AJSP
المجلة العربية للنشر العلمي

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

المجلد التاسع – العدد التسعون
تاريخ الإصدار: 2 – نيسان – 2026م
www.ajsp.net

"دور أمن المعرفة في دعم إدارة المعرفة وحماية الأصول المعرفية – دراسة تحليلية"

إعداد الباحثات:

أ. نعيمة محمد الدميني*

جامعة الملك عبد العزيز – المملكة العربية السعودية

أ.د. ريم علي الرابغي

Researchers:

Naima Mohammed Dmini. PhD Researcher* / King Abdulaziz University/ Kingdom of Saudi Arabia

Reem Ali Alrabghi. Professor, Department of Information Science, King Abdulaziz University

Received: 28/03/2026 | Revised: 29/03/2026 | Accepted: 01/04/2026 | Published: 02/04/2026

Keywords: Knowledge Security – Knowledge Management – Protection of Knowledge Assets

Abstract:

This study aimed to highlight the pivotal role of knowledge security in enhancing knowledge management and protecting intellectual assets as a strategic necessity amid the rapid digital transformation.

The study relied on the descriptive-analytical approach through a review of previous literature and an analysis of relevant content.

The study concluded that knowledge security represents the bridge connecting knowledge management and information security; it is not limited to protecting data only but extends to include human expertise and skills. The results emphasized that integrating security measures with knowledge management processes directly contributes to protecting intellectual capital in its three components (human, structural, and relational capital) from internal and external threats, thereby ensuring the sustainability of the organization's competitive advantage in the contemporary business environment.

ملخص البحث

هدفت هذه الدراسة إلى إبراز دور أمن المعرفة في تعزيز إدارة المعرفة وحماية الأصول المعرفية بوصفها ضرورة استراتيجية في ظل التحول الرقمي المتسارع. استندت الدراسة إلى المنهج الوصفي التحليلي من خلال مراجعة الأدبيات السابقة وتحليل المحتوى ذي الصلة.

توصلت الدراسة إلى أن أمن المعرفة يمثل الجسر الذي يصل بين إدارة المعرفة وأمن المعلومات؛ إذ لا يقتصر على حماية البيانات فحسب، بل يمتد ليشمل الخبرات والمهارات البشرية. وأكدت النتائج أن تكامل الإجراءات الأمنية مع عمليات إدارة المعرفة يسهم بصورة مباشرة في حماية رأس المال الفكري بمكوناته الثلاثة (البشري، والهيكلي، ورأس مال العلاقات) من التهديدات الداخلية والخارجية؛ مما يضمن استدامة الميزة التنافسية للمنظمة في بيئة الأعمال المعاصرة.

الكلمات المفتاحية: أمن المعرفة – إدارة المعرفة – حماية الأصول المعرفية

How to Cite This Article

الدميني، ن. م.، والرابغي، ر. ع. (2026). دور أمن المعرفة في دعم إدارة المعرفة وحماية الأصول المعرفية – دراسة تحليلية. المجلة العربية للنشر العلمي (AJSP)، 9(90)، (600 –625).

المقدمة:

يشهد العصر الحالي تسارعا في وتيرة تدفق المعلومات، وأصبحت إدارة المعرفة ضرورة استراتيجية لكل منظمة تسعى لتحقيق ميزة تنافسية مستدامة. ومع تزايد الاعتماد على الأنظمة الرقمية والمنصات التعاونية في مختلف عمليات إدارة المعرفة، ظهرت الحاجة الملحة لحماية هذه المعرفة من مخاطر التسريب أو الفقدان.

تهتم إدارة المعرفة باستثمار أصول المعرفة أو رأس مال المعرفة، واكتشاف القيم المخفية وغير الملموسة للأصول المعرفية والإنسانية الموجودة في المنظمة (ضليمي، 2022).

يأتي أمن المعلومات ليلعب دورا محوريا من أجل ضمان استمرار الأعمال؛ فلا يقتصر هذا الدور فقط على تأمين المعلومة والحفاظ على سرية ونزاهة المعلومات وتوافرها؛ بل يشمل تأمين البنية التحتية التي تسهل استخدامها من أجهزة وبرمجيات وعوامل بشرية ومادية (عشماوي، 2022).

يقع أمن المعرفة عند نقطة التقاطع بين إدارة المعرفة وأمن المعلومات، ويسعى لجعل معرفة العاملين في الشركة آمنة والحفاظ عليها وحمايتها من الإفصاح العرضي أو المتعمد للأشخاص غير المصرح لهم، ومن التعديل غير المصرح به (Zieba & Bongiovanni, 2022).

تناولت هذه الدراسة مفهوم أمن المعرفة وعلاقته بإدارة المعرفة، وتوضيح أهميته في حماية الأصول المعرفية وتعزيز القدرة التنافسية للمنظمات. كما تستمد هذه الدراسة أهميتها من كونها تسلط الضوء على أحد الموضوعات الحديثة التي تجمع بين مجالي إدارة المعرفة وأمن المعلومات، وتسعى إلى تقديم إطار نظري يوضح أبعاد هذا المفهوم ودوره في البيئة التنظيمية المعاصرة.

1-1 مشكلة الدراسة

في ظل التحول الرقمي المتسارع وتزايد اعتماد المنظمات على الأنظمة الإلكترونية والمنصات التعاونية في إدارة المعرفة، حظيت الأصول المعرفية بأهمية استراتيجية تعتمد عليها المنظمات في تحقيق الميزة التنافسية. غير أن هذا الاعتماد المتزايد صاحبه تنامٍ في المخاطر المرتبطة بتسريب المعرفة أو فقدانها أو التلاعب بها، سواء كان ذلك نتيجة ضعف الإجراءات الأمنية أو قصور الوعي لدى العاملين أو التهديدات الخارجية.

وعلى الرغم من الاهتمام المتزايد بكل من إدارة المعرفة وأمن المعلومات كل على حدة، فإن التكامل بينهما في إطار مفهوم أمن المعرفة لا يزال بحاجة إلى مزيد من الدراسة، خاصة فيما يتعلق بدوره في حماية الأصول المعرفية وضمان استمرارية الاستفادة منها داخل المنظمات. ومن هنا تبرز مشكلة الدراسة في الحاجة إلى توضيح مفهوم أمن المعرفة وبيان علاقته بإدارة المعرفة ودوره في حماية الأصول المعرفية في البيئة التنظيمية المعاصرة، وتتحدد مشكلة الدراسة في الإجابة عن التساؤل الرئيس الآتي:

"ما دور أمن المعرفة في دعم إدارة المعرفة وحماية الأصول المعرفية من المخاطر المحتملة؟"

2-1 أسئلة الدراسة

في سبيل تحقيق أهداف الدراسة سيتم الإجابة عن التساؤلات الآتية:

1- ما هو مفهوم أمن المعرفة وماهي أبعاده في البيئة التنظيمية؟
2- ما هي طبيعة العلاقة بين أمن المعرفة وإدارة المعرفة وما هي أوجه التكامل بينها؟
3- ماهي أهمية أمن المعرفة في حماية الأصول المعرفية من المخاطر المحتملة؟

1-3 أهداف الدراسة

تسعى الدراسة الحالية إلى تحقيق الهدف الرئيس في التعرف على دور أمن المعرفة في دعم إدارة المعرفة وحماية الأصول المعرفية والذي يتفرع منه مجموعة من الأهداف:

1- التعرف على مفهوم أمن المعرفة وأبعاده في البيئة التنظيمية
2- الكشف عن طبيعة العلاقة بين أمن المعرفة وإدارة المعرفة وتوضيح أوجه التكامل بينهما
3- إبراز أهمية أمن المعرفة في حماية الأصول المعرفية من المخاطر المحتملة

1-4 أهمية الدراسة

الأهمية النظرية:

- تسهم الدراسة في معالجة فجوة بحثية تتعلق بدور أمن المعرفة في دعم إدارة المعرفة وعملياتها وحماية الأصول المعرفية في المنظمات المعاصرة
- تقدم الدراسة منظورا تكامليا يسلط الضوء عن طبيعة العلاقة بين أمن المعرفة وإدارة المعرفة وتوضيح أوجه التكامل بينهما
- تتميز الدراسة بالكشف عن المخاطر المحتملة التي تهدد الأصول المعرفية وعن أساليب أمن المعرفة للتصدي لهذه المخاطر

الأهمية العلمية:

- توضح الدراسة عناصر أمن المعرفة التي تضمن دقة المعرفة واكتمالها وموثوقيتها في جميع مراحل دورة بما يحقق توازنا بين الحماية والمشاركة ويسهم في تعزيز الابتكار واستدامة الأداء المؤسسي.
- توضح الدراسة دور أمن المعرفة في كل مراحلها من الإنشاء إلى الأرشفة ليعاد الاستفادة من المعارف لاكتشاف وابتكار أفكار جديدة أو الحذف الآمن للبيانات في تقادم المعارف وتراجع فائدتها
- تتميز الدراسة بوصفها مرجعا علميا في مجال أمن المعرفة يمكن الاعتماد عليه في تطوير سبل حماية الأصول المعرفية في المنظمات
- قدمت الدراسة توصيات دمج أمن المعرفة في الاستراتيجية التنظيمية وتعزيز الوعي الأمني المعرفي وتبني تقنيات حماية متقدمة

1- 5 حدود الدراسة

- **الحدود الموضوعية:** تحليل محتوى الأدبيات التي تناولت موضوع أمن المعلومات وأمن المعرفة وعلاقته بإدارة المعرفة والأصول المعرفية في المنظمات
- **الحدود الزمانية:** يتناول التحليل الدراسات المنشورة في الفترة الزمنية من 2019 م إلى 2026م

2-منهج الدراسة

وفقا لأهداف الدراسة تم الاعتماد على المنهج الوصفي باستخدام أسلوب تحليل المحتوى، والذي يعتمد على تحليل الأدبيات؛ بهدف الاستفادة منها في تحقيق أهداف الدراسة الحالية.

2-1 مصطلحات الدراسة

أمن المعرفة(Knowledge Security): يشير أمن المعرفة إلى منع النقل غير المرغوب فيه للمعلومات الحساسة والخبرات العملية والتكنولوجيا، والحد من التدخلات الأجنبية في التعليم العالي والبحث العلمي وتقليل الاعتماد التي قد تعرض الأمن القومي والقدرة التنافسية للخطر (Eigner,2024) .

إدارة المعرفة (Knowledge Management): هي عمليات محددة ومنظمة تساعد على توليد المعرفة، واستخدامها ونشرها؛ بهدف استثمار ما يمتلكه المورد البشري من معارف ومهارات بما يساهم في اتخاذ القرارات وحل المشكلات وتنمية وتحسين أداء المنظمة (الحربي والحربي ،2026).

أصول المعرفة (Knowledge Assets): هي المعرفة التي تمتلكها المؤسسة والقوى العاملة لديها في شكل المعلومات والأفكار والسياسات والإجراءات والبرامج وبراءات الاختراع لدى الشركة، بالإضافة إلى أصول المعرفة التي توجد عند العملاء والموردين والشركاء الآخرين (جوهري ،2022)

3 -الدراسات السابقة

يعد موضوع أمن المعرفة وعلاقته بإدارة المعرفة والأصول المعرفية من المواضيع الحديثة التي لم تتناوله الدراسات العملية بكثرة، لذا سوف ندرج في الدراسات السابقة دراسات تناولت أمن المعلومات وذلك لأن أمن المعرفة هو جزء من أمن المعلومات، إذ يمثل المظلة الأكبر والتي يندرج تحتها أمن المعرفة وأمن الشبكات والأمن السيبراني، وسوف نستعرض فيما يلي بعض الدراسات العربية والأجنبية وفقا لترتيبها زمنيا من الأحدث إلى الأقدم ثم نعقب عليها بتوضيح أوجه التشابه والاختلاف والنقاط التي يمكن أن تستفيد منها الدراسة الحالية.

دراسة (موسى وآخرون ،2026) هدفت الدراسة إلى وضع إطار محاسبي ومؤشر مقترح للإفصاح عن مخاطر الأمن السيبراني، وقياس أثر ذلك على كفاءة القرارات الاستثمارية والقيمة الحقيقية للأسهم، من خلال تطبيقه على بنوك مصرية وشركات في قطاع الاتصالات وتكنولوجيا المعلومات خلال الفترة 2020–2024.وأظهرت النتائج أن البنوك تفصح عن مخاطر الأمن السيبراني بدرجة أكبر من شركات الاتصالات وتكنولوجيا المعلومات، وأن الإفصاح عن هذه المخاطر لا يؤثر بشكل معنوي على كفاءة القرارات الاستثمارية، لكنه يؤثر بشكل معنوي على القيمة الحقيقية للأسهم. كما لم تظهر فروق معنوية مرتبطة بالفترة الزمنية، بينما ظهرت بعض الفروق المرتبطة بنوع المؤسسة. وأوصت الدراسة بزيادة شفافية الإفصاح عن مخاطر الأمن السيبراني، ووضع معايير تنظيمية موحدة للإفصاح، وإنشاء إدارات مستقلة للأمن السيبراني داخل الشركات لمواجهة تزايد التهديدات.

دراسة (شاهين،2025) ناقشت الدراسة أهمية الحماية الإدارية للنظام العام في ظل اعتماد الدولة ومؤسساتها على الفضاء الإلكتروني في إدارة الأنشطة والبيانات، مما يجعل أي قصور في أمن المعلومات تهديدًا للمصالح الأساسية للدولة.كما تطرقت للاستخدام السلبي للإنترنت وماله من مخاطر تهدد الأمن العام، الأمر الذي يتطلب حماية النظام العام من المخاطر الإلكترونية، مع ضرورة تحقيق التوازن بين سلطات الضبط الإداري وحماية حقوق وحريات الأفراد وفقًا لمبدأ المشروعية ،وأكدت الدراسة أن الأمن السيبراني أصبح ضرورة أساسية للإدارة، خاصة مع التطور السريع في الأنظمة الذكية والأجهزة الإلكترونية، وأن ضعف حماية الشبكات قد يؤدي إلى اضطرابات وأخطاء في البيانات والمعلومات ويؤثر على دقتها وإمكانية تداولها.

دراسة (عبد المجيد وآخرون،2025) هدفت هذه الدراسة إلى التعرف على أثر أمن المعلومات على تحسين التنمية المستدامة في الشركة القابضة للكهرباء، وتقديم مجموعة من المقترحات والتوصيات التي تساعد على تطبيق أمن المعلومات، وتحقيق التنمية المستدامة، مما يعود بالنفع والفائدة على العاملين بالشركة بصفة خاصة والمجتمع ككل بصفة عامة، توصلت الدراسة إلى وجود تأثير أمن المعلومات على تحسين التنمية المستدامة من حيث (البعد البيئي – البعد الاقتصادي – البعد الاجتماعي).

دراسة(Ike,2024) هدفت إلى تحليل أمن المعلومات وإدارة المعرفة
كشفت النتائج عن وجود فجوة سياقية ومنهجية تتعلق بأمن المعلومات وإدارة المعرفة. وأظهرت المراجعة التجريبية الأولية أن دمج نظم المعلومات وإدارة المعرفة كان أمرًا حاسمًا لتعزيز الأداء التنظيمي وحماية الأصول الفكرية وتعزيز الابتكار. كما أكدت على الحاجة إلى نهج شامل يجمع بين الحلول التكنولوجية والسياسات القوية وثقافة الوعي الأمني. ووجدت الدراسة أن هذا الدمج أدى إلى تحسينات كبيرة في الكفاءة التشغيلية والابتكار، مع ضرورة التقييم والتكيف المستمرين. كما أبرزت الدراسة أهمية تقنيات الأمن المتقدمة والتحديثات المنتظمة وتدريب الموظفين للحفاظ على ممارسات فعالة في نظم المعلومات وإدارة المعرفة، بما يضمن في النهاية الاستخدام الآمن والفعال لأصول المعرفة لتحقيق نمو مستدام.

دراسة (Stefanova&Vasilev,2024)هدفت على الكشف عن دور أمن المعلومات كعنصر أساسي في تحوّل المجتمع وعمليات الأعمال وتعزيز القدرة التنافسية للمنظمات، وتحديد التحديات التي تواجه سوق العمل والمتعلقة بالصفات والكفاءات الجديدة في إدارة الموارد البشرية، واعتمدت الدراسة على المنهج المقارن من خلال مراجعة الأدبيات وتحليل الدراسات الحالية وتحديد أفضل الممارسات. وتوصلت إلى أن الانتشار الواسع لتقنيات المعلومات ووضع المعلومات في مركز النشاط الاقتصادي يفرضان تطوير كفاءات جديدة، وأن العامل البشري يمثل حجر الأساس في تحقيق أمن المعلومات ودعم استدامة المؤسسات وتنمية رأس المال البشري

دراسة (Ali &Tang,2023) سعت إلى تحليل وظيفة حقوق الملكية الفكرية بالتكامل مع إدارة المعرفة كوسيلة للمساعدة في حماية المعرفة، كما ألقت الضوء على الأدوار الرسمية وغير الرسمية للملكية الفكرية في حماية المعرفة التنظيمية. ركزت الأبحاث السابقة أساساً على حقوق الملكية الفكرية الرسمية، إلا أنّ هذه الدراسة تطرقت أيضاً عن قيمة حماية الملكية الفكرية غير الرسمية، وذلك لسهولتها في الإدارة وانخفاض تكلفتها في الاستخدام، وهو جانب مهم في الأنشطة اليومية لأي منظمة.

دراسة(صالح وآخرون،2020) هدفت هذه الدراسة إلى محاولة معرفة أثر إدارة أمن المعلومات على نجاح برنامج أمن المعلومات في بيئة الأعمال المصرية، وقد قدمت الدراسة إطارًا نظريًا لأهم العوامل والمتغيرات التي تؤثر على فعالية إدارة أمن المعلومات وأثرها على نجاح برنامج أمن المعلومات ،وقد توصلت نتائج الدراسة إلى أن إدارة أمن المعلومات لها تأثير جوهري وإيجابي على نجاح برنامج

أمن نظم المعلومات المحاسبية في البيئة المصرية، كما أوصت بضرورة اهتمام منظمات الأعمال بإدارة أمن المعلومات باعتبارها عنصرا هاما وضروريا لنجاح برنامج أمن المعلومات في منظمات الأعمال المصري.

دراسة (عايض وأبوهادي ،2019)سعت هذه الدراسة إلى تحديد أثر رأس المال الفكري في تحقيق الميزة التنافسية المستدامة في الشركات اليمنية للصناعات الغذائية، وقد توصلت الدراسة إلى أن الشركات قيد الدراسة تولي تحقيق الميزة التنافسية المستدامة بكافة أبعادها اهتماماً كبيراً، لكن اهتمامها بتحقق بعدي: (الجودة، والاستجابة للعميل) كان أكبر من اهتمامها بتحقق بعدي: (الكفاءة والإبداع أو التجديد)، كما تبدي الشركات اهتماماً كبيراً بتوفر رأس المال الفكري بكافة أبعاده، لكن اهتمامها بتوفر بعد رأس المال البشري كان أكبر من اهتمامها بتوفر بعدي: (رأس المال العلاقاتي، رأس المال الهيكلي). وقدمت الدراسة عدداً من التوصيات، أهمها: ضرورة تعزيز مستوى تحقق الميزة التنافسية المستدامة بجميع أبعادها، لاسيما بعد الكفاءة؛ كونه الأقل تحققاً، وكذلك الاستمرار في الاهتمام بتوفر رأس المال الفكري لما لذلك من أثر إيجابي في تحقيق الميزة التنافسية المستدامة.

3-1التعقيب على الدراسات السابقة

من خلال استعراض الدراسات السابقة التي تنازلت موضوع أمن المعلومات وعلاقته بإدارة المعرفة والأصول العرفية؛ يمكن استخلاص الآتي:

- اتفقت معظم الدراسات على أهمية أمن المعلومات والأمن السيبراني في حماية الصول المعلوماتية والمعرفية وتعريز أداء المنظمة كما ظهر في دراسات (موسى وآخرون ،2026) و (عبد المجيد وآخرون، 2025) و(Ike,2024).
- أكدت بعض الدراسات على الدور المحوري للعامل البشري في تحقيق أمن المعلومات، سواء من خلال رفع الوعي والتدريب أو من خلال تطوير الكفاءات، وهذا ما أشارت إليه دراسة (Stefanova & Vasilev, 2024).
- أظهرت دراسة (عبد المجيد وآخرون، 2025) ودراسة (صالح وآخرون، 2020). وجود علاقة بين أمن المعلومات وتحسين نتائج الأداء المؤسسي أو الاقتصادي أو التنموي.
- أوضحت بعض الدراسات أهمية التكامل بين أمن المعلومات وإدارة المعرفة وحماية الأصول الفكرية، وهو ما أوضحته دراسات (Ike, 2024) و(Ali & Tang, 2023).

استفادت الدراسة الحالية من الدراسات السابقة من الأطر النظرية التي تناولت العلاقة بين أمن المعلومات وإدارة المعرفة في بناء الإطار النظري للدراسة الحالية، ومن التوصيات التي أكدت على أهمية تعزيز الوعي الأمني وتدريب العاملين وتطوير السياسات والإجراءات والتي تمثل عناصر أساسية لنجاح نظم أمن المعلومات وأمن المعرفة.

على الرغم من تعدد الدراسات التي تناولت أمن المعلومات أو إدارة المعرفة كل على حدة فإن هناك نقص في الدراسات التي تناولت أمن المعرفة بوصفه مجالا مستقلا ومتكاملا مع إدارة المعرفة والأصول المعرفية لذا تسعى الدراسة الحالية بتناوله من خلال التركيز على أمن المعرفة باعتباره جزء من أمن المعلومات وتوضيح دوره في حماية الأصول المعرفية وتعزيز كفاءة أداء المنظمة.

4-الإطار النظري

4-1 مفهوم أمن المعرفة:

يقع أمن المعرفة عند تقاطع مجالين شائعين من أبحاث نظم المعلومات إدارة المعرفة وأمن المعلومات. لقد شهدت الأبحاث في هذين المجالين نمواً كبيراً في الآونة الأخيرة. ينبع الاهتمام بإدارة المعرفة من الاعتراف بأن الأصول المعرفية هي المصدر الأهم للميزة التنافسية للمؤسسة، وأما البحث في أمن نظم المعلومات فقد نما بشكل مطرد بسبب الإدراك بأن اختراق نظم المعلومات يمكن أن تكلف المؤسسة كثيراً. فقدان البيانات نتيجة سوء التعامل معها سرقة المعلومات من قبل القراصنة، تزويد غير مصرح به بالمعلومات، جميعها يمكن أن تكبد المؤسسة خسائر فعلية وضياع فرص الربح. وبينما شهد هذان المجالان نمواً ملحوظاً خلال السنوات الأخيرة، إلا أن الأبحاث التي تقع عند تقاطع هذين المجالين لا تزال في مراحلها الأولى (Desouza,2006:2) . لضمان أمن المعرفة في المؤسسة من الضروري التأكيد على أن حماية قاعدة المعرفة، والتي لا تطبق على جميع أنواع المعرفة المؤسسية، بل تقتصر على المعارف المهمة وذات القيمة والخاصة والسرية، لذا يجب أولا تصنيف المعرفة، ثم الشروع في عملية استخراج المعارف التي تتطلب الحماية (Zhang,2011:211). يمكن وصف أمن المعرفة بأنه عملية تأمين المعرفة ضد مختلف أنواع التهديدات ،وترتبط التهديدات الشائعة للمعرفة على سبيل المثال دوران الموظفين أو تقادم المعرفة أو تسربها إلى المنافسين ، وعلى الرغم من أن البعض قد يعتقد أن أمن المعرفة يتعلق بالاستعداد للتهديدات التي تأتي من خارج المنظمة، فإن العديد من التهديدات التي تواجه المعرفة تنشأ في الواقع من داخل المنظمة نفسها،و من المهم أن نضع في الاعتبار أن كل منظمة لها طابعها الخاص بها وأنه ينبغي على كل منظمة أن تبذل جهدًا في التعرف على التهديدات ذات الصلة بها (Ilvonen et al.,2016)

ويمكن القول بأن أمن المعرفة هو مجموعة السياسات والإجراءات والتقنيات التي تهدف إلى حماية المعارف ذات القيمة والأهمية والسرية داخل المؤسسة من مختلف التهديدات الداخلية والخارجية، بما يضمن الحفاظ عليها، ومنع فقدانها أو تسربها أو إساءة استخدامها، واستدامتها كمصدر للميزة التنافسية وبذلك فإن أمن المعرفة يمثل بعدًا استراتيجيًا في إدارة المؤسسات المعاصرة لأنه يحافظ على رأس المال المعرفي ويعزز استمرارية الأداء والميزة التنافسية.

4-2 عناصر أمن المعرفة

يمكن للخصائص الأساسية لأمن المعلومات أن تستخدم أيضا لفحص أمن المعرفة وتعد السلامة (Integrity) السمة التي تعتمد عليها السمات الأخرى، وتشير السلامة إلى دقة المعرفة واكتمالها في جميع مراحل دورة حياتها. فعلى سبيل المثال، يعد النسيان تهديدًا لسلامة المعرفة. أما السرّية (Confidentiality) تشير إلى أن تكون المعرفة متاحة فقط لمن لديهم تصريح بالوصول إليها. وفي حالة المعرفة المتجسّدة في الأفراد، فإن ضمان السرية يتطلب الوعي بمن يحق له الاطلاع على المعرفة المشتركة، وأين؟ وكيف؟ ولأي غرض يمكن الوثوق به في إتاحة معرفة معينة، وأخيرًا تعرَّف الإتاحة (Availability) بأنها توفر المعرفة لمن يحتاجون إليها في الوقت الذي تُطلب فيه، إن مشاركة المعرفة مع الزملاء تعد وسيلة لضمان إتاحتها، لكن في الوقت نفسه فإن السرية تكون معرضة للخطر عندما تنتشر المعرفة إلى نطاق أوسع من الأشخاص (Ilvonen et al.,2016)

- **سلامة المعرفة:**

تعرف سلامة المعرفة بأنها دمج عدة أبعاد تضمن مجتمعةً مخرجات موثوقة وآمنة وجديرة بالثقة تعبر المعادلة عن منظورنا القائل بأن كلاً من إدارة المعرفة وأمن المعلومات عنصران حاسمان لتحقيق تكامل المعرفة في نموذج لغة كبير ،حيث تشكل هذه المكونات إطارا مفاهيميا يحّقق فيه تكامل المعرفة من خلال الموازنة بين الكفاءة والشفافية والمعنى السياقي والأمن والموثوقية (Abishethvarman et al.,2025)

تكامل المعرفة (KI) = إدارة المعرفة (KM) + أمن المعلومات (IS)

- **سرية المعرفة:**

تحظى الشركات التي لديها وصولا حصريا إلى موارد المعرفة بميزة على منافسيها، ولسرية المعرفة صلة أيضا بأمنها ، وتتمثل الإضافة التي تقدمها في ارتباطها بالطابع الضمني للمعرفة، والذي يخلق مفارقة جديدة؛ فمن ناحية إن أسهل أنواع المعرفة تأمينًا هي تلك التي تبقى في صورتها الضمنية، ومن ناحية أخرى وبالنظر إلى أن المستودعات الحصرية للمعرفة الضمنية هم الموظفون، فإن مغادرتهم الشركة قد تؤدي إلى فقدان كبير لمعرفة قيمة لم تحوّل في الوقت المناسب من معرفة ضمنية إلى معرفة صريحة ومع ذلك فإن لهذه القدرات طابعا ضمنيا ويصعب تأمينها باستخدام الأساليب التقليدية وذلك لأن التدابير الأمنية التي يمكن تطبيقها على البيانات والمعلومات للحفاظ على سريتها قد بنيت انطلاقًا من طابعها الصريح ،ويمكن استخدامها مع المعرفة الصريحة، لكنها تحتاج إلى إعادة تقييم في حالة المعرفة الضمنية، كما أن الحماية غير الكافية للمعرفة قد تعيق عمليات النقل والمشاركة، وهذا الأمر له عواقب سلبية على قدرة الشركة على الابتكار (Popescul,2011).قد تفقد المعرفة سريتها في حالة نقلها عبر شبكة تكنولوجيا المعلومات والاتصالات دون استخدام التشفير أو في حالة الحصول طرف معاد على بيانات التسجيل عن طريق استخدام أساليب التصيد الاحتيالي (Moszczyńsk et al.,2022)

- **توفر المعرفة:**

يعد توفر قاعدة معرفة منظمة بشكل جيد جزءا أساسيا من نجاح أي عمل تجاري، فهي تساعد على تحسين سهولة الوصول إلى المعلومات، وتوفر موردا قيما لكل من العملاء والموظفين على حد سواء. بالإضافة إلى ذلك، من خلال إنشاء هيكل واضح ووضع إجراءات للتحكم في الوصول، يمكن ضمان بقاء محتوى قاعدة المعرفة آمنا، ومع تطبيق العمليات المناسبة يمكن الحفاظ على قاعدة معرفة فعّالة وضمان استمرارية نجاحها (Dunn,2025)

ونرى أن أمن المعرفة يرتكز على ثلاثة عناصر مترابطة: سلامة المعرفة وسريتها وتوفرها حيث تشير السلامة إلى ضمان دقة المعرفة واكتمالها وموثوقيتها في جميع مراحل دورة حياتها أما السرية فتعني حماية المعرفة من الوصول غير المصرح به، مع مراعاة طبيعتها الضمنية والصريحة. ويتمثل التوفر في إتاحة المعرفة للأشخاص المناسبين في الوقت المناسب لدعم الأداء واتخاذ القرار. ويتحقق تكامل المعرفة من خلال الدمج بين إدارة المعرفة وأمن المعلومات، بما يحقق توازنا بين الحماية والمشاركة، ويسهم في تعزيز الابتكار واستدامة الأداء المؤسسي.

4-3 أبعاد أمن المعرفة

يحتوي أمن المعرفة على ثلاثة أبعاد: الأفراد والمنتجات والعمليات، وامتدادا لهذه الأبعاد يمكن استخلاص عدة دلالات (Zieba& Bongiovanni,2022):

البعد الأول: يتعلق ببعد الأفراد قد يكون من المفيد المزج بين الإجراءات الصلبة والناعمة في أمن المعلومات (مثل الجدران النارية وتدريب الموظفين)، إذ تعتمد المنظمات على الموظفين لتطبيق ممارسات مناسبة (مثل استخدام البرمجيات المصرح بها على أجهزة العمل والاتصال عبر الشبكات الخاصة الافتراضية وغيرها).

البعد الثاني: عند النظر إلى بعد المنتجات، قد يكون من المفيد أيضاً الاستفادة من دروس إدارة أمن المعلومات (فعلى سبيل المثال، يمكن حماية الشكل الصريح للمعرفة في صورة مستندات من خلال بنود السرية أو وسمها بعلامات أمنية) وتتطلب ممارسات تعتمد على الرقمنة الذكية

البعد الثالث: يتعلق بالعمليات حيث ينبغي وضع إجراءات للتواصل المعرفي، لا سيما في حالة العلاقات مع الجهات الخارجية وعلى سبيل المثال، فإن الحكومات التي دعت مواطنيها إلى استخدام أجهزة تتبع العدوى في أعقاب جائحة كوفيد-19 سارعت إلى الاستجابة لأسئلة المستخدمين المتعلقة بالخصوصية والأمن.

بالإضافة لما سبق ينبغي دعم أمن المعرفة بتقنيات مناسبة لإدارة المعرفة ومن أمثلة هذه التقنيات: الشبكات الآمنة والمنصات المحمية بكلمات مرور والمصادقة متعددة العوامل وغيرها. ومن الضروري وجود توازن دقيق في الإفراط في إتاحة الوصول إلى المعرفة والذي قد يعرّضها للخطر، في حين أن تقييد الوصول إليها بشكل مفرط قد يعيق خلق القيمة من خلال مشاركة المعرفة. إن تحقيق التوازن بين مشاركة المعرفة وحمايتها يعد أمرا أساسيا في العمل المؤسسي.

5-العلاقة بين أمن المعرفة وإدارة المعرفة وأوجه التكامل بينهما

يشير أمن المعرفة إلى قدرة المنظمة على حماية معرفتها الفكرية من السرقة أو الاستخدام غير المصرح به، لذا تقوم المنظمات بتنفيذ حماية الملكية الفكرية (مثل براءة الاختراع أو حقوق النشر أو العلامة التجارية)، وتمنح هذه التدابير للشركة الحق في منع المنافسين من نسخ أفكارها أو ابتكاراتها، بالإضافة إلى إمكانية ترخيص حقوق ملكيتها الفكرية (Ha et al.,2021) .

تشمل إدارة المعرفة مجموعة من العمليات والمنهجيات التي تهدف إلى إنشاء، توثيق، مشاركة، وتطبيق المعرفة داخل المؤسسة لتحقيق أهدافها الاستراتيجية وزيادة كفاءتها وأدائها، وتجمع بين الإدارة الاستراتيجية وأنظمة المعلومات والأصول المعرفية، وذلك بهدف تعزيز القدرة التنافسية وتحسين اتخاذ القرار والابتكار داخل المنظمة، وبالتالي فإن إدارة المعرفة ليست مجرد نظام لتخزين المعلومات، بل هي أداة استراتيجية تُستخدم لتحويل المعرفة إلى قيمة عملية تدعم نمو المؤسسة ونجاحها المستدام من خلال عمليات إدارة المعرفة هي مجموعة من العمليات الأساسية التي تُمكّن المنظمة من إدارة المعرفة بفعالية خلال دورة حياتها وهي كالتالي (Nakash&Bolisani,2025):

1. **إنشاء المعرفة (Knowledge Creation)** :عملية توليد أفكار وحلول جديدة داخل المنظمة، سواء من خلال الابتكار أو إعادة استخدام المعرفة الموجودة. يتضمن جمع أفضل الممارسات ودمج المعرفة الصريحة والضمنية ويتطلب ثقافة تنظيمية تشجع التعلم المستمر والإبداع
2. **توثيق المعرفة (Knowledge Documentation)**: تشمل حفظ المعرفة بشكل منظم في مستودعات أو أنظمة معلومات لضمان سهولة الوصول إليها وإعادة استخدامها مستقبلاً. حيث يتم التركيز على تحويل المعرفة الضمنية إلى صريحة وتحديث المستودعات باستمرار، مع استخدام تصنيفات وأنظمة تنظيمية مثل الأنطولوجيات والخرائط المعرفية
3. **مشاركة المعرفة (Knowledge Sharing)**: نقل المعرفة بين الموظفين والوحدات التنظيمية بهدف زيادة الكفاءة والتعلم المتبادل، يمكن أن تتم هذه العملية من خلال وسائل رسمية مثل التدريب أو غير رسمية مثل الشبكات الاجتماعية المهنية. وتشكل تحديًا بسبب دوافع الأفراد المحتملة لعدم المشاركة
4. **تطبيق المعرفة (Knowledge Application)**: استخدام المعرفة في القرارات والعمليات والمنتجات أو الخدمات لتحويل المعرفة إلى قيمة فعلية. يُعتبر التفعيل العملي للمعرفة لتحقيق الأهداف التنظيمية والابتكار من أهم مراحل دورة إدارة المعرفة

هذه العمليات تشكل دورة حياة المعرفة مستمرة تساهم في تنمية قدرة المنظمة على الابتكار وتحقيق الأداء المتميز من خلال استثمار المعرفة بشكل استراتيجي

تشمل عمليات إدارة المعرفة مجموعة من الأنشطة التي تهدف إلى جمع المعرفة وتنظيمها ومشاركتها واستخدامها داخل المؤسسات لتحسين الأداء واتخاذ القرارات تتضمن هذه العمليات ما يلي (Nyame & Qin,2020)

1. **تحديد المعرفة:(Knowledge Identification)** تحديد وتحديد مصادر المعرفة داخل المؤسسة، سواء كانت ضمنية (مثل الخبرة الشخصية) أو صريحة (مثل الوثائق والبيانات) .
2. **اكتساب المعرفة(Knowledge Acquisition)** : جمع المعرفة من مصادر داخلية وخارجية، مثل الموظفين، العملاء، الشركاء، أو الأبحاث.
3. **تنظيم المعرفة(Knowledge Organization)**: تصنيف وترتيب المعرفة بطريقة تسهل الوصول إليها واستخدامها . يشمل ذلك إنشاء قواعد بيانات أو مستودعات للمعرفة .
4. **مشاركة المعرف(Knowledge Sharing)**: تسهيل تبادل المعرفة بين الأفراد والفرق داخل المؤسسة من خلال الاجتماعات، ورش العمل، أو أنظمة إدارة المعرفة.
5. **تطبيق المعرفة(Knowledge Application)** : استخدام المعرفة المكتسبة والمشتركة لتحسين العمليات، اتخاذ القرارات، وحل المشكلات .
6. **تحديث المعرفة(Knowledge Update)**: مراجعة وتحديث المعرفة بانتظام لضمان أنها تظل ذات صلة ودقيقة.

7. **حماية المعرفة (Knowledge Protection)**: ضمان أمان المعرفة من الوصول غير المصرح به أو الفقدان، من خلال تطبيق سياسات التحكم في الوصول مثل نموذج التحكم في الوصول القائم على الأدوار Role Based Access Control (RBAC)

تساعد هذه العمليات المؤسسات على تحسين الكفاءة وتعزيز الابتكار وزيادة القيمة المضافة من خلال إدارة المعرفة بشكل فعال. لا تقتصر إدارة المعرفة على تداول المعرفة فقط، بل تشمل أيضًا إدارتها بشكل ديناميكي ضمن دورة حياة متكاملة بدءًا من تحديدها وحتى حمايتها وتحديثها لضمان استدامتها داخل المنظمة.

6- دور أمن المعرفة في كل مرحلة من مراحل دورة المعرفة

تمثل عمليات إدارة المعرفة عمليات متسلسلة ومتكررة (بناء المعرفة، تخزين المعرفة مشاركة المعرفة تطبيق المعرفة) لتشكل دورة حياة تطور المعرفة وأيضا سلسة القيمة المضافة (أبو رمان، 2022)

- **مرحلة إنشاء المعرفة:** يشير أمن إنشاء المعرفة إلى مجموعة الآليات التنظيمية التي تمكن في الوقت نفسه من توليد المعرفة الجديدة وتبادلها، مع حماية الأصول المعرفية الحرجة من الفقدان أو التسرب أو سوء الاستخدام. يكمن التحدي الرئيسي في إنشاء المعرفة في الانفتاح المطلوب لمشاركة المعرفة ضمن الفرق وضرورة حماية هذه المعرفة من التهديدات الالكترونية مثل التصيد الاحتيالي أو برامج الفدية والتي ارتفعت بنسبة 118% في الحوادث المسجلة (Symantec,2019).لذا يجب على المنظمات تبني نهج متعدد الطبقات يشمل الكشف عن التهديدات في الوقت الفعلي بدعم برامج الذكاء الاصطناعي خلال مراحل دمج المعرفة بالإضافة إلى التدريب الإلزامي لبناء ثقافة وعي أمني (Liu&Wu,2020)
- **مرحلة تخزين المعرفة:** تخزين المعرفة هي عملية اختيار وتنظيم معرفة وخبرات الأفراد واستراتيجيات المنظمة وأنظمتها ودلائلها، وحفظها في مستودعات المنظمة. ويسهم تخزين المعرفة في تحويل المعرفة الضمنية إلى معرفة صريحة وتحويلها إلى مورد تنظيمي يمكن الوصول إليه من خلال قواعد البيانات والشبكات وأدوات تكنولوجيا المعلومات المناسبة. يجب تنظيم المعرفة وتخزينها لحماية قيمتها من الضياع والاستفادة منها من خلال تعزيز كفاءة أنشطة المنظمة وتحسين أدائها مما يعزز كفاءة العمل وتحقيق استراتيجية المعرفة وتحسين الأداء التنظيمي المستدام(Kordab et al,2020)
- **مرحلة مشاركة المعرفة:** أصبح الأمن مصدر قلق محوري في مشاركة المعرفة، حيث تمثل إدارة المخاطر المرتبطة بها تحدياً للمنظمات، يتضمن أمن مشاركة المعرفة استراتيجيات لإدارة المخاطر لحماية وتأمين المعرفة المشتركة داخل المنظمات، من خلال معالجة مخاطر مثل التردد في مشاركة المعرفة الهامة، والإفصاح غير المقصود عن المعرفة لأطراف غير المعنية والاحتمالية المتعلقة بفقدان أو سوء استخدام المعرفة الحيوية (Sarkheyli,2023)
- **مرحلة استخدام المعرفة:** تتعرض المنظمات للعديد من التهديدات لذا يتحتم عليها اتخاذ الإجراءات اللازمة لحماية أمن المعلومات داخل المنظمة، وأن تستفيد من التجارب التي تمر بها للحد من التعرض للمخاطر في المستقبل والاستفادة من الحلول التي اتخذتها لمواجهة تلك المخاطر لتكون بمثابة دروس مستفادة لتحقيق حفظ الخبرات والمعارف وإتاحتها للموظفين الأقل خبرة، مما يدفع المنظمات إلى الحرص على حفظ التقارير الناتجة عن إدارتها لتلك الوقائع(بامفلح،2019)

بالإضافة لما سبق لابد من توفر المنظمة على خطة واضحة في الاحتفاظ بالمعارف المهمة من خلال أرشفتها أو حذف آمن، وذلك باختيار طريقة اتلاف آمنة للبيانات والتأكد أنها لم تصبح صالحة للاطلاع على محتواها بالتالي يكون أمن المعرفة قد رافق دورة

المعرفة في كل مراحلها من الإنشاء إلى الأرشفة ليعاد الاستفادة من المعارف لتوليد وابتكار أفكار جديدة أو الحذف الآمن للبيانات في تقادم المعارف وتراجع فائدتها.

يمكن القول أن أمن المعرفة هو مجموعة من الإجراءات التقنية والإدارية والقانونية والبشرية التي تهدف إلى حماية المعرفة ذات القيمة الاستراتيجية من الفقدان أو السرقة أو التسريب من خلال عدة عناصر نذكر منها :الحماية التقنية والقانونية والسياسات الإدارية والوعي عند الأفراد ،في حين أن إدارة المعرفة تشمل عملية إنشاء المعرفة وتنظيمها وتخزينها ومشاركتها للاستفادة منها داخل المنظمة بهدف تحقيق أفضل أداء فإن أمن المعرفة يضمن حماية وضبط الأنظمة التي تساعد على تحقيق الميزة التنافسية ومنع التجسس الصناعي وضمان استمرارية الأعمال.

7-أهمية أمن المعرفة في حماية الأصول المعرفية من المخاطر المحتملة

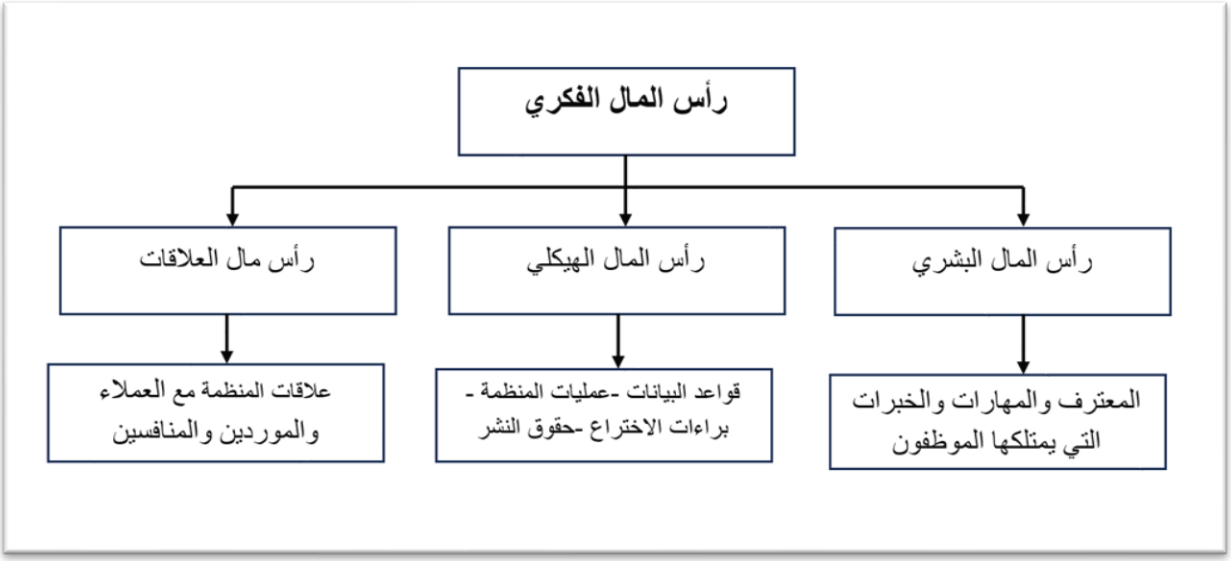
7-1الأصول المعرفية Knowledge Assets

أشير إلى مصطلح الأصول المعرفية لأول مرة في عام 2003 للإشارة إلى الموارد الفكرية المتراكمة لدى المنظمة (McInerney & Koenig, 2011)،وتشمل الأصول المعرفية المعلومات والأفكار والفهم والرؤى والمهارات التقنية والقدرات والوثائق وقواعد البيانات والبرمجيات وبراءات الاختراع والسياسات والإجراءات، وقد عرفت أصول المعرفة على أنها الخبرة العملية(know-how)التي تعتمد عليها المنظمة للاستثمار والنمو، وتعد الإدارة السليمة للأصول المعرفية عاملًا رئيسًا في تحقيق قيمة تنافسية لأصحاب المصلحة واستدامة أداء المنظمة(Boisot,2009) (Chebiego et al.,2021)

تمثل الأصول المعرفية مصدر الكفاءات والقدرات التنظيمية التي تعتبر أساسية لنجاح المنظمة وتطوير الموارد البشرية وتحقيق الميزة التنافسية، ومن أجل الاستفادة من الأصول المعرفية وإدارة المعرفة واستغلالها بفعالية، يجب على المنظمات أن تكون قادرة على تحديد هذه الموارد والحفاظ عليها. ولذلك يتعين على الشركة رسم خريطة لمخزونات أصولها المعرفية مع مراعاة أنها ديناميكية، لكي تتمكن من إنشاء أصول معرفية جديدة من الأصول الموجودة، تشمل الأصول المعرفية كلاً من الأصول الملموسة وغير الملموسة التي تعد مصدر للميزة التنافسية للشركة.

7-1-2 مكونات الأصول المعرفية

تهدف إدارة الأصول المعرفية في المنظمة إلى تحقيق أهدافها. وتشمل إدارة المعرفة كلًّا من المعرفة الصريحة الموثقة والمعرفة الضمنية الذاتية. كما تشمل جميع العمليات المرتبطة بتحديد المعرفة ومشاركتها وإنتاجها. وكما أوضح كل من Kongو Thomson (2009) أن مفهوم رأس المال الفكري يعرض المعرفة عبر ثلاثة مؤشرات شكل رقم (1) رئيسية مترابطة وهي: رأس المال البشري ورأس المال الهيكلي ورأس المال العلاقي(Alhamoudi,2023)



شكل رقم(1) مكونات رأس المال الفكري

- **رأس المال البشري(Human Capital)**

يُعد رأس المال البشري أحد المكونات الأساسية لرأس المال الفكري، الذي يشير إلى مجموعة المعارف التي تستخدمها المنظمات لتحقيق ميزة تنافسية، وتُعتبر كفاءة الموظفين أصلًا غير ملموس وضمني وفردي، يمكّن رأس المال البشري من التمييز بينه وبين رأس المال الاجتماعي والهيكلي للمنظمة وقد مثّل تراكم مهارات الموظفين وخبراتهم ومعارفهم حالة رأس المال البشري(Islam &Amin,2021)

- **رأس المال الهيكلي Structural Capital**

يمثل راس المال الهيكلي كل ما تمتلكه المنظمة من موجودات فكرية هيكلية من قواعد البيانات براءات الاختراع والاسم التجاري وحقوق النشر والتي يتم توظيفها في دعم عمليات المنظمة الداخلية والخارجية، وتكمن أهمية راس المال الهيكلي في إدارة الأعمال في زيادة الميزة التنافسية مثل الجودة العالية والمرونة والاستجابة للتغيرات والتكيف معها والتي تسهم في بناء قدرات جوهرية تعتمد عليها المنظمة في توليد مزايا تنافسية جديدة تعتمد على قدرة المنظمة المعرفية (كرجي وآخرون،2022)

يمثل رأس المال الهيكلي البنية التحتية والداعمة للموظفين التي تبقى داخل المنظمة حتى بعد مغادرة الموظفين، ويشمل قواعد البيانات وأدلة العمليات والهياكل التنظيمية والبرمجيات والإجراءات الخاصة بالمنظمة، يوفر هذا المكون البنية التحتية اللازمة للأفراد للاستفادة من مهاراتهم الشخصية وتحويلها إلى قيمة تنظيمية (حسين ،2022)

- **رأس مال العلاقات/الخارجي(Relational/External Capital)**

يشير رأس مال العلاقات إلى المعرفة حول علاقة المنظمة بالأطراف الخارجية مثل العملاء والموردين والمنافسين وأصحاب المصلحة ويمثل القيمة الناتجة عن العلاقات بين المنظمات والبيئة الخارجية والقدرة على فهم وإدراك المحيط الخارجي للمنظمة بهدف تحقيق التفوق التنافسي وتكوين الأصول القائمة على الابتكار المفتوح (محمود وخلف ،2023)

ونرى أن الأصول المعرفية تمثل الموارد الفكرية المتراكمة لدى المنظمة، والتي تشمل المهارات والوثائق البرمجيات وبراءات الاختراع، والتي تعد أساساً لتحقيق الميزة التنافسية والنمو المستدام. تنقسم هذه الأصول إلى ثلاث مكونات رئيسية: رأس المال البشري الذي يشمل مهارات وخبرات الموظفين، ورأس المال الهيكلي الذي يشمل البنية التحتية الفكرية مثل قواعد البيانات والإجراءات التي تدعم العمليات الداخلية، ورأس مال العلاقات الذي يعبر عن علاقات المنظمة مع العملاء والموردين والأطراف الخارجية الأخرى. الإدارة الفعالة للأصول المعرفية تمكن المنظمة من استغلال معرفتها بشكل أفضل، وتحويلها إلى قيمة تنافسية مستدامة، من خلال الحفاظ على هذه الموارد وتنميتها باستمرار.

7-2المخاطر التي تهدد الأصول المعرفية وسبل حمايتها

7-2-1 المخاطر التي يتعرض لها رأس المال البشري:

اختلف الباحثين في تحديد المخاطر المرتبطة برأس المال البشري والتي تعرض المنظمة إلى مخاطر مالية ومخاطر تشغيلية وتشمل هذه المخاطر ما يلي(السنهوتي،2022):

الخطر	الوصف
خطر خسارة الموارد البشرية الإستراتيجية	تدخل بعض الموارد البشرية ضمن الموارد الاستراتيجية وخسارتها تؤثر سلبا على تنافسية المؤسسة ،وذلك لأن فقدان المهارات التي تستقيل لتعمل لدى مؤسسات منافسة يشكل خطرا ،حيث يكون الخطر الإستراتيجي أكبر كلما تعلق الأمر بالمعرفة الضمنية والمهارات ،ففقدان المؤسسة لمواردها البشرية يؤدي حتما إلى انخفاض قدرتها التنافسية في الأسواق
خطر فقدان المهارات البشرية النوعية	يعني فقدان موظف ذو خبرة نادرة وعدم القدرة على تعويضه بشخص بذات المهارة والخبرة لا من خلال التوظيف أو التدريب يعرض المؤسسة إلى خطر على سبيل المثال فقدان محلل مالي قام بخبرة محاسبية حول تقييم المخاطر في المؤسسة
خطر الخطأ البشري	يتسبب أحيانا المورد البشري في أخطاء بعضها يمكن تصحيحه دون تكبد خسائر كبيرة في حين توجد أخطاء أخرى ينجم عنها خسائر كبيرة سواء كان الخطأ مقصود أو عن سوء فهم من قبل العمال يسبب الخطأ البشري خطرا على المؤسسة ككل لأن الفشل في قطا ع معين يمكن أن يؤثر سلبا على قطاع آخر داخل المؤسسة

خطر الاختلاس	ينجم خطر الاختلاس عن قيام العوامل البشرية بعملية احتيال داخلي في المؤسسة عن طريق التلاعب في الوثائق المحاسبية أو التزوير أو السرقة والعمل لحسابهم الخاص وهذا الخطر لا ينتج عنه خسائر مالية فقط بل يساهم في تشويه سمعة المؤسسة وتدهور صورتها بين المؤسسات المنافسة
خطر الخلاف (الصراع)	يتعلق خطر الصراع بالقدرة التفاوضية للعمال في المؤسسة ،حيث أن المهارات الإستراتيجية تمنح صاحبها قدرة تفاوضية كبيرة تمكنه من القيام بما يلي: • التهديد بترك العمل في الوقت الذي تكون المؤسسة بحاجة إلى خبرته • التهديد بتشويه سمعة المؤسسة • الإضراب عن العمل مما يعرقل سير عمل المؤسسة ويؤدي إلى خسارتها

- **المخاطر التي تهدد رأس المال الهيكلي**

تعطل القيادة السامة الكفاءة المؤسسية وتضعف رأس المال التنظيمي عبر سياقات متعددة، حيث تؤدي إلى ضعف التماسك المؤسسي ويصبح العاملون أقل التزاما بالأهداف المؤسسية والشهور بالإحباط في ظل قيادة لا تقدر موظفيها (جلال ومتولي،2025). تتمثل المخاطر الرئيسية الكامنة في تسريب البيانات وسرقة الملكية الفكرية وإلحاق الضرر بالبنية التحتية لتكنولوجيا المعلومات. تزال بعض المؤسسات لا تعتبر سرقة البيانات من قبل الموظفين خطراً جسيماً يستدعي السيطرة عليه، وتتمثل العوامل الرئيسية التي تدفع الموظفين إلى تسريب البيانات في المكاسب المالية وانعدام العدالة والإنصاف في بيئة العمل والتقنيات الحديثة ونقص التعليم والتوعية ونقص أدوات الإدارة اللازمة لفهم التهديدات الداخلية (Al-Harrasi et al.,2023)

- **المخاطر السيبرانية التي تهدد رأس مال العلاقات:**

نمت الهجمات السيبرانية بشكل ملحوظ من حيث حجمها وتعقيدها منذ ظهور فيروسات الحاسوب الأولى في السبعينات، ومع ارتفاع عدد الأجهزة المتصلة بالإنترنت وارتفاع نسبة الاعتماد على أنظمة تكنولوجيا المعلومات من قبل الشركات وتخصيص ميزانيات منخفضة للأمن السيبراني (جغل وزقرير،2023). يؤثر الخطر المتعلق بأمن تكنولوجيا المعلومات على إتاحة وسلامة وسرية المعلومات والبنية التحتية للشركة وتصل الهجمات الصادرة التي تهدد الشركة إلى 60% تأتي من الزبائن أو الزوار أو المجهزين أو مزودي الخدمة ،فكل هؤلاء بإمكانهم الاطلاع على المعاملات التجارية وعلى الأسرار التكنولوجية والمالية وبالتالي تسريب تلك المعلومات ،وتشمل التهديدات من خارج الشركة أنظمة الإعلام الآلي والبرمجيات الخبيثة التي يتم برمجتها وإدراجها عمدا في نظام الحاسوب لأغراض غير

أخلاقية بدون علم المالك تستخدم لعرقلة تشغيل الحاسوب والوصول إلى أنظمة الكمبيوتر الخاصة بالشركة ومن الأمثلة على البرمجيات الخبيثة ديدان الحاسوب Computer worms والفيروسات Viruses وبرامج التجسس Key Logger والذي يقوم بتسجيل المعلومات وإرسالها إلى المخترق (Ali et al.,2025)

8- دور أمن المعرفة في حماية الأصول المعرفية

8 -1 حماية رأس المال البشري:

يتجاوز دور أمن المعرفة مجرد تقديم الحماية اللازمة لتقنية للمعلومات ليصل إلى حماية المورد البشري وتطوير قدراته. يهدف هذا التوجه إلى تقليل الفجوات الناتجة عن فقدان الكفاءات أو الأخطاء غير المقصودة، مع تعزيز بيئة عمل ملائمة يسودها التعاون والالتزام التنظيمي. يستعرض الجدول أدناه تصنيفاً للمخاطر البشرية الإستراتيجية والتشغيلية، موضحاً الدور الحيوي الذي يلعبه أمن المعرفة في تحويل هذه التحديات إلى فرص لتعزيز الأداء المؤسسي والميزة التنافسية

الخطر	الدور المحتمل لأمن المعرفة
خطر خسارة الموارد البشرية الإستراتيجية	يعد التمكين من الأدوات الاستراتيجية الفعالة التي تعتمدها المؤسسات لتشجيع الموارد البشرية وتحفيزهم وزيادة الثقة بقدراتهم الذاتية مما يعزز رغبتهم المستمرة في تطوير مهاراتهم وذلك بتهيئة الظروف التي تسمح للموارد البشرية بتنمية إمكاناتهم وتطويرها لتواكب متطلبات التطور السريع ورفع كفاءات العمليات الداخلية وتحقيق الميزة التنافسية للمؤسسة (شريط،2025)
خطر فقدان المهارات البشرية النوعية	من المهم أن تحدد المنظمة من هم الموظفون ذوو المهارات العالية وتلبية حاجاتهم المهنية والاجتماعية لضمان بقائهم أطول وتبني ممارسات إدارة موارد بشرية متكاملة تركز على تعزيز العقد النفسي والالتزام التنظيمي وتوفير بيئة عمل محفزة تتيح فرص للنمو داخل المؤسسة(عابد،2025)
خطر الخطأ البشري	يتطلب الحد من الخطأ البشري داخل المنظمة اتباع منهجية متكاملة تشمل التحليل النفسي والسلوكي للموظفين وتوفير تدريب شامل ومستمر يركز على مخاطر تسريب المعلومات وأساليب الحماية وتطوير التدابير الأمنية ورفع مستوى الالتزام بها في المؤسسات (Pollock,2017)
خطر الاختلاس	قد يكون الموظف سببا في تكبد المؤسسة خسائر جسيمة سواء عن عمد أو نتيجة للجهل بسياسات أمن المعلومات وللحد من ذلك يجب تطبيق سياسات صارمة لاستخدام

	الأجهزة والتطبيقات واعتماد تقنيات أمنية متقدمة مثل المصادقة الثنائية والتشفير، بالإضافة إلى مراجعة صلاحيات الوصول وتعزيز الرقابة وبناء ثقافة مؤسسية داعمة للأمن السيبراني وتعزيز برامج التدريب والتوعية(مصباح،2025)
خطر الخلاف (الصراع)	تتعامل المنظمات مع النزاعات بإدارة الصراع بين العاملين وأُستخدام عدة استراتيجيات من أبرزها(عطية ورضوان،2026): • **التعاون:** ويعتمد على التعاون بين أطراف الصراع وتبادل المعلومات والتواصل المفتوح لتحليل أسباب الصراع والوصول إلى حل حقيقي للمشكلة • **التسوية:** يسعى الفرد إلى التقليل من الاختلافات والاهتمام بالقواسم المشتركة لإرضاء الطرف الآخر • **التجنب:**يظهر من خلال تجاهل الصراع الانسحاب ويتخذ ثلاث صور هي: 1. الإهمال وتجاهل الموقف. 2. الفصل المادي بين الأطراف المتصارعة. 3. التفاعل المحدود عند الضرورة فقط

2-8 دور أمن المعرفة في حماية رأس المال الهيكلي

يتم حماية مستودعات المعرفة داخل المنظمة من خلال التحكم في إتاحة المحتوى للأفراد عن طريق مصادقة كلمة المرور، كما تشمل ضوابط النفاذ على حماية المعلومات الخاصة بالملكية وحماية الملكية الفكرية وتستخدم بعض المستودعات إدارة الحقوق الرقمية Digital rights managementلحماية الملكية الفكرية واستثمارها في السوق (محنبي واليوبي ،2023). يشير مصطلح إدارة الحقوق الرقمية إلى مجموعة من السياسات والتقنيات والأدوات التي توجه الاستخدام الأمثل للمحتوى الرقمي ،حيث يعتمد هذا النظام على ضمان عدم وصول الأشخاص غير المصرح لهم للاطلاع على الملفات الحساسة. بالإضافة إلى أنظمة حماية تسريب البيانات Data Leak Protection (DLP)،والتي صممت لمراقبة تدفق البيانات داخل المؤسسة وتطبيق إجراءات محددة مسبقا على الأجهزة الطرفية أو الشبكات داخلها ،ويضمن دمج سياسات إدارة الحقوق الرقمية أنظمة حماية تسريب البيانات لتقليل الثغرات الأمنية إلى حد أدنى ، وتمكين المؤسسة من منع الوصول الفوري إلى أي ملف، وذلك بتوفير حماية مستمرة للمستندات باستخدام أساليب التشفير، ومنع قراءة

مستند أُرسل عن طريق الخطأ. بالإضافة إلى منع انتشار الملف على الشبكة الخارجية بعد تصفيته ومنع المخترقين المحترفين من محاولة فك تشفير محتواه(Herrera et al.,2022).

3-8 دور أمن المعرفة في حماية رأس مال العلاقات

يعتبر رأس مال العلاقات مكون أساسي يسهم في تطوير رأس المال الفكري من خلال التواصل وتبادل المعلومات بين المنظمة وعلاقاتها الخارجية ،وذلك عبر أساليب فعالة لنقل المعرفة ،الأمر الذي يعزز المعرفة التنظيمية ،ونظرا لأهمية رأس مال العلاقات والتي تسهم في ترسيخ العلاقات مع أصحاب المصلحة الخارجيين يجب الحفاظ عليه من خلال تعزيز أبعاده الأساسية المتمثلة في الآتي(جبريل وآخرون،2024):

- **الشفافية:**تعد الإدارة بالشفافية كأحد أهم أركان ومقومات نجاح التنمية المستدامة، لأنها توفر العمل في بيئة تتسم بالشفافية التامة تؤدي إلى جودة الأداء البشري والمؤسسي. وقد ثبت أن في تطبيق الممارسات الإدارية الداعمة على الشفافية حلاً للمشكلات التي تواجه المؤسسات وتعكس قابلية الفريق أو العاملين داخل المنظمة على الانفتاح على الآخرين بما يسهم في زيادة التعلم وبالتالي يمكن القول إن جوهر الشفافية يرتبط بأربع صفات وهي : المصداقية والوضوح والإفصاح والمشاركة
- **الثقة:** يقصد بها مدى قدرة الموظفين على زيادة ثقة العملاء بالمنظمة من خلال المصداقية والمهنية في التعامل كما تعكس المستوى الذي يشعر به كل طرف في الاعتماد على سلامة الوعود التي يقدمها الطرف الآخر، فهي تعتبر مفتاحا لبناء نموذج التسويق بالعلاقات، إذ تعد الثقة أساس التعامل وبناء علاقات طويلة بين المنظمة وعملائها
- **التفاعل:**يعتبر التفاعل العامل المهم الذي يؤثر في طبيعة العلاقات المختلفة بين المنظمة وعملائها، إذ يسهم وبصورة مؤثرة في تأكيد ونقل المعلومات وتطور الاتصال بينهما ،وإضافة إلى ذلك لا يمكن أن تبلغ نوعية الخدمات مستويات عالية إلا إذا كان هناك اتصال واضح بين عمال الخدمة والعملاء وبين أعضاء الفريق الواحد ،وذلك بدقة نقل الرسائل وبشكل مفهوم ضمن توقيت محدد ومناسب.

تعد حماية حقوق الملكية الفكرية الأساس الي يضمن للمنتج الحفاظ على تفوقه النسبي في السوق وتحسين الأداء المالي للمؤسسة من خلال الإيرادات الناتجة عن الترخيص وخفض النفقات وتشجيع الاستثمار وتحقيق الميزة التنافسية(حجاجي،2023) .اكتسب أمن المعلومات والأمن السيبراني أهمية قصوى وذلك يرجع لزيادة الوعي لدى المنظمات بضرورة حماية البنية التحتية لتكنولوجيا المعلومات ضد الهجمات السيبرانية ، بالإضافة إلى حماية الأفراد العاملين داخل الفضاء السيبراني ، تواجه المنظمات مجموعة متنوعة من المخاطر، تشمل الهجمات الإلكترونية والمادية، والتي تشكل تهديداً لسرية المعلومات وسلامتها وتوافرها وعندما يجد قادة الشركات أو المستثمرون أو الأطراف المهتمة الأخرى أنفسهم غير قادرين على الاعتماد على دقة المعلومات التي يتلقونها، فإن ذلك سيؤثر حتماً على عمليات اتخاذ القرار لديهم (EL-Qadi et al.,2024)

على ضوء ما سبق ،تبين أن الأصول المعرفية بمكوناتها الثلاثة (رأس المال البشري ورأس المال الهيكلي ورأس مال العلاقات) تمثل الركيزة الأساسية لتحقيق الميزة التنافسية والاستدامة في المنظمات المعاصرة. وعلى الرغم من قيمتها العالية إلا أنها تواجه تهديدات متنوعة داخلية وخارجية ، بدءاً من المخاطر المرتبطة بالعنصر البشري كفقدان الكفاءات النوعية والأخطاء البشرية المقصودة وغير المقصودة، وصولاً إلى المخاطر التقنية والهجمات السيبرانية التي تشكل خطرا على البنية التحتية وقواعد البيانات وعلاقات المنظمة الخارجية. ومن هذا المنطلق تبرز أهمية تبني استراتيجية أمن المعرفة كإطار متكامل لا يقتصر على الحماية التقنية فقط، بل يشمل

تمكين الموارد البشرية واعتماد تقنيات متقدمة مثل أنظمة منع تسريب البيانات وإدارة الحقوق الرقمية ، بالإضافة إلى تشجيع التفاعل بين المنظمة وعملائها وترسيخ قيم الشفافية والثقة مع أصحاب المصلحة مما يعزز تحويل هذه الأصول إلى قيمة اقتصادية مستدامة وحمايتها من كافة التهديدات المحتملة.

إن مجرد امتلاك المنظمة الأصول المعرفية لا يكفي ،بل إن حمايتها وصيانتها هي التي تضمن تحقيق الميزة التنافسية المستدامة، وذلك من خلال تبني استراتيجيات فعالة تسهم في حماية الرأس المال البشري كمحرك أساسي للابتكار والنمو، حيث يشمل مهارات الموظفين ومعارفهم الضمنية ورأس المال الهيكلي الذي يمثل البنية التحتية المعرفية للمنظمة ورأس مال العلاقات الذي يمثل الروابط الخارجية للمنظمة مع العملاء والموردين والشركاء الاستراتيجيين.

النتائج:

بناء على الأهداف المحددة للدراسة، تم التوصل إلى النتائج الآتية:

1. تحديد مفهوم وأبعاد أمن المعرفة: أظهرت الدراسة أن أمن المعرفة هو مفهوم متكامل يجمع بين الجوانب التقنية والجوانب التنظيمية والبشرية، مما يضمن أمن معرفة العاملين وحمايتها من الإفصاح غير المصرح به أو التعديل المتعمد.

2. طبيعة العلاقة بين أمن المعرفة وإدارة المعرفة والتكامل بينهم : تبين وجود علاقة تكاملية وطيدة؛ حيث تعمل إدارة المعرفة على تسهيل تدفق الأصول المعرفية واستثمارها، بينما يعمل أمن المعرفة كإطار تنظيمي يضمن سلامة هذا التدفق وحماية الأصول المعرفية غير الملموسة للمنظمة.

3. أهمية أمن المعرفة في حماية الأصول المعرفية من المخاطر المحتملة: أثبتت الدراسة أن أمن المعرفة يلعب دوراً محورياً في حماية الأصول المعرفية بمكوناتها الثلاث :

- رأس المال البشري من خلال تقليص مخاطر فقدان الكفاءات النوعية والحد من تسريب الخبرات
- رأس المال الهيكلي: عبر توفير حماية مستمرة للمستندات والأنظمة باستخدام التشفير وإدارة الحقوق الرقمية
- رأس مال العلاقات: بتعزيز قيم الثقة والشفافية والتفاعل الآمن مع أصحاب المصلحة الخارجيين.

التوصيات:

انطلاقا من النتائج التي توصلت إليها الدراسة، يمكن تقديم التوصيات الآتية لتعزيز أمن المعرفة ودعم إدارة المعرفة في المنظمات:

1. دمج أمن المعرفة في الاستراتيجية التنظيمية: يجب على المنظمات عدم التعامل مع أمن المعرفة كإجراء تقني فحسب بل كجزء لا يتجزأ من رؤية المنظمة واستراتيجيتها لإدارة المعرفة

2. تعزيز الوعي الأمني المعرفي: الاستثمار في برامج تدريبية مستمرة للعاملين لرفع مستوى وعيهم بأهمية المعرفة الضمنية وكيفية حمايتها من التسريب غير المقصود، والتركيز على أخلاقيات التعامل مع الأصول المعرفية.

3. تبني تقنيات حماية متقدمة: تفعيل أنظمة إدارة الحقوق الرقمية وأنظمة منع تسريب البيانات لحماية رأس المال الهيكلي، ضمان تشفير الوثائق الحساسة وبراءات الاختراع والعمليات التشغيلية.

4. توثيق وحماية المعرفة الضمنية: وضع آليات فعالة لتحويل المعرفة الضمنية التي يمتلكها الخبراء (رأس المال إلى معرفة صريحة مخزنة بشكل آمن، لتقليل مخاطر فقدان المعرفة عند مغادرة الكفاءات للمنظمة.

5. بناء بروتوكولات اتصال شفافة وآمنة مع الشركاء والعملاء، تضمن تبادل المعلومات بثقة ومصداقية، مما يحافظ سمعة المنظمة وعلاقاتها الاستراتيجية.

6. إجراء تدقيق دوري (Knowledge Security Audit) لتقييم مدى فعالية الإجراءات الأمنية المتبعة، وتحديث الثغرات الأمنية بما يتماشى مع التطورات السريعة في التحول الرقمي والهجمات السيبرانية.

7. خلق بيئة تنظيمية توازن بين مشاركة المعرفة لتحفيز الابتكار وبين الضوابط الأمنية لضمان عدم وصولها لجهات غير مصرح لها.

خاتمة

في الختام، يُعد أمن المعرفة الركيزة الأساسية التي تضمن نجاح استراتيجيات إدارة المعرفة في المنظمات الحديثة. لقد كشفت هذه الدراسة أن التهديدات التي تواجه الأصول المعرفية لا تقتصر على الهجمات السيبرانية الخارجية، بل تشمل أيضاً المخاطر المرتبطة بالعنصر البشري ونقص الوعي الأمني. إن بناء إطار أمني متكامل يجمع بين الحلول التكنولوجية المتطورة وثقافة تنظيمية واعية هو السبيل الوحيد لتحويل المعرفة إلى ميزة تنافسية مستدامة. وبناءً على ذلك، توصي الدراسة بضرورة تبني استراتيجيات أمن معرفة شاملة تواكب وتيرة التحول الرقمي وتضمن استمرارية الابتكار والنمو

المصادر

أولا: العربية

أبو رمان، معاذ خالد عبد الرحيم. (2022). أثر البوابات الإلكترونية في عمليات إدارة المعرفة: دراسة ميدانية في وزارة المياه والري الأردنية. *مجلة رماح للبحوث والدراسات*، *ع72*، 331 .374 – مسترجع من http://search.mandumah.com/Record/1328353

بامفلح، فاتن سعيد مبارك. (2019). قواعد المعرفة واستخدامها لإدارة وقائع أمن المعلومات: دراسة حالة على عمادة تقنية المعلومات بجامعة الملك عبد العزيز بجدة. *اعلم*، *ع23*، 257 .300 – مسترجع من http://search.mandumah.com/Record/970733

جبريل، وائل محمد .خالد حسين دخيل، وليد عبد الله محمد. (2024). أثر رأس مال العلاقات على إدارة الأزمات بالمصارف التجارية الليبية الخاصة بمدينتي بنغازي والبيضاء: الدور الوسيط لمتغير سلوكيات المواطنة التنظيمية. *مجلة جامعة درنة للعلوم*

الإنسانية والاجتماعية. 505–551. *2*(3), https://dujhss.uod.edu.ly/index.php/dujhss/article/download/152/149

جلال، أبو بكر أحمد صديق، ومتولي، التهامي محمد إبراهيم. (2025). القيادة السامة للأقسام الأكاديمية وأثرها على رأس المال الفكري لأعضاء هيئة التدريس بالجامعات المصرية. *مجلة كلية التربية بتفهنا الأشراف، مج3, ع3*، 2119. 2203 – مسترجع من http://search.mandumah.com/Record/1583157

جغل جميلة، زقرير عادل . (2023). الأمن السيبراني والشمول المالي في ظل التجول الرقمي للقطاع المالي. مجلة التنمية الاقتصادية, 8(1), 303–319 https://asjp.cerist.dz/en/article/229642 .

جوهري، داليا مصطفى. (2022). تأثير المعرفة كأحد الأصول الرأسمالية "رأس المال الفكري" على المؤسسات الصناعية. *المجلة العربية الدولية لإدارة المعرفة، مج1, ع1*، 115. 148 – مسترجع من http://search.mandumah.com/Record/1216687

حجاجي، محمود محمد محمود محمد. (2023). دور رأس المال الفكري في ظل اقتصاد المعرفة. *مجلة الدراسات القانونية والاقتصادية، مج9, ع4*، 52. 71 – مسترجع من http://search.mandumah.com/Record/1513683

الحربي، فهد عبد الرحمن، والحربي، فهد بدر. (2026). دور إدارة المعرفة لتحقيق التنمية المستدامة في ضوء التحول الرقمي بالتعليم الجامعي: دراسة نظرية تحليلية. *المجلة الدولية للعلوم التربوية والإنسانية المعاصرة، مج5, ع1*، 1. 56 – مسترجع من http://search.mandumah.com/Record/1646344

حسين ،إيناس علاء الدين . (2022). تأثير رأس المال الفكري في تحقيق التميز المؤسسي داخل المنظمات العامة دراسة ميدانية على مكاتب البريد المصري The Impact of Intellectual Capital on Achieving Organizational Excellence in Public Organizations A Field Study on Egyptian Post Offices. *مجلة المعهد العالي للدراسات النوعية*, *2*(4), 1243–1330.

السنهوتى، امباركه محمود السيد سليمان. (2022). تنمية رأس المال البشري في قطاع التنمية الاجتماعية بوزارة التضامن الاجتماعي. *مجلة الخدمة الاجتماعية*, *73*(1), 241–257. https://doi.org/10.21608/egjsw.2022.149836.1109

شاهين، حسن محمد عبد الموجود أحمد. (2025). الحماية الإدارية للنظام العام من المخاطر الإلكترونية. *مجلة البحوث الفقهية والقانونية، ع48*، 49022. 5017 – مسترجع من http://search.mandumah.com/Record/1588372

شريط، نسيمة. (2025). إدارة الموارد البشرية وفق مدخل إدارة الجودة الشاملة. *مجلة المنهل الاقتصادي*, *8*(2), 221–234. https://asjp.cerist.dz/en/downArticle/479/8/2/282904

صالح، رضا ابراهيم، أبو موسي، أحمد عبد السلام، أبو سعدة، & ندا حامد توفيق. (2020). دراسة أثر إدارة أمن المعلومات على نجاح برنامج أمن نظم المعلومات المحاسبية: مع دراسة ميدانية على الشركات المصرية. *مجلة الدراسات التجارية المعاصرة*, *6*(العدد 10), 101-142.مسترجع من https://doi.org/10.21608/csj.2020.136706

ضليمي ،سوسن طه .(2022).إدارة المعرفة : المفاهيم والوظائف .شركة تكوين العالمية ط2 ،ج1 جدة

عابد، إيهاب لطفي عبد العال. (2025). توسيط العقد النفسي والالتزام التنظيمي في العلاقة بين ممارسات إدارة الموارد البشرية والاحتفاظ بالموظفين دراسة تطبيقية. *مجلة راية الدولية للعلوم التجارية*, *4*(12),1419- 1510 مسترجع من https://doi-org.sdl.idm.oclc.org/10.21608/rijcs.2025.325874.1183

عايض، عبد اللطيف مصلح محمد، وأبو هادي، أحمد جابر حسين. (2019). أثر رأس المال الفكري في تحقيق الميزة التنافسية المستدامة: دراسة ميدانية في الشركات اليمنية للصناعات الغذائية .*مجلة الآداب*، *ع12* ، 170 .210 – مسترجع من http://search.mandumah.com/Record/996751

عبد المجيد، هشام عبد القادر، الزيادي، بسنت عادل رمضان، وعبد المنعم، محمد بهاء الدين. (2025). أثر أمن المعلومات على تحسين التنمية المستدامة: دراسة ميدانية على الشركة القابضة للكهرباء. المجلة العلمية للاقتصاد والتجارة، ع1، 511 – 530. مسترجع من http://search.mandumah.com/Record/1572072

عشماوي، السيد رمضان عبدالصمد. (2022). القوانين والتشريعات الحاكمة لحماية أمن المعلومات: دراسة مقارنة .*المجلة المصرية لبحوث الإعلام*، *ع80* ، 813 .836 – مسترجع من http://search.mandumah.com/Record/1347295

عطية، هند صبحي محمد، ورضوان، طارق رضوان محمد .(2026) .*أثر السلوك الأخلاقي في العلاقة بين القيادة الملهمة واستراتيجيات مواجهة الصراع التنظيمي: دراسة ميدانية على العاملين بإدارة جامعة طنطا* (رسالة دكتوراه غير منشورة). جامعة طنطا، طنطا. مسترجع من http://search.mandumah.com/Record/1651235

كرجي، سحر أحمد . عبد المحسن ،ابتسام عباس ،جودي ، حيدر حمزة .(2022) دور رأس المال الهيكلي في تعزيز التماثل التنظيمي دراسة تحليلية في وزارة العمل والشؤون الاجتماعية In *2020 International Conference on Resources Management*.

محمود، زيد خوام. خلف ،ياسر لطيف. (2023). دور راس المال العلائقي في تحقيق الاستدامة التنظيمية: بحث ميداني تحليلي في معمل السجاد العراقي.(1)*15*, *Al-Anbar University Journal of Economic & Administration Sciences* .

محنبي، منى بنت علي عبد الله، واليوبي، ليلى عابد. (2023). تصميم نموذج مقترح لوظائف مستودعات المعرفة: دراسة تحليلية لتحسين إدارة المعرفة داخل المنظمات .*المجلة العربية للنشر العلمي*، *ع57* ، 228 .258 – مسترجع من http://search.mandumah.com/Record/1437253

مصباح وبوبكر مصباح. (2025). دور الموظفين في تعزيز أو إضعاف أمن المعلومات بالمؤسسات: دراسة تحليلية في منطقة الجفرة. *مجلة جامعة فزان العلمية*, *4*(2), 130-143. مسترجع من https://fezzanu.edu.ly/fusj/index.php/FUAJ/article/download/511/331

موسى، محمد حمادة موسى محمد، البكري، محمد عبد السلام عبد العزيز، ومنسي، محمود محمد عبد المنعم. (2026). إطار محاسبي مقترح للإفصاح عن مخاطر الأمن السيبراني كمرتكز لتحسين كفاءة القرارات الاستثمارية وتحديد القيمة الحقيقية للسهم. *مجلة بحوث الأعمال، مج3، ع1*، 170 - 209. مسترجع من http://search.mandumah.com/Record/164603

ثانيا: الأجنبية

Abishethvarman, V. Sabrina, F. Kwan, P. (2025). Knowledge Integrity in Large Language Models: A State-of-The-Art Review. Information. 16. 1076. 10.3390/info16121076 https://doi.org/10.3390/info16121076?urlappend=%3Futm_source%3Dresearchgate.net%26utm_medium%3Darticle

Alhamoudi, S. (2023). Intellectual Capital in Knowledge Management Organizations. Economics World. 10. 10.17265/2328-7144/2023.04.002. https://doi.org/10.17265/2328-7144/2023.04.002

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2023). Towards protecting organisations' data by preventing data theft by malicious insiders. *International Journal of Organizational Analysis*, *31*(3), 875-888. https://doi-org.sdl.idm.oclc.org/10.1108/IJOA-01-2021-2598

Ali, A. H., Mohameed, W. K., & Alaloosh, M. S. (2025). التداعيات القانونية للعصر الرقمي: التحديات القانونية للخطر السيبراني على المعاملات التجارية. *Malaysian Journal of Syariah and Law*. https://doi.org/10.33102/mjsl.vol13no2.1036

Ali, S., & Tang, H. (2023). Is intellectual property beneficial to knowledge management? Literature review on organizational knowledge protection. *Journal of the Knowledge Economy*, *14*(4), 4100-4118.

Baghdadi, C. (2023). Tamin al-khatar al-siberani: Cyber risk insurance. Majallat Herodot lil-Ulum alInsaniyah wa al-Ijtima'iyah, 7(25), 237-257

Chebiego, B. K., Kinyua, G., & Muchemi, A. (2021). Knowledge asset as an antecedent of competitive advantage: A review of literature. *International Journal of Managerial Studies and Research*, *9*(12), 58-72.

Desouza, K. (2006). Knowledge Security: An Interesting Research Space. 25 https://www.researchgate.net/publication/228419064_Knowledge_Security_An_Interesting_Research_Space

Dunn, J. (2025, February 13). *Learn how to organize a knowledge base for better accessibility*. KnowledgeBase https://www.knowledgebase.com/

Eigner, L. (2024). Knowledge security at stake. Center for Security Studies (CSS), ETH Zurich. https://css.ethz.ch/en/center/CSS-news/2024/03/knowledge-security-at-stake.html

Elqadi، M. M. A.، Mohamed، M. A.، و Abdelmegeed ، M. H. (2024). The Role of Risk-Based Internal Auditing on the Activation of Cybersecurity to Control Information Risk: A Field Study. *الفكر المحاسبي، مج28، ع2* ، 117 .146 - مسترجع من http://search.mandumah.com/Record/1483658

Ha, S. T., Lo, M. C., Suaidi, M. K., Mohamad, A. A., & Razak, Z. B. (2021). Knowledge management process, entrepreneurial orientation, and performance in SMEs: evidence from an emerging economy. *Sustainability*, *13*(17), 9791 https://www.mdpi.com/2071-1050/13/17/9791 .

Herrera M, I., García, J. J., Ramos, J., Molina, S., Torre, I. de la, & Rodrigues, J. J. P. C. (2022). Survey of Techniques on Data Leakage Protection and Methods to address the Insider threat. *Cluster Computing*, *25*, 4289–4302. https://doi-org.sdl.idm.oclc.org/10.1007/s10586-022-03668-2

Ike, E. (2024). Information Security and Knowledge Management. European Journal of Information .and Knowledge Management. 3. 38-50. 10.47941/ejikm.2063

Ilvonen, A. Alanne, N. Helander and H. Väyrynen. (2016). Knowledge Sharing and Knowledge Security in Finnish Companies. 2016 49th Hawaii International Conference on System Sciences

(HICSS), Koloa, HI, USA, 2016, pp. 4021–4030, https://doi-org.sdl.idm.oclc.org/10.1109/HICSS.2016.499

Islam, M. S., & Amin, M. (2022). A systematic review of human capital and employee well-being: putting human capital back on the track. *European Journal of Training and Development*, *46*(5–6), 504–534 https://www.emerald.com/ejtd/article-pdf/46/5-6/504/1564207/ejtd-12-2020-0177.pdf

Kordab, M., Raudeliūnienė, J., & Meidutė-Kavaliauskienė, I. (2020). Mediating role of knowledge management in the relationship between organizational learning and sustainable organizational performance. *Sustainability*, *12*(23), 10061 https://www.mdpi.com/2071-1050/12/23/10061 .

Liu, S., & Wu, Y. (2020). Managing knowledge in the era of artificial intelligence: Opportunities and challenges. *Journal of Knowledge Management*, 24(6), 1497–1515. https://doi.org/10.1108/JKM-12-2019-0712.

Nakash, M., & Bolisani, E. (2025). Making knowledge management transparent: a new perspective on KM processes integration in the organizational framework. *Business Process Management Journal*, *31*(8), 49–66 https://www.emerald.com/bpmj/article-pdf/31/8/49/10053101/bpmj-07-2024-0566en.pdf .

Nyame, G., & Qin, Z. (2020). Precursors of role-based access control design in KMS: A conceptual framework. *Information*, *11*(6), 334. https://www.mdpi.com/2078-2489/11/6/334

Moszczyński, P., Moszczyński, M., Bryczek-Wróbel, P., Kapałka, M., Drozdowski, T., & Wróbel, J. (2022). The concept of improving the security of IT systems supporting the storage of knowledge in organizations. *Systems Science & Control Engineering*, *10*(1), 710–721. https://www.tandfonline.com/doi/pdf/10.1080/21642583.2022.2102550

Pollock, T. (2017). Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1051&context=ccerp

Popescul, D (2011): *The confidentiality – integrity – accessibility triad into the knowledge security: a reassessment from the point of view of the knowledge contribution to innovation.* Published in:

Proceedings of the 16th International Business Information Management Association Conference (Innovation and Knowledge Management, A Global Competitive Advantage), June 29-30, 2011, Kuala Lumpur, Malaysia, Editor Khalid S. Soliman (29 June 2011): pp. 1338-1345

Sarkheyli, A. (2023). "Evaluating Knowledge Sharing Risk Governance Model: A Case Study of the Ministry of Agriculture in Iran," *2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, Dubai, United Arab Emirates, pp. 1-8, https://doi-org.sdl.idm.oclc.org/10.1109/ICECCE61019.2023.10442180

Stefanova, D., & Vasilev, V. (2024). The competence "Information security" in human resources management - a key factor for competitiveness and digital transformation efficiency. *Revista Romana de Economie*, *58*, 1-12.

Symantec. (2019). *Internet Security Threat Report, Volume 24*. https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.

Zhang ,J.(2011) "Study on the knowledge security architecture of enterprise Knowledge management," 2011 International Conference on Business Management and Electronic Information, Guangzhou, 2011, pp. 211-215 https://doi-org.sdl.idm.oclc.org/10.1109/ICBMEI.2011.5914461

Zieba, M., & Bongiovanni, I. (2022). Knowledge management and knowledge security—Building an integrated framework in the light of COVID-19. Knowledge and Process Management, 29(2), 121-131. https://doi.org/10.1002/kpm.1707

حقوق الطبع والنشر © 2026 محفوظة لـ: المجلة العربية للنشر العلمي(AJSP)