



الجمهورية الجزائرية الديمقراطية الشعبية
جامعة المجاهد عبد الحفيظ بوصوف ميلة
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
قسم العلوم التجارية



الميدان: العلوم الاقتصادية والتسيير والعلوم التجارية

الشعبة: علوم تجارية

التخصص: مالية وتجارة دولية

مذكرة مكملة لنيل شهادة الماستر بعنوان:

التكامل بين الرقمنة والامن السيبراني لحماية المعاملات التجارية الدولية
تقييم تجربة البنوك الجزائرية

المشرف	اعداد الطلبة	
ركيمة فارس	صولي بشرى	1
	بوقاسة هنية	2

لجنة المناقشة:

الصفة	الجامعة	اسم ولقب الأستاذ(ة)
رئيسا	جامعة المجاهد عبد الحفيظ بوصوف ميلة	رحيم ابراهيم
مشرفا ومقررا	جامعة المجاهد عبد الحفيظ بوصوف ميلة	ركيمة فارس
ممتحنا	جامعة المجاهد عبد الحفيظ بوصوف ميلة	جوال محمد

السنة الجامعية 2025/2026



شكر وعرفان

قال رسول الله صلى الله عليه وسلم:

"...ومن صنع إليكم معروفا فكافئوه، فإن لم تجدوا ما تكافئونه فادعوا له حتى تروا أنكم قد كافأتموه".

نحمد الله سبحانه وتعالى حمدا يليق لجلاله وعظيم سلطانه على نعمته وتوفيقه لنا على إتمام هذه المذكرة.

واعترافا بالفضل وتقديرا للجميل نتوجه بجزيل التقدير والامتنان وخالص الدعاء لكل من ساعدنا من قريب أو بعيد على إنجاز هذا العمل وتذليل كل الصعوبات التي واجهتنا.

كل الشكر و الإمتنان للأستاذ المشرف، على دعمه المتواصل الذي كان له الأثر في إنجاز هذا العمل، جزاك الله خيرا وبارك في علمك

كما نتقدم بأسمى عبارات التقدير والاحترام لأعضاء لجنة المناقشة الذين قبلوا مناقشة هذه المذكرة

وفقنا الله وإياكم



الاهداء

...إلى أبي وأمي

إلى القليين الذين لم يبتلا عليّ يومًا بالحب
والدعاء، إلى من كانا سبب قوتي بعد الله
في كل خطوة.

أهديكما هذا النجاح الذي كان حلمكما قبل
أن يكون حلمي، فكل تعب بذلتماه كان
وراء وصولي إلى هذا اليوم.

حفظكما الله لي دائمًا، فأنتما أجمل ما أملك

هنية





الاهداء

وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ

صدق الله العظيم

إلى من كان دعاؤها نورًا يرافقتني في كل خطوة، إلى
أمي الحبيبة، حفظها الله وأدامها تاجًا فوق رأسي

إلى أبي العزيز، الذي علمني أن النجاح لا يأتي إلا بالصبر
والتعب، وكان سندي وقوتي طوال مسيرتي الدراسية

إلى إخوتي وعائلتي، وكل من منحني كلمة تشجيع أو
دعاء صادقًا في لحظات التعب واليأس

بشرى



فهرس المحتويات:

	شكر وعرفان
	الاهداء
	فهرس المحتويات
	فهرس الجداول
	فهرس الاشكال
أ_ز	مقدمة
19_45	الفصل الأول: الرقمنة في البنوك التجارية
20	المبحث الأول: الإطار المفاهيمي للرقمنة
20	المطلب الأول: مفهوم الرقمنة، خصائصها و أهدافها
20	الفرع الأول:تعريف الرقمنة و خصائصها
25	الفرع الثاني: اهداف الرقمنة واهميتها
26	المطلب الثاني: اسباب ومتطلبات الرقمنة
26	الفرع الاول: متطلبات الرقمنة
28	الفرع الثاني: اسباب الرقمنة
29	المطلب الثالث: التحول الرقمي في المؤسسات
29	الفرع الاول: مفهوم التحول الرقمي
32	الفرع الثاني: علاقة مفهوم التحول الرقمي بالرقمنة
34	المبحث الثاني: الرقمنة في البنوك التجارية
34	المطلب الاول: المعاملات التجارية البنكية وانواعها
35	الفرع الاول: مفهوم المعاملات التجارية البنكية
37	الفرع الثاني: انواع المعاملات التجارية البنكية
39	المطلب الثاني: اهمية الرقمنة في البنوك ومتطلباتها
39	الفرع الاول: اهمية الرقمنة في البنوك التجارية
40	الفرع الثاني: متطلبات رقمنة البنوك التجارية
41	المطلب الثالث: الخدمات المصرفية الرقمية في البنوك التجارية
41	الفرع الاول: تعريف الخدمات المصرفية الرقمية

42	الفرع الثاني: التكامل بين الرقمنة والامن السيبراني في حماية المعاملات التجارية البنكية
47 - 79	الفصل الثاني: دور التكامل بين الرقمنة و الأمن السيبراني لحماية المعاملات التجارية البنكية
48	المبحث الاول: الاطار المفاهيمي للامن السيبراني
48	المطلب الاول: مفهوم الامن السيبراني
48	الفرع الاول: تعريف الامن السيبراني ومكوناته
53	الفرع الثاني: اهمية الامن السيبراني في المعاملات التجارية الرقمية
55	المطلب الثاني: التهديدات السيبرانية واثرها على المعاملات البنكية الرقمية
55	الفرع الاول: التهديدات السيبرانية في المعاملات البنكية الرقمية
59	الفرع الثاني: اثر التهديدات السيبرانية في المعاملات البنكية الرقمية
61	المطلب الثالث: استراتيجيات التكامل بين الرقمنة والامن السيبراني
61	الفرع الاول: مفهوم التكامل بين الرقمنة والامن السيبراني
65	الفرع الثاني: محاور التكامل بين الرقمنة والأمن السيبراني
67	المبحث الثاني: إدارة المخاطر السيبرانية وآليات حماية المعاملات البنكية الرقمية
68	المطلب الأول: إدارة المخاطر السيبرانية في البنوك التجارية
68	الفرع الأول: مفهوم إدارة المخاطر السيبرانية في البنوك التجارية و مراحلها
69	الفرع الثاني: أهمية إدارة المخاطر في البنوك
71	المطلب الثاني: سياسات إدارة مخاطر الأمن السيبراني و آليات حماية المعاملات التجارية البنكية من المخاطر السيبرانية
71	الفرع الأول: سياسات إدارة مخاطر الأمن السيبراني
72	الفرع الثاني: أدوات حماية المعاملات التجارية البنكية من المخاطر السيبرانية
75	المطلب الثالث: أفضل الممارسات لحماية المعاملات التجارية البنكية و أهم التحديات
75	الفرع الأول: أفضل الممارسات لإدارة المخاطر البنكية
77	الفرع الثاني: تحديات الأمن السيبراني في البنوك التجارية
81 - 104	الفصل الثالث: دراسة ميدانية لدور التكامل بين الرقمنة و الأمن السيبراني لحماية المعاملات التجارية لمجموعة من البنوك (قسنطينة، سطيف و ميله

82	المبحث الأول: منهجية الدراسة الميدانية
82	المطلب الأول: الإجراءات المنهجية للدراسة الميدانية
82	الفرع الأول: منهج الدراسة المتبع
82	الفرع الثاني: مجتمع، عينة و حدود الدراسة
83	المطلب الثاني: أدوات ومتغيرات الدراسة
83	الفرع الأول: أدوات الدراسة
83	الفرع الثاني: متغيرات الدراسة
84	المطلب الثالث: تصميم الاستبيان و الأدوات الإحصائية المستعملة
84	الفرع الأول: تصميم الاستبيان
84	الفرع الثاني: الأدوات الإحصائية المستعملة
91	المبحث الثاني: تحليل و مناقشة نتائج الدراسة
91	المطلب الأول: عرض نتائج الدراسة
91	الفرع الأول: النتائج المتعلقة بالخصائص العامة لعينة الدراسة
93	الفرع الثاني: النتائج المتعلقة باتجاه آراء المستجوبين حول محاور الاستبيان
98	المطلب الثاني: مناقشة النتائج و اختبار الفرضية
98	الفرع الأول: مناقشة النتائج
102	الفرع الثاني: اختبار صحة الفرضية الرئيسية
106	الخاتمة
109	قائمة المراجع والمصادر
115	الملاحق
120	الملخص

فهرس الجداول

الرقم	العنوان	الصفحة
01	الفرق بين التحول الرقمي و الرقمنة	33
02	أوزان مقياس Likert الخماسي	85
03	اختبار التوزيع الطبيعي	86
04	قوة معامل الارتباط	87
05	معامل الارتباط بين عبارات محور استراتيجية الرقمنة في البنوك	87
06	معامل الارتباط بين عبارات محور ممارسات الأمن السيبراني	88
07	معامل الارتباط بين عبارات محور التكامل بين الرقمنة و الأمن السيبراني	89
08	معامل الارتباط بين عبارات محور حماية المعاملات التجارية البنكية	90
09	نتائج معامل ألفا-كرونباخ	90
10	توزيع عينة الدراسة حسب النوع	91
11	توزيع عينة الدراسة حسب حجم البنك	92
12	وجود إدارة أمن سيبراني	92

93	إجابات المحور الثاني-استراتيجية الرقمنة-	13
94	إجابات المحور الثالث-ممارسات الأمن السيبراني-	14
95	إجابات المحور الرابع-التكامل بين الرقمنة و الأمن السيبراني-	15
96	إجابات المحور الخامس-حماية المعاملات التجارية البنكية-	16
98	تحليل معامل الارتباط Pearson	17
99	تحليل التباين ANOVA	18
99	المعاملات	19
101	ملخص النتائج	20

فهرس الأشكال:

الرقم	العنوان	الصفحة
01	تكلفة الخسائر المحتملة للهجمات السيبرانية على قطاع الخدمات المالية(نسبة من صافي الدخل السنوي)	59
02	تطور الهجمات السيبرانية في القطاع المصرفي	77
03	توزيع عينة الدراسة حسب النوع	91
04	توزيع عينة الدراسة حسب حجم البنك	92
05	لدى البنك إدارة مستقلة للأمن السيبراني	92

مقدمة

يشهد العالم ثورة تكنولوجية متسارعة أدت إلى إعادة صياغة المفاهيم الاقتصادية و الخدمية، حيث لم تعد الرقمنة مجرد خيار تكميلي للمؤسسات المالية، بل أضحت ضرورة استراتيجية للبقاء و المنافسة. و تعد البنوك التجارية من أكثر المؤسسات تأثراً بهذا التحول، حيث أصبحت تعتمد بشكل متزايد على الأنظمة الرقمية والتقنيات الحديثة لتقديم خدماتها المالية والتجارية. فقد ساهمت الرقمنة في تسهيل المعاملات البنكية، وتسريع عمليات الدفع والتحويل، وتحسين تجربة العملاء من خلال الخدمات المصرفية الإلكترونية والتطبيقات الذكية.

لكن و مع هذا التطور المتسارع، برزت تحديات جديدة تتعلق بحماية البيانات و الأنظمة المالية من الهجمات الإلكترونية و الاختراقات، مما جعل الاعتماد على مبادئ و تقنيات الأمن السيبراني أمراً ضروريا لضمان سلامة المعاملات التجارية البنكية. فالأمن السيبراني يمثل مجموعة من الإجراءات والتقنيات التي تهدف إلى حماية المعلومات والأنظمة الرقمية من التهديدات السيبرانية مثل القرصنة، وسرقة البيانات، والاحتيال الإلكتروني.

1/ إشكالية الدراسة: في عالم تتسارع فيه عملية الرقمنة لتصبح شريان الحياة للمؤسسات عامة و البنوك التجارية خاصة، لم تعد البيانات مجرد أرقام و نصوص، بل أصبحت الأصول الأكثر قيمة و رأس المال الحقيقي للنجاح. فكل معاملة بنكية، و كل استراتيجية عمل يتم تخزينها و تداولها في فضاء رقمي شاسع. لكن هذا الأخير، بقدر ما يوفره من فرص هائلة للنمو و الابتكار، يَعمُجُ بتهديدات خفية و متطورة قد تحول النجاح إلى كابوس في لحظات. و هنا، يبرز الأمن السيبراني ليس كخيار تكميلي، بل كضرورة استراتيجية و حجر زاوية لضمان الاستمرارية، و حماية السمعة، وبناء الثقة في هذا العصر الجديد. من هنا تبرز مشكلة البحث في كيفية الموازنة بين السرعة في الرقمنة وبين توفير الحماية اللازمة للبيانات والأموال، مما يجعل التكامل بين الرقمنة والأمن السيبراني ضرورة حتمية وليس خيارا تقنيا فحسب. لهذا تتمحور إشكالية بحثنا في التساؤل الرئيسي التالي:

إلى أي مدى يساهم التكامل بين الرقمنة و الأمن السيبراني في حماية المعاملات التجارية البنكية الجزائية؟

التساؤلات الفرعية:

- ما المقصود بالرقمنة في القطاع البنكي؟
- ما هو الأمن السيبراني و ما هي أهم المخاطر السيبرانية التي تواجه المعاملات البنكية الرقمية؟

- كيف يساهم الأمن السيبراني في حماية الأنظمة المصرفية؟

- ما هي الآليات التي تحقق التكامل بين الرقمنة والأمن السيبراني داخل البنوك؟

2/ الفرضية الرئيسية: يساهم التكامل بين الرقمنة و الأمن السيبراني في تعزيز حماية المعاملات

التجارية البنكية، من خلال رفع مستوى أمن المعلومات و تقليل مخاطر التهديدات السيبرانية بما

يضمن سلامة العمليات البنكية الرقمية في ظل التوسع المتزايد في الاعتماد على الرقمنة.

الفرضيات الفرعية:

- لا يوجد أثر ذو دلالة معنوية لاستراتيجية الرقمنة في البنوك التجارية على حماية المعاملات التجارية البنكية عند مستوى دلالة 5% .
- لا يوجد أثر ذو دلالة معنوية للأمن السيبراني في البنوك التجارية على حماية المعاملات التجارية البنكية عند مستوى دلالة 5% .
- لا يوجد أثر ذو دلالة معنوية للتكامل بين الرقمنة والأمن السيبراني في البنوك التجارية على حماية المعاملات التجارية البنكية عند مستوى دلالة 5% .
- لا يوجد أثر ذو دلالة معنوية للخدمات البنكية الرقمية على حماية المعاملات التجارية البنكية عند مستوى دلالة 5%.

4/ أهمية الدراسة: تكتسب هذه الدراسة أهميتها من عدة جوانب، أهمها:

أ. إبراز الدور المتزايد للرقمنة في تطوير الخدمات البنكية والتجارية، مع تسليط الضوء على

أهمية تطبيق معايير الأمن السيبراني لحماية البيانات والمعاملات المالية.

ب. المساهمة في تعزيز الوعي بأهمية التكامل بين التكنولوجيا والأمن المعلوماتي داخل القطاع

المصرفي.

ت. إثراء المكتبة الجامعية بموضوع يجمع بين تكنولوجيا المعلومات و العلوم المالية و

المصرفية.

5/ أهداف الدراسة: تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف، من أهمها:

- توضيح مفهوم الرقمنة في القطاع البنكي.
- التعرف على مفهوم الأمن السيبراني ودوره في حماية المعلومات المالية.
- تحليل المخاطر الإلكترونية التي تهدد المعاملات التجارية البنكية.
- إبراز أهمية التكامل بين الرقمنة والأمن السيبراني في تحقيق بيئة مصرفية آمنة.

6/ منهج الدراسة: من أجل معالجة مختلف جوانب الموضوع قمنا باستخدام المنهج الوصفي

التحليلي في جانبه النظري باعتباره الأكثر تناسبا للمواضيع، أما في الجانب التطبيقي فاعتمدنا الدراسة الميدانية باستخدام أدواتها المتمثلة في الملاحظة و الاستبيان.

7/ هيكل الدراسة: تم تقسيم موضوع الدراسة إلى ثلاث فصول:

✓ الفصل الأول: تناولنا فيه الرقمنة في القطاع البنكي، حيث خصص المبحث الأول للرقمنة و

الثاني للرقمنة في البنوك التجارية.

✓ الفصل الثاني: تناولنا فيه التكامل بين الرقمنة و الأمن السيبراني لحماية المعاملات التجارية

الرقمية، حيث خصص المبحث الأول للأمن السيبراني و مخاطره، و التكامل بينه و بين الرقمنة، في

المبحث الثاني تناولنا إدارة المخاطر السيبرانية في البنوك التجارية و آليات الحماية.

8/ صعوبات الدراسة:

لا تخلو الأعمال من الصعوبات والعوائق خاصة في ميدان البحث العلمي، ومن أهم هذه الصعوبات التي واجهتنا خلال فترة إنجاز الدراسة ما يلي:

✓ نقص أو ندرة المراجع باللغة العربية متعلقة بالموضوع.

- ✓ صعوبة في الحصول على وثائق من أجل استعمالها كملاحق .
- ✓ صعوبة الحصول على المعلومات الخاصة بالدراسة الميدانية حيث لاقينا حذر أثناء توزيع الاستبيان في بعض البنوك، و رفضها في بعض آخر، ما اضطرنا إلى إرساله عن طريق البريد الإلكتروني لبعض الفروع بعد الاتصال بهم عبر صفحات التواصل الاجتماعي.

9/ الدراسات السابقة:

الدراسة الأولى: أثر التحول الرقمي على الأداء الوظيفي في البنوك التجارية الجزائرية ، دراسة ميدانية على بعض البنوك بولاية الطارف وهي مذكرة ماستر نوقشت بكلية العلوم الاقتصادية والتجارية وعلوم التسيير بجامعة الطارف، 2023

هدفت الدراسة إلى تحليل العلاقة بين تطبيقات التحول الرقمي من جهة، ومستوى الأداء الوظيفي داخل البنوك الجزائرية من جهة أخرى. وركزت بشكل خاص على عناصر مثل استخدام البرمجيات الحديثة، وأتمتة المعاملات، والربط الشبكي بين الإدارات. وقد خلصت الدراسة إلى أن التحول الرقمي ساهم في تحسين الأداء من حيث السرعة، وتقليل نسبة الأخطاء، ورفع جودة الخدمات المقدمة للعملاء، إلا أن ذلك يبقى مرهونا بمستوى تكوين الموارد البشرية وتوفر البنية التحتية الرقمية المناسبة.

الدراسة الثانية: أعدها الطالب ياسين عيساوي بعنوان: دور الرقمنة في تعميم الشمول المالي في الجزائر-دراسة حالة بنك السلام- مذكرة ماستر نوقشت بالمركز الجامعي بالنعامة سنة 2022.

هدفت هذه الدراسة إلى تحليل مدى مساهمة الرقمنة البنكية في توسيع قاعدة الزبائن وتحقيق الإدماج المالي، خاصة في المناطق النائية. استعرض الباحث تجربة بنك السلام في تقديم خدمات مالية رقمية موجهة للزبائن غير المتعاملين في سابقا مع البنوك، مثل القروض الرقمية، والحسابات

الإلكترونية، وتطبيقات الدفع عبر الهاتف. وقد أظهرت النتائج أن الرقمنة كانت عاملاً فاعلاً في تحسين الشمول المالي، رغم استمرار عقبات كضعف التغطية الرقمية، ونقص الثقة في الوسائل الإلكترونية ونقص لدى بعض شرائح المجتمع.

الدراسة الثالثة: أنجزت هذه الدراسة من طرف الطالب زروقي عبد الحفيظ، بعنوان: "تحليل واقع المخاطر السيبرانية في البنوك العمومية الجزائرية- دراسة ميدانية ببنك الفلاحة والتنمية الريفية BADR - وهي مذكرة ماستر نوقشت بكلية العلوم الاقتصادية، جامعة قاصدي مرباح ، ورقلة ، سنة 2021.

هدفت الدراسة إلى تشخيص طبيعة التهديدات السيبرانية التي تواجه البنوك العمومية، مع التركيز على مدى استعداد بنك الفلاحة الريفية للتعامل مع هذه التهديدات، بينت نتائج الدراسة أن البنك يعاني من ضعف نسبي والتن في تطبيق معايير الحماية الإلكترونية، خاصة في جانب التكوين المتخصص للموظفين في أمن المعلومات، رغم توفر بعض أدوات الحماية التقنية، و أوصى الباحث بأهمية تطوير استراتيجي لإدارة المخاطر السيبرانية، و تكوين فرق مختصة في الأمن السيبراني البنكي.

مصطلحات الدراسة:

البنوك التجارية: البنوك التجارية هي مؤسسات مصرفية تتولى استقبال ودائع الأفراد والمؤسسات وتقديمها في شكل قروض مقابل فوائد.

إدارة المخاطر: هي مجموعة من الواجبات و الأنشطة الوظيفية التي يبذلها المسؤولون عن المشروع للتحكم في الأخطار التي يتعرض لها و التي من شأنها خلق ظروف آمنة معقولة قبل حدوث

الحادث و بالتالي إرساء خطة للتخفيف من الآثار المادية المترتبة أثناء وقوع الخسارة و يهدف حماية المشروع من أي خسارة مفاجئة نتيجة لأي ظروف تتعرض لها المنشأة

المخاطر البنكية: هي احتمالية وقوع أحداث غير متوقعة قد تؤدي إلى خسائر مالية، أو تراجع في الأرباح أو حتى انهيار البنك، بما أن جوهر عمل البنك هو إدارة الاموال، فإن المخاطر هي جزء أصيل في هذا النشاط.

الفصل الأول: الرقمنة في البنوك

تمهيد:

شهد القطاع البنكي تحولاً متسارعاً بفعل التطور التكنولوجي، حيث أصبحت الرقمنة عنصراً أساسياً في تحديث الخدمات المالية وتحسين كفاءتها. فلم تعد البنوك تعتمد فقط على المعاملات التقليدية، بل اتجهت نحو تقديم خدمات رقمية متكاملة تتيح للعملاء إنجاز عملياتهم بسرعة وأمان ومن أي مكان. وتسهم الرقمنة في تطوير الأداء الداخلي للمؤسسات البنكية، وتعزيز تجربة العملاء، ورفع مستوى التنافسية في ظل بروز شركات التكنولوجيا المالية. وعليه، يهدف هذا الفصل إلى استعراض مفهوم الرقمنة في القطاع البنكي، و الخدمات المصرفية الرقمية فيه.

المبحث الأول: الإطار المفاهيمي للرقمنة:

يشهد العالم ثورة تقنية غير مسبقة أدت إلى إعادة تشكيل ملامح الحياة بأكملها، بما فيها الممارسات المهنية، حيث نجد في قلب هذه الثورة يبرز مصطلح الرقمنة، ليس كخيار بل ضرورة ملحة و حتمية تفرضها متطلبات الكفاءة و السرعة و الشفافية.

المطلب الأول: مفهوم الرقمنة، خصائصها و أهدافها

الفرع الأول: تعريف الرقمنة و خصائصها: هناك العديد من تعاريف الرقمنة نذكر منها ما يلي:

1/ لغويا:

- تعريف الرقمنة، فهي تعريب لكلمة "digitization"، وهي مصطلح جديد له عدة مرادفات باللغة الأجنبية منها scanning، digitalization، computerization، digitizing. كما تُرجم إلى لغتنا عدة تراجم مثل "التزقيم"، "التمثيل الرقمي"، "الأرشفة الرقمية والإلكترونية".¹

- الرقمنة² (Digitization) وفقاً للمعاجم الحديثة، منها ما أورده معجم اللغة العربية المعاصرة لأحمد مختار عمر، هي اسم مؤنث مشتق من الجذر (ر ق م) ويعني تحويل المعلومات (صورة، صوت، مستند) إلى صيغة رقمية (أرقام ثنائية 0 و 1) لتتمكن أجهزة الحاسب من معالجتها، وتخزينها، ونشرها، دون تغيير في المحتوى الأصلي، وهي عملية تمثيل للمعلومات عبر لغة الحاسب الآلي.

- الرقمنة في معجم المنجد في اللغة العربية المعاصرة: ، مشتقة من الجذر (ر ق م)، و تعني جعل الشيء رقمياً أو إدخاله في منظومة الحاسوب.³

- تعريف الرقمنة(الجذر أو الرقم) في علوم الحاسب الآلي : تحويل البيانات أو المعلومات أو الصور إلى معطيات رقمية.

¹موقع البديل، الرقمنة في اللغة العربية، مقال نشر في 14 أبريل 2019. اطلع عليه يوم 6 فيفري 2026

²أحمد مختار عمر، معجم اللغة العربية المعاصرة ،

³معلوف، هـ. المنجد في اللغة العربية المعاصرة، دار المشرق، بيروت، طبعة 2000.

يقال: رُقمَن المكتبة و نحوها، حول آلية التعامل اليدوي معها إلى لغة الحاسب الآلي الرقمية بما لديها من قدرة على النقل و الحفظ و الاسترجاع.¹

عرّف قاموس Larousse الفرنسي الرقمنة كالتالي: «ما يتعلّق بالأعداد أو يتمّ باستخدامها أو يُمثّل بها»، أو «ما يُقيّم أو يُعبّر عنه بعدد أو كمية، مثل التفوّق العددي»، وأيضًا «ما يُستخدم لتمثيل المعلومات أو المقادير مادية بواسطة رموز كالأرقام، أو من خلال إشارات ذات قيم منفصلة»، و«ما ينطبق على الأنظمة أو الأجهزة أو الأساليب التي تعتمد هذا النوع من التمثيل المنفصل، على عكس التمثيل التناظري».²

كما عرف قاموس كامبريدج الإنجليزي كلمة «digital» على أنها استخدام نظام إلكتروني يحوّل الأصوات أو الصور إلى أرقام قبل تخزينها أو إرسالها. ويُستنتج من ذلك أن الكلمتين تحمّلان نفس المعنى، وهو تمثيل الصور أو الأصوات بالأرقام. وبعبارة أخرى، فإن مصطلحي «الرقمي» و «digital» يُعدّان مرادفين.

2/ اصطلاحاً: الرقمنة هو مفهوم لا يزال متعدد الأشكال، تختلف دلالاته بين الأكاديميين والممارسين

إن التعريف البسيط للرقمنة يشير إلى عملية تحويل المعلومات التناظرية إلى معلومات رقمية على سبيل المثال، تحويل الصفحات إلى بيانات عن طريق مسح مستند ضوئياً، أو تنزيل تسجيل صوتي. كما أنها العملية التي يتم من خلالها استبدال النماذج التي تُملأ يدوياً بنماذج إلكترونية عبر الإنترنت³

¹ مجمع اللغة العربية بالقاهرة.

² Larousse 2022.

³ Gobble, MaryAnne M., Research technology management : RTM . - Arlington, VA : Industrial Research Inst., ISSN 0895-6308, ZDB-ID 616140-6. - Vol. 61.2018, 4, p. 56-59

كما عرفت وفقًا لـ Küfeoglu وآخرون (2019)، فإن الرقمنة تتضمن إنشاء واستخدام الحلول المعلوماتية في معالجة كميات كبيرة من البيانات التي يتم توليدها في جميع مراحل سلسلة العمليات داخل المؤسسة بهدف تحسين كفاءتها¹.

و يعرف سعيد يقطين الرقمنة بأنها " تحويل المادة من حالتها الورقية أو السمعية أو البصرية إلى الصيغة الرقمية التي تتيح تداولها عبر الوسائط الإلكترونية، وتخزينها ومعالجتها واسترجاعها بسهولة ويسر"². كما يقصد بالرقمنة في مؤسسات المعلومات-عملية تحويل مصادر المعلومات من شكلها التقليدي إلى الشكل الرقمي، ويتم هذا الإجراء بهدف توفير أكبر قدر من مصادر المعلومات المناسبة للمستخدمين. و هي تساهم في حفظ مصادر المعلومات لمدة أطول وكذلك إيصالها إلى أكبر قدر ممكن من المستخدمين في العالم³. يستنتج من هذا التعريف أن عملية الرقمنة تتم عبر مراحل هي:

-تحويل مصادر المعلومات من شكلها التقليدي إلى شكل رقمي، كأن نقوم بتحويل الملفات الخاصة بالمسار النهائي للموظف في الشكل الورقي إلى ملف إلكتروني باستعمال الماسح الإلكتروني ثم تخزينه في جهاز الكمبيوتر، أو في السحابة الرقمية،

-ثم يتم ربط الهيئات الادارية بواسطة الانترنت وإتاحة المجال لكل جهة حسب اختصاصها في إمكانية اطالعها على ملف أي موظف إن استدعى الأمر لذلك.

و يرى "Kanny Terry" أن الرقمنة هي عملية تحويل مصادر المعلومات على اختلاف أشكالها (كتب، دوريات، صور، تسجيلات صوتية...) إلى شكل مقروء آليا بواسطة استخدام الحاسب الآلي عبر النظام الرقمي الثنائي Bits والذي يعد وحدة المعلومات الأساسية لنظام معلومات آلي قائم على استخدام الحاسبات

¹ ELMOUTAOUKIL. A ; BELKACEM. C (2025) «Le digital, le numérique, la transition et la transformation digitales : des définitions en difficulté», Revue Française d'Economie et de Gestion «Volume 6 : Numéro 2»p 768

² سعيد يقطين، "العالم الرقمي وتحولات الكتابة والنشر"، مجلة عالم الفكر، العدد 4، المجلد 39، 2011، ص. 15.

³ مسفرة بنت دخيل الله الخثعمي، مشاريع وتجارب التحويل الرقمي في مؤسسات المعلومات: دراسة للاستراتيجيات المتبعة، مجلة RIST، مجلد 34، العدد 13، 0131، ص ص 18-51 ص 23.

الآلية، وتحويل المعلومات إلى مجموعة من الأرقام الثنائية، يمكن أن يطلق عليها "الرقمنة"، ويتم القيام بهذه العملية باستخدام مجموعة من التقنيات و الأجهزة المتخصصة.¹

3/ خصائص الرقمنة:² تتميز الرقمنة عن غيرها من التكنولوجيات الأخرى بالخصائص التالية:

- **تقليص الوقت:** فالتكنولوجيا تجعل كل الأماكن إلكترونياً متجاورة
- **تقليص المكان:** تتيح وسائل التخزين التي تستوعب حجماً هائلاً من المعلومات المخزنة والتي يمكن الوصول إليها ببسر وسهولة.
- **اقتسام المهام الفكرية مع الآلة:** نتيجة حدوث التفاعل والحوار بين الباحث ونظام الذكاء الصناعي، مما يجعل تكنولوجيا المعلومات تساهم في تطوير المعرفة وتقوية فرص تكوين المستخدمين من أجل الشمولية والتحكم في عملية الإنتاج.
- **تكوين شبكات الاتصال:** تتوحد مجموعة التجهيزات المستندة على تكنولوجيا المعلومات من أجل تشكيل شبكات الاتصال، وهذا ما يزيد من تدفق المعلومات بين المستخدمين والصناعيين وكذا منتجي الآلات ويسمح بتبادل المعلومات مع بقية النشاطات الأخرى.
- **التفاعلية:** أي أن المستعمل لهذه التكنولوجيا يمكن أن يكون مستقبل ومرسل في نفس الوقت فالمشاركين في عملية الاتصال يستطيعون تبادل الأدوار وهو ما يسمح بخلق نوع من التفاعل بين الأنشطة.
- **التزامنية:** وتعني إمكانية استقبال الرسالة في أي وقت يناسب المستخدم فالمشاركين غير مطالبين باستخدام النظام في نفس الوقت 1 .
- **اللامركزية:** وهي خاصية تسمح باستقلالية تكنولوجيا المعلومات والاتصالات والانترنت. مثلاً تتمتع

¹ ربيع نصيرة، حتمية الرقمنة كآلية لتطبيق الإدارة الإلكترونية في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية - المجلد 06 - العدد 02 - ديسمبر 2021، ص 1034-1035

² أحمد مشهور، تكنولوجيا المعلومات وأثرها على التنمية الاقتصادية، المؤتمر العربي الثالث للمعلومات الصناعية والشبكات المنظمة العربية للتربية والثقافة والعلوم، 2003، ص 7

باستمرارية عملها في كل الأحوال، فلا يمكن لأي جهة أن تعطل الانترنت.

- **قابلية التوصيل:** وتعني إمكانية الربط بين الأجهزة الاتصالية المتنوعة الصنع، أي بغض النظر عن

الشركة أو البلد الذي تم فيه الصنع، على مستوى العالم بأكمله.

- **قابلية التحرك والحركية:** أي أنه يمكن للمستخدم أن يستفيد من خدماتها أثناء تنقلاته، أي من أي مكان

عن طريق وسائل اتصال كثيرة من الحاسب الآلي النقال الهاتف النقال الخ....

- **قابلية التحويل:** وهي إمكانية نقل المعلومات من وسيط إلى آخر كتحويل الرسالة المسموعة إلى رسالة

مطبوعة أو مقروءة.

- **قابلية التحرك والحركية:** أي أنه يمكن للمستخدم أن يستفيد من خدماتها أثناء تنقلاته، أي من أي مكان

عن طريق وسائل اتصال كثيرة من الحاسب الآلي النقال الهاتف النقال الخ....

- **قابلية التحويل:** وهي إمكانية نقل المعلومات من وسيط إلى آخر كتحويل الرسالة المسموعة إلى رسالة

مطبوعة أو مقروءة.

- **الجماهيرية:** وتعني إمكانية توجيه الرسالة الاتصالية إلى فرد واحد أو جماعة معينة بدل توجيهها

بالضرورة إلى جماهير ضخمة، وهذا يعني إمكانية التحكم فيها حيث تصل مباشرة من المنتج إلى

المستهلك.

- **الشيوع و الانتشار:** وهو قابلية هذه الشبكة التوسع لتشمل أكثر فأكثر مساحات غير محدودة من العالم،

بحيث تكتسب قوتها من هذا الانتشار المنهجي لنمط المرن العالمية والكونية: وهو المحيط الذي تنشط فيه

هذه التكنولوجيا، حيث تأخذ المعلومات مسارات مختلفة ومعقدة تنتشر عبر مختلف مناطق العالم، وهي

تسمح لرأس المال بأن يتدفق إلكترونياً.

الفرع الثاني: أهداف الرقمنة و أهميتها:

1/ أهداف الرقمنة: تسعى المنظمة من خلال تطبيق الرقمنة إلى الوصول لعدة أهداف وأفاق، أهمها¹:

- الاستثمار المالي في الأدوات الرقمية وتدريب الموظفين
- قيادة جيدة للأدوات الرقمية من أحدث التقنيات
- دراسة عن استخدام أدوات جديدة في جميع قطاعات الأعمال
- التكيف المستمر مع تقنيات التسويق والمبيعات الجديدة عبر الإنترنت
- العلاقات الوثيقة بين رواد الأعمال والزلاء والشركاء والعملاء
- إدارة مشاريع أكثر تعاوناً.

2/ أهمية الرقمنة:² تتجلى أهمية الرقمنة في العناصر التالية:

- توفر الرقمنة الجهد والوقت والتكاليف تحسن الكفاءة التشغيلية
- تعمل على تبسيط الإجراءات للاستفادة من الخدمات وتحسين جودتها
- تسمح للمنظمة بالتوسع والانتشار على نطاق واسع
- يمنح طرق عصرية لتقديم الخدمات
- دعم برامج التطوير الاقتصادي من خلال تسهيل التعاملات بين القطاعين الحكومي والخاص، مما يعزز من العوائد الربحية.
- فتح فتح آفاق استثمارية جديدة من خلال التكامل بين الحكومة الإلكترونية والتجارة الإلكترونية باستخدام التطبيقات والتقنيات الحديثة.

¹حميدوش علي، بوزيد حميد، اقتصاديات الأعمال القائمة على الرقمنة" المتطلبات والعوائد "تجارب دولية"-دروس وعبر"، المجلة اللعبة المستقبل الاقتصادي، العدد 1، المجلد 8، 2020، ص67

²المرجع و الصفحة سابقا

المطلب الثاني: أسباب و متطلبات الرقمنة:

الفرع الأول: أسباب الرقمنة:¹ تتعدد أسباب التحول إلى الرقمنة بتعدد القطاعات، إلا أنها تجتمع حول

هدف اساسي و هو رفع الكفاءة ومواكبة العصر

- رفع الكفاءة التشغيلية والإنتاجية :الأتمتة تقلل من التدخل البشري والخطأ، مما يسرع إنجاز الأعمال ويقلل التكاليف.
- تحسين تجربة العملاء :يلبي التحول توقعات العملاء في الحصول على خدمات سريعة و متاحة على مدار الساعة.
- اتخاذ قرارات مبنية على البيانات :استخدام أدوات تحليل البيانات الضخمة يوفر رؤى دقيقة تدعم التخطيط الاستراتيجي.
- تعزيز التواصل والشراكات :الربط الرقمي يسهل التعاون بين الشركات، الموردين، والموظفين، خاصة في بيئات العمل عن بُعد.
- المرونة ومواجهة الأزمات: أثبتت الرقمنة أهميتها في استمرار المؤسسات خلال الأزمات (مثل جائحة كورونا).
- تقليل الأعباء المالية والإدارية: الرقمنة تساهم في خفض تكاليف الإنفاق والحد من المعاملات الورقية والبيروقراطية.
- توفير الأمان والشفافية: الرقمنة، خاصة في القطاعات المالية والضريبية، توفر مستوى أعلى من الأمان للمستثمرين وتسهل مراقبة المعاملات.

2/ تحسين الكفاءة التشغيلية وتقليل التكاليف:

- أتمتة المهام: استبدال العمليات اليدوية بأنظمة آلية يقلل من الأخطاء البشرية ويوفر الوقت.

¹ <https://elbadilabc-ar.dz> vu a le 04 fevrier 2026

- **خفض المصاريف:** تساهم الرقمنة في تقليل استهلاك الورق والمساحات التخزينية المادية، مما ينعكس إيجاباً على التكاليف والمناخ .

3/ اتخاذ قرارات مبنية على البيانات:

- تتيح الرقمنة جمع كميات هائلة من البيانات وتحليلها بدقة، مما يساعد الإدارة على فهم جمهورها المستهدف وتوقع التوجهات المستقبلية بدلاً من الاعتماد على التخمين .

4/ تحسين تجربة العميل:

- توقعات العملاء في 2027 وما بعدها تميل نحو السرعة والسهولة؛ لذا توفر الرقمنة خدمات ذاتية ومنصات رقمية تتيح الوصول للخدمات في أي وقت ومن أي مكان .

5/ التنافسية والاستدامة:

- **البقاء في السوق:** الشركات التي لا تتبنى الرقمنة تجد صعوبة في منافسة الشركات "الرقمية بالفطرة"
- **المرونة:** أظهرت الأزمات العالمية (مثل الجائحة) أن المؤسسات الرقمية هي الأكثر قدرة على التكيف مع التغيرات المفاجئة والعمل عن بُعد.

6/ الشفافية وتعزيز الثقة الحكومية:

- في القطاع العام، تهدف الرقمنة إلى "عصرنة الإدارة" وتبسيط الإجراءات البيروقراطية، مما يعزز ثقة المواطن في المؤسسات ويضمن العدالة في الوصول للخدمات (مثل الصحة والتعليم).

7/ التطور التقني المتسارع:

- ظهور تقنيات مثل الذكاء الاصطناعي (AI) ، إنترنت الأشياء (IoT) ، و الحوسبة السحابية جعل من الرقمنة "حتمية استراتيجية" لا رجعة عنها للاستفادة من هذه الأدوات في تطوير المنتجات .

الفرع الثاني: متطلبات الرقمنة: تسعى المؤسسات لتحويل أعمالها و إدارتها إلى الشكل الرقمي، وهو أمر يحتاج بدوره إلى إمكانيات ومتطلبات ينبغي توفيرها للقيام بعملية التحول الرقمي، ومن أهم هذه المتطلبات ما يلي:

1/ **القوى البشرية المؤهلة :** إن عملية الرقمنة لا تهتم بجهود فردية و إنما تحتاج إلى تكاثف الكثير من الجهود من مختلف الأشخاص المسؤولين داخل المؤسسات، وكذا موظفي مختلف الأقسام داخل المؤسسة، فكلما كان الموظفون مؤهلين و يمتلكون مهارات وكفاءات عالية، كان ذلك مساعدا في إتمام مشاريع الرقمنة بجودة عالية.

2/ **توفر البنية التحتية للاتصالات:** إذ لابد من العمل على تطوير مختلف شبكات الاتصالات بما يتوافق مع بيئة التحول التي تستدعي شبكة واسعة، ومستوعبة للكم الهائل من الاتصالات دون إهمال التجهيزات التقنية الأخرى من معدات وأجهزة وحاسبات آلية، و محاولة توفيره وإتاحته للأفراد والمؤسسات.

3/ **تطوير التنظيم الإداري و الخدمات و المعاملات الحكومية وفق تحويل تدرجي:** بإعادة تنظيم الجوانب و المحددات الهيكلية، ومختلف الوظائف الحكومية، بما يجعلها تتسجم ومبادئ الإدارة الالكترونية مثل (إلغاء إدارات، استحداث إدارات جديدة تسير التطور التكنولوجي).

4/ **وضع التشريعات القانونية اللازمة لتطبيق الرقمنة:** قبل تطبيق الرقمنة لابد من تحديد الإطار القانوني الذي يقر بالتحول الالكتروني وأثناء التطبيق أي تكملة للنقائص والفراغ القانوني اللازم، والذي يمكن أن يظهر في أي مرحلة من مراحل التحول، وبعد التطبيق بوضع قواعد قانونية ضامنة لأمن المعاملات الالكترونية و تحديد الإجراءات العقابية الخاصة بفئة المتورطين في جرائم الإدارة الالكترونية.

5/ **صناع المعرفة :** إذ تمثل القيادات الرقمية و كل ما يشمل الرأس مال الفكري و المديرون و المحللون للموارد المعرفية، فدور صناع المعرفة يكمن في محاولة خلق ثقافة معرفية جديدة داخل الإدارة الالكترونية

عن طريق تعبري طرق التفكير، وترقية أساليب العمل الإداري وفق ما يتمتعون به من خبرات ومعارف في مجال المعلوماتية.

المطلب الثالث: التحول الرقمي في المؤسسات:

الفرع الأول: مفهوم التحول الرقمي: يعد التحول الرقمي من المفاهيم الحديثة التي فرضت نفسها في مختلف المجالات، نتيجة للتطور التكنولوجي الحاصل، غير أن هذا المصطلح ما زال يفتقر إلى تعريف موحد، حيث تعددت التعريفات التي قدمها الباحثون والمختصون حول مضامينه وحدوده.

1/ تعريف التحول الرقمي:

يعرف التحول الرقمي بأنه " عملية تكامل التكنولوجيا الرقمية في جميع جوانب العمل والحياة اليومية بهدف تحسين الأداء وإضافة قيمة جديدة، حيث يتمثل التحول الرقمي في استخدام الأدوات والتقنيات الحديثة مثل الذكاء الاصطناعي، وإنترنت الأشياء، والبيانات الضخمة، والحوسبة السحابية، لتحويل العمليات والخدمات والمنتجات، مما يؤدي إلى ابتكار نماذج عمل جديدة وتحسين التجارب وال خدمات المقدمة للعملاء أو المستفيدين.¹

وجاء في تعريف آخر أن التحول الرقمي " يشير إلى عملية تغيير أساليب العمل والممارسات في المؤسسات والمنظمات باستخدام التقنيات الرقمية، ويتضمن هذا التغيير تغيرات في الهيكل التنظيمي، والعمليات، والثقافة المؤسسية والعلاقة مع العملاء والشركاء.²

¹فيولا مخزوم، قيادة التحول الرقمي في الفصول الدراسية: دور المعلم في عصر التكنولوجيا، المركز الديمقراطي العربي للدراسات الإستراتيجية والاقتصادية والسياسية، ألمانيا/برلين، 2024 ، ص 5 .

²أحمد قاسم الجمال وآخرون، التحول الرقمي في مؤسسات التعليم العالي العربية: الواقع، التحديات، والمقاربات المستقبلية، دار الكتب الوطنية، الرابطة العربية للعلوم الاجتماعية والإنسانية التابعة لاتحاد مجالس البحث العلمي العربية، بنغازي- ليبيا، سبتمبر 2023 ، ص

كما عرف ان التحول الرقمي هو " عملية انتقال مؤسسة من شكل تقليدي إلى شكل رقمي، أي التحول من معاملات ورقية إلى معاملات رقمية، القائم على تغيير مرتبط بتطبيق التكنولوجيا الحديثة بمختلف مجالات عمل المؤسسة لتحقيق أهدافها في الوقت المناسب بأقل كلفة ممكنة"¹

وقد جاء في بعض الدراسات أن التحول الرقمي " عملية تُحدث تغييرا جذريا في نموذج الأعمال، وتبتكر طرقا جديدة لتحقيق الأرباح من المنتجات والخدمات، كما يساهم بشكل كبير في تحقيق وفورات طويلة الأمد في التكاليف الإنتاجية، ويمهد الطريق لعملية التحسين الرقمي."²

2/ فوائد التحول الرقمي: لا يُعد التحول الرقمي مصطلحاً مستحدثاً في قطاع الأعمال، بل هو توصيف لمرحلة انتقالية رقمية جوهرية تمكّن المؤسسة من العمل وفق نموذج حديث. نتيجة لهذا التحول الجذري في نمط العمل وثقافة المؤسسة، تتحقق مكاسب ملموسة على مستوى الأداء والأعمال.

و هذه بعض مزايا فوائد التحول الرقمي.

زيادة الإنتاجية: تسهم تقنيات مثل الحوسبة السحابية في تقليل الوقت وتحسين الكفاءة التشغيلية في مختلف مجالات الأعمال. على سبيل المثال، يسهّل استخدام روبوت محادثة سحابي ضمن أنظمة الملفات وصول الموظفين إلى إجابات تتعلق بالاستفسارات التجارية. و بنفس الطريقة، يُسهم تحليل بيانات الأعمال القائمة من خلال تعلم الآلة في الوصول إلى تنبؤات دقيقة وتحقيق الأهداف المؤسسية بسرعة أكبر.

¹ معاوية فهد داود القواسمي، التحول الرقمي في المصارف الإسلامية: دراسة تطبيقية على المصارف الإسلامية في دولة فلسطين، الطبعة 2، دار الجنان للنشر والتوزيع، الأردن، 2025، ص 15

² Jocko Lozic & Katerina Fotova Čiković, 'Digital Transformation: The Fundamental Concept of Transformation of Business Activities, Zagreb, 2024, p. 923

تحسين تجربة العملاء: أصبح العملاء اليوم يتوقعون توفر الخدمة على مدار الساعة من خلال قنوات رقمية متنوعة، مع واجهات سهلة الاستخدام متوافقة مع الأجهزة المحمولة. من بين أهداف التحول الرقمي التي تنعكس بشكل مباشر على تجربة العملاء:

- تطوير تطبيقات وتدفقات عمل للأجهزة المحمولة
- اعتماد تقنية الاستشعار الذكي لأجل تتبع الطلبات وتنفيذها بطريقة أسرع
- التواصل الفوري مع العملاء عبر استخدام روبوتات المحادثة المدعومة بالذكاء الاصطناعي
- تحسين دعم العملاء والخدمة باستخدام عمليات سير عمل الأتمتة

تحسين تجربة المستخدم: يتيح ذلك للموظفين في المؤسسة تقديم تجربة تتماشى مع توقعات العملاء واحتياجاتهم. عبر إنشاء أنظمة داخلية تمكّن الموظفين من العمل بكفاءة أعلى، والحد من الأخطاء اليدوية، والتواصل بسرعة مع الأنظمة والخدمات والأشخاص المناسبين، تعزز المؤسسات تجربة المستخدم¹.

يسهم تعزيز تجربة المستخدم في رفع مستوى تفاعل الموظفين ورضاهم، والحد من دورانهم الوظيفي، وجعل المؤسسة وجهة مفضلة للموظفين الجدد.

خفض التكاليف التشغيلية: يسهم الاستثمار في التقنيات الرقمية بشكل ملحوظ في تقليل النفقات التشغيلية الجارية. عبر تحسين العمليات التشغيلية القائمة، يسهم التحول الرقمي في خفض تكاليف صيانة المعدات، وخدمات النقل والتوصيل، واستخدام الطاقة، والنفقات البشرية، ودعم العملاء.

يمكن تحقيق وفورات في التكاليف عبر ما يلي:

- إلغاء بعض مهام سير العمل المحددة كثيفة الموارد أو استبدالها

¹ <https://aws.amazon.com/what-is/digital-transformation> vu le 23 janvier 2026

- خفض التكاليف المتعلقة بالبنية التحتية والمعدات عبر الاستعاضة عنها بخدمات مُدارة وتقنيات الحوسبة السحابية

- تشغيل المهام تلقائيًا عبر تقنيات مثل أتمتة سير العمل، والذكاء الاصطناعي (AI) ، وأجهزة الاستشعار الذكية، والأجهزة المتصلة

التفوق على المنافسين: عبر الابتكار في الأعمال، تكتسب المؤسسات القدرة على التميز وتحقيق التفوق على المنافسين في مجالها. بفضل زيادة الإنتاجية، وانخفاض التكاليف التشغيلية، وتحسين تجربة العملاء والمستخدمين، تعزز الشركة قدرتها على تحقيق أهدافها الرئيسية بكفاءة أكبر. حيث يُساهم ذلك في تحسين النتائج وتجارب الموظفين والشركاء والعملاء¹.

الفرع الثاني: علاقة مفهوم التحول الرقمي بالرقمنة: تعتبر الرقمنة كخطوة أولى و الأساس الذي يبنى عليه التحول الرقمي، حيث توفر البيانات الرقمية والبنية التحتية اللازمة، بينما تركز الرقمنة على الجانب التقني، يتطلب التحول الرقمي تغييرات جوهرية في الثقافة المؤسسية واستراتيجيات العمل لتحقيق أقصى استفادة من التكنولوجيا الرقمية².

رغم أن الرقمنة و التحول الرقمي مرتبطان ببعضهما، إلا أن الفرق بينهما يتضح من خلال النقاط

التالية:

- الرقمنة تركز على تحويل البيانات فقط، بينما التحول الرقمي يركز على تحويل الأنشطة والعمليات.
- الرقمنة هي خطوة تمهيدية، أما التحول الرقمي فهو استراتيجية متكاملة تشمل التغيير الثقافي التشغيلي.

¹ <https://aws.amazon.com> مرجع سبق ذكره

² بن أحمد، فاطمة الزهراء، وبن أحمد نادية، " التحول الرقمي في الجزائر: الواقع والتحديات ، المجلة الجزائرية المالية العامة، المجلد 15 ، العدد 01 ،

الجزائر، 2025 ، ص 503-504

- في الرقمنة، الأدوات تُستخدم لتحسين الكفاءة، لكن في التحول الرقمي تُستخدم لإعادة تعريف كيفية تقديم القيمة.

لذلك، لا يمكن الوصول إلى تحول رقمي ناجح دون المرور أولاً بمرحلة الرقمنة، لكنها تظل خطوة محدودة إذا لم تتبعها رؤية شاملة لتطوير المؤسسة¹.

كما يمكن تلخيص الفرق بين المصطلحين في الجدول التالي:

جدول رقم 01 : الفرق بين التحول الرقمي و الرقمنة

عنصر الاختلاف	التحول الرقمي	الرقمنة
التعريف	هو نهج تتبعه المؤسسة ينطوي على الجمع بين التقنيات الرقمية بهدف إحداث تغييرات أساسية في عملياتها وثقافتها وطريقة عمل الموظفين وتقديم قيمة للعملاء، عن طريق إنشاء عمليات جديدة أو تعديل العمليات القائمة	هي عملية الانتقال إلى العمل الرقمي الذي يعتمد على استخدام التقنيات الرقمية لتغيير نموذج الأعمال وتوفير إيرادات وفرص جديدة، عن طريق تحويل البيانات الموجودة على الورق إلى أشكال رقمية، دون تحويل العمليات الأساسية
الأدوات	تتمثل الأدوات المستخدمة في تنفيذه في: الذكاء الاصطناعي، التعلم الآلي، إنترنت الأشياء، الحوسبة السحابية، الروبوتات، منصات تحليل البيانات الضخمة، أنظمة إدارة علاقات العملاء، تقنيات blockchain، الواقع الافتراضي والمعزز.	يتم تنفيذها باستخدام أدوات تشمل الماسحات الضوئية، نظم إدارة الوثائق، برامج تحويل البيانات، البرمجيات السحابية، الأجهزة الذكية والمستشعرات، برامج الأتمتة، أنظمة إدارة المحتوى، أجهزة الحفظ الرقمي.
	تحسين كفاءة وفعالية المؤسسة باستخدام التكنولوجيا الرقمية، مما يساعد على توفير التكاليف وتحسين الجودة	تقليل الوقت المُستغرق في البحث عن المعلومات، وتقليل الأخطاء البشرية،

¹مصطفى قطب، الرقمنة والتحول الرقمي: المفهوم، الفرق، والأثر على المؤسسات الحديثة، مقال منشور على موقع أكاديمية مهارات التخطيط

الهدف	وزيادة الأرباح.	وخفض التكاليف المرتبطة بالطباعة والتخزين الورقي.
النطاق	تتم هذه العملية على نطاق واسع لأنها تغطي جميع جوانب المؤسسة وأنظمتها	تتم هذه العملية على نطاق ضيق لأنها تنطوي على تحويل البيانات فقط
الأمثلة	وضع استراتيجية عمل رقمية، إنشاء منتجات وخدمات رقمية جديدة، إصلاح البنية التحتية لتكنولوجيا المعلومات للمؤسسة	مسح الوثائق الورقية في الملفات الرقمية، تحويل التسجيلات الصوتية التناظرية إلى أشكال رقمية، تحويل الملاحظات المكتوبة بخط اليد إلى نص مكتوب باستخدام برنامج التعرف البصري على الحروف
التحديات	هناك عدة مخاطر مرتبطة بالتحويل الرقمي أبرزها ارتفاع تكاليف تنفيذ تلك العملية، مقاومة التغيير لعدم قدرة الموظفين على تبني أساليب عمل جديدة، صعوبة التنفيذ واستغراقه وقتاً طويلاً.	فقدان البيانات في حال عدم دعمها بشكل كافٍ، احتمالية تعرض البيانات الرقمية للهجمات الإلكترونية، ارتفاع تكاليف تحويل البيانات وتخزينها في شكلها الرقمي

المصدر: الفرق بين التحويل الرقمي والرقمنة والأتمتة والتكنولوجيا، <https://bakkah.com/ar/knowledge-center>

المبحث الثاني: الرقمنة في البنوك التجارية:

يواجه القطاع المصرفي تحديات متسارعة فرضتها العولمة المالية و التقدم التكنولوجي الهائل، مما جعل الرقمنة البنكية المسار الوحيد لضمان البقاء و الاستمرارية في سوق تتسم بالمنافسة، و تسارع في تغير احتياجات و طلبات زبائنهم.

المطلب الأول: المعاملات التجارية البنكية و أنواعها

إنه لمن الصعب حصر جميع المعاملات التجارية المصرفية التي أصبحت تقدمها البنوك نظرا لتعددتها وتنوعها وأصبحت خاضعة لتطورات مستمرة نتيجة استخدام الوسائل التكنولوجية في تقديم الخدمات المصرفية.

الفرع الأول: مفهوم المعاملات التجارية البنكية

1/ تعريف المعاملات التجارية البنكية:

تعرف العمليات البنكية بأنها تلك العمليات التي تقوم بها المؤسسات البنكية في معاملاتها مع العملاء والموجهة والمقدمة لهم على شكل خدمات بنكية، منها ما يقدم دون مقابل مثل العمليات البنكية القاعدية كفتح وإقفال الحسابات ومنح دفتر الشيكات ودفتر الادخار، ومنها ما يقدم بمقابل عمولة تقتطعها المؤسسة البنكية مثل العمليات البنكية المتعلقة بالتجارة الخارجية.¹

وفقا لنص المادة 66 من الأمر ، 11/03 تتضمن العمليات البنكية تلقي الأموال من الجمهور وعمليات القرض وكذا فتح الحسابات البنكية ووضع وسائل الدفع تحت تصرف الزبائن وإدارة هذه الوسائل وعمليات تحويل الأموال.²

أما وفقا لنص المادة 6 من الأمر 10/04 المعدل والمتمم للأمر رقم ، 03/11 ونص المادة 72 من الأمر 03/11 فيمكن للمؤسسات البنكية القيام بجميع العمليات ذات العلاقة بنشاطها البنكي، مثل عمليات الصرف وعمليات على الذهب والمعادن الثمينة والقطع المعدنية الثمينة، وتوظيف القيم المنقولة كالسندات والأسهم وكل منتج مالي، واكتتابها وشرائها وتسييرها وحفظها وبيعها، إضافة إلى الاستشارة والمساعدة في مجال تسيير الممتلكات المنقولة والغير منقولة، والاستشارة المالية والتسيير المالي والهندسة المالية وبشكل عام كل الخدمات الموجهة لتسهيل إنشاء المؤسسات والتجهيزات وإنماءها.³

¹ الطاهر لطروش، تقنيات البنوك، الطبعة الرابعة، ديوان المطبوعات الجامعية، الجزائر، 2005 ص 21.

² نظام بنك الجزائر رقم 09/03 مؤرخ في 26 ماي، 2009 المحدد للقواعد العامة المتعلقة بشروط البنوك المطبقة على العمليات المصرفية، الجريدة الرسمية للجمهورية الجزائرية، المطبوعة الرسمية للأمانة العامة للحكومة، الجزائر، 2009 العدد، 53 المادة 2.

³ نظام بنك الجزائر رقم 13/01 مؤرخ في 8 أفريل، 2013 المحدد للقواعد العامة المتعلقة بالشروط البنكية المطبقة على العمليات المصرفية، الجريدة الرسمية للجمهورية الجزائرية، المطبوعة الرسمية للأمانة العامة للحكومة، الجزائر، 2013 العدد، 29 المادة 10 والمادة 11.

2/ الخصائص الأساسية المميزة للعمليات البنكية:¹ تتميز العمليات البنكية بخصائص أساسية تتمثل في:

- تعتبر العمليات البنكية لدى معظم التشريعات الحديثة من الأعمال التجارية بحسب الموضوع، فهي عمليات ذات طابع تجاري.
- العمليات البنكية هي أعمال انفردت بها المؤسسات البنكية منذ القدم، فهي وليدة العرف والعادات المصرفية.
- العمليات البنكية غير ملموسة وغير قابلة للتخزين و لا يمكن إعدادها وتحضيرها مسبقا، وبالتالي يعطيها صفة الخدمات.
- تقوم العمليات البنكية على الثقة بين المؤسسة البنكية وعملائها، وذلك بعد دراسة ومعرفة هذا الأخير من طرف البنك، مع إعطاء البنك أهمية لشخصية العميل، وإعطاء العميل أهمية لشخصية البنك، فالعمليات البنكية تقوم على الاعتبار الشخصي.
- نظرا للانتشار الواسع للمؤسسات البنكية خارج حدود دولها في إطار العولمة المالية، فقد أصبحت الكثير من العمليات البنكية تشترك في أحكامها العديد من الدول وهو ما حتم توحيد نصوص النماذج الخاصة بها، خاصة في ظل تمويل المشاريع الاقتصادية الدولية الخاصة بالشركات المتعددة الجنسيات وفي ظل تمويل التجارة الخارجية، وبالتالي فالعمليات البنكية هي ذات طابع دول

¹ بوكعبان عكاشة، القانون المصرفي الجزائري في ضوء الاجتهاد القضائي للمحكمة العليا ومجلس الدولة، دار الخلدونية، الجزائر، 2017، ص

الفرع الثاني: أنواع المعاملات التجارية البنكية¹

1/ قبول الودائع: تتمثل في مختلف الحسابات والودائع التي تترك لدى البنوك وهي:

- **الودائع تحت الطلب:** تقبل المصارف التجارية هذا النوع من الودائع وتحفظ بنسبة محددة كاحتياطي قانوني عليها، ويحق لأصحاب هذه الودائع سحبها في أي وقت، ولا تدفع عليها فوائد .
- **الودائع لأجل:** هي الودائع التي لا تعطي لأصحابها الحق في السحب منها، إلا بعد إخطار المصرف أو انقضاء مدة محددة، مقابل الحصول على فائدة.

- **الودائع الادخارية:** هي الودائع التي يقوم الزبائن بإيداعها لدى المصرف في صورة مدخرات، ويعطى أصحابها دفاتر تقيّد فيها دفعات الإيداع والسحب، وهذا النوع من الودائع عادة ما يبقى ثابتاً 2 لدى المصرف لفترة طويلة من الزمن لذلك يدفع المصرف عنه فوائد للمودعين.

- 2/ منح القروض:** تعتبر عملية منح القروض من الخدمات الرئيسية التي تقدمها المصارف التجارية، لذلك تقوم إدارة المصارف برسم سياستها الائتمانية، بما يحقق حسن وسلامة استخدام الأموال المتاحة لها مع تحقيق عائد مناسب، ويتم منح القروض مقابل أسعار فائدة محددة وضمانات معينة.

- 3/ فتح الاعتماد:** فتح الاعتماد هو تعهد المصرف بأن يضع تحت تصرف الزبون مبلغ معين من المال أو أي أداة أخرى على أن يكون ذلك سواء لأجل محدد أو لأجل غير محدد.

¹العربي حسيبة، جودة الخدمات المصرفية في الجزائر من وجهة نظر الزبون، مذكرة مقدمة ضمن متطلبات نيل شهادة الماجستير في العلوم التجارية تخصص: تسويق العمليات المالية والمصرفية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير قسم العلوم التجارية، جامعة الجزائر 3، 2015-

4/ **فتح الإعتمادات المستندية:** الاعتماد المستندي هو: "وسيلة دفع مضمونة وواسعة الاستعمال في التجارة الدولية، وهو تعهد مكتوب من قبل المصرف فاتح الاعتماد يعطى للمستفيد (المصدر) بناء على طلب وتعليمات المشتري (المستورد) لتنفيذ دفع مبلغ معين خلال فترة محددة مقابل مستندات.

5/ **إصدار خطابات الضمان:** تقوم المصارف بإصدار خطابات الضمان لزمائنها، وخطاب الضمان هو عبارة عن: "تعهد المصرف بدفع مبلغ إلى المستفيد لا يتجاوز حد معين لحساب طرف ثالث، لغرض معين، وقبل وقت معين"، وتحصل المصارف على عمولات نظير إصدار خطابات الضمان، مع تحمل مسؤولية تنفيذ التعهد بالدفع.

6/ **الكفالة:** حيث أن تقديمها يمثل البديل المقبول عن النقد المطلوب دفعه من المكفول تأمينا للالتزام بعمل معين. وعلى ذلك فإن الكفالة في العرف المصرفي هي: "تعهد قطعي يصدر عن المصرف بناء على طلب الزبون، يتعهد المصرف بموجبه بدفع مبلغ بحد لا يتجاوز قيمة الكفالة خلال مدة محددة وأن هذا الدفع غير معلق على شرط ما لم تنص الكفالة في متنها على شرط يعلق الدفع بتنفيذه .

7/ **خصم الكمبيالات لحساب الزبائن:** يعتبر خصم الأوراق التجارية أحد أهم أنواع التسهيلات الائتمانية المباشرة التي يمنحها المصرف لزمائنه، بغرض تشجيع الإنتاج القومي، وتنشيط التجارة الداخلية.

8/ **خدمات أخرى:** هي كل الخدمات التي تقدمها البنوك التجارية يوميا لزمائنها مقابل حصولها على عمولات مثل:

- صرف الشيكات المسحوبة على البنك بالعملة المحلية والأجنبية.

- تحصيل الشيكات لصالح زبائن البنك.

- فتح الحسابات بالعملة المحلية والأجنبية.

- إصدار الشهادات التي تثبت القيام بالعمليات المالية مع العملاء.

3/ **العمليات المتعلقة بالاستثمار في الأوراق المالية:**

- الاستثمار في الأوراق المالية إدارة محافظ الأوراق المالية لصالح العملاء المساهمة في رؤوس أموال المشاريع الاستثمارية، خدمات الهندسة المالية، خدمات أمناء الاستثمار لصالح العملاء.
- تقديم الاستثمارات المالية، دراسة الجدوى الاقتصادية للمشاريع لصالح العملاء وتجدر الإشارة إلى أن هذه الخدمات جد محدودة في البنوك الجزائرية نظرا لضعف التعامل بالأدوات المالية الاستثمارية وضعف السوق المالي أي البورصة.

المطلب الثاني: أهمية الرقمنة في البنوك و متطلباتها

تعد رقمنة القطاع المصرفي من أهم التحولات التي يشهدها النظام المالي العالمي في العصر الحديث، حيث تعتمد المؤسسات المصرفية بشكل متزايد على التكنولوجيا المالية (Fin Tech) لتقديم خدمات أكثر كفاءة، أمانا، وسرعة، وتؤثر الرقمنة على مختلف جوانب العمل المصرفي، بدءا من إدارة الحسابات والمدفوعات، وصولا إلى التحليلات المالية المتقدمة باستخدام الذكاء الاصطناعي.

الفرع الأول: أهمية الرقمنة في البنوك: تعتبر رقمنة المجال البنكي أمرا بالغ الأهمية خاصة في السنوات الأخيرة، وذلك لما توفره من فوائد كبيرة للبنوك و العملاء على حد سواء. من أهم فوائد رقمنة القطاع البنكي¹:

- 1/ **تحسين الكفاءة والسرعة:** تتيح الرقمنة للبنوك تنفيذ المعاملات المصرفية بسرعة ودقة عالية، مما يقلل من وقت الانتظار ويزيد من إنتاجية الموظفين.
- 2/ **الوصول إلى الخدمات المصرفية في أي وقت ومن أي مكان:** من خلال التطبيقات المصرفية والخدمات الإلكترونية، يمكن للعملاء إجراء المعاملات في أي وقت دون الحاجة إلى زيارة الفروع .

¹مرسي خولة- هاجر موساوي، تطبيق التحول الرقمي كآلية لتحسين أداء البنوك: دراسة حالة متعددة الجنسيات- مجلة المنهل الاقتصادي، جامعة الشهيد حمه لخضر-الوادي- المجلد، 06 العدد، 01 جوان، 2023، ص 536-5

3/ خفض التكاليف: يساعد التحول الرقمي البنوك في تقليل التكاليف التشغيلية مثل التكاليف المرتبطة بالورق والبنية التحتية التقليدية، مما يعزز الكفاءة الاقتصادية.

4/ تعزيز الأمان: باستخدام تقنيات مثل التشفير والمصادقة الثنائية، يمكن للبنوك توفير بيئة آمنة للمعاملات المالية وحماية بيانات العملاء من المخاطر.

5/ توسيع قاعدة العملاء: تتيح الرقمنة للبنوك الوصول إلى شرائح أوسع من العملاء، بما في ذلك الفئات التي قد لا تكون قادرة على زيارة الفروع بشكل منتظم.

6/ تحليل البيانات واتخاذ قرارات أفضل: تمكن الرقمنة من جمع وتحليل البيانات بشكل أكبر، مما يساعد البنوك في فهم احتياجات عملائها بشكل أفضل وتقديم خدمات مخصصة.

7/ الابتكار في الخدمات المالية: تفتح الرقمنة المجال لتطوير منتجات وخدمات مالية مبتكرة مثل الدفع الرقمي، القروض الإلكترونية، والخدمات المصرفية عبر الهاتف المحمول.

و بالتالي، فإن رقمنة القطاع البنكي تمثل خطوة استراتيجية مهمة نحو تحسين الأداء المصرفي وتقديم خدمات أكثر توافقاً مع احتياجات العملاء الحديثة.

الفرع الثاني: متطلبات الرقمنة في البنوك التجارية: تتطلب رقمنة البنوك في الجزائر تحديثاً جذرياً للبنية

التحتية التكنولوجية، وإطاراً قانونياً مرناً (قانون النقد والمصرفي 09-23)، وتعزيز الأمن السيبراني لحماية

البيانات. تشمل المتطلبات الأساسية توفير منصات دفع إلكتروني حديثة، واعتماد الحلول الذكية، وتدريب

العنصر البشري، مع ضرورة الحصول على تراخيص من بنك الجزائر، لا سيما للبنوك الرقمية المتخصصة .

1/ الإطار القانوني والتنظيمي: ضرورة الامتثال لقانون النقد والمصرفي الجديد الذي يمنح التراخيص للبنك

الرقمي ويوفر إطاراً لتأسيس البنوك الافتراضية.

2/ البنية التحتية التكنولوجية (التقنية): تحديث الأنظمة المعلوماتية للبنك، توفير شبكات اتصالات سريعة

وآمنة، واعتماد تكنولوجيات الإعلام والاتصال الحديثة.(TIC)

3/ الأمن السيبراني: تدابير صارمة لحماية البيانات، البنية التحتية المادية وغير المادية، وضمان سلامة المعاملات الرقمية.

4/ المنتجات والخدمات الرقمية: إطلاق خدمات مصرفية عبر الإنترنت (E-banking)، وتطبيقات الهاتف، الصيرفة الإلكترونية، وخدمات الصيرفة الإسلامية الرقمية.

5/ العنصر البشري والثقافة الرقمية: تأهيل وتدريب الموظفين على استخدام التكنولوجيات الحديثة ونشر الوعي لدى العمال لاستخدام القنوات الرقمية.

6/ المتطلبات المالية والشكلية: الحصول على ترخيص من بنك الجزائر (مجلس النقد والمصرفي)، وقد تشمل الشروط زيادة رأس المال للبنك الرقمي لضمان استقراره

المطلب الثالث: الخدمات المصرفية الرقمية في البنوك التجارية

الفرع الأول: تعريف الخدمات المصرفية الرقمية وخصائصها:

1/ تعريف الخدمات المصرفية الرقمية:¹

تعرف بأنها خدمات مصرفية عبر الانترنت أي قائمة على شبكة الويب العالمية حيث يمكن للمستخدمين الوصول على حساباتهم المصرفية باستخدام الانترنت ويمكنهم إجراء معاملات مالية كدفع فواتير الكهرباء ومراجعة كشف حساباتهم المصرفية الخاصة على مدار 24 ساعة.

و قد تم تعريف الخدمات المصرفية الرقمية في إطار الخدمات المالية الرقمية كما يلي:

¹ سندس بن عبد الله، الخدمات المصرفية الرقمية ودورها في ربحية البنوك التجارية الجزائرية دراسة حالة البنك الوطني الجزائري خلال الفترة 2017-2021، مجلة الاقتصاديات المالية البنكية و إدارة الأعمال، المجلد 13 / العدد 01 (2024)، ص92

"بأنها تلك الخدمة المالية التي تشمل خدمات معلوماتية وخدمات عبر شبكة الانترنت"

كما تعرف بأنها تلك الخدمات التي توفر القدرة على إجراء المعاملات المصرفية من المنزل (أو المكتب) باستخدام الهاتف أو التلفزيون أو الكمبيوتر الشخصي، مثل مراجعة أرصدة الحسابات الجارية، ودفع الفواتير، فتح حسابات جديدة، والتقدم بطل الحصول على قروض...

2/ **خصائص الخدمات المصرفية الرقمية:**¹ تتميز الخدمات المصرفية الرقمية عن التقليدية بمجموعة من الخصائص أهمها:

- **ليس لها قيود زمنية (اختصار الزمن) :** تتميز بقدرتها للوصول إلى قاعدة أوسع من الزبائن، كما توفر الخدمة في أي وقت وعلى مدار الأسبوع، إضافة إلى سرية المعاملات والتي تزيد من ثقة الزبون.
- **سهولة الاتصال :** يسمح استخدام الوسائل الالكترونية والرقمية كالهاتف والانترنت سهولة اتصال الزبون بالبنك والتعرف على الخدمات التي يقدمها عبر الانترنت.
- **خفض التكاليف :** تعتبر تكاليف تقديم الخدمة الرقمية منخفضة مقارنة بتقديم الخدمات التقليدية.
- **سرعة التحديث :** خاصية التحديث تعني القدرة على تكوين مصادر معلومات من خلال تحديث المعلومات المجمعة من طرف الزبائن ومن التفاعلات التي تحدث بين الزبون والبنك بشكل متواصل، مما يعزز كفاءة وفعالية قواعد البيانات.

الفرع الثاني: أنواع الخدمات المصرفية الرقمية:

1/ الخدمات البنكية الإلكترونية الائتمانية:² و تتمثل في:

¹المرجع السابق، ص 94

²دريد كامل آل شبيب، إدارة العمليات المصرفية، الطبعة الأولى، دار المسيرة، الأردن، 2015، ص 393

- توفير وسائل الدفع الإلكترونية: وتتمثل في توفير وإصدار وسائل دفع إلكترونية تتوب عن وسائل الدفع التقليدية، وتتمثل عموماً في: الشيك الإلكتروني؛ بطاقات القيمة المخزنة "البطاقات المغناطيسية"؛ النقدية الإلكترونية؛ بطاقات الخصم؛ بطاقات الائتمان؛ النقود الإلكترونية .

- الكمبيالة الإلكترونية: هي صك معالج إلكترونياً متفق عليه مسبقاً وفقاً لشكل معين يتضمن أمراً من الساحب عن طريق مؤسسته البنكية إلى المؤسسة البنكية المسحوب عليها تدفع مبلغاً معيناً في تاريخ معين أو قابل للتعيين أو بمجرد الاطلاع لأمر المستفيد .

2/ العمليات البنكية الإلكترونية الغير الائتمانية:¹ و تتمثل في:

- فتح وتسيير الحسابات البنكية الإلكترونية: وهي خدمات بنكية إلكترونية تتم عن طريق المواقع الإلكترونية الخاصة بالمؤسسات البنكية.

- المقاصة الإلكترونية: هي عملية تبادل المعلومات بوسائل إلكترونية من خلال مركز المقاصة الإلكترونية في البنك المركزي وتحديد صافي الأرصدة الناتجة عن هذه العملية في وقت محدد، هذه الخدمة تخص شبكات المؤسسات البنكية المرخصة لها قانوناً ضمن الجهاز البنكي .

- التحويل الإلكتروني للأموال: وهو نظام يسمح بتحويل الأموال من حساب العملاء الطالبيين للخدمة إلى حساب أطراف أخرى بطريقة إلكترونية، وقد يكون الطرفان من نفس المؤسسة البنكية أو من مؤسستان بنكيتان مختلفتان، فهي خدمة سريعة و متطورة.

3/ العمليات البنكية الإلكترونية الخارجية:² و تتمثل في:

¹المرجع السابق، ص 394

²دريد كامل آل شبيب، مرجع سبق ذكره، ص 394

- **منح الاعتماد المستندي الإلكتروني:** للاعتماد المستندي الإلكتروني نفس خصائص الاعتماد المستندي التقليدي، ما عدا أن المستندات التي يتعامل بها تتخذ الشكل الإلكتروني، غير أن هذه المستندات الإلكترونية لا تختلف في محتواها عن المستندات الورقية لمعاملات التجارة الدولية، كما أن التواصل ما بين الأطراف و إرسال الوثائق و المستندات الإلكترونية يكون عبر الوسائط الإلكترونية .

- **التحويل الآلي للمدفوعات الدولية عبر نظام SWIFT :** هي شبكة عالمية موحدة للاتصالات المالية الآمنة بين المؤسسات البنكية عبر العالم، يتم من خلالها تحويل الأموال، فهي توفر لمستخدميها السرعة والأمان في إنجاز المعاملات .

- **الاستلام السريع للأموال:** الاستلام السريع للأموال من باقي العالم من خلال نظام ويسترن يونيون لتحويل الأموال، بحيث تقوم المؤسسات البنكية عبر شبائك خاصة باستقبال أموال العملاء من الخارج عبر ذلك

خاتمة الفصل الأول:

في نهاية هذا الفصل، يتضح لنا أن الرقمنة في البنوك تمثل تحولا جوهريا في فلسفة العمل المصرفي، إذ انتقلت بالمؤسسات البنكية من النمط التقليدي القائم على الإجراءات الورقية والفروع المادية إلى نموذج رقمي يعتمد على السرعة والمرونة والابتكار. وقد ظهر لنا في هذا الفصل أن الرقمنة تركز على أسس مفاهيمية واضحة، ولها أهداف استراتيجية تسعى إلى رفع الكفاءة التشغيلية، وتعزيز القدرة التنافسية، وتحسين تجربة العميل.

كما أن تطبيق الرقمنة في البنوك التجارية لا يقتصر على تطوير الخدمات المصرفية الرقمية فحسب، بل يشمل تحديث المعاملات البنكية، وتوفير بنية تحتية تقنية متطورة، وتأهيل الموارد البشرية، وضمان الامتثال للمعايير الأمنية والتنظيمية. ورغم ما يرافق هذا التحول من تحديات تنظيمية وتقنية وأمنية، إلا أنه يفتح آفاقا واسعة للابتكار وتوسيع نطاق الخدمات المالية.

وعليه، فإن مستقبل البنوك يرتبط بمدى قدرتها على تبني استراتيجية رقمية متكاملة، تجمع بين التكنولوجيا والكفاءة البشرية، وتوازن بين التطور التقني ومتطلبات الأمان والثقة، بما يضمن استمراريته ونموها في ظل بيئة مالية تتسم بالتغير المتسارع.

الفصل الثاني:
دور التكامل بين الرقمنة و
الأمن السيبراني لحماية

تمهيد:

في عصرنا هذا، و الذي انتقلت فيه المعاملات والعمليات المالية إلى العالم الرقمي، تجد البنوك نفسها في طليعة المعركة ضد التهديدات السيبرانية، فالتطورات التقنية تعزز الابتكار، لكنها تزيد سطح التعرض للمخاطر السيبرانية وتعرض البنوك التجارية لتحديات متزايدة حيث أصبح الأمن السيبراني في البنوك مصدر قلق بالغ تتطلب معالجته نهجا استباقيا مرنا لحماية البيانات الحساسة والحفاظ على الثقة وضمان مرونة النظم المالية. ففي مجال المعاملات المصرفية، يمثل الأمن السيبراني حصناً حاسماً ضد التهديدات التي لا تعد ولا تحصى التي تواجهها المؤسسات المالية يوميًا. باعتبارها العمود الفقري للتمويل العالمي، تعمل المعاملات المصرفية على تسهيل التدفق السلس للأموال عبر الحدود، ودعم كل شيء بدءًا من تمويل التجارة إلى خدمات إدارة النقد. ومع ذلك، فإن هذه المركزية تجعلها أيضًا هدفًا رئيسيًا لمجرمي الإنترنت. المخاطر عالية بشكل لا يصدق. يمكن أن يؤدي الانتهاك إلى خسارة مالية كبيرة، وتآكل ثقة العملاء، وإلحاق ضرر طويل الأمد بالسمعة.

المبحث الأول: الإطار المفاهيمي للأمن السيبراني

يعد اليوم الأمن السيبراني خط الدفاع الأول، و صمام الأمان للبيانات التي أصبحت تكتسي أهمية كبيرة في عالم اليوم. ففي ظل التوجه نحو الرقمنة الشاملة، انتقل فيه التهديد من الحيز التقليدي إلى الفضاء السيبراني، هذا الفضاء الذي خلق بيئة مناسبة لنوع جديد من المخاطر العابرة للقارات، و هو ما جعل من الأمن السيبراني علما قائما بذاته يهدف إلى حماية الأنظمة، الشبكات و البرامج.

المطلب الأول: مفهوم الأمن السيبراني

الفرع الأول: تعريف الأمن السيبراني ومكوناته

1/ تعريف الأمن السيبراني: تعددت التعاريف المحددة للأمن السيبراني، لذا سيتناول عددا منها لتحديد تعريف الامن السيبراني:
أ. لغة:

- كلمة "الأمن" تعني السلامة واطمئنان النفس وزوال الخوف وهي أصل لغوي عربي مستخدم هذا المعنى منذ القدم.

و"السيبراني" (بالإنجليزية cyber) مشتقة من *cybernetics* و هي كلمة يونانية الأصل (*kubernáo*) بمعنى "التوجيه والتحكم"، تم استخدامها في الأدب الحديث للدلالة على الفضاء الإلكتروني والاتصالات الرقمية¹.

- الأمن السيبراني لغويا:² الأمن السيبراني مكون من "لفظتين": "الأمن"، و"السيبراني" الأمن: هو نقيض الخوف، أي بمعنى السلامة و الأمن مصدر الفعل أمن أمناً وأماناً.
و أمنه: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال. أمن من الشر، أي سلم منه.

1. ¹ <https://ar.wikipedia.org/> vu le 26 fevrier 2026

² عائشة عبيد هلا مبارك قويسني العازمي، واقع الأمن السيبراني في التعليم وعلاقته بالأمن النفس من وجهة نظر المعلمات بدولة الكويت، المجلة الدولية لنشر البحوث والدراسات، المجلد 5 - الصادر 59، تأريخ النشر: 20 سبتمبر 2024 ، ص 33

السيبراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات ترددا في معجم الأمن الدولي، وكلمة " cyber لفظةً يونانية الأصل مشتقة من كلمة " kybernetes " بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للتحكم " governor " وأشار بعض المؤرخين إلى أن أصلها يرجع إلى عالم الرياضيات الأمريكي (Norbert Wiener 1964-1894) وذلك للتعبير عن التحكم الآلي.

ب. التعريف الاصطلاحي: هناك العديد من التعاريف التي قدمت لمفهوم الأمن السيبراني، حيث يُعرف بأنه " مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة.

يعرف الأمن السيبراني من خلال الإتحاد الدولي للاتصالات على أنه مجموعة الأدوات، والمفاهيم الأمنية، والضمانات الأمنية، و المبادئ التوجيهية، و المقاربات لإدارة المخاطر، و التدريبات، و الممارسات، والتقنيات، وسبل الضمان والتكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية و المؤسسات و المستخدمين¹.

ان الأمن السيبراني" هو عبارة عن أساليب والأدوات والسياسات الأمنية المستخدمة لمواجهة تحديات الفضاء السيبراني الممثلة في الأنشطة والشبكات الإلكترونية ومجابهة كافة أنواع التهديدات و الاختراقات التي تسعى لتدمير البنية التحتية الحيوية².

الأمن السيبراني هو عملية حماية الأنظمة والبيانات والاتصالات والشبكات الموجودة والمتصلة بالإنترنت ضد الهجمات الرقمية. فهذه الهجمات، التي يشار إليها عادة باسم "الهجمات السيبرانية"، ما هي إلا محاولة اختراق، أو تعديل أو تعطيل أو دخول أو استخدام غير مشروع؛ وبالتالي، يمكن أن تتراوح

¹ الإتحاد الدولي للاتصالات ITU ، "تأمين شبكات المعلومات و الاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني"، قطاع تنمية الاتصالات، لجنة الدراسات الأولى، المسألة 22/1، فترة الدراسة (2006-2010)، ص 1.

² طاهر محمد السعيد ،سليمان خال ، متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الإقتصادية الجزائرية ، (دراسة حالة مؤسسة نفطال فرع غرداية) ،مذكرة مقدمة لإستكمال شهادة الماستر الأكاديمي، كلية العلوم الإقتصادية والتجارية وعلوم التسيير،قسم العلوم والمحاسبة ،تخصص محاسبة ،سنة 2023 - 2022 ، ص21

الهجمات السيبرانية من تثبيت رموز برمجية ضارة على جهاز حاسوب شخصي وصولاً إلى محاولة تدمير البنية التحتية لدول بأكملها¹.

كما يعرف بأنه "ممارسة الدفاع عن أجهزة الكمبيوتر و الأجهزة المحمولة و الأنظمة الالكترونية، والشبكات، والبيانات من الهجمات الخبيثة، كما يرد بمعنى أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات، والأجهزة المتصلة بالانترنت، و عليه فهو المجال الذي يتعلق بإجراءات ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع الهجمات، أو على الأقل الحد من آثارها².

و يعرفه Edward Amoroso: "مجموع الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات" و تشمل تلك الوسائل و الأدوات المستخدمة في مواجهة القرصنة و كشف الفيروسات الرقمية و وقفها، و توفير الاتصالات المشفرة³.

ت. مصطلحات تتعلق بالأمن السيبراني:

الفضاء السيبراني: "هو بيئة تفاعلية رقمية تشمل عناصر مادية و غير مادية، مكونة من مجموعة من الأجهزة الرقمية و أنظمة الشبكات و البرمجيات و المستخدمين سواء مشغلين أو مستعملين، و يطلق عليه الذراع الرابع للجيش الحديثة".

✓ الردع السيبراني: يعرف على أنه منع الأعمال الضارة ضد الاصول الوطنية في الفضاء الرقمي و الأصول التي تدعم العمليات الفضائية.

¹ <https://www.ncsc.gov.bh/ar/cyberwiser/cyber-security.html> vu le 18 fevrier 2026

² منى عبد الله السمحان، متطلبات تحقق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد 111 ، جامعة المنصورة، المملكة العربية السعودية، 2020 ، ص 9.

³ <https://hbrarabic.com> المفاهيم الإدارية الأمن السيبراني vu le 19 fevrier 2026

✓ **الهجمات السيبرانية:** أي فعل يقوض من قدرات و وظائف شبكة الحاسوب، سواء لغرض

شخصي أو سياسي، من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام.

✓ **الجريمة السيبرانية:** مجموعة الأفعال و الأعمال غير القانونية التي تتم عبر معدات أو أجهزة

إلكترونية عبر شبكة الإنترنت، و تتطلب تحكما خاصا بتكنولوجيا الحاسوب و نظم المعلومات لارتكابها

أو التحقيق فيها و مقاضاة فاعلها.¹

✓ **الثغرات:** عدم توفر الحماية اللازمة للممتلكات والأصول القيمة في أمن الحاسوب والشبكات،

يستخدم تعبير الثغرات للإشارة إلى أماكن الضعف في هذه النظم والتي تتيح للمهاجم الإعتداء على

سلامة النظام²

✓ **الجوسسة السيبرانية:** يعتبر التجسس السيبراني تلك المحاولات المتعمدة لاختراق أجهزة الكمبيوتر

والمواقع الإلكترونية التابعة للدولة المناوئة أو الخصم بهدف سرقة معلومات سرية.³

2/ **مكونات الأمن السيبراني:** للأمن السيبراني مكونات يقوم عليها تتجسد في الآتي:⁴

الحماية من البرمجيات الخبيثة والفيروسات: تستهدف هذه البرامج الخبيثة أنظمة الحاسوب من خلال

استغلال الثغرات الأمنية واختطاف الملفات السرية، حيث تشكل تهديدا كبيرا لأمن وسلامة الأنظمة

الإلكترونية، ويمكن تحقيق الحماية ضد الفيروسات من خلال تثبيت برامج مكافحة الفيروسات وتحديثها

بانتظام.

¹ <https://hbrarabic.com> vu le 23 janvier 2026

² إيمان محمد الشورة، الأمن السيبراني في البنوك الإسلامية الأردنية، البحث استكمالاً لمتطلبات الحصول على درجة البكالوريوس في المصارف الإسلامية، الجامعة الأردنية، كلية الشريعة، قسم المصارف الإسلامية، 2020، ص 9.

³ شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب التفجير من الداخل " على الساحة الدولية، العرب للنشر والتوزيع، القاهرة، 2019، ص 106.

⁴ بوازدية جمال، الأمن السيبراني، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص دراسات استراتيجية وأمنية، جامعة الجزائر 3، السنة الجامعية 2020-2021، ص 17-18.

الحماية من الاختراق: تعد القرصنة من أكثر التهديدات التي تواجهها الأنظمة الإلكترونية شيوعاً، ويمكن أن تتسبب في سرقة الملفات والحسابات الشخصية، فضلاً عن تلف البرامج وأجهزة الشبكة . وللحماية من الاختراق، يجب تحديث كلمات المرور وتفعيل ميزات الأمان و المصادقة الثنائية.

المصادقة الثنائية: تعتبر المصادقة الثنائية من أهم الإجراءات الأمنية لحماية الأنظمة الإلكترونية وتجعل من الصعب على القراصنة اختراق الحسابات، حيث يحتاج المستخدمون إلى إدخال رمز مصادقة إضافي لإتمام الدخول إلى حساباتهم.

التحديثات الأمنية: يتطلب الأمن الإلكتروني إجراءات تحديث منتظمة للبرامج و الأنظمة المستخدمة. ونظراً لأن العديد من الثغرات الأمنية تحدث بشكل مستمر، يجب إصدار تحديثات أمنية لكل برنامج لسد هذه الثغرات.

التشفير: التشفير هو حماية البيانات عن طريق تحويلها إلى شكل لا يمكن قراءته إلا من قبل الأشخاص المصرح لهم.

المراقبة الأمنية: مراقبة الأنشطة الأمنية والحوادث الأمنية على الشبكات والأنظمة لاكتشاف التهديدات المحتملة والاحتياط والاستجابة لها في الوقت المناسب .

التوعية والتدريب: تثقيف وتدريب المستخدمين وتدريبهم على مخاطر الأمن السيبراني وأفضل الممارسات لمنع التهديدات السيبرانية هو جزء مهم من استراتيجية أمنية شاملة.

إدارة التهديدات و الاستجابة للحوادث: ويشمل ذلك الاستعداد للاستجابة للحوادث الأمنية المحتملة ووضع إجراءات للتحقيق في الحوادث الأمنية والاستجابة لها بفعالية وسرعة.

الفرع الثاني: أهمية الأمن السيبراني في المعاملات التجارية الرقمية:

في عالم اليوم المترابط بواسطة الشبكات، يستفيد الجميع من برامج الدفاع السيبراني. وتتمثل أهمية الأمن السيبراني فيما يلي¹:

- تنفيذ تدابير الأمن السيبراني المناسبة للحفاظ على أمن وسرية المعلومات ضد الهجمات السيبرانية، بهدف بناء الثقة في البنية التحتية للمعلومات و الاتصالات في جميع القطاعات، وخاصة البنوك والمؤسسات المالية مع العمل على حمايتها من مخاطر القرصنة لتحقيق بيئة رقمية آمنة بالتنسيق و اتباع الأساليب الحديثة لتقييم المخاطر الأمنية والتأكد من فعالية وكفاءة البرامج المستخدمة لضمان أمن الشبكات.

- يؤكد الأمن السيبراني في القطاع المصرفي على إنشاء درع وقائي و اتخاذ تدابير وقائية مثل التوقيعات الرقمية أو المجاميع الاختبارية، للحفاظ على البيانات و المعلومات الشخصية والمالية للعملاء والمؤسسات المالية و منع التعديلات أو التلاعب غير المصرح به، فتعزيز الأمن السيبراني في البنوك يضمن تقديم الخدمات بأمان وسالمة وتأمين العمليات المصرفية والمعاملات المالية ويساعد في الحفاظ على سمعة المؤسسات المالية وضمان استقرار الأسواق المالية وحماية البيانات الحساسة من الاختراق الأمني.

¹ مروة فتحي السيد البغدادي، اقتصاديات الامن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، العدد السادس والسبعون،

- الحفاظ على استقرار الشبكة الرقمية لأنظمة المعلومات والاتصالات لضمان استمرار عمليات الشركة أو المؤسسة عن طريق تأمين الأنظمة للحفاظ عليها من التعرض للعطل أو للخطر حتى لا توقف الأنشطة.

- يستخدم تكنولوجيا متقدمة تعمل على تحليل التعليمات البرمجية وبنية الموقع للكشف عن الثغرات الأمنية والأداء والمشكلات التشغيلية التي تسهل عملية الهجوم، ويوفر حلولاً محددة لإحباط الهجمات وحماية الموقع بفعالية من البرمجيات الخبيثة والقرصنة والاختراقات المستمرة.

- تشفير جميع المعاملات الرقمية بحيث لا يمكن للمخترقين والمهاجمين والعناصر العابثة الوصول إلى البيانات والتطبيقات بسهولة لمهاجمتها أو تغيير محتواها لأن التشفير أحد أساليب الحماية والتي يصعب فك رموزها.

- تعزيز حماية أنظمة التكنولوجيا التشغيلية على جميع المستويات وكذلك مكونات الأجهزة والبرامج الخاصة بها والخدمات التي تقدمها والبيانات التي تحتوي عليها والتصدي للهجمات السيبرانية والحوادث المتعلقة بأمن المعلومات، وخاصة التي تستهدف البنوك والمؤسسات المالية يوفر بيئة آمنة وجديرة بالثقة للمعاملات في مجتمع المعلومات.

- اتخاذ كافة التدابير اللازمة من خلال الإلمام بأحدث التقنيات والتكتيكات ذات الصلة بأمن المعلومات، لحماية المستخدمين من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة، و تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية لنهب معلوماتهم الشخصية.

كما تتجلى أهمية الأمن السيبراني في قدرته على مقاومة التهديدات المتعمدة وغير المتعمدة والاستجابة والتعافي، وبالتالي التخلص من الأضرار الناجمة عن تعطيل أو إتلاف تكنولوجيا المعلومات والاتصالات أو بسبب سوء استخدامها، وكنتيجة حتمية لهذه الأهمية جعلته العديد من الدول على قمة أولوياتها وخصوصا بعد الحروب الإلكترونية التي بدأت تظهر تجلياتها بين بعض الدول الكبرى، في إشارة

صريحة إلى نهاية الحروب التقليدية التي كانت تستخدم فيها الأسلحة الثقيلة، والإعلان عن بداية حروب جديدة هي الحروب الإلكترونية¹.

المطلب الثاني: التهديدات السيبرانية و أثرها على المعاملات البنكية الرقمية

الفرع الأول: التهديدات السيبرانية في المعاملات البنكية الرقمية: يعد القطاع المالي عموماً و المصرفي خصوصاً هو الأكثر عرضة للمخاطر السيبرانية، حيث تتعامل هذه الأخيرة مع كم ضخم من البيانات والمعاملات الحساسة، غالباً ما يستهدفها المجرمون سعياً لسرقة الأموال أو تعطيل الأنشطة الاقتصادية. وتشكل الهجمات على القطاع المصرفي حوالي خمس الإجمالي.

1/ تعريف التهديدات السيبرانية:

الهجمات السيبرانية على البنوك هي محاولات اختراق الأنظمة الرقمية للبنوك بهدف سرقة البيانات المالية، تدمير الأنظمة أو التلاعب بها. قد تشمل هذه الهجمات تقنيات مثل البرمجيات الخبيثة، اختراق الشبكات، والهندسة الاجتماعية. المهاجمون قد يستهدفون أنظمة الدفع الإلكتروني، البيانات الشخصية للعملاء، أو حتى الحسابات المصرفية.²

و هي أي عمل يستهدف إضعاف قدرات ووظائف شبكة الكمبيوتر لتحقيق غايات شخصية أو سياسية . يتم ذلك عبر استغلال نقاط الضعف في النظام، مما يمكن المهاجم من التلاعب به أو تعطيله.³

¹ عائشة عبيد الله مبارك قويسني العازمي، مرجع سبق ذكره، ص 35

² الهجمات السيبرانية على البنوك، مقال نشر بتاريخ 2025 / 2 / 19، موقع سايبروان. اطلع عليه في 23 فيفري 2026

³ نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني " التهديد المتصاعد لأمن الدول"، مجلة مركز بابل للدراسات الإنسانية، جامعة بابل، العراق، المجلد 8 ، العدد 2، 2018، ص 191

كما يقصد بالتهديدات السيبرانية تلك الهجمات التي تتم باستخدام آليات و شبكات الانترنت و أجهزة الحاسوب الآلي، و تهدف إلى إلحاق الضرر بالأجهزة و الشبكات الالكترونية ذات الاتصال بالإنترنت.¹ وتعرف ايضا التهديدات السيبرانية بأنها: " فعل يهدف إلى هدم و تجاوز الجدران الرقمية التي تقوم بوظيف حماية كحواجز أمنية بغرض سرقة المعلومات و البيانات أو الإكتهاء بالاطلاع عليها و تخريبها أو حتى تغيير مضمونها، كل ذلك بهدف إلحاق الضرر بالضحية." ²

2/ أنواع الهجمات السيبرانية التي تستهدف البنوك: ³

تعد البنوك هدفا رئيسيا للهجمات السيبرانية نظرا لطبيعة المعلومات الحساسة التي تديرها. تتنوع أنواع هذه الهجمات و تشمل:

➤ **هجمات التصيد الاحتيالي :** يستخدم المهاجمون في هذه الهجمات، رسائل بريد إلكتروني أو رسائل نصية مزيفة لتوجيه الضحايا إلى مواقع إلكترونية مزيفة، حيث يُطلب منهم إدخال معلوماتهم الشخصية أو المالية.

➤ **البرمجيات الخبيثة:** يستخدم المهاجمون البرمجيات الخبيثة مثل الفيروسات أو تروجانات للوصول إلى الأنظمة البنكية وسرقة البيانات أو تعطيل الأنظمة الداخلية للبنك.

➤ **هجمات رفض الخدمة الموزعة:** في هذا النوع من الهجمات، يتم تحميل الخوادم بملايين الطلبات من أجهزة متعددة لشل أنظمة البنك وتسبب في توقف الخدمة عن العمل لفترة زمنية.

¹ عبد الغاني شرقي، التهديدات السيبرانية و إشكالية السيادة، إعادة قراءة للسيادة و معاهدة وستيفاليا، مجلة السياسة العالمية، مجلد 07، عدد 02، 2023، 275

² محمد دحماني، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني و السياسي، المجلد 07، العدد 02، 2023، ص 602.

³<https://alansariexchange.com/ar/blog/potential-cyberattacks-threaten-financial-systems> vu le 27 janvier 2026

- **هجمات التسلل الداخلي:** هذه الهجمات تحدث عندما يقوم موظف أو شخص ذو صلاحيات داخلية باستغلال موقعه للوصول إلى معلومات حساسة أو إجراء عمليات غير قانونية.
- **هجمات الوسيط:** في هذا الهجوم، يتسلل المهاجم بين العميل والبنك أثناء عملية تبادل البيانات، مما يسمح له باعتراض المعلومات مثل تفاصيل الحسابات أو كلمات المرور.
- **هجمات الهندسة الاجتماعية:** يتم في هذا النوع من الهجمات استخدام خداع نفسي لجعل الأفراد يكشفون عن معلومات حساسة مثل كلمات المرور أو بيانات الحسابات عبر الاتصال المباشر أو المواقع المزيفة.
- **هجمات الفدية:** يقوم المهاجمون بتشفير بيانات البنك أو أنظمتهم ويطلبون فدية مالية مقابل فك تشفير البيانات واستعادة الوصول إليها.
- **هجمات: SQL Injection :** في هذه الهجمات، يتم استغلال ثغرات في قواعد بيانات البنك من خلال إدخال أوامر SQL ضارة لسرقة البيانات أو تعديلها.
- **هجمات تزوير المعاملات:** يسعى المهاجمون في هذا النوع من الهجمات لتعديل المعاملات المالية في النظام المصرفي أو إجراء تحويلات غير مصرح بها من حسابات العملاء.
- **الهجمات على تطبيقات الأجهزة المحمولة:** مع تزايد استخدام التطبيقات المصرفية على الهواتف الذكية، تستهدف هذه الهجمات استغلال ثغرات التطبيقات للوصول إلى الحسابات المصرفية للمستخدمين.
- **هجمات يوم الصفر:** هجمات تستهدف ثغرات أمنية لم يكتشفها المطورون أو فرق الأمن، ووجودها المهاجمون أولاً، وسُميت بيوم الصفر لأنه لا يوجد وقت لسد الثغرة أو صد الهجوم، ويكون الدفاع ضدها صعباً للغاية لأنها:
- لم يمكن اكتشافها مسبقاً.

➤ لا توجد حلول جاهزة للحماية منها.

➤ تستخدم في هجمات مستهدفة ومتقدمة¹.

3/ الهدف من الهجمات السيبرانية على البنوك: تهدف هذه الهجمات إلى الاستفادة من الثغرات الأمنية في الأنظمة المصرفية للوصول إلى أموال العملاء أو تعطيل العمليات المصرفية، فهي يمكن أن تهدد استقرار المؤسسات المالية. و لعل أبرز هذه الأهداف تشمل²:

- **سرقة البيانات المالية:** يسعى المهاجمون لاختراق الأنظمة المصرفية للوصول إلى بيانات الحسابات المصرفية، البطاقات الائتمانية، والمعلومات المالية الحساسة للعملاء.
- **تحويل الأموال بشكل غير قانوني:** المهاجمون قد يحاولون تحويل أموال من حسابات العملاء أو من حسابات البنك إلى حسابات خارجية بهدف سرقة الأموال
- **تعطيل الأنظمة المصرفية:** بعض الهجمات تهدف إلى تعطيل أنظمة الدفع الإلكتروني أو الخدمات المصرفية عبر الإنترنت، مما يسبب اضطراباً في العمليات اليومية للبنك.
- **الحصول على معلومات سرية:** الهجمات قد تستهدف الوصول إلى معلومات حساسة تتعلق بعملاء البنك أو البيانات الداخلية للمؤسسة المالية بهدف استغلالها لاحقاً.
- **الابتزاز والتهديد:** قد يسعى المهاجمون لاختراق الأنظمة المصرفية بهدف الحصول على فدية من البنك مقابل إعادة الوصول إلى البيانات أو إيقاف الهجوم.
- **التلاعب في المعاملات المالية:** الهجمات قد تستهدف تعديل أو تزوير المعاملات المالية داخل الأنظمة البنكية، مما يؤدي إلى فقدان الثقة في النظام المصرفي. هذه الأهداف تجعل البنوك هدفاً رئيسياً للهجمات السيبرانية، مما يتطلب تطوير استراتيجيات أمنية متقدمة لحماية أنظمتها وبيانات عملائها.

¹ <https://keytime.sa/cyberattacks> vu le 03 janvier 2026

² حسن محمد الحسين ،أساسيات الأمن السيبراني، حلب، سوريا 2022، ص 234.

الفرع الثاني: أثر التهديدات السيبرانية على المعاملات البنكية الرقمية: تؤثر الهجمات السيبرانية على

البنوك بشكل عميق، حيث تتسبب في العديد من الأضرار التي تشمل الأمن المالي، والسمعة، والأعمال التشغيلية. فيما يلي بعض التأثيرات الرئيسية للهجمات السيبرانية على البنوك¹:

✓ **الخسائر المالية المباشرة:** الهجمات السيبرانية قد تؤدي إلى خسائر مالية ضخمة نتيجة للسرقات

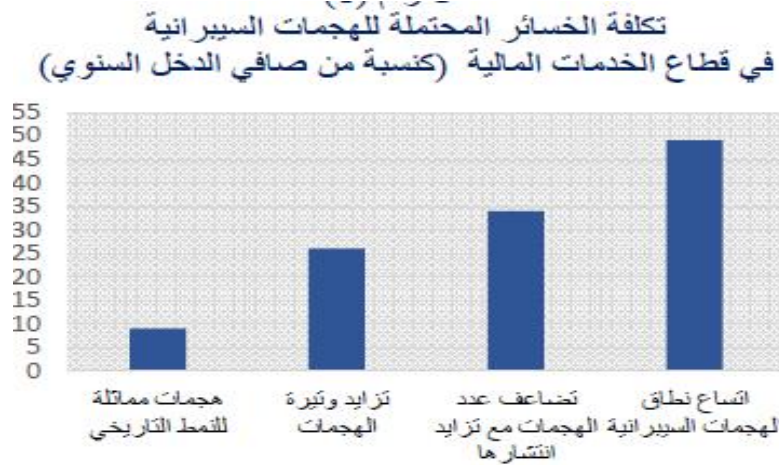
الإلكترونية أو تحويل الأموال بشكل غير قانوني، مثلما حدث في هجوم بنك بنغلاديش. بالإضافة إلى

ذلك، قد يتكبّد البنك تكاليف كبيرة في إصلاح الأنظمة المصرفية المتضررة. و فيما يلي شكل يبين

تكلفة الخسائر المالية الناتجة عن الهجمات السيبرانية:

شكل رقم 01 : تكلفة الخسائر المحتملة للهجمات السيبرانية على قطاع الخدمات المالية(نسبة من

صافي الدخل السنوي)



المصدر: صندوق النقد العربي، الأمن السيبراني في القطاع المصرفي، موجز سياسات (جوان 2019)

¹ <https://ca-paris.com/banque-innovation/> Cybersécurité en banque : une préoccupation de tous les instants vu le 03 Janvier 2026

✓ **تعطيل العمليات البنكية:** الهجمات مثل هجمات "رفض الخدمة الموزعة" قد تؤدي إلى توقف

الخدمات المصرفية عبر الإنترنت، مما يعطل عمليات الدفع والتحويلات البنكية. يمكن أن يؤدي ذلك إلى التأثير على العملاء والشركات التي تعتمد على هذه الخدمات في تعاملاتها اليومية.

✓ **تسريب البيانات الحساسة:** في حال تم اختراق البيانات المصرفية، قد يتم تسريب معلومات

حساسة للعملاء مثل أرقام الحسابات، بيانات البطاقات الائتمانية، ومعلومات شخصية أخرى. هذا يزيد من خطر استغلال هذه المعلومات في هجمات الاحتيال أو السرقة المالية¹.

✓ **تضرر سمعة البنك:** الهجمات السيبرانية قد تؤثر بشكل كبير على سمعة البنك في السوق. فقدان

ثقة العملاء في قدرة البنك على حماية بياناتهم يمكن أن يؤدي إلى تراجع أعداد العملاء وازدياد التردد في استخدام الخدمات المصرفية عبر الإنترنت.

✓ **الامتثال القانوني والمشاكل التنظيمية:** إذا كان البنك غير قادر على حماية بيانات عملائه، قد

يواجه مشاكل قانونية بسبب انتهاك قوانين حماية البيانات. قد يؤدي ذلك إلى فرض غرامات وعقوبات من الهيئات التنظيمية مثل قوانين حماية الخصوصية الأوروبية.

✓ **التأثير على الابتكار والنمو:** الهجمات السيبرانية قد تؤدي إلى تقليص قدرة البنك على الابتكار

أو تطوير خدمات جديدة بسبب التركيز المستمر على تعزيز الأمان وحماية الأنظمة من التهديدات. كما قد تؤدي هذه الهجمات إلى تأجيل خطط التوسع أو تنفيذ مشاريع جديدة.

✓ **زيادة الاستثمارات في الأمن السيبراني:** بعد الهجوم، ينبغي على البنوك استثمار مبالغ كبيرة في

تعزيز الأمن السيبراني. يشمل ذلك تحديث الأنظمة، تدريب الموظفين، واستخدام تقنيات متقدمة للكشف عن التهديدات. يمكن أن تكون هذه التكاليف على المدى الطويل باهظة.

¹ Cybersécurité en banque.Op.cit

- ✓ **التهديد للعملاء:** في حالة سرقة البيانات، قد يتعرض العملاء للاحتيال المالي، حيث يتم استخدام بياناتهم في عمليات غير قانونية مثل سحب الأموال أو إجراء معاملات غير مصرح بها. هذا يؤثر سلبيًا على العلاقة بين البنك والعملاء.
- ✓ **ضعف ثقة العملاء بالبنوك:** أي اختراق أمني في بنك قد يؤدي إلى فقدان ثقة العملاء، مما يدفعهم للبحث عن مؤسسات مالية أكثر أمانًا¹.

المطلب الثالث: استراتيجيات التكامل بين الرقمنة والأمن السيبراني:

يمثل التكامل بين الرقمنة والأمن السيبراني حجر الزاوية في حماية المعاملات التجارية البنكية في العصر الرقمي. فمع توسع الخدمات المصرفية الإلكترونية، تتزايد التهديدات السيبرانية، مما يجعل من الضروري اعتماد استراتيجيات متكاملة تجمع بين التكنولوجيا المتقدمة والحوكمة الرشيدة وإدارة المخاطر الفعالة. إن تحقيق هذا التكامل لا يقتصر على الجانب التقني فحسب، بل يشمل الأبعاد التنظيمية والبشرية، بما يضمن استدامة القطاع المصرفي وثقة العملاء واستقرار النظام المالي.

الفرع الأول: مفهوم التكامل بين الرقمنة والأمن السيبراني: يُعد التكامل بين الرقمنة والأمن السيبراني حجر الأساس لحماية العمليات المصرفية في البنوك التجارية، خاصة في ظل التحول الرقمي المتسارع واعتماد الخدمات المصرفية الإلكترونية والهواتف الذكية والحوسبة السحابية، و لا يمكن فصل الرقمنة عن الأمن السيبراني، إذ أن كل خدمة رقمية تفتح مجالًا جديدًا للمخاطر الإلكترونية

1/ تعريف التكامل بين الرقمنة و الأمن السيبراني و مراحله العملية:

¹ Cybersécurité en banque .Op.cit

أ. تعريف التكامل بين الرقمنة و الأمن السيبراني:¹

يقصد بالتكامل بين الرقمنة والأمن السيبراني ذلك النهج الاستراتيجي الذي يتم من خلاله دمج تقنيات وسياسات وإجراءات الأمن السيبراني في جميع مراحل عملية التحول الرقمي، ابتداء من مرحلة التصميم والتطوير، مروراً بالتنفيذ، وانتهاء بالمراقبة والصيانة. فهو ليس مجرد جمع بين طرفين، بل هو عملية "دمج وظيفي" تجعل الأمن جزءاً لا يتجزأ من البنية الرقمية للمنظومة.

ان التكامل بين الرقمنة والأمن السيبراني هو الانتقال من مرحلة "الحماية بعد الإصابة" إلى مرحلة "البناء المحصن"، بحيث لا يمكن تصور وجود خدمة رقمية مصرفية سليمة بدون غلاف أمني مدمج فيها، تماماً كما لا يمكن فصل الروح عن الجسد.

حيث يعرف التكامل بين الرقمنة والأمن السيبراني في البنوك التجارية بأنه: بناء منظومة مصرفية رقمية حديثة يكون الأمن فيها عنصراً أساسياً منذ مرحلة التصميم، لضمان تقديم خدمات سريعة وذكية وآمنة في الوقت نفسه.

و يشير التكامل بين الرقمنة والأمن السيبراني في البنوك التجارية إلى عملية مواءمة استراتيجية وتشغيلية يتم من خلالها دمج ضوابط وإجراءات الأمن السيبراني ضمن جميع مراحل التحول الرقمي، ابتداء من تصميم الأنظمة المصرفية الرقمية وتطويرها، مروراً بتشغيلها وإدارتها، وصولاً إلى تقييمها وتحسينها المستمر. ويهدف هذا التكامل إلى ضمان سرية البيانات المصرفية، وسلامتها، وتوافرها، مع المحافظة على كفاءة الخدمات الرقمية واستمراريتها.

و عليه يمكن القول بأن التكامل بين الرقمنة والأمن السيبراني يُعتبر استراتيجية تدمج التقنيات المصرفية الرقمية (التطبيقات، الذكاء الاصطناعي، الحوسبة السحابية) مع بروتوكولات حماية متقدمة لضمان نزاهة

¹ Bouhafes Hanen, Cyberscurity in the digital era: between digital transformation and protection challenges, Faculty of law, University Ain Temouchent, Algeria, 2025, p 118

وسريّة وتوافر العمليات المصرفية. وتهدف هذه الاستراتيجية إلى تأمين المعاملات الرقمية مع بناء ثقة العملاء¹.

ب. المراحل العملية للتكامل بين الرقمنة و الأمن السيبراني: يمكن تصور التكامل كطبقات حماية مترابطة تعمل معا في كل معاملة إلكترونية²:

➤ من بداية المعاملة:

التعريف بالمستخدم والتحقق من هويته:

- كلمات مرور،
- رموز تحقق مؤقتة،
- بصمات أو خصائص بيومترية.

هنا تتكامل الرقمنة (واجهة التطبيق) مع الأمن السيبراني (آليات المصادقة).

➤ أثناء تنفيذ المعاملة

تشفير البيانات وآليات نقل آمن:

- تستخدم البروتوكولات المشفرة مثل TLS/HTTPS لضمان سرية المعلومات
- البيانات المشفرة لا يمكن قراءتها حتى لو تم اعتراضها

هنا يتكامل عنصر نقل البيانات الرقمي مع تقنيات الأمان.

➤ بعد تنفيذ المعاملة

مراقبة السجلات وتحليل المخاطر لحظيا:

- الأنظمة تجمع وتحلل بيانات كل معاملة
- تقنيات الذكاء الاصطناعي تكشف أي سلوك غير طبيعي

¹ Bouhafes Hanen, Op.cit, pp 119-120

² Bilgin Metin, Fatma Gül Özhan, Martin Wynn, Digitalisation and Cybersecurity: Towards an Operational Framework, journal electronics, October 2025

التقنيات الرقمية تلنقي بتحليلات الأمن السيبراني لمنع الاحتيال.

2/ أهمية التكامل بين الرقمنة والأمن السيبراني: ¹

✓ **حماية البيانات الحساسة:** إن الرقمنة تزيد من حجم البيانات المتداولة إلكترونياً، ما يتطلب:

- تشفير البيانات أثناء النقل والتخزين
- أنظمة كشف التسلل
- المصادقة متعددة العوامل

✓ **ضمان استمرارية الأعمال:** أي هجوم إلكتروني قد يؤدي إلى توقف الخدمات المصرفية، مما

يسبب خسائر مالية وسمعة سيئة. لذا يجب:

- إنشاء خطط استمرارية الأعمال
- مراكز بيانات احتياطية
- أنظمة نسخ احتياطي دورية
- تعزيز الثقة لدى العملاء: كلما زاد الأمان، زادت ثقة العملاء في استخدام القنوات الرقمية، خاصة في المعاملات المالية الحساسة.

¹ Bilgin Metin, Fatma Gül Özhan, Martin Wynn, Op.cit

✓ الامتثال للتشريعات: تفرض الجهات الرقابية متطلبات صارمة لحماية البيانات، ويُعدّ التكامل

بين الرقمنة والأمن السيبراني ضرورة للامتثال التنظيمي.

الفرع الثاني: محاور التكامل بين الرقمنة والأمن السيبراني: التكامل بين هذه المحاور يضمن أن كل

"نقرة" رقمية يقوم بها العميل تكون محاطة بطبقات متعددة من الحماية غير المرئية، مما يحقق الهدف

النهائي المتمثل في بنك رقمي سريع، ولكنه حصين وموثوق. تشمل هذه المحاور: ¹

المحور الأول: التكامل على مستوى البنية التحتية : يمثل هذا المحور الأساس الذي تُبنى عليه

العمليات الرقمية، ويشمل:

- **الأمن التصميمي (Security by Design):** دمج مبادئ الأمن السيبراني منذ المرحلة الأولى

لتصميم التطبيقات المصرفية وأنظمة الدفع، وليس إضافتها كطبقة خارجية لاحقة.

- **نموذج الثقة الصفرية (Zero Trust Architecture):** تطبيق فلسفة "لا تثق أبداً، تحقق دائماً"

داخل البنية الرقمية للبنك، بحيث يتم التحقق من هوية كل جهاز ومستخدم يحاول الوصول إلى الشبكة،

مما يحمي المعاملات من الاختراق الداخلي والخارجي.

- **أمن واجهات البرمجة (API Security):** مع تزايد استخدام البنوك المفتوحة (Open Banking) ،

يصبح تأمين واجهات البرمجيات (APIs) التي تربط البنك بالشركات الأخرى ضرورة لمنع تسريب بيانات

المعاملات.

المحور الثاني: التكامل على مستوى إدارة الهوية والوصول: يهدف هذا المحور إلى التأكد من أن

الشخص الذي يقوم بالمعاملة هو صاحب الحق الشرعي:

- **المصادقة متعددة العوامل (MFA):** دمج تقنيات التحقق (كلمات المرور، الرموز المؤقتة OTP ،

البصمة الوجه) ضمن تجربة المستخدم الرقمية لضمان توازن بين السهولة والأمان.

¹ ABOUT OMAIR DELIMI ARRAK, Cybersecurity as One of the Pillars of Digital Transformation in Organizations: Selected International Experiences, Scientific Journal of Economic Dialogue, Volume: 04 / N°: 02 (2026), pp 21-30

- **التحقق البيومتري (Biometric Authentication):** استخدام الخصائص البيولوجية (بصمة الإصبع، التعرف على الصوت أو الوجه) كبديل للكلمات التقليدية، مما يصعب على المخترقين تزوير هوية صاحب الحساب.
- **إدارة الهوية الرقمية الموحدة:** ربط بيانات العميل عبر جميع القنوات الرقمية (الموبايل، الإنترنت، الصراف الآلي) في هوية واحدة مراقبة أمنياً.
- **المحور الثالث: التكامل على مستوى حماية البيانات والمعاملات:** يركز هذا المحور على حماية "المحتوى" المالي أثناء انتقاله أو تخزينه:
- **التشفير الشامل (End-to-End Encryption):** تحويل بيانات المعاملات المالية إلى رموز معقدة منذ لحظة إرسالها من هاتف العميل حتى وصولها لخادم البنك، مما يمنع قراءتها في حال اعتراضها.
- **الترميز (Tokenization):** استبدال البيانات الحساسة (مثل رقم البطاقة الائتمانية) برموز وهمية عند إجراء عمليات الشراء الرقمية، بحيث لا تُرسل البيانات الحقيقية للتاجر، مما يحميها من السرقة.
- **توقيع المعاملات رقمياً:** استخدام التوقيع الإلكتروني للتأكد من أن المعاملة لم يتم التلاعب بها أثناء النقل¹.
- **المحور الرابع: التكامل على مستوى المراقبة والتحليل الذكي:** استخدام الذكاء الاصطناعي لربط السرعة الرقمية بالقدرة على الكشف الفوري:
- **أنظمة كشف الاحتيال بالذكاء الاصطناعي (AI Fraud Detection):** خوارزميات تتعلم من أنماط المعاملات وتكتشف الشذوذ في الوقت الفعلي (مثل تحويل مبلغ ضخم في وقت غير معتاد)، وتقوم بإيقاف المعاملة فوراً وآلياً.

¹ Ibid

- **مركز عمليات الأمن (SOC):** غرفة عمليات تعمل على مدار الساعة لمراقبة حركة البيانات الرقمية والاستجابة لأي تهديد محتمل قبل أن يؤثر على المعاملات.
- **المحور الخامس: التكامل على مستوى الحوكمة والثقافة التنظيمية:** و يتمثل في الجانب الإداري والبشري الذي يضمن استمرارية التكامل:
- **ثقافة الوعي الرقمي والأمني:** تدريب الموظفين والعملاء على أن الرقمنة لا تعني التهاون في الأمان، وتوعيتهم بأساليب التصيد الاحتيالي.
- **خطط استمرارية الأعمال (Business Continuity):** وضع خطط تضمن استمرار العمليات المصرفية الرقمية حتى في حال وقوع كوارث سيبرانية، مع وجود نسخ احتياطية آمنة.
- **الامتثال التنظيمي:** التأكد من أن كل خطوة في الرقمنة تلتزم بالمعايير الدولية (مثل PCI-DSS) والقوانين المحلية لحماية البيانات¹.

المبحث الثاني: إدارة المخاطر السيبرانية وآليات حماية المعاملات البنكية الرقمية:

في ظل التحول الشامل للرقمنة في البنوك التجارية، لم يعد الخطر يقتصر على السرقات المادية أو العجز الائتماني، بل ظهر نوع جديد من المخاطر العابرة للحدود هي المخاطر السيبرانية، وإدارة هذه المخاطر لا يعني منعها كلياً بل تعني بناء أمن سيبراني يضمن استمرار العمليات البنكية حتى في ظل وجود هجمات سيبرانية.

¹ Ibid

المطلب الأول: إدارة المخاطر السيبرانية في البنوك التجارية:

تعتمد إدارة مخاطر الأمن السيبراني على استراتيجيات تساعد على ترتيب أولويات المخاطر المطلوب معالجتها؛ لرصد التهديدات الأكثر ضررا والمطلوب مواجهتها في الوقت المطلوب.

الفرع الأول: مفهوم إدارة المخاطر السيبرانية في البنوك التجارية و مراحلها:

1/ مفهوم إدارة مخاطر الأمن السيبراني:¹

تُعرف إدارة مخاطر الأمن السيبراني على أنها مجموعة خطوات تتخذ بشكل دوري لمواجهة التهديدات الإلكترونية ومعالجتها من خلال رصدها وتحديدها وتقييمها، ومن أجل إدارتها بفاعلية فإن ذلك يتطلب نظرة شاملة لهذه المخاطر وتعاون من كافة أفراد العمل، ليس فقط من أفراد إدارة المخاطر وإنما أفراد الإدارات الأخرى.

وتعرف إدارة مخاطر الأمن السيبراني أيضا بأنها عملية مستمرة لتحديد وتحليل وتقييم ومعالجة تهديدات الأمن السيبراني التي تواجهها المؤسسة.

ان إدارة المخاطر السيبرانية هي طريقة لتحسين الوعي بالموقف الأمن السيبراني للمؤسسة - تحديد التهديدات وترتيبها حسب الأولوية والحد منها.

و هي عملية تحديد وتحليل وتقييم وتخفيف أو القضاء على المخاطر التي يمكن أن تؤثر على عمليات الأعمال .في سياق التجارة الإلكترونية، تشمل إدارة المخاطر التعامل مع التهديدات السيبرانية، خروقات البيانات، الاحتيال الإلكتروني، وقضايا الشحن والتسليم، و تهدف إدارة المخاطر إلى حماية مصالح الشركة والعملاء وضمان استمرارية العمليات التجارية.

¹ <https://bakkah.com/ar/knowledge-center/how-to-perform-a-cyber-risk-assessment> vu le 19 janvier 2026

كما عرفها شحاته (2022) بأنها "مجموعة السياسات والعمليات و الأساليب الرقابية المصممة لحماية المعلومات و الأنظمة من الهجمات الالكترونية و الاختراق الأمني والتي قد تحد من إمكانية تحقيق نظام الأمن السيبراني لأهدافه المرجوة، المتمثلة في إتاحة المعلومات والسرية وسلامة العمليات التشغيلية"

2/ مراحل إدارة المخاطر:¹ يمكن تقسيم إدارة المخاطر السيبرانية إلى أربعة أجزاء مختلفة:

➤ **تعريف المخاطر:** فهم البنية التحتية لتكنولوجيا المعلومات في مؤسستك، ومعرفة مواطن الضعف، وتحديد التهديدات.

➤ **تقييم المخاطر:** تقييم احتمالية استغلال نقاط الضعف في مؤسستك وتقييم تأثير الاستغلال.

➤ **تخفيف المخاطر:** إن تطبيق التدابير، مثل الضوابط الفنية والإدارية والمادية، سيساعد على تقليل تأثير التهديدات. بالإضافة إلى ذلك، فإن تثقيف مؤسستك بشأن أفضل ممارسات الأمن السيبراني ووضع إرشادات للعمليات الأمنية استجابة الحدث سيشجع على مزيد من المرونة.

➤ **مراقبة المخاطر:** المراقبة والمراجعة المستمرة لمشهد المخاطر من خلال التقييمات المنتظمة وضوابط المراقبة استجابة الحدث لتحديد التهديدات الجديدة وتقييم فعالية تدابير تخفيف

تغطي إدارة المخاطر السيبرانية نفس المراحل الثلاث لإدارة منفذ دخول الهجمات: الاكتشاف والتقييم و التخفيف، و تتضمن مرحلة التقييم تصنيف المخاطر بحيث يمكن للمؤسسة معيار ملف تعريف المخاطر ومراقبتها بمرور الوقت.

¹ https://www.trendmicro.com/ar_sa/what-is/attack-surface/cyber-risk-scoring.html vu le 20 janvier 2026

الفرع الثاني: أهمية إدارة المخاطر في البنوك: تواجه البنوك طيفا واسعا من المخاطر، ويُعد التعامل الفعال معها أمرا جوهريا لضمان حماية الكيان المصرفي. وفيما يلي أبرز الأسباب التي تبرز أهمية إدارة المخاطر في الخدمات المالية¹:

➤ **حماية الاستقرار المالي:** دون وجود إدارة رشيدة للمخاطر، قد تتعرض السلامة المالية للبنك إلى تهديدات جسيمة. أما إدارة المخاطر المصرفية الفاعلة فتُسهم في ضمان استقرار البنك وقدرته على مواجهة التحديات الاقتصادية.

➤ **الحفاظ على السمعة وثقة العملاء:** تؤدي إدارة المخاطر غير الكفؤة إلى تداعيات مثل الاحتيال أو الاختراقات الأمنية، ما يُفضي إلى تراجع ثقة العملاء وتدهور سمعة البنك، وهنا تكمن أهمية إدارة مخاطر السمعة في المؤسسات المالية.

➤ **ضمان الالتزام التنظيمي:** ينبغي على البنوك الامتثال لمجموعة من القوانين واللوائح الصارمة لمزاولة أنشطتها بشكل قانوني. وتسهم الإدارة الجيدة للمخاطر في تحقيق هذا الامتثال، بما يشمل الاحتفاظ برؤوس أموال كافية، والتقييد بلوائح مكافحة غسل الأموال. لا يحمي هذا الامتثال من العقوبات القانونية فحسب، بل يحافظ أيضًا على سمعة البنك ويُبقي عملياته مستقرة.

➤ **دعم القرارات الاستراتيجية:** تُعين إدارة المخاطر البنوك على اتخاذ قرارات مدروسة عند التوسع إلى أسواق جديدة، أو طرح منتجات مبتكرة، أو الاستثمار في تقنيات ناشئة. ومن خلال تقييم المخاطر الكامنة، تصبح قرارات البنك أكثر توازنًا وانسجامًا مع أهدافه الاستراتيجية الطويلة المدى.

¹ <https://www.getfocal.ai/ar/blogs/risk-management-in-banking,January 31, 2026>

➤ **تخصيص رأس المال بكفاءة:** تُمكن إدارة المخاطر البنك من توجيه رأس ماله نحو فرص

استثمارية واحدة وتجنب القطاعات عالية الخطورة. ومن خلال التقييم الدقيق للمخاطر، يمكن للبنك اتخاذ

قرارات استثمارية رشيدة تُعزز من مردوديته.

المطلب الثاني: سياسات إدارة مخاطر الأمن السيبراني و آليات حماية المعاملات التجارية البنكية من المخاطر السيبرانية

الفرع الأول: سياسات إدارة مخاطر الأمن السيبراني: في ظل تزايد التهديدات الرقمية،

أصبحت السياسات والإجراءات الأمنية ضرورية لحماية الأنظمة. حيث تعتمد المؤسسات المصرفية على

مجموعة من الإجراءات المنظمةة لضمان أمان البيانات والأنظمة من الاختراقات المحتملة، و من خلال

تطبيق هذه السياسات، يمكن تقليل المخاطر وضمان استمرارية الأعمال: ¹

1/ سياسة إدارة الثغرات: تشمل إدارة الثغرات الأمنية تحديد التهديدات المحتملة ومعالجتها بشكل

استباقي. يتم ذلك من خلال دورة حياة تشمل الاكتشاف والتقييم والإصلاح. وفقًا لمعايير ISO 27001 ،

يجب أن تكون هذه العملية مستمرة لضمان فعالية الأنظمة.

من المهم أيضًا استخدام أدوات إدارة الثغرات التي تساعد في تحديد نقاط الضعف بسرعة. هذا يقلل من

فرص استغلال المتسللين لهذه الثغرات.

¹ <https://al-khwarizmi.com> vu le 31janvier 2026 أهمية الحماية السيبرانية في العصر الرقمي

2/ سياسة إدارة حوادث الأمن السيبراني: تعد إدارة الحوادث الأمنية جزءًا أساسيًا من أي استراتيجية أمنية. تشمل هذه العملية تحديد الحوادث والاستجابة لها وفقًا لمعايير NIST. يتم ذلك من خلال خطوات مثل التحليل الأولي واحتواء الحادث واستعادة الأنظمة.

من الضروري أيضًا تدريب فرق الاستجابة على التعامل مع الحوادث بفعالية. هذا يضمن تقليل الأضرار واستعادة العمليات بأسرع وقت ممكن.

3/ سياسة النسخ الاحتياطية: تعتبر النسخ الاحتياطية أحد أهم الإجراءات لضمان استمرارية الأعمال. يجب أن تشمل هذه السياسة تصميم خطط استعادة البيانات بانتظام. يتم ذلك من خلال استخدام أدوات النسخ الاحتياطية التي تعمل على تخزين البيانات بشكل آمن.

من المهم أيضًا اختبار هذه النسخ بشكل دوري لضمان فعاليتها في حالات الطوارئ. هذا يقلل من خطر فقدان البيانات ويضمن استمرارية العمليات¹.

الفرع الثاني: أدوات حماية المعاملات التجارية البنكية من المخاطر السيبرانية: تعد أدوات الحماية هي "الأدوات التقنية والتشغيلية" التي تسمح للبنوك بتقديم خدمات رقمية سريعة مع ضمان الحماية القصوى.

فيما يلي قائمة مفصلة بأهم هذه الأدوات وتقنياتها:²

1. أدوات إدارة الهوية والتحكم في الوصول : تُعد هذه الأدوات خط الدفاع الأول للتأكد من أن

الشخص الذي يقوم بالمعاملة الرقمية هو الشخص الصحيح:

- أنظمة المصادقة متعددة العوامل: أدوات تدمج أكثر من طريقة تحقق مثل: كلمة السر + رمز OTP مرسل للجوال + بصمة إصبع...

¹ Ibid

² موقع ريناد المجد، الحماية من الهجمات السيبرانية: ست أدوات للأمن السيبراني، مقال نشر في 2021/8/2 اطلع في 02 مارس 2026

- **التحقق البيومتري :** استخدام أجهزة الاستشعار في الهواتف (قارئ البصمة، التعرف على الوجه، قزحية العين) كأداة للدخول للتطبيقات المصرفية، مما يلغي خطر سرقة كلمات المرور.
- **أنظمة التحقق من الهوية وإدارة الوصول :** تستخدم البنوك أنظمة إدارة الهوية والصلاحيات لتحديد من يمكنه الوصول إلى البيانات. ويتم تطبيق سياسات Zero Trust التي تمنع أي شخص من الوصول إلا بعد التحقق الدقيق من هويته.
- 2. **أدوات حماية البيانات والمعاملات:** تستخدم هذه الأدوات لتحويل البيانات المالية إلى صيغ غير مفهومة للمخترقين:
- **بروتوكولات التشفير :** أدوات تقنية تشفر قناة الاتصال بين العميل والبنك، مما يضمن أن أي معاملة مالية (تحويل، دفع) تنتقل عبر الإنترنت بشكل مشفر وآمن.
- **تقنية الترميز:** أداة بالغة الأهمية في الدفع الإلكتروني (مثل Apple Pay أو البطاقات الافتراضية). تقوم باستبدال رقم البطاقة الحقيقي برمز وهمي مستعار. إذا اعترض المخترق الرمز، فلا يمكنه استخدامه أو استرجاع رقم البطاقة الأصلي.
- **إدارة المفاتيح:** أنظمة لإدارة مفاتيح التشفير وتخزينها بأمان لضمان سلامة البيانات المشفرة.
- 3. **أدوات أمن التطبيقات والبنية التحتية:** تتكامل هذه الأدوات مع الخوادم والبرمجيات لحمايتها من الهجمات التقنية.
- **جدار الحماية لتطبيقات الويب :** درع واقٍ يوضع أمام تطبيقات البنك على الإنترنت لرصد وحجب الهجمات التي تستهدف الثغرات في البرمجيات.

- **بوابات API الآمنة :** مع تزايد "البنوك المفتوحة" تُستخدم هذه البوابات كوسطاء آمنين لنقل البيانات بين البنك والطرف الثالث، مما يضمن أن البيانات لا تُرسل إلا للأطراف الموثوقة.
- **أمن السحابة :** أدوات متخصصة لحماية البيانات المخزنة في السحابة، وتشفيرها، ومنع الوصول غير المشروع إليها.
- **أنظمة الجدار الناري:** تعمل الجدران النارية على منع الدخول غير المصرح به إلى الشبكات المصرفية، ويتم استخدام التي توفر حماية متطورة ضد الهجمات.
- 4. **أدوات المراقبة والتحليل الذكي:** أدوات تعمل في الخلفية لمراقبة سلوك المعاملات وكشف الشذوذ¹.
- **أنظمة كشف ومنع الاحتيال :** برمجيات تعتمد على الذكاء الاصطناعي وتعلم الآلة لتحليل أنماط المعاملات في الوقت الفعلي. إذا اكتشفت معاملة غير طبيعية (مثل تسجيل دخول من دولة غريبة أو مبلغ ضخم)، تقوم بإيقافها أو طلب تحقق إضافي تلقائياً.
- **نظام إدارة المعلومات والأحداث الأمنية :** أداة تجمع السجلات من جميع الأنظمة الرقمية في البنك، وتحللها لرصد أي محاولة اختراق مجهولة قبل أن تحدث.
- **الذكاء الاصطناعي وتحليل السلوك :** تعتمد البنوك على تحليل سلوك المستخدمين لاكتشاف أي نشاط غير طبيعي، حيث أن تقنيات الذكاء الاصطناعي تستخدم لكشف عمليات الاحتيال والتصيد الاحتيالي.

¹ موقع ريناد المجد، مرجع سبق ذكره.

- أنظمة كشف التهديدات والاستجابة لها: يعتبر نظام كشف الاختراق من أشهر هذه الأنظمة حيث يراقب الشبكة ويكتشف أي نشاط غير طبيعي. ويستعمل أيضا نظام منع الاختراق يعمل على منع أي محاولة اختراق قبل أن تسبب ضررا.
 - تقنية البلوكشين (Blockchain): تُستخدم لتأمين سجلات المعاملات وضمان عدم تزويرها، خاصة في التحويلات الدولية وعقود التجارة الذكية.
5. أدوات الأمن التشغيلي والاستجابة:
- منصات الاستجابة للحوادث السيبرانية : أدوات برمجية توجه فريق الأمن خطوة بخطوة عند وقوع هجوم لعزل الأنظمة المصابة واستعادة العمليات بسرعة.
 - أدوات اختبار الاختراق: برمجيات يستخدمها خبراء الأمن لمحاكاة هجمات حقيقية على الأنظمة الرقمية لاكتشاف الثغرات وسدها قبل استغلالها من قبل المجرمين¹.
 - أنظمة المراقبة في الوقت الفعلي: توفر المراقبة اللحظية للمعاملات أداة قوية للتدخل الفوري عند اكتشاف أي نشاط غير طبيعي، هذه التقنية تعزز بشكل مباشر من حماية المعاملات البنكية بالتكنولوجيا وتجعل البنوك أكثر استعدادا لمواجهة الهجمات لحظة وقوعها.²
- المطلب الثالث: أفضل الممارسات لحماية المعاملات التجارية البنكية و أهم التحديات:

¹ موقع ريناد المجد، مرجع سبق ذكره.

² <https://techno-ville.com/securing-banking-transactions-with-technology> vu le 24fevrier 2026

الفرع الأول: أفضل الممارسات لإدارة المخاطر البنكية: من أجل إدارة المخاطر بنجاح، يجب على

البنوك تبني ممارسات شاملة ومدرّسة في إدارة مخاطر البنوك. وفيما يلي أبرز الممارسات التي ينبغي

اتباعها¹:

1. دمج إدارة المخاطر في ثقافة البنك:

يجب أن تُدمج إدارة المخاطر في جميع جوانب العمليات البنكية، بدءًا من القيادة العليا وصولًا إلى

العمليات اليومية. فإدماج هذا المفهوم في ثقافة البنك يعزز من فعالية الاستجابة للمخاطر.

2. استخدام تحليلات البيانات في مراقبة المخاطر: تُساعد أدوات تحليلات البيانات المتقدمة البنوك في

مراقبة المخاطر بشكل لحظي، واكتشاف التهديدات الناشئة بسرعة، واتخاذ قرارات مستنيرة استنادًا إلى

البيانات لتعزيز استراتيجيات التخفيف من المخاطر.

3. تعزيز الصمود السيبراني بما يتجاوز حدود الأمن الإلكتروني: يشمل بناء الصمود السيبراني

ليس فقط الحماية من الهجمات السيبرانية، بل أيضًا التأكد من قدرة البنك على التعافي سريعًا ومواصلة

العمل في حال حدوث الهجوم، مع التركيز على الاستعداد والتفاعل السريع.

4. تبني نهج إدارة المخاطر القائم على السيناريوهات: يُسهم هذا النهج في محاكاة المخاطر

المستقبلية المحتملة تحت سيناريوهات متعددة، مما يساعد البنوك على الاستعداد للمتغيرات الطارئة،

وتطوير استراتيجيات لتقليل الآثار السلبية عند حدوث أحداث غير متوقعة.

كما تعتمد المؤسسات المصرفية الرائدة على الذكاء الاصطناعي لتحسين كفاءة أنظمة إدارة

المخاطر في البنوك وتحليل البيانات المتغيرة في الوقت الفعلي.

¹ <https://www.getfocal.ai/ar/blogs.Op.cit>. vu le 03 mars 2026

5. برامج التوعية الأمنية: يتم تدريب الموظفين والعملاء على تجنب التصيد الاحتيالي والهجمات

الإلكترونية، حيث تقوم البنوك بتنفيذ اختبارات أمنية دورية لاختبار جاهزية الأنظمة والموظفين.

6. دمج المخاطر البيئية والاجتماعية والحوكمة : تُعد مخاطر البيئة والمجتمع والحوكمة من

العوامل المتزايدة الأهمية في القطاع المصرفي، ويجب على البنوك أن تأخذ هذه العوامل في الحسبان

عند وضع استراتيجيات إدارة المخاطر، وذلك لضمان الامتثال للأنظمة ومواءمة ممارساتها مع توقعات

أصحاب المصلحة.

7. إرساء حوكمة واضحة وتحديد دقيق للمسؤوليات: يجب تحديد الأدوار والمسؤوليات بوضوح

على جميع المستويات داخل البنك لضمان المساءلة الفعالة في إدارة المخاطر.

8. الامتثال المستمر للمعايير التنظيمية الامتثال المستمر للمعايير التنظيمية: يُساعد الامتثال

المستمر للمتطلبات التنظيمية البنوك على إدارة المخاطر القانونية، وضمان الشفافية، و تعزيز الثقة بين

العملاء و الجهات الرقابية.

الفرع الثاني: تحديات الأمن السيبراني في البنوك التجارية:

تواجه حماية المعاملات المصرفية الرقمية تحديات سيبرانية متزايدة ناتجة عن التطور السريع

لبرمجيات الفدية، هجمات التصيد، والاحتيال المالي الذي تجاوزت خسائره 16 مليار دولار في 2024.

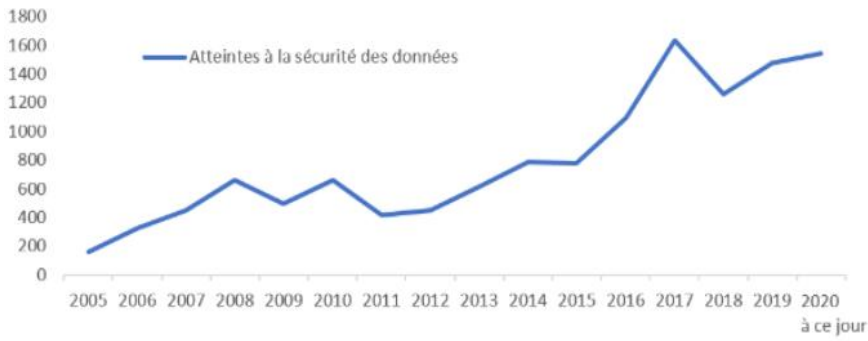
وتشمل أبرز التحديات:¹

○ تطور الهجمات الخبيثة: يواجه القطاع المصرفي هجمات متطورة مثل برمجيات الفدية، هجمات

التصيد، واختراق أنظمة نقاط البيع، حيث تم تحليل مئات الحوادث المرتبطة بجرائم مالية مباشرة.

شكل رقم 02: تطور الهجمات السيبرانية في القطاع المصرفي

¹ رؤى حمود، تحديات الأمن السيبراني في المؤسسات المالية، مقال نشر بتاريخ 2021/05/26 ، موقع شركة ريناد المجد اطلع عليه في 23



Source: Identity theft resource center

- استهداف الأنظمة المصرفية القديمة: تستغل التهديدات السيبرانية الأنظمة المصرفية التقليدية التي لم يتم تحديثها، مما يسهل اختراقها عبر ثغرات معروفة.
- ثغرات سلاسل التوريد والمزودين: تمثل الهجمات عبر سلاسل التوريد الرقمية أكثر من 60% من الاختراقات الكبرى، حيث يستهدف القراصنة الثغرات في البرمجيات والخدمات التقنية المعتمدة.
- تصاعد الاحتيال وسرقة الهوية: يُعد سرقة الهوية، واستخدام بيانات الاعتماد الشخصية أو المصرفية لفتح حسابات جديدة أو إجراء عمليات غير قانونية من أكبر التحديات.
- الهجمات على العملات المشفرة: زاد اعتماد القراصنة على استهداف البلوكتشين ومحافظ العملات المشفرة، مما أضاف بُعداً جديداً للمخاطر المالية.
- النقص في الكفاءات الأمنية: يعاني القطاع من نقص في المتخصصين المؤهلين لمواجهة التهديدات المتزايدة، بالتزامن مع التطور السريع للتكنولوجيا.
- التعطيل التشغيلي: لا تقتصر التهديدات على سرقة الأموال، بل تشمل هجمات حجب الخدمة (DDoS) التي تعطل الأنظمة وتسبب أضراراً بسمعة المؤسسة¹.

¹ رؤى حمود، مرجع سبق ذكره

خلاصة الفصل الثاني:

يمثل التكامل بين الرقمنة والأمن السيبراني حجر الزاوية في حماية المعاملات التجارية البنكية في العصر الرقمي. فمع توسع الخدمات المصرفية الإلكترونية، تتزايد التهديدات السيبرانية، مما يجعل من الضروري اعتماد استراتيجيات متكاملة تجمع بين التكنولوجيا المتقدمة والحوكمة الرشيدة وإدارة المخاطر الفعالة. إن تحقيق هذا التكامل لا يقتصر على الجانب التقني فحسب، بل يشمل الأبعاد التنظيمية والبشرية، بما يضمن استدامة القطاع المصرفي وثقة العملاء واستقرار النظام المالي.

الفصل الثالث:

دراسة ميدانية لدور التكامل بين
الرقمنة و الأمن السيبراني لحماية
المعاملات التجارية البنكية

تمهيد: بعد تطرقنا في الفصلين الأول و الثاني للمفاهيم المتعلقة بمتغيرات الدراسة التكامل بين الرقمنة و الأمن السيبراني، و حماية المعاملات التجارية البنكية، في جانبها النظري، من خلال دراسة مختلف الجوانب المتعلقة بهاذين المتغيرين، سنتناول في هذا الفصل لدراسة ميدانية لدور التكامل بين الرقمنة و الأمن السيبراني لحماية المعاملات التجارية في البنوك التجارية، على مجموعة من فروع البنوك التجارية الجزائرية.

المبحث الأول: منهجية الدراسة الميدانية:

المطلب الأول: الإجراءات المنهجية للدراسة الميدانية:

الفرع الأول: منهج الدراسة المتبع:

يتمثل المنهج المتبع في الدراسة الميدانية، الأسلوب المتبع قصد الوصول إلى الأهداف المسطرة لهذه الدراسة، و هي البحث عما إذا كان للمتغير المستقل و هو التكامل بين الرقمنة و الأمن السيبراني دورا في تحقيق المتغير التابع و هو حماية المعلومات التجارية البنكية، لذلك اعتمدنا على المنهج الوصفي التحليلي لوصف البيانات المجمعة ثم تحليل النتائج المتوصل إليها.

الفرع الثاني: مجتمع، عينة و حدود الدراسة:

1/ مجتمع :

يتمثل مجتمع الدراسة في البنوك التجارية و التي يبلغ عددها تسعة عشر بنكا تجاريا بين جزائري ، مشترك و أجنبي و التي تنشط في الوطن.

2/ عينة الدراسة:

و قد اخترنا كعينة لدراستنا بالنسبة للبنوك التجارية عينة حددت بحوالي 50 فرعا للبنوك التجارية من مجتمع السابق الذكر، تم توزيع استمارة، و قد تم الرد على 50 استمارة فقط.

3/ حدود الدراسة:

أ. الحدود المكانية: تركزت الدراسة على فروع البنوك التجارية المتواجدة في كل من ولاية ميلة، قسنطينة و سطيف.

ب. الحدود الزمانية: استمرت الدراسة الميدانية من 15 مارس إلى 05 ماي 2026.

المطلب الثاني: أدوات و متغيرات الدراسة:

الفرع الأول: أدوات الدراسة:

1/ الملاحظة: تعتبر الملاحظة من المراحل التمهيديّة التي تستعمل في البحث الاستطلاعي بعد طرح المشكلة في إطار نظري و محاولة الوصول إلى تفسيرات واقعية للتساؤلات أو الافتراضات و استعمال الملاحظة البسيطة و المباشرة باعتبارها مصدر المعلومات في الموقف الطبيعي و ذلك للتعرف على الرقمنة في البنوك التجارية و ما وضع من أمن سيبراني لحماية المعاملات التجارية الرقمية فيها.

2/ الاستمارة: لجمع البيانات اللازمة للدراسة الميدانية، حيث اعتمدت على أسلوب الاستقصاء،

و ذلك بتصميم استمارة استبيان موجه للبنوك التجارية المختارة و التي تمثل عينة الدراسة، و يهدف إعداد الاستمارة إلى ما يلي:

- التعرف على الرقمنة في البنوك و الأمن السيبراني لحماية المعاملات التجارية البنكية.

- دراسة التكامل بين الرقمنة و الأمن السيبراني لحماية المعاملات التجارية البنكية.

الفرع الثاني: متغيرات الدراسة: تحتوي الدراسة على متغيرين اثنتين الأول مستقل و الثاني تابع كما يلي:

1/ المتغير المستقل: التكامل بين الرقمنة و الأمن السيبراني: و الذي تضمن بعد الرقمنة في البنوك التجارية

من حيث البنية التحتية الرقمية، أتمتة العمليات المصرفية، استعمال التطبيقات الذكية....

و بعد الأمن السيبراني و هو يعمل لضبط سير الرقمنة في مسارها الصحيح دون انحراف، مع أمن البيانات و المعلومات.

2/ المتغير التابع: حماية المعاملات التجارية البنكية : و هو النتيجة المرجوة من التكامل بين الرقمنة و الأمن السيبراني، و يتمثل في : توفير بيئة آمنة، و سرية، استمرارية الخدمة.

المطلب الثالث: تصميم الاستبيان و الأدوات الإحصائية المستعملة:

الفرع الأول: تصميم الاستبيان: تم إعداد الاستبيان كأداة رئيسية للدراسة، و التي شملت عددا من العبارات عكست الأهداف من هذا البحث، و التي قامت عينة الدراسة بالإجابة عليها، و يضم استبيان البحث خمس (05) محاور:

1/ المحور الأول: البيانات العامة للبنك: تضمنت بيانات حول نوع البنك، حجم البنك، وجود إدارة أمن سيبراني.

2/ المحور الثاني: استراتيجية الرقمنة في البنوك التجارية: تضمن هذا المحور ست عبارات.

3/ المحور الثالث: ممارسات الأمن السيبراني: تضمن هذا المحور ثماني عبارات

4/ المحور الرابع: التكامل بين الرقمنة والأمن السيبراني: و تضمن خمس عبارات.

5/ المحور الخامس: حماية المعاملات التجارية البنكية: و تضمن أربع عبارات.

6/ تحكيم الاستبيان : بعد صياغة الأسئلة، و بتوجيه من الأستاذ المشرف، قمنا ببعض التعديلات بهدف توضيح أكثر لعبارات الإستبيان و تحديد الهدف من كل منها، تم حذف بعض العبارات التي لم و تصحيح أخرى، حتى خرجت الإستمارة في صيغتها النهائية (أنظر الملحق 01).

الفرع الثاني: الأدوات الإحصائية المستعملة: لتحقيق أهداف الدراسة وتحليل البيانات التي يتم جمعها، فقد تم استخدام العديد من الأساليب الإحصائية المناسبة و التي تعرف ببرنامج SPSS و التي تتمثل في:

- التكرارات والنسب المئوية بهدف التحليل الوصفي للمتغيرات الشخصية لعينة الدراسة؛

-المتوسط الحسابي لمعرفة درجة موافقة أفراد العينة على محاور الدراسة.

-الانحراف المعياري للتعرف على مدى انحراف استجابات أفراد الدراسة لكل عبارة من عبارات متغيرات الدراسة.

-اختبار ألفا كرونباخ لقياس ثبات أداة الدراسة، حيث يعبر على مدى صلاحية الاستبيان لاستخدامه من أجل جمع البيانات، فكلما زاد معامل إلى 0.6 كانت الأداء أكثر ثباتا ويعتبر الاستبيان مقبولا، أما في الحالة العكسية يتم التعديل.

-اختيار كولمنغروف سمرنوف من أجل معرفة طبيعة التوزيع الذي تتبعه بيانات الدراسة.

-معامل التحديد من أجل تفسير التأثير بين المتغيرات التي توجه بينهم علاقة ارتباط.

-معامل الارتباط بيرسون للتعرف على علاقة الارتباط بين المتغيرين.

1/ مقياس ليكرت Likert الخماسي: تم إعداد أسئلة الاستبيان على أساس مقياس Likert الخماسي، و ذلك حسب الجدول التالي:

جدول رقم 02 : أوزان مقياس Likert الخماسي:

موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
5	4	3	2	1
5-4.20	4.19-3.40	3.39-2.60	2.59-1.80	1.79-1

المصدر: الموقع الإلكتروني التفكير الإحصائي

2/ اختبار التوزيع الطبيعي:

جدول رقم 03: اختبار التوزيع الطبيعي:

المحور	قيمة الاختبار	مستوى الدلالة Sig
محور 2 الرقمنة	0.943	0.018
محور 3 الأمن السيبراني	0.948	0.027
محور 4 التكامل	0.968	0.188
محور 5 حماية المعاملات البنكية	0.923	0.003
الاستبيان ككل	0.114	0.174

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: من خلال الجدول السابق، نلاحظ أن قيمة مستوى الدلالة للمحاور (2، 3 و 5) هي أقل من مستوى المعنوية 0.05، و هذا يعني أن البيانات لا تتبع التوزيع الطبيعي، و بالتالي استخدام الاختبارات اللامعلمية لاختبار الفرضيات، أما المحور 4 فقيمة الاختبار أكبر من مستوى المعنوية 0.05 و هذا يعني أن التوزيع طبيعي، لكن عند حساب مقياس الالتواء و التفلطح تبين أن قيمها تقع ضمن المدى المقبول و بالتالي يمكن اعتبار أن توزيعها توزيعاً طبيعياً، صالح لاستخدام الإحصاء المعلمي.

3/ اختبار الاتساق الداخلي بين عبارات المحور الواحد: بالنسبة لهذه الخطوة الهامة يستعان بمعامل الارتباط

Person لمعرفة مدى اتساق عبارات المحاور فيما بينها، حيث يمكن القول أنّ الاستبيان يتمتع بدرجة عالية

من الصدق إذا كان المعامل الخاص بالارتباط قويا ودال إحصائيا ويمكن تجزئته إلى ما يلي:

جدول رقم 04: قوة معامل الارتباط:

0 - 0.3	علاقة ضعيفة
0.4 - 0.69	علاقة متوسطة
0.7 - 1	علاقة قوية

فيما يلي تعرض نتائج معاملات الارتباط للمتغير التابع في الجدول:

جدول رقم 05: معامل الارتباط بين عبارات محور استراتيجية الرقمنة في البنوك:

رقم العبارة	معامل الارتباط	مستوى الدلالة Sig
01	0.770	< 0.001
02	0.836	< 0.001
03	0.620	< 0.001
04	0.735	< 0.001
05	0.636	< 0.001
06	0.569	< 0.001

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: معامل الارتباط : من خلال الجدول أعلاه يتضح أن معامل ارتباط العبارات يتراوح بين (0.569 و 0.836) و جميعها موجبة تقيس نفس المفهوم الذي يقيسه المحور ككل.

مستوى الدلالة (Sig): جميع القيم أقل من 0.001 و هذا يعني أن الارتباط دال إحصائياً عند مستوى دلالة 0.01، حيث كان أعلى ارتباط للعبارة 01 (0.836)، بينما أقل قيمة له للعبارة 03 (0.569) . و بما أن كل القيم جاءت موجبة و دالة إحصائياً فإن ذلك يؤكد عبارات المحور تتصف لاتساق داخلي مرتفع، يجعلها صالحة للتطبيق على عينة الدراسة.

جدول رقم 06: معامل الارتباط بين عبارات محور ممارسات الأمن السيبراني:

رقم العبارة	معامل الارتباط	مستوى الدلالة Sig
07	0.604	< 0.001
08	0.685	< 0.001
09	0.695	< 0.001
10	0.613	< 0.001
11	0.547	< 0.001
12	0.647	< 0.001
13	0.429	0.004
14	0.441	0.001

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: معامل الارتباط: من خلال الجدول أعلاه يتضح أن معامل ارتباط العبارات يتراوح بين (0.429 و 0.695) و جميعها موجبة، مما يعني أن العبارات تسير في نفس اتجاه قياس المحور.

مستوى الدلالة Sig: أقل من 0.001 في كل العبارات ما عدا العبارة 13 حيث كان 0.004 و هذا يعني أن الارتباط دال إحصائياً عند مستوى دلالة 0.01، و قد تراوحت قيم الارتباط بين (0.429 و 0.695)، و بالرغم من انخفاض معامل ارتباط العبارتين 13 و 14 إلا أنهما لا تزالان ضمن الحدود المقبولة و دالتين إحصائياً مما يؤكد تمتع جميع عبارات هذا المحور باتساق داخلي كاف يجعلها صالحة لأداة الدراسة.

جدول رقم 07: معامل الارتباط بين عبارات محور التكامل بين الرقمنة و الأمن السيبراني:

رقم العبارة	معامل الارتباط	مستوى الدلالة Sig
15	0.471	< 0.001
16	0.722	< 0.001
17	0.682	< 0.001
18	0.683	< 0.001
19	0.411	0.003
20	0.522	< 0.001

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: أظهرت نتائج اختبار الاتساق الداخلي وجود ارتباطات موجبة ودالة إحصائياً بين عبارات المحور والدرجة الكلية له، حيث تراوحت معاملات الارتباط بين (0.411) و (0.722) عند مستويات دلالة أقل من

(0.05)، مما يدل على تمتع فقرات المحور بدرجة مقبولة إلى مرتفعة من الاتساق الداخلي، ويؤكد صلاحيتها لقياس البعد محل الدراسة.

جدول رقم 08: معامل الارتباط بين عبارات محور حماية المعاملات التجارية البنكية:

رقم العبارة	معامل الارتباط	مستوى الدلالة Sig
21	0.855	< 0.001
22	0.691	< 0.001
23	0.444	0.001
24	0.855	< 0.001

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: أظهرت نتائج اختبار الاتساق الداخلي وجود ارتباطات موجبة وقوية بين فقرات المحور والدرجة الكلية له، حيث تراوحت معاملات الارتباط بين (0.444 و 0.855)، وكانت جميعها دالة إحصائياً عند مستوى معنوية أقل من (0.05)، مما يؤكد تمتع فقرات المحور بدرجة عالية من الاتساق الداخلي وصلاحيتها لقياس البعد محل الدراسة.

4/ ثبات عبارات الاستبيان : تم استخدام معامل ألفا-كرونباخ الذي تكون قيمته مقبولة إحصائياً فقط عندما تتراوح بين 0.06 أي بدرجة % 60 وأقل من . % 95 ندون في الجدول التالي القيم المتحصل عليها:

الجدول رقم 09: نتائج معامل ألفا-كرونباخ

المجال	عدد العبارات	معامل ألفا كرونباخ
محور 2 الرقمنة	06	0.750
محور 3 الأمن السيبراني	08	0.711
محور 4 التكامل	04	0.627
محور 5 حماية المعاملات البنكية	03	0.667
محور المتغير المستقل و التابع	3	0.618

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: أظهرت نتائج اختبار الثبات باستخدام معامل ألفا كرونباخ أن قيم الثبات لمحاور الدراسة تراوحت بين (0.627) و(0.750)، وهي قيم تشير إلى توفر درجة مقبولة إلى جيدة من الاتساق الداخلي بين فقرات الاستبيان، مما يؤكد صلاحية الأداة للاستخدام في جمع البيانات وتحليلها واختبار فرضيات الدراسة.

المبحث الثاني: تحليل و مناقشة نتائج الدراسة:

المطلب الأول: عرض و تحليل النتائج:

الفرع الأول: النتائج المتعلقة بالخصائص العامة لعينة الدراسة:

1/ نوع البنك:

جدول رقم 10 توزيع عينة الدراسة حسب النوع: الشكل رقم 03 توزيع عينة الدراسة حسب النوع:



نوع البنك	التكرار	النسبة المئوية
محلي	36	72
إقليمي	5	10

دولي	9	18
المجموع	50	100

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج

SPSS27

2/ حجم البنك:

جدول رقم 11 توزيع عينة الدراسة حسب حجم البنك شكل رقم 04 توزيع عينة الدراسة حسب حجم البنك



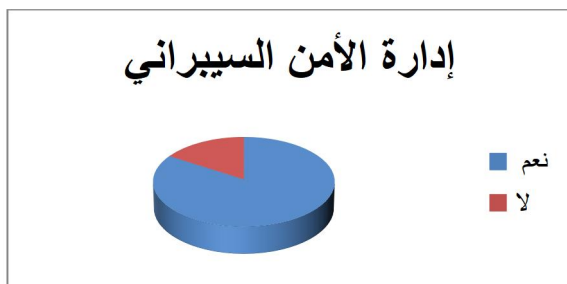
حجم البنك	التكرار	النسبة المئوية
صغير	0	0
متوسط	10	20
كبير	40	80
المجموع	50	100

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

3/ لدى البنك إدارة مستقلة للأمن السيبراني:

جدول رقم 12: وجود إدارة أمن سيبراني شكل رقم 05 لدى البنك إدارة مستقلة للأمن

السيبراني:



الإجابة	التكرار	النسبة المئوية
نعم	42	84
لا	8	16
المجموع	50	100

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق على المحور الأول: من خلال الجداول أعلاه، نلاحظ أن معظم البنوك في العينة محلية (72%) وحجمها كبير (80%)، ولديها إدارة مستقلة للأمن السيبراني بنسبة (84%) ، و هذا يعكس سياقاً جاهزاً نسبياً للتقدم أكثر نحو رقمنة و أمن سيبراني متقدمين، كما يشير إلى وعي مؤسسي عال في البنوك الكبيرة بالمخاطر الرقمية من خلال تخصيص إدارة للأمن السيبراني في هيكلها التنظيمي.

الفرع الثاني: النتائج المتعلقة باتجاه آراء المستجوبين حول محاور الاستبيان:

1/ نتائج المحور الثاني: استراتيجية الرقمنة:

جدول رقم 13: إجابات المحور الثاني-استراتيجية الرقمنة-

رقم الفقرة	التكرارات	أفق بشدة 5	أوافق 4	محايد 3	لا أوافق 2	لا أوافق بشدة 1	المتوسط ط المرجح	الانحراف ف المعياري	النسبة المئوية	اتجاه العينة	رتبة الفقرة
01	ni	21	22	2	2	3	4.12	1.08	82.4%	أوافق 4	5
	Fi	42.0%	44.0%	4.0%	4.0%	6.0%					
02	ni	19	27	2	2	0	4.26	0.72	85.2%	أفق بشدة 5	4
	Fi	38.0%	54.0%	4.0%	4.0%	0.0%					
03	ni	15	26	2	7	0	3.98	0.96	79.6%	أوافق 4	6
	Fi	30.0%	52.0%	4.0%	14.0%	0.0%					
04	ni	21	29	0	0	0	4.42	0.50	88.4%	أفق بشدة 5	1
	Fi	42.0%	58.0%	0.0%	0.0%	0.0%					
05	ni	20	30	0	0	0	4.40	0.49	88.0%	أفق بشدة 5	2
	Fi	40.0%	60.0%	0.0%	0.0%	0.0%					
06	ni	14	36	0	0	0	4.28	0.45	85.6%	أفق بشدة 5	3
	Fi	28.0%	72.0%	0.0%	0.0%	0.0%					
	المتوسط الحسابي المرجح للمحور ككل						25.46				
	الانحراف المعياري للمحور ككل							2.97			

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: تظهر النتائج ارتفاع المتوسطات المرجحة لمعظم الفقرات، حيث تراوحت بين 3.98 و 4.42، مع نسب مئوية تراوحت بين 79.6% و 88.4%، ما يدل على اتفاق غالبية أفراد العينة على أن البنك يعتمد استراتيجيات رقمية واضحة وفعالة. كما أن انخفاض قيم الانحراف المعياري نسبياً يشير إلى تقارب آراء المبحوثين وعدم وجود تشتت كبير في الإجابات. و تعكس هذه النتائج ارتفاع النضج الرقمي لدى البنوك في عينة الدراسة، و وعيها بأن الرقمنة لم تعد خياراً بل ضرورة لكي تتماشى مع مؤشرات التحول الرقمي العالمي، فالرقمنة البنكية تساهم في تقليص تكاليف المعاملات، وتسريع الخدمات المالية، ورفع الكفاءة التشغيلية للبنوك، وهو ما ينعكس إيجاباً على الإنتاجية والقدرة التنافسية لها. كما أن التوسع في الخدمات الرقمية يساهم في تعزيز الشمول المالي وزيادة حجم المعاملات الإلكترونية داخل الاقتصاد.

2/ نتائج المحور الثالث: ممارسات الأمن السيبراني:

جدول رقم 14: إجابات المحور الثالث-ممارسات الأمن السيبراني-

رقم الفقرة	التكرارات	أفق بشدة 5	أوافق 4	محايد 3	لا أوافق 2	لا أوافق بشدة 1	المتوسط المرجح	الانحراف المعياري	النسبة المئوية	اتجاه العينة	رتبة الفقرة
07	ni	2	22	10	10	6	3.08	1.14	61.6%	محايد 3	8
	%Fi	4.0%	44.0%	20.0%	20.0%	12.0%					
08	ni	15	31	2	2	0	4.18	0.69	83.6%	أوافق 4	3
	%Fi	30.0%	62.0%	4.0%	4.0%	0.0%					
09	ni	15	31	0	4	0	4.14	0.78	82.8%	أوافق 4	6
	%Fi	30.0%	62.0%	0.0%	8.0%	0.0%					
10	ni	17	29	0	3	1	4.16	0.87	83.2%	أوافق 4	4
	%Fi	34.0%	58.0%	0.0%	6.0%	2.0%					
11	ni	19	25	1	5	0	4.16	0.89	83.2%	أوافق 4	5
	%Fi	38.0%	50.0%	2.0%	10.0%	0.0%					
12	ni	17	30	3	0	0	4.28	0.57	85.6%	أفق 1	1

	بشدة 5				%0.0	%0.0	%6.0	%60.0	%34.0	%Fi	
7	أوافق 4	%82.0	0.61	4.10	0	2	1	37	10	ni	13
					%0.0	%4.0	%2.0	%74.0	%20.0	%Fi	
2	أفق بشدة 5	%84.8	0.66	4.24	0	2	0	32	16	ni	14
					%0.0	%4.0	%0.0	%64.0	%32.0	%Fi	
				32.26	المتوسط الحسابي المرجح للمحور ككل						
			3.66		الانحراف المعياري للمحور ككل						

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: تبين نتائج هذا المحور متوسطات مرتفعة نسبياً تراوحت بين 3.08 و 4.28، مع ملاحظة أن الفقرة رقم 07 جاءت بمتوسط متوسط نسبياً واتجاه محايد، ما يشير إلى وجود بعض النقائص أو التحديات المتعلقة بتطبيق بعض ممارسات الأمن السيبراني داخل البنك و المتمثلة في تقنيات الذكاء الاصطناعي. في المقابل، أظهرت باقي الفقرات مستويات مرتفعة من الاتفاق، بين 80% و 85.6%. وتعكس هذه النتائج إدراك العاملين لأهمية الأمن السيبراني في حماية البيانات والأنظمة البنكية، حيث أن تعزيز الأمن السيبراني يقلل من الخسائر الناتجة عن الجرائم الإلكترونية والاختراقات المالية، والتي هي في تصاعد و أصبحت تشكل تهديداً مباشراً لاستقرار البنوك وثقة العملاء. كما يساهم الاستثمار في الأمن السيبراني في تقليل المخاطر التشغيلية وتحسين سمعة البنك في السوق المالية.

3/ نتائج المحور الرابع: التكامل بين الرقمنة و الأمن السيبراني:

جدول رقم 15: إجابات المحور الرابع-التكامل بين الرقمنة و الأمن السيبراني-

رقم الفقرة	التكرارات	أوافق بشدة 5	أوافق 4	محايد 3	لا أوافق 2	لا أوافق بشدة	المتوسط المرجح	الانحرا ف المعياري	النسبة المئوية	اتجاه العينة	رتبة الفقرة
---------------	-----------	-----------------	---------	------------	---------------	---------------------	-------------------	--------------------------	-------------------	-----------------	----------------

					1						
2	أوافق بشدة 5	%86.8	0.48	4.34	0	0	0	33	17	ni	15
					%0.0	%0.0	%0.0	%66.0	%34.0	%Fi	
4	أوافق 4	%81.2	0.79	4.06	0	4	2	31	13	ni	16
					%0.0	%8.0	%4.0	%62.0	%26.0	%Fi	
5	أوافق 4	%80.4	0.82	4.02	0	5	1	32	12	ni	17
					%0.0	%10.0	%2.0	%64.0	%24.0	%Fi	
6	أوافق 4	%78.8	0.91	3.94	1	5	1	32	11	ni	18
					%2.0	%10.0	%2.0	%64.0	%22.0	%Fi	
3	أوافق بشدة 5	%86.4	0.47	4.32	0	0	0	34	16	ni	19
					%0.0	%0.0	%0.0	%68.0	%32.0	%Fi	
1	أوافق بشدة 5	%90.0	0.51	4.50	0	0	0	25	25	ni	20
					%0.0	%0.0	%0.0	%50.0	%50.0	%Fi	
				25.18	المتوسط المرجح للمحور ككل						
			2.43		الانحراف المعياري للمحور ككل						

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: أكدت نتائج هذا المحور وفقا للمتوسطات المرجحة التي تتراوح بين 3.94 و 4.50، مع نسب مرتفعة بين 78.8% و 90.0% ، ما يدل على اقتناع أفراد العينة بأن نجاح التحول الرقمي داخل البنوك يرتبط بوجود نظام أمني سيبراني فعال. ويؤكد هذا المحور أن الرقمنة وحدها لا تكفي لتحقيق الكفاءة المصرفية ما لم تكن مدعومة بحماية إلكترونية قوية، و أن أن الرقمنة لا يمكن أن تتجح بمعزل عن نظام أمني سيبراني متكامل.

حيث يؤدي التكامل بين الرقمنة والأمن السيبراني إلى رفع ثقة العملاء في المعاملات الإلكترونية، وزيادة استخدام الخدمات البنكية الرقمية، وبالتالي رفع حجم النشاط الاقتصادي الإلكتروني وتعزيز الاستثمار في القطاع المالي.

4/ نتائج المحور الخامس: حماية المعاملات التجارية:

جدول رقم 16: إجابات المحور الخامس-حماية المعاملات التجارية البنكية-

رقم الفقرة	التكرارات	أوافق بشدة 5	أوافق 4	محايد 3	لا أوافق 2	لا أوافق بشدة 1	المتوسط المرجح	الانحراف المعياري	النسبة المئوية	اتجاه العينة	رتبة الفقرة
21	ni	25	25	0	0	0	4.50	0.51	90.0%	أوافق بشدة 5	1
	%Fi	50.0%	50.0%	0.0%	0.0%	0.0%					
22	ni	18	28	2	2	0	4.24	0.72	84.8%	أوافق بشدة 5	3
	%Fi	36.0%	56.0%	4.0%	4.0%	0.0%					
23	ni	4	44	2	0	0	4.04	0.35	80.8%	أوافق 4	4
	%Fi	8.0%	88.0%	4.0%	0.0%	0.0%					
24	ni	25	25	0	0	0	4.50	0.51	90.0%	أوافق بشدة 5	2
	%Fi	50.0%	50.0%	0.0%	0.0%	0.0%					
المتوسط الحسابي المرحج للمحور ككل							17.28				
الانحراف المعياري للمحور ككل								1.51			

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

1. **التعليق:** من الجدول أعلاه، تظهر النتائج مستويات مرتفعة جداً من الاتفاق، حيث بلغ المتوسط المرحج

للفقرات بين 4 و 4.50 و نسب مئوية بين (80.8% و 90.0%)، وهو ما يعكس اقتناع المبحوثين بأن

إجراءات الحماية الرقمية والأمن السيبراني تساهم بفعالية في تأمين المعاملات البنكية. كما أن الانحرافات

المعيارية المنخفضة تدل على وجود انسجام واضح بين أفراد العينة حول أهمية الحماية الإلكترونية. هذه

الآخيرة التي تؤدي إلى تقليل حالات الاحتيال المالي والاختراقات الإلكترونية، ما يساهم في الحفاظ على

الاستقرار المالي وتقوية ثقة المستثمرين والعملاء في النظام البنكي و الذي يعد حجر الزاوية في زيادة معدلات "الشمول المالي". فكلما زادت حماية المعاملات، زاد تدفق السيولة عبر القنوات الرسمية، مما يقلل من حجم الاقتصاد الموازي ويدعم النمو الإجمالي للناتج المحلي، والتوسع في التجارة الإلكترونية والخدمات المالية الرقمية.

المطلب الثاني: مناقشة النتائج و اختبار الفرضية الرئيسية:

من خلال عناصر هذا المطلب تم الوقوف على اختبار الفرضية الرئيسية للدراسة وذلك من خلال مجموعة من الاختبارات كما هو موضح.

الفرع الأول: مناقشة النتائج:

1/ تحليل الارتباط بين المتغيرين) التكامل بين الرقمنة و الأمن السيبراني و حماية المعاملات التجارية البنكية)

أ. تحليل الارتباط بين التكامل بين الرقمنة و الأمن السيبراني(المتغير المستقل) و حماية المعاملات التجارية البنكية(المتغير التابع):

جدول رقم 17: تحليل معامل الارتباط Pearson

0.484	ارتباط Pearson
< 0.001	Sig
50	N

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: بناء على الجدول السابق معامل الارتباط Pearson يساوي 0.484 و قيمة مستوى الدلالة $0.001 <$ و هي أقل من 0.01 و هذا يعني أن العلاقة دالة إحصائياً و بالتالي نرفض الفرض الصفري و نقبل البديل.

اتجاه العلاقة: بما أن إشارة الارتباط موجبة و هذا يعني وجود علاقة طردية، أي كلما زاد التكامل بين الرقمنة و الأمن السيبراني كلما زادت حماية المعاملات البنكية من الهجمات السيبرانية.

قوة العلاقة: قيمة الارتباط 0.484 تشير إلى علاقة متوسطة القوة رغم أنها دالة إحصائياً إلا أن تأثيرها متوسط على العينة، و هذا يعود إلى أن حماية المعاملات البنكية لا يعتمد على التكامل التقني فقط، بل تتأثر أيضاً بمتغيرات أخرى مثل القوانين التشريعية، دور الموظفين و التي لم نتناولها.

هذا و تؤكد قيمة Sig التي تساوي 0.001 < أن هذا الدور حقيقي و مؤكد إحصائياً و لا يمكن إهماله في الاستراتيجيات البنكية.

2/ تحليل التباين بين المتغيرين (التكامل بين الرقمنة و الأمن السيبراني و حماية المعاملات التجارية البنكية)

أ. تحليل جدول التباين : (ANOVA) : يُستخدم هذا الجدول للحكم على الصلاحية العامة لنموذج

الانحدار، أي هل "التكامل بين الرقمنة و الأمن السيبراني " يؤثر فعلياً في "حماية المعاملات التجارية البنكية"؟

جدول رقم 18: تحليل التباين ANOVA

النموذج	مجموع مربعات الانحدار	درجة الحرية	متوسط المربعات	التباين المفسر F	Sig
الإنحدار	26.264	1	26.264	14.690	< 0.001
البواقي	85.816	48	1.788		
المجموع	112.080	49			

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

جدول رقم 19: المعاملات

النموذج	B	الخطأ المعياري	Beta	t	Sig
الثابت	2.720	1.981		4.906	< 0.001

التكامل بين الرقمنة و الأمن السيبراني	0.30	0.78	0.484	3.833	< 0.001
---------------------------------------	------	------	-------	-------	---------

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق:

• قيمة F: بلغت 14.690.

• الدلالة الإحصائية (Sig): القيمة أقل من 0.001، وهي أصغر بكثير من مستوى الدلالة المعتاد (0.05)

• الاستنتاج: النموذج صالح إحصائياً بشكل قوي، مما يعني أن هناك علاقة حقيقية وذات دلالة بين المتغيرين، وليست ناتجة عن الصدفة.

ب. تحليل جدول المعاملات (Coefficients) : يساعد هذا الجدول في صياغة معادلة التنبؤ وتحديد قوة واتجاه التأثير:

➤ معامل الارتباط و البيتا (Beta)

• قيمة Beta المعامل المعياري هي 0.484. بما أنها موجبة، فهناك علاقة طردية؛ أي أن زيادة الدرجات في "المتغير المستقل" تؤدي إلى زيادة الدرجات في المتغير التابع.

• القيمة (0.484) تشير إلى تأثير متوسط القوة.

➤ اختبار (t) والدلالة

• قيمة t للمتغير المستقل: هي 3.833 بمستوى دلالة أقل من 0.001.

• هذا يؤكد أن المتغير المستقل مساهم جوهري وفريد في تفسير التغيرات الحاصلة في المتغير التابع.

➤

صياغة معادلة الانحدار (غير المعيارية) من خلال العمود (Unstandardized B) ، يمكننا بناء المعادلة التالية:

$$Y=2.720 + 0.30x$$

تفسير المعادلة:

1. الثابت (2.720): هي القيمة المتوقعة للمتغير التابع "حماية المعاملات التجارية البنكية" إذا كانت قيمة المتغير المستقل التكامل بين الرقمنة والأمن السيبراني صفراً.
2. الميل (0.300) : يعني أنه مقابل كل زيادة بمقدار درجة واحدة في المتغير المستقل، يتوقع زيادة المتغير التابع بمقدار 0.300

ت. تحليل بيانات جدول ملخص النموذج:

جدول رقم 20: ملخص النتائج

النموذج	معامل الارتباط R	معامل التحديد R ²	معامل التحديد المعدل	الخطأ المعياري للتقدير
1	0.484	0.234	0.218	1.33710

المصدر: من إعداد الطالبتين بناء على مخرجات برنامج SPSS27

التعليق: معامل الارتباط $R = 0.484$ يشير إلى وجود علاقة طردية متوسطة القوة بين المتغير المستقل المتغير التابع.

معامل التحديد $R^2 = 0.234$ هذه القيمة تعني أن المتغير المستقل التكامل بين الرقمنة و الأمن السيبراني يفسر 23.4 % من التباين الحاصل في المتغير التابع حماية المعاملات التجارية البنكية. النسبة الباقية تعود لعوامل أخرى لم تتضمنها الدراسة الحالية.

معامل التحديد المعدل: 0.218 و هو تعديل لمعامل التحديد ليصبح أكثر دقة، خاصة عند تعميم النتائج على المجتمع الاصلي، و هي قريبة من القيمة السابقة مما يدل على استقرار النموذج. الخطأ المعياري للتقدير = 1.33710 يمثل مدى تشتت القيم الفعلية حول خط الانحدار، فكلما قلت هذه القيمة زادت دقة التنبؤ.

الفرع الثاني: اختبار صحة الفرضية الرئيسية:

1/ اختبار الفرضية الرئيسية: يوجد أثر ذو دلالة إحصائية للتكامل بين الرقمنة و الأمن السيبراني و بين حماية المعاملات التجارية في البنوك التجارية.

تشير النتائج أعلاه إلى وجود تأثير إيجابي (طردى) دال إحصائياً للتكامل بين الرقمنة و الأمن السيبراني على حماية المعاملات التجارية البنكية. النموذج يمتلك قدرة تفسيرية جيدة، حيث أن العلاقة بينهما حقيقية ولا تعود للصدفة.

بناءً على قيمة ($\text{Sig} < 0.001$)، و هو ما يدعم الفرضية التي تشير إلى وجود دور للتكامل بين الرقمنة و الأمن السيبراني في حماية المعاملات التجارية البنكية.

2/ النتيجة العامة: أظهرت الدراسة الميدانية وجود أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \geq 0.05$)

للتكامل بين الرقمنة و الأمن السيبراني في تعزيز حماية المعاملات التجارية البنكية. و من خلال النتائج السابقة يمكن تلخيص الاستنتاجات في ما يلي:

- **تفسير القوة الارتباطية :** ترابط وثيق يدل على وجود علاقة طردية ذات دلالة إحصائية، ما يعني أنه كلما زاد مستوى التكامل بين الرقمنة و الأمن السيبراني في البنك، زادت كفاءة حماية المعاملات التجارية فيه. و

وصف العلاقة بالمتوسطة يعكس واقعا بنكيا يتسم بالحذر، حيث يؤكد معامل الارتباط أن الرقمنة ليست مجرد تكنولوجيا معزولة، بل هي عملية تتطلب غطاء امنيا سيبرانيا موازيا لضمان سلامة المعاملات التجارية البنكية.

- تفسير القوة التنبؤية: يبين معامل التحديد 0.234 أن التكامل بين الرقمنة و الأمن السيبراني يساهم بنسبة تقارب الربع في حماية المعاملات التجارية البنكية، و تعتبر هذه النسبة مقبولة، لكنها تستدعي ضرورة البحث عن المتغيرات الأخرى المكملة (مثل التشريعات القانونية، العنصر البشري، البنية التحتية الرقمية) لتغطية ما تبقى من حماية.

- الفجوة التقنية و الأمنية: وجود أثر متوسط القوة يشير إلى وجود تحديات قد تحد من فعالية هذا التكامل، مثل تقادم بعض الأنظمة البرمجية، أو وجود ثغرات لإي بعض التطبيقات الرقمية، أو حتى نقص التنسيق بين قسمي تكنولوجيا المعلومات و المخاطر.

- دلالة النموذج: بما أن مستوى الدلالة Sig أقل من 0.05، فهذا يؤكد أن الأثر المشاهد ليس ناتجا عن الصدفة بل هو أثر حقيقي يتطلب من البنوك التجارية وضع استراتيجيات لتعزيز هذا التكامل.

خاتمة الفصل الثالث: من خلال ما تم تناوله في هذا الفصل، نستنتج أن الرقمنة وحدها لا تكفي لخلق بيئة تجارية آمنة، بل إن قيمتها المضافة كمن في تكاملها مع الأمن السيبراني. هذا و يظهر أيضا، أن إجراءات الأمن السيبراني لا تزال إجراءات تصحيحية للمسار الرقمي، بدلا من أن تكون جزءا لا يتجزأ من بنية النظام الرقمي منذ البداية.

الخاتمة

إنَّ الرقمنة التي يشهدها القطاع المصرفي فرضت واقعًا جديدًا قائمًا على السرعة، الكفاءة، وتوسيع نطاق الخدمات البنكية الرقمية، مما جعل الرقمنة عنصرًا أساسيًا في تطوير الأداء البنكي وتحسين جودة المعاملات التجارية. غير أن هذا التطور صاحبه تزايد في المخاطر والتهديدات السيبرانية التي تستهدف البيانات المالية والمعاملات الرقمية، الأمر الذي جعل الأمن السيبراني ضرورة استراتيجية وليس مجرد خيار تقني.

وقد أظهرت الدراسة أن التكامل بين الرقمنة والأمن السيبراني يمثل ركيزة أساسية لضمان حماية المعاملات التجارية داخل البنوك التجارية، حيث يساهم هذا التكامل في تعزيز سرية المعلومات، حماية البيانات من الاختراق، ضمان استمرارية الخدمات البنكية، ورفع مستوى الثقة لدى العملاء والمتعاملين. كما بينت النتائج أن نجاح هذا التكامل لا يعتمد فقط على تبني التقنيات الحديثة، بل يرتبط أيضًا بوجود سياسات أمنية فعالة، بنية تحتية رقمية قوية، وتأهيل الموارد البشرية لمواكبة التطورات التكنولوجية بالإضافة إلى التشريعات و القوانين التي ستساعد على المضي قدما نحو استراتيجية مستقبلية للتكامل التقني.

وعليه، فإن تحقيق الحماية الفعالة للمعاملات التجارية البنكية يتطلب رؤية شاملة تجمع بين التطوير الرقمي المستمر وتعزيز منظومة الأمن السيبراني، بما يضمن مواجهة التهديدات المتزايدة وتحقيق الاستقرار والأمان في البيئة المصرفية الحديثة. ومن ثم، يبقى الاستثمار في هذا التكامل ضرورة حتمية لتعزيز تنافسية البنوك وضمان استدامة نشاطها في ظل الاقتصاد الرقمي المتسارع.

نتائج الدراسة:

— تساهم الرقمنة في تحسين كفاءة المعاملات التجارية البنكية من خلال تسريع العمليات وتسهيل تقديم الخدمات البنكية الرقمية.

- _ يلعب الأمن السيبراني دورًا مهمًا في حماية البيانات البنكية والمعاملات المالية من مختلف التهديدات والهجمات الإلكترونية.
- _ توجد علاقة تكاملية بين الرقمنة والأمن السيبراني، حيث لا يمكن تحقيق خدمات رقمية فعالة دون توفير حماية سيبرانية قوية.
- _ يساهم التكامل بين الرقمنة والأمن السيبراني في تعزيز ثقة العملاء بالخدمات البنكية الرقمية وتحقيق استمرارية العمل البنكي بأمان.
- _ تواجه البنوك التجارية عدة تحديات سيبرانية نتيجة التوسع في استخدام التكنولوجيا الحديثة والخدمات الإلكترونية.
- _ تعتمد البنوك التجارية على مجموعة من الوسائل الأمنية الحديثة مثل التشفير وأنظمة الحماية الإلكترونية للحد من المخاطر السيبرانية.
- توصيات الاجرائية للبنوك التجارية:**
- **تبني استراتيجية الامن بالبناء (Security by Design):** توي الدراسة بضرورة دمج معايير الامن السيبراني منذ المراحل الاولى لتميم اي نظام رقمي جديد في البنك، و ليس كإجراء لاحق لضمان مستويات التكامل.
- **تطوير البنية التحتية الموحدة:** العمل على إيجاد منصات تقنية توحد عمليات الرقمنة مع طائفة الراء السيبرانية، مما يقلل من الثغرات التي قد تظهر عند فصل النظامين.
- **الاستثمار في الكفاءات المزدوجة:** عقد دورات تدريبية لموظفي التقنية تركز على الرقمنة الامنة، بحيث يمتلك الموظف مهارة التعامل مع التحول الرقمي و فهم مخاطر الامن السيبراني في نفس الوقت.
- مقترحات لبحوث مستقبلية:**
- إجراء دراسة مشابهة تتناول دور وعي الموظفين كمتغير وسيط بين التكامل التقني و حماية المعاملات.

- دراسة أثر التشريعات القنونية في تعزيز التكامل بين الرقمنة و الامن السيبراني في القطاع المصرفي.

قائمة المراجع والمصادر

أولاً: المراجع باللغة العربية:

1/ الكتب:

- أحمد قاسم الجمال وآخرون، التحول الرقمي في مؤسسات التعليم العالي العربية: الواقع، التحديات، والمقاربات المستقبلية، دار الكتب الوطنية، الرابطة العربية للعلوم الاجتماعية والإنسانية التابعة لاتحاد مجالس البحث العلمي العربية، بنغازي- ليبيا، سبتمبر 2023
 - أحمد مختار عمر، معجم اللغة العربية المعاصرة
 - الطاهر لطرش، تقنيات البنوك، الطبعة الرابعة، ديوان المطبوعات الجامعية، الجزائر، 2005،
 - بوكعبان عكاشة، القانون المصرفي الجزائري في ضوء الاجتهاد القضائي للمحكمة العليا ومجلس الدولة، دار الخلدونية، الجزائر، 2017،
 - دريد كامل آل شبيب، إدارة العمليات المصرفية، الطبعة الأولى، دار المسيرة، الأردن، 2015
 - حسن محمد الحسين ، أساسيات الأمن السيبراني، حلب، سوريا 2022
 - شادي عبد الوهاب منصور، حروب الجيل الخامس: أساليب" التفجير من الداخل " على الساحة الدولية، العرب للنشر والتوزيع، القاهرة، 2019.
 - معاوية فهد داود القواسمي، التحول الرقمي في المصارف الإسلامية: دراسة تطبيقية على المصارف الإسلامية في دولة فلسطين، الطبعة 2 ، دار الجنان للنشر والتوزيع، الأردن، 2025
 - معلوف، هـ. المنجد في اللغة العربية المعاصرة.. دار المشرق، بيروت، طبعة 2000.
- مجمع اللغة العربية بالقاهرة

2/ الجرائد الرسمية:

- نظام بنك الجزائر رقم 09/03 مؤرخ في 26 ماي، 2009 المحدد للقواعد العامة المتعلقة بشروط البنوك المطبقة على العمليات المصرفية، الجريدة الرسمية للجمهورية الجزائرية، المطبوعة الرسمية للأمانة العامة للحكومة، الجزائر، 2009، العدد، 53 المادة 2.
- نظام بنك الجزائر رقم 13/01 مؤرخ في 8 أفريل، 2013 المحدد للقواعد العامة المتعلقة بالشروط البنكية المطبقة على العمليات المصرفية، الجريدة الرسمية للجمهورية الجزائرية، المطبوعة الرسمية للأمانة العامة للحكومة، الجزائر، 2013، العدد، 29 المادة 10 والمادة 11.

3/ المقالات العلمية:

- أحمد مشهور، تكنولوجيا المعلومات وأثرها على التنمية الاقتصادية، المؤتمر العربي الثالث للمعلومات الصناعية والشبكات المنظمة العربية للتربية والثقافة والعلوم ، 2003 ،
- الاتحاد الدولي للاتصالات ITU ، "تأمين شبكات المعلومات والاتصالات: أفضل الممارسات من أجل بناء ثقافة الأمن السيبراني"، قطاع تنمية الاتصالات، لجنة الدراسات الأولى، المسألة، 22/1 فترة الدراسة (2006-2010)،
- بن أحمد، فاطمة الزهراء، وبن أحمد نادية، "التحول الرقمي في الجزائر: الواقع والتحديات ، المجلة الجزائرية المالية العامة، المجلد 15 ، العدد 01 ، الجزائر، 2025،
- حميدوش علي، بوزيد حميد، اقتصاديات الأعمال القائمة على الرقمنة" المتطلبات والعوائد " تجارب دولية"-دروس وعبر"، المجلة العلبة المستقبل الاقتصادي، العدد 1، المجلد 8، 2020
- ربيع نصيرة، حتمية الرقمنة كآلية لتطبيق الإدارة الإلكترونية في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية -المجلد 06 -العدد 02 - ديسمبر 2021،
- سعيد يقطين، "العالم الرقمي وتحولات الكتابة والنشر"، مجلة عالم الفكر، العدد 4، المجلد 39، 2011
- سندس بن عبد الله، الخدمات المصرفية الرقمية ودورها في ربحية البنوك التجارية الجزائرية دراسة حالة البنك الوطني الجزائري خلال الفترة 2017-2021، مجلة الاقتصاديات المالية البنكية و إدارة الأعمال، المجلد 13 /العدد 01 (2024)،
- عائشة عبيد هلا مبارك قويضي العازمي، واقع الأمن السيبراني في التعليم وعلاقته بالأمن النفس من وجهة نظر المعلمات بدولة الكويت، المجلة الدولية لنشر البحوث والدراسات، المجلد 5 - الصادر 59، تأريخ النشر: 20 سبتمبر 2024
- عبد الغاني شرقي، التهديدات السيبرانية وإشكالية السيادة، إعادة قراءة للسيادة و معاهدة وستيفاليا، مجلة السياسة العالمية، مجلد 07، عدد 02، 2023
- فيولا مخزوم، قيادة التحول الرقمي في الفصول الدراسية: دور المعلم في عصر التكنولوجيا، المركز الديمقراطي العربي للدراسات الإستراتيجية والاقتصادية والسياسية، ألمانيا/برلين، 2024
- محمد دحماني، الذكاء الاصطناعي كآلية لتعزيز الأمن السيبراني، مجلة الفكر القانوني و السياسي، المجلد 07، العدد 02، 2023

- مرسي خولة- هاجر موساوي، تطبيق التحول الرقمي كآلية لتحسين أداء البنوك: دراسة حالة متعددة الجنسيات- مجلة المنهل الاقتصادي، جامعة الشهيد حمه لخضر-الوادي- المجلد، 06 العدد 01، جوان 2023،
- مروة فتحي السيد البغدادي، اقتصاديات المن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، العدد السادس والسبعون، جوان 2021،
- مسفرة بنت دخيل الله الخثمي، مشاريع وتجارب التحويل الرقمي في مؤسسات المعلومات: دراسة للاستراتيجيات المتبعة، مجلة RIST، مجلد 34، العدد 13،
- منى عبد الله السمحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد 111، جامعة المنصورة، المملكة العربية السعودية، 2020
- مصطفى قطب، الرقمنة والتحول الرقمي: المفهوم، الفرق، والأثر على المؤسسات الحديثة، مقال منشور على موقع أكاديمية مهارات التخطيط الاستراتيجي بتاريخ 2025/07/15
- نورة شلوش، القرصنة الإلكترونية في الفضاء السيبراني " التهديد المتصاعد أامن الدول"، مجلة مركز بابل للدراسات الإنسانية، جامعة بابل، العراق، المجلد 8، العدد 2، 2018

4/ المذكرات و الرسائل الجامعية:

- العربي حسيبة، جودة الخدمات المرفية في الجزائر من وجهة نظر الزبون، مذكرة مقدمة ضمن متطلبات نيل شهادة الماجستير في العلوم التجارية تخصص: تسويق العمليات المالية والمصرفية، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير قسم العلوم التجارية، جامعة الجزائر 3، 2015-2016،
- بوازدي جمال، الأمن السيبراني، محاضرات مقدمة لطلبة السنة الثانية ماستر، تخصص دراسات استراتيجية وأمنية، جامعة الجزائر 3، السنة الجامعية 2020-2021
- طاهر محمد السعيد ،سليمان خالد ، متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية ، (دراسة حالة مؤسسة نفطال فرع غرداية) ،مذكرة مقدمة لإستكمال شهادة الماستر الأكاديمي، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم العلوم والمحاسبة ،تخصص محاسبة ،سنة 2022 - 2023
- إيمان محمد الشورة، الأمن السيبراني في البنوك الإسلامية الأردنية، البحث استكمالاً لمتطلبات الحصول على درجة البكالوريوس في المصارف الإسلامية، الجامعة الأردنية، كلية الشريعة، قسم المصارف الإسلامية، 2020

5/ المواقع الإلكترونية باللغة العربية:

- موقع البديل، الرقمنة في اللغة العربية، مقال نشر في 14 أبريل 2019.
- <https://hbrarabic.com> المفاهيم الإدارية الأمن السيبراني
- الهجمات السيبرانية على البنوك، مقال نشر بتاريخ 2025 /2/19، موقع سايبروان
- <https://al-khwarizmi.com> أهمية الحماية السيبرانية في العصر الرقمي
- <https://elbadilabc-ar.dz>
- <https://ar.wikipedia.org>
- <https://hbrarabic.com>
- موقع ريناد المجد، الحماية من الهجمات السيبرانية: ست أدوات للأمن السيبراني، مقال نشر في 2021/8/2
- رؤى حمود، تحديات الأمن السيبراني في المؤسسات المالية، مقال نشر بتاريخ 2021/05/26 ، موقع شركة ريناد المجد

ثانيا: المراجع باللغات الأجنبية:

1/ Livres:

- Gobble, MaryAnne M., Research technology management : RTM . - Arlington, VA : Industrial Research Inst., ISSN 0895-6308, ZDB-ID 616140-6. - Vol. 61.2018, 4,
- Jocko Lozic & Katerina Fotova Čiković, 'Digital Transformation: The Fundamental Concept of Transformation of Business Activities, Zagreb, 2024
- Larousse 2022
-

2/ Publications scientifiques:

- ABOUD OMAIR DELIMI ARRAK, Cybersecurity as One of the Pillars of Digital Transformation in Organizations: Selected International Experiences, Scientific Journal of Economic Dialogue, Volume: 04 / N°: 02 (2026)
- Bouhafes Hanen, Cyberscurity in the digital era: between digital transformation and protection challenges, Faculty of low, University Ain Temouchent, Algeria, 2025.
- ELMOUTAOUKIL. A ; BELKACEM. C (2025) «Le digital, le numérique, la transition et la transformation digitales : des définitions en difficulté», Revue Française d'Economie et de Gestion «Volume 6 : Numéro 2»

- Bilgin Metin, Fatma Gül Özhan, Martin Wynn, Digitalisation and Cybersecurity: Towards an Operational Framework, journal electronics, October 2025

3/ Les sites Web:

- [https://aws.amazon.com/ what-is/digital-transformation](https://aws.amazon.com/what-is/digital-transformation)
- [https:// www .alansariexchange.com/ar/blog/potential-cyberattacks-threaten-financial-systems](https://www.alansariexchange.com/ar/blog/potential-cyberattacks-threaten-financial-systems)
- [https:// www. bakkah.com/ar/knowledge-center/how-to-perform-a-cyber-risk-assessment](https://www.bakkah.com/ar/knowledge-center/how-to-perform-a-cyber-risk-assessment)
- [https:// www .ca-paris.com/banque-innovation/](https://www.ca-paris.com/banque-innovation/) Cybersécurité en banque : une préoccupation de tous les instants
- <https://www.getfocal.ai/ar/blogs/risk-management-in-banking,January 31, 2026>
- <https://keytime.sa/cyberattacks>
- <https://www.ncsc.gov.bh/ar/cyberwiser/cyber-security.html>
- <https://techno-ville.com/securing-banking-transactions-with-technology>
- https://www.trendmicro.com/ar_sa/what-is/attack-surface/cyber-risk-scoring.html

الملاحق

الملحق رقم: (01) الاستبيان

وزارة التعليم العالي و البحث العلمي
جامعة عبد الحفيظ بوالصوف-ميلة-

كلية
استمارة البحث:

الأخ الفاضل، الأخت الفاضلة،
السلام عليكم و رحمة الله و بركاته، يسرنا أن نضع بين أيديكم هذه الإستمارة التي صممت
لجمع المعلومات اللازمة للدراسة التي نقوم بإعدادها للحصول على شهادة الماستر في اختصاص
مالية و تجارة دولية، و التي موضوعها هو " التكامل بين الرقمنة و الأمن السيبراني لحماية
المعاملات التجارية في البنوك الجزائرية".
و نظراً لأهمية رأيكم في هذا المجال، نأمل منكم التكرم بالإجابة على أسئلة الاستمارة بدقة،
حيث أن مشاركتكم ضرورية و رأيكم عامل أساسي في الوصول إلى الهدف من هذه الدراسة.
نحيطكم علماً أن جميع إجاباتكم لن تستخدم إلا لأغراض البحث العلمي فقط .
تقبلوا مني فائق التقدير و الاحترام.

الطالبتان:

بوقاسة هنية

صولي بشرى

المحور الأول: البيانات العامة للبنك

1. نوع البنك:

☐ محلي ☐ إقليمي ☐ دولي

2. حجم البنك من حيث الأصول:

☐ صغير ☐ متوسط ☐ كبير

3. هل لدى البنك إدارة مستقلة للأمن السيبراني؟

☐ نعم ☐ لا

المحور الثاني: استراتيجية الرقمنة في البنك

الرقم	العبارة	مقياس ليكرت الخماسي			
		لا أوافق بشدة	لا أوافق	محايد	أوافق بشدة
01	يملك البنك استراتيجية واضحة للرقمنة و التحول الرقمي				
02	يقدم البنك خدمات مصرفية رقمية متكاملة				
03	تعتمد العمليات البنكية التجارية بشكل كبير على الانظمة الرقمية				
04	يتم تشفير جميع المعاملات البنكية الرقمية				
05	يدعم البنك الابتكار الرقمي مع الحفاظ على معايير أمان عالية				
06	تساهم الرقمنة في تسريع المعاملات التجارية البنكية				

المحور الثاني: ممارسات الأمن السيبراني

الرقم	العبارة	مقياس ليكرت الخماسي			
		لا أوافق بشدة	لا أوافق	محايد	أوافق بشدة
07	يستخدم البنك تقنيات حديثة كالذكاء الاصطناعي و الحوسبة السحابية في تعاملاته				
08	يتم تطبيق سياسات مصادقة متعددة العوامل لحماية المعاملات الرقمية				
09	يتم تقييم المخاطر الأمنية قبل إطلاق أي خدمة رقمية جديدة				
10	توجد خطة استجابة للحوادث السيبرانية واضحة ومفعلة				
11	توجد آلية فورية لاكتشاف الاحتيال الإلكتروني والاستجابة له				
12	هناك تنسيق مستمر بين إدارة تقنية المعلومات وإدارة المخاطر				
13	يتم دمج الأمن السيبراني في جميع مراحل تطوير الخدمات الرقمية				
14	يتم تقليل مخاطر الاحتيال في المعاملات التجارية الرقمية				

المحور الثالث: التكامل بين الرقمنة والأمن السيبراني:

الرقم	العبارة	مقياس ليكرت الخماسي			
		لا أوافق بشدة	لا أوافق	محايد	أوافق بشدة
15	التكامل بين الرقمنة و الأمن السيبراني يعزز ثقة العملاء				
16	يتم إجراء اختبارات اختراق دورية على الأنظمة المصرفية				
17	يشعر العملاء بثقة عالية عند استخدام القنوات الرقمية				
18	يتم قياس أداء الأمن السيبراني بمؤشرات أداء محددة				
19	تساهم التقنيات الرقمية في تحسين الكشف عن الاحتيال				
20	تساهم الرقمنة في اكتشاف الاحتيال				

المحور الرابع: حماية المعاملات التجارية البنكية

الرقم	العبارة	مقياس ليكرت الخماسي			
		لا أوافق بشدة	لا أوافق	محايد	أوافق بشدة
21	يملك البنك إطارًا واضحًا لإدارة مخاطر الأمن السيبراني(استراتيجية مكتوبة للأمن)				
22	يوفر البنك بيئة آمنة لإجراء التحويلات التجارية عبر الإنترنت				
23	تعتمد البنوك على تقنيات المصادقة المتعددة لإجراء المعاملات				

المخلص

المخلص باللغة العربية:

تهدف هذه الدراسة إلى إبراز دور التكامل بين الرقمنة والأمن السيبراني في حماية المعاملات التجارية داخل البنوك التجارية، في ظل التوسع المتزايد في استخدام الخدمات المصرفية الرقمية وتساعد التهديدات السيبرانية. وقد تناولت الدراسة مفاهيم الرقمنة والتحول الرقمي والأمن السيبراني، مع توضيح أهم الخدمات المصرفية الرقمية والمخاطر الإلكترونية التي تواجه القطاع البنكي.

اعتمدت الدراسة على المنهج الوصفي التحليلي، كما تم إجراء دراسة ميدانية باستخدام الاستبيان على مجموعة من البنوك التجارية، بهدف معرفة مدى مساهمة الرقمنة والأمن السيبراني في تعزيز أمن المعاملات البنكية الرقمية.

وتوصلت الدراسة إلى أن الرقمنة ساهمت بشكل كبير في تحسين سرعة وكفاءة الخدمات البنكية، غير أنها زادت في المقابل من حجم المخاطر السيبرانية، مما جعل الأمن السيبراني ضرورة استراتيجية لضمان حماية البيانات والمعاملات المالية. كما أثبتت النتائج وجود علاقة ذات دلالة إحصائية بين التكامل بين الرقمنة والأمن السيبراني وبين حماية المعاملات التجارية البنكية، من خلال تقليل الاختراقات الإلكترونية وتعزيز ثقة العملاء بالخدمات المصرفية الرقمية.

الكلمات المفتاحية: الرقمنة، الأمن السيبراني، البنوك التجارية، المعاملات البنكية الرقمية، الحماية السيبرانية.

Abstract in English:

The study addressed the concepts of digitalization, digital transformation, and cybersecurity, while explaining the main digital banking services and cyber risks facing the banking sector.

The study adopted the descriptive analytical approach and conducted a field study using a questionnaire distributed to a group of commercial banks in order to determine the extent to which digitalization and cybersecurity contribute to enhancing the security of digital banking transactions.

The findings revealed that digitalization has significantly improved the speed and efficiency of banking services; however, it has also increased cyber risks, making cybersecurity a strategic necessity to ensure the protection of data and financial transactions. The results also confirmed the existence of a statistically significant relationship between the integration of digitalization and cybersecurity and the protection

of commercial banking transactions by reducing cyberattacks and enhancing customer trust in digital banking services.

Keywords: digitalization, cybersecurity, commercial banks, digital banking transactions, cyber protection.

Résumé en Français:

L'étude a abordé les concepts de digitalisation, de transformation numérique et de cybersécurité, ainsi que les principaux services bancaires numériques et les risques électroniques aux quels le secteur bancaire est confronté.

L'étude s'est appuyée sur la méthode descriptive et analytique, ainsi qu'une étude de terrain réalisée à l'aide d'un questionnaire distribué à un ensemble de banques commerciales, afin d'évaluer la contribution de la digitalisation et de la cybersécurité à la sécurisation des transactions bancaires numériques.

Les résultats ont montré que la digitalisation a contribué de manière significative à l'amélioration de la rapidité et de l'efficacité des services bancaires, mais qu'elle a également accru les risques cybernétiques, ce qui fait de la cybersécurité une nécessité stratégique pour assurer la protection des données et des opérations financières. Les entre l'intégration de la digitalisation et de la cybersécurité et la protection des transactions bancaires commerciales, à travers la réduction des cyberattaques et le renforcement de la confiance des clients dans les services bancaires numériques.

Mots-clés : digitalisation, cybersécurité, banques commerciales, transactions bancaires numériques, protection cybernétique.