مجلة المعيار ISSN :1112-4377
مجلد: 27 عدد: 3 (رت 72) السنة: 2023

حماية الكيانات الرقمية وضمان استمراريتها من خلال استراتيجيات أمن المعلومات بالمستودعات الرقمية الجامعية: مستودع جامعة محمد خيضر بسكرة نموذجا

Information security strategies for the protection of digital entities and ensuring their continuity in university's repositories: special reference to the University of Biskra repository.

عقابو خالد [1]
مخبر الدراسات والبحث حول الإعلام والتوثيق العلمي والتكنولوجي (LERIST)،معهد علم المكتبات والتوثيق
جامعة عبد الحميد مهري قسنطينة 02
Khaled.agabou@univ-constantine2.dz

بومعرافي بهجة
مخبر الدراسات والبحث حول الإعلام والتوثيق العلمي والتكنولوجي (LERIST)، معهد علم المكتبات والتوثيق
جامعة عبد الحميد مهري قسنطينة 02
Behdja.boumarafi@univ-constantine2.dz

تاريخ الوصول 2022/12/16 القبول 2022/12/22 النشر على الخط 2023/03/15
Received 16/12/2022 Accepted 22/12/2022 Published online 15/03/2023

ملخص:

تناولت هذه الدراسة مفهوم استراتيجيات أمن المعلومات بالمستودعات الرقمية المؤسساتية ومدى أهميتها ودورها في حماية الكيانات الرقمية، وضمان السير الحسن لوظيفة المستودعات القائمة على مبدأ السلامة والتكاملية والاستمرارية. وقد تم إجراء هذه الدراسة بمستودع جامعة محمد خيضر بسكرة للتعرف على مختلف المكونات المادية والتكنولوجية المعتمدة لتحقيق استراتيجية أمنية متكاملة، ومعرفة مدى استغلال التقنيات الخاصة بأمن المعلومات التي يوفرها نظام إدارة المحتوى بالمستودع. اعتمدت الدراسة على المنهج الوصفي، مع استخدام أداتي الملاحظة والمقابلة لجمع البيانات البحثية وتحليلها وصولا إلى مجموعة من النتائج كانت في مجملها تشير إلى أنه قد تم وضع استراتيجية أمنية قوية نسبيا لحماية المكونات المادية للمستودع، مع أخذ الجانب الأمني المتعلق بالمحتوى الرقمي بعين الاعتبار، كما خلصت الدراسة إلى أنه هناك نقص وغياب لبعض شروط الحماية، والتي على ضوئها تم صياغة التوصيات والمقترحات التي تشير في مجملها إلى ضرورة إعادة النظر ووضع سياسات واستراتيجيات قوية وواضحة مع المراجعة الدائمة والمستمرة لكشف مختلف الثغرات ومواضع الضعف ومحاولة تجاوزها.

الكلمات المفتاحية: استراتيجيات أمن المعلومات، المستودعات الرقمية المؤسساتية، الكيانات الرقمية، إدارة المحتوى الرقمي، جامعة محمد خيضر بسكرة.

Abstract:

This study examined the concept of information security strategies in institutional digital repositories and their importance and role in protecting digital entities and ensuring their good functioning in relation of security, integrity and continuity. The repository of the University of Mohamed Kheidar Biskra is used to identify the various physical and technological components adopted to achieve an integrated security strategy, and to know the extent to which the information security techniques provided by the content management system in the repository are exploited. The study relied on the descriptive approach using observation and interview to collect and analyze research data. Results indicate that a relatively strong security strategy has been developed to protect the digital content of the repository. The study also identified a lack of some protection conditions, in light of which some recommendations were formulated such as the need to reconsider and develop strong and clear policies and strategies with permanent and continuous review to detect various gaps and weaknesses and overcome them.

Keywords: information security strategies, institutional digital repositories, digital entities, digital content management, Mohamed Kheidar Biskra University

[1] المؤلّف المراسل: **عقابو خالد** البريد الإلكتروني: **khaled.agabou@univ-constantine2.dz**

مقدمة:

توالت التطورات الحاصلة في مجال تقنية المعلومات وتعددت الوسائل والوسائط المستخدمة في تخزين المعلومات واسترجاعها وتبادلها، وكان من أهم نتائج تلك التطورات ظهور جملة من التقنيات على غرار المستودعات الرقمية الأكاديمية التي تهدف إلى إتاحة ونشر المحتوى العلمي والإنتاج الفكري الصادر عن الجامعات بعد رقمنته وإتاحته بغية الوصول إليه والاستفادة منه، ويتطلب ذلك توفير بنية تحتية تشمل المكونات البرمجية والمادية اللازمة لتحقيق هذا الهدف، بالإضافة إلى نظام إدارة المحتوى الرقمي لتسيير مختلف الكيانات الرقمية المودعة بالمستودع ونشرها على الإنترنت بهدف توسيع نطاق مرئيتها ورفع قيمتها العلمية التي كانت حبيسه الرفوف والمكتبات. واتجهت العديد من المؤسسات الأكاديمية والبحثية نحو إنشاء مستودعات رقمية بغرض حفظ الإنتاج الفكري الرقمي المنسوب لها، وتقديمه للمستفيدين من طلاب وأعضاء هيئة تدريس وموظفين، والباحثين من خارج المؤسسة المعنية.

وقد ساهمت المستودعات الرقمية المؤسساتية للجامعات في تقديم المعرفة وخصوصاً المتجددة منها، عبر تيسير الاتاحة والوصول لكافة مجتمع المستفيدين منها، تلبية لحاجاتهم وتطلعاتهم ورغباتهم في الحصول على المعلومات والمعرفة، وهي بذلك تشكل مكوناً أساسياً في نشر وإتاحة المعلومات، من خلال الربط بين منتجي المعرفة وإتاحتها لمستخدميها بما يسمح به القانون دون التعدي على حقوق الملكية الفكرية لأصحاب الحق. ويتجلى دورها بوضوح في أمن وحماية المعلومات وحفظ الكيانات الرقمية المودعة بها، عبر السياسات واللوائح الخاصة وآليات التعامل مع المعلومات لمراقبة ومتابعة المستفيدين عند الاستخدام.

أولا: الإطار المنهجي للدراسة:

1-1- مشكلة البحث:

تواجه المستودعات الرقمية للجامعات العديد من التحديات والعقبات المتعلقة بأمن وحماية المحتوى الرقمي (الكيانات الرقمية) المودعة بها، لذلك عملت مختلف المستودعات الرقمية الأكاديمية للجامعات الجزائرية على غرار مستودع جامعة محمد خيضر بسكرة على مواجهة تلك العقبات من خلال اتباع السياسات والاستراتيجيات والإجراءات والعمليات المتعلقة بأمن وحماية المعلومات لدحض مختلف المحاولات المتعلقة بالسرقة العلمية وجميع أشكال الجريمة المعلوماتية. وذلك باستخدام كل ما يوفره نظام إدارة المستودع الرقمي من أساليب وتقنيات خاصة بأمن وحماية المحتوى الرقمي، باعتبار أن الكيانات الرقمية المخزنة بالمستودعات المؤسساتية الأكاديمية من الوثائق الأساسية لما لها من أهمية ومكانة بارزة كونها تعبر عن المحتوى الفكري لهذه المؤسسات والتي تسودها عادة صفة الأصالة والابتكار، وهما المطلبين الأساسيين للإبداع الفكري وإنتاج البحوث العلمية، لذلك فهي تتطلب اهتمام خاص من قبل القائمين على المستودع الرقمي داخل المؤسسات الأكاديمية، وقد اقتضت عمليات التحول الرقمي بذل الكثير من الجهود فيما يتعلق برقمنة المنتوج الفكري وتحويله إلى كيانات رقمية بغية إتاحته ومعظم هذه الجهود تتطلب وضع خطط واعية واستراتيجيات واضحة وإدارة حقيقية لهذه الكيانات لتفادي مختلف الانزلاقات ذات العلاقة بأمن وحماية المحتوى الرقمي المنشور لذا فقد تم تحديد إشكالية الدراسة في التساؤل التالي: ما مدى التزام مستودع جامعة محمد خيضر بسكرة بالسياسات والاستراتيجيات التي تحقق الحماية الأمنية للكيانات الرقمية؟

2-1- أهمية الدراسة وأهدافها:

يعتبر بناء المستودعات الرقمية والمحتوى الرقمي أمرا هاما جدا، خاصة فيما يعيشه العالم اليوم من ثورة معلوماتية كبيرة، تنتقل فيها المعلومات والبحوث والدراسات بسرعة البرق، وأصبح العالم يتعامل مع مؤسسات من خلال مواقعها ومستودعاتها على الأنترنت،

مما جعل امتلاك المؤسسات الأكاديمية للمستودعات أمرا ضروريا للتعامل مع العالم المعرفي باعتبارها تملك محتوى رقمي الذي يحتاج وضع الخطط والسياسات اللازمة لتنظيمه وحمايته من الاستغلال غير القانوني، والجرائم المعلوماتية بجميع أشكالها. ومن هنا تكمن أهمية هذه الدراسة في التعريف بالاستراتيجيات المتبعة لحماية الكيانات الرقمية بمستودع جامعة محمد خيضر بسكرة.

أما أهداف الدراسة فيمكن حصرها فيما يلي:

- التعرف على مستودع جامعة محمد خيضر بسكرة وطبيعة الكيانات الرقمية المودعة به.
- التعرف على اهم المعايير والطرق العالمية لأمن المعلومات.
- الوقوف على أهم التهديدات والمخاطر التي تواجه أمن المحتوى الرقمي بالمستودعات الرقمية الأكاديمية.
- كشف الغطاء عن السياسات المتعلقة بأمن المعلومات بالمستودعات الجامعية.
- طرق تأمين النظام والتجهيزات المادية بمستودع جامعة محمد خيضر بسكرة محل الدراسة.

1-3- أسئلة الدراسة:

إن تحقيق الأهداف السابقة لا يكون إلا من خلال الإجابة على التساؤلات تالية:

- ما المقصود باستراتيجية أمن وحماية الكيانات الرقمية بالمستودعات الرقمية؟
- ماهي أهم المخاطر المحتملة التي تهدد محتوى المستودعات الرقمية؟
- ماهي أساليب الحماية وإجراءات الوقاية من هذه المخاطر؟
- كيف يتم تأمين نظام المعلومات بمستودع جامعة محمد خيضر بسكرة؟

1-4- منهج الدراسة:

يعرف المنهج العلمي بأنه الأسلوب الذي يعتمده الباحث لتنظيم أفكاره وتحليلها وعرضها وبالتالي الوصول إلى نتائج وحقائق معقولة حول الظاهرة وموضوع الدراسة [1].

وفي إطار تحقيق الأهداف المرجوة من الدراسة وللإحاطة باستراتيجيات أمن وحماية الكيانات الرقمية داخل المستودعات الرقمية الجامعية اعتمدنا "المنهج الوصفي"، فهو يعتمد على دراسة الظاهرة المرجوة في الواقع، ويهتم بوصفها وصفا دقيقا ويعبر عنها عن طريق وصف الظاهرة مع بيان خصائصها [2].

1-5- حدود الدراسة:

تناولت الدراسة موضوع أمن وحماية الكيانات الرقمية لمستودع جامعة محمد خيضر بسكرة، وقد استغرقت الدراسة بين شقيها النظري والتطبيقي مدة 08 أشهر بالتقريب وذلك ابتداء من شهر ديسمبر2021 إلى غاية منتصف شهر جويلية 2022م.

1-6-أدوات جمع البيانات:

اعتمد الباحث في هذه الدراسة على مجموعة من العناصر والأدوات لغرض جمع البيانات والتي من شأنها أن تعطي للدراسة طابع المصداقية والأمانة العلمية ويمكن حصرها فيما يلي:

- الإنتاج الفكري الصادر في الموضوع وذلك من خلال البحث في فهارس المكتبات ومصادر المعلومات.

[1] عليان، ربح مصطفى. أساليب البحث العلم وتطبيقاته في التخطيط والإدارة. – عمان: دار الصفاء، 2008، ص. 35.

[2] الدعيلج، إبراهيم بن عبد العزيز. مناهج وطرق البحث العلمي. – عمان: دار الصفاء للنشر والتوزيع، 2010، ص. 75.

- شبكة الأنترنت كأحد الوسائل الهامة التي تساعد في عملية البحث وجمع المادة العلمية.
- مقابلة مقننة تم إعدادها وإرسالها عبر البريد الإلكتروني والتي حاول من خلالها الباحث جمع المعلومات المتعلقة بأمن الكيانات الرقمية بمستودع جامعة محمد خيضر بسكرة، وقد تضمنت هذه المقابلة خمسة محاور رئيسية تضمن كل محور عدة أسئلة وقد حددت المحاور على الشكل التالي:

معلومات عامة حول المستودع الرقمي – التأمين المادي للأجهزة والمكونات المادية – تقنيات ووسائل الأمن الخاصة بالموارد البشرية – تأمين النظام – تأمين البيانات والمعلومات (الوقاية لمحتوى الكيانات الرقمية).

1-7- مصطلحات الدراسة:

- **المستودعات الرقمية المؤسساتية**: يعرفها قاموس علم المكتبات والمعلومات على الخط ODLIS بأنها مجموعة من الخدمات التي تقدمها الجامعة أو مجموعة من الجامعات لأعضاء مجتمعها لإدارة المواد العلمية الرقمية التي أنتجتها المؤسسة، ونشرتها وتشمل التقارير الفنية والرسائل والأطروحات الجامعية والمواد التعليمية وتلك المواد التي يتم تنظيمها في قاعدة بيانات متاحة للوصول الحر، ويتم حفظها على المدى الطويل. [1]
- **أمن المعلومات**: يشير أمن المعلومات إلى تدابير الخصوصية الرقمية الوقائية لمنع الوصول غير المرخص به إلى أجهزة الكمبيوتر وقواعد البيانات والمواقع الالكترونية، وحماية البيانات من الفساد، ويعد أمن المعلومات جانبا أساسيا لتكنولوجيا المعلومات للمؤسسات والشركات من كل نوع .[2]
- **الاستراتيجية**: هي علم وفن تحديد الأهداف والخطط والسياسات العامة المدروسة بعناية، والمناسبة للظروف البيئية التي تعمل في ظلها المنظمة، وتتضمن عملية تحديد وتقويم البدائل المتوافرة والمصممة بشكل متلاحق ومنسق لاستخدام الموارد المتاحة التي تمكن المنظمة من تحقيق أهدافها [3].
- **المحتوى الرقمي**: هو كل المعلومات والحقائق والأرقام في شكل صورة، أو مقطع صوتي، او فيديوهات أو نصوص، مخزنة في شكل رقمي، منظمة ومجهزة داخل حامل معين (صفحات ويب، قواعد بيانات، مواقع رسمية.....)، متاحة على فهارس الوصول المباشر أو الشبكات المحلية أو العالمية.[4]
- **جامعة محمد خيضر بسكرة**: تقع جامعة محمد خيضر على بعد حوالي كيلومترين (02 كلم) عن وسط مدينة بسكرة على الطريق المؤدي إلى مدينة سيدي عقبة. أنشأت جامعة محمد خيضر بالمعاهد الوطنية الآتية [5]:- معهد الري (المرسوم رقم: 254-

---

[1] العربي، أحمد عبادة. المستودعات الرقمية للمؤسسات الأكاديمية ودورها في العملية التعليمية والبحثية وإعداد آلية لإنشاء مستودع رقمي عربي. ورقة عمل، ندوة التعليم الجامعي في عصر المعلوماتية "التحديات والتطلعات.- طنطا 2011.متوفر على الرابط: http://repository.taibahu.edu.sa/handle/123456789484 تمت الزيارة يوم 20-12-2021.

[2] عبد الله، عبد الكريم فراس؛ حسان عباس، رشا. التشفير وسيلة للحصول على أمن البيانات. - بغداد: كلية تكنولوجيا هندسة الحاسوب، 2019. ص11.

[3] إبراهيم، السعيد مبروك. الإدارة الاستراتيجية للمكتبات ومرافق المعلومات. – الإسكندرية: دار الوفاء لدنيا الطباعة والنشر، 2014. ص.89

[4] طرشي، حياة. وصف المحتوى الرقمي ودوره في تفعيل البحث الموضوعي من خلال الفهارس الآلية للمكتبات الجامعية: دراسة وصفية تحليلية بمكتبات جامعات الشرق الجزائري. أطروحة مقدمة لنيل شهادة الدكتوراه في علم المكتبات والتوثيق. - قسنطينة: جامعة عبد الحميد مهري، 2020. ص 112.

[5] موقع جامعة بسكرة. متاح على الرابط: https://univ-biskra.dz/index.php/fr/34-universite/articles9/186-presentation-de-lumkb تمت الزيارة يوم: 20-12-2021

84 المؤرخ في: 18-08-1984). - معهد الهندسة المعمارية (المرسوم التنفيذي رقم: 253-84 المؤرخ في :05-08-1984). - معهد الكهرباء التقنية في عام 1986 (المرسوم التنفيذي رقم: 169-86 المؤرخ في: 18-08-1986). تحولت هذه المعاهد إلى مركز جامعي بمقتضى المرسوم رقم: 295-92 المؤرخ في: 07-07-1992. وبصدور المرسوم رقم: 219-98 المؤرخ في: 07-07-1998 تحول المركز الجامعي إلى جامعة تضم ثلاث كليات وسبعة أقسام. كما تم إضافة كلية رابعة بعد ذلك. وبمقتضى المرسوم رقم: 90/09 المؤرخ في: 17-02-2009، أصبحت الجامعة مشكلة من ست (06) كليات وواحد وثلاثين (31) قسما تضم مختلف الميادين والتخصصات.

1-8- الدراسات السابقة:

لقد تم حصر بعض الدراسات التي تناولت موضوع أمن وحماية المحتوى الرقمي في البيئة الرقمية وإتاحته من خلال مستودعات الوصول الحر وهي:

- دراسة (**الشوابكة، عدنان عواد.2019**) جاءت الدراسة من أجل التعرف على دور اجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف. ولتحقيق ذلك تم تصميم استبانة وتوزيعها على عينة الدراسة المكونة من (129) عاملا، وقد توصلت الدراسة الى ان الاجراءات الامنية في الحد من مخاطر امن المعلومات تساهم بشكل كبير في الحد من المخاطر الداخلية والخارجية والطبيعية التي يتعرض لها النظام. وقد اوصت الدراسة بضرورة قيام ادارة الجامعة بوضع تصنيفات للمعلومات بالطريقة التي تناسب اعمالها وسرية معلوماتها مع عزل البيانات والمعلومات التي يشكل عرضها للعامة ضرر للنظام. وتقييم المخاطر التي يتعرض اليها النظام بشكل دوري للوقوف على ما يمكن عمله وايجاد السبل الكفيلة باستعادة العمل، ووضع خطط الطوارئ اللازمة لضمان أمن النظام في الجامعة.
- دراسة (**عزة، فاروق جوهري، وطه، محمد طه حسين، 2019**.) بعنوان أمن المعلومات الرقمية وسبل حمايته في ظل التشريعات الراهنة حيث هدفت هذه الدراسة إلى التعرف على المخاطر التي يتعرض لها أمن المعلومات الرقمية بأشكالها المختلفة والتدابير المضادة للحد من هذه المخاطر مثل التدابير المادية والتنظيمية والتقنية بالإضافة إلى التدابير التشريعية على المستويين الوطني والدولي واهم المعايير الدولية التي تضعها منظمة ISO لضبط ممارسات أمن المعلومات، وتوصلت الدراسة لجملة من النتائج أهمها أن امن المعلومات يتعرض للعديد من المخاطر والتهديدات التي تتم في بيئة الأنترنت مع صعوبة مواكبة التدابير الأمنية المضادة لسرعة تطور الأساليب الحديثة المستعملة في عمليات الاعتداءات على أمن المعلومات، كذلك ضعف التشريعات الموجودة على أرض الواقع سواء على المستوى الوطني أو الدولي مع وجود بطئ ملحوظ في مدى كفاية التشريعات الموجودة للحد من عمليات التعدي على أمن المعلومات.
- دراسة (**علي، عادل نبيل شحات. 2017**) تناول فيها موضوع أمن وحماية المحتوى الرقمي للمستودع الرقمي للرسائل الجامعية المصرية حيث بين فيها مختلف الجهود التي بذلت من طرف المكتبة الرقمية بالمجلس الأعلى للجامعات بغية الحفاظ على أمن المحتوى الرقمي لمستودع الرسائل الجامعية، وتوصلت الدراسة من خلال الوصف والرصد والتحليل إلى جملة من النتائج نذكر منها:

✓ يتم استخدام برامج حماية ضد الفيروسات (endpoint protection) لحماية المستودع الرقمي من كل أنواع الفيروسات.
✓ يتم استخدام تقنية تشفير البيانات لنقلها بشبكة المستودع الرقمي للرسائل الجامعية المصرية.
✓ مبنى المستودع مؤمن بشكل جيد من حيث: المكان وأجهزة الإمداد بالطاقة، وأجهزة التكييف المناسبة.

• دراسة كلا من (**2010 satyanarayana, badu**) والتي تطرقت لتاريخ تطور رقمنة الأرصدة والرسائل العلمية الهندية ورصد أهم العوائق التي تعترض عمليات الرقمنة، ومن جهة أخرى حددت الدراسة العديد من التحديات التي تواجه المستودعات الرقمية مثل المخاوف التي تتعلق بالانتحال ، وانتهاكات حقوق التأليف والنشر ، ونوعية الأبحاث العلمية ، والافتقار إلى تطوير السياسيات على المستوى الجامعي ، وضعف البنية التحتية وعدم كفاية المهارات التقنية لموظفي المكتبة في عمليات الرقمنة والتحميل ، والصيانة ، بالإضافة إلى ضعف القدرة على تهيئة برامج المستودعات الرقمية المؤسسية والتعامل مع نظم التشغيل Unix and Linux. والفهم المحدود لاستخدام مخططات الميتاداتا وقضايا حق المؤلف.

ثانيا: الإطار النظري للدراسة:

تمهيد:

يتسم عصرنا الحالي بالتطور السريع والمتلاحق لتقنيات المعلومات والاتصالات وما انجر عنها من تغيرات جدرية في طرق إنشاء المعرفة وحفظها وبثها، وقد رأت الجامعات ومكتباتها أنه لا مناص من انشاء مستودعات رقمية رغم التحديات والعقبات التي تواجه عمليات الرقمنة لأن التطور السريع لتكنولوجيا المعلومات وشبكة الأنترنت أحدث الكثير من التغيرات الأساسية في العالم حيث ظهر ما يسمى بالجريمة المعلوماتية والتي أصبحت تهدد أمن المعلومات مما دفع بمختلف المؤسسات على غرار المؤسسات الأكاديمية للاهتمام باتخاذ كافة التدابير الوقائية اللازمة لحماية أمن المعلومات على مستوى مستودعاتها الرقمية، وهي تلك الأساليب المعتمدة للسيطرة على مصادر المعلومات الرقمية وحمايتها من السرقة والنسخ والتعديل والابتزاز والتلف والضياع والتزوير والاستخدام غير المرخص وغير القانوني للكيانات الرقمية بالمستودعات.

2-1- المستودعات الرقمية المؤسساتية:

أول ظهور لمصطلح المستودعات المؤسساتية في الأدب كان سنة 2002م مع قيام اتحاد المصادر الأكاديمية والنشر الأكاديمي SPARC بنشر ورقة تعرف المستودعات الرقمية المؤسساتية على انها: مجموعة رقمية تلتقط وتحفظ المخرجات الفكرية لمجتمع جامعي واحد أو الكثير من المجتمعات الجامعية [1].

ومن بين التعريفات الأخرى نذكر بإيجاز ما يلي:

▪ يعرف Stephen Penfield المستودعات المؤسسية بأنها أرشيفات على الخط المباشر تؤسس وتدار من قبل المؤسسات والمعاهد البحثية، وتحتوي على المقالات المنشورة من قبل الباحثين العاملين بهذه المؤسسات البحثية كما تتيح النص الكامل للمواد بالمجان دون قيود في الوصول والإتاحة [2].

▪ حسبClifford Lynch فإن المستودع الرقمي المؤسسي هو: أساسه جامعة وهو عبارة عن مجموعة من الخدمات التي تقدمها الجامعة لمجتمعها الأكاديمي من أجل إدارة ونشر المواد الرقمية التي أنتجتها المؤسسة وأعضاء مجتمعها. وان يكون هناك التزام

[1] عبد الجواد، سامح زينهم. المستودعات الرقمية: استراتيجيات البناء والإدارة والتسويق والحفظ. – بنها: جامعة بنها، 2014. ص50.

[2] Penfield, Stephen. a mandate to self-archive: the role of open access in institutional repositories retrieved from: http:..eprint.nottingham.ac.uk.archive.00000152.01

تنظيمي للإشراف على هذه المواد الرقمية، بما في ذلك الحفظ طويل الأجل كلما كان ذلك مناسبا، وكذلك قضية التنظيم والإتاحة أو التوزيع [1].

ومما سبق نحاول أن نخرج بتعريف للمستودع الرقمي:

وهو عبارة عن فضاء عمل تعاوني على الانترنيت لجمع وحفظ الناتج العلمي الأكاديمي للمؤسسات ومراكز الأبحاث، قصد تكوين ذاكرة جماعية. بحيث يمتاز بالتراكمية والحفظ على المدى البعيد والذي تكون نتيجته إتاحة حرة ودائمة.

2-2- الكيانات الرقمية بالمستودعات الرقمية المؤسساتية: المفهوم والأنواع:

تعرف كل من Julie Allinson and Mahendra Mahey الكيانات الرقمية بأنها أي شيء يتم تخزينه بواسطة المستودعات الرقمية، ويمكن أن يكون أي وسيط مثل الصورة والمقالة وتسجيلة الميتاداتا ويملك معرفا محددا وما وراء البيانات، كل ذلك يكون كيان رقمي [2].

ويعرفها "أسامة محمد عطية خميس" بأنها الأوعية الإلكترونية في صورتها المتقدمة والتي تحتوي معلومات مختلفة في شكل النص والصورة والصوت والرسم والحركة بعضهم أو كلهم مجتمعين لخدمة محتوى واحد [3].

وعلى ضوء ما ورد سابقا يمكننا الخروج بمفهوم أوسع وأشمل للكيانات الرقمية وهو:" تلك المحتويات والأصول الرقمية التي تحتوي معلومات وبيانات متنوعة، يتم حفظها بالمستودعات الرقمية على المدى البعيد من أجل عملية البحث والاسترجاع فيما بعد، وذلك وفق معايير محددة تضمن التكاملية والاستمرارية والسلامة لهذه الكيانات."

من خلال التعريفيات السابقة يمكن تحديد أشكال وأنواع الكيانات الرقمية التي عادة ما يتم إيداعها بالمستودعات الرقمية المؤسسية فالكيانات في أشكالها يمكن أن تكون: نصوص رقمية، أو فيديو رقمي أو صورة رقمية، كما يمكن أن تكون عبارة عن صوت رقمي.

- أما الأنواع فيمكن حصرها فيما يلي: -الرسائل والأطروحات الجامعية -المسودات pre-prints. المطبوعات الإلكترونية e-prints -العروض التقديمية للمؤتمرات -الكتب الإلكترونية -مقالات الدوريات - منشورات الجامعة - مجموعات البيانات - الصور - الكيانات التعليمية - النشرات الدورية - مدونات الحرم الجامعي - الفيديوهات التعليمية -مقاطع صوتية - مخطوطات - التقارير الفنية وأوراق العمل - الأصول الرقمية المؤسسية من المجموعات الخاصة بالمكتبة، وغيرها من الوثائق.

2-3- استراتيجيات أمن المعلومات بالمستودعات الرقمية:

2-3-1- الحاجة إلى استراتيجية أمن المعلومات:

بسبب وجود خطورة كبيرة من اختراق أو تسرب أو تحريف البيانات وجب على المنظمات توفير سبل الحماية من الاختراق وتحديد الاستراتيجيات والإجراءات الدفاعية والوقائية من التخريب والحفاظ على المعلومات من التعدي عليها بالصور العديدة والمختلفة من

[1] نورس، احمد. متطلبات بناء مستودع رقمي في جامعة البعث، مجلة جامعة البعث مج. 83. ع 34 سنة 2016. ص.139-149.

[2] Julie Allinson and Mahendra Mahey. WORKSHOP ON INNOVATION IN SCHOLARY COMMUNICATION, AVALABLE FROM: www.ukoln.ac.uk

[3] خميس، أسامة محمد عطية. الكيانات الرقمية (المحتوى الرقمي) في المستودعات الرقمية على شبة الأنترنت: المفهوم. البرمجيات. البناء. الإيداع الرقمي. ج1. - القاهرة: الشركة العربية المتحدة للتسويق والتوريدات، 2013، ص.58.

خلال وضع استراتيجية لأمن المعلومات ترتكز على النقاط الأساسية التالية: السرية والموثوقية، التكاملية وسلامة المحتوى، استمرارية توافر المعلومات والخدمات، والمسؤولية تجاه أي تصرف مرتبط بالمعلومات.[1]

2-3-2- أمن المعلومات في المستودعات الرقمية:

بما ان المستودعات الرقمية هي جزء من البيئة الرقمية فإن مفهوم أمن المعلومات في المستودعات الرقمية هو نفسه مفهوم امن المعلومات في البيئة الرقمية. وقد تعددت تعريفات أمن المعلومات في البيئة الرقمية وتنوعت حسب زاوية الرؤية فمن الناحية الأكاديمية يعرف امن المعلومات في البيئة الرقمية على أنه قضية تبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. ومن زاوية التقنية فهو الوسائل والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية [2].

ويرى الباحثان أن مفهوم أمن المعلومات في المستودعات الرقمية يدور حول تحديد الوصول أو الاطلاع على البيانات المخزنة فيها من خلال منع كل غريب من التلاعب بالأجهزة والمعلومات.

2-4- المخاطر التي تهدد محتوى الكيانات الرقمية بالمستودعات الرقمية:

وتتمثل المخاطر المهددة للمعلومات في المستودعات الرقمية في المحاور التالية:

2-4-1- المخاطر الطبيعية: وهي الحرائق، والفيضانات وغيرها من الكوارث الطبيعية المحتملة.

2-4-2- المخاطر التقنية: غالبا ما تتمثل في انقطاع التيار الكهربائي، وانقطاع في شبكة الانترنت، وتلف البيانات....

2-4-3- المخاطر التكنولوجية: وهي تلك المشاكل المهددة لأمن المعلومات وعادة ما يكون العنصر البشري هو السبب الرئيسي والفعال في هذه المخاطر وتتمثل في: القرصنة والفيروسات، وديدان الأنترنت، والتجسس على بيانات النظام، والاختراق الأمني للنظام سواء من الداخل أو من الخارج، وكذلك سرقة المعلومات.

- ولعل من أبرز المخاطر التي تتعرض لها أنظمة المستودعات الرقمية ما يلي [3]:

✓**الهاكرز Hackers**: مما يؤدي اقتحامه للشبكة إلى تفشي أسرار العمل والعاملين في النظام أو تخريب البيانات وإتلافها أو تعرض البيانات للتغيير أو التعديل أو المسح بغرض تحريف البيانات أحيانا أو سرقتها في أحيان أخرى.

✓**التنصت:** هو التجسس على مستخدمي النظام.

✓**اقتحام الفيروسات للشبكة:** والتي يمكن أن تتسبب في تعرض أجهزة الشبكة وبياناتها للتلف أو الفقدان.

✓**الاطلاع غير المرخص:** ويتمثل في إطلاع الأشخاص المصرح لهم باستخدام النظام على معلومات غير مصرح لهم بالاطلاع عليها.

✓**الاعتداء على نظام الحماية:** تعطيل أحد الأشخاص لنظام الأمن الخاص بالشبكة أو كشفه لإجراءات الحماية المتبعة.

---

[1] أحمد، أشرف السعيد. استراتيجية أمن المعلومات. – القاهرة: مطابع الشرطة، 2014. ص.13.

[2] سعيدي، سليمة. أمن المعلومات وأنظمتها في العصر الرقمي. – الإسكندرية: دار الفكر الجامعي، 2017. ص.28.

[3] علي، عادل نبيل شحات. تقنيات أمن وحماية المحتوى الرقمي للمستودع الرقمي للرسائل الجامعية المصرية، بنها: جامعة بنها، مجلة كلية الآداب مج1، ع1. 2017 متوفر على الرابط: https:..journals.ekb.eg.article_104577_7fcabd3f4ee8a3128e3194f2236c7d77.pdf
تمت الزيارة يوم: 28-12-2021

• كما توجد هناك عدة مخاطر بفعل الانسان ويمكن أن تكون غير مقصودة لأن العنصر البشري يمثل مصدرا كبيرا للخطر على امن المعلومات ونذكر منها [1]:

✓**خطر سوء التصميم**: ويقصد بسوء التصميم أن تكون هناك بعض الأخطاء الفنية في تصميم أساليب التأمين والحماية للأنظمة التي تعمل عليها الشبكة.

✓**خطر سوء الاستخدام**: هناك العديد من الأخطاء التي تنتج عن سوء استخدام العاملين لشبكات المعلومات، مما يلحق الضرر البالغ على أمن وسلامة البيانات، وينتج ذلك غالبا بسبب نقص التدريب والتأهيل للعنصر البشري.

وفي ظل التقدم السريع في تكنولوجيا المعلومات ظهرت عدة مظاهر للنصب والاحتيال في البيئة الرقمية أو بالخصوص في بيئة الوصول الحر ومختلف عناصرها ومكوناتها وعلى سبيل المثال نذكر:

✓**التزوير**: حيث يلجأ عامة المزورين إلى التلاعب بمستند صحيح لوضعه في صورة تلائم مصلحة ما من مصالحهم وحتى تتم الاستفادة من المستند بصورته الجديدة. ويلجأ المزورون إلى جعل هذا التلاعب خفيفا ما أمكن [2].

✓**إزالة المعلومات**: وتتم إزالة المعلومات من الوثيقة بإحدى الطرق التالية، إما اتلاف الجزء من الوثيقة الذي يحمل المعلومات المراد إزالتها وذلك ببتر صفحة أو أكثر من الوثيقة المتعددة الصفحات أو بقطع الجزء الأعلى أو الأسفل من الوثيقة الذي يحتوي على التاريخ أو أي فقرة يراد التخلص منها. وإما عن طريق المحو ويتم المحو من الوثائق عادة بطريقة من الطرق الثلاثة التالية: المحو الآلي أو الكشط Erasure by Abraision، أو المحو باستعمال الوسائل المذيبة Erasure with solvents، أو المحو الكيميائي Chemical Erasure.

✓**النسخ غير الشرعي**: والمعروف أيضاً باسم الانتحال المباشر، أي استخدام نص كامل من مقال أو دراسة، بدون أي تعديل، وبدون توثيق. مما أدى إلى انتشار ورواج ظاهرة النصب والاحتيال المعلوماتي.

✓**السرقة العلمية**: وهي قيام أحد الأشخاص بسرقة أعمال أو أفكار الآخرين، وإدراجها في مقالته أو دراسته على أنها اجتهاد شخصي منه، بدون ذكر المصدر الأصلي.

2-6- سبل حماية المستودعات الرقمية من مخاطر أمن المعلومات المهددة لها:

لا بد عند حماية أي معلومة في قواعد البيانات أو غيرها مراعات القواعد التالية: (السرية، التكاملية، والاستمرارية)، ووضع استراتيجية أمنية مبنية على الرد على الاستفسارات التالية: ما الذي أريد أن أحميه؟ وضد من أحمي؟ وما هي الأضرار الناجمة عن عدم تأمين المحتوى الرقمي؟ وما هي الإمكانيات والسبل المتوفرة لحماية المحتوى الرقمي على شبكة الأنترنت؟ وللإجابة عن هذه التساؤلات نتناول أربعة عناصر رئيسية خاصة بأمن المعلومات بالمستودعات الرقمية على النحو التالي:

2-6-1- التأمين المادي للأجهزة والمكونات المادية:

التأمين المادي للأجهزة يقصد به تأمين المكونات المادية للنظام من العبث بها والحفاظ عليها من التلف أو المخاطر الطبيعية كالفيضانات والحرائق، والتدخلات البشرية للأشخاص غير المرخص لهم. وهي تمثل كافة المعدات والأدوات المادية التي يتكون منها النظام كالحواسيب المخصصة للخوادم والشاشات والطابعات وكذلك الشبكة المحلية والخارجية، ووسائط التخزين المادية [1].

[1] أحمد، أشرف السعيد. المصدر السابق، ص.104.

[2] عطيات، عبد الرحمان شعبان. أمن الوثائق والمعلومات. – عمان: دار الحامد للنشر والتوزيع، 2014. ص.39.

ويتم ذلك من خلال تأمين موقع المستودع أو النظام وتوفير أجهزة الحماية من الأخطار وذلك من خلال استخدام الوسائل التالية:

- توفير أجهزة الإنذار ضد الحرائق داخل غرف الخوادم مع أجهزة الإطفاء اليدوية.
- توفير الشروط الملائمة لمبنى المستودع وذلك بمراعات شروط التهوية المناسبة وكذلك درجات الحرارة والرطوبة للحفاظ على مكونات النظام من التلف.
- غرف الخوادم يجب أن تكون غير معرضة لمياه الفيضانات وذلك بالحد من خطر التسرب وعزل الأسطح ضد مياه الأمطار.
- غرف الخوادم يجب أن تكون مغلقة وغير معرضة للاقتحام.
- توفير مصدر طاقة دائم مع مصدر بديل لتوليد الطاقة الكهربائية لتفادي توقف الأجهزة عن العمل.
- توفير الصيانة للأجهزة بشكل دوري ومستمر لضمان استمرارية عملها وعدم توقفها بسبب المشاكل التقنية.
- كابلات الشبكة يجب أن تكون من النوع الجيد (الألياف البصرية Optical fiber على سبيل المثال) مع مراعات جودة التغليف لهذه الكابلات ووضعها في أماكن آمنة غير معرضة لوصول الأشخاص غير المختصين.
- توفير أنظمة الحماية مثل كاميرات المراقبة ووسائل الإنذار المبكر ضد السرقة في حالة فتح البوابات بعد مواعيد العمل المحددة أو دخول شخص غير مصرح له إلى غرف الحواسيب.
- توفير الحراسة بصفة دائمة ومستمرة وإنشاء سجلات يتم فيها تسجيل توقيت الدخول والخروج للعاملين.

2-6-2- تقنيات الأمن الخاصة بالموارد البشرية:

يعد العنصر البشري مصدر الخطر الأكبر لذلك يجب على الإدارة العليا للمستودع الرقمي توفير الوسائل والإجراءات التي تحقق الحماية من الأحداث المستقبلية غير المرغوب فيها، وذلك بتحديد أصحاب الحقوق المتصلين بالمستودع كخطوة أولى لأن هناك العديد من المجموعات والأفراد داخل المؤسسة يمكنهم الاستفادة من المستودع لذلك يمكن تحديدهم كأصحاب حقوق ويجب اتخاذ الوقت المناسب للتأكد من كل شخص يملك اهتماما بالمستودع وتحديد الفوائد الأساسية والتي سوف تطبق على كل مجموعة من أصحاب الحقوق وذلك لضمان بداية عمل المستودع على أرضية إيجابية، وأصحاب الحقوق الأساسيين هم: الإداريون والإدارة العليا وصانعي السياسة بالجامعة، الأكاديميون " مؤلفين وباحثين"، العاملون بالمكتبة، العاملون بالدعم الفني" المختصين في الإعلام الآلي"[2].

وبعد ذلك وضع ضوابط ومعايير دقيقة لاختيار العاملين كخطوة ثانية، وصياغة برامج لتأهيلهم وتدريبهم من جانب متخصصين، طبقا لمستوى وأهمية الوظيفة ومسؤولياتها، ويعد تأهيل وتدريب العاملين من أهم وسائل رفع كفاءاتهم سواء في فترة الإعداد أو قبل دخول الخدمة بهدف إمدادهم بالمعلومات الضرورية التي تضبط سلوكهم العملي وتوعيتهم بمدى أهمية الجانب الأمني للنظام وإظهار المخاطر التي قد تنجم جراء عدم الاهتمام بموضوع أمن المعلومات بالمستودع.

ولا يكفي هذا فحسب بل يجب وضع استراتيجية خاصة لضبط سلوك العاملين بالمستودع الرقمي لتفادي مختلف الانزلاقات التي يمكن أن تحدث عمدا من طرف العنصر البشري العامل بالنظام كما يجب توفير مختلف الوسائل التي تضبط صحة الاستخدام

[1] أحمد، أشرف السعيد. المصدر السابق، ص51.

[2] عبد الجواد، سامح زينهم. المرجع السابق، ص212.

لمحتوى المستودع من طرف المستفيدين الخارجيين وحماية البيانات وحقوق الملكية الفكرية، وتختلف هذه الاستراتيجية تبعا للتقنية المستخدمة في كل نظام، وتتمثل هذه الاستراتيجية في العناصر التالية:

• **كلمات السر الخاصة بالمستخدمين:** وهي من أهم الشروط والارشادات الأمنية التي يجب مراعاتها عند فتح الحسابات للموظفين العاملين بالمستودع وتحديد المهام والصلاحيات الخاصة بكل موظف على حدا كل حسب رتبته الإدارية، وتتطلب أن تخضع لسياسة مدروسة وارشادات يمكن تلخيصها فيما يلي:

❖ الالتزام بالحد الأدنى للطول وهي ثمانية حروف حسب القياسات الدولية.

❖ يجب أن تخضع للتغيير بشكل دوري كل 60 يوم على الأقل وذلك حسب المواصفات العالمية.

❖ يجب أن تركب من مزيج بين الحروف الكبيرة والصغيرة والأرقام والرموز لكيلا يسهل كشفها.

❖ يجب ألا ترتبط بأي معلومات خاصة بالمستخدم مثل اسم الشخص، اللقب، تاريخ الميلاد...

• **التوثق من شخصيات المستخدمين:** وهي عبارة عن وسائل للتعرف على شخصيات المستخدمين عند الدخول للنظام ويتم عن طريق هذه الوسائل التحكم في الأشخاص المسموح لهم بالوصول للمعلومات لأن عكس ذلك يؤدي إلى فقدان سرية المعلومات وربما صحتها، وتتمثل هذه الوسائل في:

❖ بطاقات الهوية العادية Identity Cards التي تستعمل عند الدخول لغرف الخوادم.

❖ البطاقات الذكية المستخدمة للتعريف Smart Cards.

❖ وسائل التعريف البيولوجية Biological Identification التي تعتمد على سمات معينة في شخص المستخدم مثل بصمة اليد وملامح الوجه.

• **الأقفال الإلكترونية Electronic Locks:** والتي تؤمن الدخول إلى النظام والخروج منه وهي محددة بفترة زمنية معينة، في حالة ترك أحد الموظفين حسابه مفتوحا عن طريق الخطأ أو النسيان تقوم هذه الأقفال بغلق الحساب تلقائيا بعد مرور الفترة الزمنية المحددة وذلك لضمان عدم اختراق الحساب.

• **حذف الموظفين المنتهية مدة صلاحيتهم:** في حالة استقالة أحد الموظفين من وظيفته أو طرده لسبب ما أو احالته للتقاعد يجب على إدارة النظام حذف حسابه ومنعه من الدخول لقاعدة بيانات النظام وذلك حفاظا على سرية وخصوصية البيانات والمعلومات، وضمان عدم الوصول إليها والتلاعب بها من طرف الموظف المنتهية صلاحياته.

• **اللوائح الاشارية:** وهي عبارة عن إرشادات وتوصيات وقوانين خاصة بالاستخدام موجهة للمستفيدين الخارجيين عادة ما توضع في الصفحات الرئيسية للمستودعات يتم فيها توجيه المستفيدين لطرق الاستخدام واحترام الشروط والقوانين المنصوص عليها، ووضع قوانين حقوق الملكية الفكرية والتوصية باحترامها.

– بالإضافة إلى كل هذه الوسائل التقنية وجب كذلك على إدارة المستودع الاعتماد على أساليب الرقابة، كحراس الأمن وتوفير السجلات لتسجيل أي حدث بعد انتهاء ساعات العمل، وكذلك الاستعانة بكاميرات المراقبة لتأمين مبنى المستودع وحمايته من دخول الأشخاص غير المرخص لهم بذلك.

2-6-3- تأمين النظام والتطبيقات:

يقصد بأمن النظام والتطبيقات حماية أنظمة التشغيل المعتمدة في إدارة منظومة الحواسيب والعمل على تقليل أو منع محاولات التلاعب بالثوابت أو المفاتيح المنطقية التي تتحكم في عملية السيطرة على تنفيذ البرمجيات من جهة وعلى إدامة مراقبة نظام التشغيل على مجمل الفعاليات داخل المنظومة من جهة أخرى [1].

وبناء على ذلك يمكن تحديد مستويات الحماية طبقا لسرية وخطورة البيانات من خلال وضع سياسات مسبقة مبنية على التنبؤ بجميع الاحتمالات الواردة ووضع الخطط وتوفير التقنيات والوسائل التي من خلالها يمكن حماية النظم والتطبيقات قبل الولوج إليها والعبث بها، ولا يمكن تحقيق ذلك إلا من خلال:

- **القدرة على تحديد مصادر التهديد:** معرفة مصادر التهديد هي القدرة على معرفة نوع التهديد أولا، ثم معرفة مدى نجاح مصدر التهديد في الإضرار بالنظام من خلال تحديد نقاط الضعف الموجودة به [2]. وبعد ذلك يتم العمل على تطوير النظام تماشيا مع طبيعة كل المخاطر المهددة ووضع مختلف السبل للحد منها قبل وقوعها.
- **مضادات الفيروسات:** ويقصد بها البرمجيات التي تستخدم لمنع واكتشاف وإزالة البرمجيات الخبيثة، بما فيها فيروسات الحاسب والديدان وأحصنة طروادة، وملوثات مقاطع التحميل، والكود التخريبي وغيرها، والتي هي عبارة عن أدوات برمجية تستخدم من أجل القيام بعمليات الهجوم الفعال والمضر بالنظام. [3].

والعلاج الناجع للفيروسات يكون بصفة مسبقة من خلال منعها أو عدم السماح لها بالدخول لنظام الحاسوب إلا أن تحقيق ذلك يعد من الصعوبة ولكن إذا حدثت الإصابة بالفيروس فهناك إجراءات يمكن اتخاذها في مواجهة الفيروس أو معالجته وتقليل عواقبه، وهي عبارة عن خيارات يتم اختيار الأنسب منها والذي يوفر أعلى حماية وأقل تكلفة. عن طريق:

- ✓ الاكتشاف Detection: هو تحديد زمن حدوث الإصابة بالفيروس وتحديد مكانه.
- ✓ التعرف على الفيروس Identification: عند اكتشاف الإصابة تأتي مرحلة التعرف على نوع الفيروس الذي سبب الإصابة وذلك من خلال علامات معينة في كود الفيروس أو بسلوكه الذي يقوم به في النظام.
- ✓ إزالة الفيروس Virus Removal: بعد التعرف على نوع الفيروس تتم إزالته من الملف المصاب وإرجاع الملف إلى وضعه الأصلي وتعقب كل النسخ الأخرى من الفيروس للحد من انتشاره مرة أخرى.

- **نظام كشف التطفل على الشبكة NIDS**: " network intrusion détection system " إن عملية كشف التطفل هي عبارة عن تتبع دوري ومستمر لخطر الاختراق والتسلل هو من أساليب الدفاع المهمة للنظم الآلية. ومن المعلوم أن واحد من أكثر التهديدات الخطيرة لأمن المعلومات هو المتطفل، وبصورة عامة يشار إلى المتطفل بأسماء مختلفة ومتنوعة أبرزها الهاكر Hacker أو كاسر الأمنية Cracker، وهناك ثلاث أصناف من المتطفلين هي [4]:

[1] صادق، دلال؛ الفتال، حميد ناصر. أمن المعلومات. – عمان: دار اليازوري العلمية للنشر والتوزيع، 2008. ص99.

[2] العريشي، جبريل بن حسن؛ الشلهوب، محمد حسن. أمن المعلومات. – عمان: الدار المنهجية، 2015. ص 79.

[3] الطيطي، خضر مصباح إسماعيل. أساسيات أمن المعلومات والحاسوب. – عمان: دار الحامد، 2009. ص157.

[4] الحمامي، علاء حسين؛ العاني سعد عبد العزيز. تكنولوجيا أمنية المعلومات وأنظمة الحماية. – عمان: دار وائل للنشر والتوزيع، 2007. ص300.

✓المتنكر Masque rader: هو فرد غير مخول باستخدام الحاسوب ويخترق سيطرة الوصول إلى النظام للاطلاع على امتيازات المستخدمين القانونيين.

✓الفضولي Misfeasor: هو مستخدم مخول يصل إلى بيانات أو برامج ليس مخول بالوصول إليها أو هو مخول بالوصول لكنه يسيء الاستخدام من أجل مصلحته الشخصية.

✓ المستخدم السري Clandestine User: هو مستخدم يسيطر على مسيطرات الإشراف للنظام ويستخدمها من أجل تغيير التدقيق ومسيطرات الوصول.

وللحد من هذا التهديد يستوجب على القائمين على المستودعات اقتناء وتثبيت أنظمة كشف التطفل على الشبكة حيث تستطيع هذه البرمجيات مراقبة الحزم على اتصالات الشبكة ومحاولة اكتشاف المتطفل من خلال مقارنة نموذج المتطفل مع قاعدة بيانات مخزنة فيها نماذج الهجوم المعروفة.

• **الجدران النارية Firewalls**: يجد القائمين على الأنظمة صعوبة متزايدة في حماية أنظمة الحاسوب من المتطفلين الخارجيين وذلك لزيادة عدد الحواسيب المرتبطة بالشبكة لأن فكرة قطع اتصال حاسوب من الشبكة هو أمر مخالف لمعايير تكوين الشبكات، لذلك وجد خيار آخر وهو جدران النار Firewalls ويعد من أبرز الطرق لحماية الشبكة من أي ضرر خارجي، والهدف من جدران النار هو تقليص التدمير الذي يحصل على الشبكة من خلال تقليص حقوق وصول الخارجيين إلى الشبكة [1].

وهذه التقنية هي عبارة عن دمج البرمجيات والأجهزة لعزل العناوين المطلوبة عن غير المطلوبة لأن جدار النار سواء كان نظام برمجي أو مادي فهو مصمم لتصفية الرسائل غير المطلوبة ويسمح بالاتصالات القانونية فقط، حيث تنفذ جدران النار مهامها عن طريق موجات العزل Screening Routers والمضيفات Bastion أو الاثنان معا ويتم ترتيب العزل للسيطرة على توجيه حزمة بيانات الشبكة مثل عنوان المصدر Source واتجاه المصدر Direction.

• **أمنية البريد الالكتروني**: يعتبر البريد الالكتروني من أوساط الاتصال الموثوقة والآمنة بالنسبة لمستخدميه إذا كان للنصوص فقط، أما إذا كان هناك أشخاص يرغبون في الحصول على فائدة أكبر من استخدام البريد الالكتروني كالصفات المتطورة لبرمجيات البريد الالكتروني فإن مجرد فتح رسالة واردة تعد تجربة مخيفة لأن في تلك الرسالة يستطيع المرسل أن يرسل ملف أو عنوان أو اسم يحتوي على ملف مغشوش قد يؤدي إلى هجوم خارجي على قاعدة النظام، وذلك لما يحتويه البريد الالكتروني من أخطار متمثلة غالبا في:

✓يحتوي البريد الالكتروني على انتهاك لقانون معين (تهديد، ابتزاز ...).

✓قد يحتوي البريد الالكتروني على فايروس أو حصان طروادة ويعتقد المرسل بأنه من المؤكد أن تفتح الرسالة إذا كانت من شخص معروف.

✓يطلب البريد الالكتروني معلومات قد ترغب بإعطائها للشخص الذي ينتحل المرسل شخصيته.

ومن بين التقنيات التي يجب تأمين البريد الالكتروني بها هي:

- الأمر المهم الذي يجب التركيز عليه هو عدم فتح رسائل البريد الالكتروني غير معلومة المصدر.

- تشفير البريد الالكتروني غير المتناظر والذي يعتمد على زوج من المفاتيح المتقاربة يستخدم واحد منها للتشفير والآخر لفتح شفرة البيانات.

[1] الحمامي، علاء حسين؛ العاني سعد عبد العزيز. المصدر السابق. ص329.

- معرفة مصدر البريد الالكتروني من خلال تدقيق العناوين الحقيقية للبريد ومكان ارسال الرسالة.
- اليقظة الدائمة والتأكد من البريد وملاحقه حتى وإن كان البريد من شخص معروف لأن الفايروس عادة ما يكون في ملاحق البريد الالكتروني.

• **النسخ الاحتياطي**: بالإضافة إلى توفير كل التقنيات السابقة يجب على إدارة المستودع الأخذ بعين الاعتبار أن مختلف الأنظمة وأجهزة الكمبيوتر يمكن أن تصل لمرحلة الفشل في أي وقت ممكن، وقد تفقد السجلات الحيوية والنظم ومنتجات العمل بشكل لا رجعة فيه إذا تم تخزينها فقط على تلك الأنظمة وأجهزة الكمبيوتر، وقد يسبب هذا الفقد نقص الإنتاجية وزيادة التكلفة، لذا وجب النسخ الاحتياطي للبيانات وهو عملية نسخ وتخزين واستعادة لبيانات الكمبيوتر والتي يمكن أن تكون في أي صورة ما، ويعمل النسخ الاحتياطي على ما يلي [1]:

- توفير تخزين آمن لأصول البيانات الهامة لسير العمل في (جهة العمل).
- منع فقدان البيانات في حالة الحذف أو تلف البيانات أو فشل النظام أو حدوث الكوارث.
- السماح باستعادة البيانات المؤرشفة في الوقت المناسب في حالة حدوث كارثة أو فشل في النظام.

والغرض من هذه السياسة ضمان توفر نسخ احتياطية ومفيدة عند الحاجة إليها سواء كان ذلك لمجرد استرداد ملف معين أو عند الحاجة إلى استرداد كامل لأنظمة التشغيل. ولنجاح هذه السياسة وجب عند عملية التخزين الاحتياطي مراعات النقاط التالية:

• يجب الحفاظ على الفصل الجغرافي بين أماكن حفظ النسخ الاحتياطية وموقع جهة العمل، بمسافة مناسبة وذلك للحماية من الحرائق أو الفيضانات أو الكوارث، للابتعاد عن أي ضرر في حالة حدوث كارثة في الموقع الرئيسي.

• عند نقل وسائط النسخ الاحتياطي أو حفظها خارج الموقع يجب ضمان –وبشكل معقول– عدم تعرضها للكوارث كالسرقة أو النار، كما يجب اختيار أماكن تخزين تستخدم أساليب حماية من الكوارث البيئية وتخضع للتحكم في الوصول لضمان سلامة وسائط النسخ الاحتياطي.

• يسمح بالنسخ الاحتياطي عبر الإنترنت إذا كانت الخدمة تلبي المعايير المحددة لها.

2-6-4- أساليب الحماية وإجراءات الوقاية لمحتوى الكيانات الرقمية:

يجب على القائمين على امن المعلومات بالمستودعات أن يأخذوا في الحسبان كل أنواع المخاطر التي يمكن أن تتعرض لها محتويات الكيانات الرقمية المخزنة والمنشورة بسبب ما يتعلق بها من انتهاكات تتمثل في البيانات المفقودة أو المسروقة او حتى المتلفة. ولتأمين الكيانات الرقمية من هذه المخاطر المهددة لها يجب وضع سياسات قوية تمكن من استغلال جميع التقنيات والوسائل التي من شانها حماية المحتوى الرقمي وتأمينه ويمكن حصر مختلف هذه التقنيات فيما يلي:

• **التشفير**: وهو عملية ترميز البيانات وتحويلها من النص العادي المقروء إلى شفرات غير مفهومة تبدو غير ذات معنى، كي يتعذر قراءتها أو فهمها من أي شخص غير مرخص بالاطلاع على تلك البيانات والمعلومات بواسطة خوارزميات التشفير، ومفاتيح التشفير "Keys" ". [2].

---

[1] سياسة النسخ الاحتياطي – الهيئة الوطنية لأمن وسلامة المعلومات. متوفر على الرابط التالي: https:..nissa.gov.ly.main-services.data-backup-policy. تمت الزيارة يوم: 16-01-2022.

[2] رحمه، علي محمد دهب. التشفير وأمن المعلومات. –كردفان: جامعة كردفان، 2013. ص 19.

ومن انواعه: التشفير المتناظر الذي يعتمد على مفتاح واحد للتشفير وفك الشفرة وبذلك فإن المفتاح يجب ان يكون معروف من طرف المرسل والمستقبل، شرط ان لا يرسل المفتاح مع الرسالة وإنما يرسل بطرق أخرى.

أما النوع الثاني فهو التشفير غير المتناظر والذي يستخدم فيه المرسل والمستلم مفاتيح مختلفة (مفتاح عام ومفتاح خاص) يكون المفتاحان مرتبطان ببعضهما البعض إلا أن أي منهما لا يدل على الآخر [1].

وتكمن أهمية التشفير في قدرته على التغلب على أهم الاخطار التي يمكن أن تمس المحتوى الرقمي والمتمثلة في:

- ✓ منع الاطلاع على المعلومات المحضورة.
- ✓ منع محاولات تعديل البيانات وتحويلها لوجهة أخرى.
- ✓ منع تأخير محتويات الرسائل المتبادلة.
- ✓ التصدي لمحاولات تغيير كلمات السر الخاصة بالمستفيدين.
- ✓ منع المساس بالبيانات المخزنة في قواعد البيانات ومحاولة التعديل عليها.

ومن هنا تتضح ضرورة الاعتماد على تقنية التشفير بالمستودعات الرقمية المؤسساتية لما له من أهمية كبرى في تأمين وحماية الشبكات والمحتوى الرقمي، خاصة في ظل ظهور العديد من تقنيات التنصت والتقاط البيانات.

- **التوقيع الإلكتروني:** ذكر قاموس Robert الفرنسي التوقيع على أنه علامة شخصية أو خطية يضعها الموقع ليأكد مضمون الورقة وصدق ما كتب بها مع إقراره بتحمل المسؤولية والتزامه بما جاء فيها [2].

و هو عبارة عن تلك البيانات التي تتخذ هيئة حروف أو أرقام، أو رموز، أو إشارات تكون مدرجة بشكل إلكتروني، أو رقمي، أو ضوئي أو أي وسيلة أخرى مماثلة في رسالة معلومات أو مضافة عليها أو مرتبطة بها ولها طابع يسمح بتحديد هوية الشخص الذي وضع التوقيع وتميزه عن غيره [3].

ويستعمل التوقيع الالكتروني في حماية محتوى الكيانات الرقمية من مختلف التلاعبات ومحاولات التعدي على مضمونها لما له من حجية كبيرة في الاثبات أي أن كل محتوى رقمي لكاتب أو مؤلف معين يتضمن في طياته توقيعا إلكترونيا يكسب صاحب المحتوى الحجية القانونية وفقا للتشريعات التي أقرت بنظام التوقيع الالكتروني. لذلك وجب على أصحاب القرار بالمستودعات الرقمية استغلال هذه التقنية أو على الأقل الطلب من المؤلفين وضع التوقيعات الالكترونية عند رقمنة مؤلفاتهم قبل إيداعها بالمستودع.

- **تقنية العلامات المائية الرقمية:** العلامات الرقمية المائية هي تقنية جديدة من تقنيات التحقق من علائقية المعلومات الرقمية واسعة الانتشار عبر وسائل تناقل المعلومات المختلفة لأنها تحمي الصور الرقمية الثابتة والمتحركة، والأصوات من السرقة و تعطي

---

[1] غبيق، صلاح الهادي. التشفير وفك التشفير. مجلة العلوم الاقتصادية والسياسية لجامعة المرقب. – ليبيا. ع 02. 2013. ص508-543. متاح على الرابط: https://journals.asmarya.edu.ly تمت الزيارة يوم: 2022/01/17

[2] أبو هبة، نجوى. التوقيع الالكتروني: تعريفه مدى حجيته في الاثبات. – القاهرة: دار النهضة العربية، 2002. ص 39.

[3] البياتي، نادية ياس. التوقيع الالكتروني عبر الانترنت ومدى حجيته في الإثبات: دراسة مقارنة بالفقه الإسلامي. – عمان: دار البداية ناشرون وموزعون، 2013. ص 175.

المالك الشرعي لملفات المعلومات القدرة على التأكد من كون هذه الملفات نسخة شرعية أم أنه قد تم تحريفها بدون تخويل من مالكها [1].

والعلامة المائية الرقمية هي عملية إخفاء بيانات معينة داخل صورة أو ملف صوتي أو فيديو رقمي، وهي نوع من أنواع الوسوم (الختم) تتضمن إشارة أو علامة معينة يمكن ان تكون في شكل (عدد، نص، أو صورة) مع استخدام المفتاح لغرض الأمنية حيث يصعب على الأشخاص غير المخولين استرجاع أو معالجة العلامة المائية أو حذفها من الصورة الرقمية، وتستخدم للتحقق من صحة أو سلامة إشارة الناقل أو لإظهار هوية أصحابها.

ومن أحسن النظم المستخدمة في بناء العلامات المائية هو نظام العلامة المائية الرقمية المهجن، حيث تتضمن التقنية المهجنة استخدام طريقتين لإخفاء العلامة المائية الطريقة الأولى تستخدم المجال المكاني والطريقة الثانية تستخدم المجال الترددي في الإخفاء ويتم تحديد مواقع الإخفاء باستخدام طرق التقنيات الذكائية، التي تقسم العلامة المائية إلى جزأين لغرض إخفائها المجال المكاني والمجال الترددي بالاعتماد على المستخدم وكذلك أهمية المعلومة التي تتضمنها العلامة المائية [2].

من هذا المنطلق وجب صرف النظر تجاه هذه التقنية باعتبارها من التقنيات المتطورة التي تحمي الكيانات الرقمية وتحافظ على حقوق أصحابها ويستحسن الاعتماد على النوع الحساس من العلامات المائية الرقمية لما لها من خصائص تقنية متطورة تتجلى في:

✓وضع العلامة المائية المخفية في الصور الرقمية يصعب إدراكها أو تمييزها لأن العلامات المائية المخفية لا تحدث أي تشويه جزئي أو كلي في الصورة.

✓تعذر استخراج العلامة المائية من قبل المهاجمين حتى في حالة معرفة الخوارزمية التي تم بها عملية الإخفاء.

✓طريقة الإخفاء تكون شاملة لكل أجزاء الصورة أي أنه لا يمكن التلاعب في أي جزء من أجزاء الصورة الرقمية ففي حالة كون العلامة المائية في جزء أو حيز معين من الصورة فقط قد يمكن تجاوزه والعبث ببقية أجزاء الصورة الخالية من العلامة المائية.

✓مالك الصورة الرقمية الشرعي والمخولين وحدهم من لهم الحق في امتلاك المفتاح السري الخاص باستعادة العلامة المائية.

✓تعتمد على تقنية حساسة ضد الهجومات المتعددة التي قد تحصل للصورة.

• **التحقق من السرقة الأدبية:** بالإضافة إلى الوسائل والتقنيات السابقة الذكر يمكن لأصحاب القرار بالمستودعات الرقمية الاعتماد على مواقع التحقق من السرقة العلمية والتي يمكنها البحث بسرعة عن النسخ من المحتوى الخاص بها على شبكة الويب. حيث يمكن إما إدخال عنوان URL للمحتوى أو نسخ النص ولصقه لبدء البحث.

---

[1] الصميدعي، عامر تحسين سهيل. تطبيق تقنية حساسة لإخفاء العلامات المائية الرقمية في الصور الرقمية الثابتة. المجلة العراقية للعلوم الإحصائية، ع10. 2006. ص 107-120. متاح على الرابط:
https:..stats.mosuljournals.com.article_32585_63c1876bb604c8ab406f06738bf1c2fd.pdf تمت الزيارة يوم: 2022-01-19.

[2] عبد القادر، فردوس عدنان؛ خليل، شهباء إبراهيم؛ سليم، ندى نعمت. نظام العلامة المائية المهجن ذكائيا. مجلة الرافدين لعلوم الحاسبات والرياضيات، مج 7. ع 2. 2010. ص 125-138. متاح على الرابط: https:..www.iasj.net.iasj.download.423fccd9c52a04c9 تمت الزيارة يوم 2022-01-22.

كما يمكن التحقق من وجود محتوى مكرر باستخدام أداة مدقق الانتحال والسرقة الأدبية المجانية PLAGIARISM CHECKER. والذي يساعد مديري وصناع المحتوى من حماية منشوراتهم من السرقة العلمية ومنع نشر المحتويات المنسوخة [1]، كما يساعد في التحقق من أصالة المحتوى، وقياس نسبة الاقتباس

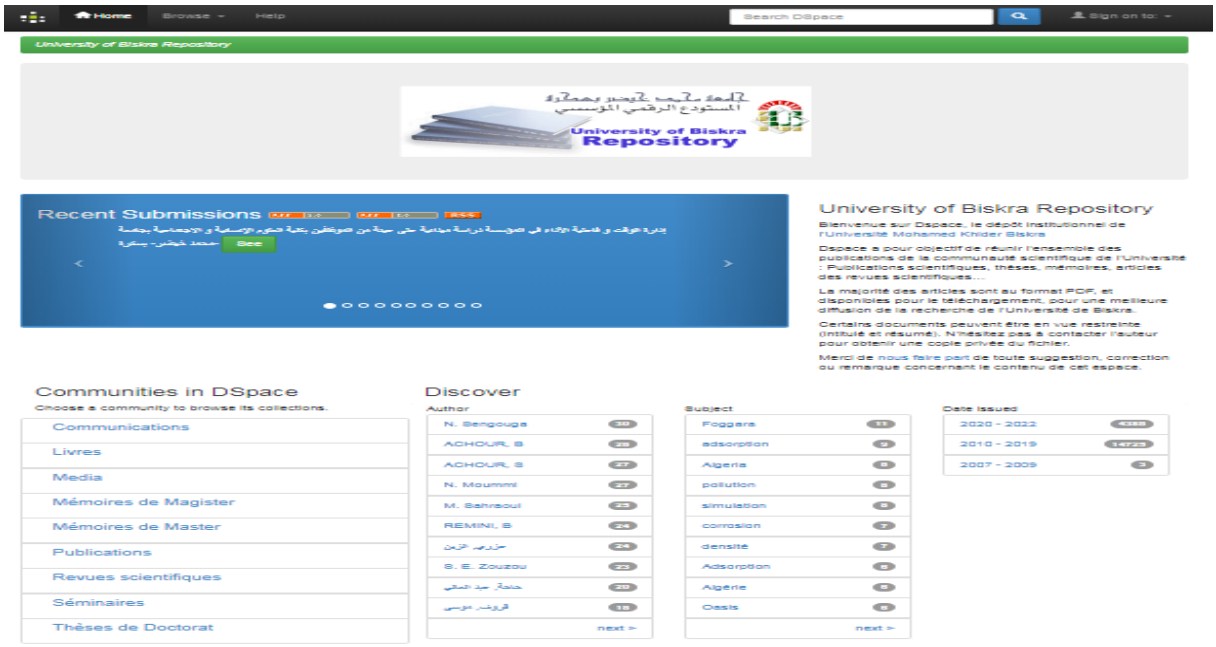
من خلال ما ذكر سابقا وجدنا أن كثرة التهديدات التي يمكن أن تواجه امن المعلومات والمحتوى الرقمي بالمستودعات الرقمية المؤسساتية واختلاف أنواعها تجبر أصحاب القرار بهذه المستودعات وخاصة أقسام تكنولوجيا المعلومات التابعة لها على وضع الاستراتيجية المناسبة لأمن المعلومات والتي تتكيف حسب طبيعة العمل بهذه المستودعات، في حدود إمكانياتها التنظيمية والميزانية المرصودة لهذه الحماية، وهذا ما سنراه في الجانب التطبيقي للدراسة، وذلك بالمقارنة بين ما يجب أن يكون، وما هو موجود بمستودع جامعة بسكرة.

ثالثا: الإطار الميداني للدراسة

3-1- التعريف بمكان الدراسة:

يعود تاريخ انشاء المستودع الرقمي لجامعة بسكرة (محمد خيضر) إلى سنة 2013، وقد تم بناؤه من قبل قسم الاعلام الآلي التابع لجامعة محمد خيضر بإشراف من إدارة الجامعة التي رأت بأنه من الواجب تبني مثل هذه المشاريع والاقتداء ببعض جامعات الوطن التي كانت سباقة في بناء وتصميم المستودعات الرقمية، ما جعلها توفر له كل الإمكانات اللازمة لضمان نجاحه، وقد تم استخدام برمجية Dspace في بنائه. يتم الولوج إليه من خلال الموقع الالكتروني للجامعة، أو الدخول مباشرة من خلال الرابط : http:dspase.univ-biskra.dz . حيث تظهر لنا واجهة المستودع على الشكل التالي:

الشكل 1: الصفحة الرئيسية لمستودع جامعة الحاج لخضر بسكرة



المصدر: الموقع الرسمي لمستودع جامعة محمد خيضر بسكرة

[1] برنامج نسبة الاقتباس في البحث العلمي. البوابة العلمية للبحوث والدراسات. متاح على الرابط: https:..www.sciegate.com.blog=برنامج-نسبة-الاقتباس-في-البحث-العلمي. تمت الزيارة يوم 25-01-2022.

3-2- تحليل أسئلة المقابلة:

الجدول 1: التوزيع النوعي والعددي للكيانات الرقمية المخزنة بمستودع جامعة محمد خيضر.

نـوع الكيان الرقمي	متوفر / غير متوفر	العدد	النسبة
كتب إلكترونيه	✓	**10**	**% 0.05**
أطروحات الدكتوراه	✓	**258**	**%1.34**
أطروحات الماجيستير	✓	**261**	**%1.4**
مذكرات الماستر	✓	**14664**	**%76.7**
مقالات الدوريات	✓	**3001**	**%15.7**
أعمال المؤتمرات	✓	**204**	**%1.06**
مقاطع فيديو تعليمية	X	/	/
صور رقمية	X	/	/
مقاطع صوتية	X	/	/
وحدات تعليمية	X	/	/
منشورات أخرى	✓	**722**	**%3.78**
المجموع الكلي		**19120**	**%100**

المصدر: من إعداد الباحث اعتمادا على بيانات مستودع جامعة محمد خيضر بسكرة

من خلال الجدول أعلاه يتبين أن الكيانات الرقمية لمستودع جامعة محمد خيضر تنحصر في 08 أنواع فقط متمثلة في الكتب الالكترونية، وأطروحات الدكتوراه، وأطروحات الماجيستير، ومذكرات الماستر، ومقالات الدوريات، وأعمال المؤتمرات، أما قسم منشورات أخرى فهو يضم المقالات التي تصدر عن مجلة العلوم الإنسانية والاجتماعية لجامعة محمد خيضر بسكرة، بالإضافة إلى المنشورات ذات الاتصال الدولي. وما نلاحظه أن هناك غياب تام لبعض أشكال الكيانات الرقمية مثل الوحدات الرقمية التعليمية، الوسائط السمعية البصرية كالصور الرقمية والفيديوهات، والمقاطع الصوتية، وقد يرجع ذلك لسياسة المستودع الذي يمنع إدراج مثل هذه الأنواع من الكيانات الرقمية كونها لا تخضع للتحكيم العلمي من وجهة نظرهم. وهذا ما يتناقض وأهداف بناء المستودعات الرقمية التي تهدف إلى إتاحة كل أنواع الكيانات، أما فيما يخص التوزيع العددي للكيانات الرقمية داخل المستودع فنلاحظ أن مذكرات الماستر هي من تعتلي سلم الترتيب بنسبة 76.7 %، هذا ما يفسره كثرة المقاعد البيداغوجية لطور الماستر بجامعة محمد خيضر وأعداد الطلبة المتخرجين في كل سنة دراسية. ثم تليها مقالات الدوريات بنسبة 15.7 %، وذلك لما تحتويه هذه المقالات من أهمية بالغة في دعم الأبحاث العلمية فالقائمون على المستودع يحرصون على جمع مختلف المقالات العلمية التي تدعم تخصصات الجامعة. بينما يوجد هناك انخفاض كبير في باقي أنواع الكيانات الرقمية.

3-2-1- المحور الأول: التأمين المادي للأجهزة والمكونات المادية:

الجدول 2: حماية مبنى النظام من المخاطر الطبيعية

نوع التأمين	نعم	لا
هل هناك نوافذ وفتوحات لتهوية غرف الخوادم؟	✓	
هل هناك أجهزة الإنذار ضد الحرائق داخل غرف الخوادم؟	✓	
هل هناك أجهزة الإطفاء اليدوية ضد الحريق؟	✓	
هل غرف الخوادم غير معرضة لمياه أمطار والفيضانات والتسربات؟		✓
هل تم عزل الأسطح ضد مياه الأمطار؟	✓	
هل تم مراعات درجات الرطوبة والحرارة داخل غرف الخوادم؟		✓

المصدر: من إعداد الباحث اعتمادا على الرد الذي وردنا من مدير المستودع.

يتبين من خلال الجدول أنه:

- تم وضع نظام تهوية ملائم لغرف الخوادم من قبل جامعة بسكرة لما لهذا البند من أهمية بالغة حفاظا على التجهيزات من ارتفاع درجات الحرارة التي قد تؤدي إلى تلف أجهزة النظام.
- تم تركيب نظام الإنذار ضد الحرائق في غرف الخوادم تحسبا لأي طارئ، مما جعل القائمين على المستودع يوفرون العدد الكافي من أجهزة الإطفاء اليدوية.
- غرف الخوادم لمستودع بسكرة بنيت دون مراعات شروط السلامة الخاصة بمياه الأمطار والفيضانات مما يجعلها عرضة للتسربات المائية مستقبلا، وقد تم الاكتفاء بعزل الأسطح فقط، وهذا يشكل خطرا على مكونات النظام.
- فيما يخص مراعات درجات الحرارة والرطوبة لا توجد هناك آلية محكمة لهذا الشرط، فقد تم الاعتماد على فتوحات ونوافذ التهوية فقط.

ويمكننا القول بأن مبنى النظام لمستودع جامعة بسكرة ليس مؤمنا بالشكل الكافي رغم توفر مختلف شروط الحماية فالتعرض لمياه الفيضانات وحده كفيل بتخريب مكونات النظام، لهذا وجب إعادة النظر في هذا الأمر وذلك من خلال حماية المبنى من تسريبات مياه الأمطار والفيضانات، أو تحويل مكونات النظام لمبنى آخر أكثر أمنا.

الجدول 3: أمن وحماية الأجهزة والمكونات المادية للنظام

نوع التأمين	نعم	لا
هل هناك غرف مغلقة لحفظ أجهزة الخوادم؟	✓	
هل هناك أنظمة حماية مثل كاميرات المراقبة وأجهزة الإنذار؟	✓	
هل هناك حراسة مستمرة لمبنى المستودع وسجلات التدوين الخاصة بتوقيت دخول وخروج العاملين؟	✓	
هل الكابلات المستعملة في الشبكة من النوع المناسب ومغلفة بشكل جيد؟	✓	
كابلات الشبكة موضوعة في أماكن آمنة ومحمية غير معرضة لوصول الأشخاص غير المختصين؟		✓
هل يتم صيانة الأجهزة بشكل دوري ومستمر لضمان استمرارية العمل؟	✓	
هل هناك مصدر طاقة كهربائية دائم؟		✓
هل هناك مصدر بديل لتوليد الطاقة الكهربائية؟		✓

المصدر: من إعداد الباحث اعتمادا على الرد الذي وردنا من مدير المستودع.

توضح بيانات الجدول أن:

- مستودع جامعة بسكرة يمتلك غرف مغلقة لحماية أجهزة الخوادم من الدخول غير المصرح، مع توفير كاميرات المراقبة، ووضع نظام حراسة دائم ومستمر عن طريق التناوب ما يجعل غرف الخوادم آمنة بنسبة كبيرة.
- تم اختيار النوع الجيد من كابلات الشبكة، لكنها لم توضع في أماكن آمنة ومحمية ما يجعلها عرضة للتلف جراء الأخطار الطبيعية والبشرية على حد سواء.
- هناك صيانة دورية ومستمرة لمكونات وأجهزة النظام بغرض استمرارية عمل المستودع، لكن الأمر الذي يعكس هذا الغرض هو انه لم يتم الأخذ بعين الاعتبار توفير مصادر الطاقة الدائمة والبديلة لمستودع جامعة بسكرة مع العلم بان هذا البند لا يمكن الاستغناء عنه في إنشاء مثل هذه المشاريع، فمصدر الطاقة البديل هو ما يساعد المستودع على العمل بصفة دائمة ومستمرة في حالة توقف المصدر الرئيسي.

ومن خلال هذه المعطيات نجد بأن مبدأ استمرارية العمل بمستودع جامعة بسكرة غير محقق رغم الحراسة المستمرة وتامين غرف الخوادم، والصيانة المستمرة لأجهزة النظام، فغياب مصادر الطاقة البديلة، وعرضة الكابلات للخطر جراء عدم وضعها في أماكن آمنة قد يؤدي لتوقف مختلف أو بعض الأجهزة عن العمل وبالتالي فشل النظام.

3-2-2- المحور الثاني: أمن الموارد البشرية:

الجدول 4: أمن الموارد البشرية العاملة بمستودع جامعة بسكرة

البند	نعم	لا
هل هناك تدريب للموظفين على كيفية استخدام النظام؟	✓	
هل يسمح النظام بفتح الحسابات للموظفين كل حسب رتبته الإدارية؟	✓	
هل يسمح النظام بتحديد صلاحيات كل موظف على حدى؟	✓	
هل يسمح النظام بتحديد كلمات المرور للموظفين كل حسب صلاحيته؟	✓	
هل كلمات المرور التي يعتمدها النظام تتسم بالقوة وعدم الاختراق؟	✓	
هل يتم تحيين كلمات المرور بشكل دوري (فترات زمنية محددة)؟	✓	
هل يوفر النظام تقنية التحكم في الوصول Access control؟	✓	
هل يوفر النظام تقنية التعرف على شخصيات الموظفين؟	✓	
هل يقوم النظام بحذف الموظفين المنتهية مدة صلاحياتهم؟	✓	

المصدر: من إعداد الباحث اعتمادا على الرد الذي وردنا من مدير المستودع.

يوضح الجدول أعلاه بأن تقنيات الحماية والأمن الخاصة بالموارد البشرية العاملة بمستودع بسكرة قد وضعت على أعلى المستويات لأنه لم يتم إهمال أي بند من بنود أمن الموارد البشرية، هذا الأمر الذي يثبت بأن نظام Dspace هو من الأنظمة الجيدة والمناسبة لبناء المستودعات الرقمية لأنه يوفر العديد من المزايا والتقنيات التي تمكن مستخدميه من وضع نظام حماية مناسب للأفراد باعتبار أن العنصر البشري يمثل أحد أكبر الأخطار المهددة لأمن المعلومات. وقد استغل مستودع جامعة بسكرة هذه الخصائص

والتقنيات للحد من هذا النوع من الأخطار، فهو لم يكتفي بتدريب الموظفين على الاستعمال الجيد والآمن للنظام فقط، وإنما تعدى ذلك إلى تحديد صلاحيات ومهام كل موظف وذلك بفتح الحسابات الخاصة بهم كل على حدا، مع ربط كل حساب بكلمات مرور خاصة تتسم بالقوة وعدم الاختراق، مع إمكانية تحيينها بشكل دوري وعلى فترات زمنية محددة لضمان عدم اختراقها، كما وفر النظام خاصية التعرف على الأفراد عن طريق تقنية التحكم في الوصول. ولضمان أمنية المعلومات أكثر يقوم نظام مستودع جامعة بسكرة بحذف حسابات الموظفين المنتهية مدة صلاحيتهم، سواء الذين أحيلوا للتقاعد أو الذين تم تحويلهم لمصالح أخرى.

الجدول 5: أمن وحماية المستودع من المستفيدين الخارجيين.

البند	نعم	لا
هل هناك نظم الإنذار المبكر عند دخول أشخاص غير مرخص لهم؟		✓
هل يستخدمون الأشخاص بطاقات الهوية العادية Identity Cards ؟		✓
هل يستخدمون الأشخاص البطاقات الذكية للتعريف Smart Cards ؟		✓
هل يوفر النظام وسائل التعريف البيولوجية Biological Identification؟		✓
هل يوفر النظام الأقفال الإلكترونية Electronic Locks لتأمين الدخول الى النظام والخروج منه؟		✓
بالنسبة للمستفيدين الخارجيين هل يقوم النظام بتحديد كلمات مرور خاصة بهم؟	✓	
هل يتم مراقبة المستفيدين عند استخدامهم للنظام؟	✓	
هل الرقابة بصفة دائمة أو بصفة دورية حسب فترات زمنية محددة؟	✓	
هل هناك لوائح إشارية ونصوص قانونية موجهة للمستفيدين حول حقوق الملكية الفكرية ؟	✓	

المصدر: من إعداد الباحث اعتمادا على الرد الذي وردنا من مدير المستودع.

نجد من خلال الجدول أعلاه بأن مستودع جامعة بسكرة لم يرتقي بعد لمستوى التحكم الجيد في الوصول من طرف الأشخاص الخارجيين، فهو لم يضع أي خطة أو استراتيجية للتوثق من شخصيات المستفيدين الخارجيين والمتمثلة في الأجهزة القارئة لوسائل التعرف على الأشخاص كبطاقات الهوية العادية Identity Cards، والبطاقات الذكية المستخدمة للتعريف Smart Cards، ووسائل التعريف البيولوجية Biological Identification. كما أنه لا يتوفر على نظم الإنذار المبكر عند دخول أشخاص غير مرخص لهم، وإنما اكتفى النظام فقط بتوفير كلمات مرور خاصة بالمستخدمين الخارجيين ومراقبتهم عند استعمال النظام، ووضع لوائح إشارية ونصوص قانونية على واجهة النظام خاصة بحقوق الملكية الفكرية على أمل أن تحول هذه اللوائح دون انتهاك حقوق التأليف والنشر.

ومن هنا يمكن القول بأن كلمات المرور بالنسبة للمستفيدين الخارجيين، والاكتفاء بالوازع القانوني هو شرط غير كافي لحماية محتوى المستودع من مختلف الانتهاكات، فكما ذكر سابقا فإن العنصر البشري هو من أكبر المخاطر المهددة لأمن المعلومات، لهذا وجب التعامل معه بصرامة وجدية فائقة، ذلك باللجوء لمختلف التقنيات التي تمنعه من تشكيل التهديد.

3-2-3- المحور الثالث: تأمين النظام والتطبيقات.

الجدول 6: أمن وحماية أنظمة التشغيل والتطبيقات

نوع التأمين	نعم	لا
هل هناك أنظمة تشغيل قوية لا تتأثر بالفيروسات؟		✓
هل يحتوي النظام على برامج الحماية ضد الفيروسات؟	✓	
هل يوفر النظام تقنية النسخ الاحتياطي؟	✓	
هل يتوفر النظام على برامج الجدران النارية **fire wall** ؟	✓	
هل هناك برامج حماية متتبعة للاختراق والتسلل؟		✓

المصدر: من إعداد الباحث اعتمادا على الرد الذي وردنا من مدير المستودع.

يتضح من خلال الجدول أعلاه بأن نظام التشغيل بمستودع جامعة محمد خيضر بسكرة لا يتسم بالقوة التي تجعله مقاوما لمختلف أنواع وأشكال الفيروسات، الأمر الذي جعل القائمين على المستودع يستنجدون ببرامج الحماية ضد الفيروسات للحد من الأخطار الناجمة عنها، كما تم الاعتماد أيضا على تقنية الجدران النارية التي تعد من أبرز الطرق لحماية الشبكة من أي ضرر خارجي وتقليص التدمير الذي يحصل على الشبكة من خلال تقليص حقوق الوصول للأشخاص الخارجيين، كما تم التحسب لمختلف الأخطار التي يمكن أن تتسبب في فقدان البيانات لذلك اعتمد القائمون على المستودع تقنية النسخ الاحتياطي، التي تضمن عدم ضياع المحتوى الرقمي للمستودع عن طريق حفظه في وسائط أخرى.

أما برامج الحماية المتتبعة للاختراق فهي غير متوفرة بمستودع جامعة بسكرة رغم خصائصها المتميزة والتي تعتبر من أساليب الدفاع المهمة للنظم الآلية حيث توفر نظام تتبع دوري ومستمر لخطر الاختراق والتسلل والحد منه.

3-2-4- المحور الرابع: أمن وحماية المحتوى الرقمي

الجدول 7: أمن وحماية محتوى الكيانات الرقمية بمستودع جامعة بسكرة.

نوع التأمين	نعم	لا
هل يتوفر النظام على تقنية تشفير البيانات؟	✓	
هل يستخدمون تقنية البقع المائية؟		✓
هل يستخدمون تقنية التوقيع الالكتروني لحماية مضمون الكيان الرقمي؟		✓
هل يتم تأمين وسائل الاتصال لنقل وتبادل البيانات؟	✓	
هل تعتمدون على تقنية الإزاحة (خوارزمية الإزاحة **Transportation**)؟	✓	
هل يسمح النظام بالنسخ الكامل للنصوص؟	✓	
هل يتم وضع معرفات للكيانات الرقمية من أجل ضمان استمراريتها والوصول إليها؟	✓	

المصدر: من إعداد الباحث اعتمادا إجابة المبحوث.

يتضح من خلال بيانات الجدول أن نظام إدارة المحتوى للمستودع الرقمي لجامعة بسكرة يعتمد على تقنية تشفير البيانات ومنع التنصت على كابلات الشبكة لتفادي الوصول للمحتوى الرقمي، ما يجعل محتوى الكيانات الرقمية باعتبارها "بيانات" آمنة ومحمية، كما تم تأمين وسائل الاتصال لنقل وتبادل هذه البيانات كالبريد الالكتروني وغيره من وسائل الاتصال، واعتماد تقنية الازاحة من خلال الخوارزميات، أما باقي التقنيات كتقنية البقع المائية الرقمية، والتوقيع الإلكتروني فهي غير معتمدة بالمستودع بالرغم من انها تعد من أهم تقنيات أمن المعلومات لأنها الوسيلة الوحيدة لحماية التكاملية وسلامة المحتوى من التعديل والتحريف فهي الإثبات الشرعي لملكية صاحب المحتوى، و فيما يخص استمرارية الكيانات الرقمية وديمومة الوصول إليها فالقائمون على المستودع يقومون بالنسخ الكامل للنصوص لتعويضها في حالة الضياع، ووضع المعرفات المعيارية الدولية للكيانات الرقمية من أجل استمراريتها ودوام الوصول إليها على المدى الطويل.

3-3- نتائج الدراسة:

توصلت الدراسة إلى جملة من النتائج التي لها علاقة بأمن المعلومات والكيانات الرقمية بمستودع جامعة محمد خيضر بسكرة والتي يمكن حصرها فيما يلي:

- أنواع الكيانات الرقمية لمستودع جامعة بسكرة تتنافى وأهداف المستودعات الرقمية التي تهدف إلى إتاحة كل أنواع الكيانات، فالمحتوى الرقمي لجامعة بسكرة مقسم إلى 08 فئات فقط كما هي موضحة سابقا، مع غياب تام لمختلف أنواع الأعمال البحثية ما قبل النشر وما بعده، ومختلف الوسائط الرقمية، ما يوضح أنه هناك غياب للوعي بأهمية هذه المنشورات من طرف المجتمع الأكاديمي لجامعة بسكرة.
- الاستراتيجية القوية لأمن المعلومات تساهم في حماية المستودع وما يتضمنه من كيانات رقمية، كونها تحقق مبدأ السلامة، والتكاملية، والاستمرارية.
- تم تأمين مبنى مستودع جامعة بسكرة ضد الأخطار الطبيعية بشكل جيد لولا إهمال شرط الحماية من مياه الأمطار والفيضانات، الامر الذي يستوجب إعادة النظر في هذا الشرط من جديد.
- تم تامين المكونات المادية للنظام بمستودع جامعة بسكرة باتباع إجراءات عديدة خاصة بغرف الخوادم واختيار النوع المناسب من كابلات الشبكة. إلا أنها غير محمية ما يجعلها عرضة للوصول غير الآمن من طرف الأشخاص غير المختصين.
- لم يتم تزويد النظام بمصادر الطاقة الدائمة والبديلة، ما يجعل استمرارية العمل غير محققة، ففي أي لحظة يمكن أن يتوقف المستودع عن العمل بسبب انقطاع التيار الكهربائي.
- مستودع جامعة بسكرة يحدد مسؤوليات الموظفين وصلاحياتهم، كإجراء أمني لسلامة النظام والمحتوى الرقمي.
- هناك بعض البنود التي تم إهمالها فيما يخص إجراءات الامن وتحديد صلاحيات المستفيدين الخارجيين من مستودع جامعة بسكرة، ما يهدد سلامة المحتوى الرقمي.
- يتم استخدام برامج الحماية ضد الفيروسات لتامين أنظمة التشغيل بمستودع جامعة بسكرة. باعتبارها أنظمة غير قوية تتأثر بالفيروسات.
- يتم استخدام برامج الجدران النارية لحماية الشبكة من أي ضرر خارجي وتقليص التدمير الذي يحصل على الشبكة من خلال تقليص حقوق الوصول للأشخاص الخارجيين.

- يستخدم مستودع جامعة بسكرة تقنية تشفير البيانات لوعي القائمين عليه بأمية هذه التقنية وما توفره من إيجابيات.
- لم يرتقي مستودع جامعة بسكرة بعد لمستوى وضع العلامات المائية الرقمية والتوقيع الالكتروني على صفحات المحتوى الرقمي، ما يجعل هذا المحتوى عرضة للتلاعب والتحريف
- يتم استخدام تقنية النسخ الاحتياطي لكافة العمليات التي تطرأ على نظام المستودع، ومختلف النصوص والكيانات الرقمية المودعة به.
- يتم وضع معرفات معيارية دولية للكيانات الرقمية المخزنة بمستودع جامعة بسكرة، بهدف استمرارية هذه الكيانات ودوام الوصول إليها.

خاتمة:

يرى الكثيرون أن إجراءات الأمن والوقاية قد تسبب عوائق كثيرة للمنظمة، وتمنعها من تحقيق أهدافها في بعض الأحيان، وذلك بسبب ما تفرضه من إجراءات وقواعد مزعجة للمدراء والموظفين، ويتناسوا أن هذه الإجراءات والقواعد ليست مقصودة لذاتها، وإنما هي موضوعة لحماية أصول المنظمة ومواردها والمحافظة عليها بحيث تكون قادرة على المواصلة وتنفيذ رسالتها. فالغنيمة التي يسعى لها المهاجمون ليست هي النظم بحد ذاتها، ولكنها هي المعلومات التي يتم معاجلتها داخل هذه النظم. والمستودعات الرقمية المؤسساتية على غرار مستودع جامعة بسكرة باعتبارها إحدى نظم المعلومات وجب عليها مراعات ذلك. وبعد ما توصلت إليه دراستنا هذه من نتائج وجب علينا نحن كباحثون وضع بعض المقترحات والتوصيات التي يمكن على أمل منا ان تساعد في حل بعض المشكلات الخاصة بأمن المعلومات بالمستودعات الرقمية للجامعات الجزائرية والنهوض بهذا القطاع لأعلى المستويات. ويمكن حصر هذه المقترحات في النقاط التالية:

- إعادة النظر في بعض شروط الحماية المتعلقة بمبنى المستودع ومحتواه من طرف المسؤولين عن مستودع جامعة بسكرة.
- ضرورة التعاون والتنسيق بين المسؤولين في الجامعات والموظفين القائمين على أمن المعلومات بالمستودعات الرقمية.
- إعداد سياسات واستراتيجيات واضحة ومكتوبة لإجراءات الأمن والحماية للمستودعات الرقمية الجامعية، وفرض أقصى العقوبات للمخالفين لهذه السياسات.
- أن تكون هناك مراجعة دائمة وبصفة دورية لهذه السياسات من أجل كشف مختلف الثغرات ونقاط الضعف ومحاولة تجاوزها.
- برمجة الدورات التدريبية للموظفين وتوعيتهم بأهمية وأهداف أمن المعلومات بالمستودعات الرقمية الاكاديمية.

قائمة المراجع:

المؤلفات:

1. إبراهيم، السعيد مبروك. الإدارة الاستراتيجية للمكتبات ومرافق المعلومات. – الإسكندرية: دار الوفاء لدنيا الطباعة والنشر، 2014.

2. أبو هبة، نجوى. التوقيع الالكتروني: تعريفه مدى حجيته في الاثبات. – القاهرة: دار النهضة العربية، 2002.

3. أحمد، أشرف السعيد. استراتيجية أمن المعلومات. – القاهرة: مطابع الشرطة، 2014.

4. البياتي، نادية ياس. التوقيع الالكتروني عبر الانترنت ومدى حجيته في الإثبات: دراسة مقارنة بالفقه الإسلامي. – عمان: دار البداية ناشرون وموزعون،2013.

5. الحمامي، علاء حسين؛ العاني سعد عبد العزيز. تكنولوجيا أمنية المعلومات وأنظمة الحماية. – عمان: دار وائل للنشر والتوزيع، 2007.

6. خميس، أسامة محمد عطية. الكيانات الرقمية (المحتوى الرقمي) في المستودعات الرقمية على شبة الأنترنت: المفهوم. البرمجيات. البناء. الإيداع الرقمي. ج1. – القاهرة: الشركة العربية المتحدة للتسويق والتوريدات، 2013.

7. الدعيلج، إبراهيم بن عبد العزيز. مناهج وطرق البحث العلمي. – عمان: دار الصفاء، 2010.

8. رحمه، علي محمد دهب. التشفير وأمن المعلومات. –كردفان: جامعة كردفان، 2013.

9. سعيدي، سليمة. أمن المعلومات وأنظمتها في العصر الرقمي. – الإسكندرية: دار الفكر الجامعي، 2017.

10. صادق، دلال؛ الفتال، حميد ناصر. أمن المعلومات. – عمان: دار اليازوري العلمية للنشر والتوزيع، 2008.

11. الطيطي، خضر مصباح إسماعيل. أساسيات أمن المعلومات والحاسوب. – عمان: دار الحامد، 2009.

12. عبد الجواد، سامح زينهم. المستودعات الرقمية: استراتيجيات البناء والإدارة والتسويق والحفظ. – بنها: جامعة بنها، 2014.

13. عبد الله، عبد الكريم فراس؛ حسان عباس، رشا. التشفير وسيلة للحصول على أمن البيانات. – بغداد: كلية تكنولوجيا هندسة الحاسوب، 2019.

14. العريشي، جبريل بن حسن؛ الشلهوب، محمد حسن. أمن المعلومات. – عمان: الدار المنهجية، 2015.

15. عطيات، عبد الرحمان شعبان. أمن الوثائق والمعلومات. – عمان: دار الحامد للنشر والتوزيع، 2014.

16. عليان، ربح مصطفى. أساليب البحث العلم وتطبيقاته في التخطيط والإدارة. – عمان: دار الصفاء، 2008.

17. محمد عبده، أشرف. أمن وحماية الوثائق الإلكترونية: المخاطر والحلول. – القاهرة: دار الجوهرة للنشر والتوزيع، 2015.

الأطروحات

18. طرشي، حياة. وصف المحتوى الرقمي ودوره في تفعيل البحث الموضوعي من خلال الفهارس الآلية للمكتبات الجامعية: دراسة وصفية تحليلية بمكتبات جامعات الشرق الجزائري. دكتوراه في علم المكتبات والتوثيق. – قسنطينة: جامعة عبد الحميد مهري، 2020.

المقالات:

19. الصميدعي، عامر تحسين سهيل. تطبيق تقنة حساسة لإخفاء العلامات المائية الرقمية في الصور الرقمية الثابتة. المجلة العراقية للعلوم الإحصائية، ع10. 2006. ص 107-120. متاح على الرابط:
https:..stats.mosuljournals.com.article_32585_63c1876bb604c8ab406f06738bf1c2fd.pdf

20. عبد القادر، فردوس عدنان؛ خليل، شهباء إبراهيم؛ سليم، ندى نعمت. نظام العلامة المائية المهجن ذكائيا. مجلة الرافدين لعلوم الحاسبات والرياضيات، مج 7. ع 2. 2010.. متاح على الرابط: https:..www.iasj.net.iasj.download.423fccd9c52a04c9

21. علي، عادل نبيل شحات. تقنيات أمن وحماية المحتوى الرقمي للمستودع الرقمي للرسائل الجامعية المصرية، بنها: جامعة بنها، مجلة كلية الآداب مج1، ع1. 2017 متوفر على الرابط:
https:..journals.ekb.eg.article_104577_7fcabd3f4ee8a3128e3194f2236c7d77.pdf.

22. غبيق، صلاح الهادي. التشفير وفك التشفير. مجلة العلوم الاقتصادية والسياسية لجامعة المرقب ليبيا. ع 02. 2013. متاح على الرابط:
https://journals.asmarya.edu.ly

23. نورس، احمد. متطلبات بناء مستودع رقمي في جامعة البعث، مجلة جامعة البعث مج. 83. ع 34 سنة 2016.

24. Julie Allinson and Mahendra Mahey. Workshop on innovation in scholary communication, avalable from: www.ukoln.ac.uk

25. Penfield, Stephen. A mandate to self-archive: the role of open access in institutional repositories retrieved from: http:..eprint.nottingham.ac.uk.archive.00000152.01

المداخلات:

26. العربي، أحمد عبادة. المستودعات الرقمية للمؤسسات الأكاديمية ودورها في العملية التعليمية والبحثية وإعداد آلية لإنشاء مستودع رقمي عربي. ورقة عمل، ندوة التعليم الجامعي في عصر المعلوماتية "التحديات والتطلعات. – طنطا 2011. متوفر على الرابط: http://repository.taibahu.edu.sa/handle/123456789484

مواقع الأنترنت:

27. برنامج نسبة الاقتباس في البحث العلمي. البوابة العلمية للبحوث والدراسات. متاح على الرابط: https:..www.sciegate.com.blog=برنامج-نسبة-الاقتباس-في-البحث-العلمي.

28. سياسة النسخ الاحتياطي – الهيئة الوطنية لأمن وسلامة المعلومات. متوفر على الرابط التالي: https:..nissa.gov.ly.main-services.data-backup-policy.

29. موقع جامعة بسكرة. متاح على الرابط: https://univ-biskra.dz/index.php/fr/34-universite/articles9/186-presentation-de-lumkb