الجمهورية العربية السورية
وزارة التعليم العالي والبحث العلمي
الجامعة السورية الخاصة
كلية العلوم الإدارية
قسم: العلوم المالية والمصرفية



دور الأمن السيبراني في حماية القطاع المصرفي

دراسة ميدانية في المصارف التقليدية الخاصة

The role of cybersecurity in protecting the banking sector:

A Field Study in Traditional Private Banks

مشروع أعد لنيل درجة الإجازة الجامعية في العلوم الإدارية قسم العلوم المالية والمصرفية

إعداد الباحثان:

محمد مروان الحاج علي

ساهر سلامه المشوح

إشراف:

الدكتورة منال صقر

العام الدراسي 2025-2026م

ملخص الدراسة

هدفت الدراسة إلى بيان دور الأمن السيبراني في حماية القطاع المصرفي في سوريا، وذلك من خلال بيان دور (الضوابط التقنية والفنية، حوكمة الأمن السيبراني، إدارة المخاطر السيبرانية، الوعي والتدريب الأمني) كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

تم الاعتماد على المنهج الوصفي التحليلي، وقد ضم مجتمع الدراسة العاملين لدى المصارف الخاصة السورية وتم أخذ عينة عشوائية من العاملين في مناصب وظيفية مختلفة. واعتمدت الاستبانة في جمع البيانات تم توزيعها الكترونياً، وقد بلغ عدد الاستبانات الموزعة الصالحة للتحليل (79) استبانة، تم تحليلها باستخدام البرنامج الإحصائي SPSS واختبار الفرضيات باستخدام الانحدار الخطي البسيط والمتعدد.

وقد توصلت الدراسة إلى وجود دور إيجابي ذو دلالة معنوية للأمن السيبراني في حماية القطاع المصرفي في سوريا، ووجود دور إيجابي ذو دلالة معنوية لـ (الضوابط التقنية والفنية، حوكمة الأمن السيبراني، إدارة المخاطر السيبرانية، الوعي والتدريب الأمني) كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

وقد أوصت الدراسة بضرورة إلزام جميع المؤسسات المصرفية بـ دمج الأمن السيبراني كبند دائم في اجتماعات مجلس الإدارة وتحديد مقاييس أداء واضحة للأمن تُرفع دورياً للإدارة العليا لضمان المتابعة واتخاذ القرار على أعلى المستويات.

الكلمات المفتاحية: الأمن السيبراني، إدارة المخاطر السيبرانية، حوكمة الأمن السيبراني، حماية القطاع المصرفي.

Abstract

This study aimed to demonstrate the role of cybersecurity in protecting the banking sector in Syria by examining the role of (technical controls, cybersecurity governance, cyber risk management, and security awareness and training) as dimensions of cybersecurity in protecting the Syrian banking sector.

The descriptive-analytical approach was employed. The study population consisted of employees of Syrian private banks, and a random sample of employees in various job positions was selected. Data was collected electronically using a questionnaire, and (79) questionnaires were deemed valid for analysis. The data were analyzed using the SPSS statistical software, and hypotheses were tested using simple and multiple linear regression.

The study concluded that cybersecurity plays a statistically significant positive role in protecting the Syrian banking sector, and that (technical controls, cybersecurity governance, cyber risk management, and security awareness and training) also play a statistically significant positive role as dimensions of cybersecurity in protecting the Syrian banking sector.

The study recommended that all banking institutions be obligated to integrate cybersecurity as a permanent item on the agenda of board meetings and to define clear security performance metrics that are periodically submitted to senior management to ensure follow-up and decision-making at the highest levels.

Keywords: Cybersecurity, Cyber Risk Management, Cybersecurity Governance, Banking Sector Protection.

قائمة المحتويات

الإطار العام للدراسة	**1**
أولاً: المقدمة	**1**
ثانياً: الدراسات السابقة	**2**
ثالثاً: مشكلة الدراسة	**7**
رابعاً: فرضيات الدراسة	**8**
خامساً: أهمية الدراسة	**8**
سادساً: أهداف الدراسة	**9**
سابعاً: متغيرات الدراسة	**9**
ثامناً: منهجية الدراسة	**10**
تاسعاً: مجتمع وعينة الدراسة	**10**
عاشراً: حدود الدراسة	**10**
أحد عشر: مصطلحات الدراسة	**11**
الفصل الأول: ماهية الأمن السيبراني	***12***
أولاً: مفهوم الامن السيبراني	**12**
ثانياً: خصائص الأمن السيبراني	**14**
ثالثاً: أهداف الأمن السيبراني	**15**
رابعاً: أهمية الأمن السيبراني	**17**
خامساً: أبعاد الامن السيبراني	**18**
سادساً: سبل تفعيل الأمن السيبراني	**22**
سابعاً: القرارات والتشريعات المتعلقة بالامن السيبراني في سورية	**24**
ثامناً: اجراءات الأمن السيبراني في القطاع لمصرفي	**25**
تاسعاً: إطار حوكمة الأمن السيبراني في البنوك	**29**
الفصل الثالث: الدراسة الميدانية	**31**
أولاً: أداة الدراسة	**31**
ثانياً: تصميم الاستبانة	**31**

ثالثاً: اختبار ثبات الاستبانة	**32**
رابعاً: تحليل خصائص عينة الدراسة	**32**
خامساً: الإحصاءات الوصفية لمتغيرات الدراسة	**34**
سادساً: اختبار فرضيات الدراسة	***42***
النتائج والتوصيات	**53**
قائمة المراجع	**56**
الملحق رقم (1) استمارة استبيان	***58***

قائمة الجداول

الجدول رقم (1) نتائج اختبار Cronbach's Alpha _____ 32
الجدول رقم (2) توزع أفراد العينة وفقاً لمتغير المؤهل العلمي _____ 32
الجدول رقم (3) توزع أفراد العينة وفقاً لمتغير عدد سنوات الخبرة في العمل _____ 33
الجدول رقم (4) توزع أفراد العينة وفقاً لمتغير الموقع الوظيفي_____ 34
الجدول رقم (5) الأهمية النسبية للموافقات _____ 35
الجدول رقم (6) نتائج قياس الضوابط التقنية والفنية _____ 35
الجدول رقم (7) نتائج قياس حوكمة الأمن السيبراني _____ 37
الجدول رقم (8) نتائج قياس إدارة المخاطر السيبرانية _____ 38
الجدول رقم (9) نتائج قياس الوعي والتدريب الأمني _____ 39
الجدول رقم (10) نتائج قياس فاعلية حماية القطاع المصرفي (المرونة السيبرانية) _____ 41
الجدول رقم (11) الدلالة الإحصائية لاختبار العلاقة بين الأمن السيبراني وحماية القطاع المصرفي ___ 42
الجدول رقم (12) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة _____ 43
الجدول رقم (13) الدلالة الاحصائية لنموذج الدراسة لأثر الأمن السيبراني في حماية القطاع المصرفي _ 43
الجدول رقم (14) الدلالة الإحصائية لاختبار العلاقة بين الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي_____ 44
الجدول رقم (15) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة _____ 45
الجدول رقم (16) الدلالة الاحصائية لنموذج الدراسة لأثر الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي_____ 45
الجدول رقم (17) الدلالة الإحصائية لاختبار العلاقة بين حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي_____ 46
الجدول رقم (18) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة _____ 47
الجدول رقم (19) الدلالة الاحصائية لنموذج الدراسة لأثر حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي_____ 47
الجدول رقم (20) الدلالة الإحصائية لاختبار العلاقة بين إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي_____ 48
الجدول رقم (21) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة _____ 49
الجدول رقم (22) الدلالة الاحصائية لنموذج الدراسة لأثر إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي_____ 49
الجدول رقم (23) الدلالة الإحصائية لاختبار العلاقة بين الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي_____ 50
الجدول رقم (24) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة _____ 51

الجدول رقم (25) الدلالة الاحصائية لنموذج الدراسة لأثر الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي _____ 51

الإطار العام للدراسة

أولاً: المقدمة

شهد العالم خلال العقود الأخيرة تحولات جوهرية متسارعة نحو الاقتصاد الرقمي، الأمر الذي جعل البنية التحتية لتكنولوجيا المعلومات تشكل الركيزة الأساسية للأنشطة المالية والاقتصادية. وفي هذا الإطار، برز القطاع المصرفي بوصفه أحد أكثر القطاعات اعتماداً على النظم الرقمية، نظراً لدوره المحوري في حفظ الأصول وإدارة التدفقات المالية، مما جعله هدفاً رئيسياً للهجمات السيبرانية المتطورة والمتزايدة تعقيداً. ولم تعد حماية هذا القطاع مسألة تقنية بحتة، بل أصبحت ضرورة استراتيجية للحفاظ على الاستقرار المالي والاقتصادي، وتعزيز ثقة المتعاملين في المؤسسات المصرفية. ويمثل الأمن السيبراني (Cybersecurity) مجموعة من التقنيات والإجراءات والضوابط التنظيمية التي تهدف إلى حماية الأنظمة والشبكات والبرمجيات والبيانات من محاولات الاختراق أو التلف أو الوصول غير المصرح به. وفي القطاع المصرفي على وجه الخصوص.

ويُعد الأمن السيبراني خط الدفاع الأول لضمان استمرارية الأعمال المصرفية وحماية السيولة وصون الثقة العامة. إذ تعتمد الخدمات المصرفية الحديثة، مثل أنظمة الدفع الإلكتروني، والخدمات المصرفية عبر الإنترنت، وتطبيقات الهاتف المحمول، اعتماداً كلياً على بيئة رقمية آمنة وموثوقة. وأي اختراق ناجح لهذه البيئة لا يقتصر أثره على المصرف المعني فحسب، بل قد يمتد ليزعزع الثقة في النظام المالي ككل. وفي البيئة السوري، ومع صدور عدد من القرارات والتعليمات المركزية في الآونة الأخيرة، ولا سيما المتعلقة بإدارة الأمن السيبراني في المؤسسات المالية، إلى جانب تفعيل دور الهيئة الوطنية لخدمات تقانة المعلومات، تتزايد أهمية دراسة مدى التزام المصارف بهذه الإجراءات، وقياس فاعليتها في مواجهة التهديدات السيبرانية الداخلية والخارجية، بما يسهم في تعزيز متانة القطاع المصرفي وحماية استقراره.

ثانياً: الدراسات السابقة

الدراسات العربية

1- دراسة (كاظم، والمشهداني، 2025) بعنوان: التكنولوجيا المالية في ظل تحديات الأمن السيبراني ودورها في القطاع المصرفي[1].

هدفت الدراسة إلى بيان مفهوم التكنولوجيا المالية وبيان دور في تطوير وتحسين الخدمات المالية التي يقدمها القطاع المصرفي، وتسليط الضوء على التحديات التي تواجه المصارف العراقية في تطبيق التكنولوجيا المالية ولا سيما تحديات الأمن السيبراني، وبيان الفرص التي تتيحها التكنولوجيا المالية في تعزيز كفاءة القطاع المصرفي وجودة خدماته المالية، ولتحقيق اهداف الدراسة تم الاعتماد على المنهج الوصفي التحليلي، وتوصلت نتائج الدراسة إلى أن هناك دوراً للتكنولوجيا المالية في تحسين جودة وكفاءة الخدمات المصرفية من خلال تسريع العمليات وتقليل التكاليف مما يسهم في تحسين تجربة الزبائن، كما أن حوكمة الأمن السيبراني تؤدي دوراً هاماً في القطاع المصرفي.

2- دراسة (بوانة، 2023) بعنوان: أثر مخاطر الأمن السيبراني على استخدام البطاقات المصرفية في المصارف الإسلامية العاملة في الأردن[2].

هدفت الدراسة إلى تبيان الأثر المحتمل لمخاطر الأمن السيبراني (مخاطر أمن المعلومات، مخاطر تطبيقات الهاتف المحمول، المخاطر التشغيلية، مخاطر الهجمات السيبرانية) في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن، ولتحقيق أهداف الدراسة تم الاعتماد على منهج كمي وصفي تحليلي، واستخدمت الاستبانة لجمع البيانات من الإدارات العليا والوسطى والدنيا في الإدارات والاقسام المستهدفة في البنوك الإسلامية وعددهم (100) فرد، وباستخدام الاستراتيجيات الاحصائية الوصفية والاستدلالية وتوصلت نتائج

[1] كاظم، عمر علي حسين، والمشهداني، بشرى نجم عبد الله (2025)، التكنولوجيا المالية في ظل تحديات الأمن السيبراني ودورها في القطاع المصرفي، المؤتمر الدولي الخامس للعلوم الإدارية والمالية، جامعة بغداد، كلية الإدارة والاقتصاد، العراق.

[2] بوانة، سهيل (2023)، أثر مخاطر الأمن السيبراني على استخدام البطاقات المصرفية في المصارف الإسلامية العاملة في الأردن، رسالة ماجستير، جامعة الإسراء، الأردن.

الدراسة إلى وجود أثر معنوي لمخاطر الأمن السيبراني وأبعاده في استخدام البطاقات المصرفية في البنوك الإسلامية العاملة في الأردن.

3- دراسة (البغدادي، 2021) بعنوان: اقتصاديات الأمن السيبراني في القطاع المصرفي[3].

هدفت الدراسة إلى إبراز التحديات التي تواجه المجتمع من أجل تحقيق الأمن السيبراني بالتطبيق على المصارف المصرية، والذي يلعب دوراً محورياً في معالجة التحديات المستقبلية نظراً لاستخدامه كتكنولوجيا لإدارة الشبكات، الأمر الذي يساعد في تحقيق عدد من أهداف التنمية المستدامة كتحسين إدارة استخدام المعدات وصيانتها، وزيادة الإنتاج الزراعي وتوسيع نطاق الوصول إلى المعلومات المتعلقة بالتفاعل الاقتصادي بين المؤسسات الخاصة والعامة، ولتحقيق أهداف الدراسة تم الاعتماد على المنهج التحليلي والمقارن، وتوصلت نتائج الدراسة إلى أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالإنترنت يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات، كما أن التطور الحادث في المخاطر السيبرانية يحفز المؤسسات المالية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً امام مجالس إدارات تلك المؤسسات، الأمر الذي يؤدي إلى خلق حافز أكبر على الاستثمار بشكل مستمر في تحسين الأمن السيبراني.

الدراسات الأجنبية

1- دراسة (ENISA Threat Landscape, 2024) بعنوان:

ENISA Threat Landscape: Finance sector

مشهد التهديدات في وكالة ENISA: القطاع المالي [4]

هدفت الدراسة إلى توفير رؤى عميقة حول التهديدات السيبرانية التي تستهدف القطاع المالي الأوروبي، وتحديد نقاط الضعف الرئيسية، وقياس تأثير الحوادث المبلغ عنها خلال الفترة 2023-2024. وقد تم اختيار هذا القطاع لأهميته الحرجة للمواطنين الأوروبيين والاستقرار المالي. اعتمدت الدراسة المنهج الوصفي التحليلي

[3] البغدادي، مروة فتحي السيد (2021)، اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، العدد 76، مصر.
[4] European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape: Finance sector. Available at: https://www.enisa.europa.eu/sites/default/files/2025

بالاعتماد على تحليل 488 حادثة تم الإبلاغ عنها علنًا وتؤثر على القطاع المالي في أوروبا. وعلى وجه الخصوص في هولندا وقد شمل التحليل تصنيف أنواع الحوادث، الضحايا المستهدفين، ودوافع الهجمات (مالية، سياسية، إلخ). وقد تم جمع البيانات بالتعاون مع السلطات الوطنية المختصة (NCAs) والمصادر المفتوحة. ركز التقرير على الحوادث التي تؤثر على القطاع المالي الأوروبي. وبينت الدراسة أن الضحايا الأكثر تكرارًا: كانت البنوك الأوروبية (مؤسسات الائتمان) هي الأكثر تضررًا، حيث شكلت 46% من إجمالي الحوادث المرصودة (301 حادثة). وكانت هجمات الفدية تؤثر بشكل أساسي على مزودي الخدمات ومنظمات التأمين. أما البرامج الضارة (مثل أحصنة طروادة المصرفية وبرامج التجسس) فقد أثرت على مؤسسات الائتمان (36%) والأفراد (24%).

2- دراسة (Amato et al, 2024) بعنوان:

Cyber risk management in the financial sector: An evaluation of current practices in modern scenarios.

(إدارة المخاطر السيبرانية في القطاع المالي: تقييم للممارسات الحالية في السيناريوهات الحديثة)[5]

هدفت الدراسة إلى استكشاف الممارسات الحالية التي تتبناها المؤسسات المالية لإدارة وتخفيف المخاطر السيبرانية في ظل التحول الرقمي المتسارع، وتحديد الثغرات بين النفقات المرتفعة على الأمن السيبراني والقياس الفعلي لفعالية هذه الاستثمارات في تقليل المخاطر. تم إجراء دراسة نظرية/تحليلية مستندة إلى بيانات وتقارير عالمية مع إشارة خاصة إلى الاتجاهات في الولايات المتحدة والاتحاد الأوروبي حيث تتركز غالبية الأبحاث والتشريعات. وقد توصلت الدراسة إلى التكلفة العالية للمخالفات: بلغ متوسط تكلفة اختراق البيانات في القطاع المالي 5.9 مليون دولار أمريكي في عام 2023، وهو أعلى بكثير من المتوسط العالمي، مما يؤكد الحاجة الملحة للإدارة الفعالة للمخاطر. وعلى الرغم من أن 96% من المؤسسات المالية العالمية زادت ميزانيات الأمن السيبراني بعد جائحة كورونا، إلا أن القليل منها لديه مقاييس واضحة وموحدة لقياس مدى فاعلية هذه الضوابط

[5] Amato, E., Fraudatario, M. C., & Bernaschi, D (2024). Cyber risk management in the financial sector: An evaluation of current practices in modern scenarios. Journal of Finance and Management (Volume,2 Issues 4)

في تقليل المخاطر الفعلية. وتشمل التحديات المتزايدة التهديدات الداخلية ومخاطر سلسلة التوريد خاصة مع تزايد الاعتماد على الحوسبة السحابية والذكاء الاصطناعي (AI).

3- دراسة (Smith, 2023) بعنوان:

"**Artificial Intelligence for Cybersecurity: A Systematic Review of Recent Developments and Future Trends.**

"الذكاء الاصطناعي للأمن السيبراني: مراجعة منهجية للتطورات الأخيرة والاتجاهات المستقبلية.[6]

هدفت الدراسة إلى تحليل أحدث التطورات في استخدام الذكاء الاصطناعي (AI) لتحسين الأمن السيبراني، في المصارف النيجيرية مع التركيز على التعلم الآلي (ML) والكشف عن التهديدات، تم إجراء مراجعة منهجية لأكثر من 100 دراسة بين 2020-2023، مع تحليل مقارن لتقنيات الذكاء الاصطناعي المستخدمة، وبينت الدراسة أن الذكاء الاصطناعي يحسن كشف التسلل بنسبة تصل إلى 30% مقارنة بالطرق التقليدية، وأن نماذج التعلم العميق (Deep Learning) فعالة في تحديد البرمجيات الخبيثة غير المعروفة سابقاً.

4- دراسة (Lee, 2023) بعنوان:

Enhancing Cyber Threat Intelligence with Machine Learning

تعزيز استخبارات التهديدات السيبرانية باستخدام التعلم الآلي[7]

هدفت الدراسة إلى تقييم قدرة خوارزميات ML على اكتشاف هجمات Zero-Day. من خلال إجراء تجارب معملية باستخدام خوارزميات Random Forest وGANs على مجموعة بيانات حديثة، تم الاعتماد على المنهج الوصفي التحليلي، وبينت الدراسة أن نموذج Random Forest حقق دقة 95% في كشف الهجمات الجديدة. وقد أظهرت الدراسة أن البعد التقني والأمني وتوفر التدريب والتوعية كان لها أثر كبير في تعزيز الاستخبارات السيبرانية.

[6] Smith, J. et al (2023) "Artificial Intelligence for Cybersecurity: A Systematic Review of Recent Developments and Future Trends , IEEE Access, vol2, no1.

[7] Lee, H. & Kumar, R (2023) "Enhancing Cyber Threat Intelligence with Machine Learning: A Case Study on Zero-Day Attacks "Computers & Security, vol1, no4

5- دراسة (Latif, 2022) بعنوان:

Cyber Security Analysis of Internet Banking in Emerging Countries – User and Bank Perspectives

(تحليل الأمن السيبراني للخدمات المصرفية عبر الإنترنت في البلدان الناشئة – من منظور المستخدم والبنك)[8]

هدفت الدراسة إلى تحليل مستوى الوعي الأمني لدى مستخدمي الخدمات المصرفية عبر الإنترنت وتحديد مواقفهم السلوكية تجاه المخاطر السيبرانية، واقتراح نموذج لسد الفجوة بين توقعات البنوك واستجابة المستخدمين السلوكية لتعزيز بيئة مصرفية إلكترونية أكثر أمانًا. تم تصميم استبيان لجمع البيانات من عينة من المستخدمين في ثلاث دول ناشئة. تم تقسيم الاستبيان إلى جزأين: الممارسات العامة للمستخدمين في الخدمات المصرفية عبر الإنترنت ووعيهم بالتهديدات ذات الصلة. واستخدمت الدراسة التحليل العاملي والانحدار لتحليل تأثير العوامل المختلفة على ثقة العملاء. تم اختيار عينة من المستخدمين من المملكة العربية السعودية، الهند، وباكستان. وتوصلت الدراسة إلى أن العوامل المؤثرة على الثقة: وجد أن جودة الخدمة المقدمة على الموقع الإلكتروني كان لها التأثير الأكبر على بناء ثقة العميل في الخدمات المصرفية عبر الإنترنت. وأن إدارة المخاطر السيبرانية تلعب دوراً هاماً في الاتجاه نحو الأمن السيبراني، ولا يزال اعتماد المستخدمين للتكنولوجيا يمثل التحدي الأكبر للقطاع المصرفي، حيث يؤثر مستوى التعليم والمعرفة الحاسوبية للمستخدمين بشكل كبير على تقبلهم لفوائد وسهولة استخدام الخدمات الإلكترونية.

التعقيب على الدراسات السابقة

تشابهت الدراسة الحالية مع الدراسات السابقة من حيث المنهج المتبع وهو المنهج الوصفي التحليلي ومن حيث الهدف في بيان أهمية الأمن السيبراني في القطاع المصرفي، وقد اختلفت عنها من حيث الحدود المكانية حيث أتت الدراسة الحالية للإسقاط على البيئة السورية بشكل عام والمصارف الخاصة السورية بشكل خاص.

[8] Latif, G. (2022). Cyber Security Analysis of Internet Banking in Emerging Countries - User and Bank Perspectives., vol 2, no 1.

وقد تشابهت الدراسة مع دراسة (Lee, 2023) في أهمية البعد التقني والأمني وتوفر الوعي والتدريب في تعزيز الأمن السيبراني، كما تشابهت مع دراسة (Latif, 2022) و دراسة (Amato et al, 2024) في أهمية إدارة المخاطر السيبرانية في تعزيز الأمن السيبراني، بينما تفردت الدراسة الحالية بتأثير حوكمة الأمن السيبراني في حماية القطاع المصرفي.

وقد اختلفت عنها من حيث شمولية المتغيرات المدروسة حيث تناولت الدراسة الحالية متغيرات أعم واشمل من المتغيرات التي تناولتها الدراسات السابقة.

ثالثاً: مشكلة الدراسة

يمثل القطاع المصرفي في سورية أحد أهم الركائز الاقتصادية، ورغم التحديات الكبيرة التي واجهها خلال السنوات الماضية كشح السيولة، أزمة الثقة بين المودعين والمصارف، وتأثير العقوبات الاقتصادية على البنية التحتية والتعاملات الدولية (مثل نظام سويفت) فإنه يبذل جهوداً واضحة للتحول نحو الرقمنة. هذا القطاع يشمل المصارف العامة والخاصة، والتي تسعى جميعها لتقديم خدمات إلكترونية جديدة تماشياً مع متطلبات الاقتصاد الرقمي، مما يوسع من مساحة تعرضها للمخاطر السيبرانية. بالتالي، فإن خصوصية هذا القطاع، المتمثلة في محاولته للنهوض والتطور التكنولوجي ضمن بيئة اقتصادية صعبة، تجعل دراسة الأمن السيبراني فيه أمراً بالغ الأهمية لضمان عدم تحول هذه الجهود إلى نقاط ضعف جديدة يمكن استغلالها من قبل المهاجمين.

وعليه تتمثل مشكلة الدراسة في الإجابة على التساؤل الآتي:

ما دور الأمن السيبراني في حماية القطاع المصرفي في سوريا؟

ويتفرع عنها التساؤلات الفرعية الآتية:

1- ما دور الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا؟
2- ما دور حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا؟
3- ما دور إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا؟
4- ما دور الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا؟

رابعاً: فرضيات الدراسة

الفرضية الرئيسية: يوجد دور ذو دلالة معنوية للأمن السيبراني في حماية القطاع المصرفي في سوريا.

يتفرع عنها الفرضيات الآتية:

1- يوجد دور ذو دلالة معنوية للضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.
2- يوجد دور ذو دلالة معنوية لحوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.
3- يوجد دور ذو دلالة معنوية لإدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.
4- يوجد دور ذو دلالة معنوية للوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

خامساً: أهمية الدراسة

تتمثل الأهمية العلمية (الأكاديمية) للدراسة في إثراء المعرفة الأكاديمية في مجال الأمن السيبراني والإدارة المصرفية من خلال سد الفجوة المعرفية إذ تُعد الدراسة إضافة نوعية للمكتبة العربية والعالمية في مجال الأمن السيبراني، خاصة في بيئات الدول التي تمر بظروف استثنائية (صراعات، وعقوبات)، حيث تندر الدراسات التي تتناول تطبيق المعايير الأمنية المصرفية الدولية في ظل هذه القيود المعقدة.

كما تتمثل الأهمية العملية (التطبيقية) بما تقدمه الدراسة من نتائج وتوصيات ذات قيمة عملية مباشرة للجهات المعنية في سورية من خلال تزويد مصرف سورية المركزي ومجلس النقد والتسليف والهيئة الناظمة لقطاع الاتصالات ببيانات موثوقة وموضوعية حول نقاط الضعف ومستويات النضج السيبراني في القطاع، مما يدعم جهودهم في صياغة وإصدار تشريعات وضوابط أمنية أكثر فاعلية وواقعية وملاءمة للظروف الراهنة.

سادساً: أهداف الدراسة

هدفت الدراسة إلى بيان دور الأمن السيبراني في حماية القطاع المصرفي في سوريا، وذلك من خلال:

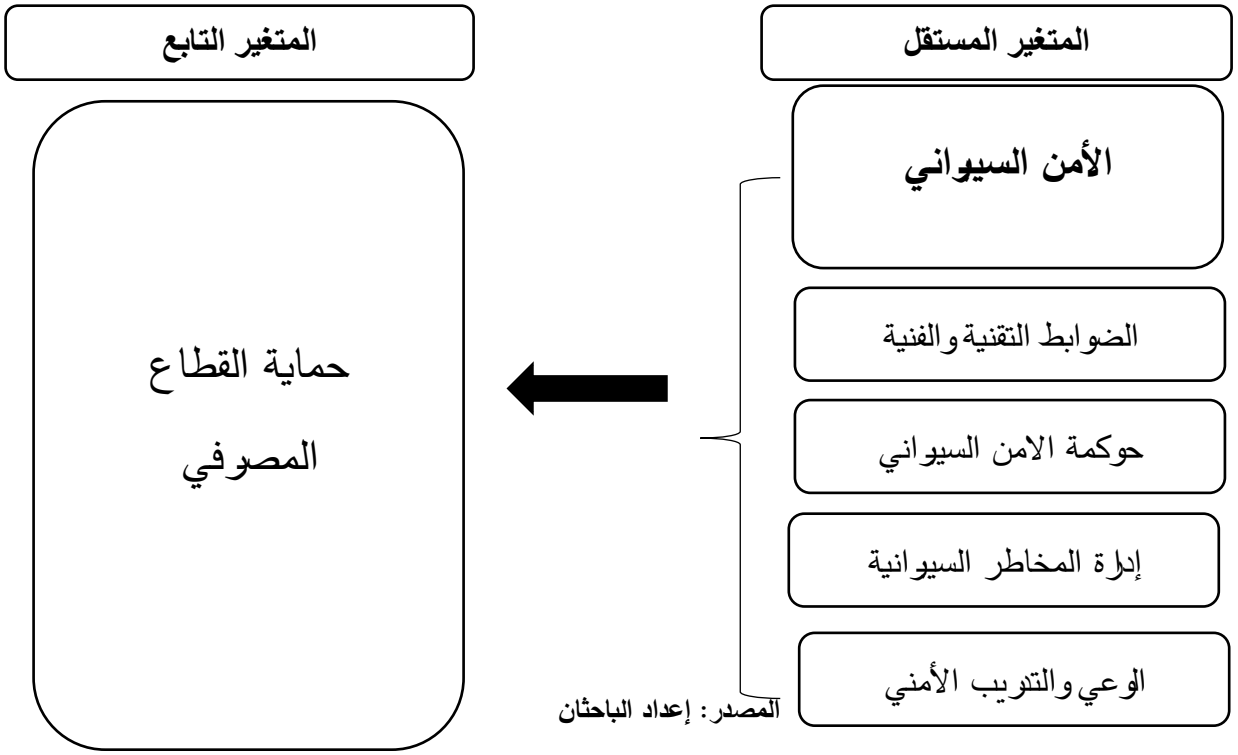
1- بيان دور الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.
2- بيان دور حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.
3- بيان دور إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.
4- بيان دور الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

سابعاً: متغيرات الدراسة

المتغير المستقل: الأمن السيبراني(Cybersecurity) (الضوابط التقنية والفنية، حوكمة الأمن السيبراني، إدارة المخاطر السيبرانية، الوعي والتدريب الأمني)

المتغير التابع: حماية القطاع المصرفي

الشكل رقم (1) أنموذج الدراسة



المصدر: إعداد الباحثان

ثامناً: منهجية الدراسة

تم الاعتماد على المنهج الوصفي التحليلي، من خلال الاطلاع على الدراسات السابقة العربية والأجنبية التي تناولت الموضوع لإعداد الجانب النظري للدراسة، والاعتماد على الاستبانة في جمع البيانات، من أجل إعداد الدراسة الميدانية.

تاسعاً: مجتمع وعينة الدراسة

ضم مجتمع الدراسة العاملين لدى المصارف الخاصة السورية وتم أخذ عينة عشوائية من العاملين في مناصب وظيفية مختلفة.

عاشراً: حدود الدراسة

الحدود المكانية: المصارف التقليدية الخاصة السورية في مدينة دمشق.

الحدود الزمانية: تمت الدراسة خلال العام 2025-2026م

الحدود البشرية: العاملين في المصارف التقليدية الخاصة السورية في مدينة دمشق.

الحدود الموضوعية: تناولت الدراسة متغيرين هما (المتغير المستقل: الامن السيبراني)، و(المتغير التابع: حماية القطاع المصرفي).

أحد عشر: مصطلحات الدراسة

الأمن السيبراني: النشاط الذي يضمن حماية الموارد البشرية والمالية المتعلقة بتقنيات الاتصالات والمعلومات، ويضمن القدرة على التعافي من الخسائر والأضرار الناتجة عن مخاطر وتهديدات محتملة، مما يسمح بإعادة الوضع الطبيعي في أسرع وقت ممكن[9].

حماية القطاع المصرفي: إطار شامل يهدف إلى ضمان سلامة واستقرار النظام المالي ككل، وحماية مصالح جميع الأطراف المعنية، وأبرزهم العملاء (المودعين والمقترضين) والمؤسسات المصرفية نفسها، وكذلك الاقتصاد الوطني. يندرج هذا المفهوم تحت مظلة أوسع تسمى حماية المستهلك المالي (أو العميل المصرفي)، بالإضافة إلى الجهود الرقابية والتشريعية التي تضمن متانة البنوك.[10]

[9] الحجرف، حسن نايف مبارك (2024)، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية، مجلة الدراسات الجامعية للبحوث الشاملة، المجلد 5، العدد 32، العراق، ص14081.

[10] Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(03), 1542-1556. , p 1544

الفصل الأول: ماهية الأمن السيبراني

شهد القطاع المصرفي العالمي تحولاً جذرياً نحو الرقمنة الشاملة، مما أسفر عن خدمات مالية مبتكرة وسهولة غير مسبوقة في الوصول إلى الأموال. ومع هذا التطور الهائل، أصبح البنك الحديث بمثابة بنية تحتية رقمية متكاملة تدير مليارات الدولارات وتخزن كميات هائلة من البيانات الشخصية الحساسة. إن هذه الرقمنة، رغم مزاياها، جعلت القطاع المصرفي هدفاً رئيسياً وذا قيمة عالية للمجرمين السيبرانيين والدول المارقة. فالهجمات السيبرانية لم تعد مجرد تهديد تقني، بل أصبحت مخاطر وجودية يمكن أن تؤدي إلى خسائر مالية فادحة، وتعطيل للأنظمة الحيوية، وفقدان كارثي لثقة العملاء والمستثمرين، بل وتهديد للاستقرار الاقتصادي ككل. في هذا السياق، لم يعد الأمن السيبراني مجرد رفاهية إضافية أو وظيفة تقتصر على قسم تكنولوجيا المعلومات، بل تحول إلى ركيزة استراتيجية أساسية لاستمرارية الأعمال وامتثالها للوائح الدولية. يهدف هذا المبحث إلى استكشاف ماهية الأمن السيبراني في القطاع المصرفي، وذلك بتعريف مفاهيمه الأساسية، وتحديد أبرز التحديات التي يواجهها، وتفصيل المنظومة المتكاملة من الضوابط التقنية، والحوكمة، وإدارة المخاطر، والوعي الأمني التي تشكل مجتمعة الدرع الواقي لهذا القطاع الحيوي.

أولاً: مفهوم الامن السيبراني

يُعد الأمن السيبراني (Cybersecurity) مفهومًا واسعًا ومتطورًا يتناول حماية الأنظمة الرقمية والمعلومات والشبكات من التهديدات والهجمات الإلكترونية. ويختلف تعريفه وتأثيره حسب وجهة النظر التي يتم تناوله منها.

يركز المنظور التقني على التكنولوجيا والإجراءات المتخذة لحماية المكونات الأساسية للنظام وهو ممارسة حماية أجهزة الحاسوب، الخوادم، الأجهزة المحمولة، الأنظمة الإلكترونية، الشبكات، والبيانات من الهجمات الرقمية التي تهدف عادةً إلى الوصول غير المصرح به، التغيير، الإتلاف، أو السرقة. [11]

[11] Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(03), 1542-1556. , p 1544

أما المنظور المؤسسي يهتم بكيفية تأثير الأمن السيبراني على استدامة الأعمال، والامتثال القانوني، وسمعة الشركة وهو مجموعة السياسات والإجراءات والتقنيات التي تضمن استمرارية العمليات التجارية وحماية الأصول المعلوماتية للمؤسسة، والالتزام باللوائح والمعايير التنظيمية[12] .

ينظر المنظور الحكومي إلى الأمن السيبراني كجزء من الأمن القومي للدولة ويتمثل بحماية البنية التحتية الحيوية للدولة (مثل شبكات الكهرباء، الاتصالات، النقل، الأنظمة المالية) والأنظمة الحكومية من الحروب السيبرانية، التجسس السيبراني، والإرهاب الإلكتروني[13].

بينما يركز المنظور البشري على الفرد ودوره في سلسلة الأمن السيبراني وهو الوعي والممارسات التي يتبعها المستخدمون لحماية هوياتهم الرقمية، أجهزتهم الشخصية، وبياناتهم الخاصة عبر الإنترنت[14].

كما يعرف بأنه مجموعة من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام من قبل غير المصرح له على شبكات الكمبيوتر، أو سوء الاستغلال واستعادة المعلومات الإلكترونية التي تحتويها بهدف ضمان واستمرارية عمل نظم المعلومات، وتأمين حماية وسرية وخصوصية البيانات الخاصة بفواعل الفضاء السيبراني، وعليه فهو المجال المتعلق بالإجراءات ومقاييس ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو للحد من آثارها في أقصى وأسوأ الأحوال[15].

كما يعرف الأمن السيبراني أنه مفهوم حديث نسبيا تم استحداثه في إطار الثورة الرقمية والتكنولوجيا المعاصرة والتي تسببت في تضخم وانتقال المعلومات والبيانات بين العديد من وسائل الاتصال عبر الأجهزة الرقمية المختلفة، وعلى ذلك يهتم الأمن السيبراني بالجانب الأمني لحماية انتقال المعلومات والبيانات بين الوسائل الرقمية المختلفة. ويرجع التنوع في المفاهيم المفسرة للأمن السيبراني إلى إعتماد سياسات الأمن السيبراني على

---

[12] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536., p 1534

[13]Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16., p 2

[14] Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643., p 630

[15] جيلالي، دلالي، وبلبشير، يعقوب (2021)، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، السنة العاشرة، العدد 1، الكويت، ص536.

شقين أساسين هما الجانب التقني والجانب التنظيمي. وتأثير ذلك على جوانب الوعي والتطبيق اللازم لجميع الأفراد[16].

ثانياً: خصائص الأمن السيبراني

تستند خصائص الأمن السيبراني ومبادئه إلى حماية الأصول المعلوماتية والرقمية بشكل شامل وفعّال. وتُعرف الخصائص الأساسية التي يسعى الأمن السيبراني لتحقيقها بالنموذج الشهير (CIA Triad) حيث يشكل نموذج CIA Triadحجر الزاوية في أي استراتيجية للأمن السيبراني، حيث يحدد الأهداف الرئيسية التي يجب أن يحققها النظام لحماية البيانات: [17]

1- السرية(Confidentiality) ضمان أن تكون البيانات والمعلومات متاحة فقط للأشخاص أو الكيانات المصرح لها بالوصول، منع التسريب، التجسس، وسرقة البيانات الحساسة. يتم تطبيقها من خلال: التشفير، ضوابط الوصول، والمصادقة متعددة العوامل.
2- السلامة/النزاهة(Integrity) ضمان دقة واكتمال البيانات ومنع أي تعديل أو حذف غير مصرح به للبيانات، سواء كان عرضيًا أو مقصودًا والتأكد من أن البيانات موثوقة ولم يتم التلاعب بها. يتم تطبيقها من خلال: التوقيعات الرقمية، والنسخ الاحتياطي.
3- التوافر (Availability) ضمان قدرة المستخدمين المصرح لهم على الوصول إلى الأنظمة والموارد والبيانات عند الحاجة إليها دون انقطاع، الحفاظ على استمرارية العمليات التجارية والخدمات. يتم تطبيقها من خلال: التكرار، النسخ الاحتياطي والاسترداد من الكوارث، والحماية من هجمات حجب الخدمة .

إلى جانب مثلثCIA ، هناك خصائص إجرائية وتنظيمية تميز الأمن السيبراني وهي:

1- الاستمرارية والمرونة: فالمرونة هي قدرة النظام على تحمل الهجمات أو الأعطال والاستمرار في العمل جزئياً أو العودة للعمل بسرعة بعد وقوع الهجوم. الأمن السيبراني لا يهدف فقط إلى منع الهجمات، بل

[16] كاعوه، عبير أحمد علي (2020)، سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية، مجلة دراسات تربوية واجتماعية، المجلد السادس والعشرين، الجزء الثالث، مصر، ص165.

[17] Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(03), 1542-1556. , p 1544

أيضاً إلى تحملها. كما أن استمرارية الأعمال هي وضع خطط واضحة لضمان أن الوظائف الحيوية للمؤسسة يمكن أن تستمر في العمل خلال وبعد وقوع حادث أمني كبير.

2- الأمن السيبراني خاصية مستمرة، حيث يجب تقييم المخاطر بشكل دوري وتحديد الثغرات ونقاط الضعف المحتملة. تستخدم المنهجية الدفاعية وتطبيق إجراءات أمنية بناءً على مستوى المخاطر المقبولة للمؤسسة، وليس مجرد تطبيق ضوابط عشوائية.

3- ضمان عدم قدرة طرف على إنكار تصرف قام به لاحقاً (مثلاً، عدم قدرة مستخدم على إنكار إرسال رسالة أو إجراء معاملة). يتم تحقيقه عادةً عبر التوقيعات الرقمية وسجلات التدقيق.

4- يجب أن تكون جميع الإجراءات والمعاملات مسجلة ومحفوظة بطريقة تسمح بتحليلها والتحقيق فيها بعد وقوع حادث أمني لتحديد كيفية حدوث الاختراق والجهة المسؤولة.

ثالثاً: أهداف الأمن السيبراني

اهتمت جميع الحكومات والمؤسسات في السنوات الماضية بالتخطيط لسياسات الأمن السيبراني، وذلك لما يحققه من العديد من الأهداف الهامة وتوفير بيئة آمنة يستطيع المستخدم الوثوق بها، وتوفير حماية للأجهزة الرقمية المستخدمة، وتقليل التهديدات والجرائم السيبرانية، كذلك مقاومة البرمجيات الخبيثة وما تسببه من إحداث أضرار لأنظمة المعلومات، وإن فرص الوقوع كضحية للجرائم السيبرانية تزداد في ضوء غياب الوعي الكافي وانتشار وتزايد الاعتماد على استخدام شبكة الإنترنت عبر العديد من الأجهزة الرقمية ورغبة الحكومات والمؤسسات في التحول الرقمي لها، كذلك الحفاظ على سرية وخصوصية جميع الوثائق والبيانات الرقمية، وضمان توافر استمرارية سير وعمل النظم الرقمية، وتوفير الحماية اللازمة للمواطنين والبني التحتية الهامة للدولة[18]. ويمكن تلخيص أهم أهداف الأمن السيبراني في كل من[19]:

1- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.

[18] كاعوه، عبير أحمد علي (2020)، سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية، مجلة دراسات تربوية واجتماعية، المجلد السادس والعشرين، الجزء الثالث، مصر، ص171.

[19] البردان، محمد فوزي أمين، وشحاته، محمد موسى علي (2020)، أثر تفعيل حوكمة تكنولوجيا المعلومات في ظل إستراتيجيات الرقمنة على الحد من مخاطر الهجمات السيبرانية بالبيئة المصرية، جامعة مدينة السادات، كلية التجارة، مصر، ص10.

2- التصدي لهجمات وحوادث مخاطر الهجمات السيبرانية التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

3- توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات وعصر الرقمنة.

4- صمود البني التحتية الحساسة للهجمات الإلكترونية.

5- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.

6- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.

7- سد ومعالجة الثغرات في أنظمة أمن المعلومات.

8- مقاومة البرمجيات الخبيثة، ما تستهدفه من أحداث أضرار بالغة للمستخدمين.

9- حد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

10- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حد سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة.

11- تدريب الأفراد على آليات وإجراءات جديدة لمواجهة التحديات الخاصة باختراق أجهزتهم التقنية بقصد الضرر بمعلوماتهم الشخصية سواء بالإتلاف أو بقصد السرقة.

12- حماية الأصول: حماية البيانات الحساسة للعملاء والملكية الفكرية والأسرار التجارية.

13- الالتزام بالقوانين واللوائح المحلية والدولية) مثل لائحة حماية البيانات العامة لتجنب الغرامات والعقوبات.

14- تقييم المخاطر السيبرانية وتطوير خطط الاستجابة للطوارئ لمواجهة أي اختراقات محتملة وتقليل الضرر.

15- تعزيز الثقة: بناء ثقة العملاء والشركاء من خلال إظهار القدرة على حماية بياناتهم.

16- التعاون الدولي: بناء شراكات دولية لمكافحة الجريمة السيبرانية العابرة للحدود.

17- تقليل الخطأ البشري: بما أن العديد من الهجمات تبدأ بخطأ من المستخدم، فإن هذا المنظور يشدد على أن الأشخاص هم خط الدفاع الأول والأخير في الأمن السيبراني[20].

[20] Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(03), 1542-1556. , p 1544

رابعاً: أهمية الأمن السيبراني

أهمية الأمن السيبراني في المصارف أمرًا بالغ الحساسية، حيث تشكل المصارف والقطاع المالي هدفًا رئيسيًا للهجمات الإلكترونية نظرًا لطبيعة الأصول التي تديرها (الأموال، والبيانات المالية الحساسة). يمثل الأمن السيبراني بالنسبة للمصارف عمودًا فقريًا يضمن الثقة والاستقرار التشغيلي والامتثال القانوني.

تتجلى أهمية الأمن السيبراني للمؤسسات المصرفية في النقاط التالية[21] :

1- حماية الأصول المالية والبيانات الحساسة

أ- حماية الأموال: الهدف الأولي هو منع الخسائر المالية المباشرة الناتجة عن عمليات الاحتيال المالي، وسرقة الأموال من حسابات العملاء، أو التحويلات غير المصرح بها) مثل هجمات .SWIFT

ب-تأمين بيانات العملاء: تقوم البنوك بتخزين كميات هائلة من البيانات الشخصية والمالية الحساسة بما في ذلك أرقام الحسابات، وتفاصيل بطاقات الائتمان، ومعلومات الهوية. حماية هذه البيانات من التسريب أو الاختراق هو أمر أساسي للحفاظ على السرية.

2- ضمان الثقة والمصداقية

أ- بناء ثقة العميل: يعتبر الأمن هو أساس العلاقة بين المصرف والعميل. أي اختراق كبير يؤدي إلى فقدان ثقة الجمهور بشكل سريع، مما قد يدفع العملاء لسحب أموالهم والبحث عن مؤسسات أكثر أمانًا.

ب-حماية السمعة: الهجمات السيبرانية الناجحة تضر بسمعة البنك على المدى الطويل، وتؤثر سلبًا على سعر أسهمه وقيمته السوقية.

3- الحفاظ على استمرارية العمليات:

أ- التوافر المستمر للخدمات: تعتمد البنوك بشكل كلي على الأنظمة الرقمية لتقديم خدماتها (التحويلات، الصراف الآلي، الخدمات المصرفية عبر الإنترنت). الأمن السيبراني يضمن التوافر المستمر لهذه الخدمات والحماية من هجمات حجب الخدمة التي تهدف إلى شل العمليات.

[21] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536., p 1534

ب–الاسترداد من الكوارث: تضمن استراتيجيات الأمن السيبراني وجود خطط فعالة لاستعادة الأنظمة والبيانات بسرعة بعد أي حادث أمني أو عطل، مما يضمن استمرارية الأعمال دون انقطاع كبير.

4– الالتزام باللوائح والمعايير:

أ– الامتثال التنظيمي: تخضع المصارف لرقابة مشددة من الهيئات المالية المركزية والدولية) مثل البنوك المركزية، ولوائح حماية البيانات العامة يتطلب الامتثال لهذه اللوائح تطبيق معايير أمنية صارمة وإجراء تدقيقات مستمرة.

ب–تجنب العقوبات: عدم الالتزام بمعايير الأمن السيبراني يؤدي إلى غرامات مالية ضخمة وعقوبات قانونية تفرضها الجهات الرقابية.

5– مكافحة الجرائم المالية المنظمة: تلعب أنظمة الأمن السيبراني دورًا حيويًا في مراقبة وتحليل المعاملات المالية للكشف عن الأنشطة المشبوهة التي قد تكون مرتبطة بغسيل الأموال أو تمويل الإرهاب وبالتالي دعم الجهود الوطنية والدولية لمكافحة الجريمة[22] .

خامساً: أبعاد الامن السيبراني

يشمل الأمن السيبراني مجموعة من الأبعاد المتكاملة التي تتجاوز الجانب التقني إلى جوانب أخرى حيوية، لأنه يؤثر على جميع نواحي الحياة الحديثة. ويمكن تلخيص أبعاد الأمن السيبراني الرئيسية في الآتي[23]:

البعد الأمني والتقني:

هذا هو البعد الأساسي والأكثر وضوحًا، ويركز على حماية الأنظمة والبيانات. وأمن البنية التحتية الحساسة: حماية شبكات الاتصالات، الطاقة، النقل، والأنظمة المالية. وأمن المعلومات: ضمان السرية والتكامل والتوافر وأمن الشبكات: استخدام جدران الحماية، وأنظمة كشف التسلل، والشبكات الافتراضية الخاصة. وأمن التطبيقات

[22] Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643., p 630

[23] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536., p 1526

والسحابة وإنترنت الأشياء: حماية البرمجيات والأجهزة الذكية والسحابات التخزينية. كذلك المرونة السيبرانية وتشمل القدرة على الصمود والاستجابة السريعة واستعادة العمل بعد وقوع هجوم سيبراني. [24]

يعد البعد التقني للأمن السيبراني جانب أساسي من جوانب الأمن السيبراني الشامل، ويركز على استخدام التقنيات والأدوات والعمليات لحماية الأصول الرقمية وأنظمة المعلومات من التهديدات السيبرانية. يشمل هذا البعد مجموعة واسعة من الممارسات والتقنيات المصممة لضمان السرية والنزاهة والتوافر للبيانات والأنظمة، وتتمثل بعض الجوانب الرئيسية للبعد التقني بالآتي: [25]

1- حماية الشبكات: يشمل ذلك تطبيق جدران الحماية، وأنظمة كشف التسلل والوقاية منه، وتقنيات تجزئة الشبكة، والشبكات الخاصة الافتراضية (VPNs) لتأمين الاتصالات ومنع الوصول غير المصرح به إلى الشبكات.
2- أمن الأجهزة: يتضمن تأمين نقاط النهاية مثل أجهزة الكمبيوتر المحمولة والأجهزة المكتبية والخوادم والأجهزة المحمولة من خلال تطبيق برامج مكافحة الفيروسات، وبرامج مكافحة البرامج الضارة، وإدارة التصحيح، وتكوين الأجهزة الآمن.
3- أمن البرمجيات: يركز على تطوير وتأمين التطبيقات والبرامج من خلال ممارسات الترميز الآمن، واختبار الاختراق، وتحليل الثغرات الأمنية، وإدارة دورة حياة التطوير الآمن (SDLC).
4- أمن البيانات: يشمل حماية البيانات الحساسة من خلال التشفير، والتحكم في الوصول، ومنع فقدان البيانات (DLP)، وإخفاء البيانات، والتدمير الآمن للبيانات.
5- إدارة الهوية والوصول (IAM): يتضمن إنشاء وإدارة هويات المستخدمين والتحكم في وصولهم إلى الموارد والأنظمة بناءً على مبادئ الامتياز الأقل والمصادقة متعددة العوامل (MFA).
6- الاستجابة للحوادث: يشمل تطوير وتنفيذ خطط للاستجابة للحوادث الأمنية، بما في ذلك تحديد الحوادث واحتوائها والقضاء عليها والتعافي منها وتحليلها.

[24] Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(03), 1542-1556. , p 1544

[25] الحجرف، حسن نايف مبارك (2024)، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية، مجلة الدراسات الجامعية للبحوث الشاملة، المجلد 5، العدد 32، العراق، ص14081.

7- المراقبة والتحليل الأمني: يتضمن جمع وتحليل السجلات الأمنية والأحداث لتحديد الأنشطة المشبوهة والاستجابة للتهديدات المحتملة في الوقت الفعلي. غالبًا ما يتم تحقيق ذلك باستخدام أنظمة إدارة معلومات الأمان والأحداث (SIEM).

8- التشفير: تستخدم تقنيات التشفير لتحويل البيانات إلى تنسيق غير قابل للقراءة، مما يضمن سريتها أثناء النقل وأثناء التخزين.

9- تقنيات المصادقة: تتحقق هذه التقنيات من هويات المستخدمين قبل منحهم حق الوصول إلى الأنظمة أو البيانات. تشمل الأمثلة كلمات المرور والرموز البيومترية والشهادات الرقمية.

10- النسخ الاحتياطي والاسترداد: تتضمن إنشاء نسخ احتياطية منتظمة للبيانات والأنظمة لضمان إمكانية استعادتها في حالة وقوع حادث أمني أو فشل في النظام.

البعد السياسي والقانوني

يتعلق هذا البعد بتنظيم الفضاء السيبراني على مستوى الدولة والمجتمع الدولي. يشمل البعد القانوني والتنظيمي: سن القوانين والتشريعات لمكافحة الجرائم الإلكترونية، وحماية البيانات الشخصية، وتحديد المسؤوليات. وتشمل السيادة الرقمية قدرة الدولة على التحكم في بياناتها وأنظمتها داخل حدودها السيبرانية. والحوكمة الرقمية وضع الأطر والسياسات التي تحكم استخدام وتطوير التكنولوجيا بشكل آمن وأخلاقي[26] . كما يتطلب التطور التكنولوجي السريع الامتثال للتشريعات من خلال تحسين الأطر القانونية للتعامل مع الأنشطة القانونية وغير القانونية على الإنترنت، حيث تعتبر الجرائم الإلكترونية في الغالب جرائم سيبرانية. بعض الدول تفتقر إلى تشريعات صارمة للتعامل مع هذه الظواهر. يشمل هذا البعد جوانب مختلفة مثل: [27]:

1. قوانين مكافحة الجرائم السيبرانية:

[26] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536., p 1530

[27] الحجرف، حسن نايف مبارك (2024)، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية، مجلة الدراسات الجامعية للبحوث الشاملة، المجلد 5، العدد 32، العراق، ص14081.

تجريم الأفعال التي تعتبر جرائم في الفضاء الإلكتروني، مثل القرصنة، والاحتيال الإلكتروني، وسرقة البيانات، ونشر البرامج الضارة، واختراق الأنظمة. تحديد العقوبات المناسبة لهذه الجرائم، وضع إجراءات للتحقيق في الجرائم السيبرانية وملاحقة مرتكبيها.

2. قوانين حماية البيانات والخصوصية:

تنظيم جمع ومعالجة وتخزين البيانات الشخصية، ومنح الأفراد حقوقًا فيما يتعلق ببياناتهم، مثل الحق في الوصول والتعديل والحذف، وفرض التزامات على المؤسسات لحماية البيانات من الوصول غير المصرح به أو الضياع أو التلف.

3. قوانين أمن الشبكات والمعلومات:

فرض معايير ومتطلبات أمنية على المؤسسات لحماية أنظمتها وشبكاتها ومعلوماتها الحساسة، وتحديد إجراءات الاستجابة للحوادث السيبرانية والإبلاغ عنها، وتنظيم عمل مقدمي خدمات الإنترنت ومزودي الخدمات الرقمية لضمان أمن خدماتهم.

4. القانون الدولي للأمن السيبراني:

يهدف إلى وضع مبادئ وقواعد دولية للتعاون في مجال الأمن السيبراني، ويتناول قضايا مثل مسؤولية الدول عن الهجمات السيبرانية التي تنطلق من أراضيها، وحظر استخدام الفضاء الإلكتروني لأغراض عدوانية، وتعزيز تبادل المعلومات والتعاون بين الدول لمكافحة الجرائم السيبرانية.

البعد الاقتصادي

التهديدات السيبرانية لها تأثير مباشر على الاقتصاديات الوطنية والعالمية. من خلال حماية القطاعات الاقتصادية: تأمين البنوك، الأسواق المالية، وشركات التكنولوجيا، لضمان استقرار المعاملات التجارية. ومنع

الخسائر المادية: الحد من الأضرار الناجمة عن سرقة الملكية الفكرية، الابتزاز، وتعطيل الأعمال. وتعزيز الثقة الرقمية خلق بيئة موثوقة تشجع على الاستثمار والتجارة الإلكترونية والتحول الرقمي[28] .

البعد الاجتماعي والبشري

يعتمد الأمن السيبراني بشكل كبير على الوعي والسلوك البشري. يمثل الأمن الاجتماعي: مواجهة المخاطر التي تهدد النسيج الاجتماعي مثل الجرائم السيبرانية، تضليل المعلومات، وتهديد القيم والأخلاق. وتثقيف الأفراد والموظفين حول كيفية حماية أنفسهم من هجمات التصيد الاحتيالي والبرمجيات الخبيثة. يُعتبر العنصر البشري "خط الدفاع الأول" والأضعف في نفس الوقت. وبناء الكفاءات: تطوير المهارات والكوادر المتخصصة في مجال الأمن السيبراني لمواجهة التهديدات المتزايدة.

سادساً: سبل تفعيل الأمن السيبراني

يتم تفعيل الأمن السيبراني من خلال مجموعة من الإجراءات والتدابير التقنية والبشرية والإدارية، والتي تهدف إلى حماية الأنظمة والشبكات والبيانات من الوصول غير المصرح به، أو التلف، أو الاستخدام غير المشروع. يمكن تقسيم سُبل تفعيل الأمن السيبراني إلى محاور رئيسية:

الإجراءات التقنية والفنية: تركز على استخدام الأدوات والبرمجيات المتخصصة لإنشاء حاجز دفاعي قوي[29]:

1- تحديث البرامج والأنظمة بانتظام: يجب تثبيت التحديثات الأمنية لنظام التشغيل والتطبيقات فور توفرها، لسد أي ثغرات يمكن استغلالها من قبل المخترقين.

2- استخدام برامج مكافحة الفيروسات والبرامج الضارة :(Antivirus) يجب تنزيل برامج موثوقة لمكافحة الفيروسات وتحديثها باستمرار لضمان الكشف والحماية من أحدث التهديدات.

3- تفعيل جدار الحماية :يعمل كحاجز بين شبكتك والإنترنت، ويراقب ويتحكم في حركة البيانات الواردة والصادرة لمنع الوصول غير المصرح به* .

[28] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. International Journal on Soft Computing, 14(3), 01-16.

[29] Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536., p 1534

4- إدارة كلمات المرور والمصادقة: كلمات مرور قوية: إنشاء كلمات مرور معقدة وطويلة (12 حرفًا على الأقل) تتضمن مزيجًا من الأحرف الكبيرة والصغيرة والأرقام والرموز.

5- المصادقة متعددة العوامل :(Multi-Factor Authentication - MFA) تفعيل هذه الخاصية في جميع الحسابات، حيث تتطلب طريقة تحقق ثانية (مثل رمز يتم إرساله إلى الهاتف) بالإضافة إلى كلمة المرور.

التوعية والتدريب البشري: يُعتبر العنصر البشري خط الدفاع الأول والأخير، لذا من الضروري[30] :

1- التدريب على الأمن السيبراني: توفير برامج تدريبية وورش عمل منتظمة للموظفين والأفراد لتعليمهم كيفية التعرف على التهديدات الشائعة.

2- التحذير من هجمات التصيد الاحتيالي: تعليم الأفراد كيفية تجنب النقر على الروابط المشبوهة أو فتح المرفقات في الرسائل الواردة من مصادر مجهولة أو غير موثوقة.

3- الحذر عند نشر المعلومات الشخصية: عدم نشر معلومات شخصية حساسة (مثل عنوان السكن، أو تفاصيل بنكية، أو أرقام الهاتف) على الإنترنت أو وسائل التواصل الاجتماعي.

السياسات والإجراءات الإدارية: تتعلق بوضع القواعد والخطط المؤسسية لضمان استمرارية الحماية[31]:

1- وضع سياسات أمنية واضحة: تحديد سياسات استخدام الأجهزة، والبريد الإلكتروني، والوصول إلى البيانات داخل المؤسسة.

2- النسخ الاحتياطي للبيانات: تنفيذ خطة منتظمة لعمل نسخ احتياطية للبيانات الهامة وتخزينها بأمان (يفضل في مكان منفصل أو سحابة آمنة)، لضمان القدرة على التعافي في حال وقوع هجوم أو تلف.

3- إدارة الوصول والصلاحيات: تطبيق مبدأ أقل الامتيازات، أي منح المستخدمين والأنظمة الحد الأدنى من الصلاحيات اللازمة لأداء وظائفهم فقط.

[30] Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).

[31] Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8)., p 9

4- خطة الاستجابة للحوادث: إعداد خطة واضحة ومُختبرة لتحديد الخطوات الواجب اتخاذها في حال وقوع حادث سيبراني (مثل الاختراق أو فقدان البيانات)، بما في ذلك الإبلاغ عن الحادث بسرعة للجهات المعنية.

إدارة مخاطر الهجمات السيبرانية:

تستهدف ضمان إدارة مخاطر الهجمات السيبرانية على نحو ممنهج لحماية الأصول المعلوماتية والتقنية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة، ويتم ذلك من خلال مجموعة الضوابط الآتية[32]:

أ- يجب على الإدارة المعنية بالأمن السيبراني في الجهة تحديد وتوثيق واعتماد منهجية وإجراءات إدارة مخاطر الأمن السيبراني في الجهة. وذلك وفقاً للاعتبارات السرية وتوافر سلامة الأصول المعلوماتية والتقنية.

ب-يجب على الإدارة المعنية بالأمن السيبراني تطبيق منهجية وإجراءات إدارة مخاطر التهديدات السيبرانية في الجهة، ويجب تنفيذ إجراءات تقييم مخاطر الهجمات السيبرانية بحد أدنى في الحالات التالية (في مرحلة مبكرة من المشاريع التقنية، قبل إجراء تغيير جوهري في البنية التقنية، عند التخطيط للحصول على خدمات طرف خارجي، عند التخطيط وقبل إطلاق منتجات وخدمات تقنية جديدة).

ت-يجب مراجعة منهجية وإجراءات إدارة مخاطر الهجمات السيبرانية وتحديثها على فترات زمنية مخطط لها (أو في حالة حدوث تغييرات في المتطلبات التشريعية والتنظيمية والمعايير ذات العلاقة)، كما يجب توثيق التغييرات واعتمادها.

سابعاً: القرارات والتشريعات المتعلقة بالامن السيبراني في سورية

تولي الحكومة السورية اهتماماً متزايداً بتنظيم مجال الأمن السيبراني في سورية، وقد تم اتخاذ عدد من القرارات والتشريعات والإجراءات في هذا الصدد.

القانون رقم 7 لعام 2023: يُنظر إليه كأحد التشريعات الرئيسية. نظّم آلية إحداث الهيئة الوطنية لخدمات تقانة المعلومات. ومنح الهيئة الحق الحصري في تقديم خدمات أمن المعلومات للجهات العامة والإشراف على متطلبات أمن المعلومات في القطاع الخاص. وناقش مفردات مثل التوقيع الرقمي، بما في ذلك:

[32] البردان، محمد فوزي أمين، وشحاته، محمد موسى علي (2020)، أثر تفعيل حوكمة تكنولوجيا المعلومات في ظل إستراتيجيات الرقمنة على الحد من مخاطر الهجمات السيبرانية بالبيئة المصرية، جامعة مدينة السادات، كلية التجارة، مصر، ص12.

أ- تحديد وضبط مواصفات منظومات التوقيع الرقمي واعتمادها.

ب-وضع الضوابط والنواظم الخاصة بإصدار شهادات التصديق الرقمي.

ت-وضع المواصفات والمعايير الخاصة بأمن وحماية الشبكات ومواقع الإنترنت.

ث-إنشاء وتشغيل خدمات أمن المعلومات وتحضير فرق الاستجابة للطوارئ المعلوماتية.

استراتيجية الأمن السيبراني: أقرت حكومة الجمهورية العربية السورية استراتيجية للأمن السيبراني تهدف إلى: تأسيس بنية أمن سيبراني قوية ومستدامة. ومراجعة الجوانب القانونية والتنظيمية المتعلقة بالأمن السيبراني، بما في ذلك إصدار تشريع شامل للأمن السيبراني بعد مراجعة كافة القوانين ذات الصلة. وتنمية القدرات وبناء المعرفة في هذا المجال.

القطاع المالي والمصرفي (مصرف سورية المركزي): بالإشارة إلى استراتيجية الأمن السيبراني، أصدر مجلس النقد والتسليف القرار رقم 15/م ن (أو قرار مشابه) المتضمن إجراءات إدارة الأمن السيبراني في المؤسسات المالية العاملة في سورية. يهدف هذا القرار إلى وضع ضوابط تضمن حوكمة فعالة لأمن وأمان بيئة تكنولوجيا المعلومات في القطاع المصرفي وتقليل المخاطر المرتبطة بحوادث الفضاء السيبراني. ويمكن ملاحظة اتجاهين رئيسيين: التشريع التنظيمي: مثل القانون رقم 7 لعام 2023 الذي أسس الإطار المؤسساتي (الهيئة الوطنية) والضوابط الأساسية للتوقيع وخدمات أمن المعلومات. والاستراتيجيات القطاعية: كإجراءات الأمن السيبراني الخاصة بالقطاع المصرفي، والتي تهدف لتعزيز الثقة بالتحول الرقمي وحماية الأصول المعلوماتية.

ثامناً: اجراءات الأمن السيبراني في القطاع لمصرفي

تعتبر إجراءات الأمن السيبراني في القطاع المصرفي أمراً بالغ الأهمية نظراً لحساسية البيانات المالية للعملاء وضمان استمرارية الأعمال المصرفية. تعتمد هذه الإجراءات على إطار شامل يغطي الحوكمة، والحماية التقنية، وإدارة المخاطر. فيما يلي أبرز محاور هذه الإجراءات، مع الإشارة إلى الجهود المبذولة في سورية، وتحديداً من قبل مصرف سورية المركزي:

الحوكمة وإدارة المخاطر(Governance & Risk Management)

تضمن حوكمة الأمن السيبراني أن الأمن السيبراني جزء من استراتيجية العمل العليا للبنك وليست مجرد مهمة تقنية. وتشمل: وضع السياسات والمعايير والإجراءات الإلزامية للأمن. تحديد المسؤوليات والصلاحيات لقيادة وإدارة الأمن على مستوى مجلس الإدارة والإدارة العليا. ضمان الامتثال للوائح المحلية والدولية (مثل معايير بازل المتعلقة بإدارة المخاطر).[33] كما توفر إدارة المخاطر السيبرانية المنهجية الاستباقية لتحديد المخاطر وتقييمها ومعالجتها. وتشمل: تحديد الأصول الحيوية (مثل أنظمة الدفع وقواعد بيانات العملاء). تقييم احتمالية وتأثير الهجمات المختلفة (مثل برامج الفدية، الاحتيال). وضع خطط الاستجابة للحوادث والتعافي من الكوارث لضمان استمرارية الأعمال بعد أي اختراق. ويجب على المؤسسات المصرفية أن يكون لديها إطار حوكمة واضح للأمن السيبراني، ويشمل ذلك[34] :

1- قيادة الإدارة العليا: تحمل مجالس الإدارة والإدارة التنفيذية المسؤولية عن تحديد شهية المؤسسة للمخاطر واعتماد سياسات الأمن السيبراني.

2- سياسات وضوابط أمن المعلومات: وضع سياسات مكتوبة تفصيلية لتنظيم جميع جوانب أمن المعلومات والالتزام بالمعايير الدولية مثل ISO 27001 لتأمين بيانات بطاقات الدفع.

3- إدارة مخاطر الطرف الثالث: تقييم المخاطر الأمنية للموردين الخارجيين ومقدمي الخدمات السحابية الذين يتعاملون مع بيانات البنك.

4- الامتثال التنظيمي: الالتزام بالتشريعات المحلية، ففي سورية، أصدر مجلس النقد والتسليف في مصرف سورية المركزي قراراً يتضمن إجراءات إدارة الأمن السيبراني في المؤسسات المالية لضمان حوكمة فعالة وضبط أمن بيئة تكنولوجيا المعلومات وتقليل مخاطر الفضاء السيبراني.

[33] Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8)., p 11

[34] Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).

الإجراءات التقنية الأساسية(Technical Controls)

تمثل الضوابط التقنية والفنية خط الدفاع الأول ضد الهجمات. وتشمل: تشفير البيانات الحساسة (للعملاء والمعاملات). جدران الحماية (Firewalls) وأنظمة كشف ومنع الاختراق (IDS/IPS). المصادقة متعددة العوامل (MFA) لمنع الوصول غير المصرح به. تحديث الأنظمة والتطبيقات بانتظام لسد الثغرات[35]. وتُعد هذه الضوابط هي خط الدفاع الأول ضد الهجمات الإلكترونية[36] :

1- تشفير البيانات:(Encryption) تشفير البيانات الحساسة للعملاء أثناء نقلها عبر الشبكات. تشفير البيانات المخزنة على الخوادم وقواعد البيانات

2- أمن الشبكات: استخدام الجدران النارية ونظم كشف ومنع التسلل وتجزئة الشبكات لفصل الأنظمة الحساسة عن باقي الشبكة.

3- تطبيق مبدأ الحد الأدنى من الامتيازات لتقييد وصول الموظفين إلى المعلومات الضرورية لعملهم فقط.

4- إدارة الثغرات والتحديثات: تطبيق برنامج شامل لإدارة التصحيحات الأمنية وتحديث الأنظمة والبرامج بشكل منتظم. وإجراء اختبارات الاختراق بشكل دوري لتحديد واكتشاف الثغرات.

الاستجابة للحوادث واستمرارية الأعمال(Incident Response & BCM)

يجب أن تكون البنوك مستعدة للتعامل مع أي خرق أمني محتمل[37] :

1- مراقبة التهديدات في الوقت الفعلي: استخدام أنظمة لمراقبة نشاط الشبكات والأنظمة واكتشاف أي مؤشرات على هجوم سيبراني مبكراً.

2- خطط الاستجابة للحوادث: وضع خطة واضحة ومُختبرة مسبقاً تحدد خطوات الاكتشاف، والاحتواء، والاستئصال، والتعافي في حال وقوع حادث سيبراني.

---

[35] Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8)., p 11

[36] Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643., p 630

[37] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16., p 12

3- خطط استمرارية الأعمال والتعافي من الكوارث :ضمان وجود نسخ احتياطية للبيانات والأنظمة تتيح استعادة الخدمات الأساسية بسرعة بعد الهجوم.

الوعي والتدريب(Awareness and Training)

يعالج الوعي والتدريب الأمني أكبر ثغرة في أي منظومة أمنية وهي العنصر البشري. ويساهم في: تثقيف الموظفين حول مخاطر التصيد الاحتيالي (Phishing) والهندسة الاجتماعية. تدريب الموظفين على التعرف على التهديدات والإبلاغ عنها بشكل فوري. توعية العملاء بممارسات الأمان الرقمي لحماية حساباتهم.[38] ويُعد العنصر البشري الحلقة الأضعف، لذا يجب التركيز على[39] :

1- تدريب الموظفين: توفير تدريب إلزامي ومستمر حول أفضل ممارسات الأمن السيبراني.

2- التوعية بالهندسة الاجتماعية: تدريب الموظفين على التعرف على هجمات التصيد الاحتيالي والبرمجيات الخبيثة.

وقد أكد مصرف سورية المركزي أن قرار إجراءات إدارة الأمن السيبراني يهدف إلى تعزيز الثقة بالتحول الرقمي وحماية الأصول المعلوماتية في القطاع المالي والمصرفي من خلال مجموعة من الضوابط المنسقة.

[38] Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643., p 630

[39] Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).

تاسعاً: إطار حوكمة الأمن السيبراني في البنوك

تُعد الحوكمة هي الآلية التي تضمن توافق الأمن السيبراني مع أهداف البنك التجارية ومتطلباته القانونية والتنظيمية.

مسؤولية الإدارة العليا(Executive Accountability)

1- لجنة الأمن السيبراني: إنشاء لجنة متخصصة تابعة لمجلس الإدارة أو الإدارة العليا تكون مسؤولة عن الإشراف على استراتيجية الأمن السيبراني، وتخصيص الموارد، ومراجعة تقارير المخاطر والأداء.

2- مؤشرات الأداء الرئيسية (KPIs) والمقاييس تحديد مقاييس واضحة لقياس فعالية ضوابط الأمن السيبراني (مثل وقت الكشف، ووقت الاستجابة، ونسبة الامتثال للسياسات)، ورفعها بانتظام للإدارة العليا.

3- دور مسؤول أمن المعلومات: يجب أن يكون لدى مسؤول أمن المعلومات خط اتصال مباشر ومستقل بمجلس الإدارة لضمان نقل الصورة الكاملة للمخاطر دون عوائق[40] .

إدارة المخاطر السيبرانية المتكاملة(Integrated Risk Management)

1- تصنيف الأصول: تصنيف أصول المعلومات بناءً على حساسيتها وأهميتها (مثل بيانات العملاء، أنظمة الدفع، بيانات الملكية الفكرية)، لتحديد مستوى الحماية المطلوب لكل فئة.

2- تقييم المخاطر: إجراء تقييمات منتظمة وموضوعية لتحديد التهديدات ونقاط الضعف التي قد تؤثر على الأصول المصرفية، وتحديد احتمالية وتأثير هذه المخاطر.

3- إطار قبول المخاطر: وضع معايير واضحة تحدد مستوى المخاطرة الذي يقبل البنك تحمله، واستخدام هذا الإطار لاتخاذ قرارات الاستثمار في الأمن[41] .

[40] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16., p 12

[41] Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).

سياسات وامتثال الأمن(Security Policies and Compliance)

1- هيكل السياسات: تطوير هيكل هرمي للسياسات يضم: سياسات عليا :(Policies) تُحدد النوايا العامة للبنك. معايير تُحدد المتطلبات الإلزامية للتقنيات المختلفة. إجراءات تُحدد الخطوات التفصيلية التي يجب اتباعها.

2- الامتثال التنظيمي: ضمان التوافق التام مع متطلبات مصرف سورية المركزي والتشريعات المحلية، وإجراء مراجعات داخلية وخارجية دورية للتحقق من الالتزام[42].

[42] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16., p 12

الفصل الثالث: الدراسة الميدانية

أولاً: أداة الدراسة

تناولت الدراسة تحليل آراء عينة الدراسة وذلك من خلال تحليل استبانة تم توزيعها الكترونياً على العاملين في مناصب وظيفية مختلفة لدى المصارف الخاصة السورية، وقد بلغ عدد الاستبانات الموزعة الصالحة للتحليل (79) استبانة، تم تحليلها باستخدام البرنامج الإحصائي SPSS الإصدار الخامس والعشرون وعند مستوى دلالة 0.05. تم استخدام عدد من المقاييس الإحصائية الوصفية والاستدلالية والاختبارات التي تلائم فرضيات الدراسة وتخدم أهدافها، وهي التكرارات والنسب المئوية، وعرض الاحصاءات الوصفية باستخدام الوسط الحسابي والانحراف المعياري واختبار الفرضيات باستخدام الانحدار الخطي البسيط والمتعدد.

ثانياً: تصميم الاستبانة

صممت الاستبانة وفق مقياس ليكرت الخماسي (5) موافق بشدة، (4) موافق، (3) محايد، (2) غير موافق، (1) غير موافق بشدة، وذلك في قسمين أساسيين: القسم الأول: مُخصص للأسئلة العامة ويشمل المعلومات الشخصية عن أفراد عينة البحث، وهي: المؤهل العلمي، عدد سنوات الخبرة، الموقع الوظيفي، وقد ضم القسم الثاني متغيرات الدراسة.

1- **المتغير المستقل: الأمن السيبراني.**

أ- الضوابط التقنية والفنية: بواقع (8) عبارات.

ب-حوكمة الأمن السيبراني: بواقع (8) عبارات.

ت-إدارة المخاطر السيبرانية: بواقع (8) عبارات.

ث-الوعي والتدريب الأمني: بواقع (8) عبارات.

2- **المتغير التابع: فاعلية حماية القطاع المصرفي (المرونة السيبرانية):** بواقع (8) عبارات.

ثالثاً: اختبار ثبات الاستبانة

تم اختبار ثبات الاستبانة باستخدام معامل ألفا كرونباخ Cronbach's Alpha وذلك لقياس الاتساق الداخلي بين عباراتها.

الجدول رقم (1) نتائج اختبار Cronbach's Alpha

المحور	اختبار الثبات معامل ألفا كرونباخ
الضوابط التقنية والفنية	0.904
حوكمة الأمن السيبراني	0.846
إدارة المخاطر السيبرانية	0.896
الوعي والتدريب الأمني	0.856
فاعلية حماية القطاع المصرفي (المرونة السيبرانية)	0.852

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يوضح الجدول رقم (1) نتائج التحليل لمعامل Cronbach's Alpha لأسئلة كل محور من محاور الاستبانة المتعلقة بمتغيرات الدراسة، حيث ظهرت بقيم أكبر من 0.7 وهي ما يمكن اعتبارها قيمة جيدة لثبات الاتساق الداخلي ومقبولة لأغراض التحليل الاحصائي، ويمكن الاعتماد على استجابات أفراد العينة في اشتقاق النتائج المتعلقة بمجتمع الدراسة.

رابعاً: تحليل خصائص عينة الدراسة

الجدول رقم (2) توزع أفراد العينة وفقاً لمتغير المؤهل العلمي

المؤهل العلمي	العدد	النسبة المئوية
إجازة جامعية	76	%96.2
معهد متوسط	2	%2.5
ماجستير	1	%1.3
المجموع	79	%100

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يوضح الجدول توزيع المؤهلات العلمية لعينة مكونة من 79 فرداً، حيث يتبيّن أن الغالبية العظمى من الأفراد يحملون إجازة جامعية، إذ بلغ عددهم 76 شخصاً، ما يمثل نسبة 96.2% من إجمالي العينة. في المقابل، بلغ عدد الحاصلين على شهادة معهد متوسط شخصين فقط بنسبة 2.5%، بينما لم يتجاوز عدد الحاصلين على درجة الماجستير شخصاً واحداً بنسبة 1.3%. ويعكس هذا التوزيع تركّزاً واضحاً في فئة الحاصلين على الإجازة الجامعية، مما يشير إلى ارتفاع المستوى التعليمي العام للعينة، مع محدودية تمثيل الفئات ذات المؤهلات العليا أو المتوسطة.

الجدول رقم (3) توزع أفراد العينة وفقاً لمتغير عدد سنوات الخبرة في العمل

عدد سنوات الخبرة	العدد	النسبة المئوية
أقل من 3 سنوات	2	%2.5
من 3 إلى أقل من 5 سنوات	36	%45.6
من 5 إلى إلى أقل من 10 سنوات	31	%39.2
10 سنوات فأكثر	10	%12.7
المجموع	79	%100

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يعكس الجدول توزيع سنوات الخبرة لدى عينة مكونة من 79 فرداً، حيث يتضح أن النسبة الأكبر من الأفراد يتمتعون بخبرة تتراوح بين 3 إلى أقل من 5 سنوات، إذ بلغ عددهم 36 شخصاً بنسبة 45.6%. يليهم من لديهم خبرة بين 5 إلى أقل من 10 سنوات بعدد 31 فرداً، أي ما يعادل 39.2%. أما من يمتلكون خبرة طويلة تمتد إلى 10 سنوات فأكثر فقد بلغ عددهم 10 أفراد بنسبة 12.7%، في حين أن أصحاب الخبرة الأقل من 3 سنوات كانوا الأقل عدداً بنسبة 2.5% فقط. ويشير هذا التوزيع إلى أن غالبية العينة تنتمي إلى فئة الخبرة المتوسطة، مما قد يعكس مرحلة مهنية نشطة تتسم بالاستقرار والنمو المهني.

الجدول رقم (4) توزع أفراد العينة وفقاً لمتغير الموقع الوظيفي

الموقع الوظيفي	العدد	النسبة المئوية
مدير	1	%1.3
رئيس قسم	13	%16.5
موظف إداري	39	%49.4
موظف فني	26	%32.9
المجموع	79	%100

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يعكس الجدول توزيع أفراد العينة البالغ عددهم 79 حسب مواقعهم الوظيفية، حيث يتبيّن أن النسبة الأكبر منهم يشغلون وظائف إدارية، إذ بلغ عدد الموظفين الإداريين 39 فرداً، ما يمثل 49.4% من إجمالي العينة. يليهم الموظفون الفنيون بعدد 26 فرداً بنسبة 32.9%، ثم رؤساء الأقسام الذين بلغ عددهم 13 بنسبة 16.5%. أما المدراء فكانوا الأقل تمثيلًا، حيث لم يتجاوز عددهم فردًا واحدًا بنسبة 1.3%. ويشير هذا التوزيع إلى أن العينة تتركز بشكل رئيسي في المستويات التنفيذية، مع تمثيل محدود للمناصب القيادية العليا.

خامساً: الإحصاءات الوصفية لمتغيرات الدراسة

تتضمن الإحصاءات الوصفية قيم كل من المتوسط الحسابي والانحراف المعياري لفقرات الاستبانة ولإجمالي كل محور للوصول إلى الأهمية النسبية لكل منها، حيث تم اعتبار أن الحد الفاصل بين الأهمية المرتفعة والمتوسطة قيمة المتوسط البالغة 3.4.

الجدول رقم (5) الأهمية النسبية للموافقات

فئات قيم المتوسط الحسابي	التقدير
من 1 الى 1.79	درجة موافقة منخفضة جدا
من 1.8 الى 2.59	درجة الموافقة منخفضة
من 2.6 الى 3.39	درجة الموافقة متوسطة
من 3.4 الى 4.19	درجة الموافقة مرتفعة
من 4.2 الى 5	درجة الموافقة مرتفعة جدا

المصدر: إعداد الباحثان

1- نتائج قياس الضوابط التقنية والفنية:

تم حساب قيم كل من المتوسط الحسابي والانحراف المعياري للضوابط التقنية والفنية وكانت النتائج كما يلي:

الجدول رقم (6) نتائج قياس الضوابط التقنية والفنية

الفقرة	5	4	3	2	1	الوسط الحسابي	الانحراف المعياري	النتيجة
يتم تحديث أنظمة التشغيل والبرامج المصرفية بشكل دوري للتعامل مع الثغرات الأمنية الجديدة.	18	55	5	1	0	4.1392	0.57142	موافقة مرتفعة
يمتلك المصرف أنظمة جدران حماية وأنظمة كشف ومنع التسلل متقدمة وفعالة.	16	61	2	0	0	4.1772	0.44605	موافقة مرتفعة
تُستخدم تقنية التشفير لحماية بيانات العملاء الحساسة أثناء تخزينها ونقلها.	19	58	2	0	0	4.2152	0.47152	موافقة مرتفعة جداً
يطبق المصرف سياسات قوية لإدارة كلمات المرور متعددة العوامل للوصول إلى الأنظمة الحيوية.	16	55	6	2	0	4.0759	0.61545	موافقة مرتفعة
يتم إجراء اختبارات اختراق دورية ومستقلة على الشبكات والتطبيقات المصرفية.	16	63	0	0	0	4.2025	0.40445	موافقة مرتفعة جداً

يعاني المصرف من تحديات في شراء وتحديث المعدات الأمنية بسبب القيود الخارجية.	12	67	0	0	0	4.1519	0.36122	موافقة مرتفعة
يتم استخدام أدوات متخصصة لمراقبة سجلات الأحداث وتحليل الأنماط الشاذة في الشبكة على مدار الساعة.	15	61	3	0	0	4.152	0.4554	موافقة مرتفعة
يُجري المصرف فحصاً أمنياً دورياً للمخالفات في إعدادات الأنظمة المصرفية الرئيسية.	16	56	7	0	0	4.1139	0.53078	موافقة مرتفعة
الضوابط التقنية والفنية	79					4.1535	0.37121	موافقة مرتفعة

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يوضح الجدول رقم (6) أن المتوسط الحسابي لكامل المحور بلغ 4.15 بموافقة مرتفعة وبانحراف معياري 0.37 حيث حظيت معظم العبارات بموافقة مرتفعة تجاوز المتوسط الحسابي لها 3.4، وبالتالي فإن المستقصى آرائهم موافقون في حكمهم على مضمون هذه العبارات، وبالتالي هناك مستوى مرتفع لتطبيق الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في المصارف الخاصة السورية وذلك من وجهة نظر أفراد العينة.

2- نتائج قياس حوكمة الأمن السيبراني:

تم حساب قيم كل من المتوسط الحسابي والانحراف المعياري لحوكمة الأمن السيبراني وكانت النتائج كما يلي:

الجدول رقم (7) نتائج قياس حوكمة الأمن السيبراني

الفقرة	5	4	3	2	1	الوسط الحسابي	الانحراف المعياري	النتيجة
توجد استراتيجية واضحة وموثقة للأمن السيبراني معتمدة من الإدارة العليا.	9	70	0	0	0	4.1139	0.31975	موافقة مرتفعة
يتم تخصيص ميزانية كافية ومستقلة سنوياً لتطوير وتحسين إجراءات الأمن السيبراني.	9	64	5	1	0	4.0253	0.47971	موافقة مرتفعة
يلتزم المصرف بالتعليمات والضوابط الصادرة عن مصرف سورية المركزي المتعلقة بإدارة الأمن السيبراني.	11	64	3	1	0	4.0759	0.47426	موافقة مرتفعة
يتم مراجعة سياسات الأمن السيبراني وتحديثها سنوياً لمواكبة التهديدات المتطورة.	15	62	1	1	0	4.1519	0.48274	موافقة مرتفعة
يُعتبر الأمن السيبراني جزءاً من عملية اتخاذ القرارات في المشاريع المصرفية الجديدة منذ مرحلتها الأولى.	10	67	1	1	0	4.0886	0.42937	موافقة مرتفعة
يتم تحديد ملكية البيانات ومستوى حساسيتها بشكل واضح داخل المصرف وتطبق عليها سياسات حماية متناسبة.	13	64	1	1	0	4.1266	0.46319	موافقة مرتفعة
يتم تضمين بنود خاصة بالأمن السيبراني في عقود التعاقد مع الموردين الخارجيين لضمان امتثالهم.	9	68	1	1	0	4.0759	0.41671	موافقة مرتفعة
هناك آلية رسمية وفعالة لإدارة تصاريح الوصول للموظفين الجدد والمغادرين.	13	66	0	0	0	4.1646	0.37315	موافقة مرتفعة
حوكمة الأمن السيبراني	79					4.1028	0.35057	موافقة مرتفعة

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يبين الجدول رقم (7) أن المتوسط الحسابي لكامل المحور قد بلغ 4.10 بموافقة مرتفعة وبانحراف معياري 0.35 حيث حظيت معظم العبارات بموافقة مرتفعة تجاوز المتوسط الحسابي لها 3.4، وبالتالي فإن المستقصى

آرائهم موافقون في حكمهم على مضمون هذه العبارات، وبالتالي هناك مستوى مرتفع لتطبيق حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في المصارف الخاصة السورية وذلك من وجهة نظر أفراد العينة.

3- نتائج قياس إدارة المخاطر السيبرانية:

تم حساب قيم كل من المتوسط الحسابي والانحراف المعياري لإدارة المخاطر السيبرانية وكانت النتائج كما يلي:

الجدول رقم (8) نتائج قياس إدارة المخاطر السيبرانية

الفقرة	5	4	3	2	1	الوسط الحسابي	الانحراف المعياري	النتيجة
يتم إجراء تقييمات دورية ومنهجية للمخاطر السيبرانية التي تواجه الأصول الحيوية للمصرف.	20	57	1	1	0	4.2152	0.52308	موافقة مرتفعة جداً
لدى المصرف خطة واضحة ومختبرة للاستجابة للحوادث السيبرانية والتعافي منها.	10	67	1	1	0	4.0886	0.42937	موافقة مرتفعة
يتم التنسيق والتبادل الفوري للمعلومات حول التهديدات السيبرانية مع المصارف الأخرى والهيئات الحكومية (كالهيئة الناظمة لقطاع الاتصالات).	8	69	1	1	0	4.0633	0.40325	موافقة مرتفعة
يتم إجراء تمارين محاكاة للهجمات السيبرانية بانتظام لاختبار جاهزية فريق الاستجابة.	8	71	0	0	0	4.1013	0.30361	موافقة مرتفعة
يتم بشكل فعال عزل وفصل شبكات الأنظمة الحيوية المصرفية عن الشبكات المكتبية العادية لتقليل المخاطر.	12	65	1	1	0	4.1139	0.45255	موافقة مرتفعة
لدى المصرف خطة مفصلة للتعامل مع هجمات حجب الخدمة الموزعة التي تستهدف الخدمات المصرفية الإلكترونية.	10	69	0	0	0	4.1266	0.33463	موافقة مرتفعة
يمتلك المصرف القدرة على تحديد الهجمات السيبرانية ذات الدافع الجيوسياسي أو التخريبي وتمييزها عن الهجمات المالية التقليدية.	13	66	0	0	0	4.1646	0.37315	موافقة مرتفعة

يتم تقييم مخاطر أمن سلسلة التوريد الناتجة عن الاعتماد على مقدمي الخدمات المحليين.	12	67	0	0	0	4.1519	0.36122	موافقة مرتفعة
إدارة المخاطر السيبرانية	79					4.1282	0.33967	موافقة مرتفعة

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يشير الجدول رقم (8) أن المتوسط الحسابي لكامل المحور بلغ 4.12 بموافقة مرتفعة وبانحراف معياري 0.33 حيث حظيت معظم العبارات بموافقة مرتفعة تجاوز المتوسط الحسابي لها 3.4، وبالتالي فإن المستقصى آرائهم موافقون في حكمهم على مضمون هذه العبارات، وبالتالي هناك مستوى مرتفع لتطبيق إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في المصارف الخاصة السورية وذلك من وجهة نظر أفراد العينة.

4- نتائج قياس الوعي والتدريب الأمني:

تم حساب قيم كل من المتوسط الحسابي والانحراف المعياري للوعي والتدريب الأمني وكانت النتائج كما يلي:

الجدول رقم (9) نتائج قياس الوعي والتدريب الأمني

الفقرة	5	4	3	2	1	الوسط الحسابي	الانحراف المعياري	النتيجة
يتلقى جميع الموظفين (بما في ذلك غير التقنيين) تدريباً إلزامياً دورياً حول مخاطر التصيد الاحتيالي.	7	70	0	2	0	4.0380	0.43686	موافقة مرتفعة
يوجد نقص واضح في الكوادر الفنية المؤهلة والمتخصصة في الأمن السيبراني داخل المصرف.	15	62	1	1	0	4.1519	0.48274	موافقة مرتفعة
يتم اختبار وعي الموظفين الأمني بشكل دوري (مثل إرسال رسائل تصيد وهمية).	14	65	0	0	0	4.1772	0.38429	موافقة مرتفعة
تخصص المصارف موارد لتدريب كوادرها على أحدث التقنيات والتهديدات الأمنية العالمية رغم صعوبة السفر والقيود.	12	67	0	0	0	4.1519	0.36122	موافقة مرتفعة

يتمتع الموظفون بالثقافة الكافية للإبلاغ الفوري عن أي حوادث أو رسائل مشبوهة دون خوف من العقاب.	14	63	1	1	0	4.1392	0.47324	موافقة مرتفعة
يمتلك الموظفون العاملون عن بعد (إن وجدوا) أدوات وبرامج حماية مناسبة ومراقبة من قبل المصرف.	15	64	0	0	0	4.1899	0.39471	موافقة مرتفعة
تأخذ برامج التوعية بالأمن السيبراني المصممة للمصرف بعين الاعتبار التهديدات المحلية الخاصة بالبيئة السورية.	13	66	0	0	0	4.1646	0.37315	موافقة مرتفعة
هناك صعوبة في اجتذاب الكفاءات السورية المتخصصة في الأمن السيبراني والاحتفاظ بها بسبب المنافسة أو الهجرة.	14	65	0	0	0	4.1772	0.38429	موافقة مرتفعة
الوعي والتدريب الأمني	79					4.1487	0.30884	موافقة مرتفعة

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يشير الجدول رقم (9) أن المتوسط الحسابي لكامل المحور بلغ 4.14 بموافقة مرتفعة وبانحراف معياري 0.30 حيث حظيت معظم العبارات بموافقة مرتفعة تجاوز المتوسط الحسابي لها 3.4، وبالتالي فإن المستقصى آرائهم موافقون في حكمهم على مضمون هذه العبارات، وبالتالي هناك مستوى مرتفع للوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في المصارف الخاصة السورية وذلك من وجهة نظر أفراد العينة.

5- نتائج قياس فاعلية حماية القطاع المصرفي (المرونة السيبرانية):

تم حساب قيم كل من المتوسط الحسابي والانحراف المعياري فاعلية حماية القطاع المصرفي (المرونة السيبرانية) وكانت النتائج كما يلي:

الجدول رقم (10) نتائج قياس فاعلية حماية القطاع المصرفي (المرونة السيبرانية)

الفقرة	5	4	3	2	1	الوسط الحسابي	الانحراف المعياري	النتيجة
يمتلك المصرف القدرة على اكتشاف معظم الحوادث السيبرانية قبل أن تتسبب بأي خسائر مالية أو تشغيلية كبيرة.	16	61	0	2	0	4.1519	0.53322	موافقة مرتفعة
استطاع المصرف الوفاء بمتطلبات "الحد الأدنى" من الخدمات المصرفية بشكل مستمر حتى أثناء وقوع حوادث أمنية.	20	57	1	1	0	4.2152	0.52308	موافقة مرتفعة جداً
يُعد وقت استعادة الأنظمة المصرفية الحيوية بعد تعرضها لهجوم سريعاً ومقبولاً.	17	62	0	0	0	4.2152	0.41358	موافقة مرتفعة جداً
زادت ثقة العملاء بالخدمات المصرفية الإلكترونية في المصرف نتيجة لتدابير الأمن السيبراني الواضحة والملموسة.	18	61	0	0	0	4.2278	0.42212	موافقة مرتفعة جداً
تعتبر بيئة تكنولوجيا المعلومات في المصرف مرنة وقادرة على التكيف مع التهديدات السيبرانية غير المتوقعة	20	57	1	1	0	4.2152	0.52308	موافقة مرتفعة جداً
يساهم مستوى الأمن السيبراني الحالي في المصرف في تعزيز التزامنا بضوابط مكافحة غسل الأموال وتمويل الإرهاب.	21	58	0	0	0	4.2658	0.44459	موافقة مرتفعة جداً
أدت الإجراءات الأمنية الحالية إلى انخفاض ملحوظ في عدد الشكاوى المتعلقة باحتيال العملاء أو فقدان بياناتهم.	17	62	0	0	0	4.2152	0.41358	موافقة مرتفعة جداً
يتمكن المصرف من استعادة العمليات المصرفية الحيوية (مثل التسويات) بشكل كامل خلال 24 ساعة من وقوع حادث كبير	20	59	0	0	0	4.2532	0.43760	موافقة مرتفعة جداً

فاعلية حماية القطاع المصرفي (المرونة السيبرانية)	79	4.2199	0.32597	موافقة مرتفعة جداً

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يشير الجدول رقم (10) أن المتوسط الحسابي لكامل المحور بلغ 4.21 بموافقة مرتفعة جداً وبانحراف معياري 0.32 حيث حظيت معظم العبارات بموافقة مرتفعة تجاوز المتوسط الحسابي لها 3.4، وبالتالي فإن المستقصى آرائهم موافقون في حكمهم على مضمون هذه العبارات، وبالتالي يؤثر الأمن السيبراني في فاعلية حماية القطاع المصرفي في سورية وذلك من وجهة نظر أفراد العينة.

سادساً: اختبار فرضيات الدراسة

اختبار الفرضية الرئيسية

يوجد دور ذو دلالة معنوية للأمن السيبراني في حماية القطاع المصرفي في سوريا.

بغرض اختبار الفرضية تم إجراء اختبار الانحدار الخطي المتعدد لاختبار العلاقة بين الأمن السيبراني كمتغير مستقل وحماية القطاع المصرفي كمتغير تابع.

الجدول رقم (11) الدلالة الإحصائية لاختبار العلاقة بين الأمن السيبراني وحماية القطاع المصرفي

Std. Error of the Estimate	Adjusted R Square	R Square	R
0.13390	0.831	0.840	**0.916[a]**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يتضــح من الجدول أعلاه أن قيمة معامل الارتباط R تســاوي (0.916)، وهو ما يبين وجود ارتباط قوي بين الأمن السـيبراني وحماية القطاع المصـرفي وأن معامل التحديد هو (0.831)، أي إن الأمن السـيبراني يفسـر (83.1%)، من التغيرات الحاصلة في حماية القطاع المصرفي.

الجدول رقم (12) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة

ANOVAa						
Sig.	F	Mean Square	Df	Sum of Squares	**Model**	
0.000[b]	97.063	1.740	4	6.961	Regression	**1**
		0.018	74	1.327	Residual	
			78	8.288	Total	

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يبين الجدول أعلاه تحليل التباين الذي يمكن من خلاله معرفة الدلالة الإحصـائية للقوة التفسـيرية للنموذج عن طريق إحصائية F، وهي (97.063)، ومعنوية الدلالة الحسابية (sig=0.000)، مما يؤكد الدلالة الإحصائية لنموذج الانحدار الخطي من الناحية الإحصائية، أي النموذج بشكل عام معنوي.

الجدول رقم (13) الدلالة الاحصائية لنموذج الدراسة لأثر الأمن السيبراني في حماية القطاع المصرفي

Sig.	**T**	**Standardized Coefficients**	**Unstandardized Coefficients**		**Model**	
		Beta	Std. Error	B		
0.161	1.417		0.205	0.290	(Constant)	
0.000	4.037	0.336	0.073	0.295	الضوابط التقنية والفنية	**1**
0.871	-0.163	-0.022	0.127	-0.021	حوكمة الأمن السيبراني	**2**
0.506	0.669	0.098	0.141	0.094	إدارة المخاطر السيبرانية	**3**
0.000	4.142	0.548	0.140	0.579	الوعي والتدريب الأمني	**4**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يشير الجدول أعلاه إلى أن (الضوابط التقنية والفنية والوعي والتدريب الأمني) هي دالة إحصائياً حسب قيم t المحسوبة والدلالة الإحصائية التي جاءت اصغر من (5%)، مما يثبت صحة الفرضية. وبالتالي يوجد دور إيجابي ذو دلالة معنوية للأمن السيبراني في حماية القطاع المصرفي في سوريا، وان كل من الضوابط التقنية والفنية والوعي والتدريب الأمني هي الأبعاد الأكثر تأثيراً في حماية القطاع المصرفي في سورية.

اختبار الفرضية الفرعية الأولى

يوجد دور ذو دلالة معنوية للضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

بغرض اختبار الفرضية تم إجراء اختبار الانحدار الخطي البسيط لاختبار العلاقة بين الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني كمتغير مستقل وحماية القطاع المصرفي كمتغير تابع.

الجدول رقم (14) الدلالة الإحصائية لاختبار العلاقة بين الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي

Std. Error of the Estimate	Adjusted R Square	R Square	R
0.17380	0.716	0.719	**0.848[a]**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يتضح من الجدول أعلاه أن قيمة معامل الارتباط R تساوي (0.848)، وهو ما يبين وجود ارتباط قوي بين الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي وأن معامل التحديد هو (0.716)، أي إن الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني تفسر (71.6%)، من التغيرات الحاصلة في حماية القطاع المصرفي.

الجدول رقم (15) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة

ANOVAa						
Sig.	F	Mean Square	Df	Sum of Squares	**Model**	
0.000[b]	197.371	5.962	1	5.962	Regression	**1**
		0.030	77	2.326	Residual	
			78	8.288	Total	

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يبين الجدول أعلاه تحليل التباين الذي يمكن من خلاله معرفة الدلالة الإحصائية للقوة التفسيرية للنموذج عن طريق إحصائية F، وهي (197.371)، ومعنوية الدلالة الحسابية (sig=0.000)، مما يؤكد الدلالة الإحصائية لنموذج الانحدار الخطي من الناحية الإحصائية، أي النموذج بشكل عام معنوي.

الجدول رقم (16) الدلالة الاحصائية لنموذج الدراسة لأثر الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي

Sig.	**T**	**Standardized Coefficients**	**Unstandardized Coefficients**		**Model**	
		Beta	Std. Error	B		
0.000	5.096		0.221	1.127	(Constant)	
0.000	14.049	0.848	0.053	0.745	الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي	**1**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يشير الجدول أعلاه إلى أن (الضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي) هي دالة إحصائياً حسب قيم t المحسوبة والدلالة الإحصائية التي جاءت اصغر من (5%)، مما يثبت صحة الفرضية.

تكون معادلة الانحدار على الشكل الآتي:

$$y = 1.127 + 0.745\ x1$$

وبالتالي يوجد دور إيجابي ذو دلالة معنوية للضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

اختبار الفرضية الفرعية الثانية

يوجد دور ذو دلالة معنوية لحوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

بغرض اختبار الفرضية تم إجراء اختبار الانحدار الخطي البسيط لاختبار العلاقة بين حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني كمتغير مستقل وحماية القطاع المصرفي كمتغير تابع.

الجدول رقم (17) الدلالة الإحصائية لاختبار العلاقة بين حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي

Std. Error of the Estimate	Adjusted R Square	R Square	R
0.18708	0.671	0.675	**0.821[a]**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يتضح من الجدول أعلاه أن قيمة معامل الارتباط R تساوي (0.821)، وهو ما يبين وجود ارتباط قوي بين حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي وأن معامل التحديد هو (0.671)، أي إن حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني تفسر (67.1%)، من التغيرات الحاصلة في حماية القطاع المصرفي.

الجدول رقم (18) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة

ANOVAa						
Sig.	F	Mean Square	Df	Sum of Squares	**Model**	
0.000[b]	159.816	5.593	1	5.593	Regression	**1**
		0.035	77	2.695	Residual	
			78	8.288	Total	

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يبين الجدول أعلاه تحليل التباين الذي يمكن من خلاله معرفة الدلالة الإحصائية للقوة التفسيرية للنموذج عن طريق إحصائية F، وهي (159.816)، ومعنوية الدلالة الحسابية (sig=0.000)، مما يؤكد الدلالة الإحصائية لنموذج الانحدار الخطي من الناحية الإحصائية، أي النموذج بشكل عام معنوي.

الجدول رقم (19) الدلالة الاحصائية لنموذج الدراسة لأثر حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي

Sig.	**T**	**Standardized Coefficients**	**Unstandardized Coefficients**		**Model**	
		Beta	Std. Error	B		
0.000	4.365		0.249	1.086	(Constant)	
0.000	12.642	0.821	0.060	0.764	حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي	**1**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يشير الجدول أعلاه إلى أن (حوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي) هي دالة إحصائياً حسب قيم t المحسوبة والدلالة الإحصائية التي جاءت اصغر من (5%)، مما يثبت صحة الفرضية.

تكون معادلة الانحدار على الشكل الآتي:

$$y = 1.086 + 0.764\ x1$$

وبالتالي يوجد دور إيجابي ذو دلالة معنوية لحوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

اختبار الفرضية الفرعية الثالثة

يوجد دور ذو دلالة معنوية لإدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

بغرض اختبار الفرضية تم إجراء اختبار الانحدار الخطي البسيط لاختبار العلاقة بين إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني كمتغير مستقل وحماية القطاع المصرفي كمتغير تابع.

الجدول رقم (20) الدلالة الإحصائية لاختبار العلاقة بين إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي

Std. Error of the Estimate	Adjusted R Square	R Square	R
0.17598	0.709	0.712	**0.844[a]**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يتضح من الجدول أعلاه أن قيمة معامل الارتباط R تساوي (0.844)، وهو ما يبين وجود ارتباط قوي بين إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي وأن معامل التحديد هو (0.709)، أي إن إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني تفسر (70.9%)، من التغيرات الحاصلة في حماية القطاع المصرفي.

الجدول رقم (21) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة

ANOVAa						
Sig.	F	Mean Square	Df	Sum of Squares	**Model**	
0.000[b]	190.628	5.903	1	5.903	Regression	**1**
		0.031	77	2.385	Residual	
			78	8.288	Total	

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يبين الجدول أعلاه تحليل التباين الذي يمكن من خلاله معرفة الدلالة الإحصائية للقوة التفسيرية للنموذج عن طريق إحصائية F، وهي (190.628)، ومعنوية الدلالة الحسابية (sig=0.000)، مما يؤكد الدلالة الإحصائية لنموذج الانحدار الخطي من الناحية الإحصائية، أي النموذج بشكل عام معنوي.

الجدول رقم (22) الدلالة الاحصائية لنموذج الدراسة لأثر إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي

Sig.	**T**	**Standardized Coefficients**	**Unstandardized Coefficients**		**Model**	
		Beta	Std. Error	B		
0.001	3.607		0.243	0.876	(Constant)	
0.000	13.807	0.844	0.059	0.810	إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي	**1**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يشير الجدول أعلاه إلى أن (إدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي) هي دالة إحصائياً حسب قيم t المحسوبة والدلالة الإحصائية التي جاءت اصغر من (5%)، مما يثبت صحة الفرضية.

تكون معادلة الانحدار على الشكل الآتي:

$$y = 0.876 + 0.810\, x1$$

وبالتالي يوجد دور إيجابي ذو دلالة معنوية لإدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

اختبار الفرضية الفرعية الرابعة

يوجد دور ذو دلالة معنوية للوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

بغرض اختبار الفرضية تم إجراء اختبار الانحدار الخطي البسيط لاختبار العلاقة بين الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني كمتغير مستقل وحماية القطاع المصرفي كمتغير تابع.

الجدول رقم (23) الدلالة الإحصائية لاختبار العلاقة بين الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي

Std. Error of the Estimate	Adjusted R Square	R Square	R
0.14658	0.798	0.800	**0.895**[a]

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يتضح من الجدول أعلاه أن قيمة معامل الارتباط R تساوي (0.895)، وهو ما يبين وجود ارتباط قوي بين الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي وأن معامل التحديد هو (0.798)، أي إن الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني يفسر (79.8%)، من التغيرات الحاصلة في حماية القطاع المصرفي.

الجدول رقم (24) الدلالة الإحصائية لاختبار القوة التفسيرية لتباين نموذج الدراسة

ANOVAa						
Sig.	F	Mean Square	Df	Sum of Squares	**Model**	
0.000[b]	308.723	6.633	1	6.633	Regression	**1**
		0.021	77	1.654	Residual	
			78	8.288	Total	

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يبين الجدول أعلاه تحليل التباين الذي يمكن من خلاله معرفة الدلالة الإحصائية للقوة التفسيرية للنموذج عن طريق إحصائية F، وهي (308.723)، ومعنوية الدلالة الحسابية (sig=0.000)، مما يؤكد الدلالة الإحصائية لنموذج الانحدار الخطي من الناحية الإحصائية، أي النموذج بشكل عام معنوي.

الجدول رقم (25) الدلالة الاحصائية لنموذج الدراسة لأثر الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي

Sig.	**T**	**Standardized Coefficients**	**Unstandardized Coefficients**		**Model**	
		Beta	Std. Error	B		
0.180	1.353		0.224	0.302	(Constant)	
0.000	17.571	0.895	0.054	0.944	الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي	**1**

المصدر: إعداد الباحثان بالاعتماد على مخرجات البرنامج الاحصائي spss

يشير الجدول أعلاه إلى أن (الوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني وحماية القطاع المصرفي) هي دالة إحصائياً حسب قيم t المحسوبة والدلالة الإحصائية التي جاءت اصغر من (5%)، مما يثبت صحة الفرضية.

تكون معادلة الانحدار على الشكل الآتي:

$$y = 0.302 + 0.944\ x1$$

وبالتالي يوجد دور إيجابي ذو دلالة معنوية للوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا.

النتائج والتوصيات

النتائج

نتيجة اختبار الفرضيات تم التوصل إلى الآتي:

1- يوجد دور إيجابي ذو دلالة معنوية للأمن السيبراني في حماية القطاع المصرفي في سوريا. تشير هذه النتيجة إلى أن تطبيق مفهوم الأمن السيبراني الشامل (بكل أبعاده من تقنية، وحوكمة، ومخاطر، وتوعية) يساهم بشكل فعال ومهم إحصائياً في تعزيز الحماية الكلية للقطاع المصرفي السوري ضد التهديدات الرقمية. هذا يثبت أن الاستثمار في استراتيجية سيبرانية متكاملة ليس مجرد تكلفة، بل هو مطلب ضروري لتحقيق الاستقرار المالي والثقة.

2- يوجد دور إيجابي ذو دلالة معنوية للضوابط التقنية والفنية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا. يؤكد هذا البعد أن الأدوات والتقنيات الملموسة هي أساس الحماية. الدور الإيجابي يعني أن استخدام جدران الحماية المتقدمة وأنظمة كشف ومنع التسلل وتشفير البيانات، وحلول إدارة الهوية والوصول وتقنية حماية نقطة النهاية يؤدي إلى تقليل كبير في الثغرات والاختراقات في الأنظمة المصرفية الأساسية.

3- يوجد دور إيجابي ذو دلالة معنوية لحوكمة الأمن السيبراني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا. تشير الدلالة المعنوية هنا إلى أن التنظيم والهيكل الإداري للأمن السيبراني لا يقل أهمية عن التقنية. الحوكمة الفعالة تعني وجود استراتيجية واضحة يقرها مجلس الإدارة، وتحديد المسؤوليات والصلاحيات بوضوح وإجراء تدقيق ومراجعة دورية للضوابط الأمنية. هذا يضمن أن الأمن السيبراني هو جزء من ثقافة العمل وليس مجرد قسم تقني. وهذا يتشابه مع دراسة (كاظم والمشهداني، 2025) في أهمية حوكمة الامن السيبراني في المصارف.

4- يوجد دور إيجابي ذو دلالة معنوية لإدارة المخاطر السيبرانية كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا. تؤكد هذه النتيجة أن عملية تحديد وتقدير وتقييم المخاطر السيبرانية بشكل مستمر (مثل مخاطر هجمات الفدية، أو تعطل الخدمات، أو سرقة البيانات) لها تأثير إيجابي في الحماية. هذا يعني أن البنوك التي لديها سجل مخاطر سيبرانية مفصل وتطبق خطط الاستجابة للحوادث والتعافي من

الكوارث تكون أكثر مرونة وقدرة على التعافي بعد وقوع أي حادث. وهذا يتشابه مع دراسة (بوانه، 2023) في أهمية إدارة المخاطر السيبرانية في القطاع المصرفي.

5- يوجد دور إيجابي ذو دلالة معنوية للوعي والتدريب الأمني كأحد أبعاد الأمن السيبراني في حماية القطاع المصرفي في سوريا. الدور الإيجابي هنا يسلط الضوء على "العنصر البشري" باعتباره الحلقة الأضعف والأقوى في آن واحد. وجود برامج توعية وتدريب مستمرة وفعالة (حول التصيد الاحتيالي، الهندسة الاجتماعية، أهمية كلمات المرور القوية، أمن الأجهزة المحمولة) يقلل من احتمالية نجاح الهجمات التي تستهدف الموظفين، مما يدعم خط الدفاع الأول للمؤسسة.

التوصيات

في ضوء النتائج السابقة فإن الطالب يوصي بالآتي:

1- الانتقال من أدوات الأمان التقليدية إلى حلول الأمن القائمة على الذكاء الاصطناعي والتعلم الآلي خاصة في مجال مراقبة السلوك غير الطبيعي داخل الشبكة، لتمكين الاكتشاف الاستباقي للتهديدات المتطورة التي يصعب كشفها بالأساليب القديمة.

2- إلزام جميع المؤسسات المصرفية بـ دمج الأمن السيبراني كبند دائم في اجتماعات مجلس الإدارة وتحديد مقاييس أداء واضحة للأمن تُرفع دورياً للإدارة العليا لضمان المتابعة واتخاذ القرار على أعلى المستويات.

3- تطبيق تمارين محاكاة هجمات الاختراق سنوية وشاملة بالتعاون مع جهات خارجية متخصصة، بالإضافة إلى إجراء تدريبات محاكاة سيناريوهات الاستجابة للحوادث بشكل ربع سنوي للتأكد من جاهزية الفرق الفنية والإدارية للتعامل مع الأزمات الحقيقية.

4- إطلاق حملات تصيد احتيالي وهمية بشكل عشوائي ومنتظم لاختبار وعي الموظفين بشكل فعلي. وتخصيص تدريب إضافي وإلزامي للموظفين الذين يفشلون في هذه الاختبارات، مع تطوير محتوى تدريبي مخصص حسب طبيعة عمل القسم (مثل تدريب خاص لموظفي التحويلات المالية)

قائمة المراجع

المراجع العربية

1- البغدادي، مروة فتحي السيد (2021)، اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، العدد 76، مصر.

2- البردان، محمد فوزي أمين، وشحاته، محمد موسى علي (2020)، أثر تفعيل حوكمة تكنولوجيا المعلومات في ظل إستراتيجيات الرقمنة على الحد من مخاطر الهجمات السيبرانية بالبيئة المصرية، جامعة مدينة السادات، كلية التجارة، مصر.

3- بوانة، سهيل (2023)، أثر مخاطر الأمن السيبراني على استخدام البطاقات المصرفية في المصارف الإسلامية العاملة في الأردن، رسالة ماجستير، جامعة الإسراء، الأردن.

4- جيلالي، دلالي، وبلبشير، يعقوب (2021)، رهانات الأمن السيبراني الوطني في ظل التحول الرقمي قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية، مجلة كلية القانون الكويتية العالمية، السنة العاشرة، العدد 1، الكويت.

5- الحجرف، حسن نايف مبارك (2024)، دور الذكاء الاصطناعي في تعزيز الأمن السيبراني: رؤى نظرية، مجلة الدراسات الجامعية للبحوث الشاملة، المجلد 5، العدد 32، العراق.

6- كاظم، عمر علي حسين، والمشهداني، بشرى نجم عبد الله (2025)، التكنولوجيا المالية في ظل تحديات الأمن السيبراني ودورها في القطاع المصرفي، المؤتمر الدولي الخامس للعلوم الإدارية والمالية، جامعة بغداد، كلية الإدارة والاقتصاد، العراق.

7- كاعوه، عبير أحمد علي (2020)، سياسات الأمن السيبراني لتعزيز التحول الرقمي بالجامعات المصرية رؤية مقترحة في ضوء الخبرات العالمية، مجلة دراسات تربوية واجتماعية، المجلد السادس والعشرين، الجزء الثالث، مصر.

المراجع الأجنبية

1- Adejumo, A., & Ogburie, C. (2025). The role of cybersecurity in safeguarding finance in a digital era. *World Journal of Advanced Research and Reviews*, *25*(03), 1542-1556.

2- Al-Alawi, A. I., & Al-Bassam, M. S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University*, *14*(7), 1523-1536.

3- Amato, E., Fraudatario, M. C., & Bernaschi, D (2024). Cyber risk management in the financial sector: An evaluation of current practices in modern scenarios. Journal of Finance and Management (Volume,2 Issues 4)

4- Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8).

5- European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape: Finance sector. Available at:
https://www.enisa.europa.eu/sites/default/files/2025

6- Lee, H. & Kumar, R (2023) "Enhancing Cyber Threat Intelligence with Machine Learning: A Case Study on Zero-Day Attacks "Computers & Security, vol1, no4

7- Latif, G. (2022). Cyber Security Analysis of Internet Banking in Emerging Countries - User and Bank Perspectives., vol 2, no 1.

8- Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, *21*(3), 625-643.

9- Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16.

10- Smith, J. et al (2023) "Artificial Intelligence for Cybersecurity: A Systematic Review of Recent Developments and Future Trends , IEEE Access, vol2, no1.

الملحق رقم (1) استمارة استبيان

الأخوة الأعزاء تحية طيبة وبعد..

يقوم الباحثان بإعداد بحث يستهدف تحديد **الأمن السيبراني في القطاع المصرفي في سوريا دراسة ميدانية في المصارف الخاصة السورية** وفي سبيل ذلك تم إعداد هذا الاستبيان لاستقصاء آرائكم، وذلك لإغناء البحث حيث أن إجاباتكم على الأسئلة ستساعد الباحثان في الوصول إلى نتائج قيمة تساهم في إغناء الدراسة علماً أن إجاباتكم ستُستخدم لأغراض البحث العلمي فقط.

ولكم مني فائق الاحترام والتقدير.....

أولاً: البيانات العامة:

الرجاء وضع علامة (x) أمام الإجابة المناسبة:

1- المؤهل العلمي:

إجازة جامعية	معهد متوسط	ماجستير	دكتوراه

2- سنوات الخبرة في العمل:

أقل من 3 سنوات	من 3 إلى أقل 5 سنوات	من 5 إلى أقل من 10 سنوات	10 سنوات فأكثر

3- الموقع الوظيفي

مدير	رئيس قسم	موظف فني	موظف إداري

ثانياً: بيانات الدراسة:

الرجاء وضع علامة (صح) في المربع المناسب للإجابة:

الرقم	الفقرات	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
المتغير المستقل: الأمن السيبراني						
1	يتم تحديث أنظمة التشغيل والبرامج المصرفية بشكل دوري للتعامل مع الثغرات الأمنية الجديدة.					
2	يمتلك المصرف أنظمة جدران حماية وأنظمة كشف ومنع التسلل متقدمة وفعالة.					
3	تُستخدم تقنية التشفير لحماية بيانات العملاء الحساسة أثناء تخزينها ونقلها.					
4	يطبق المصرف سياسات قوية لإدارة كلمات المرور متعددة العوامل للوصول إلى الأنظمة الحيوية.					
5	يتم إجراء اختبارات اختراق دورية ومستقلة على الشبكات والتطبيقات المصرفية.					
6	يعاني المصرف من تحديات في شراء وتحديث المعدات الأمنية بسبب القيود الخارجية.					
7	يتم استخدام أدوات متخصصة لمراقبة سجلات الأحداث وتحليل الأنماط الشاذة في الشبكة على مدار الساعة.					
8	يُجري المصرف فحصاً أمنياً دورياً للمخالفات في إعدادات الأنظمة المصرفية الرئيسية.					
9	توجد استراتيجية واضحة وموثقة للأمن السيبراني معتمدة من الإدارة العليا.					
10	يتم تخصيص ميزانية كافية ومستقلة سنوياً لتطوير وتحسين إجراءات الأمن السيبراني.					

11	يلتزم المصرف بالتعليمات والضوابط الصادرة عن مصرف سورية المركزي المتعلقة بإدارة الأمن السيبراني.					
12	يتم مراجعة سياسات الأمن السيبراني وتحديثها سنوياً لمواكبة التهديدات المتطورة.					
13	يُعتبر الأمن السيبراني جزءاً من عملية اتخاذ القرارات في المشاريع المصرفية الجديدة منذ مرحلتها الأولى.					
14	يتم تحديد ملكية البيانات ومستوى حساسيتها بشكل واضح داخل المصرف وتطبق عليها سياسات حماية متناسبة.					
15	يتم تضمين بنود خاصة بالأمن السيبراني في عقود التعاقد مع الموردين الخارجيين لضمان امتثالهم.					
16	هناك آلية رسمية وفعالة لإدارة تصاريح الوصول للموظفين الجدد والمغادرين.					

17	يتم إجراء تقييمات دورية ومنهجية للمخاطر السيبرانية التي تواجه الأصول الحيوية للمصرف.					
18	لدى المصرف خطة واضحة ومختبرة للاستجابة للحوادث السيبرانية والتعافي منها.					
19	يتم التنسيق والتبادل الفوري للمعلومات حول التهديدات السيبرانية مع المصارف الأخرى والهيئات الحكومية (كالهيئة الناظمة لقطاع الاتصالات).					
20	يتم إجراء تمارين محاكاة للهجمات السيبرانية بانتظام لاختبار جاهزية فريق الاستجابة.					
21	يتم بشكل فعال عزل وفصل شبكات الأنظمة الحيوية المصرفية عن الشبكات المكتبية العادية لتقليل المخاطر.					
22	لدى المصرف خطة مفصلة للتعامل مع هجمات حجب الخدمة الموزعة التي تستهدف الخدمات المصرفية الإلكترونية.					

23	يمتلك المصرف القدرة على تحديد الهجمات السيبرانية ذات الدافع الجيوسياسي أو التخريبي وتمييزها عن الهجمات المالية التقليدية.					
24	يتم تقييم مخاطر أمن سلسلة التوريد الناتجة عن الاعتماد على مقدمي الخدمات المحليين.					

25	يتلقى جميع الموظفين (بما في ذلك غير التقنيين) تدريباً إلزامياً دورياً حول مخاطر التصيد الاحتيالي.					
26	يوجد نقص واضح في الكوادر الفنية المؤهلة والمتخصصة في الأمن السيبراني داخل المصرف.					
27	يتم اختبار وعي الموظفين الأمني بشكل دوري (مثل إرسال رسائل تصيد وهمية).					
28	تخصص المصارف موارد لتدريب كوادرها على أحدث التقنيات والتهديدات الأمنية العالمية رغم صعوبة السفر والقيود.					
29	يتمتع الموظفون بالثقافة الكافية للإبلاغ الفوري عن أي حوادث أو رسائل مشبوهة دون خوف من العقاب.					
30	يمتلك الموظفون العاملون عن بعد (إن وجدوا) أدوات وبرامج حماية مناسبة ومراقبة من قبل المصرف.					
31	تأخذ برامج التوعية بالأمن السيبراني المصممة للمصرف بعين الاعتبار التهديدات المحلية الخاصة بالبيئة السورية.					
32	هناك صعوبة في اجتذاب الكفاءات السورية المتخصصة في الأمن السيبراني والاحتفاظ بها بسبب المنافسة أو الهجرة.					

المتغير التابع: فاعلية حماية القطاع المصرفي (المرونة السيبرانية) **يقيس هذا الجزء مدى نجاح الإجراءات المطبقة في تحقيق الحماية والقدرة على الاستمرار.**						
1	يمتلك المصرف القدرة على اكتشاف معظم الحوادث السيبرانية قبل أن تتسبب بأي خسائر مالية أو تشغيلية كبيرة.					
2	استطاع المصرف الوفاء بمتطلبات "الحد الأدنى" من الخدمات المصرفية بشكل مستمر حتى أثناء وقوع حوادث أمنية.					
3	يُعد وقت استعادة الأنظمة المصرفية الحيوية بعد تعرضها لهجوم سريعاً ومقبولاً.					
4	زادت ثقة العملاء بالخدمات المصرفية الإلكترونية في المصرف نتيجة لتدابير الأمن السيبراني الواضحة والملموسة.					
5	تعتبر بيئة تكنولوجيا المعلومات في المصرف مرنة وقادرة على التكيف مع التهديدات السيبرانية غير المتوقعة					
6	يساهم مستوى الأمن السيبراني الحالي في المصرف في تعزيز التزامنا بضوابط مكافحة غسل الأموال وتمويل الإرهاب.					
7	أدت الإجراءات الأمنية الحالية إلى انخفاض ملحوظ في عدد الشكاوى المتعلقة باحتيال العملاء أو فقدان بياناتهم.					
8	يتمكن المصرف من استعادة العمليات المصرفية الحيوية (مثل التسويات) بشكل كامل خلال 24 ساعة من وقوع حادث كبير					

ولكم جزيل الشكر....