

التكليف الخامس

مجتمع الدراسة ونوع العينة والأسلوب الاحصائي في بحثين مختلفين

اسم المادة : مهارات بحثية ٢
الدكتورة : أميره جادوا
اسم الباحث : خالد العتيبي



أ. دراسة الموارد البشرية

(الدراسة على العاملين في المستشفيات العامة بولاية الخرطوم، وهو ما يتض ٢٠٢٢) اعتمدت ح من قول الباحث: "ما هو أثر تطبيق وظائف إدارة الموارد البشرية علي أداء العاملين في المستشفيات العامة بولاية الخرطوم.

"يمثل هذا المجتمع الفئة المستهدفة لقياس أثر تطبيق وظائف إدارة الموارد البشرية على الأداء.

ب. دراسة الذكاء الاصطناعي (٢٠٢٥)

لا تتضمن الدراسة مجتمعًا بشريًا فعليًا، لأنها دراسة نظرية تحليلية تعتمد على مراجعة الأدبيات، كما ورد: "استخدم الباحث المنهج الوصفي وذلك بالاعتماد على مراجعة عدد من الدراسات السابقة..." وبالتالي،

مجتمع الدراسة = الدراسات والبحوث المنشورة.

أ. دراسة الموارد البشرية (٢٠٢٢)

استخدم الباحث عينة قصدية/مناسبة من العاملين المتاحين في المستشفيات، ويتضح ذلك من قوله: "تم توزيع عدد (٨٠) استبيان... "العينة لم تُحسب إحصائيًا، بل تم اختيارها وفق المتاح.

ب. دراسة الذكاء الاصطناعي (٢٠٢٥)

لا توجد عينة بشرية، لأن الدراسة تعتمد على تحليل محتوى الدراسات السابقة، وليس على استبيانات أو مقابلات.

الأسلوب الإحصائي المستخدم في حساب حجم العينة

أ. دراسة الموارد البشرية (٢٠٢٢)

لم يستخدم الباحث أي معادلة إحصائية لحساب حجم العينة مثل:

- كريجسي ومورغان
- كوكران
- أو غيرها

بل اعتمد على عدد الاستبيانات التي تمكن من توزيعها فعليًا.

ب. دراسة الذكاء الاصطناعي (٢٠٢٥)

لا يوجد حساب لحجم العينة، لأن الدراسة نظرية ولا تتضمن بيانات ميدانية.

ثانيًا: مقارنة منهجية بين الدراستين

العنصر	دراسة الموارد البشرية (٢٠٢٢)	دراسة الذكاء الاصطناعي (٢٠٢٥)
مجتمع الدراسة	العاملون في المستشفيات العامة بولاية الخرطوم لا يوجد مجتمع بشري	مراجعة أدبيات
نوع العينة	عينة قصدية من العاملين	لا توجد عينة
طريقة حساب العينة	لا توجد طريقة حساب	حجم متاح غير مطبق
منهج الدراسة	وصفي تحليلي	دراسة حالة وصفي تحليلي (مراجعة أدبيات)
طبيعة البيانات	كمية (استبيانات)	نوعية (تحليل نظري)

ثالثاً: التحليل النقدي للدراستين

١. قوة وضعف دراسة الموارد البشرية (٢٠٢٢) نقاط القوة

- وجود بيانات ميدانية يمنح الدراسة واقعية.
- استخدام استبيانات يتيح قياساً مباشراً لآراء العاملين.
- ارتباط الدراسة بسياق صحي حساس (المستشفيات العامة).

نقاط الضعف

- عدم استخدام أسلوب إحصائي لحساب حجم العينة يقلل من قوة التعميم.
- العينة قسدية وليست عشوائية، مما يحد من تمثيل المجتمع.
- لم يُذكر إطار العينة أو حجم المجتمع الأصلي.

ثالثاً: التحليل النقدي للدراستين

٢. قوة وضعف دراسة الذكاء الاصطناعي (٢٠٢٥) نقاط القوة

- دراسة حديثة تعالج موضوعاً متطوراً (الذكاء الاصطناعي والأمن السيبراني).
- تعتمد على تحليل أدبيات واسعة، مما يمنحها عمقاً نظرياً.
- تقدم رؤية شاملة حول الأطر والمعايير الدولية.

نقاط الضعف

- غياب بيانات ميدانية يجعل النتائج غير قابلة للتعميم التجريبي.
- الاعتماد على الدراسات السابقة فقط قد يؤدي إلى تحيز انتقائي في اختيار المصادر.
- عدم وجود عينة أو مجتمع يجعل الدراسة نظرية بالكامل.

ثالثاً: التحليل النقدي للدراستين

٣. المقارنة النقدية بين الدراستين

- دراسة الموارد البشرية تطبيقية لكنها تعاني من ضعف في تصميم العينة.
- دراسة الذكاء الاصطناعي نظرية لكنها قوية في التحليل المفاهيمي.
- الأولى تقدم نتائج قابلة للقياس، بينما الثانية تقدم نتائج تفسيرية.
- الأولى تعتمد على البيانات الميدانية، والثانية تعتمد على المعرفة التراكمية.

الخلاصة

كما أظهرت المقارنة بين الدراستين اختلافًا جوهريًا في المنهجية وطبيعة البيانات؛ إذ اعتمدت دراسة الموارد البشرية (٢٠٢٢) على مجتمع ميداني مكوّن من العاملين في المستشفيات العامة بولاية الخرطوم، مستخدمة عينة قصدية دون تطبيق أي أسلوب إحصائي لحساب حجم العينة، مما يحد من قوة التعميم. في المقابل، جاءت دراسة الذكاء الاصطناعي (٢٠٢٥) دراسة نظرية تحليلية لا تتضمن مجتمعًا بشريًا أو عينة، بل اعتمدت على مراجعة الأدبيات العلمية، وهو ما يمنحها عمقًا معرفيًا لكنه يفتقر إلى الأدلة التجريبية. وبذلك تمثل الدراسة الأولى نموذجًا تطبيقيًا محدود القوة الإحصائية، بينما تمثل الثانية نموذجًا نظريًا واسع التحليل لكنه غير قابل للاختبار الميداني.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You



عنوان البحث

دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني

أحمد محمد "البديوي الرحاحله"¹

¹ باحث دكتوراه، المعهد العالي للدكتوراه في الحقوق والعلوم السياسية والإدارية والاقتصادية، الجامعة اللبنانية، لبنان.

بريد الكتروني: Ahmad.rah@aol.com

HNSJ, 2025, 6(10); <https://doi.org/10.53796/hnsj610/23>

المعرف العلمي العربي للأبحاث: <https://arsri.org/10000/610/23>

تاريخ النشر: 2025/10/01م

تاريخ القبول: 2025/09/15م

تاريخ الاستقبال: 2025/09/07م

المستخلص

جاءت هذه الدراسة لتستكشف دور الذكاء (Artificial Intelligence, AI) في تعزيز إدارة مخاطر الأمن السيبراني والامتثال لها. حيث يُتيح دمج الذكاء الاصطناعي في أطر الأمن السيبراني (Cybersecurity Frameworks) تقدماً ملحوظاً في الكشف عن التهديدات والوقاية منها والاستجابة لها. وبلاستفادة من التقنيات المختلفة للذكاء الاصطناعي كخوارزميات التعلم الآلي (Machine Learning, ML) وتحليلات البيانات المتطورة، يُمكن لأنظمة الذكاء الاصطناعي تحليل مجموعات البيانات الضخمة بشكل آني لتحديد الأنماط والانحرافات التي تُشير إلى تهديدات أمنية محتملة. وقد توصلت الدراسة الى عدة نتائج كان من أهمها أن دمج تقنيات الذكاء الاصطناعي في عمليات إدارة مخاطر الأمن السيبراني والامتثال من خلال الأطر والمعايير المعتمدة يوفر مجموعة واسعة من المزايا، بما في ذلك تعزيز الكفاءة، وتحسين الدقة، واتباع نهج أكثر استباقية لإدارة المخاطر. بدءاً من أتمتة المهام الروتينية، وصولاً إلى التنبؤ بالمخاطر المستقبلية وضمان خصوصية البيانات، وعدم التحيز ويعزز من النزاهة والشفافية، يُحدث الذكاء الاصطناعي ثورة في طريقة تعامل المنظمات مع الامتثال. ومع ذلك، من المهم أن الانتباه الى أن الذكاء الاصطناعي لا يُغني عن الرقابة البشرية، بل يُمثل أداة فعالة تُكمل وتُعزز قدرات مُختصي الامتثال. ومع استمرار تطوّر البيئات التنظيمية، سيزداد دور الذكاء الاصطناعي في الامتثال بلا شك أهمية، مما يُساعد المنظمات على التغلب على تعقيدات الامتثال في العصر الرقمي.

الكلمات المفتاحية: الذكاء الاصطناعي، إدارة مخاطر الأمن السيبراني، الامتثال، أطر الأمن السيبراني، تهديدات الأمن السيبراني.

RESEARCH TITLE

The Role of Artificial Intelligence in Enhancing Compliance with Cybersecurity Risk Management

Ahmad Mohammad "Albdaiwi Alrahahleh"¹

¹ PhD Researcher - Higher Institute of Doctorate in Law, Political, Administrative and Economic Sciences , Lebanese University, Lebanon.

Email: Ahmad.rah@aol.com

HNSJ, 2025, 6(10); <https://doi.org/10.53796/hnsj610/23>

Arabic Scientific Research Identifier: <https://arsri.org/10000/610/23>

Received at 07/09/2025

Accepted at 15/09/2025

Published at 01/10/2025

Abstract

This study explores the role of artificial intelligence (AI) in enhancing Cybersecurity risk management and compliance. Integrating AI into Cybersecurity frameworks enables significant progress in detecting, preventing, and responding to threats. Leveraging various AI technologies, such as machine learning algorithms and advanced data analytics, AI systems can analyze massive data sets in real-time to identify patterns and anomalies that indicate potential security threats. The study concluded that integrating AI technologies into Cybersecurity risk management and compliance processes through established frameworks and standards offers a wide range of benefits, including enhanced efficiency, Impartiality and promotes integrity and transparency , improved accuracy, and a more proactive approach to risk management. From automating routine tasks to predicting future risks and ensuring data privacy, AI is revolutionizing the way organizations approach compliance. However, it is important to note that AI does not replace human oversight; rather, it represents an effective tool that complements and enhances the capabilities of compliance professionals. As regulatory environments continue to evolve, the role of AI in compliance will undoubtedly increase in importance, helping organizations navigate the complexities of compliance in the digital age.

Key Words: Artificial intelligence, Cybersecurity Risk Management, Compliance, Cybersecurity Frameworks, Cybersecurity Threats.

مقدمة

أدى التطور السريع في خدمات الإنترنت إلى زيادة ملحوظة في الهجمات الإلكترونية، وبرزت الحاجة إلى تأمين الأنظمة والعمليات، حيث أصبح الأمن السيبراني مصدر قلق لدى المنظمات. ويشمل الأمن السيبراني تقنيات لحماية الأنظمة والشبكات والأجهزة والبرامج والبيانات الإلكترونية والتحكم بعملية الوصول غير المصرح به. وأصبح من الضروري تطوير أطر ومعايير فعالة وآليات دفاعية مبتكرة لمواجهة هذه الهجمات الخطرة، ونظرًا لأن حلول الأمن السيبراني التقليدية أصبحت غير كافية لحماية المعلومات من التهديدات الإلكترونية. فقد ظهرت الحاجة إلى أساليب أمن سيبراني قادرة على اتخاذ قرارات آنية والاستجابة للهجمات الإلكترونية دون تأخير (Dapel, et al, 2023).

وأصبح من الضروري العمل على دمج تقنيات الذكاء الاصطناعي (AI) في أنظمة إدارة المخاطر والامتثال لتعزيز الكفاءة والدقة والاستباقية في اتخاذ القرار. حيث تُمكن تقنيات الذكاء الاصطناعي المنظمات من التنبؤ بالمخاطر، وتحسين الضوابط الداخلية وضمان الامتثال للأنظمة بشكل أكثر فاعلية خاصة تلك المرتبطة بالأمن السيبراني (المصري، فرح، 2024).

وتتضمن هذه الدراسة التعرف أهم الأدوات العملية التي يوفرها الذكاء الاصطناعي لتعزيز عمل الأمن السيبراني والتي يمكن الاستفادة منها في مواجهة التحديات التي تواجه تطبيق معايير وتعليمات إدارة المخاطر والامتثال للأمن السيبراني. والتي قد تساعد ترسيخ الفهم المتعلق بمفهوم قدرات الذكاء الاصطناعي في تحسين فعالية أنظمة إدارة المخاطر والامتثال، وبالتالي تمكينا للحاق بركب التطور التكنولوجي، بل بقيادة هذا الركب نحو مستقبل أكثر تنظيماً وعدالة، واستدامة لضمان الشفافية وتحقيق الأهداف الاستراتيجية للمنظمة بشكل عام.

كما وتركز هذه الدراسة على عرض أهم الأطر والتقنيات اللازمة لفهم ودمج الذكاء الاصطناعي في استراتيجيات إدارة المخاطر والامتثال الخاصة بالمنظمات من خلال استكشاف كيف يمكن لأدوات وتقنيات الذكاء الاصطناعي أن تضمن كفاءة وفعالية عمليات المراقبة، وتقييم المخاطر عن طريق الالتزام باللوائح، وتحسين اتخاذ القرارات على نحو استباقي ومستنير.

الإطار العام للدراسة

المشكلة البحثية وتساؤلاتها

تكمن المشكلة البحثية في معرفة مدى تأثير الذكاء الاصطناعي في إدارة المخاطر الأمن السيبراني وتعزيز الامتثال، وكيفية لعب الذكاء الاصطناعي دوراً محورياً في المنظمات. وكيف يمكن الاستفادة منه في صد الهجمات الخطرة وتعزيز الكفاءة وتقليل الخسائر، بالإضافة إلى مناقشة بعض التحديات التي قد تواجه تطبيقه. ويمكن صياغة مشكلة البحث في التساؤل الرئيسي التالي:

ما هو دور الذكاء الاصطناعي في إدارة المخاطر وتلبية متطلبات الامتثال للأمن السيبراني؟ وينبثق عن هذا السؤال الرئيسي الاسئلة الفرعية التالية:

- ✓ ماهي تقنيات الذكاء الاصطناعي المستخدمة للحد من الهجمات السيبرانية؟
- ✓ ما هي أهم الأطر ومعايير الأمن السيبراني التي يمكن أن تساعد المنظمات على فهم مخاطر الأمن السيبراني وتحسين إدارتها بشكل أفضل؟

- ✓ كيف يمكن دمج تقنيات الذكاء الاصطناعي في إدارة المخاطر وأنظمة الامتثال الحالية؟
- ✓ ما هي الفوائد والتحديات المحتملة لاستخدام الذكاء الاصطناعي في إدارة المخاطر والامتثال؟

الهدف من الدراسة

قدم الباحث مجموعة من الأهداف التي تبين دور الذكاء الاصطناعي في إدارة المخاطر وتلبية متطلبات الامتثال للأمن السيبراني وعلى النحو التالي:

- ◀ التعرف على دور الذكاء الاصطناعي في إدارة المخاطر وتلبية متطلبات الامتثال للأمن السيبراني.
- ◀ التعرف على دور الذكاء الاصطناعي في الحماية من مخاطر الأمن السيبراني.
- ◀ معرفة تأثير استخدام الأطر التنظيمية والمعايير على كفاءة وفعالية إدارة المخاطر والامتثال.
- ◀ توضيح الإطار المفاهيمي للذكاء الاصطناعي والأمن السيبراني، كما تعكسه الأدبيات والدراسات السابقة.
- ◀ تقديم توصيات حول كيفية تطبيق التقنيات الذكاء الاصطناعي بشكل فعال في إدارة المخاطر والامتثال للأمن السيبراني.

أهمية الدراسة

تتجلى أهمية الدراسة في النقاط التالية:

- تساهم الدراسة في فهم كيفية استخدام الذكاء الاصطناعي في تحسين إدارة المخاطر الأمن السيبراني.
- تساهم الدراسة في فهم كيفية استخدام الذكاء الاصطناعي في تحسين عمليات الامتثال لمتطلبات إدارة مخاطر الأمن السيبراني.
- يمكن للنتائج والتوصيات المستخلصة من هذه الدراسة أن تساهم في تحسين الأداء التنظيمي وتحقيق الأهداف بشكل عام للحكومات، للمنظمات وخاصة فيما يتعلق بالأمن السيبراني وحماية البيانات.
- إثراء الأدبيات حول دور الذكاء الاصطناعي في إدارة مخاطر الأمن السيبراني والامتثال.

مصطلحات الدراسة

- **الذكاء الاصطناعي (AI):** هو فرع من علوم الحاسوب يهدف إلى تطوير أنظمة وبرامج قادرة على محاكاة قدرات الذكاء البشري، مثل التعلم، والتفكير، واتخاذ القرار، وحل المشكلات. ويعتمد الذكاء الاصطناعي على خوارزميات وتقنيات تمكن الآلات من تحليل البيانات، والتعرف على التلخص، والتكيف مع الظروف المختلفة بشكل مستقل أو شبه مستقل (البلقاسي، منال، 2025).
- **الأمن السيبراني (Cyber Security):** الأمن السيبراني هو مجموعة من العمليات والتقنيات والممارسات لحماية الأفراد الرقميين والبنية التحتية والبيانات المتاحة عبر الفضاء الإلكتروني من الهجمات والأضرار والوصول غير المصرح به (Maleh & Maleh, 2022).
- **إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management):** بحسب تعريف توفيق (2025) إدارة مخاطر الأمن السيبراني بأنها "مجموعة السياسات والأنشطة التي تهدف إلى تحديد نقاط الضعف في الموارد المرتبطة بأنظمة المعلومات والاتصال للمنظمة، وتنفيذ إجراءات وضوابط أمن سيبراني فعالة للتخفيف من الآثار السلبية لهذه الاختراقات، والتقييم الدوري للمخاطر السيبرانية، وإدارة مخاطر الأمن السيبراني". (ص. 863).

• **الامتثال للأمن السيبراني (Cybersecurity Compliance):** يشير الامتثال للأمن السيبراني إلى الالتزام بالقوانين والمعايير والمتطلبات التنظيمية التي تضعها الحكومات والجهات المعنية بالقطاع. صُممت هذه اللوائح التنظيمية لحماية المعلومات الرقمية وأنظمة المعلومات الخاصة بالشركات من التهديدات السيبرانية، بما في ذلك الوصول غير المصرح به، والاستخدام، والإفصاح، والتعطيل، والتعديل، والتدمير. (Graham, Kaitlyn, 2025).

منهجية البحث

استخدم الباحث المنهج الوصفي وذلك بالاعتماد على مراجعة عدد من الدراسات السابقة والأدب النظري المتعلق بدور الذكاء الاصطناعي في إدارة المخاطر وتلبية متطلبات الامتثال للأمن السيبراني. حيث يعتمد البحث على استعراض وتحليل مجموعة من الدراسات والأبحاث السابقة المتعلقة بتقنية الذكاء الاصطناعي ودورها في تعزيز إدارة المخاطر وتلبية متطلبات الامتثال للأمن السيبراني. وقد تم جمع البيانات من خلال مراجعة وتحليل العديد من الدراسات والأبحاث المنشورة في المجالات العلمية والكتب والتقارير الرسمية.

وتمثلت أدوات الدراسة المستخدمة التقنيات النقدية والتحليلية لاستخلاص النتائج المتعلقة بتطبيقات الذكاء الاصطناعي في مجال إدارة المخاطر والامتثال للأمن السيبراني.

الدراسات السابقة

دراسة (الزيود، احمد، 2020) بعنوان : إدارة مخاطر الأمن السيبراني في البنوك الأردنية.

تناولت الدراسة مفهوم الأمن السيبراني من جوانب متعددة، كإدارة المخاطر السيبرانية، وأنواع التهديدات ومجالاتها. كما ناقشت الدراسة مجموعة من الأدوات التي يمكن استخدامها في إدارة تقييم المخاطر في البنوك الأردنية والتي تهدف إلى المحافظة على سلامة البنوك وتدعيم مراكزها، والتحقق من سلامة إجراءاتها، والمحافظة على أمن معلوماتها، وبياناتها وأجهزة حفظ المعلومات. كما سعت هذه الدراسة لإظهار أهمية إدارة مخاطر الأمن السيبراني في البنوك الأردنية وضرورة توضيح السياسات والإجراءات المتعلقة بالأمن السيبراني بشكل أكثر دقة. وقام الباحث بإتباع المنهج الوصفي والتحليلي لوصف أدوات إدارة وتقييم مخاطر الأمن السيبراني في البنوك الأردنية، وبيان مدى التزام البنوك الأردنية بالسياسات الخاصة بأمان المعلومات وسياسة الأمن السيبراني.

و قد أظهرت نتائج الدراسة ضرورة التزام البنوك الأردنية بتطبيق ومتابعة جميع التعليمات الصادرة من البنك المركزي الأردني فيما يتعلق بالأمن السيبراني، بالإضافة الى ضرورة قيام البنوك الأردنية بنشر دليل الحاكمية المؤسسية لتكنولوجيا المعلومات ضمن التقارير السنوية أو ضمن تقارير خاصة على مواقعها.

دراسة قاسم، زينب و رشوان، عبد الرحمن. (2022) بعنوان: أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك.

هدفت الدراسة إلى التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك الفلسطينية، وتقديم تشخيص لواقع إدارة مخاطر الأمن السيبراني من أجل دعم تطبيق الشمول المالي لتعزيز الاستقرار المالي لهذه البنوك، والاجابة على التساؤلات البحثية واختبار فرضيات الدراسة. وقد أعتمد الباحثان على المنهج الوصفي التحليلي، واستخدمت الاستبانة كأداة لجمع المعلومات. و وزعت على عدد من المتخصصين من المدراء العاملين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين؛ حيث بلغت عينة الدراسة (90) مفردة.

و أثبتت نتائج الدراسة أنه يوجد أثر لإدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة

في بورصة فلسطين، كما تقوم البنوك المدرجة في بورصة فلسطين بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي.

(Aror, Tina Akpevben and Mupa, Munashe Naphtali, 2025): "Risk and compliance paper what role does Artificial Intelligence (AI) play in enhancing risk management practices in corporation"?

جاءت هذه الدراسة لتقييم الدور الجديد الذي يلعبه الذكاء الاصطناعي في تعزيز فعالية عمليات إدارة المخاطر والامتثال في المؤسسات من خلال كيفية تطبيق تقنيات الذكاء الاصطناعي القادرة على جمع المعلومات وتحليلها ومعالجتها وتقييمها، بما في ذلك التعلم الآلي ومعالجة اللغة الطبيعية والتحليلات التنبؤية، بهدف تحديد المخاطر المختلفة وتقييمها والتخفيف منها. سواءً تعلق الأمر بكشف الاحتيال المالي، أو الأمن السيبراني، أو الانقطاعات التشغيلية، أو الامتثال، فإن أدوات الذكاء الاصطناعي تزيد من سرعة اكتشاف المخاطر، وتزيد من إمكانيات تحليل البيانات، وتوفر الدعم للمراقبة والتنبؤ في الوقت الفعلي. كما تناقش هذه الدراسة كيفية مساهمة الذكاء الاصطناعي في أتمتة مهام إدارة المخاطر والامتثال المتكررة، مما يُمكن مديري المخاطر من التركيز على المراقبة السيبرانية رفيعة المستوى. وتشير نتائج الدراسة إلى أنه و عند دمج الذكاء الاصطناعي بشكل صحيح، يُمكنه تعزيز إدارة المخاطر والامتثال في المؤسسة وزيادة مرونتها في بيئة أعمال سريعة التغير وأكثر غموضاً.

(Mehmood et al., 2025): Cyber security Governance as a Pillar of Enterprise Risk Management: Designing Compliance–Driven Framework for Operational Resilience, Policy Enforcement, and Regulatory Alignment.

تركز الدراسة على مفهوم دمج حوكمة الأمن السيبراني في أنظمة إدارة المخاطر المؤسسية، بما في ذلك استخدامها التشغيلي لتعزيز تدابير الحماية المعمول بها، وتنفيذ السياسات، والامتثال للمعايير الدولية. حيث تألف المشاركون في الدراسة من 146 متخصصاً في الأمن السيبراني وإدارة المخاطر، والذين استجابوا لاستطلاع رأي عبر الإنترنت. تُظهر هذه النتائج أن المؤسسات التي لديها برامج حوكمة متطورة، أو تلك التي تخصص موارد مثل مسؤول أمن المعلومات (Chief Information Security Officer, CISO)، وإعداد تقارير المخاطر، بالإضافة إلى تقنيات الأتمتة في هيكلها التنظيمي يمكنها الاستجابة بشكل أفضل أثناء الحوادث السيبرانية، وتتمتع بأوقات استجابة أسرع، وتتمتع بمستويات أعلى من الامتثال للوائح. وتدعو نتائج الدراسة إلى إيلاء المزيد من الاهتمام لمسألة حوكمة الأمن السيبراني، ليس فقط باعتبارها عنصراً أساسياً في الرقابة، بل أيضاً كمورد قيم لاستدامة المؤسسة وأساس لاتخاذ قرارات مواتية للمخاطر.

(Mohammed, A., 2023): Elevating Cybersecurity Audits: How AI is Shaping Compliance and Threat Detection

تهدف هذه الدراسة إلى استكشاف التأثير التحويلي للذكاء الاصطناعي على عمليات تدقيق الأمن السيبراني من خلال تسليط الضوء على قدراته في تحسين الامتثال، وأتمتة الكشف عن التهديدات، وتبسيط سير عمل التدقيق. فمن خلال استخدام التعلم الآلي (ML) ومعالجة اللغة الطبيعية (NLP)، واكتشاف الانحرافات في المعلومات، والتحليلات التنبؤية، يُمكن الذكاء الاصطناعي المدققين من تحديد نقاط الضعف، واكتشاف الأنماط غير العادية، وتقييم الامتثال وبشكل آني. بالإضافة إلى المساعدة في تقليل الأخطاء البشرية وزيادة دقة التدقيق. كما تستكشف الدراسة كيف يضمن الذكاء

الاصطناعي الامتثال لأطر عمل مثل اللائحة العامة لحماية البيانات (General Data Protection Regulation, GDPR)، وقانون نقل التأمين الصحي والمساءلة (Health Insurance Portability and Accountability Act, HIPA)، ومعايير أمن معلومات بطاقات الدفع (Payment Card Industry Data Security Standard, PCIDSS). وتختتم الدراسة بعرض لأفضل الممارسات للمؤسسات التي تسعى إلى الاستفادة من الذكاء الاصطناعي لإجراء عمليات تدقيق أمن سيبراني أكثر فعالية وإدارة امتثال.

(Chettier, Thiyagarajan Mani and Boyina, Venkata Ashok Kumar and Ranginenis, Sandeep, 2025): AI-Powered Risk Assessment and Compliance in Cloud Cybersecurity.

قدمت هذه الدراسة تصوراً حول استخدام التعلم الآلي (ML) والذكاء الاصطناعي (AI) لتحسين القدرة على الكشف عن التهديدات السيبرانية، وأتمتة مراقبة الامتثال، وتقليل نقاط الضعف في الأنظمة، كما تُقدم الدراسة نهجاً مُعزّزاً بالذكاء الاصطناعي لتقييم مخاطر الأمن السيبراني في الحوسبة السحابية والامتثال للوائح الأمن السيبراني. من خلال تطبيق التحليلات السلوكية، واكتشاف الانحرافات في القواعد الأمنية، والتحليلات التنبؤية للكشف عن التهديدات السيبرانية قبل وقوعها. يُمكن للذكاء الاصطناعي تحليل مجموعات البيانات الضخمة لتحديد ثغرات الامتثال، والتوصية بالحلول، وتقديم تقارير جاهزة للتدقيق مع تقليل النفقات التشغيلية والأخطاء البشرية. ومن نتائج هذه الدراسة أنها بينت الفوائد التي يمكن أن تجنيها المؤسسات من استخدام الذكاء الاصطناعي لإدارة الامتثال، كخفض تكاليف التدقيق، وتحسين حوكمة الأمن السيبراني، وتسريع إعداد التقارير التنظيمية. كما تشير النتائج إلى ضرورة استخدام تطبيقات الذكاء الاصطناعي لتأمين بيانات الحوسبة السحابية، وتوصي بمزيد من الاعتماد عليها في أطر الأمن السيبراني.

(Folorunso, et al. , 2024, a): A governance framework model for cloud computing: role of AI, security, compliance, and management.

جاءت هذه الدراسة لتقترح نموذجاً شاملاً لإطار حوكمة يدمج أدوار وقواعد الذكاء الاصطناعي، والأمن، والامتثال، والإدارة بهدف تعزيز فعالية عمليات الحوسبة السحابية للمنظمة. ويلعب الذكاء الاصطناعي دوراً حاسماً في تحسين تخصيص الموارد وتحسين عمليات صنع القرار في إطار حوكمة الحوسبة السحابية. وذلك من خلال الاستفادة من خوارزميات التعلم الآلي (ML)، وتحليلات تنبؤية، ومراقبة عمليات الامتثال بشكل آلي ومؤتمت، مما يعزز الكفاءة التشغيلية ويقلل من الأخطاء البشرية.

علاوة على ذلك، يُسهّل دمج الذكاء الاصطناعي في إدارة الأمن الكشف عن التهديدات والاستجابة لها في الوقت الفعلي، مما يسمح للمؤسسات بالتخفيف بشكل استباقي من المخاطر المرتبطة باختراقات البيانات والهجمات الإلكترونية. يُعدّ الامتثال للمتطلبات التنظيمية أمراً أساسياً لضمان المساءلة التنظيمية وتقليل المخاطر القانونية. يتضمن نموذج الحوكمة المقترح عمليات تحقق امتثال مؤتمتة وآليات إعداد تقارير، مما يضمن الالتزام باللوائح التنظيمية الخاصة بالمنظمة، مثل اللائحة العامة لحماية البيانات (General Data Protection Regulation, GDPR) وقانون نقل التأمين الصحي والمساءلة (Health Insurance Portability and Accountability Act, HIPAA). وتوصلت الدراسة إلى أن فعالية حوكمة الحوسبة السحابية تتجلى في المكونات الأساسية للذكاء الاصطناعي، والأمن، والامتثال، والإدارة. ويلعب الذكاء الاصطناعي دوراً محورياً في تعزيز حوكمة الحوسبة السحابية من خلال تحسين الموارد، واكتشاف التهديدات، ومراقبة الامتثال التنظيمي.

(ShaikhMuhammad, Adeel, 2025): AI-Powered Cybersecurity Compliance.

تبحث هذه الدراسة في جدوى تطبيق الحلول القائمة على الذكاء الاصطناعي لتعزيز الامتثال للأمن السيبراني في المنظمات. فهي تقدم إطار عمل يستخدم تقنيات معالجة اللغة الطبيعية (NLP) والتعلم الآلي (ML)، والتي تفحص الأطر القانونية لاستخراج قواعد الامتثال، وتفحص في الوقت نفسه سجلات النظام بحثاً عن أنشطة عدم الامتثال. كما تشرح الورقة البحثية العقبات الرئيسية أمام نشر أنظمة الامتثال القائمة على الذكاء الاصطناعي، وتوضح كيفية معالجة هذه الصعوبات. وبالتالي، يمكن للذكاء الاصطناعي أن يُعزز بشكل كبير عمليات التحقق من الامتثال، ويعزز إمكانية تحديد التهديدات في المنظمات، مما يعني إمكانات كبيرة لتوجيه امتثال الأمن السيبراني وإدارة المخاطر في المستقبل. وتشير نتائج الدراسة إلى أن أدوات الذكاء الاصطناعي، مثل استخراج القواعد من نماذج معالجة اللغة الطبيعية (NLP) لاستخدامها في تحديد قواعد الامتثال، ونماذج التعلم الآلي (ML) للكشف عن الانحرافات في البيانات والتي لديها القدرة على تعزيز تحسين مراقبة الامتثال من خلال البساطة والكفاءة والمرونة.

دراسة الزيود، احمد. (2020) بعنوان : ادارة مخاطر الأمن السيبراني في البنوك الأردنية.

تناولت الدراسة مفهوم الأمن السيبراني من عدة جوانب، كإدارة المخاطر السيبرانية، وأنواع التهديدات ومجالاتها. كما ناقشت الدراسة مجموعة من الأدوات التي يمكن استخدامها في إدارة تقييم المخاطر في البنوك والتي تهدف إلى المحافظة على سلامة البنوك والتحقق من سلامة إجراءاتها، والمحافظة على أمن معلوماتها، وبياناتها وأجهزة حفظ المعلومات. كما سعت هذه الدراسة لإظهار أهمية إدارة مخاطر الأمن السيبراني في البنوك الأردنية وضرورة توضيح السياسات والإجراءات المتعلقة بالأمن السيبراني بشكل أكثر دقة. وقام الباحث بإتباع المنهج الوصفي والتحليلي لوصف أدوات إدارة وتقييم مخاطر الأمن السيبراني في البنوك الأردنية، وبيان مدى التزام البنوك الأردنية بالسياسات الخاصة بأمان المعلومات وسياسة الأمن السيبراني.

و قد أظهرت نتائج الدراسة ضرورة التزام البنوك الاردنية بتطبيق ومتابعة جميع التعليمات الصادرة من البنك المركزي الأردني فيما يتعلق بالأمن السيبراني، بالإضافة الى ضرورة قيام البنوك الأردنية بنشر دليل الحاكمية المؤسسية لتكنولوجيا المعلومات ضمن التقارير السنوية أو ضمن تقارير خاصة على مواقعها.

دراسة قاسم، زينب و رشوان، عبد الرحمن.(2022) بعنوان: أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك.

هدفت الدراسة إلى التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك الفلسطينية، وتقديم تشخيص لواقع إدارة مخاطر الأمن السيبراني من أجل دعم تطبيق الشمول المالي لتعزيز الاستقرار المالي لهذه البنوك، والاجابة على التساؤلات البحثية واختبار فرضيات الدراسة. وقد اعتمد الباحثان على المنهج الوصفي التحليلي، واستخدمت الاستبانة كأداة لجمع المعلومات. و وزعت على عدد من المتخصصين من المدراء العاملين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين؛ حيث بلغت عينة الدراسة (90) مفردة. و أثبتت نتائج الدراسة أنه يوجد أثر لإدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، كما تقوم البنوك المدرجة في بورصة فلسطين بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي.

(Aror, Tina Akpevben and Mupa, Munashe Naphtali, 2025): "Risk and compliance paper what role does Artificial Intelligence (AI) play in enhancing risk management practices in corporation"?

جاءت هذه الدراسة لتقييم الدور الجديد الذي يلعبه الذكاء الاصطناعي في تعزيز فعالية عمليات إدارة المخاطر والامتثال في المؤسسات من خلال كيفية تطبيق تقنيات الذكاء الاصطناعي القادرة على جمع المعلومات وتحليلها ومعالجتها وتقييمها، بما في ذلك التعلم الآلي، ومعالجة اللغة الطبيعية والتحليلات التنبؤية، بهدف تحديد المخاطر المختلفة وتقييمها والتخفيف منها. سواءً تعلق الأمر بكشف الاحتيال المالي، أو الأمن السيبراني، أو الانقطاعات التشغيلية، أو الامتثال، فإن أدوات الذكاء الاصطناعي تزيد من سرعة اكتشاف المخاطر، وتزيد من إمكانيات تحليل البيانات، وتوفر الدعم للمراقبة والتنبؤ في الوقت الفعلي. كما تناقش هذه الدراسة كيفية مساهمة الذكاء الاصطناعي في أتمتة مهام إدارة المخاطر والامتثال المتكررة، مما يُمكن مديري المخاطر من التركيز على المراقبة السيبرانية رفيعة المستوى. وتشير نتائج الدراسة إلى أنه و عند دمج الذكاء الاصطناعي بشكل صحيح، يُمكنه تعزيز إدارة المخاطر والامتثال في المؤسسة وزيادة مرونتها في بيئة أعمال سريعة التغير وأكثر غموضًا.

(Mehmood et al., 2025): Cyber security Governance as a Pillar of Enterprise Risk Management: Designing a Compliance-Driven Framework for Operational Resilience, Policy Enforcement, and Regulatory Alignment

تركز الدراسة على مفهوم دمج حوكمة الأمن السيبراني في أنظمة إدارة المخاطر المؤسسية، بما في ذلك استخدامها التشغيلي لتعزيز تدابير الحماية المعمول بها، وتنفيذ السياسات، والامتثال للمعايير الدولية. حيث تألف المشاركون في الدراسة من 146 متخصصًا في الأمن السيبراني وإدارة المخاطر، والذين استجابوا لاستطلاع رأي عبر الإنترنت. تُظهر هذه النتائج أن المؤسسات التي لديها برامج حوكمة متطورة، أو تلك التي تخصص موارد مثل مسؤول أمن المعلومات (Chief Information Security Officer, CISO)، وإعداد تقارير المخاطر، بالإضافة إلى تقنيات الأتمتة في هيكلها التنظيمي يمكنها الاستجابة بشكل أفضل أثناء الحوادث السيبرانية، وتتمتع بأوقات استجابة أسرع، وتتمتع بمستويات أعلى من الامتثال للوائح. وتدعو نتائج الدراسة إلى إيلاء المزيد من الاهتمام لمسألة حوكمة الأمن السيبراني، ليس فقط باعتبارها عنصرًا أساسيًا في الرقابة، بل أيضًا كمورد قيم لاستدامة المؤسسة وأساس لاتخاذ قرارات مواتية للمخاطر.

(Mohammed, A., 2023): Elevating Cybersecurity Audits: How AI is Shaping Compliance and Threat Detection

تهدف هذه الدراسة إلى استكشاف التأثير التحويلي للذكاء الاصطناعي على عمليات تدقيق الأمن السيبراني من خلال تسليط الضوء على قدراته في تحسين الامتثال، وأتمتة الكشف عن التهديدات، وتبسيط سير عمل التدقيق. فمن خلال استخدام التعلم الآلي (ML) ومعالجة اللغة الطبيعية (NLP)، واكتشاف الانحرافات في المعلومات، والتحليلات التنبؤية، يُمكن الذكاء الاصطناعي المدققين من تحديد نقاط الضعف، واكتشاف الأنماط غير العادية، وتقييم الامتثال وبشكل آني. بالإضافة إلى المساعدة في تقليل الأخطاء البشرية وزيادة دقة التدقيق. كما تستكشف الدراسة كيف يضمن الذكاء الاصطناعي الامتثال لأطر عمل مثل اللائحة العامة لحماية البيانات (General Data Protection Regulation (GDPR))، وقانون نقل التأمين الصحي والمساءلة (Health Insurance Portability and Accountability Act (HIPA))، ومعايير أمن معلومات بطاقات الدفع (Payment Card Industry Data Security Standard)،

(PCIDSS)، مع التكيف مع احتياجات الامتثال المتغيرة بمرور الوقت. وتختتم الدراسة بعرض لأفضل الممارسات للمؤسسات التي تسعى إلى الاستفادة من الذكاء الاصطناعي لإجراء عمليات تدقيق أمن سيبراني أكثر فعالية وإدارة امتثال.

(Chettier, Thiyagarajan Mani and Boyina, Venkata Ashok Kumar and Ranginenis, Sandeep, 2025): AI-Powered Risk Assessment and Compliance in Cloud Cybersecurity.

قدمت هذه الدراسة تصوراً حول استخدام التعلم الآلي (ML) والذكاء الاصطناعي (AI) لتحسين القدرة على الكشف عن التهديدات السيبرانية، وأتمتة مراقبة الامتثال، وتقليل نقاط الضعف في الأنظمة، كما تُقدم الدراسة نهجاً مُعززاً بالذكاء الاصطناعي لتقييم مخاطر الأمن السيبراني في الحوسبة السحابية والامتثال للوائح الأمن السيبراني. من خلال تطبيق التحليلات السلوكية، واكتشاف الانحرافات في القواعد الأمنية، والتحليلات التنبؤية للكشف عن التهديدات السيبرانية قبل وقوعها. يُمكن للذكاء الاصطناعي تحليل مجموعات البيانات الضخمة لتحديد ثغرات الامتثال، والتوصية بالحلول، وتقديم تقارير جاهزة للتدقيق مع تقليل النفقات التشغيلية والأخطاء البشرية. ومن نتائج هذه الدراسة أنها بينت الفوائد التي يمكن أن تجنيها المؤسسات من استخدام الذكاء الاصطناعي لإدارة الامتثال، كإخفاض تكاليف التدقيق، وتحسين حوكمة الأمن السيبراني، وتسريع إعداد التقارير التنظيمية. كما تشير النتائج إلى ضرورة استخدام تطبيقات الذكاء الاصطناعي لتأمين بيانات الحوسبة السحابية، وتوصي بمزيد من الاعتماد عليها في أطر الأمن السيبراني.

(Folorunso, et al. , 2024, a): A governance framework model for cloud computing: role of AI, security, compliance, and management.

جاءت هذه الدراسة لتقترح نموذجاً شاملاً لإطار حوكمة يدمج أدوار وقواعد الذكاء الاصطناعي، والأمن، والامتثال، والإدارة بهدف تعزيز فعالية عمليات الحوسبة السحابية للمنظمة. و يلعب الذكاء الاصطناعي دوراً حاسماً في تحسين تخصيص الموارد وتحسين عمليات صنع القرار في إطار حوكمة الحوسبة السحابية. وذلك من خلال الاستفادة من خوارزميات التعلم الآلي (ML)، وتحليلات تنبؤية، ومراقبة عمليات الامتثال بشكل آلي ومؤتمت، مما يعزز الكفاءة التشغيلية ويقلل من الأخطاء البشرية. علاوة على ذلك، يُسهّل دمج الذكاء الاصطناعي في إدارة الأمن الكشف عن التهديدات والاستجابة لها في الوقت الفعلي، مما يسمح للمؤسسات بالتخفيف بشكل استباقي من المخاطر المرتبطة باختراقات البيانات والهجمات الإلكترونية. يُعدّ الامتثال للمتطلبات التنظيمية أمراً أساسياً لضمان المساءلة التنظيمية وتقليل المخاطر القانونية. يتضمن نموذج الحوكمة المقترح عمليات تحقق امتثال مؤتمتة وآليات إعداد تقارير، مما يضمن الالتزام باللوائح التنظيمية الخاصة بالمنظمة، مثل اللائحة العامة لحماية البيانات (General Data Protection Regulation, GDPR) وقانون نقل التأمين الصحي والمساءلة (Health Insurance Portability and Accountability Act, HIPAA). وتوصلت الدراسة إلى أن فعالية حوكمة الحوسبة السحابية تتجلى في المكونات الأساسية للذكاء الاصطناعي، والأمن، والامتثال، والإدارة. ويلعب الذكاء الاصطناعي دوراً محورياً في تعزيز حوكمة الحوسبة السحابية من خلال تحسين الموارد، واكتشاف التهديدات، ومراقبة الامتثال التنظيمي.

(ShaikhMuhammad, Adeel, 2025): AI-Powered Cybersecurity Compliance.

تبحث هذه الدراسة في جدوى تطبيق الحلول القائمة على الذكاء الاصطناعي لتعزيز الامتثال للأمن السيبراني في المنظمات. فهي تقدم إطار عمل يستخدم تقنيات معالجة اللغة الطبيعية (NLP) والتعلم الآلي (ML)، والتي تفحص الأطر

القانونية لاستخراج قواعد الامتثال، وتخصص في الوقت نفسه سجلات النظام بحثاً عن أنشطة عدم الامتثال. كما تشرح الورقة البحثية العقبات الرئيسية أمام نشر أنظمة الامتثال القائمة على الذكاء الاصطناعي، وتوضح كيفية معالجة هذه الصعوبات. وبالتالي، يمكن للذكاء الاصطناعي أن يُعزز بشكل كبير عمليات التحقق من الامتثال، ويعزز إمكانية تحديد التهديدات في المنظمات، مما يعني إمكانات كبيرة لتوجيه امتثال الأمن السيبراني وإدارة المخاطر في المستقبل. وتشير نتائج الدراسة إلى أن أدوات الذكاء الاصطناعي، مثل استخراج القواعد من نماذج معالجة اللغة الطبيعية (NLP) لاستخدامها في تحديد قواعد الامتثال، ونماذج التعلم الآلي (ML) للكشف عن الانحرافات في البيانات والتي لديها القدرة على تعزيز تحسين مراقبة الامتثال من خلال البساطة والكفاءة والمرونة.

المحتوى النظري للدراسة

المبحث الأول: الذكاء الاصطناعي والأمن السيبراني

◀ مفهوم الذكاء الاصطناعي

الذكاء الاصطناعي (Artificial Intelligence) AI هو أحد فروع علم الحاسوب، وإحدى الركائز الأساسية التي تقوم عليها صناعة التكنولوجيا في العصر الحالي (مقاتل و حسني، 2021). وقد عرّفت محسن، لمياء (2024) الذكاء الاصطناعي "على أنه علم من علوم الحاسب، يهدف إلى ابتكار وتصميم أنظمة الحاسبات الذكية، التي تحاكي أسلوب الذكاء البشري نفسه، لتتمكن تلك الأنظمة من أداء المهام بدلاً من الإنسان، ومحاكاة وظائفه وقدراته باستخدام خواصها الكيفية وعلاقتها المنطقية والحسابية". (ص.19).

◀ أنواع الذكاء الاصطناعي حسب مجالات الاستخدام

تعتمد أدوات واستراتيجيات الأمن السيبراني الحديثة على مزيج من المكونات المتعلقة بالذكاء الاصطناعي؛ حيث يتم تصنيف الذكاء الاصطناعي بناءً على مجالات الاستخدام نذكر منها ما يلي، والتي يمكن أن تخدم عمل الأمن السيبراني (Folorunso, et al. , 2024, a):

❖ التعلم الآلي (Machine Learning, ML): يعمل التعلم الآلي (ML) على تمكين أجهزة الكمبيوتر والآلات

من تقليد الطريقة التي يتعلم بها البشر، وأداء المهام بشكل مستقل، وتحسين أدائها ودقتها من خلال الخبرة والتعرض لمزيد من البيانات باستخدام خوارزميات رياضية وإحصائية لتحليل البيانات واكتشاف الأنماط فيها؛ مما يسمح للنظام باتخاذ قرارات أو تقديم تنبؤات دقيقة. (حسان، ساره، 2025). ويتم استخدام التعلم الآلي بشكل متزايد للكشف عن التهديدات، ورصد الأنماط والقضاء عليها في مراحلها الأولى قبل أن تتمكن من إحداث الأضرار بفضل قدرتها على فرز ملايين الملفات وتحديد الملفات التي يحتمل أن تشكل خطراً، وكشف ثغرات الشبكة، وتوقع متى وكيف ستحدث الهجمات الإلكترونية المستقبلية.

❖ الشبكة العصبية (Neural Network, NN): الشبكات العصبية (NN) هي برنامج أو نماذج حسابية وتعلم

آلي مستوحاة من طريقة عمل الدماغ البشري. تتخذ القرارات باستخدام العمليات التي تحاكي الطريقة التي تعمل بها الخلايا العصبية البيولوجية. وتستخدم هذه الشبكات في معالجة المعلومات والتعلم من البيانات، مما يجعلها مثالية للتنبؤات المعقدة بهدف تحديد الظواهر ووزن الخيارات والوصول إلى الاستنتاجات المتوقعة أو غير المتوقعة. (التير، فاطمة علي وآخرون، 2024). حيث تكمن أهمية أنظمة الأمن السيبراني القائمة على الشبكات العصبية الاصطناعية (ANN) في قدرتها على تحليل مجموعات ضخمة من البيانات وتحديد الأنماط. سواء كان

الأمر يتعلق بمراقبة حركة مرور الشبكة، أو تحليل سلوك المستخدم، أو مسح سجلات النظام، فإن الشبكات العصبية الاصطناعية قادرة على معالجة البيانات بسرعات تفوق القدرات البشرية بكثير بهدف التعرف على البيانات المشبوهة والتهديدات المحتملة.

❖ **أنظمة الخبراء (Expert Systems, ES):** تعرف أنظمة الخبراء (ES) بأنها برنامج حاسوبي مصمم لحل المشكلات المعقدة وتوفير القدرة على اتخاذ القرار مثل الخبير البشري باستخدام تقنيات الذكاء الاصطناعي، وهو يقوم بذلك عن طريق استخراج المعرفة من قاعدة المعرفة الخاصة به باستخدام قواعد المنطق والاستدلال وفقاً لاستفسارات المستخدم (Veena, P, 2023). ويمكن استخدام أنظمة الخبراء (ES) لفحص الشبكات بحثاً عن الثغرات الأمنية من خلال مراقبة حركة مرور الشبكة واستخدام قواعد محددة مسبقاً. وكشف هجمات التصيد والتطفل، ورصد أي أنشطة غير معتادة قد تشير إلى هجوم إلكتروني.

❖ **المنطق الضبابي (Fuzzy Logic, FL):** تقوم تطبيقات المنطق الضبابي (FL) بتحليل وتعديل المعلومات غير المؤكدة، والتعامل مع حالات عدم اليقين عن طريق قياس درجة صحة الفرضيات المختلفة من خلال اللجوء إلى أساليب التحليل المنطقي باستخدام المفاهيم الرياضية لتوفير حلول فعالة لبعض المشكلات التي تواجه البشر من خلال الدمج بين التفكير البشري ونظم اتخاذ القرار (الشرقاوي، ماجد أبو النجا، 2023، ص. 296). ويعتبر المنطق الضبابي أداة فعالة ومتعددة الاستخدامات لتحسين أنظمة الأمن السيبراني وأنظمة إستخبارات التهديدات السيبرانية. حيث يوفر لأنظمة الأمن السيبراني القدرة على معالجة حالات عدم اليقين وعدم الدقة في البيانات والمعلومات، وتوفير معلومات استخباراتية أكثر دقة وفائدة للمستخدمين. (Sharma, et al., 2023).

❖ **البرمجة اللغوية الطبيعية (Natural Language Processing, NLP):** وهي أحد أنواع الذكاء الاصطناعي الذي يختص بالتعامل مع اللغات البشرية وفهمها، وهو يتحمل مهمة التواصل بين الآلة والإنسان من خلال اللغات البشرية كاللغة العربية، كما أنه يساعد الآلة على استخراج معلومات ذات معنى من المحتوى المختلف والتعبير عنه (محسن، ليماء، 2024).

وبرزت أهمية معالجة اللغة الطبيعية (NLP) كتقنية محورية في تعزيز تدابير الأمن السيبراني، فمعالجة اللغة الطبيعية تتضمن مهاماً مثل تصنيف النصوص، وتحليل المشاعر، وترجمة اللغات، والإجابة على الأسئلة، وتطوير روبوتات الدردشة. وتُعد معالجة اللغة الطبيعية في مجال الأمن السيبراني أداة فعالة لتعزيز كشف الاحتيال ومنعه. فهي تُمكن الأنظمة من معالجة وتحليل البيانات النصية غير المهيكلة، مثل رسائل البريد الإلكتروني للعملاء، والتعليقات الإلكترونية، وأوصاف المعاملات، لاستخلاص معلومات مفيدة. كما تستطيع خوارزميات معالجة اللغة الطبيعية (NLP) كشف الكلمات المفتاحية المتعلقة بالاحتيال، حيث يمكن لأنظمة الذكاء الاصطناعي تصفية وتفسير كميات كبيرة من البيانات النصية التي قد تعطي مؤشراً قوياً لأنشطة احتيالية. وهذا يُتيح لمحلي الاحتيال فهماً أفضل للمخاطر المحتملة، ما يسمح بإجراء تقييمات أكثر إستهدافاً للتهديدات (Barone, n.d).

◀ أهم مزايا الذكاء الاصطناعي في مجال الأمن السيبراني

أشارت محسن (2024) إن استخدام تقنيات الذكاء الاصطناعي في مجال الحماية السيبرانية وسيلة قوية وفعالة للحماية الشاملة للأنظمة، والشبكات والبيانات من التهديدات الأمنية، وذلك من خلال توفير المزايا التالية الجديرة بالاهتمام في منظمات الأعمال:

- **البحث عن خصائص الهجمات الإلكترونية:** يُحلل الذكاء الاصطناعي كميات هائلة من البيانات لتحديد أنماط ومؤشرات الاختراق، و يُساعد هذا النهج فرق الأمن على تحديد سلوك الشبكة المشبوه، ومحاولات تسجيل الدخول غير الاعتيادية، وحركة البيانات غير الطبيعية من أجهزة إنترنت الأشياء أو نقاط الضعف في الوقت الفعلي، وهذا يساعد على تكوين وتقوية الضوابط والعمليات لتحسين المرونة السيبرانية بأقصى فعالية. (Mohammed, A., 2023).
- **سرعة الاستجابة للحوادث السيبرانية:** يعمل الذكاء الاصطناعي على تحسين الاستجابة للحوادث من خلال أتمتة عملية اكتشاف التهديدات وتحليلها والتخفيف من حداثها. وبالتالي، يُقلّل الوقت المستغرق من لحظة الاكتشاف إلى اتخاذ الإجراء، ويُقلّل من آثار الاختراقات المحتملة.
- كما تُوفّر الأنظمة المُدعّمة بالذكاء الاصطناعي سياقًا مُحسّنًا لتحديد أولويات التنبيهات الأمنية، وتُحدّد الأسباب الجذرية للتخفيف من نقاط الضعف ومنع المشاكل المستقبلية (Aror, Tina Akpevben and Mupa, Munashe) (Naphtali, 2025).
- **تعزيز الدفاعات:** يُقدم الذكاء الاصطناعي إمكانية تسهيل شرح التوصيات والتحليلات الناتجة عن أنماط اختراقات محتملة، ومساعدة فرق الأمن السيبراني على عزل الأجهزة المُخرقة، وحظر حركة البيانات الضارة، وإيقاف البرامج الضارة من خلال مراقبة الأنظمة باستمرار.
- بالإضافة إلى ذلك، يُتنبأ بالمناطق عالية الخطورة التي يُحتمل حدوث اختراقات فيها، مما يُمكن المنظمات من معالجة نقاط الضعف بشكل استباقي قبل إثارة مخاوف جدية (Goodman,2025).
- **تحليل البيانات للتحقق من هوية المستخدمين:** وذكر Goodman أن أدوات الذكاء الاصطناعي تُساعد فرق الأمن السيبراني على تحليل بيانات مصادقة المستخدم، مثل بصمات الأصابع، وأنماط الكتابة، وأنماط الصوت. كما يُمكنها مراقبة سلوك المستخدم أثناء الجلسات، واكتشاف أي حالات شاذة، وتفعيل عمليات تحقق إضافية عند الحاجة.
- **تحديد هوية الهجمات لجهات تهديد محددة:** يمكن للذكاء الاصطناعي تحليل الأدوات المستخدمة، و بروتوكولات الإنترنت (Internet Protocols, IP) ، والأنماط السلوكية، وربط الحوادث بجهات تهديد معروفة، هذا يُسهّل على فرق الأمن فهم وتحديد مجموعات التهديد المحددة.
- **تحسين الكشف عن التصيد الاحتيالي والبريد العشوائي:** يساعد الذكاء الاصطناعي على فحص روابط البريد الإلكتروني والمرفقات والرسائل، مما يمنع محاولات التصيد الاحتيالي والبريد العشوائي قبل تفاقمها.

المبحث الثاني: إدارة مخاطر الأمن السيبراني والامتثال

◀ مفهوم الأمن السيبراني

عرّفت المادة رقم (2) من قانون الأمن السيبراني الأردني لسنة 2019 الأمن السيبراني بأنه "الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الاخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك".

وبمنظور أوسع؛ فالأمن السيبراني يشمل الاستراتيجيات، والعمليات والضوابط التي تطبقها المنظمات لحماية سرية، وسلامة وتوافر أصول المعلومات الخاصة بها، بالإضافة الى ما يشملها الفضاء السيبراني ككل؛ والذي يتضمن البنى التحتية السحابية، والمنصات المحمولة، والتقنيات التشغيلية وإنترنت الأشياء (The Internet of Things, IoT).

ويتمثل الهدف الأساسي للأمن السيبراني في إنشاء بيئة رقمية مرنة ومستقرة بحيث يمكن للعمليات الحيوية أن تستمر دون انقطاع حتى في أثناء مواجهة الهجمات السيبرانية، ولا يقتصر الأمن السيبراني على منع الهجمات فحسب؛ بل يشمل أيضًا

الكشف في الوقت المناسب، والاستجابة الفعالة والتعافي السريع من الحوادث السيبرانية. وبالتالي، يجب أن يكون الأمن السيبراني عملية مستمرة ومتكررة ومدمجة في كل جانب من جوانب عمليات المنظمة وهياكل الحوكمة. (David, Rajesh, 2025, P14).

كما يُعتبر الأمن السيبراني عنصراً أساسياً للحفاظ على سرية المعلومات وضمان استمرارية العمليات الحاسوبية والاتصالات المرتبطة بها (المصري، ٢٠٢٤). ولذلك، يُعد الأمن السيبراني ذا أهمية استراتيجية للمضي قدماً بثقة في العصر الرقمي. وتتمثل الأهداف العامة للأمن السيبراني فيما يلي: (Maleh & Maleh, 2022).

- التوافر : الذي يضمن وصول المستخدمين إلى أنظمة المعلومات.
- السلامة : التي تُحدد صحة البيانات.
- الإثبات : الذي يضمن عدم إنكار المعاملة مع إمكانية تدقيق النتائج المُقدمة.
- السرية : التي تمنع الوصول غير المقصود أو غير المشروع إلى المعلومات السرية.

◀ أنواع الهجمات السيبرانية

عرّف فريق منظمة الصحة العالمية (2024) الهجوم السيبراني بأنه "محاولة لإلحاق الضرر عمداً بشخص (مجموعة أشخاص) أو مؤسسة عن طريق شن هجوم على نظمهم الرقمية (مثل أجهزة الحاسوب) لسرقة البيانات أو التطبيقات التي يعتبرونها سرية و/أو يعتمدون عليها، أو العبث بتلك البيانات أو التطبيقات أو تعطيل الوصول إليها أو تدميرها، وتكون الهجمات السيبرانية أكثر شيوعاً عندما يمتلك الشخص أو المؤسسة نظاماً موصولة بالإنترنت".

حيث تشمل أنواع التهديدات السيبرانية أشكالاً، نذكر منها على سبيل المثال لا الحصر بعض هذه الأنواع كما هو مبين في الجدول رقم (1). (Shaheen & Jaiswal & Kumar, 2025).

جدول (1) أنواع التهديدات السيبرانية

❖ البرمجيات الخبيثة (Malware):
• الفيروسات (Viruses) : برمجيات خبيثة تنتشر من جهاز كمبيوتر إلى آخر، وتتسبب تلف الملفات أو البرامج.
• برامج الفدية (Ransomware) : برمجيات خبيثة تقوم بتشفير البيانات وتطلب دفع مبلغ مقابل مفتاح فك التشفير.
• أحصنة طروادة (Trojans): برامج ضارة مخفية على شكل برامج شرعية، وبمجرد تثبيتها، تسمح بالوصول غير المصرح به إلى النظام المصاب.
• برامج التجسس (Spyware): هي برامج تراقب وتجمع المعلومات سرّاً من مستخدم أو مؤسسة دون موافقتهم.
❖ التصيد الاحتيالي والهندسة الاجتماعية (Phishing and Social Engineering)
التصيد الاحتيالي (Phishing): يتلاعب المهاجمون بالأفراد للكشف عن معلومات حساسة مثل كلمات المرور، أو أرقام بطاقات الائتمان. من خلال رسائل بريد إلكتروني أو مكالمات هاتفية أو مواقع ويب مزيفة تبدو شرعية.
هجمات التستر (Pretexting): حيث ينشئ المهاجم سيناريو ملفقاً لسرقة معلومات الضحية،
الهجمات بالإغراء (Baiting): حيث يعرض المهاجم شيء مغرٍ لإقناع المستخدمين بتنزيل ملفات ضارة بهدف الاضرار ببيانات الضحية.
❖ أنواع أخرى من الهجمات السيبرانية:
➤ رفض الخدمة (Denial of Service, DoS) ورفض الخدمة الموزع (Distributed Denial of Service, DDoS): يهدف هجوم رفض الخدمة إلى إغراق نظام أو شبكة لدرجة أنه يصبح غير متاح للمستخدمين.

حيث تستخدم أجهزة متعددة لإغراق الهدف بحركة المرور، مما يجعل من الصعب تخفيفها.
➤ رجل في المنتصف (Man In The Middle, MITM): وهو هجوماً إلكترونيًا يسرق فيه أحد المخترقين معلومات حساسة عن طريق التنصت على الاتصالات بين هدفين عبر الإنترنت. (Lindemulder & Kosinski, 2024).
➤ البرمجة النصية عبر المواقع (Cross-Site Scripting, XSS): والتي تعني أن مهاجماً يقوم بتضمين نص JavaScript ضار لاستهداف قاعدة بيانات موقع الويب. أو من خلال هجمات الحقن (SQL Injection) ، في قاعدة البيانات بهدف عرض، أو تغيير أو حذف السجلات المخزنة في قاعدة بيانات المستهدفة.
➤ هجوم إنترنت الأشياء (IoT): هو محاولة خبيثة لاستغلال ثغرات أمنية في الأجهزة المتصلة بالإنترنت، مثل أجهزة المنازل الذكية، كاميرات المراقبة. وقد يسيطر المهاجمون على الجهاز بهدف سرقة بيانات حساسة أو تعطيل الخدمة بشكل كلي. (Amod, 2024).

◀ إدارة مخاطر الأمن السيبراني

عرّف شحاتة (2022) إدارة مخاطر الأمن السيبراني (Cybersecurity Risk Management, CRM) بأنها "مجموعة السياسات، والعمليات، والأساليب الرقابية المصممة لحماية المعلومات والأنظمة من الهجمات الإلكترونية والاختراق الأمني والتي قد تحد من إمكانية تحقيق نظام الأمن السيبراني لأهدافه المرجوة والمتمثلة في إتاحة المعلومات، والسرية وسلامة العمليات التشغيلية للمنظمة".

◀ منهجية إدارة مخاطر الأمن السيبراني

تهدف منهجية إدارة مخاطر الأمن السيبراني إلى تحديد مخاطر الأمن السيبراني الكامنة، وتقييم الأثر، والاحتمالية، وتحديد خطط التعامل مع هذه المخاطر بحيث يجري اتخاذ قرار التعامل وفقاً لذلك. ويجري استخدام الأصول، وثغرات الأمن السيبراني، وتهديدات الأمن السيبراني والضوابط كمدخلات محتملة لفهم مخاطر الأمن السيبراني ضمن هذه المنهجية (الهيئة الوطنية للأمن السيبراني، 2025). ويظهر الشكل (1) مراحل منهجية إدارة مخاطر الأمن السيبراني:

شكل (1): مراحل منهجية إدارة مخاطر الأمن السيبراني



المصدر: من تصميم الباحث

وتشمل المنهجية أيضاً الإجراءات اللازمة للتعامل مع المخاطر المحتملة، واستخدام أدوات ومعايير لقياس وتقييم الفعالية في إدارة المخاطر، بالإضافة إلى تحديد الأحداث المحتمل مواجهتها أثناء تطبيق استراتيجيات إدارة المخاطر في المنظمة (مركز إيداع الأوراق المالية، ب.ت)، وتتكون المنهجية من الخطوات التالية:

أولاً : مرحلة تحديد المخاطر (Risk Identification)

في هذه المرحلة، يجري حصر أصول الجهة، وتصنيفها، كما يجري تطوير سيناريوهات مخاطر الأمن السيبراني المتوقعة وفقاً لتهديدات الأمن السيبراني المحتملة، وثغرات الأمن السيبراني؛ وذلك بهدف تحديد مخاطر الأمن السيبراني الكامنة. كما يتم تحديد الضوابط المطبقة حالياً؛ لمعالجة سيناريوهات مخاطر الأمن السيبراني المتوقعة وتحديد المستوى المقبول من مخاطر الأمن السيبراني لدى المنظمة.

ثانياً: مرحلة تقييم المخاطر (Risk assessment)

يجري في هذه المرحلة تقييم مخاطر الأمن السيبراني، حسب سيناريوهات مخاطر الأمن السيبراني من خلال دراسة الاحتمالية والأثر.

ثالثاً: مرحلة معالجة المخاطر (Risk mitigation)

يتم في هذه المرحلة اتخاذ قرار التعامل مع مخاطر الأمن السيبراني، سواء كان ذلك بقبول تلك المخاطر (القبول)، أم (المشاركة)، أم (التخفيف) أم تجنب وقوعها (التجنب)، ومن ثم تحديد خطط التعامل مع المخاطر وتنفيذها. ويتم تحديث سجل مخاطر الأمن السيبراني؛ ليشمل خطط التعامل، ومخاطر الأمن السيبراني المتبقية.

رابعاً: مرحلة المتابعة والتقييم (Constant monitoring and Review)

يتم في هذه المرحلة متابعة أنشطة إدارة مخاطر الأمن السيبراني التي تقوم بها الجهة ومراقبتها، وتقييمها من خلال إدارة مخاطر الأمن السيبراني؛ ولتحديث سجل مخاطر الأمن السيبراني دورياً، أو بناءً على تغيرات المخاطر، أو تهديدات الأمن السيبراني، أو الضوابط التي يجري تطبيقها.

◀ مفهوم الامتثال للأمن السيبراني

يشير مفهوم الامتثال للأمن السيبراني الى عملية مستمرة من الالتزام بالمعايير، والقواعد، واللوائح وأفضل الممارسات المعمول بها لحماية البيانات الحساسة والحفاظ على سلامة أنظمة المعلومات الخاصة بها. Edwards & Weaver (2024).

كما يتضمن الامتثال للأمن السيبراني مواءمة بروتوكولات وعمليات أمن المنظمة مع المتطلبات التي تحددها الهيئات التنظيمية ومعايير المعتمدة والتفويضات القانونية. والهدف الأساسي من جهود الامتثال هذه هو تقليل المخاطر المرتبطة بالتهديدات السيبرانية وتعزيز الحوكمة. ف نطاق الامتثال للأمن السيبراني واسع ومتعدد الأوجه، ويشمل مجموعة واسعة من الأنشطة والسياسات والضوابط التي تساهم مجتمعة في بيئة معلومات آمنة. وغالباً ما تمتد هذه الأنشطة عبر مجالات مختلفة، بما في ذلك حماية البيانات، وأمن الشبكات، وحماية بيانات السحابة، وإدارة المخاطر، والاستجابة للحوادث، والحوكمة. حيث يحتوي كل مجال على متطلبات وإرشادات محددة يجب على المنظمات اتباعها لتحقيق الامتثال والحفاظ عليه. على سبيل المثال، قد تتضمن حماية البيانات تشفير البيانات الحساسة سواء كانت مخزنة أو أثناء نقلها، بينما قد يتطلب أمن الشبكات تنفيذ جدران حماية، وأنظمة كشف التسلل، وتقييمات منتظمة للثغرات الأمنية. (Cybellium, 2024).

◀ أطر الأمن السيبراني (Cybersecurity Standards and Frameworks)

معايير يمكن تعريف أطر ومعايير الأمن السيبراني بأنها مجموعة منظمة من السياسات والإرشادات وأفضل الممارسات المصممة لمساعدة المنظمات على إدارة مخاطر الأمن السيبراني والحد منها. وتوفر هذه الأطر خارطة طريق شاملة لتقييم

التحديات المحتملة ورصدها والتخفيف من حدتها. حيث تساعد هذه الأطر المنظمات على تنفيذ استراتيجية أمنية استباقية، وإدارة المتطلبات التنظيمية والعمليات. وتُمكن هذه الأطر والمعايير قادة الأمن - مثل مديري أمن المعلومات، وفرق إدارة المخاطر، وقيادات تكنولوجيا المعلومات - من تقييم وضعهم الأمني بفعالية، بالإضافة إلى حالة الموردين الخارجيين، مما يضمن اتباع نهج موحد للتخفيف من حدة التهديدات السيبرانية (Taherdoost, 2022). ويتضمن الجدول رقم (2) أبرز هذه الأطر والمعايير الدولية.

جدول رقم(2) - أبرز أطر عمل الأمن السيبراني

اسم الاطار	الغاية منه
إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا (NIST- CSF)	يُعَدّ (NIST-CSF) مجموعة مرنة من الإرشادات وأفضل الممارسات المُصممة لمساعدة المنظمات على تعزيز أمن معلوماتها وإدارة مخاطر الأمن السيبراني. (OLAES, TERRY, 2025).
المنظمة الدولية للمعايير ISO/IEC 27001& 27002	تُركز ISO-27001 على تطوير إطار إداري شامل، بينما تُقدّم ISO-27002 إرشادات حول تطبيق الضوابط. وتوفر هذه المعايير مجتمعةً إدارةً مُهيكلَةً للمخاطر تتماشى مع أهداف المنظمة (FADDOM, 2025).
حماية البنية التحتية الحيوية لشركة موثوقة الكهرباء في أمريكا الشمالية	تُوفر هذه الضوابط مجموعة من الإجراءات ذات الأولوية لحماية المؤسسات من المخاطر السيبرانية المعروفة. وتُقدّم هذه الضوابط إرشادات واضحة حول تنفيذ استراتيجيات الأمن، مع التركيز على المجالات الحيوية التي يُمكن أن تُحسّن بشكل كبير من دفاع المؤسسة السيبراني (Faddom, 2025).
أهداف السيطرة على تكنولوجيا المعلومات والتكنولوجيا الشبيهة	هو إطار عمل لإدارة تكنولوجيا المعلومات، ويُحدد الإطار العمليات والضوابط التي تُحسّن فعالية الحوكمة والإدارة. يُساعد COBIT المؤسسات على مواءمة أهداف تكنولوجيا المعلومات لديها مع الأهداف الاستراتيجية للأعمال، وإدارة المخاطر مع تحسين استخدام الموارد. (Faddom, 2025).
مصفوفة التحكم السحابي	وهي إطار عمل للتحكم في الأمن السيبراني للحوسبة السحابية. تُحدد هذه المصفوفة ضوابط أمنية خاصة بالسحابة، مما يُساعد مُقدّمي الخدمات والمستخدمين على تقييم مخاطر أمن السحابة وإدارتها. كما تُساعد المصفوفة المؤسسات على الامتثال للمتطلبات التنظيمية وإدارة

المخاطر في تطبيقات السحابة.(Faddom,2025).		
الغاية منه	اسم الاطار	
وهي إطار لتعزيز إجراءات وممارسات حماية البيانات لمواطني الاتحاد الأوروبي. وتشمل هذه اللائحة على جميع المؤسسات المنشأة في الاتحاد الأوروبي، أو أي شركة تجمع وتخزن البيانات الخاصة بمواطني الاتحاد الأوروبي (Faddom,2025).	General Data Protection (GDPR)(Regulation	إطار عمل اللائحة العامة لحماية البيانات
يُلزم هذا القانون باتباع نهج لتأمين معلومات الحكومة الأمريكية. ويُلزم الوكالات بتطوير وتوثيق وتنفيذ برنامج لأمن المعلومات، بما يتماشى مع أهداف الأمن القومي. ويعمل الامتثال لهذا المعيار على تحسين حماية البيانات الحكومية من خلال وضع معايير أمنية إلزامية (Faddom,2025).	The Federal Information Security Management Act (FISMA)	قانون إدارة أمن المعلومات الفيدرالي
هو إطار عمل للأمن السيبراني يُلزم مؤسسات الرعاية الصحية بتطبيق ضوابط لتأمين وحماية خصوصية المعلومات الصحية الإلكترونية (Pansy, 2024).	Health Insurance Portability and Accountability Act (HIPAA)	قانون نقل التأمين الصحي والمساءلة
هو إطار عمل يركز على ضمان إدارة مزودي الخدمات للبيانات بأمان لحماية خصوصية عملائهم (Faddom,2025).	System and Organization Controls 2 (SOC 2)	الامتثال لمعايير SOC 2
يوفر هذا المعيار ضمان الامتثال للوائح الرعاية الصحية المعقدة. كما توفير إرشادات لحماية السجلات الصحية الإلكترونية وإدارة خصوصية البيانات (Mulugeta, Henock, 2023).	Health Information Trust Alliance (HITRUST)	معايير تحالف ثقة المعلومات الصحية
هو معيار موحد لتطبيق الأمن السيبراني في جميع أنحاء قاعدة الصناعات الدفاعية. ويهدف إلى تأمين المعلومات غير السرية الخاضعة للرقابة (CUI) المشتركة بين المقاولين والمقاولين من الباطن في عقود الدفاع (Pansy, 2024).	Cybersecurity Maturity Model Certification (CMMC)	شهادة نموذج نضج الأمن السيبراني

◀ فوائد الامتثال لمعايير الأمن السيبراني

تعمل المنظمات على إنشاء أنظمة فعالة والتي تسعى من خلالها لحماية خصوصية بيانات عملائها بالرغم من تحملها تكاليف مادية أثناء قيامها بذلك، مع ذلك؛ تترك المنظمات الفوائد الجمة التي يمكن أن يقدمها الامتثال لأمن المعلومات وخاصة المتعلقة بالأمن السيبراني. وسنذكر أهم مزايا الامتثال للأمن السيبراني في المنظمات وعلى النحو التالي. (حمود، 2021):

- ❖ يُساعد المنظمة على تجنب الغرامات والعقوبات.
- ❖ يحمي سمعة المنظمة.
- ❖ يُعزز قدرات إدارة البيانات الخاصة بالمنظمة.
- ❖ يُحسن صورة المنظمة في بيئة شديدة المنافسة.
- ❖ يُعزز ثقافة المنظمة في أمن المعلومات.
- ❖ التوافق الأمني يدعم ضوابط الوصول والمساءلة.

◀ دور الذكاء الاصطناعي في تفادي الهجمات السيبرانية

أصبح الذكاء الاصطناعي مؤخراً وسيلة مهمة تُستخدم في مجال الأمن السيبراني. وقد بدأت معظم المنظمات باستخدام أنظمة الذكاء الاصطناعي للكشف عن الهجمات السيبرانية والوقاية منها، نتيجةً لتزايد حجم وتعقيد هذه التهديدات يومياً. حيث يكمن دور الذكاء الاصطناعي في صد هذه الهجمات بمايلي: (Rizvi, Mohammed, 2023).

❑ **الكشف عن التهديدات:** يمكن لأنظمة الذكاء الاصطناعي تحديد المخاطر المعروفة وغير المحددة باستخدام خوارزميات متطورة ونماذج التعلم الآلي (ML) التي تُحلل كميات كبيرة من البيانات وتحدد الأنماط التي تشير إلى وجود تهديد. كما يُستخدم التعلم العميق (DL) بهدف التعرف على البرامج الضارة، وعمليات التصيد الاحتيالي وغيرها من التهديدات الإلكترونية وتصنيفها. بالإضافة الى استخدام معالجة اللغة الطبيعية (NLP) لتحليل مصادر البيانات غير المنظمة، مثل مواقع التواصل الاجتماعي والمنديات الإلكترونية ومحتويات الروابط، لتحديد التهديدات المحتملة. كما يمكن لهذه النماذج استخراج المعلومات من البيانات النصية واستخدامها لتحسين دقة كشف التهديدات.

❑ **منع التهديدات:** يمكن لأنظمة الذكاء الاصطناعي تحديد التهديدات السيبرانية المحتملة واتخاذ تدابير استباقية لمنعها والحد من التسبب بأضرار جسيمة. فيما يلي بعض الأمثلة على كيفية استخدام الذكاء الاصطناعي لمواجهة التهديدات:

❑ **منع التطفل (Intrusion Prevention):** يمكن لأنظمة منع التطفل القائمة على الذكاء الاصطناعي اكتشاف عمليات التطفل وإيقافها قبل دخولها إلى الشبكة.

❑ **منع البرامج الضارة (Malware Prevention):** يمكن لأنظمة مكافحة البرامج الضارة القائمة على الذكاء الاصطناعي اكتشاف ومنع تثبيت البرامج الضارة.

❑ **منع التصيد الاحتيالي (Phishing Prevention):** يمكن لأنظمة مكافحة التصيد الاحتيالي القائمة على الذكاء الاصطناعي اكتشاف هجمات التصيد الاحتيالي ومنعها من خلال تحليل رسائل البريد الإلكتروني وتحديد المحتوى المشبوه.

❑ **تقييم الثغرات الأمنية (Vulnerability Assessment):** يمكن لأنظمة تقييم الثغرات الأمنية القائمة على الذكاء

الاصطناعي تحديد نقاط الضعف في الشبكة واتخاذ تدابير استباقية للتخفيف منها.

□ **التحكم في الوصول (Access Control):** يمكن لأنظمة التحكم في الوصول القائمة على الذكاء الاصطناعي تحديد التهديدات المحتملة ورفض الوصول للمستخدمين غير المصرح لهم.

◀ دور الذكاء الاصطناعي في الامتثال لإدارة مخاطر الأمن السيبراني

تعتمد المنظمات عادةً على الأساليب اليدوية لمراجعة عملية الامتثال للوائح التنظيمية، ولكنها قد تستغرق وقتًا طويلاً، وتتطلب كميات هائلة من العمل، واحتمالات عالية للأخطاء. لذلك، يتطلب الامتثال للأمن السيبراني مراجعة شاملة. وتوجد في الاتحاد الأوروبي والولايات المتحدة الأمريكية مجموعة أطر وقواعد تتعلق باستخدام الذكاء الاصطناعي لأغراض الامتثال. توضح النقاط التالية كيف يمكن للذكاء الاصطناعي أن يسهم بشكل كبير في الامتثال (Koneru, 2024):

- **الامتة في تقييم مخاطر الأمن السيبراني:** تستخدم المنظمات بشكل متزايد خوارزميات الذكاء الاصطناعي لتقييم المخاطر تلقائياً، مما يقلل من التدخل البشري. ويُعد الذكاء الاصطناعي أكثر كفاءةً من البشر في تقييم المخاطر، بما في ذلك تلك التي قد تتداخل مع عمليات التحقق من الثغرات الأمنية والامتثال وإدارة أنظمة المعلومات. يمكن لأدوات مثل (User Entity Behavior Analytics, UEBA) وهي أداة لتحليل سلوك المستخدم تهدف إلى تحديد الحالات غير المقبولة ومساعدة فرق الأمن على التركيز على معالجة نقاط الضعف وزيادة دقة تقييم المخاطر.
- **المراقبة المستمرة والامتثال:** تتمتع تقنيات الذكاء الاصطناعي المتمثلة بخوارزميات التعلم الآلي القدرة على تحليل البيانات الضخمة، واكتشاف الانحرافات، حتى أنه يُحدد الحالات غير المقبولة وبكفاءة أعلى. و يساعد الذكاء الاصطناعي الإبلاغ الفوري عن النتائج التي يمكن أن تساعد بشكل كبير الامتثال باللوائح التنظيمية، وبالتالي تحسين الوضع الأمني للمنظمة. كما تضمن نماذج الذكاء الاصطناعي الدقة والتعرف السريع على المخاطر، وتضمن الامتثال الاستباقي من خلال استخدام الأنماط التاريخية للمساعدة في بناء دفاعات قوية للأمن السيبراني.
- **الاستجابة للحوادث المدعومة بالذكاء الاصطناعي:** يعزز هذا النهج التعامل مع حوادث الأمن السيبراني من خلال استخدام تقنيات حديثة مثل الامتة والتعلم الآلي. وبالتالي، فإنه يتيح الكشف عن التهديدات في الوقت الفعلي، مما يساعد فرق الأمن السيبراني على التحليل السريع واعتماد استراتيجيات التخفيف. يتيح الاستخدام الفعال للبيانات التاريخية للذكاء الاصطناعي الاستجابة للحوادث بشكل أسرع مع كشف أكثر دقة.
- **تجاوز التعقيدات التنظيمية:** تساعد التقنيات المدعومة بالذكاء الاصطناعي المنظمات على الالتزام بالقانون. تُبسّط معالجة اللغة الوطنية (NLP) تفسير المفردات القانونية المعقدة، وتساعد على استخراج البيانات ذات الصلة، وتضمن امتثال المنظمات. كما تُسهّل عملية الامتثال التنظيمي بجعلها أكثر كفاءة وسرعةً. وتُصبح هذه القدرة ضروريةً لتطبيق لوائح مرنة مثل اللائحة العامة لحماية البيانات (GDPR) وقانون نقل التأمين الصحي والمساءلة (HIPAA) وأطر الأمن السيبراني، وذكر Adeel, S. M (2025) أنه يتم تحويل نصوص الامتثال إلى نصوص قابلة للقراءة آلياً؛ وذلك بهدف المساعدة على فهم نموذج الذكاء الاصطناعي وتطبيقه تلقائياً. حيث يُمكن لمكاتب التحقق من لوائح الامتثال المحددة بشكل متكرر دون الحاجة إلى إشراف دقيق، مما يُقلل من الأخطاء البشرية، وبالتالي يُؤثر ذلك إيجاباً على أداء المنظمة.
- **الامتثال التنبؤي:** تُساعد أدوات الذكاء الاصطناعي المعتمدة على التعلم الآلي (ML) في التنبؤ بالهجوم الإلكتروني أو الحادث بناءً على أنماط استخدام البيانات المتاحة، مما يُساعد على اتخاذ إجراءات استباقية قبل فوات الأوان، ويُساعد على تحقيق أعلى مستوى من الامتثال. (Folorunso et al. 2024,b)

◀ تأثير الذكاء الاصطناعي في عمليات الامتثال لمتطلبات الأمن السيبراني

تشير دراسة (Mbonigaba Celestin, et al. (2025) بأن قطاع التكنولوجيا في الهند قد أصبح يعتمد على الذكاء الاصطناعي في عمليات الامتثال لمتطلبات أمن المعلومات وذلك من العام 2020 إلى عام 2024 وبنسبة وصلت الى 85%. كما تشير نتائج هذه الدراسة أيضًا إلى أن هذه الشركات تُعطي الأولوية لحلول الامتثال القائمة على الذكاء الاصطناعي للحد من المخاطر وتعزيز الحوكمة. وأن الامتثال المعتمد على الذكاء الاصطناعي قد حسن كفاءة حوكمة الشركات من 59.2% إلى 73.6%، وخفض حالات فشل الامتثال بنسبة 37%، وخفض التكاليف القانونية بنسبة 95.0%. بحسب Mbonigaba يلخص الجدول (2) تقنيات الذكاء الاصطناعي الأساسية التي تستخدمها الشركات لأتمتة عمليات الامتثال وتخفيف المخاطر باستخدام الذكاء الاصطناعي:

جدول رقم (2) – استخدام تقنيات الذكاء الاصطناعي لأتمتة عمليات الامتثال وتخفيف المخاطر

تقنيات الذكاء الاصطناعي	2023 (%)	2024 (%)
لغة الآلة (ML)	70	80
معالجة اللغة الطبيعية (NLP)	60	70
أتمتة العمليات الروبوتية (RPA, Robotic Process Automation)	40	50
التحليلات التنبؤية (Predictive Analytics)	45	55

كما يظهر الجدول (3) تأثير تقنيات الذكاء الاصطناعي على إدارة المخاطر (Mbonigaba Celestin, et al. (2025):

جدول رقم (3) – تأثير تقنيات الذكاء الاصطناعي على إدارة المخاطر

تطبيق الذكاء الاصطناعي	التأثير على إدارة المخاطر	النتيجة الإحصائية
لغة الآلة (ML)	الكشف التلقائي عن الانحرافات	انخفاض حوادث الامتثال بنسبة 30%
معالجة اللغة الطبيعية (NLP)	تحليل النصوص التنظيمية	توفير 52% من الوقت في التحليل
التحليلات التنبؤية (Predictive Analytics)	التنبؤ بالاختراقات الأمنية المحتملة	زيادة في الكشف المبكر عن التهديدات بنسبة 35%.
مراقبة الامتثال الآلية	ضمان الالتزام بالمعايير	انخفاض بنسبة 25% في انتهاكات الامتثال.
استخبارات التهديدات في الوقت الفعلي	تصورات فورية حول التهديدات الناشئة	قدرات استجابة أسرع بنسبة 40%.
التحليل السلوكي	الكشف عن أنشطة المستخدم غير القانونية	انخفاض التهديدات الداخلية بنسبة 50%

قد ذكر (Crudu, Vasile & Mold Stud Team (2025) مجموعة من المؤشرات التي تثبت تأثير اعتماد ودمج تقنيات الذكاء الاصطناعي في إدارة الامتثال لإدارة المخاطر الأمن السيبراني وعلى النحو التالي:

- يمكن لأطر الامتثال الاستفادة من تقنيات الذكاء الاصطناعي، فالأدوات المصممة لتحليل المتطلبات التنظيمية تساعد المؤسسات على موازنة ممارساتها مع معايير تنظيمية كاللائحة العامة لحماية البيانات (GDPR) وقانون التأمين الصحي والمساءلة (HIPAA). حيث تشير التقارير إلى أن الشركات التي تتبنى أدوات الذكاء الاصطناعي هذه توفر ما يصل إلى 30% من تكاليف الامتثال. علاوة على ذلك، يمكن لأتمتة عمليات إعداد التقارير أن تعزز النزاهة والشفافية، وبالتالي توطد ثقة أصحاب المصلحة.

- كما تشير الأبحاث إلى أن حلول الذكاء الاصطناعي قد قلّصت وقت اكتشاف المخاطر بنسبة تصل إلى 50%، مما يُمكن المنظمات من الاستجابة السريعة للتهديدات المحتملة.

- تطبيق المراقبة المستمرة من خلال خوارزميات الذكاء الاصطناعي التي تُحدد المخالفات فوراً. حيث تشهد المنظمات التي تستخدم الذكاء الاصطناعي للمراقبة المستمرة للامتثال انخفاضاً بنسبة 40% في حوادث عدم الامتثال. هذا الموقف الاستباقي يُمكن أن يمنع العقوبات الباهظة الناتجة من عدم الامتثال والضرر الذي يُلحق الضرر بسمعة هذه المنظمات.

- استخدام تقنيات التعلم الآلي (ML) للمساعدة في إنفاذ السياسات. من خلال تحليل بيانات الامتثال التاريخية، حيث يُمكن للذكاء الاصطناعي اقتراح تعديلات على الممارسات الحالية لمواءمتها بشكل أفضل مع المتطلبات المتطورة. وهذا يضمن إطار عمل ديناميكي للامتثال. وتُظهر الإحصائيات أن الشركات التي تُحدّث إجراءات الامتثال بانتظام تشهد زيادة بنسبة 30% في معدلات الالتزام.

- يُمكن لأنظمة الذكاء الاصطناعي فرض ضوابط الوصول من خلال التعرف على أنماط سلوك المستخدم، مما يُقلل في النهاية من التهديدات الداخلية. وقد تبين أن المنظمات التي تُطبق هذه الإجراءات بانخفاض بنسبة 25% في خروقات البيانات المُعزاة إلى أفعال داخلية.

- إعطاء الأولوية لتدريب الموظفين على أدوات الذكاء الاصطناعي للاستفادة من أقصى إمكاناتهم في مهام الامتثال والذي يُعزز من الفعالية الإجمالية. وتكشف الدراسات أن برامج التدريب تزيد معدلات نجاح الامتثال بنسبة 35% عند دمجها مع تحسينات الذكاء الاصطناعي.

- يمكن لتقنيات الذكاء الاصطناعي تعزيز الرقابة والرصد، مما يقلل من انتهاكات الامتثال. وقد أدى اعتماد برامج الامتثال الآلية إلى انخفاض حوادث عدم الامتثال بنسبة 30% للمنظمات التي تدمج هذه تقنيات الذكاء الاصطناعي. ينبغي على المتخصصين النظر في الاستفادة من خوارزميات التعلم الآلي لتحليل أنماط الوصول إلى البيانات واستخدامها، وتحديد السلوكيات الشاذة بفعالية.

- يمكن أن يؤدي دمج الذكاء الاصطناعي في برامج تدريب الموظفين إلى رفع مستوى الوعي بقضايا الامتثال. وتوفر التحليلات القائمة على الذكاء الاصطناعي وحدات تدريبية مخصصة بناءً على مقاييس الأداء الفردية، مما قد يؤدي إلى زيادة في الاحتفاظ بالمعرفة لدى الموظفين بنسبة 20%.

أبرز تحديات الأمن السيبراني في عصر الذكاء الاصطناعي:

باستقراء الأدبيات (بكه، 2025، ب، الصياد، والسالم، 2023، مركز الإمارات للدراسات والبحوث الاستراتيجية، 2024، فضل الله، 2025، كامل، عبد الرحمن، 2025)، وبالرغم من الفوائد المتعددة التي يحققها استخدام الذكاء الاصطناعي في مجال الأمن السيبراني، فقد حددت هذه الدراسات مجموعة من المخاطر والتحديات؛ والتي يمكن تلخيصها مايلي:

- ❖ **التحيز في صنع القرار:** في حال استخدام أنظمة الذكاء الاصطناعي القائمة على مجموعات البيانات التي تحتوي على معلومات أو خوارزميات متحيزة في مجال الأمن السيبراني؛ فقد يؤدي ذلك إلى قرارات تمييزية ضد جماعات أو أفراد معينين وأن تكون لها عواقب وخيمة على المنظمة.
- ❖ **الافتقار إلى القابلية للتفسير والشفافية:** تتسم الخوارزميات المستخدمة لاتخاذ قرارات بشأن التهديدات الأمنية بعدم الشفافية في كثير من الأوقات، وهو ما يصعب من تفسير قرارات الذكاء الاصطناعي السيئة ويُفقد القدرة على تحسينها، وبالتالي يتأثر أمن المنظمة بالسلب.
- ❖ **إساءة استخدام الذكاء الاصطناعي:** قد يضر الذكاء الاصطناعي بالأمن السيبراني عندما يُستخدم في أغراض ضارة مثل إنشاء أخبار مزيفة، أو نشر دعاية سلبية يستفاد منها في اختراق امني أو سرقة بيانات للعملاء.
- ❖ **الكلفة المالية العالية:** ان التكلفة الباهظة لتقنيات الذكاء الاصطناعي، ومحدودية معرفة الشركات الصغيرة والمتوسطة بإمكانيات الذكاء الاصطناعي يُشكل تحدياً مهماً يلزم هذه الشركات بالعمل على تجاوزه من خلال مواكبة التهديدات التي قد تؤثر على سمعة الشركة وتحد من تطورها في ظل منافسة شديدة.
- ❖ **انتهاك خصوصية البيانات:** هناك العديد من المخاوف فيما يتعلق بموضوع خصوصية البيانات التي تعالجها وتحللها تطبيقات الذكاء الاصطناعي في الأمن، إذ أن تلك التطبيقات والخوارزميات قادرة على التعرف على البيانات، وهو ما يفرض ضرورة الامتثال للوائح الخصوصية من خلال الفحص القانوني قبل نشر أنظمة الذكاء الاصطناعي.

الخاتمة

في ختام هذه الدراسة، فقد تم عرض نظرة شاملة على دور تقنيات الذكاء الاصطناعي في تحسين إدارة مخاطر الأمن السيبراني والامتثال. وسلطت الضوء على التهديدات السيبرانية، وأهمية وجود تقنيات ذكية لمواجهتها. كما أكدت الدراسة على الدور الحاسم لإدارة المخاطر السيبرانية المبنية على أطر ومعايير معتمدة في التخفيف من حدة التهديدات السيبرانية ومواجهة التحديات التي قد تواجه تطبيقها في المنظمة.

أولاً: نتائج الدراسة

من خلال استعراض الدراسات السابقة ومعرفة أهدافها والنتائج التي توصلت إليه ومقارنة نقاط التشابه الاختلاف بينهم وبين الدراسة الحالية، وتوصلت الدراسة إلي مجموعة من النتائج:

1. أظهرت نتائج الدراسة الى أن الذكاء الاصطناعي (AI) يُحسن من القدرات الفنية والادارية لكشف التهديدات السيبرانية، والاستجابة للحوادث و الامتثال للوائح التنظيمية مثل اللائحة العامة لحماية البيانات (GDPR)، وقانون التأمين الصحي والمساءلة (HIPAA) وغيرها من الأطر والمعايير الدولية أو المحلية، والتي تشكل عصب الدفاعات السيبرانية الحديثة والدرع الاستباقي الذي يُمكنه التنبؤ بالهجمات قبل وقوعها، وتحليلها بشكل فوري، والتصدي لها بفعالية بهدف تحسين وضعها الأمني.
2. كما أظهرت الدراسة أهمية دمج الذكاء الاصطناعي في الامتثال التنظيمي والذي يُمثل فرصة جيدة لتعزيز الأمن السيبراني، وتبسيط عمليات الامتثال، ودعم مرونة المنظمات في بيئة رقمية متزايدة التعقيد.
3. أظهرت الدراسة أيضاً دور تقنيات الذكاء الاصطناعي بأنواعه المختلفة - كالتعلم الآلي (ML)، ومعالجة اللغة الطبيعية (NLP)، والتحليلات التنبؤية (Predictive Analytics) - تقدماً كبيراً في الكشف المبكر عن التهديدات

السيبرانية، وتحليل سلوك الشبكات بشكل آني، بما يسهم في سرعة الاستجابة للهجمات المتطورة، وتصنيف البرامج الضارة، ومنع هجمات التصيد الاحتيالي، نظرًا لقدرتهما الكبيرة على معالجة كميات هائلة من البيانات، واكتشاف الأنماط، ومراعاة ديناميكية التهديدات.

4. توصلت الدراسة الى وجود عدد من التحديات والمخاطر التي قد تواجه هذا استخدام الذكاء الاصطناعي في مواجهة الهجمات السيبرانية، وأنه من الأهمية بمكان مواجهة هذه التحديات من خلال تعزيز الرقابة السيبرانية الذكية والبشرية على نشاطات الذكاء الاصطناعي بهدف تعظيم الفائدة المرجوة من هذه التقنيات.

ثانياً: التوصيات

في ضوء النتائج التي تم التوصل إليها من خلال الدراسة النظرية، يوصى الباحث بما يلي:

1. أن تقوم المنظمات بتعزيز أطر الأمن السيبراني لحماية البيانات القانونية الحساسة، وتطبيق التشفير، وكشف التهديدات المدعومة بالذكاء الاصطناعي، وضوابط الوصول الصارمة للبنية التحتية الرقمية.
2. اعتماد نهج امتثال متطور يدمج أسلوب أئمة مراحل الامتثال لإدارة مخاطر الأمن السيبراني باستخدام الذكاء الاصطناعي مع دور العامل البشري، وذلك لضمان الحوكمة الأخلاقية، واتخاذ قرارات نزيهة، والبعد عن التحيز ضد جماعات أو أفراد معينين.
3. أن تقوم المنظمات بمواكبة أحدث التطورات في مجال الذكاء الاصطناعي والتقنيات المرتبطة بإدارة مخاطر الأمن السيبراني والامتثال. فمع استمرار تطور تقنيات الذكاء الاصطناعي تتطور معها التهديدات. والذي يفرض على المنظمات البقاء في طليعة التطور لحماية نفسها.
4. تطوير الكفايات والقدرات من خلال عقد برامج تدريبية متخصصة بالتعاون مع مراكز الأبحاث، والهيئات المحلية والدولية والجامعات والتي تعنى بتقنيات الذكاء الاصطناعي، ونشر الوعي السيبراني للأفراد والمنظمات من خلال نشاطات لانهجية كإطلاق مسابقات وطنية، وتنظيم "فعاليات هاكاثون" متخصصة لتحفيز المبتكرين في مجالات الأمن السيبراني والذكاء الاصطناعي.
5. تعزيز الشراكة بين القطاعين العام والخاص، والتعاون مع المنظمات الدولية من خلال تبادل البيانات حول تهديدات ومخاطر الأمن السيبراني.
6. العمل بجاء من قبل المنظمات لمواكبة أحدث التقنيات في مجال الذكاء الاصطناعي والأمن السيبراني. فمع استمرار تطور تقنية الذكاء الاصطناعي، تتطور معها وبالتوازي التهديدات التي تُشكلها والفرص التي يمكن الاستفادة منها.
7. إجراء المزيد من الأبحاث لتقييم أثر الذكاء الاصطناعي على الأمن السيبراني.

المراجع العلمية

❖ المراجع العربية :

- البلقاسي، منال. (2025). التعليم المستدام في ظل الذكاء الاصطناعي. دار الثقافة الروسية للنشر (القاهرة)، دار عقل للنشر (دمشق). ط(1)، مجلد(1).
- الهيئة الوطنية للأمن السيبراني. (2025). الإطار الوطني لإدارة مخاطر الأمن السيبراني. (NFCRM-1:2025). المملكة العربية السعودية. تم الاسترجاع من الرابط: <https://nca.gov.sa/ar/public-consultations>.
- بكه. (5 يناير، 2025، ب). الذكاء الاصطناعي والأمن السيبراني: العلاقة والفرق بينهما وتحدياتهما. تم الاسترجاع من الرابط: <https://2u.pw/RPYaIYxA>.
- توفيق، احمد. (2025). العلاقة بين اختراقات الأمن السيبراني والافصاح عنها وقرار الاستثمار في الشركات المصرية والدور المعدل للإفصاح عن إدارة مخاطر الأمن السيبراني -دراسة تجريبية. المجلة العلمية للبحوث التجارية (جامعة المنوفية)، 57(2)، 902-851. Doi: 10.21608/sjsc.2025.370124.1576.
- حسان، ساره. (يونيو 1، 2025). علم الآلة Machine Learning - مفتاح التطور التكنولوجي. أكاديمية ابن سينا. تم الاسترجاع بتاريخ (10 يوليو، 2025)، الرابط: <https://2u.pw/LFT6b>.
- فضل الله، هيثم. (2025). دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني دراسة تحليلية للتحديات والحلول المستقبلية. المجلة المصرية للدراسات المتخصصة. 13. 1362-1341. ejos.2025.422622/10.21608.
- كامل، عبد الرحمن. (2025). استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة: تحليل الممارسات الدولية واستشراف التحديات المستقبلية. المجلة العربية للدراسات الأمنية، 41(1)، 16-04. <https://doi.org/10.26735/CXSD7939>.
- مركز إيداع الأوراق المالية. (ب.ت). إدارة المخاطر. تم الاسترجاع بتاريخ (23 آب، 2025)، تم الاسترجاع من الرابط: <https://www.sdc.com.jo/ar/risk-management#ui-id-7>. الأردن.
- المصري، فرح. (2024). دور الذكاء الاصطناعي في تحسين الأمن السيبراني. مجلة النخبة للدراسات والأبحاث، 3(2). التير، فاطمة علي وآخرون. (2024). استخدام الشبكات العصبية الاصطناعية في التنبؤ بمبيعات مصنع اسمنت زليتن. المجلة الأفروآسيوية للبحث العلمي (AAJSR). 2(4). 264-275. تم الاسترجاع من الرابط: <https://aajsr.com/index.php/aajsr/article/view/282>.
- فريق منظمة الصحة العالمية. (6 فبراير، 2024). الهجمات السيبرانية على البنية التحتية الصحية. تم الاسترجاع من الرابط: <https://www.who.int/ar/news-room/questions-and-answers/item/cyber-attacks-on-critical-health-infrastructure>.
- محسن، لمياء. (2024) مجالات الذكاء الاصطناعي (تطبيقات وأخلاقيات). العربي للنشر والتوزيع. ط(1)، مجلد (1).
- مركز الإمارات للدراسات والبحوث الاستراتيجية. (2024). تقرير الذكاء الاصطناعي في عام 2024: الاتجاهات والتحديات. تم الاسترجاع من الرابط: <https://2u.pw/AFkX9>.

- الشرقاوي، ماجد أبو النجا. (2023). الأبعاد الاقتصادية للذكاء الاصطناعي - تقييم جاهزية الاقتصاد المصري. مجلة الدراسات القانونية والاقتصادية، 9(1)، 283-283. doi: 10.21608/jdl.2023.192966.1119.357-283.
- الصيد، مي؛ والسالم، وفاء. (2023). دور الذكاء الاصطناعي في تطوير مهارات البحث العلمي لدى طالبات كلية التربية بجامعة الملك سعود، مجلة البحوث التربوية والنوعية. (19)، (247-288).
- شحاتة، شحاتة السيد. (2022). نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية. المجلة العلمية للدراسات والبحوث المالية والإدارية، مج13، ع2، 26 - 37. مسترجع من: <http://search.mandumah.com/Record/1290731>
- قاسم، زينب و رشوان، عبد الرحمن. (2022). أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك. المؤتمر العلمي الدولي الأول بعنوان "أثر الأمن السيبراني على الأمن الوطني". خلال الفترة 21-20 ديسمبر/2022، جامعة عمان العربية بالاشتراك مع مديرية الأمن العام، الأردن.
- حمود، رؤى. (November 25, 2021). ست مزايا خفية يقدمها الامتثال لمعايير الأمن السيبراني لمنظمتك. تم الاسترجاع من الرابط: <https://short-link.me/18dVv>.
- الزيود، احمد. (2020). ادارة مخاطر الأمن السيبراني في البنوك الأردنية. مجلة الألفية للعلوم الاقتصادية والإدارية، مجلد 1 (1) . <https://doi.org/10.47340/MJEAS.V11i.2.2020>
- قانون الأمن السيبراني الأردني رقم (16) لسنة 2019.

❖ المراجع الاجنبية:

- Aror, Tina Akpevben and Mupa, Munashe Naphtali. (2025). "Risk and compliance paper what role does Artificial Intelligence (AI) play in enhancing risk management practices in corporations?" .World Journal of Advanced Research and Reviews. 27(01), 1072-1080. Article DOI: <https://doi.org/10.30574/wjarr.2025.27.1.2607>.
- Adeel, S. M. (2025). Ai-Powered Cybersecurity Compliance: Bridging Regulations and Innovation. Journal of Current Trends in Computer Science Research, 4(3), 01-23. DOI: 10.33140/JCTCSR.
- Barone, Ryan. (n.d). what is NLP (Natural Language Processing) in Cybersecurity? Retrieved on (August 18, 2025), by URL: <https://bolster.ai/glossary/nlp-in-cybersecurity>.
- Chettier, Thiyagarajan Mani and Boyina, Venkata Ashok Kumar and Rangineni, Sandeep. (2025). AI-Powered Risk Assessment and Compliance in Cloud Cybersecurity, International Journal of Computer Trends and Technology (IJCTT). vol. 73, no. 3, pp. 57-63, 2025. Crossref, <https://doi.org/10.14445/22312803/IJCTT-V73I3P107>.
- Crudu, Vasile & MoldStud Team. (21 July, 2025).The Role of AI in Cybersecurity Regulations and Compliance - Insights for Specialists. Retrieved by URL <https://moldstud.com/articles/p-the-role-of-ai-in-cybersecurity-regulations-and-compliance-insights-for-specialists>.
- David, Rajesh. (2025). Cyber security Risk Management and Compliance for Modern Enterprises. Zenodo. v1. <https://doi.org/10.5281/zenodo.15322509>.

- Faddom. (January 13, 2025). Top 10 Cybersecurity Frameworks to Know in 2025. Retrieved from URL: <https://faddom.com/top-10-cybersecurity-frameworks-to-know-in-2025>.
- Graham, Kaitlyn. (January 06, 2025). What is Cybersecurity Compliance? List of Compliance Regulations by Industry. Available at: <https://www.bitsight.com/blog/what-is-cybersecurity-compliance>.
- Goodman, Courtney. (January 16, 2025). AI in Cybersecurity: Transforming Threat Detection and Prevention. Retrieved by: <https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity>.
- Mehmood et al. (2025). Cyber security Governance as a Pillar of Enterprise Risk Management: Designing a Compliance-Driven Framework for Operational Resilience, Policy Enforcement, and Regulatory Alignment. Annual Methodological Archive Research Review, 3(5), 59-77. <https://doi.org/10.63075/0jv35d33>.
- Mbonigaba Celestin, et al. (2025). The Future of AI-Driven Legal Compliance: How Artificial Intelligence is Enhancing Corporate Governance and Regulatory Adherence, International Journal of Current Research and Modern Education, Volume 10, Issue 1, Page Number 26-36.
- Olaes, Terry. (January 17, 2025). What is the NIST Cybersecurity (CSF) 2.0 Framework. Retrieved from URL: <https://www.balbix.com/insights/nist-cybersecurity-framework>.
- Shaikh Muhammad, Adeel. (January 31, 2025). AI-Powered Cybersecurity Compliance: Bridging Regulations and Innovation. TechRxiv. DOI: 10.36227/techrxiv.173835413.30326598/v1.
- Shaheen Nusrat & Jaiswal, Sunny & Kumar, Mandeep. (2025). Cyber Security Strategies: Protecting Digital Assets in a Rapidly Evolving Threat Landscape. DeepMisti Publication.
- Amod, Farah. (July 30, 2024). What are Internet of Things (IoT) attacks? <https://www.paubox.com/blog/what-are-internet-of-things-iot-attacks>.
- Cybellium. (2024). Cybersecurity Compliance: A Study Guide: A Comprehensive Guide to Learn Cybersecurity Compliance. Kindle Edition. Limited Edition.
- Edwards, Jason & Weaver, Griffin. (2024). The Cybersecurity guide to governance, risk, and compliance. John Wiley & Sons. 1st Edition. DOI: 10.1002/9781394250226.
- Folorunso, et al. (2024, a). A governance framework model for cloud computing: role of AI, security, compliance, and management. World Journal of Advanced Research and Reviews. 24. 1969-1982. 10.30574/wjarr.2024.24.2.3513.
- Folorunso et al. (2024, b). Impact of AI on Cybersecurity and security compliance. Global Journal of Engineering and Technology Advances, 21(01), 167–184. 10.30574/gjeta.2024.21.1.0193.
- Koneru, Gagan. (August 5, 2024). The Future of Cybersecurity Compliance: How AI is leading the Way. (Retrieved by URL: <https://cloudsecurityalliance.org/blog/2024/08/05/the-future-of-cybersecurity-compliance-how-ai-is-leading-the-way>).
- Lindemulder, Gregg & Kosinski, Matthew. (11 June 2024). "What is a man-in-the-middle (MITM) attack?" Retrieved by: <https://www.ibm.com/think/topics/man-in-the-middle>.
- Pansy. (Dec 06, 2024). "13 Cybersecurity Standards You Must Know (Industry-Specific)". Retrieved by URL: <https://sprinto.com/blog/cybersecurity-standards>.
- Dapel et al. (2023). Artificial Intelligence Techniques in Cybersecurity Management. In:

- Jahankhani, H. (Eds) Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-20160-8_14.
- Mulugeta, Henock. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. Risks. 11. 10.3390/risks11060101.
- Mohammed, A. (2023). Elevating Cybersecurity Audits: How AI is Shaping Compliance and Threat Detection. Aitoz Multidisciplinary Review, 2(1), 35-43.
- Rizvi, Mohammed. (2023). enhancing Cybersecurity: The power of artificial intelligence in threat detection and prevention. International Journal of Advanced Engineering Research and Science (IJAERS). Vol-10, Issue-5.
- Sharma et al. (2023). Use of Fuzzy Logic in Cyber Security System: Cyber Threat Intelligence. International Journal of Students' Research in Technology & Management, 11(3), 10–19. <https://doi.org/10.18510/ijstrtm.2023.1133>.
- Veena. P. (2023). Artificial Intelligence and Expert System. Journal of Computer Engineering (IOSR-JCE). PP 01-09.
- Maleh, Y., Maleh, Y. (2022). Understanding Cybersecurity Standards. In: Cybersecurity in Morocco. Springer Briefs in Cybersecurity. Springer, Cham. https://doi.org/10.1007/978-3-031-18475-8_2.
- Taherdoost, H. (2022). Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview. Electronics, 11, 2181. <https://doi.org/10.3390/electronics11142181>.

عنوان البحث

أثر تطبيق وظائف إدارة الموارد البشرية على أداء العاملين بالتطبيق على المستشفيات العامة بولاية الخرطوم.

د. محمد علي حسن الطاهر¹ د. اسماعيل محمد عبد الجليل² د. حاتم عثمان ادم اسماعيل³

¹ أستاذ مساعد - جامعة قاردين سيتي. السودان

² أستاذ مساعد - جامعة وادي النيل. السودان

³ أستاذ مساعد - أكاديمية العلوم الهندسية والطبية السودان

HNSJ, 2022, 3(3); <https://doi.org/10.53796/hnsj3318>

تاريخ القبول: 2022/02/23م

تاريخ النشر: 2022/03/01م

المستخلص

تناولت الدراسة أثر تطبيق وظائف إدارة الموارد البشرية على أداء العاملين. هدفت الدراسة للتعرف على أثر تطبيق وظائف إدارة الموارد البشرية على أداء العاملين، استخدم الباحث المنهج الوصفي التحليلي ومنهج دراسة الحالة، واستنتجت الدراسة علاقة بين استراتيجيات الموارد البشرية وأداء العاملين دعمت جزئياً، أوصت الدراسة بضرورة بوضع مرتبات و أجور تنافسية بالمقارنة مع المستشفيات الأخرى ووضع حوافز مادية ومعنوية مناسبة لتشجيع العاملين.

الكلمات المفتاحية: إدارة الموارد البشرية، أداء العاملين.

RESEARCH TITLE**THE IMPACT OF APPLYING THE FUNCTIONS OF HUMAN RESOURCE MANAGEMENT ON THE PERFORMANCE OF THE APPLICATION'S EMPLOYEES ON PUBLIC HOSPITALS IN THE STATE OF KHARTOUM**

**Dr.Mohammed Ali Hassan al-Taher¹ Dr. Ismail Mohammed Abdel Jalil²
Dr. Hatem Othman Adam Ismail³**

¹ Assistant Professor - Garden City University. Sudan

² Assistant Professor - Nile Valley University. Sudan

³ Assistant Professor - Academy of Engineering and Medical Sciences, Sudan

HNSJ, 2022, 3(3); <https://doi.org/10.53796/hnsj3318>

Published at 01/03/2022

Accepted at 23/02/2021

Abstract

This study dealt with Impact of Applying the Functions of Management Human Resources on Employees Performance. This study aimed to high light the impact of using human resource Strategies in developing the Performance in private hospitals, and the study followed all of the descriptive approach. The study found that the existence of a Relation ship between Human Resource Strategies and Employee partially supported. The study recommended that the study recommends setting competitive salaries and wages compared to other hospitals.

Key Words: Management of Human Resources, Employees Performance.

المقدمة:

شكلت جائحة كورونا تحدياً كبيراً علي مستوى تقديم الخدمات الطبية في المستشفيات الحكومية والخاصة علي حد سواء ,بسبب خوف العاملين من إنتقال العدوى اليهم بسبب أن أدوت ومعدات الحماية غير متوفرة بشكل كافي مما جعلهم يتهربون من أداء أعمالهم بحجج واهيه وهذا الوضع خلق تنمراً واضحاً من العاملين تجاه إداراتهم . إن المستشفيات السودانية تواجه ضغوطات متنامية وسريعة التغير بسبب الديمغرافيا السكانية وأنماط الامراض والتحديات التي تواجه قطاع المستشفيات السودانية وهي جزء من التحديات الاجتماعية والاقتصادية العامة . وأهم هذه التحديات هي نقص التمويل والاعتماد المتزايد علي الرسوم التي يدفعها المرضى . ومن هنا ينبغي الارتقاء بمستوى الاداء للكوادر البشرية ومستوي الخدمات الصحية المقدمة في المستشفيات الخاصة والعامة إذ أصبح هذا الامر مطلباً ملحاً وضروريا لاغني عنه . ويجب وضع أهداف مدروسة تتكيف مع كل التحديات والتغيرات التي تمر بها في الوقت الحاضر أو التغيرات التي قد تحدث في المستقبل وذلك لضمان المحافظة علي أعلى مستوى من جودة الخدمات المقدمة للمرضى.

المحور الأول: الإطار المنهجي**مشكلة الدراسة:**

لأهمية القطاع الصحي ولأن العاملين فيه يتعاملون مع المستفيدين من المرضى الذين يأملون أن يتلقوا رعاية وخدمات صحية مميزة وبأسرع وقت فإن ذلك يتطلب رفع مستوى دافعية العاملين بالمستشفيات العامة بولاية الخرطوم لتحقيق أهداف هذه المؤسسات والعاملين والمستفيدين في آن واحد. تمثلت مشكلة الدراسة في السؤال التالي:

ما هو أثر تطبيق وظائف إدارة الموارد البشرية علي أداء العاملين في المستشفيات العامة بولاية الخرطوم

أهداف الدراسة:

تسعي الدراسة إلي تحقيق الأهداف التالية:

1. التعرف علي عمل المستشفيات العامة بولاية الخرطوم في جانب تطبيق وتنمية وتطوير أداء الموارد البشرية ومدى تطبيق وظائف إدارة الموارد البشرية.
2. إبراز أثر إستخدام الوظائف العامة بالموارد البشرية في تنمية وتطوير أداء المستشفيات العامة.
3. توضيح الاثر الايجابي لإستخدام وظائف إدارة الموارد البشرية .

أهمية الدراسة:

تكمن أهمية الدراسة في الآتي:

الأهمية العلمية:

1. الدور العلمي الذي يمكن أن تقدمه في تزويد الباحثين بقاعدة بيانات تدعم تطبيق وظائف إدارة الموارد البشرية.
2. أن إدارة الموارد البشرية لها دور فاعل وأساسي في تحقيق الفعالية و الكفاية الإدارية في المستشفيات العامة.

الأهمية العملية:

1. تقييم ودراسة وظائف إدارة الموارد البشرية وأثرها علي فعالية أداء العاملين في المستشفيات العامة.
2. إمكانية الاستفادة من نتائج الدراسة في تطوير تطبيق وظائف إدارة الموارد البشرية في المستشفيات العامة.

فرضيات الدراسة:

تختبر الدراسة الفرضيات التالية:

1. هناك علاقة ذات دلالة إحصائية بين وظائف إدارة الموارد البشرية و فعالية أداء العاملين بالمستشفيات العامة.
2. هناك علاقة ذات دلالة إحصائية بين وظائف إدارة الموارد البشرية و كفاءة أداء العاملين بالمستشفيات العامة.

مصادر جمع البيانات:

منهجية الدراسة:

اعتمدت الدراسة علي المنهج التحليلي الوصفي باعتباره الأكثر توافقاً مع أهداف الدراسة الميدانية وإجراءاتها , ويقوم هذا المنهج علي دراسة الظاهرة كما توجد في الواقع , ويسهم في وصفها وصفاً دقيقاً يوضح خصائصها عن طريق جمع المعلومات وتحليلها وتفسيرها.

المحور الثاني: الدراسات السابقة

دراسة مسودة (2004م) :

تناولت الدراسة أثر تطوير الموارد البشرية الصحية في تحقيق الجودة الشاملة متخذة المستشفيات الأردنية الخاصة. وتمثلت مشكلة الدراسة في معرفة أثر تطوير الموارد البشرية الصحية في تحقيق الجودة الشاملة في المستشفيات الأردنية الخاصة. توصلت الدراسة لنتائج أهمها أنه لا يوجد تعريف محدد للجودة أو إدارة الجودة الشاملة وإنما هي وجهات نظر متعددة. وقد خلصت الدراسة إلى توصيات أهمها، ضرورة قيام القطاع الصحي في الأردن بإنشاء جائزة تقديرية على مستوى الدولة لتحقيق الميزة التنافسية بين المستشفيات، تعزيز آليات التطوير والتدريب في المستشفيات الأردنية، تطوير السياسات والإجراءات والبروتوكولات الإدارية والفنية المعززة للجودة والتحسين المستمر للعلاقات مع المرضى ومستوى الكفاءة التشغيلية

تختلف هذه الدراسة عن دراسة الباحثون في أنها تناولت أثر تطوير الموارد البشرية الصحية في تحقيق الجودة الشاملة متخذة المستشفيات الأردنية الخاصة ، بينما تناولت دراسة الباحث أثر تطبيق وظائف إدارة الموارد البشرية علي أداء العاملين.

دراسة: حمزة (2013م) :

تناولت الدراسة أثر تنظيم الموارد البشرية علي كفاءة الأداء، بديوان الضرائب حيث تمثلت مشكلة الدراسة في ماهي الهياكل التنظيمية القائمة وما نوعها؟ ما هي المشاكل التنظيمية والهيكلية التي تواجه ديوان الضرائب في الوقت الحالي. هل يوفر تنظيم الموارد البشرية المرونة اللازمة لرفع كفاءة الأداء؟ هدفت الدراسة الي معرفة أثر

تنظيم الموارد البشرية علي كفاءة الأداء وكيفية تطوير العمل ورفع مستوى الأداء والمحافظة علي الاستقرار والمواكبة والاستمرارية في العمل وتحقيق الاهداف وتنفيذ الخطط. توصلت الدراسة الي العديد من النتائج منها: أن الهيكل التنظيمي الحالي للديوان لا يحقق التكامل بين أنشطة الوحدات والادارات مع إدارة الموارد البشرية. ولا يوجد تنسيق وتكامل بين الادارات وإدارة الموارد البشرية، وأن إدارة الموارد البشرية لها علاقة بتدريب الموظف ورسم سياسة المصلحة . وأوصت الدراسة بعدة توصيات أهمها: لابد من تطوير مناسب للهيكل التنظيمي داخل الديوان لمواجهة النمو السريع والزيادة المضطردة في إعادة القوي العاملة والتطورات الاجتماعية والاقتصادية الجارية في المجتمع وتحديد أهداف كل وحدة تنظيمية وصياغة اختصاصاتها بصورة واضحة.

تختلف هذه الدراسة عن دراسة الباحث في أنها تناولت أثر تنظيم الموارد البشرية علي كفاءة الأداء، بديوان الضرائب، بينما تناولت دراسة الباحث أثر تطبيق وظائف إدارة الموارد البشرية علي أداء العاملين.

دراسة: لصور (2017م)

تناولت الدراسة التفاعل بين ممارسات إدارة الموارد البشرية وإدارة المعرفة وأثرها في متطلبات الجودة الشاملة. حيث تمثلت مشكلة الدراسة في السؤال أي مدى تقوم الشركات العاملة في صناعة النفط والغاز في اليمن بتطبيق كل من ممارسات إدارة الموارد البشرية وإدارة المعرفة وإدارة الجودة الشاملة؟ وهل توجد علاقة إرتباط بين ممارسات إدارة الموارد البشرية وإدارة المعرفة وإدارة الجودة الشاملة. هدفت الدراسة إلي الدراسة الي توضيح مفاهيم إدارة الموارد البشرية وإدارة المعرفة وإدارة الجودة الشاملة، والتعرف علي درجة تطبيق ممارسات إدارة الموارد البشرية وإدارة المعرفة من وجهة نظر العاملين، واختبار طبيعة علاقات الارتباط بين ممارسات إدارة الموارد البشرية وإدارة المعرفة وإدارة الجودة الشاملة في عينة الدراسة. خلصت الدراسة إلي عدة نتائج تؤكد صحة الفرضيات أهمها : أن الشركات عينة الدراسة تمارس إدارة الموارد البشرية وإدارة المعرفة بشكل جيد ، وتظهر النتائج علاقات إرتباطية معنوية قوية نسبيا بين ممارسات إدارة الموارد البشرية وإدارة المعرفة وإدارة الجودة الشاملة وعلاقات تأثير بين المتغيرات السابقة وبشكل متفات ، وأتضح من نتائج التحليل الاحصائي وجود علاقة تأثير بين ممارسات إدارة الموارد البشرية وإدارة المعرفة مجتمعة وكل من التزام الادارة العليا والتحسين المستمر وتمكين العاملين كمحاور لإدارة الجودة الشاملة. واختتم الباحث دراسته بعدد من التوصيات بناء علي النتائج التي توصل إليها، منها التي تساعد قيادة الشركات علي إزالة الغموض حول إدارة الموارد البشرية وإدارة المعرفة وأهمية العلاقة بينهما في دعم فلسفة الجودة الشاملة وتلافي أوجه القصور التي رافقت التطبيق وتوصيات أخرى تسعى الي لفت نظر جهات الاختصاص من مثل هذه الفلسفات الحديثة.

تختلف هذه الدراسة عن دراسة الباحث في أنها تناولت التفاعل بين ممارسات إدارة الموارد البشرية وإدارة المعرفة وأثرها في متطلبات الجودة الشاملة ، بينما تناولت دراسة الباحث أثر تطبيق وظائف إدارة الموارد البشرية علي أداء العاملين.

دراسة: آدم (2018م)

تناولت الدراسة أثر نظم معلومات الموارد البشرية علي أداء المؤسسات الحكومية دراسة حالة وزارة تنمية الموارد البشرية، حيث تمثلت مشكلة الدراسة في التحديات والصعوبات التي تواجه المؤسسات الحكومية جراء التغيرات

والتحولات المتسارعة التي تحدث في البيئة التي تعمل فيها من سوء التوازن وتقدير إحتياجاتها من الموارد البشرية وغياب عملية التخطيط المستمر وضعف الهياكل، هدفت الدراسة إلي معرفة مدي تطبيق الاساليب والوسائل والبرامج العلمية في مجال إدارة الموارد البشرية من خلال إستخدام نظم معلومات الموارد البشرية في وزارة تنمية الموارد البشرية، وقد توصلت الدراسة إلي مجموعة من الاستنتاجات أهمها ما يأتي : تطبيق نظم معلومات الموارد البشرية يحسن مستوى الاداء ، تساهم نظم معلومات الموارد البشرية بالوزارة علي تحقيق الاهداف والخطط ، كما تساعد علي النمو والتطور والاستجابة لمتغيرات البيئة الداخلية والخارجية وتنظيم الانتاج وتحقيق الكفاءة والفاعلية . قد انتهت الدراسة بمجموعة من التوصيات تمثلت أهمها : بالإهتمام بتطبيق جميع وظائف نظم معلومات الموارد البشرية لتحقيق المذيد من الكفاءة والفاعلية مما يساعد في تحقيق أهدافها ، وأن تهتم بتحديث وتطوير نظم معلومات الموارد البشرية حتي تتسم بالوضوح والدقة والسرعة في عملية التخطيط الجيد للموارد البشرية ، علي الوزارة تقليل الاعتماد علي الاعمال الورقية في جمع ومعالجة و تخزين وإسترجاع المعلومات .

تختلف هذه الدراسة عن دراسة الباحث في أنها تناولت أثر نظم معلومات الموارد البشرية علي أداء المؤسسات الحكومية دراسة حالة وزارة تنمية الموارد البشرية ، بينما تناولت دراسة الباحث أثر تطبيق وظائف إدارة الموارد البشرية علي أداء العاملين .

دراسة: موسي (2019م)

تناولت الدراسة أثر إستراتيجية إدارة الموارد البشرية علي أداء المنظمة بالتطبيق علي منظمات التعليم العالي الاهلي في السودان، حيث تمثلت مشكلة البحث في هذه الدراسة في السعي للاستفادة من مفهوم إستراتيجية إدارة الموارد البشرية وفلسفة الادارة الفعالة من خلال التعريف بهما وإبراز مزاياهما ومعرفة العلاقة بينهما والأثر الذي يمكن ان تلعبه استراتيجية إدارة الموارد البشرية في تحقيق فعالية وكفاءة اداء المنظمات ومخرجاتها. التعرف علي المفاهيم والنظم والنظريات الخاصة بإستراتيجية الموارد البشرية المتمثلة في التخطيط ، الاستقطاب ، التوظيف ، التنمية والتطوير ، التعويض والمكافآت ثم التقييم والمتابعة وأثرها علي أداء المنظمة. توصلت الدراسة الى عدة نتائج اهمها: وجود أثر لاستراتيجية إدارة الموارد البشرية علي اداء الجامعات والكليات الاهلية في السودان وعلي أداء العاملين بها بنسب متفاوتة كما يوجد عدم رضا للعاملين بنظام التعويضات وعدم إشراكهم في إتخاذ القرار بالجامعات والكليات الخاصة ، ايضا يوجد ضعف في رقابة التعليم العالي علي اداء هذه المؤسسات التعليمية الاهلية. وأوصت الدراسة بأهمية فهم الادارة العليا لإستراتيجية إدارة الموارد البشرية وبنائها ، وتمكين العاملين وتعريفهم بأهمية استراتيجية ادارة الموارد البشرية ، ومراجعة نظام التعويضات في الجامعات والكليات الاهلية والعمل علي إشراك العاملين في صنع وإتخاذ القرار ات.

تختلف هذه الدراسة عن دراسة الباحث في أنها تناولت أثر إستراتيجية إدارة الموارد البشرية علي أداء المنظمة بالتطبيق علي منظمات التعليم العالي الاهلي في السودان ، بينما تناولت دراسة الباحث أثر تطبيق وظائف إدارة الموارد البشرية علي أداء العاملين .

المحور الثالث: الإطار النظري

أولاً: تعريف إدارة الموارد البشرية:

تعرف إدارة الموارد البشرية بأنها "أحدى الوظائف أو الإدارات الأساسية في المنظمة، ومحور عملها جميع الموارد البشرية التي تعمل فيها وكل مايتعلق بها من أمور وظيفية، كما يمكننا القول ان إدارة الموارد البشرية هي سلسلة القرارات الخاصة بالعلاقات الوظيفية المؤثرة في فاعلية المنظمة والعاملين فيها" (Randall, 1995, 36) . عرفها مايكل بول وفقاً للثلاثة نقاط التالية: إنها العملية الخاصة باستيعاب الأفراد، إنها العملية الخاصة بتطوير الأفراد العاملين، إنها العملية الخاصة بالمحافظة علي الأفراد العاملين، وذلك من أجل تحقيق أهداف المنظمة وتحقيق أهدافهم الخاصة (Pool, 1993, 3).

يعرفها آخر إدارة الموارد البشرية بأنها تعني الاهتمام الكامل والشامل بكل ما يهم الموارد البشرية في المنظمة الادارية، وهي إحدى الروابط الأساسية التي تربط المنظمة ببيئتها الاجتماعية وتحمل قيم وأخلاقيات وفلسفة تلك البيئة كما تؤثر هي علي البيئة أيضاً بنفس القدر (ابوسن، 2009م، 14). من خلال ما تقدم يتبين للباحث أن إدارة الموارد البشرية هي عملية خاصة بتطوير، واستيعاب، والمحافظة علي العاملين.

ثانياً: أهمية إدارة الموارد البشرية

استحوذت إدارة الموارد البشرية وعبر مراحل تطورها علي أهمية خاصة بالنسبة لمنظمات الأعمال وغيرها وهذه الأهمية نابعة من أهمية الدور الذي تلعبه، وأهمية العنصر البشري ودوره في المنظمات حتي أصبح لا يراود أحد شك أن خلف كل منظمة ناجحة تقف إدارة موارد بشرية ناجحة في برامجها سواء كانت هذه البرامج في إطار اختيار الافراد، أو تدريبهم، أو تقويم أدئهم، أو صيانتهم والاحتفاظ بهم، أو من إرتباط قوي بين نجاح المنظمة (لا سيما منظمة الأعمال) وبين برامج الموارد البشرية (الموسوي، 2004م، 20).

ثالثاً: أهداف إدارة الموارد البشرية

أن أهداف الموارد البشرية هي أهداف المنظمة أيضاً، ويجمع الباحثون علي أن لإدارة الموارد البشرية هدفين رئيسيين وهما: (السالم، 2012م، 33)

أ/ العمل علي تحقيق سعادة الأفراد العاملين بالمنظمة الإدارية.

ب/ العمل علي تحقيق الكفاية في الإنتاج.

ويمكن بلورة أهداف إدارة الموارد البشرية علي النحو التالي: (أبوسن، 2009م، 18)

1/ الحصول علي الأفراد الأكفاء للعمل في مختلف الوظائف من أجل إنتاج السلع أو الخدمات بأحسن الطرق وأقل التكاليف وتحقيق الميزة التنافسية.

2/ الاستفادة القصوي من جهود العاملين في إنتاج السلع والخدمات وفق المعايير الكمية والنوعية المحددة مسبقاً.

3/ تحقيق انماء وولاء العاملين وتنمية علاقات التعاون بينهم والعمل علي زيادة رغبتهم في العمل فيها.

4/ تنمية قدرات العاملين من خلال تدريبهم لمواجهة التغيرات المتلاحقة في البيئة التنافسية.

5/ توفير بيئة عمل جيدة تمكن العاملين من أداء عملهم بصورة جيدة، وتزيد من إنتاجيتهم ومكاسبهم المادية.

- 6/ إيجاد سياسات موضوعية تمنع سوء استخدام العاملين وتقادي المهام التي تعرضهم لحوادث العمل الصناعية والأمراض المهنية.
- 7/ تحقيق العدالة وتكافؤ الفرص لجميع العاملين في المنظمة من حيث الترقية والأجور والتدريب والتطوير عندما يصبحون مؤهلين لذلك.
- 8/ يتوقع العاملون أيضاً وجود ضمان اجتماعي وصحي جيد.
- 9/ تزويد العاملين بكل البيانات التي يحتاجونها بغرض أداء أعمالهم وتوصيل أرائهم ومقترحاتهم للمسؤولين قبل اتخاذ قرار معين يؤثر عليهم.
- 10/ الإحتفاظ بالسجلات المتعلقة بكل شخص يعمل في المنظمة وبما ينسجم وطبيعة عمله. (السالم, 2012م, 35).

رابعاً: وظائف إدارة الموارد البشرية

وتتمثل وظائف إدارة الموارد البشرية في الآتي (حنفي, 2007م, 11)

أ/ تحليل العمل: تعني هذه الوظيفة التعرف على الأنشطة والمهام المكونة للوظيفة، وتوصيف هذه الوظيفة وتحديد المسؤوليات الملقاة علي عاتقها، وتصميم الوظيفة بشكل مناسب وتحديد مواصفات من يشغلها.

ب/ تخطيط القوي العاملة: تعني بتحديد احتياج المنظمة من أنواع واعداد العاملين، ويتطلب هذا تحديد طلب المنظمة من العاملين، وتحديد ماهو معروض ومتاح منها، والمقارنة بينهما لتحديد صافي العجز والزيادة في القوي العاملة بالمنظمة، فهو وسيلة لضمان الحصول علي الأفراد اللازمين لسير العمليات الانتاجية والتسويقية والادارية المختلفة خلال فترة زمنية مستقبلية من كفاءات محددة بأعداد معينة" (زويلف, 1998م, 48)، كما أنه يوصف علي أنه تقرير الطلب والعرض (التنبؤ) لتحقيق التنمية والانتاجية المتوازنة (النجار, 1998م, 111) وتتبع أهمية تخطيط القوي العاملة من أهمية وظيفة الموارد البشرية للمنظمات، فأى عمل ناجح لا بد وأن يسبق بتخطيط سليم من شأنه أن يساعد علي إنجاحه (عباس, 2000م, 56). فهو يساعد في تحديد احتياجاتها المستقبلية من القوي البشرية، ومن ثم يساعد في تخفيض تكلفة الانتاج التي تنتج عن النقص والاختناق أو الزيادة في القوي العاملة، كما يساعد المنظمة في تحديد القوي البشرية التي تتطلب تدريباً أو إعادة تدريب لرفع قدراتها الأدائية وحسن استخدامها، يساعد المنظمة أيضاً في مواجهة أية تغيرات قد تحدث في بيئتها الداخلية والخارجية كازدياد الهجرة الي خارج الدولة أو الي داخلها (درة, 1986م, 150).

ت/ الإختيار والتعيين: وتهتم هذه الوظيفة بالبحث عن العاملين في سوق العمل وتصفيتهم من خلال طلبات التوظيف، والاختبارات، والمقابلات الشخصية وغيرها من الاساليب، وذلك ضماناً لوضع الفرد المناسب في المكان المناسب

ث/ تصميم هيكل الاجور: وتهتم هذه الوظيفة بتحديد القيمة والاهمية النسبية لكل وظيفة، وتحديد أجرها وتحديد درجات أجرية للوظائف، كما تهتم بإدارة سليمة لنظام الاجور حتي يتم ضمان مقابل سليم للقيم والاهميات المختلفة للوظائف.

سياسات الاجور غير العادلة تكون بمثابة عنصر خطير في مجال علاقات العمل يؤدي الي هبوط معنويات

العاملين ويخلق حالة من عدم الرضاء ويرفع من معدلات الغياب ودوران العمل ويضر بالانتاجية (هاشم, 1996م, 52)

ج/ تصميم أنظمة الحوافز: وتعني الوظيفة بمنح مقابل عادل للأداء المتميز ويمكن تحفيز العاملين علي أدائهم الفردي، أو أدائهم الجماعي، فتظهر الحوافز الفردية والجماعية، وأيضاً هناك حوافز علي أساس أداء المنظمة ككل.

ح/ تصميم أنظمة مزايا وخدمات العاملين: تهتم المنظمات بمنح عاملها مزايا عينية مثل المعاشات والتأمينات الخاصة بالمرض والعجز والبطالة، كما تهتم المنظمات بتقديم خدمات للعاملين في شكل خدمات مالية واجتماعية ورياضية وقانونية، وقد تمتد الي الإسكان والمواصلات وغيرها.

خ/ تقييم الاداء: تهتم كل المنظمات تقريباً بتقييم أداء موظفيها، ويتم ذلك من خلال أساليب معينة، وغالباً ما يقوم بالتقييم الرؤساء المباشرين بغرض التعرف علي الكفاءة العامة للعاملين، وبغرض التعرف علي أوجه القصور في هذا الاداء.

ع/ التدريب: تمارس المنظمات أنشطة التدريب بغرض رفع كفاءة ومعارف ومهارات العاملين، وتوجيه اتجاهاتهم نحو أنشطة معينة، وعلي الشركة ان تحدد احتياج المرؤوسين للتدريب، وان تستخدم الأساليب والطرق المناسبة وأن تقيم فعالية التدريب.

غ/ تخطيط المسار الوظيفي: تهتم هذه الوظيفة بالتخطيط للتحركات الوظيفية المختلفة للعاملين بالمنظمة، وعلي الأخص فيما يمس النقل والترقية والتدريب، ويحتاج هذا الي التعرف علي نقاط القوة لدي الفرد، ونقاط الضعف لديه.

ثالثاً: مفهوم الأداء

يختلف المفكرون والكتاب حول مفهوم الأداء فيري البعض بأنه "يقصد بمفهوم الأداء المخرجات أو الأهداف التي يسعى النظام الي تحقيقها" (عبد المحسن, 1997م, 150). مفهوم تقييم الأداء هو إيجاد مقياس يمكن من خلاله معرفة مدي تحقيق المنظمة للأهداف المخطط لها ومقارنتها بالأهداف المحققة ومعرفة وتحديد مواطن الانحرافات عن ما تم التخطيط له مسبقاً وتحديد أسباب تلك الانحرافات وأساليب معالجتها(نايف, 1998م, 358).

رابعاً: العوامل المؤثرة علي الأداء

من العوامل المؤثرة علي الأداء في المؤسسة هي (مرعي, 2001م, 7):

أ/ تاريخ وثقافة المؤسسة والمفاهيم والقيم الثقافية السائدة.

ب/ حجم وقطاع المؤسسة.

ت/ التوجهات الاستراتيجية والاقتصادية والثقافية والانسانية للمؤسسة: تحدد التوجهات الاستراتيجية للمؤسسة مجال معايير أنظمة التقييم لان كل منها يتطلب القدرات الكافية لديهم للتطوير المستقبلي للمؤسسة.

ث/ أسلوب الإدارة العامة السائد: وتأخذ في الحسبان أولويات المؤسسة ويناسب مدي الحركة المتبعه في الممارسة الإدارية من مرونة أو تجديد أو ركود.

ج/ أسلوب إدارة الموارد البشرية السائد: إذ أن المؤسسات التي لا توجد فيها أسس إدارة الموارد البشرية يكون فيها نظام التقييم مختلفاً ولا يعبر عن التطور الحاصل في عالم الإدارة الحديثة.

ح/ طبيعة العلاقات الاجتماعية القائمة: البيئة المحيطة مثل النقابات، الدولة، الزبائن، الموردين.

خامساً: مفهوم الفعالية

وتعرف الفعالية بكل بساطة بأنها أداء الأعمال الصحيحة لذلك لا بد لنا من معرفة الأعمال الصحيحة وتحديدتها وتعريفها لنتمكن من أدائها . يعرف الكثيرون الفعالية بأنها الإنتاج! بما يعني أن فاعلية إنسان ما تقاس بمقياس واحد، هو مدى إنتاج هذا الإنسان، والصحيح أنه ليست هذه هي الفاعلية Effectiveness إن تعريف الفاعلية في كتب الإدارة شي آخر اسمه الكفاءة . وهي الحصول على أكبر المخرجات من أقل المدخلات وتعريف الفاعلية الإدارية نسبي يختلف باختلاف تصور المقيّم لها (المنيف، 1983م، 350).

سادساً: قياس الفعالية

بالرغم من أن أبعاد الفاعلية والعلاقات المتداخلة بينها ليست واضحة بصورة جلية حتى الآن إلا أنه تم الاتفاق على بعد واحد وهو الوقت ، حيث أن الاختبار النهائي للفعالية التنظيمية يتمثل فيما إذا كانت المنظمة قادرة على أن تدعم بقاءها بصفة مستمرة في البيئة ، حيث يقول جيزون Jason إن المقياس الأخير لفاعلية التنظيم هو عامل الوقت حيث في المدى القصير تتضمن المؤشرات الممكنة ما يلي (جاكسون، 1988م، 59) :

- 1- الإنتاج : و يعكس قدرة المنظمة على الإنتاج (مهما كان ذلك) بالكمية و النوعية التي تتطلبها البيئة .
- 2- الكفاءة : و يمكن تعريفها كنسبة المخرجات للمدخلات، و تستخدم فيها عدة مقاييس مثل تكلفة الوحدة المنتجة و العائد على رأس المال و معدل الضياع من المواد و الخامات و كذلك الوقت الضائع و ما شابه ذلك من مؤشرات الكفاءة.
- 3- الرضا: يتطلب إدراك المنظمة كنظام اجتماعي الاهتمام بالمنافع التي يحصل عليها عضو المنظمة و المنافع التي يمكن أن تعود على عملائها، و يسمى هذا المعيار الرضا و تتضمن مقاييسه معدل الغياب و التأخر و الشكاوى .

سادساً: مفهوم الكفاءة

أما الكفاءة من وجهة نظر الإدارة : " فهي النظام القادر علي تخفيض تكاليف الموارد اللازمة لانجاز الأهداف المحددة والمرغوبة دون التضحية بمخرجات النظام " . بمعنى أنها القدرة علي أداء الأشياء بطريقة صحيحة ، ومن ثمة فهي تعتمد علي مفهوم المدخلات والمخرجات فالنظام الكفاء هو الذي يتمكن من تحقيق مخرجات تفوق المدخلات المستخدمة (ادريس، 2002م، 145).

سابعاً: قياس الكفاءة

هناك العديد من المؤشرات و المعايير المستعملة في هذا الخصوص منها :

أ- مؤشرات " معايير " مباشرة:

تتضمن هذه المعايير قياس عمليات المنظمة من خلال مقارنة المخرجات " السلع و الخدمات" بالمدخلات " الموارد المستخدمة" خلال مدة زمنية معينة و تشمل ما يلي:

المقاييس الكلية للكفاءة، المقاييس الجزئية للكفاءة، المقاييس النوعية للكفاءة، و قد تعجز مثل هذه المؤشرات عن توفير المقاييس الدقيقة خصوصا في بعض الانشطة الخدمية التي يتعذر فيها استخدام مثل هذه المقاييس.(ادريس، 2002م، 146)

ب- مؤشرات " معايير " غير مباشرة:

تعاني المعايير المباشرة من القصور في قياس الكفاءة في بعض المنظمات للأسباب الآتية:

1- عدم دقة البيانات المتعلقة بالمدخلات و المخرجات بالمقارنة مع متطلبات تحقيق سبل القياس المطلوبة للكفاءة.

2- عدم دقة المقارنات التي تعد محور قياس الكفاءة، و كذلك صعوبة إجرائها بين الوحدات و الأقسام المختلفة للمنظمة.

لذلك فان القياسات غير المباشرة تعد في بعض المجالات طريقا أفضل في قياس الكفاءة، و ذلك عن طريق قياس الرغبة في العمل، و التعرف على درجات رضا الافراد العاملين، و الروح المعنوية، هذا إضافة إلى دراسة و تحليل إمكانية الاستثمار الرشيد للموارد البشرية و المادية و المالية و المعلومات المتاحة (الشماع، 2000م، 232).

المحور الرابع: الدراسة الميدانية:

يحتوى هذا الفصل على تحليل البيانات المتعلقة بمعدل الاستبانة والتحليل العاُملى لمتغيرات الدراسة وبالإضافة الى درجة إعتمادية متغيرات الدراسة وتعديل فرضيات الدراسة وبجانب الاحصاء الوصفى ، والمتوسطات ، والانحراف المعياري لمتغيرات الدراسة ثم تحليل الفرضيات .

أولاً: معدل الاستجابة:

تم توزيع عدد (80) إستبيان بمساعدة مقدرة ومشكورة تمكن الدارس من استلام ردود المبحوثين في فترة وجيزة . الجدول التالي يوضح معدل الاستجابة للمبحوثين.

جدول (3/1) معدل إستجابة المبحوثين (حجم العينة = 77)

ان	دد	سبة %
لإستبانات الموزعة		1%
لإستبانات المستردة		96%
لإستبانات التي لم ترد		3%
لإستبانات الغير صالحة للتحليل		%
لإستبانات الصالحة للتحليل		96%

المصدر :إعداد الباحث من بيانات الدراسة الميدانية 2021م

يلاحظ من الجدول أن عدد الاستبانات المستردة يساوي (77) استبيان بنسبة (96.3%) من إجمالي الاستبانات الموزعة، الاستبانات التي لم ترد (3) استبيان بنسبة (3.7%). بينما يبلغ عدد الاستبانات الغير صالحة للتحليل (0) استبيان بنسبة (0%). أما عدد الاستبانات الصالحة للتحليل فيساوي (77) استبيان بنسبة

(96.3%) من إجمالي الاستبيانات الموزعة وهي نسبة تعتبر كبيرة في البحوث التي تعتمد علي قوائم الأسئلة أو الاستبيانات وتعكس مدى إستجابة المبحوثين ومدى وضوح عبارات الاستبيان المستخدمة في جمع بيانات الدراسة الميدانية.

ثانياً: التحليل العاملي:

أخضعت بيانات الاستبيان للتحليل العاملي بغرض فهم الاختلافات بين مجموعة كبيرة من متغيرات الاستجابة. حيث أن التحليل العاملي يستعمل متغيرات معيارية لتوزع عليها بنود المتغيرات بحسب إنحرافاتها عن الوسط الحسابي وتكون العلاقات بين المتغيرات داخل العامل الواحد أقوى من العلاقة مع المتغيرات في العوامل الأخرى (زغلول، 2003).

تستند متغيرات هذه الدراسة بواسطة التحليل العاملي على الافتراضات التي تقدمت بها دراسة (Hair et al 2010) كشرط لقبول نتائجها وهي :

- 1 - وجود عدد كافي من الارتباطات ذات دلالة إحصائية في المصفوفة
- 2 - ألا تقل قيمة (KMO) عن (0.6)
- 3 - ألا يقل إختبار (Bartlett's) عن (0,05)
- 4 - أن تكون قيم الاشتراكات الأولية (Cummunalities) للبند أكثر من (0,50)
- 5 - ألا يقل تشبع (Loading) العامل عن (0,50). مع مراعاة عدم وجود قيم متقاطعة تزيد عن (0,50) في العوامل الأخرى.

- 6 - ألا تقل قيم الجذور الكامنة (Eigen values) عن الواحد

1- التحليل العاملي للمتغير المستقل إستراتيجيات إدارة الموارد البشرية:

أجري التحليل العاملي لعدد (35) عبارة تستخدم لقياس إستراتيجيات إدارة الموارد البشرية يعرض ملخص نتائج التحليل العاملي الذي أجري على المتغير المستقل (إستراتيجيات إدارة الموارد البشرية). في الاختبار الأول من التحليل العاملي وجدت عبارات لها قيم الاشتراكات الأولية (Cummunalities) أقل من (0,50) تم استبعادها.

جاءت المصفوفة في (7) أعمدة، اشتمل النموذج الأول علي (10) عبارات شكلت الاجور والمرتبات ،اشتمل النموذج الثاني علي (6) عبارات شكلت تخطيط الموارد البشرية ، اشتمل النموذج الثالث علي (5)عبارات شكلت التدريب ، اشتمل النموذج الرابع علي (4)عبارات شكلت تقييم الاداء، اشتمل النموذج الخامس علي (3)عبارات شكلت الاختيار والتعيين، اشتمل النموذج السادس علي (2) عبارة شكلت الاستقطاب، اشتمل النموذج السابع علي (2) عبارة شكلت الحوافز.

جدول (3/3) التحليل العاملي للمتغير المستقل إستراتيجيات إدارة الموارد البشرية :

7	6	5	4	3	2	1	الاجور والمرتبات
0.011	0.027	0.210	0.195	0.294	0.191	0.824	لدي المستشفى نظم حوافز عادلة
0.010	-0.009	0.114	0.223	0.277	0.075	0.808	تتابع المستشفى باهتمام وبشكل مستمر برامج الحوافز التي تقدمها مثيلاتها من المستشفيات في سوق العمل
0.147	0.196	0.088	0.111	0.125	0.204	0.780	ادي الاستقرار في الاجور والمرتبات في المستشفى الى رضا العاملين
0.097	0.163	0.203	0.294	0.202	0.185	0.742	تتم مراجعة خطة الحوافز في المستشفى استنادا على المنافسة الموجودة من قبل المؤسسات الصحية
0.050	0.215	0.014	0.238	0.116	0.219	0.683	تقدم المستشفى اجور ومرتبات تنافسية مقارنة مع المستشفيات الاخرى
-0.164	0.379	0.030	0.027	0.293	0.274	0.657	تقدم المستشفى للعاملين اجور ومرتبات مجزية
0.432	0.218	0.031	0.276	-0.138	0.161	0.640	ادي وجود الضمان الاجتماعي الى رضا العاملين بالمستشفى
-0.034	-0.040	0.401	-0.194	0.290	0.124	0.605	تمنح الحوافز في المستشفى استنادا الى نتائج تقييم اداء العاملين
-0.022	0.056	0.354	0.471	0.269	0.207	0.535	النظام الاداري (نظم، لوائح، قوانين) بالمستشفى مرضي للعاملين
0.253	0.356	-0.013	0.153	0.202	0.215	0.535	ساهمت المرتبات والاجور التي تدفعها المستشفى في تقليل معدل دوران العمل
							تخطيط الموارد البشرية
0.145	0.111	0.215	0.036	0.030	0.787	0.281	يسمح للعاملين الاشتراك في وضع استراتيجية الموارد البشرية
-0.009	0.106	0.116	0.252	0.276	0.744	0.263	تحظى خطة الموارد البشرية باهتمام كبير من العاملين والادارة
-0.135	0.183	0.207	0.251	0.228	0.735	0.172	توجد خطة استراتيجية للموارد البشرية في المستشفى
0.039	0.151	0.290	0.149	0.266	0.726	0.303	تعطي ادارة المستشفى تخطيط الموارد البشرية الحجم الذي يناسب من الاهمية في تخطيطها الاستراتيجي
0.375	-0.100	0.244	-0.129	0.189	0.653	0.065	يحقق تخطيط الموارد البشرية التنبؤ بهيكل الموارد البشرية كما ونوعا
0.091	0.354	0.219	0.436	0.246	0.504	0.227	تعتمد المستشفى على الوصف الوظيفي في استقطاب العاملين
							التدريب
0.105	0.162	0.052	0.301	0.763	0.208	0.246	تهتم المستشفى بتدريب جميع العاملين كل في مجاله
0.127	0.171	0.386	-0.032	0.755	0.050	0.208	يتم تحديد الاحتياجات التدريبية في المستشفى وفق المسار الوظيفي
0.033	0.290	0.117	0.306	0.750	0.117	0.240	يوجد لدى المستشفى خطة تدريبية
0.091	0.004	0.051	0.199	0.747	0.298	0.206	تتابع ادار التدريب عملية تنفيذ التدريب
0.098	0.018	0.046	0.190	0.694	0.423	0.330	تقوم المستشفى بقياس العائد من التدريب
							تقييم الاداء
-0.026	0.074	0.017	0.764	0.139	- 0.009	0.094	تسود روح المساءلة وتحمل المسؤولية بين العاملين بالمستشفى
-0.033	0.161	0.039	0.668	0.161	0.274	0.331	تتوفر بالمستشفى انظمة عمل لاداء الاعمال في المستشفى

0.102	0.141	0.174	0.622	0.351	0.149	0.395	ترقية العاملين بالمستشفى تتم وفق عملية تقييم الاداء
0.038	0.032	0.149	0.564	0.225	0.284	0.481	يوجد نظام دقيق وعادل لتقييم العاملين
							الاختيار والتعيين
-0.002	0.118	0.802	0.150	0.084	0.350	0.195	يقوم التعيين على اختيار الشخص المناسب في المكان المناسب
0.170	0.208	0.725	-0.016	0.173	0.133	0.038	تستخدم المستشفى المقابلات عند الاختيار والتعيين
0.090	0.078	0.710	0.178	0.054	0.297	0.261	تتم عملية الاختيار والتعيين وفق المعايير التي تحددها الوظيفة لشاغلها
							الاستقطاب
0.200	0.783	0.180	0.190	0.132	0.109	0.234	ادي وجود الضمان الاجتماعي الى رضا العاملين بالمستشفى
-0.050	0.715	0.322	0.111	0.247	0.171	0.288	تقدم المستشفى اجور ومراتب تنافسية مقارنة مع المستشفيات الاخرى
							الحوافز
0.791	0.038	0.042	-0.127	0.151	0.021	0.170	تزداد حوجة الفرد للحافز المعنوى كلما زاد مستواه الفكري والثقافي
0.606	0.159	0.407	0.288	0.136	0.199	-0.074	من معايير الاستقطاب ان تكون للفرد الرغبة والقدرة على العمل ضمن الفريق الواحد
74.909						Cumulative %	
0.878						Kaiser-Meyer-Olkin Measure of Sampling Adequacy.	
2013.380						Bartlett's Test of	

المصدر :إعداد الباحث من بيانات الدراسة الميدانية 2021

جدول (3/5) التحليل العاملي للمتغير التابع (الاداء) :

2	1	الفعالية
0.162	0.904	توفر الموارد البشرية الكفاءة يساعد على تميز الخدمات وجودتها
0.264	0.890	يحقق المستشفى اهدافه المخطط انجازها
0.210	0.869	توجد اهداف واضحة وقابلة للقياس بالمستشفى
0.163	0.834	تدعم الادارة العليا السياسات والنظم التي تحقق الاهداف الاستراتيجية
0.243	0.773	يحقق المستشفى نسبة عالية من الارباح
0.291	0.770	يتم تقييم الاهداف باستمرار
		الكفاءة
0.826	0.074	يوجد برنامج تحسين مستمر للخدمات بالمستشفى
0.732	0.246	تتيح ادارة المستشفى نظم اتصال تفاعلي بين الادارة والعاملين
0.553	0.476	يقوم المستشفى بالاستخدام الامثل لموارده المتاحة
70.841		Cumulative %
0.907		Kaiser-Meyer-Olkin Measure of Sampling Adequacy.
440.355		Bartlett's Test of

المصدر :إعداد الباحث من بيانات الدراسة الميدانية 2021

ثالثاً: الاعتمادية:

للتأكد من درجة الاعتمادية تم إختبار أسئلة الاستبانة بالاعتماد على مقياس الاعتمادية حيث يوضح الجدول أدناه أن معامل الاعتمادية (كرونباخ ألفا) كان بدرجة عالية من الاعتمادية حيث بلغ معامل الاعتمادية بالنسبة للعبارات المكونة لمتغيرات المستقل الاجور والمرتبات (0.930)، تخطيط الموارد البشرية (0.904)، التدريب (0.916)، تقييم الاداء (0.830)، الاختيار والتعيين (0.827)، الاستقطاب (0.801)، الحوافز (0.513)، أما المتغير الوسيط الدافعية (0.832)، أما لمتغيرات التابع الفعالية (0.935)، الكفاءة (0.634).

جدول (3/6) يوضح درجة الاعتمادية لمتغيرات الدراسة

Cronbach's alpha	عدد العبارات		
0.930	10	الاجور والمرتبات	المتغير المستقل
0.904	6	تخطيط الموارد البشرية	
0.916	5	التدريب	
0.830	4	تقييم الاداء	
0.827	3	الاختيار والتعيين	
0.801	2	الاستقطاب	
0.513	2	الحوافز	
0.935	6	الفعالية	المتغير التابع
0.634	3	الكفاءة	

المصدر: إعداد الباحث من بيانات الدراسة الميدانية 2021

رابعاً: المتوسطات والانحرافات المعيارية :

الجدول أدناه يوضح الوسط الحسابي والانحراف المعياري لابعاد المتغير المستقل (الاجور والمرتبات، تخطيط الموارد البشرية، التدريب، تقييم الاداء، الاختيار والتعيين، الاستقطاب، الحوافز، الدافعية، الفعالية، الكفاءة). يلاحظ من الجدول أن الوسط الحسابي الاجور والمرتبات (وسط حسابي = 2.96، انحراف معياري = 0.97)، يليه الوسط الحسابي تخطيط الموارد البشرية (وسط حسابي = 2.77، انحراف معياري = 1)، يليه الوسط الحسابي التدريب (وسط حسابي = 2.99، انحراف معياري = 1)، يليه الوسط الحسابي تقييم الاداء (وسط حسابي = 2.64، انحراف معياري = 0.98)، يليه الوسط الحسابي الاختيار والتعيين (وسط حسابي = 2.16، انحراف معياري = 0.95)، يليه الوسط الحسابي الاستقطاب (وسط حسابي = 2.34، انحراف معياري = 1)، يليه الوسط الحسابي الحوافز (وسط حسابي = 1.99، انحراف معياري = 0.92). ويلاحظ أن جميع هذه الأوساط الحسابية تقل عن الوسط الفرضي المستخدم في برنامج التحليل الإحصائي SPSS ومن جانب آخر ومن ذات الجدول يتضح أن الوسط الحسابي والانحراف المعياري للمتغير الوسيط الدافعية هو (الوسط حسابي = 2.26، الانحراف معياري = 0.90)، أما المتغير التابع يلاحظ ان الوسط الحسابي للفعالية (الوسط الحسابي = 2.67، الانحراف المعياري = 0.95)، والكفاءة (الوسط الحسابي = 2.19، الانحراف المعياري = 0.81).

جدول (3/7) يوضح المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة :-

اسم المتغير	نوع المتغير	الوسط الحسابي	الانحراف المعياري
الاجور والمرتبات	مستقل	2.96	.97
تخطيط الموارد البشرية	مستقل	2.77	1
التدريب	مستقل	2.99	1
تقييم الاداء	مستقل	2.64	.98
الاختيار والتعيين	مستقل	2.16	.95
الاستقطاب	مستقل	2.34	1
الحوافز	مستقل	1.99	.93
الدافعية	وسيط	2.26	.90
الفعالية	تابع	2.67	.95
الكفاءة	تابع	2.19	.80

المصدر إعداد الباحث من بيانات الدراسة الميدانية (2021)

خامساً: الارتباطات بين متغيرات الدراسة :

أجري تحليل الارتباطات على بيانات الدراسة الميدانية للوقوف على الصورة المبدئية للارتباطات البينية بين

متغيرات الدراسة . الجدول أدناه يوضح الارتباطات بين متغيرات الدراسة.

جدول (3/8) يوضح الارتباطات بين متغيرات الدراسة : Person's Correlation Coefficient for All

Variable

المتغيرات	الاجور والمرتبات	تخطيط الموارد البشرية	التدريب	تقييم الاداء	الاختيار والتعيين	الاستقطاب	الحوافز	الفعالية	الكفاءة
الاجور والمرتبات	1								
تخطيط الموارد البشرية	.624(**)	1							
التدريب	.634(**)	.617(**)	1						
تقييم الاداء	.696(**)	.571(**)	.612(**)	1					
الاختيار والتعيين	.489(**)	.618(**)	.440(**)	.405(**)	1				
الاستقطاب	.584(**)	.502(**)	.508(**)	.470(**)	.496(**)	1			
الحوافز	.295(**)	.353(**)	.337(**)	.223(**)	.368(**)	.316(**)	1		
الدافعية	.432(**)	.382(**)	.411(**)	.595(**)	.283(**)	.428(**)	.266(**)	1	
الفعالية	.612(**)	.656(**)	.659(**)	.639(**)	.437(**)	.544(**)	.125(**)	.567(**)	1
الكفاءة	.576(**)	.429(**)	.473(**)	.548(**)	.474(**)	.415(**)	.216(**)	.567(**)	.567(**)

المصدر إعداد الباحث من بيانات الدراسة الميدانية (2021)

من الجدول اعلاه نجد أن بعد تخطيط الموارد البشرية يرتبط ارتباط إيجابي مع الاجور والمرتبات

حيث كانت قيمة (الارتباط = .624) نجد أن التدريب يرتبط ارتباط إيجابي مع الاجور والمرتبات حيث

كانت قيمة (الارتباط = .634)، ونجد ان التدريب يرتبط ارتباط إيجابي مع تخطيط الموارد البشرية حيث

كانت قيمة (الارتباط = 0.617) ، ونجد أن تقييم الاداء يرتبط ارتباط ايجابي مع الاجور والمرتببات حيث كانت قيمة (الارتباط = 0.696) ، ونجد أن تقييم الاداء يرتبط ارتباط ايجابي مع تخطيط الموارد البشرية حيث كانت قيمة (الارتباط = 0.571) ، ، ونجد ان تقييم الاداء يرتبط ارتباط ايجابي مع التدريب حيث كانت قيمة (الارتباط = 0.612) ، ونجد ان الاختيار والتعيين يرتبط ارتباط ايجابي مع الاجور والمرتببات حيث كانت قيمة (الارتباط = 0.489) ، ونجد أن الاختيار والتعيين يرتبط ارتباط ايجابي مع تخطيط الموارد البشرية حيث كانت قيمة (الارتباط = 0.618) ، ونجد ان الاختيار والتعيين يرتبط ارتباط ايجابي مع التدريب حيث كانت قيمة (الارتباط = 0.440) ، ونجد أن الاختيار والتعيين يرتبط ارتباط ايجابي مع تقييم الاداء حيث كانت قيمة (الارتباط = 0.405) ، ونجد أن الاستقطاب يرتبط ارتباط ايجابي مع الاجور والمرتببات حيث كانت قيمة (الارتباط = 0.584) ، ونجد ان الاستقطاب يرتبط ارتباط ايجابي مع تخطيط الموارد البشرية حيث كانت قيمة (الارتباط = 0.502) ، ونجد ان الاستقطاب يرتبط ارتباط ايجابي مع التدريب حيث كانت قيمة (الارتباط = 0.508) ، ونجد ان الاستقطاب يرتبط ارتباط ايجابي مع تقييم الاداء حيث كانت قيمة (الارتباط = 0.470) ، ونجد ان الاستقطاب يرتبط ارتباط ايجابي مع الاختيار والتعيين حيث كانت قيمة (الارتباط = 0.496) ، ونجد ان الحوافز ترتبط ارتباط ضعيف مع الاجور والمرتببات حيث كانت قيمة (الارتباط = 0.292) ، ونجد ان الحوافز ترتبط ارتباط ضعيف مع تخطيط الموارد البشرية حيث كانت قيمة (الارتباط = 0.353) ، ونجد ان الحوافز ترتبط ارتباط ضعيف مع التدريب حيث كانت قيمة (الارتباط = 0.337) ، ونجد ان الحوافز ترتبط ارتباط ضعيف مع الاختيار والتعيين حيث كانت قيمة (الارتباط = 0.368) ، ونجد ان الحوافز ترتبط ارتباط ضعيف الاستقطاب مع حيث كانت قيمة (الارتباط = 0.316) ، ونجد ان الدافعية ترتبط ارتباط ايجابي مع الاجور والمرتببات حيث كانت قيمة (الارتباط = 0.432) ، ونجد ان الدافعية ترتبط ارتباط مع تخطيط الموارد البشري حيث كانت قيمة (الارتباط = 0.382) ، ونجد ان الدافعية ترتبط ارتباط ايجابي مع التدريب حيث كانت قيمة (الارتباط = 0.411) ، ونجد ان الدافعية ترتبط ارتباط ايجابي مع تقييم الاداء حيث كانت قيمة (الارتباط = 0.595) ، ونجد ان الفعالية ترتبط ارتباط ايجابي مع الاجور والمرتببات حيث كانت قيمة (الارتباط = 0.612) ، ونجد ان الفعالية ترتبط ارتباط ايجابي مع تخطيط الموارد البشرية حيث كانت قيمة (الارتباط = 0.656) ، ونجد ان الفعالية ترتبط ارتباط ايجابي مع التدريب حيث كانت قيمة (الارتباط = 0.659) ، ونجد ان الفعالية ترتبط ارتباط ايجابي مع تقييم الاداء حيث كانت قيمة (الارتباط = 0.539) ، ونجد ان الفعالية ترتبط ارتباط ايجابي مع الاختيار والتعيين حيث كانت قيمة (الارتباط = 0.437) ، ونجد ان الفعالية ترتبط ارتباط ايجابي مع الاستقطاب حيث كانت قيمة (الارتباط = 0.544) ، ونجد ان الفعالية ترتبط ارتباط ضعيف مع الحوافز حيث كانت قيمة (الارتباط = 0.125) ، ونجد ان الفعالية ترتبط ارتباط ايجابي مع الدافعية حيث كانت قيمة (الارتباط = 0.550) ، ونجد ان الكفاءة ترتبط ارتباط ايجابي مع الاجور والمرتببات حيث كانت قيمة (الارتباط = 0.576) ونجد ان الكفاءة ترتبط ارتباط ايجابي مع تخطيط الموارد البشرية حيث كانت قيمة (الارتباط = 0.429) ونجد ان الكفاءة ترتبط ارتباط ايجابي مع التدريب حيث كانت قيمة (الارتباط = 0.473) ونجد ان الكفاءة ترتبط ارتباط ايجابي مع تقييم الاداء حيث كانت قيمة (الارتباط = 0.548) ونجد ان الكفاءة ترتبط ارتباط ايجابي مع الاختيار والتعيين حيث كانت قيمة (الارتباط = 0.474) ونجد

ان الكفاءة ترتبط ارتباط ايجابي مع الاستقطاب حيث كانت قيمة (الارتباط = 0.415). ونجد ان الكفاءة ترتبط ارتباط ضعيف مع الحوافز حيث كانت قيمة (الارتباط = 0.216). ونجد ان الكفاءة ترتبط ارتباط ايجابي مع الفعالية حيث كانت قيمة (الارتباط = 0.567).

سادساً: إختبار علاقة مكونات إستراتيجيات الموارد البشرية و أداء العاملين :

الجدول التالي يوضح الانحدار لمكونات استراتيجيات الموارد البشرية و أداء العاملين , لقد تم استخدام (Beta coefficient) إختبار تحليل الانحدار المتعدد والذي يهدف الى التعرف على تأثير أبعاد إستراتيجيات الموارد البشرية على (أداء العاملين). تم الاعتماد على معامل (Beta) لمعرفة التغير المتوقع في المتغير التابع بسبب التغير الحاصل في وحدة واحدة من المتغير المستقل ، كما تم الاعتماد على (R^2) للتعرف على قدرة النموذج على تفسير العلاقة بين المتغيرات المستقلة والمتغير التابع ، بالإضافة إلى استخدام إختبار F لتعرف على معنوية نموذج الانحدار . وقد تم الاعتماد على مستوى الدلالة 0.05 للحكم على مدى معنوية التأثير، حيث تم مقارنة مستوى المعنوية المحتسب مع قيمة مستوى الدلالة المعتمد، وتعد التأثيرات ذات دلالة احصائية اذا كانت قيمة مستوى الدلالة المحتسب أصغر من مستوى الدلالة المعتمدة (0.05) والعكس صحيح ومن خلال تحليل الانحدار تم التوصل على انه لا توجد علاقة بين الاجور والمرتبات و الفعالية حيث بلغت بيتا (0.035) مستوى المعنوية (0.770) ، وتوجد علاقة بين تخطيط الموارد البشرية و الفعالية حيث بلغت بيتا (0.314) مستوى المعنوية (0.007)، وتوجد علاقة بين التدريب و الفعالية حيث بلغت بيتا (0.282) مستوى المعنوية (0.010)، وتوجد علاقة بين تقييم الاداء و الفعالية حيث بلغت بيتا (0.227) مستوى المعنوية (0.041)، ولا توجد علاقة بين الاختيار والتعيين و الفعالية حيث بلغت بيتا (-0.006) مستوى المعنوية (0.948) ، ولا توجد علاقة بين الاستقطاب و الفعالية حيث بلغت بيتا (0.182) مستوى المعنوية (0.063) ، وتوجد علاقة بين الحوافز و الفعالية حيث بلغت بيتا (-0.200) مستوى المعنوية (0.016) كما موضح في الجدول أدناه

جدول (3/9) يوضح العلاقة بين أبعاد إستراتيجيات الموارد البشرية و الفعالية

المتغير المستقل	الفعالية	sig
الاجور والمرتبات	.035	0.770
تخطيط الموارد البشرية	.314	0.007
التدريب	.282	0.010
تقييم الاداء	.227	0.041
الاختيار والتعيين	.006	0.948
الاستقطاب	.182	0.063
الحوافز	.200	0.016
R^2	.630	
Adjusted R^2	.590**	
ΔR^2	.630	
F change	16.756	

Note: Level of significant: * $p < 0.10$, ** $p < 0.05$, *** $p < 0.001$

المصدر إعداد الباحث من بيانات الدراسة الميدانية (2021)

جدول (3/10) يوضح العلاقة بين أبعاد إستراتيجيات الموارد البشرية و الكفاءة:

المتغير المستقل	الكفاءة	Sig
الاجور والمرتببات	.276	0.068
تخطيط الموارد البشرية	.107	0.450
التدريب	.093	0.489
تقييم الاداء	.251	0.069
الاختيار والتعيين	.260	0.038
الاستقطاب	.020	0.871
الحوافز	.019	0.849
R ²	.421	
Adjusted R ²	.363*	
Δ R ²	.421	
F change	7.176	

Note: Level of significant: *p<0.10, **p<0.05, ***p<0

المصدر إعداد الباحث من بيانات الدراسة الميدانية (2021)

من خلال الجدول اعلاه لقد تم التوصل لتحليل الانحدار على أنه لا توجد علاقة بين الاجور والمرتببات و الكفاءة حيث بلغت بيتا (.276) مستوى المعنوية (0.068) ، ولا توجد علاقة بين تخطيط الموارد البشرية و الكفاءة حيث بلغت بيتا (.107) مستوى المعنوية (0.450)، ولا توجد علاقة بين التدريب و الكفاءة حيث بلغت بيتا (.093) مستوى المعنوية (0.489)، ولا توجد علاقة بين تقييم الاداء و الفعالية حيث بلغت بيتا (.251) مستوى المعنوية (0.069)، و توجد علاقة بين الاختيار والتعيين و الكفاءة حيث بلغت بيتا (.260) مستوى المعنوية (0.038) ، ولا توجد علاقة بين الاستقطاب و الكفاءة حيث بلغت بيتا (.020) مستوى المعنوية (0.871) ، ولا توجد علاقة بين الحوافز و الكفاءة حيث بلغت بيتا (.019) مستوى المعنوية (0.849).

الخاتمة:

أولاً: النتائج

من خلال الدراسة الميدانية توصل الباحثون إلى النتائج الآتية:

1. وجود علاقة بين أستراتيجيات الموارد البشرية وأداء العاملين دعمت جزئياً.
2. وجود علاقة ذات دلالة إحصائية بين أستراتيجيات الموارد البشرية والدافعية للعاملين دعمت جزئياً.
3. وجود علاقة بين الدافعية وأداء العاملين دعمت بالكامل والدافعية تتوسط العلاقة بين إستراتيجيات الموارد البشرية و أداء العاملين تقبل التوسط جزئياً.
4. توجد علاقة ذات دلالة إحصائية بين تخطيط الموارد البشرية والكفاءة.
5. لا توجد علاقة ذات دلالة إحصائية بين الاختيار والتعيين والفعالية.

6. لا توجد علاقة ذات دلالة إحصائية بين الأجور والمرتبات والكفاءة.

7. توجد علاقة ذات دلالة إحصائية بين الحوافز والفعالية.

ثانياً: التوصيات

بناءً على النتائج التي تم التوصل إليها يوصى الباحثان بالآتي:

1. وضع مرتبات وأجور تنافسية بالمقارنة مع المستشفيات الأخرى.
2. وضع حوافز مادية ومعنوية مناسبة لتشجيع العاملين.
3. وضع إستراتيجية وخطه للإختيار والتعيين طويل الأجل تتسم بالمرونة وتراعي توفر المعارف والخبرات.
4. الاهتمام بالعنصر البشري وتدريبه بخطط تدريبية متنوعة وتنفيذها وتأهيله بصورة تضمن إلمامه بأدق تفاصيل وتقنيات عمله.
5. التركيز على العمل الجماعي وخلق فرق العمل من أجل تشارك ونقل المعرفة والمهارات بين العاملين.
6. / العمل على تقليل معدل الدوران الوظيفي من خلال أجور عادلة ومناسبة تراعي الكفاءة والخبرة والأحتفاظ بالعاملين.
7. مراعاة الجانب المعنوي للعاملين وتخوفهم من العدوي بفيروس كورونا وتعزيز جانب الحماية لهم.

المصادر والمراجع:

المصادر العربية:

- حمزة، عبد الهادي السمانى عثمان، (2013م)، أثر تنظيم الموارد البشرية علي كفاءة الأداء، بديوان الضرائب ولاية الخرطوم، مقدمة لنيل درجة الدكتوراة في الادارة العامة، جامعة الخرطوم.
- مسودة، مازن (2004م)،: أثر تطوير الموارد البشرية الصحية في تحقيق الجودة الشاملة متخذة المستشفيات الأردنية الخاصة الفترة (1995-2003) دراسة حالة، مقدمة لنيل درجة الدكتوراه من جامعة السودان.
- لصور، نضال محسن احمد (2017) بعنوان "التفاعل بين ممارسات إدارة الموارد البشرية وإدارة المعرفة وأثرها في متطلبات الجودة الشاملة: دراسة علي شركات النفط والغاز اليمنية" رسالة دكتوراة غير منشورة قسم إدارة الاعمال كلية الدراسات التجارية جامعة السودان للعلوم والتكنولوجيا.
- آدم، عباس ادم (2018) أثر نظم معلومات الموارد البشرية علي أداء المؤسسات الحكومية دراسة حالة وزارة تنمية الموارد البشرية رسالة دكتوراة إدارة عامة غير منشورة جامعة السودان للعلوم والتكنولوجيا الخرطوم.
- موسي، حامد حمد الله (2019م)، إستراتيجية ادارة الموارد البشرية وأثرها في اداء المنظمة الخرطوم - جامعة السودان - كلية التجارة - رسالة دكتوراة ادارة اعمال غير منشورة.
- أبوسن، أحمد أبراهيم، (2009م)، إدارة الموارد البشرية، شركة مطابع السودان للعملة المحدودة، الخرطوم، ط 3.

- الموسوي، سنان، (2004م)، إدارة الموارد البشرية وتأثيرات العولمة عليها، دار مجدلوي للنشر والتوزيع ، عمان، الاردن.
 - السالم، مؤيد سعيد، (2012م) إدارة الموارد البشرية - مدخل استراتيجي تكاملي، (الاردن ثراء للنشر والتوزيع.
 - حنفي، عبد الغفار ، (2007م)، السلوك التنظيمي وإدارة الموارد البشرية، الدار الجامعية، الاسكندرية، مصر .
 - زويلف، مهدي حسن (1998م)، إدارة الافراد، مدخل كمي، دار مجدلوي للنشر ، عمان، الاردن، ط 3.
 - النجار، فريد، (1998م)، إدارة الموارد ووظائف الافراد وتنمية الموارد البشرية، مؤسسة شباب الجامعة، الاسكندرية، مصر.
 - عباس، سهيلة محمد - وعلي حسنين علي، (2000م) ، إدارة الموارد البشرية، دار وائل للطباعة والنشر، الاردن، ط 1.
 - درة، عبد الباري - وزهير الصباغ، (1986م) إدارة القوي البشرية- منحنى نظمي ، دار الندوة للنشر والتوزيع، عمان، الاردن .
 - هاشم، زكي محمود ، (1996م) إدارة الموارد البشرية، ذات السلاسل، الكويت ط 2 .
 - عبد المحسن ، توفيق محمد (1997م)، تقييم الأداء، دار النهضة العربية، بيروت، لبنان.
 - مرعي، محمد(2001م)، دليل نظام التقييم في المؤسسات والادارات، دار الرضا للنشر، دمشق، سوريا.
 - المنيف، إبراهيم عبدالله (1983م) ، الإدارة : المفاهيم . الأسس . المهام (الرياض : دار العلوم للطباعة والنشر.
 - جاكسون، جون و اخرون (1988م)، نظرية التنظيم منظور كلي للادارة ، ترجمة خالد حسن زروق ، مراجعة حامد سوداي عطية ، معهد الادارة العامة ، السعودية.
 - ادريس، ثابت عبد الرحمان (2002م) ، كفاءة وجودة الخدمات اللوجيستية ، ، الدار الجامعية الإسكندرية.
 - الشماع، خليل محمد محسن ، خيضر كاظم حمود (2000م)- نظرية المنظمة، دار المسيرة عمان.
- المصادر الأجنبية:**

Randal, Schuler . S, (1995) Managing Human Resources, Fifth ed West Publishing Company, New York, ,

Pool, (1993) ,Michael, Human Resource Management in an International Perspective, the International Journal of Human Resource Management, Vol. 1.