جامعة القدس المفتوحة

عمادة الدراسات العليا والبحث العلمي

دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً

The Role of Artificial Intelligence in Reducing the Spread of Cybercrimes: Distinguishing the Performance of Members of the Security Services as a Mediator Variable

إعداد:

مروان محمود طرده

بإشراف:

الدكتور: رسلان محمد

قدمت هذه الخطة استكمالاً لمتطلبات درجة الماجستير في برنامج القيادة

والإدارة الاستراتيجية جامعة القدس المفتوحة (فلسطين)

2025

الإجازة

دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً

The Role of Artificial Intelligence in Reducing the Spread of Cybercrimes: Distinguishing the Performance of Members of the Security Services as a Mediator Variable

إعداد:

مروان محمود طرده

بإشراف:

الدكتور: رسلان محمد

نوقشت هذه الرسالة، وأجيزت بتاريخ 2025/7/30 من قبل أعضاء لجنة المناقشة المدرجة أسمائهم وتواقيعهم

أعضاء لجنة المناقشة

د. رسلان أحمد محمد	جامعة القدس المفتوحة	مشرفا ورئيسا.....
د. مروان عادل علاونة	جامعة الاستقلال	عضواً.....
د. ماجد عطا الله حمايل	جامعة القدس المفتوحة	عضواً.....

التفويض

أنا الموقع أدناه؛ **مروان الطردة** أفوض جامعة القدس المفتوحة بتزويد نسح من رسالتي للمكتبات أو المؤسسات أو الأشخاص عند طلبهم بحسب التعليمات النافذة بالجامعة.

اسم الطالب: مرون محمود الطردة

الرقم الجامعي :0330012310200

التوقيع. مروان الطردة

التاريخ: 30/7/ 2025

إقرار

أنا الموقع أدناه مقدم الرسالة التي تحمل عنوان:

"دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً"

"The Role of Artificial Intelligence in Reducing the Spread of Cybercrimes: Distinguishing the Performance of Members of the Security Services as a Mediator Variable"

أقر بأن ما اشتملت عليه هذه الرسالة من نتاج جهدي الخاص، باستثناء ما تمت الإشارة إليه حيث ورد، وأن هذه الرسالة ككل أو أي جزء منها لم يقدم من قبل لنيل درجة أو لقب علمي أو بحث علمي لدى أي مؤسسة بحثية أخرى.

Declaration

I declare that what included in this study by my own effort, with the exception where is mentioned, and this thesis as a whole or any part has not been submitted before to obtain a degree or scientific title or scientific research with any other research institution.

الاسم: مروان محمود الطردة

التوقيع: مروان الطردة

التاريخ: 2025/7/30م

الإهداء

إلى

من رحل جسدهُ، وبقيت روحهُ في القلب نبضًا لا يخبو...

والدي، طيّبَ الله ثراه، فقد كان النور الذي دلّني، والعزم الذي سكنني... أهدي هذا العمل لروحك الطاهرة.

إلى

أمي، نبع الدعاء والحنان، تلك التي كانت لي وطنًا، حين ضاقت الأوطان، وكان دعاؤها نبراسي وسندي.

إلى

زوجتي، رفيقة الحلم والتعب، التي شاركتني التفاصيل واحتملت الغياب، شكري لكِ لا توفيه كلمات.

إلى

زملائي الذين شاركوني الطريق، وساندوني في كل محطة، أنتم شركاء هذا الإنجاز.

إلى

فلسطين... قضيتي الكبرى، وأرضي التي لا تغيب عن القلب...

أهدي هذا الجهد المتواضع وفاءً وانتماءً، وعهدًا بأن يبقى القلم مقاومًا ما بقي فينا نبض.

الشكر والتقدير

الحمد لله الذي بنعمته تتمّ الصالحات، وبتوفيقه تتحقق الغايات.

أتقدمُ بأسمى آيات الشكر والعرفان إلى مشرفي **الأستاذ الدكتور:**

مرسلان محمد

الذي كان نعم الداعم والموجّه، فلم يبخل بعلمه، ولا بوقته، وكان لتوجيهاته القيمة وملاحظاته العلمية الرفيعة أثرٌ بالغ في قيمة هذه الرسالة العلمية، والارتقاء بمستواها. فله مني كل التقدير والاحترام على جهوده المشكورة ومساندته الصادقة طوال فترة إعداد هذا العمل.

كما أتقدم بجزيل الشكر والعرفان إلى **جامعة القدس المفتوحة**، هذه المؤسسة العريقة التي منحتني البيئة الأكاديمية المحفّزة والداعمة، وكانت دومًا منارة للعلم وخدمة المجتمع الفلسطيني.

ولا يفوتني أن أتقدّم بخالص التقدير والامتنان إلى جميع أعضاء الهيئة التدريسية الأفاضل، الذين كان لعطائهم العلمي وتفانيهم في التعليم بالغ الأثر في تكويني الأكاديمي والبحثي. فقد نهلت من علمهم، واستفدت من خبراتهم، وكانوا مثالًا يُحتذى في الجدية والالتزام.

لكم جميعًا مني كل الاحترام والدعاء الصادق، وأسأل الله أن يجزيكم خير الجزاء، وأن يوفقكم لمزيد من العطاء في خدمة العلم والوطن.

الباحث

قائمة المحتويات

قائمة الجداول

قائمة الملاحق

دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً

إعداد: مروان طرده

إشراف الدكتور: رسلان محمد

2025

ملخص

هدفت الدراسة إلى استكشاف دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً، واستخدم المنهج الوصفي والتحليلي، والاستبيان أداة لجمع البيانات، وتمثل مجتمّع الدراسة جميع العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية والذي بلغ عددهم 327 موظفا، وبلغ حجم عينة الدراسة 178 موظفا جرى اختيارهم بطريقة عشوائية، وجرى تحليل البيانات باستخدام البرنامج الإحصائي SPSS.

وقد توصلت الدراسة إلى مجموعة من النتائج التي من أبرزها: أن مستوى تطبيق الذكاء الاصطناعي لدى العاملين في وحدة الجرائم الإلكترونية مرتفع، مع تركيز ملحوظ على التعلم الآلي، ما يعكس التزام الأجهزة الأمنية بتبني التقنيات الحديثة لتعزيز الكفاءة الأمنية، تميز الأداء يلعب دورًا وسيطًا في العلاقة بين استخدام الذكاء الاصطناعي ومستوى الحد من الجرائم الإلكترونية، إذ يسهم الأداء العالي للعاملين في تعزيز قدرتهم على مواجهة الجرائم بفعالية أكبر.

أوصت الدراسة بمجموعة من التوصيات كان من أهمها: الاستثمار في تقنيات الذكاء الاصطناعي الحديثة مع التركيز على تطوير مهارات العاملين لاستثمار هذه التقنيات بشكل أمثل، تعزيز البرامج التدريبية المتخصصة في تقنيات التعلم العميق لتوسيع معارف العاملين وزيادة استخدام هذه التقنية المهمة.

الكلمات المفتاحية: الذكاء الاصطناعي، الحد من انتشار الجرائم الالكترونية، تميز أداء، منتسبي الأجهزة الأمني

The Role of Artificial Intelligence in Reducing the Spread of Cybercrimes: Distinguishing the Performance of Members of the Security Services as a mediator Variable

Prepared by: Marwan Tarda

Supervised by: Dr. Raslan Mohammad

2025

Abstract

This study aimed to exploration the role of artificial intelligence in reducing the spread of cybercrimes: The performance of members of the security services was characterized by an intermediate variable. To achieve the objectives of the study, a descriptive analytical approach was adopted. The study population represented workers in the cybercrime unit in the Palestinian security services, which numbered (327) employees. Approximately, the size of the study sample was (178) and a random sample was selected Data were also analyzed using statistical software (SPSS).

The study reached a number of results, the most prominent of which were: The level of application of artificial intelligence among employees of the Cybercrime Unit of the Palestinian security services was high. The results revealed a high level of reduction in the spread of cybercrime among employees of the Cybercrime Unit of the Palestinian security services. The results also revealed a high level of performance excellence among employees of the Cybercrime Unit of the Palestinian security services. The results also indicated a mediator role for the excellence of performance between artificial intelligence (AI) in its various dimensions (machine learning, deep learning) in the Palestinian security services and the spread of cybercrime. The results also indicated a highly positive relationship between the excellence of performance of Palestinian security personnel and the prevalence of cybercrime in society, as perceived by employees of the Crime Control Unit. The results indicated a highly positive relationship between AI and the prevalence of cybercrime in society, and a moderately positive relationship between AI and the excellence of performance of Palestinian security personnel.

The study recommended a set of recommendations, the most important of which were: investing in modern AI technologies to enhance their capabilities to monitor and respond to crimes more effectively; improving coordination between various security units to enhance the effectiveness of efforts to combat cybercrime.

Keywords: Artificial intelligence, combating cybercrime, performance excellence, security personnel. .

الفصل الأول

الإطار العام للدراسة

1.1 مقدمة

2.1 مشكلة الدراسة

3.1 أسئلة الدراسة

4.1 أهداف الدراسة

5.1 أهمية الدراسة

6.1 فرضيات الدراسة

7.1 حدود الدراسة ومحدداتها

8.1 مصطلحات الدراسة

الفصل الأول
الإطار العام للدراسة

1.1 مقدمة:

يُعد الذكاء الاصطناعي فرعًا من علوم الحاسوب يركّز على تطوير أنظمة قادرة على محاكاة القدرات الذهنية البشرية في مجالات التعلم، التحليل، واتخاذ القرار. وقد أصبح هذا العلم محورياً في تعزيز قدرات الأجهزة الأمنية على مواجهة الجرائم الإلكترونية، إذ يمكن من خلاله تحليل البيانات واكتشاف الأنماط المشبوهة بكفاءة عالية.

كما يسهم تميز أداء منتسبي الأجهزة الأمنية في زيادة فعالية هذه الأنظمة؛ إذ يمكنهم اتخاذ قرارات مستندة إلى المعلومات والتحليلات التي يوفرها الذكاء الاصطناعي، ما يعزز القدرة على الحد من الجرائم الإلكترونية.

وكشفت السنوات الأخيرة النقاب عن تكنولوجيا متطورة، لم تكشفها عقود من الزمن، إلا أنه لم يرق لبعضهم أن يحسن استخدامها، حين أساء استخدامها وألحق الضرر بالآخرين، وإزاء ذلك يبرز دور كلٌ منا في محاربة هذه الجريمة وصد مرتكبيها، ولا سيما رجال القانون؛ إذ أنها تُعد تحدياً كبيراً أمامهم وذلك لاختلافها النوعي عن الجريمة التقليدية، فالمجرم الإلكتروني يسب ويسرق ويخرب ويقتل وهو في بيته ولم يغادر مكانه دون أن يبذل الكثير من الجهد (لخضر وناصري، 2018).

وأحرزت التكنولوجيا الذكية تقدماً في جميع مناحي الحياة محلياً ودولياً ووصول التكنولوجيا المعلوماتية لكافة فئات المجتمع ومؤسساته (عطايا، 2015)، وبالرغم مما أسهمت به هذه الطفرة العلمية في تحسين أساليب الحياة إلا أنه لا يمكن تجاهل ما استحدث من مشاكل مرافقة هذا التطور متمثلةً في ما يعرف

بالجريمة الإلكترونية التي تنوعت وتميزت بوسائلها وطرقها وأنواعها ما استدعى بالضرورة استحداث قوانين خاصة تعالج هذه الجرائم الحديثة لخطورتها من حيث طبيعتها وطرق إثباتها وتحقق أركانها والعقوبة الرادعة التي تضمن الاستخدام الآمن لشبكات المعلومات والقضاء الإلكتروني لجميع الفئات (الجبور وآخرون، 2020).

يعد الذكاء الاصطناعي من المصطلحات الحديثة ومن الميادين المهمة التي تسترعي اهتمام الباحثين والعلماء، ومع الانتشار المتسارع لاستخدام الذكاء الاصطناعي في شتى ميادين الحياة أصبحت تقنيات الذكاء الاصطناعي أكثر تطوراً في السنوات الأخيرة، وتلعب دوراً في المجتمع، وجرى استخدامها في مجالات مختلفة مثل المجالات الطبية والقانونية والعديد من المجالات الأخرى، ولعل أبرز تلك المجالات مواجهة الجرائم المستحدثة، لذلك يمكن لهذه التقنيات مواجهة خطر إلكتروني معين مثل الجرائم الالكترونية (الأخنش والعيداني، 2023).

وتُعَدُّ الجرائم الإلكترونية من أخطر الجرائم التي تواجه الأفراد والمؤسسات؛ كونها جرائم صامتة تتجاوز الحدود الجغرافية؛ إذ تستخدم شبكة الإنترنت وأجهزة الحاسوب في تنفيذ أعمال إرهاب إلكتروني واختراق وقرصنة البيانات، ومع ذلك لم تدم هذه الجريمة لفترة طويلة حتى ظهرت تقنية الذكاء الاصطناعي ذات المستوى العالي كحاجز لمكافحة الجرائم الإلكترونية، وبخاصة في الدول المتقدمة، فعن طريق السلطات الرقمية وتوقعات الجريمة قبل وقوعها ووسائل أخرى، أسهم الذكاء الاصطناعي بشكل كبير في مكافحة الجريمة الإلكترونية، وانقسمت التشريعات العربية بين من يعمل على تنظيم قوانين خاصة بالجرائم الإلكترونية وبين من قام بتعديل القوانين القديمة لمواكبة التطورات الحاصلة في مبدأ مشروعية مكافحة تلك الجرائم (قاسم، 2024).

بناءً على ما تقدم، فيتوجب على الدول الحرص على تطوير أنظمة المكافحة القانونية ضد الجرائم الإلكترونية، وذلك بإدخال نصوص تشريعية عقابية وإجرائية تتلاءم مع ظاهرة الإجرام الحديثة، وسن تشريعات خاصة ومستقلة في إطار إصلاح المنظومة التشريعية والقضائية، ومن أجل ضمان سرعة البحث والتحقيق في كشف الجرائم المستحدثة والقبض على المجرم المعلوماتي.

يرى الباحث أن دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية يمثل محورًا أساسيًا وذلك من تحسين أداء منتسبي الأجهزة الأمنية وتزويدهم بأدوات تحليل البيانات والتنبؤ بها. إذ أن دمج التقنيات الحديثة في مكافحة الجرائم الإلكترونية يعتبر خطوة استراتيجية نحو بيئة أكثر أمانًا. لذا هدفت هذه الدراسة لاستكشاف دور الذكاء الاصطناعي في الحد من انتشار الجرائم الالكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً

2.1 مشكلة الدراسة:

نظراً لعمل الباحث في الأجهزة الأمنية الفلسطينية، ونظراً لامتلاكه رؤية مباشرة لطبيعة التعامل مع تلك الجرائم وآليات مواجهتها، ومن خلال ملاحظاته، تبين أن وحدة الجرائم الإلكترونية تواجه تحديات مهنية في تنفيذ الإجراءات الخاصة بالجرائم الإلكترونية، فعلى الرغم من وجود العديد من الإجراءات التي تعالج بعض أنواع الجرائم الإلكترونية، إلا أن هناك أشكالاً لهذه الجرائم نظراً لتشعب تلك الأشكال من الجرائم نحتاج إلى تقنيات متطورة للحد منها، بالإضافة إلى ذلك، يتوجب اتباع إجراءات محددة للتحقيق في مثل هذه الجرائم من حيث صعوبة الكشف عنها، ومعاينها، وضبطها، وبخاصة فيما يتعلق بالأجهزة الإلكترونية. لذلك يمكن تلخيص مشكلة الدراسة في التساؤل الرئيس الآتي: **ما دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً؟**

وتنبثق منه التساؤلات الفرعية الآتية:

3.1 أسئلة الدراسة:

1.ما مستوى تطبيق الذكاء الاصطناعي في الجهاز الأمني الفلسطيني من وجهة نظر العاملين في وحدة مكافحة الجرائم؟

2.ما مستوى الحد من انتشار الجرائم الإلكترونية لدى العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية؟

3. ما مستوى تميز الأداء لدى العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية؟

4.هل هناك علاقة بين الذكاء الاصطناعي وانتشار الجرائم الإلكترونية في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم؟

5.هل هناك علاقة بين الذكاء الاصطناعي وتميز أداء العاملين في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم؟

6.هل هناك اختلاف في آراء العاملين في وحدة مكافحة الجرائم حول مستوى تطبيق الذكاء الاصطناعي ومستوى أداء العاملين في الجهاز الأمني الفلسطيني مستوى الجرائم الإلكترونية في المجتمع تبعاً لمتغيرات (الجنس، سنوات الخبرة، الرتبة العسكرية، المسمى الوظيفي)؟

4.1 أهداف الدراسة:

1. تعرف مستوى تطبيق تقنيات الذكاء الاصطناعي في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم.

2. قياس مستوى الحد من انتشار الجرائم الإلكترونية لدى العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية.
3. تحديد مستوى تميز الأداء لدى العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية.
4. الكشف عن طبيعة العلاقة بين الذكاء الاصطناعي وانتشار الجرائم الإلكترونية في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم.
5. تعرف العلاقة بين الذكاء الاصطناعي وتميز أداء العاملين في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم.
6. فحص الاختلاف في آراء العاملين في وحدة مكافحة الجرائم حول مستوى تطبيق الذكاء الاصطناعي ومستوى أداء العاملين في الاجهزة الأمنية الفلسطينية ومستوى الجرائم الإلكترونية في المجتمع تبعاً لمتغيرات الجنس، وسنوات الخبرة، والرتبة العسكرية، والمسمى الوظيفي.

5.1 أهمية الدراسة:

الأهمية النظرية: تتجلى الأهمية النظرية لهذه الدراسة في تقديم إطار معرفي غني حول موضوع الذكاء الاصطناعي وتميز أداء العاملين، إلى جانب تسليط الضوء على الجرائم الإلكترونية. تُعد الدراسة مصدراً علمياً يمكن للباحثين الاستفادة منه في تطوير دراسات مستقبلية، بالإضافة إلى اعتماد نتائجها لبناء رؤى وتصورات شاملة حول المتغيرات ذات الصلة التي قد تكون محورًا للدراسات المستقبلية.

الأهمية التطبيقية: تُسهم هذه الدراسة في تعزيز قدرة الأجهزة الأمنية الفلسطينية على مواجهة الجرائم الإلكترونية من خلال تطبيق تقنيات الذكاء الاصطناعي للتنبؤ بالجرائم واتخاذ قرارات استباقية. كما توفر إطاراً لتطوير كفاءة العاملين في تحليل البيانات والتعامل مع الأنظمة الذكية التي من شأنها مساعدة

صانعي القرار في وضع استراتيجيات أمنية حديثة تسهم في تحسين الأداء الأمني، وتعزيز سرعة الاستجابة، وبناء بيئة أكثر أماناً واستقراراً داخل المجتمع الفلسطيني.

6.1 فرضيات الدراسة:

1. لا توجد علاقة ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) بين تميز أداء العاملين في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم.
2. لا توجد علاقة ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) بين الذكاء الاصطناعي وانتشار الجرائم الإلكترونية في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم.
3. لا توجد علاقة ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) بين الذكاء الاصطناعي وتميز أداء العاملين في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم.
4. لا يوجد دور وسيط لتميز الاداء ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) بين الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية في المجتمع؟
5. لا تُوجَد فُرُوق ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) لمستوى تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تعزى لمتغير (الجنس، سنوات الخبرة، الرتبة العسكرية، المسمى الوظيفي).
6. لا تُوجَد فُرُوق ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) لمستوى تميز أداء العاملين في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تعزى لمتغير (الجنس، سنوات الخبرة، الرتبة العسكرية، المسمى الوظيفي).

7.1 حدود الدراسة ومحدداتها:

الحدود الزمنية: تم إجراء هذه الدراسة خلال العام الدراسي 2025م.

الحدود الموضوعية: اقتصرت هذه الدّراسة على تناول موضوع دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً.

الحدود المكانية: الأجهزة الأمنية الفلسطينية (وحدة مكافحة الجرائم).

الحدود البشرية: العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية (الاستخبارات العسكرية، الشرطة، المخابرات، الأمن الوقائي).

محدداتها:

- بسبب الظروف السياسية والاقتصادية التي أدت إلى الدوام بنظام الطوارئ، ما حد من الوصول إلى جميع أفراد مجتمع الدراسة.
- بعض أفراد العينة قد لا يمتلكون خبرة أو معرفة كافية بالذكاء الاصطناعي، ومن ثَمّ، فقد تكون إجاباتهم مبنية على تصور عام أكثر من تجربة عملية.

8.1 مصطلحات الدراسة:

الذكاء الاصطناعي: هو استخدام أنظمة وبرامج ذكية قادرة على تحليل البيانات الضخمة واكتشاف الأنماط غير الطبيعية وتحديد التهديدات الإلكترونية أو تنفيذ الهجمات بشكل آلي. يتم تقييمه بناءً على قدرته على تعزيز الأمن السيبراني أو استغلال الثغرات لتحقيق أهداف غير مشروعة.

أداء العاملين: هو قدرة العاملين على التفاعل بفعالية مع التكنولوجيا الحديثة وبخاصة الذكاء الاصطناعي، لمواجهة التحديات المرتبطة بالجرائم الإلكترونية. يشمل ذلك مهاراتهم في فهم الأنظمة الذكية، استخدامها بشكل صحيح، وتحليل المخاطر الأمنية، بالإضافة إلى الاستجابة السريعة والدقيقة للتهديدات لتحقيق الحماية الإلكترونية المطلوبة.

الجرائم الإلكترونية: هي الأنشطة غير القانونية التي تُنفَّذ باستخدام التكنولوجيا الرقمية والذكاء الاصطناعي لاستهداف الأفراد أو المؤسسات، سواء من خلال سرقة البيانات، التلاعب بالأنظمة، أو استغلال الثغرات الأمنية. ويتحدد التعامل مع هذه الجرائم بقدرة العاملين على استخدام التقنيات الذكية بشكل فعال، وتحسين أدائهم للكشف عن التهديدات، تقليل المخاطر، واستجابة سريعة ومبتكرة للحفاظ على الأمن السيبراني.

الفصل الثاني

الإطار النظري والدراسات السابقة

الإطار النظري

الدراسات السابقة

التعقيب على الدراسات السابقة

الفصل الثاني

الإطار النظري والدراسات السابقة

1.2 الإطار النظري:

تمهيد:

تناول الفصل الثاني الإطار النظري والدراسات السابقة، وقد قسم الباحث الإطار النظري إلى ثلاثة مباحث: المبحث الأول جرى الحديث فيه عن الذكاء الاصطناعي، والمبحث الثاني تحدث عن الجرائم الإلكترونية، أما المبحث الثالث فقد عرج الباحث على أداء الأجهزة الأمنية، أما الدراسات السابقة فقد قسمت إلى الدراسات المتعلقة بالذكاء الاصطناعي والجرائم الإلكترونية، ودراسات متعلقة بالأداء لمنتسبي الأجهزة الأمنية، واختم الفصل بالتعقيب على الدراسات السابقة.

المبحث الأول: الذكاء الاصطناعي

ارتبط الذكاء الاصطناعي بالأجهزة الرقمية والإلكترونية مثل الحواسيب، الهواتف الذكية، والروبوتات. يُشير مصطلح الذكاء الاصطناعي (AI) إلى الأنظمة أو الأجهزة التي تحاكي الذكاء البشري لأداء مهام معينة، وتستطيع تحسين أدائها استنادًا إلى المعلومات التي تجمعها. وقد أفادت الصحافة الرقمية من تقنيات الذكاء الاصطناعي، مثل الواقع الافتراضي، الواقع المعزز، الروبوتات المذيعة، وتقنيات التعلم العميق، وغيرها. (متولي وفرحات، 2022).

ويتوقع الخبراء أن يعزز الذكاء الاصطناعي المتصل بالشبكة من فعالية الإنسان، لكنه قد يهدد استقلاليته وقدراته أيضًا. قد تتساوى أجهزة الكمبيوتر مع الذكاء البشري أو تتفوق عليه في مهام مثل اتخاذ القرارات المعقدة، والاستدلال، والتعلم، والتحليلات المتقدمة. ستسهم الأنظمة الذكية في المجتمعات، والمركبات،

والمباني، والمرافق، والمزارع، والعمليات التجارية في توفير الوقت والمال والجهد، ما يمنح الأفراد فرصة للاستمتاع بمستقبل أكثر تخصصًا ورفاهية. ومع ذلك، تبرز مخاوف وتحديات تواجه المجتمعات بسبب النظام المعقد والمتزايد، بما في ذلك نسيج معلوماتي عالمي من البرامج والأجهزة المعتمدة على الذكاء الاصطناعي، التي يمكن اختراقها، بالإضافة إلى قواعد البيانات المتصلة، وأجهزة الاستشعار، والكاميرات، وغيرها (الدبيسي، 2021).

نشأة الذكاء الاصطناعي:

برز مفهوم الذكاء الاصطناعي بادئ ذي بدء من خلال نشر ورقة بحثية بعنوان (الآلات الحاسوبية والذكاء) من تأليف تورينج لاقتراح طرق تقييم ما إذا كانت الآلات قادرة على التفكير (Bozkurt, Aras and others, 2021)

وقام العالم مكارتي بتوسيع الفكرة من خلال مؤتمر عقد في جامعة دارتموت عندما استخدم مصطلح الذكاء الاصطناعي لوصف الحاسبات الآلية ذات المقدرة على أداء وظائف العقل البشري (خوالد، أبو بكر، 2019).

وبعد ذلك أخذ الذكاء الاصطناعي منحى جديد وأصبح يحتوي على خطوط بحث مختلفة في مجالات متعددة مثل (التعلم الآلي والمعلوماتية والنظام القائم على المعرفة والتعرف على الأنماط) وبذلك حافظ على تقدمه في بداية الثمانينيات. ومن ثم تطورت هذه المصطلحات المختلفة بمرور الوقت وجرى تصنيفها جميعها ضمن الذكاء الاصطناعي، وهو مصطلح عام شامل يشمل التطورات السابقة والحالية.

ومن المجموعات الفرعية للذكاء الاصطناعي:

1. **التعلم الآلي:** الذي نشأ من فكرة تعرف الأنماط وفكرة أن جهاز الحاسوب أو نظام آخر سيكون قادراً على التعلم دون تشفير لمهام محددة، والتعلم الآلي هو فرع من فروع الذكاء الاصطناعي يركز على تطوير خوارزميات ونماذج تتيح للآلات التعلم من البيانات وتحسين أدائها بمرور الوقت دون الحاجة إلى برمجة صريحة. يعتمد التعلم الآلي على تحليل البيانات واستخراج الأنماط والتوجهات منها، ما يمكِّن الأنظمة من اتخاذ قرارات أو إجراء تنبؤات بناءً على المعلومات المتاحة، وهو الكشف التلقائي عن التهديدات الذي يمنح الآلات القدرة على تحديد الأنماط والتنبؤات بأقل قدر من التدخل البشري لتعرف الصور المعقدة والنصوص وأنماط البيانات الأخرى لإنتاج رؤى وتوقعات دقيقة (Basha, 2019).

2. **التعلم العميق:** هو تطوير الشبكات العصبية الاصطناعية لاستخراج البيانات عالية الأبعاد، لاكتشاف الهياكل المعقدة، ولتحقيق أداء تنبؤي أفضل، والتعلم العميق (Deep Learning) هو أحد فروع الذكاء الاصطناعي (AI) والتعلم الآلي (Machine Learning)، ويعتمد على الشبكات العصبية الاصطناعية (Artificial Neural Networks) لمحاكاة طريقة تفكير الدماغ البشري في تحليل البيانات واتخاذ القرارات، وهو أحد أساليب الذكاء الاصطناعي الذي يعلم أجهزة الكمبيوتر بطريقة مستوحاة من الدماغ البشري للتعرف على الصور المعقدة والنصوص والأصوات وأنماط البيانات الأخرى لإنتاج رؤى وتوقعات دقيقة (Al-Marghilani, 2022).

أما في الوقت الحالي، فيجري استخدام خوارزميات (برمجيات) التعلم العميق والتعلم الآلي والذكاء الاصطناعي بشكل متكرر في ممارسة الموضوعات المذكورة أعلاه، وترتبط هذه المفاهيم ببعضها، ولكنها تختلف من حيث ميزات معينة. والشكل الآتي يوضح العلاقة بين الذكاء الاصطناعي والتعلم الآلي والتعلم العميق. (Bozkurt, Aras and others, 2021).

بناء على ما تقدم، فإنّ الباحث يرى أنّ المجموعات الفرعية للذكاء الاصطناعي تعدّ نهجاً يستخدم طبقات متعددة من الشبكات العصبية لاستخراج الميزات والأنماط من البيانات، ما يجعله قادرًا على التعامل مع البيانات الضخمة والمعقدة مثل الصور، الصوت، والنصوص. كلما زاد عدد الطبقات، زادت قدرة النموذج على التعلم من البيانات وتفسيرها بطريقة أكثر تعقيدًا

مفهوم الذكاء الاصطناعي:

الذكاء الاصطناعي هو العلم الذي يجعل الآلات تفكر مثل البشر، أي حاسوب له عقل، فالذكاء الاصطناعي له سلوكيات وخصائص معينة تتسم بها البرامج الحاسوبية تجعلها تحاكي القدرات الذهنية البشرية وأنماط عملها ومن أهم هذه الخاصيات القدرة على التعلم والاستنتاج، ورد الفعل على أوضاع لم تبرمج عليها الآلة (مكاوي، 2018، ص21).

ويمكن **تعريفه** بأنه: "جزء من علوم الحاسب الآلي الذي يهدف لمحاكاة قدرة معرفية لاستبدال الإنسان في أداء وظائف مناسبة في سياق معين تتطلب ذكاء"(العمري، 2021، ص309).

أما (Kaplan, Hanelein, 2019) فقد عرف الذكاء الاصطناعي على أنه قدرة النظام على تفسير البيانات الخارجية بشكل صحيح، والتعلم من هذه البيانات واستخدام تلك المعرفة لتحقيق أهداف ومهام محددة من خلال التكييف المرن.

عرف (Mccarthy, 2007) الذكاء الاصطناعي هو خصائص معينة وسلوك تتسم بها البرامج الحاسوبية تجعلها تحاكي القدرات الذهنية البشرية وأنماط عملها، ومن أهم هذه الخاصيات القدرة على التعلم والاستنتاج ورد الفعل على أوضاع لم تبرمج في الآلة.

وعرفه الباحث بأنه استخدام أنظمة وبرامج ذكية قادرة على تحليل البيانات الضخمة واكتشاف الأنماط غير الطبيعية وتحديد التهديدات الإلكترونية أو تنفيذ الهجمات بشكل آلي. يجري تقييمه بناءً على قدرته على تعزيز الأمن السيبراني أو استغلال الثغرات لتحقيق أهداف غير مشروعة.

أهمية الذكاء الاصطناعي:

تعتبر أهمية الذكاء الاصطناعي من خلال توفر عدد كبير من البرمجيات الجاهزة الموجهة لتعلم بمساعدة المعلم او لتعلم الذاتي والمعتمدة على تعلم الحاسوب باستخدام الأنترنت ومن ثمّ نقل المعرفة، وتوفر البرمجيات للمعلمين طرق تدريس ومهارات تساعد في تطويرهم، بالإضافة لإمكانية استخدامها للنقاش وتبادل آراء المعلمين والطالع على الأساليب التعليمية الحديثة، وكل هذا ينعكس على تطوير العملية التعليمية التعلمية ككل (سوالمة، 2022).

ويرى الباحث أن الذكاء الاصطناعي يقوم بحفظ الخبرات البشرية، وأدى تطور لغات البرمجة من خلال الذكاء الاصطناعي الى استخدام اللغات الطبيعية للإنسان؛ إذ تساعد الحواسيب الذكية في القيام بالمهام الصعبة التي تصعب على الأنسان وتساعد في صنع القرار بعيد عن التحيز والعنصرية والأحكام المسبقة.

أهداف الذكاء الاصطناعي:

من أهداف الذكاء الاصطناعي كما حددتها (إيمان، 2020):

1. تكرار الذكاء الإنساني
2. حل مشكلة المهام المكثفة للمعرفة.
3. عمل اتصال ذكي بين الإدراك والفعل.

4. تحسين التفاعل الاتصال الإنساني، الإنساني الحاسوبي، الحاسوبي.

5. تمكين الآلات من معالجة المعلومات بشكل أقرب لطريقة الأنسان في حل المسائل؛ بمعنى آخر المعالجة المتوازية؛ إذ يجري تنفيذ عدة أوامر في الوقت نفسه.

6. فهم أفضل لماهية الذكاء البشري عن طريق فك أغوار الدماغ حتى يمكن محاكاته، وهما يعملان ضمن قاعدة معروفة، تفيد أن الجهاز العصبي والدماغ البشري أكثر الأعضاء تعقيدا بشكل مترابط ودائم في تعرف الأشياء.

يرى الباحث أن أهداف الذكاء الاصطناعي تشمل تكرار الذكاء الإنساني، حل المهام المعقدة، تحسين التواصل بين البشر والآلات، وتمكين الآلات من معالجة المعلومات بطريقة تشبه البشر. كما تهدف لفهم الذكاء البشري من خلال دراسة الدماغ.

أنواع الذكاء الاصطناعي:

النوع الأول الذكاء الاصطناعي الضيق ويعنى الذكاء الذي يعمل وفق برمجة محددة ومعينة مسبقاً ولا يمكن تعديتها، مثل تصنيف البريد الإلكتروني كرسائل غير مرغوب فيها، أو أنه ليس عشوائياً (قاسم، 2024).

النوع الثاني: الذكاء الاصطناعي الواسع ويعني الذكاء الذي لديه القدرة على جمع المعلومات وتحليلها، ويمكن الشخص من اكتساب المهارات والقدرات والعمل بصفة مستقلة وذاتية ويؤدي إلى الدور الذي يقوم به الإنسان (رانا، 2022).

النوع الثالث: الذكاء الاصطناعي الفائق ويعنى الذي يفوق قدرات الإنسان وعرفه الفيلسوف نيك بوسترم في جامعة أكسفورد أنه فكر أذكى أو أفضل من العقول البشرية في جميع المجالات، وبما في ذلك الإبداع العلمي والحكمة العامة المهارات الاجتماعية (قاسم، 2024).

ويستنتج الباحث، أن الذكاء الاصطناعي الضيق يعمل وفق برمجة محددة ولا يتجاوزها، ما يجعله مناسبًا لمهام محددة مثل تصنيف البريد الإلكتروني. أما الذكاء الاصطناعي الواسع، فيتميز بقدرته على جمع وتحليل المعلومات، ما يمكّن الأنظمة من اكتساب المهارات والعمل بشكل مستقل. وأخيرًا، الذكاء الاصطناعي الفائق بأنه يتجاوز قدرات الإنسان؛ إذ يمكن أن يتفوق على العقل البشري في مجالات متعددة، بما في ذلك الإبداع والمهارات الاجتماعية.

خصائص الذكاء الاصطناعي:

من البرامج الذكية التي يتسم بها أي برنامج تعليم تحتوي على مجموعة من الخصائص وهي:

أ. **إمكانية تمثيل المعرفة:** إن برامج الذكاء الاصطناعي على عكس البرامج الإحصائية تحتوي على أسلوب لتمثيل المعلومات، إذ تستخدم هيكلة خاصة لوصف المعرفة، وهذه الهيكلة تتضمن الحقائق والعالقة بين هذه الحقائق والقواعد التي تربط هذه العلاقات، ومجموعة الهياكل المعرفية تكون فيما بينها قاعدة المعرفة، وهذه القاعدة توفر أكبر قدر ممكن من المعلومات عن المشكلة المراد إيجاد حلًا لها. أي يحتوي برنامج التعليم الذكي على نوعين من المعرفة: المعرفة التي تتعلق بموضع البرنامج الذي يدرس: وهي متغيرة تبعا لتغير البرنامج، المعرفة التربوية: وهي المعرفة المتعلقة بقواعد تدريس الموضوع، وهي ثابتة بكل مجال تخصصي (زايد، زموري، 2021).

ب. **استخدام الأسلوب التجريبي المتفائل:** من الصفات المهمة في مجال الذكاء الاصطناعي أن برامجها تقتحم المسائل التي ليس لها طريقة حل عامة معروفة، وهذا يعني أن البرامج التي تستخدم خطوات متسلسلة تؤدي إلى الحل الصحيح، ولكنها تختار طريقة معينة للحل تبدو جيدة، مع

الاحتفاظ باحتمالية تغيير الطريقة إذا اتضح أن الخيار الاول يؤدي إلى حل سريعاً (حسني، مقاتل، 2021).

ت. **قابلية التعامل مع المعلومات الناقصة:** قابلية تطبيقات الذكاء الاصطناعي على إيجاد بعض الحلول حتى لو كانت المعلومات غير متوافرة بأكملها في الوقت الذي يتطلب فيه الحل، وإن تبعات عدم تكامل المعلومات يؤدي إلى استنتاجات أقل واقعية، ولكن من جانب آخر قد تكون الاستنتاجات صحيحة (زايد، زموري، 2021).

ث. **القدرة على التعلم:** من الصفات المهمة للتصرف الذكي القابلية للتعلم من الخبرات والممارسات السابقة، إضافة إلى قابلية تحسين الأداء. (حسني، مقاتل، 2021).

ج. **قابلية الاستدلال:** وهي القدرة على استنباط الحلول الممكنة لمشكلة معينة من واقع المعطيات المعروفة والخبرات السابقة، وبخاصة المشكلات التي لا يمكن معها استخدام الوسائل التقليدية المعروفة للحل، هذه القابلية تتحقق على الحاسوب بتخزين جميع الحلول الممكنة، إضافة إلى استخدام قوانين أو استراتيجيات الاستدلال وقوانين المنطق (سالمي، وكمال، 2020).

ح. **معالجة اللغة الطبيعية:** من الخصائص المميزة لبرنامج التعلم الذكي التفاعل عن طريق اللغة الطبيعية للمستخدم، فجودة التواصل بين البرنامج والمتعلم تتحسن بشكل ملحوظ إذا استطاع البرنامج أن يفهم مدخلات لغة المتعلم الطبيعية سواء أكانت مكتوبة أم منطوقة، فتنمي الحوار الفعال، وتشخص أخطاء المتعلم على التقدم في معالجة اللغة الطبيعية، وتساعد على فهم اللغة وإنتاجها (حسني، مقاتل، 2021).

من خلال ما سبق تتميز برامج الذكاء الاصطناعي بعدة خصائص، منها إمكانية تمثيل المعرفة من خلال هيكلة خاصة تضم الحقائق والقواعد، واستخدام الأسلوب التجريبي المتفائل لحل المسائل المعقدة. كما أنها قادرة على التعامل مع المعلومات الناقصة وتقديم حلول رغم عدم اكتمال البيانات، بالإضافة إلى القدرة على التعلم من الخبرات السابقة والاستدلال لحل المشكلات. وأخيرًا، تتميز بمعالجة اللغة الطبيعية، مما يحسن التفاعل بين البرنامج والمتعلم.

استخدامات الذكاء الاصطناعي:

يوجد العديد من استخدامات الذكاء الاصطناعي في مجموعة متنوعة من المجالات، من بينها التي ذكرها (باعشن، 2011).

1. استخدام الذكاء الاصطناعي في المراقبة على أنظمة الحاسبات.
2. استخدام الذكاء الاصطناعي في تخزين البيانات وأنظمة الحفظ.
3. استخدام الذكاء الاصطناعي في جدولة الأعمال.
4. استخدام الذكاء الاصطناعي في إدارة الأزمات.
5. استخدام الذكاء الاصطناعي في تشكيل وتعديل نظام المعلومات.
6. استخدام الذكاء الاصطناعي في تدريب العاملين.

يرى الباحث من خلال تطبيق الذكاء الاصطناعي في المراقبة على أنظمة الحاسبات، يمكن للأجهزة الأمنية الكشف عن الأنشطة المشبوهة في الوقت الفعلي، كما يسهم في تخزين البيانات الحد من الجريمة الإلكترونية، وكذلك يسهل تحليل المعلومات بسرعة وكفاءة، ويمكن استخدام الذكاء الاصطناعي في

جدولة الأعمال وتدريب العاملين، مما يعزز من أداء منتسبي الأجهزة الأمنية، ومن ثمّ، يمثل الذكاء الاصطناعي متغيرًا وسيطًا حيويًا في تعزيز القدرات الأمنية والحد من انتشار الجرائم الإلكترونية.

الهندسة الاجتماعية:

تعد الهندسة الاجتماعية مفهوماً حديثاً يشير إلى استخدام التكنولوجيا والوسائط الرقمية لتحقيق أهدافاً اجتماعية محددة، وتتضمن الهندسة الاجتماعية تصميم وتنظيم الفضاء الرقمي والتلاعب بالمعلومات والتفاعلات الاجتماعية بهدف تحقيق تأثيرات معينة على المجتمع، ويتم استخدام الهندسة الاجتماعية في العديد من المجالات مثل: التسويق والسياسة والترفيه، والتعليم، إلخ (العمري والعمري، 2024).

وقد عرفها صاحب كتاب الهندسة الاجتماعية "فن اختراق البشر" بأنها: فعل التلاعب بالشخص لاتخاذ إجراء معين قد يكون أو لا يكون في مصلحته، ويمكن أن يشمل الحصول على المعلومات حق الوصول للهدف لاتخاذ إجراءات معينه (Christopher, 2017).

ومن الناحية الاجتماعية فإن الهندسة الاجتماعية تعرف بأنها التأثير في مجمل السلوك لاجتماعي ونمط الحياة والتفكير للمجتمع برمته، بحيث يسعى المهندس الاجتماعي في هذه الحالة إلى تعيير سلوك الأفراد وطريقة تصرفاتهم وأسلوب تفكيرهم، من أجل الوصول إلى الهدف الذي يرنوا إليه (آل محيا ومكين، 2025).

يسعى المهندس الاجتماعي من خلال استخدامه العديد من الأساليب الاحتيالية إلى الوصول إلى الهدف المنشود، وهو الحصول على المعلومات السرية أياً كان نوعها. وهنا يأتي دور الهندسة الاجتماعية في عملية اختراق الأجهزة من خلال عدد من أساليب الاحتيال عن طريق شخص يسمى (مهندس اجتماعي يتمتع بمهارات اجتماعية وتقنية عالية، بالإضافة إلى قدرته على التمثيل وإقناع الضحية بشكل غير

مباشر بشتى الطرق للوصول إلى المعلومات المطلوبة وتختلف الطرق المستخدمة في الهندسة الاجتماعية التي منها على سبيل المثال: أن المهندس الاجتماعي قد ينتحل شخصية موظف بنك ويقوم بالاتصال على أحد عملاء البنك وبطريقته الخاصة يحصل على جميع البيانات البنكية، وهذه الطريقة تعتبر منتشرة بكثرة وأغلب الضحايا هم من كبار السن. أيضا قد ينتحل شخصية عامل صيانة أجهزة وشبكات حاسب الى أو يعمل بشكل مؤقت في إحدى الشركات ويختلط بالموظفين الذين لديهم صلاحيات الدخول الأنظمة المنشاة (آل محيا ومكين، 2025).

فأساليب الهندسة الاجتماعية القائمة على أساس تقني منها:

الاحتيال الإلكتروني: يشير مفهوم الاحتيال الإلكتروني إلى تلقي رسالة عبر البريد الإلكتروني من موقع احتيالي يحمل صفة شركة ائتمانية أو بنك ويشابه تماماً الموقع الرسمي وتحتوي الرسالة على رابط للتحقق من بيانات الشخص الضحية كاسم المستخدم وكلمة السر، ثم تنقل الضحية إلى الصفحة الرئيسة للموقع الأساسي بعد أن جرى الحصول على بياناته الشخصية (محمد، 2018).

الاحتيال الصوتي، ويتم هذا النوع من الاحتيال عندما يجري المحتالون اتصالاً ما، ببعض الأشخاص الذين يمثلون الضحايا دون سابق إنذار، يدّعون فيه حدوث عملية احتيال أو قرب حدوثها، ويكون لديهم بعض المعلومات المتعلقة بالشخص المتصل به، وقد يتظاهرون بأنهم من موظفي أحد البنوك أو غيرهم من الموظفين لدى المؤسسات الأخرى التي تحظى بالثقة، ومن ثم يحاولون إقناع الشخص بتحويل بعض المال، أو سحب النقد وتسليمه، أو الإفصاح عن معلومات أو بيانات سرية خاصة، قد تستخدم فيما بعد للوصول إلى الموارد المالية للضحية أو حساباته البنكية (العمري والعمري، 2024).

الرسائل الاقتحامية المزعجة هي رسائل إلكترونية بعناوين مشوقة للقراءة مثل تهنئة من صديق، أو تأكيد بيع أو غيرها وبداخل تلك الرسائل ما يسبب تدمير الجهاز وسرقة معلوماته، ومن هنا، فإن الرسائل

الاقتحامية المزعجة عبارة عن رسائل يحصل من خلالها استدراج الضحية إما لفتح رابط يحتوي على فيروسات أو الوصول المعلومات من الضحية، فهي تركز على الجانب العاطفي للشخص لفتح المرفقات التي تتضمن الرسالة (محمد، 2018).

لذلك تعتمد الهندسة الاجتماعية على التلاعب بالسلوك البشري للحصول على معلومات حساسة. ويستخدم المهندسون الاجتماعيون تقنيات متعددة، مثل الاحتيال الإلكتروني والاحتيال الصوتي، لاستدراج الضحايا وكسب ثقتهم، لذلك للتقنيات الذكية دور في تحليل البيانات واكتشاف الأنماط المشبوهة بسرعة باستخدام الذكاء الاصطناعي في المراقبة على الأنظمة الإلكترونية، ويمكن للأجهزة الأمنية تعرف محاولات الاختراق قبل وقوعها، كما أن تحليل البيانات الكبيرة يمكن أن يساعد في تحديد الاتجاهات السلوكية المرتبطة بالجرائم الإلكترونية.

المبحث الثاني: الجرائم الإلكترونية:

أن ظهور الأجهزة الإلكترونية والانترنت يعتبر ذو خطورة عالية خاصة في ظل انتشار الجريمة الإلكترونية المنظمة، التي تتجاوز حدود الدول، ويمكن اختراقها ونشر المعلومات الخاصة بها وأخذها ويمكن أن تصل إلى مجاوزة مستوى خصوصية حياة الأفراد، وإن أغلب عملية الاغتيالات والاحتيال والنصب والسرقة تتم عن طريق أجهزة الحاسوبية والانترنت.

مفهوم الجرائم الإلكترونية:

الجرائم لغةً اشتقت من الجرم، وتعني الذنب أو التعدي، وعرفت الشريعة الإسلامية الجريمة بأنها إيتان فعل محرم معاقب على فعله، أو ترك معاقب تركه، وله جزاء عاجل في الدنيا وجزاء أجل في الأخرة، أما الجريمة فقهاً عرفها الفقيه جارو هي كل فعل أو ترك يعاقب عليه القانون بعقوبة جنائية ولا يبرره استعمال حق ولا أداء واجب(الحلبي، 2011، ص27).

مفهوم الجرائم الإلكترونية شرعيا: عرفها حجازي، (2007) هي جريمة ترتكب باستخدام الأجهزة الحاسوبية أو الشبكة أو تقع على المنظومات المعلوماتية أو الشبكة وقد أكدت التعليمات التوضيحية والتنفيذية لهذا القانون على هذه المعيار.

والمشرع الفلسطيني عرفها أنها سلوك إنساني يرتكب بواسطة حاسب آلي، إخلالًا بقواعد القانون الجنائي يترتب عليها المساس بمصلحة يحميها الشارع ويوقع القضاء بحكم قضائي بات على مرتكبه الجزاء المناسب (إيمان، 2020).

مفهوم الجرائم الإلكترونية فقهياً وهي السلوك الإجرامي الذي يرتكب عبر الفضاء الإلكتروني بالاستعانة بالخدمات المعلوماتية المضافة لجهاز الهاتف المحمول سواء باستخدام شبكة الإنترنت أو شبكة اتصال الهاتف (أحمد، 2015)

وعرف صالح (2023) الجرائم الإلكترونية على أنها الاعتداء القانوني الذي يرتكب بوساطة المعلومات الحاسوبية بغرض تحقيق الجريمة.

ويرى الباحث أن الجرائم الإلكترونية هي الأنشطة غير القانونية التي تُنفَّذ باستخدام التكنولوجيا الرقمية والذكاء الاصطناعي لاستهداف الأفراد أو المؤسسات، سواء من خلال سرقة البيانات، التلاعب بالأنظمة، أو استغلال الثغرات الأمنية. ويتحدد التعامل مع هذه الجرائم بقدرة العاملين على استخدام التقنيات الذكية بشكل فعال، وتحسين أدائهم للكشف عن التهديدات، تقليل المخاطر، واستجابة سريعة ومبتكرة للحفاظ على الأمن السيبراني.

أنواع الجرائم الإلكترونية:

من الأنواع الشائعة للجرائم الإلكترونية كآلاتي:

1.الاحتيال المالي

وهي الجرائم الماسة في حق الأفراد والمؤسسات بجميع أنواعها ويهدف المجرمون في ذلك إلى جني الأموال الطائلة من خلال الابتزاز الذي يمارس على الأفراد والمؤسسات، وإن جرائم الابتزاز الواقعة على الأفراد ويمكن تأثيرها أن يمتد إلى أمن المجتمع خاصة في المجتمعات القبلية التي ترى أن العار لا يمكن إلا أن يكون في الانتقام له من خلال الدم، وتتشكل الخطورة بشكل أكبر عند استخدام هذه الجرائم ضد الشركات العملاقة الكبرى، والمؤسسات المالية فتسبب لها ضررً كبيراً في عندما تهاجم أنظمة حكومية

يخلف ذلك ضرر بالغ في الاقتصاد القومي لبعض الدول وممارسة التجسس الصناعي والعسكري وتخريب المعلوماتي ينعكس أثره على المجتمع وتعد جرائم تزوير البيانات أكثر الجرائم شيوعاً من بين الجرائم الإلكترونية ويتم ذلك من خلال الدخول إلى قاعدة البيانات الموجودة ويتم من خلال تعديل البيانات حيث الإلغاء أو الإضافة ويمكن إلى دول الاستعمال والاحتلال ممارسة الجرائم بطريقة بشعة من خلال استخدمها في صنع المتفرجات وتفجيرها عن بعد(عبد الحليم، 2014).

2. سرقة البيانات

سرقة البيانات والمعلومات والاعتداء على خصوصيتها وإساءة استخدامها وتحريف السجلات الرسمية، وسرقة المعلومات وبيعها كالبحوث أو الدراسات ذات العلاقة بالتطور التقني أو الصناعي أو العسكري، وتعتبر من الجرائم الإضرار بالبيانات من أخطر الجرائم التي قد تؤثر في المؤسسات وتشمل الأنشطة كتعديل أو محو أو سرقة أو إتلاف البيانات ويرتكب تلك الجرائم أشخاص محترفون يطلق عليهم مصطلح المحترفون ذوو القبعات السوداء، ويقومون بذلك من أجل الاستفادة المالية وقد تكبدت المؤسسات خسارة مالية كبيرة (البداينة، 2014).

3. انتهاك الخصوصية

تحصل هذه الجرائم عبر المس بشخصية المجني عليه، وتسمى بجرائم الإنترنت الشخصية، مثل: جريمة سرقة الهوية أو التنصت أو سرقة الاشتراك في موقع شبكات الإنترنت، كذلك تحصل من خلال الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات الشخصية للأفراد، أو الاطلاع عليها، أو حذفها، أو تغييرها بما يحقق هدف المجرم، وأكثر ما يتعرض له الأشخاص هو الاعتداء على حرمة المراسلات الخاصة التي تتعدد في الفتح والاخفاء والاختلاس والتعدي أو إفشاء الأسرار وتعتبر من أقوى الوسائل التي يتبعها منفذ الجريمة الإلكترونية وهي الاتخاذ من رسائل البريد الإلكتروني فرصة للإيقاع بالضحايا

والتي يتم إرسال الملايين منها يومياً شأنها شأن بقية وسائل التواصل الأخرى، ومن أشهر الجرائم المرتبطة بالبريد الإلكتروني هي جرائم إرسال الفيروسات والتهكير والتشهير والغش وغير ذلك (العجمي، 2014).

4.نشر الشائعات والبيانات المضللة

في عصر الرقمنة أصبحت الأخبار الكاذبة تمثل تحدياً كبيراً يواجه المجتمعات والأفراد على المستوى العالمي، وأسهمت الوسائل الإلكترونية بالإسراع في عملية انتشارها، ما أدى إلى التأثير وبشكل سلبي على الثقة بالمعلومات وهي شكل من أشكال التهديد للاستقرار الاجتماعي والسياسي، ووصفت الإشاعة بأنها المعلومات أو الأخبار التي يصعب التحقق من صحتها أو كذبها، ولكن تحمل أهمية خاصة بالنسبة للأشخاص الذين يستقبلونها، وتنتشر بسرعة بين المهتمين، وغالباً ما يتم نشرها في أوقات حرجة ويكون لها تأثير عميق (القرالة، 2024).

ويستنتج الباحث أن الجرائم الإلكترونية تُعد من أبرز نتائج التطور التكنولوجي الحديث، ولم تَعُد تقتصر على الأفراد، بل باتت تهدد المؤسسات والدول وتسبب أضراراً اقتصادية وأمنية واجتماعية. وقد سهّل الانتشار الواسع للتقنيات الرقمية تنفيذ هذه الجرائم وزيادة تأثيرها. لذلك، جرى التطرق الى الجرائم الإلكترونية بأنواعها وأبعادها، بهدف توضيح مخاطرها المتصاعدة وأهمية التوعية بطرق الوقاية منها في عصر رقمي سريع التغير.

خصائص الجرائم الإلكترونية:

هناك مجموعة من الخصائص الإلكترونية أهمها:

- جريمة عابرة للحدود: يعتبر من الجرائم عابر للحدود، ولا يعترف فيها ويمكن أن تمتد إلى أكثر من دولة ما ينمي قضايا عدة مثل الاختصاص والإجراءات والتحري (مرابطي، 2023).

- جريمة صعبة الاكتشاف والإثبات: فتتميز هذه الجريمة في صعوبة بالغة في اكتشافها، وإذا اكتشفت من محض الصدفة؛ لأن مرتبكها لم يترك في الغالب أي أثر خارجي مرئي أو قيام الجاني بتدمير الدلائل (مسعود، 2021).

- جريمة ناعمة: تُصنف الجرائم الإلكترونية كجرائم "ناعمة" لأنها لا تتضمن عنفًا جسديًا أو تأثيرًا مباشرًا على الأشخاص. بدلاً من ذلك، تستهدف هذه الجرائم المعلومات والبيانات، ما يجعلها أقل وضوحًا وأكثر تعقيدًا في التعريف والمواجهة (ممدوح، 2021).

- قلة الإبلاغ عن الجريمة: تُعد قلة الإبلاغ عن الجرائم الإلكترونية من المشكلات الرئيسية التي تواجه سلطات إنفاذ القانون. العديد من الضحايا قد يشعرون بالخوف من الإبلاغ عن الجريمة أو يعتقدون أن الأمر لن يُحل، مما يؤدي إلى عدم تسجيل هذه الجرائم بشكل دقيق (مرابطي، 2023).

- طرق مواجهة الجرائم الإلكترونية: لمواجهة الجرائم الإلكترونية، يجب تعزيز الوعي بالأمان السيبراني وتوفير التدريب اللازم للأفراد والمؤسسات. كما ينبغي تحسين التعاون بين الجهات الحكومية والشركات الخاصة لمشاركة المعلومات حول التهديدات والجرائم (مرابطي، 2023).

- جريمة عدم وجود مفهوم مشترك للجريمة المعلوماتية تعتبر الجرائم المعلوماتية موضوعًا؛ إذ لا يوجد مفهوم مشترك حول تعريفها. وهذا يعيق جهود مكافحة هذه الجرائم، إذ تختلف القوانين والتشريعات من دولة إلى أخرى (بونعارة، 2015).

- وقوع الجريمة المعلوماتية في أثناء المعالجة الآلية للبيانات؛ إذ يستغل الجناة الثغرات في الأنظمة للحصول على معلومات حساسة أو إلحاق الضرر بالبيانات (منخرفيس، 2023).

- الجريمة الإلكترونية جريمة مستحدثة: تُعتبر الجرائم الإلكترونية من الجرائم المستحدثة في العصر الحديث، نتيجة للتطور التكنولوجي السريع. ومع تزايد الاعتماد على التكنولوجيا، تزداد أيضًا الفرص للجريمة، ما يتطلب استراتيجيات جديدة لمكافحتها (مسعود، 2021).

وبين الباحث أن الجرائم الإلكترونية تتميز بعدة خصائص، منها كونها جرائم عابرة للحدود وصعبة الاكتشاف والإثبات؛ إذ غالبًا ما تترك الجريمة آثارًا خفية. كما تُصنف كجرائم "ناعمة" تستهدف المعلومات بدلاً من الأشخاص، ما يجعل الإبلاغ عنها أقل شيوعًا. بالإضافة إلى ذلك، تفتقر الجرائم المعلوماتية إلى مفهوم مشترك، ما يعقد جهود مكافحتها في ظل التقدم التكنولوجي المستمر.

طرق الحد من الجرائم الإلكترونية:

من أهم طرق الحد من الجرائم الإلكترونية ما يأتي:

الشرطة الاستباقية:

تُعنى الشرطة الاستباقية بردع الجريمة من خلال استباق الأحداث، وذلك بالاعتماد على الأدلة والبيانات المتاحة. تشمل هذه الإجراءات تفعيل الأجهزة الأمنية من خلال تحليل المعلومات المتعلقة بالجرائم والتهديدات المحتملة.

وتعتبر البيانات التي يجري جمعها من المصادر المختلفة أداةً فعالة في مكافحة الجريمة. كما تلعب التكنولوجيا الحديثة دورًا حيويًا في تحسين كفاءة هذه العمليات، ما يُسهم في تعزيز السلامة العامة وتقليل

معدلات الجريمة، ومن المهم أن توفر هذه الإجراءات للجهات الأمنية القدرة على التصرف بسرعة وفعالية، ما يُساعد في التصدي للجرائم قبل وقوعها (إبراهيم، 2020).

الشرطة الرقمية:

تُعنى الشرطة الرقمية بتوظيف الأجهزة التكنولوجية لمراقبة الأنشطة الإجرامية في مختلف المجالات. يعتمد رجال الشرطة على الاستفادة من الأدلة الرقمية المتاحة، مثل البيانات الموجودة في الأجهزة الإلكترونية والرسائل المشفرة، بما في ذلك رسائل البريد الإلكتروني ووسائل التواصل الاجتماعي، وتتطلب مواجهة الجرائم الإلكترونية استخدام تطبيقات الذكاء الاصطناعي، ما يبرز أهمية وجود إطار قانوني ينظم العمل في هذا المجال. تساعد هذه التطبيقات في تحليل البيانات بشكل فعال، ما يسهل تعرف الأنماط الإجرامية وتوقع الجرائم قبل حدوثها (إبراهيم، 2020).

التحقيقات الرقمية

تُعنى التحقيقات الرقمية بتحسين كفاءة الأدلة الجنائية باستخدام التقنيات الحديثة لجمع وتحليل البيانات من مصادر متنوعة مثل الملفات الرقمية والرسائل الإلكترونية. تلعب هذه التقنيات دورًا أساسيًا في تحسين جودة الأدلة المقدمة في المحاكم، ما يتطلب تفعيل إجراءات قانونية مناسبة لضمان استخدامها الفعّال. كما يُعد التعاون بين الأجهزة الأمنية والتقنيات الحديثة ضروريًا لرفع كفاءة مكافحة الجريمة، مع توفير بنية تحتية رقمية متطورة لضمان سلامة المعلومات وسرعة الوصول إليها، ما يُسهم في تحقيق نتائج إيجابية في التحقيقات (إبراهيم، 2020).

وبناء على ما تقد، فقد توصل الباحث إلى أن طرق الحد من الجرائم الإلكترونية تتمثل في استخدام الشرطة الاستباقية لتحليل البيانات والتصدي للجرائم قبل وقوعها، بالإضافة إلى توظيف الشرطة الرقمية

لمراقبة الأنشطة الإجرامية من خلال الأدلة الرقمية وتطبيقات الذكاء الاصطناعي. كما تُعزز التحقيقات الرقمية كفاءة الأدلة الجنائية عن طريق جمع وتحليل البيانات بشكل فعال، ما يتطلب تفعيل إجراءات قانونية مناسبة وتعاون بين الأجهزة الأمنية والتقنيات الحديثة.

تناول الباحث فيما سبق مفهوم الذكاء الاصطناعي، مشيرًا إلى ارتباطه بالأجهزة الرقمية وقدرته على محاكاة الذكاء البشري لأداء مهام معينة، ما يعزز فعالية الأفراد في مجالات متعددة. كما جرى استعراض أنواع الذكاء الاصطناعي، بما في ذلك الضيق والواسع والفائق، وأبرز خصائصه مثل القدرة على التعلم ومعالجة اللغة الطبيعية. وناقش البحث أيضًا الهندسة الاجتماعية كأداة تستخدم في الجرائم الإلكترونية، مع عرض أساليب الاحتيال المختلفة مثل الاحتيال الإلكتروني والاحتيال الصوتي. كما جرى تعريف الجرائم الإلكترونية وأنواعها، مثل الاحتيال المالي وسرقة البيانات، مع الإشارة إلى خصائصها المتمثلة في كونها عابرة للحدود وصعبة الاكتشاف. وأخيرًا، جرى تقديم طرق للحد من هذه الجرائم، مثل الشرطة الاستباقية والتحقيقات الرقمية، التي تعتمد على التكنولوجيا الحديثة لتحسين الأمن السيبراني.

المبحث الثالث: الأداء لمنتسبي الأجهزة الأمنية:

أعطي كل من العلماء والإداريين والباحثين اهتمام في موضوع أداء العاملين للعلاقة الوطيدة؛ إذ تربط الموظف بالمنظمة وتأثير الموظف في منظمته بالرجوع إلى سلوكه وأدائه وقدراته ومهاراته، فتسعى المنظمة إلى الارتقاء بموظفيها من خلال التدريب والتأهيل والتحفيز والتقييم والنظر في حاجاتهم المادية والمعنوية (Chiang, sun& walkup, 2018).

مفهوم أداء العاملين:

وهي المخرجات والأهداف التي تسعى المنظمة في تحقيقها عن طريق العاملين فيها، فمفهوم أداء العاملين يعكس كلا من الأهداف التي تسعى المنظمات إلى تحقيقها عن طريق مهام وواجبات يقوم بها العاملين داخل المنظمة (هلسه، 2020).

وأداء العاملين هو تنفيذ الموظف لأعماله ومسؤولياته التي تكلفه بها المنظمة أو الجهة التي ترتبط وظيفته بها. أي أن الأداء هو محصلة النتائج والمخرجات التي حققها الفرد نتيجة الجهد المبذول من خلال قيام الفرد بالمهام والواجبات والمسؤوليات الموكلة إليه (أبو حميد، 2020).

ويعتبر مفهوم الأداء من المفاهيم الواسعة التي تنطوي على العديد من المصطلحات المتعلقة بالنجاح والفشل، واختلط العديد من الكتاب والباحثين في مجال الموارد البشرية بين المصطلح أداء العاملين والمصطلحات أخرى مرادفة تستخدم في ادبيات نظريات الإدارة مثل الإنتاجية، والكفاءة، والفاعلية، وذلك إلى جانب لفظ الكفاءة الإنتاجية أو الكفاءة الأداء (سعيد، 2018).

ويرى الباحث أن أداء العاملين يتمثل في القدرة العاملين على التفاعل بفعالية مع التكنولوجيا الحديثة وبخاصة الذكاء الاصطناعي، لمواجهة التحديات المرتبطة بالجرائم الإلكترونية. يشمل ذلك مهاراتهم في

فهم الأنظمة الذكية، استخدامها بشكل صحيح، وتحليل المخاطر الأمنية، بالإضافة إلى الاستجابة السريعة والدقيقة للتهديدات لتحقيق الحماية الإلكترونية المطلوبة.

أهمية أداء منتسبي الأجهزة الأمنية:

تكمن أهمية أداء منتسبي الأجهزة الأمنية في:

حماية الأمن الوطني: يُعد الأداء الفعّال لمنتسبي الأجهزة الأمنية أحد الركائز الأساسية للحفاظ على الأمن الوطني. فهم مسؤولون عن مواجهة التهديدات الداخلية والخارجية، ما يسهم في استقرار الدولة وسلامة المواطنين (عقل، 2022).

التحقيق في الجرائم: يُسهم الأداء المهني لمنتسبي الأجهزة الأمنية في سرعة وكفاءة التحقيقات الجنائية. ذلك يساعد على كشف الجرائم وتقديم الجناة إلى العدالة، مما يعزز الشعور بالأمان في المجتمع، وتطبيق القانون والنظام: يلعب منتسبو الأجهزة الأمنية دورًا حاسمًا في تطبيق القوانين والنظم؛ إذ أن أداءهم الجيد يضمن عدم انتهاك الحقوق والحريات، مما يساهم في بناء مجتمع عادل ومنظم (الدرابيع، 2023).

تعزيز الثقة العامة: عندما يتمتع أفراد الأجهزة الأمنية بأداء عالٍ، يزداد مستوى الثقة بين المواطنين والسلطات. هذه الثقة تُعزز من التعاون بين المجتمع والأجهزة الأمنية، ما يسهم في تحقيق الأمان الشامل، والاستجابة السريعة للطوارئ: يمتلك المنتسبون المهارات اللازمة للاستجابة السريعة والفعّالة في حالات الطوارئ. أداؤهم الجيد يمكن أن يحدث فرقًا كبيرًا في إنقاذ الأرواح وتقليل الأضرار خلال الأزمات (عقل، 2022).

التدريب والتطوير المستمر: يتطلب الحفاظ على مستوى عالٍ من الأداء التزامًا بالتدريب والتطوير المستمر. ذلك يمكن المنتسبين من مواكبة التغيرات والتحديات الأمنية الجديدة، ما يضمن فعالية واستدامة الأمن (الدرابيع، 2023).

يرى الباحث أن أداء منتسبي الأجهزة الأمنية يُعتبر أساسيًا لحماية الأمن الوطني وتعزيز الثقة العامة بين المواطنين والسلطات، ما يسهم في تحقيق الأمان الشامل. كما يلعبون دورًا حاسمًا في التحقيق في الجرائم وتطبيق القوانين، ويتطلب الحفاظ على كفاءتهم التزامًا بالتدريب والتطوير المستمر لمواجهة التحديات الأمنية الجديدة.

مكونات أداء منتسبي الأجهزة الأمنية:

يتكون أداء العاملين في الأجهزة الأمنية من الآتي (جيدول واعمر، 2019)

1. **الكفاية:** تعني العمل بكفاءة دون إهدار الموارد، سواء أكانت مادية، مالية، بشرية، أم معلوماتية. لذلك، فإن الإدارة الناجحة هي التي تتجنب المواقف التي قد تؤدي إلى فقدان موارد المؤسسة.
2. **الفاعلية:** تشير إلى مدى تحقيق الأهداف المرسومة. على سبيل المثال، من الأهداف التي يمكن وضعها والسعي لتحقيقها: زيادة الأرباح، توسيع سوق العمل، وتحقيق رضا العاملين.
3. **الإنتاجية:** تعكس قدرة المنظمة على تحقيق أكبر عدد من الأهداف باستخدام أقل قدر من الموارد. إذا تمكنت المنظمة من تحقيق أهدافها بموارد متاحة، فإنها تعتبر منظمة فعالة. وعندما تحقق الكفاءة والفاعلية معًا، تصبح المنظمة منتجة.
4. **الأهداف:** هي ما تسعى المنظمة لتحقيقه، ويجب أن تتضمن خطتها قائمة من الأهداف التي تهدف إلى إنجازها، وقد تكون هذه الأهداف استراتيجية.

يرى الباحث أن أداء العاملين في الأجهزة الأمنية يتشمل الكفاية التي تعني العمل بكفاءة دون إهدار الموارد، والفاعلية التي تشير إلى مدى تحقيق الأهداف المرسومة. بالإضافة إلى ذلك، تعكس الإنتاجية قدرة المنظمة على تحقيق الأهداف باستخدام أقل قدر من الموارد، بينما تُحدد الأهداف ما تسعى المنظمة لتحقيقه من خلال خطط استراتيجية واضحة.

معايير أداء منتسبي الأجهزة الأمنية:

أداء منتسبي الأجهزة الأمنية يُعدّ من العناصر الأساسية التي تسهم في استقرار المجتمع وحمايته. يتطلب هذا الأداء تحقيق عدة معايير، مثل (أبو حميد، 2020):

أ- الاحترافية والكفاءة: يجب أن يمتلك أفراد الأجهزة الأمنية المهارات اللازمة والمعرفة الكافية لأداء مهامهم بكفاءة عالية، سواء في حفظ الأمن أو في التعامل مع الحالات الطارئة.

ب- الالتزام بالقانون: من الضروري أن يلتزم منتسبو الأجهزة الأمنية بالقوانين المحلية والدولية، مع احترام حقوق الإنسان، مما يعزز ثقة المجتمع فيهم.

ت- الاستجابة السريعة: القدرة على التحرك بسرعة وفعالية في الأوقات الحرجة تعدّ من أبرز خصائص الأداء الأمني الجيد.

ث- الشفافية والمساءلة: يجب أن يتمتع منتسبو الأجهزة الأمنية بمستوى عالٍ من الشفافية، ويجب أن يكونوا خاضعين للمساءلة لضمان عدم تجاوزهم للحدود المسموح بها.

ج- العمل الجماعي والتنسيق: النجاح في المهام الأمنية يتطلب تنسيقًا جيدًا بين مختلف الوحدات والأفراد، بالإضافة إلى العمل الجماعي الفعّال.

ويستنتج الباحث مما سبق، أن أداء منتسبي الأجهزة الأمنية يتطلب تحقيق عدة معايير أساسية، تشمل الاحترافية والكفاءة لضمان أداء المهام بكفاءة عالية، والالتزام بالقانون واحترام حقوق الإنسان لتعزيز الثقة المجتمعية. كما تُعتبر الاستجابة السريعة والشفافية والمساءلة، بالإضافة إلى العمل الجماعي والتنسيق الفعّال، من العناصر الضرورية لنجاح الأداء الأمني وتحقيق استقرار المجتمع.

أبعاد أداء منتسبي الأجهزة الأمنية:

البعد الأول: أداء المهام: يعني الدرجة التي يؤدي بها العامل مهام وظيفته لتحقيق الأهداف التنظيمية (Bachrach et al., 2007)، وإن قدرة الموظفين على الاستكشاف تعزز أداء المهام من خلال استغلالهم الفعال. بالإضافة إلى ذلك، من منظور الملاءمة الاستراتيجية، فإن استكشاف الموظفين واستغلالهم لهما تأثير إيجابي في أداء المهام. يُعتبر استغلال الموظف آلية فعالة تفسر جزئيًا العلاقة بين الاستكشاف وأداء المهام يجدر بالذكر أن العلاقة بين استكشاف الموظف واستغلاله تكون أقوى في بيئات ذات توجه تنافسي منخفض، كما أشار إليه(Zhang, et al, 2022) .

أشار غويتز ووالد (2021) إلى أن أداء المهام والأداء الابتكاري في التدريب العملي يتحسنان بشكل ملحوظ من خلال توافق الأداء العام للموظف. وقد أوضحا أيضًا أن العدالة التنظيمية لها تأثير كبير؛ إذ أن توافق الشخص مع الوظيفة يؤثر بشكل أكبر على الأداء.

البعد الثاني: الأداء السياقي: ويعني سلوك الدور الإضافي الطوعي الذي لم يُضمّن في مسؤوليات عمل الموظف أو نظام المكافآت (Christian et al., 2011)

يعد الأداء الوظيفي للموظفين مرتبطًا بشكل وثيق بكلا الطرفين: الموظفين والمؤسسات، وهو يؤدي إلى مجموعة من النتائج التنظيمية الإيجابية .(Sonnentag et al., 2008) وتعتبر هذه النتائج بمثابة المسار الذي يعزز سلوك الموظف داخل المنظمة لتحقيق أهدافها (Motowidlo & kell, 2012).

الأداء السياقي يشير إلى السلوكيات التي تسهم في تعزيز الفعالية التنظيمية من خلال تأثيراتها في الجوانب النفسية والاجتماعية والتنظيمية في الوظائف التي يؤديها الموظفون. هذه السلوكيات تلعب دورًا مهمًا في تحسين بيئة العمل وتحقيق الأهداف التنظيمية (Motowidlo & kell, 2012)

البعد الثالث: الأداء التكيفي: نظراً لأن البيئة تصبح أكثر اضطراباً، فإن قدرة الموظفين على التعامل مع حالات الطوارئ والتعلم بسرعة وحل المشكلات الجديدة تصبح قدرات مطلوبة

لم تتناول الآراء السابقة حول أداء العمل جميع جوانب السلوكيات الفردية التي تسهم في فعالية الوظيفة في الأنظمة غير المؤكدة والمترابطة .(DeNisi, and Murphy, 2017) نتيجة لذلك، أصبح الأداء التكيفي، الذي يُعرف بقدرة الموظفين على التكيف مع مواقف العمل المتغيرة بسرعة محط اهتمام، بوصفه وسيلة لفهم الطبيعة الديناميكية لأداء الموظف بشكل أفضل في بيئة الأعمال الحالية السريعة التغير.

لخص حسنين (2020) أبعاد تميز أداء العاملين ويشمل ما يأتي:

– تنفيذ المهام: إذ أن المقصود منها عبارة عن " السلوكيات التي تساعد في إنجاز عمليات أساسية وجوهرية في المنظمة الإنتاج المباشر وتقديم الخدمات...إلخ، وأي أداء يسهم في تنفيذ وتحقيق أعمال المنظمة أو منشأة العامل، وهو كلّ أداءٍ يسهمُ بشكل مباشر أو غير مباشر فِي تنفيذ عمليات المنظّمة، أي أنّ أداء المهامّ يعكس جهد الفرد وإنجازاته لمختلف الأَعمَال والوظائف المُوكَلَةَ إليه.

– التطور الوظيفي: وهو منهج معرفي يعتمد على افتراضات العلوم السلوكية ويهدف إلى زيادة فاعلية المنظمة عبر إحداث تغيير مخطط في عملياتها وسلوكيات أفرادها والتكنولوجيا المستخدمة.

– التحلي بالمسؤولية: وهي الالتزام المستمر للعاملين في المنظمة بالتصرف الأخلاقي والمشاركة في حل القضايا الاجتماعية والاقتصادية والبيئية والقانونية والتطوعية، بهدف تحسين ظروف العاملين والمنظمة والبيئة والمجتمع ككل.

– تحقيق الأهداف: وهي التطلعات والنتائج المطلوب تحقيقها في المستقبل على المدى الطويل.

من خلال ما سبق، فإن أداء منتسبي الأجهزة الأمنية يتكون من عدة أبعاد رئيسية، أولها أداء المهام الذي يعكس قدرة الموظفين على تحقيق الأهداف التنظيمية من خلال استغلال فعال لمهاراتهم. البعد الثاني هو الأداء السياقي، الذي يشمل السلوكيات الطوعية التي تعزز الفعالية التنظيمية وتسهم في تحسين بيئة العمل. أما البعد الثالث، فهو الأداء التكيفي، الذي يعبر عن قدرة الموظفين على التكيف مع التغيرات السريعة وحل المشكلات الجديدة في بيئات العمل المتغيرة.

دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية

في عالمنا اليوم، تزداد الحاجة إلى وجود جدار حماية يحمي المجتمع من الجرائم المتزايدة. يلعب الذكاء الاصطناعي دورًا كبيرًا في هذا المجال؛ إذ يمكن استخدام الشبكات العصبية والخوارزميات للتنبؤ بالجريمة قبل وقوعها. تعمل هذه الخوارزميات على تحليل البيانات بشكل مستمر لتحديد الأنماط والمخاطر المحتملة، ما يساعد الجهات المسؤولة على اتخاذ الإجراءات اللازمة بشكل أسرع وأكثر فعالية. يمكن للدول الاستفادة من تقنيات الذكاء الاصطناعي لمواجهة التحديات الأمنية؛ إذ تسهم في تحسين الاستجابة للجرائم وتوفير بيئة أكثر أمانًا للمواطنين (رانا، 2022).

دور الذكاء الاصطناعي في تمييز أداء منتسبي الأجهزة الأمنية

الذكاء الاصطناعي دورًا مهمًا في الأجهزة الأمنية، خاصة في الدول الفقيرة التي تعتمد على الأساليب التقليدية لمكافحة الجريمة. ومع التطور التكنولوجي، أصبح بالإمكان استخدام الذكاء الاصطناعي لتحليل كميات ضخمة من المعلومات المتاحة عبر وسائل التواصل الاجتماعي، وكاميرات المراقبة، ووسائل الإعلام، والبيانات الحكومية للبحث عن أي معلومات تتعلق بمرتكبي الجرائم(علي، 2021).

تستخدم بعض المؤسسات الأمنية، مثل الولايات المتحدة، أجهزة محاكاة أبراج الهواتف الخلوية المعروفة باسم "ستينجراي". هذه الأجهزة تعمل على جمع البيانات من الأجهزة المحمولة في منطقة معينة، ما يتيح الوصول إلى قواعد البيانات، الرسائل، والاتصالات، علاوة على ذلك، يمكن للذكاء الاصطناعي أن يسهم في تخفيف التوتر بين الأطراف المتنازعة وتقليل الخسائر البشرية من خلال التنبؤ بمواقع الغارات الجوية وتنبيه المدنيين في المناطق المستهدفة (علي، 2021).

المؤسسة الأمنية الفلسطينية

منذ نشوء السلطة الوطنية الفلسطينية عملت المؤسسة الأمنية بكافة أذرعها على فرض سيادتها لقيام بمهامها لخدمة المواطن الفلسطيني، ووظفت العديد من الكفاءات الذين يعملون لتحقيق هدفها، فنجد أن العاملين في تلك المؤسسات يسعون إلى تحقيق الاستقرار الأمني والسياسي والاقتصادي للفلسطينيين، وهذا يشير إلى سعي العاملين في المؤسسة الأمنية إلى تطبيق معايير الحوكمة من أجل خدمة الوطن والمواطن.

إن المؤسسة الأمنية الفلسطينية جزء أصيل من الحوكمة كونها المؤسسة الأولى التي يقع على عاتقها تأمين المكون السياسي للدولة والكيان الاقتصادي وحماية النسيج الاجتماعي، بالإضافة حماية الأفراد

وتأمين الخدمات الأمنية التي تقع على عاتقها، وتحقيق هدفها الاستراتيجي الأساسي وهو حفظ الأمن والأمان للوطن والمواطن (الخطة الاستراتيجية لقطاع الأمن 2017–2022، 11).

القطاع الأمني من الجهات الرئيسية المكلفة بتوفير الأمن والعدالة، بالإضافة إلى إدارتها والمؤسسات التي تمارس الرقابة عليها. وينظم الإطار القانوني والإطار السياسي المهام التي تنفذها هذه الجهات، كما يحكم سلطاتها وهيكليتها التنظيمية. الجهات الرئيسية المكلفة بتوفير الأمن والعدالة، ومن هذه الأجهزة وزارة الداخلية، الأمن الوقائي، المخابرات العامة، الأمن الوطني، الدفاع المدني، الشرطة، التوجيه السياسي والوطني، الاستخبارات العسكرية، هيئة التدريب العسكري، الخدمات الطبية العسكرية (عيسى، 2014).

رؤية المؤسسة الأمنية (القطاع الأمني)

حسب ما ورد في الخطة الاستراتيجية لقطاع الأمن للعام 2017–2022، لوزارة الداخلية

"دولة مستقلة ينعم مواطنيها بالأمن والأمان"

رسالة المؤسسة الأمنية الفلسطينية (القطاع الأمني)

"تعزيز شعور المواطن بالأمن والأمان ومواجهة التحديات بالجهود الموحدة والأدوار المحددة والقدرات العالية لمؤسسات قطاع الأمن بالوسائل التي يتيحها القانون والمعاهدات الدولية على أسس من المهنية والكفاءة والشفافية وصيانة الحريات والحقوق العامة والخاصة والشراكة المحلية والدولية للمساهمة في خلق بيئة آمنة ومستقرة ومزدهرة"

الأهداف الاستراتيجية للمؤسسة الأمنية الفلسطينية

جاءت أهداف المؤسسة الأمنية منسجمة مع رؤيتها الواردة في خطتها للعام 2017–2022. دولة مستقلة ينعم مواطنيها بالأمن والأمان؛ إذ وضعت أهدافا رئيسية لتحقيق رؤيتها ضمن خطتها وقد جرى تحديد ثلاثة أهداف استراتيجية للمؤسسة الأمنية الفلسطينية حسب توجهاتها وأولوياتها الاستراتيجية وهي كما يأتي:

أولا: تعزيز الأمن وحماية الوطن

ثانيًا: حوكمة المؤسسة الأمنية

ثالثًا: بناء قدرات قوى الأمن

تقييم أداء الأجهزة الأمنية

لم تختلف الكثير من التقييمات التي أجريت على أداء السلطة الوطنية الفلسطينية فيما يتعلق بحكمها لقطاعها الأمني، إذ أُجري عدد لا يستهان به من تلك التقييمات منذ عام 1995 ومن النتائج التي توصلت إليها، أن الأجهزة الأمنية عانت من (فريدريك، وليتهولد، 2008)

- التسيس.
- الولاءات الشخصية القوية التي تحكمها
- تضخم عدد أفرادها
- تداخل المهام والمسؤوليات المنوطة بها
- قلة تعاون تلك الأجهزة مع بعضها

- افتقارها للخبرات الإدارية

تناول المبحث الثالث موضوع أداء منتسبي الأجهزة الأمنية، مشيرًا إلى أهمية هذا الأداء في حماية الأمن الوطني وتعزيز الثقة العامة بين المواطنين والسلطات. وقد عُرف أداء العاملين بأنه مخرجات الأهداف التي تسعى المنظمات لتحقيقها، ويتضمن الكفاءة والفاعلية والإنتاجية. جرى تحديد عدة مكونات ومعايير للأداء، مثل الاحترافية والالتزام بالقانون، والاستجابة السريعة. كما جرى تناول أبعاد الأداء، التي تشمل أداء المهام والأداء السياقي والتكيفي. بالإضافة إلى ذلك، تم التركيز على دور الذكاء الاصطناعي في تحسين الأداء الأمني من خلال تحليل البيانات والتنبؤ بالجرائم. وأخيرًا، تم الإشارة إلى رؤية وأهداف المؤسسة الأمنية الفلسطينية.

2.2 الدراسات السابقة:

الدراسات المتعلقة بالذكاء الاصطناعي والجرائم الإلكترونية:

الدراسات العربية

دراسة قاسم (2024) هدفت هذه الدراسة إلى معرفة دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية دراسة مقارنة بين القانون اليمني والقانون الفلسطيني، ولتحقيق أهداف الدراسة استخدم الباحث المنهج الوصفي التحليلي لمعرفة آلية استخدام الذكاء الاصطناعي في مواجهة الجريمة الإلكترونية، والمنهج المقارن من خلال المقارنة بين الأنظمة القانونية ودورها في مكافحة الجريمة الإلكتروني، أكدت الدراسة على دور استخدام الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية قبل حدوثها، أو المساعدة في التوصل لإثبات الجريمة والكشف عن هوية المجرمين بعد حدوث الجريمة، وبينت الدراسة خطورة الجرائم الإلكترونية على مستوى الأفراد أو المجتمع أو الدول من خلال قيام المجرمين باستخدام هذه الجرائم لجني الأموال من المؤسسات المتضررة من جرائمها؛ كونها جرائم عابرة للقارات، ويصعب كشفها أو التنبؤ بها بسهولة، وكشفت الدراسة عن إمكانية استخدام التقنيات الصناعية في مواجهة جرائم المحتلين للبلدان وإمكانية إرباك التقنيات الاصطناعية التي يعتمد عليها العدو في جرائمه ضد الشعوب.

دراسة محمود (2024) أدى التطور التكنولوجي إلى ابتكار وسائل دفع إلكترونية تعززت بفضل شبكة الإنترنت وظهور التجارة الإلكترونية، ما أسهم في تقليل الوقت والتكاليف وتحقيق مزايا لم تكن متاحة عبر وسائل الدفع التقليدية في البيئة المصرية، ومع ذلك، لا تخلو هذه الوسائل من العيوب؛ إذ تحمل المخاطر المرتبطة بالجرائم الإلكترونية وجرائم البطاقات البنكية، وتتعرض الأوراق التجارية الإلكترونية، مثل الكمبيالات والسندات والشيكات الإلكترونية، لمخاطر التلاعب والتحايل، ما يشكل تهديدًا لحامليها ومصادرها، ويؤثر سلبًا في الاقتصاد الوطني والدولي. لذا، من الضروري وجود نظام قانوني متكامل

لحماية هذه الأوراق وأطراف المعاملات، وتعتبر الأوراق التجارية الإلكترونية من التزامات المشتري في العقود الإلكترونية، ما يجعلها متميزة عن العقود التقليدية؛ إذ تسهل المعاملات التجارية، خصوصًا في التجارة الدولية، من خلال تيسير تحويل الأموال عبر الإنترنت. في الوقت نفسه، تشهد نظم المعلومات ثورة كبيرة مع ظهور تطبيقات جديدة ومعايير حديثة، أبرزها تقنيات الذكاء الاصطناعي. يُعنى هذا المجال بدراسة ومحاكاة الذكاء البشري، ما يؤدي إلى تطوير حاسبات ذكية قادرة على إنجاز مهام تتطلب قدرات عالية من الاستنتاج والإدراك، وهي صفات كانت محصورة في البشر في الماضي.

دراسة عضيات وأبو عيادة (2023) بعنوان: تفعيل دور تطبيقات الذكاء الاصطناعي في آلية رصد الجرائم.

هدفت هذه الدراسة إلى اقتراح تصور استشرافي ديناميكي جديد في دور تطبيقات الذكاء الاصطناعي في آلية رصد الجرائم المستقبليَّة، بما يتماشى مع تغييرات وتطورات الثورة الصناعية الرابعة في الجانب المعرفي والعلمي وتكنولوجيا المعلومات من خلال تفعيل برامج تطبيقات الذكاء الاصطناعي الأمنية. واعتُمد المنهج المسحي الوصفي التطويري، وجرى بناء استبانة كأداة للتعرف على واقع تفعيل برامج تطبيقات الذكاء الاصطناعي الأمنية في آلية رصد جرائم المستقبل من وُجهة نظر العاملين في وحدة الجرائم الإلكترونية، وأظهرت النتائج أن تفعيل تطبيقات الذكاء الاصطناعي جاء بدرجة مُتوسطة وبناءً على نتائج الدراسة، وَوَفقًا لرؤية الباحثين تم تطوير رُؤية استشرافية مُقترحة لتفعيل برامج تطبيقات الذكاء الاصطناعي الأمنية لدى العاملين في وحدة مُكافحة الجرائم الإلكترونية، وتعرف درجة مُلاءمتها من جهة نظر الخبراء والمختصين؛ إذ تكوَّنت هذه الرؤية من ثلاثة مجالات هي: مُراقبة وقائية عن الجرائم، والكشف عن الجرائم، والعقوبة. إذ تُوصي دراسة التخطيط للتحول بمنع جرائم المستقبل منعًا ذكيًّا،

وتأسيس بيئة ذكية، لتواكب المتغيرات في العصر الحالي، وتحسين أوضاع مُكافحة الجرائم المستقبلية، من خلال زيادة المخصصات المالية وميزانية مُحددة للتوسع في البنى الذكية للحكومة الرقمية.

دراسة الأخشن والعيداني (2023) هدفت إلى تحديد ماهية الذكاء الاصطناعي والجريمة المعلوماتية وبيان تعريفهما وأبرز خصائصهما والكشف عن مدى وجود علاقة مؤثرة بني الذكاء الاصطناعي من جهة ومكافحة الجريمة الالكترونية من جهة أخرى. تمثلت نتائج الدراسة في أن تقنيات الذكاء الاصطناعي هي نتاج جهود بحثية وتطبيقية عبر مراحل مختلفة من التاريخ وهي أنظمة ذات قدرات فائقة وتسعى لأن تكون ذات تأثير فعال في مستويات مختلفة للجرائم أهمها مجابهة الجرائم المعلوماتية، كما أظهرت الدراسة أن الجرائم الالكترونية جرائم مستحدثة تطورت في العصر الحديث وطرق مواجهتها تلتقي مع نظم الذكاء الاصطناعي فائقة القدرات.

دراسة الشاعر (2023) هدفت إلى استكشاف دور الذكاء الاصطناعي في تعزيز إجراءات التحقيق الجنائي المتعلقة بالجرائم الإلكترونية من خلال إجراء دراسة مقارنة. حيث تسلط الدراسات القانونية والفلسفية والاجتماعية الضوء على أهمية تحقيق الشرعية الإجرائية وتعزيز التضامن الاجتماعي، نظراً لأن الأضرار الناتجة عن الجرائم تؤثر في المجتمع بأسره بالإضافة إلى الأفراد، ما ينعكس سلبًا على الشعور بالأمان داخل المجتمع. تسعى هذه الدراسات إلى دفع المشرع إلى تعديل وتطوير التشريعات لضمان حقوق المجني عليهم والمتهمين والمدعين بالحق المدني. هناك مجالات متنوعة يمكن للذكاء الاصطناعي أن يلعب دورًا فيها في العمل الشرطي والأمني، وغالبًا ما تقع ضمن استراتيجيات المدن الذكية، التي تهدف إلى استخدام التقنيات المتطورة مثل الذكاء الاصطناعي لضمان أمن وسلامة السكان، وتشمل تقنيات الذكاء الاصطناعي كاميرات مراقبة ذكية قادرة على تحليل الصور والفيديو لاكتشاف وجود المشتبه بهم أو الأمور غير الطبيعية وإرسال تنبيهات لمركز التحكم. كما تُستخدم تقنيات تعلم الآلة في

الأمن الإلكتروني، بالإضافة إلى الطائرات الذكية بدون طيار (الدرونز) للمراقبة الجوية. وتُعتبر تطبيقات "التنبؤ الشرطي" من بين الأدوات الحديثة التي تستخدمها بعض الجهات الشرطية الرائدة حاليًا لمكافحة الجريمة؛ إذ تعتمد على تقنيات الذكاء الاصطناعي في مجال التحقيق الجنائي لكشف العديد من الجرائم، وأبرزها الجرائم الإلكترونية.

دراسة النعمي، (2023) بعنوان: دور الجهات المسؤولة عن الجريمة الإلكترونية في اليمن في توعية الجمهور بخاطر الجريمة الإلكترونية.

هدفت الدراسة إلى الكشف عن واقع الجريمة الإلكترونية في اليمن، ومعرفة دور الجهات المسئولة عن الجريمة الإلكترونية في اليمن في توعية الجمهور بمخاطر الجريمة الإلكترونية، وقد اعتمدت الدراسة على المنهج الوصفي الذي جُمعت بواسطته البيانات الكمية والكيفية للدراسة معاً، وقد استخدم الباحث التصميم التفسيري؛ إذ جُمعت في المرحلة الأولى من هذا التصميم بيانات كمية باستخدام استبانة الذي جرى تطبيقها على عينة عشوائية بلغت 400 من مستخدمي الإنترنت بأمانة العاصمة صنعاء، تلا ذلك جمع البيانات الكيفية باستخدام أداة المجموعات المركزة، التي شرحت النتائج الكمية وفصلتها، وامتد جمع البيانات الكيفية بهذه الدراسة؛ بحيث شمل أداة المقابلة المعمقة مع مدراء ومسئولي إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجريمة الإلكترونية.

توصلت الدراسة إلى ارتفاع معدل الاستخدام اليومي للمبحوثين للإنترنت، وأن نسبة (47%) من الجمهور عينة الدراسة قد تعرضوا لنوع واحد على الأقل من الجرائم الإلكترونية، وأشارت النتائج إلى المعرفة الجيدة للمبحوثين بالمفاهيم العامة للجريمة الإلكترونية، والوعي الضعيف للمبحوثين بطرق الوقاية من الجريمة الإلكترونية، كما توصلت الدراسة إلى فشل إدارات الإعلام والعلاقات العامة بالجهات المسئولة عن الجرائم الإلكترونية في اليمن في أعمال توعية وتثقيف الجمهور بمخاطر الجريمة الإلكترونية.

دراسة فرج (2022) بعنوان: "الجريمة الالكترونية وتداعياتها على أمن الوطن والمواطن بين المكافحة القانونية وأجهزة الكشف والتحري".

يعرف زماننا هذا العديد من التطورات الظاهرة من الناحية العلمية، ولعل أبرزها على الإطلاق ما تشهده الثورة المعلوماتية والإلكترونية وانتشار لا محدود للشبكة العنكبوتية، بغية تطوير الحياة وتسهيلها هذا الجانب الايجابي، غير أنه مقابل ذلك أنتجت هذه الطفرة العلمية جرائم معاصرة تخالف الجانب الكلاسيكي لها التي اصطلح عليها بالجريمة الالكترونية أو المعلوماتية، جريمة تمس عمق قيم الأفراد والهيئات وحتى سيادة الدول وهذا جانبها السلبي، ما استدعى الإسراع إلى الحد من عواقب التطور العلمي بالتشخيص الدقيق والكامن بغية ضبط حدودها ومنه سهولة التحكم فيها.

دراسة عبد الباقي (2018) بعنوان: جرائم الحاسوب-فلسطين جرائم الحاسوب-تحقيق: الدليل (القانون)

تناولت هذه الدراسة التحقيق في الجرائم الإلكترونية وكيفية ضبط الأدلة الرقمية وجمعها من الموضوعات المستجدة في فلسطين وغيرها من دول العالم. كما أن طبيعة الأدلة الرقمية وكيفية التعامل معها من قبل جهات التحقيق تعتبر من الموضوعات ذات الأهمية القانونية والعملية. ويقوم بالتحقيق في الجرائم الالكترونية نيابة متخصصة وفق إجراءات وقواعد إثبات خاصة، يساعدها في ذلك ضابطة قضائية متخصصة بالجرائم الالكترونية، على عكس الجرائم التقليدية التي تختص بالتحقيق فيها النيابة العامة تساعدها الضابطة القضائية ذات الاختصاص العام وفقاً لقواعد التحقيق والإثبات التقليدية. ويعترض عمل النيابة العامة والضابطة القضائية العديد من الصعوبات، من أهمها القصور التشريعي وضعف التخصص لدى القائمين على التحقيق وجمع أدلة هذا النوع من الجرائم. إن تعزيز وتقوية التحقيق في الجرائم الإلكترونية يقوم على وضع إجراءات إدارية لقسم التحقيق لضمان السيطرة الفعّالة على قضايا

الجرائم الإلكترونية، إضافةً إلى وضع مبادئ توجيهية للأدلة الإلكترونية الجنائية وصولاً إلى تحقيق ناجح وفعال في الجرائم الإلكترونية.

الدراسات الأجنبية

دراسة جيمي (Jimmy, 2024) بعنوان دور الذكاء الاصطناعي في التنبؤ بالتهديدات الإلكترونية

هدفت هذه الدراسة إلى استكشاف الدور الحاسم الذي يلعبه الذكاء الاصطناعي في التنبؤ بالتهديدات الإلكترونية، والتأكيد على قدراته في اكتشاف التطفل، وتحليل البرامج الضارة، ومنع التصيد الاحتيالي، والكشف عن الاحتيال. وتشمل تقنيات الذكاء الاصطناعي الرئيسية التي تمت مناقشتها التعلم الخاضع للإشراف وغير الخاضع للإشراف لاكتشاف الشذوذ، والشبكات العصبية لتعرف الأنماط المعقدة، و NLP لتحليل مؤشرات التصيد الاحتيالي أو التهديد المحتملة في النص. يتم نشر هذه التقنيات في وظائف الأمن السيبراني المختلفة، باستخدام البيانات التاريخية وحركة المرور على الشبكة وأنماط السلوك الضارة لتدريب النماذج التي يمكنها اكتشاف الهجمات الإلكترونية ومنعها والاستجابة لها في الوقت الفعلي. من خلال الجداول والرسوم البيانية، تسلط الورقة الضوء على مزايا الذكاء الاصطناعي في الأمن السيبراني، مثل اكتشاف التهديدات بشكل أسرع، وتحسين الدقة، وكفاءة التكلفة، مع معالجة تحديات مثل الاعتماد على جودة البيانات والاعتبارات الأخلاقية. علاوة على ذلك، ندرس دمج الذكاء الاصطناعي في أطر الأمن السيبراني وإمكاناته لتحويل استراتيجيات منع التهديدات المستقبلية. في النهاية، تؤكد هذه الورقة الدور الحاسم للذكاء الاصطناعي كمؤشر ومستجيب للتهديدات الإلكترونية، بحجة أنه مع تطور التكنولوجيا، سيصبح الذكاء الاصطناعي أحد الأصول التي لا غنى عنها في مكافحة الجرائم الإلكترونية.

دراسة المرجيلاني (Al-Marghilani, 2022) بعنوان: تطوير نموذج جديد يستند إلى الذكاء الاصطناعي (AI) لتحسين عمليات تحديد الهوية للمشتبه بهم في مجال الجرائم المالية ومسرح الجريمة

هدفت إلى تطوير نموذج جديد يستند إلى الذكاء الاصطناعي (AI) لتحسين عمليات تحديد الهوية للمشتبه بهم في مجال الجرائم المالية ومسرح الجريمة، وقامت الدراسة بتطوير نموذج جديد يعتمد على التعلم العميق (Deep Learning) لتوليف رسم الوجه (FSS) للمشتبه فيه. ويتكون النموذج المقترح من ثلاث مراحل: المرحلة الأولى: المعالجة السابقة لتحسين جودة الصورة، المرحلة الثانية: استخراج الميزات باستخدام نموذج Mobile Net المستند إلى DL، المرحلة الثالثة: توليف رسم الوجه باستخدام خوارزمية QOFFO، كانت نتائج الدراسة مشجعة حيث أظهر النموذج المقترح (DLESS-S1) تفوقا على الطرق المقارنة في عدة جوانب. فيما يتعلق بدقة تحديد الهوية، فقد وصل متوسط الدقة إلى 93.4% مما يشير إلى كفاءة عالية في تمييز الهويات. كما تميز النموذج بجودة رسم ممتازة؛ إذ بلغ متوسط خطأ التربيع المتوسط (MSE 0.0001) ما يعكس دقة عالية في تحليل البيانات، بالإضافة إلى ذلك، كان وقت الحساب للنموذج فعالا: وقد بلغ متوسط وقت الحساب 0.002 ثانية، مما يبرز الكفاءة في سرعة استجابة النظام، ويعكس هذا التفوق الشامل للنموذج المقترح إمكانية تطبيقه بفاعلية في سياقات مختلفة تتطلب دقة وكفاءة في مجالات تحديد الهوية وجودة الرسم.

دراسة بولسون (Powelson, 2022) بعنوان: دور الذكاء الاصطناعي في تعزيز فاعلية برامج مكافحة غسل الأموال ومكافحة الجرائم المالية،

هدفت الدراسة إلى تسليط الضوء على دور الذكاء الاصطناعي في تعزيز فاعلية برامج مكافحة غسل الأموال ومكافحة الجرائم المالية، وقامت الدراسة بمراجعة الأدبيات حول الذكاء الاصطناعي ومكافحة

غسل الأموال ومكافحة الجرائم المالية، كما أجرت الدراسة تحليلا للتحديات والفرص المرتبطة بتطبيق الذكاء الاصطناعي في هذا المجال، وأظهرت نتائج الدراسة أن الذكاء الاصطناعي يمكن أن يكون أداة فعالة في تعزيز فاعلية برامج مكافحة غسل الأموال ومكافحة الجرائم المالية، ويمكن أن يساعد الذكاء الاصطناعي في تحسين المكونات التالية لبرامج مكافحة غسل الأموال.

دراسة أومير (Umair, 2022) بعنوان: تطوير نموذج تنبؤ بالجرائم باستخدام ذاكرة ثنائية الاتجاه طويلة المدى (Bi LSTM–) لتحسين دقة التنبؤ

هدفت إلى تطوير نموذج تنبؤ بالجرائم باستخدام ذاكرة ثنائية الاتجاه طويلة المدى (Bi LSTM–) لتحسين دقة التنبؤ، وجرى جمع بيانات الجريمة الزمانية والمكانية، وتم تقسيمها إلى مجموعة تدريب ومجموعة اختبار، وتدريب نموذج Bi–LSTM على مجموعة التدريب، ثم تقييم أدائه على مجموعة الاختبار. وأظهرت نتائج الدراسة أنه رغم استخدام تقنيات التعلم الآلي والتعلم العميق، تظهر مشكلات دقة في التنبؤ بالجرائم، ولتجاوز هذه التحديات. واقترحت الدراسة استخدام ذاكرة ثنائية الاتجاه طويلة المدى (Bi–LSTM)، وهي نوع من الشبكات العصبية التكرارية (RNN) التي تستخدم في معالجة اللغة الطبيعية (NLP)؛ إذ تتميز Bi–LSTM بقدرتها على معالجة المعلومات في النص من كلا الاتجاهين، ما يساعدها في فهم العلاقات بين الكلمات في الجملة بشكل أفضل، وهذا النهج يشير إلى تقديم حل مبتكر لتحسين دقة التنبؤ بالجرائم في ظل التحديات الحالية التي تواجهها وكالات إنفاذ القانون.

الدراسات المتعلقة بالأداء لمنتسبي الأجهزة الأمنية:

الدراسات العربية

دراسة الدرابيع (2023) هدفت هذه الدراسة إلى معرفة واقع تطبيق الحوافز والترقيات وعلاقتها بتحسين أداء المنتسبين في الأمن الوطني الفلسطيني، استخدم الباحث المنهج الوصفي التحليلي، وجرى تحليل البيانات بواسطة برنامج التحليل الإحصائيSPSS ، وتكون مجتمع الدراسة من جميع منتسبي جهاز الأمن الوطني في محافظة الخليل، خلال العام (2023) والبالغ عددهم(290)، وقد طور الباحث أداة الدراسة الاستبانة. إذ جرى توزيعها على عينة الدراسة البالغة (150) منتسب ومنتسبة لجهاز الأمن الوطني. خلصت الدراسة إلى عدة نتائج أهمها: تبين أن منح الحوافز المعنوية والمادية أثرت بشكل إيجابي في أداء المنتسبين وتحفيزهم للعمل بجدية واجتهاد ، وأن الجهاز الأمني يمنح الترقية للمنتسبين الذين يقومون بأعمال استثنائية بدرجة متوسطة بصرف النظر عن أقدميتهم، كما تبين أن مستوى الأداء الوظيفي لمنتسبي الأجهزة الأمنية الفلسطينية جاء بدرجة مرتفعة وتبني معايير الجودة في الأداء الوظيفي وتوفير فرص المشاركة في وضع الخطط المستقبلية واتخاذ القرارات الإدارية، وظهر أن هناك علاقة ارتباطية بين تطبيق الحوافز والترقيات وتحسين أداء العاملين في الأجهزة الأمنية الفلسطينية في محافظة الخليل. كما خلصت الدراسة إلى عدة توصيات نذكر منها: تعزيز التركيز على تقدير وتكريم المنتسبين الذين يقومون بأعمال استثنائية، بغض النظر عن أقدميتهم، وذلك عن طريق تطوير نظام ترقيات يعتمد على الأداء والجهد المبذول.

دراسة عقل (2022) بعنوان أثر نظام إدارة الأداء على أداء العاملين في الأجهزة الأمنية الفلسطينية: الدور المعدل للتدريب والتطوير

هدفت الدراسة إلى مناقشة إدارة الأداء على أنها وسيلة للحصول على نتائج أفضل من المنظمة بأكملها من خلال الفهم والإدارة ضمن إطار عمل متفق عليه، وأداء الأهداف المخططة والمعايير ومتطلبات الكفاءة". جرى استخدام المنهج الوصفي خلصت الدراسة إلى توافق مجتمع الدراسة بدرجة مرتفعة على واقع نظام إدارة الأداء في المنظمة الأمنية الفلسطينية من حيث: تخطيط الأداء، الاتصال والتواصل، مراقبة وتقييم الأداء، التشخيص، في حين وافق المجتمع بدرجة متوسطة على واقع نظام إدارة الأداء من حيث جمع البيانات وتوثيقها. من ناحية أداء العاملين، وافق مجتمع الدراسة بدرجة مرتفعة على واقع أداء العاملين في المنظمة الأمنية الفلسطينية من حيث أداء المهام والأداء السياقي، في حين وافق المجتمع بدرجة متوسطة على واقع الأداء التكيفي للعاملين. وتبين وجود أثر معنوي ي لنظام إدارة الأداء على تطوير أداء العاملين في الأجهزة الأمنية الفلسطينية؛ إذ وجد الباحثون أن هناك علاقة إيجابية ذات دلالة إحصائية بين إدارة الأداء وأداء الموظف. وتبين أيضا وجود أثر معنوي للتدريب على أداء العاملين؛ إذ يلعب التدريب دور المعدل والمطور في أداء العاملين في الأجهزة الأمنية الفلسطينية. وخلصت الدراسة إلى عدم وجود فروق معنوية في أداء العاملين في الأجهزة الأمنية تُعزى للمتغيرات الديموغرافية (العمر، المؤهل العلمي، سنوات الخبرة، المسمى الوظيفي، الجنس، الجهاز)، وان العلاقة بين (نظام إدارة الأداء) و(الأداء التكيفي) مقبولة و 55.8 % من التأثيرات في الأداء التكيفي تعود إلى نظام إدارة الأداء والعلاقة بين (نظام إدارة الأداء) و(الأداء السياقي) مقبولة وأن 62.8 % من التأثيرات على الأداء التكيفي تعود إلى نظام إدارة الأداء؛ إذ أن العلاقة بين (نظام إدارة الأداء) و(أداء العاملين) قوية، وأن 70 % من التغيير في أداء العاملين يُعزى إلى ادارة الاداء والعلاقة بين (نظام إدارة الأداء) و(أداء المهام) مقبولة، وأن 61% من التغيير في أداء العاملين يُعزى إلى أداء المهام.

دراسة الشروقي (2018) بعنوان: تأثير ممارسات إدارة الموارد البشرية في التميز المؤسسي في وزارة الداخلية بمملكة البحرين

هدفت الدراسة إلى تعرف أثر ممارسات إدارة الموارد البشرية على التميز المؤسسي في وزارة الداخلية البحرينية باستخدام المنهج الوصفي التحليلي، وتوصلت الدراسة إلى مجموعة من النتائج تمثل أهمها: يتوفر في وزارة الداخلية مستوى مرتفع من التميز المؤسسي وبمستوى متوسط من تخطيط الموارد البشرية، العامل الديموغرافي الوحيد الذي كان له تأثير في تقدير التميز المؤسسي هو الجنس في حين لم يكن للمستوى الوظيفي وسنوات الخبرة أي تأثير، مستوى الاستقطاب والتعيين على مستوى مرتفع مع ملاحظة وجود ضعف نسبي في ربط سياسات الاستقطاب والتعيين بالاحتياجات المستقبلية من الموارد البشرية.

دراسة (القحطاني (2017) بعنوان تطوير القيادات الإدارية ودورها في تحسين الأداء المؤسسي: دراسة تطبيقية على محافظات ومراكز إمارة الرياض.

هدفت الدراسة إلى تعرف أثر تطوير القيادات الإدارية في تحقيق وتحسين الأداء المؤسسي في محافظات ومراكز إمارة الرياض، واقتصرت على المستويات الإشرافية والبالغ عددهم (542) وبلغ حجم عينة الدراسة (234)، واستخدم المنهج الوصفي التحليلي. وتوصلت الدراسة على عدة نتائج تمثل أهمها بوجود حالة من تطوير القيادات بالإمارة عن طريق رفع مستويات الأداء الذي يصل إلى التميز، وتحديد الاحتياجات التدريبية لتنوير القيادات الإدارية بطريقة علمية، وكذلك استخدام التقنية الحديثة، وتحاول القيادات الادارية تحسين الأداء المؤسسي عبر خطوات واضحة وهي تحسين مهارات التواصل مع المراجعين والمرؤوسين، تعزيز ثقافة الانضباط في العمل لدى العاملين، وقد أوصت الدراسة بالعديد من التوصيات تمثل أهمها بضرورة تطوير القيادات الإدارية من خلال القضاء على معوقات التطوير والتي

من أهمها تحسين أنظمة الحوافز المادية والمعنوية للمتميزين، ودعمهم بالتقنيات الحديثة للمساهمة في تحسين الأداء المؤسسي.

دراسة تربان (2014) هدفت الدراسة الوقوف على دور أكاديمية فلسطين للعلوم الأمنية في تحسين أداء العاملين في وزارة الداخلية والأمن الوطني بغزة، ولتقديم توصيات قد تسهم في سبل تعزيزه وقد استخدم الباحث المنهج الوصفي التحليلي موظفاً الاستبانة أداة لجمع بيانات الدراسة أما عينة دراسته فتمثلت في (139) خريجاً من خريجي الأكاديمية وهي بواقع (19%) من مجتمع الدراسة وقد خلصت الدراسة إلى درجة مرتفعة من رضا عينة الدراسة على دور الأكاديمية في الارتقاء بهم في أهم الجوانب ذات العلاقة بمهام عملهم: المعرفي والقيمي والمهاري؛ إذ احتل الجانب القيمي المرتبة الأولى بنسبة 42.86 %فيما احتل الجانب المعرفي المرتبة الثانية بنسبة 19.7% فيما جاء الجانب المهاري في المرتبة الثالثة بنسبة 19.7 % كما قدم الباحث جملة من التوصيات ذات العلاقة التي يرى أنها قد تسهم في تحسين أداء دور الأكاديمية في تحسين أداء منتسبي وزارة الداخلية والأمن الوطني بغزة ومن أهمها ضرورة تعزيز العلاقة ما بين الأكاديمية والوزارة وتوفير الحوافز المناسبة للخريجين وتعزيز الجوانب المهارية في البرامج التعليمية المخصصة لتأهيل منتسبي وزارة الداخلية والأمن الوطني.

دراسة العبيدي، وآخرون، (2022) بعنوان: "دور الإدارة العراقية في مكافحة الجرائم المعلوماتية المخلة بالأمن العام"

في العقود الأخيرة برزت ثورة من نوع آخر متعلقة بوسائل الاتصال والمعلومات، نتيجة التطور الذي تجسد أساسا في انتشار أجهزة الحاسب الآلي التي تطورت بشكل مستمر، بالإضافة إلى البرامج المتقدمة، وشبكات الاتصال التي قربت ملايين البشر ببعضهم، وأتاحت فرصا جديدة للاطلاع على المعلومات وتبادلها، وحتى التفاوض وإبرام عقود مختلفة خصوصا عبر شبكة الأنترنت، بل الأكثر من ذلك يمكن

عبر هذه الأخيرة تسليم المنتجات كالبرامج، أو القطع الموسيقية، أو الصحف الالكترونية، أو تقديم الخدمات، مثل الاستشارات القانونية أو الطبية. لكن ما دامت الجريمة ظاهرة اجتماعية، تتأثر طبيعتها وحجمها بالتحولات الاقتصادية والاجتماعية والثقافية دولياً ووطنياً، فقد ظهر للوجود نمط جديد من الإجرام، تجسد في انتشار الجرائم المعلوماتية أو الإلكترونية، والتي تعدّ من أكبر السلبيات التي خلفتها الثورة المعلوماتية، لكون هذه الجرائم تشمل في اعتداءاتها قيما جوهرية تخص الأفراد والمؤسسات، وليس على مستوى العراق فحسب بل وحتى الدول في نواحي الحياة كافة ، كما أن هذه الجرائم تركت في النفوس شعورا بعدم الثقة بخصوص التعامل والاستفادة من ثمار هذه الثورة الجديدة.

الدراسات الأجنبية

دراسة (Miller, 2020) بعنوان

"Leadership Styles In Policing And Officers' Job Satisfaction "

هدفت الدراسة إلى تعرف دور قيادة الشرطة في التأثير على الأداء و الرضا الوظيفي من المرؤوسين، من خلال التعرف على نموذج السلوكيات القيادية الإيجابية، حاولت الدراسة تحديد العلاقة بين الأسلوب القيادي والرضا الوظيفي للضباط، شملت الدراسة عينة مكونة من (94) ضابط وعدد قليل من القادة الذين شاركوا في الدراسة، حيث تم تطبيق النمط الكمي في إجراء المسوحات وتحليل البيانات وقد توصلت الدراسة إلى مجموعة من النتائج: وجد علاقة بين درجات الرضا الوظيفي عامة و خصائص القيادة التحويلية مع التركيز على مساهمة كبيرة للسمات المثالية. فشل إظهار أي علاقات مهمة بين الرضا الوظيفي العام وأي من المعاملات أو أساليب القيادة المتبعة.

دراسة (Amistoso et al, 2019) بعنوان

Performance Management System of a Security Agency in the Philippines

هدفت الدراسة إلى معرفة ممارسات إدارة الأداء لوكالة أمنية في سيبو، الفلبين. استخدمت الدراسة تصميمًا ارتباطيًا وصفيًا. كان المستجيبون 131 مستجيبًا يتكونون من حراس أمن وضباط أمن وحراس رئيسيين ومسؤولين عن نوبات العمل. طُلب منهم الإجابة على الاستبيان الذي أعده الباحث، كشفت النتائج أن معظم المستجيبين قيموا أن إدارة الأداء تمارس بشكل كبير فيما يتعلق بالالتزام وتحديد الأهداف وتقييم الأداء والمراقبة والتقييم والتدخل التنموي. وخلصت الدراسة إلى أن مستوى أفضل الممارسات وتطبيقها في إدارة الأداء يُمارس بمستوى عالٍ، إذ يُجري المدراء مراقبةً مستمرةً لخططهم وإجراءاتهم، بما يضمن فعالية وكفاءة أداء مهام الإدارة. ويوصي الباحثون باعتماد وتطبيق دليل نظام إدارة الأداء المقترح.

التعقيب على الدراسات السابقة

ملخص الأطروحة

عنوان الأطروحة	اسم الباحث (APA)	المنهج المستخدم	أهم نتيجة
دور الذكاء الاصطناعي في الحد من انتشار الجرائم الالكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً	طرده (2025)	المنهج الوصفي والتحليلي (استبيان بمقياس لكرت، تحليل إحصائي باستخدام t-test، ANOVA، تحليل الارتباط)	وجود علاقة إيجابية قوية (معامل ارتباط = 0.744) بين تطبيق الذكاء الاصطناعي وأداء منتسبي وحدة مكافحة الجرائم الإلكترونية، مع مستويات عالة لتطبيق الذكاء الاصطناعي (متوسط = 3.85، 77%) وتمز الأداء (متوسط = 4.20، 88.4%)

الدراسات المتفقة والمختلفة

عنوان الدراسة	اسم الباحث	المنهج	التوافق مع الأطروحة	تفاصيل التوافق والاختلاف
دور الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية	قاسم (2024)	وصفي تحليلي مقارن	متفقة	الدراسة تركز على استخدام الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وتتناول الأنظمة القانونية، مما يدعم موضوع الأطروحة.
تأثير وسائل الدفع الإلكترونية على الجرائم الإلكترونية	محمود (2024)	وصفي	متفقة	تسلط الضوء على المخاطر المرتبطة بالجرائم الإلكترونية في سياق التطورات التكنولوجية، مما يتوافق مع الأطروحة.
تفعيل دور تطبيقات الذكاء الاصطناعي في رصد الجرائم	عضيات وأبو عيادة (2023)	مسحي وصفي	متفقة	تتناول الدراسة تفعيل الذكاء الاصطناعي في رصد الجرائم، مما يتماشى مع موضوع الأطروحة حول الذكاء الاصطناعي.
العلاقة بين الذكاء الاصطناعي ومكافحة الجريمة المعلوماتية	الأخشن والعيداني (2023)	وصفي	متفقة	تبرز العلاقة بين الذكاء الاصطناعي والجرائم الإلكترونية، مما يدعم فكرة الأطروحة.
استكشاف دور الذكاء الاصطناعي في التحقيق الجنائي للجرائم الإلكترونية	الشاعر (2023)	مقارنة	متفقة	تركز على دور الذكاء الاصطناعي في تعزيز التحقيقات الجنائية، مما يتماشى مع الأطروحة حول تحسين الأداء الأمني.
دور الجهات المسؤولة عن الجريمة الإلكترونية في توعية الجمهور	النعمي (2023)	وصفي	متفقة بشكل جزئي	تركز الدراسة على توعية الجمهور بمخاطر الجرائم الإلكترونية، بينما الأطروحة تركز على الأداء والتقنيات الأمنية.
الجريمة الإلكترونية وتداعياتها على الأمن	فرج (2022)	وصفي	متفقة	تناقش تأثير الجرائم الإلكترونية على الأمن، مما يعزز من أهمية الدور الذي يلعبه الذكاء الاصطناعي في مكافحة هذه الجرائم.

جرائم الحاسوب في فلسطين	عبد الباقي (2018)	وصفي	متفقة	تتعلق بدراسة الجرائم الإلكترونية وتأثيرها على التحقيقات، مما يتماشى مع موضوع الأطروحة.
دور الذكاء الاصطناعي في التنبؤ بالتهديدات الإلكترونية	(Jimmy, 2024)	وصفي	متفقة	تركز على الذكاء الاصطناعي في الأمن السيبراني، مما يتوافق مع محتوى الأطروحة حول استخدام الذكاء الاصطناعي في الحد من الجرائم الإلكترونية.
تطوير نموذج جديد لتحسين تحديد الهوية باستخدام الذكاء الاصطناعي	(Al–Marghilani, 2022)	تجريبي	متفقة بشكل جزئي	تتعلق بدور الذكاء الاصطناعي في تحسين عمليات التحقيق، مما يدعم موضوع الأطروحة.
تعزيز فاعلية مكافحة غسل الأموال باستخدام الذكاء الاصطناعي	(Powelson, 2022)	مراجعة أدبيات	متفقة	تناقش كيفية استخدام الذكاء الاصطناعي في مكافحة الجرائم المالية، مما يدعم موضوع الأطروحة حول الذكاء الاصطناعي في مواجهة الجرائم.
تطوير نموذج تنبؤ بالجرائم باستخدام الذكاء الاصطناعي	(Umair, 2022)	تجريبي	متفقة	تقدم نموذجًا يعتمد على الذكاء الاصطناعي للتنبؤ بالجرائم، مما يدعم الأطروحة بشكل مباشر.
أثر نظام إدارة الأداء على أداء العاملين في الأجهزة الأمنية	عقل (2022)	وصفي	متفقة	تبرز أهمية الأداء في الأجهزة الأمنية، مما يتماشى مع موضوع الأطروحة حول تميز الأداء.
تأثير ممارسات إدارة الموارد البشرية على الأداء المؤسسي	الشروقي (2018)	وصفي	متفقة	تتعلق بتأثير إدارة الموارد البشرية على الأداء، مما يتماشى مع موضوع الأطروحة حول تحسين أداء منتسبي الأجهزة الأمنية.
تطوير القيادات الإدارية ودورها في تحسين الأداء المؤسسي	القحطاني (2017)	وصفي	متفقة	تناقش دور القيادة في تحسين الأداء، مما يتوافق مع موضوع الأطروحة حول تطوير الأداء الأمني.

دور أكاديمية فلسطين في تحسين أداء العاملين	تربان (2014)	وصفي	متفقة	تركز على التحسين في التعليم والتدريب للعاملين، مما يتماشى مع موضوع الأطروحة حول تعزيز القدرات الأمنية.
دور الإدارة العراقية في مكافحة الجرائم المعلوماتية	العبيدي وآخرون (2022)	وصفي	متفقة	تتعلق بمكافحة الجرائم الإلكترونية وتأثيرها، مما يدعم موضوع الأطروحة حول الذكاء الاصطناعي في مكافحة الجرائم.
تأثير القيادة على الأداء والرضا الوظيفي للضباط	(Miller, 2020)	وصفي	متفقة بشكل جزئي	تركز على القيادة والرضا الوظيفي، بينما الأطروحة تركز على الذكاء الاصطناعي وأداء الأجهزة الأمنية.
نظام إدارة الأداء لوكالة أمنية في الفلبين	(Amistoso et al, 2019)	وصفي	متفقة	تتعلق بممارسات إدارة الأداء في الوكالات الأمنية، مما يتماشى مع موضوع الأطروحة حول تحسين الأداء.

نسبة استخدام المنهج

المنهج الوصفي يشكل 58.8% عددها 20.

المنهج الوصفي التحليلي يشكل مع 11.8% عددها 4.

المنهج المسحي يشكل مع 8.8% عددها 3.

المنهج التجريبي يشكل مع 11.8% عددها 4.

المنهج المقارن يشكل مع 8.8% عددها 3.

الفجوة البحثية

هناك نقص في الدراسات التي تربط بين تطبيق الذكاء الاصطناعي وتحسين أداء منتسبي الأجهزة الأمنية الفلسطينية، وبخاصة في سياق وحدة مكافحة الجرائم الإلكترونية، ومعظم الدراسات السابقة تركز على الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية بشكل عام أو على جوانب قانونية وتوعوية، كما أن هناك حاجة لدراسات تستكشف تأثير التغيرات الديمغرافية (مثل التدريب على الذكاء الاصطناعي) في الأداء باستخدام مناهج تجريبية أو مختلطة.

تتميز الدراسة الحالية عن الدراسات السابقة بأنها تبرز التركيز على الذكاء الاصطناعي كأداة أساسية في مكافحة الجرائم الإلكترونية، مما يعكس الاتجاه المتزايد نحو استخدام التكنولوجيا الحديثة في هذا المجال. وتعكس الدراسة الحالية التفاعل بين الذكاء الاصطناعي وأداء منتسبي الأجهزة الأمنية؛ إذ يُعتبر الأداء المتفوق للموظفين متغيراً وسيطاً، ما يفتح المجال لفهم كيف يمكن أن تؤثر الكفاءات البشرية على فعالية تطبيقات الذكاء الاصطناعي في مكافحة الجرائم.

الفصل الثالث

طريقة الدارسة وإجراءاتها

1.3 المقدمة

2.3 منهج الدراسة

3.3 مجتمّع الدراسة

4.3 عينة الدراسة

5.3 أداة الدراسة

6.3 صدق أداة الدراسة

7.3 ثبات أداة الدراسة

8.3 متغيرات الدراسة

9.3 إجراءات تنفيذ لدراسة

10.3 الأساليب الإحصائيّة

الفصل الثالث

طريقة الدراسة وإجراءاتها

1.3 تمهيد:

يتناول هذا الفصل وصفاً كاملاً ومفصلاً لطريقة الدراسة وإجراءاتها التي قام بها الباحث لتنفيذ هذه الدراسة وتشمل وصف منهج الدراسة، مجتمّع الدراسة، وعينة الدراسة، أداة الدراسة، صدق الأداة، ثبات الأداة، إجراءات الدراسة، والتحليل الإحصائيّ.

2.3 منهج الدراسة:

استخدم الباحث المنهجَ الوصفيّ التحليليّ وهو طريقة في البحث عن الحاضر، وتهدف إلى تجهيز بيانات لإثبات فروض معينة تمّهيدَاً للإجابة عن تساؤلات محددة–سلفاً–بدقة تتعلّق بالظواهر الحاليّة والأحداث الراهنة التي يمكن جمع المعلومات عنها في زمان إجراء البحث وذلك باستخدام أدوات مناسبة (أبو سمرة والطيطي، 2020). والهدف منَ استخدام المنهج الوصفيّ هنا مَعرِفَة دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً.

3.3 مجتمّع الدراسة:

تكون مجتمّع الدراسة العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية والتي بلغ عددها (327) موظف تقريباً حسب إحصائيّة الأجهزة الأمنية الفلسطينية، وبناءً على مشكلّة الدراسة، موزعين حسب الأجهزة التي تضم وحدة الجرائم الإلكترونية، بحيث بلغ عدد الأفراد في جهاز الاستخبارات

(32) فرداً، و(144) في جهاز الشرطة، و(81) في جاهز المخابرات، (70) في جهاز الأمن الوقائي، فإنّ مجتمّع الدراسة المستهدف سيكون العاملين في وحدة الجرائم الإلكترونية.

4.3 عينة الدراسة:

أما عينة الدراسة، فقد اختيرت كالآتي:

أولاً –العينة الاستطلاعية (Pilot Study) اختيرت عينة استطلاعية مكونة من (30) من العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية، ومن خارج عينة الدراسة المستهدفة، وذلك بغرض التأكد من صلاحية ادوات الدراسة واستخدامها لحساب الصدق والثبات.

ثانياً– عينة الدراسة (Sample Study): تم حساب عينة الدراسة عن طريق معادلة ستيفن ثامسون (Thompson, 2012).

$$n = \frac{N \times p(1-p)}{[N-1 \times (d^2 \div z^2)] + p(1-p)}$$

حيث:

N: حجم المجتمع

Z: الدرجة المعيارية المقابلة لمستوى الدلالة 0.95 وتساوي 1.96.

d: نسبة الخطأ وتساوي 0.05.

P: القيمة الاحتمالية وتساوي 0.50

تكونت عينة الدراسة من العينة العشوائية المتاحة للمجتمّع الأصليّ المستهدف وجرى توزيع الاستبانة على العاملين في وحدة الجرائم الإلكترونية، وجرى استرجاع منها (178) استبانة حسب

متغيرات الدراسة التالية: الجنس، المؤهل العلمي، المسمى الوظيفي، سنوات الخبرة، الرتبة العسكرية، والجداول التالية توضّح خصائص العينة الديموغرافية (1.3).

جدول (1.3): خصائص العينة الديموغرافية

المتغير	الخيارات	العدد	النسبة المئوية
الجنس	ذكر	145	%81.5
	انثى	33	%18.5
المؤهل العلمي	دبلوم فأقل	33	%18.5
	بكالوريوس	100	%56.2
	دراسات عليا	45	%25.3
المسمّى الوظيفيّ	مدير	35	%19.7
	رئيس قسم	45	%25.3
	موظف	98	%55.0
عدد سنوات الخبرة	أقلّ من 10 سنوات	51	%28.7
	من 10–أقل 20 سنة	83	%46.6
	20 سنة فأكثر	44	%24.7
الرتبة العسكرية	نقيب فأقل	91	%51.1
	رائد	46	%25.8
	مقدم	29	%16.4
	عقيد	7	%3.9
	عميد فأعلى	5	%2.8

تشير نتائج الجدول (1.3) إلى ما يأتي:

- **متغير الجنس:** جاء أكبر عدد من المستجيبين من الذكور وعددهم (145) فرداً وبنسبة (81.5%) من عينة الدراسة، وأقلّهم عدّداً من الإناث وعددهم (33) وبنسبة (18.5%) من عينة الدراسة
- **متغير المؤهل العلميّ:** جاء أكبر عدد من المستجيبين من حملة البكالوريوس وعددهم (100) فرداً وبنسبة (56.2%) من عينة الدراسة، تلاه حملة درجة ماجستير وعددهم (45) وبنسبة

مئوية (25.3%)، وأقلّهم عدّداً من حملة دبلوم وعددهم (33) وبنسبة (18.5%) من عينة الدراسة.

- **أمّا فيما يَخُصّ متغير المسمّى الوظيفيّ:** فقد جاء أكبر عدد من المستجيبين من خيار (موظّف) وعددهم (98) فرداً وبنسبة (55.0%) من عينة الدراسة، تلاه رئيس قسم وعددهم (45) وبنسبة مئوية (25.3%)، ثم تلاه مدير وعددهم (35) وبنسبة مئوية (19.7%)؟
- **أمّا متغير عدد سنوات الخبرة:** فقد جاء أكبر عدد من المستجيبين من الفئة (من 10 – أقل من 20 سنة) وعددهم (83) فرداً وبنسبة (46.6%) من عينة الدراسة، تلاه ذوي الخبرة (أقلّ من 10 سنوات) وعددهم (51) وبنسبة مئوية (28.7%)، وأقلّهم عدّداً ممّن لديهم خبرة 20 سنة فأكثر وعددهم (44) فرداً وبنسبة (24.7%) من عينة الدراسة.
- **أمّا متغير الرتبة العسكرية:** فقد جاء أكبر عدد من المستجيبين من الفئة نقيب فأقل وعددهم (91) فرداً وبنسبة (51.1%) من عينة الدراسة، تلاه الفئة رائد وعددهم (46) وبنسبة مئوية (25.8%)، تلاه الفئة مقدم وعددهم (29) وبنسبة مئوية (16.4%)، تلاه الفئة عقيد وعددهم (7) وبنسبة مئوية (3.9%)، وأقلّهم عدّداً ذوي الفئة عميد فأعلى وعددهم (5) فرداً وبنسبة (2.8%) من عينة الدراسة.

5.3 أداة الدراسة

جرى تطوير استبانة بالاعتماد على الدراسات السابقة مكونة من قسمين: القسم الأول مكون من معلومات عامة عن المبحوثين تتضمن (الجنس، المؤهل العلمي، سنوات الخبرة، المسمى الوظيفي، الرتبة العسكرية) والقسم الثاني يضم فقرات التي تقسم إلى ثلاثة محاور وهي: المحور الأول يضم فقرات تقيس مستوى استخدام تطبيقات الذكاء الاصطناعي (AI)، والمحور الثاني يقيس الحد من انتشار الجرائم

الالكترونية، والمحور الثالث يقيس تميز أداء منتسبي الأجهزة الأمنية، وبعد ذلك يقوم الباحث بعمل مجموعة من الأسئلة تتمحور حول دور الذكاء الاصطناعي في الحد من انتشار الجرائم الالكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً.

6.3 صدق أداة الدراسة:

جرى التحقق من صدق أداة الدراسة من خلال الأخذ بآراء متخصصين في القيادة والإدارة الاستراتيجية في الجامعات الفلسطينية، وقد أبدى المحكمين آرائهم حول فقرات الاستبانة، وجرى الأخذ بذلك حتى خرجت الاستبانة في شكلها النهائي.

كما جرى التحقّقَ من صدق أداة الدراسة بحساب مُعامِل الارتباط بيرسون (Person correlation) لفقرات الدراسة مع الدرجة الكلّيّة للأداة، وذلك كما هو واضح في الجدول (2.3).

(2.3) نتائج مُعامِل الارتباط بيرسون (Person correlation) لمصفوفة ارتباط كلّ فقرة من فقرات المقياس مع الدرجة الكلّيّة للمقياس.

الرقم	المحور الأول: استخدام تطبيقات الذكاء الاصطناعي	قِيمة (ر)	القِيمة الاحتماليّة
	أولا: التعلم الآلي (Machine Learning)	0.641	0.00
.1	تستخدم خوارزميات التعلم الآلي لتحديد الأنشطة المشبوهة، ورصد الهجمات	0.541	0.00
.2	تحليل البيانات السابقة والتعلم منها للتنبؤ بأساليب الهجمات القادمة	0.641	0.00
.3	تصنيف رسائل البريد الاحتيالية أو التصيّدية بشكل دقيق	0.590	0.00
.4	تحديد الرسائل الخطيرة قبل وصولها للمستخدم	0.630	0.00
.5	تحليل الأدلة الرقمية بسرعة وبكفاءة	0.666	0.00
.6	تستخدم كميات ضخمة من البيانات لتدريب الأنظمة على مواجهة الهجمات السيبرانية المتقدمة	0.555	0.00
*	**ثانيا: التعلم العميق (Deep Learning)**	0.654	0.00
.7	تستخدم الدوائر الفلسطينية المختصة في مكافحة الجرائم الإلكتروني نماذج التعلم العميق في عملها	0.543	0.00
.8	يستخدم التعلم العميق نماذج مثل الشبكات العصبية لكشف البرمجيات الخبيثة	0.604	0.00

.9	يتم التعرف من خلال التعلم العميق على الرسائل والمواقع المزيفة للتصدي لهجمات التصيد	0.708	0.00
.10	يمكن لنماذج التعلم العميق كشف الهجمات غير المعروفة	0.720	0.00
.11	تستطيع خوارزميات التعلم العميق اكتشاف هجمات لم تسجل من قبل	0.663	0.00
.12	تساعد نماذج التعلم العميق في تمييز الأنشطة الشاذة التي قد تدل على اختراق الحساب	0.629	0.00
.13	تساعد نماذج التعلم العميق في الكشف عن حملات التضليل والابتزاز أو التخطيط لهجمات إلكترونية	0.565	0.00
المحور الثاني: الحد من انتشار الجرائم الالكترونية			
*	**أولاً: الاحتيال المالي**	0.801	0.00
.14	تحذير المواطنين من التعامل مع أية رسائل تطالبه بإدخال بياناته البنكية	0.600	0.00
.15	تعريف المؤسسات المصرفية المحلية بأشكال ومخاطر الاحتيال المالي	0.622	0.00
.16	تستخدم أنظمة مراقبة ذكية تعتمد على الذكاء الاصطناعي لمكافحة الاحتيال المالي	0.612	0.00
.17	استخدام نماذج التعلم الآلي للتعرف على محاولات اختراق الحسابات المالية	0.577	0.00
.18	تستخدم أنظمة التعرف على السلوك لحماية البنوك والمصارف	0.618	0.00
.19	تستخدم خوارزميات التعرف على الوجوه، وبصمات الصوت، وأنماط الكتابة في تتبع هوية الجناة في مجال التحايل المالي	0.574	0.00
*	**ثانياً: سرقة البيانات**	0.831	0.00
.20	تنظم حملات توعية مستمرة لتحذير المواطنين من سرقة بياناتهم	0.514	0.00
.21	تتوفر البنية التحتية لمكافحة سرقة البيانات الإلكترونية	0.565	0.00
.22	تتخذ إجراءات احترازية للحفاظ على سرية البيانات الإلكترونية للمواطنين	0.707	0.00
.23	تعريف المواطنين بحالات متنوعة حول سرقة البيانات	0.584	0.00
.24	التعامل بشكل فعّال مع حالات سرقة البيانات	0.647	0.00
.25	تسترجع المؤسسات والدوائر المختصة البيانات في حالة تعرضها للسرقة	0.676	0.00
*	**ثالثاً: انتهاك الخصوصية**	0.820	0.00
.26	تنتشر ظاهرة انتهاك الخصوصية الإلكترونية للمواطنين	0.482	0.00
.27	توعية المواطنين بعدم تبادل بياناتهم الخاصة مع أيٍ كان	0.541	0.00
.28	تنسق وزارة الداخلية مع المؤسسات المختصة الأخرى في مجال الأمن السيبراني	0.673	0.00
.29	مراقبة الشبكات لاكتشاف أي نشاط مشبوه أو غير مصرح به	0.653	0.00
.30	تستخدم أنظمة كشف التسلل أو منعه	0.691	0.00
.31	متابعة الأفراد أو المؤسسات التي تعرضت للانتهاك	0.677	0.00
*	**رابعاً: نشر الشائعات والبيانات المضللة**	0.675	0.00
.32	تستخدم خوارزميات الذكاء الاصطناعي لرصد المحتوى المشبوه	0.605	0.00

.33	التعاون مع شركات التكنولوجيا مثل تويتر وفيس بوك لحذف المحتوى المضلل	0.618	0.00
.34	استقطاب الأفراد ذوي الخبرة في مجال مكافحة الجرائم الإلكترونية للعمل في الأجهزة المختصة	0.618	0.00
.35	إطلاق حملات تحذر من تصديق أو مشاركة كل ما ينشر	0.607	0.00
.36	نشر أدوات تساعد الناس على التمييز بين الصحيح والزائف	0.674	0.00
.37	اتخاذ إجراءات قانونية صارمة بحق مروجي الشائعات المضللة	0.624	0.00
المحور الثالث: تميز أداء منتسبي الأجهزة الأمنية			
*	**أولاً: تنفيذ المهام**	0.807	0.00
.38	أُظهر حرصاً دائماً على جودة العمل الذي أقدمه.	0.525	0.00
.39	أتمكّن من استخدام الأدوات التكنولوجية المطلوبة لإنجاز المهام بكفاءة.	0.570	0.00
.40	أراجع نتائج عملي بشكل دائم لضمان دقتها.	0.598	0.00
.41	أتعامل مع ضغوط العمل بكفاءة دون أن يؤثر ذلك على جودة أدائي.	0.662	0.00
.42	التعاون مع أطراف دولية لتنفيذ مهام العمل	0.607	0.00
*	**ثانياً: التحلي بالمسؤولية**	0.795	0.00
.43	أبادر في تقديم الملاحظات البناءة لتحسين العمل الجماعي.	0.509	0.00
.44	أعمل على خلق بيئة عمل إيجابية بين زملائي.	0.601	0.00
.45	أُظهر احترامًا دائمًا لقوانين المؤسسة وثقافتها التنظيمية.	0.519	0.00
.46	أساند زملائي خلال الأزمات أو أوقات الضغط الكبير في العمل.	0.627	0.00
*	**ثالثاً: التطور الوظيفي**	0.802	0.00
.47	أتعامل مع التغييرات المفاجئة في المهام بكفاءة.	0.601	0.00
.48	أبحث باستمرار عن فرص لتطوير مهاراتي في استخدام الذكاء الاصطناعي.	0.663	0.00
.49	أتعلم من التجارب السابقة لتعديل طريقة عملي نحو الأفضل.	0.598	0.00
.50	أتكيف مع اختلاف ظروف العمل دون التأثير على الإنتاجية.	0.590	0.00
*	**رابعاً: تحقيق الأهداف**	0.721	0.00
.51	أضع خطة واضحة لتحقيق المهام المرتبطة بأهداف المؤسسة الأمنية	0.564	0.00
.52	أتابع مؤشرات الأداء لضمان تحقيق الأهداف بدقة.	0.556	0.00
.53	أستخدم التحليل الذكي للبيانات لتقييم فعالية العمليات الأمنية.	0.667	0.00
.54	أعمل باستمرار على تحسين مستوى أدائي لتحقيق الأهداف العامة للمؤسسة.	0.629	0.00

تشير المعطيات الواردة في الجدول (2.3) إلى أنّ جميع قِيم مصفوفة ارتباط فقرات كلّ مجال مع الدرجة الكلّيّة للمجال دالة إحصائيّاً، مّا يشير إلى قوة الاتساق الداخليّ لفقرات كلّ مجال من مجالات

الأداة، وأنها تشترك معا في قياس دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً، على ضوء المقياس الذي تمّ اعتمّاده.

7.3 ثبات أداة الدراسة:

حسب الباحث الثبات بطريقة الاتساق الداخليّ، يقصد بالاتساق الداخليّ لأسئلة الاستبانة بأنها قوة الارتباط بين درجات كلّ مجال ودرجات أسئلة الاستبانة الكلّيّة، والصّدق ببساطة هو أنّ تقيسَ أسئلةُ الاستبانة أو الاختبار ما وضعت لقياسه، أيّ يقيس فعلاً الوظيفة التي يفترض أنه يقيسها. ولمَعرِفَة الاتساق الداخليّ جرى حساب معادلة الثبات كرو نباخ ألفا، وذلك كما هو موضّح في الجدول (3.3).

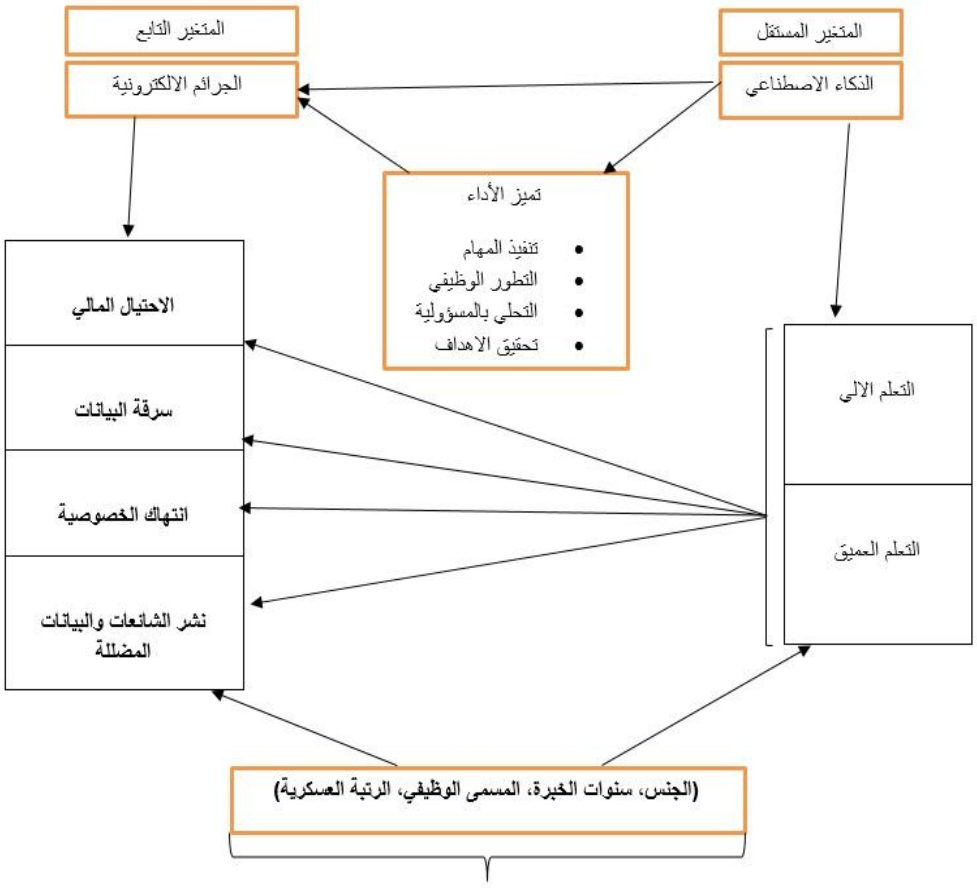
(3.3) نتائج مُعامِل كرو نباخ ألفا لثبات أداة الدراسة

المحور	المجال	عدد فقرات	قِيمة ألفا
استخدام تطبيقات الذكاء الاصطناعي	التعلم الآلي	6	0.84
	التعلم العميق	7	0.86
	الدرجة الكلّيّة	13	0.91
الحد من انتشار الجرائم الإلكترونية	الاحتيال المالي	6	0.84
	سرقة البيانات	6	0.84
	انتهاك الخصوصية	6	0.83
	نشر الشائعات والبيانات المضللة	6	0.85
	الدرجة الكلّيّة	24	0.94
تميز أداء منتسبي الأجهزة الأمنية	تنفيذ المهام	5	0.81
	التحلي بالمسؤولية	4	0.87
	التطور الوظيفي	4	0.78
	تحقيق الأهداف	4	0.83
	الدرجة الكلّيّة	17	0.93
للإجماليّ	الدرجة الكلّيّة	54	0.96

تشير المعطيات الواردة في الجدول (3.3) إلى أنّ قِيمة ثبات أداة الدراسة عند الدرجة الكلّيّة بلغت (0.96) وبذلك يتمّتع المقياس بدرجة عالية من الثبات وقابلة لاعتمّادها لتحقيق أهداف الدراسة.

أمّا محاور الاستبانة فبلغت قِيمة مُعامِل ألفا كرو نباخ لمحور استخدام تطبيقات الذكاء الاصطناعي؛ إذ تتراوح بين (0.84 – 0.86)، بينما لجميع المجالات (0.91)، ولمحور الحد من انتشار الجرائم الإلكترونية حيث تتراوح بين (0.83 – 0.85)، بينما لجميع المجالات (0.94)، ولمحور تميز أداء منتسبي الأجهزة الأمنية حيث تتراوح بين (0.78 – 0.87)، بينما لجميع المجالات (0.93).

أنموذج الدراسة:



الشكل رقم(1): أنموذج الدراسة

المصدر: من اعداد الباحث

8.3 متغيرات الدراسة

أولا: المتغير المستقل: الذكاء الاصطناعي ويشمل الابعاد:

-التعلم الالي

-التعلم العميق.

ثانيا: المتغير التابع: انتشار الجرائم الالكترونية، ويشمل الابعاد:

- الاحتيال المالي.

- سرقة البيانات.

- انتهاك الخصوصية.

- نشر الشائعات والبيانات المضللة.

ثالثا: المتغير الوسيط: تميز أداء العاملين ويشمل الابعاد:

- تنفيذ المهام.

- التطور الوظيفي.

- التحلي بالمسؤولية.

- تحقيق الأهداف.

9.3 إجراءات تنفيذ لدراسة:

اتبع الباحث الخطوات الآتية عند إعداد الدراسة:

- قام الباحث بالاطلاع على الأدب النظري والدراسات السابقة والبحوث العلمية والمراجع العربية والأجنبية ذات العلاقة.
- تصميم أداة الدراسة (الاستبانة) والتحقق من صدقها وثباتها.
- تجهيز الاستبانة وإعدادها بصورتها النهائية بشكل الإلكتروني.
- تم توزيع الاستبانة على عينة استطلاعية لحساب الصدق والثبات لأداة الدراسة.

- تم توزيع الاستبانة بعد الحصول على كتاب رسمي من عمادة كلية الدراسات العليات والبحث العلمي في الجامعة، لتسهيل مهمة جمع بيانات الدراسة الحالية.
- وبعد عملية توزيع الاستبانة الإلكترونية ومتابعة الردود وتحميلها من خلال تطبيق نماذج جوجل تم تفريغ البيانات على ملف (Excel) تمهيداً لتجهيزها لعملية التحليل اللازمة باستخدام التحليل الإحصائي (SPSS).
- إجراء المعالجات اللازمة لاستخراج النتائج، وتحليلها، ومناقشتها، ومقارنتها مع الدراسات السابقة، واقتراح التوصيات المناسبة.

10.3 الأساليب الإحصائيّة:

وزّع الباحث الاستبانة وحلّلتها من خلال برنامج (SPSS) وجرى استخدام الاختبارات الإحصائيّة التالية:

1- التكرارات والنسب المئوية.

2- المتوسّطات الحسابيّة، الانحرافات المعياريّة.

3- اختبار كرو نباخ ألفا لمَعرِفَة ثبات فقرات الاستبانة.

4- مُعامِل الارتباط بيرسون (Person correlation) لمَعرِفَة صدق فقرات الاستبانة.

5- اختبار تحليل الانحدار المتُعدّد لمعرفة أثر أبعاد المتغير المستقل على التابع ومعرفة تأثير المتغير الوسيط.

6- اختبار (ت) (Independent-Sample T-Test) لمَعرِفَة الفرق في المتوسّطات.

7- اختبار تحليل التباين الأحادي (One-Way Analysis of Variance) للمقارنة بين المتوسّطات أو التَوصّل إلى قرار يتعلّق بوجود فروق بين متوسّطات أو عدم وجودها.

مفتاح التصحيح:

- جرى تفريغ الاستبانة حسب مقياس ليكرث الخماسيّ بحيث نعطي الدرجات التالية للاختيارات وهي:

موافق بشدة	موافق	متوسّطة	غير موفق	غير موفق بشدة
5	4	3	2	1

لفهم الدراسة يمكن الاستعانة بمفتاح المتوسّطات الحسابيّة التالية كما في (4.3).

(4.3) مفتاح التصحيح لفقرات المقياس

المتوسّط الحسابيّ	المقياس	الوزن النسبيّ
2.33-1	مُنخفضة	%20 - %46.6
3.66-2.34	متوسّطة	%46.8 -%73.2
5- 3.67	مرتفعة	%73.4 - %100

الفصل الرابع

نتائج الدراسة

1.4 تحليل نتائج الدراسة:

الإجابة عن التساؤل الأول: ما مستوى تطبيق الذكاء الاصطناعي لدى العاملين في وحدة الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية؟

للإجابة عنِ السؤال السابقِ جرى استخراج المتوسّطات الحسابيّة والانحرافات المعياريّة لمستوى تطبيق الذكاء الاصطناعي لدى العاملين في وحدة الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية، وذلك كما هو موضّح في الجداول (1.4) (2.4):

جداول (1.4) المتوسّطات الحسابيّة والانحرافات المعياريّة لأبعاد تطبيق الذكاء الاصطناعي

الأبعاد	المتوسّط الحسابيّ	الانحراف المعياريّ	الوزن النسبيّ	الدرجة
التعلم الآلي	4.03	0.59	%80.6	مرتفعة
التعلم العميق	3.85	0.64	%77.0	مرتفعة
الدرجة الكلّيّة	**3.94**	**0.57**	**%78.8**	**مرتفعة**

يلاحظ من الجدول (1.4) ما يأتي:

- **مستوى تطبيق الذكاء الاصطناعي:** أن الدرجة الكلّيّة جاءت مرتفعة؛ إذ بلغ الوسط الحسابيّ (3.94) والوزن النسبيّ (78.8%)، وكان أعلى بعد أهمّية هي (التعلم الآلي) ووسطها الحسابيّ (4.03) ووزنها النسبيّ (80.6%)، وأقلّ بعد اهتمّامًا هي (التعلم العميق) ووسطها الحسابيّ (3.85) ووزنه النسبيّ (77.0%).

هنا يمكن القول، إنّ العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية تعمل على تطبيق الذكاء الاصطناعي بدرجة مرتفعة وذلك بالتركيز على بعد التعلم الآلي، ونجد أن هناك اهتماماً بهذا البعد من أجل الوصول إلى أعلى مستوى من المهارات الأساسية التي تدعم تطبيق الذكاء الاصطناعي وتعتبر

التعلم الآلي من أجل الوصول إلى العلم العميق لذا فالمتعلم يتدرج في تطبيق المهارات وصولاً إلى التعلم العميق من أجل استغلال تطبيقات الذكاء الاصطناعي لتسهيل عمل وحدة الجرائم الإلكترونية في تحقيق أهداف الوحدة.

وجاءت النتيجة الكلية لتطبيق الذكاء الاصطناعي بدرجة مرتفعة، والجدول (2.4) يبين مستوى تطبيق الذكاء الاصطناعي.

جداول (2.4) المتوسّطات الحسابيّة والانحرافات المعياريّة لقياس مستوى تطبيق الذكاء الاصطناعي ورتبت الفقرات تنازلياً حسب المتوسط الحسابي

*	التعلم الآلي	المتوسّط الحسابيّ	الانحراف المعياريّ	الوزن النسبيّ	الدرجة
.1	تستخدم خوارزميات التعلم الآلي لتحديد الأنشطة المشبوهة، ورصد الهجمات	4.16	0.70	83.3	مرتفعة
.2	تستخدم كميات ضخمة من البيانات لتدريب الأنظمة على مواجهة الهجمات السيبرانية المتقدمة	4.11	0.80	82.1	مرتفعة
.3	يجري تحليل البيانات السابقة والتعلم منها للتنبؤ بأساليب الهجمات القادمة	4.07	0.69	81.3	مرتفعة
.4	يجري تصنيف رسائل البريد الاحتيالية أو التصيّدية بشكل دقيق	4.00	0.82	80.0	مرتفعة
.5	يجري تحليل الأدلة الرقمية بسرعة وبكفاءة	3.95	0.80	79.0	مرتفعة
.6	يجري تحديد الرسائل الخطيرة قبل وصولها للمستخدم	3.93	0.91	78.5	مرتفعة
	الدرجة الكلّيّة	**4.03**	**0.59**	**%80.6**	**مرتفعة**
*	**التعلم العميق**	**المتوسّط الحسابيّ**	**الانحراف المعياريّ**	**الوزن النسبيّ**	**الدرجة**
.7	تساعد نماذج التعلم العميق في الكشف عن حملات التضليل والابتزاز أو التخطيط لهجمات إلكترونية	4.01	0.80	80.1	مرتفعة
.8	يمكن لنماذج التعلم العميق كشف الهجمات غير المعروفة	3.96	0.85	79.1	مرتفعة
.9	تساعد نماذج التعلم العميق في تمييز الأنشطة الشاذة التي قد تدل على اختراق الحساب	3.91	0.78	78.2	مرتفعة
.10	يجري تعرف من خلال التعلم العميق على الرسائل والمواقع المزيفة للتصدي لهجمات التصيّد	3.85	0.81	77.0	مرتفعة
.11	يستخدم التعلم العميق نماذج مثل الشبكات العصبية لكشف البرمجيات الخبيثة	3.79	0.92	75.8	مرتفعة
.12	تستطيع خوارزميات التعلم العميق اكتشاف هجمات لم تسجل	3.76	0.90	75.2	مرتفعة

	من قبل				
13.	تستخدم الدوائر الفلسطينية المختصة في مكافحة الجرائم الإلكتروني نماذج التعلم العميق في عملها	3.75	0.97	74.9	مرتفعة
	الدرجة الكلّيّة	**3.85**	**0.64**	**%77.0**	**مرتفعة**

يُلاحظ منَ نتائج الجدول رقم (2.4) ما يأتي:

- فيما يَخُصّ **بالتعلم الآلي**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.03) والوزن النسبيّ (80.6%)، وكانت أكثر الفقرات أهمّية (تستخدم خوارزميات التعلم الآلي لتحديد الأنشطة المشبوهة، ورصد الهجمات) حيث بلغ الوسط الحسابيّ لها (4.16) والوزن النسبيّ (83.3%)، بينما أقلّ الفقرات أهمّية (يتم تحديد الرسائل الخطيرة قبل وصولها للمستخدم) وبلغ الوسط الحسابيّ لها (3.93) والوزن النسبيّ (78.5%).
- فيما يَخُصّ **بالتعلم العميق**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (3.85) والوزن النسبيّ (77.0%)، وكانت أكثر الفقرات أهمّية (تساعد نماذج التعلم العميق في الكشف عن حملات التضليل والابتزاز أو التخطيط لهجمات إلكترونية) حيث بلغ الوسط الحسابيّ لها (4.01) والوزن النسبيّ (80.1%)، بينما أقلّ الفقرات أهمّية () وبلغ الوسط الحسابيّ لها (3.75) والوزن النسبيّ (74.9%).

الإجابة عن التساؤل الثاني: ما مستوى الحد من انتشار الجرائم الإلكترونية لدى العاملين في وحدة الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية؟

للإجابة عنِ السؤال السابقِ جرى استخراج المتوسّطات الحسابيّة والانحرافات المعياريّة لمستوى الحد من انتشار الجرائم الإلكترونية لدى العاملين في وحدة الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية، وذلك كما هو موضّح في الجداول (3.4) (4.4):

جداول (3.4) المتوسّطات الحسابيّة والانحرافات المعياريّة لأبعاد الحد من انتشار الجرائم الإلكترونية

الأبعاد	المتوسّط الحسابيّ	الانحراف المعياريّ	الوزن النسبيّ	الدرجة
الاحتيال المالي	4.12	0.62	%82.4	مرتفعة
سرقة البيانات	4.07	0.65	%81.4	مرتفعة
انتهاك الخصوصية	4.01	0.67	%80.2	مرتفعة
نشر الشائعات والبيانات المضللة	3.98	0.69	%79.6	مرتفعة
الدرجة الكلّيّة	**4.04**	**0.58**	**%80.8**	**مرتفعة**

يلاحظ من الجدول(3.4) ما يلي:

- **مستوى الحد من انتشار الجرائم الإلكترونية:** أن الدرجة الكلّيّة جاءت مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.04) والوزن النسبيّ (80.8%)، وكان أعلى بعد أهمّية هي (الاحتيال المالي) ووسطها الحسابيّ (4.12) ووزنها النسبيّ (82.6%)، وأقلّ بعد اهتمّامًا هي (نشر الشائعات والبيانات المضللة) ووسطها الحسابيّ (3.98) ووزنه النسبيّ (79.6%).

هنا يمكن القول، إنّ العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية تعمل على الحد من الجرائم الإلكترونية بدرجة مرتفعة وذلك بالتركيز على بعد الاحتيال المالي، ونجد أن هناك اهتماماً بهذا البعد، ما يعكس ضرورة التركيز على هذا النوع من الجرائم نظرًا لتأثيره الكبير على المجتمع. في المقابل، وتجد أن سرقة البيانات يمكن استخدامها في التأثير على أمن المجتمع لذا تعمل وحدة الجرائم على مكافحتها بشكل مرتفع، فنجد أن انتهاك الخصوصية يتم التعامل معه في وحدة الجرائم الإلكترونية

وصولاً إلى الحد من تلك الانتهاكات، كما أن نشر الشائعات والبيانات المضللة غالباً ما تكون من أجل الاخلال في النظام لذا تعمل وحدة الجرائم الإلكترونية متابعتها بشكل مستمر.

وجاءت النتيجة الكلية لمستوى الحد من انتشار الجرائم الإلكترونية بدرجة مرتفعة، والجدول (4.4) يبين مستوى الحد من انتشار الجرائم الإلكترونية.

جداول (4.4) المتوسّطات الحسابيّة والانحرافات المعياريّة لقياس مستوى الحد من انتشار الجرائم الإلكترونية ورتبت الفقرات تنازلياً حسب المتوسط الحسابي

*	الاحتيال المالي	المتوسّط الحسابيّ	الانحراف المعياريّ	الوزن النسبيّ	الدرجة
.14	يجري تحذير المواطنين من التعامل مع أية رسائل تطالبه بإدخال بياناته البنكية	4.35	0.78	87.0	مرتفعة
.15	يجري تعريف المؤسسات المصرفية المحلية بأشكال ومخاطر الاحتيال المالي	4.23	0.91	84.6	مرتفعة
.16	تستخدم خوارزميات التعرف على الوجوه، وبصمات الصوت، وأنماط الكتابة في تتبع هوية الجناة في مجال التحايل المالي	4.08	0.81	81.7	مرتفعة
.17	تستخدم أنظمة مراقبة ذكية تعتمد على الذكاء الاصطناعي لمكافحة الاحتيال المالي	4.07	0.82	81.5	مرتفعة
.18	تستخدم أنظمة التعرف على السلوك لحماية البنوك والمصارف	4.05	0.83	81.0	مرتفعة
.19	تستخدم نماذج التعلم الآلي للتعرف على محاولات اختراق الحسابات المالية	3.97	0.89	79.4	مرتفعة
	الدرجة الكلّيّة	**4.12**	**0.62**	**%82.4**	**مرتفعة**
*	**سرقة البيانات**	**المتوسّط الحسابيّ**	**الانحراف المعياريّ**	**الوزن النسبيّ**	**الدرجة**
.20	تنظم حملات توعية مستمرة لتحذير المواطنين من سرقة بياناتهم	4.24	0.82	84.7	مرتفعة
.21	تتخذ إجراءات احترازية للحفاظ على سرية البيانات الإلكترونية للمواطنين	4.16	0.82	83.3	مرتفعة
.22	تعرف المواطنين بحالات متنوعة حول سرقة البيانات	4.11	0.80	82.1	مرتفعة
.23	يجري التعامل بشكل فعّال مع حالات سرقة البيانات	4.02	0.92	80.3	مرتفعة
.24	تسترجع المؤسسات والدوائر المختصة البيانات في حالة تعرضها للسرقة	3.97	0.93	79.4	مرتفعة

.25	تتوفر البنية التحتية لمكافحة سرقة البيانات الإلكترونية	3.93	0.92	78.7	مرتفعة
	الدرجة الكلّيّة	**4.07**	**0.65**	**%81.4**	**مرتفعة**
*	**انتهاك الخصوصية**	**المتوسّط الحسابيّ**	**الانحراف المعياريّ**	**الوزن النسبيّ**	**الدرجة**
.26	توعية المواطنين بعدم تبادل بياناتهم الخاصة مع أيٍ كان	4.25	0.77	84.9	مرتفعة
.27	تنتشر ظاهرة انتهاك الخصوصية الإلكترونية للمواطنين	4.10	0.91	81.9	مرتفعة
.28	تنسق وزارة الداخلية مع المؤسسات المختصة الأخرى في مجال الأمن السيبراني	4.04	0.94	80.9	مرتفعة
.29	متابعة الأفراد أو المؤسسات التي تعرضت للانتهاك	4.00	0.86	80.0	مرتفعة
.30	تستخدم أنظمة كشف التسلل أو منعه	3.88	0.95	77.5	مرتفعة
.31	مراقبة الشبكات لاكتشاف أي نشاط مشبوه أو غير مصرح به	3.83	0.98	76.5	مرتفعة
	الدرجة الكلّيّة	**4.01**	**0.67**	**%80.2**	**مرتفعة**
	نشر الشائعات والبيانات المضللة	**المتوسّط الحسابيّ**	**الانحراف المعياريّ**	**الوزن النسبيّ**	**الدرجة**
.32	إطلاق حملات تحذر من تصديق أو مشاركة كل ما ينشر	4.08	0.85	81.6	مرتفعة
.33	استقطاب الأفراد ذوي الخبرة في مجال مكافحة الجرائم الإلكترونية للعمل في الأجهزة المختصة	4.04	0.89	80.8	مرتفعة
.34	تستخدم خوارزميات الذكاء الاصطناعي لرصد المحتوى المشبوه	4.02	0.82	80.5	مرتفعة
.35	اتخاذ إجراءات قانونية صارمة بحق مروجي الشائعات المضللة	3.99	0.96	79.8	مرتفعة
.36	نشر أدوات تساعد الناس على التمييز بين الصحيح والزائف	3.95	0.96	79.0	مرتفعة
.37	التعاون مع شركات التكنولوجيا مثل تويتر وفيس بوك لحذف المحتوى المضلل	3.80	1.04	76.1	مرتفعة
	الدرجة الكلّيّة	**3.98**	**0.69**	**%79.6**	**مرتفعة**

يُلاحظ منَ نتائج الجدول رقم (4.4) ما يأتي:

- فيما يَخُصّ **بالاحتيال المالي**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.12) والوزن النسبيّ (82.4%)، وكانت أكثر الفقرات أهمّية (يتم تحذير المواطنين من التعامل مع أية رسائل تطالبه بإدخال بياناته البنكية)؛ إذ بلغ الوسط الحسابيّ لها (4.35) والوزن النسبيّ

(87.0%)، بينما أقلّ الفقرات أهمّية (يتم استخدام نماذج التعلم الآلي لتعرف محاولات اختراق الحسابات المالية) وبلغ الوسط الحسابيّ لها (3.97) والوزن النسبيّ (79.4%).

- فيما يَخُصّ **بسرقة البيانات**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.07) والوزن النسبيّ (81.4%)، وكانت أكثر الفقرات أهمّية (تنظم حملات توعية مستمرة لتحذير المواطنين من سرقة بياناتهم)؛ إذ بلغ الوسط الحسابيّ لها (4.24) والوزن النسبيّ (84.7%)، بينما أقلّ الفقرات أهمّية (تتوفر البنية التحتية لمكافحة سرقة البيانات الإلكترونية) وبلغ الوسط الحسابيّ لها (3.93) والوزن النسبيّ (78.7%).
- **فيما يَخُصّ بانتهاك الخصوصية**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.01) والوزن النسبيّ (80.2%)، وكانت أكثر الفقرات أهمّية (يتم توعية المواطنين بعدم تبادل بياناتهم الخاصة مع أيٍ كان)؛ إذ بلغ الوسط الحسابيّ لها (4.25) والوزن النسبيّ (84.9%)، بينما أقلّ الفقرات أهمّية (يتم مراقبة الشبكات لاكتشاف أي نشاط مشبوه أو غير مصرح به) وبلغ الوسط الحسابيّ لها (3.83) والوزن النسبيّ (76.5%).
- **فيما يَخُصّ بنشر الشائعات والبيانات المضللة**، فقد جاءت الدرجة الكلّيّة مرتفعة حيث بلغ الوسط الحسابيّ (3.98) والوزن النسبيّ (79.6%)، وكانت أكثر الفقرات أهمّية (يتم إطلاق حملات تحذر من تصديق أو مشاركة كل ما ينشر)؛ إذ بلغ الوسط الحسابيّ لها (4.08) والوزن النسبيّ (81.6%)، بينما أقلّ الفقرات أهمّية (يتم التعاون مع شركات التكنولوجيا مثل تويتر وفيس بوك لحذف المحتوى المضلل) وبلغ الوسط الحسابيّ لها (3.80) والوزن النسبيّ (76.1%).

الإجابة عن التساؤل الثالث: ما مستوى تميز الأداء لدى العاملين في وحدة الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية؟

للإجابة عنِ السؤال السابقِ جرى استخراج المتوسّطات الحسابيّة والانحرافات المعياريّة لمستوى تميز الأداء لدى العاملين في وحدة الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية، وذلك كما هو موضّح في الجداول (5.4) (6.4):

جداول (5.4) المتوسّطات الحسابيّة والانحرافات المعياريّة لأبعاد تميز الأداء

الأبعاد	المتوسّط الحسابيّ	الانحراف المعياريّ	الوزن النسبيّ	الدرجة
تنفيذ المهام	4.10	0.61	%82.0	مرتفعة
التحلي بالمسؤولية	4.28	0.62	%85.6	مرتفعة
التطور الوظيفي	4.23	0.56	%84.6	مرتفعة
تحقيق الأهداف	4.18	0.60	%83.6	مرتفعة
الدرجة الكلّيّة	**4.20**	**0.52**	**%84.0**	**مرتفعة**

يلاحظ من الجدول (5.4) ما يلي:

- **مستوى تميز الأداء:** أن الدرجة الكلّيّة جاءت مرتفعة حيث بلغ الوسط الحسابيّ (4.20) والوزن النسبيّ (84.0%)، وكان أعلى بعد أهمّية هي (التحلي بالمسؤولية) ووسطها الحسابيّ (4.28) ووزنها النسبيّ (85.6%)، وأقلّ بعد اهتمّامًا هي (تنفيذ المهام) ووسطها الحسابيّ (4.10) ووزنه النسبيّ (82.0%).

هنا يمكن القول، إن العاملين في وحدة الجرائم الإلكترونية في الأجهزة الأمنية غالباً ما يتم اختيارهم من أفضل العاملين في اتقان المهارات الحاسوبية، لأنهم يتعاملون مع العديد من المهام التي تتطلب مهارة عالية من أجل الحفاظ على أمن الوطن والمواطن، فنجد أن التحلي بالمسؤولية يتمتع بها معظم العاملين في وحدة الجرائم الإلكترونية، ومع التطور المستمر في البرامج الحاسوبية نجد أن التطور الوظيفي يحظى بأهمية لدى العاملين من أجل تحقيق الأهداف المنشودة خلال تنفيذ المهام.

وجاءت النتيجة الكلية لمستوى تميز الأداء بدرجة مرتفعة، والجدول (6.4) يبين مستوى تميز الأداء.

جداول (6.4) المتوسّطات الحسابيّة والانحرافات المعياريّة لقياس مستوى تميز الأداء ورتبت الفقرات تنازلياً حسب المتوسط الحسابي

*	تنفيذ المهام	المتوسّط الحسابيّ	الانحراف المعياريّ	الوزن النسبيّ	الدرجة
38.	أُظهر حرصاً دائماً على جودة العمل الذي أقدمه.	4.35	0.71	87.0	مرتفعة
39.	أراجع نتائج عملي بشكل دائم لضمان دقتها.	4.19	0.76	83.7	مرتفعة
40.	أتعامل مع ضغوط العمل بكفاءة دون أن يؤثر ذلك على جودة أدائي.	4.17	0.76	83.4	مرتفعة
41.	أتمكّن من استخدام الأدوات التكنولوجية المطلوبة لإنجاز المهام بكفاءة.	4.16	0.82	83.3	مرتفعة
42.	يتم التعاون مع أطراف دولية لتنفيذ مهام العمل	3.65	0.98	72.9	متوسطة
	الدرجة الكلّيّة	**4.10**	**0.61**	**%82.0**	**مرتفعة**
*	**التحلي بالمسؤولية**	**المتوسّط الحسابيّ**	**الانحراف المعياريّ**	**الوزن النسبيّ**	**الدرجة**
43.	أساند زملائي خلال الأزمات أو أوقات الضغط الكبير في العمل.	4.32	0.74	86.4	مرتفعة
44.	أُظهر احترامًا دائمًا لقوانين المؤسسة وثقافتها التنظيمية.	4.29	0.74	85.8	مرتفعة
45.	أعمل على خلق بيئة عمل إيجابية بين زملائي.	4.28	0.73	85.5	مرتفعة
46.	أبادر في تقديم الملاحظات البناءة لتحسين العمل الجماعي.	4.24	0.71	84.7	مرتفعة
	الدرجة الكلّيّة	**4.28**	**0.62**	**%85.6**	**مرتفعة**
*	**التطور الوظيفي**	**المتوسّط الحسابيّ**	**الانحراف المعياريّ**	**الوزن النسبيّ**	**الدرجة**
47.	أتعلم من التجارب السابقة لتعديل طريقة عملي نحو الأفضل.	4.33	0.68	86.5	مرتفعة
48.	أبحث باستمرار عن فرص لتطوير مهاراتي في استخدام الذكاء الاصطناعي.	4.22	0.77	84.5	مرتفعة
49.	أتعامل مع التغييرات المفاجئة في المهام بكفاءة.	4.20	0.68	84.0	مرتفعة
50.	أتكيف مع اختلاف ظروف العمل دون التأثير على الإنتاجية.	4.17	0.77	83.5	مرتفعة
	الدرجة الكلّيّة	**4.23**	**0.56**	**%84.6**	**مرتفعة**
	تحقيق الأهداف	**المتوسّط الحسابيّ**	**الانحراف المعياريّ**	**الوزن النسبيّ**	**الدرجة**
51.	أعمل باستمرار على تحسين مستوى أدائي لتحقيق الأهداف العامة للمؤسسة.	4.30	0.75	86.0	مرتفعة
52.	أضع خطة واضحة لتحقيق المهام المرتبطة بأهداف المؤسسة الأمنية	4.27	0.65	85.4	مرتفعة

53.	أتابع مؤشرات الأداء لضمان تحقيق الأهداف بدقة.	4.13	0.73	82.6	مرتفعة
54.	أستخدم التحليل الذكي للبيانات لتقييم فعالية العمليات الأمنية.	4.06	0.83	81.1	مرتفعة
	الدرجة الكلّيّة	**4.18**	**0.60**	**%83.6**	**مرتفعة**

يُلاحظ منَ نتائج الجدول رقم (6.4) ما يأتي:

- فيما يَخُصّ **بتنفيذ المهام**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.10) والوزن النسبيّ (82.0%)، وكانت أكثر الفقرات أهمّية (أُظهر حرصاً دائماً على جودة العمل الذي أقدمه) ؛ إذ بلغ الوسط الحسابيّ لها (4.35) والوزن النسبيّ (87.0%)، بينما أقلّ الفقرات أهمّية (يتم التعاون مع أطراف دولية لتنفيذ مهام العمل) وبلغ الوسط الحسابيّ لها (3.65) والوزن النسبيّ (72.9%).
- فيما يَخُصّ **بالتحلي بالمسؤولية**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.28) والوزن النسبيّ (85.6%)، وكانت أكثر الفقرات أهمّية (أساند زملائي خلال الأزمات أو أوقات الضغط الكبير في العمل) ؛ إذ بلغ الوسط الحسابيّ لها (4.32) والوزن النسبيّ (86.4%)، بينما أقلّ الفقرات أهمّية (أبادر في تقديم الملاحظات البناءة لتحسين العمل الجماعي) وبلغ الوسط الحسابيّ لها (4.24) والوزن النسبيّ (84.7%).
- فيما يَخُصّ **بالتطور الوظيفي**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.23) والوزن النسبيّ (84.6%)، وكانت أكثر الفقرات أهمّية (أتعلم من التجارب السابقة لتعديل طريقة عملي نحو الأفضل) ؛ إذ بلغ الوسط الحسابيّ لها (4.33) والوزن النسبيّ (86.5%)، بينما أقلّ الفقرات أهمّية (أتكيف مع اختلاف ظروف العمل دون التأثير على الإنتاجية) وبلغ الوسط الحسابيّ لها (4.17) والوزن النسبيّ (83.5%).
- فيما يَخُصّ **بتحقيق الأهداف**، فقد جاءت الدرجة الكلّيّة مرتفعة؛ إذ بلغ الوسط الحسابيّ (4.18) والوزن النسبيّ (83.6%)، وكانت أكثر الفقرات أهمّية (أعمل باستمرار على تحسين مستوى

أدائي لتحقيق الأهداف العامة للمؤسسة) حيث بلغ الوسط الحسابيّ لها (4.30) والوزن النسبيّ (86.0%)، بينما أقلّ الفقرات أهمّية (أستخدم التحليل الذكي للبيانات لتقييم فعالية العمليات الأمنية) وبلغ الوسط الحسابيّ لها (4.06) والوزن النسبيّ (81.1%).

2.4 الإجابة عن فرضيات الدراسة:

الفرضية الأولى: لا يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده الأربعة في المجتمع

للوقوف على الدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده الأربعة في المجتمع، كما هو موضّح في الجدول (7.4)

جداول (7.4) نتائج اختبار تحليل الانحدار المتُعدّد للدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده الأربعة في المجتمع

المحور	المعيار	مُعامِل الارتباط	التباين المفسر R^2	F	مُعامِل الانحدار	T	الدلالة
انتشار الجرائم الإلكترونية	الثابت	0.757	0.574	117.789	1.156	5.648	0.000
	التعلم الآلي				0.183	2.516	0.000
	التعلم العميق				0.558	8.322	0.001
	الذكاء الاصطناعي				0.758	14.772	0.000

نلاحظ من الجدول (7.4) أن مستوى الدلالة أقل من (0.05) وبذلك يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده الأربعة في المجتمع، وكانت نسبة التباين المفسر (57.4%)، وهذا يشير إلى أنه يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستَوَى الدلالة

(α≤0.05) بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده الأربعة في المجتمع بحيث بلغ معامل الارتباط (0.757).

الفرضية الفرعية الأولى: لا يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من الاحتيال المالي في المجتمع

للوقوف على الدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من الاحتيال المالي في المجتمع، كما هو موضّح في الجدول (8.4)

جداول (8.4) نتائج اختبار تحليل الانحدار المتُعدّد للدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من الاحتيال المالي في المجتمع

المحور	المعيار	مُعامِل الارتباط	التباين المفسر R^2	F	مُعامِل الانحدار	T	الدلالة
الاحتيال المالي	الثابت	0.722	0.522	95.415	1.122	4.861	0.000
	التعلم الآلي				0.244	2.95	0.003
	التعلم العميق				0.523	6.881	0.000
	الذكاء الاصطناعي				0.780	13.586	0.000

نلاحظ من الجدول (8.4) أن مستوى الدلالة أقل من (0.05) وبذلك يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من الاحتيال المالي في المجتمع، وكانت نسبة التباين المفسر (52.2%)، وهذا يشير إلى أنه يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من الاحتيال المالي في المجتمع بحيث بلغ معامل الارتباط (0.722).

الفرضية الفرعية الثانية: لا يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من سرقة البيانات في المجتمع

للوقوف على الدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من سرقة البيانات في المجتمع، كما هو موضّح في الجدول (9.4)

جداول (9.4) نتائج اختبار تحليل الانحدار المتُعدّد للدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من سرقة البيانات في المجتمع

المحور	المعيار	مُعامِل الارتباط	التباين المفسر R^2	F	مُعامِل الانحدار	T	الدلالة
سرقة البيانات	الثابت	0.660	0.435	67.486	1.270	4.867	0.000
	التعلم الآلي				0.273	2.853	0.006
	التعلم العميق				0.245	6.343	0.000
	الذكاء الاصطناعي				0.735	11.275	0.000

نلاحظ من الجدول (9.4) أن مستوى الدلالة أقل من (0.05) وبذلك يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من سرقة البيانات في المجتمع، وكانت نسبة التباين المفسر (43.5%)، وهذا يشير إلى أنه يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من سرقة البيانات في المجتمع بحيث بلغ معامل الارتباط (0.660).

الفرضية الفرعية الثالثة: لا يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من انتهاك الخصوصية في المجتمع

للوقوف على الدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من انتهاك الخصوصية في المجتمع، كما هو موضّح في الجدول (10.4)

جداول (10.4) نتائج اختبار تحليل الانحدار المتُعدّد للدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من انتهاك الخصوصية في المجتمع

المحور	المعيار	مُعامِل الارتباط	التباين المفسر R^2	F	مُعامِل الانحدار	T	الدلالة
انتهاك الخصوصية	الثابت	0.637	0.405	59.615	1.213	4.414	0.000
	التعلم الآلي				0.201	2.052	0.042
	التعلم العميق				0.516	5.695	0.000
	الذكاء الاصطناعي				0.731	10.705	0.000

نلاحظ من الجدول (10.4) أن مستوى الدلالة أقل من (0.05) وبذلك يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من انتهاك الخصوصية في المجتمع، وكانت نسبة التباين المفسر (40.5%)، وهذا يشير إلى أنه يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من انتهاك الخصوصية في المجتمع؛ إذ بلغ معامل الارتباط (0.637).

الفرضية الفرعية الرابعة: لا يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من نشر الشائعات والبيانات المضللة في المجتمع.

للوقوف على الدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من نشر الشائعات والبيانات المضللة في المجتمع، كما هو موضّح في الجدول (11.4)

جداول (11.4) نتائج اختبار تحليل الانحدار المتُعدّد للدور الوسيط لتميز الأداء بين الذكاء الاصطناعي بأبعاده في الاجهزة الأمنية الفلسطينية والحد من نشر الشائعات والبيانات المضللة في المجتمع

المحور	المعيار	مُعامِل الارتباط	التباين المفسر R^2	F	مُعامِل الانحدار	T	الدلالة
نشر الشائعات والبيانات المضللة	الثابت	0.672	0.451	71.872	1.020	3.712	0.000
	التعلم الآلي				0.213	2.155	0.002
	التعلم العميق				0.649	7.172	0.000
	الذكاء الاصطناعي				0.786	11.332	0.000

نلاحظ من الجدول (11.4) أن مستوى الدلالة أقل من (0.05) وبذلك يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من نشر الشائعات والبيانات المضللة في المجتمع، وكانت نسبة التباين المفسر (45.1%)، وهذا يشير إلى أنه يوجد دور وسيط لتميز الأداء ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده في الأجهزة الأمنية الفلسطينية والحد من نشر الشائعات والبيانات المضللة في المجتمع؛ إذ بلغ معامل الارتباط (0.672).

الفرضية الثانية: لا توجد علاقة ذات دلالة إحصائيّة عند مُستوَى الدلالة ($\alpha \leq 0.05$) بين تميز أداء العاملين بأبعاده في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم.

جرى استخدام اختبار (Pearson Correlation) لمعرفة العلاقة بين تميز أداء العاملين بأبعاده في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم، وذلك كما هو موضّح في الجداول (12.4):

الجدول(12.4) نَتائِج اختبار (Pearson Correlation) للعلاقة بين تميز أداء العاملين بأبعاده في الاجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده

المتغيرات		الاحتيال المالي	سرقة البيانات	انتهاك الخصوصية	نشر الشائعات والبيانات المضللة	انتشار الجرائم الإلكترونية
تنفيذ المهام	الارتباط R	**0.521	**0.426	**0.556	**0.487	**0.573
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000
التحلي بالمسؤولية	الارتباط R	**0.630	**0.458	**0.605	**0.534	**0.642
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000
التطور الوظيفي	الارتباط R	**0.630	**0.498	**0.585	**0.544	**0.651
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000
تحقيق الأهداف	الارتباط R	**0.607	**0.500	**0.537	**0.581	**0.643
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000
تميز الأداء	الارتباط R	**0.675	**0.532	**0.644	**0.607	**0.709
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000

نلاحظ من الجدول (12.4) أن مستوى الدلالة أقل من (0.05) وبذلك توجد علاقة ذات دلالة إحصائيّة عند مُستوَى الدلالة ($\alpha \leq 0.05$) بين تميز أداء العاملين بأبعاده في الأجهزة الأمنية الفلسطينية وانتشار الجرائم الإلكترونية بأبعاده في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم، بحيث بلغ معامل الارتباط للدرجة الكلية (0.709) مما يشير إلى علاقة إيجابية بدرجة مرتفعة.

الفرضية الثالثة: لا توجد علاقة ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده وانتشار الجرائم الإلكترونية بأبعادها في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم.

جرى استخدام اختبار (Pearson Correlation) لمعرفة العلاقة بين الذكاء الاصطناعي بأبعاده وانتشار الجرائم الإلكترونية بأبعادها في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم، وذلك كما هو موضّح في الجداول (12.4):

الجدول(12.4) نَتائِج اختبار (Pearson Correlation) للعلاقة بين الذكاء الاصطناعي بأبعاده وانتشار الجرائم الإلكترونية بأبعادها

المتغيرات		الاحتيال المالي	سرقة البيانات	انتهاك الخصوصية	نشر الشائعات والبيانات المضللة	انتشار الجرائم الإلكترونية
التعلم الآلي	الارتباط R	**0.626	**0.553	**0.543	**0.538	**0.636
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000
التعلم العميق	الارتباط R	**0.705	**0.651	**0.625	**0.668	**0.747
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000
الذكاء الاصطناعي	الارتباط R	**0.715	**0.648	**0.628	**0.649	**0.744
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000

نلاحظ من الجدول (12.4) أن مستوى الدلالة أقل من (0.05) وبذلك توجد علاقة ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده وانتشار الجرائم الإلكترونية بأبعادها في المجتمع من وجهة نظر العاملين في وحدة مكافحة الجرائم، بحيث بلغ معامل الارتباط للدرجة الكلية (0.744) ما يشير إلى علاقة إيجابية بدرجة مرتفعة.

الفرضية الرابعة: لا توجد علاقة ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده وتميز أداء العاملين بأبعاده في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم.

تمّ استخدام اختبار (Pearson Correlation) لمعرفة العلاقة بين الذكاء الاصطناعي بأبعاده وتميز أداء العاملين بأبعاده في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم، وذلك كما هو موضّح في الجداول (13.4):

الجدول(13.4) نَتائِج اختبار (Pearson Correlation) للعلاقة بين الذكاء الاصطناعي بأبعاده وتميز أداء العاملين بأبعاده

المتغيرات		تنفيذ المهام	التحلي بالمسؤولية	التطور الوظيفي	تحقيق الأهداف	تميز الأداء
التعلم الآلي	الارتباط R	**0.535	**0.407	**0.549	**0.487	**0.570
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000
التعلم العميق	الارتباط R	**0.528	**0.366	**0.575	**0.474	**0.559
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000
الذكاء الاصطناعي	الارتباط R	**0.570	**0.413	**0.603	**0.515	**0.605
	مستوى الدلالة	0.000	0.000	0.000	0.000	0.000

نلاحظ من الجدول (13.4) أن مستوى الدلالة أقل من (0.05) وبذلك توجد علاقة ذات دلالة إحصائيّة عند مُستوَى الدلالة (α≤0.05) بين الذكاء الاصطناعي بأبعاده وتميز أداء العاملين بأبعاده في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم، بحيث بلغ معامل الارتباط للدرجة الكلية (0.605) ما يشير إلى علاقة إيجابية بدرجة متوسطة.

الفرضية الخامسة: لا تُوجَد فُرُوق ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) لمستوى تطبيق الذكاء الاصطناعي في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تعزى لمتغير (الجنس، المؤهل العلمي، المسمى الوظيفي، سنوات الخبرة، الرتبة العسكرية).

أولاً: الجنس

جرى استخدام اختبار(ت) المتوسّطات الحسابية والانحرافات المعيارية في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تطبيق الذكاء الاصطناعي في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس، كما هو موضّح في جدول رقم (14.4).

جدول (14.4): نتائج اختبار (ت) في متوسّطات تطبيق الذكاء الاصطناعي في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس

المتغيرات	الجنس	العدد	المتوسّط الحسابيّ	الانحراف المعياريّ	درجات الحريّة	قيمة ت المحسوبة	الدالة الإحصائية
التعلم الآلي	ذكر	145	4.04	0.58	176	0.327	0.744
	انثى	33	4.00	0.62			
التعلم العميق	ذكر	145	3.85	0.66		-0.190	0.849
	انثى	33	3.87	0.56			
الذكاء الاصطناعي	ذكر	145	3.95	0.58		0.062	0.950
	انثى	33	3.94	0.55			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (14.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تطبيق الذكاء الاصطناعي في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس، وذلك لأنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.950) أي أنّ هذه القِيمة أكبر من قِيمة ألفا (0.05).

ثانياً: المؤهل العلمي

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي، كما هو مُوضّح في الجدول رقم (15.4).

جدول (15.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) للتعرف إلى الفروق بين متوسّطات تطبيق الذكاء الاصطناعي في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
التعلم الآلي	بين المجموعات	1.346	2	0.673	1.939	0.147
	داخل المجموعات	60.762	175	0.347		
	المجموع	62.108	177			
التعلم العميق	بين المجموعات	6.226	2	3.113	8.179	0.000
	داخل المجموعات	66.610	175	0.381		
	المجموع	72.836	177			
الذكاء الاصطناعي	بين المجموعات	3.296	2	1.648	5.213	0.006
	داخل المجموعات	55.325	175	0.316		
	المجموع	58.621	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (15.4) إلى أنه توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات تطبيق الذكاء الاصطناعي في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي، عند الدرجة الكلية وعند التعلم العميق، حيث أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.006) أي أنّ هذه قِيمة أقل من قِيمة ألفا (0.05)، بينما لا توجد فروق عند بعد التعلم الآلي.

ولمعرفةِ مصدرِ الفروقِ جرى استخدامُ اختبارِ (LSD) تبعاً إلى متغير المؤهل العلمي، كما هو مُوضّحٌ في الجدولِ (16.4).

جدول (16.4): نتائج اختبار (LSD) للفروق بين متوسطات تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي

المتغيرات	المؤهل العلمي	المتوسط الحسابي	دبلوم فأقل	بكالوريوس	دراسات عليا
التعلم العميق	دبلوم فأقل	3.67			
	بكالوريوس	3.82			
	دراسات عليا	4.22	0.556421	0.408009	
الذكاء الاصطناعي	دبلوم فأقل	3.82			
	بكالوريوس	3.91			
	دراسات عليا	4.22	0.396056	0.312590	

الفرق في المقارنات دالة إحصائياً عند مستوى الدلالة (0.05)

تُشيرُ مُعطياتُ الجدولِ السّابقِ إلى أنّ هناك فروقًا بينَ حملة درجة دراسات العليا من جهة وبين كل من حملة درجة (دبلوم فأقل، بكالوريوس) لصالح حملة درجة دراسات العليا لأن المتوسط الحسابي لديهم أكبر.

ثالثاً: المسمى الوظيفي

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي، كما هو مُوضّح في الجدول رقم (17.4).

جدول (17.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) لتعرف الفروق بين متوسّطات تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
التعلم الآلي	بين المجموعات	2.706	2	1.353	3.986	0.020
	داخل المجموعات	59.402	175	0.339		
	المجموع	62.108	177			
التعلم العميق	بين المجموعات	7.256	2	3.628	9.681	0.000
	داخل المجموعات	65.580	175	0.375		
	المجموع	72.836	177			

الذكاء الاصطناعي	بين المجموعات	4.655	2	2.327	7.547	0.001
	داخل المجموعات	53.967	175	0.308		
	المجموع	58.621	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (17.4) إلى أنه توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي، عند الدرجة الكلية وعند التعلم الآلي، والتعلم العميق؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.001) أي أنّ هذه قِيمة أقل من قِيمة ألفا (0.05).

ولمعرفةِ مصدرِ الفروقِ تمّ استخدامُ اختبارِ (LSD) تبعاً إلى متغير المسمى الوظيفي، كما هو مُوضّحٌ في الجدولِ (18.4).

جدول (18.4): نتائج اختبار (LSD) للفروق بين متوسطات تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي

المتغيرات	المسمى الوظيفي	المتوسط الحسابي	مدير	رئيس قسم	موظف
التعلم الآلي	مدير	3.92			
	رئيس قسم	3.88			
	موظف	4.14	0.222449	0.264777	
التعلم العميق	مدير	3.75			
	رئيس قسم	3.56			
	موظف	4.03	0.272886	0.470165	
الذكاء الاصطناعي	مدير	3.84			
	رئيس قسم	3.72			
	موظف	4.08	0.247668	0.367471	

الفرق في المقارنات دالة إحصائياً عند مستوى الدلالة (0.05)

تُشيرُ مُعطياتُ الجدولِ السّابقِ إلى أنّ هناك فروقًا بينَ حملة الموظفين من جهة وبين كل من (مدير، رئيس قسم) لصالح حملة درجة الموظفين لأن المتوسط الحسابي لديهم أكبر.

رابعاً: سنوات الخبرة

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تطبيق الذكاء الاصطناعي في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة، كما هو مُوضّح في الجدول رقم (19.4).

جدول (19.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) لتعرف الفروق بين متوسّطات تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
التعلم الآلي	بين المجموعات	0.264	2	0.132	0.373	0.689
	داخل المجموعات	61.844	175	0.353		
	المجموع	62.108	177			
التعلم العميق	بين المجموعات	0.846	2	0.423	1.029	0.360
	داخل المجموعات	71.989	175	0.411		
	المجموع	72.836	177			
الذكاء الاصطناعي	بين المجموعات	0.406	2	0.203	0.610	0.545
	داخل المجموعات	58.216	175	0.333		
	المجموع	58.621	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (19.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة، عند الدرجة الكلية وعند التعلم الآلي، والتعلم العميق؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.545) أي أنّ هذه قِيمة أكبر من قِيمة ألفا (0.05).

خامساً: الرتبة العسكرية

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية، كما هو مُوضّح في الجدول رقم (20.4).

جدول (20.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) لتعرف الفروق بين متوسّطات تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
التعلم الآلي	بين المجموعات	2.740	4	0.685	1.996	0.097
	داخل المجموعات	59.368	173	0.343		
	المجموع	62.108	177			
التعلم العميق	بين المجموعات	2.745	4	0.686	1.693	0610.
	داخل المجموعات	70.091	173	0.405		
	المجموع	72.836	177			
الذكاء الاصطناعي	بين المجموعات	2.050	4	0.512	1.565	1410.
	داخل المجموعات	56.571	173	0.327		
	المجموع	58.621	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (20.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات تطبيق الذكاء الاصطناعي في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية، عند الدرجة الكلية وعند التعلم الآلي، والتعلم العميق؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.114) أي أنّ هذه قِيمة أكبر من قِيمة ألفا (0.05).

الفرضية السادسة: لا تُوجَد فُرُوق ذات دلالة إحصائيّة عند مُستوَى الدلالة ($\alpha \leq 0.05$) لمستوى الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تعزى لمتغير (الجنس، المؤهل العلمي، المسمى الوظيفي، سنوات الخبرة، الرتبة العسكرية).

أولاً: الجنس

جرى استخدام اختبار(ت) المتوسّطات الحسابية والانحرافات المعيارية في متوسّطات استجابات أفراد عينة الدراسة حول مستوى الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس، كما هو موضّح في جدول رقم (21.4).

جدول (21.4): نتائج اختبار (ت) في متوسّطات الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس

المتغيرات	الجنس	العدد	المتوسّط الحسابيّ	الانحراف المعياريّ	درجات الحريّة	قيمة ت المحسوبة	الدالة الإحصائية
الاحتيال المالي	ذكر	145	4.15	0.62	176	1.026	0.306
	انثى	33	4.03	0.68			
سرقة البيانات	ذكر	145	4.10	0.66		1.336	0.183
	انثى	33	3.93	0.63			
انتهاك الخصوصية	ذكر	145	4.02	0.67		0.381	0.703
	انثى	33	3.97	0.68			
نشر الشائعات والبيانات المضللة	ذكر	145	3.99	0.71		0.281	0.779
	انثى	33	3.95	0.63			
الحد من انتشار الجرائم الإلكترونية	ذكر	145	4.07	0.59		0.838	0.403
	انثى	33	3.97	0.58			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (21.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس، وذلك لأنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.403) أي أنّ هذه القِيمة أكبر من قِيمة ألفا (0.05).

ثانياً: المؤهل العلمي

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي، كما هو مُوضّح في الجدول رقم (22.4).

جدول (22.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) لتعرف الفروق بين متوسّطات الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
الاحتيال المالي	بين المجموعات	2.482	2	1.241	3.232	0.042
	داخل المجموعات	67.202	175	0.384		
	المجموع	69.684	177			
سرقة البيانات	بين المجموعات	4.089	2	2.045	5.012	0.008
	داخل المجموعات	71.398	175	0.408		
	المجموع	75.488	177			
انتهاك الخصوصية	بين المجموعات	4.786	2	2.393	5.608	0.004
	داخل المجموعات	74.674	175	0.427		
	المجموع	79.460	177			
نشر الشائعات والبيانات	بين المجموعات	6.288	2	3.144	6.906	0.001
	داخل المجموعات	79.671	175	0.455		

المضللة	المجموع	85.959	177			
الحد من انتشار الجرائم الإلكترونية	بين المجموعات	4.274	2	2.137	6.609	0.002
	داخل المجموعات	56.593	175	0.323		
	المجموع	60.867	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (22.4) إلى أنه توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي، عند الدرجة الكلية وعند جميع الأبعاد؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.002) أي أنّ هذه قِيمة أقل من قِيمة ألفا (0.05).

ولمعرفةِ مصدرِ الفروقِ تمّ استخدامُ اختبارِ (LSD) تبعاً إلى متغير المؤهل العلمي، كما هو مُوضّحٌ في الجدولِ (23.4).

جدول (23.4): نتائج اختبار (LSD) للفروق بين متوسطات الحد من انتشار الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي

المتغيرات	المؤهل العلمي	المتوسط الحسابي	دبلوم فأقل	بكالوريوس	دراسات عليا
الاحتيال المالي	دبلوم فأقل	4.07			
	بكالوريوس	4.06			
	دراسات عليا	4.37	0.295960	0.307071	
سرقة البيانات	دبلوم فأقل	3.95			
	بكالوريوس	4.02			
	دراسات عليا	4.38	0.428283	0.363838	
انتهاك الخصوصية	دبلوم فأقل	3.92			
	بكالوريوس	3.94			
	دراسات عليا	4.35	0.428956	0.418586	
نشر الشائعات والبيانات المضللة	دبلوم فأقل	3.87			
	بكالوريوس	3.89			
	دراسات عليا	4.37	0.499663	0.475404	
الحد من	دبلوم فأقل	3.95			

انتشار الجرائم الإلكترونية	بكالوريوس	3.98			
	دراسات عليا	4.37	0.413215	0.391225	

الفرق في المقارنات دالة إحصائياً عند مستوى الدلالة (0.05)

تُشيرُ مُعطياتُ الجدولِ السّابقِ إلى أنّ هناك فروقًا بينَ حملة درجة دراسات العليا من جهة وبين كل من حملة درجة (دبلوم فأقل، بكالوريوس) لصالح حملة درجة دراسات العليا لأن المتوسط الحسابي لديهم أكبر.

ثالثاً: المسمى الوظيفي

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى الحد من انتشار الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي، كما هو مُوضّح في الجدول رقم (24.4).

جدول (24.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) لتعرف الفروق بين متوسّطات الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
الاحتيال المالي	بين المجموعات	2.224	2	1.112	2.885	0.059
	داخل المجموعات	67.460	175	.385		
	المجموع	69.684	177			
سرقة البيانات	بين المجموعات	1.460	2	.730	1.725	0.181
	داخل المجموعات	74.028	175	.423		
	المجموع	75.488	177			
انتهاك الخصوصية	بين المجموعات	1.701	2	.851	1.914	0.151
	داخل المجموعات	77.759	175	.444		
	المجموع	79.460	177			
نشر الشائعات والبيانات المضللة	بين المجموعات	2.052	2	1.026	2.141	0.098
	داخل المجموعات	83.907	175	0.479		
	المجموع	85.959	177			

الحد من انتشار الجرائم الإلكترونية	بين المجموعات	1.935	2	.968	2.873	0.059
	داخل المجموعات	58.932	175	.337		
	المجموع	60.867	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (24.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي، عند الدرجة الكلية وعند الأبعاد؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.059) أي أنّ هذه قِيمة أكبر من قِيمة ألفا (0.05).

رابعاً: سنوات الخبرة

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى الحد من انتشار الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة، كما هو مُوضّح في الجدول رقم (25.4).

جدول (25.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) لتعرف الفروق بين متوسّطات الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
الاحتيال المالي	بين المجموعات	0.960	2	0.480	1.222	0.297
	داخل المجموعات	68.724	175	0.393		
	المجموع	69.684	177			
سرقة البيانات	بين المجموعات	0.727	2	0.364	0.851	0.429
	داخل المجموعات	74.760	175	0.427		
	المجموع	75.488	177			
انتهاك	بين المجموعات	0.744	2	0.372	0.827	0.439

الخصوصية	داخل المجموعات	78.716	175	0.450		
	المجموع	79.460	177			
نشر الشائعات والبيانات المضللة	بين المجموعات	0.169	2	0.085	0.172	0.842
	داخل المجموعات	85.790	175	0.490		
	المجموع	85.959	177			
الحد من انتشار الجرائم الإلكترونية	بين المجموعات	0.587	2	0.293	0.851	0.429
	داخل المجموعات	60.281	175	0.344		
	المجموع	60.867	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (25.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة، عند الدرجة الكلية وعند الأبعاد؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.429) أي أنّ هذه قِيمة أكبر من قِيمة ألفا (0.05).

خامساً: الرتبة العسكرية

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى الحد من انتشار الجرائم الإلكترونية في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية، كما هو مُوضّح في الجدول رقم (26.4).

جدول (26.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) لتعرف الفروق بين متوسّطات الحد من انتشار الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
الاحتيال المالي	بين المجموعات	.331	4	.083	0.206	0.935
	داخل المجموعات	69.353	173	.401		

	المجموع	69.684	177			
سرقة البيانات	بين المجموعات	.485	4	.121	0.279	0.891
	داخل المجموعات	75.003	173	.434		
	المجموع	75.488	177			
انتهاك الخصوصية	بين المجموعات	1.103	4	.276	0.609	0.657
	داخل المجموعات	78.357	173	.453		
	المجموع	79.460	177			
نشر الشائعات والبيانات المضللة	بين المجموعات	3.134	4	.784	1.637	0.167
	داخل المجموعات	82.825	173	.479		
	المجموع	85.959	177			
الحد من انتشار الجرائم الإلكترونية	بين المجموعات	.890	4	.222	0.641	0.634
	داخل المجموعات	59.978	173	.347		
	المجموع	60.867	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (26.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات الحد من انتشار الجرائم الإلكترونية في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية، عند الدرجة الكلية وعند الأبعاد؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.634) أي أنّ هذه قِيمة أكبر من قِيمة ألفا (0.05).

الفرضية السابعة: لا تُوجَد فُرُوق ذات دلالة إحصائيّة عند مُستَوَى الدلالة ($\alpha \leq 0.05$) لمستوى تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تعزى لمتغير (الجنس، المؤهل العلمي، المسمى الوظيفي، سنوات الخبرة، الرتبة العسكرية).

أولاً: الجنس

جرى استخدام اختبار(ت) المتوسّطات الحسابية والانحرافات المعيارية في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تميز الأداء في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس، كما هو موضّح في جدول رقم (27.4).

جدول (27.4): نتائج اختبار (ت) في متوسّطات تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس

المتغيرات	الجنس	العدد	المتوسّط الحسابيّ	الانحراف المعياريّ	درجات الحريّة	قيمة ت المحسوبة	الدالة الإحصائية
تنفيذ المهام	ذكر	145	4.06	0.54	176	1.917	0.063
	انثى	33	3.97	0.83			
التحلي بالمسؤولية	ذكر	145	4.30	0.60		0.935	0.351
	انثى	33	4.19	0.71			
التطور الوظيفي	ذكر	145	4.25	0.55		0.732	0.465
	انثى	33	4.17	0.64			
تحقيق الأهداف	ذكر	145	4.22	0.56		4.510	0.133
	انثى	33	4.05	0.78			
تميز الأداء	ذكر	145	4.23	0.48		1.644	0.102
	انثى	33	4.07	0.65			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (27.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تميز الأداء في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الجنس،

وذلك لأنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.102) أي أنّ هذه القِيمة أكبر من قِيمة ألفا (0.05).

ثانياً: المؤهل العلمي

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تميز الأداء في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي، كما هو مُوضّح في الجدول رقم (28.4).

جدول (28.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) للتعرف إلى الفروق بين متوسّطات تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
تنفيذ المهام	بين المجموعات	3.360	2	1.680	4.663	0.011
	داخل المجموعات	63.059	175	.360		
	المجموع	66.419	177			
التحلي بالمسؤولية	بين المجموعات	1.580	2	.790	2.064	0.130
	داخل المجموعات	67.000	175	.383		
	المجموع	68.580	177			
التطور الوظيفي	بين المجموعات	1.200	2	.600	1.899	0.153
	داخل المجموعات	55.303	175	.316		
	المجموع	56.503	177			
تحقيق الأهداف	بين المجموعات	2.503	2	1.251	3.528	0.031
	داخل المجموعات	62.067	175	.355		
	المجموع	64.570	177			
تميز الأداء	بين المجموعات	1.993	2	.997	3.798	0.024
	داخل المجموعات	45.926	175	.262		
	المجموع	47.920	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (28.4) إلى أنه توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات تميز الأداء في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي، عند الدرجة الكلية وعند الأبعاد (تنفيذ المهام، تحقيق الأهداف)؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.024) أي أنّ هذه قِيمة أقل من قِيمة ألفا (0.05)، بينما لا توجد فروق عند الأبعاد (التحلي بالمسؤولية، التطور الوظيفي).

ولمعرفةِ مصدرِ الفروقِ جرى استخدامُ اختبارِ (LSD) تبعاً إلى متغير المؤهل العلمي، كما هو مُوضّحٌ في الجدولِ (29.4).

جدول (29.4): نتائج اختبار (LSD) للفروق بين متوسطات تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المؤهل العلمي

المتغيرات	المؤهل العلمي	المتوسط الحسابي	دبلوم فأقل	بكالوريوس	دراسات عليا
تنفيذ المهام	دبلوم فأقل	3.96			
	بكالوريوس	4.07			
	دراسات عليا	4.37	0.406869		
تحقيق الأهداف	دبلوم فأقل	4.00			
	بكالوريوس	4.21			
	دراسات عليا	4.35	0.350505		
تميز الأداء	دبلوم فأقل	4.07			
	بكالوريوس	4.19			
	دراسات عليا	4.39	0.323182		

الفرق في المقارنات دالة إحصائياً عند مستوى الدلالة (0.05)

تُشيرُ مُعطياتُ الجدولِ السّابقِ إلى أنّ هناك فروقًا بينَ حملة درجة دراسات العليا من جهة وبين كل من حملة درجة دبلوم فأقل لصالح حملة درجة دراسات العليا؛ لأن المتوسط الحسابي لديهم أكبر.

ثالثاً: المسمى الوظيفي

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تميز الأداء في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي، كما هو مُوضّح في الجدول رقم (30.4).

جدول (30.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) للتعرف إلى الفروق بين متوسّطات تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
تنفيذ المهام	بين المجموعات	0.565	2	0.283	0.751	0.474
	داخل المجموعات	65.854	175	0.376		
	المجموع	66.419	177			
التحلي بالمسؤولية	بين المجموعات	1.796	2	0.898	2.354	0.098
	داخل المجموعات	66.784	175	0.382		
	المجموع	68.580	177			
التطور الوظيفي	بين المجموعات	0.829	2	0.414	1.303	0.274
	داخل المجموعات	55.674	175	0.318		
	المجموع	56.503	177			
تحقيق الأهداف	بين المجموعات	0.590	2	0.295	0.806	0.448
	داخل المجموعات	63.981	175	0.366		
	المجموع	64.570	177			
تميز الأداء	بين المجموعات	0.593	2	0.296	1.096	0.337
	داخل المجموعات	47.327	175	0.270		
	المجموع	47.920	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (30.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير المسمى الوظيفي، عند الدرجة الكلية وعند الأبعاد،

حيث أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.337) أي أنّ هذه قِيمة أكبر من قِيمة ألفا (0.05).

رابعاً: سنوات الخبرة

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تميز الأداء في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة، كما هو مُوضّح في الجدول رقم (31.4).

جدول (31.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) للتعرف إلى الفروق بين متوسّطات تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
تنفيذ المهام	بين المجموعات	0.212	2	0.106	0.280	0.756
	داخل المجموعات	66.207	175	0.378		
	المجموع	66.419	177			
التحلي بالمسؤولية	بين المجموعات	0.533	2	0.266	0.685	0.506
	داخل المجموعات	68.048	175	0.389		
	المجموع	68.580	177			
التطور الوظيفي	بين المجموعات	0.055	2	0.027	0.085	0.919
	داخل المجموعات	56.449	175	0.323		
	المجموع	56.503	177			
تحقيق الأهداف	بين المجموعات	0.265	2	0.132	0.360	0.698
	داخل المجموعات	64.306	175	0.367		
	المجموع	64.570	177			
تميز الأداء	بين المجموعات	0.122	2	0.061	0.222	0.801
	داخل المجموعات	47.798	175	0.273		
	المجموع	47.920	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (31.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير سنوات الخبرة، عند الدرجة الكلية وعند الأبعاد، حيث أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.801) أي أنّ هذه قِيمة أكبر من قِيمة ألفا (0.05).

خامساً: الرتبة العسكرية

جرى استخدام اختبار تحليل التباين الأحاديّ (ANOVA) في متوسّطات استجابات أفراد عينة الدراسة حول مستوى تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية، كما هو مُوضّح في الجدول رقم (32.4).

جدول (32.4): نتائج اختبار تحليل التباين الأحاديّ (ANOVA) للتعرف إلى الفروق بين متوسّطات تميز الأداء في الاجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية

المتغيرات	مصدر التباين	مجموع المربعّات	درجات الحريّة	متوسّط المربعّات	قيمة ف	الدلالة الإحصائية
تنفيذ المهام	بين المجموعات	2.319	4	0.580	1.565	0.186
	داخل المجموعات	64.100	173	0.371		
	المجموع	66.419	177			
التحلي بالمسؤولية	بين المجموعات	2.385	4	0.596	1.558	0.188
	داخل المجموعات	66.195	173	0.383		
	المجموع	68.580	177			
التطور الوظيفي	بين المجموعات	0.368	4	0.092	0.284	0.888
	داخل المجموعات	56.135	173	0.324		
	المجموع	56.503	177			
تحقيق الأهداف	بين المجموعات	1.791	4	0.448	1.234	0.298
	داخل المجموعات	62.779	173	0.363		
	المجموع	64.570	177			
تميز الأداء	بين المجموعات	1.026	4	0.256	0.946	0.439

	داخل المجموعات	46.894	173	0.271		
	المجموع	47.920	177			

** دالة إحصائيا عند المستوى 0.01 * دالة إحصائيا عند المستوى 0.05

تشير المعطيات الواردة في الجدول (32.4) إلى أنه لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.05$) بين متوسّطات تميز الأداء في الأجهزة الأمنية الفلسطينية من وجهة نظر العاملين في وحدة مكافحة الجرائم تُعزى إلى مُتغير الرتبة العسكرية، عند الدرجة الكلية وعند الأبعاد؛ إذ أنّ قيمة الدالة الإحصائية عند الدرجة الكلية بلغت (0.439) أي أنّ هذه قِيمة أكبر من قِيمة ألفا (0.05).

الفصل الخامس

مناقشة النتائج والتوصيات

1.5 تفسير نتائج أسئلة الدراسة ومناقشتها

2.5 تفسير نتائج فرضيات الدراسة ومناقشتها

3.5 التوصيات

الفصل الخامس

مناقشة النتائج والتوصيات

يتناول هذا الفصل أهمّ النتائج والتوصيات التي تَوصّلتِ إليها الدراسة التي هدفت إلى مَعرِفَة دور الذكاء الاصطناعي في الحد من انتشار الجرائم الإلكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً، وفي القسم الأول لخص الباحث أهمّ النتائج التي تَوصّل إليها من خلال دراسته. وتبع ذلك توصياته للدراسة التي من الممكن أن تؤخذ بعين الاعتبار من قبل الأجهزة الأمنية الفلسطينية والجهات المُختصّة.

1.5 تفسير نتائج أسئلة الدراسة ومناقشتها

1.1.5 تفسير نتائج السؤال الأول مناقشته

أظهرت النتائج أن مستوى تطبيق الذكاء الاصطناعي لدى العاملين في وحدة الجرائم الإلكترونية مرتفع، مع تركيز ملحوظ على التعلم الآلي كأكثر الجوانب أهمية، في حين جاء التعلم العميق في المرتبة الأخيرة. ويُعزى هذا إلى الوعي المتزايد بأهمية الذكاء الاصطناعي في مواجهة التهديدات الإلكترونية، إضافة إلى التدريب المستمر، ما يعكس توجهاً إيجابياً نحو استخدام التقنيات الحديثة لتعزيز الكفاءة الأمنية.

تتفق هذه النتيجة مع دراسة محمود (2024)، ودراسة المرجيلاني (Al-Marghilani, 2022)، بينما تختلف هذه النتيجة مع دراسة عضيات وأبو عيادة (2023)، بحيث أظهرت درجة متوسطة.

يعود ذلك إلى الوعي المتزايد بأهمية الذكاء الاصطناعي في مواجهة التهديدات الإلكترونية، بالإضافة إلى الجهود المستمرة في التدريب والتطوي، ما يعكس التزام الأجهزة الأمنية بتعزيز الكفاءة الأمنية من خلال تبني تقنيات الذكاء الاصطناعي.

2.1.5 تفسير نتائج السؤال الثاني مناقشته

أظهرت النتائج أن مستوى الحد من انتشار الجرائم الإلكترونية لدى العاملين في وحدة الجرائم الإلكترونية مرتفع، مع تركيز خاص على مكافحة الاحتيال المالي، في حين كان الاهتمام أقل بقضايا نشر الشائعات. ويُعزى هذا إلى استخدام تقنيات متقدمة، والتوعية المجتمعية، والتنسيق الفعّال بين الجهات الأمنية، مما ساهم في تعزيز فعالية الجهود المبذولة في مواجهة الجرائم الإلكترونية، تتفق هذه النتيجة مع دراسة المرجيلاني (Al-Marghilani, 2022).

يُعزى ذلك إلى استخدام تقنيات الذكاء الاصطناعي مما ساهم في تحسين القدرة على الكشف عن الجرائم المالية ومعالجتها، وتلعب التوعية المجتمعية دورًا هامًا في تقليل مخاطر الاحتيال، ما يعزز إدراك المواطنين لأساليب الاحتيال وتساعدهم في اتخاذ تدابير وقائية.

3.1.5 تفسير نتائج السؤال الثالث مناقشته

أظهرت النتائج أن مستوى تميز الأداء لدى العاملين في وحدة الجرائم الإلكترونية مرتفع، مع تركيز بارز على التحلي بالمسؤولية. ويُعزى ذلك إلى اختيار العاملين وفق كفاءاتهم التقنية، والتزامهم العالي بمهامهم، إضافة إلى روح التعاون بينهم، وسعيهم المستمر لتطوير مهاراتهم والتكيف مع التغيرات في بيئة العمل، مما يعزز من كفاءة الأداء العام.

تتفق النتيجة مع دراسة الدرابيع (2023)، ودراسة تربان (2014)، ودراسة عقل (2022)، بينما تختلف مع دراسة عقل (2022)، ودراسة الشروقي (2018)؛ إذ كانت النتيجة متوسطة.

تعزى النتيجة إلى الكفاءة للعاملين مما يضمن وجود خبرات متخصصة قادرة على التعامل مع التحديات المعقدة. كما أن التزام العاملين بمهامهم يعكس رغبتهم في تحقيق المهام الوكلة إليهم، وهذا يسهم في تعزيز القدرة على مواجهة الجرائم الإلكترونية.

2.5 تفسير نتائج فرضيات الدراسة ومناقشتها

1.2.5 تفسير نتائج الفرضية الأولى ومناقشتها

أظهرت النتائج أن تميز الأداء يلعب دورًا وسيطًا في العلاقة بين استخدام الذكاء الاصطناعي في الأجهزة الأمنية ومستوى انتشار الجرائم الإلكترونية. إذ يسهم الذكاء الاصطناعي في رفع كفاءة أداء العاملين، ما يعزز قدرتهم على مواجهة الجرائم الإلكترونية بفعالية أكبر، ويؤكد أهمية استثمار هذه التقنيات الحديثة للحد من التهديدات الأمنية.

يُعزى ذلك إلى أن الذكاء الاصطناعي يعزز كفاءة أداء العاملين، مما يمكنهم من التعامل مع التهديدات بشكل أكثر فعالية وسرعة. من خلال تحسين عمليات التحليل والتنبؤ، يزيد الذكاء الاصطناعي من قدرة وحدة الجرائم الإلكترونية على التصدي للجرائم بشكل عام، كما يُظهر استخدام الذكاء الاصطناعي أهمية استثمار الموارد في تعزيز الأمن الإلكتروني.

2.2.5 تفسير نتائج الفرضية الثانية ومناقشتها

أظهرت النتائج وجود علاقة إيجابية بين تميز أداء العاملين في الأجهزة الأمنية ومستوى انتشار الجرائم الإلكترونية؛ إذ يسهم الأداء العالي، خاصة في تنفيذ المهام والتحلي بالمسؤولية، في الحد من هذه الجرائم. ويعكس ذلك فعالية الاستراتيجيات الأمنية المتبعة، وأثر التدريب وتطوير المهارات في تعزيز كفاءة العاملين وقدرتهم على مواجهة التحديات الأمنية بكفاءة.

تتفق النتيجة مع دراسة عبد الباقي (2018) ودراسة أومبر (Umair, 2022) ودراسة العبيدي وآخرون (2022).

يُعزى ذلك إلى أن تميز الأداء في تنفيذ المهام والتحلي بالمسؤولية، يسهم بشكل مباشر في تقليل هذه الجرائم، كما أن أثر التدريب المستمر وتطوير المهارات يعزز من قدرة العاملين على مواجهة التحديات الأمنية بكفاءة.

3.2.5 تفسير نتائج الفرضية الثالثة ومناقشتها

أظهرت النتائج وجود علاقة إيجابية بين استخدام الذكاء الاصطناعي وانتشار الجرائم الإلكترونية؛ إذ يسهم الذكاء الاصطناعي، من خلال أدوات مثل التعلم الآلي والتعلم العميق، في تعزيز قدرة الأجهزة الأمنية على رصد الجرائم ومواجهتها. ويؤكد ذلك أهمية توظيف هذه التقنيات الحديثة والتدريب عليها لرفع كفاءة العاملين وتحسين مستوى الأمان في المجتمع.

تتفق النتيجة دراسة قاسم (2024) ودراسة الشاعر (2023) ودراسة جيمي (Jimmy, 2024) ودراسة بولسون (Powelson, 2022).

يُعزى ذلك إلى أن الذكاء الاصطناعي من خلال أدوات مثل التعلم الآلي والتعلم العميق يعزز قدرة الأجهزة الأمنية على رصد الجرائم بشكل فعال، ويسهم في تحليل البيانات واكتشاف الجرائم والتصدي لها.

4.2.5 تفسير نتائج الفرضية الرابعة ومناقشتها

أظهرت النتائج وجود علاقة إيجابية متوسطة بين استخدام تقنيات الذكاء الاصطناعي وتميز أداء العاملين في الأجهزة الأمنية، حيث يسهم الذكاء الاصطناعي في تحسين تنفيذ المهام وزيادة المسؤولية. كما يعزز التدريب المستمر على هذه التقنيات قدرة العاملين على التكيف، مما يرفع من كفاءتهم وفعالية وحدة مكافحة الجرائم.

5.2.5 تفسير نتائج الفرضية الخامسة ومناقشتها

أظهرت الدراسة وجود توافق في آراء العاملين حول تطبيق الذكاء الاصطناعي في الأجهزة الأمنية، بصرف النظر عن الجنس أو سنوات الخبرة أو الرتبة العسكرية. في المقابل، تبين أن المؤهل العلمي والمسمى الوظيفي يؤثران في هذه الآراء، حيث أظهر حملة الدراسات العليا والموظفون تقييمًا أعلى، ما يعكس دور المعرفة المتخصصة والخبرة العملية في تشكيل تصوراتهم حول فعالية استخدام الذكاء الاصطناعي في العمل الأمني.

6.2.5 تفسير نتائج الفرضية السادسة ومناقشتها

أظهرت الدراسة أن العاملين في وحدة مكافحة الجرائم لديهم تقييمات متقاربة لجهود الحد من انتشار الجرائم الإلكترونية، بغض النظر عن الجنس أو المسمى الوظيفي أو سنوات الخبرة أو الرتبة العسكرية، ما يعكس انسجامًا في وجهات النظر. كما تبين أن المؤهل العلمي يلعب دورًا في تعزيز هذا التقييم، إذ أظهر حملة الدراسات العليا إدراكًا أكبر لفعالية تلك الجهود، نتيجة امتلاكهم لمهارات ومعارف أوسع في مجال مكافحة الجرائم الإلكترونية.

7.2.5 تفسير نتائج الفرضية السابعة ومناقشتها

أظهرت نتائج الدراسة أن العاملين في وحدة مكافحة الجرائم في الأجهزة الأمنية الفلسطينية يتفقون بشكل عام في تقييمهم لمستوى تميز الأداء، بصرف النظر عن اختلافاتهم في الجنس أو المسمى الوظيفي أو سنوات الخبرة أو الرتبة العسكرية، مما يعكس روح العمل الجماعي والانسجام في بيئة العمل. كما تبين أن المؤهل العلمي يلعب دورًا في تشكيل تصورات الأفراد حول الأداء، إذ يميل أصحاب المؤهلات العليا إلى تقييم الأداء بشكل أكثر تميزًا، نتيجة امتلاكهم لمعارف ومهارات متقدمة تسهم في فهم أعمق لأساليب العمل وتحقيق أداء أفضل.

3.5 التوصيات

يوصي الباحث بناءً على النتائج السابقة ما يلي:

---

1. تعزيز البرامج التدريبية المتخصصة في تقنيات التعلم العميق لتوسيع معارف العاملين وزيادة استخدام هذه التقنية المهمة.

من خلال إعداد خطة تدريب سنوية تتضمن ورش عمل ودورات متقدمة في التعلم العميق، بالشراكة مع خبراء محليين ودوليين، مع توفير منصات تعليمية إلكترونية للمتابعة الذاتية.

2. زيادة التركيز على مكافحة نشر الشائعات والبيانات المضللة من خلال تطوير آليات رصد ومتابعة متخصصة.

عن طريق إنشاء وحدة رصد إلكترونية مزودة بأنظمة ذكاء اصطناعي للكشف الفوري عن الأخبار الكاذبة، وربطها بخط ساخن وفريق تحقق ميداني.

3. الاستمرار في تطوير برامج اختيار وتدريب العاملين لضمان ملاءمتهم العالية للمهام التقنية والأمنية.

عن طريق اعتماد اختبارات قدرات تقنية ونفسية قبل التعيين، مع وضع برنامج تدريب تأسيسي إلزامي لجميع المجندين الجدد قبل مباشرتهم العمل.

4. الاستثمار في تقنيات الذكاء الاصطناعي الحديثة مع التركيز على تطوير مهارات العاملين لاستثمار هذه التقنيات بشكل أمثل.

وذلك بتخصيص ميزانية سنوية لتحديث الأجهزة والبرمجيات، وربط أي عملية شراء تقني ببرنامج تدريب متزامن للمستخدمين النهائيين.

5. وضع نظم تقييم أداء دقيقة تربط بين جودة الأداء ونتائج مكافحة الجرائم.

من خلال تصميم نظام نقاط أداء رقمي يقيس الإنتاجية والدقة والاستجابة، مع تقديم مكافآت وحوافز للعاملين ذوي الأداء المتميز.

6. مواصلة تحديث وتطوير أنظمة الذكاء الاصطناعي المستخدمة في الأجهزة الأمنية.

وذلك بإجراء مراجعة نصف سنوية للأنظمة الحالية، وإبرام عقود صيانة وتطوير مع شركات متخصصة لضمان استمرار الكفاءة.

7. دمج الذكاء الاصطناعي في إجراءات العمل اليومية لتسهيل المهام وتعزيز الإنتاجية.

عن طريق تطوير تطبيقات ذكية مخصصة للمهام الميدانية والإدارية، وربطها بشبكات العمل الداخلية لسهولة الوصول والتحديث.

8. تقديم برامج توعوية مكثفة لجميع الفئات بغض النظر عن المؤهل لضمان فهم موحد لأهمية الذكاء الاصطناعي.

وذلك بتنفيذ حملات توعوية دورية عبر المحاضرات، الفيديوهات التثقيفية، والنشرات الداخلية المبسطة.

9. تشجيع تبادل الخبرات بين العاملين لتعزيز الانسجام والتفاهم حول الجهود الأمنية.

من خلال تنظيم لقاءات شهرية وجلسات عصف ذهني مشتركة بين الإدارات، مع عرض قصص نجاح وتجارب عملية.

10. تطوير برامج تدريبية متقدمة لأصحاب المؤهلات العليا لتعزيز القدرات القيادية والتقنية.

من خلال عقد برامج تدريب دولية ومحلية متخصصة في القيادة التقنية، مع توفير فرص ابتعاث قصير المدى للمؤسسات المتقدمة في المجال الأمني.

المراجع:

المراجع العربية:

إبراهيم، علي. (2020). تطبيقات الذكاء الاصطناعي في مواجهة الجرائم الإلكترونية، المجلة القانونية، 1(2). 785.

أبو بكر، خوالد (2019). تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال. الطبعة الأولى: المركز الديموقراطي العربي للدراسات الاستراتيجية والسياسية والاقتصادية، برلين، المانيا

أبو حميد، محمد. (2020). أثر الحافز المادية والمعنوية على أداء العاملين. المجلة العربية للنشر العملي. 21. 6-20.

أبو سمرة، محمود والطيطي، محمد. (2020). مناهج البحث العلمي من التبيين إلى التمكين، اليازوري للنشر والتوزيع، عمان.

أحمد، طارق صادق. (2015). جرائم الهاتف المحمول، دراسة مقارنة بين القانون المصري والإماراتي والنظام السعودي، ط1، المركز القومي للإصدارات القانونية، القاهرة، ص 33.

الأخنش، أمينة والعيداني، محمد. (2023). الذكاء الاصطناعي كآلية لمجابهة الجريمة الإلكترونية، مجلة القانون والعلوم البينية، 2 (2)، 528-544.

آل محيا، عبد الإله ومكين، أروى. (2025). أثر الهندسة الاجتماعية على مخاطر الأمن السيبراني في البنوك في مدينة الرياض في المملكة العربية السعودية، مجلة العلوم الاقتصادية والإدارية والقانونية، 9 (1)، 1-25.

إيمان، حسني. (2022)، توظيف تقنيات الذكاء الاصطناعي في مجال العمل الإعلامي، مجلة الدراسات الإعلامية، 6(21)، 238-245.

إيمان، صبرة. (2020). حقوق المجني عليه في الجرائم الإلكترونية في التشريع الفلسطيني: دارس مقارنة القانون والشريعة الإسلامية، رسالة ماجستير، الجامعة الإسلامية بغزة، فلسطين.

باعشن، نادية. (2011)، دور الذكاء الاصطناعي في إدارة الأعمال، المجلة العلمية للبحوث والدراسات التجارية، (3)، 377-391.

البداينة، ذياب. (2014). الجريمة الإلكترونية المفهوم والأسباب، ندوة علمية حول الجرائم المستحدثة، عمان: الجامعة الأردنية.

بونعارة، ياسمينة (2015). الجريمة الإلكترونية، المعاير جامعة الأمير عبد القادر للعلوم الإسلامية قسنطينة، الجزائر. 39.

تربان، كمال. (2014). دور أكاديمية فلسطين للعلوم الأمنية في تحسين أداء العاملين في وزارة الداخلية والأمن الوطني بغزة وسبل تعزيزه، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، 22 (4)، 175-205.

الجبور، رامي والكريميين، ايمن والمجالي، ماجدة (2020)، العلاقة بين لعبة البوبجي والميل إلى العنف لدى الأبناء من وجهة نظر الآباء والأمهات في المجتمع الأردني –دراسة مسحية على عينة من أهالي إقليم الشمال، مجلة دراسات العلوم الانسانية والاجتماعية، مجلد 47، عدد1.

جيدول، إعمر وقويدر، أحمد. (2019). الحوافز وعلاقتها بأداء العاملين دراسة ميدانية بالشركة الجزائرية للتأمينات وكالة الجفنة، رسالة ماجستير، جامعة زيان عاشور الجفنة، الجزائر.

حجازي، عبد الفتاح بيومي. (2007). مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية ودار شتات للنشر والبرمجيات، المجلة الكبرى، ص 385.

حسني، هنية. ومقاتل، ليلى، (2021)، الذكاء الاصطناعي وتطبيقاته التربوية لتطوير العلمية التعليمية، مجلة علو الإنسان والمجتمع، 10(4).

الحلبي، خالد عياد. (2011). إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، ط1، دار الثقافة للنشر والتوزيع، عمان.

الدبيسي، عبد الكريم (2021)، الإعلام الرقمي وتحديات الذكاء الاصطناعي، عمان: دار المسيرة للنشر.

الدرابيع، العميد. (2023). الحوافز والترقيات وعلاقتها بتحسين أداء المنتسبين في الأمن الوطني الفلسطيني أنموذجاً. رسالة ماجستير. جامعة الخليل. فلسطين. الخليل.

رانا، عبد المحسن. (2022). آليات مكافحة الجرمية الإلكترونية في السعودية: دراسة تحليلية، المجلة القانونية، دون مجلد وعدد.

زايد، أحلام وزموري، كمال. (2021). الذكاء الاصطناعي وتطبيقاته في القطاع الصحي –الإمارات العربية المتحدة نموذجاً–، مجلة البشائر الاقتصادية، 7 (1)، 1–20.

سالمي، نصر الدين، وكمال، بن دقفل. (2020)، دور الذكاء الاصطناعي في عملية تخطيط المنتج في شركة الاتصالات اوريدو الجزائر، مجلة العلوم الاقتصادية والتسيير والعلوم التجارية، 13(1).

سعيد، سمير، أبو جليدة، (2018). أثر استراتيجيات إدارة الموارد البشرية في أداء العاملين في شركات الاتصالات الليبية، رسالة ماجستير منشورة، جامعة الشرق الأوسط، كلية الأعمال، الأردن.

سوالمة، إيناس. (2022). فاعلية تطبيق مبني على الذكاء الاصطناعي في تنمية مهارات التفكير المنطقي والدافعية نحو تعلم الحاسوب لدى طلبة الصف الثامن الأساسي، رسالة ماجستير غير منشورة، جامعة الشرق الأوسط، عمان.

الشاعر، سعود عبد القادر. (2023). دور الذكاء الاصطناعي في تفعيل إجراءات التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة). مجلة البحوث القانونية والاقتصادية. 13(83). 1-37.

الشروقي، خليفة. (2018). تأثير ممارسات إدارة الموارد البشرية في التميز المؤسسي في وزارة الداخلية بمملكة البحرين. بحث مقدم للأكاديمية الملكية للشرطة، كلية تدريب الضباط، قسم الدراسات العليا ضمن متطلبات الحصول على درجة الماجستير في العلوم الإدارية والأمنية (الدفعة الثانية).

صالح، سلمى. (2023). جهود منظمات مكافحة الجريمة المعلوماتية في تحقيق الأمن السيبراني، مجلة دراسات في الخدمة الاجتماعية، 3 (63)، 809-851.

عبد الباقي، مصطفى، (2018) " التحقيق في الجرائم الإلكترونية وإثباتها في فلسطين": دراسة مقارنة. جرائم الحاسوب–فلسطين. مقال نشر في مجلة دراسات: علوم التشريعية والقانون، مج 45، عدد 4، ملحق 2.

عبد الحليم، يعقوب. (2014). الإعلام الجديد والجريمة الإلكترونية، الدار العالمية للنشر، السعودية.

العبيدي، سيف والعبيدي، عمر. (2022)، "دور الإدارة العراقية في مكافحة الجرائم المعلوماتية المخلة بالأمن العام". مجلة الصدى الدراسات القانونية والسياسية المجلد 4 العدد (3)، ص23-46.

العجمي، عبد الله. (2014). المشكلات العلمية والقانونية للجرائم الإلكترونية دراسة مقارنة، رسالة ماجستير، جامعة الشرق الأوسط.

حسنين، فادي. (2020). أثر سياسات إدارة الموارد البشرية على التميز المؤسسي في المؤسسات الدولية العاملة في قطاع غزة، رسالة ماجستير، جامعة القدس، فلسطين.

عضيات، أنس وأبو عيادة، هبة. (2023). تفعيل دور تطبيقات الذكاء الاصطناعي في آلية رصد الجرائم، المجلة العربية للدراسات الأمنية، 39 (2)، 205-219.

عطايا، إبراهيم. (2015). الجريمة الإلكترونية وسبل مواجهتها فـــي الشريعة الإسلامية والأنظمة الدولية (دراسة تحليلية تطبيقية)، مجلة كلية الشريعة والقانون، 30 (2)، 403-360.

عقل، نضال. (2022). أثر نظام إدارة الأداء على أداء العاملين في الأجهزة الأمنية الفلسطينية: الدور المعدل للتدريب والتطوير، رسالة ماجستير، الجامعة العربية الأمريكية، فلسطين.

علي، شريف. (2021). دور الذكاء الاصطناعي في نشر وتعزيز ثقافة السلام في مناطق النزاعات المسلحة، المجلة القانونية.

العمري، حسن. (2021). الذكاء الاصطناعي ودوره في العلاقات الدولية، المجلة العربية للنشر العلمي، (29). 303-321.

العمري، صالح والعمري، عبد الرحمن. (2024). الآثار الاجتماعية للهندسة الاجتماعية في الفضاء الرقمي على المجتمع السعودي، المجلة الدولية للتصاميم والبحوث التطبيقية، 3 (8)، 1-32.

عيسى، عوني سليمان. (2014). الصلابة النفسية وعلاقتها بضغوط الحياة لدى العاملين في المؤسسة الأمنية في محافظتي الخليل وبيت لحم، رسالة ماجستير غير منشورة، جامعة القدس، فلسطين.

فرج، الحسين، (2022). الجريمة الالكترونية وتداعياتها على أمن الوطن والمواطن بين المكافحة القانونية وأجهزة الكشف والتحري. مجلة الإدارة العامة والقانون والتنمية مجلد3، عدد (1)، ص 72-82.

فريدريك، وليتهولد. (2008). التشريعات الصادرة عن السلطة الوطنية الفلسطينية بشِأن قطاع الأمني، ترجمة ياسين السيد، الناشر مركز جنيف للرقابة الديمقراطية على القوات المسلحة، رام الله، فلسطين.

قاسم، مراد. (2024). دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية، المجلة العصرية للدراسات القانونية، 2(2)، 91-114.

القحطاني، حمود. (2017). تطوير القيادات الإدارية ودورها في تحسين الأداء المؤسسي: دراسة تطبيقية على محافظات ومراكز إمارة الرياض.

القرالة، أسحار. (2024). المسؤولية الجزائية عن نشر الأخبار الكاذبة بالوسائل الإلكترونية، رسالة ماجستير، جامعة الشرق الأوسط، عمان.

لخضر، دولي وناصري، نفيسة. (2018). دور الذكاء الاصطناعي في مواجهة الجرائم الالكترونية، مجلة المؤشر للدراسات الاقتصادية، 2(2)، 52-67.

متولي، هالة وفرحات، دعاء (2022)، تقنيات الذكاء الاصطناعي وانعكاساتها على محتوى الرسالة الإعلامية بمواقع الصحف الأجنبية، المجلة المصرية لبحوث الإعلام، (8)، 1495-1522.

محمود، الشاهد. (2024). الإطار القانوني لتأثر الأوراق التجارية الإلكترونية بتقنيات الذكاء الاصطناعي. مجلة المعهد العالي للدراسات النوعية. 4(4).991- 1044.

مرابطي، ميساء. (2023). الجريمة الإلكترونية: بني حدود الخطر وضرورات المواجهة، مجلة الحكومة والقانون الاقتصادي، العدد1.

مسعود، شهيرة. (2021). الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، جامعة عبد الحميد بن باديس مستغانم.

مكاوي، مرام. (2018). الذكاء الاصطناعي على أبواب التعليم، مجلة القافلة، 67 (6)، 21 – 25.

ممدوح، العدوان (2021). المسؤولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة، مجلة القانون والتكنولوجيا، العدد4.

محمد، مها. (2018). الهندسة الاجتماعية وشبكات التواصل وتأثيرها على المجتمع العربي.

منخر فيس، يمنية (2023). الجرائم الإلكترونية عبر مواقع التواصل الاجتماعي ذات الأبعاد الاجتماعية والأخلاقية، مجلة الحقوق والعلم الإنسانية، 2(3).

النعمي، فهمي. (2023). دور الجهات المسئولة عن الجريمة الإلكترونية في اليمن في توعية الجمهور بمخاطر الجريمة الإلكترونية. مجلة جامعة صنعاء للعلوم الإنسانية، مجلد 3 عدد 1.

هلسه، محمد. (2020). أثر إدارة الوقت على أداء العاملين في مديريات التربية والتعليم الفلسطينية: دراسة تطبيقية على مديرية تربية بيت لحم، بحوث ومقالات، مجلة جامعة فلسطين للأبحاث والدراسات.

المراجع الأجنبية

Amistoso, J., Etcuban, J., Gimena, 1j.,. (2019). Performance Management System of a Security Agency in the Philippines, Asian Journal of Managerial Science 8(2):14-21

Al-Marghilani, A. (2022). Target detection algorithm in crime recognition using artificial intelligence. Computers, Materials, & Continua, 71(1), 809-824. doi:https://doi.org/10.32604/cmc.2022.021185

Bachrach, D. G., Wang, H., Bendoly, E., & Zhang, S. (2007). Importance of organizational citizenship behaviour for overall performance evaluation: Comparing the role of task interdependence in China and the USA. Management and Organization Review, 3, 255–276.

Basha, S. (2019). Deep Learning and Parallel Computing Environment for Bioengineering Systems, Dharmendra Singh Rajput, 153-164.

Bozkurt, A. Karadeniz, A. Baneres, D. Guerrero-Roldán, A. Rodríguez, E. (2021). Artificial Intelligence and Reflections from Educational Landscape: A Review of AI Studies in Half a Century. MDPI,13(2), 800; https://doi.org/10.3390/su13020800.

Chiang, W. C., Sun, L., & Walkup, B. R. (2018). Business volatility and employee performance. American Journal of Business, 33(3), 96-119

Christian, M. S., Garza, A. S., & Slaughter, J. E. (2011). Work engagement: A quantitative review and test of its relations with task and contextual performance. Personnel Psychology, 64, 89–136.

Christopher, H. (2017). Social Engineering: The Art of Human Hacking, , WILEY Publishing.

DeNisi, A.S. and Murphy, K.R. (2017). Performance appraisal and performance management: 100 years of progress? Journal of Applied Psychology. 102(3):421.

Jimmy, F.(2024). The Role of Artificial Intelligence in Predicting Cyber Threats. *International Journal of Scientific Research and Management (IJSRM)* 11(08):935-953.

Kaplan, A, Haenlein, M. (2019). Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence, *Business Horizons, Vol. 62, Issue. 1, PP. 15-25*.

Mccarthy, J. (2007). From here to human-level AI. Artificial Intelligence, (171(, 1174-1182.

Miller, A .(2020) .Leadership Styles In Policing And Officers' Job Satisfaction .:*Proquest*

Motowidlo, S. J., & Kell, H. J. (2012). Job Performance. In N. W. Schmitt, & S. Highhouse (Eds.), Handbook of Psychology: Industrial and organizational psychology, 12,. 82-103.

Powelson, K. (2022). The impact of artificial intelligence on anti-money laundering programs to detect and prevent financial crime (Order No. 30241947). Avail- able from ProQuest Dissertations & Theses Global. (2754870882). Retrieved from https://www.pro- quest.com.

Sonnentag, S., Volmer, J., & Spychala, A. (2008). Job performance. In The SAGE Handbook of Organizational Behavior: Volume I - Micro Approaches (pp. 427–450). SAGE Publications Inc

Umair, M. B. (2022). Hybrid of deep learning and exponential smooth- ing for enhancing crime forecasting accuracy. PLoS One, 17(9) https://doi.org/10.1371/journal.pone.0274172.

Zhang, Y. (2012). The impact of performance management system on employee Performance -Analysis with WERS 2004 (Master's thesis, University of Twente).

الملاحق

الملحق رقم (1) قائمة بأسماء المحكمين

الرقم	الاسم	مكان العمل	التخصص
1	د. ماجد حمايل	جامعة القدس المفتوحة	تقنية المعلومات
2	د. يونس جعفر	جامعة القدس المفتوحة	إدارة الأعمال
3	د. مجيد منصور	الجامعة العربية الأمريكية	إدارة الأعمال
4	د. شاهر عبيد	جامعة القدس	إدارة الأعمال
5	د. يوسف أبو زر	جامعة القدس المفتوحة	علوم الحاسوب
6	د. حسين عبد القادر	جامعة الاستقلال	إدارة وتنمية
7	د. فضل عيدة	جامعة القدس المفتوحة	الإدارة العامة
8	د. ميساء بربار	جامعة بيرزيت	إدارة الأعمال
9	د. ماجد ملحم	جامعة القدس المفتوحة	الاقتصاد
10	د. عبد القادر الدراويش	جامعة القدس المفتوحة	إدارة عامة

ملحق رقم (2) الاستبانة

جامعة القدس المفتوحة

عمادة الدراسات العليا والبحث العلمي

برنامج ماجستير القيادة والادارة الاستراتيجية

الموظف الكريم / الموظفة الكريمة

السلام عليكم ورحمة الله وبركاته،

الموضوع: جمع بيانات لأغراض البحث العلمي

في إطار البحث العلمي يقوم الباحث بإجراء دراسة بعنوان:

دور الذكاء الاصطناعي في الحد من انتشار الجرائم الالكترونية: تميز أداء منتسبي الأجهزة الأمنية متغيراً وسيطاً وذلك استكمالا لمتطلبات الحصول على درجة الماجستير في القيادة والادارة الاستراتيجية، آملين تعاونكم بالإجابة على فقرات هذه الاستبانة الموجهة بكل صدق وموضوعية، ومراعاة الدقة قدر الإمكان، نظرا لأهمية أجابتكم على نتائج هذه الدراسة، شاكرين جهودكم وتكريس جزء من وقتكم لتشجيع البحث العلمي، ودعم مسيرة العلم، علماً بأن هذه البيانات ستستخدم لأغراض البحث العلمي فقط.

وتقبلوا فائق الاحترام والتقدير

الباحث: مروان محمود طردة

إشراف: د. رسلان محمد

الرجاء وضع الإشارة (×) في المربع المناسب لرأيكم:

القسم الأول: المعلومات الديمغرافية

الجنس	☐ ذكر	☐ انثى	
المؤهل العلمي	☐ دبلوم فأقل	☐ بكالوريوس	☐ دراسات عليا
المسمى الوظيفي	☐ مدير	☐ رئيس قسم	☐ موظف
سنوات الخبرة	☐ أقل من 10 سنوات	☐ 10–أقل من 20 سنة	☐ 20 سنة فأكثر
الرتبة العسكرية	☐ نقيب فأقل ☐ رائد ☐ مقدم ☐ عقيد ☐ عميد فأعلى		

القسم الثاني: فقرات الاستبانة

الرجاء وضع إشارة (×) أمام كل فقرة بما يناسب درجة استجابتك:

المحور الأول: استخدام تطبيقات الذكاء الاصطناعي (AI): يُعد من أبرز التطبيقات الحديثة للتكنولوجيا في مجال الأمن السيبراني.						
الرقم		موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
البعد الأول: التعلم الآلي (Machine Learning)، وهو الكشف التلقائي عن التهديدات الذي يمنح الآلات القدرة على تحديد الأنماط والتنبؤات بأقل قدر من التدخل البشري للتعرف على الصور المعقدة والنصوص وأنماط البيانات الأخرى لإنتاج رؤى وتوقعات دقيقة.						
.1	تستخدم خوارزميات التعلم الآلي لتحديد الأنشطة المشبوهة، ورصد الهجمات					
.2	يتم تحليل البيانات السابقة والتعلم منها للتنبؤ بأساليب الهجمات القادمة					
.3	يتم تصنيف رسائل البريد الاحتيالية أو التصيّدية بشكل دقيق					
.4	يتم تحديد الرسائل الخطيرة قبل وصولها للمستخدم					
.5	يتم تحليل الأدلة الرقمية بسرعة وبكفاءة					
.6	تستخدم كميات ضخمة من البيانات لتدريب الأنظمة على مواجهة الهجمات السيبرانية المتقدمة					
البعد الثاني: التعلم العميق (Deep Learning)، هو أحد أساليب الذكاء الاصطناعي الذي يعلم أجهزة الكمبيوتر بطريقة مستوحاة من الدماغ البشري للتعرف على الصور المعقدة والنصوص والأصوات وأنماط البيانات الأخرى لإنتاج رؤى وتوقعات دقيقة.						
.7	تستخدم الدوائر الفلسطينية المختصة في مكافحة الجرائم الإلكتروني نماذج التعلم العميق في عملها					
.8	يستخدم التعلم العميق نماذج مثل الشبكات العصبية لكشف البرمجيات الخبيثة					
.9	يتم التعرف من خلال التعلم العميق على الرسائل والمواقع المزيفة للتصدي لهجمات التصيد					
.10	يمكن لنماذج التعلم العميق كشف الهجمات غير المعروفة					
.11	تستطيع خوارزميات التعلم العميق اكتشاف هجمات لم تسجل من قبل					
.12	تساعد نماذج التعلم العميق في تمييز الأنشطة الشاذة التي قد تدل على اختراق الحساب					
.13	تساعد نماذج التعلم العميق في الكشف عن حملات التضليل والابتزاز أو التخطيط لهجمات إلكترونية					
المحور الثاني: الحد من انتشار الجرائم الالكترونية: هو التقليل من الأنشطة غير القانونية التي تُنفذ باستخدام التكنولوجيا الرقمية والذكاء الاصطناعي لاستهداف الأفراد أو المؤسسات، سواء من خلال سرقة البيانات، أو التحايل المالي، أو انتهاك الخصوصية، أو نشر						

الشائعات المضللة وغير ذلك من ممارسات خطيرة، الأمر الذي يتطلب مزيجاً من التقنيات المتقدمة والتشريعات الصارمة، والوعي المجتمعي.						
البعد الأول: الاحتيال المالي: هو نوع من أنواع الجرائم الإلكترونية التي يهدف المجرم من خلاله إلى سرقة الأموال أو الحصول على مزايا مالية بطرق غير مشروعة، وغالباً ما يتم ذلك عبر الإنترنت باستخدام بأساليب ذكية ومضللة						
.14	يتم تحذير المواطنين من التعامل مع أية رسائل تطالبه بإدخال بياناته البنكية					
.15	يتم تعريف المؤسسات المصرفية المحلية بأشكال ومخاطر الاحتيال المالي					
.16	تستخدم أنظمة مراقبة ذكية تعتمد على الذكاء الاصطناعي لمكافحة الاحتيال المالي					
.17	يتم استخدام نماذج التعلم الآلي للتعرف على محاولات اختراق الحسابات المالية					
.18	تستخدم أنظمة التعرف على السلوك لحماية البنوك والمصارف					
.19	تستخدم خوارزميات التعرف على الوجوه، وبصمات الصوت، وأنماط الكتابة في تتبع هوية الجناة في مجال التحايل المالي					
البعد الثاني: سرقة البيانات، هي واحدة من أخطر الجرائم الإلكترونية في الوقت الحاضر، لأنها قد تفتح الباب للاحتيال أو الابتزاز أو حتى انتهاك الخصوصية الشخصية والمؤسساتية						
.20	تنظم حملات توعية مستمرة لتحذير المواطنين من سرقة بياناتهم					
.21	تتوفر البنية التحتية لمكافحة سرقة البيانات الإلكترونية					
.22	تتخذ إجراءات احترازية للحفاظ على سرية البيانات الإلكترونية للمواطنين					
.23	يتم تعريف المواطنين بحالات متنوعة حول سرقة البيانات					
.24	يتم التعامل بشكل فعّال مع حالات سرقة البيانات					
.25	تسترجع المؤسسات والدوائر المختصة البيانات في حالة تعرضها للسرقة					
ثالثاً: انتهاك الخصوصية، هو التعدي على حق شخص فيما يتعلق بمعلوماته الشخصية أو حياته الخاصة، ويحدث هذا الانتهاك بطرق عديدة كنشر صور أو بيانات لشخص آخر دون موافقته، أو التنصت على مكالماته، أو اختراق حساباته الإلكترونية، أو جمع معلومات عنه دون علمه.						
.26	تنتشر ظاهرة انتهاك الخصوصية الإلكترونية للمواطنين					
.27	يتم توعية المواطنين بعدم تبادل بياناتهم الخاصة مع أي كان					
.28	تنسق وزارة الداخلية مع المؤسسات المختصة الأخرى في مجال الأمن السيبراني					
.29	يتم مراقبة الشبكات لاكتشاف أي نشاط مشبوه أو غير مصرح به					
.30	تستخدم أنظمة كشف التسلل أو منعه					

.31	يتم متابعة الأفراد أو المؤسسات التي تعرضت للانتهاك					
رابعاً: نشر الشائعات والبيانات المضللة، يعد من السلوكيات الخطيرة، خاصة في عصر الإنترنت ووسائل التواصل الاجتماعي، كنشر الأخبار غير المؤكدة، والمعلومات الخاطئة، بقصد خداع الآخرين وإثارة البلبلة أو الذعر أو تشويه سمعة شخص أو جهة معينة أو التأثير على الرأي العام، وكل هذه الممارسات الخطيرة تؤثر على الأمن المجتمعي والثقة العامة والقرار الفردي،						
.32	تستخدم خوارزميات الذكاء الاصطناعي لرصد المحتوى المشبوه					
.33	يتم التعاون مع شركات التكنولوجيا مثل تويتر وفيس بوك لحذف المحتوى المضلل					
.34	يتم استقطاب الأفراد ذوي الخبرة في مجال مكافحة الجرائم الإلكترونية للعمل في الأجهزة المختصة					
.35	يتم إطلاق حملات تحذر من تصديق أو مشاركة كل ما ينشر					
.36	يتم نشر أدوات تساعد الناس على التمييز بين الصحيح والزائف					
.37	يتم اتخاذ إجراءات قانونية صارمة بحق مروجي الشائعات المضللة					
المحور الثالث: تميز أداء منتسبي الأجهزة الأمنية: هو قدرة العاملين على التعامل بفعالية مع التكنولوجيا الحديثة وخاصة الذكاء الاصطناعي، لمواجهة التحديات المرتبطة بالجرائم الإلكترونية. ويشمل ذلك مهاراتهم في فهم الأنظمة الذكية، واستخدامها بشكل صحيح، وتحليل المخاطر الأمنية، بالإضافة إلى الاستجابة السريعة والدقيقة للتهديدات لتحقيق الحماية الإلكترونية المطلوبة						
أولاً: تنفيذ المهام						
.38	أُظهر حرصاً دائماً على جودة العمل الذي أقدمه.					
.39	أتمكّن من استخدام الأدوات التكنولوجية المطلوبة لإنجاز المهام بكفاءة.					
.40	أراجع نتائج عملي بشكل دائم لضمان دقتها.					
.41	أتعامل مع ضغوط العمل بكفاءة دون أن يؤثر ذلك على جودة أدائي.					
.42	يتم التعاون مع أطراف دولية لتنفيذ مهام العمل					
ثانياً: التحلي بالمسؤولية						
.43	أبادر في تقديم الملاحظات البناءة لتحسين العمل الجماعي.					
.44	أعمل على خلق بيئة عمل إيجابية بين زملائي.					
.45	أُظهر احترامًا دائمًا لقوانين المؤسسة وثقافتها التنظيمية.					
.46	أساند زملائي خلال الأزمات أو أوقات الضغط الكبير في العمل.					
ثالثاً: التطور الوظيفي						
.47	أتعامل مع التغييرات المفاجئة في المهام بكفاءة.					
.48	أبحث باستمرار عن فرص لتطوير مهاراتي في استخدام الذكاء الاصطناعي.					
.49	أتعلم من التجارب السابقة لتعديل طريقة عملي نحو الأفضل.					
.50	أتكيف مع اختلاف ظروف العمل دون التأثير على الإنتاجية.					

رابعاً: تحقيق الأهداف						
.51	أضع خطة واضحة لتحقيق المهام المرتبطة بأهداف المؤسسة الأمنية					
.52	أتابع مؤشرات الأداء لضمان تحقيق الأهداف بدقة.					
.53	أستخدم التحليل الذكي للبيانات لتقييم فعالية العمليات الأمنية.					
.54	أعمل باستمرار على تحسين مستوى أدائي لتحقيق الأهداف العامة للمؤسسة.					

انتهى الاستبيان