تدريس مقرر أمن المعلومات بأقسام ومدارس المكتبات والمعلومات في ضوء معايير الأمن السيبراني: دراسة مسحية (الجزء الأول)(*)

Teaching an Information Security Course in Library and Information Departments and Schools in Light of Cybersecurity Standards: A Survey Study (Part I)

د. لمياء مختار عبد الحميد

مدرس المكتبات والمعلومات

كلية الآداب – جامعة حلوان

Email: Lamiaa_mokhtar@arts.helwan.edu.eg

ORCID: 0009-0002-6734-8039

المستخلص:

تهدف الدراسة إلى الاستعداد لمواجهة التحديات الناجمة عن التقدم السريع في تكنولوجيا المعلومات، إذ يعد أمن المعلومات بمثابة مزيج من العمليات والتقنيات والممارسات التي تجري بشكل يومي؛ للحفاظ على المعلومات وتنظيم عملية الوصول إليها. وتهدف الدراسة أيضًا إلى إلقاء الضوء على موضوع الأمن السيبراني باعتباره منبثقًا من أمن المعلومات، ولكنه يركز على حماية البرامج والأجهزة والشبكات والتطبيقات والبيانات من أي هجوم سيبراني داخلي أو خارجي داخل المكتبات أو مؤسسات المعلومات، ويمكن الإشارة إليه أيضًا بأمن تكنولوجيا المعلومات. هذا وتتيح تلك الدراسة التعرف على الأقسام العلمية التي تقوم بتدريس مقرر أمن المعلومات أو الأمن السيبراني في صورة مقرر مستقل، أو تدخله في جزء من مقرر لديها، ومدى ملاءمته لسوق العمل، مع وصف تلك المقررات بالجامعات محل الدراسة وتحليلها، وكذا رصد المسميات المختلفة للمقرر، من أجل تقديم نموذج توصيف مقترح لمقرر أمن المعلومات قد يكون توصيفًا استرشاديًّا لأقسام المكتبات بالجامعات المصرية وفقًا لبنود المعيارين اللذين أصدرتهما المنظمة الدولية للتوحيد القياسي (أيزو)، وهما معيار (ISO/IEC ٢٧٠٠٢) ومعيار (ISO/IEC ٢٧٠٣٢).

وقد اعتمدت الدراسة على المنهج المسحي لحصر مقررات أمن المعلومات أو الأمن السيبراني بأقسام ومدارس المكتبات والمعلومات على المستوى المحلي والإقليمي، وعلى مستوى الولايات المتحدة الأمريكية وكندا، للتعرُّف على ماهية تدريس تلك المقررات والمسمى

(*) يُنْشَر القسم الثاني من الدراسة في العدد رقم ٣٥ (سبتمبر ٢٠٢٥).

الذي يندرج تحته داخل هذه الأقسام، مع استخدام أسلوب تحليل المحتوى Content Analysis، لدراسة توصيفات تلك المقررات وتحليلها بغرض دراسة مدى توافقها للتطبيق داخل أقسام المكتبات في جمهورية مصر العربية.

وقد حُلِّلَت تلك المقررات من خلال قائمة مراجعة جرى إعدادها مسبقًا لأغراض البحث، حيث تكوَّن مجتمع الدراسة من (٣٠) قسمًا علميًّا على المستوى المحلي والإقليمي، وعلى مستوى الولايات المتحدة الأمريكية وكندا.

وقد خلصت الدراسة إلى مجموعة من النتائج كان أبرزها: إنه لا يوجد سوى قسم المكتبات والمعلومات بجامعة سوهاج، وهو القسم العلمي الوحيد، الذي ذكر في توصيف مقرره "أمن المعلومات وضبط جودتها" أنه يعتمد في إعداده على المعيارين اللذين أصدرتهما المنظمة الدولية للتوحيد القياسي (أيزو)، في حين لم يتوفر ذلك في باقي المقررات محل الدراسة، علمًا بأن جامعة بني سويف هي الجامعة الوحيدة – من ضمن الجامعات محل الدراسة– التي تقدم مقررًا له علاقة بأمن المعلومات في مرحلة الدكتوراه، تحت مسمى "الجرائم المعلوماتية والأمن القومي" بشكل إجباري. هذا ويقدم عدد (٢٩) مقررًا داخل الجامعات محل الدراسة من أصل (٤٩) مقررًا، عن أمن المعلومات أو الأمن السيبراني في مرحلة الماجستير، وهي أكثر المراحل التعليمية تطبيقًا للمقرر.

الكلمات الدالة:

أمن المعلومات – الأمن السيبراني – الأمن السيبراني المجتمعي – التهديدات السيبرانية – التصيد الاحتيالي

Abstract:

The study aims to prepare for the challenges resulting from the rapid progress in information technology, as information security is a combination of daily processes, technologies and practices to preserve information and organize access to it. The study also aims to shed light on the topic of cybersecurity as an offshoot of information security, but it focuses on protecting programs, devices, networks, applications and data from any internal or external cyberattack within libraries or information institutions. It can also be referred to as information technology security. This study allows identifying the academic departments that teach the information security or cybersecurity course as an independent course or include it in part of a course they have and its suitability for the labor market, with a description of those courses in the universities under study and analyzing them, as well as monitoring the different names of the course, in order to provide a proposed description model for the information security course that may be a guiding description for library departments in Egyptian universities according to the provisions of the two standards issued by the International

Organization for Standardization (ISO), namely (ISO/IEC 27002) and (ISO/IEC 27032).

The study relied on the survey method to limit information security or cybersecurity courses to library and information departments at the local and regional levels and at the level of the United States of America and Canada, to identify the nature of teaching these courses and the name under which they fall within these departments, while using the Content Analysis method to study the descriptions of these courses and analyze them for the purpose of studying the extent of their compatibility with application within library departments in the Arab Republic of Egypt.

These courses were analyzed through a checklist that was prepared in advance for research purposes, as the study community consisted of (30) scientific departments at the local and regional levels and at the level of the United States of America and Canada.

The study concluded with a set of results, the most prominent of which were: There is only the Department of Libraries and Information at Sohag University, which is the only scientific department, which stated in the description of its course "Information Security and Quality Control" that it relies in its preparation on the two standards issued by the International Organization for Standardization (ISO), while this was not available in the rest of the courses under study, noting that Beni Suef University is the only university - among the universities under study - that offers a course related to information security at the doctoral level, under the name "Information Crimes and National Security" on a mandatory basis. In addition, (29) courses are offered within the universities under study out of (49) courses, on information security or cybersecurity at the master's level, which is the educational level that most applies the course.

Keywords:

Information Security - Cybersecurity - Community Cybersecurity - Cyber Threats - Phishing.

المقدمة:

من منطلق أن المكتبات هي مركز لنشر المعلومات والمعرفة سواء داخل المجتمع أوخارجه، فقد كان لزامًا عليها مواكبة التطورات التكنولوجية التي تحدث حولها، وذلك بتوفير العديد من المصادر الرقمية لتقديم الخدمات الرقمية لمستفيديها، الأمر الذي أدى إلى انتشار الجرائم الإلكترونية للتعدي إما على خصوصية مستفيديها وبياناتهم، وإما على حقوق الملكية الفكرية أو ما تقدمه من معلومات، ما يستدعي أقسام المكتبات لتضع في عين الاعتبار تأهيل طلابها أختصاصي مكتبات تلك المكتبات، وتجهيزهم بالمعرفة والتدريب على كيفية

الحفاظ على أمن المعلومات والأمن السيبراني وتفادي المخاطر المحتملة لهما، وتعزيز السلوك الأخلاقي المعلوماتي والسيبراني لديهم.

وفي ظل التطورات التكنولوجية التي يشهدها العالم الرقمي تعد تهديدات أمن المعلومات والأمن السيبراني من أكثر القضايا أهمية، والتي يجب أن تتنبه لها قطاعات المكتبات ومؤسسات المعلومات المختلفة في المستقبل، سواء كانت تلك التهديدات الأمنية تهديدات لأمن أجهزة الكمبيوتر أو تهديدات لأمن المعلومات أو تهديدات سيبرانية... إلخ، حيث يعد عدم فهم مدى خطورة هذه الهجمات من العوامل المؤثرة في تزايدها.

لقد أحدثت شبكة الإنترنت تطورًا كبيرًا في شكل تبادل الأفراد للبيانات والمعلومات وفي تواصلهم مع بعضهم، بل في طريقة عملهم واكتسابهم للمعرفة. وعلى الرغم من الميزات التي جلبتها شبكة الإنترنت؛ فإنها تمثل أيضًا تحديًا أخلاقيًّا لشكل تبادل وتداول هذه المعلومات والبيانات دون التعدي على حقوق الملكية الفكرية؛ إذ أصبحت أغلب مجموعات المكتبات رقمية فضلًا عن قواعد البيانات التي تُتَاح من خلالها والخدمات الرقمية الأخرى التي تقدمها، الأمر الذي يجعل من الضروري على أعضاء هيئة التدريس بمدارس المكتبات والمعلومات نشر الوعي بأخلاقيات استخدام شبكة الإنترنت، ومن ثمَّ التعريف بأمن المعلومات والأمن السيبراني؛ لمواجهة تلك التحديات التي من الممكن أن تواجه المكتبات ومؤسسات المعلومات ومستخدميها في المستقبل.

وقد أظهر استطلاع الرأي الذي أجرته شركة Price Water House Coopers (PWC) (PwC, 2024) عن الثقة الرقمية العالمية لعام ٢٠٢٤، وقد شمل ٣٨٧٦ مديرًا تنفيذيًّا في مجال الأعمال والتكنولوجيا في كبرى الشركات العالمية، أن:

١- ٣٠% فقط من المشاركين في استطلاع الرأي لديهم إيرادات تبلغ ١٠ مليارات دولار أو أكثر، خاصة لتحسين الأمن السيبراني لديها.

٢- حوالي ثلث المؤسسات المشاركة في الاستطلاع ليس لديها خطة لإدارة المخاطر لمعالجة التحديات التي يواجهها مقدمو الخدمات السيبرانية، على الرغم من أن الهجمات السيبرانية هي مصدر القلق الأكبر لتلك الشركات.

٣- نصف عينة الاستطلاع كانوا "راضين جدًّا" عن قدراتهم التكنولوجية في مجالات الأمن السيبراني الرئيسة.

٤- أكثر من ٣٠% لا يتبعون الممارسات القياسية للدفاع السيبراني.

لذلك، أصبح الوعي بأمن المعلومات والأمن السيبراني أمرًا ملحًّا بين طلاب الجامعات؛ لاستخدامهم مختلف الوسائل التكنولوجية في كافة جوانب الحياة اليومية، علمًا بأن قطاع الجامعات من أكثر القطاعات انفتاحًا لتسهيل التعاون بين الباحثين حول العالم، وتأتي الهجمات السيبرانية مثلًا فتشكل تهديدًا لأمن المعلومات أيًّا كان نوعها، ما يجعلهم أكثر فئة مستهدفة من تلك الهجمات، إما للحصول على بيانات ائتمانية وإما للحصول على بيانات علمية مهمة.

هذا وقد رصدت المراكز الوطنية للتميز الأكاديمي " (CAE)" The National Centers of Excellence Academic (CAE, 2022) عدد (٣٠٠) مؤسسة تعليمية تقدم برامج عن أمن المعلومات أو عن الأمن السيبراني. ووفقًا للمركز الوطني للأمن السيبراني بالمملكة المتحدة (Center, 2019)، فقد أشار إلى أن قطاع الجامعات ثالث أكثر القطاعات عرضة للهجمات السيبرانية؛ ففي أغسطس ٢٠١٨ اكتشف الباحثون بالمركز أكثر من (٣٠٠) موقع وصفحات مزيفة لتسجيل للدخول إلى (٧٦) جامعة في (١٤) دولة، منها المملكة المتحدة، عن طريق انتحال شخصيات شركاء الجامعات أو مورديها، وذلك بتوجيه الضحايا إلى تلك المواقع عن طريق البريد الإلكتروني، ثم بعد إدخال بيانات اعتمادهم سواء من شهادات أو بيانات ابتعاث إلى تلك المواقع المزيفة تجري سرقة تلك البيانات، الأمر الذي يهدد البيانات الأكاديمية وحقوق الملكية الفكرية، وقد جاء هذا الهجوم السيبراني في أعقاب حملة إيرانية سابقة بين عامَي ٢٠١٣ و٢٠١٧، استهدف مبنى لحسابات أكثر من (١٠٠) ألف أستاذ جامعي في جميع أنحاء العالم، أدى إلى فقدان أكثر من (٣٠) تيرابايت من البيانات الأكاديمية وحقوق الملكية الفكرية.

ولذلك قامت المنظمة الرسمية التي تمثل جامعات المملكة المتحدة من خلال تقرير أعدته عن وضع الأمن السيبراني داخل جامعاتها، بوضع مجموعة من الضوابط التي يجب على الجامعات اتباعها للمحافظة على أمنها السيبراني على النحو التالي (UK & Center, 2023):

١- فهم المخاطر والتحديات التي تواجه جامعتك، ويدخل في ذلك الفئات التي تستهدفك.

٢- تعزيز وضع الأمن السيبراني داخل جامعتك، من خلال إدارة فعالة ومتمكنة من كل جوانب المؤسسة، من خلال وضع ضمانات تكنولوجية، وثقافات أمنية إيجابية لكل منتسبي الجامعة، ويدعمها شفافية واضحة.

٣- وضع عناصر تحكم أساسية لاكتشاف الهجمات السيبرانية والتصدي لها أو تأجيلها.

٤- وضع ضوابط أمنية قوية تقنية وغير تقنية للتعامل اللحظي مع أي هجمات قد

تحدث.

٥- خلق ثقافة التحسين المستمر، من خلال التدريب والاختبارات وتبادل الخدمات والخبرات والتجارب مع المجتمع.

مصطلحات الدراسة:

أمن المعلومات Information Security: (Marron,2024)

يعني حماية المعلومات وأنظمة المعلومات من الوصول غير المصرح، من أجل توفير ما يلي:

أ- **النزاهة:** وهي الحماية من التعديل أو التدمير للمعلومات، وتتضمن أيضًا عدم إنكار المعلومات أو صحتها.

ب- **السرية:** وهي الحفاظ على القيود المصرح بها على الوصول والإفصاح، بما في ذلك وسائل حماية المعلومات الشخصية والمعلومات المهمة.

ت- **التوافر أو الإتاحة:** أي ضمان الوصول إلى المعلومات واستخدامها في الوقت المناسب وبشكل موثوق به.

الأمن السيبراني Cybersecurity:

وفقًا لقاموس "أكسفورد" Oxford Dictionary: هو التدابير المتخذة للحماية من الاستخدام الإجرامي للبيانات الإلكترونية (Oxford Dictionart, n.d.).

وقد عرفه الموقع الرسمي لوزارة الأمن الداخلي الأمريكية "CISA": بأنه فن حماية الشبكات والأجهزة والبيانات من الوصول غير المصرح به أو الاستخدام الإجرامي، وممارسة ضمان سرية المعلومات وسلامتها وتوافرها، بمعنى كل ما هو معتمد على أجهزة الكمبيوتر أو شبكة الإنترنت (CISA,٢٠٢١).

أما الاتحاد الدولي للاتصالات (ITU) فعرفه بأنه: مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمانات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمُستخدم، وتشمل تلك الأصول أجهزة الحاسب المتصلة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات وإجمالي المعلومات المنقولة أو المخزنة في البيئة السيبرانية (Union, n.d.).

وعرفته أيضًا مؤسسة "جارتنر" (Gartner) بأنه: مزيج من الأشخاص والسياسات والعمليات

والتقنيات، التي تستخدمها المؤسسة لحماية أصولها السيبرانية، وأمن تكنولوجيا المعلومات، وأمن إنترنت الأشياء، وأمن المعلومات، وأمن التكنولوجيا التشغيلية (Gartner, n.d.).

وأوضحت شركة "أي بي أم" (IBM) أن الأمن السيبراني يشير إلى تقنية أو إجراء أو ممارسة لمنع الهجمات السيبرانية أو التخفيف من تأثيرها (Lindemulder & Kosinski, 2024).

الأمن السيبراني المجتمعي Community Cybersecurity: (تعريفًا إجرائيًّا)

بناءً على التعريفات السابقة يمكن استخلاص التعريف على النحو التالي: إنه مجموعة التدابير والسياسات لحماية أصول المعلومات في المجتمع من التهديدات السيبرانية المحتملة، وآثار ذلك على المجتمع من أجل حمايته، لتوفير بيئة رقمية آمنة خالية من التهديدات والمخاطر للمحافظة على أمن وسلامة المعلومات داخل المجتمع، ويتم ذلك من خلال برامج التوعية المجتمعية.

التهديدات السيبرانية Cyber threat: (Technology, n.d.)

هي أي حدث أو ظرف يحتمل أن يؤثر سلبًا على العمليات التنظيمية (كالمهمات أو الوظائف أو الصورة أو السمعة) أو يحتمل أن يؤثر أيضًا على الأصول التنظيمية أو الأفراد من خلال نظام معلومات معد لهذا الغرض، إما عن طريق الوصول غير المصرح به أو التدمير أو الكشف أو تعديل المعلومات أو رفض الخدمة، حيث يمكن استخدام إحدى تلك الثغرات الأمنية لتهديد أمن النظام.

التصيد الاحتيالي Phishing: (Technology, n.d.)

أسلوب لمحاولة الحصول على البيانات المهمة، إما من خلال البريد الإلكتروني أو مواقع إلكترونية، حيث يتنكر المهاجم في صورة شركة مشروعة أو شخص حسن السمعة.

أولًا: الإطار المنهجي:

١/١ مشكلة الدراسة وأهميتها:

تمثلت مشكلة الدراسة ومبرراتها في قلة المقررات البينية، التي يتطلبها نظام التعليم الحالي بأقسام المكتبات والمعلومات على مستوى جمهورية مصر العربية، وذلك لما يشهده العالم من تداخلات في مختلف التخصصات، تتطلب معها إدخال مثل هذه المقررات ومن ضمنها مقرر منفصل عن أمن المعلومات أو الأمن السيبراني، مما استدعى معه التعرف على مدى توافر ذلك المقرر داخل أقسام ومدارس المكتبات على المستوى المحلي والإقليمي وعلى مستوى الولايات المتحدة الأمريكية وكندا، للتعرف على كيفية تطبيقه من خلال

التوصيف المقترح.

ولا شك أن من المبررات الرئيسة لموضوع الدراسة، إن معظم طلاب الجامعات في الوقت الحالي يستخدمون مختلف الوسائل التكنولوجية للحصول على المعلومات دون المعرفة بما هي الشروط والواجبات، التي يجب عليهم معرفتها واستخدامها للمحافظة على أمنهم وأمن الأجهزة التي يستخدمونها، ما استوجب معه إعداد بند من ضمن بنود المقرر المقترح يناقش هذه الجوانب الأمنية وكيفية استخدامها وتطبيقها، وهذا ما أكده كل من "روكوارد" و"بيي" (Rukwaro & Bii, 2016) أن هناك اختلافًا كبيرًا بين المناهج التي يجري تدريسها لطلاب أقسام المكتبات والمعلومات حول العالم وبين احتياجات سوق العمل، الأمر الذي يتطلب معه إدخال مقررات حديثة تتماشى ومتطلبات سوق العمل الحالية. ووفقًا للتقرير الصادر عن شركة (IBM) (IBM, 2023) بلغ متوسط التكلفة العالمية لاختراق البيانات عام ٢٠٢٣ (٤,٤٥) ملايين دولار أمريكي، أي بزيادة قدرها (١٥%) على مدى السنوات الثلاث السابقة، وهذا ما يترتب عليه ظهور وسائل وتقنيات يصعب معها التحكم فيها وتعقبها للحفاظ على أمن المعلومات بشكل مستمر.

كما يعد قلة وجود مقرر منفصل عن أمن المعلومات أو الأمن السيبراني داخل أقسام المكتبات بجمهورية مصر العربية، من المبررات الرئيسة أيضًا لهذه الدراسة.

تحاول الدراسة الإجابة عن التساؤلات التالية:

١- ما مدى توافر المعيار الذي أصدرته المنظمة الدولية للتوحيد القياسي (أيزو) (ISO/IEC ٢٧٠٠٢) لأمن المعلومات ومعيار (ISO/IEC٢٧٠٣٢) للأمن السيبراني داخل مقررات أمن المعلومات والأمن السيبراني بأقسام المكتبات بالجامعات محل الدراسة؟

٢- ما مدى تكامل وتناسق توصيفات مقرر أمن المعلومات والأمن السيبراني بأقسام المكتبات محل الدراسة لجميع جوانب الموضوع؟

٣- ما المسميات المختلفة لمقرر أمن المعلومات أو الأمن السيبراني داخل أقسام ومدارس المكتبات محل الدراسة؟

٤- ما المبررات التي تستدعي إدخال مقرر أمن المعلومات أو الأمن السيبراني لأقسام المكتبات بجمهورية مصر العربية وبالوطن العربي؟

٥- ما التصور المقترح لمقرر أمن المعلومات والأمن السيبراني لتدريسه داخل أقسام

المكتبات بجمهورية مصر العربية؟

وتكمن أهمية الدراسة فيما يلي:

تستمد هذه الدراسة أهميتها من ضرورة توعية أقسام المكتبات والمعلومات بجمهورية مصر العربية وبالوطن العربي بأهمية إدخال مقرر لأمن المعلومات والأمن السيبراني لحماية أصولها المادية وحماية مقرراتها الإلكترونية، أو تطوير مقررات أمن المعلومات بمختلف مسمياتها بما يتماشى والتطورات التكنولوجية الحالية، ولتوعية طلابها أيضًا وحمايتهم من مخاطر الهجمات المعلوماتية والسيبرانية، ويأتي ذلك نتيجة لاستخدام جميع طلاب الجامعات تقريبًا لشبكة الإنترنت في كل مهامهم اليومية، ولهذا فإن الاعتماد فقط على التكنولوجيا للحماية من مخاطر الهجمات المعلوماتية والسيبرانية ليس كافيًا. ومن أجل ذلك يجب تعزيز الوعي لدى الطلاب تجاه تلك الهجمات للتصدي لها بفاعلية من خلال مقرر دراسي لتلبية متطلبات العصر الرقمي، فهم المسؤولون في المستقبل عن أمن معلومات تلك المكتبات والمؤسسات التابعة لها، ولا بد أن تكون لديهم الخبرة في هذا المجال.

٢/١ أهداف الدراسة:

١- التعرف على الأقسام العلمية التي تقوم بتدريس مقرر أمن المعلومات أو الأمن السيبراني في صورة مقرر مستقل، أو التي تدخله في جزء من مقرر لديها، ومدى ملاءمته لسوق العمل على المستوى المحلي والإقليمي، وعلى مستوى الولايات المتحدة الأمريكية وكندا.

٢- وصف وتحليل مقررات أمن المعلومات بالجامعات محل الدراسة.

٣- رصد المسميات المختلفة لمقرر أمن المعلومات داخل أقسام المكتبات محل الدراسة.

٤- التعرف على المبررات التي تستدعي إدخال مقرر أمن المعلومات لأقسام المكتبات والمعلومات بجمهورية مصر العربية وبالوطن العربي.

٥- تقديم نموذج توصيف مقترح لمقرر أمن المعلومات قد يكون توصيفًا استرشاديًّا لأقسام المكتبات بالجامعات المصرية، وفقًا لبنود المعيارين اللذين أصدرتهما المنظمة الدولية للتوحيد القياسي (أيزو) معيار(ISO/IEC ٢٧٠٠٢) لأمن المعلومات ومعيار (ISO/IEC٢٧٠٣٢) للأمن السيبراني.

٣/١ حدود الدراسة ومجالها:

تناولت الدراسة دراسة وتحليل مقرر أمن المعلومات والأمن السيبراني بأقسام ومدارس

المكتبات والمعلومات على المستوى المحلي والإقليمي وعلى مستوى الولايات المتحدة الأمريكية وكندا وفقًا للوائح الأقسام على النحو التالي:

أولًا: أقسام المكتبات والمعلومات بجمهورية مصر العربية بالجامعات التابعة للمجلس الأعلى للجامعات.

ثانيًا: أقسام المكتبات والمعلومات على مستوى الوطن العربي وفقًا لوزارة التعليم العالي والبحث العلمي بكل دولة من دول الوطن العربي.

ثالثًا: أقسام ومدارس المكتبات والمعلومات على مستوى الولايات المتحدة الأمريكية وكندا وفقًا لاعتماد تلك البرامج من الجمعية الأمريكية للمكتبات (ALA).

ومراجعة تلك المقررات الـ (٤٩) التي حُصِرَت بما جاء في المعيارين اللذين أصدرتهما المنظمة الدولية للتوحيد القياسي (أيزو) معيار (ISO/IEC ٢٧٠٠٢) لأمن المعلومات ومعيار (ISO/IEC ٢٧٠٣٢) للأمن السيبراني، للتعرف على مدى تحقيقهما للبنود الواردة فيه للحصول على محتوى مقرر متكامل الأركان، حيث تمت مرحلة تحليل تلك المقررات من خلال قائمة المراجعة المعدة مسبقًا لهذا الغرض، وذلك في الفترة من ٢٠٢٤/١٠/٢٠ وحتى ٢٠٢٤/١٢/١.

٤/١ منهج الدراسة وأدواته:

اعتمدت الدراسة على المنهج المسحي لحصر ووصف مقررات أمن المعلومات أو الأمن السيبراني بأقسام ومدارس المكتبات والمعلومات على المستوى المحلي والعربي وعلى مستوى الولايات المتحدة الأمريكية وكندا، للتعرُّف على ماهية تدريس ذلك المقرر والمسمى الذي يندرج تحته.

وقد استُخدِم أسلوب تحليل المحتوى Content Analysis لدراسة وتحليل توصيفات تلك المقررات لدراسة مدى توافقها للتطبيق داخل أقسام المكتبات في جمهورية مصر العربية، وتحقيقها لبنود معيارَي المنظمة الدولية للتوحيد القياسي (أيزو)؛ معيار (ISO/IEC ٢٧٠٠٢) لأمن المعلومات ومعيار (ISO/IEC٢٧٠٣٢) للأمن السيبراني.

١/٤/١ أدوات جمع البيانات:

تمثلت في قائمة المراجعة المعدة من قِبل الباحثة، والتي جرى من خلالها تحليل المقررات الدراسية المرتبطة بموضوع البحث بأقسام المكتبات والمعلومات بالجامعات المصرية التابعة لوزارة التعليم العالي والبحث العلمي وأقسام المكتبات والمعلومات بالوطن

العربي التابعة أيضًا لوزارات التعليم العالي والبحث العلمي، وأيضًا على أقسام ومدارس المكتبات والمعلومات المعتمدة من جمعية المكتبات الأمريكية (ALA) بالولايات المتحدة الأمريكية وكندا.

وقد جُمِّعَ محتوى العناصر الواردة في قائمة المراجعة من خلال الاعتماد على نموذج التوصيف الصادر عن الهيئة القومية لضمان جودة التعليم والاعتماد، حيث قُسمت قائمة المراجعة إلى تسعة محاور، تناولت جميع جوانب المقرر الدراسي على النحو التالي (بيانات أساسية عن المقرر، أهداف المقرر، محتوى المقرر، أساليب التعليم المتبعة، أساليب التقويم، المصادر التي جُمِّعَ المقرر من خلالها، الساعات التدريسية للمقرر، مخرجات التعلم، نواحي القصور التي من الممكن أن تؤثر على جودة المقرر)، وقد حُكِّمَت قائمة المراجعة من قبل مجموعة من أساتذة المكتبات*.

٢/٤/١ مجتمع الدراسة:

وفقًا لعملية الحصر التي قامت بها الباحثة ينقسم مجتمع الدراسة إلى ثلاثة مستويات:

أولًا: على مستوى جمهورية مصر العربية: حصرت الباحثة من خلال الرجوع لموقع وزارة التعليم العالي والبحث العلمي بالدولة عدد (٥) أقسام علمية بالجامعات تابعة لها تقوم بتدريس مقرر عن أمن المعلومات أو الأمن السيبراني باختلاف مسمياتها من أصل (١٩) قسمًا علميًّا.

ثانيًا: على مستوى الوطن العربي: حصرت الباحثة من خلال الرجوع لموقع وزارة التعليم العالي والبحث العلمي بكل دولة عدد (٨) أقسام علمية بالجامعات تابعة لها، تقوم بتدريس مقرر أمن المعلومات أو الأمن السيبراني باختلاف مسمياتها من أصل (٣٢) قسمًا علميًّا.

ثالثًا: على مستوى الولايات المتحدة الأمريكية وكندا: حصرت الباحثة عدد (١٧) جامعة معتمدة من جمعية المكتبات الأمريكية (ALA) تقدم مقررات خاصة بأمن المعلومات أو بالأمن السيبراني، من أصل (١٠٠) جامعة اطلِع عليها. (Association, 2015).

(*) السادة محكمي قائمة المراجعة:

أ.د. أحمد فرج أحمد: أستاذ المكتبات والمعلومات بكلية الآداب – جامعة الفيوم.

أ.د. أماني محمد السيد: أستاذ المكتبات والمعلومات بكلية الآداب – جامعة حلوان.

أ.د. إيناس حسين صادق: أستاذ المكتبات والمعلومات بكلية الآداب – جامعة حلوان.

أ.م.د. تغريد أبو الحسن راضي: أستاذ المكتبات والمعلومات المساعد بكلية الآداب – جامعة حلوان.

وقد تنوعت تلك المقررات الدراسية بين مقررات للتعليم الجامعي الأساسي ومقررات للدراسات العليا، وتراوحت تلك المقررات بين المقررات الإجبارية والاختيارية، وقد استطاعت الباحثة الحصول على توصيفات مقررات أقسام المكتبات بجمهورية مصر العربية أو الدول العربية، إما من خلال مواقع الأقسام على شبكة الإنترنت وفقًا للائحة المتاحة على موقع القسم العلمي، أو من خلال الاتصالات الشخصية مع بعض الأساتذة داخل تلك الأقسام العلمية في حالة تعذر الحصول عليها من الموقع، بينما مقررات الأقسام الأوروبية اكتفت فيها الباحثة بالتوصيفات المتاحة على مواقع الأقسام على شبكة الإنترنت لتعذر التواصل مع مسؤولين من الداخل، ليصبح إجمالي المقررات الدراسية (٤٩) مقررًا دراسيًّا جرى تحليلها.

ويوضح الجدول رقم (١) مجتمع الدراسة مقسمين وفقًا للترتيب السابق:

جدول رقم (١)

يوضح الأقسام العلمية محل الدراسة التي تشتمل على مقرر عن أمن المعلومات أو الأمن السيبراني

م	الجامعة	مسمى المقرر	المرحلة الجامعية	الموقع الإلكتروني	عدد الساعات (نظري)	عدد الساعات (عملي)	نوع المقرر (اجباري / اختياري)
الجامعات بجمهورية مصر العربية							
١	جامعة القاهرة	أمن المعلومات	ماجستير (تخصص تقنية المعلومات) (لائحة جديدة)	https://2cm.es/RnKk	٣	–	اختياري
٢	جامعة سوهاج	أمن المعلومات وضبط جودتها	الليسانس (الفرقة المستوى الرابع – الفصل الدراسي الأول (لائحة جديدة)	https://2cm.es/OTvK	٢	–	إجباري
٣	جامعة طنطا	أمن المعلومات	البرنامج المميز تقنية المعلومات (المستوى الثاني – الفصل الدراسي الثاني)	https://2cm.es/RnK9	٢	١	إجباري
٤	جامعة الفيوم	١–أمن وسلامة المعلومات	الليسانس (الفرقة الرابعة – المستوى السابع) (لائحة جديدة)	https://2cm.es/RnJk	٢	–	اختياري
		٢– أمن وحرية المعلومات	الليسانس (الفرقة الرابعة – المستوى الثامن) (لائحة جديدة)	https://2cm.es/RnJk	٢	–	اختياري
٥	جامعة بني سويف	١– أمن وحماية المعلومات	الليسانس (برنامج بمصروفات – المستوى السابع) (لائحة جديدة)	https://2cm.es/OTuX			إجباري

		٢- الجرائم المعلوماتية والأمن القومي	الدكتوراه (شعبة علوم المعلومات – الفصل الدراسي الأول)	https://2cm.es/OTuX	٣	–	إجباري
الجامعات العربية							
١	جامعة الأميرة نورة بنت عبد الرحمن (السعودية)	أمن المعلومات واستخداماتها	بكالوريوس – قسم المكتبات والمعلومات (المستوى السادس)	https://2cm.es/RnEC	٣	–	إجباري
٢	جامعة الملك سعود (السعودية)	مبادئ أمن المعلومات وتطبيقاتها	بكالوريوس – كلية العلوم الإنسانية والاجتماعية – قسم علم المعلومات – للفرقة الرابعة داخل كلٍّ من (مسار إدارة المعلومات وخدماتها، مسار إدارة السجلات والحفظ الرقمي)	https://2cm.es/RnyK	٣	–	إجباري
٣	جامعة الإمام عبد الرحمن بن فيصل (السعودية)	أمن وسلامة المعلومات	برنامج بكالوريوس علم المعلومات – قسم علم المعلومات – كلية الآداب (الفرقة الرابعة – الفصل الدراسي الثاني) – بالدمام	https://2cm.es/Rnyo	٢	–	إجباري
٤	جامعة طيبة (السعودية)	أمن المعلومات	بكالوريوس – قسم المعلومات ومصادر التعلم – برنامج علم المعلومات (المستوى الرابع)	https://2cm.es/OTmJ	٣	–	إجباري
٥	جامعة الحسين بن طلال (الأردن)	١- مقدمة في أمن المعلومات والشبكات	بكالوريوس – قسم علم المكتبات/ تكنولوجيا المعلومات	https://2cm.es/OTml	٣	–	اختياري
		٢- أمن المعلومات والسجلات	ماجستير – قسم علم المكتبات – تخصص إدارة المعلومات والأرشفة الرقمية	https://2cm.es/OTml	٣	–	اختياري
٦	جامعة الزرقاء (الأردن)	أمن المعلومات	بكالوريوس – كلية العلوم التربوية – برنامج تكنولوجيا المكتبات والمعلومات	https://2cm.es/OTn1	٣	–	اختياري
٧	جامعة الأقصى (فلسطين)	الفضاء الإلكتروني وأمن المعلومات	بكالوريوس – قسم علوم المكتبات (المستوى الثالث)	https://2cm.es/OTmy	٢	–	اختياري
٨	جامعة السلطان قابوس (عُمان)	أساسيات أمن المعلومات	بكالوريوس – قسم دراسات المعلومات – كلية الآداب والعلوم الاجتماعية (الفصل الثامن)	https://2cm.es/OTmW	٣	–	إجباري

الجامعات الأجنبية المعتمدة من جمعية المكتبات الأمريكية (ALA) بالولايات المتحدة الأمريكية وكندا							
اختياري	–	3	https://2cm.es/OTn7	Master of Library and Information Science	1-Introduction to Information Security.	Dominican University College of Applied Social Science (Information Studies Department)	١
اختياري	–	3	https://2cm.es/OTn7		2-Organizational Information Security.		
اختياري	–	3	https://2cm.es/OTn7		3-Information Privacy.		
اختياري	–	3	https://2cm.es/OTn7		4-Cybersecurity Governance.		
اختياري	–	٣	https://2cm.es/OTnk	Master of Science in Information Studies (MSIS)	Strategic Communication for Information Security & Privacy	The University of Texas at Austin (School of Information)	٢
اختياري	–	٣	https://2cm.es/RnBA	Master of Science in Information Security and Privacy	1-Introduction to Information Security and Privacy	The University of Texas at Austin (School of Information and Center for Identity)	3
اختياري	-	3	https://2cm.es/RnBA		2-Information Security & Privacy in Society.		
اختياري	-	3	https://2cm.es/RnBA		3-Public Policy, Information Security, and Privacy.		
اختياري	-	3	https://2cm.es/RnBA		4-Business Governance and Controls for Information Security and Privacy.		
اختياري	-	3	https://2cm.es/RnBA		5-Strategic Communication for Information Security & Privacy.		
اختياري	-	3	https://2cm.es/RnBA		6-Information Security.		
اختياري	–	٣	https://2cm.es/OTnF	Master of Science with majors in Library Science or Information Science	1-Information and Cyber Security	University of North Texas (Department of Information Science)	٤
اختياري	–	٣	https://2cm.es/OTnF	(MS-IS with Concentration in Health Librarianship)	2-Information Security and Cyber security		
اختياري	-	٣	https://2cm.es/RnBR	Special bachelor's Program	1-Cybersecurity and Information Assurance (Information Security)	Rutgers University (School of Communication and Information)	5
اختياري	-	3	https://2cm.es/OTnW	Master of Information	2-Information Security Management		

اختياري	-	3	https://2cm.es/OTo7	Master of Science in Information (MSI)	Information Systems Field (Principles of Cybersecurity)	Drexel University (College of Computing and Informatics)	6
إجباري	-	١	https://2cm.es/RnCy	Master of Science in Informatics (specific field: Cybersecurity & Privacy)	1-Information Security: Overview.	San Jose State University (School of Information)	7
إجباري	-	1	https://2cm.es/RnCy		2-Information Security: Information Assurance.		
إجباري	-	3	https://2cm.es/OTox	Master of Science in Information (MSI)	Organizational Information Security	Florida State University (School of Information - College of Communication & Information)	8
اختياري	-	٣	https://2cm.es/RnCQ	Master of Science in Information Studies (MSIS)	1-Cyber Intelligence	University of South Florida (College of Arts and Sciences - School of Information)	9
اختياري	-	3	https://2cm.es/RnCQ		2-Advanced Cyber Intelligence		
إجباري	–	٢	https://2cm.es/OToR	Master in Knowledge, Information and Data Science	1- Information Governance	University College London (Faculty of Arts and Humanities)	١٠
اختياري	–	٢	https://2cm.es/OToR	Master in Archives and Records Management	2- Information Governance		
إجباري	-	3	https://2cm.es/RnDa	Master of Science in Library and Information Science in (Information Security Management)	1- Introduction to Information Security	Syracuse University (School of Information Studies)	١١
اختياري	-	3	https://2cm.es/RnDa	Master Certificate in Information) Security (Management	2-Information Technology Security Architecture		
اختياري	-	3	https://2cm.es/RnDa	Master in (Information Security (Management	3-Information Security Policy		
اختياري	-	3	https://2cm.es/RnDa	Master Certificate in (Information Security	4-Leading Issues in Information Security		

				(Management			
اختياري	–	٣	https://2cm.es/OTpj	Master in library and information science: Information Technology	1-Survey of Information Security	University of Wisconsin - Milwaukee	12
اختياري	-	3	https://2cm.es/OTpj		2-Information Security Management		
اختياري	-	٣	https://2cm.es/OTpv	Master of Library and Information Studies	Human Factors in information Security	University of Wisconsin -Madison	13
اختياري	-	٣	https://2cm.es/OTpA	Master of Library and Information Science (MLIS)	Intelligence & Analytics	University of Maryland (College of Information)	١٤
اختياري	–	٣	https://2cm.es/OTpG	Master of Library and Information Studies	Technology for Information Studies (Cybersecurity Essentials)	University of Oklahoma (School of Library and Information Studies)	١٥
اختياري	–	٣	https://2cm.es/OTpO	Master of Science in Data Science and Informatics (Data Science/Data Analytics)	Foundations of Information Systems Security	Texas Woman's University (School of Library and Information Studies)	١٦
اختياري	–	٣	https://2cm.es/RnE0	Graduate Certificate in Information Architecture	Information Security	McGill University -Quebec (Information Studies (Faculty of Arts)	١٧

صعوبات الدراسة:

من الصعوبات التي واجهت الباحثة خلال عملية حصر توصيفات مقرر أمن المعلومات على مستوى الوطن العربي أو على مستوى جمهورية مصر العربية، صعوبة الحصول على التوصيف الكامل من خلال موقع القسم العلمي، وهذا ما استوجب معه التواصل بشكل مباشر مع الأساتذة القائمين على تدريس المقرر الدراسي لاستيفاء محاور قائمة المراجعة من خلاله، حتى يتسنى الحصول على نتائج كاملة للخروج بتحليل متوازن النتائج على مستوى مجتمع الدراسة، وهذه الأقسام هي (قسم المكتبات والمعلومات– جامعة سوهاج)، (قسم علوم المعلومات – جامعة الفيوم)، (قسم علوم المعلومات – جامعة بني سويف).

١/٥ الدراسات السابقة:

قامت الباحثة بالبحث في العديد من قواعد البيانات المتخصصة والمتعلقة بموضوع الدراسة المتاحة من خلال بنك المعرفة المصري (EKB)، وموقع المكتبة الرقمية السعودية، وبالدخول على إحدى الشبكات الاجتماعية الأكاديمية مثل (ResearchGate)، بالإضافة إلى البحث في العديد من محركات البحث العامة بغرض الإلمام وفهم الجانب المحدد لموضوع أمن المعلومات والأمن السيبراني، وبما يتفق مع أهداف موضوع الدراسة، وذلك عن طريق الدراسات المتعلقة فقط بإدخال مقرر أمن المعلومات أو الأمن السيبراني إلى أقسام ومدارس المكتبات، وأيضًا الدراسات المتعلقة بمدى وعي طلبة الجامعات لموضوع الدراسة، بالإضافة إلى الدراسات المتعلقة بدور المكتبات الجامعية لنشر هذا الوعي بين المجتمع الأكاديمي، وقد رُتبَت هذه الدراسات ترتيبًا زمنيًّا من الأحدث إلى الأقدم، حيث بُحِثَ بالكلمات التالية:

- أمن المعلومات في التعليم (Information security in education).
- أمن المعلومات في الجامعات (Information Security in Universities).
- تأثير أمن المعلومات على المكتبات (The Impact of Information Security on Libraries).
- ممارسات أمن المعلومات داخل المكتبات (Information Security Practices in Libraries).
- مفاهيم الأمن السيبراني (Cybersecurity Concepts).
- أنواع التهديدات السيبرانية في المكتبات (Types of Cyber Threats in Libraries).
- مبادرات الأمن السيبراني في الجامعات (Cybersecurity Initiatives in Universities).

١/٥/١ الدراسات العربية:

هدفت دراسة كل من (العكيلي و البياتي، ٢٠١٧) إلى التعرف على أهمية أمن المعلومات لدى طلاب أقسام المكتبات والمعلومات في الجامعات العراقية، ومدى علاقة ذلك الوعي الطلابي بالمقررات الدراسية، حيث اعتمدت الدراسة على المنهج المسحي لجمع بيانات الدراسة وتحليلها، وقد خلصت الدراسة إلى مجموعة من النتائج أهمها: هناك وعي

لدى الطلاب بأهمية حماية المعلومات وما هي المعلومات الواجب حمايتها، غير أن مقرر الحوسبة وفروعه، والذي يدرس داخل أقسام المكتبات والمعلومات، افتقر إلى التغطية الجيدة لموضوع أمن المعلومات وتطبيقاته، فضلًا عن معرفة متوسطة لدى الطلاب بناءً على خبراتهم الشخصية حول تجريب وسائل حماية المعلومات، بينما كانت أبرز توصيات الدراسة ضرورة وجود مقرر دراسي خاص بأمن المعلومات وتطبيقاته، وانتهت الدراسة باقتراح توصيف لمقرر أمن المعلومات.

٢/٥/١ الدراسات الأجنبية:

أوضح كل من "إجبينوفيا" و"إيشولا" (Igbinovia & Ishola, 2023) أن التوسع التكنولوجي في المكتبات الجامعية أدى إلى ازدياد ظهور الجرائم الإلكترونية، وهذا ما استوجب ضرورة تزويد موظفي المكتبات الجامعية بالمعرفة المطلوبة لمكافحة هذا التهديد، ومن ثمَّ هدفت الدراسة إلى إلقاء الضوء على أثر تعليم الأمن السيبراني "Cyber Security" في تدريس علم المكتبات والمعلومات، حيث قامت الدراسة باستخدام المنهج الوصفي التحليلي اعتمادًا على الاستبيان والمقابلة الشخصية بوصفها أدوات لجمع بيانات الدراسة، حيث جرى توزيع عدد ١٣٤ استبانة على موظفي المكتبات الجامعية، بينما جرت المقابلة مع عدد ٦ رؤساء مدارس للمكتبات بدولة نيجيريا، وقد خلصت الدراسة إلى أن المعرفة لدى اختصاصي المكتبات الجامعية بدولة نيجيريا عن الأمن السيبراني ومخاطره منخفضة إلى حدٍّ ما، لكنهم يمتلكون المعرفة الأساسية عنه على الرغم من عدم تعليمهم ذلك العلم بمدارس المكتبات لديهم، وقد أدت هذه المعرفة المنخفضة إلى تعرض تلك المكتبات للعديد من التهديدات السيبرانية، غير أنهم أظهروا مستوى عاليًا من الالتزام بأخلاقيات استخدام الإنترنت والرغبة في تعلم المزيد عن ذلك العلم، وقد جرى الكشف في هذه الدراسة عن توجه إدارة المكتبات الجامعية تجاه قضايا الأمن السيبراني، والعمل على نشرها في المكتبات الجامعية، بينما أظهرت نتيجة المقابلة الشخصية مع رؤساء مدارس المكتبات أن غالبية مدارس المكتبات لا تقدم دورات عن الأمن السيبراني بسبب ندرة القوى العاملة الماهرة لديها، وقد أوصت الدراسة بضرورة نشر هذا العلم بين المكتبات الجامعية من أجل استدامتها بوصفها مؤسسة معلومات بهدف تقديم خدمات عالية الجودة للمستفيدين منها.

هدفت دراسة كل من "دونماد" و"تيلا" (Dunmade & Tella, 2023) إلى استكشاف دور المكتبات وأمناء المكتبات في تعزيز السلوك الأخلاقي السيبراني بين طلاب الدراسات العليا بدولة نيجيريا لضمان سلامة وأمن هؤلاء الطلاب، وقد بحثت الدراسة في التحديات

التي يواجهها أمناء المكتبات في نشر أخلاقيات استخدام شبكة الإنترنت، وسلطت الدراسة أيضًا الضوء على الاستراتيجيات التي يمكن للمكتبات اعتمادها لتعزيز السلوك المسؤول من خلال شبكة الإنترنت، حيث توصلت الدراسة إلى نقص الوعي بمخاطر الأمن السيبراني بين طلاب الدراسات العليا، وكذلك الحاجة إلى تدريب أمناء المكتبات على كيفية تعزيز السلوك الأخلاقي السيبراني وتوفير المواد التدريبية لذلك؛ من أجل نشر السلوك الأخلاقي السيبراني بين طلاب الدراسات العليا.

وأوضح كل من "جو" و"تينماز" (Guo & Tinmaz, 2023) من خلال الدراسة التي قاما بها على ثماني جامعات عامة محلية بالصين بواقع ١٧١٠ طلاب، لمعرفة مدى الوعي لديهم بالوصف والتحليل حول الهجمات السيبرانية وكيفية تفاديها، أن ما يقرب من ٥٠% من الطلاب يقضون أكثر من أربع ساعات على شبكة الإنترنت، وقد تفوقت الطالبات على الطلاب في الوقت المخصص للإنترنت، باستخدام الهواتف المحمولة كأكثر الوسائل انتشارًا بين الطلاب، لكن الدراسة أظهرت ضعفًا شديدًا لدى جميع الطلاب الذين شملتهم الدراسة في إدارة كلمة المرور الخاصة بهم في مختلف التطبيقات، لكن الطلاب الذكور تفوقوا على الطالبات بمستوى وعي مرتفع حول الهجمات السيبرانية وكيفية الحماية منها. وقد أوضحت الدراسة أيضًا أن فرق التخصصات لا يحدث فرقًا في مستوى الوعي بالأمن السيبراني والقوانين المرتبطة به، لكنه يُحدث فرقًا في الطريقة المراد بها تدريس مقرر للأمن السيبراني، فالطلاب المتخصصون في المجالات المتعلقة بالكمبيوتر يفضلون دراسة أكثر تعمقًا مع مزيد من التدريبات العملية، بينما الطلاب ذوو التخصصات النظرية يفضلون الدراسة عن طريق الإعلانات أو الدعاية دون الانخراط في الجوانب التقنية، وقد أوصت الدراسة بضرورة الحاجة إلى أساليب تعليمية شاملة تشمل جميع جوانب الأمن السيبراني، مع ضرورة قيام المؤسسات بالتفكير في تصميم استراتيجيات تعليمية تلبي احتياجات الطلاب في التخصصات الأكاديمية المختلفة.

وهذا ما أكده الحربي والصديق (Alharbi & Tassaddiq, 2021) من ضرورة التوعية بأهمية الأمن السيبراني بين طلاب الجامعات، من خلال الدراسة التي قاما بها على طلاب جامعة المجمعة بالمملكة العربية السعودية، مستخدمين المنهج الكمي لتجميع تلك البيانات، والتي أظهرت أن أغلب المشاركين في الدراسة لم تكن لديهم معرفة بالمفاهيم الأساسية للأمن السيبراني أو معرفة بأفضل الممارسات حول كيفية الحفاظ على الأجهزة التي يمتلكونها من تلك الهجمات، سواء كانت تصيدًا احتياليًّا أو برامج وفيروسات ضارة، وقد خلصت الدراسة

إلى ضرورة تضمين الجامعة برنامجًا للتوعية والتدريب عن الأمن السيبراني للطلاب بشكل دوري.

وقد أشار كل من "ويافي" و"ياكوماه" و"كيسي" (Wiafe, Yaokumah & Kissi, 2020) إلى أن القرارات الأخلاقية السيبرانية لها عواقب أخلاقية وقانونية واجتماعية بالغة الخطورة على الأفراد والمنظمات والمجتمعات ككل، حيث أجريت الدراسة على مجموعة من الطلاب بشأن التعرف على النوايا السيبرانية غير الأخلاقية لديهم، وأظهرت الدراسة أن (٢٤%) لديهم النية للانخراط في القرصنة الإلكترونية، وحوالي (١٣%) لديهم النية لانتهاك خصوصية الآخرين، كما أن ما يقرب من (٣٠%) من المشاركين لديهم النية لارتكاب قرصنة البرمجيات، بينما أبدى (١٨,٦%) رغبتهم في المشاركة في أنشطة القرصنة، الأمر الذي يترتب علية ضرورة توافر مبادئ توجيهية قانونية بالمكتبات لتوجيه الطلاب وإرشادهم إلى المسار الأخلاقي السليم، ففي حالة عدم وجود تلك المبادئ بشكل واضح للطلاب، قد يعوق ذلك المكتبات من القدرة على معالجة قضايا الأخلاقيات السيبرانية بشكل فعال، حيث يعتبر توفير برامج تثقيفية للعاملين بالمكتبة ومستخدميها من الطلاب التحدي الحقيقي للمكتبات.

أما كل من "مونياندي" و"سامسودين" و"مونياندي" (Muniandy, Samsudin & Muniandy, 2017)، فأوضحوا في الدراسة التي قاموا بها عن سلوك الأمن السيبراني بين طلاب التعليم العالي في دولة ماليزيا أن الطلاب الذين شملتهم الدراسة يفتقرون إلى أفضل الممارسات التي من شأنها أن تحميهم من مخاطر الهجمات السيبرانية التي تمثلت بعضها في (التصيد الاحتيالي، كلمة مرور آمنة، البرامج الضارة)، حيث أظهرت الدراسة أن سلوك الطلاب غير مرضٍ، ولذلك أوصت بضرورة التوعية في أوساط التعليم العالي حول مدى أهمية الأمن السيبراني، وأفضل الممارسات التي تساعد في ذلك.

من خلال العرض السابق للدراسات السابقة تبين أن أغلب الدراسات أشارت إلى أهمية إدخال مقرر لأمن المعلومات أو الأمن السيبراني إما من خلال أقسام المكتبات والمعلومات بالكليات كمقرر دراسي أو من خلال المكتبات الجامعية كدورات تدريبية للتوعية بمجال أمن المعلومات والأمن السيبراني.

وقد لاحظت الباحثة ندرة الدراسات باللغة العربية عن إدخال مقرر عن أمن المعلومات أو الأمن السيبراني داخل أقسام المكتبات والمعلومات بالجامعات، فلم تجد الباحثة سوى دراسة واحدة تتحدث عن إدخال أمن المعلومات باعتباره مقررًا دراسيًا وتأثير

ذلك على وعي الطلاب بأقسام المكتبات بالجامعات العراقية، وهذا من الأسباب التي أدت إلى توجه الباحثة لإبراز أهمية تدريس هذا المقرر بأقسام المكتبات والمعلومات بجمهورية مصر العربية، نظرًا لما يشهده العالم من تطور تكنولوجي يجري بشكل لحظي يستوجب معه التوعية المستمرة للطلاب لجعلهم قادرين على مواجهة تلك التحديات.

وقد اتفقت أغلب الدراسات على افتقار الطلاب الذين شملتهم الدراسات السابقة إلى الوعي بمجال أمن المعلومات والأمن السيبراني ومدى المخاطر المترتبة على تلك المخاطر. وأغلب تلك الدراسات أيضًا قد اعتمدت على استخدام المنهج الوصفي التحليلي والمنهج المسحي للكشف عن المتطلبات والتحديات التي من الممكن أن تواجه أقسام المكتبات أو المكتبات عند تقديم موضوع أمن المعلومات أو الأمن السيبراني باعتباره مقررًا دراسيًّا أو دورة تدريبية للتوعية.

والفرق بين دراسة الباحثة والدراسات السابقة في ذلك المجال، أن الباحثة حاولت قدر المستطاع تجميع كل ما يتعلق بأمن المعلومات والأمن السيبراني داخل مقرر دراسي مكتمل الجوانب نظريًّا وعمليًّا، معتمدًا في إعداده على المعيار الذي أصدرته المنظمة الدولية للتوحيد القياسي (أيزو) (ISO/IEC ٢٧٠٠٢) لأمن المعلومات ومعيار (ISO/IEC ٢٧٠٣٢) للأمن السيبراني، سبيلًا لتحقيق المعيارية في التطبيق.

ثانيًا: الإطار النظري:

١/٢ مقدمة:

لقد جذبت التكنولوجيا الحديثة عددًا كبيرًا من التأثيرات الإيجابية للمجتمع التعليمي، منها تحسين الوصول إلى المعلومات، وتعزيز إنتاجية الطلاب، وتعد وسيلة لتقديم الدعم القائم على التكنولوجيا، غير أن تلك التكنولوجيا قد جلبت مجموعة من التحديات؛ فبجانب الإمكانات التكنولوجية التي توفرها للطلاب ظهر لها بعض العيوب التي يجب الانتباه لها ووضعها في عين الاعتبار؛ للمحافظة على أمن وسلامة المعلومات التي يتداولها الطلاب إذا استخدمت بشكل غير مناسب، سواء كان هذا الاستخدام بطريقة مقصودة أو غير مقصودة، ولذلك يجب تحسين معرفة ووعي الطلاب بمفاهيم أمن المعلومات والأخلاقيات السيبرانية والسلامة السيبرانية، والأمن السيبراني، لتوفير الوسائل المناسبة لهم لحمايتهم، الأمر الذي يترتب عليه ترسيخ فكر أمن وسلامة المعلومات لدى الطلاب.

إن رفع الوعي بأمن المعلومات والأمن السيبراني بين طلاب الجامعات يعتبر أمرًا بالغ الأهمية أكثر من أي وقت مضى، إذ بات الطلاب هدفًا لهذه الهجمات بشكل مرتفع نظرًا

لمقدار الوقت الذي يقضيه الطلاب على شبكة الإنترنت سواء من أجل البحث على شبكة الإنترنت لأغراض تعليمية، أو من أجل التواصل مع أساتذتهم أو زملائهم. إذًا رفع الوعي بالأمن السيبراني بين الطلاب يعد أمانًا لحاضرنا ومستقبلنا.

ومع التقدم السريع في تكنولوجيا المعلومات والاعتماد بصورة كبيرة على شبكات المعلومات، أصبح الأفراد يعتمدون بشكل كبير على شبكة الإنترنت في مختلف جوانب الحياه اليومية، منها التعليم والخدمات العامة والتفاعلات الاجتماعية والترفيه، فوفقًا للتقرير الصادر عن موقع tatistaS (tsta,Sta٢٠٢٤) للتحليلات، وُجِدَ أن عدد مستخدمي شبكة الإنترنت على مستوى العالم وصل اعتبارًا من أبريل ٢٠٢٤ إلى (٥,٤٤) مليارات مستخدم في جميع أنحاء العالم، وهذ ما يمثل (٦٧,١) من سكان العالم، منهم (٥,٠٧) مليارات بما يعادل نسبة (٦٦,٦%) من سكان العالم مستخدمين لشبكات التواصل الاجتماعي، أيا أن حوالي (٩٤%) من مستخدمي الإنترنت يمتلكون حسابات للتواصل الاجتماعي؛ ما يجعلهم عرضة للهجمات السيبرانية سواء بشكل مباشر أو غير مباشر، الأمر الذي يتطلب معه ضرورة التوعية، ووفقًا للتقرير الصادر عن مركز موارد سرقة الهوية بالولايات المتحدة الأمريكية(the Identity Theft Resource Center (ITRC)، (ITRC, 2024)، سُجِّلَ (٢,٣٦٥) اختراقًا للبيانات عام ٢٠٢٣، بلغ عدد ضحاياها (٣٤٣,٣٣٨,٩٦٤) شخصًا، حيث شهد عام ٢٠٢٣ زيادة في نسبة اختراقات البيانات بنسبة (٧٢%) منذ عام ٢٠٢١، كما تعرضت (١٧٢) مؤسسة تعليمية لاختراقات غير مشروعة على بياناتهم، بينما قلَّ عدد ضحايا تلك الاختراقات من الأشخاص بنسبة (١٦%) منذ عام ٢٠٢٢ نتيجة لانتشار الوعي بالأمن السيبراني.

وقد أوصت مبادرة أمن الشبكات العلمية (SNSI, 2022) بإنشاء حملة لتحسين الوعي بأمن المعلومات بين كل منتسبي الجامعات، سواء من أعضاء هيئة تدريس وموظفين وطلاب، يكون مركزها المكتبة المركزية بالجامعات، باعتبارها مركزًا للتعلم داخل الحرم الجامعي، وذلك عن طريق الدورات وورش العمل، وكذلك إنشاء حملة لتطوير الممارسات الأمنية بشكل مدروس من قِبلها داخل الجامعات عن طريق تقديم الاستشارات المتعلقة بالأمن والخصوصية بشكل مباشر وسريع لكل منتسبيها، مع توفيرها دائمًا نسخًا احتياطية لكل ما تقتنيه تحسبًا لأي مستجدات قد تطرأ عليها، ويمكنها أيضًا عمل شراكات مع كليات الجامعة للمساعدة على إنجاح هذه الحملات التوعوية.

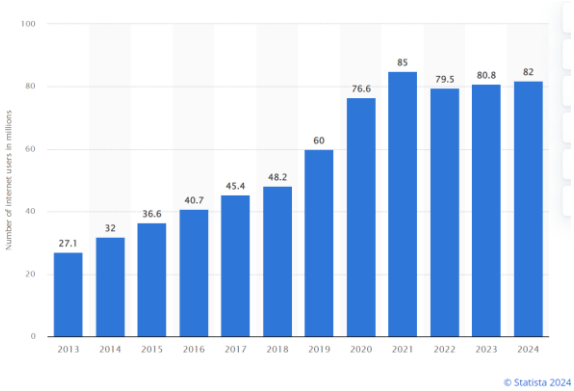
وقد أشار "جانك" و"تشو" و"كوينج" (Jank, Chu & Koenig, 2013) إلى عملية الدمج

التي تتم بين علم المكتبات والعلوم الأخرى، مثل الدمج في التعليم والاتصالات في الولايات المتحدة الأمريكية، والإدارة والأعمال في الصين الذي أخذ في الارتفاع سواء في المرحلة الجامعية أو في مرحلة الدراسات العليا، وهذا ما يشير إلى أن تعليم علم المكتبات والمعلومات مستمر في التغيُّر بداية من القرن الحادي والعشرين.

وأكد كل من "إدزرك" و"تانيان" و"جاكبسون" و"بيكر" و"راي" و"دا سيلفا" (Idziorek, Tannian & Jacobson, 2011)؛(Peker, Ray & da Silva, 2018)، ضرورة تعليم الأمن السيبراني لجميع الطلاب تقنيين أو غير تقنيين، وذلك لاستمرار زيادة حجم الهجمات السيبرانية، وزيادة اعتماد معظم الطلاب على الأجهزة التكنولوجية لتلبية احتياجاتهم التعليمية، ما جعل أغلب هؤلاء الطلاب عرضة لهذه الهجمات، فتعليم الطلاب غير التقنيين يسد فجوة هائلة في تعليم الأمن السيبراني، حيث تركز الدراسة على تعليم الطلاب بشكل عملي من خلال الأنشطة والعروض التقديمية حول كيفية حماية أنفسهم وأجهزتهم على مدار اليوم دون التعمق في الجوانب التقنية الدقيقة التي يدرسها الطلاب التقنيون، حيث يعد تعليم الطلاب في الجامعات والمدارس خطوة مهمة لمكافحة المشكلة المجتمعية المتمثلة في تعليم جميع مستخدمي تكنولوجيا المعلومات حول أمن الأجهزة الخاصة بهم.

ومن المتوقع وفقًا للتقرير الصادر عن (Statista,٢٠٢٣) (Statista) أن تستمر إيرادات الأمن السيبراني في جميع أنحاء العالم، والتي بلغت (١٦٦,٢) مليار دولار أمريكي في عام ٢٠٢٣، لتأخذ في النمو بمعدل مرتفع لتصل إلى (٢٧٣,٥) مليار دولار أمريكي بحلول عام ٢٠٢٨. لقد أصبح انتشار الأمن السيبراني في الدول المتقدمة أمرًا معقدًا بشكل مستمر، حيث من المتوقع أن يُربَط (٢٦) مليار جهاز بإنترنت الأشياء على مستوى العالم بحلول عام ٢٠٣٠، ومن المتوقع أيضًا أن ينمو الأمن السيبراني في الدول النامية نتيجة انتشار الأجهزة المرتبطة بإنترنت الأشياء أيضًا.

ووفقًا للبيانات الصادرة عن منصة (Statista) لعام ٢٠٢٤، قد وصل عدد مستخدمي شبكة الإنترنت إلى ما يقرب من (٨٢) مليون مستخدم في يناير ٢٠٢٤، مقارنة بعدد (٨١) مليون مستخدم العام الماضي، أي أن العدد يتزايد سنويًّا، مقارنة بعام ٢٠١٣ الذي وصل فيه العدد لـ (٢٧,١) مليون مستخدم لشبكة الإنترنت (Galal, 2024).



شكل رقم (١) يوضح عدد مستخدمي شبكة الإنترنت في مصر(Galal, 2024)

وعلى الرغم من الفوائد الهائلة لشبكة الإنترنت، فإنها تحمل في طياتها العديد من السلبيات المحتملة إذا ما استُخدِمَت بشكل غير سليم، الأمر الذي جعل من الضروري التعريف بماهية أمن المعلومات والأمن السيبراني في الجامعات، نظرًا لأن طلاب الجامعات هم أكثر الفئات عرضة للهجمات السيبرانية؛ لأنهم يعتمدون على شبكة الإنترنت بشكل كبير.

٢/٢ تطوير ممارسات أمن المعلومات داخل مؤسسات المكتبات:

أصبحت شبكة الإنترنت جزءًا لا يتجزأ من مختلف جوانب الحياة اليومية للأشخاص، للحصول على المعلومات والبيانات، الأمر الذي يترتب عليه مزيد من التهديدات الأمنية. وهذا ما أوضحه "أريجبيسولا" و"نواوليس" (Aregbesola & Nwaolise, 2023) من أن هناك مجموعة من الخطوات لتطوير ممارسات أمن المعلومات داخل مؤسسات المكتبات:

١- البنية التحتية الآمنة للشبكة: وذلك بالتأكد من أن البنية التحتية لشبكة المكتبة آمنة من خلال تنفيذ برامج جدران الحماية غير القابلة للاختراق، وبرامج كشف التسلل والوقاية منها، والعمل على تحديث معدات وبرامج الشبكة بشكل منتظم.

٢- إنشاء سياسة للأمن السيبراني: عن طريق تحديد المبادئ التوجيهية والإجراءات والمسؤوليات المتعلقة بالأمن السيبراني، على أن تغطي تلك السياسات مجالات حماية البيانات وضوابط الوصول وأمن الشبكة والاستجابة للحوادث أو أي حدث طارئ.

٣- استخدام التشفير والبروتوكولات الآمنة: عن طريق تشفير البيانات والاتصالات المهمة باستخدام خوارزميات تشفير قوية، كاستخدام بروتوكولات آمنة مثل (HTTPS) للخدمات ومواقع الويب من خلال شبكة الإنترنت لحماية البيانات في

أثناء النقل.

٤- الحفاظ على تحديث البرامج: يجب تحديث البرامج وتطبيقات البرامج وأنظمة التشغيل بصورة منتظمة لمعالجة أي نقاط ضعف قد تظهر.

٥- النسخ الاحتياطي والتعافي من الكوارث: عن طريق عمل استراتيجية نسخ منتظمة لضمان إمكانية استعادة البيانات في حالة وقوع حادث إلكتروني أو فقدان للبيانات، عن طريق تخزين تلك البيانات بشكل آمن خارج الشبكة لمنع فقدان البيانات بسبب التلف المادي أو السرقة.

٦- ضوابط وصول المستخدم: عن طريق تنفيذ ضوابط لوصول المستخدمين للبيانات حسب الصلاحيات الممنوحة، وذلك فقًا للوظيفة أو المنصب، وكذلك مراجعة الحسابات المصرح لها بشكل دوري للتعرف على حسابات مَن غادروا الجامعة من منتسبيها ولا يحق لهم استخدامها.

٧- تقييمات أمنية بشكل منتظم: وذلك بعمل تقييمات أمنية بشكل دوري لتحديد نقاط الضعف في أنظمة المكتبة، حيث يجب أن يشمل فحص تلك الثغرات الأمنية وإجراء اختبارات للاختراق وتقييم للمخاطر الأمنية بشكل مستمر.

٨- خطة للاستجابة للحوادث المحتملة: عن طريق تحديد الخطوات الواجب اتخاذها في حالة وقوع حادث يتعلق بالأمن السيبراني، والتي من ضمنها خطوات الإبلاغ عن تلك الحوادث، واحتواء أضرارها والعمل على تخفيفها لاستعادة العمل بأسرع وقت ممكن، مع المحافظة على تحديث هذه الخطة باستمرار.

٩- إقامة شراكات تعاون مع المؤسسات الأخرى: عن طريق عمل شراكات مع المكتبات الأكاديمية الأخرى ومنظمات الأمن السيبراني والجهات المعنية الأخرى، للاطلاع على كل ما هو جديد ويستحدث في هذا المجال.

٣/٢ مفاهيم الأمن السيبراني في قطاع التعليم:

أشار كل من "برلي" وآخرين (Burley, et al.,2017) في التقرير الصادر ضمن سلسلة مناهج الحاسب وضمن فريق العمل المعني بإدخال مقرر الأمن السيبراني إلى قطاع التعليم، أنه ينبغي لقطاع التعليم إدخال مبادرات لإدخال مقررات دراسية جديدة خاصة بالأمن السيبراني كمقررات مستقلة، أو من خلال دورات تدريبية ضمن المقررات الحالية، حيث تقوم المفاهيم التالية بتعزيز العقلية الأمنية للأشخاص في مختلف مجالات المعرفة، لتوفير

مخطط تنظيمي لربط معرفة الطلاب في رؤية متماسكة مع مقررات الأمن السيبراني، ويمكن توضيح تلك المفاهيم فيما يلي:

١/٣/٢ مفاهيم الفكر السيبراني:

تعد مفاهيم الفكر السيبراني حجر الأساس لعملية إدارة أمن المعلومات على شبكة الإنترنت، والتي تضمن تعزيز تطبيق مقرر الأمن السيبراني في التعليم كما يلي:

١- النزاهة: التأكد من دقة وموثوقية البيانات.

٢- التوفر: إمكانية الوصول إلى البيانات والمعلومات والنظام.

٣- المخاطر: احتمالية المكسب أو الخسارة.

٤- التفكير العدائي: وهي عملية تفكير تأخذ في الاعتبار الإجراءات المحتملة للهجمات السيبرانية التي تقف عائقًا أمام النتيجة المطلوبة.

٥- تنظيم التفكير: وهي عملية تأخذ في الاعتبار التفاعل بين القيود الاجتماعية والتقنية لضمان تنفيذ المطلوب.

٢/٣/٢ مفاهيم الأخلاقيات السيبرانية:

تعد مفاهيم الأخلاقيات السيبرانية النظام الذي يتعامل مع ما هو جيد وما هو سيئ، ومع الواجب والالتزام الأخلاقي للتعامل مع بيئات الإنترنت، أي أنه مرتبط بالقدرة على التصرف بشكل أخلاقي مع شبكة الإنترنت، حيث يمكن تضمين مجموعة من المواضيع الرئيسة التي تندرج تحت هذا المفهوم:

١- السرقة العلمية.

٢- حقوق النشر.

٣- الاستخدام العادل للمعلومات.

٤- القرصنة.

٥- مشاركة الملفات.

٦- بروتوكولات التعامل مع شبكة الإنترنت.

٧- نشر معلومات غير دقيقة أو غير صحيحة.

٨- التنمر الإلكتروني.

٩- إدمان شبكة الإنترنت.

٣/٣/٢ مفاهيم السلامة السيبرانية:

تتمثل السلامة السيبرانية في القدرة على التصرف بطريقة آمنة ومسؤولة على شبكة الإنترنت، للمحافظة على المعلومات أيًا كانت نوعيتها أو شكلها. ويمكن تضمين مجموعة من المواضيع الرئيسة التي تندرج تحت هذا المفهوم، مثل:

١- المحتالون على شبكة الإنترنت.

٢- المحتوى غير اللائق.

٣- الاتصالات غير المرغوب فيها.

٤- التهديدات من خلال شبكة الإنترنت.

٥- إدمان شبكة الإنترنت.

وهذا ما أوضحه أيضًا كل من "كافيثا" و"بريثا" (Kavitha & Preetha, 2019)؛ إذ وضعا أساسيات للأمن السيبراني يجب على المؤسسات أن تتبعها عند وضع خططها الاستراتيجية للحفاظ على أمن وسلامة معلوماتها على النحو التالي:

١- تحديد التهديدات.

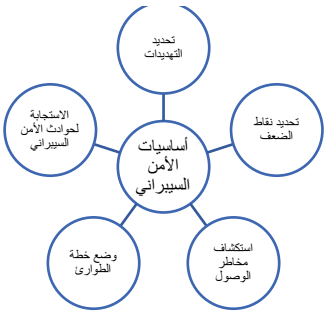
٢- تحديد نقاط الضعف.

٣- استكشاف مخاطر الوصول.

٤- وضع خطة الطوارئ.

٥- الاستجابة لحوادث الأمن السيبراني.

ويمكن توضيحها من خلال الشكل التالي:



شكل رقم (٢)

يوضح أساسيات الأمن السيبراني التي يجب على المؤسسات أن تتبعها عند وضع خططها الاستراتيجية

٤/٢ أنواع الهجمات السيبرانية الأكثر انتشارًا حول العالم على سبيل المثال وليس الحصر: (Kavitha & Preetha, 2019) ؛ (Himmat, et al.,2023)

١- هجمات الحرمان من الخدمة DOS (Denial of Service Attacks).

هي إحدى الهجمات التي يقوم فيها المهاجم بملء ذاكرة النظام بحيث يحرم من له حق استخدام الشبكة أو النظام من الوصول إليه.

٢- الهجمات المحلية عن بعد (R L٢A remote to local):

يستغل فيها المهاجم الثغرات الأمنية الموجودة بالشبكات المحلية للوصول عن بعد إليها بشكل غير قانوني وكأنه مستخدم قانوني لهذه الشبكة.

٣- مستخدم الوصول لجذر النظام ystemUser to Root Access to The S:

يستطيع المهاجم هنا الوصول إلى حساب مستخدم عادي للشبكة أو النظام وانتحال هويته للوصول إلى جذور الشبكة أو النظام والعمل على تخريبها بناءً على اكتشافه للثغرات الأمنية الموجودة.

٤- التحقيق Probing:

يعتبر التحقيق نوعًا آخر من الهجمات؛ حيث يقوم المهاجم بفحص الشبكة لجمع المعلومات واكتشاف الثغرات الأمنية بها للتعرف على نقاط الضعف بها، ويمكن أن يطلق عليها أيضًا هجمات استطلاعية، ومن ثم استغلال تلك المعلومات للقيام بهجوم محكم في التوقيت المناسب.

٥- هجمات الوصول Access Attacks:

يستطيع فيها المهاجم الوصول إلى جهاز ليس له الحق في الوصول إليه.

٦- الجريمة السيبرانية Cyber crime:

فيها تُستَخْدَم أجهزة الكمبيوتر والإنترنت لتحقيق مكاسب مادية.

٧- التجسس السيبراني Cyber espionage:

عن طريق استخدام شبكة الإنترنت للتجسس على الآخرين لتحقيق منفعة ما.

٨- الحرب السيبرانية Cyber war:

تقوم بها دولة ما بقصد تعطيل شبكة دولة أخرى لتحقيق مكاسب تكتيكية وعسكرية.

٩- الهجمات السلبية Passive Attacks:

هجوم يقوم في المقام الأول على التنصت دون التدخل في قاعدة البيانات.

١٠- الهجمات الخبيثة Malicious Attacks:

هجوم متعمد للتسبب بضرر يؤدي إلى اضطراب واسع النطاق.

١١- الهجمات غير الخبيثة Non Malicious Attacks:

هجوم غير مقصود بسبب سوء التعامل أو الأخطاء التشغيلية مع فقدان بسيط للبيانات.

١٢- هجمات شبكة الهواتف المتنقلة MANET Mobile Ad Hoc) Attacks):

الهجمات التي تهدف إلى إبطاء أو إيقاف تدفق المعلومات بين أجهزة الشبكة.

١٣- الهجوم على أجهزة الاستشعار اللاسلكية work Sensor Net lessWire (WSN):

هجوم يمنع أجهزة الاستشعار من استكشاف هجمات نقل البيانات والمعلومات عبر الشبكة.

ووفقًا للتقرير الذي أصدره الاتحاد الدولي للاتصالات (ITU)

(International Telecommunication Union) (ITU,٢٠٢٣) حدد فيه خمس ركائز لمؤشر الأمن السيبراني العالمي (The Global Cybersecurity Index (GCI) تحدد اللبنات الأساسية لثقافة الأمن السيبراني الوطنية كما يلي:

١- التدابير القانونية: تقاس بوجود الهيئات والأطر القانونية داخل الدولة المعنية بالأمن السيبراني والجرائم الإلكترونية.

٢- التدابير الفنية: تقاس بوجود الهيئات والأطر الفنية داخل الدولة المعنية بالأمن السيبراني.

٣- التدابير التنظيمية: تقاس بوجود مؤسسات داخل الدولة لتنسيق السياسات واستراتيجية تطوير الأمن السيبراني على المستوى الوطني.

٤- تنمية القدرات: تقاس بوجود هيئات وقطاعات معتمدة ومعترف بها للقيام بالعملية التنظيمية داخل الدولة، ووجود برامج ومراكز بحثية متخصصة في المجال، وكذلك وجود برامج تعليمية متطورة باستمرار.

٥- التعاون: يُقَاس بإجراءات تعتمد على وجود الشراكات والأطر التعاونية وشبكات

تبادل المعلومات.

فلقد أصبحت الهجمات السيبرانية آخذة في الارتفاع؛ فوفقًا لما أوردته "بترويكز" (Petrowicz,2021) يقع هجوم سيبراني كل ثماني دقائق، وقد أصبحت المؤسسات الأكاديمية هدفًا لتلك الهجمات لما تحتويه من كمٍّ هائل من البيانات الشخصية والبحثية، ووفقًا للتقرير الصادر عن المركز الوطني للأمن السيبراني فإن قطاع الجامعات ثالث أكثر القطاعات عرضة للهجمات السيبرانية.

٥/٢ أنواع التهديدات السيبرانية في المكتبات:

الأمن السيبراني هو تغطية الحماية المادية للأجهزة والبرامج من الوصول غير المصرح به عبر الوسائل التكنولوجية، وفيما يلي مجموعة المواضيع الرئيسة التي تندرج تحت هذا المفهوم:

١- الفيروسات والبرامج الضارة ذاتية النسخ (and Worms Viruses): تنتشر من جهاز إلى آخر من خلال شبكة الإنترنت عن طريق ثغرة أمنية بالنظام، ونتيجة لخطأ بشري عن طريق فتح ملف أو تشغيل برنامج (Sheikh,2021).

٢- حصان طروادة (Trojan): يعد من البرامج الضارة التي تسبب ضررًا بالغًا للأجهزة وبرامج النظام، حيث يشتمل إما على ملف أو برنامج أو جزء من التعليمات البرمجية، لكي يبدو برنامجًا شرعيًّا أصليًّا للإيقاع بالضحايا إما لسرقة البيانات أو للتجسس (Sheikh,2021).

٣- برامج التجسس (Spayware): تهدف هذه البرامج إلى تجميع المهاجم معلومات عن المستخدمين أو أنظمتهم باعتبارها نوعًا من أنواع التعدي على الخصوصية، إما لابتزاز المستخدم أو لتحميل برامج ضارة إليه، ودون أن يشعر المستخدم به (Merriam-Webster, n.d.).

٤- التصيد (phishing): أسلوب لمحاولة الحصول على البيانات المهمة، إما من خلال البريد الإلكتروني أو من خلال مواقع إلكترونية، حيث يتنكر المهاجم في صورة شركة مشروعة أو شخص حسن السمعة (Technology, n.d.).

٥- التصيد بالرمح Spear phishing: أسلوب يشبه التصيد العادي، ولكنه تصيد مصمم خصيصًا لفرد أو مؤسسة معينة (Rosencrance & Bacon, 2021).

٦- التصيد الصوتي oice PhishingV: أسلوب احتيال عبر الهاتف، لجمع معلومات

مالية أو شخصية من الهدف أو الضحية (Rosencrance & Bacon, 2021).

٧- صيد الحيتان Whaling: هجوم يستهدف خداع الموظفين البارزين فقط، مثل المدير المالي أو الرئيس التنفيذي، من أجل الكشف عن معلومات مهمة لا تتاح إلا من خلالهم (Rosencrance & Bacon, 2021).

٨- برامج الفدية (Ransomware): نوع من البرامج الضارة التي تمنع المستخدمين من الوصول إلى ملفاتهم أو نظامهم وتطلب الفدية لاستعادة تلك الملفات، حيث ارتفع عدد ضحايا هجمات الفدية عام ٢٠٢٣ بنسبة (١٢٨,١٧%) مقارنة بعام ٢٠٢٢ (Chesti, et al, 2020) ؛ (Paganini,2024).

٩- الهندسة الاجتماعية Engineering Social: أسلوب يعتمد على التفاعل البشري لخداع المستخدمين من أجل خرق الإجراءات الأمنية، من أجل الوصول غير المصرح إلى الأنظمة أو الشبكات أو المواقع المادية أو لتحقيق مكاسب مادية، عن طريق الحصول على معلومات مهمة من المفترض أن تكون محمية دائمًا (P.S, M, & Sundaresan, 2018) & (Rosencrance & Bacon, 2021).

وقد بيّن كل من "إجبينوفيا" و"إيشولا" (Igbinovia & Ishola, 2023) مخاطر الأمن السيبراني الشائعة في المكتبات كما يلي:

١- البرامج الضارة قد تعرض سلامة مجموعات المكتبات الرقمية وقواعد البيانات المتاحة من خلالها للخطر، ومن ثم تعطيل خدماتها.

٢- يشكل التصيد الاحتيالي تهديدًا كبيرًا لمستخدمي المكتبة وموظفيها، فقد يؤدي الوصول غير المصرح إلى تعريض بيانات المستخدمين للخطر، مع احتمالية أن يؤدي ذلك إلى مزيد من الهجمات الإلكترونية.

٣- يمكن أن تؤدي هجمات برامج الفدية إلى شل عمليات المكتبة عن طريق تشفير الملفات المهمة، بما في ذلك المجموعات الرقمية وقواعد البيانات، ما يعرض المكتبة إلى خسائر مالية ويضر بسمعتها، إذا اختارت دفع الفدية أو فقدت إمكانية الوصول إلى المعلومات المهمة.

٤- يمكن للمهاجمين استغلال الشبكات غير الآمنة للمكتبات في اعتراض البيانات والمعلومات المهمة عبر الشبكة، ما يؤدي إلى انتهاكات محتملة للخصوصية والوصول غير المصرح إلى أنظمة المكتبة.

٥- قد تحتوي البرامج والأنظمة القديمة على ثغرات أمنية غير مصححة يمكن استغلالها في الوصول غير المصرح به واختراق البيانات أو انقطاع الخدمة.

٦/٢ تعزيز الأخلاقيات السيبرانية بين مستخدمي المكتبات:

الأخلاقيات السيبرانية توضح كيفية التعامل بشكل سليم وصحيح مع شبكة الإنترنت بما تحتويه من معلومات، وفيما يلي بعض الأخلاق السيبرانية التي يجب على المرء اتباعها في أثناء استخدامه شبكة الإنترنت:

١- التواصل والتفاعل بين الأشخاص بشفافية لضمان مشاركة المعرفة والمعلومات بشكل آمن.

٢- تعزيز فكر الاستخدام المسؤول للتكنولوجيا.

٣- الالتزام بتداول المعلومات المتاحة على شبكة الإنترنت بشكل قانوني يضمن حقوق الملكية الفكرية لأصحابها.

٤- الالتزام بعدم استخدام كلمة المرور الخاصة بشخص آخر تحت أي ظرف من الظروف.

٥- الالتزام بالضوابط القانونية بعدم إرسال أي من البرامج الضارة إلى أجهزة الآخرين بغرض إحداث أي ضررٍ.

٦- الالتزام بعدم مشاركة المعلومات الشخصية للشخص نفسه أو لأشخاص آخرين تحت أي ظرف من الظروف، للمحافظة على عدم استغلال تلك المعلومات بشكل خطأ ولترسيخ مبدأ احترام الخصوصية.

٧- الالتزام بعدم انتحال شخصية شخص آخر، لما يترتب على ذلك من مشكلات فيما بعد.

٨- الالتزام بعدم التحايل على قوانين حقوق الطبع والنشر، بغرض الحصول على المعلومات بأي طريقة حتى وإن كانت طريقة غير قانونية.

ووفقًا لتقرير الإفلا (IFLA, 2022) وُجد أن المكتبات ترغب في تعزيز الأمن السيبراني في المجالات التالية:

١- حماية أنظمة المكتبات من مخاطر وتهديدات الأمن السيبراني من أجل تقديم خدماتها بشكل مستمر وبكفاءة عالية.

٢- ضمان حماية مستخدمي المكتبة من التهديدات المرتبطة باستخدام الإنترنت في

أثناء استخدامهم شبكة المكتبة.

٣- ضمان المكتبات حماية استخدام شبكاتها بشكل سليم لا يسبب أي أضرار للآخرين، وذلك عن طريق توعية مستخدميها للامتثال للقوانين والسياسات من قبل المكتبات.

٤- ضمان التوازن بين تحقيق أقصى حماية ممكنة وبين احترام حقوق الإنسان فيما يتعلق بالخصوصية.

٥- حماية خصوصية معلومات المستخدمين.

٧/٢ الاستراتيجية المقترحة لتعزيز الأمن السيبراني داخل المكتبات:

١- قيام قسم أمن المعلومات بالمكتبات بإجراء اختبارات الاختراق السيبراني بصفة منتظمة، حيث سيساعد ذلك على التعرف على أنواع المستخدمين الذين يشكلون خطرًا على المكتبة، كما ستساعد في اكتشاف الموظفين الذين يحتاجون إلى تدريب إضافي.

٢- تنفيذ برنامج توعوي عن الأمن السيبراني، يجنب المكتبات كثيرًا من تلك الهجمات ويجعل كلًا من موظفي المكتبة ومستخدميها أقل عرضة لأن يصبحوا ضحايا لتلك الهجمات.

٣- توفير بريد إلكتروني آمن للمكتبة، وكذلك توفير بوابات ويب لفحص رسائل البريد الإلكتروني، للبحث عن الروابط الضارة وتصفيتها، ومن ثمَّ تقليل إمكانية قيام أيٍّ من الموظفين بالضغط على تلك الروابط.

٤- المحافظة على تحديث برامج مكافحة الفيروسات والبرامج الضارة باستمرار.

٥- التأكيد على موظفي المكتبة ومستخدميها عدم استخدام كلمة المرور نفسها بالحسابات الشخصية وحسابات العمل.

٨/٢ تأثير بعض التقنيات الحديثة في تعزيز تدابير الأمن السيبراني للمكتبات:

١/٨/٢ تقنية الذكاء الاصطناعي والتعلم الآلي:

يستطيع أن يشكل الذكاء الاصطناعي والتعلم الآلي دورًا حيويًّا في مجال الأمن السيبراني من خلال أتمتة اكتشاف التهديدات والاستجابة لها، حيث يمكن لهذه التقنيات الحديثة تحليل كميات كبيرة من البيانات لتحديد الانتهاكات الأمنية المحتملة، حيث يمكن للأنظمة التي تعمل بالذكاء الاصطناعي أن تساعد في مراقبة الحركة الشبكة (Aregbesola & Nwaolise, 2023).

٢/٨/٢ تقنية "البلوكتشين" اللامركزية (Blockchain):

تستطيع تقنية "البلوكتشين" اللامركزية (kchainBloc) مقاومة أي محاولة احتيال من الممكن أن تحدث على شبكة المكتبة، حيث يمكنها تعزيز سلامة البيانات والخصوصية، من أجل حماية حقوق الملكية الفكرية، ومنع الوصول غير المصرح به أو إجراء تعديلات على البيانات المهمة، والعمل أيضًا على تحسين التعاون بين مستخدمي المكتبة وموظفيها. إن هدف "البلوكتشين" (Blockchain) الأساسي منح مستخدمي المكتبة إمكانية الوصول غير المقيد إلى محتواها الرقمي أو إلى المحتوى المطبوع مع تقليل المخاطر لحماية خصوصية كل مستخدم وهويته (Jha,2023).

٣/٨/٢ مبدأ الثقة المعدومة (Principle Zero Trust):

أسلوب من أساليب الأمن السيبراني الذي يقوم على مبدأ "الثقة مع التحقق" للحفاظ على البيانات، فهو يتعامل مع جميع الشبكات وحركة المرور عليها، حتى وإن كانت من أشخاص مصرح لهم، على أنها مصدر تهديدات محتملة، ولا يوجد تطبيق أو مستخدم أو جهاز في نظام المعلومات موثوق به. ولهذا يجب إعادة تقييم الثقة والتحقق منها في كل مرة يطلب فيها الشخص الوصول للشبكة، حيث تعتبر هندسة الثقة المعدومة هي البنية التحتية للشبكة (المادية والافتراضية) للمكتبة باعتبارها خطوة لبناء مبدأ الثقة المعدومة (Rose, Borchert, Mitchell, & Connelly, 2020).

٤/٨/٢ تحليلات سلوك المستخدم User Behavior Analytics (UBA):

يعتبر نوعًا من برامج الأمان التي تستخدم التحليلات السلوكية وخوارزميات التعلم الآلي لتحديد سلوك المستخدم والجهاز غير الطبيعي الذي من المحتمل أن يشكل خطرًا على الشبكة، حيث يمنح رؤى أمنية أفضل ويعزز برامج أمان الثقة المعدومة، كما أنه لا يقوم بتتبع أنماط سلوك المستخدم فحسب، بل يتتبع ويراقب أيضًا الخوادم وأجهزة إنترنت الأشياء، بحثًا عن أي سلوك شاذ أو أي نشاط قد يشير إلى أي تهديد أمني محتمل، وذلك لتبسيط عمل المتخصصين الفنيين الذين يركزون على الأمن (Gartner, ٢٠١٧).

٥/٨/٢ أمن البيانات السحابية Security Data Cloud (Alvarenga,2022):

يشير أمن البيانات السحابية إلى التقنيات والسياسات والخدمات وضوابط الأمان التي تحمي أي نوع من البيانات في السحابة من الضياع أو التسريب أو سوء الاستخدام، من خلال الانتهاكات والتسرب والوصول غير المصرح به، حيث يجب أن تتضمن استراتيجية أمن البيانات السحابية ما يلي:

١- تأمين البيانات المستخدمة داخل تطبيق المؤسسة.

٢- تأمين نقل البيانات في أثناء تحركها داخل شبكة المؤسسة من خلال التشفير وإجراءات الأمان الأخرى.

٣- حماية البيانات غير النشطة المخزنة في أي موقع على شبكة المؤسسة.

٦/٨/٢ أمن إنترنت الأشياء (IOTInternet Of Things) (Security, 2022):

يشير إنترنت الأشياء إلى شبكة من الأجهزة المتصلة بشبكة الإنترنت سواء كانت أجهزة كمبيوتر أو أجهزة ذكية يمكنها الاتصال بشبكة الإنترنت، حيث لا تتطلب أجهزة إنترنت الأشياء إلا القليل من المدخلات من المستخدم، بل قد لا تتطلب في بعض الأحيان مدخلات بعد مدخلات الإعدادات الأولى، حيث تُرسَل البيانات عبر الإنترنت لمعالجتها ومشاركتها مع الأجهزة الأخرى من خلال تقنيات (Bluetooth)، (Wi-Fi)، (RFID)، ما يتطلب معه قيام المؤسسات بالتحقق من إمكانات الأمان وسبل الحفاظ على أمن وسلامة البيانات المرسلة والمستقبلة مع زيادة عدد أجهزة إنترنت الأشياء داخل المؤسسات، الأمر الذي يتطلب معه قيام المؤسسات بتنفيذ خطط وسياسات لتقليل احتمالية وقوع حوادث أمن سيبرانية على شبكة المؤسسة على النحو التالي:

١- عمل شبكة (Wi-Fi) خاصة بالزائرين.

٢- عمل كلمة سر (Password) خاصة بأجهزة إنترنت الأشياء إن كان نظام المؤسسة يسمح بذلك.

٣- التأكد من تشفير البيانات التي أنشئت بواسطة أجهزة إنترنت الأشياء.

٤- إيقاف تشغيل أي خدمات تشغيل تلقائية من خلال أجهزة إنترنت الأشياء.

٥- تحديث أجهزة إنترنت الأشياء باستمرار بأحدث البرامج.

٦- مراقبة أي مشكلات تتعلق بأمان إنترنت الأشياء واكتشافها وتصحيحها.

٧- تقييد وصول شبكات إنترنت الأشياء إلى الأنظمة التي تتضمن بيانات مهمة.

٩/٢ مبادرات الوعي بالأمن السيبراني بالجامعات على سبيل المثال وليس الحصر:

قامت الولايات المتحدة الأمريكية بإنشاء المبادرة الوطنية لتعليم الأمن السيبراني The National Initave For Cybersecurity Education) (NICE)" لتحسين وضع الأمن السيبراني على المدى الطويل في التعليم، حيث وضعت من أجل ذلك مجموعة من التشريعات والاستراتيجيات لتطوير تعليم الأمن السيبراني (NICE, 2010).

وفي المملكة المتحدة يعد تعزيز تعليم مهارات الأمن السيبراني أحد المكونات الأساسية للبرنامج الوطني لتأمين الفضاء السيبراني، حيث قامت الحكومة بدمج الأمن السيبراني في جميع مستويات التعليم بدءًا من سن ١١ عامًا، عن طريق تقديم الدعم للمدارس، وتوفير الدعم للجامعات عن طريق تقديم التدريب المهني ودعم البحوث الجامعية، وإتاحة فرص عمل في مجال الأمن السيبراني، كما ركز البرنامج الوطني لتأمين الفضاء السيبراني على تحديد التحديات التي قد تواجه تنفيذ البرنامج في التعليم (UK. Cabinet Office & National Security and intelligence, 2011).

وفي فنلندا أجرى "ليتو" (Lehto, 2019) دراسة على ثماني جامعات، تبين من خلالها أن تعليم الأمن السيبراني آخذ في الارتفاع في هذه الجامعات، حيث اتجهت تلك الجامعات لاستخدام نموذجين للتعليم في هذا المجال: النموذج الأول منهج يركز على الأمن السيبراني بشكل عام، والنموذج الثاني منهج يركز على دمج دراسات الأمن السيبراني في المناهج الأخرى، من أجل نشر الوعي بأهمية الأمن السيبراني على مستوى المجتمع الفنلندي.

ومن المبادرات العربية التي تهدف إلى تنمية مهارات الطلاب بالأمن السيبراني، مبادرات "أجيال مصر الرقمية" بجمهورية مصر العربية، والتي تعتبر مظلة لعدد من المبادرات الرقمية المقدمة جميعها بالمجان لمختلف المراحل العمرية، بدءًا من المرحلة الابتدائية ووصولًا إلى طلبة الجامعات والخريجين من مختلف الخلفيات الأكاديمية، لتنمية مهاراتهم التكنولوجية في مجال الاتصالات وتكنولوجيا المعلومات، ومن الموضوعات التي تغطيها المبادرة على سبيل المثال: الأمن السيبراني، علوم البيانات، الذكاء الاصطناعي، الفنون الرقمية؛ حيث تهدف المبادرة إلى تخريج جيل قادر على مواكبة متطلبات سوق العمل المحلي والعالمي، وذلك بالتعاون مع عدد من الجامعات الدولية والشركات المحلية والعالمية المتخصصة في مجال الاتصالات وتكنولوجيا المعلومات (المعلومات، ٢٠٢٤).

أما مبادرة "بأمان نتعلم" بالمملكة العربية السعودية لرفع الوعي بالأمن السيبراني، التي أطلقها المركز الوطني الإرشادي للأمن السيبراني بالتعاون مع وزارة التعليم (السيبراني، د.ت.)، فتهدف إلى رفع الوعي بالأمن السيبراني بين الطلاب وتقليل المخاطر التي قد يتعرض لها الطالب في أثناء ممارسة مهامه التعليمية اليومية باستخدام شبكة الإنترنت، وما هي الإجراءات الواجب مراعاتها لتحصين أجهزة الكمبيوتر أو الأجهزة الذكية الخاصة بالطالب، ولنجاح تلك المبادرة قام المركز الوطني الإرشادي بالتعاون مع وزارة التعليم لإعداد ونشر المواد التوعوية للوصول الفعال للفئات المستهدفة، وتواصل المركز مع هيئة

الاتصالات وتقنية المعلومات لنشر الدليل الإرشادي للتعليم عن بعد لما يصل إلى ٤٠ مليون مستخدم خلال الشهر الأول من الدراسة.

كما أوضح "جاربا" و"سيراج" و"موسى" و"عثمان" (Garba, Siraj, Musa, & Othman, 2020) أن الاستخدام المتزايد لشبكة الإنترنت باستخدام مختلف الأجهزة الإلكترونية بين الطلاب، وضعهم في خطر متزايد لاحتمال أن يقعوا فريسة لتلك الهجمات بدون قصد أو معرفة، ولذلك فإن توعيتهم بماهية الأمن السيبراني يؤهلهم لحماية أنفسهم من هذه الهجمات المحتملة في المستقبل، حيث شملت الدراسة عدد ٢٠١ طالب وطالبة بكليات علوم الحاسب، تبين أن أغلبهم لديهم مستوى مُرضٍ عن الأمن السيبراني، بينما أكثر من نصف الطلاب لا يدركون كيفية حماية بياناتهم من تلك الهجمات، وأثبتت الدراسة أن الطالبات هم أكثر عرضة لتلك الهجمات.

وهو ما أكده أيضًا "ليش" (Lestch, 2015) من أن المدارس تمتلك بيانات غاية في الأهمية سواء عن الطلاب أو المدرسين أو العاملين بها، وهذا ما يستوجب معها حمايتها والحفاظ عليها بأحدث الوسائل والأساليب للحماية من تلك الهجمات، مع التوعية على إعداد كلمات مرور أكثر أمانًا.

هذا وقد أوضح أيضًا رحمن وسيراج وزيزي وخالد (Rahman, Sairj, Zizi & Khalid, 2020) أهمية إدخال تعليم الأمن السيبراني داخل المدارس في دولة ماليزيا، نتيجة لمجموعة من العوامل التي توصلت إليها الدراسة نوردها فيما يلي:

١- الطلاب المشاركون كانوا أقل استعدادًا لإنفاق المال أو الوقت على الندوات أو البرامج حول الأمن السيبراني، وهذا ما يمكن تفاديه عن طريق توفير المعلمين ومديري المدارس تنظيم تلك الندوات أو البرامج.

٢- ضرورة أن تصبح المدارس مراكز للمعرفة لكشف القضايا المتعلقة بالأمن السيبراني بالنسبة للمجتمع.

٣- ضرورة توفير مخصصات مالية حكومية لتغطية نفقات هذه البرامج والندوات.

٤- توفير تعليم الأمن السيبراني بالمدارس يعمل على تغيير عقلية كل منتسبي تلك المدارس.

٥- توفير معسكرات صيفية تابعة للمدارس للتوعية بأهمية الأمن السيبراني على غرار المعسكر الصيفي لطلاب المدارس المسمى بـ "GenCyber" التابع لمؤسسة العلوم

الوطنية NSF "(National Science Foundation)" ووكالة الأمن القومي الأمريكية "(NSA) National Security Agency"

ولذلك يعتبر الوعي بأهمية أمن المعلومات والأمن السيبراني بين الأوساط الأكاديمية يمكن أن يشكل دورًا فعالًا في الحماية من مخاطر تلك الهجمات، فالجامعات هي خط الدفاع ضد الهجمات السيبرانية وذلك من خلال:

١- برامج التوعية لأعضاء هيئة التدريس والطلاب:

يعد خط الدفاع الأول للجامعات ضد هذه الهجمات برامج التوعية المقدمة لأعضاء هيئة التدريس أو للطلاب، حيث سيعد الحفاظ على الوعي الأمني في ظل التطورات التكنولوجية الحالية والمستقبلية التحدي الأكبر للجامعات، لاعتبار الجامعات مركزًا لنقل المعلومات سواء داخل الدولة أو خارجها لخلق مزيد من التواصل بين الباحثين حول العالم.

٢- مصداقية الوصول:

عن طريق تحديد الجامعات لأساليب وصول محددة ومقصورة فقط على منتسبيها، على أن تراجع هذه الأساليب على فترات قريبة للتأكد من أمانها للحفاظ على سلامة شبكة الجامعة، وعدم وقوعها في أيدي المحتالين ممن يستطيعون الحصول على تلك الأساليب السليمة للوصول إلى شبكة الجامعة والتنقل خلالها دون اكتشافه.

٣- تصميم شبكة الجامعة:

يعد تصميم شبكة الجامعة من أكبر التحديات التي تواجهها الجامعات، عن طريق كيفية توفيرها لأقصى درجات الحماية لكل جوانب شبكتها، ودون تأثير ذلك على تداول البيانات والمعلومات بين المنتسبين لها، ولذلك فمن الأفضل للجامعات تقسيم الشبكة الخاصة بها إلى مجموعة من الشبكات الصغيرة داخل الشبكة الأم، لتوفير مزيد من الأساليب الأمنية التي تُطلب عند الدخول إلى كل شبكة من هذه الشبكات دون أن يؤثر ذلك على سرعة الشبكة أو إتاحتها باستمرار دون انقطاع.

ومن خلال تعريف الطلاب بمبادئ أمن المعلومات ومبادئ الأمن السيبراني المنبثق من أمن المعلومات بشكل جيد، يمكن في هذه الحالة أن نحقق آلية أمنية ناجحة للطلاب وللمكتبات والمؤسسات التابعة لها فيما بعد، على اعتبار أن الطلاب هم المسؤولون عن تلك المكتبات والمؤسسات في المستقبل.

١٠/٢ المعلومات التي يجب حمايتها من مخاطر الهجمات السيبرانية داخل الجامعات:

١- البيانات الشخصية للطلاب وأعضاء هيئة التدريس والموظفين.

٢- أرقام الضمان الاجتماعي للطلاب وأعضاء هيئة التدريس والموظفين.

٣- أرقام بطاقات الائتمان للطلاب وأعضاء هيئة التدريس والموظفين.

٤- بيانات السجلات الطبية.

٥- كشوف الالتحاق والغياب والحضور.

٦- وثائق التعليم الخاص.

٧- أسماء الطلاب وأعضاء هيئة التدريس والموظفين.

٨- عناوين الطلاب وأعضاء هيئة التدريس والموظفين.

٩- أرقام هواتف الطلاب وأعضاء هيئة التدريس والموظفين.

١٠- عناوين البريد الإلكتروني.

١١- السجل الجنائي للطلاب وأعضاء هيئة التدريس والموظفين.

١١/٢ الوعي بالجرائم الإلكترونية لدى طلاب الجامعات:

يعد قطاع التعليم العالي أحد القطاعات المعرضة لخطر الهجمات السيبرانية، سواء كانت تلك الهجمات على البيانات الشخصية لأيٍّ من منتسبي الجامعات، أو فقدان الملكية الفكرية لبراءات الاختراع لدى الجامعات، لذلك أصبح من الضروري تضمين مقرر الأمن السيبراني والتوعية به حاجة ملحة في ظل التطورات التكنولوجية المتسارعة. ولذلك أوضحت دراسة كل من "أودريان" و"أجونديلي" و"إديم" و"أنوانا" (Awodiran, Ogundele, Idem, & Anwana, 2023)، أن جرائم الفضاء الإلكتروني على مستوى العالم وعلى مستوى دولة نيجيريا على وجه الخصوص تتزايد بشكل كبير، ويعد الطلاب الفئة الأكثر استخدامًا لشبكة الإنترنت وهم الأكثر عرضة لهذه المخاطر، لنقص الوعي بتلك الجرائم أو حول كيفية التعامل معها، حيث جرت الدراسة على عدد ١٧١ طالبًا جامعيًا بجامعة "آفي بابالولا" (Afe Babalola) بنيجيريا، وكانت نتيجتها أن وعي الطلاب بالجرائم الإلكترونية منخفض بشكل عام، وتوصلت الدراسة إلى فروق ذات دلالة إحصائية بين مدى الوعي لتلك الجرائم بين الطلبة والطالبات. وقد أوصت الدراسة بضرورة بذل مزيد من الجهود من أجل نشر الوعي بالجرائم السيبرانية وكيفية الحماية منها للحد من تلك الجرائم. وهذا ما أكده أيضًا كل من "جابرا" و"سيرات" و"هاجار" و"داودا" (Gabra, Sirat, Hajar & Dauda, 2020) تجاه وعي

الطلاب حول أهمية الأمن السيبراني في الجامعات النيجيرية، حيث اتفقت نتائجها مع نتائج دراسة "أودريان" و "أوجنديل" و "إيدم" و"أنوانا" (Awodiran, Ogundele, Idem, & Anwana, 2023)، كما أوضحت الدراسة أن معظم الجامعات النيجيرية تفتقر إلى برامج توعية عن الأمن السيبراني.

وقد أكد القحطاني (Alqahtani, 2022) أهمية التوعية بالأمن السيبراني بين طلاب الجامعات، حيث جرت الدراسة على طلاب جامعة كلية الإمام عبد الرحمن بن فيصل من خلال استطلاع لرأي لعدد (٤٥٠) طالبًا حول درجة وعيهم بالأمن السيبراني من خلال كلمة المرور، وأمن مواقعهم الإلكترونية، وبياناتهم ومعلوماتهم على وسائل التواصل الاجتماعي، وتوصلت الدراسة إلى أن درجة معرفة الطلاب بالأمن المطلوب أن تكون عليه كلمة المرور سواء في البريد الإلكتروني أو بالمتصفحات أو من خلال وسائل التواصل الاجتماعي، تؤثر بشكل كبير في أهمية الوعي بالأمن السيبراني لدى الطلاب، غير أنه تبين من خلال الدراسة أيضًا أن مستويات الوعي بالأمن السيبراني لدى الطلاب ما زالت منخفضة خصوصًا عندما يتعلق الأمر بأمن كلمة المرور الخاصة بهم لحماية حساباتهم أو مواقعهم الإلكترونية، كما يستطيع الطلاب الحفاظ على معلوماتهم الشخصية من الانتشار على وسائل التواصل الاجتماعي مع معرفتهم الجيدة حول كيفية الإبلاغ عن التهديدات المشبوهة على وسائل التواصل الاجتماعي.

كما أشار أيضًا التحالف الوطني للأمن السيبراني The National Cyber security Alliance (NCSA) (Alliance, 2023) إلى سلوكيات الأمن السيبراني بين الأفراد لعام ٢٠٢٣، والتي يؤثر مدى الوعي بالجرائم الإلكترونية عليها، حيث جرى استطلاع رأي لأكثر من ٦٠٠٠ فرد في جميع أنحاء كل من الولايات المتحدة الأمريكية والمملكة المتحدة وكندا وألمانيا وفرنسا ونيوزيلندا لفحص سلوكيات ومواقف واتجاهات الأمن السيبراني، حيث أعرب (٦١%) من المشاركين عن مخاوفهم من أن يصبحوا ضحايا لجرائم الأمن السيبراني، كما توصل استطلاع الرأي إلى أن (٣٧%) يشعرون بالخوف، و(٣٩%) يشعرون بالإحباط بسبب الأمن من خلال شبكة الإنترنت الذي يسلط الضوء على القلق الرقمي، بينما أفاد (٤٤%) فقط من المشاركين في الولايات المتحدة الأمريكية أنهم تمكنوا من الوصول إلى برامج التدريب عن الأمن السيبراني، فضلًا عن أن (٣٨%) من الأمريكيين يستخدمون أدوات لتعزيز أمان كلمات المرور.

١/١١/٢ بعض الإرشادات التي قام بها المركز الوطني للأمن السيبراني بالمملكة المتحدة البريطانية (NCSC) للحماية من هجمات التصيد الاحتيالي عن طريق مجموعة من الطبقات الدفاعية (Centre, 2018):

١- الطبقة الأولى: جعل من الصعب على المحتالين والمهاجمين الوصول للمستخدمين من خلال رسائل البريد الإلكتروني التصيدية، وذلك عن طريق وضع تدابير أمنية لتصفية أو حظر الرسائل التي من المحتمل أن تكون ضارة.

٢- الطبقة الثانية: مساعدة المستخدمين على اكتشاف رسائل البريد الإلكتروني التصيدية في حال لم تُكتَشَف في الطبقة الأولى من طبقات الدفاع، عن طريق برامج التدريب للتوعية بمخاطر هذه الرسائل.

٣- الطبقة الثالثة: وضع تدابير أمنية إضافية في حال لم تُكتَشَف رسائل البريد الإلكتروني الضارة في الطبقتين الأولى والثانية، كأن يتم تصديق الدخول للبريد الإلكتروني على مرحلتين؛ لمنع المهاجم من الوصول مباشرة إلى رسائل البريد الإلكتروني حتى وإن حصل على كلمة مرور المستخدم.

٤- الطبقة الرابعة: وجود خطة محدثة باستمرار للاستجابة بسرعة للحوادث والهجمات، والتي تُختَبَر بانتظام للتأكد من تعاملها بشكل سليم مع أي هجمات قد تحدث.

١٢/٢ المعيار الدولي لنظم إدارة أمن المعلومات:

مما لا شك فيه أن المكتبات يجب أن تكون على دراية كافية بأمن المعلومات وقضاياها وتخصيص المزيد من الموارد لحماية تلك المعلومات، الأمر الذي يتطلب معه وجود معايير تنظيمية تحقق هذا الغرض، ولذلك عليها أن تتبع أحد المعايير الصادرة من إحدى الجهات الموثوقة من أجل اعتماد أفضل الممارسات الأمنية للحفاظ على المعلومات لديها، وكذلك استخدام مواردها بكفاءة. وبحكم أن المنظمة الدولية للتوحيد القياسي (أيزو) رائدة في مجال أمن المعلومات وإدارتها؛ فسيُعتَمَد على المعايير الصادرة عنها لتكون بمثابة الركيزة الأساسية للمكتبات للاسترشاد بها عند إعداد خطتها الاستراتيجية فيما بعد للحفاظ على أمن معلوماتها، ومن هذه المعايير ما يلي:

١/١٢/٢ معيار (ISO/IEC 27002) لأمن المعلومات والأمن السيبراني وحماية الخصوصية – ضوابط أمن المعلومات (Governance, 2022):

المعيار الدولي الصادر عن المنظمة الدولية للتوحيد القياسي (أيزو)، والذي يحدد

مواصفات نظام إدارة أمن المعلومات Information Security Management System (ISMS) خاص بالهيئات أو المؤسسات، يتوافق مع أفضل ممارسات أمن المعلومات على مستوى العالم. ويمكن تشكيل وتطويع هذا المعيار لكي يتناسب مع مواصفات واحتياجات الهيئات أو المؤسسات، إذ الهدف منه توفير تقنيات شاملة لأمن المعلومات وضوابط إدارة الأصول لأي مؤسسة تحتاج إلى برنامج جديد لإدارة أمن المعلومات لديها أو ترغب في تحسين سياسات وممارسات أمن المعلومات الحالية، حيث يقدم معيار ISO/IEC٢٧٠٠٢ الصادر عام ٢٠٢٢ عدد (٩٣) عنصر تحكم أمني بدلًا من (١١٤) عنصرًا بمعيار ISO/IEC٢٧٠٠٢ الصادر عام (٢٠١٣)، ويعد المعيار من أفضل الممارسات التي يمكن استخدامها لتجنب المخاطر التي من الممكن مواجهتها، ويقسم المعيار على خمس سمات رئيسة للتسهيل على المؤسسات في إدارة معلوماتها على النحو التالي (Harvey, 2024):

١- نوع التحكم (وقائي: عن طريق النسخ الاحتياطية، كشفي: عن طريق برامج كشف الفيروسات والاختراقات، إمكانية الوصول للشبكة).

٢- خصائص أمن المعلومات: (السرية، النزاهة، توافر المعلومات).

٣- مفاهيم الأمن السيبراني الخمس، هي: (التحديد، الحماية، الكشف، الاستجابة، الاسترداد).

٤- القدرات التشغيلية: (إدارة أصول الحوكمة، حماية المعلومات، أمن الموارد البشرية، الأمن المادي، أمن الأنظمة والشبكات، أمن التطبيقات، التكوين الآمن، إدارة الهوية والوصول، إدارة التهديدات والضعف، الاستمرارية، أمن علاقات الموردين، القانون والامثال، إدارة أحداث أمن المعلومات، ضمان أمن المعلومات).

٥- مجالات الأمن وتشمل: (الحوكمة والنظام البيئي لحوكمة أمن نظام المعلومات وإدارة المخاطر وإدارة الأمن السيبراني للنظام البيئي بما في ذلك أصحاب المصلحة الداخليين والخارجيين).

وأما عناصر التحكم البارزة، فتشتمل على: فهم تهديدات أمن المعلومات، أمن المعلومات لاستخدام الخدمات السحابية، جاهزية تكنولوجيا المعلومات والاتصالات لاستمرارية العمل، مراقبة الأمن المادي، إدارة التكوين، حذف المعلومات، إخفاء البيانات، منع تسريب البيانات، أنشطة الرصد، تصفية الويب، الترميز الآمن للحسابات (ISO/IEC, ٢٠٢٢).

٢/١٢/٢ معيار (ISO/IEC٢٧٠٣٢) للأمن السيبراني (ISO/IEC,٢٠٢٣):

معيار دولي للأمن السيبراني يقوم بتقديم إرشادات للمؤسسات حول كيفية إدارة مخاطر الأمن السيبراني وتنفيذ الضوابط الأمنية لحماية الخدمات المرتبطة بالإنترنت وأنظمة شبكات تكنولوجيا المعلومات والاتصالات وتقديم إرشادات للتعامل مع التهديدات الشائعة لأمن الإنترنت مثل (هجمات الهندسة الاجتماعية، هجمات يوم الصفر، هجمات الخصوصية، القرصنة، البرامج غير المرغوب فيها)، ويهدف هذا المعيار إلى تحقيق مجموعة من الضوابط، هي:

- الاستعداد للهجمات.
- منع الهجمات.
- كشف ورصد الهجمات.
- الرد على الهجمات.

ويركز إطار عمل وثيقة المعيار على الحفاظ على السرية والنزاهة وتوافر المعلومات عبر الإنترنت والأصالة والموثوقية، ويتضمن إرشادات حول مجموعة من الموضوعات مثل: (معلومات عن التهديدات، كيفية الاستجابة للحوادث، معلومات عن الوعي الأمني). هذا، وتستخدم وثيقة معيار (ISO/IEC٢٧٠٣٢) بعضًا من المفاهيم الواردة بمعيار (ISO/IEC ٢٧٠٠٢)؛ لتوضيح العلاقة بين أمن الإنترنت وأمن الويب وأمن الشبكات والأمن السيبراني.

١٣/٢ متطلبات إدخال مقرر أمن المعلومات والأمن السيبراني إلى أقسام المكتبات والمعلومات:

١- متطلبات إدارية: توفير كوادر أكاديمية مؤهلة وملمة بكل جوانب وأخلاقيات الأمن السيبراني.

٢- متطلبات البنية التحتية: تزويد أقسام المكتبات بالموارد اللازمة لتزويد الطلاب بإمكانية الوصول إلى أحدث التقنيات والبرامج، لتسهيل متابعة الطلاب لأحدث الممارسات الأخلاقية السيبرانية.

٣- المتطلبات التعليمية: توفير المواد التعليمية.

٤- المتطلبات الفنية: المهارات والخبرات التي يجب على الطلاب أن يكونوا ملمين بها عن المقرر.

٥- المتطلبات التشريعية: عن طريق وضع سياسات ومبادئ توجيهية للسلوك المناسب

عبر الإنترنت من أجل نشر الوعي بقوانين حقوق الملكية الفكرية وحقوق الطبع والنشر والقواعد المحددة لاستخدام المعلومات أيًّا كان مصدرها أو شكلها.

٦- المتطلبات التقنية: توفير برامج مكافحة الفيروسات وأدوات الأمان التي تضمن سلامة الطلاب.

١/١٣/٢ الاستراتيجيات المقترحة لإدخال مقرر أمن المعلومات والأمن السيبراني إلى أقسام المكتبات والمعلومات:

١- إدخال مقرر أمن المعلومات والأمن السيبراني، ومن الأفضل أن يتم بشكل مشترك بين أقسام المكتبات وبين كلية الحاسبات والمعلومات لتحقيق الاستفادة المرجوة منه وبين المكتبات للتطبيق العملي للطلاب.

٢- عقد دورات وورش عمل من قبل كلية الحاسبات والمعلومات لأعضاء هيئة التدريس بأقسام المكتبات حول كيفية توظيف وتطبيق مقرر أمن المعلومات والأمن السيبراني.

٣- تأكيد أن مرحلة تأهيل الطلاب للتعامل مع مختلف المخاطر الأمنية تتم في مرحلة التعليم الجامعي.

٤- ضرورة التعرف على مقررات أمن المعلومات والأمن السيبراني بمدارس المكتبات التي خضعت لاعتماد الجمعية الدولية للمكتبات "ALA"، وتطبيقها على أقسام المكتبات في الوطن العربي.

٥- لضمان مستوى موحد لخريجي أقسام المكتبات في الوطن العربي، يجب أن تتكاتف جميع الأقسام العلمية بتوحيد مقرراتها لضمان استمرارية التطوير، ورفع مستوى الخريجين.

٢/١٣/٢ فوائد إدخال مقرر عن أمن المعلومات والأمن السيبراني لأقسام المكتبات على مستوى جمهورية مصر العربية:

١- تمكين الطلاب من إنشاء ومراقبة وإدارة نظام إدارة المكتبة أو مركز المعلومات أو المؤسسة التي يوجدون بها مستقبلًا.

٢- يستطيع الطلاب التفريق بين الموضوعات العامة، التي يمكن أن تتاح بدون أي قيود، وأيضًا الموضوعات الخاصة أو شديدة الخصوصية، التي تتاح لمجموعة معينة من الأفراد.

٣- تعريف الطلاب لمجموعات الحفظ المختلفة تبعًا لأهمية الموضوع وعدد النسخ التي من المفروض أن توجد وأماكن وجودها.

٤- أن يستطيع الطلاب معرفة من لهم الحق في استخراج البيانات واستخدامها أو حفظها.

٥- أن يتعرف الطلاب على كيفية حماية البيانات عند نقلها من مكان لآخر.

٦- أن يتعرف الطالب على من له الحق في حذف البيانات نهائيًا، هل تتم بواسطة شخص واحد أو أكثر من شخص.

٧- أن يتعرف الطلاب على النواحي القانونية والتشريعية لكيفية التعامل مع البيانات.

٨- أن يتعرف الطلاب على الأماكن التي من المفروض أن توجد بها الخوادم، وهل يوثر ذلك على أمن البيانات أو الصيانة الدورية.

٩- تعريف الطلاب كيفية إنشاء سياسات ومعايير خاصة بالمؤسسة التي يعمل بها للحفاظ على أمن المعلومات بها.

٣/١٣/٢ من الخيارات المطروحة أمام أقسام المكتبات والمعلومات لإدخال مقرر عن أمن المعلومات والأمن السيبراني بها لكي تتناول مختلف قضاياه:

١- الأمن السيبراني المجتمعي في صورة مقرر مستقل: برنامج غير تقني يركز على تحديات الأمن السيبراني ونقاط القوة والضعف وآثار ذلك على المجتمع.

٢- أمن المعلومات: مقرر أعم وأشمل لكل قضايا المعلومات المادية والرقمية وتخصيص جزء من محتوى المقرر لقضايا الأمن السيبراني والأمن السيبراني المجتمعي.

٤/١٣/٢ معوقات من المحتمل أن تقف عائقًا أمام أقسام المكتبات والمعلومات لتطبيق مقرر أمن المعلومات والأمن السيبراني بها:

- تحديات مهارية: من الممكن أن يقف قلة الطلاب الذين يتمتعون بالمهارات التكنولوجية والمعرفة اللازمة عائقًا لتنفيذ ممارسات الأمن السيبراني الفعالة داخل أقسام المكتبات والحفاظ عليها.
- تحديات مادية: من الممكن أن تقف الموارد المادية عائقًا لتنفيذ ممارسات الأمن السيبراني داخل أقسام المكتبات، من أجل توفير البنية التحتية اللازمة لتوفير شبكة إنترنت آمنة، وكذلك توفير الأدوات والبرامج الحديثة اللازمة لتنفيذها.

- تحديات تنظيمية وقانونية: قد تكون اللوائح والأطر القانونية للأمن السيبراني غير واضحة بشكل سليم للطلاب، ما يخلق حالة من عدم اليقين بالمسؤوليات تجاه أهمية الأمن السيبراني لحماية البيانات.
- محدودية وعي الطلاب: قد تكون برامج التوعية والتدريب التي تلقاها الطلاب من قبل غير كافية، فقد يكونون غير مدربين بشكل كافٍ على أحدث تهديدات الأمن السيبراني والتدابير الوقائية لها، وأفضل الممارسات التي يجب اتباعها.