مؤشر مقترح للإفصاح عن استخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية

إعداد

أ/ نورهان صبحي محمد عطية

مدرس مساعد محاسبة بمعهد أكتوبر العالي للهندسة والتكنولوجيا

٢٠٢٥م – ١٤٤٦هـ

قسم المحاسبة والمراجعة ... كلية التجارة ... جامعة مدينة السادات

ملخص الدراسة

تمثل الهدف الرئيسي للدراسة في تقديم مؤشر مقترح للإفصاح عن استخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية، وتناولت الدراسة طبيعة وأهمية الإفصاح عن إستخدام نظم الذكاء الاصطناعي. فضلاً عن دراسة وتحليل أهم متطلبات الإفصاح عن الذكاء الاصطناعي والنظريات الداعمة لذلك. بالإضافة إلى أثر الافصاح عن إستخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية، من خلال بيان تأثير كلاً من الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية، الإفصاح عن كشف التهديدات للهجمات السيبرانية، الإفصاح عن وقت الاستجابة للهجمات السيبرانية، الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية على الحد من مخاطر الهجمات السيبرانية. وأظهرت نتائج الدراسة التطبيقية وجود أثر الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية على الحد من مخاطر الهجمات السيبرانية. وكذلك وجود أثر الإفصاح عن كشف التهديدات للهجمات السيبرانية على الحد من مخاطر الهجمات السيبرانية ". كما توصلت الدراسة إلى وجود أثر للإفصاح عن وقت الاستجابة للهجمات السيبرانية على الحد من مخاطر الهجمات السيبرانية ". وأخيراً وتوصلت الدراسة إلى وجود أثر للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية على الحد من مخاطر الهجمات السيبرانية.

القسم الأول: الإطار العام للدراسة

١/١ ـ مقدمة:

يعيش العالم اليوم ثورة حقيقية في مجال الاتصالات وتكنولوجيا المعلومات ولم يعد بإمكان أي دولة تتطلع إلى الإنجاز والتطوير، بهدف تحقيق التنمية المستدامة على كافة الأصعدة، أن تحقق ذلك دون أن يكون هذا القطاع أحد ركائزها الأساسية. وقد بدأت وزارة الاتصالات عملها منذ عام ١٩٩٩، لتطوير قطاع تكنولوجيا المعلومات والاتصالات الوطني. وتسعى الوزارة جاهدة لتحقيق الاقتصاد الرقمي من خلال استخدام أدوات تكنولوجيا المعلومات والاتصالات لتوفير العدالة الاجتماعية للجميع. وتتمثل مهمتها في تمكين تطوير مجتمع قائم على المعرفة، واقتصاد رقمي قوي يعتمد على التمتع بالحقوق الرقمية، إلى جانب تطوير صناعة تكنولوجيا المعلومات والاتصالات الوطنية التنافسية والإبداعية. وتدعم استراتيجية الاتصالات وتكنولوجيا المعلومات ٢٠٣٠ تحقيق أهداف رؤية مصر ٢٠٣٠ من خلال بناء مصر الرقمية .وتشمل هذه الأهداف تطوير البنية التحتية لتكنولوجيا المعلومات والاتصالات، وتعزيز الشمول الرقمي، وتحقيق الشمول المالي، وتعزيز بناء القدرات وتشجيع الابتكار، ومحاربة الفساد، وضمان الأمن المعلوماتي، وتعزيز مكانة مصر على المستويين الإقليمي والدولي (تقرير إستراتيجية مصر ٢٠٣٠ في الاتصالات وتكنولوجيا المعلومات، ٢٠٢١).

أدى ظهور التقنيات الجديدة في نظم المعلومات والتكنولوجيا الرقمية إلى ترابط غير مسبوق بين بلدان العالم والشركات والأفراد مما زاد من مخاطر الهجمات السيبرانية. وازدادت في الأونة الأخيرة كثافة وخطورة هذه الهجمات مما جعل بعض المنظمات الدولية مثل صندوق النقد الدولي والمنتدى الاقتصادي العالمي تضع المخاطر الهجمات السيبرانية في صدارة المخاطر النظامية التي تواجه النظام الاقتصادي العالمي. وتُعد الهجمات السيبرانية من أبرز

التهديدات التي تواجه المنشآت في العصر الرقمي، حيث تتسبب في خسائر مالية فادحة، وتسريب معلومات حساسة، وتراجع ثقة العملاء والمستثمرين. وتتمثل هذه الهجمات في أشكال متعددة، مثل البرامج الخبيثة، والتصيد الإلكتروني، والاختراقات المتعمدة للأنظمة والشبكات. وتكمن خطورة هذه التهديدات في تطورها المستمر وتعقيدها المتزايد، لا سيما مع استخدام تقنيات الذكاء الاصطناعي من قِبل المهاجمين لتنفيذ هجمات ذكية يصعب اكتشافها بالطرق التقليدية. كما أن الاعتماد المتزايد على التكنولوجيا والتكامل الرقمي بين الأنظمة يزيد من اتساع تعرض الشركة للهجوم، مما يجعل من الضروري تبني أنظمة دفاع متقدمة وإستراتيجيات أمن معلومات شاملة لمواجهة هذه المخاطر وضمان استمرارية الأعمال وسلامة البيانات (بانقا،٢٠١٩).

وفي إطار ما شهدته الأونة الأخيرة من تطورات مذهلة في الأجهزة والألات والأنظمة الذكية والتي توجت بالثورة الصناعية الرابعة، وما أفرزته من العديد من تقنيات الذكاء الاصطناعي، والتي تسهم في تعزيز القدرة علي معالجة البيانات باستخدام نظم الذكاء الاصطناعي، الأمر الذي دفع المنشآت نحو إطلاق مواقعها الإلكترونية علي شبكة الإنترنت وتحميلها ببيانات كمية ووصفية وصور وجداول مهيكلة وغير مهيكلة، وذلك كمصدر متجددا للبيانات والمعلومات الملائمة والموثقة لاتخاذ القرارات التي تتعلق بالجوانب المالية والاجتماعية والبيئية على حد سواء (Agyei-Mensah,2017).

ومع الانتشار السريع لاستخدام الذكاء الاصطناعي (AI) في الشركات على مدى العقد الماضي، ظهرت بعض المخاوف بشأن حقوق الإنسان، وأمن أو خصوصية البيانات وغيرها من القضايا الأخلاقية التي يمكن أن تكون على المحك بسبب عدم السيطرة على استخدام الذكاء الاصطناعي والهجمات السيبرانية التي قد تواجه الشركات. ومع ذلك، فإن المخاوف المتعلقة بالشفافية في استخدام الذكاء الاصطناعي لم تنعكس بعد في أي معايير للإفصاح عن المعلومات غير المالية، ولا في اللوائح الحالية. ويعد الافصاح المحاسبي عن استخدام نظم الذكاء الاصطناعي- كونه حديثًا- اختياريا، وهذا يعني عدم توحيد في معايير الإفصاح من حيث محتوى الإفصاح والكمي ومكان الإفصاح (Bonsón et al., 2021).

وتستهدف هذه الدراسة تقديم مؤشر مقترح للإفصاح عن إستخدام الذكاء الاصطناعي في محاولة لزيادة مستوى إفصاحات الشركات عن إستخدام التقنيات الحديثة من أجل المساعدة في الحد من مخاطر الهجمات السيبرانية التي قد تواجه الشركات، واقتراح مجموعة من العناصر ذات الصلة لهيكلة المعلومات بشأن استخدام الشركات للذكاء الاصطناعي لتحسين الشفافية وتخفيف المخاطر وإظهار مسؤولية حقيقية للشركات عند استخدامها لهذه التقنيات.

٢/١ ـ مشكلة الدراسة:

بدأت التطورات الأخيرة في الذكاء الاصطناعي وتقنياته في إعادة تشكيل نماذج أعمال الشركات نتيجة إدخال الابتكارات التكنولوجية في جميع عملياتها. وجاءت هذه التقنيات لتعطي للشركات فرصًا جديدة لزيادة الربحية والعائد على نسبة رأس المال من خلال الكفاءة العالية، وتوفير التكاليف، وتوليد الإيرادات، العمل بجودة أعلى، أو زيادة رضا الموظفين وتنويع المصادر الجديدة لخلق القيمة، وأن تصبح أكثر تنافسية ومستدامة. وتعد الأتمتة الذكية استثماراً رئيسياً للشركات في كل مكان حول العالم. حيث تساعد الشركات في إدارة العمليات التجارية، التعلم الآلي وأتمتة العمليات الروبوتية. ويرى أنصار ثورة الذكاء الاصطناعي أن هذا التطور خطوة للأمام لمواجهة تحديات المستقبل (Stancheva-Todorova,2018).

ومع ذلك، قد يؤدي استخدام الذكاء الاصطناعي إلى إثارة بعض المخاوف حول حقوق الإنسان أو أمن البيانات أو الخصوصية أو غيرها من القضايا الأخلاقية التي تنتج عندما يتم دمج الذكاء الاصطناعي في عمليات صنع القرار. حيث إن نماذج أعمال الشركات في ظل إستخدام تقنيات الذكاء الاصطناعي تتمتع بمستوى عالٍ من الأتمتة، وجمع ضخم للبيانات وبالتالي احتمال حدوث التلاعب والتحيزات وتسريب هذه البيانات أو استغلالها، وعلى الرغم من المخاطر المحتملة الكبيرة في الآونة الأخيرة الناتجة عن إستخدام تقنيات الذكاء الاصطناعي، لم يتم وضع أي تشريع للتخفيف من مخاطر استخدام الذكاء الاصطناعي من خلال مطالبة الشركات بالتمتع بشفافية عالية حيال ذلك. ومع ذلك، فقد بدأت بالفعل بعض الشركات في الحد من هذه المخاوف من خلال الافصاح طوعا عن هذه المعلومات في غير المالية الخاصة بهم. مستوحاة جزئيًا من مبادرات المفوضية الأوروبية مثل المبادئ التوجيهية الأخلاقية للذكاء الاصطناعي الموثوق به، المنشورة في ٢٠١٩، أو ما يعرف بالورقة البيضاء عن الذكاء الاصطناعي: "نهج أوروبي للتميز والثقة"، حيث شملت على اللائحة الأوروبية لأسس الذكاء الاصطناعي، قانون الذكاء الاصطناعي، الذي نُشر في أبريل ٢٠٢١ (Bonsón and Bednárová,2022)

ويعتبر الإفصاح عن الذكاء الاصطناعي أمرًا جديدًا تمامًا، وهذا يعني ضمناً الافتقار إلى توحيد معايير هذا الافصاح. لذلك، أولاً، يجب التوصل إلى توافق في الآراء بشأن كيف يتم الإفصاح؛ ما هي العناصر الأساسية للإفصاح عن استخدام الذكاء الاصطناعي؟ وما هي المعلومات التي يجب أن تكون تم الافصاح عنها لتلبية الاحتياجات المعلوماتية لمختلف أصحاب المصلحة، وذلك من خلال الإفصاح عن تلك المعلومات في تقارير الاستدامة لتحقيق شفافيتها في ضوء نقص المبادئ التوجيهية للإفصاح عن إستخدام الذكاء الاصطناعي.

ويعد الإفصاح عن استخدام نظم الذكاء الاصطناعي خطوة حيوية نحو تحقيق اقتصاد عالمي مستدام من خلال ما تقدمه من تعزيز لمساءلة الشركات عن الآثار المترتبة على أنشطتها المختلفة، وأصبح هناك حاجة ماسة إلى الإفصاح المحاسبي عن تقنيات الذكاء الاصطناعي التي تستخدمها الشركة والمخاطر المرتبطة بهذه التقنيات، (والذي يعتبر جزء مهم من المسؤولية الرقمية للشركات)؛ لتحسين الشفافية، التخفيف من المخاطر وإثبات مسؤولية الشركة الناتجة عن استخدام الذكاء الاصطناعي. **ومن ثم يمكن صياغة مشكلة الدراسة في مجموعة من الأسئلة التالية:**

١/٢ ما هي أهمية استخدام نظم الذكاء الاصطناعي، وما هي مزايا استخدامها في شركات الاتصالات؟
٢/٢ ما هي متطلبات الإفصاح المحاسبي عن استخدام نظم الذكاء الاصطناعي في شركات الاتصالات؟
٣/٢ ما هي أهم التحديات والمخاطر التي تواجه شركات الاتصالات عند استخدام نظم الذكاء الاصطناعي؟
٤/٢ إلى أي مدى يؤثر الإفصاح المحاسبي عن إستخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية؟

١/٣ـ أهداف الدراسة:

يتجسد الهدف الرئيسي للدراسة في تقديم مؤشر مقترح للإفصاح المحاسبي عن استخدام نظم الذكاء الاصطناعي وانعكاس ذلك على الحد من مخاطر الهجمات السيبرانية، **وذلك سعيًا نحو تحقيق الأهداف الفرعية التالية:**

- ١/٣ تحديد أهمية استخدام نظم الذكاء الاصطناعي، والكشف عن مزايا استخدامها في شركات الاتصالات.
- ٢/٣ التعرف على متطلبات الإفصاح المحاسبي عن استخدام نظم الذكاء الاصطناعي في شركات الاتصالات.
- ٢/٣ دراسة وتحليل أهم التحديات والمشاكل التي تواجه تطبيق إستخدام نظم الذكاء الاصطناعي في شركات الاتصالات.
- ٣/٣ التعرف على مدى تأثير الإفصاح المحاسبي عن إستخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية.

٤/١ـ أهمية الدراسة:

يمكن إبراز أهمية الدراسة من حيث الأهمية العلمية والعملية على النحو التالي:

- **الأهمية العلمية:** تتمثل الأهمية العلمية للدراسة في النقاط التالية:

أ. تزايد الحاجة إلى الإفصاح المحاسبي عن إستخدام نظم الذكاء الاصطناعي سواء بالنسبة للوحدة الاقتصادية أو المجتمع ككل لما له من انعكاس على زيادة المصداقية لدي أصحاب المصالح، التي تُمثل أحد أركان الشفافية والمساءلة في بيئة الأعمال الرقمية.

ب. تأتى أهمية الدراسة من خلال إظهار مدى الحاجة إلى الإفصاح المحاسبي عن إستخدام نظم الذكاء الاصطناعي بما يخدم متخذي القرارات الاستثمارية والعملاء.

ج. تقييم مدى التزام الشركات بالإفصاح عن الاستخدام الفعلي لنظم الذكاء الاصطناعي في التصدي للمخاطر السيبرانية.

د. تتضح أهمية الدراسة من الناحية العلمية من خلال متابعة الجهود العلمية والدراسات التي تم إجراءها في هذا المجال بغرض تقديم مؤشر مقترح للإفصاح عن إستخدام نظم الذكاء الاصطناعي من أجل توفير دليل من الناحية التطبيقية على أهمية الالتزام من قبل شركات الاتصالات بالإفصاح المحاسبي عن إستخدام نظم الذكاء الاصطناعي والمخاطر المختلفة المرتبطة به.

هـ. ندرة الأبحاث العربية – في حدود علم الباحثة – التي تطرقت إلى الإفصاح المحاسبي عن إستخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية في حدود علم الباحثين.

- **الأهمية العملية:** تتمثل الأهمية العملية للدراسة في النقاط التالية:

أ. إن الإفصاح عن معلومات لمدى إستخدام نظم الذكاء الاصطناعي يوفر معلومات لأصحاب المصلحة حول مدى ثقتهم في هذه الشركات والمخاطر المتوقعة لاستخدام هذه التقنيات.

ب. تقديم دليل عملي حول مدى إفصاح شركات الاتصالات عن استخدام نظم الذكاء الاصطناعي وانعكاس ذلك على الحد من مخاطر الهجمات السيبرانية في هذه الشركات.

ج. تقديم دليل عملي حول الغرض من قيام شركات الاتصالات بالإفصاح المحاسبي عن استخدام نظم الذكاء الاصطناعي وانعكاس ذلك على الحد من مخاطر الهجمات السيبرانية.

١/٥ـ منهجية الدراسة:

وتشمل منهجية الدراسة على منهج الدراسة والأساليب الإحصائية وأساليب جمع البيانات على النحو التالي:

أ. منهج الدراسة: تتبني الدراسة على المنهج الاستنباطي والمنهج الاستقرائي على النحو التالي:

- ✓ **المنهج الاستنباطي:** يعتمد الباحثون على المنهج الاستنباطي وذلك لبناء الإطار النظري للدراسة، وصياغة مشكلة وفروض الدراسة، وذلك من خلال دراسة وتحليل الدراسات السابقة المرتبطة بموضوع الدراسة والبحوث العلمية المنشورة بالدوريات والمجلات العلمية وعلى شبكة الانترنت التي تخص موضوع الدراسة، بهدف تقديم مؤشر مقترح للإفصاح عن استخدام نظم الذكاء الاصطناعي للحد من مخاطر الهجمات السيبرانية.
- ✓ **المنهج الاستقرائي:** يستخدم الباحثون المنهج الاستقرائي في إعداد الدراسة التطبيقية واستخدام أسلوب تحليل المحتوي لعينة من شركات الاتصالات في البيئة المصرية لقياس مستوى الإفصاح المحاسبي عن استخدام نظم الذكاء الاصطناعي والمخاطر المرتبطة بذلك.

ب. أساليب جمع البيانات:

يتم إستخدام أسلوب تحليل المحتوي الذي يبني على البيانات الفعلية المستخرجة من تقارير الشركات محل الدراسة، ونشرات كتاب الإفصاح الصادر عن بورصة الأوراق المالية المصرية والمواقع الإلكترونية لهذه الشركات.

٦/١ـ خطة الدراسة:

القسم الأول: الإطار العام للدراسة.

القسم الثاني: عرض وتحليل الدراسات السابقة.

القسم الثالث: الإطار النظري

القس الرابع: الدراسة التطبيقية

النتائج والتوصيات

القسم الثاني: عرض وتحليل الدراسات السابقة

يمكن عرض وتحليل الدراسات السابقة حسب ارتباطها بمتغيرات الدراسة وذلك من خلال تقسيم الدراسات السابقة إلى مجموعتين على النحو التالي:

١/٢- المجموعة الأولى: الدراسات السابقة التي تناولت الإفصاح المحاسبي عن نظم الذكاء الاصطناعي:

استهدفت دراسة (Bonsón, et al., 2021(A)) بعنوان" Artificial Intelligence Disclosure in the Annual Reports of Spanish IBEX-35 Companies (2019–2018)" التعرف على مدى قيام الشركات بالإفصاح المحاسبي عن إستخدام الذكاء الاصطناعي، وكذلك التعرف على أي نوع من التقارير التي يتم الإفصاح فيها، والتعرف على المعلومات التي يتم الإفصاح عنها المتعلقة بالذكاء الاصطناعي. وكذلك التعرف على المبادئ أو اللوائح الأخلاقية التي يجب أن تتبعها تطبيقات الذكاء الاصطناعي وكيف يجب أن يتم الإفصاح عنها. وأجريت الدراسة على الشركات الإسبانية من خلال تحليل مقارن مع بيانات ٢٠١٨ و٢٠١٩ في تقارير الاستدامة للتحقق من كيفية تطور الإفصاح المحاسبي عن الذكاء الاصطناعي، وذلك لاكتساب رؤى لتطوير إرشادات المعلومات غير المالية المتعلقة بالذكاء الاصطناعي. وتوصلت النتائج إلى إن تقارير الذكاء الاصطناعي آخذة في الازدياد بسبب الاهتمام بهذه التقنيات في الشركات ولكنه ينمو بطريقة غير منظمة، وأن اعتماد الأساليب الأخلاقية للذكاء الاصطناعي في غاية الأهمية في المرحلة الأولية. كما خلصت الدراسة إلى ان هناك حاجة لمبادئ توجيهية واضحة حول ماهية المعلومات ذات صلة للإفصاح عن الذكاء الاصطناعي وإلزامية للشركات للإفصاح عنها والمبادئ الأخلاقية أو اللوائح التي يجب أن تمتثل لها تطبيقات الذكاء الاصطناعي حتى يمكن تنفيذها دون آثار سلبية على المجتمع. شملت المعلومات التي يتم الإفصاح عنها في تقارير الاستدامة في: التطبيقات التي تطورها هذه الشركات و/أو تستخدمها، ومبادرات إستخدام تقنيات الذكاء الاصطناعي، المخاطر المحتملة المتعلقة بالذكاء الاصطناعي، المشاكل الأخلاقية الناشئة عن استخدام هذه التقنيات.

وتناولت دراسة (Bonsón, et al.,2021(B)) بعنوان" Artificial intelligence activities and ethical approaches in leading listed companies in the European Union". التعرف على المعلومات المتعلقة بالذكاء الاصطناعي (AI) المدرجة من قبل الشركات الأوروبية المدرجة في تقاريرها السنوية و / أو تقارير الاستدامة، وكذلك تقديم إطار متكامل لممارسات الإفصاح باستخدام تقنيات الذكاء الاصطناعي في الشركات الأوروبية. وذلك للتأكد من الافصاحات المتعلقة بتطوير واستخدام الشركات لتقنيات الذكاء الاصطناعي، تحديد مدى إفصاح الشركات عن المبادئ أو الإرشادات الأخلاقية المتعلقة بالذكاء الاصطناعي والتعرف على العوامل التي تفسر هذه الممارسات. وأجريت الدراسة على عدد ٢٠٠ تقرير لعدد من الشركات المدرجة في المؤشرات الرئيسية لألمانيا والسويد وفنلندا وفرنسا وإسبانيا وإيطاليا، من منظور نوعي وكمي. يتم تحليل جميع التقارير باستخدام منهجية تحليل المحتوى لتحديد تعبيرات مثل "الذكاء الاصطناعي" و"التعلم الآلي" و"التعلم العميق" و"البيانات الضخمة"، ثم تصنيفها وفقًا لذلك. وتوصلت نتائج الدراسة إلى أن هناك اهتمام متزايد بتقنيات الذكاء الاصطناعي، على الرغم من أن ٤١.٥٪ من الشركات لا تبلغ عن أي نشاط في مجال الذكاء الاصطناعي، كما أنه لا يزال اعتماد الأساليب الأخلاقية للذكاء الاصطناعي في مرحلة أولية للغاية، وتبلغ نسبة أقل من

٥٪ من الشركات عن هذه المسألة. كما يُظهر التحليل الكمي أن الشركات الكبرى والشركات في صناعات التكنولوجيا والاتصالات والشركات الموجودة في بلدان الجنوب تعتبر من أكثر الشركات التي تفصح عن نشاط الذكاء الاصطناعي. كما أن غالبية الشركات التي تفصح عن المبادئ الأخلاقية تنتمي إلى صناعات التكنولوجيا والاتصالات.

بينما سعت **دراسة (Bonsón & Bednárová, 2022) بعنوان" Artificial Intelligence Disclosures in Sustainability Reports: Towards an Artificial Intelligence Reporting Framework"** إلى التعرف على العناصر الأساسية والمعلومات التي يجب أن يتم الافصاح عنها لتلبية الاحتياجات المعلوماتية لمختلف أصحاب المصلحة، واقتراح والتحقق من صحة مجموعة من العناصر العامة التي يجب الافصاح عنها لهيكلة المعلومات حول الذكاء الاصطناعي والتي تعتبر جزء مهم من المسؤولية الرقمية للشركات لتحسين الشفافية، والتخفيف من المخاطر وإثبات المسؤولية الحقيقية في استخدام الذكاء الاصطناعي. وتم تقديم الاستبيان عبر الإنترنت لمعرفة الرأي حول أهمية كل عنصر من العناصر المقترحة كدليل للإفصاح عن المعلومات المتعلقة باستخدام الذكاء الاصطناعي في التقارير غير المالية. من خلال دليلاً تضمن عناصر المعلومات العامة (نموذج حوكمة الذكاء الاصطناعي؛ الأخلاق والمسؤولية؛ الإستراتيجية) وذلك لتطوير معايير تقارير الذكاء الاصطناعي. **وتوصلت** الدراسة إلى أن بعض نظم الذكاء الاصطناعي التي تستند إلى المعلومات الشخصية لها عواقب على خصوصيتهم. ويوجد مبادرات مثل قانون حماية المعلومات الشخصية والوثائق الإلكترونية في كندا، وتمثلت المعلومات التي تم الاتفاق عليها للإفصاح عن الذكاء الاصطناعي تتمثل في: نموذج الحوكمة ومراقبة النظام والتي تتمثل في كيفية إدارة الذكاء الاصطناعي داخل المنظمة ومعلومات حول المراقبة المستمرة. الأخلاق والنزاهة والمتمثلة في الأخلاق المتعلقة باستخدام الذكاء الاصطناعي. وأخيراً الإستراتيجية والمتمثلة في كيفية الإفصاح المحاسبي عن المخاطر المرتبطة بالذكاء الاصطناعي وتحديدها وإدارتها.

وتناولت دراسة (Shiyyab et al.,2023) بعنوان" The impact of artificial intelligence disclosure on financial performance"، تحديد مدى إفصاح البنوك الأردنية عن استخدامها لتقنيات الذكاء الاصطناعي في عملياتها، وتأثير الإفصاح عن المصطلحات المرتبطة بالذكاء الاصطناعي على الأداء المالي. وأجريت الدراسة على البنوك الأردنية من خلال تحليل المحتوى لتحليل انتشار الذكاء الاصطناعي والمعلومات ذات الصلة في البيانات النصية للتقارير السنوية من ١١٥ تقريراً سنوياً لـ ١٥ بنكاً أردنياً مدرجاً في بورصة عمان للفترة من ٢٠١٤ إلى ٢٠٢١، وتوصلت نتائج الدراسة إلى زيادة مستمرة في ذكر مصطلحات مرتبطة بالذكاء الاصطناعي منذ عام ٢٠١٤. ومع ذلك، لا يزال مستوى الإفصاح المرتبط بالذكاء الاصطناعي ضعيفاً في بعض البنوك، مما يشير إلى أن البنوك الأردنية ما زالت في المراحل الأولى من تبني وتنفيذ تقنيات الذكاء الاصطناعي. كما تشير النتائج إلى أن الإفصاح عن الكلمات المفتاحية المرتبطة بالذكاء الاصطناعي له تأثير على الأداء المالي للبنوك، حيث أن للذكاء الاصطناعي تأثيراً إيجابياً على الأداء المحاسبي من حيث العائد على الأصول (ROA) والعائد على حقوق الملكية (ROE)، وتأثيراً سلبياً على إجمالي النفقات، مما يدعم الرأي السائد بأن الذكاء الاصطناعي يعزز الإيرادات ويقلل التكاليف.

وقدمت دراسة (Weaver, 2024) بعنوان "The Artificial Intelligence Disclosure (AID) Framework: An Introduction". إطاراً للإفصاح عن الذكاء الاصطناعي شامل ومفصل يهدف إلى تطوير الافصاح عن الذكاء الاصطناعي من خلال تقارير الاستدامة، وتوصلت الدراسة إلى أن تقديم إطار للإفصاح عن الذكاء الاصطناعي يوفر طريقة للشفافية في استخدام الذكاء الاصطناعي تكون واضحة ومتسقة وموجزة وقابلة للاستخدام البشري والآلي. مما يسمح للمستخدمين بإنجاز أفضل للأعمال بشكل أسرع وأكثر كفاءة دون إغفال الإضافات البشرية الحاسمة. وخلصت الدراسة إلى أن اعتماد نهج متسق للإفصاح عن الذكاء الاصطناعي من خلال إطار عمل يبسط التوقعات والعناصر اللازمة للحفاظ على الأخلاقيات المتعلقة بالذكاء الاصطناعي.

٢/٢- المجموعة الثانية: الدراسات السابقة التي تناولت العلاقة بين استخدام نظم الذكاء الاصطناعي ومخاطر الهجمات السيبرانية:

تناولت دراسة (Radanliev et al.,2020) بعنوان: "Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains" تحليل تأثير تقنيات الذكاء الاصطناعي والتعلم الآلي على سلاسل التوريد في الصناعة، واستكشاف كيف يمكن لهذه التقنيات تعزيز مرونة وأمان سلاسل التوريد، خاصة في المنشآت الصغيرة والمتوسطة. بالإضافة إلى تطوير إطار تحليلي لتقييم المخاطر السيبرانية يمكنه التنبؤ بالمخاطر السيبرانية وتحليلها في الوقت الحقيقي، مما يساعد في اتخاذ قرارات مستنيرة لتعزيز الأمان السيبراني. وتوصلت الدراسة إلى أن النظام المقترح المدعوم بالذكاء الاصطناعي والتعلم الآلي يمكنه التكيف مع التهديدات السيبرانية المتغيرة وتحليل المخاطر في الوقت الحقيقي، مما يعزز من مرونة سلاسل التوريد. وأبرزت الدراسة أن دمج تقنيات الذكاء الاصطناعي والتعلم الآلي مع إنترنت الأشياء الصناعي يمكن أن يؤدي إلى تحسينات كبيرة في أمان وفعالية سلاسل التوريد. وأشارت الدراسة إلى أن هنا نقص في خطط الاسترداد من الكوارث في العديد من الاتجاهات التكنولوجية الحالية، مما يستدعي تطوير استراتيجيات واضحة للتعافي من الهجمات السيبرانية.

وسعت دراسة (Bécue et al.,2021) بعنوان "Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities" إلى تقييم كيفية توظيف تقنيات الذكاء الاصطناعي في أنظمة التصنيع الذكية، مع التركيز على التطبيقات الدفاعية والهجومية. ودراسة فعالية تقنيات التعلم الآلي والتنقيب عن البيانات في أنظمة الكشف عن التسلل، خاصة في بيئات التكنولوجيا التشغيلية، بالإضافة إلى تحليل التحديات التقنية والتشغيلية والأمنية التي تواجهها المنشآت عند دمج الذكاء الاصطناعي في عملياتها. وتوصلت الدراسة إلى أن تقنيات الذكاء الاصطناعي تُحسِّن من قدرات أنظمة الكشف عن التسلل، مما يُعزِّز من أمان أنظمة التصنيع. وأشارت الدراسة إلى أن المهاجمين السيبرانيين يستخدمون تقنيات الذكاء الاصطناعي لتطوير هجمات أكثر تعقيدًا وفعالية، مما يزيد من صعوبة اكتشافها والتصدي لها.

وتناولت دراسة (De Azambuja et al.,2023) بعنوان "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey"، العلاقة بين الأمن السيبراني والذكاء الاصطناعي، وتوصلت الدراسة

إلى تزايد تأثير الهجمات الإلكترونية على أداء المنشآت في القطاع الصناعي، مستغلةً نقاط ضعف الأجهزة المتصلة بالشبكة. كما أدى تزايد الرقمنة والتقنيات المستخدمة في سياق الصناعة إلى زيادة الاستثمارات في الابتكار والأتمتة. ومع ذلك، هناك مخاطر مرتبطة بهذا التحول الرقمي، لا سيما فيما يتعلق بالأمن السيبراني. وأشارت الدراسة إلى أن استخدام تقنيات مثل الشبكات العصبية التلافيفية (CNN)، والشبكات العصبية المتكررة (RNN)، والشبكات العميقة (DBN) يمكن أن يُحسِّن من قدرات الكشف عن الهجمات السيبرانية والتصدي لها.

بينما استهدفت دراسة (Khalaf & Steiti, 2024) بعنوان" Artificial Intelligence Predictions in Cyber Security: Analysis and Early Detection of Cyber Attacks" التعرف على تنبؤات الذكاء الاصطناعي في تحليل الهجمات السيبرانية والكشف المبكر عنها، مع التركيز على كيفية تمكين الذكاء الاصطناعي من كشف الهجمات السيبرانية من خلال التقييم والتنبؤ مع التركيز على قدرتها على تحديد التهديدات السيبرانية والتخفيف من حدتها بشكل استباقي للحد من آثارها. كما يناقش البحث أيضًا تحديات المهارات والقضايا الأخلاقية المرتبطة بحلول الأمن السيبراني القائمة على الذكاء الاصطناعي. كما تُستخدم خوارزميات الذكاء الاصطناعي لتحليل الهجمات الإلكترونية والكشف المبكر عنها باستخدام لغة برمجة بايثون، وتوصلت النتائج إلى وجود دور هام خوارزميات التعلم الآلي في تعزيز إجراءات الأمن السيبراني، وتصنيف التهديدات الإلكترونية بدقة مع تقليل النتائج الإيجابية والسلبية الخاطئة.

سعت دراسة (Lysenko et al.,2024) بعنوان" The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats" إلي تحليل دور الذكاء الاصطناعي في الأمن السيبراني، واستكشاف كيفية مساهمة تقنيات الذكاء الاصطناعي، مثل التعلم الآلي والتعلم العميق في تحسين قدرات الكشف عن التهديدات والاستجابة لها. بالإضافة إلى دراسة مدى قدرة الأتمتة المدعومة بالذكاء الاصطناعي على تقليل الوقت اللازم لاكتشاف التهديدات والتعامل معها. كما هدفت الدراسة إلى تقييم التحديات والمخاطر المرتبطة باستخدام الذكاء الاصطناعي. وأظهرت نتائج الدراسة أن استخدام تقنيات الذكاء الاصطناعي يُحسّن من قدرة الأنظمة على اكتشاف التهديدات السيبرانية، خاصة تلك التي يصعب اكتشافها بالطرق التقليدية. كما توصلت الدراسة إلي أن الأتمتة المدعومة بالذكاء الاصطناعي ساهمت في تقليل الوقت اللازم للاستجابة للحوادث الأمنية، مما يقلل من الأضرار المحتملة. وخلصت الدراسة إلي أن استخدام الذكاء الاصطناعي أدي إلى تقليل الحاجة للتدخل البشري في عمليات المراقبة والكشف، مما يسمح للفرق الأمنية بالتركيز على المهام الأكثر تعقيدًا.

بينما تناولت دراسة (Sontan & Samuel, 2024) بعنوان" The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities دور الذكاء الاصطناعي في مجال الأمن السيبراني، من خلال تغطيةً المبادئ الأساسية والمنهجيات المتقدمة والاعتبارات الأخلاقية. بالإضافة إلى استكشاف تقنيات الذكاء الاصطناعي الأساسية، مثل التعلم الآلي ومعالجة اللغة الطبيعية. وكذلك التعرف على دور الذكاء الاصطناعي في تعزيز الكشف عن التهديدات، وتحليل نقاط الضعف، والاستجابة للحوادث. وكذلك التعرف على المخاوف الأخلاقية والمتعلقة

بالخصوصية المحيطة بنشر الذكاء الاصطناعي في مجال الأمن السيبراني، مع التأكيد على أهمية اتخاذ القرارات المسؤولة، وحماية الخصوصية، والشفافية. وتوصلت الدراسة إلى أن إستخدام تقنيات الذكاء الاصطناعي يساعد في تسريع تخفيف حدة التهديدات وتعزيز الوضع الأمني العام، وذلك من خلال تسريع أوقات الاستجابة للحوادث، وتقليل الأخطاء البشرية، وقدرات التعلم المستمر، كما توصلت الدراسة إلى أن تقنيات الذكاء الاصطناعي تُمكّن من تطبيق حلول فعّالة للغاية، وتحديد الهجمات الإلكترونية بكفاءة وسرعة، واختيار الاستجابة الأمثل للحوادث الأمنية، وتقييم عواقبها، وتحديد آلية الاستجابة الفورية. وتوصلت الدراسة إلى أن تقنيات الذكاء الاصطناعي المستخدمة في نظام الأمن السيبراني تمكن من إتخاذ القرارات من حيث تحديد التهديدات، والوقاية من المخاطر، وأتمتة الحماية.

كما هدفت دراسة (Weng& Wu, 2024) بعنوان" Leveraging artificial intelligence to enhance data security and combat cyber attacks. إلى التعرف على كيفية الاستفادة من الذكاء الاصطناعي لتعزيز أمن الشبكات والبيانات، مع التركيز على تطبيقاته في الكشف عن التهديدات، وأتمتة الاستجابة، والتحليل التنبؤي وتقديم رؤى ثاقبة حول فعالية الذكاء الاصطناعي في مجال الأمن السيبراني واقتراح استراتيجيات لتطبيقه. وتشير النتائج إلى أن الذكاء الاصطناعي لديه القدرة على تحسين تدابير الأمن السيبراني بشكل كبير، حيث يوفر كشفًا أسرع للتهديدات، وتقييمًا أكثر دقة للمخاطر، وقدرات استجابة مُحسّنة. كما توصلت الدراسة إلي وجود العديد من التحديات التي تواجه تطبيق الذكاء الاصطناعي تمثلت في: جودة البيانات وكميتها، قد تولد أنظمة الذكاء الاصطناعي إنذارات كاذبة، تهديدات المهاجمين للذكاء الاصطناعي، مخاوف الخصوصية، بالإضافة إلى تحديات التنفيذ المتمثلة في البنية التحتية والعمليات الأمنية الحالية.

وتناولت دراسة (Ajayi et al.,2025) بعنوان" The impact of artificial intelligence on cyber security in digital currency transactions. تأثير الذكاء الاصطناعي على الأمن السيبراني في معاملات العملات الرقمية لتقييم فعالية الذكاء الاصطناعي في كشف المعاملات الاحتيالية باستخدام مجموعات بيانات مثل قاعدة بيانات REKT، ومجموعة بيانات معاملات التشفير، وتقارير مكافحة غسل الأموال بتتبع التشفير، ومجموعة بيانات المعاملات المالية IEEE DataPort. وتكشف النتائج أن الذكاء الاصطناعي يُحسّن من كشف الاحتيال وتخفيف المخاطر، كما تشير النتائج إلى ارتباط الاعتماد المتزايد على نماذج كشف الاحتيال المدعومة بالذكاء الاصطناعي بانخفاض كبير في التهديدات السيبرانية، وخلصت نتائج إلى أن تدابير الأمن المدعومة بالذكاء الاصطناعي قللت من الأنشطة الاحتيالية بنسبة تصل إلى ٧٦.٨٦%، مما يؤكد فعاليتها.

٣/٢- التعليق على الدراسات السابقة:

على الرغم من أن الدراسات مثل(Radanliev et al. ,2020 ، Bécue et al. ,2021) قد ركّزت بعمق على الجوانب الفنية لتطبيقات الذكاء الاصطناعي في الأمن السيبراني، إلا أنها لم تتناول بشكل كافٍ مدى إفصاح المنشآت عن استخدام هذه الأنظمة في تقاريرها المالية أو غير المالية، مما يشير إلى فجوة بحثية واضحة في قياس أو تنظيم هذا النوع من الإفصاح. كما اتفق أغلب الباحثين على أن الذكاء الاصطناعي يُعد أداة فعّالة لتعزيز أمن الأنظمة، لكنهم أيضًا حذروا من أن هذه التقنية قد تصبح سلاحًا لحدوث مخاطر الهجمات السيبرانية، بالإضافة إلى أن معظم الدراسات ركّزت على فعالية الذكاء الاصطناعي في رصد الهجمات

وكشف التسلل، لكنها لم تربط بين هذه الاستخدامات وأهداف الحوكمة الرشيدة مثل الشفافية والمساءلة، التي تتحقق من خلال الإفصاح المنظم للمستخدمين الخارجيين (المستثمرين، الجهات الرقابية، أصحاب المصلحة).

ويتضح لدي الباحثين الحاجة إلى تصميم مؤشر إفصاح مقترح يشمل عناصر محددة مثل تقنيات الذكاء الاصطناعي المستخدمة في الحد من مخاطر الهجمات السيبرانية، الأهداف التي تخدمها (الكشف المبكر، الاستجابة للحوادث، تحليل السلوك غير الطبيعي... إلخ)، وأثرها على تقليل الحوادث السيبرانية وتكاليفها. بالإضافة إلى الإفصاح عن المخاطر المرتبطة باستخدامها مثل تحيز الخوارزميات. وبالتالي، فإن اقتراح مؤشر إفصاح عن استخدام نظم الذكاء الاصطناعي في مواجهة الهجمات السيبرانية يمثل مساهمة بحثية أصيلة تعالج فجوة واضحة في الأدبيات.

القسم الثالث: الإطار النظري

مع التوسع السريع في اعتماد نظم الذكاء الاصطناعي داخل المنشآت خلال العقد الماضي، برزت مخاوف متزايدة تتعلق بحقوق الإنسان، وأمن البيانات، والخصوصية، فضلاً عن القضايا الأخلاقية المرتبطة بالاستخدام غير المنضبط لهذه التقنيات. ورغم ذلك، لا تزال المخاوف المرتبطة بالشفافية في استخدام الذكاء الاصطناعي غير معكوسة في معايير الإفصاح عن المعلومات غير المالية أو في التشريعات واللوائح المعمول بها حاليًا. ويُعد الإفصاح الطوعي عن استخدام تقنيات الذكاء الاصطناعي ممارسة حديثة، تتركز بشكل أساسي في القطاعات المالية والتكنولوجية والاتصالات. ويهدف هذا الإفصاح إلى تنظيم المعلومات المتعلقة باستخدام الذكاء الاصطناعي داخل المنشآت، وتعزيز مستوى الشفافية، والحد من المخاطر، وإظهار التزام المنشآت بالمسؤولية في هذا المجال. كما يتضمن إطارًا للإفصاح عن عناصر المعلومات الأساسية، مثل: نموذج حوكمة الذكاء الاصطناعي، والأخلاقيات والمسؤولية، والاستراتيجية، إضافةً إلى متطلبات إفصاح أكثر تفصيلًا للأنظمة الآلية المخصصة لصنع القرار، لا سيما تلك المصنفة ضمن فئات المخاطر المتوسطة إلى العالية (Bonsón & Bednárová, 2022).

١/٣ مفهوم وأهداف إستخدام نظم الذكاء الاصطناعي:

لقد حظي مفهوم الذكاء الاصطناعي بقبول واسع وزاد انتشاره في كافة المجالات، ولا يمكن للمنشآت على مستوى العالم تجاهله، لذا اكتسب الذكاء الاصطناعي زخمًا عالميًا، حيث أن استخدامه يضمن أن القرارات التي سوف تتخذها المنشآت دقيقة وذات جدوى (Bhagat et al., 2022).

وقد أدى التطور المستمر بمجالات تقنية المعلومات والحاسوب لزيادة الاهتمام بالأبحاث والدراسات الخاصة بفهم طبيعة الذكاء الإنساني والقدرات العقلية البشرية، مع محاولة محاكاة ذلك ضمن تصميم برامج حاسوبية لديها القدرة على محاكاة العقل البشرية لاستخدامها في العديد من التطبيقيات، وتسهل أداء العديد من النشاطات البشرية في الحياة المعاصرة، مع تحول هذه البحوث لأنظمة تجريبية واقعية (Iftikhar et al., 2020) .

كما عرف الذكاء الاصطناعي بأنه أحد علوم الحاسب الآلي الحديثة التي تبحث عن أساليب متطورة للقيام بأعمال واستنتاجات متشابهة ولو بحدود، تلك الأسباب التي ينسب لذكاء

الانسان بهدف إعادة البناء من خلال استخدام الوسائل الاصطناعية، والحواسيب، والتفكير والإجراءات الذكية (Dongre et al., 2020) .

ويرى (Iftikhar et al., 2020) أن الذكاء الاصطناعي يتكون من ثلاثة جوانب رئيسية وهي: التعلم والاستدلال والتصحيح الذاتي، والتي تتجمع معاً لاستحضار العقل الاصطناعي، الذي يمكن من خلال أداء العديد من المهام.

كما أن الذكاء الاصطناعي يعد جزء من علوم الحاسب الالي الذي يهدف لمحاكاة قدرة معرفية لاستبدال البشر في أداء العديد من الوظائف المناسبة، ويعتبر الذكاء الاصطناعي العلم الذي يهتم بصنع آلات ذكية تتصرف كما هو متوقع من الانسان أن يتصرف(Al-Sayyed et al.,2021).

وعرف (Hasan, 2021) الذكاء الاصطناعي بأنه سلوك وخصائص معينة تتسم بها البرامج الحاسوبية، تجعلها تحاكي القدرات الذهنية البشرية وانماط عملها ومن اهم هذه الخاصيات القدرة على التعلم والاستنتاج ورد الفعل على اوضاع لم تبرمج في الآلة.

وعرف كل من (AlKoheji & Al-Sartawi, 2022) الذكاء الاصطناعي يعرف محاكاة لذكاء الانسان وفهم طبيعته عن طريق عمل برامج للحاسب الآلي قادرة على محاكاة السلوك الإنساني المتسم بالذكاء.

ويري (Bhagat et al., 2022) أن الذكاء الاصطناعي هو عبارة عن استخدام تقنية التعلم الآلي إلى جانب معالجة تعلم اللغة لصياغة حل لمشكلة ما باستخدام منطق محدد جيدًا يدعم الحل، لذا يعمل الذكاء الاصطناعي على نفس التشبيه الذي يتعامل فيه الإنسان مع الموقف بحكمته وخبرته.
وعرف الذكاء الاصطناعي بأنه تقنية تسهم في إدارة المهام والعمليات بآليات أكثر ذكاء وتطور من الإنسان الذي اخترعها، والتي من ضمنها المعرفة المقومات الحسية، وبما يساعدها على التعلم التلقائي والتطور الذاتي (Jain،2023).

ومن خلال ما سبق يمكن للباحثة تعريف الذكاء الاصطناعي بأنه أحد مجالات تكنولوجيا المعلومات يركز على تطوير الأنظمة والبرامج التي تمكن الآلات من أداء المهام التي تتطلب ذكاءً بشريًا. ويشمل هذا الذكاء القدرة على التعلم من التجارب والتحليلات التنبؤية لأتمتة العمليات المحاسبية، وتحليل البيانات المالية، وتقديم رؤى دقيقة لدعم اتخاذ القرارات المالية، وكذلك التنبؤ بالاتجاهات المالية، وتحليل المخاطر، وتقديم تقارير مالية أكثر شفافية وموثوقية.
وقد أشارت العديد من الدراسات إلى وجود مجموعة من الأهداف الرئيسية والفرعية لاستخدام نظم الذكاء الاصطناعي، وفيما يلي عرض أهداف إستخدام نظم الذكاء الاصطناعي على النحو التالي: (Iftikhar et al., 2020; Bhagat et al., 2022; Hasan, 2021):

١. إنجاز الأعمال بشكل أسرع وأفضل بكثير من أدائها بالطريقة التقليدية الورقية الإمكانية الوصول للبيانات والمعلومات المطلوبة بسهولة.
٢. تمكين صناع القرار من اتخاذ القرارات بطريقة موضوعية عقلانية ورشيدة بعيدا عن التأثير العاطفي فضلًا عن الدور الذي تؤديه انظمة دعم ومساندة القرارات، والسرعة والدقة في الإجراءات الإدارية، الأمر الذي يؤدي إلى القضاء على بيروقراطية العمل الإداري.

٣. الحد من ظاهرة الفساد الإداري، وذلك من خلال تحقيق مبدأ المساواة بين المتعاملين بأسلوب موحد والقضاء على الوساطة والمحسوبية.
٤. التواصل المستمر بين الجهات الإدارية فيما بينها عن طريق تطبيقات معينة، ويتيح ذلك امكانية
٥. الوصول إلى البيانات الضرورية اللازمة عند اتخاذ قرار معين.
٦. القضاء على التراخي الإداري في العمل وعدم الانشغال بالأنشطة غير الضرورية الثانوية وسرعته
٧. رفع كفاءة التخطيط الإداري الاستراتيجي للمنشأة.
٨. يهدف الذكاء الاصطناعي إلى الوصول إلى الأنظمة التي تتمتع بالذكاء والعمل بنفس الطريقة التي يعمل بها البشر من خلال الاعتماد على التعلم والفهم ومن خلال ذلك تقدم لمستخدميها خدمات مختلفة تتميز بالدقة والسرعة في الإنجاز.
٩. يسهم الذكاء الاصطناعي في المحافظة على الخبرات البشرية المتراكمة بنقلها الى الآلات الذكية.

ومن خلال ما سبق يمكن القول إن الذكاء الاصطناعي يساعد على معالجة المشكلات المعقدة وتحليل البيانات الضخمة، والكشف عن الاحتيال المالي التي تقترح باستخدام الذكاء الاصطناعي، والكشف عن المعاملات المشبوهة بسرعة وبدقة.

٢/٣- التحديات التي تواجه استخدام نظم الذكاء الاصطناعي:

على الرغم من المزايا العديدة التي تقدمها نظم الذكاء الاصطناعي، إلا أن هناك بعض التحديات التي قد تنشأ عند استخدامه، ويمكن عرض أهم التحديات التي تواجه استخدام نظم الذكاء الاصطناعي في المجال المحاسبي على النحو التالي: (Lin & Hazelbaker,2019; Dongre et al.,2020; Yi et al.,2023)

١. **فقدان الوظائف البشرية**: قد يؤدي استخدام الذكاء الاصطناعي في المجال المحاسبي إلى تقليل الحاجة إلى المحاسبين التقليديين، حيث يمكن للأتمتة تولي المهام الروتينية مثل تسجيل البيانات، وإعداد التقارير المالية، ومن ثم فقدان الوظائف أو تقليل فرص العمل في مجال المحاسبة للمبتدئين، حيث تصبح العديد من المهام مؤتمتة (Yi et al.,2023) .
٢. **تكاليف التنفيذ الأولية:** تطوير وتنفيذ نظم الذكاء الاصطناعي يتطلب تكاليف مرتفعة في البداية، بما في ذلك شراء البرامج، تدريب الموظفين، وتحديث البنية التحتية التقنية، وهذا يمثل هذا عبئًا كبيرًا على الشركات الصغيرة والمتوسطة التي قد لا تملك الميزانية الكافية لتحمل تكاليف التنفيذ والصيانة (Dongre et al.,2020).
٣. **التعقيد التقني وصعوبة التكيف:** يتطلب الذكاء الاصطناعي فهمًا تقنيًا عاليًا لتنفيذه واستخدامه بشكل فعال، فعدم قدرة المحاسبين على التكيف مع الأنظمة الجديدة قد يسبب صعوبات في التعامل مع الأدوات الجديدة (Hazelbaker,2019) .
٤. **المشاكل المتعلقة بدقة البيانات:** يعتمد الذكاء الاصطناعي على جودة البيانات المدخلة، وإذا كانت البيانات التي يتم إدخالها في النظام غير دقيقة أو غير كاملة، قد ينتج عن ذلك أخطاء كبيرة في التقارير نتيجة التحليلات غير الدقيقة (Dongre et al.,2020).
٥. **مخاطر الأمان والخصوصية:** مع تطور التكنولوجيا وزيادة اعتماد الأنظمة المحاسبية على الذكاء الاصطناعي، تزداد المخاطر المرتبطة بالأمن السيبراني والخصوصية، قد تكون الأنظمة عرضة للاختراق، مما يعرض المعلومات المالية الحساسة للخطر، مما قد

يؤدي ذلك إلى اختراق البيانات المالية الحساسة أو التلاعب بها، مما يتسبب في خسائر كبيرة للشركات (Hazelbaker,2019).

٦. **صعوبة تفسير القرارات:** بعض أنظمة الذكاء الاصطناعي تستخدم الخوارزميات المعقدة (مثل الشبكات العصبية)، مما يجعل من الصعب على المحاسبين أو المدراء فهم كيفية اتخاذ القرارات أو تفسير نتائج التحليل، ومن ثم عدم القدرة على تفسير القرارات المالية وهذا يمكن أن يؤدي إلى قلة الثقة في النظام، خصوصًا إذا كانت هناك حاجة إلى تبرير القرارات أمام الإدارة أو الجهات التنظيمية (Hazelbaker,2019).

٧. **الاعتماد على الأنظمة الجاهزة:** إن الاعتماد على نظم الذكاء الاصطناعي الجاهزة قد يحد من المرونة في تخصيص النظام ليناسب احتياجات الشركة الفريدة، وهذا قد يؤدي هذا إلى تحديات في تنفيذ استراتيجيات مالية مخصصة أو تلبية احتياجات معينة للشركة (Yi et al.,2023).

ومن خلال ما سبق يمكن الإشارة إلى وجود بعض التحديات التي يجب مراعاتها، وتشمل هذه التحديات فقدان الوظائف، التكاليف الأولية العالية، المخاطر الأمنية، الاعتماد المفرط على التكنولوجيا، وصعوبة التكيف مع الأنظمة الجديدة. بالتالي، يجب على الشركات تحقيق توازن بين الاستفادة من نظم الذكاء الاصطناعي ومعالجة هذه التحديات لضمان نجاح التطبيق بشكل مستدام.

٣/٣- ماهية الإفصاح عن استخدام نظم الذكاء الاصطناعي:

لقد جلب التطور السريع للتكنولوجيا على مدى العقد الماضي فوائد كبيرة للشركات من حيث الكفاءة العالية، وتوفير التكاليف، وتوليد الإيرادات، والعمل بجودة أعلى، أو زيادة رضا الموظفين. ومع ذلك، في الوقت نفسه، تثار بعض المخاوف بشأن حقوق الإنسان، وأمن البيانات، والخصوصية أو غيرها من القضايا الأخلاقية، والتي قد تكون على المحك عندما يتم دمج الذكاء الاصطناعي في عمليات صنع القرار. وعلى الرغم من المخاطر المحتملة الكبيرة الناتجة عن إستخدام نظم الذكاء الاصطناعي، لم يتم وضع أي تشريع مؤخرًا للتخفيف من مخاطر استخدام الذكاء الاصطناعي من خلال مطالبة الشركات بالشفافية الكاملة بشأن استخداماته. ومع ذلك، بدأت بعض الشركات بالفعل في الاستجابة لهذا الطلب من خلال الكشف طواعية عن مثل هذه المعلومات في تقريرها غير المالي. مستوحاة جزئيًا من مبادرات المفوضية الأوروبية مثل المبادئ التوجيهية الأخلاقية للذكاء الاصطناعي الموثوق به، والتي نُشرت في عام ٢٠١٩، أو الكتاب الأبيض حول الذكاء الاصطناعي: نهج أوروبي للتميز والثقة، الذي أرسي الأساس للتنظيم الأوروبي للذكاء الاصطناعي، قانون الذكاء الاصطناعي، الذي نُشر في أبريل ٢٠٢١ (European Reporting Lab,2021).

على مدار العقدين الماضيين، كان بإمكاننا أن نشهد كيف بدأت الشركات في جميع أنحاء العالم وطورت الإفصاح غير المالي لاستكمال بياناتها المالية. في البداية، كان هناك نفس ضغط أصحاب المصالح، والذي تطلب من الشركات أن تكون شفافة بشأن أدائها البيئي والاجتماعي والحوكمة بسبب التأثيرات السلبية المحتملة على البيئة والمجتمع ككل. وقد أدى هذا إلى تطوير معايير إعداد التقارير المقبولة عمومًا مثل مبادرة إعداد التقارير العالمية (GRI)، وEMAS، وISO 26000، وSA 80,000، وما إلى ذلك، والتي طورت إرشادات ومؤشرات أداء رئيسية للإفصاح غير المالي. وبعد فترة وجيزة، تم وضع التشريع

في بعض البلدان وأصبح الإفصاح غير المالي إلزاميًا، وخاصة للشركات الكبيرة (European Commission,2021).

وفي ٢١ أبريل ٢٠٢١، اقترحت المفوضية الأوروبية the European Financial Reporting Advisory Group (EFRAG) إطارًا قانونيًا، يعمل كمقترح لتنظيم النهج الأوروبي للذكاء الاصطناعي، جنبًا إلى جنب مع خطة منسقة مع الدول الأعضاء بشأن الذكاء الاصطناعي. والهدف الرئيسي هو تحديد القواعد والإجراءات اللازمة للتميز والثقة في الذكاء الاصطناعي في نطاق أوروبا المناسبة للعصر الرقمي وضمان سلامة وحقوق الأفراد والشركات الأساسية. يتبع الإطار نهجًا قائمًا على المخاطر ويميز بين أربع فئات من أنظمة الذكاء الاصطناعي: (المخاطر غير المقبولة؛ المخاطر العالية؛ المخاطر المحدودة؛ والمخاطر الدنيا. واعتمادًا على مستوى المخاطر، ستكون الشركة ملزمة (أو لا) بمستوى معين من الإفصاح. على سبيل المثال، سيتم حظر أنظمة الذكاء الاصطناعي المصنفة ضمن فئة المخاطر غير المقبولة (التطبيقات وأنظمة الذكاء الاصطناعي التي قد تسبب ضررًا جسديًا/نفسيًا، أو تتلاعب بالسلوك البشري أو تستغل قدرات الضعف البشرية، أو أي تطبيق يسمح بالتسجيل الاجتماعي أو تحديد الهوية عن بعد في الوقت الفعلي في الأماكن العامة) تلقائيًا(Bonsón and Bednárová, 2022).

ويعرف الإفصاح عن استخدام نظم الذكاء الاصطناعي بأنه عملية تقوم من خلالها الشركات والمنشآت بالكشف عن كيفية تبنيها لهذه التقنيات في عملياتها، يتطلب ذلك تقديم معلومات واضحة حول أهداف الذكاء الاصطناعي، وآثاره المحتملة، وكيفية إدارة المخاطر المرتبطة به. الإفصاح يعزز الشفافية ويطمئن أصحاب المصالح بأن الشركات تتبع ممارسات مسؤولة في استخدام الذكاء الاصطناعي(ElNashar,2024).

كما يشير الإفصاح عن استخدام نظم الذكاء الاصطناعي إلى عملية تقديم معلومات شفافة ودقيقة حول كيفية اعتماد المنشأة أو الشركة على تقنيات الذكاء الاصطناعي في عملياتها، بما في ذلك جوانب مثل المحاسبة، اتخاذ القرارات، تحسين الكفاءة التشغيلية، أو تقديم خدمات جديدة. يتضمن الإفصاح شرحًا لكيفية استخدام الذكاء الاصطناعي، والبيانات التي تتم معالجتها، والتأثيرات المحتملة على أصحاب المصالح، إضافة إلى المخاطر والفرص المرتبطة بهذا الاستخدام (Kostygina et al.,2023) .

وتتطلب أنظمة الذكاء الاصطناعي عالية المخاطر إدارة شاملة للمخاطر وضمان جودة البيانات والدقة وإمكانية تتبع النتائج والأمن السيبراني، وستخضع أنظمة الذكاء الاصطناعي ذات المخاطر المحدودة لمتطلبات شفافية أقل (على سبيل المثال، يجب أن يكون المستخدمون على الأقل على دراية بأنهم يتفاعلون مع خوارزمية). من ناحية أخرى، بالنسبة لأنظمة الذكاء الاصطناعي ذات المخاطر الدنيا، لن تكون هناك حاجة إلى الإفصاح (على سبيل المثال، ألعاب الفيديو أو مرشحات البريد العشوائي). ومن أجل الإفصاح عن نظم الذكاء الاصطناعي، يجب أولاً التوصل إلى توافق في الآراء بشأن كيفية الافصاح؛ وما هي العناصر الأساسية وما هي المعلومات التي يجب الافصاح عنها لتلبية احتياجات أصحاب المصالح المختلفين (Walmsley,2021).

٤/٣- مبررات الإفصاح عن استخدام نظم الذكاء الاصطناعي:

يعد الإفصاح عن استخدام نظم الذكاء الاصطناعي من الاستراتيجيات الهامة للشركات في ظل التحول الرقمي السريع، وهناك عدة أسباب رئيسية تدفع الشركات إلى الإفصاح عن تبنيها لهذه التقنيات يمكن عرضها على النحو التالي: (Kostygina et al.,2023 ; ElNashar,2024; Shiyyab et al.,2023)

١. **تعزيز الشفافية والمصداقية:** حيث أن الشركات التي تفصح عن كيفية استخدام الذكاء الاصطناعي تسهم في بناء الثقة مع أصحاب المصالح مثل العملاء والمستثمرين، هذا الإفصاح يوضح أن الشركة تتبع ممارسات شفافة ومسؤولة، مما يعزز مصداقيتها في السوق (Shiyyab et al.,2023) .

٢. **التوافق مع اللوائح والقوانين:** هناك تزايد في القوانين واللوائح تفرض على الشركات الإفصاح عن استخدامات نظم الذكاء الاصطناعي، خاصة إذا كانت تؤثر على حقوق العملاء مثل الخصوصية وحماية البيانات، والامتثال لهذه اللوائح يحمي الشركات من الغرامات والعقوبات القانونية(ElNashar,2024).

٣. **إدارة المخاطر:** يساعد الإفصاح عن استخدام نظم الذكاء الاصطناعي في توضيح كيفية إدارة المخاطر المرتبطة بتطبيق الذكاء الاصطناعي، مثل التحيز في الخوارزميات أو التأثير على الخصوصية. وتفصح الشركات عن هذه المخاطر تقدم صورة أنها تعمل على التحكم في تلك التحديات بطرق مسؤولة Kostygina et al.,2023).

٤. **تعزيز الابتكار وجذب الاستثمارات:** يظهر الإفصاح عن استخدام الذكاء الاصطناعي أن الشركة تستثمر في الابتكار والتكنولوجيا المتقدمة، مما يجذب المستثمرين الذين يبحثون عن شركات تعتمد على التكنولوجيا لتحقيق النمو المستدام Shiyyab et al.,2023).

٥. **تحسين السمعة العامة:** تساعد الشركات التي تفصح عن استخدام نظم الذكاء الاصطناعي بشكل مسؤول في تحسين صورتها العامة، وخاصة في القطاعات التي تتطلب استخدام الذكاء الاصطناعي بمسؤولية، مثل قطاع الاتصالات أو القطاع المالي(ElNashar,2024).

٦. **التفاعل مع أصحاب المصالح:** يمكن للإفصاح عن استخدام الذكاء الاصطناعي أن يكون وسيلة للتواصل مع أصحاب المصالح، وإشراكهم في فهم كيفية تطبيق التكنولوجيا، مما يساعد في بناء علاقات أقوى وأكثر تعاونًا معهم ElNashar,2024).

٧. **الاستجابة لتوقعات المجتمع:** يتوقع المجتمع أن تكون الشركات ذات شفافية عالية حول كيفية استخدام نظم الذكاء الاصطناعي، خاصة فيما يتعلق بالأخلاقيات والعدالة الاجتماعية. فالإفصاح عن نظم الذكاء الاصطناعي يساعد في تلبية هذه التوقعات ويحمي الشركات من النقد الاجتماعي (Kostygina et al.,2023).

ومن خلال ما سبق يمكن للباحثة استنتاج أن الإفصاح عن استخدام الذكاء الاصطناعي يعزز الثقة، ويساعد في إدارة المخاطر، ويلبي التزامات قانونية واجتماعية، كما يساعد في جذب الاستثمارات وتعزيز الابتكار، مما يجعل الإفصاح أداة استراتيجية ضرورية لتحقيق النجاح المستدام.

٣/٥- متطلبات الإفصاح عن استخدام نظم الذكاء الاصطناعي:

عند الإفصاح عن المعلومات المتعلقة بالذكاء الاصطناعي، من المهم أن تصف كل شركة أولاً السياق الذي تُستخدم فيه تكنولوجيا الذكاء الاصطناعي، ولماذا وكيف. ونظرًا لأن الإفصاح عن الذكاء الاصطناعي هو اتجاه جديد إلى حد ما، فهناك نقص في الإرشادات حول ما يجب الإفصاح عنه وكيفية الإفصاح عنه. لذا هناك حاجة ملحة لمعايير إعداد التقارير المتعلقة بالذكاء الاصطناعي المعترف بها دوليًا والمقبولة عمومًا، والتي من شأنها أن تمثل إجماعًا عالميًا وأفضل ممارسة للإفصاح عن تأثيرات استخدام الذكاء الاصطناعي في الشركة. ويهدف إعداد التقارير المتعلقة بالذكاء الاصطناعي بناءً على المعايير إلى ضمان التزام الشركة بالحقوق الأساسية مثل الحريات والخصوصية وحماية البيانات وعدم التمييز مع دمج تكنولوجيا الذكاء الاصطناعي، وبعبارة أخرى، فإنه سيُظهر مسؤوليتها الرقمية. وفي ضوء محاولات المنظمات المهنية في تقديم إطار للإفصاح عن المعلومات المتعلقة بنظم الذكاء الاصطناعي يمكن عرض أهم العناصر الواجب الإفصاح عنها على النحو التالي:

١. **الأهداف والاستخدامات**: ويشمل توضيح الغرض من استخدام نظم الذكاء الاصطناعي في الشركة، ويتضمن هذا الإفصاح تفاصيل حول كيف تسهم هذه الأنظمة في تحقيق أهداف الشركة، وكذلك الإفصاح عن المجالات التي يُستخدم فيها الذكاء الاصطناعي بشكل محدد، مثل التحليل البياني، التنبؤ المالي، أتمتة العمليات، أو التحليلات التنبؤية والحلول التكيفية التي تلبي احتياجات وتفضيلات المستخدمين المتنوعة. حيث أنه من خلال الاستفادة من تقنيات الذكاء الاصطناعي، يمكن تحليل أنماط البيانات المعقدة وأتمتة المهام المتكررة واستخلاص رؤى ذات قيمة لدفع الابتكار والقدرة التنافسية (Bonsón and Bednárová, 2022).
٢. **نموذج الحوكمة ومراقبة النظام:** لكي تكون الشركات ذات شفافية عالية فينبغي عليها توفير بيانات بشأن كيفية إدارة الذكاء الاصطناعي داخل الشركة. ومن ثم، ينبغي توفير المعلومات التالية: ما هو هيكل الحوكمة؛ من هو المسؤول؛ وجود أقسام أو لجان مثل مسؤول حماية البيانات أو لجنة المراقبة؛ معلومات حول المراقبة المستمرة وكذلك أنظمة وعمليات التحقق الخارجية. وكذلك الإفصاح عن بنية حوكمة الذكاء، والإفصاح عن كيفية إدارة الذكاء الاصطناعي داخل الشركة (Bonsón and Bednárová, 2022).
٣. **الاستراتيجية:** يمكن للشركة أيضًا الإفصاح عن أنشطة التدريب الجارية المتعلقة باستخدام الذكاء الاصطناعي المشاريع التي تركز على تحقيق أهداف التنمية المستدامة، يمكن أيضًا الكشف عن العلاقات مع أصحاب المصالح، ويجب إيلاء أكبر قدر من الاهتمام لتقييم المخاطر، وبعض التطبيقات مثل التعرف على الوجه أكثر، ويجب إجراء تقييم مناسب للمخاطر ووصفها، وأنشطة التدريب (الداخلية والخارجية) حول استخدام الذكاء الاصطناعي، والاستراتيجية لضمان الشفافية وإمكانية المراجعة والتفسير وإمكانية الوصول وسهولة الاستخدام والثقة (Bonsón, et al., 2021).

٤. **المخاوف التنظيمية والأخلاقية**: إن الشركات التي تستخدم تقنيات الذكاء الاصطناعي (AI) ملتزمة بجميع اللوائح والمبادئ التوجيهية الأخلاقية ذات الصلة التي تحكم استخدام الذكاء الاصطناعي، وإدراك أهمية حماية الخصوصية وحماية البيانات والتخفيف من التحيزات في خوارزميات الذكاء الاصطناعي لدعم حقوق الأفراد، لذا يجب علي الشركات الإفصاح عن مدى الامتثال للقوانين المحلية والدولية المتعلقة باستخدام الذكاء الاصطناعي، مثل قوانين حماية البيانات أو المتطلبات الأخلاقية ويجب أن توضح الشركة كيف تتأكد من أن تقنيات الذكاء الاصطناعي متوافقة مع هذه اللوائح (Kar et al., 2022) .

٥. **المخاطر وإدارتها**: في حين يقدم الذكاء الاصطناعي العديد من الفرص، فإنه ينطوي أيضًا على العديد من المخاطر، تشمل هذه المخاطر التحيزات المحتملة في جمع البيانات والمخرجات الخوارزمية، وانتهاكات الخصوصية، وثغرات الأمان، والعواقب غير المقصودة لاتخاذ القرارات الآلية. بالإضافة إلى ذلك، قد يفرض الاعتماد على أنظمة الذكاء الاصطناعي تحديات تتعلق بالمساءلة والشفافية والقدرة على التفسير، مما يؤدي إلى معضلات أخلاقية ومخاوف مجتمعية. وتشمل وكيفية معالجة المخاطر من خلال أدوات تصحيح الأخطاء وتقنيات الاختبار الدورية، ويشرح كيفية إدارة المخاطر المرتبطة باستخدام الذكاء الاصطناعي (Kar et al., 2022).

٦. **تقييم المخاطر:** بعد إجراء تقييم المخاطر، يجب تصنيف تطبيقات الذكاء الاصطناعي بناءً على مستوى المخاطر. بهذه الطريقة، تتطلب التطبيقات ذات مستوى المخاطر الأعلى إفصاحًا أكثر تفصيلاً حول كيفية جمع البيانات وتخزينها وإدارتها؛ وكيف تعمل الخوارزمية؛ والمخاطر المحتملة والتحيزات وخطط التخفيف Bonsón, et al., (2021).

٧. **الفوائد:** على الرغم من وجود العديد من المخاطر، فإن فوائد تبني الذكاء الاصطناعي كبيرة وبعيدة المدى، حيث يسهل الذكاء الاصطناعي توفير التكاليف وتحقيق الكفاءة التشغيلية والابتكار المتسارع من خلال تبسيط العمليات وتحسين تخصيص الموارد. علاوة على ذلك، تعمل الرؤى التي يقودها الذكاء الاصطناعي على تمكين الشركات من اتخاذ قرارات وتخفيف المخاطر واغتنام الفرص في البيئات الديناميكية. علاوة على ذلك، يعزز الذكاء الاصطناعي تجارب المستخدم وإمكانية الوصول من خلال التوصيات المخصصة والأتمتة الذكية (Bonsón, et al., 2021).

ومن خلال ما سبق يمكن القول إنه على الرغم من الفرص والفوائد المترتبة على تطبيق الذكاء الاصطناعي، لا يزال الإفصاح عن الذكاء الاصطناعي طوعيًا. ويُترك قرار الافصاح عن المعلومات، وإلى أي مدى، ونوع المعلومات لتقدير الشركات. كما إن الافتقار إلى رؤية مشتركة ومعايير إعداد تقارير للذكاء الاصطناعي يؤدي إلى ممارسات إفصاح مختلفة اعتمادًا على تصورات الشركات.

٦/٣- النظريات الداعمة للإفصاح عن الذكاء الاصطناعي:

يوجد العديد من النظريات المحاسبية التي يمكن أن تدعم الإفصاح عن إستخدام نظم الذكاء الاصطناعي ويمكن للباحثة عرضها على النحو التالي:

- **نظرية أصحاب المصالح: (Stakeholder Theory)**

تُعتبر نظرية أصحاب المصالح إطارًا لفهم كيفية تأثير الشركات على مختلف أصحاب المصالح الذين يتأثرون بأنشطتها مثل المستثمرين، العملاء، الموظفين، المجتمع، والحكومات، وهي تمتد لتشمل الإفصاح عن استخدامات الذكاء الاصطناعي. في سياق هذا الإفصاح، تتعامل الشركات مع أصحاب المصالح المتنوعين مثل المستثمرين، العملاء، الموظفين، المجتمع، والحكومات. وفي ضوء نظرية أصحاب المصالح يجب أن يكون أصحاب المصالح على دراية بكيفية استخدام نظم الذكاء الاصطناعي والآثار المرتبطة بها، بما في ذلك الأمور المتعلقة بالأمان والخصوصية، حيث أن الإفصاح عن استخدام نظم الذكاء الاصطناعي يساعد في تهدئة مخاوف أصحاب المصالح بشأن التحيز، الأتمتة، أو انتهاك حقوق الإنسان Sandström (&Spodenkiewicz,2023) . ونظرًا لأن أصحاب المصالح لديهم اهتمامات متباينة، يجب أن تركز الشركات على الإفصاح عن تأثير الذكاء الاصطناعي من عدة جوانب: التأثير الاقتصادي (الأرباح أو الخسائر)، التأثير الاجتماعي (الخصوصية والأمان)، والتأثير البيئي (استدامة استخدام البيانات) مما يعزز من ثقة أصحاب المصالح. على سبيل المثال، العملاء بحاجة لفهم كيف يتم استخدام بياناتهم بواسطة نظم الذكاء الاصطناعي، والمستثمرون يريدون معرفة الأثر المالي المتوقع من هذه التقنية (Smaili et al., 2022). ومن ثم يمكن للباحثة القول إن نظرية أصحاب المصالح تعد أحد الأدوات لدعم الحاجة إلى الإفصاح عن الذكاء الاصطناعي لتعزيز الشفافية والمساءلة تجاه جميع الفئات المتأثرة بتطبيقاته.

- **نظرية الإشارة (Signaling Theory)**

تركز نظرية الإشارة على كيفية إرسال الشركات إشارات للمستثمرين وأصحاب المصالح لتقديم معلومات حول جودة أدائها أو استراتيجياتها، في إطار الإفصاح عن الذكاء الاصطناعي، وتعتمد الشركات على الإشارة لنقل معلومات هامة تتعلق بتبني نظم الذكاء الاصطناعي وتأثيرات استخداماتها، بهدف تعزيز ثقة أصحاب المصالح، حيث أنه من خلال الإفصاح عن تبني الذكاء الاصطناعي، ترسل الشركات إشارة إلى السوق بأنها متقدمة تكنولوجيًا وتتبنى الابتكار، وهذا يعزز من سمعتها بين المستثمرين والعملاء، ويعتبر مؤشرًا على مستقبل الشركة الواعد في تحقيق التحول الرقمي. كما أن الإفصاح عن استخدام الذكاء الاصطناعي يساعد في توضيح الغموض حول طبيعة العمليات التقنية الجديدة وكيفية تطبيقها (Sandström &Spodenkiewicz,2023). كما أن الإفصاح عن استخدام نظم الذكاء الاصطناعي يرسل إشارة بأنها ملتزمة بالمسؤولية الاجتماعية والحوكمة الرشيدة، هذا يساعد في تحسين العلاقة مع أصحاب المصالح مثل العملاء والحكومات الذين قد يكون لديهم مخاوف بشأن التأثيرات الاجتماعية لاستخدام هذه التقنية. ومن خلال ما سبق يمكن للباحثة القول إن نظرية الإشارة تعد أداة قوية لتوضيح كيفية استخدام الذكاء الاصطناعي، والتأكيد على التزام الشركات بالابتكار والممارسات الأخلاقية، مما يساعد على بناء الثقة وجذب الاستثمارات (Bonsón et al., 2023).

- **نظرية الشرعية(Legitimacy Theory) :**

تفسر نظرية الشرعية كيفية سعي الشركات للحصول على قبول اجتماعي من خلال التصرف بطريقة تتماشى مع توقعات المجتمع وأصحاب المصالح. وفي إطار الإفصاح عن الذكاء الاصطناعي، تُستخدم نظرية الشرعية لتفسير الأسباب التي تدفع الشركات للإفصاح عن كيفية استخدام تقنيات الذكاء الاصطناعي، بهدف الحفاظ على شرعيتها في نظر المجتمع. وتستخدم الشركات الإفصاح عن الذكاء الاصطناعي كوسيلة للتماشي مع القيم والمعايير الاجتماعية، مثل حماية الخصوصية، الأمان، وعدم التحيز. كما أن الإفصاح عن كيفية استخدام هذه التكنولوجيا يساهم في الحفاظ على الشرعية من خلال التوضيح بأنها تتبنى ممارسات مسؤولة وأخلاقية. ويمكن أن يكون ذلك حاسمًا، خصوصًا في القطاعات التي تواجه فيها الشركات تحديات قانونية أو اجتماعية تتعلق بالذكاء الاصطناعي (مثل حماية البيانات، التوظيف، الأتمتة). كما يعد الإفصاح عن استخدام نظم الذكاء الاصطناعي جزءًا من استراتيجية الشركات للحفاظ على شرعيتها من خلال إظهار التزامها بالامتثال للقوانين والمعايير عندما تواجه الشركات ضغوطًا من الجهات التنظيمية أو الحكومات لتنظيم استخدام الذكاء الاصطناعي (Bonsón et al., 2021). ومن خلال ما سبق يمكن للباحثة القول ان نظرية الشرعية تفسر كيف يُعد الإفصاح عن استخدام نظم الذكاء الاصطناعي أداة للشركات للحفاظ على قبول المجتمع وتجنب فقدان شرعيتها من خلال الإفصاح عن مدي التزامها بالقيم الاجتماعية وتوقعات أصحاب المصالح مما يعزز من استدامتها وشرعيتها.

- **نظرية الوكالة (Agency Theory):**

تركز نظرية الوكالة على العلاقة بين الملاك والوكلاء، حيث يوكِّل الملاك الإدارة لاتخاذ القرارات نيابة عنهم. في إطار الإفصاح عن الذكاء الاصطناعي، يمكن تفسير الإفصاح عن استخدام الذكاء الاصطناعي من منظور نظرية الوكالة على أنه وسيلة لتقليل التباين في المعلومات بين الإدارة والمساهمين، وتعزيز الثقة والشفافية في استخدام التقنيات المتقدمة. حيث يساعد الإفصاح عن استخدام نظم الذكاء الاصطناعي في تقليل هذا التباين عن طريق تقديم معلومات واضحة حول كيفية استخدام التقنية في تحسين العمليات، تقليل التكاليف، أو زيادة الإيرادات (Sandström &Spodenkiewicz,2023). كما يمكن أن يحد من تضارب المصالح بين الإدارة والمساهمين، حيث أنه عندما تقوم الإدارة باستخدام تقنيات متقدمة مثل الذكاء الاصطناعي لتعزيز الأداء المالي للشركة، فإن تقديم تقارير شفافة حول هذه العمليات يساعد في تعزيز ثقة المساهمين بأن الإدارة تستخدم موارد الشركة بطريقة مسؤولة ومربحة ويقلل من الشكوك حول كيفية استغلال الإدارة للموارد ويزيد من شفافية العمليات (Ben-Amar& McIlkenny,2015). ومن خلال ما سبق يمكن للباحثة القول إن نظرية الوكالة تبرز أهمية الإفصاح عن استخدام نظم الذكاء الاصطناعي كوسيلة للتغلب على تحديات عدم تماثل المعلومات وتضارب المصالح بين الإدارة والمساهمين. ومن ثم تعزيز الشفافية، المساءلة، والثقة بين الأطراف المختلفة، مما يؤدي إلى تحسين العلاقة بين الملاك والإدارة ويدعم استدامة الشركة.

٧/٣- أثر الافصاح عن إستخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية:

أصبح العملاء في حاجة متزايدة إلى الاطمئنان بشأن أمن بياناتهم وسلامة تعاملاتهم الرقمية، لا سيما في ظل الانتشار المتسارع للهجمات السيبرانية التي تستهدف المنشآت في قطاعات حيوية مثل الاتصالات والخدمات المالية. وفي هذا السياق، يُعد الإفصاح عن استخدام الشركات لنظم الذكاء الاصطناعي في حماية بنيتها الرقمية خطوة محورية تعزز ثقة العملاء والمستثمرين على حدٍ سواء. لحاجتهم إلى معلومات عن مدى جاهزية المنشأة في مواجهة المخاطر السيبرانية، بل يكشف أيضًا عن التزامها بأعلى معايير الحوكمة الرقمية. كما أن الإفصاح عن هذه التقنيات يساهم في رفع مستوى الوعي المجتمعي بأهمية الذكاء الاصطناعي كأداة دفاعية، ويوفر للمستخدمين والجهات الرقابية معلومات ضرورية لتقييم كفاءة وفعالية السياسات الأمنية المطبقة، وهو ما يؤدي في النهاية إلى خلق بيئة رقمية أكثر أمانًا واستقرارًا. وهناك العديد من المعلومات التي يجب الإفصاح عنها فيما يتعلق بالحماية من الهجمات السيبرانية تتمثل فيما يلي:

- **الاستعداد للتهديد:** في ظل تصاعد وتيرة الهجمات السيبرانية وتزايد تعقيدها، أصبح الاستعداد المسبق للتعامل مع التهديدات الرقمية ضرورة حتمية وليس مجرد خيار. ويُقصد بالاستعداد للتهديد تبني المؤسسات لنهج استباقي يشمل بناء بنية تحتية رقمية مرنة، وتطبيق سياسات أمن معلومات فعالة، إلى جانب الاستثمار في التكنولوجيا المتقدمة، وعلى رأسها نظم الذكاء الاصطناعي. حيث تلعب هذه النظم دورًا محوريًا في رصد السلوكيات الشاذة، وتحليل البيانات الضخمة للتعرف على التهديدات قبل وقوعها، وتقديم إنذارات مبكرة تساعد على اتخاذ قرارات سريعة وحاسمة. ويشمل الاستعداد للتهديد أيضًا رفع الوعي الأمني لدى العاملين، وتدريب الفرق التقنية على سيناريوهات الهجوم، وتحديث الأدوات الدفاعية بشكل دوري. ويساعد الإفصاح الواضح عن البنية التحتية السيبرانية المدعومة بالذكاء الاصطناعي في إظهار مدى جاهزية المنشأة للتعامل مع التهديدات. فعندما تُفصح الشركة عن اعتمادها على أنظمة تحليل تنبؤية وخوارزميات ذكاء اصطناعي، فإنها توضح التزامها بالتحول الرقمي الآمن، مما يعكس قدرتها على التصدي المبكر للهجمات المحتملة، وتكوين صورة واضحة للجهات الرقابية والمستثمرين عن جاهزيتها الأمنية (Khalaf & Steiti, 2024) .
- **كشف التهديدات :**أدى التطور المتسارع في تقنيات الذكاء الاصطناعي إلى إحداث تحول جذري في آليات كشف التهديدات السيبرانية، حيث باتت المؤسسات تعتمد على أدوات ذكية قادرة على تحليل كميات هائلة من البيانات في الوقت الفعلي، واكتشاف الأنماط غير الطبيعية التي قد تشير إلى وجود نشاط ضار. وتستخدم هذه الأنظمة تقنيات مثل التعلم الآلي (Machine Learning) والتعلم العميق (Deep Learning) في تدريب النماذج على التمييز بين السلوك العادي والمشبوه، ما يسمح بالتنبؤ بالهجمات قبل وقوعها أو في مراحلها الأولى، مثل محاولات التصيد الاحتيالي، وتسريبات البيانات، وهجمات البرامج الخبيثة. ومن أبرز مزايا استخدام الذكاء الاصطناعي في هذا المجال هو تقليل الاعتماد على المراقبة اليدوية، وتسريع عملية الكشف والاستجابة، وتعزيز قدرة المؤسسات على التعامل مع التهديدات

المعقدة والمتطورة باستمرار. وتُسهم أنظمة الذكاء الاصطناعي في رفع كفاءة عمليات كشف التهديدات الإلكترونية عبر مراقبة البيانات الضخمة وتحليل الأنماط السلوكية في الوقت الحقيقي. وعندما تُفصح المؤسسات عن هذه القدرات، فإنها تُظهر امتلاكها لأدوات تقنية متقدمة تستطيع اكتشاف التهديدات غير المعروفة وتقليل الاعتماد على الوسائل التقليدية في الكشف، ما يعزز استباقية المنشأة في منع الاختراقات (Weng& Wu, 2024).

- **وقت الاستجابة :**يمكن لأنظمة الكشف والاستجابة المستندة إلى الذكاء الاصطناعي أن تساعد المنشأة على تحسين قدراتها في الكشف عن التهديدات والاستجابة لها للهجمات المتقدمة. كما أنها تساعد في الاستجابة لاستخراج البيانات، والهجمات المستهدفة المتقدمة، والبرامج الضارة، والهندسة الاجتماعية، والهجمات المشفرة. وتُعد سرعة الاستجابة أحد العوامل الجوهرية في الحد من الأضرار الناتجة عن الهجمات السيبرانية. ويمكن للأنظمة الذكية المؤتمتة أن تتخذ إجراءات فورية لحظر التهديد أو عزله. ومن خلال الإفصاح عن هذه الإمكانيات، ترسل المنشأة رسالة واضحة عن قدرتها على احتواء الهجمات خلال لحظات حاسمة، مما يرفع مستوى ثقة العملاء ويقلل من التكاليف المحتملة المرتبطة بالتعطل أو التسريب (Lysenko et al.,2024).
- **تقييم الأنظمة بعد الاستجابة:** يُعد تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية خطوة حاسمة في دورة الحماية الرقمية، إذ يمكّن المؤسسة من تحليل فعالية الإجراءات التي تم اتخاذها، وتحديد الثغرات التي استُغلت، ومدى كفاءة نظم الذكاء الاصطناعي في اكتشاف الهجوم واحتوائه. ويُعزز الإفصاح عن هذه المراجعات الدورية مصداقية المؤسسة، حيث يُظهر التزامها المستمر بالتحسين والتطوير، ويُتيح للجهات الرقابية تقييم مدى التعلّم المؤسسي من التجارب السابقة. كما أن الإفصاح عن نتائج التقييم يُسهم في تعزيز الشفافية، ويشجع على تبادل المعرفة وأفضل الممارسات بين الشركات، مما يؤدي إلى بناء بيئة سيبرانية أكثر مرونة واستعدادًا للمخاطر المستقبلية(Sontan & Samuel, 2024).

ومن خلال ما سبق يمكن القول إن استمرار إستخدام نظم الذكاء الاصطناعي في جوانب عالمنا الرقمي، سيزيد من خطر الهجمات الإلكترونية بشكل كبير. وأن الإفصاح عن استخدام نظم الذكاء الاصطناعي في التصدي للهجمات السيبرانية لا يقتصر على كونه إجراءً إعلاميًا، بل يمثل أحد مكونات الحوكمة الرشيدة للأمن السيبراني، ويُسهم بشكل فعّال في تقليل المخاطر، وتعزيز جاهزية المؤسسات في بيئة رقمية معقدة ومليئة بالتحديات.

القسم الرابع: الدراسة التطبيقية

يتناول هذا القسم الدراسة التطبيقية للتعرف على أثر الإفصاح عن استخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية، وذلك من خلال اختبار فروض الدراسة بالتطبيق على جميع شركات الاتصالات، كما يتناول هذا القسم الهدف من الدراسة التطبيقية وأهميتها، ثم يتناول المنهجية البحثية للدراسة المستخدمة لقياس المتغيرات واشتقاق الفروض، ويتناول هذا القسم أيضاً عرضاً للطريقة البحثية المناسبة لجمع وتحليل البيانات؛ بهدف قياس أثر الإفصاح عن استخدام نظم

الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية ، ولتحقيق أهداف الدراسة التطبيقية، يقدم هذا القسم وصفاً لمجتمع الدراسة ووصفاً لطريقة وأسباب اختيار عينة الدراسة، وكذلك مصادر الحصول على البيانات، ثم يقدم القسم اشتقاق نموذج الدراسة والأساليب الإحصائية لاختبار الفروض وتفسير نتائج الدراسة التطبيقية.

١/٤ـ الهدف من الدراسة التطبيقية:

تهدف الدراسة التطبيقية الحالية إلى قياس أثر الإفصاح عن استخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية من خلال قياس أثر كلاً من (الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ـ الإفصاح عن كشف التهديدات للهجمات السيبرانية ـ الإفصاح عن وقت الاستجابة للهجمات السيبرانية ـ الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية)، من خلال التحليل الاحصائي لبيانات عينة الدراسة التي تم جمعها، حيث يتم جمع البيانات من شركات الاتصالات في البيئة الصرية، ثم اجراء مجموعة من الاختبارات الاحصائية بهدف الوصول إلي نتائج الدراسة.

٢/٤ـ قياس متغيرات الدراسة:

تشمل هذه الدراسة على متغير مستقل ومتغير تابع يتم قياسهم كما يلي:

- **المتغير المستقل: الإفصاح عن إستخدام نظم الذكاء الاصطناعي:** وتم قياس هذا المتغير من خلال مؤشر للإفصاح بالاعتماد على الدراسات السابقة، ويمكن إيضاح بنود المؤشر على النحو التالي:

جدول رقم (١) قياس الإفصاح عن إستخدام نظم الذكاء الاصطناعي

مؤشر مقترح للإفصاح عن استخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية	
أولاً:	**١. الاستعداد للتهديد**
١	تُفصح الشركة عن تبنّي استراتيجيات ذكاء اصطناعي ضمن سياساتها الأمنية.
٢	يتم الإفصاح عن خطط استباقية للتعامل مع تهديدات مستقبلية باستخدام نظم الذكاء الاصطناعي
٣	تُوضح الشركة مكونات البنية التحتية المرتبطة بالحماية الذكية.
٤	يتم تقديم مؤشرات حول تدريب الموظفين على استخدام تقنيات الذكاء الاصطناعي في الأمن السيبراني.
٥	تُدرج الشركة مدى تكامل الذكاء الاصطناعي ضمن استراتيجيتها العامة لإدارة المخاطر.
ثانيا:	**٢. كشف التهديدات**
٦	تُفصح الشركة عن استخدام خوارزميات تعلم آلي في مراقبة الشبكات والأنظمة.
٧	يتم الإعلان عن دور نظم الذكاء الاصطناعي في كشف التهديدات غير المعروفة.
٨	توضح التقارير استخدام الذكاء الاصطناعي في اكتشاف محاولات التصيّد الاحتيالي والهجمات الاحتيالية.
٩	تُبين الشركة اعتمادها على أدوات تحليل سلوك المستخدم (UEBA) القائمة على

	الذكاء الاصطناعي.
١٠	تُفصح الشركة عن مستوى دقة أنظمة الكشف الذكية ومدى تحديثها الدوري.
ثالثاً:	**٣. وقت الاستجابة**
١١	تُدرج الشركة متوسط زمن الاستجابة للتهديدات خلال الفترة المالية.
١٢	يتم الإفصاح عن استخدام أدوات استجابة مؤتمتة في الوقت الفعلي.
١٣	تُظهر الشركة مدى قدرتها على احتواء التهديدات فور اكتشافها باستخدام نظم الذكاء الاصطناعي
١٤	تُفصح الشركة عن آليات التواصل والتنسيق الداخلي والخارجي عند وقوع هجوم.
١٥	تُوضح مدى اعتماد سيناريوهات الاستجابة على التحليلات الذكية للتهديدات.
رابعاً:	**٤. تقييم الأنظمة بعد الاستجابة**
١٦	تُفصح الشركة عن آلية تقييم أداء نظم الذكاء الاصطناعي بعد الحوادث.
١٧	يتم تقديم تقارير مراجعة دورية توضح نقاط القوة والضعف في النظام.
١٨	يتم الإفصاح عن التوصيات الفنية الناتجة عن التقييم ومدى تنفيذها.
١٩	تُدرج مؤشرات التحسين المستمر الناتجة عن تحليل الأداء بعد الهجوم.
٢٠	تُفصح الشركة عن تبنيها نماذج ذكاء اصطناعي قابلة للتعلم من الأخطاء السابقة.

من إعداد الباحثين بالاعتماد على (Khalaf & Steiti, 2024؛ Weng& Wu, 2024؛ Lysenko et al.,2024)

- **المتغير التابع:** والمتمثل في مخاطر الهجمات السيبرانية، ويتم قياسه من خلال الإعتماد على مؤشر الإفصاح لدراسة (موسي،٢٠٢٥) على النحو التالي:

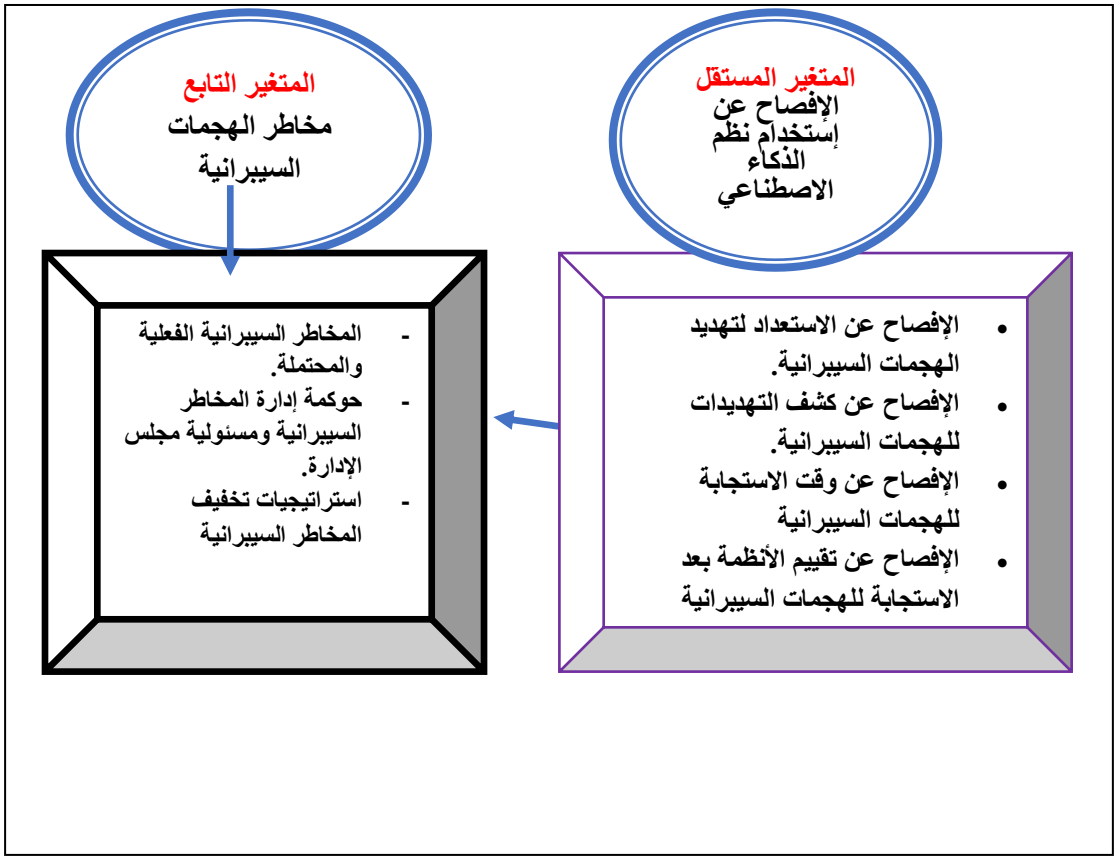
جدول رقم (٢) قياس مخاطر الهجمات السيبرانية

مخاطر الهجمات السيبرانية	
أولاً:	المخاطر السيبرانية الفعلية والمحتملة
١	وصف طبيعة الحوادث والهجمات السيبرانية المحتمل التعرض لها مستقبلا
٢	الغرض من الهجمات السيبرانية (التجسس- تعطيل العمليات- التشويش- السرقة والإبتزاز)
٣	مصدر الهجمات والحوادث السيبرانية المحتملة
٤	مخاطر البنية التحتية للمعلومات والخدمات السحابية للعملاء
٥	مخاطر إساءة إستخدام الممتلكات الفكرية أو الأصول الأخر ى (الأجهزة والبرامج والتطبيقات)
٦	مخاطر الاستعانة ببرامج مفتوحة المصدر
٧	مدي تعرض المنشأة لمخاطر الطرف الثالث، والتغيرات التي حدثت في ذلك التعرض
٨	مدي تعرض المنشأة لمخاطر وسائل التواصل الاجتماعي
٩	مخاطر سرية وخصوصية البيانات المخزنة في الفضاء السيبراني
١٠	الإفصاح عن الضوابط والإجراءات الرقابية المرتبطة بالمخاطر السيبرانية
ثانياً:	حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة
١١	هيكل حوكمة إدارة المخاطر السيبرانية
١٢	الإطار العام لإدارة المخاطر السيبرانية والإفصاح والتقرير عنها

١٣	المسؤوليات المذكورة في إستراتيجية الأمن السيبراني للمنشأة، والتغيرات التي طرأت عليها
١٤	مسئولية لجنة المراجعة في التقرير والإفصاح عن المخاطر الأمنية وقضايا الأمن السيبراني
١٥	التقرير عن مساهمة الإدارة في تصميم وتقييم نظام إدارة مخاطر أمن المعلومات
١٦	مسئولية لجنة إدارة المخاطر بشأن المخاطر السيبرانية
١٧	الإفصاح عن وصف مشاركة المجلس في الإشراف على المخاطر والفرص المتعلقة بالأمن السيبراني
١٨	الإفصاح عن وصف الأمن السيبراني و/ أو مخاطر أمن المعلومات.
١٩	وجود فريق متخصص في إدارة أمن المعلومات والرقابة الأمنية على العمليات الإلكترونية للمنشأة
٢٠	الالتزام بالتشريعات والقوانين واللوائح الصادرة عن الجهات المختصة المتعلقة بالأمن السيبراني
ثالثاً	**استراتيجيات تخفيف المخاطر السيبرانية**
٢١	الإفصاح عن الجهود المبذولة في التعليم والتدريب (الإدارة، والموظفين)، للتخفيف من المخاطر السيبرانية
٢٢	تكاليف الاستثمار في التكنولوجيا والأدوات الرقمية، والعوائد المتوقعة نتيجة تطبيقها
٢٣	الإفصاح عن المعلومات المتعلقة بقياس جهود الأمن السيبراني الجارية
٢٤	مدى إمكانية الإعتماد على الخبراء (طرف ثالث) في مجال الأمن السيبراني
٢٥	مدى توافر معلومات توضح ممارسات المنشأة لحماية وتخزين واسترجاع البيانات إلكترونيا
٢٦	التقرير عن إجراءات الاستجابة للحوادث في نظم المعلومات (خطة الطوارئ/ اختبارات الاختراق)
٢٧	عدد الرسائل والتعليمات الإرشادية لتوعية العملاء بالمخاطر السيبرانية عبر موقع المنشأة
٢٨	عدد الشهادات التي حصلت عليها المنشأة في الأمن السيبراني/ حوكمة تكنولوجيا المعلومات
٢٩	الأطر العالمية التي تتبناها المنشأة لحوكمة تكنولوجيا المعلومات
٣٠	الافصاح عن عدد الدورات التدريبية المنعقدة داخل وخارج المنشأة

المصدر: (موسي،٢٠٢٥)

ويمكن تصوير نموذج الدراسة بالشكل التالي:



شكل (١) علاقات متغيرات الدراسة

٣/٤ وصف مجتمع وعينة الدراسة:

يتمثل مجتمع الدراسة التطبيقية الحالية في قطاع الاتصالات في البيئة المصرية، وتمثلت عينة الدراسة تمثلت في شركات الاتصالات، التي تتوافر فيها البيانات الخاصة بالدراسة التطبيقية، وتم جمع البيانات منها لفترة الدراسة والتي تغطي خمسة سنوات (٢٠١٩-٢٠٢٣) لجمع مجموعة من البيانات التي تقيس متغيرات الدراسة، ويمكن جمع البيانات المناسبة وتحليلها ثم عرض وتفسير النتائج.

٤/٤ فروض الدراسة:

تسعى الدراسة إلى اختبار الفروض التالية:

- ✓ **الفرض الأول:** يوجد أثر ذو دلالة معنوية للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية.
- ✓ **الفرض الثاني:** يوجد أثر ذو دلالة معنوية الإفصاح عن كشف التهديدات للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية.
- ✓ **الفرض الثالث:** يوجد أثر ذو دلالة معنوية الإفصاح عن وقت الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية.

✓ **الفرض الرابع:** يوجد أثر ذو دلالة معنوية الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية.

٥/٤ أساليب التحليل الاحصائي:

تم الاعتماد على مجموعة من الأساليب الإحصائية لتحليل البيانات خلال البرنامج الإحصائي SPSS، ومن أهم هذه الأساليب **الإحصاء الوصفي** عن الخصائص الإحصائية للمتغيرات والاتجاه العام للبيانات والمتوسط الحسابي والانحراف المعياري، وكذلك اختبار **الارتباط** لقياس العلاقة بين متغيرات الدراسة المختلفة. اختبار **الانحدار** لقياس أثر المتغير المستقل على التابع، ولقد تم إعداد ورقة عمل Excel لجمع عدد من البيانات الواجب جمعها من التقارير المالية المنشورة لعينة الدراسة، وتم إعداد هذه الورقة لتكون صالحة للتحليل الاحصائي، حتى يتم نقلها إلى برنامج التحليل الاحصائي SPSS، وبعد ذلك يتم اجراء التحليل وتفسير النتائج.

➢ **اختبار صلاحية البيانات للتحليل الإحصائي:**

تم استخدام اختبار (Kolmogorov – Smirnov) واختبار (Shapiro–Wilk) للتأكد من أن نمط التوزيع الذي تسلكه بيانات الدراسة هو توزيع طبيعي وذلك بالنسبة لمتغيرات الدراسة، ويوضح الجدول التالي قيم الاختبارات ومستوى المعنوية لكل متغير أمام كل اختبار:

جدول رقم (٣) التوزيع الطبيعي لمتغيرات الدراسة

المتغيرات	Kolmogorov-Smirnov		Shapiro-Wilk Statistic	
	Value	Sig.	Value	Sig.
الاستعداد للتهديد	.250	.002	.849	.005
كشف التهديدات	.205	.028	.726	.032
وقت الاستجابة	.187	.064	.926	.128
تقييم الأنظمة بعد الاستجابة	.249	.002	.618	.029
المخاطر السيبرانية الفعلية والمحتملة	.148	.200	.513	.047
حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة	.150	. 020	.737	. 021
استراتيجيات تخفيف المخاطر السيبرانية	.217	.014	.607	.047

المصدر: نتائج التحليل الاحصائي.

ويتضح من الجدول السابق أن البيانات تتبع التوزيع الطبيعي لأبعاد المتغير المستقل للدراسة والتي تتمثل في (استخدام نظم الذكاء الاصطناعي) حيث بلغت قيمة المعنوية (٠٠,) وهي أقل من (٠٥,) وكذلك المتغير التابعة والتي تتمثل في مخاطر الهجمات السيبرانية بلغت قيمة المعنوية على التوالي (٠١,) و (٠٠,) وهي أقل من (٠٥,). وبناءً على ذلك فإن البيانات الخاصة بمتغيرات الدراسة تتبع التوزيع الطبيعي.

➢ **التحليل الوصفي لمتغيرات الدراسة:**

يظهر الجدول التالي نتائج توصيف متغيرات الدراسة وذلك على مدار سنوات الدراسة وعلى مستوى كل المشاهدات وذلك كما يلي:

جدول رقم (٤) الإحصاءات الوصفية

الشركة		الاستعداد للتهديد	كشف التهديدات	وقت الاستجابة	تقييم الأنظمة بعد الاستجابة	المخاطر السيبرانية الفعلية والمحتملة	حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة	استراتيجيات تخفيف المخاطر السيبرانية
فودافون	Minimum	4.000	2.000	2.000	2.000	3.000	4.000	3.000
	Maximum	5.000	4.000	4.000	4.000	8.000	9.000	7.000
	Mean	4.600	2.800	3.000	2.800	6.200	5.400	5.800
	Std. Deviation	0.548	0.837	0.707	0.837	2.049	2.191	1.643
	Variance	0.300	0.700	0.500	0.700	4.200	4.800	2.700
أورنج	Minimum	3.000	0.000	2.000	2.000	3.000	3.000	4.000
	Maximum	5.000	4.000	5.000	4.000	7.000	7.000	7.000
	Mean	4.000	2.600	3.600	3.200	5.600	5.600	5.600
	Std. Deviation	1.000	1.517	1.517	0.837	1.673	1.673	1.140
	Variance	1.000	2.300	2.300	0.700	2.800	2.800	1.300
اتصالات	Minimum	1.000	2.000	1.000	0.000	4.000	5.000	4.000
	Maximum	5.000	3.000	4.000	5.000	6.000	9.000	8.000
	Mean	3.200	2.400	2.800	2.600	4.800	6.800	6.000
	Std. Deviation	1.643	0.548	1.304	2.074	0.837	1.483	2.000
	Variance	2.700	0.300	1.700	4.300	0.700	2.200	4.000
WE	Minimum	2.000	1.000	2.000	1.000	5.000	5.000	4.000
	Maximum	5.000	5.000	4.000	4.000	8.000	9.000	7.000
	Mean	3.600	3.000	3.000	2.800	7.000	6.600	5.600
	Std. Deviation	1.140	1.581	0.707	1.095	1.414	1.517	1.517
	Variance	1.300	2.500	0.500	1.200	2.000	2.300	2.300
Total	Minimum	1.000	0.000	1.000	0.000	3.000	3.000	3.000
	Maximum	5.000	5.000	5.000	5.000	8.000	9.000	8.000
	Mean	3.850	2.700	3.100	2.850	5.900	6.100	5.750
	Std. Deviation	1.182	1.129	1.071	1.226	1.651	1.714	1.482
	Variance	1.397	1.274	1.147	1.503	2.726	2.937	2.197

ويلاحظ من الجدول السابق، أن الشركات الاربعة في الدراسة هناك تحسن ملحوظ في مستوى الاستعداد للتهديد لعينة الدراسة خلال سنوات الدراسة (2019-2023) حيث بلغ المتوسط الحسابي (3.850) بانحراف معياري (1.182) وبمعامل اختلاف بلغ (1.397)، كما بلغ مستوى كشف التهديدات لعينة الدراسة خلال سنوات الدراسة (2019-2023) حيث بلغ المتوسط الحسابي (2.700) بانحراف معياري (1.129) وبمعامل اختلاف بلغ (1.274) كما بلغ وقت الاستجابة لعينة الدراسة خلال سنوات الدراسة (2019-2023) حيث بلغ المتوسط الحسابي (3.100) بانحراف معياري (1.071) وبمعامل اختلاف بلغ (1.147) كما بلغ م تقييم الأنظمة بعد الاستجابة لعينة الدراسة خلال سنوات الدراسة

(2019-2023) حيث بلغ المتوسط الحسابي (2.850) بانحراف معياري (1.226) وبمعامل اختلاف بلغ (1.503) كما بلغ المخاطر السيبرانية الفعلية والمحتملة لعينة الدراسة خلال سنوات الدراسة (2019-2023) حيث بلغ المتوسط الحسابي (5.900) بانحراف معياري (1.651) وبمعامل اختلاف بلغ (2.726) كما بلغ حوكمة إدارة المخاطر السيبرانية ومسئولية مجلس الإدارة لعينة الدراسة خلال سنوات الدراسة (2019-2023) حيث بلغ المتوسط الحسابي (6.100) بانحراف معياري (1.714) وبمعامل اختلاف بلغ (2.937) كما بلغ استراتيجيات تخفيف المخاطر السيبرانية لعينة الدراسة خلال سنوات الدراسة (2019-2023) حيث بلغ المتوسط الحسابي (5.750) بانحراف معياري (1.482) وبمعامل اختلاف بلغ (2.197)

٦/٤ تحليل نتائج اختبار فروض الدراسة:

- **اختبار أثر الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية:**

ينص الفرض الأول للدراسة يوجد أثر ذو دلالة معنوية للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية ، وقام الباحثون بإجراء اختبار الارتباط والانحدار للمتغيرات المتمثلة في الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية و مخاطر الهجمات السيبرانية وبالاعتماد على نتائج تحليل الانحدار الخطى البسيط وتحليل الارتباط، وكانت النتائج كما يلي:

جدول رقم (٥)

الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية و مخاطر الهجمات السيبرانية

Model	R	R Square	Adjusted R Square	Sig.
1	٠.632	٠.399	0.398	0.000

أظهرت نتائج الدراسة في جدول رقم (٥) إلى أن قيمة R بلغ 0.632 ووجود علاقة ارتباط بين الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية و مخاطر الهجمات السيبرانية بمعدل63.2%، مما يعني وجود علاقة طردية بين الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية و مخاطر الهجمات السيبرانية ، وكذلك يوجد تأثير للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية على مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته0.399 والذي يعكس أن المتغير المستقل (الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية) يفسر بنسبة (39.9%) من التغيرات في المتغير التابع (مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥%

كما تم إجراء تحليل التباين ANOVA وتحليل الانحدار الخطى البسيط، ويوضح الجدول رقم (٦) نتائج الاختبار على النحو التالي:

جدول رقم (٦)

- تحليل التباين ANOVA وتحليل الانحدار الخطى البسيط

Model	Unstandardized Coefficients		Standardized Coefficients	Sig.	T
	B	Std. Error	Beta		
(Constant)	2.169	.135		.000	16.120
الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية	٠.504	.034	0.632	.000	14.879

ويبين الجدول رقم (٦) أن المتغير المستقل له تأثير ذو دلالة معنوية على المتغير التابع " مخاطر الهجمات السيبرانية " حيث ان المعنوية ٠٠٠, وهي أقل من٠.٠٥، وقيمة معامل الانحدار للمتغير المستقل ٠.٥٠٤, وهي قيمة المتغير التابع عند ثبات باقي المتغيرات، بناء على ما سبق تكون معادلة الانحدار على النحو الآتي:

- **Y = 2.169+0.504 B1 + e**

ومن ثم يمكن قبول الفرض الذي ينص على أنه يوجد أثر ذو دلالة معنوية للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية.

- **اختبار أثر الإفصاح عن كشف التهديدات للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية:**

ينص الفرض الأول للدراسة يوجد أثر ذو دلالة معنوية للإفصاح عن كشف التهديدات للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية ، وقام الباحثون بإجراء اختبار الارتباط والانحدار للمتغيرات المتمثلة في الإفصاح عن كشف التهديدات للهجمات السيبرانية و مخاطر الهجمات السيبرانية وبالاعتماد على نتائج تحليل الانحدار الخطى البسيط وتحليل الارتباط، وكانت النتائج كما يلي:

جدول رقم (٧)

الإفصاح عن كشف التهديدات للهجمات السيبرانية و مخاطر الهجمات السيبرانية

Model	R	R Square	Adjusted R Square	Sig.
1	0.777	0.604	0.602	0.000

أظهرت نتائج الدراسة في جدول رقم (٧) إلى أن قيمة R بلغت0.777, ووجود علاقة ارتباط بين الإفصاح عن كشف التهديدات للهجمات السيبرانية و مخاطر الهجمات السيبرانية بمعدل77.7%، مما يعني وجود علاقة طردية بين الإفصاح عن كشف التهديدات للهجمات السيبرانية و مخاطر الهجمات السيبرانية ، وكذلك يوجد تأثير للإفصاح عن كشف التهديدات للهجمات السيبرانية على مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته 0.604 والذي يعكس أن المتغير المستقل (الإفصاح عن كشف التهديدات للهجمات

السيبرانية) يفسر بنسبة (60.4%) من التغيرات في المتغير التابع (مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥% .

كما تم إجراء تحليل التباين ANOVA وتحليل الانحدار الخطى البسيط، ويوضح الجدول رقم (٨) نتائج الاختبار على النحو التالي:

جدول رقم (٨)

- تحليل التباين ANOVA وتحليل الانحدار الخطى البسيط

Model	Unstandardized Coefficients		Standardized Coefficients	Sig.	T
	B	Std. Error	Beta		
(Constant)	٠.896	٠.145		٠.000	6.166
الإفصاح عن كشف التهديدات للهجمات السيبرانية	٠.773	٠.034	٠.777	٠.000	22.521

ويبين الجدول رقم (٨) أن المتغير المستقل له تأثير ذو دلالة معنوية على المتغير التابع " مخاطر الهجمات السيبرانية " حيث ان المعنوية ,000 وهي أقل من٠.٠٥، وقيمة معامل الانحدار للمتغير المستقل ٠.773 وهي قيمة المتغير التابع عند ثبات باقي المتغيرات، بناء على ما سبق تكون معادلة الانحدار على النحو الآتي:

- **Y = ٠.896+ ٠.773B1 + e**

ومن ثم يمكن قبول الفرض الذي ينص على أنه يوجد أثر ذو دلالة معنوية للإفصاح عن كشف التهديدات للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية.

- **اختبار أثر الإفصاح عن وقت الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية:**

ينص الفرض الأول للدراسة يوجد أثر ذو دلالة معنوية للإفصاح عن وقت الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية ، وقام الباحثون بإجراء اختبار الارتباط والانحدار للمتغيرات المتمثلة في الإفصاح عن وقت الاستجابة للهجمات السيبرانية ومخاطر الهجمات السيبرانية وبالاعتماد على نتائج تحليل الانحدار الخطى البسيط وتحليل الارتباط، وكانت النتائج كما يلي:

جدول رقم (٩)

الإفصاح عن وقت الاستجابة للهجمات السيبرانية ومخاطر الهجمات السيبرانية

Model	R	R Square	Adjusted R Square	Sig.
1	0.730	0.532	0.531	0.000

أظهرت نتائج الدراسة في جدول رقم (٩) إلى أن قيمة R بلغت 0.730 ووجود علاقة ارتباط بين الإفصاح عن وقت الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية بمعدل ٠.73%، مما يعني وجود علاقة طردية بين الإفصاح عن وقت الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية ، وكذلك يوجد تأثير للإفصاح عن وقت الاستجابة للهجمات السيبرانية على مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته 0.532والذي يعكس أن المتغير المستقل (الإفصاح عن وقت الاستجابة للهجمات

السيبرانية) يفسر بنسبة (53.2 %) من التغيرات في المتغير التابع (مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥%

كما تم إجراء تحليل التباين ANOVA وتحليل الانحدار الخطى البسيط، ويوضح الجدول رقم (١٠) نتائج الاختبار على النحو التالي:

جدول رقم (١٠)

- تحليل التباين ANOVA وتحليل الانحدار الخطى البسيط

Model	Unstandardized Coefficients		Standardized Coefficients	Sig.	T
	B	Std. Error	Beta		
(Constant)	٠-.071	٠.217		٠.000	-0.327
الإفصاح عن وقت الاستجابة للهجمات السيبرانية	٠.984	٠.051	٠.730	٠.000	19.464

ويبين الجدول رقم (١٠) أن المتغير المستقل له تأثير ذو دلالة معنوية على المتغير التابع " مخاطر الهجمات السيبرانية " حيث ان المعنوية 000, وهي أقل من٠.٠٥، وقيمة معامل الانحدار للمتغير المستقل 0.984, وهي قيمة المتغير التابع عند ثبات باقي المتغيرات، بناء على ما سبق تكون معادلة الانحدار على النحو الآتي:

- **Y = -0.071+ 0.984B1 + e**

ومن ثم يمكن قبول الفرض الذي ينص على أنه يوجد أثر ذو دلالة معنوية للإفصاح عن وقت الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية.

- **اختبار أثر الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية:**

ينص الفرض الأول للدراسة يوجد أثر ذو دلالة معنوية للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية، وقام الباحثون بإجراء اختبار الارتباط والانحدار للمتغيرات المتمثلة في الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية وبالاعتماد على نتائج تحليل الانحدار الخطى البسيط وتحليل الارتباط، وكانت النتائج كما يلي:

جدول رقم (١١)

الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية

Model	R	R Square	Adjusted R Square	Sig.
1	0.646	0.417	0.415	0.000

أظهرت نتائج الدراسة في جدول رقم (١١) إلى أن قيمة R بلغت 0.646 ووجود علاقة ارتباط بين الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية بمعدل 64.6%، مما يعني وجود علاقة طردية بين الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية ، وكذلك يوجد تأثير

للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية على مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته0.417 والذي يعكس أن المتغير المستقل (الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية) يفسر بنسبة (41.7%) من التغيرات في المتغير التابع (مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥%
كما تم إجراء تحليل التباين ANOVA وتحليل الانحدار الخطى البسيط، ويوضح الجدول رقم (١٢) نتائج الاختبار على النحو التالي:

جدول رقم (١٢)

- تحليل التباين ANOVA وتحليل الانحدار الخطى البسيط

Model	Unstandardized Coefficients		Standardized Coefficients	Sig.	T
	B	Std. Error	Beta		
(Constant)	1.415	٠.178		٠.000	7.957
الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية	٠.667	٠.043	٠.646	٠.000	15.435

ويبين الجدول رقم (١٢) أن المتغير المستقل له تأثير ذو دلالة معنوية على المتغير التابع " مخاطر الهجمات السيبرانية " حيث ان المعنوية 000, وهي أقل من٠.٠٥، وقيمة معامل الانحدار للمتغير المستقل ٠.667وهي قيمة المتغير التابع عند ثبات باقي المتغيرات، بناء على ما سبق تكون معادلة الانحدار على النحو الآتي:

- **Y = 1.415+ .667 B1 + e**

ومن ثم يمكن قبول الفرض الذي ينص على أنه يوجد أثر ذو دلالة معنوية للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية.

تحليل الانحدار المتعدد للمتغيرات المستقلة:

يتمثل الفرض الرئيسي للدراسة في" يوجد أثر ذو دلالة معنوية للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية، للإفصاح عن كشف التهديدات للهجمات السيبرانية، للإفصاح عن وقت الاستجابة للهجمات السيبرانية، للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية فى الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية، وقام الباحثون بإجراء اختبار الانحدار المتعدد وكانت النتائج كما يلي:

جدول رقم (١٣)

إختبار الانحدار المتعدد

Model	R	R Square	Adjusted R Square	Sig.
1	0.819	0.671	0.667	0.000

- وقد أظهرت نتائج الدراسة في جدول رقم (١٣) إلى أن قيمة R بلغت 0.819 ووجود علاقة ارتباط بين الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، الإفصاح عن كشف التهديدات للهجمات السيبرانية ، الإفصاح عن وقت الاستجابة للهجمات السيبرانية ،الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية والحد من مخاطر الهجمات السيبرانية بمعدل 81.9%، مما يعني وجود علاقة طردية بين الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، الإفصاح عن كشف التهديدات للهجمات السيبرانية ، الإفصاح عن وقت الاستجابة للهجمات السيبرانية ،الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية والحد من مخاطر الهجمات السيبرانية،

وكذلك يوجد تأثير للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، للإفصاح عن كشف التهديدات للهجمات السيبرانية ، للإفصاح عن وقت الاستجابة للهجمات السيبرانية ،للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية فى الحد من مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته 0.671 والذي يعكس أن المتغيرات المستقلة (الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، الإفصاح عن كشف التهديدات للهجمات السيبرانية ، الإفصاح عن وقت الاستجابة للهجمات السيبرانية ،الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية)يفسر بنسبة (67.1%) من التغيرات في المتغير التابع (الحد من مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥%.

- كما تم إجراء تحليل التباين ANOVA وتحليل الانحدار الخطى، ويوضح الجدول رقم (١٤) نتائج الاختبار على النحو التالي

جدول رقم (١٤)

- نتائج اختبار الانحدار المتعدد

Model	Unstandardized Coefficients		Sig.	T
	B	Std. Error		
(Constant)	٠.031	٠.185	٠.866	٠.169
الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية	٠.134	٠.047	٠.005	2.854
الإفصاح عن كشف التهديدات للهجمات السيبرانية	٠.617	٠.064	٠.000	9.680
الإفصاح عن وقت الاستجابة للهجمات السيبرانية	٠.604	٠.075	٠.000	8.029
الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية	٠.389	٠.079	٠.000	4.923

ويبين الجدول رقم (١٤) أن المتغير المستقل له تأثير ذو دلالة معنوية على المتغير التابع " الحد من مخاطر الهجمات السيبرانية " حيث ان المعنوية ٠.٠٠٠ وهي أقل من٠.٠٥، بناء على ما سبق تكون معادلة الانحدار على النحو الآتي:

- **Y = 0.٠31+ 0.134 B1 + 0.617 B2+ 0.604B3 + 0.389 B4 + e**

القسم الرابع: نتائج وتوصيات الدراسة:

١/٥ نتائج الدراسة:

يمكن استخلاص العديد من النتائج المتعلقة بأثر الإفصاح عن استخدام نظم الذكاء الاصطناعي في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية كما يلي:

- أظهرت النتائج أن الإفصاح عن استخدام تقنيات الذكاء الاصطناعي يساهم في زيادة ثقة المستثمرين والعملاء في شركات الاتصالات، حيث أن وجود تقارير دورية تُظهر كيفية استخدام التقنيات الذكية (مثل أنظمة التعلّم الآلي لرصد التهديدات) يعكس مستوىً عاليًا من الحوكمة الرقمية.
- أوضحت نتائج الدراسات أن الشركات التي تفصح بوضوح عن اعتمادها على نظم الذكاء الاصطناعي في تقاريرها السنوية أو تقارير الاستدامة كانت أقل تعرضًا لهجمات سيبرانية. كما أن الإفصاح عن استخدام نظم الذكاء الاصطناعي لا يُستخدم فقط كأداة لتحقيق الشفافية، بل كوسيلة ردع للجهات المهاجمة (إظهار جاهزية النظام الدفاعي).

- أظهرت النتائج أن مستوى الإفصاح الحالي عن استخدام نظم الذكاء الاصطناعي لدى شركات الاتصالات لا يزال في مراحله الأولية، ويتسم بالعمومية الشديدة ويأتي غالباً ضمن تقارير الحوكمة أو الاستدامة تحت بنود مثل "التحول الرقمي" أو "الاستثمار في التكنولوجيا المتقدمة"، دون تقديم تفاصيل فنية أو تشغيلية حول طبيعة هذه النظم.
- توصلت النتائج إلى عدم وجود إطار أو معيار موحد تتبعه الشركات للإفصاح عن استخدام نظم الذكاء الاصطناعي، مما أدى إلى تفاوت كبير في مستوى المعلومات المقدمة بين شركة وأخرى، هذا التباين يجعل من الصعب على المستثمرين والجهات الرقابية والمحللين المقارنة بين الشركات.
- توصلت نتائج الدراسة الميدانية إلى **"وجود أثر للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية "، حيث** أن قيمة R بلغ٠.٦٣٢٠. ووجود علاقة ارتباط بين الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية و مخاطر الهجمات السيبرانية بمعدل٦٣.٢%، مما يعني وجود علاقة طردية بين الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية و مخاطر الهجمات السيبرانية ، وكذلك يوجد تأثير للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية على مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته٠.٣٩٩ والذي يعكس أن المتغير المستقل (الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية) يفسر بنسبة (٣٩.٩%) من التغيرات في المتغير التابع (مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥%
- توصلت نتائج الدراسة الميدانية إلى **"وجود أثر للإفصاح عن كشف التهديدات للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية** "حيث أن قيمة R بلغت٠.٧٧٧, ووجود علاقة ارتباط بين الإفصاح عن كشف التهديدات للهجمات السيبرانية و مخاطر الهجمات السيبرانية بمعدل٧٧.٧%، مما يعني وجود علاقة طردية بين الإفصاح عن كشف التهديدات للهجمات السيبرانية و مخاطر الهجمات السيبرانية ، وكذلك يوجد تأثير للإفصاح عن كشف التهديدات للهجمات السيبرانية على مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته ٠.٦٠٤ والذي يعكس أن المتغير المستقل (الإفصاح عن كشف التهديدات للهجمات السيبرانية) يفسر بنسبة (٦٠.٤%) من التغيرات في المتغير التابع (مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥%
- توصلت نتائج الدراسة الميدانية إلى **"وجود أثر للإفصاح عن وقت الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية** "حيث قد أظهرت نتائج الدراسة إلى أن قيمة R بلغت٠.٧٣٠ ووجود علاقة ارتباط بين الإفصاح عن وقت الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية بمعدل ٧٣.٠%، مما يعني وجود علاقة طردية بين الإفصاح عن وقت الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية ، وكذلك يوجد تأثير للإفصاح عن وقت الاستجابة للهجمات السيبرانية على مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته٠.٥٣٢ والذي يعكس أن المتغير المستقل (الإفصاح عن وقت الاستجابة للهجمات السيبرانية) يفسر بنسبة (٥٣.٢%) من التغيرات في المتغير التابع (مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥%.

- توصلت نتائج الدراسة الميدانية إلى **"وجود أثر للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية في الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية "** حيث أن قيمة R بلغت٠.٦٤٦ ووجود علاقة ارتباط بين الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية بمعدل ٦٤.٦%، مما يعني وجود علاقة طردية بين الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية و مخاطر الهجمات السيبرانية ، وكذلك يوجد تأثير للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية على مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته٠.٤١٧ والذي يعكس أن المتغير المستقل (الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية) يفسر بنسبة (٤١.٧%) من التغيرات في المتغير التابع (مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥% .
- أظهرت نتائج الدراسة الميدانية " **وجود أثر للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، للإفصاح عن كشف التهديدات للهجمات السيبرانية ، للإفصاح عن وقت الاستجابة للهجمات السيبرانية ،للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية فى الحد من مخاطر الهجمات السيبرانية بشركات الاتصالات في البيئة المصرية** " حيث أن قيمة R بلغت 0.819 ووجود علاقة ارتباط بين الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، الإفصاح عن كشف التهديدات للهجمات السيبرانية ، الإفصاح عن وقت الاستجابة للهجمات السيبرانية ،الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية والحد من مخاطر الهجمات السيبرانية بمعدل 81.9%، مما يعني وجود علاقة طردية بين الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، الإفصاح عن كشف التهديدات للهجمات السيبرانية ، الإفصاح عن وقت الاستجابة للهجمات السيبرانية ،الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية والحد من مخاطر الهجمات السيبرانية، وكذلك يوجد تأثير للإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، للإفصاح عن كشف التهديدات للهجمات السيبرانية ، للإفصاح عن وقت الاستجابة للهجمات السيبرانية ،للإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية فى الحد من مخاطر الهجمات السيبرانية حيث أن معامل التحديد بلغ قيمته 0.671 والذي يعكس أن المتغيرات المستقلة (الإفصاح عن الاستعداد لتهديد الهجمات السيبرانية ، الإفصاح عن كشف التهديدات للهجمات السيبرانية ، الإفصاح عن وقت الاستجابة للهجمات السيبرانية ،الإفصاح عن تقييم الأنظمة بعد الاستجابة للهجمات السيبرانية) يفسر بنسبة (67.1%) من التغيرات في المتغير التابع (الحد من مخاطر الهجمات السيبرانية)، وذلك عند مستوي دلالة ٥%.

٢/٥ توصيات الدراسة:

يمكن للباحثين عرض أهم التوصيات في ضوء النتائج السابق ذكرها على النحو التالي:

١. تطوير إطار إفصاح لشركات الاتصالات، بالتعاون مع الجهاز القومي لتنظيم الاتصالات(NTRA) ، للإفصاح عن استخدام نظم الذكاء الاصطناعي والكشف عن التهديدات غير المعروفة" أو "نظام استجابة آلي للحوادث البسيطة."

٢. يجب أن يكون الإفصاح عن استخدام نظم الذكاء الاصطناعي جزءاً لا يتجزأ من تقرير الحوكمة، مع توضيح كيف تشرف الإدارة العليا ومجلس الإدارة على هذه النظم وكيف يتم تقييم فعاليتها.

٣. قيام شركات الاتصالات بإدراج بنود واضحة ومحددة حول تقنيات الذكاء الاصطناعي المستخدمة في الأمن السيبراني ضمن تقاريرها المالية أو تقارير الاستدامة.

٤. ضرورة تدريب العاملين على كيفية التعامل مع أنظمة الذكاء الاصطناعي الدفاعية، وتحليل تنبيهاتها، بما يرفع من كفاءة الاستجابة المبكرة للهجمات.

٥. إدراج الإفصاح عن استخدام الذكاء الاصطناعي كجزء أساسي من خطة إدارة المخاطر في الشركات، بما يعزز من اتخاذ قرارات استباقية لمواجهة التهديدات.

٦. إطلاق حملات توعية وتثقيفية تظهر للمستخدمين كيف تساهم تقنيات الذكاء الاصطناعي في حماية خصوصيتهم وأمنهم الرقمي.

المراجع

أولاً: المراجع العربية:

بانقا، علم الدين. (٢٠١٩). مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي، سلسلة دراسات تنموية، المعهد العربي للتخطيط بالكويت، العدد ٦٣.

تقرير إستراتيجية مصر ٢٠٣٠ في الاتصالات وتكنولوجيا المعلومات، https://mcit.gov.eg/ar/Digital_Egypt.

لبيب، عمر خالد محمد. الخولي، هالة عبد الله؛ فراج، ثناء عطية. (٢٠٢١). العلاقة بين الإفصاح الاختياري عن أبعاد استدامة منشآت الأعمال المدرجة بالبورصة المصرية وتكلفة رأس المال، مجلة الدراسات التجارية المعاصرة، كلية التجارة، جامعة كفر الشيخ، العدد ١١، مجلد ٧، الجزء الثالث.

موسى، عمرو عادل عبد الفتاح. (٢٠٢٥). قياس أثر الإفصاح عن المخاطر السيبرانية على تكلفة رأس المال وانعكاسات ذلك على قيمة المنشأة: دراسة تطبيقية. رسالة دكتوراة غير منشورة، كلية التجارة، جامعة مدينة السادات.

ثانيا: المراجع الأجنبية:

Ajayi, A. J., Joseph, S., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The impact of artificial intelligence on cyber security in digital currency transactions. Available at SSRN 5137847.

Al-Sayyed, S., Al-Aroud, S., & Zayed, L. (2021). The effect of artificial intelligence technologies on audit evidence. Accounting, 7(2), pp. 281-288.

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), 3849-3886.

Ben-Amar, W., & McIlkenny, P. (2015). Board Effectiveness and the Voluntary Disclosure of Climate Change Information, Business Strategy and the Environment, 24(8), pp. 704–719, Available through: LUSEM Library website http://www.lusem.lu.se/library.

Bhagat, P. R., Naz, F., & Magda, R. (2022). Artificial intelligence solutions enabling sustainable agriculture: A bibliometric analysis. PloS one, 17(6), e0268989.

Bonsón, E., & Bednárová, M. (2022). Artificial Intelligence Disclosures in Sustainability Reports: Towards an Artificial Intelligence Reporting Framework. In Digital Transformation in Industry: Digital Twins and New Business Models .(pp. 391-407). Cham: Springer International Publishing.

Bonsón, E., Alejo, V., & Lavorato, D. (2021(A)). Artificial intelligence disclosure in the annual reports of Spanish IBEX-35 companies (2018–2019). In Digital Transformation in Industry: Trends, Management, Strategies (147-155). Cham: Springer International Publishing.

Bonsón, E., Bednárová, M., & Perea, D. (2023). Disclosures about algorithmic decision making in the corporate reports of Western European companies, International Journal of Accounting Information Systems, vol. 48. Available through: LUSEM Library website http://www.lusem.lu.se/library.

Bonsón, E., Lavorato, D., Lamboglia, R., & Mancini, D. (2021(B)). Artificial intelligence activities and ethical approaches in leading listed companies in the European Union. International Journal of Accounting Information Systems, 43, 100535.

De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. Electronics, 12(8), 1920.

Dongre, N., Pandey, A., & Gupta, O. P. (2020). Artificial Intelligence in accounting: opportunities & challenges. J. Xi'an Univ. Archit. Technol, 12, 1858-1864.

ElNashar, T. A. (2024). Artificial Intelligence Firms' Voluntary Disclosure for Estimated Nonrevenue Warranties: A Perspective for an Effective Probability Approach to Reliability and Risk Avoidance. Available at SSRN 4871962.

European Reporting Lab @ EFRAG. (2021). Proposals for a relevant and dynamic EU sustainability reporting standard-setting.

Hasan, A. R. (2021). Artificial Intelligence (AI) in accounting & auditing: A Literature review. Open Journal of Business and Management, 10(1), 440-465.

Iftikhar, P., Kuijpers, M. V., Khayyat, A., Iftikhar, A., & De Sa, M. D. (2020). Artificial intelligence: a new paradigm in obstetrics and gynecology research and clinical practice. Cureus, 12(2).

Jain, R. (2023). The Impact of Artificial Intelligence on Business: Opportunities and Challenges. Available at SSRN 4407114.

Khalaf, M. A., & Steiti, A. (2024). Artificial intelligence predictions in cyber security: Analysis and early detection of cyber-attacks. Babylonian Journal of Machine Learning, 2024, 63-68.

Kostygina, G., Kim, Y., Seeskin, Z., LeClere, F., & Emery, S. (2023). Disclosure Standards for Social Media and Generative Artificial

Intelligence Research: Toward Transparency and Replicability. Social media+ society, 9(4), 20563051231216947.

Lin, P., & Hazelbaker, T. (2019). Meeting the challenge of artificial intelligence: what CPAs need to know. The CPA Journal, 89(6), 48-52.

Lysenko, S., Bobro, N., Korsunova, K., Vasylchyshyn, O., & Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. Economic Affairs, 69, 43-51.

Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., ... & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. Cybersecurity, 3, 1-21.

Sandström, N., & Spodenkiewicz, S.(2023). Board Effectiveness and Artificial Intelligence Disclosure. Master's Thesis, School of Economic and Management, Lund University.

Shiyyab, F. S., Alzoubi, A. B., Obidat, Q. M., & Alshurafat, H. (2023). The impact of artificial intelligence disclosure on financial performance. International Journal of Financial Studies, 11(3), 115.

Smaili, N., Radu, C., & Khalili, A. (2022). Board effectiveness and cybersecurity disclosure, Journal of Management and Governance, pp. 1–23, Available through: LUSEM Library website http://www.lusem.lu.se/library.

Sontan, A. D., & Samuel, S. V. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(2), 1720-1736.

Stancheva-Todorova, E. P. (2018). How artificial intelligence is challenging accounting profession. Journal of International Scientific Publications" Economy & Business, 12, 126-141.

Walmsley, J. (2021). Artificial intelligence and the value of transparency. AI & society, 36(2), 585-595.

Weaver, K. D. (2024). The Artificial Intelligence Disclosure (AID) Framework: An Introduction. arXiv preprint arXiv:2408.01904.

Weng, Y., & Wu, J. (2024). Leveraging artificial intelligence to enhance data security and combat cyber-attacks. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 5(1), 392-399.

Yi, Z., Cao, X., Chen, Z., & Li, S. (2023). Artificial intelligence in accounting and finance: Challenges and opportunities. IEEE Access, 11, 129100-129123.

AlKoheji, A., & Al-Sartawi, A. (2022, May). Artificial intelligence and its impact on accounting systems. In European, Asian, Middle Eastern, North African Conference on Management & Information Systems (pp. 647-655). Cham: Springer International Publishing.