Cybersecurity Gaps in Reflect of the Development of Suspicion-Specific Capabilities

Prof. Dr. Qais Abrahim Hussain, Ameer Jasim Hussain

University of Iraqia
College of Administration and Economics

فجوات الامن السيبراني في ظل تنمية القدرات المحددة للارتياب

أعداد

الأستاذ الدكتور قيس أبراهيم حسين الباحث أمير جاسم حسين

الجامعة العراقية، كلية الإدارة والاقتصاد، قسم إدارة الاعمال

[1]*Date of Receiving:04 August 2023;*
Date of Acceptance:23 September2023;
Date of Publication: 05 October 2023

ABSTRACT

The research aimed to test the effect of Technical Suspiciousness in cybersecurity with the effect of dimensions. For the purpose of completing the scientific picture of the research, the descriptive approach was adopted and data was collected by means of a questionnaire, which is the research standard. The research population was (105) a sample of civilian employees, ranks, and officers in the Directorate of Communications and Information Systems in the Ministry of The Ministry of Interior is in implementation, and to choose the research hypotheses, a set of statistical methods were adopted using the outputs of the statistical program (SPSS V25 and the AMOS program)). The research reached the most prominent result, which is the presence of an impact of technical Suspiciousness in the gap in the requirements for implementing cybersecurity technology in the Directorate of Communications and Information Systems in the Ministry of Interior. The Iraqi Ministry of Interior, according to the field of application of the research, has developed a number of recommendations and mechanisms that increase the directorate's ability to bridge the gap and reduce technical uncertainty.

Keywords: *Technical Suspiciousness; Cybersecurity*

المستخلص

[1] *How to cite the article:* Hussain Q.A., Hussain A.J.; (October 2023); Cybersecurity Gaps in Reflect of the Development of Suspicion-Specific Capabilities; *International Journal of Law, Management and Social Science*, Vol 7, Issue 4, 1-17

هدف البحث الى اختبار تأثير الارتياب التقني في الامن السيبراني بتأثير الابعاد ولغرض اكمال الصورة العلمية للبحث تم اعتماد المنهج الوصفي وجمع البيانات بوساطة الاستبانة التي تعد مقياس البحث حيث كان مجتمع البحث من (105) عينة من الموظفين المدنيين والمراتب والضباط في مديرية الاتصالات والنظم المعلوماتية في وزارة الداخلية قيد التطبيق، ولاختيار فرضيات البحث تم اعتماد مجموعة اساليب احصائية باستخدام مخرجات برنامج(SPSS V25) الاحصائي وبرنامج (AMOS) اذ توصل البحث الى ابرز نتيجة تمثل في وجود تاثير للارتياب التقني في فجوة متطلبات تطبيق تقنية الامن السيبراني في مديرية الاتصالات والنظم المعلوماتية في وزارة الداخلية العراقية وفق مجال تطبيق البحث، وقد وضع الباحث عدد من التوصيات والاليات التي تزيد من قدرة المديرية على تجسير الفجوة، وتقليل من الارتياب التقني.

الكلمات المفتاحية: الارتياب التقني، الامن السيبراني

المقدمة

يعد الارتياب في اصله سلوك متجذر في النفس الانسانية على مدى التتبع التاريخي للمصطلح وهو مؤثر جدلي في كل اوجه المنطلقات واساليب التفكير في جميع المجالات ، لاسيما الاقتصادية والادارية منها، وفي داخل المنظمة وخارجها ، اذ يكون ملازم للموظف العامل في مختلف مجالات الوظيفة ومؤثراً قوياً في اتخاذ القرار في جميع مستويات الادارة العليا والوسطى والدنيا ، لذلك تسعى المنظمات الرصينة الى اكتشاف بوادر الارتياب التقني في المنظمة قبل حدوثه خصوصاعندما يتوجه الى نشاط ما او وظيفة تقنية (N Metayer,E Jean Louis,2004:47)، ونتيجة لازدياد الرقمنة وتطور التكنولوجيا المعلوماتية المتسارع ، أضحت المنظمات متجهة الى إيجاد الامن المعلوماتي الرامي لحماية البيانات والحفاظ على سريتها، والحيلولة دون سرقتها او الاضرار بها ، فضلاً عن صد الهجمات السيبرانية ومكافحة الجرائم المرتبطة بها، والعمل على حماية الافراد والمنظمات والأنظمة ذات الصلة من حالات الاختراق والتهديدات الخطيرة، والتأثير في خصوصيتها والمحافظة على حساسيتها وإدارة العملية الإنتاجية والسير بها لشواطئ الأمان، لاسيما وان الصناعات الحديثة وبجميع أنواعها أصبحت اكثر ارتباط بتكنولوجيا المعلومات ، وعلى هذا الأساس واجه الامن المعلوماتي تحديات وتهديدات متنوعة ومتسارعة ، جعل من الواجب القيام بعمل مرتفع المستوى من الأنشطة التقنية الهادفة لحماية البيانات والمعلومات والمعدات التقنية من أي شكل من اشكال الوصول غير المصرح به.

المبحث الاول: منهجية البحث

أولا : مشكلة البحث

تشكل عملية دراسة وبحث وتحليل سلوكيات الموظفين في المنظمات الحديثة احدى مرتكزات ادارة الاعمال الناجحة لانها تؤدي الى تقليص دائرة الصراعات بين الموظفين ونشاطات المنظمة وهو مايؤثر على انتاجية المنظمة ومردودها الاقتصادي والثقافي لذلك تتركز مشكلة البحث في محاولة الاجابة على التساؤلات الاتية :

التساؤل الاول: ما مستوى تأثير الارتياب والارتياب التقني على اتخاذ القرار تجاه تقنية الامن السيبراني في مديرية الاتصالات والنظم المعلوماتية؟

التساؤل الثاني : هل يوجد تأثير لتطبيق تقنية الامن السيبراني مع وجود الارتياب التقني في مديرية الاتصالات والنظم المعلوماتية؟

ثانيا : اهمية البحث

ان اهمية البحث تتمحور في مايحمل من مادة علمية مؤثرة وناجعة على مستوى الجانب التطبيقي لتأثير الارتياب التقني في تقنية الامن السيبراني ومن خلال النقاط ادناه :

1- ان دراسة وتحليل الارتياب والارتياب التقني في المنظمة يقنن من المشاكل المتبادلة فيها.

2- يعطي هذا البحث نظرة جديدة لسلوك الارتياب التقني للموارد البشرية تجاه انشطة المنظمة بصورة عامة وتجاه الامن السيبراني بصورة خاصة.

3-تسليط الضوء على الاثار المهمة المترتبة من نتائج ممارسات الارتياب التقني في تقنية مهمة جدا وفتية في مديرية الاتصالات والنظم المعلوماتية وامكانية تصميم النتائج على مستوى الوزارات الاخرى.

الثا: اهداف البحث

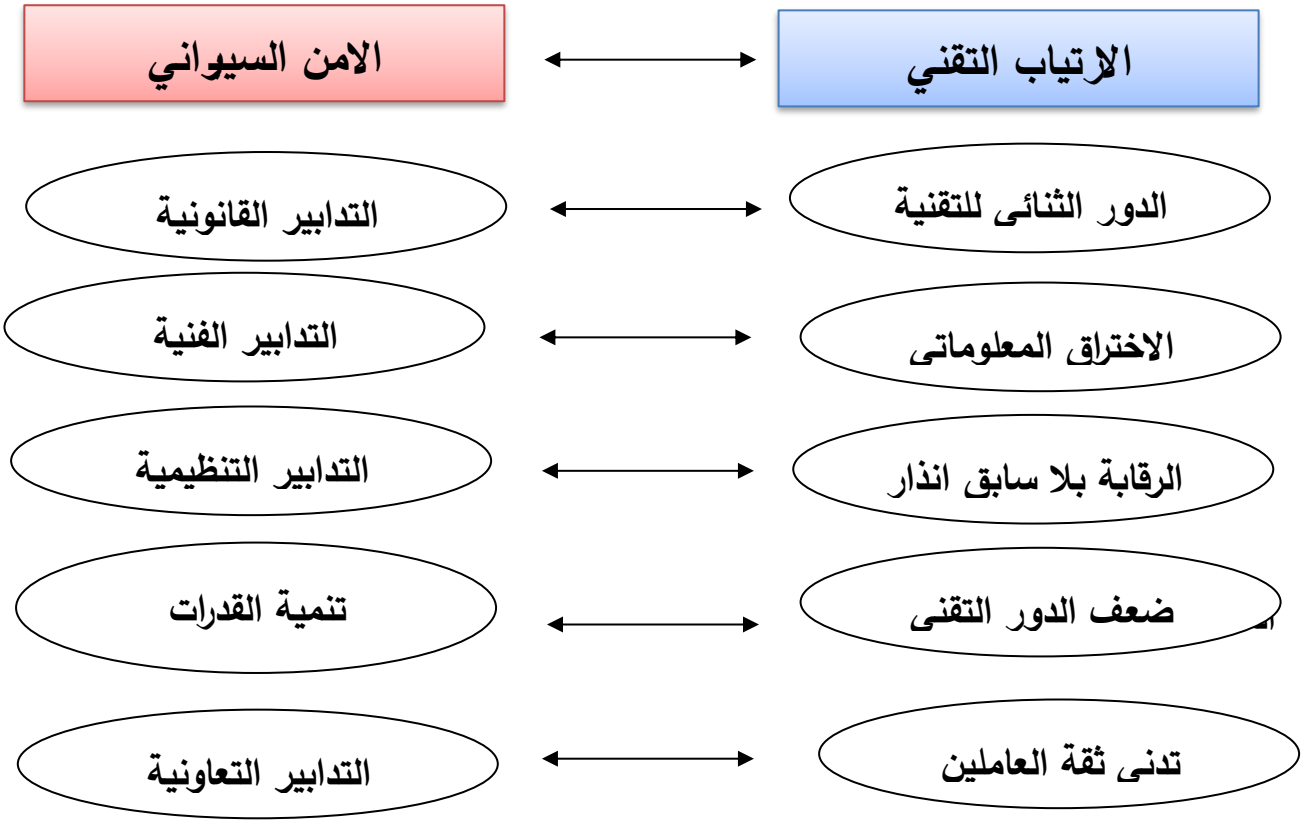
يهدف البحث الى كشف وتحليل عن تأثير الارتياب التقني في تقنية الامن السيبراني وفق معيار (GCI V4) ويمكن تحديد مكامن التأثير فيما يأتي :

1- تحديد تأثير سلوك الارتياب التقني في الامن السيبراني وفق معيار (GCI V4) في ضوء اجابات عينة الدراسة.

2- تحديد تأثير الارتياب التقني والامن السيبراني وعلاقتهما في مديرية الاتصالات والنظم المعلوماتية في وزارة الداخلية قيد البحث.

رابعا: انموذج البحث وفرضياته

يوضح الشكل (1) انموذج البحث والذي يبين علاقة تأثير المتغير المستقل وابعاده في المتغير



الشكل (1) الأنموذج الفرضي للبحث أعداد الباحثان

ومن اجل تحقيق اهداف البحث واختبار الانموذج الفرضي قد تم صياغة مجموعة فرضيات رئيسة وكما ياتي:

1- الفرضية الرئيسة (H01): لا توجد علاقة ارتباط ذو دلالة معنوية مابين الارتياب التقني وفجوة الامن السيبراني على وفق متطلبات المعيار (GCI V4).

2- الفرضية الرئيسة الثانية (H02) : لا يوجد تأثير ذو دلالة معنوية للارتياب التقني في فجوة الامن السيبراني وفق متطلبات المعيار (GCI V4).

خامسا: مجتمع وعينة البحث

اختار الباحث (مديرية الاتصالات والنظم المعلوماتية في وزارة الداخلية) في بغداد بيئة للبحث والدراسة وتم توزيع الاستبانة على عينة البحث البالغة (105) موظف.

المبحث الثاني : الجانب النظري

اولا: سلوكيات الارتياب التقني

1- مفهوم الارتياب التقني: ان الارتياب بحد ذاته هو بناء معرفي داخلي ويعتبر جزء حيوي لا يتجزأ من ادراك المحسوسات والملموسات في تشخيص الاشياء داخليا وخارجيا, اما في مجال علوم ادارة الاعمال والمنظمات فالارتياب يعطي فهم اخر لارتباطه بنشاطات المنظمة ووظائفها فهو يتناسب عكسيا مع البيئة المحيطة فكلما انخفضت نسبة الارتياب ازدادت نسبة الثقة بانظمة وتقنيات ووظائف المنظمة مثل تقنية الامن السيبراني قيد البحث ويرى الباحثان ان مفهوم سلوكيات الارتياب لتقني تمثل سلوك داخلي يعمل على تشخيص وتحليل وتحقيق التعامل مع متطلبات اتخاذ القرار داخل المنظمة.(I Ja Suntana and Others,2023:2)

2- اهمية الارتياب التقني: من وجهة نظر (JB McComic and Others,2023:3) يعد تحليل ومراقبة الارتياب لدى الموظفين في المنظمة يشكل اهمية كبيرة لدى الادارة العليا والوسطى وحتى المرؤوسين,

ويساعدهم في تشخيص المشاكل والصراعات في المنظمة والموظفين ويمكن تلخيص بعض النقاط المهمة وهي كالاتي:

ا- يمثل سلوك الارتياب والارتياب التقني لدى الموظفين حاجز مهم في مسار العمل.

ب- تؤدي مراقبة الارتياب التقني والسيطرة عليه الى زيادة الثقة لدى الموظفين.

ت- تؤدي انخفاض مستويات الارتياب التقني الى ارتفاع التفاعل مع التقنيات المختلفة المستخدمة في المنظمة.

ث- تؤدي السيطرة على معدلات الارتياب التقني لدى الموظفين في المنظمة الى زيادة الانتاجية والجودة وتحصين المنظمة من التهديدات الخارجية والداخلية.

ثانيا: الامن السيبراني

1- **مفهوم الامن السيبراني:** يقصد بالامن السيبراني هو حماية قواعد البيانات الحساسة لكل منظمة بهدف صد كل الاختراقات والهجمات والاستخدام غير الامثل للبيانات وسائر العمليات الانتاجية بهدف حماية الاقتصاد القومي وتحقيق ادارة ناجحة. (شويرب،جيلالي،165:2023) كما انه يمثل الهدف في تعزيز قدرة الدول على تهيئة ودعم بيانات خالية من اي اثار سلبية موجهة نحو بيئة المنظمة على مستوى الشبكات المغلقة والمفتوحة وحماية الأتساق بين الشبكات الانتاجية والاليات والتقنيات الحديثة من اجل تغيير معايير وتوازنات قوية لا تهدد السلم والامن الاقتصادي (جمال الدين،191:2023).

2- **اهمية الامن السيبراني:** لم تعد قافية اهمية الامن السيبراني سيما وهو اصبح احد الضروريات الحساسة في حياتنا اليومية ويمكن تلخيص بعض النقاط كالاتي:

ا- يمثل الامن السيبراني عنصر مهم واساسي في حياة المورد البشري في داخل المنظمة وخارجها.

ب- يمثل الامن السيبراني جدار الصد الاول في المنظمة لحماية البيانات والعمليات الانتاجية.

ت- يمثل الامن السيبراني ثورة فتية في عالم المنظمة الحديثة وسلوك الموظفين.

ث- يعزز الامن السيبراني الامان الرقمي في المنظمة.

ج- يحسن الامن السيبراني الممارسات والسلوكيات للموظفين في المنظمة داخليا وخارجيا.

(ال حماده،2705:2023).

3- أبعاد الامن السيبراني:

أ- التدابير القانونية: ان استخدام الانترنت ادى الى زيادة المساحة الرقمية العالمية وتقلص المساحة التفاعلية الاجتماعية اذ بلغ مستخدمي محركات الانترنت في العالم 4,9 مليار مشترك وبنسبة 63% من سكان العالم وهذا يؤدي الى ظهور جريمة الكترونية وتطفل وتصيد واستخدام غير مرخص به لملايين الخصوصيات الفردية والجماعية للموارد البشرية والمنظمات والمصارف ومراكز القرار الحاسم مما دفع اصحاب المصلحة والقرار الى تشريع قوانين ولوائح تهذب استخدام الحاسوب ومحركات الانترنت.(زيدان،72:2023)

ب- التدابير الفنية: ان التطور الحاصل في تقنية الامن السيبراني والذي سوف يحصل انما مرتبط ارتباط مباشر بتطور انماط حياة الانسان فكلما تطورت الجريمةالالكترونية تطورت وسائل واساليب كبحها ويالها من مسابقة مخيفة بحيث ارتبطت الجريمة بالوعي الالكتروني الافتراضي لمستخدمين الانترنت كما وضح مؤشر الامن السيبراني (GCI V4) الصادر عن الاتحاد الدولي للاتصالات حيث اعلن عن حصول مصر المركز 23 عالميا من بين 182 دولة بينما تصدرت امريكا 100 بعدها بريطانيا في مجال دعم الامن السيبراني. (صالح,2023 :812)

ت- التدابير التنظيمية: ان القيام بانشطة الكترونية بطريقة امنة يحتاج الى فضاء سيبراني امن قائم على اساس دعامة قوية تكبح التهديدات والاستخدام غير الامن وهذا يتم عن طريق بناء مغلق كليا للانظمة الفرعية لكل منظمة قائمة على اساس مردود اقتصادي واداري من اجل تحقيق اهداف المنظمة والتحضير لرؤيا واضحة ورسالة واعدة في حماية الموظف والمنظمة في ان واحد. (الهام علي سيد احمد عبدالله, 2023: 7).

ث- تنمية القدرات: تسعى الكثير من الدول والمنظمات للحصول على السيادة السيبرانية في عصر التطور والسرعة والمنافسة وانظمة الاتمتة الحديثة ولاتوجد منظمة بدون قدرات سيبرانية وبالتالي فان بناء سد سيبراني قوي لاي منظمة يعود عليها بإنتاجية مستدامة كما هو الحال في شركات العالم المسيطرة على السوق وبالخصوص سوق الهواتف المحمولة والبرمجيات الالكترونية الحساسة مثل شركة ايفون وشركة غالاكسي كنموذجين متسابقين. (شرايطية،2020 : 396)

ج- الاختراق المعلوماتي: ان اهم العوامل التي ساعدت على تنمية ودعم خصوصيات رقمنة الامن السيبراني في المنظمات والموظفين هو ظهور جائحة كورونا وبروز انماط تنظيمية جديدة وكانت النتائج اجابية بدل ان تكون سلبية بسبب التحشدات القوية لهذه الجائحة العابرة للقارات من خلال صناعة بيئة ريادة اعمال ناجحة وتقديم حلةل تقنية ناجعة لدعم تلك البيئة مما أدى الى توسع ورصانة وقوة الأمن السيبراني وأنخفاض مؤشرات الأختراق الأفتراضي والتصيد والأستخدام غير المرخص به.(بن زرارة وأخرون،60:2023)

المبحث الثالث: الجانب التطبيقي

اولا-الثبات بالاعتماد على قيم معامل الفاكرونباخ

يشير مفهوم الثبات بالعموم الحصول على نفس النتائج تقريبا في حالة تكرار توزيع المقياس مرة أخرى , بعد فترة زمنية معينه ويستعمل في ذلك معامل (الفاكرونباخ) الذي يجب ان تكون قيمته اكبر او تساوي (0.70) كي تعد مقبولة , اذ يتضح من الجدول (1) ان جميع قيم معامل (الفاكرونباخ) المستخرجة هي اكبر من المعيار الموضوع وعليه تعد جيدة أي ان المقاييس المستخدمة في الدراسة لديها ثبات جيد

الجدول (1) " نتائج معامل ألفا كرونباخ "

متغيرات وابعاد البحث	معامل ألفا كرونباخ	المعيار	القرار
الدور الثنائي للتقنية	0.893	اكبر او تساوي 0.70	ثبات جيد
الاختراق المعلوماتي	0.889		ثبات جيد
الرقابة بلا سابق انذار	0.911		ثبات جيد
ضعف الدور التقني	0.896		ثبات جيد
تدني ثقة العاملين بالتقنية	0.908		ثبات جيد
الارتياب التقني	0.918		ثبات جيد
التدابير القانونية	0.811		ثبات جيد
التدابير الفنية	0.823		ثبات جيد
التدابير التنظيمية	0.778		ثبات جيد
تنمية القدرات	0.795		ثبات جيد
التدابير التعاونية	0.9		ثبات جيد
فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4	0.857		ثبات جيد

المصدر : مخرجات برنامج SPSS V.25

ثانيا–اختبار (التجزئة النصفية)

للزيادة في التأكد من ان المقياس المستخدم يتمتع بثبات جيد لجاء الباحث الى الاعتماد على اختبار التجزئة النصفية، اذ عند تطبيق هذه الطريقة وجد أن معامل (Spearman-Brown) للاستبانة بلغ (0.895), اما معامل التجزئة النصفة للاستبانة باستخدام معامل Guttman فقد بلغ(0.891) مما يعني أنها بمقاييسها المختلفة ذات ثبات جيد ,و يمكن اعتمادها في أوقات مختلفة.

الجدول(2) اختبار التجزئة النصفية

Cronbach's Alpha	Part 1	Value	0.953
		N of Items	34
	Part 2	Value	0.932
		N of Items	34
	Total N of Items		68
Correlation Between Forms			0.810
Spearman-Brown Coefficient	Equal Length		0.895
	Unequal Length		0.895
Guttman Split-Half Coefficient			0.891

ألمصدر : برنامج SPSS V.25

ثالثا – التحليل الوصفي لمتغيرات البحث

1–متغير الارتياب التقني

يوضح الجدول (3) والشكل (2) نتائج التحليل الوصفي لأبعاد متغير الارتياب التقني وكما يلي :

- أجمالاً فقد حقق **متغير الارتياب التقني** وسطا حسابيا بلغ قيمته (3.410) وبمستوى متوسط وبانحراف معياري (0.614) ومعامل اختلاف بلغ (18.01), إذ بلغت نسبة توفر هذا المتغير (68.2%) اما حجم الفجوة فقد بلغت النسبة (31.8%) مما يدل على قلة تشتت اجابات العينة وتأكيدهم على اهمية متغير **الارتياب التقني** , اذ حالة تلازم العاملين نتيجة للاستخدام السلبي للتقنية، حيث يعانون من ازدواجية في تصرفاتهم وممارسة أدوار رقابية غير معلنة. يرتبط هذا بحالات الاختراق المعلوماتي الناجمة عن ضعف في التنظيم التقني، مما يؤدي إلى ظهور نقاط ضعف في الأمن وغياب الثقة. اذ ينبغي تعزيز التنظيم والتأكد من وجود سياسات وإجراءات فعالة للأمن المعلوماتي والحماية من الاختراقات. يشمل ذلك التدريب المستمر للعاملين على ممارسات أمن المعلومات وتحديث الأنظمة والبرامج للحفاظ على مستوى عالٍ من

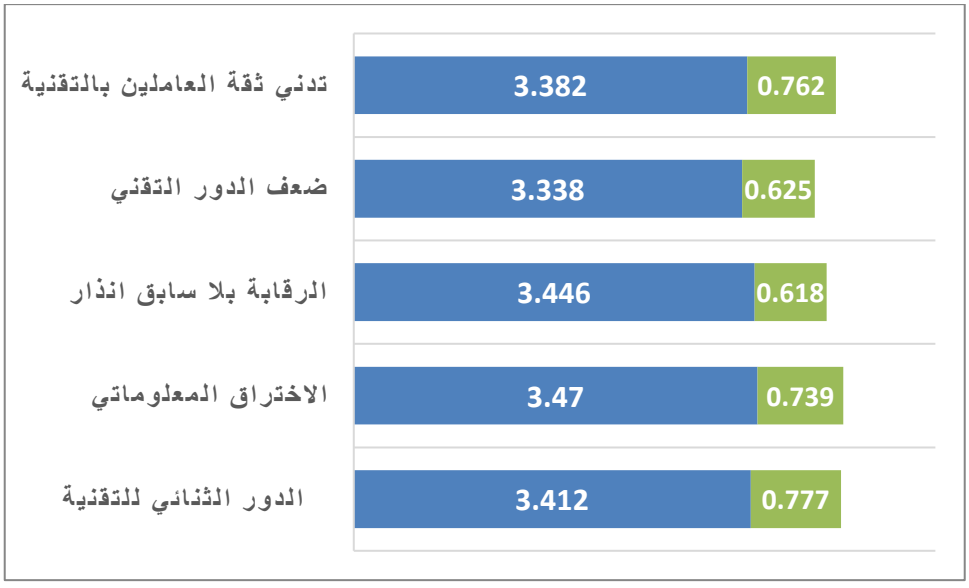
الأمان و تعزيز التوعية بأهمية الأمن والحفاظ على البيانات الحساسة. يمكن توفير برامج تدريبية للعاملين حول مفاهيم الأمان والمخاطر التقنية وكيفية التعامل معها بشكل فعال.

- بينت النتائج ان اعلى (وسط حسابيٍ) أجماليْ كان عند بعد(**الاختراق المعلوماتي**) إذ بلغ (3.470) وبمستوى (**متوسط**) بانحراف معياري بلغ (0.739) ومعامل اختلاف بلغ (21.3), إذ بلغت نسبة توفر هذا البعد (69.4%) اما حجم الفجوة فقد بلغت النسبة (30.6%), إذ جاء هذا البعد بالترتيب (**الثالث**) من حيث الاهمية النسبية لأبعاد **متغير متغير الارتياب التقني**. اذ يشير ذلك انه يمكن أن يشمل ذلك الوصول غير المصرح به إلى أنظمة الكمبيوتر أو قراءة ونسخ الملفات الشخصية أو القيام بعمليات التجسس الإلكتروني. اذ ان تأثير الاختراق المعلوماتي يكون سلبيًا بشكل كبير، حيث ينتهك خصوصية الأفراد ويعرض معلوماتهم الحساسة للمخاطر. يمكن أن يتسبب في الإضرار بالسمعة الشخصية والمهنية، والإلحاق الضرر بالمديرية والأعمال التجارية، وسرقة الهوية واستخدامها في أنشطة غير قانونية
- كما بينت النتائج ان اقل (وسط حسابيٍ) أجماليْ كان عند (**ضعف الدور التقني**) إذ بلغ (3.338) وبمستوى (**متوسط**) بانحراف معياري بلغ (0.625) ومعامل اختلاف بلغ (18.72) إذ بلغت نسبة توفر هذا البعد (66.8%) اما حجم الفجوة فقد بلغت النسبة (33.2%) إذ جاء هذا البعد بالترتيب (**الثاني**) من حيث الاهمية النسبية لأبعاد **متغير الارتياب التقني** وتشير النتائج الى ان قد يكون هناك نقص في التعليم والمعرفة التقنية للأفراد، مما يحد من قدرتهم على فهم وتطبيق التقنية في حل المشكلات , اضافة الى انه قد بكون هناك قلة في الوعي التقني للأفراد، حيث قد يكونون غير مدركين للتكنولوجيا المتقدمة وتطوراتها الحديثة، مما يؤثر على قدرتهم على الاستفادة منها في حياتهم اليومية القلق اضافة الى مقاومة بعض العاملين للتغيير اذ قد يعاني البعض من قلق أو مقاومة للتغيير التقني، مما يمنعهم من استكشاف وتجربة التطبيقات والحلول التقنية الجديدة.
- استطاع بعد (**الرقابة بلا سابق انذار**) ان يحتل المرتبة(الاولى) من حيث المفاضلة بالأبعاد الاخرى لمتغير **متغير الارتياب التقني**

الجدول (3) نتائج التحليل الوصفي لأبعاد متغير الارتياب التقني

ت	ابعاد متغير الارتياب التقني	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	نسبة الاتفاق	نسبة عدم الاتفاق	T	SIG	ترتيب الابعاد
1	الدور الثنائي للتقنية	3.412	0.777	22.77	68.2	31.8	0.154	0.878	5
2	الاختراق المعلوماتي	3.470	0.739	21.3	69.4	30.6	0.948	0.346	3
3	الرقابة بلا سابق انذار	3.446	0.618	17.93	68.9	31.1	0.744	0.459	1
4	ضعف الدور التقني	3.338	0.625	18.72	66.8	33.2	-0.993	0.323	2
5	تدني ثقة العاملين بالتقنية	3.382	0.762	22.53	67.6	32.4	-0.236	0.814	4
	متغير الارتياب التقني	3.410	0.614	18.01	68.2	31.8	0.156	0.876	

المصدر : برنامج SPSS V.25



الشكل (2) الوسط والانحراف لأبعاد متغير الارتياب التقني

2-متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4

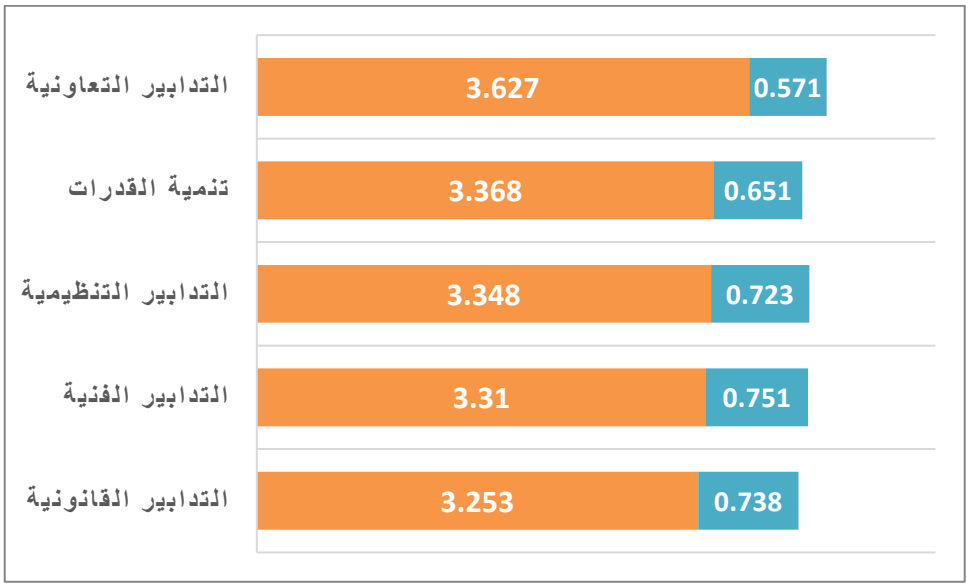
يوضح الجدول (3) والشكل (2) نتائج التحليل الوصفي لأبعاد متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4 وكما يلي :

- اما أجمالاً فقد حقق متغير **فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4** وسطا حسابيا بلغ قيمته (3.381) وبمستوى متوسط وبانحراف معياري (0.550) ومعامل اختلاف بلغ (16.27), إذ بلغت نسبة توفر هذا المتغير (67.6%) اما حجم الفجوة فقد بلغت النسبة (32.4%) مما يدل على قلة تشتت اجابات العينة وتأكيدهم على اهمية **متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4** , اذ ان فجوة الأمن السيبراني يشمل مجموعة من التدابير لحماية الأنظمة والشبكات الإلكترونية والبيانات من التهديدات السيبرانية. ويتضمن الأمن السيبراني التدابير القانونية التدابير الفنية, التدابير التنظيمية, تنمية القدرات, التدابير التعاونية
- بينت النتائج ان اعلى (وسط حسابيٍ) أجماليْ كان عند بعد(**التدابير التعاونية**) إذ بلغ (3.627) وبمستوى (**جيد**) بانحراف معياري بلغ (0.571) ومعامل اختلاف بلغ (15.743), إذ بلغت نسبة توفر هذا البعد (72.5%) اما حجم الفجوة فقد بلغت النسبة (27.5%), إذ جاء هذا البعد بالترتيب (**الاول**) من حيث الاهمية النسبية لأبعاد **متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4.**
- كما بينت النتائج ان اقل (وسط حسابيٍ) أجماليْ كان عند (**التدابير القانونية**) إذ بلغ (3.253) وبمستوى (**متوسط**) بانحراف معياري بلغ (0.738) ومعامل اختلاف بلغ (22.687) إذ بلغت نسبة توفر هذا البعد (65.1%) اما حجم الفجوة فقد بلغت النسبة (34.9%) إذ جاء هذا البعد بالترتيب (**الرابع**) من حيث الاهمية النسبية لأبعاد **متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4**
- استطاع بعد (**التدابير التعاونية**) ان يحتل المرتبة(الاولى) من حيث المفاضلة بالأبعاد الاخرى لمتغير **متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4** .

الجدول (4) نتائج التحليل الوصفي لأبعاد متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4

ت	ابعاد متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4	الوسط الحسابي	الانحراف المعياري	معامل الاختلاف	نسبة الاتفاق	نسبة عدم الاتفاق	T	SIG	ترتيب الابعاد
1	التدابير القانونية	3.253	0.738	22.687	65.1	34.9	-1.995	0.049	4
2	التدابير الفنية	3.310	0.751	22.689	66.2	33.8	-1.198	0.234	5
3	التدابير التنظيمية	3.348	0.723	21.595	67.0	33.1	-0.726	0.469	3
4	تنمية القدرات	3.368	0.651	19.329	67.4	32.6	-0.489	0.626	2
5	التدابير التعاونية	3.627	0.571	15.743	72.5	27.5	3.975	0.000	1
	متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4	3.381	0.550	16.27	67.6	32.4	-0.343	0.732	

المصدر: برنامج SPSS V.25



الشكل (3) الوسط والانحراف لأبعاد متغير فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4

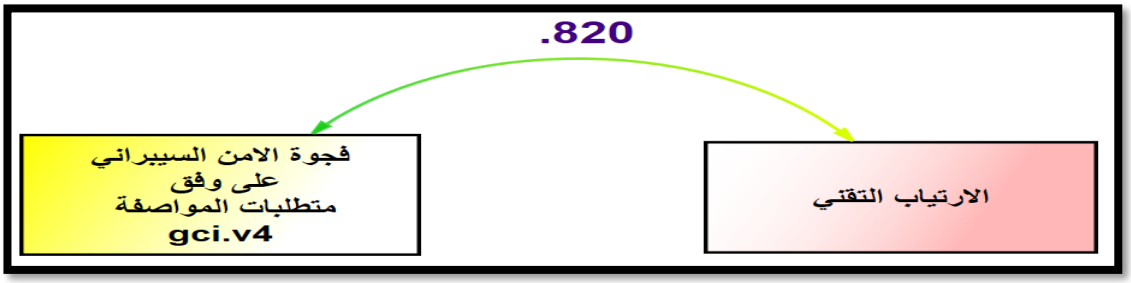
المصدر : مخرجات Excel

رابعاً – اختبار فرضيات البحث

1- الفرضية الرئيسية (الاولى)

(لا توجد علاقة ارتباط ذو دلالة معنوية ما بين الارتياب التقني و فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4)

بلغ معامل الارتباط بين **الارتياب التقني و فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4** (0.820) عند مستوى دلالة (0.000) وهي اقل من مستوى الدلالة(0.05) , اذ بلغت قيمة (Z) المحسوبة (11.393) وهي اكبر من قيمة (Z) الجدولية البالغة (1.96) وتدل هذه النتيجة الى معنوية قيمة الارتباط , اذ جاءت بمستوى قوية , وهذا يعني قبول الفرضية البديلة والتي تنص على (**توجد علاقة ارتباط ذات دلالة معنوية ما بين الارتياب التقني و فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4)**



الشكل (4) قيم الارتباط بين ابعاد الارتياب التقني وفجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4

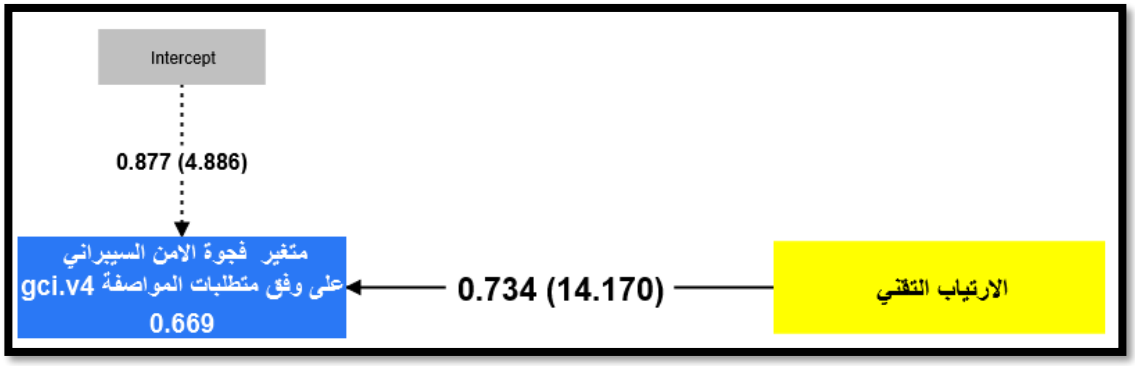
2 – الفرضية الرئيسية (الثانية)

(لا يوجد تأثير ذو دلالة معنوية الارتياب التقني في فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4)

فجوة الامن السيبراني على وفق متطلبات المواصفةgci.v4) 0.734 +0.877 =الارتياب التقني(

اذ يوضح الجدول (4) والشكل (4) نتائج تحليل الأثر بين **الارتياب التقني في فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4** , اذ حققت (F) المستخرجة ما قيمته (200.785) اذ تشير هذه النتيجة الى وجود تأثير معنوي بينها ,كما يظهر من قيمة (t) المستخرجة والبالغة (14.170) ان تأثير المعلمة (β) هو تأثير حقيقي حيث ان زيادة التأثير بمقدار الوحدة الواحدة سيؤدي الى زيادة **فجوة الامن**

السـيبراني على وفق متطلبات المواصـفة gci.v4 بمقدار (73 %) اذ ان حجم الأثر بلغ (1.417) وهو بمستوى (كبير) ,اذ استطاع متغير **الارتياب التقني** من تفسير ما نسبة (66%) من التغيرات التي تطرأ على **فجوة الامن السـيبراني على وفق متطلبات المواصـفة gci.v4**. وفي ضـوء ما تقدم نقبل الفرضـية البديلة ونرفض فرضـية العدم أي (**يوجد تأثير ذو دلالة معنوية لمتغير الارتياب التقني في فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4)**



الشكل (5) تحليل اثر الارتياب التقني في فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4

الجدول (5) تحليل اثر ابعاد الارتياب التقني في فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4

المتغير المعتمد	ابعاد متغير الارتياب التقني		(R)	(R^2)	(R^2) Adj	(F)	(t)	(Z)	حجم الاثر	قوة الاثر	Sig	القرار
فجوة الامن السيبراني على وفق متطلبات المواصفة gci.v4	الدور الثاني للتقنية	(α)	0.788	0.621	.6170	160.737	12.678	10.500	1.2678	كبيرة	0.000	قبول الفرضية البديلة
		(β)	1.477									
	الاختراق المعلوماتي	(α)	0.735	0.540	0.535	114.979	10.723	9.253	1.0723	كبيرة	0.000	قبول الفرضية البديلة
		(β)	1.482									
	الرقابة بلا سابق انذار	(α)	0.674	0.454	0.449	81.530	9.029	8.057	0.9029	كبيرة	0.000	قبول الفرضية البديلة
		(β)	1.314									
	ضعف الدور التقني	(α)	0.702	0.493	0.488	95.203	9.757	8.581	0.9757	كبيرة	0.000	قبول الفرضية البديلة
		(β)	1.317									
	تدني ثقة العاملين بالتقنية	(α)	0.665	0.443	0.437	77.796	8.820	7.896	0.882	كبيرة	0.000	قبول الفرضية البديلة
		(β)	1.757									
	الارتياب التقني	(α)	0.820	0.672	0.669	200.785	14.170	11.393	1.417	كبيرة	0.000	قبول الفرضية البديلة
		(β)	0.877									
			0.734									

المبحث الرابع: الاستنتاجات والتوصيات

اولا:الاستنتاجات

خصص هذا الجزء لعرض اهم الاستنتاجات المشتقة من الجانب التطبيقي وهي كالاتي:

1- اظهرت نتائج البحث في المديرية عينة البحث تأثير الارتياب التقني في فجوة الامن السيبراني وهذا مؤشر على تفاعل الموظفين مع تقنية الامن السيبراني بمعزل عن بعض الحواجز التي تتعلق بتنمية قدراتهم ومهاراتهم والاختراق المعلوماتي وبعض التدابير الفنية.

2- تمثل تقنية الامن السيبراني للموظفين داخل المنظمة وخارجها جدار صد ضد الاختراقات الافتراضية والتي تزيد من مؤشر الارتياب التقني.

3- ممكن دعم وتطوير تقنية الامن السيبراني لما يحقق من رفد مؤشر جودة الانتاجية في حال وضع في دائرة مغلقة وتم مواكبته مع التطور المتسارع تحت مظلة العالمية.

ثانيا: التوصيات

من خلال الاستنتاجات التي تم التوصل اليها فان الباحثان يوصيان مديرية الاتصالات والنظم المعلوماتية في وزارة الداخلية العراقية ماياتي:

1- الاهتمام بالمراقبة المبكرة لمؤشرات الارتياب التقني لدى الموظفين العاملين في المنظمة.

2- توفير قسم خاص بالتدريب والتأهيل في مجال الامن السيبراني حصرا ويكون ضمن مساحة مغلقة, ويكون مغلقا افتراضيا واداريا من اجل رفع مستويات المهارة والكفاءة لدى الموظفين.

3- رفد الجامعات والمعاهد بتخصص الامن السيبراني على مستوى الدراسات العليا والمهنية ليصبح ثقافة سائدة مثل ثقافة الاسعافات الاولية.

المصادر

أولا: المصادر العربية

- بن زرارة, أمينة, أعراب, & فطيمة. (2023). الحلول الرقمية الابتكارية في مجال حماية الهوية و الخصوصية والأمن السيبراني خلال جائحة كوفيد-19. مجلة رقمنة للدراسات الإعلامية والاتصالية, 3(1), 58-66.
- جمال الدين, هـ. (2023). الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية, 24(1), 189-230.
- د. الهام علي سيد أحمد عبد الله. (2023). مراجعة شاملة للأدبيات: كشف الفروق والتقاطعات بين أمن المعلومات والأمن السيبراني: د. الهام علي سيد أحمد عبد الله. مجلة مركز جزيرة العرب للبحوث التربوية والإنسانية, 1(2), 1-21.
- د. مسعد عبدالرحمن زيدان قاسم زيدان. (2023). الجرائم السيبرانية وآثارها على الأمن المجتمعى فى ضوء القانون الدولى العام.
- شرايطية. (2020). السيادة السيبرانية في الصين بين متطلبات القوة وضروريات الأمن القومي.

ثانيا: المصادر الأجنبية

- McCormick, J. B., Hopkins, M., Lehman, E. B., & Green, M. J. (2023). Political views and organizational distrust affect rural residents' willingness to share personal data for COVID-19 contact tracing: A cross-sectional survey study. *Journal of Clinical and Translational Science*, *7*(1), e91.
- Metayer, N., Jean-Louis, E., & Madison, A. (2004). Overcoming Historical and Institutional Distrust. *Ethnicity & Disease*, *14*, 46-52.
- Xue, J., Deng, Z., Wu, T., & Chen, Z. (2023). Patient distrust toward doctors in online health communities: integrating distrust construct model and social-technical systems theory. *Information Technology & People*, *36*(4), 1414-1438.