مجلة كلية الآداب

مجلة دورية علمية محكمة

نصف ســنوية

العدد الثامن والأربعون
أكتوبر ٢٠١٧

مجلة كلية الآداب.. مج ١، ع ١ (أكتوبر ١٩٩١م) .
بنها : كلية الآداب . جامعة بنها، ١٩٩١م
مج؛ ٢٤ سم.
مرتان سنويا (١٩٩١) وأربعة مرات سنويا (أكتوبر ٢٠١١) ومرتان سنويا (٢٠١٧)

١ . العلوم الاجتماعية . دوريات . ٢. العلوم الإنسانية . دوريات.

مجلة كلية الآداب جامعة بنها

مجلة دورية محكمة

العدد الثامن والأربعون

الشهر : أكتوبر ٢٠١٧

رقم الإيداع ٦٣٦١ : ٦٣٦٣ لسنة ١٩٩١

ISSN: 1687-2525

المجلة مكشفة من خلال اتحاد المكتبات الجامعية المصرية

ومكشفة ومتاحة على قواعد بيانات دار المنظومة على الرابط:

http://www.mandumah.com

ومكشفة ومتاحة على بنك المعرفة على الرابط:

http://jfab.journals.ekb.eg

هيئة تحرير المجلة

تقنيات أمن وحماية المحتوى الرقمي للمستودع الرقمي للرسائل الجامعية المصرية

إعـــداد

عادل نبيل شحات علي

مدرس المكتبات والمعلومات

كلية الآداب ـ جامعة بنها

e-mail
adelaly911@yahoo.com

مستخلص

يهدف المستودع الرقمي للرسائل الجامعية المصرية إلي إتاحة ونشر المحتوى العلمي للإنتاج الفكري الصادر عن الجامعات المصرية، المتمثل في الرسائل العلمية إلكترونيا من خلال رقمنة الرسائل العلمية التي أجازتها الجامعات المصرية، وتتطلب ذلك توفير بنية تحتية تشمل المكونات البرمجية والمادية اللازمة لتحقيق هذا الهدف، بالاضافة إلي نظام لإدارة المحتوى الرقمي لإدارتها ونشرها الكترونيا علي الشبكة العنكوتية؛ من أجل توسيع الاستفادة من الرسائل الجامعية ورفع قيمتها العلمية التى كانت حبيسه الأرفف والمكتبات.

وتبرز أهمية أمن المحتوى الرقمي للمستودع في ظل تزايد التهديدات واختراق المواقع والشبكات من قبل قراصنة الانترنت، علي الرغم من جميع الجهود التي تبذلها شركات تقنية المعلومات، إلا أن الهاجس الأمني في ظل البيئة الإلكترونية يعد من أولي اهتمامات مؤسسات المعلومات للحفاظ علي المحتوى الرقمي المنشور، ويعد أمن الوثائق والمحتوى الرقمي شريان حيوي خصوصا علي نطاق الاقتصاد الوطني، وسعت وحدة المكتبة الرقمية بالمجلس الاعلي للجامعات الحفاظ علي أمن المحتوى الرقمي للمستودع من خلال وضع تجهيزات مادية وبرمجية للحفاظ علي المحتوى الرقمي للرسائل الجامعية المصرية، وتحاول الدراسة التعرف علي السياسات الأمنية سواء كانت سياسات خاصة بالتجهيزات المادية، أو بالتجهيزات البرمجية، والتي تحدد الحماية الأمنية للمستودع الرقمي، وتحليل المخاطر التي قد تنجم من جراء عدم الاهتمام بموضوع أمن وحماية المحتوى الرقمي للرسائل الجامعية المصرية ،واعتماد إجراءات الوقاية والدفاع الإلكتروني، وذلك للخروج بنتائج يمكن أن توضح معالم أمن وحماية المستودع الرقمي للرسائل الجامعية المصرية الذي يعد قناة الكترونية للتعريف بالرسائل المصرية علي المستوى الوطني والدولي بالإضافة إلي توسيع نطاق الإفادة من محتوى تلك المصادر الحيوية وإتاحتها عالميا مما يساعد علي رفع القيمة التنافسية للجامعات المصرية.

القسم الأول : المقدمة المنهجية

١/٠ تمهيد

يشير (سالم،٢٠٠٩) إلى أن " الرسائل الجامعية من الوثائق الأساسية التي يتكون منها الرصيد الوثائقي للمكتبات الجامعية، وهي تحتل مكانة بارزة لكونها تنفرد بمحتوياتها الفكرية التي تسودها عادة الأصالة والابتكار، وهما شرطان أساسيان للإبداع الفكري، وإنتاج البحوث العلمية. لذلك فهي تتطلب اهتمام خاص من قبل المكتبيين المتخصصين وإعطائها القدر الكافي من العناية بالتركيز على استخدام أحدث التقنيات في معالجتها، وتخزينها، وتقديمها للدارسين، والباحثين بسرعة ويسر، وبما أن المعلومة الورقية تقف أمامها عدة حواجز منها التطورات المتعددة التي صاحبت تطور المجتمع في مختلف الأصعدة، فقد بات لزاما التفكير في طرق أخرى، تعيد لهذه المعلومات قيمتها الحقيقية، خاصة في ظل تطور طبيعة وشخصية الباحث المعاصر التي أخذت عنصري السرعة والدقة في أولى أولويات بحثه وحتى في شخصيته.

ولذا يؤكد (معمر، ٢٠١٠) على أن ظاهرة الرقمنة أحدث وأنسب وسيلة ينبغي الاعتماد عليها للسيطرة والتحكم الجيد في تسيير وتنظيم وتوزيع الرسائل والمذكرات الجامعية، وهذا ما جعل العديد من مؤسسات التعليم العالى سواء بشكل منفرد أو عبر تجمعات وطنية أو إقليمية ترقمن رسائلها وتنشرها إلكترونيا عبر الإنترنت.

ولم تكن مصر بمعزل عن هذه التجارب التى اتخذت فى بعض أوقاتها الاتجاه الفردى لمؤسسات التعليم العالى، بقيام بعض الجامعات المصرية بمجهودات فردية فى هذا الاتجاه، لكن جهودها اقتصرت على عمليات رقمنة محدودة القيمة مع حدود إتاحة لا تتجاوز نطاق الجامعة .

ولقد لعبت الثورة التكنولوجية التي عرفها العالم في النصف الثاني من القرن العشرين، دورا كبيرا في تغيير العديد من المفاهيم التي كانت بمثابة مسلمات، وتم تعويضها بمفاهيم جديدة، ساهمت في تحليل ودراسة وحدات المجتمع الدولي، و حلٌ

الكثير من مشاكله. فدخل العالم مرحلة متقدمة ضمن آفاق عصر المعلومات، بهدف الإستفادة من التقنيات المتوفرة في مجال المعلومات، والتي أصبحت معيارا يقاس به تقدُم المجتمعات وتطورها. إن العالم اليوم أصبح كقرية صغيرة، أوجبت تجاوز البعد الزماني والمكاني. فقامت الدول بتطوير الآليات التقنية والوسائل لمتابعة تنفيذ تلك السياسات وتحقيق أعلى كفاءة ممكنة وتهيئة المناخ لملائمة التطورات العالمية المتجددة.

وبما أن المعلومات هى ركيزة من ركائز الأمن القومى التى يجب حمايتها كما هو الحال فى المعلومات العسكرية والأمنية والمعلومات هي ذاكرة الأمة التي تحفظ لها حضارتها وثقافتها لذا يجب أن تتخذ كل الأساليب والطرق لحمايتها من السرقة والتخريب، وخصوصا في ظل الثورة التكنولوجية الحديثة وسعى معظم الدول التحول إلي مجتمع المعلومات والتسارع في إنشاء قواعد البيانات القومية المتاحة علي الانترنت في ظل الاعتماد الكبير للقطاعات التجارية والمالية والمصرفية والعلمية والخدمية والاجتماعية على أدوات وتقنيات المعلومات والاتصالات يعتبر أمن المعلومات من المواضيع الأساسية الساخنة والمتجددة في عالم تقنيات المعلومات والاتصالات، ومع التطورات التي نشهدها حاليًا في العالم نجد أن معظم الدول العربية الآن ترفع شعار التحول إلى مجتمع المعلومات وتشييد بنية معلوماتية قومية شاملة على كل المستويات.

والمشروع الأكثر تأثيرا هو المشروع الذى تم طرحه من خلال وحدة المكتبة الرقمية التابعة لمشروع ICTP بالمجلس الأعلى للجامعات، إذ يسعى إلي رقمنه الرسائل الجامعية التي أجازتها الجامعات المصرية من خلال التعاون بين وحدة المكتبة الرقمية التابعة لمشروعICTP بالمجلس الأعلى للجامعات، والجامعات المصرية ممثلة فى كل الجامعات الحكومية المصرية وبتمويل من مشروع ICTP حيث سعى المشروع إلى إنشاء النواة الأساسية للمستودع الرقمى للرسائل الجامعية

المصرية والدوريات وأعمال المؤتمرات، بالإضافة إلي تجهيز البنية التحتية المادية والبرمجية اللازمة لإعداد وإتاحة الرسائل الجامعية والدوريات وأعمال المؤتمرات المصرية في صورة إلكترونية.

وبالتالي ظهرت تحديات أمن المعلومات فى مجتمع يمتلك بنية معلوماتية واسعة يجعله يواجه تهديدات فى أمن المعلومات، تتسم بالشمول والاتساع حيث تتعاظم مخاطر أمن المعلومات ترقى إلى مستوى تهديد الأمن القومى ككل، فيجب أن تكون هناك وسائل لمواجهتها تحت مظله منظومة أمن قومي خاصة أن إدارة المعلومات داخل البنية القومية أمر يتطلب فهم ورؤية جديدة لأساليب وأدوات ومناهج وإدارة تداول المعلومات

١/١ أهمية الدراسة :

يشير (قاسم،٢٠٠٣؛ ص١٢٣) على ضرورة توخى الحيطة والحذر وبذل أقصى ما يمكن من جهد فى التخطيط لبرامج الرسائل الجامعية الالكترونية، لأن تكلفة أى جهد يبذل فى التخطيط لا تساوى شيئا بالمقارنة بتكلفة المخاطرة غير المحسوبة فى هذا المجال. فالتراث الفكرى أمانة والرسائل الجامعية من أغنى ودائع الأمانة، بينما يشير (عبد الحفيظ، ٢٠٠٧؛ ص١٣٣) إلى "انتهاء معظم دول العالم المتقدم من مرحلة التنظير منذ ما يقرب من عشرين عاماً تقريبا، أما الآن فهى تسعى نحو رقمنه جميع مقتنياتها من الرسائل الجامعية وإتاحتها على شكل وثائق مطبوعة PDF على شبكة المعلومات الدولية الإنترنت".

وهذا يجعل الحيطة والحذر فى رقمنه الرسائل أساسا مهما، لكن ذلك لا يمنع بأى شكل المضى قدما فى تخطيط برامج التحويل الرقمى للرسائل الجامعية حفظا رقميا ورقمنة على السواء.

وإذا كانت الرسائل الجامعية تمثل أحد الأشكال الهامة من مصادر المعلومات

بالمكتبات الجامعية فإنها تمتاز بتوافر عناصر مهمة للبحث العلمى الأصيل، وذلك بما تتسم به من تميز وإبداع وأمانة علمية والتزام بمناهج البحث العلمى والإشراف والمناقشة والتقييم والحداثة والموضوعية، كما أنها تمثل نتاج فكرى ومؤشر أصيل محكم يُستدل به على مدى تقدم الدول وتطورها على المستوى العالمى.

ولأن الرسائل الجامعية هى فى الغالب حبيسة محل إيداعها فى الجامعة سواء كانت المكتبات المركزية أو أى من الوحدات الأخرى الخاصة بذلك، وبالتالى فالحصول عليها والإفادة منها غير متاحة لجميع الأفراد مثل بقية المصادر المعلوماتية الأخرى، وبما يجعلها قيمة معلوماتية واقتصادية يمكن أن تشكل موردا لأى جامعة إذا تم تسويقها بطريقة علمية بالإضافة إلى تأثيرها الإيجابى بما يحد من عملية التكرار للبحث العلمى، ولكن ذلك قد يكون له جوانب سلبية تتصل بالتعدى على حقوق الملكية المادية والفكرية.

ومع تبنى وحدة المكتبة الرقمية بالمجلس الأعلى للجامعات مشروع إنشاء المستودع الرقمى للرسائل الجامعية المصرية بما يضمن حصر وضبط وتحويل الرسائل الجامعية المصرية إلى الشكل الرقمى، وهو ما يضمنه مشروع المستودع الرقمى للرسائل الجامعية الذى انطلق عام (٢٠٠٨) لرقمنة الرسائل المطبوعة ، بعد الانتهاء من عمليات الحفظ الرقمى للرسائل التى تم إيداعها فى شكل رقمى خلال المرحلة الأولى من المشروع ، والتى امتدت خلال الفترة من (٢٠٠٩/٢٠١٠) وتأتى المرحلة الثانية لرقمنة الرسائل المتاحة فى شكل مطبوع فى الفترة من (٢٠١٠/٢٠١١) ليتم استكمال عمليات الرقمنة خلال عام (٢٠١١/٢٠١٢) فى المرحلة الثالثة، وبعد انتهاء المرحلة الثالثة قامت كل جامعة بالاشراف والانتهاء من تكشيف وتحميل الرسائل العلمية علي نظام ادارة المحتوى للمستودع الرقمي.

ما سبق يؤكد على أهمية الدراسة التى تتناول كيفية تأمين وحماية المحتوى الرقمي

لمستودع الرسائل الجامعية المصرية من أعمال التخريب والسرقة سواء من خارج المؤسسة أو من داخلها، كما أنها تحاول أن تضع أمام المهتمين ومتخذى القرار بمشروع المستودع الرقمى للرسائل بالجامعات المصرية جميع الوسائل والطرق التى يمكن من خلالها التعرف على واقع أمن وحماية التجهيزات المادية والبرامجية للمحتوى الرقمى للرسائل الجامعية المصرية بشقيها من مختلف الجوانب، وذلك للتغلب على ما يمكن أن يواجه المشروع من مشكلات وعوائق إذ أن أمن المعلومات أحد أكبر التحديات التي تواجهها شبكة الانترنت من كثرة التهديدات وجرائم المعلومات عليها.

٢/١ مشكلة الدراسة:

لقد بُذلت كثيرا من الجهود المصرية فيما يتعلق بعملية حصر وحفظ ورقمنة الرسائل الجامعية المصرية من أجل إتاحتها فى شكل رقمى، لكن معظم هذه الجهود لم تخرج بما هو مرجو منها بما يعطى الانطباع بأن معظم هذه الجهود كانت تفتقد إلى الخطة الواعية والاستراتيجية الواضحة والإرادة الحقيقية، فمعظم الجامعات العربية لم تستقر بعد على نظام يتم بمقتضاه تيسير سبل الحصول على الرسائل خارج الجامعات التى أجازتها فلا زالت نزعة التملك هى المسيطرة على معظم الجامعات والقائمين على مكتباتها.

ولكن عمليات التحويل الرقمى تلك ليست عمليات بسيطة بل هى عمليات تتداخل فيها مقومات كثيرة وعناصر ومختلفة تتمثل فى الإطار التنظيمى والإداري والتمويل ومشكلاته، والقوى البشرية اللازمة لإنجاز ذلك، كما أن التحويل الرقمى يعتمد بالأساس على مقومات مادية وتقنية غاية فى التعقيد بالإضافة إلى التحديات القانونية المترتبة على عمليات التحويل، وخاصة فيما يتعلق بحقوق الملكية المادية والفكرية للباحثين وللجامعات، وقد زادت المشكلة حدة مع تزايد حركة البحث العلمى فى الجامعات المصرية وتزايد أعداد الرسائل الجامعية.

ونظرا لارتفاع معدل المواقع المتخصصة في سرقة البيانات وظهور قراصنة الانترنت بالاضافة إلي أنه لا يوجد أمن مطلق في ظل تطبيقات الويب والفضاء الخارجي ونجاح وصلابة الأمن المعلوماتي للمؤسسات أحد أهم مقاييس نجاح هذه المؤسسات.

فمن أهم مبادئ أمن المستودع الرقمي للرسائل الجامعية المصرية هو حماية المحتوى الرقمي للمستودع من أعمال التخريب، والسرقة خصوصا في ظل التهديدات واختراق المواقع من قبل قراصنة الانترنت، وعلي الرغم من جميع الجهود التي تبذلها شركات تقنية المعلومات، إلا أن الهاجس الأمني في ظل البيئة الإلكترونية يعد من أولي اهتمامات هذه الشركات، وتحاول هذه الدراسة بالخروج بمؤشرات لمسئولي المستودع الرقمي للرسائل الجامعية المصرية لتحديد المتطلبات اللازمة لضمان أمن وحماية المحتوى الرقمي للمستودع، ووضع السياسات الأمنية التي تحدد الحماية وتحليل المخاطر بالإضافة إلى معرفة وسائل الهجوم الإلكتروني وكيفية تجنبها والحفاظ علي أمن المعلومات بإعتماد إجراءات الوقاية والدفاع الإلكتروني.

٣/١ أهداف الدراسة

تستهدف الدراسة تسليط الضوء على تقنيات أمن وحماية المحتوى الرقمى للرسائل بمشروع المستودع الرقمى للرسائل الجامعية المصرية ، ومدى كفاءة أنظمة الحماية المادية والبرامجية للمحتوى الرقمي للمستودع ، وبشكل أكثر تفصيلا يمكن رصد مجموعة من الأهداف التى تعمل الدراسة على تحقيقها وهى :

١- التعرف علي مشروع المستودع الرقمي للرسائل الجامعية المصرية .

٢- التعرف علي تقنيات أمن الشبكات المحتوى الرقمي.

٣- التعرف علي التهديدات التي تواجه أمن المستودع الرقمي للرسائل الجامعية المصرية.

٤- التعرف علي طرق وأساليب أمن المقومات المادية والبرامجية للمستودع الرقمي للرسائل الجامعية المصرية .

ويمكن تحقيق الأهداف السابقة من خلال الإجابة على مجموعة التساؤلات التالية:

١. ما المستودع الرقمي للرسائل الجامعية المصرية؟
٢. ما أهداف المستودع الرقمي للرسائل الجامعية المصرية؟
٣. ما أهمية تأمين وحماية المحتوى الرقمي بمستودع الرسائل الجامعية المصرية؟
٤. ما طرق معالجة الرسائل الجامعية بالمستودع الرقمي للرسائل الجامعية المصرية؟
٥. كيفية تأمين التجهيزات المادية و البرامجية بمشروع المستودع الرقمى للرسائل الجامعية المصرية؟

١/٤ مجال الدراسة وحدودها :

يتناول البحث موضوع امن وحماية المحتوى الرقمي للمستودع الرقمي للرسائل الجامعية المصرية المتاحة من خلال بوابة اتحاد المكتبات الجامعية المصرية www.eulc.edu.eg منذ بداية انشاء المستودع الرقمي للرسائل الجامعية المصرية بتاريخ ٢٠٠٩/٧/١ حتى الآن.

١/٥ منهج الدراسة وأدوات جمع البيانات :

تعتمد الدراسة على المنهج الوصفى التحليلى حتى يمكن الإجابة على تساؤلات الدراسة وتحقيق أهدافها، من خلال قدرة هذا المنهج على رصد ووصف وتحليل أمن وحماية المحتوى الرقمى للرسائل بمشروع المستودع الرقمى للرسائل الجامعية المصرية، وبما يسمح برسم صورة لأساليب أمن وحماية المستودع الرقمى للرسائل الجامعية المصرية بما يمكن من الإفادة منها فى ضوء واقع أمن وحماية المحتوى

الرقمي علي شبكة الانترنت، وفى هذا الإطار يعتمد الباحث على مجموعة من أدوات جمع البيانات أهمها:

١- الإنتاج الفكرى الصادر فى الموضوع حيث تم البحث فى فهارس المكتبات لحصر الإنتاج الفكري الذى يتناول موضوع الدراسة، وتأتى أيضا شبكة الإنترنت كأحد الوسائل الهامة التى تساعد فى عمليات البحث والاتصال للحصول على المصادر التى تناولت اجراءات أمن المحتوى الرقمي للمستودع الرقمي للرسائل الجامعية المصرية.

٢- قائمة مراجعة

حاول الباحث جمع البيانات المتعلقة بأمن المحتوى الرقمي للمستودع الرقمي للرسائل الجامعية المصرية ، من خلال إعداد قائمة مراجعة تحتوى على مجموعة من المحاور اللازمة لإنجاز البحث ورصد اجراءات امن المحتوى الرقمي للمستودع بمختلف الجوانب كما يلي :

جدول (١) محاور قائمة المراجعة

المحور	البنود الفرعية
مشروع المستودع الرقمي للرسائل الجامعية المصرية	٦
الأمن المادي والبيئى للمستودع الرقمي للرسائل الجامعية المصرية	٢١
أمن الموارد البشرية	١١
إدارة أمن البيانات	١٣
المجموع	٥١

تم الاعتماد علي مجموعة من المصادر في اعداد هذه القائمة منها :

- المواصفة الدولية القياسية لأمن البيانات الصادرة عن منظمة الأيزو ISO/IEC 270002:2013
- العربي، أحمد عبادة. (٢٠١٥). معيار المنظمة الدولية للتوحيد القياسي آيزو ٢٧٠٠٢ لسياسات أمن المعلومات: دراسة وصفية تحليلية لمواقع الجامعات العربية. *مجلة جامعة طيبة للآداب والعلوم الإنسانية: جامعة طيبة – كلية الآداب والعلوم الإنسانية، مج٤، ع١٧* ، ٦٦١ – ٧٣٨.
- بامفلح ، فاتن سعيد. حماية أمن المعلومات بشبكة المكتبات بجامعة ام القرى : دراسة حالة .. المؤتمر الثاني عشر للاتحاد العربي للمكتبات والمعلومات (اعلم) . ٤-٨ نوفمبر ٢٠٠١

٣- **النظام الفرعى** لإدارة المحتوى الرقمى للرسائل على برنامج مكتبات المستقبل System(FLS) Future Library.

٤- **المقابلة:** واعتمد الباحث على هذه الأداة فى جمع البيانات من خلال المقابلة مع السيد المهندس/ محمد محمد الرافعي . مبرمج وأحد مصممي نظام إدارة المحتوى الرقمي لنظام المستقبل لإدارة المكتبات بمركز تقنية الاتصالات والمعلومات بجامعة المنصورة وذلك للإجابة علي بعض الأسئلة الخاصة بأساليب حماية المستودع الرقمي للرسائل الجامعية المصرية.

٦/١ مصطلحات الدراسة :

تتعد المصطلحات المستخدمة فى هذه الدراسة وهى:

- الأمن : security

يعرف قاموس odlis لمصطلحات المكتبات والمعلومات الأمن في مجال الحوسبة بأنه "التكنولوجيا المتقدمة لمنع الاشخاص الغير مرخص لهم، وخصوصا المتسللين والمخترقين، من الوصول إلي الأنظمة والملفات المحمية بما في ذلك تشفير البيانات والكشف عن الفيروسات وجدران الحماية بمعنى اعم جميع التدابير التي تتخدها

المؤسسة لمنع الاشخاص غير المخولين من الوصول إلي المعلومات السرية وهو مصطلح عام يشمل جميع المعدات والموظفين والممارسات والاجراءات المتبعة لمنع سرقة أو تدمير المواد والمعدات وحماية الموظفين والمستفيدين من الاجراءات الضارة "

امن المعلومات : information security

يعرف قاموس odlis أمن المعلومات "حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة ووسائط المعلومات"

حماية البيانات : data protection

يعرف المعجم الموسوعي لمصطلحات المكتبات والمعلومات حماية البيانات بأنه " الأساليب المتبعة لحماية صحة وأمن وسلامة المعلومات الشخصية التي تحتفظ بها المؤسسات في شكل إلكتروني ومدى الاعتماد عليها والوثوق من صحتها"

إدارة الحقوق الرقمية digital rights management

يعرف المعجم الموسوعي لمصطلحاتالمكتبات والمعلومات إدارة الحقوق الرقمية بأنه "نظام للتعرف على حقوق الملكية الفكرية *intellectual property rights* المتعلقة بأعمال معينة في شكل رقمي *digital format* والتي بإمكانها توصيل الأفراد بتلك الأعمال على أساس التصريح لهم بذلك. وهدف نظم إدارة الحقوق الإلكترونية هو التوزيع الإلكتروني للمواد وفي نفس الوقت حماية تلك المواد من النسخ أو الوصول غير المصرح به إلى تلك المواد"

التشفير : encryption

يعرف قاموس odlis لمصطلحات المكتبات والمعلومات التشفير بأنه "عملية تحويل البيانات الواردة في رسالة الى شفرة سرية قبل الارسال عبر قنوات الاتصالات السلكية واللاسلكية العامة لجعل المحتوى غير مفهومة للجميع ولكن مفهومة للمرسل اليه والمخول بالرسالة . في الحوسبة ، ويتم ذلك غالبا التعديل عن طريق خوارزمية تحول.

التشفير هو مقياس الأمن المتخذ لحماية المعلومات السرية ، مثل أرقام بطاقة الائتمان المستخدمة في المعاملات التجارية عبر الإنترنت"

الرسائل الجامعية Theses

تعرف (سالم، ٢٠٠٩) الرسالة العلمية بأنها ذلك " العمل الأكاديمى المجاز من طرف الجامعة،هو بمثابة خلاصة حلقة زمنية دراسية كاملة لمختلف أطوار التكوين (ماجستير، دكتوراه)".

المستودع الرقمى Digital Repository

يعرفه (فراج،٢٠٠٧) المستودع الرقمى بأنه" ذلك المقر الذى يحفظ فيه الإنتاج الفكرى الرقمى ويكون منظم بأسلوب علمى إذا تحوى وظائف ذلك الإنتاج الفكرى كالميتاداتا، ويتيح ذلك المقر إمكانية البحث والاسترجاع والتحميل الهابط من محتواه فى الغالب يكون هناك إمكنية الإضافة إلى مجموعات ذلك المقر "

مشروع المستودع الرقمى للرسائل الجامعية

هو الاسم الذى أطلقته وحدة المكتبة الرقمية على علميات التحويل الرقمى للرسائل الجامعية وإتاحتها من خلال بوابة اتحاد المكتبات الجامعية المصرية www.eulc.edu.eg .

٧/١ الدراسات السابقة :

وقد حصر الباحث مجموعة من الدراسات التى اهتمت بموضوع أمن وحماية الرسائل الجامعية المحتوى الرقممي ومشكلات الاتاحة للمحتوى الرقمي من خلال المستودعات الرقمية في البيئة الرقمية والتى يمكن تتبعها تاريخيا فيما يلي:

تتناول دراسة (**العميرى، ٢٠١٦**) واقع ممارسات أمن المعلومات في المكتبة الرئيسية بجامعة السلطان قابوس ومدى توافقها ممع المعيار الدولي لأمن المعلومات ISO/IEC 27002 والوقوف علي جوانب الضعف في السياسات الأمنية واتخاذ

التوصيات لتحسينها، وركزت الدراسة علي ثلاثة أبعاد وهي أمن الموارد البشرية، والأمن المادي والبيئي، وأمن التقنيات، واعتمدت الدراسة علي منهج دراسة الحالة وكشفت نتائج الدراسة عن توافق ممارسات أمن المعلومات في المكتبة الرئيسية مع ممارسات المعيار الدولي لأمن المعلومات وخرجت الدراسة بمجموعة من التوصيات أهمها ضرورة الاستمرار في تدريب وتوعية المستفيدين في المكتبات حول الاستخدام الأمثل لمصادر وخدمات المعلومات .

ويؤكد **(عمر، ٢٠١٥)** علي أهمية أمن المعلومات في مكافحة الجرائم الإلكترونية وتهدف الدراسة إلي التعريف بمفهوم أمن المعلومات وبث ثقافة حمايتها، والتوعية بالمخاطر والتحديات التي تتعرض لها، ومحاربة الجريمة الإلكترونية والوقوف علي تجربة المركز السوداني لأمن المعلومات وتقييمها من حيث مهامه وواجباته وخدماته. تأتي أهمية هذه الدراسة من أهمية الموضوع نفسه، حيث إن موضوع أمن المعلومات يعد واحدا من أهم الموضوعات الجارية والتي تحتاج إلي إجراء المزيد من الدراسات والأبحاث عليها وخصوصا الدراسات التي ترفع من نسبة الوعي بأمن المعلومات لعامة أفراد المجتمع ولتحقيق هذه الأهداف اتبعت الدراسة المنهج الوصفي التحليلي ومنهج دراسة الحالة وذلك لتناسبهما مع مثل هذا النوع من الدراسات وتوصلت الدراسة إلي مجموعة من النتائج والتوصيات نلخصها في ضرورة الاهتمام بالجانب التعليمي لأمن المعلومات وبتثقيف أفراد المجتمع بأهميته، وعقد التظاهرات العلمية الخاصة به والتأكيد علي ضرورة إنشاء مجموعة من المراكز الخاصة بأمن المعلومات علي غرار المركز السوداني لأمن المعلومات.

وتؤكد دراسة (Kumar,2014) أن الأنظمة في عالم الشبكات تعاني من هجمات متعددة داخلية وخارجية، قد تؤدي إلي تعطل الخدمات أو إصابتها بتأثيرات ضارة أو تدميرها لذا يعد تطبيق أجهزة الأمان مثل جدران الحماية وأنظمة كشف التسلل وحماية حركة مرور الشبكة مع الشبكات الخاصة الإفتراضية واستخدام

البروتوكولات الآمنة للشبكات من الأمور المهمة لتعزيز الأمن الكامل للشبكات وللمستودعات الرقمية .

أما دراسة **(حسين، ٢٠١٢)** فقد تناولت قضية أمن المعلومات وتبادلها عبر الشبكات من القضايا التي تشغل بال ليس فقط الباحثين والمختصين، بل المنظمات الدولية والعالم المرتبط بها أيضاً، وذلك نظراً للأهمية الفائقة لتقنيات المعلومات في شتى مجالات الحياة في هذا العصر، ولا شك أن تزايد الاعتماد على المعلومات وشبكاتها يزيد أيضاً من تأثير الأخطار التي يمكن أن تواجهه، ولذا فلابد من تواصل عمليات السعي إلى مواجهة هذه الأخطار والاهتمام بتطوير الأساليب والوسائل التقنية اللازمة للمواجهة هذه الأخطار، إضافة إلى إيجاد أفضل القواعد الإدارية التي تساهم في دعم هذه المواجهة من أجل الحد من الأخطار المحتملة بل والسعي إلى التخلص منها إن أمكن.

ويشير **(حافظ ،٢٠١٠)** إلي أن للاطراحات مكانة خاصة كشل من أشكال مصادر المعلومات لاسيما في المكتبات الجامعية والبحثية نظرا لأنها عصارة فكرة الباحثين والدارسين وقد اتجهت المكتبات ومؤسسات المعلومات عامة في الآونة الاخيرة إلي رقمنة ما لديها من رصيد أو انتاج فكري وظهرت العديد من المشروعات الرقمية المعنية بتحويل واتاحة الانتاج الفكري في الشكل الرقمي ويعد وضع الاطروحات في شكل رقمي واتاحتها من التحديات التي تواجه المكتبات الجامعية لما يتطلب ذلك من عمليات اجراءات التحويل الرقمي والخزن والاسترجاع فضلا عن حماية هذا المحتوى الرقمي.

وتناول دراسة **(النقيب، ٢٠١٠)** التحديات الأمنيةالمشاريع الرقمنة بمؤسسات المعلومات العربية ونظمها وتطبقاتها في البيئة الرقمية المحملة علي شبكات المعلومات وقابليتها للتعرض للضرر والخطر، مثل اختراقات ومخاطر نظم إدارة

المحتوى الرقمي وفاعلية الآليات المطبقة لإدارة المخاطر، ومكونات نظم إدارة المحتوى الرقمي . وتوصلت الدراسة إلي دم كفاية إجراءات الرقابة المطبقة لمواجهة المخااطر التي تترض لها ثلاثة عناصر من مكوونات إدارة المحتوى الرقمي بمؤسسات المعلومات العربية، نتيجية التركيز علي الجوانب الفنية دو الإهتمام بالجوانب الأمنية.

ولخص كلا من **(Satyanarayana , Babu,2008)** تاريخ تطور رقمنة الرسائل العلمية الهندية ورصد أهم العوائق التي تعترض عمليات الرقمنه مع اقتراح خطة نموذجية لتسريع عمليات رقمنة الرسائل معتمدين فى ذلك على الإرشادات التوجيهية التي صدرت مؤخرا عن (لجنة المنح الجامعية الهندية)، والتى تشجع على إيداع الرسائل العلمية فى شكل إلكترونى وفق المعايير العالمية، ونشر المستودعات الرقمية المؤسسية فى الهند، ومن جهة أخرى حددت الدراسة العديد من التحديات التى تواجه المستودعات الرقمية مثل المخاوف التى تتعلق بالانتحال، وانتهاكات حقوق التأليف والنشر، ونوعية الأبحاث العلمية، والافتقار إلى تطوير السياسات على المستوى الجامعي، وضعف البنية التحتية وعدم كفاية المهارات التقنية لموظفي المكتبات في عمليات الرقمنة والتحميل، والصيانة، بالإضافة إلى ضعف القدرة على تهيئة برامج المستودعات الرقمية المؤسسية والتعامل مع نظم التشغيل يونيكس أو لينكس UNIX or Linux. والفهم المحدود لاستخدام مخططات الميتاديتا وقضايا حق المؤلف.

يلقى **((Damodhar,2002)** الضوء على الاتجاهات الحديثة فى إتاحة مصادر المعلومات بالمكتبات الجامعية وذلك لكونها تمثل مخازن عظيمة لمصادر المعلومات المختلفة الأشكال، والتى أصبح الوصول متاحاً من أى مكان فى العالم عبر شبكة الإنترنت، كما رصد الدراسة وجود تفاوت بين المكتبات الأكاديمية الهندية فى رقمنه مجموعاتها وإتاحتها عبر الإنترنت وأن أغلب هذه المكتبات مازالت تقدم

خدماتها بشكل تقليدى، إلا أن الدراسة أكدت على أن المكتبات الهندية لا يمكن أن تظل معزولة عن الاستفادة من التكنولوجيا الحديثة في رقمنه رسائلها الجامعية وإتاحتها عبر الإنترنت ، وبناء على ذلك فقد رصدت الدراسة واقع المكتبات الهندية ووضعت تصوراً خاصا بالمستقبل فيما يتعلق بعمليات الرقمنه وإنشاء المكتبات الرقمية فى الجامعات الهندية .

القسم الثاني : الإطار النظرى للدراسة

٢/٠ : تمهيد :

المعلومات هي من أهم الموجودات الضرورية في أي مؤسسة؛ لذا فإن هناك حاجة ملحة لحمايتها من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. وأمن المعلومات علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية.

٢/١ مفهوم أمن المعلومات :

ويرى (الصوفي،٢٠٠٣ ؛ص٢٢) "أن مجتمع المعلومات الذي نشهده هو مجتمع المصالح المتبادلة وللانضمام إلى هذا المجتمع لا يتم إلا من خلال خلق الظروف المناسبة للإبداع والابتكار والتمكن من صنع التكنولوجيا واستخدامها وتطويرها لتخدم الباحثين وأهدافهم في التطور والتقدم، وهذا يتطلب إقامة المزيد من المحتوى العربي على شبكة الانترنت لإثبات الوجود، الحضارة، الإبداع، وزيادة الوعي بالرهانات التي

تطرحها البيئة الجديدة والعمل على ضمان حماية وأمن المعلومات لنضمن بذلك الانخراط في مجتمع المعلومات على طريق المساهم المشارك وليس على طريق المشاهد المستهلك".

ولن يتم تأمن المعلومات والمحتوى الرقمي العربي إلا من خلال التمكن من التكنولوجيا الحديثة وتطويرها لخدمة الباحثين والمستفيدين من ذلك المحتوى والحفاظ عليه من كل أنواع التخريب والسرقة.

٣/٢ أمن المعلومات في البيئة الرقمية:.

ويشير **(الهادي،٢٠٠٦؛ ص١٤)** إلي أن أمن المعلومات ونظمها في البيئة الرقمية يمثل حماية للمعلومات من حيث توافرها وإضفاء الثقة فيها وتأكيد سلامتها. ويعبر توافر المعلومات علي خاصية من خصائص نظم المعلومات الممكن الوصول إليها واستخدامها علي أساس فوري في إطار نمط محدد ومطلوب، كما يصبح في الإمكان الوصول إلي النظام عندما يطلب بطريقة معتمدة ووفقا لمواصفات ملائمة لهذا للنظام، وتعتبر السرية خاصية ترتبط بعدم تغيير البيانات والمعلومات أو فقدها أو إهدارها وإتاحتها فقط لأشخاص وكيانات معتمدة ومصرح لها فقط باستخدامها، وتتضمن العمليات التي تستخدم أساليب التشفير والحجب لمحتويات البيانات والمعلومات أو السماح بها في أوقات وفي طرق معتمدة. أما السلامة فهي خاصية البيانات والمعلومات الدقيقة والكاملة التي تحفظ بدرجة كبيرة من الدقة والاكتمال.

ويرى الكثير أن أمن المعلومات لا يعنى منعها أو حجبها وعدم الوصول إليها بل تعنى إتاحتها فقط للأشخاص المصرح لهم بالحصول عليها واستخدامها

٤/٢ المخاطر التي تتعرض لها الشبكات:

تلخص **(باملفح ، ٢٠٠١)** المخاطر التي تتعرض لها الشبكات في المحاور التالية :.

- مخاطر طبيعية (الكوارث الطبيعية . الحريق...الخ)
- مخاطر عامة (انقطاع التيار الكهربائي . انقطاع الانترنت . سرقة البيانات)

- مخاطر تكنولوجية (الفيروسات . ديدان الانترنت . التجسس علي البريد الإلكتروني . الإختراق الأمنى للنظام من الداخل او الخارج)

ومن أبرز المخاطر التي تتعرض لها الشبكات ما يلي :

١.اقتحام الهاكرز Hackers• والكراكرز Crackers**للشبكة مما يؤدي إلى تفشي أسرار العمل والعاملين، أو تخريب البيانات وإتلافها أو تعرض البيانات للتغيير أو التعديل أو المسح بغرض تحريف البيانات أحيانًا أو سرقتها في أحيان أخرى.

٢. التصنت علي كابلات الشبكة.

٣. التجسس على مستخدمي الشبكة.

٤. إقحام الفيروسات للشبكة سواء كانت فيروسات مزعجة فقط أم مدمرة تعرض أجهزة الشبكة وبياناتها للتلف أو الفقدان.

٥. إطلاع الأشخاص المصرح لهم باستخدام الشبكة على معلومات غير مصرح لهم بالإطلاع عليها.

٦. التشويش على الإشارات المنقولة عبر الكابلات.

٧. تعطيل أحد الأشخاص لنظام الأمن الخاص بالشبكة أو كشفه لإجراءات الحماية المتبعة.

ونلاحظ في ظل التقدم السريع في تكنولوجيا المعلومات والاتصالات تعرض الشبكات وما تحوية من محتوى رقمي أو أية بيانات إلي كثير من المخاطر سواء كانت مخاطر تقنية أو مخاطر بشرية

•الهاكرز **Hackers** هو الشخص الذي حقق مهارة تقنية عالية ويجد متعة خاصة في الدخول غير المشروع الى أنظمة الحاسبات الكبيرة عبر الشبكات

** الكراكر **Cracker** شخص يخترق النظم الأمنية بغرض سرقة أو إفساد البيانات، أي أن هدفه تخريبي أو إجرامي

٢/٥ مظاهر النصب و الاحتيال في عالم النشر الإليكتروني

ويرى **(فؤاد، ٢٠١٠)** أن تكنولوجيا المعلومات والاتصالات وفرت للمكتبات الأدوات والوسائل اللازمة لتسهيل عملية الحصول على المعلومات وتبادلها وجعلها في متناول المستفيد منها بسرعة وفعالية، حيث أصبح المستفيد بإستطاعته الابحار بحرية كبيرة ضمن الموارد المعلوماتية الإلكترونية المتاحة على شبكة الانترنت. هذا من ناحية ومن ناحية أخرى كثرت مظاهر النصب والإحتيال الإليكتروني الذي يستهدف المعلومات التي تعتبر العمود الفقري للبيئة الجديدة، فالمعلومات والبيانات لها قيمة في حد ذاتها فضلا على أنها ذات قيمة علمية، ثقافية، إقتصادية، سياسية .... الخ ولهذا نجد أن النصب والاحتيال في مجال المعلومات قد يفوق النصب والاحتيال في مجال المال وفيما يلي يمكن تناول مظاهر النصب والاحتيال علي شبكة الانترنت في النقاط الثلاثة الآتية :

- **النسخ غير الشرعي:** مكنت التطورات الحديثة من إنتشار ظاهرة النسخ اللامحدودة للأعمال والمعلومات على نطاق واسع داخل البيئة الإلكترونية مما أدى إلى إنتشار ورواج ظاهرة النصب والاحتيال المعلوماتي التي تنعكس سلبا على اعتماد النشر الإليكتروني.

- **سرقة المعلومات:** تعتبر ظاهرة سرقة المعلومات من أهم مظاهر النصب في عالم النشر الإليكتروني التي تعتبر واحدة من السلبيات العديدة التي أفرزتها التكنولوجيا الحديثة والتي من شأنها أن تعمل على الحد من انتشارها داخل البيئة الأكاديمية.

- **سرقة البرامج :**وهوالقيام بنسخ البرامج أو تزويرها واستخدامها بطريقة غير شرعية وإعادة ترويجها ضاربين عرض الحائط بذلك الحق في الملكية لأصحابها.

نلاحظ أن تكنولوجيا المعلومات والاتصالات لها عوامل ايجابية وسلبية وتتمثل العوامل الإيجابية في توفير الوقت والجهد في الحصول علي المعلومات وتبادلها

وتتمثل العوامل السلبية في مظاهر النصب والاحتيال في سرقة المعلومات ونسخها وسرقة البرامج وتخريب البيانات.

٦/٢ أساليب حماية المحتوى الرقمي علي شبكة الانترنت

وتعرض **(باملفح ،٢٠٠١)** "للأساليب التي تتبع لحماية الشبكة والمحافظة على أمن المعلومات فيها، ولابد من مراعاة تطبيق بعض تلك الأساليب عند التخطيط للشبكة وإنشائها، في حين يراعى البعض الآخر عند اختيار البرامج، هذا إلى جانب الأساليب المرتبطة بالقائمين على الشبكة ومستخدميها."

وقبل تناول أساليب حماية المحتوى الرقمي علي شبكة الانترنت نطرح هنا مجموعة من الأسئلة حيث لا يمكن البدء في إجراءات أمن المنشأة قبل الإجابة عليها ويمكن تلخيصها فيما يلي :

- ماذا نحمي؟
- ونحمى ضد من؟
- ما الأضرار الناجمة عن عدم تأمين المحتوى الرقمي علي شبكة الانترنت؟
- إلي أي مدى يمكن حماية المحتوى الرقمي علي شبكة الانترنت؟

وفيما يلي تلخيص لأبرز الأساليب المتبعة لحماية المحتوى الرقمي علي شبكة الانترنت :.

أولاً: الأمن المادي والبيئى physical and environmental security

ويرى **(داود، ٢٠٠٠)** أن الحماية الفيزيائية لشبكات المعلومات تتمثل في اختيار المكان والتجهيزات الملائمة للشبكة وتنقسم الحماية المادية لمباني الشبكات إلي ما يلي:

١- الحماية العامة للمبنى

الحماية العامة لمبنى الشبكة يتمثل في اختيار موقع مبنى الشبكة بعيد عن الأخطار

البيئية المحتملة بحيث تكون بعيدة عن خزانات الوقود وخزانات المياه ...الخ.

٢- الحماية ضد الحريق

يجب الالتزام ببعض الإجراءات الاحترازية لحماية مبنى الشبكة من أخطار الحريق وتقليل خسائره إلي اقصى درجة ومنها :.

- استخدام المواد المقاومة للحريق
- منع التدخين في أماكن الشبكات الحساسة
- المحافظة علي تهوية وتكييف مبنى الشبكة
- استخدام خزائن واقية ضد الحريق لوسائط تخزين البيانات
- استخدام وسائل اكتشاف الحريق والإنذار بحدوثه

٣- حماية الخدمات الأساسية

وهي التي يؤثر تعطيلها علي أداء الشبكة مثل مصدر الطاقة الكهربية بحيث يضمن الاستمرار بالإمداد بالطاقة (Uninterruptible Power Supply (ups وهو يقوم بتخزين الطاقة الكهربية في حالة توافرها واخراجها في حالة انقطاعها ويتم بواسطته تشغيل خادم الشبكة ومكوناتها الأخرى لفترة وجيزة تكون كافية لإغلاق النظام بشكل طبيعي حتى لا يتم فقد البيانات أو تلفها أو تحريفها عند انقطاع التيار الكهربائي وهناك نوعان من (ups) هما :

- **مصدر الطاقة الدائمة المباشر Online Power Supplies**

وتقوم بتزويد الحاسب بالطاقة بشكل مستمر حيث يتوافر جهاز ups بين مصدر الطاقة الاعتيادية وبين جهاز الحاسب

- **مصدر الطاقة الدائمة البديل Switched Power Supplies**

ويقوم بتفعيل عمل الطاقة الاحتياطية في حالة انقطاع الطاقة الاعتيادية فقط. ويعمل مصدر الطاقة البديل المتصل بالحاسب على مراقبة تقلبات مستوى الطاقة، وفي حالة

توقف الطاقة الاعتيادية يقوم بالتحويل إلى مصدر الطاقة البديل، ويقوم مولد الطاقة في هذه الحالة بتوصيل الطاقة من مصدرها الاعتيادي مباشرة إلى الحاسب

ويراعى أيضا الاهتمام بتكييفات الهواء لمبنى الشبكة عن طريق توفير الأجهزة المطلوبة والصيانة المستمرة لوحدات التكييف وإعداد وحدات تكييف بديلة واستبدال وحدات التكييف في حال تعطلها.

نلاحظ أن الحماية الفيزيائية لمبنى شبكة المعلومات والمحتوى الرقمي لا تقل أهمية عن حماية الاجهزة والبرامج حيث أنها هي التي تضم وتحوى الأجهزة والبرامج وسلامتها من سلامة وأمن الشبكة .

ثانيا : التحكم في الوصول إلى الشبكة وإتاحة مواردها : access control system

ويحدد (**أبو السعود**،٢٠٠٠؛ ص٣٧١) أساليب ضبط الوصول إلى الشبكة لحمايتها من التعرض لعمليات الاقتحام ،ولا يقتصر الأمر هنا على حماية الشبكة من اقتحام الأشخاص الغير مصرح لهم بالدخول إليها واستخدام مواردها، ولكن يتجاوزه إلى حمايتها أيضًا من محاولة دخول أشخاص مصرح لهم إلى ملفات ومصادر غير مصرح لهم باستخدامها. ولتحقيق ذلك لابد من تخصيص اسم أو رقم تعريف user ID وكلمة مرور Password لكل مستخدم للشبكة حيث تعد هذه هي الخطوة المتبعة لمنع اقتحام الشبكات يتبعها التحقق من أن المستخدم لديه حقوق ممارسة ما يريد ممارسته على موارد الشبكة مثل حق الإنشاء للملفات والفهارس، أو حق المسح والاستعراض أو التغيير أوالفتح والقراءة أو الكتابة..الخ، ويمكن أن يمنح المستخدم حقًا أو اكثر من تلك الحقوق حسب تصنيفه، كما يمكن تخصيص صفات للملفات نفسها مثال: ملف للقراءة فقط، ملف للقراءة والكتابة، ملف غير قابل للإلغاء، ملف غير قابل للنسخ ،ويمكن تصنيف الوصول إلي الشبكة ومواردها عن طريق احد أساليب الاتاحة التالية :.

١- إتاحة على مستوى مشاركة

٢- إتاحة على مستوى مستخدم

٣-العلامة المائية الرقمية

يؤكد كلا من (طه و عبد الرحيم ، ٢٠٠٧) أن التطور السريع في الاتصالات وتقنيات الوسائط المتعددة أدى ضرورة استخدام تقنيات لحماية حقوق الملكية الفكرية ومراقبة النسخ غير الشرعي للبيانات والمعلومات ومن أهم هذه التقنيات تقنية العلامة المائية الرقمية

ومما سبق يتضح أن ضبط الوصول إلي الشبكة وإتاحة مواردها أحد أساليب حماية الوصول إلي المحتوى الرقمي علي الشبكة بالاضافة إلي تحديد صلاحيات المستخدم طبقا للمهمة المنوط بها داخل الشبكة، وتتفاوت هذه الصلاحيات من أعلاها إلي ادناها حسب وظيفة كل مستخدم.

ثالثا : تشفير البيانات Data Encryption

يشير مصطلح كلمة تشفير إلى تحويل النص العادي (Plaintext) من شكل مقروء، بواسطة خوارزميات التشفير ومفاتيح (Keys) التشفير ، إلى هيئة نص مرمز (Ciphertext) وغير مقروءة، ثم إعادة فك الترميز(Decryption) هذا وإعادة النص إلى أصله بواسطة الخوارزميات أيضا ومن قبل الأشخاص المسموح لهم بذلك (الذين يملكون أدوات فك التشفير). ويمكن تصنيف أنواع التشفير إلي ما يلي:

أنواع التشفيرEncryption Types

ويصنف (**غبيق، ٢٠١٣**) التشفير بناءً على المفاتيح المستخدمة في التشفير وفك التشفير إلى نوعين تشفير متماثل Symmetric Encryption وتشفير غير متماثلAsymmetric Encryption :

- **تشفير متماثل Symmetric Encryption:**

ويعرف أيضا بتشفير المفتاح الخاص Private Key Encryption حيث يستخدم فيه نفس المفتاح لتشفيرالرسالة ولفك التشفير يجب أن يتفق الطرفان على مفتاح التشفير مما يؤدي لمشكلة عند توزيع المفتاح عبر الشبكات فربما يحدث التقاط لهذا المفتاح، وبالتالي كشف المراسلات بين الطرفين لذلك يجب تبادل المفاتيح بطريقة تضمن سريتها

- **تشفير غير متماثلsymmetric Encryption :**

ويعرف أيضا بتشفير المفتاح العام Public Key Encryption حيث يستخدم فيه زوج من المفاتيح أحدهما لتشفير الرسالة والآخر لفك التشفير يعرف الأول بالمفتاح العام Public Key سمي بذلك لانه يكون معروف للمستخدمين في البيئة المعينة، ويستخدم لتشفير الرسائل ،أما الثاني فيعرف بالمفتاح الخاص Private Key سمي بذلك لانه معروف لمستخدم واحد فقط هو مالكه ويستخدم لفك الرسائل المشفرة بالمفتاح العام المقابل له.يعاب على هذه الطريقة كثرة المفاتيح المستخدمة في التشفير وفك التشفير.

نلاحظ أن تشفير البيانات في الوقت الراهن له أهمية كبيرة في تأمين وحماية الشبكات والمحتوى الرقمي خصوصا في ظل تزايد تقنية التصنت علي كابلات شبكة الانترنت لمعرفة البيانات والتقاطها

رابعاً: استخدام الحوائط النارية firewall

يمكن وصف الجدران النارية، بأنها عبارة عن جهاز (hardware) أو نظام (software) يقوم بالتحكم في مسيرة ومرور البيانات في الشبكة أو بين الشبكات والتحكم يكون إما بالمنع أو السماح

ويرى كلا من **(القحطاني، الغثبر، ٢٠٠٩)** أنه بسبب كثرة الأخطار التي تهدد شبكات المعلومات من خارجها، نشأت فكرة إقامة جدارن الحماية التي تسمى

أيضا الجدران النارية، التى يمكن وصفها بأنها نظام مؤلف من برنامج (software) يعمل في حاسوب وقد يكون حاسوبا عاديا مثل الحواسيب الشخصية، أو حاسوبا بنى بمواصفات خاصة ليكون أكثر قدرة علي تلبية المتطلبات الفنية الخاصة بجدران الحماية، وفكرة جدران الحماية تشبه فكرة نقطة التفتيش التى تسمح بمرور أناس، وتمنع مرور آخرين، بناء علي تعليمات مسبقة، ويهدف تصميم جدران الحماية من فرز كل البيانات الداخلة والخارجة من وإلي الشبكة سواء علي مستوى الجهاز الواحد، أو علي مستوى الشبكة ويجب أن تمر بالجدار الناري أولاً قبل الانتقال للطرف الآخر ويكون التحكم في البيانات عن طريق استثنائها.

يلاحظ مما سبق ان استخدام الجدران النارية خيار للتحكم في الدخول والخروج من وإلي شبكة الانترنت بهدف حماية الشبكة الداخلية من أي اختراق لها من الخارج ويمكن أن تكون الجدران النارية أجهزة أو برامج

خامسا : الحماية من الفيروسات Virus protection software

ويشير (**بسيوني** ،٢٠٠٣،ص ١١٨) إلي أن الفيروسات هي برامج صغيرة تلحق نفسها بملف ما وتقوم بإعادة نسخ نفسها بسرعة كبيرة من ملف إلي آخر ومن كمبيوتر إلي آخر وتعمل بشكل مستقل عن ملفات التشغيل الآخرى، وتقوم بالسيطرة علي الذاكرة ومساحة القرص الصلب مسببة أضراراً كبيرة للأجهزة والملفات، كفيلة بتدمير البرامج والمعلومات أو إصابة الأجهزة بالخلل. ويتم تصنيف الفيروسات علي عدة طرق منها طريقة الهجوم ومكان الهجوم ونوعية الملفات وحجم التدمير ومن اشهرها ما يلي :.

فيروسات قطاع الاستنهاض boot sector virus

وهو من اقدم الفيروسات التي تصيب الأقراص الصلبة والمرنة وتكمن خطورته في إصابة جزء أساسي من القرص مخصص لتوجيه الجهاز في تحميل نظام التشغيل

فيروسات عدوى الملفات file infector virus

وهو فيروس يلحق نفسه كملف في البرامج التنفيذية، وينسخ نفسه بسرعة علي الاقراص ورسائل البريد الإلكتروني الالكتروني وتكمن خطورته في الانتشار السريع واصابة ملفات البرامج التنفيذية الآخرى.

فيروس الماكروmacro virus

يتميز بسرعة الانتشار ولا يصيب إلا البرامج التطبيقية مثل برامج معالجة النصوص ولحماية الاجهزة ووحدات التخزين بما عليها من محتوى يجب استخدام البرامج المضادة للفيروسات حيث توجد شركات عديدة تنتجها من بينها symantec, command, mcafee وغيرها وتعمل تلك البرامج الآتي :.

١- فحص ذاكرة الحاسب عند بدء التشغيل بحثا عن أي فيروسات
٢- فحص وحدات التخزين بحثا عن أي فيروسات لإزالتها
٣- فحص الملفات المراد تحميلها علي وحدات التخزين للتأكد من سلامتها من الفيروسات
٤- فحص الملفات سواء المتاحة للمشاركة ام المنقولة عبر الانترنت .
٥- الفحص المستمر للنظام للتأكد من خلوه من الفيروسات والتنبيه عنها في حالة وجودها .

نلاحظ أن الفيروسات يمكن أن تدمر الأجهزة والملفات وتنتقل هذه الفيروسات عن طريق الانترنت أو وسائط التخزين (usb) ولابد من توفير برامج حماية ضد كل أنواع الفيروسات ولابد من تحديث هذه البرامج كل فترة زمنية

سادسا : النسخ الاحتياطي backup

ويعرف **(اليوسفي، ٢٠١١)** النسخ الاحتياطي بأنه الاحتفاظ بنسخ احتياطية من ملفات المستخدم وملفات نظام التشغيل، حتى يتمكن المستخدم من الرجوع إليها في حال تم فقدانها، ويقصد باستعادة النظام المساعدة في استرداد ملفات نظام التشغيل

إلى فترة سابقة من الزمن يتم تحديدها تشمل نقاط الاستعادة، بمعنى استعادة كافة الملفات التي تم انشائها في ذلك الوقت أو كانت موجودة قبله، ويتم اللجوء إلي هاتين العمليتين عند حصول عطب مفاجئ في القرص الصلب؛ بسبب دخول فيروس غير متوقع إلى الجهاز، أو تحميل برامج ضارة، أو حصول تغيير غير متوقع على نظام التشغيل.

إن برامج النسخ الاحتياطي التقليدية تساعد على تنظيم و ترتيب الجدول الزمني لعمليات النسخ الاحتياطي أو الاستعادة، وصيانة الملفات المستعادة بشكل دائم، كذلك التحديث الآلي المستمر لهذه البرامج بشكل دوري يجعل القيام بذلك أسهل. وقد تعددت أشكال النسخ الاحتياطي واستعادة البيانات بعد العطل المفاجئ في القرص الصلب وتنوعت بمرور السنوات، إذ يمكن حصر أشكال النسخ الاحتياطي فيما يلي :.

١- نسخ كامل لكافة الملفات والبرامجfull backup

٢- نسخ تراكمي incremental backup

٣- نسخ تفاضلي differential backup

ونلاحظ أن من أسياسيات حماية المحتوى الرقمي النسخ الاحتياطي لقاعدة البيانات والمفات والبرامج علي فترات زمنية محددة وذلك لاستدعائها في حال فقدانها او تلفها وقد تم تطوير الكثير من البرمجيات المتخصصة في هذا المجال

ثامنا : ضبط الوصول

تحدد **(بامفلح،٢٠٠١)** الأساليب المتبعة لتحقيق الحماية من خلال مستخدمي النظام سواء كانوا موظفين أم مستفيدين:

أ. الموظفون:

يعد الموظفون من العناصر الأساسية التي قد تؤدي إلى إلحاق الضرر بالمعلومات، وتهديد أمنها سواء بشكل مقصود في حالة رغبتهم الإساءة للهيئة التي يتبعونها لأي دافع من الدوافع (كراهية، أو ملل، أوطمع، أو إثبات الذات) أم كانت

بشكل غير مقصود بسبب ضعف مستوى إعدادهم فنيًا للتعامل مع النظام، لذا ينبغي اتباع ما يلي:

١ –تحديد كلمات مرور للموظفين، على أن يراعى تحديد صلاحيات كل موظف بما يتناسب مع طبيعة عمله، فمن غير الملائم منح جميع الموظفين صلاحية الدخول إلى جميع مناطق العمل على النظام وإجراء التعديلات على البيانات والبرامج لأن ذلك قد يعرض النظام للخطر، ومن ناحية أخرى فإن منح الصلاحيات بدون حدود أمر لا ضرورة له؛ حيث أن هناك مناطق عمل لا تعني جميع الموظفين ولا تخص عملهم.

٢ –اختيار الموظفين بعناية تامة خصوصًا أولئك الذين يتعاملون مع بيانات حساسة والذين يمنحون صلاحيات عالية، حيث ينبغي التأكد من أمانتهم وإخلاصهم وذلك بإجراء تحريات عنهم وملاحظة سلوكياتهم بعد عملهم.

٣ – تدريب الموظفين بشكل جيد تجنبًا للعديد من المشكلات التي قد تواجهها الشبكة ومواردها نتيجة لضعف المستوى الفني للعاملين عليها؛ ومنها على سبيل المثال حذف شئ من البيانات بطريقة الخطأ أو تحديث البرامج أو إزالتها بطريقة خاطئة مما يؤثر على النظام والعمل القائم، فلابد من تدريب الموظفين على استخدام الأجهزة بكفاءة من ناحية، وكذلك تدريبهم على سبل التعامل مع المشكلات البسيطة التي قد تواجههم وكيفية التغلب عليها من ناحية أخرى.

٤– التأكد من إزالة بيانات الموظفين المنتهية مدة خدمتهم في المؤسسة من قائمة مستخدمي النظام، وقد يتطلب الأمر تغيير كلمة المرور الخاصة بمجموعة من الموظفين عند انتهاء خدمة أحدهم،.ويرى البعض ضرورة اتباع إجراءات أخرى حرصًا على الأمن من جانب الموظفين كأن لا تمنح صلاحيات عالية للموظفين حديثي التعيين، وكذلك ضرورة تضمين عقود عمل المتعاقدين لشرط يمنع إفشاء المعلومات الحساسة أو الإجراءات الأمنية للنظام.

ب. المستفيدون:

يسري عليهم بعض ما يسري على الموظفين حيث أنه إذا لم يتم تدريب مستخدم النظام بشكل كافي فإنه قد يلحق الضرر بالنظام وذلك بنقل الفيروسات أو إلحاق الضرر بالأجهزة .وقد يتعمد بعض المستفيدين إلحاق الضرر بالنظام في حالة تصورهم أن هناك إجراءات أمنية متشددة تتبع ضدهم بشكل يؤدي إلى إزعاجهم بدون مبرر مقنع بالنسبة لهم، مما يضطرهم إلى التحايل على النظام ومحاولة إلحاق الضرر به، ومن هنا يرى البعض ضرورة توعية المستفيدين بطريقة سليمة بالأسباب التي تدعو إلى استخدام كلمات المرور، والخروج من النظام، وتعريفهم بالأسباب التي تدعو إلى ضرورة عمل مسح للأقراص في حالة جلبها معهم للتأكد من خلوها من الفيروسات.

نلاحظ أن حماية الشبكات ونظم إدارة المحتوى الرقمي من العاملين والمستفيدين من أولي اهتمامات مسئولي الشبكات والمحتوى الرقمي لأنه ممكن ان يتم تخريب المحتوى من خلال العاملين أنفسهم أو المستفيدين الذين يتعاملوا مع المحتوى الرقمي بقصد أو من غير قصد لذا لابد من وضع اجراءات لوصول المستفيدين إلي المحتوى الرقمي وتحديد صلاحيات العاملين بنظم إدارة المحتوى الرقمي.

القسم الثالث : الدراسة الميدانية :

١/٣ مشروع المستودع الرقمى للرسائل:

في ضوء التطور الهائل فى عالم الحاسبات الآلية ونظم المعلومات والزيادة الملحة لتبادل المعلومات والبيانات بأسرع وقت ممكن، تم إنشاء شبكة الجامعات المصرية عام ١٩٨٧م بمقرها الرئيسي بمبنى المجلس الأعلى للجامعات بجامعة القاهرة، بهدف ربط الجامعات المصرية بعضها ببعض بحيث يمكنهم المشاركة فى الموارد المختلفة المتاحة لدى كل جامعة، ومن ثم أصبحت شبكة الجامعات هى أول شبكة محلية

وقومية للجامعات المصرية وتم ربط شبكة الجامعات المصرية بالشبكة الأوربية الأكاديمية والبحثية European Academic and Research Network (EARN)) عام ١٩٨٩م .

وبداية من عام ٢٠٠٥ استضافت شبكة الجامعات المصرية مشروعات تطوير التعليم العالي، وشملت ستة مشروعات رئيسية، من بينها مشروع تطوير نظم وتكنولوجيا المعلومات في التعليم العالي (ICTP) والذي ضم مجموعة من المشروعات الفرعية هي:

١- تطوير البينة الأساسية لشبكات معلومات الجامعات

٢- نظم المعلومات الإدارية

٣- التعليم الإلكتروني

٤- المكتبات الرقمية

٥- التدريب علي تكنولوجيا المعلومات

وأشار (مشروع تطوير نظم وتكنولوجيا المعلوماتICTP،2009) فى خطته عام ٢٠٠٩ إلى أن تنفيذ مشروع المستودع الرقمي للرسائل الجامعية ضمن مشروع المكتبات الرقمية، وتم بالتعاون بين وحدة المكتبة الرقمية بالمجلس الأعلى للجامعات، والجامعات المصرية على أن يتم التنفيذ بالمكتبات المركزية للجامعات وإعطاء أولوية للرسائل التى تم إجازتها خلال العشر سنوات الأخيرة فى قطاعات الطب والهندسة والعلوم.

وهدف هذا المشروع في البداية إلى إتاحة النصوص الكاملة لأكثر من ١٠٠ ألف رسالة جامعية أجازتها الجامعات المصرية، و شملت عملية التحويل الرقمى للرسائل الجامعية توفير بنية تحتية تشمل المكونات البرمجية والمادية اللازمة لعمليات التحويل الرقمى للرسائل الجامعية إلى جانب نظام لإدارة المحتوى الرقمي الناتج عن عملية الرقمنة ، بالإضافة إلي نظام لبناء وتجهيز الرسائل الجامعية الالكترونية ، كما

يحدد المخطط مجموعة المميزات التى يوفرها مشروع المستودع الرقمى للرسائل وهى :

١. تحقيق الضبط والسيطرة الكاملة على الرسائل الجامعية التي أجازتها الجامعة الحكومية مما يساعد في القضاء على التكرار غير المرغوب فيه.
٢. توفير قناة إلكترونية للتعريف بالرسائل الجامعية التي تجيزها الجامعات المصرية على المستوى الوطني الدولي.
٣. توسيع نطاق الإفادة من محتوى تلك المصادر الحيوية وإتاحتها عالميا مما يساعد على رفع القيمة التنافسية للجامعات المصرية.
٤. اختصار الوقت الذي يتطلبه طلبة الدراسات العليا للتعرف على الرسائل التي إجازتها الجامعات المصرية خلال الفترة الزمنية التي يشملها المشروع.
٥. تخفيض تكاليف النشر حيث أن الانتقال من النشر التقليدي إلى النشر الالكتروني سوف يساعد على خفض التكاليف اللازمة لإدارة المصادر وتوزيعها وحفظها.
٦. إتاحة محتوى تلك المصادر الحيوية مجانا للجامعات المصرية وتحصيل اشتراكات من الجهات والهيئات خارج نطاق المجلس الأعلى للجامعات سواء محليا أو عالميا.
٧. متابعه إحصائيات الإفادة من الرسائل الجامعية التي أجازتها الجامعات المصرية.

١/١/٣ أهداف مشروع المستودع الرقمى للرسائل الجامعية المصرية:

سعى مشروع المستودع الرقمى للرسائل الجامعية المصرية وفق ما جاء (باجتماع مديرى مشروع المستودع الرقمى بالجامعات المصرية ، ٢٠٠٩) إلى تحقيق مجموع من الأهداف هى:

١. توفير التجهيزات المادية والبرمجة اللازمة لتنفيذ المشروع.

٢. إعداد معيار لإتاحة النصوص الكاملة للرسائل الجامعية في صورة رقمية.
٣. أعداد قواعد لوصف المصادر الإلكترونية (الميتاداتا) وفقا للمعايير العالمية إلى جانب اعتماد أسلوب موحد لإعداد مستخلصات الرسائل الجامعية.
٤. الاتفاق على الجوانب الفنية المتعلقة بالإتاحة الإلكترونية مثل محدد الكيان الرقمي والعناوين المفتوحة.
٥. تجهيز الأدلة الإرشادية والمواد التدريبية التي ستعتمد عليها الجامعات في إتاحة كل المواد في صورة رقمية.
٦. فحص الرسائل المتاحة بصورة إلكترونية وإدخالها مباشرة علي النظام.
٧. إجراء عمليات المسح الضوئي للرسائل وفقا للمعايير والقواعد الخاصة بإتاحة المواد الإلكترونية والتي يتم الاتفاق عليها من حيث قوة الإظهار وشكل المادة النهائية.
٨. إجراء عمليات التعرف الضوئي على الحروف للرسائل المتاحة باللغة الإنجليزية.
٩. إعادة تجليد الرسائل التي تمت معالجتها.
١٠. إعداد الآليات والأدوات وأدلة العمل اللازمة لبناء وتجهيز الرسائل الجامعية الإلكترونية.

ونلاحظ أن التحويل الرقمى للرسائل كان موجها فى البداية ليتم بشكل مركزى على مستوى الجامعات المصرية الحكومية ، من خلال إنشاء مركز للمسح الضوئى بشبكة الجامعات المصرية ، ولكن الواقع ينفى ذلك حيث تم توزيع المشروع على الجامعات ليكون بكل جامعة إدارة لمشروع المستودع الرقمى للرسائل ، كما أن إدخال البيانات الببليوجرافية للرسائل ومستخلصاتها على النظام الآلى لإدارة المكتبات (Future Library System (FLS قد تم فى مرحلة سابقة على مشروع المستودع الرقمى حيث تم الانتهاء من إعداد فهارس للمكتبات المركزية بالجامعات المصرية.

٣/١/٣- متطلبات تنفيذ مشروع المستودع الرقمى للرسائل :

تطلب تنفيذ مشروع المستودع الرقمى للرسائل الجامعية كما جاء فى خطة نظم تطوير تكنولوجيا المعلومات توافر مجموعة من المقومات هى:

- التجهيزات المادية والبرمجية:.

تم تجهيز المستودع الرقمي بمجموعة من التجهيزات المادية والبرامجية تتضح من الجدول التالي :

جدول (٢) التجهيزات المادية والبرمجية للمستودع الرقمي

البند	التجهيزات	متوفر	غير متوفر
التجهيزات المادية	خوادم	√	
	أجهزة جدران نارية	√	
تجهيزات برمجية	برنامج ادارة محتوى رقمي	√	
	برامج حماية من الفيروسات	√	
	برامج جدران نارية firewall	√	

تم تجهيز المستودع الرقمي للرسائل الجامعية المصرية بمكونات مادية وبرمجية يمكن حصرها فيما يلي:

١- تم تخصيص عدد(٦) خوادم بالمجلس الأعلى للجامعات لتحميل الرسائل ولأغراض الإتاحة إلى جانب توفير إمكانيات التخزين الإحتياطى اللازمة للمحتوى الرقمي للمستودع من إجمالي عدد (١٨) خادم تخدم شبكة الجامعات المصرية.

٢- تم تخصيص عدد (٤) أجهزة جدران نارية (firewall hardware) لحماية المستودع الرقمي للرسائل الجامعية.

٣- تجهيز وحدة المكتبة الرقمية بالمجلس الأعلى للجامعات بالمعدات اللازمة للتحويل والمراقبة والفحص.

ويتضح من ذلك أن إدارة المشروع فى استراتيجيتها قد ركزت على المتطلبات المادية والتشريعية دون الخوض فى التفاصيل التنظيمية على مستوى المشروع فى كل جامعة من الجامعات بما يعطى وضع هذه التنظيمات للقائمين على المشروعات فى كل جامعة حسب ظروفها .

التجهيزات البرمجية

- تم توفير نظام لإدارة المحتوى الرقمي حيث تم الاعتماد علي نظام المستقبل لإدارة المكتبات (future library system)
- تم تخصيص عدد من برامج الحماية من الفيروسات لحماية المحتوى الرقمي للمستودع.
- تم تخصيص عدد من برامج جدران الحماية (firewall software).

ويتضح مما سبق ان إدارة المشروع قد وفرت كل التجهيزات البرمجية وذلك من أجل تحقيق أهداف المستودع الرقمي واتاحة المحتوى الرقمي للرسائل الجامعية المصرية وتجهيزها ببرامج حماية لتأمين هذا المحتوى.

٢/٣ الرسائل الجامعية التي تم رقمنتها بمشروع المستودع الرقمي للرسائل الجامعية

استطاع مشروع المستودع الرقمي للرسائل الجامعية المصرية من رقمنة الرسائل الجامعية التى أجازتها عدد (٢٤) جامعة حكومية مصرية من خلال تجهيز وحدة للنشر والتحويل الرقمي بالمكتبات المركزية للجامعات المصرية، وقد ساهمت كل جامعة في هذا المشروع الوطني بما لديها من رسائل علمية وفق الجدول التالي :

جدول رقم (٣) عدد الرسائل الرقمية المرفوعة علي نظام المستقبل بالجامعات المصرية*

م	الجامعة	عدد الرسائل التى تم تحميلها علي النظام الآلي	النسبة المئوية
١	جامعة عين شمس	59773	26.5
٢	جامعة المنصورة	25459	11.3
٣	جامعه الاسكندريه	25354	11.2
٤	جامعة بنها	20750	9.2
٥	جامعة طنطا	16827	7.4
٦	جامعة أسيوط	13319	5.9
٧	جامعة المنيا	13139	5.8
٨	جامعة المنوفية	10957	4.9
٩	جامعة القاهرة	8446	3.7
١٠	جامعة قناة السويس	6422	2.8
١١	جامعة الزقازيق	6284	2.8
١٢	جامعة بني سويف	4016	1.8
١٣	جامعة سوهاج	3503	1.6
١٤	جامعة حلوان	3272	1.4
١٥	جامعة الفيوم	2463	1.1

* تم الحصول علي هذه البيانات من تقارير النظام الفرعي " المستودع الرقمي " لنظام المستقبل لإدارة المكتبات بتاريخ ٢٠١٦/٧/١

م	الجامعة	عدد الرسائل التى تم تحميلها علي النظام الآلي	النسبة المئوية
١٦	جامعة كفر الشيخ	2055	0.9
١٧	جامعه جنوب الوادى	1210	0.5
١٨	جامعة بورسعيد	925	0.4
١٩	جامعة دمياط	657	0.3
٢٠	جامعة مدينة السادات	577	0.3
٢١	جامعة أسوان	174	0.1
٢٢	جامعة السويس	118	0.1
٢٣	جامعة دمنهور	113	0.1
٢٤	جامعة الازهر	69	0.03
	الاجمالي	225882	

يتضح من الجدول السابق أن مشروع المستودع الرقمي للرسائل الجامعية المصرية ساهم فيه كل الجامعات المصرية بما تملكه من رسائل علمية حيث بلغ عدد الجامعات المصرية المشاركة في المشروع (٢٤) جامعة بمجموع عدد (٢٢٥٨٨٢) رسائل تم رقمنتهم وتحميلهم ورفعهم علي النظام الآلي أي ما يقرب من ربع مليون رسالة وهو ما يعد ثروة علمية قومية يجب توسيع الإستفادة منه والمحافظة عليه من السرقة والتخريب وهو نتاج كل جهود المكتبات الجامعية حيث جاءت في المقدمة جامعة عين شمس بعدد (٥٩٧٧٣) رسالة علمية بنسبة (٢٦.٥%) ويعود ذلك أن جامعة عين شمس من اقدم الجامعات المصرية بالاضافة إلي صدور قرار أو توصيه تلزم الجامعات بأن تودع نسخة من كل رسالة يتم إجازتها بالمكتبة المركزية لجامعة

عين شمس. وجاء المرتبة الثانية جامعة المنصورة بعدد (٢٥٤٥٩) رسالة بنسبة (١١.٣%) ثم جاءت في المركز الثالث جامعة الاسكندرية بعدد رسائل (٢٥٣٥٤) رسالة بنسبة (١١.٢%)

٣/٣ قائمة الزيارت للمستودع الرقمي للرسائل حسب الدول

يعد المستودع الرقمي للرسائل الجامعية المصرية من المشاريع القومية التي تمت بنجاح وكان لها صدى علي المستوى العربي والدولي وهذا ما نلاحظه عند رصد الدول التى قامت بالبحث خلال المحتوى الرقمي للرسائل الجامعية المصرية حيث بلغت (٨٩) دولة بزيارات مختلفة طبقا لتقارير النظام الفرعي للمستودع الرقمي لنظام المستقبل لإدارة المكتبات إلا أن الباحث فضل رصد اعلي ثمان دول في الدخول علي المستودع الرقمي للرسائل الجامعية خلال عام ٢١٦ وتم رصدهم في الجدول التالي:

جدول رقم (٤) قائمة بزيارات الدول للمستودع الرقمي للرسائل الجامعية المصرية

م	الدولة	عدد الزيارات
1	مصر	1087896
2	الاتحاد الأوربي	30974
3	الولايات المتحدة	29298
4	السعودية	25298
5	رومانيا	15753
6	ليبيا	10603
7	الجزائر	8502
8	سوريا	5652
9	الكويت	5279
10	الإمارت	4697

يتضح من الجدول السابق أن دولة مصر العربية جاءت في المرتبة الاولي من حيث عدد الزيارات للمستودع الرقمي للرسائل الجامعية ويرجع ذلك إلي التسويق

والإعلان عن مخرجات المشروع في الدورات التدريبية التي تعقدها المكتبات الرقمية بالجامعة المصرية للتدريب علي استخدام قواعد البيانات العالمية، ثم جاء في المركز الثاني الاتحاد الأوربي وجاء في المركز الثالث دولة الولايات المتحدة الامريكية في الدخول علي المحتوى الرقمي للمستودع الرقمي للرسائل ويدل ذلك علي نجاح التجربة المصرية في رقمنة ونشر الرسائل العلمية علي شبكة الإنترنت والمتمثل في المستودع الرقمي للرسائل الجامعية المصرية

٣/٤ الأمن المادي والبيئى لمبنى المستودع الرقمي للرسائل الجامعية المصرية:

يعد أمن المبنى والبيئة المحيطة به من أساسيات تأمين الشبكات لذا تم تجديد مبنى المستودع الرقمي للرسائل الجامعية المصرية بمبنى شبكة الجامعات المصرية بالمجلس الإعلي للجامعات . في جامعة القاهرة في الدور الثاني علوى في عام ٢٠٠٩ لتحقيق معايير الأمن والسلامة .

٣/٤/١ الحماية العامة لمبنى المستودع الرقمي للرسائل الجامعية

يجب أن تتوافر بعض المعايير العامة لحماية مباني المستودعات الرقمية بما يحقق أهدافها وخدماتها واستمراريتها، والجدول التالي يوضح بنود حماية مبنى المستودع الرقمي للرسائل الجامعية:

جدول (٥) يوضح بنود حماية مبنى المستودع الرقمي الرسائل الجامعية المصرية

م	البند	نعم	لا
١	هل تم تخصيص غرف مغلقة لحفظ أجهزة خادم شبكة المستودع ؟	√	
٢	هل كل الكابلات ألياف ضوئية fiber optics؟	√	
٣	هل تمديد كابلات الشبكة في أماكن أمنة ومحمية وغير معرضة لوصول غير المختصين لها؟	√	
٤	هل كابلات الشبكة مغلفة ومحمية من العبث بها أو اتلافها؟	√	
٥	هل تم تأمين النوافذ والفتحات الموجودة في غرف الخوادم؟	√	
٦	هل تم تأمين الأبواب والمنافذ باستخدام أجهزة إنذار آلية تقوم بتشغيل أجراس للتنبيه في حالة دخول أشخاص للموقع في غير أوقات العمل؟	√	
٧	هل هناك أنظمة حماية (كاميرات مراقبة . أجهزة أنذار...) ؟	√	
	هل يتم صيانة الأجهزة بشكل سليم لضمان استمرارية عملها وسلامتها؟	√	

يتضح من الجدول السابق أنه تم تأمين مبنى المستودع الرقمي للرسائل الجامعية المصرية بشكل كامل عند تجديده حيث تم استبدال وتغيير كل كابلات الشبكة إلي كابلات ألياف ضوئية (fiber optics) ودفنها في الحوائط والأسقف المعلقة وتغليفها بالعوازل البلاستيك لحمايتها ولمنع التصنت عليها بالاضافة إلي تأمين مداخل ومخارج المستودع بأجهزة انذار وكاميرات مراقبة وبأحدث التقنيات من أجل توفير كل سبل الأمان والحماية للمبنى وتجهيزاته .

٢/٤/٣ حماية مبنى المستودع الرقمي ضد الحريق

مما لاشك فيه أن الحرائق من أكبر الأخطار التي تهدد المنشأت والمباني، وعدم إتخاذ تدابير صارمة للسيطرة عليه قد يؤدي إلى تخريب المنشأة بالكامل، والجدول التالي يوضح أساليب حماية المستودع الرقمي للرسائل الجامعية ضد الحريق.

جدول (٦) يوضح حماية المستودع الرقمية ضد الحريق

م	البند	نعم	لا
١	هل نوعية حساسات الحرارة مطابقة للمواد ومكان الأستخدام؟	√	
٢	هل المساحة بين حساسات الحرارة في حدود المسموع بها وكذا ارتفاع الحساس؟	√	
٣	هل نظم الإنذار من النوع المعتمد؟	√	
٤	هل لوحة الانذار مقسمة حسب المناطق للحريق؟	√	
٥	هل نوعية أجهزة الاطفاء اليدوية مناسبة لنوع الحرائق؟	√	
٦	هل مكان جهاز الاطفاء اليدوى ظاهر ويخدم المساحة المطلوبة؟	√	
٧	هل تم مراعاة العدد والمسافات البينية بين أجهزة الإطفاء اليدوية؟	√	
٨	هل الاثاث المستخدم والفرش مقاوم للاشتعال؟	√	

يتضح من الجدول السابق أنه :

١- تم تجهيز المستودع بطفايات حريق وأجهزة إنذار ضد الحريق وتم مراعاة المسافات البينية بين كل جهاز انذار وفق معايير الأمن والسلامة .

٢- يتم صيانة طفايات الحريق وأجهزة الانذار بشكل دوري ووفق جدول زمنى محدد.

٣- تم تأثيث مبنى المستودع وتجهيزاته بأثاث غير قابل للإشتعال.

٣- تم فرش المستودع بأنواع مقاومة للإشتعال.

٥- تم دفن كل الأسلاك المستخدمة في الحائط وتم عزلها جيدا.

٦- تم دهن مبنى المستودع بدهانات ومواد مقاومة للحريق.

٣/٤/٣ حماية المستودع الرقمي للرسائل ضد المياه :

يراعي حماية جميع المباني والمنشآت من الرطوبة والمياة التي تسبب ضررا بالغاً علي المباني والحوائط وبالتالي تؤثر علي العمر الافتراضي للمبنى لذا تم مراعاة

وحماية المستودع ضد الرضوبة والمياة عند تجديد المبنى ويتضح ذلك في الجدول التالي:

جدول (٧) حماية المستودع الرقمية ضد الرطوبة والمياة

م	البند	نعم	لا
١	هل تم عزل الأساسات ضد المياه الجوفية أو مياة الصرف أو الكيماويات الموجودة في التربة أو مياه الأمطار؟	√	
٢	هل تم عزل الحمامات بمواد تمنع تسرب المياة إلي المباني؟	√	
٣	هل تم عزل الأسطح ضد الرطوبة ومياه الأمطار؟	√	
٤	هل تم عزل الحوائط القريبة من منسوب المياه الجوفية؟	√	

يراعي حماية جميع المنشآت وعزل مبانيها عزلا تاما ضد الرطوبة والمطر والمياة الجوفية والسطحية ورشحهما التي تضر بالمباني وتتلف عناصر موادها الإنشائية والبنائية ومن ثم تؤثر علي عمر المبنى الإفتراضي لذا تم مراعاة هذه المعايير في تجديد وتصميم مبنى المستودع الرقمي للرسائل الجامعية الذي يقع بشبكة الجامعات المصرية بمنى المجلس الاعلي للجامعات بجامعة القاهرة، حيث تم عزل الأساسات والاسطح وأرضية الحمامات بمواد عازلة تمنع تسريب المياة.

٣/٤/٥ حماية الخدمات الأساسية

إن توفير وتأمين الطاقة الكهربية أمراً ضرورياً لإستمرار عمل الشبكات وحماية البيانات والمعلومات من الفقدان، ويتم ذلك عن طريق مصادر طاقة دائمة مباشرة أو بديلة، والجدول التالي يوضح مدى تأمين الطاقة الكهربية للمستودع الرقمي للرسائل الجامعية المصرية :

جدول (٨) توفير مصادر الطاقة للمستودع الرقمي

م	البند	نعم	لا
١	هل يتوفر مصدر طاقة دائمة مباشرة online power supplies؟	√	
٢	هل يتوفر مصدر الطاقة الدائمة البديل switched power supplies؟	√	

يلاحظ من الجدول السابق أنه تم توفير مصادر طاقة كهربية للمستودع الرقمي بديلة في حال توقف مصادر الطاقة الدائمه والمباشرة وذلك عن طريق مزود الطاقة الكهربائي الاحتياطي Uninterruptible Power Supply لحماية الخوادم والأجهزة من أي تذبذب في الطاقة الكهربية سواء من إنخفاض جهد التيار المفاجئ أو ارتفاعه المفاجيء، الذي يمكن أن يؤثر بالسلب علي خوادم المستودع ومن ناحية أخرى فقد تم تجهيز المستودع الرقمي بأجهزة تكييف للحفاظ علي درجة حرارة غرفة المستودع الرقمي خاصة في فصل الصيف للحفاظ علي أجهزة الحاسب الآلي.

٥/٣ أمن الموارد البشرية :

قد يمثل العامل البشري تهديدا لشبكة المعلومات سواء كان بقصد أو بغير قصد، لذا وجب تحديد صلاحيات الموظفين والمستفيدين منعا لأي تهديد أو اختراق من قبل العاملين أوالمستفيدين من خلال ضبط الوصول إلي المستودع الرقمي للرسائل الجامعية المصرية :

١/٥/٣ صلاحيات الموظفين:

يمكن تصنيف الأشخاص الذين يتعاملوا مع المستودع الرقمي للرسائل الجامعية إلي موظفين ومستخدمين، والجدول التالي يوضح صلاحيات موظفي مع المستودع الرقمي:

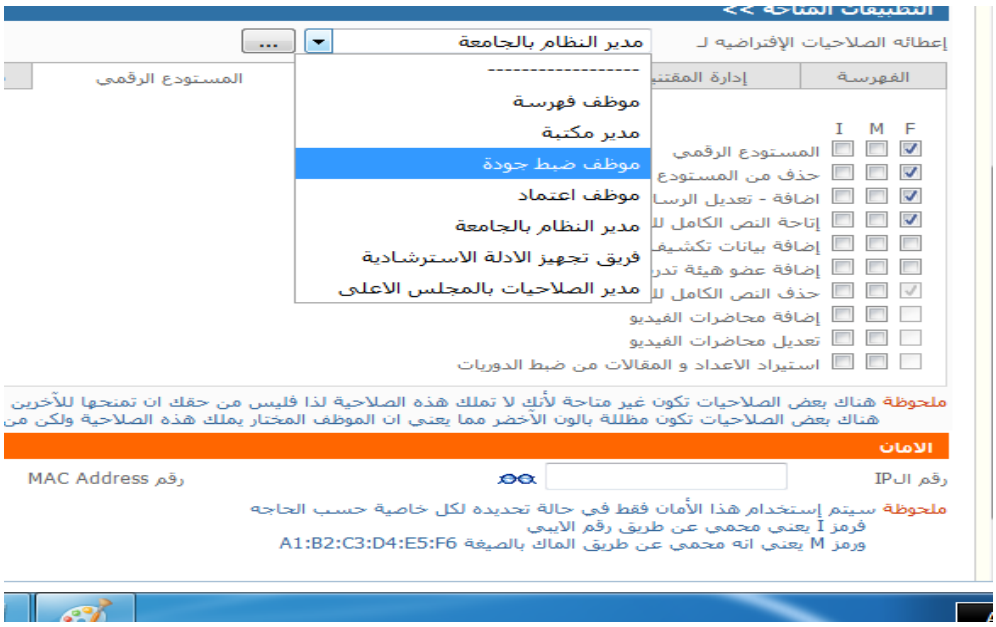
جدول(٩) يوضح صلاحيات الموظفين بالمستودع الرقمي للرسائل الجامعية المصرية

م	البند	نعم	لا
١	هل يسمح النظام بتحديد كلمات المور للموظفين وفق صلاحياتهم؟	√	
٢	هل يقوم النظام بتحديد نوعية كلمات السر حتى تتسم بالقوة وعدم الاختراق؟		×
٣	هل تم تدريب الموظفين علي كيفية استخدام النظام ؟	√	
٤	هل يقوم النظام بحذف الموظفين المنتهية مدة صلاحياتهم؟	√	

يتضح مما سبق أن تم تحديد مجموعة من الصلاحيات لموظفي المستودع الرقمي بما يتفق مع عملهم ونشاطهم، حيث يتيح المستودع الرقمي للرسائل إنشاء حسابات للموظفين العاملين علي النظام وتحديد صلاحيات كل منهم حسب نشاطه داخل المكتبة ووضع إجراءات صارمة لكل موظف من أجل الحفاظ علي أسم الدخول وكلمة السر منها :.

١- عدم إفشاء اسم الدخول وكلمة السر الخاصة به لأي شخص.
٢- تغيير كلمات المرور كل فترة زمنية .
٣- تحديد صلاحيات الموظفين بدقة شديدة
٤- مراقبة نشاط كل موظف من عمليات الإدخال والحذف
٥- عدم وضع أي فلاشات (usb) بأجهزة المستودع الرقمي للرسائل الجامعية المصرية .
٦- تجميد نشاط الموظفين المخالفين لهذه الإجراءات

والشكل التالي يوضح مستويات صلاحيات العاملين علي نظام المستودع الرقمي وتحديد صلاحيات كل وظيفة محددة بالاضافة إلي ربط هذه الصلاحيات بمستويات أمان محددة .



شكل (١) يوضح صلاحيات الموظفين علي المستودع الرقمي

يمكن ولوج الموظفون إلي المستودع الرقمي للرسائل الجامعية بثلاثة مستويات أمان حيث يمكن تحديد وضبط صلاحيات الدخول إلي المستودع الرقمي للرسائل الجامعية وهي كما يلي:

١- المستوى الأول عن طريق اسم المستخدم وكلمة السر ويرمز له بالرمز (F) ويمكن تغيير كلمة السر كل فترة، أما اسم المستخدم فهو ثابت لا يمكن تغييره، ويمكن تخصيص كلمات المرور بحيث تضم حروفا وأرقاما ورموزاً ولكن النظام لا يشترط ذلك أن كان ذلك يعد نقطة ضعف في النظام يراعي تعديلها.

٢- المستوى الثاني عن طريق ربط اسم المستخدم وكلمة السر برقم الحاسب الآلي علي شبكة الانترنت Internet protocol (IP). ويرمز له بالرمز (I) وعند تحديد هذا الخيار لا يمكن الدخول علي النظام إلا من خلال اسم المستخدم ورقم (IP) الحاسب الآلي.

٣- المستوى الثالث عن طريق ربط اسم المستخدم وكلمة السر برقم Mac Address لجهاز الحاسب الآلي (Media Access Control Address) وتعني عنوان التحكم بالوصول إلى الوسائط في مختلف أنظمة تشغيل الكمبيوتر وهو رقم فريد وخاص بكل جهاز ومسؤول عن التعريف على الشبكة، صُمّم خصيصًا لكافة بطاقات الشبكة.

إلا أنه يعاب علي النظام أنه لا يحدد نوعية كلمات المرور للموظفين كاستخدام الحروف والأرقام والرموز كشرط أساسي لتسجيل كلمات مرور قوية لذا وجب تعديل ذلك بحيث لا يتم تسجيل كلمات المرور للموظفين إلا اذا اشتملت علي حروف وأرقام ورموز حيث تعد ذلك نقطة ضعف في النظام .

٢/٥/٣ المستفيدون :.

يتيح نظام النظام الآلي بإنشاء حسابات للمستفيدين وتحديد صلاحيات كل منهم بغرض حماية المحتوى الرقمي من السلوك المخالف للمستفيدين كما يتضح من الجدول التالي :.

جدول(١٠) صلاحيات المستفيدين من المستودع الرقمي للرسائل الجامعية المصرية

م	البند	نعم	لا
١	هل يقوم النظام بتحديد كلمات المرور للمستفيدين وتحديد صلاحياتهم	√	
٢	هل يقوم النظام بتحديد نوعية كلمات السر للمستفيدين لتتسم بالقوة وعدم الاختراق		×
٣	هل يقوم النظام بحذف المستفيدين المنتهيين صلاحياتهم	√	
٤	هل يتم مراجعة صلاحيات المستفيدين كل فترة زمنية	√	
٥	هل يتم متابعة مستمرة لنشاط المستخدمين علي النظام	√	
٦	هل تم تدريب المستفيدين علي كيفية استخدام المحتوى الرقمي للرسائل الجامعية	√	
٧	هل يتم وضع علامات مائية تحفظ حقوق الملكية الفكرية للمستودع		×

يتضح من الجدول السابق أن صلاحيات المستفيدين تم تحديدها وفق القواعد التالية :

١- عدم إعطاء اسم المستخدم وكلمة المرور لأي مستفيد أخر

٢- مراجعة صلاحيات المستفيدين كل فترة زمنية

٣- المتابعة المستمرة لنشاط المستخدمين علي النظام

٤- تدريب المستفيدين علي كيفية استخدام المحتوى الرقمي للرسائل الجامعية ضمن الدورات التدريبية السنوية الذي تعقدها وحدة المكتبة الرقمية بالمجلس الأعلي للجامعات بالجامعات المصرية ضمن برنامجها التدريبي علي استخدام بنك المعرفة المصري وقواعد البيانات.

والشكل التالي يوضح شاشة تسجيل المستفيدين بالنظام وتحديد صلاحياتهم

شكل رقم (٢) يوضح صلاحيات المستفيدين من المستودع الرقمي

٦/٣ إدارة أمن البيانات:

يعد أمن البيانات والمعلومات من أهم مسؤليات المستودع الرقمي ويتم ذلك وفق معايير وأدوات واجراءات مخصصة لتلك الحماية ، وذلك من خلال عدة مهام كتشفير

البيانات ومكافحة الفيروسات وإغلاق الثغرات الأمنية ومتابعتها.

١/٦/٣ تشفير بيانات

مع انتشار الإنترنت بشكلٍ كبير ليصبح في متناول الجميع لدرجة الاعتماد عليه في أقل تفاصيل حياتنا اليومية، برزت الحاجة بصفة عامة لاستخدام تقنيات حماية هذه البيانات كتشفيرهذة البيانات واخفائها وبصفة خاصة بيانات المستودعات والشبكات والجدول التالي يوضح بنود تشفير البيانات

جدول(١١) تشفير البيانات بالمستودع الرقمي

م	البند	نعم	لا
١	هل يتم استخدام تقنية تشفير البيانات؟	√	
٢	هل يتم استخدام تقنية اخفاء البيانات؟	√	
٣	هل توجد برامج حماية لتتبع الإختراق والتسلل؟	√	

يتضح مما سبق أن نظام أدارة المحتوى للمستودع الرقمي يستخدم تقنية تشفير البيانات في نقل البيانات من وإلي المستودع الرقمي للرسائل الجامعية بحيث لا يمكن الوصول إلي المحتوى الرقمي من خلال التصنت علي كابلات الشبكة مما يشكل حاجز أمان يحمى الحقوق المادية والفكرية للمحتوى الرقمي للرسائل الجامعية المصرية خاصة وأن نظام المستودع الرقمي يعمل بالكامل على الشبكة الدولية للمعلومات Fully Web based system

٢/٦/٣ استخدام الحوائط النارية firewall للمستودع الرقمي :

في إطار حماية المستودع الرقمي للرسائل الجامعية المصرية فقد تم التعاون بين شبكة الجامعات المصرية ووحدة تطوير التعليم العالي مع شركة (IBM)؛ لتركيب وتشغيل أجهزة أمن شبكات حديثة مجانية مقدمة من قبل الشركة للجامعات

الحكومية الحديثة، حيث تم تزويد شبكة الجامعات المصرية بعدد (٣) أجهزة جدران نارية firewall hardware بالإضافة أيضا إلي برامج جدران نارية firewall software وهذه البرامج تستخدم تقنية IBM Internet Security ((IBM ISS Systems كجدران حماية لأنظمة تشغيل لينكس سيرفر linux servers وحماية IPS للأجهزة وحظر حركة مرور الشبكة غير المرغوب فيها وكشف ومنع وقوع هجمات الشبكة الخبيثة، ويتم التحكم في هذه الاجهزة والبرامج من خلال وحدة تحكم مركزية للتحكم في مرور البيانات بشبكة الجامعات المصرية إلا أن الباحث لم يستطع الحصول علي نوع الأجهزة أو البرامج من المبرمجين خوفا منهم من أي اختراقات.

٣/٦/٣ حماية المستودع الرقمي ضد الفيروسات :

تعد الفيروسات والبرامج الخبيثة من أكثر أنواع التهديدات لأنظمة الحاسب حيث تستغل نقاط الضعف في أنظمة الحاسب ومنذ ظهور الفيروسات والصراع مستمر بين مطوري الشبكات والهجمات الفيروسية التي تسبب ضررا بالغا بنظم التشغيل وتخريب البيانات، والجدول التالي يوضح حماية المستودع الرقمي من الفيروسات:

جدول (١٢) بنود حماية المستودع الرقمي ضد الفيروسات

م	البند	نعم	لا
١	هل يتم الاعتماد علي أنظمة تشغيل أقل تأثرا بالفيروسات يونكس، لينكس؟	√	
٢	هل يتم توفير برنامج للتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة؟	√	
٣	هل يتم توفير برامج حماية من الفيروسات؟	√	

سعى مسئولو المستودع الرقمي للرسائل الجامعية المصرية نحو توفير برامج حماية للسيرفرات ضد الفيروسات التى تتسبب في إضرار كبيرة للأجهزة والملفات وتصيب الأجهزة بالعطل حيث قد تم التعاقد علي تركيب برنامج حماية من الفيروسات

endpoint protection وهي حزمة كاملة من شركة symantec وهي شركة عالمية متخصصة في برامج الكمبيوتر خاصة برامج حماية وأمن الشبكات بهدف الحماية ضد الفيروسات وملفات التجسس والهاكر

وطبقا لكراسة المواصفات الفنية للمناقصة العامة رقم G/NCB/ICTP/2010/٧٥ لمشروع تطوير البنية الأساسية لشبكة الجامعات المصرية٢٠١٠ والخاصة بتوفير التجهيزات الأمنية لشبكة الجامعات المصرية وكانت تمثل البنود التالية :.

١- الإدارة الموحدة للتهديدات (Complete Unified Threat (UTM management هو الحل الشامل الذي برز مؤخرا في الشبكة الأمنية منذ عام ٢٠٠٤ ، وزادت أهميته علي نطاق واسع كحل لتأمين الشبكة الرئيسية والناحية النظرية، وهي تمثل :.

- جدار الحماية التقليدية وجميع المنتجات الأمنية التي لديها القدرة على أداء المهام الأمنية المتعددة لأجهزة جدران الحماية firewalling.
- وأجهزة منع التسلل ومكافحة الفيروسات (anti-virus).
- وأجهزة مراقبة المحتوى.
- وأجهزة مكافحة البريد المزعج.
- والشبكة الافتراضية الخاصة (A virtual private network (VPN هو آلية لتوفير بيئة آمنة وموثوق بها للنقل عبر الإنترنت. ويستخدم VPN لمنع الوصول غير المصرح به للمستخدمين، وتستخدم تقنية التشفير لمنع المستخدمين غير المصرح به من قراءة الحزم شبكة. يمكن استخدام VPN لإرسال أي نوع من أنواع بيانات من خلال الشبكة بشكل آمن، بما في ذلك الفيديو والصوت أو البيانات.

٤/٦/٣ النسخ الاحتياطي

النسخ الاحتياطي هو اجراء نسخة من الملفات الرقمية المهمة سواء كانت ملفات

العمل أوالملفات الشخصية أو ملفات نظام التشغيل وغيرها من الملفات بغرض حفظها من الضياع أو فقدان الملفات الاصلية واسترجاعا عند الحاجة لها لأي سبب والجدول التالي يوضح خطوات النسخ الإحتياطي للمستودع الرقمي للرسائل الجامعية .

جدول (١٣) بنود النسخ الاحتياطي للمستودع الرقمي للرسائل الجامعية

م	البند	نعم	لا
١	هل يتم نسخ احتياطي لكل بيانات النظام الفرعي للمستودع الرقمي؟	√	
٢	هل يتم النسخ علي فترات منتظمة وفقا ما يلائم العمل؟	√	
٣	هل يتم مراجعة هذه النسخ الاحتياطية بصورة منتظمه للتأكد من فعاليه وسلامته؟	√	
٤	هل يتم النسخ الاحتياطي الكامل؟	√	
٥	هل يتم النسخ الاحتياطي التراكمي أو التزايدي؟	√	
٦	هل يتم النسخ الاحتياطي التباينى أوالتفاضلي؟	√	

يحتفظ مسئولو المستودع الرقمي للرسائل الجامعية بنسخ احتياطية من ملفات المستخدم وملفات قواعد البيانات والمحتوى الرقمي للمستودع، ويتم النسخ الإحتياطي كل أسبوع نسخا كاملا full backup للملفات الخاصة بالمستخدمين وحقوقهم وكلمات المرور الخاصة بهم وقواعد البيانات والمحتوى الرقمي لمستودع الرسائل الجامعية المصرية ويتم حفظ هذه النسخ الاحتياطية علي أقراص صلبة وشرائط ممغنطة حتى وصل عدد هذه النسخ الاحتياطية التي يحتفظ بها المسئولين عن المستودع الرقمي للرسائل إلي (١٠٠) نسخة احتياطية حتى الآن ويتم حفظ هذه النسخ الاحتياطية بوحدة المكتبة الرقمية بشبكة الجامعات المصرية حتى يتمكن مسئولي المستودع من الرجوع إليها في حال فقدانها

نتائج الدراسة :.

توصلت الدراسة من خلال الرصد والوصف والتحليل إلى مجموعة من النتائج المتصلة بأمن وحماية المحتوى الرقمي لمشروع المستودع الرقمى للرسائل الجامعية المصرية وهي:

١- بناء المستودعات الرقمية للمحتوى الرقمي يحتاج إلي خطط ودراسات لنجاح عملية الرقمنة .

٢- وحدة المكتبة الرقمية بالمجلس الاعلي للجامعات هي الجهة المسئولة عن التخطيط وإدارة المستودع الرقمي للرسائل الجامعية المصرية.

٣- نظام المستقبل لإدارة المكتبات هو النظام المستخدم لإدارة المحتوى الرقمي للرسائل الجامعية المصرية .

٤- تم تأمين مبنى المستودع الرقمي للرسائل الجامعة المصرية بشبكة الجامعات المصرية من الناحية المادية بإتباع إجراءات عديدة خاصة بالمكان

٥- تم توفير أجهز الإمداد بالطاقة ups للمستودع الرقمي بشبكة الجامعات المصرية في حالة انقطاع التيار الكهربائي .

٦- تم توفير أجهزة تكييف للمستودع الرقمي بشبكة الجامعات المصرية لحماية الأجهزة من ارتفاع درجة الحرارة .

٧- تم تأمين نظام المستقبل لإدارة المكتبات عن طريق ثلاثة مستويات أمان .

٨- يتم استخدام أجهزة الجدران النارية firewall hardware وبرامج الجدران النارية firewall software

٩- يتم استخدام تقنية تشفير البيانات لنقل البيانات بشبكة المستودع الرقمي للرسائل الجامعية المصرية .

١٠- يتم استخدام برامج حماية ضد الفيروسات (endpoint protection) لحماية المستودع الرقمي من كل أنواع الفيروسات.

١١- يتم استخدام تقنية الإدارة الموحدة للتهديدات لحماية المستودع الرقمي للرسائل الجامعية المصرية.

١٢- يتم تحديد صلاحيات الموظفين والمستفيدين من النظام الفرعي لإدارة المحتوى الرقمي كإجراء حماية للمحتوى الرقمي للرسائل الجامعية المصرية.

١٣- يتم النسخ الاحتياطي لكافة الملفات وقاعدة البيانات وأسماء الدخول وكلمات المرور للمستودع الرقمي للرسائل الجامعية المصرية أسبوعيا لاستدعائها عند الحاجة ويتم حفظ النسخ علي أقراص صلبة وممغنطة بشبكة الجامعات المصرية.

١٤- يتم معالجة المحتوى الرقمي للرسائل الجامعية علي نظام المستقبل لإدارة المكتبات قبل الاتاحة .

توصيات الدراسة :.

في إطار ما توصلت إليه الدراسة من نتائج يمكن تحديد مجموعة من التوصيات وهي :.

١-ضرورة إعداد سياسات مكتوبة لإجراءات أمن وحماية المستودع الرقمي للرسائل الجامعية المصرية علي أن يتم الالتزام بها بشكل كامل.

٢-ضرورة زيادة عدد أجهزة الخوادم المخصصة للمستودع الرقمي للرسائل الجامعية المصرية في ظل زيادة أعداد المحتوى الرقمي للرسائل الجامعية المصرية

٣-أن يكون هناك نوع من أشكال التعاون والتنسيق بين المسئولين عن امن المعلومات بشبكة الجامعات المصرية .

٤-أن يكون هناك دائما مراجعة لسياسات أمن المعلومات كل فترة

٥-ان يكون هناك تقارير عن امن المعلومات بالمستودع الرقمي للرسائل الجامعية المصرية

٦-تدريب العاملين عن أهداف وسياسات أمن المعلومات بالمستودع الرقمي للرسائل الجامعية المصرية.

قائمة المصادر

أبو السعود، سيد مصطفى(٢٠٠٠) .كيف تصبح مديرًا لشبكة الكمبيوتر .- القاهرة : دار الكتب العلمية.

بامفلح، فاتن سعيد (٢٠٠١). حماية أمن المعلومات بشبكة المكتبات بجامعة ام القرى : دراسة حالة.. المؤتمر الثاني عشر للاتحاد العربي للمكتبات والمعلومات (اعلم). ٤-٨ نوفمبر.

توماس إتش، تير. بث كريمر . ترجمة حشمت قاسم (٢٠٠٣) . الحفظ التاريخى طويل المدى للرسائل الجامعية الالكترونية. دراسات عربية فى المكتبات وعلم المعلومات.- ٨،١يناير .

جامعة المنصورة . مركز تقنية المعلومات والاتصالات . نظام المستقبل لإدارة المكتبات.

[٢٠١١/٧/١٤] متاح

في : >http://www.eulc.edu.eg/news/index_files/frame.htm [<.

حافظ ، سرفيناز احمد محمد (٢٠١٠).المستودعات الرقمية للرسائل الجامعية العربية : دراسة تقويمية. المؤتمر الحادي والعشرين للاتحاد العربي للمكتبات والمعلومات (اعلم) . المكتبة الرقمية العربية (٦-٨ اكتوبر)

حسنين، رجب عبدالحميد. (٢٠١٢). أمن شبكات المعلومات الإلكترونية: المخاطر والحلول. *Cybrarians Journal: البوابة العربية للمكتبات والمعلومات، ٣٠* .

حشمت قاسم (٢٠٠٥) .المكتبات الوطنية وتضافر الجهود العربية لمواجهة تحديدات التراث الإلكترونى. مجلة مكتبة الملك فهد الوطنية . ٢،١١.

داود، حسن طاهر (٢٠٠٠). الحاسب وأمن المعلومات . الرياض : معهد الإدارة العامة.

سالم، باشيوة (٢٠٠٩). الرقمنة في المكتبات الجامعية الجزائرية دراسة حالة المكتبة الجامعية المركزية "بن يوسف بن خدة" .- 21 -.Cybrarians Journal، -. (2009) >>1/2/2010.- مسترجع من:
http://www.journal.cybrarians.info/index.php?option=com_content&view=article&id=132:----------q---q---&catid=62:2010-06-30-13-37-<54&Itemid=62

الشامي ، أحمد محمد ، وحسب الله، سيد . (١٩٨٨. (*المعجم الموسوعي لمصطلحات المعلومات والمكتبات*. الرياض: دار المريخ

صالح بن محمد المسند (٢٠٠٣) . جبريل بن حسن عريشي . نحو مكتبة رقمية للرسائل الجامعية المجازة من الجامعات والكليات السعودية . فى: السجل العلمى لندوة المكتبة الرقمية: الواقع وتطلعات المستقبل .– الرياض : مكتبة الملك عبد العزيز العامة. متاح على http://www.spl.org.sa

الصوفي، عبد اللطيف (٢٠٠٣). المكتبات في مجتمع المعلومات، دار الهدى للنشر والتوزيع،.ص.٢٢

طه، دجان بشير وعبد الرحيم ، فرقد حامد(٢٠٠٧) . حماية حقوق الملكية للوثائق النصية . مجلة الرافدين لعلوم الحاسبات والرياضيات ، ٢ ،٨٧.

عبد الحميد بسيوني(٢٠٠٣). الحماية من أخطار الإنترنت . القاهرة : دار الكتب العلمية للنشر والتوزيع .

العربي، أحمد عبادة. (٢٠١٥). معيار المنظمة الدولية للتوحيد القياسي آيزو ٢٧٠٠٢ لسياسات أمن المعلومات: دراسة وصفية تحليلية لمواقع الجامعات العربية. *مجلة جامعة طيبة للآداب والعلوم الإنسانية: جامعة طيبة – كلية الآداب والعلوم الإنسانية، ٤، ٧*

عمر، معاوية مصطفى محمد. (٢٠١٥). أهمية أمن المعلومات في مكافحة الجرائم الإلكترونية: دراسة حالة المركز السوداني لامن المعلومات. *مجلة جامعة بحري للآداب والعلوم الإنسانية: جامعة بحري، ٤، ٧ .*

العميري، منال بنت حمدان بن سعيد (٢٠١٦) . *واقع ممارسات أمن المعلومات في المكتبة الرئيسية بجامعة السلطان قابوس ومدى توافقها مع المعيار الدولي لأمن المعلومات (ISO/IEC 27002): دراسة حالة . (اطروحة ماجستير)* . جامعة السلطان قابوس. كلية الآداب والعلوم الإجتماعية . قسم دراسات المعلومات.

غبيق، صلاح الهادي. (٢٠١٣). التشفير وفك التشفير. *مجلة العلوم الاقتصادية والسياسية: الجامعة الأسمرية الإسلامية – كلية الاقتصاد والتجارة، ع٢* ، ٥٠٨ – ٥٤٣. مسترجع من http://search.mandumah.com/Record/765466

فراج، عبد الرحمن (٢٠٠٧). مصادر الوصول الحر فى مجال المكتبات وعلم الملعومات : دليل إرشادى . المعلوماتية. ٢٠ (ديسمبر).ص ص ٤٦-٤٩.متاح أيضا على http://arab-librarians.blogspot.com/2007/11/blog- post_3888.html[accessed [29/1/2008

فردي، لخضر (٢٠٠٨). رقمنه الرسائل الجامعية لتعظيم الاستفادة منها وترقيتها فى الجامعات العربية . العربية ٣٠٠٠، ٨،٣١، (ابريل) .

فؤاد، بن ضيف الله (٢٠١٠). أمن المعلومات أحد السبل لحماية الملكية الفكرية.- cybrarians journal .- 24 (ديسمبر) .- <٢٠١١/٧/١> .- متاح في : http://www.cybrarians.info/journal/no9/info-secuirty.htm

قاسم، عاطف السيد (٢٠٠٦). حفظ وصيانة المعلومات الالكترونية فى المكتبات المصرية : دراسة تحليلية للمفاهيم والمعايير والتطبيقات. (أطروحة دكتوراه) . جامعة المنوفية . كلية الآداب . قسم المكتبات والمعلومات .

قاسم، عاطف السيد (٢٠٠٩). حفظ المعرفة فى العالم الرقمى : مستقبل المكتبات والمعلومات والإنترنت . الإسكندرية : دار الثقافة العلمية ، ٢٠٠٩.

القحطاني، محمد عبد الله علي والغثبر، خالد بن سليمان (٢٠٠٩). أمن المعلومات بلغة ميسرة.. ط١.. الرياض : مركز التميز لأمن المعلومات .

محمد محمد الهادي (٢٠٠٦). توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية .- cybrarians journal .- 9 (يونيو) .- <٢٠١٥/٧/١> .- متاح في : http://www.cybrarians.info/journal/no9/info-secuirty.htm

مشيرة أحمد صالح محمد(٢٠٠٧). أساليب حماية وأمن المعلومات في النظم الآلية والشبكات في المكتبات ومراكز المعلومات بالقاهرة الكبرى . اطروحة ماجستير . القاهرة : جامعة عين شمس . كلية الاداب. قسم المكتبات والمعلومات.

معمر، جميلة (٢٠١٠). نحو رقمنة الرسائل الجامعية في المكتبة المركزية في جامعة قسطنطينية- الجزائر .أعمال المؤتمر الحادى والعشرين للاتحاد العربى للمكتبات والمعلومات (أعلم).المكتبة الرقمية العربية عربيا : الضرورة، الفرص والتحديات. لبنان. اكتوبر، ٦-٨.

النقيب، متولى محمود النقيب (٢٠٠٥). تقنيات التخزين الالكتروني أساس إدارة المحتوى الرقمى للمكتبات. بحث مقدم إلى مؤتمر الاستثمار فى بنية المعلومات والمعرفة تحت رعاية المنظمة العربية للتنمية الإدارية فى الفترة من ٢٨-٣١ أغسطس.. الإسكندرية .

النقيب، متولي محمود أحمد. (٢٠١٠). التحديات الأمنية لمشاريع الرقمنة بمؤسسات المعلومات العربية. *مجلة بحوث في علم المكتبات والمعلومات: جامعة القاهرة – كلية الآداب – مركز بحوث نظم وخدمات المعلومات، ٥* .

هلال، رءوف عبد الحفيظ (٢٠٠٧) . الرسائل الجامعية العربية : التخطيط للإفادة منها. مجلة المكتبات والمعلومات العربية .٢٧، ٤، أكتوبر.

وحدة المكتبة الرقمية (٢٠٠٩) . مشروع المستودع الرقمى للرسائل بالجامعات المصرية . القاهرة :المجلس الأعلى للجامعات ..٢٠٠٩/٤/٢٤.

وزارة التعليم العالى (٢٠٠٩) . مشروع تطوير نظم وتكنولوجيا المعلومات في التعليم العالي (المرحلة الثانية). القاهرة : وزارة التعليم العالي. مسترجع من /http://www.ictp.org.eg/index.php/ar

اليوسفى، مشاعل عبد العزيز (٢٠١١) . برامج استعادة النظام وبرامج النسخ الاحتياطي ودورها في حماية البيانات الرقمية . <١/٧/٢٠١١ > .- متاح في : http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/44-physical-security/1218-recovery-system-and-backup-software-and-its-role-in-the-protection-of-digital-data.html

Crespo Nogueira, C. (Ed.)(2010), Committee on Conservation and Restoration & International Council on Archives *Glossary of Basic Archival and Library Conservation Terms. English with Equivalents in Spanish, German, Italian, French and Russian*. Berlin, Boston: De Gruyter Saur. Retrieved 4 Feb. 2016, from https://www.degruyter.com/view/product/161505

damodhar,p .(2002) developing digital university libraries in india . hyderabad: inflibnet centre,2002. Retreived 22 april 2016, from https://ir.inflibnet.ac.in/handle/1944/44

Kumar, A. (2014). *Unifying the conceptual levels of network security through the use of patterns* . Available from ProQuest Dissertations & Theses Global. . Retrieved from https://search.proquest.com/docview/1547945259?accountid=178282

Satyanarayana , K V and Babu, B Ramesh (2008). Trends in the development of E-Theses in India: issues, constraints,and solutions. Retrieved 20 mar.2016, form http://coeia.edu.sa/index.php/ar/asuurance-awarness/articles/44-physical-security/1218-recovery-system-and-backup-software-and-its-role-in-the-protection-of-digital-data.html

Reitz, JM (2007). *ODLIS: Online dictionary for library and information science*, , 7 July 2016 . retrieved 15 oct. ,2016 ,form https://www.abc-clio.com/ODLIS/odlis_A.aspx

Security and protection Technology for digital repository contents to digital dissertations Egyptian

abstract

This study discusses techniques security and protection of digital repository for Thesis Egyptian university, which aims to provide the scientific content of the intellectual production of the Egyptian universities of Theses by building a digital repository for Thesis that are sanctioned by the Egyptian universities during the first decade of the twenty-first century that Include the provision of scientific digitization infrastructure include software components and material resources for the digitization of theses to the system for managing digital content output from the process of digitization.

And highlights the importance of the security of digital content for the repository in the light of the increasing threats and penetration sites by hackers in spite of all efforts by the IT companies but the preoccupation with security in the electronic environment is one of the primary concerns of the unity of the digital library Supreme Council of Universities to maintain the security of digital content for the repository The security of documents and digital content, especially on the vital artery of national economy-wide development of the necessary material equipment and software to maintain the digital content of the thesis and the Egyptian undergraduate study attempts to identify the security policies, both policies were a private physical logistics or equipment code Which sets out protection for warehouse and digital analysis of the risks that may arise as a result of lack of interest in the subject of security and protection of digital content for thesis undergraduate Egyptian adoption of prevention and defense-mail, so get out the results may illustrate the features of security and protection of the repository for digital dissertations Egyptian Channel, which is the definition of electronic communications for the university, which processed the Egyptian universities to the national and international level in addition to expanding access the content of the biomass sources and made available globally, which helps to raise the value of the competitiveness of Egyptian universities.