المجلة الأردنية في إدارة الأعمال، المجلّد **21**، العدد **1**، **2025**
DOI: https://doi.org/10.35516/jjba.v21i1.1864

The Role of Artificial Intelligence Systems in Combating Cybercrime: A Field Study in Jordan

Sabah Adel Aref Al-Rawashdeh [1]

ABSTRACT

This study aimed to identify the role of artificial intelligence in combating electronic crimes in the Jordanian Public Security Directorate/Electronic Crimes Unit. The study population consisted of administration managers and employees of the Cybercrime unit in the Jordanian Public Security Directorate. The interview method and the intentional sample were used for the purposes of representing the study population. The study sample amounted to (132) members. The study relied on the descriptive analytical approach to achieve its objectives, a questionnaire was used to collect data, and the study relied on the statistical program (SPSS) for data analysis. The results of the analysis of the respondents' answers showed that there is a role for artificial intelligence in combating electronic crimes in the Jordanian Public Security Directorate/Electronic Crimes Unit. The study recommended the need to strengthen and benefit from artificial-intelligence systems and programs and employ them in the work of the Electronic Crimes Unit, in addition to working on modernizing and updating them.

Keywords: Artificial intelligence, Cybercrime, Public Security Directorate/Cybercrime Unit, Jordan.

1 Assistant Professor, Royal Police Academy, Jerash, Jordan.

Received on 15/10/2023 and Accepted for Publication on 31/12/2023.

دور أنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية: دراسة ميدانية في الأردن

صباح عادل عارف الرواشدة[1]

ملخص

هدفت هذه الدراسة إلى التعرف إلى دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية في مديرية الأمن العام الأردنية/وحدة الجرائم الإلكترونية. تمثل مجتمع الدراسة في مديري الإدارة وموظفي وحدة الجرائم الإلكترونية في مديرية الأمن العام الأردنية. وتم استخدام أسلوب المقابلة والعينة القصدية لغايات تمثيل مجتمع الدراسة، وبلغت عينة الدراسة (132) مفردة، واعتمدت الدراسة المنهج الوصفي التحليلي لتحقيق أهدافها. تم استخدام الاستبانة لجمع البيانات، واعتمدت الدراسة على البرنامج الإحصائي(SPSS) لتحليل البيانات. وأظهرت نتائج تحليل إجابات أفراد العينة أن هناك دوراً للذكاء الاصطناعي في مكافحة الجرائم الإلكترونية في مديرية الأمن العام الأردنية/وحدة الجرائم الإلكترونية. وأوصت الدراسة بضرورة تعزيز أنظمة وبرامج الذكاء الاصطناعي والاستفادة منها وتوظيفها في أعمال وحدة الجرائم الإلكترونية، إضافة إلى تحديثها باستمرار.

الكلمات الدالة: الذكاء الاصطناعي، الجرائم الإلكترونية، مديرية الأمن العام/ وحدة الجرائم الإلكترونية، الأردن.

المقدمة

تعد مكافحة الجرائم الإلكترونية أحد التحديات الرئيسية التي تواجه المجتمع في العصر الحديث. فمع التطور التكنولوجي المتسارع وانتشار استخدام الإنترنت والتقنيات الرقمية، أصبحت الجرائم الإلكترونية تشكل تهديدًا خطيرًا للأفراد والمؤسسات على مستوى العالم. إن الهجمات الإلكترونية المتطورة والاختراقات السرية تتطلب استخدام تقنيات متقدمة لمكافحتها والحد من آثارها السلبية. وفي هذا السياق، تأتي أنظمة الذكاء الاصطناعي كأداة قوية وفعالة لمكافحة الجرائم الإلكترونية. وتعتمد هذه الأنظمة على القدرة على تحليل كميات ضخمة من البيانات واستخلاص أنماط ومعلومات مهمة، مما يمكنها من اكتشاف السلوكيات الاحتيالية وتحديد الأنشطة غير القانونية على الإنترنت. بالإضافة إلى ذلك، تتميز أنظمة الذكاء الاصطناعي بالقدرة على التعلم الذاتي والتكيف مع التهديدات الجديدة، مما يساهم في تعزيز فاعلية استراتيجيات مكافحة الجرائم الإلكترونية. وتهدف هذه الدراسة إلى سد الفجوة الموجودة في البحوث السابقة المتعلقة بتطبيق أنظمة الذكاء الاصطناعي في مجال مكافحة الجرائم الإلكترونية.

وفي عصرنا الحالي، تعتبر الجرائم الإلكترونية من أكبر التحديات التي تواجه الاقتصاد العالمي بأكمله، حيث تم استخدام أنظمة الذكاء الاصطناعي الحديثة لحماية أمن المعلومات وعدم اختراقها، وذلك بتكلفة باهظة الثمن. وفي وقتنا الحاضر، تسعى جميع الحكومات إلى الاهتمام بمنظومة الذكاء الاصطناعي لما لها من أهمية بالغة في سير أعمال المنظمة على أكمل وجه وبالتالي تحقيق أهدافها المنشودة، التي من خلالها يتم رفع مستوى أداء المنظمة. وفي هذا العصر المتصف بالتغير السريع والتطورات الهائلة، يجب على المنظمات التي تبحث عن التقدم والبقاء أن تسعى جاهدة لتوظيف أنظمة الذكاء الاصطناعي ذات الكفاءة العالية لضمان سير أعمالها على أكمل وجه والتقليل من الجرائم الإلكترونية قدر المستطاع. ويجب على المنظمات التي تبحث عن التميز والتقدم في ظل العالم المتغير والمنافسة الشديدة أن تتبنى مفهوم الذكاء الاصطناعي الذي بدوره يميزها عن باقي

1 أستاذ مساعد، أكاديمية الشرطة الملكية، جرش، الأردن.

تاريخ استلام البحث 2023/10/15 وتاريخ قبوله 2023/12/31.

المنظمات، والذي يساعدها في زيادة كفاءة وسرعة مكافحة الجريمة، وبالتالي نمو وتقدم المنظمة. وهناك العديد من التحديات، مثل تحديات العولمة والتغير السريع في بيئات الأعمال، مما يوجب على وحدة مكافحة الجريمة الإلكترونية في مديرية الأمن العام الأردنية التوجه إلى توظيف أنظمة الذكاء الاصطناعي في أعمالها، وذلك لتحقيق أهدافها المنشودة، ومن أبرزها التقليل من الجرائم الإلكترونية وصولاً إلى مجتمع أمن خالٍ من الجريمة.

على الرغم من وجود العديد من الدراسات التي تبحث في استخدام التكنولوجيا في مكافحة الجرائم الإلكترونية، فما زالت هناك فجوات وتحديات معينة لم يتم التطرق إليها بشكل كافٍ. إحدى الفجوات الرئيسية تتعلق بقلة الدراسات التي تتناول تطبيق أنظمة الذكاء الاصطناعي في مديرية الأمن العام الأردنية/وحدة الجرائم الإلكترونية. وهذا يعني أنه لا تتوفر لدينا معرفة كافية حول تجربة الوحدة ونتائجها في استخدام تلك الأنظمة. لذلك، تأتي هذه الدراسة لتسد هذه الفجوة من خلال تقديم تقييم شامل لاستخدام أنظمة الذكاء الاصطناعي في وحدة الجرائم الإلكترونية وتحليل نتائجها. بالإضافة إلى ذلك، تسعى الدراسة لملء الفجوة في فهمنا لفاعلية أنظمة الذكاء الاصطناعي في الكشف عن الجرائم الإلكترونية بشكل عام. فقد تكون الدراسات السابقة اعتمدت بشكل أساسي على الطرق التقليدية لمكافحة الجرائم الإلكترونية، ولم تركز بشكل كبير على استخدام التقنيات الحديثة مثل الذكاء الاصطناعي. لذا، يهدف هذا البحث إلى تعزيز فهمنا للقدرات والتحديات التي تواجه استخدام أنظمة الذكاء الاصطناعي في هذا السياق.

يشهد العالم اليوم تزايدًا في عدد الجرائم الإلكترونية وتعقيدها، مما يتطلب اعتماد استراتيجيات متقدمة لمكافحتها. إن تقنيات الذكاء الاصطناعي، مثل التحليل التنبؤي والتعلم الآلي، توفر إمكانية فريدة للتعامل مع هذه التحديات، وذلك من خلال تحسين عمليات التحقيق والكشف عن الجرائم الإلكترونية وتحليل البيانات الضخمة. يضاف إلى ذلك أن الجهات الأمنية قد تعاني من قيود الموارد والضغوط الزمنية، مما يعوق قدرتها على مواجهة الجرائم الإلكترونية بشكل فعال. وباستخدام أنظمة الذكاء الاصطناعي، يمكن تحقيق توفير في الجهد والوقت المستخدمين في عمليات التحقيق، مما يعزز الكفاءة والفاعلية العامة للوحدة.

علاوة على ذلك، يمكن أن تساهم هذه الدراسة في تعزيز التفاهم والتعاون بين الباحثين والممارسين في مجال مكافحة الجرائم الإلكترونية. فعن طريق تحليل التحديات والمشاكل الموجودة في تطبيق أنظمة الذكاء الاصطناعي، يمكن تحديد نقاط القوة والضعف، وبناء نقاط اتصال مشتركة لتعزيز التعاون المشترك بين الجهات الأمنية ذات العلاقة بمكافحة الجرائم الإلكترونية على الصعيدين المحلي والدولي.

وحدة الجرائم الإلكترونية: النشأة والأهمية

أسست وحدة الجرائم الإلكترونية في الأردن تحت مظلة مديرية الأمن العام في سنة 2015، وذلك تلبيةً للتحديات التي أحدثها التطور السريع في تكنولوجيا المعلومات والاتصالات، والتزايد المستمر في استخدام الإنترنت والتكنولوجيا الرقمية في الحياة اليومية والأعمال التجارية. وتهدف هذه الوحدة إلى مكافحة الجرائم الإلكترونية وحماية المجتمع الأردني من التهديدات الإلكترونية.

تلعب وحدة الجرائم الإلكترونية دورًا حيويًا في تعزيز الأمن الإلكتروني في الأردن. حيث تعمل الوحدة على تحليل وتقييم التهديدات الإلكترونية والجرائم المرتبطة بالتكنولوجيا، وتنفيذ الإجراءات الوقائية والتحققية اللازمة للتصدي لهذه الجرائم ومتابعة المتهمين، وتعمل أيضًا على تطوير السياسات والإجراءات المناسبة لتعزيز الوعي الأمني وتعليم الجمهور والمؤسسات المختلفة حول أهمية الأمان الإلكتروني وطرق الوقاية من الجرائم الإلكترونية. تتبع وحدة الجرائم الإلكترونية في الأردن أساليب شاملة ومتطورة في مكافحة الجرائم الإلكترونية. حيث تستخدم تقنيات متقدمة في جمع الأدلة الرقمية وتحليلها، وتتعاون مع الجهات المختلفة في الأردن والدول الأخرى لتبادل المعلومات وتعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية.

يعاني الأردن، مثل العديد من الدول الأخرى، من زيادة حالات الجرائم الإلكترونية وتهديدات الأمن الإلكتروني. وتعزز وحدة الجرائم الإلكترونية في الأردن قدرة الدولة على التصدي لهذه التهديدات وتقديم الحماية للمجتمع والاقتصاد الوطني، كما تسهم في خلق بيئة آمنة وموثوقة للاستخدام الآمن للتكنولوجيا وتعزيز التجارة الإلكترونية والاستثمار في قطاعات التكنولوجيا. وتعتبر وحدة الجرائم الإلكترونية في الأردن مرجعًا رئيسيًا

لمكافحة الجرائم التقنية، حيث تتولى التحقيق في الجرائم الإلكترونية وجمع الأدلة الرقمية وتحليلها. كما تقدم الدعم الفني والاستشارات القانونية للمحققين والمدعين العامين والجهات المعنية في مجال تقنيات الجرائم الإلكترونية.

يتولى مديرو وحدة الجرائم الإلكترونية في الأردن تنسيق الجهود المشتركة للتحقيق وملاحقة المتورطين في الجرائم الإلكترونية، بما في ذلك التزوير الإلكتروني والاحتيال والتهديدات الإلكترونية والاختراقات السيبرانية. وتقوم الوحدة أيضًا بتقديم النصح والإرشاد للجمهور والمؤسسات لتعزيز الوعي الأمني وتعزيز ممارسات الأمان الرقمي. وتستند أهمية وحدة الجرائم الإلكترونية في الأردن إلى عدة جوانب. أولاً، فإن الجرائم الإلكترونية تشكل تهديدًا حقيقيًا للأفراد والمؤسسات والحكومات، وتؤثر على الاستقرار الاقتصادي والأمن الوطني. وبالتالي، يعمل الجهاز على حماية المواطنين والمصالح الوطنية من هذه التهديدات. ثانيًا، تعتبر وحدة الجرائم الإلكترونية في الأردن جزءًا من مكافحة الجرائم العابرة للحدود، حيث يمكن للجرائم الإلكترونية أن تكون مرتبطة بجرائم تنظيم العصابات المنظمة والإرهاب وغسل الأموال. وبالتالي، فإن تعاون وحدة الجرائم الإلكترونية وتنسيقها مع الجهات المعنية المحلية والدولية يعززان الجهود الرامية لمكافحة هذه الجرائم وتحقيق العدالة.

تُعَدُّ المراجع العلمية المتخصصة مصدرًا هامًا لفهم دور وحدة الجرائم الإلكترونية في الأردن وأهميتها في مكافحة الجرائم الإلكترونية. وتشير دراسة أجرتها ندى سليمان (2019) إلى أن وحدة الجرائم الإلكترونية في الأردن قد قامت بتحقيق نجاحات كبيرة في مكافحة الجرائم الإلكترونية وتعزيز الأمن الرقمي في المملكة. وقد تم تطوير الإطار القانوني والتشريعات المتعلقة بالجرائم الإلكترونية في الأردن لتكون أكثر فعالية وملاءمة للتحديات الحديثة في هذا المجال. وبحسب دراسة أخرى قام بها محمد الخصاونة (2020)، فإن وحدة الجرائم الإلكترونية في الأردن تعمل بنجاح على تعزيز التوعية الأمنية بين المواطنين والمؤسسات، وذلك من خلال تقديم المشورة والإرشاد فيما يتعلق بالتدابير الأمنية الواجب اتخاذها لحماية المعلومات الشخصية والبيانات الحساسة وتجنب الاحتيال الإلكتروني. بالإضافة إلى ذلك، يشير محمد العبادي (2018) إلى أن وحدة الجرائم الإلكترونية في الأردن تقوم بدور حاسم في تعزيز الثقة الرقمية وتوفير بيئة آمنة للتجارة الإلكترونية والأنشطة المصرفية عبر الإنترنت. ومن خلال تطوير القدرات التقنية وتبني أحدث التقنيات الأمنية، تعمل الوحدة على توجيه الكوادر الأمنية والمحققين وتدريبهم للتعامل مع التهديدات الإلكترونية وجمع الأدلة الرقمية اللازمة لملاحقة المتسببين في الجرائم الإلكترونية ومحاسبتهم.

وتتعاون وحدة الجرائم الإلكترونية في الأردن مع عدة جهات محلية ودولية، مثل الأجهزة الأمنية والمصرفية والهيئات القضائية وشركات تكنولوجيا المعلومات ومقدمي خدمات الإنترنت. هذا التعاون يساهم في تعزيز التبادل الدولي للمعلومات والخبرات وتطوير استراتيجيات مشتركة لمكافحة الجرائم الإلكترونية على المستويين الإقليمي والدولي. ومن المهم أيضًا أن نشير إلى الدور الحكومي الريادي في دعم وحدة الجرائم الإلكترونية في الأردن. حيث تتبنى الحكومة الأردنية سياسات واستراتيجيات قوية لتعزيز الأمن الرقمي ومكافحة الجرائم الإلكترونية، وتوفير الموارد اللازمة والتدريب المستمر للكوادر الأمنية والتقنية المعنية بهذا المجال. باختصار، تعد وحدة الجرائم الإلكترونية في الأردن جهة فاعلة وحيوية في مجال مكافحة الجرائم الإلكترونية وتعزيز الأمن الرقمي.

الذكاء الاصطناعي وتطبيقاته في مكافحة الجرائم الإلكترونية

الذكاء الاصطناعي (Artificial Intelligence) هو مجال من مجالات علوم الحاسوب يهتم بتطوير أنظمة وتقنيات تمكن الأجهزة الذكية من تنفيذ مهام تتطلب تفكيرًا واتخاذ قرارات مشابهة لتلك التي يقوم بها البشر. ويستخدم الذكاء الاصطناعي تقنيات وأساليب مثل التعلم الآلي (Machine Learning)، والتعلم العميق (Deep Learning)، ومعالجة اللغات الطبيعية (Natural language Processing)، والتعلم التعزيزي (Reinforcement Learning) لتمكين الأنظمة الذكية من التعلم والتكيف والتفاعل بشكل مستقل.

في مجال مكافحة الجرائم الإلكترونية، يلعب الذكاء الاصطناعي دورًا حاسمًا في التصدي للتهديدات الأمنية ومعالجة الجرائم الإلكترونية.

وفيما يلي بعض التطبيقات والمكونات الرئيسية للذكاء الاصطناعي في هذا السياق.

1- تحليل البيانات: يمكن للذكاء الاصطناعي تحليل كميات

ضخمة من البيانات المتعلقة بالجرائم الإلكترونية، مثل السجلات، والبيانات المالية، والتقارير الأمنية. وتستخدم نماذج التعلم الآلي للكشف عن أنماط وتلميحات مشتبه فيها واستخلاص معلومات قيمة تساعد في التحقيق والتوجيه الأمني (Haddawy & Keizer, 2018).

2- الكشف عن السلوك غير المشروع: يستخدم الذكاء الاصطناعي تقنيات تعلم الآلة لبناء نماذج تحليلية تستطيع تحديد السلوكيات غير المشروعة أو الغريبة في الأنشطة الرقمية، مثل اختراقات القرصنة والتلاعب بالبيانات (Ahuja & Puri, 2021).

3- التصنيف والتحقق من الهوية: يمكن للذكاء الاصطناعي تحليل السلوك الرقمي للمستخدمين والأجهزة لتحديد الأنشطة غير العادية والتحقق من الهوية. ويتم استخدام تقنيات تعلم الآلة والتعلم العميق لتصنيف السلوكيات والتحقق من صحة الهوية للحماية من الاحتيال والتهديدات والهجمات المتقدمة (Karthik & Satyadev, 2020).

4- الاكتشاف المبكر للتهديدات: يستخدم الذكاء الاصطناعي تقنيات تحليل البيانات والتعلم الآلي للكشف المبكر عن التهديدات الجديدة والمتقدمة. ويمكن للنماذج الذكية تحليل الأنماط والسمات المشتركة للهجمات السابقة واستخلاص توقعات وتنبؤات للتهديدات المستقبلية (Sapra & Sehgal, 2021).

وبجانب تلك التطبيقات، يمكن أن يسهم الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية من خلال:

1- تحليل الصور والفيديو: يستخدم الذكاء الاصطناعي تقنيات التعلم العميق لتحليل الصور والفيديوهات المرتبطة بالجرائم الإلكترونية، مثل التلاعب بالصور والفيديوهات وتحديد الوجوه والأشياء ذات الصلة. ويمكن لهذا التحليل أن يساعد في تحديد الأدلة وتحديد المشتبه بهم وتوفير أدلة قوية في التحقيقات الجنائية (Dutta & Ghosal, 2020).

2- التنبؤ والتحليل الاستراتيجي: يستخدم الذكاء الاصطناعي تقنيات التعلم الآلي لتحليل البيانات المتعلقة بالجرائم الإلكترونية والسلوكيات الجنائية السابقة، مما يمكنه من توفير توقعات وتنبؤات استراتيجية للتهديدات المحتملة ونمط الجرائم المستقبلية. ويمكن استخدام هذه التحليلات في اتخاذ قرارات استراتيجية لتحسين الأمن السيبراني وتعزيز الجهود الوقائية (Saha & Roy, 2021).

3- الروبوتات والأتمتة: يمكن استخدام الذكاء الاصطناعي في تطوير الروبوتات والأتمتة للمساهمة في مكافحة الجرائم الإلكترونية. ويمكن للروبوتات الذكية تنفيذ المهام المتعلقة بالأمن السيبراني، مثل مراقبة الشبكات والكشف عن الاختراقات وتنفيذ إجراءات الحماية المطلوبة بشكل أوتوماتيكي وفعال (Pandey & Gupta, 2020).

هذه المكونات والتطبيقات تمثل جزءًا من الجهود المستمرة لاستخدام الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية يتطور باستمرار، وتظهر تقنيات جديدة ومتقدمة لتحسين الأداء والكفاءة في هذا المجال. على سبيل المثال:

1. الشبكات العصبية المتصاعدة (Spiking Neural Networks): تعد هذه التقنية نموذجًا جديدًا للشبكات العصبية المستوحاة من التشغيل الحي للدماغ. وتتميز بقدرتها على التعامل مع الإشارات الزمنية والتأكيد على الأحداث والتفاعل الديناميكي، مما يمكنها من اكتشاف التهديدات الجديدة وغير المعروفة بشكل أفضل وبدقة أعلى (Wu et al., 2020).
2. الذكاء الاصطناعي الشامل :(AI+) يعتمد هذا المفهوم على دمج تقنيات الذكاء الاصطناعي مع تقنيات أخرى مثل البيانات الضخمة والحوسبة السحابية وإنترنت الأشياء. ويعمل الذكاء الاصطناعي الشامل على تحليل البيانات الكبيرة وتحقيق تكامل المعلومات من مصادر مختلفة لتوفير رؤى أكثر شمولية في مجال مكافحة الجرائم الإلكترونية (Li et al., 2021).
3. تعلم الآلة التعاوني (Cooperative Machine Learning): يتميز هذا المفهوم بقدرته على تعزيز التعلم والأداء من خلال تعاون الأنظمة الذكية المستقلة بعضها مع البعض الآخر. ويمكن لهذا النوع من التعلم تحسين قدرة الأنظمة الذكية على الكشف عن الجرائم الإلكترونية ومعالجتها وتحديث النماذج التحليلية باستمرار (Zhong et al., 2022).

وتظهر هذه الابتكارات الجديدة أن الذكاء الاصطناعي يلعب دورًا مهمًا في مكافحة الجرائم الإلكترونية، حيث يساهم في تحسين قدرة المنظمات والجهات الأمنية على التعامل مع

التحديات السيبرانية المتزايدة. ومن خلال استخدام مجموعة متنوعة من التقنيات والتطبيقات، يتم تعزيز القدرة على اكتشاف الجرائم والتحقيق فيها ومكافحة التهديدات السيبرانية. ومن الجوانب الإيجابية الأخرى لاستخدام الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، يمكن أن نذكر:

- الزمن الفعال والاستجابة السريعة: يتيح الذكاء الاصطناعي قدرة سريعة على التعامل مع حجم كبير من البيانات وتحليلها، مما يتيح رصد الأنشطة المشبوهة والتصدي للتهديدات بشكل فعال في الوقت الحقيقي. وهذا يمنح الجهات الأمنية قدرة أفضل على اتخاذ قرارات سريعة وتنفيذ إجراءات مناسبة لمكافحة الجرائم الإلكترونية (Chauhan et al., 2021).
- تحسين دقة التحقيقات: باستخدام تقنيات التعلم الآلي وتحليل البيانات، يمكن للذكاء الاصطناعي تحسين دقة التحقيقات الجنائية وتحليل الأدلة، بحيث يتمكن من استخلاص أنماط ومعرفة متعمقة من البيانات، مما يسهم في تحديد المشتبه بهم وتوفير أدلة قوية لدعم عمليات التحقيق (Sharma et al., 2020).
- التحليل التنبؤي والتوقعات: يمكن للذكاء الاصطناعي تحليل البيانات التاريخية والتنبؤ بالسلوكيات المستقبلية والتهديدات المحتملة. ويساعد ذلك في اتخاذ إجراءات وتنفيذ استراتيجيات لمكافحة الجرائم الإلكترونية.
- ترويج التوعية والتدريب: يعمل الذكاء الاصطناعي على توفير أدوات وتقنيات لتدريب وتوعية الجهات المعنية بمكافحة الجرائم الإلكترونية؛ إذ يمكن تطوير برامج تعليمية وعقد ورش عمل تستخدم تقنيات الذكاء الاصطناعي لتدريب المحققين والمحللين على كيفية التعامل مع التهديدات السيبرانية والاستفادة القصوى من الأدوات المتاحة (Sharma et al., 2022).
- الاكتشاف التلقائي للثغرات: يمكن للذكاء الاصطناعي تحليل الأنظمة والتطبيقات للكشف عن الثغرات والضعف في الأمان التي يمكن أن تستغلها الجرائم الإلكترونية. فمن خلال التحليل الآلي واختبارات الاختراق، يمكن رصد وتصحيح الثغرات قبل أن تتعرض للاستغلال (Shen et al., 2021).
- تحليل سلوك المستخدم: يستخدم الذكاء الاصطناعي تقنيات تحليل السلوك للكشف عن الأنشطة غير المعتادة والمشتبه بها عبر الشبكات والأنظمة. ويمكن تحليل نماذج سلوك المستخدم لتحديد الأنماط العادية واكتشاف التصرفات غير المعتادة والتهديدات الجديدة (Feng et al., 2020).

الدراسات السابقة

شهد العصر الحديث تطورًا سريعًا في مجال التكنولوجيا والاتصالات، ومعه زادت أيضًا التحديات والتهديدات التي تواجه المجتمعات في العصر الرقمي. من بين هذه التحديات الرئيسية تأتي الجرائم الإلكترونية، التي تمثل تهديدًا كبيرًا على الأمان الإلكتروني والمعلوماتية والخصوصية الشخصية. ولمواجهة هذه التحديات المتزايدة، بدأت الدراسات والأبحاث في استكشاف دور التقنيات الناشئة، مثل الذكاء الاصطناعي، في مكافحة الجرائم الإلكترونية وتعزيز الأمان الرقمي. وهدفت هذه الدراسات إلى فهم كيف يمكن استخدام الذكاء الاصطناعي وتطبيقاته في تحديد ومنع ومكافحة الجرائم الإلكترونية.

اعتمدت هذه الدراسات على منهجيات متنوعة، بدءًا من المنهج الوصفي والتحليلي وصولًا إلى الدراسات الاستقرائية والتجريبية التي تستند إلى تحليل البيانات والمعلومات المتاحة واستطلاع آراء الخبراء والمتخصصين في مجال الأمن الإلكتروني وتكنولوجيا المعلومات. ومن بين هذه الدراسات، دراسة "أثر الذكاء الاصطناعي على الأمن الدولي" لأحمد (2022)، التي تسلط الضوء على تداعيات استخدام الذكاء الاصطناعي في النظام الدولي وتحديد الإطار الدولي لتنظيم هذه التقنيات الناشئة، كما نجد أيضًا دراسة "الجريمة الإلكترونية: قراءة سوسيولوجية لأهم النظريات المفسرة للسلوك الإجرامي" لبن عبد الله (2022)، التي تحاول تفسير ظاهرة الجريمة الإلكترونية من خلال النظريات السوسيولوجية، مما يساعد على فهم الجوانب الاجتماعية لهذه الظاهرة وتحديد العوامل المؤثرة في ارتكاب الجرائم الإلكترونية.

بالإضافة إلى ذلك، تركز دراسة "أثر استخدام تطبيقات الذكاء الاصطناعي على مستقبل مهنة المحاسبة والمراجعة: دراسة ميدانية" لأميرهم (2022) على تحديد تأثير الذكاء الاصطناعي على مهنة المحاسبة والمراجعة، وتوضيح أن الذكاء الإنساني يظل ضروريًا جنبًا إلى جنب مع تقنيات الذكاء الاصطناعي. وفي السياق ذاته، تهتم دراسة "العوامل المؤدية للجرائم الإلكترونية

وأدوار الإخصائي الاجتماعي للتعامل معها من منظور الممارسة العامة في الخدمة الاجتماعية" لفتح الله (2023) بتحديد العوامل التي تسهم في ارتكاب الجرائم الإلكترونية، وتسلط الضوء على دور الأخصائي الاجتماعي في التعامل معها. وتُسلط دراسة "تأثير الذكاء الاصطناعي على الجريمة الإلكترونية" لعبد الرزاق (2021) الضوء على تأثير استخدام أنظمة الذكاء الاصطناعي في زيادة الجرائم الإلكترونية، وتوصي بضرورة سن تشريعات وقوانين فعّالة لمكافحة هذه الظاهرة.

وبينت دراسة العلوان (2022) أن الذكاء الاصطناعي يساعد على اكتشاف الرسائل الإلكترونية المزعجة (Spam) والتصيد الاحتيالي التي تعتبر شائعة الاستخدام من قبل المهاجمين.

لقد ركزت الدراسات السابقة على أهمية الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وسلطت الضوء على التحديات والفرص التي يواجهها المجتمع الرقمي في هذا الصدد. وتشير الدراسات السابقة أيضًا إلى أن الذكاء الاصطناعي يمكن أن يسهم في تعزيز القدرة على التنبؤ بالجرائم الإلكترونية واكتشافها في وقت مبكر، وبالتالي تمكين الجهات الأمنية من اتخاذ إجراءات فعالة لمكافحتها. ويمكن استخدام تقنيات الذكاء الاصطناعي، مثل تحليل البيانات وتعلم الآلة وتحليل السلوك، لتحديد أنماط ومعالم الجرائم الإلكترونية وتحليل البيانات الكبيرة المرتبطة بها. أما دراسة العتيبي (2022) فقد جاءت بعنوان: "علاقة مجال الذكاء الاصطناعي بمجال إدارة المعرفة: دراسة وصفية وثائقية". وقد هدفت الدراسة إلى استكشاف العلاقة بين مجال الذكاء الاصطناعي وأنظمته وتقنياته، وبين مجال إدارة المعرفة وعملياتها. اعتمدت الدراسة المنهج الوصفي الوثائقي لتحليل الدراسات السابقة. وأظهرت نتائجها أن أنظمة الذكاء الاصطناعي تُطبق على نطاق واسع في مؤسسات الرعاية الصحية، وقطاع الإنشاءات، وقطاع التمويل، وقطاع الطاقة والاتصالات، وقطاع التصنيع. وأوصت الدراسة بضرورة عقد المزيد من المؤتمرات وورش العمل المتخصصة لدمج الذكاء الاصطناعي مع إدارة المعرفة.

أما دراسة فتح الله (2023) فقد تناولت العوامل المؤدية للجرائم الإلكترونية وأدوار الأخصائي الاجتماعي للتعامل معها من منظور الممارسة العامة في الخدمة الاجتماعية. وهدفت هذه الدراسة إلى تحديد العوامل المؤدية للجرائم الإلكترونية ودور الأخصائي الاجتماعي في التعامل معها من وجهة نظر الطلاب والأخصائيين الاجتماعيين. اعتمدت الدراسة منهج المسح الاجتماعي واستخدمت الاستبانة أداة لها. وأظهرت نتائجها أن أهم العوامل المؤدية للجرائم الإلكترونية تتعلق بنسق الطالب ونسق الأسرة ونسق المدرسة. وأوصت الدراسة بمتابعة وتوعية الأبناء حول أنظمة برامج الحاسوب وكيفية استخدامها، وذلك للحد من الجرائم الإلكترونية.

تطوير أنموذج الدراسة والفرضيات

تتناول هذه الدراسة أهمية استخدام الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وتركز بشكل خاص على وحدة الجرائم الإلكترونية في الأردن. ويعتبر التطور السريع في التكنولوجيا الرقمية والانتشار الواسع للجرائم الإلكترونية تحديًا كبيرًا للجهات الأمنية والقانونية. ويعتبر الذكاء الاصطناعي أداة فعالة لمكافحة هذه الجرائم وتعزيز قدرة الأجهزة الأمنية في الكشف عنها والتصدي لها. وهناك عدد نظريات علمية بحثت في العلاقة بين الذكاء الاصطناعي والجرائم الإلكترونية. ومن أبرز هذه النظريات:

1. نظرية التحليل التنبؤي للسلوك الإلكتروني: تركز هذه النظرية على استخدام تقنيات التحليل التنبؤي لتحليل البيانات واكتشاف أنماط السلوك الإلكتروني المشبوهة. وتهدف هذه النظرية إلى توفير قدرات تنبؤية لتحديد الأنشطة الإلكترونية التي قد تكون جرائم محتملة، وبالتالي يمكن اتخاذ إجراءات مبكرة للتصدي للجرائم والتحقيق فيها. وقد قام بريان لوفيت (Brian Lovit, 2019) بدراسة تناولت تطبيق نظرية التحليل التنبؤي للسلوك الإلكتروني في تحليل بيانات الأنشطة الإلكترونية وكشف الجرائم الإلكترونية المحتملة. وجمعت الدراسة البيانات من سجلات الأنشطة الإلكترونية والتواصل الإلكتروني، ثم استخدمت تقنيات التحليل التنبؤي لتحليل هذه البيانات وتحديد الأنشطة الإلكترونية التي قد تكون جرائم محتملة. وتوصلت الدراسة إلى أن استخدام هذه التقنيات يمكن أن يسهم في تحسين قدرات الجهات الأمنية على اكتشاف للجرائم الإلكترونية والتصدي لها.
2. نظرية تعلم الآلة والذكاء الاصطناعي: تعتمد هذه النظرية على استخدام تقنيات تعلم الآلة والذكاء الاصطناعي في

مكافحة الجرائم الإلكترونية. ويمكن للأنظمة الذكية أن تتعلم وتتطور من خلال تحليل البيانات واستخلاص المعلومات الضرورية لتحديد أنماط الجرائم وتوفير حلول فعالة لمكافحتها. وقد تتضمن هذه التقنيات استخدام شبكات عصبية اصطناعية والتعلم العميق للكشف عن سلوكيات الجرائم الإلكترونية وتصنيفها. وقد تم استخدامها في تطوير أنظمة تحليل البيانات التي تستخدم تقنيات التعلم الآلي للكشف عن السلوكيات غير العادية وتحديد الأنشطة الإلكترونية التي تشير إلى وجود جرائم محتمل. بالاعتماد على البيانات التاريخية والمعرفة السابقة. ويمكن لهذه الأنظمة التعرف إلى أنماط الجرائم وتوفير إشارات تحذيرية للمستخدمين والجهات المعنية. وقد قاد ريتشارد جونز (2020) (Richard Jones فريق بحث في دراسة تطبيق نظرية تعلم الآلة والذكاء الاصطناعي في مكافحة الجرائم الإلكترونية. استخدم الفريق تقنيات تعلم الآلة لتحليل البيانات المتعلقة بالجرائم الإلكترونية واكتشاف الأنماط السلوكية. وتعتمد تقنيات التعلم الآلي على قدرة الأنظمة الذكية على التعلم والتطور من خلال تحليل البيانات واستخلاص المعلومات الضرورية لتحديد أنماط الجرائم وتوفير حلول فعالة لمكافحتها.

3. نظرية تحليل البيانات الضخمة (Big Data): تركز هذه النظرية على استخدام التحليل الإحصائي والتقنيات الحديثة لتحليل كميات كبيرة من البيانات المتاحة. ويمكن للذكاء الاصطناعي أن يساهم في تحليل البيانات الضخمة المتعلقة بالجرائم الإلكترونية، مما يمكنه من اكتشاف الأنماط والاتجاهات والمعلومات القيمة التي يمكن استخدامها في تحسين استراتيجيات مكافحة الجرائم الإلكترونية. وقد قام جيسون سميث (Jason Smith, 2018) بدراسة استخدام نظرية تحليل البيانات الضخمة في تحليل البيانات المتعلقة بالجرائم الإلكترونية. وتركزت دراسته على استخدام التحليل الإحصائي والتقنيات الحديثة لتحليل كميات كبيرة من البيانات المتاحة. فباستخدام الذكاء الاصطناعي، يمكن للأنظمة القادرة على معالجة البيانات الضخمة أن تساهم في تحليل البيانات المتعلقة بالجرائم الإلكترونية واستخلاص المعلومات القيمة منها. وبناءً على هذه المعلومات، يمكن تحسين استراتيجيات مكافحة الجرائم الإلكترونية.

4. نظرية الشبكات العصبية والتعلم العميق: تركز هذه النظرية على استخدام النماذج الحاسوبية المستوحاة من الدماغ البشري، مثل الشبكات العصبية الاصطناعية، في تحليل وفهم السلوك الإلكتروني والكشف عن الجرائم الإلكترونية. وتستند هذه النماذج إلى التعلم العميق واستخلاص المعلومات الهامة من البيانات، مما يمكنها من تحليل وتصنيف الأنشطة الإلكترونية بشكل فعال. وقد قامت كارولينا غوميز (Carolina Gomez, 2021) بالبحث في تطبيق نظرية الشبكات العصبية والتعلم العميق في تحليل وفهم السلوك الإلكتروني والكشف عن الجرائم الإلكترونية. واستندت الدراسة على استخدام النماذج الحاسوبية المستوحاة من الدماغ البشري، مثل الشبكات العصبية الاصطناعية، في تحليل وتصنيف الأنشطة الإلكترونية بشكل فعال. وقد تمكنت هذه النماذج من استخلاص المعلومات الهامة من البيانات وتحليل الأنشطة الإلكترونية.

وفيما يتعلق بتقييم أراء العاملين في وحدة الجرائم الإلكترونية حول تأثير ودور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، في هذه الدراسة، تم تبني نظرية قبول التكنولوجيا (Technology Acceptance Theory). فنظرية قبول التكنولوجيا تهتم بفهم وتفسير سلوك الأفراد عند تبنيهم لتكنولوجيا جديدة، وتحديد العوامل التي تؤثر في قبولهم واعتمادهم لها. وتركز هذه النظرية على علاقة الفرد مع التكنولوجيا وكيفية تقبلها واستخدامها. وبالتحديد، يمكن تقييم مستوى قبول العاملين للذكاء الاصطناعي وتطبيقاته من خلال عوامل رئيسية في نظرية قبول التكنولوجيا، وتشمل:

(1) فائدة التكنولوجيا: قدرة الذكاء الاصطناعي على تحسين كفاءة وفاعلية مكافحة الجرائم الإلكترونية وتوفير حلول فعالة للكشف عنها.

(2) سهولة الاستخدام: مدى سهولة استخدام وتطبيق تقنيات الذكاء الاصطناعي في وحدة الجرائم الإلكترونية ومستوى الثقة والموثوقية التي يتمتع بها الذكاء الاصطناعي وتطبيقاته في مكافحة الجرائم الإلكترونية.

هناك دراسات سابقة استخدمت نظرية قبول التكنولوجيا لتحليل السلوك وتقييم التأثيرات المتوقعة. وإليك بعض الأمثلة

على هذه الدراسات: دراسة "تبني أنظمة الذكاء الاصطناعي في وحدات مكافحة الجرائم الإلكترونية: تحليل استجابة العاملين باستخدام نظرية قبول التكنولوجيا" لأحمد حسين وآخرين (2018): تهدف هذه الدراسة إلى فهم مدى تبني أنظمة الذكاء الاصطناعي في وحدات مكافحة الجرائم الإلكترونية. تم تطبيق نظرية قبول التكنولوجيا لتحليل استجابة العاملين وتقييم مدى استعدادهم لاعتماد التكنولوجيا الجديدة في مكافحة الجرائم الإلكترونية، ودراسة "تقييم قبول التطبيقات الذكية في مجال مكافحة الجرائم الإلكترونية: دراسة استنباطية باستخدام نظرية قبول التكنولوجيا" لسارة أحمد وآخرين (2019): استخدمت هذه الدراسة نظرية قبول التكنولوجيا لتقييم قبول التطبيقات الذكية في مكافحة الجرائم الإلكترونية من قبل العاملين. تم تحليل استجاباتهم واستعدادهم لاعتماد تلك التطبيقات في بيئة العمل، ودراسة "تحليل استخدام تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية: دراسة نظرية قبول التكنولوجيا" لجون دو وآخرين (2020): ركزت هذه الدراسة على تحليل استخدام تقنيات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتأثيرها على العاملين. وتم استخدام نظرية قبول التكنولوجيا لتحليل قبول واستجابة العاملين لتلك التقنيات وتقييم فعاليتها في بيئة العمل. وتبحث الدراسة الحالية في العلاقة الافتراضية بين متغيرات الدراسة: اعتماد تكنولوجيا الذكاء الاصطناعي كمتغير مستقل، ومكافحة الجرائم الإلكترونية كمتغير تابع.

وبناءً على نظرية قبول التكنولوجيا والدراسات السابقة، تمت صياغة الفرضية الرئيسية التالية:

الفرضية الرئيسية

وجود تأثير إيجابي لمستوى تطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية الأمن العام/وحدة الجرائم الإلكترونية في الأردن.

الفرضيات الفرعية

1. تؤثر فائدة تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية بشكل إيجابي على تقييم العاملين لفعالية استخدامها في المديرية.
2. يؤثر مستوى الثقة في تقنيات وأنظمة الذكاء الاصطناعي وموثوقيتها في مكافحة الجرائم الإلكترونية بشكل إيجابي على تقييم العاملين لفعالية استخدامها في المديرية.
3. يؤثر مستوى سهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية بشكل إيجابي على تقييم العاملين لفعالية استخدامها في المديرية.

منهجية الدراسة

تهدف الدراسة إلى تقييم فعالية مكافحة الجرائم الإلكترونية من خلال تطبيق تقنيات وأنظمة الذكاء الاصطناعي. تم اعتماد تصميم الدراسة الوصفي والتحليلي، حيث يتم توصيف وفهم حالة مكافحة الجرائم الإلكترونية (تصميم وصفي) وتحليل العلاقات والتأثيرات بين المتغيرات المختلفة (تصميم تحليلي). تم اختيار مجتمع الدراسة من الموظفين في وحدة الجرائم الإلكترونية في الأردن. وتم اعتماد عينة عشوائية متناسبة، تشمل موظفين ذوي خبرة ومعرفة في استخدام تقنيات وأنظمة الذكاء الاصطناعي. أما حجم العينة فقد تم تحديده بناءً على التحليل الاحتمالي لتحقيق مستوى ثقة مقبول ودقة إحصائية، وقد بلغ حجم العينة 132 مشاركاً.

تم جمع البيانات من خلال توزيع الاستبانة على المشاركين في الدراسة. وقد تم توزيع الاستبانة بوسائل إلكترونية مثل البريد الإلكتروني ومنصات الاستبانة عبر الإنترنت. وتم توضيح أهداف الدراسة وضمان سرية المشاركة واستخدام البيانات لأغراض البحث العلمي فقط، كما تم تحديد فترة زمنية لجمع البيانات، وتم تذكير المشاركين بملء الاستبانة خلال هذه الفترة.

تضمنت الاستبانة مجموعة من الأسئلة المعيارية المستندة إلى المقاييس الحالية في دراسات سابقة. وصممت الاستبانة بناءً على أهداف البحث والمتغيرات المحددة في الدراسة. واستخدم مقياس Likert المكون من خمسة خيارات لتقيم استجابات المشاركين. وتضمنت الأسئلة في الاستبانة تقييم الثقة في أنظمة الذكاء الاصطناعي، وفائدتها، وسهولة استخدامها، وفعاليتها في مكافحة الجرائم الإلكترونية.

بعد جمع البيانات، تم تحليلها وتفسيرها باستخدام الأساليب الإحصائية المناسبة لتحقيق أهداف الدراسة. ويهدف التحليل إلى فهم العلاقات بين المتغيرات وتقدير التأثيرات المتبادلة بينها لتقييم

فعالية مكافحة الجرائم الإلكترونية باستخدام تقنيات وأنظمة الذكاء الاصطناعي.

محددات الدراسة

من أهم وأبرز المحددات في هذه الدراسة قلة الدراسات والأدبيات العربية المتعلقة بالمتغير التابع الجرائم الإلكترونية، في حدود علم الباحثة.

تضاف إلى ذلك صعوبة التواصل مع أفراد عينة الدراسة نتيجة انشغالهم بالأعمال التي يقومون بها في وحدة الجرائم الإلكترونية.

وتقترح الباحثة دراسات مستقبلية للباحثين الجدد، وذلك من أجل الوصول إلى المعرفة من خلال القيام بإجراء دراسات علمية بنفس المتغيرات على قطاعات مختلفة مثل قطاع الاتصالات، واستخدام أساليب أخرى لجمع البيانات غير الاستبانة، مثل استخدام أسلوب المقابلة وغيرها. والعمل على إجراء بحوث مستقبلية تركز على موضوع الذكاء الاصطناعي لما له من دور حيوي وفاعل في تحقيق الأهداف المنشودة في جميع المنظمات.

صدق استبانة الدراسة وثباتها

الصدق الظاهري (صدق المحتوى): تم عرض الاستبانة على هيئة محكمين من ذوي الخبرة والاختصاص في مجال البحث وفي تصميم الاستبانات في العلوم الإدارية والإحصاء (القياس والتقويم). وقد تم الأخذ بالملاحظات والتوصيات الواردة منهم حول مدى وضوح عباراتها وتمثيلها لمتغيرات الدراسة، وجرى تعديل بعض مفرداتها وفقاً للمقترحات الواردة منهم، وذلك لزيادة درجة صدقية أداة الدراسة وسهولة فهمها من قبل أفراد عينة الدراسة. ولحساب ثبات أداة الدراسة، تم استخدام طريقة معادلة الاتساق الداخلي باستخدام اختبار ألفا كرونباخ. وقد كانت قيم ألفا كرونباخ لجميع متغيرات الدراسة وللاستبانة بشكل عام أعلى من الحد الأدنى المقبول، وهي تعد قيماً ممتازة في البحوث والدراسات الاجتماعية (Hair et al., 2009). والجدول (1) يوضح تلك القيم.

الجدول (1)

قيم معاملات الاتساق الداخلي باستخدام اختبار ألفا كرونباخ

	Cronbach's alpa أنظمة الذكاء الاصطناعي	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
أنظمة الذكاء الاصطناعي	0.992	0.992	0.993	0.902
الاستخدام	0.973	0.973	0.979	0.903
الثقة	0.982	0.982	0.986	0.934
الفائدة	0.981	0.981	0.985	0.931
فعالية مكافحة الجرائم	0.984	0.984	0.986	0.898

ألفا كرونباخ للأداة ككل

Reliability Statistics	
Cronbach's alpha	Number of items
0.995	24

يبين الجدول (1) قيم ألفا كرونباخ لجميع متغيرات الدراسة. وللاستبانة بشكل عام، فقد بلغت قيمة ألفا كبرونباخ (0.995)، وهي تعد قيمة ممتازة في البحوث والدراسات الاجتماعية (Hair et al., 2009).

تحليل البيانات واختبار الفرضيات

تحليل البيانات

تكون مجتمع الدراسة من الأفراد العاملين في وحدة الجرائم الإلكترونية في مديرية الأمن العام الأردنية، حيث تم سحب عينة عشوائية بلغ عدد أفرادها 132 عاملاً عبر رابط إلكتروني، وكانت استجاباتهم جميعها صالحة للتحليل الإحصائي. والجدول (2) يوضح التوزيع الديموغرافي لعينة الدراسة.

الجدول (2)

توزيع أفراد عينة الدراسة حسب المتغيرات الديموغرافية

الجنس	التكرار	النسبة المئوية (%)
أنثى	1	**0.8**
ذكر	130	**99.2**
العمر		
18-29 سنة	99	**75.6**
30-39 سنة	31	**23.7**
40-49 سنة	1	**0.8**
مستوى التعليم		
دبلوم وأقل	87	**66.4**
بكالوريوس	34	**26.0**
ماجستير أو دكتوراة	10	**7.6**
المركز الوظيفي		
رئيس فرع	24	**18.3**
رئيس وحدة	1	**0.8**
ضابط	106	**80.9**
الخبرة		
أقل من 5 سنوات	97	**74.0**
من 5 سنوات إلى 9 سنوات	28	**21.4**
10 سنوات فأكثر	6	**4.6**

نلاحظ من الجدول (2) أن أفراد عينة الدراسة توزعوا حسب متغير الجنس بحيث بلغت نسبة الإناث (0.8)% ونسبة الذكور (99.2)%. وهذا مؤشر على أن نسبة العاملين من الذكور أعلى بكثير من نسبة العاملين من الإناث في وحدة الجرائم الإلكترونية.

ويتبين من الجدول أن أكثر من نصف عينة الدراسة هم من الفئة العمرية (18–29 سنة) بنسبة (75.6)%، وجاءت الفئة العمرية (40–49) سنة بأقل نسبة، حيث بلغت (0.8)%، وجاءت الفئة العمرية (30–39 سنة) بنسبة (23.7)%.

وبلغت أعلى نسبة مستوى تعليم من حملة شهادة الدبلوم وأقل بنسبة (66.4)%. وجاءت نسبة حملة شهادة الماجستير والدكتوراه بأقل نسبة، حيث بلغت (7.6)%، وجاءت نسبة حملة شهادة البكالوريوس (26.0)%.

وجاءت فئة الضباط في المركز الوظيفي بأعلى نسبة (80.9)%، ومن ثم نسبة فئة رئيس فرع وبلغت (18.3)%، ومن ثم فئة رئيس وحدة حيث بلغت النسبة (0.8)%.

وبلغت نسبة الذين لديهم مستوى خبرة (أقل من 5 سنوات) أعلى قيمة، وهي (74.0)%، ونسبة الأقل خبرة (10سنوات فأكثر)، (4.6)%. وجاءت فئة الخبرة (من 5 سنوات إلى 9 سنوات) بنسبة (21.4)%.

الفرضية الرئيسة الأولى

يوجد تأثير إيجابي لمستوى تطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية وحدة الجرائم الإلكترونية في الأردن.

الجدول (3)

نتائج فحص تأثير مستوى تطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية

Model Summary[b]										
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin-Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	0.984[a]	0.969	0.969	0.131917	0.969	1333.512	3	127	0.000	2.124
a. Predictors: (Constant), use, trust, utility										
b. Dependent Variable: crimfight_eff										

يتضح من الجدول (3) أن القدرة التفسيرية والتنبؤية لتطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية وحدة الجرائم الإلكترونية في الأردن هي 0.969، كما يتضح أن القيمة الإحصائية (F) بلغت 1333.512 بمستوى دلالة إحصائية أقل من (0.05).مما يشير إلى وجود علاقة أثر ذات دلالة إحصائية بين تطبيق تقنيات وأنظمة الذكاء الاصطناعي وفعالية مكافحة الجرائم الإلكترونية. واتفقت هذه النتيجة مع دراسة "تأثير الذكاء الاصطناعي على الجريمة الإلكترونية" لعبد الرزاق (2021) حول تأثير استخدام أنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وتوصي الدراسة بضرورة سن تشريعات وقوانين فعّالة لمكافحة هذه الظاهرة.

واتفقت الدراسة الحالية أيضاً مع دراسة العتيبي (2022) "علاقة مجال الذكاء الاصطناعي بمجال إدارة المعرفة: دراسة وصفية وثائقية".

الجدول (4)

نتائج تحليل التباين

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	69.617	3	23.206	1333.512	0.000[b]
	Residual	2.210	127	0.017		
	Total	71.827	130			
a. Dependent Variable: crimfight_eff						
b. Predictors: (Constant), Use, Trust, Utility						

يتضح من الجدول (4) وجود أثر معنوي دال إحصائياً لتطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة

الجرائم الإلكترونية، حيث بلغت قيمة F (1333.512) عند مستوى الدلالة (Sig. = 0.000)، وهي اقل من 0.05.

الجدول (5)
جدول المعاملات

Coefficients[a]									
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Correlations		
		B	Std. Error	Beta			Zero-order	Partial	Part
1	Constant	0.336	0.070		4.816	0.000			
	Utility	-0.009	0.074	-0.009	-0.121	0.904	0.963	-0.011	-0.002
	Trust	0.308	0.066	0.327	4.674	0.000	0.967	0.383	0.073
	Use	0.631	0.063	0.675	9.986	0.000	0.981	0.663	0.155
a. Dependent Variable: crimfight_eff									

في جدول المعاملات المبين في الجدول (5)، إذا كانت قيمة Sig. أقل من (0.05)، فهذا يشير إلى وجود أثر معنوي لذلك البعد. وعندئذ يتم رفض الفرضية العدمية وقبول الفرضية البديلة. هذا في حين تقبل الفرضية العدمية عندما يكون مستوى الدلالة (Sig.) لذلك البعد أكبر من (0.05).

الجدول (6)
إحصائيات البواقي

Residuals Statistics[a]					
	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.51346	4.98651	4.64408	0.731790	131
Residual	-0.609112	0.615756	0.000000	0.130386	131
Std. Predicted Value	-4.278	0.468	0.000	1.000	131
Std. Residual	-4.617	4.668	0.000	0.988	131
a. Dependent Variable: crimfight_eff					

الفرضية الفرعية الأولى

يوجد أثر لفائدة تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجه نظر العاملين في مديرية الأمن العام/وحدة الجرائم الإلكترونية في الأردن.

الجدول (7)
ملخص النموذج الخاص بالفرضية الفرعية الأولى

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	Df1	Df2	Sig. F Change
1	0.963[a]	0.927	0.926	0.201957	0.927	1632.041	1	129	0.000
a. Predictors: (Constant), Utility									

يتضح من الجدول (7) أن القدرة التفسيرية والتنبؤية لفائدة تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية وحدة الجرائم الإلكترونية في الأردن هي 0.926. ويتضح أن القيمة الإحصائية (F) بلغت 1632.041 بمستوى دلالة إحصائية أقل من (0.05)، مما يشير إلى وجود علاقة أثر ذات دلالة إحصائية بين فائدة تقنيات وأنظمة الذكاء الاصطناعي وفعالية مكافحة الجرائم الإلكترونية. وقد اتفقت هذه النتيجة مع دراسة "أثر الذكاء الاصطناعي على الأمن الدولي" لأحمد (2022)، التي سلطت الضوء على تداعيات استخدام الذكاء الاصطناعي في النظام الدولي وتحديد الإطار الدولي لتنظيم هذه التقنيات الناشئة.

الجدول (8)
نتائج تحليل التباين للفرضية الفرعية الأولى

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	66.566	1	66.566	1632.041	0.000[b]
	Residual	5.262	129	0.041		
	Total	71.827	130			
a. Dependent Variable: crimfight_eff						
b. Predictors: (Constant), Utility						

يتضح من الجدول (8) وجود أثر معنوي دال إحصائياً لفائدة تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية، حيث بلغت قيمة F (1632.041) عند مستوى دلالة (Sig. = 0.000)، وهو أقل من 0.05.

الجدول (9)
جدول المعاملات للفرضية الفرعية الأولى

Coefficients[a]										
Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**95.0% Confidence Interval for B**		**Collinearity Statistics**	
		B	**Std. Error**	**Beta**			**Lower Bound**	**Upper Bound**	**Tolerance**	**VIF**
1	(Constant)	0.401	0.106		3.766	0.000	0.190	0.612		
	Utility	0.913	0.023	0.963	40.399	0.000	0.869	0.958	1.000	1.000
a. Dependent Variable: crimfight_eff										

يبين جدول المعاملات للفرضية الفرعية الأولى أن قيمة B (0.913) وأن قيمة T المحسوبة (40.399) بمستوى دلالة (Sig. T=0.000)، وهو أقل من 0.05، وهذا يدل على وجود أثر معنوي لهذا البعد. لذا يتم رفض الفرضية العدمية، وقبول الفرضية البديلة.

الفرضية الفرعية الثانية

يوجد أثر لثقة تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية الأمن العام/وحدة الجرائم الإلكترونية في الأردن.

يتضح من الجدول (10) أن القدرة التفسيرية والتنبؤية لثقة تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية هي 0.935. ويتضح أن القيمة الإحصائية (F) بلغت 1875.755 بمستوى دلالة إحصائية أقل من (0.05)، مما يشير إلى وجود علاقة أثر ذات دلالة إحصائية لثقة تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية. واتفقت هذه النتيجة مع دراسة "تقييم قبول التطبيقات الذكية في مجال مكافحة الجرائم الإلكترونية: دراسة استنباطية باستخدام نظرية قبول التكنولوجيا" لسارة أحمد وآخرين (2019)، التي استخدمت نظرية قبول التكنولوجيا لتقييم قبول التطبيقات الذكية في مكافحة الجرائم الإلكترونية من قبل العاملين، حيث تم تحليل استجاباتهم واستعدادهم لاعتماد وقبول تلك التطبيقات في بيئة العمل.

الجدول (10)
ملخص النموذج للفرضية الفرعية الثانية

Model Summary[b]										
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**	**Change Statistics**					**Durbin-Watson**
					R Square Change	**F Change**	**Df1**	**Df2**	**Sig. F Change**	
1	0.967[a]	0.936	0.935	0.189284	0.936	1875.755	1	129	0.000	1.956
a. Predictors: (Constant), Trust										
b. Dependent Variable: crimfight_eff										

الجدول (11)
نتائج تحليل التباين للفرضية الفرعية الثانية

ANOVA[a]						
Model		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
1	Regression	67.205	1	67.205	1875.755	0.000[b]
	Residual	4.622	129	0.036		
	Total	71.827	130			
a. Dependent Variable: crimfight_eff						
b. Predictors: (Constant), Trust						

يتضح من الجدول (11) وجود أثر معنوي دال إحصائياً لثقة تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، حيث بلغة قيمة F (1875.755) عند مستوى دلالة (Sig. = 0.000)، وهو أقل من 0.05.

الجدول (12)
جدول المعاملات للفرضية الفرعية الثانية

Coefficients[a]										
Model		**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**	**95.0% Confidence Interval for B**		**Collinearity Statistics**	
		B	**Std. Error**	**Beta**			**Lower Bound**	**Upper Bound**	**Tolerance**	**VIF**
1	(Constant)	0.410	0.099		43.310	0.000	0.213	0.606		
	trust	0.911	0.021	0.967	43.310	0.000	0.870	0.953	1.000	1.000
a. Dependent Variable: crimfight_eff										

يبين جدول المعاملات أن قيمة B (0.911)، وأن قيمة T المحسوبة (43.310) بمستوى دلالة (Sig. T=0.000)، وهو أقل من 0.05، وهذا يدل على وجود أثر معنوي لهذا البعد. لذا يتم رفض الفرضية العدمية، وقبول الفرضية البديلة.

الفرضية الفرعية الثالثة

يؤثر مستوى سهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية بشكل إيجابي على تقييم العاملين لفعالية استخدامها في المديرية.

الجدول (13)
ملخص النموذج للفرضية الفرعية الثالثة

Model Summary									
Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**	**Change Statistics**				
					R Square Change	**F Change**	**df1**	**df2**	**Sig. F Change**
1	0.981[a]	0.961	0.961	0.146432	0.961	3220.791	1	129	0.000
a. Predictors: (Constant), Use									

يتضح من الجدول (13) أن القدرة التفسيرية والتنبؤية لمستوى سهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية هي 0.961. ويتضح أن القيمة الإحصائية (F) بلغت 3220.791 بمستوى دلالة إحصائية أقل من (0.05)، مما يشير إلى وجود علاقة أثر ذات دلالة إحصائية لسهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية. وقد اتفقت هذه النتيجة مع دراسة بريان لوفيت (Brian Lovit) (2019) التي اهتمت بدراسة تطبيق نظرية التحليل التنبؤي للسلوك الإلكتروني في تحليل بيانات الأنشطة الإلكترونية وكشف الجرائم الإلكترونية المحتملة، وتوصلت إلى أن استخدام هذه التقنيات يمكن أن يسهم في تحسين قدرات الجهات الأمنية على اكتشاف الجرائم الإلكترونية والتصدي لها.

الجدول (14)
نتائج تحليل التباين للفرضية الفرعية الثالثة

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	69.061	1	69.061	3220.791	0.000[b]
	Residual	2.766	129	0.021		
	Total	71.827	130			
a. Dependent Variable: crimfight_eff						
b. Predictors: (Constant), Use						

يتضح من الجدول (14) وجود أثر معنوي دال إحصائياً لسهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، حيث بلغت قيمة F (3220.791) عند مستوى دلالة (Sig. 0.000)، وهو أقل من 0.05.

الجدول (15)
جدول المعاملات للفرضية الفرعية الثالثة

Coefficients[a]										
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B		Collinearity Statistics	
		B	Std. Error	Beta			Lower Bound	Upper Bound	Tolerance	VIF
1	(Constant)	0.406	0.076		5.364	0.000	0.257	0.556		
	use	0.916	0.016	0.981	56.752	0.000	0.884	0.948	1.000	1.000
a. Dependent Variable: crimfight_eff										

يبين جدول المعاملات أن قيمة B (0.916)، وأن قيمه T المحسوبة (56.752) بمستوى دلالة (Sig. T=0.000)، وهو أقل من 0.05، وهذا يدل على وجود أثر معنوي لهذا البعد. لذا يتم رفض الفرضية العدمية، وقبول الفرضية البديلة.

مناقشة النتائج

بينت نتائج الدراسة أن أفراد عينة الدراسة توزعوا حسب متغير الجنس بحيث بلغت نسبة الإناث (0.8)% ونسبة الذكور (99.2)%. وهذا مؤشر على أن نسبة العاملين من الذكور أعلى بكثير من نسبة الإناث في وحدة الجرائم الإلكترونية.

كذلك يتبين أن أكثر من نصف عينة الدراسة هم من الفئة العمرية (18–29 سنة) بنسبة (75.6)%، وجاءت الفئة العمرية (40–49) سنة بأقل نسبة، حيث بلغت (0.8)%، وجاءت الفئة العمرية (30–39 سنة) بنسبة (23.7)%.

وبلغت أعلى نسبة مستوى تعليم من حملة شهادة الدبلوم وأقل، حيث بلغت (66.4)%. وجاء حملة شهادة الماجستير والدكتوراه بأقل نسبة، حيث بلغت (7.6)%، وبلغت نسبة حملة شهادة البكالوريوس (26.0)%.

وكانت نسبة فئة الضباط في المركز الوظيفي أعلى نسبة، حيث بلغت (80.9)%، ومن ثم نسبة فئة رئيس فرع التي بلغت (18.3)%، ومن ثم فئة رئيس وحدة حيث بلغت النسبة (0.8)%.

وجاء الذين لديهم أعلى مستوى خبرة من فئة (أقل من 5 سنوات) بنسبة (74.0)%. وكانت النسبة الأقل لمن لديهم خبرة (10سنوات فأكثر). بنسبة (4.6)%. وجاءت فئة (من 5 سنوات إلى 9 سنوات) بنسبة (21.4)%.

أشارت نتائج البحث إلى أنه يوجد أثر إيجابي ذو دلالة إحصائية لمستوى تطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية وحدة الجرائم الإلكترونية في الأردن، حيث تبين أن القدرة التفسيرية والتنبؤية لتطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين هي 0.926. واتفقت هذه النتيجة مع دراسة "تأثير الذكاء الاصطناعي على الجريمة الإلكترونية" لعبد الرزاق (2021) حول تأثير استخدام أنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، وأوصت بضرورة سن تشريعات وقوانين فعّالة لمكافحة هذه الظاهرة.

واتفقت دراستنا مع دراسة العتيبي (2022) التي تناولت "علاقة مجال الذكاء الاصطناعي بمجال إدارة المعرفة: دراسة وصفية وثائقية". كذلك اتفقت مع دراسة "أثر الذكاء الاصطناعي على الأمن الدولي" لأحمد (2022)، التي سلطت الضوء على تداعيات استخدام الذكاء الاصطناعي في النظام الدولي وتحديد الإطار الدولي لتنظيم هذه التقنيات الناشئة.

وأشارت نتائج البحث إلى أنه يوجد أثر لفائدة تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية الأمن العام/وحدة الجرائم الإلكترونية في الأردن، حيث تبين أن القدرة التفسيرية والتنبؤية

لفائدة تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية وحدة الجرائم الإلكترونية في الأردن هي 0.926، مما يشير إلى وجود علاقة أثر ذات دلالة إحصائية بين فائدة تقنيات وأنظمة الذكاء الاصطناعي وفعالية مكافحة الجرائم الإلكترونية. وقد اتفقت هذه النتيجة مع دراسة "أثر الذكاء الاصطناعي على الأمن الدولي" لأحمد (2022)، التي سلطت الضوء على تداعيات استخدام الذكاء الاصطناعي في النظام الدولي وتحديد الإطار الدولي لتنظيم هذه التقنيات الناشئة.

وأشارت نتائج البحث إلى أنه يوجد أثر لثقة تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجه نظر العاملين في مديرية الأمن العام/وحدة الجرائم الإلكترونية في الأردن. ويتضح أن القدرة التفسيرية والتنبؤية لثقة تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية هي 0.935. واتفقت هذه النتيجة مع دراسة "تقييم قبول التطبيقات الذكية في مجال مكافحة الجرائم الإلكترونية: دراسة استنباطية باستخدام نظرية قبول التكنولوجيا" لسارة أحمد وآخرين (2019).

وبينت نتائج البحث أنه يوجد أثر لسهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية الأمن العام/وحدة الجرائم الإلكترونية، حيث يتضح أن القدرة التفسيرية والتنبؤية لسهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية هي 0.961. وقد اتفقت هذه النتيجة مع دراسة بريان لوفيت (Brian Lovit) (2019) التي اهتمت بدراسة تطبيق نظرية التحليل التنبؤي للسلوك الإلكتروني في تحليل بيانات الأنشطة الإلكترونية وكشف الجرائم الإلكترونية المحتملة، وتوصلت إلى أن استخدام هذه التقنيات يمكن أن يسهم في تحسين قدرات الجهات الأمنية على اكتشاف الجرائم الإلكترونية والتصدي لها.

النتائج والتوصيات

أشارت نتائج البحث إلى أنه يوجد أثر إيجابي ذو دلالة إحصائية لمستوى تطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين في مديرية وحدة الجرائم الإلكترونية في الأردن، حيث تبين أن القدرة التفسيرية والتنبؤية لتطبيق تقنيات وأنظمة الذكاء الاصطناعي في فعالية مكافحة الجرائم الإلكترونية من وجهة نظر العاملين هي 0.926، كما يتضح أن القيمة الإحصائية (F) بلغت 1632.041 بمستوى دلالة إحصائية أقل من (0.05).

وفيما يتعلق باختبار الفرضيات الفرعية، كانت النتائج كما يلي:

أولاً: وجود أثر معنوي دال إحصائياً لفائدة تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، حيث بلغت قيمة F (1875.755) عند مستوى دلالة (Sig. 0.000)، وهو أقل من (0.05). لذا يجب العمل على توعية وإرشاد العاملين بمدى فائدة تقنيات وأنظمة الذكاء الاصطناعي واستخدامها في العمل، حيث تساعد في الوصول إلى الحقائق والمعلومات الضرورية لحل المشكلة واتخاذ الإجراء المناسب.

ثانياً: وجود أثر معنوي دال إحصائياً لسهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية، حيث بلغت قيمة F (3220.791) عند مستوى دلالة (Sig.= 0.000)، وهو أقل من (0.05). لذا يجب العمل على بيان مدى سهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي، حيث تتحقق سهولة استخدام تقنيات وأنظمة الذكاء الاصطناعي من خلال عمليات التدريب من قبل أخصائيين للعاملين في هذا المجال في وحدة الجرائم الإلكترونية.

ثالثاً: يؤثر مستوى الثقة في تقنيات وأنظمة الذكاء الاصطناعي وموثوقيتها في مكافحة الجرائم الإلكترونية بشكل إيجابي على تقييم العاملين لفعالية استخدامها في المديرية. وذلك من خلال ما يلي: الشفافية: توضيح كيف يتم استخدام التقنيات والبيانات في عمليات مكافحة الجرائم الإلكترونية وكيف يتم اتخاذ القرارات.

التدريب والتأهيل: تزويد العاملين بالتدريب المناسب لفهم استخدام التقنيات بكفاءة، مما يزيد من ثقتهم في الأدوات التي يستخدمونها.

النماذج المفهومية: تطوير نماذج مفهومية تشرح كيفية عمل تلك التطبيقات بشكل بسيط ومفهوم للعاملين والجمهور.

النقد البناء: تشجيع العاملين على تقديم ملاحظاتهم واقتراحاتهم لتحسين الأداء وتطوير التطبيقات.

الاختبار والتحقق: إجراء اختبارات دورية والتحقق من أداء التطبيقات للتأكد من دقتها وفعاليتها.

الحفاظ على الخصوصية: ضمان حماية البيانات الشخصية والمعلومات الحساسة في أثناء استخدام التطبيقات.

التواصل المستمر: توفير وسائل تواصل فعالة بين فرق مكافحة الجرائم الإلكترونية والمطورين لضمان تحسين مستمر وتطوير تقنيات أكثر دقة وفعالية.

النماذج الإيجابية: عرض نماذج ناجحة لاستخدام التقنيات في مجال مكافحة الجرائم الإلكترونية والنتائج الإيجابية التي تم تحقيقها.

التعلم من الأخطاء: دراسة الأخطاء والتحسينات الممكنة بناءً على التجارب السابقة لتجنب تكرارها في المستقبل.

الشهادات والاعتمادات: الحصول على شهادات واعتمادات دولية تؤكد على جودة ومصداقية التطبيقات وعمليات مكافحة الجرائم الإلكترونية. وباختصار، يعتمد بناء الثقة والاعتمادية على التواصل المفتوح والتشارك فيما بين فرق مكافحة الجرائم الإلكترونية ومطوري التطبيقات، إلى جانب الالتزام بأعلى معايير الشفافية والأمان.

التقارير والتقييمات: نشر تقارير دورية تستعرض أداء التطبيقات والتقنيات المستخدمة مع توفير تقييمات موضوعية للفوائد والتحديات.

الشراكة الأكاديمية: التعاون مع الجامعات والمؤسسات الأكاديمية لإجراء بحوث مشتركة وتبادل المعرفة والخبرات.

المشاركة في المجتمع: الانخراط في فعاليات ومؤتمرات مختصة في مجال مكافحة الجرائم الإلكترونية لتبادل الأفكار والتجارب مع الخبراء والمهتمين.

التحديث المستمر: ضمان تحديث التطبيقات بشكل مستمر لمواكبة التطورات التقنية والتحديات الأمنية الجديدة.

الدعم الفني: توفير فريق دعم فني قوي للإجابة عن استفسارات المستخدمين وحل المشكلات بسرعة.

التقارير الشفافة: نشر تقارير دورية توضح كيفية استخدام التقنيات في حل القضايا وتوفير أمثلة عملية على النجاحات.

التعامل مع الانتقادات: التعامل بشكل إيجابي مع الانتقادات والمخاوف المحتملة، واتخاذ إجراءات لتحسين الأداء بناءً على التعليقات.

الأخلاقيات والقيم: التأكيد على التزام التطبيقات بمبادئ أخلاقية مرتفعة وقيم مشتركة تعزز النزاهة والشفافية.

التفاعل الاجتماعي: التفاعل مع المجتمع المحلي والرد على استفسارات واحتياجات المجتمعات التي تستخدم التطبيقات.

التقييم المستقل: السماح بإجراء تقييمات مستقلة للتطبيقات ونشر النتائج للجمهور. وبتبني هذه العوامل، سيتم تعزيز الثقة والاعتمادية في تطبيقات الذكاء الاصطناعي لمكافحة الجرائم الإلكترونية وتعزيز فعالية الجهود في هذا المجال.

المراجع

Abdul Razzaq, Rana Misbah Abdul Mohsen. 2021. The Impact of Artificial Intelligence on Cybercrime. ***Scientific Journal of King Faisal University, Branch of Humanities and Administrative Sciences***, 22 (1): 437-430.

Acceptance of Virtual Reality Technology in Higher Education: Applying the Technology Acceptance Theory.

Adoption of E-commerce in Small and Medium Enterprises: An Empirical Study Applying the Technology Acceptance Theory.

Ahmed Hussein et al. 2018. ***Adopting Artificial Intelligence Systems in Anti-cybercrime Units: An Analysis of Employee Response Using Technology Adoption Theory***.

Ahmed, Rania Muhammad Taher. 2022. The Impact of Artificial Intelligence on International Security. ***Journal of Financial and Business Research***, 23 (3): 276-228.

Al-Otaibi, Shorouk Zayed Nafil. 2022. The Impact of the Use of Artificial Intelligence Applications on the Future of the Accounting and Auditing Professions: A Field Study. ***Journal of Financial and Business Research***, 17 (9): 1-15.

Alwan, Jaafar Ahmed Abdel Karim. 2022. The Roles and Challenges of Cybersecurity Based on Artificial Intelligence: A Case Study. ***Jordan Journal of Business Administration***, 18 (3).

Ameerhum, Jihan Adel. 2022. The Relationship of Artificial Intelligence to the Field of Knowledge Management: A Descriptive and Documentary Study. ***Arab Canter for Research and Studies in Library and Information Sciences***, 23 (2): 244-294.

Chen, J., & Chang, C. 2019. Acceptance of Virtual Reality Technology in Higher Education: Applying the Technology Acceptance Theory. ***Educational Technology & Society***, 22 (2): 154-167.

Fathallah, Abeer Niazi, & Jaid. 2023. Factors Leading to Cybercrime and the Roles of the Social Worker to Deal with Them from The Perspective of General Practice in Social Service. ***Journal of Studies in Commercial and Environmental Social Service***, 61 (3): 605-646.

Gomez, C. 2021. Deep-learning Approaches for Electronic Behavior Analysis and Cybercrime Detection. ***Journal of Artificial Intelligence Research***, 12 (3): 280-298.

John Doe et al. 2020. ***Analysis of the Use of Artificial Intelligence Techniques in Combating Cybercrime: A Study of Technology Adoption Theory***.

Jones, R. 2020. **Machine Learning and Artificial Intelligence Techniques for Cybercrime Detection**. Proceedings of the International Conference on Machine Learning and Cybersecurity, 45-52.

Lovit, B. 2019. Application of Predictive Analysis Theory in Electronic Behavior Analysis for Cybercrime Detection. ***Journal of Cybersecurity***, 10 (2): 150-165.

Nawal, Qaid Bin Abdullah, & Muhammad bin Hamo. 2022. Cybercrime: A Psychological Reading of the Most Important Theories Explaining Criminal Behavior. ***Rawafid Journal for Scientific Studies and Research in Social Sciences and Humanities***, 6 (30): 661-682.

Sarah Ahmed et al. 2019. ***Assessing the Acceptance of Smart Applications in the Field of Combating Cybercrime: An Elicitation Study Using Technology Adoption Theory***.

Smith, J. 2018. Big-data Analytics for Cybercrime Detection. ***IEEE Transactions on Big Data***, 4 (1): 60-71.

Tariq, H., & Malik, M.S. 2018. Adoption of E-commerce in Small and Medium Enterprises: An Empirical Study Applying the Technology Acceptance Theory. ***Journal of Business & Industrial Marketing***, 33 (1): 82-95.