HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير العربي للعام 2024 = 0.44

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 الاستقبال: 2025/09/07م تاريخ القبول: 2025/09/15م تاريخ النشر: 2025/10/01م

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) تقدمًا ملحوظًا في الكشف عن التهديدات والوقاية منها والاستجابة لها. وبالاستفادة 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 ادارة مخاطر الأمن السيبراني والامتثال من خلال الأطر والمعايير المعتمدة يوفر مجموعةً واسعةً من المزايا، بما في ذلك تعزيز الكفاءة، وتحسين الدقة، واتباع نهجٍ أكثر استباقية لإدارة المخاطر. بدءًا من أتمتة المهام الروتينية، وصولًا إلى التنبؤ بالمخاطر المستقبلية وضمان خصوصية البيانات، وعدم التحييز ويعزز من النزاهة والشفافية، يُحدث الذكاء الاصطناعي ثورةً في طريقة تعامل المنظمات مع الامتثال. ومع ذلك، من المهم أن الانتباه الى أن الذكاء الاصطناعي لا يُغني عن الرقابة البشرية، بل يُمثّل أداةً فعّالة تُكمّل وتُعزّز قدرات مُختصي الامتثال. ومع استمرار تطوّر البيئات التنظيمية، سيزداد دور الذكاء الاصطناعي في الامتثال بلا شك أهميةً، مما يُساعد المنظمات على التغلّب 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 فعّالة 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 إدارةِ المخاطر والامتثال لتعزيز الكفاءة والدقة والاستباقية في اتخاذ القرار. حيث تُمكّن 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 ادارة المخاطر والامتثال للأمن السيبراني. والتي قد تساعد ترسيخ الفهم المتعلق بمفهوم قدرات الذكاء الاصطناعي في تحسين فعالية أنظمة إدارة المخاطر والامتثال، وبالتالي تمكنها اللحاق بركب التطور التكنولوجي، بل بقيادة هذا الركب نحو مستقبل أكثر تنظيمًا وعدالة، واستدامة لضمان الشفافية وتحقيق الاهداف 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 دورًا محوريًا 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 الرئِيسي 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 والامن السيبراني، كما تعكسه الادبيات 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 ادارة 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 ادارة مخاطر الامن 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 التخلص، 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 والانشطة التي تهدف إلى تحديد نقاط الضعف في الموارد المرتبطة بأنظمة المعلومات والاتصال للمنظمة، وتنفيذ اجراءات وضوابط أمن سيبراني فعالة للتخفيف من الأثار السلبية لهذه الاختراقات، والتقييم الدوري للمخاطر السيبرانية، ولإدارة 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 المجلات 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 : ادارة 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 دقةً. 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، بالاضافة 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 العامين، 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 تُزيد من سرعة اكتشاف المخاطر، وتزيد من إمكانات تحليل البيانات، وتُوفر الدعم للمراقبة والتنبؤ في الوقت الفعلي. كما تناقش هذه الدراسة كيفية مساهمة الذكاء الاصطناعي في أتمتة مهام إدارة المخاطر والامتثال المتكررة، مما يُمكّن 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 التعقيد وأكثر غموضًا.

(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 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 قيّم لاستدامة المؤسسة وأساس لاتخاذ قرارات مواتية للمخاطر.

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

تهدف هذه الدراسة الى 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، يُمكّن 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 إستخدام التعلم الآلي(ML) والذكاء الاصطناعي(AI) لتحسين القدرة على الكشف عن التهديدات السيبرانية، وأتمتة مراقبة الامتثال، وتقليل نقاط الضعف في الأنظمة، كما تُقدم الدراسة نهجًا مُعززًا بالذكاء الاصطناعي لتقييم مخاطر الأمن السيبراني في الحوسبة السحابة 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، كانخفاض تكاليف التدقيق، وتحسين حوكمة الأمن السيبراني، وتسريع إعداد التقارير التنظيمية. كما تشير النتائج إلى ضرورة استخدام تطبيقات الذكاء الاصطناعي لتأمين بيئات الحوسبة السحابة، 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 نموذجًا شاملًا لإطار حوكمة يدمج أدوار وقواعد الذكاء الاصطناعي، والأمن، والامتثال، والإدارة بهدف تعزيز فعالية عمليات الحوسبة السحابة للمنظمة. و يلعب الذكاء الاصطناعي دورًا حاسمًا في تحسين تخصيص الموارد وتحسين عمليات صنع القرار في إطار حوكمة الحوسبة السحابة. 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 أمرًا أساسيًا لضمان المساءلة التنظيمية وتقليل المخاطر القانونية. يتضمن نموذج الحوكمة المُقترح عمليات تحقق امتثال مؤتمته 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 الى أن فعالية حوكمة الحوسبة السحابية تتجلى في المكونات الأساسية للذكاء الاصطناعي، والأمن، والامتثال، والإدارة. ويلعب الذكاء الاصطناعي دورًا محوريًا 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 بحثًا 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. و تشير 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 دقةً. 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، بالاضافة 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 العامين، 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 تُزيد من سرعة اكتشاف المخاطر، وتزيد من إمكانات تحليل البيانات، وتُوفر الدعم للمراقبة والتنبؤ في الوقت الفعلي. كما تناقش هذه الدراسة كيفية مساهمة الذكاء الاصطناعي في أتمتة مهام إدارة المخاطر والامتثال المتكررة، مما يُمكّن 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 التعقيد 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 قيّم لاستدامة المؤسسة وأساس لاتخاذ قرارات مواتية للمخاطر.

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

تهدف هذه الدراسة الى 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، يُمكّن 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 إستخدام التعلم الآلي(ML) والذكاء الاصطناعي(AI) لتحسين القدرة على الكشف عن التهديدات السيبرانية، وأتمتة مراقبة الامتثال، وتقليل نقاط الضعف في الأنظمة، كما تُقدم الدراسة نهجًا مُعززًا بالذكاء الاصطناعي لتقييم مخاطر الأمن السيبراني في الحوسبة السحابة 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، كانخفاض تكاليف التدقيق، وتحسين حوكمة الأمن السيبراني، وتسريع إعداد التقارير التنظيمية. كما تشير النتائج إلى ضرورة استخدام تطبيقات الذكاء الاصطناعي لتأمين بيئات الحوسبة السحابة، 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 نموذجًا شاملًا لإطار حوكمة يدمج أدوار وقواعد الذكاء الاصطناعي، والأمن، والامتثال، والإدارة بهدف تعزيز فعالية عمليات الحوسبة السحابة للمنظمة. و يلعب الذكاء الاصطناعي دورًا حاسمًا في تحسين تخصيص الموارد وتحسين عمليات صنع القرار في إطار حوكمة الحوسبة السحابة. 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 أمرًا أساسيًا لضمان المساءلة التنظيمية وتقليل المخاطر القانونية. يتضمن نموذج الحوكمة المُقترح عمليات تحقق امتثال مؤتمته 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 الى أن فعالية حوكمة الحوسبة السحابية تتجلى في المكونات الأساسية للذكاء الاصطناعي، والأمن، والامتثال، والإدارة. ويلعب الذكاء الاصطناعي دورًا محوريًا 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 بحثًا 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. و تشير 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 (AI) Artificial Intelligence هو أحد فروع علم الحاسوب، وإحدى الركائز الأساسية التي تقوم عليها صناعة التكنولوجيا في العصر الحالي (مقاتل و حسني،2021). وقد عرَّفت 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 الإصطناعي 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 الاضرار 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 وتعلُّم 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 او 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. سواءً 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 مصمّم 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 بحثًا عن الثغرات الأمنية من خلال مراقبة حركة مرور الشبكة واستخدام قواعد مُحددة مسبقًا. 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 الى 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 فعّالة 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 والانسان 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 مهامًا مثل تصنيف النصوص، وتحليل المشاعر، وترجمة اللغات، والإجابة على الأسئلة، وتطوير روبوتات الدردشة. وتُعد معالجة اللغة الطبيعية في مجال الأمن السيبراني أداة فعّالة لتعزيز كشف الاحتيال ومنعه. فهي تُمكّن الأنظمة من معالجة وتحليل البيانات النصية غير المُهيكلة، 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 قويًا لأنشطة احتيالية. وهذا يُتيح لمحللي الاحتيال فهمًا أفضل للمخاطر المحتملة، ما يسمح بإجراء تقييمات أكثر إستهدافًا 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 حدتها. 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 المُخترقة، 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 يُمكّن 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 او 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، بالاضافة الى ما يشمله 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 قدمًا بثقة في العصر الرقمي. وتتمثل الأهداف العامة الأمن 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 يعتبرونا 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 نظماً موصولة بالإنترنت".

حيث تشمل أنواع التهديدات السيبرانية أشكالًا، 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 متخفية على شكل برامج شرعية، وبمجرد تثبيتها، تسمح بالوصول غير المصرح به إلى النظام المصاب.
• **برامج التجسس(Spyware):** هي برامج تراقب وتجمع المعلومات سرًا 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 ملفقًا 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 هجومًا 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 مهاجمًا يقوم بتضمين نص JavaScript ضار لاستهداف قاعدة بيانات موقع الويب. أو من خلال **هجمات الحقن** (SQL Injection) SQLi, 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 او تعطيل الخدمة بشكل كلي.(Amod, 2024).

- **إدارة مخاطر الأمن السيبراني**

عَرّف 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 الى تحديد مخاطر الأمن السيبراني الكامنة، وتقييم الأثر، والاحتمالية، وتحديد خطط التعامل مع هذه المخاطر بحيث يجري اتخاذ قرار التعامل وفقًا 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). ويُظهر الشكل(1) مراحل منهجية ادارة مخاطر الأمن السيبراني:

شكل (1): مراحل منهجية ادارة مخاطر الأمن السيبراني

المصدر: من تصميم الباحث

وتشمل المنهجية أيضاً الاجراءات اللازمة للتعامل مع المخاطر المحتملة، واستخدام ادوات ومعايير لقياس وتقييم الفعالية في ادارة المخاطر، بالاضافة الى تحديد الاحداث المحتمل مواجهتها اثناء تطبيق استراتيجيات ادارة 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 وفقًا لتهديدات الأمن السيبراني المحتملة، وثغرات الأمن السيبراني؛ وذلك بهدف تحديد مخاطر الأمن السيبراني الكامنة. كما يتم تحديد الضوابط المطبقة حاليًا؛ 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 دوريًا، 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. فنطاق الامتثال للأمن السيبراني واسع ومتعدد الأوجه، ويشمل مجموعة واسعة من الأنشطة والسياسات والضوابط التي تساهم مجتمعة في بيئة معلومات آمنة. وغالبًا 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 سواءً 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

التهديدات المحتملة ورصدها والتخفيف من حدتها. حيث تساعد هذه الأطر المنظمات على تنفيذ استراتيجية أمنية استباقية، وإدارة المتطلبات التنظيمية والعمليات. وتُمكّن 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)	NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), CYBERSECURITY FRAMEWORK (CSF)	يُعدّ(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	ISO/IEC 27001& 27002	تُركز ISO–27001 على تطوير إطار إداري شامل، بينما تُقدم ISO–27002 إرشاداتٍ حول تطبيق الضوابط. وتوفر هذه المعايير مجتمعةً إدارةً مُهيكلةً للمخاطر تتماشى مع أهداف المنظمة(FADDOM,2025).
حماية البنية التحتية الحيوية لشركة موثوقية الكهرباء في أمريكا الشمالية	The North American Electric Reliability Corporation's Critical Infrastructure Protection (NERC–CIP)	تُوفر هذه الضوابط مجموعة من الإجراءات ذات الأولوية لحماية المؤسسات من المخاطر السيبرانية المعروفة. وتُقدم 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	Control Objectives for Information and Related Technology (COBIT)	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	Cloud Control Matrix	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).
اسم الاطار		الغاية منه
إطار عمل اللائحة العامة لحماية البيانات	General Data Protection Regulation(GDPR)	وهي إطار لتعزيز إجراءات وممارسات حماية البيانات لمواطني الاتحاد الأوروبي. وتشمل هذه اللائحة على جميع المؤسسات المُنشأة في الاتحاد الأوروبي، أو أي شركة تجمع وتخزن البيانات الخاصة بمواطني الاتحاد الأوروبي (Faddom,2025).
قانون إدارة أمن المعلومات الفيدرالي	The Federal Information Security Management Act (FISMA)	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 المعيارعلى تحسين حماية البيانات الحكومية من خلال وضع معايير أمنية إلزامية (Faddom,2025).
قانون نقل التأمين الصحي والمساءلة	Health Insurance Portability and Accountability Act (HIPAA)	هو إطار عمل للأمن السيبراني يُلزم مؤسسات الرعاية الصحية بتطبيق ضوابط لتأمين وحماية خصوصية المعلومات الصحية الإلكترونية (Pansy, 2024).
الامتثال لمعايير SOC 2	System and Organization Controls 2 (SOC 2)	هو إطار عمل يركز على ضمان إدارة مزودي الخدمات للبيانات بأمان لحماية خصوصية عملائهم (Faddom,2025).
معيار تحالف ثقة المعلومات الصحية	Health Information Trust Alliance (HITRUST)	يوفر هذا المعيار ضمان الامتثال للوائح الرعاية الصحية المعقدة. كما توفير إرشادات لحماية السجلات الصحية الإلكترونية وإدارة خصوصية البيانات (Mulugeta, Henock, 2023).
شهادة نموذج نضج الأمن السيبراني	Cybersecurity Maturity Model Certification (CMMC)	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).

- **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؛ تدرك المنظمات الفوائد الجمة التي يمكن أن يقدمها الامتثال لأمن المعلومات وخاصة المتعلق بالأمن السيبراني. وسنذكر أهم مزايا الامتثال للأمن السيبراني في المنظمات وعلى النحو التالي. (حمود،2021):

- ❖ يُساعد المنظمة على تجنب الغرامات والعقوبات.
- ❖ يَحمي 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 مهمةً 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 يوميًا .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 تُحليل كميات كبيرة من البيانات وتُحدد الأنماط التي تشير إلى وجود تهديد. كما يُستخدم التعلم العميق (DL) بهدف التعرف على البرامج الضارة، وعمليات التصيد الاحتيالي وغيرها من التهديدات الإلكترونية وتصنيفها. بالاضافة الى استخدام معالجة اللغة الطبيعية (NLP) لتحليل مصادر البيانات غير المنظمة، مثل مواقع التواصل الاجتماعي والمنتديات 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 لادارة مخاطر الأمن السيبراني

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

- **الأتمتة في تقييم مخاطر الأمن السيبراني:** تستخدم المنظمات بشكل متزايد خوارزميات الذكاء الاصطناعي لتقييم المخاطر تلقائيًا، 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 الى 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 الأتمتة 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) تفسيرَ المفردات القانونية المعقدة، وتساعد على استخراج البيانات ذات الصلة، وتضمن امتثال المنظمات. كما تُسهّل عملية الامتثال التنظيمي بجعلها أكثر كفاءةً 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) انه يتم تحويل نصوص الامتثال إلى نصوص قابلة للقراءة آليًا؛ وذلك بهدف المساعدة على فهم نموذج الذكاء الاصطناعي وتطبيقه تلقائيًا. حيث يُمكن لمكاتب التحقق من لوائح الامتثال المحددة بشكل متكرر دون الحاجة إلى إشراف دقيق، مما يُقلل من الأخطاء البشرية، وبالتالي يُؤثر ذلك إيجابًا على أداء المنظمة.
- **الامتثال التنبئي:** 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 حسّن كفاءة حوكمة الشركات من 59.2% إلى 73.6%، وخفض حالات فشل الامتثال بنسبة 37%، وخفض التكاليف القانونية بنسبة 0.95%. 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 الالة (ML)	70	80
معالجة اللغة الطبيعية (NLP)	60	70
أتمتة العمليات الروبوتية(Robotic Process Automation ,RPA)	40	50
التحليلات التنبؤية(Predictive Analytics)	45	55

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

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

تطبيق الذكاء الاصطناعي	التأثير على إدارة المخاطر	النتيجة الإحصائية
لغة الالة (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 ادارة الامتثال لادارة المخاطر الأمن السيبراني وعلى النحو التالي:**

- يمكن لأطر الامتثال الاستفادة من تقنيات الذكاء الاصطناعي، فالأدوات المصممة لتحليل المتطلبات التنظيمية تساعد المؤسسات على مواءمة 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 يُمكّن المنظمات من الاستجابة السريعة للتهديدات المحتملة.
- تطبيق المراقبة المستمرة من خلال خوارزميات الذكاء الاصطناعي التي تُحدد المخالفات فورًا. حيث تشهد المنظمات التي تستخدم الذكاء الاصطناعي للمراقبة المستمرة للامتثال انخفاضًا 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:

بإستقراء الادبيات (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 او 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.

اولاً: 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) يُحسّن 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 فرصةً 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، يوصـى 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 اسلوب أتمتة مراحل الامتثال لادارة 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 لامنهجية 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 بجد 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), 851-902. Doi: 10.21608/sjsc.2025.370124.1576.

حسان، ساره.(يونيو 1, 2025).علم الآلة Machine Learning – مفتاح التطور التكنولوجي.اكاديمية 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. 1341-1362. 10.21608/ejos.2025.422622.

كامل ،عبد الرحمن. (2025). استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة: تحليل الممارسات الدولية واستشراف التحديات المستقبلية. المجلة العربية للدراسات الأمنية, *41*(1), 04-16. https://doi.org/10.26735/CXSD7939.

مركز إيداع الأوراق المالية.(ب.ت). ادارة 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), 283–357. doi: 10.21608/jdl.2023.192966.1119.

الصياد، مي؛ والسالم، وفاء.(2023). دور الذكاء الاصطناعي في تطوير مهارات البحث العلمي لدى طالبات كلية التربية بجامعة الملك سعود، مجلة البحوث التربوية والنوعية. (19)، (288–247).

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 /21–20ديسمبر/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، مجلد1 (1) . https://doi.org/10.47340/MJEAS.V1I1.2.2020.

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.

ShaikhMuhammad, 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/ijsrtm.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.