Journal of Insights in Basic and Applied Sciences

Volume 2, Issue 2, 2026, Pages: 344-361

Journal homepage: https://jibas.com.ly/index.php/jibas/en

The Integrative Role of Mathematics in Information Security, Mathematical Modeling and Decision Support through Information Systems

Prof. Ibtisam Mustafa Sasi[1 *], Prof. Atiqa Milad Mahmoud Mousa AlZawam [2], Prof. Iman Salem Khalifa Qashout [3]

[1,2] Department of General Sciences, Faculty of Natural Resources, Al-Ajilat, University of Zawia, Zawia, Libya

[3] Department of Computer Science, Faculty of Science, Rigdaleen, Sabratha University, Sabratha, Libya

الدور التكاملـي للرياضيات في أمن المعلومات والنمذجة الرياضية ودعم اتخاذ القرار عبر نظم المعلومات

أ. ابتسام مصطفى ساسي[1*]، أ.عتيقة ميلاد محمود موسي الزوام [2]، أ. ايمان سالم خليفة قشوط [3]

[2،1] قسم العلوم العامة، كلية الموارد الطبيعية العجيلات، جامعة الزاوية، الزاوية، ليبيا

[3] قسم الحاسوب، كلية العلوم رقدالين، جامعة صبراته، صبراته، ليبيا

[*]Corresponding author: ab.sasi@zu.edu.ly

Received: April 20, 2026	Accepted: May 28, 2026	Published: June *25*, 2026

Abstract

Contemporary institutions face increasing challenges in managing information risks due to the growing complexity of digital environments and the diversity of threat sources, in this context, an important question emerges regarding the actual role of mathematics in strengthening information security and improving the quality of related decisions, this research addresses this issue by analyzing the structural relationship between mathematics, information security, mathematical modeling and decision support systems.

The research adopts a descriptive-analytical approach to examine the mathematical foundations underlying digital protection mechanisms, it explains how mathematical models are used to measure and analyze risks and explores the role of decision support systems in transforming quantitative results into comparable decision alternatives, the analysis focuses on the transition from qualitative risk assessment to quantitative approaches based on probability theory and optimization models, which help reduce uncertainty and enhance the objectivity of security decisions.

The findings indicate that the integration of mathematical analysis, risk management and modeling contributes to improving the efficiency of information systems by reorganizing decision-making processes within a structured quantitative framework, the research also concludes that mathematical modeling represents a central mechanism for linking security data

with institutional decision environments, thereby reducing bias and supporting rational decision-making.
The paper proposes an integrative conceptual framework that clarifies the interaction among these components within a unified analytical system, this framework provides a scientific basis for developing quantitative models that can be applied and tested in future research.

Keywords: Mathematics, Information Security, Mathematical Modeling, Risk Analysis, Decision Support Systems.

الملخص

تواجه المؤسسات المعاصرة تحديات متزايدة في إدارة المخاطر المعلوماتية نتيجة التعقيد المتنامي للبيئات الرقمية وتعدد مصادر التهديد، وفق هذا السياق، يبرز التساؤل حول الدور الحقيقي للرياضيات في تعزيز فعالية أمن المعلومات وتحسين جودة القرارات المرتبطة به، يعالج هذا البحث هذه الإشكالية من خلال تحليل العلاقة البنيوية بين الرياضيات وأمن المعلومات والنمذجة الرياضية ونظم دعم القرار.

اعتمد البحث المنهج الوصفي التحليلي بهدف تفكيك الأسس الرياضية التي تقوم عليها آليات الحماية الرقمية وبيان كيفية توظيف النماذج الرياضية في قياس المخاطر وتحليلها ثم استكشاف دور نظم دعم القرار في تحويل النتائج الكمية إلى بدائل قابلة للمفاضلة، وركز التحليل على الانتقال من المقاربة النوعية للمخاطر إلى المقاربة الكمية القائمة على الاحتمالات ونماذج التحسين بما يسمح بتقليل الغموض وتعزيز موضوعية الاختيار الأمني.

توصل البحث إلى أن التكامل بين التحليل الرياضي وإدارة المخاطر والنمذجة يسهم في رفع كفاءة نظم المعلومات عبر إعادة تنظيم عملية اتخاذ القرار في إطار كمي منضبط، كما خلص إلى أن النمذجة تمثل آلية مركزية لربط البيانات الأمنية ببيئة القرار المؤسسي، بما يحد من التحيز ويعزز الرشادة.

يقترح البحث إطارًا مفاهيميًا تكامليًا يوضح آلية التفاعل بين هذه المكونات ضمن منظومة تحليلية واحدة، ويوفر أساسًا علميًا لتطوير نماذج كمية قابلة للتطبيق في الدراسات المستقبلية.

الكلمات المفتاحية: الرياضيات، الأمن المعلوماتي، النمذجة الرياضية، تحليل المخاطر، دعم القرار.

الفصل الأول: الإطار العام والمنـهجي

1.1 المقدمة

في العقود الأخيرة، شهد العالم تحولاً رقمياً سريعاً غيّر بشكل جذري طريقة عمل المؤسسات والمجتمعات. أصبحت أنظمة المعلومات حالياً العمود الفقري لإدارة البيانات وتشغيل العمليات واتخاذ القرارات الاستراتيجية، مما جعل أمن المعلومات وكفاءة دعم القرار من أهم التحديات في عصرنا الرقمي.

لكن الرياضيات هنا ليست مجرد نظرية معقدة بعيدة عن الواقع، بل هي الأساس الذي تقوم عليه كل هذه الأنظمة: من الخوارزميات والتشفير إلى نماذج التحليل والتنبؤ، فمثلا التشفير الحديث الذي نستخدمه يومياً في حماية بياناتنا يعتمد على نظرية الأعداد والجبر، أنظمة التشفير الشهيرة مثل (RSA) تعتمد على صعوبة تحليل الأعداد الكبيرة إلى عواملها الأولية، بينما التشفير بالمنحنيات الإهليلجية يستخدم بنى جبرية متقدمة لحماية اتصالاتنا، باختصار، أمن المعلومات ليس فقط إجراءً تقنياً، بل هو تطبيق مباشر للرياضيات الدقيقة.

من ناحية أخرى، تساعدنا النمذجة الرياضية على فهم المشكلات الواقعية وتحويلها إلى صيغ قابلة للتحليل، من خلال النماذج الرياضية، نستطيع وصف العلاقات بين مختلف العوامل، محاكاة السيناريوهات المستقبلية وتقليل الغموض عند اتخاذ قرارات معقدة، أنظمة دعم القرار تعتمد بشكل كبير على التحليل الإحصائي، نماذج التحسين ونظريات الاحتمال لتحسين جودة القرارات وتقليل المخاطر.

إذاً، العلاقة بين الرياضيات وأمن المعلومات والنمذجة ودعم القرار ليست مجرد علاقة جانبية، بل هي تكامل عميق، الرياضيات هي القاعدة النظرية التي تبنى عليها حمايتنا الرقمية وأدوات التحليل ونماذج اتخاذ القرار، لهذا السبب، من المهم دراسة هذا الدور التكاملي وفهم أبعاده النظرية والتطبيقية بشكل منهجي.

1.2 الدراسات السابقة

الدراسة الأولى بعنوان :

"Mathematical Approaches Transform Cybersecurity from Protoscience to "Science، والمنشورة في مجلة "Applied Sciences":

هدفت دراسة (Trenchev et al., 2023) إلى تحليل مدى إسهام المناهج الرياضية في تحويل الأمن السيبراني من مجال تطبيقي قائم على الخبرة إلى علم منظم يستند إلى أسس منهجية واضحة. اعتمد الباحثون المنهج التحليلي الاستقرائي من خلال مراجعة الأدبيات الرياضية المرتبطة بالأمن السيبراني، مع التركيز على نظريات مثل نظرية الألعاب، والسلاسل الماركوفيّة، ونظرية الكوارث، ونماذج التحسين الرياضي.

توصلت الدراسة إلى أن استخدام الأطر الرياضية يسهم في توصيف التفاعلات بين المهاجم والمدافع بصورة كمية، كما يساعد في بناء نماذج تنبؤية تقلل من درجة عدم اليقين، وتعزز من كفاءة أنظمة الحماية الرقمية. وأكدت النتائج أن غياب التكامل الرياضي المنهجي يُضعف القدرة على تطوير نظريات أمنية قابلة للتحقق العلمي.

يستفيد البحث الحالي من هذا الطرح في تأكيد أن الرياضيات تمثل بنية تأسيسية لأمن المعلومات، وأن إدماجها ضمن إطار تكاملي مع النمذجة ودعم القرار يعد ضرورة علمية لتطوير نظم المعلومات المعاصرة.

- **الدراسة الثانية بعنوان:**

"Advanced mathematical modeling of mitigating security threats in smart grids through deep ensemble model"، والمنشورة في مجلة "Scientific Reports":

هدفت دراسة (Sharaf et al., 2024) إلى تطوير نموذج رياضي متقدم للتخفيف من التهديدات الأمنية في شبكات الكهرباء الذكية (Smart Grids)، من خلال تصميم نموذج كشف تسلل قائم على التعلم العميق التجميعي(Deep Ensemble Learning) مدعوم بخوارزميات تحسين رياضية، اعتمدت الدراسة منهجاً تجريبياً قائماً على النمذجة الرياضية وتحليل البيانات، حيث تم توظيف خوارزمية Mountain Gazelle Optimization (MGO) لاختيار الخصائص المثلى، إلى جانب استخدام ثلاث نماذج تصنيف عميق هي: LSTM، وAutoencoder Deep، وExtreme Learning Machine، مع ضبط المعاملات باستخدام خوارزمية Dung Beetle Optimizer (DBO).

أظهرت النتائج التجريبية تفوق نموذج (MGODEL-ID) المقترح مقارنة بعدة نماذج تقليدية مثل ANNوSVM وRandom Forest، حيث حقق دقة بلغت (98.31%)، إضافة إلى تحسن واضح في مؤشراتPrecision وRecall وF1-Score، كما بيّنت الدراسة أن الدمج بين النمذجة الرياضية وخوارزميات التحسين والتعلم العميق يسهم في تعزيز كفاءة نظم كشف التسلل وتقليل المخاطر الأمنية في البيئات السيبرانية المعقدة.

يستفاد من هذا العمل في تأكيد أهمية التكامل بين الأسس الرياضية المتقدمة وتقنيات الذكاء الاصطناعي في بناء أنظمة معلومات أكثر أمانًا، كما تعزز الطرح القائل بأن الرياضيات تمثل الإطار البنيوي الذي تقوم عليه نماذج الأمن ودعم القرار في النظم الحديثة.

- **الدراسة الثالثة بعنوان:**

"Impact of Mathematical Models in IT System Design and Optimization"، والمنشورة في المجلة الدولية لتقنية المعلومات والبحوث والتطبيقات (IJITRA)":

هدفت دراسة (Veeranan et al., 2024) إلى تحليل أثر النماذج الرياضية في تصميم أنظمة تقنية المعلومات وتحسين أدائها، مع التركيز على دور أدوات التحسين الرياضي في رفع كفاءة الأنظمة وتقليل التكلفة التشغيلية عبر دورة حياة النظام، اعتمدت الدراسة منهجاً تحليلياً مفاهيمياً مدعوماً بأمثلة تطبيقية

ودراسات حالة، حيث تناولت أنواع النماذج الرياضية (الحتمية، الاحتمالية، والإرشادية)، إضافة إلى تقنيات التحسين مثل البرمجة الخطية، والخوارزميات الجينية، والمحاكاة الحرارية، ونظرية الطوابير.

أوضحت الدراسة أن النماذج الرياضية تسهم في تبسيط الأنظمة المعقدة، وتمكين المصممين من التنبؤ بسلوك النظام قبل التنفيذ الفعلي، كما تساهم في تحسين تخصيص الموارد وتقليل زمن التوقف والأخطاء التشغيلية، وأكدت النتائج أن دمج تقنيات التحسين مع النماذج الرياضية يؤدي إلى رفع كفاءة النظام بنسبة ملحوظة، خاصة في تطبيقات الشبكات، وتخطيط السعة، وجدولة القوى العاملة.

كما أبرزت الدراسة أهمية الحفاظ على النماذج الرياضية خلال دورة حياة النظام لضمان التحسين المستمر، مشيرة إلى أن ما بين 60%-80% من أنشطة نظم المعلومات تتركز في الدعم والصيانة، مما يجعل النمذجة أداة استراتيجية طويلة المدى وليست أداة تصميم أولي فقط.

يستفاد من هذا العمل في تعزيز البعد المتعلق بالنمذجة الرياضية داخل نظم المعلومات، وربطه بدعم اتخاذ القرار وتحسين الأداء المؤسسي، بما يدعم الطرح التكاملـي للرياضيات في البيئة الرقمية.

- **الدراسة الرابعة بعنوان:**

"Dealing with uncertainty in cybersecurity decision support"، والمنشورة في مجلة "Computers & Security":

هدفت دراسة (Zhang & Malacaria, 2025) إلى معالجة إشكالية عدم اليقين في نماذج دعم اتخاذ القرار في الأمن السيبراني، خاصة فيما يتعلق بعدم دقة مقاييس فعالية أدوات الحماية. انطلقت الدراسة من فرضية أن مقاييس الأمن السيبراني تعتمد بدرجة كبيرة على تقديرات خبراء، وأن غياب الدقة الكمية قد يؤدي إلى نتائج غير مستقرة في نماذج الاستثمار الأمني، اعتمد الباحثان نموذج الرسم البياني الاحتمالي للهجمات (Probabilistic Attack Graphs) لتمثيل سيناريوهات التهديد، ودمجا ذلك بإطار ألعاب ستاكلبرغ(Stackelberg Games) لتمثيل التفاعل بين المهاجم والمدافع. كما قدّما نموذجين لمعالجة عدم اليقين هما:

1. **Minmax Regret** المستند إلى منهجية التحسين المتين (Robust Optimization)، والذي يهدف إلى تقليل أقصى ندم محتمل عبر جميع السيناريوهات.
2. **Min-Product of Risks**، وهو نموذج مقترح يهدف إلى تقليل حاصل ضرب المخاطر عبر جميع السيناريوهات، بما يوفر توازناً أفضل بين الأداء والمتانة الإحصائية.

أظهرت النتائج التجريبية من خلال محاكاة متعددة لرسوم هجوم عشوائية وبأحجام مختلفة أن نموذج (Min-Product) يحقق متوسط مخاطر أقل مقارنةً بنموذج (Minmax Regret)، مع أداء حسابي أكثر كفاءة في معظم الحالات، كما بيّنت الدراسة أن النموذج المقترح أكثر ملاءمة للقرارات متعددة الأبعاد، مثل قرارات الاستثمار في أمن إنترنت الأشياء (IoT).

يستفيد البحث الحالي من هذا العمل في تأكيد أهمية إدماج أدوات التحسين الرياضي المتين ضمن نظم دعم القرار الأمني، كما تعزز الطرح القائل بأن الرياضيات لا تقتصر على بناء نماذج تحليلية، بل تؤدي دوراً محورياً في تحقيق التوازن بين الدقة والمرونة في بيئات عدم اليقين.

1.3 مشكلة البحث

على الرغم من التقدم التقني المتسارع في مجال نظم المعلومات، وما صاحب ذلك من تطور ملحوظ في أدوات الحماية الرقمية وأنظمة دعم القرار، إلا أن كثيراً من الدراسات تتناول هذه المجالات بصورة منفصلة؛ إذ يبحث أمن المعلومات غالباً من زاوية تقنية بحتة، بينما تُعالج النمذجة الرياضية ضمن سياقات تحليلية مستقلة، ويُنظر إلى نظم دعم القرار باعتبارها أدوات إدارية أو معلوماتية منفصلة عن جذورها الرياضية، هذا الفصل المعرفي يُضعف الفهم الشامل لطبيعة الترابط البنيوي بين هذه المكونات، ويؤدي إلى معالجة جزئية لمشكلات معقدة بطبيعتها.

لذا تكمن الإشكالية الجوهرية في غياب إطار تكاملي يوضح بصورة منهجية كيف تسهم الرياضيات، بوصفها بنية معرفية أساسية في بناء أنظمة آمنة ونماذج تحليلية دقيقة وآليات فعّالة لدعم اتخاذ القرار داخل

نظم المعلومات، فبينما تؤكد الأدبيات أن الخوارزميات الأمنية تستند إلى نظريات رياضية متقدمة وأن النماذج الكمية تمثل أساس التحليل واتخاذ القرار الرشيد، فإن الربط المنهجي بين هذه الأبعاد لا يزال محدوداً في كثير من الطروحات العربية، خاصة في سياق الدراسات التكاملية.

ومن ثم، ينطلق هذا البحث من التساؤل الرئيس الآتي:

سـ) ما طبيعة الدور التكاملـي الذي تؤديه الرياضيات في تعزيز أمن المعلومات، وتطوير النمذجة الرياضية، ودعم اتخاذ القرار عبر نظم المعلومات؟

ويتفرع عن هذا التساؤل عدد من الأسئلة الفرعية، من أبرزها:

1. كيف تشكل الأسس الرياضية قاعدة نظرية لأنظمة أمن المعلومات الحديثة؟
2. ما موقع النمذجة الرياضية في تحليل المخاطر وتقليل عدم اليقين داخل نظم المعلومات؟
3. كيف تسهم الأدوات الرياضية في تحسين كفاءة نظم دعم اتخاذ القرار؟
4. ما ملامح الإطار التكاملـي الذي يربط بين هذه المكونات في بنية واحدة مترابطة؟

1.4 أهداف البحث

يهدف هذا البحث إلى تجاوز الطرح الوصفي المجزأ، والانتقال إلى تحليل تكاملي يبرز مركزية الرياضيات في البنية المعرفية لنظم المعلومات الحديثة، ويعزز من فهم طبيعة العلاقة بين الأمن والتحليل الكمي والقرار المؤسسي الرشيد:

1. تحليل الأسس الرياضية التي يقوم عليها أمن المعلومات المعاصر.
2. بيان دور النمذجة الرياضية في توصيف المشكلات المعلوماتية وتحليلها.
3. توضيح العلاقة بين الأدوات الرياضية ونظم دعم اتخاذ القرار.
4. بناء إطار مفاهيمي تكاملي يبرز الترابط البنيوي بين الرياضيات وأمن المعلومات والنمذجة ودعم القرار عبر نظم المعلومات.

1.5 أهمية البحث

تنبع أهمية هذا البحث من كونه يتناول تقاطعاً معرفياً دقيقاً بين ثلاث مجالات رئيسة تشكل الركيزة الأساسية للتحول الرقمي المعاصر، وهي: أمن المعلومات، والنمذجة الرياضية، ونظم دعم اتخاذ القرار، وفي ظل التوسع المتسارع في الاعتماد على نظم المعلومات في إدارة العمليات المؤسسية واتخاذ القرارات الاستراتيجية، أصبحت الحاجة ملحّة إلى إطار علمي يوضح البنية الرياضية التي تستند إليها هذه النظم، ويكشف طبيعة العلاقة التكاملية بين مكوناتها.

تكمن الأهمية النظرية للبحث في سعيه إلى تجاوز الطرح الجزئي الذي يتناول كل مجال بصورة منفصلة، وذلك من خلال بناء تصور تكاملي يبرز الدور البنيوي للرياضيات في تصميم آليات الحماية الرقمية، وتحليل المخاطر، وتطوير النماذج الكمية الداعمة للقرار.

أما من الناحية التطبيقية، فتبرز أهمية البحث في إظهار كيفية توظيف الأدوات الرياضية في رفع كفاءة نظم أمن المعلومات وتقليل المخاطر التشغيلية، إضافة إلى تحسين جودة القرارات المؤسسية من خلال نماذج كمية أكثر دقة وموضوعية، كما يسهم البحث في توجيه صناع القرار نحو تبني مقاربات تحليلية قائمة على النمذجة والتحسين بدلاً من الاعتماد على التقديرات الحدسية أو الخبرة غير المنهجية.

1.6 منهج البحث

يعتمد هذا البحث على المنهج الوصفي التحليلي بوصفه منهجاً ملائماً لدراسة الظواهر العلمية ذات الطابع النظري والتكاملي، حيث يتيح هذا المنهج استعراض الأدبيات العلمية الحديثة وتحليلها بصورة نقدية منظمة، بهدف استخلاص العلاقات البنائية بين مفاهيم الدراسة وبناء إطار مفاهيمي متكامل.

1.7 حدود البحث

الحدود الموضوعية: ينحصر البحث في تحليل الدور التكاملي للرياضيات في ثلاث مجالات محددة، هي: أمن المعلومات، والنمذجة الرياضية، ونظم دعم اتخاذ القرار عبر نظم المعلومات، ولا تتناول الدراسة الجوانب التقنية التفصيلية الخاصة ببناء الخوارزميات البرمجية أو تنفيذ أنظمة أمنية فعلية، كما لا تدخل في تحليل برمجي تطبيقي لأنظمة محددة، بل تركز على البنية النظرية والتحليلية التي تؤسس لهذا التكامل.

الحدود الزمنية: تقتصر مراجعة الأدبيات على الدراسات الحديثة المنشورة خلال الفترة (2015–2025)، وذلك لضمان مواكبة التطورات المتسارعة في مجالات الأمن السيبراني وتقنيات النمذجة والتحسين الرياضي.

الحدود التطبيقية: يركز البحث على نظم المعلومات في السياق المؤسسي العام، دون تخصيصها لقطاع بعينه (مثل القطاع المصرفي أو الصناعي أو الصحي)، وذلك بهدف بناء إطار عام قابل للتكييف في بيئات متعددة.

الفصل الثاني: الإطار المفاهيمي والنظري

2.1 الرياضيات كأساس علمي لنظم المعلومات

أولاً: المفاهيم الرياضية الأساسية:

تعد الرياضيات البنية المعرفية التي تقوم عليها نظم المعلومات الحديثة، إذ تشكل الإطار المنطقي الذي تُبنى من خلاله الخوارزميات، وقواعد البيانات وآليات المعالجة الرقمية، فكل عملية معلوماتية بدءاً من تخزين البيانات وحتى تحليلها واسترجاعها، تعتمد على نماذج رياضية ضمنية تنظم العلاقات بين المتغيرات وتحدد آليات التحويل والمعالجة.

ومن أبرز المفاهيم الرياضية التي تمثل أساساً لنظم المعلومات ما يلي:

1. **المنطق الرياضي**: كما عرفه الفندي تعريفا وصفيا بأنه نظرية استنباطية لقوانين الاستنباط، أو أنه علم الاستنباطات التي تعرض استنباطيا، أو على نحو أكثر تفصيلا: "نظرية حسابية موضوعها قوانين الاستنباط التي تتوصل اليها النظرية استنباطيا (أي بالبرهان)" (الفندي، 1972، ص. 119).
   وهو يستخدم في بناء أنظمة الاستدلال وتصميم لغات البرمجة وبناء قواعد البيانات العلائقية، ويُعد المنطق الثنائي (Boolean Logic) حجر الأساس في تصميم الدوائر الرقمية وأنظمة المعالجة.
2. **نظرية المجموعات والعلاقات:** تعتمد قواعد البيانات العلائقية على مفاهيم المجموعات والعلاقات الرياضية، وهو ما أرساه Codd (1970) في نموذجه العلائقي لقواعد البيانات، حيث استند إلى الجبر العلاقي كأساس نظري لبناء قواعد البيانات الحديثة.
3. **الجبر الخطي (Linear Algebra):** يشكل الجبر الخطي الأساس الرياضي لتمثيل البيانات في صورة متجهات ومصفوفات، ويستخدم على نطاق واسع في تحليل البيانات والتعلم الآلي ومعالجة الصور (Strang, 2016)، وتؤكد التطبيقات المعاصرة أن كثيراً من خوارزميات التحليل تعتمد على عمليات مصفوفية بحتة.
4. **نظرية الاحتمالات والإحصاء:** تتيح هذه النظرية توصيف عدم اليقين في البيانات، وتحليل الأنماط وبناء النماذج التنبؤية داخل نظم المعلومات، وهو ما يؤكد عليه Ross (2014) في عرضه لتطبيقات الاحتمالات في النظم المعقدة.

إن هذه المفاهيم تمثل البنية الرياضية التي تُترجم لاحقاً إلى خوارزميات وآليات تقنية داخل أنظمة المعلومات.

ثانيا: العلاقة بين الرياضيات والتقنية:

تتسم العلاقة بين الرياضيات والتقنية بطابع بنيوي عميق، إذ تمثل الرياضيات الإطار النظري الذي تستند إليه التطبيقات التقنية في تصميمها وتشغيلها وتقييم أدائها، فالتقنية الرقمية كنظم المعلومات أو شبكات

الاتصال أو أنظمة الأمن السيبراني، لا تقوم على إجراءات عشوائية بل على نماذج رياضية تصف العلاقات بين المتغيرات وتحدد آليات التحسين واتخاذ القرار.

حيث أشار Trenchev et al. (2023) إلى أن التحول من الممارسات التقنية الحدسية إلى أنظمة أمنية قائمة على أسس علمية يستلزم اعتماد أدوات رياضية منظمة، مثل نظرية الألعاب والنماذج الاحتمالية والتحسين الرياضي، بما يضمن إمكانية التحقق العلمي والتنبؤ بالسلوك المستقبلي للأنظمة، وهذا الطرح يعكس أن التقنية تصبح أكثر نضجاً كلما ارتكزت على بنية رياضية واضحة.

كما أكدت دراسة Veeranan et al. (2024) أن النماذج الرياضية تمثل أداة مركزية في تصميم نظم تقنية المعلومات وتحسين أدائها، حيث تتيح تبسيط الأنظمة المعقدة، وتحليل كفاءتها قبل التنفيذ الفعلي، وتخصيص الموارد بصورة مثلى، وبيّنت الدراسة أن دمج أدوات التحسين الرياضي ضمن مراحل تصميم النظام يسهم في تقليل التكلفة التشغيلية ورفع مستوى الاعتمادية.

من منظور فلسفي علمي، يمكن القول إن التقنية تمثل "الامتداد العملي" للرياضيات، إذ تُحوَّل البنى المجردة إلى تطبيقات تشغيلية عبر الخوارزميات والبرمجيات، وهذه العلاقة تتسم بالتفاعلية؛ فالتحديات التقنية الجديدة تدفع إلى تطوير أدوات رياضية أكثر تقدماً، كما حدث في مجالات التشفير الحديث وتحليل الأنظمة المعقدة، وعليه فإن فهم نظم المعلومات بوصفها أنظمة تقنية يستلزم إدراك بنيتها الرياضية الكامنة، لأن هذا الإدراك يمثل الأساس لتحليل أدائها وتقييم مخاطرها وتحسين كفاءتها.

2.2 الرياضيات وأمن المعلومات

أولا: الأساس الرياضي للتشفير:

يمثل التشفير أساسا لأمن المعلومات، ويقوم في بنيته العميقة على مشكلات رياضية يفترض أنها صعبة الحل حسابيًا، فالأمن في النظم الحديثة لا يعتمد على سرية الخوارزمية، بل على صعوبة المسألة الرياضية التي تستند إليها، وهو ما يعرف بمبدأ "الأمن القائم على التعقيد الحسابي".

تعتمد أنظمة التشفير بالمفتاح العام على مسائل رياضية مثل تحليل الأعداد الصحيحة الكبيرة إلى عواملها الأولية أو مسألة اللوغاريتم المنفصل أو المشكلات المرتبطة بالمنحنيات الإهليلجية، ويعد افتراض صعوبة هذه المسائل خلال زمن متعدد الحدود الأساس النظري لبناء بروتوكولات آمنة (Katz & Lindell, 2021). فلو أمكن حل هذه المسائل بكفاءة، لانعدمت فعالية النظام التشفيري.

كما يرتبط تصميم نظم التشفير الحديثة بمفهوم الأمن البرهاني (Provable Security)، حيث تبنى الخوارزميات وفق نماذج رياضية دقيقة، ويثبت أمانها عبر اختزالها إلى مسألة رياضية صعبة، وهذا الانتقال من التشفير القائم على الحدس إلى التشفير القائم على البرهان الرياضي يمثل تحولا منهجيا في أمن المعلومات.

بالتالي، تقييم قوة نظام تشفير لا يتم عبر اختباره تجريبيًا فقط، بل من خلال تحليل خصائصه الرياضية، ومدى ارتباط أمانه بمشكلة حسابية غير قابلة للحل عمليًا، وهنا تتجلى مركزية الرياضيات، إذ يصبح أمن المعلومات امتدادًا مباشرًا لنظرية التعقيد الحسابي والجبر العددي.

ثانيا: التحليل الاحتمالي للمخاطر:

يمثل التحليل الاحتمالي أحد أهم التطبيقات الرياضية في مجال أمن المعلومات، إذ يتيح الانتقال من توصيف التهديدات بصورة وصفية إلى قياسها كمياً وتقدير احتمال وقوعها وأثرها المتوقع، فبيئة الأمن السيبراني تتسم بدرجة عالية من عدم اليقين، سواء من حيث طبيعة الهجمات أو تكرارها أو شدتها، وهو ما يجعل من أدوات الاحتمالات والإحصاء ضرورة منهجية وليست اختياراً تحليلياً.

يقوم التحليل الاحتمالي للمخاطر على تمثيل سيناريوهات الهجوم في صورة متغيرات عشوائية يمكن تقدير توزيعها الاحتمالي، ومن ثم حساب القيمة المتوقعة للخسارة أو مستوى المخاطر الكلي للنظام، ويستخدم في هذا السياق مفهوم الخطر (Risk) بوصفه دالة في احتمال الحدث وتأثيره، أي:

$$Risk = P(Event) \times Impact$$

غير أن التقدير الدقيق لهذه القيم يتطلب نماذج رياضية قادرة على تمثيل الاعتماديات بين مكونات النظام، خاصة عندما تكون الهجمات مترابطة أو متسلسلة.

في هذا الإطار، تشير دراسة Zhang and Malacaria (2025) إلى أن اتخاذ القرار في الأمن السيبراني يصبح أكثر تعقيداً في ظل عدم دقة التقديرات الاحتمالية، مما يستدعي استخدام نماذج رياضية متينة(Robust Models) قادرة على التعامل مع نطاقات احتمالية بدلا من قيم نقطية ثابتة، وقد بينت الدراسة أن دمج رسوم الهجوم الاحتمالية (Probabilistic Attack Graphs) مع أدوات التحسين المتين يسهم في تقليل أثر عدم اليقين على القرار الأمني.

يعكس هذا الطرح أن التحليل الاحتمالي لا يقتصر على قياس التهديدات، بل يمتد إلى دعم قرارات تخصيص الموارد الأمنية وتحديد أولويات الحماية، فكلما كان النموذج الاحتمالي أكثر دقة في تمثيل المخاطر، كانت القرارات الناتجة عنه أكثر رشداً وفاعلية.

لذا، فإن الرياضيات ممثلة في نظرية الاحتمالات والتحسين تمثل الأداة المركزية لتحويل المخاطر الأمنية من ظواهر غير محددة إلى كميات قابلة للقياس والمقارنة.

ثالثا: دور الخوارزميات الرياضية:

لا يكتمل فهم العلاقة بين الرياضيات وأمن المعلومات دون الوقوف عند الخوارزميات، باعتبارها الأداة التي تترجم البنى الرياضية المجردة إلى إجراءات تنفيذية داخل النظام الرقمي، فالخوارزمية هي صياغة رياضية منظمة لخطوات حسابية محددة، تهدف إلى تحقيق وظيفة أمنية معينة، مثل التشفير أو المصادقة أو كشف التسلل.

ففي مجال التشفير، تقوم الخوارزميات على تحويل النصوص إلى صيغ مشفرة باستخدام عمليات حسابية تستند إلى خصائص عددية أو جبرية محددة، ويؤكد Katz and Lindell (2021) أن قوة الخوارزمية التشفيرية لا تقاس بسرعة تنفيذها فقط، بل بمدى ارتباطها بمشكلة رياضية يصعب حلها حسابياً، بحيث يصبح كسر النظام مساوياً لحل تلك المسألة.

أما في مجال كشف التسلل (Intrusion Detection)، فتستخدم خوارزميات تعتمد على نماذج إحصائية أو تعلم آلي لتحليل الأنماط غير الطبيعية في حركة البيانات، وهنا تلعب مفاهيم مثل الانحدار الاحتمالي والتصنيف وتحليل التباين دوراً أساسياً في تصميم الخوارزمية، فعملية الكشف ذاتها تمثل تطبيقاً لنموذج رياضي يحاول تقليل الخطأ بين التنبؤ والواقع.

كذلك تُستخدم خوارزميات التحسين الرياضي في تخصيص الموارد الأمنية، كاختيار المواقع المثلى لنشر أدوات الحماية أو توزيع ميزانية الأمن بين مكونات النظام المختلفة، وفي هذا السياق تُصاغ المشكلة في صورة دالة هدف تخضع لقيود معينة، ثم تحل باستخدام تقنيات التحسين العددي أو البرمجة الخطية.

إن الخوارزمية الأمنية ليست مجرد برنامج تنفيذي، بل هي تجسيد رياضي عملي لنموذج نظري، مما يعزز فكرة أن الرياضيات تمثل البنية العميقة التي يقوم عليها أمن المعلومات، فكل طبقة أمنية داخل النظام يمكن إرجاعها إلى خوارزمية، وكل خوارزمية يمكن ردّها إلى صياغة رياضية محددة.

2.3 النمذجة الرياضية في تحليل الأنظمة

أولا: تعريف النموذج الرياضي:

عرفه الخياط بأنه "عباره عن تمثيل رياضي لظاهرة أو متغير أو حالة معينة، ويكون عادة بدلالة سياقات ورموز رياضية من ثوابت ومتغيرات ومعادلات ومتراجعات أو أشكال بيانية وخوارزميات." (الخياط، 2011، ص. 46).

كما يمكن تعرفه بأنه تمثيل تجريدي لنظام واقعي باستخدام رموز وعلاقات رياضية تصف التفاعلات بين مكوناته، ولا يهدف النموذج إلى استنساخ الواقع بصورة حرفية، بل إلى تبسيطه من خلال تحديد المتغيرات الجوهرية والعلاقات المؤثرة بينها، بما يسمح بتحليل سلوك النظام والتنبؤ بمخرجاته في ظل شروط معينة.

يستخدم النموذج الرياضي لتحويل النظام من كيان تقني معقد إلى بنية قابلة للتحليل الكمي، بحيث يمكن توصيف الأداء وقياس الكفاءة وتحليل الاستقرار واختبار السيناريوهات قبل التنفيذ الفعلي.
ويقوم أي نموذج رياضي على ثلاثة عناصر أساسية:

1. **المتغيرات** التي تمثل مكونات النظام أو حالاته.
2. **العلاقات الرياضية** التي تربط بين هذه المتغيرات.
3. **الافتراضات والقيود** التي تحدد نطاق صلاحية النموذج.

وبذلك يصبح النموذج أداة تحليلية تستخدم لفهم سلوك النظام تحت ظروف مختلفة، سواء تعلق الأمر بأداء شبكة معلومات أو توزيع موارد أو تقدير مخاطر.

ثانيا: أنواع النماذج الرياضية:

يمكن تصنيف النماذج الرياضية المستخدمة في تحليل الأنظمة إلى عدة أنماط رئيسة، يختلف كل منها في طبيعة المتغيرات وطريقة التمثيل:

1. **النماذج الحتمية (Deterministic Models):** تفترض هذه النماذج أن العلاقات بين المتغيرات محددة بدقة، بحيث يؤدي نفس الإدخال إلى نفس المخرجات، وتستخدم غالبًا في مسائل التحسين وتخصيص الموارد.
2. **النماذج الاحتمالية (Probabilistic Models):** تأخذ هذه النماذج في الاعتبار عنصر عدم اليقين وتعتمد على التوزيعات الاحتمالية لوصف المتغيرات العشوائية، وهي شائعة في تحليل المخاطر وأنظمة الشبكات.
3. **النماذج الديناميكية (Dynamic Models):** تصف سلوك النظام عبر الزمن، وغالبًا ما تصاغ في صورة معادلات تفاضلية أو فرقية، وتستخدم في تحليل تطور الأنظمة المعقدة.

ويعتبر اختيار نوع النموذج قرارًا منهجيًا يعتمد على طبيعة المشكلة ودرجة عدم اليقين فيها، فكلما زادت تعقيدات النظام ازدادت الحاجة إلى نماذج أكثر مرونة وقدرة على تمثيل التفاعلات المتغيرة.

ثالثا: خطوات بناء النموذج الرياضي:

عملية بناء النموذج الرياضي ليس هدفاً بحد ذاته، بل هو وسيلة لتحويل مشكلة معقدة إلى بنية كمية قابلة للفهم والتحليل والتنبؤ، فكلما كانت خطوات البناء أكثر دقة ووضوحاً، كانت النتائج الناتجة عنه أكثر موثوقية وقابلية للاستخدام في دعم القرار، وتمر عملية بناء النموذج الرياضي بعدة مراحل منهجية:

1. **تحديد المشكلة وصياغتها بدقة:**

تبدأ عملية النمذجة بتحديد المشكلة المراد تحليلها بصورة واضحة ومحددة، ويشمل ذلك تعريف نطاق النظام والهدف من التحليل والنتيجة المطلوبة (تنبؤ، تحسين، تقييم مخاطر، إلخ).

2. **تحديد المتغيرات والمعلمات الأساسية:**

في هذه المرحلة يتم اختيار العناصر المؤثرة في النظام وتمييزها إلى:

- متغيرات قابلة للتغيير (Decision Variables).
- معلمات ثابتة (Parameters).
- متغيرات عشوائية إذا كان النظام يتضمن عدم يقين.

يجب اختيار المتغيرات بدقة، لأن إدخال متغيرات غير ضرورية يزيد من تعقيد النموذج دون تحسين دقته.

3. **صياغة العلاقات الرياضية:**

تترجم العلاقات بين مكونات النظام إلى معادلات أو متباينات رياضية تمثل التفاعل بينها، وهي:

- خطية أو غير خطية.
- احتمالية.
- ديناميكية عبر الزمن.

في هذه المرحلة تتحول المشكلة من وصف لفظي إلى صياغة كمية قابلة للحساب.

4. **تحديد القيود والشروط:**

كل نظام يعمل ضمن حدود معينة، مثل قيود الموارد أو الزمن أو الطاقة أو الميزانية، وتُدمج هذه القيود في النموذج لضمان أن تكون الحلول الناتجة واقعية وقابلة للتطبيق.

5. **حل النموذج وتحليل النتائج:**

بعد بناء الصياغة الرياضية، يستخدم أسلوب مناسب للحل (تحليل جبري، تقنيات تحسين، محاكاة عددية)، وتشمل هذه المرحلة تفسير النتائج في ضوء المشكلة الأصلية.

6. **التحقق من صحة النموذج:**

تختبر ملاءمة النموذج من خلال مقارنة نتائجه بالبيانات الواقعية أو بتحليل الحساسية لمعرفة مدى تأثر النتائج بتغير المدخلات، فإذا أظهر النموذج انحرافاً كبيراً عن الواقع تتم إعادة صياغته أو تعديل افتراضاته.

2.4 دعم اتخاذ القرار عبر نظم المعلومات

أولاً: مفهوم نظم دعم اتخاذ القرار (DSS):

يعرف نظم دعم القرار بأنه "نظام حاسوبي في المستوى الإداري للمؤسسة يضم البيانات، الأدوات التحليلية والنماذج من أجل دعم اتخاذ القرارات شبه المهيكلة وغير المهيكلة" (بحيري، والبدوي، 2008، ص. 22).

تقوم نظم دعم القرار عادةً على ثلاث مكونات رئيسة:

1. قاعدة بيانات تحتوي على المعلومات ذات الصلة بالمشكلة.
2. قاعدة نماذج تضم أدوات تحليل رياضي أو إحصائي.
3. واجهة تفاعلية تسمح للمستخدم بتعديل الفرضيات واختبار السيناريوهات.

جوهر DSS لا يكمن في تخزين البيانات، بل في تحويل البيانات إلى معرفة تحليلية قابلة للاستخدام في اتخاذ القرار وفي البيئات الرقمية المعاصرة، حيث تتزايد كمية البيانات وتعقيدها ويصبح الاعتماد على نظم دعم القرار ضرورة لضبط عملية الاختيار وتقليل التحيز.

ثانياً: أدوات التحليل الكمي في نظم دعم القرار:

يعتمد دعم القرار عبر نظم المعلومات على مجموعة من الأدوات الكمية التي تتيح تقييم البدائل بصورة منهجية، من أبرزها:

1. **التحليل الإحصائي:** يستخدم لتحليل الأنماط واستخلاص العلاقات بين المتغيرات وتقدير احتمالات حدوث الأحداث، ويسهم في تحويل البيانات الخام إلى مؤشرات كمية قابلة للمقارنة.
2. **نماذج التحسين الرياضي:** تستخدم لتحديد الحل الأمثل في ظل قيود معينة، مثل تخصيص الموارد أو تقليل التكلفة أو تعظيم الكفاءة، وتصاغ المشكلة عادة في صورة دالة هدف تخضع لقيود ثم تُحل باستخدام تقنيات التحسين العددي أو البرمجة الخطية.
3. **تحليل السيناريوهات:** يتيح اختبار بدائل متعددة تحت افتراضات مختلفة، مما يساعد على تقييم أثر التغيرات المحتملة في البيئة المحيطة بالنظام.
4. **تحليل الحساسية:** يستخدم لقياس مدى تأثر النتائج بتغير المدخلات، وهو أداة مهمة لفهم استقرار القرار في ظل عدم اليقين.

تُظهر هذه الأدوات أن دعم القرار في نظم المعلومات ليس عملية وصفية، بل عملية تحليلية كمية تعتمد على نماذج رياضية واضحة.

ثالثاً: دور النماذج الرياضية في ترشيد القرار:

تمثل النماذج الرياضية الأساس التحليلي لنظم دعم القرار، تتيح تحويل المشكلة من صياغة لفظية إلى بنية كمية يمكن تقييمها موضوعيا، فعند وجود عدة بدائل يقوم النموذج بتحديد العلاقة بين المتغيرات المؤثرة وقياس أثر كل بديل على دالة الهدف، مما يقلل من الاعتماد على الحدس الشخصي.

في سياق أمن المعلومات، تستخدم النماذج الرياضية لتحديد أولويات الحماية وتخصيص الموارد الأمنية وتقدير المخاطر المحتملة قبل اتخاذ القرار النهائي، فبدلاً من اتخاذ قرار استثماري في مجال أمني بناء على تقدير عام، يمكن صياغة المشكلة في نموذج رياضي يقارن بين العائد المتوقع ومستوى المخاطر، ومن ثم اختيار البديل الذي يحقق التوازن المطلوب.

كما تسهم النماذج في تقليل التحيز المعرفي، إذ تُخضع جميع البدائل لمعيار حسابي موحد، مما يعزز موضوعية القرار، وبهذا يتحقق ترشيد القرارات في نظم المعلومات عند دمج البيانات الغنية مع النماذج الرياضية داخل بيئة تحليلية متكاملة ومنظمة.

الفصل الثالث: التحليل وبناء الإطار التكاملـي

3.1 تحليل العلاقة بين الأمن والنمذجة

تمثل العلاقة بين أمن المعلومات والنمذجة الرياضية علاقة بنيوية وليست علاقة تطبيق جزئي، فالأمن في البيئة الرقمية لا يتحقق بمجرد وجود أدوات تقنية للحماية، بل من خلال تحويل مفاهيم التهديد والضعف والمخاطر إلى متغيرات قابلة للقياس داخل نموذج رياضي منظم، ومن هنا فإن النمذجة لا تعد مرحلة لاحقة للأمن، بل آلية تحليلية لفهمه وإدارته.

تؤكد الأدبيات الحديثة في مجال الأمن السيبراني أن الانتقال من الممارسات الأمنية الحدسية إلى الأطر القائمة على التحليل الرياضي هو ما يمنح الأمن صفة "العلمية" (Trenchev et al., 2023)، فبدلاً من التعامل مع الهجمات بوصفها أحداثًا معزولة، يتم تمثيلها داخل نماذج رياضية تُظهر احتمالات حدوثها ومسارات انتشارها وتأثيرها المتوقع على النظام.

كما أوضح Zhang and Malacaria (2025) أن قرارات الأمن السيبراني في ظل عدم اليقين لا يمكن أن تكون فعالة دون تمثيل المخاطر ضمن نموذج كمي يأخذ في الاعتبار تعدد السيناريوهات، وقد بينت دراستهما أن دمج رسوم الهجوم الاحتمالية مع أدوات التحسين المتين يسمح بتحويل التهديدات الأمنية إلى عناصر قابلة للمقارنة داخل إطار قرار رياضي.

بذلك يمكن تحليل العلاقة بين الأمن والنمذجة عبر ثلاث مستويات مترابطة:

أولًا: تحويل التهديد إلى متغير:

التهديد الأمني في صورته الأولية يمثل حدث احتمالي غير منظم، إلّا أن النمذجة الرياضية تعيد تعريفه كمتغير يمكن تقدير احتماله أو تأثيره، سواء عبر توزيع احتمالي أو قيمة عددية تمثل مستوى الخطورة، وبهذا يتحول الأمن من توصيف كيفي إلى توصيف كمي.

ثانيًا: تحويل المخاطر إلى دالة هدف:

عند إدخال المخاطر ضمن نموذج رياضي، تصبح قابلة للصياغة في صورة دالة هدف يمكن تقليلها أو تحسينها، فبدلاً من القول بضرورة "تقليل المخاطر"، يتم التعبير عنها كعلاقة رياضية بين احتمال الهجوم وتأثيره، ثم تستخدم تقنيات التحسين لاختيار الاستراتيجية الأنسب.

ثالثًا: تحويل الحماية إلى مسألة تخصيص موارد:

تمثل الحماية الأمنية عادة قرارًا يتعلق بتوزيع موارد محدودة، وهنا تستخدم النماذج الرياضية لتحديد كيفية تخصيص هذه الموارد بصورة تقلل الخطر الكلي للنظام، وهو ما يعكس التكامل بين الأمن والنمذجة.

من خلال هذا التحليل يتضح أن النمذجة تمثل البنية التي يعاد من خلالها تنظيم المفاهيم الأمنية في إطار كمي منضبط، أي بدون النمذجة يبقى الأمن عملية تقديرية تعتمد على الخبرة، أما بوجودها فيتحول إلى نظام تحليلي قابل للتقييم والتحسين.

وبذلك تتشكل الحلقة الأولى في الإطار التكاملـي للبحث: (الأمن لا يُدار تقنيًا فقط، بل يُبنى ويُحلل رياضيًا).

3.2 دور الرياضيات في تقليل المخاطر المعلوماتية

لا يمكن إدارة المخاطر بشكل فعال دون استخدام أدوات كمية قادرة على تحويل التهديدات غير المنظمة إلى صيغ قابلة للقياس والتحليل المنهجي، فالرياضيات تعمل كوسيلة عملية لتقدير الاحتمالات

وموازنة الخسائر وتحديد مستويات الاستثمار في الحماية، التحول من إجراءات نوعية إلى تقييمات كمية يعزز قدرة صناع القرار على مقارنة البدائل واتخاذ قرارات قائمة على تحليل موضوعي بدلاً من الحدس أو الخبرة الفردية.

أولاً: الصياغة الكمية للمخاطر السيبرانية:

يشير تعريف (Quantification of Cyber Risk) إلى أنه العملية التي يتم من خلالها تقييم المخاطر السيبرانية بعد تحديدها، ثم تحليلها باستخدام نماذج رياضية لتحويلها إلى قياسات عددية يمكن استخدامها في اتخاذ القرار وتعزيز البنية الأمنية (Karyda, 2021)، هذه الصياغة تتجاوز التصنيفات الوصفية التقليدية (كعالي/متوسط/منخفض)، إلى مقاييس كمية معبر عنها كاحتمالات أو مؤشرات عددية، مما يجعلها أكثر قابلية للمقارنة والتحسين.

فعلى سبيل المثال، تُستخدم الأساليب الاحتمالية لتقدير احتمالات التعرض لهجمات وتحديد مستوى التأثير المتوقع عند حدوثها، بما يتيح تحديد أولويات التحسين الأمني، فإن تحويل التهديدات إلى متغيرات عددية يعد المرحلة الأولى في تقليل المخاطر عن طريق الرياضيات.

ثانياً: النماذج الاحتمالية وتقليل عدم اليقين:

التحليل الاحتمالي يعتبر من أهم الأدوات التي تقدمها الرياضيات للتعامل مع عدم اليقين في المخاطر المعلوماتية، فالهجمات السيبرانية لا تحدث بشكل منتظم أو متوقع بدقة ولذا تعتمد المنهجيات الكمية على توزيع احتمالي يربط بين مدى الضعف في النظام واحتمالية الاستغلال، ويمكن تمثيل هذا النوع من العلاقة عبر دوال احتمالية تصف احتمال وقوع الخطر كمجموع لعوامل متعددة.

تقدم الأدبيات الحديثة نماذج تحليلية تستخدم مثل هذه الأساليب الاحتمالية لتقييم المخاطر بشكل ديناميكي يسمح بتحديث تقديرات الخطر مع تطور الظروف الأمنية (Cheimonidis et al., 2025)، وهذا يعني أن الرياضيات لا تقلل من عدم اليقين بإلغائه، بل بتحويله إلى نظم تحليلية يمكن التعامل معها بصورة أكثر دقة واتساقًا.

ثالثاً: التحسين الرياضي في إدارة المخاطر:

بعد تحويل المخاطر إلى صياغة كمية، تصبح الرياضيات أداة في عمليات التحسين لتقليل المخاطر الكلية في النظام، حيث تعتمد هذه العمليات على نماذج تحسين رياضي تهدف إلى:

1. تحديد المستوى الأمثل للاستثمار في الحماية.
2. إيجاد توزيع موارد يقلل من الخسائر المتوقعة.
3. مقارنة سيناريوهات متعددة لاتخاذ القرار الأفضل.

من الأمثلة البارزة نموذج (*Gordon–Loeb*) الذي يحدد مستوى الاستثمار الأمني الأمثل بحيث لا يتجاوز نسبة معينة من الخسارة المتوقعة من الاختراق، وذلك باستخدام دوال رياضية تربط بين احتمال الخطر وتأثيره والتكلفة الأمنية (Gordon & Loeb, 2002)، هذا النوع من النماذج يعكس كيف يمكن للرياضيات أن توجه تخصيص الموارد بشكل يقلل من المخاطر على مستوى النظام ككل.

رابعاً: رفع دقة اتخاذ القرار وتقليل التحيز:

تُسهم النماذج الرياضية في تقليل المخاطر أيضًا من خلال تحسين عملية اتخاذ القرار بشكل أدق وأكثر موضوعية، فالنماذج التي تعتمد تحليلا كميا للمتغيرات والقيود توفر تقديرات دقيقة لإمكانيات الخطر، وتتيح مقارنة تأثيرات الخيارات المختلفة، وهذا يقلل الاعتماد على التقديرات الحدسية أو الخبرات السابقة غير المنهجية، مما يرفع من جودة القرارات الأمنية المستندة إلى البيانات.

كما أن تحليل الحساسية الذي توفره النماذج يمكن أن يُظهر كيف تؤثر التغيرات الصغيرة في المتغيرات الأساسية على النتائج، مما يتيح لصناع القرار فهمًا أفضل لنقاط الضعف والفرص في منظومتهم الأمنية.

جدول (1): المقاربات الرياضية في تقليل المخاطر المعلوماتية ومجالات استخدامها

المقاربة الرياضية	الأساس الرياضي	طبيعة عدم اليقين	آلية تقليل المخاطر	مجال الاستخدام في الأمن المعلوماتي	الميزة الرئيسة
النماذج الاحتمالية (Probabilistic Models)	نظرية الاحتمالات والتوزيعات الإحصائية	عدم يقين قابل للقياس احتماليًا	تقدير احتمال وقوع الحدث وتأثيره وحساب القيمة المتوقعة للخطر	تقييم احتمالات الهجمات، تحليل التهديدات، تقدير الخسائر	تحويل المخاطر إلى مؤشرات كمية قابلة للمقارنة
النماذج البايزية (Bayesian Models)	نظرية بايز وتحديث الاحتمالات	عدم يقين ديناميكي يتغير مع المعلومات الجديدة	تحديث تقدير المخاطر عند توفر بيانات إضافية	تحليل التهديدات المتغيرة، نظم الكشف المبكر	مرونة عالية في البيئات المتغيرة
نماذج التحسين الرياضي (Optimization Models)	البرمجة الخطية وغير الخطية ونظرية التحسين	قيود موارد مع وجود مخاطر متعددة	تقليل دالة الخطر الكلي أو تعظيم العائد الأمني تحت قيود	تخصيص الميزانيات الأمنية، توزيع أدوات الحماية	تحقيق التوازن الأمثل بين التكلفة ومستوى الأمان
النماذج المتينة (Robust Models)	التحسين المتين وتحليل السيناريوهات	عدم يقين في القيم التقديرية نفسها	اختيار قرار يحقق أفضل أداء عبر أسوأ السيناريوهات المحتملة	قرارات الاستثمار الأمني طويلة الأجل	تقليل حساسية القرار تجاه الأخطاء التقديرية
نماذج المحاكاة (Simulation Models)	النمذجة العددية والمحاكاة الحاسوبية	عدم يقين متعدد العوامل	اختبار سيناريوهات افتراضية قبل التنفيذ الفعلي	محاكاة الهجمات واختبار الاستجابة	تقليل المخاطر التشغيلية قبل التطبيق

3.3 النموذج التكاملـي المقترح

انطلاقًا من التحليل السابق للعلاقة بين الأمن والنمذجة، ودور الرياضيات في تقليل المخاطر المعلوماتية، يتضح أن هذه المجالات لا تعمل بصورة منفصلة، بل ضمن سلسلة مترابطة من التحويلات المفاهيمية والكمية، لذا، يقترح هذا البحث إطارًا تكامليًا يوضح كيف تنتقل المفاهيم الرياضية من مستوى التجريد النظري إلى مستوى القرار العملي داخل نظم المعلومات، كإطار مفاهيمي تحليلي.

أولاً: البنية العامة للنموذج:

يقوم النموذج التكاملـي المقترح على خمس طبقات مترابطة:

1. **طبقة الأساس الرياضي:**

تمثل هذه الطبقة القاعدة النظرية للنظام، وتشمل:

- نظرية الاحتمالات (لتوصيف عدم اليقين).
- نماذج التحسين (لتخصيص الموارد).
- أدوات النمذجة الرياضية (لصياغة العلاقات).

في هذه المرحلة، لا يكون التركيز على الأمن مباشرة، بل على توفير الأدوات الكمية التي ستُستخدم لاحقًا في توصيفه.

2. **طبقة المعالجة الأمنية:**

في هذه الطبقة يتم تحويل مفاهيم الأمن إلى متغيرات قابلة للتحليل، وتشمل:

- التشفير (كآلية حماية).
- تحليل التهديدات.
- تقييم نقاط الضعف.
- تقدير احتمال الهجوم وأثره.

هنا يبدأ الانتقال من الإطار الرياضي المجرد إلى التطبيق الأمني.

3. **طبقة التحليل النموذجي:**

تمثل هذه الطبقة نقطة التحول المركزية في النموذج، حيث:

- تتحول المخاطر إلى دوال رياضية.
- تُحدد القيود (ميزانية – موارد – زمن).
- تُبنى سيناريوهات متعددة.
- تُقارن البدائل وفق معيار كمي موحد.

في هذه المرحلة، يصبح الأمن مسألة تحليل رياضي منظم وليس إجراءً تقنيًا معزولًا.

4. **طبقة دعم اتخاذ القرار:**

تُغذَّى نتائج التحليل النموذجي إلى نظم دعم القرار (DSS)، حيث:

- تُعرض السيناريوهات الممكنة.
- تُحسب النتائج المتوقعة لكل بديل.
- يُختار البديل الذي يحقق أدنى مستوى خطر وأعلى كفاءة.

هنا تتحول الرياضيات من أداة تحليل إلى أداة ترشيد قرار.

5. طبقة النتائج النظامية:

تنعكس القرارات المختارة على أداء النظام عبر:

- تقليل المخاطر المعلوماتية.
- تحسين تخصيص الموارد.
- تعزيز استقرار النظام.
- رفع كفاءة الاستجابة الأمنية.

ثانيًا: الشكل المفاهيمي للنموذج:

يمكن تمثيل النموذج التكاملـي المقترح بالشكل التالي:

الإطار التكاملـي المقترح للعلاقة بين الرياضيات وأمن المعلومات ودعم القرار:

شكل (1): الإطار التكاملـي المقترح للعلاقة بين الرياضيات وأمن المعلومات ودعم القرار:

يوضح الشكل تسلسل الانتقال من الأساس الرياضي إلى القرار المؤسسي، حيث تمثل الرياضيات البنية التحتية التحليلية، بينما تمثل النمذجة حلقة الربط بين الأمن ودعم القرار، ويُظهر الشكل أن تقليل المخاطر لا يتحقق مباشرة عبر التشفير فقط، بل عبر دمج التحليل الرياضي في عملية اتخاذ القرار.

ثالثًا: القيمة المضافة للنموذج:

تكمن القيمة العلمية للنموذج في أنه:

- لا يعالج الأمن كمسألة تقنية فقط.
- لا يعالج النمذجة كعملية حسابية منفصلة.
- لا يعالج القرار كعملية إدارية معزولة.

بل يربط هذه العناصر ضمن بنية واحدة مترابطة، بما يسمح بفهم ديناميكية انتقال المعلومات والتحليل والقرار داخل النظام.

كخلاصة، يمثل هذا النموذج محاولة لتنظيم العلاقة بين الرياضيات وأمن المعلومات والنمذجة ودعم القرار في إطار واحد متكامل، وهو لا يهدف إلى استبدال النماذج القائمة، بل إلى توفير رؤية تحليلية تُظهر كيف تتكامل هذه المكونات لتعزيز كفاءة نظم المعلومات وتقليل مخاطرها.

الفصل الرابع: النتائج والتوصيات

في ضوء التحليل المفاهيمي الذي تناول العلاقة بين الرياضيات وأمن المعلومات والنمذجة ودعم اتخاذ القرار، يمكن استخلاص جملة من النتائج النظرية والتطبيقية التي تعكس القيمة العلمية للبحث، وذلك على النحو الآتي:

4.1 النتائج النظرية

تكشف النتائج النظرية في ضوء التحليل النظري الذي تم بناؤه عبر الفصول السابقة، أن العلاقة بين الرياضيات وأمن المعلومات ليست علاقة توظيف تقني جزئي، بل علاقة تأسيس بنيوي، فقد تبين أن الرياضيات تمثل القاعدة المعرفية التي تشتق منها آليات الحماية الرقمية، سواء عبر نظريات الاحتمال التي تنظّم فهم عدم اليقين، أو عبر نماذج التحسين التي تضبط تخصيص الموارد، أو عبر أدوات النمذجة التي تحوّل العلاقات المعقدة إلى صيغ كمية قابلة للتحليل.

وانطلاقًا من ذلك، أظهر التحليل أن أمن المعلومات لا يمكن التعامل معه بوصفه منظومة تقنية مستقلة، لأن فعاليته ترتبط بقدرته على تحويل التهديدات والمخاطر إلى متغيرات قابلة للقياس والمقارنة، وهنا برزت النمذجة الرياضية بوصفها الحلقة المركزية التي يعاد من خلالها تنظيم المفاهيم الأمنية ضمن إطار كمي منضبط، يسمح بتوصيف المخاطر في صورة دوال وعلاقات، بدلاً من بقائها في نطاق التقدير الوصفي.

كما أوضح البحث أن إدخال المخاطر ضمن بنية نموذجية رياضية يسهم في تقليل الغموض المرتبط بها، إذ تتحول من تصنيفات عامة إلى قيم قابلة للتحليل والمفاضلة، هذا يعني أن النمذجة لا تكتفي بتفسير الظاهرة الأمنية، بل تمكّن من إدارتها بصورة أكثر موضوعية عبر ربطها بمعايير كمية موحدة.

في السياق ذاته، أظهر البحث أن التكامل بين الرياضيات والنمذجة ونظم دعم القرار يؤدي إلى انتقال نوعي في طريقة التعامل مع الأمن المعلوماتي، حيث يصبح القرار الأمني نتيجة عملية تحليلية قائمة على مقارنة بدائل وسيناريوهات وليس استجابة ظرفية أو حدسية، ومن ثم فإن القيمة النظرية الأساسية التي يقدمها البحث تتمثل في بلورة إطار تكاملي يوضح أن كفاءة نظم المعلومات لا تتحقق عبر تعزيز أدوات الحماية فحسب، بل عبر دمج التحليل الرياضي داخل منظومة القرار ذاتها.

بذلك يمكن القول إن النتيجة الجوهرية للبحث تتمثل في إعادة تأطير دور الرياضيات داخل البيئة الرقمية المعاصرة، بوصفها عنصرًا حاكمًا في ضبط الأمن وإدارة المخاطر وترشيد القرار، لا مجرد أداة خلفية في تصميم الأنظمة.

4.2 النتائج التطبيقية

على الرغم من أن البحث اعتمد المنهج الوصفي التحليلي، فإن الإطار التكاملـي المقترح يكشف عن دلالات تطبيقية مهمة، من أبرزها:

1. إمكانية توظيف النموذج التكاملـي في تصميم سياسات أمنية قائمة على التحليل الكمي بدلًا من التقدير الحدسي.
2. دعم المؤسسات في تحديد أولويات الاستثمار الأمني وفق معايير رياضية واضحة.
3. تعزيز دور نظم دعم القرار في إدارة المخاطر السيبرانية داخل القطاعات الحساسة مثل المصارف والبنية التحتية الرقمية.
4. توفير أساس نظري يمكن تطويره إلى نماذج تطبيقية كمية في دراسات لاحقة.

4.3 التوصيات

1. ضرورة تعزيز الدراسات التكاملية التي تربط بين الرياضيات وأمن المعلومات ونظم دعم القرار.
2. تشجيع البحوث التي تطور نماذج كمية لقياس المخاطر السيبرانية في البيئات العربية.
3. إدراج مقررات متخصصة في النمذجة الرياضية للأمن السيبراني ضمن برامج تقنية المعلومات.
4. اعتماد أدوات تحليل كمية عند تقييم المخاطر المعلوماتية داخل المؤسسات.
5. دمج النماذج الرياضية في نظم دعم القرار بدلًا من الاكتفاء بالتقارير الوصفية.
6. الاستثمار في تطوير كفاءات قادرة على فهم التحليل الرياضي للأمن.
7. تطوير نموذج رياضي تطبيقي مشتق من الإطار المقترح واختباره في بيئة مؤسسية حقيقية.

8. دراسة أثر الذكاء الاصطناعي على تعزيز النماذج الكمية في إدارة المخاطر.
9. بناء قواعد بيانات وطنية لدعم النماذج الاحتمالية في الأمن المعلوماتي.

الخاتمة

سعى هذا البحث إلى معالجة إشكالية معرفية تتمثل في تحديد طبيعة العلاقة بين الرياضيات وأمن المعلومات والنمذجة الرياضية ودعم اتخاذ القرار عبر نظم المعلومات، في ظل التحولات الرقمية المتسارعة التي جعلت من إدارة المخاطر المعلوماتية قضية مركزية في المؤسسات الحديثة، حيث انطلق البحث من فرضية مفادها أن الرياضيات لا تمثل أداة مساعدة في البيئة الرقمية فحسب، بل تشكل البنية العميقة التي تقوم عليها آليات الحماية والتحليل والترشيد.

ومن خلال المنهج الوصفي التحليلي، تم تفكيك المفاهيم الأساسية المرتبطة بالرياضيات ونظم المعلومات، ثم تحليل الأساس الرياضي للتشفير وإدارة المخاطر، قبل الانتقال إلى دراسة دور النمذجة في تحويل المخاطر من توصيف نوعي إلى صياغة كمية قابلة للقياس، وقد أظهر التحليل أن الأمن المعلوماتي يفقد كثيرًا من فاعليته إذا لم يُدمج داخل إطار رياضي يسمح بتقدير الاحتمالات ومقارنة البدائل وتحسين القرارات تحت قيود الموارد.

كما بيّن البحث أن النمذجة الرياضية تمثل الحلقة المركزية التي تربط بين التحليل الأمني ونظم دعم القرار، فهي تتيح تحويل البيانات الأمنية إلى مدخلات كمية تُغذّي عمليات المفاضلة والاختيار داخل بيئة القرار، وبذلك ينتقل الأمن من كونه استجابة تقنية إلى كونه عملية تحليلية منظمة تستند إلى أدوات رياضية واضحة.

أسفر هذا المسار التحليلي إلى اقتراح إطار تكاملي يوضح تفاعل الرياضيات والتحليل الأمني والنمذجة ودعم القرار ضمن منظومة واحدة مترابطة، بما يسهم في تقليل المخاطر المعلوماتية وتعزيز كفاءة نظم المعلومات، ولا يدّعي هذا النموذج تقديم حل تطبيقي نهائي، بل يقدم تصورًا نظريًا منظمًا يمكن تطويره في دراسات لاحقة نحو نماذج كمية قابلة للاختبار.

تختتم القيمة العلمية للبحث في إعادة تأطير موقع الرياضيات داخل منظومة الأمن الرقمي، بوصفها عنصرًا حاكمًا في فهم المخاطر وإدارتها وفي ترشيد القرار المؤسسي، بما يعزز من استقرار النظم المعلوماتية في بيئات تتسم بالتعقيد وعدم اليقين.

المراجع

[1] **أولًا: المراجع** العربية:

[2] بحيري، ن. م.، والبدوي، إ. أ. (2008). نظم دعم القرار. منشورات جامعة السودان المفتوحة.

[3] الخياط، ب. ي. ذ. (2011). مدخل إلى النمذجة الرياضية باستخدام MATLAB: الجزء الأول، الأساسيات والنمذجة المتقطعة. دار ابن الأثير للطباعة والنشر، جامعة الموصل.

[4] الفندي، م. ث. (1972). أصول المنطق الرياضي (Logistique). دار النهضة العربية للطباعة والنشر.

ثانياً: المراجع الأجنبية:

[5] Codd, E. F. (1970). A relational model of data for large shared data banks. Communications of the ACM, 13(6).

[6] Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4).

[7] Karyda, M. (2021). Cyber risk quantification. In S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, & X. S. Wang (Eds.), Encyclopedia of cryptography, security and privacy. Springer.

[8] Katz, J., & Lindell, Y. (2021). Introduction to modern cryptography (3rd ed.). CRC Press.

[9] Ross, S. M. (2014). Introduction to probability models (11th ed.). Academic Press.

[10] Sharaf, S. A., Ragab, M., Albogami, N., Al-Malaise Al-Ghamdi, A., Sabir, M. F., Maghrabi, L. A., Ashary, E. B., & Alaidaros, H. (2024). Advanced mathematical modeling

of mitigating security threats in smart grids through deep ensemble model. Scientific Reports, 14, 23069.

[11] Strang, G. (2016). Introduction to linear algebra (5th ed.). Wellesley-Cambridge Press.

[12] Trenchev, I., Dimitrov, W., Dimitrov, G., Ostrovska, T., & Trencheva, M. (2023). Mathematical approaches transform cybersecurity from protoscience to science. Applied Sciences, 13(11), 6508.

[13] Veeranan, K., Vaidhyanathan, P., Selvi, T., & Martin, A. (2024). Impact of mathematical models in IT system design and optimization. International Journal of Information Technology, Research and Applications (IJITRA), 3(1).

[14] Zhang, Y., & Malacaria, P. (2025). Dealing with uncertainty in cybersecurity decision support. *Computers & Security, 148*, 104153.