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

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير للعام 2022 = 4.91

عنوان البحث

القيادة الرقمية ودورها في تعزيز سلوك الامن السيبراني في المنظمات

دراسة تحليلية لآراء عينة من العاملين في المصارف الأهلية في النجف الاشرف

ا.م.د. أميرة هاتف حداوي[1] أ.م.د. ضرغام علي مسلم [2] أ.د. صفاء تايه محمد[3]

[1] جامعة الفرات الأوسط التقنية، الكلية التقنية إدارية، العراق . بريد الكتروني: amira.hatf@atu.edu.iq

[2] جامعة الفرات الأوسط التقنية، الكلية التقنية إدارية، العراق. بريد الكتروني: dr.dhrgam.ameedi.cku@atu.edu.iq

[3] جامعة الكوفة، كلية الادارة واقتصاد، العراق. بريد الكتروني: safat.bakash@uokufa.edu.iq

HNSJ, 2024, 5(1); https://doi.org/10.53796/hnsj51/46

تاريخ النشر: 2024/01/01م تاريخ القبول: 2023/12/15م

المستخلص

هدف البحث التعرف على مستوى القيادة الرقمية في مجموعة من المصارف الاهلية وبيان تأثيرها في تعزيز سلوك الأمن السيبرياني، اذ تعامل هذا البحث مع القيادة الرقمية كمتغير مستقل من خلال أبعادها (الرؤية الرقمية، الابتكار الرقمي، المعرفة الرقمية، المشاركة والتعاون) وسلوك الأمن السيبراني كمتغير تابع من خلال أبعاده (تأمين الجهاز، إنشاء كلمة المرور، الوعي ألاستباقي، والتحديث).

وإجابة مشكلة البحث على عدد من التساؤلات كان من أهمها هو: ما مدى مساهمة القيادة الرقمية في تعزيز سلوك الأمن السيبراني؟ وماهو مدى اهتمام المصارف المبحوثة في تعزيز سلوك الامن السيبراني من خلال قيادتها الرقمية ؟ ومن اجل تحقيق غايات البحث والإجابة عن تساؤلاته تم اختيار مجموعة من المصارف الأهلية العاملة في محافظة النجف الاشرف ، واعتمدت الاستبانة كأداة لجمع البيانات وقد تمثلت عينة البحث بمجموعة من الأفراد العاملين في المصارف الأهلية في محافظ النجف الاشرف حيث تم توزيع (120) استبانة وقد تم تجميعها، وكانت من بينها (97) استمارة صالحة للتحليل الإحصائي أي بنسبة تمثيل بلغت 81%،وقد تضمنت الدراسة فرضيات لاختبار علاقة الارتباط والتأثير بين المتغيرات وباعتماد البرامج الإحصائية (spss v.25) و (smartpls v.4) لتحليل النتائج التي توصل اليها البحث والتي كانت من أهمها توجد علاقة تأثير ايجابية بين القيادة الرقمية وسلوك الامن السيبراني للعاملين.

الكلمات المفتاحية: القيادة الرقمية ،سلوك الأمن السيبراني، المصارف الاهلية.

RESEARCH TITLE

DIGITAL LEADERSHIP AND ITS ROLE IN ENHANCING CYBERSECURITY BEHAVIOR IN ORGANIZATIONS
An Analytic study of a sample of workers in private banks in Najaf Al -Ashraf

Asst. Prof. Dr. Amira Hatf Haddawi[1] Asst. Prof. Dr. ProfDhrgam Ali Muslim [2]
Asst. Prof. Dr. Safaa Tayeh Muhammad[3]

[1] Al-Furat Al-Awsat Technical University, Administrative Technical College, Iraq. Email: amira.hatf@atu.edu.iq
[2] Al-Furat Al-Awsat Technical University, Administrative Technical College, Iraq. E -Mail: dr.dhrgam.ameedi.cku@atu.edu.iq
[3] University of Kufa, College of Administration and Economy, Iraq. Email: Safat.bakash@uokufa.edu.iq

HNSJ, 2024, 5(1); https://doi.org/10.53796/hnsj51/46

Published at 01/01/2024 **Accepted at 15/12/2023**

Abstract

The aim of the research is to identify the level of digital leadership in a group of private banks and to demonstrate its impact in enhancing cybersecurity behavior. This research dealt with digital leadership as an independent variable through its dimensions (digital vision, digital innovation, digital knowledge, participation and cooperation) and cybersecurity behavior as a dependent variable. Through its dimensions (device security, password creation, proactive awareness, and updating),

The research problem answered a number of questions, the most important of which was: To what extent does digital leadership contribute to enhancing cybersecurity behavior? What is the extent of the researched banks' interest in enhancing cybersecurity behavior through their digital leadership? In order to achieve the objectives of the research and answer its questions, a group of private banks operating in the Najaf Governorate .AL ASHARAF

The questionnaire was adopted as a tool for collecting data. The research sample represented a group of individuals working in private banks in the governorate of Najaf, AL ASHARAF where (120) questionnaires were distributed and collected, and among them (97) questionnaires were valid for statistical analysis, meaning a representation rate of 81%. It included The study established hypotheses to test the relationship of correlation and influence between variables, and by adopting statistical programs (SPSS v.25) and SMARTPLS v.4) to analyze the results reached by the research, the most important of which was that there is a positive influence relationship between digital leadership and cyber security behavior of workers.

Key Words: digital leadership, cyber security behavior, private banks.

المقدمة

نعيش عصر رقمي متزايد ، تستمر المنظمات في الحصول على المزيد من الأصول الرقمية ونقل معلوماتها واتصالاتها إلى الشبكات عبر الإنترنت ومع هذا التحول في موقع المعلومات يأتي نوع جديد من التهديد الأمن السيبراني بدلا من القلق على فقدان المعلومات من خلال السرقة المادية للملفات ، تواجه المنظمات احتمال فقدان المعلومات والأصول عبر العالم الإلكتروني ، سواء كان ذلك من خلال مصادر داخلية أو خارجية في مواجهة التكنولوجيا المتطورة والتهديدات الوشيكة على المعلومات ، تجد المنظمات صعوبة متزايدة في التنبؤ بأنواع المخاطر التي قد تواجهها والتي تقوم بتطبيق أنظمة الأمان من خلال تقنيات مختلفة لضمان حماية معلوماتها ضد المهاجمين ومنظمات أخرى ، ومع ذلك حتى الأكثر كثافة يمكن أن تتأثر تدابير الأمان إذا كان موظفوها يتصرفون بطريقة تفرض مخاطر على أمن المعلومات على الإنترنت لقد أصبحت معنية بشكل متزايد بتطوير وحماية أنظمة أمن المعلومات الخاصة بها بالرغم من المحاولات لتأمين البنية التحتية للمعلومات ، إلا أن الموظفين داخلها لا يزالون يشكلون أكبر مصدر تهديد لأمن المعلومات على الإنترنت.

وفي الآونة الاخيرة اتجهت الأنظار الى تحقيق اساليب وتقنيات الأمن السيبراني من خلال طرق عدّة أهمها العمل على تمكين الافراد العاملين ومشاركتهم في السلطة، ومنحهم المزيد من صلاحيات اتخاذ القرار والتحفيز الذاتي والتدريب والتطوير المستمر، مما يؤدي الى زيادة مستوى المعرفة والخبرة لديهم لمواجهة عمليات اختراق الأنظمة الالكترونية والتكنولوجية والمعلومات والبيانات السرية الخاصة بمنظماتهم ونتيجة ذلك، فإن البحث الحالي يركز على معرفة دور التمكين القيادي في تعزيز الأمن السيبراني، وبناء على ذلك قسم البحث الى اربعة مباحث تضمن الاول منهجية البحث العلمية ،اما الثاني فتناول الاطار النظري ،وشمل الثالث الجانب العملي، وحصد الرابع اهم الاستنتاجات والتوصيات .

المبحث الاول / المنهجية العلمية للبحث

اولاً–مشكلة البحث:

يعد التطور التكنولوجي الجديد الذي نشهده لم يغير النظم الادارية والاقتصادية والصناعية والسياسية والاجتماعية فحسب بل تعدى ذلك الى حياة الفرد اليومية في ظل العصر الرقمي المتسارع ووسائل الاتصال الواسعة والتغيرات المتسارعة والتحديات المستمرة التي تواجه البشرية، وبفضل الاستثمارات الضخمة في البنية التحتية الرقمية وحجم التمكين في التحول الرقمي، اكدت نتائج دراسة (Bassett,2016:1)ان مجتمع امن المعلومات ادرك الحلقة الأضعف في سلسلة الأمن السيبراني هي السلوك البشري في تعامله مع أجهزة الكمبيوتر والاجهزة الالكترونية بشكل مباشر وان اغلبها تعمل ضمن شبكة عالمية يمكن اختراقها وهذا يحدث الكثير من المشاكل بسبب الكم الهائل من المعلومات والمعارف الحساسة والمهمة بالنسبة للمنظمة وزبائنها وحتى اسلوب العمل المتوفرة على هذه الشبكة ، وبناء على ذلك كان لابد من انتهاج اسلوب القيادة الرقمية كونها من اساليب القيادة المهمة في بناء القدرات التنظيمية التي تمكن المنظمات من التعامل مع مختلف المتغيرات والتطورات التي تتسم بها بيئة الاعمال الديناميكية في العصر المعرفي الرقمي المتسارع ، مما الزمها الى تدريب العاملين على كيفية حماية البيانات والمعلومات التي توضع على حاسباتها والحفاظ على امنية المعلومات والحرص على ايجاد صيغ متنوعة للتعامل

بينهم ونظام حماية الشبكة والذي يطلق عليه الامن السيبراني فيها، يتم التأكيد باستمرار على أهمية الأمن السيبراني في المجتمع الحديث، مع تلك الهجمات الالكترونية ،لذلك نحاول من خلال هذا البحث معرفة" نمط القيادة الرقمية ودورها في تعزيز سلوك الامن السيبراني للمنظمة المبحوثة والمتمثلة بمجموعة من المصارف الاهلية في النجف الاشرف من اجل الوصول الى مستويات النجاح في سوق المنافسة. ويمكن بيان مشكلة البحث من خلال التساؤل الرئيس الآتي :

(ما هو دور القيادة الرقمية في تعزيز سلوك الامن السيبراني)؟ ويتفرع من هذا التساؤل عدد من التساؤلات الفرعية وكما يأتي:

1. ما هو دور الابتكار الرقمي في تعزيز سلوك الامن السيبراني ؟
2. ما هو دور الرؤية الرقمية في تعزيز سلوك الامن السيبراني؟
3. ما هو دور المعرفة الرقمية في تعزيز سلوك الامن السيبراني ؟
4. ما هو دور المشاركة والتعاون في تعزيز سلوك الامن السيبراني؟

ثانياً-أهمية البحث

تتمثل اهمية البحث في النقاط الاتية :

1- تكمن اهمية البحث الحالي في كونه ركز على مفهوم حديث الا وهو القيادة الرقمية والذي يعد اسلوبا هاما لإغناء مهارات العاملين وتعزيز سلوك الامن السيبراني لديهم في المصارف المبحوثة.

2- يعد البحث الحالي من الدراسات الحديثة التي تناولت موضوع القيادة الرقمية واثرها في تعزيز سلوك الامن السيبراني.

3- تسعى نتائج البحث الى جذب انظار القائمين لاتخاذ القرارات والتخطيط لأهمية تطبيق القيادة الرقمية بشكل صحيح ورفع مستوى سلوك الامن السيبراني وتعزيزه في المنظمة المبحوثة.

4- يقدم البحث الحالي مقترحات عملية صالحة للتطبيق في المصارف المبحوثة بما يسهم في تعزيز سلوك الامن السيبراني.

ثالثاً-اهداف البحث

يهدف البحث الى تحقيق الاهداف الآتية:

1. تحديد مستوى اعتماد القيادة الرقمية في المصارف المبحوثة في النجف الاشرف وامكانية تحقيقها لسلوك الامن السيبراني.
2. استكشاف دور الابتكار الرقمي في دعم سلوك الامن السيبراني للمصارف المبحوثة في النجف الاشرف.
3. بيان اهمية الرؤية الرقمية في تعزيز قدرات المصارف المبحوثة في النجف الاشرف على تحقيق سلوك الامن السيبراني.
4. التعرف على دور المعرفة الرقمية في تعزيز قدرة المصارف المبحوثة في النجف الاشرف على ادارة سلوك الامن السيبرياني.
5. تحديد مستوى المشاركة والتعاون في المصارف المبحوثة في النجف الاشرف.

6. اختبار مستوى العلاقة والتأثير بين القيادة الرقمية وسلوك الامن السيبراني في المصارف المبحوثة في النجف الاشرف.

رابعاً–فرضيات البحث

استنادا لما ورد في مشكلة البحث واهدافه واستكمالا للأسس المنهجية للبحث يمكن استعراض فرضيات البحث من خلال الآتي:

***الفرضية الرئيسة الأولى (توجد علاقة ارتباط ذات دلالة إحصائية بين القيادة الرقمية في تعزيز سلوك الامن السيبراني)**

وتنبثق من فرضية الارتباط الرئيسة عدد من الفرضيات الفرعية وهي كالآتي:

1- الفرضية الفرعية الأولى(توجد علاقة ارتباط ذات دلالة إحصائية بين الابتكار الرقمي وتعزيز سلوك الامن السيبراني).

2- الفرضية الفرعية الثانية (توجد علاقة ارتباط ذات دلالة إحصائية بين الرؤية الرقمية وتعزيز سلوك الامن السيبراني) .

3- الفرضية الفرعية الثالثة (توجد علاقة ارتباط ذات دلالة إحصائية بين المعرفة الرقمية وتعزيز سلوك الامن السيبراني).

4- الفرضية الفرعية الرابعة (توجد علاقة ارتباط ذات دلالة إحصائية بين المشاركة والتعاون وتعزيز سلوك الامن السيبراني).

***الفرضية الرئيسة الثانية (توجد علاقة تأثير ذات دلالة معنوية للقيادة الرقمية في تعزيز سلوك الامن السيبراني)**

وتنبثق من فرضية التأثير الرئيسة عدد من الفرضيات الفرعية وهي كالآتي:

1- الفرضية الفرعية الأولى (توجد علاقة تأثير ذات دلالة معنوية للابتكار الرقمي في تعزيز سلوك الامن السيبرياني)

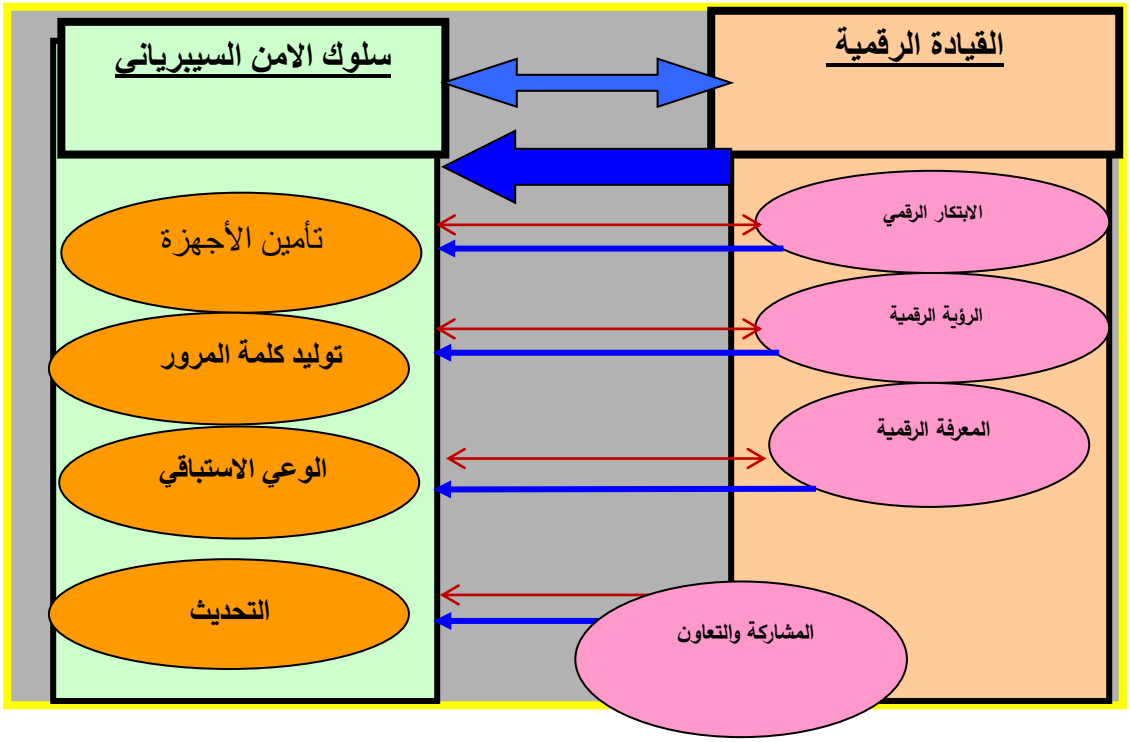
2- الفرضية الفرعية الثانية (توجد علاقة تأثير ذات دلالة معنوية للرؤية الرقمية في تعزيز سلوك الامن السيبرياني)

3- الفرضية الفرعية الثالثة (توجد علاقة تأثير ذات دلالة معنوية للمعرفة الرقمية في تعزيز سلوك الامن السيبرياني)

4- الفرضية الفرعية الرابعة (توجد علاقة تأثير ذات دلالة معنوية للمشاركة والتعاون في تعزيز سلوك الامن السيبرياني)

خامساً- المخطط الفرضي للبحث

يوضح المخطط الفرضي للبحث شكل العلاقات الافتراضية بين متغيراته الرئيسة وابعادها الفرعية والتي يمكن بيانها من خلال الشكل (1)



شكل (1) الانموذج الفرضي للبحث

سادساً -مجتمع وعينة البحث:

لاختبار صحة انموذج وفرضيات البحث الحالي وتحقيق اهدافه ، تم تطبيق موضوع بحثنا في منظمة خدمية ، وبالتحديد على القطاع المصرفي العراقي كمجتمع ، وكانت العينة (97) موظف ممن لديهم خبرة واسعة في العمل الوظيفي في المصارف الاهلية في النجف الاشرف المتمثلة ب (بغداد، سومر، الاتحاد العراقي، الاهلي العراقي، التنمية الدولي، بارسيان، الشرق الاوسط العراقي للاستثمار، المستشار، الخليج التجاري، المنصور) ، اذ تم توزيع استمارات الاستبانة عليهم من اجل تحليل اجاباتهم احصائياً للوصول الى نتائج البحث.

المبحث الثاني : الاطار النظري للبحث

اولاً: القيادة الرقمية Digital leadership

1- مفهوم القيادة الرقمية Concept of digital leadership

اصبحت التكنولوجية الرقمية حقيقة في المجتمع واحدثت ظاهرة جديده في ممارسات الاتصال ، وبالذات وسيلة الاتصال الافتراضي تكتسب مكانة في المجتمع ، واصبحت تطبيقات الاتصال المتمثلة,twitter, telegram (whatsapp) من الضروريات الملحة في المجتمع، والتي تعدمن التطبيقات الشائعة في مجالات الحياة كافة هذه الظاهرة العالمية شملت ايضا اسلوب القيادة ودفعت الحاجه للتفكير في المستقبل ، اذا كان القادة يرغبون التنافس في عالم تنافسي محتدم عليهم ان يعتمدوا نمط التفكير المستقبلي القادر على توقع القدرات التكنولوجية ((Antonopoulou, H., Halkiopoulos,2021,405-406)، مما ادى الى ادخال العديد من المصطلحات

الجديدة من قبل الباحثين كالقيادة عن بعد، والقيادة الرقمية ،والقيادة الافتراضية الامر الذي بات واضحا لتحولها الى ظاهرة عالمية توثر بشكل مباشر على المشهد القيادي وتكتسب مكانة مهمة في المنظمات .

تعددت تعريفات القيادة الرقمية وتنوعت بتنوع مقاصد الباحثين ومأربهم ،وعرفت بانها (تأثير اجتماعي بواسطة تكنولوجيا المعلومات والاتصالات لأحداث تغيير جذري في المواقف والمشاعر ،والتفكير ،والسلوك والاداء مع الافراد والجماعات والمنظمات واقامة علاقات افتراضيه من التأثير ، وانها تقنية الموارد والعمليات القيادية الهيكلية ودورها يكمن ببناء الوعي وانفتاح افراد المجتمع من اجل الوصول الى تكنولوجيا المعلومات والاتصالات الجديدة والموارد التي يمكن ان تساعد لتحقيق اهدافهم) (Baenfor,2016:134)، واشار ("Rogers,2016;22) ان القيادة الرقمية "تشير الى ممارسات وسلوكيات القائد من خلال استخدام الادوات الرقمية كوسائل التواصل الاجتماعي والتواصل عبر تطبيقات الويب مثل برنامج zoom ، والمؤتمرات والفيديوات وغيرها من الادوات الرقمية التي تتطور كل يوم ،والقيادة الرقمية لا تعني ان يكون القائد خبيرا في استخدام ادوات وتطبيقات التكنولوجيا وصيانتها وحل مشكلاتها بل الكيفية التي يكون مطلعا على اخر تقنيات التكنولوجيا ليستطيع توجيه والتأثير على العاملين بما يعود بالمنفعة على تحقيق اهداف المنظمة بفاعلية ، واضاف (Van Ee, J., El Attoti, I., Ravesteyn, P., & De Waal, B. M. ,2020) بان القيادة الرقمية تعد نمط حيوي يهدف الى استثمار الثورة الرقمية لتحقيق ميزة تنافسية لضمان النجاح في مستقبل التحولات الرقمية ،والقائد الرقمي هو الشخص القادر على تحفيز من يعملون تحت اشرافه دون التقيد بزمان او مكان وتدبير العمل بطريقة تركز على تبادل المعلومات معهم.

ويرى الباحثين وبناءً على ما تقدم "القيادة الرقمية "هيمزيج من الكفاءة والثقافة الرقمية التي تدفع نحو التغيير والاستفادة من التكنولوجيا الرقمية ، وتشير الى القدرة على تحديد وتحقيق الفرصة لنمو الاعمال والقيمة من خلال توجيه العاملين لاستخدام التكنولوجيا الرقمية.

2- مبادىء تطوير القيادة الرقمية للتعامل مع التحديات الرقمية .

حدد (Rüth, R., & Netzer, T. 20203-8) مجموعة من المبادئ التي يجب اخذها بنظر الاعتبار عند اتباع نمط القيادة الرقمية تمثلت بالاتي:

أ- الثقة :تعني الثقة في المهارات المهنية والاجتماعية للموظفين ومنحهم الفرصة للسيطرة على انفسهم وتحمل المسؤولية .

ب- شبكات التواصل : ان اقامة القنوات والمنصات الاجتماعية المختلفة للتواصل بين الناس من اهم المهام للقيادة في البيئة الرقمية مما ينبغي على القيادة اقامة الشبكات عبر جميع المستويات داخلية وخارجية لتعزيز التعاون المتعدد التخصصات وتمهيد الطريق امام تبادل الخبرات والتعلم .

ت- الانفتاح : والتي تمثل الاتصالات المفتوحة والشفافية والتي تعد امرا ضروريا للقائد الرقمي ،حيث يختلف الموظفون من اداء الخدمات على النحو الامثل والفعل ويمكنهم التصرف بشكل دائم لصالح المنظمة ،وينبغي على الموظفين معرفة المتطلبات وتزويد القادة الرقميين بالمعلومات بشكل استباقي ،فالانفتاح يعني تعزيز التبادل والتشارك المعرفي بين الافراد ورؤساء العمل بشكل كافي .

ث- الرشاقة :تمثل القدرة على التكيف بسرعة مع المتغيرات البيئية باستمرار والتعلم من التجارب ،وتعد مقياس للاستجابة بسرعة ومرونة للمتغيرات بكفاءة وفاعلية.

3- ابعاد القيادة الرقمية :

تعددت وجهات نظر الباحثين في تصنيف ابعاد القيادة الرقمية حيث يرى (Francera, S., & Bliss, J. 2011,349) ان ابعاد القيادة الرقمية تتمثل بالخبرة الرقمية ،والبصيرة الرقمية ، في حين يرى (يوسف والجدرواي، 2019) بان ابعاد القيادة الرقمية تمثلت في (الابداع ، الاقناع ،المعرفة)، فيما يرى (Tanniru, M. R. 2018)ابعاد القيادة الرقمية تتمثل في (البصيرة الرقمية ،الاستراتيجية الرقمية ،الثقافة الرقمية ،الكفاءة الرقمية ،فيما اشار(Pancheva, S. 2018, 9) ان ابعاد القيادة الرقمية قد تمثلت باربع ابعاد وهي (الرؤية الرقمية ،المعرفة الرقمية ،الابتكار الرقمي ،والمشاركة والتعاون)، واتفق الباحثين مع (Pancheva, S,2018) في تحديد ابعاد القيادة الرقمية والمتضمنة (بعد الابتكار الرقمي ،بعد المعرفة الرقمية ،وبعد المشاركة والتعاون) كونها الاكثر اتفاق بين الباحثين والاكثر ملائمة لاهداف وبيئة التطبيق للبحث الحالي وسيتم تناولها بشيء من الايجاز :

أ- الابتكار الرقمي : اشار (de Araujo, L. M., Priadana, et al ,2021: 45)الابتكار بانه الاستعداد للأشياء غير متوقعة والمألوفة والانطلاق بأفكار جديدة من خلال الابتكار والذي يمكن ان يؤثر على مجال نماذج العمل والمنظمة من المكاتب غير ورقية الى المكاتب المنزلية والى عمليات الانتاج الالي، فمن صفات القائد الرقمي هو التخلي عن الهياكل الجامدة والقدرة على الانطلاق بفكرة جديده وتطوير وتنفيذ هذه الافكار بشيء من الابداع بما يساعد على تحقيق الاهداف ومواجهة المشكلات التي تواجه تحقيق هذه الاهداف والتحول الرقمي ،ويرتبط الابتكار الرقمي بتكنولوجيا المعلومات والاتصالات وطريقة استخدامها من اجل تحسين الخدمات والمنتجات بطريقة مبتكرة وجديدة.

ب- الرؤية الرقمية : تعني القدرة على الرؤية من خلال الضباب والتخطيط للمستقبل ومن ثم تغيير المستقبل ، فهذا يعني تحول الرؤية القديمة الى شيء جديد ويمكن ان يكون لديك تأثير حقيقي على ما ينبغي ان تكون عليه هذه الرؤية ،والقائد الرقمي يمتلك رؤية واضحة حول عملية التحول الرقمي وينظم الاهداف من خلال وضع الخطط الصحيحة والمدروسة للعمل فيما لا يترك مجال للصدفة ،وانها ضرورية لقادة الأعمال في جميع الصناعات(Consulting head lines. 2020, 55-56) واشار (Goethal, G., Sorenson, G,2020) استخدام الرؤية الرقمية الخاصة بك عامل نجاح رئيسي، يتطلب تحقيقها مناهج مبتكرة. والتفكير التصميمي هو المنهجية الإبداعية لإطلاق العنان للابتكار، إنه قادر على الإجابة على سؤال حول كيفية استخدام منصات الذكاء الاصطناعي والقدرات الحالية لتحويل العمليات التجارية إلى رقمية، إن معرفة الأساس التكنولوجي والإبداع في تطبيق قدراته يضعان قادة الأعمال وتكنولوجيا المعلومات في موقع الهيمنة على تقنية المعلومات، إنه المثلث السحري: الرؤية – الابتكار – المعرفة، التحول الرقمي هو تحول جذري ، مما يجعل المنظمات تعيد التفكير في كيفية هيكلة نفسها والمنافسة في السوق، يمكن للقادة المساعدة في التفاوض بشأن هذا الانتقال من خلال التجديد الاستباقي لما سيبدو عليه المستقبل الرقمي المختلف جذريًا لبدء صياغة هذه الرؤية ، يجب على القادة أولاً تحديد الفوائد التي يريدون اكتسابها من خلال التقنيات الرقمية ، وماهي الاستراتيجيات التي سيشترك بها العملاء

والموظفين والمستثمرين. أن بعض المنظمات تمر بثلاث خطوات متميزة لصياغة رؤاها الرقمية: تحديد هدف واضح ، إشراك المنظمة وتطوير الرؤية بمرور الوقت، الرؤية الرقمية الملهمة هي حجر الزاوية في التحول الرقمي الناجح، على الرغم من أن العديد من المديرين التنفيذيين يبدون مدركين لتأثيرها على أعمالهم ، إلا أن القليل منهم قد أدمج الرقمية في رؤية استراتيجية مقنعة للمستقبل، هذه الرؤى لا تركز ببساطة على الخاتمة عند تطبيق التقنيات الجديدة، بل يوضحون كيف يمكن للمنظمات تحسين تجربة عملائها ، وتبسيط عملياتها أو تحويل نماذج أعمالها، هذه ليست مهمة بالسهلة، ولا ينبغي تركها لكبار القادة وحدهم بل هي رحلة يقوم التنفيذيون بزرع البذرة في الأعلى ، وبعد ذلك يجب إشراك الأشخاص على جميع المستويات في المنظمة لجعل الرؤية تنمو وتتطور.

ت – المعرفة الرقمية : أصبحت الرقمنة والابتكارات التكنولوجية مكونًا أساسيًا لمنظمات اليوم وتؤثر بشكل مباشر على عمليات الإدارة فيها، حيث تمكّن الابتكارات التكنولوجية التي تم إنشاؤها حديثًا ان تحقق قدر أكبر من المرونة في اتخاذ قراراتها مقارنة بالتي لم يتم رقمنتها ، وان إدارة المعرفة هي أحد العناصر التي تبني مزايا تنافسية من حيث الأساليب والاستراتيجيات المستخدمة كإدخال منتجات جديدة والتحسين المستمر لتسهيل عملياتها ، وإعادة إنتاجها لاحتياجات المنظمات المنافسة(Rot , 2020 : 555).

يمكن تعريف ادارة المعرفة الرقمية على انه تطوير الابتكارات التكنولوجية في إدارة المعرفة وربط التحديات ، والقدرة على تحديد البيانات من مواقع مختلفة داخل المنظمة من حيث القدرة على جمع بيانات الكترونيا وربطها بالأداء والأنشطة التي يقوم بها الموظفون وتحسين البيانات والجمع والمعالجة الأولية لها وتعد مكونًا أساسيًا للمنظمة وتؤثر بشكل مباشر على عمليات الإدارة وتمكنها من تحقيق قدر أكبر من المرونة في اتخاذ القرار مقارنة بالتي لم يتم رقمنتها(Buntak , 2020 : 42-43)

ث–المشاركة والتعاون : وهو العملية التي تشير الى استخدام المعرفة الجماعية من خلال اشكال تبادل الخبرة والتي تخلو من التسلسل الهرمي ،حيث تشمل اكبر عدد من الموظفين سواء كانت على هيئة ورش عمل وجه لوجه او ورش عمل افتراضية عبر منصات الكترونية بحيث يكون لكل شخص لديه الفرصة لطرح افكاره وآرائه للمشاركة في عملية صنع القرار (Sheninger , E. 2019, 22).

ثانيا /سلوك الامن السيبراني Cyber security behaviour

1–مفهوم سلوك الأمن السيبراني The Concept of Cybersecurity

من الصعوبات البحثية التي تواجه الباحث هي صعوبة تحديد المصطلحات حيث لا يمكن تحديد المصطلحات وفق تعريفات محددة تكون جامعة وشاملة لذا فإن الباحث يجد نفسه أمام كم هائل من التعريفات التي تزيد حاجته أحيانا ولعل مفهوم الامن السيبراني واحدا من هذه المفاهيم التي تعددت تعريفاتها طبقا لتعدد دراساتها حيث ان مفهوم الامن السيبراني لغويا يمكن تقسيمه لكلمتين:–

الأمن : هو نقيض الخوف والأمن مصدره الفعل أمن أمنا وامانا وآمنة يعني اطمئن النفس وزوال الخوف وسكون القلب(إبراهيم, المعجم الوجيز : مجمع اللغة العربية ,١٩٨٩ ص ٢٥) حيث قال تعالى :((الَّذِي أَطْعَمَهُمْ مِنْ جُوعٍ وَآمَنَهُمْ مِنْ خَوْفٍ))(سورة قريش الآية (٤) .

اما السيبراني : هو أحد المصطلحات الحديثة واحتل الصدارة في معجم دراسات الأمن الدولي حيث ان كلمة cyberيونانية الاصل مشتقة من كلمة kybernetes بمعنى الشخص المسؤول عن ادارة دفة السفينة وتستخدم

أحيانا للمتحكم governor كما وان بعض الباحثين يرجعون أصلها إلى العالم الأمريكي Norbert Wieners وهو عالم بالرياضيات واستخدمها دلالة عن التحكم الالي ويعد من وضع حجر الأساس للسبرنتيقية ووصفها بكتابه Cybernetics or Control and communication in the Animal and the machine بانها تعني التحكم والتواصل ، اما اصطلاحاً و في زحمة التسارع العلمي والمعرفي والاكتشافات المبهرة في شتى الميادين ،شكل ظهور نظم المعلومات الصدارة في أذهان جميع المنظمات باختلاف حجمها ونوعها إذ تعدّ اهم العناصر الشائعة التي تسهم في دفع قادة المنظمات لإدارة المعلومات وحمايتها من خلال ضمان جودة المعلومات والحفاظ عليها من الاستغلال والاستخدام، إذ ان تطور التقنيات التكنولوجية والاجهزة الذكية بشكل واسع حول العالم وبسرعة عبر شبكات الانترنت العالمية أدى الى زيادة احتمالية تعرض هذه التقنيات والأجهزة الى الهجوم والاختراق بسهولة ومحاولة التلاعب والاستخدام غير المصرح به من قبل بعض الأطراف (Lu & Da, 2018: 1). ونتيجة لذلك توجهت أغلب المنظمات الى تضمين مفهوم سلوك الامن السيبراني ضمن انشطتها وعملياتها الذي يعدّ من اهم التقنيات القادرة على ضمان توفير الحماية لجميع انظمة المعلومات والاتصالات في المنظمة ومعالجة جميع الجوانب الالكترونية على وجه التحديد (Evans et al., 2016: 4667).

وبذلك جذبت سلوكيات الأمن السيبراني للموظفين في الآونة الأخيرة الكثير من الاهتمام من قبل الباحثين ، ومن ثم، فإن السلوكيات لها آثار مباشرة على الأمن في المنظمات ، تشير الأبحاث السابقة إلى العديد من العوامل مثل: القواعد التنظيمية ، والوعي الأمني ، والدافع ، والقيادة ، والثقافة التنظيمية تؤثر على نزوع الموظف إلى المشاركة في الإجراءات التي يمكن أن تحمي المعلومات الرقمية للمنظمة، وقد تكون المنظمات ذات الاهتمامات الخاصة لحماية معلوماتها الرقمية قادرة على المبادرة بأختيار الموظفين الذين سينخرطون في بعض السلوكيات لحماية الأصول الرقمية ،سيكون وسيلة هامة في مجال الأمن ,لاحظ الباحثون أن هناك الكثير من الاختلاف حول كيفية تصور السلوكيات المتعلقة بالأمن السيبراني على أفضل وجه Kosseff, J. 2017(0)، ويوضح الجدول (1) بعض تعاريف الأمن السيبراني على وفق آراء مجموعة من الباحثين وكما يأتي:

جدول (1) بعض تعاريف سلوك الأمن السيبراني

ت	الباحث والسنة	التعريف
1	(Kemmerer, 2003: 3)	مجموعة من الاساليب الدفاعية لحماية البيانات والمعلومات الخاصة بالمنظمة التي يتم استخدامها لاكتشاف المتسللين المحتملين وإحباطهم.
2	(Zimmerman, 2014: 14)	عملية تضمن سرية ونزاهة تكنولوجيا المعلومات وتشتمل على العديد من المهام مثل هندسة الأنظمة القوية وإدارة التكوين وسياسة ضمان المعلومات والتدريب الشامل للقوى العاملة.
3	(Sinha et al., 2015: 19)	هو احد مصادر تحقيق الاستدامة في المنظمات في جميع انحاء العالم والذي يعمل على حماية وجدولة جميع الموارد المحدودة في المنظمات من خلال تخصيصها او نشرها، مع اخذ الوقت في نظر الاعتبار واستجابات الخصوم للوضع الأمني وأوجه عدم اليقين المحتملة.
4	(Evans et al., 2016: 4667)	النشاط او العملية او القدرة او الحالة التي يتم بموجبها حماية انظمة المعلومات والاتصالات والمعلومات الواردة فيها او الدفاع ضد الضرر والحماية من الاستخدام والاستغلال والتعديل.

المصدر : اعداد الباحثين بالاستناد الى ما ورد في البحوث والدراسات .

2- أهمية سلوك الأمن السيبراني

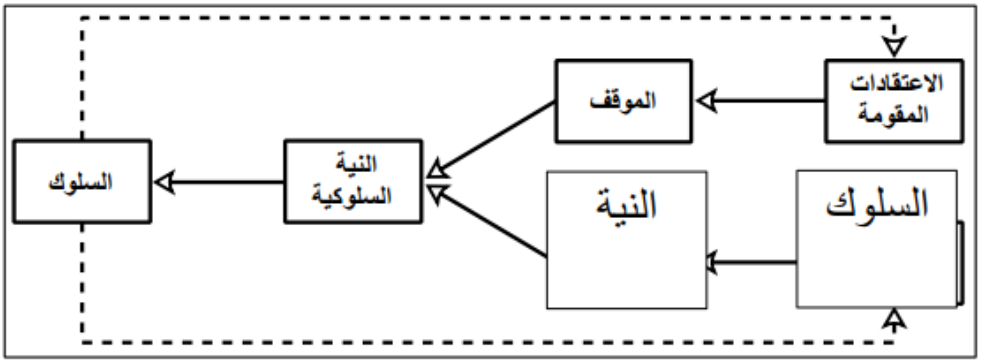
تنامت اهمية سلوك الأمن السيبراني نتيجة للتقنيات والعمليات التي يعتمدها خصيصاً لحماية الشبكات وأجهزة الكومبيوتر وقواعد البيانات ومختلف التطبيقات الاخرى من اي هجمة او اختراق او وصول غير مصرح به من قبل الاطراف الخارجية، مما يؤدي الى تطوير تكنولوجيا المعلومات وكذلك خدمات الانترنت (Wu et al., 2018: 3-4).

يعدّ سلوك الأمن السيبراني من أهم مصادر القوة ليس للأشخاص والمختصين فحسب بل لجميع المنظمات المختلفة ، وتبرز اهميته نتيجة الى ما يحققه من ارتباط ما بين نظم الاتصالات والأنترنت وعدم إمكانية عزل الاجهزة عن الشبكات المحلية والشبكات واسعة النطاق التي يحتاجونها، وان اعتماد المنظمات المختلفة على هذه المعلومات والتقنيات تزداد يوماً بعد يوم بازدياد التطورات التكنولوجية في العالم (Sun et al., 2018: 1745). ووفقاً لما يراه (Kruse et al., 2017: 6) في الوقت الحاضر أصبح من أهم أجزاء أمن الدولة والأمن الاجتماعي عن طريق المعايير والاجراءات التي يضعها لمنع الأستخدامات غير السلمية وغير المصرح بها للمعلومات وما يمثل من تهديد للأمن الدولي والبنى التحتية لمختلف المعلومات.

وأشار (Sinha et al., 2015: 21) أنّ الأمن السيبراني يوفر للمنظمة الاستراتيجيات المرنة التي تمكنها ان تتلائم مع المتغيرات البيئية المختلفة عن طريق توفير الآليات او التكتيكات الخاصة بالأمن السيبراني مقابل التطور المستمر للأخطار، ولا يقتصر الأمن السيبراني على تعزيز البعد التقني في المنظمة بل يتجاوز ذلك الى تفسير الأبعاد الثقافية والاجتماعية والاقتصادية والعسكرية، اضافة الى (Thaw, 2013: 8) أنّ الأمن السيبراني يعتمد على مزيج من التحديات السياسية والتقنية والاجتماعية والثقافية مما يؤدي إلى تعزيز وحماية البنى التحتية لجميع المعلومات التي تتسم بالحساسية، ويسعى الأمن السيبراني إلى تحقيق تعاون ما بين منظمات الأعمال أو المنظمات الحكومية مع شركات الاتصالات والمعلومات، لتعزيز من عملية خلق القدرات الوطنية لمواجهة الجرائم السيبرانية والحد منها، وهناك مجموعة من النظريات التي فسرت سلوك الامن السبرياني وكان من ضمنها مايأتي:

أ- نظرية الفعل المبرر/ نظرية السلوك المخطط

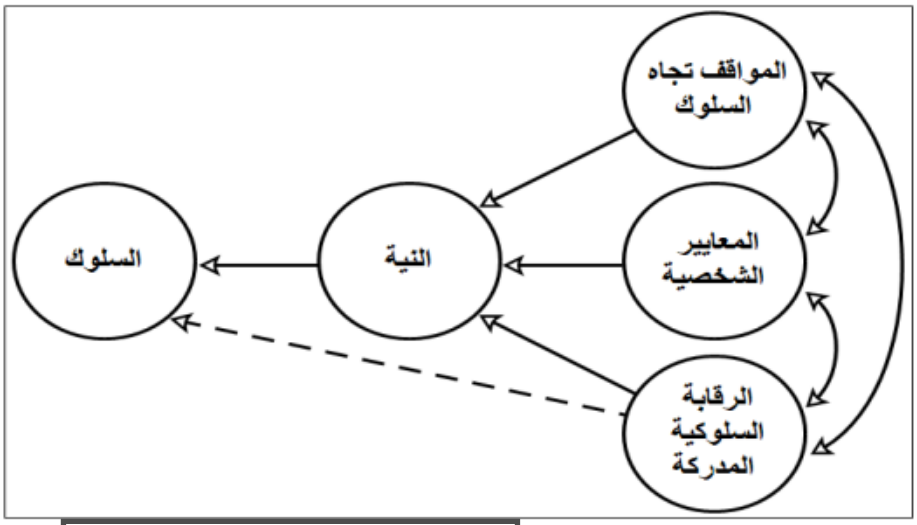
تستند هذه النظرية على الإجراء المعقول ونظرية السلوك المخطط على مفهومين: (1) الأشخاص المعقولون ويستفيدون من المعلومات عندما يقررون الاختيار بين السلوكيات ، و (2) ينظر الناس إلى الآثار المترتبة على سلوكهم, يتم توجيه السلوك نحو الأهداف أو النتائج ، ويختار بحرية تلك السلوكيات التي من شأنها تحريكهم نحو تلك الأهداف ،وتأخذ النظريات في الاعتبار أربعة مفاهيم: النية السلوكية ، والموقف ، والأعراف الاجتماعية ، والتحكم السلوكي المدرك النية في التصرف لها تأثير مباشر على السلوك الفعلي كدالة في الموقف والمعايير الذاتية، الموقف هو وظيفة كل من العواقب الشخصية المتوقعة من التصرف والقيمة العاطفية وضعت على تلك النتائج, والشكل(2) يوضح نظرية الفعل المبرر(Redondo, I., & Puelles, M. 2017, 66-67).



شكل (2) : نظرية الفعل المبرر (المسبب)

Source: Miner,Johm,(2006). "Organizational Behavior from theory to practice", M.E sharpe published, Printed in the United States of America.

ب-نظرية السلوك المخطط : اشار (Middleton,John. 2002,99) ان هذه النظرية تشير للتحكم في العمل: من الإدراك إلى السلوك. الآثار: لتشجيع المستخدمين على تغيير سلوك الأمان ، يجب على النظام إنشاء رسائل تؤثر على نوايا المستخدمين ؛ في المقابل ، يتم تغيير النوايا عن طريق التأثير على مواقف المستخدمين من خلال تحديد المعايير الاجتماعية والسيطرة السلوكية وبذلك يجب على المستخدمين إدراك أنه يمكنهم التحكم في إكمال مهامهم بنجاح وأمان ،والشكل (3): يوضح نظرية السلوك المخطط.



شكل (3) نظرية السلوك المخطط

الشكل رقم (١) ق

Source:Sheeran, P., & Orbell, S. (2000). Self-schemas and the theory of planned behaviour. *European journal of social psychology*, *30*(4), 533-550.

ج-نظرية مراحل التغيير

يقوم هذا النموذج بتقييم استعداد الشخص لبدء سلوك جديد ، وتقديم استراتيجيات أو عمليات التغيير لإرشادها خلال مراحل التغيير إلى العمل والصيانة, التغيير هو عملية تنطوي على التقدم من خلال عدة مراحل التأمل

(الأفكار) ، والإعداد (الأفكار والعمل) ، والعمل (تغيير السلوك الفعلي) ، والصيانة ، وإنهاء الخدمة ، لذلك يجب أن تتطابق التدخلات لتغيير السلوكيات وتؤثر على المرحلة المناسبة للتقدم خلال المراحل المبكرة ، يطبق الناس العمليات المعرفية والعاطفية والتقييمية مع تحرك الناس نحو الصيانة أو الإنهاء ، فهم يعتمدون أكثر على الالتزامات والتكيف ، والتغيير من أجل الافضل ،لتحرر نفسك من العادات السيئة (Mowbray, T, J, 2013,37-38)

عقد معهد حماية البنية التحتية للمعلومات ورشة عمل مدتها يومان للجمع بين أعضاء مجتمع العلوم السلوكية ومجتمع الأمن السيبراني ، ودراسة كيفية نقل النتائج التي تم تقييمها بنجاح إلى واقع عملي ، وإنشاء مجموعات من الباحثين الراغبين في إجراء تقييم تجريبي لنتائج واعدة وتقييم قابليتها للتطبيق على الأمن السيبراني خلقت ورشة العمل فرصة لتشكيل مجموعات من الباحثين والممارسين المتحمسين واعتماد طرق أكثر فعالية لدمج العلوم السلوكية مع الأمن السيبراني وهذا هو ، ورشة العمل هي الخطوة الأولى في ما نأمل أن تكون شراكة مستمرة بين علوم الكمبيوتر والسلوكيات التي من شأنها تحسين فعالية سلوك الأمن السيبراني ,Sheeran, P., & Orbell. (S. 2000, 55)

أ- تحديد النتائج الموجودة التي يمكن أن تعزز الأمن السيبراني في المدى القريب.

ب- تحديد النتائج العلمية السلوكية المحتملة التي يمكن تطبيقها ولكنها تستلزم إجراء تقييمات تجريبية لتأثيراتها على الأمن السيبراني.

ت- -تحديد مجالات الأمن السيبراني والمشاكل التي يمكن أن يكون لتطبيق المفاهيم من العلوم السلوكية تأثير إيجابي.

ث -إنشاء مستودعاً للمعلومات حول العلوم السلوكية والأمن السيبراني.

4- ابعاد سلوك الامن السيبراني:

قام (Egelman & Peer, 2015) بتحديد أربعة ابعاد أساسية لسلوك الامن السيبراني وفيما يلي تعريف هذه الابعاد:

1- **تأمين الأجهزة Device Securement:** يشير الى استخدام كلمات المرور في قفل الأجهزة وانشاء القفل التلقائي للأجهزة او قفلها يدويا قبل مغادرتها.

2- **توليد كلمات المرور Password Generation:** يشير الى اختيار كلمات مرور قوية وعدم إعادة استخدام كلمات المرور بين الحسابات المختلفة.

3- **الوعي الاستباقي Proactive Awareness:** يشير الى انتباه الفرد الى الإشارات في المواقع مثل عنوان URL وغيرها من المؤشرات في المواقع او البريد الالكتروني واخذ الحضر عند إعطاء المعلومات الى المواقع وان يكون الفرد استباقيا في التبليغ عن المشاكل الأمنية.

4- **التحديث Updating:** يشير الى درجة قياس المستخدمين بتثبيت التحديثات الأمنية بشكل مستمر والتاكد من استخدام البرامج بأحدث اصداراتها

المبحث الثالث :الجانب العملي للبحث

اولاً- ترميز المتغيرات والمقاييس المعتمدة

تم اختيار ابعاد متغيرات البحث استنادا لما ورد في الادبيات العلمية حول القيادة الرقمية و سلوك الامن السيبراني , فقد تم الاعتماد في قياس متغير القيادة الرقمية على الابعاد المعتمدة من قبل(Pancheva, S. 2018, 9) والمتمثلة بـ(الابتكار الرقمي، الرؤية الرقمية ، المعرفة الرقمية ،المشاركة والتعاون) , اما متغير سلوك الامن السيبراني فقد تم الاعتماد على الابعاد من قبل (Egelman & Peer, 2015 والمتمثلة بـ(تأمين الاجهزة ، توليد كلمة المرور ،الوعي الاستباقي، التحديث) ولتسهيل عمليات التحليل الاحصائي في المتغيرات الرئيسة والابعاد الفرعية تم تحديد رموز لها والتي يمكن بيانها من خلال الجدول (2) كالآتي:

الجدول(2) ترميز متغيرات ومقاييس البحث

ت	المتغيرات الرئيسية	الابعاد الرئيسية	الفقرات	مصدر المقياس
1	القيادة الرقمية DL	المعرفة الرقميةN	N11-N14	Pancheva, S. 2018,
		الابتكار الرقميI	I6-I10	
		الرؤية الرقميةV	V1-V5	
		المشاركة والتعاون P	P15-P19	
2	سلوك الامن السيبرياني SB	تامين الاجهزةS	(S20-S23)	Egelman & Peer, 2015
		توليد كلمة المرور C	C24- C28	
		الوعي الاستباقي A	A29-A32	
		التحديث U	U33-U34	

ثانياً- صدق وثبات اداة البحث

لقد تم اختبار صدق وثبات فقرات الاستبانة من خلال نتائج معامل الفا كرونباخ (Cronbach Alpha) وعن طريق البرنامج الاحصائي (SPSS.var23) ويبين الجدول (3) نتائج صدق وثبات اداة البحث والتي كانت جميعها تفوق القيمة المعيارية 0.70 وذلك وكما يأتي :

الجدول (3) نتائج اختبار صدق وثبات اداة البحث

ت	المتغيرات الرئيسة وابعادها	عدد الفقرات	معامل الفا كرونباخ (Cronbach Alpha)
.1	المعرفة الرقميةN	4	0.76
.2	الابتكار الرقميI	5	0.79
.3	الرؤية الرقميةV	5	0.75
.4	المشاركة والتعاونP	5	0.77
متغير القيادة الرقمية DL		19	0.92
.5	تأمين الجهازS	4	0.81
.6	انشاء كلمة المرورC	4	0.74
.7	الوعي الاستباقيA	4	0.74
.8	التحديثU	4	0.81
متغير سلوك الامن السيبراني SB		16	0.91

المصدر :اعداد الباحثين استناداً على مخرجات التحليل الاحصائي في برنامج SPSS.var23

ثالثاً –تحليل ابعاد متغير القيادة الرقمية وفقاً لإجابات العينة

لقد أظهر تحليل البيانات الخاصة باجابات عينة البحث على استمارة الاستبيان المتضمنة المقاييس الخاصة بمتغير القيادة الرقمية في البحث ما يأتي:

1. بلغ الوسط الحسابي لإجمالي متغير القيادة الرقمية (3.25) وهو أعلى من الوسط الفرضي على مساحة ميزان الاختبار البالغ (3) المعول عليه لتفحص مستويات استجابة أفراد العينة المبحوثة وبلغ الانحراف المعياري (0.58) وبأهمية نسبية(65%) .
2. جاء بُعد المعرفة الرقمية بالمرتبة الأولى من حيث الأهمية النسبية التي بلغت (67%) و بوسط حسابي قدره (3.35) وانحراف معياري قدره (0.64) وجاءت الابعاد الأخرى متسلسلة بالأهمية , إذ احتل بُعد الابتكار الرقمي المرتبة الثانية باهمية نسبية (65%) وبوسط حسابي مقداره (3.26) وبانحراف معياري يبلغ (0.67) وبُعد المشاركة والتعاون بالمرتبة الثالثة باهمية نسبية (65%) وبلغ الوسط الحسابي (3.20) والانحراف المعياري (0.65) في حين جاء بُعد الرؤية الرقمية بالمرتبة الرابعة باهمية نسبية (64%) وبوسط حسابي مقداره (3.18) وبانحراف معياري يبلغ (0.64) .
3. تشير النتائج اعلاه ان المصارف المبحوثة لديهماهتمام جيدبابعاد القيادة الرقميةمن حيث الاستفادة من المعرفة الرقمية المتوفرة لديهم وتشجيع انشطة الابتكار الرقمي مع التركيز على المشاركة والتعاون بين العاملين مع السعي الى الالتزام بالرؤية الرقمية التي تتبانها تلك المصارف, الامر يمكن لاداراتها الاستفادة من تلك الابعاد في تحسين الاجراءات التنظيمية بالشكل الذي يساهم في تعزيز اسس القيادة الرقمية فيها.

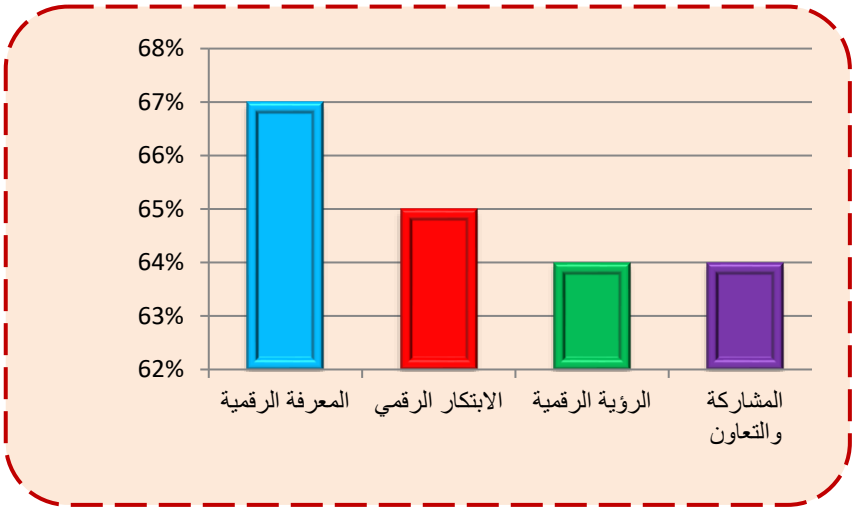
واستناداً على ما تقدم يمكن توضيح ترتيب الابعاد حسب الأهمية النسبية والوسط الحسابي والانحراف المعياري كما في الجدول(4)

الجدول(4) ترتيب ابعاد القيادة الرقمية حسب اهميتها

المتغيرات والابعاد	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية (شدة الإجابة)	الترتيب
المعرفة الرقميةN	3.35	0.64	0.67	الاول
الابتكار الرقميI	3.26	0.67	0.65	الثاني
الرؤية الرقميةV	3.18	0.64	0.64	الرابع
المشاركة والتعاونP	3.20	0.65	0.64	الثالث
اجماليمتغير القيادة الرقمية DL	3.25	0.58	0.65	

المصدر :اعداد الباحثين استناداً على مخرجات التحليل الاحصائي في برنامج SPSS.var23

ويصور الشكل (4) خلاصة النتائج لمتغير القيادة الرقمية والنسب المئوية لابعادها الأساسية.



الشكل (4) النسب المئوية لابعاد القيادة الرقمية حسب أهميتها

رابعاً– تحليل ابعاد سلوك الامن السيبراني وفقاً لإجابات العينة

لقد أظهر تحليل البيانات الخاصة باجابات عينة البحث على استمارة الاستبيان المتضمنة المقاييس الخاصة بابعاد سلوك الامن السيبرانيفي البحث ما يأتي :

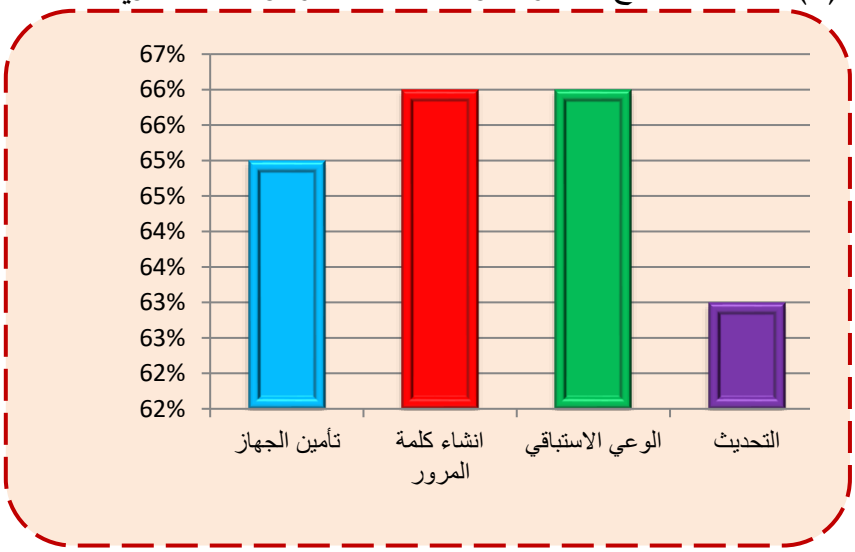
1. بلغ الوسط الحسابي لإجمالي مجال سلوك الامن السيبراني(**3.24**) وهو أعلى من الوسط الفرضي على مساحة ميزان الاختبار البالغ (3) ، المعول عليه لتفحص مستويات استجابة أفراد العينة المبحوثة و بانحراف معياري قدره (**0.59**) وأهمية نسبية(**65%**) .
2. جاء بُعد الوعي الاستباقي من حيث الأهمية النسبية ليحتل المرتبة الاولى بأهمية نسبية مقدارها (**66%**) وبوسط حسابي قدره (**3.29**) وبانحراف معياري مقداره (0.66) وجاءت الابعاد الأخرى متسلسلة بالأهمية , حيث احتل بُعد انشاء كلمة المرور بالمرتبة الثانية باهمية نسبية (**66%**) وبوسط حسابي مقداره (3.29) وبانحراف معياري مقداره(0.72), وبُعد تأمين الجهاز بالمرتبة الثالثة باهمية نسبية مقدارها (**65%**) وبلغ الوسط الحسابي (3.23) وبلغ الانحراف المعياري (0.71) في حين جاء بُعد التحديث بالمرتبة الرابعة باهمية نسبية (63%) وبوسط حسابي مقداره (3.17) وبانحراف معياري يبلغ (0.68) ..
3. تشير النتائج اعلاه ان المصارف المبحوثة تهتم بسلوك الامن السيبراني وذلك من خلال اهتمامها بتعزيز اساليب الوعي الاستباقي لمختلف الظروف المحيطة باعمال المصارف مع التأكيد على ضرورة الاهتمام بانشاء كلمة المرورة للحفاظ على معلومات الزبائن مع اهتمامها الجيد بتأمين اجهزتها المستخدمة في الانشطة المصرفية المتعددة لزيادة امن المعلومات وحسابات المشتركين مع ضرورة تحديثها بشكل متواصل, وظهر ذلك من خلال تقارب مقدار الاهمية النسبية لكل بعد من ابعاد متغير سلوك الامن السيبراني مع افضلية في اهمية الوعي الاستباقي, ويوضح الجدول (5) الاوساط الحسابية والانحرافات المعيارية الخاصة بابعاد سلوك الامن السيبراني.

الجدول(5)ترتيب الاهمية النسبية بين ابعادسلوك الامن السيبراني

المتغيرات والابعاد	الوسط الحسابي	الانحراف المعياري	الأهمية النسبية (شدة الإجابة)	الترتيب
تأمين الجهازS	3.23	0.71	0.65	الثالث
انشاء كلمة المرورC	3.29	0.72	0.66	الثاني
الوعي الاستباقيA	3.29	0.66	0.66	الاول
التحديثU	3.17	0.68	0.63	الرابع
اجماليمتغير سلوك الامن السيبراني SB	3.24	0.59	0.65	

المصدر :اعداد الباحثين استناداً على مخرجات التحليل الاحصائي في برنامج SPSS.var23

ويصور الشكل (5) خلاصة النتائج لمتغير سلوك الامن السيبرانيوالنسب المئوية لابعادها الأساسية.



الشكل (5) النسب المئوية لابعاد سلوك الامن السيبراني حسب أهميتها

خامساً –اختبار وتحليل فرضية علاقة الارتباط

استكمالاً للعمليات الوصفية والتشخيصية القائمة على معطيات التحليل الوصفي للمتغيرات، وانسجاماً مع أهداف البحث ، واختباراً لأنموذجها، تهدف هذه الفقرة إلى اختبار علاقات الارتباط في ضوء تساؤلات البحث حيث تم وضع عدد من الفرضيات لتحديد طبيعة العلاقة بين متغيرات نموذج البحث الفرضي , ولغرض التحقق من ذلك تم تصنيف وتبويب البيانات الواردة في استمارة الاستبيان لغرض تحليلها ومعالجتها وفق طرائق وأساليب إحصائية ملائمة مع الاعتماد على تحليل ارتباط بيرسون.

اختبار الفرضية الرئيسة الأولى :

- **الفرضية الرئيسة الاولى (H1):** توجد علاقة ارتباط ذات دلالة إحصائية بين القيادة الرقمية و سلوك الامن السيبراني.

تعبر معطيات الجدول (6) عن قبول الفرضية الرئيسة الاولى وذلك بوجود علاقة ارتباط موجبة بين القيادة الرقمية و سلوك الامن السيبراني على المستوى الكلي ، ويتضح من خلال المؤشرات التي تشير إلى وجود ارتباط

موجب على المستوى الكلي بمقدار (0.702) وبدلالة معنوية بمستوى (1%) , ومن ذلك نستنتج تحقق الفرضية الرئيسية الاولى.

الجدول (6) نتائج علاقات الارتباط بين متغير القيادة الرقمية وابعاده ومتغير سلوك الامن السيبراني

الفرضية الفرعية	نص الفرضية	مقدار علاقات الارتباط	النتيجة
الاولى	توجد هناك علاقة ارتباط موجبة احصائية بين المعرفة الرقمية وسلوك الامن السيبراني	0.710**	قبول الفرضية
الثانية	توجد هناك علاقة ارتباط موجبة احصائية بين الابتكار الرقمي وسلوك الامن السيبراني	0.689*	قبول الفرضية
الثالثة	توجد هناك علاقة ارتباط موجبة احصائية بين الرؤية الرقمية وسلوك الامن السيبراني	0.444**	قبول الفرضية
الرابعة	توجد هناك علاقة ارتباط موجبة احصائية بين المشاركة والتعاون وسلوك الامن السيبراني	0.662**	قبول الفرضية
الفرضية الرئيسة	توجد هناك علاقة ارتباط موجبة احصائية بين القيادة الرقمية وسلوك الامن السيبراني	0.702**	قبول الفرضية

(*) تعني الارتباط معنوي عند مستوى الدلالة (0.05= α) (**) تعني الارتباط معنوي عند مستوى الدلالة (0.01= α)

المصدر : من إعداد الباحثين وفقا لمخرجات التحليل الاحصائي في برنامج SPSS.var23

اختبار الفرضيات الفرعية لعلاقات الارتباط

لقد اشارت نتائج التحليل الاحصائي للفرضيات الفرعية على مستوى الابعاد بقبول الفرضية الفرعية الاولى وذلك بوجود علاقة ارتباط احصائية بين بُعد المعرفة الرقمية وسلوك الامن السيبراني بمقدار (0.710) وبدلالة معنوية بمستوى (1%) .

كما اشارت النتائج الى قبول الفرضية الفرعية الثانية بوجود علاقة ارتباط احصائية بُعد الابتكار الرقمي وسلوك الامن السيبراني بمقدار (0.689) وبدلالة معنوية بمستوى (5%).

كما اظهرت النتائج قبول الفرضية الفرعية الثالثة بوجود علاقة ارتباط احصائية بين بُعد الرؤية الرقمية وسلوك الامن السيبراني بمقدار (0.444) وبدلالة معنوية بمستوى (1%).

كما اوضحت النتائج قبول الفرضية الفرعية الرابعة بوجود علاقة ارتباط احصائية بين بُعد المشاركة والتعاون وسلوك الامن السيبراني بمقدار (0.662) وبدلالة معنوية بمستوى (1%).

سادساً- اختبار وتحليل فرضية علاقة التأثير

استكمالاً لاختبار أنموذج البحث وفرضياتها ، استلزم الأمر تحديد درجة تأثير القيادة الرقمية بأبعادها الاربعة في متغير سلوك الامن السيبراني ، وهذا ما جاء في الفرضية الرئيسة الثانية والتي تنص على (وجود علاقة تأثير ذو دلالة إحصائية للقيادة الرقمية في سلوك الامن السيبراني) وذلك على النحو الآتي :

اختبار الفرضية الرئيسة الثانية:

يتولى هذا المحور مهمة الكشف عن طبيعة التأثير الواردة في الفرضية الرئيسة الثانية التي تشير إلى وجود علاقة تأثير ذو دلالة إحصائية للقيادة الرقمية في سلوك الامن السيبراني, ولغرض اثبات قبول تلك الفرضية او رفضها لابد من معرفة نتائج تحليل اختبارات الانحدار البسيط لمتغيرات البحث على المستوى الكلي او على مستوى الابعاد الفرعية .

وبناءا على ما جاء من النتائج المبينة في الجدول (7) والتي تظهر نتيجة التأثير بين متغيرات البحث القيادة الرقمية و سلوك الامن السيبراني والتي اثبتت وجود تأثير معنوي بين متغيري البحث وذلك حسب نتيجة التحليل (P–Value=0.000) ، وقد بلغت قيمة (F) (66.221) التي تعد قيمة معنوية مقبولة عند مستوى معنوية (5%) ، كما ان القدرة التفسيرية لهذا الانموذج بلغت وفقاً لقيمة (R^2) والبالغة (0.49) ، وهذا يشير إلى ان متغير القيادة الرقمية يفسر ما قيمته (49%) من المتغير المستجيب والمتمثل بسلوك الامن السيبراني وعلى هذا الاساس فان هذا الامر يؤدي الى تحقق الفرضية الثانية على المستوى الكلي .

الجدول (7) نتائج فرضيات التأثير لمتغير القيادة الرقمية في سلوك الامن السيبراني

الفرضية الفرعية	نص الفرضية	قيمة معامل التحديد R^2	قيمة F	درجة التحليل Sig	النتيجة
الاولى	توجد هناك علاقة تأثير احصائية للمعرفة الرقمية في سلوك الامن السيبراني	0.50	69.027	0.000**	قبول الفرضية
الثانية	توجد هناك علاقة تأثير احصائية للابتكار الرقمي في سلوك الامن السيبراني	0.47	61.345	0.000**	قبول الفرضية
الثالثة	توجد هناك علاقة تأثير احصائية للرؤية الرقمية في سلوك الامن السيبراني	0.20	16.731	0.000**	قبول الفرضية
الرابعة	توجد هناك علاقة تأثير احصائية للمشاركة والتعاون في سلوك الامن السيبراني	0.44	53.109	0.000**	قبول الفرضية
الفرضية الرئيسة	توجد هناك علاقة تأثير احصائية للقيادة الرقمية في سلوك الامن السيبراني	0.49	66.221	0.000**	قبول الفرضية

المصدر: من إعداد الباحثين وفقا لمخرجات التحليل الاحصائي في برنامج SPSS.var23

اختبار الفرضيات الفرعية لعلاقات التأثير

لقد اشارت نتائج التحليل الاحصائي للفرضيات الفرعية على مستوى الابعاد بقبول الفرضية الفرعية الاولى وذلك بوجود علاقة تأثير احصائية لبُعد المعرفة الرقمية في سلوك الامن السيبراني حسب نتيجة التحليل (P–Value=0.000) ، وقد بلغت قيمة (F) (69.027) التي تعد قيمة معنوية مقبولة عند مستوى معنوية (5%) ، كما ان القدرة التفسيرية لهذا البُعد بلغت وفقاً لقيمة (R^2) والبالغة (0.50) ، وهذا يشير إلى ان بُعد المعرفة الرقميةيفسر ما قيمته (50%) من المتغير المستجيب والمتمثل بسلوك الامن السيبراني.

كما اوضحت النتائج الى قبول الفرضية الفرعية الثانية وذلك بوجود علاقة تأثير احصائية لبُعد الابتكار الرقمي في سلوك الامن السيبراني حسب نتيجة التحليل (P-Value=0.000) ، وقد بلغت قيمة (F) (61.345) التي تعد قيمة معنوية عند مستوى معنوية (5%) ، كما ان القدرة التفسيرية لهذا البُعد بلغت وفقاً لقيمة (R^2) والبالغة (0.47) ، وهذا يشير إلى ان بُعد الابتكار الرقمييفسر ما قيمته (47%) من المتغير المستجيب والمتمثل للقيادة بسلوك الامن السيبراني.

كما اظهرت النتائج قبول الفرضية الفرعية الثالثة بوجود علاقة تأثير احصائية لبُعد الرؤية الرقمية في سلوك الامن السيبراني حسب نتيجة التحليل (P-Value=0.000) ، وقد بلغت قيمة (F) (16.731) التي تعد قيمة معنوية عند مستوى معنوية (5%) ، كما ان القدرة التفسيرية لهذا البُعد بلغت وفقاً لقيمة (R^2) والبالغة (0.20) ، وهذا يشير إلى ان بُعد الرؤية الرقمية يفسر ما قيمته (20%) من المتغير المستجيب والمتمثل بسلوك الامن السيبراني.

كما اوضحت النتائج الى قبول الفرضية الفرعية الرابعة وذلك بوجود علاقة تأثير احصائية لبُعد المشاركة والتعاون في سلوك الامن السيبراني حسب نتيجة التحليل (P-Value=0.000) ، وقد بلغت قيمة (F) (53.109) التي تعد قيمة معنوية عند مستوى معنوية (5%) ، كما ان القدرة التفسيرية لهذا البُعد بلغت وفقاً لقيمة (R^2) والبالغة (0.44) ، وهذا يشير إلى ان بُعد المشاركة والتعاونيفسر ما قيمته (44%) من المتغير المستجيب والمتمثل للقيادة بسلوك الامن السيبراني.

المبحث الرابع :الاستنتاجات والتوصيات

اولاً-الاستنتاجات

1- تعد ممارسات القيادة الرقمية في المصارف المبحوثة أحد العوامل المساهمة في تحسين سلوك الامن السيبراني والتي يمكن من خلالها تحسين ادائها التنافسي.
2- ان المصارف المبحوثة لديها اهتمام مقبول بتطبيق اسس القيادة الرقمية من اجل مواكبة التغيرات المحيطة بها والعمل على تحسين واقع الاجراءات التنظيمية بما يعزز من سلوك الامن السيبراني.
3- ان المصارف المبحوثة تبدي استعداد في تبني سلوك الامن السيبراني في بيئة العمل من اجل تعزيز موقعها التنافسي.
4- ان المصارف المبحوثة تهتم بالمعرفة الرقمية بما يزيد من قدرتها في تحسين ادائها المصرفي.
5- تهتم المصارف المبحوثة بالابتكار الرقمي في بيئة العمل و هذا بدوره ينعكس على تحسين سلوك الامن السيبراني وتقديم الخدمات المصرفية بصورة مثلى.
6- تركز المصارف المبحوثة على المشاركة والتعاون من اجل تحسين ادائها المصرفي .
7- تهتم المصارف المبحوثة بالرؤية الرقمية بما ينسجم وقدرات المصارف في تطبيق الاساليب الرقمية الحديثة.

ثانياً-التوصيات

1- ضرورة اهتمام المصارف المبحوثة باختيار قياداتها وفق مواصفات خاصة والتي تمكنها من تطبيق اساليب القيادة الرقمية .

2- ينبغي على ادارة المصارف المبحوثة توفير الاجراءات التنظيمية والظروف المساهمة في تعزيز القدرة على تبني سلوك الامن السيبراني باتجاه تحقيق اهدافها.

3- ضرورة تحسين اساليب المعرفة الرقمية للمصارف المبحوثة المنسجمة مع امكانياتها في التعامل مع الظروف المتغيرة في بيئة الاعمال ومواكبتها من اجل تنشيط فاعلية ادائها المصرفي.

4- ينبغي وضع اجراءات تنظيمية تساهم في تطوير انشطة الابتكار الرقمي في جميع المستويات التنظيمية من خلال برامج التعلم والتدريب المستمر.

5- التأكيد على تعزيز اسس المشاركة والتعاون من اجل تقديم الخدمات المصرفية بشكل امثل ومواكبة التطورات الحاصلة في بيئة الاعمال والاستجابة لمتغيراتها.

6- ينبغي على المصارف المبحوثة العمل على تحديث الرؤية الرقمية بما ينسجم مع متغيرات العمل المصرفي .

7- ضرورة اعتماد الانشطة التي تدعم الحفاظ على معلومات العملاء في المصارف المبحوثة من خلال السعي لتعزيز سلوكيات الامن السيبراني واعتماد الادوات التقنية الحديثة

References

1. Antonopoulou, H., Halkiopoulos, C., Barlou, O., & Beligiannis, G. N. (2021). Associations between Traditional and Digital Leadership in Academic Environment: During the COVID-19 Pandemic.Emerging Science Journal, 5(4), 405-428
2. Conference on Software Engineering, 2003. Proceedings. (pp. 705-715.(
3. Data-driven cybersecurity incident prediction: A survey. IEEE Communications Surveys & Tutorials, 21(2), 1744-1772.
4. de Araujo, L. M., Priadana, S., Paramarta, V., & Sunarsi, D. (2021). Digital leadership in business organizations. International Journal of Educational Administration, Management, and Leadership, 45- 56.
5. Egelman, S., & Peer, E. (2015, April). Scaling the security wall: Developing a security behavior intentions scale (sebis). In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, p. 2979.
6. Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. Security and behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9(17), 4667-4679.
7. Goethal, G., Sorenson, G., & Burns , J. (2020), LEADERSHIP IN THE DIGITAL AGE.
8. Kemmerer, R. A. (2003, May). Cybersecurity. In 25th International

9. Lu, Y., & Da Xu, L. (2018). Internet of Things (IoT) cybersecurityresearch: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103-2115..
10. Middleton, John.(2002). Organizational Behavior, Capstone Publishing, London.
11. Miner,Johm,(2006). "Organizational Behavior from theory to practice", M.E sharpe published, Printed in the United States of America.
12. Mowbray, T. J. (2013). Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions. John Wiley & Sons.
13. Pancheva, S. (2018, Jul 09). The Challenges of Leadership in the Digital Era. Retrieved from Stratx-Exl: https://www.stratx-exl.com/industry-insights/thechallenges-of-leadership-in-the-digital-era
14. Rot A., & Sobinska M. (2020). Challenges for Knowledge Management in Digital Business Models. 2020 10th International Conference on Advanced Computer Information Technologies (ACIT).
15. Rüth, R., & Netzer, T. (2020). The key elements of cultural intelligence as a driver for digital leadership success. Leadership, Education, Personality: An Interdisciplinary Journal, 2(1), 3-8
16. Sheeran, P., & Orbell, S. (2000). Self-schemas and the theory of planned behaviour. European journal of social psychology, 30(4), 533-550.
17. Sheeran, P., & Webb, T. L. (2016). The intention–behavior gap. Social and personality psychology compass, 10(9), 503-518.
18. Sheninger , E. (2019). In Pillars of digital leadership .) PP 1-4). International Center for Leadership in Education.
19. Sinha, A., Nguyen, T. H., Kar, D., Brown, M., Tambe, M., & Jiang, A. X From physical security to cybersecurity. Journal of Cybersecurity(2015) 35-19,(1)1.
20. Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2018
21. Tanniru, M. R. (2018). Digital Leadership. In Management of Information Systems. IntechOpen.
22. Van Ee, J., El Attoti, I., Ravesteyn, P., & De Waal, B. M. (2020). BPM Maturity and Digital Leadership: An exploratory study. Communications of the IIMA, 18(1), 2
23. Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J.(2018)Cybersecurity for digital manufacturing. Journal of manufacturing.