حوليات آداب عين شمس المجلد 51 (عدد يوليو – سبتمبر 2023)
http://www.aafu.journals.ekb.eg
(دورية علمية محكمة)
جامعة عين شمس
كلية الآداب

التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت

د/ خالد مخلف الجنفاوي*

عقيد دكتور/ أستاذ مشارك علم الاجتماع والجريمة/ أكاديمية سعدالعبدالله للعلوم الأمنية بالكويت
K_jnfaw173@hotmail.com

تاريخ الاستلام: 2021/06/15
تاريخ قبول البحث: 2021/08/01
تاريخ النشر: 2023/09/30

المستخلص:

هدفت هذه الدراسة إلى تسليط الضوء حول التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني في الكويت وذلك من وجهة نظر عينة من ضباط الشرطة الأكاديميين. وتم الاستفادة من المنهج الوصفي التحليلي في تحليل وتفسير بيانات الدراسة. تم جمع البيانات من عينة عشوائية مكونة من (80) ضابطاً وزعت عليهم جميعاً استبيان إلكتروني. ومن أهم نتائج الدراسة أنّ مستوى تطبيق المؤسسات الوطنية للتحول الرقمي وإدارة الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت كان متوسطاً.

كذلك بينت الدراسة عدم وجود فروق ذات دلالة إحصائية حول التحول الرقمي وإدارة الأمن السيبراني راجعة لمتغيِّرات (العمر، المؤهل العلمي، الخبرات العملية، الدورات التدريبية)، وفقاً لاستجابات عينة الدراسة.

وأوصت الدراسة بضرورة إجراء مزيد من البحوث والدراسات عن موضوع إدارة الأمن السيبراني على أن تشمل مجتمعات وعينات أخرى، وكذلك ضرورة استقطاب خبرات متخصصة ومحترفة في المؤسسات الوطنية بدولة الكويت، وزيادة التعاون والتنسيق مع المنظمات الخاصة والإقليمية والدولية فيما يتعلق بإدارة الأمن السيبراني.

الكلمات المفتاحية :التحول الرقمي، الأمن السيبراني.

مقدمة:

ثورة المعلومات والمعرفة بدأت في بدايات القرن العشرين، ولكن أخذت طابعاً متسارعاً في سبعينيات العقد التاسع عشر، ونتيجة لهذه الثورة المعرفية تطورت القطاعات الزراعية والصناعة والصناعية والخدماتية والأمنية وغيرها من القطاعات، فالمعلومات والمعرفة أصبحت حالياً أساساً للكثير من السلع والخدمات الجديدة، فإنتاج السلع الرقمية أو المعلوماتية تحتاج إلى خبرة كبيرة، وكما هي الحياة متغيرة ومتقلبة، فالمعلومات تتصف بذات الصفة، فهي تتميز بالتبدل والتغير المستمرين، وهي على ما يبدوا تعد بمثابة شريان الحياة للمؤسسات ككل، هذا وقد أصبحت البيئة التي تعيشها المنظمات في ظل العولمة أكثر انفتاحاً ومنافسة كونها معتمدة على قواعد ثابتة أساسها تكنولوجيا المعلومات، وبهذا تحول الاعتماد على الأنظمة التقليدية بإدارة التجارة والصناعة والقطاعات التربوية والصحية وغيرها من القطاعات لأخرى بديلة معتمدةً الأساليب الحديثة والتي أساسها التكنولوجيا الرقمية.

وبهذا سعت العديد من حكومات معظم دول العالم بما فيها الدول العربية الولوج إلى العالم الالكتروني بهدف تقديم وإيصال المعلومات والخدمات الكترونياً للمستفيدين في كافة المجالات (السالمي، 2005).

كما وأنه ونتيجة لانتشار شبكة الانترنت، بات للكثيرين تسويق الكثير من السلع والخدمات، لتصل لمن أراد، كما أن منصات التواصل الاجتماعي أصبحت ميداناً للعابثين لأجل الوصول لمرتاديها وتنفيذ ما يصبون من سرقة معلومات وغيرها من الكثير من الجرائم الإلكترونية (العلاق، 2014).

ونتيجة لظهور الكثير من التطبيقات الإلكترونية مثل التجارة الإلكترونية والحكومة الإلكترونية والأعمال الإلكترونية الكثيرة، فمن الممكن القيام باستخدامها بأساليب وطرق مخالفة للتشريعات والتنظيمات القانونية(ياسين، 2018).

وبهذا وللأسف نتج عن هذه التطورات والتطبيقات الكثير من الجرائم، إذ باتت ظاهرة جرائم الكمبيوتر والإنترنت، أو جرائم التقنية العالية، أو الجريمة الإلكترونية تعتبر جرائم مستحدثة أو مستجدة نسبيا تقرع في جنباتها أجراس الخطر لتنبه مجتمعات العصر الراهن لحجم المخاطر وهول الخسائر الناجمة عنها، باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية الواسعة، (بيانات ومعلومات وبرامج بكافة الأنواع)؛ فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية، توجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت، وهذا وحده، يظهر مدى خطورة جرائم الكمبيوتر، فهي تطال الحق في المعلومات، وتمس الحياة الخاصة للأفراد وتهدد الأمن وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري (Katherine & et.al.، 2014).

وبات من الضرورة بمكان اتباع سياسات واستراتيجيات تسهم في الحدّ من هذه الجرائم، وكذلك إشراك المجتمع ومؤسساته العامة والخاصة بذلك. وبهذا فإن هناك الكثير من المخاطر مرتبطة بتكنولوجيا المعلومات، لذا أصبحت من الضرورات الملحة استخدام أنظمة أمن لأجل الحماية من هذه المخاطر، الأمر الذي أدى لتطوير أنظمة لأجل ذلك عرفت بإدارة الأمن السيبراني، وهي مهتمة بتوفير أنظمة وبروتوكولات متطورة لحماية المعلومات من الاختراق، فضلاً عن مراقبة التهديدات وتقييمها في إطار استجابة منظم واتخاذ قرارات سريعة الاستجابة (Ribas. et..al، 2013).

والأمن السيبراني يعرف بأنه مجموع الوسائل التقنية والتنظيمية والإدارية المستخدمة لمنع الاختراقات عبر أجهزة الحاسوب والاستخدام غير المصرح به للمعلومات ؛ سوء استخدام واسترجاع المعلومات الإلكترونية وأنظمة المعلومات لأجل ضمان استمرارية أنظمة المعلومات وتشغيلها وتعزيز الحماية والسرية والخصوصية البيانات الشخصية، وكذلك اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء الإلكتروني، لذلك يعد الأمن السيبراني سلاحًا استراتيجيًا في أيدي الحكومات والأفراد، خاصة وأن الحرب الإلكترونية أصبحت جزءًا لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول (Saudi Arabian Monetary Authority ، 2017).

ولأهمية الأمن السيبراني أصبحت الحاجة ملحة للقائمين بالمؤسسات الوطنية بدولة الكويت بات من الضرورة بمكان تحسين مهارات منتسبيها لأجل الحدّ من المخاطر المرتبطة بأمن المعلومات والاختراقات الإلكترونية التي تواجهها. ولعلَّ هذا الحديث يعيدنا إلى موضوع هذه الدّراسة، إذ سيتم محاولة التعرف على مستوى التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني في الكويت، كما سيتم تقديم مجموعة من التَّوصيات التي يمكن أن تساهم في زيادة اهتمام الجهات المعنية بموضوع التحول الرقمي وكيفية مواجهة تحديات الأمن السيبراني في الكويت، وبالتالي المساهمة في منع أو تقليل الجرائم الإلكترونية.

مشكلة الدراسة:

برزت في الوقت الحاضر وسائل تكنولوجية حديثة نتاج ثورة معلوماتية ودخلت جميع مناحي الحياة وأصبح الاعتماد عليها ضرورياً لا يستغني عنه الإنسان. ولما كانت هذه الوسائل التكنولوجية منتشرة بشكل واسع أصبحت عرضة لارتكاب الجرائم المختلفة من خلالها، فهناك الكثير من الجرائم المرتبطة بالاختراقات وسرقة المعلومات الإلكترونية والمالية(العلاق، 2014).

وبهذا بات من الضروري ونتيجة لثورة المعلوماتية توفر قواعد وأنظمة حماية تحدّ من هذه المخاطر. وبما أن الجرائم الاختراقات بتزايد، كما أنواعها بتتطور، بات من الحاجات الملحة وضع استراتيجيات وسياسات تسهم في الحدّ من ذلك، وهذا فعلاً ما تقوم به إدارة الأمن السيبراني من خلال مواجهة خطر الهجمات الإلكترونية

الخبيثة على المؤسسات الوطنية الكويتية، كما وأن هذه الجرائم تهدد الأمن المجتمعي وتخلق الكثير من المشاكل الاجتماعية، هذا ولا تألوا المؤسسات الوطنية جهداً لأجل الحدّ من ذلك من خلال تسخير الكثير من الموازنات المالية لأجل تطوير أنظمة الحماية والأمان، إلا أن هناك بعض القائمين على التعامل مع هذه الهجمات السيبرانية تنقصه المعرفة والخبرة. لهذا تأتي هذه الدراسة لأجل تسليط الضوء حول هذا الموضوع، مع التوصية على زيادة التعاون ما بين مؤسسات الدولة وتنظيمات المجتمع المدني للحدّ من الاختراقات المعلوماتية وحماية أمن المعلومات، إذ أن المحافظة أم هام للأمن القومي في أي دولة بما فيهم الكويت.

تساؤل الدراسة:

تحاول الدراسة الإجابة عن السؤال التالي:

ما مستوى تطبيق المؤسسات الوطنية لمتطلبات التحول الرقمي وإدارة الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت ؟

فرض الدراسة:

توجد فروق ذات دلالة إحصائية حول التحول الرقمي وإدارة الأمن السيبراني راجعة لمتغيِّرات (العمر، المؤهل العلمي، الخبرات العملية، الدورات التدريبية)، وفقاً لاستجابات ضباط الشرطة الأكاديميين بالكويت.

أهداف الدراسة:

1- التعرف على مستوى تطبيق المؤسسات الوطنية لمتطلبات التحول الرقمي وإدارة الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت.

2- الكشف عن مدى وجود فروق بمعدلات إجابات عينة الدراسة حول التحول الرقمي وإدارة الأمن السيبراني راجعة لمتغيِّرات (العمر، المؤهل العلمي، الخبرات العملية، الدورات التدريبية)، وفقاً لاستجابات ضباط الشرطة الأكاديميين بالكويت.

أهمية الدراسة:

1- الأهمية النظرية:

وقع الاختيار على هذا الموضوع للتعريف بأهمية التحول الرقمي للمؤسسات الوطنية بالكويت، كما تهدف إلى التعرف على مستوى ومقدرة ضباط الأكاديميين بالكويت في الحدّ من الصعوبات أو التحديات التي تواجه عملية تحقيق أمن المعلومات والأمن السيبراني، كما يمكن تبيين أهمية الدراسة في الآتي:

- أهمية الموضوع بالنسبة لأفراد المجتمع المحلي بالكويت.
- أهمية موضوع الدراسة في تعزيز مبادئ واستراتيجيات الأمن السيبراني.

- تستمد هذه الدراسة أهميتها من طبيعة العينة المستهدفة والتي هي من النادر أن يتم التعرف على توجهاتها؛ والمتمثلة في الضباط الأكاديميين بالكويت .
- قلة الدراسات ذات الصلة بالدراسة وبالأخص التي تم تطبيقها في الكويت، لذا فهي ذات أهمية للمهتمين.
- وضع مقترحات وتوصيات للمهتمين تسهم بتحسين التحول الرقمي وإدارة الأمن السيبراني لدى المؤسسات الوطنية بالكويت.

ب–الأهمية التطبيقية:

يمكن للفئات التالية الإستفادة من الدراسة الحالية:

- الضباط الأكاديميين والمهتمين بإدارة الأمن السيبراني: يمكنهم الاستزادة من هذه الدراسة لأجل التعرف على الاستراتيجيات والسياسات الرامية لأجل تحسين وتطوير أمن المعلومات وإدارة الأمن السيبراني لدى المؤسسات الوطنية بالكويت.
- مخططي السياسات المرتبطة بأمن المعلومات بدولة الكويت: من خلال وضع سياسات واستراتيجيات تسهم بتطوير التحول نحو الرقمية، والحدّ من الصعوبات والتحديات التي تواجه إدارة الأمن السيبراني لدى المؤسسات الوطنية بالكويت.
- الباحثون: يمكنهم البدء بإجراء دراسات أخرى جديدة، على أن تشمل متغيرات وفئات مختلفة.

المفاهيم الرئيسية للدراسة:

التحول الرقمي:

التحول الرقمي أو الرقمنة هو عملية تحويل قطاعات الأعمال الخاصة والحكومية والذي يعتمد بشكل أساسي على التقنيات الرقمية لأجل تسهيل عملية تقديم السلع والخدمات للعملاء، وكذلك تسهيل استراتيجيات التدريس، وتحسين مستويات الخدمات للعملاء، وتسيير وتسهيل تعاملات الموارد البشرية.

الأمن السيبراني:

هو مجموعة من الوسائل التقنية والإدارية والتنظيمية والتشغيلية الرامية لمنع الاستخدام غير القانوني وغير المصرح به، سوء استخدام واسترجاع المعلومات الإلكترونية وأنظمة المعلومات والاتصالات، ويهدف الأمن السيبراني ضمان توافر واستمرارية عمل المعلومات وتعزيز الحماية والسرية و خصوصية البيانات الخاصة بالأفراد والمؤسسات الوطنية.

الإطار النظري للدراسة:

التحول الرقمي:

التكنولوجيا ولما فيها من أهمية وخطر ولما تتركه في النفوس من أثر تعتبر اليوم بلا منازع المدرسة الكبرى للمجتمع وهي بهذا النعت جديرة لما يتوفر لها من شتى الاختصاصات ولما يتاح لها من مختلف الأزمنة، فهي إذن مسؤولية ولها رسالة تربوية بهما، وبسواهما نطالبها كما نطلب من المدرسة الرسمية. فالتوجه إلى

وسائل الإعلام في سبيل التنمية الأخلاقية والاجتماعية للأطفال أضحى اليوم مطمحاً ما بعده مطمح. ومطلباً تسعى جاهدة إليه المجتمعات، إن اختراع الراديو ووسائل الاتصال والانترنت من أرقى ما وصل إليه العقل البشري في العصر الحديث، بل من أعظم ما أنجزته الحضارة الإنسانية في القرن العشرين وهي سلاح ذو حدين للخير وقد تستعمل في الشر .

هذا ودخلت التكنولوجيا الرقمية بما فيها الانترنت كل منزل واجتذب كل الناس سواء كانوا مدفوعين للاستمتاع والترفيه أم كانوا يلتمسون فيه بديلاً للثقافة والمعرفة والتزود بالمعلومات وإشباع الحاجات النفسية الفنية والأدبية والعلمية والمعرفية.

ماهية التحول الرقمي:

هناك بعض التعريفات لمفهوم التحول الرقمي أو الرقمنة، منها:

1- هي عملية من خلالها يتم إحلال التقنيات الرقمية لأجل تسهيل خدمة الإنسان والتقنيات الرقمية.

2- هي عبارة عن الأجهزة والبرمجيات والأدوات والوسائل والطرق التي تساعد المنظمة على تسجيل وتخزين ومعالجة واستخدام واسترجاع المعلومات(الخفاف، 2011).

3- هي مجموعة أدوات وأنظمة وأجهزة وموارد إلكترونية تعمل بشكل أساسي على إنشاء البيانات وتخزينها معالجتها.

4- عملية تبادل البيانات والمعلومات والمراسلات والوثائق والصور وتقديم السلع والخدمات والبرامج والاستشارات بطريقة الكترونية عن بعد وآمنة وسهلة وذات جودة في أقل وقت وجهد وتكاليف داخل وبين المنظمات بأنواعها المختلفة حتى تصل إلى نظام عمل بلا أوراق (أبو النصر، 2020، 50).

ومن أبرز الأمثلة على التكنولوجيا الرقمية المنصات الرقمية وخاصة التعليمية منها ووسائل التواصل الاجتماعي والألعاب عبر الانترنت، والهواتف الذكية. ومن أبرز ثمارها التعلم الرقمي والذي يستخدم التكنولوجيا بشكل أساسي، وشمل كافة مراحل التعليم الدراسية المدرسية والجامعية(Mansell، 2002). نظرا للظروف التي يمر بها العالم نتيجة جائحة فيروس كورونا (كوفيد 19). وبهذا فإن التحول الرقمي يشمل استخدام الأجهزة والبرمجيات والمعالجات وشبكات الانترنت والتي يتم تسخيرها لتسهيل وخدمة أغراض الإنسان واحتياجاته المختلفة.

نشأتها وتطورها:

اهتم الإنسان منذ القدم بالمعرفة وتكنولوجيا المعلومات، ومن أجل الاستفادة من هذه المعلومات قام بجهود مضنية لأجل ذلك فقد اخترع بعض الآلات فقد اخترع (المحسب الحجري) في بابل منذ)3000(سنة قبل الميلاد، ومن ثم اخترع (محسب الخرز والأسلاك) في مصر، وبعد ظهور الإسلام وانتشاره وفي عام)800م(قام (محمد

بن موسى الخوارزمي) في حل المسائل، وذلك بتقسيم حل المسألة إلى مجموعة خطوات أطلق على هذا الأسلوب اسم (الخوارزميات)، وفي سنة (1643م)، اخترع العالم الفرنسي (بليز باسكال) الآلة أطلق عليها اسم سباسكلين(Pascalene) وهي آلة ميكانيكية تستطيع القيام بالعمليات الحسابية البسيطة من جمع وطرح لمجمعة من أرقام تتكون من ثمان خانات، وبعدها قام العالم البريطاني جورج بول بتطوير نظام حسابي أطلق عليه الجبر البولياني(Boolean algebra)، إذ اعتمد هذا العالم في تشغيل نظامه على منطق الخطأ والصواب والذي يعد أساس تصميم الدارات المنطقية للكمبيوتر وبدأ مع ظهور هذا النظام التطور السريع لتكنولوجيا المعلومات.

وفي سنة 1939م، طور أول جهاز كمبيوتر رقمي يعتمد على المنطق البولياني في عمله اطلق عليه اسم (ABC)، وفي سنة 1947، تم تطوير أول ترانزستور ليستخدم بدل الأنابيب المفرغة التي كانت تستخدم سابقاً، طورت بعد ذلك الحواسيب التي تقوم بالمعالجة في الوقت الحقيق وبدأ معه تطور لغات البرمجة حيث تم تطوير لغة (BASIC) سنة 1964م، ومن لغة باسكال (Pascal) ولغة الفورتان (Fortran)، وكذلك تم تطوير لغة تعتبر من أهم اللغات على الإطلاق وهي (لغة السي) التي ظهرت بعد ذلك (الشبكات) إذ جاءت الفكرة من خلال ربط مجموعة من الحواسيب مع بعضها من أجل استخدام في القطاع العسكري في بادئ الأمر ثم بدأ تتطور هذه الفكرة لإنشاء شبكات محلية وشبكات إقليمية لتكون بعد ربطها مع بعضها الانترنت (Internet) (الخفاف، 2011).

كما وبدأ العلماء بتطوير التكنولوجيا الرقمية بمنتصف القرن العشرين، استندت تقنياتهم إلى مفاهيم رياضية اقترحها عالم الرياضيات الألماني بالقرن السابع عشر (جوتفريد فيلهلم) (Gottfried Wilhelm) الذي اقترح نظاماً ثنائياً للحوسبة، ألهم هذا الابتكار رموزاً رقمية مثل الكود القياسي الأمريكي للمعلومات (ASCII) والذي يصف الأشياء بالأرقام، وبهذا فإن التكنولوجيا الرقمية هي عملية أساسية ثنائية يتم تسجيل المعلومات الرقمية في كود ثنائي لمجموعة من الأرقام (0 و1)، وتسمى أيضاً (بت) (bits)، وبهذا فإن التكنولوجيا الرقمية تتيح ضغط كميات هائلة من المعلومات على أجهزة تخرين صغيرة يمكن حفظها ونقلها بسهولة، كما وتعمل الرقمنة أيضاً على تسريع سرعات نقل البيانات، كما وغيرت التكنولوجيا الرقمية كيفية تواصل الناس وتعلمهم وعملهم(Compaine، 2001).

هذا واعتمدت الاتصالات السلوكية واللاسلكية على أساليب الرقمية لنقل الرسائل، كما وحلت التكنولوجيا الرقمية محل الإشارات السلكية والاتصالات والكابلات، كما وغيرت الطباعة الرقمية باستخدام تقنيات التصوير الكهربائي والبيانات المنسقة كيفية نشر الكتب والمجلات، إذ يمكن نسخ الكثير من الكتب وحفظها بمكتبة رقمية، كما وفي أوائل العقد الأول من القرن الحادي والعشرين، ظهرت أجهزة الكمبيوتر الرقمية المربوطة بشبكات الانترنت بأشكال وأحجام مختلفة، كما وتم انتاج الكثير من الأفلام والرسوم المتحركة باستخدام أجهزة الكمبيوتر(Mansell، 2002).

المزايا والسلبيات للتحول الرقمي:

يرى (الشيشاني، 2010)، بأن هناك الكثير من الفوائد للتحول الرقمي أو للرقمنة، وتمثل في الآتي:

1- ساهمت بمنح الشّعور بالحريّة للإنسان، فبات من السهولة بمكان الحصول على الأشياء بالوقت الذي يختاره الإنسان.

2- إتاحة الفرصة للتّواصل وتبادل الأفكار والآراء مع الآخرين، وفتحت أبواباً للحوار وللنّقاش مع مختلف الشعوب بمختلف المواضيع.

3- استحداث مفهوم التّجارة والحكومة الإلكترونيّة، وتيسير عمليّات الشراء والبيع وتبادل العُملات من خلال الإنترنت.

4- ساهمت في تقديم الخدمات عن بعد، وأدت إلى توفير الجهد والوقت،

5- أوجدت التعلّم عن بُعد، وفتحت مجالاً كبيراً أمام البحوث العالمية العلميّة.

6- المساعدة على سرعة إنجاز المَهام في أيّ وقت على مدار اليوم والعام. بنت جسراً لتقريب المسافات وجعل العالم قرية صغيرة.

7- استحداث وظائف جديدة، مثل برمجة وتطوير مواقع الويب والمعدّات.

كما وأنه من خلال التكنولوجيا الرقمية بات من السهولة بمكان التعرف على آخر الأخبار من خلا لوسائل التّكنولوجيا في الإعلام عن طريق معرفة آخر الأخبار والتّفاصيل مهما تباعدت المسافات، وذلك بما أوجدته الصّحافة الإلكترونيّة من خدمة مُتابعة الأحداث أولاً بأول.

وفيما يتعلق بالسلبيات فإن الإكثار من استخدام وسائل الرقمنة يؤدي إلى العزلة الاجتماعية وانتشار القنوات المرتبطة بالدجل والشعوذة نتيجة الانفتاح الإعلامي، وانتشار المواقع غير الأخلاقية، وكذلك انتشار وظهور الجرائم الإلكترونية والمالية بأشكالها المختلفة.

الأمن السيبراني:

يتضمن الأمن السيبراني حماية المعلومات والأجهزة الرئيسية من التهديدات السيبرانية، وبهذا يكون جزء مهم من أنظمة الشركات التي التي تكون مهتمة بالاحتفاظ بقواعد بيانات ضخمة من معلومات عملائها. كما أن الأمن السيبراني مرتبط بشكل أساسي بالمنصات الاجتماعية، وكذلك حيثما يكون هناك تقديم معلومات للمنظمات الحكومية والمتصفة بالسرية والسياسية، كما أنها مرتبطة بحماية البيانات الحكومية من الهجمات السيبرانية، هذا وأن هناك استثمار الكثير من المال لأجل حماية كل هذه المعلومات من خلال الأنظمة السيبرانية، كما أن هناك تزايد في عدد الأشخاص الذين يحاولون الوصول إلى المعلومات عبر الانترنت كل يوم، كما تتزايد التهديدات التي

تتعرض لها المعلومات، كما تقدر تكلفة جرائم الانترنت بالمليارات (ASM Technologies Limited , 2018).وبهذا فإن الأمن السيبراني مرتبط بشكل أساسي بالمحافظة على المعلومات والبيانات للأفراد والمؤسسات، وحمايتها من الاختراق غير المشروع.

التعريف بالأمن السيبراني:

الأمن السيبراني مصطلح جاء من الكلمة اللاتينية (سايبر Cyber) والتي تعني (فضاء المعلومات)، وبهذا فإن الأمن السيبراني يعني إلى (أمن الفضاء المعلوماتي)، وبهذا فهو معني بالأمن المرتبط بشبكات الانترنت وكذلك شبكات الاتصالات (البهي، 2017). ويعرف الأمن السيبراني بأنه مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهكين من المخاطر في الفضاء السيبراني"، وبهذا يعرف بأنه " النظام الذي يعمل على حماية ضد الاستخدام الإجرامي أو غير المصرح به للبيانات الإلكترونية، أو هو كافة التدابير المتخذة لتحقيق ذلك " (Kennedy،2017).

وبهذا فإن أي إساءة استخدام غير مصرح به أو إجرامية للبيانات أو الأجهزة الإلكترونية يُفهم على أنها تهديد إلكتروني. وترى الدراسة الحالية بأن الأمن السيبراني يتمثل بالنظام المستخدم لأجل حماية الأجهزة والشبكات من الاختراق بشكل غير مشروع.

أقسام الأمن السيبراني وأهميتها:

قسم(Moore، 2018) الأمن السيبراني إلى عدة أقسام يمكن إيجازها على النحو الآتي:

1- أمن الاتصالات (**Communications Security**:) وهو الذي يهدف إلى الحماية من التهديدات المؤثرة على البنية التحتية والتقنية والحفاظ عليها من التلاعب.

2- أمن العمليات (**Operations Security**:) وهو الذي يهدف إلى حماية التلاعب بالعمليات أو طريقة سير العمل.

3- أمن المعلومات (**Information Security**:) يحمي أمن المعلومات (المعلومات) من غير المصرح به الوصول إليها، وحماية خصوصيتها، وكذلك المحافظة عليها من السرقة، ومن الأمثلة على أمن المعلومات (استخدام الحماية من خلال التشفير).

4-الأمن المادي (**Physical Security**): وهو تمثل حماية الأصول المادية المرتبطة والمتعلقة بالنظام السيبراني، وهذه الأصول يمكن ان تكون عبارة عن خوادم وتخزين مكونات الشبكة، وتتضمن حمايتها ضد الوصول الغير المصرح به .

5-أمن التطبيقات (**Application Security**): يحمي أمان التطبيقات من التهديدات التي تحدث بسبب عيوب في تصميم التطبيق أو التطوير أو التثبيت أو التحديث أو الصيانة.

6-الأمن العسكري (**Military Security**): وهي تمثل نظام حماية من الوصول إلى الأصول المادية ذات الجانب السياسي أو العسكري أو الاستراتيجي .

7-أمن الشبكات (**Networks Security**): يحمي أمان الشبكة قابلية الاستخدام والسلامة في الشبكة والمكونات المرتبطة بها والاتصال والمعلومات عبر الشركة، ومن الأمثلة على أمان الشبكة (مكافحة الفايروسات ومكافحة برامج التجسس).

ووتري الدراسة الحالية بأن الأمن السيبراني مرتبط بشكل اساسي بأمن المعلومات سواء أكانت مرتبطة بالشبكات أو بأنظمة الكمبيوتر.

متطلبات تطبيق مبادئ الأمن السيبراني:

هناك عدة عناصر ضرورية ومتطلبات هامة لتطبيق مبادئ الأمن السيبراني، يمكن إجمالها على النحو الآتي (Kennedy، 2017):

1-العناصر المادية (**Hardware**): وهي عبارة عن الأجهزة والقطع الفنية والإلكترونية والأدوات المادية التي تمثل البنية التحتية الأساسية اللازمة لتشغيل نظم المعلومات .

2-العناصر البرمجية (**Software**): وهي المكونات غير المادية والتي تشتمل على النظم والبرمجيات الأساسية والمطلوبة لتشغيل نظم المعلومات.

3-القوى البشرية (**Human Resources**):

تمثل القوى البشرية الأفراد الأكفاء وذوي المهارات في مجال تكنولوجيا المعلومات ونظم المعلومات، الذين يقع على ع اتقهم تشغيل النظم وإدامتها في المنظمة.

4-دعم الإدارة العليا لعملية تطبيق نظم المعلومات:

يجب أن يكون هناك اقتناع كامل ودعم مطلق من الإدارة العليا لعمليات تطبيق نظم المعلومات في المنظمة وعدم تعجل النتائج إلى حين اكتمال حلقة الحوسبة أو الأتمتة للعمليات والوظائف الإدارية في المنظمة.

5-إعادة تصميم الهيكل التنظيمي لتلبية متطلبات تكنولوجيا المعلومات:

وهي عملية إعادة ووصف للوظائف الموجودة في المنظمة وما يتبعه من إلغاء أو استحداث الوظائف على أسس حديثة تأخذ بعين الاعتبار التطورات التكنولوجية المتسارعة واحتياجات تطبيق نظم المعلومات.

6- الشبكات والاتصالات: وهي الوسيلة التي يتم من خلالها مرور البيانات من مكان لآخر.

وبهذا فإن العناصر المادية والبرمجية والبشرية ودعم الإدارة وتصميم الهيكل التنظيمي من المتطلبات الرئيسية لإدارة الأمن السيبراني، إلا أن العنصر البشري وتدريبهم وتحسين مهارته يعتبر الأبرز من هذه المتطلبات.

مزايا تطبيق الأمن السيبراني:

يهتم الأمن السيبراني بالمحافظة على سرية المعلومات وخصوصيتها، خلال منع الوصول إلى المعلومة إلا من خلال صاحب العلاقة ويتم التحقق من ذلك من خلال استخدام هوية المستخدم لهذه الخدمة (الجنابي، 2017). كما يعنى الأمن السيبراني بالمحافظة على تجانس ووحدة المعلومات، من خلال منع العبث والتغيير في البيانات، وكذلك توفير المعلومات وتجهيزها عند الطلب بعد التأكد من صلاحية هويته، وهناك عدة مزايا لتطبيقه تتمثل بالآتي (الوكيل، 2017):

1- القدرة على تحقيق وفورات بالكلف مقابل نتائج عالية ودقيقة، بمعنى أن تكون هناك جدوى اقتصادية من الناحية الاقتصادية والمادية.

2- العمل عن بعد إذ يمكن للمراقب ان يقوم بعمله بعيداً عن الوصول إلى مكان العمل، الأمر الذي يبعده من الكثير من المخاطر.

3- يمكن التعرف من خلال البرامج الرقابية على مقدار الإنحراف في الأداء.

هذا ويمكن للأمن السيبراني بشكل كبير تحقيق وفورات مرتفعة بالوقت مقابل شمولية وتكاملية في النتائج، مقارنة مع النظام اليدوي.

دور الأمن السيبراني في الحدّ من الجرائم:

يهدف الأمن السيبراني بشكل مباشر إلى الانتقال من العمل التقليدي إلى استخدام التقنيات الحديثة بأشكالها المختلفة بعمليات الاطلاع على الوثائق وكذلك الاتصالات اللازمة لممارسة العمل الرقابي، ومن أهميها شبكات الحاسب الآلي التي تقوم على ربط الوحدات التنظيمية التنفيذية مع الأجهزة الرقابية في التشكيلات التي تعمد بشكل أساسي على رقابتها لتسهيل الحصول على البيانات والمعلومات بسرعة ودقة مرتفعة، وبأقل وقت وتكاليف قليلة، الأمر الذي يؤدي إلى تسريع الأداء وزيادة المعرفة، وبطبيعة الحال يؤدي إلى اتخاذ القرارات المناسبة والتعرف على مقدار الانحرافات في إنجاز المهام المناطة بالأجهزة التنفيذية(الجنابي، 2017). وبهذا يمكن من خلال عملية

المراقبة على أجهزة الحاسب الآلي التعرف على أجهزة المخترقين، والتعرف على هويتهم، وبهذا أصبح الأمن السيبراني من الأساليب المهمة بالتعرف على مرتكبي الجرائم.

أهداف الأمن السيبراني:

هناك عدة أهداف من وراء تطبيق الأمن السيبراني، يمكن إجمالها على النحو الآتي(الجنابي، 2017):

1- ضمان استمرارية عمل تطبيقات نظم المعلومات.

2- العمل على حماية خصوصية وسرية المعلومات الشخصية سواء للأفراد أو المنظمات العامة أو الخاصة.

3- استخدام التدابير اللازمة لأجل حماية المواطنين من المخاطر المترتبة على دخول شبكة الانترنت.

4- حماية الأجهزة التقنية وكذلك التشغيلية.

5- المحافظة على شبكات المعرفة والمعلومات.

بهذا فإن الأمن السيبراني يشكل حماية لأنظمة التكنولوجيا من خلال تفعيل أنظمة الحماية للأفراد والمؤسسات.

النظريات المفسرة للجرائم المرتبطة بالأمن السيبراني:

هناك الكثير من النظريات المفسرة للجرائم المرتبطة بالأمن السيبراني وأغلبيتها جرائم إلكترونية مالية مرتبطة بالاختراق الحواسيب بأسلوب غير شرعي، إلا أننا ولمحدودية عدد الصفحات في هذه الدراسة يمكن إيجاز أهمها على النحو الآتي:

1-نظرية هيرشي وجتفردسون (الأنومي لميرتون):

ترى هذه النظرية بأن الأشخاص يقترفون الكثير من الأعمال الإجرامية والغير مقبولة اجتماعياً لأجل الحصول على الثروة، والوصول للثراء يواجهها الكثير من الصعوبات لأجل تحقيقها بالطرق السليمة قانونياً أو اجتماعياً، لذا يقوم بعض الأشخاص بارتكاب الجرائم الإلكترونية لجملة من الأسباب من أبرزها سهولة القيام بها وكبر المجتمع المستهدف وقلة المخاطر وسرعة أو آنية المردود .

وبهذا يُلاحظ بأن هذه النظرية تركز بأن المخترقين يقوم بارتكاب الجريمة لأجل الثراء الفاحش وكذلك سرعة ارتكابها وقلة مخاطرة نتيجة لصعوبة إثباتها.

2-نظرية الفرصة:

ظهرت الكثير من النظريات والتي هدفها بالأساس هو تفسير السلوك الإجرامي فيما يخص الجرائم الإلكترونية، إذ أن نظرية (الفرصة) تعتبر أميزها، فاستخدام شبكات التواصل الاجتماعي والانترنت بالعموم، أوجدت مرتعاً خصباً للجناة الذين يوسمون (بالمتحفزين)، لوجود أهداف ثمينة وسهلة في الواقع الافتراضي، في ظل غياب الحراسة، وبهذا يمكن أن تحدث الجريمة في حال التقاء عوامل أساسية ثلاث ألا وهي (الجاني المتصف بالتحفز، والهدف المرجو (المناسب)، وغياب الحراسة)، وبهذا فإن غياب أحد العوامل يمنع من القيام بالاتصال

المباشر، الأمر الذي يفشل الجريمة، كما أن نظرية النشاط الرتيب ساهمت بوضع تفسير السلوك الإجرامي للجناة، كما ويمكن تفسير تعاظم ضحايا الجرائم الإلكترونية من خلال الكثير من التغيرات في النشاطات الروتينية بشكل يومي، فمن خلال ظهور الانترنت وشبكات التواصل الاجتماعي تغيرت طريقة الأشخاص الذين يتفاعلون ويتواصلون بها مع غيرهم، وبهذا وبما أن التفاعل والتواصل عبر الشبكات التواصل الاجتماعي أصبح روتينياً، زاد عدد الساعين لارتكابها، فالجريمة الالكترونية تتكون من جاني متحفز والمستهدف الملائم(استهداف المال أو حتى الهوية)، والحراسة القادرة (برامج المضادة للفيروسات وكذلك برامج الحماية (البداينة، 2014).

كما ويلاحظ بأن المجرم لا يمكنه القيام بارتكاب الجريمة إلا في حال ضعف مقدرة البرامج الأمن والحماية على اكتشافه، وبهذا يجب وضع أنظمة ذكية ومتطورة تعمل بشكل أساسي على الحدّ من الجرائم الإلكترونية.

البحوث والدراسات السابقة:

التالي عرضا للبحوث والدراسات السابقة والمرتبطة بشكل مباشر بموضوع الدراسة الحالية، وذلك مرتبة ترتيبا تصاعدا من الأقدم إلي الأحدث:

1-دراسة (القرني، 2007):

هدفت الدراسة لأجل التعرف على مدى تطبيق الإدارة الإلكترونية بالمجالات الأمنية والإدارية لدى الجهاز الأمنية في منطقة الرياض، هذا وخلصت الدراسة بأن للإدارة الإلكترونية كبيرة بتحسين مستويات التعاملات والخدمات للمواطنين من خلال الإبلاغ عن الشكاوي المرتبطة بالجرائم الالكترونية، هذا وأوصت الدراسة بضرورة توفير الإمكانات البشرية والمادية لأجل تطبيق متطلبات الإدارة الإلكترونية بمدينة الرياض، كما وبينت الدراسة بوجود فروق ذات دلالة إحصائية فيما يتعلق ب (المستوى التعليمي، الدورات التدريبية، العُمر، والخبرة والمعرفة).

2-دراسة المصري وآخرين(Elmasri et al,2016):

وهي بعنوان الشرق الأوسط الرقمي: تحويل المنطقة إلى اقتصاد رقمي قائد". هدفت هذه الدراسة الموسعة تقديم مسح شامل للواقع الرقمي، أي ما يتصل بثورة المعلومات وتكنولوجيا المعلومات والاتصالات في المنطقة العربية. وتأتي أهمية الدراسة من واق أن "مؤشر ماكينزي للرقمنة" هو الجهد الأول من نوعه لتقدير مستوى الرقمنة وأثرها في دول الشرق الاوسط.واستخدمت الدراسة المنهج الوصفي المسحي. وشملت عينة الدراسة كل من البحرين، ومصر، والأردن، والكويت، ولبنان، وعمان، وقطر، والسعودية، ودولة الامارات العربية المتحدة. وقدمت الدراسة معلومات وبيانات قيمة حول استخدام وسائل التواصل الأجتماعي في تلك الدول. كما أظهرت نتائج الدراسة، بين أمور عديدة أخرى، أن الرقمنة في كل من الامارات وقطر والبحرين، قطعت أشواطاً متقدمة، فيما تتخلف نسبيا الكويت ومصر ولبنان، ويقع ألاردن والسعودية وعمان بين هاتين الفئتين.

3-دراسة البهي (2017):

هدفت الدراسة لأجل التعرف على مفهوم الردع السيبراني والمتطلبات اللازمة لأجل ذلك، وبينت الدراسة بأن استراتيجية الردع في البعد السيبراني غير مطبقة، كما أن هناك نقص في التشريعات القانونية، كما أنه لا يوجد استراتيجية واضحة لأجل ذلك، لهذا تبنت الدراسة بضرورة وضع استراتيجية مرتبطة بعملية الردع السيبراني.

4-دراسة الجنابي(2017):

هدفت الدراسة لأجل التعرف على مدى فعالية القوانين الدولية والوطنية في الحدّ من الجرائم المرتبطة بالهجمات السيبرانية، بينت الدراسة بأن هذه الهجمات في تزايد مستمر، كما وبينت الدراسة بأن التشريعات الوطنية لا تزال مقصرة في ذلك، هذا وأوصت الدراسة بضرورة تضافر الجهود فيما يخص إبرام المعاهدات والاتفاقيات على المستوى الإقليمي والدولي والوطني لأجل الحدّ من الهجمات السيبرانية.

5-دراسة جالينيك وآخرون (Galinec..et..al,2017):

هدفت الدراسة إلى التعرف على أهمية الأمن السيبراني في الحدّ من الهجوم التكنولوجي، هذا واستخدمت الدراسة المنهج الوصفي التحليلي لأجل تحقيق أهداف الدراسة، كما وبينت الدراسة بأن وحدة الأمن السيبراني تقوم على مرتكزات أساسية ألا وهي (خطة العمل، الهجوم السيبراني (من قبل المجرمين) الجريمة السيبرانية، الدفاع السيبراني، العمليات السيبرانية، الأمن السيبراني، الاستراتيجية الوطنية للأمن السيبراني، إشراك أفراد المجتمع ومؤسسات المجتمع العامة والخاصة) كما وخلصت الدراسة لمجموعة من النتائج كان من أبرزها بأن استخدام الأمن اليبراني يعمل على زيادة الأمن المعلوماتي ويربك المجرمين، إذ يقوم على إجراءات دفاعية تستند بشكل أساسي على تكنولوجيا المعلومات، كذلك أوصت الدراسة إلى ضرورة استخدام الأمن السيبراني كاستراتيجية أساسية للحدّ من الجرائم الإلكترونية في كرواتيا

6-دراسة ناكاما وبوليت(Nakama& Paullet , 2018):

هدفت الدراسة إلى تعلى ما لطلاب عبر المراحل الدراسية بالجامعة إلى كيفية التصدي للهجمات السيبرانية، وذلك باستخدام المنهج التحليلي، وبالاعتماد على عينة قوامها (450) طالباً يدرسون في جامعة هواوي، أشارت الدراسة إلى أن هناك مجموعة من المهارات المهمة في ديناميكيات الدورات الدراسية على الإنترنت في الكليات الجامعية الأولى للتغلب على قيودها السياقية والمتمثلة بتعلم كيفية التنقل في نظام إدارة التعلم، وإرسال وتلقي الرسائل بفعالية بين الطلاب وأعضاء هيئة التدريس، وساهمت الدراسة في إكساب الطلاب استراتيجيات التعلم عبر الإنترنت لأن الطلاب قد يشعرون أنهم غير قادرين على إكمال المهام الأكاديمية دون مساعدة، والتي يمكن أن تهدد القيمة الذاتية، ونتيجة لذلك يفشل العديد من طلاب الجامعات في طلب المساعدة المطلوبة، معتبرين أنها محرجة.

7-دراسة القحطاني (2019):

هدفت الدراسة إلى التعرف على مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي من وجهة نظرهم؛ من خلال التعرف على آرائهم حول المفهوم الأقرب له وأهم الجرائم التي يتعامل معها وطرق الوقاية المجتمعية من جرائم الفضاء السيبراني والمعوقات المجتمعية لتحقيق الوقاية من هذه الجرائم، واستخدمت الدراسة منهج المسح الاجتماعي بأسلوب العينة، بالتطبيق على عينة عشوائية من طلاب وطالبات الجامعات السعودية في المستويات الدراسية المختلفة وبلغت عينة الدرسة (486) طالباً وطالبة، واعتمدت الدراسة على الاستمارة الإلكترونية لتجميع البيانات، أظهرت نتائج الدراسة أن أقرب مفهوم للأمن السيبراني من وجهة نظر عينة الدراسة هو استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به،ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها، في حين جاءت جريمة (الاحتيال الإلكتروني / النصب الإلكتروني) كأكثر جريمة يتعامل معها الأمن السيبراني؛ في حين تعتبر التوعية الإعلامية للمجتمع حول طرقه هي أهم طرق الوقاية المجتمعية لمشكلات الفضاء السيبراني.

8-دراسة الصحفي وعسكول (2019):

هدفت الدراسة إلى الكشف عن مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، ولتحقيق هدف الدراسة اعتمدت الدراسة على المنهج الوصفي التحليلي، حيث تكون مجتمع الدراسة من جميع معلمات الحاسب للمرحلة الثانوية بمدينة جدة للعام الدراسي (2019)، وعددهن (352) معلمة حسب المعلومات الواردة من إدارة تعليم جدة، توصلت الدراسة إلى مجموعة من النتائج من أهمها بأن المستوى الوعي بمفاهيم الأمن السيبراني كان منخفضاً، كما وأكدت النتائج عدم وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد عينة الدراسة في درجة وعي معلمات الحاسب بالأمن السيبراني تعزى لمتغيرات الدراسة الحالية (سنوات الخبرة، المؤهل العلمي، العمر، و الدورات التدريبية).

9-دراسة ريدي وريدي (2020:(Reddy & Reddy,

هدفت هذه الدراسة إلى التعرف على التحديات التي يواجهها الأمن السيبراني وعلى أحدث التقنيات وأساليب الأمن السيبراني والاتجاهات التي تغير وجه الأمن السيبراني، وتوصلت الدراسة إلى أن أمن المعلومات والأمن السيبراني يعدان موضوعًا واسعًا أصبح أكثر أهمية لأن العالم أصبح مترابطًا للغاية، حيث يتم استخدام الشبكات لإجراء المعاملات الهامة، كما بينت النتائج استمرار حدوث الجرائم الإلكترونية في اختلاف المسارات إلى جانب الأدوات والتهديدات السيبرانية الجديدة التي تظهر بشكل مختلف كل يوم، تمثل عائقاً أمام المؤسسات في ما يتعلق بكيفية تأمين بنيتها التحتية.

التعقيب على البحوث والدراسات السابقة:

من خلال ما تم عرضه من بحوث ودراسات سابقة مرتبطة بشكل مباشر بموضوع الدراسة يمكن التوصل إلي الآتي:

1- قلة البحوث والدراسات السابقة المرتبطة بموضوع الدراسة بشكل مباشر لدى المؤسسات الوطنية بالكويت، وخصوصاً من وجهة نظر الضباط الأكاديميين بالكويت.

2- أن هذه الدراسة تعتبر من الدراسات الحديثة جداً إذ تم إجرائها في العام الجامعي 2020 /2021.

3- تتشابه الدراسة الحالية مع البحوث والدراسات السابقة فيما يخص موضوع الدراسة المتمثل في التحول للرقمية وإدارة الأمن السيبراني.

4- كذلك تتشابه في إتباعها المنهج الوصفي التحليلي لأجل تحقيق أهداف الدراسة.

5- اختلفت الدراسة الحالية عن سواها من خلال العينة والمتمثلة في الضباط الأكاديميين بالكويت، إذ هناك ندرة بالتركيز على هذه العينة بوجه الخصوص.

6- تمّ الاستفادة من البحوث والدراسات السابقة، في الإطار النظري وفي بناء الإستبيان الإلكتروني وتحليل نتائج الدراسة.

7- أيضا تم الإستفادة من البحوث والدراسات السابقة في التعرف على مدى التطابق أو الاختلاف بين نتائج الدراسة الحالية ونتائج البحوث والدراسات السابقة.

الإطار المنهجي للدِّراسة:

نوع الدراسة:

تعتبر الدراسة الحالية من نمط الدراسات الوصفية / التحليلية لملاءمته لأهداف الدراسة، تلك الدراسات التي تعتمد على دراسة الظاهرة والقيام بوصف هذه الظاهرة وصفاً دقيقاً، وتحليل بياناتها والعلاقة بين مكوناتها كماً وكيفاً والربط والتحليل والتفسير وصولاً إلى الاستنتاجات ليبنُى عليها النتائج والتوصيات (عبيدات وآخرون، 2001). وتتميز الدراسات الوصفية / التحليلية بالمرونة في استخدام الأدوات والأساليب والقدرة علي فهم وتحليل الظاهرة المدروسة وبالتالي القدرة علي تقديم ووصف معبر ودقيق عنها (أبو النصر، 2015، 150).

منهج الدراسة:

تم الاستفادة من منهج المسح الاجتماعي بأسلوب العينة، للتعرف علي آراء ووجهات نظر واتجاهات عينة الدراسة. ويعد منهج المسح الاجتماعي من أشهر مناهج البحث المستخدمة في الدراسات الوصفية / التحليلية، حيث يقوم هذا المنهج بالتعرف علي الظاهرة كما هي في الواقع، والتعرف علي جوانب القوة والضعف فيها، حتي

يتمكن الباحث من التوصل إلي مجموعة من المقترحات والتوصيات التي يمكن أن تساهم في إحداث تغييرات جزئية أو كلية في الظاهرة أو المشكلة المدروسة (أبو النصر، 2014، 210).

حدود الدراسة:

تتمثل حدود الدراسة في التالي:

1- الحدود المكانية: هذه الدراسة تقتصر على المؤسسات الوطنية بالكويت.

2- الحدود الزمنية: تمّ إجراء هذه الدراسة خلال العام الجامعي 2021/2020م.

3- الحدود البشرية: ضباط الشرطة الأكاديميين بالكويت.

مجتمع الدراسة وعيِّنته:

تكوّن مجتمع الدراسة من جميع الضباط الأكاديميين بالكويت، والذي يبلغ حجمهم حوالي 550 ضابط. ونظراً لصعوبة جمع البيانات من جميع هؤلاء الضباط، ونظرا للظروف التي تمر بها البلاد من جائحة فيروس كورونا (كوفيد 19)، تم أخذ عينة عشوائية منهم حجمها (80) ضابطاً، بنسبة 15 % تقريبا من مجتمع الدراسة.

أداة جمع البيانات:

للحصول على المعلومات والبيانات المطلوبة للإجابة عن تساؤل الدراسة واختبار فرض الدراسة تم تصميم استبيان، اعتمد في بناءه علي الإطار النظري، مع الاستفادة من أدوات جمع البيانات في بعض البحوث والدراسات السابقة وخاصة دراسة كل من: (القحطاني، 2019، والصحفي وعسكول، 2019، و دراسة ناكاما وبوليت(Nakama& Paullet ، 2018)، ودراسة القرني، 2007).

هذا وقد بلغ عدد فقرات الاستبان بعد التمحيص والتَّطوير (33) فقرة. وتكون من جزأين، هما: الجزء الأول اشتما على البيانات الأولية، واشتمل الجزء الثاني على فقرات شارحة لموضوع الدِّراسة. ولقد صُمم الاستبيان بناءً على نموذج ليكرت (ScaleLikert) الخماسي، وذلك حرصًا على تحقيق مزيد من الدقة والتحديد في الإجابات من المبحوثين.

وتضمن الاستبيان درجة الموافقة على كل فقرة مقسمة إلى (6) فئات، حيث تمَّ إدخال هذه الاستجابات على الحاسوب حسب ما هو مبيَّن في جدول رقم(1).

جدول رقم (1)

درجة الاستجابة ورمزها

درجة الاستجابة	الرمز
بدرجة كبيرة جداً	5
بدرجة كبيرة	4
بدرجة متوسِّطة	3
بدرجة قليلة	2
بدرجة قليلة جداً	1

وبناءً على الرُّموز المقترنة بالاستجابات المختلفة، تمَّ احتساب المتوسِّط الحسابي للاستجابات بدافع الحكم على درجة الموافقة لكل فقرة من فقرات الاستبانة، كما وتمَّ تحديد ثلاثة مستويات هي (منخفض، متوسط، مرتفع)، بناءً على المعادلة التالية:

طول الفئة = (الحد الأعلى للبديل– الحد الأدنى للبديل) ÷ عدد المستويات

(5-1) ÷ 3 =1.33

وبالتَّالي: المنخفض: من (1) أقل من (2.33)، المتوسط: من (2.33) أقل من (3.66). المرتفع: من (3.66) إلى (5).

صدق أداة جمع البيانات:

تم تطبيق صدق المحكمين علي أداة جمع البيانات، وذلك من خلال عرض الاستبيان علي عدد 6 محكمين من الزملاء في أكاديمية سعد العبد الله للعلوم الأمنية بالكويت وزملاء آخرين في كل من: قسم علم الاجتماع والخدمة الاجتماعية بجامعة الكويت، وكلية الخدمة الاجتماعية بجامعة حلوان بمصر، والذين ساهموا في تطوير وتحسين الاستبيان.

ثبات أداة جمع البيانات:

تم استخدام معادلة (كرونباخ– ألفا) لحساب ثبات التَّجانس، وجدول رقم (2) يوضِّح ذلك:

جدول رقم (2)

معاملات ثبات التَّجانس لأداة الدراسة ومجالاتها

الفقرات	المجال	ثبات التَّجانس	عدد الفقرات
1-6	الأوَّل: الجهود التنظيمية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني	0.86	6
7-10	الثَّاني: الجهود الفنية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني	0.90	4
11-13	الثَّالث: الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بدولة الكويت والمؤسسات العربية والدولية.	0.82	3

14-18	الرَّابع: الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني	0.86	5
19-25	الخامس: القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني	0.88	7
26-33	السادس: متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية	0.80	8
	الكليّ	**0.85**	**33**

يظهر من جدول رقم (2) أنَّ معاملات ثبات الاستقرار والتَّجانس الخاصة بأداة الدِّراسة ومجالاتها، تُعتبر مؤشِّرات كافية يمكن اعتمادها أداةً في الدِّراسة في شكلها النِّهائي. إذ ورد في الدِّراسات السَّابقة كمعيار للثبات؛ بلوغُ معامل الثبات نسبةً أكبر من 70%، وبناءً على ذلك تعتبر جميع معاملات الثبات المشار إليها في جدول رقم (5) أعلى من هذه النِّسبة. هذا وقد بين (Miller، 2013)، بأنه إذا كان معامل الثبات أكثر من (70%) يعدّ ثباتاً مرتفعاً، ومن هذا المنطلق تُعتبر معاملات الثَّبات في هذه الدِّراسة عاليةً.

أساليب تفريغ وجدولة وتحليل بيانات الدراسة:

استخدمت الدراسة نظام برنامج الحزمة الإحصائية للعلوم الاجتماعية (الإصدار العشرون)(20SPSS,ver). وتم استخدام المعاملات الإحصائية التالية: التكرارات والنسب المئوية والترتيب والوسط الحسابي والإنحراف المعياري واختبار تحليل التباين الأحادي(One Way ANOVA) واختبار Independent Samples T-Test .

عملية جمع البيانات:

نظرا لما يشهده العالم من انتشار لجائحة كورونا (كوفيد –19) قام الباحث بتوزيع الاستبيان إلكترونياً. كذلك تم توزيع الاستبيان باليد لبعض الضباط، ومجموعة ثالثة تم ارسال الاستبيان علي بعض وسائل التواصل الاجتماعي.

نتائج الدراسة:

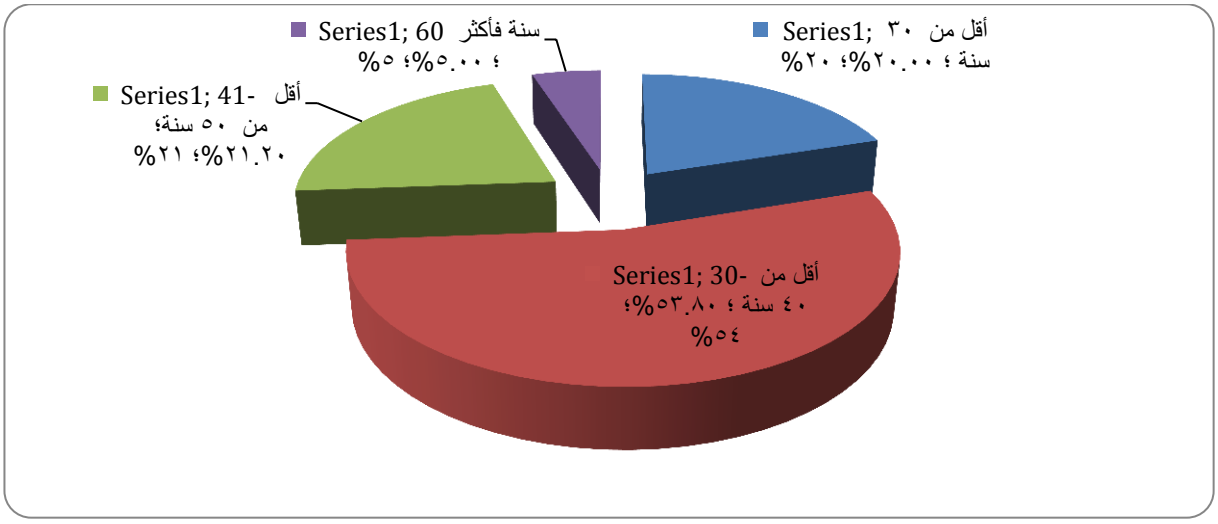
أولا: البيانات الأولية

1- **العُمر:**

جدول رقم (3)
توزيع أفراد عينة الدراسة حسب مُتغيِّر العُمر

العُمر	التَّكرار ك	النِّسبة المئوية %
أقل من 30 سنة	16	20.0 %
30- أقل من 40 سنة	43	53.8 %
41- أقل من 50 سنة	17	21.2 %
60 سنة فأكثر	4	5.0 %
المجموع	**80**	**100%**

يلاحظ من جدول رقم (3) بأنَّ نسبة ذوي الأعمار (30- أقل من40 سنة)، هي النسبة الأعلى، إذ بلغت (53.8 %)، يليها ذوي الأعمار(41-أقل من 50سنة)، بنسبة بلغت (21.2%)، ومن ثم ذوي الأعمار (أقل من 30 سنة بنسبة بلغت (20.0%)، وأخيراً، ذوي الأعمار (60 سنة فأكثر)، بنسبة بلغت (5.0%)، هذا ويبين الشكل رقم (1)، هذه النسب.



شكل رقم (1)

توزيع أفراد عينة الدراسة حسب مُتغيِّر العُمر

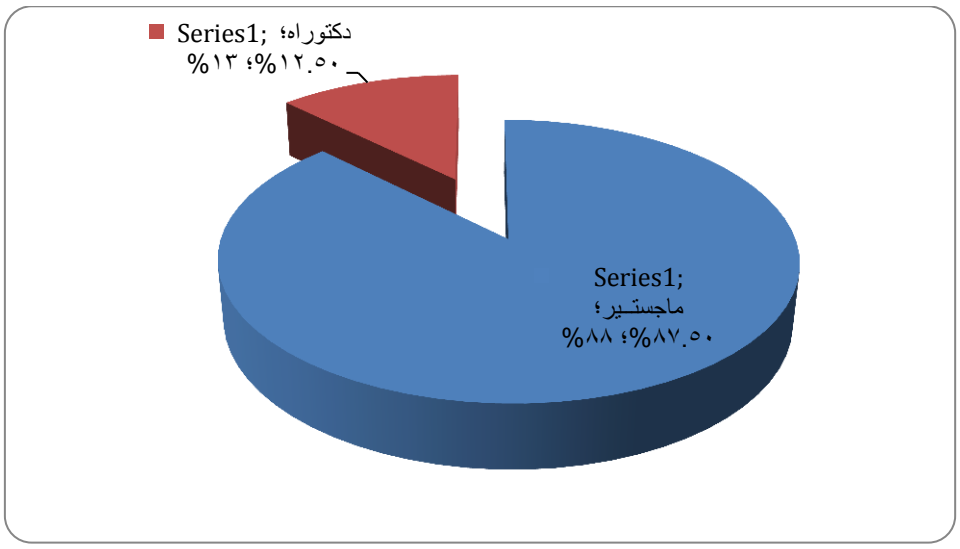
2-المؤهِّل العلميّ:

جدول رقم (4)

توزيع أفراد عيِّنة الدِّراسة حسب متغيِّر المؤهِّل العلميّ

المؤهِّل العلميّ	ك	%
ماجستير	70	87.5 %
دكتوراه	10	12.5%
المجموع	**80**	**100%**

تُظهر بيانات جدول رقم (4) أنَّ النِّسبة الأعلى تعود إلى للحاصلين على (الماجستير)، إذ بلغت نسبتهم (87.5%)، يليهم الحاصلين على شهادة الدكتوراه، بنسبة بلغت(12.5%)، وبهذا فإنَّ الحاصلين على درجة الماجستير هي النسبة الأعلى بهذه الدراسة، هذا ويجب على المؤسسات الوطنية تشجيعهم ودعهم لأجل الحصول على درجة الدكتوراه؛ للاستفادة منهم بالتحول الرقمي وإدارة الأمن السيبراني، هذا ويبين الشكل رقم (2) هذه النسب.



شكل رقم (2)

توزيع أفراد عيِّنة الدِّراسة حسب متغيِّر المؤهِّل العلميّ

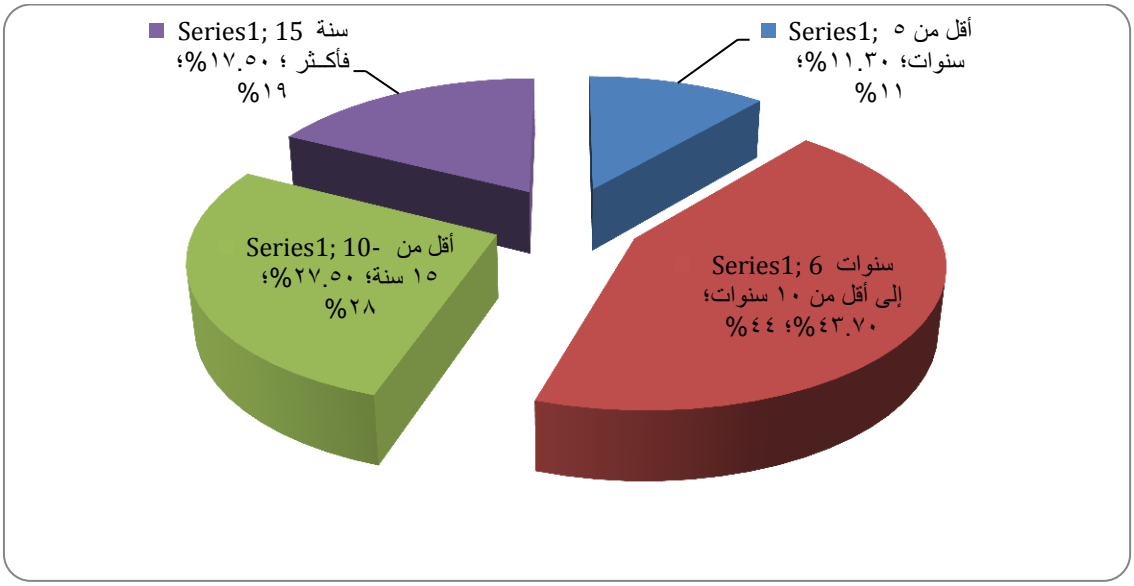
3-الخبرات العملية:

جدول رقم (5)

توزيع أفراد عيِّنة الدِّراسة حسب متغيِّر الخبرات العملية

الخبرات العملية	ك	%
أقل من 5 سنوات	9	11.3 %
6 سنوات إلى أقل من 10 سنوات	35	43.7%
10- أقل من 15 سنة	22	27.5%
15 سنة فأكثر	14	17.5%
المجموع	**80**	**100%**

تُظهر بيانات جدول رقم (5) أنَّ النِّسبة الأعلى تعود إلى لذوي الخبرات المتوسطة (6- أقل من 10 سنوات)، إذ بلغت نسبتهم (43.7%)، يليهم ذوي الخبرات (10- أقل من 15 سنة) بنسبة بلغت(27.5%)، ومن ثم ذوي الخبرات (15 سنة فأكثر)، بنسبة بلغت (17.5 %)، ومن ثم ذوي الخبرات (أقل من 5 سنوات)، بنسبة بلغت (11.3%)، هذا ويبين الشكل رقم (3) هذه النسب.



شكل رقم (3)

توزيع أفراد عيِّنة الدِّراسة حسب متغيِّر الخبرات العملية

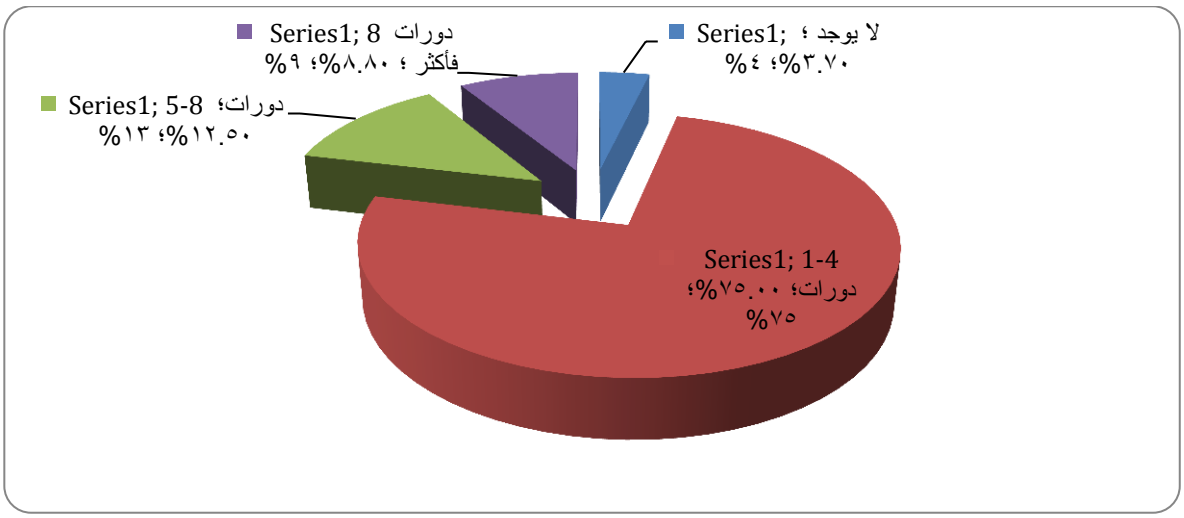
4-الدورات التدريبية:

جدول رقم (6)

توزيع أفراد عيِّنة الدِّراسة حسب متغيِّر الدورات التدريبية

الدورات التدريبية	ك	%
لا يوجد	3	3.7 %
1-4 دورات	60	75.0 %
5-8 دورات	10	12.5 %
8 دورات فأكثر	7	8.8 %
المجموع	**80**	**100%**

تُظهر بيانات جدول رقم (6) أنَّ النِّسبة الأعلى تعود إلى للحاصلين على عدد من الدورات المتوسطة (1-4 دورات)، إذ بلغت نسبتهم (75.0%)، يليهم ذوي الحاصلين على دورات (5-8 دورة) بنسبة بلغت(12.5%)، ومن ثم الحاصلين على دورات (8 دورات فأكثر)، بنسبة بلغت (8.8%)، أما بالنسبة لنسبة لغير الحاصلين على دورات نهائياً، فنسبتهم بلغت (3.7%)، وبهذا يجب تحسين وتطوير مهارات إعداد الضباط من خلال إشراكهم بدورات متخصصة مكثفة مرتبطة بإدارة المعلومات الرقمية و الأمن السيبراني، هذا ويبين الشكل رقم (4) هذه النسب.



شكل رقم (4)

توزيع أفراد عيِّنة الدِّراسة حسب متغيِّر الدورات التدريبية

مناقشة نتائج الدِّراسة:

يمكن تلخيص نتائج الدِّراسة، من خلال الإجابة عن أسئلتها الآتية:

أولاً: النتائج المرتبطة بسؤال الدراسة: ما مستوى تطبيق المؤسسات الوطنية لمتطلبات التحول الرقمي وإدارة الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت؟ وللإجابة عن هذا السؤال تمَّ إيجاد كُلٍّ من الوسط الحسابيّ والانحراف المعياريّ والترتيب، الخّاصة بتفاعل أفراد عيِّنة الدِّراسة مع الفقرات المرتبطة بمجالات الدراسة الستة. وجدول رقم (7) يوضِّح هذه النتائج.

جدول رقم (7)

الوسط الحسابيّ والانحراف المعياريّ والترتيب الخاصُّ بإجابات أفراد العيِّنة المتعلقة "بالسؤال الأوَّل"

الفقرة	المجال	الوسط الحسابي	الانحراف المعياري	التَّرتيب	درجة الموافقة
1	الأوَّل: الجهود التنظيمية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني	3.35	0.663	4	متوسِّطة
2	الثَّاني: الجهود الفنية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني	**3.62**	**0.74**	1	متوسِّطة
3	الثَّالث: الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية	**3.61**	**1.11**	2	متوسِّطة
4	الرَّابع: الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني	**3.39**	**0.90**	3	متوسِّطة
4	الخامس: القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني	**3.10**	**0.54**	5	متوسِّطة
4	السادس: متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية	2.98	0.65	6	متوسِّطة
	البعد الكلي	**3.34**	**0.76**		متوسِّطة

يلاحظ بأنَّ مستوى تطبيق المؤسسات الوطنية لمتطلبات التحول الرقمي والأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت كانت متوسِّطة، إذْ بلغ المتوسِّط الحسابي (3.34)، بانحراف معياري مقداره (0.76)، وبهذا يجب تعزيز السياسات والاستراتيجيات المرتبطة بتحسين متطلبات التحول الرقمي وإدارة الأمن السيبراني، كما يجب أيضا تحفيزهم مادياً ومعنوياً لأجل ذلك. كما وأنَّ المتوسِّط الحسابي لِ " الجهود الفنية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني " أكبر مقارنةً مع المجالات الأخرى، إذ بلغ المتوسِّط الحسابي (3.62)، والانحراف المعياري(0.74)، يليها " الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بدولة الكويت والمؤسسات العربية والدولية" بمتوسِّط حسابي مقداره (3.61)، بانحراف معياري مقداره (1.11)، تليها (الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني) بمتوسِّط حسابي مقداره (3.39)، وبانحراف معياري مقداره (0.90)، تليها " الجهود التنظيمية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني" بمتوسِّط حسابيّ مقداره (3.35)، وانحراف معياري (0.66)، وأخيراً، البعد السادس والمتمثل في " متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية "، بمتوسط حسابي بلغ (2.98)، وانحراف معياري مقداره (0.65). وهذه النتيجة تتطابق مع دراسة (القحطاني، 2019)، إذ بينت بأن مستوى الوعي بالأمن السيبراني كان متوسطاً، كما تختلف مع ما توصلت إليه دراسة (الصحفي وعسكول، 2019)، إذ بيّنت هذه الأخيرة، أنَّ مستويات الوعي بالأمن السيبراني كانت منخفضة.

ويمكن عرض أبعاد الدراسة الستة (الجهود التنظيمية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني، الجهود الفنية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني، الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية، الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني، القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني، متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية) وفقاً للعرض الآتي:

البُعد الأوَّل: الجهود التنظيمية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني:

جدول رقم (8)

المتوسِّط الحسابي والانحراف المعياري ودرجة الموافقة الخاصَّة

ب" الجهود التنظيمية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني"

الفقرة	العبارة	الوسط الحسابي	الانحراف المعياري	(التَّرتيب)	درجة الموافقة
1-	يتم إعداد وتنفيذ إستراتيجية واضحة حول الأمن السيبراني	3.56	0.61	3	متوسِّطة
2-	هناك اتفاقيات شراكة ما بين مركز الأمن السيبراني والجهات الحكومية والخاصة بشأن الأمن السيبراني.	3.75	0.91	1	مرتفعة
3-	تقوم المؤسسات الوطنية بالكويت بتطوير أنظمة الكمبيوتر	3.09	0.92	5	متوسِّطة

	بشكل دوري لتحسين الأمن السيبراني				
4-	تقوم المؤسسات الوطنية بالكويت بمتابعة التطورات في كل ما يتعلق بحماية الأنظمة والشبكات.	3.12	0.75	4	متوسِّطة
5-	توفر المؤسسات الوطنية بدولة الكويت ميزانية لأجل تحسين منظومة التحول الرقمي وتفعيل وتحسين منظومة الأمن السيبراني.	3.59	0.55	2	متوسِّطة
6-	تنظم المؤسسات الوطنية بالكويت دورات تدريبية متخصصة فيما يتعلق بمنظومة التحول الرقمي، وكذلك إدارة الأمن السيبراني لتحسين مهارات عامليه وتطويرها.	3.04	0.24	6	متوسِّطة
	البعد الكليّ	3.35	0.663		متوسِّطة

لقد تباين المتوسِّط الحسابيّ لإجابات أفراد العيِّنة عن العبارات المتعلّقة بمجال " الجهود التنظيمية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني"، إذ تراوح ما بين (3.75– 3.4)، ويُظهر جدول رقم (8) بأنَّ المتوسِّط العام لإجابات أفراد العيِّنة حول هذا المجال، قد بلغ (3.35)، "بدرجة متوسطة"، وأنَّ متوسِّط الانحراف المعياري بلغ (0.663)، وقد حصلت الفقرة (2) على أعلى متوسِّط حسابي (3.75) بانحراف معياري مقداره (0.91) (بدرجة مرتفعة) والتي نصّها " هناك اتفاقيات شراكة ما بين مركز الأمن السيبراني والجهات الحكومية والخاصة بشأن الأمن السيبراني"، تلاه المتوسِّط الحسابي المتعلق بالفقرة (5) والتي نصّها " توفر المؤسسات الوطنية بدولة الكويت ميزانية لأجل تحسين منظومة التحول الرقمي وتفعيل وتحسين منظومة الأمن السيبراني"، والذي بلغ (3.59) بانحراف معياري مقداره (0.55).

وفيما يتعلق بالفقرة (6) والتي نصّها " تنظم المؤسسات الوطنية بالكويت دورات تدريبية متخصصة فيما يتعلق بمنظومة التحول الرقمي، وكذلك إدارة الأمن السيبراني لتحسين مهارات عامليه وتطويرها"، كان متوسطها الحسابي أقلَّ من غيره في باقي العبارات، حيث بلغ (3.04) بانحراف معياري مقداره (0.24) (بدرجة متوسطة). وهذا إن دلَّ على شيء فإنَّه يدُلُّ على أنَّ هناك تنظيم لدورات تدريبية متخصصة فيما يتعلق بمجال إدارة الأمن السيبراني، إلا أنهُ دون المستوى المطلوب، وبهذا فإنه بات من الضرورة بمكان زيادة الاهتمام بإشراك العاملين بدورات تدريبية متخصصة بمجال إدارة الأمن السيبراني والتحول الرقمي.

البعد الثاني: الجهود الفنية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني:

جدول رقم (9)
المتوسِّط الحسابي والانحراف المعياري ودرجة الموافقة لإجابات أفراد العينة الخاصَّة ب" الجهود الفنية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني "

الفقرة	العبارة	الوسط الحسابي	الانحراف المعياري	(الترتيب)	درجة الموافقة
7-	تستخدم المؤسسات الوطنية بالكويت شبكة حماية قادرة على اكتشاف كافة التهديدات.	3.78	0.79	2	مرتفعة
8-	تقوم المؤسسات الوطنية بالكويت بتحديث أنظمة الحماية	3.87	0.75	1	مرتفعة

	بشكل دوري للحدّ من الجرائم المرتبطة بالأمن السيبراني.				
9-	تتناسب برمجيات حماية الأنظمة والشبكات مع طبيعة الأعمال في المؤسسات الوطنية بالكويت .	3.56	0.80	3	متوسِّطة
10-	تطور المؤسسات الوطنية بالكويت قاعدة البيانات وأنظمة الحماية المرتبطة بالأمن والحماية بشكل مستمر ودوري.	3.28	0.63	4	متوسِّطة
	البعد الكليّ	**3.62**	**0.74**		متوسِّطة

تراوح المتوسِّط الحسابيّ لإجابات أفراد العيِّنة على العبارات المتعلّقة بالبعد الثَّاني:"الجهود الفنية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني"، ما بين (3.87–3.28) ويُظهر جدول رقم (9) بأنَّ المتوسِّط العام لإجابات أفراد العيِّنة حول هذا المجال، قد بلغ (3.62)، "بدرجة متوسطة" وأنَّ متوسِّط الانحراف المعياري قد بلغ (0.74)، وأنَّ الفقرة (8) قد حصلت على أعلى متوسِّط حسابي (3.87) وبانحراف معياري مقداره (0.75) (بدرجة مرتفعة)، والتي نصّها "تقوم المؤسسات الوطنية بالكويت بتحديث أنظمة الحماية بشكل دوري للحدّ من الجرائم المرتبطة بالأمن السيبراني"، وهذا جيد ويجب الاستمرار به، تلاه المتوسِّط الحسابي المتعلق بالفقرة (7) والتي نصّها " تستخدم المؤسسات الوطنية بالكويت شبكة حماية قادرة على اكتشاف كافة التهديدات " والذي بلغ (3.78) بانحراف معياري مقداره (0.79).

وفيما يتعلق بالفقرة (10) والتي نصّها " تطور المؤسسات الوطنية بالكويت قاعدة البيانات وأنظمة الحماية المرتبطة بالأمن والحماية بشكل مستمر ودوري"، كان متوسِّطها الحسابي أقلَّ من غيرها، حيث بلغ (3.28) بانحراف معياري مقداره (0.63) (بدرجة متوسطة). وهذا يدلُّ على أنَّها تقوم بتطوير قاعدة البيانات وانظمة الحماية، إلا أنها دون المستوى المطلوب، لذا فإنهُ من الأهمية بمكان القيام على التطوير بشكل دوري ومستمر ؛ إذ أنها مرتبطة بالمنظومة التكنولوجية، والتكنولوجيا كما هو معروف بتطور وتجدد مستمرين، لذا فإن التطوير والتحديث من المسلمات الأساسية والضرورية.

البعد الثالث: الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية:

جدول رقم (10)

المتوسِّط الحسابي والانحرافات المعيارية ودرجة موافقة أفراد العينة الخاصَّة

ب (الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية)

الفقرة	العبارة	الوسط الحسابي	الانحراف المعياري	(الترتيب)	درجة الموافقة
11-	تنسق المؤسسات الوطنية بدولة الكويت بشكل مستمر مع المؤسسات العربية والإقليمية لتذليل لأجل تسهيل التحول الرقمي وكذلك حل المشكلات المرتبطة بإدارة الأمن السيبراني.	3.40	1.19	2	متوسِّطة
12-	تقوم المؤسسات الوطنية بدولة الكويت بالتنسيق مع المؤسسات العامة والخاصة (مزود خدمة الانترنت، ومزودي البيانات) .	3.36	0.89	3	متوسِّطة
13-	تنسق المؤسسات الوطنية بدولة الكويت مع الهيئات الدولية	4.09	1.27	1	مرتفعة

	(الاتحاد الدولي للاتصالات) لأجل الحدّ الجرائم المرتبطة بالأمن السيبراني.				
	البعد الكلي	**3.61**	**1.11**		متوسِّطة

تباين المتوسِّط الحسابيّ لإجابات أفراد العيِّنة عن العبارات المتعلقة ببعد الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية، ما بين (4.09–3.36) ويُظهر جدول رقم رقم (10) أنَّ المتوسط العام لإجابات أفراد العيِّنة فيما يتعلق بهذا البعد قد بلغ (3.61)، "بدرجة متوسطة"، وأنَّ الانحراف المعياري العام بلغ (1.11)، وأنَّ الفقرة (13) حصلت على أعلى متوسِّط حسابي (4.09) وبانحراف معياري مقداره (1.27) (بدرجة مرتفعة) والتي نصّها " تنسق المؤسسات الوطنية بالكويت مع الهيئات الدولية (الاتحاد الدولي للاتصالات) لأجل الحدّ الجرائم المرتبطة بالأمن السيبراني"، تلاه المتوسِّط الحسابي المتعلق بالفقرة رقم (11) والتي نصّها " تنسق المؤسسات الوطنية بالكويت بشكل مستمر مع المؤسسات العربية والإقليمية لتذليل لأجل تسهيل التحول الرقمي وكذلك حل المشاكل المرتبطة بإدارة الأمن السيبراني"، والذي بلغ (3.40) بانحراف معياري مقداره (1.19).

وفيما يتعلق بالفقرة رقم (12) والتي نصّها " تقوم المؤسسات الوطنية بالكويت بالتنسيق مع المؤسسات العامة والخاصة (مزود خدمة الانترنت، ومزودي البيانات)"، كان متوسِّطها الحسابي أقلَّ المتوسِّطات حيث بلغ (3.36) بانحراف معياري مقداره (0.89) (بدرجة متوسطة). وهذا يدلُّ على أنَّ مستوى التنسيق جيِّد، إلا أنَّهُ ليس بالمستوى المَرْجُو؛ لذا يجب أخذ ذلك بعين الاعتبار عند وضع استراتيجيات تطويرية جديدة.

البعد الرابع:الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني:

جدول رقم (11)

المتوسِّط الحسابي والانحرافات المعيارية ودرجة موافقة أفراد العيِّنة الخاصَّة

(الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني)

الفقرة	العبارة	الوسط الحسابي	الانحراف المعياري	(التَّرتيب)	درجة الموافقة
14-	تطور المؤسسات الوطنية بدولة الكويت البنية التحتية اللازمة لأجل تسهيل التحول الرقمي وكذلك تطوير منظومة إدارة الأمن السيبراني.	3.64	0.91	1	متوسِّطة
15-	شبكة المعلومات المستخدمة لدى المؤسسات الوطنية بدولة الكويت قادرة على الحدّ من الجرائم المرتبطة بإدارة الأمن السيبراني.	3.53	0.98	2	متوسِّطة
16-	يتم تطوير شبكة الأنظمة والحماية باستمرار .	3.34	0.95	3	متوسِّطة
17-	تستخدم المؤسسات الوطنية بدولة الكويت كل ما هو جديد	3.21	0.78	5	متوسِّطة

	فيما يتعلق بأنظمة الحماية.				
18-	تتعاون المؤسسات الوطنية بدولة الكويت مع المؤسسات الدولية والعربية للحدّ من اختراق أنظمة الشبكات.	3.24	0.88	4	متوسِّطة
	البعد الكلي	**3.39**	**0.90**		متوسِّطة

تُظهر بيانات الجدول رقم (11) بأنَّ المتوسِّط الحسابيّ لإجابات أفراد العيِّنة على العبارات المتعلقة ببعد "الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني"، كان متراوحًا ما بين (3.64–3.24)، كما ويبيِّن جدول رقم (11) بأنَّ المتوسِّط العام لإجابات أفراد العيِّنة فيما يتعلَّق بهذا البعد قد بلغ (3.39)، "بدرجة متوسِّطة" وبلغ الانحراف المعياري العام (0.90)، وأنَّ الفقرة (14) قد تحصَّلت على أعلى متوسِّط حسابي (3.64) وبانحراف معياري مقداره (0.91)، (بدرجة متوسطة) والتي نصّها " تطور المؤسسات الوطنية بالكويت البنية التحتية اللازمة لأجل تسهيل التحول الرقمي وكذلك تطوير منظومة إدارة الأمن السيبراني"، وهذا جيد ويجب الاستمرار بذلك، تلاه المتوسِّط الحسابي المتعلق بالفقرة رقم (15) والتي نصّها " شبكة المعلومات المستخدمة لدى المؤسسات الوطنية بالكويت قادرة على الحدّ من الجرائم المرتبطة بإدارة الأمن السيبراني"، والذي بلغ (3.53) بانحراف معياري مقداره (0.98).

وأما فيما يتعلق بالفقرة رقم (17) والتي نصّها " تستخدم المؤسسات الوطنية بالكويت كل ما هو جديد فيما يتعلق بأنظمة الحماية" كان متوسِّطها الحسابي أقل المتوسطات حيث بلغ (3.21) بانحراف معياري مقداره (0.78) (بدرجة متوسطة). وهذا يدلُّ على أن تطوير أنظمة الحماية جيد، غير أنَّ ذلك يبقى دون المستوى المطلوب؛ لذا يجب أخذ ذلك بعين الاعتبار وضرورة استخدام كل ما جديد فيما يتعلق بأنظمة الحماية.

البعد الخامس:القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني:

جدول رقم (12)

الوسط الحسابي والانحرافات المعيارية ودرجة موافقة أفراد العينة

نحو (القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني)

الفقرة	العبارة	الوسط الحسابي	الإنحراف المعياري	الترتيب	درجة الموافقة
19-	توجد قوانين وأنظمة لدى المؤسسات الوطنية بدولة الكويت تسمح بتحسين وتطوير إدارة الأمن السيبراني والتحول الرقمي.	3.10	0.62	4	متوسطة
20-	هناك تشريعات وأنظمة لدى المؤسسات الوطنية بالكويت تسهل عملية تبادل المعلومات فيمايتعلق بإدارة الأمن السيبراني مع المؤسسات الإقليمية والدولية.	3.12	0.60	3	متوسطة
21-	يوجد تعليمات وقوانين وتعليمات محددة يتم توجيه المواطنين والمؤسسات على أساسها.	3.10	0.66	5	متوسطة
22-	القوانين والأنظمة والتشريعات الحالية لدى المؤسسات الوطنية بالكويت تسهل من إدارة الأمن السيبراني والتحول الرقمي.	3.23	0.59	1	متوسطة

23-	يتم تطوير القوانين والتشريعات لدى المؤسسات الوطنية بالكويت بشكل دوري ومستمر بما يتواءم مع التحول الرقمي وتطوير إدارة الأمن السيبراني .	3.21	0.58	2	متوسطة
24-	القوانين والتشريعات في الكويت تعتمد التوقيع الإلكترونية في المعاملات الإلكترونية التي تقدمها المؤسسات الإلكترونية.	3.00	0.42	6	متوسطة
25-	القوانين والتشريعات في الكويت تحقق الردع المناسب لأي تهديدات يتعلق بالأمن السيبراني.	2.95	0.35	7	متوسطة
	المجموع الكلي	**3.10**	**0.54**		متوسطة

تباينت المتوسطات الحسابيّة لإجابات أفراد العينة على العبارات فيما يتعلق ببعد القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني، ما بين (3.23–2.95) ويظهر جدول رقم رقم (12) بأن المتوسط العام لإجابات أفراد العينة حول البعد السابق، بلغ (3.10) (بدرجة متوسطة)، كما وبلغ متوسط الإنحراف المعياري (0.54)، وإنّ الفقرة (22) حصلت على أعلى متوسط حسابي (3.23) وبانحراف معياري مقداره (0.59) (بدرجة متوسطة) والتي نصها (القوانين والأنظمة والتشريعات الحالية لدى المؤسسات الوطنية بالكويت تسهل من إدارة الأمن السيبراني والتحول الرقمي)، وبهذا فإن القوانين والتشريعات المرتبطة إدارة الأمن السيبراني تسهل من إدارة الأمن السيبراني والتحول الرقمي، وهذا جيد ويجب تعزيز ذلك، تلاه المتوسط الحسابي المتعلق بالفقرة رقم (23) والتي نصها (يتم تطوير القوانين والتشريعات لدى المؤسسات الوطنية بدولة الكويت بشكل دوري ومستمر بما يتواءم مع التحول الرقمي وتطوير إدارة الأمن السيبراني)، وهذا جيد إلا أنه يجب تعزيز ذلك لأجل حماية البيانات والمعلومات، وبمتوسط حسابي بلغ(3.21) بانحراف معياري مقداره (0.58) (بدرجة متوسطة).

وفيما يتعلق بالفقرة رقم (25) والتي نصها (القوانين والتشريعات في دولة الكويت تحقق الردع المناسب لأي تهديدات يتعلق بالأمن السيبراني) كان متوسطها الحسابي أقل المتوسطات حيث بلغ (2.95) بانحراف معياري مقداره (0.35) (بدرجة متوسطة)، وبهذا فإنه بات من الضرورات الملحة تشديد العقوبة من خلال سن القوانين وتشريعات صارمة، هدفها الأوحد ردع التهديدات المرتبطة بالأمن السيبراني.

البعد السادس: متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية:

جدول رقم (13)
الوسط الحسابي والانحراف المعياري ودرجة الموافقة نحو
(البعد السادس: متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية)

الفقرة	العبارة	الوسط الحسابي	الإنحراف المعياري	الترتيب	درجة الموافقة
26-	الثغرات الأمنية في مجال الأمن السيبراني ترجع إلى الجمهور المستفيدين من خدمات المؤسسات الوطنية لقلة خبرتهم في استخدام الخدمات الالكترونية لدى المؤسسات.	3.17	0.63	1	متوسطة
27-	إدراج مقررات علمية في المدارس والجامعات في مجال الأمن السيبراني يساهم في الحد من التهديدات الالكترونية.	3.02	0.67	4	متوسطة

28-	إعتماد تخصصات علمية بدرجتي الدبلوم والبكالوريوس في مجال الأمن السيبراني يعزز حماية المعلومات لدى المؤسسات الوطنية.	2.85	0.65	7	متوسطة
29-	تقديم برامج توعوية عبر وسائل الاعلام لتبصير الجمهور بأهم التطورات في مجال حماية أمن المعلومات.	3.02	0.70	5	متوسطة
30-	متابعة المجلات العلمية المتخصصة في مجال الشبكات بشكل دوري للاطلاع على أحدث الطرق العلمية في مجال الأمن السيبراني.	3.06	0.66	3	متوسطة
31-	مراجعة البرامج المستخدمة والحماية لدى المؤسسات الوطنية بشكل مستمر لضمان الحماية المطلوبة وسد الثغرات الأمنية.	3.06	0.60	2	متوسطة
32-	إعداد الكوادر الوطنية المؤهلة علمياً وفنياً يساهم في تعزيز الأمن السيبراني في المؤسسات الوطنية.	2.95	0.65	6	متوسطة
33-	الحد من العمالة الوافدة في المؤسسات الوطنية يقلل من فرص الاختراقات الأمنية وحماية أمن المعلومات.	2.75	0.65	8	متوسطة
	المجموع الكلي	**2.98**	**0.65**		

اختلفت المتوسطات الحسابيّة لإجابات أفراد العينة على العبارات فيما يتعلق بالبعد السادس(متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية) ما بين (3.17–2.54) ويظهر جدول رقم (13) بأن المتوسط العام لإجابات أفراد العينة حول هذا البعد، بلغ (2.98) (بدرجة متوسطة)، كما وبلغ متوسط الانحراف المعياري (0.65)، وإنّ الفقرة (26) حصلت على أعلى متوسط حسابي (3.17) وبانحراف معياري مقداره (0.63) (بدرجة متوسطة) والتي نصها (الثغرات الأمنية في مجال الأمن السيبراني ترجع إلى الجمهور المستفيدين من خدمات المؤسسات الوطنية لقلة خبرتهم في استخدام الخدمات الالكترونية لدى المؤسسات)، وبهذا بات من الضرورة بمكان تعزيز خبرة الجمهور باستخدام الخدمات الإلكترونية من خلال عقد ندوات ومؤتمرات متخصصة مرتبطة أمن المعلومات، تلاه المتوسط الحسابي المتعلق بالفقرة رقم (31) والتي نصها (مراجعة البرامج المستخدمة والحماية لدى المؤسسات الوطنية بشكل مستمر لضمان الحماية المطلوبة وسد الثغرات الأمنية)، والذي بلغ (3.06) بانحراف معياري مقداره (0.60) (بدرجة متوسطة)، وهذا جيد، إلا انه يجب تعزيز ذلك ما أمكن لما لهذ من دور أساسي بحماية الشبكة وأمن المعلومات.

أما فيما يتعلق بالفقرة رقم (33) والتي نصها (الحد من العمالة الوافدة في المؤسسات الوطنية يقلل من فرص الاختراقات الأمنية وحماية أمن المعلومات) كان متوسطها الحسابي أقل المتوسطات حيث بلغ (2.75) بانحراف معياري مقداره (0.65) (بدرجة متوسطة)، وبهذا يجب تعزيز الجهود المبذولة لأجل وضع استراتيجية متكاملة للحدّ من المخاطر الإلكترونية والاختراقات الأمنية وحماية أمن المعلومات.

ثانياً: النَّتائج المتعلقة باختبار فرض الدراسة

نصَّ فرض الدراسة على ما يلي:" توجد فروق ذات دلالة إحصائية حول التحول الرقمي وإدارة الأمن السيبراني راجعة لمتغيِّرات (العمر، المؤهل العلمي، الخبرات العملية، الدورات التدريبية)، وفقاً لاستجابات ضباط الشرطة الأكاديميين بالكويت ".

1- العمر:

جدول رقم (14)

نتائج اختبار تحليل التباين الأحادي (**One Way ANOVA**) لفحص دلالة الفروق الخاصَّة ب(العُمر)

الأبعاد	مصدر التباين	مجموع المربَّعات	درجات الحرية	متوسِّط المربعات	قيمة F	الدَّلالة Sig
البعد الأوَّل: الجهود التنظيمية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني	بين المجموعات	1.63	3	0.54	3.21	0.13
	داخل المجموعات	4.73	76	0.16		
	المجموع	6.36	79			
البعد الثَّاني: الجهود الفنية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني	بين المجموعات	0.21	3	1.05	0.25	0.85
	داخل المجموعات	7.62	76	0.27		
	المجموع	7.83	79			
البعد الثَّالث: الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية.	بين المجموعات	1.21	3	0.40	1.22	0.11
	داخل المجموعات	9.19	76	0.328		
	المجموع	10.40	79			
البعد الرَّابع: الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني	بين المجموعات	0.95	3	0.31	0.55	0.65
	داخل المجموعات	16.11	76	0.57		
	المجموع	17.06	79			
البعد الخَّامس: القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني	بين المجموعات	0.92	3	0.31	0.99	0.12
	داخل المجموعات	17.54	76	0.59		
	المجموع	18.46	79			
البعد السادس: متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في	بين المجموعات	0.84	3	0.21	0.45	0.19

المؤسسات الوطنية	داخل المجموعات	17.54	76	0.44		
	المجموع	18.38	79			

يشير جدول رقم (14) إلى أنَّ قيمة (مستوى الدلالة) أكبر من (0.05)، وبما أن قاعدة القرار تُظهر بأنَّه في حال كان مستوى الدلالة أكبر من (0.05)، فإنَّه لا توجد فروقات بين استجابات ضباط الشرطة الأكاديميين بالكويت، وبهذا يتبيَّن لنا عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى دلالة ($\alpha \leq 0.05$)، (حول التحول الرقمي وإدارة الأمن السيبراني راجع لمُتغيِّر العُمر، وفقاً لاستجاباتهم). ومردّ ذلك أنَّ أغلبيَّة عيِّنة الدِّراسة ذوي أعمار متقاربة، وبهذا فَهُم يمتازون بمستويات متقاربة ولا يوجد فروق كبيرة حول التحول الرقمي وإدارة الأمن السيبراني وفقاً لاستجاباتهم، وهذه النتيجة تتطابق مع دراسة (الصحفي وعسكول، 2019)، إذ بينت عدم وجود فروق فيما يتعلق بمتغير العمر، إلا أنها تختلف مع ما توصلت إليه دراسة (القرني، 2007)، إذ بينت بوجود فروق دالة احصائيا لمتغير العُمر.

2- المؤهل العلمي:

جدول رقم (15)

نتائج اختبار **Independent Samples T-Test**

لفحص دلالة الفروق الخاصَّة ب(المؤهل العلمي)

المؤهل العلمي / البعد	ماجستير (n = 70)		دكتوراه (n =10)		قيمة t	مستوى الدلالة (Sig)
	المتوسط الحسابي	الانحراف المعياري	المتوسط الحسابي	الانحراف المعياري		
البعد الأوَّل: الجهود التنظيمية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني	3.850	0.218	3.837	0.215	0.320	0.621
البعد الثَّاني: الجهود الفنية للمؤسسات الوطنية بدولة الكويت لتطوير إدارة الأمن السيبراني	3.824	0.199	3.852	0.212	0.858	0.247
البعد الثَّالث: الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية.	3.788	0.259	3.877	0.175	2.350	0.105
البعد الرَّابع: الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني	3.421	0.354	3.299	0.245	0.311	0.666
البعد الخَّامس: القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني	3.824	0.655	3.645	0.553	0.858	0.244
البعد السادس: متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية	3.788	0.455	3.254	0.144	2.399	0.775

يُظهر جدول رقم (15) أنَّ قيمة (مستوى الدلالة (Sig)) أكبر من (0.05)، وبما أن قاعدة القرار تُظهر بأنَّه في حال كان مستوى الدلالة أكبر من (0.05)، فإنَّه لا توجد فروقات بين استجابات ضباط الشرطة الأكاديميين بدولة الكويت، وبهذا يتبيَّن لنا عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى دلالة ($\alpha \leq 0.05$)، (حول التحول الرقمي وإدارة الأمن السيبراني راجع لمُتغيِّر المؤهل العلمي، وفقاً لاستجاباتهم). ومردّ ذلك أنَّ أغلبيَّة عيِّنة الدِّراسة حاصلين على درجة الماجستير، وبهذا فَهُم يمتازون بمستويات متقاربة ولا يوجد فروق كبيرة حول التحول الرقمي وإدارة الأمن السيبراني وفقاً لاستجاباتهم، وهذه النتيجة تتطابق مع دراسة (الصحفي وعسكول، 2019)، إذ بينت عدم وجود فروق فيما يتعلق بمتغير المؤهل العلمي، إلا أنها تختلف مع ما توصلت إليه دراسة (القرني، 2007)، إذ بينت بوجود فروق دالة احصائيا لمتغير المستوى التعليمي.

3- الخبرات العملية:

جدول (16)

نتائج اختبار تحليل التباين الأحادي (**One Way ANOVA**) لفحص دلالة الفروق الخاصَّة ب(الخبرات العملية)

الأبعاد	مصدر التباين	مجموع المربَّعات	درجات الحرية	متوسِّط المربعات	قيمة **F**	الدَّلالة **Sig**
البعد الأوَّل: الجهود التنظيمية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني	بين المجموعات	1.681	3	0.560	1.067	0.385
	داخل المجموعات	10.500	76	0.525		
	المجموع	12.181	79			
البعد الثَّاني: الجهود الفنية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني	بين المجموعات	.647	3	0.216	0.386	0.765
	داخل المجموعات	11.191	76	0.560		
	المجموع	11.838	79			
البعد الثَّالث: الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية.	بين المجموعات	4.944	3	0.989	3.273	0.110
	داخل المجموعات	23.865	76	0.302		
	المجموع	28.809	79			
البعد الرَّابع: الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني	بين المجموعات	4.316	3	0.863	1.738	0.136
	داخل المجموعات	39.233	76	0.497		
	المجموع	43.548	79			
البعد الخَّامس: القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني	بين المجموعات	6.100	3	1.220	2.424	0.421

	داخل المجموعات	39.755	76	0.503		
	المجموع	45.856	79			
البعد السادس: متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية	بين المجموعات	8.637	3	1.727	5.208	0.211
	داخل المجموعات	26.200	76	0.332		
	المجموع	34.837	79			

يتبين من الجدول رقم (16) بأن قيمة (مستوى الدلالة (Sig)) أكبر من (0.05)، وبما أن قاعدة القرار تُظهر بأنَّه في حال كان مستوى الدلالة أكبر من (0.05)، فإنَّه لا توجد فروقات بين استجابات ضباط الشرطة الأكاديميين بالكويت، وبهذا يتبيَّن لنا عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى دلالة ($\alpha \leq 0.05$)، (حول التحول الرقمي وإدارة الأمن السيبراني راجع لمُتغيِّر الخبرات العملية، وفقاً لاستجاباتهم). ومردّ ذلك أنَّ أغلبيَّة عيِّنة الدِّراسة يملكون خبرات متقاربة، وبهذا فَهُم يمتازون بمستويات متقاربة ولا يوجد فروق كبيرة فيما يتعلق بالتحول الرقمي وإدارة الأمن السيبراني وفقاً لاستجاباتهم، وهذه النتيجة تتطابق مع دراسة (الصحفي وعسكول، 2019)، إذ بينت عدم وجود فروق فيما يتعلق بمتغير سنوات الخبرة، إلا أنها تختلف مع ما توصلت إليه دراسة (القرني، 2007)، إذ بينت بوجود فروق دالة احصائيا لمتغير الخبرة.

4- الدورات التدريبية:

جدول رقم (17)

نتائج اختبار تحليل التباين الأحادي (**One Way ANOVA**) لفحص دلالة الفروق الخاصَّة ب(الدورات التدريبية)

الأبعاد	مصدر التباين	مجموع المربَّعات	درجات الحرية	متوسِّط المربعات	قيمة **F**	الدَّلالة **Sig**
البعد الأوَّل: الجهود التنظيمية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني	بين المجموعات	1.375	3	0.344	1.002	0.411
	داخل المجموعات	27.435	76	0.343		
	المجموع	28.809	79			
البعد الثَّاني: الجهود الفنية للمؤسسات الوطنية بالكويت لتطوير إدارة الأمن السيبراني	بين المجموعات	3.195	3	0.799	1.583	0.187
	داخل المجموعات	40.353	76	0.504		
	المجموع	43.548	79			
البعد الثَّالث: الجهود المرتبطة بالتنسيق ما بين المؤسسات الوطنية بالكويت والمؤسسات العربية والدولية.	بين المجموعات	1.697	3	0.424	.769	0.549
	داخل المجموعات	44.158	76	0.552		
	المجموع	45.856	79			

البعد الرَّابع: الجهود المرتبطة برصد وتقييم التهديدات المرتبطة بإدارة الأمن السيبراني	بين المجموعات	5.524	3	1.381	3.769	0.117
	داخل المجموعات	29.313	76	0.366		
	المجموع	34.837	79			
البعد الخَّامس: القوانين والتشريعات المرتبطة بإدارة الأمن السيبراني	بين المجموعات	2.246	3	0.561	1.514	0.206
	داخل المجموعات	29.677	76	0.317		
	المجموع	31.923	79			
البعد السادس: متطلبات تعزيز الأمن السيبراني وحماية الخصوصية في المؤسسات الوطنية	بين المجموعات	2.063	3	0.413	1.219	0.308
	داخل المجموعات	26.747	76	0.339		
	المجموع	28.809	79			

يتضح من الجدول رقم (17) بأن قيمة (مستوى الدلالة (Sig)) أكبر من (0.05)، وبما أن قاعدة القرار تُظهر بأنَّه في حال كان مستوى الدلالة أكبر من (0.05)، فإنَّه لا توجد فروقات بين استجابات ضباط الشرطة الأكاديميين بالكويت، وبهذا يتبيَّن لنا عدم وجود فروق ذات دلالة إحصائيَّة عند مستوى دلالة ($\alpha \leq 0.05$)، (حول التحول الرقمي وإدارة الأمن السيبراني راجع لمُتغيِّر الدورات التدريبية، وفقاً لتوجهاتهم). ومردّ ذلك أنَّ أغلبيَّة عيِّنة الدِّراسة مشتركين بدورات تدريبية متقاربة، وبهذا فَهُم يمتازون بمستويات متقاربة ولا يوجد فروق كبيرة فيما يتعلق بالتحول الرقمي وإدارة الأمن السيبراني وفقاً لتوجهاتهم، وهذه النتيجة تتطابق مع دراسة (الصحفي وعسكول، 2019)، إذ بينت عدم وجود فروق فيما يتعلق بمتغير الدورات التدريبية، إلا أنها تختلف مع ما توصلت إليه دراسة (القرني، 2007)، إذ بينت بوجود فروق دالة احصائيا لمتغير الدورات التدريبية.

وفي ضوء ما سبق يمكن رفض فرض الدراسة، حيث أنه لا توجد فروق ذات دلالة إحصائية حول التحول الرقمي وإدارة الأمن السيبراني راجعة لمتغيِّرات (العمر، المؤهل العلمي، الخبرات العملية، الدورات التدريبية)، وفقاً لاستجابات ضباط الشرطة الأكاديميين بالكويت ".

ملخص أهم نتائج الدراسة:

1- مستوى تطبيق المؤسسات الوطنية للتحول الرقمي وإدارة الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بدولة الكويت كان متوسطاً.

2- عدم وجود فروق ذات دلالة إحصائية حول التحول الرقمي وإدارة الأمن السيبراني راجعة لمتغيِّرات (العمر، المؤهل العلمي، الخبرات العملية، الدورات التدريبية)، وفقاً لاستجابات ضباط الشرطة الأكاديميين بدولة الكويت.

توصيات الدراسة:

1- ضرورة استقطاب خبرات متخصصة ومحترفة في المؤسسات الوطنية بدولة الكويت، وكذلك زيادة التعاون والتنسيق مع المنظمات الخاصة والإقليمية والدولية فيما يتعلق بالتحول الرقمي والأمن السيبراني.

2- ضرورة حثّ المراكز البحثية والكليات وكذلك الجامعات في دولة الكويت على إنشاء مساقات وتخصصات متخصصة بالتحول الرقمي والأمن السيبراني.

3- ضرورة إشراك الضباط الأكاديميين بالكويت بورش تدريبية فيما يتعلق بالتحول الرقمي ولأمن السيبراني لانعكاساته الإيجابية على تطوير وتحسين مهاراتهم (بغضّ النظر عن العمر والمؤهل العلمي، والخبرات، والدورات التدريبية)، إذ بيّنت الدراسة عدم وجود فروق ما بين الضباط.

4- ضرورة إجراء بحوث ودراسات أخري عن موضوع التحول الرقمي والأمن السيبراني على أن تشمل مجتمعات وعينات أخرى.

5- ضرورة إصدار تشريعات وقوانين رادعة في الكويت تعمد بشكل أساسي على الحدّ من الاختراقات الغير شرعية للحواسيب.

6- تسخير ميزانيات مالية لتطوير قاعدة البيانات وأنظمة الحماية بشكل دوري ومستمر لأجل الحدّ من الاختراقات لهذه القواعد والأنظمة.

7- تعزيز الجهود المبذولة لأجل وضع استراتيجية متكاملة للحدّ من المخاطر الإلكترونية والاختراقات الأمنية وحماية أمن المعلومات.

8- تشديد العقوبة من خلال سن القوانين وتشريعات صارمة، هدفها الأساس ردع التهديدات المرتبطة بالأمن السيبراني.

9- من المؤمل أن تؤخذ النتائج التي توصلت إليها هذه الدراسة بعين الاعتبار لدى المؤسسات الوطنية بدولة الكويت والقطاعات ذات الصلة، عند وضع إستراتيجيات مرتبطة بالتحول الرقمي وتطوير إدارة الأمن السيبراني .

بناء استراتيجية مقترحة:

بعد قيام الباحث بالدراسة النظرية والميدانية السابقة، تبين أن هناك كثير من الاحتياجات التدريبية للضباط الإداريين فيما يتعلق بالتحول نحو الرقمية وإدارة الأمن السيبراني، لهذا قام الباحث بتطوير هذا البرنامج؛ لأجل تحقيق أهداف الدراسة، والمتمثلة في التعريف بأهمية إدارة الأمن السيبراني والتحول الرقمي، وتحديد مهام وأدوار المشاركين والمنظمين في البرنامج، وتحسين مهارات المشتركين نحو الأفضل فيما يخص إدارة الأمن السيبراني.

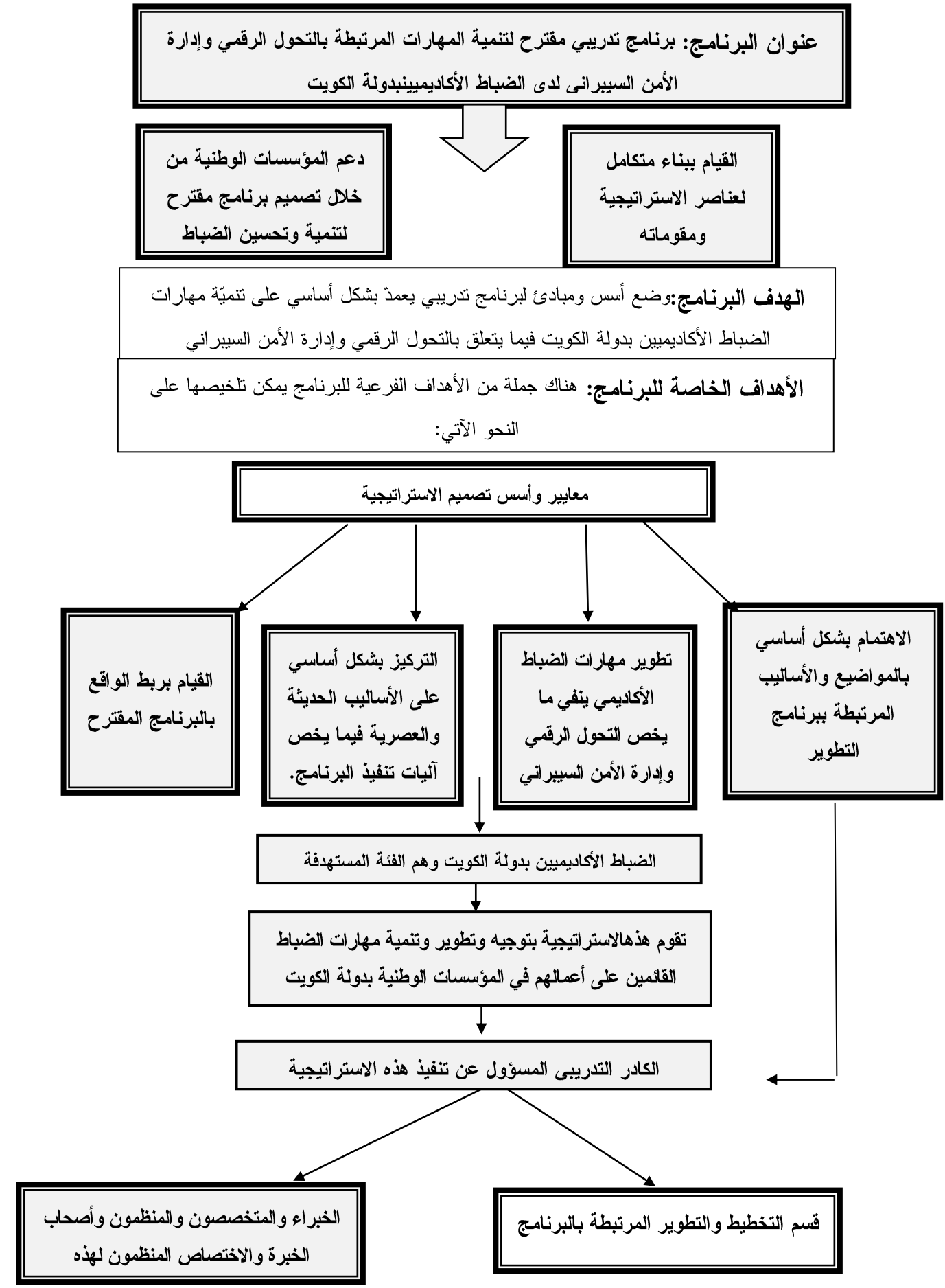
وسيبين الجدول رقم (18) مجموعة من المحاور الأساسية فيما يخص الاستراتيجية المقترحة لتنمية مهارات الضباط الأكاديميين بالكويت.

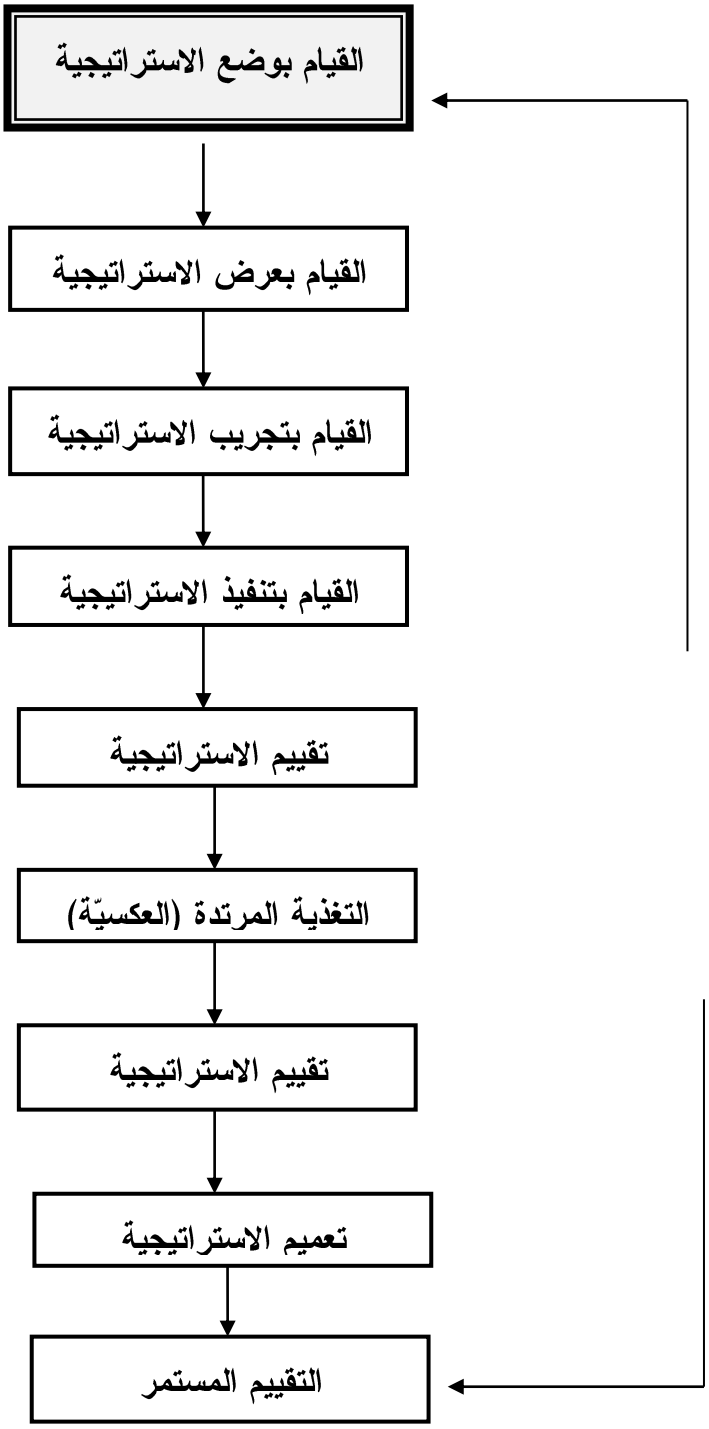
جدول رقم (18)

المحاور الأساسية والعامة للبرنامج المعدّ والمقترح؛ لأجل تنمية مهارات الضباط الأكاديميين بدولة الكويت فيما يتعلق بتحول الرقمي وإدارة الأمن السيبراني

مجالات البرنامج	التنفيذ وآليته
البعد الأول: القيام بتحديد الأهداف المرجوة من البرنامج	تحديد الأهداف المستهدفة، وتقوم اللجنة المختصة بالإعداد للبرنامج برصد الميزانية؛ لأجل القيام بتنفيذ البرنامج، ويتمّ المتابعة والتنسيق؛ لأجل توزيع المهام من خلال الاجتماعات التي سيتمّ عقدها.
البعد الثاني: آلية الدعم اللوجستي (البنية التحتية)	تقوم اللجنة بالتعرف على الضعف فيما يخص الوضع الحالي للضباط الأكاديميين بدولة الكويت، والرؤية المستقبلية؛ لأجل التغلب على هذا الضعف من خلال تحديد الاحتياجات التدريبية فيما يخص بالحدّ من الضعف، وتنمية مكامن القوة لديهم.
المحور الثالث: إعادة الهيكلة والتنمية والتطوير	القيام بتحديد خطوات وآليات العمل من قبل القائمين على وضع الدورات المرتبطة بوضع البرنامج، والقيام على تطويرها وتحديها بما يتواءم مع الاحتياجات المتطورة والمحدثة والمرتبطة بالتحول الرقمي وأمن المعلومات والأمن السيبراني .
المحور الرابع: تنظيم المعلومات وتطويرها	يتمّ تحديد الوقت اللازم؛ لأجل القيام بتطوير هذا البرنامج؛ كما يتمّ توفير المعلومات اللازمة لأجل تنمية مهارات الضباط الأكاديميين بدولة الكويت، ويتمّ تطويع الأساليب الحديثة في ذلك من خلال الربط الإلكتروني، والقيام بالوصول إلى المعلومات والحصول إلكترونيا، ويجب أن يتوفر الدعم من المؤسسات الوطنية بالكويت لأجل تحقيق هذه الأهداف.
المحور الخامس: الارتباط ما بين الضباط والقائمين على التدريب	يجب على الضباط القيام بعملية التوثيق والتدوين لكل ما يحتاجون إليه من أعمال ما قبل الدورة وما بعدها، كما ويجب الدعم المعنوي والمادي للضباط، ويجب الاعتماد على عملية الربط ما بين الواقع والمضمون للدورة، إذ يجب اتباع أسلوب المحاكاة، من خلال اتباع أساليب تدريبية حديثة بهذا المجال، كما يجب ربط هذه الدورة بمقتضيات واحتياج المؤسسات الوطنية بدولة الكويت ذات العلاقة.

ومن خلال الشكل التالي رقم (5)، سيتمّ توضيح الاستراتيجية التدريبي المقترح المهارات المرتبطة بالتحول الرقمي وإدارة الأمن السيبراني لدى الضباط الأكاديميين بالكويت.


عنوان البرنامج: برنامج تدريبي مقترح لتنمية المهارات المرتبطة بالتحول الرقمي وإدارة الأمن السيبرانى لدى الضباط الأكاديميينبدولة الكويت
القيام ببناء متكامل لعناصر الاستراتيجية ومقوماته
دعم المؤسسات الوطنية من خلال تصميم برنامج مقترح لتنمية وتحسين الضباط
الهدف البرنامج:وضع أسس ومبادئ لبرنامج تدريبي يعمدّ بشكل أساسي على تنميّة مهارات الضباط الأكاديميين بدولة الكويت فيما يتعلق بالتحول الرقمي وإدارة الأمن السيبراني
الأهداف الخاصة للبرنامج: هناك جملة من الأهداف الفرعية للبرنامج يمكن تلخيصها على النحو الآتي:
معايير وأسس تصميم الاستراتيجية
الاهتمام بشكل أساسي بالمواضيع والأساليب المرتبطة ببرنامج التطوير
تطوير مهارات الضباط الأكاديمي ينفي ما يخص التحول الرقمي وإدارة الأمن السيبراني
التركيز بشكل أساسي على الأساليب الحديثة والعصرية فيما يخص آليات تنفيذ البرنامج.
القيام بربط الواقع بالبرنامج المقترح
الضباط الأكاديميين بدولة الكويت وهم الفئة المستهدفة
تقوم هذهالاستراتيجية بتوجيه وتطوير وتنمية مهارات الضباط القائمين على أعمالهم في المؤسسات الوطنية بدولة الكويت
الكادر التدريبي المسؤول عن تنفيذ هذه الاستراتيجية
قسم التخطيط والتطوير المرتبطة بالبرنامج
الخبراء والمتخصصون والمنظمون وأصحاب الخبرة والاختصاص المنظمون لهذه



شكل رقم (5)

مخطط مقترح لبرنامج تدريبي مقترح لتنمية المهارات المرتبطة بالتحول الرقمي وإدارة الأمن السيبراني لدى الضباط الأكاديميين بالكويت

بعد ما تمّ عرض الاستراتيجية وخصائصها، سيتم عرض تفصيلي للفئة المستهدفة من هذا البرنامج، وعدد الساعات، وكذلك الامتيازات المترتبة على الاشتراك بهذا البرنامج، وسيتمّ تفصيل ذلك على النحو الآتي:

الفئة المستهدفة: الضباط الأكاديميين بالكويت.

عدد المشاركين: يمكن إشراك ما بين 20–30 مشارك بالدورة.

المدربون: خبراء متخصصون فيما يتعلق بتطوير التكنولوجيا الرقمية وإدارة الأمن السيبراني.

منح المشاركين شهادات معتمدة من قبل: لمركز الذي سيتمّ تدريب الضباط الأكاديميين فيه.

مهام المدرب:

1- التعرف على قدرات الضباط الأكاديميين من حيث الخبرات والمؤهلات والمعلومات والمهارات.

2- شرح الأهداف التدريبية وعرض مكونات البرنامج التدريبي.

3- شرح الاستراتيجية المقترحة لهذا البرنامج والمرتبطة بشكل أساسي بالتحول الرقمي والأمن السيبراني.

4- شرح وتوضيح مفهوم وأهداف وآليات التحول الرقمي والأمن السيبراني.

5- رصد التحديات التي تواجه تحقيق التحول الرقمي والأمن السيبراني.

6- تقديم مجموعة من المقترحات والتوصيات تساهم في مواجهة عمليات تحقيق التحول الرقمي والأمن السيبراني.

Abstract

Digital Transformation of National Institutions and Cybersecurity Challenges from the ic Police Officers in KuwaitView Point of Academ

BY Khaled M. Al-jenfawi

This study aimed to shed light on the digital transformation of national institutions and the challenges of cybersecurity in Kuwait and the researcher followed a descriptive / analytical method during its study. The level of implementation of national institutions for digital transformation and cybersecurity management from the point of view of academic police officers in Kuwait was average.

Also , the study showed that there were no statistically significant differences on digital transformation and cybersecurity management due to variables (age, academic qualification, practical experiences, training courses), according to the responses of the sample.

The study recommended the necessity of conducting new research studies on the topic of cybersecurity management that includes other communities and samples, as well as the need to attract specialized and professional expertise in the national institutions in the State of Kuwait, as well as increasing cooperation and coordination with private, regional and international organizations in relation to cybersecurity management.

Key words: digital transformation, cybersecurity

مراجع الدراسة

أولاً: المراجع العربية

1- أبو النصر، مدحت محمد، (2014)، مناهج البحث في الخدمة الاجتماعية، المجموعة العربية للنشر والتوزيع، القاهرة، مصر.
2- أبو النصر، مدحت محمد، (2020)، " الخدمة الاجتماعية الإلكترونية "، بحث منشور في المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والآداب والعلوم، المجلد الأول، العدد الأول، بنها: أكتوبر.
3- البداينة، ذياب، (2014)، " الجرائم الالكترونية (الأسباب والمفهوم) "،الملتقى العلمي خلال الفترة 2-2014/9/4م.
4- البهي، رغدة (2017)، " الردع السيبراني: المفهوم والإشكاليات والمتطلبات "، مجلة العلوم السياسية، مفعلة على الموقع الإلكتروني: https://democraticac.de.
5- الجنابي، ليلى، (2017)، فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، بحث منشور على الموقع: https://www.ssrcaw.org.
6- الخفاف، مها الطاهر، (2011). مقدمة في نظم المعلومات الإدارية، دار وائل للنشر والتوزيع، عمان، الأردن.
7- السالمي، علاء عبد الرزاق محمد حسن (2005)، الإدارة الالكترونية، دار وائل للنشر والتوزيع، عمان، الأردن.
8- الشيشاني، عامر (2010)، أثر تكنولوجيا المعلومات وتكنولوجيا الاتصالات المتطورة في اكتساب ميزة تنافسية" دراسة ميدانية على الشركة الأردنية للاتصالات الخلوية موبايلكوم(MObileCom)، رسالة ماجستير، غير منشورة، جامعة آل البيت، المفرق.
9- الصحفي، مصباح أحمد وعسكول، سناء صالح (2019). " مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة "، مجلة البحث العلمي في التربية، (10)20، .534-493
10-العلاق، بشير (2014)، التسويق الإلكتروني، دار اليازوري للنشر والتوزيع، عمان، الأردن.
11-القحطاني، نوره (2019). مدى توافر الوعى بالأمن السيبرانى لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية، مجلة شئون اجتماعية، جمعية الاجتماعيين في الشارقة، 36(144)، 85-120

12-القرني، عبد الرحمن (2007)، تطبيقات الإدارة الإلكترونية بالأجهزة الأمنية، رسالة ماجستير غير منشورة، جامعة الملك نايف الأمنية .

13-الوكيل، سامي(2017)، الأمنالسيبراني .. حماية وطنية لأمن الفرد والمجتمع في المملكة، وكالة الأنباء السعودية، متاح على الموقع الإلكتروني: https://www.spa.gov.sa.

14-عبيدات، ذوقان وعدس، عبد الرحمن وعبد الحق، كايد (2001)، البحث العلمي، مفهومه وأدواته وأساليبه، دار الفكر للنشر والتوزيع، عمان، الأردن.

15-ياسين، سعد غالب (2018)، الإدارة الإلكترونية، دار اليازوري للنشر والتوزيع، عمان، الأردن.

ثانياً: المراجع الأجنبية

1- ASM Technologies Limited , (2018), Introduction to Cyber Security, Executive Summary.
2- Compaine, B. (2001),The Digital Divide: Facing a Crisis or Creating a Myth? Cambridge, Mass.: MIT Press.
3- Elmasry, Tarek, Benni, Enrico, Patel, Jigar and Peter aus dem Moore, Jan (2016). Digital Middle East: Transforming the Region into a Leading Digital Economy. McKinsey & Company,(9-23).
4- Galinec,G, Moznik, D Guberina,B (2017), Cybersecurity and cyber defense: national level strategic approach, Automatic Journal, 58(3):273-286.
5- Katherine T, Murphy, L , Smith, J, (2014), Case Studies Of Cybercrime And Its Impact On Marketing Activity And Shareholder Value, Academy of Marketing Studies Journal, http://ssrn.com.
6- Kennedy, C., (2017), The internet of things: The cyber security risks and how to protect against them, https://www.itproportal.com.
7- Mansell, R,(2002), Inside the Communication Revolution: Evolving Patterns of Social and Technical Interaction. Oxford and New York: Oxford University Press.
8- Miller, D (2013) Measurement by the physical educator , Why and Low, (3RD. ED) Indianapolis, Indiana, WM. C. Brown Communication, INC.
9- Moore, M,(2018), Adversarial Tactics, Techniques & Common Knowledge. Welcome to ATT&CK., https://attack.mitre.org/wiki/Main.
10- Nakama, W., Paullet. M. (2018), The Urgency for Cybersecurit Education Impact of Early College Innovation in Hawaii Rural Communities, Professional School Counseling Journal, 9(4), 305-3013.
11- Reddy, N., & Reddy, G. (2020). A Study of Cyber Security Challenges and Its Emerging Trends On Latest Technologies, Peridot Technologies, 26(9), 202-2020.
12- Ribas, C, Massad, E., Burattini, M, Yamamoto, J., (2013) Information security management system: A case study in a Brazilian healthcare organization. https://www.researchgate.net..
13- Saudi Arabian Monetary Authority , (2017), Cyber Security Framework, Saudi Arabian Monetary Authority. .

Sekaran, U. & Bougie, R. (2013).Research Methods For Business: A Skill –Building Approach, 6th. Ed., John Wiley & Sons.