IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية
مجلة كلية الكوت الجامعة
ISSN (E) : 2616 - 7808 II ISSN (P) : 2414 - 7419
www.kutcollegejournal.alkutcollege.edu.iq
k.u.c.j.sci@alkutcollege.edu.iq
عدد خاص - المؤتمر العلمي السابع للعلوم الادارية والاقتصادية - 2-3 يوليو/تموز 2024

# دور إدارة المعرفة في الامن السيبراني للشركات ، دراسة تطبيقية في شركة الجود لتكنولوجيا الزراعة الحديثة

م.د نور نعيم رضا [1] ، م.د حسين علي عبد الله [2] ، احمد كامل خيرالله [3]

**انتساب الباحثين**
[1] كلية الادارة والاقتصاد، جامعة واسط، العراق، واسط ، 52001
[2] كلية الادارة والاقتصاد، جامعة كربلاء، العراق، كربلاء، 56001
[3] كلية الادارة والاقتصاد، الجامعة المستنصرية، العراق، بغداد، 00964

[1] nrida604@uowasit.edu.iq
[2]Hussein.abdallah@uokerbala.edu.iq
[3] ahmedkamel1990.ak@gmail.com

[1] **المؤلف المراسل**

**معلومات البحث**
**تاريخ النشر:** أيلول 2024

**المستخلص**
يهدف البحث الى معرفة دور إدارة المعرفة في الامن السيبراني ، في شركة الجود لتكنولوجيا الزراعة الحديثة ، من خلال تساؤلات بحثية مفادها توضح توجهات البحث لمعرفة مدى تأثير ادارة المعرفة في الامن السيبراني للشركات ، ولإنجاز تحقيق اهداف البحث تم اختيار مجموعة من الفرضيات ، واعتمد الباحثون على المنهج التحليلي الوصفي كمنهج للبحث ، واعتمد الباحثون على الاستبيان كأداة للبحث من اجل الوصول الى نتائج البحث ، وتمثلت عينة البحث بمجموعة من العاملين في شركة الجودة لتكنولوجيا الزراعة الحديثة والبالغ عددهم (48) موظف ' اذ تم معالجة البيانات احصائيا بواسطة مجموعة من الادوات الاحصائية بالاعتماد على البرنامج الاحصائي SPSS V. 26 وقد توصل البحث الى مجموعة من النتائج أهمها، إدارة المعرفة أمر ضروري لتعزيز الأمن السيبراني للشركات، فهي تساعد المؤسسات على تحسين ممارسات الأمن السيبراني ، وزيادة الوعي بين الموظفين، وحماية المعلومات والأصول الهامة من التهديدات السيبرانية ، كما تم تقديم مجموعة من التوصيات أهمها على القادة ان يعطون الأولوية لإدارة المعرفة في خلق ثقافة الوعي بالأمن السيبراني وتعزيز اعتماد أفضل الممارسات داخل المنظمة.

**الكلمات المفتاحية :** إدارة المعرفة، الامن السيبراني، شركة الجود لتكنولوجيا الزراعة الحديثة.

# The Role of Knowledge Management in Corporate Cybersecurity, an Applied Study at Al-Joud Company for Modern Agriculture Technology

**Dr. Noor Naeem Reda [1] , Dr. Hussein Ali Abdullah [2] , Ahmed Kamel Khairallah [3]**

**Affiliation of Authors**
[1] College of Administration and Economics, Wasit University, Iraq, Kut, 52001
[2] College of Administration and Economics, University of Karbala, Iraq, Karbala, 56001
[3] College of Administration and Economics, Al-Mustansiriya University, Iraq, Baghdad, 00964

[1] nrida604@uowasit.edu.iq
[2]Hussein.abdallah@uokerbala.edu.iq
[3] ahmedkamel1990.ak@gmail.com

[1] **Corresponding Author**

**Paper Info.**
**Published:** Sept. 2024

**Abstract**
The research aims to find out the role of knowledge management in cybersecurity, in Al-Joud Company for Modern Agriculture Technology, through research questions that clarify the research directions to determine the extent of the impact of knowledge management on companies' cybersecurity. To achieve the research objectives, a set of hypotheses was chosen, and the researchers relied on the method. Descriptive analytical method as a research method, and the researchers relied on the questionnaire as a research tool in order to reach the research results. The research sample was represented by a group of employees at the Quality Company for Modern Agriculture Technology, numbering (48) employees. The data was processed statistically using a set of statistical tools based on the program Statistical SPSS V. 26. The research reached a set of results, the most important of which is that knowledge management is essential to enhancing cybersecurity for companies, as it helps organizations improve cybersecurity practices, increase awareness among employees, and protect important information and assets from cyberthreats. A set of The most important recommendations are that leaders should give priority to knowledge management in creating a culture of cybersecurity awareness and promoting the adoption of best practices within the organization

**Keywords:** Knowledge Management, Cybersecurity, Al-Joud Company for Modern Agriculture Technology

**المقدمة**

في المشهد الرقمي سريع التطور اليوم، أصبح الأمن السيبراني مصدر قلق بالغ للمؤسسات في جميع أنحاء العالم. مع تزايد التهديدات السيبرانية من حيث التعقيد والتكرار، اكتسب دور إدارة المعرفة في تعزيز الأمن السيبراني للشركات اهتمامًا متزايدًا. تركز هذه الدراسة التطبيقية على شركة الجود للتكنولوجيا الزراعية الحديثة لاستكشاف كيفية مساهمة ممارسات إدارة المعرفة في وضع الأمن السيبراني للشركة.

تبدأ الدراسة بتحديد المنهجية العلمية ثم الإطار النظري لإدارة المعرفة، فضلا عن الإطار النظري للأمن السيبراني وتعد شركة الجود شركة رائدة في مجال التكنولوجيا الزراعية، والتي تشمل حماية بيانات الملكية، وحماية الملكية الفكرية، وضمان سلامة الأنظمة الآلية.

ومن خلال نهج كمي يعتمد على الاستبيان أداة لجمع البيانات، التي تم توزيعها على العاملين في الشركة قيد البحث، يحدد البحث الوضع الحالي لممارسات إدارة المعرفة وتأثيرها على تدابير الأمن السيبراني. تكشف النتائج أن الإدارة الفعالة للمعرفة تعزز الأمن السيبراني من خلال تعزيز ثقافة التعلم المستمر، وتسهيل النشر السريع لمعلومات التهديدات، وتمكين الإدارة الاستباقية للمخاطر.

تسلط الدراسة الضوء أيضًا على العديد من أفضل الممارسات لدمج إدارة المعرفة في استراتيجيات الأمن السيبراني، مثل تنفيذ برامج تدريبية قوية، وتطوير مستودعات المعرفة الشاملة، وتعزيز التعاون بين الإدارات. بالإضافة إلى ذلك، فإنه يؤكد على أهمية التزام القيادة واعتماد التقنيات المتقدمة في دعم هذه المبادرات.

وفي الختام يوضح البحث أن إدارة المعرفة تلعب دوراً حيوياً في تعزيز الأمن السيبراني المؤسسي في شركة الجود. ومن خلال إدارة المعرفة بشكل منهجي، يمكن للمؤسسات توقع التهديدات السيبرانية والاستجابة لها والتخفيف من حدتها بشكل أفضل، مما يؤدي في النهاية إلى تأمين عملياتها والحفاظ على ميزة تنافسية في الصناعة. توفر الأفكار المكتسبة من هذه الدراسة إرشادات قيمة للشركات الأخرى التي تسعى إلى تعزيز أمنها السيبراني من خلال ممارسات إدارة المعرفة الفعالة

**المحور الاول: المنهجية العلمية للبحث**

**اولا:- مشكلة البحث**

في عالمنا المترابط أصبح الأمن السيبراني أهم شيء يؤثر على كل جزء من حياتنا، لا سيما فيما يتعلق بالبنية التحتية الحيوية. هناك الكثير من التعريفات للبنية التحتية الحيوية. في عام 1996، أصدر رئيس الولايات المتحدة أمرًا تنفيذيًا (EO) أدرج سبع مجالات للبنية التحتية الحيوية للولايات المتحدة وذكر المكتب التنفيذي أن أهم المجالات هي: نظام الشبكات الكهربائية، والنقل، والاتصالات. سيكون للضرر الذي يلحق بأي منها تأثير على قابلية جميع البنية التحتية الحيوية الأخرى للحياة. الهدف الرئيسي من هذه المقالة هو توفير الجوانب النظرية لنموذج إدارة الأمن السيبراني الذي يمكن استخدامه لضمان أمن البنية التحتية الحيوية في مؤسسة أو شركة [1] .

استنادًا إلى تعريفات الأمن السيبراني والحوادث الإلكترونية المعتمدة، من الممكن تحديد أهم الأهداف من أجل ضمان الأمن السيبراني. الهدف الأول هو السرية التي تضمن أن الأفراد المصرح لهم فقط هم من يمكنهم تلقي المعلومات أو تغييرها أو إدارتها. الهدف الثاني هو النزاهة، والتي تضمن أن الأشخاص أو العمليات المصرح لهم فقط هم القادرون على إجراء أي تغييرات في النظام. ثالثًا - تتم إدارة توفر النظام والمعلومات من قبل النظام ومشغليه. يضمن هذا الهدف أن الكيانات المصرح لها فقط هي التي ستتمكن من الوصول إلى المعلومات أو الموارد المخزنة أو المستخدمة في البنية التحتية للمؤسسة. تشير اللوائح المستندة إلى القانون بوضوح إلى أن الأمن السيبراني والإدارة يرتبطان ارتباطًا وثيقًا وجوانب مهمة جدًا لكل منظمة. من أجل ضمان أمن البنية التحتية الحيوية، من المسلم به أن الأمن السيبراني لا يقل أهمية عن الأمن المادي[2].

في عالم من التغيير المستمر وحيث تتنافس المنظمات حرفيًا مع كل فرد في الشبكة العالمية، هناك العديد من الدراسات حول كيفية التمييز وسط الابتكارات المستمرة بشكل متزايد، والتقنيات المحسنة بشكل متزايد والمعرفة على نطاق أوسع. تزداد الحاجة إلى تكيف المؤسسات، نظرًا للانقطاعات الناتجة عن مستوى العولمة، والتقلبات الشديدة، والمنافسة الشديدة، والتغيرات الديموغرافية، والانفجار في المعرفة، تقوم وسائل الإعلام، بشكل أسرع، بتغيير مناخ الأعمال، وكل يوم يصبح أكثر وضوحًا يعد التعلم التنظيمي وإدارة المعرفة، وكذلك الابتكار، من المتطلبات الأساسية لمواجهة هذا النوع من الاتجاه العالمي[ 3 ].

مما سبق يمكن تلخيص مشكلة البحث بإثارة التساؤل الاتي ما هي طبيعة العلاقة بين ادارة المعرفة والامن السبراني؟

**ثانيا: اهمية البحث**

**1- الأهمية النظرية**

- هنالك ندرة في البحوث التي اهتمت بدراسة طبيعة العلاقة التي تجمع بين ادارة المعرفة وبين الامن السبراني في نموذج

فرضي واحد، لذا فان البحث الحالي هو البحث الوحيد الذي يسعى للتعرف على طبيعة العلاقة .

- الاسهام في تقديم اطار نظري يستوعب متغيرات البحث، عن طريق عرض خلاصة افكار الباحثين والمفكرين في المجال المعرفي.
- يسعى البحث إلى محاولة زيادة وعي القائمين على أمر الشركة قيد البحث بأهمية تبني نمط ادارة المعرفة كفلسفة عمل في الشركة وكيفية تأثيرها على الامن السيبراني.

**2- الأهمية التطبيقية**

- البحث الحالي يساعد في معالجة المعوقات التي قد تواجه الشركات الخدمية من ناحية تبني ادارة المعرفة التي تسهم في تطوير وتعزيز الامن السيبراني في المنظمات وتأثيرها على النتائج التنظيمية.
- لا توجد دراسات تسلط الضوء على الامن السيبراني في الشركات العراقية عموما وفي شركة عينة البحث بالاخص، التي يمكن من خلالها معرفة كيفية توظيف ادارة المعرفة وتأثيرها على عمل تلك الشركة.
- فتح الآفاق المستقبلية لمختلف الباحثين من اجل القيام بدراسات مستقبلية في هذا المجال .

**ثالثا: اهداف البحث**

للبحث مجموعة من الأهداف يسعى إلى تحقيقها وكما يأتي:

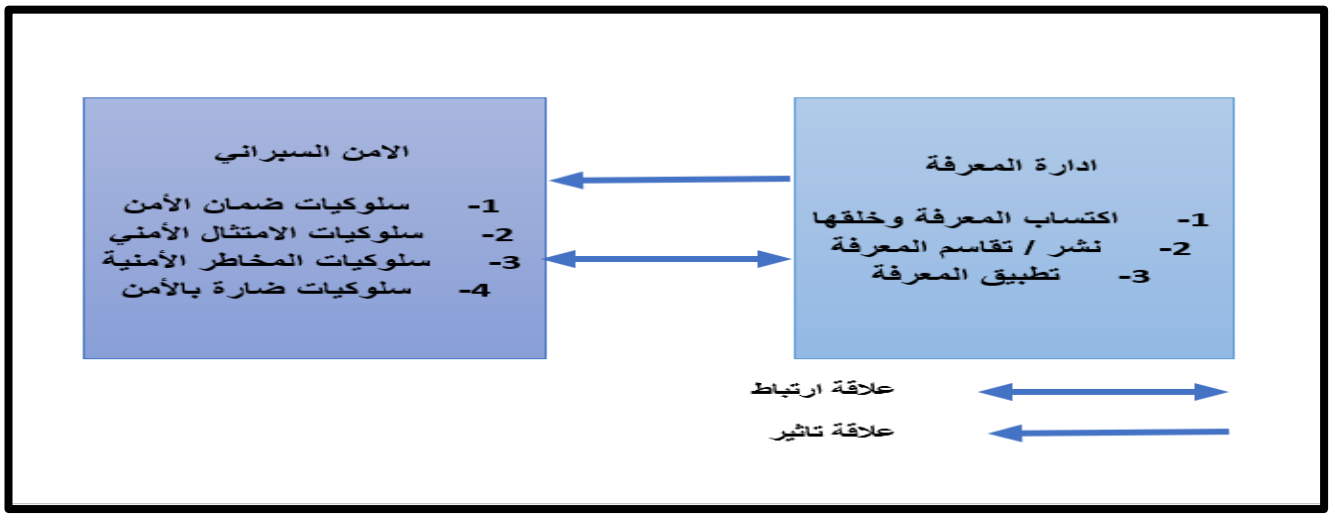
1. تقديم إطار مفاهيمي حول متغيرات البحث (ادارة المعرفة، الامن السبراني).
2. التعرف على مستوى تطبيق متغيرات البحث (ادارة المعرفة، الامن السبراني) لدى الشركة عينة البحث.
3. اختبار وقياس مستوى علاقة الارتباط بين المتغيرين
4. تشخيص تأثير ادارة المعرفة بأبعادها في تعزيز الامن السيبراني.

**رابعا : التعاريف الجرائية للبحث و مخططه الفرضي**

يتكون نموذج البحث من متغيرين مهمين هما

1- المتغيل المستقل :- ادارة المعرفة هي قدرة المنظمة على ادارة المعرفة التي يمتلكها العاملون من خلال توفير كافة الوسائل التي تساعد في صقلها وتطويرها بطريقة تمكن من ديموميتها لتحقيق اهداف المنظمة .

2- المتغير التابع :- الامن السيبراني للشركات هو عملية توفير اساليب الردع الوقائية التي تسهم في الحفاظ على معلومات وبيانات الشركات من التهديدات الخارجية ويمكن بيان هذه المتغيرات كما موضح في الشكل (1).




**الشكل (1) يوضح المخطط الفرضي للبحث**

**المصدر:- اعداد الباحثين**

**خامسا: فرضيات البحث**

1- توجد علاقة ارتباط ذات دلالة معنوية بين ادارة المعرفة والامن السيبراني.

2- يوجد تأثير ذو دلالة معنوية للإدارة المعرفة في لامن السيبراني.

**سادسا: مجتمع وعينة البحث**

**تمثل مجتمع البحث**

**المحور الثاني: الإطار النظري للبحث**

**اولا :- إدارة المعرفة**

**1- مفهوم ادارة المعرفة**

في اقتصاد المعرفة اليوم، يجب على الشركات تكييف وتحديث معرفتها التنظيمية باستمرار توصف المعرفة عادة بأنها مورد مهم يجب إدارته بشكل استراتيجي. أصبح مفهوم إدارة المعرفة شائعًا للغاية وكان موضوع بحث للعديد من العلماء. يعتقد [4] أن وظيفة إدارة المعرفة هي "حماية المعرفة التي يمتلكها الأفراد وتنميتها، وحيثما أمكن، نقل الأصول إلى شكل يمكن أن يشارك فيه الموظفون الآخرون بسهولة أكبر في الشركة [5]. اذ يعد تنفيذ إدارة المعرفة أحد عوامل الجذب الرئيسية بين الباحثين والممارسين. بينما تحاول المنظمات بدء إدارة المعرفة، فإن أحد الاهتمامات الرئيسية التي تظهر هي كيفية تحقيق ذلك. العديد من الشركات التي تحاول الشروع في إدارة المعرفة غير متأكدة من أفضل نهج لاعتماده. يبدو أن هناك اتفاقًا عامًا في الأدبيات على أن النهج الاجتماعي والتكنولوجي المركب مثالي. لذلك سيتم تمهيد الطريق إلى الأمام إذا كانت المنظمات على دراية بالعوامل الرئيسية التي ستجعل اعتمادها ناجحًا [6]

**2- اهداف إدارة المعرفة**

يمكن تحقيق أهداف إدارة المعرفة باستخدام مناهج مختلفة على النحو التالي: إنشاء عمليات إدارة المعرفة وبناء البنية التحتية التقنية على سبيل المثال شبكة الإنترنت / الإنترانت، وأنظمة إدارة المعرفة، ومستودعات المعرفة، وأدوات عقد المؤتمرات عبر الفيديو، وإنشاء منظمة تعليمية وتعزيز ثقافة صديقة للمعرفة [5].

**3- استراتيجية إدارة المعرفة**

تتفق جميع المؤلفات الأكاديمية على أنه لكي يتم تنفيذ المفهوم في منظمة ما، يجب أن تكون هناك استراتيجية والتزام بالتنفيذ. قسم Zack (1999) المعرفة إلى ثلاث فئات بما في ذلك المعرفة الأساسية core knowledgeوالمعرفة المتقدمة advanced knowledge والمعرفة المبتكرة innovative knowledge. ان على المنظمات وصف خريطة المعرفة الاستراتيجية الخاصة بها وفقًا لفئة المعرفة وأيضًا بالمقارنة مع المنافسين، لتحديد الفجوة بين ما يجب القيام به من أجل القدرة التنافسية وما يتم القيام به بالفعل (الفجوة الاستراتيجية)، واعتماد استراتيجية المعرفة مثل الاستكشاف exploration والاستغلال exploitation والعدوانية aggressive والمحافظة conservative أو مزيج منها combination of them. يجب أن تخلق استراتيجية إدارة المعرفة فهمًا لمصادر المعرفة الخاصة بالمنظمة وأين يقيمون؛ توضيح دور المعرفة في خلق القيمة؛ تشمل عددًا من المشاريع أو الأنشطة المتكاملة على مراحل بمرور الوقت بما في ذلك المكاسب السريعة وكذلك الفوائد طويلة الأجل. من الضروري تحديد استراتيجية المعرفة لضمان توجيه جهود إدارة المعرفة ودعمها من خلال الاستراتيجية التنافسية للشركة [6]

**4- خصائص إدارة المعرفة**

أن إدارة المعرفة يجب أن تتناول الخصائص المتنوعة لمنظمة مثل الهيكل والثقافة والعملية. ترتبط إدارة المعرفة بإطار عمل محدد للحصول على المعرفة الضمنية والصريحة واكتسابها وتنظيمها ونقلها داخل المنظمة. يمكن بعد ذلك استخدام المعرفة من قبل الموظفين ليكونوا فعالين ومنتجين في عملهم، وبالتالي تعظيم الميزة التنافسية للمؤسسة [5] .

وتم تلخيص خصائص إدارة المعرفة: [5]

- التوطين - يشير إلى جميع الأنشطة التي تشير إلى مكان وجود المعرفة
- استخدام المعرفة - يشير إلى إنشاء مجموعة من الأدوار والمهارات لاستخدام المعرفة بشكل فعال
- اكتساب المعرفة وتطويرها - يشير إلى ثقافة احتضان المعرفة التي يتم اكتسابها وتطويرها
- تدوين المعرفة - يشير إلى القدرة على إعادة استخدام المعرفة بشكل ناجح ومستمر
- نقل المعرفة - يشير إلى نقل المعرفة واستخدام المعرفة المنقولة.

**5- تكنولوجيا المعلومات**

ترتبط إدارة المعرفة بتقنية المعلومات، حيث يبدو أن أحدهما يقود إنشاء الآخر. من المقبول على نطاق واسع أن قواعد البيانات والشبكات الداخلية ومنصات المعرفة والشبكات هي اللبنات الأساسية الداعمة لإدارة المعرفة. إنها تجعل تسجيل المعرفة أسهل بكثير للبحث عنها واستخدامها. يرى الباحثين أن تكنولوجيا المعلومات هي إدارة تخزين المستندات والوصول إليها. عادةً ما تحتفظ تكنولوجيا المعلومات بقواعد البيانات، ونقاط وصول الأجهزة والبرامج، واستمرارية المعلومات. ومع ذلك، يمكن أن يفشل أي مشروع لإدارة المعرفة عندما يرى تقنيو تكنولوجيا المعلومات الجانب التقني فقط. يجب أن يكونوا مدركين ومثقفين في

عمليات إدارة المعرفة للحصول على نتائج أفضل. بمجرد تحقيق ذلك، ستصبح تكنولوجيا المعلومات لاعباً رئيسياً في جهود إدارة المعرفة المستمرة للشركات. على العكس من ذلك، فإن الافتقار إلى التكنولوجيا في مبادرة إدارة المعرفة يجعل من الصعب قياس الأنشطة عندما تواجه مبادرة إدارة المعرفة سؤالًا حول عائد الاستثمار. إن مفتاح تحقيق الانسجام بين إدارة المعرفة وتكنولوجيا المعلومات هو فهم المبادئ الأساسية للغاية: هناك أشياء تقوم بها أجهزة الكمبيوتر والتكنولوجيا بشكل جيد، وهناك أشياء يقوم بها البشر بشكل جيد. إن العديد من إخفاقات تكنولوجيا المعلومات وإدارة المعرفة، والكثير من التوتر بين الاثنين هي نتيجة المحاولات المتكررة لإجبار نموذج واحد على العمل في نطاق الآخر [6].

لقد ثبت أن تكنولوجيا المعلومات تزيد من سرعة تدفق المعرفة وربما تقلل من تكلفة استخدام المعلومات. هناك مجموعة واسعة من تقنيات المعلومات التي تدعم إدارة المعرفة والتي يمكن تطبيقها ودمجها في النظام الأساسي التكنولوجي للمؤسسة. يمكن تجميعها في واحدة أو أكثر من الفئات التالية: ذكاء الأعمال، وقاعدة المعرفة، والتعاون، وإدارة المحتوى والوثائق، والبوابات، وإدارة علاقات العملاء، واستخراج البيانات، وسير العمل، والبحث والتعلم الإلكتروني. نظرًا لاعتماد إدارة المعرفة على تكنولوجيا المعلومات، لا يزال ينظر إلى إدارة المعرفة على أنها إدارة معلومات من قبل العديد من المنظمات. نتيجة لذلك، غالبًا ما يرتبط بالحلول التكنولوجية مثل الشبكات الداخلية وقواعد البيانات، يجب على المؤسسات أن تدرك أن تقنية المعلومات ليست سوى أداة وليست حلاً نهائيًا [6] .

**6- ابعاد عمليات إدارة المعرفة**

عمليات إدارة المعرفة هي مفتاح نجاح نظام إدارة المعرفة في أي مؤسسة. حدد العديد من الباحثين المراحل المختلفة المتسلسلة والمتداخلة لعمليات إدارة المعرفة. قدمت شركة( Ernst and Young (1998) أربع عمليات لإدارة المعرفة تتكون من التخطيط والاكتساب والتطبيق والتقييم. قسمت ( Demarest (1997)) عمليات إدارة المعرفة إلى البناء والتجسيد والنشر والاستخدام حيث يشير البناء إلى عملية اكتشاف أو هيكلة نوع من المعرفة، يشير التجسيد إلى عملية اختيار مستودع للمعرفة، ويشير النشر إلى العمليات البشرية وتشير البنية التحتية التقنية التي تجعل المعرفة المتجسدة متاحة للأشخاص داخل الشركة والاستخدام إلى الهدف النهائي لأي نظام إدارة معرفة وهو تطبيق تلك المعرفة المكتسبة من أجل إنشاء منتجات أو خدمات جديدة. قام ( Alavi and Leidner (2001) بفحص الخصائص المختلفة وإنتاج أربعة أبعاد واسعة للعملية وهي الإنشاء والتخزين / الاسترجاع والنقل والتطبيق. يمكن وصف بعض الجوانب العامة لعملية إدارة المعرفة نظريًا على النحو التالي: [7].

**أ- اكتساب المعرفة وخلقها:** يشير اكتساب المعرفة عادة إلى إجراءات الحصول على المعلومات ومعالجتها وفهمها واستدعائها من خلال عدد من الأساليب. يحدد اكتساب المعرفة كيف يتعرف الناس على المعلومات الجديدة، وكيف يتم التقاط هذه المعلومات الجديدة في الدماغ وكيف يمكن تذكر تلك المعلومات الملتقطة من العقل لاستخدامها في المستقبل في أي موقف جديد يمكن أيضًا وصف اكتساب المعرفة التنظيمية على أنه عملية تطوير معرفة جديدة من المعرفة الموجودة داخل قاعدة المعرفة الضمنية والصريحة للمؤسسة يجب على المنظمات الحصول على المعرفة من داخل وخارج المنظمة. يجب أن يتبادل الأشخاص معارفهم مع شركائهم أو زملائهم في العمل بحيث يمكن أن يحدث رفع مستوى معرفتهم على أساس مستمر ويمكنهم الحصول على تعليقات حول تجربة مشروعهم من الآخرين من أجل تحسين المشاريع المتتالية. اقترح نوناكا وتوياما وكونو (2000) نموذجًا لإنشاء المعرفة يتكون من ثلاثة عناصر:

- عملية: (التنشئة الاجتماعية ، والاستخراج ، الجمع ، والاستيعاب ) وهي عملية تكوين المعرفة من خلال التحويل بين المعرفة الضمنية والصريحة
- فضاء المعرفة: البيئة المشتركة أو مكان إنشاء المعرفة .
- أصول المعرفة: التي تشمل المدخلات والمخرجات والمشرف على عملية تكوين المعرفة. يجب أن تتفاعل العناصر الثلاثة لخلق المعرفة مع بعضها البعض لتشكيل دوامة المعرفة التي تخلق المعرفة.

**ب- نشر / تقاسم المعرفة :** يتم تعريف نشر المعرفة بأنه عملية نشر أو توزيع المعرفة في جميع أنحاء المنظمة. يعتمد الاستخدام الفعال للمعرفة إلى حد كبير على تبادل المعرفة. يتم نشر المعرفة بشكل أكبر، حيث يستخدمها الناس ويخلقون معرفة جديدة من حيث المنتجات والخدمات الجديدة. كانت معظم الدراسات أكثر اهتمامًا باكتساب المعرفة وبذلت جهودًا أقل لتبادل أو نشر المعرفة المكتسبة أو نقل المعرفة (نيفيس وآخرون ، 2000). تتطلب مشاركة المعرفة (الصريحة أو الضمنية) جهدًا من جانب الفرد للقيام بالمشاركة. هنالك أربع آليات لمشاركة المعرفة الفردية داخل المنظمات:

- المساهمة بالمعرفة في قواعد البيانات التنظيمية .

- تبادل المعارف غير الرسمية داخل أو عبر الفرق أو وحدات العمل .
- تبادل المعرفة في التفاعلات غير الرسمية .
- تقاسم المعرفة داخل مجتمعات الممارسة (أي المنتديات التطوعية التي تم إنشاؤها حول موضوع اهتمام معين). يتم تعريف مشاركة المعرفة على أنها تبادل الخبرات أو الأحداث أو الأفكار أو التفاهم بشأن أي شيء مع توقع اكتساب المزيد من الأفكار والفهم

**ج- تطبيق المعرفة:** يجد معظم المؤلفين أن تطبيق المعرفة هو مصدر الميزة التنافسية وليس المعرفة نفسها. يتضمن تطبيق المعرفة تطبيق المعرفة لصنع القرار ، واتخاذ الإجراءات وحل المشكلات التي يمكن أن تؤدي في النهاية إلى خلق المعرفة ، ومن ثم يجب التقاط المعرفة التي تم إنشاؤها ومشاركتها وتطبيقها بشكل فعال ومن ثم تستمر الدورة في التحرك. ناقش نوناكا وتاكيوشي (1995) قدرة المنظمة على خلق المعرفة، لكنهما افترضوا أنه بمجرد إنشائها ، سيتم تطبيقها بشكل فعال. إن تطبيق المعرفة المستفادة من التجربة والمصادر يضع مزيدًا من التركيز على فعالية إدارة المعرفة، وان التطبيق الفعال للمعرفة يساعد الشركات في زيادة الكفاءة وخفض التكاليف، خلصت بعض تقارير الدراسات الاستقصائية والدراسات التجريبية إلى أن المشكلات في تنفيذ إدارة المعرفة ترجع أساسًا إلى مشاكل استخدام المعرفة، على الرغم من هذه الحقيقة، نادرًا ما يتم توفير أي استراتيجيات للاستخدام الفعال والمستهدف للمعرفة. على الرغم من وجود العديد من التحديات أثناء تطبيق المعرفة الحالية، إلا أن تكنولوجيا المعلومات تلعب دورًا مهمًا في تطبيق المعرفة. يمكن لتقنية المعلومات زيادة تكامل المعرفة وتطبيقها من خلال تسهيل عملية التقاط المعرفة وتحديثها وإمكانية الوصول إليها

**ثانيا :- الامن السيبراني للشركات**

**1- مفهوم الامن السيبراني**

ظهرت انواع متنوعة و جديدة من التهديدات الامنية في القرن الحادي والعشرين ، وقد تحايلت على التحليل التقليدي التي ترادف التهديد والامن. كما ويدعو نموذج الحالي للامن الى هيكل اداري قائم على المرونة والاستعداد المرتبط بادارة الحوكمة و المخاطر والممارسات الاستباقية. المجال الجديد الاكثر شهرة يتمثل بالامن السيبراني، كونه يؤثر على جميع المستويات الحياتية اليومية، في القطاعين العام والخاص، والمجموعات والافراد ، فالامن السيبراني يمثل الرد على التهديدات المتزايدة للجرائم الالكترونية، وتم تطوير المفهوم لتوفر بيئة حوسبة امنة ومامونة للمستخدمين. كما وفشلت العديد من المؤسسات الوطنية و الدولية في تطوير التعريف الشامل للامن السيبراني . وقد ادى ذلك الى حدوث ثغرة في فهم الامن السيبراني، من حيث الجمع بين انشطة الحياة الواقعية والعالم الاصطناعي المتصل دوليا. كما وحاول الاتحاد الدولي للاتصالات (ITU) وصف تعريف للامن السيبراني يمكن القول على انه مجموعة من الادوات والمفاهيم والسياسات الامنية وضمانات الامن والمبادئ والاساليب التوجيهية و ادارة المخاطر والاجراءات والتدريب وتقديم افضل الممارسات و والتقنيات والضمانات التي يمكن استخدامها لحماية البيئة السيبرانية، بالاضافة الى اصول المؤسسات والمستخدمين ومحاولات الامن السيبراني في ضمان تحقيق صيانة الخصائص الامنية للمؤسسة واصول المستخدمين ضد تلك المخاطر الامنية ذات الصلة في البيئة السيبرانية ، حيث من المعتقد توافر الاهداف العامة والسرية والنزاهة. اود أن ازعم أن الامن السيبراني يمكن اعتباره مصطلحا شاملا بالعديد من المخاطر الامنية المتباينة والمجزاة والتي يشترك جميعها في عامل واحد مشترك " استخدام الانترنت.و الفضاء والانترنت". و يوضح التعريف اعلاه ان الحقل معقد جدا حيث يتعذر على فاعل امان واحد التعامل معه. تدعم هذه الحجة ان هذا النوع من الامن يتطور في مساحات بين مختلف القطاعات و المناطق الجغرافية اي و الدولية والاقليمية والمحلية والوطنية ، وبين القطاع العام والخاص [8].

**2- الأمن السيبراني هو شأن للخبراء**

تعتبر تكنولوجيا المعلومات ذات اهمية كبيرة للمؤسسات وبالتالي الامن السيبراني ايضا ، ومع ذلك فالمديرين يعتبرون الامن السيبراني امرا يخص الخبراء ، كون الخبراء لديهم معرفة لاتخاذ التدابير اللازمة لمثل هذا المجال المعقد. ولان تكنولوجيا المعلومات مهمة للعمليات التجارية، و استعداداً لاستثمار الجهود و الاموال في امن تكنولوجيا المعلومات [9] .

رايهم في تكنولوجيا المعلومات في المنظمة واضح جدا. ، اذ ان النظام الغير المتاح سيكون له عواقب وشديدة على الاعمال الاساسية، سواء كان اي نوع من السبب تقني ام عطل خارجي فلا يهم حقا. كون مقاطعة العمل يسبب عواقب وخيمة ، وتعد تقنية المعلومات عامل اساسي لتمكين منظمتهم.

ويرى المديرون بان ذلك "وعيي مرتفع بما يكفي" ويفضلون ان يهتم الخبراء بالامن السيبراني. و يتعين على الاشخاص الاخرين من ذوي الصلة في المنظمة الاهتمام بمشاكل متعلقة بالامن السيبراني، و ينصب التركيز للمستجيب على الوعي الامني

السيبراني للمستخدمين المعنيين ، كما و يجب ان يكون مستخدمو انظمة تكنولوجيا المعلومات في المؤسسة على دراية . فليس هناك حاجة للتكامل في العمليات، لانه يؤثر ايضا على المستخدمين الغير ملائمين . وتم التاكيد على هذا في البيان حول التدريب، وليس كل شخص في المنظمة ملزم بحضور التدريب على الامن السيبراني.

بالاضافة الى ذلك ، كما ان المديرون يختلفون حول "يجب دمج جميع الخبرات في مجال الامن السيبراني والوعي". غالبا لا يكون الامن السيبراني جزءا من الاعمال الاساسية. على سبيل المثال . يعتبر اختبار الامان مهمة للمؤسسة الخارجية، ومع ذلك. فان التناقض مع عبارة "يمكن لشركات التأمين تقديم المشورة بشان الأمن السيبراني" غير محل للتقدير.

كما ويمكن للمرء ان يذكر ان معرفة المديرين في العامل الرابع "الفطرة السليمة. تكنولوجيا المعلومات تدور حول التكنولوجيا، وبالتالي يركز المجيبون على مخاطر التكنولوجيا والوسائل؛ يتحكم البشر في التكنولوجيا، لذا فهم ايضا عامل خطر. ينعكس كل هذا فيما يلي : تشير الدرجات المطلقة في الملحق ج الى التركيز على المخاطر المتعلقة بالتكنولوجيا ووسائل التخفيف التي تركز على التكنولوجيا على الرغم من ان الأمن السيبراني لا يتم حله بالوسائل التكنولوجية فقط لان المخاطر المتعلقة بالبشر تمثل ايضا مشكلة.

يتفق المديرون على "نظرا لان مؤسستنا تستخدم تكنولوجيا المعلومات، تحتاج مؤسستنا الى اتخاذ اجراءات مماثلة لمؤسسة تكنولوجيا المعلومات". ينعكس هذا ايضا في البيان القائل بأن الوقاية خير من التعافي من حادث. في النهاية، لا ينبغي المبالغة في الأمن السيبراني، فالشديد المفرط ليس جيدا ايضا. ومع ذلك، فان المديرين لا يعتبرون انفسهم الفاعلين المناسبين للتعامل مع الأمن.

الخلاصة: يعتقد المديرون في هذا العامل ان تكنولوجيا المعلومات هي ركيزة اعمالهم الاساسية. ومع ذلك، فان المديرين لا يعتبرون انفسهم اشخاصا معينين لحل هذه المشكلات. يجب على الخبراء ان يقرروا النهج. المديرين انفسهم لديهم إلى حد ما نهج " الفطرة السليمة نحو التركيز على المخاطر والتدابير التكنولوجية، والمخاطر البشرية ويجب اتخاذ التدابير. [8]

**3- ابعاد الامن السيبراني**

ان هناك الكثير من الخلافات التي لاحضها العلماء حول افضل الطرق لتصور سلوكيات الامن السيبراني و اكدت معظم الدراسات على التنبؤ بسلوكيات السيبرانية الايجابية ومن ثم تحديدها، في حين يركز البعض الاخر على التنبؤ بسلوكيات سلبية .وربما تكون طريقة البحث فيها اشكالية لان السوابق السلوكية الايجابية ، كالامتثال للسياسة تكون مميزة بطبيعتها عن السوابق السلوكية السيبرانية السلبية المحفوفة بالمخاطر ويتم اعتماد انموذج رباعي الابعاد للتهديدات كما يأتي : [10]

**أ- سلوكيات ضمان الأمن**

سلوكيات ضمان الامن هي السلوكيات التي تكون فيها نية واضحة لدى الموظف في المساعدة لحماية امن معلومات المنظمة، باعتبارها اجراءات جيدة و مجدية وخيرة من ناحية الموظف، وممكن ان تتضمن تجاوز ما هو مطلوب من قبل المنظمة بهدف حماية المعلومات وتحقيق الامان والضمانات الواعية وسلوكيات النظافة الاساسية، فالموظفين يحتاجون لمستوى عالٍ من الخبرة التكنولوجية على الرغم من ذلك يمكن القول ان هنالك اجراءات ابسط، كاختيار شخص قوي كلمة المرور ومراقبة لجهاز الكمبيوتر الخاص بك بحثا عن علامات الفيروس، والتي يقوم بها اي مستخدم نهائي. و قد تكون هذه السلوكيات مرتبطة بسلوكيات المواطنة التنظيمية كونها خيرية في طبيعتها وتظهر الرغبة في تقديم المساعدة للمنظمة.

**ب- سلوكيات الامتثال الأمني**

تعتبر سلوكيات الامتثال الامني هي السلوكيات التي تتماشى مع السياسات خاصة بالامن المؤسسي (في حين ان السلوكيات الخاصة بالامتثال الامني هي سلوكيات متعمدة، وقد تكون سلوكيات الامتثال الامني اما نتيجة للعمل او التقاعس عن العمل. وببساطة قد يكون الموظفون يتبعون القواعد المتمثلة بأمن المعلومات او لا ينخرطون في السلوك المحفوف بالمخاطر او الضار. فقد حددت الابحاث السابقة العوامل المحفز ه الداخلية والخارجية والتي قد تؤثر على السلوكيات المتوافقة، كما وان سمات الشخصية المعينة يمكن ان تسهم تحقيق احساس الموظف بالسلوك الشخصي ويجب ان تكون محور للبحث في المستقبل. وتشمل سوابق نية الامتثال سلوك الموظف السابق، واليقين وشدة العقوبة وسلوك الاقران والمعايير التنظيمية ، ومدى فعالية الامتثال للمعلومات التنظيمية الامنة [11]

**ج- سلوكيات المخاطر الأمنية**

هي "السلوكيات التي قد تعرض امن معلومات المؤسسة للخطر" والتي تنطوي على اجراءات يتصرف الموظفون بما يتوقع الا يفعلوه قد لا يقصد المنخرطون في هذه السلوكيات ان يلحق الضرر بالمنظمة، ولكنهم قد ينظرون الى هذه السلوكيات باعتبارها ملائمة لانجاز عملهم ، وقد يكون لاي سلوك مخاطرة عواقب

سلبية على المنظمة. يمكن اداء هذه السلوكيات للموظفين بأي مستوى من الخبرة التكنولوجية. ويمكن ان تتضمن بعض الامثلة على تلك السلوكيات المتمثلة بالمخاطر الامنية هو الابتعاد عن جهاز الكمبيوتر الخاص بك دون قفله اولا او كتابة كلمة المرور للعمل حيث قد يراها الاخرون. و تتشابه سلوكيات المخاطر الامنية مع اخطاء الانظمة الساذجة وسلوكيات الترقيع الخطيرة وانتهاكات الامان الغير ضارة على النحو المحدد كما وان نوايا الموظفين لاداء اعلى اذا كانوا يعتقدون ان القيام بذلك سيحسن من ادائهم الوظيفي [11].

**د- سلوكيات ضارة بالأمن**

وهي تلك السلوكيات التي تضر بالامن و تمنع الموظفين في المنظمات من القيام بها وستتسبب في الحاق الضرر بامن معلومات المنظمة، وهذه السلوكيات بشكل عام خبيثة بطبيعتها ويمكن ان تؤدي الى اجراءات تأديبية من قبل كل من المنظمة والحكومة. تعتبر هذه السلوكيات ضارة بالأمن بشكل عامو و اكثر خطورة من السلوكيات الضارة بالأمن. قد تتطلب هذه السلوكيات مستوى عالٍ من الخبرة التكنولوجية من الموظف ويمكن اعتبارها مشابهة في طبيعتها لسلوكيات العمل ذات النتائج العكسية الموجهة تنظيميا [10].

**المحور الثالث / الجانب التطبيقي للبحث**

**اولا :- نبذة عن الشركة المبحوثة**

تعتبر شركة الجود لتكنولوجيا الزراعة الحديثة وانتاج المنظفات والمطهرات والمعقمات و ذات المسؤولية المحدودة و التابعة للعتبة العباسية المقدسة والركيزة الاساسية في احياء المنتوج الوطني المغيب والذي يصب في خدمة الزبون المحلي وسد النقص الحاصل في السوق ، حيث باشرت العمل عام 2014 و قد كانت البداية في انتاج الاسمدة الزراعية والمخصبات النوعية و المركبة ، التي تستخدم لمختلف المحاصيل والخضروات الزراعية.

وتنتج هذه الاسمدة عبر مجموعة من المصانع التي تحتوي على خطوط انتاج وفحص متكاملة، ليتطور العمل بعدها لانتاج المنظفات الصناعية و المنزلية ، كما وتطورت خلال الفترة الوجيزة حتى وصلت الى المستويات المتقدمة، وهي تركز الان على المنتجات ذات الاداء الفعال والجودة العالية.

و لاجل المحافظة على الجودة العالية تبنت الشركة استراتيجية صناعية وطنية وخدمية وطبقت المفاهيم الادارية الحديثة وتعمقت في مجال البحث العلمي وسخرت جميع الطاقات والخبرات المحلية والعقول العراقية وهيئت لها جميع الامكانيات في هذا المجال بغية الوصول الى كل ما يمكنه تطوير صناعتها.

**ثانيا :- التحليل الاحصائي الوصفي**

في هذا المبحث تم حساب المتوسطات الحسابية والانحرافات المعيارية ومستوى الموافقة لفقرات الدراسة، المتغير المستقل (ادارة المعرفة) والمتغير التابع (الامن السبراني).

**1- المتغير المستقل ادارة المعرفة**

يتضح من الجدول (1) أن المتوسط الحسابي الإجمالي لاستجابات افراد العينة على فقرات متغير ادارة المعرفة بلغ ما مقداره (3.6475) وهو يقع ضمن مستوى (أتفق) في معيار الحكم، وبلغ الانحراف المعياري (1.0583) وهذا يشير إلى عدم تشتت الاجابات، كون متوسطات جميع فقرات هذا المتغير وقعت ضمن مستوى (أتفق) في معيار الحكم مما يشير إلى أن هناك اتفاقا لدى أفراد العينة على فقرات متغير ادارة المعرفة ومفهومها لتحقيق أهداف المنظمة والذي عبرت عنه عبارات هذا المتغير.

**جدول (1) يبين المتوسطات الحسابية والانحرافات المعيارية ومستوى الموافقة لاستجابات أفراد البحث على فقرات ادارة المعرفة**

| الفقرة | المتوسط الحسابي | الأنحراف المعياري | مستوى الموافقة |
|---|---|---|---|
| 1. | 3.88 | 0.91 | أتفق |
| 2. | 3.60 | 1.05 | أتفق |
| 3. | 3.73 | 1.05 | أتفق |
| 4. | 3.79 | 1.01 | أتفق |
| 5. | 3.55 | 1.02 | أتفق |

| | | | |
|---|---|---|---|
| 6. | 3.67 | 1.12 | أتفق |
| 7. | 3.52 | 1.22 | أتفق |
| 8. | 3.65 | 1.04 | أتفق |
| 9. | 3.63 | 1.03 | أتفق |
| الإجمالي | 3.6475 | 1.0583 | أتفق |

المصدر : من اعداد الباحثين بالأعتماد على نتائج برنامج **spss.26**

**2- المتغير التابع (الامن السيبراني)**

يتضح من الجدول (2) ان المتوسط الحسابي الإجمالي لاستجابات افراد العينة على فقرات الامن السيبراني بلغ ما مقداره (3.6258) وهو يقع ضمن مستوى (أتفق) في معيار الحكم، وبلغ الانحراف المعياري (1.05) وهذا يشير إلى عدم تشتت الاجابات، وأن متوسطات جميع فقرات هذا المتغير وقعت ضمن مستوى (أتفق) في معيار الحكم مما يشير إلى أن هناك اتفاقا لدى افراد العينة على فقرات متغير الامن السيبراني ومفهومه والتطبيق العملي له داخل المنظمة الذي عبرت عنه عبارات هذا المتغير.

**جدول (2) يبين المتوسطات الحسابية والانحرافات المعيارية ومستوى الموافقة لفقرات المتغير التابع الامن السبراني**

| الفقرة | المتوسط الحسابي | الانحراف المعياري | مستوى الموافقة |
|---|---|---|---|
| 1 | 3.64 | 1.06 | أتفق |
| 2 | 3.53 | 1.02 | أتفق |
| 3 | 3.73 | 0.96 | أتفق |
| 4 | 3.63 | 1.06 | أتفق |
| 5 | 3.60 | 1.03 | أتفق |
| 6 | 3.51 | 1.11 | أتفق |
| 7 | 3.76 | 1.17 | أتفق |
| 8 | 3.76 | 0.93 | أتفق |
| 9 | 3.63 | 1.03 | أتفق |
| الإجمالي | 3.6258 | 1.05 | أتفق |

المصدر : من اعداد الباحثين بالأعتماد على نتائج برنامج **spss.26**

**ثالثا:-اختبار الفرضيات**

سيتم في هذه الفقرة التحقق من كل فرضية على حدة، ولهذا الغرض تم حساب الارتباط بين المتغير المستقل وعلاقته مع المتغير التابع لبيان طبيعة الارتباط من حيث القيمة والاتجاه والمعنوية، وقد تم استعمال الانحدار الخطي البسيط لبيان تأثير المتغير المستقل في المتغير التابع وفيما يلي عرض تفصيلي للتحقق من فرضيتي البحث :

1- **الفرضية الاولى : وتنص على "توجد علاقة ارتباط ذات دلالة احصائية بين ادارة المعرفة والامن السيبراني .**

ولبيان قبول الفرضية من عدمها تم حساب معامل ارتباط بيرسون بين ادارة المعرفة والامن السيبراني وكما هو موضح في الجدول رقم (3) اذ يتضح من خلال جدول (3) قوة علاقة الارتباط بين اجمالي المتغير المستقل مع المتغير التابع ، اذ بلغت قيمة معامل الارتباط (0.783) عند مستوى دلالة (0.01) ، لذا فأننا نقبل الفرضية الاولى التي تنص على وجود علاقة ارتباط ذات دلالة احصائية بين ادارة المعرفة (والامن السيبراني في الشركة قيد البحث.

**جدول (3) يبين المخرجات الاحصائية للعلاقة بين ادارة المعرفة والامن السيبراني**

| البُعد | معامل الارتباط | مستوى الدلالة |
|---|---|---|
| ادارة المعرفة | 0.783** | 0.01 |

**2 - الفرضية الثانية: يوجد تأثير ذو دلالة احصائية لإدارة المعرفة في الامن السيبراني .**

لبيان قبول الفرضية من عدمها تم اجراء تحليل الانحدار الخطي البسيط بين ادارة المعرفة والامن السبراني اذ اثبتت نتائج بأن ادارة المعرفة حققت تأثير معنوي كبير في الامن السيبراني اذ بلغت قيمة (B) (0.782)كما هو مذكور في جدول (4) اذ ان المتغير المستقل ادارة المعرفة يفسر (71%) من التغيرات الحاصلة في المتغير المعتمد (الامن السيبراني) والنسبة المتبقية تعود الى متغيرات اخرى غير داخلة في النموذج ، اذ بلغت قيمة معامل التحديد R2 (0.710) ، لاومن هنا نقبل الفرضية الثانية .

**جدول (4) يبين معاملات الانحدار الخطي لتأثير ادارة المعرفة في الامن السبراني**

| البُعد | معامل التحديد $R^2$ | قيمة F | مستوى الدلالة | الثابت | قيمة B | قيمة t | مستوى الدلالة |
|---|---|---|---|---|---|---|---|
| ادارة المعرفة | 0.710 | 270.300 | 0.01 | ثابت الانحدار | 0.782 | 3.010 | 0.01 |
| | | | | الامن السيبراني | 0.825 | 15.176 | 0.01 |

المصدر : اعداد الباحثين بالاعتماد على نتائج برنامج **spss.26**

**المحور الرابع - الاستنتاجات والتوصيات**

**أولا: الاستنتاجات**

توصل البحث الى مجموعة من الاستنتاجات اهمها:

1- تلعب إدارة المعرفة دورًا حاسمًا في الأمن السيبراني للشركات من خلال الاستفادة من البيانات والمعلومات لتعزيز عملية صنع القرار الأمني وحماية المؤسسات من التهديدات السيبرانية. ومن خلال إدارة المعرفة بشكل فعال، يمكن للمؤسسات تحسين قدراتها في مجال الأمن السيبراني وتخفيف المخاطر.

2- أدى تنفيذ ممارسات إدارة المعرفة القوية إلى تعزيز وضع الأمن السيبراني لشركة الجود للتكنولوجيا الزراعية الحديثة بشكل كبير. ومن خلال جمع وتنظيم ونشر المعرفة المتعلقة بالأمن السيبراني بشكل منهجي، تمكنت الشركة من تحديد التهديدات المحتملة والتخفيف من حدتها بشكل استباقي.

3- سهلت ممارسات إدارة المعرفة الفعالة التعاون والتواصل بشكل أفضل بين الإدارات المختلفة. ومن خلال مشاركة المعرفة المتعلقة بالأمن السيبراني عبر المؤسسة، يمكن للموظفين من مختلف الإدارات العمل معًا بكفاءة أكبر لمواجهة التحديات الأمنية.

**ثانيا: التوصيات**

كما تم تقديم مجموعة من التوصيات أهمها:

1- على القادة ان يعطون الأولوية لإدارة المعرفة في خلق ثقافة الوعي بالأمن السيبراني وتعزيز اعتماد أفضل الممارسات داخل المنظمة.

2- للحفاظ على فعالية ممارسات إدارة المعرفة، يوصى بأن تقوم شركة الجود بتحديث أنظمة إدارة المعرفة الخاصة بها بشكل مستمر. ستضمن التحديثات المنتظمة أن تظل قاعدة المعرفة ذات صلة وشاملة.

3- الاستثمار المستدام في برامج التدريب المستمرة أمرا بالغ الأهمية. يجب توفير وحدات تدريبية يتم تحديثها بانتظام لجميع الموظفين لإبقائهم على اطلاع بأحدث التهديدات والممارسات المتعلقة بالأمن السيبراني.

**المصادر**

[1] Johnson, T. A. (Ed.). (2015). Cybersecurity: Protecting critical infrastructures from cyber-attack and cyber warfare. CRC Press.

practices on organizational performance: A balanced scorecard approach. Journal of Enterprise Information Management

[7] Chawla, A., & Saxena, S. (2016). A confirmatory factor analysis of knowledge management assessment instrument in Indian higher educational institutions. International Journal of Quality & Reliability Management.

[8] Munk, T. H . (2015) Cyber-security in the European Region: Anticipatory governance and practices. The University of Manchester (United Kingdom).

[9] Van Meijeren, P. M (2016) Perspectives on Cyber Security: Managerial perspectives on cyber security and the role of end user awareness.

[10] Dreibelbis, R. C (2016) It's more than just changing your password: Exploring the nature and antecedents of cyber-security behaviors.

[11] Guo, K. H. (2013) Security-related behavior in using information systems in the workplace: A review and synthesis. Computers & Security, 32, 242-251

[2] Bedi, P., Goyal, S. B., & Kumar, J. (2020, December). Cyber Security Management Model for Critical Infrastructure and Improving the Security Level on Transferring Digital Data. In International Conference on Innovations in Bio-Inspired Computing and Applications (pp. 525-534). Springer, Cham.

[3] Dickel, D. G., & de Moura, G. L. (2016). Organizational performance evaluation in intangible criteria: a model based on knowledge management and innovation management. RAI Revista de Administração e Inovação, 13(3), 211-220.

[4] Brooking, A. (1999). Corporate memory: strategies for knowledge management, London: International Thomson Business Press

[5] Paliszkiewicz, J., Gołuchowski, J., & Koohang, A (2015) Leadership, trust, and knowledge management in relation to organizational performance: Developing an instrument. Online Journal of Applied Knowledge Management, 3(2), 19-35.

[6] Valmohammadi, C., & Ahmadi, M. (2015). The impact of knowledge management