مجلة جامعة دمشق للآداب والعلوم الإنسانية
مجلد 40 – عدد 4 (2024): 277-294

Damascus University Journal of arts and humanities sciences Vol 40-No.4 (2024):277-294

متطلبات الأمن السيبراني في مكتبة الأسد الوطنية: دراسة حالة

ميس عبد الكريم إسماعيل[*1]، ياسين شريف الحجيمي[2]

1 * دكتوراه في علم المكتبات والمعلومات، محاضرة في قسم المكتبات، كلية الآداب والعلوم الإنسانية، جامعة دمشق. Mays.ismael@damascusuniversity.edu.sy

2 ماجستير قانون دولي، كلية الحقوق ، جامعة بغداد.

المخلص:

تعتبر المواقع الإلكترونية الوسيلة الأهمّ للوصول للخدمات والمعلومات التي يحتاجها المستفيدين من المكتبات، وبوجود التطورات التكنولوجية والتقنية الحديثة وشبكة الإنترنت فأصبح بإمكان كل مكتبة أو مركز معلومات أن تنشئ موقع خاص بها وإتاحة كل ما يخصّ هذه المكتبة عبر هذا الموقع لكن بالرغم من كل الإيجابيات التي توفرها شبكة الإنترنت والمواقع الالكترونية يوجد بعض السلبيات التي قد تضرب بالموقع والتي تؤدي الى إيقاف الموقع وخدماته وهنا ظهرت أهمية الأمن السيبراني فقد أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت إلى ظهور أنماط جديدة من الجرائم كالجرائم السيبرانية ومن هنا تبرز أهمية البحث الحالي التي هدفت إلى التحقق من متطلبات تحقيق الأمن السيبراني في مكتبة الأسد الوطنية، والتحقق من واقع الأمن السيبراني فيها، ولتحقيق تلك الأهداف استخدمت الباحثة المنهج الوصفي التحليلي، وأعدت الباحثة أدوات الدراسة المتمثلة في المقابلة والملاحظة المباشرة، وتكونت أسئلة المقابلة من أربعة بنود أساسية هي: المتطلبات المادية، والإدارية، والبشرية، والتقنية، وتكونت عينة الدراسة من المسؤولين في مكتبة الأسد عن الموقع الالكتروني وأمن المعلومات فيها بالإضافة لإجراء مقابلة مع مجموعة من الخبراء والاختصاصيين في مجال تكنولوجيا المعلومات الأمن السيبراني، وتم الحديث عن استراتيجية الأمن السيبراني التي أعدتها وزارة الاتصالات والتقانة التي اعتمد مجلس الوزراء خلال جلسته المنعقدة بتاريخ 2023/6/20بهدف التصدي للاختراقات السيبرانية المعادية وتحصين البيانات الحكومية على شبكة الانترنت والشبكات المتصلة بها وتأسيس بنية أمن سيبراني مستدامة توفر الحماية المتكاملة للأصول المعلوماتية وفقا لأهميتها ،ويضمن توزيع الأدوار وتحديد الصلاحيات بين جميع الأطراف سواء داخل المؤسسات أو على المستوى الوطني وتم التوصل إلى مجموعة من المقترحات التي يمكن أن تسهم في تطوير تطبيق

تاريخ الإيداع: 2024/07/18
تاريخ القبول: 2024/09/16

ISSN (online): 2789-6552
http://journal.damascusuniversity.edu.sy/index.php/index/index

الأمن السيبراني في مكتبة الأسد الوطنية حتى نستطيع تعزيز الثقة بين المستخدمين والمؤسسات المتعاملة مع المكتبة، وبالتالي الحفاظ على سمعتها ودورها الرئيسي في خدمة المجتمع والحفاظ على التراث الثقافي والمعرفي واقتراح استراتيجيات وإجراءات جديدة لتعزيز الأمن السيبراني في المكتبة وتقديم توصيات لتحسين البنية التحتية التقنية والتدابير الوقائية وتعزيز وعي وتدريب الموظفين والمستخدمين من خلال تصميم برامج تدريبية.

الكلمات المفتاحية: الأمن السيبراني، أمن المعلومات، المكتبات الوطنية، مكتبة الأسد.

Cybersecurity Requirements At Al-Assad National Library: A Case Study

Mais Abdul Karim Ismail*[1], Yaseen Sharif Al-Hijimi[2]
1. Damascus University, specialization in Library and Information Sciences. Mays.ismael@damascusuniversity.edu.sy
2. Baghdad University, specialization in Law.

Abstract:
Websites are considered the most important means of accessing services and information needed by library users, thanks to modern technological and technical advancements and the Internet. Every library or information center can now create its own website and provide all relevant information through it. However, despite the many advantages provided by the Internet and websites, there are some drawbacks that can affect the website, potentially leading to its shutdown and the interruption of its services. This is where the importance of cybersecurity comes in. The rapid development in information and communication technology and the Internet has led to the emergence of new types of crimes, such as cybercrimes.
Hence, the significance of the current research lies in its aim to verify the requirements for achieving cybersecurity at the Al-Assad National Library and to assess the current state of cybersecurity there, To achieve these objectives, the researcher employed the descriptive- and prepared study tools, including interviews and direct observations. The interview questions consisted of four main items: material, administrative, human, and technical requirements There was talk about the cybersecurity strategy prepared by the Ministry of Communications and Technology, which was approved by the Council of Ministers during its session held on 6/20/2023, with the aim of confronting hostile cyber intrusions, fortifying government data on the Internet and related networks, and establishing a sustainable cybersecurity structure that provides integrated protection for information assets according to their importance. It ensures the distribution of roles and the definition of powers among all parties, whether within institutions or at the national level. The study sample included officials responsible for the website and information at the Al-Assad National Library, as well as a group of experts and specialists in information technology and cybersecurity. The research concluded with a set of proposals that could contribute to the development of cybersecurity applications at the Al-Assad National Library, thereby enhancing trust between users and the institutions dealing with the library, preserving its reputation and primary role in serving the community, and safeguarding cultural and knowledge heritage, Additionally, the research proposed new strategies and procedures to enhance cybersecurity in the library and provided recommendations for improving technical infrastructure, preventive measures, and raising awareness and training employees and users through the design of training programs.

Keywords: Cybersecurity, Information Security, National Libraries, Al-Assad Library.

Received: 18/07/2024
Accepted: 16/09/2024

منهجية الدراسة:

أهمية البحث:

تأتي أهمية الدراسة الحالية من أهمية الأمن السيبراني بشكل عام وخصوصا إنه يعتبر من المواضيع الحديثة نسبياً، وقد أتت هذه الدراسة لتحديد أهمية الأمن السيبراني في المكتبات الوطنية بشكل عام وفي مكتبة الأسد الوطنية بشكل خاص باعتبارها موضوع الدراسة والتي تتخصص بحماية المعلومات الثقافية والتاريخية حيث تحتوي مكتبة الأسد الوطنية على موارد ثقافية وتاريخية هامة للبلد والمجتمع، والتي يجب حمايتها من التهديدات السيبرانية كالاختراقات والتلاعب والسرقة الإلكترونية وكذلك ضمان الوصول الآمن، وبناء الثقة والمصداقية والامتثال للقوانين والتشريعات حيث أن التعرض لهجمات سيبرانية يمكن أن يتسبب في خسائر اقتصادية وأضرار كبيرة للمكتبة باختصار يعكس البحث الحالي مدى التزام مكتبة الأسد الوطنية بحماية المعلومات وضمان الوصول الآمن إليها، مما يعزز الثقة والمصداقية ويساهم في تحقيق الأهداف الرئيسية للمكتبة كمؤسسة ثقافية وتعليمية وبحثية ،وهنا سيكون هذا البحث بمثابة اختبار حقيقي لتحديد ما متطلبات تحقيق الأمن السيبراني في مكتبة الأسد الوطنية وما هو الواقع الحالي لتطبيق الامن السيبراني فيها.

أهداف البحث:

تهدف الدراسة الى ما يلي:

- تسليط الضوء على الأمن السيبراني بشكل عام وأهميته في المكتبات الوطنية بشكل خاص.
- التعرف على نشأة وتطور وتحديثات الموقع الالكتروني الخاص بمكتبة الأسد الوطنية.
- تقديم صورة متكاملة عن واقع تطبيق الأمن السيبراني في مكتبة الأسد الوطنية.
- التعرف على متطلبات تطبيق الأمن السيبراني في مكتبة الاسد الوطنية.
- تحديد الطرق المتبعة لحماية المعلومات الحساسة من الوصول غير المصرح والسرقة الإلكترونية.
- التعرف على الوسائل المتبعة لضمان توافر المعلومات والخدمات المكتبية بشكل مستمر دون تعرضها للتعطل أو الاختراقات التي قد تؤثر على إمكانية الوصول إليها.
- تسليط الضوء على طرق حماية الأنظمة والشبكات والأجهزة المستخدمة في المكتبة من الاختراقات والهجمات السيبرانية
- التعرف على طرق ضمان سرية وخصوصية المعلومات الشخصية للمستخدمين الذين يستخدمون خدمات المكتبة الإلكترونية
- تسليط الضوء على التدابير اللازمة للتصدي للتهديدات السيبرانية المتنوعة مثل الفيروسات الإلكترونية، وبرامج التجسس، وهجمات الحجب الخدمة، وغيرها.
- تسليط الضوء على الطرق المتبعة لتعزيز وعي الموظفين والمستخدمين بشأن مخاطر الأمن السيبراني.
- تحديد البرامج المتبعة لتقديم التدريب اللازم للموظفين والمستخدمين وذلك للتعرف على الهجمات السيبرانية والتصدي
- تقديم مجموعة من المقترحات التي يمكن أن تسهم في تطوير تطبيق الأمن السيبراني في مكتبة الاسد الوطنية وكذلك تعزيز الثقة بين المستخدمين والمؤسسات المتعاملة مع المكتبة.

مشكلة البحث:

تنبع مشكلة الدراسة من ملاحظة أنّ العديد من المؤسسات ومراكز المعلومات تتعرض لهجمات واختراقات كبيرة وهذا يؤدي الى الوصول الى البيانات الخاصة بها ومنها يتم نهب المعلومات وتخريب العمل وآلياته المختلفة وهذا يؤثر سلبا على

عملية سير العمل وهنا تبرز أهمية الأمن السيبراني وهذا ما أكد علية مركز أمن المعلومات التابع للهيئة الوطنية لخدمات الشبكة حيث تم رصد عدة هجمات استهدفت مخدمات البريد الالكتروني التابعة لبعض الجهات العامة والخاصة، بالإضافة لوجود برنامج خبيث (Raccoon) الذي يصيب نظم التشغيل لذا لابد من توافر متطلبات مختلفة لحفظ أمن المعلومات والبيانات وسريتها في المؤسسات ومراكز المعلومات السورية بشكل عام وفي مكتبة الاسد الوطنية بشكل خاص وبناءً على ذلك تطرح الباحثة التساؤلات التالية:

- ماذا يقصد بمفهوم الامن السيبراني بشكل عام وما هو الفرق بينه وبين أمن المعلومات؟
- ماهي استراتيجية الامن السيبراني المتبعة في سوريا؟
- متى تمّ إنشاء الموقع الالكتروني الخاص بمكتبة الاسد الوطنية وإتاحته عبر شبكة الإنترنت، وهل تمّ تصميم الموقع على شبكة الانترنت طبقاً للمعايير الدولية لتصميم مواقع الويب؟
- ما هو الوضع الحالي للبنية التحتية للأمن السيبراني في مكتبة الأسد الوطنية؟
- ماهي نقاط القوة والضعف في الأنظمة والسياسات الحالية لاستراتيجية الامن السيبراني في مكتبة الاسد؟
- ماهي التهديدات السيبرانية المحتملة التي تواجه المكتبة؟
- هل يوجد أحداث وهجمات سيبرانية سابقة تعرضت لها المكتبة من قبل حتى نتمكن من فهم الأنماط والتقنيات المستخدمه؟
- ماهي السياسات والإجراءات الأمنية الحالية المتبعة في المكتبة وماهي مدى فعاليتها؟
- ماهي البرامج المتبعة لتعزيز وعي وتدريب الموظفين والمستخدمين؟

فروض البحث:

- إنّ التهديدات والثغرات التي تعاني منها مكتبة الأسد الوطنية تعود بسبب السياسات والإجراءات الأمنية الحالية والتي تعتبر غير كافية لحماية المكتبة من التهديدات السيبرانية الحديثة.
- كثرة المخاطر والهجمات السيبرانية التي تتعرض لها المكتبة يعود بسبب نقص التدريب والوعي الذي يمكن أن يؤدي إلى ممارسات غير آمنة وتزيد من فرص التعرض للاختراقات بالإضافة لعدم الوعي بأهمية الأمن السيبراني بين موظفي المكتبة.
- السياسات والإجراءات الأمنية الحالية في مكتبة الأسد الوطنية غير محدثة بما يكفي لمواجهة التهديدات السيبرانية الحديثة حيث أن السياسات القديمة قد لا تكون فعالة في مواجهة التهديدات السيبرانية التي تتطور باستمرار.
- يمكننا مواجهة التهديدات السيبرانية والتقليل منها في مكتبة الأسد الوطنية، وذلك ومن خلال الاستثمار في تقنيات أمنية متقدمة وتطوير سياسات فعالة يمكن أن يحسن الوضع الأمني للمكتبة.

منهج الدراسة وأدواتها:

لتحقيق أهداف الدراسة سيتمّ الاعتماد على (المنهج الوصفي التحليلي) كونه يعدّ من أكثر المناهج البحثية الملائمة لدراسة متطلبات الأمن السيبراني في مكتبة الاسد الوطنية وكذلك التعرف على الواقع الحالي، وسيتمّ ذلك من خلال الملاحظة المباشرة والمقابلة مع المسؤولين عن أمن المعلومات في مكتبة الاسد وكذلك مقابلة الأخصائيين في مجال وتكنولوجيا المعلومات والامن السيبراني لتحديد المتطلبات بدقة.

حدود الدراسة:

1-الحدود الموضوعية: الأمن السيبراني، مكتبة الاسد الوطنية، وكافة الموضوعات ذات الصلة والقريبة منها.

2-الحدود الزمانية: بداية شهر شباط من عام 2024حتى انتهاء الدراسة في منتصف شهر حزيران من عام 2024.

الدراسات السابقة:

تناولت دراسة (نبيلة الحداد. عام 2022) بعنوان "متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية: دراسة حالة" الرصد والتحليل متطلبات الامن السيبراني في المكتبات الجامعية اليمنية والتحقق من واقع الأمن السيبراني فيها ولتحقيق تلك الأهداف استخدمت الباحثة المنهج الوصفي التحليلي وكان من أهم نتائج الدراسة أن الأمن السيبراني يحافظ على أمن البيانات والمعلومات في المكتبات وسريتها ويساعد في التصدي للهجمات الخارجية.

هدفت دراسة (السمحان، منى عبد الله صال. عام 2020) بعنوان: "متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود" الى التعرف على متطلبات تحقيق الأمن السيبراني في لأنظمة المعلومات الإدارية في جامعة الملك سعود واعتمد البحث على الاستبانة لجمع المعلومات من عينة من العاملين بجامعة الملك سعود بالرياض لتعرف وجهة نظرهم حول كيفية تحقيق الأمن السيبراني بالجامعة من خلال المتطلبات: المادية والبشرية والإدارية والتقنية.

" هدفت الدراسة Venessa,Burton-Howard,V.(2018).Protecting small busniss information from cyber security criminals:A qualitive study (Doctoral dissertation ,Colorado Technical Unversity"
بعنوان "حماية المعلومات التجارية الصغيرة من مجرمي الأمن السيبراني" الى معرفة الصعوبات التي تواجه المديرين الاختصاصيين بأمن المعلومات في حماية المعلومات والبيانات التجارية، بالإضافة الى مدى حماية الملكية الفكرية من الاختراقات الأمنية والانتهاكات التي يقوم بها قراصنة الانترنت.

المقدمة:

تتمحور أهمية الامن السيبراني في مكتبة الأسد الوطنية بحماية المعلومات الثقافية والتاريخية حيث تحتوي مكتبة الأسد الوطنية على موارد ثقافية وتاريخية هامة للبلد والمجتمع، والتي يجب حمايتها من التهديدات السيبرانية كالاختراقات والتلاعب والسرقة الإلكترونية وكذلك ضمان الوصول الآمن للمعلومات يجب أن يتمكن المستخدمون من الوصول إلى موارد المكتبة بأمان دون تعريض معلوماتهم للخطر، وهذا يتطلب توفير بنية تحتية وسياسات أمنية فعاله وبناء الثقة والمصداقية حيث تسهم إجراءات الأمن السيبراني الجيدة في بناء الثقة بين المكتبة والمستخدمين، وتعزز مصداقيتها كمؤسسة تهتم بحماية خصوصية وأمان المعلومات والامتثال للقوانين والتشريعاتت حيث يتطلب الحفاظ على سلامة المعلومات الالتزام بالقوانين والتشريعات المتعلقة بالأمن السيبراني، وهنا في هذا البحث سنقوم بتحديد مدى الامتثال وتحديث السياسات والإجراءات وفقًا للمتطلبات القانونية وتجنب الأضرار الاقتصادية والسمعية حيث يمكن لتعرض لهجمات سيبرانية أن يتسبب في خسائر اقتصادية وأضرار سمعية للمكتبة، وبالتالي، يعمل البحث على تحديد وتقليل هذه المخاطر.

أولا-الأمن السيبراني (مفهومه، أهدافه، مبادئه):

1- مفهوم الأمن السيبراني وأمن المعلومات والهجمات السيبرانية:

عرفت السيبرانية بأنها: تكتب سيبراني وسيبيراني وهى صفة لما هو مرتبط بتقنية المعلومات والحواسيب وتعني فضاء الإنترنت أو العالم الافتراضي.

ويشمل مجال الأمن السيبراني العديد من التحديات والتهديدات التي تتعرض لها الأنظمة الإلكترونية والشبكات، مثل الاختراقات الهجمات الضارة، والبرامج الخبيثة، وسرقة البيانات، والقرصنة الإلكترونية، والتجسس السيبراني، والاعتداءات الإلكترونية الأخرى.

أما الأمن مفهوم السيبراني بشكل عام (Cyber Security): هو 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 والمستخدم. تشمل أصول المنظمة والمستخدم أجهزة الحوسبة المتصلة والموظفين والبنية التحتية والتطبيقات والخدمات وأنظمة الاتصالات وإجمالي المعلومات المنقولة و/أو المخزنة في البيئة السيبرانية. يسعى الأمن السيبراني إلى ضمان تحقيق وصيانة الخصائص الأمنية للمؤسسة وأصول المستخدم ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية. (فوزي ،اسلام،103،2019)

ومن وجهة نظر أخرى(يعرفه الاتحاد الدولي للاتصالات) الأمن السيبراني : بأنه مجموعة من المهمات، مثل تجميع وسائل، وسياسات، واجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر ،وتدريبات وممارسات وتقنيات، يمكن استخدامها لحماية البيئة السيبرانية. (جاب الله، عادل موسى عوض/2243،2022)

ويشمل مجال الأمن السيبراني العديد من التحديات والتهديدات التي تتعرض لها الأنظمة الإلكترونية والشبكات، مثل الاختراقات الهجمات الضارة، والبرامج الخبيثة، وسرقة البيانات، والقرصنة الإلكترونية، والتجسس السيبراني، والاعتداءات الإلكترونية الأخرى. (Caulkins. 2019).

أما بالنسبة لمفهوم أمن المعلومات: فهو حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل أو من أي خطر يهددها مثل وصول أي شخص غير مخول للوصول اليها والعبث في بياناتها والاطلاع عليها وذلك من خلال توفير الوسائل والطرق اللازمة لحمايتها من المخاطر الداخلية والخارجية وموضوع أمن المعلومات هو موضوع قديم ولكن زادت الحاجة والطلب علية مع انتشار استخدام الإنترنت والاعتماد علية في كافة مجالات الحياة مما تطلب نقل البيانات والمعلومات عبر الشبكات المتعددة. (دعدوع،2016).

هذا بالنسبة لمفهوم أمن المعلومات والامن السيبراني أما الاختلاف بينهما فهو:

أن أمن المعلومات يدرس كيفية تحقيق أمن المعلومات بمختلف أشكالها (ورقية إلكترونية)، أما الأمن السيبراني فيهتم في كيفية توفير أمن المعلومات الالكترونية فقط.

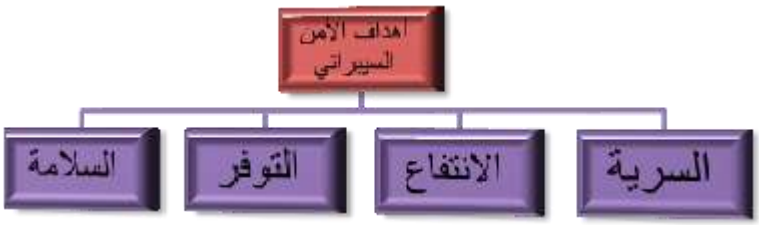
وأخيرا مفهوم الهجمات السيبرانية فتعرف: بأنها لم تكن معروفة إلا في وقت قريب وهذا ما شكل إحدى أهم التحديات الراهنة التي واجهها المختصون، وبالخصوص في تحديد طبيعتها وعناصرها. (الفتالوي، 2016، ص3).

فتعرف بأنها: الهجمات التي تشنها بعض الدول ويكون مسرحها هو الفضاء الالكتروني، بغرض إلحاق الضرر بالمنشآت والبنية التحتية والأهداف العسكرية للدولة التي تعرضت للهجوم. (قرني، أماني وأخرون،666،2022).

2- أهداف الأمن السيبراني:

هناك العديد من الأهداف المتعلقة بالأمن السيبراني والشكل رقم (1) يوضح هذه الأهداف والتي من أهمها:

الشكل رقم (1): أهداف الأمن السيبراني



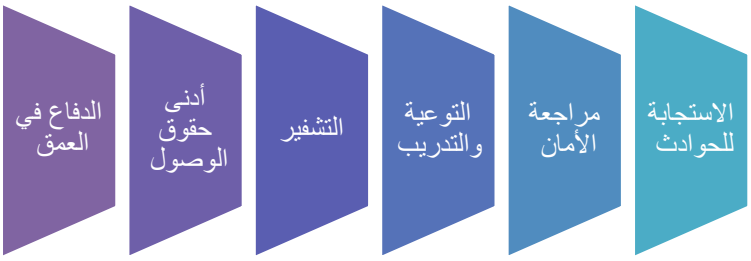
المصدر: من إعداد الباحث بالاعتماد على (Sammons and Cross. 2016).

- السرية (Confidentiality): واحدة من الأهداف الرئيسية للأمن السيبراني هي ضمان سرية البيانات والمعلومات الحساسة. يتعلق ذلك بمنع وصول غير المصرح به إلى المعلومات الحساسة وحمايتها من التسريب أو الاستخدام غير المشروع. يتطلب ذلك تنفيذ تقنيات التشفير وضمان أنظمة إدارة الهوية والوصول الصارمة.
- الانتفاع (Integrity): تهدف الأمان السيبراني أيضًا إلى ضمان سلامة البيانات والمعلومات من التلاعب أو التغيير غير المصرح به. يتعلق الأمر بالحفاظ على سلامة البيانات وضمان أنها لم تتعرض للتلاعب أو التغيير غير القانوني. يتطلب ذلك تنفيذ تقنيات الكشف عن التلاعب والتوقيع الرقمي وضبط الوصول إلى البيانات.
- التوفر (Availability): يهدف الأمن السيبراني أيضًا إلى ضمان توافر البيانات والخدمات الرقمية بشكل مستمر. يعني ذلك أن الأنظمة والشبكات والخدمات يجب أن تكون متاحة وقابلة للوصول في أي وقت عند الحاجة إليها. يتطلب ذلك تنفيذ إجراءات الاحتياطات والاستعداد للكوارث والنسخ الاحتياطي للبيانات.
- السلامة (Safety): تهدف جوانب السلامة في الأمن السيبراني إلى حماية البيانات والمعلومات من التلف أو الضياع. يشمل ذلك ضمان استمرارية العمليات والحماية من الحوادث الطبيعية أو البشرية أو الفنية التي يمكن أن تؤدي إلى تعطل الأنظمة أو فقدان البيانات.(Sammons and Cross. 2016).

3- مبادئ الأمن السيبراني:

مبادئ الأمن السيبراني هي المبادئ الأساسية التي يتم اتباعها لتحقيق الحماية والأمان في المجال السيبراني. تعتبر هذه المبادئ أساسية لتطوير استراتيجيات الأمن السيبراني وتنفيذها بشكل فعال. فيما يلي شرح مفصل لبعض مبادئ الأمن السيبراني الرئيسية (Gupta. 2018):

الشكل رقم (2): مبادئ الأمن السيبراني



المصدر: من إعداد الباحثان.

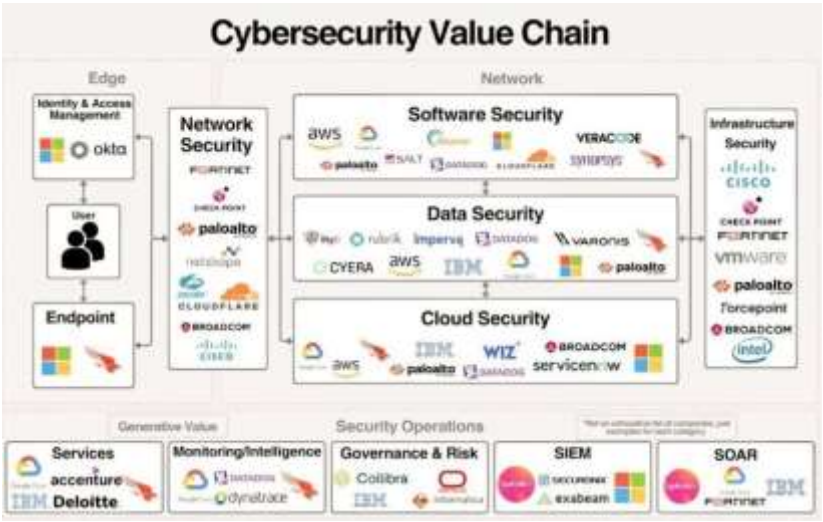
- مبدأ الدفاع في العمق (Defense in Depth): يشير هذا المبدأ إلى استخدام مجموعة متنوعة من الإجراءات الأمنية والحماية على مختلف مستويات النظام. وبدلاً من الاعتماد على إجراءات أمنية فردية، يتم تنفيذ عدة طبقات من الحماية لتقليل فرص الاختراق والتلاعب. يشمل ذلك استخدام جدران الحماية، ونظام الكشف والاستجابة للتهديدات، وتحديثات البرامج الأمنية المنتظمة، والتدريب والتوعية للموظفين.
- مبدأ أدنى حقوق الوصول (Least Privilege): يتعلق هذا المبدأ بتقديم أدنى مستوى من الامتيازات وحقوق الوصول اللازمة للمستخدمين والأنظمة لأداء وظائفهم المحددة فقط. يتم تقييد الوصول إلى الموارد الحساسة والنظم الحيوية فقط لمن يحتاجون إليها. هذا المبدأ يقلل من فرص استغلال الاختراقات من قبل المهاجمين ويحد من التأثيرات السلبية في حالة وقوع انتهاك للأمن.
- مبدأ التشفير (Encryption): يهدف هذا المبدأ إلى حماية البيانات المرسلة أو المخزنة عبر الشبكات أو الأنظمة باستخدام تقنيات التشفير. يتم تحويل البيانات إلى ترميز غير قابل للقراءة للمحافظة على سرية المعلومات ومنع الوصول غير المصرح به. يستخدم التشفير في العديد من الجوانب مثل الاتصالات اللاسلكية، والبريد الإلكتروني، وإدارة الهوية والوصول.
- مبدأ التوعية والتدريب (Awareness and Training): يعد الموظفون أحد أهم أصول أمن المعلومات. يتطلب هذا المبدأ رفع مستوى التوعية وتوفير التدريب المستمر للموظفين بشأن مخاطر الأمن السيبراني وكيفية التعامل معها. يساعد ذلك في تعزيز الوعي بأفضل الممارسات الأمنية والتصرف السليم عند التعامل مع المعلومات الرقمية.
- مبدأ مراجعة الأمان (Security Review): يتطلب هذا المبدأ إجراء مراجعات منتظمة لنظم المعلومات والتكنولوجيا المستخدمة في المؤسسة. يهدف ذلك إلى تحديد الثغرات الأمنية المحتملة وتقييم فعالية إجراءات الحماية المتبعة. يشمل ذلك تنفيذ اختبارات الاختراق والتدقيق الأمني للأنظمة والتطبيقات والشبكات.
- مبدأ الاستجابة للحوادث (Incident Response): يتعلق هذا المبدأ بتطوير استراتيجية وخطة استجابة سريعة وفعالة للتعامل مع الحوادث الأمنية والاختراقات المحتملة. يتضمن ذلك تحديد الإجراءات والتوجيهات لاستعادة النظام وتقييم التأثيرات والتحقيق في الحادث وتعزيز الحماية للمستقبل.

يجب أن يتم تنفيذ هذه المبادئ الأساسية بشكل متكامل ومتناسق لتحقيق الأمان السيبراني الشامل. إلى جانب ذلك، يجب أن تتم مراعاة القوانين واللوائح القابلة للتطبيق في المجال السيبراني وتوفير التحديثات والتطبيقات الأمنية اللازمة.(Gupta. 2018)

- المفاهيم والتقنيات التي تضمن نجاح تكامل منظومة الأمن السيبراني في الأنظمة الحديثة التقنية:
- إدارة الهوية والوصول: يشمل الإجراءات والتقنيات التي تستخدم للتحكم في من يمكنه الوصول إلى الأنظمة والمعلومات داخل المؤسسة، وذلك من خلال التحقق من هوية المستخدمين وإدارة صلاحيات الوصول.
- أمن الشبكة: يركز على حماية الشبكات من الهجمات الإلكترونية، ويشمل استخدام الجدران النارية، وأنظمة الكشف عن التسلل، والتقنيات الأخرى التي تمنع الوصول غير المصرح به وتحمي البيانات أثناء انتقالها عبر الشبكة.
- أمن البرمجيات: يتعامل مع حماية البرمجيات والتطبيقات من الثغرات الأمنية والهجمات البرمجية، من خلال فحص الأكواد البرمجية والتأكد من أنها خالية من العيوب الأمنية وتحديثها بشكل دوري.

- أمن البيانات: يركز على حماية البيانات من الضياع أو التسريب أو الوصول غير المصرح به، وذلك من خلال تقنيات التشفير، وإدارة البيانات، والسياسات التي تضمن سلامة وسرية المعلومات.
- أمن السحابة: يشمل الإجراءات والتقنيات التي تحمي البيانات والخدمات المخزنة والمستخدمة في بيئات الحوسبة السحابية، وذلك من خلال مراقبة وتأمين الوصول إلى الموارد السحابية وضمان سلامة البيانات المخزنة فيها.
- أمن البنية التحتية: يهتم بحماية البنية التحتية التقنية للمؤسسة، بما في ذلك الأجهزة والبرمجيات والشبكات التي تدعم تشغيل أنظمة المعلومات، وذلك من خلال توفير حماية شاملة ضد الهجمات والاستغلالات الأمنية.
- الخدمات: تتضمن تقديم خدمات الأمن السيبراني من قبل الشركات المتخصصة، مثل الاستشارات، والتدقيق، والتقييم الأمني للمساعدة في تحسين مستوى الأمان في المؤسسات.
- المراقبة/الذكاء: يشمل استخدام أدوات وتقنيات لمراقبة الأنظمة والشبكات بشكل مستمر للكشف عن الأنشطة غير العادية أو التهديدات، بالإضافة إلى جمع وتحليل المعلومات الأمنية لاتخاذ إجراءات استباقية.
- الحوكمة والمخاطر: يتناول وضع السياسات والإجراءات التي تضمن إدارة المخاطر الأمنية بشكل فعال، وضمان الامتثال للمعايير واللوائح الأمنية.
- إدارة معلومات الأمن والأحداث: نظام يجمع ويحلل المعلومات الأمنية من مصادر متعددة في الوقت الفعلي، للمساعدة في اكتشاف الحوادث الأمنية والتعامل معها بسرعة.
- تنسيق الأمن والأتمتة والاستجابة: يتضمن استخدام أدوات لتنسيق العمليات الأمنية وأتمته الاستجابات للحوادث الأمنية، مما يساعد في تقليل الوقت اللازم للرد على التهديدات.

مرفق أمثلة من الشركات التي تقدم هذه التقنيات والخدمات والتي تضمن تكامل عمل هذه التقنيات وتوفيرها لأعلى مستوى الأمن والحماية.(القحطاني ،مجدل ،2024).



ثانيا: مكتبة الاسد الوطنية:

1- موقع مكتبة الاسد ونشأتها:

هي المكتبة الوطنية الرئيسية في سوريا، وتقع في العاصمة دمشق، وتأسست المكتبة في عام 1984 تعد المكتبة واحدة من أهم المؤسسات الثقافية والعلمية في البلاد، وتهدف إلى جمع وتنظيم وحفظ التراث الثقافي والمعرفي السوري وتقديمه للباحثين والجمهور العام. (دياب،فردوس وأخرون،2024).

2- أهمية مكتبة الأسد الوطنية:

- حفظ التراث الثقافي :تحتفظ المكتبة بمجموعة كبيرة من المخطوطات والكتب والوثائق التي تمثل جزءًا مهمًا من التراث الثقافي والتاريخي لسوريا.
- مصدر رئيسي للبحث العلمي: توفر المكتبة موارد قيمة للباحثين والأكاديميين في مختلف المجالات العلمية والثقافية.
- دعم التعليم: تساهم المكتبة في دعم التعليم من خلال توفير مصادر معرفية متنوعة للطلاب والمعلمين.
- التوعية الثقافية: تنظم المكتبة فعاليات ومعارض وندوات تهدف إلى تعزيز الوعي الثقافي بين الجمهور .
- التعاون الدولي: تساهم المكتبة في تعزيز التعاون الثقافي والعلمي بين سوريا والدول الأخرى من خلال تبادل المعلومات وعقد الاتفاقيات.

3- الموقع الإلكتروني لمكتبة الأسد الوطنية:

يعتبر بوابة رقمية هامة للوصول إلى خدمات ومجموعات المكتبة، يهدف الموقع إلى تسهيل الوصول إلى المعلومات والموارد المختلفة التي توفرها المكتبة، كالبحث في الفهرس الالكتروني الخاص بالمكتبة.

4- محتويات الموقع الإلكتروني:

- واجهة المستخدم: تصميم سهل الاستخدام وبسيط، يتيح للزوار التنقل بسهولة بين مختلف الأقسام يتضمن خيارات بحث متقدمة للوصول الى بيانات المصدر الذي يحتاجونه.
- الفهرس الإلكتروني: يوفر الوصول إلى الفهرس الإلكتروني للمكتبة، حيث يمكن للباحثين والطلاب العثور على الكتب والوثائق المتاحة، يتضمن الفهرس بيانات مفصلة عن كل مادة، مثل العنوان، المؤلف، سنة النشر، والموضوع .
- الأخبار والفعاليات: يعرض أحدث الأخبار والمستجدات المتعلقة بالمكتبة، يتضمن جدولاً بالفعاليات والندوات والمعارض التي تنظمها المكتبة .
- خدمات المكتبة: (استفسار مكتبي، ملاحظات وشكاوى، استعلام عن دخول المكتبة، طلب خدمة مكتبية، وخدمة البحث في الفهرس الالكتروني. تم الوصول لهذه المعلومات من خلال الاعتماد على ملاحظة الباحثين للموقع وبالاعتماد على المصدر التالي. (حسن، سلام، ص282،2019).

ثالثا: أهمية الأمن السيبراني في المكتبات الوطنية:

يلعب الأمن السيبراني في المكتبات الوطنية دورًا حيويًا في حماية المعلومات والبيانات الحيوية، وضمان استمرارية الوصول إلى الخدمات والمحتويات الرقمية بشكل آمن حيث تتجلى أهمية الأمن السيبراني في المكتبات الوطنية من وجهة نظر الباحثان بالاعتماد على مصادر متخصصة بالأمن السيبراني واسقاطها على المكتبات الوطنية حيث تجلت في النقاط التالية :

1-حماية المعلومات الحساسة: تحتوي المكتبات الوطنية على مجموعات ضخمة من الوثائق التاريخية والمخطوطات والكتب النادرة، بالإضافة إلى معلومات المستخدمين حيث يضمن الأمن السيبراني حماية هذه المعلومات من الوصول غير المصرح به والسرقة الإلكترونية .

2-ضمان استمرارية الخدمات :تضمن الإجراءات الأمنية السيبرانية استمرارية عمل الأنظمة والخدمات الرقمية في المكتبات الوطنية، مما يمنع تعطل الخدمات نتيجة للهجمات الإلكترونية مثل هجمات حجب الخدمة.

3- حماية الخصوصية: يحمي الأمن السيبراني خصوصية المستخدمين من خلال تأمين البيانات الشخصية والحساسة، ومنع الوصول غير المصرح به أو تسريب البيانات .

4-الامتثال للقوانين واللوائح: يساهم التزام المكتبات الوطنية بالمعايير القانونية والتشريعية المحلية والدولية المتعلقة بحماية البيانات والأمن السيبراني، مما يقلل من مخاطر العقوبات القانونية

5-الثقة والمصداقية :يعزز الأمن السيبراني الثقة بين المكتبة والجمهور، حيث يشعر المستخدمون بالأمان أثناء استخدامهم لخدمات المكتبة الرقمية، مما يزيد من الإقبال على الاستفادة من موارد المكتبة.

6-منع التهديدات السيبرانية: تساعد استراتيجيات الأمن السيبراني الفعالة في الكشف المبكر عن التهديدات السيبرانية والتصدي لها قبل أن تتسبب في أضرار جسيمة، سواء كانت تهديدات داخلية أو خارجية.

7-الحفاظ على سمعة المكتبة :الحوادث السيبرانية يمكن أن تؤدي إلى أضرار بالغة في سمعة المكتبة الوطنية. من خلال تأمين الأنظمة والمعلومات، يمكن الحفاظ على سمعة المكتبة كمؤسسة موثوقة وآمنة .

8-دعم الأبحاث والدراسات :تتيح حماية المعلومات والدراسات المخزنة في المكتبات الوطنية للباحثين والعلماء الوصول الآمن إلى مواردهم دون مخاطر تعطل أو سرقة البيانات، مما يدعم البحث العلمي ويعزز المعرفة.

9-تعزيز التوعية والتعليم :يمكن أن تلعب المكتبات الوطنية دورًا في زيادة الوعي بأهمية الأمن السيبراني من خلال تقديم ورش عمل وبرامج تعليمية، مما يسهم في بناء مجتمع أكثر وعيًا واستعدادًا لمواجهة التهديدات السيبرانية .

وأخيراً تعتبر المكتبات الوطنية مستودعات للمعرفة والثقافة، وأمنها السيبراني ضروري للحفاظ على هذه الأصول القيمة، من خلال تنفيذ استراتيجيات فعالة للأمن السيبراني، تضمن المكتبات الوطنية حماية معلوماتها وخدماتها، وتعزز ثقة المستخدمين، وتضمن الامتثال للقوانين، وتدعم البحث والتعليم المستدامين.

رابعا: الاستراتيجية الوطنية للأمن السيبراني التي أعدتها وزارة الاتصالات والتقانة السورية:

اصدر السيد الرئيس الدكتور بشار الأسد القانون رقم (20) للعام 2022 القاضي بإعادة تنظيم القواعد القانونية الجزائية للجريمة المعلوماتية التي تضمنها المرسوم التشريعي رقم(17) للعام 2012، وقد اعتمد مجلس الوزراء خلال جلسته المنعقدة بتاريخ 2023/6/20 استراتيجية للأمن السيبراني التي أعدتها وزارة الاتصالات والتقانة بهدف التصدي للاختراقات السيبرانية المعادية وتحصين البيانات الحكومية على شبكة الانترنت والشبكات المتصلة بها وتأسيس بنية أمن سيبراني مستدامة توفر

الحماية المتكاملة للأصول المعلوماتية وفقا لأهميتها ،ويضمن توزيع الادوار وتحديد الصلاحيات بين جميع الأطراف سواء داخل المؤسسات أو على المستوى الوطني، وتتحدد أهداف هذه الاستراتيجية في:

أ. تأسيس بنية أمن سيبراني قوية ومستدامة توفر الحماية الكاملة.

ب. ادارة فعالة ومتكاملة لمواجهة التهديدات والتصدي للمخاطر على مستوى سورية، وتطوير القوالب التنظيمية والتشريعية ووضع القواعد القانونية الملائمة.

ت. تطوير وصقل الامكانات الوطنية والبشرية والتقنية وتشجيع الابحاث والتحقيقات والبحث العلمي في هذا المجال وتعزيز التنسيق والتعاون.

أما بالنسبة لبرامج الاستراتيجية:(أمن البنى التحتية، تطوير الإطار القانوني والتنظيمي، نشر ثقافة الوعي السيبراني، بناء القدرات والمعرفة الشراكات والتعاون الاقليمي والدولي تطوير هياكل وظيفية متخصصة). (وزارة الاتصالات والتقانة ،2023).

خامسا: الوضع الحالي للأمن السيبراني في مكتبة الأسد الوطنية:

إنّ مكتبة الأسد الوطنية، كما هو الحال في أي مؤسسة حديثة تتعامل مع المعلومات الرقمية، لذلك يُعد الأمن السيبراني جزءًا أساسيًا من استراتيجيات الحماية، فبعد القيام بإجراء المقابلة مع المسؤولين عن الموقع وإدارته وتحديثه في مكتبة الأسد الوطنية تم التوصل الى مجموعة المعلومات التالية:

1-البنية التحتية التكنولوجية: مكتبة الأسد الوطنية تعتمد على بنية تحتية تكنولوجية تتضمن أنظمة حاسوبية وشبكات وأجهزة تخزين للمعلومات، هذه البنية التحتية تدعم تقديم خدمات المكتبة المختلفة، من إدارة المجموعات والبحث ضمن الفهرس الالكتروني.

2-إجراءات حماية البيانات: تعتمد المكتبة على مجموعة من الإجراءات الأمنية الأساسية لحماية البيانات التي توفرها الشركة العامة للاتصالات، لحماية الشبكات لكن بشكل بسيط وغير متطور ولا يوجد بروتوكولات تشفير البيانات الحساسة أثناء نقلها وتخزينها.

3-التحكم بالوصول: استخدام أنظمة إدارة الهوية والوصول (IAM) للتحكم في وصول المستخدمين إلى الموارد المختلفة داخل المكتبة، وتطبيق سياسات كلمة المرور القوية وعزل الشبكة الداخلية بالإضافة للنسخ الاحتياطي.

4-التحديثات والصيانة: يتم تحديث الموقع والبرمجيات بشكل دوري بحسب ماهو متوفر لدى المسؤولين عن ذلك لكن هذا المتوفر شيء بسيط ولا يتناسب مع مكتبية كبيرة ومهمة ك مكتبة الأسد.

5-وعي إداري :إدراك الإدارة العليا لأهمية الأمن السيبراني واتخاذ خطوات لتحسين الوضع الأمني، لكن لعدم توفر الميزانية لا يمكن تحديث الأنظمة وتنفيذ السياسات الأمنية.

6- تطبيق تقنيات أساسية: لا يوجد تقنيات أمنية أساسية مثل جدران الحماية وأنظمة كشف التسلل .

7- تحديات التحديث: تتأخر بعض الأنظمة في الحصول على التحديثات الأمنية اللازمة، مما يجعلها عرضة للثغرات والهجمات السيبرانية، وبالتالي صعوبة مواكبة التهديدات السيبرانية المتطورة بشكل مستمر.

8-نقص التدريب :الحاجة إلى برامج تدريب وتوعية متقدمة للموظفين والمستخدمين حول أهمية الأمن السيبراني وأساليب الحماية، فمن خلال المقابلات التي تمت مع الكادر الوظيفي لاحظنا الوعي بين بعض الموظفين حول السياسات الأمنية

والإجراءات الصحيحة للتعامل مع البيانات بالإضافة الى ان المسؤولين عن الموقع موظفين اثنين أحدهم يحمل الشهادة الثانوية ولكنه لدية خبرة لمدة عشر سنوات بالعمل على المواقع وادارتها والموظف الثاني هندسة معلوماتية.

9-إجراءات استجابة الطوارئ: عند الوصول الى هذا المحور كانت الاستجابة عبارة عن وجود نسخة احتياطية يتم العمل عليها حتى يتم استعادة الموقع عند التعرض للاختراق ؟،وقد تبين انّ موقع المكتبة تعرض للإختراق في عام 2012 لكن تم استرجاعه بعد عدة ساعات هذا وكما ذكرت المسؤولة عن ادارة الموقع.

10- الهجمات السيبرانية:

- الفدية: هي تهديدات تتضمن تشفير البيانات وطلب فدية مقابل فك التشفير، مما يعطل خدمات المكتبة.
- البرمجيات الخبيثة: برمجيات ضارة تستهدف الأنظمة بهدف سرقة البيانات أو تخريب الأنظمة.
- الهجمات الداخلية: تهديدات من داخل المكتبة، مثل الموظفين غير الراضين أو الذين لديهم وصول غير مصرح به للأنظمة الحساسة.

تضمن هذه الإجراءات مجتمعاً سيبرانياً آمناً داخل مكتبة الأسد الوطنية، وتحمي المعلومات والموارد الرقمية من التهديدات المختلفة لكن ليست بنفس الدرجة المتوقعه أو المطلوبة وخصوصا كمكتبة مثل مكتبة الأسد الوطنية.

خامسا: متطلبات تطبيق الامن السيبراني في مكتبة الاسد الوطنية:

أنّ تطبيق الأمن السيبراني بشكل ممتاز في مكتبة الأسد الوطنية يتطلب تحقيق مجموعة من المتطلبات المادية والإدارية والبشرية والتقنية، وفيما يلي تفصيل لكل من هذه المتطلبات بحسب رأي الباحثان وأخصائي الأمن السيبراني اللذين تم التواصل معهم لتحديد مقترحاتهم حول متطلبات تطبيق الأمن السيبراني في مكتبة الاسد الوطنية:

1- المتطلبات المادية:

- الميزانية: تخصيص ميزانية كافية لشراء وتحديث البرمجيات والأجهزة الأمنية وذلك لتمويل البرامج التدريبية والتوعوية للموظفين والمستخدمين.
- الأجهزة والمعدات: شراء أجهزة الحاسوب المتقدمة والخوادم التي تدعم تطبيقات الأمن السيبراني توفير أجهزة الحماية المادية مثل كاميرات المراقبة وأنظمة التحكم في الوصول.
- البنية التحتية الشبكية: تحديث وتوسيع البنية التحتية الشبكية لتدعم حلول الأمن السيبراني المتقدمة وتوفير خطوط إنترنت عالية السرعة واتصالات آمنة.

2- المتطلبات الإدارية:

- السياسات والإجراءات: وضع سياسات واضحة للأمن السيبراني تشمل جميع الجوانب المتعلقة بحماية البيانات وإدارة الحوادث وتطوير إجراءات استجابة الطوارئ وخطط الطوارئ للحوادث السيبرانية.
- الهيكل التنظيمي: تعيين فريق مختص بالأمن السيبراني يتضمن مدير أمن المعلومات ومسؤولي أمن السيبراني، تحديد صلاحيات ومسؤوليات واضحة للفريق الأمني.
- الإدارة والمراقبة: تطبيق نظام إدارة أمن المعلومات (ISMS) لضمان استمرارية تحسين إجراءات الأمن السيبراني، تنظيم اجتماعات دورية لمراجعة حالة الأمن السيبراني واتخاذ القرارات اللازمة.

3- المتطلبات البشرية:

- التدريب والتوعية: تنظيم ورش عمل وبرامج تدريبية مستمرة للموظفين لزيادة وعيهم بمخاطر الأمن السيبراني وأساليب الحماية، تقديم برامج توعية للمستخدمين حول أهمية الأمن السيبراني وكيفية حماية بياناتهم الشخصية.
- التوظيف والتأهيل: توظيف خبراء في مجال الأمن السيبراني وتقنية المعلومات، وتوفير برامج تدريبية متقدمة لشهادات معترف بها في مجال الأمن السيبراني (مثلCISSP، CEH).
- التعاون والتنسيق: تعزيز التعاون بين الأقسام المختلفة داخل المكتبة لضمان تطبيق سياسات الأمن السيبراني بشكل متكامل، بناء شراكات مع مؤسسات أخرى للحصول على الدعم والخبرات في مجال الأمن السيبراني.

4- المتطلبات التقنية:

- البرمجيات والحلول الأمنية: استخدام برامج الحماية من الفيروسات وبرامج مكافحة البرمجيات الخبيثة وتطبيق حلول التشفير لحماية البيانات أثناء النقل والتخزين.
- أنظمة الحماية الشبكية: استخدام جدران الحماية (Firewalls) وأنظمة كشف التسلل (IDS) وأنظمة منع التسلل، (IPS) تطبيق تقنيات الشبكة الافتراضية الخاصة (VPN) لتأمين الاتصالات الخارجية.
- إدارة الوصول والهوية: نفيذ نظام إدارة الهوية والوصول (IAM) لضمان الوصول المصرح به فقط للموارد الحساسة، استخدام تقنيات المصادقة متعددة العوامل (MFA) لتعزيز أمان الحسابات.
- إدارة الحوادث والاستجابة: تطبيق نظام إدارة الحوادث الأمنية (SIEM) لمراقبة الأنشطة وتحليل الحوادث الأمنية، وتطوير وتحديث خطط الاستجابة للحوادث السيبرانية وإجراء تدريبات دورية لمحاكاة الهجمات.
- التحديث والصيانة: التأكد من تحديث جميع الأنظمة والبرمجيات بانتظام لسد الثغرات الأمنية وتنفيذ جداول صيانة دورية للبنية التحتية التقنية لضمان استمرارية الأداء الفعال.

النتائج:

توصلت الدراسة الحالية الى مجموعة من النتائج الهامة والتي تتجلى في عدة نقاط وهي:

1- تبذل مكتبة الأسد الوطنية جهودًا لتحسين الوضع الأمني، لكنها لا تزال تعاني من بعض التحديات التي تحتاج إلى مواجهة، من خلال تعزيز الوعي، وتحديث الأنظمة، وتطوير خطط استجابة فعالة، يمكن للمكتبة تحقيق مستوى أعلى من الأمان السيبراني وحماية مواردها القيمة من التهديدات المتزايدة.

2- لايوجد سياسات دورية لتحديث الأنظمة والبرمجيات المستخدمة في المكتبة لضمان الحماية من الثغرات الأمنية المعروفة بالإضافة الى أنه لايوجد صيانة دورية للبنية التحتية التقنية لضمان استمرارية العمل وكفاءة الأنظمة بالشكل المرموق لمكتبة الأسد.

3- حتى نستطيع تحقيق أمن سيبراني فعال في مكتبة الأسد الوطنية يتطلب توافر مجموعة متكاملة من المتطلبات المادية والإدارية والبشرية والتقنية، من خلال تلبية هذه المتطلبات، يمكن للمكتبة حماية بياناتها ومواردها وضمان تقديم خدمات آمنة وفعالة للمستخدمين.

4- الحاجة الى تغيير أوتدريب الكادر الوظيفي المسؤول عن ادارة الموقع وحمايته والعمل على تدريبه في مجال حماية البيانات والمعلومات.

التوصيات:

1–تعزيز الوعي والتدريب :تنظيم ورش عمل وبرامج تدريبية للموظفين حول الأمن السيبراني والممارسات الأمنية الجيدة.

2–تحديث الأنظمة: تخصيص ميزانية لتحديث الأنظمة والبنية التحتية التكنولوجية بشكل دوري واعتماد حلول أمنية متقدمة مثل أنظمة إدارة الحوادث الأمنية (SIEM) وأنظمة الحماية المتقدمة من التهديدات.

3–تطوير خطة استجابة الطوارئ: وضع خطة شاملة للاستجابة للطوارئ السيبرانية والهجمات المحتملة، وإجراء تدريبات منتظمة لمحاكاة الهجمات واختبار جاهزية الأنظمة.

4–تعزيز التعاون مع مؤسسات أخرى: التعاون مع مكتبات وطنية ودولية أخرى لتبادل الخبرات وأفضل الممارسات في مجال الأمن السيبراني، والمشاركة في شبكات ومنتديات الأمن السيبراني للحصول على آخر المستجدات والتطورات .

المراجع:

المراجع العربية:

1. جاب الله، عادل موسى عوض.2022. وسائل حماية الأمن السيبراني.–مصر: جامعة ام القرى، العدد الرابع والثلاثون الإصدار الأول يناير 2022،ج3.
2. حسن، سلام.(2019). دراسة تحليلية تقييمه لعينه مختارة من المواقع الثقافية السورية على الشبكه العنكبوتيه، المجلد 79، عدد يناير علوم اجتماعية، الصفحة 254–288.
3. الحداد، نبيلة. عام 2022.(متطلبات تحقيق الأمن السيبراني في المكتبات الجامعية اليمنية :دراسة حالة). اليمن: جامعة البيضاء (مجلة جامعة البيضاء).
4. دعدوع، شهيرة.(2016). مفهوم أمن المعلومات. متاح عبر الرابط: https://mawdoo3.com
5. الفتلاوي، أحمدأبيس.(2016).الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر. المحقق الحلي للعلوم القانونية والسياسية،3.
6. فوزي، إسلام. عام (2019).(الأمن السيبراني: الأبعاد الاجتماعية والقانونية تحليل سوسيولوجي). مصر، المجلة الاجتماعية القومية،ع2(مقالة الكترونية).
7. قرني، أماني حمدي، وخطاب، إيمان عبد المنعم. (2022). دور مواقع الإعلام الرقمي في حماية الأمن السيبراني: دراسة تحليلية لعينة من المواقع الخاصة بالأمن السيبراني.–المجلة المصرية لبحوث الإعلام.– العدد 80،ج2.
8. القحطاني، مجدل. عام (2024).–سلسة مفاهيم متعلقة بالأمن السيبراني.–متاح عبر الرابط: https://www.linkedin.com/posts/dr-mejdal_%D9%85%D8%A7%D9%87%D9%8A-%D8%B3%D9%84%D8%B3%D9%84%D8%A9-%D8%A7%D9%84%D9%85%D9%81%D8%A7%D9%87%D9%8A%D9%85-%D9%88%D8%A7%D9%84%D8%AA%D9%82%D9%86%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%AA%D9%8A-%D8%AA%D8%B6%D9%85%D9%86-%D9%86%D8%AC%D8%A7%D8%AD-activity-7210734438341615616-ezMX
9. دياب، مها، ودياب، فردوس.(2024). مكتبة الأسد الوطنية.. بيت للعلم والأدب ونافذة على عوالم المعرفة.–دمشق: صحيفة الثورة.–متاح عبر الرابط: https://thawra.sy/?p=529677 ،تاريخ الدخول 2024/6/5.
10. وزارة الاتصالات والتقانة السورية.(2023).–اعتماد استراتيجية الأمن السيبراني في سورية.–متاح عبر الرابط: https//www.moct.gov.sy/news-0121

المراجع الأجنبية:

1. Sammons, J., & Cross, M. (2016). The basics of cyber safety: Computer and mobile device safety made easy. Elsevier.
2. Caulkins, B., Marlowe, T., & Reardon, A. (2019). Cybersecurity skills to address today's threats. In Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA9 (pp. 187-192). Springer International Publishing.
3. Gupta, B. B. (Ed.). (2018). Computer and cyber security: principles, algorithm, applications, and

perspectives. CRC Press.