الأمنُ السيبرانِيُّ ومنظومةُ التعليمِ الدوليةِ

إعداد

الدكتور/ محمد زين العابدين علي حنفي عميرة ١٤٤٤هـ/٢٠٢٣م

(الأستاذ المساعد بجامعتي القاهرة والطائف)

drzaien@yahoo.com

(الكلمات المفتاحية: الأمنُ السيبراني، الهجمات الإلكترونية، التدابير الفعالة، المنظومة التعليمية، المتعلم، المنهج التعليمي، البيئة الدراسية،المُعلِّم، المعايير).

مُقدمةٌ:

يعتمدُ العالَمُ في الوقت الراهن على التكنولوجيا أكثر من أي وقت مضى نتيجة لذلك، تجلت أهميةُ البيانات الرقمية. ومن ثمَّ تقوم الحكومات والمؤسسات اليوم بتخزين كثير من هذه البيانات على أجهزة الكمبيوتر العملاقة ونقلها عبر الشبكات إلى أجهزة الكمبيوتر الفرعية الأخرى. هذه الأجهزة والأنظمة الأساسية لها نقاط ضعف تؤدي عند استغلالها إلى تهديد سُمعةِ المؤسسات المعنية وأهدافها.

وفي ظل هذا التوسع الهائل في استخدام تكنولوجيا الاتصالات ارتفعت الرقابةُ ووسائلُ التجسس على الأفراد وليس على المؤسسات فقط، فأصبحت عملياتُ الرقابة على الاتصالات ووسائل التواصل الاجتماعي واضحةً لا تُصدَّق فمن اختراقات الأفراد (الهاكرز) للأمن الشخصي إلى اختراقات الأجهزة الأمنية، وهذا جعل حياة البشر وخصوصياتهم مخترقة بشكل جلي، وكثرت عمليات الابتزاز والجرائم الالكترونية من خلال ذلك، فلم يعد يَسْلَم فرد من هذه العمليات القذرة، سواء كان مسؤولًا أو مواطنًا.

وقد بدأت كثيرٌ من الدول تدرك أن التغيراتِ المتسارعة في التكنولوجيا تؤدي الى تهديدات ليست بالسهلة ، ولذا لا بد من ضرورة العمل على ضمان أمن المعلومات من خلال خطوات مهمة للأمن السيبراني ، فالأمنُ السيبراني يعتمد على مجموعة كبيرة من وسائل قانونية وتقنية لمقاومة الاستخدام غير القانوني للشبكة العنكبوتية ومن أجل حماية نظم المعلومات ووسائل الاتصالات لحماية المؤسسات من أخطار الفضاء السيبراني.

إن العملَ على بناء جدران الحماية لمنع الهجمات الالكترونية وتقليل تأثير رقابة واختراقات الحسابات وأنظمة المعلومات الحكومية والخاصة مسألةٌ في غاية الأهمية، فلا يمكن حماية المؤسسات والمنظومة التعليمية والمعلومات والبيانات بدون ذلك، وبدون زيادة الثقة بأنظمة المعلومات الدولية، فالفضاءُ السيبراني هو عالم غير مادي ولكن لأن وسائل الاتصالات وخزن المعلومات تستخدمه من خلال شبكات الانترنت والشبكة العنكبوتية في العالم وفي الفضاء، فالمعلوماتُ يتمُّ تخزينُها ولذا من الضروري حمايتها من الاختراق والسرقة والتجسس.

وبالرغم من أن الحكومات الالكترونية أصبحت تسير بتطور جيد في العديد من الدول، فهذا يستدعي اهتمامًا أكبر في عمليات الحماية كونها تُقدِّم الخدمات الالكترونية للمواطن وهو ما يستدعي اداء جيد مشمول بالحماية حفاظًا على أمن المؤسسات الدولية، وهو يحتاج أيضًا الى بناء معايير لتطوير سياسات أمن المعلومات لاسيما منها التعليمية. ولا شك أن تطبيق التدابير الفعالة للأمن السيبراني يمثلُ تحديًا كبيرًا اليوم نظرًا لوجود أجهزة وبرامج كثيرة واعتماد أغلب الشركات والمؤسسات في كافة القطاعات على أجهزة الحاسب الآلي والبرامج وملحقاتها من أجهزة الشبكة وغيرها.(ششمدين/ ٢٠٠٣)

ومن الملاحظ للجميع أنَّ الدول أصبحت ترتب أمورها لمواجهة حروب المستقبل التي تعتمد على التخريب والتدمير من خلال الفضاء السيبراني، وهذا أصبح جزءًا من تكتيك واستراتيجيات الدول المتقدمة، لمواجهة هذه الحروب أو القيام بها، وأصبحت عملياتُ مقاومةِ هذه الحروب جزءًا لا يتجزأ من استراتيجيات الدفاع لدول كثيرة، ومن هنا جاءت أهمية الدراسة.

ومن هذا المنطلق تسعى الدراسةُ الراهنةُ إلى تَعرُّفِ فاعلية معايير الأمن السيبراني في المنظومة التعليمية الدولية وحمايتها من الهجمات والقرصنة الإلكترونية، ومدى انعكاس ذلك على جميع مكونات وعناصر المنظومة التعليمية والمجتمع الإقليمي والدولي المعاصر.

الدراساتُ السابقةُ:

لا توجد دراساتٌ تناولت فاعلية الأمن السيبراني في المنظومة التعليمية الدولية في أي مستوى تعليمي في حدود علم الباحث معتمدًا في ذلك على مراكز مصادر البحث العلمية، وعلى شبكة المعلومات الدولية، ولكن توجد دراساتٌ ذات صلة بموضوع الدراسة الراهنة. يمكن عرضُها فيما يلي للإفادة منها في تأصيل الإطار النظري لهذه الدراسة ودعم مشكلاتها والإجابة عن بعض تساؤلاتها:

١- دراسة (السحيباني ١٩٩٦)، موضوعها: كفاءةُ الإجراءات الإدارية في المحافظة على أمن المعلومات. وقد أكدت على ضرورة توظيف متخصصين في أمن المعلومات، واستخدام الرقم السري لدخول المباني وغرف الحاسب الآلي، وإشعار العاملين بوجود مراقبة مستمرة عليهم،وصيانة أجهزة الحاسب الآلي ، وإجراء تجارب لاختبار طرق الاستجابة عند حدوث طارئ أو كارثة، وضرورة إصدار سياسات لأمن المعلومات.

٢- دراسة (العنزي ٢٠٠٣)، موضوعها: جرائمُ نظمِ المعلومات. وقد كشفت الدراسةُ عن أهمية وسائل الحماية في ضبط الجريمة الإلكترونية وهو ما يتوافق مع الدراسة الراهنة في موضوع حماية شبكات المنظومة التعليمية الدولية من المخاطر حيث أكدت على ضرورة تركيب برامج وأجهزة الحماية وإعدادها الإعداد المناسب والقيام بالتحديث المستمر لتقوم

بصد جميع الهجمات وتسجيلها من خلال تفعيل خصائص تسجيل الأحداث وتسجيلها (Logs).

٣ – دراسة (Emarah,2007)، موضوعها: The Control of Firewalls using Active Networks" ضبط جدران الحماية باستخدام الشبكات النشطة. تتناول مشكلة تغيير إعدادات جدران الحماية المبنية على تصفية حزم البيانات بوضع برامج صغيرة مسبقة التعريف داخل تلك الأجهزة التي تمكِّن من تعديل أو إعادة توجيه حزم البيانات بفتح أو إغلاق المنافذ تبعًا لمحتوى الحزم باستخدام تقنيات الشبكة النشطة (Active Network. ومن توصياته التوجه نحو نموذج عام لبرمجة الشبكة يتمتع بخصائص ذكية أهمها: خاصية التنقل، وخاصية الحماية، وخاصية الفعالية. وتختلف هذه الدراسة عن دراسة (عمارة) بتناولها الأخطار المحتملة على الشبكات وتدابير تجنبها وضمنت جدران الحماية كواحد من أهم تدابير الوقاية.

٤– دراسة (Idris and Shanmugam 2007)، موضوعها: "Hybrid Intelligent Intrusion Detection" نظامُ هجين للكشف الذكي عن التجسس على شبكات الحاسب. وقد تناولت مشكلة عدم كفاية نظام كشف التجسس (IDS) لمنع التجسس على شبكات الحاسب الآلي كونها محدودة الإمكانات وتتركز قدرتها على المراقبة وتحتاج للتحديث اليومي لظهور بُرَيْمجات تجسس يوميًا. وقد أوصت بضرورة استخدام النظام الهجين واستخدام جهاز عالي الأداء من حيث المعالجة. وتتوافق مع الدراسة الراهنة في أهمية جدران الحماية الذكية المعروفة بالاختصار (UTM) وضرورة استخدامها على بوابات شبكات الحاسب الآلي، واختلفت عن الدراسة الراهنة في اقتصارها على جدران الحماية

وعدم تطرقها إلى نواحي الحماية الأخرى التي غطتها الدراسة من منظور الحماية من المخاطر المحتملة.

٥- دراسة (Rehman وآخرون ٢٠١٥)، موضوعها:"واقعُ أنظمةِ إدارة الأمن السيبراني في معاهد التعليم العالي بجامعات باكستان"، وقد أوصت بضرورة وجود إدارة للمخاطر الموجودة، ووضع سياسات أمنية لمعالجتها.

٦- دراسة (البكري ٢٠١٧)، موضوعها: أمن المعلومات بالمكتبات الجامعية السودانية. هدفت التعرف على مخاطر عدم تأمين المعلومات وكيفية تأمينها بالنسبة للمكتبات الجامعية، واستخدمت المنهج التاريخي من خلال الاطلاع على الأدبيات المنشورة وأداة الملاحظة للمكتبات الجامعية بالسودان.

٧- دراسة (Dieta mhono 2017)، موضوعها: زيادة الوعي لدى طلاب جامعة تالين لتكنولوجيا المعلومات في السنة الأولى من غير تخصص تكنولوجيا المعلومات. وقد صَمَّمت برنامجًا لزيادة الوعي لديهم، واستخدمت عينة من ١٧ طالبة حيث حقق البرنامج نجاحًا في زيادة الوعي لدى طلاب جامعة تالين في تكنولوجيا المعلومات.

٨- دراسة (العتيبي ٢٠١٧)، موضوعها: دور الأمن السيبراني في تعزيز الأمن الإنساني. من أهم نتائجها: أن الإجراءات الفنية لحماية الفضاء السيبراني للمؤسسة متوفرة بدرجة كبيرة للنظام آلياً في حالة عدم استخدامه لفترة زمنية محددة. وأن الإجراءات التقنية لحماية الفضاء السيبراني الخاص بالمؤسسة متوفرة بدرجة كبيرة، استخدام القياسات الحيوية (بصمة العين – بصمة الأصبع – بصمة الصوت) لمرور المُصرّح لهم.وأوصت بضرورة اتباع الوسائل العلمية والعملية لحفظ الأمن السيبراني.

٩- دراسة (El Hissi وآخر ٢٠١٨)، موضوعها: اقتراح إطار لحوكمة الأمن

السيبراني في الجامعات الحكومية بالمغرب. وحضدت على استخدام نظام الأمن السيبراني في المؤسسات الأكاديمية الذي يؤدي إلى فوائد عديدة إدارية ومادية وأكاديمية.

١٠- دراسة (الشيتي ٢٠١٩)، موضوعها:"تقييم سياسات أمن وخصوصية المعلومات في مؤسسات التعليم بالمملكة العربية السعودية"، توصلت إلى ضرورة وجود برامج توعية الموظفين وتشجيع البحوث في مجال الأمن السيبراني وأهمية تكامل وصحة البيانات في مؤسسات التعليم.

١١- دراسة (المعهد العربي للتخطيط ٢٠١٩)، موضوعها: مخاطرُ الهجمات الإلكترونية السيبرانية وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي. حاولت تسليط الضو على أهمية المخاطر الإلكترونية وآثارها الاقتصادية وكيفية إدارتها، وأعطت نماذج دولية لحوادث الإصابة بها. وهدفت من ذلك الى زيادة الاهتمام بالاستثمار في الأمن الإلكتروني واستدراك الثغرات في التخطيط الاقتصادي لمواجهة هذه المخاطر.

١٢- دراسة (السمحان ٢٠٢٠)، موضوعها: متطلباتُ تحقيقِ الأمنِ السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. وقد هدفت معرفة متطلبات الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، وقد استفادت الدراسةُ الراهنةُ من أداتها في بناء المعايير الأمنية الواجب توافرها في منظومة التعليم الدولية لدى المؤسسات التعليمية الجامعية في العالم.

وبالنظر إلى الدراسات السابقة نجد تأكيدها أهمية وسائل الحماية في ضبط الجريمة الإلكترونية و ضرورة توظيف متخصصين في أمن المعلومات، واستخدام الرقم السري لدخول المباني وغرف الحاسب الآلي، وإشعار العاملين بوجود مراقبة مستمرة عليهم،وصيانة أجهزة الحاسب الآلي ، وإجراء تجارب لاختبار طرق الاستجابة عند حدوث

طارئ أو كارثة، وضرورة إصدار سياسات لأمن المعلومات. والتوجه نحو نموذج عام لبرمجة الشبكة يتمتع بخصائص ذكية أهمها: خاصية التنقل، وخاصية الحماية، وخاصية الفعالية. وضرورة استخدام النظام الهجين وجهاز عالي الأداء من حيث المعالجة. وضرورة الوعي عند الجميع بمخاطر الأمن السيبراني ومتطلبات تحقيقه في المؤسسات المختلفة لاسيما التعليمية منها لإيجاد مُدخلات وبيئات دراسية مناسبة، وعمليات تعليمية فعالة، ومُخرجات تعليمية سليمة. وتجنب مخاطره السلبية في العالم الذي نجني نتائجه الآن في كل مجالات الحياة، ومواجهته بأساليب الحماية العلمية لتحقيق الأهداف المرجوة. وهو ما يُدَعِّم مشكلة الدراسة الراهنة.

مشكلةُ الدراسةِ:

في السنوات الاخيرة اعتمدت المؤسساتُ التعليميةُ بشكل كبير في تسيير أعمالها على تقنية المعلومات وشكلت شبكات الاتصال وسطًا تنساب فيه البيانات وتسكن فيه خزائن المعلومات وتحتاج هذه الشبكات إلى حماية تصون سلامة محتوياتها وتضمن استمرارية عملها، ونظرًا لكثرة الأخطار التي تهدد سلامة البيانات التي تنساب في الشبكات أو البيانات المحتضنة في خزائنها وتعدد الأخطار التي تهدد استقرار تلك الشبكات وأمنها كالإصابة بالفيروسات والبرامج الضارة ومحاولات الاختراق لأغراض سرقة المعلومات أو التغيير أو التعديل أو الحذف والعبث، تأتي أهمية الحماية على مدار الساعة لمكوِّنات شبكات المعلومات المادية والبرمجية بتثبيت أجهزة وبرامج الحماية في بوابات الشبكات المحلية وداخل تلك الشبكات، وإدارة تلك الأجهزة والبرمجيات من الزاوية الأمنية وسد الثغرات أولًا بأول لتضييق فرص قراصنة المعلومات والمنافسين والأعداء من التمكن من اختراق أو سرقة أية بيانات من شبكات المعلومات.

إن المشكلات الأمنيةَ التي أوجدتها شبكاتُ الحاسب وبخاصة شبكة الانترنت والتي تتلخص بتعطيل وتدمير المواقع الحكومية والتجارية، والتسلل إلى الشبكات وسرقة أسرار الشركات والحكومات والمؤسسات التعليمية ، وترويج برامج التخريب والتجسس والقرصنة، وسرقة المواقع وانتهاك حقوق الملكية الفكرية، بالإضافة إلى أن شبكة الانترنت صارت وسيلة اتصال فعالة للعصابات والمجرمين والمخالفين للقانون والأعراف الاجتماعية والأخلاقية السائدة، وتوفر بيئة خصبة للجرائم المنظمة، وتشكل ميدانًا حديثًا من ميادين الحرب الإلكترونية. كما أنها تُوْجِد تربة مُناسبة لنمو شبكات التجسس العالمية التي تمارس نشاطات جمع المعلومات وانتهاك الخصوصية على مدار الساعة. وقد تجلى ذلك في مكونات وعناصر المنظومة التعليمية الدولية ، فظهر تأثيره واضحًا في محتوى المناهج التعليمية، وبرامج إعداد المُعلمين، والوسائل والأنشطة التعليمية، والبيئات التعليمية، وأساليب التقويم. مما انعكس على العملية التعليمية. وتتحدد مشكلةُ الدراسةِ الراهنةِ في التساؤل البحثي التالي: ما مدى توافر معايير الأمن السيبراني في منظومة التعليم الدولية وحمايتها من الهجمات والقرصنة الإلكترونية، وانعكاس ذلك على جميع مكونات وعناصر المنظومة التعليمية والمجتمع الإقليمي والدولي المعاصر؟ وينبثق عنه التساؤلات البحثية الفرعية التالية:

١- ما مفهومُ الأمنِ السيبراني؟

٢- ما منظومةُ التعليمِ الدولية؟

٣- ما معاييرُ الأمنِ السيبراني الواجب توافرها في منظومة التعليم الدولية؟

٤- ما أنواعُ الأمنِ السيبراني؟

٥- ما فوائدُ الأمن السيبراني؟

٦- ما التحدياتُ التي تواجه الأمن السيبراني؟

٧- ما طريقةُ تطبيقِ الأمن السيبراني؟

٨- ما تدابيرُ الأمن السيبراني؟

٩- ما مدى توافر معايير الأمن السيبراني في منظومة التعليم الدولية لمواجهة الهجمات والقرصنة الإلكترونية وانعكاس ذلك على المجتمع الإقليمي والدولي؟

أهدافُ الدراسةِ:

تهدفُ الدراسةُ الراهنةُ إلى ما يلي:

١-تحديد مفهوم منظومة التعليم الدولية بمكوناتها وعناصرها الأساسية.

٢- تحديد معايير الأمن السيبراني الواجب توافرها في منظومة التعليم الدولية في الجامعات الدولية.

٣- بيان مفهوم الأمنِ السيبراني وأنواعه وفوائده في حماية المنظومة التعليمية الدولية.

٤- بيان التحديات التي تواجه الأمن السيبراني.

٥- بيان طرق تطبيق الأمن السيبراني.

٦- حصر التدابير الاحتياطية اللازمة لتجنب مخاطر القرصنة الإلكترونية التي تتعرض لها المنظومة التعليمية الدولية.

٧- تحديد مدى فاعلية الأمن السيبراني في المنظومة التعليمية الدولية لمواجهة الهجمات والقرصنة الإلكترونية وانعكاس ذلك على المجتمع الإقليمي والدولي.

حدودُ الدراسةِ:

أُطِّرت الدراسة بالحدود التالية:

الحدود الموضوعية: تقتصرُ الدراسةُ على موضوع مدى توافر معايير الامن السيبراني في منظومة التعليم الدولية.

الحدود البشرية: تقتصرُ الدراسةُ على أعضاء هيئة التدريس والمنسوبين في الجامعة.

الحدود الزمنية: الفصل الدراسي الثاني لعام ٢٠٢٢/٢٠٢١م.

الحدود المكانية: تقتصرُ الدراسةُ على عينة عشوائية من أعضاء هيئة التدريس ومنسوبي بعض الجامعات في أفريقيا وآسيا وأوروبا وأمريكا. وهذه الجامعات تمَّ تحديدها على النحو التالي: (جامعة القاهرة/بمصر، وجامعة جين جي/ بتايوان NCCU Taiwan، وجامعة اسطنبول/ بتركيا ISTANBUL UNIVERSITY ، وجامعة هارفارد/بأمريكا HARVARD UNIVERSITY .

منهجُ الدراسةِ:

تستخدم الدراسةُ المنهجَ الوصفي التحليلي في رصد الواقع التعليمي الراهن للوقوف على مدى توافر معايير الأمن السيبراني وفاعليته في منظومة التعليم الدولية.

عينةُ الدراسةِ:

تكونت عينةُ الدراسةِ من (٢٠٠٠) من اعضاء هيئة التدريس والمنسوبين في الجامعات بالقارات الأربع، وتمَّ اختيارهم عشوائيًا وتقسيمهم إلى مجموعات أربع، قوام كل مجموعة (٥٠٠) عضو تدريسي ومنسوب.

أداةُ الدراسةِ:

تستخدم الدراسةُ الاستبانةَ كأداةٍ لقياس مدى توافر معايير الأمن السيبراني في منظومة التعليم الدولية وفاعليته في تحقيق أهداف الدراسة. وقد بلغت المعايير (٧٠) سبعين معيارًا محددة على النحو التالي:

١- المعايير الإدارية(٢٠) عشرون معيارًا.

٢- المعايير المادية (١٠) عشرة معايير.

٣- المعايير البشرية (١٠) عشرة معايير.

٤- المعايير التقنية (٣٠) ثلاثون معيارًا.

أهميَّةُ الدراسةِ:

تبدو أهميَّةُ الدراسة الحالية في النقاط التالية:

١- تُعدُّ الدراسةُ من المبادرات الأولى في تعرُّف دور الأمن السيبراني في المنظومة التعليمية الدولية.

٢- إعداد استبانة مضمنة معايير الأمن السيبراني، وذلك للوقوف على مدى توافر المعايير الأمنية في المؤسسات الجامعية ودورها في تفعيل الأمن السيبراني في منظومة التعليم الدولية.

٣- توضيح المخاطر الإلكترونية التي تواجه منظومة التعليم الدولية وانعكاس ذلك على جميع مكوناتها وعناصرها الأساسية.

٤- عرض الحلول المُناسِبة لمواجهة المخاطر الإلكترونية.

٥- تُعدُّ مصدرًا مُهمًا للعاملين بمجال الامن السيبراني في تعرُّف دور المؤسسات التعليمية في مواجهة المخاطر السيبرانية التي تتطلب منظومة تعليمية دولية سليمة وبيئات تعليمية وحماية إلكترونية مناسبة ، والتي تستتبع بالتالي تحديد مسؤولية القائمين بها، وتحديد السلوك الواجب اتباعه لتحقيق أهدافها.

مُصطلحاتُ الدراسةِ

الأمنُ السيبراني Cyber Security :

لُغةً: مُكَوَّن من لفظتين: (الأمن)، و (السيبراني). الأمن: هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أَمِنَ أَمْنًا أَمَانًا وأَمَنَةً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويُقال: أَمِنَ من الشر، أي سَلِمَ منه.(آبادي/٢٠٠٥)

السيبراني: كلمة (Cyber) لفظة يونانية الأصل مشتقة من كلمة (kybernetes) بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازًا للمتحكم. (governor) وأشار بعض المؤرخين إلى أن أصلها يرجع إلى عالم الرياضيات الأمريكي (Norbert Wieners 1894 – 1964) وذلك للتعبير عن التحكم الآلي.

اصطلاحًا: يُعرَّف بأنه حماية الأنظمة والشبكات والبرامج والموقع الجغرافي من أية مشكلة أو عائق أو هجمات إلكترونية يحول دون أداء عملها بشكل فعال ومثمر. وتهدف الهجمات الإلكترونية عادةً إلى الوصول إلى المعلومات الحساسة بهدف تغييرها أو إتلافها أو ابتزاز الأموال من المستخدمين أو مقاطعة عملها بشكل مؤثر على فعالية المؤسسات المعنية المختلفة لاسيما التعليمية منها.

وقد عَرَّفَتْهُ وزارة الدفاع الأمريكية بأنَّه: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث.". في حين أعتبر الإعلان الأوروبي أنَّه: "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات."(السمحان/٢٠٢٠)

ويمكن تعريفه إجرائيًا بأنه: أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها.(العنزي/ ٢٠٠٣)

وهناك العديد من المفاهيم المرتبطة بالأمن السيبراني، من أهمها☹السمحان/٢٠٢٠)

الفضاء السيبراني: عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI بأنه: "فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية". فهو بيئة تفاعلية حديثه، تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين.

الردع السيبراني: يعرف بأنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية".

الهجمات السيبرانية: تُعرَّف بأنها: "فعلًا يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام".

الجريمة السيبرانية: "مجموعة الأفعال والأعمال غير القانونية التي تتم غعبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها:.(الموسوعة السياسية https://political-encylopedia.org/dictionary/)

وإجمالًا يمكن القول: إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر (الفضاء السيبراني بصفة عامة) من مختلف الهجمات والاختراقات والتهديدات السيبرانية التي قد تُهدد المنظومة التعليمية الدولية.

ويُمكنُ الإجابة عن تساؤلات الدراسة على النحو التالي:

أولًا– منظومةُ التعليمِ:

تتكونُ منظومةُ التعليم من خمسة عناصر ومكونات أساسية ، وهي:

١- *المُدخلات: Inputs*

وتشملُ جميعَ العناصر والمكونات الداخلة في نظام التعليم سواء كانت بشرية ، أو مادية ، أو معنوية ، كأهداف نظام التعليم وبيئة النظام التعليمي ، والمُتعلم بكافة خصائصه وسماته ، والمُعلم بكافة قدراته وإمكاناته ، والمنهج بأهدافه ومحتواه وأيدولوجياته ، وأساليب تدريسه ووسائله التعليمية وتقنياته ، وأنشطته الصفية وغير الصفية ، وأساليب التقويم ، وكذلك الأفراد المعاونين والفنيين في العملية التعليمية.

٢- *العمليات: Processes*

وتشملُ جميعَ الأساليب ، والتفاعلات ، والعلاقات والأنشطة التي تهدف إلى تحويل مُدخلات منظومة التعليم بصورتها الأولى إلى مُخرجات تتناسب وأهداف تلك المنظومة ، وخلال هذه المرحلة يتم القيام بالواجبات والإجراءات التي يتحقق من خلالها وصول النظام إلى أهدافه. ويتوقف نجاح النظام التعليمي على كفاءة عملياته وقدرة هذه العمليات على الاستفادة من مُدخلات النظام بالقدر المناسب ، ومن ثَمَّ إخراج النتائج والمُخرجات المرغوبة لهذا النظام.

وتدخلُ طرقُ وأساليبُ واستراتيجياتُ التعليم والتعلم ، والإدارةُ التعليمية والمدرسية ، وعملياتُ التقويم والحماية الإلكترونية في نطاق عمليات النظام التعليمي.

٣- *المُخرجات: Outputs*

وتشملُ الإنجازات والنتائج النهائية التي يُحققُها النظام التعليمي متمثلة في الأهداف التي تحققت لهذا النظام ، ومدى انعكاس تلك الأهداف على نمو المتعلم عقليًا ، ومهاريًا ، ووجدانيًا ، وأَيْدُولُوجِيًا.

والمُخرجاتُ هي الناتج الفعلي لعمليات أية منظومة تعليمية ، حيثُ تتحدد تلك المُخرجات على ضوء أهداف النظام ووظائفه ، وتتوقف جودةُ المُخرجات على: نوعية المُدخلات ، ومستوى دقة العمليات الخاضعة لمعايير علمية وموضوعية سليمة وصحيحة. وتتركزُ مُخرجاتُ النظم التعليمية عمومًا في المُخرجات البشرية متمثلة في الأفراد خريجي المنظومة.

٤- التغذية الراجعة: Feed Back

وتشملُ المعلوماتِ والبيانات المتعلقة بعناصر النظام التعليمي عمومًا والتي يتمُّ من خلالها إجراء أية تعديلات أو توافقات ، أو تطويرات في هذا النظام، وغالبًا ما يتمُّ الحصول على هذه المعلومات والبيانات من خلال وصف مُخرجات النظام وتحليلها في ضوء معايير علمية وموضوعية سليمة وصحيحة مستقاة من أهداف النظام. بعبارة أخرى فإن التقويم في أي نظام تعليمي هو الذي يعطي المؤشرات على مدى تحقق أهداف هذا النظام وإنجازها ، وهو الذي يبين الإيجابيات والسلبيات في أي جزء من أجزاء النظام تمهيدًا لاتخاذ القرارات والإجراءات المُناسِبة للتغلب على السلبيات. والتغذيةُ الراجعةُ في أي نظام تعليمي تشملُ:

(أ) تقويمُ مُدخلاتِ النظام:

وهو يهدف إلى جمع معلومات عن جميع أنواع المُدخلات الداخلة للنظام التعليمي ، وتحليلها للعمل على انتقاء أفضل المُدخلات وتحسين نوعيتها.

(ب) تقويمُ عملياتِ النظام:

ويهدفُ إلى مراقبة عمليات النظام التعليمي ، وتحديد مدى تفاعل وترابط وتكامل واستمرار العمليات ، وتحديد الصعوبات التي قد تواجه سير العمليات وتفاعلها.

(ج) تقويمُ مُخرجاتِ النظام:

ويهدفُ إلى تحديد التغيرات التي حدثت في مُخرجات النظام التعليمي الفعلية ، وذلك من خلال نموذج مُخرجات معياري مشتق من أهداف النظام الذي يحدد إلى أي مدى تحققت الأهداف؟ وبأي مستوى؟ ، ومدى التعديلات المرغوبة التي أحدثها النظام في سلوك المُتعلم وانعكاس ذلك على البيئة الحياتية والمجتمع الإقليمي والدولي.

٥- *بيئةُ النظامِ: System environment*

وتشملُ الوسطَ المحيط بأي نظام تعليمي من: أبنية تعليمية وأثاث وتجهيزات تعليمية إلكترونية وغير إلكترونية. كما تشمل الظروف الاجتماعية والاقتصادية ، والسياسية ، والثقافية ، والمادية المحيطة بالنظام. وكذلك ظروف الطقس ، والمُناخ ، والإضاءة المحيطة بموقع المؤسسات التعليمية ... وغير ذلك من العوامل.

ويرى البعضُ أن منظومة التعليم تتكون فقط من المكونات الثلاثة الأولى (المُدخلات ، والعمليات ، والمُخرجات). أما التغذية الراجعة وبيئة النظام فهما عاملان مؤثران على المنظومة أكثر من كونهما عناصر أو مكونات للمنظومة.

وأخيرًا يُمكنُ القول: إنَّ المنظومةَ مجموعةٌ من المكونات والعناصر المترابطة والمتفاعلة التي تعمل مشتركة معًا من أجل تحقيق أهداف محددة وغايات مشتركة. ثُمَّ يتمُّ مُعالجتُها لإنتاج مُخرجات معينة ومحددة للبيئة. أي أن النظام مجموعة من المكونات المترابطة في كلٍ واحد ، بينها علاقات تفاعلية منظمة وعلاقات تبادلية مع النظم الأخرى لغرض بلوغ هدف أو مجموعة أهداف محددة.(صبري/ ٢٠١٠ ، والعبيدي/ ٢٠١٨ ، وشاكر/٢٠٢٠)

وجديرٌ بالذكر في هذا الصدد أنَّ أيةَ منظومةٍ بشريةٍ قد بُنِيت على منوال منظومة الكون الذي خلقه الله فأبدع في خلقه ، وشتان بين منظومة الكون والمنظومات البشرية أيًا كانت

، فالأولى مُحْكَمَةُ البنيان كاملة لا يعتريها النقص ولا تتعرض للقرصنة والاختراق والتجسس ولا تحتاج إلى التعديل أو التغيير أو التطوير. أما المنظومات البشرية فيعتريها النقص والقرصنة والاختراق والتجسس والسرقة وعدم الكمال وتحتاج من وقت لآخر إلى التعديل والتغيير والتطوير والحماية إذا حادت عن منهجِ الله وشرائعِه الذي أعدَّه لصلاح البشرية جمعاء ، فخالق البشر هو أدرى بما يُصْلِحُهم ويُقَوِّمهم لتنجحَ منظوماتهم التي قَنَّنُوهَا لحياتهم الأرضية. فيقول الله تعالى:"يا معشرَ الجنِّ والإنسِ إنْ استطعتمْ أَنْ تَنْفُذُوا مِنْ أَقْطَارِ السمواتِ والأرضِ فَانْفُذُوا لا تَنْفُذُونَ إِلَّا بِسُلْطَانٍ، فَبِأَيِ آلاء رَبِّكُمَا تُكَذِّبَانِ، يُرْسَلُ عليكما شُواظٌ مِنْ نارٍ ونُحَاسٌ فلا تَنْتَصِرَانِ فَبِأَيِ آلَاءِ رَبُّكُما تُكذِّبانِ"(الرحمن، الآيات: ٣٣ – ٣٦)

ثانيًا– قائمةُ معايير الأمنِ السيبراني الواجب توافرها في منظومة التعليم الدولية

أولًا– المعاييرُ الإداريةُ للأمن السيبراني الواجب توافرها في منظومة التعليم الدولية:

١– توجد إدارة خاصة بالأمن السيبراني للمنظومة التعليمية في الجامعة.

٢– توجد سياسات أمنية لأنظمة المعلومات الإدارية بالجامعة.

٣– تطبيق الإجراءات الإدارية اللازمة للأمن السيبراني داخل أنظمة المعلومات بالجامعة.

٤– تُوجِد الإدارةُ خطةً أمنيةً فعالةً لمواجهة المخاطر التي تتعرض لها أنظمة معلومات العملية التعليمية في الجامعة.

٥– يتم تقييم مخاطر الأمن السيبراني من قِبل إدارة أنظمة المعلومات بشكل دوري.

٦– تلتزم الوحداتُ الإداريةُ في الجامعة بالخطة التنظيمية للأمن السيبراني.

٧– تطبق إدارة الجامعة الأصول المعلوماتية والتقنية للأمن السيبراني.

٨– تعملُ إدارةُ الأمن السيبراني على حماية البريد الإلكتروني.

٩- تطبقُ إدارة الجامعة أمن الشبكات، والتطبيقات، وإنترنت الأشياء، والأمن السحابي، والتشغيلي لمواجهة أية هجمات سيبرانية من الداخل أو الخارج.

١٠- تُفَعِّلُ إدارةُ الجامعة الأمن السيبراني في حماية الأجهزة المكتبية والمحمولة الشخصية لأعضاء هيئة التدريس والمعاونين.

١١- تطبق إدارةُ الجامعة الأمنَ السيبراني لحماية بيانات ومعلومات الجامعة والمنظومة التعليمية.

١٢- تشفرُ الجامعة أنظمة المعلومات الإدارية.

١٣- تحتفظُ الجامعةُ بنسخ احتياطية للبيانات والمعلومات الإدارية.

١٤- تحتفظُ الجامعةُ بنسخٍ احتياطية للبيانات والمعلومات والمعارف المضمنة بالمنظومة التعليمية.

١٥- تُفَعِّلُ إدارةُ الجامعة المثلَّث الأمني السيبراني من حيث سرية وسلامة وتوافر المعلومات.

١٦- تعملُ إدارةُ الجامعة على تعليم المستخدم مجموعةً من الآليات والمبادئ التي ينبغي على كل شخص معرفتها والعلم بها ليتعامل بها مع الكمبيوتر.

١٧- تقوم إدارةُ الجامعةِ بحماية الموقع الالكتروني من التوقف وحجب برامج التجسس لضمان فاعلية منظومة التعليم الدولية.

١٨- تعملُ إدارةُ الجامعة على توحيد بيئةِ العمل لضمان فاعلية منظومة التعليم الدولية.

١٩- تعمل إدارةُ الجامعة على توعية أعضاء هيئة التدريس والمعاونين بمخاطر هجمات برامج الفدية، والهجمات السحابية، والتصيد الاحتيالي، والذكاءِ الاصطناعي، وهجمات إنترنت الأشياء.

٢٠- تُحددُ إدارةُ الجامعة القضايا الخارجية والداخلية لبيئة المنشأة التعليمية والتي تؤثر على قدرتها في تحقيق النتائج المرجوة.

ثانيًا- المعاييرُ الماديةُ للأمنِ السيبراني الواجب توافرها في منظومة التعليم الدولية:

١- تمتلكُ الجامعةُ نظامَ حمايةٍ عالٍ للأمن السيبراني.

٢- توفر الجامعةُ الجوانب المادية اللازمة لتحقيق الأمن السيبراني في منظومة التعليم الدولية.

٣- توفر الجامعةُ نظامَ حماية عالٍ لأنظمة المعلومات الإدارية.

٤- تزود الجامعةُ منسوبيها بأجهزة حديثة ومتطورة لإدارة أنظمةِ المعلومات بها.

٥- توفر الجامعةُ الصيانةَ الدورية والمستمرة لأجهزة تقنيةِ المعلومات لتحقيق الأمن السيبراني في منظومة التعليم الدولية لضمان فاعليتها.

٦- تُحدِّثُ الجامعةُ برامجَ التطبيقات الحاسوبية لمنسوبيها باستمرار.

٧- توفر الجامعةُ الدعمَ التقني اللازم لمنسوبيها لمعالجة المشكلات الطارئة.

٨- تمتلكُ الجامعةُ برامجَ حديثة لتوفير الحماية والأمن السيبراني لأنظمة المعلومات الإدارية.

٩- تمتلك الجامعةُ نظامَ حَوكمةٍ تقني لتوفير الأمن السيبراني للتعاملات الإلكترونية.

١٠- تمتلك الجامعةُ بظامَ شبكي آمن لتبادل المعلومات والمعارف في منظومة التعليم الدولية.

ثالثًا- المعاييرُ البشريةُ للأمنِ السيبراني الواجب توافرها في منظومة التعليمِ الدولية:

١- تقوم الجامعةُ بتوعية الموظفين والإداريين والأكاديميين بأهمية تطبيق الأمن السيبراني في المنظومة التعليمية الدولية.

٢- تدرب الجامعة الموظفين والإداريين والأكاديميين على تفعيل الأمن السيبراني.

٣- تؤهل الجامعةُ الموارِدَ البشريةَ القائمة على تقنيات المعلومات في مجال تطبيق الأمن السيبراني.

٤- توفر الجامعةُ الدعمَ الفني لمنسوبيها لتطبيق الأمن السيبراني في المنظومة التعليمية الدولية.

٥- تقيم الجامعة لقاءات دورية للمختصين بتطبيق الأمن السيبراني لتعريفهم بالمستجدات في المجال.

٦- تمَّ توقيعك على بند (المحافظة على سرية المعلومات) قبل البدء في العمل بالجامعة.

٧ - يتلقى الموظف قبل البدء في عمله توضيحًا بالمهام والمسؤوليات ذات العلاقة بأمن أنظمة المعلومات الإدارية.

٨- يتمُّ تذكير الموظف أثناء عمله ومن وقت لآخر بالمهام والمسؤوليات مع تبليغه بكل جديد.

٩- توجد إجراءات واضحة لإدارة الأصول المعلوماتية التي بعهدة الموظف.

١٠- يوجد تنسيق وتناغم وتعاون بين جميع متُخصصي أنظمة المعلومات والمعارف الإلكترونية في الجامعة.

رابعًا- المعاييرُ التقنيةُ للأمن السيبراني الواجب توافرها في منظومة التعليم الدولية:

١- توجد بالجامعة أنظمة حماية أمنية للأجهزة التقنية والحاسوبية كنظام هجين.

٢- تُحدَّث أنظمة وبرامج الحاسب الآلي بالجامعة بشكل دوري.

٣- تُحدَّث برامج الحماية لأجهزة الحاسب الآلي بالجامعة.

٤- توجد أنظمةُ حماية للمعلومات السرية للمستخدم في الجامعة.

٥- تطبق إدارةُ الجامعة ضوابط الأمن السيبراني لهويات الدخول والصلاحيات للمصرح لهم من خلال بصمة الصوت والعين والأصبع.

٦- تطبق إدارةُ الجامعة معايير موضوعية وعلمية لحماية أنظمة المعلومات ومعالجتها لدى المستخدمين.

٧- توفر الجامعة برامج حماية ضد الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة لأنظمة المعلومات الإدارية على أجهزة الجامعة.

٨- تطبق إدارةُ الجامعة الأمن السيبراني لحماية البريد الإلكتروني.

٩- تطبع الوثائق السرية على طابعة عامة في جهة العمل.

١٠- تنقلُ معلومات خاصة بالعمل للمنزل وتستخدم جهاز الكمبيوتر الخاص بك في المنزل للعمل عليه.

١١- عند القيام بحذف ملف من جهاز الكمبيوتر هل يمكن استرداد هذه المعلومات؟.

١٢- تقوم بتسجيل الدخول إلى حساب العمل باستخدام الكمبيوتر في أماكم عامة مثل المكتبة، مقهى إنترنت أو لوبي فندق.

١٣- تستخدم نفس كلمة المرور لحسابات العمل في حساباتك الشخصية في الفيس بوك، وتويتر، والبريد الإلكتروني الشخصي.

١٤- سبق وإن طلب منك رئيسك بالعمل أو أي شخص آخر في عملك كلمة المرور الخاصة بك هل تعطيه إياها؟.

١٥- درجةُ الأمان التي تشعر بها لجهازك.

١٦- تعرف هجوم التصيد الإلكتروني وتحدده.

١٧- تعرف هجوم إنترنت الأشياء وتحدده.

١٨- تعرف مخاطر هجمات برامج الفدية وكيفية التعامل معها.

١٩- تعرف مخاطر هجوم الذكاء الاصطناعي على المنظومة التعليمية.

٢٠- تعرف كيفية الاحتيال عبر البريد الإلكتروني.

٢١- تعرف استخدام جدران الحماية النارية والخوادم الوكيلة.

٢٢- - تسمح بالرسائل الفورية (الدردشة) عبر أجهزة وشبكات الجامعة.

٢٣- سبق وأن أعطيتَ كلمة المرور الخاصة بك شخصًا آخر.

٢٤- تسمح بتنزيل البرامج وتثبيتها على جهاز الكمبيوتر الخاص بك في العمل.

٢٥- يمكن استخدام أجهزتك الشخصية مثل هاتفك المحمول لتخزين أو نقل معلومات سرية خاصة بالجامعة.

٢٦- جهازُ الكمبيوتر الخاص بك له قيمة لدى المخترقين حتى يستهدف.

٢٧- درجة الحذر عند فتح مرفق في البريد الإلكتروني.

٢٨- التحديثُ تلقائيًا في جهاز الكمبيوتر الخاص بك.

٢٩- عند تهيئة كورص صلب أو محو ملفات داخل الكورص الصلب هل المعلومات المحفوظة وبشكل دائم تُفْقَدُ؟.

٣٠- تعرف بمن تتصل في حالة حدوث اختراق أو اعتداء لجهازك؟.

ثالثًا- أنواع الأمن السيبراني: (الروسان/٢٠٢١، دحام/٢٠٢١)

الأمنُ السيبراني Cyber security: هو عبارة عن مجموعةٍ من العمليات اللازمة لاتخاذ تدابير أمنية مختلفة؛ وذلك من أجل حماية الشبكات والبيانات الشخصية التي تُنشر على الإنترنت من أية تهديدات إلكترونية، وفيما يلي يُمكن عرض أبرز أنواعه:

١- *أمن الشبكات Network Security:* يوفر حمايةً لشبكات الحاسوب بأنواعها المتعددة من أية هجمات، سواء أكانت داخلية أو خارجية بالنسبة للشبكة، وذلك من خلال استخدام أحدث التقنيات المختلفة لمنع البرامج الخطرة أو سرقة أية من البيانات الأخرى. وهو يُستخدم في عدة بروتوكولات مختلفة؛ وذلك لمنع الهجمات الإلكترونية، حيث يسمح فقط للمستخدم المصرح له بالوصول إلى الشبكة الآمنة.

٢- *أمن التطبيقات Application security*: والذي يسعى إلى إفشال أي نوع من الهجمات على الأمن السيبراني، وذلك بواسطة استخدام العديد من الأجهزة والبرامج، خلال مرحلة تطوير المشروع الإلكتروني. ومن خلال هذا النوع تستطيع الشركات أو المؤسسات اكتشاف مجموعةَ البيانات الحساسة، والتي يجب حمايتها بشكلٍ كبير، ويوجد عدة طرق مرتبطة بأمن التطبيقات، وهي: برنامج مضاد للفيروسات، جدران الحماية، عملية التشفير والتي يتم القيام بها من خلال برامج خاصة.

٣- *الأمنُ السحابي Cloud Security:* حيث تميل معظم المؤسسات في الوقت الراهن نحو استخدام الذكاء الاصطناعي وذلك لِتُحَسِن من عملها، بالإضافة إلى تعزيز تجربة العملاء، وفعالية إنجاز العمليات. إنَّ كميةَ البيانات الهائلة في المؤسسات يزيد من صعوبة الاحتفاظ بها بصورة مادية، ومن الممكن أن تكون هذه البيانات غير منظمة، أو أنها من مصادر غير معروفة، ولذلك تقدم مجموعة من الشركات خدمات لحل هذه المشكلة ومنها: خدمات أمازون ويب Amazon Web Services، خدمات مايكروسوفت أزور Microsoft Azure، خدمات جوجل كلاود Google Cloud. حيث تُقدم كل منها لعملائها نظامًا مُخصصًا للحوسبة السحابية، تُمَكن المستخدمين من تخزين البيانات ومراقبتها وذلك باستخدام تطبيق الأمن السحابي Cloud Security.

٤- *أمنُ إنترنت الأشياء Internet of Things security:* عبارة عن ثورة تكنولوجية قائمة بذاتها، وذلك وفقًا لتقرير صادر عن شركة (Bain and Company) .وقد ذكر التقرير أن حجم السوق الخاص بأمن إنترنت الأشياء سوف يتوسع بمقدار ٥٢٠ مليار دولار أمريكي خلال العام ٢٠٢١، ومن خلال شبكة الأمان الخاصة بها سيقوم أمن إنترنت الأشياء بتوفير أجهزة مهمة للمستخدم كأجهزة الاستشعار، والطابعات، وأجهزة توجيه (wifi)٢ [وبواسطة القيام بدمج النظام مع أمن إنترنت الأشياء، سيتم تزويد المؤسسات].بتحليلات واسعة وأنظمة مُختلفة، وبذلك يتم الحد من مشكلة تهديد الأمن.

٥- *الأمنُ التشغيلي Operational Security*: وهو يهدف إلى إدارة المخاطر لجميع مجالات الأمن السيبراني الداخلي، وغالبًا ما يقوم باستخدام هذا النوع مجموعةٌ من مسؤولي إدارة المخاطر وذلك لضمان وجود خطة بديلة إذا ما تعرضت بيانات المستخدمين لأي هجوم كان. أيضًا يضم الأمن التشغيلي بيانًا يشتمل على توضيح كيفية توعية الموظفين بأفضل الأعمال التي يجب القيام بها من أجل حماية أمان المعلومات الشخصية والتجارية.

٦- *التعافيُ من الكوارث واستمرارية الأعمال Disaster recovery and business continuity:* وهو يشير إلى الكيفية التي تتم فيها استجابة المؤسسة لأي حادث اختراق تتسبب بفقدان بعض البيانات، أو العمليات المخزنة. وتتجسد هذه العملية من خلال استعادة المؤسسة لقدرتها التشغيلية بالكيفية التي كانت عليها قبل حادثة الاختراق لضمان استمرارية العمل بأعلى قدرة وكفاءة.

٧- *تعليمُ المستخدم النهائي End-user education:* وهو يُشكِّلُ مجموعةً من الآليات والمبادئ التي ينبغي على كل شخص يتعامل مع الكمبيوتر معرفتها والعلم بها، ثُمَّ ممارستها لضمان عدم إدخال أي نوع من أنواع الفيروسات إلى الجهاز الذي يعمل عليه بطريق الخطأ، وبالتالي تهديد أمن النظام بالكامل.

رابعًا- فوائد الأمن السيبراني: (الروسان/٢٠٢١، وأبو شوالي)

يعتقد البعض أن الأمن السيبراني يتمثل ويحل فقط بإنزال بعض البرامج أو تركيب جهاز (مثل الجدر النارية أو برامج الحماية من الفيروسات) للحماية من التهديدات الأمنية، وينسى أن انقطاع التيار الكهربائي أو عدم اخذ نسخ احتياطية أو عدم الاهتمام بالأمن الفيزيائي يُعتبر تهديد أمنى، فما هي الفائدة للشركات إذا تم تطبيق الأمن السيبراني بشكل فعال؟، دعونا نعرج على بعض هذه الفوائد:

١- حماية بيئة العمل :أكبرُ ميزة لتطبيق أمن المعلومات في الشركات هي أن توفر حمايةً رقمية شاملة لعملك. سيسمح هذا للموظفين بالعمل والتأكد من أنهم ليسوا في خطر من التهديدات المحتملة، مما يؤثر إيجابيًا على سير العمل وجَنْي النتائج المرجوة.

٢- حماية المعلومات الشخصية أو المالية أو المعلومات المهمة :وهي قيمةٌ جدًا في العصر الرقمي. إذا كان الفيروس أو المخترق أو الموظف الداخلي قادرًا على الحصول على معلومات شخصية أو مالية أو معلومات مهمة تتعلق بموظفيك أو عملائك، فيمكنهم بيع هذه المعلومات أو استخدامها لسرقة أموالهم مما يضر الشركة وسمعتها وقد يتوقف عملها بسبب ذلك.

٣- العمل بأمان للموظفين :بدون حلول الأمن السيبراني، قد تكون أنت وموظفك معرضين دائمًا للخطر من أي هجوم الكتروني محتمل من الداخل والخارج. إذا أصيبت الأنظمة أو

الخوادم أو الشبكة، أو حتى أجهزة الكمبيوتر الشخصية يمكن أن يعيق إنتاجيتها ويجبرك على استبدال أجهزة الكمبيوتر أو يمكن أن تفقد المعلومات المهمة الموجودة عليها مما يؤثر على سير العمل أو انقطاعه.

٤- حمايةُ الإنتاجية :يمكن للفيروسات أو الهجمات الإلكترونية أو المشاكل في الكهرباء إبطاء أجهزة الشبكة أو الخوادم أو الكمبيوترات الشخصية، وجعل العمل عليها مستحيلًا من الناحية العملية. يمكن أن يسبب هذا الكثير من الوقت الضائع لموظفيك، وغالبًا ما يؤدي إلى توقف أعمالك بالكامل.

٥- حمايةُ الموقع الالكتروني من التوقف :أغلبُ الشركات لديها موقع إلكتروني حيث أصبح ضرورة ملحة الآن وجود موقع إلكتروني يساعد في العمل سواء تجاريًا أو ترويجيًا أو خدميًا، من المحتمل أن تستضيف موقع الويب الخاص بك داخل شركتك. إذا أصيبت الأنظمة الداخلية باي خلل أو فيروس أو قرصنة أو أية مشكلة اخرى فهناك احتمال كبير أن يتم تعطيل الموقع الإلكتروني الخاص بك. هذا يعني ليس خسارة الأموال فحسب، بل خسارة ثقة العملاء أيضًا ويمكن أن تتسبب بعض الفيروسات أو القرصنة أو المشاكل الأخرى في أضرار دائمة للنظام.

٦- حجبُ برامج التجسس :برامج التجسس هي شكل من أشكال التهديدات الأمنية المصممة للتجسس على أجهزة الكمبيوتر، ويمكن أن تقوم هذه البرامج بنقل المعلومات إلى مجرمي الإنترنت. في حال تطبيق الأمن السيبراني مثل الجدر النارية أو أنظمة منع الاختراق intrusion prevention system (IPS) أن يمنع برامج التجسس أو الإختراقات الأمنية من الحدوث ويضمن استمرارية العمل بشكل أفضل.

٧- منعُ البرامجِ الإعلانية :Adware البرامج الإعلانية أو كما تسمى Adware هو شكل من أشكال فيروسات الكمبيوتر التي تملأ جهاز الكمبيوتر بالإعلانات وهو شائع إلى حد ما ومع ذلك يمكن أن يكون لهذه الإعلانات تأثير حقيقي على الإنتاجية ويمكن أن تسمح للفيروسات الأخرى أو الإختراقات الأمنية بالدخول إلى أجهزة الكمبيوتر بمجرد النقر على الإعلان عن طريق الخطأ أو بشكل متعمد.

٨- توحيدُ بيئة العمل :تطبيق الأمن السيبراني وتوصياته يوفر للشركات حلًا شاملًا للحماية من مجموعة متنوعة من المشكلات والتهديدات الأمنية. يجب أن تتضمن حلول الأمن السيبراني وجود جُدر حماية (firewall) وبرامج مكافحة الفيروسات والبريد العشوائي والأمن اللاسلكي وترشيح المحتوى عبر الإنترنت ووجود أجهزة للحماية من انقطاع التيار الكهربائي وتحديد أماكن عمل آمنة وفصلها عن بعضها البعض وغيره من التوصيات.

٩- دعمُ موظفي تكنولوجيا المعلومات :معظمُ مخترقي الإنترنت ومبرمجي الفيروسات قد يتمتعون بخبرة أكثر بكثير من الموظف العادي عندما يتعلق الأمر بالجريمة الرقمية. يمكن من خلال تطبيق الأمن السيبراني تزويد فريقك بالمزايا والدعم الذي يحتاجون إليه لمحاربة المجرمين والتهديدات الأمنية.

١٠- ثقةُ العملاء :حماية بيئة العمل من جميع أنواع التهديدات الأمنية المتوقعة يمكن أن تزيد الثقة بين الشركة وعملائها، حيث سيشعرون بثقة أكبر عند التعامل مع الشركة أو استخدام خدماتها أو استشارتها.

١١- القدرةُ على توفير استراتيجيات مُخصصة ومُدعمة للأمن السيبراني من خلال تهيئة وضع أمني قوي ضد أي هجمات خطيرة تهدف إلى الوصول أو تغيير أو حذف أو تدمير أو ابتزاز أنظمة المنظمة أو المستخدم والبيانات الحساسة.

خامسًا- التحدياتُ التي يواجهها الأمنُ السيبراني: (دحام/٢٠٢١)

تتنوع العملياتُ التي من الممكن للمؤسسات العامة والأشخاص القيام بها على شبكة الإنترنت مثل حفظ ومشاركة الصور، ومقاطع الفيديو، ومعلومات بطاقات الائتمان، والبيانات الشخصية، مما يُمثل تحديًا أمامَ الأمنِ السيبراني في كيفية المحافظة على جميع المعلومات آمنة وبعيدة عن السرقة والاستغلال، حيث يوجد العديد من التحديات التي يواجهها الأمن السيبراني،من أبرزها مايلي:

١- *هجماتُ برامج الفدية :Ransomware attacks* تُعدُّ من أكثر أنواع التحديات الشائعة في مختلف أرجاء العالم، وتتضمن هجمات مُعدَّة مسبقًا لاختراق بيانات المستخدمين ومنعهم من الوصول إليها إلا بعد دفع مبلغ من المال (الفدية)، حيث لن تتمكن من تشغيل أعمالها اليومية إلا بعد التفاوض مع منفذي هذا الاختراق ودفع المبلغ الذي يطالبون به، ومن الممكن أن لا يفرج هؤلاء الأشخاص عن البيانات حتى بعد دفع الفدية رغبةً منهم في الحصول على المزيد من الأموال.

٢- *الهجماتُ السحابيةCloud attacks:* وهي اختراق الأنظمة الأساسية التي يتم تحميل البيانات إليها على شبكة الإنترنت من أجل سرقة بيانات المستخدمين الموجودة عليها. ويستخدم الكثير من الناس والمؤسسات الأنظمة السحابية، وقد تكون هذه الهجمات ذات آثار كارثية فيما لو طُبِّقت على مؤسسة لأنه من الممكن أن تُعرِّض مثل هذه الهجمات المؤسسات إلى الانهيار التام.

٣- *هجماتُ التصيد الاحتيالية Phishing attacks:* وهي من الهجمات الشائعة، حيث يسرق المخترق بيانات المستخدم بما في ذلك معلومات تسجيل الدخول للمواقع المختلفة، وأرقام بطاقات البنوك والائتمان. لا يمنع المُخترق في هجمات التصيد المستخدم الأصلي

من الوصول إلى بياناته، وإنَّما يستخدم المعلومات الخاصة به للقيام بأعمال نصب واحتيال مثل التسوق عبر الإنترنت، وتحويل الأموال بطريقة غير قانونية .

٤- *هجماتُ البلوكتشين والعملات المشفرة Block chain and crypto currency attacks:*

وهي تستهدف بيانات الشركات الكبيرة الأمر الذي من شأنه أن يُعرِّض بيانات العملاء فيها والعمليات التجارية التي تقوم بها إلى مخاطر كبيرة وآثار كارثية لا حصر لها.

٥- *هجماتُ الذكاءِ الاصطناعي AI attacks:* يستخدمه منفذو هجمات الكومبيوتر كوسيلة للوصول إلى المعلومات والبيانات الخاصة بالشركات والتي تكون ذات قيمة عالية من أجل تحقيق مكاسب مادية على حساب هذه الشركات.

٦- *الهجماتُ الداخلية Insider attacks:* وهي من التحديات الكبيرة التي تواجه الأمن السيبراني لا سيما أنها عمليات تخريب تصدر من داخل الشركة أو المؤسسة ذاتها ومن قِبل أشخاص يعملون فيها بهدف تسريب بعض البيانات لشركات منافسة أخرى. وهي تؤدي إلى إلحاق خسائر مالية كبيرة في الشركة التي تتعرض لها.

٧- *هجماتُ إنترنت الأشياء IOT Attacks*: وهي تستهدف أجهزة حوسبية، ورقمية، وميكانيكية يُمكنها نقل البيانات بشكل مستقل عبر الشبكات الإلكترونية، ومن الأمثلة على هذه الأجهزة أجهزة الكمبيوتر المكتبية والمحمولة، والهواتف المحمولة الذكية، وأجهزة الأمان الذكية وغيرها من الأجهزة. ومع تزايد استخدام أجهزة إنترنت الأشياء من قِبل الناس والشركات تزايدت التحديات التي يمكن أن تواجه الأمن السيبراني أيضًا، فالوصول إلى هذه الأجهزة من قِبل المخترقين يفسح مجالاً واسعاً أمام القيام بهجمات مُضرَّة تُعرف باسم هجمات إنترنت الأشياء.

سادسًا– طريقةُ تطبيقِ الأمنِ السيبراني: (أبو شوالي)

يُعدُّ تطبيقُ الأمن السيبراني – والطريقة التي سوف أذكرها – مبنية على توصيات الأيزو ISO2700 ٢٧٠٠١ ويمكن تناول ذلك على النحو التالي:

١– *بيئةُ ووضعُ المنشأةِ:* يجب على المؤسسة فهم المنشأة وبيئتها ووضعها من حيث تحديد القضايا الخارجية والداخلية ذات الصلة والتي تؤثر على قدرتها في تحقيق النتائج المرجوة. بالإضافة الى فهم احتياجات وتوقعات الجهات المعنية حيث يجب عليها تحديد كافة الجهات المهتمة ذات الصلة ومتطلباتها المعنية.

٢– *القيادةُ:* يجب على الإدارة العليا إظهار الإلتزام فيما يتعلق بنظام أمن المعلومات من خلال ضمان سياسة أمن المعلومات وأهدافها الموضوعة وتوافقها مع التوجه الإستراتيجي، ودمج متطلبات أمن المعلومات في عملياتها، وتوفير الموارد اللازمة والتواصل مع كافة الجهات والتأكيد على أهمية الإدارة الفعالة لأمن المعلومات والتأكد من تحقيق النتائج المرجوة منه، وتوجيه ودعم الأشخاص للمساهمة في فعالية النظام وتشجيع التحسين المستمر، ودعم أدوار الإدارات الأخرى ذات الصلة لإثبات قيادتهم. كما يجب على الإدارة العليا أيضًا وضع سياسة لأمن المعلومات تراعي من خلالها أهداف المؤسسة وأمن المعلومات، والإلتزام بالمتطلبات المعمول بها والمتعلقة بأمن المعلومات ويشمل الإلتزام بالتحسين المستمر لنظام أمن المعلومات. ويجب على سياسة أمن المعلومات أن تكون متاحة كمعلومة موثقة والتواصل من خلال إرسالها داخل المؤسسة أو الشركة، وأن تكون متاحة للجهات المعنية، حسب ما هو مناسب.

٣– *التخطيطُ:* يجب تطوير إستراتيجية لإزالة أو تعطيل الوظائف غير الضرورية من الأنظمة، وإصلاح الثغرات المعروفة بسرعة. من المحتمل أن يؤدي الفشل في القيام بذلك

إلى زيادة خطر تعرض النظم والمعلومات. وعند التخطيط لنظام إدارة أمن المعلومات يجب على المؤسسة تحديد المخاطر وكيفية معالجتها، وذلك بتمكين نظام إدارة أمن المعلومات من تحقيق النتائج المرجوة ومنع أو تقليل الآثار غير المرغوب فيها، وتحقيق التحسين المستمر. ويجب على المؤسسة أيضًا وضع خطة لمعالجة هذه المخاطر وكيفية تنفيذ ذلك من خلال تفعيلها في عمليات نظام إدارة أمن المعلومات وتقييم فعاليتها.

ويجب على المؤسسة وضع معايير لعملية تطبيق وتقييم مخاطر أمن المعلومات، وتشمل :معايير قبول المخاطر، ومعايير إجراء تقييمات المخاطر الأمنية، والتأكد من تكرار إجراءات التقييم المستمرة للمخاطر المتعلقة بأمن المعلومات وأنها تؤدي إلى نتائج متسقة وصالحة وقابلة للمقارنة. وتتم عملية تحديد مخاطر أمن المعلومات من خلال تطبيق عملية التقييم لها لتحديد المخاطر المرتبطة بالسرية والنزاهة وتوافر المعلومات وتحديد أصحاب المخاطر، وتحليل مخاطر أمن المعلومات من خلال تقييم العواقب المحتملة التي قد تنتج إذا وقعت وتحققت وتقييم الاحتمال الواقعي لحدوثها، وتحديد مستويات المخاطر. كما يجب تقييم مخاطر أمن المعلومات من خلال مقارنة نتائج تحليلها مع معايير المخاطر وإعطاء الأولوية للمخاطر الأكثر تهديدًا وتأثيرًا.

ويجب على المؤسسة تحديد عملية معالجة مخاطر أمن المعلومات وذلك من خلال تحديد خيارات معالجتها المناسبة، مع مراعاة نتائج تقييم المخاطر وتحديد جميع الضوابط اللازمة لتنفيذ خيارات معالجتها المختارة، وصياغة خطة لمعالجة مخاطر أمن المعلومات، والحصول على موافقة أصحاب المخاطر على تلك الخطة وقبول مخاطر أمن المعلومات المتبقية.

٤- *الدعمُ:* يجب على المؤسسة توفير الموارد اللازمة للإنشاء والتنفيذ والصيانة المستمرة لنظام أمن المعلومات. وتحديد الكفاءة اللازمة للأشخاص الذين يقومون بالعمل تحت سيطرتها مما يؤثر على أداء أمن المعلومات الخاص بها، والتأكد من قدراتهم المؤهلة، وعند الضرورة، اتخاذ الإجراءات اللازمة لاكتساب الكفاءة المطلوبة، وتقييم فعالية الإجراءات المتخذة. ويجب أن يكونوا على دراية بسياسة أمن المعلومات، ومساهمتهم في فعالة نظام إدارة أمن المعلومات، بما في ذلك فوائد تحسين أداء أمن المعلومات، والآثار المترتبة على عدم الإمتثال لمتطلبات نظام إدارة أمن المعلومات. ويجب على المؤسسة تحديد الاتصالات الداخلية والخارجية ذات الصلة بنظام إدارة أمن المعلومات بما في ذلك: على ماذا يتم الاتصال؛ ومتى ووقت الاتصال؛ ومع من الاتصال؛ ومن يجب عليه الاتصال؛ والعمليات التي من خلالها يتم تنفيذ الاتصال.

٥- *التشغيلُ:* يجب على المؤسسة تخطيط وتنفيذ ومراقبة العمليات اللازمة لتلبية متطلبات أمن المعلومات، ويجب عليها أيضًا تنفيذ خطط لتحقيق أهداف أمن المعلومات. ويجب عليها التحكم في التغييرات المخطط لها ومراجعة عواقب التغييرات غير المقصودة، واتخاذ إجراءات لتخفيف أية آثار ضارة حسب الحاجة. والتأكد من أن العمليات الخارجية يتم تحديدها والتحكم فيها.

٦- *تقييمُ الأداء:* يجب على المؤسسة تقييم أداء أمن المعلومات وفعالية نظام إدارته من خلال تحديد ما الذي يجب مراقبته وقياسه بما في ذلك عمليات وضوابط أمن المعلومات، وطرق الرصد أو المراقبة والقياس والتحليل والتقييم حسب الحاجة لضمان نتائج صحيحة، ومتى يتم إجراء الرصد والقياس؟ ومن يقوم بالرصد والقياس؟ ومتى يتم تحليل نتائج الرصد والقياس وتقييمها؟ ومن يقوم بتحليل وتقييم هذه النتائج؟. وبالتالي يجب على الإدارة العليا

القيام بمراجعة نظام أمن المعلومات على فترات زمنية مخططة لضمان استمرار ملاءمتها وكفاءتها وفعاليتها. ويجب الأخذ بعين الإعتبار أن تشمل مراجعة الإدارة حالة الإجراءات من مراجعات الإدارة السابقة، والتغييرات في القضايا الخارجية والداخلية ذات الصلة بنظام إدارة أمن المعلومات، وردود الأفعال على أداء أمن المعلومات، وردود الفعل من الجهات المعنية وذات الصلة، ونتائج تقييم المخاطر وحالة خطة معالجتها، وفرص التحسين المستمر.

٧- *التحسيناتُ:* يجب على المؤسسة عند حدوث عدم المطابقة لأي إجراء أو توصية أن تقوم باتخاذ إجراء على عدم المطابقة، واتخاذ الإجراءات للسيطرة عليه وتصحيحه والتعامل مع العواقب وتقييم الحاجة إلى اتخاذ إجراءات للقضاء على سبب عدم المطابقة، من أجل ألا تتكرر أو تحدث في مكان آخر من خلال مراجعة عدم المطابقة، وتحديد أسباب عدم المطابقة، وتحديد ما إذا كانت هناك أوجه تشابه مماثلة، أو يمكن أن تحدث.

وأيضًا من طرق تحقيق الأمن السيبراني على المستوى الفردي:

(أ) الموثوقيةُ :عند تقديم معلوماتك الشخصية، يرجى استخدام مواقع الويب الموثوقة فقط، وأفضل قاعدة عامة هنا هي التحقق من عنوان .URL إذا كانت بداية موقع الويب تحتوي علىhttps ، فهذا يعني أن موقع الويب هو موقع آمن، ولكن إذا كان عنوان URL يحتوي على http بدونs ، فتجنب إدخال أي معلومات حساسة، مثل معلومات بطاقة الائتمان أو رقم الضمان الاجتماعي.

(ب) الإيميلُ الاحتيالي : لا تفتح مرفقات البريد الإلكتروني أو تنقر على رابط لرسالة من مصدر غير معروف، لأن إحدى الطرق الأكثر شيوعًا للسرقة أو الاختراق هي من خلال

رسائل البريد الإلكتروني السرية (مثل رسائل البريد الإلكتروني التي يرسلها أشخاص تثق بهم.

*(ج) تحديثُ نظام هاتفك المحمول :*احرص دائمًا على تحديث جهازك. غالبًا ما تحتوي تحديثات البرامج على تصحيحات مهمة لمعالجة مشكلات الأمان، وتتركز هجمات الاختراق الناجحة على الأجهزة القديمة التي لا تحتوي على أحدث برامج الأمان.

*(د) النسخةُ الاحتياطيةُ :*قمْ بعمل نسخ احتياطية من الملفات بشكل منتظم لمنع هجمات أمن الإنترنت إذا كنت بحاجة إلى تنظيف الجهاز بسبب هجوم سابق على الشبكة ، فسوف تساعدك على تخزين الملفات في مكان آمن ومستقل.

سابعًا– تدابيرُ الأمنِ السيبراني: (أبو شوالي)

إن تطبيق التدابير الفعالة للأمن السيبراني يمثل تحديًا كبيرًا اليوم والغد نظرًا لوجود أجهزة وبرامج كثيرة واعتماد أغلب الشركات والمؤسسات في كافة القطاعات على أجهزة الحاسب الآلي والبرامج وملحقاتها من أجهزة الشبكة وغيرها. وإن الهدف الرئيس لحماية المعلومات هو ضمان سرية وسلامة (نزاهة) وتوافر المعلومات .(CIA) وإن أي حدث أو مشكلة تهدد المثلث الأمني (سرية، وسلامة، وتوافر المعلومات) يَعدُّ تهديدًا أمنيًا يجب التعامل معه وحله أو وضع آليات أو إجراءات لتفاديه أو التقليل من آثاره.

ولا شك أن الأمن السيبراني يتكون من مجموعة متطورة من الأدوات، وأساليب إدارة المخاطر، والتقنيات، والتدريب، وأفضل الممارسات المصممة لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الوصول غير المصرح به أو الإنقطاع. وفيما يلي يمكن تناول هذه التدابير:

١- *سِريةُ المعلومات* :*Confidentiality* المقصود بسرية المعلومات هي ضمان أن يصل إليها فقط الأشخاص المصرح لهم بالوصول إلى هذه المعلومات بالإضافة الى وضع أسس ومعايير لعملية الوصول والصلاحيات اللازمة لذلك بما يضمن بشكل قاطع أن الأشخاص المصرح لهم بالوصول إلى هذه المعلومة هم فقط يمكنهم الحصول عليها وليس غيرهم.

٢- *سَلامةُ (نزاهة) المعلومات* :*Integrity* والمقصود بها الحفاظ على تناسق ودقة البيانات طوال دورة حياتها بأكملها والتأكد من عدم تغييرها أو استبدالها خلال دورة حياة المعلومات. ويجب عدم تغيير البيانات أثناء النقل، واتخاذ خطوات لضمان عدم إمكانية تغيير البيانات بواسطة أشخاص غير مصرح لهم، وأذونات الملفات وعناصر تحكم وصول المستخدم. ربما يستخدم بعض الأدوات أو البرامج لمنع حدوث تغييرات خاطئة أو الحذف العرضي من قبل المستخدمين المصرح لهم.

ويجب أن تتوافر بعض الوسائل للكشف عن أية تغييرات في البيانات قد تحدث نتيجة للأحداث غير البشرية أو تعطل الخادم. وبالتالي قد يستخدم التشفير للتحقق من النزاهة. ويتطلب أن تكون النسخ الإحتياطية أو التكرار متاحة لإستعادة البيانات المتأثرة إلى حالتها الصحيحة.

٣- *توافرُ المعلوماتِ* :*Availability* والمقصود بها أن تكون المعلومة متوفرة عند طلبها أو الحاجة إليها في أي وقت. ويتم ضمان التوافر بشكل أفضل من خلال الحفاظ على جميع الأجهزة بحالة سليمة وفعالة، وإجراء الإصلاحات فورًا عند الحاجة، والتأكد أن نظام التشغيل يحصل على التحديثات والترقيات الضرورية. ويفضل وجود خطة شاملة لإستعادة القدرة على العمل بعد الكوارث. وأن تتوافر إجراءات وقائية ضد فقدان البيانات أو انقطاعها في الإتصالات نتيجة الأحداث غير المتوقعة مثل الكوارث الطبيعية والحرائق.

ولمنع فقدان البيانات يتم تخزين نسخة احتياطية في مكان معزول جغرافيًا، وفي خزنة مضادة للحريق ومقاومة للماء والمفاجاءات.

ويجبُ حماية الأجهزة والبرامج والبيانات من التوقف التي يتعذر الوصول إليها بسبب الإجراءات الضارة مثل هجمات رفض الخدمة DOS وتطفل الشبكات network intrusions باستخدام جدران الحماية النارية والخوادم الوكيلة IDS/IPS .

ثامنًا– مدى توافر معايير الأمن السيبراني في منظومة التعليم الدولية:

أوضحت النتائجُ بشكل إجمالي عن توافر معايير الأمن السيبراني في الجامعات التعليمية، حيث جاء التقدير المئوي للوزن النسبي للمعايير السبعين طرديًّا وكان أعلى نسبة لها في جامعة هارفارد/ بأمريكا بنسبة (٩٧,٤%) وجامعة اسطنبول بنسبة (٩٥,٣%)، وجامعة جين جي/ بتايوان بنسبة (٩٠,١%)، ثم جاء أقل نسبة لها في جامعة القاهرة/ بمصر بنسبة (٨٠,٣%). وهي نسب مرتفعة تعكس أهمية معايير الأمن السيبراني في منظومة التعليم الدولية كواقع يتحقق في الجامعات الأمريكية والأوروبية والآسيوية باستثناء جامعات الشرق أوسط التي تتطلب اهتمامًا كبيرًا من المسؤولين المعنيين بتوفير الإمكانات والبيئات والكفاءات اللازمة لمواجهة الهجمات والقرصنة الإلكترونية وتلاشي انعكاسها على المجتمع الإقليمي والدولي.

وقد أظهرت النتائج أيضًا أن للموسسات التعليمية الجامعية دورًا كبيرًا في الاهتمام بالامن السيبراني وتفعيله، ولا بد من إيجاد الإطار التشريعي والتنظيمي التربوي المؤيد لتوضيح مخاطر الامن السيبراني على المجتمع، وأن أساتذة الجامعات يؤيدون استمرارية عمل تقنيات المعلومات، وأن استقرار الفضاء السيبراني يستدعيي سياسات لمعالجة الثغرات الأمنية، وأنه لابد من دعم الجهود التربوية والتعليمية بالآليات الفعالة بوضع مناهج توعوية

لأهمية الامن السيبراني ، والإفادة من أفضل الممارسات والتجارب الناجحة، التي تعزز الثقة في الفضاء السيبراني، وتُوْجِد بيئة داعمة لنمو النشاط التعليمي والعلمي في الفضاء السيبراني، وتتطلب المكافحةُ الفاعلةُ أجهزةً مُتخصِصةً، وعناصرَ تتميز بالكفاءة والقدرة على الإحاطة بجوانب كيفية إدارة أنظمة المعلومات وطرق معالجة البيانات، والحقوق المتصلة بها في منظومة التعليم الدولية.

ومن ثَمَّ توصي الدراسةُ الراهنةُ بضرورة تفعيل معايير الأمن السيبراني في منظومة التعليم الدولية، وإدراج مجال الفضاء السيبراني ضمن مناهج التعليم في المؤسسات التعليمية المختلفة، والحث على مجالات البحث العلمي والابتكار في مجال الأمن السيبراني، وتوعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية الاحترافية لديهم وإرساء بنية تحتية للدخول إلى مجال صناعة البرمجيات العالمية.

المراجع

أولًا- المراجع العربية:

القرآنُ الكريمُ.

آبادي، الفيروز (١٤٢٦هـ/ ٢٠٠٥)، "القاموس المحيط" ط ٨، بيروت: مؤسسة الرسالة، ص ١١٧٦.

أبو شوالي، "الأمن السيبراني :cyber security أهميته، وما الغاية منه؟"-https://www.rmg sa.com/cyber-security

البكري ، يوسف الشيخ.(٢٠١٧)،"أمن المعلومات بالمكتبات الجامعية السودانية بالإشارة إلى مكتبتي جامعة النيلين وجامعة وادي النيل" في المؤتمر الثالث والعشرون لجمعية المكتبات الخاصة، قطر

دحام، مها.(٢٠٢١)،"ما هي أنواع الأمن السيبراني؟ وما أبرز التحديات التي يواجهها؟" https://sotor.com

تمت الكتابة بواسطة: مها دحام تم التدقيق بواسطة: هدى الخطيب آخر تحديث: ١١:١٠ ، ٢١ نوفمبر ٢٠٢١.

الروسان، فرح.(٢٠٢١)،"ما هي أنواع الأمن السيبراني؟"" https://mawdoo3.com/

تمت الكتابة بواسطة: فرح الروسان تم التدقيق بواسطة: ديما ابو عليم آخر تحديث: ٠٩:٤٦ ، ١٧ نوفمبر ٢٠٢١

السحيباني،عبد الله.(١٩٩٦)،"كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات" رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

السمحان، منى عبد الله.(٢٠٢٠)،"متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود"مجلة كلية التربية، العدد ١١١، يوليو، كلية التربية، جامعة المنصورة.

https://maed.journals.ekb.eg/article_140786_92feaa0b360fd79ceb4b6c5d7a95be72.pdf

شاكر، أسماء. (٢٠٢٠) ، "مكونات منظومة التدريس")،

ششمدين، عفاف.(٢٠٠٣)،"الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات" دمشق.

الشيتي، إيناس إبراهيم.(٢٠١٩)،"تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربية السعودية: دراسة تطبيقية على جامعة القصيم"، ماجستير غير منشورة، جامعة القصيم.

صبري ، ماهر إسماعيل.(٢٠١٠) ، "المناهج ومنظومة التعليم" ، الطبعة الثالثة منقحة ، سلسلة الكتاب الجامعي العربي ، مكتبة الرشد ، الرياض: ص ٣٨ – ٤٠.

العبيدي ، إبراهيم. (٢٠١٨)، مبادئ التعليم – عناصر العملية التعليمية ،١٩ يوليو https://mawdoo3.com/%

العتيبي، عبد الرحمن بن بجاد.(٢٠١٧)،"دور الأمن السيبراني في تعزيز الأمن الإنساني"أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية"كلية العلوم الإستراتيجية.

العنزي، سليمان.(٢٠٠٣)،"وسائل التحقيق في جرائم نظم المعلومات" رسالة ماجستير ، الرياض: جامعة نايف العربية للعلوم الأمنية.

المعهد العربي للتخطيط،(٢٠١٩)،"مخاطر الهجمات الإلكترونية السيبرانية وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي" على الموقع https://www.researchgate.net/institution/Arab_Planning_Institute2

الموسوعة السياسية بتاريخ ٢٠٢٠/٤/٦ على الموقع https://political-encyclopedia.org/dictionary/

ثانيًا– المراجع الأجنبية:

-Brenton,C& Hunt, C. (2003) Mastering – Network security, SYBEX Inc. US.

-El Hissi, Y.& Arezki, S.(2018).Conceptualization of an Information System Governance Model Dedicated to the Governance of Scientific Research in Moroccan University,2018 4th International Conference on Computer and Technology Applications.

-Emarah,S. (2007) : The Control of Firewalls using Active Networks, Information Technology and national security Conference, Riyadh.

-Idris,N & Shanmugam,B (2007): Hybrid Intelligent Intrusion Detection System, InformationTechnology and national security Conference, Riyadh.

-Rehman, H.,Masood ,A.& Cheema ,A.(2013). Information Security Management in Academic Institutes of Pakistan,2nd .National Conference of Information Assurance(NCIA)