HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

مجلة العلوم الإنسانية والطبيعية
مجلة علمية محكمة (التصنيف: NSP)
معامل التأثير للعام 2022 = 4.91

عنوان البحث

استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الالكترونية في البلديات

معن نايل محمود المعايطة[1]

[1] وزارة الادارة المحلية، بلدية الكرك الكبرى، الأردن.

HNSJ, 2024, 5(4); https://doi.org/10.53796/hnsj54/24

تاريخ النشر: 2024/04/01م تاريخ القبول: 2024/03/15م

المستخلص

هدفت الدراسة الى بيان الأمن السيبراني ودوره في تعزيز حماية الشبكات الالكترونية في البلديات وقد تناولت الدراسة أهمية الأمن السيبراني مفهومه وعناصره , كذلك أكدت الدراسة على ان حماية امن المعلومات أصبح ضرورة باعتبار ان اختراق المعلومات يشكل خطر على مؤسسات الدولة والأفراد والبلدات مما يهدد البيانات والشيكات الالكترونية ,

واعتمدت الدراسة على استخدام المنهج الوصف لدراسة الظواهر الاجتماعية والامنية , حيث تقوم الدِّراسة على توظيف هذا المنهج لبيان الأمن السيبراني ودوره في تعزيز حماية الشبكات الالكترونية في البلديات

وقد توصلت الدراسة الى مجموعة من النتائج والتوصيات, حيث أكدت الدراسة على أهمية التعاون والتنسيق بين الحكومات والقطاع الخاص والمؤسسات الدولية في مجال الأمن السيبراني، حيث يمكن أن يساهم هذا التعاون في تبادل المعلومات وتطوير السياسات والتشريعات اللازمة لمكافحة التهديدات السيبرانية بشكل فعال. وأوصت الدراسة بأنه على البلديات تحقيق أمان البيانات والحفاظ على استقرار الأنظمة والخدمات المقدمة للمواطنين , من خلال وضع إستراتيجية وسياسات وإجراءات أمنية صارمة تنظم استخدام الأنظمة والبيانات والموارد في البلدية.

الكلمات المفتاحية: الامن السيبراني , حماية الشبكات الالكترونية, البلديات

RESEARCH TITLE

CYBERSECURITY STRATEGIES AND THEIR ROLE IN ENHANCING THE PROTECTION OF ELECTRONIC NETWORKS IN MUNICIPALITIES

Ma,an Nayel Mahmoud Al-Maayta[1]

[1] Ministry of Local Administration / Greater Karak Municipality, Jordan.

HNSJ, 2024, 5(4); https://doi.org/10.53796/hnsj54/24

Published at 01/04/2024 **Accepted at 15/03/2024**

Abstract

The study aimed to explain cybersecurity and its role in enhancing the protection of electronic networks in municipalities. The study addressed the importance of cybersecurity, its concept and its elements. The study also emphasized that protecting information security has become a necessity, given that information penetration poses a threat to state institutions, individuals, and towns, which threatens electronic data and checks.

The study relied on the use of the descriptive approach to study social and security phenomena, as the study is based on employing this approach to explain cybersecurity and its role in enhancing the protection of electronic networks in municipalities.

The study reached a set of results and recommendations, as the study emphasized the importance of cooperation and coordination between governments, the private sector and international institutions in the field of cybersecurity, as this cooperation can contribute to the exchange of information and the development of policies and legislation necessary to combat cyber threats effectively. The study recommended that municipalities must achieve data security and maintain the stability of systems and services provided to citizens, by developing a strict security strategy, policies and procedures that regulate the use of systems, data and resources in the municipality.

Key Words: cybersecurity, protection of electronic networks, municipalities

المقدمة

تزايدت أهمية الأمن السيبراني بشكل كبير مع تطور التكنولوجيا وانتشار استخدام الإنترنت والتحول الرقمي في مختلف جوانب الحياة اليومية، مما جعل الأنظمة الإلكترونية عرضة لمختلف أنواع الهجمات والتهديدات. ويشير مصطلح الأمن السيبراني إلى حماية الأنظمة الإلكترونية والشبكات والبيانات من الهجمات الإلكترونية والتهديدات السيبرانية. يعتبر الأمن السيبراني جزءاً حيوياً من الأمن الشامل للدول والمؤسسات والأفراد في عصر الاتصالات الرقمية.

وتشمل التهديدات السيبرانية مجموعة متنوعة من الهجمات مثل البرامج الضارة والتصيد الاحتيالي والاختراقات السيبرانية والتصيد السيبراني والتصيد الاجتماعي والهجمات الموزعة للخدمة بالإضافة إلى التجسس الإلكتروني وسرقة البيانات والاختراقات الهندسية الاجتماعية.

وتعتمد استراتيجيات الأمن السيبراني على مجموعة من الإجراءات والتقنيات والسياسات التي تهدف إلى حماية الأنظمة والبيانات، وتشمل ذلك استخدام تقنيات التشفير والتحقق الثنائي للعوامل وتطبيق السياسات الأمنية وتحديث البرمجيات بانتظام وتدريب الموظفين على ممارسات الأمان الجيدة.بالإضافة إلى ذلك، يعتبر التعاون والتنسيق بين الحكومات والقطاع الخاص والمؤسسات الدولية أمراً بالغ الأهمية في مجال الأمن السيبراني، حيث يمكن أن يساهم هذا التعاون في تبادل المعلومات وتطوير السياسات والتشريعات اللازمة لمكافحة التهديدات السيبرانية بشكل فعال.

وتعد حماية الشبكات الإلكترونية جزءاً حيوياً من الأمن السيبراني، حيث تهدف إلى حماية البيانات والأنظمة الإلكترونية من التهديدات والهجمات الإلكترونية المحتملة.ويعد تأمين الشبكات الإلكترونية أمراً بالغ الأهمية في عصر التكنولوجيا الرقمية، حيث يتزايد التنوع والتعقيد للهجمات السيبرانية باستمرار. ومن خلال استخدام تقنيات وإجراءات الحماية المناسبة، يمكن للبلديات تقليل مخاطر التعرض للهجمات والاختراقات الإلكترونية وحماية البيانات الحساسة والأصول الرقمية. حيث تعتمد فعالية حماية الشبكات الإلكترونية على مزيج من التقنيات والسياسات والإجراءات، ويجب تطبيقها بشكل متكامل ومنتظم لضمان حماية البيانات والأنظمة بشكل فعال في ظل التهديدات المتزايدة في عالم الإنترنت.

مشكلة الدراسة : تبرز إشكالية الدراسة في بحث موضوع استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الالكترونية في البلديات , حيث هناك عدة تحديات ومشكلات قد تواجه دراسة استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الإلكترونية في البلديات، ومن هذه المشكلات ابرزها نقص الموارد المالية والبشرية, وقلة الوعي الأمني والقيود التشريعية والتنظيمية والتهديدات الجديدة والمتطورة: تتطور التهديدات السيبرانية باستمرار، مما يعني أن البلديات يجب أن تكون على اطلاع دائم بأحدث التقنيات والأساليب لمواجهة هذه التهديدات بفعالية. ويجب أن تكون هناك استراتيجيات واضحة ومتكاملة للتعامل مع التهديدات السيبرانية وحماية البيانات والأنظمة الإلكترونية في البلديات، ويجب تحديث هذه الاستراتيجيات بانتظام لمواكبة التطورات التكنولوجية والتهديدات الجديدة.

أهمية الدراسة : تبرز أهمية الدراسة من نطاقين علمي وعملي

الأهمية العلمية : قد تشكل أهمية البحث نقله نوعية في المعرفة عن استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الالكترونية في البلديات ,و التي قد تفيد المكتبات الوطنية ومراكز البحث والمكتبات الأردنية والعربية لمعرفة أهمية الأمن السيبراني .

الأهمية العملية : حيث تبرز اهمية استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الالكترونية في البلديات وما قد يشكله التهديد السيبراني الالكتروني من مخاطر على الشبكة الالكترونية , لذا أصبحت الحاجة الى منظومة امنية الكترونية تكافح الغزو الكتروني والحفاظ على سرية البيانات، وسلامة الأنظمة، وتوفير للخدمات الرقمية

أهداف الدراسة : سعت الدراسة لبيان الأهداف التالية :

1. بيان أهمية الأمن السيبراني مفهومه عناصره أهدافه
2. التعرف على كيفية حماية الشبكات الالكترونية
3. بيان أهمية الأمن السيبراني في حماية بيانات البلديات

أسئلة الدراسة : سعت الدراسة للاجابة على التساؤلات التالية :

1. ما أهمية الأمن السيبراني, وما مفهومه وعناصره وأهدافه؟
2. كيف يمكن حماية الشبكات الالكترونية ؟
3. ما أهمية الأمن السيبراني في حماية بيانات البلديات ؟

منهجية الدراسة: استخدمت الدراسة المنهج الوصفي التحليلي كطريقة لدراسة الظواهر أو المشكلات العلمية من خلال القيام بالوصف بطريقة علمية، لتحليل الظواهر الاجتماعية الأمنية ومن ثم الوصول إلى تفسيرات منطقية لها دلائل وبراهين تمنح الباحث القدرة على تحليل وتفسير استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الالكترونية في البلديات

مصطلحات الدراسة

الامن السيبراني : هو مجموعة من الإجراءات والتقنيات والسياسات التي تهدف إلى حماية الأنظمة الإلكترونية والشبكات والبيانات من التهديدات السيبرانية والهجمات الإلكترونية. ويهدف الأمن السيبراني إلى الحفاظ على سرية البيانات، وسلامة الأنظمة، وتوفير للخدمات الرقمية..[1]

حماية الشبكات الإلكترونية: تعني مجموعة من السياسات والإجراءات والتقنيات التي تهدف إلى حماية البنية التحتية للشبكات والأجهزة والبيانات من التهديدات السيبرانية والهجمات الإلكترونية. يتضمن ذلك الحفاظ على سلامة الشبكات والحماية من الاختراقات وضمان الاستجابة الفعالة للتحديات الأمنية.[2]

البلدية : هي وحدة إدارية محلية تتولى إدارة شؤون المدينة أو البلدة التابعة لها. تعتبر البلديات من الجهات الحكومية المحلية المسؤولة عن تقديم الخدمات الأساسية للمواطنين على المستوى المحلي، وتشمل هذه الخدمات مجموعة واسعة من المجالات مثل البنية التحتية والصحة والتعليم والبيئة والتخطيط الحضري والسياحة والثقافة والرياضة والحوكمة المحلية.[3]

المبحث الأول : الأمن السيبراني مفهومه عناصره أهدافه

الأمن السيبراني يعني الجهود المبذولة لحماية الأنظمة الإلكترونية والشبكات والبيانات من التهديدات السيبرانية. ويتكون مفهوم الأمن السيبراني من عدة عناصر ويهدف إلى تحقيق أهداف محددة وتبرز عناصر الأمن السيبراني:بالسرية والتي تتعلق بالحفاظ على سرية البيانات ومنع الوصول غير المصرح بها. والسلامة التي تهدف إلى ضمان صحة وموثوقية البيانات ومنع التلاعب بها. وضمان توافر البيانات والخدمات عند الحاجة.[4]

اولا :مفهوم الأمن السيبراني

الأمن السيبراني يشير إلى مجموعة من التقنيات والسياسات والإجراءات التي تهدف إلى حماية الأنظمة الإلكترونية والبيانات من التهديدات السيبرانية والهجمات الإلكترونية. يهدف الأمن السيبراني إلى الحفاظ على سلامة البيانات، وسرية

[1] – الخزاعله , عبير (2021). مفهوم الأمن السيبراني, موقع موضوع , 17, تشرين ثاني , الاردن.

[2] – الدماطي, رامي عبداللطيف(2016). أمن شبكات المعلومات الإلكترونية ,مركز الجزيرة للدراسات,29,تشرين اول, قطر.

[3] – يارا ,تعامرة(2017). تعريف البلدية, موقع موضوع , 4, تموز , الاردن.

[4] – البهي , رغدة (2019). "الردع السيبراني: المفهوم والإشكاليات والمتطلبات, المركز الديمقراطي العربي. 10, اب, برلين.

المعلومات، وسلامة الأنظمة، وتوفير التوافرية للخدمات الرقمية. وتشمل مجالات الأمن السيبراني عدة جوانب تقنية وسياسية تتعلق بحماية البيانات والأنظمة، من ابرزها:[5]

1. حماية البنية التحتية الرقمية: وتتضمن ذلك حماية الشبكات والخوادم والأجهزة الإلكترونية من الاختراقات والهجمات السيبرانية.
2. تشفير البيانات: وهو عملية تحويل البيانات إلى صيغة غير قابلة للقراءة إلا بواسطة الأشخاص المصرح لهم، مما يحمي البيانات من الاستيلاء عليها أثناء النقل أو التخزين.
3. إدارة الهوية والوصول: وتتمثل في تحديد من يمكنه الوصول إلى البيانات والأنظمة، وتطبيق سياسات الوصول المناسبة.
4. الكشف عن الاختراق والاستجابة: وهو عملية رصد الأنشطة غير المعتادة في النظام والتعرف على محاولات الاختراق والتصدي لها والاستجابة بشكل فوري للتهديدات.
5. توعية الأمان السيبراني: وتشمل تثقيف المستخدمين بممارسات الأمان الجيدة والتصرف الآمن عبر الإنترنت.

وقد تزايدت أهمية الأمن السيبراني مع تزايد التكنولوجيا واعتماد المجتمع على الإنترنت في مختلف جوانب الحياة. تقدم التهديدات السيبرانية تحديات جديدة باستمرار، وتتطلب استراتيجيات وتقنيات متطورة للتصدي لها وحماية البيانات والأنظمة الحيوية. [6]

ثانيا :أهمية الأمن السيبراني

تبرز أهمية الأمن السيبراني في عدة جوانب تتعلق بالحماية الشاملة للأنظمة الإلكترونية والبيانات، وتشمل على النحو التالي:

1. حماية البيانات الحساسة: يعتبر الأمن السيبراني أساسيًا لحماية البيانات الحساسة والمعلومات الهامة من الاختراقات والتسريبات غير المصرح بها.
2. ضمان استمرارية الأعمال: توفير الحماية للأنظمة الحيوية والمهمة يساعد في ضمان استمرارية الأعمال والخدمات الأساسية دون انقطاعات غير مرغوب فيها.
3. الحفاظ على سمعة المؤسسات: تعزيز الأمان السيبراني يسهم في الحفاظ على سمعة المؤسسات والشركات وتفادي التسريبات السلبية التي قد تؤثر سلبًا على سمعتها.
4. تعزيز الثقة الرقمية: يساعد الأمن السيبراني في تعزيز الثقة بين المستخدمين والعملاء عبر الإنترنت، مما يؤدي إلى تعزيز الاستخدام الآمن للتكنولوجيا الرقمية.
5. منع الخسائر المالية: يمنع الأمن السيبراني الهجمات الإلكترونية التي قد تتسبب في خسائر مالية كبيرة نتيجة للتعطيلات في الخدمات أو سرقة المعلومات الشخصية.
6. الامتثال للتشريعات والتنظيمات: يساعد الأمن السيبراني على الامتثال للتشريعات والتنظيمات القانونية المتعلقة بحماية البيانات الشخصية والمعلومات الحساسة.

لذلك يمثل الأمن السيبراني عنصرًا حيويًا في العصر الرقمي الحالي، حيث يلعب دورًا حاسمًا في حماية البيانات والأنظمة

[5] – بوغرارة يوسف(2018). "الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري". مجلة الدراسات الإفريقية وحوض النيل, مصر

[6] – Newman, E. (2016). Human Security: Reconciling Critical Aspirations with Political 'Realities'. British Journal of Criminology Advance Access, 56(6), 1165–1183.

وضمان استمرارية الأعمال وبناء الثقة بين المستخدمين عبر الإنترنت[7]

ثالثا : عناصر الأمن السيبراني

اما عناصر الأمن السيبراني فتشمل مجموعة من الأساليب والتقنيات والسياسات التي تعمل معًا لضمان حماية الأنظمة الإلكترونية والبيانات من التهديدات السيبرانية. وتشمل هذه العناصر الأساليب التالية :[8]

1. التحليل الأمني والتقييم: يتضمن هذا العنصر تقييم وتحليل الثغرات الأمنية في البنية التحتية للشبكة والتطبيقات والأجهزة، وتقييم مخاطر الأمن السيبراني.
2. الوقاية والحماية: تتضمن هذه العناصر الإجراءات والتقنيات التي تستخدم لمنع واحتواء الهجمات السيبرانية، مثل استخدام جدران الحماية، وبرامج مكافحة الفيروسات، وأنظمة اكتشاف التسلل.
3. الكشف والاستجابة: يشمل هذا العنصر عمليات الكشف عن الانتهاكات والهجمات السيبرانية، وتقديم الاستجابة الفورية لها للحد من الأضرار والتأمين على استمرارية الخدمات.
4. إدارة الهوية والوصول: تتمثل هذه العناصر في تحديد وإدارة الهويات والصلاحيات للمستخدمين في البنية التحتية الرقمية، وتطبيق سياسات الوصول والتحقق من الهوية.
5. التوعية والتدريب: تشمل هذه العناصر التثقيف والتوعية بمخاطر الأمن السيبراني وتدريب الموظفين على ممارسات الأمان الجيدة وكيفية التعامل مع التهديدات السيبرانية.
6. تطبيق السياسات والتشريعات: يتعلق هذا العنصر بتطبيق السياسات والتشريعات القانونية المتعلقة بالأمن السيبراني، وضمان الامتثال لها من قبل المؤسسات والشركات.

وتتعاون هذه العناصر معًا لتوفير حماية شاملة للأنظمة الإلكترونية والبيانات، وتقليل مخاطر التعرض للهجمات السيبرانية والحفاظ على سلامة الأنظمة والمعلومات[9]

رابعا: استراتيجيات الامن السيبراني

وهناك العديد من الاستراتيجيات التي يمكن اتباعها لتعزيز الأمن السيبراني وحماية الأنظمة الإلكترونية والبيانات. من بين هذه الاستراتيجيات:[10]

1. تطوير سياسات الأمن: إنشاء وتطبيق سياسات الأمن القوية والمحدثة لضمان الامتثال بالمعايير الأمنية المحددة، بما في ذلك سياسات إدارة الهوية والوصول وسياسات استخدام البيانات والتحقق من الهوية.
2. تحسين التحقق من الهوية: تعزيز عمليات التحقق من الهوية مثل استخدام كلمات مرور قوية والمصادقة المتعددة العوامل والتحقق البيومتري.
3. تقديم التدريب والتوعية: توفير التدريب المستمر للموظفين حول مخاطر الأمن السيبراني وكيفية التصرف في حالة التعرض لها، بالإضافة إلى تعزيز التوعية بين المستخدمين النهائيين حول ممارسات الأمان الجيدة.

---

[7] – الأشقر , جبور منى(2016). السيبرانية هاجس العصر. بيروت: جامعة الدول العربية – المركز العربي للبحوث القانونية والقضائية،لبنان.

[8] – طلال ياسين العسي وعدي أحمد عناب(2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد19، العدد الاول، جامعة الزرقاء، الاردن.

[9] – الموسوي، علي محمد كاظم (2019). المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان

[10] – Marie Baezner, Patrice Robin,(2018) Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS),.

4. تحديث وصيانة البرمجيات والأجهزة: تطبيق تحديثات الأمان وإجراء الصيانة الدورية للبرمجيات والأجهزة لسد الثغرات الأمنية المعروفة وتحسين الحماية.
5. تطبيق أمان الشبكة: استخدام جدران الحماية وأنظمة اكتشاف التسلل وأجهزة الأمان الشبكي لرصد ومنع الهجمات السيبرانية.
6. تطوير خطط استجابة للطوارئ: إنشاء خطط استجابة للطوارئ للتصدي للاختراقات والهجمات السيبرانية بشكل فعال وتقديم الاستجابة السريعة والفعالة.
7. تعزيز التعاون والشراكات: التعاون مع المؤسسات الحكومية والقطاع الخاص والمجتمع المدني لتبادل المعلومات وتعزيز القدرة على التصدي للتهديدات السيبرانية.
8. استخدام تقنيات التشفير: تشفير البيانات والاتصالات لحماية البيانات من الوصول غير المصرح به والتأكد من سرية المعلومات.

هذه هي بعض الاستراتيجيات الرئيسية في مجال الأمن السيبراني، ويمكن تنفيذها كجزء من إطار شامل لتعزيز الأمان السيبراني في المؤسسات والمنظمات.[11]

المبحث الثاني : حماية الشبكات الالكترونية

ان حماية الشبكات الإلكترونية تتمثل في تطبيق مجموعة من السياسات والتقنيات والإجراءات التي تهدف إلى حماية البنية التحتية الرقمية والبيانات المتداولة عبر الشبكات من التهديدات السيبرانية والهجمات الإلكترونية. وباستخدام هذه الإجراءات والتقنيات، يمكن للمؤسسات تحقيق حماية فعالة للشبكات الإلكترونية وضمان سلامة البيانات واستقرار الأنظمة. وتتضمن عملية حماية الشبكات الإلكترونية العديد من الخطوات والإجراءات، من بينها:[12]

1. تحديد التهديدات والمخاطر: يجب على المؤسسات تحديد وتقييم التهديدات المحتملة والمخاطر التي قد تواجهها الشبكة الإلكترونية، مما يساعدها على التركيز على النقاط الأكثر تعرضًا واتخاذ التدابير الوقائية المناسبة.
2. تطبيق أمان الشبكة: يشمل ذلك استخدام جدران الحماية وأجهزة الأمان الشبكي والبرامج المكافحة للفيروسات والبرامج الضارة، وتحديثها وتكوينها بشكل منتظم للحماية ضد التهديدات الجديدة.
3. تطبيق الإجراءات الأمنية القوية: يجب تطبيق السياسات والإجراءات الأمنية القوية مثل التحقق من الهوية وإدارة الصلاحيات وتشفير البيانات لضمان حماية البيانات ومنع الوصول غير المصرح به.
4. التحديثات والصيانة الدورية: يجب إجراء التحديثات والصيانة الدورية للأنظمة والبرمجيات والأجهزة لسد الثغرات الأمنية المعروفة وتحسين الأمان.
5. التوعية والتدريب: يجب توفير التدريب المستمر للموظفين حول مخاطر الأمان السيبراني وممارسات الأمان الجيدة، بالإضافة إلى التوعية بالتهديدات السيبرانية وكيفية التصرف في حالة التعرض لها.
6. الرصد والاستجابة: يجب إعداد أنظمة لرصد الأنشطة غير المعتادة على الشبكة والاستجابة السريعة للتهديدات والهجمات السيبرانية للحد من الأضرار وتأمين استمرارية الخدمات.

ويمكن حماية الشبكات الإلكترونية من التهديدات السيبرانية والهجمات الإلكترونية بإتباع مجموعة من الإجراءات والتقنيات

[11] – الفتلاوي أحمد عبيس نعمة(2016). "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر". مجلة المحقق الحلي للعلوم القانونية والسياسية,

[12] – الفتلاوي أحمد عبيس نعمة(2016). "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر". مجلة المحقق الحلي للعلوم القانونية والسياسية,

الفعّالة، وفيما يلي بعض الطرق الرئيسية لحماية الشبكات الإلكترونية:[13]

1. استخدام جدران الحماية (Firewalls): تعمل جدران الحماية على منع الوصول غير المصرح به إلى الشبكة من خلال مراقبة وتصفية حركة المرور الشبكي.
2. تحديث البرامج والأنظمة بانتظام: يجب تطبيق التحديثات الأمنية والصيانة الدورية للبرمجيات والأنظمة لسد الثغرات الأمنية المعروفة وتعزيز الأمان.
3. تشفير البيانات: يُستخدم التشفير لتحويل البيانات إلى شكل غير قابل للقراءة إلا بواسطة الأطراف المصرح لها، مما يضمن سرية المعلومات عند الارسال والاستقبال.
4. استخدام برامج مكافحة الفيروسات والبرامج الضارة: يساعد استخدام برامج مكافحة الفيروسات والبرامج الضارة في اكتشاف ومنع البرامج الضارة من التسلل إلى الشبكة وإتلاف البيانات.
5. استخدام أنظمة اكتشاف التسلل (Intrusion Detection Systems): تُستخدم أنظمة اكتشاف التسلل لرصد وتحليل السلوك غير المعتاد على الشبكة وتنبيه عند اكتشاف نشاط مشبوه.

هذه بعض الطرق الفعّالة لحماية الشبكات الإلكترونية، ومن المهم تنفيذ مجموعة شاملة من التدابير الأمنية لتعزيز الأمان والمقاومة ضد التهديدات السيبرانية المتزايدة.

ان الهدف الرئيسي من حماية الشبكات الإلكترونية هو حماية البيانات من التهديدات السيبرانية والهجمات الإلكترونية المحتملة. وتشمل هذه التهديدات على سبيل المثال الاختراقات، والبرمجيات الضارة، والتصيد الاحتيالي، والتصيدين، وغيرها من الأنشطة الضارة التي قد تؤدي إلى سرقة المعلومات أو تلفها أو إتلافها. وتحمي حماية الشبكات الإلكترونية البيانات من هذه التهديدات وتضمن سلامتها وسرية وسلامة البيانات، وتضمن استمرارية الأعمال وحفظ سمعة المؤسسات والشركات.[14]

ومن ابرز الأهداف الرئيسية لحماية البيانات من خلال حماية الشبكات الإلكترونية:[15]

1. سرية البيانات: تحمي حماية الشبكات الإلكترونية البيانات من الوصول غير المصرح بها، سواء كان ذلك من داخل المؤسسة أو من خارجها، وتضمن أن تظل البيانات سرية ومحمية.
2. سلامة البيانات: تهدف حماية الشبكات الإلكترونية إلى حماية البيانات من التلاعب والتلف والتعديل غير المصرح به، وضمان صحة واكتمال البيانات.
3. توفير الوصول الشرعي: يضمن حماية الشبكات الإلكترونية أن يكون الوصول إلى البيانات متاحًا فقط للأشخاص المصرح لهم، وفقًا للصلاحيات المناسبة وبطرق شرعية.
4. حفظ استمرارية الأعمال: يساهم حماية الشبكات الإلكترونية في منع حدوث انقطاع في الخدمات وتوفير استمرارية الأعمال من خلال الحفاظ على توافر البيانات وسلامتها.
5. حفظ سمعة المؤسسات: يساهم حماية البيانات في حفظ سمعة المؤسسات والشركات من خلال حماية البيانات الحساسة ومنع تسربها أو سرقتها، وبالتالي حماية العملاء والشركاء والمستثمرين من الأضرار المحتملة.

---

[13] – المبيضين , ابراهيم (2022). التهديدات السيبرانية من أكثر الجرائم انتشارا حول العالم,صحيفة الغد, 25, تموز , الاردن.

[14] – طلال ياسين العسي وعدي أحمد عناب(2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد19، العدد الاول، جامعة الزرقاء، الاردن.

[15] – Lehto Martti , Neittaanmäk Pekka(2015) .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing,. Switzerland

وتعتبر حماية الشبكات الإلكترونية جزءًا أساسيًا من استراتيجية الأمن السيبراني لأي منظمة أو مؤسسة، وهي تساهم بشكل كبير في الحفاظ على سلامة البيانات واستمرارية الأعمال.[16]

البحث الثاني : أهمية الامن السيبراني في حماية بيانات البلديات

تعد البلديات في الأردن جزءًا أساسيًا من الهيكل الإداري المحلي وتلعب دورًا مهمًا في تقديم الخدمات الأساسية للمواطنين وتنمية المجتمعات المحلية. إليك مقدمة عن البلديات في الأردن: وقد تأسست البلديات في الأردن بموجب قوانين تنظيمية خاصة، وشهدت تطورًا مستمرًا على مر السنين، حيث تم تعزيز دور البلديات وتوسيع اختصاصاتها في مجالات متعددة، مما جعلها تلعب دورًا أكبر في تحقيق التنمية المحلية. ويتم تنظيم البلديات في الأردن وفقًا للقوانين والتشريعات المحلية، حيث يوجد نظام هيكلي متعدد المستويات يتضمن المجالس البلدية على مستوى الأحياء والبلديات على المستوى المحلي والمحافظات على المستوى الإقليمي.[17]

وتقوم البلديات في الأردن بتقديم مجموعة واسعة من الخدمات العامة للمواطنين، مثل خدمات النقل والبنية التحتية والتخطيط العمراني والصحة والتعليم والبيئة والثقافة والرياضة وغيرها. كما تشارك البلديات في تنمية المشاريع الاقتصادية وتشجيع الاستثمارات المحلية. وتواجه البلديات في الأردن العديد من التحديات مثل الضغوط المالية ونقص الموارد وتحديات البيئة والتنمية، ولكنها في الوقت نفسه تتمتع بفرص كبيرة لتعزيز التنمية المحلية وتحقيق التقدم والرفاهية للمجتمعات المحلية.[18]

اولا: وظائف البلديات في الأردن:

تتمتع البلديات في الأردن بالاستقلالية المحددة في إدارة شؤونها المحلية واتخاذ القرارات المناسبة وفقًا للتشريعات والسياسات المحلية والوطنية. حيث تعتبر البلديات في الأردن جزءًا حيويًا من البنية الإدارية والتنموية، وتلعب دورًا أساسيًا في تحسين جودة الحياة للمواطنين وتعزيز التنمية المحلية. وتستند البلديات في الأردن على مجموعة واسعة من الوظائف الأنشطة والمسؤوليات التي تهدف إلى تحسين جودة الخدمة للمجتمعات المحلية وتحقيق التنمية المستدامة. ومن ابرز الوظائف الرئيسية للبلديات في الأردن:[19]

1. تقديم الخدمات الأساسية: تشمل هذه الخدمات النقل والطرق والبنية التحتية، مثل تركيب وصيانة الإنارة العامة وتحسين الطرق وإدارة النفايات وتوفير المياه الصالحة للشرب والصرف الصحي.
2. التخطيط العمراني: تقوم البلديات بوضع الخطط العمرانية للمناطق المحلية وتنظيم البناء والتطوير العقاري والمحافظة على التنوع والهوية الثقافية للمنطقة.
3. الرعاية الصحية والتعليم: تقوم بتقديم الخدمات الصحية الأساسية للمواطنين من خلال تشغيل المرافق الصحية المحلية وتوفير التعليم الأساسي والثانوي والتدريب المهني.

---

[16] – حمد عبيس نعمة الفتلاوي وزهراء عماد محمد(2020). تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد44، العدد1، كلية القانون والعلوم السياسية –جامعة الكوفة، الكوفة، العراق.

[17] – Mabunda, N., & Ndou, S. D. (2019). The role of project management on local economic development programs: a case of Greater Giyani Local Municipality. International Conference on Public Administration and Development Alternative (IPADA).

[18] – جوغي، خديجة، وعطية، العربي. (2020). أثر تطبيق نظام الحكومة الإلكترونية على أداء قطاع الخدمات الحكومية في بلديات الجنوب الشرقي الجزائري .المجلة الجزائرية للتنمية الاقتصادية: جامعة قاصدي مرباح – ورقلة، مج7, ع1 ، 176 – 161. الجزائر,

[19] – الحديد، نضال. (2014). تطوير الخدمات البلدية والمرافق العامة .المدينة العربية: منظمة المدن العربية، عدد 164 ص، 77 – 72.,

4. البيئة والحفاظ على الموارد الطبيعية: تشمل هذه الوظيفة تنفيذ السياسات والبرامج لحماية البيئة المحلية، والحفاظ على الموارد الطبيعية مثل الغابات والمياه والمساحات الخضراء.
5. تنظيم الأنشطة الاقتصادية: تسهل البلديات بيئة الأعمال المحلية وتشجع على الاستثمار وتقوم بتوفير الدعم للمشاريع الصغيرة والمتوسطة وتعزيز النمو الاقتصادي المحلي.
6. النشاطات الثقافة: تنظم الفعاليات الثقافية والفنية والرياضية التي تعزز التواصل الاجتماعي وتعزز الهوية المحلية والتنمية الشخصية.
7. الإدارة المحلية: تقوم البلديات بتنظيم الانتخابات المحلية وإدارة الموظفين وتنفيذ السياسات الحكومية على المستوى المحلي.

ثانيا : أهمية الأمن السيبراني في حفظ بيانات البلديات

أهمية الأمن السيبراني في حفظ بيانات البلديات لا يمكن إغفالها، حيث تعتبر بيانات البلديات من أكثر أنواع البيانات حساسية وتحتاج إلى حماية وتأمين دائم لعدة أسباب:[20]

1. حفظ البيانات الحساسة: تحتوي بيانات البلديات على معلومات حساسة تتعلق بالمواطنين والخدمات الحكومية المقدمة، مثل المعلومات الشخصية، والسجلات الطبية، والبيانات المالية. وبالتالي، يجب ضمان حفظ هذه البيانات وعدم تسربها أو سرقتها.
2. ضمان استمرارية الخدمات: تعتمد البلديات على البيانات لتقديم الخدمات الأساسية للمواطنين، مثل الرعاية الصحية، والتعليم، وخدمات البنية التحتية. لذلك، يجب ضمان توافر البيانات واستمرارية تقديم الخدمات بشكل آمن.
3. الامتثال للتشريعات واللوائح: تخضع البلديات للعديد من التشريعات واللوائح التي تحدد متطلبات الأمان وحماية البيانات، مثل قوانين حماية البيانات الشخصية. ويجب على البلديات الامتثال لهذه التشريعات لتجنب العقوبات والتبعات القانونية.
4. منع التهديدات السيبرانية: تتعرض البلديات لتهديدات سيبرانية متنوعة مثل الاختراقات، والبرمجيات الضارة، وهجمات الفدية. يجب تطبيق إجراءات الأمن السيبراني المناسبة لمنع هذه التهديدات وحماية البيانات.
5. حفظ سمعة البلدية: تتأثر سمعة البلديات بشكل كبير بمدى حماية بيانات المواطنين والمستخدمين، وتحمل البلديات المسؤولية عن حفظ سرية وسلامة هذه البيانات. وبالتالي، يجب تبني استراتيجيات قوية للأمن السيبراني للحفاظ على سمعة البلدية.

لذا فإن الأمن السيبراني يلعب دورًا حاسمًا في حفظ بيانات البلديات، وضمان سلامة واستمرارية الخدمات الحكومية المقدمة للمواطنين.

ثالثا : إستراتيجية البلديات لمواجهة تهديدات الأمن السيبراني

وتستند إستراتيجية البلديات لمواجهة تهديدات الأمن السيبراني على مجموعة من الإجراءات والتدابير الوقائية والاستجابية التي تهدف إلى حماية بياناتها وخدماتها وأنظمتها من الهجمات السيبرانية. ومن اهم الاستراتيجيات الرئيسية:[21]

[20] – الصوالحي , سمر (2023). الأمن السيبراني ركيزة الحروب الحديثة وتحديات الأمن القومي, صحيفة الراي 11 ,كانون ثاني, الاردن.

[21] – الهياجنة , وليد (2019). مجلس النواب يقر قانون الأمن السيبراني,وكالة الإنباء الأردنية ,3, تموز, الأردن.

1. التوعية والتدريب: تشمل هذه الاستراتيجية توفير التوعية للموظفين والمسؤولين في البلديات حول تهديدات الأمن السيبراني وكيفية التعرف عليها والتعامل معها. كما يجب تقديم التدريب المناسب لهم لتطبيق أفضل الممارسات في حماية الأنظمة والبيانات.
2. تطبيق السياسات والإجراءات الأمنية: يجب على البلديات وضع سياسات وإجراءات أمنية صارمة لحماية البيانات وأنظمة المعلومات، بما في ذلك تحديد صلاحيات الوصول وتشفير البيانات وإدارة الهوية والوصول.
3. تحديث الأنظمة والبرامج: يجب على البلديات تحديث وصيانة أنظمتها وبرمجياتها بانتظام لضمان توافر التحديثات الأمنية وإصلاح الثغرات الأمنية المعروفة.
4. تنفيذ أمن الشبكات: يشمل ذلك تطبيق تقنيات أمان الشبكات مثل جدار الحماية ونظام اكتشاف التسلل وتشفير الاتصالات لمنع الوصول غير المصرح به وحماية بيانات البلديات.
5. الاستعداد والاستجابة: يجب أن تكون البلديات مستعدة للتعامل مع الحوادث السيبرانية من خلال وجود خطة استعداد واستجابة تتضمن إجراءات لتقييم الضرر واستعادة البيانات والتواصل مع الجهات المعنية.
6. التعاون مع القطاع الخاص والحكومي: يجب أن تعمل البلديات على تعزيز التعاون مع الشركات الخاصة والجهات الحكومية المعنية بالأمن السيبراني لمشاركة المعلومات والخبرات والموارد في مجال حماية الأنظمة والبيانات.

باعتبار تنوع التهديدات السيبرانية وتطورها المستمر، يجب على البلديات تطبيق استراتيجيات شاملة ومتعددة الأوجه لحماية بياناتها وضمان استمرارية تقديم الخدمات للمواطنين بشكل آمن وموثوق.

ان استراتيجيات الأمن السيبراني تلعب دورًا حيويًا في تعزيز حماية الشبكات الإلكترونية في البلديات، حيث تهدف إلى تحقيق أمان البيانات والحفاظ على استقرار الأنظمة والخدمات المقدمة للمواطنين , وتشمل هذه الاستراتيجية وضع سياسات وإجراءات أمنية صارمة تنظم استخدام الأنظمة والبيانات والموارد في البلدية، وتحدد المسؤوليات والتدابير الأمنية اللازمة لحماية البيانات. وتحديث الأنظمة والبرمجيات بانتظام لضمان توافر التحديثات الأمنية وإصلاح الثغرات الأمنية المعروفة وتعزيز القدرة على مواجهة التهديدات الجديدة. واستخدام تقنيات الحماية الأمنية مثل جدار الحماية وأنظمة الكشف عن التسلل والتشفير للاتصالات لمنع الوصول غير المصرح به وحماية البيانات من الاختراقات.[22]

ان توفير التوعية والتدريب المناسب للموظفين والمسؤولين في البلدية حول تهديدات الأمن السيبراني وكيفية التعرف عليها والتعامل معها بشكل فعال. مع وجود خطة استجابة للحوادث السيبرانية تتضمن إجراءات لتقييم الضرر واستعادة البيانات والتواصل مع الجهات المعنية للتعامل مع الوضع بشكل سريع وفعال. والتعاون والتبادل الدولي للمعلومات الذي يلعب دورًا هامًا في تعزيز الأمان السيبراني، حيث يمكن للبلديات الاستفادة من تجارب البلديات الأخرى وتحليل الاتجاهات العالمية في مجال الأمن السيبراني.[23]

يمكن القول أن البلديات تعتمد بشكل كبير على البيانات الحساسة والخدمات الحكومية الأساسية، فإن تطبيق هذه الاستراتيجيات بشكل فعال يساهم في تعزيز حماية الشبكات الإلكترونية وضمان استمرارية تقديم الخدمات بشكل آمن وموثوق.

[22] – عنتر ,احمد (2023). تقنيات الأمن السيبراني والتحديات المستقبلية, مركز الجزيرة للدراسات ,4 كانون اول,قطر.

[23] – المومني, زياد (2023). استراتيجية أمن المعلومات تأتي في اطار مفهوم الامن الوطني, وكالة الانباء الاردنية ,29, ايلول , الأردن.

الخاتمة والنتائج والتوصيات

أولاً: الخاتمة

شكَّلت خاتمة الدِّراسة حصيلة النتائج التي تمثل الإجابة عن أسئلة الدِّراسة بالإضافة إلى تقديم مجموعة من التوصيات, وقد تناولت الدِّراسة استراتيجيات الأمن السيبراني ودورها في تعزيز حماية الشبكات الالكترونية في البلديات , وقد بينت الدراسة أهمية الأمن السيبراني بالتزامن مع تطور التكنولوجيا وانتشار استخدام الإنترنت والتحول الرقمي في مختلف جوانب الحياة اليومية، مما جعل الأنظمة الإلكترونية عرضة لمختلف أنواع الهجمات والتهديدات. ويشير مصطلح الأمن السيبراني إلى حماية الأنظمة الإلكترونية والشبكات والبيانات من الهجمات الإلكترونية والتهديدات السيبرانية. يعتبر الأمن السيبراني جزءاً حيوياً من الأمن الشامل للدول والمؤسسات والأفراد في عصر الاتصالات الرقمية.

وبينت الدراسة مواجهة التهديدات السيبرانية من الهجمات مثل البرامج الضارة والتصيد الاحتيالي والاختراقات السيبرانية والتصيد السيبراني والتصيد الاجتماعي والهجمات الموزعة للخدمة بالإضافة إلى التجسس الإلكتروني وسرقة البيانات والاختراقات الهندسية الاجتماعية.

وأكدت الدراسة اهمية وضع استراتيجيات الأمن السيبراني لحماية الأنظمة والبيانات، والتي تشمل استخدامات تقنيات التشفير والتحقق الثنائي للعوامل وتطبيق السياسات الأمنية وتحديث البرمجيات بانتظام وتدريب الموظفين على ممارسات الأمان الجيدة.بالإضافة إلى ذلك، يعتبر التعاون والتنسيق بين الحكومات والقطاع الخاص والمؤسسات الدولية أمراً بالغ الأهمية في مجال الأمن السيبراني، حيث يمكن أن يساهم هذا التعاون في تبادل المعلومات وتطوير السياسات والتشريعات اللازمة لمكافحة التهديدات السيبرانية بشكل فعال.

وأكدت الدراسة على اهمية حماية الشبكات الإلكترونية والتي تهدف لحماية البيانات والأنظمة الإلكترونية من التهديدات والهجمات الإلكترونية المحتملة.ويعد تأمين الشبكات الإلكترونية أمراً بالغ الأهمية في عصر التكنولوجيا الرقمية، حيث يتزايد التنوع والتعقيد للهجمات السيبرانية باستمرار. ومن خلال استخدام تقنيات وإجراءات الحماية المناسبة،

وبينت الدراسة دور للبلديات في التقليل من مخاطر التعرض للهجمات والاختراقات الإلكترونية وحماية البيانات الحساسة والأصول الرقمية. من خلال الاعتماد علة التقنيات والسياسات والإجراءات، ويجب تطبيقها بشكل متكامل ومنتظم لضمان حماية البيانات والأنظمة بشكل فعال في ظل التهديدات المتزايدة في عالم الإنترنت.

ثانيا : نتائج الدراسة :

1- بينت الدراسة أهمية الأمن السيبراني بعد ان تعرضت الأنظمة الإلكترونية لمختلف أنواع الهجمات والتهديدات والتي تؤثر البلديات والمؤسسات والأفراد في عصر الاتصالات الرقمية.

2- بينت الدراسة ان بيانات البلديات تتعرض للتهديدات السيبرانية التي تتمثل في الهجمات مثل البرامج الضارة والتصيد الاحتيالي والاختراقات السيبرانية والتصيد السيبراني والتصيد الاجتماعي والهجمات الموزعة للخدمة بالإضافة إلى التجسس الإلكتروني وسرقة البيانات والاختراقات الهندسية الاجتماعية.

3- أكدت الدراسة بالأهمية القصوى وضع استراتيجيات الأمن السيبراني لحماية الأنظمة والبيانات، والتي تشمل استخدامات تقنيات التشفير والتحقق الثنائي للعوامل وتطبيق السياسات الأمنية وتحديث البرمجيات بانتظام وتدريب الموظفين على ممارسات الأمان الجيدة.

4- اكدت الدراسة على اهمية التعاون والتنسيق بين الحكومات والقطاع الخاص والمؤسسات الدولية في مجال الأمن السيبراني، حيث يمكن أن يساهم هذا التعاون في تبادل المعلومات وتطوير السياسات والتشريعات اللازمة لمكافحة التهديدات السيبرانية بشكل فعال.

5- أكدت الدراسة على اهمية حماية الشبكات الإلكترونية والتي تهدف لحماية البيانات والأنظمة الإلكترونية من التهديدات والهجمات الإلكترونية المحتملة.ويعد تأمين الشبكات الإلكترونية أمراً بالغ الأهمية في عصر التكنولوجيا الرقمية،

6- بينت الدراسة على دور للبلديات في التقليل من مخاطر التعرض للهجمات والاختراقات الإلكترونية وحماية البيانات الحساسة والأصول الرقمية. من خلال الاعتماد علة التقنيات والسياسات والإجراءات، ويجب تطبيقها بشكل متكامل ومنتظم لضمان حماية البيانات والأنظمة بشكل فعال في ظل التهديدات المتزايدة في عالم الإنترنت.

ثالثا :التوصيات

1. أوصت الدراسة بأنه على البلديات تحقيق أمان البيانات والحفاظ على استقرار الأنظمة والخدمات المقدمة للمواطنين , من خلال وضع إستراتيجية وسياسات وإجراءات أمنية صارمة تنظم استخدام الأنظمة والبيانات والموارد في البلدية
2. أوصت الدراسة بضرورة توفير التوعية والتدريب المناسب للموظفين والمسؤولين في البلديات حول تهديدات الأمن السيبراني وكيفية التعرف عليها والتعامل معها بشكل فعال..
3. من الضروري على البلديات تعزيز التعاون مع الشركات الخاصة والجهات الحكومية المعنية بالأمن السيبراني لمشاركة المعلومات والخبرات والموارد في مجال حماية الأنظمة والبيانات.
4. على البلديات تحديث وصيانة أنظمتها وبرمجياتها بانتظام لضمان توافر التحديثات الأمنية وإصلاح الثغرات الأمنية المعروفة.
5. على البلديات وضع سياسات وإجراءات أمنية صارمة لحماية البيانات وأنظمة المعلومات، بما في ذلك تحديد صلاحيات الوصول وتشفير البيانات وإدارة الهوية والوصول

المراجع

اولا : المراجع العربية

الأشقر , جبور منى(2016). السيبرانية هاجس العصر. بيروت: جامعة الدول العربية – المركز العربي للبحوث القانونية والقضائية،لبنان.

البهي , رغدة (2019). "الردع السيبراني: المفهوم والإشكاليات والمتطلبات, المركز الديمقراطي العربي. 10, اب, برلين.

بوغرارة يوسف(2018). "الأمن السيبراني: الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبيري". مجلة الدراسات الإفريقية وحوض النيل, مصر

جوغي، خديجة، وعطية، العربي. (2020). أثر تطبيق نظام الحكومة الإلكترونية على أداء قطاع الخدمات الحكومية في بلديات الجنوب الشرقي الجزائري .المجلة الجزائرية للتنمية الاقتصادية: جامعة قاصدي مرباح – ورقلة، مج,7 ع1 ، 176 – 161, الجزائر.

الحديد، نضال. (2014). تطوير الخدمات البلدية والمرافق العامة .المدينة العربية: منظمة المدن العربية، عدد 164 ص، 77 – 72,.

حمد عبيس نعمة الفتلاوي وزهراء عماد محمد(2020). تكييف الهجمات السيبرانية في ضوء القانون الدولي، مجلة الكوفة للعلوم القانونية والسياسية، المجلد44، العدد1، كلية القانون والعلوم السياسية –جامعة الكوفة، الكوفة، العراق.

الخزاعله , عبير (2021). مفهوم الأمن السيبراني, موقع موضوع , 17, تشرين ثاني , الاردن.

الدماطي, رامي عبداللطيف(2016). أمن شبكات المعلومات الإلكترونية ,مركز الجزيرة للدراسات,29,تشرين اول, قطر

الصوالحي , سمر (2023). الأمن السيبراني ركيزة الحروب الحديثة وتحديات الأمن القومي, صحفة الراي11 ,كانون ثاني, الاردن.

طلال ياسين العسي وعدي أحمد عناب(2019). المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد19، العدد الاول، جامعة الزرقاء، الاردن.

عنتر ,احمد (2023). تقنيات الأمن السيبراني والتحديات المستقبلية, مركز الجزيرة للدراسات ,4 كانون اول,قطر.

الفتلاوي أحمد عبيس نعمة(2016). "الهجمات السيبرانية: مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر". مجلة المحقق الحلي للعلوم القانونية والسياسية

المبيضين , ابراهيم (2022). التهديدات السيبرانية من أكثر الجرائم انتشارا حول العالم,صحيفة الغد, 25, تموز , الاردن.

الموسوي، علي محمد كاظم (2019). المشاركة المباشرة في الهجمات السيبرانية، المؤسسة الحديثة للكتاب، لبنان

المومني, زياد (2023). استراتيجية أمن المعلومات تأتي في اطار مفهوم الامن الوطني, وكالة الانباء الاردنية ,29, ايلول , الأردن.

الهياجنة , وليد (2019). مجلس النواب يقر قانون الأمن السيبراني,وكالة الإنباء الأردنية ,3, تموز , الأردن.

يارا ,تعامرة(2017). تعريف البلدية, موقع موضوع , 4, تموز , الاردن.

ثانيا: المراجع الاجنبية

Lehto Martti , Neittaanmäk Pekka(2015) .Cyber Security: Analytics, Technology and Automation. Switzerland : Springer International Publishing,. Switzerland

Mabunda, N., & Ndou, S. D. (2019). The role of project management on local economic development programs: a case of Greater Giyani Local Municipality. International Conference on Public Administration and Development Alternative (IPADA).

Marie Baezner, Patrice Robin,(2018) Trend Analysis: Cyber Sovereignty and Data Sovereignty, Center for Security Studies (CSS),.

Newman, E. (2016). Human Security: Reconciling Critical Aspirations with Political ‘Realities’. British Journal of Criminology Advance Access, 56(6), 1165-1183.