# سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية

**د. عبير أحمد علي كاعوه**

مدرس بقسم أصوا التربية

كلية الدراسات العليا للتربية- جامعة القاهرة

# الملخص

هدفت الدراسة الحالية لتقديم رؤية مقترحة لتضمين سياسات الأمن السيبراني بالجامعات المصرية في ضوء التحول الرقمي، حيث توجهت الحكومه المصرية لتطبيق استراتيجية التحول الرقمي لجميع الهيئات والمؤسسات لرفع مستوى أدائها، وبالتالي تعمل الجامعات المصرية لتطوير أدائها وتوفير متطلبات التحول الرقمي لجميع احتياجاتها ويتم ذلك في ظل بيئة خارجية تتسم تتزايد التغيرات المتسارعة لتكنولوجيا الإتصالات مما يمثل تحديا للتحول الرقمي وتزايد الاعتماد على الخدمات الرقمية في التواصل والعمل من بعد ما يتسبب لتعرض الجامعات للاختراقات المختلفة والمخاطر السيبرانية المتعدده، وعرضت الدراسة مفهوم التحول الرقمي للجامعات ومبررات التحول الرقمي للجامعات، وخطوات ومتتطلبات تطبيق التحول الرقمي، وجهود الجامعات المصرية للتحول الرقمي، ثم تعرف مفهوم الأمن السيبراني، وأهدافه وأهميته، وأهم المخاطر السيبرانية، وكيفية الحماية منها، وعرض لبعض التجارب الدولية لسياسات الأمن السيبراني كمناخ داعم لحماية البنية التحتية الرقمية للجامعات، ما يسهم في دعم أداء الجامعة وبالتالي تحسين تصنيفها عالميا، وتأكيد الدور التكاملي للجامعات مع باقي قطاعات الدولة من اقتصاد وصناعة وتسهيل عملية التنسيق والتواصل بينهم من خلال بنية تكنولوجيا رقمية آمنة.

وقد توصلت الدراسة لوضع رؤية مقترحة لسياسات الأمن السيبراني للجامعات المصرية بالاستفادة من الخبرات الدولية.

**الكلمات المفتاحية**: الأمن السيبراني، التحول الرقمي للجامعات، التجارب الدولية لسياسات الأمن السيبراني

**Abstract**

This study aimed to present a proposed vision for the inclusion of cybersecurity policies in Egyptian universities in light of digital transformation. As the Egyptian government has directed to implement the digital transformation strategy for all bodies and institutions to raise the level of their performance. and therefore Egyptian universities are working to develop their performance and provide the requirements for digital transformation for all their needs. and this is done in an external environment characterized by the increasing rapid changes in communication technology. which represents a challenge to the digital transformation and the increasing dependence on digital services in Communication and remote work. which causes universities to be exposed to various penetrations and risks The study presented the concept of digital transformation for universities. the justifications for the digital transformation of universities. the steps and requirements for applying digital transformation. and the efforts of Egyptian universities for digital transformation. then defines the concept of cybersecurity. its objectives and importance. the most important cyber risks. and how to protect them. and a presentation of some international experiences of cybersecurity policies As a supportive climate to protect universities› digital infrastructure. Which contributes to supporting the university's performance and thus improving its global ranking. confirming the integrative role of universities with the rest of the state's sectors of economy and industry. and facilitating coordination and communication between them through a secure digital technology infrastructure.

The study reached a proposed vision for the cybersecurity policies of Egyptian universities. by making use of international experiences.

**key words**: Cybersecurity. The digital transformation of universities. International experiences of cybersecurity policies

## المقدمة

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 التعلم الافتراضي، والتعلم الرقمي، والتعلم الذكي، الأمر الذي أسفر عنه دخول الجامعات في سباق التحدي والاستجابة للتطور الرقمي وامتلاك بنية تحتية رقمية قادرة على المنافسة عالميًّا في الفضاء السيبراني المستجد المتضمن عددًا لا نهائيًّا من الكيانات الافتراضية.

ويترتب على ذلك ضرورة تبنِّي الجامعات إستراتيجية رقمية واضحة للتحول للمستقبل الرقمي من خلال بناء أنظمة معلوماتية غنية بالبيانات الرقمية، ومن خلال الحوسبة السحابية، وإنترنت الأشياء، والاتصالات النقالة، والتوظيف المكثف لتكنولوجيا المعلومات بشكل تستفيد منه الجامعات في جميع مجالاتها التعليمية، والخدمية، والإدارية. (Edelhard & etc al. 2019. 100)

ويعد التحول الرقمي من أبرز الاتجاهات والسمات العالمية اليوم، وهو يهدف إلى تمكين المؤسسات في قطاع الأعمال والخدمات من التوافق مع طبيعة متغيرات العصر الرقمي، وقد استهدفت رؤية مصر 2030 التطوير التكنولوجي الشامل لكل قطاعات الدولة بمنظومة وطنية تستطيع التعامل التنافسي مع الكيانات إقليميًّا، وعالميًّا، ونتيجةً لتوجه الحكومة المصرية إلى تطبيق إستراتيجية التحول الرقمي لجميع الهيئات والمؤسسات لرفع مستوى أدائها وجدت الجامعات المصرية نفسها أمام ضرورة تطوير أدائها وتوفير متطلبات التحول الرقمي في جميع مجالاتها، وإثبات القدرة على استيعاب التكنولوجيا الجديدة وقبولها واستخدامها في ظل التحديات والتغيرات السريعة التي تحيط بها عالميًّا( رؤية مصر 2030).

ويحقق التحول الرقمي للجامعات المرونة والفاعلية التي تسهم في التكامل بين وظائف الجامعة بتوفير فرص لتقديم خدمات مبتكرة وإبداعية بعيدًا عن الطرق التقليدية في تقديم الخدمات، وبالتالي المساهمة في تحسين الاقتصاد الرقمي للدولة ( البار،2019، 2)، ويعتمد التحول الرقمي للجامعات على قوة البنية التحتية والدعم الفني اللازم لتطبيق تكنولوجيا المعلومات والاتصال واستخدامها وتوظيفها التوظيف الأمثل في جميع المجالات الرقمية للجامعة؛ التعليمية والإدارية والخدمية، وعلى كافة المستويات، ما يسهل وييسر عمليات التواصل والتعاون بين جميع العاملين داخل الجامعة بشكل منظم وأداة داعمة لتحليل البيانات وتحويلها إلى معلومات تستطيع استخدامها في صناعة القرارات بشكل أسرع وبطريقة أفضل تعمل على تحسين الجودة وسهولة الانتشار في نطاق أوسع (Jensen. 2019.15).

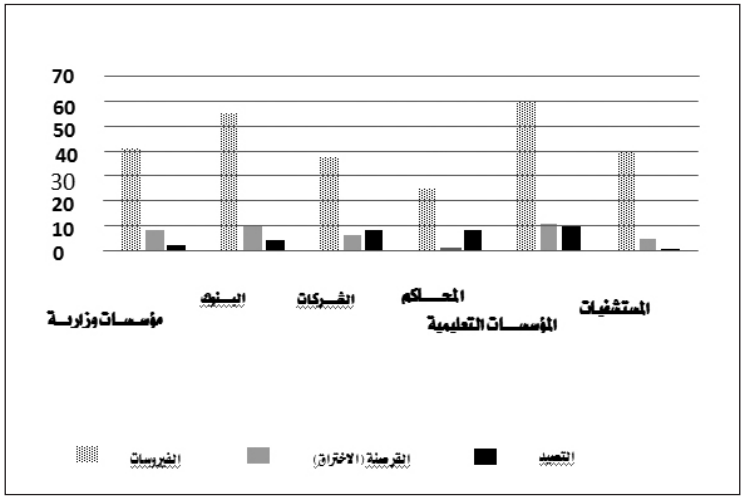
ورغم الاعتماد الأساسي على شبكة المعلومات والاتصالات في جميع الخدمات والمهام الرقمية للجامعات وما تتيحه هذه الشبكة من عديد الفرص التي يقدمها الإنترنت للجامعة الرقمية إلا أن استخدام الإنترنت يواجه مجموعة من المخاطر والعقبات؛ كخطر التهديدات والاختراقات الإلكترونية والتي ازدادت بطريقة ملحوظة في الفترة الحالية، كما أن تَنامِي خطر هذه الهجمات الإلكترونية بشكل مزعج هو أمرٌ يعوق التطور ويؤثر سلبًا على عمليات التحول الرقمي وعلى القدرة على جمع البيانات والأصول والعمليات ( أبو دوح، 2018، 1)، الأمر الذي شجع العديد من الحكومات في المجتمع الدولي على تخصيص جزء من مواردها المالية تستطيع به زيادة قدرتها على مواجهة تلك الهجمات والتصدي لها، ويتم ذلك عن طريق وسائل الحماية وتأمين البنية التحتية الرقمية التي هى أساس التحول الرقمي، ما يتطلب انتهاج عدد من السياسات واتخاذ إجراءات متنوعة من جانب الحكومات فيما يسمى بـ(سياسات الأمن السيبراني) لتعزيز الثقة والحماية، والاستفادة من مزايا التحول الرقمي والتطوير المصاحب له Tiwari. et al.2016.40.

ويمثل الأمن السيبراني الركيزة الأساسية لأي تحول رقمي للمؤسسات، وهو يعتمد على الاستفادة من التكنولوجيات الرقمية دون خوف، وزيادة فرص الابتكار والتطوير،

كما أنه يوفر للدولة القدرة على حماية مؤسساتها ومصالحها، وقد أصبح إعداد جيش للأمن السيبراني من ضروريات العصر الرقمي بسبب تنامي الاستغلال السيئ المنحرف للشبكات الإلكترونية لتحقيق أهداف إجرامية، ما يؤثر على خصوصية المعلومات للمؤسسات والأفراد(Kortjan .2013.30)، ففي عام 2020 ازدادت وتيرة الهجمات السيبرانية بكل أنواعها مع انتشار فيروس كورونا المستجد وزيادة عدد المستخدمين على الإنترنت وزيادة الإعتماد على الخدمات الرقمية في التواصل والعمل من بعد ( مركز المعلومات ودعم اتخاذ القرار، 2020 ،1 ).

ويهتم مؤشر الأمن السيبراني العالمي (GCI) Global Cybersecurity Index للاتحاد الدولي للاتصالات التابع للأمم المتحدة بمتابعة قياس وتقييم التهديدات والتوعية بتلك الهجمات وماهية خسائرها على مستوى الدول من خلال تقرير يصدر بشكل دوري منذ عام 2009، من خلال خمسة أبعاد هى: البعد التقني والبعد القانوني والبعد التنظيمي وبناء القدرات، والتعاون الدولي، وقد سجلت مصر عام 2017 الترتيب العالمي 14 والإقليمي الثاني وتراجع الترتيب عام 2018 الى الترتيب 23 عالميا والرابع إقليميًا ويشير ذلك التراجع لضعف القدرة على التصدي للهجمات السيبرانية في مصرITU.2019.57 ، وفي دراسة أجريت لمكتب الأمم المتحدة هدفت إلى قياس توافر برامج وطنية للأمن السيبراني، خلصت إلى أن ٪59 من عينة الدراسة هى من تمتلك سياسات وبرامج للأمن السيبراني مخططًا لها، وأن حوالي ٪40 من هذه الدول تولت المؤسسات التعليمية بها التخطيط ومتابعة تطبيق برامج الأمن السيبراني فيها30–ITU. 2012.20 .

وطبقا لدراسة مسحية قامت بها هيئة المعلومات وتكنولوجيا الاتصال عام 2016 (The Public Sector ICT Survey. 2016.، فإن المؤسسات التعليمية تتعرض للهجمات السيبرانية بنسبة أكبر مقارنة بمؤسسات القطاعات الأخرى، كما يوضحها الشكل التالي:




**المصدر: The Public Sector ICT Survey 2016**

وعليه فإن الأمر يستدعى تعزيز مفاهيم وآليات الأمن السيبراني للجامعات لحماية المعلومات والبيانات والأبحاث العلمية الخاصة بها والتي تتصف بالبيانات الحساسة، وضرورة العمل على تثقيف بيئة الجامعة عن الانتهاكات والمخاطر السيبرانية وتوفير طرق الوقاية ضد الهجمات السيبرانية( Sarker et al. 2019.14).

وبالتالي اهتمت المؤسسات التربوية في مختلف دول العالم بتنمية مفاهيم الأمن السيبراني للمعلم والطلاب والعاملين بما يمكِّن المجتمع من القدرة على التعامل بوعي مع شبكات الإنترنت والتصدي للوصول غير المسموح عبر الشبكات، وقد أدرج الاتحاد الأوروبي المفاهيم المتعلقة بالأمن السيبراني ضمن المقررات الدراسية منذ عام 2009 في 24 دولة أوروبية، وتمت بالمثل إجراءات مشابهة في عدد من الدول في آسيا مثل اليابان والهند وسنغافورا، ولم تكن الدول العربية في منأى عن الصورة الأمنية للفضاء السيبراني؛ فقد خطت المملكة العربية السعودية خطى واسعة في مجال الأمن السيبراني؛ حيث صدر المرسوم الملكي أكتوبر 2017عام بإنشاء هيئة وطنية لحماية الأمن السيبراني لحماية مصالح الدولة بأكملها، وتختص جامعة نايف للعلوم الأمنية بالرياض بدور متميز في مجال الأمن السيبراني (Solms & Solms. 2015.114–119)؛ حيث تعمل

على نشر المعرفة والثقافة، وإثراء المهارات العلمية في أمن المعلومات بجميع كلياتها ومراكزها، وقد تنوعت أنشطتها بين دورات تدريبية ومؤتمرات علمية في موضوعات مختلفة، ومنها: الجريمة المعلوماتية، وأمن المعلومات، والشبكات، ومكافحة القرصنة السيبرانية، وذلك إيمانًا منها بأن دور الجامعة الأكاديمي يشمل تطوير مجال الأمن السيبراني (عالم، 2018، 7). وتعمل الإمارات العربية المتحدة على تعزيز الأمن السيبراني في مجتمعها لدى المواطنين والمقيمين من خلال عدة مبادرات؛ حيث تم إطلاق إستراتيجية دبي للأمن الإلكتروني من مركز دبي للأمن الإلكتروني تعزيزًا لمكانة دبي كمدينة عالمية رائدة في الابتكار والسلامة والأمن، وترسيخًا لمكانتها بوصفها المدينة الأكثر أمانًا في الفضاء الإلكتروني، بالإضافة إلى إطلاق مؤشر دبي للأمن الإلكتروني لوضع معايير لضمان تحقيق الأمن الإلكتروني في الإمارة، إلى جانب التأكد من وجود أنظمة أمن وشبكة اتصالات وأنظمة معلومات لدى الجهات الحكومية، والتزامها بتنفيذ متطلبات أمن المعلومات الصادرة من المركز، وتوفير منصة رقمية eCrimeوإتاحة تطبيق (مجتمعي آمن) عبر الهواتف الذكية لأفراد المجتمع، وهو التطبيق الذي أطلقته النيابة العامة الاتحادية في يونيو 2018 للإبلاغ عبر أربع وسائل، هى: الصور، الفيديو، والتسجيل الصوتي، وتحميل الرابط، وغيرها من المبادرات، إلا أن الإمارات أكدت في إستراتيجيتها للأمن السيبراني أهمية دور المؤسسات الأكاديمية لدعم عمل المنظومة بأكملها باعتبارها المحرك الأساسي لتحقيق أهدافها في الأمن السيبراني ( الهيئة العامة لتنظيم قطاع الاتصالات ، 2019، 24).

وفي مصر نص دستور 2014 في مادته 31 على أن " أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون" ، وفي إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري تم إنشاء المجلس الأعلى لتأمين البنية التحتية للاتصالات والمعلومات (المجلس الأعلى للأمن السيبراني) التابع لرئاسة مجلس الوزراء برئاسة وزير الاتصالات وتكنولوجيا المعلومات لعام 2015، وقد وضع المجلس استراتيجية

وطنية للأمن السيبراني (2017–2021) لتأمين البنى التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف قطاعات الدولة وتقديم الخدمات الإلكترونية بشكل متكامل، وتتضمن الإستراتيجية عددًا من البرامج التي تدعم الأهداف الإستراتيجية للأمن السيبراني بما يدعم التحول نحو اقتصاد رقمي متكامل يحافظ على مصالح الدولة ويسهم في نهضتها ( المجلس الأعلى للأمن السيبراني، 2017، 3).

وقد شهد عام 2017 تضاعف عدد حوداث الأمن السيبراني عالميًّا، حيث تم تسجيل حوالي ٪40 زيادةً في عدد الاختراقات الأمنية للبيانات عالميًّا، وخسائر سنوية مقدارها 608 مليار دولار أمريكي بسبب الجرائم السيبرانية عالميًّا، ومعدل خسائر إجمالية قدره 3.9 مليار دولار أمريكي لاختراقات البيانات عالميًّا ( الهيئة العامة لتنظيم قطاع الاتصالات ، 2019، 3)، بينما تخطت خسائر الهجمات الإلكترونية لعام 2020 التريليون دولار، ومن المتوقع أن تصل خسائر تلك الهجمات إلى 6 تريليون دولار عام 2021، ومن المتوقع أن يتكبد العالم خسائر سنوية تقدر بحوالي 10.5 تريليون دولار بحلول عام 2025 ( مركز المعلومات ودعم اتخاذ القرار، 2020 ،5 ).

ويتضح من خلال ما سبق حتمية الدور الأساسي الذي فرضه التحول الرقمي في تنمية المجتمعات علميًّا واقتصاديًّا من أجل إيجاد بيئة مجتمعية آمنة رقميًّا، وهو ما تهدف إليه جميع الحكومات والمؤسسات على مستوى العالم، فإلى جانب التقنيات الرقمية وتوفير الأجهزة وملحقاتها ينبغي الاهتمام بالموارد والكفاءات البشرية لتطبيق برامج الأمن السيبراني، حيث تمثل اختراقات الأمن السيبراني أكثر الحوادث التي تؤثر سلبًا على الأمن القومي والإقتصاد في القرن الحالي وتتنوع هذه الحوادث من اختراق لأنظمة البنية التحتية الحرجة للمعلومات والاتصالات أو اختراق البرمجيات أواستهداف المؤسسات ( مركز المعلومات ودعم اتخاذ القرار، 2020 ،1 )، وقد أجمعت العديد من الدراسات والتقارير الدولية على أن الموارد البشرية تسهم بأكثر من ٪90 في برامج الأمن السيبراني من خلال (الدراسات الأكاديمية، وتطوير البرمجيات، والبرامج التدريبية، والقوانين والسياسات، والاتفاقيات الدولية، والسياسة الإعلامية) ( Joshi &

Patil. 2012.)، ويعتمد جميع ذلك على القدرات البشرية بشكل خاص، ويعد نقص الكوادر المؤهلة من المعوقات التي تزيد من المخاطر الأمنية للمؤسسات(عالم، 2018، 3)، الأمر الذي وجه النظر إلى ضرورة أن يكون التخطيط لسياسات الأمن السيبراني على مستوى دول العالم ضمن القضايا الوطنية الهامة والتي لا تقل خطورةً عن إعداد جيش لحماية الحدود الطبيعية، وبخاصة أنه لا توجد دولة في مأمن من الهجمات السيبرانية، وبالتالي يُعَدُّ الأمن السيبراني أولوية في السياسات والإستراتيجيات المستقبلية.

**مشكلة الدراسة**

بالرغم من الجهود المبذولة من جانب وزارة التعليم العالي بمصر، وتزايد الحاجة إلى سرعة تطبيق التحول الرقمي للجامعات المصرية لما يضيفه هذا التحول من مهارات رقمية لجميع العاملين بالجامعات وخريجيها، بالإضافة إلى اكتساب الجامعة ميزة تنافسية في التصنيفات العالمية إلا أن عددًا من المؤتمرات والدراسات أشار إلى أهمية توفير البنى التحتية الملائمة لاستخدام أنظمة تكنولوجيا المعلومات والاتصالات والذي يعد أساس نجاح التحول الرقمي، ولكن هذا الأمر محاط بالعديد من القيود التي ما تزال تواجهها الدول النامية؛ حيث يلاحظ محدودية القدرة على تحديد وتخفيف المخاطر التي تتفاقم بسبب التكنولوجيا، بما في ذلك الهجمات الإلكترونية (مشروع إستراتيجية التحول الرقمي لأفريقيا،2020، 4)، ويعتبر الاستعداد للتحول الرقمي بالوعي والتخطيط لسياسات الأمن السيبراني أحد أهم المهارات الرقمية التي تساعد الجامعات على حماية هذا التحول من عدد من الخسائر والتهديدات التي تعوق سير التطور، والتي تؤثر سلبًا على النتائج المرجوة من التحول الرقمي، ويعد ذلك من المتطلبات الأمنية بالغة الأهمية للتحول الرقمي للجامعات في مصر، وخصوصا بعد انتشار العديد من محاولات اختراق شبكات المعلومات والاتصالات بغرض السرقة أو تدمير المعلومات (أمين، 2018، 95)، ولكن يلاحظ أن الكادر التعليمي يفتقد تلك المهارات والأدوات الأمنية، وكذلك تفتقد الإستراتيجية الوطنيه للأمن السيبراني في مصر لبرنامج حماية البنى التحتية للمؤسسات التعليمية وبخاصة فى ضوء مبادرات التحول الرقمي في مصر (المجلس الأعلى للأمن السيبراني، 2017، 5).

وقد نتج عن غياب دور الجامعة كأحد أهم المؤسسات التربوية بمصر في التخطيط لسياسات الأمن السيبراني – سواء في خطط وزارة التعليم العالي أو الإستراتيجية الوطنية للأمن السيبراني – افتقاد الكادر التعليمي إلى كفاءات ومهارات والوعي بالأدوات والتخطيط لمفاهيم الأمن السيبراني، وبالتالي احتياج جميع الأطراف داخل الجامعات إلى الدعم والتدريب على مهارات الأمن السيبراني وتأهيل الكوادر لتكون درعًا لصد الهجمات السيبرانية لتعزيز أدائهم وبناء قدراتهم على التصدي لمخاطر الإنترنت، وبالتالي حماية البنية التحتية الرقمية والقدرة على المنافسة العالمية في مجال الرقمنة.

**ويتمثل السؤال الرئيس للدراسة فيما يلي:**

**كيف يسهم الأمن السيبراني في تعزيز التحول الرقمي للجامعات المصرية؟**

**ويتفرع منه عددا من الأسئلة الفرعية كما يلي:**

1. ما مفهوم التحول الرقمي للجامعات؟ وما فلسفته؟ وما أهم متطلبات تطبيقه؟
2. ما الجهود المبذولة للتحول الرقمي في الجامعات المصرية؟
3. ماهية الأمن السيبراني؟ وما أهمية تطبيقه؟
4. ما سياسات الأمن السيبراني التي تطبقها الدول المختلفة لتأمين الجامعات الرقمية؟
5. ما التصور المقترح لسياسات الأمن السيبراني لتعزيز التحول الرقمي في الجامعات المصرية؟

**منهج الدراسة، وخطواتها**

تستعين الدراسة بالمنهج الوصفي لوصف وتحليل مشكلة الدراسة، ووصف التحول الرقمي للجامعات، وأهم متطلبات تطبيقه، ومعرفة وتحديد العلاقات بين مكونات التحول الرقمي، وسياسات الأمن السيبراني، وأهميته، وكيفية تخطيطه في الدول المختلفة، وأهم وسائل التوعية التي يتم تطبيقها في المجتمعات المختلفة، وكيفية التغلب على المخاطر والتهديدات السيبرانية للاستعانة بها لوضع الخطط المستقبلية للعلاج في الجامعات المصرية.

كما تستعين الدراسة بالمنهج المستقبلي لرسم تصور مقترح لسياسات الأمن السيبراني بحيث تستطيع أن تحمي البنية التكنولوجيا الرقمية الداعمة للتحول الرقمي للجامعات المصرية.

**وتسير خطوات الدراسة على النحو التالي:**

- عرض وتحليل الدراسات السابقة الخاصة بالتحول الرقمي للجامعات، والخاصة بالأمن السيبراني.
- تحديد مفهوم التحول الرقمي، وأهم متطلبات نجاحه.
- عرض بعض المبادرات والجهود في مصر للتحول الرقمي للجامعات.
- تحديد مفهوم الأمن السيبراني، وأهميته وأساليب الحماية من المخاطر السيبرانية.
- عرض بعض نماذج الخبرات المختلفة لسياسات الأمن السيبراني للدول المختلفة.
- إعداد التصور المقترح لسياسة الأمن السيبراني التي تستطيع حماية البنية الرقمية للجامعات لتعزيز آليات التحول الرقمي المطبقة في الجامعات بمصر.

**أهداف الدراسة**

- تعرف ماهية التحول الرقمي للجامعات.
- تعرف الجهود والمبادرات المصرية للتحول الرقمي بالجامعات.
- تعرف ماهية الأمن السيبراني وأهم متطلبات تطبيقه.
- تعرف سياسات الأمن السيبراني للدول المختلفة لتأمين البنية التحتية.
- وضع تصور مستقبلي لسياسات الأمن السيبراني في مصر لتعزيز التحول الرقمي بالجامعات.

**أهمية الدراسة**

**تتزامن الدراسة الحالية مع الظروف التالية:**

- السعي الجاد لجميع مؤسسات الدولة بمصر نحو التحول الرقمي حيث يعد التحول الرقمي في مصر جزءًا أساسيًّا من خطتها الرامية إلى التحول إلى الاقتصاد الرقمي.

- توجه وزارة التعليم العالي للتحول الرقمي بالجامعات المصرية.
- التوسع في مشروعات دعم البنية التحتية للجامعات المصرية.
- صدور تشريعات جديدة للجامعات المصرية والتي يعد من أهمها تعديل اللائحة التنفيذية لقانون تنظيم الجامعات في ضوء الاعتماد على النظام الإلكتروني والهجين للتعليم.
- استمرار جائحة كورونا والتي أثرت على قدرة الجامعات على التدريس بالنظام التقليدي للتعليم، والاتجاه نحو النظام الرقمي للتعليم، بالاعتماد على البنية التحتية الرقمية.
- تزايد خطر الهجمات الإلكترونية التي تهدد بقاء واستمرار البنى الرقمية للجامعات.

**مصطلحات الدراسة**

- **التحول الرقمي**: يعرف على أنه " انتقال المؤسسات من الواقع المادي الملموس إلى الوجود على شبكات الانترنت لجميع عمليات وأنشطة المؤسسة" (Kuzu. 2020.9)

ويمكن توضيح التحول الرقمي للجامعات اجرائيا أنه الانتقال من نظم التعليم التقليدية إلى نظم التعليم الإلكترونية، ودعم عمليات التغيير الجذري لجميع مجالات الجامعة، والاعتماد في ذلك بشكل أساس على البنية التحتية الرقمية الشاملة.

- **الأمن السيبراني**: يعرف على أنه "مجموعة الإجراءات التقنية والإدارية والتي تشمل العمليات والآليات التي تطبقها المؤسسات لتأمين البنية الرقمية بها والحفاظ على سرية البيانات والمعلومات" (Wilson. 2014.3).

ويمكن توضيحه اجرائيا على أنه مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع اختراق شبكات المعلومات وتوفير الحماية الأمنية للبنية التحتية الرقمية للمؤسسات.

- **السياسات**: مجموعة القواعد والتنظيمات الإدارية التي توضع من خلال الإدارة العليا للمؤسسة.

**أولًا: الدراسات السابقة ذات الصلة بموضوع الدراسة**

فيما يلي عرض للدراسات السابقة التي تعرضت للتحول الرقمي للجامعات، والتي تناولت الأمن السيبراني، مع تناولها بالتوضيح والتفسير، والإشارة إلى أهمية الدور التربوي للتوعية بالأمن السيبراني وإعداد الكوادر المؤهلة، وسوف يتم توضيح هذه المحاور على النحو التالي:

- **دراسات حول التحول الرقمي للجامعات**

**1 . «التحول الرقمي للجامعات المصرية – المتطلبات والآليات» – (علي، 2011):**

هدفت هذه الدراسة إلى تعرف ماهية التحول الرقمي في الجامعات، وأهم متطلبات تطبيقه، وعرضت لجهود التحول بالجامعات المصرية، وأهم التحديات والصعوبات التي تواجه تطبيق التحول الرقمي، وقدمت اقتراحًا لآليات تطبيق التحول الرقمي في الجامعات المصرية، وقد توصلت الدراسة إلى أنه من الضروري تحليل البيئة الداخلية والخارجية للجامعات المصرية بغرض الوقوف بشكل واضح على جوانب القوة والضعف للجامعات المصرية، وبالتالي القدرة على وضع إستراتيجية للتحول الرقمي تعتمد على تنمية الموارد البشرية في الجامعة، والوعي بآليات التحول الرقمي، ونشر الثقافة الرقمية داخل وخارج الجامعات المصرية.

**2 . «التحول الرقمي في الجامعات المصرية كمتطلب لتحقيق مجتمع المعرفة» (أمين، 2018):**

هدفت هذه الدراسة إلى تحليل وتحديد مفهوم مجتمع المعرفة، وأبعاده المختلفة، وكذلك تحليل وتحديد مفهوم التحول الرقمي، ونماذجه، وأسس بنائه، وعرض لبعض الجهود التي بذلت للتحول الرقمي في الجامعات المصرية وبعض الجامعات الأجنبية، واعتمدت الدراسة على تحديد آليات التحول الرقمي بالجامعات المصرية، وهى: وضع إستراتيجية للتحول الرقمي، ونشر ثقافة التحول الرقمي، والمتطلبات البشرية، والتقنية، والأمنية، والتشريعية، وقد توصلت الدراسة إلى أن متطلبات التحول الرقمي في الجامعات المصرية تمثل مجموعة من الأسس والقواعد الأساسية اللازم

توافرها في الجامعات لبناء مجتمع المعرفة، وذلك من خلال عدد من الآليات التي تم تحديدها في الدراسة والتي يعد من أهمها: وضع إستراتيجية للتحول الرقمي لتطوير الكفايات والقدرات داخل الجامعات، والتأكيد على نشر ثقافة التحول الرقمي، وضرورة توفير أساليب وإجراءات أمنية؛ لأنه من الأمور بالغة الأهمية التي تساعد على حماية المعلومات والبيانات من الاختراق في ضوء الثورة التكنولوجية وازدياد شبكات الاتصالات والمعلومات، وبخاصة بعد انتشار العديد من محاولات اختراق منظومات الحواسيب بغرض سرقة أو تدمير المعلومات.

**3 . «مستقبل الجامعات: هل الأولوية للرقمنة؟» 2018 . Efimov. & Laptreva**

هدفت هذه الدراسة إلى تعرُّف التحديات والمعوقات التي تواجه تطبيق الرقمنة في الجامعات، وتأثير تلك السلبيات على أولويات التطوير لدى إدارة الجامعة، وقد أكدت الدراسة أن التحدي الأهم للجامعات 2035 هو الرقمنة، والقدرة على توظيف واستخدام الانتشار الواسع للتكنولوجيا في التعليم وإدارة الجامعات، ويشكل التنامي المتسارع للاقتصاد الرقمي موقف استدعاء التطوير في جميع جوانب البنية التحتية الرقمية من حيث (شبكات الكمبيوتر، البرمجيات، الأنظمة الإلكترونية، بيئات التعلم الرقمية)، وعلى ذلك تعد الرقمنة من القضايا الملحة الحالية والتحدي الذي يواجه الجامعات في نفس الوقت، وقد توصلت الدراسة إلى نتيجة، وهى أنه بقدر ما تطبق الجامعات الرقمنة تنعكس صورتها ومكانتها بين الجامعات وتتعزز القدرة التنافسية الرقمية لها.

**4 . «رقمنة التعليم العالي: المدخل المؤسسي لخريطة التعليم والتعلم»: Edelhard & etc al. 2019**

هدفت هذه الدراسة إلى تعرف السياسات المؤثرة على عمليات التحول الرقمي للجامعات والتي تمثلت في: سياسات خارج الجامعة تتبع سلطات الدولة، وسياسات داخلية تخص إدارة الجامعة، بالإضافة إلى تأثير أعضاء هيئة التدريس والطلاب والمستفيدين على القرارات الإدارية للجامعة، وقد أوضحت الدراسة أن التناسق بين سياسات الدولة وإدارة الجامعة يؤدي إلى تفعيل عمليات التحول الرقمي وترسيخ

الأمان في تبادل المعلومات بينهما، وذلك على العكس من المناخ الإداري غير التنظيمي الذي يعد من المعوقات التي تحول دون الوصول إلى تطبيق آليات التحول الرقمي.

**5 . «التحول الرقمي للجامعات – دراسة حالة للتخطيط الإستراتيجي» -: Kuzu. 2020**

هدفت هذه الدراسة إلى تعرُّف تأثير التخطيط الإستراتيجي على التحول الرقمي للجامعات، وقد شملت عينة الدراسة عددًا من الجامعات التركية التي تحتل مكانة مرتفعة في التصنيف العالمي، كما هدفت إلى تعرُّف طرق وأساسيات بناء النظم الرقمية لتلك الجامعات، وقد خرجت الدراسة بعدد من النتائج، من أهمها: ضرورة التخطيط المناسب لبناء بيئة التعلم الرقمي التي تتناسب مع إمكانيات وقدرات الجامعة، وضرورة العمل على متابعة تطبيق تلك الخطة ونشر الوعي بثقافة المهارات الرقمية، والاهتمام بخطط تطوير البنية الرقمية باستمرار، وضرورة إشراك المتعلم في تلك الخطط، وأهمية التدريب على كيفية التواصل الرقمي وضمان الاستخدام الآمن له.

**6 . «رؤية مقترحة لتحويل الجامعات المصرية الحكومية إلى جامعات ذكية في ضوء مبادرة التحول الرقمي للجامعات»: (الدهشان والسيد، 2020)**

هدفت هذه الدراسة إلى تعرف مفهوم الجامعات الذكية وخصائصها ومتطلباتها، واستعراض متطلبات تحقيق التحول الرقمي للجامعات المصرية، وكذلك تحديد متطلبات تحويل الجامعات المصرية الحكومية إلى جامعات ذكية في ضوء مبادرة التحول الرقمي لها من وجهة نظر أعضاء هيئة التدريس في بعض الجامعات المصرية، وقد توصلت الدراسة إلى وضع رؤية مقترحة لتحويل الجامعات المصرية الحكومية إلى جامعات ذكية في وجود مجتمع جامعي ذكي قادر على المنافسة العالمية والابتكار والإبداع، وتعتمد هذه الرؤية على تحديد رؤية رقمية واضحة، وإدارة ذكية، وتوافر عناصر بشرية ذكية، وتجهيز بيئة تعليمية ذكية، وتجهيز بنية تحتية ذكية، مع التأكيد على التوعية بالتحول الرقمي للجامعات بين جميع الأطراف المعنية، وتوفير التشريعات اللازمة للوصول للجامعة الذكية، وضمان أمن وسلامة المعلومات على مواقع تلك الجامعة، بالإضافة إلى أهمية توافر الإمكانات المادية والمالية اللازمة والداعمة لنجاح التحول الرقمي للجامعات المصرية.

- **دراسات حول الأمن السيبراني**

**1 . «دور الجامعات المصرية في مواجهة الجرائم الإلكترونية لدى الطلاب» محمود، 2011**

هدفت هذه الدراسة إلى تعرف ماهية الجريمة الإلكترونية، وأنواعها، وخصائص المجرم الإلكتروني، والجرائم الإلكترونية على ضوء وظائفها. ووضع البحث في نهايته تصورًا لدور الجامعة في مكافحة الجرائم الإلكترونية علي ضوء وظائف الجامعة والمتمثلة في التدريس والبحث العلمي وخدمة المجتمع. وتوصل البحث إلى أنه من الآثار العملية والتكنولوجية السلبية للجرائم الإلكترونية زيادة الفجوة بين الدول المتقدمة والدول النامية، إذ أصبحت الدول تحتكر المعلومات وتسطو على مراكز الحاسب الآلي، كما أنها تقوم بسرقة المعلومات بعدة أساليب، منها: تحطيم هذه المعلومات، أو تغيير أو استنساخ البيانات، وهى بذلك تحارب، وسلاحها هو الحاسوب، مما يتطلب ضرورة الوعي بإجراءات الحماية ضد الجرائم السيبرانية، وعلى الجامعات المصرية دور فاعل من خلال وظائفها الثلاثة لتفعيل تلك الآليات والعمل على نشرها في المجتمع المصري.

**2 . «المسئولية الاجتماعية للأمن السيبراني لطلاب الجامعة، وقياس آثارها من خلال طرق التدريس» Pawlowski & Jung. 2015**

هدفت الدراسة إلى تعرف وعي الطلاب بماهية آليات الأمن السيبراني، والتوعية بالأخطار والتهديدات السيبرانية التي قد تلحق الضرر على المستويين الشخصي والمؤسسي، وتوصي الدراسة بضرورة دراسة الأمن السيبراني ضمن مقدمة نظم المعلومات لطلاب الجامعات، الأمر الذي يشكل أهميةً تتزايد مع التطور التكنولوجي المتلاحق، وأهمية الاعتماد على تدريسه بطرق متميزة ومبدعة للطلاب لضمان استمرار تطور المجتمع بأمان سيبراني في حياتهم الشخصية والمهنية.

**3 . «التطبيقات الرقمية للأمن السيبراني، مدخل لإدارة الجامعات – VFU برنامج التعلم الذكي» Nedyalkova. Bakardjieva. & Nedyalkov .2016**

هدفت هذه الدراسة إلى تعرف آليات الإدارة الرقمية للجامعات، وكيفية التنسيق بالتوازن بين توفير البيئة الرقمية الآمنة لجميع كليات الجامعة، والإدارات الفرعية،

والطلاب وغيرها، ولتحقيق ذلك المستوى الأمني قامت الجامعة بتوفير تطبيق رقمي خاص بها، وعملت على تدريب أعضاء هيئة التدريس والطلاب عليه، ومنحت الطالب الحق في استخدامه حتى التخرج.

**4 . «تعليم الأمن السيبراني بالدول النامية: البيئة التعليمية» (Catota. .Morgan. & Sicker.2019)**

هدفت هذه الدراسة إلى توضيح أهمية بناء القدرات الوطنية المؤهلة للأمن السيبراني والتي يتم الاعتماد عليها في مواجهة الهجمات السيبرانية بنجاح، وأهمية رسم إستراتيجية وطنية للأمن السيبراني تستطيع حماية البنية التكنولوجية الرقمية، والبنية التحتية للدولة، وتواجه بعض الدول وبخاصة النامية منها عددًا من التحديات التي تتعلق بالقدرة على التصدي للهجمات السيبرانية مما يعطل أسباب التنمية للدولة. وأوضحت الدراسة ستة أبعاد يعتمد عليها بناء الإستراتيجية الوطنية للأمن السيبراني، وهى: (صياغة أهداف البرنامج، والتوعية، والتعاون وتكامل الأدوار بين الصناعة والجامعة، وتصميم منهج مناسب لتدريس الأمن السيبراني، وخرجت الدراسة بتوصية لتطوير التأمين السيبراني لأنه أصبح من التحديات الآنية والتي تحتاج إلى مزيد من الوقت لدراستها.

**5 . «الأسباب الطارئة لتضمين مفاهيم الأمن السيبراني لمؤسسات التعليم العالي» (Ma-ranga. & Nelson .2019)**

هدفت هذه الدراسة إلى تعرف طرق تأمين الجامعات من الهجمات السيبرانية ، وما تقوم به 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 ومفاهيم الأمن السيبراني، وإمداد إدارة الجامعات بأدوات الحماية الرقمية.

**6 . «وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم» ( الصانع، وآخرون، 2020)**

هدفت هذه الدراسة إلى تحديد درجة وعي المعلمين بالأمن السيبراني بمدينة الطائف بالمملكة العربية السعودية من وجهة نظرهم، وتحديد درجة استخدام المعلمين لأساليب

وإستراتيجيات حماية الطلبة من مخاطر الإنترنت من وجهة نظرهم، ومعرفة العلاقة الارتباطية بين وعي المعلمين بالأمن السيبراني واستخدامهم لأساليب وإستراتيجيات حماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية لديهم في مدينة الطائف، وفي إطار ذلك أوضحت الدراسة ماهية الأمن السيبراني، ومجالات استخدامه، وأساليب حماية الطلبة من مخاطر الإنترنت، وتعزيز القيم والهوية الوطنية، وقد توصلت الدراسة إلى ضرورة نشر ثقافة الوعي بالأمن السيبراني بين معلمي جميع المراحل الدراسية العامة للتوعية بمخاطر الإنترنت بمختلف أنواعها، وأهمية إعداد برامج تقنية تهدف إلى تدريب المعلمين على أساليب الحماية، وتضمين قيم المواطنة والهوية الوطنية في جميع المقررات والمناهج في كافة المراحل الدراسية، مع ضرورة توظيف المصطلحات التي تخدم كل فئة عمرية.

**التعليق على الدراسات السابقة**

- استفادت الدراسة الحالية من الدراسات السابقة في إعداد الإطار النظري للدراسة المتعلق بمفهوم التحول الرقمي، وأيضًا مفهوم الأمن السيبراني، كما استفادت في توضيح رؤية التصور المقترح.
- واتفقت الدراسة الحالية مع الدراسات السابقة في التأكيد على أهمية التحول الرقمي للجامعات للتوافق مع الثورة التكنولوجية.
- كما اتفقت الدراسة الحالية مع الدراسات السابقة في التأكيد على ضرورة توفير متطلبات أمنية لسياسات الأمن السيبراني من خلال التدريب والتوعية والبرامج التعليمية لحماية البيئة الرقمية للجامعات، وبالتالي تعزيز التحول الرقمي في مصر.
- بينما تختلف الدراسة الحالية عن الدراسات السابقة في وضع رؤية مقترحة لاستخدام سياسات الأمن السيبراني في الجامعات المصرية للتمكن من حماية خطوات تطبيق التحول الرقمي في مصر، الأمر الذي لم تتعرض له الدراسات السابقة.

**ثانيًا: الإطار النظري للدراسة**

ستوضح الدراسة مفهوم التحول الرقمي للجامعات والأمن السيبراني كما يلي:

**المحور الأول: التحول 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 التحول الرقمي ومميزاته ومتطلبات تطبيقه من خلال العرض التالي:

**1 . مفهوم التحول الرقمي للجامعات**

يعني التحول الرقمي للجامعات: "عملية التحول الرقمي باستخدام التكنولوجيا الرقمية في الجامعات حتى تمتلك القدرة على التواجد في عصر الثورة التكنولوجية (Brothers & Spies. 2017.12)، وثمة رؤية أخرى لهذا المفهوم ، وهى أنه: إعادة هيكلة إدارة الجامعة وبيئتها التعليمية وتعلم الطلاب وجميع الخدمات الجامعية بطريقة رقمية أو تقنية مما يؤدي إلى زيادة كفاءة أداء الجامعات"( Viire Taks. Lady .(Tomas & Kleinheyer .2019.5

بينما توضح دراسة أخرى أن التحول الرقمي للجامعة هو: "الانتقال من نظام تقليدي إلى نظام رقمي قائم على تكنولوجيا المعلومات والاتصالات في جميع مجالات العمل الجامعي في ضوء مجموعة من المتطلبات المتمثلة في وضع إستراتيجية للتحول الرقمي، ونشر ثقافة التحول الرقمي، وتصميم البرامج التعليمية الرقمية، وإدارة تمويل التحول الرقمي، بالإضافة إلى المتطلبات البشرية والتقنية والأمنية والتشريعية". (أمين، 2018، 5).

ويشير( البار، 2019، 3) إلى أن تقنيات التحول الرقمي عبارة عن " تزايد قطاع تقنية المعلومات فيما يخص الأجهزة والتطبيقات وزيادة الإنتاجية بشرط ألا تتعرض هذه التقنيات لأي خلل، وأن تمتلك القدرة على التنافس في الأسواق ".

ويعرف (الدهشان، والسيد، 2020، 1260) التحول الرقمي للجامعات بأنه: "عملية انتقال الجامعات التقليدية إلى جامعات رقمية من خلال الاستخدام المكثف لتكنولوجيا

المعلومات والاتصالات داخل الجامعة، واستبدال العناصر والعمليات المادية بأخرى افتراضية، وتقديم كافة خدماتها بصورة إلكترونية لزيادة قدرتها على الاستجابة للمتغيرات الخارجية المعاصرة".

وثمة تعريف آخر لمفهوم التحول الرقمي للجامعات، وهو أنه: "انتقال المؤسسة من التعامل التقليدي ومن الموارد المادية إلى التعامل التكنولوجي المعتمد على الإنترنت والاستخدام الواسع لتكنولوجيا المعلومات والاتصالات في ضوء الاستجابة لمتغيرات البيئة الخارجية" (Schallmo & Williams .2018.6).

يتضح مما سبق أن انتقال الجامعات التقليديه إلى جامعات الرقمية يستلزم الاستخدام المكثف للتكنواوجيات الرقمية سواء في آلية التواصل أو التعليم عن بعد، منتجة بذلك بيانات ومعلومات ذات أهمية كبيرة عن طريق البنية التحتية الخاصة بها.

**2 . المبررات التي تدعو إلى التحول الرقمي**

**أصبحت الضرورة ملحة لتحول الجامعات رقميًّا، ويعود ذلك بشكل أساسي إلى عدد من المبررات، وهى:**

**أ.الثورة المعرفية**: فقد أدت الثورة المعرفية إلى وجود فجوة رقمية بين الدول الغنية والدول الفقيرة، وعملت على تغيير مسار الأداء التقليدي للعديد من مؤسسات المجتمع بما فيها المؤسسات التعليمية لمواكبة تلك التطورات واستثمار الإمكانات الاقتصادية والمادية التي تمتلكها لتطوير التعليم وبنيته التحتية والتغلب على تحديات المرحلة المعاصرة (أمين، 2018، 47).

**ب- الثورة الرقمية**: وهى تتمثل في جميع الأجهزة الرقمية المحيطة بنا، بالإضافة إلى الكتب الرقمية، والمقالات الإلكترونية، مما يدل على سيطرة الوسائل الرقمية الحديثة على غيرها في مجال الاتصال ومعالجة تبادل المعلومات، ويتسم العصر الرقمي بمزايا الوسائل الرقمية المستخدمة، وهى السرعة، والدقة، وتقريب المسافات، وإلغاء الحدود، ما يؤثر على التعلم الرقمي وإضافة التفاعلية لطرق التدريس وتلبية جميع حاجات المتعلمين (EFimov .and laptreva . 2018.1927)

ج- **تحسين كفاءة الأداء**: أصبح التحول الرقمي من الضروريات بالنسبة لكافة المؤسسات والهيئات التي تسعى إلى التطوير وتحسين خدماتها وتسهيل وصولها للمستفيدين، ولا يعني التحول الرقمي فقط تطبيق التكنولوجيا داخل المؤسسة، بل هو برنامج شامل كامل للمؤسسة، وطريقة وأسلوب عملها داخليًّا، كما أنه يشمل أيضًا كيفية تقديم الخدمات للجمهور المستهدف لجعل الخدمات تتم بشكل أسهل وأسرع، ويهتم التحول الرقمي بكيفية استخدام التكنولوجيا داخل المؤسسات مما يساعد على تحسين الكفاءة التشغيلية وتحسين الخدمات التي يتم تقديمها وتسهيل الحصول عليها بما يضمن توفير الوقت والجهد معًا(البار،2019 ،3).

د- **احتياجات المهارات الرقمية المتغيرة لسوق العمل**: ستؤثر اختراقات التكنولوجيا الرئيسية في السنوات العشر القادمة على أشكال العمل وهيكل أسواق العمل، فضلًا عن جوانب أخرى من الحياة؛ مثل: التعليم والصحة والزراعة، ومن منظور تنمية المهارات من المتوقع أن تكون آثار التغيير التكنولوجي عميقة لتعليم ورفع مهارات تعليم الشباب والأطفال، وتعد تنمية القدرات من أجل توقع الاحتياجات المتغيرة للمهارات الرقمية في العمل والحياة أمرًا حاسمًا بالنسبة لجميع البلدان، وينبغي توجيه الجامعات إلى ابتكار وتوفير مهارات للوظائف في الاقتصاد الرقمي من خلال تعزيز القدرات المؤسسية والكفاءات الرقمية للمعلمين والطلاب، وسد الفجوة في توفير هذه المهارات بين المؤسسات النظامية وغير النظامية، وتعزيز مبادرات تنمية القدرات، وإقامة علاقات مع أصحاب العمل، وضمان القدرة على تحمل التكاليف وتوافرها والاستفادة من تكنولوجيا الأدوات والأجهزة الرقمية (اليونسكو 2018، 4.5).

هـ- **ضعف تمويل الجامعات**: تتفاقم مشاكل ومعوقات التمويل لمواجهة النمو السكاني وما يترتب عليه بالضرورة من زيادة الطلب على التعليم العالي، وتؤثر هذه المشاكل على قدرة الدولة على الاستجابة لرغبة المواطنين في الانخراط في التعليم الجامعي في مناطق يصعب في العادة إنشاء جامعات فيها أو يصعب على أهلها الانتقال منها إلى الجامعات البعيدة عنهم سواء في الداخل أو في الخارج، ويؤدي إنشاء البنية

التحتية الرقمية إلى تحقيق مزايا هامة تتمثل في خفض تكاليف التعليم الجامعي على الطالب، خاصة تكاليف المعيشة والمواصلات وخلافه، مما يتيح فرصة لأكبر عدد من الطلاب من مختلف قطاعات المجتمع للاستفادة من التعليم العالي، كما أنه من المتوقع أن يؤدي إنشاء البنية التحتية الرقمية إلى خفض التكاليف مقارنةً بتكاليف التعليم التقليدي التي تتزايد مع زيادة الطلبة المنتظمين نتيجة التوسع في المباني والمرافق والزيادة في أعضاء هيئة التدريس والموظفين الإداريين (معهد البحوث والاستشارات، 1426هـ، 17)

**3 . خطوات تطبيق التحول الرقمي**

حتى يسير تطبيق التحول الرقمي بصورة ناجحة ينبغي اتباع سبع خطوات حددتها دراسة ( Arakan.2016. 1–8):

- **الخطوة الأولى**: قيادة واضحة: حيث ينبغي التخطيط لإستراتيجية رقمية شاملة وفق الإمكانات الرقمية المتاحة، ومعرفة جوانب القوة والضعف في تلك الإستراتيجية.
- **الخطوة الثانية**: تغيير الثقافة السائدة من خلال إدارة قوية، ويتوفر ذلك من خلال التدريب والتحفيز لجميع العاملين على تطوير مهاراتهم الرقمية لبناء إدارة رقمية قوية.
- **الخطوة الثالثة**: التواصل مع جميع المحيطين بالإدارة: حيث ينبغي تشكيل الطريقة التي يتواصل بها الأفراد بأسلوب يعتمد على التقنيات الرقمية المتاحة لتسهيل القدرة على التخطيط المستمر لتخطي المعوقات.
- **الخطوة الرابعة**: التكيف مع الثقافة المعلوماتية: فمن الضروري إيجاد فرص مختلفة لتقديم خدمات مبتكرة وإبداعية باستخدام منظومة من الأجهزة والبيانات الرقمية، والتخزين والبرمجيات التي تعمل ضمن بيئات تقنية.
- **الخطوة الخامسة**: التجريب السريع: أي القدرة على الانتشار والتوسع للوصول إلى أكبر عدد من المستفيدين، وتحديد المتطلبات لخطط الاستثمار.

- **الخطوة السادسة**: التفكير بريادة وفاعلية بحيث تصبح البيئة حاضنة للتكنولوجيا المتطورة وتستطيع التعامل الرقمي بطلاقة وتضمن العديد من الأسس والمقومات الرقمية.
- **الخطوة السابعة**: من المنافسون؟ حيث يتم تحليل البيئة الخارجية قبل القيام بأي عملية للتحول الرقمي ومعرفة من ينافس في هذه البيئة، وتضمن دراسة المنافسين والتطورات التكنولوجية والتغيرات السريعة لها تجميع المعلومات الأساسية لنجاح عملية التحول الرقمي.

ويتبين لنا من خلال ما سبق أن التحول الرقمي للجامعات لا يعتمد على التجهيزات الرقمية بقدر اعتماده على ما يصاحب هذه التقنيات من ترسيخ للثقافة الرقمية وإعداد للكوادر المؤهلة والمهارات الرقمية التي تفعل التحول الرقمي. ولبناء رؤية رقمية واضحة وصياغة إستراتيجية للتطوير الرقمي ينبغي تكوين صورة كاملة عن واقع تكنولوجيا المعلومات والاتصالات بما يساعد على تطوير مكانتها المستقبلية، ويتضمن ذلك الإجراءات التالية (علام، 2020، 205):

**أ- تحليل الفجوة الرقمية**: ويتم ذلك من خلال الهوة الفاصلة بين ما تملكه المؤسسة التعليمية كمنظمة من معرفة وأدوات يمكن استغلالها وما لديها من قدرات على النفاذ إلى مصادر المعلومات والمعرفة من ناحية، وبين ما لا تملكه وتحتاجه أدواتها وليس لديها القدرة على استغلاله من ناحية أخرى.

**ب- تحليل المستوى التكنولوجي**: ويتم ذلك من خلال تحليل مستوى التقدم التكنولوجي في أداء الأعمال داخل المؤسسة التعليمية كمنظمة، وتحديد درجة الاستفادة من التكنولوجيا المتاحة، والمقارنة بين التكلفة والعائد، وتقييم مدى استخدام التكنولوجيا المتاحة، ومعرفة مدى فعالية التكنولوجيا المستخدمة في المنظمة.

**ج- تحديد كفاءة نظم المعلومات**: حيث تعد المعلومات هى الأساس الحيوي للمنظمات الرقمية، ومن ثم فإن التحـول الرقمي للمؤسسة التعليمية يجـــب أن يتضمن تحـــليل العناصر التالية: إنتاج المعلومات ، عرض وتداول المعلومات ، حفظ وتحديث واسترجاع المعلومات.

**د- معرفة مدى الاستعداد للتحول الإلكتروني لدى المنظمة، والذي يمكن أن يُقاس من خلال خمسة عناصر رئيسة**، هى: البنية التحتية، والقيادة الإلكترونية، ورأس المال البشري، وأمن وخصوصية المعلومات، وبيئة العمل الافتراضية.

**4 . فوائد التحول الرقمي**

يتميز التحول الرقمي بالعديد من المزايا التي تعود على الجامعة والمعلم والمتعلم، ويمكن توضيح عددا من هذه المزايا ( Rof. Bikfalvi & Marques. 2020.7):

- سيصبح المعلم عنصرًا ذاتيًّا للمعرفة، وسيواصل توجيه طلابه.
- توفير التكلفة والجهد المبذول للجامعة التقليدية.
- تحسين كفاءة الأداء.
- القدرة على الانتشار الأكبر.

وقد أضاف ترينـد (Jonsen .2019 . 15 – 17) بعض الفوائد الأخرى كما يلي:

- تعزيز المهارات الرقمية، بالإضافة إلى تعزيز التعلم الذاتي للمتعلم.
- القدرة على إدارة الوقت بطريقة أكثر فاعلية.
- تسهيل التكامل بين وظائف خدمات الجامعة، وأداء ذلك بطريقة مبتكرة.
- تحسين جوانب متعددة للجودة، بالإضافة إلى تحسين رضا المستفيد، ويعد التحول الرقمي أحد حلول ضمان استمرارية التعلم خلال فترات الأزمات والأوبئة المرضية كالذي مرت به الجامعات خلال جائحة كورونا ( Covid -19)، وما حدث من إجراءات التعليق الكامل أو الجزئي للدراسة.
- دعم جودة العملية التعليمية الرقمية، وتطبيق أنماط غير تقليدية لأساليب التعلم والتعليم.

**5 . متطلبات التحول الرقمي**

يحتاج تطبيق التحول الرقمي بالجامعات إلى عدد من المتطلبات التي تتنوع لتشمل متطلبات إدارية، ومتطلبات تقنية، ومتطلبات تعليمية، ومتطلبات الموارد البشرية، ومتطلبات تشريعية، ويمكن تفصيل ذلك كما يلي:

**أ- متطلبات إدارية:**

وهى تتمثل في بناء الإدارة الرقمية والتي تساعد على تبسيط العمليات الإدارية باستخدام أحدث البرامج الرقمية على شبكة الإنترنت، وتبسيط الإجراءات، وتقليل استخدام الورق إلى أقل ما يمكن، وتمنح الإدارة الرقمية مجموعة من المزايا لتسهيل التواصل الرقمي، مثل: تجميع البيانات والمعلومات، وبالتالي سهولة صنع القرار واتخاذه، وتوفير الخدمات الرقمية، والقدرة على زيادة مجالات التعاون بين العاملين وبين الإدارة والمستفيدين، ويشمل ذلك أيضًا وضع قواعد البيانات الرقمية لسهولة الوصول إلى المعلومات وإمكانية تخزين مستودعات البيانات الرقمية ( Andersson. et al. 2018. 18 –20 )

**ب- متطلبات البنية التحتية:**

تعد البنية التحتية الرقمية ضرورة لتوفير شبكات رقمية للتواصل بالسرعة المطلوبة واللازمة لدعم الوظائف والخدمات الضرورية، ولذلك يجب أن يتم توضيح متطلبات السرعة والتكنولوجيا والتغطية، وتتمثل هذه البنية في الأجهزة المادية المستخدمة لربط الكمبيوتر والمستخدمين، ووجود خادم (سرفر) جيد ليتمكن المستخدم من القيام بمهامه بشكل قوي وسريع، والقدرة على حفظ وتبادل المعلومات والبيانات من خلال هذه الشبكة الرقمية، ويلعب الإنترنت دورًا هامًّا في البنية التحتية لتكنولوجيا المعلومات الجديدة، وتتيح هذه البنية الرقمية للمتعلمين حلولًا مبتكرة ومتنوعة تناسب احتياجاتهم المختلفة. وتسهل البنية التحتية الرقمية تطوير وتوفير واستخدام وتبادل النظم الرقمية (المنتجات والخدمات)، وتشمل هذه البنية شبكات الاتصالات الثابتة واللاسكية بما في ذلك الشبكات فائقة السرعة، وشبكات الألياف البصرية الأرضية، وخطوط الألياف عبر خطوط الكهرباء، والاتصال بالأقمار الصناعية، والاتصالات المتنقلة، والبث الأرضي الرقمي، ومراكز البيانات، ومراكز الاتصالات، والأجهزة الرقمية والذكية، وكذلك الأجهزة والمنصات الرقمية (Microstratgy.2016.1–13).

تعد البنية الرقمية الميسورة التكلفة والسهلة المنال والموثوقة هى الأساس لتحقيق تحوُّل رقمي شامل، وتعد المنصات الرقمية أيضًا عنصرًا أساسيًّا في البنية التحتية الرقمية

(الاتحاد الأفريقي2030–2020، 8 ، 9)، وعليه فإن البنية التحتية تعد الهيكل التنظيمي لتشغيل الخدمات اللازمة للجامعات، وهذه هى الخطوة الأساسية التي تدعم الهيكل الكلي للتطوير وتسهل الخدمات الاجتماعية.

ولتوفير الدعم الفني للعملية التعليمية تشمل هذه البنية شبكة الربط الإلكتروني التي تصل الجامعات بعضها بعضًا، والهيكلية التي ستقدم عليها الشبكة والتي تحدد أجهزة الربط الإلكتروني وأجهزة الحاسوب التي تستخدم للاتصال والتصفح، ومن ثم البرمجيات التي ستوفر التطبيقات التعليمية التي ستسهل التعامل مع المحتوى التعليمي مثل: (نور الدين والعتيبي، 2020، –129 130)

- الشبكات والتي من المفروض أن تكون ذات تدفق عالٍ لضمان سرعة تنزيل المناهج والتطبيقات وتبادل البيانات في التعليم التفاعلي.
- الهيكلة تعتمد في الأساس على مركزية البيانات المعالجة من خلال استخدام أجهزة خوادم عالية القدرة الحسابية والسعة التخزينية وأجهزة حاسوب طرفية، وهذا النوع من الأنظمة يتطلب استثمارًا مبدئيًّا كبيرًا في إنشاء شبكة تعليمية عالية السعة، إلا أنه يثبت فاعلية وجدوى اقتصادية على المدى البعيد.
- البرمجيات التعليمية التي توفر تطبيقات لإدارة التعليم وإدارة المحتوى الإلكتروني وأنظمة التحكم والسيطرة والمتابعة للشبكة.

**ج- الكوادر البشرية المؤهلة:**

للوصول إلى التحول الرقمي المتكامل فإن الاقتصار على توفير الأجهزة والتقنيات يعد أمرًا غير كافٍ، حيث يستوجب هذا الوصول توافر الكفاءات والكوادر البشرية المؤهلة القادرة على متابعة سير المعلومات والبيانات، والقدرة على التعامل مع التقنيات التكنولوجية، وينبغي عدم إغفال الدور الهام لإستراتيجية التغيير لتجنب التشتت والفوضى وضياع الجهود المبذولة (Higher Education Authority.2019.1.2)، وتتمثل الأولوية في هذا الصدد في تطبيق إصلاح تنظيمي يؤدي إلى تحسين بيئة ممارسة أنشطة الأعمال التقليدية، حيث يعمل التحول التكنولوجي على أتمتة الكثير

من المهام الروتينية، وسيؤدي الإنترنت أيضًا إلى الاستغناء عن الكثير من المهام التي يؤديها الموظفون والإداريون أصحاب الياقات البيضاء، ويضفي هذا أهمية على مختلف أنواع المهارات التي تكملها الأتمتة ولا تحل محلها، ولهذا سيضطر العمال إلى تطوير مهاراتهم في الغالب طوال حياتهم الوظيفية (البنك الدولي، 2016، 32).

**د- المتطلبات التعليمية:**

يستلزم الدارس الإلكتروني تعرف حقوقه وواجباته وتوعيته بمسؤولياته تجاه المجتمع الإلكتروني، حيث لا يصبح التعلم الإليكتروني مطلبًا أساسيًا للتكيف مع مجتمع إليكتروني فقط ولكن يصبح مطلب أساسيًا أيضًا لتحقيق شعور المواطن بالأمن المعلوماتي والحصول على محتوى معلوماتي من مصدر موثوق بها وسهل الوصول إليها وييسر تعاملاته وعلاقاته مع الآخرين المحيطين به، وأوصت ( جمال الدين، 2009، 17) بما يلي:

- أن يتم تبني وثيقة حقوق وواجبات وواجبات الدارس الإليكتروني في الجامعات والمدارس والمكتبات ولكن بعد تكييفها وفقًا لظروف المؤسسات والمجتمع ويتم البدء الفوري باستخدامها في البرامج التي تقدم إليكترونيًا للحاجة الماسة إليها.
- تدريس مقرر للثقافة الإلكترونية والقانونية بالمدارس والجامعات وبشكل خاص في كليات التربية ومؤسسات إعداد المعلم، ويمكن أن يدور هذا المقرر حول أهمية كل من التربية والثقافة القانونية الإلكترونية وتحديد العلاقة بينها وأثر كل منها في الآخر ودور مؤسسات التربية المباشر وغير المباشر في نشر الثقافة القانونية الإليكترونية وتوعية الطلاب وأعضاء هيئة التدريس والعاملين بالمؤسسات التعليمية وأفراد المجتمع ككل، على أن يتم تدريس هذا المقرر من خلال الشبكة العالمية للمعلومات والتوعية بمفاهيم ومضامين الثقافة الإلكترونية ودورها في استتباب الأمن المعلوماتي.

**هـ- المتطلبات الأمنية:**

نظرًا لاعتماد التحول الرقمي على شبكات الإنترنت ولأهمية المعلومات والبيانات التي تنتقل على تلك الشبكات يعد توفير الأساليب والإجراءات الأمنية من الأمور بالغة

الأهمية التي تساعد على حماية المعلومات والبيانات من الاختراق في ضوء الثورة التكنولوجية وازدياد شبكات الاتصالات والمعلومات، وبخاصة بعد انتشار عديد من محاولات اختراق منظومات الحواسيب بغرض سرقة أو تدمير المعلومات، ولتحقيق ذلك لابد من مراعاة ما يلي (أمين، 2018، 100، 101):

- وضع آليات الرقابة والمتابعة لنظم المعلومات والشبكات والأجهزة.
- وضع قواعد لتخزين واستخدام البيانات والمعلومات بشكل آمن.
- وضع القواعد المنظمة التي تحد من السرقات أو السطو الإلكتروني وانتهاكات خصوصة المعلومات في التحول الرقمي.
- وضع إستراتيجية لأمن المعلومات تضمن التعاون بين القطاعين العام والخاص.
- وضع نظام للتحكم في خصوصية البيانات والمعلومات وجودتها وتكاملها.

**و- المتطلبات التشريعية:**

من الضروري توافر قوانين وتشريعات تتواءم مع التحول الرقمي وتلازم تطبيقه، ويستلزم الأمر:

- وضع تشريعات تسهل إجراءات التحول الرقمي.
- وضع تشريعات تسمح بالاعتراف بمؤهلات البرامج الرقمية.
- توفير الضمانات القانونية والتشريعية اللازمة لنشأة الجامعة الرقمية.

فتوفير الإطار التشريعي اللازم لتأمين المعاملات الرقمية وحماية البيانات المتصلة بالجامعة والمستفيدين يساعد على إيجاد حث مناسب للمشاركة الفعالة لدى جميع الأطراف المعنية من أفراد ومؤسسات مجتمعية (الدهشان والسيد، 2020، 1273).

**ز- متطلبات تقنية:**

نتيجةً لاستخدام التكنولوجيات المتقدمة ظهرت فرص جديدة تتطلب إعادة اكتساب مهارات رقمية جديدة، بالإضافة إلى تهديدات الفيروسات والقرصنة والاختراقات المنتشرة على أجهزة الحاسوب، وضعف الدراية بوسائل الأمن وحماية المعلومات

على الحاسوب بما يمنع الوصول غير المشروع للبيانات والمعلومات – وهو ما يعرف بالأمن السيبراني – ويزداد الاحتياج إلى سياسات الأمن السيبراني كلما ازداد استخدام التكنولوجيا بشكل أكبر في حياة الأفراد، وبالتالي فإنه من الضروري زيادة التأكيد على وعي الأفراد بالأمن السيبراني (Australian Computer Society . 2016. 7 .8) ، وتعد الاستفادة من الضوابط الأمنية مطلبًا هامًّا مهما لتعزيز العملية التعليمية داخل الجامعات.

**6 . معوقات التحول الرقمي للجامعات**

تؤثر العديد من العوامل على تطبيق التحول الرقمي في التعليم الجامعي، ومنها معوقات داخل الجامعة، وبعضها خارجها، يمكن توضيح ذلك كما يلي:

**أ- المعوقات الداخلية**

- **الجوانب المادية**: وتتمثل في غياب الرؤية الإستراتيجية الرقمية الواضحة للجامعات، والافتقار إلى الدعم والتخطيط الإداري والقانوني للجامعة، وإهمال المتابعة والتقييم المستمر لخطوات التحول الرقمي (Boneva . 2018. 107)
- **البنية التحتية الرقمية**: إن الحائل الأساسي لإنشاء البنية التحتية في الدول النامية هو القصور في الاستثمار المتوفر، وتبدو هذه الإشكالية بشكل أكثر حدةً في المناطق الريفية التي تتدنى فيها الخدمات، ولهذا فإن المطلوب هو إيجاد طريقة قائمة في الأساس على الاستخدام والخدمات؛ حيث لا تعتبر التقنية غاية في ذاتها، ولكنها مجرد أداة (مركز الدراسات الإستراتيجية، 2020، 63).
- **الجوانب البشرية**: يمثل نقص الكفاءات القادرة على قيادة خطوات التحول الرقمي داخل المؤسسة أحد المعوقات التي تحول دون الوصول إلى التطبيق الرقمي الصحيح للإدارة، فهذا النقص في الكفاءات يؤدي إلى صعوبة الحصول على الخدمة أو على المعرفة بسرعة، كما يؤدي إلى ضعف المحتوى الرقمي المقدم، والعزوف عن التدريبات الموجهة من إدارة الجامعة، أو عدم الرغبة في تغيير الثقافة التنظيمية السائدة (Schallmo & Williams . 2018 . 7).

**ب- المعوقات الخارجية:**

- **التطوير التكنولوجي**: تمثل الفجوة الرقمية في الدول منخفضة الدخل عائقًا أمام تطبيق التحول الرقمي في الجامعات والتعليم عمومًا. حيث تؤدي هذه الفجوة إلى التفاوت في الوصول إلى الشبكات وفي القدرة على مواكبة وملاحقة التقنيات التكنولوجية العديدة المتسارعة والمتقدمة، وفي القدرة على متابعة سير التعليم عن بعد، بالإضافة إلى صعوبة التعامل مع تكنولوجيا التعليم ( David.Pellini&Jordan 2020. 3–5)
- **مهارات سوق العمل**: تؤدي التكنولوجيا المتقدمة إلى أتمتة بعض الوظائف لتحل محل العاملين، لكنَّ ثمة مهامَّ ومهنًا جديدة ستتاح للإنسان، وستبرز الحاجة إلى وظائف تحليلية يقوم بها، مما يقود إلى مشكلة التطوير في النظم التعليمية الرقمية باستمرار، وقد أكدت منظمة الإسكوا (لجنة الأمم المتحدة الاقتصادية والاجتماعية لغرب آسيا) على ضرورة إجراء إصلاحات في قطاع التعليم تزود الأطفال والشباب من جميع الفئات العمرية بالمهارات التي يتطلبها الاقتصاد الحديث (الإسكوا ، 2018، 8).

**7 . حوكمة التحول الرقمي**

أدى التطور السريع وازدياد حجم المعلومات إلى تعقيد عملية التحكم والإفادة من التطبيقات التي انتشرت في شتى مجالات العمل وعلى جميع المستويات بصورة لا غنى عنها لتحقيق التقدم وأداء الأعمال بفعالية وكفاءة، ولا يخفى ما رافق هذا التقدم والانتشار الواسع للتقنية من بعض المخاطر والتهديدات، فظهرت ضرورة الترابط بين التقنية والحوكمة والأعمال، وتم تحديد هذا المصطلح إلى حوكمة التحول الرقمي وإدارة المخاطر وهيكلة العمليات والإجراءات والتصميم التقني( Rof. Bikfalvi & Marques. 2020.13).

وقد برزت هذه المصطلحات بصورة هامة متوافقة مع إستراتيجيات المؤسسات للتطوير والحد من المخاطر؛ حيث تساعد الحوكمة في ضبط منظومة المحيط التفاعلي المرتبطة مع التحول الرقمي؛ حيث تتشابك مجموعة مركبة من المكونات الخاصة

والفرعية؛ مثل: الشركات المساندة، وأنظمة الأعمال، والوسائط التفاعلية بشكل مباشر أو غير مباشر لاستكمال العمليات والإجراءات، وبهذا تشكل حوكمة التحول الرقمي طريقًا واضحًا لتسهيل الأعمال بشكل يواكب التطور(البار،2019، 5).

وعلى ذلك يتواءم التحول الرقمي للجامعات مع توجهات التحول الرقمي للحكومة مما يؤدي إلى تسهيل عملها وتيسير إجراءات التحول الرقمي لها، ما يجعل جميع مؤسسات الدولة في تكامل رقمي مع بعضها.

**8 . 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 300 بتاريخ 2003/ 3/ 13 ، ويتم متابعة تطوير وقياس أداء مؤسسات التعليم العالي في مصر من خلال عدد من المشروعات، منها: مشروع تطوير نظم تكنولوجيا المعلومات، وهو يهدف إلى:

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

**أ- مشروع تطوير البنية الأساسية لشبكة المعلومات:**

- تحديث وتطوير شبكة المعلومات الجامعية بحيث يمكن لجميع كليات ومعاهد الجامعة الاتصال بالإنترنت من خلال خطوط اتصال سريعة وآمنة.

- إعداد وتدريب فريق عمل قادر على إدارة شبكة معلومات الجامعة.
- توفير نظام حماية لشبكة الجامعة.
- تطوير خدمة البريد الإلكتروني.

**ب- مشروع البوابة الإلكترونية:**

البوابة الإلكترونية هى الجامعة التي من خلالها يستطيع أي زائر للبوابة الإلكترونية من داخل أو خارج الجامعة التعرف والاستفادة من الخدمات المقدمة على البوابة، كما يمكن من خلالها توظيف أفضل التقنيات والبرمجيات المتوفرة لزيادة التعاون والتواصل بين مختلف الكليات بالجامعة وبين الجامعات بعضها بعضًا، وتعمل وزارة التعليم العالي على توفير الدعم المالي والفني للبوابة الإلكترونية بما يكفل الوصول إلى أعلى مستويات الأداء.

**ج- مشروع نظم المعلومات الإدارية:**

تضع وزارة التعليم العالي ضمن أولوياتها العاجلة إدخال وتطوير تكنولوجيا المعلومات والاتصالات في منظومة التعليم العالي، ويتضح ذلك من خلال المحور الثالث من منظومة التعليم العالي في مصر المستقبل والذي يختص باستخدام تقنيات المعلومات والاتصالات لرفع القدرة التعليمية والبحثية والإدارية لمنظومة التعليم العالي والبحث العلمي.

- التطوير المستمر للبرامج العلمية والتدريبية والمناهج الدراسية وطرق تدريسها.
- استحداث أنماط جديدة من التعليم تتواكب مع التطور العالي وتستجيب للطلب المتزايد على التعليم العالي.

**د- مشروع التعليم الإلكتروني:**

**يهدف هذا المشروع إلى:**

- إنشاء مراكز للتعليم الإلكتروني داخل كل جامعة.
- إتاحة المقررات الإلكترونية للطلاب لرفع مستواهم العلمي وإتاحة التفاعلية بينهم.

- توفير بيئة تعليمية مرنة بها إستراتيجيات تعتمد على استخدام أساليب التدريس بشكل حديث.
- تشكيل بيئة إلكترونية تساهم في دعم القرارات وسرعة إنجاز المعاملات الإدارية .
- الاستغلال الأمثل للبيئة التحتية (الشبكة).
- توفير مجتمع إلكتروني تتواصل فيه أطراف العملية التعليمية عبر المنتديات والبريد الإلكتروني دون حاجز للوقت والمكان.

**هـ- مشروع المكتبة الرقمية:**

**يهدف هذا المشروع إلى:**

- ميكنة إجراءات العمل في المكتبات.
- ربط مكتبات الجامعة ببعضها من خلال شبكة الجامعات المصرية.
- البدء في فهرسة موحدة لمقتنيات المكتبة.

**و- مشروع التدريب على تكنولوجيا المعلومات والاتصالات:**

تم إطلاق هذا المشروع في إطار بناء قدرات أعضاء هيئة التدريس والإداريين والطلاب بالجامعة على استخدام تكنولوجيا المعلومات والاتصالات الحديثة من خلال تقديم خدمات التدريب، و يهدف إلى:

- رفع كفاءة استخدام نظم المعلومات والموارد التكنولوجية المتاحة بالجامعة.
- رفع معدل الاستفادة من مصادر المعلومات الإلكترونية والمحتوى الرقمي بالجامعة.

وفي إطار توجه وزارة التعليم العالي نحو التحول الرقمي للجامعات المصرية جاء في إستراتيجيتها (2018) الإشارة إلى خطة شاملة لتدريب جميع العاملين في الجامعات المصرية على برامج رقمية تستهدف القدرة على التحول الرقمي للبنية التحتية بالجامعات، وضرورة الحصول على شهادة أساسيات التحول الرقمي من وزارة التعليم العالي والبحث العلمي (89) ، بالإضافة إلى مبادرة أطلقتها وزارة التعليم العالي والبحث العلمي في مصر عن مسابقة لأفضل جامعة في مجال التحول الرقمي بين الجامعات

المصرية ، وذلك في إطار التوجيهات الرئاسية للعام الدراسي 2020/ 2019، وقد تم إعلان نتيجة المسابقة، حيث حصلت جامعة المنصورة على المركز الأول، وجاءت جامعة جنوب الوادي في المركز الثاني، وحصلت جامعة المنيا على المركز الثاني مكرر.

وبالنسبة لجائزة أفضل جامعة على مستوى الاستعداد للعام الدراسي حصلت جامعة دمياط على المركز الأول، وجاءت جامعة المنصورة في المركز الثاني، وجامعة طنطا في المركز الثاني مكرر.

**المنصة الرقمية لوزارة التعليم العالي للعام الجامعي 2021/ 2020**

**https: / /egypt-hub.edu.eg**

- تم إطلاق منصة لجميع الجامعات المصرية للتعلم عن بعد، وهى تمثل نقلة حقيقية للتحول الرقمي للمنظومة التعليمية تماشيًا مع إستراتيجية الدولة.
- إنشاء بوابة رقمية موحدة للجامعات المصرية للتواصل بين أعضاء هيئة التدريس والطلبة أثناء العملية التعليمية تهدف إلى ما يلي:
  - التوسع في نشر المحتوى التفاعلي.
  - تفعيل التواصل بين أعضاء هيئة التدريس والباحثين والطلبة.
  - تقديم الخدمات إلكترونيًّا للمجتمع الجامعي.

**وتقدم المنصة الرقمية لأعضاء هيئة التدريس الفرصة لعدد من المهام التالية:**

- نشر المحتويات التعليمية ليستفيد منها سائر الطلبة.
- إمكانية نشر المحاضرات رقميًّا مباشرة.
- التدريب الرقمي من أجل تمكين أعضاء هيئة التدريس من مهارات التقنيات الرقمية.
- ميكنة الغياب والحضور.

وتقدم المنصة للطلبة العديد من المميزات، مثل: (حضور المحاضرات المذاعة في بث مباشر، حسابات office 365، زيادة القدرة على الالتزام والتركيز، مشاهدة محاضرات مسجلة).

**المحور الثاني: الأمن 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.

**1 . مفهوم الأمن السيبراني**

أوضحت الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (2018) مفهوم الأمن السيبراني بأنه: "حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحتويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول استخدام أو استغلال غير مشروع، ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي، ونحو ذلك" (262) .

ويعرف الأمن السيبراني بأنه: "ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها، أو إتلافها، أو زيادة المال من المستخدمين، أو مقاطعة العمليات التجارية" (قاري، وآخرون، 2019 ،7).

ويعرف الأمن السيبراني بأنه: "حماية الأفراد وبياناتهم وحساباتهم من الهجمات الإلكترونية، ويقاس بالدرجة التي يحصل عليها المعلم من خلال إجابته على فقرات مقياس الأمن السيبراني" (الصانع وآخرون ، 2020، 48).

وتحدده المنتشري (2020، 462) بأنه: "مفهوم أمني خاص 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 الهجمات أو الأفراد ذوي الصلة بتلك المعلومات" .

كما تم توضيحه على أنه: "التدخلات التقنية والاحتياطات اللازمة لحماية أجهزة الحاسوب وشبكات الإنترنت والبيانات والمعلومات الشخصية من الوصول غير المصرح به للحفاظ على سلامة ونزاهة البيانات المخزنة في الأجهزة الرقمية" ( Rich-ardson etc al.2020.25 ).

كما يعرف بأنه: "جميع إجراءات حماية شبكات المعلومات ضد كافة الأعمال والممارسات التي تستهدف التلاعب بتلك المعلومات وإلحاق الأذى بالمستخدمين، بما يشمل الحماية ضد الاختراق، وبث البرمجيات الخبيثة والفيروسات، والوصول غير المصرح به، وغير ذلك من الممارسات السلبية" (المنتشرى وحريري، 2020، 102).

ومن خلال جميع هذه التعريفات نستخلص أن الأمن السيبراني هو مفهوم حديث نسبيًا تم استحداثه في إطار الثورة الرقمية والتكنولوجيا المعاصرة والتي تسببت في تضخم وانتقال المعلومات والبيانات بين العديد من وسائل الاتصال عبر الأجهزة الرقمية المختلفة، وعلى ذلك يهتم الأمن السيبراني بالجانب الأمني لحماية انتقال المعلومات والبيانات بين الوسائل الرقمية المختلفة. ويرجع التنوع في المفاهيم المفسرة للأمن السيبراني إلى إعتماد سياسات الأمن السيبراني على شقين أساسين هما الجانب التقني والجانب التنظيمي. وتأثير ذلك على جوانب الوعي والتطبيق اللازم لجميع الأفراد.

**2 . أهداف الأمن السيبراني**

اهتمت جميع الحكومات والمؤسسات في السنوات الماضية بالتخطيط لسياسات الأمن السيبراني، وذلك لما يحققه من العديد من الأهداف الهامة التي يمكن توضيحها كما يلي (Kortjan .2013. 46):

- توفير بيئة آمنة يستطيع المستخدم الوثوق بها.
- توفير حماية للأجهزة الرقمية المستخدمة.
- تقليل التهديدات والجرائم السيبرانية.
- مقاومة البرمجيات الخبيثة وما تسببه من إحداث أضرار لأنظمة المعلومات.

- القدرة على متابعة خطط التطوير والتحسين الرقمي بالمؤسسة.

وتستهدف الإستراتيجية الوطنية للأمن السيبراني (2017، 2021) في مصر ما يلي(9):

- 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 بمختلف أطيافه.

- 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 الخصوصة وحماية الهوية الرقمية وأمن المعلومات.

**3 . أهمية الأمن السيبراني**

إن فرص الوقوع كضحية للجرائم السيبرانية تزداد في ضوء غياب الوعي الكافي، وانتشار وتزايد الاعتماد على استخدام شبكة الإنترنت عبر العديد من الأجهزة الرقمية، ورغبة الحكومات والمؤسسات في التحول الرقمي لها (Shiling ford. 2011. 8 Stewarb. &)، وهذا ما يؤكد أهمية الأمن السيبراني الذي يتميز بعدد من المزايا التي تضيف له أهمية كبيرة، ويمكن توضيح ذلك كما يلي:

- الحفاظ على سرية وخصوصية جميع الوثائق والبيانات الرقمية.
- ضمان توافر استمرارية سير وعمل النظم الرقمية.
- توفير الحماية اللازمة للمواطنين والبني التحتية الهامة للدولة.

وتنعكس هذه الأهمية بشكل خاص على المؤسسات التعليمية لما تقوم به هذه المؤسسات من دور مهم في التوعية، وإعداد الكوادر الوطنية المؤهلة، ويمكن توضيح بعض نقاط أهميته التربوية فيما يلي:

- تضم المؤسسات التعليمية الجيل الرقمي الذي يتزايد استخدامه للمصادر الرقمية ووسائل التواصل الاجتماعي (المنتشري، 2020، 464).
- الأضرار النفسية والمعنوية التي تؤثر على المعلم عند تعرضه للاختراقات والجرائم السيبرانية مما ينعكس سلبًا على الطالب (Wilson . 2014 .5) .
- الخسائر العلمية للأبحاث والوثائق التعليمية عند التسلل إلى شبكات المعلومات الخاصة بالمؤسسات التعليمية. حيث تزامن مع أزمة فيروس كورونا المستجد استهدفت أجهزة الكمبيوتر التابعة لجامعة كاليفورنيا- سان فرانسيسكو بفيروسات معقدة على الأجهزة الخاصة بكلية الطب والتي كانت تعمل وقتها على أبحاث خاصة بفيروس كورونا المستجد وقام الفيروس بتشفير جميع البيانات والملفات على الأجهزة، وحاولت الجامعة التغلب على الفيروس ومحاولة فك التشفير الخاص بالملفات إلا أنها لم تستطع ذلك،وتم طلب فدية بدأت ب 3 ملايين دولار، إلا أن الجامعة رفضت وعرضت مبلغ 780000 دولار لكن العرض قوبل بالرفض، وأعلن الهاكر أنه يطلب 1.14 مليون دولار والتي اضطرت الجامعة إلى دفعهم للحصول على مفتاح فك التشفير الخاص بالفيروس لاستعادة ملفات الأبحاث مرة أخرى، وليست هذه الحادثة الوحيدة على مستوى الجامعات في عام 2020 حيث استهدفت فيروس جامعة يوتاUtah والتي اضطرت في النهاية إلى دفع مبلغ 457000 دولار لفك تشفير ملفات الطلبه ( مركز المعلومات ودعم اتخاذ القرار، 2020 ،15 ).

وبالنسبة للقيادات التعليمية فقد أشارت (قاري وآخرون ،2019، 11) أهمية الوعي بمفاهيم الأمن السيبراني لنظام التعليم، حيث ينبغي على قادة المؤسسات التعليمية وضع خطة شاملة للأمن السيبراني، وقام بعضهم بتقديم خمسة أسباب أساسية للاهتمام بالتدريب في هذا المجال بصورة عاجلة، وهى:

- **المسئولية**: باعتبار القادة في التعليم مسئولين عن اختراق الشبكات في حالة الإهمال.
- **المساءلة القانونية**: تحتوي سجلات المؤسسات التعليمية على معلومات سرية عن جميع الطلاب والموظفين، مثل: المعلومات الطبية، والأسرية، وغيرها، وهذه السجلات تحتاج إلى مستويات مرتفعة من الحماية تجنبًا للمساءلة القانونية.

- **السمعة المهنية**: حيث إن اختراق البيانات السرية يمكن أن يضر بسمعة المؤسسة ومنسوبيها.
- **التدريب والتعليم**: ففي ظل انطلاق التعليم نحو التحول الرقمي ظهرت الحاجة إلى توعية الطلاب والمعلمين بأساليب حماية أمن البيانات منعًا لتأثر العملية التعليمية تأثرًا سلبيًّا.
- **السجلات الرقمية**: ليست كل الهجمات تدور حول سرقة البيانات، بل إن بعضها قد يؤدي إلى تلفها أو تغييرها أو حتى مجرد التنصت، وفي جميع الأحوال يجب الاعتراف بأنها مشكلة حقيقية، ولذلك فإنه من الضروري وضع خطة لتجنبها والحد من آثارها قدر المستطاع.

**4 . مجالات استخدام الأمن السيبراني**

**يستخدم الأمن السيبراني في مجالات عديدة، من أهمها: (الصانع وآخرون 2020، 50)**

- حماية جميع أنواع الأجهزة الخاصة المحمولة والمعدات التقنية، وكذلك وسائط التخزين من خطر الهجمات والاختراقات الإلكترونية، والتدمير الجزئي والكلي.
- التعامل الآمن مع خدمات تصفح الإنترنت من خلال نشر المعلومات والإجراءات التي تعمل على توعية الأفراد بخطورة الهجمات والجرائم الإلكترونية ووسائل الاحتيال.

**5 . المخاطر السيبرانية**

تتمثل المخاطر السيبرانية في جميع الممارسات التي لها غرض إجرامي في الفضاء السيبراني والتي تستهدف الأفراد والمؤسسات والحكومات، ويمكن تصنيفها إلى قسمين: الأول: يستهدف الأجهزة الرقمية وشبكات المعلومات. والآخر: يستهدف الأفراد الذين يستخدمون الإنترنت بشكل شخصي أو داخل وظائفهم المختلفة في الحكومات (Tiwari. et al.2016.46)

وتتخذ المخاطر السيبرانية أنواعًا وأشكالًا متعددة، ومنها: الفيروسات ، والتنمر الإلكتروني، وتشويه السمعة، والقرصنة، والتصيد، وطبقا لاحصائيات عام 2020 فان

٪28 من الهجمات السيبرانية على البيانات تضمنت استخدام الفيروسات و ٪52 من الهجمات تضمنت تقنيات الاختراق (مركز المعلومات ودعم اتخاذ القرار، 2020 ،5 ) ويمكن توضيح ماهية المخاطر بشكل موجز كما يلي:

- **الفيروسات**: هى برامج حاسوبية ضارة تنتقل عبر الأجهزة الرقمية بعدة طرق، وتنتشر بين الملفات وتشكل أضرارًا بالغة الخطورة، وهى تتنوع في أشكالها وقوة تأثيرها واستمرارها داخل الجهاز الرقمي، ويمكن أن تصل خطورتها إلى حد تدمير البيئة الرقمية وتعطيل حركتها.(Tochi. et al 2012. 6)
- **التنمر الإلكتروني**: يمثل التنمر الإلكتروني أكثر أشكال الجرائم الإلكترونية انتشارًا خصوصًا بين طلبة المدارس والجامعات، وهو يصنف على أنه شكل من أشكال التحرش الرقمي؛ حيث يضر الضحية فترة طويلة، ويتم ملاحقته والسيطرة على تصرفاته وتهديد الضحية بالإيذاء والفضيحة والتحقير، وقد انتشر في السنوات الماضية بشكل كبير( Menesini.& Nocentini. 2009. 231).
- **تشويه السمعة**: حيث تستهدف الضحية عن طريق نشر معلومات غير صحيحة والإساءة إلى الشخص والتقليل من مكانته باستخدام صور غير صحيحة أو فديوهات تمت معالجتها لتخدم أهداف الجريمة، وإرسالها عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني، كما يمكن أن تستهدف تشويه سمعة المؤسسات أيضًا بقصد التقليل من مركزها التنافسي في السوق (Nathanael J.2012. 779) .
- **القرصنة**: هى عملية الدخول غير المصرح في الأنظمة المعلوماتية الرقمية بهدف كسر الحمايات الأمنية لنظم المعلومات والحصول على معلومات وبيانات سرية سواء للأفراد أو المؤسسات أو الحكومات، والتسبُّب في خسارتها (Hall & Watson .2016.8).
- **التصيُّد**: وهو من أسهل المخاطر السيبرانية في الإعداد؛ حيث يقوم المتصيد بإنشاء موقع على الإنترنت (لمؤسسات أو شركات مجهولة) وإرسال رسائل عبر البريد الإلكتروني من تلك المواقع بغرض الحصول على بيانات ومعلومات شخصية يتم الاستفادة منها في أغراض إجرامية (Vayansky. & Kumar.2018.16).

- **إرهاب الإنترنت**: تستخدم التنظيمات الإرهابية الإنترنت لتنفيذ مجموعة واسعة ومتنوعة من الأغراض التي تشمل: التجنيد، والتمويل، والدعاية، والتدريب، والتحريض على ارتكاب أعمال إرهابية، وجمع المعلومات ونشرها لأغراض إرهابية، كما تستخدم شبكة الإنترنت لتيسير الاتصال بين كافة التنظيمات الإرهابية (الأمم المتحدة، 2013 ، 1).
- **انتهاك أمن المعلومات**: تتعرض جميع استخدامات نظم المعلومات وتطبيقاتها الرقمية المحملة على شبكات الحاسبات للهجمات الضارة أو الفشل وإفشاء سرية معلوماتها أو عدم حفظ خصوصية بيانات الهيئات والمتعاملين معها أو التأخر في توافرها في الوقت الملائم لمن يحتاج إليها بسرعة، أي أنه توجد مخاطر جمة تتمثل في الوصول غير المتعمد، والاستخدام غير الملائم وغير المخصص، أو فشل النظم ذاتها لأسباب عرضية جانبية، مع العلم بأن كثيرًا من نظم وتطبيقات المعلومات سواء كانت عامة أو خاصة كتلك التي تستخدم في الأغراض الحربية والأمنية والبنوك والمستشفيات وغيرها تمثل أرضية خصبة للإرهاب المعلوماتي المتنامي اليوم (الهادي، 2006).
- **الملكية الفكرية**: وتشمل الأضرار الناتجة من وضع اسم المدعي على عمل علمي، أو تزوير ختم المؤلف، والاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة (المنتشري وحريري، 2020، 108).

ويوضح الشكل التالي الهجمات الأكثر انتشاراً في عام 2020

**شكل (2)**

**أنواع الهجمات الأكثر انتشارا في 2020**


**المصدر: مركز المعلومات ودعم اتخاذ القرار، 2020 ،4**

**5 . أساليب الحماية من المخاطر السيبرانية**

من أهم وسائل الحماية الواجب اتباعها وتطبيقها للتصدي للمخاطر السيبرانية تنمية الوعي لدى مستخدم الإنترنت بكيفية الاستخدام الآمن عبر الشبكات، فبعد وقوع العديد من حالات الهجمات السيبرانية في العديد من الدول التي استهدفت مدارس وجامعات وغيرها من المؤسسات تطلب الأمر قيام الوزارة بدور واضح تجاه التخطيط للأمن السيبراني لحماية بيئتها من هذه الهجمات، وقد طرح "طوني" (Hunt.2015.8–10) بعض تلك المبادرات والتي تتمثل في:

**ا- الهيئة الرسمية (الوزارة)**

- ضرورة وضع خطة عمل معلنة تستهدف كيفية التعامل مع المخاطر السيبرانية والانتهاكات المختلفة.
- تشمل المبادرة التنسيق بين الجامعات المختلفة.
- التعاون بين الوزارة وبعض الجهات والمؤسسات التي تستطيع توضيح إيراز كيفية التصدي لمواجهة الجرائم السيبرانية، ومتابعة الجامعات.
- متابعة الجامعات للتأكد من التطبيق والالتزام بالخطة المعلنة للتعامل الآمن مع التكنولوجيا الرقمية بما يشمل الأمن السيبراني.
- توفير دورات تدريبية لجميع العاملين بالوزارة والجامعات على كيفية التوعية بالأمن السيبراني، وأيضًا التوعية بكيفية التعامل عند وقوعهم ضحية للمخاطر السيبرانية.
- نشر الاهتمام بمفاهيم الأمن السيبراني من خلال عقد الندوات وورش العمل، والتخطيط لأسبوع للأمن السيبراني، وطباعة كتيبات بهذا الشأن، والإعلان على مواقع التواصل الاجتماعي.

**ب- الجامعة**

تساهم الجامعة بشكل فعال في استقرار المجتمع وأمنه، وحماية شباب المجتمع من المخاطر والتهديدات المعاصرة التي تواجههم، وبشكل خاص المخاطر المرتبطة بالجانب الثقافي والمعلوماتي الرقمي والتي تؤثر على الأفراد أثناء تعاملهم مع التطبيقات الرقمية المختلفة، ويمكن تحديد الأدوار المنوطة بالجامعة في مجال الإرشاد والتوعية بأساسيات الأمن السيبراني فيما يلي:

- رفع مستوى الوعي بالجرائم السيبرانية.
- التوعية بالمخاطر الأمنية.
- إقامة الندوات والمؤتمرات الخاصة بالأمن السيبراني.

– دعوة الكفاءات البشرية في مجال الأمن السيبراني للاشتراك في هذه الندوات والمؤتمرات ، وإدراج مقررات دراسية خاصة بمفاهيم الأمن السيبراني ضمن البرامج التعليمية المختلفة بالجامعة.

**ويمكن للإدارة الجامعية العمل على:**

- وضع خطط مقترحة للتوعية.
- توفير وحدة للأمن السيبراني للإشراف على تقديم التوعية والحماية.
- التعامل مع البيانات والمعلومات من خلال متخصصين.
- إصدار نشرات دورية خاصة بمفاهيم الأمن السيبراني.

**ج- المعلم (عضو هيئة التدريس)**

يمثل المعلم أهم العوامل المؤثرة في المتعلمين، ويمكن تحديد الأدوار المنوطة بالمعلم في هذا الصدد فيما يلي:

- تضمين الأنشطة التي تعكس رفع مستوى الوعي للطلاب.
- تنظيم دورات متخصصة في مجال الأمن السيبراني.
- التنسيق بين الجامعات المختلفة والجهات المشرفة على الأمن السيبراني.
- التخطيط لآلية واضحة لكيفية إدراج مفاهيم الأمن السيبراني في المقررات المختلفة.
- ابتكار أساليب حديثة للتدريس تتناسب مع التطور التكنولوجي الهائل، ومحاولة تضمين ذلك في المنهج.

كما يمكن للمعلم الاستعانة ببعض الإستراتيجيات التي تستخدم للحماية من مخاطر الهجمات السيبرانية (الصانع وآخرون، 55،56،2020)، ومنها ما يلي:

- استخدام كلمة مرور قوية يصعب وصول القراصنة إليها، وقد تطورت كلمة المرور في الآونة الأخيرة؛ حيث شملت بصمة العين، والإصبع، والوجه، والصوت، وهندسة اليد، وهذا يعني تأمين وتحديد إمكانية الوصول إلى النظام من خلال أنظمة التعريف والتحويل والتي تتضمن وسائل تعرف شخصية المستخدم.

- التدريب على المواطنة الرقمية، وهو من أهم طرق تنمية الأمن السيبراني، وذلك من خلال تعرف مجموعة القواعد والضوابط والمعايير والأعراف والمبادئ المتبعة في الاستخدام الأمثل للتكنولوجيا الرقمية والتي يحتاجها جميع من يستخدم الإنترنت بغض النظر عن أعمارهم أو مستوياتهم التعليمية أو طبيعة عملهم، وذلك كي يتعلموا طريقة التعامل مع التقنيات ليحفظوا أمنهم من الاختراق وليساهموا في المحافظة على أمن الوطن.
- عمل نسخة احتياطية من البيانات والملفات الخاصة بنظم المعلومات أو الحالة التقنية، مثل: كلمات المرور الخاصة، والبريد الإلكتروني، والبيانات المخزنة داخل أو خارج النظام.
- الوقاية من الفيروسات التي تهاجم النظام، وذلك بتثبيت برنامج التحقق من الفيروسات في الذاكرة وتحديثه باستمرار لضمان قدرته على مواجهة الفيروسات الحديثة والمتطورة، وتجهيز نسخ احتياطية من البرمجيات لاسترجاعها في حال تعرض النسخة الأصلية للتلف، ومن خلال التوعية بعدم تحميل أي برنامج غير موثوق به في حساباتهم، أو فتح روابط مجهولة.
- تجنب التواصل مع أشخاص مجهولين عبر مواقع الإنترنت، والإفصاح بشكل مباشر عند التعرض لأي شكل من أشكال الجرائم السيبرانية.
- تخصيص مرشد تربوي للأمن السيبراني لتوجيه من تعرض للمخاطر السيبرانية من خلال جلسات إرشادية.

وأوصت دراسة (Stewart & Shilingford.2011) بالدور الهام المهم للإفادة من تنظيم مخيمات صيفية متخصصة للتوعية بموضوعات الأمن السيبراني، مثل: (تاريخ الإنترنت، ومفاهيم التشفير، والمخاطر السيبرانية، والتصيد، والهجمات السيبرانية، والقرصنة، وأخلاقيات الإنترنت، وكيفية الاستخدام الآمن لمواقع التواصل الاجتماعي)، وتتضمن تلك المخيمات المعلمين والطلاب وأفراد المجتمع.

وتعتبر نظم التكنولوجيا الرقمية في العصر الحالي هى هى المحرك الأساسي لجميع المؤسسات والمنظمات، وقد أصبحت أنظمة المعلومات الرقمية أكثر تعقيدًا مع تقدم

التكنولوجيا، وتحتاج كل مؤسسة إلى إنشاء وتخطيط مساحة كافية من سياسات الأمن السيبراني وممارستها، ومعالجة الجانب التقني، ومعرفة أحدث التهديدات الأمنية باستمرار، وتوعية العاملين بها، ويتم ذلك في إطار دعم من سياسة الأمن السيبراني بالدولة، بالإضافة إلى التزام الوزارة بمتابعة التنفيذ.

وقد أشارت دراسة (المنتشري، 2020، 118–110) إلى عدد من الآليات الفعّالة التي يجب اتباعها كمخطط إستراتيجي من قبل الدولة ، وهى كما يلي:

- تشييد مؤسسات خاصة بالأمن السيبراني.
- التخطيط لإستراتيجية وطنية للأمن السيبراني.
- سن القوانين لآليات تطبيق الأمن السيبراني، ومعاقبة مرتكبي المخاطر والانتهاكات السيبرانية.
- ينبغي إدراج مفاهيم الأمن السيبراني ضمن أدلة للمعلمين، والتأكيد على نقل خبراتهم أثناء التدريس للطلاب.
- إدراج مقرر دراسي خاص بالجرائم السيبرانية للتوعية بكيفية التعامل الأمثل مع الوسائل التقنية.

وعليه فإن أهمية وضرورة إستخدام سياسات الأمن السيبراني في الجامعات تتزايد للتغلب على مشكلات عوائق الإختراقات الشبكية مما يعرض الجامعات لخطر الجهود المتكرره وضياع وقتها باستمرار في محاولة القدرة على مواكبة التطور السريع في تكنولوجيا المعلومات من أجهزة وبرامج، الأمر الذي تصدت له العديد من الجامعات العالمية بإدراج سياسات الأمن السيبراني من خلال إستراتيجيات متنوعة واضحة المعالم بحيث تستخدمها بالطريقة التي تضمن تطوير أدائها وترقية الحياة الرقمية لدولها.

**6 . التجارب الدولية لسياسات الأمن السيبراني**

تنوعت سياسات وإستراتيجيات الأمن السيبراني في العديد من الدول، وتدرجت اتجاهاتها لتشمل العديد من أشكال وأنواع الحماية الأمنية التي يتم تطبيقها، وقد سجلت خبرات الدول المختلفة عددًا من التجارب الناجحة والتي يمكن توضيح بعضها فيما يلي:

**ا- التجارب العربية**

- **المملكة العربية السعودية**

تعد تجربة المملكة العربية السعودية إحدى أهم التجارب العربية الرائدة في مجال الأمن السيبراني، ويتم ذلك تحت إشراف (الهيئة الوطنية للأمن السيبراني) والتي تم تأسيسها عام 2017 تحت إشراف خادم الحرمين الشريفين، وهى الجهة المختصة في المملكة بالأمن السيبراني والمرجع الوطني في شئونه، وقد تم تصنيفها في عام 2019 في المرتبة 13 عالميًّا والأولى عربيًّا من بين 175 دولة، وبالنسبة للجهود التربوية المبذولة لتعزيز الأمن السيبراني بالمملكة فإنه يمكن توضيح أبرزها كما يلي .https: / /www. /my.gov.sa ( )

**كلية الأمن السيبراني والبرمجة والذكاء الاصطناعي: .https: / /www.mbsc edu.sa /ar /about**

تم إنشاء هذه الكلية في مارس 2018، وهى تهدف إلى تأهيل الكوادر والقدرات الوطنية الشابة بأحدث الوسائل التقنية التي تسعى إلى تحقيق رؤية المملكة 2030 والتي تساعد على الحماية ضد الهجمات السيبرانية. وتوفر الكلية الدراسة للمستوى الجامعي لمدة أربع سنوات، والدراسات العليا لمدة عام أو عامين، بالإضافة إلى برامج للماجستير والدكتوراه في تخصصات الأمن السيبراني المختلفة.

**جامعة نايف العربية للعلوم الأمنية: https: / /nauss.edu.sa /ar-sa /pages/ default.aspx**

تأسست هذه الجامعة عام 1980م بقرار من مجلس وزارة الداخلية العرب لتكون أول جامعة عربية تعنى بالدراسات العليا في مجالات الأمن بمفهومه الشامل، ومقرها الرياض، وتتمتع الجامعة بعضوية مراقب في المجالس الوزارية العربية التالية: (مجلس الوزراء، الداخلية، العدل، الإعلام، الشئون الاجتماعية، البيئة، الصحة، الشباب)، بالإضافة إلى توقيع مذكرات تفاهم زاد عددها على (200) مذكرة مع عديد من الجامعات والهيئات والمنظمات الدولية.

وتحقيقًا لأهداف الجامعة بنشر المعرفة والثقافة وإثراء المهارات العلمية في أمن المعلومات أسهمت كثير من كليات الجامعة ومراكزها بعدة أنشطة وعدد من الدورات التدريبية فيما يخص الجريمة المعلوماتية، وأمن المعلومات، والشبكات، ومكافحة القرصنة السيبرانية من خلال التدريب في معامل مجهزة بالجامعة، والمؤتمرات واللقاءات العلمية بمقر الجامعة والمكتبة الأمنية بها، كما تمت متابعة تصنفيات الدول للأمن السيبراني من خلال المؤشر العالمي (GCI)، ويمكن توضيح أهم أدوار الجامعة للتوعية بسياسات الأمن السيبراني للمملكة من خلال:

- تعزيز مهارات العاملين في مجال الأمن السيبراني من خلال دورات تدريبية.
- رفع مستوى الوعي العام لمستخدمي الإنترنت ووسائل التقنية المختلفة من خلال برامج توعوية تناسب جميع مستويات وفئات المجتمع بقطاعاته المختلفة.
- الإسهام في وضع وتطوير الإستراتيجيات والحلول التقنية والإرشادية للتصدي والكشف عن الجرائم السيبرانية المختلفة.
- استقطاب الكفاءات العلمية والبحثية المتميزة.
- إثراء الأدبيات بالبحوث والدراسات.
- عقد واستضافة الفعاليات العلمية المختلفة من مؤتمرات وملتقيات ومحاضرات وندوات لتبادل الخبرات والاطلاع على آخر المستجدات.
- فتح قنوات للتعاون والشراكات والتحالفات في الهيئات والبرامج والمراكز المتخصصة.
- تشييد المكتبة الأمنية بالجامعة.

**برنامج الأمن السيبراني:**

تم الإعداد لبرنامج متخصص في مجال الأمن السيبراني يهدف إلى تلبية الاحتياجات التقنية والمعرفية للأجهزة ذات العلاقة بالفضاء السيبراني والذي يعد الفضاء الخامس للحرب بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية

وخصوصية البيانات، واتخاذ جميع التدابير اللازمة للحماية من مخاطر الهجمات السيبرانية التي تسعى إلى الحصول على الأموال عن طريق الفدية أو خلق النزاعات السياسية بين الدول أو التخريب بشكل عام.

ويعتبر الأمن السيبراني سلاحًا إستراتيجيًّا في يد الحكومات والأفراد، لا سيما أن الحرب السيبرانية أضحت جزءًا لا يتجزأ من الإستراتيجيات الحديثة للحروب والهجمات بين الدول (عالم، 2018، 22-21).

**مبادرة "بأمان نتعلم" (https: / /nt3lm.com /ksa/ )**

أطلقت الهيئة الوطنية للأمن السيبراني ممثلة في (المركز الوطني الإرشادي للأمن السيبراني بالسعودية) بالتعاون مع (وزارة التعليم) حملة بعنوان: (بأمان – نتعلم) وذلك في إطار جهود المركز لرفع الوعي والمعرفة بالأمن السيبراني لتجنب المخاطر السيبرانية وتقليل آثارها.

وتتزامن هذه الحملة مع بداية العام الدراسي، ومِنْ ثَمَّ فإنها تسعى إلى توعية الطالب بالمخاطر السيبرانية أثناء ممارسة مهامه التعليمية اليومية باستخدام شبكة الإنترنت، حيث نشر المركز الدليل الإرشادي للتعليم عن بعد الذي يساهم في تحصين شبكة المنزل ضد الاختراقات، وتوضيح أبرز الإجراءات الوقائية الواجب مراعاتها لتحصين الحاسب الآلي والأجهزة الذكية، كما أنه يقدم إرشادات تتعلق بالخصوصية وأساسيات تجهيز وتخصيص مكان في المنزل لتلقي الدروس الافتراضية، وأبرز العادات الحميدة اليومية الواجب الاعتياد عليها عند التعامل مع هذه الأنظمة التعليمية الإلكترونية، كما يقدِّم الدليل تجربة حية للنظام التعليمي الجديد، وأبرز ما ينبغي تطبيقه لحماية الطالب من الاختراقات التقنية.

وقد اهتم المركز بعد تطبيق الإجراءات الاحترازية لفيروس كورونا (COIVD-19) بالتوعية بكيفية التعليم عبر الشبكات، ونشر على صفحته دليلًا إرشاديًّا للتعلم عن بعد لتذكير الطلاب والمعلمين وأولياء الأمور بأهمية الأمن السيبراني أثناء الدراسة عن بعد، بالإضافة إلى نشر الممارسات الأمنية الصحيحة التي تستهدف طلاب المدارس، والطلاب الجامعيين، وكذلك المعلمين وأعضاء هيئة التدريس والمدربين.

- **الإمارات العربية المتحدة**

تم تسجيل دولة الإمارات العربية المتحدة في الصدارة عالميًّا في مجال حث وتوجيه الشباب على العمل في مجال الأمن السيبراني مقارنةً بنظرائهم دوليًّا، ويمكن توضيح أبرز الجهود التربوية المبذولة في دولة الإمارات لتعزيز الأمن السيبراني كما يلي:

**كلية تقنية المعلومات (جامعة الإمارات العربية المتحدة) ( https: / /cit.uaeu. ac.ae /ar/ )**

تهدف هذه الكلية إلى إجراء الأبحاث الأمنية للجمع بين الخبرة في التعليم والبحث والتجربة في مجال أمن المعلومات والخصوصية، وإجراء الأبحاث التي تساعد مؤسسات القطاع الحكومي والخاص على حماية أصولهم المعلوماتية، لذا تقوم الكلية بكشف المخاطر وتطوير الحلول للتقليل من هذه المخاطر وحماية البنى التحتية الحيوية للدولة من الهجمات السيبرانية، وذلك من خلال البحث في المجالات التالية:

- الأمن والخصوصية لتطبيقات المشاركة الاستشارية.
- مخططات الخصوصية لتطبيقات الصحة الإلكترونية.
- أمن البنية التحتية السيبرانية والمادية.
- الحرب السيبرانية والتجسس.

**البرنامج الوطني لبناء القدرات في الأمن السيبراني.**

(https://www.tra.gov.ae/ar/national-cybersecurity-strategy.aspx)

يعد هذا البرنامج أحد البرامج الأساسية ضمن الإستراتيجية الوطنية للأمن السيبراني، وهو يختص بتنمية المهارات في الأمن السيبراني سواء للشباب المتخصصين في المجال الأمن أو العاملين في المجالات المتعلقة بتقنية المعلومات والحاسب الآلي أو الطلاب والهواة، وهو بذلك يسهم في تعزيز جاهزية الدولة للاستجابة للحوادث السيبرانية، ودعم البحث والابتكار، إضافةً إلى تأمين البنية التحتية الرقمية للدولة، ويهدف إطار الكفاءات إلى سد الفجوة بين مخرجات التعليم وسوق العمل من خلال مساعدة الجامعات على تطوير برامجها التعليمية بما يلبي متطلبات سوق العمل. كما يعمل البرنامج بالتعاون مع

الجهات المعنية على إدراج الأمن السيبراني في المناهج التعليمية في مدارس الدولة، وإضافة تخصصات ومسابقات خاصة بالأمن السيبراني في الجامعات. كما تم إطلاق مبادرة البرنامج الوطني لبناء القدرات في الأمن السيبراني، ويهدف هذا البرنامج إلى تحقيق أهدافه من خلال أربعة محاور، هى: (الإطار الإرشادي للكفاءات، والدعم الأكاديمي، والدورات التدريبية، والفعاليات).

ويسعى البرنامج أيضا لتشجيع الجامعات على تضمين الأمن السيبراني في التخصصات الجامعية المتعلقة بتقنية المعلومات، مثل: البرمجة، والشبكات، وغيرها، حيث يحصل خريجو هذه التخصصات على المعلومات الضرورية المتعلقة بالأمن السيبراني.

ويتلخص هدف هذا البرنامج في إعداد شباب قادرين على الوقوف في وجه الهجمات السيبرانية واكتشاف مواطن الضعف في الأنظمة الرقمية وتقويتها؛ لأن التدمير المستقبلي لن يكون تدميرًا ماديًّا، بل هو تعطيل للمهام والخدمات، وخلق لحالات من الفوضى والذعر.

**ب- التجارب الأجنبية**

- **الولايات المتحدة الأمريكية**

كانت الولايات المتحدة من أولى الدول التي بدأت التعامل مع الأمن السيبراني كمهمة ذات بعد إستراتيجي، وذلك لتجنب التهديد المتنامي للاقتصاد الرقمي، مما أجبر السلطات الأمريكية على السعي لتوفير الدفاعات السيبرانية وتأمين الفضاء السيبراني للمجتمع الأمريكي، وفي عام 2003 تم وضع "الإستراتيجية الوطنية لحماية الفضاء السيبراني" بمشاركة الهيئات والوزارات الاتحادية مع وزارة الأمن الداخلي في الولايات المتحدة الأمريكية، وتم تطوير أنظمة الكشف عن التهديدات والهجمات السيبرانية، بالإضافة إلى مبادرات التعاون الدولية والتي تهدف إلى حماية الفضاء السيبراني وبناء بيئة دولية متعاونة.

وفي عام 2008 بدأت مرحلة انتقالية جديدة في تطوير سياسات الأمن السيبراني، وكان الهدف منها هو القضاء على الجرائم السيبرانية في النظام الأمريكي، وتم تطوير

سياسة الفضاء الإلكتروني، واستهدفت الإستراتيجية تطوير الإمكانات البشرية، ومحو الأمية الحاسوبية.

وفي عام 2011 تم وضع "الإستراتيجية الدولية للفضاء السيبراني" والتي استهدفت إنشاء منصة رقمية موحدة للتشارك الدولي في شأن قضايا الفضاء الإلكتروني لتعزيز سياسة الأمن السيبراني، والاهتمام ببناء القدرات على المستوى الدولي، وتقديم المساعدة إلى البلدان النامية من خلال توفير الموارد والمعارف والأخصائيين اللازمين، وإعداد إستراتيجيات الأمن السيبراني الوطنية.

وقد اهتمت الولايات المتحدة الأمريكية بتضمين إستراتيجية الأمن السيبراني في جميع الهيئات والمؤسسات داخل أمريكا، والتأكيد على أهمية سن القوانين والتشريعات لتدعيم تلك السياسات وتأمين البنية التحتية الرقمية لأمريكا، وتعتبر الولايات المتحدة الأمريكية من الدول التي تواجه عددًا هائلًا من الهجمات السيبرانية كل عام، وهذا ما يفسر وجود حوالي 58٪ من شركات الأمن الإلكتروني حول العالم بها. (Haizler. 2017.31.32)

وأما جهود الأمن السيبراني التربوية في الولايات المتحدة فيمكن توضيح أبرزها كما يلي:

**المركز القومي لبحوث التعليم السيبراني المتكامل: ( (https: / /nicerc.org**

تم تأسيس هذا المركز عام 2016 ، وهو يهدف إلى تعزيز قدرات جميع المتعلمين في الأمن السيبراني، وإعداد الكوادر الوطنية من الطلاب التي تمتلك القدرة على تعرف الفضاء السيبراني بكل أبعاده ومجالاته، وذلك من خلال:

- دراسة مفهوم الأمن السيبراني.
- دراسة كيفية حماية أجهزة الحاسوب والشبكات من الهجمات الإلكترونية.
- احتياج سوق العمل للمتخصصين في مختلف وظائف الأمن السيبراني، وذلك لاعتماد العديد من المجالات على الأنظمة الرقمية.
- اكتساب المهارات الضرورية على المستوى الدولي التي تتعلق بالقدرة على التصدي للمشكلات وتحليل المخاطر.

**دراسة تخصص الأمن السيبراني في جامعات أمريكا:**

اتجه عدد من الجامعات الأمريكية إلى تدريس تخصص الأمن السيبراني ضمن برنامج تعليمي متخصص في مفاهيم الأمن السيبراني، ويستغرق الحصول على درجة البكالوريوس في تخصص الأمن السيبراني من 4-3 سنوات، بينما تستغرق درجة الماجستير من سنة إلى سنتين، والدكتوراه من 3- 5 سنوات، ويمكن إتاحة البرنامج عبر الإنترنت في حالة عدم القدرة على الالتحاق المباشر بالجامعات من أي مكان في العالم.

STUDY CYBER SECURITY IN THE USA

https://www.studyusa.com/en/field-of-study/511/cyber-security

كما تنظم عدد من الجامعات الأمريكية دورات تدريبية قصيرة على الشبكة لمدة ثلاثة أشهر كتمهيد لتعرف التخصص السيبراني بعمق أكثر، ويمكن للدارس الاختيار من بين عدد من التخصصات، وهي: )متخصص حماية البيانات، خبير طوارئ، أخصائي أمن معلومات ، متخصص في جرائم أمن المعلومات، مطور برامج الأمن الذكية، مسئول الأمن الرقمي)، ومن ضمن الجامعات الأمريكية التي تقدم البرنامج التعليمي المتخصص في الأمن السيبراني: جامعة جورج ماسون، جامعة تاميا، جامعة ولاية ميسوري.

- **أستراليا**

تعرضت أستراليا لأول هجوم سيبراني في عام 1989م والذي استهدف التليفونات في مدينة ملبورن بأستراليا، وقامت باستحداث إدارة وطنية للفضاء تستهدف حماية المؤسسات من الهجمات الفضائية، إلا أن أستراليا أدركت أهمية التعاون في مجال الأمن السيبراني وأهمية الاستفادة من الخبرات الدولية في هذا المجال، ووجهت تعاونها مع الولايات المتحدة الأمريكية في أكثر من مجال، ويمكن توضيح أحد هذه المجالات التربوية كما يلي: (Smith & Ingram . 2017.20)

**مركز الأمن السيبراني الإستراتيجي (https: / /www.cyber.gov.au/ )**

يستهدف تكوين شبكة تعاونية بين المؤسسات في أستراليا للحماية من الهجمات السيبرانية وتطوير المهارات والكفاءة الوطنية للمتخصصين في مجال الأمن السيبراني،

والتدريب المهني بالتركيز على فئة الطلاب والجامعات بأستراليا، وإقامة المسابقات في ذلك المجال، بالإضافة إلى تقديم أدلة استرشادية عن كيفية "حماية نفسك رقميًّا وكيفية التعامل مع التهديدات السبيرانية"، وعن أهم جهات التواصل الرقمي للدولة.

ويسعى المركز إلى إتاحة كيفية التعامل الآمن الرقمي في القطاعات المختلفة في الدولة للأفراد والأسر، والمشروعات الصغيرة والمتوسطة، وكذلك المصانع الكبيرة، وتوفير بعض برامج الحماية للحاسوب والهواتف الذكية على صفحة المواطن الرقمية.

وفي أحدث المبادرات الدولية التي تؤكد تعاظم دور الإنترنت والفضاء الرقمي في تشكيل سياسات الدول الخارجية أطلقت أستراليا إستراتيجيتها الدولية للانخراط في الفضاء السيبراني (التكنولوجيا من أجل التنمية والشئون الإلكترونية الشاملة)؛ حيث تهدف إلى تكوين فضاء سيبراني مفتوح دولي آمن وحر من خلال ثمانية أقسام، هى: التجارة الإلكترونية، والأمن السيبراني، والجريمة الإلكترونية، والأمن الدولي، والفضاء الإلكتروني، وحوكمة الإنترنت، وحقوق الإنسان، والديمقراطية الرقمية.

Australia's Cyber Security Strategy 2020

https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

و تعمل الإستراتيجية على تشجيع ابتكار حلول في مجال الأمن الإلكتروني بالتعاون مع الجهات المعنية من القطاع الخاص والمجتمع المدني والمؤسسات الأكاديمية والأفراد والحكومات، سواء على النطاق المحلي أو الإقليمي أو الدولي، وذلك في ضوء لا مركزية السيطرة على الشبكة الدولية، والسماح لكل الجهات بالمنافسة.

**ثالثا: الرؤية المقترحه لسياسات الأمن السيبراني لتعزيز التحول الرقمي في الجامعات المصرية**

تمثل الرؤية المقترحة تضمين سياسات الأمن السيبراني بالجامعات المصرية لتعزيز القدرة على التحول الرقمي من خلال عددا من الآليات المقترحة التي يمكن لجميع

المستويات تنفيذها وتطويرها حسب موقعها لمواجهة والتصدي للمشكلات التي تسببها المخاطر السيبرانية المعاصرة، وتهدف الآليات المقترحة الى:

- تشكيل مجتمع واعٍ ومتسلح بآليات التصدي للمخاطر السيبرانية.
- رفع كفاءة الجامعات وتحسين ممارساتها الرقمية.
- تنمية قدرات أعضاء هيئة التدريس وتدريبيهم على وسائل الحماية من مخاطر الشبكات الرقمية.
- تزويد المتعلمين بالمهارات الرقمية ومهارات التعامل الآمن على الشبكات الرقمية.
- تطوير البرامج التعليمية بالجامعات لتتضمن مفاهيم الأمن السيبراني.

**مرتكزات الرؤية المقترحة**

- استراتجية الأمن السيبراني
- تأهل الكوادرالبشرية
- توافر التقنيات المطلوبة

**آليات الرؤية المقترحة**

ولتطبيق تلك الأهداف تتضمن الرؤية ثلاثة آليات لمستويات مخطط متكامل ومنسق بينهم بما يسهم لتصميم وتوظيف البيئة الرقمية الآمنة، ويدعم التحول نحو الاقتصاد الرقمي المتكامل بما يأصل نشر ثقافة الأمن السيبراني كثقافة داعمة للتغيير ويحقق التنمية في جميع المجالات ورفع مستوى التنافسية للجامعات المصرية، وتتضمن مستويات الرؤية المقترحة:

**مستوى الإدارات العليا**

**ويضم التعاون الدولي، القوانيين والتشريعات .**

- **التعاون الدولي:**

– التعاون الدولي في تبادل الكفاءات البشرية في مجال الأمن السيبراني.

– التعاون في بناء إستراتيجية دولية للفضاء السيبراني الآمن.

- **القوانيين والتشريعات:**

– التنسيق بين وزارة التعليم العالي والبحث العلمي وبين الجهات الحكومية المشرفة على الأمن السيبراني لاتخاذ وتطبيق كافة الاحتياطات والإجراءات اللازمة لحماية البنية الرقمية.

– سن القوانين والتشريعات اللازمة لحماية الفضاء السيبراني.

– تصميم تطبيقات إلكترونية للإبلاغ عن الجرائم السيبرانية.

– تشجيع وحث جميع أفراد المجتمع لتأهيل قدراتهم الرقمية بشكل صحيح.

– إطلاق مبادرات تستهدف مفاهيم الأمن السيبراني.

**المستوى المؤسسي**

**ويضم وزارة التعليم العالي، والجامعات**

– وضع استراتيجية رقمية تتضمن مجالات الأمن السيبراني.

– إشراك أعضاء هيئة التدريس أثناء وضع إستراتيجية الجامعة في وضع الخطط وبرامج التوعية الهادفة لتعزيز مفاهيم الأمن السيبراني.

– نشر ثقافة ومفاهيم الأمن السيبراني داخل بيئة الجامعة.

– التوعية بأساليب الحماية الإداريـة والفنية لجميع من يتعامل مع البيئة الرقمية للجامعات.

– إتاحة مواقع رقمية للإبلاغ عن الجرائم السيبرانية ضد أي بيانات داخل الجامعات.

– تنظيم مخيمات ومسابقات تحفز على مناقشة حلول الحماية ضد الهجمات السيبرانية.

– عقد دورات تدريبية وورش عمل توضح كيفية حدوث الاختراقات السيبرانية، وكيفية مواجهتها والتصدي لها.

– تأمين الخدمات الرقمية الإدارية بالجامعات والتي يمكن إجمالها في الوظائف التالية: التسجيل/ الجدولة/ تقديم المحتوى الرقمي/ التواصل الرقمي/ المحاضرات

المتزامنة وغير المتزامنه/ سجل درجات الطالب/ الإمتحانات وبنوك الأسئلة/ الأنشطة والواجبات والقدرة على إدارة جميع هذه الوظائف بمنتهى السرية والآمن.

**المستوى التربوي**

**تتضمن البرامج التعليمية للأمن السيبراني، والمعلم**

- إعداد برامج تعاونية مشتركة بين الجامعات المصرية والجامعات العالمية ذات الخبرة في مجال الأمن السيبراني.
- إدراج مقررات دراسية للأمن السيبراني ضمن برامج إعداد المعلم في كليات التربية.
- إدراج مقرر دراسي للأمن السيبراني للطلاب الجامعيين قبل التخرج.
- إصدار نشرات دورية توضح أهمية التوعية بمفاهيم الأمن السيبراني.

إن المعلم يواجه في هذا العصر جيلًا رقميًّا واعيًا وعلى دراية بالتقنيات الحديثة التي من الممكن أن تتحول إلى أداة خطيرة إذا لم توجه بالشكل الصحيح، ويتضح دور المعلم في تثقيف وتضمين أساليب الحماية للطلاب من خلال العديد من الأساليب التالية:

- تضمين أعضاء هيئة التدريس أساليب وإستراتيجيات الأمن السيبراني أثناء التدريس.
- تطبيق برامج الأنشطة الطلابية التي تستهدف تنمية الوعي بالأمن السيبراني.
- توفير برامج إرشادية لضحايا الجرائم السيبرانية وكيفية التعامل لحل المشكلة.

**متطلبات تطبيق الرؤية المقترحة**

- إدارة رقمية مرنة وقادرة على مسايرة التطور والتنمية.
- التوعية بأهمية تكوين كوادر وطنية مؤهلة للتصدي للهجمات السيبرانية.
- توفير الإمكانات اللازمة لتطبيق الرؤية المقترحة.
- المشاركة الفعالة بين جميع أفراد المجتمع والقيادات الإدارية في تطبيق الرؤية المقترحة.

**التوصيات**

1. وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية.
2. الإسترشاد بالتجارب والخبرات والإتفاقيات الدولية لأمن الفضاء السيبراني.
3. تدريب أفراد مجتمع الجامعة على كيفية استخدام قواعد الحماية عبر الشبكات الرقمية.
4. ضرورة توفير برامج تعليمية لتنمية مفهوم الأمن السيبراني من خلال التعليم الرقمي بالجامعات.

# قائمة المراجع

**أولا: المراجع العربية**


- أبو دوح، خالد كاظم (2018): الأمن الأسيبراني للدول والأفراد – الأمر الذي لابد منه، مجلة العربية، ع398 ، ابريل ،الرياض .
- الأمم المتحدة(2013): استخدام الإنترنت في أغراض إرهابية مكتب الأمم المتحدة المعني بالمخدرات والجريمة ، نيويورك.
- الإسكوا (2018): التكنولوجيا من أجل التنمية المستدامة – استحداث فرص العمل اللائق وتمكين الشباب في البلدان العربية، الدورة (30)، بيروت.
- البنك الدولي(2016): العوائد الرقمية – عرض عام – تقرير عن التنمية في العالم، واشنطون.
- الصانع، نوره عمر وآخرون (2020): وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الأنترنت وتعزيز القيم والهوية الوطنية لديهم، المجلة العلمية لكلية التربية، جامعة أسيوط، 26(6) يونيو 2020، –41 90.
- المجلس الأعلى للأمن السيبراني( 2017 ): الاستراتيجية الوطنية للأمن السيبراني 2017ـ 2021، رئاسة مجلس الوزراء، القاهرة، جمهورية مصر العربية.
- المنتشري، فاطمة يوسف، وحريري، رنده (2020): درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جده من وجهة نظر المعلمات، المجلة العربية للتربية النوعية، 4(13)، يوليو 2020، –65 140.
- المنتشري، فاطمة يوسف (2020): دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، المجلة العربية للعلوم التربوية والنفسية، 4(17) يوليو 2020، 275–485.

- الهيئة العامة لتنظيم قطاع الاتصالات (2019): الاستراتيجية الوطنية للأمن السيبراني، يونيو، الإمارات.
- اليونسكو(2018): مهارات من أجل عالم متصل – مذكرة مفاهيمية، أسبوع التعلم بالأجهزة المحمولة، بيروت.
- أمين،مصطفى احمد( 2018): التحول الرقمي في الجامعات المصرية كمتطلب لتحقيق مجتمع المعرفة، مجلة الإدارة التربوية، ع19، سبتمبر 2018، ص 11–117.
- جمال الدين، نجوى يوسف (2009): حقوق وواجبات الدارس الإليكتروني في العصر الرقمي – رؤية تحليلية، المؤتمر الدولي الأول للتعلم الإليكتروني والتعليم عن بعد، المركز الوطني للتعليم الإلكتروني والتعليم عن بعد، 16–18 مارس 2009، الرياض، المملكة العربية السعودية.
- قاري، ريم عبدالرحيم والصاني، ريم علوي وعلام، نوف خالد (2019): مفاتيح الأمن السيبراني في التعليم، جدة.
- معهد البحوث والاستشارات) 1426هـ(: الجامعات الإلكترونية، الإصدار الثامن، جامعة الملك عبد العزيز، السعودية.
- مركز الدراسات الاستراتيجية (2010): دور مؤسسات التعليم العالي في اختراق الحاجز الرقمي، جامعة الملك عبدالعزيز، المملكة العربية السعودية.
- مركز المعلومات ودعم اتخاذ القرار (2020): أهم اختراقات الأمن السيبراني لعام 2020 ، مجلس الوزراء، جمهورية مصر العربية، ديسمبر 2020.
- نور الدين، عسلي والعتيبي، راشدغازي (2020): تطوير أداء الجامعات العربية في ظل تطبيق التعليم الألكتروني متطلبات وآفاق مع الإشارة لتجربتي مصر والسعودية، مجلة التعليم عن بعد والتعليم المفتوح ، جامعة بني سويف، اتحاد الجامعات العربية، 8(14)، مايو 2020، 103ـ 147.
- وزارة التخطيط والمتابعة والاصلاح (2016): رؤية مصر 2030، استراتيجية التنمية المستدامة، مصر 2030 ، المحاور الرئيسة: الأهداف ، مؤشرات القياس، مصر.

## ثانيا: المراجع الأجنبية


- Andersson. Per.. Movin. Staffan.. Mahring. Magnus. Teigland. Robin. & wennberg Karl. (2018): Managing Digital Transformation. Stockholm School of Eton Economics Institute for Research. Brand Factory.
- Arkan Caglayan. (2016): Digital transformation - Seven steps to Success - How businesses can Stay relevant and Competitive in today's new digital era. Microsoft. 1 -10.
- Boneva. Miroslava. (2018): Challenges Related to the Digital Transformation of Business Companies. The 6th International Conference Innovation Management. Entrepreneurship and Sustainability. May 2018. 101 - 114
- Brothers Patrick. & Spies Maria (2017): Digital Transformation in Higher Education. NAVITAS VENTURES.
- Communications Authority of Kenya; Kenya National Bureau of Statistics. (2017): The Public Sector ICT Survey 2016. Nairobi: Kenya National Bureau of Statistics.
- David. Raluca. Pellini. Arnaldo. & Jordan. Katy (2020): Education during the Covid-19 Crisis - opportunities and Constraints of using Edtech in low-income Countries. Blavatnik School of Government. University of OXFORD. 110-.
- Edelhard Cathrin.. Fossland. Trine. Aamodt. Olaf. & Degn. Lise.. (2019): Digitalisation in Higher education mapping Institutional approaches For Teaching and Learning .Quality in Higher Education. 25(1). 98 -114.
- Efimov Valeriis. & Laptreva Alla V. (2018): The Future of Universities: is Digitalization the Priority? - Expert view. Journal of Siberian Federal University. Humanities & Social Sciences. 11 (12). 1925-1946.

- Haizler. Omry (2017): The United States' Cyber Warfare History: Implications on Modern Cyber Operational structures and Policymaking. Cyber Intelligence and Security.1(1).3145-.
- Hunt. Toni (2015): Cyber Security A wareness in Higher Education. Central Washington. University. 114-.
- ITU (2012): Measuring the Information Society– Studies & research-. United Nations Economic and Council. United Kingdom.
- ITU (2019): Global cybersecurity Index (GCI) 2018 – Studies & research-. United Nations Economic and Council. United Kingdom.
- Jensen. Trine (2019): Higher Education in The Digital Era The current state of transformation around the world. International Association of universities (IAU). 2019.
- Joshi. Milind J. & Patil. Bhaskar Vijayrao (2012): Computer virus - Their problems and Major exchat at-tacks in Real Life. Journal of Advanced Computer Science & Technology. 1 (4).
- Kuzu. Omur Hakan (2020): Digital Transformation in Higher Education – A case Study on Strategic Plans. Higher Education in Russia.29(3). 923-.
- Maranga Mayieka. & Nelson Masese (2019): Emerging Issues in Cyber Security for Initiutions of Higher Education. International Journal of Computer Science & Network. 8(4). August 2019.2277-5420.
- Menesini. Ersilia & Nocentini. Annalaura (2009): Cyber bullying Definition and Measurement- Some Critical Considerations. Zeitschrift fur psychologue. 217(4). 230232-.
- National Defence office:(2016): Cyber Security. A Generic Reference curriculum of the Commander Military. Kingston.
- Nathanael J. Fast. Yeri Cho (2012): Power defensive denigration and the assuaging effect of gratitude expression. Journal of Experimental Social Psychology. 48(3). 778 – 782.

- Nedyalkova Anna. Bakardjieva. Teodora. & Nedyalkov. krasimir (2016): Application of Digital Cyberesecurty Approaches to University Management – VFU Smart Student. International Conferences ITS. ICEdu Tech and STE 2016.173 – 180.
- Pawlowski. Suzanne. & Jung. Yoonhyuk (2015): Social Representations of Cybersecurity by university Students and Implications for Instructional Design. Journal of Information Systems Education.26(3). 281294-.
- Richardson. M.. Lemoine. P.. Stephens W.. & waller. R. (2020): Planning for Cyber Security in Schools -The Human Factor. Educational planning.27(2). 2339-.
- Rof Albert. Bikfalvi Andrea & Marques Pilar (2020): Digital Transformation for Business Model Innovation in Higher Education: overcoming the Tensions. Sustainability .12. 4980 Jun 2020. 115-.
- Sarker Kaushik. Rahman Hasibur. Rahman khandaker. Arman Md. Scohl. Biswas Saikat. Bhuiyan Touhid (2019): A Comparative analysis of The Cyber Security Stratgey of Bangladesh. International Journal on Cybernetics (IJCI). 8(2). April 2019. 122-.
- Schallmo Daniel R A.. & Williams. Christopher A. (2018): Digital Transformation Now! - Guiding the Successful Digitalization of your Business Model. Springer.
- Solms Rossouw. Solms Sune (2015): Cyber Safety Education in Developing countries. Journal of Systemics.13 (2). 114119-.
- Stewart. Khadija. & Shilingford. Nadine (2011): Cyber girls summer Camp - Exposing middle school Females to Internet Security. Master thesis. University of Minnesota.Strategy of Bangladesh. International Journal on Cybernetics & Informatics. (I JCI). 8(2). 120-.
- Tiwari. Soumya. Bhalla. Anshika. & Rawat. Ritu (2016): Cyber - Crime and Security. International Journal of advanced research in Computer Science and Software engineering. 6(4). 4652-.

- Vayansky. Ike & Kumar SathishA.p (2018): phishing - Challenges and Solutions. computer Fraud & Security. (1). 1520-
- Viire Taks kertu Laats. Lady Tomas. Tokar Alexandr & Kleinheyer Bernd (2019): White paper on digital transformation of Universities internationalization process. CHEDTEB. European.
- Wilson. Charles E. (2014): Cyber security education the emergence of an accredited academic discipline. Journal of the colloquium information system Security education. 2 (1).213-

**ثالثا: المواقع الإلكترونية**

- الإتحاد الأفريقي: مشروع استراتيجية التحول الرقمي( أفريقيا 2020، 2030).
https://dspace.zu.edu.ly/xmlui/handle/1913/
- البار، عدنان مصطفى (2019): تقنيات التحول الرقمي.https: / /www.kau.edu.sa
- البرنامج الوطني لبناء القدرات في الأمن السيبراني.
(https://www.tra.gov.ae/ar/national-cybersecurity-strategy.aspx)
- المركز القومي لبحوث التعليم السيبراني المتكامل: https: / /nicerc.org
- المنصة الإلكترونية الموحدة لوزارة التعليم العالي في مصر:
https://egypt-hub.edu.eg
- الهادي، محمد محمد (2006): توجهات أمن وشفافية المعلومات في ظل الحكومة الألكترونية،Cybrarain Journal ،ع9، يونيو 2006 بتاريخ 12/ 11 / 2020
http://www.journal.cybrarians.info/index.php?id=3703%A2009-07-43-59-09-15&tmpl=component&option=com_content
- الهيئة الوطنية للأمن السيبراني بالممكلكة العربية السعودية
https://www.mbsc.edu.sa/ar/about
- جامعة نايف العربية للعلوم الأمنية:

https://nauss.edu.sa/ar-sa/pages/default.aspx

- قاري، ريم عبدالرحيم والصاني، ريم علوي وعلام، نوف خالد (2019): مفاتيح الأمن السيبراني في التعليم، جدة.

https://jarirreader.com/book/13405/

- عالم، محمد أسعد ( 2018): دور الجامعات في الأمن السيبراني، جامعة نايف العربية للعوم الأمنية كنموذج، 12–13 فبراير 2018 www.itu.int.com
- كلية تقنية المعلومات (جامعة الإمارات العربية المتحدة) .https: / /cit.uaeu /ac.ae /ar
- مبادرة "بأمان نتعلم" /https: / /nt3lm.com /ksa
- محمود، مديحة فخري(2011): حول دور الجامعات المصرية في مواجهة الجرائم الألكترونية لدى الطلاب، دراسات تربوية

https://almohakmoonalarab.ahlamontada.com/t94-topic

- وحدة إدارة المشروعات بوزارة التعليم العالي في مصر

http://portal.mohesr.gov.eg/ar-eg/Pages/Projects-Management-Unit.aspx

- موقع وزارة التعليم العالي والبحث العلمي بمصر

http://portal.mohesr.gov.eg/ar-eg/Pages/Higher-education-in-numbers.aspx

- Australian Computer Society (2016):

https://50years.acs.org.au/home

- Australia's Cyber Security Strategy 2020

https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

- Catota. Frankie. Morgan. Granger. & Sicker Douglasmar. (2019): cybersecurity education in developing nation: the Ecuadorian environment. Journal of CYBERSECURITY. 119-.

https://academic.oup.com/cybersecurity/article/51//
tyzoo15382610/

- Hall. Gary & watson. Erin (2016): Hacking - Computer Hacking. Security testing Penetration Testing and Basic Security.

https://www.amazon.in/Hacking-Computer-Security-Testing-Penetration-ebook/dp/B01N1UPX8D

Higher Education Authority (2019): Digital Transformation and Empowering Technologies in Higher Education. February 2019

Doil https://hea.ie/assets/uploads/2017190212/04/_FutureFocus_Digital..

- Kortjan. Noluxolo (2013): A Cyber Security Awareness and Education Framework for South Africa.

https://www.researchgate.net/publication/337488454_The_South_African

- Microstrategy (2016): Digital Transformation of Higher Education with Microstrategy 10.

https://www.microstrategy.com/us/resources/library/guides/digital

- Smith. Frank. & Ingram. Graham. (2017:(Organising cyber Security in Australia and Beyond. Australian Journal of International Affairs

https://www.tandfonline.com/doi/abs/10.108010357718.2017.132/0972

- Universities Australia(2019): Submission to Australia's 2020 Cyber Security Strategy Discussion paper November (2019).

https://www.universitiesaustralia.edu.au/submission/submission-to