وزارة التعليم العالي والبحث العلمي

جامعة الشهيد الشيخ العربي التبسي – تبسة–

كلية العلوم الاقتصادية، العلوم التجارية، وعلوم التسيير

قسم العلوم الاقتصادية

الرقم التسلسلي: ...../ 2024

مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي (ل م د)

فرع: العلوم الاقتصادية

التخصص: اقتصاد نقدي وبنكي

المذكرة موسومة بـ:

إنعكاسات الأمن السيبراني على أمن المعلومات في البنوك

إعداد الطالبتين:

شيمـــاء مرزوق

زين تركية إجلال

إشـــــــــراف أ.د:

مهـري عبـــد المالك

أعضاء لجنة المناقشة:

الاســم واللقــب	الرتبــة العلميــة	الصفـــة
عثمان عثمانية	أستـــــــاذ	رئيســـــا
مهري عبد المالك	أستـــــــاذ	مشرفـا ومقررا
وئام مـــــلاح	أستـــــــاذ	عضوا مناقشا

السنة الجامعية : 2023-2024

شكر وعرفان

" الحمد لله والشكر لله عز وجل أولا وأخيرا الذي أعاننا على اتمام هذا العمل المتواضع "

ويسعدنا أن نتقدم بجزيل الشكر والتقدير إلى من آمن بقدرتنا على تحقيق النجاح وأرشدنا إلى الأستاذ الدكتور "مهري عبد المالك"

كما أنقدم بالشكر والتقدير والامتنان للأساتذة الكرام "أعضاء لجنة المناقشة" لتفضلهم بمناقشة هذه المذكرة، وعلى القيمة العلمية المضافة من قبلهم إلى هذا البحث.

كما لايفوتنا شكر كافة أساتذة وطاقم إدارة كلية العلوم الإقتصادية.

إهـــــداء

" إلى أمي العزيزة، ملكة قلبي ونجمة تضيء دربي في الظلام، أنت بطلتي وملجئي في كل موقف. وإلى أبي الغالي، الصديق الوفي والرجل الذي علمني معنى الشجاعة والإصرار. ولأخوي الأعزاء، جناحي وسندي، لقلبين ينبضان بالحب، وروحين تمثلان قوتي وعزمي. وإلى جدتي الغالية، الصديقة المخلصة والمعلمة الحكيمة، شكرا على نورك الدائم وحكاياتك الجميلة التي أضاءت حياتي. وإلى كل من ذكرت ولم أذكر، أحبكم بكل ما أوتيت من قلبي".

"إلى عالم من التحديات والتجارب، وإلى عالم لا محدود من الفرص، إلى كل لحظة مررت بثقلها وخفتها، إلى البحث الذي أضاء دربي بنور المعرفة والتفكير، وإلى كل من شاركني في هذه الرحلة، سواء بكلمة تشجيعية أو بفكرة بناءة، إلى كل قلب شاركني اللحظات الصعبة والسهلة على حد سواء، وإلى من تحملوا صبرا وتفانوا في دعمي وتحفيزي".

"إلى أستاذتي "ممو سعيدة" إلى من كانت لي سندا وأختا لكي مني كل الحب والتقدير"

"أدعو الله أن يجزيكم خيرا على كل ما قدمتم لي، وأن يجعل كل عمل تقومون به في ميزان حسناتكم شكرا لكم من القلب. هذه المذكرة لكم، رمزا لتعبير الامتنان والإعتراف بدوركم الرائع في رحلتي الأكاديمية".

شيماء

إهداء

إلى من حاكت سعادتي بخيوط منسوجة من قلبها، إلى ملاكي في الحياة، إلى من كان دعاءها سر نجاحي، وحنانها بلسم جراحي.

(أمي العزيزة) .

إلى مصدر الأمان الذي أستمد منه قوتي.

(والدي العزيز)

إلى فقيد القلب لقد حققت الوعد.

(جدي رحمه الله)

إلى عائلتي، إلى كل من علمني حرفا إلى من ساندني ولو بكلمة.

إجلال

الفهارس

فهرس المحتويات

فهرس الجداول

فهرس الأشكال

فهرس الملاحق

المقدمة العامة

انتشرت المعلومات بشكل واسع في حياتنا اليومية مما جعل العصر الحالي يتميز بلقب "عصر المعلومات"، يعتبر القطاع المصرفي واحدا من أكثر القطاعات اعتمادا على تقنيات المعلومات، ويعزى ذلك إلى طبيعة العمليات المعقدة التي تقوم بها البنوك والضرورة الملحة للدقة والسرعة في تنفيذها، فقد فتحت شبكة الانترنت آفاقا واسعة أمام البنوك وساهمت في تعزيز كفاءة أنظمة المدفوعات والخدمات المصرفية، بالإضافة إلى تخفيض تكاليف التشغيل المرتبطة بهذه البنوك، وهو ما أتاح لها توسيع نطاق العمل وخلق مزيد من الفرص التنافسية في أسواقها.

في هذا الإطار توجه صناع القرار على المستوى الدولي إلى الإستعانة بالمجهود العلمي والأكاديمي لتقديم البدائل العلمية التي شكلت احدى أهم مضامين السياسات الأمنية وطنيا اقليميا ودوليا المقترحة، والتي تجلت في طرح تصورات واستراتيجيات الأمن السيبراني حيث يتم تحديث الأنظمة المصرفية وتطويرها باستمرار لتلبية متطلبات العصر الرقمي، للحفاظ على الثقة في النظام المصرفي وضمان سلامة المعلومات.

يعتبر أمن المعلومات في سياق البنوك عنصرا حيويا لا يمكن الاستهانة به، حيث تعتمد هذه الأخيرة على تقنيات المعلومات لتخزين ومعالجة البيانات المالية والشخصية للعملاء والمؤسسات، وتتوقف عمليات البنوك على حماية بيانات العملاء والمعلومات المالية من التهديدات السيبرانية المتزايدة، بالإعتماد على مجموعة شاملة من السياسات والتقنيات التي تهدف إلى تأمين البيانات وحمايتها من الوصول غير المصرح به والاختراقات.

ومع ذلك تظل البنوك مستهدفة للعديد من التهديدات السيبرانية المتطورة، التي تشمل الاختراقات الإلكترونية والبرمجيات الخبيثة والهجمات الاحتيالية. تتطلب مواجهة هذه التحديات جهودا مستمرة لتطوير وتعزيز استراتيجيات الأمان، بما في ذلك تحسين التكنولوجيا الدفاعية، وتعزيز الوعي بالأمان لدى الموظفين والعملاء، وتعزيز التعاون بين البنوك والجهات المعنية لمكافحة الجرائم الالكترونية وتقوية البنية التحتية للأمن السيبراني.

إن حدة الهجمات السيبرانية في ظل التطور التكنولوجي المتسارع، جعلت البنوك الجزائرية عرضة لمخاطر جديدة تتعلق بسرقة البيانات المالية والمعلومات الحساسة للعملاء، والتي من الممكن أن تتسبب في خسائر مالية هائلة وتأثيرات سلبية على سمعة البنك وثقة العملاء وفي ظل هذا

السيناريو تتعزز أهمية تبني استراتيجيات أمنية متقدمة تتناسب مع التحديات السيبرانية الحديثة لمكافحة التهديدات بفعالية.

1. التساؤل الرئيسي:

من خلال ما سبق تبرز معالم الإشكالية لهذه الدراسة كالآتي :

ما مدى مساهمة الأمن السيبراني في تعزيز أمن المعلومات في البنوك الجزائرية ؟

2. الأسئلة الفرعية:

من خلال الإشكالية السابقة يمكن طرح عدة تساؤلات فرعية نذكر منها ما يلي:

- ما هي مستحقات الأمن السيبراني في البنك؟
- ما هي مستحقات أمن المعلومات في البنك؟
- هل يوجد تأثير للأمن السيبراني على أمن المعلومات في البنك؟
- هل توجد علاقة ذات دلالة إحصائية عند مستوى دلالة $\alpha = 0.05$ بعدم وافقة موظفي البنك الخارجي لولاية تبسة على توفر متطلبات الأمن السيبراني في البنك؟
- هل توجد علاقة ذات دلالة إحصائية عند مستوى دلالة $\alpha = 0.05$ بموافقة موظفي البنك الخارجي لولاية تبسة على توفر عناصر أمن المعلومات في البنك؟
- هل توجد علاقة ذات دلالة إحصائية عند مستوى دلالة $\alpha = 0.05$ بعدم إدراك موظفي البنك الخارجي لولاية تبسة نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك؟

3. فرضيات الدراسة:

من خلال إشكالية الدراسة يمكن وضع الفرضية الرئيسية التالية:

- تلعب الجهود المبذولة في مجال الأمن السيبراني دورا أساسيا في منع الهجمات الإلكترونية وحماية البيانات والمعلومات الحساسة في القطاع البنكي بالجزائر.

ومن خلال الفرضية الرئيسية تتدرج عدة فرضيات فرعية كالتالي:

- هناك مستحقات للأمن السيبراني في البنك.
- هناك مستحقات لأمن المعلومات في البنك.
- هناك تأثير للأمن السيبراني على أمن المعلومات في البنوك.
- يوافق موظفو البنك الخارجي لولاية تبسة على توفر متطلبات الأمن السيبراني فيه عند مستوى دلالة $\alpha = 0.05$.
- يوافق موظفو البنك الخارجي لولاية تبسة على توفر عناصر أمن المعلومات فيه عند مستوى دلالة $\alpha = 0.05$.

4. دو افع إختيار الموضوع:

يمكن حصر أهم الأسباب لإختيار هذا الموضوع فيما يلي:

1.4. الأسباب الذاتية: وتتمثل فيما يلي:

- الموضوع يدخل ضمن التخصص.
- الرغبة الشخصية في إنشاء مؤسسة خاصة ومثل هذه المواضيع تطور من إمكانياتي وتساعد على النجاح المستقبلي.

2.4. الأسباب الموضوعية: وتتمثل فيما يلي:

- يعتبر من المواضيع الحديثة نسبيا في العالم والجزائر على وجه الخصوص.
- التطلع لتبيان أهمية الأمن السيبراني ودوره في حياتنا اليومية التي أضحت لا تخلو من المعاملات المصرفية الإلكترونية بمختلف أشكالها والتهديدات التي تحيط بها.
- إدراكنا لأهمية حماية أنظمة المعلومات في الأنظمة المصرفية.

5. أهمية الدراسة:

تنبع أهمية هذه الدراسة كونها تسلط الضوء على قضية مهمة، إذ ستناقش موضوع الأمن السيبراني والهجمات السيبرانية، والربط بينه وبين أمن المعلومات وسريتها في البنوك ومدى تأثيره عليها، وتزداد أهميتها بالبيئة محل الدراسة وهي أحد أهم وأكبر البنوك في الجزائر الخاصة بالقطاع الفلاحي، بنك الفلاحة والتنمية الريفية "المجمع الجهوي للاستغلال" تبسة، وكذا البنك الخارجي الجزائري وكالة -

تبسة-، إضافة الى ابراز الوضع الراهن للأمن السيبراني ودوره في حماية المعلومات من كافة التهديدات السيبرانية في القطاع المصرفي، فإن هذه الجهود تعزز أيضا الاستقرار الاقتصادي وتحمي البنية التحتية الرقمية للبلد مما يعزز الأمن القومي بشكل شامل.

6. أهداف الدراسة:

يمكن إيجاز الأهداف الجوهرية لهذه الدراسة فيما يلي:

- ✍ تقديم أساسيات الأمن السيبراني والهجمات السيبرانية.
- ✍ التطرق إلى المفاهيم المتعلقة بأمن المعلومات في البنوك.
- ✍ معرفة ما اذا كان هناك تأثير للأمن السيبراني على أمن المعلومات في البنوك.
- ✍ تسليط الضوء على التحديات التي تواجه أمن الجهاز المصرفي، والاجراءات اللازمة لحماية المعلومات في البنوك من التعرض للهجمات السيبرانية.
- ✍ تقديم بعض التوصيات في ضوء نتائج الدراسة، بما يؤدي الى الحفاظ على أمن المعلومات في البنوك الجزائرية وحمايتها من التعرض للهجمات السيبرانية بما يضمن الحماية المادية والحماية البرمجية وحماية الأفراد.

7. منهج الدراسة وأدوات التحليل:

تم الاعتماد على المنهج الوصفي والمنهج التحليلي من خلال تحليل المعلومات المتعلقة بالجانب النظري، وذلك للتعرف على الأمن السيبراني وكذا الهجمات السيبرانية، وتبيان مدى خطورتها على كافة فئات المجتمع وأمنهم الاجتماعي والمصرفي ليس على المستوى المحلي فقط بل يشمل المستوى الإقليمي والدولي، وذلك استعانة بمصادر المعلومات المختلفة من كتب ومجلات ودراسات سابقة.

أما في الجانب التطبيقي فتم الاستعانة بمنهج دراسة الحالة حيث تم الاعتماد على الاستبيان بهدف التعرف على انعكاسات الأمن السيبراني على أمن المعلومات في المجمع الجهوي للاستغلال التابع لبنك الفلاحة والتنمية الريفية -تبسة-، وكذا في البنك الخارجي الجزائري وكالة -تبسة-، وتم جمع البيانات الإحصائية الخاصة بالمجمع وتبويبها وتفسيرها تفسيرا موضوعيا بهدف إختبار الفرضيات وإستخلاص النتائج بإستخدام البرنامج الإحصائي SPSS.

8. حدود الدراسة:

من أجل محاولة الإحاطة بالإشكالية الرئيسية لموضوع الدراسة وفهم جوانبها المختلفة تم تحديد مجال زماني ومكاني لها كالآتي:

1.8. الدراسة الأولى:

- **المجال الزمني:** تمت الدراسة خلال الفترة الزمنية الممتدة ما بين 2024/05/12 و2024/05/23.
- **المجال المكاني:** تمت الدراسة التطبيقية في المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية - تبسة-.

2.8. الدراسة الثانية:

- **الحدود الزمنية:** كانت فترة اجراء الدراسة التطبيقية لهذا الموضوع وإعداده خلال شهري مارس وأفريل 2024 في البنك الخارجي الجزائري وكالة تبسة رقم 46.
- **الحدود المكانية:** يتمثل المجال المكاني الذي تم اختياره للقيام بالدراسة البنك الخارجي الجزائري وكالة 46 تبسة.
- **الحدود الموضوعية:** ترتكز الدراسة بصفة عامة نظريا وتطبيقيا على توضيح دور الأمن السيبراني كمتغير مستقل على اتخاذ حماية أمن المعلومات في البنوك كمتغير تابع في البنك الخارجي الجزائري بوكالة تبسة.
- **الحدود البشرية:** تمثلت الحدود البشرية حسب موضوع الدراسة باستقصاء آراء موظفي البنك الخارجي الجزائري وكالة 46 تبسة.

9. هيكل الدراسة:

وفي محاولة منا للإجابة عن الإشكالية ركزنا على خطة تتضمن جزئين كما يلي:

- **الجزء الأول:** الأدبيات النظرية للأمن السيبراني وأمن المعلومات في البنوك يضم ثلاث أقسام (إطار نظري وأساسيات لكل من الأمن السيبراني، أمن المعلومات في البنوك،

الهجمات السيبراني)، وتم التوصل إلى أن اجراءات وتقنيات الأمن السيبراني تساهم بشكل كبير في حماية البيانات الحساسة ف البنوك من الهجمات السيبرانية المحتملة الوقوع.

- **الجزء الثاني:** دراسة ميدانية للمجمع الجهوي للاستغلال لبنك بدر -تبسة- ويضم (تقديم عام للمؤسسة، الدراسة الميدانية)، تم اختبار فرضيات الدراسة المتعلقة بمدى مساهمة الأمن السيبراني في توفير أمن للمعلومات في البنوك وتقديم النتائج وكذا التوصيات.

- **الجزء الثالث:** أضيف هذا الجزء للجانب التطبيقي للدراسة وذلك من أجل تبيان انعكاسات الأمن السيبراني على أمن المعلومات في البنك الخارجي الجزائري وكالة 46 - تبسة، وقد تم تقسيم هذا الجزء الى ثلاث أقسام، حيث تم تقديم البنك الخارجي الجزائري وكالة تبسة في أول قسم، أما في القسم الثاني فقد تم فيه تحديد الإطار المنهجي للدراسة، وأخيرا خصص القسم الثالث لتحليل النتائج المتحصل عليها من الدراسة واختبار الفرضيات ومناقشتها.

10. 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:

- يظهر هذا الموضوع بشكل جديد نسبيا ويعاني من نقص في المراجع باللغة العربية.
- صعوبة في الحصول على وثائق من أجل استخدامها كملاحق.
- قصر المدة **المعينة** للدراسة التطبيقية بالمجمع الجهوي للاستغلال.
- غياب الثقافة التوعوية والتعليمية في مجال حماية البيانات المصرفية نسبيا.

الجزء الأول:

الأدبيات النظرية للأمن السيبرانى

وأمن المعلومات فى البنوك

تمهيد

في عصر 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 المؤسسات المالية 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. ولأجل ذلك نعالج في الجزء الأول الأقسام التالية :

1. **الدراسات السابقة.**
2. **مدخل مفاهيمي للأمن السيبراني.**
3. **أساسيات حول أمن المعلومات في البنوك.**
4. **الإطار النظري للهجمات السيبرانية.**

1. الدراسات سابقة

في هذا القسم سيتم تقديم نظرة شاملة على الدراسات السابقة التي استكشفت الأمن السيبراني وأمن المعلومات في البنوك، حيث يهدف هذا القسم إلى توضيح البحوث والدراسات السابقة التي تناولت هذا الموضوع الحيوي، والتي ستشكل الأساس لفهم السياق الحالي وتحديد الفجوات التي تستدعي البحث والتحليل الجديد حول تأثير الأمن السيبراني على أمن المعلومات في البنوك.

1.1. دراسات عربية محلية وأجنبية

تعد الدراسات السابقة حجر الأساس لأي بحث علمي ناجح، فهي تمثل البوابة لفهم الموضوع بشكل عميق وتقدم للباحث خارطة طريق واضحة لبحثه، وفي الآتي سوف يتم مراجعة وتقييم الدراسات العربية المحلية حول انعكاسات الأمن السيبراني على أمن المعلومات في البنوك.

الجدول رقم (01): يوضح دراسة عبد القادر، بومدين وعبد اللطيف، 2023 بعنوان: أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة دراسة حالة بنك BDL بغرداية.

دراسة (عبد القادر، بومدين وعبد اللطيف 2023)	
عنوان الدراسة	أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة دراسة حالة بنك BDL بغرداية.
نوع الدراسة	مقال علمي (مجلة أبحاث إقتصادية معاصرة)، جامعة غرداية، الجزائر، المجلد السادس، العدد الأول، ص: 253-372.
مجتمع الدراسة	عملاء بنك التنمية المحلية BDL بولاية غرداية.
عينة الدراسة	عينة من 127 فردا من عملاء بنك التنمية المحلية BDL في غرداية.
المنهج المتبع في الدراسة	المنهج الوصفي التحليلي.
هدف الدراسة	➢ التعرف على واقع بنك التنمية المحلية لولاية غرداية الجزائر في مجال الجاهزية الإلكترونية لبيئته المادية والبشرية وأمنه السيبراني. ➢ محاولة تقييم مدى تأثير جاهزية البيئة المادية والبشرية للأمن السيبراني في استخدام الخدمات المصرفية الالكترونية. ➢ الكشف عن مدى تأثير جاهزية البيئة المادية والبشرية للأمن السيبراني في التقليل من المخاطر المدركة والمتوقعة للعملاء. ➢ جاءت هذه الدراسة للإجابة عن التساؤل الأساسي التالي: ما مدى تأثير جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة لدى عينة من عملاء بنك BDL بغرداية؟ والذي يقود إلى تساؤلات ثانوية:

	هل هناك عالقة تأثير مباشرة ذات دلالة إحصائية لجاهزية البيئة المادية والبشرية لألمن السيبراني في تقليل المخاطر المدركة لدى عينة عملاء بنك التنمية المحلية بوالية غرداية؟، هل هناك عالقة تأثير مباشرة ذات دلالة إحصائية لتقليل المخاطر المدركة في استخدام الخدمات المصرفية الإلكترونية لدى عينة عملاء بنك التنمية المحلية بوالية غرداية؟، هل هناك عالقة تأثير مباشرة ذات دلالة إحصائية لجاهزية البيئة المادية والبشرية للأمن السيبراني في استخدام الخدمات المصرفية الإكترونية لدى عينة عملاء بنك التنمية المحلية بولاية غرداية؟
أدوات الدراسة	الإستبيان، برامج (Pathanalysis) و (AMOS V.25) الإحصائية لتحليل نتائج التقييم.
أهم لنتائج الدراسة	➢ مستوى بعدي جاهزية البيئة المادية للأمن السيبراني وبعد جاهزية البيئة البشرية للأمن السيبراني كان متوسط في عمومه، يُرجع الباحثين سبب ذلك إلى حداثة مصطلح الأمن السيبراني من جهة، وعدم الفهم الجيد لأسئلة الاستبانة المخصصة لهذا البعد من قبل المستجوبين من جهة أخرى؛ ➢ وجود تأثير ذو دلالة إحصائية لجاهزية البيئة المادية والبشرية للأمن السيبراني في تقليل المخاطر المدركة لدى عينة عملاء بنك التنمية المحلية بولاية غرداية عند مستوى دلالة 0.05؛ ➢ وجود تأثير ذو دلالة إحصائية لتقليل المخاطر المدركة في استخدام الخدمات المصرفية الالكترونية لدى عينة عملاء بنك التنمية المحلية بولاية غرداية عند مستوى دلالة 0.05؛ ➢ وجود تأثير ذو دلالة إحصائية لجاهزية البيئة المادية والبشرية للأمن السيبراني على استخدام الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة لدى عينة عملاء بنك التنمية المحلية بولاية غرداية عند مستوى 0,05 دلالة.

المصدر: صواق عبد القادر وآخرون، **أثر جاهزية الأمن السيبراني على الخدمات المصرفية الإلكترونية من خلال تقليل المخاطر المدركة دراسة حالة بنك BDL بغرداية.**

الجدول رقم (02): يوضح دراسة محمد ومواد 2023 بعنوان: تحديات الامن السيبراني لأنظمة المعلومات في البنوك والمؤسسات المالية.

دراسة (محمد ومواد 2023)	
عنوان الدراسة	تحديات الامن السيبراني لأنظمة المعلومات في البنوك والمؤسسات المالية.
نوع الدراسة	مقال علمي (مجلة إنارة للدراسات الاقتصادية، الإدارية والمحاسبية)، جامعة فرحات عباس، سطيف، المجلد 04، العدد 01، ص، ص: 57-73.
مجتمع الدراسة	دراسة منظور لا يوجد.
عينة الدراسة	دراسة منظور لا يوجد.
المنهج المتبع في الدراسة	المنهج الوصفي التحليلي.
هدف الدراسة	➢ هدفت هذه الدراسة إلى تسليط الضوء على الجرائم الالكترونية وأمن المعلومات المالية في القطاع المصرفي والمالي. ➢ تسليط الضوء على معايير أمن وشفافية نظم المعلومات. ➢ محاولة تقييم مدى تأثير جاهزية البيئة المادية والبشرية للأمن السيبراني في استخدام الخدمات المصرفية الالكترونية. ➢ جاءت هذه الدراسة للإجابة عن التساؤل الأساسي التالي: ما حجم الجرائم الالكترونية التي تحدث في البنوك والمؤسسات المالية؟ والأسئلة الفرعية التالية: كيف يمكن تدمير نظام المعلومات في البنوك والمؤسسات المالية؟ ما أهم طرق الوقاية من الجرائم الالكترونية؟
أدوات الدراسة	الإستبيان، برامج (Pathanalysis) و (AMOS V.25) الإحصائية لتحليل نتائج التقييم.
أهم نتائج الدراسة	➢ أمن المعلومات في القطاع البنكي يمثل منصة إستراتيجية لمناقشة التحديات الأمنية التي تواجهها البنوك والمؤسسات المالية؛ ➢ ضرورة تأمين وحماية البنى التحتية في المؤسسات المالية والاقتصادية مع تعزيز الوعي لدى الخبراء والمهنيين؛ ➢ ضرورة العمل على تطبيق مزيد من الأمان على عمليات التحويل المصرفية الالكترونية من خلال توفير تقنيات أمن الأنظمة لمواجهة التهديدات وسد الثغرات؛ ➢ ضرورة تأمين وحماية البنى التحتية في المؤسسات المالية والاقتصادية مع تعزيز الوعي لدى الخبراء والمهنيين.

المصدر: شايب محمد- حمادي مواد، **تحديات الأمن السيبراني في البنوك والمؤسسات المالية.**

الجدول رقم (03): يوضح دراسة أم الخير 2024 بعنوان كسب رهان الأمن السيبراني ضمان لتعزيز الأمن والدفاع الوطنيين في الجزائر.

دراسة (أم الخير 2024)	
عنوان الدراسة	كسب رهان الأمن السيبراني ضمان لتعزيز الأمن والدفاع الوطنيين في الجزائر.
نوع الدراسة	مقال علمي (مجلة البحوث في الحقوق والعلوم السياسية)، تيارت، الجزائر، المجلد التاسع، العدد الثاني، ص: 53-76.
مجتمع الدراسة	دراسة منظور لايوجد.
عينة الدراسة	دراسة منظور لايوجد.
المنهج المتبع في الدراسة	المنهج الوصفي التحليلي.
هدف الدراسة	جاءت هذه الدراسة للإجابة عن التساؤل الأساسي التالي: إلى أي مدى ستساهم الاستراتيجية المعتمدة من قبل الدولة الجزائرية في كسب الحرب الإلكترونية وتحقيق الأمن السيبراني؟
أدوات الدراسة	الاستبيان، برامج (Pathanalysis) و (AMOS V.25) الإحصائية لتحليل نتائج التقييم.
أهم نتائج الدراسة	➢ إعداد استراتيجيات لتحقيق الأمن السيبراني وجعله أولوية للحفاظ على أمن الأنظمة الرقمية؛ ➢ نشر الثقافة الرقمية لدى البنوك والمؤسسات للتصدي للهجمات السيبرانية؛ ➢ استحداث جملة من النصوص القانونية تتلازم مع طبيعة الهجمات.

المصدر: معتوق أم الخير، **كسب رهان الأمن السيبراني ضمان لتعزيز الأمن والدفاع الوطنيين في الجزائر.**

2.1. الدراسات العربية الأجنبية

تعد الدراسات السابقة الأجنبية مصدرا غنيا للمعلومات حول مختلف المواضيع العلمية، حيث تقدم الدراسات السابقة منظورا عالميا حول موضوع البحث، وتمكن من الاطلاع على أحدث النتائج والدراسات التي أجريت في مختلف دول العالم، وتتيح مقارنة النتائج والدراسات التي أجريت في مختلف الدول، هذا ما يساعد على فهم الموضوع بشكل أفضل ويفتح آفاقا جديدة للبحث العلمي.

الجدول رقم (04): دراسة الشمالي، 2016 بعنوان: أمن وسرية المعلومات وأثرها في الأداء المصرفي دراسة حالة البنوك العاملة في الأردن، الأردن.

دراسة (الشمالي، 2016)	
عنوان الدراسة	أمن وسرية المعلومات وأثرها في الأداء المصرفي دراسة حالة البنوك العاملة في الأردن.
نوع الدراسة	مقال علمي (مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والاقتصادية)، الأردن، المجلد الثاني، العدد السابع، ص، ص: 187-200.
مجتمع الدراسة	26 بنكا، 13 بنكا تجاريا أردنيا، 03 مصارف إسلامية أردنية، 09 بنوك أجنبية
عينة الدراسة	عينة من 135 فردا من عمال البنوك العاملة في الأردن.
المنهج المتبع في الدراسة	المنهج الوصفي التحليلي.
هدف الدراسة	➢ هدفت هذه الدراسة إلى التعرف على أمن المعلومات وحريتها وأثرها في الأداء المصرفي في البنوك العاملة في الأردن من خلال تسليط الضوء على الإجراءات الازمة لأمن المعلومات وسريتها وكيفية تطبيقها في البنوك العاملة في الأردن ➢ ومعرفة تأثير أمن وسرية المعلومات على الاداء المصرفي ➢ جاءت هذه الدراسة للإجابة عن التساؤل الأساسي التالي: ما أثر أمن المعلومات وسريتها على الأداء المصرفي في البنوك العاملة في الأردن؟ والأسئلة الفرعية التالية: ما هو دور الحماية المادية في الأداء المصرفي في البنوك العاملة في الأردن؟ ما هو دور حماية الأفراد في الأداء المصرفي في البنوك العاملة في الأردن؟ ما هو دور الحماية البرمجية في الأداء المصرفي في البنوك العاملة في الأردن؟
أدوات الدراسة	الاستبيان، برامج (ANOVA) الإحصائية لتحليل نتائج التقييم.
أهم نتائج الدراسة	➢ وجود أثر الأمن المعلومات وسريتها (الحماية المادية حماية الأفراد الحماية البرمجية) في الأداء المصرفي في البنوك العاملة في الأردن؛ ➢ ضرورة قيام إدارة البنوك بالممارسات العملية اللازمة النظر أمن المعلومات وحريتها وتعميق ثقافتها في مختلف المستويات الإدارية عن طريق إعداد البرامج تدريبية لجميع المستويات الإدارية؛ ➢ زيادة الإنفاق على برامج أمن وسرية المعلومات والسعي للحصول على الشهادات العالمية المطابقة لأنظمة المعلومات الدولية.

المصدر: الشمالي قاسم حسين، **أمن وسرية المعلومات وأثرها في الأداء المصرفي دراسة تطبيقية على البنوك العاملة في الأردن.**

الجدول رقم (05): دراسة منى 2016 دراسة بعنوان: السيبرانية هاجس العصر، مصر.

دراسة (منى 2016)	
عنوان الدراسة	السيبرانية هاجس العصر.
نوع الدراسة	كتاب (مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والإقتصادية)، الأردن، المجلد الثاني، العدد السابع، ص، ص: 09-215.
مجتمع الدراسة	دراسة منظور لا يوجد
عينة الدراسة	دراسة منظور لا يوجد
المنهج المتبع في الدراسة	المنهج الوصفي التحليلي.
هدف الدراسة	➢ إلقاء الضوء على عدد من المفاهيم والمسائل التي ترتبط بالأمن السيبراني عبر ترشيحها وتشخيص واقعها ورصد أبعادها؛ ➢ إبراز أهمية الأمن السيبراني.
أدوات الدراسة	دراسة منظور لا توجد أدوات دراسة.
أهم نتائج الدراسة	➢ الاعتماد المتزايد على البنى التحتية الخاصة بتقنيات المعلومات والاتصال من قبل الدول والأفراد والمؤسسات عامل محفز لتصاعد نسبة المخاطر على أمن المعلومات؛ ➢ اتخاذ تدابير وإجراءات تضمن إدارة مخاطر تقنيات المعلومات.

المصدر: منى الأشقر جبور، **السيبرانية هاجس العصر.**

الجدول رقم (06): يوضح دراسة فيصل 2019 بعنوان: الأمن السيبراني وأمن المعلومات، السعودية.

(دراسة فيصل 2019)	
عنوان الدراسة	الأمن السيبراني وأمن المعلومات، السعودية.
نوع الدراسة	أطروحة مقدمة ضمن متطلبات نيل شهادة الدكتوراه في الاقتصاد، جامعة قاصدي مرباح ورقلة، 2019، ص، ص: 1-30.
مجتمع الدراسة	استقصاء آراء عينة من المديرون الماليون والمحاسبون وموظفو إدارة تكنولوجيا المعلومات والمراجع الخارجي لشركات الاتصالات، وشركات تكنولوجيا المعلومات، والبنوك العاملة في المملكة العربية السعودية.
عينة الدراسة	عينة من 300 موظفي شركات الاتصالات، شركات تكنولوجيا المعلومات والبنوك العاملة في المملكة العربية السعودية.
المنهج المتبع في الدراسة	المنهج الاستنباطي والاستقرائي.

هدف الدراسة	➢ إلقاء الضوء على تنوع وتعدد المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية واستكشاف أسبابها من خلال المعايير المستخدمة في الأمن السيبراني وتحديد الأكثر تأثيرا؛ ➢ معرفة معايير الأمن السيبراني التي يتم استخدامها عند تطبيقها على أمن المعلومات في المؤسسة؛ ➢ توضيح المحاولات التي تقوم بها المؤسسات للتحوط من المخاطر؛ ➢ جاءت هذه الدراسة للإجابة عن التساؤل الأساسي التالي: ما هي الوسائل التقنية والإدارية التكنولوجية والعمليات والممارسات المصممة التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به؟ والذي يقود إلى تساؤلات ثانوية: ما هي طبيعة المخاطر التي تتعرض لها نظم المعلومات الإلكترونية وماهي أنواعها؟ ما هي أسبا تعرض نظم المعلومات الإلكترونية لتلك المخاطر؟ ما هي المعايير الدولية التي يتم استخدامها في إطار حوكمة أمن المعلومات؟ هل تساهم معايير حوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الإلكترونية؟
أدوات الدراسة	الاستبيان، وبرنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS)لتحليل النتائج.
أهم النتائج الدراسة	➢ يوجد اتفاق معنوي وتجانس في الآراء بين مفردات عينة الدراسة بشأن تعدد المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وتعد المخاطر الخارجية متمثلة في البرامج الخبيثة والاختراقات من أكثر المخاطر أهمية؛ ➢ يعد التدمير المتعمد للبيانات والإدخال المتعمد لبيانات غير صحيحة من أقل المخاطر أهمية؛ ➢ يود اتفاق في آراء مفردات العينة بشأن اختلاف الأهمية النسبة للمخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية؛ ➢ يوجد اتفاق في آراء مفردات العينة حول تعدد أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية، ويعد عدم وجود سياسات وبرامج محددة لأمن المعلومات من أهم تلك الأسباب؛ ➢ يقوم عدد كبير من مفردات العينة بتطبيق المعايير الدولية لحوكمة أمن المعلومات بصورة منفردة، إلا أنها لا تعمل على تطبيق حوكمة أمن المعلومات ضمن استراتيجية الشركة للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية على الرغم من إدراك مفردات العينة لأهمية تطبيق حوكمة أمن المعلومات والفوائد المتحققة منها.

المصدر: عسيري فيصل محمد، **الأمن السيبراني وحماية أمن المعلومات.**

الجدول رقم (07): دراسة مروة (2021) بعنوان: اقتصاديات الأمن السيبراني في القطاع المصرفي، الاسكندرية.

(دراسة مروة2021)	
عنوان الدراسة	اقتصاديات الأمن السيبراني في القطاع المصرفي.
نوع الدراسة	مقال (مجلة البحوث القانونية والاقتصادية، مصر، المجلد الحادي عشر، العدد السادس والسبعون، ص ص: 1546-1516.
مجتمع الدراسة	دراسة منظور لا يوجد
عينة الدراسة	دراسة منظور لا يوجد
المنهج المتبع في الدراسة	المنهج التحليلي المقارن.
هدف الدراسة	➢ إبراز التحديات التي تواجه المجتمع من أجل تحقيق الأمن السيبراني من خلال معرفة دور الدولة في التصدي لهذه الظاهرة والوقاية منها؛ ➢ ابراز التحديات التي تواجه المجتمع من أجل تحقيق الأمن السيبراني.
أدوات الدراسة	دراسة منظور لا توجد أدوات دراسة.
أهم نتائج الدراسة	➢ معالجة اللوائح المتعلقة بالمخاطر التشغيلية والتقنية يساعد في تحقيق عدد من أهداف التنمية المستدامة؛ ➢ ادراج المخاطر السيبرانية ضمن المخاطر التشغيلية للمؤسسات المالية والمصرفية ومراجعتها بشكل مستمر؛ ➢ توسيع نطاق الوصول إلى المعلومات المتعلقة بالتفاعل الاقتصادي بين المؤسسات العامة والخاصة.

المصدر: فتحي مروة السيد البغدادي، **اقتصاديات الأمن السيبراني في القطاع المصرفي.**

3.1. الدراسات باللغة الأجنبية

تعد الدراسات السابقة باللغة الأجنبية مصدرا غنيا للمعلومات حول مختلف المواضيع العلمية، حيث تقدم الدراسات السابقة باللغة الأجنبية منظورا عالميا حول موضوع البحث، وتمكن من الإطلاع على أحدث النتائج والدراسات التي أجريت في مختلف دول العالم، وتتيح مقارنة النتائج والدراسات التي أجريت في مختلف الدول، هذا ما يساعد على فهم الموضوع بشكل أفضل ويفتح آفاقا جديدة للبحث العلمي.

الجدول رقم (08): Sushma, Lewis,2011), Information Security Effectiveness a Research Framework, Issues in Information Systems.

Stady (Sushma, Lewis,2011)	
عنوان الدراسة	Information Security Effectiveness: A Research Framework, Issues in Information Systems.
نوع الدراسة	Scientific article (Issue in Information Systems2011), Robert Morris University, Moon Township, Prennsylvania, US, Volume XII, Number01, p, p: 246-255.
مجتمع الدراسة	موظفي نظم المعلومات.
عينة الدراسة	120 موظف.
المنهج المتبع في الدراسة	المنهج الوصفي التحليلي.
هدف الدراسة	تهدف هذه الدراسة إلى فهم تأثير عمليات التدقيق الأمني والسياسيات الأمنية وأنشطة الردع في المنظمات على فعالية أمن المعلومات.
أدوات الدراسة	الاستبيان ونتائج SPSS.
أهم نتائج الدراسة	تظهر النتائج أن مجال أمن المعلومات وتدقيق الأنظمة يعزز من فعالية أمن المعلومات وتشير النتائج الى وجود علاقة ذات دلالة إحصائية بين تدقيق الأنظمة وفعالية أمن المعلومات.

المصدر: Sushma Mishra, Lewis Chasalow, **Information Security Effectiveness: A Research Framework, Issues in Information Systems**

الجدول رقم (09): Stady (G. NIKHITA, G.J. UGANDER, 2022), Cyber security challenges and its emaergning trends on latest technologies.

Stady (G. NIKHITA, G.J. UGANDER, 2022)	
عنوان الدراسة	Cyber security challenges and its emaergning trends on latest technologies.
نوع الدراسة	R.F. CSE second year (Chaitanya Bharathi) Institute of Technology, Osmania University and Founder Director Peridot , Hyderabad, India, 2022 p, p 01-16.
مجتمع الدراسة	دراسة منظور لايوجد.

عينة الدراسة	دراسة منظور لايوجد.
المنهج المتبع في الدراسة	المنهج الوصفي التحليلي.
هدف الدراسة	تهدف هذه الدراسة إلى إلقاء الضوء على التحديات التي يواجهها الأمن السيبراني وتركز على أحدث ما يتعلق بتقنيات الأمن السيبراني وأخلاقياته والاتجاهات التي تغير وجه الأمن السيبراني.
أدوات الدراسة	لا يوجد.
أهم نتائج الدراسة	كشفت النتائج أن الأمن السيبراني موضوع واسع، حيث يتم استخدام الشبكات لتنفيذ المعاملات الهامة. تستمر الجرائم السيبرانية في التباعد في مسارات مختلفة مع مرور كل عام جديد. وكذلك الأمر بالنسبة لأمن المعلومات أحدث التقنيات الثورية، إلى جانب الأدوات السيبرانية الجديدة والتهديدات التي يتم الكشف عنها.

المصدر: J.G. NIKHITA REDDY, G UGANDER REDDY, 2022), **Cyber security challenges and its emaergning trends on latest technologies**

4.1. أوجه المقارنة بين الدراسة الحالية والدراسات السابقة

ستتم مقارنة وتحليل الدراسة الحالية مع الدراسات السابقة وتلخيص ما يميزها عن الدراسات السابقة كالآتي:

- **أوجه التشابه والاختلاف بين الدراسة الحالية والدراسات السابقة العربية المحلية والأجنبية**

الجدول رقم (10): أوجه التشابه والإختلاف بين دراسة (محمد ومورد 2023) والدراسة الحالية

أوجه التشابه بين دراسة محمد ومورد (2023) والدراسة الحالية	
الموضوع	تتناول كلتا الدراستين أثر الأمن السيبراني على أمن المعلومات في البنوك
المنهج	تعتمد كلتا الدراستين على المنهج الوصفي التحليلي.
النتائج	➢ ضرورة العمل على تطبيق مزيد من الأمان على عمليات التحويل المصرفية الالكترونية من خلال توفير تقنيات أمن الأنظمة لمواجهة التهديدات وسد الثغرات.
أدوات الدراسة	لا يوجد

أوجه الإختلاف بين دراسة (محمد ومواد 2023) والدراسة الحالية		
الدراسة	**دراسة (محمد ومواد 2023)**	**الدراسة الحالية**
نوع الدراسة	مقالة منشورة	مذكرة ماستر
مجتمع الدراسة	دراسة منظور لا يوجد.	موظفو البنك الخارجي الجزائري وكالة تبسة رقم 46
عينة الدراسة	دراسة منظور لا يوجد.	28 فردا من البنك الخارجي الجزائري وكالة تبسة
التركيز	الجرائم الالكترونية وأمن المعلومات المالية في القطاع المصرفي والمالي.	الأمن السيبراني له تأثير على أمن المعلومات.
النتائج	تسليط الضوء على معايير أمن وشفافية نظم المعلومات.	وعي موظفي البنك بأهمية الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لوكالة تبسة.

الجدول رقم (11): أوجه التشابه والإختلاف بين دراسة عبد اللطيف، بومدين وعبد القادر (2023) والدراسة الحالية.

أوجه التشابه بين دراسة (عبد اللطيف، بومدين وعبد القادر2023) والدراسة الحالية	
الموضوع	تتناول كلتا الدراستين أثر الامن السيبراني على الخدمات المصرفية.
المنهج	تعتمد كلتا الدراستين على المنهج الوصفي التحليلي.
النتائج	التعرف على واقع بنك التنمية المحلية لولاية غرداية الجزائر في مجال الجاهزية الإلكترونية لبيئته المادية والبشرية وأمنه السيبراني.
أدوات الدراسة	تستخدم كلتا الدراستين الإستبيان.

أوجه الاختلاف بين دراسة عبد اللطيف، بومدين وعبد القادر (2023) والدراسة الحالية		
الدراسة	دراسة (عبد اللطيف، بومدين وعبد القادر 2023)	الدراسة الحالية
نوع الدراسة	رسالة ماجستير	مذكرة ماستر

مجتمع الدراسة	عملاء بنك التنمية المحلية -غرداية-	موظفو البنك الخارجي الجزائري وكالة تبسة رقم 46
عينة الدراسة	127 عميل من بنك التنمية المحلية بولاية غرداية	28 فردا من البنك الخارجي الجزائري وكالة تبسة
التركيز	أثر جاهزية البيئة المادية والبشرية للأمن السيبراني على استخدام الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة.	الأمن السيبراني له تأثير على أمن المعلومات.
النتائج	الكشف عن مدى تأثير جاهزية البيئة المادية والبشرية للأمن السيبراني في التقليل من المخاطر المدركة والمتوقعة للعملاء.	وعي موظفي البنك بأهمية الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لوكالة تبسة.

الجدول رقم (12): أوجه التشابه والإختلاف بين دراسة أم الخير 2024 والدراسة الحالية

أوجه التشابه بين دراسة (أم الخير2024) والدراسة الحالية	
الموضوع	تتناول كلتا الدراستين موضوع الامن السيبراني.
المنهج	تعتمد كلتا الدراستين على المنهج الوصفي التحليلي.
النتائج	إعداد استراتيجيات لتحقيق الأمن السيبراني وجعله أولوية للحفاظ على أمن الأنظمة الرقمية.
أدوات الدراسة	لا يوجد

أوجه الإختلاف بين دراسة (أم الخير2024) والدراسة الحالية		
الدراسة	دراسة (أم الخير 2024)	الدراسة الحالية
نوع الدراسة	مقال	مذكرة ماستر
مجتمع الدراسة	دراسة منظور لا يوجد	موظفو البنك الخارجي الجزائري وكالة تبسة رقم 46
عينة الدراسة	دراسة منظور لا يوجد	28 فردا من البنك الخارجي الجزائري وكالة تبسة
التركيز	الهجمات السيبرانية وإستراتجيات الأمن	الأمن السيبراني له تأثير على أمن

	السيبراني.	المعلومات
النتائج	استحداث جملة من النصوص القانونية تتلازم مع طبيعة الهجمات.	وعي موظفي البنك بأهمية الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لوكالة تبسة.

أوجه التشابه والإختلاف بين الدراسة الحالية والدراسات السابقة العربية والأجنبية

الجدول رقم (13): أوجه التشابه والإختلاف بين دراسة (دراسة الشمالي، 2016) والدراسة الحالية

أوجه التشابه بين دراسة دراسة الشمالي، (2016) والدراسة الحالية	
الموضوع	تتناول كلتا الدراستين الأمن السيبراني
المنهج	تعتمد كلتا الدراستين على المنهج الوصفي التحليلي.
النتائج	وجود أثر ذو دلالة إحصائية الحماية المادية على أمن المعلومات في البنك.
أدوات الدراسة	تستخدم كلتا الدراستين الإستبيان

أوجه الإختلاف بين دراسة (دراسة الشمالي، 2016) والدراسة الحالية		
الدراسة	**(دراسة الشمالي، 2016)**	**الدراسة الحالية**
نوع الدراسة	مقالة منشورة	مذكرة ماستر
مجتمع الدراسة	26 بنكا، 13 بنكا تجاريا أردنيا، 03 مصارف إسلامية أردنية، 09 بنوك أجنبية	موظفو البنك الخارجي الجزائري وكالة تبسة رقم 46
عينة الدراسة	عينة من 135 فردا من عمال البنوك العاملة في الأردن.	28 فردا من البنك الخارجي الجزائري وكالة تبسة
التركيز	أثر أمن المعلومات وسريتها على الأداء المصرفي	الأمن السيبراني له تأثير على أمن المعلومات
النتائج	ضرورة قيام إدارة البنوك بالممارسات العملية اللازمة النظر أمن المعلومات وحريتها وتعميق ثقافتها في مختلف المستويات الإدارية عن طريق إعداد البرامج تدريبية لجميع المستويات الإدارية.	وعي موظفي البنك بأهمية الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لوكالة تبسة.

الجدول رقم (14): أوجه التشابه والإختلاف بين دراسة: منى (2016) والدراسة الحالية

أوجه التشابه بين دراسة منى (2016) والدراسة الحالية	
الموضوع	تتناول كلتا الدراستين الأمن السيبراني.
المنهج	تعتمد كلتا الدراستين على المنهج الوصفي التحليلي.
النتائج	الاعتماد المتزايد على البنى التحتية الخاصة بتقنيات المعلومات والاتصال من قبل الدول والأفراد والمؤسسات عامل محفز لتصاعد نسبة المخاطر على أمن المعلومات.
أدوات الدراسة	دراسة منظور لا يوجد.

أوجه الإختلاف بين دراسة منى (2016) والدراسة الحالية		
الدراسة	**(منى 2016)**	**الدراسة الحالية**
نوع الدراسة	كتاب	مذكرة ماستر
مجتمع الدراسة	دراسة منظور لا يوجد	موظفو البنك الخارجي الجزائري وكالة تبسة رقم 46
عينة الدراسة	دراسة منظور لا توجد عينة	28 فردا من البنك الخارجي الجزائري وكالة تبسة
التركيز	المسائل التي ترتبط بالأمن السيبراني البنى التحتية الخاصة بتقنيات المعلومات والاتصال	الأمن السيبراني له تأثير على أمن المعلومات
النتائج	الاعتماد المتزايد على البنى التحتية الخاصة بتقنيات المعلومات والاتصال من قبل الدول والأفراد والمؤسسات عامل محفز لتصاعد نسبة المخاطر على أمن المعلومات.	وعي موظفي البنك بأهمية الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لوكالة تبسة.

الجدول رقم (15): أوجه التشابه والإختلاف بين دراسة عبد اللطيف، بومدين وعبد القادر (2023) والدراسة الحالية.

أوجه التشابه بين دراسة دراسة فيصل (2019) والدراسة الحالية	
الموضوع	تتناول كلتا الدراستين الأمن السيبراني وأمن المعلومات.
النتائج	يوجد اتفاق معنوي وتجانس في الآراء بين مفردات عينة الدراسة بشأن تعدد المخاطر التي تتعرض لها نظم المعلومات.
أدوات الدراسة	تستخدم كلتا الدراستين الإستبيان.

أوجه الإختلاف بين دراسة فيصل (2019) والدراسة الحالية		
الدراسة	**دراسة فيصل (2019)**	**الدراسة الحالية**
نوع الدراسة	أطروحة دكتوراه	مذكرة ماستر
مجتمع الدراسة	المديرون الماليون والمحاسبون وموظفو إدارة تكنولوجيا المعلومات والمراجع الخارجي لشركات الاتصالات، وشركات تكنولوجيا المعلومات، والبنوك العاملة في المملكة العربية السعودية.	موظفو البنك الخارجي الجزائري وكالة تبسة رقم 46
عينة الدراسة	عينة من 300 موظفي شركات الاتصالات، شركات تكنولوجيا المعلومات والبنوك العاملة في المملكة العربية السعودية.	28 فردا من البنك الخارجي الجزائري وكالة تبسة
المنهج	الإستقرائي والإستنباطي	الوصفي التحليلي
التركيز	المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية.	الأمن السيبراني له تأثير على أمن المعلومات.
النتائج	يقوم عدد كبير من مفردات العينة بتطبيق المعايير الدولية لحوكمة أمن المعلومات بصورة منفردة، إلا أنها لا تعمل على تطبيق حوكمة أمن المعلومات ضمن استراتيجية الشركة للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية على الرغم من إدراك مفردات العينة لأهمية	وعي موظفي البنك بأهمية الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لوكالة تبسة.

	تطبيق حوكمة أمن المعلومات والفوائد المتحققة منها.	

الجدول رقم (16): أوجه التشابه والإختلاف بين دراسة: مروة (2021) والدراسة الحالية

أوجه التشابه بين دراسة (دراسة مروة2021) والدراسة الحالية	
الموضوع	تتناول كلتا الدراستين الأمن السيبراني في القطاع المصرفي
المنهج	تعتمد كلتا الدراستين على المنهج التحليلي.
النتائج	➢ معالجة اللوائح المتعلقة بالمخاطر التشغيلية والتقنية يساعد في توسيع نطاق الوصول إلى المعلومات؛ ➢ ادراج المخاطر السيبرانية ضمن المخاطر التشغيلية للمؤسسات المالية والمصرفية ومراجعتها بشكل مستمر.
أدوات الدراسة	دراسة منظور لا يوجد

أوجه الإختلاف بين دراسة (دراسة مروة2021) والدراسة الحالية		
الدراسة	**(مروة2021)**	**الدراسة الحالية**
نوع الدراسة	مقال	مذكرة ماستر
مجتمع الدراسة	دراسة منظور لا يوجد	موظفو البنك الخارجي الجزائري وكالة تبسة رقم 46
عينة الدراسة	دراسة منظور لا توجد عينة	28 فردا من البنك الخارجي الجزائري وكالة تبسة
التركيز	التحديات التي تواجه المجتمع من أجل تحقيق الأمن السيبراني، ومعرفة دور الدولة في التصدي لهذه الظاهرة والوقاية منها.	الأمن السيبراني له تأثير على أمن المعلومات
النتائج	معالجة اللوائح المتعلقة بالمخاطر التشغيلية والتقنية يساعد في تحقيق عدد من أهداف التنمية المستدامة.	وعي موظفي البنك بأهمية الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لوكالة تبسة.

الجدول رقم (17): أوجه التشابه والإختلاف بين دراسة Stady (Sushma Mishra, LewisChasalow,2011) والدراسة الحالية

أوجه التشابه بين دراسة Stady (Sushma Mishra, Lewis Chasalow,2011) والدراسة الحالية	
الموضوع	➢ كلتا الدراستين تتناولان دور موضوعي أمن المعلومات؛ ➢ تركز الدراستان على تحليل أدوات الحفاظ على أمن وسلامة البيانات والمعلومات.
المنهج	➢ تعتمد كلتا الدراستين على المنهج الوصفي التحليلي.
أدوات الدراسة	➢ استخدمت كلتا الدراستين على الاستبيان للوصول الى نتائج الدراسة.
النتائج	➢ توصلت كلتا الدراستين إلى تظهر النتائج أن مجال أمن المعلومات وتدقيق الأنظمة يعزز من فعالية أمن المعلومات.

أوجه الاختلاف بين دراسة (Sushma Mishra, Lewis Chasalow,2011) والدراسة الحالية		
الدراسة	**Stady (Sushma Mishra, Lewis Chasalow,2011)**	**الدراسة الحالية**
نوع الدراسة	مقال علمي	مذكرة ماستر
مجتمع الدراسة	موظفي نظم المعلومات	موظفو البنك الخارجي الجزائري وكالة تبسة رقم 46
عينة الدراسة	120 موظف	28 فردا من البنك الخارجي الجزائري وكالة تبسة
التركيز	الردع والتدقيق الأمني والفعالية الأمنية.	الأمن السيبراني له تأثير على أمن المعلومات.
النتائج	تشير النتائج الى وجود علاقة ذات دلالة إحصائية بين تدقيق الأنظمة وفعالية أمن المعلومات.	وعي موظفي البنك بأهمية الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لوكالة تبسة.

الجدول رقم (18): أوجه التشابه والاختلاف بين دراسة Stady (G. NIKHITA REDDY, GJUGANDER REDDY, 2022) والدراسة الحالية

أوجه التشابه بين دراسة Stady (GJ. NIKHITA REDDY, GJ UGANDER REDDY, 2022) **والدراسة الحالية**	
الموضوع	➢ كلتا الدراستين تتناولان دور موضوعي الأمن السيبراني؛ ➢ تركز الدراستان على تحليل أدوات الحفاظ على أمن وسلامة البيانات والمعلومات.
المنهج	➢ تعتمد كلتا الدراستين على المنهج الوصفي التحليلي.
النتائج	➢ توصلت كلتا الدراستين إلى أهمية الأمن السيبراني في الحفاظ على أمن المعلومات.

أوجه الاختلاف بين دراسة Stady (G. NIKHITA REDDY, G.J. UGANDER REDDY, 2022) **والدراسة الحالية**		
الدراسة	Stady (G. NIKHITA REDDY, G.J. UGANDER REDDY, 2022)	**الدراسة الحالية**
نوع الدراسة	مذكرة ماجستير	مذكرة ماستر
مجتمع الدراسة	لا يوجد	موظفو البنك الخارجي الجزائري وكالة تبسة وكالة رقم 46
عينة الدراسة	لا يوجد	28 فردا من البنك الخارجي الجزائري وكالة تبسة
التركيز	الجرائم السيبرانية والتهديدات الناجمة عنها.	الأمن السيبراني له تأثير على أمن المعلومات.
النتائج	أهمية البنية التحتية للبيانات والتكنولوجيا والدعم والقدرات الإدارية والموارد البشرية.	الأمن السيبراني له تأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك.

أظهرت مراجعة الدراسات السابقة إهتماما متزايدا بدور الأمن السيبراني في حماية أمن المعلومات، حيث أكدت الدراسات على فوائده في توفير الأمن للمعلومات والبيانات المالية في البنوك، وكذا مواجهته لمختلف التحديات المتمثلة أساسا في الهجمات السيبرانية.

2. مدخل مفاهيمي للأمن السيبراني

أدى التطور التكنولوجي وما رافقه من ثورة في الإعلام والمعلومات والاتصالات إلى ظهور مفاهيم حديثة ومن أهمها مفهوم الأمن السيبراني، الأمر الذي جعل من موضوعه أهمية كبيرة كونه يعد سلاحا استراتيجيا تسعى خلفه الحكومات والدول لحمايتها من أية اختراق وهذا استجابة لإدراكهم لحجم التهديدات والتحديات الناتجة عن مخاطر الأمن السيبراني والتي تطال الدولة ومؤسساتها وأفرادها ككل، ولرسم خارطة الطريق نحو تعزيز أمن الفضاء السيبراني بكافة أشكاله.

1.2. تعريف الأمن السيبراني

بما أن الأمن السيبراني هو ركيزة أساسية لمجتمع المعلومات وركيزة مهمة لأنشطة الحكومات والأفراد، يتناول القسم التالي تعريف الأمن السيبراني:

- **الأمن السيبراني** يعرف من خلال الاتحاد الدولي للاتصالات على أنه مجموعة الأدوات، والمفاهيم الأمنية، والضمانات الأمنية، والمبادئ التوجيهية، والمقاربات لإدارة المخاطر، والتدريبات، والممارسات، والتقنيات، وسبل الضمان والتكنولوجيات التي يمكن استخدامها لحماية البيئة السيبرانية والمؤسسات والمستخدمين.[1]
- **الأمن السيبراني** يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، من خلال مجموعة من الوسائل المستخدمة تقنيا وتنظيميا وإداريا في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال إتباع التدابير والإجراءات اللازمة لحماية البيانات.[2]
- **الأمن السيبراني** هو أمن الشبكات وأنظمة المعلومات والبيانات والأجهزة المتصلة بالأنترنت ويشير إلى الإجراءات والتدابير ومعايير الحماية التي يجب اتخاذها أو الالتزام بها من أجل التصدي للتهديدات أو منع الانتهاكات أو الحد من آثارها بكل الطرق ويرتبط ارتباطا وثيقا بأمن المعلومات، لأنه في معظم الحالات يكون الوصول إلى المعلومات وبنائها والتحقق منها وتداولها فضلا عن تزويرها واستغلالها أساسا لهجمات المعلومات على شبكة الانترنت.[3]

---

[1] 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)، ص1.

[2] منى عبد الله السمحان، **متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**، مجلة كلية التربية-جامعة المنصورة، العدد 111، يوليو 2020، ص 9.

[3] منى الأشقر جبور، **السيبرانية: هاجس العصر**، دراسات وأبحاث (1)، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، بيروت، 2016، ص 25.

ومن خلال ما تطرقنا في التعريفات السابقة يجدر بنا القول أن **الأمن السيبراني** هو مجموعة من الإجراءات والتقنيات التي تهدف لحماية المعلومات من الهجمات والتهديدات الأمنية، ويشمل ذلك حماية الشبكات والأجهزة والبرمجيات من الهجمات التقنية المحتملة والمعروفة باسم الهجمات السيبرانية، والتي عادة ما تنطوي على محاولات التطفل أو الاختراق أو التلاعب الغير المصرح به، وتعتمد استراتيجيات الأمن السيبراني على توفير طبقات من الحماية بدءا من الحماية الوقائية مرورا باكتشاف الهجمات والتدابير المضادة لها وصولا إلى استعادة النظام إلى حالته الطبيعية.

2.2. مكونات الأمن السيبراني

للأمن السيبراني مكونات يقوم عليها تتجسد في الآتي:[1]

- **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.
- **الحماية من الاختراق**: تعد القرصنة من أكثر التهديدات التي تواجهها الأنظمة الإلكترونية شيوعا، ويمكن أن تتسبب في سرقة الملفات والحسابات الشخصية، فضلا عن تلف البرامج وأجهزة الشبكة. وللحماية من الاختراق، يجب تحديث كلمات المرور وتفعيل ميزات الأمان والمصادقة 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 والأنظمة المستخدمة. ونظرا 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 والاحتيال والاستجابة لها في الوقت المناسب.

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

- **التوعية والتدريب**: تثقيف وتدريب المستخدمين وتدريبهم على مخاطر الأمن السيبراني وأفضل الممارسات لمنع التهديدات السيبرانية هو جزء مهم من استراتيجية أمنية شاملة.
- **إدارة التهديدات والاستجابة للحوادث**: ويشمل ذلك الاستعداد للاستجابة للحوادث الأمنية المحتملة ووضع إجراءات للتحقيق في الحوادث الأمنية والاستجابة لها بفعالية وسرعة.

3.2. أهمية الأمن السيبراني

في عالم اليوم المترابط بواسطة الشبكات يستفيد الجميع من برامج الأمن السيبراني لدوره الحيوي في حماية الأفراد والمنظمات والمجتمعات من التهديدات المتزايدة التي تشكلها الجرائم السيبرانية والتجسس السيبراني، وتتمثل أهمية الأمن السيبراني فيما يلي:

- تنفيذ تدابير الأمن السيبراني المناسبة للحفاظ على أمن وسرية المعلومات ضد الهجمات السيبرانية، بهدف بناء الثقة في البنية التحتية للمعلومات والاتصالات في جميع القطاعات، وخاصة البنوك والمؤسسات المالية مع العمل على حمايتها من مخاطر القرصنة لتحقيق بيئة رقمية آمنة بالتنسيق واتباع الأساليب الحديثة لتقييم المخاطر الأمنية والتأكد من فعالية وكفاءة البرامج المستخدمة لضمان أمن الشبكات.[1]
- يؤكد الأمن السيبراني في القطاع المصرفي على إنشاء درع وقائي واتخاذ تدابير وقائية مثل التوقيعات الرقمية أو المجاميع الاختبارية، للحفاظ على البيانات والمعلومات الشخصية والمالية للعملاء والمؤسسات المالية ومنع التعديلات أو التلاعبات غير المصرح بها، فتعزيز الأمن السيبراني في البنوك يضمن تقديم الخدمات بأمان وسلامة وتأمين العمليات المصرفية والمعاملات المالية ويساعد في الحفاظ على سمعة المؤسسات المالية وضمان استقرار الأسواق المالية وحماية البيانات الحساسة من الاختراق الأمني.
- 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 تتوقف الأنشطة.[2]
- يستخدم تكنولوجيا متقدمة تعمل على تحليل التعليمات البرمجية وبنية الموقع للكشف عن الثغرات الأمنية والأداء والمشكلات التشغيلية التي تسهل عملية الهجوم، ويوفر حلولا محددة لإحباط الهجمات وحماية الموقع بفعالية من البرمجيات الخبيثة والقرصنة والاختراقات المستمرة.

---

[1] خالد ظاهر عبد الله جابر السهيل المطيري، **دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي**، مجلة البحوث الفقهية والقانونية، العدد الثامن والثلاثون، الكويت، جوان 2022، ص 1003.

[2] منى عبد الله السمحان، **مرجع سابق**، ص 12.

- 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.[1]
- 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.[2]
- اتخاذ كافة التدابير اللازمة من خلال الإلمام بأحدث التقنيات والتكتيكات ذات الصلة بأمن المعلومات، لحماية المستخدمين من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة، وتدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية لنهب معلوماتهم الشخصية.[3]

3. أساسيات حول أمن المعلومات في البنوك

يعتبر قطاع البنوك من أكثر القطاعات تعرضا للهجمات السيبرانية نظرا للطبيعة الحساسة للبيانات والمعاملات المالية. تتطلب عمليات البنوك اليومية التي تتم عبر الإنترنت والتكنولوجيا الحديثة حماية مستمرة وفعالة للمعلومات ضد مخاطر القرصنة الإلكترونية والاختراقات. وعليه تسعى البنوك لوضع إطار عمل شامل يهدف إلى حماية البيانات المالية والشخصية للعملاء والمؤسسات وضمان استمرارية الخدمات المصرفية وامتثالها للتشريعات والمعايير الأمنية الدولية.

1.3. تعريف أمن المعلومات في البنوك

يشكل موضوع أمن المعلومات المتداولة عبر الإنترنت قلقا متزايدا بين المستخدمين، حيث تتطور الوسائل التقنية ووسائل التخزين وتبادل المعلومات، مما يطور الأساليب الخبيثة المستخدمة لسرقة المعلومات أو التلاعب بها. وبالتالي، أصبح وجود قسم لأمن المعلومات والمعلوماتية في المؤسسات أمرا ضروريا لحماية بيانات المؤسسة خاصة في القطاع المالي، فأمن المعلومات في القطاع المصرفي يكتسي أهمية استثنائية.

---

[1] https://www.kutub.info/library/book/21854، تاريخ الاطلاع: 2024/03/16، توقيت الاطلاع: 23:35.

[2] مروة فتحي السيد البغدادي، **اقتصاديات الأمن السيبراني في القطاع المصرفي**، مجلة البحوث القانونية والاقتصادية، العدد السادس والسبعون، جوان 2021، ص 4.

[3] كلية العلوم الانسانية والاجتماعية والعلوم الانسانية وآخرون، **الجزائر والتهديدات السيبرانية: نحو مستقبل آمن سيبرانيا**، الملتقى الدولي الأول العابر للتخصصات، جامعة أحمد دراية، أدرار، 11-12 ماي 2022، ص ص 3-4.

- **أمن المعلومات** إن حماية أجهزة الحاسوب وكذلك البيانات والمعلومات من الأخطار المختلفة هي التعريف الأساسي لأمن المعلومات، يشمل ذلك مجموعة من الإجراءات والتدابير الوقائية التي تستخدمها البنوك والمؤسسات المالية لضمان أمن وسرية بياناتها، وتهدف هذه التدابير إلى حمايتها ضد التهديدات الداخلية والخارجية، بما في ذلك السرقة، التلاعب، الاختراق والتدمير، حيث تعتبر البيانات التي تحتفظ بها البنوك ذات أهمية قصوى لأنها تمثل أموالا رقمية وحقوق مالية يتحتم على البنوك وضع استراتيجية شاملة لأمن المعلومات تغطي أنظمتها وبنيتها التحتية الافتراضية وآليات الحماية الداخلية لمنع سوء الاستخدام من قبل الموظفين والوصول غير المصرح به إلى أنظمة التحكم والمعالجة لتمتد هذه الإستراتيجية أيضا لتشمل العملاء، حيث تعمل على تعزيز الوعي والتعامل المسؤول مع المعلومات للتأكيد على أهميتها والحاجة إلى الحماية، وتتمحور استراتيجية حماية البيانات المصرفية حول تعزيز النظام الداخلي من خلال معالجة أي نقاط ضعف في المعلومات.[1]
- **أمن المعلومات** هو حماية المعلومات من الاختراق والوصول غير المصرح به وإساءة الاستخدام والتجسس ووصول الدخلاء إلى البيانات، إتلافها، تدميرها أو تغييرها، ويشمل المصطلح الأدوات والأساليب والإجراءات المطلوبة لتحقيق الحماية اللازمة لحماية المعلومات من المخاطر التي قد تواجهها من مصادر داخلية وخارجية.[2]
- **أمن المعلومات** هو توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها عن طريق توفير الأدوات والوسائل اللازمة لحماية أمن المعلومات من المخاطر الداخلية أو الخارجية من خلال معايير وإجراءات لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين، خاصة المتعلقة بالبنوك والمؤسسات المالية وتقليل المخاطر التي قد تؤثر على توافر المعلومات وسريتها وسلامتها إلى مستوى مقبول ومحدد بشكل جيد، يتضمن برنامج أمن المعلومات الجيد عنصرين أساسيين: تحديد المخاطر وإدارة المخاطر.[3]
- **أمن المعلومات المصرفية** هو استخدام إجراءات وتدابير مختلفة لضمان الحماية اللازمة لجميع البرامج والأنظمة المستخدمة لمعالجة المعلومات وضمان سلامتها يعد من الموارد والمزايا الرئيسية التي يجب على البنوك والمؤسسات المالية الحفاظ عليها، فهو الوسيلة الأساسية لضمان سلامة المعلومات التي تتعامل معها، حيث يقوم بتأمين تلك المعلومات من خلال اتخاذ إجراءات تقنية وإدارية تضمن

---

[1] دلندة دوادي-زهرة بن حود، **أمن المعلومات المصرفية**، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماجستير، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، ورقلة، ص17.

[2] بوازدية جمال، **مرجع سابق** ، ص 27.

[3] شايب محمد-حمادي موراد، **تحديات الأمن السيبراني لأنظمة المعلومات في البنوك والمؤسسات المالية**، مجلة إنارة للدراسات الإقتصادية، الإدارية والمحاسبية، المجلد الرابع، العدد الأول، جوان 2023، ص 66.

سلامتها وتوافرها وسريتها، بالتالي يعتبر هذا النهج الشامل للأمن المعلوماتي أساسيا لضمان استمرارية الأعمال وسلامة المعلومات في البنوك والمؤسسات المالية، ويعتبر جزءا لا يتجزأ من استراتيجية الأمن الشاملة لهذه الجهات.[1]

ومن خلال ما تطرقنا في التعريفات السابقة يجدر بنا القول أن **أمن المعلومات في البنوك** يشير إلى الجهود والتدابير التي تتخذها المؤسسات المالية لحماية المعلومات الشخصية والبيانات المالية للعملاء والمؤسسات من التهديدات الإلكترونية والاختراقات، حيث يهدف إلى ضمان سلامة المعلومات وسرية البيانات وسلامة العمليات المصرفية، تتضمن تدابير أمن المعلومات في البنوك الحماية من الاختراقات الإلكترونية، وتشفير البيانات، وإنشاء سياسات وإجراءات لإدارة المخاطر، وتوفير تدريب للموظفين، وتنفيذ أنظمة مراقبة واختبارات أمنية دورية.

2.3. العناصر الأساسية لأمن المعلومات

يتعين على النظام الأمني الفعال أن يشمل جميع الجوانب ذات الصلة بنظام المعلومات، ويمكن تحديد هذه الجوانب عبر:

- **استمرارية توفر المعلومات**: يتعرض توافر المعلومات أو البيانات للخطر عندما لا يعمل النظام بشكل منتظم، من حيث قدرته على وصول المستخدمين إلى المعلومات أو الموارد، مما يؤثر على عليهم وكذلك على الوظائف، فاستمرار عمل نظم المعلومات، وعدم انقطاع استخدام المعلومات أو الوصول إليها من قبل مستخدمي دون تأخير، وهذا يعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته بما في ذلك جميع التدابير اللازمة لضمان استمرار البنك في تقديم الخدمات والتفاعل مع المعلومات والوصول إليها وعدم تعرض المستخدمين لخطر التلاعب أو التخريب من خلال استخدام تدابير الحماية المناسبة، بما في ذلك البرمجيات والمعدات ضد التطفل والهجوم.
- **سلامة المحتوى واكتماله**: أي أنه يجب التأكد من أن المحتوى لم يتم العبث به، وعدم إتلاف أي جزء من أجزائه (سواء تم إتلافه كليا أو جزئيا)، حيث يضمن نظام الأمن دقة محتوى المعلومات في أي مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة المعالجة الداخلية للمعلومات أو من خلال التدخل غير المشروع، من خلال ضمان عدم تعديلها، تغييرها، إتلافها أو التلاعب بها في أي مرحلة من مراحل المعاجلة، وضمان عدم حذف أي جزء من البيانات المنقولة،[2] وهذا يعني أن

[1] Bojidar Bojinov, **Banking security- Major manifestations and aspects**, Academy of Economics-svishtov, department of finance and credit, Narodnostopanski arhiv 3/2016, p 4.

[2] دلندة داودي-زهرة بن حود، **مرجع سابق** ، ص ص 18-20.

الحفاظ على سلامة المعلومات من التخريب والتزوير أمر بالغ الأهمية، خاصة في ظل الخسائر المالية الضخمة في البنوك والمؤسسات المالية.

- **سرية المعلومات وموثوقيتها:** ويشمل ذلك جميع التدابير اللازمة لضمان عدم إفشاء المعلومات أو الوصول إليها من قبل أي شخص غير الأشخاص المصرح لهم بذلك إلى المعلومات الحساسة أو السرية. ولتحقيق ذلك، يجب على المؤسسات البنكية والمالية استخدام أساليب الحماية المناسبة باستخدام مجموعة متنوعة من الوسائل، مثل تشفير الرسائل ومنع التعرف على تلك المعلومات أو مسار إرسالها.[1]

3.3. أهمية أمن المعلومات في البنوك

أمن المعلومات في البنوك أمر حيوي يتطلب الاهتمام الكبير حيث يتعامل هذا القطاع مع معلومات حساسة وشخصية للعملاء، لذا تعتبر الاستراتيجيات الشاملة لحماية هذه المعلومات وضمان سلامتها جزءا لا يتجزأ من نجاح البنوك، حيث تكمن أهميتها في:

- **حماية البيانات الحساسة:** تتعامل البنوك مع كميات هائلة من البيانات الحساسة، مثل معلومات الحسابات المصرفية، والبيانات الشخصية للعملاء، يساهم أمن المعلومات في الحفاظ على سرية وسلامة بيانات العملاء والمعلومات المالية الحساسة ومعاملات الدفع فأمن المعلومات يحمي البيانات وسريتها حيث يعمل النظام على تقديم العديد من السياسات والإجراءات والضوابط المختلفة التي تساعد البنوك على حماية هذه البيانات من السرقة، مما يقلل من فرص الوصول غير المصرح به والاستخدام غير القانوني لهذه البيانات، وزيادة القدرة على مواجهة جميع الهجمات السيبرانية.
- **ضمان استمرارية الخدمات المصرفية:** يساعد أمن المعلومات في تأمين استمرارية تقديم الخدمات المصرفية دون تعرض لانقطاعات ناتجة عن هجمات سيبرانية أو انتهاكات أمنية.
- **منع الاحتيال المالي:** يلعب أمن المعلومات دورا حيويا في تقليل فرص الاحتيال المالي والاحتيال الإلكتروني الذي يمكن أن يتسبب في خسائر مالية كبيرة للعملاء والمؤسسات المالية.[2]
- **الامتثال للتشريعات واللوائح:** يساعد أمن المعلومات في ضمان الامتثال للتشريعات واللوائح الخاصة بحماية البيانات والمعلومات المالية، مما يساهم في تشغيل المؤسسات المالية بشكل قانوني وآمن.

---

[1] آن سعيد ابراهيم عبد الواحد، **سياسات أمن المعلومات وعلاقتها بفاعلية نظم المعلومات الإدارية في الجامعات الفلسطينية، قطاع غزة**، قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال، كلية الإقتصاد والعلوم الإدارية، جامعة الأزهر، غزة، 2015، ص 16.

[2] حسين علي قاسم الشمالي، **أمن وسرية المعلومات و أثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن**، مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والاقتصادية، المجلد الثاني، العدد السابع، جوان 2017، ص 192.

- **بناء الثقة والسمعة**: أمن المعلومات المصرفية يعد عنصرا حيويا لضمان سلامة العمليات المالية وحماية البيانات الحساسة، لأنه يعزز ثقة العملاء والمستثمرين في البنوك والمؤسسات المالية، مما يساهم في بناء سمعة إيجابية وتعزيز العلاقات مع العملاء ويتطلب تنفيذ إجراءات أمنية قوية واستخدام تقنيات متقدمة لمواجهة التهديدات السيبرانية المتزايد، لحماية هذه البيانات من السرقة أو الوصول غير المصرح به، مما قد يؤدي إلى عواقب وخيمة مثل الاحتيال، وسرقة الهوية، وخسارة الأموال يساعد ذلك على منع الاحتيال، وحماية أموال العملاء، وتعزيز ثقتهم في البنك.
- **حماية البنية التحتية لتكنولوجيا المعلومات**: تعتمد البنوك على أنظمة تكنولوجيا المعلومات لتقديم خدماتها للعملاء، ويعد أمن المعلومات ضروريا لحماية هذه الأنظمة من الهجمات السيبرانية والأعطال مما قد يؤدي إلى انقطاع الخدمات وخسارة الأموال، يساعد ذلك على ضمان استمرارية عمل البنك حتى في حالات الأزمات.[1]
- **تعزيز ثقافة أمن المعلومات**: يعد نشر ثقافة أمن المعلومات بين جميع موظفي البنك ضروريا لضمان التزامهم بحماية البيانات والأنظمة، ويساعد ذلك على زيادة الوعي بالمخاطر السيبرانية، تحسين سلوكيات الموظفين وتعزيز أمن المعلومات بشكل عام.
- **تحسين قدرة التنبؤ بالمخاطر**: يحسن أمن المعلومات قدرة البنك على التنبؤ بالمخاطر السيبرانية والوقاية منها لتقليل احتمالية وقوع الهجمات، خسارة الأموال وزيادة القدرة على مواجهة جميع الهجمات السيبرانية.
- **تحسين سمعة البنك**: للبنك تجنب حوادث الانتهاكات الأمنية والتسريبات التي قد تؤثر سلبا على سمعته ومصداقيته، من خلال تطبيق إجراءات أمنية صارمة، يمكن للبنك الامتثال للتشريعات واللوائح الخاصة بحماية البيانات، مما يساهم في تعزيز سمعته ككيان مالي موثوق عندما يكون البنك معروفا بسياساته القوية في مجال أمن المعلومات، يمكنه بناء علاقات قوية مع العملاء والشركاء التجاريين، فيزيد ذلك من ثقة العملاء والمستثمرين في البنك ويعزز سمعته.
- **مواكبة التطورات التكنولوجية**: تعد مواكبة التطورات التكنولوجية في مجال أمن المعلومات أمرا حتميا لضمان استمرارية حماية البيانات والأنظمة من المخاطر الجديدة بشكل عام، فأمن المعلومات يعد ضروريا لضمان سلامة ونجاح البنوك في بيئة رقمية متغيرة.[2]

---

[1] Bank of Japan, **The importance of information security for financial institutions and proposed countermeasures**, with a focus on internet-based financial services, 2000, p p 16-17.

[2] زيدان محمد-حمو محمد، **أمن المعلومات المصرفية كمطلب لتبني التسويق الالكتروني في البنوك الجزائرية**، مجلة رؤى اقتصادية، جامعة حسيبة بن بوعلي، الشلف، جوان 2015، ص 172.

4.3. علاقة الأمن السيبراني بأمن المعلومات في البنوك

من خلال ما تم طرحه سابقا تتجلى لنا العلاقة الوطيدة بين الأمن السيبراني وأمن المعلومات في البنوك.[1]

تعكس العلاقة بين أمن المعلومات والمعلومات المصرفية تبادلا مستمرا بين متخصصي الأمن السيبراني ومتخصصي أمن المعلومات، فعلى الرغم من أن الأمن السيبراني يركز على حماية البنية التحتية التقنية والتطبيقات من التهديدات الإلكترونية، إلا أن أمن المعلومات يتعامل مع وسائل تخزين ومعالجة المعلومات بشكل عام بما في ذلك البيانات المصرفية.

متخصصو الأمن السيبراني يعملون على حماية البنية التحتية للبنوك والمؤسسات المالية، مثل الخوادم والشبكات ونقاط النهاية، لمنع الاختراقات والاستيلاء غير المصرح به على المعلومات المصرفية، ويقومون بتحليل التهديدات والثغرات المحتملة واتخاذ التدابير الوقائية لحماية هذه الأصول الرقمية الحساسة.

من جانبهم، متخصصو أمن المعلومات في المؤسسات المالية يعملون على حماية البيانات المصرفية وضمان سلامتها وامتثالها للتشريعات واللوائح المتعلقة بالخصوصية والأمان، ويتناولون قضايا مثل إدارة الوصول والتشفير والمراقبة الداخلية لضمان أن البيانات المصرفية تظل آمنة وخاصة.

يشكل الأمن السيبراني وأمن المعلومات علاقة متكاملة، فكل منهما يعمل بدوره كجزء لا يتجزأ من استراتيجية الأمان للمؤسسات المالية، من خلال التكامل بين جهودهما لتعزيز القدرة على حماية المعلومات المصرفية وضمان سلامتها، ويشكلان جزءا أساسيا من جهود المؤسسات المالية لمواجهة التحديات الأمنية المتزايدة وتبادل المعلومات حول التهديدات السيبرانية الحالية.

4. الإطار النظري للهجمات السيبرانية

بالتزامن مع التطور الكبير في تكنولوجيا المعلومات والاتصالات وزيادة الاعتماد عليها، تجلى ما يسمى بالهجمات السيبرانية في شكل تهديدات عالمية يتعرض لها الأمن السيبراني وحماية البيانات والخصوصية، وهي تحديات سيبرانية شكلت تهديدا خطيرا لأمن ومرونة البنى التحتية والأنظمة المتصلة بشبكاتها ويمكن أن تؤدي إلى تآكل ثقة الجمهور في البيئة الرقمية حيث تغيرت مفاهيم القوة والصراع والحرب وارتبطت طبيعتها بالفضاء السيبراني، ولهذا السبب يتطلب التصدي لها باتباع نهج شامل ومنسق وتعاوني ويتعين على أصحاب المصلحة تبادل المعرفة، وبناء القدرات والخبرات وتقييم المخاطر على المستويين الإقليمي والعالمي.

[1] https://www.simplilearn.com/information-security-vs-cyber-security-article#، تاريخ الإطلاع: 2024/05/21، توقيت الإطلاع: 14:21.

1.4. تعريف الهجمات السيبرانية

تستهدف العديد من تعاريف الهجمات السيبرانية النموذج القانوني لأركان جرائم تقنية المعلومات التقليدية، وفي أغلب الأحوال جرائم الإرهاب السيبراني أو الحروب السيبرانية، إلا أن الهجوم السيبراني يعد القاسم المشترك الذي يجمع بين كل هذه الجرائم التي يمكن أن ترتكب على مرافق البنى التحتية للمدن الذكية داخل دائرة الفضاء الإلكتروني.

- **الهجمات السيبرانية** هي تقنية متطورة تعكس التطورات الحاصلة في مجال برمجيات الحاسوب، وهي عملية استغلال نقاط الضعف لاختراق البيانات في أنظمة المعلومات بهدف تدميرها، سرقتها أو التلاعب بها، ويعد قطاع المؤسسات البنكية والمالية مكونا مهما من مكونات النظام المالي، حيث يحتوي على كميات هائلة من المعلومات والبيانات الحساسة، وهو أكثر عرضة لخطر استغلال هذه التقنية التي يمكن أن تؤدي إلى تعطيل الخدمات التي يقدمها وتهديد الاستقرار المالي، حيث شهد هذا القطاع سلسلة من الهجمات السيبرانية الكبرى.[1]
- **الهجمات السيبرانية** هي مصطلح يشمل الاختراقات التي تمكن التسلل من غير المصرح لهم الولوج إلى المواقع الالكترونية بغرض تدميرها، يتضمن بشكل أساسي الإضعاف من قدرات ووظائف شبكات الحاسوب المستهدفة، من خلال جهاز حاسوب أو أكثر أو شبكات للوصول بشكل غير قانوني إلى أنظمة وشبكات البنوك والمؤسسات المالية، للحصول على بيانات سرية من خلال استغلال نقطة ضعف معينة تمكن المهاجمين من التلاعب بالنظام.[2]
- **الهجمات السيبرانية** هي نوع من المناورات الهجومية التي تحاول إلحاق الضرر بحاسوب أو نظام حاسوبي أو شبكة حاسوبية عن طريق الوصول غير المصرح به وتعريض الأنظمة الحساسة للخطر، أي محاولة لتعطيل أنظمة الحاسوب أو تدميرها أو السيطرة عليها، أو كشف أو تغيير أو حجب أو حذف أو التلاعب أو سرقة البيانات الموجودة في هذه الأنظمة، وهو أيضا محاولة لإساءة استخدام الأصول أو الاستغلال المتعمد للأنظمة أو الأجهزة أو الشبكات الضعيفة، وتهدف المحاولات إلى استغلال النظام أو الجهاز أو الشبكة بطريقة لا تتوافق مع القانون. قد تختلف الدوافع وراء الهجمات السيبرانية، ولكن أهم الأسباب التي تبرز هي المصالح المالية والمعلوماتية، وقد تستخدم الهجمات السيبرانية من قبل دول ذات سيادة أو أفراد أو جماعات أو جمعيات أو منظمات أو

---

[1] بوطلاعة وداد بوكورو منال، **الهجمات السيبرانية على البنية التحتية الحرجة دراسة في ضوء القانون الدولي العام**، مجلة حقوق الإنسان والحريات العامة، المجلد السابع، العدد الثاني، ديسمبر 2022، ص ص 325-326.

[2] أميرة عبد العظيم محمد عبد الجواد، **المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام**، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 2020، ص 394.

عصابات تسعى إلى تعطيل البنية التحتية لدول بأكملها، وقد تنشأ هذه الهجمات السيبرانية من مصادر مجهولة قد تكون جزءا من الحرب السيبرانية أو الإرهاب السيبراني.[1]

ومن خلال ما تطرقنا في التعريفات السابقة يجدر بنا القول أن **الهجمات السيبرانية** هي عملية تحدث في الفضاء الإلكتروني، حيث يصل المتسللون بشكل غير قانوني إلى البيانات الموجودة على جهاز كمبيوتر أو جهاز مستهدف بهدف سرقتها أو إساءة استخدامها، يستطيع الهاكرز سواء من دول أخرى أو أفراد ذوي خبرة عالية في تكنولوجيا المعلومات أو أجهزة الكمبيوتر الوصول إلى المواقع المحظورة في أي نوع من شبكات وأنظمة الكمبيوتر، وقد تشمل أنشطتهم المواقع الإلكترونية المهمة مثل المواقع المصرفية التسبب في الإضرار بسمعة بنك واستقراره المالي، حيث يقومون باختراقها قصد الحصول على البيانات المالية الحساسة للعملاء والمستخدمين، أو للتسبب في الإضرار بسمعة البنك واستقراره المالي، أو لجمع المال وقد تكون مثل هذه الهجمات الإلكترونية جزءا من شن حرب إلكترونية ضد مؤسسات دولة بأكملها.

2.4. خصائص الهجمات السيبرانية

تشكل الهجمات السيبرانية تهديدا خطيرا يستهدف الأنظمة الإلكترونية والبيانات الحساسة في العصر الرقمي الحالي، تتميز هذه الهجمات بخصائصها المتعددة التي تشمل:[2]

- الهجمات السيبرانية هي هجمات ذات تقنية عالية تعكس ذروة ثورة المعلومات، يمكن أن تحدث في أي وقت وفي فترة زمنية قصيرة .
- الهجمات السيبرانية لا تعرف حدودا جغرافية ووسائلها متنوعة ومتطورة، وتتعلق بأكثر المجالات التكنولوجية تطورا وتغيرا في الحياة الحديثة وأهدافها وعواقبها غير محدودة.
- يصعب تحديد موقع الهجمات السيبرانية شديدة التأثير وتحديدها لأنها لا تترك أي أثر أو دليل على حدوثها، ويرجع ذلك إلى أن معظم الهجمات السيبرانية يتم اكتشافها عن طريق الصدفة على مدى فترة طويلة من الزمن، وتتطلب مستوى عال من المهارة التقنية لاكتشاف مصدر الهجوم.
- للهجمات السيبرانية ميزة أخرى هي تدمير البيانات والمعلومات، ويصعب اكتشافها لأنها لا تترك أي أثر يمكن تتبعه بسهولة، بالإضافة إلى أن الضحية لا يكون على علم بها إلا بعد مرور بعض الوقت على حدوثها.

---

[1] عماد الدين محمد كامل عبد الحميد، **الهجمات السيبرانية على البنى التحتية للمدن الذكية: التحديات القانونية واستراتيجية المواجهة**، البحث العلمي والمجلة، كلية الإمام مالك للشريعة والقانون، دراسات علوم الشريعة والقانون، العدد الثالث، سبتمبر 2023، ص59.

[2] نور أمير موصلي، **الهجمات السيبرانية في ضوء القانون الدولي الانساني**، بحث مقدم استكمالا لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الانساني، الجامعة الافتراضية السورية، 2021، ص ص 10-11.

- سرعة وغياب الأدلة وصعوبة الإثبات، بالإضافة إلى توافر الوسائل التقنية التي تعيق الوصول إلى الأدلة والإثباتات.
- ارتفاع مستوى مهارة وخبرة الجناة في مجال الاتصالات.
- استخدام الحواسيب والتكنولوجيا الحديثة لتنفيذ الهجمات.
- تعرض الأجهزة الأمنية للهجمات نتيجة لنقص الخبرة التقنية اللازمة لكشف هذه الهجمات والبحث عنها.

3.4. أنواع الهجمات السيبرانية على البنوك

هناك أنواع مختلفة من الهجمات السيبرانية ذات مستويات مختلفة من المخاطر التي يمكن أن يساعد الأمن السيبراني في مكافحتها.

- **هجمات التصيد الاحتيالي:** هي ممارسة ارسال اتصالات تستهدف أفرادا أو منظمات معينة، مثل موظفي البنوك أو المؤسسات المالية، لخداع الضحايا عن طريق إرسال رسائل احتيالية عبر البريد الإلكتروني جماعية غير مستهدفة يتم إرسالها إلى العديد من الأشخاص تطلب معلومات حساسة مثل التفاصيل المصرفية أو تشجعهم على النقر فوق رابط أو زيارة موقع ويب مزيف باستخدام بياناتهم الشخصية، والتظاهر بأنها صادرة من مصدر موثوق. الهدف منها الوصول إلى أنظمة البنك أو سرقة بيانات حساسة (سرقة كلمات المرور، معلومات الحسابات المصرفية، أو بيانات بطاقات الائتمان)، تثبيت برامج ضارة على جهاز الضحية، للوقاية يجب التحقق من مصدر الرسائل قبل الرد، استخدام كلمات مرور قوية وفريدة من نوعها لكل حساب فتح أي مرفقات أو روابط من جهات غير معروفة.[1]
- **هجمات برامج الفدية:** هي برامج ضارة تقوم بالاستيلاء على الحاسوب من خلال الوصول إلى البيانات الموجودة على حاسوب الضحية، واستغلال نقاط الضعف أو الثغرات الموجودة في الجهاز لتشفيرها بمفتاح تشفير غير معروف للمستخدم وطلب فدية لفك تشفيرها. الهدف منها تعطيل أنظمة البنك وابتزاز الأموال، وللوقاية يجب تحديث أنظمة التشغيل والبرامج بشكل دائم، استخدام برامج مكافحة الفيروسات، عمل نسخ احتياطية من البيانات بشكل منتظم.[2]
- **هجمات الحرمان من الخدمة:** هي هجوم يستهدف البنوك التي توفر الخدمات المصرفية الالكترونية من خلال تعطيل صفحة الويب التابعة للبنك إرسال كمية كبيرة من البيانات إلى خادم البنك لإغراقه ومنعه من تقديم الخدمات للعملاء تشفيرها التي تؤثر سلبا على مراكز البيانات. الهدف منها تعطيل

---

[1] عبد الرحمان محمد سليمان رشوان، زينب عبد الحفيظ أحمد قاسم، **أثر إدارة مخاطر الامن السيبراني على دعم الاستقرار والشمول المالي في البنوك**، المؤتمر العلمي الدولي الأول بعنوان "أثر الأمن السيبراني على الأمن الوطني"، جامعة عمان العربية بالاشتراك مع مديرية الأمن العام، ديسمبر 2022، ص 10.

[2] أسامة حسام الدين، **أساسيات الامن السيبراني**، أكاديمية سيسكو بجامعة طيبة، سبتمبر 2017، ص 55.

خدمات البنك وإلحاق الضرر بسمعته، وللوقاية يجب استخدام أنظمة الحماية من هجمات حرمان الخدمة، مراقبة حركة البيانات بشكل دائم، تقييد الوصول إلى بعض الخدمات في حالات الطوارئ.

- **هجمات الهندسة الاجتماعية:** هي استخدام أساليب التلاعب النفسي لخداع موظفي البنك للكشف عن معلومات سرية أو تنفيذ عمليات غير مصرح بها. الهدف منها الوصول إلى أنظمة البنك أو سرقة بيانات حساسة، ويجب للوقاية تدريب موظفي البنك على كيفية التعرف على أساليب الهندسة الاجتماعية، تطبيق إجراءات أمنية صارمة للتحقق من هوية المستخدمين.
- **هجمات البرامج الضارة:** هي برامج ضارة تثبت على أجهزة الحاسوب أو الأجهزة المحمولة للوصول إلى البيانات أو التحكم في الأجهزة تعمل على تقليص أداء النظام حيث تقوم هذه البرامج بإغلاقه وتحتفظ بالبيانات المرهونة فإذا لم يقوم المستخدم بالدفع تقوم هذه البرامج بإيقاف تشغيل النظام والاحتفاظ بالبيانات المخترقة ولأنها مدمجة بعمق في الحاسوب، يستحيل على المستخدم العادي استعادة السيطرة على البيانات. الهدف منها سرقة المعلومات الشخصية أو المالية، تعطيل أنظمة البنك، أو نشر برامج ضارة أخرى، للوقاية منها يجب استخدام برامج مكافحة الفيروسات، تحديث أنظمة التشغيل والبرامج بشكل دائم، عدم تحميل البرامج من مصادر غير موثوقة.[1]
- **القنابل البرمجية:** تعرف القنابل البرمجية القنبلة المعلوماتية أيضا بالشفرة الموقوتة، وهي نوع من البرامج الخبيثة الصغيرة التي يتم إدخالها بشكل غير قانوني وإخفائها مع برامج أخرى، هذه البرامج ليست ملفات كاملة من الناحية الشكلية، بل هي شيفرات برمجية موضوعة في مجموعة من الملفات، مقسمة هنا وهناك بحيث لا يمكن التعرف عليها ولا يمكن اكتشافها لأشهر أو سنوات لأنها تتجمع معاً وفقاً لترتيب معين في وقت أو مكان معين أو عند وقوع حدث معين تستخدم هذه البرامج. تهدف الى تدمير المعلومات والبيانات أو لتعديل برامج ومعلومات النظام، وللوقاية منها يجب تشفير البيانات، النسخ احتياطي للبيانات، التحديث المستمر للنظام.[2]

4.4. أهداف الهجمات السيبرانية على البنوك

يمكن تقسيم أهداف الهجمات السيبرانية على البنوك إلى فئتين رئيسيتين:

- **الأهداف المالية**

  - **السرقة:** قد يكون الهدف الرئيسي لبعض الهجمات السيبرانية هو سرقة المعلومات الحساسة كسرقة البيانات الشخصية والمالية للعملاء مثل أرقام الحسابات المصرفية وكلمات المرور أو معلومات بطاقات الائتمان، وذلك باستخدام أساليب مختلفة مثل التصيد الاحتيالي وبرامج

[1] شايب محمد، حمادي مراد، **مرجع سابق** ، 2023، ص 62.

[2] نور أمير الموصلي، **مرجع سابق** ، ص ص 16-17.

الفدية والبرامج الضارة والهجمات الهندسية الاجتماعية لخداع العملاء أو موظفي البنك للكشف عن بياناتهم، مما يسبب الخسارة المالية للعملاء والضرر بسمعة البنك.

- **الابتزاز:** ابتزاز الأموال من البنوك أو المؤسسات المالية من خلال تعطيل أنظمتها أو من أجل سرقة بيانات حساسة منها مثل معلومات العملاء أو البيانات المالية أو خطط الأعمال، وذلك بعد الوصول الغير مصرح به إلى الحاسوب مستغلين نقاط ضعف أو ثغرات في النظام ثم تشفير البيانات باستخدام مفتاح تشفير غير معروف ثم المطالبة بفدية لفك تشفيرها أو تهديدهم بنشرها أو بيعها إذا لم يدفعوا الفدية، مما يسبب الخسارة المالية للبنك والضرر بسمعته.
- **التخريب:** يهدف بعض المهاجمين إلى تعطيل أنظمة البنوك والحاق الضرر بعملياتها سواء على مستوى المنظمات أو البنية التحتية، وذلك باستخدام هجمات الحرمان من الخدمة أو برامج الفدية أو البرامج الضارة، مما يؤدي إلى توقف المواقع الإلكترونية وتعطيل الخدمات الأساسية للبنوك أي انقطاع الخدمات للعملاء وبالتالي خسارة مالية للبنك والضرر بسمعته.

- **الأهداف غير المالية**

- **التجسس:** يستخدم بعض المهاجمين الهجمات السيبرانية للتجسس على المنافسين التجاريين أو الدول الأخرى للحصول على المعلومات السرية والحساسة المتعلقة بالابتكارات التقنية أو الاستراتيجيات التجارية، باستخدام أساليب مختلفة مثل الاختراق الإلكتروني والبرامج الضارة والهجمات الهندسية الاجتماعية، وبالتالي حصول المنافسين على ميزة غير عادلة وخسارة مالية للبنك.[1]
- **الإضرار بالسمعة:** قد يعجز البنك عن حماية المعلومات الشخصية أو السرية للعملاء، وذلك من خلال شن هجمات سيبرانية واسعة النطاق على مستواه تظهر ضعف أنظمته الأمنية ونشر أخبار عن الهجمات على وسائل التواصل الاجتماعي، مما يسبب آثار طويلة الأمد على سمعة البنك وفقدان ثقة العملاء.[2]
- **زعزعة الاستقرار المالي:** زعزعة استقرار النظام المالي من خلال شن هجمات سيبرانية واسعة النطاق على البنوك في دولة معينة، مما قد يؤدي إلى انخفاض قيمة العملة، وفقدان ثقة العملاء في النظام المالي وخسارة مالية كبيرة للبنوك وأضرار اقتصادية واسعة النطاق.[3]

[1] https://www.rmg-sa.com/ ، تاريخ الاطلاع: 2024/03/29، توقيت الاطلاع: 14:55.

[2] https://fastercapital.com/arabpreneur/ ، تاريخ الاطلاع: 2024/03/29، توقيت الاطلاع: 15:52.

[3] https://www.rmg-sa.com/ ، تاريخ الاطلاع: 2024/03/29، توقيت الاطلاع: 14:55.

خلاصة الجزء الأول:

إستهدفنا من خلال هذه الجزء ضبط مفاهيم الأمن السيبراني وكذا المعرفة التقنية، وما ينجم عنها من مخاطر تستهدف بالدرجة الاولى برامج الحماية الموكل لها الحفاظ على النظام المعلوماتي البنكي، وتحديد مدى مسؤولية مديري نظم الحماية عن وضع استراتيجية امنية محترفة مراعية للمعايير العالمية لأمن المعلومات، ونظرا لأهمية الموضوع تم دراسته في العديد من المناسبات العلمية والتقنية سابقا لإثبات مدى حساسية حماية الأنظمة البنكية من أي اختراق.

الجزء الثاني:

واقع تأثير الأمن السيبراني على أمن المعلومات في البنوك

تمهيد:

للتعرف أكثر على واقع الأمن السيبراني وأمن المعلومات داخل المؤسسة والعلاقة بينهما في المؤسسة، سنقوم في هذا الفصل بعرض الدراسة الميدانية للأمن السيبراني وانعكاساته على أمن المعلومات في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة، وهذا لتدعيم المفاهيم النظرية المدروسة في الجانب النظري، وذلك من خلال التعرف على المؤسسة وأهم مهامها وأهدافها وتحليل هيكلها التنظيمي، ثم تحديد الإطار المنهجي الذي تمت فيه الدراسة الميدانية وفي الأخير يتم عرض وتحليل بيانات الدراسة الميدانية بالاعتماد على برنامج spss وإختبار الفرضيات وتحقيق أهداف الدراسة.

من أجل تحقيق أهداف الدراسة الميدانية فقد تم تقسيم الجزء الثاني إلى الأقسام التالية:

1. **تقديم عام لمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة.**
2. **الإطار المنهجي للدراسة الميدانية.**
3. **عرض وتحليل نتائج الدراسة الميدانية.**

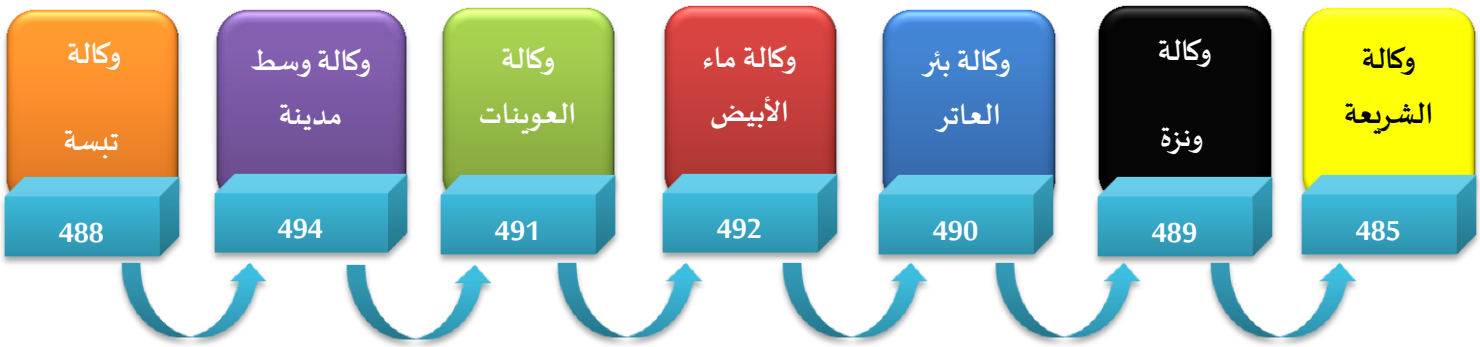
1. تقديم عام لمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية -تبسة-

يشكل بنك الفلاحة والتنمية الريفية ركيزة أساسية في البنية المالية والاقتصادية للجزائر حيث يلعب دورا حيويا في دعم القطاع الزراعي والتنمية الريفية، يتمتع البنك بحضور دائم ونشاط ملحوظ في السوق الجزائرية من خلال تقديمه لمجموعة واسعة من الخدمات المالية المخصصة للفلاحين والمزارعين والمشاريع الريفية. بفضل توجهه الاجتماعي والتنموي، يعتبر بنك الفلاحة والتنمية الريفية شريكا موثوقا للجهات الحكومية والمجتمع المدني في تعزيز الاقتصاد القروي وتحقيق التنمية المستدامة في الجزائر.

1.1. نشأة وتعريف المجمع الجهوي للاستغلال -تبسة-

أنشأ المجمع الجهوي للاستغلال تبسة بواسطة المرسوم الرئاسي الصادر بتاريخ 13 مارس 1982 المؤرخ في مارس 1982 وهي الممثلة لبنك الفلاحة والتنمية الريفية على مستوى ولاية تبسة كونها وكالة رئيسية للفرع الجهوي 012 أو ما يسمى بالمجموعة الجهوية للاستغلال لبنك الفلاحة والتنمية الريفية وهي تقع في حي "نهج العقيد محمد الشريف" هو مكان استراتيجي اذ يتوسط معظم المرافق العمومية في المدينة ووكالة بدر تبسة -488- يتفرع منها 6 وكالات أخرى وهي وكالة كانت في الماضي تابعة للبنك الوطني الجزائري إلى غاية مارس 1982، حيث تحولت إلى بنك الفلاحة والتنمية الريفية وهذا لتلبية حاجات السكان وخاصة أن الفلاحة هي النشاط الأكثر انتشارا في المنطقة وهي حاليا تتعامل مع 20.000 زبون يتكفل بهم موظفو الوكالة، والجدير بالذكر أن هذه الوكالة يتبعها (06) وكالات أخرى و المخطط التالي يوضح هذه الوكالات:

الشكل رقم (1): مخطط يمثل الوكالات التابعة لبنك الفلاحة والتنمية الريفية –تبسة-



المصدر: من إعداد الطالبة

2.1. الهيكل التنظيمي

اتخذ المجمع هيكل تنظيمي يتماشى مع التطورات التي تشهدها المنظومة المصرفية الجزائرية من اصلاحات نقدية وتطور تكنولوجي لتحسين جودة الخدمة البنكية والشكل الموالي يوضح الهيكل التنظيمي.

الشكل رقم (2): مخطط يمثل الهيكل التنظيمي للمجمع الجهوي للاستغلال لبنك بدر –تبسة-

المصدر: من إعداد الطالبة إعتمادا على المراجع المقدمة من مصالح المجمع الجهوي للاستغلال

3.1. أهداف المجمع الجهوي للاستغلال

يفرض المناخ الاقتصادي الجديد الذي تشهده الساحة المصرفية المحلية والعالمية على بنك الفلاحة والتنمية الريفية التي تلعب دورا أكثر ديناميكية والأكثر فاعلية في تمويل الاقتصاد الوطني من جهة اخرى وتدعيم مركزه التنافسي في ظل المتغيرات الراهنة من جهة أخرى وبذلك أصبح لازما على القائمين على البنك وضع استراتيجية أكثر فعالية لمواجهة التحديات التي تفرضها البيئة المصرفية.

وأمام كل هذه الأوضاء وجب على المسؤولين إعادة النظر في أساليب التنظيم وتقنيات التسيير التي يتبعها البنك والعمل على ترقية منتجاته وخدماته المصرفية من أجل إرضاء العملاء والاستجابة لانشغالاتهم.

وفي هذا الصدد لجأ بنك الفلاحة والتنمية الريفية مثله مثل البنوك العمومية الأخرى إلى القيام بأعمال ونشاطات متنوعة على مستوى عال من الجودة للوصول الى استراتيجية تتمثل في جعله مؤسسة مصرفية كبيرة وشاملة يتدخل في تمويل كل العمليات، وبهذا أصبح يحظى بثقة المتعاملين الاقتصاديين والعملاء على حد سوى، وهذا قصد تدعيم مكانته ضمن

الوسط المصرفي.

ومن أهم الأهداف المسطرة من طرف إدارة المجمع الجهوي للاستغلال ما يلي:

- توسيع وتنويع مجالات تدخل البنك كمؤسسة مصرفية شاملة.
- تحسين نوعية وجودة الخدمات.
- تحسين العلاقات مع العملاء.
- الحصول على أكبر حصة من السوق.
- العمل المصرفي قصد تحقيق أقصى قدر من الربح.

وبغية تحقيق تلك الأهداف قام البنك بتهيئة الإنطلاق في المرحلة الجديدة التي تتميز بتحولات هامة نتيجة انفتاح السوق المصرفية أمام البنوك الخاصة المحلية والأجنبية، حيث قام البنك بتوفير شبكات جديدة ووضع وسائل تقنية حديثة وأجهزة وأنظمة معلوماتية، كما بذل القائمون على البنك

بمجهودات لتأهيل موارده، وترقية الاتصال داخل وخارج البنك مع إدخال تعديلات على التنظيمات والهياكل الداخلية للبنك تتوافق مع المحيط المصرفي الوطني واحتياجات السوق.

كما سعى البنك إلى التقرب أكثر من الزبائن وهذا بتوفير مصالحة تتكفل بمطالبهم وانشغالاتهم والحصول على أكبر قدر من المعلومات الخاصة باحتياجاتهم و يسعى أيضا لتحقيق هذه الأهداف بفضل قيامه بـ:

- رفع حجم الموارد بأقل التكاليف.
- توسيع نشاطات البنك فيما يخص التعاملات.
- تسيير صارم لخزينة البنك بالدينار و العملة الصعبة.

2. الإطار المنهجي للدراسة الميدانية

يقوم البحث العلمي على أساس مجموعة من الخطوات والقواعد العامة التي يتم في إطارها البحث وتتمثل أساسا في تحديد المنهج المتبع الذي يتماشى وطبيعة الموضوع المختار للدراسة وإبراز أهم الأدوات المستعملة لتحليل البيانات ثم تحديد مجالات الدراسة المكانية والزمنية والبشرية والموضوعية، دون أن ننسى الاختيار الصائب لعينة البحث من مجتمع الدراسة.

1.2. المنهج المستخدم وأدوات الدراسة

أولا: المنهج المستخدم

يقول ديكارت أنه: "لا يمكن التفكير في بحث حقيقة ما بدون منهج لأن الدراسات والأبحاث دون منهج تمنع العقل من الوصول إلى الحقيقة"[1]، ويشير المنهج إلى أسلوب التفكير والعمل الذي يعتمده الباحث لتنظيم أفكاره وتحليلها وعرضها، وبالتالي الوصول إلى نتائج وحقائق معقولة حول الظاهرة موضوع الدراسة.[2]

[1] مروان عبد المجيد ابراهيم، **أسس البحث العلمي لإعداد الرسائل الجامعية**، دار الوراق، عمان: الأردن، الطبعة الأولى، 2000، ص 60.

[2] ربحي مصطفى عليان وعثمان محمد غنيم، **مناهج وأساليب البحث العلمي: النظرية والتطبيق**، دار الصفاء، عمان: الأردن، الطبعة الأولى، 2000، ص 33.

ان أي بحث علمي لابد أن يتم وفق منهج علمي محدد معترف به لدى الباحثين وفي هذا الإطار تتعدد مناهج البحث حسب طبيعة الموضوع المبحوث فيه، أما في دراستنا سيتم اعتماد المنهج الوصفي التحليلي باعتباره الطريقة التي يمكن أن يعتمد عليها الباحث لوصف الموضوع المراد دراسته من خلال منهجية علمية صحيحة، وعلى ضوء طبيعة الموضوع والأهداف التي نسعى لتحقيقها في إطار هذه الدراسة الوصفية التحليلية فإننا لا نقف عند جمع المعلومات لوصف الظاهرة فحسب وإنما نعتمد إلى تحليلها وكشف العلاقات بين أبعادها المختلفة من أجل تقديرها والوصول إلى استنتاجات تساعد على فهم الظاهرة من خلال تحليل الدور الرئيسي الذي تلعبه الامن السيبراني وانعكاساته على أمن المعلومات في المؤسسة محل الدراسة.

ثانيا: أدوات الدراسة

إن أي دراسة علمية لابد وأن تعتمد في جمع وتصنيف وتحليل البيانات على مجموعة من الأدوات وذلك من أجل الوصول إلى الحقائق العلمية الصحيحة للمشكلة محل الدراسة، وفي دراستنا هذه اعتمدنا على الأدوات التالية:

1/ أدوات جمع البيانات

يشير مفهوم الأداة إلى الوسيلة التي تجمع بها البيانات اللازمة للدراسة، وغالبا ما يستخدم الباحثون عددا كبيرا من أدوات جمع البيانات من بينها الملاحظة، الاستبيان، المقابلة بالإضافة إلى البيانات الإحصائية على إختلاف أنواعها، ولتحقيق أهداف الدراسة في هذه المرحلة تم إختيار الوسيلة الأكثر مناسبة، وهي الإستبيان.

أ. الإستبيان (الإستمارة)

يقصد بالإستبيان مجموعة من الأسئلة المصممة لجمع البيانات اللازمة عن المشكلة تحت الدراسة، وهي أهم الوسائل الفعالة في جمع البيانات شريطة أن يكون الباحث على معرفة دقيقة بالبيانات المطلوب جمعها وبكيفية قياس المتغيرات المرغوب دراستها.[1]

من أجل تحقيق هدف الدراسة تم تصميم استبيان مقسم إلى ثلاثة أجزاء كما يلي: (أنظر الملحق رقم 01)

[1] ربحي مصطفى عليان وعثمان محمد غنيم، **مرجع سبق ذكره**، ص 115.

البيانات الشخصية: وهو يشمل بيانات وصفية ووظيفية عن أفراد العينة وهو يحتوي على 4 فقرات: الجنس، السن، المستوى التعليمي، الخبرة.

المحور الأول: يتعلق برأي المبحوث في محور مستحقات الأمن السيبراني وبيئته في البنك ويتكون من 16 سؤال أساسي.

المحور الثاني: يتعلق برأي المبحوث في محور مستحقات أمن المعلومات وبيئته في البنك ويتكون من 16 سؤال أساسي.

المحور الثالث: يتعلق برأي المبحوث في محور تأثير الأمن السيبراني على أمن العلومات في البنك ويتكون من 20 سؤال أساسي.

كما تم وضع سلم ترتيبي لهذه الأرقام لإعطاء الوسط الحسابي مدلولا باستخدام المقياس الترتيبي للأهمية وذلك للإستفادة منها فيما بعد عند تحليل النتائج، وذلك كما هو موضح في الجدول التالي:

الجدول رقم (19): مقياس الإجابة على سلم ليكرت

التصنيف	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1

المصدر: من إعداد الطالبة

- المدى: 5-1= 4 (5 أعلى نقطة لمقياس ليكرت و 1 أدنى نقطة فيه).
- طول المدى: 4/5 = 0.8 (طول المدى = المدى/عدد الدرجات).
- يتم بعد ذلك حساب المتوسط الحسابي المرجح ثم يحدد الاتجاه حسب قيم هذا المتوسط كما يلي:

من 01 ← 1.79 .....غير موافق بشدة.

من 1.80 ← 2.59 ..... غير موافق.

من 2.60 ← 3.39 ..... محايد.

من 3.40 ← 4.19 ..... موافق.

من 4.20 ← 5 ..... موافق بشدة

ب. إجراءات توزيع الإستبيان

بعد إعداد الصورة الأولية للإستبيان، تم عرضها على بعض الأساتذة وبعدها تمت مراجعته وتصحيحه حسب توجيهاتهم، وهكذا تم إعداد الإستبيان في صورته النهائية. وبعدها تم تطبيقه ميدانيا على عينة من العاملين بمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة، وذلك من خلال إتباع الخطوات التالية:

- الحصول على موافقة الإدارة لتطبيق الدراسة ميدانيا على أفراد العينة.
- تسليم الإستبيانات لإدارة المؤسسة من أجل توزيعها على أفراد عينة الدراسة.
- إستعادة الإستبيانات.

2/ أدوات تحليل البيانات

إن البيانات المجمعة ومهما كانت دقتها وكميتها فهي لا قيمة لها إلا إذا تمت معالجتها عن طريق الأدوات الإحصائية المناسبة لطبيعة وأهداف الدراسة، وفي دراستنا هذه تم الاعتماد على برنامج SPSS. (حزمة البرامج الإحصائية للعلوم الاجتماعية)، حيث يعد هذا البرنامج من أكثر البرامج الإحصائية استخداما من قبل الباحثين في المجالات التربوية والفنية والهندسية والزراعية في إجراء التحليلات الإحصائية اللازمة، من خلال هذا البرنامج تم استعمال بعض الأدوات الإحصائية المعروفة وتتمثل هذه الأدوات فيما يلي:

- **التكرارات والنسب المئوية**: وذلك للتعرف على خصائص عينة الدراسة.
- **المتوسط الحسابي**: وذلك لمعرفة مدى ارتفاع وانخفاض إجابات عينة الدراسة لكل عبارة من عبارات محاور الدراسة ومن خلاله يمكن ترتيب عبارات المحاور حسب الأهمية النسبية.
- **الإنحراف المعياري**: للتعرف على مدى تركز الإجابات عن العبارات وتشتتها عن وسطها الحسابي.
- **معامل ألفا كرونباخ**: لمعرفة دلالة الثبات لأداة الدراسة ومحاورها.

- **معامل الإرتباط سبيرمان:** لمعرفة إن كان هناك علاقة بين الفقرات والمجال (البعد أو المتغير) الذي تنتمي اليه، حيث الارتباط يكون قويا عند اقترابه للواحد، وضعيفا عند اقترابه للصفر، ويكون ايجابي عندما يكون الإرتباط قوي، وعكسي عندما يكون الارتباط سالبا.

- **معامل الإرتباط بيرسون:** لمعرفة أن كان هناك علاقة بين (مجال أو بعد) الدراسة بالدرجة الكلية لفقرات الإستبانة.

- **اختبار معامل الانحدار البسيط:** عند مستوى معنوية ($\alpha \leq 0.05$): وذلك لإختبار فرضيات الدراسة الميدانية أي الكشف عن الأثر ذو الدلالة الإحصائية بين متغيرات الدراسة المتغير المستقل (الأمن السيبراني) والمتغير التابع (أمن المعلومات).

2.2. مجتمع الدراسة والعينة

سيتناول هذا المطلب وصفا لمجتمع الدراسة المتمثل في جميع المستويات في المؤسسة. ونظرا لصعوبة اجراء الدراسة على المجتمع ككل سيتم التطرق أيضا في هذا المطلب للعينة التي سيتم اختيارها من أجل إجراء الدراسة عليها.

أولا: مجتمع الدراسة

يعرف مجتمع الدراسة بشكل عام على أنه: مجموعة الأشياء المراد دراستها إما لوصفها أو إستقراء السمات العامة لها، أو لاستقراء العلاقة بينها للوصول إلى السنن الكونية.[1]

تركز هذه الدراسة على موضوع انعكاسات الأمن السيبراني على أمن المعلومات بالمؤسسة، ويتمثل مجتمع الدراسة في جميع المستويات الإدارية بمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة محل الدراسة.

ثانيا : عينة الدراسة

العينة هي جزء من المجتمع الأصلي، والذي يحتوي على بعض العناصر التي تم اختيارها منه بطريقة معينة، وذلك بقصد دراسة خصائص المجتمع الأصلي.[2]

---

[1] سعيد اسماعيل صيني، **قواعد أساسية في البحث العلمي**، مؤسسة الرسالة، بيروت، الطبعة الأولى، 1994، ص 220.

[2] سعيد اسماعيل صيني، **مرجع سابق**، ص 23.

تم إختيار عينة عشوائية من الموظفين بالمؤسسة محل الدراسة، وتم توزيع (50) إستمارة إستبيان على الموظفين وعلى ذلك يكون عدد مفردات عينة البحث وفق المراحل التالية في المؤسستين محل الدراسة والموضحة في الجدول التالي:

الجدول رقم (20): تعداد استمارات الدراسة في المؤسسة

الاستبانات	الموزعة	المسترجعة	المفقودة	المستبعدة	النهائية
المجموع	50	40	6	4	40
النسبة المئوية	%100	%80	%12	%8	%80

المصدر: من إعداد الطالبة

ثالثا: مجالات الدراسة

تعبر مجالات الدراسة على الحدود البشرية والمكانية والزمنية والموضوعية التي تمت فيها الدراسة وتتمثل في:

- **المجال البشري**: إقتصرت الدراسة على عينة عشوائية من الموظفين العاملين بمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة.
- **المجال المكاني**: موضوع هذه الدراسة هو انعكاسات الأمن السيبراني على أمن المعلومات في المؤسسة، والدراسة الميدانية تمت بمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة.
- **المجال الزمني**: ان أي دراسة تستلزم فترة زمنية لإجرائها تتحدد حسب طبيعة الموضوع وقدرة الباحث على جمع المعلومات اللازمة عنه، ومدى التسهيلات المقدمة من طرف المؤسسة لإتمام الدراسة، وفي هذا الإطار تم أخذ الموافقة على القيام بهذه الدراسة في شهر ماي من عام 2024، وتمت الدراسة الميدانية فعلا بدءا من 12 ماي 2024 إلى غاية 23 ماي من نفس السنة لجمع المعلومات من خلال توزيع الإستمارة والحصول على الإجابات اللازمة.

3.2. إختبار صدق وثبات أداة الدراسة

سيتم التركيز في هذا المطلب على أداة الدراسة المتمثلة في الإستبيان من حيث صدقها، حيث تستخدم مجموعة من الطرق لإثبات صدق وثبات الاستبانة وهي :

1/ صدق أداة الدراسة

يقصد بمعامل الصدق، مدى صلاحية الإستبيان في قياس السلوك الذي صمم من أجله، أي أنه لا يقيس شيئا آخر بدلا منه. وتجدر الإشارة، أنه لا يوجد إختبار عديم الصدق تماما أو تام الصدق، وإنما تتوقف درجة الصدق على مدى ثبات الإختبار.[1]

ويتكون الصدق من نوعين هما:

- **الصدق الظاهري**: من أجل التأكد من مدى صدق أداة الدراسة المتمثلة في الإستبيان في قياس ما وضعت من أجل قياسه، وهو مدى تطبيق الأمن السيبراني في المؤسسة محل الدراسة من خلال درجة توفر أسسه ودرجة توفر مجالات تطبيقه وانعكاساته على أمن المعلومات بالمؤسسة، تم عرض الإستبيان على مجموعة من الأساتذة المحكمين من أجل معرفة آرائهم حوله، ومدى مناسبته لموضوع الدراسة وهدفها. وبناءا على ملاحظات الأساتذة وآرائهم تم تعديل الإستبيان وتصميمه في صورته النهائية.
- **صدق المقياس:** ويتكون بدوره من الإتساق الداخلي والصدق البنائي:

الإتساق الداخلي: ويقصد به مدى إتساق كل فقرة من فقرات الإستبانة مع المجال (البعد أو المتغير) الذي تنتمي إليه هذه الفقرة، وتستخدم الباحثة معامل الإرتباط سبيرمان بين كل من الفقرة والمجال الذي تنتمي اليه.

أولا: الاتساق الداخلي لمحور(مستحقات الأمن السيبر اني وبيئته في البنك)

- يوضح الجدول رقم 03 أدناه معامل الإرتباط بين كل فقرة من فقرات المحور الأول والدرجة الكلية للمحور، والذي يبين أن معاملات الإرتباط المبينة دالة عند مستوى معنوي ($\alpha \leq 0.01$)

[1] محمد عبد الفتاح الصيرفي، **البحث العلمي: الدليل التطبيقي للباحثين**، دار وائل، عمان: الأردن، الطبعة الأولى، 2002، ص 85.

لأن القيمة الإحتمالية أقل من مستوى المعنوية، وبذلك يعتبر المجال صادقا لما وضع لقياسه، وعليه كل فقرات هذا المجال صالحة للتحليل بدون حذف.

الجدول رقم (21): معامل الإرتباط سبيرمان بين كل فقرة من فقرات محور مستحقات الأمن السيبراني وبيئته في البنك والدرجة الكلية لهذا المحور في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية -تبسة-

الفقرات	معامل الإرتباط	القيمة الإحتمالية
1. يمتلك البنك الوعي الكافي والإحاطة الشاملة بمخاطر التهديدات السيبرانية التي قد تواجهه.	0.865**	0.000
2. تحيط بالبنك تهديدات سيبرانية بإمكانها أن تدمر نظم المعلومات.	0.831 **	0.000
3. يتولى البنك فعالية إجراءات الوقاية والتدابير المتخذة لمواجهة الهجمات السيبرانية.	0.860 *	0.010
4. يطبق البنك سياسات واجراءات واضحة للأمن السيبراني.	0.830 **	0.000
5. الانتقال من البنية التقليدية إلى البنية الرقمية يتطلب استثمارات ضخمة وتغييرات هيكلية تمنع البنوك من تنفيذ استراتيجيات الأمن السيبراني الشاملة	0.777 **	0.000
6. يواجه البنك نقص في الموارد البشرية والمهارات الفنية اللازمة لتنفيذ سياسات الأمن السيبراني بشكل فعال.	0.831 **	0.000
7. اغفال البنك عن توفير التدريب المناسب للموظفين في مجال الأمن السيبراني	0.754 **	0.000
8. يواجه البنك صعوبة في تحديث أنظمته التكنولوجية القديمة مما يزيد من التحدي في تطبيق أحدث التقنيات والإجراءات الأمنية	0.941 **	0.000
9. تنفيذ تقنيات التشفير المعتمدة على المعايير الدولية لتأمين البيانات المالية والشخصية للعملاء	0.798 **	0.000

10. تعزيز إجراءات التحقق المزدوج والتعرف على الهوية لتقليل مخاطر الوصول غير المصرح به	0.866 **	0.000
11. تنفيذ آليات الرصد المستمرة لنشاطات الشبكة والبيانات للكشف المبكر عن أي تهديدات محتملة	0.863 **	0.000
12. تطوير سياسات صارمة لإدارة الوصول والتحكم في الصلاحيات لضمان أقصى درجات الحماية من الاختراقات الداخلية والخارجية	0.815 **	0.000
13. تعزيز الاستجابة الفعالة للتهديدات الجديدة في عالم الأمن السيبراني مما يحد من تأثيرها السلبي على البنك وعملائه	0.866 **	0.000
14. التقليل من مخاطر الاختراقات وتسريبات البيانات مما يحافظ على سمعة البنك وثقة العملاء	0.815 **	0.000
15. تقوية الشراكات مع الجهات التنظيمية والشركاء التجاريين مما يساهم في تعزيز مكانة البنك في السوق المالية	0.727 **	0.000
16. تحقيق الاستدامة المالية والحفاظ على مكانته كرائد في قطاع الخدمات المالية	0.815 **	0.000

** الارتباط دال إحصائيا عند مستوى المعنوية ($\alpha \leq 0.01$)

المصدر: من إعداد الطالبة بالإعتماد على مخرجات spss

ثانيا: الاتساق الداخلي لمحور (مستحقات أمن المعلومات وبيئته في البنك)

- يوضح الجدول رقم 04 أدناه معامل الإرتباط بين كل فقرة من فقرات المحور الثاني من المحور الثاني والدرجة الكلية للمحور، والذي يبين أن معاملات الإرتباط المبينة دالة عند مستوى معنوية ($\alpha \leq 0.01$) لأن القيمة الإحتمالية أقل من مستوى المعنوية، وبذلك يعتبر المجال صادقا لما وضع لقياسه، وعليه كل فقرات هذا المجال صالحة للتحليل بدون حذف.

الجدول رقم (22): معامل الإرتباط سبيرمان بين كل فقرة من فقرات محور مستحقات أمن المعلومات وبيئته في البنك والدرجة الكلية لهذا البعد.

الفقرات	معامل الإرتباط	القيمة الإحتمالية
1. تعاني البنوك بشكل متزايد من هجمات الاختراق والاختراقات السيبرانية التي تهدد سرية وسلامة المعلومات الحساسة	0.946**	0.000
2. تظل البنوك عرضة للتهديدات السيبرانية نتيجة للثغرات الأمنية والهجمات المتطورة	0.942**	0.000
3. يطبق البنك سياسات واجراءات لتحقيق الأمن الشامل للبيانات	0.801 **	0.000
4. يواجه البنك تحديات فريدة في مجال أمن المعلومات نتيجة لضرورة التوازن بين سهولة الوصول للعملاء وحماية البيانات المالية الحساسة	0.813**	0.000
5. قلة الخبرة والكفاءة في مجال أمن المعلومات تجعل من التحدي تطبيق تقنيات متقدمة داخل البنوك	0.790**	0.000
6. التحديات المالية والميزانية المحدودة تقف كعائق أمام قدرة البنك على الاستثمار في حلول أمن المعلومات الشاملة	0.882**	0.000
7. الافتقار لاستخدام تقنيات الكشف المبكر والاستجابة الفعالة للحفاظ على سلامة البيانات وثقة العملاء	0.790**	0.000
8. تعقيدات الشراكات مع جهات خارجية ومقدمي الخدمات الأمنية تحول دون تبني البنك لتقنيات أمن المعلومات المتطورة	0.813 **	0.000
9. توفير سياسات صارمة تحدد الإجراءات الأمنية المطلوبة لحماية البيانات المالية والشخصية للعملاء والموظفين	0.917**	0.000
10. توفير اجراءات للتعامل مع حوادث الأمان مثل اختراقات البيانات	0.830**	0.000

والاحتيال بما في ذلك خطط الطوارئ وإجراءات الاستجابة السريعة		
11. توعية وتدريب الموظفين بشأن أفضل الممارسات في مجال الأمان وحماية المعلومات	0.852**	0.000
12. تبني آليات لتقييم وتحسين الأمان بناء على التهديدات الجديدة وتطورات التكنولوجيا	0.849**	0.000
13. توفير بيئة موثوقة وآمنة يعزز من فرص الابتكار والنمو في البنك حيث يشعر الموظفون والعملاء بالراحة في التفاعل مع النظام المصرفي	0.790 **	0.000
14. توفير إطار قوي لأمان المعلومات يسهم في تعزيز الثقافة الأمنية داخل البنك مما يزيد من وعي الموظفين ويقلل من مخاطر الاختراقات	0.880**	0.000
15. تقليل مخاطر فقدان البيانات والتعرض للهجمات السيبرانية مما يقلل من تكاليف الاستجابة للحوادث الأمنية ويعزز كفاءة العمليات المصرفية	0.812**	0.000
16. توفير تكاليف إضافية نتيجة لتقليل التهديدات السيبرانية وزيادة الكفاءة التشغيلية	0.864**	0.000

** الإرتباط دال إحصائيا عند مستوى المعنوية ($\alpha \leq 0.01$)

المصدر: من إعداد الطالبة بالإعتماد على مخرجات spss

ثالثا: الاتساق الداخلي لمحور (تأثير الأمن السيبراني على أمن العلومات في البنك)

- يوضح الجدول رقم 05 أدناه معامل الإرتباط بين كل فقرة من فقرات المحور الثاني من المحور الثاني والدرجة الكلية للمحور، والذي يبين أن معاملات الإرتباط المبينة دالة عند مستوى معنوية ($\alpha \leq 0.01$) لأن القيمة الإحتمالية أقل من مستوى المعنوية، وبذلك يعتبر المجال صادقا لما وضع لقياسه، وعليه كل فقرات هذا المجال صالحة للتحليل بدون حذف.

الجدول رقم (23): معامل الإرتباط سبيرمان بين كل فقرة من فقرات محور تأثير الأمن السيبراني على أمن العلومات في البنك و الدرجة الكلية لهذا البعد.

الفقرات	معامل الإرتباط	القيمة الإحتمالية
1. الحفاظ على سلامة بيانات العملاء والمعاملات المالية يعكس التزام البنك بأعلى معايير الأمان ويبني علاقات طويلة الأمد مع العملاء	0.942**	0.000
2. توفير تجارب مالية آمنة وموثوقة يجعل العملاء يشعرون بالراحة والثقة في التعامل مع البنك والاستمرار في استخدام خدماته	0.952**	0.000
3. التواصل الفعال مع العملاء حول التهديدات السيبرانية المحتملة والإجراءات المتخذة لمواجهتها يزيد من ثقتهم في البنك وسمعته	0.942 **	0.000
4. تقديم حلول أمان مبتكرة وفعالة يؤكد على التزام البنك بحماية مصالح عملائه ويعزز الثقة في قدرته على التعامل مع التهديدات السيبرانية	0.953**	0.000
5. تشكل آليات الأمن السيبراني درعا حصينا يحمي البيانات المالية والمعاملات الإلكترونية من الوصول الغير مصرح به	0.895**	0.000
6. اعتماد السياسات والإجراءات الأمنية الصارمة يضمن تطبيق المعايير الأمنية العالية ويقيد محاولات الاختراق	0.853**	0.000
7. تبني تقنيات الكشف المبكر والتحليل المستمر يمكنه تحديد والتصدي للتهديدات السيبرانية المحتملة قبل حدوث الاختراقات	0.802**	0.000
8. تطبيق إجراءات الوقاية والاستجابة الفعالة يحد من فرص الاختراقات ويقلل من تأثيرها على البيانات المالية	0.894 **	0.000
9. استخدام الهوية الرقمية والتحقق الثنائي يعزز أمان المعاملات المالية عبر الانترنت ويحميها من الاختراقات	0.854**	0.000
10. تطبيق نظام متقدم للكشف عن التسلل يستخدم تحليل السلوك وتقنيات التعرف على النمط لاكتشاف الاختراقات والتصدي لها بشكل فعال	0.830**	0.000

11. تطوير وتحديث نظم الأمان السيبراني بشكل دوري يضمن استمرارية الحماية ضد التهديدات الجديدة والمتطورة	0.828**	0.000
12. توفير خدمات النسخ الاحتياطي واستعادة البيانات يضمن استمرارية العمليات المالية في حالة حدوث اختراقات أو فقدان للبيانات	0.892**	0.000
13. استخدام التقنيات البيومترية مثل بصمات الأصابع والتعرف على الوجه يعزز الحماية ويقلل من فرص الاختراقات بشكل فعال	0.874 **	0.000
14. توفير آليات التشفير والتوقيع الرقمي يمنع الاختراقات ويضمن سلامة المعاملات المالية الإلكترونية	0.772**	0.000
15. تطبيق تقنيات التعقب والتعقيد لتقييد الوصول إلى البيانات المالية للأشخاص المعتمدين فقط و أنظمة النسخ الاحتياطي واستعادة البيانات	0.854**	0.000
16. تطبيق تقنيات الذكاء الاصطناعي يمكن من تحليل النمط السلوكي والتنبؤ بالهجمات السيبرانية المحتملة	0.803**	0.000
17. توفير التدريب المستمر للموظفين والعملاء حول أحدث التهديدات السيبرانية يعزز قدرتهم على التعامل مع المخاطر بفعالية	0.876**	0.000
18. تحفيز الموظفين على تبني أفضل الممارسات في إدارة كلمات المرور والوصول الآمن إلى البيانات يعزز أمن النظام المالي	0.803**	0.000
19. تعزيز التواصل المستمر مع العملاء حول مخاطر الأمان السيبراني يسهم في تعزيز تبادل المعلومات الآمن والحفاظ على البيانات الحساسة	0.801**	0.000
20. إشراك الموظفين والعملاء في عمليات التقييم والتحليل لتحديد نقاط الضعف في الأمان السيبراني يسهم في تعزيز الحماية والتحسين المستمر	0.772**	0.000

** الإرتباط دال إحصائيا عند مستوى المعنوي ($\alpha \leq 0.01$)

المصدر: من إعداد الطالبة بالإعتماد على مخرجات spss

- **الصدق البنائي:** يعتبر الصدق البنائي أحد مقاييس صدق الأداة الذي يقيس مدى تحقق الأهداف التي تريد الأداة الوصول إليها. ويعرف من مدى إرتباط كل مجال (البعد أو

المتغير)الدراسة بالدرجة الكلية لفقرات الإستبانة وهنا نستعمل معامل الإرتباط بيرسون لمعرفة الصدق البنائي.

الجدول رقم (24): معامل الإرتباط بيرسون بين كل محور من محاور الإستبيان والدرجة الكلية للإستبانة

	الأبعاد	معامل الإرتباط	القيمة الإحتمالية
المحور الأول	مستحقات الأمن السيبراني وبيئته في البنك	0.964**	0.000
المحور الثاني	مستحقات أمن المعلومات وبيئته في البنك	0.997**	0.000
المحور الثالث	تأثير الأمن السيبراني على أمن المعلومات في البنك	0.975**	0.000
الكل			

** الإرتباط دال إحصائيا عند مستوى المعنوية ($\alpha \leq 0.01$)

المصدر: من إعداد الطالبة بالإعتماد على مخرجات spss

يبين الجدول 06 السابق أن جميع معاملات الإرتباط في جميع مجالات الإستبيان دالة إحصائيا، وأن محتوى كل بعد من أبعاد الإستبيان له علاقة قوية بهدف الدراسة عند مستوى معنوية ($\alpha \leq 0.01$)، لأن القيمة الإحتمالية أقل من مستوى المعنوية لكل بعد، وبذلك تعتبر جميع أبعاد الإستبيان صادقة لما وضعت لقياسه، وعليه كلها صالحة للتحليل بدون حذف.

1/ ثبات أداة الدراسة

بعد عرض الإستبيان على الأساتذة المحكمين والتأكد من صدقه الظاهري، تم توزيعه على عينة الدراسة لمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة. تمت عملية استرجاع الإستبيانات والقيام بعمليات الترميز وادخال البيانات للحاسوب باستخدام برنامج الحزم الاحصائية للعلوم الاجتماعية Statistical package for social sciences SPSS ومن أجل ثبات

الإستبيان، والذي يعني أن النتائج ستكون نفسها تقريبا إذا تكرر تطبيقها على نفس أفراد العينة. تم استخدام معامل ألفا كرونباخ Cronbach's Alpha وجاءت النتائج كما يلي:

الجدول رقم (25): قياس ثبات محاور الإستبيان

المحور	عدد عبارات المحور	قيمة معامل ألفا كرونباخ
مجموع العبارات والقيمة العامة للمعامل	**52**	**0.994**

المصدر: من إعداد الطالبة اعتمادا على مخرجات برنامج spss

يظهر الجدول السابق أن معامل ألفا كرونباخ عالي، حيث:

- بلغت قيمة معامل ألفا كرونباخ الخاصة بالإستبيان بشكل عام 0.994.

وبشكل عام، وبما أن كل قيم المعامل عالية فهذا يعني أن الإستبيان يتمتع بدرجة ثبات تجعل منه أداة مقبولة وصالحة للدراسة.

3. عرض وتحليل نتائج الدراسة الميدانية في المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

نهدف من خلال هذا المبحث إلى عرض نتائج الدراسة حول متغيراتها المعتمدة بشكل مفصل، للتعرف على الخصائص الشخصية للعينة وتحليل وتفسير إجابات الموظفين الخاصة بمحاور الدراسة وأخيرا اختبار فرضيات الدراسة الميدانية.

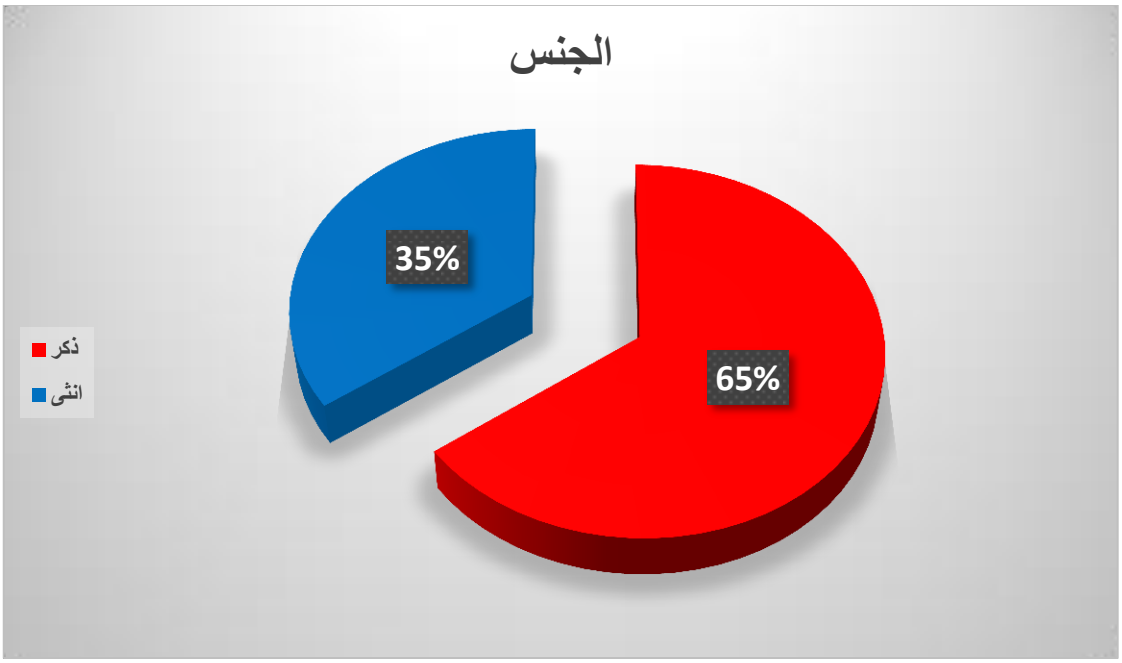
1.3. عرض وتحليل البيانات الشخصية في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

يهدف هذا المطلب إلى التعرف على الخصائص الشخصية الخاصة بأفراد عينة الدراسة من خلال متغيرات: الجنس، السن، المستوى التعليمي، الخبرة.

أولا: متغير الجنس

يمثل الشكل التالي تلخيصا للنتائج المتعلقة بتوزيع أفراد العينة حسب الجنس:

الشكل رقم (03): توزيع أفراد العينة حسب الجنس في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة



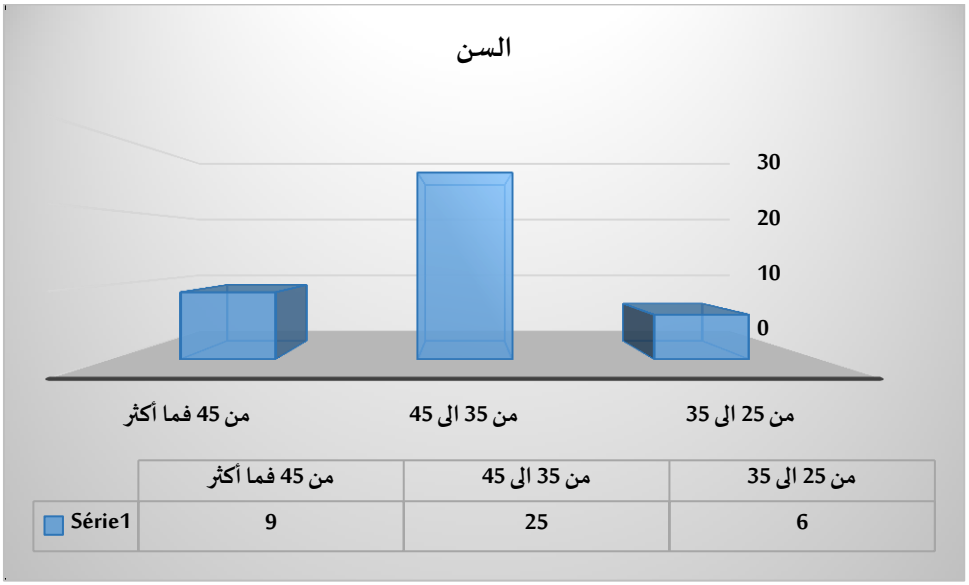
المصدر: من إعداد الطالبة بالاعتماد على مخرجات spss

يشير الشكل رقم (03): إلى أن نسبة 65% من عينة الدراسة ذكور وأن نسبة 35% فقط من أفراد العينة إناث نستنتج من هذا الشكل أن نسبة الذكور أكبر من نسبة الإناث وهذا يدل على أن الغالبية العظمى من الموظفين في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة من الذكور وهذا ملاحظ في كل المؤسسات الجزائرية. قد يكون السبب في ذلك يرجع إلى ثقافة المجتمع التي قد لا تفضل تقدم الأنثى على الرجل في كثير من مناحي الحياة العملية والإجتماعية أو قد تكون لأسباب أخرى وقد يعود إلى طبيعة عمل المؤسسة الاقتصادية الذي يعتمد على الذكور.

ثانيا: متغير السن

يمثل الشكل التالي تلخيصا للنتائج المتعلقة بتوزيع أفراد العينة حسب السن:

الشكل رقم (04): توزيع أفراد العينة حسب السن في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة



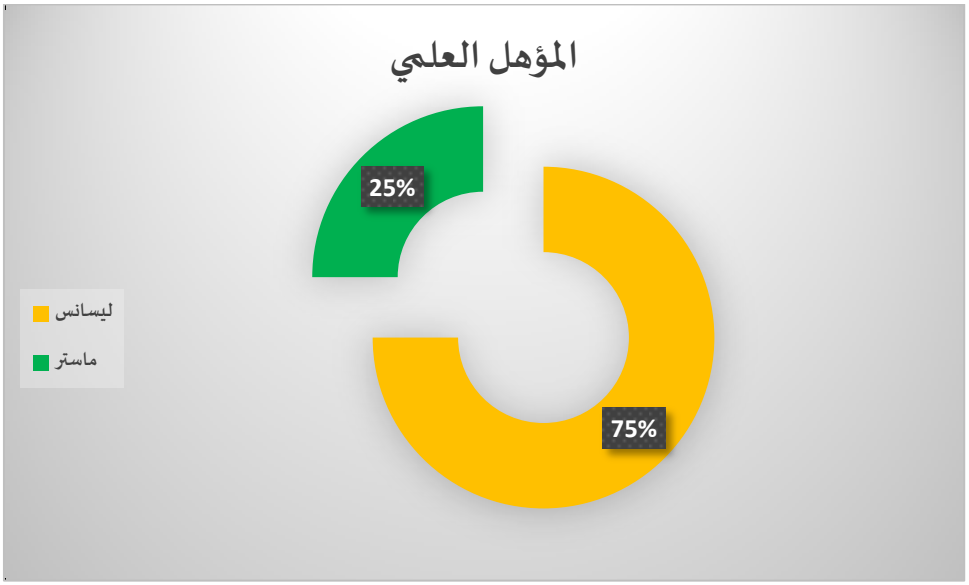
المصدر: من اعداد الطالبة بالاعتماد على مخرجات spss

يتبين من الشكل رقم (04) أن نسبة 62% هي للذين تتراوح أعمارهم ما بين (35 إلى 45 سنة) ونسبة 23% هي للذين أعمارهم من 45 فما أكثر، و نسبة 15% هي للذين أعمارهم ما بين (25 إلى 35 سنة)، وهذا يشير إلى أن مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة تحافظ على العاملين ذوي الخبرة كما تقوم باستقطاب موظفين جدد ذوي خبرة وهذا ما تبينه النتائج السابقة وكذلك يلاحظ من هذا الجدول أن توزيع أعمار المبحوثين يتسم بالتوازن النسبي إلى حد ما ولعل ذلك يدعم تواصل الأجيال.

ثالثا المستوى التعليمي

يمثل الشكل التالي تلخيصا للنتائج المتعلقة بتوزيع أفراد العينة حسب المستوى التعليمي:

الشكل رقم (05): توزيع أفراد العينة حسب المستوى التعليمي في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة



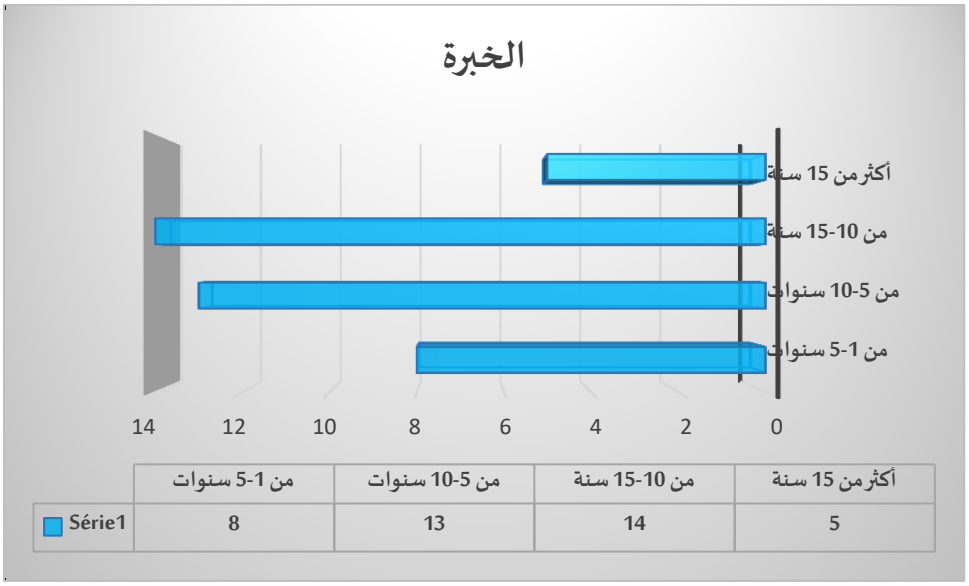
المصدر: من اعداد الطالبة بالاعتماد على مخرجات spss

يتبين من الشكل رقم (05) أن نسبة 7% من عينة الدراسة متحصل على شهادة جامعية ليسانس ونسبة 25% من الذين هم متحصلون على شهادة جامعية ماستر.

يستنتج من الجدول أعلاه أن هنالك نسبة كبيرة من المبحوثين اي غالبية الموظفين في المؤسسة هم متحصلون على شهادات جامعية عليا، وهذا قد يعطي مؤشر ايجابي إذ أن معظم المبحوثين لديهم مؤهلات عليا مما يعني أن سياسة المؤسسة قد تتجه إلى تعيين أصحاب المؤهلات العليا في الوظائف القيادية.

رابعا- سنوات الخبرة: يمثل الشكل التالي تلخيصا للنتائج المتعلقة بتوزيع أفراد العينة حسب سنوات الخبرة

الشكل رقم (06): توزيع أفراد العينة حسب سنوات الخبرة في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة



المصدر: من اعداد الطالبة بالاعتماد على مخرجات spss

يشير الشكل رقم (06) إلى أن نسبة عينة الدراسة الذين تقع خبراته من 10 الى 15 سنوات 35% بينما أن نسبة 32% تتراوح خبراتهم من 05 إلى 10 سنة ونسبة 20% خبراتهم هي من 1- 5 سنوات ونسبة 13% خبراتهم هي اكثر من 15 سنة.

ومن خلال ما تقدم يمكن القول أن توزيع أفراد العينة حسب خبراتهم في المؤسسة يتسم بالتوازن الموضوعي إذ لا يعقل أن يكون كل افراد العينة متساويين في الخبرة ولذا فإن هذا التباين مبرر ومفيد وفيه إثراء لمختلف المبحوثين من خلال تبادل الآراء والأفكار والخبرات وهذا قد ينعكس إيجابا على أداء هذا القطاع .

ومن خلال هذا المطلب تعرفنا على الخصائص الشخصية لعينة الدراسة في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة ، والمتمثلة في الجنس، السن، المستوى التعليمي، الخبرة.

ليتم بعدها عرض نتائج الإجابة على أسئلة استمارة الدراسة، والتعرف على رأي عينة الدراسة منها، من خلال المطلب الموالي.

2.3. عرض النتائج المتعلقة بأسئلة الدراسة في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

سنقوم في هذا المطلب بعرض النتائج المتعلقة بأسئلة الدراسة، وتحليلها وتفسيرها، وذلك للتعرف على اتجاهات الموظفين في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة نحو كل محور من محاور الدراسة.

أولا: رأي المبحوثين في محور مستحقات الأمن السيبراني وبيئته في البنك في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

نهدف من خلال هذا المحور إلى إلقاء الضوء على اتجاهات العاملين بمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة، حول **مستحقات الأمن السيبراني وبيئته في البنك** في المؤسسة وعلى ضوء استجابة العينة، سوف يتم الإعتماد على التوزيعات التكرارية لإجابات عينة الدراسة والنسب المئوية لها وصولا إلى الوسط الحسابي والإنحراف المعياري.

الجدول رقم (26): استجابات عينة الدراسة نحو العبارات التي تصف محور مستحقات الأمن السيبراني وبيئته في البنك في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

الفقرات	المتوسط الحسابي	الإنحراف المعياري	الاهمية
واقع الأمن السيبراني في البنك			
1. يمتلك البنك الوعي الكافي والإحاطة الشاملة بمخاطر التهديدات السيبرانية التي قد تواجهه	4.40	0.841	2
2. تحيط بالبنك تهديدات سيبرانية بإمكانها أن تدمر نظم المعلومات	4.53	0.751	1
3. يتولى البنك فعالية إجراءات الوقاية والتدابير المتخذة لمواجهة الهجمات السيبرانية	3.43	0.501	3

4. يطبق البنك سياسات واجراءات واضحة للأمن السيبراني	3.35	0.483	4
تحديات البنك في تطبيق سياسات الأمن السيبراني			
5. الانتقال من البنية التقليدية إلى البنية الرقمية يتطلب استثمارات ضخمة وتغييرات هيكلية تمنع البنوك من تنفيذ استراتيجيات الأمن السيبراني الشاملة	4.72	0.452	1
6. يواجه البنك نقص في الموارد البشرية والمهارات الفنية اللازمة لتنفيذ سياسات الأمن السيبراني بشكل فعال	3.97	0.577	3
7. اغفال البنك عن توفير التدريب المناسب للموظفين في مجال الأمن السيبراني	3.75	0.439	4
8. يواجه البنك صعوبة في تحديث أنظمته التكنولوجية القديمة مما يزيد من التحدي في تطبيق أحدث التقنيات والإجراءات الأمنية	4.02	0.947	2
متطلبات وشروط سياسات الأمن السيبراني			
9. تنفيذ تقنيات التشفير المعتمدة على المعايير الدولية لتأمين البيانات المالية والشخصية للعملاء	4.70	0.464	1
10. تعزيز إجراءات التحقق المزدوج والتعرف على الهوية لتقليل مخاطر الوصول غير المصرح به	4.03	0.620	2
11. تنفيذ آليات الرصد المستمرة لنشاطات الشبكة والبيانات للكشف المبكر عن أي تهديدات محتملة	3.87	0.607	3
12. تطوير سياسات صارمة لإدارة الوصول والتحكم في الصلاحيات لضمان أقصى درجات الحماية من الاختراقات الداخلية والخارجية	3.68	0.474	4
فعالية وجدوى تطبيق سياسات الأمن السيبراني			

13. تعزيز الاستجابة الفعالة للتهديدات الجديدة في عالم الأمن السيبراني مما يحد من تأثيرها السلبي على البنك وعملائه	3.55	0.504	3
14. التقليل من مخاطر الاختراقات وتسريبات البيانات مما يحافظ على سمعة البنك وثقة العملاء	3.68	0.474	2
15. تقوية الشراكات مع الجهات التنظيمية والشركاء التجاريين مما يساهم في تعزيز مكانة البنك في السوق المالية	3.78	0.423	1
16. تحقيق الاستدامة المالية والحفاظ على مكانته كرائد في قطاع الخدمات المالية	3.68	0.474	2
المتوسط العام لمحور مستحقات الأمن السيبراني وبيئته في البنك	3.94	0.495	

المصدر: من اعداد الطالبة بالاعتماد على مخرجات spss

يتضح من الجدول (08) أن أفراد عينة الدراسة موافقون على محور مستحقات الأمن السيبراني وبيئته في البنك. وهذا ما يعكسه المتوسط الحسابي، إذ بلغ (3.94) وهو متوسط يقع ضمن الفئة الرابعة من فئات ليكرت الخماسي (3.40 – 4.19)، وهي الفئة التي تشير إلى استجابة موافق، وانحراف معياري قدره (0.495)، نرى أن هناك تشتتا متوسطا نوعا ما في الإجابات.

ثانيا: رأي المبحوثين في مستحقات أمن المعلومات وبيئته في البنك في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

نهدف من خلال هذا المحور إلى إلقاء الضوء على اتجاهات العاملين بمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة، حول **مستحقات أمن المعلومات وبيئته في البنك** في المؤسسة وعلى ضوء استجابة العينة، سوف يتم الإعتماد على التوزيعات التكرارية لإجابات عينة الدراسة والنسب المئوية لها وصولا إلى الوسط الحسابي والإنحراف المعياري.

الجدول رقم (27): استجابات عينة الدراسة نحو العبارات التي تصف محور مستحقات أمن المعلومات وبيئته في البنك في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

الفقرات	المتوسط الحسابي	الإنحراف المعياري	الأهمية
واقع أمن المعلومات في البنك			
1. تعاني البنوك بشكل متزايد من هجمات الاختراق والاختراقات السيبرانية التي تهدد سرية وسلامة المعلومات الحساسة	2.88	0.791	4
2. تظل البنوك عرضة للتهديدات السيبرانية نتيجة للثغرات الأمنية والهجمات المتطورة	3.15	0.770	3
3. يطبق البنك سياسات واجراءات لتحقيق الأمن الشامل للبيانات	3.70	0.464	1
4. يواجه البنك تحديات فريدة في مجال أمن المعلومات نتيجة لضرورة التوازن بين سهولة الوصول للعملاء وحماية البيانات المالية الحساسة	3.58	0.712	2
تحديات البنك في تطبيق تقنيات أمن المعلومات			
5. قلة الخبرة والكفاءة في مجال أمن المعلومات تجعل من التحدي تطبيق تقنيات متقدمة داخل البنوك	3.98	0.530	3
6. التحديات المالية والميزانية المحدودة تقف كعائق أمام قدرة البنك على الاستثمار في حلول أمن المعلومات الشاملة	4.10	0.632	1
7. الافتقار لاستخدام تقنيات الكشف المبكر والاستجابة الفعالة للحفاظ على سلامة البيانات وثقة العملاء	3.93	0.526	4
8. تعقيدات الشراكات مع جهات خارجية ومقدمي الخدمات الأمنية تحول دون تبني البنك لتقنيات أمن المعلومات المتطورة	4.00	0.555	2
متطلبات توفير سياسات أمن المعلومات			
9. توفير سياسات صارمة تحدد الإجراءات الأمنية المطلوبة لحماية	3.73	0.679	4

البيانات المالية والشخصية للعملاء والموظفين			
10. توفير اجراءات للتعامل مع حوادث الأمان مثل اختراقات البيانات والاحتيال بما في ذلك خطط الطوارئ وإجراءات الاستجابة السريعة	3.83	0.549	3
11. توعية وتدريب الموظفين بشأن أفضل الممارسات في مجال الأمان وحماية المعلومات	3.95	0.597	1
12. تبني آليات لتقييم وتحسين الأمان بناء على التهديدات الجديدة وتطورات التكنولوجيا	3.85	0.580	2
جدوى تطبيق سياسات أمن المعلومات			
13. توفير بيئة موثوقة وآمنة يعزز من فرص الابتكار والنمو في البنك حيث يشعر الموظفون والعملاء بالراحة في التفاعل مع النظام المصرفي	3.98	0.530	1
14. توفير إطار قوي لأمان المعلومات يسهم في تعزيز الثقافة الأمنية داخل البنك مما يزيد من وعي الموظفين ويقلل من مخاطر الاختراقات	3.85	0.622	3
15. تقليل مخاطر فقدان البيانات والتعرض للهجمات السيبرانية مما يقلل من تكاليف الاستجابة للحوادث الأمنية ويعزز كفاءة العمليات المصرفية	3.90	0.545	2
16. توفير تكاليف إضافية نتيجة لتقليل التهديدات السيبرانية وزيادة الكفاءة التشغيلية	3.83	0.594	4
المتوسط العام لمحور مستحقات أمن المعلومات وبيئته في البنك	3.76	0.544	

المصدر: من اعداد الطالبة بالاعتماد على مخرجات spss

يتضح من الجدول (27) أن أفراد عينة الدراسة موافقون على محور مستحقات أمن المعلومات وبيئته في البنك. وهذا ما يعكسه المتوسط الحسابي، إذ بلغ (3.76) وهو متوسط يقع ضمن الفئة الرابعة من فئات ليكرت الخماسي (3.40 – 4.19)، وهي الفئة التي تشير إلى استجابة موافق ، وانحراف معياري قدره (0.544)، نرى أن هناك تشتتا متوسطا نوعا ما في الإجابات.

ثالثا: رأي المبحوثين في تأثير الأمن السيبراني على أمن المعلومات في البنك في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

نهدف من خلال هذا المحور إلى إلقاء الضوء على اتجاهات العاملين بمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة، حول **تأثير الأمن السيبراني على أمن المعلومات في البنك** في المؤسسة وعلى ضوء استجابة العينة، سوف يتم الإعتماد على التوزيعات التكرارية لإجابات عينة الدراسة والنسب المئوية لها وصولا إلى الوسط الحسابي والإنحراف المعياري.

الجدول رقم (28): استجابات عينة الدراسة نحو العبارات التي تصف محور تأثير الأمن السيبراني على أمن المعلومات في البنك في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

الفقرات	المتوسط الحسابي	الإنحراف المعياري	الأهمية
تعزيز ثقة العملاء وحماية سمعة البنك			
1. الحفاظ على سلامة بيانات العملاء والمعاملات المالية يعكس التزام البنك بأعلى معايير الأمان ويبني علاقات طويلة الأمد مع العملاء	**4.03**	**0.660**	**2**
2. توفير تجارب مالية آمنة وموثوقة يجعل العملاء يشعرون بالراحة والثقة في التعامل مع البنك والاستمرار في استخدام خدماته	**3.90**	**0.672**	**4**
3. التواصل الفعال مع العملاء حول التهديدات السيبرانية المحتملة والإجراءات المتخذة لمواجهتها يزيد من ثقتهم في البنك وسمعته	**3.98**	**0.660**	**3**

4. تقديم حلول أمان مبتكرة وفعالة يؤكد على التزام البنك بحماية مصالح عملائه ويعزز الثقة في قدرته على التعامل مع التهديدات السيبرانية	4.05	0.677	1
حماية البيانات والمعاملات المالية من الاختراق			
5. تشكل آليات الأمن السيبراني درعا حصينا يحمي البيانات المالية والمعاملات الإلكترونية من الوصول الغير مصرح به	4.00	0.599	1
6. اعتماد السياسات والإجراءات الأمنية الصارمة يضمن تطبيق المعايير الأمنية العالية ويقيد محاولات الاختراق	3.90	0.545	3
7. تبني تقنيات الكشف المبكر والتحليل المستمر يمكنه تحديد والتصدي للتهديدات السيبرانية المحتملة قبل حدوث الاختراقات	3.95	0.504	2
8. تطبيق إجراءات الوقاية والاستجابة الفعالة يحد من فرص الاختراقات ويقلل من تأثيرها على البيانات المالية	3.90	0.591	4
اجراءات الحماية من الهجمات السيبرانية			
9. استخدام الهوية الرقمية والتحقق الثنائي يعزز أمان المعاملات المالية عبر الانترنت ويحميها من الاختراقات	3.95	0.552	2
10. تطبيق نظام متقدم للكشف عن التسلل يستخدم تحليل السلوك وتقنيات التعرف على النمط لاكتشاف الاختراقات والتصدي لها بشكل فعال	4.02	0.530	1
11. تطوير وتحديث نظم الأمان السيبراني بشكل دوري يضمن استمرارية الحماية ضد التهديدات الجديدة والمتطورة	3.88	0.516	3
12. توفير خدمات النسخ الاحتياطي واستعادة البيانات يضمن استمرارية العمليات المالية في حالة حدوث اختراقات أو فقدان للبيانات	3.85	0.580	4
التكنولوجيا			
13. استخدام التقنيات البيومترية مثل بصمات الأصابع والتعرف	3.88	0.563	4

على الوجه يعزز الحماية ويقلل من فرص الاختراقات بشكل فعال			
14. توفير آليات التشفير والتوقيع الرقمي يمنع الاختراقات ويضمن سلامة المعاملات المالية الإلكترونية	3.93	0.474	3
15. تطبيق تقنيات التعقب والتعقيد لتقييد الوصول إلى البيانات المالية للأشخاص المعتمدين فقط وأنظمة النسخ الاحتياطي واستعادة البيانات	3.95	0.552	2
16. تطبيق تقنيات الذكاء الاصطناعي يمكن من تحليل النمط السلوكي والتنبؤ بالهجمات السيبرانية المحتملة	4.00	0.506	1
تعزيز الوعي بين الموظفين والعملاء			
17. توفير التدريب المستمر للموظفين والعملاء حول أحدث التهديدات السيبرانية يعزز قدرتهم على التعامل مع المخاطر بفعالية	3.97	0.577	3
18. تحفيز الموظفين على تبني أفضل الممارسات في إدارة كلمات المرور والوصول الآمن إلى البيانات يعزز أمن النظام المالي	4.00	0.506	2
19. تعزيز التواصل المستمر مع العملاء حول مخاطر الأمان السيبراني يسهم في تعزيز تبادل المعلومات الآمن والحفاظ على البيانات الحساسة	3.90	0.496	4
20. إشراك الموظفين والعملاء في عمليات التقييم والتحليل لتحديد نقاط الضعف في الأمان السيبراني يسهم في تعزيز الحماية والتحسين المستمر	4.02	0.480	1
المتوسط العام لمحور تأثير الأمن السيبراني على أمن المعلومات في البنك	3.95	0.521	

المصدر: من اعداد الطالبة بالاعتماد على مخرجات spss

يتضح من الجدول (28) أن أفراد عينة الدراسة موافقون على محور تأثير الأمن السيبراني على أمن المعلومات في البنك. وهذا ما يعكسه المتوسط الحسابي، إذ بلغ (3.95) وهو متوسط يقع ضمن

الفئة الرابعة من فئات ليكرت الخماسي (3.40 – 4.19)، وهي الفئة التي تشير إلى استجابة موافق ، وانحراف معياري قدره (0.521)، نرى أن هناك تشتتا متوسطا نوعا ما في الإجابات.

وعليه من خلال هذا المطلب تم عرض وتحليل إجابات المبحوثين حول أسئلة محاور الدراسة، التي تعبر على متغيرات إشكالية الدراسة، وبهذا نكون قد حددنا اتجاهاتهم وآرائهم حول موضوع الدراسة، ومعرفة واقعه في هذه المؤسسة، ولكن هذا لا يكفي لإعطاء إجابة مقنعة عن الإشكالية، لذا لابد من اكتشاف العلاقة بين هذه المتغيرات وهذا ما سيتم القيام به في المطلب الموالي من خلال اختبار فرضيات الدراسة.

3.3. اختبار فرضيات الدراسة في مؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة

نسعى من خلال هذا المطلب اختبار فرضيات الدراسة الميدانية الخاصة بمؤسسة المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية تبسة.

1/ اختبار صحة الفرضية الاولى

محتوى الفرضية: هناك مستحقات الأمن السيبراني وبيئته في البنك

H0. ليس هناك مستحقات الأمن السيبراني وبيئته في البنك.

H01. يوجد هناك مستحقات الأمن السيبراني وبيئته في البنك.

بما أن المحور الأول من استمارة الاستبيان يتبع التوزيع الطبيعي فإنه يخضع للاختبارات المعلمية وستكون الإحصائية المناسبة لاختبار هذه الفرضية هو اختبار ستيودينت للعينة الأحادية عند مستوى معنوية 0.05 والجدول التالي يبين النتائج:

الجدول رقم (29): نتائج اختبار ستيودنت للفرضية الأولى

	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	T	مستوى الدلالة T
المحور الأول	**3.95**	**0.496**	**39**	**12.058**	**0.000**

المصدر: من اعداد الطلبة بالاعتماد على مخرجات spss

من خلال الجدول أعلاه نلاحظ:

- أن متوسط العينة يساوي 3.95 بانحراف معياري قدره 0.496 وقيمة T المحسوبة تساوي 12.058 وهي أكبر من قيمة t الجدولية التي تساوي 2,02 أي أن (T_t=2.02[1]) < (T_c=12.058[2]) وذلك عند درجة معنوية (Sig=0.000) أصغر من مستوى الدلالة (**α ≤ 0,05**)، لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة على أساس أنه يوجد هناك مستحقات الأمن السيبراني وبيئته في البنك.

2/ اختبار صحة الفرضية الثانية

محتوى الفرضية: هناك مستحقات أمن المعلومات وبيئته في البنك

H0. ليس هناك مستحقات أمن المعلومات وبيئته في البنك.

H01. يوجد هناك مستحقات أمن المعلومات وبيئته في البنك.

بما أن المحور الثاني من استمارة الاستبيان يتبع التوزيع الطبيعي فإنه يخضع للاختبارات المعلمية وستكون الإحصائية المناسبة لاختبار هذه الفرضية هو اختبار ستيودينت للعينة الأحادية عند مستوى معنوية 0.05 والجدول التالي يبين النتائج :

[1] F_t = قيمة إختبار تحليل التباين لخط الإنحدار المجدولة عند مستوى الدلالة (α ≤ 0,05)، ودرجة حرية (1.28).

[2] F_c = قيمة اختبار تحليل التباين لخط الانحدار المحسوبة عند مستوى الدلالة (α ≤ 0,05).

الجدول رقم (30): نتائج اختبار ستيودنت للفرضية الثانية

	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	T	مستوى الدلالة T
المحور الأول	**3.76**	**0.544**	**39**	**8.871**	**0.000**

المصدر: من اعداد الطلبة بالاعتماد على مخرجات spss

من خلال الجدول أعلاه نلاحظ:

- أن متوسط العينة يساوي 3.76 بانحراف معياري قدره 0.544 وقيمة T المحسوبة تساوي 8.871 وهي أكبر من قيمة t الجدولية التي تساوي 2,02 أي أن (T_t=2.02[1]) < (T_c=8.871[2]) وذلك عند درجة معنوية (Sig=0.000) أصغر من مستوى الدلالة (**$\alpha \leq$ 0,05**) ، لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة على أساس أنه يوجد هناك مستحقات أمن المعلومات وبيئته في البنك.

3/ اختبار صحة الفرضية الثالثة

محتوى الفرضية: هناك تأثير للأمن السيبراني على أمن المعلومات في البنك

H0. ليس هناك تأثير للأمن السيبراني على أمن المعلومات في البنك.

H01. يوجد هناك تأثير للأمن السيبراني على أمن المعلومات في البنك.

بما أن المحور الثالث من استمارة الاستبيان يتبع التوزيع الطبيعي فانه يخضع للاختبارات المعلمية وستكون الإحصائية المناسبة لاختبار هذه الفرضية هو اختبار ستيودينت للعينة الأحادية عند مستوى معنوية 0.05 والجدول التالي يبين النتائج:

[1] F_t = قيمة إختبار ستيودنت المجدولة عند مستوى الدلالة ($\alpha \leq 0,05$)، ودرجة حرية (1.39).

[2] F_c = قيمة اختبار ستيودنت المحسوبة عند مستوى الدلالة ($\alpha \leq 0,05$).

الجدول رقم (31): نتائج اختبار ستيودنت للفرضية الثالثة

	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	T	مستوى الدلالة T
المحور الثالث	**3.95**	**0.521**	**39**	**11.563**	**0.000**

المصدر: من اعداد الطلبة بالاعتماد على مخرجات spss

من خلال الجدول أعلاه نلاحظ:

- أن متوسط العينة يساوي 3.95 بانحراف معياري قدره 0.521 وقيمة T المحسوبة تساوي 11.563 وهي أكبر من قيمة t الجدولية التي تساوي 2,02 أي أن (T_t=2.02[1]) < (T_c=11.563[2]) وذلك عند درجة معنوية (Sig=0.000) أصغر من مستوى الدلالة (**α ≤ 0,05**) ، لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة على أساس أنه يوجد هناك تأثير للأمن السيبراني على أمن المعلومات في البنك.

وبالتالي نلاحظ أن كل الفرضيات محققة.

وعليه تم من خلال هذا المطلب اختبار فرضيات الدراسة المتمثلة في الفرضيات الفرعية الثلاثة التي تعبر عن الإشكالية الرئيسية للدراسة لمعرفة انعكاسات الأمن السيبراني على أمن المعلومات في المؤسسة، وتم الإعتماد على اختبار ستيودنت لقياس هذا الدور، وأظهرت النتائج وجود أثر ذو دلالة إحصائية بين متغيرات الدراسة.

- أن متوسط العينة يساوي 3.76 بانحراف معياري قدره 0.544 وقيمة T المحسوبة تساوي 8.871 وهي أكبر من قيمة t الجدولية التي تساوي 2,02 أي أن (T_t=2.02[3]) < (T_c=8.871[4]) وذلك عند درجة معنوية (Sig=0.000) أصغر من مستوى الدلالة (α ≤ 0,05) ، لذلك نرفض الفرضية

[1] F_t = قيمة إختبار ستيودنت المجدولة عند مستوى الدلالة (α ≤ 0,05)، ودرجة حرية (1.39).

[2] F_c = قيمة اختبار ستيودنت المحسوبة عند مستوى الدلالة (α ≤ 0,05).

[3] F_t = قيمة إختبار ستيودنت المجدولة عند مستوى الدلالة (α ≤ 0,05)، ودرجة حرية (1.39).

[4] F_c = قيمة اختبار ستيودنت المحسوبة عند مستوى الدلالة (α ≤ 0,05).

الصفرية ونقبل الفرضية البديلة على أساس أنه يوجد هناك مستحقات أمن المعلومات وبيئته في البنك.

- أن متوسط العينة يساوي 3.76 بانحراف معياري قدره 0.544 وقيمة T المحسوبة تساوي 8.871 وهي أكبر من قيمة t الجدولية التي تساوي 2,02 أي أن (T_t=2.02[1]) < (T_c=8.871[2]) وذلك عند درجة معنوية (Sig=0.000) أصغر من مستوى الدلالة ($\alpha \leq 0,05$) ، لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة على أساس أنه يوجد هناك مستحقات أمن المعلومات وبيئته في البنك.

- أن متوسط العينة يساوي 3.95 بانحراف معياري قدره 0.521 وقيمة T المحسوبة تساوي 11.563 وهي أكبر من قيمة t الجدولية التي تساوي 2,02 أي أن (T_t=2.02[3]) < (T_c=11.563[4]) وذلك عند درجة معنوية (Sig=0.000) أصغر من مستوى الدلالة ($\alpha \leq 0,05$)، لذلك نرفض الفرضية الصفرية ونقبل الفرضية البديلة على أساس أنه يوجد هناك تأثير للأمن السيبراني على أمن المعلومات في البنك.

[1] F_t = قيمة إختبار ستيودنت المجدولة عند مستوى الدلالة ($\alpha \leq 0,05$)، ودرجة حرية (1.39).

[2] F_c = قيمة اختبار ستيودنت المحسوبة عند مستوى الدلالة ($\alpha \leq 0,05$).

[3] F_t = قيمة إختبار ستيودنت المجدولة عند مستوى الدلالة ($\alpha \leq 0,05$)، ودرجة حرية (1.39).

[4] F_c = قيمة اختبار ستيودنت المحسوبة عند مستوى الدلالة ($\alpha \leq 0,05$).

خلاصة الجزء الثاني:

لقد حاولنا في هذا الفصل الميداني معرفة انعكاسات الأمن السيبراني على أمن المعلومات في المؤسسة، حيث تبين لنا أن المؤسسة تعتمد على الأمن السيبراني والتي تساهم من خلاله في أمن معلومات المؤسسة.

كما تناول هذا الفصل وصفاً لمنهج الدراسة، والمؤسسة محل الدراسة وكذا عينة الدراسة، بالإضافة إلى أداة الدراسة المستخدمة وطرق إعدادها، وصدقها وثباتها، مع تحديد الاجراءات التي قامت بها الباحثة في تقنين أدوات الدراسة وتطبيقها، وأخيرا المعالجات الإحصائية المعتمدة في تحليل نتائج الدراسة واختبار الفرضيات. وقد تبين لنا أن هناك تأثير للأمن السيبراني على أمن المعلومات في المؤسسة.

وفي الأخير خرجنا بجملة من النتائج التي سيتم تلخيصها من خلال الخاتمة العامة ومن خلالها تم اعطاء للمؤسسة مجموعة من الاقتراحات والتوصيات التي يمكنها الإستفادة منها.

الجزء الثالث:

الدراسة التطبيقية بالبنك الخارجي الجزائري وكالة - تبسة 46-

تمهيد:

بعد التطرق في الجزء السابق إلى تأثير الأمن السيبراني على أمن المعلومات في البنوك الجزائرية، وتمت دراسته على مستوى المجمع الجهوي للاستغلال لبنك الفلاحة والتنمية الريفية -تبسة-، جاء هذا الجزء كدراسة إضافية للموضوع وإسقاطها عمليا على مستوى بنك آخر لتكون الدراسة أكثر فاعلية.

حيث إرتأينا في هذا الجزء أبراز إنعكاسات الأمن السيبراني على أمن المعلومات في البنك الخارجي الجزائري وكالة تبسة رقم 46 من خلال عينة، بعرض نتائج التحليل الإحصائي للبيانات في الإستبيان، وتحليل آراء عينة الدراسة، بالإعتماد على الأساليب الكمية وبالذات الإحصائية لإختبار الفرضيات، وعليه فقد تم تقسيم هذا الفصل الى ثلاثة مباحث كانت كالتالي:

- القسم الأول: بطاقة تعريفية بالبنك الخارجي الجزائري وكالة تبسة
- القسم الثاني: الإطار المنهجي للدراسة؛
- القسم الثالث: تحليل نتائج الدراسة وإختبار الفرضيات.

1. بطاقة تعريفية بالبنك الخارجي الجزائري وكالة تبسة

يعتبر البنك الخارجي الجزائري مؤسسة وطنية هدفها الرئيسي تسهيل وتطوير وتنمية العلاقات الاقتصادية والمالية للجزائر مع دول العالم، وذلك في إطار التخطيط الوطني ومن أهم وظائفه تسهيل تنمية مجالات العمليات التجارية مع سائر بلدان العالم ويمكن له التدخل في مختلف العمليات البنكية.

لذلك سيتم التعريف بالبنك الجزائري الخارجي الأم ثم بوكالة تبسة رقم 46 موقع التربص وتقديم هيكله التنظيمي.

1.1. التعريف بالبنك الخارجي الجزائري ونشأته

نشأة البنك الخارجي الجزائري:

تأسس البنك الخارجي الجزائري بموجب الأمر 67-204 المؤرخ في 1967/10/10 على أساس انه شركة وطنية أي بنك إيداع، وقد سجل هذا قائمة ضمن قائمة البنوك بصفة تلقائية، وبحكم القانون اكتسب صفة الوسيط المالي بالقيام بالعمليات التجارية مع الدول الأجنبية، يسير هذا البنك من طرف وزير المالية مع مراعاة القواعد التقنية الخاصة بالسياسة العامة المبلغة إلى رئيسه المدير العام، وقد تم تكوين البنك الخارجي الجزائري نهائيا ابتداءا من 1968/01/01، وقد خصص له في البداية رأس مال يقدر بـ 20 مليون دينار جزائري مقدمة من الدولة ومنذ سنة 1970، كان البنك الخارجي الجزائري يمول شركات معينة فقط مثل سوناطراك والنقل البحري... الخ، ليتغير وضع البنك الخارجي الجزائري بعد إعادة تكوين المؤسسات الصناعية الكبيرة التي قامت بها السلطات العمومية في بداية الثمانينات حيث أصبح البنك شركة ذات أسهم[1].

2.1. التعريف بالبنك الخارجي الجزائري وكالة تبسة رقم 46

نظرا للتطورات التي يشهدها النظام المصرفي وسعيا منه لتحقيق التنمية ومواكبة التطور، قامت البنوك بإنشاء وحدات لها حتى تتمكن من مزاولة نشاطها عبر كافة التراب الوطني، وتقريب الخدمات من المواطنين إضافة للمساهمة في إحداث التنمية المحلية، هذه الوحدات تكون على مستوى الولايات وتتحدد مهامها تحت وصاية الإدارة المركزية للبنك.

[1] معلومات مقدمة من طرف مسؤول مصلحة الزبائن في وكالة تبسة رقم 46

1- نشأة البنك الخارجي الجزائري وكالة تبسة رقم 46

استجابة للحاجات المالية المحلية أنشأ البنك الخارجي الجزائري وحدة وكالة تبسة رقم 46 حيث تأسست بتاريخ 02 جانفي 1990، وهي خاضعة لأحكام القانون التجاري.

تتمثل وظيفتها الأساسية في تسهيل وتنمية العلاقات الاقتصادية بين الجزائر والدول الأخرى، تقوم هذه الوكالة أيضا باستقبال الودائع ومنح الاعتمادات بالنسبة للمستوردين والضمانات بالنسبة للمصدرين الجزائريين لتسهيل مهمتهم في التصدير، وتضع اتفاقات واعتمادات مع البنوك الأجنبية ونظرا لتعدد مهام الوكالة فقد قسمت إلى قسمين:[1]

- **قسم خاص بالائتمان:** يقوم بقبول الودائع ومنح القروض.

- **قسم خاص بالعمليات الخارجية:** يقوم بتجهيز وتمويل الشركات الكبرى (مثل: سوناطراك وشركة الإسمنت وشركة مناجم الحديد تبسة).

ثم بدأت عمليات الوكالة تتوسع تدريجيا فأصبحت تنفرد بتسيير حسابات الشركات الصناعية الكبرى في ميدان المحروقات والصناعات الكيماوية والبتروكيماوية.

2 - مهام البنك الخارجي الجزائري وكالة تبسة رقم 46

من أبرز مهام الوكالة ما يلي:

- إدارة العلاقات التجارية مع الزبائن؛
- تنظيم وتحليل وإدارة ملفات القروض للخواص والمؤسسات ذات الطابع الاقتصادي أو ذات الطابع الصناعي؛
- المعالجة الإدارية والمحاسبية لعمليات الزبائن بالعملة الوطنية والأجنبية.

أما بالنسبة لمهام مدير الوكالة فتتمثل في الإشراف على:

- تطوير وتقييم رأس المال الاقتصادي للوكالة؛
- تنظيم وتطوير وتنشيط ومراقبة نشاطات الوكالة؛
- السهر على التكوين وتقديم المعلومات وتطوير مستوى موظفي الوكالة؛

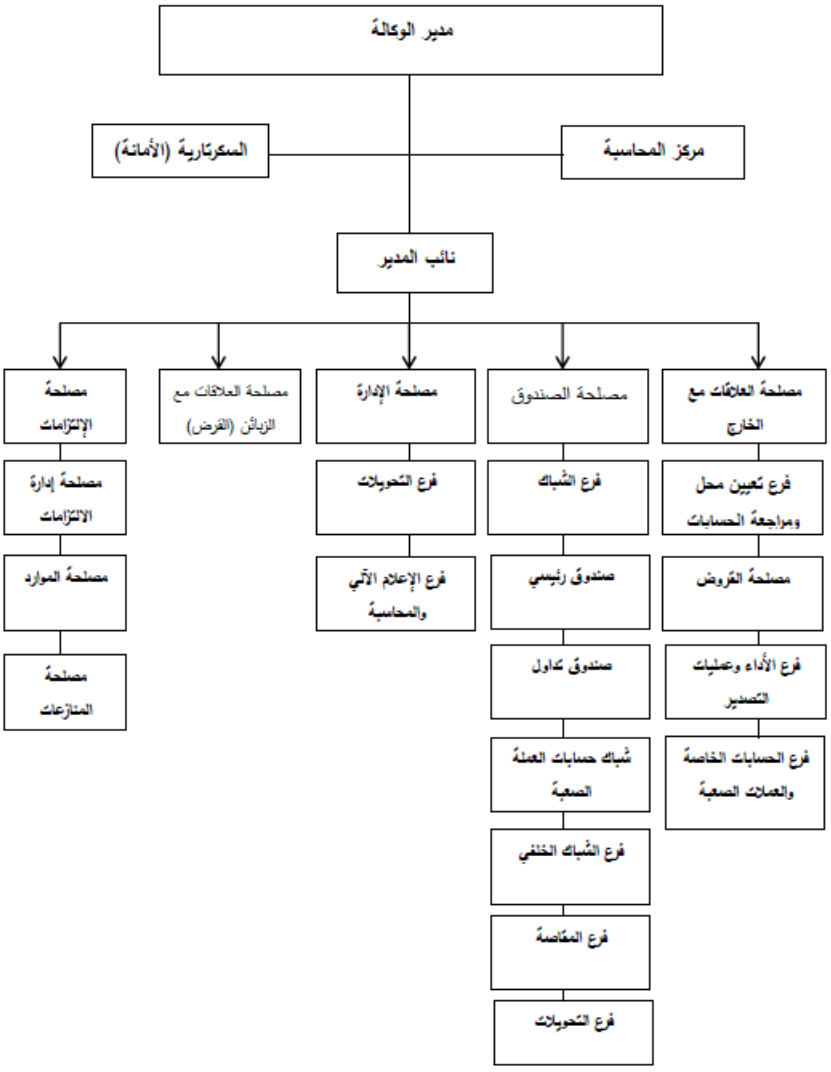
[1] معلومات مقدمة من طرف مسؤول مصلحة الزبائن في وكالة تبسة رقم 46

- السهر على السير الحسن للخدمات المقدمة للزبائن؛
- تقديم تقارير بصفة دورية عن نشاطات الوكالة.[1]

3.1. الهيكل التنظيمي للبنك الخارجي الجزائري وكالة تبسة رقم 46

للبنك الخارجي الجزائري في ولاية تبسة وكالة واحدة وهي وكالة تبسة رقم 46 وفيما يلي تقديم ودراسة هيكلها التنظيمي:

الشكل (07): الهيكل التنظيمي لوكالة تبسة رقم 46



المصدر: الوثائق الداخلية لوكالة تبسة

[1] معلومات مقدمة من طرف مسؤول مصلحة الزبائن في وكالة تبسة رقم 46

1- المدير: وهو خاضع مباشرة تحت سلطة مدير الشبكة، ويعتبر المسؤول الأول عن تسيير البنك والنتائج التجارية لهيكله هو ممثل البنك الخارجي الجزائري على المستوى المحلى مكلف بالمهام التالية:

- تقييم عمل الاستغلال للإدارة بإعطاء التعليمات والتوجيهات؛
- استقبال الزبائن في حالة وجود مشكلة لتسويتها؛
- السهر على تطبيق القوانين التي تدير البنك؛
- الإمضاء على البريد.

2- المدير المساعد: ويوجد تحت سلطة المباشرة لمدير الفرع، وتتمثل مهامه الأساسية في: تحقيق نشاطات وأهداف الفرع وكذلك يقوم مقام المدير في حالة غيابه؛

- ويقوم كذلك بتسيير الوسائل البشرية والعتاد إضافة إلى الجانب المتعلق بالميزانية وأمن الفرع؛
- ويقوم كذلك بتسيير الوسائل البشرية والعتاد إضافة إلى الجانب المتعلق بالميزانية وأمن الفرع.

3- سكرتارية (الأمانة): وتتكلف بالبريد الوارد والصادر عن الوكالة والقيام بالأعمال المكتبية وكذلك ضمان وسائل الاتصال على مستوى الفرع هاتف، فاكس أنترنت ...) وتوصيل الملاحظات ونشرها الصادرة عن المدير.

4- مصلحة المحاسبة: وتقوم هذه المصلحة بعدة مهام مثل مراقبة العمليات المحاسبية التي تجري في المصالح الأخرى ومراقبة الوثائق المحاسبية لكل المصالح وتقوم بالتحقق من كتابات المحاسبة والجرد وهي المسؤولة عن كتابة الوثائق المحاسبية الشرعية والقانونية للبنك وهذه المصلحة تتفرع إلى:

أ- مصلحة المحفظة:

وتقوم بالمهام التالية:

- ضمان الاحتفاظ بالأوراق التجارية وسندات الصندوق المقدمة من طرف العملاء من اجل تحصيلها قبل تاريخ استحقاقها؛
- مقاصة الأوراق التجارية الشيكات وغيرها من القيم؛
- القيام بعملية الاكتتاب الاحتفاظ والرهن الحيازي السندات الصندوق؛

- دفع الأوراق التجارية؛

-إرسال القيم إلى البنوك الأخرى للتحصيل.

ب- مصلحة عمليات الصندوق:

وتقوم بالمهام التالية:

- استقبال الزبائن وتسيير حساباتهم وحسابات المستخدمين؛
- القيام بالتسديدات، والتحويلات والوضع تحت التصرف؛
- ضمان دفع وسحب الأموال (دينار وعملة صعبة)؛
- إصدار الشيكات المصادقة أو المصرفية؛
- معالجة عملية الصرف اليدوي؛
- القيام بمنح الشيكات ودفاتر التوفير؛
- ضمان تأجير الخزانات الحديدية.

5- المكلف بالزبائن: تابع لمدير الفرع وتكمن مهمته في وضع مخطط النشاط الاقتصادي للفرع عن طريق البحث والمشاركة استثمار الزبائن.

6- مصلحة التعهد والالتزامات: موضوعة تحت سلطة ومسؤولية رئيس المصلحة وتقوم بالنشاطات المتعلقة بدراسة وتحليل ملفات التمويل وذلك بتقديم الآراء حول الملفات المعالجة وترسلها إلى المديرية المركزية للإقرار فيها، وتقوم بالمصادقة على فتح وغلق الحسابات وكذلك ضمان المتابعة المستمرة وتحصيل الديون المتعثرة والمتنازع فيها وإعداد تقارير دورية حول شروط إنجازها، وتقوم بإعداد ومنح عقود الالتزامات اتفاقية منح التمويل عقود الكفالات والقبول وتتابع تطبيق الشروط المصرفية بصفة عامة في مجال الالتزامات.

7- المراقبة: وتقوم بالمراقبة اليومية المحاسبية والسهر على مسك الجيد للحسابات وهي مكلفة أيضا بالأعمال المتعلقة (فتح وغلق النظام المعلوماتي، نسخ وضعيات نهاية اليوم...)

8-خدمات مصرفية: تتمثل في مجموع العمليات التي تقدمها الوكالة مثل: تقديم القروض وعمليات الصندوق وعمليات التجارة الخارجية (الاعتماد المستندي).[1]

2. الإطار المنهجي للدراسة

يعد الإطار المنهجي بمثابة الخارطة التي توجه الباحث في مساره البحثي، فهو يحدد الخطوات التي سيتبعها والطرق التي سيستخدمها لجمع وتحليل البيانات، كما يساعد على ضمان دقة وموضوعية البحث، وهذا ما سوف يتم تسليط الضوء عليه في هذا المبحث.

1.2. عينة الدراسة وأدوات جمع البيانات

سوف يتم في هذا المطلب تحديد كل من عينة الدراسة وكذا أدوات جمع البيانات بغية الوصول إلى نتائج يمكن تعميمها.

يتمثل مجتمع وعينة الدراسة كما يلي:

1- **مجتمع الدراسة:** عند القيام بالدراسة الميدانية ينبغي على الباحث تحديد تعريف واضح لمجتمع الدراسة للمساعدة في تحديد الأسلوب العلمي، حيث يتمحور مجتمع الدراسة في العناصر قيد الدراسة في البنك الخارجي الجزائري وكالة تبسة رقم 46.

2- **عينة الدراسة:** وهي عبارة عن انتقاء مجموعة من العناصر من مجتمع الدراسة الجمع البيانات والعمل على تحقيق ما ستتوصل اليه الدراسة من أهداف.

حيث تم توزيع 40 استبيان على وظيفي في وكالة تبسة، إلا أنه تم قبول 35 استبيان فقط. وبالتالي تم الاعتماد على 35 استبيان كنموذج للدراسة، وهذا ما يوضحه الجدول التالي الموالي:

الجدول رقم (32): عينة الدراسة

عدد أفراد الدراسة	عدد الاستبانات الموزعة	عدد الاستبانات المسترجعة	عدد الاستبانات الصالحة
40	40	35	28

المصدر: من اعداد الطالبة

[1] معلومات مقدمة من طرف مسؤول مصلحة الزبائن في وكالة تبسة -46-

3- **طرق جمع البيانات:** تم الإعتماد على الإستبيان الذي يعتبر من الطرق التي يلجأ لها الباحثون وذلك من خلال توجيه مجموعة من العبارات المكتوبة إلى المبحوث حول موضوع البحث والحصول على إجابات لهذه العبارات، وقد تم تطوير الدراسة بالإستعانة على عدد من الدراسات والكتب المتعلقة بموضوع إنعكاسات الأمن السيبراني على أمن المعلومات في البنوك، وقد تم صياغة عبارات الإستبيان للدراسة الحالية بما يتوافق مع فرضيات الدراسة.

2.2. الأساليب الإحصائية المستخدمة في الدراسة

لتحقيق أهداف الدراسة وتحليل البيانات سيتم الاعتماد على طرق إحصائية يتم من خلالها وصف المتغيرات وتحديد نوعية العلاقة الموجودة بينها.

1- وصف أداة الدراسة (الاستبيان): يعد الإستبيان أداة بحثية تتكون من مجموعة من الأسئلة المصممة لجمع المعلومات من عينة الدراسة حول موضوع محدد، حيث يضم هذا الجزء العبارات المتعلقة بالإستبيان وقد تم توزيعها على 04 محاور كما هو مبين في الجدول التالي:

جدول رقم (33): يوضح عبارات الإستبيان

المحور	عدد الأسئلة
المحور الأول: البيانات الشخصية	05
المحور الثاني: الأمن السيبراني	16
المحور الثالث: أمن المعلومات	12
المحور الرابع: نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	11

المصدر: من اعداد الطالبة

2- أدوات التحليل: تم الاعتماد على برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSSV28)[1]في هذا التحليل الميداني بعد توزيع الاستبيان والحصول على إجابات وذلك باستخدام الأدوات الإحصائية التالية:

2-1- التكرارات والنسب المئوية: حيث استخدمت في وصف خصائص مجتمع الدراسة، وفي تحديد الاستجابة اتجاه محاور أداة الدراسة، وتحسب بالقانون الموالي:

$$\text{التكرار النسبي} = \frac{\text{تكرار المجموعة} \times 100}{\text{المجموع الكلي التكرارات}}$$

2-2- معامل ألفا كرونباخ:[2] تم استخدامه لتحديد معامل ثبات أداة الدراسة، ويعبر عنه بالمعادلة التالية:

$$\boldsymbol{a} = \frac{n}{n-1}\left(1 - \frac{\sum Vi}{Vt}\right)$$

حيث:

- α: هو معامل ألفا كرونباخ، وهو قيمة تتراوح بين 0 و 1؛
- K: هو عدد الأسئلة في أداة الدراسة؛
- Vt: هو التباين في مجموع درجات أداة الدراسة؛
- Vi: هو التباين في درجات كل سؤال في أداة الدراسة.

2-3- المتوسط الحسابي والانحراف المعياري: تم حسابهم لتحديد استجابات أفراد الدراسة نحو محاور وأسئلة أداة الدراسة حيث أن الانحراف المعياري عبارة عن مؤشر إحصائي يقيس مدى التشتت في التغيرات ويعبر عنه بالعلاقة الموالية:

$$\delta = \frac{\sqrt{\sum(Xi - \bar{X})^2}}{N}$$

[1] الحزمة الإحصائية للعلوم الاجتماعية (Statistical package for social science)، عبارة عن حزم حاسوبية متكاملة لإدخال البيانات وتحليلها.

[2] (Cronbachs Alpha) مقياس أو مؤشر الثبات أداة الدراسة والقياس موثوقية الاختبار.

2-4- معامل ارتباط بيرسون: يستخدم معامل ارتباط بيرسون لتحديد مدى ارتباط متغيرات الدراسة ببعضها، وتم حسابه انطلاقا من برنامج الحزمة الإحصائية الاجتماعية "SPSS"

3- مقياس التحليل: تم الاعتماد على مقياس ليكارت الثلاثي لقياس الأبعاد المتعلقة

بانعكاسات الأمن السيبراني على أمن المعلومات في البنوك، حيث يختار المجيب من الأسئلة إجابة واحدة من بين ثلاث بدائل كالتالي:

الجدول رقم (34): يوضح بدائل الأسئلة حسب (مقياس ليكارت الثلاثي)

الدرجة	التقييم
1	لا أوافق
2	محايد
3	أوافق

المصدر: من إعداد الطالبة

الجدول رقم (35): معيار مقياس التحليل

المصدر: من إعداد الطالبة

المتوسط المرجح	(1-1.67)	(1.68-2.34)	(2.35-3)
اتجاه الإجابة	لا أوافق	محايد	موافق

بعد ترميز وتفريغ البيانات باستخدام برنامج **SPSS V28**، سيتم التعامل مع قيم المتوسطات الحسابية التي توصلت إليها الدراسة على النحو التالي:

لتحديد طول خلايا مقياس ليكرت الثلاثي المستخدم في استبانة الدراسة تم حساب المدى: **(أعلى درجة في المقياس - أدنى درجة في المقياس) = (3-1) = 2**، وللحصول على طول الخلية الصحيح

نقوم بقسمة المدى العام على عدد درجات الموافقة وذلك على نحو التالي: $\frac{2}{3} = 0.67$، وبإضافة هذه القيمة في كل مرة للحد الأدنى لدرجة الموافقة نحصل على الحد الأعلى وهكذا مع كل درجات الموافقة، وتفيد هذه العملية في التعرف على موقف مشترك لإجمالي أفراد العينة حيث:

- إذا تراوحت قيمة المتوسط الحسابي المرجح لدرجة الموافقة حول أي عبارة من عبارات الاستبانة بين **[1 – 1.67]** فإن هذا يعني أن درجة الموافقة تمثل **موافقة منخفضة**؛
- إذا تراوحت قيمة المتوسط الحسابي المرجح لدرجة الموافقة حول أي عبارة من عبارات الاستبانة بين **[1.68 – 2.34]** فإن هذا يعني أن درجة الموافقة تمثل **موافقة متوسطة**؛
- إذا تراوحت قيمة المتوسط الحسابي المرجح لدرجة الموافقة حول أي عبارة من عبارات الاستبانة بين **[2.35 – 3]** فإن هذا يعني أن درجة الموافقة تمثل **موافقة عالية**.

3.2. إختبار جاهزية البيانات للتحليل

يدل صدق الدراسة على تحقيق ما هو مطلوب قياسه ومدى استطاعة أداة الدراسة قياسه، فقد تم التأكد من صدق الدراسة من خلال:

- **الصدق الظاهري:** لقد تم التأكد من صدق محتوى الأداة المستخدمة في الدراسة، حيث تم عرضها بعد تطوير الشكل الأولي لها والتأكد من سلامة الصياغة الملحق رقم (01).
- **ثبات الأداة:** هو الاتساق في نتائج الأداة ويقصد به إمكانية الحصول على نفس النتائج لو أعيد استخدام الأداة مرة ثانية. ومن أجل التحقق من اتساق الأداة تم استعمال أداء الاتساق الداخلي (الفاكرونباخ)، حيث كلما كان معامل الفاكرونباخ أكبر من (0.6) كلما دل على وجود اتساق داخلي.

جدول رقم (36): أداة الاتساق الداخلي (الفاكرونباخ)

معامل الثبات الكلي	
عدد العبارات	**39**
الفاكرونباخ	**0.888**

المصدر: من اعداد الطالبة بالاعتماد على ليكرت (Likert Scale)

من خلال الجدول تبين أن معامل الثبات الكلي لأداة جمع البيانات بلغ (0.888) وهو جيد لأنه تجاوز (0.6)، ويدل أن الاستبيان يتمتع بدرجة عالية من الثبات ويمكن الإعتماد عليه في الدراسة التطبيقية.

يعد الإطار المنهجي بمثابة البوصلة لضمان دقة وموضوعية البحث، حيث يحدد الخطوات والأدوات التي سيستخدمها الباحث لجمع وتحليل البيانات، وقد تم تصميمه بعناية فائقة لضمان دقة وموضوعية الدراسة، وتم تحديد عينة الدراسة وأدوات جمع البيانات هي أيضا بعناية، كما تم إختيار الأساليب الإحصائية المناسبة لتحليل البيانات، وأخيرا التأكد من صدق أداة الدراسة من خلال الإختبارات مختلفة.

وبفضل هذا الإطار المنهجي المتين، يمكن جمع وتحليل البيانات بثقة وتحقيق أهداف البحث بكفاءة.

- **اختبار التوزيع الطبيعي لعينة الدراسة:** من أجل تحديد الاختبارات الإحصائية الملائمة للدراسة؛ يتم اعتماد الاختبارات المعلمية في حالة كانت البيانات تتبع التوزيع الطبيعي؛ بينما يتم اعتماد الاختبارات اللامعلمية في حالة كانت البيانات لا تتبع التوزيع الطبيعي.

ويستخدم هذا الاختبار لمعرفة طبيعة توزيع بيانات ظاهرة معينة في كونها تتبع التوزيع الطبيعي (الاعتدالي) من عدمه، وهذا الاختبار ضروري في اختبار الفرضيات، وكذا في اختيار نوعية الأدوات والأساليب الإحصائية التي ستستخدم في الدراسة، ولأن معظم الاختبارات المعلمية تشترط أن يكون توزيع البيانات طبيعيا.

وفي هذه الدراسة تم استخدام اختبار **Kolmogorov-Smirnov** لمعرفة توزيع البيانات، وبالاعتماد على مقارنة قيمة مستوى الدلالة المحسوبة وقيمة مستوى الدلالة المعتمدة في الدراسة 0.05،

فإذا كانت قيمة مستوى الدلالة المحسوبة أقل منها فإن البيانات لا تتبع التوزيع الطبيعي، ويتم الاعتماد على الاختبارات اللامعلمية، والعكس يتم الاعتماد على الاختبارات المعلمية إذا كان مستوى الدلالة المحسوبة أكبر من المعتمدة في الدراسة، والجدول التالي يوضح نتائج اختبار **Kolmogorov-Smirnov**:

جدول رقم (37): نتائج اختبار Kolmogorov-Smirnov

	الأمن السيبراني	أمن المعلومات	نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك
N	28	28	28
Test Statistic	.153	.135	.155
Asymp. Sig. (2-tailed)	.105	.200*	.084

المصدر: من إعداد الطالبة بالاعتماد على مخرجات برنامج SPSS V28.

نلاحظ من الجدول أعلاه أن القيمة الاحتمالية للمحور الأول (الأمن السيبراني) تساوي 0.105 وهي أكبر من مستوى المعنوية المعتمدة في الدراسة 0.05، كذلك يتبين أن القيمة الاحتمالية للمحور الثاني (أمن المعلومات) تساوي *0.200؛ حيث تشير النجمة * إلى الحد الأقصى لمعنوية الاختبار، كما أن القيمة الاحتمالية للمحور الثالث (نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك) تساوي 0.084 وهي أيضا أكبر من مستوى المعنوية المعتمدة في الدراسة 0.05، وبالتالي بيانات الدراسة تتبع التوزيع الطبيعي، مما يسمح باستخدام الاختبارات المعلمية لتحليل البيانات واختبار فرضيات الدراسة.

صدق الاتساق البنائي:

يقيس مدى تحقق الأهداف التي تسعى الأداة الوصول إليها، وهو يبين مدى ارتباط محاور الاستبانة مع الدرجة الكلية للاستبيان، وتم ذلك من خلال حساب معامل الارتباط بيرسون بين درجة كل محور من محاور الاستبانة والدرجة الكلية لها، والجدول التالي يبين المجالات التي تنتمي إليها قيم الارتباط:

جدول رقم (38): المجالات التي تنتمي إليها قيم الارتباط

ارتباط طردي					ارتباط عكسي					
تام	قوي جدا	قوي	متوسط	ضعيف	ضعيف جدا	ضعيف	متوسط	قوي	قوي جدا	تام
+1	+0.9	+0.7	+0.5	+0.3	0	-0.3	-0.5	-0.7	-0.9	-1

Source: EMEN BNYMFAREJ, Data analysis, the statistical economic and social research and training center for Islamic countries (SESRIC) Ankara, Türkiye, 2015, p: 25.

وفيما يلي نتائج الاختبار:

جدول رقم (39): الاتساق البنائي لمحاور الاستبانة

المحاور		المحور الإجمالي
الأمن السيبراني	Pearson Correlation	.715
	Sig. (2-tailed)	.000
	N	28
أمن المعلومات	Pearson Correlation	.824
	Sig. (2-tailed)	.000
	N	28
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	Pearson Correlation	.847
	Sig. (2-tailed)	.000
	N	28

المصدر: من إعداد الطالبة بالاعتماد على مخرجات برنامج SPSS.

بناءً على الجدول أعلاه، يمكننا قراءة النتائج الإحصائية لصدق الاتساق البنائي لمحاور استبانة الدراسة بالشكل التالي:

يمكن ملاحظة أن كلا محوري استبانة الدراسة تتراوح قيم معامل الارتباط بينها وبين الدرجة الكلية للاستبانة بين 0.715 و0.847، وهذا يعني أنها تتمتع بارتباط طردي قوي مع الدرجة الكلية، وبالتالي فهي تقيس ما وضعت لقياسه ولا تقيس شيئا آخر.

وعلى ضوء ما سبق، يمكن القول إن محاور استبانة الدراسة تتمتع بصدق اتساق بنائي مرتفع، وهذا يعني أنها تعبر بشكل جيد عن المتغير الذي تهدف إلى قياسه، وتمثل مجاله النظري بشكل واضح.

اختبار الثبات:

يقصد بثبات الاستبانة، أنه يعطي نفس النتائج لو تمت إعادة توزيع الاستبانة أكثر من مرة، وتحت نفس الظروف والشروط، بمعنى إذا أعيد توزيع الاستبانة بعد فترات زمنية معينة ولأكثر من مرة نجد استقرار النتائج وعدم تغيرها بشكل كبير، وللتحقق من ثبات أداة الدراسة تم اعتماد طريقتين:

طريقة ألفا كرونباخ Alpha Cronbach's: يستخدم معامل الثبات ألفا كرونباخ، للحكم على دقة القياس، بقياس مدي توافق الإجابات مع بعضها البعض، وموثوقية النتائج بأن يعطي المقياس قراءات متقاربة عند تكرار استخدامه في أوقات مختلفة، وأن يكون معامل ألفا كرونباخ يزيد عن القيمة المعيارية (0.7)، والجدول الموالي يوضح نتائج اختبار ألفا كرونباخ:

الجدول رقم (40): نتائج اختبار ألفا كرونباخ لمحاور الدراسة

	عدد العبارات	معامل الثبات
الاستبانة ككل	39	0.888
محور الأمن السيبراني	16	0.825
محور أمن المعلومات	12	0.804
محور نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	11	0.808

المصدر: من إعداد الطالبة بالاعتماد على مخرجات برنامج SPSS.

بناءً على الجدول أعلاه، يمكننا قراءة النتائج الإحصائية لاختبار ألفا كرونباخ لمحاور الدراسة بالشكل التالي:

- **الاستبانة ككل:** هذه الاستبانة تتمتع بثبات عالٍ، حيث أن معامل ألفا كرونباخ لها هو **0.888**، وهو قيمة تفوق القيمة المعيارية (0.7) بكثير. هذا يعني أن الاستبانة تحقق اتساقًا عاليًا بين إجابات المشاركين على مختلف العبارات التي تضمها، وأنها تعطي نتائج موثوقة ودقيقة عند تكرار استخدامها في أوقات مختلفة. وعدد العبارات التي تضمها الاستبانة هو **39** عبارة، وهو عدد كافٍ لتغطية جميع المفاهيم المراد قياسها.
- **محور الأمن السيبراني:** هذا المحور أيضًا يتمتع بثبات عالٍ، حيث أن معامل ألفا كرونباخ له هو **0.825**، وهو قيمة تفوق القيمة المعيارية (0.7) بكثير. هذا يعني أن هذا المحور يحقق اتساقًا عاليًا بين إجابات المشاركين على مختلف العبارات التي يضمها، وأنه يعطي نتائج موثوقة ودقيقة عند تكرار استخدامه في أوقات مختلفة. وعدد العبارات التي يضمها هذا المحور هو **16** عبارة، وهو عدد كافٍ لتغطية جميع المفاهيم المراد قياسها.
- **محور أمن المعلومات:** هذا المحور كذلك يتمتع بثبات عالٍ، حيث أن معامل ألفا كرونباخ له هو **0.804**، وهو قيمة تفوق القيمة المعيارية (0.7) بكثير. هذا يعني أن هذا المحور يحقق اتساقًا عاليًا بين إجابات المشاركين على مختلف العبارات التي يضمها، وأنه يعطي نتائج موثوقة ودقيقة عند تكرار استخدامه في أوقات مختلفة. وعدد العبارات التي يضمها هذا المحور هو **12** عبارة، وهو عدد كافٍ لتغطية جميع المفاهيم المراد قياسها.
- **محور نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك:** هذا المحور كذلك يتمتع بثبات عالٍ، حيث أن معامل ألفا كرونباخ له هو **0.808**، وهو قيمة تفوق القيمة المعيارية (0.7) بكثير. هذا يعني أن هذا المحور يحقق اتساقًا عاليًا بين إجابات المشاركين على مختلف العبارات التي يضمها، وأنه يعطي نتائج موثوقة ودقيقة عند تكرار استخدامه في أوقات مختلفة. وعدد العبارات التي يضمها هذا المحور هو **11** عبارة، وهو عدد كافٍ لتغطية جميع المفاهيم المراد قياسها.

إذًا، يمكن استنتاج أن جميع محاور الدراسة تظهر ثباتًا عاليًا في قياس مفهومها، ولا تخضع لأية تغيرات كبيرة في نتائجها بسبب زمان أو ظروف إجراء الدراسة، وبالتالي فإن هذه الدراسة تتمتع بثبات مرتفع.

3. تحليل نتائج الدراسة وإختبار الفرضيات

في هذا المبحث سوف يتم التطرق إلى النقاط الأساسية المتمثلة في عرض وتحليل أهم نتائج الدراسة والمتمثلة في البيانات الشخصية، وعرض وتحليل محاور الدراسة بالإعتماد على مجموعة من الأساليب الإحصائية التي تم الحصول عليها إعتمادا على نتائج نظام SPSS من البيانات الواردة في الملحق.

1.3. تحليل النتائج المتعلقة بالبيانات الشخصية

في هذا المطلب سوف نقوم بعرض نتائج البيانات الوصفية العامة المتعلقة بالجنس، السن، المنصب الوظيفي، الخبرة المهنية، الشهادة المتحصل عليها، وقد كانت كالتالي:

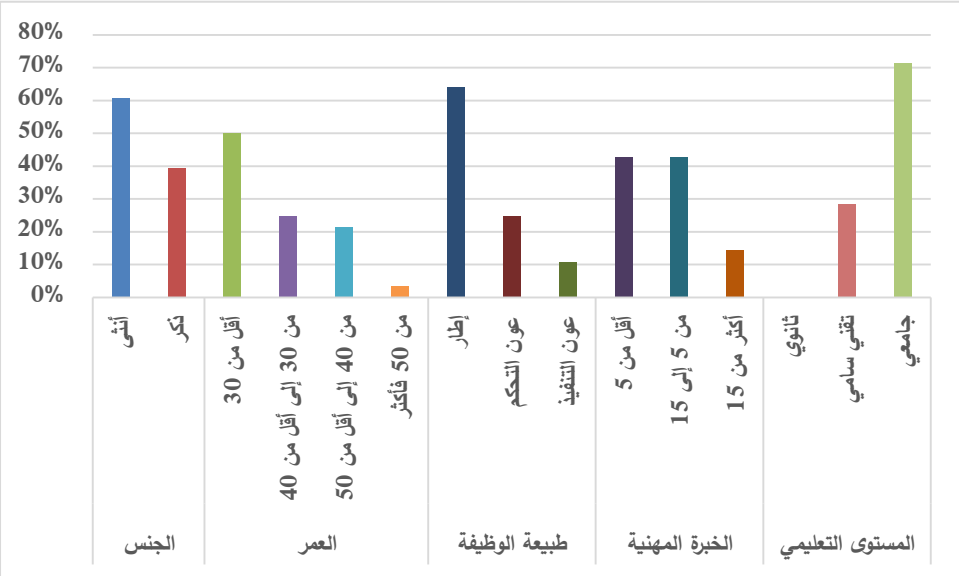
الجدول رقم (41): يبين توزيع عينة الدراسة حسب البيانات الشخصية

		التكرار	النسبة
الجنس	أنثى	17	%60.7
	ذكر	11	%39.3
العمر	أقل من 30	14	%50.0
	من 30 إلى أقل من 40	7	%25.0
	من 40 إلى أقل من 50	6	%21.4
	من 50 فأكثر	1	%3.6
طبيعة الوظيفة	إطار	18	%64.3
	عون التحكم	7	%25.0
	عون التنفيذ	3	%10.7
الخبرة المهنية	أقل من 5	12	%42.9
	من 5 إلى 15	12	%42.9
	أكثر من 15	4	%14.3

المستوى التعليمي	ثانوي	0	%0.0
	تقني سامي	8	%28.6
	جامعي	20	%71.4

المصدر: من إعداد الطالبة بالاعتماد على مخرجات برنامج SPSS.

الشكل رقم (08): يبين توزيع عينة الدراسة حسب البيانات الشخصية



المصدر: من إعداد الطالبة بالاعتماد على مخرجات برنامج SPSS.

من الجدول والشكل أعلاه، نلاحظ ما يلي:

توزيع الجنس في العينة يُظهر تفوقًا للإناث بنسبة **60.7%** مقابل **39.3%** للذكور، مما يعكس تقديرًا للتنوع الجندري ويمكن أن يساهم في تعزيز الإبداع والابتكار من خلال وجهات نظر متنوعة. التوزيع المتوازن نسبيًا بين الجنسين يدل على تنوع جيد في العينة من حيث الجنس، مما يمكن أن يعزز الأداء الجماعي ويوفر توازنًا في وجهات النظر.

فيما يتعلق بالعمر، نجد أن الغالبية العظمى من المشاركين تتراوح أعمارهم بين **أقل من 30** سنة، مما يعكس ميول البنك لتوظيف الأفراد الأصغر سنًا ويشير إلى وجود حيوية وتجدد في القوى العاملة. الفئات العمرية الأخرى مثل **من 30 إلى أقل من 40** ومن **40 إلى أقل من 50** تشير إلى وجود خبرة

مهنية متوسطة ونضج مهني، بينما الفئة العمرية **من 50 فأكثر** تدل على وجود قدر من الحكمة والخبرة الطويلة، رغم قلة تمثيل هذه الفئة.

بالنسبة لطبيعة الوظيفة، نجد أن أغلبية المشاركين هم من الإطارات بنسبة **64.3%**، مما يعكس وجود قيادة وتخطيط استراتيجي، بينما يشير تمثيل **أعوان التحكم** و**أعوان التنفيذ** إلى وجود تنوع في المهارات التقنية والتشغيلية وكفاءة في تنفيذ المهام اليومية.

فيما يخص الخبرة المهنية، نجد توزيعًا متنوعًا، حيث يمتلك الأفراد خبرة تتراوح من **أقل من 5** سنوات إلى **أكثر من 15** سنة. النسب الأعلى تتركز في الفئات التي لديها خبرة من **5 إلى 15** سنة، مما يشير إلى وجود استقرار وظيفي وخبرة مهنية متوسطة، بينما تشير الخبرة الطويلة إلى معرفة عميقة بالمجال.

أخيرًا، المستوى التعليمي للمشاركين يميل إلى مستوى تعليمي أعلى، حيث أن **71.4%** منهم جامعيون و**28.6%** منهم تقنيون سامون، مما يعكس تقديرًا للتعليم العالي والمعرفة المتخصصة. النسبة العالية للأفراد ذوي التعليم الجامعي والدراسات العليا تدل على أن البنك الخارجي في ولاية تبسة يقدر التعليم العالي ويعتمد على مهارات ومعارف متخصصة في عملياته.

2.3. عرض وتحليل النتائج المتعلقة بمتغيرات الدراسة

يوضح هذا المطلب نتائج الدراسة التي سوف يتم عرضها وتحليلها والتي تعتبر كمخرجات لإجابات عينة الدراسة حسب العبارات التي وردت في الاستبيان حيث كانت كالتالي:

1. العبارات المتعلقة بمحور الأمن السيبراني

يتضمن هذا المحور تحليل نتائج الأبعاد التالية: تجميع البيانات وتخزينها، المعالجة التحليلية للبيانات والتنقيب في البيانات، وأيضا القرار، وهذا بالإعتماد على نتائج تحليل" SPSS V28 "، حيث يتضمن هذا المحور16عبارة، وقد تضمن كل من التوزيع النسبي والمتوسطات الحسابية وكذلك الإنحرافات المعيارية للإجابات المتعلقة بعبارات الأمن السيبراني مع تحديد إتجاه كل عبارة.

أولا: تجميع البيانات وتخزينها

يوضح الجدول التالي كل من التوزيع النسبي والمتوسطات الحسابية وكذلك الإنحرافات المعيارية للإجابات المتعلقة بعبارات بعد تجميع البيانات وتخزينها مع تحديد إتجاه كل عبارة.

الجدول (42): المتوسطات الحسابية والانحراف المعياري لفقرات محور الأمن السيبراني

العبارات	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
1. السياسات والإجراءات الأمنية المطبقة في البنك فعالة.	2.29	0.94	4	متوسطة
2. التدريب والوعي الأمني للموظفين في البنك يتم بشكل مستمر وفعّال.	2.46	0.69	2	مرتفعة
3. خطط الاستجابة للحوادث الأمنية محدثة وتُطبق بشكل فوري عند الحاجة.	2.32	0.82	3	متوسطة
4. هناك تعاون ممتاز بين الأقسام المختلفة في البنك لضمان الأمن السيبراني.	2.68	0.55	1	مرتفعة
المتطلبات الإدارية	**2.4375**	**0.58**	/	**مرتفعة**
5. البنك يستخدم أحدث التقنيات لحماية البيانات والمعلومات.	2.36	0.83	4	مرتفعة
6. أنظمة الكشف عن الاختراقات والتصدي لها تعمل بكفاءة عالية.	2.43	0.74	3	مرتفعة
7. نظام التحديثات الأمنية للبرمجيات المستخدمة في البنك فعّال ويتم بانتظام.	2.61	0.63	1	مرتفعة
8. الشبكات والاتصالات البنكية مؤمنة بشكل جيد ضد التهديدات الخارجية.	2.54	0.64	2	مرتفعة
المتطلبات التقنية	**2.4821**	**0.59**	/	**مرتفعة**
9. موظفو البنك لديهم الكفاءة اللازمة للتعامل مع التهديدات الأمنية السيبرانية.	2.11	0.79	4	متوسطة
10. الموظفون الجدد يمتلكون مستوى معرفة أمنية جيد عند التحاقهم بالبنك.	2.32	0.77	3	متوسطة

العبارات	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
11. البنك يضم خبراء أمنيين مؤهلين للتعامل مع الحوادث الأمنية.	2.36	0.83	2	مرتفعة
12. الدورات التدريبية الأمنية المقدمة للموظفين تعزز مهاراتهم الأمنية بشكل فعّال.	2.43	0.84	1	مرتفعة
المتطلبات البشرية	**2.3036**	**0.66**	/	**متوسطة**
13. الأنظمة المادية للرقابة متوفرة وتعمل بكفاءة لحماية مراكز البيانات.	2.25	0.89	1	متوسطة
14. الأجهزة الأمنية مثل الجدران النارية وأنظمة الكشف عن الاختراقات تُصان وتُحدث بشكل دوري.	2.25	0.84	2	متوسطة
15. الإجراءات المتبعة للحفاظ على سلامة البنية التحتية المادية للبنك مُطبقة بشكل صارم.	2.18	0.91	4	متوسطة
16. الأنظمة الأمنية للوصول إلى البنك ومرافقه تضمن أعلى مستويات الأمان.	2.18	0.95	3	متوسطة
المتطلبات المادية	**2.2143**	**0.65**	/	**متوسطة**
الأمن السيبراني	**2.3594**	**0.42**	/	**مرتفعة**

المصدر: من إعداد الطالبة بالاعتماد على مخرجات برنامج SPSS.

من جدول النتائج أعلاه يتضح ما يلي:

بالنسبة للعبارة الأولى، يتضح أن المتوسط الحسابي للآراء حول فعالية السياسات والإجراءات الأمنية المطبقة في البنك هو **2.29** مع انحراف معياري **0.94** وترتيب **4**، ودرجة موافقة **متوسطة**. هذا يشير إلى أن هناك تقييم متوسط لفعالية السياسات والإجراءات الأمنية، مع وجود تباين في الآراء بين الموظفين. يمكن تفسير هذا على أن البنك يمتلك أساسًا جيدًا للأمن السيبراني، لكن قد يكون هناك حاجة لتعزيز هذه السياسات والإجراءات لتحقيق مستوى أعلى من الفعالية.

أما بالنسبة للعبارة الثانية، فالمتوسط الحسابي للآراء حول التدريب والوعي الأمني للموظفين في البنك يتم بشكل مستمر وفعّال هو **2.46** مع انحراف معياري **0.69** وترتيب **2**، ودرجة موافقة **مرتفعة**.

هذا يعني أن هناك تقييم أعلى نسبيًا للتدريب والوعي الأمني، مع وجود توافق أكبر بين الموظفين حول هذا الجانب. يدل ذلك على أن البنك يولي اهتمامًا لتدريب الموظفين ورفع مستوى الوعي الأمني، وهو ما يعتبر عنصرًا مهمًا في تعزيز الأمن السيبراني بشكل عام.

بالنسبة للعبارة 3، يتضح أن المتوسط الحسابي للآراء حول خطط الاستجابة للحوادث الأمنية المحدثة والتي تُطبق بشكل فوري عند الحاجة هو **2.32** مع انحراف معياري **0.82** وترتيب **3**، ودرجة موافقة **متوسطة**. هذا يشير إلى أن هناك تقييم متوسط لفعالية خطط الاستجابة للحوادث الأمنية، مع وجود تباين في الآراء بين الموظفين. يمكن تفسير هذا على أن البنك يمتلك خطط استجابة للحوادث، لكن قد يكون هناك حاجة لتحديثها وتطبيقها بشكل أكثر فعالية وسرعة.

بالنسبة للعبارة 4، يتضح أن المتوسط الحسابي للآراء حول التعاون الممتاز بين الأقسام المختلفة في البنك لضمان الأمن السيبراني هو **2.68** مع انحراف معياري **0.55** وترتيب **1**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي للتعاون بين الأقسام، مما يعكس وجود جهود مشتركة وتنسيق جيد لضمان الأمن السيبراني، وهو أمر حيوي للحفاظ على بيئة عمل آمنة.

المتطلبات الإدارية: المتوسط الحسابي العام لبعد المتطلبات الإدارية يشير إلى تقييم **مرتفع** بمعدل **2.4375**، مما يعكس وجود إجراءات وسياسات أمنية متبعة بشكل فعّال في البنك. هذا يدل على أن البنك يولي اهتمامًا كبيرًا للجوانب الإدارية للأمن السيبراني، مثل التدريب المستمر للموظفين والتعاون بين الأقسام، وهو ما يُعد أساسيًا لتحقيق الأمن السيبراني الشامل.

بالنسبة للعبارة 5، يتضح أن المتوسط الحسابي للآراء حول استخدام البنك لأحدث التقنيات لحماية البيانات والمعلومات هو **2.36** مع انحراف معياري **0.83** وترتيب **4**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم جيد للتقنيات المستخدمة في حماية البيانات، لكن المتوسط الحسابي يدل على أن هناك مجالًا للتحسين. الانحراف المعياري يعني أن تقييمات الموظفين لهذا الجانب قد تختلف، مما يستدعي النظر في كيفية تعزيز الثقة في التقنيات المستخدمة لحماية البيانات والمعلومات.

بالنسبة للعبارة 6، يتضح أن المتوسط الحسابي للآراء حول كفاءة أنظمة الكشف عن الاختراقات والتصدي لها هو **2.43** مع انحراف معياري **0.74** وترتيب **3**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم جيد لأنظمة الكشف عن الاختراقات والتصدي لها، مما يعكس وجود نظام أمني يعمل بكفاءة،

لكن الانحراف المعياري يدل على وجود بعض التباين في الآراء، مما يستدعي النظر في كيفية تحسين هذه الأنظمة لتعزيز الأمان بشكل أكبر.

بالنسبة للعبارة 7، يتضح أن المتوسط الحسابي للآراء حول فعالية نظام التحديثات الأمنية للبرمجيات المستخدمة في البنك هو **2.61** مع انحراف معياري **0.63** وترتيب **1**، ودرجة موافقة **مرتفعة**. هذا يعني أن هناك تقييم إيجابي لنظام التحديثات الأمنية، مما يدل على أن البنك يحرص على تحديث برمجياته بانتظام لمواجهة التهديدات الجديدة، وهو جانب مهم للحفاظ على أمان البيانات.

بالنسبة للعبارة 8، يتضح أن المتوسط الحسابي للآراء حول أمان الشبكات والاتصالات البنكية ضد التهديدات الخارجية هو **2.54** مع انحراف معياري **0.64** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن البنك يتخذ تدابير لحماية شبكاته واتصالاته، وأن هناك تقديرًا جيدًا لهذه التدابير، لكن قد يكون هناك حاجة لمزيد من التحسينات لضمان أعلى مستويات الحماية من التهديدات الخارجية.

المتطلبات التقنية: المتوسط الحسابي العام لبعد المتطلبات التقنية يشير إلى تقييم **مرتفع** بمعدل **2.4821**، مما يعكس استخدام البنك لتقنيات متقدمة وفعّالة في حماية البيانات والمعلومات. هذا يدل على التزام البنك بتطبيق أحدث الحلول التقنية لضمان سلامة الشبكات والاتصالات البنكية، وهو ما يُعد ركيزة مهمة في تحقيق الأمن السيبراني.

بالنسبة للعبارة 9، يتضح أن المتوسط الحسابي للآراء حول كفاءة موظفي البنك في التعامل مع التهديدات الأمنية السيبرانية هو **2.11** مع انحراف معياري **0.79** وترتيب **4**، ودرجة موافقة **متوسطة**. هذا يشير إلى أن هناك تقييم متوسط لكفاءة الموظفين، مما يعكس وجود مجال لتحسين القدرات الأمنية للموظفين ورفع مستوى التدريبات الأمنية لمواجهة التهديدات السيبرانية بشكل أكثر فعالية.

بالنسبة للعبارة 10، يتضح أن المتوسط الحسابي للآراء حول مستوى المعرفة الأمنية للموظفين الجدد عند التحاقهم بالبنك هو **2.32** مع انحراف معياري **0.77** وترتيب **3**، ودرجة موافقة **متوسطة**. هذا يعني أن الموظفين الجدد يمتلكون معرفة أمنية جيدة، لكن قد يكون هناك حاجة لتعزيز برامج التوجيه والتدريب لضمان استعدادهم الكامل للتعامل مع التحديات الأمنية.

بالنسبة للعبارة 11، يتضح أن المتوسط الحسابي للآراء حول تأهيل خبراء البنك الأمنيين للتعامل مع الحوادث الأمنية هو **2.36** مع انحراف معياري **0.83** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يشير

إلى أن هناك تقديرًا جيدًا للخبراء الأمنيين في البنك وقدرتهم على التعامل مع الحوادث الأمنية، مما يعكس وجود فريق مؤهل يمكن الاعتماد عليه في حالات الطوارئ الأمنية.

بالنسبة للعبارة 12، يتضح أن المتوسط الحسابي للآراء حول فعالية الدورات التدريبية الأمنية المقدمة للموظفين في تعزيز مهاراتهم الأمنية هو **2.43** مع انحراف معياري **0.84** وترتيب **1**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي للدورات التدريبية الأمنية، مما يعكس جهود البنك في تطوير قدرات الموظفين الأمنية، وهو أمر مهم للحفاظ على بيئة عمل آمنة.

المتطلبات البشرية: المتوسط الحسابي العام لبعد المتطلبات البشرية يشير إلى تقييم **متوسط** بمعدل **2.3036**، مما يعكس وجود مستوى معرفة وكفاءة متوسط في التعامل مع التهديدات الأمنية بين موظفي البنك. هذا يدل على أهمية تعزيز الكفاءات البشرية من خلال التدريب المستمر وتوظيف خبراء أمنيين مؤهلين، وهو ما يُعد عنصرًا حاسمًا في تحقيق الأمن السيبراني.

بالنسبة للعبارة 13، يتضح أن المتوسط الحسابي للآراء حول كفاءة الأنظمة المادية للرقابة في حماية مراكز البيانات هو **2.25** مع انحراف معياري **0.89** وترتيب **1**، ودرجة موافقة **متوسطة**. هذا يعني أن هناك تقييم متوسط لكفاءة هذه الأنظمة، مما يدل على وجود مجال لتحسين الإجراءات الأمنية المادية لضمان حماية أكثر فعالية لمراكز البيانات.

بالنسبة للعبارة 14، يتضح أن المتوسط الحسابي للآراء حول صيانة وتحديث الأجهزة الأمنية مثل الجدران النارية وأنظمة الكشف عن الاختراقات هو **2.25** مع انحراف معياري **0.84** وترتيب **2**، ودرجة موافقة **متوسطة**. هذا يشير إلى أن البنك يعتني بصيانة وتحديث أجهزته الأمنية، لكن الانحراف المعياري يدل على وجود تباين في الآراء، مما يستدعي النظر في كيفية تحسين دورية الصيانة والتحديث لتعزيز الأمان.

بالنسبة للعبارة 15، يتضح أن المتوسط الحسابي للآراء حول الإجراءات المتبعة للحفاظ على سلامة البنية التحتية المادية للبنك هو **2.18** مع انحراف معياري **0.91** وترتيب **4**، ودرجة موافقة **متوسطة**. هذا يشير إلى أن هناك تقييم متوسط للإجراءات المتبعة، مما يعكس وجود مجال لتحسين وتشديد الإجراءات لضمان حماية أفضل للبنية التحتية المادية للبنك.

بالنسبة للعبارة 16، يتضح أن المتوسط الحسابي للآراء حول الأنظمة الأمنية للوصول إلى البنك ومرافقه لضمان أعلى مستويات الأمان هو **2.18** مع انحراف معياري **0.95** وترتيب **3**، ودرجة موافقة **متوسطة**. هذا يعني أن الأنظمة الأمنية للوصول تُقيّم بأنها توفر مستوى متوسط من الأمان، مع وجود تباين كبير في الآراء، مما يستدعي النظر في كيفية تعزيز هذه الأنظمة لتوفير أمان أكثر شمولية وفعالية.

المتطلبات المادية: المتوسط الحسابي العام لبعد المتطلبات المادية يشير إلى تقييم **متوسط** بمعدل **2.2143**، مما يعكس وجود تدابير أمنية مادية متوسطة الفعالية في حماية مراكز البيانات والبنية التحتية للبنك. هذا يدل على ضرورة تحسين الأنظمة المادية للرقابة والصيانة الدورية للأجهزة الأمنية لتعزيز الأمن السيبراني.

الأمن السيبراني: المتوسط الحسابي العام لمحور متطلبات الأمن السيبراني يشير إلى تقييم **مرتفع** بمعدل **2.3594**، مما يعكس وجود استراتيجية شاملة وفعّالة للأمن السيبراني في البنك. هذا يدل على أن البنك يحقق مستوى جيد من الأمن السيبراني، مع التأكيد على أهمية الاستمرار في تطوير وتحسين جميع جوانب الأمن السيبراني لضمان حماية شاملة ومتكاملة.

02- العبارات المتعلقة بمحور أمن المعلومات

يتضمن هذا المحور تحليل نتائج الأبعاد التالية: إستمرارية توفر المعلومات، سلامة المحتوى وإكتماله، سرية المعلومات وموثوقيتها وأيضا الخصوصية، وهذا بالإعتماد على نتائج تحليل" SPSS V28 "، حيث يتضمن هذا المحور12عبارة، وقد تضمن كل من التوزيع النسبي والمتوسطات الحسابية وكذلك الإنحرافات المعيارية للإجابات المتعلقة بعبارة أمن المعلومات مع تحديد إتجاه كل عبارة.

الجدول (43): المتوسطات الحسابية والانحراف المعياري لفقرات محور أمن المعلومات

العبارات	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
17. المعلومات متاحة ويمكن الوصول إليها بشكل مستمر دون انقطاع.	2.43	0.74	2	مرتفعة

العبارات	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
18. أنظمة النسخ الاحتياطي والاسترجاع تعمل بكفاءة لضمان استمرارية المعلومات.	2.43	0.74	2	مرتفعة
19. الإجراءات المتبعة لضمان توفر المعلومات في حالات الطوارئ مُطبقة بشكل فعّال.	2.46	0.74	1	مرتفعة
استمرارية توفر المعلومات	**2.4405**	**0.60**	/	**مرتفعة**
20. يحافظ البنك على سلامة واكتمال المحتوى المخزن والمعالج فيه.	2.57	0.57	1	مرتفعة
21. الإجراءات الأمنية تضمن عدم تعرض المحتوى للتلف أو التغيير غير المصرح به.	2.54	0.74	2	مرتفعة
22. التحقق من صحة المعلومات وتحديثها يتم بانتظام لضمان دقتها واكتمالها.	2.54	0.74	2	مرتفعة
سلامة المحتوى واكتماله	**2.5476**	**0.57**	/	**مرتفعة**
23. المعلومات الحساسة محمية بإجراءات أمنية صارمة لضمان سريتها.	2.64	0.73	1	مرتفعة
24. الوصول إلى المعلومات مقيد بمستويات تصريح محددة لضمان موثوقيتها.	2.54	0.64	3	مرتفعة
25. التدابير المتخذة لحماية المعلومات من الاختراق تُطبق بشكل مستمر وفعّال.	2.54	0.74	2	مرتفعة
سرية المعلومات وموثوقيتها	**2.5714**	**0.49**	/	**مرتفعة**
26. بيانات العملاء محمية بإجراءات خصوصية تضمن عدم الكشف عنها بشكل غير مصرح.	2.43	0.79	3	مرتفعة
27. السياسات المتعلقة بخصوصية البيانات مُحدثة وتُطبق بشكل صارم.	2.46	0.79	2	مرتفعة
28. التزام البنك بقوانين الخصوصية يضمن حماية معلومات العملاء بشكل كامل.	2.71	0.60	1	مرتفعة
الخصوصية	**2.5357**	**0.59**	/	**مرتفعة**
أمن المعلومات	**2.5238**	**0.40**	/	**مرتفعة**

المصدر: من إعداد الطالبة بالاعتماد على مخرجات برنامج SPSS.

من جدول النتائج أعلاه يتضح ما يلي:

بالنسبة للعبارة 17، يتضح أن المتوسط الحسابي للآراء حول استمرارية توفر المعلومات وإمكانية الوصول إليها دون انقطاع هو **2.43** مع انحراف معياري **0.74** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي لتوفر المعلومات بشكل مستمر، مما يعكس التزام البنك بضمان الوصول الدائم إلى المعلومات، وهو جانب حيوي لاستمرارية الأعمال والخدمات.

بالنسبة للعبارة 18، يتضح أن المتوسط الحسابي للآراء حول كفاءة أنظمة النسخ الاحتياطي والاسترجاع في البنك هو **2.43** مع انحراف معياري **0.74** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يعني أن البنك يتخذ تدابير مستمرة وفعّالة لضمان استمرارية المعلومات، وهو ما يعتبر عنصرًا مهمًا في تعزيز أمن المعلومات وحمايتها من الفقدان.

بالنسبة للعبارة 19، يتضح أن المتوسط الحسابي للآراء حول فعالية الإجراءات المتبعة لضمان توفر المعلومات في حالات الطوارئ هو **2.46** مع انحراف معياري **0.74** وترتيب **1**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن البنك يتخذ إجراءات مدروسة وفعّالة لضمان توفر المعلومات حتى في الظروف الطارئة، مما يؤكد على قوة البنك في إدارة المخاطر والحفاظ على استمرارية العمليات البنكية.

استمرارية توفر المعلومات: يُظهر المتوسط الحسابي العام لآراء الموظفين حول بعد استمرارية توفر المعلومات، الذي يعكس العبارات من 17 إلى 19، أنه **2.4405** مع انحراف معياري **0.60**، مما يشير إلى تقييم **مرتفع** لفعالية الإجراءات المتبعة لضمان توفر المعلومات بشكل مستمر. هذا يعكس التزام البنك بتوفير المعلومات بشكل دائم وفعّال، مما يُعد عنصرًا أساسيًا في الحفاظ على سير العمليات البنكية بلا انقطاع.

بالنسبة للعبارة 20، يتضح أن المتوسط الحسابي للآراء حول حفاظ البنك على سلامة واكتمال المحتوى المخزن والمعالج فيه هو **2.57** مع انحراف معياري **0.57** وترتيب **1**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي للإجراءات التي يتخذها البنك لحماية المحتوى، مما يعكس جهود البنك في ضمان سلامة واكتمال المعلومات المخزنة والمعالجة.

بالنسبة للعبارة 21، يتضح أن المتوسط الحسابي للآراء حول الإجراءات الأمنية التي تضمن عدم تعرض المحتوى للتلف أو التغيير غير المصرح به هو **2.54** مع انحراف معياري **0.74** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يعني أن البنك يتخذ تدابير أمنية موثوقة لحماية المحتوى، مما يساهم في الحفاظ على سلامة واكتمال المعلومات.

بالنسبة للعبارة 22، يتضح أن المتوسط الحسابي للآراء حول التحقق من صحة المعلومات وتحديثها بانتظام لضمان دقتها واكتمالها هو **2.54** مع انحراف معياري **0.74** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن البنك يولي اهتمامًا كبيرًا للتحقق من صحة المعلومات وتحديثها، مما يضمن دقتها واكتمالها، وهو جانب مهم للحفاظ على جودة المعلومات.

سلامة المحتوى واكتماله: يُظهر المتوسط الحسابي العام لآراء الموظفين حول بعد سلامة المحتوى واكتماله، الذي يعكس العبارات من 20 إلى 22، أنه **2.5476** مع انحراف معياري **0.57**، مما يشير إلى تقييم **مرتفع** لفعالية الإجراءات الأمنية المتبعة لحماية المحتوى. هذا يعكس الجهود المبذولة لحماية المحتوى من أي تلف أو تغيير غير مصرح به، مما يُعد ضروريًا للحفاظ على جودة ودقة المعلومات.

بالنسبة للعبارة 23، يتضح أن المتوسط الحسابي للآراء حول حماية المعلومات الحساسة بإجراءات أمنية صارمة لضمان سريتها هو **2.64** مع انحراف معياري **0.73** وترتيب **1**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي للإجراءات الأمنية المتخذة لحماية المعلومات الحساسة، مما يعكس التزام البنك بسرية المعلومات ويؤكد على فعالية الإجراءات المتبعة لضمان هذه السرية.

بالنسبة للعبارة 24، يتضح أن المتوسط الحسابي للآراء حول تقييد الوصول إلى المعلومات بمستويات تصريح محددة لضمان موثوقيتها هو **2.54** مع انحراف معياري **0.64** وترتيب **3**، ودرجة موافقة **مرتفعة**. هذا يعني أن البنك يطبق سياسات تقييد الوصول بفعالية، مما يساهم في حماية المعلومات ويضمن موثوقيتها، وهو جانب مهم للحفاظ على سرية وأمان المعلومات.

بالنسبة للعبارة 25، يتضح أن المتوسط الحسابي للآراء حول التدابير المتخذة لحماية المعلومات من الاختراق وتطبيقها بشكل مستمر وفعّال هو **2.54** مع انحراف معياري **0.74** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن البنك يتخذ تدابير مستمرة وفعّالة لحماية المعلومات من أي اختراقات، مما يدل على وجود نظام أمني قوي يحمي المعلومات من التهديدات السيبرانية.

سرية المعلومات وموثوقيتها: يُظهر المتوسط الحسابي العام لآراء الموظفين حول بعد سرية المعلومات وموثوقيتها، الذي يعكس العبارات من 23 إلى 25، أنه **2.5714** مع انحراف معياري **0.49**، مما يشير إلى تقييم **مرتفع** لفعالية الإجراءات المتبعة لضمان سرية المعلومات. هذا يعكس التدابير الصارمة المتخذة لضمان أن المعلومات تظل سرية وموثوقة، مما يُعد حيويًا للحفاظ على ثقة العملاء وسلامة النظام البنكي.

بالنسبة للعبارة 26، يتضح أن المتوسط الحسابي للآراء حول حماية بيانات العملاء بإجراءات خصوصية لضمان عدم الكشف عنها بشكل غير مصرح هو **2.43** مع انحراف معياري **0.79** وترتيب **3**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن البنك يتخذ تدابير لحماية خصوصية بيانات العملاء، مما يعكس التزامه بضمان الخصوصية وحماية البيانات من الكشف غير المصرح به.

بالنسبة للعبارة 27، يتضح أن المتوسط الحسابي للآراء حول تحديث وتطبيق السياسات المتعلقة بخصوصية البيانات بشكل صارم هو **2.46** مع انحراف معياري **0.79** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يعني أن البنك يحافظ على تحديث سياسات الخصوصية ويطبقها بصرامة، مما يضمن الحفاظ على خصوصية بيانات العملاء وحمايتها بشكل فعّال.

بالنسبة للعبارة 28، يتضح أن المتوسط الحسابي للآراء حول التزام البنك بقوانين الخصوصية لضمان حماية معلومات العملاء بشكل كامل هو **2.71** مع انحراف معياري **0.60** وترتيب **1**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي لالتزام البنك بقوانين الخصوصية، مما يؤكد على قوة البنك في حماية معلومات العملاء وضمان خصوصيتهم بما يتوافق مع القوانين والتنظيمات.

الخصوصية: يُظهر المتوسط الحسابي العام لآراء الموظفين حول بعد الخصوصية، الذي يعكس العبارات من 26 إلى 28، أنه **2.5357** مع انحراف معياري **0.59**، مما يشير إلى تقييم **مرتفع** لفعالية الإجراءات المتبعة لضمان خصوصية البيانات. هذا يعكس الالتزام القوي بسياسات الخصوصية والتدابير المتبعة لضمان عدم الكشف عن بيانات العملاء بشكل غير مصرح به، مما يُعد أساسيًا للحفاظ على الثقة والأمان في البيئة البنكية.

أمن المعلومات: يُظهر المتوسط الحسابي العام لآراء الموظفين حول بعد أمن المعلومات أنه **2.5238** مع انحراف معياري **0.40**، مما يشير إلى تقييم **مرتفع** بشكل عام لأمن المعلومات في البنك.

هذا يعني أن البنك يحقق مستوى جيد من الحماية للمعلومات، مع التأكيد على أهمية الاستمرار في تطوير وتحسين جميع عناصر أو جوانب أمن المعلومات لضمان حماية شاملة ومتكاملة.

03- العبارات المتعلقة بمحور نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة أمن المعلومات وأداء البنك

يتضمن هذا المحور تحليل نتائج العبارات المتعلقة بمحور نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة أمن المعلومات وأداء البنك، وهذا بالإعتماد على نتائج تحليل" SPSS29.0.10 "، حيث يتضمن هذا المحور 11عبارة وقد تضمن الجدول كل من التوزيع النسبي والمتوسطات الحسابية وكذلك الإنحرافات المعيارية للإجابات.

الجدول (44): المتوسطات الحسابية والانحراف المعياري لفقرات محور نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك

العبارات	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الموافقة
29. تطبيق الأمن السيبراني يعزز من سلامة المعلومات البنكية.	2.64	0.62	3	مرتفعة
30. الاهتمام بالأمن السيبراني يقلل من حوادث الاختراقات الأمنية.	2.61	0.69	4	مرتفعة
31. الإجراءات الأمنية السيبرانية تحافظ على خصوصية بيانات العملاء.	2.64	0.68	2	مرتفعة
32. تحسن أداء البنك نتيجة لتطبيق معايير الأمن السيبراني.	2.46	0.84	7	مرتفعة
33. التدريبات الأمنية تساهم في رفع كفاءة الموظفين في التعامل مع التهديدات السيبرانية.	2.46	0.84	7	مرتفعة
34. الاستثمار في الأمن السيبراني يقود إلى تحسين الثقة بين البنك وعملائه.	2.61	0.69	4	مرتفعة

35. الأمن السيبراني يدعم استمرارية الأعمال ويقلل من فترات التوقف.	2.61	0.69	4	مرتفعة
36. التزام البنك بالأمن السيبراني يعزز من موقعه التنافسي في السوق.	2.43	0.74	9	مرتفعة
37. الأمن السيبراني يساعد في الحفاظ على سمعة البنك ومصداقيته.	2.39	0.79	10	مرتفعة
38. التقنيات الأمنية الحديثة تساهم في كشف التهديدات السيبرانية بشكل مبكر.	2.32	0.91	11	متوسطة
39. الأمن السيبراني يقلل من المخاطر المالية المرتبطة بالهجمات الإلكترونية.	2.68	0.67	1	مرتفعة
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	**2.5325**	**0.44**	/	**مرتفعة**

المصدر: من إعداد الطالبة بالاعتماد على مخرجات برنامج SPSS.

من جدول النتائج أعلاه يتضح ما يلي:

بالنسبة للعبارة 29، يتضح أن المتوسط الحسابي للآراء حول تعزيز تطبيق الأمن السيبراني لسلامة المعلومات البنكية هو **2.64** مع انحراف معياري **0.62** وترتيب **3**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي لتأثير الأمن السيبراني على سلامة المعلومات، مما يعكس الاعتقاد بأن الإجراءات الأمنية السيبرانية تسهم بشكل فعّال في حماية المعلومات البنكية.

بالنسبة للعبارة 30، يتضح أن المتوسط الحسابي للآراء حول تقليل الاهتمام بالأمن السيبراني لحوادث الاختراقات الأمنية هو **2.61** مع انحراف معياري **0.69** وترتيب **4**، ودرجة موافقة **مرتفعة**. هذا يعني أن هناك تقديرًا جيدًا لدور الأمن السيبراني في الحد من الحوادث الأمنية، مما يدل على أهمية الاستثمار في الأمن السيبراني لتقليل المخاطر الأمنية.

بالنسبة للعبارة 31، يتضح أن المتوسط الحسابي للآراء حول حفاظ الإجراءات الأمنية السيبرانية على خصوصية بيانات العملاء هو **2.64** مع انحراف معياري **0.68** وترتيب **2**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن الإجراءات الأمنية السيبرانية تُقيّم بأنها فعّالة في حماية خصوصية بيانات العملاء، مما يعزز الثقة في البنك ويساهم في حماية سمعته ومصداقيته.

بالنسبة للعبارة 32، يتضح أن المتوسط الحسابي للآراء حول تحسين أداء البنك نتيجة لتطبيق معايير الأمن السيبراني هو **2.46** مع انحراف معياري **0.84** وترتيب **7**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي لتأثير الأمن السيبراني على أداء البنك، مما يعكس الاعتقاد بأن الإجراءات الأمنية تسهم في تحسين الكفاءة والفعالية العامة للبنك.

بالنسبة للعبارة 33، يتضح أن المتوسط الحسابي للآراء حول مساهمة التدريبات الأمنية في رفع كفاءة الموظفين في التعامل مع التهديدات السيبرانية هو **2.46** مع انحراف معياري **0.84** وترتيب **7**، ودرجة موافقة **مرتفعة**. هذا يعني أن التدريبات الأمنية تُقيّم بأنها فعّالة في تعزيز قدرات الموظفين، مما يساهم في تقوية الدفاعات الأمنية للبنك ضد التهديدات السيبرانية.

بالنسبة للعبارة 34، يتضح أن المتوسط الحسابي للآراء حول قيادة الاستثمار في الأمن السيبراني إلى تحسين الثقة بين البنك وعملائه هو **2.61** مع انحراف معياري **0.69** وترتيب **4**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقديرًا جيدًا لأهمية الاستثمار في الأمن السيبراني وتأثيره الإيجابي على بناء الثقة مع العملاء، مما يعزز العلاقة بين البنك وعملائه ويساهم في تحقيق ميزة تنافسية.

بالنسبة للعبارة 35، يتضح أن المتوسط الحسابي للآراء حول دعم الأمن السيبراني لاستمرارية الأعمال وتقليله لفترات التوقف هو **2.61** مع انحراف معياري **0.69** وترتيب **4**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن هناك تقييم إيجابي لتأثير الأمن السيبراني على استمرارية الأعمال، مما يعكس الاعتقاد بأن الإجراءات الأمنية تسهم في تقليل الانقطاعات وتعزيز الكفاءة التشغيلية للبنك.

بالنسبة للعبارة 36، يتضح أن المتوسط الحسابي للآراء حول تعزيز التزام البنك بالأمن السيبراني لموقعه التنافسي في السوق هو **2.43** مع انحراف معياري **0.74** وترتيب **9**، ودرجة موافقة **مرتفعة**. هذا يعني أن هناك تقديرًا جيدًا لأهمية الأمن السيبراني في تحسين الموقع التنافسي للبنك، مما يدل على أن الاستثمار في الأمن السيبراني يُنظر إليه كعامل مهم للتميز في السوق.

بالنسبة للعبارة 37، يتضح أن المتوسط الحسابي للآراء حول مساعدة الأمن السيبراني في الحفاظ على سمعة البنك ومصداقيته هو **2.39** مع انحراف معياري **0.79** وترتيب **10**، ودرجة موافقة **مرتفعة**. هذا يشير إلى أن الأمن السيبراني يُقيّم بأنه يلعب دورًا مهمًا في حماية سمعة البنك والحفاظ على مصداقيته، مما يؤكد على أهمية الإجراءات الأمنية في بناء الثقة مع العملاء والشركاء.

بالنسبة للعبارة 38، يتضح أن المتوسط الحسابي للآراء حول مساهمة التقنيات الأمنية الحديثة في كشف التهديدات السيبرانية بشكل مبكر هو **2.32** مع انحراف معياري **0.91** وترتيب **11**، ودرجة موافقة **متوسطة**. هذا يشير إلى أن هناك تقييم متوسط لفعالية التقنيات الأمنية الحديثة في الكشف المبكر عن التهديدات، مما يعكس وجود مجال لتحسين وتطوير هذه التقنيات لتعزيز القدرة على الاستجابة السريعة للتهديدات السيبرانية.

بالنسبة للعبارة 39، يتضح أن المتوسط الحسابي للآراء حول تقليل الأمن السيبراني للمخاطر المالية المرتبطة بالهجمات الإلكترونية هو **2.68** مع انحراف معياري **0.67** وترتيب **1**، ودرجة موافقة **مرتفعة**. هذا يعني أن هناك تقييم إيجابي لدور الأمن السيبراني في تقليل المخاطر المالية، مما يدل على أهمية الإجراءات الأمنية في حماية البنك من الخسائر المالية التي قد تنجم عن الهجمات الإلكترونية.

بناءً على النتائج المقدمة للمحور الثالث، الذي يتناول نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك، يُظهر المتوسط الحسابي العام أنه **2.5325** مع انحراف معياري **0.44**. هذا يشير إلى تقييم **مرتفع** من قبل الموظفين لتأثير الأمن السيبراني على البنك.

التقييم المرتفع يعكس إدراك الموظفين للفوائد الكبيرة التي يجلبها الأمن السيبراني، بما في ذلك تعزيز سلامة المعلومات البنكية، تقليل حوادث الاختراقات الأمنية، والحفاظ على خصوصية بيانات العملاء. كما يُعتبر دليلاً على أن الاستثمار في الأمن السيبراني يُسهم في تحسين الثقة بين البنك وعملائه، ويدعم استمرارية الأعمال ويقلل من فترات التوقف، مما يعزز من موقع البنك التنافسي في السوق ويساعد في الحفاظ على سمعته ومصداقيته.

بشكل عام، تُظهر النتائج أن الأمن السيبراني يُعتبر عاملاً مهمًا في تحقيق الأداء الفعّال للبنك ويُساهم بشكل ملحوظ في تقليل المخاطر المالية المرتبطة بالهجمات الإلكترونية. هذه النتائج تُؤكد على أهمية الأمن السيبراني كجزء لا يتجزأ من استراتيجية البنك الشاملة للأمن والحماية.

3.3 إختبار فرضيات الدراسة

بهدف إختبار الفرضيات تم إستخدام الأسلوب الاحصائي "معامل بيرسون" حيث تتمثل قاعدة القرار بقبول أو رفض فرضيات الدراسة.

01- نتائج إختبار الفرضية الأولى: حيث تنص الفرضية الأولى على ما يلي:

H_0: لا يوافق موظفو البنك الخارجي لولاية تبسة على توفر متطلبات الأمن السيبراني فيه عند مستوى دلالة $\alpha = 0.05$.

H_1: يوافق موظفو البنك الخارجي لولاية تبسة على توفر متطلبات الأمن السيبراني فيه عند مستوى دلالة$\alpha = 0.05$.

وللإجابة عن الفرضية السابقة تم استخدام اختبار one sample T-Test، وكانت نتائج الاختبار كالآتي:

الجدول رقم (45): جدول نتائج اختبار one sample T-Test بالنسبة للفرضية الأولى

	N	Mean	Std. Deviation	Std. Error Mean
الأمن السيبراني	28	2.3594	.41896	.07918

		Standardizer[a]	Point Estimate	Confidence %95 Interval	
				Lower	Upper
الأمن	Cohen's d	.41896	.858	.417	1.287

	Test Value = 2						
	t	Df	Significance One-Sided p	Significance Two-Sided p	Mean Difference	95% Confidence Interval of the Difference Lower	95% Confidence Interval of the Difference Upper
الأمن السيبراني	4.539	27	.000	.000	.35938	.1969	.5218

السيبراني	Hedges' correction	.43107	.834	.405	1.251

المصدر: من إعداد الطالبة إعتمادا على نتائج نظام SPSS من البيانات الواردة في الملحق

من خلال الجداول أعلاه يتضح ما يلي:

متوسط درجة الموافقة قدره **2.3594** ويقع ضمن النطاق **[2.35 – 3]**، مما يشير إلى موافقة عالية من قبل الموظفين على توفر متطلبات الأمن السيبراني.

ولتقييم دلالة هذه النتائج إحصائيًا، تم إجراء **اختبار t للعينة الواحدة**، حيث بلغت قيمة t **4.539**، وكانت قيمة p للجانبين **0.000**، هذه القيم تدل على وجود فرق ذو دلالة إحصائية بين متوسط الدرجة والقيمة المرجعية المحددة مسبقًا (التي هي 2)، وذلك عند مستوى معنوية **0.05** وعليه، يمكن رفض الفرضية الصفرية التي تفترض عدم وجود موافقة معنوية، وقبول الفرضية البديلة التي تؤكد موافقة الموظفين على توفر متطلبات الأمن السيبراني في البنك.

من الجدير بالذكر أن **فاصل الثقة** للفرق بين متوسط الدرجة والقيمة المرجعية يتراوح بين **.1969** و**.5218**، مما يعزز الثقة في استقرار هذه النتيجة عبر عينات مختلفة ويؤكد على دلالتها الإحصائية.

أخيرًا، يشير **حجم التأثير** المقاس بواسطة **Cohen's d** و**Hedges' correction** إلى أن الفرق بين متوسط الدرجة والقيمة المرجعية له أهمية عملية ومعنوية كبيرة، حيث أن قيمة **Cohen's d** هي **.858** وقيمة **Hedges' correction** هي **.834**، مما يدل على أن الأمن السيبراني يُعتبر متطلبًا مهمًا في البنك الخارجي لولاية تبسة وفقًا لتقييم موظفي البنك.

بناءً على ما سبق، يمكن الاستنتاج بأن الفرضية الأولى قد تم تأكيدها بشكل قوي من خلال البيانات المجمعة والتحليل الإحصائي، مما يعكس مدى الاهتمام والوعي بأهمية الأمن السيبراني في البنك الخارجي لولاية تبسة.

02- نتائج إختبار الفرضية الثانية: حيث تنص الفرضية الثانية على ما يلي:

تنص الفرضية الثانية على ما يلي:

H_0: لا يوافق موظفو البنك الخارجي لولاية تبسة على توفر عناصر أمن المعلومات فيه عند مستوى دلالة $\alpha = 0.05$.

H_1: يوافق موظفو البنك الخارجي لولاية تبسة على توفر عناصر أمن المعلومات فيه عند مستوى دلالة $\alpha = 0.05$.

وللإجابة عن الفرضية السابقة تم استخدام اختبار one sample T-Test، وكانت نتائج الاختبار كالآتي:

الجدول رقم (46): جدول نتائج اختبار one sample T-Test بالنسبة للفرضية الثانية

	N	Mean	Std. Deviation	Std. Error Mean
أمن المعلومات	28	2.5238	40436.	07642.

	Test Value = 2						
			Significance			95% Confidence Interval of the Difference	
	t	df	One-Sided p	Two-Sided p	Mean Difference	Lower	Upper
أمن المعلومات	6.855	27	.000	.000	.52381	.3670	.6806

				Confidence %95 Interval	
		Standardizer[a]	Point Estimate	Lower	Upper
أمن	Cohen's d	.40436	1.295	.783	1.794

1.744	.761	1.259	.41604	Hedges' correction	**المعلومات**

المصدر: من إعداد الطالبة إعتمادا على نتائج نظام SPSS من البيانات الواردة في الملحق

من خلال الجداول أعلاه يتضح ما يلي:

متوسط درجة الموافقة قدره **2.5238** والذي يقع ضمن النطاق **[2.35 – 3]**، مما يشير إلى تأكيد الموظفين على توفر عناصر أمن المعلومات بشكل جيد في البنك.

ولتحديد ما إذا كانت هذه النتائج تحمل دلالة إحصائية، تم إجراء **اختبار t للعينة الواحدة**، والذي أسفر عن قيمة t تبلغ **6.855**، وقيم p للجانبين تساوي **0.000**، هذه القيم تدل على وجود فرق ذو دلالة إحصائية بين متوسط الدرجة والقيمة المرجعية (التي هي 2)، وذلك عند مستوى معنوية **0.05**. وبالتالي، يمكن رفض الفرضية الصفرية التي تفترض عدم وجود موافقة معنوية، وقبول الفرضية البديلة التي تؤكد على توفر عناصر أمن المعلومات في البنك.

من النقاط البارزة في التحليل **فاصل الثقة** للفرق بين متوسط الدرجة والقيمة المرجعية، الذي يتراوح بين **3670. و6806.**، ويعزز هذا الفاصل الثقة في استقرار النتيجة عبر عينات مختلفة ويؤكد على دلالتها الإحصائية.

بالإضافة إلى ذلك، يشير **حجم التأثير** المقاس بواسطة **Cohen's d** و**Hedges' correction** إلى أن الفرق بين متوسط الدرجة والقيمة المرجعية له أهمية عملية ومعنوية كبيرة، حيث أن قيمة **Cohen's d** هي **1.295** وقيمة **Hedges' correction** هي **1.259**، مما يدل على أن تأثير توفر عناصر أمن المعلومات في البنك مهم وملموس.

وفقًا للتحليل الإحصائي المفصل، يمكن الاستنتاج بأن الفرضية الثانية قد تم تأكيدها بقوة، مما يعكس التزام البنك الخارجي لولاية تبسة بأمن المعلومات ويبرز الجهود المبذولة لضمان حماية البيانات والمعلومات بشكل فعال.

نتائج اختبار الفرضية الرئيسية:

حيث تنص الفرضية على ما يلي:

H_0: لا يدرك موظفو البنك الخارجي لولاية تبسة نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك عند مستوى دلالة $\alpha = 0.05$.

H_1: يدرك موظفو البنك الخارجي لولاية تبسة نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك عند مستوى دلالة $\alpha = 0.05$.

وللإجابة عن الفرضية السابقة تم استخدام اختبار one sample T-Test، وكانت نتائج الاختبار كالآتي:

الجدول رقم (47): جدول نتائج اختبار one sample T-Test بالنسبة للفرضية الرئيسية

	N	Mean	Std. Deviation	Std. Error Mean
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	28	2.5238	40436.	07642.

	Test Value = 2						
			Significance			95% Confidence Interval of the Difference	
	T	Df	One-Sided p	Two-Sided p	Mean Difference	Lower	Upper
نتائج الاهتمام بتطبيق الأمن	6.855	27	.000	.000	.52381	.3670	.6806

السيبراني على سلامة المعلومات وأداء البنك							

		Standardizer[a]	Point Estimate	%95 Confidence Interval	
				Lower	Upper
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	Cohen's d	.40436	1.295	.783	1.794
	Hedges' correction	.41604	1.259	.761	1.744

المصدر: من إعداد الطالبة إعتمادا على نتائج نظام SPSS من البيانات الواردة في الملحق

من خلال الجداول أعلاه يتضح ما يلي:

متوسط درجة الموافقة قدره **2.5325** والذي يقع ضمن النطاق **[2.35 – 3]**، مما يشير إلى إدراك الموظفين لأهمية الأمن السيبراني في حماية المعلومات وتعزيز أداء البنك.

لتحديد ما إذا كانت هذه النتائج تحمل دلالة إحصائية، تم إجراء **اختبار t للعينة الواحدة**، والذي أسفر عن قيمة t تبلغ **6.471**، وقيم p للجانبين تساوي **0.000**، هذه القيم تدل على وجود فرق ذو دلالة إحصائية بين متوسط الدرجة والقيمة المرجعية (التي هي 2)، وذلك عند مستوى معنوية **0.05**. وبالتالي، يمكن رفض الفرضية الصفرية التي تفترض عدم وجود إدراك معنوي، وقبول الفرضية البديلة التي تؤكد على إدراك الموظفين لنتائج الأمن السيبراني على سلامة المعلومات وأداء البنك.

من النقاط البارزة في التحليل **فاصل الثقة** للفرق بين متوسط الدرجة والقيمة المرجعية، الذي يتراوح بين **3636. و7013.**، ويعزز هذا الفاصل الثقة في استقرار النتيجة عبر عينات مختلفة ويؤكد على دلالتها الإحصائية.

بالإضافة إلى ذلك، يشير **حجم التأثير** المقاس بواسطة **Cohen's d** و**Hedges' correction** إلى أن الفرق بين متوسط الدرجة والقيمة المرجعية له أهمية عملية ومعنوية كبيرة، حيث أن قيمة **Cohen's d** هي **1.223** وقيمة **Hedges' correction** هي **1.189**، مما يدل على أن تأثير الأمن السيبراني على سلامة المعلومات وأداء البنك مهم وملموس.

ووفقًا للتحليل الإحصائي المفصل السابق، يمكن الاستنتاج بأن الفرضية الرئيسية قد تم تأكيدها بقوة، مما يعكس وعي موظفي البنك بأهمية الأمن السيبراني وتأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لولاية تبسة. هذا الإدراك يشير إلى مستوى عالٍ من الوعي الأمني ويبرز الجهود المبذولة لضمان بيئة عمل آمنة وفعالة.

نتائج إختبار الفرضيات:

من خلال ما سبق يمكن إختبار الفرضيات كما يلي:

❖ نتائج إختبار الفرضية الأساسية:

- ❖ بلغت قيمة t **4.539**، وكانت قيمة p للجانبين **.0000**، هذه القيم تدل على وجود فرق ذو دلالة إحصائية بين متوسط الدرجة والقيمة المرجعية المحددة مسبقًا (التي هي 2)، وذلك عند مستوى معنوية **0.05**. وعليه، يمكن رفض الفرضية الصفرية التي تفترض عدم وجود موافقة معنوية، وقبول الفرضية البديلة التي تؤكد موافقة الموظفين على توفر متطلبات الأمن السيبراني في البنك.
- ❖ من الجدير بالذكر أن **فاصل الثقة** للفرق بين متوسط الدرجة والقيمة المرجعية يتراوح بين **1969.** و**5218.**، مما يعزز الثقة في استقرار هذه النتيجة عبر عينات مختلفة ويؤكد على دلالتها الإحصائية.
- ❖ أخيرًا، يشير **حجم التأثير** المقاس بواسطة **Cohen's d** و**Hedges' correction** إلى أن الفرق بين متوسط الدرجة والقيمة المرجعية له أهمية عملية ومعنوية كبيرة، حيث أن قيمة **Cohen's d** هي **858.** وقيمة **Hedges' correction** هي **834.**، مما يدل على أن الأمن السيبراني يُعتبر متطلبًا مهمًا في البنك الخارجي لولاية تبسة وفقًا لتقييم موظفي البنك.

❖ نتائج إختبار الفرضيات الفرعية:

✓ الفرضية الفرعية الأولى:

- ❖ قيمة t تبلغ 6.855، وقيم p للجانبين تساوي 000.0، هذه القيم تدل على وجود فرق ذو دلالة إحصائية بين متوسط الدرجة والقيمة المرجعية (التي هي 2)، وذلك عند مستوى معنوية 0.05 وبالتالي، يمكن رفض الفرضية الصفرية التي تفترض عدم وجود موافقة معنوية، وقبول الفرضية البديلة التي تؤكد على توفر عناصر أمن المعلومات في البنك.
- ❖ من النقاط البارزة في التحليل فاصل الثقة للفرق بين متوسط الدرجة والقيمة المرجعية، الذي يتراوح بين 3670. و6806.، ويعزز هذا الفاصل الثقة في استقرار النتيجة عبر عينات مختلفة ويؤكد على دلالتها الإحصائية.
- ❖ بالإضافة إلى ذلك، يشير حجم التأثير المقاس بواسطة Cohen's d و Hedges' correction إلى أن الفرق بين متوسط الدرجة والقيمة المرجعية له أهمية عملية ومعنوية كبيرة، حيث أن قيمة Cohen's d هي 1.295 وقيمة Hedges' correction هي 1.259، مما يدل على أن تأثير توفر عناصر أمن المعلومات في البنك مهم وملموس.

✓ الفرضية الفرعية الثانية:

- ❖ أسفر t عن قيمة تبلغ **6.471**، وقيم p للجانبين تساوي **000.0**، هذه القيم تدل على وجود فرق ذو دلالة إحصائية بين متوسط الدرجة والقيمة المرجعية (التي هي 2)، وذلك عند مستوى معنوية **0.05**. وبالتالي، يمكن رفض الفرضية الصفرية التي تفترض عدم وجود إدراك معنوي، وقبول الفرضية البديلة التي تؤكد على إدراك الموظفين لنتائج الأمن السيبراني على سلامة المعلومات وأداء البنك.
- ❖ من النقاط البارزة في التحليل **فاصل الثقة** للفرق بين متوسط الدرجة والقيمة المرجعية، الذي يتراوح بين **3636. و7013.**، ويعزز هذا الفاصل الثقة في استقرار النتيجة عبر عينات مختلفة ويؤكد على دلالتها الإحصائية.

- بالإضافة إلى ذلك، يشير **حجم التأثير** المقاس بواسطة **Cohen's d** و **Hedges' correction** إلى أن الفرق بين متوسط الدرجة والقيمة المرجعية له أهمية عملية ومعنوية كبيرة، حيث أن قيمة **Cohen's d** هي **1.223** وقيمة **Hedges' correction** هي **1.189**، مما يدل على أن تأثير الأمن السيبراني على سلامة المعلومات وأداء البنك مهم وملموس.
- ووفقًا للتحليل الإحصائي المفصل السابق، يمكن الاستنتاج بأن الفرضية الثالثة قد تم تأكيدها بقوة، مما يعكس وعي موظفي البنك بأهمية الأمن السيبراني وتأثيره الإيجابي على الحفاظ على سلامة المعلومات وتحسين أداء البنك الخارجي لولاية تبسة. هذا الإدراك يشير إلى مستوى عالٍ من الوعي الأمني ويبرز الجهود المبذولة لضمان بيئة عمل آمنة وفعالة.

خلاصة الجزء الثالث:

من خلال دراستنا للأمن السيبراني وأمن المعلومات في البنوك والتوصل الى أن من أهم العوامل التي يعتمد عليها البنك الخارجي الجزائري وكالة –تبسة–، وكذا التعريف بالأهداف المنوطة بها، زيادة على عرض هيكلها التنظيمي، بالإضافة الى إلقاء نظرة عامة على البنك الخارجي الجزائري وكالة تبسة، وفي الأخير بالإعتماد على أسلوب الإستبيان قمنا بمعالجة البيانات عن طريق برنامج الحزمة الإحصائية للعلوم الإجتماعية SPSS V28، وتم من خلال هذه الدراسة إختبار الفرضيات الخاصة بالموضوع حيث تم:

01- قبول الفرضية الأساسية حيث يتضح إدراك موظفو البنك الخارجي لولاية تبسة نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك عند مستوى دلالة $\alpha = 0.05$؛

02- قبول الفرضية الفرعية الأولى حيث يتضح موافقة موظفو البنك الخارجي لولاية تبسة على توفر متطلبات الأمن السيبراني فيه عند مستوى دلالة$\alpha = 0.05$؛

03- قبول الفرضية الفرعية الثانية حيث يتضح موافقة موظفو البنك الخارجي لولاية تبسة على توفر عناصر أمن المعلومات فيه عند مستوى دلالة $\alpha = 0.05$.

الخاتمة العامة

في ختام هذه الدراسة، يمكننا القول أن الأمن السيبراني له مساهمة كبيرة في حماية المعلومات في البنوك حيث يؤثر على تلبية الخدمات المصرفية التي تلعب دورا حاسما في المنظومة الإقتصادية، وتطوير الأنظمة السيبرانية سيؤدي بتلقائية حتمية إلى تطوير المنظومة المصرفية وتعزيز الثقة في التكنولوجيا، تجربة العمل في منظومة مصرفية رقمية لن تكتمل إلا بتوفير الحماية السيبرانية.

لتحقيق الأمن السيبراني المصرفي، ينبغي على مقدمي الخدمات المصرفية توفير خدمات إحترافية ومحترمة وذات أمان عالي، بالإضافة إلى الإستجابة الفعالة لاحتياجات السوق المصرفية، علاوة على ذلك فإنه ينبغي تطوير وتحسين البنية التحتية التكنولوجية عن طريق نقل الخبرات من الدول الرائدة في المجال، بالإضافة إلى تشجيع وتقديم الفرص المهنية للشباب المبتكر المتخصص في المجال.

وأخيرا، يمكننا القول أن الأمن السيبراني له أثر كبير على تطوير المنظومة المالية وكذا حماية نظام المعلومات المصرفي، وبالتالي على نجاح المؤسسة المصرفية. لذا ينبغي على المؤسسات المصرفية تدريب موظفيها على التقنيات المستحدثة بصفة دورية في الأمن السيبراني لتحقيق الإستدامة المالية، وهذا ما يؤكد صحة الفرضية المبية عليها الدراسة بأن تلعب الجهود المبذولة في مجال الأمن السيبراني تلعب دورا أساسيا في منع الهجمات الإلكترونية وحماية البيانات والمعلومات الحساسة في القطاع البنكي بالجزائر.

1. نتائج الدراسة

من خلال هذه الدراسة تم التوصل إلى مجموعة من النتائج النظرية والتطبيقية نوجز أهمها فيما يلي:

1.1. نتائج الدراسة النظرية

- من الصعب تطبيق نظام مصرفي إلكتروني يحول دون فشل بلا توفير تقنيات الأمن سيبراني.
- إن تطوير نظام أمني سيبراني يؤدي تلقائيا إلى توفير درع حماية للخدمات المصرفية الرقمية.
- إن التواصل المستمر مع مصلحة الإعلام الآلي لكل بنك يمكن أن يساعد على سد ثغرات الأمن السيبراني وبالتالي منظومة مصرفية محمية.
- زيادة وعي وثقافة موظفي البنوك يسهل من تجسيد الأمن السيبراني.

بشكل عام نتائج الدراسة تدعم أهمية تحسين إجراءات الأمن السيبراني لحماية نظام المعلومات المصرفي.

2.1. نتائج الدراسة التطبيقية

- ✍ هناك علاقة قوية بين الأمن السيبراني ونظام المعلومات المصرفي لمؤسسة المجمع الجهوي للاستغلال لبنك بدر -تبسة-.
- ✍ مؤسسة المجمع الجهوي للاستغلال لبنك بدر -تبسة- تضع تقنيات أمن المعلومات في قمة أولوياتها.
- ✍ إن أغلبية موظفي المجمع الجهوي للاستغلال لبنك بدر -تبسة- يتمتعون ويعززون الوعي بالحماية ضد الهجمات السيبرانية بينهم وبين العملاء.
- ✍ مؤسسة المجمع الجهوي للاستغلال لبنك بدر -تبسة- تسعى لتطوير حماية البيانات والمعاملات المالية من الإختراق .
- ✍ مؤسسة المجمع الجهوي للاستغلال لبنك بدر -تبسة- تضل عرضة للتهديدات السيبرانية نتيجة للثغرات الأمنية والهجمات المتطورة كما هو الحال في العالم بأسره.
- ✍ التزام البنك الخارجي لولاية تبسة بأمن المعلومات ويبرز الجهود المبذولة لضمان حماية البيانات والمعلومات بشكل فعال.
- ✍ يقوم البنك بتدريبات أمنية تقيم فعّالة في تعزيز قدرات الموظفين، مما يساهم في تقوية الدفاعات الأمنية للبنك ضد التهديدات السيبرانية.
- ✍ إدراك الموظفين للفوائد الكبيرة التي يجلبها الأمن السيبراني، بما في ذلك تعزيز سلامة المعلومات البنكية، تقليل حوادث الاختراقات الأمنية، والحفاظ على خصوصية بيانات العملاء.

2. الإقتراحات والتوصيات

في ظل النتائج التي تم التوصل إليها يمكن تقديم بعض الإقتراحات والتوصيات التي من الممكن أن تساهم في تعزيز الأمن السيبراني في المنظومة المصرفية الجزائرية:

- ✍ تخصيص قسم لإدارة الهجمات السيبرانية المتجددة بإستمرار.
- ✍ تطوير ميزانية المصارف من خلال إدماج موظفي البنوك في دورات متخصصة لتلقي الخبرات من المؤسسات الرائدة عالميا في مجال الأمن السيبراني.
- ✍ السعي لإبرام إتفاقيات مع الشركات المختصة في مجال الأمن السيبراني.
- ✍ تحديث أنظمة تكنولوجيا المعلومات بشكلٍ دوري لضمان حمايتها من الثغرات الأمنية.

✍ تحفيز الشباب المبتكر بإقامة مسابقات بجوائز قيمة لكل من يكتشف ثغرات النظام السيبراني.

3. آفاق الدراسة

بعد دراستنا لهذا الموضوع تم اقتراح بعض العناوين التي تستحق الدراسة والتحليل، أهمها:

✍ دور التدريب والتوعية في بناء ثقافة الأمن السيبراني في البنوك والتصدي للهجمات السيبرانية.

✍ دور الذكاء الإصطناعي في اكتشاف ومكافحة الإحتيال المالي في البنوك الرقمية.

✍ تأثير الإبتكار التكنولوجي على استراتيجيات أمن المعلومات في البنوك ومواجهة التهديدات السيبرانية.

✍ تقييم الثغرات الأمنية الجديدة والتهديدات المستقبلية للبنوك: رؤية مستقبلية لتطورات أمن المعلومات.

قائمة المصادر والمراجع

المراجع باللغة العربية:

الكتب:

1. منى الأشقر جبور، **السيبرانية: هاجس العصر**، دراسات وأبحاث (1)، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية، بيروت، 2016.

المذكرات:

1. دلندة دوادي- زهرة بن حود، **أمن المعلومات المصرفية**، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماجستير، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، ورقلة.
2. آن سعيد ابراهيم عبد الواحد، **سياسات أمن المعلومات وعلاقتها بفاعلية نظم المعلومات الإدارية في الجامعات الفلسطينية، قطاع غزة**، قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في إدارة الأعمال، كلية الإقتصاد والعلوم الإدارية، جامعة الأزهر، غزة، 2015.
3. نور أمير موصلي، **الهجمات السيبرانية في ضوء القانون الدولي الانساني**، بحث مقدم استكمالا لمتطلبات نيل درجة ماجستير التأهيل والتخصص في القانون الدولي الانساني، الجامعة الافتراضية السورية، 2021.

الملتقيات:

1. كلية العلوم الانسانية والاجتماعية والعلوم الانسانية وآخرون، **الجزائر والتهديدات السيبرانية: نحو مستقبل آمن سيبرانيا**، الملتقى الدولي الأول العابر للتخصصات، جامعة أحمد دراية، أدرار، 11-12 ماي 2022.
2. عبد الرحمان محمد سليمان رشوان، زينب عبد الحفيظ أحمد قاسم، **أثر إدارة مخاطر الامن السيبراني على دعم الاستقرار والشمول المالي في البنوك**، المؤتمر العلمي الدولي الأول بعنوان "أثر الأمن السيبراني على الأمن الوطني"، جامعة عمان العربية بالاشتراك مع مديرية الأمن العام، ديسمبر 2022.
3. أسامة حسام الدين، **أساسيات الامن السيبراني**، أكاديمية سيسكو بجامعة طيبة، سبتمبر 2017.

المجلات والمنشورات:

1. 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).
2. منى عبد الله السمحان، **متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود**، مجلة كلية التربية- جامعة المنصورة، العدد 111، يوليو 2020.

3. خالد ظاهر عبد الله جابر السهيل المطيري، **دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي**، مجلة البحوث الفقهية والقانونية، العدد الثامن والثلاثون، الكويت، جوان 2022.

4. مروة فتحي السيد البغدادي، **اقتصاديات الأمن السيبراني في القطاع المصرفي**، مجلة البحوث القانونية والاقتصادية، العدد السادس والسبعون، جوان 2021.

5. شايب محمد-حمادي موراد، **تحديات الأمن السيبراني لأنظمة المعلومات في البنوك والمؤسسات المالية**، مجلة إنارة للدراسات الإقتصادية، الإدارية والمحاسبية، المجلد الرابع، العدد الأول، جوان 2023.

6. حسين علي قاسم الشمالي، **أمن وسرية المعلومات و أثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن**، مجلة جامعة القدس المفتوحة للأبحاث والدراسات الإدارية والاقتصادية، المجلد الثاني، العدد السابع، جوان 2017.

7. زيدان محمد-حمو محمد، **أمن المعلومات المصرفية كمطلب لتبني التسويق الالكتروني في البنوك الجزائرية**، مجلة رؤى اقتصادية، جامعة حسيبة بن بوعلي، الشلف، جوان 2015.

8. بوطلاعة وداد بوكورو منال، **الهجمات السيبرانية على البنية التحتية الحرجة دراسة في ضوء القانون الدولي** العام، مجلة حقوق الإنسان والحريات العامة، المجلد السابع، العدد الثاني، ديسمبر 2022.

9. أميرة عبد العظيم محمد عبد الجواد، **المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام**، مجلة الشريعة والقانون، العدد الخامس والثلاثون، الجزء الثالث، 2020.

10. عماد الدين محمد كامل عبد الحميد، **الهجمات السيبرانية على البنى التحتية للمدن الذكية: التحديات القانونية واستراتيجية المواجهة**، البحث العلمي والمجلة، كلية الإمام مالك للشريعة والقانون، دراسات علوم الشريعة والقانون، العدد الثالث، سبتمبر 2023.

المحاضرات:

1. بوازدية جمال، **الأمن السيبراني**، محاضرات مقدمة لطلبة السنة الثانية ماستر، جامعة الجزائر 3، تخصص دراسات استراتيجية وأمنية، السنة الجامعية 2020-2021.

المراجع باللغة الأجنبية:

المقالات:

1. Bojidar Bojinov, **Banking security- Major manifestations and aspects**, Academy Economics-svishtov, department of finance and credit, Narodnostopanski arhiv of 3/2016.

2. Bank of Japan, **The importance of information security for financial institutions and proposed countermeasures**, with a focus on internet-based financial services, 2000, p p 16-17.

المو اقع الإلكترونية:

1. https://www.kutub.info/library/book/21854

2. https://www.simplilearn.com/information-security-vs-cyber-security-article#

3. https://www.rmg-sa.com/

4. https://fastercapital.com/arabpreneur/


الملاحق

وزارة التعليم العالي والبحث العلمي

جامعة الشهيد الشيخ العربي التبسي –تبسة-

كلية العلوم الاقتصادية والتجارية وعلوم التسيير

استمارة استبيان

السلام عليكم ورحمة الله وبركاته

في إطار التحضير لإعداد مذكرة تخرج ماستر على مستوى كلية العلوم الاقتصادية والتجارية وعلوم التسيير تخصص اقتصاد نقدي وبنكي بجامعة الشهيد الشيخ العربي التبسي –تبسة- حول موضوع: **انعكاسات الأمن السيبراني على أمن المعلومات في البنوك**، نضع بين أيديكم هذا الاستبيان للحصول على معلومات من وجهة نظركم كموظفين لدى الوكالة الغرض منه البحث العلمي حصرا وللمساعدة في الوصول الى نتائج وتوصيات قيمة تفيد الواقع وتساهم في تطور المستقبل.

ونريد أن نتقدم لكم بجزيل الشكر والتقدير سلفا لأنكم ستخصصون جزءا من وقتكم للإجابة على فقرات هذا الاستبيان وذلك بوضع علامة (x) أمام الخيار الذي يعبر عن وجهة نظركم، بما يتفق مع مواقفكم الصريحة التي ستساهم في الوصول الى نتائج حقيقية وواقعية.

قبل الشروع في مبادرتكم لملء الاستبيان نريد أن نحيطكم بأساسيات الأمن السيبراني الذي يعد مجموعة من الإجراءات والتقنيات المصممة لحماية الأنظمة الإلكترونية والشبكات والبيانات من الهجمات والتهديدات السيبرانية (الرقمية)، وبالنسبة لأمن المعلومات: حماية البيانات والمعلومات بأنواعها الذهنية والورقية والالكترونية من كافة الهجمات.

تقبلوا منا فائق التقدير والاحترام لتعاونكم.

من اعداد الطالبة

مرزوق شيماء

تحت إشراف الدكتور

عبد المالك مهري

السنة الجامعية: 2023 - 2024

القسم الأول: البيانات الشخصية

البنك: .....

السن: من 25 الى 35 ☐ من 35 الى 45 ☐ من 45 فما أكثر ☐

الجنس: ذكر ☐ أنثى ☐

المؤهل العلمي: ليسانس ☐ ماستر ☐ ماجستير ☐

سنوات الخبرة: من 1-5 سنوات ☐ من 5-10 سنوات ☐ من 10-15 سنة ☐ أكثر من 15 سنة ☐

القسم الثاني: البيانات العلمية

المحور الأول: مستحقات الأمن السيبراني وبيئته في البنك

الرقم	العبارات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	واقع الأمن السيبراني في البنك					
01	يمتلك البنك الوعي الكافي والإحاطة الشاملة بمخاطر التهديدات السيبرانية التي قد تواجهه					
02	تحيط بالبنك تهديدات سيبرانية بإمكانها أن تدمر نظم المعلومات					
03	يتولى البنك فعالية إجراءات الوقاية والتدابير المتخذة لمواجهة الهجمات السيبرانية					
04	يطبق البنك سياسات واجراءات واضحة للأمن السيبراني					
	تحديات البنك في تطبيق سياسات الأمن السيبراني					
05	الانتقال من البنية التقليدية إلى البنية الرقمية يتطلب استثمارات ضخمة وتغييرات هيكلية تمنع البنوك من تنفيذ استراتيجيات الأمن السيبراني الشاملة					
06	يواجه البنك نقص في الموارد البشرية والمهارات الفنية اللازمة لتنفيذ سياسات الأمن السيبراني بشكل فعال.					
07	اغفال البنك عن توفير التدريب المناسب للموظفين في مجال الأمن السيبراني					
08	يواجه البنك صعوبة في تحديث أنظمته التكنولوجية القديمة مما يزيد من التحدي في تطبيق أحدث التقنيات والإجراءات الأمنية					
	متطلبات وشروط سياسات الأمن السيبراني					

09	تنفيذ تقنيات التشفير المعتمدة على المعايير الدولية لتأمين البيانات المالية والشخصية للعملاء					
10	تعزيز إجراءات التحقق المزدوج والتعرف على الهوية لتقليل مخاطر الوصول غير المصرح به					
11	تنفيذ آليات الرصد المستمرة لنشاطات الشبكة والبيانات للكشف المبكر عن أي تهديدات محتملة					
12	تطوير سياسات صارمة لإدارة الوصول والتحكم في الصلاحيات لضمان أقصى درجات الحماية من الاختراقات الداخلية والخارجية					
فعالية وجدوى تطبيق سياسات الأمن السيبراني						
13	تعزيز الاستجابة الفعالة للتهديدات الجديدة في عالم الأمن السيبراني مما يحد من تأثيرها السلبي على البنك وعملائه					
14	التقليل من مخاطر الاختراقات وتسريبات البيانات مما يحافظ على سمعة البنك وثقة العملاء					
15	تقوية الشراكات مع الجهات التنظيمية والشركاء التجاريين مما يساهم في تعزيز مكانة البنك في السوق المالية					
16	تحقيق الاستدامة المالية والحفاظ على مكانته كرائد في قطاع الخدمات المالية					

المحور الثاني: مستحقات أمن المعلومات وبيئته في البنك

الرقم	العبارات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
واقع أمن المعلومات في البنك						
01	تعاني البنوك بشكل متزايد من هجمات الاختراق والاختراقات السيبرانية التي تهدد سرية وسلامة المعلومات الحساسة					
02	تظل البنوك عرضة للتهديدات السيبرانية نتيجة للثغرات الأمنية والهجمات المتطورة					
03	يطبق البنك سياسات واجراءات لتحقيق الأمن الشامل للبيانات					
04	يواجه البنك تحديات فريدة في مجال أمن المعلومات نتيجة لضرورة التوازن بين سهولة الوصول للعملاء وحماية البيانات المالية					

	الحساسة					
تحديات البنك في تطبيق تقنيات أمن المعلومات						
05	قلة الخبرة والكفاءة في مجال أمن المعلومات تجعل من التحدي تطبيق تقنيات متقدمة داخل البنوك					
06	التحديات المالية والميز انية المحدودة تقف كعائق أمام قدرة البنك على الاستثمار في حلول أمن المعلومات الشاملة					
07	الافتقار لاستخدام تقنيات الكشف المبكر والاستجابة الفعالة للحفاظ على سلامة البيانات وثقة العملاء					
08	تعقيدات الشراكات مع جهات خارجية ومقدمي الخدمات الأمنية تحول دون تبني البنك لتقنيات أمن المعلومات المتطورة					
متطلبات توفير سياسات أمن المعلومات						
09	توفير سياسات صارمة تحدد الإجراءات الأمنية المطلوبة لحماية البيانات المالية والشخصية للعملاء والموظفين					
10	توفير اجراءات للتعامل مع حوادث الأمان مثل اختر اقات البيانات والاحتيال بما في ذلك خطط الطوارئ وإجراءات الاستجابة السريعة					
11	توعية وتدريب الموظفين بشأن أفضل الممارسات في مجال الأمان وحماية المعلومات					
12	تبني آليات لتقييم وتحسين الأمان بناء على التهديدات الجديدة وتطورات التكنولوجيا					
جدوى تطبيق سياسات أمن المعلومات						
13	توفير بيئة موثوقة وآمنة يعزز من فرص الابتكار والنمو في البنك حيث يشعر الموظفون والعملاء بالراحة في التفاعل مع النظام المصرفي					
14	توفير إطار قوي لأمان المعلومات يسهم في تعزيز الثقافة الأمنية داخل البنك مما يزيد من وعي الموظفين ويقلل من مخاطر الاختر اقات					
15	تقليل مخاطر فقدان البيانات والتعرض للهجمات السيبر انية مما يقلل من تكاليف الاستجابة للحوادث الأمنية ويعزز كفاءة العمليات المصرفية					
16	توفير تكاليف إضافية نتيجة لتقليل التهديدات السيبر انية وزيادة الكفاءة التشغيلية					

المحور الثالث: تأثير الأمن السيبراني على أمن المعلومات في البنك

الرقم	العبارات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	تعزيز ثقة العملاء وحماية سمعة البنك					
01	الحفاظ على سلامة بيانات العملاء والمعاملات المالية يعكس التزام البنك بأعلى معايير الأمان ويبني علاقات طويلة الأمد مع العملاء					
02	توفير تجارب مالية آمنة وموثوقة يجعل العملاء يشعرون بالراحة والثقة في التعامل مع البنك والاستمرار في استخدام خدماته					
03	التواصل الفعال مع العملاء حول التهديدات السيبرانية المحتملة والإجراءات المتخذة لمواجهتها يزيد من ثقتهم في البنك وسمعته					
04	تقديم حلول أمان مبتكرة وفعالة يؤكد على التزام البنك بحماية مصالح عملائه ويعزز الثقة في قدرته على التعامل مع التهديدات السيبرانية					
	حماية البيانات والمعاملات المالية من الاختراق					
05	تشكل آليات الأمن السيبراني درعا حصينا يحمي البيانات المالية والمعاملات الإلكترونية من الوصول الغير مصرح به					
06	اعتماد السياسات والإجراءات الأمنية الصارمة يضمن تطبيق المعايير الأمنية العالية ويقيد محاولات الاختراق					
07	تبني تقنيات الكشف المبكر والتحليل المستمر يمكنه تحديد والتصدي للتهديدات السيبرانية المحتملة قبل حدوث الاختراقات					
08	تطبيق إجراءات الوقاية والاستجابة الفعالة يحد من فرص الاختراقات ويقلل من تأثيرها على البيانات المالية					
	اجراءات الحماية من الهجمات السيبرانية					
09	استخدام الهوية الرقمية والتحقق الثنائي يعزز أمان المعاملات المالية عبر الانترنت ويحميها من الاختراقات					
10	تطبيق نظام متقدم للكشف عن التسلل يستخدم تحليل السلوك وتقنيات التعرف على النمط لاكتشاف الاختراقات والتصدي لها بشكل فعال					

11	تطوير وتحديث نظم الأمان السيبراني بشكل دوري يضمن استمرارية الحماية ضد التهديدات الجديدة والمتطورة					
12	توفير خدمات النسخ الاحتياطي واستعادة البيانات يضمن استمرارية العمليات المالية في حالة حدوث اختراقات أو فقدان للبيانات					
التكنولوجيا						
13	استخدام التقنيات البيومترية مثل بصمات الأصابع والتعرف على الوجه يعزز الحماية ويقلل من فرص الاختراقات بشكل فعال					
14	توفير آليات التشفير والتوقيع الرقمي يمنع الاختراقات ويضمن سلامة المعاملات المالية الإلكترونية					
15	تطبيق تقنيات التعقب والتعقيد لتقييد الوصول إلى البيانات المالية للأشخاص المعتمدين فقط و أنظمة النسخ الاحتياطي واستعادة البيانات					
16	تطبيق تقنيات الذكاء الاصطناعي يمكن من تحليل النمط السلوكي والتنبؤ بالهجمات السيبرانية المحتملة					
تعزيز الوعي بين الموظفين والعملاء						
17	توفير التدريب المستمر للموظفين والعملاء حول أحدث التهديدات السيبرانية يعزز قدرتهم على التعامل مع المخاطر بفعالية					
18	تحفيز الموظفين على تبني أفضل الممارسات في إدارة كلمات المرور والوصول الآمن إلى البيانات يعزز أمن النظام المالي					
19	تعزيز التواصل المستمر مع العملاء حول مخاطر الأمان السيبراني يسهم في تعزيز تبادل المعلومات الآمن والحفاظ على البيانات الحساسة					
20	إشراك الموظفين والعملاء في عمليات التقييم والتحليل لتحديد نقاط الضعف في الأمان السيبراني يسهم في تعزيز الحماية والتحسين المستمر					

Corrélations

		مستحقات.الأمن.السيبراني	مستحقات.أمن.المعلومات	تأثير.السيبراني.على.امن.المعلومات	الكل
مستحقات.الامن.السيبراني	Corrélation de Pearson	1	.951**	.883**	.964**
	Sig. (bilatérale)		.000	.000	.000
	N	40	40	40	40
مستحقات.أمن.المعلومات	Corrélation de Pearson	.951**	1	.976**	.997**
	Sig. (bilatérale)	.000		.000	.000
	N	40	40	40	40
تأثير.الأمن. السيبراني.على.أمن.المعلومات	Corrélation de Pearson	.883**	.976**	1	.975**
	Sig. (bilatérale)	.000	.000		.000
	N	40	40	40	40
الكل	Corrélation de Pearson	.964**	.997**	.975**	1
	Sig. (bilatérale)	.000	.000	.000	
	N	40	40	40	40

**. La corrélation est significative au niveau 0.01 (bilatéral).

Récapitulatif de traitement des observations

		N	%
Observations	Valide	40	100.0
	Exclue[a]	0	.0
	Total	40	100.0

a. Suppression par liste basée sur toutes les variables de la procédure.

Statistiques de fiabilité

Alpha de Cronbach	Nombre d'éléments
.994	52

Statistiques

		الجنس	السن	المؤهل.العلمي	الخبرة
N	Valide	40	40	40	40
	Manquant	0	0	0	0

الجنس

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	انثى	14	35.0	35.0	35.0
	ذكر	26	65.0	65.0	100.0
	Total	40	100.0	100.0	

السن

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	من 25 الى 35	6	15.0	15.0	15.0
	من 35 الى 45	25	62.5	62.5	77.5
	من 45 فما أكثر	9	22.5	22.5	100.0
	Total	40	100.0	100.0	

المؤهل.العلمي

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	ليسانس	30	75.0	75.0	75.0
	ماستر	10	25.0	25.0	100.0
	Total	40	100.0	100.0	

الخبرة

		Fréquence	Pourcentage	Pourcentage valide	Pourcentage cumulé
Valide	من 1-5 سنوات	8	20.0	20.0	20.0
	من 5-10 سنوات	13	32.5	32.5	52.5
	من 10-15 سنة	14	35.0	35.0	87.5
	أكثر من 15 سنة	5	12.5	12.5	100.0
	Total	40	100.0	100.0	

Statistiques descriptives

	N	Minimum	Maximum	Moyenne	Ecart type
a1	40	3	5	4.40	.841
a2	40	3	5	4.53	.751
a3	40	3	4	3.43	.501
a4	40	3	4	3.35	.483
a5	40	4	5	4.72	.452
a6	40	3	5	3.97	.577
a7	40	3	4	3.75	.439
a8	40	2	5	4.02	.947
a9	40	4	5	4.70	.464
a10	40	3	5	4.03	.620
a11	40	3	5	3.87	.607
a12	40	3	4	3.68	.474
a13	40	3	4	3.55	.504
a14	40	3	4	3.68	.474
a15	40	3	4	3.78	.423
a16	40	3	4	3.68	.474
مستحقات.الامن.السيبراني	40	3.06	4.50	3.9453	.49581
N valide (liste)	40				

Statistiques descriptives

	N	Minimum	Maximum	Moyenne	Ecart type
b1	40	2	4	2.88	.791
b2	40	2	4	3.15	.770
b3	40	3	4	3.70	.464
b4	40	2	4	3.58	.712
b5	40	3	5	3.98	.530
b6	40	3	5	4.10	.632
b7	40	3	5	3.93	.526
b8	40	3	5	4.00	.555
b9	40	3	5	3.73	.679
b10	40	3	5	3.83	.549
b11	40	3	5	3.95	.597
b12	40	3	5	3.85	.580
b13	40	3	5	3.98	.530
b14	40	3	5	3.85	.622
b15	40	3	5	3.90	.545
b16	40	3	5	3.83	.594
مستحقات.امن.المعلومات	40	3	5	3.76	.544
N valide (liste)	40				

Statistiques descriptives

	N	Minimum	Maximum	Moyenne	Ecart type
c1	40	3	5	4.03	.660
c2	40	3	5	3.90	.672
c3	40	3	5	3.98	.660
c4	40	3	5	4.05	.677
c5	40	3	5	4.00	.599
c6	40	3	5	3.90	.545
c7	40	3	5	3.95	.504
c8	40	3	5	3.90	.591
c9	40	3	5	3.95	.552
c10	40	3	5	4.02	.530
c11	40	3	5	3.88	.516
c12	40	3	5	3.85	.580
c13	40	3	5	3.88	.563
c14	40	3	5	3.93	.474
c15	40	3	5	3.95	.552
c16	40	3	5	4.00	.506
c17	40	3	5	3.97	.577

c18	40	3	5	4.00	.506
c19	40	3	5	3.90	.496
c20	40	3	5	4.02	.480
تاثير.السيبراني.على.امن.المعلومات	40	3	5	3.95	.521
N valide (liste)	40				

Statistiques sur échantillon uniques

	N	Moyenne	Ecart type	Moyenne erreur standard
مستحقات.الامن.السيبراني	40	3.95	.496	.078

Test sur échantillon unique

	Valeur de test = 3					
					Intervalle de confiance de la différence à 95 %	
	t	ddl	Sig. (bilatéral)	Différence moyenne	Inférieur	Supérieur
مستحقات.الامن.السيبراني	12.058	39	.000	.945	.79	1.10

Statistiques sur échantillon uniques

	N	Moyenne	Ecart type	Moyenne erreur standard
مستحقات.امن.المعلومات	40	3.76	.544	.086

Test sur échantillon unique

	Valeur de test = 3					
					Intervalle de confiance de la différence à 95 %	
	t	ddl	Sig. (bilatéral)	Différence moyenne	Inférieur	Supérieur
مستحقات.امن.المعلومات	8.871	39	.000	.763	.59	.94

Statistiques sur échantillon uniques

	N	Moyenne	Ecart type	Moyenne erreur standard
تاثير.السيبراني.على.امن.المعلومات	40	3.95	.521	.082

Test sur échantillon unique

	Valeur de test = 3					
					Intervalle de confiance de la différence à 95 %	
	t	Ddl	Sig. (bilatéral)	Différence moyenne	Inférieur	Supérieur
تاثير.السيبراني.على.امن.المعلومات	11.563	39	.000	.953	.79	1.12

الملاحق الخاصة بالدراسة الميدانية للبنك الخارجي الجزائري

ملحق رقم (01): إستمارة الإستبيان

وزارة التعليم العالي والبحث العلمي
جامعة الشهيد الشيخ العربي التبسي – تبسة
كلية العلوم الاقتصادية والتجارية وعلوم التسيير
تخصص: اقتصاد نقدي وبنكي

الاستبانة

سيدي الفاضل، سيدتي الفاضلة، تحياتي لكم:

في إطار تقديم مذكرة مكملة لنيل شهادة الماستر، نضع بين أيديكم هذه الاستبانة حول: "**انعكاسات الأمن السيبراني على أمن المعلومات في البنوك**". دراسة حالة البنك الخارجي الجزائري – تبسة.

"نحن نقدر وقتكم وآرائكم. مشكورون على المشاركة في هذه الاستبانة".

من إعداد الطالبة

- **زين تركية إجلال**

إشراف الأستاذ

- **مهري عبد المالك**

الأمن السيبراني: هو مجموعة من الإجراءات والتقنيات التي تُستخدم لحماية الشبكات، والأنظمة، والبرامج من الهجمات الإلكترونية.

- **أمن المعلومات:** هو حماية المعلومات من الوصول غير المصرح به، والاستخدام، والكشف، والتعديل، والتدمير، أو الإزالة.

المحور الأول: البيانات الشخصية

الجنس	ذكر ☐	أنثى ☐

العمر (بالسنوات)	أقل من 30 ☐	من 30 إلى أقل من 40 ☐	من 40 إلى أقل من 50 ☐	من 50 فأكثر ☐

طبيعة الوظيفة	إطار ☐	عون التحكم ☐	عون التنفيذ ☐

الخبرة المهنية (بالسنوات)	أقل من 5 ☐	من 5 إلى 15 ☐	أكثر من 15 ☐

المستوى التعليمي	ثانوي ☐	تقني سامي ☐	جامعي ☐

من فضلك ضع x حول الإجابة المناسبة.

من فضلك ضع x حول التقييم المناسب.

العبارات	لا أوافق	محايد	أوافق

المحور الثاني: الأمن السيبراني

المتطلبات الإدارية			
1. السياسات والإجراءات الأمنية المطبقة في البنك فعالة.			
2. التدريب والوعي الأمني للموظفين في البنك يتم بشكل مستمر وفعّال.			
3. خطط الاستجابة للحوادث الأمنية محدثة وتُطبق بشكل فوري عند الحاجة.			
4. هناك تعاون ممتاز بين الأقسام المختلفة في البنك لضمان الأمن السيبراني.			
المتطلبات التقنية			
5. البنك يستخدم أحدث التقنيات لحماية البيانات والمعلومات.			
6. أنظمة الكشف عن الاختراقات والتصدي لها تعمل بكفاءة عالية.			
7. نظام التحديثات الأمنية للبرمجيات المستخدمة في البنك فعّال ويتم بانتظام.			
8. الشبكات والاتصالات البنكية مؤمنة بشكل جيد ضد التهديدات الخارجية.			
المتطلبات البشرية			
9. موظفو البنك لديهم الكفاءة اللازمة للتعامل مع التهديدات الأمنية السيبرانية.			
10. الموظفون الجدد يمتلكون مستوى معرفة أمنية جيد عند التحاقهم بالبنك.			
11. البنك يضم خبراء أمنيين مؤهلين للتعامل مع الحوادث الأمنية.			
12. الدورات التدريبية الأمنية المقدمة للموظفين تعزز مهاراتهم الأمنية بشكل فعّال.			
المتطلبات المادية			
13. الأنظمة المادية للرقابة متوفرة وتعمل بكفاءة لحماية مراكز البيانات.			
14. الأجهزة الأمنية مثل الجدران النارية وأنظمة الكشف عن الاختراقات تُصان وتُحدث بشكل دوري.			
15. الإجراءات المتبعة للحفاظ على سلامة البنية التحتية المادية للبنك مُطبقة بشكل صارم.			
16. الأنظمة الأمنية للوصول إلى البنك ومرافقه تضمن أعلى مستويات الأمان.			

المحور الثالث: أمن المعلومات

استمرارية توفر المعلومات			
17. المعلومات متاحة ويمكن الوصول إليها بشكل مستمر دون انقطاع.			
18. أنظمة النسخ الاحتياطي والاسترجاع تعمل بكفاءة لضمان استمرارية المعلومات.			
19. الإجراءات المتبعة لضمان توفر المعلومات في حالات الطوارئ مُطبقة بشكل فعّال.			
سلامة المحتوى واكتماله			
20. يحافظ البنك على سلامة واكتمال المحتوى المخزن والمعالج فيه.			
21. الإجراءات الأمنية تضمن عدم تعرض المحتوى للتلف أو التغيير غير المصرح به.			
22. التحقق من صحة المعلومات وتحديثها يتم بانتظام لضمان دقتها واكتمالها.			
سرية المعلومات وموثوقيتها			
23. المعلومات الحساسة محمية بإجراءات أمنية صارمة لضمان سريتها.			
24. الوصول إلى المعلومات مقيد بمستويات تصريح محددة لضمان موثوقيتها.			
25. التدابير المتخذة لحماية المعلومات من الاختراق تُطبق بشكل مستمر وفعّال.			
الخصوصية			
26. بيانات العملاء محمية بإجراءات خصوصية تضمن عدم الكشف عنها بشكل غير مصرح.			
27. السياسات المتعلقة بخصوصية البيانات مُحدثة وتُطبق بشكل صارم.			
28. التزام البنك بقوانين الخصوصية يضمن حماية معلومات العملاء بشكل كامل.			

المحور الرابع: نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك

29. تطبيق الأمن السيبراني يعزز من سلامة المعلومات البنكية.			
30. الاهتمام بالأمن السيبراني يقلل من حوادث الاختراقات الأمنية.			
31. الإجراءات الأمنية السيبرانية تحافظ على خصوصية بيانات العملاء.			
32. تحسن أداء البنك نتيجة لتطبيق معايير الأمن السيبراني.			
33. التدريبات الأمنية تساهم في رفع كفاءة الموظفين في التعامل مع التهديدات السيبرانية.			
34. الاستثمار في الأمن السيبراني يقود إلى تحسين الثقة بين البنك وعملائه.			
35. الأمن السيبراني يدعم استمرارية الأعمال ويقلل من فترات التوقف.			
36. التزام البنك بالأمن السيبراني يعزز 47 من موقعه التنافسي في السوق.			
37. الأمن السيبراني يساعد في الحفاظ على سمعة البنك ومصداقيته.			
38. التقنيات الأمنية الحديثة تساهم في كشف التهديدات السيبرانية بشكل مبكر.			
39. الأمن السيبراني يقلل من المخاطر المالية المرتبطة بالهجمات الإلكترونية.			

الملحق رقم (02):نتائج SPSS

One-Sample Kolmogorov-Smirnov Test

	الأمن السيبراني	أمن المعلومات	نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك
N	28	28	28
Test Statistic	.153	.135	.155
Asymp. Sig. (2-tailed)	.105	.200	.084

Correlations

		الأمن السيبراني	أمن المعلومات	نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	المحور الإجمالي
الأمن السيبراني	Pearson Correlation	1	.339	.368	.715**
	Sig. (2-tailed)		.077	.054	.000
	N	28	28	28	28
أمن المعلومات	Pearson Correlation	.339	1	.639**	.824**
	Sig. (2-tailed)	.077		.000	.000
	N	28	28	28	28
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	Pearson Correlation	.368	.639**	1	.847**
	Sig. (2-tailed)	.054	.000		.000
	N	28	28	28	28
المحور الإجمالي	Pearson Correlation	.715**	.824**	.847**	1
	Sig. (2-tailed)	.000	.000	.000	
	N	28	28	28	28

**. Correlation is significant at the 0.01 level (2-tailed).

Reliability Statistics

Cronbach's Alpha	N of Items
.888	39

Reliability Statistics

Cronbach's Alpha	N of Items
.825	16

Reliability Statistics

Cronbach's Alpha	N of Items
.804	12

Reliability Statistics

Cronbach's Alpha	N of Items
.808	11

		Count	Column N %
الجنس	أنثى	17	60.7%
	ذكر	11	39.3%
العمر	أقل من 30	14	50.0%
	من 30 إلى أقل من 40	7	25.0%
	من 40 إلى أقل من 50	6	21.4%
	من 50 فأكثر	1	3.6%
طبيعة الوظيفة	إطار	18	64.3%
	عون التحكم	7	25.0%
	عون التنفيذ	3	10.7%
الخبرة المهنية	أقل من 5	12	42.9%
	من 5 إلى 15	12	42.9%
	أكثر من 15	4	14.3%
المستوى التعليمي	ثانوي	0	0.0%
	تقني سامي	8	28.6%
	جامعي	20	71.4%

	Mean	Std. Deviation
السياسات والإجراءات الأمنية المطبقة في البنك فعالة.	2.29	.937
التدريب والوعي الأمني للموظفين في البنك يتم بشكل مستمر وفعّال.	2.46	.693
خطط الاستجابة للحوادث الأمنية محدثة وتُطبق بشكل فوري عند الحاجة.	2.32	.819
هناك تعاون ممتاز بين الأقسام المختلفة في البنك لضمان الأمن السيبراني.	2.68	.548
البنك يستخدم أحدث التقنيات لحماية البيانات والمعلومات.	2.36	.826
أنظمة الكشف عن الاختراقات والتصدي لها تعمل بكفاءة عالية.	2.43	.742
نظام التحديثات الأمنية للبرمجيات المستخدمة في البنك فعّال ويتم بانتظام.	2.61	.629
الشبكات والاتصالات البنكية مؤمنة بشكل جيد ضد التهديدات الخارجية.	2.54	.637
موظفو البنك لديهم الكفاءة اللازمة للتعامل مع التهديدات الأمنية السيبرانية.	2.11	.786
الموظفون الجدد يمتلكون مستوى معرفة أمنية جيد عند التحاقهم بالبنك.	2.32	.772
البنك يضم خبراء أمنيين مؤهلين للتعامل مع الحوادث الأمنية.	2.36	.826
الدورات التدريبية الأمنية المقدمة للموظفين تعزز مهاراتهم الأمنية بشكل فعّال.	2.43	.836
الأنظمة المادية للرقابة متوفرة وتعمل بكفاءة لحماية مراكز البيانات.	2.25	.887
الأجهزة الأمنية مثل الجدران النارية وأنظمة الكشف عن الاختراقات تُصان وتُحدث بشكل دوري.	2.25	.844
الإجراءات المتبعة للحفاظ على سلامة البنية التحتية المادية للبنك مُطبقة بشكل صارم.	2.18	.905
الأنظمة الأمنية للوصول إلى البنك ومرافقه تضمن أعلى مستويات الأمان.	2.18	.945
الأمن السيبراني	2.4077	.43470

	Mean	Std. Deviation
المعلومات متاحة ويمكن الوصول إليها بشكل مستمر دون انقطاع.	2.43	.742
أنظمة النسخ الاحتياطي والاسترجاع تعمل بكفاءة لضمان استمرارية المعلومات.	2.43	.742
الإجراءات المتبعة لضمان توفر المعلومات في حالات الطوارئ مُطبقة بشكل فعّال.	2.46	.744
يحافظ البنك على سلامة واكتمال المحتوى المخزن والمعالج فيه.	2.57	.573
الإجراءات الأمنية تضمن عدم تعرض المحتوى للتلف أو التغيير غير المصرح به.	2.54	.744
التحقق من صحة المعلومات وتحديثها يتم بانتظام لضمان دقتها واكتمالها.	2.54	.744
المعلومات الحساسة محمية بإجراءات أمنية صارمة لضمان سريتها.	2.64	.731
الوصول إلى المعلومات مقيد بمستويات تصريح محددة لضمان موثوقيتها.	2.54	.637
التدابير المتخذة لحماية المعلومات من الاختراق تُطبق بشكل مستمر وفعّال.	2.54	.744
بيانات العملاء محمية بإجراءات خصوصية تضمن عدم الكشف عنها بشكل غير مصرح.	2.43	.790
السياسات المتعلقة بخصوصية البيانات مُحدثة وتُطبق بشكل صارم.	2.46	.793
التزام البنك بقوانين الخصوصية يضمن حماية معلومات العملاء بشكل كامل.	2.71	.600
أمن المعلومات	2.5238	.40436
Valid N (listwise)		

	Mean	Std. Deviation
تطبيق الأمن السيبراني يعزز من سلامة المعلومات البنكية.	2.64	.621
الاهتمام بالأمن السيبراني يقلل من حوادث الاختراقات الأمنية.	2.61	.685
الإجراءات الأمنية السيبرانية تحافظ على خصوصية بيانات العملاء.	2.64	.678
تحسن أداء البنك نتيجة لتطبيق معايير الأمن السيبراني.	2.46	.838
التدريبات الأمنية تساهم في رفع كفاءة الموظفين في التعامل مع التهديدات السيبرانية.	2.46	.838
الاستثمار في الأمن السيبراني يقود إلى تحسين الثقة بين البنك وعملائه.	2.61	.685
الأمن السيبراني يدعم استمرارية الأعمال ويقلل من فترات التوقف.	2.61	.685
التزام البنك بالأمن السيبراني يعزز من موقعه التنافسي في السوق.	2.43	.742
الأمن السيبراني يساعد في الحفاظ على سمعة البنك ومصداقيته.	2.39	.786
التقنيات الأمنية الحديثة تساهم في كشف التهديدات السيبرانية بشكل مبكر.	2.32	.905
الأمن السيبراني يقلل من المخاطر المالية المرتبطة بالهجمات الإلكترونية.	2.68	.670
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	2.5325	.43543

	N	Mean	Std. Deviation	Std. Error Mean
الأمن السيبراني	28	2.3594	.41896	.07918

Test Value = 2

	t	df	Significance One-Sided p	Significance Two-Sided p	Mean Difference	95% Confidence Interval of the Difference Lower	95% Confidence Interval of the Difference Upper
الأمن السيبراني	4.539	27	.000	.000	.35938	.1969	.5218

		Standardizer[a]	Point Estimate	Confidence Interval 95% Lower	Confidence Interval 95% Upper
الأمن السيبراني	Cohen's d	.41896	.858	.417	1.287
	Hedges' correction	.43107	.834	.405	1.251

	N	Mean	Std. Deviation	Std. Error Mean
أمن المعلومات	28	2.5238	40436.	07642.

Test Value = 2

	t	df	Significance One-Sided p	Significance Two-Sided p	Mean Difference	95% Confidence Interval of the Difference Lower	95% Confidence Interval of the Difference Upper
أمن المعلومات	6.855	27	.000	.000	.52381	.3670	.6806

		Standardizer[a]	Point Estimate	Confidence Interval 95% Lower	Confidence Interval 95% Upper
أمن المعلومات	Cohen's d	.40436	1.295	.783	1.794
	Hedges' correction	.41604	1.259	.761	1.744

	N	Mean	Std. Deviation	Std. Error Mean
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	28	2.5238	40436.	07642.

Test Value = 2

	T	df	Significance One-Sided p	Significance Two-Sided p	Mean Difference	95% Confidence Interval of the Difference Lower	95% Confidence Interval of the Difference Upper
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	6.855	27	.000	.000	.52381	.3670	.6806

			Point Estimate	Confidence %95 Interval	
		Standardizer[a]		Lower	Upper
نتائج الاهتمام بتطبيق الأمن السيبراني على سلامة المعلومات وأداء البنك	Cohen's d	.40436	1.295	.783	1.794
	Hedges' correction	.41604	1.259	.761	1.744

الملخص

الملخص

تهدف هذه الدراسة إلى تبيان تأثير الأمن السيبراني على أمن المعلومات في البنوك، حيث تم اختيار المجمع الجهوي لبنك بدر –تبسة- لإجراء الدراسة التطبيقية، في حين تم استخدام الاستبيان كأداة لجمع البيانات، وتم توزيع الاستبيان على موظفي المؤسسة بواقع 50 إستمارة، وقد تم استخدام المنهج الوصفي التحليلي وأيضا المنهج الإحصائي للوصول إلى نتائج ولاختبار الفرضيات وذلك من خلال الإستعانة بالبرنامج الإحصائي (SPSS).

وخلصت الدراسة إلى نتائج أهمها:

- ✓ وجود علاقة ذات دلالة إحصائية بين الأمن السيبراني وأمن المعلومات في البنوك.
- ✓ يساهم الأمن السيبراني في حماية المعلومات البنكية من الهجمات السيبرانية.

الكلمات المفتاحية: أمن سيبراني، أمن معلومات، بنوك، هجمات سيبرانية.

Abstract:

This study aims to demonstrate the impact of cybersecurity on information security in banks. The regional complex of Badr Bank -Tebessa- was chosen to conduct the applied study, while the questionnaire was used as a tool for collecting data. The questionnaire was distributed to the institution's employees in 50 forms, and it was used The descriptive and analytical approach as well as the statistical approach to arrive at results and test hypotheses through the use of the statistical program (SPSS).

The study concluded with the most important results:

- ✓ There is a statistically significant relationship between cybersecurity and information security in bank.
- ✓ Cybersecurity contributes to protecting banking information from cyber attacks.

Keywords: cyber security, information security, banks, cyber attacks.