جامعة سوهاج
كلية التربية
المجلة التربوية

متطلبات تحقيق الأمن السيبراني بالجامعات المصرية فى ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس (جامعة بنها أنموذجاً)

إعداد

أ.د/ صلاح الدين محمد توفيق
أستاذ أصول التربية
كلية التربية / جامعة بنها

أ.م. د/ شيرين عيد مرسي
أستاذ أصول التربية المساعد
كلية التربية / جامعة بنها

تاريخ استلام البحث : ٦ نوفمبر ٢٠٢٢م – تاريخ قبول النشر: ٢٣ نوفمبر ٢٠٢٢م

DOI: 10.12816/EDUSOHAG.2023.

مستخلص البحث:

مع تزايد اعتماد المجتمع على تطبيقات التحول الرقمي؛ أصبح المجتمع أمام جرائم متكاملة الأركان تمثل مجموعة من الأنشطة والأعمال غير المشروعة في مكونات الانترنت والتي تعد من أخطر التحديات التي تواجه أمن المعلومات ، وتترك وراءها العديد من الأضرار التي استدعت ضرورة إيجاد تشريعات حول الفضاء السيبراني واستخداماته وقوانين تضبطه ، مع ضرورة توافر تشكيلة متنوعة من الضمانات الأمنية وأنظمة تأمين وحماية تتناسب وطبيعة البيئة الرقمية الجديدة، تبلورت بشكل أساسي في ظهور ما يسمى بالأمن السيبراني الذي أصبح يمثل نهجًا استراتيجيًا للتخطيط والتصميم والتشغيل؛ يتضمن كافة الجوانب التعليمية والاجتماعية والاقتصادية والإنسانية، وله تأثير فعال على المعلومات والحفاظ عليها، كونه يرتبط ارتباطًا وثيقًا بسلامة مصادر الثروة المعلوماتية في عصر التحول الرقمي لكافة المؤسسات ومنها الجامعات، ومن ثم سعى البحث الحالي إلى التعرف على متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس، من خلال استعراض مفهوم الأمن السيبراني ونشأته وأبعاده وأهدافه وأهميته، وتحديد أهم متطلبات تحقيق الأمن السيبراني بالجامعات المصرية فى ظل التحول الرقمي، وأهم المعوقات التي تحول دون تحقيق هذه المتطلبات من وجهة نظر أعضاء هيئة التدريس بجامعة بنها، واستخدمت الدراسة المنهج الوصفي لتحقيق أهدافها، من خلال إعداد استبانة لتعرف أهم متطلبات تحقيق الأمن السيبراني بجامعة بنها فى ظل التحول الرقمي ، على عينة بلغ قوامها ٢٤٨ عضو هيئة تدريس، وتوصل البحث إلى اتفاق العينة على متطلبات تحقيق الأمن السيبراني بجامعة بنها فى ظل التحول الرقمي ، والتي تمثلت في مجموعة من المتطلبات التقنية والمادية والبشرية والمعرفية، ومعوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها.

الكلمات المفتاحية : الأمن السيبراني، متطلبات الأمن السيبراني، الجامعات المصرية، التحول الرقمي.

Requirements for achieving cybersecurity in Egyptian universities from the point of view of faculty In light of the digital transformation members

Abstract

With the increasing reliance of society on digital infrastructure; Society has become faced with integrated crimes that represent a group of illegal activities and actions in the components of the Internet, which is one of the most serious challenges facing information security, and leaves behind many damages that necessitated the need to create legislation about cyberspace and its uses and laws that control it, with the need to provide a variety of safeguards. Security and security and protection systems commensurate with the nature of the new digital environment, essentially crystallized in the emergence of the so-called cyber security, which has become a strategic approach to planning, design and operation; It includes all educational, social, economic and humanitarian aspects, and has an effective impact on information and its preservation, as it is closely related to the safety of information resources in the era of digital transformation for all institutions, including universities. The digital transformation of universities by reviewing the concept of cybersecurity, its origins, dimensions, objectives and importance, and identifying the most important requirements for achieving cyber security in Egyptian universities in light of digital transformation and the most important obstacles that prevent the achievement of these requirements from the point of view of the faculty members at Benha University, the study used the descriptive approach to achieve its objectives, by preparing a questionnaire to identify the most important requirements for achieving cybersecurity at Benha University in light of digital transformation, on a sample of 248 faculty members. Which represented a set of technical, material, human and cognitive requirements, and obstacles to achieving cybersecurity requirements at Benha University.

Keywords: cybersecurity, cybersecurity requirements, Egyptian universities, digital transformation

مقدمة :

يواجه مستقبل الجامعات تحولات مستمرة؛ نظرًا لتزايد الاعتماد على تكنولوجيا المعلومات والاتصالات التي قدمتها الثورة العلمية والتكنولوجية المصاحبة للمجتمعات المعاصرة، مما أنتج أشكالًا جديدة من مفاهيم التعلم في الجامعات، تعتمد على كل من التعلم الافتراضي، والتعلم الرقمي، والتعلم الذكي، الأمر الذي أسفر عن دخول الجامعات في سباق التحدي والاستجابة للتطور الرقمي، وامتلاك بنية تحتية رقمية قادرة على المنافسة عالميًّا في الفضاء السيبراني المستجد المتضمن عددًا لا نهائيًا من الكيانات الافتراضية.

وهو ما دعا إلى ضرورة تبني الجامعات إستراتيجية رقمية واضحة، للتحول نحو هذا المستقبل الرقمي وتطبيقاته المختلفة، خاصة مع توجه الحكومة المصرية إلى تطبيق إستراتيجية التحول الرقمي لمختلف المؤسسات لرفع مستوى أدائها.

وعليه، وجب على الجامعات المصرية ضرورة تطوير أدائها، وتوفير متطلبات التحول الرقمي في جميع مجالاتها، وإثبات قدرتها على استيعاب التكنولوجيا الجديدة، وقبولها، واستخدامها، في ظل التحديات والتغيرات السريعة التي تحيط بها عالميًّا.

ومع تزايد اعتماد المجتمع على تطبيقات التحول الرقمي للجامعات، وتضاعف الاعتماد على المنصات الرقمية ووسائلها، أصبحت التكنولوجيا عرضة للتأثر باحتراف ارتكاب الجرائم الإلكترونية، أو ما يعرف (بالجريمة السيبرانية *Cyber Crime*) والتي اتجه البعض إلى استخدامها لإخافة الآخرين وإخضاعهم. *(يوسف ، ٢٠٠٨، ١٠٧)،(العريان ،٢٠١١، ٢٣)* ، وقد تعددت صورها في اختراق شبكات المعلومات، والتلاعب بالمعلومات وإيذاء المستخدمين والتطبيقات بصور وأساليب متعددة. *(Alkhatani،2020,5)*. كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاتها، وتختلف هجمات الهاكرز باختلاف الجهات والأماكن والأزمنة، مستخدمة أدوات وآليات اختراق متجددة ومتطورة طوال الوقت. *(الصايغ، ٢٠١٩، ٤)*.

وعليه، أصبح المجتمع أمام جرائم حقيقية ومتكاملة الأركان، تتم عن طريق شبكات الإنترنت، وأجهزة الحاسوب بأشكال كثيرة ومتعددة. *(المملكة العربية السعودية، الإستراتيجية الوطنية للأمن السيبراني، ٢٠٢٠، ١٣)، (الشهري ،٢٠١٣، ٢٤٦). (ناصر، ٢٠٢٢، ٨٨)، (فوزي، ٢٠١٩، ١٠١)*، وقد عرّفها مايكل شميت *(Michael, N,1999,13)*، على أنها" مجموعة من الإجراءات التي

تتخذها الدولة للهجوم على نُظم المعلومات المعادية؛ بهدف التأثير عليها والإضرار بها، وفي الوقت نفسه للدفاع عن نُظم المعلومات الخاصة بالدولة المهاجمة.

وتمثل تلك الجرائم السيبرانية مجموعة من الأنشطة والأعمال غير المشروعة وغير القانونية وغير النظامية، الناشئة في مكون أو أكثر من مكونات الإنترنت مثل (المواقع الإلكترونية، وغرف المحادثة، أو البريد الإلكتروني)، *(يوسف،٢٠٠٨، ١١٣)*، والتي تعد من أخطر التحديات التي تواجه أمن المعلومات، خاصة أنها أصبحت تصل لكل فئات المجتمع ومؤسساته، وتترك وراءها العديد والعديد من الخسائر والأضرار . *(Kushzhanov & Aliyev، 2018,94)( ) (Alkaabi,A, 14268) Yan, Z., Xue, Y., & Lou, Y., 2021,1 2.,*

وقد أكدت إحصاءات *(المركز المصري للدراسات الاقتصادية ECES)*، تقدير الخسائر العالمية المتوقعة جراء تلك الجرائم السيبرانية بنحو ٦ تريليون دولار مع حلول عام ٢٠٢١ ، وهو ما يمثل ضعف المبلغ في عام ٢٠١٥، وهذه التكاليف نابعة من الأضرار الكثيرة التي تخلفها الجرائم السيبرانية، ومنها سرقة البيانات، أو تخريبها، وسرقة الأموال، وتعطيل الإنتاجية، واختراق الأنظمة، والإضرار بالسمعة. *(مركز المعلومات ودعم اتخاذ القرار، ٢٠٢٠، ٥).*

كما أشار تقرير *«مؤسسة دبي للمستقبل »* إلى ارتفاع تكلفة مكافحة الجرائم السيبرانية، والتي بلغت(٣) تريليون دولار عام ٢٠٢٠ م، كما أشار التقرير أيضًا إلى تزايد عدد الجرائم الإلكترونية إلى ٣٣ % مع تفشي وباء كورونا عالميًا عام ٢٠٢٠م https://www.dubaifuture.ae/ar/insights/dubai-future-foundations-

كما وصل حجم الإنفاق على أمن المعلومات "الأمن السيبراني" إلى ١٨٠ مليار دولار سنويًّا، طبقا لتقرير إدارة تحالف القطاع الخاص العالمي التابع للأمم المتحدة في ديسمبر ٢٠٢٠ م *(الأمم المتحدة ،٢٠١٩)*، ومن المتوقع أن يصل الإنفاق العالمي على الأمن السيبراني إلى ١٣٣,٧ مليار دولار بنهاية عام٢٠٢٢م *(سليمان،٢١، ٦٢).*

ومن ثم فإن الأمر خطير، يستدعي ضرورة إيجاد تشريعات حول الفضاء السيبراني واستخداماته والقوانين التي تضبطه، مع ضرورة توافر تشكيلة متنوعة من الضمانات الأمنية، وأنظمة تأمين وحماية محكمة، وضرورة توفير مجموعة من الأنشطة أو العمليات تتناسب وطبيعة البيئة الرقمية الجديدة. *(مركز المعلومات ودعم القرار بمجلس الوزراء ،٢٠١٨)*، *(السواط وآخرون ،٢٠٢٠، ٢٧٩)*، فضلًا عن ضرورة اتباع مجموعة من الإستراتيجيات اللازمة والإجراءات والوسائل المستخدمة، للحفاظ على سرية المعلومات الإلكترونية الخاصة بالأفراد والمؤسسات، لمنع

الاختراقات عبر أجهزة الحاسوب والاستخدام غير المصرح به للمعلومات، وتعزيز الحماية التي يبرز دورها بشكل كبير جدًا في عصرنا الحالي الذي يشهد تغيرات متسارعة في مجال أنظمة المعلومات، والاعتماد الكبير على الإنترنت في التعامل، مما يجعله عرضة للتهديدات الخارجية *(اللصاصمه، ومناور، ٢٠٢٢، ٨٣)* **، وكذلك اتخاذ جميع التدابير الأمنية، والمساهمة في الحد من هذه المخاطر.** *(الجنفاوي، ٢٠٢١، ٧٨)، (إبراهيم ،٢٠٢١، ٣٠٠).*

فقد أصبح من الضرورات الملحة، استخدام أنظمة أمن للحماية من هذه المخاطر، تبلورت بشكل أساسي في ظهور ما يسمى (بالأمن السيبراني*cyber security)* **كبعد جديد ضمن أجندة حقل الدراسات الأمنية.**

ويمثل الأمن السيبراني الركيزة الأساسية لأي تحول رقمي للمؤسسات، وهو يعتمد على الاستفادة من التكنولوجيات الرقمية دون خوف، وزيادة فرص الابتكار والتطوير، كما يعدُّ سلاحًا إستراتيجيًا في أيدي الحكومات والأفراد، بل أصبح يمثل نهجًا إستراتيجيًا للتخطيط والتصميم والتشغيل؛ يتضمن جميع الجوانب التعليمية والاجتماعية والاقتصادية والإنسانية، وله تأثير فعال على المعلومات والحفاظ عليها، كونه يرتبط ارتباطًا وثيقًا بسلامة مصادر الثروة المعلوماتية في عصر التحول الرقمي لكل المؤسسات، ومنها الجامعات. *(Kappelman, L. & McLean, E, (2019,32)، (الصانع وآخرون، ٢٠٢٠، ٤٩).* **أي أنه يمثل مجالًا أساسيًّا من مجالات أي تحول رقمي، وهو أحد أهم ركائزه.** *(علام ،٢٠٢١، ٣). (الغامدي ،٢٠٢١ ، ١٤٦)*

وانطلاقا من أن الجامعة لها دور حاسم في تطوير وتقدم المجتمع؛ باعتبارها إحدى المؤسسات التربوية المهمة التي تقع في قمة السلم التعليمي، ويقع عليها العديد من المسئوليات المتعلقة بمواجهة مشكلات المجتمع، وتلبية احتياجاته، فضلا عن أنها تستقبل عددًا كبيرًا من أعضاء هيئة التدريس والطلاب من فئات متنوعة من حيث الفكر، والمستوى الاجتماعي والاقتصادي، كما يمكن أن تقوم بدور مهم في توعية هؤلاء الطلاب وأعضاء هيئة التدريس بماهية الجرائم السيبرانية، وكيفية مكافحة هذا النوع من الجرائم في ضوء التحول الرقمي للجامعات، وهو ما يتطلب ضرورة تطوير التعليم الجامعي بصفة مستمرة، في ظل ما يشهده المجتمع من تحولات تكنولوجية ورقمية، خاصة أن البشرية تستعد الآن للتحول نحو العصر الرقمي الذي ستؤدي فيه أجهزة الحاسب وشبكاته المتطورة دورًا مهمًّا، وما ستحدثه التقنيات وتكنولوجيا الاتصالات من تغيرات جذرية في نظم الحياة بشكل عام *.(الدهشان، والسيد،*

٢٠٢٠، ١٢٥٢). فالجامعات في الوقت الحالي تواجه العديد من التحولات المستمرة الناتجة عن الاندفاع المتزايد نحو التوظيف المكثف لتكنولوجيا المعلومات والاتصالات التي قدمتها الثورة العلمية والتكنولوجية المصاحبة للمجتمعات المعاصرة، (كاعوه، ٢٠٢٠ ، ١٣٧).

وهذا الاندفاع المتزايد نحو التوظيف المكثف لتكنولوجيا المعلومات والاتصالات (الفضاء السيبراني)، والتحول نحو العصر الرقمي، جعل الجامعة عرضة للجرائم الإلكترونية، خاصة مع وجود كادر تعليمي يفتقد المهارات والكفاءات والوعي بالأدوات الأمنية والتخطيط لمفاهيم الأمن السيبراني، مع عدم وجود برنامج لحماية البنى التحتية للمؤسسات التعليمية ومنها الجامعات وبخاصة فى ضوء مبادرات التحول الرقمي في مصر(الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧/ ٢٠٢١، ٥) وبالتالي يحتاج جميع الأطراف داخل الجامعات إلى الدعم والتدريب على مهارات الأمن السيبراني، وتأهيل الكوادر لتكون درعًا لصد الهجمات السيبرانية، لتعزيز أدائهم، وتنمية قدراتهم على التصدي لمخاطر الإنترنت، وبالتالي حماية البنية التحتية الرقمية والقدرة على المنافسة العالمية في مجال الرقمنة.

وهو بالفعل ما سعى إليه العديد من المؤسسات التعليمية، فقد أكد العديد من الدراسات أن هناك حراكًا كبيرًا في العالم أجمع، نحو حماية البنية التحتية الرقمية، وأمن المعلومات والشبكات والأمن السيبراني، من خلال الانضمام لاتفاقيات محاربة جرائم الإنترنت. كما تركز المؤسسات التعليمية على تحقيق أعلى استفادة من تكنولوجيا المعلومات والاتصالات وحماية أنظمتها؛ حفاظًا على سرية بياناتها وحماية الشبكات والأنظمة، فاتجهت نحو تطويع سياساتها وتوعية العاملين بها وتثقيفهم بمتطلبات الأمن السيبراني. (القحطاني، ٢٠١٩)، (الجندي، ومحمد، ٢٠١٩)، (الموجي وآخرون ٢٠٢١)، وعليه تحددت أهمية تعزيز مفهوم الأمن السيبراني، وتحقيق متطلباته بالجامعات في ضوء التحول الرقمي.

وإدراكا لأهمية تعزيز مفهوم الأمن السيبراني، والدعوات المستمرة بضرورة تحقيق متطلباته بالجامعات في ضوء التحول الرقمي لمواجهة الجرائم السيبرانية، فقد اهتم عدد من الباحثين بدراسة آليات تعزيزها بين الشباب الجامعي؛ فقد هدفت دراسة باولوفسكي وجونغ (Pawlowski & Jung ,2015) إلى تعرف مدى وعي طلاب الجامعة بماهية آليات الأمن السيبراني، والأخطار والتهديدات السيبرانية التي قد تلحق الضرر على المستويين الشخصي والمؤسسي، وأوصت بضرورة دراسة الأمن السيبراني ضمن مقدمة نظم المعلومات لطلاب الجامعات، لأنه

يشكل أهميةً تتزايد مع التطور التكنولوجي المتلاحق، وأهمية الاعتماد على تدريسه بطرق متميزة ومبدعة للطلاب في حياتهم الشخصية والمهنية؛ لضمان استمرار تطور المجتمع في ظل أمن سيبراني.

كما اهتمت دراسة رحمن *(Rehman ,2015)* بتحليل واقع أنظمة إدارة الأمن السيبراني في معاهد التعليم العالي بجامعات باكستان، وأوصت بضرورة وجود إدارة للمخاطر والانتهاكات السيبرانية، ووضع سياسات أمنية لمعالجة هذه المخاطر والانتهاكات، مع ضرورة وجود إدارة خاصة بالأمن السيبراني وأمن المعلومات بالجامعات.

وهدفت دراسة مانجولد *(Mangold،2016)* إلى ضرورة إكساب الطلاب الوعي وزيادة معرفتهم بمفاهيم بالأمن السيبراني، وأوصت بإقامة الدورات التدريبية الخاصة بالأمن السيبراني، وإقامة المعسكرات السيبرانية لتلبية الطلب المتزايد على المختصين في الأمن السيبراني، لدى طلاب المراحل الثانوية والجامعات.

كما توصلت دراسة كل من صادقياني *(Sadaghiani ,2018)*، و *(العريشي،٢٠١٨) إلى* أن أبرز أدوار الجامعة في تعزيز ثقافة أمن المعلومات في المجتمع، تتمثل في تنمية الوعي بثقافة الأمن السيبراني، والإسهام في توعية المجتمع بالمخاطر السيبرانية، مع ضرورة مراقبة الطلاب عبر الإنترنت، وأوصت بأهمية إدراج التربية السيبرانية في المقررات والمناهج الدراسية، وتعليم الطلاب ممارساتها الصحيحة.

وتطرقت دراسة نينكيو *(Ninkeu, N. & Buttler, W. ، 2018)* إلى بيان مفاهيم الأمن السيبراني، والانتهاكات السيبرانية التي ينبغي تعزيزها لدى الطلاب الجامعيين، وأظهرت نتائج الدراسة ضرورة تعزيز الأمن السيبراني، وتوعية الطلاب بمفاهيمه ومخاطره المجتمعية، مع ضرورة تحقيق متطلباته.

وهدفت دراسة ناكاما وبول *(Nakama,D & Paulle,k ,2018)* إلى تعليم طلاب الجامعة كيفية التصدي للهجمات السيبرانية في مجتمعات هاواي الريفية؛ وتنمية بعض المهارات لدى الطلاب؛ ليتعلموا كيفية التنقل في نظام إدارة التعلم، وإرسال الرسائل وتلقيها بفعالية بين الطلاب وأعضاء هيئة التدريس، وتوصلت الدراسة إلى ضرورة تنمية مفاهيم الأمن السيبراني لدى طلاب الجامعة عبر المراحل الدراسية بها.

واقترحت دراسة هسي *(Hissi, S. & Haqiq, A.2018)* إطارًا لحوكمة الأمن السيبراني في الجامعات الحكومية بالمغرب، وتوصلت إلى أن استخدام نظام للأمن السيبراني في المؤسسات الأكاديمية سيحقق فوائد متعددة إدارية ومادية وأكاديمية.

وأوصت دراسة ساركر *(Sarker,2019)* بضرورة تعزيز مفاهيم الأمن السيبراني وآلياته، وتوفير متطلباته داخل الجامعات، لحماية البيانات الحساسة والمعلومات والأبحاث العلمية الخاصة بها، مع تثقيف بيئة الجامعة عن الانتهاكات والمخاطر السيبرانية، وتوفير طرق الوقاية من الهجمات السيبرانية.

كما هدفت دراسة مارانجا ونيلسون *(Ma ranga & Nelson ,2019)* إلى تعرف طرق تأمين الجامعات من الهجمات السيبرانية، والآليات التي تتبعها الجامعات في مجال التخطيط لآليات الأمن السيبراني، والتي من أهمها: توعية أعضاء هيئة التدريس والطلاب من خلال البرامج التبادلية بين الجامعات لأعضاء هيئة التدريس والطلاب، وكذلك المؤتمرات والندوات العلمية التي تناقش موضوعات الأمن السيبراني ومفاهيمه، وإمداد إدارة الجامعات بأدوات الحماية الرقمية.

وأكدت دراسة *(القحطاني ،٢٠١٩)* أهمية توفير الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي من وجهة نظرهم، وطرق الوقاية المجتمعية من جرائم الفضاء السيبراني ومعوقاته المجتمعية، وأظهرت نتائج الدراسة أن جريمة "الاحتيال الإلكتروني والنصب" هي أكثر جريمة يتعامل معها الأمن السيبراني، وتعدُّ التوعية الإعلامية أهم طرق الوقاية المجتمعية من مشكلات الفضاء السيبراني.

كما أشار كل من ويجناتو وبراباو *(Wijayanto,H. & Prabowo, 2020)* إلى إن الحاجة إلى الوعي بالأمن السيبراني وتطبيقاته وبرامجه أصبحت أكثر إلحاحًا، في ظل الظروف التي تواجه العالم بأكمله.

وهدفت دراسة ريدمان وجونيور *(Redman, S. & Joiner, 2020)* إلى تنمية الوعي بمفهوم الأمن السيبراني، ولتحقيق ذلك تم إعداد مقرر يدرس مبادئ الأمن السيبراني، وتم تطبيقه على طلاب البكالوريوس في جامعة نيو ساوث ويلز، وكان عنوان المقرر "مقدمة في الأمن السيبراني".

وتوصلت دراسة *(السمحان ،٢٠٢٠)* إلى معرفة متطلبات تحقيق الأمن السيبراني في أنظمة المعلومات الإدارية بجامعة الملك سعود ، وتوصلت إلى أن أهم المتطلبات لتحقيق الأمن

السيبراني، تتمثل في إدراج مجال الفضاء السيبراني ضمن مناهج التعليم الجامعي في المملكة، وتشجيع الاستثمار في مجال الأمن السيبراني.

وأكدت دراسة *(الشهراني، ٢٠٢٠)* أن تثقيف الأجيال الواعدة وتعليمهم مفاهيم الأمن السيبراني التي تتضمن حماية البريد الإلكتروني وحماية البيانات والمعلومات وأمن الأجهزة المحمولة والتشفير، يعد جزءًا أساسيًا من حركة التحول الرقمي.

كما أوصت دراسة موسكال *(Moskal، 2020)* بضرورة الاهتمام بتحقيق متطلبات الأمن السيبراني؛ باعتباره أهم دعائم الاقتصاد الأمريكي وضرورة إنشاء مركز وادارة للأمن السيبراني في الجامعات الأمريكية، يهدف إلى زيادة الوعي بالجرائم والهجمات السيبرانية لتحقيق الأمن في الفضاء السيبراني.

وأشار ليتو *(Lehto,M,2018)* إلى أن على الجامعات تطبيق الأمن السيبراني؛ لحماية البيانات والمعلومات والوثائق المهمة التي تخزن في أجهزتها، وأهمية تدريس الأمن السيبراني في الجامعات؛ لدوره في حماية الأفراد والمؤسسات من المخاطر المختلفة.

وأوصت دراسة روس *(Ross ,2020)* بضرورة توافر الوعي الكافي لدى شرائح المجتمع المختلفة، من أجل حماية البيانات الشخصية، وتعرف السلوكيات الصحيحة للاستخدام الآمن للإنترنت، وتعرف الوجوه المتعددة للجرائم والهجمات السيبرانية، والآثار المترتبة عليها، والتي لا تقف عند حدود الأفراد والمؤسسات، بل تتعداها إلى الدول والحكومات.

كما رأت دراسة *(البيشي، ٢٠٢١)*، أنه من الأهمية توعية الطلاب وأعضاء هيئة التدريس بمتطلبات الأمن السيبراني، ونشرها كثقافة متكاملة؛ حتى يتسنى لكل فرد الحفاظ على بياناته وسريتها، وخصوصيتها، وقدمت الدراسة مجموعة من التوصيات، من أبرزها تخصيص موازنة لتوفير متطلبات الأمن السيبراني وتطبيقاته، وإيلاء مزيد من الاهتمام لبرامج حماية وأمن المعلومات؛ لأثرها في تحقيق ثقة المستفيد الرقمية.

وهدفت دراسة أولفن وفانجين *(Ulven,J & Wangen,2021)* إلى وضع منهجية لمواجهة مخاطر الأمن السيبراني في التعليم العالي، وتعرُّف متطلبات الأمن السيبراني ومصادره، وتوصلت إلى أن الأمن السيبراني له أهمية كبيرة في حماية وأمن المعلومات، وأن هناك تسعة مخاطر إلكترونية حقيقية بحاجة إلى أمن سيبراني.

كما هدفت دراسة ماثيو *(Matthew,M,2021)* إلى تعليم الأمن السيبراني للمراهقين والبالغين غير التقنيين، من خلال تصميم برنامج للتوعية بالأمن السيبراني لديهم، لتوعيتهم بأخطار الأمن السيبراني التي يتعرضون لها ، وتمكينهم من الدفاع عن أنفسهم ضد الهجوم بشكل أفضل، وتوصلت إلى أن الطلاب يتعرضون للعديد من الهجمات الإلكترونية التي تؤثر عليهم بالسلب، كما أشارت إلى وجود مجموعة من الحلول التي يمكن من خلالها التصدي للهجمات الإلكترونية.

وحديثًا سعت دراسة *(فرج، ٢٠٢٢)*، إلى تحقيق العديد من الأهداف، أهمها إلقاء الضوء على دواعي تعزيز ثقافة الأمن السيبراني في ضوء التحول الرقمي بجامعة الأمير سطام بن عبد العزيز، وأوصت بأهمية إذكاء الوعي بالأمن السيبراني لدى الطلاب، وإدراك منافع البرمجيات المتاحة لمكافحة المخاطر السيبرانية، وتصميم حملات للتوعية بالمخاطر السيبرانية.

ويتضح مما سبق تعدد الدراسات التي اهتمت بتعزيز مفهوم الأمن السيبراني وتنوعها، وتوالي الدعوات المستمرة بضرورة تحقيق متطلباته بالجامعات في ضوء التحول الرقمي لمواجهة الجرائم السيبرانية.

وعليه يلزم الاهتمام بالأمن السيبراني؛ باعتباره قضية أمن قومي، وهدفًا ومقومًا أساسيًا لحماية البيانات والشبكات والأنظمة الإلكترونية المختلفة من الهجمات والاختراقات؛ للوصول إلى فضاء إلكتروني آمن وموثوق، كأحد مستحدثات التطورات التكنولوجية والرقمية الحديثة التي نعايشها في عالمنا المعاصر مؤخرا، مع ضرورة توعية الأجيال بأهمية الأمن السيبراني وماهيته، وتحقيق متطلباته التي أصبحت جزءًا أساسيًا من حركة التحول الرقمي وتطويره، وعليه تتضح ضرورة قيام الجامعات بتحقيق متطلبات الأمن السيبراني بها في ضوء التحول الرقمي، وهو ما يستهدفه البحث الحالي.

مشكلة البحث وأسئلته :

في ظل زيادة توجه الجامعات لمواكبة التطور التقني والمعلوماتي، وتغلغل وسائل تقنية المعلومات والاتصالات في نواحي الحياة المختلفة، وفي ظل ما شهدته الجامعات من تحول رقمي شامل لجميع أدوارها، فقد زاد من حجم انتشار البيانات والمعلومات وتبادلها، الأمر الذي ساعد في زيادة حجم الاختراقات وظهور نوع جديد من الجرائم، يختلف إلى حد كبير في شكله ووسائله ومرتكبيه عن مفهوم الجرائم بشكلها التقليدي، وهو ما اصطلح على تسميته بـ *"الجرائم*

السيبرانية "التي تزداد خطورتها بزيادة عدد مستخدمي هذه التقنيات يومًا بعد يوم، وعليه أصبح الفضاء السيبراني بيئة خصبة لتلك الجرائم السيبرانية والهجمات الإلكترونية التي تخطت خسائرها (١) تريليون دولار في عام ٢٠٢٠ م، ووصلت إلى (٦) تريليون دولار في ٢٠٢١م، ومن المتوقع أن يتكبد العالم خسائر تقدر بحوالي ١٠.٥ تريليون دولار بحلول ٢٠٢٥م، من قبل المتسللين السيبرانيين، سواء كانوا أفرادا أو مجموعات منظمة إلى جانب النشاطات الإرهابية الممولة من قبل بعض الدول، نتيجة للطابع المفتوح لتلك الساحة الافتراضية، وعدم وجود رقابة قانونية محكمة عليها. *(تقرير مجلس الوزراء المصري ودعم اتخاذ القرار ،٢٠٢٠، ١٣)*

وتأكيدا لذلك، أشارت المعلومات الصادرة عن الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧/٢٠٢١)، أنها تعاملت مع كم هائل من التحديات والأخطار السيبرانية التي تمثلت في: خطر الإرهاب والحرب السيبرانية، وخطر اختراق وتخريب البنى التحتية للاتصالات وتكنولوجيا المعلومات، وخطر سرقة الهوية الرقمية والبيانات الخاصة *(الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧/ ٢٠٢١، ٦)*

الأمر الذي فرض تحديات على مختلف مؤسسات التعليم خاصة الجامعي، ودفع كثيرًا من تلك المؤسسات إلى وضع آليات لتحقيق متطلبات الأمن السيبراني، وتأمين أنظمة البيانات والمعلومات بها، وضرورة حماية قواعد هذه البيانات وأنظمتها من تلك الاختراقات.

وهو ما أوصت به دراسة *(كاعوه ،٢٠٢٠)* من حيث تضمين سياسات الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي للجامعات، مع تكثيف الاهتمام بتوعية تلك الجامعات بتطبيق معايير أمن المعلومات؛ من أجل القدرة على مواجهة أي هجوم محتمل، أو دخول غير مصرح به على أنظمة المعلومات.

وذلك بناء على ما توصلت إليه من تزايد الاعتماد على الخدمات الرقمية في التواصل والعمل عن بعد، مما يتسبب في تعرض الجامعات للاختراقات المختلفة والمخاطر السيبرانية المتعددة، فضلا عن عدم وجود سياسات واضحة للأمن السيبراني أو برامج حماية مناسبة.

كما أوصت دراسة *(شعبان، ٢٠٢١)* بضرورة تعرُّف دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، وتوصلت نتائجها إلى تقديم تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، وأوصت بضرورة التوعية بالأمن السيبراني من خلال التدريس، وتشجيع

البحث العلمي في مجال الأمن السيبراني، وتوضيح ضرورة إنشاء إدارة مختصة بأمن المعلومات، وذلك بناء على ما توصلت إليه من وجود ضعف معرفي بجامعة القاهرة عن تكنولوجيا المعلومات وفي سياسات حماية أنظمة المعلومات والبيانات، والافتقار لإدارة خاصة تتعلق بأمن المعلومات بجامعة القاهرة، بالإضافة إلى قلة الخبرة والوعي والتدريب للفنيين والموظفين بنظم المعلومات، مما أدى إلى حدوث مخاطر عديدة تتعلق بالاختراقات الأمنية والتهديدات المستمرة لأنظمة الجامعة.

وقد أثار العدد المتزايد لهذه الجرائم السيبرانية قلق العديد من الباحثين والممارسين؛ مما حدا بهم لتأكيد الحاجة الملحة لمزيد من المتخصصين في مجال الأمن السيبراني، للحفاظ على كفاءة أمن المعلومات وفاعليته في المؤسسات التعليمية، ومنها الجامعات.

ولهذا تبرز أهمية الدراسة الحالية، في كونها تسعى لتوضيح المتطلبات التي تحقق الأمن السيبراني في الجامعات المصرية عامة وجامعة بنها خاصة، حتى يمكن المحافظة على معلوماتها الإلكترونية مستقبلًا، ويجعلها تحس بالأمن والاستقرار وعدم الخوف من أي قرصنة على مواقعها الإلكترونية، والحفاظ على سريتها وتحصينها من أي تخريب أو اختراق إلكتروني.

وعليه، تأتي هذه الدراسة لمعرفة متطلبات تحقيق الأمن السيبراني بالجامعات المصرية، في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس، مع الأخذ في الحسبان ملاءمة هذه المتطلبات للإمكانيات المتاحة والمتوفرة، وعليه يمكن بلورة مشكلة الدراسة في السؤال الرئيس الآتي:

ما متطلبات تحقيق الأمن السيبراني بجامعة بنها فى ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس ؟

ويتفرع من السؤال الرئيس مجموعة من الأسئلة الفرعية، هي:

١. ما الإطار المفاهيمي للتحول الرقمي للجامعات المصرية.
٢. ما الإطار الفلسفي للأمن السيبراني؟
٣. ما المتطلبات المختلفة لتحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي؟
٤. ما معوقات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي؟

٥. ما واقع ملاءمة تحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس؟

٦. ما دلالة الفروق بين متوسطات درجات أفراد العينة من أعضاء هيئة التدريس ؟

٧. ما التصور المقترح لتحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي؟

أهداف البحث:

هدف البحث الحالي إلى:

١– تحليل الإطار المفاهيمي للتحول الرقمي للجامعات المصرية.

٢– تحديد الإطار الفلسفي للأمن السيبراني من حيث مفهومه، وأهدافه، وأبعاده، وخصائصه.

٣– تعرُّف المتطلبات (التقنية والمادية والبشرية والمعرفية) لتحقيق الأمن السيبراني بالجامعات.

٤– الكشف عن معوقات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي.

٥– توضيح مدى ملاءمة تحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات من وجهة نظر أعضاء هيئة التدريس.

٦– تعرُّف دلالة الفروق بين متوسطات درجات أفراد العينة من أعضاء هيئة التدريس.

٧– وضع تصور مقترح لتحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي.

أهمية البحث:

تتحدد أهمية البحث في النقاط الآتية:

١. الرغبة في التحول نحو تطبيق متطلبات الأمن السيبراني، وما سيحققه من فوائد في الجامعات في تأمينها من الجرائم التي تواجهها، وسرعة تفادي أي أخطار قد تضر بها.

٢. تنمية الوعي بتقنية المعلومات وتعرُّف جوانبها الإيجابية والسلبية لدى أعضاء هيئة التدريس بجامعة بنها لمواجهة الجرائم الإلكترونية.

٣. تعزيز الأمن السيبراني لدى جميع فئات المجتمع بشكل عام، في ظل الثورة المعلوماتية والتدفق الهائل للمعلومات في العصر الرقمي.
٤. توعية المسئولين بالجامعة بالمنافع التي تواكب التحولات التي يسعى إليها مختلف الجامعات في هذا الجانب المهم في تحقيق الأمن السيبراني، وتحديد مدى الاستجابة لمتطلبات العصر وتحدياته.
٥. مساعدة المسئولين بالجامعة في تحقيق سرية المعلومات وخصوصيتها، والحفاظ على سلامة البيانات بشكل مستمر ولفترة طويلة.

منهج البحث وأدواته:

اعتمد البحث الحالي على المنهج الوصفي الذي يقوم على وصف الظاهرة كما هي في الواقع وتحليلها وتفسيرها، ثم الوصول إلى استنتاجات ودلالات ذات مغزى، والاستعانة بالأدبيات والدراسات السابقة المتعلقة بموضوع البحث، حيث يعد المنهج الوصفي هو الأمثل لاستطلاع آراء أعضاء هيئة التدريس حول مدى ملاءمة تحقيق متطلبات الأمن السيبراني بجامعة بنها، ومن ثم وضع تصور مقترح لتحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات.

ووفقًا لطبيعة البحث ومنهجه، تم الاعتماد على الاستبانة كأداة رئيسة لجمع البيانات، والتي تغطي جوانب وأبعاد موضوع البحث، لتعرف آراء عينة من أعضاء هيئة التدريس حول مدى ملاءمة متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي.

حدود البحث:

اقتصر البحث الحالي على الحدود الآتية:

الحد الموضوعي: يتمثل في دراسة المتطلبات اللازمة لتحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي، من خلال رصد وجهات نظر أعضاء هيئة التدريس في ذلك، ووضع تصور مقترح لتلبية تلك المتطلبات.

الحد البشري: ويتمثل في أعضاء هيئة التدريس بجامعة بنها (مدرس، أستاذ مساعد، أستاذ) بكليات الجامعة، وقد اقتصر البحث على عينة عشوائية بسيطة، بلغ قوامها (٢٤٨)

عضو هيئة تدريس، يمثلون نسبة (١٠ %) من المجتمع الأصلي الذي بلغ نحو (٢٤٥٦) عضو هيئة تدريس *(الإدارة العامة لمركز المعلومات والتوثيق بوزارة التعليم العالي، ٢٠٢١)*.

الحد الزمني: تم البدء في إجراءات الدراسة الميدانية مع بداية مارس من العام ٢٠٢٢، واستمرت حتى الانتهاء من تلك الإجراءات.

مصطلحات البحث:

اشتمل البحث الحالي على المصطلحات الآتية:

الأمن السيبراني *(Cyber Security)*

الأمن: هو حصيلة إجراءات وتدابير تحمي من الأخطار وهي من الحاجات البشرية الأساسية.

السيبراني: أصلها كلمة يونانية مأخوذة من كلمة ***cyber*** والمشتقة من ***cybernetics*** ، وقد ظهرت حديثا في قواميس اللغة الإنجليزية، وتعني باللغة العربية (إلكتروني) وتشمل كل ما يتصل بأجهزة الكمبيوتر وتكنولوجيا المعلومات والواقع الافتراضي.

وتعرف إجرائيا بأنها: كل ما يرتبط بتقنية المعلومات والحاسب الآلي، ويقصد بها فضاء الإنترنت، أو العالم الافتراضي الذي يولَج إليه عبر شبكات الإنترنت المترابطة والمفتوحة للجميع.

الأمن السيبراني: يعرف إجرائيا بأنه: جميع الإجراءات والوسائل التقنية والتدابير والجهود التي ينبغي أن توفرها جامعة بنها لأعضاء هيئة التدريس بها، بهدف حماية المصادر المختلفة من (البرمجيات والأجهزة المحمولة، والبيانات الرقمية الشخصية) من التجاوزات والتدخلات غير المشروعة أو سوء الاستغلال، ومقاومة محاولات الاختراق أو الحوادث غير المتوقعة، وتعزيز خصوصيتها وتشفيرها، واتخاذ إجراءات حماية أعضاء هيئة التدريس من مخاطر الفضاء السيبراني.

وتعرف متطلبات الأمن السيبراني إجرائيا بأنها: "مجموعة من الشروط والمستلزمات الضرورية اللازمة لتحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي".

التحول الرقمي للجامعة *(University Digital Transformation)*

يعرف التحول الرقمي في الدراسة الحالية إجرائيًا بأنه "عملية تحويل الجامعات التقليدية إلى جامعات رقمية، وهو ما يعتمد بشكل أساسي على التقنيات الرقمية، من خلال الاستخدام المكثف لتكنولوجيا المعلومات والاتصالات داخل الجامعة، في ضوء مجموعة من المتطلبات

المادية والبشرية والمعرفية والتقنية المختلفة، بالإضافة إلى المتطلبات اللازمة لمواجهة الهجمات الإلكترونية، والحد من اختراق شبكات المعلومات والتلاعب بالمعلومات وإيذاء المستخدمين بصور وأساليب متعددة".

خطوات البحث:

لتحقيق أهداف البحث الحالي، سارت خطواته وفق المحاور الآتية:

المحور الأول: الإطار المفاهيمي للتحول الرقمي للجامعات المصرية.

المحور الثاني: الإطار الفلسفي للأمن السيبراني.

المحور الثالث: متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي.

المحور الرابع: معوقات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي.

المحور الخامس: واقع ملاءمة تحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي من وجهة نظر أعضاء هيئة التدريس.

المحور السادس: تصور مقترح لكيفية تحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي.

المحور الأول: الإطار المفاهيمي للتحول الرقمي للجامعات.

تتجه معظم حكومات عالم اليوم إلى تطبيق إستراتيجية التحول الرقمي في جميع مؤسساتها، لرفع مستوى الخدمات وجودة الأداء، وبالنسبة للجامعات فإن التحول الرقمي يمثل القضية الأكثر أهمية في ضوء الاقتصاد الرقمي الذي يعيشه العالم في الوقت الحالي، ويمكن تناول الإطار المفاهيمي للتحول الرقمي للجامعات من خلال ما يلي:

أولا – مفهوم التحول الرقمي للجامعات

لا يوجد تعريف ثابت للتحول الرقمي؛ لأن المصطلح يستخدمه الكثيرون لأسباب كثيرة، ومن زوايا عديدة، لدرجة أنه أصبح مصطلحا شاملًا يستخدم في الصحة، والصناعة، والتجارة، والتعليم وغيرها من المجالات، لذا تناوله العديد من الباحثين بالتعريف، وفيما يلي توضيح ذلك:

عرفه البعض على أنه عملية مدعمة بالتقنيات الرقمية، والتي تحدث تغيرات في المؤسسات، ولها تأثير هائل على التقييم التنظيمي عن طريق الإنترنت، وتحليل البيانات

الضخمة والحوسبة السحابية، وتقنيات الهاتف المحمول والذكاء الاصطناعي.(2021,1530 *Feroz, A. & Chiravuri, A.)*

بينما يعرفه البعض على أنه تطبيق التكنولوجيا الحديثة، لبناء نماذج أعمال جديدة وبرامج وعمليات من شأنها أن تؤدي إلى مزايا تنافسية جديدة، وتحقيق كفاءة أعلى *(Vial،G, 2019,121).*

في حين قد يشير التحول الرقمي إلى قدرة مؤسسات التعليم الجامعي على إدراك عمليات متطورة وحديثة، تستهدف إحداث تغيير نوعي، للانتقال من النظم التقليدية للنظم الحديثة التي تعتمد بشكل كامل على التكنولوجيا والتقنيات الحديثة، بما يحقق أداءً وظيفيًّا متميزًا. *(سبع،٢٠٢١ ، ٢٨).*

فالتحول الرقمي عملية تؤثر بشكل كبير على جميع أنشطة مؤسسات التعليم الجامعي، يتخلل ذلك جميع العمليات والأماكن والأشكال والأهداف الخاصة بالتعليم والتعلم والبحث في مجال التعليم الجامعي *(Ismail, M. & Zaki, M. 2017,7)*

كما يشمل هذا التحول الرقمي تطوير بنى تحتية جديدة، وزيادة استخدام الوسائط الرقمية والتقنيات في التعليم والتعلم والبحث، وخدمات الدعم والإدارة والاتصال، بالإضافة إلى تطوير المهارات الرقمية لكل عناصر منظومة التعليم الجامعي من طلاب وموظفين وأعضاء هيئة التدريس *(Rampelt, F.& Knoth, A. 2019,3)*

كما يُقصد به: عملية الانتقال من الاتجاهات التعليمية التقليدية الحالية إلى الاتجاهات التعليمية المستقبلية التي تركز على إنتاج المعرفة وابتكارها، وتوجيه التعليم نحو التعلم الذاتي والمستمر، والتركيز على المعرفة بالممارسة ونشرها عبر الإنترنت، وذلك من خلال نظام إداري يخضع للمساءلة والتقويم والمشاركة المجتمعية *(عبد الله،٢٠٢١، ١٠٧٩).*

كما يعرف بأنه: نوع التعليم الذي يحقق الاتصال والتواصل بين الطلاب والمعلمين إلكترونيا، من خلال شبكة أو شبكات إلكترونية تعليمية، وذلك بتوفير متطلبات التعليم الرقمي التعليمية، والتقنية، والتخطيطية. *(الشريف،٢٠٢١، ٣٦٠٥)*

ويشير مفهوم التحول الرقمي في الجامعة إلى: قدرة مؤسسات التعليم الجامعي على الانتقال من نظام تقليدي إلى نظام رقمي قائم على تكنولوجيا المعلومات والاتصالات، في جميع مجالات العمل الجامعي، بما يحقق أداءً وظيفيًّا متميزًا، ويعزز الميزة التنافسية لهذه المؤسسات، ويتمثل التحول الرقمي بمؤسسات التعليم الجامعي في مدى توافر (البنية

الأساسية لشبكات المعلومات، والتعليم الرقمي، والتدريب على تكنولوجيا المعلومات، والمكتبات الرقمية). *(منصور، ٢٠٢١، ١٧٣).*

✓ **<u>وبناء على ما سبق، يمكن تحديد مفهوم التحول الرقمي في الجامعات فيما يأتي:</u>**

- **الاستخدام المكثف للتكنولوجيات الرقمية، سواء في آلية التواصل أو التعليم عن بُعد، لإنتاج بيانات ومعلومات ذات أهمية كبيرة في البنية التحتية الخاصة بها.**
- **الاعتماد على التطبيقات التكنولوجية والتقنيات الحديثة في تنفيذ العمليات التعليمية والإدارية.**
- **وجود بنية تحتية تكنولوجية وأجهزة اتصالات حديثة، تمكن الجامعة من تقديم خدماتها بشكل إلكتروني عبر شبكة الإنترنت.**
- **شمولية التحول لكل عناصر الجامعة، من أعضاء هيئة تدريس وطلاب وإداريين ومحتوى وأساليب تقويم، فالتحول الرقمي ليس هدفا في حد ذاته، وإنما وسيلة للتطوير الجامعي والتكيف مع مستجدات العصر.**

وعليه، يلاحظ أن التحول الرقمي يعنى أكثر من مجرد استخدام الحاسبات والتجهيزات التكنولوجية، فهو أساليب منظمة في التفكير والمنهجية العلمية في تحليل المشكلات، والهدف الأساسي من تطبيق التحول الرقمي يكمن في تطوير التعليم وتحسين أساليب التعلم والتدريس؛ لضمان الحصول على نتائج أكثر فاعلية، والإسهام في الارتقاء بمهارات التعلم لدى الطلاب، ومساعدتهم على الابتكار والإبداع، والوصول إلى أعلى معدلات الجودة في التعليم.

بينما تعرفه الدراسة الحالية إجرائيا بأنه: "عملية تحويل الجامعات التقليدية إلى جامعات رقمية، والتي يعتمد بشكل أساسي على التقنيات الرقمية خلال الاستخدام المكثف لتكنولوجيا المعلومات والاتصالات داخل الجامعة، في ضوء مجموعة من المتطلبات المتمثلة في وضع إستراتيجية للتحول الرقمي، ونشر ثقافة التحول الرقمي، بالإضافة إلى المتطلبات اللازمة لمواجهة الهجمات الإلكترونية، والحد من اختراق شبكات المعلومات والتلاعب بالمعلومات وإيذاء المستخدمين بصور وأساليب متعددة".

ثانيا - أهداف عملية التحول الرقمي في التعليم الجامعي

يحقق التحول الرقمي عددا من الأهداف الجوهرية في التعليم الجامعي، منها: *(عبد الحميد، ٢٠٢١، ١٤٠). (المطرف، ٢٠٢٠، ١٦٥)*

١. **نشر ثقافة التحول الرقمي، وبناء العقلية الرقمية لدى كل من قيادات وأعضاء هيئة التدريس والطلاب والموظفين داخل الجامعات.**
٢. **امتلاك الجامعة بنية معلوماتية متطورة تمكنها من ممارسة نشاطها عبر شبكة الإنترنت محليا ودوليا.**
٣. **تحسين طرق الاتصال بين الجهات الإدارية والأكاديمية والمسئولين داخل وخارج الجامعة، وتوفير بناء تنظيمي شبكي يسهّل التواصل مع الأفراد والمؤسسات محليا وعالميا.**
٤. **توطيد ثقافة صنع القرار القائمة على البيانات؛ وهذا يتضمن تبني فكر رقمي للطلاب وأعضاء هيئة التدريس والقياديين والموظفين في الجامعة.**
٥. **تحسين مقاييس الطلاب، مثل: معدلات الاحتفاظ ومعدلات التخرج ومعدلات النجاح في الدورات التعليمية والتدريبية، وغيرها من مختلف مؤشرات النجاح الأخرى، مما يعزز خبرات الطلاب التعليمية.**
٦. **تعزيز التنافسية في التعليم الجامعي وتحفيز مؤشراتها، من خلال اعتماد الطرق الرقمية كمعيار أساسي للتميز.**
٧. **تحسين موارد الجامعات ورفع كفاءتها، وهذا يشتمل جميع الإجراءات بالجامعة، بدءًا من تحسين عملية الاتصال بين المسئولين إلى خفض تكاليف استخدام الطاقة.**

وهنا يمكن القول بأنه لكي تتمكن أي جامعة من تحقيق إستراتيجية تحول رقمي ناجح؛ فإن ذلك يتطلب وضع أهداف محددة وواضحة تسير في ضوئها، خاصة أن التحول الرقمي يمكن أن يدعم التعليم الجامعي للتحول من السؤال عن المستقبل إلى التنبؤ به وتشكيله، واتخاذ قرارات استباقية ومستنيرة، واتخاذ إجراءات بناء على تلك المعلومات.

ثالثا - متطلبات التحول الرقمي للجامعات

تعد متطلبات التحول الرقمي في الجامعات مطلبًا أساسيًّا لتحقيق مجتمع المعرفة، فتعطي المعرفة قيمتها وقدرتها على التطبيق، وعلى التجديد والنماء.

هذا، وقد كشف مجتمع المعلومات عن تقادم المكون المعرفي لخريجي الجامعات، فالتحول الرقمي يتطلب المزيد من تحسين الكفاءات المهنية وتطوير مهارات الاتصال الجماعي، وتحديثها بشكل مستمر، وكذلك القدرة على التكيف والتغير السريع في الوظائف أو الواجبات المعدلة أو الأكثر تعقيدًا.

<u>ومن أهم المتطلبات التي يفرضها التحول الرقمي على الجامعات ما يأتي</u>: *(الشمري، ٢٠٢١، ١٦٧٨- ١٦٨١) (المفيز، وآخرون، ٢٠٢١، ٦٥٦).*

١. **اتخاذ الإجراءات القانونية اللازمة والتنظيمية الهادفة إلى تطوير التعلم عبر الإنترنت.**
٢. **أن تطوير إمكانيات عضو هيئة التدريس ومهاراته التكنولوجية واتجاهاته ومعارفه من أكبر عوامل نجاح التحول الرقمي.**
٣. **دعم البيئة التحية الرقمية، والقضاء على الفجوة الرقمية على شتى المستويات، لضمان المساواة في الوصول للبنية التحتية.**
٤. **إنشاء بوابة معلومات إلكترونية ومصادر تعلم ومحتوى رقمي ومنصات تعلم عبر الإنترنت.**
٥. **تطوير إستراتيجية عمل تسمح بتطبيق التقنيات الرقمية بشكل فعال، مع مراعاة احتياجات العملاء.**
٦. **التحول إلى التدريس والتعلم الرقمي، وإكساب الطلاب المهارات الرقمية.**
٧. **دعم طرق التعلم الفردية والتعلم مدى الحياة، وكذلك توفير الأنشطة الرقمية، ومحو الأمية المعلوماتية لدى الطلاب.**
٨. **توفير مناهج جديدة لمواكبة الثورة التكنولوجية والتحول الرقمي، وطرح حلول وأدوات جديدة لتحسين جودة النظام التربوي، بما يتوافق مع المعايير الدولية والمعايير الوطنية معا.**
٩. **استحداث طرق تقويم فعالة تتناسب مع عملية التعلم الجديدة، وطرق تقييم شامل لقدرة الطالب.**

١٠. إشراك خبراء تكنولوجيا المعلومات في عملية تطوير برامج التعلم للتحول الرقمي.

١١. تشكيل نظام لتقييم الخبراء والمستخدمين لضمان جودة محتوى الدورات التدريبية عبر الإنترنت.

١٢. تشجيع تمويل البحث التطبيقي والرقمي وريادة الأعمال.

١٣. توفير موظفين متخصصين ومدربين وإعادة تأهيلهم مهنيا وتدريبهم باستمرار.

١٤. دعم الابتكار واستخدام أساليب جديدة لحل المشكلات ومحو الأمية الرقمية.

١٥. بناء نظام لاكتشاف الطلاب الموهوبين، وتوجيههم على أساس ملف كفاءاتهم وتطورهم الشخصي.

١٦. إكساب الطلاب المهارات اللازمة للانخراط في التحول الرقمي بشكل فاعل فالتحول الرقمي جعل المعرفة ليست حكرا على الجامعات؛ فلقد أصبح التعليم والتعلم جزءًا لا يتجزأ من الاقتصاد.

١٧. دراسة نماذج التعاون بين الجامعات وريادة الأعمال في مختلف القطاعات الاقتصادية والتنمية، بما يحقق جودة الإدارة التعليمية، حتى تتناسب مع نمو التحول الرقمي.

١٨. تبني إستراتيجية لمواجهة مقاومة التغيير، الناتجة عن اعتياد الأفراد على أسلوب عملهم والراحة وروتين العمل اليومي والجمود الثقافي والخوف من الجديد.

١٩. تيسير عمليات نقل المعرفة المجانية، والانخراط في المجتمعات الافتراضية.

٢٠. الوصول إلى تحقيق التكامل بين التعليم الرسمي والتعليم غير الرسمي من خلال دعم عمليات التدريب، وتحقيق مبدأ التعلم مدى الحياة والتعلم الذاتي.

٢١. بناء رؤية رقمية وصياغة إستراتيجية التطوير، من خلال تكوين رؤية شاملة وواضحة حول تقنية المعلومات والاتصالات في الجامعة، لتعرف مكانتها المستقبلية، وتوفير الإطار التشريعي والدعم الإداري والمالي اللازمين لترجمة الرؤية الرقمية إلى واقع.

كما يتطلب التحول الرقمي بالجامعات توافر العديد من المتطلبات التي تضمن تقديم خدمات جامعية متميزة، وتحقق مستوى أداء مناسب للجامعات، *ومن بين هذه المتطلبات ما يلي:* *(باغة، ٢٠١٩، ٤٤- ٤٥)، (الخميسي، ٢٠٢٠، ٦٨- ٦٩)، (إبراهيم، ٢٠١٩، ١١) (الإقبالي، ٢٠١٩، ٤٤٧)، (مرج، ٢٠٢٠، ١٠٤، ١٠٥، ١١١)*

١- وجود إستراتيجية للتحول الرقمي تتضمن رؤية واضحة عن ما تريد الجامعة أن تكون عليه في المستقبل لإزالة الفجوة الرقمية **Digital gap** أو تقليصها، في ضوء تحليل بيئة الجامعة الداخلية والخارجية، ومن ثم وضع أهداف إستراتيجية تتضمن إحداث تحولات جذرية في الإجراءات الخاصة بالنظم الجامعية، ومنها: نظم القبول، والتسجيل، والتقويم ... وغيرها، وهيكلة البنية التحتية بما تشمله من أجهزة وشبكات وبرمجيات، وتأهيل الموارد البشرية وتنميتها تكنولوجيًّا، وتقدير تكلفة التحول وتسهيلات التطبيق والاستخدام.

٢- توفير الدعم القيادي والإداري لجهود التحول الرقمي، وذلك من خلال تركيز القيادات والمسئولين على الممارسات الإدارية المرتبطة بالتكنولوجيا غالية الثمن، والتي تكون غير متاحة لجميع المستفيدين.

٣- تطوير البنية التحتية الرقمية بالجامعة، وتشمل المبنى الجامعي الذكي، والأجهزة الحديثة والبرامج والتطبيقات التكنولوجية.

٤- توفير الإمكانات المادية والمالية اللازمة للتحول الرقمي، خاصة أن هذا التحول يتطلب استخدام العديد من الوسائل والأجهزة الإلكترونية الحديثة.

٥- تغيير الثقافة التنظيمية السائدة بمختلف الأوساط الأكاديمية والإدارية داخل الجامعة، من خلال نشر ثقافة استخدام التكنولوجيا والإنترنت والتعليم عن بعد كمطلب لتحقيق الميزة التنافسية للجامعة.

٦- تنمية الموارد البشرية بالجامعة من خلال برامج التدريب والتنمية المهنية والتي تضم مزيجًا من المهارات التقنية والمهارات المعرفية والمهارات الأخلاقية – والمهارات الإستراتيجية المتعلقة بالتحول الرقمي.

٧- تحديث نظم المعلومات حول الكفاءات التكنولوجية من أعضاء هيئة التدريس ذوي القدرات والمهارات التكنولوجية والكفايات المتميزة.

٨- توفير الإطار التشريعي اللازم لتأمين المعاملات الرقمية، وحماية المعلومات والبيانات المتعلقة بالجامعة بما يهيئ المناخ المناسب للتفاعل والمشاركة بين جميع الأطراف المستفيدة.

٩- تحقيق ما يعرف بالخدمة العريضة التي تضمن وصول المعلومات بتكلفة بسيطة، وبإمكانات تلبي رغبات المستفيدين، حتى في المناطق التي تعاني من القصور في مجال

تقنية الاتصالات، وذلك من خلال إتاحة فرصة الوصول المجاني للمستفيدين إلى المواقع الخاصة بالمنصات الرقمية للتعليم والتعلم، وتلقي الخدمات المتنوعة في إطار تشاركي فعال ومستدام.

١٠- الاستفادة من إمكانات الهيئات والمؤسسات الخبيرة في مجال تقنية المعلومات والاتصالات في دعم توجه الجامعات نحو التحول الرقمي، وتشجيع الشراكات بينها وبين الجامعات، وكذلك مع مختلف المنظمات والكيانات المجتمعية ذات الصلة، ومنها منظمات المجتمع المدني والأحزاب السياسية والوزارات الأخرى المساندة، كالصحة والاتصالات والإعلام والمواصلات والداخلية... وغيرها.

وهنا يمكن القول بأن تطبيق التحول الرقمي بالجامعات يحتاج إلى عدد من المتطلبات التي تتنوع لتشمل متطلبات إدارية، وتقنية، وتعليمية، وتشريعية، وموارد بشرية.

رابعا - التحديات التي يفرضها التحول الرقمي

إن الثورة التكنولوجية التي يمر بها العالم أحدثت العديد من التحولات داخل المجتمعات، فتحول الاقتصاد التقليدي إلى التحول الرقمي، والذي بدوره فرض على الدول محو الأمية الرقمية للشعوب، وترسيخ مبدأ التعلم مدى الحياة لديهم، مما يتطلب تغيير الهيكل التعليمي في المؤسسات التعليمية؛ لتوفير المتخصصين الذين يجيدون التعامل مع تكنولوجيا المعلومات والاتصالات، ويتمتعون بقدر كبير من المرونة لإعادة التدريب.

- ✓ *الأمر الذي فرض عددا من التحديات التي أصبحت تواجه المجتمعات، والتي يجب عليها التصدي له، ويأتي في مقدمتها ما يلي: (الشمري، ٢٠٢١، ١٦٧٥)، (عبد الحميد ،٢٠٢١، ١٤١)، (Boneva,M ., 2018,107)، (Schallmo & Williams ,2018,7)، (الإسكوا ، ٢٠١٨ ، ٨).*
- مواجهة العواقب الاجتماعية للرقمنة، مثل ارتفاع المهارات المطلوبة من الوظائف وتقليل عدد الموظفين.
- غياب الرؤية الإستراتيجية الرقمية الواضحة للجامعات، والافتقار إلى الدعم والتخطيط الإداري والقانوني للجامعات، وإهمال المتابعة والتقييم المستمر لخطوات التحول الرقمي.
- تدني مستوى البنية التحتية بالجامعات المصرية، وضعف التجهيزات الإلكترونية.
- ضعف الوعي التكنولوجي لدى كثير من الطلاب وأعضاء هيئة التدريس.

- عدم قناعة متخذي القرار وأعضاء هيئة التدريس بأهمية التحول الرقمي وما تفرضه التقنية من أساليب وطرق تعلم جديدة.
- ارتفاع التكلفة الاقتصادية لشراء الأجهزة التكنولوجية والتطبيقات الرقمية، والذكية، وصيانتها، وتشغيلها.
- ضعف قدرة أغلب أعضاء هيئة التدريس بالجامعات على التعامل مع التطبيقات التكنولوجية لتيسير مهامهم التعليمية والبحثية والإدارية، مع نقص الكفاءات القادرة على قيادة خطوات التحول الرقمي داخل الجامعة.
- المشاكل المعقدة الخاصة بالاتصال بالإنترنت، والتي قد تستغرق وقتًا طويلًا لاكتشافها وإصلاحها.
- ضعف مرونة الهياكل التنظيمية في الجامعات، وغلبة الجمود على شكل التنظيمات الجامعية الحالية.
- مشكلة التطوير في النظم التعليمية الرقمية باستمرار، وقد أكدت منظمة الإسكوا (لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا) ضرورة إجراء إصلاحات في قطاع التعليم، لتزويد الأطفال والشباب من جميع الفئات العمرية بالمهارات التي يتطلبها الاقتصاد الحديث.

وهنا يمكن القول بأن هناك العديد من العوامل التي تؤثر على تطبيق التحول الرقمي في التعليم الجامعي، ومنها تحديات داخل الجامعة، وبعضها خارجها، ومن الملاحظ على هذه التحديات أن بعضها مرتبط بالجانب المادي اللازم للتحول الرقمي، مثل توافر شبكة اتصال قوية وتطبيقات تكنولوجية حديثة تيسر تقديم الخدمات الرقمية، مع توافر منظومة أمنية لشبكة معلومات الجامعة، وبعض التحديات مرتبط بالجانب البشري المتمثل في عدم تقبل بعض منسوبي الجامعات للتحول الرقمي أو ضعف قدرتهم على استخدام التطبيقات التكنولوجية الحديثة، إلا أنه من الممكن التغلب على هذه التحديات من خلال نشر ثقافة التحول الرقمي، وتنمية المهارات الرقمية لدى أفراد المجتمع الجامعي، من أعضاء هيئة تدريس وطلاب وجهاز إداري.

خامسا - جهود الجامعات المصرية للتحول الرقمي

تم إنشاء وحدة إدارة مشروعات تطوير التعليم العالي، لتكون وحدة لها كيانها المستقل من النواحي الفنية والمالية والإدارية لإدارة ومتابعة تنفيذ مشروعات الخطة الإستراتيجية للتعليم العالي بقرار وزاري رقم ٣٠٠ بتاريخ للعام ٢٠٠٣، ويتم متابعة تطوير وقياس أداء مؤسسات التعليم العالي، من خلال عدد من المشروعات، منها: (مشروع تطوير نظم تكنولوجيا المعلومات)، ويهدف إلى: *(كاعوه، ٢٠٢٠، ١٦٥)*

- ❖ دعم مركز معلومات التعليم العالي بالمجلس الأعلى للجامعات لاستكمال وتوطين جميع مشروعاته.
- ❖ وضع الآليات التي تضمن التكامل التام بين جميع تطبيقات نظم المعلومات والاتصالات.
- ❖ تقديم عدد من الخدمات الإلكترونية لأعضاء هيئة التدريس والطلاب من خلال بوابة إلكترونية لكل جامعة.

ويقوم المشروع بتمويل عدد من المشروعات بالجامعات، ويعمل المجلس الأعلى للجامعات على رفع درجة الاستفادة من تكنولوجيا المعلومات بالجامعات، ويساعد على تقليل الفجوة الرقمية من خلال العمل بالمعايير التالية *(وحدة إدارة المشروعات، وزارة التعليم العالي بمصر)، (https: //www.heep.edu.eg)*

١. مشروع تطوير البنية الأساسية لشبكة المعلومات.
٢. مشروع البوابة الإلكترونية.
٣. مشروع نظم المعلومات الإدارية.
٤. مشروع التعليم الإلكتروني.
٥. مشروع المكتبة الرقمية.
٦. مشروع التدريب على تكنولوجيا المعلومات والاتصالات.
٧. المنصة الرقمية لوزارة التعليم العالي للعام الجامعي ٢٠٢٠/ ٢٠٢١.

ويلاحظ تعدد جهود الجامعات المصرية وتنوعها في التحول الرقمي، والتي جمعت بين تحديث وتطوير شبكة المعلومات الجامعية خلال مشروع (تطوير البنية الأساسية لشبكة المعلومات)، وتوظيف أفضل التقنيات والبرمجيات المتوفرة لزيادة التعاون والتواصل بين مختلف الكليات بالجامعة وبين الجامعات وبعضها، من خلال مشروع (البوابة الإلكترونية)، مع

استحداث أنماط جديدة من التعليم، تواكب التطور العالمي، وتستجيب للطلب المتزايد على التعليم العالي من خلال مشروع (نظم المعلومات الإدارية)، إضافة إلى إنشاء مراكز للتعليم الإلكتروني داخل كل جامعة(مشروع التعليم الإلكتروني) فضلا عن ميكنة إجراءات العمل في المكتبات.

وربط مكتبات الجامعة ببعضها من خلال شبكة الجامعات المصرية خلال مشروع (المكتبة الرقمية)، مع رفع كفاءة استخدام نظم المعلومات والموارد التكنولوجية المتاحة بالجامعة، ورفع معدل الاستفادة من مصادر المعلومات الإلكترونية والمحتوى الرقمي بالجامعة، من خلال مشروع (التدريب على تكنولوجيا المعلومات والاتصالات)، وأخيرًا إطلاق منصة لجميع الجامعات المصرية للتعلم عن بعد(المنصة الرقمية)، وهي تمثل نقلة حقيقية للتحول الرقمي للمنظومة التعليمية؛ تماشيًا مع إستراتيجية الدولة.

المحور الثاني: الإطار الفلسفي للأمن السيبراني.

الأمن السيبراني هو الحل الأمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته وأنظمته المختلفة، والتقليل من المخاطر التي تنشأ من سوء الاستخدام والوصول غير المشروع للبيانات، ويترتب على ذلك ضرورة بناء مجتمع واعٍ بأساليب الأمن السيبراني، وإعداد القدرات والكوادر الوطنية المؤهلة لمواجهة التهديدات السيبرانية، وسن القوانين والتشريعات الخاصة بالتعامل مع التهديدات.

أولا – نشأة الأمن السيبراني:

ارتبطت نشأة الأمن السيبراني باعتماد الأفراد على الإنترنت في جميع أعمالهم، من تنمية تجارتهم، وحساباتهم البنكية، والتعليم، والتواصل الاجتماعي، وإنهاء إجراءاتهم الحكومية، بالإضافة إلى مهام عديدة ومختلفة، فالمعلومات التي يستخدمونها بالغة الحساسية والأهمية، وأصبحت عرضة للخطر والاختراق والاستيلاء عليها، فنشأ مجال الأمن السيبراني لتأمين الأجهزة التقنية بجميع أشكالها وأنواعها، بما تحتويه من أنظمة وبيانات ومعلومات يتم تداولها من خلال شبكة الإنترنت، وبات من أهم العلوم في عصر التكنولوجيا، والتي تستخدم للحفاظ على هذه الثروة المعلوماتية المهمة لكل من الجهات الحكومية والأهلية والأفراد في الفضاء السيبراني الذي يعد أعم وأشمل من شبكة الإنترنت؛

لارتباطه باستخدام العديد من الشبكات حول العالم، كشبكة الألياف البصرية والشبكات اللاسلكية *(صائغ ، ٢٠١٨، ٣١)*

كما ارتبطت نشأة الأمن السيبراني بظهور الهجمات والاختراقات منذ منتصف خمسينات القرن الماضي، وتزايدت أهميته مع ظهور وانتشار شبكة الإنترنت التي فتحت الباب لمجالات جديدة يتم من خلالها حفظ ونقل المعلومات إلكترونيا، وقد ارتبط بذلك تطور موازٍ في مفهوم حماية المعلومات، للانتقال من الحماية المادية إلى الحماية الإلكترونية التي تتطلب مواكبة سريعة لسرعة تطور تكنولوجيا الأنظمة، والشبكات، والبرمجيات الحديثة، من خلال حزم من الآليات التي تكفل الحماية بمفهومها الجديد، وتحد من المخاطر الإلكترونية، مثل جدر الحماية، وأنظمة كشف التسلل، وتطبيقات مكافحة الفيروسات، وتقنيات التشفير، وإدارة المعلومات، وغيرها، حيث يستهدف الأمن السيبراني ضمان توافر واستمرارية نظم المعلومات، وتعزيز حماية سرية وخصوصية البيانات لجميع الأشخاص والكيانات العامة والخاصة.

ثانيا – مفهوم الأمن السيبراني:

يُعد مفهوم الأمن السيبراني من المفاهيم الحديثة نسبيًا، والتي ظهرت في إطار الثورة الرقمية والتكنولوجية المعاصرة، والتي أدت إلى تدفق المعلومات بشكل كبير وغير مسبوق، مع تعدد وسائل الاتصال إلى مصادر المعلومات عبر أجهزة الحواسيب، وغيرها من الأجهزة المحمولة، وفي هذا السياق ظهر مفهوم الأمن السيبراني ليعبر عن الجانب الأمني المرتبط بحماية تلك المعلومات، وكان هذا المفهوم محل اهتمام العديد من المؤسسات والباحثين.

والأمن السيبراني مصطلح جاء من الكلمة اللاتينية (سايبر Cyber) ومعناها تخيلي أو افتراضي، ودرج استخدامها لوصف الفضاء الذي يضم الشبكات المحوسبة التي تعني (فضاء المعلومات)، *(البطيكي، ٢٠٠٤، ٢٤٣)*، ومنها اشتقت صفة السيبراني والسيبرانية " Cybernetic" وتعني: علم التحكم الأوتوماتيكي، أو علم الضبط . وبهذا فإن الأمن السيبراني يعني (أمن الفضاء المعلوماتي)، وبهذا فهو معنيٌّ بالأمن المرتبط بشبكات الإنترنت، وكذلك شبكات الاتصالات. *(الجنفاوي، ٢٠٢١، ٨٥)*

وتختلف تعاريف الفضاء السيبراني حسب طبيعة كل دولة أو مؤسسة، وباختلاف رؤيتها وإستراتيجيتها في التعامل مع مجال الفضاء السيبراني، وعلى حسب الزاوية التي نظر

إليه منها ، إلا أن جميع هذه التعاريف اشتركت في مضمون واحد متقارب في المعنى، هو : "استهداف مواقع إلكترونية من خلال وسائل إلكترونية أخرى".

- ✓ ***وعليه سيتم تسليط الضوء على تعريف الأمن السيبراني فيما يلي:***

الأمن السيبراني بحسب تعريف الاتحاد الدولي للاتصالات في تقريره حول اتجاهات الإصلاح في الاتصالات للعام ٢٠١٠ – ٢٠١١ ، هو: مجموعة من المهام، مثل تجميع وسائل وسياسات وإجراءات أمنية، ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين . *(Hamadoun, I. 2008,2)*

وهو كذلك مفهوم يعبر عن مجموعة الآليات والإجراءات، والوسائل، والتدابير المتخذة لحماية جهاز كمبيوتر أو شبكة من الوصول غير المصرح به أو الضرر ؛ والتي تهدف إلى سلامة المعلومات المخزنة وأمنها، وحماية البرمجيات وأجهزة الكمبيوتر من التجاوزات والهجمات والاختراقات والتهديدات، لما تحتويه من معلومات. *(جاب الله،٢٠٢١، ٤٩)*. *(Richardson, M. &Waller, R. 2020,24)*

واتفق كل من ريتشارد *(Richard A.,2003,3)* وإدوارد *(Edward, A,2006,1)* ، في تعريف الأمن السيبراني على أنه وسائل دفاعية، من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة، وكشف وإحباط المحاولات التي يقومون بها، وكذلك كشف الفيروسات ووقفها.

ويعرف كذلك بأنه: أمن الشبكات والأنظمة المعلوماتية، والبيانات والمعلومات والأجهزة المتصلة بالإنترنت. وعليه، فهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير للحماية، من المفترض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أسوأ الأحوال *(أبو حسين، ٢٠٢١، ١٨)*.

كما يُعرف بأنه: العملية التي تؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، وتضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه في أسرع وقت ممكن،

بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة. *(جبور، ٢٠١٢ ، ٥)، (جبور، ٢٠١٦، ٢٦)،(حسن، ٢٠١٧ ، ٢١٤).*

واتفق ***(NICCS، 2014,4) National Initiative for Cybersecurity Careers and Studies***، مع التعريف السابق في تعريف الأمن السيبراني على أنه العملية التي يتم بموجبها حماية الأنظمة التقنية الحديثة والمعلومات من الضرر المحتمل أو الاستخدام غير المصرح به، كما يتم بموجبها استعادة الأنظمة والمعلومات عند حدوث الهجمات الإلكترونية.

كما تم تعريفه باعتباره مجموعة من الممارسات التي ترمي إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية أيًّا كان نوعها، وهذه الممارسات تتنوع بين تدابير احتياطية استباقية قبل وقوع الضرر، وعلاجية بعد وقوعه. *(الطيار، ٢٠٢٠، ٢٦٤).*

كما تم تعريفه بأنه مختلف الجهود والإجراءات التي تنتهجها الدول والمؤسسات، فيما يتصل بتوفير بيئة آمنة عبر الفضاء الإلكتروني، وما يتصل بتكنولوجيا المعلومات والتقنيات الرقمية، على نحو يحد من مخاطرها تجاه الأحداث بصفة خاصة، وأفراد المجتمع بصفة عامة. *(آل مسعود، ٢٠٢٠، ٤١٨).*

ويعرف كذلك بأنه مجموعة من الأدوات التنظيمية والتقنية والإجرائية والممارسات الهادفة إلى حماية أصول المعلومات، مثل الحواسيب والشبكات والبرمجيات وما بداخلها من بيانات، من التهديدات الداخلية والخارجية، والتلف، والتغيير أو تعطيل الوصول للمعلومات أو الخدمات. *(الغامدي، ٢٠٢١، ١٤٨).*

ويمكن القول بأن الأمن السيبراني سواء كان (نشاطًا، أو عملية، أو جهودًا وإجراءات، أو أدوات، أو تدابير، أو ممارسات) فإنه يحتاج إلى بناء قدرات أمنية عالية الجودة، تستهدف البنى التحتية لأنظمة الاتصالات وتقنية المعلومات، والتي تعد أساسًا وجزءًا مهمًّا من الفضاء السيبراني، وتدريب الطلاب والأفراد والمؤسسات لصد أي هجوم أو اعتداء يستهدف الفضاء السيبراني.

وفي ضوء التعريفات السابقة، يتضح أنه بالرغم من تباين المفاهيم التي قدمها الباحثون، فإنها تتفق وتتكامل في جوهرها، وتشير إلى أن الأمن السيبراني هو مجموعة من التقنيات والإستراتيجيات التي تتعلق بالعمليات الإلكترونية بشكل عام، كما أنه يمثل

مفهومًا أمنيًّا خاصًّا بحماية المعلومات، وكل ما له صلة بتلك المعلومات من عمليات وخدمات وأجهزة وتقنيات، ضد أي شكل من أشكال الوصول غير المسموح به، أو استخدام تلك المعلومات بشكل سلبي، أو بما يمثل خطرًا على الجهات أو الأفراد ذوي الصلة بتلك المعلومات.

كما يتضح من عرض التعريفات المرتبطة بالأمن السيبراني أنها لا تقف على طريقة أو وسيلة من أجل حماية المعلومات والشبكات، بل تفتح الطريق لأي أسلوب أو إجراء؛ من أجل تحقيق أمن المعلومات والشبكات، وقد يرجع ذلك إلى تطور المخترق السيبراني وإمكاناته التقنية.

ثالثا - أنواع الأمن السيبراني

في ضوء التعريفات المتنوعة للأمن السيبراني، يمكن تحديد أنواع مختلفة له، تتمثل في الآتي: *(triada network ,2019,2)*

أمن الشبكات *(Network Security)* وفيه تتم حماية أجهزة الحاسوب من الهجمات التي قد يتعرّض لها داخل الشبكة وخارجها، ومن أبرز التقنيات المُستخدمة لتطبيق أمن الشبكات جدار الحماية الذي يعمل واقيًا بين الجهاز الشخصي والأجهزة الأخرى في الشبكة، بالإضافة إلى أمن البريد الإلكتروني.

أمن التطبيقات *(Application Security)* وفيه تتم حماية المعلومات المتعلقة بتطبيق على جهاز الحاسوب، كإجراءات وضع كلمات المرور، وعمليات المصادقة، وأسئلة الأمان التي تضمن هوية مستخدم التطبيق.

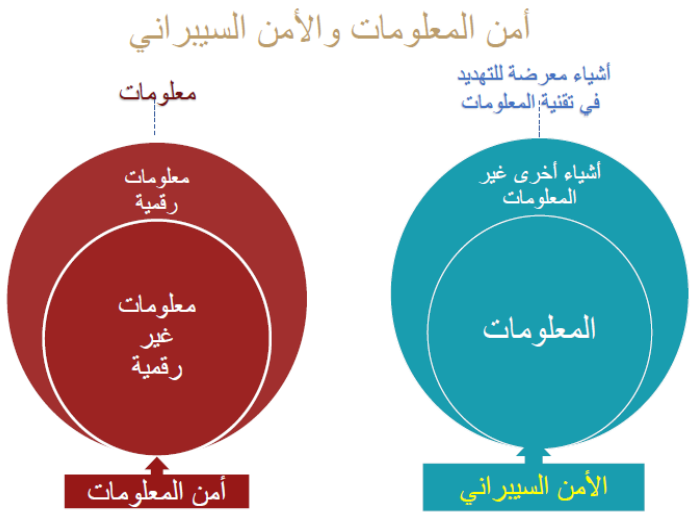
الأمن السحابي *(Cloud Security)* تُعرف البرامج السحابية بأنّها برامج تخزين البيانات وحفظها عبر الإنترنت، ويلجأ الكثير إلى حفظ بياناتهم عبر البرامج الإلكترونية عوضًا عن برامج التخزين المحلية، ممّا أدى إلى ظهور الحاجة إلى حماية تلك البيانات، فتعنى البرامج السحابية بتوفير الحماية اللازمة لمستخدميها.

الأمن التشغيلي *(Operational Security)* وهو إدارة مخاطر عمليات الأمن السيبراني الداخلي، وفيه يوَظَّف خبراء إدارة المخاطر لإيجاد خطة بديلة في حال تعرُّض بيانات المستخدمين لهجوم إلكتروني، ويشمل كذلك توعية الموظفين وتدريبهم على أفضل الممارسات لتجنب المخاطر.

الفرق بين الأمن السيبراني وأمن المعلومات:

إن أمن المعلومات والأمن السيبراني مصطلحان متشابهان، لكنهما ليسا متطابقين، حيث إن مفهوم الأمن السيبراني أوسع وأكثر شمولًا من أمن المعلومات، فيشمل تأمين البيانات والمعلومات التي تداول عبر الشبكات الداخلية أو الخارجية، والتي يتم تخزينها في خوادم داخل أو خارج المؤسسات من الاختراقات والوصول غير الشرعي لها، في حين يُعنى أمن المعلومات بالوسائل الضرورية لاكتشاف كل هذه التهديدات وتوثيقها وصدها، ويشمل كل ما من شأنه حماية المعلومة التي قد تكون في نظام حاسوبي *(صائغ ، ٢٠١٨، ٣٢) (الموجي، ومحمود، وإمام،٢٠٢١، ٢١)*، فهو يمثل كل شيء عن حماية المعلومات ، التي تركز بشكل عام على سرية وسلامة وتوافر المعلومات.

ويلاحظ أن كلًّا من الأمن السيبراني وأمن المعلومات يعملان على حماية البيانات من الاختراقات والهجمات وأي خطر محتمل الحدوث، وعلى الرغم من أن هنالك تشابهًا كبيرًا بينهما من حيث المفهوم، فإنهما مختلفان بعض الشيء، ففي الوقت الذي يعمل أحدهما لحماية البيانات في مكانٍ واحد، يعمل الآخر على حماية البيانات بشكلٍ عام. والشكل التالي يوضح ذلك:.....



شكل(١)
الفرق بين الأمن السيبراني وأمن المعلومات
المصدر: *(الحربي ، ٢٠٢٠، ٦)*

Print:(ISSN 1687-2649) Online:(ISSN 2536-9091)

ويتضح أن الأمن السيبراني يختلف عن فكرة (الأمن المعلوماتي). فالأمن المعلوماتي ينحصر نطاقه في إطار ومنظور فكرة حماية (النظام المعلوماتي، والشبكة المعلوماتية، والبيانات والحاسوب، وبرامجه، والموقع الإلكتروني) بمفهومها المجرد، من حيث مضمونها ومحتواها كقيمة مادية أو معنوية بالمعنى الضيق، وليست من وجهة أو منظور أمني سيادي ودفاعي يتعلق بمصالح قومية عليا.

غير أن الأمن السيبراني أوسع نطاقًا وأشمل من الأمن المعلوماتي؛ لأنه يزيد على فكرتي (الحماية، والتأمين) فكرة (الدفاع السيبراني) كأساس وإطار ومبرر لحماية المصالح الحيوية والوطنية ذات الصلة بسيادة الدولة على فضائها الإلكتروني، والتصدي للاعتداءات من خلال مجموعة النظم، والخطط، والتدابير، والأدوات، والسياسات، والإستراتيجيات، والتكتيكات والأساليب الضرورية والحيوية للحفاظ على الأمن القومي، والنظام العام، وسياسات الدولة في المجال الاقتصادي، والاجتماعي، والتقني، ومنشآتها ومؤسساتها الحيوية. *(الجمل،٢٠٢٠، ٢٥٤– ٢٥٥).*

إن وجود وجه تشابه بين "أمن المعلومات" و"الأمن السيبراني" يؤدي بالعديد من الباحثين لاستخدامهما للتعبير عن معنى واحد، إذ أن كلًّا منهما يلتقيان في الاهتمام بأمن المعلومات الإلكترونية، إلى جانب أن الأمن السيبراني يهتم بأمن جميع ما يوجد بالسايبر ومن ضمنه أيضا أمن المعلومات، ولكن رغم ذلك توجد اختلافات جوهرية بين المصطلحين، إذ أن أمن المعلومات يهتم بالمعلومات الورقية على عكس الأمن السيبراني الذي لا يهتم بذلك، كما يرتكز اهتمام الأمن السيبراني على ما هو متاح على السايبر، عكس أمن المعلومات الذي لا يهتم بذلك. *(العابد،٢٠٢٠، ٢٠٦). (قاسم ، ٢٠١٩ ، ١٧)*

رابعا – أهداف الأمن السيبراني:

اهتمت الحكومات والمؤسسات كافة في السنوات الماضية بالتخطيط لسياسات الأمن السيبراني، وذلك لما يحققه من العديد من الأهداف المهمة التي يمكن توضيحها فيما يلي:
أشار كل من *(صائغ ، ٢٠١٨ ، ١٠٣– ١٠٥)، و(السمحان، ٢٠٢٠، ١٢)* إلى *مجموعة متنوعة من أهداف الأمن السيبراني، تمثلت في :*

١. تعزيز حماية أنظمة التقنيات التشغيلية على جميع الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.

٢. التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

٣. توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.

٤. صمود البنى التحتية الحساسة للهجمات الإلكترونية.

٥. توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.

٦. التخلص من نقاط ضعف أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.

٧. سد الثغرات في أنظمة أمن المعلومات.

٨. مقاومة البرمجيات الخبيثة، وما تستهدفه من أحداث وأضرار بالغة بالمستخدمين وأنظمة المعلومات.

٩. الحد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

١٠. اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء، من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

١١. تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الإضرار بمعلوماتهم الشخصية، سواء بالإتلاف أو السرقة.

وأضافت *(المنتشري،٢٠١٩، ١٥٤)* أهدافًا أخرى للأمن السيبراني في ضوء أبعاده الدينية والاجتماعية والاقتصادية والسياسية، هي كما يأتي:

- **الحماية الدينية والأخلاقية: حيث أصبح من الممكن تجاوز القيم والمعايير والضوابط الاجتماعية، فهناك مواقع إباحية تعمل على تدمير القيم والأخلاق، وتبعد الإنسان عن دينه وعاداته وتقاليده، وتدفعه لارتكاب الجرائم وفعل المحرمات، فالأمن السيبراني يقدم الحلول التكنولوجية والحماية التامة من مثل هذه المواقع المدمرة.**
- **الحماية الوطنية: إن الفضاء السيبراني أصبح مجالًا للحروب الإلكترونية الخفية التي بسببها تدمر مقدرات الوطن وإمكانياته، وقد تستخدم أفراد هذا الوطن ضمن جيوشها المعادية دون معرفتهم، فالأمن السيبراني يجعل لهذا المواطن حزام أمان، يستطيع من خلاله الحذر من مثل هذه الحروب والتنبه لها.**

- **الحماية المالية: فعن طريق الأمن السيبراني سيتم معرفة جميع أنواع وطرق الاحتيال الإلكترونية التي تستهدف المعلومات البنكية، والبطاقات الائتمانية، وبطاقات الصرف الآلي الشخصية، والإعلانات والدعايات التجارية المضللة.**
- **الحماية الشخصية: يتعلم الفرد من خلال الأمن السيبراني عدم الإدلاء بأي معلومات شخصية، مثل كلمات المرور الخاصة، ومكان العمل والسكن، وغير ذلك من المعلومات التي لا يمكن لأي شخص غريب الاطلاع عليها.**

كما اتفق كل من *(الجنابي، ٢٠١٧)، (الربيعة، ٢٠٢٠، ١٣)* على عدة أهداف لتطبيق الأمن السيبراني، يمكن إجمالها في:

- **ضمان استمرارية عمل تطبيقات نظم المعلومات.**
- **حماية خصوصية وسرية المعلومات الشخصية، سواء للأفراد أو المؤسسات العامة أو الخاصة.**
- **حماية المواطنين من المخاطر المترتبة على دخول شبكة الإنترنت المختلفة .**
- **حماية الأجهزة التقنية وكذلك التشغيلية من أي محاولات للولوج بشكل غير مسموح به لتحقيق أهداف غير مشروعة.**
- **المحافظة على شبكات المعرفة والمعلومات.**
- **حماية مصلحة المؤسسات الحيوية وأمنها والبنى التحتية الحساسة فيها.**

وتستهدف الإستراتيجية الوطنية للأمن السيبراني(٢٠١٧ / ٢٠٢١) في مصر تحقيق ما يلي:

- **مواجهة المخاطر السيبرانية، وتعزيز الثقة في البنى التحتية للاتصالات والمعلومات وتطبيقاتها وخدماتها في شتى القطاعات الحيوية.**
- **تأمين البنية التحتية من أجل تحقيق بيئة رقمية آمنة وموثوقة للمجتمع المصري.**
- **الدعم السياسي والمؤسسي الإستراتيجي والتنفيذي، ويشمل ذلك الوعي بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية.**
- **وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات.**

تعددت أهداف الأمن السيبراني بصفة عامة، ولذلك تعددت أهدافه في الجامعات المصرية، والتي يمكن إيجازها فيما يلي : *(المنيع، ٢٠٢٢، ١٦٣).*

- ✓ **تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بالطلاب وأعضاء هيئة التدريس.**
- ✓ **حماية شبكة المعلومات والاتصالات من أي اختراق محتمل، والتي لها دور رئيس في تدفق المعلومات والبيانات من مقدم الخدمة إلى مستقبِلها.**
- ✓ **حماية شبكة المعلومات من أي هجوم محتمل؛ وذلك عن طريق معرفة التقنيات المرتبطة بأمن المعلومات ودراستها.**
- ✓ **تشفير جميع المعاملات الرقمية؛ بحيث يعجز أي مخترق عن مهاجمتها أو العبث بمحتوياتها.**
- ✓ **توفير بيئة العمل الآمنة، وذلك من خلال العمل الواعي عبر الشبكة العنكبوتية.**

ويتضح مما سبق أنه بالرغم من تعدد أهداف الأمن السيبراني، فإنها تتركز حول حماية المعلومات من السرقة أو الاختراق أو الهجوم. وعليه يمكن وصف الأمن السيبراني في ضوء تلك الأهداف بأنه يمثل الحفاظ على سلامة البيانات، وحماية خصوصيتها، مع تحسين توافر البيانات للمستخدمين المصرح لهم.

خامسا – أبعاد الأمن السيبراني:

تتعدد أبعاد الأمن السيبراني، ومن أهم هذه الأبعاد ما يأتي:*(صائغ، ٢٠١٨، ٣٦– ٣٨).(جبور، ٢٠١٦، ٢٨)*، www.un.org/en/un-coronavirus-communications-team/un-mobilizesglobal-

١- **الأبعاد العسكرية**: **وتتمثل في قدرته على ربط الوحدات العسكرية ببعضها، بما يسمح بسهولة تبادل المعلومات والسرعة في اتخاذ القرارات العسكرية وتدمير الأهداف عن بُعد، وتنشأ أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشآت النووية، وما قد ينتج عنها من تهديد لأمن الدول والحكومات ويؤدي إلى كوارث.**

٢- **الأبعاد السياسية** : **تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسي وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد**

يحدث من خلالها زعزعة لاستقرار أمن الدول والحكومات، حيث تصل بسرعة فائقة إلى أكبر شريحة ممكنة من المواطنين، بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها.

٣- **الأبعاد الاقتصادية**: يرتبط الأمن السيبراني ارتباطًا وثيقًا بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة، فأغلب الدول تعتمد في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة والمعلومات على كل المستويات؛ مما يبرز الدور الخطير للأمن السيبراني في حماية الاقتصاد المعرفي من السرقة، وتأكيد الملكية الفكرية.

٤- **الأبعاد القانونية**: ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومع ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي بمثابة البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع وحفظ الحقوق فيه، بجميع ما يتضمن من أبعاد، ويقوم الأمن السيبراني في هذا البعد على حماية المجتمع المعلوماتي، ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.

٥- **الأبعاد الاجتماعية**: تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكل مواطن بأن يعبر عن أفكاره، والاطلاع على مختلف المعلومات، والانفتاح عبر جميع الثقافات المختلفة، وهنا يكمن دور الأمن السيبراني وأهميته في حماية القيم الجوهرية للمجتمع وصيانتها، كالانتماء، والمعتقدات الدينة، والعادات والتقاليد...الخ. وفي هذا السياق تعمل المنظمات والهيئات على نشر ثقافة الأمن السيبراني، وتطالب بضرورة تعاون كل أفراد المجتمع في تحقيقه، للحد من مخاطر الهجمات والجرائم السيبرانية التي ـ بما لا شك فيه ـ تطول المجتمع ككل، وتهدد أمنه واستقراره، بالعمل على هدم قيمه وضياع هويته الثقافية.

يتضح مما سبق تعدد أبعاد الأمن السيبراني ما بين اقتصادية، واجتماعية، وسياسية، وإنسانية، مما يدل على أن الأمن السيبراني له القدرة على حماية أمن ومصلحة الدولة وشعبها في مختلف مجالات الحياة اليومية، وذلك لكونه مرتبطًا ارتباطًا وثيقًا

بسلامة وأمن البيانات والمعلومات التي تعدُّ ثروة هذا العصر؛ فهي مصدر الإنتاج، والإبداع، والابتكار، والقدرة على الاتصال والتواصل بين البشر.

سادسا – أهمية الأمن السيبراني في ضوء التحول الرقمي

مع بدايات القرن الواحد والعشرين، تأكدت حقيقة النظر للمعلومات باعتبارها أصولًا يتعين توفير الحماية لها؛ لأن أي ضرر يصيبها يترتب عليه تداعيات خطيرة، سواء على مستوى الدول أو المؤسسات أو الأفراد، وذلك في ظل هيمنة بيئة التحول الرقمي التي لم تعد خيارًا، بل أصبحت ضرورة ملحة للتطور، وهو ما دعا المؤتمر السابع للشباب إلى إطلاق مبادرة "التحول الرقمي في مصر"، مع تأكيد أن المبادرة تُعد متطلبًا ضروريًّا من متطلبات الأمن القومي المصري.

ولتحقيق الأمن السيبراني في عصر التحول الرقمي يتم الاعتماد على الفضاء السيبراني **Cyber Space** كوسيط تعمل فيه جميع الشبكات والحاسبات والبرمجيات، بالإضافة إلى حوسبة المعلومات ونقلها وتخزينها، وذلك على مستوى العالم أجمع، مما نتج عنه ارتفاع نسبة الانتهاكات الإلكترونية التي يترتب عليها إلحاق الضرر بالعديد من الدول ومنظمات الأعمال والأفراد على مستوى العالم. وطبقًا للمركز المصري للدراسات الاقتصادية **FCES** فقد تم تقدير الخسائر العالمية المتوقعة جراء تلك الانتهاكات بنحو ٦ تريليون دولار مع حلول عام ٢٠٢١ ، وهو ما يعد أكبر تحول للثروة في العالم من مجتمع الأعمال القانوني إلى مجتمع غير قانوني. *(عطية، ٢٠٢١ ، ٥٤).*

مما سبق تتأكد ضرورة توافر تشكيلة متنوعة من الضمانات الأمنية التي تناسب طبيعة البيئة الرقمية الجديدة، مما ترتب عليه ظهور اصطلاح " الأمن السيبراني " **Cyber Security** الذي أصبح أمرًا حتميًّا لتحقيق رحلة تحول رقمي آمنة في مختلف دول العالم، بل يعد الركيزة الأساسية لأي تحول رقمي، حيث تستند إليه المصداقية الرقمية لجميع المؤسسات . *(شواب، ٢٠٢٠، ٢).*

وهو ما أكده بالفعل الخبراء في *(الهيئة الوطنية للأمن السيبراني، ٢٠١٨)* من أن الأمن السيبراني يعدُّ مجالًا لأي تحول رقمي، فهو يحمي البيانات والبنية التحتية من أي هجمات سيبرانية، وخاصة عندما حدث هجوم تقني في العقد السابق، وأصبح مصدر قلق للحكومة والعامة والقطاعات الخاصة؛ لذا يجب التصدي لمثل هذه الهجمات ومعالجتها بشكل ذكي

ومبتكر، وفي ظل مواكبة التطور التكنولوجي والتحول الرقمي كان لا بد من مواجهة العقبات والمعوقات الإلكترونية، بما يتناسب مع أهمية المعلومات لكل فرد أو مؤسسة وحماية هذه المعلومات من أي هجوم إلكتروني قد يؤثر سلبًا على المؤسسات المختلفة، ومنها الجامعات. *(الغامدي، ٢٠٢١ ، ١٤٦).*

وبالمقابل، تزداد الجرائم السيبرانية كلما ازدادت هيمنة تكنولوجيا المعلومات والاتصالات على النسق العام للحياة، ففي بيئة التحول الرقمي أصبحنا أمام جرائم حقيقية ومتكاملة الأركان، تتم عن طريق شبكة الإنترنت بأشكال مختلفة، كسرقة الأموال، النصب والاحتيال، والتخطيط لعمليات إرهابية، وترويج الأخبار المضللة، وكذلك القرصنة كجريمة أكثر شيوعًا في العالم الرقمي.*(طالة، ٢٠٢٠ ، ٥٧).* ومع الأهمية الكبيرة للأمن السيبراني في ضوء التحول الرقمي، توجد أهمية تربوية للأمن السيبراني، ساهم في انتشارها استخدام وسائل الوصول إلى شبكة الإنترنت عبر العديد من الأجهزة المحمولة بالإضافة إلى الحواسيب، واعتماد الحياة المعاصرة في معظم مجالاتها على التكنولوجيا الرقمية، ووقوع العديد من المؤسسات حول العالم ضحية لأحد أشكال المخاطر والانتهاكات السيبرانية، وما يترتب على تلك المخاطر والانتهاكات من الأضرار المادية والنفسية والمعنوية التي تؤثر على المؤسسات التعليمية التربوية، وهذه الأضرار تُكسب الأمن السيبراني أهمية خاصة بالنسبة لكل فرد في عالم اليوم.

ومما يزيد من الأهمية التربوية للأمن السيبراني أنه قد يتعرض الأفراد بمختلف المؤسسات إلى الانتهاكات والمخاطر السيبرانية، دون أن يكون لديهم دراية بتلك المخاطر والانتهاكات ومدى خطورتها على التصفح الآمن للإنترنت، وهو ما يدعو إلى ضرورة رفع مستوى الوعي بأهمية الأمن السيبراني لدى هؤلاء الأفراد، وضرورة تضافر جهود الجامعات ووزارة التعليم العالي ومؤسسات المجتمع المدني في هذا الشأن.

ويمكن إيجاز الأهمية التربوية للأمن السيبراني على النحو الآتي: *(المنتشري،٢٠٢٠، ١٠٣)*

- ضمان سرية الوثائق التعليمية وخصوصيتها والحفاظ على سلامتها بشكل مستمر.
- متابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن في المدرسة.
- حماية المعلمات والمدرسة من الهجمات السيبرانية في الفضاء السيبراني.

وأضافت (*السمحان، ٢٠٢٠، ١٢*) مجموعة نقاط تمثل أهمية الأمن السيبراني، خاصة في عالم اليوم المترابط بواسطة الشبكات التي يستفيد منها الجميع، وتتمثل تلك النقاط فيما يلي:

- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بمنع العبث بها.
- تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها.
- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درعًا واقيًا للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيقِ مبادئ الأمن السيبراني.

ومع توضيح أهمية الأمن السيبراني بصفة عامة أو أهميته التربوية، يتضح أن الأهمية الأسمى له تتمثل في قدرته على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التحرر من الخطر أو الضرر الناجم عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات، ونتيجة لأهمية الأمن السيبراني في واقع مجتمعات اليوم، فقد جعله العديد من الدول على رأس أولوياتها، خاصة بعد الحروب الإلكترونية التي بدأت تظهر آثارها في بعض الدول، ومن بينها مصر بمختلف مؤسساتها التعليمية، وعلى رأسها الجامعات.

سابعا – مظاهر اهتمام مصر بقضايا الأمن السيبراني خلال العشر سنوات الأخيرة

تشهد مصر حراكًا قويًّا في مجال الأمن السيبراني، والذي تجسد في انضمام مصر للاتفاقية العربية لمكافحة جرائم الإنترنت والإرهاب الإلكتروني، وإنشاء المجلس الأعلى للأمن السيبراني، للحد من آثار اختراق أمن المعلومات على الأمن القومي للدول، كتأمين ميكنة الخدمات الإلكترونية، وإنشاء مركز سيرت المصري، حيث يقدم المركز منذ عام ٢٠١٢م الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات والخدمات المصرفية والحكومية؛ من أجل مساعدتها على مواجهة تهديدات الأمن السيبراني.(*البابلي، ٢٠٢٠، ٨*)

كما بدأت مصر باتباع بعض الآليات لتقليص مخاطر الهجمات السيبرانية، فأطلقت إستراتيجية موحدة في مجال الأمن السيبراني بعنوان "الأمن السيبراني آفاق وتحديات"، وذلك على هامش المؤتمر السنوي لتطوير الصناعة في ٢٠١٥، وركزت الإستراتيجية على سبل

تأمين شبكات البنية التحتية وتطبيقات التحكم الصناعي وتأمين الخدمات الإلكترونية . ***(محمود ، ٢٠٢٠، ٧٠-٧١).***

وفي السياق ذاته، قامت مصر بإطلاق القمر الصناعي طيبة ١ في ٢٢ نوفمبر ٢٠١٩م، لأغراض الاتصالات وحماية الأمن القومي الإلكتروني "طيبة -١"، ويغطي مصر بالكامل فيما يخص الاتصالات والإنترنت، والقمر الصناعي "طيبة ١" هو الأول في سلسلة "طيبة سات"، والتي ستحدث نقلة نوعية في خدمات الاتصالات في مصر وأفريقيا، ويشمل مجال تغطية القمر الصناعي مصر وبعض دول شمال أفريقيا ودول حوض النيل، ويدعم جهود الدولة في مكافحة الجريمة والإرهاب وتأمين البنية التحتية المعلوماتية من الأخطار السيبرانية التي باتت ظاهرة تهدد أمن الشعوب واستقرارها، كما يسهم في توفير خدمات الإنترنت عريض النطاق، للأغراض الحكومية والتجارية". ***(هيئة الاستعلامات المصرية "إطلاق القمر الصناعي طيبة ١)***

وتظهر جهود جمهوريه مصر العربية في إطلاق الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧- ٢٠٢١)، والتي أطلقها المجلس الأعلى للأمن السيبراني، من أجل تأمين البنى التحتية للاتصالات والمعلومات بشكل متكامل، لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، ورفع مستوى الوعي بالأمن السيبراني، وتجنب المخاطر والتهديدات السيبرانية وتقليل آثارها، وذلك في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري، وبما يدعم التحول نحو اقتصاد رقمي متكامل. ***(الإستراتيجية الوطنية للأمن السيبراني(٢٠١٧/٢٠٢١)، ٣).***

وقد تكللت جهود تعزيز التعليم الرقمي والتكنولوجيا الرقمية بالعمل مع العديد من الجهات التعليمية والجامعات والأكاديميات، لتفعيل برنامج التعليم عن بعد، والذي ازداد استخدامه بشكلٍ واضحٍ خلال أزمة كورونا، لتمكين معظم الجامعات من إجراء المحاضرات عن بعد، باستخدام تكنولوجيا الاتصالات والمعلومات، وتعزيز التدريس والتدريب الذاتي وإثراء المعرفة وتطوير مهارات الإبداع، والعمل في مجموعات، والانفتاح على العالم والثقافات الأخرى. ***(مشرف، ٢٠٢١، ٤٤٠)*** **، كما تم تطبيق برنامج التعليم عن بعد لدى العديد من الجامعات المصرية، تم تفعيل المنصَّات الإلكترونية باعتبارها فصولًا افتراضية تقدم خبرات ومواقف تعليمية متعددة، لتوفير الخدمات المساعدة للتعليم عن بعد للجامعات**

الحكومية مجانًا، وعليه تم الاعتماد على منصة بنك المعرفة المصري، ومن ثم فقد أسهمت الرؤية الاستشرافية للجامعات المصرية لتسريع التحول الرقمي في استمرارية الأعمال وتقديم تجربة خدمات رقمية آمنة خلال جائحة "كوفيد- ١٩" وتسهيل تقديم مزيد من الخدمات الرقمية.*(مشرف ، ٢٠٢١، ٤٥٦)*

وقد وقّعت مصر في ٢٠١٧ اتفاقية التعاون بين المعهد القومي للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيسكو العالمية؛ بهدف إطلاق أول أكاديمية للأمن السيبراني، تهدف إلى تطبيق المهارات اللازمة لمواجهة تحديات الأمن السيبراني .*(سليمان، ٢٠٢١، ٣٩)*.

وفي العام نفسه(٢٠١٧م) أبدت مصر استعدادها في مجال الأمن السيبراني، حيث أصدر الاتحاد الدولي للاتصالات تقرير مؤشر قياس استعداد الدول في هذا المجال؛ من أجل دفع المزيد من الجهود في مجال اعتماد الأمن السيبراني وتكامله على نطاق عالمي، وقد تقدمت سنغافورة والولايات المتحدة الأمريكية وماليزيا وعمان واستونيا وموريشيوس وأستراليا، وفرنسا، وكندا، وروسيا. كما أكد هذا التقرير أن مصر لديها استعداد قوي في مجال الأمن السيبراني، من خلال هيكلة بنية تحتية، وتبنّيها إستراتيجيات وطنية في هذا المجال، كما عقدت اتفاقيات عديدة دعت من خلالها لتبادل الخبرات ونشر

ثقافة الوعي بالأمن السيبراني، من خلال تبنيها سياسات وطنية، كما قدمت الكثير من المبادرات والملتقيات والمنتديات، وعقدت مؤتمرات واتفاقيات في مجال الأمن السيبراني، وقد تغلبت مصر بذلك على أزمات الثقة التي تهدد انتشار ثقافة الأمن السيبراني محليًّا وعالميًّا من خلال خمسة معايير حددها مؤشر قياس ITU، هي: الإمكانات (التقنية – التنظيمية- القانونية – التعاون – إمكانات النمو)

وتحتل مصر المرتبة ٢٣ عالميًّا والرابعة عربيًّا في المؤشر العالمي للأمن السيبراني (GCI Global Cybersecurity Index) لعام٢٠١٩ م، والذي يصدره الاتحاد الدولي للاتصالات التابع للأمم المتحدة، كما جاءت مصر في المرتبة الرابعة عشرة من بين ١٩٣ دولة من دول أعضاء الاتحاد. وكذلك جاءت في المرتبة الثانية عربيًّا فيما يتعلق بمستويات الالتزام بالأمن السيبراني بعد سلطنة عمان التي جاءت في المركز الرابع عالميًا والأول عربيًا. *(علام ، ٢٠٢١ ، ١٢)*.

والجدول التالي يوضح مظاهر اهتمامات مصر بقضايا الأمن السيبراني خلال العشر سنوات الأخيرة

جدول(١)

مظاهر اهتمامات مصر بقضايا الأمن السيبراني خلال العشر سنوات الأخيرة

التاريخ	نوع الاهتمام والمشاركة
أبريل ٢٠٠٩	تأسس المركز المصرى للاستجابة لطوارئ الإنترنت والحاسب الآلى (سيرت).
يوليو ٢٠٠٩	إتاحة خدمة الرصد والاستجابة للحوادث على مدار ٢٤ ساعة يومياً طوال الأسبوع.
٢٠١٢	المشاركة فى التدريبات السيبرانية العملية التى نظمها فريق الاستجابة لطوارئ الحاسوب بآسيا والمحيط الهادى (APCERT)، وفريق الاستجابة لطوارئ الحاسوب التابع لمنظمة المؤتمر الإسلامى (OICCERT)، والاتحاد الدولى للاتصالات (ITU). كما عقدت مصر اتفاقيات تعاون مع فريق الطوارئ للحاسوب بالولايات المتحدة (US-CERT)، ووكالة أمن الإنترنت الكورية (KISA) فى مدينة سيول، والهيئة الماليزية للأمن السيبرانى.
٢٠١٢	تنظيم البعثات الخاصة إلى فنلندا وأستونيا لاستكشاف فرص التعاون فى مجال الأمن السيبرانى من خلال فرق الاستجابة لطوارئ الحاسوب وفى مجال التوقيع الإلكترونى.
٢٠١٢	عرض إطار الأمن السيبرانى المصرى فى واحدة من الجلسات الرئيسية لمنتدى حوكمة الإنترنت ٢٠١٢ فى أذربيجان
أكتوبر ٢٠١٢	المشاركة فى مؤتمر بودابيست للفضاء الإلكترونى فى المجر ٢٠١٢.
ديسمبر ٢٠١٢	بدء تشغيل خدمة اختبار الاختراق.
مارس ٢٠١٣	تم تدشين المركز العربى الإقليمى للأمن السيبرانى (ITU-ARCC) حيث أسهمت مصر بدور حيوى فى أعمال المركز.
مايو ٢٠١٣	تنظيم ورشة العمل الأولى للأمن السيبرانى فى القرية الذكية تحت رعاية الجهاز القومى لتنظيم الاتصالات لمناقشة قضايا الأمن السيبرانى.
أكتوبر ٢٠١٣	احتل المركز المصرى للاستجابة لطوارئ الإنترنت المرتبة الثالثة حسب مؤشر الأمن السيبرانى العالمى للإتحاد الدولى للاتصالات.
ديسمبر ٢٠١٣	افتتاح مبنى المركز المصرى للاستجابة للطوارئ المعلوماتية الجديد (CERT).
٢٠١٤	انضمت مصر إلى اتفاقية الاتحاد الأفريقى بشأن أمن الفضاء الإلكترونى وحماية البيانات ذات الطابع الشخصى.

ديسمبر ٢٠١٤	احتلت مصر المركز ٢٧ من بين ١٩٣ دولة وفقاً لما جاء فى مؤشر قياس استعدادات الدول فى مجال الأمن السيبرانى الذى أصدره الاتحاد الدولى للاتصالات وشركة (API).
ديسمبر ٢٠١٤	تم تشكيل المجلس الأعلى للأمن السيبرانى فى مصر.
يونيو ٢٠١٥	أعلنت غرفة صناعة تكنولوجيا المعلومات والاتصالات عن ٤ محاور لبحث مستقبل تطوير وتنمية أمن المعلومات فى مصر لتكون أول استراتيجية موحدة فى مجال الأمن السيبرانى.
نوفمبر ٢٠١٦	استضاف الجهاز القومى لتنظيم الاتصالات المؤتمر الإقليمى الخامس للأمن السيبرانى ومنتدى (FIRST) فرست الإقليمى للمنطقة العربية والإفريقية لتأكيد تبادل الخبرات والتعاون.
نوفمبر ٢٠١٦	النسخة– الدورة – السابعة من مؤتمر القاهرة للأمن الإلكترونى بمشاركة خبراء من جميع أنحاء العالم.
٢٠١٦	توقيع اتفاقية تعاون بين المعهد القومى للاتصالات التابع لوزارة الاتصالات وتكنولوجيا المعلومات وشركة سيسكو العالمية.
أبريل ٢٠١٧	نظمت سايبر تالنش مسابقة أمن المعلومات الوطنية المصرية بالقاهرة برعاية شركة (TREND MICRO).

أبريل ٢٠١٧	شاركت مصر فى مؤتمر المنطقة المركزية للاتصالات الذى استضافته القياده المركزية الأمريكية فى واشنطن لتبادل وجهات النظر فى استراتيجيات الأمن السيبرانى الوطنية ومبادرات تكنولوجية المعلومات.
يونيه ٢٠١٧	احتلت مصر المركز ١٤ عالمياً والثانى إفريقياً وعربياً فى مؤشر قياس استعدادات الدول فى مجال الأمن السيبرانى الذى أصدره الاتحاد الدولى للاتصالات (ITU).
نوفمبر ٢٠١٧	فاز الفريق المصرى بالمركز الأول فى المسابقة الدولية TREND MICRO CTF COMPETITION فى اليابان والتى تنافس فيها مع فرق من اليابان وكوريا الجنوبية وبولندا وإسرائيل ورومانيا وتايوان وروسيا.
نوفمبر ٢٠١٧	شاركت مصر فى المنتدى الإقليمى للاتحاد الدولى للاتصالات ومنظمة فرست، وورشة عمل لتقييم الجاهزية للاستجابة للطوارئ المعلوماتية للمنطقة العربية والإفريقية.

نوفمبر ٢٠١٧	شاركت مصر فى المؤتمر الإقليمى السادس للأمن السيبرانى بعمان والذى نظمه الاتحاد الدولى للاتصالات (ITU).
ديسمبر ٢٠١٧	اطلاق أول أكاديمية للأمن السيبرانى فى مصر لتثقيف وتطبيق مهارات التعامل مع تحديات الأمن السيبرانى.
أبريل ٢٠١٨	شاركت مصر فى مؤتمر اختراقات الأمن السيبرانى (HITB).
يوليو ٢٠١٨	شاركت مصر فى مؤتمر قمة إفريقيا للدفاع السيبرانى.
أغسطس ٢٠١٨	شاركت مصر فى مؤتمر فى اجتماع لجنة الدراسات ١٧ التابعة للاتحاد الدولى للاتصالات (ITU).
أكتوبر ٢٠١٨	شاركت مصر فى المؤتمر الإقليمى السابع للأمن السيبرانى ٢٠١٨.
سبتمبر ٢٠١٨	نظم مركز المعلومات ودعم القرار بمجلس الوزراء جلسة نقاشية بعنوان:الأمن السيبرانى وحماية الهوية المصرية فى البيئة الرقمية الحديثة.
ديسمبر ٢٠١٨	المجلس الأعلى للأمن السيبرانى يطلق الاستراتيجية الوطنية للأمن السيبرانى (٢٠١٧-٢٠٢١).
فبراير ٢٠١٩	ماستر كارد تنظم أول منتدى حول الأمن السيبرانى فى القاهرة.
مارس ٢٠١٩	غرفة تكنولوجيا المعلومات والاتصالات تنظم المؤتمر السنوى الخامس للأمن السيبرانى.

المصدر: *(فوزي، ٢٠١٩، ١٢٢- ١٢٤)*

يتضح من الجدول السابق(١) اتجاه مصر نحو تحقيق الأمن السيبراني، من خلال التنسيق والتعاون مع الجهات الإقليمية والدولية، وكذلك انضمامها للاتفاقيات الدولية فى مجال التصدي لجرائم الإرهاب الإلكتروني؛ وذلك للاستفادة من الخبرات الدولية فى مجال الأمن السيبراني، كما حرصت مصر على وجود بنية تحتية قوية، مع السعي لتحقيق استقرار الأمن القومي، وإذكاء الوعي السيبراني، والقضاء على أزمة الثقة، إضافة إلى رسم سياسة إستراتيجية للأمن السيبراني.

المحور الثالث: متطلبات تحقيق الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي

تتمثل متطلبات تحقيق الأمن السيبراني في مجموعة من الشروط والمستلزمات الضرورية التي يلزم توافرها، حتى يمكن تحقيق الأمن السيبراني بالجامعات في ضوء التحول الرقمي، وكذلك في القدرة على التأثير من خلال استخدام وسائل الاتصال وشبكاته المعلوماتية، بالإضافة إلى العديد من العناصر والمتطلبات التي تتمثل في الآتي :.....

- ***دعم وتعزيز البنية التكنولوجية:*** تحتاج مختلف المؤسسات ومنها الجامعات لأجهزة ذات كفاءة وقدرة عالية وشبكات اتصال متعددة، وكذا برمجيات متطورة، بالإضافة إلى العنصر البشري المدرَّب من أجل البنية التحتية للأمن السيبراني، حيث تستطيع الجامعات بذلك التأثير على مختلف الكليات باستخدام القدرات الإلكترونية من جهة، وتأمين نفسها من الأخطار الممكنة من جهة أخرى. *(بوتيف، ٢٠١٩، ١٢٧).*
- ***محاربة الفيروسات والقضاء على البرامج الخبيثة:*** وهي برامج مصممة لتنفيذ عمليات قرصنة على أجهزة وشبكات بعض المؤسسات ومن ضمنها الجامعات، وتستخدم لتعطيل البنية التحتية، وتحويل عمليات الاتصال، وسرقة البيانات والمعلومات؛ بغرض التأثير على أجهزة هذه المؤسسات.
- ***القدرة على إجراء العمليات الإلكترونية:*** وتتمثل في اختراق الشبكات ومهاجمة أنظمة المعلومات وتسمى القدرة الهجومية اما القدرة الدفاعية فهي تتمثل في عمليات الحماية من الهجمات المختلفة وإمكانيات تشغيل الاجهزة ببرمجيات خاصة ومعينة، أما القدرة الاستطلاعية فتتمثل في الدخول إلى الحواسب الآلية والتجسس على الشبكات المحلية، وإجراء العمليات الاستخباراتية؛ بغرض معرفة خطوات الخصم. *(الصباحي، ٢٠١٦، ٥).*
- ***تبني سياسات دفاعية وامتلاك القوة السيبرانية***: تتمثل القوة السيبرانية في القدرة على التأثير، من خلال استخدام وسائل الاتصال وشبكاته المعلوماتية، وتتطلب تحقيق أقصى درجات الأمن السيبراني من خلال تبني سياسات دفاعية، وعمليات حماية، وتطوير ضد

الأخطار المحتملة، ومنع تعرضها للهجمات المعادية، ومن أبرز أنماط القوة السيبرانية ما يأتي:

١- *تبني نمط القوة الصلبة:* وهو استخدام المقدرات والأدوات فى عمل تخريبي، عبر قطع كابلات الاتصالات، أو تدمير أنظمة الاتصالات أو الأقمار الصناعية، أو حتى استعمال البرامج التخريبية وتنفيذ عمليات سرقة منظمة للبيانات.

٢- تبني نمط القوة الناعمة: ويتمثل في استخدام القدرات السيبرانية فى جانب التأثير الناعم على الطرف الآخر، عبر نظريات التشويش، وتغيير مسارات القوة، والتلاعب بالمعلومات، وتوظيف نتائجها لخدمة المصالح المستهدفة. *(الصادق، ٢٠١٥، ٢).*

وأضافت *(السحمان، منى عبد الله، ٢٠٢٠، ١٦)* مجموعة من المتطلبات، منها:

- ✓ **الموثوقية: وتعني استخدام المواقع الموثوق بها عند تقديم معلومات شخصية.**
- ✓ **البريد الاحتيالي: ويعني عدم وجود مرفقات البريد الإلكتروني، أو النقر فوق روابط الرسائل من مصادر غير معروفة، إذ أن إحدى الطرق الأكثر شيوعًا التي يتعرض فيها الأشخاص للسرقة أو الاختراق تكون عبر رسائل البريد الإلكتروني المبهمة أو المتخفية على أنها مرسلة من شخص موثوق به.**
- ✓ **النسخ الاحتياطي: ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام؛ لمنع هجمات الأمان على الإنترنت.**
- ✓ **المراقبة: الحرص على توفير المراقبة والمتابعة اللازمة والمستمرة للأنشطة المعلوماتية على الشبكة بالشكل الدقيق.**

ويمكن إضافة عدد من المتطلبات المتنوعة لتحقيق الأمن السيبراني في الجامعات، وجامعة بنها على وجه الخصوص، تتمثل في الآتي:

(أ) المتطلبات التقنية :

- ❖ **وجود قسم خاص وإدارة مركزية مختصة بأمن المعلومات والأمن السيبراني بين مختلف كليات الجامعة.**
- ❖ **التقييم الدوري لمخاطر الأمن السيبراني على أنظمة المعلومات بها.**
- ❖ **اهتمام الجامعة بعمل نسخ احتياطية للملفات بشكل دوري.**

- **الالتزام بفحص الملفات التي يتم تحميلها من المواقع غير المعروفة أو خدمات مشاركة الملفات الواردة عن طريق البريد الإلكتروني الجامعي.**
- **حسن اختيار مواقع نقاط الشبكة: فلا بد من الدقة عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية من الاختراق.**
- **تجنُّب إرسال أي معلومات حساسة مثل كلمات المرور وأرقام بطاقات الائتمان عبر البريد الإلكتروني.**
- **تطبيق التحول الرقمي في كل مدخلات الجامعة.**
- **وجود بوابة معلومات إلكترونية ومصادر تعلم ومحتوى رقمي ومنصات تعليمية إلكترونية.**
- **رفع درجة الحذر لدى أعضاء هيئة التدريس عند فتح مرفق في البريد الإلكتروني على صفحاتهم الإلكترونية.**
- **تطوير البنى التحتية السيبرانية بالجامعة؛ للحد من الاختراق والتجسس والقرصنة الإلكترونية.**
- **استخدام كلمة مرور معقدة قوية لا يمكن تخمينها، وتغيرها من وقت لآخر.**
- **إتقان المهارات التقنية في الأمن السيبراني، واستخدام البيانات في اكتشاف التهديدات والاستجابة للحوادث السيبرانية.**

(ب) المتطلبات المادية

- **توفير برامج حديثة لتدريب الهيئة التدريسية على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم.**
- **توفير الدعم الفني والتقني اللازم لأعضاء هيئة التدريس لمعالجة المشكلات الطارئة.**
- **زيادة الإنفاق على حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات للمؤسسات المختلفة من المخاطر السيبرانية.**
- **توفير بنية تحتية تكنولوجية وأجهزة اتصالات حديثة، تمكن الجامعة من تقديم خدماتها بشكل إلكتروني.**
- **امتلاك نظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الإلكترونية بين أعضاء هيئة التدريس.**

- **منح الجوائز المادية والمعنوية للمتميزين والمبدعين من أعضاء هيئة التدريس في مجال الأمن السيبراني.**
- **امتلاك برامج حديثة لحماية الهوية الرقمية مثل (برنامج المواطنة الرقمية).**
- **توفير المخصصات المالية اللازمة لتحقيق الأمن السيبراني.**

(ت)(ج) المتطلبات البشرية :

- **توعية أعضاء هيئة التدريس بمخاطر إرسال المعلومات الشخصية عبر الرسائل النصية أو البريد الإلكتروني.**
- **اختيار كلمة مرور قوية للحسابات الشخصية، تحتوي على حروف وأرقام ورموز.**
- **عقد لقاءات دورية للمختصين في تطبيق الأمن السيبراني؛ لتعريفهم بالمستجدات في المجال.**
- **تبادل الخبرات مع الجامعات الأجنبية والعربية في مجال الأمن السيبراني.**
- **تنظيم حملات توعية لأعضاء هيئة التدريس للتعريف بالأمن السيبراني، ومخاطره ، وتحقيق متطلباته.**
- **تعزيز مهارات أعضاء هيئة التدريس في مجال الأمن السيبراني، من خلال عقد دورات تدريبية متخصصة في استخدام جميع الوسائل التقنية بطرق آمنة.**
- **تفعيل التواصل مع مؤسسات المجتمع المدني لنشر ثقافة الأمن السيبراني.**
- **عقد بروتوكولات تعاون بين إدارة الأمن المعلوماتي بالجامعة وإدارة الأمن التابعة لها.**
- **تطوير العنصر البشري وتنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات.**
- **إسناد إدارة وتشغيل الشبكات المعلوماتية للعناصر البشرية ذات الكفاءة والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة.**

(ث)(د) المتطلبات المعرفية :

- **توعية أعضاء هيئة التدريس وتثقيفهم بمتطلبات الأمن السيبراني لحماية البريد الإلكتروني، وإدارة أمن المعلومات.**
- **مراجعة البيانات والمعلومات المتوفرة على شبكاتها؛ من أجل تحديثها حال تعرضها للجرائم السيبرانية.**

- ❖ تنمية وعي الطلاب بثقافة الأمن السيبراني في ضوء التحول الرقمي للجامعات.
- ❖ توفير مناهج جديدة؛ لمواكبة الثورة التكنولوجية والتحول الرقمي بما يتوافق مع المعايير الدولية.
- ❖ إعداد دراسات بحثية حول احتياجات الطلاب من المعلومات وثقافة الأمن السيبراني.
- ❖ توضيح إيجابيات ثقافة الأمن السيبراني خصوصًا في مضامينها المستقبلية على المجتمع.
- ❖ وضع إستراتيجيات لدمج وتضمين الموضوعات الخاصة بثقافة الأمن السيبراني في بعض المناهج والمقررات الدراسية بالجامعات.
- ❖ تطوير الإطار التشريعي الملائم لأمن الفضاء السيبراني، وتشديد العقوبات على جرائم الفضاء السيبراني، وحماية الخصوصية وحماية الهوية الرقمية.
- ❖ الاهتمام بتعريف الطلاب بالاصطياد الإلكتروني وتحديد مصادره.
- ❖ تنمية الوعي بمفاهيم انتهاكات الأمن السيبراني ومخاطرها، من خلال عرض فيديوهات تعريفية موجزة على المنصات التعليمية.
- ❖ تنمية وعي أعضاء هيئة التدريس بأهمية التحقُّق من المصادر الموثوق بها للحصول على معلومات تتعلق بعملهم.
- ❖ وضع إجراءات وسياسات لحفظ الأمن السيبراني داخل الجامعات، وفقا للضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني.
- ❖ نشر ثقافة التعامل مع الأمن السيبراني باعتباره قضية أمن قومي، هدفها حماية البيانات والمعلومات من الهجمات والاختراقات، للوصول إلى فضاء إلكتروني آمن وموثوق.
- ❖ تنويع الأنشطة المرتبطة بالمناهج الجامعية ومواءمتها للتحول الرقمي للجامعة.

المحور الرابع: معوقات تحقيق الأمن السيبراني بالجامعات في ضوء التحول الرقمي.

تتعدد معوقات تحقيق الأمن السيبراني، وتتمثل فيما يسمى بالجرائم الإلكترونية، وهي الجرائم التي ترتكب ضد أفراد أو مجموعات، مع وجود دافع إجرامي لإلحاق الضرر عمدًا بسمعة الضحية، أو التسبب بالأذى الجسمي أو النفسي للشخص بشكل مباشر أو غير مباشر ، باستخدام شبكات الاتصال الحديثة مثل الإنترنت (غرفة الدردشة، البريد الإلكتروني

، ...) والهواتف الجوالة (الرسائل النصية القصيرة، ورسائل الوسائط المتعددة)، وتشمل الجرائم الإلكترونية أي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت، ومن ضمن هذه المعوقات ما يلي:

١- ضعف القوانين الرادعة : بعض البلاد العربية ليس لديها قوانين متخصصة في الجريمة الإلكترونية، والقليل من البلدان يحاول سن تشريعات لهذا النوع من الجرائم، إلا أنها ما زالت في مراحلها الأولى، وتحتاج إلى المزيد من التحسينات والتنقيح. *(البداينة، ٢٠١٤، ١٥).*

٢- انتهاك الخصوصية: حيث تعد من الحقوق الفردية التي نصت عليها التشريعات الداخلية والاتفاقات الدولية. *(المنتشري، ٢٠٢٠، ١٠٦ -١٠٨)، (الإستراتيجية الوطنية للأمن السيبراني ، ٢٠١٧ ، ٢٠٢١)، ومن صور انتهاك الخصوصية في الفضاء السيبراني ما يلي:*

- ✓ **إدخال معلومات وهمية، وانتحال المعتدي إحدى الشخصيات بهدف الحصول على مبالغ مالية.**
- ✓ **التجسس الإلكتروني، وهي جريمة تقنية بحتة، يتم فيها استخدام وسائل تقنية المعلومات المتاحة وتتطلب مهارات تقنية عالية، وعادة ما يكون هدفها تتبع العيوب واصطياد الأخطاء والوصول غير المصرح به إلى أجهزة وبرامج ومصادر معلومات مهمة، سواء كانت اقتصادية أو حكومية أو خاصة، من أجل الحصول على عائد معين، قد يكون ماديًّا، أو معلوماتيًّا فقط ،** ***ومن أشهر جرائم التجسس الإلكتروني ما يلي :(القحطاني، ٢٠٠٠ ، ٢٧٢).***

أ- التجسس على أنشطة الحاسب الآلي.

ب- اختراق مواقع الإنترنت والتعديل فيها وانتهاك حرمتها.

ج- اختطاف المواقع بالدخول عليها والسيطرة عليها تمامًا.

د- تعديل برامج الحاسب الآلي أو بياناته.

هـ- استخدام الحاسب الآلي وبرامجه بدون تصريح.

٣- انتهاك أمن المعلومات : تعرف المعلوماتية إجرائيًّا بمجموعة البيانات التي تخضع للمعالجة والتحليل والتفسير لأغراض معينة؛ لتحقيق زيادة المعرفة، وتشمل الانتهاكات المعلوماتية جرائم الدخول إلى نظام معلوماتي، وسرقة المعلومات وتزيفها وتضليلها، وإعاقة

العمل المعلوماتي وتغيير المعلومات السرية، وتعطيل الأنظمة.(*جبور، ٢٠١٢، ٢٨- ٢٩*). وأحيانا تسمى بالجريمة المعلوماتية، وتسمى أيضا بالجريمة المتصلة بتكنولوجيا المعلوماتية والجريمة ذات التقنية العالية وتعرف بأنها "الجريمة التي تغطي جميع الأفعال غير المشروعة للاهتمام بتكنولوجيا المعلومات والاتصالات من حيث الأجهزة والبرمجيات" *(ثاني،٢٠٢٢، ١٢٨٨)*

٤- انتهاك الملكية الفكرية: يتخذ العدوان في جرائم انتهاك حقوق الملكية الفكرية أبعادًا جديدة ، فتقنية المعلومات ساعدت في التعامل مع المعلومات بسهولة كبيرة، ومن ثم لم يعد هناك صعوبة في ارتكاب عدوان عليها، بل أن كل ما يمكن أن يعد استيلاء أو حيازة في إطار هذه الجرائم، يمكن أن يتم بمجرد النقر بأقل مجهود ممكن، ومن دون خسائر مالية، فيكون العدوان على هذه الشاكلة سهلا، مما يمكن كل من يرغب في انتهاك حقوق المؤلف من القيام بذلك، دون تكبد عناء الجريمة أو بذل المجهود اللازم لارتكابها *(الخيلي، ٢٠١١، ٤٨)*.

٥- انتحال شخصية المواقع: تعرف المواقع الإلكترونية إجرائيًا بمجموعة من الصفحات الإلكترونية ومصادر المعلومات التي يمكن التفاعل معها ومشاهدتها عبر الحواسيب أو الأجهزة النقالة، ويمكن للمجرمين انتهاك وتدمير المواقع الإلكترونية، والتلاعب بالبيانات والمعلومات، والإضرار بها، وتهديدها بالفيروسات والبرامج الخبيثة والاختراقات، ومع أن هذا الأسلوب يعدُّ حديثا نسبيًا، إلا أنه أشد خطورة وأكثر صعوبة في اكتشافه من انتحال شخصية الأفراد، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التي يتم الاتصال بها من خلال نظم الحواسيب الخادمة المحمية (Secured server) فيمكن بسهولة اختراق مثل هذا الحاجز الأمني على الموقع للسيطرة عليه، ومن ثم تحويله إلى موقع بيئي، أو يحاول المجرم اختراق موقع لأحد مقدمي الخدمة المشهورين، ثم يقوم بتركيب البرنامج الخاص به هناك، مما يؤدى إلى توجيه أي شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور.*(قنديلجي، والسامرائي، ٢٠١٢، ١٧٩)*.

٦- الإرهاب الإلكتروني السيبراني: الإرهاب الإلكتروني السيبراني هو إرهاب المستقبل، وهو الخطر القادم الذي لا يمكن التخلص منه إلا بتكاتف جهود دولية وإقليمية؛ وذلك نظرًا لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن من خلال وسائل الاتصالات

وتقنية المعلومات مهاجمتها، في ظل جو مريح وهادئ، والسبب أنه لا يحتاج سوى إلى وجود شبكة معلوماتية، وجهاز حاسوب يمكن العمل من خلاله. *(البياتي،٢٠٢٢، ٩٠).*

ومع التقدم التقني وتقدم وسائل الاتصالات، تميز الإرهاب الإلكتروني عن غيره من أنواع الإرهاب بالطريقة العصرية، المتمثلة في استخدام الموارد المعلوماتية والوسائل الإلكترونية التي جلبتها التقنية في عصر المعلومات، لذا فإن الأنظمة الإلكترونية والبنية التحتية المعلوماتية هي هدف الإرهابيين *(الجنبيهي، ٢٠٠٦، ١١٠). . (العجلان، ٢٠٠٨، ٥٠)*

٧- اختراق البنى التحتية للاتصالات وتكنولوجيا المعلومات وتخريبها: ظهرت أنماط جديدة من الهجمات السيبرانية، تستهدف نشر برمجيات خبيثة وفيروسات، لتخريب أو تعطيل البنى التحتية للاتصالات وتكنولوجيا المعلومات، وذلك عبر عدة قنوات، تشمل الشبكات اللاسلكية (البريد الإلكتروني ومواقع الإنترنت والشبكات الاجتماعية وشبكات الاتصالات السلكية)، مما يؤثر تأثيرًا ملموسًا على البنى التحتية لتلك المنشآت والمرافق، وعلى الخدمات والأعمال المرتبطة بها، وقد ثبت عمليا أنها ليست بمنأى عن التعرض للهجمات السيبرانية الشرسة، حتى لو كانت غير متصلة بالإنترنت.

٨- إخفاء الهويات الرقمية والبيانات الخاصة : أصبح لظهور بعض التقنيات كالمعلومات المشفرة ، دور في إخفاء هوية المستخدمين، ما أتاح للمحتالين نشر تقنيات لسرقة المعلومات دون الخوف من الكشف عن هويتهم.

وتعد إخفاء أو سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمي الإنترنت ومستقبل الخدمات الإلكترونية، حيث قد تتعرض البيانات الشخصية للمستخدم إلى السرقة؛ بهدف انتحال شخصيته والاستيلاء على ممتلكاته وأمواله، أو للزج باسمه في تعاملات مشبوهة أو غير قانونية. وعادة ما يستعين سارق الهوية بمعلومات موجودة بالفعل على الإنترنت، وبخاصة على مواقع شبكات التواصل الاجتماعية، فضلًا على أنه قد تتعرض الأدوات والأنظمة المستخدمة في إجراء المعاملات الإلكترونية للسرقة أو التخريب؛ مما يشكّل خطرًا كبيرًا على مصالح المستخدمين ومستقبل الخدمات الإلكترونية، كما قد تتعرض البيانات الخاصة بالمؤسسات العامة والشركات للسرقة، مما يكبدها خسائر فادحة، مادية وأدبية.

٩- **القصور في برامج التوعية الأمنية: إن برامج التَّوعية بالأمن السيبراني من أكثر الطرق فعالية في محاربة الجريمة الإلكترونية، ولكن هناك نقص شديد جدًا في برامج التوعية بالأمن السيبراني على مستوى الأفراد والمؤسسات والحكومات. وقد يستغل المجرمون عوامل قلة فعالية برامج التَّوعية بالأمن السيبراني المتاحة في ارتكاب مثل هذه الجرائم، خاصة أن هذه البرامج متوفرة باللغة الإنجليزية .**

✓ **وأضافت** *(العابد، سكينة، ٢٠٢٠، ٢٠٩)* **مجموعة من أخرى من المعوقات تتمثل فيما يلي:**

معوقات فنية: وهي المعوقات الناتجة عن الأخطاء التقنية في مختلف أنظمة أمن المعلومات والأمن السيبراني، والتي يغلب عليها الطابع الفني، دون أن يكون هناك أي تدخل بشري أو أن تكون بسبب كارثة طبيعية مثل: عيوب التصميم والتشغيل، وتشتت المعلومات (إذا كانت مخزنة في أماكن كثيرة ويجري التعامل معها عبر شبكات متعددة).

معوقات بشرية: ويقصد بها المعوقات الناتجة عن العنصر البشري مباشرة، فقد يتسبب العنصر البشري ـ عمدًا أو عن طريق الخطأ ـ في الضرر، أو الوصول إلى المعلومات والاطلاع عليها دون أن يكون له الصلاحية بذلك، أو إتلافها، أو تسريبها إلى جهات خارجية.

معوقات طبيعية: يقصد بها الكوارث الطبيعية التي ليس للإنسان أو التجهيزات الفنية دخل في حدوثها، كالزلازل، والبراكين، والفيضانات، والصواعق، والحرائق. وقد تُلحق هذه الكوارث أضرارًا كبيرة بأنظمة المعلومات، وقد تؤدي إلى انقطاع الخدمات الإلكترونية نهائيًا في حالة إصابتها المراكز الرئيسة لتقديم تلك الخدمات.

زيادة تعقيد الهجمات الإلكترونية : من معوقات الأمن السيبراني زيادة تعقيد الهجمات الإلكترونية، وذلك تزامنًا مع تقدّم المجال الإلكتروني، إذ أسفر استحداث مجالات تعلم الآلة، والذكاء الاصطناعي، والعملات المشفرة وغيرها عن زيادة البرامج الضارة التي تُعرّض بيانات الشركات والحكومات والأفراد لخطر دائم.

نقص الخبراء في قطاع الأمن السيبراني : ويقصد به النقص الحاد في الخبراء، وهو ما أحد أهم معوقات الأمن السيبراني، إذ يعاني هذا المجال من قلة المختصين فيه.

الاتصال غير الآمن بالإنترنت: إنّ الاعتماد المفرط على الاتصال غير الآمن بالإنترنت، قد يؤدي إلى انهيار أنظمة تبادل المعلومات، ويزيد احتمال انتشار البرامج الضارة.

انتشار المعلومات المغلوطة : إن النشر المتعمد للمعلومات المغلوطة باستخدام الروبوتات أو المصادر الآلية، يُعرّض سلامة مستخدمي المعلومات الإلكترونية للخطر.

تطوّر عمليات الاحتيال : ازدياد عمليات الاحتيال خداعًا، إذ أصبح البعض يستهدف بيانات الأشخاص عن طريق خداعهم بالنقر على أحد الروابط، وقلة وعي الأشخاص بذلك، وتوظيف التعليم الإلكتروني في صياغة رسائل أكثر إقناعًا لخداع الأشخاص المثقفين بشأن عمليات الاحتيال.

الهجمات الإلكترونية المادية : تتعدّى الهجمات الإلكترونية المادية نطاق البيانات الإلكترونية؛ إذ أصبح هناك من يهاجم بيانات محطات المياه، والكهرباء، والقطارات.

إمكانية الوصول لأطراف إضافية (الأطراف الثلاثة) : وتعني الأطراف الثلاثة إتاحة المستخدم وصول أطراف أخرى إلى بياناته، ومن أمثلة ذلك تسجيل الدخول إلى المواقع باستخدام تطبيقات التواصل الاجتماعي أو البريد الإلكتروني، ما يتيح لمستخدمي تلك المواقع الوصول إلى معلومات الشخص*(Michelle, M ,2021,5)*

✓ **ومما سبق استخلاص مجموعة من معوقات الأمن السيبراني، من أهمها:**

- ❖ **سهولة اختراق المعلومات الشخصية والمنصات التعليمية بسبب التطور التكنولوجي الهائل الذي أتاح إمكانية الوصول غير المسموح به.**
- ❖ **استخدام العديد من التطبيقات في مواقع مختلفة لنفس قاعدة البيانات.**
- ❖ **قلة توافر برامج حماية كافية ضد برامج الاختراق الحديثة.**
- ❖ **تبادل أرقام المرور السرية للأنظمة الإلكترونية بين الهيئة التدريسية.**
- ❖ **عدم استخدام برامج حماية أصلية موثوقة، والاعتماد على استخدام البرامج المنسوخة.**
- ❖ **ضعف آليات وسياسات حماية البنية التحتية السيبرانية، وكذلك ضعف آليات حماية الأجهزة وأنظمة البيانات والمعلومات.**
- ❖ **قلة الدورات التدريبية المنعقدة لأعضاء هيئة التدريس في مجال الأمن السيبراني.**
- ❖ **قلة الوعي بقانون الجرائم المعلوماتية وعقوبات نشر الوثائق والمعلومات السرية وإفشائها.**
- ❖ **غياب التطبيق الفعلي للتشريعات والقوانين الرادعة لمرتكبي الجرائم الإلكترونية.**
- ❖ **الافتقار إلى الرؤى والبيانات التي تمكن الجامعات من إدارة المخاطر الإلكترونية بكفاءة وفعالية.**

- ضعف التعاون بين موظفي التقنيات في الجامعات لتحقيق الأمن السيبراني.
- عدم وجود قسم خاص بأمن المعلومات والأمن السيبراني داخل الجامعة.
- استخدام الأجهزة الشخصية كالهواتف المحمولة لنقل معلومات سرية خاصة بالجامعة.
- تدني مستوى خبرة الموظفين بالأمن السيبراني.
- التحايل للتحكم في الوصول إلى الوسائط، من خلال تسخير برامج وهمية مهمتها إظهار الأشخاص كمستخدمين فعليين داخل الشبكة.

المحور الخامس: واقع ملاءمة تحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات من وجهة نظر أعضاء هيئة التدريس (إجراءات الدراسة الميدانية)

يتناول هذا الجزء إجراءات الدراسة الميدانية، وأداتها وكيفية تصميم هذه الأداة، وتوصيف عينة الدراسة، وخطوات تطبيق أداة الدراسة، وأساليب المعالجة الإحصائية، وعرض وتحليل وتفسير نتائج الدراسة الميدانية.

أولاً: إجراءات الدراسة الميدانية:

وتتحدد إجراءات الدراسة الميدانية فيما يلي:

١- اهداف الدراسة الميدانية:

استهدفت الدراسة الميدانية للبحث الحالي ما يلي: .....

- التعرف على مدى ملاءمة تحقيق متطلبات الأمن السيبراني بجامعة بنها، في ضوء التحول الرقمي للجامعات من وجهة نظر أعضاء هيئة التدريس بجامعة بنها، وذلك من خلال محورين اساسين، هما متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي، ومعوقات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي.
- معرفة دلالة الفروق بين متوسطات درجات أفراد العينة من أعضاء هيئة التدريس حول تلك المحاور تبعا لنوع التخصصات (نظرية – عملية) و(الدورات التدريبية التي حصل عليها عضو هيئة التدريس).

٢- تصميم وإعداد أداة الدراسة الميدانية:

- **الاستبانة:**

استخدمت الدراسة الحالية الاستبانة وتم اعدادها وتوزيعها إلكترونياً على أفراد العينة، باعتبارها إحدى الأدوات التي تفيد فى جمع البيانات والمعلومات التي تغطى كافة جوانب موضوع الدراسة، وذلك من خلال إجابة أفراد العينة على بنود هذه الاستبانة.

وقد اعتمدت الدراسة الحالية على الاستبانة التي تتضمن في محتواها على مجموعة من العبارات للتعرف على مدى ملاءمة تحقيق متطلبات الأمن السيبراني بجامعة بنها فى ظل التحول الرقمي للجامعات، واهم المعوقات التي تحول دون تطبيق هذه المتطلبات من وجهة نظر أعضاء هيئة التدريس بجامعة بنها.

وقد سار بناء الاستبانة على النحو التالي:

وضع الاستبانة في صورتها المبدئية(الأولية):

- **تم وضع الاستبانة فى صورتها المبدئية في ضوء الإطار النظري للبحث الحالي والاطلاع على بعض الاستبانات التي تم استخدامها في الدراسات السابقة ذات الصلة بموضوع البحث ، وتكونت الاستبانة في صورتها الأولية من خمسة ابعاد : هما (المتطلبات التقنية والمادية والبشرية والمعرفية، ومعوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها) ، وقد تم عرضها على مجموعة من المحكمين تمهيدًا لتطبيقها، وبأخذ ملاحظاتهم قامت الباحثة بإعادة بناء الاستبانة وإعدادها لتكون فى صورتها النهائية.**

صدق الاستبانة:

للتأكد من صدق الاستبانة المستخدمة فى الدراسة، تم إتباع الطرق التالية:

- **صدق المحتوى (المحكمين):**

يدل صدق المحتوى على مدى تمثيل محتوى الاستبانة للنطاق السلوكي الشامل للسمة المراد الاستدلال عليها، على أن يكون المحتوى ممثلاً تمثيلاً جيداً لنطاق العبارات التي يتم تحديدها مسبقاً.

ويعرف ذلك بصدق المحكمين، وللتأكد من صدق الاستبانة المستخدمة تم عرضها على نخبة من المحكمين لإبداء آرائهم وملاحظتهم حول مدى مناسبة الاستبانة فى تحقيق

أهداف الدراسة، وملائمة الفقرات للبنود الخاصة بها وقد تم تعديل بعض البنود فى ضوء مقترحات السادة المحكمين وبذلك أصبحت الاستبانة في صورتها النهائية، وقد تمثلت تلك التعديلات فيما يلي:

- إضافة بعض التعديلات اللغوية على بعض عبارات الاستبانة.
- إعادة صياغة بعض العبارات واختصارها لتكون أكثر وضوحا.
- إعادة ترتيب بعض فقرات الاستبانة.

وبعد إجراء التعديلات والملاحظات التي قام بها السادة المحكمين أصبحت الاستبانة تتكون من خمسة ابعاد، وهم على النحو التالي:

- البعد الأول: المتطلبات التقنية لتحقيق الأمن السيبراني ، وتضمن (١٥) عبارة.
- البعد الثاني: المتطلبات المادية لتحقيق الأمن السيبراني ، وتضمن (٩) عبارات.
- البعد الثالث: المتطلبات البشرية لتحقيق الأمن السيبراني ، وتضمن (١٤) عبارة.
- البعد الرابع: المتطلبات المعرفية لتحقيق الأمن السيبراني، وتضمن (١٧) عبارة.
- البعد الخامس: معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها، وتضمن (١٥) عبارة.

وبالتالي فإنه تمثلت عدد عبارات الاستبانة ككل في (٧٠) عبارة.

- <u>الصدق الذاتي:</u>

لحساب صدق الاستبانة تم تطبيقها على عينة استطلاعية بلغ قوامها (٣٠) عضو هيئة تدريس بجامعة بنها، ولمعامل الصدق الذاتي أهمية فى أنه يمثل الحد الأعلى لمعامل صدق الاستبانة، ويتم حساب الصدق الذاتي للاستبانة عن طريق حساب الجذر التربيعي لمعامل الثبات، أي أن:

معامل الصدق الذاتي = $\sqrt{\text{معامل الثبات}}$.

وبذلك يكون معامل الصدق الذاتي لكل بعد من ابعاد الاستبانة، كما هو موضح فى الجدول الآتي:

جدول (٢)
معامل الصدق الذاتي للاستبانة (ن = ٣٠)

الابعاد	عدد العبارات	معامل الصدق
المتطلبات التقنية	١٥	٠.٩٧٣
المتطلبات المادية	٩	٠.٩٧٠
المتطلبات البشرية	١٤	٠.٩٧٥
المتطلبات المعرفية	١٧	٠.٩٨١
معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها	١٥	٠.٩٧٦

وطبقا لما ورد في الجدول السابق (٢) فإن قيم معامل الصدق جاءت مرتفعة؛ مما يعني أن ارتباط ابعاد الاستبانة ببعضها قويًا، ويدل ذلك على الصدق العالي لعبارات الاستبانة.

- **صدق الاتساق الداخلي:**

لمعامل صدق الاتساق الداخلي أهمية كبيرة باعتباره يمثل الحد الأدق لصدق الاستبانة، وقد تم حساب صدق الاتساق الداخلي من خلال حساب معامل الارتباط بين درجة كل عبارة والدرجة الكلية للبعد الذي تنتمي إليه العبارة، والجدول الآتي يوضح ذلك.

جدول (٣)
معامل الارتباط بين درجة كل عبارة والدرجة الكلية للبعد الذي تنتمي إليه العبارة

البعد	المفردة	معامل الارتباط	المفردة	معامل الارتباط	المفردة	معامل الارتباط	لمفردة	معامل الارتباط
متطلبات التقنية	١	**٠.٧٤٧	٥	**٠.٨٤٥	٩	**٠.٦٦٠	١٣	**٠.٧٩٨
	٢	**٠.٨٤١	٦	**٠.٨٣٤	١٠	**٠.٧٦٣	١٤	**٠.٧٠٩
	٣	**٠.٥٥٩	٧	**٠.٦٣٩	١١	**٠.٦٩٠	١٥	**٠.٨٤٧
	٤	**٠.٩١٦	٨	**٠.٧٤٤	١٢	**٠.٨١٧		
متطلبات المادية	١	**٠.٧٧٥	٤	**٠.٨٩٧	٦	**٠.٧٢٣	٨	**٠.٨٦٣
	٢	**٠.٨١٢	٥	**٠.٨٣٣	٧	**٠.٨٥٧	٩	**٠.٨٤٠
	٣	**٠.٨٥٧						
متطلبات البشرية	١	**٠.٨٤٠	٥	**٠.٨٦٣	٩	**٠.٨٤٠	١٢	**٠.٩٢٠
	٢	**٠.٧٢٤	٦	**٠.٨٢٤	١٠	**٠.٩٥٧	١٣	**٠.٨٥٥
	٣	**٠.٨٥٧	٧	**٠.٧٢٢	١١	**٠.٨٩٤	١٤	**٠.٩٠٠
	٤	**٠.٨٦٠	٨	**٠.٨٦١				
متطلبات المعرفة	١	**٠.٩١١	٦	**٠.٨٩٤	١٠	**٠.٨٩٥	١٤	**٠.٨٨٣
	٢	**٠.٨٤٧	٧	**٠.٨٧٤	١١	**٠.٩٢٦	١٥	**٠.٨٨٢
	٣	**٠.٨٩٢	٨	**٠.٨٣٨	١٢	**٠.٨٧٦	١٦	**٠.٩٤٢
	٤	**٠.٨٧٧	٩	**٠.٨٦٣	١٣	**٠.٩٦٣	١٧	**٠.٨٤٨
	٦	**٠.٨٣٥						
معوقات تحقيق متطلبات الأمن السيبراني	١	**٠.٥٦٢	٥	**٠.٧٧٩	٩	**٠.٨٤٦	١٣	**٠.٨١٤
	٢	**٠.٥٠٣	٦	**٠.٨٦٥	١٠	**٠.٨٠١	١٤	**٠.٨٢٤
	٣	**٠.٨٤٦	٧	**٠.٨٠٧	١١	**٠.٨٩٩	١٥	**٠.٩٢٩
	٤	**٠.٦٤٣	٨	**٠.٨٧٩	١٢	**٠.٧٧٢		

(قيمة معامل الارتباط دالة عند مستوي ٠.٠١)**

يتضح من الجداول (٣) أن جميع قيم معاملات الارتباط بين درجة العبارة ودرجة البعد الذي تنتمي إليه جميعها دالة عند مستوى (٠.٠١) مما يحقق الصدق التكويني للاستبانة، أي صدق الاتساق الداخلي لجميع عبارات الاستبانة بالنسبة للبعد الذي تنتمي اليه.

جـ- ثبات الاستبانة:

تم حساب معامل الثبات عن طريق معامل ألفا كرونباخ باستخدام البرنامج الإحصائي SPSS V.18، وهي كما يوضحها الجدول التالي:

جدول (٤)
معامل ثبات ابعاد الاستبانة

البعد	عدد العبارات	معامل الثبات
المتطلبات التقنية	١٥	٠.٩٤٧
المتطلبات المادية	٩	٠.٩٤١
المتطلبات البشرية	١٤	٠.٩٥٠
المتطلبات المعرفية	١٧	٠.٩٦٢
معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها	١٥	٠.٩٥٣

يتضح من الجدول السابق (٤) أن قيم معامل الثبات تتراوح بين (٠.٩٤١ – ٠.٩٦٢) وهي جميعها قيم مرتفعة، مما يدل على أن معامل ثبات الاستبانة مرتفع، الأمر الذي يعني إمكانية تطبيق الاستبانة والوثوق والاطمئنان نسبيا الى النتائج التي ستسفر عنها.

٣- **عينة الدراسة**:

تم اختيار عينة الدراسة الميدانية بطريقة عشوائية من المجتمع الأصلي للدراسة، والمتمثل في السادة أعضاء هيئة التدريس بجامعة بنها، وقد تم الفصل بين أعضاء هيئة التدريس، من حيث انتمائهم للكليات النظرية أو العملية؛ لأن هدف الدراسة هو تعرف متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات، وتم اختيار العينة من السادة المدرسين والأساتذة المساعدين والأساتذة بجامعة بنها، وقد تم تحديدها طبقا للخطوات التالية:

- تحديد المجتمع الأصلي الذي تجرى عليه الدراسة والمتمثل في السادة أعضاء هيئة التدريس بجامعة بنها والبالغ عددهم (٢٤٥٦) عضو هيئة تدريس.
- اختيار عينة ممثلة للمجتمع الذي تجرى عليه الدراسة، وذلك بما لا يقل عن نسبة (١٠ %) من مجتمع الدراسة؛ بحيث تكون ممثلة له، ونتائجها صادقة يمكن تعميمها، وقد بلغ عددها (٢٤٨) عضو من أعضاء هيئة التدريس بجامعة بنها.

إجراءات تطبيق الاستبانة:

سارت إجراءات تطبيق الاستبانة على النحو التالي:

- بعد اعداد وتصميم الاستبانة فى صورتها النهائية والتحقق من الصدق والثبات، تم تطبيقها إلكترونياً على أفراد العينة.

- تم توزيع الاستبانات على أفراد العينة إلكترونياً حيث تم تصميم الاستبانة وتم توزيعها على عينة الدراسة حتى الوصول الى عدد استجابات ملائم نسبيا.
- بلغ عدد الاستبانات التي تم استيفاؤها (٢٤٨) استبانة تم تطبيقها على أعضاء هيئة التدريس بجامعة بنها، وقد اشتملت العينة الفعلية على (١٥٤) بالكليات العملية، (٩٤) بالكليات النظرية بجانب (٣٠) استبانة للعينة الاستطلاعية وتم تطبيقها عليهم قبل تطبيق الاستبانة بشكل نهائي، ويوضح جدول رقم (٥) توزيع أفراد العينة حسب نوع الكلية والتخصص.

جدول (٥)
توزيع أفراد العينة حسب نوع الكلية والتخصص

الكلية / العينة	الكليات العملية (١٥٤)				الكليات النظرية (٩٤)			المجموع
	الحاسبات والمعلومات	التمريض	الزراعة	الهندسة	التربية	الآداب	الحقوق	
ك	٤٠	٦٠	٣٠	٢٤	٥٥	٢٣	١٦	٢٤٨
%	١٦,١	٢٤,٢	١٢,١	٩,٧	٢٢,٢	٩,٣	٦,٤	١٠٠ %
%	٦٢,١				٣٧,٩			١٠٠ %

- تم تصحيح الاستجابات وفقاً لمقياس ليكرت الثلاثي على النحو الآتي:
- موافق بدرجة كبيرة = ٣
- موافق بدرجة متوسطة = ٢
- موافق بدرجة ضعيفة = ١

٤- الأساليب الإحصائية المستخدمة:

اعتمدت الدراسة فى التحليل الإحصائي للبيانات على استخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية Statistical Package for Social Sciences (SPSS V.18)، بحيث تم استخدام المعالجات الإحصائية التالية:

- حساب معامل ألفا كرونباخ لحساب ثبات الاستبانة.

- **حساب معامل الارتباط لبيرسون لحاسب معامل الارتباط بين درجة كل عبارة والدرجة الكلية للبعد الذي تنتمي إليه العبارة (الاتساق الداخلي للعبارات).**
- **حساب التكرارات والنسبة المئوية لاستجابات أفراد العينة، حيث تعتبر النسبة المئوية أكثر تعبيراً عن الدرجات الخام.**
- **التقدير الرقمي = (ك ١ × ٣) + (ك ٢ × ٢) + (ك ٣× ١). حيث:**

ك١: موافق بدرجة كبيرة

ك٢: موافق بدرجة متوسطة.

ك٣: موافق بدرجة ضعيفة.

$$\text{الوزن النسبي} = \frac{\text{التقدير الرقمي}}{\text{ن}} \times ١٠٠$$

حيث (ن) هو عدد أفراد عينة الدراسة وهو يساوى (٢٤٨).

ولتحديد نسبة التحقق من درجة الموافقة لدى أفراد العينة بصفة عامة لكل عبارة، تم حساب.

- **المدى الكلى = أعلى وزن نسبى – أقل وزن نسبى.**

$$\text{فرق المدى} = \frac{\text{المدى الكلى}}{٣}$$

وذلك لتحديد مرتبة عبارات الاستبانة، حيث:

تم الحكم علي درجة الموافقة وذلك لكل عبارة ضمن أداة الدراسة وفق مقياس ليكرت المفسر لاستجابات عينة البحث وذلك على النحو التالي:

جدول (٦)

مقياس دلالة المتوسط الحسابي

درجة الموافقة	المتوسط الحسابي	
	الي	من
موافق بدرجة ضعيفة	١.٦٦	١
موافق بدرجة متوسطة	٢.٣٣	١.٦٧
موافق بدرجة كبيرة	٣	٢.٣٤

ثانياً: تحليل نتائج الدراسة الميدانية وتفسيرها:

تتضح نتائج الدراسة الميدانية من خلال عرض التحليل الإحصائي الذي تم إجراؤه على محاور الاستبانة، وفيما يلي عرض لهذه النتائج بالتفصيل:

١ -تحليل ابعاد الاستبانة:

استهدفت الاستبانة تعرف متطلبات تحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات من وجهة نظر أعضاء هيئة التدريس بجامعة بنها، ويندرج تحت ذلك خمسة أبعاد رئيسية، وفيما يلي عرض النتائج لهذه الأبعاد إجمالاً:

جدول (٧)

درجة الموافقة على الأبعاد إجمالًا والاستبانة ككل (من وجهة نظر عينة الدراسة) (ن = ٢٤٨)

الابعاد	عدد المؤشرات	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	درجة الموافقة
المتطلبات التقنية	١٥	٢.٢٩	٠.٥١	٧٦.٣٣	متوسطة
المتطلبات المادية	٩	٢.١٠	٠.٥٩	٧٠.٠٠	متوسطة
المتطلبات البشرية	١٤	٢.٠٧	٠.٥٨	٦٩.٠٠	متوسطة
المتطلبات المعرفية	١٧	٢.٠٥	٠.٦٢	٦٨.٣٣	متوسطة
معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها	١٥	٢.٣٢	٠.٥٣	٧٧.٣٣	متوسطة
اجمالي الاستبانة	٧٠	٢.١٧	٠,٥٧	٧٢.٢	متوسطة

يتضح من الجدول السابق (٧) أن: درجة الموافقة على الاستبانة ككل جاءت متوسطة بمتوسط (٢,١٧)، وبنسبة (٧٢.٢%)، ومعنى هذا أن أفراد العينة يجمعون بدرجة متوسطة على تحقيق هذه المتطلبات، وقد يرجع ذلك إلى اتخاذ الجامعة خطوات فعلية لتحقيق متطلبات الأمن السيبراني خاصة في ضوء التحول الرقمي للجامعات، كما انها تأخذ قضية تحقيق متطلبات الأمن السيبراني على محمل الجد، ولا تتوانى عن تحقيق كافة المتطلبات التقنية والمادية والبشرية والمعرفية من أجل تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بأعضاء هيئة التدريس، وحماية شبكة المعلومات والاتصالات من أي اختراق محتمل غير

إنها لا تزال في حاجة للاهتمام بتلك المتطلبات والتغلب على المعوقات وصولاً لمستويات أعلى وديناميات أكثر تأثيرًا والتي لم تظهر كمستويات موافقة كبرى لأي من المحاور فقد جاءت المتطلبات التقنية متوسطة بمتوسط (٢.٢٩)، وبنسبة (٧٦.٣٣%)، كما جاءت المتطلبات المادية متوسطة بمتوسط (٢.١٠)، وبنسبة (٧٠%)، وهو ومن ناحية أخرى جاءت المتطلبات البشرية ايضا متوسطة بمتوسط (٢.٠٧)، وبنسبة (٦٩%)، كما جاءت المتطلبات المعرفية هي الاخرى متوسطة بمتوسط (٢.٠٥)، وبنسبة (٦٨.٣٣%)،ما يشير الى ان الجامعة قد اتخذت خطوات متقاربة لتلبية كل من المتطلبات التقنية والمادية والبشرية والمعرفية وان مالت قليلًا نواحي المتطلبات التقنية وهو وضع طبيعي في ضوء التحول الرقمي للجامعات ، تلاها المتطلبات المالية والتي حصلت على نسبة (٧٠%)، وقد يرجع ذلك ان الجامعة لا تتوانى عن توفير الموارد المالية الذاتية، ولكن يبقى الوضع مرهونا بالسياسة التمويلية المتبعة من قبل وزارة التعليم العالي، والتي تعتمد على الإنفاق الحكومي على توفير متطلبات الأمن السيبراني وتوفير برامج حماية تواجه الهجمات السيبرانية، وهو الأمر الذي جعل أفراد العينة يرون أنه أمر يصعب تحقيقه دون تغيير اللوائح والقوانين المختصة بتلك المتطلبات المالية.

كما يلاحظ ان معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها حصلت أيضا على نسبة موافقة متوسطة بمتوسط (٢.٣٢)، وبنسبة (٧٧,٣٣%). وقد جاءت هذه النتائج متفقة مع ما توصل إليه بحث فينيسا بيرتون *(Venessa Burton ،2018)*؛ والتي خلصت إلى اتفاق افراد عينه البحث على وجود معوقات تحول دون تحقيق متطلبات الأمن السيبراني ، وقد يرجع ذلك الى ضعف القوانين المتبعة في حماية أمن المعلومات في بيئة الإنترنت، وعدم تحديثها بصفة مستمرة في أمن المعلومات؛ نظراً لعدم مواكبتها للجرائم الحديثة، لذلك فهي ليست فعالة بالشكل الكافي، كما أن القوانين تفتقر إلى آلية واضحة للتطبيق؛ نتيجة تنوع الاختراقات الأمنية وتطورها، كما اتفقت مع نتائج دراسة *(الخضري وسلامي وكليبي ،٢٠٢٠)*؛ والتي توصلت إلى وجود اتفاق بين أفراد عينة البحث حول تعدد أسباب حدوث المخاطر والهجمات السيبرانية والذي يعد اهم وأول المعوقات التي تحول دون

تحقيق متطلبات الأمن السيبراني ، ويرجع ذلك إلى عدم وجود سياسات أمنية واضحة وبرامج حماية. وتتفق كذلك مع دراسة *(الشيتى، ٢٠١٤)* والتي تضمنت أهم معوقات تحقيق متطلبات الأمن السيبراني بالجامعات والمتمثلة في ضعف سياسات حماية المعلومات وعدم مواكبتها للتغيرات السائدة في مجال الاختراقات والتهديدات الأمنية بالجامعات.

تحليل عبارات ابعاد الاستبانة :

بعد تحليل كل بعد من ابعاد الاستبانة إجمالاً، سيتم تحليل عبارات كل بعد من هذه الابعاد بالتفصيل على النحو التالي:

البعد الأول: المتطلبات التقنية:

هدف هذا البعد إلى تعرف درجة موافقة افراد العينة على المتطلبات التقنية لتحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات، ويندرج تحت هذا البعد (١٥) عبارة يوضحها جدول (٨).

جدول (٨)
المتطلبات التقنية لتحقيق الأمن السيبراني بجامعة بنها
(ن = ٢٤٨)

م	العبارة	موافق بدرجة كبيرة		موافق بدرجة متوسطة		موافق بدرجة صغيرة		المتوسط	الانحراف المعياري	التقدير الرقمي	الوزن النسبي	مستوى الدلالة	درجة التحقق	الترتيب حسب الرتبة
		ك١	%	ك٢	%	ك٣	%							
١	تحرص الجامعة على وجود قسم خاص وادارة مركزية مختصة بأمن المعلومات والأمن السيبراني بين مختلف كلياتها.	٧٧	٣١.٠	١٠٠	٤٠.٣	٥	٢٨.٦	٢.٠٢	٠.٧٧	٥٠٢	٢٠٢.٤	٠.٠٥	متوسطة	١٣
٢	تقوم الجامعة بعمل تقييم دوري لمخاطر الأمن السيبراني على أنظمة المعلومات بها.	٦٦	٢٦.٦	١٠٨	٤٣.٥	٧٤	٢٩.٨	١.٩٧	٠.٧٥	٤٨٨	١٩٦.٨	٠.٠١	متوسطة	١٤
٣	تهتم الجامعة بعمل نسخ احتياطية للملفات بشكل دوري.	٩٥	٣٨.٣	١٠١	٤٠.٧	٥٢	٢١.٠	٢.١٧	٠.٧٥	٥٣٩	٢١٧.٣	٠.٠١	متوسطة	١١
٤	تهتم الجامعة بعمليات التحديث الضرورية والدورية لبيئة التشغيل المستخدمة لسد الثغرات الأمنية.	٨١	٣٢.٧	١٢٥	٥٠.٤	٤٢	١٦.٩	٢.١٦	٠.٦٩	٥٣٥	٢١٥.٧	٠.٠١	متوسطة	١٢
٥	تتحرى الجامعة الدقة عند اختيار نقاط الاتصال بشبكات المعلومات، ووضعها في مواقع مؤمنة ومحمية من الاختراق.	١٠١	٤٠.٧	١١٦	٤٦.٨	٣١	١٢.٥	٢.٢٨	٠.٦٧	٥٦٦	٢٢٨.٢	٠.٠١	متوسطة	٧
٦	تلتزم الجامعة بفحص الملفات التي يتم تحميلها من المواقع غير المعروفة أو	١٠٥	٤٢.٣	١٠٥	٤٢.٣	٣٨	١٥.٣	٢.٢٧	٠.٧١	٥٦٣	٢٢٧.٠	٠.٠١	متوسطة	٨

	خدمات مشاركة الملفات الواردة عن طريق البريد الإلكتروني الجامعي.												
٧	تحرص الجامعة على عدم ارسال اية معلومات حساسة مثل كلمات المرور وارقام بطاقات الائتمان عبر البريد الإلكتروني.	١٦٣	٦٥.٧	٧٠	٢٨.٢	١٥	٦.٠	٢.٦٠	٠.٦٠	٦٤٤	٢٥٩.٧	٠.٠١	كبيرة	٢
٨	تقوم الجامعة بتشفير جميع المعاملات الرقمية بها. باستخدام برامج تشفير الملفات.	١٠١	٤٠.٧	٨٩	٣٥.٩	٥٨	٢٣.٤	٢.١٧	٠.٧٨	٥٣٩	٢١٧.٣	٠.٠١	متوسطة	١١
٩	تسعى الجامعة لتطبيق التحول الرقمي في كل مدخلات الجامعة.	١٤٩	٦٠.١	٨٥	٣٤.٣	١٤	٥.٦	٢.٥٤	٠.٦٠	٦٣١	٢٥٤.٤	٠.٠١	كبيرة	٣
١٠	تتمتع الجامعة بوجود بوابة معلومات إلكترونية ومصادر تعلم ومحتوى رقمي ومنصات تعليمية الكترونية.	١٦٣	٦٥.٧	٧٩	٣١.٩	٦	٢.٤	٢.٦٣	٠.٥٣	٦٥٣	٢٦٣.٣	٠.٠١	كبيرة	١
١١	ترفع الجامعة درجة الحذر لدى أعضاء هيئة التدريس عند فتح مرفق في البريد الإلكتروني على صفحتها الالكترونية..	١٠٢	٤١.١	١١٧	٤٧.٢	٢٩	١١.٧	٢.٢٩	٠.٦٧	٥٦٩	٢٢٩.٤	٠.٠١	متوسطة	٥
١٢	تهتم الجامعة بضرورة تطوير البنية التحتية السيبرانية بها للحد من الاختراق والتجسس	١٠٣	٤١.٥	١٠٨	٤٣.٥	٣٧	١٤.٩	٢.٢٧	٠.٧٠	٥٦٢	٢٢٦.٦	٠.٠١	متوسطة	٩

	والقرصنة الإلكترونية.												
١٣	تفعل الجامعة البني التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام وفي الخدمات الحكومية الالكترونية بوجه خاص.	٩٩	٣٩.٩	١٢١	٤٨.٨	٢٨	١١.٣	٢.٢٩	٠.٦٦	٥٦٧	٢٢٨.٦	متوسطة	٠.٠١	٦
١٤	تؤكد الجامعة عل ضرورة استخدام كلمة مرور معقدة قوية لا يمكن تخمينها للوصول إليها وتغيرها من وقت لآخر.	١٤٥	٥٨.٥	٨٦	٣٤.٧	١٧	٦.٩	٢.٥٢	٠.٦٢	٦٢٤	٢٥١.٦	كبيرة	٠.٠١	٤
١٥	تشجع الجامعة أعضاء هيئة التدريس على إتقان المهارات التقنية في الأمن السيبراني واستخدام البيانات في اكتشاف التهديدات والاستجابة للحوادث السيبرانية.	٨٨	٣٥.٥	١٢٥	٥٠.٤	٣٥	١٤.١	٢.٢١	٠.٦٧	٥٤٩	٢٢١.٤	متوسطة	٠.٠١	١٠

ومن تحليل البيانات الواردة في الجدول السابق (٨) يتضح أن:

- **احتلت بعض العبارات درجة تحقق كبيره، حيث جاءت العبارة رقم (١٠) في المرتبة (الاولى)، وهي:(تتمتع الجامعة بوجود بوابة معلومات إلكترونية ومصادر تعلم ومحتوى رقمي ومنصات تعليمية الكترونية). وسجلت درجة تحقق كبيرة بمتوسط (٢,٦٣) وتعزو الدراسة هذه النتيجة الى ان جامعة بنها تسعي باستمرار لتحقيق سياسة الجامعة للتحول الرقمي ورفع وتحسين القدرات التكنولوجية لعمليات التعليم والتعلم خلال مركز التعلم الإلكتروني بجامعة بنها ، ومنصة إدارة التعلم عن بعد، والمنصة الإلكترونية لإدارة التعلم (LMS) القائمة على نظام موودل الهادفة لتوفير فرصة للتعلم لجميع طلاب الجامعة فى**

بيئة تعليمية مناسبة يتواصل من خلالها الطلاب مع أعضاء هيئة التدريس تطبيقا لنظام التعليم الهجين والذي يعتمد على الدمج بين التعلم وجها لوجه والتعلم عن بعد. وقد يشير ذلك الى اهتمام الجامعة بتلبية متطلبات الأمن السيبراني خاصة المتطلبات التقنية والاهتمام بحصول الطلاب وأعضاء هيئة التدريس على الحساب الخاص بهم للدخول على المنصة من خلال التواصل مع وحدات الخدمات التكنولوجية بالكليات، أو من خلال منسقي التعلم الإلكتروني بالأقسام العلمية بالكلية.

- وهو ما اتفق تماما مع العبارة رقم (٩) حيث جاءت في المرتبة (الثالثة)، وهي: (تسعى الجامعة لتطبيق التحول الرقمي في كل مدخلات الجامعة). وسجلت درجة تحقق كبيرة بمتوسط (٢,٥٤)،

ومما يؤكد ذلك وجود برنامج " أمن المعلومات واكتشاف الأدلة الجنائية الرقمية "بكلية الحاسبات والذكاء الاصطناعي بجامعة بنها ويعد هذا التخصص فريد من نوعه وتنفرد به جامعة بنها على باقي كليات الحاسبات والمعلومات الحكومية على مستوى الجمهورية وبدأت الدراسة في البرنامج من العام الأكاديمي ٢٠١٨–٢٠١٩ ويقوم أساسا على تحقيق الأمن السيبراني وهو العلم المختص بتأمين المعلومات المتداولة عبر شبكة الانترنت أو المحفوظة على أجهزة تخزين البيانات المختلفة من المخاطر التي تهددها خاصة مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لأخر.

- كما جاءت العبارة رقم (٧) في المرتبة (الثانية)، وهي (تحرص الجامعة على عدم ارسال اية معلومات حساسة مثل كلمات المرور وارقام بطاقات الائتمان عبر البريد الإلكتروني). وسجلت درجة تحقق كبيرة بمتوسط (٢,٦٠) مما يدل على وعي أعضاء هيئة التدريس بجريمة سرقة كلمات المرور وارقامها السرية عبر شبكة الانترنت حيث إنها جريمة شائعة وتسبب الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات أو حذفها أو الاطلاع عليها سواء المعلومات الشخصية، أو المعلومات الخاصة بالبنوك ،أو المؤسسات، أو الحكومات والقيام بتهديدهم أما لتحقيق هدف مادي أو سياسي وكذلك الكسب المادي أو المعنوي أو السياسي غير المشروع مثل تزوير بطاقات الائتمان وسرقة الحسابات المصرفية منها.

- **كما حصلت العبارة رقم (١٤) على المرتبة (الرابعة)، وهي:(تؤكد الجامعة عل ضرورة اختيار كلمة مرور معقدة قوية لا يمكن تخمينها للوصول إليها والاهتمام بتغييرها من وقت لآخر) وسجلت درجة تحقق كبيرة بمتوسط (٢,٥٢) وهذا يشير إلى وعي أفراد مجتمع الدراسة المتوسط وغير الكافي بأهمية اختيار كلمة مرور قوية وتغييرها كل فترة ، مما يؤكد ضرورة أن يهتم أفراد مجتمع الدراسة بذلك، وألا يكون سرعة الوصول إلى بياناتهم الدائم هو الذي يجعلهم يختارون كلمة مرور سهلة ولا يغيرونها إلا إذا نسوها. وهو ما يتفق مع دراسة كل من *(العريشي والدوسري، ٢٠١٨)،(صائغ، ٢٠١٨)* حيث طرحت تلك الدراسات بعض الإجراءات الواجب اتخاذها للحماية في الفضاء السيبراني، حيث ذكر العمل على تغيير كلمات المرور بشكل دوري، وتحديث نظام تشغيل الحاسوب باستمرار، واستخدام برامج مكافح الفيروسات، والحرص على استخدام المتصفح الخفي عند الولوج للشبكات العامة، وإغلاق الأجهزة غير المستخدمة، ووضع كلمات مرور على الشبكة اللاسلكية المنزلية، أو أي شبكة تعمل بها.**
- **أما باقي العبارات فقد حصلت على درجة موافقة متوسطة وتشابهت كل من العبارة رقم (١١) التي اختلت المرتبة (الخامسة)، وهي: (ترفع الجامعة درجة الحذر لدى أعضاء هيئة التدريس عند فتح مرفق في البريد الإلكتروني على صفحتها الالكترونية) والتي تشير إلى وعي أفراد مجتمع الدراسة بخطورة فتح أي رابط يصل إليهم من مصدر مجهول، مما يعني أنهم يعرفون مدى المفاسد المترتبة على ذلك مع العبارة رقم (١٣) التي احتلت المرتبة (السادسة)، وهي: (تفعل الجامعة البني التحتية اللازمة لدعم الثقة في التعاملات الالكترونية بوجه عام وفي الخدمات الحكومية الالكترونية بوجه خاص). حيث سجلت كل منهما درجة تحقق متوسطة بمتوسط (٢,٢٩)، مما يشير الى اهتمام جامعة بنها بتأمين البنى التحتية لأمن البيانات المعلومات الخاصة بأعضاء هيئة التدريس، وحماية شبكة المعلومات والاتصالات من أي اختراق محتمل، والتي تقوم بدوراً رئيسياً في تدفق المعلومات والبيانات من مقدم الخدمة إلى مستقبل الخدمة، ولذلك من الضروري توعية العاملين بمخاطر استخدام الأجهزة الشخصية مثل الهاتف المحمول لتخزين أو نقل معلومات سرية خاصة بالجامعة، ومنح الحوافز المادية والمعنوية للموظفين المتميزين والمبدعين في مجال الأمن السيبراني.**

- **وجاءت هذه النتيجة متفقة مع ما توصلت إليه دراسة *(الصاحب،٢٠١٣)*؛ والتي أكدت على أنه من الضروري توفير وثيقة متعلقة بسياسة الأمن المعلوماتي في الجامعات، على أن تكون متبوعة بالعديد من الإجراءات والتعليمات التي يجب أن يلتزم بها كافة المستفيدين من هذه السياسات في الجامعة، وأنه يجب أن تتم صياغة السياسات بناء على المخاطر المحددة، وأنه من الضروري إنشاء إدارة خاصة تهتم بأمن المعلومات في الجامعة. واتفقت كذلك مع دراسة رحمان وآخرون *(Rehman et al،2015)*؛ والتي أوصت بضرورة وجود إدارة للمخاطر، ووضع سياسات أمنية لمعالجة هذه المخاطر. كما اتفقت ايضا مع نتائج دراسة فينيسا بيرتون *(Venessa Burton،2018)*؛ والتي أوصت بضرورة توحيد القوانين التي تتصدى لهذه الجرائم، بالإضافة إلى وضع سياسات واستراتيجيات لأمن المعلومات تكون كافية لتنظيم ممارسات الأمن والحماية. كما اتفقت مع دراسة *(الشيتى،٢٠١٤)*، والتي أوصت بضرورة وجود برامج توعية الموظفين، وضرورة نشر الوعي بالأمن السيبراني بين أعضاء هيئة التدريس والموظفين بالجامعة.**
- **كما حصلت العبارة رقم (٥) على المرتبة (السابعة)، وهي :(تتحرى الجامعة الدقة عند اختيار نقاط الاتصال بشبكات المعلومات، ووضعها في مواقع مؤمنة ومحمية من الاختراق). وسجلت درجة تحقق متوسطة بمتوسط (٢,٢٨)، مما يشير الى عدم الدقة في اختيار مواقع نقاط الشبكة: فلا بد من الدقة عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية من الاختراق .**
- **واحتلت كل من العبارة رقم (٦) التي جاءت في المرتبة(الثامنة) والعبارة رقم (١٢) التي جاءت في المرتبة (التاسعة) نفس المتوسط الحسابي حيث سجلت كل منهما درجة تحقق متوسطة بمتوسط حسابي (٢,٢٧)، وهما على التوالي العبارتان:(تلتزم الجامعة بفحص الملفات التي يتم تحميلها من المواقع غير المعروفة أو خدمات مشاركة الملفات الواردة عن طريق البريد الإلكتروني الجامعي)، و(تهتم الجامعة بضرورة تطوير البنية التحتية السيبرانية بها للحد من الاختراق والتجسس والقرصنة الإلكترونية)**
- **كما حصلت العبارة رقم (١٥) على المرتبة (العاشرة)، وهي :(تشجع الجامعة إتقان المهارات التقنية في الأمن السيبراني واستخدام البيانات في اكتشاف التهديدات والاستجابة للحوادث السيبرانية) وسجلت درجة تحقق متوسطة بمتوسط (٢,٢١)**

- **بينما جاءت كل من العبارة رقم (٨) والعبارة رقم (٣) في المرتبة (الحادية عشر) حيث حققتا كلا منهما درجة موافقة متوسطة بمتوسط (٢,١٧) وهما:(تهتم الجامعة بعمل نسخ احتياطية للملفات بشكل دوري) ، و(تقوم الجامعة بتشفير جميع المعاملات الرقمية بها. باستخدام برامج تشفير الملفات) وهذا يدل على أن معظم أعضاء هيئة التدريس لديهم وعي بعمل النسخ الاحتياطية من البيانات الخاصة به بشكل دوري لأنه أمر بالغ الأهمية خوفا من فقد الجهاز أو احتياجه أو إعادة تهيئته لسبب ما أو تثبيت عدد من التطبيقات المهمة أو إضافة جهات اتصال أو تعديلها والذي يتطلب من المستخدم المبادرة في نسخ بياناته احتياطيا. إضافة الى وعي الجامعة بأهمية وجود برامج الحماية من الفيروسات وهي برامج تعمل على مكافحة الفيروسات أو البرامج الخبيثة ومنعها من دخول الحاسب ثم حذفها بشكل نهائي مثل الديدان أو أحصنة طروادة أو برامج التجسس وغيرها من البرامج الخبيثة والمضرة بالنظام، وهو ما يتفق مع نتائج دراسة *(ياسين،٢٠٠٩، ٣٥٢)*، التي اكدت ضرورة وضع نظام حماية فعال يقلل إلى أدنى حد ممكن مشكلة كشف المعلومات ذات الأهمية القصوى. ومن ضمن تلك الإجراءات عمل نسخ احتياطية لبعض الملفات المهمة؛ خشية من التدمير، أو الفقدان.**
- **كما جاءت العبارة رقم (٤) في المرتبة (الثانية عشر) حيث حققت درجة موافقة متوسطة بمتوسط (٢,١٦) وهي:(تهتم الجامعة بعمليات التحديث الضرورية والدورية لبيئة التشغيل المستخدمة لسد الثغرات الأمنية) مما يدل على ان الجامعة لا تعطي الاهتمام الكامل بعمليات التحديث المستمر لمواجهة الثغرات الأمنية بالرغم من جامعة بنها تسعي باستمرار لتحقيق سياسة الجامعة في مواجهة الجرائم السيبرانية.**
- **كما جاءت العبارة رقم (١) في المرتبة (الثالثة عشر) حيث حققت درجة موافقة متوسطة بمتوسط (٢,٠٢) والتي تنص على:(تحرص الجامعة على وجود قسم خاص وادارة مركزية مختصة بأمن المعلومات والأمن السيبراني بين مختلف كلياتها) ، ويمكن أن يعزى ذلك إلى انه بالرغم من إنشاء الجامعة مركز أمن المعلومات والتعليم الالكتروني والتعليم عن بعد، يختص بإدارة وحوكمة أمن المعلومات من خلال تطبيق الإجراءات الأمنية اللازمة لضمان سلامة الأصول التقنية والمعلوماتية للجامعة، وضمان إدارة فعالة لجميع مخاطر ومهددات أمن المعلومات المحتملة وتطبيق الحلول التقنية الوقائية اللازمة، ورفع مستوى الوعي في**

الأمن السيبراني الا ان أعضاء هيئة التدريس بالجامعة ليس لديهم المعرفة الكاملة عن تلك المراكز، وقد يرجع ذلك أيضا الى ان معظم الجامعات تضع مهام أمن المعلومات على قسم يتعلق بتكنولوجيا الاتصالات والمعلومات وأنظمة المعلومات، ولا يتم تخصيص قسم خاص وادارة مركزية مختصة بأمن المعلومات ذاتها.

- **كما جاءت العبارة رقم (٢) في المرتبة (الرابعة عشر) حيث حققت درجة موافقة متوسطة بمتوسط (١,٩٧) وهي:(تقوم الجامعة بعمل تقييم دوري لمخاطر الأمن السيبراني على أنظمة المعلومات بها.) ويمكن أن يعزى ذلك إلى انه بالرغم من وجود برنامج أمن المعلومات يختص بإدارة وحوكمة أمن المعلومات وهو ما تمت الاشارة اليه بالعبارة التي احتلت المرتبة الثالثة الا انه لا يقوم بتطبيق الإجراءات الأمنية اللازمة لضمان سلامة الأصول التقنية والمعلوماتية للجامعة، ورفع مستوى الوعي في الأمن السيبراني.**

البعد الثاني: المتطلبات المادية:

هدف هذا البعد إلى تعرف درجة موافقة افراد العينة على المتطلبات المادية لتحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات، ويندرج تحت هذا البعد (٩) عبارات يوضحها جدول (٩).

جدول (٩)
المتطلبات المادية لتحقيق الأمن السيبراني بجامعة بنها
(ن = ٢٤٨)

م	العبارة	موافق بدرجة كبيرة		موافق بدرجة متوسطة		موافق بدرجة صغيرة		المتوسط	الانحراف المعياري	التقدير الرقمي	الوزن النسبي	الدلالة	درجة التحقق	الترتيب حسب الرتبة
		ك١	%	ك٢	%	ك٣	%							
١	توفر الجامعة برامج حديثة لتدريب الهيئة التدريسية على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم.	٨٢	٣٣.١	١٠١	٤٠.٧	٦٥	٢٦.٢	٢.٠٧	٠.٧٧	٥١٣	٢٠٦.٩	٠.٠١	متوسطة	٥
٢	توفر الجامعة الدعم الفني والتقني اللازم لأعضاء هيئة التدريس لمعالجة المشكلات الطارئة	٨٨	٣٥.٥	١٠٣	٤١.٥	٥٧	٢٣.٠	٢.١٣	٠.٧٦	٥٢٧	٢١٢.٥	٠.٠١	متوسطة	٢
٣	تعمل الجامعة على زيادة الإنفاق على حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات للمؤسسات المختلفة من المخاطر السيبرانية	٨٤	٣٣.٩	١١٧	٤٧.٢	٤٧	١٩.٠	٢.١٥	٠.٧١	٥٣٣	٢١٤.٩	٠.٠١	متوسطة	١
٤	توفر الجامعة بنية تحتية تكنولوجية وأجهزة	٧٦	٣٠.٦	١٣٣	٥٣.٦	٣٩	١٥.٧	٢.١٥	٠.٦٧	٥٣٣	٢١٤.٩	٠.٠١	متوسطة	١

	اتصالات حديثة تمكن الجامعة من تقديم خدماتها بشكل الكتروني												
٥	تمتلك الجامعة نظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الالكترونية بين أعضاء هيئة التدريس.	٧١	٢٨.٦	١٢٩	٥٢.٠	٤٨	١٩.٤	٢.٠٩	٠.٦٩	٥١٩	٢٠٩.٣	٠.٠١	متوسطة	٣
٦	تمنح الجامعة الجوائز المادية والمعنوية للمتميزين والمبدعين من أعضاء هيئة التدريس في مجال الأمن السيبراني	٦٢	٢٥.٠	١٢٦	٥٠.٨	٦٠	٢٤.٢	٢.٠١	٠.٧٠	٤٩٨	٢٠٠.٨	٠.٠١	متوسطة	٧
٧	تمتلك الجامعة برامج حديثة لحماية الهوية الرقمية مثل (برنامج المواطنة الرقمية).	٦٣	٢٥.٤	١٣٤	٥٤.٠	٥١	٢٠.٦	٢.٠٥	٠.٦٨	٥٠٨	٢٠٤.٨	٠.٠١	متوسطة	٦
٨	توفير المخصصات المالية اللازمة لتحقيق الأمن السيبراني.	٧٨	٣١.٥	١١٣	٤٥.٦	٥٧	٢٣.٠	٢.٠٨	٠.٧٣	٥١٧	٢٠٨.٥	٠.٠١	متوسطة	٤
٩	تمتلك الجامعة نظام شبكي آمن لتبادل المعلومات الإدارية	٨٤	٣٣.٩	١١٧	٤٧.٢	٤٧	١٩.٠	٢.١٥	٠.٧١	٥٣٣	٢١٤.٩	٠.٠١	متوسطة	١

ومن تحليل البيانات الواردة في الجدول السابق (٩) يتضح أن:

- **حصلت كل من العبارات (٣) التي نصت على: (تعمل الجامعة على زيادة الإنفاق على حماية البنى التحتية للاتصالات وتكنولوجيا المعلومات للمؤسسات المختلفة من المخاطر**

السيبرانية)، والعبارة رقم (٤) التي نصت على: (توفر الجامعة بنية تحتية تكنولوجية وأجهزة اتصالات حديثة تمكن الجامعة من تقديم خدماتها بشكل الكتروني)، وكذلك العبارة رقم (٩) والتي تنص على :(تمتلك الجامعة نظام شبكي آمن لتبادل المعلومات الإدارية) على المراتب الأولى بدرجة موافقة متوسطة بمتوسط حسابي (٢.١٥) وتعزو الباحثة هذه النتيجة الى الوعي لدى جامعة بنها بأهمية الأمن السيبراني في تأمين البنى التحتية لأمن المعلومات والبيانات للمؤسسات المختلفة، وحماية شبكة المعلومات والاتصالات من أي اختراق محتمل، والتي تؤدي دوراً رئيسياً في تدفق المعلومات والبيانات من مقدم الخدمة إلى مستقبل الخدمة، ولذلك من الضروري زيادة الإنفاق على حماية البنى التحتية ، ومنح الحوافز المادية والمعنوية للموظفين المتميزين والمبدعين في مجال الأمن السيبراني

- تلاها العبارة رقم (٢) التي نصت على: (توفر الجامعة الدعم الفني والتقني اللازم لأعضاء هيئة التدريس لمعالجة المشكلات الطارئة) حيث احتلت المرتبة الثانية بدرجة تحقق متوسطة بمتوسط حسابي (٢,١٣)، واحتلت العبارة رقم (٥) التي نصت على: (تمتلك الجامعة نظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الالكترونية بين أعضاء هيئة التدريس) المرتبة الثالثة بدرجة موافقة متوسطة بمتوسط (٢,٠٩)، تلاها العبارة رقم (٨)، حيث احتلت المرتبة الرابعة بدرجة موافقة متوسطة بمتوسط (٢,٠٨) وقد نصت على: (توفير المخصصات المالية اللازمة لتحقيق الأمن السيبراني) .
- حصلت العبارة رقم (١) على المرتبة الخامسة والتي تنص على (توفر الجامعة برامج حديثة لتدريب الهيئة التدريسية على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم ومكافحة البرمجيات الضارة) على درجة موافقة متوسطة وبمتوسط حسابي (٢,٠٧)، وربما يعزى ذلك إلى قلة تناول أعضاء هيئة التدريس مسألة الدراية بالتكنولوجيات وتوافر الأدوات التكنولوجية لضمان الحماية من شتى المخاطر السيبرانية، فتعزيز أعضاء هيئة التدريس الإدراك النظري ليس كافياً إذا لم تكتسب المعارف العلمية أو التكنولوجية اللازمة، وتشمل المعارف العلمية إعلام أعضاء هيئة التدريس بفوائد البرمجيات المتاحة للأمن السيبراني، إذ تؤدى تعزيز برامج هذه البرمجيات دوراً رئيسياً في مكافحة المخاطر السيبرانية، وتعتبر فئة أعضاء هيئة التدريس الفئة الأكثر عرضة

للمخاطر التي تهدد الأمن السيبراني نظراً إلى تفاعلهم مع خدمات الاتصالات ، وتختلف هذه النتيجة مع دراسة *(الصانع وآخرون ،٢٠٢٠)* والتي أظهرت ارتفاع وعى المعلمين بالأمن السيبراني.

- **ويرجع مجيء العبارة رقم (٧) ونصها: (تمتلك الجامعة برامج حديثة لحماية الهوية الرقمية مثل (برنامج المواطنة الرقمية). بالمرتبة قبل الأخيرة بدرجة موافقة متوسطة وبمتوسط حسابي بلغ (٢,٠٥) وربما يعزى ذلك إلى قلة تثقيف أعضاء هيئة التدريس بجامعة بنها بالوسائل الأكثر فعالية للحماية من الرسائل الاقتحامية للهوية الرقمية ، فإذا قام عضو هيئة التدريس بفتح الوثيقة المرفقة فيمكن لبرامج مكافحة الفيروسات المحدثة ولبرمجيات أنظمة التشغيل أن تتيح تجنب الإصابة، وتعتبر مرشحات مكافحة الرسائل الاقتحامية عنصراً مهم للحرص على أن يبقى البريد الإلكتروني أداة تواصل فعالة، وتعتبر وسيلة مهمة لتفادى اقتحام الأجهزة، وتختلف هذه النتيجة مع دراسة *(العريشي، الدوسري ،٢٠١٨)* والتي أوصت بضرورة تثقيف وعي الطلاب بأهمية نشر ثقافة أمن المعلومات، وتنظيم حملات على مستوى الجامعة لتعزيز الأمن المعلوماتي.**
- **بينما احتلت العبارة رقم (٦) المرتبة الأخيرة، والتي نصت على: (تمنح الجامعة الجوائز المادية والمعنوية للمتميزين والمبدعين من أعضاء هيئة التدريس في مجال الأمن السيبراني) وقد حصلت على درجة موافقة متوسطة بمتوسط (٢,٠١) مما يشير الى انه بالرغم من اهتمام الجامعة بتحقيق متطلبات الأمن السيبراني سواء التقنية والبشرية والمعرفية الا ان المتطلبات المادية لا تنال نفس الاهتمام وقد يرجع الى ضعف المخصصات المالية بالجامعة او لا يوجد تمويل كافي لمنح الجامعة الجوائز المادية والمعنوية للمتميزين والمبدعين من أعضاء هيئة التدريس في مجال الأمن السيبراني.**

البعد الثالث: المتطلبات البشرية:

هدف هذا البعد إلى تعرف درجة موافقة افراد العينة على المتطلبات البشرية لتحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات، ويندرج تحت هذا البعد (١٤) عبارات يوضحها جدول (١٠).

جدول (١٠)
المتطلبات البشرية لتحقيق الأمن السيبراني بجامعة بنها
(ن = ٢٤٨)

م	العبارة	موافق بدرجة كبيرة		موافق بدرجة متوسطة		موافق بدرجة صغيرة		المتوسط	الانحراف المعياري	التقدير الرقمي	الوزن النسبي	الدلالة	درجة التحقق	الترتيب حسب الرتبة
		ك١	%	ك٢	%	ك٣	%							
١	تقوم الجامعة بتوعية أعضاء هيئة التدريس بمخاطر إرسال المعلومات الشخصية عبر الرسائل النصية أو البريد الإلكتروني.	١٠٩	٤٤.٠	١٠٠	٤٠.٣	٣٩	١٥.٧	٢.٢٨	٠.٧٢	٥٦٦	٢٢٨.٢	٠.٠١	متوسطة	٢
٢	تحرص الجامعة	١٢٨	٥١.٦	٩٧	٣٩.١	٢٣	٩.٣	٢.٤٢	٠.٦٦	٦٠١	٢٤٢.٣	٠.٠١	كبيرة	١

Print:(ISSN 1687-2649) Online:(ISSN 2536-9091)

	على وضع استراتيجيات للمساعدة في الحد من الجرائم الإلكترونية وتعزيز الأمن السيبراني												
٣	تؤهل الجامعة الموارد البشرية القائمة على تقنية المعلومات في مجال تطبيق الأمن السيبراني	٧٦	٣٠.٦	١٣٦	٥٤.٨	٣٦	١٤.٥	٢.١٦	٠.٦٥	٥٣٦	٢١٦.١	٠.٠١	متوسطة	٣
٤	تقوم الجامعة بعمل لقاءات دورية	٥٨	٢٣.٤	١٢٤	٥٠.٠	٦٦	٢٦.٦	١.٩٧	٠.٧١	٤٨٨	١٩٦.٨	٠.٠١	متوسطة	١٠

	للمخاطر المرتبطة بتطبيق الأمن السيبراني لتعزيز فهم المساءلة في المجال.	٥٤	٢١.٨	١٢٠	٤٨.٤	٧٤	٢٩.٨	١.٩٢	٠.٧٢	٤٧٦	١٩١.٩	٠.٠١	متوسطة	١٤
٥	تنبأ الجامعة الخاصة بالمراكز الجامعية الأجنبية والعربية في مجال الأمن السيبراني	٥٤	٢١.٨	١٢٠	٤٨.٤	٧٤	٢٩.٨	١.٩٢	٠.٧٢	٤٧٦	١٩١.٩	٠.٠١	متوسطة	١٤
٦	تنظم الجامعة حملات توعية لأعضاء هيئة التدريس للتعامل	٥٢	٢١.٠	١٣٥	٥٤.٤	٦١	٢٤.٦	١.٩٦	٠.٦٨	٤٨٧	١٩٦.٤	٠.٠١	متوسطة	١١

	رية ف بالأم ن الس يبرا ني، ومخ اطر ه ، وتد قيق متط لبا ت ه.												
٧	تعز ز الج معة مهل رات أع ضا ء هيئ ة التد ريس في مجا ل الأم ن الس يبرا ني من خلا ل عقد دور ات تدر يبية متخ صصة في أسا ليب تخدا م كافة الوسا ئل التق نية بطر ق آمنه	٥٦	٢٢.٦	١٢٢	٤٩.٢	٧٠	٢٨.٢	١.٩٤	٠.٧١	٤٨٢	١٩٤.٤	٠.٠١	متوسطة	١٢

Print:(ISSN 1687-2649) Online:(ISSN 2536-9091)

٨	تعقد الجامعة شراكات بينها وبين الجامعات المصرية لتنفيذ منتديات عن ثقافة الأمن السيبراني.	٦٤	٢٥.٨	١٢٢	٤٩.٢	٦٢	٢٥.٠	٢.٠١	٠.٧١	٤٩٨	٢٠٠.٨	٠.٠١	متوسطة	٩
٩	تفعل الجامعة التواصل مع المؤسسات المجتمع المدني لنشر ثقافة الأمن السيبراني.	٦٠	٢٤.٢	١١٣	٤٥.٦	٧٥	٣٠.٢	١.٩٤	٠.٧٤	٤٨١	١٩٤.٠	٠.٠١	متوسطة	١٣
١٠	توفر الجامعة خبراء ومختصين	٦١	٢٤.٦	١٢٩	٥٢.٠	٥٨	٢٣.٤	٢.٠١	٠.٦٩	٤٩٩	٢٠١.٢	٠.٠١	متوسطة	٨

	في الأمن السيبراني؛ لفحص الأجهزة والبرمجيات بصفة دورية في الجامعات.												
١١	تقوم الجامعة بعقد بروتوكولات تعاون بين إدارة الأمن المعلوماتي بالجامعة وإدارة الأمن التابعة لها.	٦٢	٢٥.٠	١٤١	٥٦.٩	٤٥	١٨.١	٢.٠٧	٠.٦٥	٥١٣	٢٠٦.٩	٠.٠١	متوسطة	٦
١٢	تحرص الجامعة على تطوير العناصر البشري	٦٣	٢٥.٤	١٣٢	٥٣.٢	٥٣	٢١.٤	٢.٠٤	٠.٦٨	٥٠٦	٢٠٤.٠	٠.٠١	متوسطة	٧

	وتنمية الكوادر البشرية والمهارات اللازمة للتفعيل منظومة الأمن السيبراني في مختلف القطاعات.												
١٣	تهتم الجامعة بالعناصر البشرية الكفؤ والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة.	٧٢	٢٩.٠	١٤٢	٥٧.٣	٣٤	١٣.٧	٢.١٥	٠.٦٤	٥٣٤	٢١٥.٣	٠.٠١	متوسطة	٤

١٤	تحرص الجامعة على وضع وتنفيذ خطط وحملات للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية المؤمنة للأفراد والمؤسسات.	٦٨.٠	٢٧.٤	١٣٢.٠	٥٣.٢	٤٨.٠	١٩.٤	٢.٠٨	٠.٦٨	٥١٦	٢٠٨.١	٠.٠١	متوسطة	٥

ومن تحليل البيانات الواردة في الجدول السابق(١٠) يتضح أن:

- حصلت العبارة(٢) على المرتبة الاولي التي تنص على : (تحرص الجامعة على وضع استراتيجيات لمساعدة أعضاء هيئة التدريس في الحد من الجرائم الإلكترونية وتعزيز الأمن السيبراني) وربما يرجع ذلك الى مدي حرص جامعة بنها على مساعدة أعضاء هيئة التدريس على الحد من الجرائم الالكترونية وتعزيز الأمن السيبراني وقد يرجع ذلك الى معرفتها الكاملة بأن معظم الهجمات الإلكترونية تنشأ بسبب خطأ بشري يرتبط بنقص المعرفة حول اختلاف ديناميات الجرائم الإلكترونية والأمن السيبراني، وأن زيادة المعرفة والوعي من قبل أعضاء هيئة التدريس وغيرهم من الموظفين المعنيين بديناميات

الأمن السيبراني يعد ضروريًا للغاية في الحد من تلك الجرائم وهو ما يتفق مع دراسة كل من (جاد الحق ، ٢٠١٩) (Ahmed, A.2020) (Mohammed I. Alghamdi,2020) والتي سعت كلا منها لتطوير رؤية استراتيجية لمكافحة الجرائم الإلكترونية لتعزيز الأمن السيبراني ، من خلال التعرف على طبيعة وأنواع الجرائم الإلكترونية وأبعاد الأمن السيبراني، ودور مكافحة الجرائم الإلكترونية في تعزيز الأمن السيبراني.

- ويرجع مجيء الفقرة (١) ونصها :(تمتلك الجامعة برامج حماية للرسائل الاقتحامية والبرمجيات الضارة لحماية المعلومات الشخصية اثناء ارسالها عبر الرسائل النصية أو البريد الإلكتروني) بالمرتبة الثانية وبمتوسط حسابي(٢,٢٨) وربما يعزي ذلك الى ان الجامعة لديها العديد من الوسائل الأكثر فعالية للحماية من الرسائل الاقتحامية، فإذا قام عضو هيئة التدريس بفتح البريد الإلكتروني الخاص به وما يحمله من وثائق مرفقة فيمكن لبرامج مكافحة الفيروسات المحدثة ولبرمجيات أنظمة التشغيل أن تتيح تجنب الإصابة، وتعتبر مرشحات مكافحة الرسائل الاقتحامية عنصراً مهم للحرص على أن يبقى البريد الإلكتروني أداة تواصل فعالة، وتعتبر وسيلة مهمة لتفادي اقتحام الأجهزة.
- كما يرجع مجيء الفقرة (١٣) ونصها :(تهتم الجامعة بالعناصر البشرية الكفؤ والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة) بالمرتبة الرابعة وبمتوسط حسابي بلغ (٢.١٥) وربما يعزي ذلك الى وعي الجامعة بان دور التقنية لن يكون مقتصرا على توفير الأجهزة وملحقاتها وإنما يقوم العنصر البشري وتحديدا الأجيال الصاعدة الدور الكبير والأساسي في توجيه وتطويع الأجهزة التقنية والبرامج المساندة لها. وهو المكون الأساس والجوهري الذي يجب أن تبنى عليه البرامج التي ستعمل على تنفيذ برنامج الأمن السيبراني. حيث أجمعت كثير من الدراسات والتقارير الدولية على أن العنصر البشري يسهم بأكثر من ٩٠ % في برامج الأمن السيبراني وذلك ب (دراسات أكاديمية، تطوير برمجيات، تطوير أجهزة تقنية، ثقافة مجتمعية، برامج تدريبية، قوانين وسياسات، اتفاقيات دولية، وسياسة إعلامية) وكل هذه العناصر تعتمد على القدرات البشرية بشكل خاص)(Joshi& Patil,2012)
- أما العبارة (٦) ونصها: (تنظم الجامعة حملات توعية لأعضاء هيئة التدريس للتعريف بالأمن السيبراني، ومخاطره ، وتحقيق متطلباته) فقد احتلت المرتبة الحادية عشر وكونها

جاءت بدرجة موافقة متوسطة يعزي الى ان جامعة بنها تمتلك درجة متوسطة من الوعي بمفاهيم الأمن السيبراني وعدم دعوتها بتنظيم حملات للتوعية به، وهو ما يشير إلى عدم معرفتها بخطورة التفريط في الأمن السيبراني، وأهمية الوعي به.

- كما احتلت العبارة (٧) ونصها: (تعزز الجامعة مهارات أعضاء هيئة التدريس في مجال الأمن السيبراني من خلال عقد دورات تدريبية متخصصة في استخدام كافة الوسائل التقنية بطرق آمنه) المرتبة الثانية عشر بمتوسط حسابي مقداره(١,٩٤) ، وهذا يشير إلى وعي أفراد مجتمع الدراسة كان متوسط وغير كافي بأهمية التسجيل في الدورات التدريبية في مجال الأمن السيبراني، ووعيهم بقدرة المهارات التي تقدم لهم في الدورات التدريبية في الأمن السيبراني على حمايتهم من الاختراقات الخطيرة لمعلوماتهم الحاسوبية كانت متوسطة.
- حصلت العبارة رقم (١٠) ونصها: (توفر الجامعة خبراء ومختصين في الأمن السيبراني؛ لفحص الأجهزة والبرمجيات بصفة دورية في الجامعات من أجل تطبيق الأمن السيبراني مما يعزز ثقة المستخدمين) على المرتبة الثامنة بمتوسط حسابي (٢,٠١)، ويمكن تفسير ذلك في ضوء أن أساليب وتقنيات الأمن السيبراني بحاجة إلى قدرات فنية وبرمجية ومعرفة عميقة بالجريمة السيبرانية، وهذا يجعل جامعة بنها تتجه لاستشارة ذوي الخبرة، ويمكن تفسير هذه النتيجة من جهة أخرى حيث إن معظم الجامعات المصرية تهتم بالأمن السيبراني وتدعو الجامعات إلى الانتماء للاتفاقات واستشارة المراكز المختصة، مثل: الاستراتيجية الوطنية للأمن السيبراني ، وأكاديمية الأمن السيبراني في مصر المختصة بتثقيف وتطبيق مهارات التعامل مع تحديات الأمن السيبراني، والمركز العربي الإقليمي للأمن السيبراني (ITU-ARCC) ، والمركز المصري للاستجابة لطوارئ الإنترنت ، والجهاز القومي لتنظيم الاتصالات لمناقشة قضايا الأمن السيبراني. والمركز المصري للاستجابة للطوارئ المعلوماتية الجديد (CERT).
- وجاءت العبارة (٥) ونصها: (تتبادل الجامعة الخبرات مع الجامعات الأجنبية والعربية في مجال الأمن السيبراني) في ادني المراتب حيث احتلت المرتبة الرابعة عشر والأخيرة بمتوسط حسابي (١.٩٢) وقد يرجع ذلك الى قلة التعاون مع الدول الصديقة والمنظمات الدولية والاقليمية ذات الصلة: ومن ثم ضعف تبادل الخبرات وتنسيق المواقف

في مجال أمن الفضاء السيبراني ومكافحة الجرائم السيبرانية، على الرغم من ان تلك الجرائم لا تعترف بالحدود الجغرافية أو السياسية.

البعد الرابع : المتطلبات المعرفية :

هدف هذا البعد إلى تعرف درجة موافقة افراد العينة على المتطلبات المعرفية لتحقيق الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات، ويندرج تحت هذا البعد (١٧) عبارات يوضحها جدول (١١).

جدول (١١)
المتطلبات المعرفية لتحقيق الأمن السيبراني بجامعة بنها
(ن = ٢٤٨)

م	العبارة	موافق بدرجة كبيرة		موافق بدرجة متوسطة		موافق بدرجة صغيرة		المتوسط	الانحراف المعياري	التقدير القمي	الوزن النسبي	الدلالة	درجة التحقق	الترتيب حسب الرتبة
		ك١	%	ك٢	%	ك٣	%							
١	تتجه الجامعة نحو توعية وتثقيف أعضاء هيئة التدريس بمتطلبات الأمن السيبراني لحماية البريد الالكتروني، وإدارة امن المعلومات.	٧٦	٣٠,٦	١٢٣	٤٩,٦	٤٩	١٩,٨	٢,١١	٠,٧٠	٥٢٣	٢١٠,٩	٠,٠١	متوسطة	٤
٢	تقوم الجامعة بمراجعة البيانات والمعلومات المتوفرة على شبكاتها	٨٩	٣٥,٩	١١٤	٤٦,٠	٤٥	١٨,١	٢,١٨	٠,٧١	٥٤٠	٢١٧,٧	٠,٠١	متوسطة	٢

Print:(ISSN 1687-2649) Online:(ISSN 2536-9091)

	امن أجل تحديثها حال تعرضها للجرائم السيبرانية.												
٣	تعمل الجامعة على تحقيق أعلى استفادة من تكنولوجيا المعلومات والاتصالات وحماية أنظمتها حفاظاً على سرية بياناتها وحماية الشبكات والأنظمة.	٩٧	٣٩,١	١١٤	٤٦,٠	٣٧	١٤,٩	٣,٢٤	٠,٧٠	٥٥٦	٢٢٤,٢	٠,٠١	متوسطة	١
٤	تسعي الجامعة الي تنمية وعي الطلاب بثقافة الأمن السيبراني في ضوء التحول الرقمي للجامعات.	٦٧	٢٧,٠	١٢٣	٤٩,٦	٥٨	٢٣,٤	٢,٠٤	٠,٧١	٥٠٥	٢٠٣,٦	٠,٠١	متوسطة	٨
٥	توفر الجامعة مناهج جديدة؛ لمواكبة الثورة التكنولوجية	٦٦	٢٦,٦	١٢٠	٤٨,٤	٦٢	٢٥,٠	٢,٠٢	٠,٧٢	٥٠٠	٢٠١,٦	٠,٠١	متوسطة	١٠

	والتحول الرقمي بما يتوافق مع المعايير الدولية والوطنية.												
٦	تحذف الجامعة البيانات التالفة التي تعرضت لهجمات سيبرانية	٧٤	٢٩.٨	١١٨	٤٧.٦	٥٦	٢٢.٦	٢.٠٧	٠.٧٢	٥١٤	٢٠٧.٣	٠.٠١	متوسطة	٦
٧	توضح الجامعة لأعضاء هيئة التدريس إيجابيات ثقافة الأمن السيبراني خصوصا في مضامينها المستقبلية على المجتمع.	٥٨	٢٣.٤	١٢٥	٥٠.٤	٦٥	٢٦.٢	١.٩٧	٠.٧١	٤٨٩	١٩٧.٢	٠.٠١	متوسطة	١٣
٨	تضع الجامعة استراتيجيات لدمج وتضمين الموضوعات الخاصة بثقافة الأمن	٦٣	٢٥.٤	١١٧	٤٧.٢	٦٨	٢٧.٤	١.٩٨	٠.٧٣	٤٩١	١٩٨.٠	٠.٠١	متوسطة	١٢

	السيبرا ني في بعض المناه ج والمقر رات الدرا سية بالجام عات.												
٩	تعمل الجامع ة على تطوير الإطار التشر يعي الملائم لأمن الفضاء السيبرا ني وتشد يد العقوبا ت على جرائم الفضاء السيبرا ني وحماي ة الخصو صية وحماي ة الهوية الرقمية .	٦٣	٢٥.٤	١٢٥	٥٠.٤	٦٠	٢٤.٢	٢.٠١	٠.٧١	٤٩٩	٢٠١.٢	٠.٠١	متوسطة	١١
١٠	تهتم الجامع ة بتنمية الوعي الفكري والثقا في لدى الطلاب حول هجوم الاصط ياد الالكتر وني وتحديد ه كأحد المخاط ر السيبرا	٦١	٢٤.٦	١١٦	٤٦.٨	٧١	٢٨.٦	١.٩٦	٠.٧٣	٤٨٦	١٩٦.٠	٠.٠١	متوسطة	١٤

	نية												
١١	تقوم الجامعة بمجموعة من الحملات الإعلامية التوعوية للحد من الشائعات والمعطومات المفبركة التي تهدد حياة الأشخاص والدولة، موظفة مختلف الوسائل الإعلامية.	٦٤	٢٥.٨	١٠٨	٤٣.٥	٧٦	٣٠.٦	١.٩٥	٠.٧٥	٤٨٤	١٩٥.٢	٠.٠١	متوسطة	١٥
١٢	تنمي الجامعة وعي أعضاء هيئة التدريس بأهمية التحقّق من المصادر الموثوق بها؛ لحصولهم على معلومات تتعلق بدراستهم.	٨١	٣٢.٧	١١١	٤٤.٨	٥٦	٢٢.٦	٢.١٠	٠.٧٤	٥٢١	٢١٠.١	٠.٠١	متوسطة	٥
١٣	تضع الجامعة إجراءات، وسيا	٦٩	٢٧.٨	١٢٨	٥١.٦	٥١	٢٠.٦	٢.٠٧	٠.٦٩	٥١٤	٢٠٧.٣	٠.٠١	متوسطة	٦

	سات لحفظ الأمن السيبرا ني داخل الجامعا ت، وفقا للضوا بط الأسا سية الصادر ة من الهيئة الوطنيـ ة للأمن السيبرا ني.												
١٤	توفر برامج الجامع ة السرية اللازمة على حسابا ت المست خدمين من أعضاء الهيئة التدري سية والمحا فظة على خصو صيتها	٧٣٠	٢٩,٤	١٠٩,٠	٤٤,٠	٦٦,٠	٢٦,٦	٢,٠٣	٠,٧٥	٥٠٣	٢٠٢,٨	٠,٠١	متوسطة	٩
١٥	تهتم الجامع ة بعقد المؤتم رات والندوا ت العلمية والحوا رات التفاعل ية مع الطلاب باستمر ار للتنوع ية الفكرية وإكسا	٧٠	٢٨,٢	١٠٣	٤١,٥	٧٥	٣٠,٢	١,٩٨	٠,٧٧	٤٩١	١٩٨,٠	٠,٠١	متوسطة	١٢

	ب المعارف والمهارات اللازمة لحماية البيانات"												
١٦	تتعامل الجامعة مع ثقافة الأمن السيبراني باعتباره قضية أمن قومي هدفه حماية البيانات والمعلومات من الهجمات والاختراقات، للوصول إلى فضاء الكتروني آمن وموثوق.	٧٥	٣٠.٢	١١٠	٤٤.٤	٦٣	٢٥.٤	٢.٠٥	٠.٧٥	٥٠٨	٢٠٤.٨	٠.٠١	متوسطة	٧
١٧	تحرص الجامعة على تنويع الأنشطة المرتبطة بالمناهج الجامعية ومواءمتها مع التحول الرقمي للجامعة.	٨١.٠	٣٢.٧	١١٥.٠	٤٦.٤	٥٢.٠	٢١.٠	٢.١٢	٠.٧٢	٥٢٥	٢١١.٧	٠.٠١	متوسطة	٣

ومن تحليل البيانات الواردة في الجدول السابق رقم (١١) يتضح أن:

- حصلت العبارة رقم (٣) ونصها: (تعمل الجامعة على تحقيق أعلى استفادة من تكنولوجيا المعلومات والاتصالات وحماية أنظمتها حفاظاً على سرية وخصوصية بياناتها وحماية الشبكات والأنظمة) على المرتبة الأولى بمتوسط بلغ (٢,٢٤)، ويمكن تفسير ذلك في ضوء التحول الرقمي لكافة الأقسام الإدارية والأكاديمية بالجامعات وكذا التقنيات والتطورات التي طرأت على تكنولوجيا الاتصالات والمعلومات، والحاجة إلى حماية الأنظمة والشبكات والبيانات من التلف ومن الجرائم الإلكترونية والمحافظة على سرية البيانات والمعلومات وحماية الشبكات والأنظمة، كما تأتي هذه النتائج في سياق مواجهة الجرائم السيبرانية؛ خاصةً أن القائمين على تلك الجرائم محترفين ولديهم خبرات وقدرات تقنية هائلة ويصعب مواجهتهم إلا من خلال سياسات وآليات وبرامج وجدر حماية قوية وفعالة، وصيانتها بشكل دوري لأجل الحفاظ عليها.

وترى الدراسة أن الحفاظ على سرية وخصوصية بيانات أعضاء الهيئة التدريسية يجعلهم يثقون بالمحتوى والأنظمة لذا تهتم جامعة بنها بسرية وخصوصية المستخدم، إضافة إلى أن الحفاظ على سرية وخصوصية المستخدمين يمنح الجامعة سمعة أكاديمية، وهذا يجعلها أكثر اهتماماً بموضوع سرية وخصوصية البيانات والمستخدمين من اعضاء هيئة التدريس وغيرهم.

- حصلت العبارة رقم (٢) ونصها: (تقوم الجامعة بمراجعة البيانات والمعلومات المتوفرة على شبكاتها من أجل تحديثها حال تعرضها للجرائم السيبرانية) على المرتبة الثانية بمتوسط حسابي بلغ (٢,١٨)

ويمكن تفسير ذلك من خلال أهمية البيانات والمعلومات المتوفرة على شبكات الجامعة، وضرورة إصلاحها للاستفادة منها. وتفسر الدراسة هذه النتيجة أيضا من خلال أن تطبيقات الأمن السيبراني تتضمن برامج حماية وأمن البيانات والمعلومات ، وهذا يفيد أعضاء هيئة التدريس من خلال حماية بياناتهم والمعلومات المتوفرة، وحماية تلك البيانات تجعل عضو هيئة التدريس يلجأ لها عند الحاجة، وتضمن برامج الحماية ومتطلبات الأمن السيبراني هذه البيانات من الاختراق أو التلف، وهذا يعزز ثقة عضو

هيئة التدريس بأن الجامعة تحفظ بياناته. كذلك فإن حماية وأمن المعلومات يحافظ على سرية أعضاء هيئة التدريس وخصوصية بياناته، مما يجعل المجرم السيبراني غير قادر للوصول إليها.

- يتشابه تفسير النتيجة السابقة مع تفسير نتائج العبارة رقم (١٢) والتي نصت على: (تنمي الجامعة وعي أعضاء هيئة التدريس بأهمية التحقّق من المصادر الموثوق بها؛ لحصولهم على معلومات تتعلق بدراستهم) وقد حصلت علي المرتبة الخامسة بمتوسط (٢,١٠)، وقد يعزي ذلك إلى أن نشر الوعي بخطورة الجرائم السيبرانية وطرق الوقاية منها ، أهمية لا تقل عن أهمية الوسائل الوقائية ، فمهما كانت قوة التجهيزات التقنية الأمنية في الجامعة، فإنه يسهل اختراقها إذا لم يكن عند موظفيها وعي أمني؛ لأن العنصر البشري أكبر ثغرة تتم عبرها الاختراقات، ومع ذلك فإن الواقع العملي ينبأ عن أن الاهتمام به كعنصر من عناصر أمن المعلومات أقل من غيره ؛ لهذا نجد إن كثيرا من قاصدي الاعتداء الإلكتروني يلجؤون إلى ما يسمى بالهندسة الاجتماعية، وهي احتيال نفسي على مستخدم الحاسب ؛ ليتمكن المعتدي من الوصول للمعلومة، كأن يتصل بالموظف ويوهمه أنه من قسم الدعم الفني، ويطلب منه رقمه السري.
- حصلت العبارة رقم (١) ونصها : (تتجه الجامعة نحو توعية وتثقيف أعضاء هيئة التدريس بمتطلبات الأمن السيبراني لحماية البريد الالكتروني، وإدارة امن المعلومات) على المرتبة الرابعة بمتوسط حسابي بلغ (٢,١١)، وتفسر الدراسة هذه النتيجة من خلال أن تطبيقات الأمن السيبراني تتضمن برامج لحماية البريد الإلكتروني وإدارة أمن المعلومات والبيانات، وهذا يفيد المستفيدين من خلال حماية بياناتهم والمعلومات المتوفرة، وحماية تلك البيانات تجعل المستفيد يلجأ لها عند الحاجة، وتضمن برامج الحماية ومتطلبات الأمن السيبراني هذه البيانات من الاختراق أو التلف، وهذا يعزز ثقة المستفيد بأن الجامعة تحفظ بياناته. كذلك فإن حماية وأمن المعلومات يحافظ على سرية المستفيد وخصوصية بياناته، مما يجعل المجرم السيبراني غير قادر للوصول إليها واختراقها أو ارسال رسائل تهدد هذه البيانات؛ مما يزيد ثقة المستفيد بأن بياناته والمعلومات المتوفرة والبرامج والشبكات آمنة وغير معرضة للمخاطر، وهذا انعكس على الثقة الرقمية لديه.

- **حصلت كل من العبارة رقم (٦) ونصها: (تحذف الجامعة البيانات التالفة التي تعرضت لهجمات سيبرانية) والعبارة رقم (١٣) ونصها: (تضع الجامعة إجراءات، وسياسات لحفظ الأمن السيبراني داخل الجامعات، وفقا للضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني) على المرتبة السادسة بمتوسط (٢,٠٧) ، وترى الدراسة بالنسبة للعبارة (٦) أن البيانات التالفة تشكل عبء على الجامعة لأنها تأخذ حيز في برامج وتطبيقات التخزين، ولعدم القدرة على الاستفادة منها لاحقاً، إضافة إلى أن البيانات التالفة قد تشمل محتوى سلبي، أو محتوى يمكنه إتلاف مزيد من البيانات والمعلومات، أما نتيجة العبارة (١٣) فتأتي في سياق مواجهة الجرائم السيبرانية؛ خاصةً أن القائمين على الجرائم السيبرانية محترفين ولديهم خبرات وقدرات تقنية هائلة ويصعب مواجهتهم إلا من خلال إجراءات، وسياسات لحفظ الأمن السيبراني داخل الجامعات، وفقا للضوابط الأساسية والسياسات والآليات الصادرة من الهيئة الوطنية للأمن السيبراني**
- **حصلت الفقرة رقم (١٤) على المرتبة التاسعة والتي تنص على : (توفر برامج الجامعة السرية اللازمة على حسابات المستخدمين من أعضاء الهيئة التدريسية والمحافظة على خصوصيتها) ،**

بمتوسط حسابي (٢,٠٣) وهذا ينبثق عن طبيعة العمل بالمؤسسات الأكاديمية حسابات المستخدمين من أعضاء هيئة تدريس وباحثين وخبراء وطلاب وإداريين لها خصوصية وبيانات مهمة جداً، لذا تسعى الجامعات لحمايتها من الدخول غير المصرح به، أو مداهمتها بالفيروسات.

وترى الدراسة أن الحفاظ على سرية وخصوصية بيانات المستخدمين يجعلهم يثقون بالمحتوى

والأنظمة لذا تهتم جامعة بنها بسرية وخصوصية المستخدم، إضافة إلى أن الحفاظ على سرية وخصوصية المستخدمين يمنح الجامعة سمعة أكاديمية، وهذا يجعلها أكثر اهتماماً بموضوع سرية وخصوصية البيانات والمستخدمين.

- **بينما جاءت العبارة (١٠) ونصها: (تهتم الجامعة بتنمية الوعي الفكري والثقافي لدى الطلاب حول هجوم الاصطياد الالكتروني وتحديده كأحد المخاطر السيبرانية) بالمرتبة الرابعة عشر وبمتوسط حسابي بلغ (١,٩٦)، وهي مرتبة متأخرة الى حد ما وربما يعزى**

ذلك إلى حداثة الأمن السيبراني وتنوع برامجه وأساليبه ، أو أن نظام الأمن السيبراني لن يطور بصورة تامة ما لم تول اقصى درجة من الاهتمام لإذكاء وعي المجتمع والمستخدمين، فلا يمكن للمجتمع تحقيق الوعي الفكري والثقافي للطلبة حول المخاطر السيبرانية ما لم تكن حملات التوعية أحد عناصره الأساسية، ومن المسائل الأهم التي يتم التركيز عليها لإعداد وشن حملات التوعية بالمخاطر السيبرانية هي أمن الإنترنت، والسرية، والاحتيال، والانتحال، والبرمجيات الضارة، وتتفق هذه النتيجة مع دراسة *(القحطاني ،٢٠١٩)* والتي أكدت على أن معدل الجرائم الإلكترونية وهجوم الاصطياد الالكتروني يزداد بسبب قلة الوعي الفكري والثقافي لدى الطلاب وانهم غير مدركين لمخاطر التهديدات التي تأتي من خلال الإنترنت وأن جريمة الاحتيال الإلكتروني والنصب أكثر جريمة يتعامل معها الأمن السيبراني، وتعتبر التوعية الإعلامية هي أهم طرق الوقاية المجتمعية لمشكلات الفضاء السيبراني.

واتفقت كذلك مع دراسة *(غوص، والشريف، ٢٠٢٢)* التي اكدت أن طالبات المرحلة المتوسطة ليس لديهن المهارات اللازمة والخبرات الكافية بجرائم الانترنت، وعدم الإلمام الرقمي بمفردات الأمن السيبراني، على الرغم من استخدام الطالبات للإنترنت والمنصات التعليمية والهواتف الذكية.

- وحصلت العبارة رقم (١٦) ونصها: (تتعامل الجامعة مع ثقافة الأمن السيبراني باعتباره قضية أمن قومي هدفه حماية البيانات والمعلومات من الهجمات والاختراقات، للوصول إلى فضاء الكتروني آمن وموثوق).علي المرتبة السابعة بمتوسط (٢,٠٥)، وقد يعزي ذلك إلى أن التحول للثورة المعلوماتية ودخول العصر الرقمي وما نتج عنه من تهديدات وجرائم سيبرانية شكلت تحديا للأمن القومي ، وهو ما استدعى وجود ضمانات أمنية للبيئة الرقمية، لحماية المصالح الحيوية للدولة، تبلورت في انضمام مصر للاتفاقية العربية لمكافحة جرائم الإنترنت والإرهاب الإلكتروني وإنشاء المجلس الأعلى للأمن السيبراني، للحد من آثار اختراق أمن المعلومات على الأمن القومي للدول إلى تأمين ميكنة الخدمات الإلكترونية، وإنشاء مركز سيرت المصري، فضلا على إطلاق القمر الصناعي طيبة ١ في ٢٢ نوفمبر ٢٠١٩م، لأغراض الاتصالات وحماية الأمن القومي الإلكتروني "طيبة –١"، ويغطي مصر بالكامل فيما يخص الاتصالات والإنترنت، إضافة

الى جهود جمهوريه مصر العربية في اطلاق الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧– ٢٠٢١)، من أجل تأمين البني التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، ورفع مستوى الوعي بالأمن السيبراني وتجنب المخاطر والتهديدات السيبرانية وتقليل آثارها، وذلك في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري، وبما يدعم التحول نحو اقتصاد رقمي متكامل يحقق طموحات المواطنين في تنمية اجتماعية واقتصادية شاملة ويحمي مصالحهم، ويحافظ علي مصالح الدولة العليا ويسهم في نهضتها وازدهارها ورخاءها، وتتفق هذه النتيجة مع دراسة سمحان (٢٠٢٠) والتي أكدت على أهمية الأمن السيبراني في الحفاظ على أمن وحماية المعلومات وسلامة الوطن. وهنا يمكن التأكيد على ان الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات معلوماً أن صناع القرار في أي دولة تسعي للتطور وملاحقة التغيرات المجتمعية، أصبحت تصنف الأمن السيبراني كأولوية في سياساتها الدفاعية الوطنية ، وهو ما ظهر بوضوح عندما أعلنت أكثر من ١٣٠ دولة حول العالم عن تخصيص أقساماً وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني.

وهنا يمكن القول ان الأمن السيبراني يلامس الأمن القومي بشكل وثيق. فالتقنيات التي وسعت الآفاق، وأثرت الثقافة، وسمحت للثقافة المحلية بالامتداد إلى المجال العالمي، باتت تهدد الهوية الوطنية والقومية، مع تأثر الأجيال الصاعدة بما يصلها وبما تصل إليه عبر الإنترنت، حيث تبدو الهوية وكأنها خاضعة لعملية إعادة تشكيل، من خلال تكنولوجيا المعلومات، وحرص الغالبية العظمى من الناس، على استخدامها في تكوين مجتمعهم الخاص، وبيئتهم المميزة.

- كما حازت عبارة " تهتم الجامعة بعقد المؤتمرات والندوات العلمية والحوارات التفاعلية مع الطلاب باستمرار للتوعية الفكرية وإكساب المعارف والمهارات اللازمة لحماية البيانات" متوسط حسابي منخفض سجل (١,٩٨) ، وهذا مؤشر على أن جامعة بنها لها دور متوسط في إكساب المعارف والمهارات اللازمة لحماية البيانات والتوعية بمخاطر الاستخدام السلبي لتكنولوجيا الاتصال وتعزيز ثقافة المواطنة الرقمية والأمن السيبراني.

- **كما احتلت عبارة (تقوم الجامعة بمجموعة من الحملات الإعلامية التوعوية للحد من الشائعات والمعلومات المفبركة التي تهدد حياة الأشخاص والدولة، موظفة مختلف الوسائل الإعلامية.) المرتبة الأخيرة بمتوسط حسابي (١,٩٥) ويمكن تفسير تلك النتيجة بأنه بالرغم من ان الإعلام بمختلف أشكاله له دور وقائي ومهم في الحد من انتشار تلك الجرائم وفي التوعية بالقضايا الأمنية وفى زيادة مستوى الوعي واليقظة وتنمية الحس الاجتماعي الوطني في التصدي للجرائم والهجمات السيبرانية ، وبالتالي تنمية مهارات البحث ومعرفة القوانين والجرائم السيبرانية، الا ان جامعة بنها لا تهتم بهذا الجانب الوقائي .**

البعد الخامس : معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها

هدف هذا البعد إلى تعرف درجة موافقة افراد العينة على معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات، ويندرج تحت هذا البعد (١٧) عبارة يوضحها جدول (١٢).

جدول (١٢)
معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها
(ن = ٢٤٨)

م	العبارة	موافق بدرجة كبيرة		موافق بدرجة متوسطة		موافق بدرجة صغيرة		المتوسط	الانحراف المعياري	التقدير الرقمي	الوزن النسبي	الدلالة	درجة التحقق	الترتيب حسب الرتبة
		ك١	%	ك٢	%	ك٣	%							
١	سهولة اختراق المعلومات الشخصية والمنصات التعليمية بسبب التطور التكنولوجي الهائل والذي أتاح إمكانية الوصول غير المسموح به.	١١٧	٤٧,٢	٨٣	٣٣,٥	٤٨	١٩,٤	٢,٢٨	٠,٧٧	٥٦٥	٢٢٧,٨	٠,٠١	متوسطة	١٠
٢	استخدام العديد من التطبيقات في مواقع مختلفة لنفس قاعدة البيانات.	١١٩	٤٨,٠	٩٦	٣٨,٧	٣٣	١٣,٣	٢,٣٥	٠,٧٠	٥٨٢	٢٣٤,٧	٠,٠١	كبيرة	٦

Print:(ISSN 1687-2649) Online:(ISSN 2536-9091)

٣	قلة توفير برامج حماية كافية ضد برامج الاختراق الحديثة.	١١٣	٤٥,٦	١٠٧	٤٣,١	٢٨	١١,٣	٢,٣٤	٠,٦٧	٥٨١	٢٣٤,٣	٠,٠١	كبيرة	٧
٤	تبادل ارقام المرور السرية بين الهيئة التدريسية للأنظمة الالكترونية.	٩٦	٣٨,٧	٨٩	٣٥,٩	٦٣	٢٥,٤	٢,١٣	٠,٧٩	٥٢٩	٢١٣,٣	٠,٠١	متوسطة	١٢
٥	عدم استخدام برامج حماية أصلية موثوقة والاعتماد على استخدام البرامج المنسوخة.	١١٥	٤٦,٤	١٠٧	٤٣,١	٢٦	١٠,٥	٢,٣٦	٠,٦٦	٥٨٥	٢٣٥,٩	٠,٠١	كبيرة	٤
٦	ضعف آليات وسياسات حماية البنية التحتية السيبرانية والأجهزة وأنظمة البيانات والمعلومات .	١١٥	٤٦,٤	١٠٤	٤١,٩	٢٩	١١,٧	٢,٣٥	٠,٦٨	٥٨٢	٢٣٤,٧	٠,٠١	كبيرة	٦
٧	قلة الدورات التدريبية المنعقدة لأعضاء هيئة التدريس في مجال الأمن السيبراني.	١٢٣	٤٩,٦	١٠٢	٤١,١	٢٣	٩,٣	٢,٤٠	٠,٦٥	٥٩٦	٢٤٠,٣	٠,٠١	كبيرة	٣
٨	قلة الوعي بقانون الجرائم المعلوماتية وعقوبة نشر الوثائق والمعلومات السرية وافشائها.	١٣٣	٥٣,٦	٩١	٣٦,٧	٢٤	٩,٧	٢,٤٤	٠,٦٦	٦٠٥	٢٤٤,٠	٠,٠١	كبيرة	١

٩	غياب التطبيق الفعلي للتشريعات والقوانين الرادعة لمرتكبي الجرائم الإلكترونية.	١٢٣	٤٩,٦	١٠٤	٤١,٩	٢١	٨,٥	٢,٤١	٠,٦٤	٥٩٨	٢٤١,١	٠,٠١	كبيرة	٢
١٠	الافتقار إلى الرؤى والبيانات التي تمكن الجامعات من إدارة المخاطر الإلكترونية بكفاءة وفعالية.	١١٣	٤٥,٦	١٠٩	٤٤,٠	٢٦	١٠,٥	٢,٣٥	٠,٦٦	٥٨٣	٢٣٥,١	٠,٠١	كبيرة	٥
١١	ضعف التعاون بين موظفي التقنيات في الجامعات لتحقيق الأمن السيبراني.	٩٨	٣٩,٥	١٢٩	٥٢,٠	٢١	٨,٥	٢,٣١	٠,٦٢	٥٧٣	٢٣١,٠	٠,٠١	متوسطة	٨
١٢	عدم وجود قسم خاص بأمن المعلومات والأمن السيبراني داخل الجامعة.	١٠٣	٤١,٥	١٠٨	٤٣,٥	٣٧	١٤,٩	٢,٢٧	٠,٧٠	٥٦٢	٢٢٦,٦	٠,٠١	متوسطة	١١
١٣	استخدام الأجهزة الشخصية كالهواتف المحمولة لنقل معلومات سرية خاصة بالجامعة.	١٠٢	٤١,١	١٠٠	٤٠,٣	٤٦	١٨,٥	٢,٢٣	٠,٧٤	٥٥٢	٢٢٢,٦	٠,٠١	متوسطة	١١
١٤	تدني مستوى الخبرة لدي الموظفين	١٠٩,٠	٤٤,٠	١١٥,٠	٤٦,٤	٢٤,٠	٩,٧	٢,٣٤	٠,٦٥	٥٨١	٢٣٤,٣	٠,٠١	كبيرة	٧
١٥	التحايل على التحكم في الوصول الى الوسائط خلال تسخير برامج وهمية مهمتها الظهور باعتبارها مستخدمين فعليين داخل الشبكة.	١١١	٤٤,٨	١٠١	٤٠,٧	٣٦	١٤,٥	٢,٣٠	٠,٧١	٥٧١	٢٣٠,٢	٠,٠١	متوسطة	٩

- **ومن تحليل البيانات الواردة في الجدول السابق رقم(١٢) يتضح تعدد معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها مع تعدد أساليب وتكنيكيات ارتكاب الجرائم الإلكترونية ،حيث جاء أعلى متوسط حسابي (٢,٤٤) للعبارة "(٨) والتي تنص على :(قلة الوعي بقانون الجرائم المعلوماتية وعقوبة نشر الوثائق والمعلومات السرية وافشائها)، وهي تقع في فئة الموافقة الكبيرة، ويعزو ذلك الى عدم الوعي بقانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨م والذي يعتبر من أحدث التشريعات الوطنية المصرية في حماية جرائم تقنيات المعلومات، وذلك لاشتماله على العديد من صور الجرائم التي تتم في بيئة الإنترنت والنص على العقوبات التي تقع على مرتكبي مثل هذه الجرائم ، وكذلك تحديد العلاقة التي تربط مزودي خدمات الإنترنت بالمستخدم لهذه الخدمة والتزامات كلا منهم حتى لا يقع تحت طائلة القانون، فعلى سبيل المثال جاء في نص في المادة ١٦ على عقوبة الحبس مدة لا تقل عن سنة وغرامة مالية لا تقل عن خمسين ألف جنيه ولا تتجاوز مائتين وخمسين ألف جنية لكل من اعترض بوجه حق أي معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة الإنترنت أو أحد أجهزة الحاسب الآلي ، بالإضافة إلى التأكيد على حماية عناصر أمن المعلومات *CIA* ، كما نصت المادة ١٧ من القانون سابق الذكر ،على العقوبة بالحبس مدة لا تقل عن سنتين وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه كل من أتلف أو عطل أو عدل مسار أو ألغي متعمدا وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة أو المعالجة أو المولدة أو المخلفة على أي نظام معلوماتي وما في حكمة أيا كانت الوسيلة التي استخدمت في الجريمة نشير إلى أن قانون جرائم تقنية المعلومات المصري قد نص على جرائم أخرى تهدد أمن المعلومات مثل جرائم الاعتداء على البريد الإلكتروني وجرائم الاعتداء على تصميم المواقع الإلكترونية وجرائم الاعتداء على الأنظمة المعلوماتية وتهديد سلامتها مع توقيع أقصى العقوبة على من قام بواحدة من تلك الجرائم سواء مكافحة بالحبس أو بالغرامة المالية أو بإحدى العقوبتين ، وعلية جاءت العبارة رقم (٩)، وهي:(غياب التطبيق الفعلي للتشريعات والقوانين الرادعة لمرتكبي الجرائم الإلكترونية) بمتوسط حسابي (٢.٤١)، وقد يرجع ذلك الى نفس التفسير للعبارة السابقة وعدم الوعي بالقانون وتشريعاته.**

- **كما جاءت العبارة رقم (٧) ، وهي: (قلة الدورات التدريبية المنعقدة لأعضاء هيئة التدريس في مجال الأمن السيبراني) في المرتبة الثالثة بمتوسط حسابي (٢.٤٠) ، تلتها العبارة رقم (٥)، وهي: (عدم استخدام برامج حماية أصلية موثوقة والاعتماد على استخدام البرامج المنسوخة) في المرتبة الرابعة بمتوسط حسابي (٢.٣٦) .كما احتلت العبارات رقم (١٠، ٦، ٣، ١١، ١٥)، كل من المرتبة (الخامسة ، والسادسة ، والسابعة ، والثامنة ، التاسعة)، وهي على التوالي : (الافتقار إلى الرؤى والبيانات التي تمكن الجامعات من إدارة المخاطر الإلكترونية بكفاءة وفعالية)، (ضعف آليات وسياسات حماية البنية التحتية السيبرانية والأجهزة وأنظمة البيانات والمعلومات)،(تدني مستوى الخبرة لدي الموظفين) ، (ضعف التعاون بين موظفي التقنيات في الجامعات لتحقيق الأمن السيبراني) ، وتعزو الدراسة هذه النتيجة إلى تدني مستوى الخبرة لدى الموظفين، وضعف التعاون بين موظفي عمادة التقنية والمعلومات في الجامعات لتحقيق الأمن السيبراني، واستخدام الأجهزة الشخصية مثل الهاتف المحمول لتخزين أو نقل معلومات سرية خاصة بالجامعة؛ تشكل أبرز المعوقات تحقيق الأمن السيبراني في الجامعات بصفة عامة وجامعة بنها خاصة.**

واجمالا يتضح أن معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها جاءت بمستوى مرتفع وترى الدراسة أن هذه النسبة تمثل إشكالية كبرى في منظومة التعليم الجامعي بصفة عامة ، ولابد من إيجاد حلول لمواجهة هذه المعوقات، وقد اتفقت هذه النتيجة مع النتائج التي توصلت إليها دراسة *(المنتشري، وحريري ، ٢٠٢٠)* ، وهذا يؤكد انه كلما تقدمت وسائل تكنولوجيا المعلومات والاتصالات تقدمت معها المعوقات التي تحول دون تطبيق متطلبات الأمن السيبراني.

دلالة الفروق بين المجموعات:

وتم التحقق من صحة فرضية البحث من خلال اختبار(ت) لعينتين مستقلتين لحساب الفرق بين متوسطي درجات عينة الدراسة وفقا لمتغير الكلية ، وذلك للإجابة عن السؤال السادس من أسئلة الدراسة والخاص ب : ما دلالة الفروق بين متوسطات درجات أفراد العينة من أعضاء هيئة التدريس، وللتحقق من فرضية الدراسة ، وجاءت النتائج على النحو التالي:

الفرض الأول: لا توجد فروق ذات دلالة إحصائية بين متوسطي درجات استجابات أفراد مجموعة الدراسة تبعاً لمتغير الكلية (نظرية / عملية) فى كل بعد من ابعاد الاستبانة.

لاختبار صحة الفرض الاول تم حساب اختبار (ت) لعينتين مستقلتين Independent T-Test لدلالة الفرق بين متوسطي درجات استجابات أفراد مجموعة الدراسة تبعاً لمتغير الكلية (نظرية / عملية) فى كل بعد من ابعاد الاستبانة ، وظهرت النتائج كما هو موضح بالجدول الآتي:

جدول (١٣)

" نتائج اختبار (ت) لعينتين مستقلتين Independent T-Test لدلالة الفرق بين متوسطي درجات استجابات أفراد مجموعة الدراسة تبعاً لمتغير الكلية (نظرية / عملية) فى كل بعد من ابعاد الاستبانة

البعد	التخصص	العدد	المتوسط	الانحراف المعياري	قيمة (ت)	درجات الحرية	مستوى الدلالة
المتطلبات التقنية	نظرية	٩٤	٣٢.٩٧	٧.٩٣	٢.٣١٦	٢٤٦	٠.٠٥ دالة
	عملية	١٥٤	٣٥.٢٧	٧.٤٠			
المتطلبات المادية	نظرية	٩٤	١٧.٩٥	٥.٦٢	٢.١٥٢	٢٤٦	٠.٠٥ دالة
	عملية	١٥٤	١٩.٤٤	٥.١١			
المتطلبات البشرية	نظرية	٩٤	٢٨.١٠	٩.١٣	١.٣٢٥	٢٤٦	٠.١٨٧ غير دالة
	عملية	١٥٤	٢٩.٤٩	٧.٣٤			
المتطلبات المعرفية	نظرية	٩٤	٣٣.٥٠	١١.٠٥	١.٥٩٨	٢٤٦	٠.١١١ غير دالة
	عملية	١٥٤	٣٥.٧١	١٠.٢٩			
معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها	نظرية	٩٤	٣٦.٤٣	٨.٦٣	٢.٤٦٠	٢٤٦	٠.٠٥ دالة
	عملية	١٥٤	٣٣.٩٠	٧.٣١			

يتضح من الجدول السابق (١٣) ما يلي:

- **وجود فرق دال إحصائيًا عند مستوي ($\alpha \leq 0.05$) بين متوسطي درجات استجابات أفراد مجموعة الدراسة تبعاً لمتغير الكلية (نظرية / عملية) فى بعدى (المتطلبات التقنية ، المتطلبات المادية)، لصالح الكليات العملية مما يدل على ان التخصص له تأثير قوي في ايجاد اختلاف في اراء أعضاء هيئة التدريس بالكليات العملية والنظرية بالنسبة لهذ البعد ، وهذا يدل على أن الكليات العملية تعزز ثقافة الأمن السيبراني والسعي لتحقيق متطلباته التقنية والمادية التي تكون بحاجة لها بصورة أكبر من الكليات النظرية، وقد يرجع ذلك الى ان الكليات العملية تلتزم بالعديد من الدروس التكنولوجية والتدريبات العملية أكثر من الكليات النظرية والتي قد تجعلهم اكتر احتياجا لتوفير المتطلبات التقنية**

وما تحتاجه من ماديات ونفقات ، وربما يرجع ذلك الى عدم الدراية التامة للكليات النظرية بثقافة الأمن السيبراني ، على الرغم من أنَّ هذه الثقافة لا تتوقف على تخصص نظري أو عملي، وإنما هي وسائل تكنولوجية توعوية يجب ان تتاح للجميع.

- وجود فرق دال إحصائيًا عند مستوي ($\alpha \leq 0.05$) بين متوسطي درجات استجابات أفراد مجموعة الدراسة تبعاً لمتغير الكلية (نظرية / عملية) فى محور (معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها)، لصالح الكليات النظرية ، مما يعني ان الكليات النظرية يواجهون مجموعة من المعوقات تحتاج الى توجيه وتنمية الوعي لديهم تجاه ثقافة الأمن السيبراني السائدة بالجامعة من حيث واقعها أو معوقاتها، أكثر من الكليات العملية، وذلك نظرا لطبيعة الدراسة بها، حيث ان الدراسة بالكليات النظرية ترتبط بالجوانب الخاصة بالتنمية المتكاملة للشخصية الإنسانية، ويبتعدون عن النواحي التطبيقية ومعايشة الواقع ومواجهة تحدياته ومعوقاته، وقد يجهلون المعرفة ويفتقدون الكثير من المعلومات خارج إطار تخصصهم ، كما يفتقرون إلى المعلومات العامة التي يحتاجها الشخص في كثير من مجالات الحياة ، وقد يرجع الافتقار إلى الثقافة المعرفية او ضعفها إلى قلة أو عدم القراءة، على عكس طلاب الكليات العملية والتي تتعلق الدراسة فيها بالنواحي التطبيقية والمهارات العملية، ومعايشة الواقع والوعي الكامل بخطورة معوقات تحقيق الأمن السيبراني والجرائم الالكترونية وكيفية مواجهتها، وحرصهم على مواجهة هذا النوع الدخيل من المعوقات والجرائم السيبرانية على المجتمع.
- لا يوجد فرق ذو دلالة إحصائية عند مستوي ($\alpha \leq 0.05$) بين متوسطي درجات استجابات أفراد العينة تبعاً لمتغير التخصص (الكليات النظرية والعملية) فى بعدى (المتطلبات البشرية ، المتطلبات المعرفية)، وهذا يعني ان أعضاء هيئة التدريس في الكليات النظرية والعملية يتفقون على تحقيق هذه المتطلبات ، وقد يرجع ذلك الى ان تلك المتطلبات أساسية لا يمكن الاستغناء عنها ، وان هذه المتطلبات لا تتوقف على كلية محددة أو تخصص محدد، وإنما هي وسائل تكنولوجية توعوية متاحة لجميع أعضاء هيئة التدريس بغض النظر عن مستوى دراستهم او تخصصاتهم. وربما يرجع ذلك ايضا إلى شعور جميع أفراد الدراسة بدور الجامعة في تعزيز ثقافة الأمن السيبراني

وضرورة تحقيق متطلباته خاصة البشرية منها والمعرفية أكثر من توفير المتطلبات التقنية والمادية .

الفرض الثاني: لا توجد فروق ذات دلالة إحصائية بين متوسطات درجات استجابات أفراد مجموعة الدراسة تبعاً لمتغير عدد الدورات التدريبية التي حصل عليها عضو هيئة التدريس في مجال التحول الرقمي والأمن السيبراني فى كل بعد من ابعاد الاستبانة.

- لاختبار صحة الفرض الثاني تم حساب اختبار تحليل التباين أحادي الاتجاه ANOVA One–Way لحساب الفرق بين متوسطات درجات استجابات أفراد مجموعة الدراسة تبعاً لمتغير عدد الدورات التدريبية التي حصل عليها عضو هيئة التدريس في التحول الرقمي والأمن السيبراني فى كل بعد من ابعاد الاستبانة، وظهرت النتائج كما هو موضح بالجدول الآتي:

جدول (١٤)

نتائج اختبار (ANOVA) لدلالة الفروق بين متوسطات درجات استجابات أفراد مجموعة الدراسة تبعاً لمتغير عدد الدورات التدريبية التي حصل عليها عضو هيئة التدريس في التحول الرقمي والأمن السيبراني فى كل بعد من ابعاد الاستبانة

البعد	الإحصاءات الوصفية				البيان	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	مستوى الدلالة
	عدد الدورات	١	٢	٣						
المتطلبات التقنية	العدد	٥٦	١١٢	٨٠	بين المجموعات	٢٧.٠٥	٢	١٣.٥٢	٠.٢٢٨	٠.٧٩٦ غير دالة
	المتوسط	٣٤.٣٨	٣٤.٠٩	٣٤.٨٥	داخل المجموعات	١٤٥٠٠.٤٣	٢٤٥	٥٩.١٩		
					المجموع	١٤٥٢٧.٤٨	٢٤٧			
المتطلبات المادية	العدد	٥٦	١١٢	٨٠	بين المجموعات	٢.٨٤	٢	١.٤٢	٠.٠٤٩	٠.٩٥٢ غير دالة
	المتوسط	١٦.٦٨	١٨.٩٥	١٩.٩١	داخل المجموعات	٧٠٥٦.٢٨	٢٤٥	٢٨.٨٠		
					المجموع	٧٠٥٩.١٣	٢٤٧			
المتطلبات البشرية	العدد	٥٦	١١٢	٨٠	بين المجموعات	٦.٨٩	٢	٣.٤٥	٠.٠٥٢	٠.٩٤٩ غير دالة
	المتوسط	٢٨.٩١	٢٨.٨٢	٢٩.٢٠	داخل المجموعات	١٦٠٩٥.٧٨	٢٤٥	٦٥.٧٠		
					المجموع	١٦١٠٢.٦٧	٢٤٧			
المتطلبات المعرفية	العدد	٥٦	١١٢	٨٠	بين المجموعات	٥٢.٣٤	٢	٢٦.١٧	٠.٢٣١	٠.٧٩٤ غير دالة
	المتوسط	٣٥.٧٠	٣٤.٧٥	٣٤.٤٨	داخل المجموعات	٢٧٨٠٦.٧٩	٢٤٥	١١٣.٥٠		
					المجموع	٢٧٨٥٩.١٣	٢٤٧			
معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها	العدد	٥٦	١١٢	٨٠	بين المجموعات	١٢٥.٧٧	٢	٦٢.٨٩	١.٠٠٤	٠.٣٦٨ غير دالة
	المتوسط	٣٥.٢٧	٣٤.٠٩	٣٥.٦٥	داخل المجموعات	١٥٣٤٤.٢٩	٢٤٥	٦٢.٦٣		
					المجموع	١٥٤٧٠.٠٦	٢٤٧			

ملاحظة : (١ =لا يوجد ، ٢ = من (١ – ٣) دورات ، ٣ = أكثر من (٣) دورات)

يوضح الجدول السابق (١٤) أن:

يتضح من خلال الجدول السابق أن قيمة " ف" تساوي (٠.٢٢٨) ، (٠.٠٤٩)، (٠.٠٥٢)، (٠.٢٣١) بالنسبة لكل من المتطلبات التقنية والمادية والبشرية والمعرفية بالترتيب ، كما جاءت قيمة " ف" بالنسبة لمعوقات تحقيق متطلبات الأمن السيبراني تساوي (١.٠٠٤)، وفي الحالتين (المتطلبات / المعوقات) يلاحظ ان قيمة (ف) هي قيمة غير دالة عند مستوى الدلالة(٠.٠٥) في درجة استجابة أعضاء هيئة التدريس لمتطلبات تحقيق للأمن السيبراني تعزى لاختلاف الدورات التدريبية، وقد يرجع ذلك إلى أن أعضاء هيئة التدريس بغض النظر عن الدورات التدريبية فإن مستوى الوعي بالأمن السيبراني

واضح لديهم إلى حد بعيد باعتبار أنه يمكن ملاحظته بسهولة، وتدربوا عليه عمليا من واقع عملهم وتعاملهم مع التقنيات الحديثة والحاسب وتكنولوجيا المعلومات والاتصالات والتحول الرقمي والأمن السيبراني بصورة مستمرة .

ويمكن تفسير هذه النتيجة بأن نشر ثقافة التدريب على التكنولوجيا الحديثة من المتطلبات الضرورية لعمل الجامعة في العصر الرقمي الذي يتطلب إدخال التقنيات الرقمية في العملية التعليمية، ويفرض على عضو هيئة التدريس اكتساب مهارات وجدارات تكنولوجية ليتمكن من التعامل مع تقنية المعلومات وتنمية مهارات البحث العلمي، في ظل تكنولوجيا المعلومات والاتصال الحديثة، وقد اختلفت هذه النتيجة مع النتيجة التي توصلت لها دراسة *(المنتشري، وحريري ، ٢٠٢٠)*، التي أظهرت وجود فروق ذات دلالة إحصائية تعزى إلى متغير دورات تدريبية في الأمن السيبراني، واتفقت مع النتيجة التي توصلت لها دراسة *(الصحفي ، ٢٠١٩)*، التي أشارت إلى عدم وجود فروق ذات دلالة إحصائية بين متوسطات استجابات أفراد عينة الدراسة في درجة وعي معلمات الحاسب بالأمن السيبراني تعزى إلى متغير الدورات التدريبية.

المحور السادس: تصور مقترح لتحقيق متطلبات الأمن السيبراني بالجامعات المصرية فى ضوء التحول الرقمي .

انطلاقًا من نتائج الدراسة النظرية التي تضمنت تحليلًا نظريًا للأسس الفكرية للتحول الرقمي للجامعات وتحديد الإطار الفلسفي للأمن السيبراني من حيث مفهومه، وأهدافه، وابعاده، وخصائصه، والتعرف على معوقات تحقيق الأمن السيبراني بالجامعات في ضوء التحول الرقمي، واستنادًا إلى الوضع الراهن الذي تم التوصل إليه من خلال الدراسة الميدانية والذي تم من خلاله تحديد مدى ملاءمة تحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات من وجهة نظر أعضاء هيئة التدريس ، يمكن وضع تصور مقترح لتحقيق متطلبات الأمن السيبراني بجامعة بنها في ضوء التحول الرقمي للجامعات وفقا للخطوات التالية:

أولا: أهداف التصور المقترح:

- **تنمية الوعي بتقنية المعلومات والتعرف على جوانبها الإيجابية والسلبية لدى أعضاء هيئة التدريس بجامعة بنها لمواجهة الجرائم الإلكترونية.**
- **تعزيز الأمن السيبراني لدى كافة فئات المجتمع بشكل عام في ظل الثورة المعلوماتية والتدفق الهائل للمعلومات في العصر الحالي.**
- **تعزيز الاستخدام الرشيد لمصادر المعلومات المختلفة، والتعامل مع كافة متغيرات الثورة الرقمية المعاصر بعقلية مستنيرة مدركة لإيجابيات وسلبيات التواصل عبر الفضاء السيبراني.**
- **تطوير استراتيجية وطنية وحماية البنية التحتية للمعلومات الحساسة، بالإضافة الى ردع الجريمة السيبرانية.**
- **تحقيق سريه وخصوصية المعلومات، والحفاظ على سلامة البيانات بشكل مستمر.**
- **تفعيل دور الإعلام بمختلف وسائله في مجال التوعية بمخاطر وتهديدات الفضاء السيبراني.**
- **تعزيز التكامل والتعاون بين كافة قطاعات وأجهزة الدولة ذات الصلة والقطاع الخاص لمواجهة المخاطر والاستجابة السريعة للهجمات الرقمية.**

ثانيا: مصادر اشتقاق التصور المقترح: تم اشتقاق التصور المقترح من المصادر الاتية....

- **الإطار النظري للبحث**
- **الإطار الميداني للبحث**
- **الادبيات والدراسات السابقة في المجال**

ثالثا: منطلقات التصور المقترح: انطلق التصور المقترح لتحقيق متطلبات الأمن السيبراني فى ظل التحول الرقمي من مجموعة من المنطلقات هي:

- **ان تحقيق متطلبات الأمن السيبراني بجامعة بنها فى ظل التحول الرقمي للجامعات بات من اهم المتطلبات التي ينبغي على التعليم الجامعي الوفاء بها.**
- **ان ثقافة تنمية الأمن السيبراني وتلبية متطلباته بجامعة بنها لم يصل بعد الى الشكل المأمول.**

رابعا: جوانب التصور المقترح:

انطلاقا من فلسفة التصور المقترح ومرتكزاته، وفي ضوء ما توصلت إليه الدراسة الميدانية من نتائج، يقدم البحث الحالي بعض الآليات المقترحة التي يمكن من خلالها تلبية المتطلبات اللازمة

لتحقيق الأمن السيبراني بجامعة بنها فى ظل التحول الرقمي للجامعات، وذلك في الجوانب التالية:

الجانب الأول: المتطلبات التقنية.

- **استخدام تقنيات وبرامج حماية متقدمة للبريد الإلكتروني وللحسابات الرسمية، مضادة للفيروسات قادرة على التصدي لأي هجمات مشبوهة.**
- **توفير موقع الكتروني في كل الجامعات على شبكة الانترنت يتم تحديثه باستمرار.**
- **حفظ نسخة احتياطية من الملفات والمجلدات، بحيث أنه لو فقدت بيانات أو معلومات نتيجة تعرضها للفيروسات، يكون هناك نسخة منها.**
- **عدم إرسال الصور عبر الإنترنت أثناء التحدث مع الغرباء .**
- **عدم الاحتفاظ بالبيانات الحساسة في الحاسب الالي مثل البيانات المالية والشخصية خشية وقوعها بأيدي الارهابين.**
- **استخدام المواقع الموثوق بها عند تقديم معلومات شخصية.**
- **عدم فتح مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة.**
- **الحرص دائما على تحديث الأجهزة.**
- **توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية.**
- **مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث أضرار بالغة للمستخدمين .**
- **اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة**
- **استخدام كلمة مرور قوية لدخول النظام مع التأكد من ضبط اعدادات المتصفح الأمنية.**

الجانب الثاني: المتطلبات المادية.

- **رصد موازنة لخطة تطبيق الأمن السيبراني في الجامعات المصرية.**
- **توفير الدعم المالي الكافي لشراء الاجهزة الحاسوبية والبرامج والتطبيقات الحديثة.**
- **توفير الدعم المالي المناسب لصيانة الاجهزة الحاسوبية والبرامج المطلوبة.**
- **رصد مبالغ مالية للاستعانة بخبراء في مجال الأمن السيبراني.**
- **تخصيص ميزانية لمنظومة الأمن السيبراني؛ لزيادة تطوير إمكانياتها وقدراتها، لمواجهة تلك الجرائم والتهديدات، ولتطوير البرامج والتطبيقات المستخدمة في الجامعات.**
- **توفير المخصصات المالية اللازمة للربط الشبكي في الجامعات المصرية.**
- **توفير المخصصات المالية اللازمة لبرامج تدريب وتأهيل أعضاء هيئة التدريس داخلياً وخارجياً.**
- **تزويد العاملين بأحدث الأجهزة والبرامج التقنية، لمساعدتهم في الحصول على المعلومات الدقيقة، وتعزيز السلامة المعلوماتية.**
- **منح الحوافز المادية والمعنوية للموظفين المتميزين والمبدعين في مجال الأمن السيبراني.**

الجانب الثالث: المتطلبات البشرية.

- **توفير قاعات تدريب لأعضاء هيئة التدريس تحتوي على جميع الاحتياجات التدريبية التي ترفع من القدرات الإلكترونية لديهم.**
- **إقامة المؤتمرات والندوات العلمية بشكل دوري للتوعية الفكرية لأعضاء هيئة التدريس ،ومناقشة مخاطر الهجمات الإلكترونية .**
- **التدريب المستمر للكوادر الفنية وتأهيلهم بمهارات احترافية عالية وفق المعايير المهنية المعترف بها على كيفية التعامل مع تلك الهجمات.**
- **رفع درجة الوعي لدي أعضاء هيئة التدريس بالمخاطر والتهديدات المصاحبة للتطور السريع لاستخدام التكنولوجيا.**
- **عقد ورش تدريبية باستمرار عن الذكاء السيبراني الاستراتيجي، وكيفية توظيفه في جميع قطاعات الدولة الحيوية، لتقليل مخاطر التهديدات السيبرانية المحتملة.**

- **الحراك العلمي الدولي من خلال عقد شراكات واتفاقيات دولية بين الجامعات، بهدف زيادة تأهيل المختصين للتعامل مع تلك الجرائم والمجالات ذات العلاقة.**
- **تكثيف وسائل التوعية للكوادر البشرية بالجرائم السيبرانية عامة والهندسة الاجتماعية على وجه الخصوص التي من الممكن الوقوع فيها دون العلم بذلك.**
- **تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.**
- **زيادة أعداد الكوادر المؤهلة للعمل في مجال الأمن السيبراني لتواكب متطلبات الاقتصاد العالمي المرتكز على التقنية.**
- **تطوير مهارات الطلاب البحثية لتكوين كوادر مهنية متخصصة في مجال إدارة الأمن السيبراني، وتعزيز الوعي الأمني لديهم، بما يتماشى مع التطور التكنولوجي.**

الجانب الرابع: المتطلبات المعرفية.

- **التعرف على اللائحة التنفيذية لقانون مكافحة الجرائم الالكترونية، وآليات تطبيق قانون تلك الجرائم، وخصوصًا المتعلقة بالتحريض والشائعات واختراق الحسابات الرسمية.**
- **إدراج مقرر "الأمن السيبراني" في التعليم الجامعي كونه أحد التخصصات المدرجة حالياً في الجامعات المصرية الأخرى.**
- **ضرورة الاستفادة من التجارب السابقة للدول المختلفة في مجال تحقيق الأمن السيبراني ، وطرق مكافحة الجرائم السيبرانية والمخاطر المترتبة عليها.**
- **إدخال بعض المقررات الجديدة التي تعلى بهذه المشكلة، مثل الثقافة القانونية، وتضمين الموضوعات الخاصة بثقافة أمن المعلومات في بعض المقررات مثل مقرر حقوق الإنسان.**
- **تنويع الأنشطة المرتبطة بالمناهج الجامعية ومواءمتها مع التحول الرقمي للجامعة.**
- **تعزيز ثقافة أمن المعلومات في المجتمع والإسهام في نشر المعرفة النظرية والتطبيقية في مجال الأمن السيبراني.**
- **التعامل مع ثقافة الأمن السيبراني باعتباره قضية أمن قومي هدفه حماية البيانات والمعلومات من الهجمات والاختراقات، للوصول إلى فضاء الكتروني آمن وموثوق.**

الجانب الخامس: القضاء على معوقات تحقيق متطلبات الأمن السيبراني بجامعة بنها.

- **الوعي بخطورة التهديدات السيبرانية وضرورة التعامل معها كأولوية وبأعلى قدر من الجدية.**
- **وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية وحماية الهوية الرقمية وأمن المعلومات.**
- **وضع الإطار التنظيمي وانشاء منظومة وطنية لحماية أمن الفضاء السيبراني**
- **تأمين البني التحتية للاتصالات وتكنولوجيا المعلومات ونظم وقواعد البيانات والمعلومات القومية وبوابات الخدمات الحكومية والمواقع الحكومية على الانترنت.**
- **تنمية الكوادر البشرية والخبرات اللازمة لتفعيل منظومة الأمن السيبراني في مختلف القطاعات.**
- **التعاون مع الدول الصديقة والمنظمات الدولية والاقليمية ذات الصلة وتبادل الخبرات وتنسيق المواقف في مجال أمن الفضاء السيبراني ومكافحة الجرائم السيبرانية.**
- **وضع وتنفيذ خطط وحملات للتوعية المجتمعية بالفرص والمزايا التي تقدمها الخدمات الالكترونية المؤمنة للأفراد والمؤسسات.**

خامسا: متطلبات تنفيذ التصور المقترح

- **الإيمان بأن الأمن السيبراني أفضل وأقصر الطرق لحماية البيانات والأنظمة.**
- **تخصيص قسم لأمن وحماية المعلومات مهمته متابعة وتحديث برامج حماية وأمن المعلومات والأنظمة الإدارية والأجهزة التقنية.**
- **اعتماد آليات توثيق للوثائق العلمية والمراسلات الإدارية والأكاديمية بالجامعات آمنة ومحمية من الاختراق أو التهديديات الإلكترونية.**
- **الاعتماد على أقوى البرامج لمقاومة البرمجيات الخبيثة والفيروسات التي تتلف البيانات والأجهزة.**
- **تطوير أنظمة تقنية تمنع وصول العابثين إلى المعلومات الشخصية للمستخدمين والمستفيدين من أنظمة الجامعة وبرامجها.**
- **إدراج مجال الفضاء السيبراني ضمن مناهج التعليم الجامعي.**
- **تشجيع بحوث ودراسات الأمن السيبراني في رسائل الماجستير والدكتوراه.**

- ❖ إسهام بعض أعضاء هيئة التدريس في تصميم بعض البرامج التي يكون هدفها تطهير الإنترنت من المواقع الإرهابية، ومنع المستخدمين من الحصول على معلومات غير صحيحة .
- ❖ إنشاء مركز معلوماتي تابع للجامعة، على أن يكون من ضمن اختصاصات هذا المركز اقتراح القواعد والتشريعات الخاصة بالمعلوماتية والإنترنت، واعداد تقارير إحصائية، ومتابعة ما تم عالميًا في هذا المجال.
- ❖ التعاون مع بعض الوزارات مثل الإعلام لوضع إستراتيجية إعلامية هادفة لنشر الوعي الجماهيري. بمخاطر الجريمة الإلكترونية وتأثيرها على الشباب
- ❖ إنشاء كلمة مرور قوية مكونة من رموز وأرقام وحروف، والحذر من الضغط على اللينكات مجهولة المصدر المرسلة عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي، والحرص على عمل النسخ الاحتياطي للبيانات والملفات.

سادسا : معوقات تحقيق التصور المقترح

- ❖ سهولة اختراق المعلومات الشخصية والمنصات التعليمية بسبب التطور التكنولوجي الهائل والذي أتاح إمكانية الوصول غير المسموح به.
- ❖ استخدام العديد من التطبيقات في مواقع مختلفة لنفس قاعدة البيانات.
- ❖ قلة توفير برامج حماية كافية ضد برامج الاختراق الحديثة.
- ❖ تبادل ارقام المرور السرية بين الهيئة التدريسية للأنظمة الالكترونية.
- ❖ عدم استخدام برامج حماية أصلية موثوقة والاعتماد على استخدام البرامج المنسوخة.
- ❖ ضعف آليات وسياسات حماية البنية التحتية السيبرانية والأجهزة وأنظمة البيانات والمعلومات.
- ❖ قلة الدورات التدريبية المنعقدة لأعضاء هيئة التدريس في مجال الأمن السيبراني.
- ❖ قلة الوعي بقانون الجرائم المعلوماتية وعقوبة نشر الوثائق والمعلومات السرية وافشائها.
- ❖ غياب التطبيق الفعلي للتشريعات والقوانين الرادعة لمرتكبي الجرائم الإلكترونية.
- ❖ الافتقار إلى الرؤى والبيانات التي تمكن الجامعات من إدارة المخاطر الإلكترونية بكفاءة.

- ضعف التعاون بين موظفي التقنيات في الجامعات لتحقيق الأمن السيبراني.
- عدم وجود قسم خاص بأمن المعلومات والأمن السيبراني داخل الجامعة.
- استخدام الأجهزة الشخصية كالهواتف المحمولة لنقل معلومات سرية خاصة بالجامعة.
- تدني مستوى الخبرة لدي الموظفين.
- ضعف المواد القانونية والاجراءات القضائية الداخلية والدولية وعدم الانسجام بينهما في تبني وتحديث التشريعات لمكافحة الانتهاكات السيبرانية لكونها عابرة للحدود وتتنوع آثارها الناتجة منها.

خاتمة البحث

في الختام، لا بدّ من الوعي بأهمية الأمن السيبراني؛ خاصة أنه يعد إضافة حديثة إلى أجندة الأمن العالمي، حيث يهتم بحماية الدول والمواطنين من إساءة استخدام شبكات الكمبيوتر لأغراض الإرهاب والتجسُّس الاقتصادي والمكاسب الإجرامية. ويأتي ذلك في إطار التحول الرقمي للجامعات الذي يتسم بتكنولوجيا المعلومات الحديثة والمعاصرة التي تُعد ضرورة من ضرورات عصرنا الحالي، بل وصارت أداة استراتيجية هامة تسهل الوصول السريع إلى الميزة التنافسية. تلك الطفرة الكبيرة في وسائل الاتصالات وشبكات المعلومات والدخول في عصر العولمة والإنترنت؛ اظهرت مخاطر كبيرة وتهديدات متعددة جديدة بكل المؤسسات ومنها الجامعات وذلك من شأنه أن يستدعى كافة الوسائل المتاحة والممكنة لتعزيز أمن المعلومات، وحماية الشبكات والبرامج والأنظمة من الهجمات الرقمية التي تسعى إلى المعلومات الحساسة من أجل إتلافها أو تغييرها ، وعليه، أصبحت ضرورة التعرف على متطلبات الأمن السيبراني وتحقيقها في ضوء التحول الرقمي للجامعات أمراً حتمياً .

مراجع البحث

أولا: المراجع العربي

١. إبراهيم، أحمد حسن (٢٠١٩): التحول الرقمي" نقلة نوعية للتحرر من البيروقراطية والفساد الإداري"، مجلة الاقتصاد والمحاسبة، نادي التجارة، القاهرة، ع ٦ ٧٧ ، ص ص٨–١١.

٢. إبراهيم، منال حسن محمد (٢٠٢١): الوعي بجوانب الأمن السيبراني في التعليم عن بعد، المجلة العلمية لجامعة الملك فيصل ، العلوم الإنسانية والإدارية، جامعة الملك فيصل ، السعودية، مج٢٢، ع٢، ص ص٢٩٩–٣٠٧.

٣. أبو حسين، حنين جميل (٢٠٢١): الإطار القانوني لخدمات الأمن السيبراني: دراسة مقارنة ، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط ، عمان، الأردن، ص ص١– ١٣٩.

٤. الإدارة العامة لمركز المعلومات والتوثيق بوزارة التعليم العالي (٢٠٢١): بيان بأعضاء هيئة التدريس بجامعة بنها في العام الجامعي ٢٠٢٠/٢٠٢١، قطاع مكتب الوزير، وزارة التعليم العالي.

٥. الإقبالي، حامد أحمد (٢٠١٩): مقتضيات التحول إلى التعلم الرقمي الموجه لصغار السن في الوطن العربي، المجلة التربوية، كلية التربية ، جامعة سوهاج، مج ٦٨ ، ع٦٦ ، ص ص٤١١–٤٣٤.

٦. آل مسعود، علي يحيى(٢٠٢٠): الأمن السيبراني وآلياته في الحد من السلوكيات الاحترافية للأحداث في المملكة العربية السعودية: دراسة نظرية تحليلية، مجلة كلية التربية، جامعة كفر الشيخ ، مج ٢٠ ، ع ٤، ص ص٤١١–٤٣٤.

٧. الأمم المتحدة (٢٠١٩): تحالف عالمي جديد لاستثمارات بتريليونات الدولارات من القطاع الخاص لتحقيق أهداف التنمية المستدامة ، إدارة الشؤون الاقتصادية والاجتماعية، نيويورك، أكتوبر، ص ص ١–٣ .
https://www.un.org/development/desa/ar/news/financing/gisd-alliance-launches.html

٨. الإسكوا (٢٠١٨): التكنولوجيا من أجل التنمية المستدامة : استحداث فرص العمل اللائق وتمكين الشباب في البلدان العربية، الدورة (٣٠)، بيروت ، ص ص ١–٤٢ .
https://archive.unescwa.org/sites/www.unescwa.org/files/ministerial_sessions/docs/technology_for_sustainable_development-ar.pdf

٩. اللصاصمه، عبد الكريم سلمان، ومناور، فايز عبد القادر(٢٠٢٢): الأدوار الأكاديمية والتوعوية للجامعات الأردنية الرسمية نحو أمن المعلومات الإلكترونية من وجهة نظر أعضاء هيئة التدريس فيها، مجلة كلية الآداب ، كيلة الآداب ، جامعة عين شمس، ، مج٥٠، مارس، ص ص٨٢–٦٩.
١٠. البابلي ، عمار ياسر(٢٠٢٠) : أمن الفضاء الإلكتروني ، معهد الدراسات العربية، جامعة الدول العربية، القاهرة.
١١. باغة، محمد محمد (٢٠١٩): التحول الرقمي من عصر السركي إلى عصر الرقمنة، مجلة إدارة الأعمال، جمعية إدارة الأعمال العربية، القاهرة، ص ص٢٤–٤٥.
١٢. بوتيف، سامي محمد(٢٠١٩): دور الاستراتيجيات الاستباقية فى مواجهة الهجمات السيبرانية ، الردع السيبرانى نموذجا ، المجلة الجزائرية للحقوق والعلوم السياسية ، الجزائر، مج ٤ ، ع ٧، ص ص١٢١–١٣٥.
١٣. البعلبكي ، منير (٢٠٠٤): المورد: قاموس إنجليزي – عربي، دار العلم للملايين ، بيروت ، ص ص١–٢٢٤٤.
١٤. البداينة، ذياب موسى (٢٠١٤) :الجرائم الالكترونية : المفهوم والأسباب ، ورقة مقدمة في الملتقى العلمي : الجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، المنعقد في الفترة من ٤/٢ –٩/ ٢٠١٤، كلية العلوم الاستراتيجية عمان ، الأردن، ص ص١–٢٨.
١٥. البياتي، راجي يوسف محمود (٢٠٢٢): الإرهاب السيبراني: نماذج من الجهود الدولية للحد منه ، مجلة تكريت للعلوم السياسية ، كلية العلوم السياسية ، جامعة تكريت، العراق ، ع٢٨ ، يونيو، ص ص٨٧–١٢١.
١٦. البيشي، منير عبد الله مفلح (٢٠٢١): الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، الجامعة الإسلامية بغزة – شئون البحث العلمي والدراسات العليا، مج ٢٩ ، ع ٦، نوفمبر، ص ص٣٥٣–٣٧٢.
١٧. جاب الله، وليد عبد الرحيم(٢٠٢١): الأمن السيبراني بين الاحتكار والاستثمار، مجلة الديمقراطية، مؤسسة الأهرام، القاهرة، مج ٢١ ، ع ٨٢، ابريل، ص ص٤٩–٥٣.
١٨. جبور، منى الأشقر(٢٠١٦): السيبرانية: هاجس العصر، دراسات وابحاث (١)، جامعة الدول العربية، المركز العربي للبحوث القانونية، بيروت ، ص ص ١– ٢١٨.

١٩. جبور، منى الأشقر (٢٠١٢): الأمن السيبراني: التحديات ومستلزمات المواجهة. اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، المركز العربي للبحوث القضائية والقانونية، جامعة الدول العربية، بيروت، في الفترة من ٢٧– ٢٨ أغسطس، ص ص ٩٦٦–١٠٦٦.
https://journals.ekb.eg/article_250062_798efc55350b93931f7d66f72addfe72.pdf

٢٠. الجمل، حازم حسن أحمد (٢٠٢٠): الحماية الجنائية للأمن السيبراني في ضوء رؤية المملكة ٢٠٣٠ ، مجلة البحوث الأمنية، كلية الملك فهد الأمنية ، مركز الدراسات والبحوث، السعودية، مج ٣٠ ، ع ٧٧، أغسطس، ص ص٢٤٣–٣٢٨.

٢١. الجنابي، ليلى(٢٠١٧): فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية، متاح على https://www.ssrcaw.org.

٢٢. الجنبيهى، منير محمد ، والجنبيهى ممدوح محمد (٢٠٠٦) : جرائم الانترنت والحاسب الآلي ووسائل مكافحتها ، دار الفكر الجامعي للنشر ، الإسكندرية ، ص ص ١–٢٥٠.

٢٣. الجندي، علياء عبد الله، حسن، نهير طه (٢٠١٩)، دور الممارسة التطبيقية للأمن السيبراني في تنمية المهارات ودقة التطبيق العملي للأمن المعلوماتي لدى طالبات الجامعة، مجلة عالم التربية، ، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية ، القاهرة ، مج٦٧، ع٣، ص ص١٤–٨٤.

٢٤. الجنفاوي، خالد مخلف (٢٠٢١): التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت، المجلة العربية للآداب والدراسات الإنسانية، المؤسسة العربية للتربية والعلوم والآداب، مصر، ع ١٩، يوليو، ص ص٧٥–١٢٣.

٢٥. الحربي ، ايمن عبد الرحمن (٢٠٢٠): ندوة عن مقدمة في الأمن السيبراني ، واحة ام القرى للاستشارات، معهد البحوث والدراسات الاستشارية، السعودية . عمادة التعليم الإلكتروني والتعليم عن بعد في الفترة من ١٤/ ١٥ –٤.

٢٦. حسن، سعيد عبد اللطيف(٢٠١٧):اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، دار النهضة العربية للنشر والتوزيع ،القاهرة، ط٤، ص ص ١–٢٧٣.

٢٧. حيمد، محمد مسعد، وجاد الحق، مصفي مصطفي(٢٠١٩): رؤية استراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة، المجلة العربية الدولية للمعلوماتية، اتحاد الجامعات العربية ، جمعية كليات الحاسبات والمعلومات ، السعودية، مج٧، ع١٢، ص ص٨٣–١٠٠.

٢٨. الخميسي، السيد سلامة (٢٠٢٠): التعليم في زمن كورونا (COVID–١٩): تجسير الفجوة بين البيت والمدرسة، المجلة الدولية للبحوث في العلوم التربوية، مج٣، ع ٤، المؤسسة الدولية لأفاق المستقبل، أستونيا، ص ص٥١–٧٣.

٢٩. الخيلي، شمسان ناجي صالح(٢٠١١): جرائم الاعتداء على الملكية الفكرية بواسطة الإنترنت ، دار النهضة العربية للنشر ، القاهرة، ص ص ١–١١٤.

٣٠. الدهشان، جمال علي خليل، والسيد، سماح السيد محمد (٢٠٢٠): رؤية مقترحة لتحويل الجامعات المصرية الحكومية إلى جامعات ذكية في ضوء مبادرة التحول الرقمي للجامعات، المجلة التربوية، كلية التربية، جامعة سوهاج، ج ٧٨، ص ص١٢٤٩–١٣٤٤.

٣١. الربيعة صالح بن علي بن عبد الرحمن(٢٠٢٠): الأمن الرقمي وحماية المستخدم من مخاطر الإنترنت، وثيقة هيئة الاتصالات وتقنيه المعلومات، الرياض ، المملكة العربية السعودية، ص ص ١–٦٩.

٣٢. سبع، سنية محمد أحمد سليمان(٢٠٢١): تأثير التحول الرقمي وجودة الخدمة التعليمية على رضا الطلاب:دراسة تطبيقية على طلاب جامعة المنصورة، المجلة العلمية للدراسات التجارية والبيئية ، كلية التجارة بالإسماعيلية، جامعة قناة السويس ، مج ١٢ ، ع ٤، ص ص٢٤–٦٩.

٣٣. سليمان، ايناس ممدوح محمد (٢٠٢١): دور الأمن السيبرانى فى مواجهة الارهاب الالكتروني، مجلة العلوم القانونية والاقتصادية ، كلية الحقوق، جامعة عين شمس ، مج ٦٤ ، ع ١، يوليو، ص ص١–٥٢.

٣٤. سليمان، إيمان علاء الدين(٢٠٢١): الأمن السيبراني: المفهوم والتداعيات في السياسة العالمية ، قضايا ونظرات تجديد الوعي بالعالم الإسلامي والتغيير الحضاري، تقرير ربع سنوي، مركز الحضارة للدراسات والبحوث،ع٢١، ابريل، ص ص ٦٢–٧١.

٣٥. السمحان، منى عبد الله (٢٠٢٠). "متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود". مجلة كلية التربية ، جامعة المنصورة، ع ١١١، يوليو، ص ص٢–٢٩.

٣٦. السواط، حمد بن حمود بن حميد وآخرون (٢٠٢٠): العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، مجلة البحث العلمي في التربية، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس، ع ٢١ ، ج ٤، ابريل، ص ص٢٧٨–٣٠٦.

٣٧. الشايع ، خالد سعد(٢٠١٩): الأمن السيبراني" مفهومه وخصائصه وسياساته"، الدار العالمية للنشر والتوزيع، القاهرة، ص ص ١–٣٤٨.

٣٨. الشريف، دعاء حمدي محمود مصطفى (٢٠٢١): تصور مقترح لتأسيس بيئة التمكين لإنجاح التحول الرقمي في التعليم واستدامته في ضوء رؤية مصر الرقمية، المجلة التربوية، كلية التربية، جامعة سوهاج، ج ٩١، نوفمبر، ص ص ٣٦٠٤–٣٥٦١.

٣٩. الشمري، ذهب نايف (٢٠٢١): متطلبات تحقيق التحول الرقمي بالجامعات السعودية: جامعة حائل دراسة حالة، المجلة التربوية، كلية التربية، جامعة سوهاج، ج ٩٥، أكتوبر، ص ص١٦٦٥–١٧٢٢.

٤٠. الشهراني، بيان ناصر محمد (٢٠٢٠): أثر برنامج تدريبي قائم على تصميم ألعاب تعليمية إلكترونية باستخدام برنامجGame Marek لإكساب مفاهيم الأمن السيبراني لدى طالبات المرحلة المتوسطة، مجلة البحث العلمي في التربية، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس، ع٢١، ج٩، سبتمبر، ص ص ٦١٤–٦٥١.

٤١. الشهري، ناصر علي (٢٠١٣) : أمن المعلومات وعى مثالي وحماية حصينه، مطابع الحميضى ، الرياض ، المملكة العربية السعودية ، ص ص ١– ٣٩٢.

٤٢. شعبان، رشا عبد القادر محمد الهندي(٢٠٢١): تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء بعض خبرات بعض الدول، مجلة جامعة الفيوم للعلوم التربوية والنفسية، كلية التربية ، جامعة الفيوم، مج١١،ع١٥، سبتمبر، ص ص ٣٨٣–٣٣٨.

٤٣. شواب، كلاوس (٢٠٢٠): الثورة الصناعية الرابعة، ملخصات لكتب عالمية، تصدر عن مؤسسة محمد بن زايد للمعرفة، دبي، الإمارات، ص ص ١– ٢٦٨.

٤٤. الشيتى، إيناس ابراهيم (٢٠١٤) : تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربي السعودية دراسة تطبيقية على جامعة القصيم، الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات ، القاهرة، مج١٤، ص ص ١١–٢٤.

٤٥. الصادق، عادل عبد(٢٠١٥): الفضاء الإلكتروني وأسلحة الانتشار الشامل بين الردع وسباق التسلح ،

مؤتمر حروب الفضاء السيبرانى ، هولندا ، مايو ، متاح على https:// wordpress.seconf.com

٤٦. الصانع، نورة عمر وسليمان، واخرون(٢٠٢٠): وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم، مجلة كلية التربية ، جامعة أسيوط. مج ٣٦ ، ع٦، ص ص٤٢–٩٠.

٤٧. الصباحي، نسرين الشحات(٢٠١٦): الابعاد العسكرية للقوة السيبرانية على الأمن القومي للدول ، دراسة حالة إسرائيل منذ ٢٠١٠ ، المركز القومي الديمقراطي ، برلين ،المانيا، ص ص ١–١٠.

٤٨. صائغ، وفاء حسن عبد الوهاب (٢٠١٨): وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية، المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية ، مصر، ع ١٤ ، ج ٣، يوليو، ص ص١٨–٧٠.

٤٩. طاله، لامية (٢٠٢٠): التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها، مجلة معالم للدراسات القانونية والسياسية، كلية علوم الاعلام والاتصال، جامعة الجزائر، الجزائر، مج٤، ع٢، ص ص٥٦–٦٩.

٥٠. الطيار، حسين بن سليمان بن راشد(٢٠٢٠): الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية، مجلة جامعة الطائف للعلوم الإنسانية، جامعة الطائف، السعودية، مج ٦، ع ٢١، يونيو، ص ص ٢٥٥– ٢٩٨.

٥١. العابد، سكينة(٢٠٢٠): أمن المعلومات عبر شبكات التواصل الاجتماعي: موقع فيسبوك نموذجا، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب ، مصر، مج١،ع١، أكتوبر، ص ص٢٠١–٢١٨.

٥٢. عبد الحميد، أسماء عبد الفتاح نصر (٢٠٢١): متطلبات تحقيق التحول الرقمي بجامعة الأزهر لمواجهة تحديات الثورة الصناعية الرابعة، مجلة التربية، كلية التربية، جامعة الأزهر، ع ١٩٠ ، ج ١، إبريل، ص ص١٢٩–١٧٣.

٥٣. عبد الله، شاريهان محمد الصادق (٢٠٢١): رؤية مستقبلية لتطوير أدوار أعضاء هيئة التدريس بجامعة المنوفية في ضوء متطلبات التحول الرقمي، المجلة التربوية، كلية التربية، جامعة سوهاج، ج ٨٨، أغسطس، ص ص١٠٦٧–١١٠٥.

٥٤. العجلان، عبد الله بن عبد العزيز بن فهد(٢٠٠٨) : الإرهاب الالكتروني في عصر المعلومات ، بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الإنترنت"، والمنعقد بالقاهرة في المدة من ٤/٢ يونيو، ص ص١–٢١.

٥٥. العريان، محمد على (٢٠١١): الجرائم المعلوماتية : انعكاسات دورة المعلومات على قانون العقوبات، دار الجامعة الجديدة، الإسكندرية، ص ص ١–٢٦٣.

٥٦. العريشي، جبريل، والدوسري، سلمى (٢٠١٨): دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع، مجلة مكتبة الملك فهد الوطنية، مكتبة الملك فهد الوطنية بالرياض، السعودية، مج ٢٤، ع٢، ص ص١–٦١.

٥٧. عطية، أحمد محمد صلاح(٢٠٢١): التحول الرقمي في مصر: هلي يلقي بمسئوليات جديدة على المراجع، مجلة البحوث التجارية، كلية التجارة، جامعة الزقازيق ، مج ٤٣ ، ع ١، يناير، ص ص٥٣–٦٥.

٥٨. علام، أسماء أحمد أبو زيد (٢٠٢١): استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني دراسة تحليلية مقارنة، المجلة المصرية لبحوث الرأي العام، كلية الإعلام، مركز بحوث الرأي العام ، جامعة القاهرة ، مج٢٠، ع٢. يونيو، ص ص١–٤٣.

٥٩. غوص، اميرة عبد الرحمن حسن، والشريف، باسم نايف محمد(٢٠٢٢): فاعلية توظيف بعض التطبيقات التعليمية الذكية في تقديم وحدة مقترحة عن الأمن السيبراني على التحصيل المعرفي والاتجاهات نحوه لدى طالباتِ المرحلةِ المتوسطةِ بِالمدينةِ المنورةِ، مجلة التربية ،كلية التربية بالقاهرة، جامعة الازهر، ج٣، ع١٩٥،يوليو، ص ص٦٨٥–٧٣٤.

٦٠. الغامدي، عهود أحمد(٢٠٢١): الأمن السيبراني في تحقيق الميزة التنافسية: دراسة ميدانية على موظفي مطار الملك عبد العزيز الدولي بجدة، مجلة العلوم الإقتصادية والإدارية والقانونية، المركز القومي للبحوث غزة، مج ٥، ع ٩ ، مايو، ص ص١٤٤–١٦٤.

٦١. فرج، علياء عمر كامل إبراهيم (٢٠٢٢): دواعي تعزيز ثقافة الأمن السيبراني في ضوء التحول الرقمي: جامعة الأمير سطام بن عبد العزيز نموذجا، المجلة التربوية، جامعة، كلية التربية سوهاج، ج ٩٤، فبراير، ص ص٥٠٩–٥٣٧.

٦٢. فوزي، إسلام (٢٠١٩): الأمن السيبراني: الأبعاد الاجتماعية والقانونية: تحليل سوسيولوجي، المجلة الاجتماعية القومية، المركز القومي لبحوث الاجتماعية والجنائية، القاهرة، مج٥٦، ع٢، مايو، ص ص٩٩–١٣٩.

٦٣. قاسم، أيمن ،عطيف، مريم (٢٠١٩) : الأمن السيبراني ، مكتبة الملك فهد ، المملكة العربية السعودية.ص ص١– ١٦٤.

٦٤. القحطاني، نورة ناصر (٢٠١٩): مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي دراسة ميدانية، مجلة شؤون اجتماعية، جمعية الاجتماعيين بالشارقة، الامارات، مج ١٤٤، ع٣٦، ص ص٨٥–١٢٠.

٦٥. قنديلجي، عامر إبراهيم، السامرائي، إيمان فاضل (٢٠١٢): شبكة المعلومات والاتصالات، دار المسيرة للطباعة والنشر، عمان، ص ص١–٣١٤.

٦٦. كاعوه، عبير أحمد علي (٢٠٢٠): سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية، مجلة كلية التربية، جامعة حلوان، مج ٢٦، ج٣، يونيو، ص ص١٣٤–٢٠٠.

٦٧. كلاع، شريفة، (٢٠٢٢): الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور بالجلفة، الجزائر، مج ١٥ ، ع ١، ابريل، ص ص٢٩٢–٣١٤.

٦٨. محمود، احمد جلال(٢٠٢٠): إثر التهديدات غير التقليدية للأمن على العلاقات الدولية المعاصرة ، مؤتمر الأمن السيبراني في الشرق الاوسط ، مركز بحوث الشرق الاوسط والدراسات المستقبلية ، جامعة عين شمس، ص ص٣٨–٨٤.

٦٩. مرج، زغدود (٢٠٢٠): التعليم الافتراضي في وقت الأزمات الواقع والرهانات: دراسة حالة وزارة التربية الوطنية الجزائرية، مجلة دراسات في العلوم الإنسانية والاجتماعية، مركز البحث وتطوير الموارد البشرية، جامعة سكاريا، تركيا. مج ٣،ع ٤٤، ص ص٩٩–١١٤.

٧٠. مركز المعلومات ودعم اتخاذ القرار(٢٠٢٠): أهم اختراقات الأمن السيبراني لعام ٢٠٢٠ ، مجلس الوزراء، جمهورية مصر العربية، ديسمبر، ص ص ١–٣.

٧١. مشرف ، شيرين عيد مرسي (٢٠٢١): سيناريوهات مستقبلية لمواجهة مظاهر الفاقد التعليمي في إطار جائحة كورونا ، مجلة كلية التربية ، جامعة بني سويف، ع١٠، ج٢، ص ص٣٩٢–٥١٠.

٧٢. المجلس الأعلى للأمن السيبراني(٢٠١٧): الاستراتيجية الوطنية للأمن السيبراني(٢٠١٧–٢٠٢١)، رئاسة مجلس الوزراء، القاهرة، جمهورية مصر العربية، ص ص١–٩.

٧٣. المطرف، عبد الرحمن بن فهد (٢٠٢٠) : التحول الرقمي للتعليم الجامعي في ظل الأزمات بين الجامعات الحكومية والجامعات الخاصة، مجلة كلية التربية، جامعة اسيوط ، مج ٢٦، ع ٧، ص ص ١٥٨–١٨٤.

٧٤. المفيز، خولة بنت عبد الله، والعيفان ، مي بنت محمد ، والريس ،إيمان بنت إبراهيم(٢٠٢١): تحديات التحوُّل الرقمي في المدارس المطبقة لبوابة المستقبل في المملكة العربية السعودية، مجلة العلوم التربوية ، كلية التربية ، جامعة الملك سعود، الرياض ، السعودية، مج ٣٣ ، ع ٤، نوفمبر، ص ص٦٥٣–٦٧٦.

٧٥. المركز المصري للدراسات الاقتصادية (٢٠١٩)، ندوة "على أعتاب التغيير : التجارة والتنمية في عصر المعلومات"، القاهرة، ٢٣/١٢/٢٠١٩ : متاح على: www.eces.org.eg

٧٦. المملكة العربية السعودية (٢٠٢٠): الاستراتيجية الوطنية للامن السيبراني، نظرة عامة، المركز الاعلامي للهيئة الوطنية للامن السيبراني، الرياض، السعودية، ص ص٤٢–١.

٧٧. المنتشري، حليمة يوسف (٢٠١٩): الأمن السيبراني والمواطنة الرقمية المفهوم والعلاقة: ورقة عمل مقدمة للمؤتمر الدولي الثورة الصناعية الرابعة وأثرها على التعليم في الفترة من ٢١ – ٢٣ يناير، مجلة الإداري، معهد الإدارة العامة، صحار، سلطنة عمان، س٤١، ع١٥٧، ص ص١٥٠–١٧١.

٧٨. المنتشري، فاطمة يوسف، حريري، رنده (٢٠٢٠): درجة وعى معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، المجلة العربية للتربية النوعية، المؤسسة العربية للتربية والعلوم والآداب، القاهرة، ع١٤، ص ص٩٥–١٤٠.

٧٩. منصور، محمود عبد الله محمد (٢٠٢١): التحول الرقمي كآلية لتنمية رأس المال البشري بمؤسسات التعليم الجامعي، مجلة دراسات في الخدمة الاجتماعية، كلية الخدمة الاجتماعية، جامعة حلوان، ع ٥٤ ، ج ١، ابريل، ص ص١٦١–١٩٨.

٨٠. المنيع، الجوهرة عبد الرحمن إبراهيم (٢٠٢٢): متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠، المجلة العلمية لكلية التربية ، جامعة أسيوط ، مج٣٨، ع١، يناير، ص ص١٥٦–١٩٤.

٨١. الموجي، كوثر السعيد ومحمود، دينا كمال وإمام، أحمد عزمي(٢٠٢١): تصور مقترح لتفعيل الأمن السيبراني بوزارة ومديريات الشباب والرياضة بجمهورية مصر العربية، مجلة بني سويف لعلوم التربية البدنية والرياضية، جامعة بني سويف، ع٤، ص ص١٢–٣٦.

٨٢. ناصر، محمد (٢٠٢٢): أشكال انتهاك الفضاء السيبراني ووسائلها وأثارها، مجلة الندوة للدراسات القانونية، قسنطينة، الجزائر ع ٤٠، مارس، ص ص٨٦–١٢٠.

٨٣. ناني، لحسن(٢٠٢٢): جنوح الاحداث السيبراني، مجلة الفكر القانوني والسياسي ، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي الاغواط ، الجزائر، مج٦ ، مايو، ص ص١٢٨٦–١٢٩٦.

٨٤. وحدة إدارة المشروعات بوزارة التعليم العالي في مصر، متاح على:.....
http://portal.mohesr.gov.eg/ar-eg/Pages/Projects-Management Unit.aspx

٨٥. ياسين، سعد غالب (٢٠٠٩):نظم المعلومات الإدارية ، دار اليازوري العلمية للنشر والتوزيع، عمان ، الأردن، ص ص١–٢٦٩

٨٦. يوسف، امير فرج (٢٠٠٨): الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، الإسكندرية، ص ص ١–٥٩١.

ثانيا: المراجع الأجنبي

1. Alghamdi, M. (2020): A Strategic Vision to Reduce Cybercrime to Enhance Cyber Security, Webology, 17 (2), pp 289-295.
2. Alkaabi, A. (2020): A strategic Vision to Reduce Cyber-crime and Enhance Cyber security, International Journal of Advanced Science and Technology, 29(7), pp 14268-14274.
3. Alkhatani, N. (2020) :Security awareness model for digital transformation in - 96 -Raqi high schools. Security Awareness Model for Digital Transformation in Saudi High Schools, pp1-9.
4. Boneva, M. (2018): Challenges Related to the Digital Transformation of Business Companies. The 6th International Conference Innovation Management. Entrepreneurship and Sustainability. May, pp 101-114. https://www.researchgate.net/publication/331375032_Challenges_Related_to_the_Digital_Transformation_of_Business_Companies
5. Debra, N. & Karen, P. (2018): The Urgency for Cybersecurity Education: The Impact of Early College Innovation in Hawaii Rural Communities, Information Systems Education Journal (ISEDJ), 16(4), ISCAP, August, pp 41-52. https://files.eric.ed.gov/fulltext/EJ1188021.pdf
6. Edward, A. (2006): Cyber Security, Silicon Press, October, pp 1-200.
7. Hissi, S. & Haqiq, A. (2018): Conceptualization of an information system governance model dedicated to the governance of scientific research in the Moroccan University, 4th International Conference on Computer and Technology Applications (ICCTA), pp 54-58.
8. Feroz, A. & Chiravuri, A. (2021): Digital transformation and environmental sustainability: A review and research agenda. Sustainability, 13(3), pp1303-1530.
9. Ismail, M. & Zaki, M. (2017): Digital Business Transformation and Strategy: What Do We Know So Far. Cambridge Service Alliance, November, pp 1-35. https://www.researchgate.net/publication/322340970_Digital_Business_Transformation_and_Strategy_What_Do_We_Know_So_Far
10. Hamadoun, I. (2008): Cyber security, Geneva: International Telecommunication Union (ITU), pp1-27. https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-CYBER-2008-PDF-E.pdf
11. Joachim, B.& Gaute, W. (2021): A Systematic Review of Cybersecurity Risks in Higher Education, Faculty of Information Technology and Electrical Engineering, Future Internet, 13(2), pp1-40.

12. Joshi, M. J. & Patil, B. (2012): Computer virus -Their problems and Major exchat at-tacks in Real Life. Journal of Advanced Computer Science & Technology. 1 (4).
13. Kappelman, L. & McLean, E. (2019): A Study of Information Systems Issues, Practices, and Leadership in Europe. European Information Systems, 28(1), pp 26-42.
14. Kushzhanov, N. V., & Aliyev, U. Z. (2018): Changes in society and security awareness. Қазақстан Республикасы, 94
15. Lehto, M. (2018): Cyber security education and research in the finland's universities and universities of applied sciences. Cyber security and threats: Concepts, methodologies, tools, and applications, IGI Global, pp 248-267.
16. Mangold, L.V. (2016): An Analysis of Knowledge Gain in Youth Cybersecurity Education Programs.
17. Maranga, M. & Nelson, M. (2019): Emerging Issues in Cyber Security for Initiutions of Higher Education. International Journal of Computer Science & Network. 8(4). August, pp 371-379.
18. Matthew, M. (2021): Cybersecurity Education for Non-Technical learning, Masters Theses & Doctoral Dissertations, Dakota State University, march, pp 1-108.
https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1365&context=theses
19. Michelle, M. (2021): "Top Cybersecurity Threats in 2021", University of San Diego.
20. Michael, N. (1999): Computer Network Attack and The Use of Force in International Law: Thoughts on a normative framework, Columbia journal of transnational law, pp 1-41
21. Moskal, E. (2020): A model for establishing a cyber-security center of excellence. Information systems education journal. 13 (6), pp 97-101.
22. Nakama, D. & Paullet, K. (2018): The Urgency for Cybersecurity Education, The Impact of Early College Innovation in Hawaii Rural Communities, Information Systems Education Journal (ISEDJ), 16(4), ISCAP, August, pp 41-52.
23. National Initiative for Cybersecurity Careers and Studies (NICCS) (2014): "Cyber glossary" Dept. of Homeland Security [Online. Available: http://niccs.us-ert.gov/glossary#cybersecurity.
24. Ninkeu, N. & Buttler, W. (2018): Cyber education outside the cyber space: the Case of catholic university institute of Buea. International journal of technology in teaching and learning. 14 (2), pp90-101.
25. Pawlowski, S. & Jung, Y. (2015): Social Representations of Cybersecurity by university Students and Implications for Instructional Design. Journal of Information Systems Education.26(3), pp 281-294.

https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1100&context=jise

26. Rampelt, F.& Knoth, A. (2019): Bologna Digital 2020 White Paper on Digitalisation in the European Higher Education Area, pp1-47. https://www.researchgate.net/publication/333520288_Bologna_Digital_2020_-_White_Paper_on_Digitalisation_in_the_European_Higher_Education_Area/link/5cf178bd299bf1fb184e72fa/download

27. Redman, S. & Joiner, K. F. (2020): Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities? Creative Education, 11(12), pp 2541 –2558.

28. Rehman, H, A.& Cheema, A. (2015): Information Security Management in Academic Institutes of Pakistan,2nd. National Conference of Information Assurance (NCIA), pp 47-51.

29. Richard, A. (2003): Cyber security, University of California Santa Barbara (USB), Department of Computer Science, pp1-14. https://industry.ucsb.edu/sites/industry.ucsb.edu/files/pdf/dick.pdf

30. Richardson, M. &Waller, R. (2020): Planning for cyber security in schools: The human factor**.** Educational Planning, **2**(2), pp 23-39.

31. Ross, T. (2020) :Technology in the K-12 education system, October, pp 1-18.

32. Sadaghiani, T, A. (2018): Integrating cybersecurity education in K-6 curriculum: Schoolteachers, IT experts, and parents' perceptions، pp1-24.

33. Sarkar, K.& Rahman, H. (2019): A Comparative analysis of The Cyber Security Stratgey of Bangladesh. International Journal on Cybernetics (IJCI). 8(2). April, pp 1-21. https://arxiv.org/ftp/arxiv/papers/1905/1905.00299.pdf

34. Schallmo ،D. R.& Williams, C. A. (2018): Digital Transformation Now! Guiding the Successful Digitalization of your Business Model. Springer, pp1-80. https://link.springer.com/content/pdf/10.1007/978-3-319-72844-5.pdf

35. Triada network,(2019): "Different types of cyber security", triada network,

36. Ulven, J, B. & Wangen, G. (2021): A Systematic Review of Cybersecurity Risks in Higher Education, Faculty of Information Technology and Electrical Engineering, Future Internet, 13(2), 39, pp2-40.

37. Vial, G. (2019) :Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), pp 118-144.

38. Wijayanto, H., & Prabowo, I. A. (2020) :Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. Journal Sisfokom (Sistem Informasi dan Komputer), 9(3), pp 395-399.

39. Yan, Z., Xue, Y., & Lou, Y. (2021) :Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers. Computers in Human Behavior, 121 (10), pp1-39.