهاتي سلبية؛ كون تطبيقات الذكاء الاصطناعي تعرقل العمل الأمني وتخدم مرتكبي الجرائم، وتعيق السيطرة على الفوضى الرقمية" فقد سجلت أقل مؤشر للوسط

الحسابي، وبلغ الوسط الحسابي (1.09)، وهذا ينفي وجود اتجاهات سلبية أو محايدة لدى العينة موضوع الدراسة.

واتفقت هذه النتائج مع نتائج دراسة (أبو علان، 2022) التي أشارت إلى دور الذكاء الاصطناعي الفعال في الكشف عن الجرائم الالكترونية، وكذلك اتفقت مع نتائج دراسة (الداغر، 2021) التي أسفرت عن إيجابية اتجاهات العينة نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية، والحد من انتشارها، وكذلك التنبؤ بالكوارث المحتمل حدوثها.

نتائج التساؤل الثاني: مجالات توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين.

الجدول رقم (4) الوسط الحسابي، الانحراف المعياري والنسب والتكرارات لمجالات توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
8	الطائرة دون طيار (Drones) والتي تستخدم لتقييم أمان الشبكات اللاسلكية، وتحديد نقاط الوصول غير المصرح بها، وكذلك فحص البنية التحتية وتحديد فيما إذا تعرضت للاختراق	2.93	0.026	97.7%	مرتفع	1
3	كاميرات (آي بي) المستخدمة لمراقبة الأماكن الحيوية، ومطابقة أوجه الأفراد في هذه الأماكن مع أوجه الأفراد المسجلين مسبقا في قوائم الأجهزة الأمنية	2.92	0.027	97.3%	مرتفع	2
10	تطبيقات التحليل الاجتماعي التي تحلل بيانات شبكات التواصل الاجتماعي، وتكشف احتمالية وقوع أعمال شغب في منطقة معينة	2.92	0.027	97.3%	مرتفع	3
11	تطبيق التتبع الديناميكي (GPS) لرصد التحركات وتحديد الموقع الجغرافي	2.86	0.035	95.3%	مرتفع	4
1	أجهزة محاكاة أبراج الهواتف الخلوية (ستينجراي)؛ وهي أجهزة رصد وتجسس تطلق ترددات تمكنها من الاطلاع على البيانات والرسائل والاتصالات في منطقة معينة بأكملها	2.84	0.037	94.7%	مرتفع	5
4	التطبيقات الذكية القادرة على كشف زيف الصور، والعروض المرئية والسمعية (الفيديو) مثل تطبيق "إنفيديا"، وتقنية البحث العكسي للصور	2.65	0.048	88.3%	مرتفع	6
5	تطبيق (Tin Eye) الذي يتتبع مصدر الصور	2.65	0.048	88.3%	مرتفع	7
7	تطبيق (Fico-Falcon) الذي يستند إلى شبكة عصبية تمكنه من اكتشاف الاحتيال في المعاملات المالية، والتعامل معه بطريقة رقمية	2.35	0.048	78.3%	مرتفع	8
9	التطبيقات الذكية المعنية بالكشف عن البرامج الضارة (الفيروسات)	2.32	0.047	77.3%	متوسط	9

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
12	التطبيقات الذكية المعنية بالتنبؤ بالتهديدات التي قد تتعرض لها المؤسسات من خلال تحليل بيانات التجارب السابقة	2.24	0.043	74.7%	متوسط	10
6	التطبيقات الذكية القادرة على تحليل الوثائق والتقارير القانونية، واستنباط البيانات المهمة بشكل فوري مثل تطبيق (COIN)	2.11	0.031	70.3%	متوسط	11
2	بصمة المخ؛ وهي تقنية تمسح دماغ المشتبه به للتحقق من وجود معلومات يمتلكها عن جريمة معينة	1.6	0.049	53.3%	منخفض	12
	الوسط الحسابي للفقرات جميعها	**2.533**	**0.039**	**84.4%**	مرتفع	

تعكس بيانات الجدول رقم (4) المتوسطات الحسابية والانحرافات المعيارية ومؤشرات الوسط الحسابي لمجالات توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين؛ حيث احتلت الفقرة رقم (8) التي تنص على "الطائرة دون طيار (Drones)" المرتبة الأولى، وسجلت أعلى مؤشر للوسط الحسابي، وبلغ الوسط الحسابي (2.93)، وهذا يدل على أن مؤشر الموافقة على هذه الفقرة مرتفع جدا، كما واحتلت الفقرتان (3) و(10) "كاميرات (آي بي)" و"تطبيقات التحليل الاجتماعي التي تحلل بيانات شبكات التواصل الاجتماعي" المرتبة الثانية بدرجة مرتفعة، وبالوسط الحسابي ذاته (2.92)، وحصدت الفقرة (11) التي تنص على "تطبيق التتبع الديناميكي (GPS)" المرتبة الثالثة بدرجة مرتفعة، وبلغ الوسط الحسابي (2.86)، كما واحتلت الفقرة المتعلقة بأجهزة محاكاة أبراج الهواتف الخلوية (ستينجراي) المرتبة الرابعة بدرجة مرتفعة، وجاءت الفقرات (6، 9، 12) بمؤشر موافقة متوسط، بينما سجلت الفقرة رقم (2) التي تنص على "بصمة المخ" أقل مؤشر للوسط الحسابي؛ حيث بلغ الوسط الحسابي (1.6)، وهو مؤشر منخفض من الموافقة، وكذلك بلغ الوسط الحسابي لجميع فقرات المحور (2.533) وبدرجة مرتفعة.

وتعكس هذه النتائج تعدد مجالات الذكاء الاصطناعي التي من شأنها مكافحة جرائم الفضاء السيبراني وتعزيز أمنه، ويرى المختصون الأردنيون أن أبرز المجالات تتمثل بالتطبيقات المعنية بتقييم أمان الشبكات اللاسلكية، وتحديد نقاط الوصول غير المصرح بها، وفحص البنية التحتية، ومراقبة الأماكن الحيوية، وكذلك تحليل البيانات الاجتماعية، ورصد التحركات وتحديد الموقع الجغرافي، كما واتفقت هذه النتائج مع نتائج دراسة (الهنائي، 2024) التي عكست أهمية الاستعانة بنظام (جي بي اس) لرصد النقاط السوداء.

نتائج التساؤل الثالث: أشكال الجرائم الإلكترونية والتهديدات السيبرانية التي تقتضي توظيف تطبيقات الذكاء الاصطناعي لمكافحتها من وجهة نظر المختصين الأردنيين.

الجدول رقم (5) الوسط الحسابي، الانحراف المعياري والنسب والتكرارات لأشكال الجرائم الإلكترونية والتهديدات السيبرانية التي تقتضي توظيف تطبيقات الذكاء الاصطناعي لمكافحتها

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
6	التهديد والابتزاز	2.96	0.197	98.7%	مرتفع	1
7	قرصنة البيانات والحسابات، والتعدي عليها بالإتلاف أو التحريف	2.96	0.197	98.7%	مرتفع	2
1	الاحتيال والنصب	2.94	0.239	98%	مرتفع	3
3	السب والتشهير والقذف	2.92	0.273	97.3%	مرتفع	4
4	الدعاية المضللة، والترويج للشائعات	2.53	0.502	84.3%	مرتفع	5
2	انتهاك الخصوصية، والملكية الفكرية	2.43	0.498	81%	مرتفع	6
9	التجسس الصناعي والعسكري الذي يلحق ضررا بالاقتصاد القومي	2.42	0.496	80.7%	مرتفع	7

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
10	الأخطار التي تصيب الكابلات البحرية التي تضرب البنى التحتية محدثة خللا في عمل المؤسسات المرتبطة خدماتها بشكبة الانترنت	2.18	0.386	72.7%	**متوسط**	**8**
5	إثارة الفتن الطائفية	1.98	0.2	66%	**متوسط**	**9**
8	الإرهاب الالكتروني	1.98	0.2	66%	**متوسط**	**10**
	الوسط الحسابي للفقرات جميعها	**2.53**	**0.319**	**84.3%**	**مرتفع**	

توضح بيانات الجدول رقم (5) المتوسطات الحسابية والانحرافات المعيارية ومؤشرات الوسط الحسابي لأشكال الجرائم الالكترونية والتهديدات السيبرانية التي تقتضي توظيف تطبيقات الذكاء الاصطناعي لمكافحتها من وجه نظر المختصين الأردنيين؛ حيث احتلت الفقرتان (6) و(7) واللتان تشيران إلى "التهديد والابتزاز" و" قرصنة البيانات والحسابات، والتعدي عليها بالإتلاف أو التحريف" على التوالي المرتبة الأولى بدرجة مرتفعة، وبأعلى متوسط حسابي (2.96)، واحتلت الفقرة رقم (1) والتي تشير إلى "الاحتيال والنصب" المرتبة الثانية بدرجة مرتفعة، وبمتوسط حسابي (2.94)، وكانت المرتبة الثالثة من نصيب الفقرة رقم (3) المتعلقة بجرائم السب والتشهير والقذف، حيث جاءت بدرجة مرتفعة وبمتوسط حسابي بلغ (2.92)، كما وجاءت الفقرة رقم (4) المتعلقة بالدعاية المضللة في المرتبة الرابعة، وبدرجة مرتفعة ومتوسط حسابي بلغ (2.53)، بينما جاءت الفقرتان رقم (5) و(8) المتعلقتان بإثارة الفتن الطائفية والإرهاب الإلكتروني في المرتبة الأخيرة بدرجة متوسطة، وبالوسط الحسابي ذاته (1.98)، الأمر الذي يوضح أن درجة أشكال الجرائم الالكترونية والتهديدات السيبرانية التي تقتضي توظيف تطبيقات الذكاء الاصطناعي لمكافحتها من وجه نظر المختصين الأردنيين مرتفعة.

وتسفر هذه الأشكال الإجرامية التي جاءت بدرجة مرتفعة عن وجود ضرورة لتوظيف تطبيقات الذكاء الاصطناعي في التصدي لها من وجهة نظر المختصين الأردنيين، وكذلك عن تعرض الفضاء السيبراني الأردني بشكل كبير لهذه التهديدات المتمثلة بالابتزاز والقرصنة والاحتيال والنصب، بينما لوحظ غياب تعرضه للتهديدات الطائفية والإرهابية، مما يعكس سيطرة الأجهزة الأمنية الأردنية على مثل هذه العمليات الإجرامية، وقدرتها بالسيطرة على خلاياها.

ولا بد من الإشارة إلى تنامي المخاوف بشأن حقوق المواطنين الأساسية مع تنامي توظيف التطبيقات الذكية في العمل الأمني، مما هدد الخصوصية الرقمية بالتآكل.

واتفقت هذه النتائج مع نتائج دراسة (سالم وأبو الجدايل، 2023) التي رتبت جريمة التلاعب في المعلومات بقصد اتلافها في مقدمة الجرائم الإلكترونية التي ينبغي توظيف تقنيات الذكاء الاصطناعي للحد منها، كما واتفقت مع نتائج دراسة (Shetty, Choi & Park, 2024) التي استندت إلى تحليل (102) مطالبة توضيح تزايد سبل الاستخدام غير الأخلاقي مع تزايد توظيف تطبيقات الذكاء الاصطناعي في مجالات الحياة المختلفة، الأمر الذي يستدعي توظيف التطبيقات بطريقة مضادة؛ حيث إن تزايد استخدامها بطريقة غير أخلاقية يمنح استخدامها بطريقة أخلاقية الفرصة ذاتها، وبذلك تعالج التهديدات والجرائم بالأدوات الذكية التي طورت البرامج الخبيثة وكذلك الحميدة، وهنا يأتي دور المختصين في الأمن السيبراني للتفريق بين البرامج، وتوظيف الحميد منها للحد من الخبيث قدر المستطاع.

نتائج التساؤل الرابع: ما مقومات نجاح توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين.

الجدول رقم (6) الوسط الحسابي، الانحراف المعياري والنسب والتكرارات لمقومات نجاح توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
5	استحداث إطار قانوني تشريعي يستهدف تنظيم استخدام هذه التطبيقات من قبل الأفراد والمؤسسات، ويضبط أداءهم في نقل الأحداث	2.97	0.171	99%	**مرتفع**	**1**
4	تحصين مؤسسات الدولة والمجتمع المدني من الاختراق السيبراني من خلال شيفرات موثوقة	2.96	0.197	98.7%	**مرتفع**	**2**
1	دعم أداء المؤسسات الأمنية من خلال رفدها بالإمكانيات المادية والبشرية والتقنية	2.92	0.273	97.3%	**مرتفع**	**3**
3	تطوير أداء العاملين في الجهاز الأمني من خلال	2.92	0.273	97.3%	**مرتفع**	**4**

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
	عقد الدورات التدريبية وورش العمل، وتنظيم اللقاءات الدورية مع المتخصصين في مجال الذكاء الاصطناعي والأمن السيبراني					
2	استحداث منصات اتصالية تعزز تفاعل الأجهزة الأمنية والمواطنين، وتنشر الوعي الأمني، وتقدم البرامج التوعوية، وتنظم الحملات الإعلامية التي تعد خطابا موحدا يعزز الوحدة الوطنية والتعايش المجتمعي	2.29	0.456	76.3%	متوسط	5
	الوسط الحسابي للفقرات جميعها	**2.812**	**0.274**	**93.7%**	**مرتفع**	

توضح بيانات الجدول رقم (6) المتوسطات الحسابية والانحرافات المعيارية ومؤشرات الوسط الحسابي لمقومات نجاح توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين؛ حيث جاءت الفقرة رقم (5) التي تشير إلى "استحداث إطار قانوني تشريعي يستهدف تنظيم استخدام هذه التطبيقات من قبل الأفراد والمؤسسات، ويضبط أداءهم في نقل الأحداث" في المرتبة الأولى وبدرجة مرتفعة، كما وسجلت أعلى مؤشر للوسط الحسابي؛ إذ بلغ الوسط الحسابي (2.97)، وتلتها الفقرة رقم (4) والمتعلقة بتحصين مؤسسات الدولة والمجتمع المدني من الاختراق السيبراني من خلال شيفرات موثوقة في المرتبة الثانية وبدرجة مرتفعة، وبلغ الوسط الحسابي (2.96)، وجاءت الفقرتان (1) و(3) واللتان تشيران إلى دعم أداء المؤسسات الأمنية من خلال رفدها بالإمكانيات المادية والبشرية والتقنية، وكذلك تطوير أداء العاملين في المرتبة الثالثة ذاتها، وبدرجة مرتفعة ووسط حسابي بلغ (2.92)، بينما حصدت الفقرة رقم (3) والمتعلقة باستحداث منصات اتصالية تعزز تفاعل الأجهزة الأمنية والمواطنين المرتبة الأخيرة بدرجة متوسطة، وبوسط حسابي (2.29)، وجاءت مقومات النجاح ككل بدرجة مرتفعة ووسط حسابي (2.812).

وتعكس هذه النتائج مرتكزات نجاح توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني؛ حيث خلص المختصون الأردنيون إلى ضرورة وجود إطار قانوني تشريعي يتوازى مع سرعة الابتكار في ظل تعدد تطبيقات التتبع والتحليل الذكي لتنظيم عملية التوظيف، وكذلك ضرورة اللجوء إلى شيفرات موثوقة بغية تحصين أنظمة المؤسسات الأردنية وتأمين معلوماتها من أجل نعت العملية بالناجحة، بينما لم يعر المختصون الأهمية ذاتها للركيزة المتعلقة باستحداث منصات اتصالية تعزز تفاعل الأجهزة الأمنية والمواطنين، مما يدل على وعي المواطنين الأردنيين وتعايشهم المجتمعي نتيجة للوجود الفعلي للمنصات الاتصالية المعنية بتقديم البرامج التوعوية.

واتفقت هذه النتائج مع نتائج دراسة (قاسم، 2024) التي أسفرت عن توجه الأنظمة السعودية والإماراتية لاستحداث تشريعات مستقلة لتطورات علم الذكاء الاصطناعي بفرعيه الصناعي والقانوني، وكذلك تطوير أداء الأجهزة الأمنية، كما واتفقت مع نتائج دراسة (الهنائي، 2024) التي اقترحت تكاتف الرؤى لإقرار مشروع قانوني شامل للذكاء الاصطناعي، وكذلك عقد الدورات التدريبية في القطاعات الأمنية.

نتائج التساؤل الخامس: ما التحديات المصاحبة لتوظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين.

الجدول رقم (7) الوسط الحسابي، الانحراف المعياري والنسب والتكرارات للتحديات المصاحبة لتوظيف تطبيقات الذكاء الاصطناعي

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
2	ضعف البنية القانونية والتشريعية	2.98	0.141	99.3%	مرتفع	1
6	غياب الدعم المادي المناسب لتغطية تكاليف التطبيقات والبرمجيات	2.97	0.171	99.0%	مرتفع	2
5	غياب تدريب وتأهيل الموارد البشرية الأمنية للتعامل مع تطبيقات الذكاء الاصطناعي	2.81	0.394	93.7%	مرتفع	3
1	تضارب معلومات المصادر وبياناتها الإحصائية	2.45	0.5	81.7%	مرتفع	4
7	خلل في البرمجة أو أعطال أنظمة تشغيل التطبيقات	2.3	0.461	76.7%	متوسط	5

رقم الفقرة	نص الفقرة	الوسط الحسابي	الانحراف المعياري	مؤشر الوسط الحسابي	المستوى	الترتيب
3	المساس بحربات الأفراد الخاصة	2.2	0.402	73.3%	متوسط	6
4	وقوع تطبيقات الذكاء الاصطناعي فريسة للتحيز جراء نقص البيانات؛ مما يؤدي إلى وجود عناصر مضطربة تحد من قيمة المعلومات	1.90	0.302	63.3%	متوسط	7
	الوسط الحسابي للفقرات جميعها	**2.516**	**0.339**	**83.9%**	مرتفع	

تشير بيانات الجدول رقم (7) إلى المتوسطات الحسابية والانحرافات المعيارية ومؤشرات الوسط الحسابي للتحديات المصاحبة لتوظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين؛ حيث جاء تحدي ضعف البيئة القانونية والتشريعية في المرتبة الأولى، وبدرجة مرتفعة ووسط حسابي بلغ (2.98)، وتلاه تحدي غياب الدعم المادي المناسب لتغطية تكاليف التطبيقات والبرمجيات في المرتبة الثانية، وبدرجة مرتفعة ووسط حسابي بلغ (2.97)، أما المرتبة الثالثة؛ فكانت من نصيب التحدي المتعلق بغياب تدريب وتأهيل الموارد البشرية الأمنية للتعامل مع تطبيقات الذكاء الاصطناعي، كما وجاء تحدي المرتبة الثالثة بدرجة مرتفعة ووسط حسابي (2.81)، ثم تلاه تحدي تضارب معلومات المصادر وبياناتها الإحصائية في المرتبة الرابعة، وكذلك بدرجة مرتفعة ووسط حسابي (2.45)، بينما جاء تحدي وقوع تطبيقات الذكاء الاصطناعي فريسة للتحيز في المرتبة الأخيرة، كما وسجل أقل مؤشر للوسط الحسابي (1.90)، وجاءت التحديات ككل بدرجة مرتفعة، ووسط حسابي (2.516).

ويرى المختصون الأردنيون أن البيئة التشريعية المنظمة لتوظيف تطبيقات الذكاء الاصطناعي هشة، وعاجزة عن التصدي لبعض التجاوزات نظرا لعدم كفاية عناصرها، كما أن سبل المحاسبة القانونية لتلك التوظيفات المشبوهة أو المدبلجة تكاد تكون معدومة نظرا لحداثة توظيفها في العمل الأمني ومكافحة الجريمة، الأمر الذي يستدعي فرض إطار قانوني تشريعي يكفل عدم تجاوز الشرعية، كما ويرجع ظهور التحديات المادية إلى حاجة تطبيقات الذكاء الاصطناعي لإمكانات مادية كبيرة تغطي تكاليف تحديث الأجهزة الحالية، واقتناء أجهزة أكثر تطورا، وكذلك التعامل مع شبكات الاتصال الحديثة، والتي تتطلب اتصالا دائما وسريعا بشبكة الانترنت، لذا اتفقت هذه النتائج مع مع نتائج دراسة (الهنائي، 2024) التي عكست أبرز تحديات تطبيق الذكاء الاصطناعي في المجال الأمني، والمتمثلة بارتفاع تكلفة الأجهزة والتقنيات.

واتفقت هذه النتائج مع نتائج دراسة (أبو علان، 2022) التي كشفت عن التحديات المرتبطة بسلسلة التطورات التكنولوجية في وزارتي الاتصالات وتكنولوجيا المعلومات في مدينتي رام الله والبيرة في فلسطين، وهي: تحديات البنية التحتية، والموازنات المالية، وكذلك الكادر البشري.

نتائج التساؤل السادس: هل توجد فروقات ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في اتجاهات المختصين الأردنيين نحو توظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتعزيز الأمن السيبراني تعزى للمتغيرات الديموغرافية لعينة الدراسة: (النوع الاجتماعي، والفئة العمرية، والدرجة العلمية).

الجدول رقم (8) نتائج تحليل المتغيرات الديمغرافية

المتغير	نوع التحليل	الفئات	الوسط الحسابي	قيمة T	قيمة F	مستوى الدلالة الاحصائية (Sig.)
النوع الاجتماعي	T	ذكور	2.4800	-2.782	-	0.006
		إناث	2.5253			
الفئة العمرية	ANOVA	35-25	2.5579	-	4.097	0.02
		45-36	2.4882			
		46 فأكثر	2.4955			
الدرجة العلمية	ANOVA	بكالوريوس	2.4911	-	4.384	0.039
		دراسات عليا	**2.5315**			

تشير بيانات الجدول (9) إلى الآتي:

- بلغت قيمة مستوى الدلالة الاحصائية بالنسبة للنوع الاجتماعي (0.006) وهي أقل من (0.05)، وهذا يدل على وجود فروقات ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لتوظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني تعزى لمتغير

النوع الاجتماعي؛ حيث كان مؤشر الموافقة للإناث أعلى من مؤشر الموافقة للذكور وفقا لقيم الوسط الحسابي المبينة في الجدول أعلاه.

- توجد فروقات ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لتوظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين تعزى لمتغير الفئة العمرية، حيث بلغت قيمة مستوى الدلالة الاحصائية (0.02) وهي أقل من (0.05)، لذلك يتم رفض الفرضية العدمية، حيث كان مؤشر الموافقة للفئة العمرية (25-35) أعلى من مؤشر الموافقة لباقي الفئات العمرية وفقا لقيم الوسط الحسابي المبينة في الجدول أعلاه.

- توجد فروقات ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) لتوظيف تطبيقات الذكاء الاصطناعي في مكافحة الجرائم الالكترونية وتعزيز الأمن السيبراني من وجهة نظر المختصين الأردنيين تعزى لمتغير الدرجة العلمية، حيث بلغت قيمة مستوى الدلالة الإحصائية (0.039) وهي أقل من (0.05)، لذلك يتم رفض الفرضية العدمية، حيث كان مؤشر الموافقة للمستجيبين من حملة شهادات الدراسات العليا أعلى من مؤشر الموافقة للمستجيبين من حملة شهادات البكالوريوس وفقا لقيم الوسط الحسابي المبينة في الجدول أعلاه.

التوصيات

تعرض الدراسة في ضوء النتائج التي تم التوصل إليها بعض التوصيات على النحو الآتي:

1. ضرورة توجه الجهات الأردنية المختصة لاستحداث إطار قانوني تشريعي يستهدف تنظيم استخدام هذه التطبيقات من قبل الأفراد والمؤسسات، ويضبط أداءهم في نقل الأحداث نتيجة لضعف البيئة القانونية والتشريعية.

2. ضرورة رفد المركز الوطني للأمن السيبراني بالدعم المادي والفني والتقني لتمكين المؤسسات الأردنية والمجتمع المدني من الاستعانة بخبراء المركز لتأمين المعلومات من خلال شيفرات موثوقة، وتحصين قنوات الاتصال من الاختراقات غير المشروعة.

المصادر والمراجع

أبو علان، ك. (2022). *معوقات تطبيق الذكاء الاصطناعي في الحد من ممارسة الجريمة الإلكترونية من وجهة نظر العاملين في وزارة الاتصالات وتكنولوجيا المعلومات في محافظة رام الله والبيرة. رسالة ماجستير منشورة*، جامعة القدس، فلسطين.

الحديدي، م.، واللبان، ش. (2009). فنون الاتصال والاعلام المتخصص. (ط1). القاهرة: الدار المصرية اللبنانية.

الحمايدة، خ.، الضلاعين، ع.، اللحام، م.، الضلاعين، ن.، الشمايلة، م.، وكافي، م. (2017). *الإعلام السياسي ونظريات التأثير الإعلامية*. عمان: دار الإعصار العلمي للنشر والتوزيع.

دائرة الموازنة العامة. (2023). المركز الوطني للأمن السيبراني. الفصل 3210.

الداغر، م. (2021). اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر. *المجلة العربية لبحوث الإعلام والاتصال*، 33. https://doi.org/10.21608/JKOM.2021.195915

الدسوقي، م. (2022). جرائم تقنيات الذكاء الاصطناعي والشخصية القانونية الإلكترونية المستقلة. *مجلة البحوث القانونية والاقتصادية*، 81. https://doi.org/10.21608/mjle.2022.282445

زايد، ح. (2020). نظرية انتشار المبتكرات في مواقع التواصل الاجتماعي في أزمة كورونا. كلية الإعلام، جامعة ذي قار. https://doi.org/10.13140/RG.2.2.30144.89601

سالم، د.، وأبو الجدايل، م. (2023). فاعلية استخدام الهيئة الوطنية للأمن السيبراني بالمملكة العربية السعودية لتقنيات الذكاء الاصطناعي كتوجه مستقبلي: دراسة استشرافية. *بحوث عربية في مجالات التربية النوعية*، 30(1).

سليم، آ. (2024). اتجاهات الإعلاميين الأردنيين نحو الفرص والتحديات التي تفرضها تقنيات الذكاء الاصطناعي في إنتاج المضامين الإعلامية الرقمية. *رسالة ماجستير منشورة*، كلية الإعلام، جامعة البترا، المملكة الأردنية الهاشمية.

شعيب، أ.، وريان، ج. (2023). القضايا المستحدثة للمرأة الجزائرية في البرامج التلفزيونية. *رسالة ماجستير منشورة*، كلية العلوم الإنسانية والاجتماعية، جامعة محمد خيضر بسكرة. http://archives.univ-biskra.dz/handle/123456789/28274

صبرة، إ. (2020). حقوق المجني عليه في الجرائم الإلكترونية في التشريع الفلسطيني: دراسة مقارنة مع القانون والشريعة الإسلامية. *رسالة ماجستير غير منشورة*، الجامعة الإسلامية، غزة. https://search.mandumah.com/Record/1353747

العلاق، ب. (2010). *نظريات الاتصال*. عمان: دار اليازوري العلمية للنشر والتوزيع.

عميره، ع. (2019). حجم الإنفاق العالمي لأنظمة الذكاء الاصطناعي. *جريدة المال*، 2019/11/26. https://almalnews.com/97-

قاسم، م. (2024). "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية. *المجلة العصرية للدراسات القانونية، رام الله، فلسطين*، 2(2).

https://doi.org/10.70411/MJLS.2.2.202495

محروس، أ. (2024). المسؤولية الإدارية تجاه أخطاء تطبيقات الذكاء الاصطناعي. *المجلة القانونية*، 22(1)، 90-114. https://doi.org/10.70411/MJLS.2.2.202495

المري، ر. (2023). أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية"، *مجلة الشريعة والقانون بدمنهور، 40(1)، 1298-1373*. http://search.mandumah.com/Record/1352757

الهنائي، ع. (2024). تطبيقات الذكاء الاصطناعي في المجال الأمني: دراسة مطبقة على دول مجل التعاون لدول الخليج العربية. *مجلة الدراسات القانونية والاقتصادية*، 10(4). https://jdl.journals.ekb.eg/article_395429.html

النيادي، ح. (2022). الدليل السيبراني المستمد من الذكاء الاصطناعي. *المجلة القانونية*، 14(4). https://search.emarefa.net/detail/BIM-1446083.

References

Allport, G. W. (1954). *The Nature of Prejudice*. Cambridge.

AL-Marghilani, AA. (2022). Target detection algorithm in crime recognition using artificial intelligence. *Comput Mater Contin*, 71(1)

Bhavani, T. (2020). *The role of AI and Cyber Security for social media*. USA: IEEE International Parallel and Distributed Processing Symposium Workshops.

Csonka, P. (2020). Internet Crime, the Draft Council of Europe Convention on Cyber- Crime: A Response to the Challenge of Crime in the Age of the internet. *Computer Law & Security Report*, 28(15).

Geise, A. (2018). The current and future impact of artificial intelligence on business. *International Journal of Scientific and Technology Research*, 7(5).

Nunnally, J. (1978). *Psychometric Theory*. (2nd ed.). New York: McGraw-Hill.

Ramirez, M., Ariza, L., & Miranda, M. (2022). The disclosure of information security in listed companies in Latin America-proposal for a cyber security disclosure index. *Journal of sustainability*, 14(3).

Reddt, M., & Reddy, G. (2020). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. *Peridot Technologies*, 26 (9).

Shetty, S., Choi, K., & Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. *International Journal of Cybersecurity Intelligence & Cybercrime*, 7(2).

Twaig, R. (2019). Whose Robot Is It Anyway? Liability for Artificial-Intelligence Based Robots. *University of Illinois Law Review*, 2020.

Umair, M., Letchmunan, S., Fadratul, H., & Tieng, W. (2024). Leveraging transfer learning with deep learning for crime prediction. *PLoS ONE Journal*, 19(4).

Villasenor, O. (2019). *Artificial intelligence, geopolitics, and information integrity: The Global Race for Technological Superiority: Discover the Security Implications.* Milano: ISPI and Brookings.

Zhang, Z., Hamadi, H., Damiani, E., Chan, Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security. *Cornell University Library*.