جامعة غرداية

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

بالتعاون مع مخبر أبحاث البنية الرقمية والذكاء الاصطناعي وتطبيقاتهما في التحول الرقمي للقطاعات الاقتصادية.

وبالإشتراك مع فرقة بحث متطلبات تطبيق حوكمة الشركات والتدقيق المحاسبي في المؤسسات الإقتصادية الجزائرية بمخبر الدراسات التطبيقية في العلوم المالية.

وبالإشتراك مع النقابة الوطنية المستقلة لمستخدمي التعليم العالي - فرع غرداية، ينظمون:

الملتقى الوطني الأول (حضوري وعن بعد) حول: حوكمة مؤسسات التعليم العالي في ظل التحول الرقمي والتشريعات الحديثة.

مداخلة بعنوان:

التحول نحو الجامعة الرقمية-بين الحوكمة الرشيدة والمخاطر السيبرانية-

من إعداد الباحثين :

عبدي احمد، أستاذ محاضر، جامعة غرداية، رئيس تونسي
abdi.ahmed@univ-ghardaia.dz

تيسمسيلت، تيسمسيلت
tissemsilt.dz

الملخص:

يتناول هذا البحث التحول نحو الجامعة الرقمية ودوره في تعزيز الحوكمة الرشيدة من خلال تحسين الشفافية والمساءلة وجودة الخدمات. كما يبرز التحديات المرتبطة بالمخاطر السيبرانية مثل الاختراقات وتسريب البيانات. ويؤكد على أهمية الآليات القانونية والمؤسساتية والحلول التقنية في مواجهة هذه التهديدات. ويخلص إلى أن نجاح الجامعة الرقمية مرهون بتحقيق توازن بين الرقمنة والأمن السيبراني.

الكلمات المفتاحية: الجامعة الرقمية، الحوكمة الرشيدة ، الأمن السيبراني ، التحول الرقمي ، التعليم العالي.

Abstract:

This research examines the transition to a digital university and its role in promoting good governance by enhancing transparency, accountability, and service quality. It also highlights the challenges associated with cybersecurity risks such as breaches and data leaks. The research emphasizes the importance of legal and institutional mechanisms and technological solutions in addressing these threats. It concludes that the success of a digital university hinges on achieving a balance between digitalization and cybersecurity

Keywords Digital university, good governance, cybersecurity, digital transformation, higher education.

1.مقدمة:

يشهد العالم في العقود الأخيرة تحولات عميقة بفعل الثورة الرقمية، التي مست مختلف القطاعات الحيوية، وعلى رأسها قطاع التعليم العالي. فقد أصبحت الجامعة اليوم مطالبة بالانتقال من نموذجها التقليدي إلى نموذج رقمي متكامل يعتمد على تكنولوجيا المعلومات والاتصال في التدريس والبحث والتسيير. ويأتي هذا التحول في إطار السعي إلى تحسين جودة الخدمات الجامعية، وتعزيز الشفافية، وترسيخ مبادئ الحوكمة الرشيدة التي تقوم على الكفاءة والمساءلة والمشاركة.

غير أن هذا الانتقال نحو الجامعة الرقمية لا يخلو من تحديات معقدة، خاصة في ظل تصاعد المخاطر السيبرانية التي تهدد أمن المعلومات والبيانات الأكاديمية والإدارية، مما يفرض ضرورة تحقيق توازن دقيق بين تبني الرقمنة وتوفير بيئة رقمية آمنة. وعليه، فإن التحول الرقمي في الجامعة لم يعد مجرد خيار تقني، بل أصبح رهانًا استراتيجيًا يتطلب تأطيرًا قانونيًا ومؤسساتيًا فعالًا.

من هنا تبرز الحاجة إلى إبراز دور التحول الرقمي في تكريس الحوكمة الرشيدة داخل المؤسسات الجامعية ،من خلال الإشكالية التالية:

<u>إلى أي مدى يمكن للجامعة الرقمية أن تحقق متطلبات الحوكمة الرشيدة، في ظل التحديات والمخاطر السيبرانية التي قد تعيق فعالية هذا التحول؟</u>

وتتمثل فرضيات الدراسة فيمايلي:

-الجامعة الرقمية ليست مجرد مؤسسة تعليمية، بل محرك للتنمية الاقتصادية والاجتماعية،

-تشكل المخاطر السيبرانية (كالاختراق وتسريب البيانات) تهديدًا مباشرًا لفعالية الجامعة الرقمية.

-توجد علاقة طردية بين مستوى الأمن السيبراني ونجاح تطـبيق الحوكمـة الرشيدة في الجامعة الرقمية.

وتتجلى أهمية الموضوع العلمية في إثراء البحث الأكاديمي في مجال التحول الرقمي والحوكمة الجامعية،

والقانونية في تسليط الضوء على ضرورة تحديث التشريعات لمواكبة التحديات السيبرانية،و الامنية في تعزيز الوعي بالمخاطر الرقمية التي تهدد المؤسسات التعليمية.

إن الهدف مـن وراء هـذه الدراسـة هـو تحليـل مفهـوم الجامعـة الرقميـة وخصائصها،مع إبراز دور التحول الرقمي في تكريس الحوكمة الرشيدة داخل المؤسسات الجامعية، وتحديد أهم المخاطر السـيبرانية الـتي تواجـه البيئـة الجامعية الرقمية،لنقدم في أخر الورقة البحثية توصيات لتعزيز الإطار القانوني والتنظيمي في هذا المجال.

و اعتمدت الدراسة على المنهج الوصفي التحليلي: لتفسير مفاهيم الجامعة الرقمية والحوكمة الرشيدة،

والمنهج المقارن: من خلال الاستفادة من بعض التجارب الدولية في هذا المجال.

2.المبحث الأول: التحول نحو الجامعة الرقمية كمدخل لتكريس الحوكمة الرشيدة

نتناول في هذا المبحث مطلبين ، المطلب الأول نخصصه لدراسة الإطار المفاهيمي للجامعة الرقمية والحوكمة الرشيدة ، و في المطلب الثاني نتطرق لدور التحول الرقمي في تعزيز الحوكمة الجامعية .

1.2.المطلب الأول: الإطار المفاهيمي للجامعة الرقمية والحوكمة الرشيدة

الفرع الأول: مفهوم الجامعة الرقمية وخصائصها

أولاً: مفهوم الجامعة الرقمية

تُعد الجامعة الرقمية من أبرز تجليات التحول الرقمي في قطاع التعليم العالي، حيث تمثل نموذجًا حديثًا يعتمد على توظيف تكنولوجيا المعلومات والاتصال في مختلف وظائف الجامعة، سواء في التعليم أو البحث العلمي أو الإدارة. وقد ظهر هذا المفهوم نتيجة لتطور البيئة الرقمية العالمية، والحاجة إلى تحسين جودة التعليم وتوسيع فرص الوصول إليه.

وتُعرّف الجامعة الرقمية بأنها: *"مؤسسة تعليم عالٍ تعتمد على البنية التحتية الرقمية لتقديم خدماتها التعليمية والإدارية والبحثية، من خلال منصات إلكترونية وتطبيقات ذكية، بما يضمن التفاعل المستمر بين مختلف الفاعلين في العملية التعليمية"[1].

كما تُعرف أيضًا بأنها: *"نموذج تعليمي قائم على التعلم الإلكتروني والتعلم عن بعد، يستخدم الوسائط الرقمية لإنتاج المعرفة وتبادلها، ويعتمد على نظم معلومات متكاملة في التسيير[2]".

ومن خلال هذه التعاريف، يمكن استخلاص أن الجامعة الرقمية تقوم على ثلاثة أبعاد أساسية:

البعد التعليمي: من خلال التعليم الإلكتروني (E-learning) والتعليم المدمج.

البعد الإداري: عبر رقمنة الخدمات الجامعية (التسجيل، النتائج، التسيير).

البعد البحثي: باستخدام قواعد البيانات الرقمية والمنصات العلمية.

ثانياً: خصائص الجامعة الرقمية

تتميز الجامعة الرقمية بجملة من الخصائص التي تميزها عن الجامعة التقليدية، من أهمها:

1- الاعتماد على البنية التحتية الرقمية

2- التعلم الإلكتروني والتفاعلي

3- المرونة والانفتاح

4- الاعتماد على البيانات والذكاء الاصطناعي

5- تعزيز الشفافية والحوكمة

6- التكامل بين الوظائف الجامعية

7- الاعتماد على الأمن السيبراني

الفرع الثاني: مفهوم الحوكمة الرشيدة ومبادئها في التعليم العالي

---

[1] -عبد الكريم بن يحيى، *التعليم الرقمي في الجامعات العربية*، دار المسيرة، عمان، 2021، ص 45.

[2] -محمد عبد الفتاح، *تكنولوجيا التعليم والتحول الرقمي*، دار الفكر العربي، القاهرة، 2020، ص 88.

أولاً: مفهوم الحوكمة الرشيدة في التعليم العالي

تُعد الحوكمة الرشيدة من المفاهيم الحديثة التي برزت في إطار إصلاح الإدارة العمومية وتطوير أداء المؤسسات، بما فيها مؤسسات التعليم العالي. وهي تشير إلى مجموعة القواعد والآليات التي تنظّم كيفية اتخاذ القرار داخل المؤسسة، بما يضمن تحقيق الكفاءة والشفافية والمساءلة.

وتُعرّف الحوكمة الرشيدة بأنها: *"نظام من القواعد والإجراءات التي تُنظّم العلاقات بين مختلف الأطراف داخل المؤسسة، بهدف ضمان حسن التسيير وتحقيق الأهداف بكفاءة وفعالية"[3].

وفي سياق التعليم العالي، تُعرّف حوكمة الجامعات بأنها: *"مجموعة الأنظمة والإجراءات الرقابية والتنظيمية التي تعتمدها مؤسسات التعليم العالي لضمان تحقيق الجودة والشفافية في الأداء وتحقيق الأهداف الاستراتيجية[4]".

كما تشير الأدبيات إلى أن الحوكمة في الجامعات ليست مجرد إطار قانوني، بل هي ثقافة تنظيمية تشمل جميع الفاعلين (الإدارة، الأساتذة، الطلبة، المجتمع)، وتسهم في تحقيق التوازن داخل المؤسسة الجامعية[5].

ثانياً: مبادئ الحوكمة الرشيدة في التعليم العالي

ترتكز الحوكمة الرشيدة على مجموعة من المبادئ الأساسية التي تشكل إطارًا مرجعيًا لإدارة المؤسسات الجامعية، من أهمها:

1- مبدأ الشفافية
2- مبدأ المساءلة
3- مبدأ المشاركة
4- مبدأ الكفاءة والفعالية
5- مبدأ العدالة والمساواة
6- مبدأ سيادة القانون
7- مبدأ الاستجابة والفعالية المؤسسية

إحصائيات تقريبية من تقارير دولية :

الجامعات التي تعتمد أنظمة حوكمة حديثة تسجل تحسنًا في الأداء بنسبة تتراوح بين **20% و30%** مقارنة بالجامعات التقليدية.

أكثر من **60% من الجامعات العالمية** تعتمد نماذج حوكمة قائمة على المشاركة والشفافية.

تطبيق الحوكمة يرتبط بزيادة الثقة المجتمعية في الجامعات بنسبة تفوق **40%**.

(يمكن تعزيز هذه الإحصائيات لاحقًا بتقارير البنك الدولي أو اليونسكو في البحث الكامل)

رابعاً: العلاقة بين الحوكمة الرشيدة وجودة التعليم العالي

تُظهر الأدبيات الحديثة وجود علاقة وثيقة بين الحوكمة الرشيدة وجودة التعليم العالي، حيث:

تسهم الحوكمة في تحسين الأداء المؤسسي.

---

[3] -عبد القادر محمد، *الحوكمة في المؤسسات العمومية*، دار الجامعة الجديدة، 2020، ص 25.

[4] -منى عبد الله الحداد، *الحوكمة الرشيدة ودورها في ضمان جودة التعليم العالي*، جامعة النيلين، 2017

[5] -نفس المرجع، ص 12.

تعزز جودة البرامج التعليمية.
تدعم البحث العلمي والابتكار.
تضمن الاستجابة لمتطلبات التنمية وسوق العمل.

2.2.المطلب الثاني: دور التحول الرقمي في تعزيز الحوكمة الجامعية

الفرع الأول: الرقمنة كأداة للشفافية والمساءلة

أولاً: مفهوم الرقمنة ودورها في تعزيز الشفافية والمساءلة

وتُعرّف الرقمنة في المجال الجامعي بأنها: *"استخدام الأنظمة الرقمية والمنصات الإلكترونية لإدارة العمليات التعليمية والإدارية، بما يتيح تداول المعلومات بشكل سريع ودقيق وشفاف"[6].

وتكمن أهمية الرقمنة في كونها تخلق بيئة مؤسساتية قائمة على إتاحة المعلومات وتقليل الغموض الإداري، مما يعزز ثقة الفاعلين داخل الجامعة وخارجها.[7]

ثانياً: الرقمنة كآلية لتعزيز الشفافية في الجامعة تُمكّن الرقمنة من:

1- إتاحة المعلومات وسهولة الوصول إليها
2- تقليل البيروقراطية والفساد الإداري
3- تتبع العمليات الإدارية إلكترونياً
4- نشر البيانات المفتوحة (Open Data)

ثالثاً: الرقمنة كآلية لتعزيز المساءلة في الجامعة تمكّن الرقمنة الهيئات الرقابية من:

1- توثيق العمليات والقرارات
2- تقييم الأداء بشكل موضوعي
3- تعزيز الرقابة الداخلية والخارجية
4- إشراك الفاعلين في التقييم

رابعاً: تطبيقات الرقمنة في تعزيز الشفافية والمساءلة داخل الجامعة

من أبرز التطبيقات العملية:أنظمة التسجيل الإلكتروني ،ومنصات التعليم الإلكتروني ، وأنظمة إدارة الموارد البشرية، و البوابات الجامعية الرقمية ، وأنظمة إدارة الامتحانات والنتائج .

وتسهم هذه التطبيقات في تحسين جودة التسيير وتقليل الأخطاء البشرية وتعزيز الثقة في المؤسسة الجامعية [8].

خامساً: إحصائيات حول دور الرقمنة في تعزيز الشفافية والمساءلة

تشير العديد من الدراسات والتقارير إلى النتائج الإيجابية لاعتماد الرقمنة في المؤسسات التعليمية:

أظهرت تقارير عربية أن استخدام الأنظمة الرقمية أدى إلى **تقليل الفساد الإداري بنسبة تتراوح بين 25% و40%** في المؤسسات العمومية.

تشير دراسات إلى أن الرقمنة ساهمت في **تحسين سرعة إنجاز المعاملات الإدارية بنسبة تفوق 50%**.

---

[6] -محمد الهادي، *التحول الرقمي في المؤسسات التعليمية*، دار الفكر، 2021، ص 33.
[7] -أحمد إبراهيم، *الإدارة الإلكترونية في الجامعات*، دار المسيرة، 2020، ص 71.

[8] -يوسف قنديل، *إدارة الجامعات في العصر الرقمي*، 2020، ص 44.

أكثر من **70% من الجامعات العالمية** تعتمد أنظمة رقمية لإدارة شؤونها الإدارية والأكاديمية.
اعتماد المنصات الرقمية أدى إلى **زيادة رضا الطلبة بنسبة تقارب 35%** في بعض التجارب الدولية.[9]

الفرع الثاني: الرقمنة وتحسين جودة التسيير والخدمات الجامعية

أولاً: مفهوم جودة التسيير والخدمات الجامعية في ظل الرقمنة

تُعد جودة التسيير والخدمات الجامعية من أهم مؤشرات نجاح مؤسسات التعليم العالي، حيث تعكس قدرة الجامعة على تقديم خدمات تعليمية وإدارية فعالة تلبي احتياجات الطلبة والأساتذة. ومع التحول الرقمي، أصبح مفهوم الجودة مرتبطًا بمدى توظيف التكنولوجيا في تحسين الأداء وتبسيط الإجراءات.
وتُعرّف جودة الخدمات الجامعية بأنها: *"مدى قدرة المؤسسة الجامعية على تقديم خدمات تعليمية وإدارية بكفاءة وفعالية، بما يحقق رضا المستفيدين[10]".
وقد أسهمت الرقمنة في إعادة تشكيل هذا المفهوم، حيث أصبحت الجودة تعتمد على السرعة، الدقة، سهولة الوصول إلى الخدمات، ودرجة رضا المستخدمين عن الأنظمة الرقمية[11].

ثانياً: دور الرقمنة في تحسين جودة التسيير الإداري تسمح الرقمنة
1- أتمتة العمليات الإداريةمما تقليل الأخطاء البشرية وتسريع الإجراءات وتحسين الكفاءة الإدارية[12].
2- تحسين اتخاذ القرار أكدت الدراسات أنهاتسهم في تسريع اتخاذ القرار وتقليل التكاليف التشغيلية[13].
3- رفع كفاءة الموارد البشرية تنمية العنصر البشري وتحسين الأداء المؤسسي[14].
4- تقليل التكاليف وتحسين الكفاءةمما يعزز الفعالية الاقتصادية للمؤسسة الجامعية[15].

ثالثاً: دور الرقمنة في تحسين جودة الخدمات الجامعية

1- تحسين جودة الخدمات التعليميةوقد أظهرت الدراسات وجود **أثر إيجابي مباشر للرقمنة على جودة التعليم الجامعي** من حيث الفعالية والتفاعل[16].
2- تسهيل الوصول إلى الخدماتمما يسهل على الطلبة الحصول على الخدمات بسرعة وكفاءة[17].
3- تحسين تجربة الطالب الجامعي تبسيط الإجراءات وتحسين ظروف الطلبة داخل الجامعة[18].

---

[9] -فاطمة الزهراء، *المساءلة الإدارية في المؤسسات العمومية*، 2020، ص 66.
[10] -أحمد إبراهيم، *جودة الخدمات في المؤسسات التعليمية*، دار المسيرة، 2020، ص 41.
[11] -حسن زيتون، *تكنولوجيا التعليم*، عالم الكتب، 2018، ص 88.
[12] -عبد الكريم قنديل، *الإدارة الإلكترونية*، 2021، ص 73.
[13] -كريمة حوامد، *دور الرقمنة في جودة التعليم العالي*، 2024
[14] -نفس المرجع.
[15] -محمد عبد الفتاح، *الإدارة الرقمية الحديثة*، 2020، ص 55.
[16] -قصير لبنى، *رقمنة التعليم العالي في الجزائر*، 2024
[17] -عبد الرزاق بن حليم، *التحول الرقمي وجودة الخدمات*، 2025
[18] -دراسة جامعة ورقلة حول الخدمات الجامعية الرقمية

4- تطوير البحث العلميمما يرفع من جودة الإنتاج العلمي داخل الجامعة[19].

رابعاً: تطبيقات الرقمنة في تحسين الخدمات الجامعية

من أبرز التطبيقات:-الأنظمة المعلوماتية الجامعية (ERP) و منصات التعليم الإلكتروني (LMS) و المكتبات الرقمية و الأنظمة الذكية لإدارة الامتحانات وتطبيقات الهواتف الذكية الجامعية .

وقد ساهمت هذه التطبيقات في تحسين سرعة ودقة الخدمات وتعزيز كفاءة الأداء المؤسسي[20] .

خامساً: إحصائيات حول تأثير الرقمنة على جودة التسيير والخدمات

تشير الدراسات الحديثة إلى نتائج مهمة، منها:

أظهرت دراسة أن الرقمنة أدت إلى **تحسن ملحوظ في جودة الخدمات الإدارية من حيث السرعة والدقة وسهولة الوصول**

وجود **أثر إيجابي مباشر للرقمنة على جودة الخدمة التعليمية** في الجامعات الجزائرية

بينت دراسة ميدانية أن الرقمنة ساهمت في **تحسين رضا الطلبة وتبسيط الإجراءات الإدارية بشكل واضح**

تشير دراسات قياسية إلى أن التحول الرقمي في الجامعات الجزائرية شهد **تطورًا ملحوظًا في تحسين جودة التعليم رغم وجود هامش للتطوير** .

-تحسين سرعة الخدمات الإدارية بنسبة تفوق **40–60%**

-تقليل الأخطاء الإدارية بنسبة تقارب **30%**

-ارتفاع مستوى رضا الطلبة عن الخدمات الرقمية بأكثر من **35%**

-اعتماد متزايد للأنظمة الرقمية في الجامعات الجزائرية خلال السنوات الأخيرة

3.المبحث الثاني: تحديات التحول الرقمي في الجامعة بين المخاطر السيبرانية وآليات المواجهة

أما في المبحث الثاني ،نتطرق في المطلب الأول لمخاطر السيبرانية في البيئة الجامعية الرقمية، وفي المطلب الثاني نتناول آليات مواجهة المخاطر السيبرانية وتعزيز الأمن الرقمي .

1.3.المطلب الأول: المخاطر السيبرانية في البيئة الجامعية الرقمية

الفرع الأول: طبيعة التهديدات السيبرانية

أولاً: مفهوم التهديدات السيبرانية في الجامعة

وتُعرّف التهديدات السيبرانية بأنها: *"مجموعة المخاطر والأفعال غير المشروعة التي تستهدف الأنظمة المعلوماتية بهدف اختراقها أو تعطيلها أو سرقة البيانات منها[21]".

وتزداد خطورة هذه التهديدات في الجامعات بسبب: الانفتاح الرقمي و كثرة المستخدمين (طلبة، أساتذة، إداريون و ضعف الوعي الأمني في بعض الحالات و الاعتماد على شبكات مفتوحة .

ثانياً: أنواع التهديدات السيبرانية في الجامعة الرقمية

---

[19] -يوسف قنديل، *إدارة المعرفة الرقمية*، 2020، ص 102.

[20] -نفس المرجع، ص 110.

[21] -سمير العلي، *الأمن السيبراني وحماية المعلومات*، دار الكتاب الحديث، 2019، ص 33.

1- الاختراقات الإلكترونية (Cyber Intrusions)وتشير الدراسات إلى أن **التهديدات الداخلية أصبحت من أخطر أشكال الاختراق في الجامعات**، حيث قد يقوم بعض الطلبة باستغلال الثغرات للوصول إلى الأنظمة.
2- تسريب البيانات (Data Breaches)وقد بلغت **متوسط تكلفة خرق البيانات في قطاع التعليم حوالي 3.65 مليون دولار**، مما يعكس خطورة هذا النوع من الجرائم[22].
كما يُعد قطاع التعليم من أكثر القطاعات تعرضًا لاختراق البيانات عالميًا، بسبب القيمة العالية للمعطيات التي يمتلكها[23].
3- الهجمات الإلكترونية (Cyber Attacks)تشمل مجموعة واسعة من الأساليب، من أبرزها:
أ- هجمات التصيد الإلكتروني (Phishing) وقد أظهرت الدراسات أن **100% من مؤسسات التعليم العالي تعرضت لمحاولات تصيد إلكتروني** في بعض الحالات[24].
ب- هجمات البرمجيات الخبيثة (Malware)وقد ارتفعت هذه الهجمات في الجامعات بنسبة **26% خلال السنوات الأخيرة[25].**
ج- هجمات الفدية (Ransomware)وقد أظهرت الدراسات أن **80% من مؤسسات التعليم تعرضت لهجمات فدية** في بعض الفترات[6]
د- هجمات حجب الخدمة (DDoS)تستهدف تعطيل مواقع الجامعة وخدماتها الإلكترونية.
ثالثاً: خصائص التهديدات السيبرانية في الجامعات
تتميز التهديدات السيبرانية في البيئة الجامعية بعدة خصائص:
-التنوع والتطور المستمر: حيث تتغير أساليب الهجوم بشكل دائم و**-الطابع العالمي:** يمكن تنفيذ الهجمات من أي مكان في العالم و**-الاستهداف المزدوج:** (مؤسساتي + فردي) و**-الاعتماد على الهندسة الاجتماعية:** استغلال ضعف وعي المستخدمين .
كما أن البيئة الجامعية تُعد هدفًا جذابًا نظرًا لاحتوائها على بيانات علمية وبحثية ذات قيمة عالية[26].
رابعاً: إحصائيات حول التهديدات السيبرانية في التعليم العالي
تشير التقارير الحديثة إلى خطورة الوضع السيبراني في الجامعات:
حوالي **91% من مؤسسات التعليم العالي تعرضت لهجمات سيبرانية خلال سنة واحدة**
أكثر من **30% من هذه المؤسسات تتعرض لهجمات بشكل أسبوعي**
قطاع التعليم يُعد **الأكثر استهدافًا عالميًا سنة 2025**
متوسط عدد الهجمات بلغ **أكثر من 4000 هجوم أسبوعيًا لكل مؤسسة تعليمية**

---

[22] -تقرير حول خروقات البيانات في قطاع التعليم
[23] -تقرير حول استهداف قطاع التعليم سيبرانياً
[24] -تقرير الحكومة البريطانية حول الأمن السيبراني في التعليم
[25] -نفس التقرير الحكومة البريطانية حول الأمن السيبراني في التعليم
[26] -نفس المرجع

حوالي **40% من المؤسسات التعليمية تتعرض لآثار سلبية مباشرة بعد الهجمات**

الفرع الثاني: آثار المخاطر السيبرانية على الجامعة

أولاً: الآثار الأكاديمية (التعليم والبحث العلمي)تؤثر المخاطر السيبرانية بشكل مباشر على العملية التعليمية والبحث العلمي داخل الجامعة، حيث قد تؤدي الهجمات إلى:

تعطيل المنصات التعليمية الرقمية.و**فقدان أو التلاعب بالبيانات الأكاديمية** و**استهداف الأبحاث العلمية وقواعد البيانات**، وقد أكدت الدراسات أن الهجمات السيبرانية يمكن أن تؤدي إلى **انقطاع العملية الأكاديمية بشكل كامل في بعض الحالات** نتيجة تعطيل الأنظمة الرقمية[27].

ثانياً: الآثار الإدارية والتنظيمية

تنعكس المخاطر السيبرانية على التسيير الإداري للجامعة بشكل واضح، كما أن الهجمات مثل هجمات الفدية قد تؤدي إلى **شلل إداري مؤقت أو كلي** بسبب عدم القدرة على الوصول إلى الأنظمة[28] .

ثالثاً: الآثار المالية والاقتصادية

تُعد الخسائر المالية من أبرز آثار المخاطر السيبرانية، كما أن تكلفة خرق البيانات في المؤسسات التعليمية تُعد مرتفعة، نظرًا لقيمة البيانات الحساسة التي تمتلكها [29].

رابعاً: الآثار القانونية

تؤدي المخاطر السيبرانية إلى مسؤوليات قانونية على عاتق الجامعة، خاصة في حال:تسريب البيانات الشخصية للطلبة والأساتذة

خامساً: الآثار على السمعة المؤسسيةتؤثر الهجمات السيبرانية بشكل كبير على صورة الجامعة، وقد أشارت الدراسات إلى أن المؤسسات التعليمية التي تتعرض لهجمات سيبرانية تعاني من **ضرر كبير في سمعتها نتيجة تسريب البيانات أو تعطيل الخدمات[30]** .

سادساً: الآثار الأمنية والاجتماعيةتمتد آثار المخاطر السيبرانية إلى الجوانب الأمنية والاجتماعية كما أن ضعف الوعي الأمني لدى المستخدمين يزيد من حدة هذه المخاطر[31] .

سابعاً: إحصائيات حول آثار المخاطر السيبرانية في الجامعاتتؤدي إلى **تعطيل العمليات التعليمية والإدارية بشكل مباشر**

إحصائيات تحليلية تقريبية:

أكثر من **60% من المؤسسات التعليمية** تتعرض لتعطيل جزئي أو كلي للخدمات بعد الهجمات

حوالي **30–50% من الجامعات** تعاني من خسائر مالية مباشرة نتيجة الهجمات

ما يقارب **40% من الهجمات تؤدي إلى تسريب بيانات حساسة**

---

[27] -سمير العلي، *الأمن السيبراني وحماية المعلومات*، دار الكتاب الحديث، 2019، ص 85.

[28] -تقرير IBM حول الأمن السيبراني في التعليم

[29] -تقرير Solix حول الأمن السيبراني في التعليم العالي

[30] -تقرير حول استهداف قطاع التعليم بالهجمات السيبرانية

[31] -مقال حول تأثير الهجمات السيبرانية على المؤسسات التعليمية

ارتفاع كبير في استهداف الجامعات بسبب التحول نحو التعليم الرقمي[32] .

2.3.المطلب الثاني: آليات مواجهة المخاطر السيبرانية وتعزيز الأمن الرقمي

الفرع الأول: الآليات القانونية والمؤسساتية لمواجهة المخاطر السيبرانية في الجامعة

أولاً: مفهوم الآليات القانونية والمؤسساتية في مجال الأمن السيبرانيوتكتسي هذه الآليات أهمية خاصة في البيئة الجامعية نظرًا لحساسية البيانات التي يتم تداولها، وتعدد المستخدمين، واتساع نطاق الخدمات الرقمية.

ثانياً: الآليات القانونية لمواجهة المخاطر السيبرانية

1- التشريعات الوطنية المتعلقة بالأمن السيبراني

في السياق الجزائري، يُعد الإطار القانوني للأمن السيبراني قائمًا على مجموعة من النصوص، من أهمها

-قوانين مكافحة الجرائم المعلوماتية و-قوانين حماية المعطيات الشخصية و-قوانين تنظيم الاتصالات

وقد عرّف المشرع الأمن السيبراني بأنه مجموعة من السياسات والآليات التي تهدف إلى حماية البيانات والأنظمة من أي تهديد يمس سلامتها أو سريتها .

2- التجريم والعقوباتوتفرض عقوبات جزائية (حبس وغرامات) لردع الجرائم السيبرانية، وهو ما يشكل وسيلة أساسية لحماية المؤسسات الجامعية[33].

3- حماية البيانات الشخصيةوقد أصبحت هذه الحماية ضرورة في ظل تزايد الهجمات التي تستهدف قواعد البيانات الجامعية.

4- الاتفاقيات الدولية والتعاون القانوني

إلا أن الدراسات تشير إلى وجود **صعوبة في مواجهة الجرائم السيبرانية بسبب طبيعتها العابرة للحدود** .

5- السياسات والاستراتيجيات الوطنية للأمن السيبرانيوتمثل هذه الاستراتيجيات إطارًا توجيهيًا للمؤسسات الجامعية.

ثالثاً: الآليات المؤسساتية لمواجهة المخاطر السيبرانية

1- الهيئات الوطنية المختصة بالأمن السيبراني

تقوم الدول بإنشاء هيئات متخصصة لمراقبة التهديدات

2- وحدات الأمن السيبراني داخل الجامعاتتعمل الجامعات الحديثة على إنشاء:-مراكز أمن معلومات

-فرق تقنية متخصصة .

.3- سياسات الحوكمة الرقمية داخل الجامعة

وهو ما يعزز الرقابة الداخلية ويحد من المخاطر.

4- التكوين والتوعية

وقد أكدت الدراسات أن ضعف الوعي يُعد من أبرز أسباب نجاح الهجمات السيبرانية.

5- الشراكات والتعاون المؤسسي

تعتمد الجامعات على التعاون مع:

---

[32] -مقال إدارة المخاطر السيبرانية في المؤسسات التعليمية

[33] -نفس المرجع.

-مؤسسات حكومية وشركات تكنولوجيا و-مراكز بحثية بهدف تبادل الخبرات وتعزيز القدرات الأمنية.

رابعاً: إحصائيات حول فعالية الآليات القانونية والمؤسساتية

تشير التقارير إلى أهمية هذه الآليات في الحد من المخاطر:

-الدول التي تعتمد استراتيجيات وطنية للأمن السيبراني تحقق **مستوى أعلى من الحماية بنسبة تفوق 40%** مقارنة بغيرها .

-أكثر من **70% من الدول** لديها أطر قانونية للأمن السيبراني 0

-المؤسسات التي تعتمد سياسات أمن معلومات داخلية تقل فيها الحوادث السيبرانية بنسبة تصل إلى **50%** .

-ضعف الإطار القانوني والمؤسساتي يُعد من أبرز أسباب تفاقم الجرائم السيبرانية عالميًا

خامساً: التحديات التي تواجه الآليات القانونية والمؤسساتية

رغم أهميتها، تواجه هذه الآليات عدة تحديات:-بطء التشريعات مقارنة بسرعة التطور التكنولوجي

-ضعف التنسيق بين الهيئات و نقص الكفاءات المتخصصة و صعوبة إثبات الجرائم السيبرانية .

الفرع الثاني: الحلول التقنية والتدابير الوقائية لمواجهة المخاطر السيبرانية في الجامعة الرقمية

أولاً: مفهوم الحلول التقنية والتدابير الوقائية

وتُعرّف الحماية التقنية بأنها: *"مجموعة البرمجيات والأنظمة التي تُستخدم لرصد الهجمات الإلكترونية ومنعها أو الحد من آثارها"[34].

أما التدابير الوقائية فهي: *"إجراءات استباقية تعتمد على السياسات الأمنية والتوعية والتدريب بهدف تقليل احتمالية وقوع الهجمات[35]".

ثانياً: الحلول التقنية لحماية الجامعة الرقمية

1- أنظمة الجدران النارية (Firewalls)

تُعد الجدران النارية خط الدفاع الأول ضد الهجمات السيبرانية، وتُستخدم بشكل واسع في حماية الشبكات الجامعية.[36]

2- أنظمة كشف ومنع الاختراق (IDS/IPS)-وتُعد من أهم أدوات حماية الأنظمة الجامعية الحديثة.[37]

3- التشفير (Encryption):يُستخدم التشفير لحماية البيانات أثناء نقلها أو تخزينها، بحيث تصبح غير قابلة للقراءة إلا من طرف مخول .ويُعد من أقوى وسائل حماية البيانات الحساسة داخل الجامعات[38].

4- أنظمة المصادقة المتعددة (Multi-Factor Authentication)

تعتمد هذه التقنية على أكثر من خطوة للتحقق من هوية المستخدم، وتهدف إلى تقليل خطر اختراق الحسابات الجامعية[39].

---

[34] -سمير العلي، *الأمن السيبراني وحماية المعلومات*، دار الكتاب الحديث، 2019، ص 91.

[35] -محمد عبد الفتاح، *إدارة الأمن الرقمي*، دار الفكر العربي، 2020، ص 77.

[36] -حسن عبد الله، *أمن الشبكات المعلوماتية*، 2021، ص 64.

[37] -علي السالمي، *تقنيات كشف الاختراقات*، 2019، ص 88.

[38] -فاطمة الزهراء، *تشفير البيانات وأمن المعلومات*، 2020، ص 102.

[39] -يوسف قنديل، *أنظمة المصادقة الرقمية*، 2021، ص 59.

5- النسخ الاحتياطي للبيانات (Backup Systems)
تسمح هذه الأنظمة بـ:-حفظ نسخ من البيانات بشكل دوري و-استرجاع المعلومات في حال الهجمات أو الأعطال وتقليل آثار هجمات الفدية .
6- أنظمة الحوسبة السحابية الآمنة
تُستخدم السحابة لتخزين البيانات الجامعية لكنها تتطلب إعدادات أمنية صارمة لتفادي الاختراق.[40]
ثالثاً: التدابير الوقائية داخل الجامعة
1- وضع سياسات أمن المعلوماتوهي خطوة أساسية في تقليل المخاطر السيبرانية.
2- التوعية والتكوين:وقد أثبتت الدراسات أن **80% من الهجمات السيبرانية تنجح بسبب الخطأ البشري**[41].
3- المراقبة المستمرة للشبكاتوذلك للكشف المبكر عن أي تهديد.
4- تحديث الأنظمة والبرمجياتيُعد تحديث الأنظمة من أهم الإجراءات الوقائية، .
5- اختبار الاختراق (Penetration Testing)
تقوم الجامعات بإجراء اختبارات دورية لمحاكاة الهجمات بهدف:اكتشاف الثغرات وتقييم مستوى الحماية
تحسين الأنظمة الأمنية .
رابعاً: إحصائيات حول فعالية الحلول التقنية والتدابير الوقائية
تشير الدراسات الحديثة إلى:
-استخدام أنظمة الحماية المتقدمة يقلل من الهجمات السيبرانية بنسبة **تصل إلى 60%**
-أكثر من **70% من المؤسسات التعليمية تعتمد أنظمة جدران نارية متقدمة**
-تطبيق المصادقة الثنائية يقلل من اختراق الحسابات بنسبة **أكثر من 90%**
-ضعف التوعية الأمنية يؤدي إلى نجاح **80% من الهجمات السيبرانية**
-المؤسسات التي تعتمد النسخ الاحتياطي تقل فيها خسائر هجمات الفدية بنسبة **50%** تقريبًا
كما تؤكد تقارير دولية أن المؤسسات التعليمية التي تستثمر في الأمن السيبراني تحقق **مستويات أعلى من الاستقرار الرقمي والاستمرارية التعليمية**.
خامساً: تحديات تطبيق الحلول التقنية والتدابير الوقائية
رغم فعاليتها، تواجه هذه الحلول عدة تحديات:
-ارتفاع تكاليف الأنظمة الأمنية
-نقص الكفاءات التقنية
-التطور المستمر للهجمات السيبرانية
-ضعف الثقافة الرقمية لدى المستخدمين
تُعد الحلول التقنية والتدابير الوقائية من أهم الركائز في حماية الجامعة الرقمية من المخاطر السيبرانية، حيث تجمع بين الوسائل التكنولوجية المتقدمة

---

[40] -تقرير اليونسكو، *الأمن السيبراني في التعليم الرقمي*، 2020.
[41] -تقرير IBM للأمن السيبراني في التعليم، 2021.

والإجراءات التنظيمية الوقائية. غير أن فعاليتها تتطلب استثمارًا مستمرًا في البنية التحتية، وتكوين الموارد البشرية، وتعزيز الوعي الأمني لضمان بيئة جامعية رقمية آمنة ومستقرة[42].

4.خاتمة

يتضح من خلال هذا البحث أن التحول نحو الجامعة الرقمية لم يعد خيارًا ثانويًا، بل أصبح ضرورة استراتيجية فرضتها التطورات التكنولوجية ومتطلبات جودة التعليم العالي. وقد ساهم هذا التحول في تعزيز مبادئ الحوكمة الرشيدة داخل الجامعة، خاصة من حيث الشفافية وتحسين جودة التسيير والخدمات. غير أن هذا التقدم الرقمي يقابله تصاعد في المخاطر السيبرانية التي تهـدد أمـن المعلومات واستمرارية الخدمات الجامعية. لذلك فإن نجاح الجامعة الرقمية لا يتحقق فقط من خلال الرقمنة، بل يتطلب أيضًا منظومة متكاملة من الحماية القانونية والتقنية والمؤسساتية لضمان بيئة تعليمية آمنة ومستقرة.

وخلص البحث إلى أن فعالية الجامعة الرقمية ترتبط بمدى قوة الأمن السيبراني المطبق، ولابد من إدماج الأمن السيبراني كعنصر أساسي في استراتيجيات التحول الرقمي الجامعي.

5.قائمة المراجع:

أولا:الكتب:

-عبد الكريم بن يحيى، التعليم الرقمي في الجامعات العربية، دار المسيرة، عمان، 2021 .
-محمد عبد الفتاح، تكنولوجيا التعليم والتحول الرقمي، دار الفكر العربي، القاهرة، 2020 .
-عبد القادر محمد، الحوكمة في المؤسسات العمومية، دار الجامعة الجديدة، 2020 .
-منى عبد الله الحداد، الحوكمة الرشيدة ودورها في ضمان جودة التعليم العالي، جامعة النيلين، 2017

[42] -البنك الدولي، *التحول الرقمي والأمن السيبراني*، 2021..