جامعة المنصورة
كلية التربية

القيادات الأكاديمية وأدوارها في تعزيز ممارسات الأمن السيبراني بالجامعات الأمريكية وإمكانية الإفادة منها بالجامعات المصرية

إعداد

د./ هاني رزق عبدالجواد الألفي
أستاذ التربية المقارنة والإدارة التربوية المساعد
الكلية التطبيقية – جامعة حائل

مجلة كلية التربية – جامعة المنصورة
العدد ١١٩ – ابريل ٢٠٢٢

القيادات الأكاديمية وأدوارها في تعزيز ممارسات الأمن السيبراني بالجامعات الأمريكية وإمكانية الإفادة منها بالجامعات المصرية

د. / هاني رزق عبدالجواد الألفي
أستاذ التربية المقارنة والإدارة التربوية المساعد
الكلية التطبيقية – جامعة حائل

ملخص الدراسة

هدفت الدراسة إلى العمل على تطوير أدوار القيادات الأكاديمية في تعزيز ممارسات الأمن السيبراني بالجامعات المصرية ؛ وذلك بالإفادة من أدوار القيادات الأكاديمية بالجامعات الأمريكية . استخدمت الدراسة المنهج الوصفي ؛ وذلك لملائمته لطبيعتها. وقد توصلت الدراسة إلى وضع معالم رؤية مقترحة لتطوير أدوار القيادات الأكاديمية بالجامعات المصرية ؛ تتضمن تلك الرؤية ثمانية محاور رئيسة تشمل (فلسفة الرؤية المقترحة، منطلقات الرؤية المقترحة، مبررات الرؤية المقترحة، أهداف الرؤية المقترحة، متطلبات تنفيذ الرؤية المقترحة، معوقات تنفيذ الرؤية المقترحة وإمكانية التغلب عليها) . وقد أوصت الدراسة بضرورة التزام القيادات الأكاديمية بتطبيق الرؤية المقترحة، وحل مايواجهها من مشكلات وتحديات. مع ضرورة التزام القيادات الأكاديمية بتوفير المتطلبات البشرية والمالية والمادية لتطوير ممارسات الأمن السيبراني بالجامعات المصرية .

Abstract

The study aimed to develop the roles of academic leaders in enhancing cybersecurity practices in Egyptian universities; By taking advantage of the roles of academic leaders in American universities. The study used the descriptive approach; Because of its suitability to its nature. The study came up with a proposed vision for developing the roles of academic leaders in Egyptian universities. That vision includes eight main axes that include (the philosophy of the proposed vision, the premises of the proposed vision, the justifications of the proposed vision, the objectives of the proposed vision, the stages of building the proposed vision, requirements for implementing the proposed vision, obstacles to implementing the proposed vision and the possibility of overcoming them, and the entities entrusted with implementing the proposed vision. The study recommended the necessity of academic leaders' commitment to implementing the proposed vision, and solving the problems and challenges they face, with the need for academic leaders to commit to providing the human, financial and material requirements for developing cybersecurity practices in Egyptian universities.

مقدمة

لقد أصبحت تقنية المعلومات الإدارية عنصر أساسي وهام في المؤسسات الأكاديميـــة ؛ لكونها أداة مهمة في عملية إنجاز الأعمال بشكل كفء ودقيق وسريع، وكذلك مواجهة التحـــديات الجديدة التي تفرضها الثورة المعلوماتية في الوقت الحاضر .

وتعد الإدارة الالكترونية إحدى ثمار التطور التقني في مجال الاتصالات، فبعـــد بـــروز ثورة المعلومات وثورة الاتصالات التي ساعد عليها تطور أجهزة الحاسب الآلي وتقنياته، جاءت الإدارة الالكترونية كرد فعل واقعي لاستخدام تطبيقات الحاسب الآلي في مجالات الخدمة العامـــة لتطوير طرق العمل التقليدية إلى طرق أكثر مرونة وفعالية من ناحية، والاستفادة مـــن منجـــزات الثورة التقنية في توفير الوقت والجهد والتكلفة من ناحية أخرى.

لذا أصبح استخدام تكنولوجيا المعلومات والاتصالات نظامًا متكاملًا تمامًا في كل وظيفة من وظائف حوكمة المؤسسات خاصة التعليمية منها، بما في ذلك مؤسسات التعلـــيم الجـــامعي . (علي، ٢٠١٩)

ونتيجة لاستخدام الإدارة الالكترونية في تنفيذ المهام والمسؤوليات المختلفة بالجامعات ؛ فقد تعرضت لهجمات عدة منها الاحتيال وسرقة المعلومات وتغيير البيانات ، حيـــث أن العمـــل الالكتروني معرض لتلك الهجمات ، والتي ينظـــر إليهـــا (Abdulrahman and Omar,2018) على أنها تحديات تحد من كفاءة الإدارة الالكترونية وتقلل من فعاليتها ؛ لذا اتجهت الجامعات من أجل الحفاظ على النتائج والمكتسبات التي تحققت من تطبيق الإدارة الالكترونية إلى البحث عـــن أساليب جديدة تدعم من الخطوط الدفاعية للجامعات في مواجهة تلك الهجمات ؛ وبحيث تعطي لها حصانة قوية للوقاية منها .(نشأت ، ٢٠٢١)

وتسمى تلك الأساليب بإجراءات أو ممارسات أو بـــرامج الأمـــن الـــسيبراني (cyber security). يشير (Almarashdeh and Alsmadi, 2017) أن الجامعات تحتاج إلـــى جعـــل الأمن السيبراني من ضمن أولوياتها. حيث أن الهجمات الإلكترونية السيبرانية ليست أقل خطورة من الأزمات والكوارث التي تخلفها الممارسات الخاطئة في العمل الجامعي.

هناك إشكالية كبيرة إذن كما يشير (Ani,et al,2017) تطرح أسئلة عديدة تتبلور حول لماذا التعليم العالي عامة والجامعي خاصة مجال خصب للعديد من الهجمـــات الـــسيبرانية ذات التأثير الخطير والضار؟

ذكر (Catota,et al,2019) تعدد أسباب ذلك ؛ حيث أشار إلى أن عمل الجامعات يتركز على درجة كبيرة من الثقافة الأكاديمية الفريدة ، والتي تتسم بدرجة من الانفتاح والشفافية والحرية والاستقلالية التي تفتقر إليها معظم الصناعات والمؤسسات في كافة القطاعات . إضافة إلى أن هناك سبب آخر يتعلق بالتاريخ – على وجه التحديد ، حيث أكد Abdulrahman and Omar,2018). أن الجامعات كانت من أولى المؤسسات المجتمعية التي تستخدم الإدارة الالكترونية في ممارسة مهامها والأكثر من ذلك أنها المؤسسة الأولى التي تعاملت مع شبكة الانترنت بشكل واسع وفعال أكثر من غيرها من المؤسسات المجتمعية ؛ لذا فإنها دائماً كانت وماتزال أهدافًا رئيسة للهجمات السيبرانية ، ومع الوصول المتكرر والمتواصل إلى الإنترنت . كما يشير (Ani,et al,2017) أن هناك جهات وأشخاص تحاول الوصول إلى المدى والمعرفة البحثية والأكاديمية الذي يمكن أن تصل إليها تلك الجامعات ، وبالتالي من المحتمل أن تكون نقاط ضعفها معروفة جدًا ومفهومة من قبل المهاجمين عبر الإنترنت .

في الواقع إذن ، يكتسب الأمن السيبراني – الآن – شهرة واسعة ويتم استخدامه على نطاق واسع بالجامعات في العالم المتقدم والنامي ؛ خاصة بعد جائحة كورونا والتي اعتمدت فيها الجامعات على الإدارة الالكترونية في ممارسة مهامها الأكاديمية والإدارية . فكما يشير Pavel (,et al,2021) تعددت الهجمات السيبرانية التي دمرت كثيراً من الملفات الالكترونية الجامعية وأخفت ملفات وعدلت ملفات منها نتائج الطلاب ، ورواتب العاملين ومكافئات الطلاب ؛ حتى الأبحاث العلمية لم تسلم من السرقة والإخفاء . مما تسبب في أضراراً مالية وأكاديمية وبحثية خطيرة . فعلى سبيل المثال تعرضت جامعة كالجاري (University of Calgary) وميلانو (Milano Università) بإيطاليا ، وجامعات باريس(Université de Paris) وتولوز(Toulouse University) بفرنسا ولندن(University of London) وأدنبرا(Edinburgh University) ببريطانيا ونيويورك(New York University) وكاليفورنيا (University of California) بالولايات المتحدة الأمريكية ، و جامعتي كيب تاون(University of Cape Town) وبريتوريا (University of Pretoria) بجنوب أفريقيا ، وجامعة الإمارات وجامعة الملك سعود بالمملكة العربية السعودية لهجمات سيبرانية كانت تحاول تدمير ملفات الجامعة واتلافها . ولولا وجود إجراءات للأمن السيبراني بتلك الجامعات لتعرضت ملفاتها للسرقة والإتلاف. (Alquda and Muradkhan, 2021)

يشير (Catota,et al,2019) أن الانتهاكات الأكثر إثارة للقلق هي الأماكن التي تتعرض فيها سلامة الموارد البشرية كالطلاب وأعضاء هيئة التدريس والعاملين للخطر. فالجامعات مكلفة بحماية مواردها البشرية ، لكن نتيجة ضعف بنيتها التحتية للأمن السيبراني يمكن أن تعرضهم للخطر. (Pavel ,et al,2021) يحدث ذلك عندما يتم اختراق الدوائر التلفزيونية المغلقة ، والمنصات الالكترونية في العديد من الجامعات ، والدخول على النظام الالكتروني للمعاملات الإدارية الرسمية ، بل وسرقة الحسابات الرسمية للجامعات. ولهذه الأسباب تحتاج الجامعات إلى بذل المزيد من الجهود لضمان حماية تطبيقات الجامعات وأنظمتها والعمل على التغلب على أي تحديات تواجهها .

في الولايات المتحدة الأمريكية شهدت جامعاتها أعوام قاسية من الهجمات الإلكترونية خاصة في أعوام ٢٠١٩،و ٢٠٢٠، و٢٠٢١ وفقًا (Naidu and Zainuddin , 2021) ، يعد التعليم الجامعي الأمريكي القطاع الأكثر عرضة للتهديدات السيبرانية. في (أغسطس) ٢٠٢١ ، ارتفع متوسط عدد الهجمات الالكترونية ضد الجامعات في الولايات المتحدة بنسبة ٣٠٪ ، مقارنة بـ ٦,٥٪ في جميع القطاعات الأخرى. تم زيادة ميزانية الأمن السيبراني في الجامعات الأمريكية ، وتوجيهها نحو تحديث استراتيجيات الجامعات في مواجهة التهديدات السيبرانية ، وتكثيف البرامج التدريبية لزيادة الوعي الأمني لدى الموارد البشرية لتعزيز حماية البيانات عبر مختلف الأجهزة والشبكات ، إضافة إلى تطوير عمليات صيانة البرامج الالكترونية والأنظمة الالكترونية بالجامعات ، وتطوير ممارسات القيادات الأكاديمية في مواجهة التهديدات ، وتفعيل أدوارها. ((Redman,et al,2020

يؤكد (Fouad,2021)أن الأمن السيبراني بالجامعات الأمريكية يعد جزءاً لا يتجزأ من المهام اليومية لكل قيادة جامعية . حيث تحتاج القيادات الأكاديمية لفهم واكتشاف وتجنب التهديدات السيبرانية التي قد يواجهونها أثناء ممارستهم لأنشطتهم اليومية. كما يشير Naidu and (Zainuddin , 2021) أنه للمساعدة في الوصول إلى هذه النقطة، فقد تطلب الأمر إشراك القيادات الأكاديمية في اللجان المسؤولة عن مواجهة التهديدات السيبرانية ، والمشاركة في وضع استراتيجية الجامعة في الحماية من الهجمات السيبرانية . إضافة إلى القيام بجولات ميدانية على الكليات والإدارات المختلفة للتأكد من حسن سير العمل في تنفيذ خطط واستراتيجيات الجامعة تجاه الأحداث السيبرانية . كما تعمل القيادات على تفعيل أدوار الموارد البشرية والطلاب من

خلال الالتزام بالحصول على البرامج التدريبية ، والمشاركة في لجان الأمن السيبراني بكل كلية وإدارة.

أما في مصر فالوضع يبدو في بداية طريق طويل نحو التوجه لرسم معالم استراتيجية الأمن السيبراني بكل جامعة مصرية ، فمازالت جهود الجامعات قاصرة على تقديم القليل من البرامج التدريبية للمستفيدين ، وشراء بعض البرامج (anti virus) ضد بعض المهاجمين أو المخترقين (Hackers) لبرامج الجامعة . وهو ما يشير إلى ضرورة الاهتمام بتطوير ممارسات الأمن السيبراني وتفعيل أدوار القيادات الأكاديمية بكل جامعة.

في هذه الدراسة، سنسلط الضوء على الوضع الحالي لأدوار القيادات الأكاديمية في تطوير ممارسات الأمن السيبراني بالجامعات الأمريكية ، وكيف يمكن استثمار ذلك في تطوير أدوار القيادات الأكاديمية المصرية .

مشكلة الدراسة

تعد القدرة على الاتصال الآمن بالأنظمة الافتراضية عنصرًا مهمًا داخل أي نظام جامعي داعم لبيئة العمل والتعلم .(علي، ٢٠١٩)،(Alkhsabah, 2017)، Abdulrahman (and Omar,2018) هذا هو الحال بشكل خاص داخل الجامعات، حيث تمارس المهام والأنشطة المختلفة بواسطة التكنولوجيا الالكترونية. فالبيئة الجامعية تضم أشكالاً إلكترونية رقمية مختلفة ، وأنظمة معلوماتية متنوعة إضافة إلى أنظمة بنية تحتية متعددة الطبقات مع مستويات مختلفة من الوصول والاتصال. (علي، ٢٠١٩) لكن لسوء الحظ ، جعلت هذه البيئة الجامعية المفتوحة أهدافاً للهجمات السيبرانية الإلكترونية .

لذا ، تواجه الجامعات –سنوياً – فيضاناً مستمرًا من الهجمات الإلكترونية السيبرانية. التي كلفتها خسارات كبيرة مالية وفنية ؛ تبلورت في ضياع المعلومات والبيانات ، وتشويهها وتغييرها لتحقيق أهداف خبيثة تصب في مصلحة المهاجمين إضافة إلى سرقة الاختبارات النهائية والفصلية ، والنتائج الطلابية ، ونتائج البحوث العلمية ، وتقارير الأقسام العلمية والكليات واللجان المختلفة .

في الجامعات المصرية، وعلى الرغم من وقوع العديد من الهجمات السيبرانية التي لم تعلن عنها الجامعات إما خوفاً من التأثير على سمعتها الأكاديمية أو اللامبالاة من قبل بعض الجامعات. (شعبان ،٢٠٢١) إلا أنها لم تتخذ خطوات جدية – إلى الآن – في مواجهة تلك

الهجمات والقضاء عليها . واكتفت العديد من الجامعات بشراء بعض البرامج للوقاية من الفيروسات الالكترونية؛ إلا أن هذه البرامج لم تفلح في وقاية الجامعات من الهجمات الالكترونية . (عرفه ، والعراقي ،٢٠٢١)

وقد عبرت العديد من الدراسات العلمية والتقارير عن مظاهر ومعالم الوضع الراهن لممارسات الأمن السيبراني بالجامعات المصرية على النحو التالي:

١- ما أشارت إليه الدراسة الاستطلاعية التي أجراها الباحث على عدد ٤٠ قيادة جامعية من جامعات(المنصورة ، وبني سويف ، الإسكندرية ، والقاهرة ، وبورسعيد) والتي أكدت على خلو الجامعات المصرية من خطط لإدارة ممارسات الأمن السيبراني بتلك الجامعات ، وضعف مهارات الأمن السيبراني لدى القيادات الأكاديمية ، وعدم الرغبة في مواجهة التهديدات السيبرانية إما لعدم المعرفة بماهية الأمن السيبراني أو لعدم وجود آلية للتحفيز ، إضافة إلى نقص البرامج التدريبية في مجالات الأمن السيبراني الموجهة للقيادات خاصة والموارد البشرية الجامعية عامة .

٢- ما أشارت إليه دراسات (شعبان ، ٢٠١٧) ، (جمال الدين ،٢٠٢٠) (شعبان ،٢٠٢١) ، (عرفه ، والعراقي ،٢٠٢١) ؛ من أن :

- ممارسات الأمن السيبراني في الجامعات المصرية مازالت محدودة للغاية وقاصرة على تحقيق درجة الوقاية من الهجمات السيبرانية، وتكاد تقتصر على بعض برامج حماية البيانات، والدورات التدريبية للمستفيدين.
- لا يزال هناك انقطاع بين متخصصي الأمن السيبراني وقادة الجامعات. حيث تنشغل القيادات بالقضايا الأكاديمية والبحثية والخدمية؛ مما تتأثر مشاركتهم الإشرافية والتنفيذية بمواجهة المخاطر والتهديدات السيبرانية التي تتعرض لها جامعاتهم. وهذا يعني أن الكثير من القيادات الأكاديمية محدودي المعرفة بقضايا الأمن السيبراني.
- خلو اللوائح والقوانين الجامعية من التركيز أو إبداء الاهتمام بقضايا وممارسات الأمن السيبراني بالجامعات المصرية؛ مما يشير إلى وجود خلل تشريعي في تشريعات الجامعات المصرية يتعين علاجه وبسرعة قصوى.
- سلبية القيادات الأكاديمية في مواجهة التهديدات والهجمات السيبرانية، وترك ذلك للمتخصصين.

٣- على الرغم من تشكيل المجلس الأعلى للأمن السيبراني بقرار من رئيس مجلس الوزراء بالعام ٢٠١٤ برئاسة وزير الاتصالات ، وعضوية ممثلين عن كل من وزارات: البترول ، الدفاع، الداخلية ،الكهرباء ،الخارجية، الصحة، التموين ،الموارد المائية ، البنك المركزي ، جهاز المخابرات العامة، إضافة إلى ٣ أعضاء من ذوي الكفاءة والخبرة. إلا أنه أغفل تمثيل وزارة التعليم العالي بممثل لها يقدم مقترحات ويبادر بالنقاشات ، ويوضح ما تعانيه الجامعات من مشكلات ومعوقات تتعلق بالأمن السيبراني وممارساته بداخلها ؛ مما يشير إلى مواصلة اغفال جوانب الأمن السيبراني بالجامعات على المستوى الحكومي ؛ وإلى الآن مازال تشكيل هذا المجلس كما هو دون تغيير . (قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤)

٤- ما أشار إليه تقرير مركز المعلومات بمجلس الوزراء؛ من ضرورة تطوير الوضع الحالي لممارسات الأمن السيبراني بالجامعات المصرية وإصلاح ما تعانيه تلك الممارسات من أخطاء ، مع ضرورة تقديم وتطوير لمبادرات ومشروعات تتعلق بالأمن السيبراني وأمن المعلومات بشكل عام. (مركز معلومات مجلس الوزراء،٢٠٢٠)

وعلى ضوء ما تقدم من دراسات علمية وقرارات حكومية وتقارير رسمية ؛ اتضح معاناة الجامعات المصرية من مشكلات وتحديات عدة في مجابهة الأخطار والتهديدات السيبرانية ، وخلو اللوائح الجامعية من الاهتمام بالإدارة المثلى لهذه التهديدات وسلبية القيادات الأكاديمية في مواجهة التهديدات السيبرانية ؛ لذا صار هناك حاجة ماسة لتطوير ممارسات الأمن السيبراني بالجامعات المصرية بالتركيز على أدوار القيادات الأكاديمية الجامعية ولا مانع من الإفادة من ممارسات القيادات الأكاديمية بالجامعات الأمريكية – وبما يتلاءم مع طبيعة البيئة الجامعية في الجامعات المصرية – على اعتبار أن الخبرة الأمريكية في مجال الأمن السيبراني أحد أبرز الخبرات على مستوى العالم.

يتبلور السؤال الرئيس للدراسة حول

كيف يمكن الإفادة من أدوار القيادات الأكاديمية بالجامعات الأمريكية في تعزيز ممارسات الأمن السيبراني في تطوير أدوار وممارسات القيادات الأكاديمية بالجامعات المصرية؟

ويتفرع من التساؤل الرئيس التساؤلات الفرعية التالية :

١- ما أبرز الاتجاهات الحديثة في الإدارة الالكترونية بالجامعات؟

٢- ما الأسس النظرية التي ترتكز عليها فلسفة الأمن السيبراني في الجامعات؟
٣- ما أبرز أدوار القيادات الأكاديمية بالجامعات الأمريكية في تعزيز ممارسات الأمن السيبراني؟
٤- كيف يمكن تطوير أدوار القيادات الأكاديمية بالجامعات المصرية لتعزيز ممارسات الأمن السيبراني؟

أهداف الدراسة

هدفت الدراسة إلى تحقيق ما يلي:

١- تحليل أبرز الاتجاهات الحديثة في الإدارة الالكترونية للجامعات.
٢- تحليل الأسس النظرية التي يرتكز عليها الأمن السيبراني في الجامعات.
٣- تحليل أبرز أدوار القيادات الأكاديمية الجامعات الأمريكية في تعزيز ممارسات الأمن السيبراني.
٤- تحديد إجراءات تطوير أدوار القيادات الأكاديمية بالجامعات المصرية لتعزيز ممارسات الأمن السيبراني.

أهمية الدراسة

تتبلور أهمية الدراسة الحالية فيما يلي :

١- قلة الدراسات العلمية في مجال الأمن السيبراني في الجامعات المصرية عامة والقيادات الأكاديمية الجامعية خاصة ؛ مما يعد إضافة للمكتبة العربية .
٢- تعدد الهجمات والتهديدات السيبرانية خاصة بعد تفعيل ممارسات التعلم عن بعد من خلال المنصات الالكترونية إضافة إلى ممارسة المهام الإدارية والالكترونية الجامعية الكترونياً؛ مما يستلزم الاهتمام بممارسات الأمن السيبراني تنظيراً وتطبيقاً.
٣- فتح المجال أما الباحثين للقيام بمزيد من البحوث والدراسات التي تتناول جوانب وتوجهات وممارسات الأمن السيبراني بالجامعات والمؤسسات التعليمية .
٤- الاستجابة لتوجهات الدولة المصرية ورؤيتها ٢٠٣٠ الهادفة إلى استثمار التكنولوجيا الرقمية في المؤسسات المصرية – خاصة – التعليمية منها ؛ وما يتطلبه ذلك من توفير درجات عالية من الأمان لصد التهديدات الالكترونية السيبرانية المحتملة .

مصطلحات الدراسة

- الأمن السيبراني :

قبل التطرق لتعريف الأمن السيبراني ؛ فإنه يتعين تحديد ما المقصود بكلمة سيبراني . يشير (Fouad,2021) أن السيبرانية تعني الالكترونية ، وقد اتفق علماء المعلوماتية على إطلاق لفظ "سيبراني" على ما يتعلق بالشبكات الإلكترونية المرتبطة الإنترنت، والتطبيقات المتنوعة مثل (التويتر ، الفيس بوك ، الواتس أب ، وغيرها) .

بينما الأمن السيبراني يعرف بأنه تطبيق التقنيات والضوابط لحماية الأنظمة الجامعية من الهجمات الإلكترونية. (Redman,et al,2020) كما أنه مجموعة من الممارسات التي يتم استخدامها من قبل الجامعات للحماية من الوصول غير المصرح به إلى مراكز البيانات والأنظمة المختلفة. (الخضري،٢٠٢٠) بينما يعتقد البعض بأنه استراتيجية أمنية ضد الهجمات الخبيثة المصممة للوصول إلى أو تعديل أو حذف أو تدمير أو ابتزاز أنظمة الجامعة الالكترونية المتصلة بالشبكة العنكبوتية. (Aljohni ,et al,2021) مجموعة الأساليب التفاعلية التي يتم فيها تخصيص الموارد لحماية الأنظمة من التهديدات الالكترونية. .(Abdulrahman and Omar,2018)

ويقصد به في الدراسة الحالية الخطط والبرامج والأساليب التي تطبقها الجامعات المصرية للوقاية والحماية من التهديدات الالكترونية السيبرانية بأنواعها المختلفة .

- القيادات الأكاديمية : والمقصود بها في الدراسة الحالية من يتولون مناصب قيادية أكاديمية بالجامعات (رئيس القسم ، ووكيل الكلية ، وعميد الكلية ، نائب رئيس جامعة ، رئيس جامعة) .
- ممارسات : تعرف بأنها أداء فعل مرة واحدة أو أكثر بقصد تثبيته أو تحسينه . كما تعرف بأنها أي أداء لفعل أو سلوك يؤدي إلى التعلم.(أحمد،٢٠٢١) كما ينظر إليها على أنها تطبيق العلم النظري أو المعرفة على وجه الخصوص عن طريق التجربة لأداء أو متابعة عمل أو مهنة .(الفقيه،٢٠١٩)

بينما يقصد بها في الدراسة الحالية مجموعة المهام التي ترتبط بتنفيذ أنشطة تتعلق بصورة مباشرة أو غير مباشرة بمجال الأمن السيبراني بالجامعة.

منهج الدراسة

استخدمت الدراسة المنهج الوصفي؛ وذلك لملائمته ومناسبته لطبيعتها؛ واتضح ذلك من خلال جمع المعلومات التي تتعلق بالاتجاهات الحديثة في الإدارة الالكترونية بالجامعات، والأسس النظرية التي ترتكز عليها فلسفة الأمن السيبراني في الجامعات، وأبرز أدوار قيادات الجامعات الأمريكية في تعزيز ممارسات الأمن السيبراني؛ وتصنيف تلك المعلومات وتنظيمها وتحليلها واستخلاص بعض الإجراءات التي يمكن الإفادة منها في تطوير ممارسات القيادات الأكاديمية الجامعية المصرية.

الدراسات السابقة

تناولت الدراسة الحالية الدراسة السابقة مرتبة من الأحدث إلى الأقدم مع توضيح أهدافها ومنهجها المستخدم وأبرز نتائجها وتوصياتها، وتم تقسيمها إلى دراسات عربية وأخرى أجنبية على النحو التالي :

أولاً الدراسات العربية:

١. دراسة سراج (٢٠٢٢)

هدفت الدراسة إلى التطوير البحثي لمجال الأمن السيبراني في المجالات التربوية ، استخدمت الدراسة المنهج الوصفي ، وتوصلت الدراسة إلى أن الاتجاهات البحثية في الأمن السيبراني يجب أن تركز على منهجية الأمن السيبراني في مؤسسات التعليم قبل الجامعي والجامعي ، ممارسات الأمن السيبراني في المؤسسات التعليمية ، الاتجاهات الحديثة في مجال الأمن السيبراني ، الدراسات المقارنة للمؤسسات الجامعية وممارساتها للأمن السيبراني ، مشكلات الأمن السيبراني ومقترحات حلها ، تطوير ممارسات الأمن السيبراني في مؤسسات التعليم قبل الجامعي والجامعي ، آليات تفعيل ثقافة الأمن السيبراني في المؤسسات التعليمية ، المنصات التعليمية والأمن السيبراني ، الأدوار القيادية في مواجهة التهديدات السيبرانية . كما أوصت الدراسة بمزيد من الاهتمام بمجال الأمن السيبراني في المؤسسات التربوية ؛ حيث أنه مجال مازال يعاني من الإهمال .

٢. دراسة فرج (٢٠٢٢)

هدفت الدراسة تحديد مبررات تفعيل الأمن السيبراني في جامعة الأمير سطام ، استخدمت الدراسة المنهج الوصفي ، توصلت الدراسة إلى أن من أبرز مبررات تفعيل الأمن

السيبراني بجامعة الأمير سطام : حماية ووقاية الجامعة من حالات السرقة والاحتيال الالكتروني على معلومات وبيانات الجامعة ، زيادة وعي الكوادر البشرية بالجامعة بأهمية تطبيق إجراءات الأمن السيبراني بالجامعة، التيسير من التعامل الالكتروني في تنفيذ الممارسات الأكاديمية والإدارية بالجامعة . أوصت الدراسة بضرورة تفعيل ثقافة الأمن السيبراني لدى القيادات الجامعية ، والموارد البشرية بالجامعة .

٣. دراسة البيشي (٢٠٢١)

هدفت الدراسة إلى توضيح واقع ممارسات الأمن السيبراني في الجامعات بالسعودية وأثر ذلك على تعزيز الثقافة الرقمية، ولتحقيق أهداف الدراسة استخدم المنهج الوصفي التحليلي. وتوصلت الدراسة إلى أن واقع ممارسات الأمن السيبراني في الجامعات السعودية جاء مرتفعا ، كما اتضح أن مستوى الثقة الرقمية جاء أيضاً مرتفعا ، وقد اتضح أن هناك تأثير للأمن السيبراني في تعزيز وتفعيل الثقة الرقمية، واتضح عدم وجود فروق دالة إحصائياً للأمن السيبراني وأثر ذلك على تعزيز وتفعيل الثقة الرقمية ترجع لعدد سنوات الخبرة إضافة للدرجات العلمية. وأوصت الدراسة بضرورة زيادة الميزانية المخصصة للأمن السيبراني بالجامعات السعودية إضافة إلى زيادة الاهتمام بإجراءات أمن المعلومات ، وضرورة التطوير والتحسين المستمر لقدرات الموارد البشرية بالجامعة خاصة القيادات الأكاديمية الجامعية تجاه التهديدات السيبرانية.

٤. دراسة شعبان (٢٠٢١)

هدفت الدراسة إلى وضع مقترح لتفعيل أدوار جامعة القاهرة في نشر ثقافة الأمن السيبراني لدى طلاب الدراسات العليا بالإفادة من ممارسات بعض الدول، استخدمت الدراسة المنهج المقارن، وتوصلت إلى معالم المقترح بالاعتماد على العناصر التالية: أهداف المقترح، الفلسفة التي يرتكز عليها، متطلبات تنفيذ المقترح ، أساليب تنفيذ المقترح ، مراحل تنفيذ المقترح ، إجراءات تقويم المقترح ، إجراءات التحسين المستمر . كما أوصت الدراسة بتوفير التمويل اللازم لتنفيذ المقترح ، وتعميمه على الجامعات المصرية، كما أوصت الدراسة بمزيد من الاهتمام بممارسات الأمن السيبراني بالجامعات المصرية حيث تقتصر الممارسات على بعض الجهود الفردية المبعثرة لعرض بعض برامج الأمن السيبراني وبعض البرامج التدريبية ذات الهدف الربحي للمستفيدين الخارجيين.

٥. دراسة عرفه ، والعراقي (٢٠٢١)

هدفت الدراسة الحالية إلى التعرف على مستوى الوعي الغـذائي والـصحي وبعـض مهارات الأمن السيبراني لدى طلبة قسم الاقتصاد المنزلي بكلية التربية النوعية جامعـة دميـاط خلال جائحة كورونا. استخدمت الدراسة المنهج الوصفي . كما استخدمت الاستبانة كأداة لجمـع المعلومات من أفراد العينة . أوضحت النتائج وجود فروق ذات دلالة إحصائية عنـد مـستوى ($p\leq0.01$)بين متوسط درجات الطلاب في الاختبارين القبلي والبعدي للتوعية التغذية والـصحية لصالح الاختبار البعدي. كما توجد فروق ذات دلالة إحصائية عند مستوى ($p\leq0.01$) بين متوسط درجات الطلاب في الاختبارين القبلي والبعدي لبعض مهارات الأمن السيبراني لصالح الاختبـار البعدي. وشددت الدراسة على أهمية تحسين الوعي الغذائي والصحي والتوعية بالأمن الـسيبراني بين طلبة الجامعات في ظل جائحة كورونا.كما أوصت الدراسة بتفعيل ثقافة الأمـن الـسيبراني بالجامعات المصرية لتطوير أسلوب مواجهتها للتهديدات السيبرانية.

٦. دراسة الكردي (٢٠٢١)

هدفت الدراسة إلى التعرف على واقع ممارسات الأمن السيبراني بالجامعات الفلـسطينية بالتركيز على جامعة النجاح ، استخدمت الدراسة المنهج الوصفي ، وتوصلت الدراسة أن مستوى الأمن السيبراني كان متوسطاً، وأن هناك فروق دالة حول واقع ممارسات التعليم الإلكترونـي وذلك لذوي الخبرة من ١٠-٢٠ عاماً ، أوصت الدراسة بضرورة تطـوير ممارسـات الأمـن السيبراني من خلال زيادة البرامج التدريبية وورش العمل التي تقـدم للقيـادات والمرؤوسـين ، وضرورة التزام القيادة الجامعية بتوفير الموارد المالية اللازمة لاستحداث برامج الأمن السيبراني في الحرم الجامعي .

٧. دراسة الخضري (٢٠٢٠)

هدفت الدراسة إلى تحديد درجة تـوافر الـوعي بـالأمن الـسيبرانى وكـذلك الـذكاء الاصطناعي لدى طلاب الجامعات السعودية. استخدمت الدراسة المـنهج الوصـفي. وتوصـلت الدراسة إلى أن درجة وعي الطلاب بالأمن السيبراني والذكاء الاصـطناعي جـاءت متوسـطة. أوصت الدراسة بضرورة الاهتمام بزيادة الوعي لدى الكوادر البشرية بالجامعات السعودية بالأمن السيبراني والذكاء الاصطناعي . وضرورة إعداد وتقديم برامج تدريبية للقيادات وأعضاء هيئـة

التدريس والموظفين الإداريين والطلاب للتدريب على كيفية تطبيق إجراءات الأمن السيبراني . وضرورة تدريب تلك الفئات على كيفية تطبيق منهجية الذكاء الاصطناعي .

٨. دراسة السمحان (٢٠٢٠)

هدفت الدراسة للتعرف على آليات تطبيق إجراءات الأمن السيبراني بإحدى الجامعات السعودية –جامعة الملك سعود أنموذجاً . استخدمت الدراسة المنهج الوصفي ، كما استخدمت الاستبانة كأداة لجمع المعلومات. توصلت الدراسة إلى من أبرز المتطلبات : تدريب الكوادر البشرية على التطبيق ، توافر برامج حديثة ومتطورة للأمن السيبراني ، توفير الموارد المالية للتطبيق ، التزام القيادة بالتطبيق. أوصت الدراسة بضرورة نشر ثقافة الأمن السيبراني على كافة الموارد البشرية بالجامعة مع التركيز على الطلاب ، كما أوصت الدراسة بضرورة توعية القيادات الأكاديمية الجامعية بأهمية الأمن السيبراني وتطبيق إجراءاته بالجامعة.

٩. دراسة شرف (٢٠١٩)

هدفت الدراسة إلى توضيح أبرز معوقات تطبيق التعليم الإلكتروني بجامعة الأقصى بفلسطين. استخدمت الدراسة المنهج الوصفي ، كما استخدمت الدراسة الاستبانة كأداة لجمع المعلومات . توصلت الدراسة إلى أن أبرز الصعوبات التي واجهت تطبيق التعليم الالكتروني كانت : نقص التدريب على تطبيق التعليم الالكتروني ، ضعف الاتصال بشبكة الانترنت ، نقص التمويل خاصة فيما يتعلق بالصيانة الدورية على منصات التعليم الالكتروني . أوصت الدراسة بضرورة وضع خطة لتطبيق التعليم الالكتروني بالجامعة ، ووضع خطة لصيانة برامج ومنصات التعليم الالكتروني بالجامعة .

١٠.دراسة القحطاني (٢٠١٩)

هدفت الدراسة إلى التعرف على آراء طلاب الجامعات السعودية على مدى وعيهم بإجراءات الأمن السيبراني . استخدمت الدراسة المنهج الوصفي. كما استخدمت الدراسة الاستبانة كأداة لجمع المعلومات. توصلت الدراسة إلى أن درجة وعي الطلاب بمفهوم الأمن السيبراني ، كما توصلت الدراسة إلى توافر معوقات للتطبيق الناجح لاستراتيجية الأمن السيبراني ومنها عدم اللحاق بالتطورات الحادثة في مجال الأمن السيبراني ، استخدام برامج قديمة في التعامل مع جرائم أمن المعلومات . أوصت الدراسة بضرورة توعية الطلاب بكيفية تطبيق إجراءات الأمن السيبراني بالجامعة ، وضرورة تطوير البنية التحتية بالجامعة لاحتضان

الاتجاهات الحديثة في الأمن السيبراني التوعية، ضرورة تغليظ عقوبات السرقة والاحتيال على المنصات الالكترونية بالجامعة .

١١.دراسة العريشي، والدوسري (٢٠١٨)

هدفت الدراسة إلى تحديد أدوار المؤسسات الجامعية في تفعيل ثقافة وقيم أمن المعلومات ، استخدمت الدراسة المنهج الوصفي . توصلت الدراسة إلى أن من أبرز أدوار المؤسسات الجامعية توعية الطلاب بأهمية أمن المعلومات ، وضع وتطوير برامج للتدريب على كيفية تطبيق أمن المعلومات ، وضع أسس لحوار إيجابي بين خبراء أمن المعلومات والطلاب لمناقشة القضايا التي تسهم في فهم الطلاب لأمن المعلومات ، إعداد دراسة بحثية لتحديد احتياجات ومتطلبات الطلاب من أمن المعلومات ، تضمين المقررات الدراسية بقضايا أمن المعلومات وإجراءات تطبيقها في الحرم الجامعي . وقد أوصت الدراسة بضرورة تفعيل ثقافة الأمن السيبراني لدى القيادات الأكاديمية الجامعية.

ثانياً الدراسات الأجنبية

١- دراسة(2021) Alexei

هدفت الدراسة الحالية إلى تحديد أبرز التهديدات الإلكترونية السيبرانية لمؤسسات التعليم العالي في بعض مؤسسات التعليم العالي حول العالم. استخدمت الدراسة المنهج الوصفي. توصلت الدراسة إلى أن أبرز التهديدات كانت : هجمات البرامج الضارة على معلومات مؤسسات التعليم العالي، وهجمات ما يسمى بالتصيد الاحتيالي بغرض الحصول على النفع المالي إضافة إلى ضعف تأمين شبكات المؤسسات ضد التهديدات السيبرانية . أوصت الدراسة بتفعيل دور الموارد البشرية في وضع استراتيجيات الأمن السيبراني في مؤسسات التعليم العالي .

٢- دراسة(2021),Naidu ,et al

لوباء كوفيد -١٩ تأثير كبير على طريقة تنظيم الدراسات في مؤسسات التعليم العالي (HEIs). منذ مارس ٢٠٢٠ ، كانت الطريقة الوحيدة لمواصلة العملية التعليمية هي التعلم عن بعد. لذلك ظهرت بكثرة التهديدات الالكترونية. ركز البحث على تحديد نوع الاعتداءات التي لها أكبر تأثير على الأصول المعرفية والبشرية والأكاديمية والإدارية بمؤسسات التعليم العالي ، بالإضافة إلى تقديم توصيات لتحسين الأمن السيبراني في بيئات التعلم الإلكتروني. تتضمن

الممارسات الموصى بها بشكل متكرر تطوير ممارسات الأمن السيبراني ، تفعيل دور المـــوارد البشرية في تطوير تلك الممارسات ، تطوير برامج الحماية.

٣- دراسة Pavel , et al,(2021)

كانت مؤسسات التعليم العالي (HEIs) دائمًا هدفًا للهجمات السيبرانية بـــسبب أصـــول المعلومات التي تمتلكها. أدى الانتقال إلى الدراسة عبر الإنترنت كنتيجة للقيود المفروضـــة فـــي ربيع عام ٢٠٢٠ إلى زيادة تهديدات الأمن السيبراني للأوساط الأكاديمية بسبب نقاط الضعف في منصات التعلم عبر الإنترنت وتطبيقات مؤتمرات الفيديو. هدفت الدراسة الحاليـــة إلـــى تحليـــل تحديات الأمن السيبراني لمؤسسات التعليم العالي في دولـــة مولـــدوفا(Moldova) اســـتخدمت الدراسة المنهج الوصفي ، أشارت نتائج الدراسة أن مؤسسات التعليم العالي في مولدوفا مستهدفة من قبل الهجمات الإلكترونية وكذلك الدولية ، وأن طبيعة التهديدات كانت تتمثـــل فـــي البـــرامج الضارة ضد الملفات الهامة في المجالات البحثية والإدارية. أوصت الدراسة بوضع استراتيجيات لتلك المؤسسات لحمايتها من أخطار التهديدات السيبرانية، إضافة إلى نشر ثقافة الأمن الـــسيبراني في تلك المؤسسات.

٤- دراسة Shafik ,2021

تطرح هذه المقالة إشكالية عدم الاهتمام بمجال الأمن السيبراني كمجال للبحث والتحليـــل في قطاع التعليم العالي، على الرغم من الارتفاع الهائل في التهديدات الإلكترونية السيبرانية ضـــد الكليات والجامعات في جميع أنحاء العالم. هدفت الدراسة إلى استكـــشاف التعقيـــدات الإداريـــة بمؤسسات التعليم العالي وتأثيرها السلبي على مواجهة التهديدات السيبرانية باعتبار ذلـــك تحـــديًا لتلك المؤسسات. استخدمت الدراسة المنهج الوصفي. وتوصلت الدراسة إلى أن التعقيدات الإدارية التي تمثل تهديداً للأمن السيبراني للجامعة تتمثل في المركزية الخانقة ، إصدار الأوامر والنواهي ، الخوف الشديد من مخالفة التعليمات ، العقاب الصارم ضد الموظفين . أوصت الدراسة بتطبيق اللامركزية في مؤسسات التعليم العالي ، والسماح للموظفين بالمشاركة في اتخاذ القرارات ، كما أوصت الدراسة بضرورة وضع تدابير محتملة لتحسين مرونة قطاع التعليم العالي ضد التهديدات الإلكترونية السيبرانية.

٥- دراسة Garba,et al (2020)

هدفت الدراسة إلى استكشاف مدى وعي الطلاب وإدراكهم وحماسهم لتعلم الأمن السيبراني في الجامعات النيجيرية . استخدمت الدراسة المنهج الوصفي. أشارت النتائج إلى أن الطلاب لديهم معرفة أساسية بالأمن السيبراني ، لكنهم ليسوا على دراية بكيفية حماية بياناتهم .كما أن معظم الجامعات ليس لديها برنامج توعية نشط للأمن السيبراني لتحسين معرفة الطلاب حول كيفية حماية أنفسهم من أي تهديدات .أظهر الدراسة أيضاً أن الطلاب الذين شملهم الاستطلاع أبدوا اهتمامًا بمعرفة المزيد عن الأمن السيبراني. أوصت الدراسة بضرورة نشر ثقافة الأمن السيبراني في الجامعات النيجيرية لزيادة إدراك طلابها خاصة ، ومواردها البشرية عامة بأبعاد تلك الثقافة وعناصرها وأهميتها .

٦- دراسة Catota,et al,(2019)

تعتمد القدرة على منع الهجمات الإلكترونية السيبرانية ضد النظام التعليمي على مدى توافر البنية التحتية الحيوية متمثلة في موارد بشرسة ماهرة للتعامل مع تلك الهجمات . هدفت الدراسة إلى استكشاف التحديات التي يواجهها نظام التعليم العالي في الإكوادور في النهوض باستراتيجية الأمن السيبراني. استخدمت الدراسة المنهج الوصفي . وتوصلت إلى أن التحديات التي تواجهها استراتيجية الأمن السيبراني تشمل: قلة الموارد البشرية المتخصصة في مجال الأمن السيبراني ، ضعف البنية التحتية ، قصور في التدريب والتأهيل . أوصت الدراسة بتقديم مبادرات لتطوير ممارسات الأمن السيبراني في مؤسسات التعليم العالي بدولة الإكوادور تتلخص في مبادرة لتعزيز تدريب الموارد البشرية على كيفية تطبيق إجراءات لأمن السيبراني ، مبادرة دعم قدرات البحث (والتطوير) و الوعي بالأمن السيبراني.

٧- دراسة Muniandy,et al,(2017)

هدفت الدراسة إلى تحليل سلوك الطلاب ببعض الكليات التي تقع في شمال ماليزيا (Malaysia) تجاه ممارسات الأمن السيبراني. استخدمت الدراسة المنهج الوصفي. وتوصلت الدراسة إلى أن سلوك الطلاب بشكل عام تجاه ممارسات الأمن السيبراني كان متوسطاً، وأرجعت الدراسة ذلك إلى قلة البرامج التدريبية المقدمة للطلاب ، عدم مشاركة الطلاب في تنفيذ ممارسات الأمن السيبراني بالجامعة . أوصت الدراسة بتكثيف البرامج التدريبية المقدمة للطلاب والتركيز على كيفية مواجهة التهديدات السيبرانية، كما أوصت بمزيد من الاهتمام بمجال الأمن السيبراني

في الجامعات الماليزية من خلال البرامج التدريبية، وضع رؤى لكيفية تفعيل ممارسات الأمن السيبراني، مشاركة الموارد البشرية في تفعيل ممارسات الأمن السيبراني.

يتضح مما سبق اتفاق الدراسات السابقة جميعها على أهمية الأمن السيبراني في الجامعات حيث تعمل على وقايتها وحمايتها من التهديدات السيبرانية المختلفة ، كما اتفقت على أن مجال الأمن السيبراني على الرغم من أهميته إلا أنه مجال يحتاج إلى مزيد من الاهتمام كما أكدته دراسات (سراج ،٢٠٢٢) ؛ (شعبان ،٢٠٢١) ؛ (عرفه ، والعراقي ،٢٠٢١) ؛(٢٠٢١, Shafik)، كما اتفقت الدراسات على استخدام المنهج الوصفي ؛ وذلك لملائمته لطبيعتها ؛ من حيث جمع المعلومات عن موضوع الدراسة وتنظيمها وتحليلها، والإفادة منها في تطوير إجراءات وممارسات الأمن السيبراني بالجامعات. بينما اختلفت الدراسات السابقة مع الدراسة الحالية في أن الدراسات السابقة لم تتعرض إلى الدور القيادي المؤثر والهام في تفعيل ممارسات الأمن السيبراني بالجامعات واقتصرت على عرض ممارسات الأمن السيبراني بوجه عام دون التعرض لأدوار القيادات الأكاديمية في وضع وتنفيذ وتقويم تلك الممارسات وهي ما عملت الدراسة الحالية على تحقيقه لسد هذه الفجوة البحثية والمساهمة في تطوير أدوار القيادات الأكاديمية الجامعية في تحسين ممارسات الأمن السيبراني بالجامعات المصرية. استفادت الدراسة الحالية من الدراسات السابقة في عرض الإطار النظري وتوضيح مشكلة الدراسة وتوجهاتها، إضافة إلى التعرف على أبرز النتائج التي توصلت إليها تلك الدراسات لتبدأ الدراسة الحالية مما انتهت إليه الدراسات السابقة.

مبررات اختيار القيادات الأكاديمية بالجامعات الأمريكية للإفادة منها

١- أشار تقرير للبنك الدولي بالعام 2021 إلى أن الجامعات الأمريكية هي أكثر الجامعات على مستوى العالم التي يقع بها هجمات سيبرانية ، وأن مستوى نجاح الجامعات الأمريكية في صد هذه الهجمات يتعدى ٩٠,٢% وهي نسبة مرتفعة تشير إلى قدرات متميزة لتلك الجامعات ؛ وأرجع التقرير أحد عوامل النجاح إلى فهم القيادات الأكاديمية الجامعية لطبيعة أدوارها في مواجهة تلك الهجمات ، وأن ممارساتها يغلب عليها السرعة والدقة والتعاون .(Callejas,et al,2021)

٢- تميز الخبرة الجامعية الأمريكية وسمعتها الرصينة في تطوير نظم للحماية والوقاية من التهديدات السيبرانية ؛ الأمر الذي جعلها محط اهتمام كثير من جامعات العالم والتي

تطلب دعمها ومساعدتها في تطوير نظم وإجراءات الأمن السيبراني لديها ؛ ومن أبـــرز الدول التي تتعاون التي تتعاون جامعاتها مع الجامعات الأمريكية في تطوير نظم الأمـــن السيبراني : دول الخليج العربي كالمملكة العربية السعودية، والإمارات العربية المتحـــدة ، والدول الأفريقية كالمغرب ، وجنوب أفريقيا ، وكينيا .(Fouad ,2021)

٣- العلاقات الطيبة بين الجامعات المصرية والأمريكية والتـــي تكلـــل باتفاقيـــات تعـــاون وزيارات ومشاريع مشتركة ، الأمر الذي يمكن معه استثمار تلك العلاقات في تطـــوير أدوار القيادات الأكاديمية في تعزيز ممارسات الأمن السيبراني بالجامعـــات المـــصرية وبالإفادة من خبرة القيادات الأكاديمية بالجامعات الأمريكية .

المحور الأول: الإدارة الالكترونية

برزت الإدارة الالكترونية كمدخل إداري حديث يعتمد على الوسائل التكنولوجيـــة فـــي ممارسة المهام والمسؤوليات الجامعية؛ ومن ثم البعد عن الأساليب التقليدية الروتينية الورقية التي كانت تتطلب وقتاً وجهداً مضاعفاً لتنفيذ تلك المهام. وقد لاقت الإدارة الالكترونية نجاحاً ملموســـاً خاصة خلال أوقات تفشي جائحة كورونا حيث اعتمد العمل الجامعي في تنفيذ كثير مـــن مهامـــه على الإدارة الالكترونية وأدواتها في استقبال وإرسال البيانات والمعلومات إلى المستفيدين داخـــل وخارج الجامعات.

مفهوم الإدارة الالكترونية

تعرف بأنها نظام حديث يعتمدُ على التكنولوجيا (التقنية) الإلكترونيّة في تنفيذ الأعمـــال الإدارية والفنية والأكاديمية، ويهدفُ إلى تغيير الإدارة (الورقية) التقليديّة إلى إدارةٍ تعتمدُ علـــى استثمار إمكانات الحاسب الآلي وتطبيقاته. .(Abdulrahman and Omar,2018) . كما أنهـــا استخدام تقنية المعلومات لتحسين إدارة الجامعات من خلال تبسيط العمليات والإجراءات وتحسين تدفق المعلومات داخل وحداتها وأقسامها. (Alkhsabah, 2017)

كما ينظر إليها على أنها حزمة برامج مصممة لإدارة المعلومات والسجلات الإلكترونية ضمن سير عمل الجامعة باستخدام تقنيات مختلفة، بحيث يتيح للمستخدم إدارة إنشاء الـــسجلات وتخزينها والتحكم فيها. ويمكن أن تساعد في أتمتة العمليات وزيادة كفائتها. كما ينظر إليها علـــى أنها إدارة حديثة تستخدم وسائل التقنية لتنفيذ المهام والمـــسؤوليات الجامعيـــة. Al-Ma’aitah, (2019)

إذن تعد الإدارة الالكترونية مدخل إداري حديث يتوائم مع متطلبات عصر المعلومات والاتصالات ، بحيث يعمل على الوفاء بتوقعات المستفيدين من الخدمات الجامعية مع الاستثمار الأمثل للموارد المادية و البشرية في إطارها الالكتروني فتبتعد عن الأدوات التقليدية للإدارة الجامعية إلى أدوات تكنولوجية تستخدم الحاسوب والشبكات والبرامج التقنية والانترنت في تنفيذ مهامها وأعمالها المختلفة.

أهداف الإدارة الالكترونية

الإدارة الالكترونية أهدافها محددة في العمل الجامعي؛ والتي من أبرزها: Alkhsabah, (2017)(Al-Ma'aitah, 2019) .(نشأت ، ٢٠٢١)

١- تطوير العمل الجامعي، بما يؤدّي إلى تغيير الأدوات التقليدية المُستخدمة من أوراق ومستندات وأقلام ودفاتر إلى أدواتٍ تكنولوجية إلكترونيّة.
٢- تطوير مستوى جودة الخدمة المقدمة إلى المستفيدين بالشكل الأمثل والأفضل.
٣- السرعة في إنجاز المهام وحل المشكلات التي تواجه العمل.
٤- تقليل كلفة تنفيذ المهام والأعمال والمسؤوليات؛ فلم يعد هناك حاجة إلى شراء أو صيانة أو استبدال للأدوات التقليدية.
٥- زيادة الإنتاجية للموارد البشرية والجامعة بشكل عام نتيجة اختصار كثير من الإجراءات الروتينية وتركيز الجهود نحو تحقيق الأهداف المرسومة.
٦- تحسين وتطوير التعاون بين الموارد البشرية بالجامعة من خلال خلق مناخ من الحوار والتفاعل الدائم فيما بينهم.

يتضح مما سبق تعدد أهداف الإدارة الالكترونية، وهي تشير في مجملها إلى البعد عن الأساليب والطرق الورقية في تنفيذ المهام الجامعية إلى أدوات ووسائل إلكترونية تيسر من تنفيذ تلك المهام؛ مما يساهم في تقليل الوقت والجهد والتكلفة في تحقيق الأهداف ويطور من العلاقات بين وحدات الجامعة من جانب وبين الجامعة وقطاعات المجتمع من جانب آخر.

متطلبات الإدارة الالكترونية

من أبرز متطلبات الإدارة الالكترونية؛ ما يلي: Al-Jamal and Abu-Shanab, (2016) (الروقي ، ٢٠١٦) (Abdulrahman and Omar,2018)

١. بنية تحتية تكنولوجية؛ تشمل شبكة اتصالات سلكية ولاسلكية بحيث يكون لـــديها القـــدرة على استقبال ونقل المعلومان والبيانات بين كافة وحدات وأقسام الجامعة، وكافة قطاعات المجتمع.
٢. وسائل الكترونية نستطيع من خلالها ممارسة مهام الإدارة الالكترونية والتي تشمل أجهزة الحاسب الآلي (الشخصي والمحمول) الهواتف الشبكية وغيرها من الوسائل.
٣. توافر الاتصال بالشبكة العنكبوتية (الانترنت) لاستقبال وإرســـال البيانـــات والمعلومـــات بالسرعة والدقة المطلوبة ؛ وذلك للمستفيدين الداخليين والخارجيين .
٤. تنمية قدرات ومهارات للموارد البشرية بالجامعة؛ من خلال البرامج التدريبيـــة المقدمـــة والتي تجعل تلك الموارد على معرفة بكل جديد بآليـــات الإدارة الالكترونيـــة ووســـائلها المختلفة.
٥. توافر التمويل المناسب لتطوير ممارسات الإدارة الالكترونيـــة؛ مـــن تـــدريب للمـــوارد البشرية وشراء وصيانة للأجهزة.
٦. التزام القيادة الجامعية بدعم وتطوير ممارسات الإدارة الالكترونية والاقتنـــاع بجـــدواها وفوائدها لتحسين جودة الخدمة المقدمة للمستفيدين.
٧. توافر برامج حماية للمعلومات والبيانات الجامعية من خطر الاختراق والسرقة وهو مـــا تسمى ببرامج الأمن السيبراني.
٨. توافر التشريعات واللوائح القانونية التي تيسر وتقنن من ممارســـات الإدارة الالكترونيـــة بالجامع

لاشك أن تلك المتطلبات تعمل على نجاح تطبيق الإدارة الالكترونية بالجامعـــة ؛ ممـــا يساهم في سرعة ودقة العمل الأمر الذي يترتب عليه رضا المستفيدين الـــداخليين والخـــارجيين ، هذا إضافة إلى تقليل الأخطاء في تنفيذ المهام بل وسرعة تداركها وعلاجها ، وتطوير العلاقـــات بين الموارد البشرية بالجامعة وزيادة الترابط بين وحداتها وأقسامها .

وظائف الإدارة الالكترونية

يوجد العديد من أنظمة الإدارة الالكترونية. يوفر كل منها وظائف مـــصممة خصيـــصاً لاحتياجات محددة للجامعات، وبحيث تتضمن هذه الأنظمة الوظائف الأساسية التالية: (الروقـــي ، ٢٠١٦) (Alkhsabah, 2017)(Al-Ma’aitah, 2019) (نشأت ، ٢٠٢١) :

١- التحكم في الأمان : هذه الميزة ضرورية للتحكم في الوصول إلى المعلومات. يجب أن يكون للنظام آلية لحماية المستندات المحظور أتاحتها للجمهور وتلك المتاحة للاطلاع عليها.

٢- الإضافة والتعيين والتحكم في الإصدار : يجب أن يسمح نظام الإدارة الإلكترونية للمستخدمين بإضافة مستندات إلى النظام وتعيين مستندات وتطويرها.

٣- التقاط البيانات الوصفية واستخدامها : يجب أن يسمح نظام الإدارة الإلكترونية الحديث للمستخدم بالتقاط واستخدام البيانات الوصفية المناسبة وفقًا لاحتياجات الجامعة.

٤- التخزين : يوفر نظام الإدارة الإلكترونية القدرة على تخزين البيانات والمعلومات مع توافر الحماية لها.

٥- التحويل التلقائي : توفر هذه الوظيفة للمستخدم التحويل التلقائي للمستند من تنسيق ملف إلى آخر على سبيل المثال من مستند (Word) إلى ملف (PDF) .

تعد هذه الوظائف أساسية لتحقيق أهداف الإدارة الإلكترونية؛ ومن ثم بدونها لن تصبح هذه الإدارة فعالة في تحقيق ما خطط لها. وكل وظيفة من هذه الوظائف لها مهام محددة لا تتقاطع ولا تتعارض مع غيرها من المهام، كما أن الوظائف مرتبطة ومتشابكة مع بعضها فنياً وإدارياً لتحقيق الهدف من تطبيقها.

الاتجاهات الحديثة في الإدارة الالكترونية

نتيجة للتطور الحادث في مجال الإدارة الالكترونية على مستوى المؤسسات عامة والجامعات خاصة ؛ فقد اتضح عدداً من الاتجاهات الحديثة التي تعبر عن تحسين في أساليبها وإجراءات تنفيذها للمهام والأنشطة المختلفة ؛ ومن أبرز تلك الاتجاهات :

- المنصات الالكترونية الرقمية

لقد ولت الأيام التي كانت تنفيذ المهام الأكاديمية والإدارية تتم بالطرق التقليدية الورقية، حيث كانت الأسلوب الرئيس بل والوحيد في كثير من الأحيان. لكن الآن تتمتع التكنولوجيا الرقمية بالفرصة غير المقيدة، لكي تحل محل الأساليب القديمة التقليدية؛ مما يوفر للجامعات ثروة من الفرص لتنفيذ مهامها بأساليب بسيطة عن طريق بضع نقرات على الماوس. **(Almarashdeh and Alsmadi, 2017)**

يمكن أن تكون المنصة الرقمية(**digital electronic platform**) بمثابة نظام لإدارة المهام والمسؤوليات الجامعية. بل يمكن النظر إليها كأداة لإنشاء بيئة عمل افتراضية. بينما تختلف كل منصة من حيث الوظيفة والميزات، يمكن لجميع المنصات الرقمية أن تدعم جميع أنواع الأعمال الأكاديمية والإدارية، عبر الإنترنت. (Almarashdeh and Alsmadi, 2017) نظرًا لأن الإنترنت والتكنولوجيا الرقمية أصبحتا جزءًا لا يتجزأ من حياتنا العامة والعملية، فقد أصبح العمل أيضًا عبر الإنترنت، مما يفرض حلول تقنية متخصصة لدعم العمل عبر الإنترنت .أعطت جائحة كورونا دفعة كبيرة للعمل عبر الإنترنت. ونتيجة لذلك، فإن معظم الكليات والجامعات والمؤسسات المهنية قد اعتمدت بالفعل أو هي بصدد اعتماد المنصات الالكترونية الرقمية لدعم العمل الجامعي .

مفهومها

تشير المنصة الرقمية إلى أنها تقنية تكون عادةً في شكل برنامج أو تطبيق يتم تشغيله على شبكة الانترنت ويتم استخدامه لأداء نشاطات الجامعة المختلفة. (Alquda ,et al,2021) كما ينظر إليها على أنها برنامج تكنولوجي مستخدم لدمج وتبسيط وتنفيذ العمليات الأكاديمية والإدارية بالجامعة. وتعرف أيضاً بأنها أداة إلكترونية للتواصل بين الموارد البشرية بأقسام وإدارات وكليات الجامعة فيما بينها لتبادل المعلومات والبيانات التي يتطلبها ممارسات المهام المختلفة. (Catota,et al,2019).

ومن ثم فإنها أداة للتواصل مع المستفيدين للرد على استفساراتهم وأسئلتهم. وتعتبر وسيلة لإنشاء بيئة عمل افتراضية للقيادات والمرؤوسين لتبادل النقاشات والايضاحات والاستفسارات والمعلومات والبيانات التي من شأنها تطوير ممارسات العمل الجامعي والتقليل من المشكلات التي تقع أثناء تأدية المهام.

وظائفها ومميزاتها

تتعدد الوظائف والمميزات للمنصات الالكترونية؛ كما يلي:

١- سهولة الوصول إلى المعلومات والبيانات

تتيح المنصة الرقمية الوصول إلى مكتبة كاملة من الموارد عبر الإنترنت. تم تصميمها لتنظيم المعلومات بطريقة تجعلها في متناول جميع المستخدمين (المصرح لهم بذلك) . يمكن لجميع الموارد البشرية الوصول إلى المعلومات في أي وقت ومن أي مكان بمساعدة الإنترنت،

سواء كان ذلك جهاز كمبيوتر محمول أو جهاز لوحي أو هاتف ذكي. ثم هناك أيضًا خيار تنزيل المواد والوصول إليها للاستخدام دون اتصال بالإنترنت. Abdulrahman and (Omar,2018).

٢- محتوى حديث

تسمح المنصة للموارد البشرية بالجامعات بتحديث المعلومات والبيانات بشكل فعال فتوفر كثيراً من التكلفة والسرعة والدقة. إضافة إلى قابليتها على إضافة مواد وموارد إضافية، والتي يمكن للمستخدمين الوصول إليها لدعم ممارساتهم لمهامهم. (Alquda ,et al,2021)

٣- التقارير المتقدمة

تسمح المنصات للموارد البشرية بإنشاء وتخصيص وتنزيل التقارير التي توفر رؤى حول تقدم العمل أو مستوى إنجاز المهام أو تنفيذ الأنشطة وما إلى ذلك.

٤- تعلم الوسائط المتعددة

باستخدام المنصات الرقمية، يمكن إنشاء محتوى وسائط متعددة لإشراك كافة الموارد البشرية، ودمجهم في الأنشطة الجامعية، وتحفيزهم على السرعة في إنجاز المهام . محتوى الوسائط المتعددة قد يكون على شكل رسائل الكترونية، فيديوهات لاجتماعات، وصور وتسجيلات صوتية. (أشرف ،٢٠١٩)

٥- قنوات اتصال جديدة

تعمل المنصات كقنوات اتصال بين الرؤساء والمرؤوسين في تبادل المعلومات وتقديم الاستفسارات وتلقي الايضاحات. يمكن للموارد البشرية استخدام المنصات في الاجتماعات، المناقشات عبر الانترنت حول الموضوعات المختلفة ، التواصل مع زملائهم في الكلية بل والجامعة على الفور وحل المشكلات عند ظهورها. مما يجعل بيئة العمل أكثر تعاونية وتفاعلية وشخصية. (Al-Jamal and Abu-Shanab, 2016)

٦- الوصول إلى مصادر وموارد العمل

لا ينتهي العمل أبدًا من خلال المنصة الرقمية. فيمكن للموارد البشرية الوصول إلى مواردهم عبر الإنترنت على مدار ٢٤ ساعة في اليوم، ٣٦٥ يومًا في السنة. يمكنهم حتى إجراء المعاملات الإدارية وإرسالها للرؤساء بأي وقت. يساعد الوصول إلى موارد العمل (المعلومات

والبيانات) في جميع الأوقات على تعزيز العمل حتى بعد ساعات العمل العادية. Al-Jamal and (Abu-Shanab, 2016)

نظرًا لأن التكنولوجيا صارت ضرورة ماسة للتيسير من تنفيذ المهام والمسؤوليات المختلفة، يصبح من الضروري للجامعات تسخيرها لصالحها. حيث تعتمد الجامعات الآن بشكل متزايد على المنصات الالكترونية الرقمية في تنفيذ المهام الأكاديمية والإدارية. خاصة وأنها توفر وصولاً على مدار الساعة إلى موارد العمل المختلفة، وفي أي وقت ومكان . كما أنها توفر مجموعة من أدوات الاتصال للتواصل بين الموارد البشرية داخل وخارج الجامعة.

ثانياً : برامج الذكاء الاصطناعي

ينسب أول استخدام للذكاء الصناعي(Artificial intelligence) للعام ١٩٥٦ بكلية دارتموث "Dartmouth College " بالولايات المتحدة الأمريكية إلا أنه دخل بصورة مكثفة في عالم التعليم العالي في مطلع التسعينات أيضاً بالولايات المتحدة الأمريكية كما يشير (Abdulrahman and Omar,2018) . وفقًا لـ .(Ahmed, et al,2019)، تجاوز الذكاء الاصطناعي في أسواق التعليم العالي مليار دولار في عام ٢٠٢٠ ومن المتوقع أن ينمو بمعدل سنوي مركب يزيد عن ٤٠٪ بين عامي ٢٠٢١ و ٢٠٢٧ . مع كل هذه الضجة، هناك قدر كبير من الارتباك حول ماهية الذكاء الاصطناعي ، والتأثير الذي قد يكون له على تنفيذ الأنشطة المختلفة بمؤسسات التعليم العالي.

مفهوم الذكاء الاصطناعي

يُعرّف الذكاء الاصطناعي بأنه تطوير أنظمة الكمبيوتر التي تستخدم المنطق والسمات البشرية الأخرى لأداء المهام الجامعية بشكل مستقل، ويوفر طرقًا للجامعات لتبسيط العمليات وسير العمل من خلال الأتمتة .(Ahmed, et al,2019)

كما تعرف بأنها استخدام واستثمار الاتجاهات الحديثة في المجالات التقنية لاستشراف آفاق وتوجهات الجامعات على المدى القصير والطويل .(Alquda ,et al,2021) كما ينظر إليها على أنها استثمار أنظمة الكمبيوتر والحواسب التقنية المتقدمة في تطوير الممارسات الجامعية ، وتحليل وتفسير البيانات والتنبؤ باتجاهاتها المستقبلية . (Alqudah and Muradkhanli, 2021)

أهداف وأهمية الذكاء الاصطناعي

يمكّن التعلم الآلي، وهو مجموعة فرعية من الذكاء الاصطناعي، أنظمة الكمبيوتر من التحليل والتعلم من مجموعات البيانات الواسعة لإكمال العمليات الجامعية العادية و المعقدة (Ahmed, et al,2019) . وفقًا لـ (Fouad,2021) هذه الأنظمة مبنية على شبكات عصبية – مجموعات كثيفة من المسارات الحسابية التي تنقل البيانات وتفسرها وتعالجها لتيسر من ممارسة الأنشطة الجامعية. كما يمكن الذكاء الاصطناعي إحداث تغيير كبير في الكليات والجامعات من جميع الأنواع والأحجام. عند تسخيرها لتعزيز الممارسات الأكاديمية والإدارية والبحثية ،(Hujran et al,2015)يمنح الذكاء الاصطناعي الجامعات القدرة على توقع اتجاهات تسجيل الطلاب وتحسين جهود التوظيف ورفع الأداء الأكاديمي والإداري. (Alqudah and Muradkhanli, 2021) بل وتوقع مسار واتجاهات البحوث المستقبلية بناءً على النتائج الواردة في التقارير المتنوعة .

طرق تأثير الذكاء الاصطناعي على الجامعات

تشير دراسات .(Alqudah and Muradkhanli, 2021) (Ahmed, et al,2019) أن الذكاء الاصطناعي قد يؤثر على الجامعات بالطرق التالية:

- تطوير الإجراءات الإدارية من خلال وضع نماذج مبتكرة لإنجاز تلك الإجراءات بالاعتماد على ممارسات مبتكرة أي الابتكار في طرق تنفيذ تلك الإجراءات اختصاراً للوقت والجهد .
- تطوير الأنشطة البحثية من خلال التنبؤ بالاتجاهات المستقبلية للبحوث العلمية ، وتطوير القدرة على التفسير والتحليل للبيانات والمعلومات البحثية.
- ستتغير ممارسات انتقاء واختيار الطلاب .ستكون الكليات والجامعات قادرة على تركيز جهودها بشكل أفضل من خلال إنشاء خوارزميات يمكنها التنبؤ بالمتقدمين الذين من المرجح أن يتم قبولهم وتسجيلهم. يمكن أن تحدد هذه الخوارزميات أيضًا الطلاب المسجلين الذين من المرجح أن يتقدموا ويتخرجوا ويصبحوا خريجين بارعين. (Hujran,et al,2015)
- ستصبح عملية القبول في الكليات أسرع وأكثر تخصيصًا .من خلال أتمتة العديد من الأنشطة الإدارية أثناء عملية القبول، بما في ذلك إجراءات التأشيرة واختيار سكن

الطلاب وتسجيل الدورات، ستكون الكليات والجامعات قادرة على توفير تجارب قابلة للتخصيص للطلاب .

- ستكون جهود الاحتفاظ بالطلاب أكثر استباقية من رد الفعل. كما يشير(Fouad,2021) من خلال تحديد علامات الإنذار المبكر للطلاب ، والطلاب الذين من المرجح أن يواجهوا صعوبات أكاديمية، حيث سيتمكن الإداريون بالتعاون مع الأكاديميين من إنشاء خطط استباقية تتوقع الصعوبات التي يتوقع أن يواجهها الطلاب بدلاً من انتظار وقوعها .
- يبدو أن الميزة الرئيسية للذكاء الاصطناعي هي توفير الوقت والجهد والمال في تنفيذ العمليات الإدارية كالقبول والتسجيل والفصل وغيرها والأكاديمية كمعرفة نتائج الطلاب مبكراً من خلال دراسة امكاناتهم وقدراتهم ، كما سيتم التعرف على المشكلات التي يمكن أن يقعوا بها في المستقبل ليتم تلافيها . أيضاً من خلال استخدام الذكاء الاصطناعي سيتم انجاز المهام التي تستغرق وقتًا طويلاً وجعل حل المشكلات أكثر كفاءة. (أشرف ،٢٠١٩)

يتضح مما سبق ، أن الذكاء الاصطناعي هو محاولة لإنشاء أدوات الكترونية يمكنها فعل الأشياء التي كانت قاصرة فقط على الممارسات البشرية . يعتمد الذكاء الاصطناعي اليوم على التعلم الآلي. يتعلق الأمر بإيجاد أنماط لكيفية التعامل مع فيضان ضخم من البيانات ثم استخدام هذه الأنماط لاتخاذ القرارات وممارسة الأنشطة الجامعية. يستخدم علماء البيانات الأنماط السابقة لتخمين ما يمكن أن يحدث ، أو كيف ستتصرف الموارد البشرية في المستقبل. وهي نتائج غاية في الأهمية إذا ما أحسن تنفيذها في العمليات الأكاديمية والإدارية في الجامعات المصرية .

المحور الثاني الأسس الفكرية للأمن السيبراني بالجامعات

يعبر الأمن السيبراني عن ممارسات دقيقة لحماية الشبكات والأجهزة والبيانات الجامعية من التلف أو الضياع أو السرقة أو الوصول غير المصرح به . فكما يحمي الأمن الجامعي المباني والأشخاص الموجودين في الجامعة من التهديدات الأمنية المختلفة، فإن الأمن السيبراني يحمي التقنيات الرقمية ومستخدميها من المخاطر الرقمية.

مفهوم الأمن السيبراني

يعد الأمن السيبراني مصطلح حديث . يعرف في بعض الجامعات باسم أمن تكنولوجيا المعلومات أو أمن المعلومات الإلكترونية(IT) .

وهو عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به، وسوء الاستغلال، واستعادة المعلومات الالكترونية، ونظم الاتصالات والمعلومات التي تحتويها. (Al-Jamal and Abu-Shanab, 2016) كما يعد الأمن السيبراني مجالًا يهتم بحماية المعلومات القيمة والحساسة في الجامعة من الهجمات الإلكترونية من قبل المتسللين والجهات التي ترغب في تدمير تلك المعلومات وسرقتها. (ابن إبراهيم،٢٠٢١)

ويعرف كذلك بأنه ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. حيث تهدف هذه الهجمات عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها؛ أو ابتزاز الأموال من المستخدمين. .(Abdulrahman and Omar,2018) كما ينظر إليه على أنه فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي وممارسة ضمان السرية والنزاهة وتوافر المعلومات. (سراج،٢٠٢٢)

يتضح مما سبق بأن الأمن السيبراني مجموعة من التدابير والإجراءات التي تم تصميمها وتطبيقها لحماية الأنظمة الالكترونية الجامعية والمعلومات الحساسة من الهجمات والتهديدات الالكترونية سواء كانت تلك التهديدات تنشأ من داخل أو خارج الجامعة .

كما يتضح أن المفهوم يرتبط بثلاثة عناصر:

- الموارد البشرية: كالقيادات الأكاديمية الجامعية وأعضاء هيئة التدريس والطلاب والإداريين؛ ومن ثم يجب عليهم فهم مبادئ الأمن السيبراني وممارساته.
- العمليات: بحيث يجب أن يكون لدى الجامعات إطار عمل لكيفية تعاملها مع الهجمات الإلكترونية. وبحيث يرشد جميع المستخدمين، ويشرح لهم كيفية تحديد الهجمات وحماية الأنظمة واكتشاف التهديدات والاستجابة لها والتعافي من الهجمات الناجحة؟
- التكنولوجيا: التكنولوجيا ضرورية لمنح الجامعات والمستخدمين أدوات وبرامج أمان اليكترونية لحماية أنفسهم من الهجمات الإلكترونية.

المفاهيم المرتبطة بمفهوم الأمن السيبراني

يرتبط مفهوم الأمن السيبراني ؛ بعدة مفاهيم من أبرزها :

- الهجمات السيبرانية؛ وتعرف بأنها محاولات جادة من قبل المتسللين أو المخربين الالكترونيين ؛ بقصد تخريب أو سرقة ، أو تدمير أنظمة الجامعة الالكترونية وما ترتبط بها من أنظمة فرعية ووثائق وملفات . (Abdulrahman and Omar,2018)

- الجرائم السيبرانية ؛ الأعمال والأفعال والممارسات الإجرامية غير القانونية التي تتم بواسطة محترفين بصورة فردية أو يتبعون جهات مختلفة ؛ بقصد السيطرة على نظام الجامعة الالكتروني. (Catota,et al,2019)
- المهاجمين أو المخربين السيبرانيين: أفراد أو كيانات تقوم بأفعال وسلوكيات مخالفة للقوانين – غالباً – ما يكونوا على درجة من الاحترافية في التخطيط والتنفيذ للهجمات السيبرانية على المؤسسات ومنها الجامعات.
- الردع السيبراني؛ إجراءات سريعة وفورية تأتي كرد حاسم على المخربين السيبرانيين؛ بحيث تعمل تلك الإجراءات على منعهم في المستقبل من تكرار تلك الهجمات والعمل على اكتشافهم وفضحهم واتخاذ الإجراءات القانونية تجاههم. (Ani,et al,2017)
- الخطر السيبراني ؛ مجموعة من الأفعال التي تشكل أو تمثل تحركات ضارة من قبل بعض الجهات غير الواضحة لمسؤولي الجامعة ؛ والتي تستلزم اتخاذ قرارات فورية لمواجهة تلك الأفعال والقضاء عليها في مهدها . (Fouad,2021)

يتضح مما سبق ارتباط المفاهيم السابقة بمفهوم الأمن السيبراني؛ حيث أن مفهوم الأمن السيبراني مفهوم عام وشامل يتضمن كل هذه المفاهيم، كما يمكن التأكيد بأن كثيرًا من المشكلات التي تتعلق بالخلط بين المفاهيم في مجال الأمن السيبراني ناتجة من عدم التحديد الدقيق لتلك المفاهيم؛ ومن ثم فلابد من توضيحها بشكل دقيق ، كما أن المعرفة بتلك المفاهيم سوف تؤثر في أساليب التعامل مع كافة القضايا السيبرانية فأسلوب مواجهة الخطر السيبراني سوف يختلف عن أسلوب مواجهة الجرائم السيبرانية وأيضاً عن أسلوب مواجهة التهديدات السيبرانية وهكذا .

أهداف الأمن السيبراني

يعد تحقيق الأمن السيبراني في الجامعات؛ هدف أساس؛ تسعى إلى تحقيقه؛ فمن خلاله تستطيع حماية جميع فئات البيانات والمعلومات من السرقة والتلف. ومن ثم ؛ فبدون منهجية واضحة للأمن السيبراني، لا يمكن لأي جامعة الدفاع عن نفسها ضد حملات التهديد وخرق البيانات، مما يجعلها هدفًا سهلاً لمجرمي الإنترنت.

لذا هدفت الجامعات من تطبيق منهجية الأمن السيبراني؛ إلى تحقيق مايلي : Ani,et al,2017)(Catota,et al,2019)

١- وقاية الحرم الجامعي من أية أخطار أو تهديدات الكترونية .
٢- حماية الجامعات من الهجمات السيبرانية الالكترونية .
٣- التدخل السريع للحيلولة دون تفاقم الأوضاع داخل الجامعات في حالة التعرض لهجمات فعلية.
٤- تنمية قدرات الموارد البشرية الجامعية على مواجهة التهديدات السيبرانية.
٥- تطوير ممارسات الموارد البشرية الجامعية لصد أي هجمات سيبرانية.
٦- تطوير خطط الجامعة في التعامل مع الأزمات والكوارث السيبرانية.
٧- رسم سيناريوهات لمواجهات مستقبلية مع المهاجمين السيبرانيين.

يتضح مما سبق أن الأمن السيبراني كمنهجية وممارسات تطبق بقصد الوقاية أو منع وقوع التهديدات السيبرانية من الأساس ، والتدخل فيها حال وقوعها بهدف التقليل والحد من آثارها ؛ ومن ثم وضع إجراءات سريعة للتعافي والرجوع إلى الوضع الطبيعي . سواء كان ذلك عن طريق وضع خطط أو تنفيذ إجراءات أو رسم سيناريوهات .

أهمية الأمن السيبراني وأهدافه

مع تزايد عدد المستخدمين والأجهزة والبرامج الالكترونية في الجامعات، جنبًا إلى جنب مع زيادة طوفان البيانات – الكثير منها حساس أو سري – تزداد أهمية الأمن السيبراني. فالحجم المتزايد للمهاجمين السيبرانيين وتقنيات الهجوم وتطورها يزيد من تعقيد المشكلة .

في الجامعات اليوم، يستفيد الجميع من برامج الأمن السيبراني. على المستوى الفردي، يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الملفات والبيانات الجامعية، وتدمير منصات التعليم عن بعد، وتدمير الدروس الجامعية المسجلة ؛ إضافة إلى محاولات الابتزاز وفقدان البيانات المهمة مثل الامتحانات الفصلية والنهائية التي يتم إعدادها الكترونياً . Abdulrahman (and Omar,2018) هذا إضافة إلى تدمير الأبحاث العلمية والكتب الدراسية والمراجع العلمية الالكترونية التي يتم استخدامها في شرح الدروس. فيعتمد الجميع الآن على النواحي الالكترونية في كل الأمور داخل الجامعة سواء كانت أمور أكاديمية أو بحثية أو خدمية أو إدارية وفي كل الوحدات الأكاديمية أو الإدارية. ويعد تأمين هذه الوحدات وغيرها أمرًا ضروريًا للحفاظ على عمل الجامعة .

لذا يمكن التأكيد بأن أهداف الأمن السيبراني بالجامعات تتبلور فيما يلي : (Redman,et al,2020)

١- وقاية الجامعات من التهديدات والأخطار والهجمات السيبرانية .
٢- تطوير برامج الحماية ؛ لمواجهة التطور الكبير في أساليب المهاجمين السيبرانيين.
٣- تطوير أساليب المواجهة والتعامل مع كافة الأخطار والتحديات السيبرانية .
٤- تطوير ممارسات القيادات الأكاديمية في مواجهة التهديدات والأخطار السيبرانية.
٥- تطوير أداء الموارد البشرية بالجامعة في مواجهة كافة الأخطار والتهديدات السيبرانية.
٦- سرعة التعافي من الهجمات السيبرانية ؛ واكتساب دروس مستفادة يمكن من خلالها تطوير خطط وسيناريوهات المواجهة في المستقبل .

أنواع تهديدات الأمن السيبراني في الجامعات

تتنوع أنواع تهديدات الأمن السيبراني في الجامعات؛ والتي من أبرزها:

١- التصيد : أكثر أنواع الهجمات الإلكترونية السيبرانية شيوعًا. وهو ممارسة إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني الواردة من مصادر حسنة السمعة. ويكون الهدف هو سرقة البيانات الحساسة مثل الأرقام السرية ومعلومات تسجيل الدخول للحساب الشخصي بالجامعة سواء على المنصة الالكترونية، أو المكتبة وغيرها . (Ani,et al,2017)
٢- برامج الفدية: نوع من البرامج الضارة. المصممة لابتزاز الأموال عن طريق منع الوصول إلى الملفات الشخصية أو نظام الكمبيوتر حتى يتم دفع الفدية.
٣- البرمجيات الخبيثة: نوع من البرامج المصممة للحصول على وصول غير مصرح به أو إلحاق الضرر بجهاز الكمبيوتر .

وأياً كانت التهديدات السيبرانية على الجامعات ؛ فإنها تحتاج من القيادات الأكاديمية الوعي والفهم بخطورتها ؛ وأنها يمكن أن تؤثر سلباً على الأداء الجامعي بوجه عام مالم تكن هناك استجابة سريعة ودقيقه منهم وبالتعاون مع المتخصصين والخبراء بالجامعة للقضاء على أي تهديد يواجهها . وحتى يرجع الحرم الجامعي إلى حالة الاستقرار التي كان ينعم بها قبل وجود تلك التهديدات.

مجالات الأمن السيبراني

تحتوي استراتيجية الأمن السيبراني القوية بالجامعات على طبقات من الحماية للدفاع ضد الجرائم الإلكترونية، بما في ذلك الهجمات الإلكترونية التي تحاول الوصول إلى البيانات أو تغييرها أو تدميرها؛ وابتزاز الأموال من المستخدمين أو الجامعة؛ أو تهدف إلى تعطيل العمليات والأنشطة الجامعية العادية. يشير كل من (Ani,et al,2017)، (Catota,et al,2019)، (Fouad,2021) أن أبرز مجالات الأمن السيبراني ؛ ما يلي :

١- أمان البنية التحتية الحرجة : وهي ممارسات لحماية أنظمة الكمبيوتر الجامعية والشبكات والأصول الأخرى التي تعتمد عليها الجامعة.

٢- أمان الشبكة : وهي تدابير أمنية لحماية شبكة الكمبيوتر من المتطفلين، بما في ذلك الاتصالات السلكية واللاسلكية.

٣- أمان التطبيق : وهي العمليات التي تساعد في حماية التطبيقات التي تمارسها كليات وإدارات الجامعة المختلفة.

٤- أمان المعلومات : وهي تدابير لحماية البيانات الجامعية ، الأكثر حساسية من الوصول غير المصرح به أو التعرض للتهديد أو السرقة .

٥- تعليم المستخدم النهائي : أي بناء الوعي الأمني للموارد البشرية بالجامعة لتعزيز أمنها من التهديدات والهجمات السيبرانية ؛ من خلال البرامج التدريبية المتخصصة .

٦- التعافي من الكوارث : وهي أدوات وإجراءات للاستجابة للأحداث غير المتوقعة أو المخطط لها أو المفاجئة ، مثل الكوارث الطبيعية أو انقطاع التيار الكهربائي أو حوادث الأمن السيبراني.

٧- تأمين التخزين : إجراءات محددة لتخزين البيانات والمعلومات الجامعية. وهذا يشمل التشفير ونسخ البيانات غير القابلة للتغيير.

إذن تتعدد مجالات الأمن السيبراني بالجامعات ما بين وقاية وتدخل وحماية وتطوير موارد بشرية لتحسين أساليب القضاء على التهديدات السيبرانية. وهذه المجالات من جانب آخر توضح حجم الخطر السيبراني الذي يحيط بالجامعات ؛ ومن ثم يجب أن يكون هناك وعي من قبل القيادات الأكاديمية والموارد البشرية بهذا الخطر وضرورة مواجهته بأساليب فعالة .

تحديات الأمن السيبراني

يواجه الأمن السيبراني في الجامعات تحديات مستمرة من قبل المتسللين كفقدان البيانات والمعلومات ، وانتهاك الخصوصية ، وزيادة المخاطر بشكل كبير ، والتغيير والتحديث في استراتيجيات الأمن السيبراني. يشير (Catota,et al,2019) أن هناك خمسة تحديات رئيسة تواجه الأمن السيبراني في الجامعات ؛ وهي:

التحدي الأول : أحد أكثر تحديات الأمن السيبراني خطورة هي الطبيعة المتطورة للمخاطر والتهديدات الأمنية السيبرانية. فمع ظهور تقنيات جديدة، ومع استخدام التكنولوجيا بطرق جديدة أو مختلفة، يتم تطوير طرق هجوم جديدة لتتلاءم مع حجم التطورات في ممارسات الأمن السيبراني بالجامعات. قد تكون مواكبة هذه التغييرات المتكررة والتقدم في الهجمات، وكذلك تحديث الممارسات للحماية منها، أمرًا صعبًا على الجامعات (Fouad,2021)

التحدي الثاني : ضمان تحديث جميع عناصر الأمن السيبراني بالجامعات باستمرار؛ للحماية من نقاط الضعف المحتملة. قد يكون هذا صعبًا بشكل خاص بالنسبة للجامعات الصغيرة التي لا يوجد بها أطقم عمل محترفة أو موارد داخلية متوفرة . (Garba,et al,2020)

التحدي الثالث : تعدد المحاولات والتهديدات نتيجة لكثرة المخربين وسارقي البيانات الجامعية تعد تحد ثالث ، فنتيجة لسهولة اختراق الملفات الجامعية والمواقع الجامعية نتيجة لعدم تأمينها بشكل كافٍ ؛ فيكثر عدد المخربين ، وتتعدد محاولاتهم وخاصة إذا نجحت إحداها . (Hujran,et al,2015)

التحدي الرابع : عدم التزام القيادة الجامعية ؛ والتي تتبلور في عدم اكتراثها بوجود استراتيجية لتطوير الممارسات السيبرانية في الحرم الجامعي ، وعدم مشاركتها في وضع خطط إدارة الأزمات السيبرانية ، وخطط التعافي ، وعدم توفيرها لمتطلبات الأمن السيبراني سواء في جوانبه البشرية أو المالية أو المادية. (Garba,et al,2020)

التحدي الخامس: نقص في كفاءة الموارد البشرية الجامعية – خاصة – في تعاملها مع التهديدات السيبرانية ؛ وذلك نتيجة قلة البرامج التدريبية ، وعموميتها ، وعدم مسايرتها للاتجاهات الحديثة في مجال الأمن السيبراني إضافة إلى عدم اهتمام الموارد البشرية بمجال الأمن السيبراني والاقتصار فقط على ممارسة المهام الموكولة لهم في المجالات الأكاديمية والبحثية والإدارية والخدمية . (Pavel,et al,2021)

يتضح مما سبق تعدد التحديات التي تواجه الأمن السيبراني بالجامعات ؛ ومن ثم وجب عليها مواجهتها والتعامل معها بأسلوب موضوعي يبتعد عن العشوائية . والخطوة الأولى تتعلق بتوفير متطلبات الأمن السيبراني من فهم ووعي القيادة الجامعية بأهمية تطوير ممارسات الأمن السيبراني ومن ثم ضمان التزامها ، وتوفير الموارد البشرية المؤهلة للتعامل مع التهديدات السيبرانية ، والموارد المالية والمادية المناسبة، مع تطوير وتحسين مستمر لأساليب وممارسات الأمن السيبراني لتتلاءم مع تعدد وتنوع وتطور محاولات اختراق الجامعة وتهديدها.

لماذا يعد التعليم الجامعي هدفًا للجرائم السيبرانية؟

هناك أسباب رئيسة تجعل التعليم الجامعي هدفًا للجرائم السيبرانية . فمع اختلاف أماكن التعليم الجامعي في الحجم والغرض والمكانة، يمكن أن تختلف دوافع الجرائم أيضًا. Muniandy (et al,2017) فعلى سبيل المثال، ما قد يكون تهديدًا شائعًا للجامعات ذات الشهرة العالمية قد لا يمثل تهديداً للجامعات الأقل في الشهرة، كما أن التهديدات التي تواجه الجامعات الكبيرة في الحجم والعدد قد لا تكون هي نفس التهديدات التي تواجه الجامعات الصغيرة وهكذا. لذلك، تحتاج الجامعات إلى تقييم لطبيعة ونوعية المخاطر التي تواجهها أو التي يمكن أن تواجهها؛ لتحديد الأسباب بدقة عالية، ولكن تكاد تجمع الأدبيات إلى أن الأسباب الأكثر شهرة لوقوع الجرائم والتهديدات السيبرانية؛ ما يلي :

١- تعطيل واسع النطاق لشبكة الكلية أو الجامعة؛ فالهجمات الالكترونية تعد نوعًا شائعًا من الهجمات على جميع الجامعات. ويكون الهدف الرئيس خفض إنتاجيتها وتشويه سمعتها. ويمكن أن يكون هذا الهجوم سهلًا نسبيًا على مجرمي الإنترنت ، خاصةً إذا كانت الشبكة المستهدفة ضعيفة الحماية. (Garba,et al,2020)

٢- سرقة البيانات والمعلومات الهامة : فجميع الجامعات تحتفظ ببيانات غاية في الخطورة كعناوين الباحثين والخبراء وأعضاء هيئة التدريس والطلاب. يمكن أن يكون هذا النوع من المعلومات ذا قيمة لمجرمي الإنترنت لعدة أسباب ، منها بيع المعلومات لطرف ثالث أو استخدامها كأداة للمساومة وابتزاز الأموال . (Catota,et al,2019) والأمر الخطر أيضاً ما يتعلق بالجوانب المالية وأرصدة الجامعات ، خاصة وأن دفع الرسوم الدراسية والاحتفاظ بها يكون الكترونياً ، لذا فإنها تمثل هدفًا رئيسيًا لمجرمي الإنترنت. ومن ثم فبدون الحماية المناسبه من جانب الجامعات ، فإن هذا يمثل نقطة ضعف يستغلها المهاجمين السيبرانيين.(Hujran,et al,2015)

٣- التجسس : غالبًا ما ينظر إلى الجامعات كمراكز للبحث العلمي الرصين، حيث يُعتقد أن الأبحاث العلمية في المجالات الطبية والهندسية والأمنية التي أجرتها وتجريها الجامعات قد تتعرض للاختراق من قبل المتسللين؛ وتصبح لذلك عرضة للتجسس بصور مختلفة، باعتبارها أروع ما تنتجه العقول البشرية وتتوصل إليه في سبيل تحقيق رفاهية هذا العالم(fouad,2021).

يتضح مما سبق أن الأسباب الرئيسة لوقوع التهديدات والهجمات السيبرانية بالجامعات واضحة ومحددة ؛ ومن ثم يتعين وضع إجراءات للحماية والوقاية من تلك الهجمات ؛ وذلك من خلال علاج نقاط الضعف التي تتبلور في عدم وجود استراتيجية للأمن السيبراني بالجامعات تتضمن إجراءات لتطوير جوانب الحماية في الشبكات الالكترونية الجامعية . فالقضاء على أسباب وقوع الهجمات السيبرانية سيمكن الجامعات من الحفاظ على مواردها الالكترونية من التهديد والتدمير .

أساليب وطرق الهجمات والتهديدات السيبرانية بالجامعات

تتعدد طرق الهجمات والتهديدات السيبرانية في الجامعات، ومن أبرزها :

١- التصيد الاحتيالي: غالبًا ما تتخذ عمليات التصيد الاحتيالي شكل رسالة بريد إلكتروني أو رسالة فورية وهي مصممة لخداع المستخدم ليثق بالمصدر في محاولة احتيالية للوصول إلى بياناته ومعلوماته . (Naidu and Zainuddin , 2021). يتم تسليط الضوء على هذا النوع من الهجوم باعتباره التهديد الأكبر الذي يواجه الجامعات بكل دول العالم، مما يشير إلى أن المتسللين يستهدفون القطاع بانتظام باستخدام هذه الطريقة. Catota,et (al,2019)

٢- برامج الفدية / البرامج الضارة، تمنع هجمات برامج الفدية والبرامج الضارة المستخدمين من الوصول إلى الشبكة أو الملفات أو البيانات الخاصة بهم وتتسبب في حدوث اضطراب، ومشكلات في استرجاع تلك الملفات والبيانات. وقد يكون الهدف الأساس من تنفيذ هذه البرامج من قبل المهاجمين الحصول على فدية مالية لاستعادة الملفات المسروقة (Abdulrahman and Omar,2018)

٣- الاختراق : من خلال معرفة كلمات السر أو أرقام الأمان للمستخدمين ؛ ويعتمد ذلك على مهارة المهاجمين لشبكة الجامعة ، وضعف برامج الحماية ؛ مما يسهل من نفاذ هؤلاء المهاجمين إلى ملفات الجامعة في كافة الأنشطة والتحكم فيها . (Fouad,2021)

يتضح مما سبق أن الخطأ البشري يلعب دورًا رئيساً في وقوع هذه التهديدات. ومع ذلك، ومع تحسين التدريب على ممارسات الأمن السيبراني ، والوعي بدوافع وطرق المهاجمين ، وتطبيق استراتيجية واضحة للأمن السيبراني ؛ يمكن للجامعات أن تحمي نفسها بشكل أفضل من الهجمات الإلكترونية .

تأثيرات الهجمات السيبرانية

تتعدد تأثيرات الهجمات السيبرانية على الجامعات ؛ ومنها :

١- التأثيرات الاقتصادية: والتي تتعلق بالخسائر الاقتصادية التي تصيب الجامعة ومن أبرزها؛ تكلفة إصلاح الأنظمة الالكترونية التالفة ، الفدية المطلوبة لاسترجاع البيانات المسروقة، سرقة الملكية الفكرية ومعلومات الجامعة.

٢- تأثيرات السمعة: والتي تتعلق بصورة الجامعة لدى المجتمع والمستفيدين؛ ومن أبرزها؛ فقدان ثقة المستفيدين، فقدان عدد من المستفيدين الحاليين والمستقبليين. خسارة المنافسة مع المنافسين في بعض الجوانب.

٣- التأثيرات التنظيمية: والتي تتعلق بالجوانب الإدارية والتنظيمية بالجامعة؛ ومن أبرزها إعادة النظر في بعض الإجراءات الإدارية التي ثبت بالدليل عدم فعاليتها ؛ ومن ثم احتياجها إلى التعديل والتغيير ، تطوير بعض الإجراءات واختصارها .

نظرًا لطبيعة التهديدات والجرائم الإلكترونية ومدى صعوبة اكتشافها ، فمن الصعب فهم التكاليف المباشرة وغير المباشرة للعديد من الانتهاكات الأمنية. هذا لا يعني أن الضرر الذي يلحق بالسمعة -على سبيل المثال -حتى لو حدث خرق صغير للبيانات أو أي حدث أمني آخر ليس كبيرًا. ولكن يجب أن تضمن جميع الجامعات، بغض النظر عن أنشطتها وحجمها ، فهم جميع الموارد البشرية لتهديدات الأمن السيبراني وكيفية مواجهتها والحد منها.

المحور الثالث أدوار القيادات الأكاديمية في تعزيز ممارسات الأمن السيبراني بالجامعات الأمريكية

مع استمرار قطاع التعليم الجامعي الأمريكي في إحراز تقدم كبير في رحلة التحول الرقمي كما يشير (Pavel ,et al,2021) ، أصبحت الكليات والجامعات أهدافًا للهجمات الإلكترونية السيبرانية ؛ من هجمات برامج الفدية إلى انتهاكات البيانات . حيث وقعت العديد من الجامعات الأمريكية ضحية للهجمات الإلكترونية في السنوات الأخيرة. Naidu and (Zainuddin , 2021) وزاد من تفاقم الوضع التحول المفاجئ والكلي إلى التعلم عن بعد نتيجة جائحة كورونا.

في الواقع ، كان التعليم الجامعي هو الصناعة الأكثر تضررًا ، حيث واجه ما يقرب من ٦٤٪ من الجامعات الأمريكية هجمات سيبرانية خطيرة عن طريق البرامج الضارة. Garba,et (al,2020)

تشير دراسة (Aljohni ,et al,2021) إلى أن الكليات والجامعات تحتل المرتبة الثالثة في انتهاكات البيانات. بالإضافة إلى ذلك، أشار تقرير الأمن السيبراني التعليمي لعام ٢٠٢١ إلى أن انتهاكات البيانات كانت المصدر الرئيسي للمخاطر بالنسبة للجامعات الأمريكية.(نقلاً عن سراج ،٢٠٢٢) لذلك كانت صناعة التعليم الجامعي الأمريكي كما يشير (السمحان،٢٠٢٠) تأخذ الأولوية الآن في التأهب السيبراني من بين ١٧ صناعة أمريكية أخرى . وكما يشير Garba,et (al,2020) أن هناك 85٪ من الجامعات تم زيادة تمويلها للأمن السيبراني إضافة إلى زيادة الاستثمارات لحماية المعلومات البحثية الهامة والملكية الفكرية. وفي الوقت نفسه، تم تطوير البنية التحتية الحالية لتكنولوجيا المعلومات بالجامعات لزيادة الحماية من الهجمات الإلكترونية.

يتم إلزام الجامعات الأمريكية بتفعيل مواد قانون التعليم العالي Higher Education Act (HEA)الذي يؤكد على ضرورة أن تكون لدى كل جامعة أمريكية سياسات وضمانات وقائية وممارسات المراقبة والإدارة المتعلقة بأمن المعلومات؛ وأن يتم التأكد من ممارسة مواد القانون من خلال لجان المراجعة الداخلية والخارجية . (Redman,et al,2020)

في الآونة الأخيرة زادت المطالبات على الرئيس بايدن ، لتطوير بنية تحتية قوية للأمن السيبراني تقلل من جميع المخاطر ولا تترك مجالًا للانتهاكات. انطلاقاً من أن الأمن السيبراني ليس فقط أمرًا حاسمًا للحماية من الخسارة الاقتصادية وتجنب التعطيل، ولكنه ضروري أيضًا

لحمايـــة المـــوارد الجامعيـــة مـــن أي نـــوع مـــن الـــضرر. (George Washington University,2022)

يتضح مما سبق تعرض المؤسسات الأمريكية للكثير من التهديـــدات الـــسيبرانية ؛ وأن المؤسسات الجامعية كانت أكثرها تهديداً ووقوعاً لتلك الهجمات في أحرامها الجامعيـــة ؛ الأمـــر الذي أدى إلى تفعيل ممارسات الأمن السيبراني وزيادة التمويل المخـــصص لهـــا فـــي ميزانيـــة الجامعات من منطلق الأهمية القصوى لحماية الأصول البشرية والمادية والمالية للجامعات . كما اتضح التزام الجامعات بوضع سياسات للأمن السيبراني لكل جامعة وضرورة تفعيلها وفقاً لقانون التعليم العالي . كما ازدادت المطالبات بوضع رؤى لتطوير البنيـــة التحتيـــة للأمـــن الـــسيبراني بالجامعات على اعتبار أنه ليس من الأهمية فقط ممارسة الأمن الـــسيبراني بـــل تطـــوير تلـــك الممارسات وتحسينها بشكل دائم لتتواكب مع التطورات في مجال الأمن السيبراني والتطـــورات أيضاً في أساليب ووسائل المهاجمين والمخربين الالكترونين.

مفهوم الأمن السيبراني بالجامعات الأمريكية

الأمن السيبراني هو كافة الإجراءات التي تطبقها الجامعات الأمريكية لحماية الأجهـــزة والشبكات من الوصول أو التعديل غير المصرح به . (Redman,et al,2020) كما يشير الأمن السيبراني إلى التقنيات والعمليات والممارسات التي تصممها الجامعات لحماية الشبكات والأجهزة والتطبيقات والبيانات من أي نوع من الهجمـــات الإلكترونيـــة. (Wilbanks,2016) ينطبـــق المفهوم على مجموعة متنوعة من السياقات داخل كافة الكليات العملية والنظرية وكافـــة الإدارات والأقسام ، فالمفهوم لا يختلف مدلوله باختلاف المكان . ويرتبط مفهوم الأمن السيبراني بالجامعات الأمريكية – أيضاً– بالتهديدات والهجمات الضارة المحتملة التي تسعى إلى الوصول غير القانوني إلى البيانات أو تعطيل العمليات الرقمية أو إتلاف المعلومات الجامعية. والتي يمكن أن تنشأ مـــن جهات مختلفة ، بما في ذلك الجواسيس والقراصنة والجماعات الإرهابية والمنظمات الإجراميـــة والمتسللين المنفردين والموظفين الساخطين والمتنمرين على العمل داخل الجامعـــة . (George Washington University,2022)

أهداف وأهمية الأمن السيبراني بالجامعات الأمريكية

تشتهر الجامعات الأمريكية في جميع أنحاء العالم بجودة أبحاثها وخبراتها، وتنتج المزيد من الأبحاث الأكاديمية أكثر مـــن أي دولـــة أخـــرى. (Redman,et al,2020) قيمـــة هـــذه

المساهمات في الاقتصاد كبيرة؛ وقد قُدرت بملياري دولار من عائدات الملكية الفكرية فقط بين عامي ٢٠١٨ و ٢٠٢٠. (Naidu and Zainuddin , 2021) ونظرًا لقيمة تلك الجامعات، فإن بعض المنظمات والأفراد على استعداد لاتخاذ أي إجراء ضروري للحصول على بياناتها وملفاتها ووثائقها، بما في ذلك ارتكاب الجرائم الإلكترونية؛ لذا ليس من المستغرب أن يكون "أمن المعلومات" قد احتل المرتبة الأولى في قائمة أفضل ١٠ قضايا تتعلق بتكنولوجيا المعلومات في عام ٢٠٢١ للتعليم الجامعي الأمريكي.(Redman,et al,2020) وبناءاً على ذلك فقد وضعت بعض الجامعات الأمريكية إجراءات محددة لتفعيل ممارسات الأمن السيبراني تهدف إلى:

١- التقليل من الخسائر المالية التي تعاني منها الجامعات.
٢- حماية ووقاية الجامعات من التهديدات السيبرانية .
٣- الحفاظ على سمعة الجامعات من الضرر مما يؤدي إلى انخفاض في الطلبات والتسجيل، أو فقدان التبرعات والمنح.
٤- الحفاظ على ولاء القيادات الأكاديمية الجامعية والموظفين والطلاب للجامعة.
٥- الحفاظ على المستندات الهامة للجامعة في كافة مجالات عملها.
٦- التيسير من المعاملات الالكترونية في كافة جوانب العمل الجامعي.
٧- وضع استراتيجية للحفاظ على أمن المعلومات.

ومن أجل تحقيق هذه الأهداف وجب على الجامعات تصنيف أصولها على أساس أهميتها وأولويتها. وتحديد التهديدات والمخاطر المحتملة، وتحديد أسلوب التعامل لكل تهديد ، و مراقبة أي أنشطة غير معتادة أو مألوفة كمحاولات خرق وسرقة البيانات، والصيانة المتكررة والاستجابة لأية قضايا ذات صلة، وتحديث سياسات التعامل مع المخاطر والتهديدات ، بناءاً على التقييمات السابقة. ومن ثم تحافظ الجامعات على سمعتها وقدرتها على حماية ووقاية نفسها من التهديدات والمخاطر السيبرانية .

مبادئ الأمن السيبراني في الجامعات الأمريكية

تتعدد مبادئ الأمن السيبراني بالجامعات الأمريكية. وينظر لهذه المبادئ كما تشير (et, Aljohni al,2021) على أنها موجهات لمساعدة مجتمع الحرم الجامعي على كيفية إدارة المعلومات والأصول الأخرى بأمان. وهذه المبادئ الأربعة ؛ هي:

١- الأمن السيبراني مسؤولية الجميع : مجتمع الحرم الجامعي بأكمله مسؤول عن تأمين المعلومات من خلال اتباع سياسات وعمليات وضوابط الجامعة أو عن طريق تطوير سياسات وعمليات وضوابط خاصة بكل وحدة أكاديمية وإدارية . (George Washington University,2022)

٢- الأمن السيبراني جزء من دورة حياة التطوير: تتضمن دورة حياة التطوير لأي نظام تحديد عمليات وضوابط الأمان وتطويرها وتنفيذها وصيانتها. ويصبح النظام أكثر أمانًا عند مراعاة ما يلي :(New York University,2022)

- خصوصية المعلومات : حماية خصوصية المعلومات المتعلقة بأعضاء هيئة التدريس والموظفين والطلاب ومجموعات أو معلومات الجامعة الأخرى .
- ضمان المعلومات : يجب أن يتضمن تصميم الأنظمة ضوابط التسجيل وعمليات المراجعة للكشف عن الاستخدام غير المناسب ودعم التحقيقات في الحوادث .
- سهولة الاستخدام : يجب تطوير العمليات والضوابط بحيث يمكن للمستخدم بسهولة متابعة العملية أو استخدام عنصر التحكم .

٣- الأمن السيبراني هو إدارة الأصول : يجب أن تتضمن إدارة النظام العمليات والضوابط التي تؤمن المعلومات من خلال مراعاة: تصنيف المعلومات ؛ فيجب على الكليات والإدارات التي تمتلك المعلومات تحديد المعلومات وتحديد ضوابط التعامل معها والتي يجب مراعاتها . وتحديد الأشخاص المسموح للوصول إلى المعلومات أو تعديلها أو حذفها. (George Washington University, ٢٠٢٢)

٤- الأمن السيبراني هو تفاهم مشترك لمجتمع الحرم الجامعي: وهو مسؤول عن فهم المخاطر والتهديدات والحوادث المرتبطة بتأمين المعلومات. يجب أن يكون هناك أيضًا فهم لكيفية الإبلاغ عن الحوادث وإدارتها. ويجب أن تأخذ الجامعات في الاعتبار :(University of California,2022)

- وضع إجراءات لاستيفاء متطلبات التعامل مع التهديدات والمخاطر.
- تحديد وتنفيذ استراتيجيات التخفيف من الأضرار.
- إدارة المخاطر بشكل مناسب ضمن دورة حياة العمل تطوير النظام.
- يجب أن تظل القيادة ومجتمع الحرم الجامعي على علم بالتهديدات الحالية والناشئة .
- يجب على القيادة النظر في تكاليف تنفيذ الضوابط ووضعها بميزانية الجامعة.

- إدارة الحوادث سيقوم مجتمع الحرم الجامعي بالإبلاغ عن الحوادث المتعلقة بأمن المعلومات.
- ستتم إدارة الحوادث بطريقة سرية ومناسبة وفي ضوء القواعد المعمول بها .

وتلتزم الجامعات الأمريكية بهذه المبادئ عند ممارستها للأمن السيبراني ضد التهديدات الحالية والمحتملة.

يتضح مما سبق؛ أن ممارسة الأمن السيبراني بالجامعات تعتمد على أسس محددة تنطلق من الجماعية والتعاون والتفاهم في تنفيذ الأنشطة والمهام بين القيادات الأكاديمية وأعضاء هيئة التدريس والموظفين ؛ فالعمل الفردي لن يجدي في مواجهة التهديدات والهجمات السيبرانية، كما أن الانفراد باتخاذ القرارات من قبل القيادات الأكاديمية أو المتخصصين غير ذات مضمون إذا لم يرتبط بتفاهم مشترك بين كل الفئات التي تعمل بالجامعة ؛ وبحيث يكون الهدف الرئيس منصب على الحفاظ على موارد الجامعة وممتلكاتها من التخريب .

أساليب الأمن السيبراني بالجامعات الأمريكية

أشار (Wilbanks,2016) أن قيادات التعليم الجامعي الأمريكي استثمرت ملايين الدولارات في الأمن السيبراني في السنوات الماضية، ومع ذلك، فإن التهديد الذي يلوح في الأفق هو أن نظام البرمجيات وبرامج الأمن السيبراني تتغير وتتطور كل يوم، وأصبح المتسللون أكثر تطوراً. حاليًا، كما يؤكد (Peker ,et al,2018) العديد من أقسام تكنولوجيا المعلومات في وضع البحث عن أساليب جديدة ومبتكرة لتطوير برامج الأمن السيبراني لتطوير الاستجابة للتهديدات فور حدوثها. وتطوير برامج للحماية تصد أي تهديد محتمل.

تطور الجامعات الأمريكية – حالياً – استراتيجية استباقية من شأنها أن تخفف من المخاطر وتسمح لها بالتعافي في حالة وقوع هجمات سيبرانية. ومن أبرز أساليب هذه الاستراتيجية:

١- وضع إجراءات لالتقاط إشارات الإنذار المبكر لقرب وقوع هجمات سيبرانية.؛ وتتضمن تلك الإجراءات نظم الكترونية للالتقاط الإشارات والتي تبدو في صورة محاولات من جهات غير معروفة للدخول على قواعد البيانات لسرقتها أو اتلافها. .(Aljohni ,et al,2021)

٢- وضع إجراءات التدخل السريع في حال وقوع الهجمات السيبرانية؛ والتي تتضمن نجاح بعض الجهات الغريبة لتشويه المعلومات أو سرقتها ومن ثم تتدخل الجامعات للحيلولة دون مزيد من الهجمات ومحاولة اصلاح نقاط الضعف. (Peker ,et al,2018)

٣- وضع إجراءات للعمل التعاوني الجماعي من خلال فرق عمل متخصصة للمواجهة والتدخل ؛ فلا يمكن المواجهة بصورة فردية ؛ حيث تتكون في الجامعات فرق متخصصة للمواجهة تتعاون مع أعضاء هيئة التدريس والموظفين والطلاب . (Tibi ,et al,2019)

٤- وضع إجراءات للتعافي ؛ تتبلور تلك الإجراءات في تحديد نقاط الضعف والقوة في إجراءات التعامل ؛ ثم وضع إجراءات للتحسين تركز على تلافي نقاط الضعف وسد الفجوات الموجودة لتطوير أساليب التعامل في المستقبل . (Garba,et al,2020)

يتضح مما سبق ؛ تعدد أساليب المواجهة والتعامل مع التهديدات السيبرانية ، ما بين إجراءات للوقاية وأخرى للتدخل ؛ وهذه الإجراءات تشير إلى اهتمام الجامعات بالحفاظ على مكانتها وصورتها في المجتمع من خلال القضاء على مايواجهها من مخاطر على اعتبار أنها مؤسسات مجتمعية تمتلك كل عناصر النجاح والتفوق في التعاطي مع كافة القضايا ، ومن غير المقبول أن تتعرض إلى مخاطر وهجمات دون أن يكون لها رد فعل حازم وحاسم . فالجامعات تعمل على تكوين سمعتها خلال عشرات السنوات ولكن في غضون دقائق محدودة قد تهدد هذه السمعة بسبب عدد من الهجمات التي فشلت في التعامل معها.

متطلبات تطبيق ممارسات الأمن السيبراني

أشارت دراسات (Peker ,et al,2018)، (Tibi ,et al,2019)، (Aljohni ,et al,2021) إلى ضرورة وجود مجموعة من المتطلبات لنجاح القيادات الأكاديمية في مواجهة التهديدات السيبرانية ؛ ومن أبرز تلك المتطلبات :

١- تبني ثقافة واعية للأمن السيبراني. الخطوة الأولى والمهمة كانت غرس ثقافة أمنية في الجامعات. للقيام بذلك ، تم تنفيذ عدد من المبادرات لإشراك جميع الموظفين (بما في ذلك القيادات) في جهد جماعي نحو حماية الأنظمة والبيانات. أو كما تشير .(Aljohni ,et al,2021) الرغبة كانت في تحول الجامعة لبيئة يدرك فيها الجميع أهميتها الخاصة لحماية كافة الأنشطة والعمليات ؛ وبحيث يشعر الجميع بأنهم مسؤولين ؛ فيتم تشجيعهم على تقديم

مساهمات من خلال مشاركة الأفكار والمخاوف التي تعد أفضل أرضية لتبني السياسات الأمنية ومبادرات التوعية بالشكل المناسب .

٢- الاستثمار في تدريب وتوعية القيادات الأكاديمية بالأخطار السيبرانية، يعتبر من أهم المتطلبات للاستعداد للأمن السيبراني. نظرًا لأن العديد من التهديدات السيبرانية تستغل قصور مهارات العامل البشري، فمن المناسب أن تستثمر الجامعات ليس فقط في الضمانات التقنية ولكن أيضًا وبشكل خاص في القوى البشرية – خاصة – القيادية لتحسين قدرتها على مواجهة التهديدات المتطورة. يساعد تثقيف القيادات حول مخاطر التهديدات السيبرانية على تقليل احتمالية أن يصبحون أهدافًا سهلة عن طريق التصيد الإلكتروني أو القرصنة أو البرامج الضارة. (Peker ,et al,2018) تتكون برامج التدريب والتوعية من مجموعة من المراحل والأساليب والموضوعات التي تتعلق بممارسات الأمن السيبراني كوضع الخطط ورسم السيناريوهات وتطوير إجراءات المواجهة ، ويجب أن يتم تصميمه وفقًا لكل جامعة ومتطلباتها من الأمن السيبراني. (Peker ,et al,2018)

٣- وضع خطة أمنية فعالة بالتنسيق بين المتخصصين والقيادات الأكاديمية. يجب وضع خطة تصف بوضوح كيف تقف الجامعة وتتقدم نحو حماية أنظمتها وبياناتها؟ ومع ذلك، فمن الضروري أن يكون القادة على دراية بالخطط والاحتياجات الأمنية للجامعة، ليتم وضع تلك الخطط بناءاً على أسس واضحة قائمة على دراسة واعية لواقع عملها.(Aljohni ,et al,2021) وهذا مهم بشكل خاص لضمان التمويل الكافي وفي الوقت المناسب لأي احتياجات قد تتطلبها الجامعات لتأمين أنظمتها أو الاستجابة للتهديدات السيبرانية .

٤- تحقيق المرونة ، وليس مجرد تجنب المخاطر: احتاجت القيادات إلى التركيز على مرونة الجامعات بأكملها (بما تضمه من كليات وإدارات) للاستجابة للتهديدات السيبرانية ، حتى يمكن التخفيف من المخاطر والحد منها. (Wilbanks,2016) من الواضح أن الخطوة الأولى كانت هي تقوية الشبكة الالكترونية للجامعة من خلال أدوات المراقبة والإجراءات التقنية المضادة. ومع ذلك ، وجب على القيادات الانتباه إلى تنفيذ الضوابط الفنية والإدارية وأن يقوموا شخصيًا بمراجعة نتائج أي تقييمات واختبارات أمنية لفهم الجوانب التي تحتاج إلى التحسين. (Tibi ,et al,2019) فالعمل على تعزيز الموقف الأمني للجامعة كما يشير (Redman,et al,2020) ، بدلاً من التركيز بشكل أساسي على الاستجابة للحوادث

، يمكن أن يقطع شوطًا طويلاً في حماية الأعمال وضمان التعافي السريع في حالة حدوث أي خطر .

٥- تقييم إجراءات الأمان السيبراني؛ وذلك لتحديد المخاطر والتهديدات ونقاط الضعف التي تواجه الجامعات. ويعد هذا المتطلب خطوة حاسمة لتفعيل أدوار القيادات نحو تقييم الوضع الأمني للجامعة والقياس الموضوعي لأي تقدم ناتج عن تنفيذ البرامج الجديدة والتدابير المضادة التقنية والبرامج التدريبية التي تم تقديمها. (Peker ,et al,2018) تحتاج الجامعات إلى إجراء تقييم كامل للمخاطر والتهديدات ونقاط الضعف الحالية أثناء معالجتها من خلال مقاييس لقياس الجهود بشكل موضوعي. يمكن للقيادات تقييم عواقب وتأثير كل نشاط أو احتمالية وقوع نوع معين من التهديدات السيبرانية واستنباط كيفية التخفيف من المشكلات الأكثر أهمية.(Aljohni ,et al,2021) ستساعد هذه الاجراءات بعد ذلك في تحديد كيفية تعامل القيادات مع التهديدات باستخدام منهجيات مناسبة وتحديد أفضل الأساليب في حماية النظام. يساعد التقييم، قبل كل شيء، القيادات الأكاديمية بالجامعات على تعزيز ثقافة الوعي بالمخاطر .

٦- وضع وتوظيف سياسة الأمن السيبراني المصممة لحماية الجامعة: يمكن لسياسة الأمن السيبراني الجيدة تحقيق عدة فوائد ؛ منها: زيادة الوعي لدى القيادات بالمخاطر المحتملة ، وإعطاء نظرة ثاقبة لهم حول نقاط الضعف المحتملة وكيفية تصحيحها ؛ بحيث يمكن للقيادات بالتعاون مع المتخصصين والعاملين بالجامعة أن يكونوا مجهزين بشكل أفضل لمنعها ، (Tibi ,et al,2019) كما تقدم إرشادات واضحة للقيادات حول الاستخدام المقبول لجميع الأصول والبيانات الرقمية في الجامعة ؛ ووصف أهداف الإجراءات المتخذة بحيث تجسد جميع الإجراءات التفصيلية التي يتعين على القيادات اتباعها والتي تعتبر حاسمة لنجاح الجامعة في المواجهات. (Garba,et al,2020)

٧- التعاون: التعاون بين القيادات الأكاديمية داخل وخارج الجامعة عندما يتعلق الأمر بالأمن السيبراني قد يكون استراتيجية مفيدة . (Redman,et al,2020) يمكن لتبادل المعلومات بين القيادات أن يسهل من تبادل الدروس المستفادة ، وخاصة في تحديد اتجاهات التهديدات وأساليب المواجهة. كما أنه يساعد القيادات على تطوير إجراءات الوقاية من الهجمات السيبرانية .(Aljohni ,et al,2021) ويسهم في تشكيل فرق لمناقشة التهديدات السيبرانية وتحليلها وبيان آثارها وكيفية التخفيف من هذه الآثار؟ (Peker ,et al,2018)

إن مشاركة القيادات الأكاديمية في وضع سياسة الأمن السيبراني وتنفيذها؛ لهو دليل على زيادة وعي القيادات بخطورة التهديدات السيبرانية التي تواجه الجامعة، والرغبة في الحفاظ على ممارسة مهام الجامعة بشكل طبيعي، وتقنين إجراءات وقاية الجامعة وحمايتها من كافة الأخطار.

القيادات الأكاديمية الجامعية وأدوارها

لكي يكون قادة الجامعات فعّالين في مواجهة التهديدات السيبرانية ، فإنهم يحتاجون إلى المعرفة الفنية والمهارات التقنية والإدارية ، للمشاركة الفاعلة في التخطيط المناسب وإدارة المشاريع والمبادرات السيبرانية. وهذه مهمة كبيرة تتطلب فهم مجموعة واسعة من موضوعات الأمن السيبراني وأساليبه. تتطلب استراتيجية الأمن السيبراني ؛ المشاركة من جميع مستويات القيادة في جميع أنحاء الجامعة. الفارق الرئيس بين هذه المستويات المختلفة هو مقدار المعرفة التقنية والفنية المطلوبة للنجاح. تختلف الأدوار والألقاب عبر الجامعات ذات الأحجام والأنشطة المختلفة ، لكن مقدار المعرفة التقنية التي يتطلبها المتخصصين تختلف اختلافًا كبيرًا عن تلك التي تتطلبها القيادات الأكاديمية الجامعية . (Redman,et al,2020) وفي هذا النطاق تؤكد دراسات (Wilbanks,2016) ، (Aljohni ,et al,2021) إن قضايا الأمن السيبراني في الجامعات ليست مشكلة تقنية بحتة بل مشكلة متعددة الأبعاد تحتاج معالجتها نهج متعدد التخصصات . فظاهرياً ، يعتبر هجوم برامج الفدية الذي يحجب بيانات الجامعة هجومًا تقنيًا ؛ ولكن كما يشير (Tibi ,et al,2019) فإن جزءاً لا يتجزأ من المخاطر السيبرانية والأمن السيبراني هي مشاكل الإدارة الجامعية ذاتها. كالبطيء في اتخاذ القرار والتردد والعشوائية؛ الذي يزيد من نجاح التهديدات السيبرانية في تحقيق أهدافها.

ومع ذلك، تظل القيادات الأكاديمية بحاجة إلى ما يكفي من الفطنة الفنية لفهم طبيعة الأمن السيبراني ، والقدرة على حل الخلافات، وإبداء الآراء الحاسمة في وضع الرؤى والخطط المختلفة للتعامل الأمثل مع التهديدات السيبرانية. (Redman,et al,2020)

لذلك قامت الجامعات الأمريكية بتوفير برامج تدريبية للقيادات الجامعية غير المتخصصة في المجالات التقنية ؛ لإمدادهم بأطر عمل وأفضل الممارسات لإدارة المخاطر المتعلقة بالأمن السيبراني منفصلة عن البنية التحتية لتكنولوجيا المعلومات المتخصصة المرتبطة عادةً بهذا الموضوع . (Garba,et al,2020) وبحيث تتضمن محتوى هذه البرامج محاضرات

ومناقشات تفاعلية ودراسات حالة تتعلق بالوعي العام بالأمن السيبراني ، ودور القادة غير التقنيين في إدارة الأمن السيبراني ، كيفية قياس مستوى الأمان الإلكتروني للجامعة ؟ كيفية التحدث بلغة الأمن السيبراني مع المتخصصين؟ ، وكيفية التأكد من أن الجامعة آمنة عبر الإنترنت قدر الإمكان؟). (George Washington University,2022)

ولكي نكون أكثر تفصيلاً وايضاحاً في عرض أدوار القيادات الأكاديمية في تنفيذ ممارسات الأمن السيبراني بالجامعات الأمريكية . فيمكن تناولها من خلال العناصر التالية:

١. صياغة استراتيجية الأمن السيبراني

تساهم القيادات الأكاديمية الجامعية في صياغة استراتيجية التعامل مع التهديدات السيبرانية؛ كما بجامعات جورج واشنطن ونيويورك وكاليفورنيا ، (New York University,2022) ،(University of California,2022) بحيث يتم تشكيل لجنة عليا من القيادات الجامعية وبحيث تمثل كل كلية ومعهد بعضو في هذه اللجنة إضافة إلى عدد من المتخصصين في مجال الأمن السيبراني، لوضع معالم تلك الاستراتيجية، والتي تهدف إلى:(New York University,2022) (George Washington University,2022) (University of California,2022)،)

- اتخاذ القرارات بشأن الهجمات السيبرانية التي تواجه الجامعة.
- التخطيط للمواجهة والتدخل في الهجمات السيبرانية.
- التقييم للإجراءات التي اتخذها المتخصصون في مواجهة الهجمات السيبرانية.
- الاشراف على تطوير خطط المواجهة للتهديدات السيبرانية.

كما تتكون هذه الاستراتيجية من:

- الإجراءات الإدارية التي يجب اتخاذها عند مواجهة التهديدات السيبرانية.
- الإجراءات القانونية المناسبة عند التعامل مع التهديدات السيبرانية.
- خطوات الامتثال والاستجابة التي يجب اتخاذها عند التعامل مع الهجمات الإلكترونية.
- إجراءات الإبلاغ عن الهجمات الإلكترونية.

٢. إطلاق حملات للتوعية بممارسات الأمن السيبراني.

تشرف القيادات الجامعية على إطلاق حملات للتوعية بممارسات الأمن السيبراني ؛ ففي بعض الجامعات الأمريكية كجامعات جورج واشنطن ، ونيويورك، وكاليفورنيا ونيوجيرسي

(New Jersey) وماريلاند(Maryland) تنفذ تلك الحملات تحت إشراف القيادات الجامعية ، وذلك كما يؤكد (Redman,et al,2020) لإنشاء "ثقافة عامة للتوعية الإلكترونية"(A general culture for electronic awareness) لمكافحة التصيد الاحتيالي ، وتستمر هذه الحملات مدة لا تقل عن شهر ؛ وغالباً ماتكون في شهر أكتوبر من كل عام . ويتم تسميته بالشهر الوطني للتوعية بالأمن السيبراني.(National Cybersecurity Awareness Month) وفي هذا الشهر يتم مراجعة وتحديث استراتيجيات الجامعات للأمن السيبراني، كما يتم تنفيذ حملة للتوعية بأخطار التهديدات السيبرانية ، وإجراءات للوقاية والتدخل فيها ، وتحديد دور كل فرد في الجامعة تجاه تلك التهديدات . كما يتم تقديم كتيبات مجانية تتضمن إرشادات لكيفية التعامل مع التهديدات السيبرانية وملصقات ، ومقاطع فيديو تشرح كيفية الحماية الشخصية من التهديدات الالكترونية . (George Washington University,2022)) ، (New York University,2022)، (University of California,2022) ، (New Jersey University,2022)، (University of Maryland,2022)

٣. المشاركة في التقييم السنوي لممارسات كليات الجامعة وإداراتها:

حيث يتم تشكيل فريق للتقييم برئاسة نائب رئيس الجامعة وعميد كلية علوم الحاسب ومدير الأمن السيبراني لتقييم الإجراءات التي اتخذتها الكليات والإدارات تجاه الأمن السيبراني ؛ كما بجامعات كولورادو (Colorado)، ونيفادا(Nevada) ومن أبرز تلك الإجراءات: ((University of University of Colorado,2022) Nevada,2022)

- التأكد من توافر استعدادات لمواجهة التهديدات السيبرانية .
- توافر سياسات مفعلة للأمن السيبراني .
- توافر البنية التحتية للتكنولوجيا .
- نوعيات البرامج التدريبية التي تم تقديمها إلى أعضاء هيئة التدريس والموظفين والطلاب .
- شكل التعاون بين أقسام الكلية وإدارتها عند التعامل مع التهديدات السيبرانية .

ويعتمد هذه التقييم على تقارير موثقة تتضمن كافة الإجراءات التي تم اتخاذها وبيان سلبياتها وايجابياتها ومقترحات مستقبلية لتطوير وتحسين تلك الممارسات، ويتم اعتماد تلك التقارير من المجالس الحاكمة لكل كلية ورفعة إلى لجنة التقييم. كما يمكن أن تعتمد اللجنة على التقارير التي تقوم بها الكليات من خلال خبرائها، أو تشكيل لجان مستقلة من داخل الجامعة للتقييم

ورفع تقاريرها مباشرة إلى لجنة التقييم مع إخطار عميد كل كليـــة بمـــضمون التقريـــر لاتخـــاذ إجراءات التحسين.

٤. نشر الممارسات الصحيحة

تشارك القيادات الجامعية في جامعة جورج واشنطن بالاشراف على تطبيق الممارســـات الصحيحة في مجال الأمن السيبراني والتي ثبت جودتها وتميزها في المؤسسات المناظرة. إضافة إلى الإشراف على نشر أفضل ممارسات الأمن السيبراني التي طبقت سابقاً في كليـــات وإدارات الجامعة واتضح تميزها في تطوير أساليب الوقاية والمواجهة ؛ ويتم توزيع الممارســـات علـــى كافة كليات وإدارات الجامعة. وتستخدم هذه الممارسات كمورد أساسي عند تطوير معايير الأمن السيبراني بالجامعات. (George Washington University,2022)

٥- تطوير التعاون بين الجامعات والمعهد الوطني للمعايير والتكنولوجيا

تعمل القيادات الجامعية بجامعات جورج واشنطن ونيويورك على تطوير التعـــاون مـــع المعهـــد الـــوطني للمعـــايير والتكنولوجيـــا National Institute of Standards and Technology)؛ وذلك لتطوير معايير وممارسات الأمن السيبراني لمواجهة التهديدات المختلفة ، ويتم تحديد أطر التعاون من خلال تشكيل فريق عمل مشترك من رؤســـاء الجامعـــات ومـــدير المعهد يندرج منه فريق فني من المتخصصين بكل من الجامعات والمعهد . ويتم تطبيق المعايير والممارسات المطورة بالتعاون بين أفراد الفرق على مواقف مصطنعة للتأكد من جودة المعـــايير والممارســـات ؛ ومـــن ثـــم يـــتم اعتمادهـــا للتطبيـــق الفعلـــي . (George Washington University,2022) ، (New York University,2022)

٦- المشاركة في وضع معالم برامج إدارة المخاطر

تشارك القيادات الجامعية في تطوير برامج لإدارة المخاطر بالجامعات ؛ و الذي يعمـــل على تلافي الأزمات وتقليل تأثيرها على الحرم الجامعي . وتعتقد القيادات أنه من خـــلال وجـــود برامج لإدارة المخاطر ، يمكن التأكد من أن الجامعة مستعدة تمامًا في حالة وقوع هجـــوم مـــا أو تهديد محتمل . ولا يعني الاستعداد هنا تمكين الموارد البشرية الجامعيـــة مـــن التعـــرف علـــى الهجمات السيبرانية فقط ، ولكن أيضًا القدرة على التصرف بسرعة إذا تـــم تنفيـــذ أي هجـــوم أو تهديد ما.

في هذا النطاق يشير (Fouad,2021)أن مشاركة القيادة والتزامها بالتخطيط والتنفيذ للبرنامج أمرًا حاسمًا لنجاحه. وهذا ما يحدث في جامعات واشنطن وتكساس(Texas) حيث يتم تعيين مدير تنفيذي للبرنامج متخصص في الأمن السيبراني، ويتم دعم البرنامج مالياً، مع تحديد أهداف البرنامج ، والتي تشمل :(George Washington University,2022) (2022, University of Texas)

- تحديد المخاطر الحالية بكل كلية وإدارة وقسم .
- تحديد المخاطر المستقبلية "محتملة الحدوث" .
- تطوير استراتيجيات التخفيف على أساس تلك المخاطر .
- توثيق الاستراتيجيات المستخدمة في التنفيذ .
- إنشاء إجراءات تغذية مرتدة مستمرة بين مجلس البرنامج والفريق ومسؤولي الإدارات والأقسام بالجامعة .

ولا تتوقف القيادات الجامعية عند المشاركة في التخطيط والتنفيذ للبرنامج؛ بل تسعى إلى تطوير البرنامج بعد انتهاء كل مواجهة لأي تهديد سيبراني .

٧- التدريب والتأهيل للموارد البشرية للجامعة

تعمل القيادات الجامعية على تطوير قدرات الموارد البشرية بالجامعات التي تنتمي إليها في مجالات الأمن السيبراني من خلال وضع نظام للتدريب تحت مسمى SafeColleges كما بجامعات كاليفورنيا ونيوجرسي ؛ حيث يتم التخطيط للنظام من خلال تشكيل لجنة تضم أحد نواب رئيس الجامعة ومدير تطوير الموارد البشرية ومدير مركز التدريب ؛ ويكون من أبرز مهامها التخطيط لتقديم وتطوير البرامج التدريبية الموجهة للموارد البشرية وتفوض اللجنة أحد الكفاءات المتخصصة في مجال التدريب بالإشراف على البرامج التدريبية ورفع تقريره للجنة لاعتماده.(Aljohni al,2021 et,) تقدم هذه البرامج للقيادات الأكاديمية وأعضاء هيئة التدريس والموظفين والطلاب ، وتضم تلك الدورات الموضوعات التالية (نظرة عامة على الأمن السيبراني ، أساليب الحماية من البرامج الضارة ، أساسيات أمان كلمة المرور ، أساسيات أمان الملفات ، سلامة البريد الإلكتروني والرسائل).(Redman,et al,2020)

٨- **الشراكة بين الجامعات وشركات الأمن السيبراني**

تهتم القيادات الجامعية بجامعات نيويورك وكولورادو (Colorado) وماساتشوستس (Massachusetts) بإضافة خبرات جديدة لتطوير ممارسات الأمن السيبراني بالجامعات ؛ لذا نجد بعض القيادات الجامعية تعقد شراكات وتعاون مع بعض الشركات المتخصصة في الأمن السيبراني ؛ وذلك لتحقيق عدة أهداف منها : تطوير إجراءات الحماية لبيانات الجامعة ، تطوير ممارسات الأمن السيبراني ، تطوير قدرات الموارد البشرية بالجامعات من خلال البرامج التدريبية ، المشاركة في تقديم البرامج العلمية كالشهادات الاحترافية في الأمن السيبراني وبرامج الدبلوم والماجستير والدكتوراه. (University of Colorado,2022)، (University of Massachusetts,2022) ومن أبرز الشراكات بين الجامعات وشركات الأمن السيبراني؛ الشراكة بين جامعة نيويورك وشركة(Wiz Industry (Cloud للأمن السيبراني، وجامعة كولورادو وشركة(Deepwatch Industry Security) ، وجامعة ولاية ماساتشوستس وشركة (Nuance Industry Software) .

٩- **وضع إطار عمل لتحسين الأمن السيبراني بالجامعات**

تلتزم القيادات الجامعية في بعض الجامعات الأمريكية كجامعة ولاية بنسلفانيا وتكساس بإصدار قرارات بوضع إطار عمل لتحسين ممارسات الأمن السيبراني بالجامعات. يتضمن هذا الإطار لمحة عامة عن إطار عمل الأمن السيبراني ، ومعايير الأمن السيبراني بالجامعة وكيفية استيفاءها ، إضافة إلى الممارسات الجيدة للأمن السيبراني. ويتم توزيع الإطار على كافة الكليات والإدارات بالجامعة. ولا يقتصر الأمر على توزيع الإطار بل العمل به أو بمعنى آخر تفعيله ، كما يتم تقديم تقرير سنوي عن إطار العمل يتضمن الملاحظات التي تم اكتشافها عند العمل بالإطار كنقاط الضعف التي تم ملاحظتها ومن ثم يتم علاجها وتضمين التعديلات بالإطار الجديد. (University of pennsylvania,2022) ، (University of Texas ,2022)

١٠- **وضع دليل أمن المعلومات:**

في إطار حرص القيادات الجامعية على أمن المعلومات وتنويعها لأساليب الوقاية والحماية تلجأ بعض الجامعات كجامعات جورج واشنطن ونيويورك وجامعة بنسلفانيا ؛ بوضع أدلة لأمن المعلومات، يقوم بوضع تلك الأدلة خبراء تكنولوجيا المعلومات بالجامعة . تدعم هذه الأدلة تطوير وتنفيذ سياسة أمن المعلومات وصيانتها. جنباً إلى جنب مع الوصول إلى الموارد

التكنولوجية الأخرى، وبحيث يتضمن الدليل أهداف الدليل ومبرراته، وإجراءات الحماية لمعلومات وبيانات الجامعة ، وكيفية تنفيذ تلك الإجراءات ، وأدوار الكليات والإدارات الداخلية تجاه حماية المعلومات . (George Washington University,2022)، (New York University,2022) (University of pennsylvania,2022)

١١- توفير المنصات الالكترونية

تقوم القيادات الجامعية ببعض الجامعات الأمريكية كجامعات شيكاغو (Chicago)وميسوري (Missouri) بتأسيس وتفعيل منصات الكترونية على مواقع الجامعات ؛ وذلك لتحقيق عدة أهداف منها : تزويد الموارد البشرية بكافة المعلومات عن التهديدات السيبرانية والأخطار المحيطة بالجامعة ، الرد على استفسارات المستفيدين فيما يتعلق بالتهديدات السيبرانية من قبل خبراء الأمن السيبراني بالجامعة . كما تساعد هذه المنصات فرق المخاطر بكل جامعة على تقييم السيناريوهات بسرعة وتقدير التأثيرات المختلفة . (University of Missouri,2022) و(University of Chicago ,2022)

١٢- المساهمة في التخطيط والتصميم للخطة الاستراتيجية للأمن السيبراني بالجامعات

ففي جامعات كنتاكي (Kentucky) ، وكولورادو (Colorado)تقوم القيادات الجامعية بالعمل على تصميم خطة استراتيجية للأمن السيبراني؛ من خلال تشكيل لجنة عليا للخطة الاستراتيجية برئاسة رئيس الجامعة وأحد نوابه وعدد من عمداء الكليات ، والمدير التنفيذي للخطة الاستراتيجية. يندرج منها عدد من اللجان الفرعية المنوط بها مهام التنفيذ. تحدد الخطة إطار عمل أولويات الجامعة وأقسامها فيما يتعلق بالأمن السيبراني. وبحيث يتم التشاور مع الكليات والإدارات المختلفة أثناء صياغة الخطة وبحيث تكون الكليات شركاء أساسيين في تنفيذها. وستدعم الخطة الاستراتيجية بخطة تنفيذ أكثر تفصيلاً تشرف عليها اللجنة. (University of Kentucky,2022) ((University of Colorado,2022

١٣- المساهمة في إنشاء أندية الأمن السيبراني

كما بجامعات نيويورك ، ونيوجيرسي تسعى القيادات الجامعية إلى إنشاء أندية للأمن السيبراني بهدف زيادة الوعي بالمسائل والقضايا المتعلقة بالأمن السيبراني داخل الجامعة وخارجها إضافة إلى تشجيع الممارسات الآمنة عبر الإنترنت، وتعزيز أهمية مواجهات التهديدات والقرصنة الالكترونية. ويسمح لكافة أفراد المجتمع الجامعي من أعضاء هيئة التدريس والطلاب

والموظفين بالدخول إلى النادي والانخراط ببرامجه (New York University,2022) (New Jersey University,2022). كما ينظم نادي الأمن السيبراني مسابقات الأمن السيبراني ، ويعرض لمشاريع الأمن السيبراني بالجامعة وإجراءاتها لاطلاع أفراد مجتمع الحرم الجامعي عليها.

١٤- تشكيل فريق التخطيط للأمن السيبراني

في بعض الجامعات الأمريكية كجامعات فلوريدا(Florida) ولويزيانا(Louisiana) ، وبوسطن (Boston) تعمل القيادات الجامعية على تطوير جوانب الوقاية من الأخطار والتهديدات السيبرانية ؛ وذلك من خلال تشكيل ما يسمى بفريق التخطيط حيث يصدر رئيس الجامعة قرار بإنشاء هذا الفريق ويكون من مهامه وقاية الجامعة من خطر التهديدات السيبرانية وتقوية إجراءات الحماية . (University of Florida,2022)

(Louisiana State University,2022) ، (Boston University,2022) يشمل هذا الفريق عدد من الموظفين الذين يعملون في إدارة الأمن السيبراني وإدارة الحوادث السيبرانية(cyber incident management) ، وإدارة حالات الطوارئ (emergency management) ، وموظفي تكنولوجيا المعلومات ، وأعضاء هيئة التدريس المتخصصين في الأمن السيبراني بالجامعة ، وبعض الشركاء الفيدراليين(Federal Partners) من خارج الجامعة. (Louisiana State University,2022) يرأس الفريق أحد نواب رئيس الجامعة ويعاونه مدير تنفيذي عضو هيئة تدريس متخصص في الأمن السيبراني. يركز عمل الفريق على صياغة الخطط التنفيذية لكل كلية وإدارة وقسم والاشراف والمتابعة على تنفيذها، وتقديم الدعم الفني لها. يعتمد عمل الفريق على فهم مسؤولي الكليات والإدارات والأقسام للتهديدات السيبرانية المحتملة والتي قد تؤثر على عملهم؛ ومن ثم يبدأ الفريق في تدريب هؤلاء المسؤولين على فهم طبيعة هذه التهديدات ثم تحديد كيفية التعامل معها؟ (University of Florida,2022) كما يعمل الفريق مع المسؤولين على تحديد التهديدات السيبرانية المحتملة، ومناطق الضعف التي يمكن لهذه التهديدات التأثير فيها والدخول من خلالها .

١٥- تفعيل أدوار مراكز الأمن السيبراني

تلعب مراكز الأمن السيبراني(cyber security centers) بالجامعات الأمريكية دوراً هاماً في الحفاظ على حالة الثبات والاستقرار في أحرامها الجامعية . يشير (Tibi ,et al,2019)

أن تحقيق هذه المراكز لأدوارها مرهون بالقيادة الجامعية التي تؤمن بأهمية هذه المراكز وتدعم عملها من خلال الوفاء بكافة متطلباتها البشرية والمالية والمادية .

تعمل القيادات الجامعية على فتح قنوات اتصال مباشرة بينها وبين قيادة تلك المراكز ؛ وذلك للاطلاع بصفة مستمرة على الأوضاع داخل الجامعات ، وتلبية احتياجات تلك المراكز . ففي مركز الأمن السيبراني بجامعة كاليفورنيا – على سبيل المثال – تقوم بعض القيادات الجامعية كرئيس الجامعة ونوابه بحضور بعض الاجتماعات واللقاءات التي يعقدها المركز ، كما تشارك تلك القيادات في إعداد خطط المواجهة ، والاطلاع على الإجراءات التي يتخذها المركز تجاه التهديدات السيبرانية ، كما تشارك في فرق العمل التي يشكلها المركز عند مواجهة التهديدات ؛ وذلك لاكتساب الخبرة في المواجهة ، إضافة إلى السرعة في اتخاذ القرارات – خاصة – التي قد تحتاج إلى موافقة تلك القيادات. (university of California,2022)

يتضح مما سبق أن تهديدات الأمن السيبراني شكلت خطرًا متزايدًا على الجامعات الأمريكية. كما اتضح أن الجامعات تعد أهدافاً لهذه التهديدات ؛ وذلك لسببين. أولا أن الجامعات مثلها كالمؤسسات المالية والتجارية والعسكرية تضم مجموعة متنوعة من المواد المالية والبشرية و البيانات والمعلومات البحثية الهامة ، ثانياً أن ثقافة الوصول المفتوح لمواقع الجامعات أسهل كثيراً من غيرها من المؤسسات المؤمنة كالمؤسسات العسكرية ؛ مما يجعلها هدفاً سهل المنال للمخربين ؛ وهو ما احتاطت إليه الجامعات الأمريكية نتيجة كثرة تلك التهديدات وعملت على تفعيل مراكز وفرق الأمن السيبرانية في أحرامها الجامعية إضافة إلى تفعيل البروتوكولات الإرشادية وتوزيعها على الموارد البشرية بالجامعات لزيادة الوعي بالتهديدات السيبرانية وتطوير ممارساتهم تجاهها .

إذن ؛ كان للقيادات الأكاديمية بالجامعات الأمريكية دوراً هاماً في تفعيل وتطوير ممارسات الأمن السيبراني في الجامعات؛ فكان ذلك – أيضاً– من خلال التواصل بين خبراء تكنولوجيا المعلومات والأمن السيبراني وقادة الجامعات بصورة مستمرة لاطلاعهم على الممارسات والتطورات الحادثة في الحرم الجامعي، مما زاد من قدراتهم على فهم التهديدات السيبرانية و فَعل مشاركاتهم الإيجابية في اتخاذ القرارات والتخطيط ووضع الاستراتيجيات الخاصة بالأمن السيبراني بالجامعة . كما لم تمنع الوظائف الأكاديمية للقيادات الجامعية من التعرض والخبرة في قضايا الأمن السيبراني: فغالبية القيادات الأكاديمية بالجامعات مشاركون

على مستوى الكليات أو الجامعة في فرق الأمن السيبراني ، ويحصلون على دورات تدريبية في مجال الأمن السيبراني . بل ويضعون قضايا الأمن السيبراني على جداول أعمالهم.

المحور الرابع تطوير أدوار القيادات الجامعية المصرية لتعزيز ممارسات الأمن السيبراني

وفقًا لنتائج الإطار النظري ونتائج الدراسات السابقة، ودراسة أدوار القيادات الأكاديمية بالجامعات الأمريكية في تعزيز ممارسات الأمن السيبراني، فقد خلصت الدراسة الحالية إلى وضع رؤية مقترحة لأدوار القيادات الأكاديمية بالجامعات المصرية في تعزيز ممارسات الأمن السيبراني؛ وسيتم تناول ذلك تفصيلًا وفق ثمانية محاور رئيسة تشمل :

١- فلسفة الرؤية المقترحة.

٢- منطلقات الرؤية المقترحة.

٣- مبررات الرؤية المقترحة.

٤- أهداف الرؤية المقترحة.

٥- مراحل بناء الرؤية المقترحة:

أ- التخطيط .

ب- تشخيص الواقع.

ج- إجراءات التنفيذ؛ وتشمل: (الرؤية والرسالة-الأهداف- التعليم والتدريب-الشراكة – التقويم).

٦- متطلبات تنفيذ الرؤية المقترحة.

٧- معوقات تنفيذ الرؤية المقترحة وإمكانية التغلب عليها.

٨- الجهات المنوط بها تنفيذ الرؤية المقترحة.

أولاً : فلسفة الرؤية المقترحة

تنطلق فلسفة الرؤية المقترحة من النظرة إلى الجامعات باعتبارها مؤسسات مدعمة ومعززة للتقدم العلمي والتكنولوجي في المجتمع ، وتسهم بدور رئيس في الحياة الثقافية ، إضافة إلى انتاجها للمعرفة وتثقيفها لموارد بشرية مؤهلة تأهيلا عالياً والتي تعتمد عليهم الاقتصادات الحديثة. ومن ثم فإن الحفاظ على ذلك الدور منوط بقيادة جامعية متميزة تعمل على حماية ووقاية تلك المؤسسة من كافة الأخطار المحدقة بها تخطيطاً وتنفيذاً وتقويماً باستخدام كافة الأساليب والمداخل العلمية.

ثانياً: منطلقات الرؤية المقترحة

تنطلق الرؤية المقترحة من مجموعة من المنطلقات؛ ويمكن تناولها تفصيلًا على النحو التالي:

١- رؤية مصر ٢٠٣٠ والتي ترتكز في أحد محاورها على التنمية الشاملة للجامعات المصرية من خلال تطوير كوادرها القيادية ومواردها البشرية وبنيتها الأساسية خاصة التقنية منها؛ وذلك للاضطلاع بدورها الحاسم في خدمة المجتمع وتنمية البيئة المحلية.

٢- التوجهات العالمية في مجال تطوير الجامعات؛ والتي تركز على التطوير التقني التكنولوجي في ممارسة مهامها الأكاديمية والبحثية والخدمية.

٣- نتائج وتوصيات ومقترحات الدراسات السابقة : والتي أوصت بتطوير الأداء القيادي لمواجهة التحديات التي تواجه الجامعات خاصة ما يتعلق بالتهديدات السيبرانية.

ثالثاً: مبررات الرؤية المقترحة.

تتمثَّل في المبررات التي استدعت وجود الرؤية المقترحة، والتي من أبرزها:

١- الإسهام في تحقيق رؤية مصر (٢٠٣٠م).

٢- التطورات المستجدة والتوجهات العالمية التي تنادي بأدوار فاعلة للقيادات الجامعية في تفعيل ممارسات الأمن السيبراني .

٣- كثرة التهديدات السيبرانية التي تواجه الجامعات المصرية خاصة بعد توجهها نحو تفعيل ممارساتها الالكترونية في الجوانب الأكاديمية والفنية والإدارية والبحثية مما يستدعي تطوير ممارسات الأمن السيبراني وتفعيل أدوار قياداتها الجامعية .

٤- توافر موارد بشرية متميزة ومتخصصة في مجال الأمن السيبراني بالجامعات المصرية والتي يمكن استثمارها في تنفيذ الرؤية المقترحة .

رابعًا: أهداف الرؤية المقترحة

تسعى الرؤية المقترحة لتحقيق العديد من الأهداف، وتتمثَّل في الآتي:

١- تفعيل أدوار القيادات الجامعية المصرية في تنفيذ ممارسات الأمن السيبراني .

٢- تحديد إطار للتعليم والتدريب تسير عليه القيادات الجامعية المصرية ؛ بحيث يتفق مع المعايير المثالية للتعليم والتدريب في الأمن السيبراني .

٣- وضع نظام متميز لتقويم أدوار القيادات الجامعية المصرية وتحديد مجموعة الأساليب التي يمكن الاعتماد عليها، سواء الأساليب الداخلية أو الخارجية ؛ والتي ترتبط بممارسات الأمن السيبراني .

٤- تحديد أهم المعوقات التي يمكن أن تحول دون تفعيل أدوار القيادات الجامعية في تنفيذ ممارسات الأمن السيبراني، وسبل التغلب على تلك المعوقات.

خامسًا: مراحل بناء الرؤية المقترحة

لا يمكن بناء الرؤية المقترحة دون تحديد خطوات ومراحل واضحة للبناء، والتي من أبرزها:

المرحلة الأولى : التخطيط

تُعتبر مرحلة التخطيط لبناء الرؤية المقترحة من أهم المراحل التي يجب الاهتمام بها؛ حيث إنّ أيّ خلل في هذه المرحلة يحول دون تنفيذ تلك الرؤية، ويؤدي إلى عدم تنفيذها على الوجه الأكمل؛ ويمكن تحديد مراحل التخطيط لبناء الرؤية المقترحة على النحو التالي:

١- تحديد مبادئ الفلسفة التي ستُبنى عليها الرؤية المقترحة. والتي لا بد أن تتفق مع الممارسات العالمية وثوابت العمل الجامعي ، ويتم تحديد تلك المبادئ في صورة نقاط رئيسة محددة يمكن إيضاحها بشكل تفصيلي في مجموعة إجراءات تفصيلية .

٢- تحديد القيم التي ستبنى عليها الرؤية؛ وبحيث تتلخص تلك القيم في: الالتزام ، والمشاركة ، والتعاون .

٣- تحديد عناصر الرؤية المقترحة، ووضع مجموعة من القراءات المتعمقة والنماذج الفعلية لممارسات قيادية متميزة، ودراستها بشكل متعمق للاستفادة منها في التعرف على نقاط القوة والضعف فيها، ومن ثم تبنِّي نقاط القوة، ومحاولة إيجاد حلول لنقاط الضعف، وتبنِّي تلك الحلول في الرؤية المقترحة.

٤- وضع الرؤية المقترحة في شكل مشروع يتم عرضه على مجالس الجامعات ، وقيام تلك الجهات بتحديد النقاط السلبية في ذلك المقترح، والقيام بإعادة صياغتها وتلافيها.

٥- تحديد متطلبات تنفيذ الرؤية المقترحة في شكل قائمة محددة وواقعية وواضحة يمكن تحقيقها .

المرحلة الثانية: تشخيص الواقع

تنطلق عملية تشخيص الواقع من أجل تحديد نقاط القوة والضعف بالجامعات المصرية عامة والقيادات الجامعية خاصة للتحوُّل نحو تبنِّي الرؤية المقترحة، وهي على النحو التالي:

- **نقاط القوة:**

١- وجود رؤية مصر (٢٠٣٠م) التي تتضمن محددات رئيسة يمكن الاعتماد عليها في بناء الرؤية المقترحة، والتي تتعلق بإعادة بناء البنية التكنولوجية في الجامعات المصرية وتفعيل وتأصيل أدوار القيادات الجامعية حول الحفاظ عليها والتطوير الدوري لها.

٢- توجُّه الدولة في الآونة الأخيرة وبعض الجامعات المصرية كجامعة القاهرة لتبنِّي مفاهيم تدعم التحول نحو تطوير ممارسات الأمن السيبراني وتفعيل دور القيادات الجامعية تجاهه.

٣- توجُّه القيادات الجامعية المصرية – جامعة القاهرة أنموذجاً – نحو الاستثمار في برامج الأمن السيبراني سواء للدراسة، أو الإعداد والتطوير؛ ما يُحقِّق لها مكاسب على المدى القريب والبعيد.

٤- ميول القيادات الجامعية المصرية نحو تفعيل ممارسات الأمن السيبراني، وتنمية قدرات أفرادها، وتحقيق مزيد من الآمان للحرم الجامعي.

٥- توافر مراكز تدريب على أعلى مستوى بالجامعات مزودة بكافة الإمكانات .

٦- توافر خبراء متخصصين في تدريب القيادات الجامعية على كيفية تنفيذ أدوارهم تجاه ممارسات الأمن السيبراني بالجامعات.

- **نقاط الضعف:**

١- قلة وجود متخصِّصين في الأمن السيبراني في بعض الجامعات.

٢- تركيز بعض القيادات الجامعية المصرية في المقام الأول على تحقيق فائض اقتصادي ، وممارسات الأدوار الأكاديمية .

٣- تعقُّد بعض الإجراءات التشريعية والإدارية بالجامعات.

٤- عدم اقتناع بعض القيادات الجامعية بأهمية وجود رؤية فاعلة للأمن السيبراني بالجامعات، ومعارضتهم لتفعيل ممارسات تلك الرؤية .

٥- التكلفة المالية التي ستقع على الجامعات من جرّاء إنشاء رؤية مقترحة للأمن السيبراني بالجامعات.

- **إجراءات التحسين**

١- إعداد متخصصين في مجال الأمن السيبراني في الجامعات التي تعاني من ندرة هؤلاء المتخصصين .

٢- التأكيد للقيادات الأكاديمية وبالأدلة والشواهد أن تحقيق مكاسب مالية للجامعة مرهون بالحفاظ على سمعتها وصورتها في المجتمع والتي يمكن أن تتأثر نتيجة الهجمات السيبرانية عليها ؛ مما قد يخل بتلك الصورة ويسهم في عدم تحقيق المكاسب المالية المأمولة .

٣- تشكيل لجنة من القانونين بالجامعة لدراسة الإجراءات القانونية والعمل على تعديلها وتغييرها للتيسير من تطبيق إجراءات الأمن السيبراني . أما الإجراءات الإدارية فيمكن وضع نماذج إجرائية للتعامل مع ممارسات الأمن السيبراني بحيث لا تتعارض تلك الإجراءات مع الإجراءات الجامعية للمهام والأنشطة الإدارية والأكاديمية أو البحثية الأخرى وبحيث لا يحدث تعارض أو تداخل معها .

٤- تعريف القيادات الأكاديمية بأهمية الأمن السيبراني بالجامعة وأهمية تطبيق الرؤية المقترحة، والتأكيد على اهتمام القيادة السياسية ورؤية مصر ٢٠٣٠ بالأمن السيبراني للحفاظ على المؤسسات المصرية من التهديد والاختراق ، كما يمكن وضع الاهتمام بالأمن السيبراني والمشاركة في اللجان ذات الصلة كمعيار لتقويم أداء القيادات الأكاديمية واستمرارها في مناصبها .

٥- التوضيح للقيادات الأكاديمية بأن الرؤية المقترحة تكلفة تطبيقها بالجامعات غير مرتفعة إذا ما تم مقارنتها بالفوائد التي ستجنيها الجامعات من تطبيقها وممارسة أنشطتها؛ كما ستصبح تلك التكلفة قليلة للغاية خاصة إذا ما كانت الجامعات تمتلك متخصصين في الأمن السيبراني ، ولديها شبكة الكترونية مفعلة لتنفيذ الأنشطة والمهام المختلفة.

المرحلة الثالثة: إجراءات تنفيذ الرؤية المقترحة

يمكن تناوُل إجراءات تنفيذ الرؤية المقترحة التي سيتم تبنِّيها من قبل القيادات الجامعية المصرية من خلال تحديد أهم عناصرها، والتي تشمل:

الإجراء الأول: بناء رؤية ورسالة لأدوار القيادات الجامعية

١- الرؤية

في البداية، وقبل بناء الرؤية؛ ينبغي أنْ ترتكز الرؤية على مجموعة أُسس تتمثَّل فيما يأتي:

أ- دعمها لعملية الأمن السيبراني بالجامعة.

ب- التزامها بدمج المعارف العلمية للأمن السيبراني بالنواحي التطبيقية والممارسات العملية الجامعية.

ت- احترامها لروح البحث والإبداع في مجال الأمن السيبراني.

ث- دعمها لمفهوم الاستدامة في مجالات الأمن السيبراني.

ج- اهتمامها بإعداد وتطوير مهارات الكوادر البشرية في مجال الأمن السيبراني بصورة رئيسة.

ح- دعمها لثقافة تنظيمية لدى الموارد البشرية بالجامعة نحو تبنِّي مفاهيم الأمن السيبراني عند ممارسة مهامها المختلفة .

وبناءً على ذلك؛ فإن رؤية القيادات الجامعية تتمثَّل في ((*تميز القيادات الأكاديمية المصرية عالمياً في وقاية وحماية الجامعات من التهديدات السيبرانية*")) .

٢- الرسالة

تُعتبر الرسالة ترجمة واقعية لرؤية القيادة الجامعية فيما يتعلق بجوانب الأمن السيبراني، ومن المهم وقبل صياغة الرسالة مراعاة الدراسة المتعمقة لرؤية الجامعة ورسالتها فيما يتعلق بجوانب الأمن السيبراني ؛ بحيث تشتق رؤية ورسالة القيادة الجامعية من رؤية ورسالة الجامعة .

ولعل من أبرز الأسس التي ترتكز عليها رسالة القيادات الجامعية:

أ- التخطيط لتفعيل ممارسات الأمن السيبراني بالحرم الجامعي.

ب- دفعها للموارد البشرية لتنمية قدراتهم وامكاناتهم في مجال الأمن السيبراني، من خلال تدريبهم بشكل متميز.

ت- توفير المتطلبات البشرية والمالية لتحقيق الرسالة .

ث- دعم العمل الجماعي لتحقيق فلسفة الأمن السيبراني في الجامعة.

ج- دعم المواهب البشرية المختلفة الموجودة بالجامعة.

ح- تقويم ممارسات الأمن السيبراني وتطويرها بشكل مستمر .

وبناءً على ذلك؛ فإن رسالة القيادات الجامعية تتمثل في أنْ "تسعى القيادات الجامعية إلى تفعيل ثقافة الأمن السيبراني وتطوير ممارساته في الحرم الجامعي من خلال التخطيط الجيد والتنفيذ الاحترافي والتقويم الشامل بما يحقق طموحات الجامعات عامة والقيادات خاصة في تحويل الجامعات – في أحد أدوارها – إلى مراكز متخصصة في الأمن السيبراني تفيد نفسها وتخدم غيرها من المؤسسات المجتمعية.

الإجراء الثاني: أهداف الرؤية المقترحة

تتمثَّل أهداف الرؤية المقترحة فيما يلي:

أ- التحسين المستمر لقدرات القيادات الجامعية على المشاركة في التخطيط لمبادرات الأمن السيبراني بالجامعة.

ب-تثقيف وتوعية القيادات الجامعية بخطورة الهجمات السيبرانية وكيفية مواجهتها .

ت-إعداد موارد بشرية متخصصة في مجال الأمن السيبراني لكي تصبح ككتل حرجة تنمي قدرات الموارد البشرية بالجامعة.

ث-عقد العديد من الشراكات مع بعض الشركات العالمية ؛ للاستفادة من قدراتها في تطوير إمكانات الجامعات في مجال الأمن السيبراني ، واعتبار الجامعات فيما بعد كمراكز معتمدة لتلك الشركات.

ج-الاستثمار الأمثل لامكانات الجامعة المادية والبشرية في تطوير برامج للأمن السيبراني وتقديمها بمقابل مالي للمؤسسات المجتمعية العامة والخاصة والاستثمارية.

ح-توظيف وتطبيق الأبحاث العلمية بشكل مباشر في تطوير ممارسات الأمن السيبراني بالجامعة .

خ-توفير الدعم المادي والمعنوي لتطوير ممارسات الأمن السيبراني بالجامعة.

الإجراء الثالث التطوير التنظيمي

ويتبلور هذا الإجراء في ضرورة وجود وحدة تنظيمية أو مركز منوط به حماية الجامعة من التهديدات السيبرانية ، ويشكل بقرار من رئيس الجامعة وبرئاسته أو برئاسة أحد نوابه وبحيث

يضم مجموعة من الأعضاء المتخصصين ، ويتم اختيار أحدهم ليكون مديراً تنفيذياً للمركز أو الوحدة . ويكون من مهام المركز/الوحدة تطوير إجراءات الحماية من التهديدات السيبرانية ، إعداد خطط وسيناريوهات للمواجهة ، إعداد برامج للوقاية والحماية ، إعداد موارد بشرية جامعية مؤهلة للتعامل مع التهديدات السيبرانية، تقديم برامج تدريبية احترافية لإعداد المستفيدين في مجالات الأمن السيبراني .

الإجراء الرابع: التعليم والتدريب في الرؤية المقترحة

وفيما يخص التعليم والتدريب بالرؤية، فيتعين أن يرتكز على:

أ- تقديم برامج تعليمية متنوعة للقيادات الجامعية لتنمية مهارات الأمن السيبراني لديهم؛ وبحيث يصير لديهم المعرفة الكافية بجدوى وأهمية ممارسات الأمن السيبراني؛ وكيفية تطبيق تلك الممارسات في الجامعة.

ب-مشاركة القيادات الجامعية بفعاليات الأمن السيبراني من ندوات ومؤتمرات – خاصة – ما يتعلق منها بالأدوار الحديثة للقيادات الجامعية تجاه ممارسات الأمن السيبراني.

ت-تقديم برامج تدريبية للموارد البشرية بالجامعة وكذلك الطلاب لزيادة وعيهم بممارسات الأمن السيبراني وتنمية قدراتهم على تفعيلها وتطبيقها عند ممارسة مهامهم المختلفة.

ث-توفير مراجع علمية متميزة في مجال الأمن السيبراني وتضمينها بمكتبات الجامعة المختلفة للاطلاع والاستزادة العلمية للقيادات والموارد البشرية بالجامعة.

ج-إعداد مراكز تدريب متخصصة تهدف إلى تنمية الكوادر البشرية التي تعمل بالجامعة وخارجها في مجالات الأمن السيبراني.

سادسًا: متطلبات تنفيذ الرؤية المقترحة

يرتكز تنفيذ الرؤية المقترحة على العديد من المتطلبات، وتتمثَّل في الآتي:

١- تبنِّي القيادات الجامعية لفلسفة رؤية مصر (٢٠٣٠م) التي تدعم التوجه نحو تأسيس بنية تكنولوجية بالجامعات المصرية والحفاظ عليها وصيانتها.

٢- تهيئة القيادات الجامعية لتقبُّل فكرة تطوير وتنفيذ ممارسات الأمن السيبراني بالجامعات، من حيث الاستعداد بتوفير تمويل للإنفاق عليه، وتهيئة الموارد البشرية بالجامعات لقبول تطوير وتطبيق تلك الممارسات وبيان أهميتها وجدواها لتحسين الأداء.

٣- توفير البرامج التدريبية الكافية لتنمية مهارات الأمن السيبراني لدى القيادات الجامعية ؛ بما يمكنهم من اتخاذ القرارات المهمة فيما يخصّ بتنفيذ الرؤية المقترحة .

٤- التزام القيادات الجامعية بتنفيذ الرؤية المقترحة وتطوير ممارسات الأمن السيبراني بالجامعات.

٥- توفير قيادات في الوحدات الأكاديمية بكل جامعة تعمل على نشر ثقافة الأمن السيبراني، وتعمل أيضًا على تهيئة الموارد البشرية للتغيير الثقافي فيما يتعلق بممارسات الأمن السيبراني بتبك الوحدات والإدارات.

٦- توفير البرامج التدريبية الكافية للموارد البشرية بالجامعات، بما يمكنهم من تطوير ممارساتهم للأمن السيبراني .

٧- توجيه الأهداف الاستراتيجية للجامعات المصرية نحو تحقيق استراتيجية الأمن السيبراني بالجامعات.

٨- تشكيل لجنة متخصصة برئاسة القيادات الجامعية بكل جامعة منوط بها توفير متطلبات تنفيذ وتطوير ممارسات الأمن السيبراني.

٩- مراجعة اللوائح الجامعية وتعديلها بما يتلاءم مع الرؤية المقترحة.

١٠- تحديد مجموعة من المعايير الفنية والإدارية والتقنية القياسية؛ لمعرفة مدى الإنجاز الذي تَحقَّق وسيتحقَّق في تنفيذ الرؤية المقترحة.

١١- التدرج في إنشاء الرؤية المقترحة؛ بحيث يكون هناك تقويم مستمر لتلافي أيّ سلبيات يمكن أن تظهر في التطبيق، وهذا يتطلَّب وجود نظام متميز للتقويم المستمر.

١٢- العمل على إشراك الخبراء المتخصصين بكل جامعة في نشر ثقافة الأمن السيبراني على مواردها البشرية.

١٣- توفير الميزانية المالية الخاصة بتنفيذ الرؤية المقترحة؛ وتخصيص تلك الميزانية للإنفاق على تصميم البرامج التدريبية وتنفيذها ، والتخطيط لتطوير ممارسات الأمن السيبراني، تطوير برامج الأمن السيبراني ، تشكيل لجان الأمن السيبراني .

سابعًا: معوقات تنفيذ الرؤية المقترحة وسبل التغلب عليها:

هناك العديد من المعوقات التي يمكن أن تواجه تنفيذ الرؤية المقترحة ، ويمكن إيضاح تلك المعوقات في نقاط رئيسة، مع بيان كيفية التغلب عليها؛ وتتمثل تلك المعوقات فيما يلي:

١- عدم رغبة بعض القيادات الجامعية في تفعيل أدوارها لتطوير ممارسات الأمن السيبراني بالجامعات؛ على اعتبار أن تلك الممارسات فنية بحته ولا دخل لهم بها. ويمكن التغلب على هذا المعوق بتعريف القيادات الجامعية بالاتجاهات الحديثة في الإدارة الجامعية والتي توسع من أدوار القيادات الجامعية والتي من أبرزها الاشراف على وضع استراتيجية الأمن السيبراني بجامعاتها؛ وذلك كما يحدث بالجامعات الأمريكية على سبيل المثال، إضافة إلى أن رؤية مصر ٢٠٣٠ توسع من صلاحيات القيادات الجامعية ولا تحصرها في مهام نمطية تقليدية وهو ما يتم تسميته بداخل الرؤية" بالقيادة الشاملة " ، كما يمكن التأكيد بأنه ليس المطلوب من القيادات الأكاديمية المعرفة المتخصصة في مجال الأمن السيبراني بل المعرفة العامة بأسس وقواعد الأمن السيبراني وأساليبه .

٢- التخوف من التكلفة المالية المرتفعة والتي قد يتطلبها تطوير ممارسات الأمن السيبراني. ويمكن التغلب على هذا المعوق بالتأكيد على عدم الاحتياج إلى مبالغ مالية مرتفعة لتطوير تلك الممارسات؛ حيث يمكن استثمار المتخصصين في الجامعات بوضع برامج لمواجهة التهديدات السيبرانية، وتنمية مهارات القيادات والموارد البشرية بالجامعة.

٣- معارضة بعض الموارد البشرية بالجامعات لتنفيذ الرؤية وتطوير ممارسات الأمن السيبراني؛ ويمكن التغلب على ذلك المعوق من خلال التأكيد على أهمية الموارد البشرية في العمل الجامعي ودورهم الحيوي في تميز أداء الجامعة وأن من شأن تلك الرؤية والممارسات أن تطور من أداء الجامعة وتقيها من التهديدات الالكترونية السيبرانية ، كما يمكن وضع آليات لتحفيز الموارد البشرية على تنفيذ الرؤية وممارسات الأمن السيبراني إضافة إلى التأكيد بأن تنفيذ الرؤية لن يخل بمراكزهم الوظيفية في الجامعة بل سيعمل على تغيير بعض الممارسات أو المهام المكلفين بها دعماً لتحقيق الرؤية المقترحة .

٤- وضع رؤية وأهداف استراتيجية واضحة تُبيِّن: الأسس التي سيسير عليها الهيكل المقترح، والخطوات الفعلية والإجرائية، وكل جهة منوط بها العمل داخل هذا المقترح.

توصيات الدراسة

توصي الدراسة الحالية؛ بضرورة:

١- التزام القيادات الجامعية بتطبيق الرؤية المقترحة، وحل مايواجهها من مشكلات وتحديات.

٢- التزام القيادات الجامعية بتوفير المتطلبات البشرية والمالية والمادية لتطوير ممارسات الأمن السيبراني بالجامعات.

٣- الاشراف على تقديم برامج تدريبية للقيادات الجامعية خاصة في الصف الثاني (الأكاديمية والإدارية) بهدف فهم التهديدات السيبرانية؛ وكيفية مواجهتها، وأهمية الدقة والسرعة في اتخاذ القرارات تجاه تلك التهديدات.

٤- الاشراف على تصميم وتقديم البرامج التدريبية لأعضاء هيئة التدريس والإداريين بالجامعة لتنمية قدراتهم ومهاراتهم في التعامل مع التهديدات السيبرانية.

٥- الاشراف على تصميم وتقديم برامج تدريبية للطلاب في مجالات الأمن السيبراني

٦- الالتزام بإنشاء مركز /وحدة متخصصه للأمن السيبراني بالجامعات منوط به وقاية الجامعات من خطر التهديدات السيبرانية وتطوير إجراءات الحماية، وتطوير ممارسات الأمن السيبراني . وبحيث يشكل له مجلس إدارة برئاسة رؤساء الجامعات أو أحد نوابهم إضافة إلى عدد من أعضاء هيئة التدريس المتخصصين في مجال الأمن السيبراني .

٧- إصدار قرار بتشكيل فريق من الخبراء في مجال الأمن السيبراني. يسمى فريق التدخل يكون من مهامه التدخل لمواجهة التهديدات السيبرانية التي قد تصيب الجامعات، وإعداد خطط وسيناريوهات المواجهة.

٨- توجيه عمداء بإصدار قرارات بإعداد فرق من المتخصصين في تقنية المعلومات وترتبط بفريق الخبراء لمواجهة التهديدات السيبرانية بكلياتهم .

٩- التوجيه بتحديث جميع برامج الأمن السيبراني لمواجهة كافة التهديدات الالكترونية التي تواجه الجامعات.

١٠- التوجيه بضرورة استخدام استراتيجيات متنوعة في مكافحة الهجمات الإلكترونية السيبرانية .

١١- القيام بزيارات ميدانية للمركز المقترح تأسيسه والفرق العاملة في مجال الأمن السيبراني للاطلاع على ممارساتهم في مواجهة التهديدات السيبرانية.

١٢- تطوير العلاقات بين الجامعات والشركات والمؤسسات المتخصصة الوطنية في مجال الأمن السيبراني؛ وذلك لتبادل الخبرات وتطوير الممارسات لكافة الأطراف .

١٣- الامتثال للبروتوكولات الخاصة بالأمن السيبراني والصادرة من الجهات الرسمية الوطنية.

١٤- إعداد أدلة إرشادية من قبل المتخصصين وتوزيعها على الكليات وعلى الموارد البشرية والطلاب لتطوير ممارساتهم وزيادة وعيهم بالأخطار والتهديدات السيبرانية وكيفية مواجهتها.

المراجع

أولاً المراجع باللغة العربية

١- ابن إبراهيم ، منال (٢٠٢١) الوعي بجوانب الأمن السيبراني في التعليم عن بعد، المجلة العلمية لجامعة الملك فيصل – العلوم الإنسانية والإدارية ، ٢٢(٢) ، ٢٩٩-٣٠٧.

٢- أحمد، أدهم إبراهيم (٢٠٢١) أثر ممارسات القيادة الاستراتيجية على التوجه الريادي: دراسة مقارنة بين كلية تدريب خانيونس وكلية الدراسات المتوسطة بجامعة فلسطين في قطاع غزة، مجلة العلوم الإقتصادية والإدارية والقانونية، المركز القومي للبحوث بغزة، ٥(٧) ، ٣٦-٦٧.

٣- أشرف ، محمد (٢٠١٩) صعوبات استخدام التعليم الإلكترونى فى كلية التربية بجامعة الأقصى من وجهة نظر أعضاء الهيئة التدريسية والطلبة وتصور مقترح لعلاجها، مجلة الدراسات العليا- جامعة النيلين ، ١٣(٥٠) ، ٢٠٣-٢٢٣.

٤- البيشي، منير (٢٠٢١) الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية – الجامعة الإسلامية بغزة، ٢٩(٦) ، ٣٥٣-٣٧٢.

٥- جمال الدين ، جمال (٢٠٢٠) معوقات تطبيق الإدارة الإلكترونية بكليات التربية الرياضية بالجامعات المصرية، المجلة العلمية للتربية البدنية وعلوم الرياضة – جامعة بنها ، ٢٥(٦) ، ١-١٢.

٦- الخضري ، جيهان ، سلامي ،هدى ، كليبي ، نعمة (٢٠٢٠) الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة، مجلة تطوير الأداء الجامعي – جامعة المنصورة ، ١٢(١) ، ٢١٧-٢٣٣.

٧- الروقي ، مطلق (٢٠١٦) مدى تطبيق الإدارة الإلكترونية في كليات جامعة شقراء، مجلة العلوم التربوية- جامعة الأمير سطام بن عبدالعزيز، ١(٢)، ١٢٥-١٦٤.

٨- سراج ، شيماء(٢٠٢٢) التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي، المجلة العربية للعلوم التربوية والنفسية ، المؤسسة العربية للتربية والعلوم والآداب، ع٢٦، ١٩٩-٢١٢.

٩- السمحان ، منى (٢٠٢٠) متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية – جامعة المنصورة، ١١١(١) ، ٢-٢٩.

١٠- شعبان ، رشا (٢٠١٧) وعي طلاب الدراسات العليا بجامعة القاهرة بأبعاد المواطنة الرقمية وسبل تنميتها: بحث ميداني، المجلة التربوية – جامعة سوهاج ، ج٧٩، ١٤٣٧-١٤٨٣.

١١- شعبان ، رشا (٢٠٢١) تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، مجلة جامعة الفيوم للعلوم التربوية والنفسية، ١٥(١١) ، ٣٣٨-٣٨٣.

١٢- العريشي ، جبريل ، والدوسري سلمى (٢٠١٨) دور مؤسسات التعليم العالي في تعزيز ثقافة أمن المعلومات في المجتمع، مجلة مكتبة الملك فهد الوطنية، ٢٤(٢) ، ٣٠٢-٣٧٣.

١٣- علي، خالد (٢٠١٩) معوقات تطبيق الإدارة الإلكترونية في الجامعات المصرية وآليات علاجها: دراسة تطبيقية على جامعة عين شمس، المجلة العلمية للاقتصاد والتجارة – جامعة عين شمس ، ٣، ١٨٥-٢٣٤.

١٤- الغامدي ، سميحة (٢٠١٩) واقع الإدارة الإلكترونية وعلاقته بتطوير العمل الإداري في جامعة الباحة، مجلة البحث العلمي في التربية- جامعة عين شمس، ١٩(١١)، ٣٣٧-٣٨٠.

١٥- فرج، علياء(٢٠٢٢) دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي: جامعة الأمير سطام بن عبدالعزيز نموذجا، المجلة التربوية – جامعة سوهاج ، ج٩٤، ٥٠٩-٥٣٧.

١٦- الفقيه، هند(٢٠١٩) ممارسات القيادة الأخلاقية بالمدارس اليابانية وإمكانية الإفادة منها بالمدارس السعودية، المجلة العربية للعلوم النفسية والتربوية ،ع٩، ١-١٨.

١٧- القحطانى، نورة(٢٠١٩) مدى توافر الوعي بالأمن السيبرانى لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية، مجلة الشؤون الاجتماعية – جمعية الاجتماعيين في الشارقة، ٣٦(١٤٤) ، ٨٥-١٢٠.

١٨- الكردي ، كاظم (٢٠٢١) الأمن السيبراني والتعليم الإلكتروني في جامعات فلسطين من وجهة نظر أعضاء الهيئة التدريسية: جامعة النجاح الوطنية أنموذجاً ، المجلة العربية للمعلوماتية وأمن المعلومات، المؤسسة العربية للتربية والعلوم والآداب، ع٥، ١٠٣-١٢٣.

١٩- مجلس الوزراء ، المجلس الأعلى للأمن السيبراني ، قرار رئيس مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤ متاح على الموقع التالي ، https://www.escc.gov.eg/page1_1.html.

٢٠- نشأت ، إنجي(٢٠٢١) دور تطبيق الإدارة الإلكترونية في التطوير الإداري بجامعة عين شمس، المجلة العلمية للبحوث والدراسات التجارية- جامعة حلوان ، ٣٥(٣) ، ١-٧١.

ثانياً المراجع الأجنبية

1- Abdulrahman, O., & Omar, I. M. (2018). The Impact of Applying Electronic ManagementSystem on the English Language Level: A Case study at Cihan University. InternationalJournal of Research and Engineering, 5(7), 457-464.
2- Ahmed, J., Amir, S., Ahmad, F. (2019). Artificial intelligence and its prospective use in armedforces. Electronic Research Journal of Engineering, Computer and Applied Sciences, 1,100-117.
3- Aljohni ,Wejdan ., Mohamed, Nazar Elfadil., Jarajreh, Mutsam and Gasmelsied , Mwahib (2021) Cybersecurity Awareness Level: The Case of Saudi Arabia University Students, International Journal of Advanced Computer Science and Applications 12(3): 276-281.
4- Al-Jamal, M., & Abu-Shanab, E. (2016). The influence of open government on e-governmentwebsite: the case of Jordan. International Journal of Electronic Governance, 8(2), 159–179.
5- Alkhsabah, M. A. I. (2017). Reality of Use of Electronic Management and its Impact on JobPerformance in Tafila Technical University. International Journal of Academic Researchin Accounting, Finance and Management Sciences, 7(1), 329–341.
6- Al-Ma'aitah, M. (2019). Drivers of E-Government Citizen Satisfaction and Adoption: The Caseof Jordan. International Journal of E-Business Research (IJEBR), 15(4), 40-55.
7- Almarashdeh, I., & Alsmadi, M. K. (2017). How to make them use it? Citizens acceptance of M-government. Applied Computing and Informatics, 13(2), 194–199.
8- Ani, Uchenna P, Daniel Hongmei (Mary) He, and Ashutosh Tiwari. 2017. "Review of Cybersecurity Issues in Industrial Critical

Infrastructure: Manufacturing in Perspective." Journal of Cyber Security Technology 1 (1): 32–74.

9- Alquda ,Mohammad Ali and, Muradkhan, Leyla (2021) Electronic Management and Its Role in Developing thePerformance of E-government in Jordan , Electronic Research Journal of Engineering, Computer and Applied Sciences,3, 65-82.

10- Alqudah, M. A., and Muradkhanli, L. (2021). Artificial Intelligence in Electric Government;Ethical Challenges and Governance in Jordon. Electronic Research Journal of SocialSciences and Humanities, 3(1), 65-74.

11- Boston University(2022) Cybersecurity Best Practices - Protect , Retrieved , https :/ / protectourpower.org/cybersecuritybestpractices/boston-university.

12- Callejas, Jorge Flores ؛ Afifi ,Aicha and Lozinskiy, Nikolay(2021) Cybersecurity in the United Nations system organizations, Report of the Joint Inspection Unit, United Nations , Geneva, Retrieved https://www.unjiu.org/ sites/www.unjiu.org/ files/ jiu_ rep_2021_3_english.pdf.

13- Catota, Frankie E ؛Morgan1 , M. Granger and Douglas C. Sicker(2019) Cybersecurity education in a developing nation: the Ecuadorian environment, Journal of Cybersecurity, 00(0) ,1–19 doi: 10.1093/cybsec/tyz001.

14- Fouad ,Noran Shafik (2021) Securing higher education against cyberthreats: from an institutional risk to a national policy challenge, Journal of Cyber Policy, 6:2, 137-154, DOI: 10.1080/23738871.2021.1973526

15- Garba, Adamu Abdullahi,. Sirat ,Maheyzah Binti ,. Othman, Siti Hajar and Dauda Ibrahim Bukar(2020) Cyber Security Awareness Among University Students: A Case Study, Science Proceedings Series 2(1):82-86

16- Garba, Adamu Maheyzah Binti Sirat Siti Hajar Othman Siti Hajar Othman Ibrahim Bukar Dauda(2020) Cyber Security Awareness Among University Students: A Case Study, International Journal of Advance Science and Technology 29(10):767-776.

17- George Washington University(2022) Cybersecurity | Corporate and Foundation Relations | The George Washington University, Retrived, https://cfr.gwu.edu/rfp / cybersecurity.

18- George Washington University(2022) Cybersecurity News, Retrived https://www .cps. gwu. edu / cybersecurity-news.

19- George Washington University(2022) Cybersecurity @ GW | Cyber Security and Privacy Research Institute (CSPRI) | The George Washington University, Retrived , https:// cspri.seas.gwu.edu/cybersecurity-gw.

20- Hujran, O., Al-Debei, M. M., Chatfield, A., and Migdadi, M. (2015). The imperative ofinfluencing citizen attitude toward e-government adoption and use. Computers in HumanBehavior, 53, 189–203.

21- Louisiana State University(2022) Self-described 'Hacker' and Cybersecurity Expert Joins LSU Faculty, Retrieved , https://www.lsu.edu /news/cybersecurity-expert-joins-lsu.php

22- Muniandy ,Lalitha ؛ Muniandy ,Balakrishnan and Zarina Samsudin(2017) Cyber Security Behaviour among Higher Education Students in Malaysia, Journal of Information Assurance & Cyber security, 2017,1-13, DOI: 10.5171/2017.800299.

23- Naidu , Denan and Zainuddin ,Ahmad (2021) Cyber Security Threat Analysis in Higher Education Institutions during Covid-19 Pandemic,journal of syper security ,11(2),13-21.

24- New Jersey University(2022) Cybersecurity Awareness Month, Retrieved , https:// www.njcu.edu/directories/offices-centers/information-technology/systems-and-services/information-security/cybersecurity-awareness-month.

25- New York University(2022) Professional Pathways: Cybersecurity | NYU School of Global Public Health, Retrieved , https://publichealth . nyu.edu/events-news/ events/ professional-pathways-cybersecurity.

26- New York University(2022) Cybersecurity Awareness Training, Retrieved, https: //www.nyu.edu/life/information-technology/cybersecurity/cybersecurity-awareness-training.html.

27- Pavel ,Nistiriuc؛ Arina ,Alexei and Alexei Anatolie(2021) Empirical Study of Cyber Security Threats in Moldovan Higher Education Institutions, The 12th International Conference on Electronics, Communications and Computing21-22 October, 2021, Chisinau, Republic of Moldova ,1-4.

28- Peker ,Yesem,. Ray, Lydia and Stephanie P da Silva (2018) Online Cybersecurity Awareness Modules for College and High School Students, National Cyber Summit Research Track,24-33.
29- Redman, S. , Yaxley, K. and Joiner, K. (2020) Improving General Undergraduate Cyber Security Education: A Responsibility for All Universities?. *Creative Education*, **11**, 2541-2558.
30- Tibi ,Moanes H.,. Hadeje , Kholod and Watted ,Bashier (2019) Cybercrime Awareness among Students at a Teacher Training College International Journal of Computer Trends and Technology (IJCTT) –67 (6):11-17.
31- University of California,(2022) Cybersecurity: Make It a Habit!, Retrieved ,https:// security .ucop .edu/resources/security-awareness/habits.html.
32- University of California,(2022) Cybersecurity, Retrieved ,https://www. University ofcalifornia.edu/current-issues/cybersecurity.
33- University of Chicago(2022) Information Security, Retrieved , https://security.uchic ago. edu.
34- University of Colorado(2022) Technology, Cybersecurity and Policy, Retrieved, https://www.colorado.edu/engineering/academics/degree-programs/technology-cybersecurity-and-policy.
35- University of Kentucky(2022) Cybersecurity Certificate Program, Retrieved , https://www.engr.uky.edu/students/undergraduate/academic-enhancements/ certificates-and-minors/cybersecurity.
36- university of Maryland(2022) Maryland Cybersecurity Centre, Retrieved, https ://cyber.umd.edu/.
37- University of Massachusetts(2022) Cybersecurity Institute, Retrieved, https://infosec.cs.umass.edu/.
38- University of Missouri(2022) Centres and Signature Programs , cybersecurity centre, Retrieved , https://engineering.missouri.edu/ceri-center/cybersecurity.
39- University of Nevada(2022) Cybersecurity Centre, Retrieved , https:// www. unr.edu/cybersecurity.
40- University of Pennsylvania (2022) office of information security, Retrieved, https://www.isc.upenn.edu/security/overview.
41- University of Texas(2022) cybersecurity concentration, Retrieved, https://www.cs.utexas. edu/ concent rations/cybersecurity.

42- University of Texas(2022) Cybersecurity Curriculum, Retrieved, https:// techbootcamps.utexas.edu/cybersecurity/curriculum.
43- Wilbanks, L.R. Cyber Security Requirements for Institutions of Higher Education [NASFAA Presentation]. (2016, July 10). Retrieved from http: // fsaconferences . ed.gov/conferences/library/ 2016/ NAS FAA/ 2016NASFAACybersecurityReq uirementsforIHEs.pdf.