



جامعة ميدأوشن

كلية العلوم الإنسانية

تخصص قانون رقمي

دور الأنظمة الحديثة في حماية المعلومات السرية من مخاطر الاختراق

دراسة تطبيقية على البنك المركزي السعودي

إعداد الطالب/

صالح بن سعد محمد الشهراني

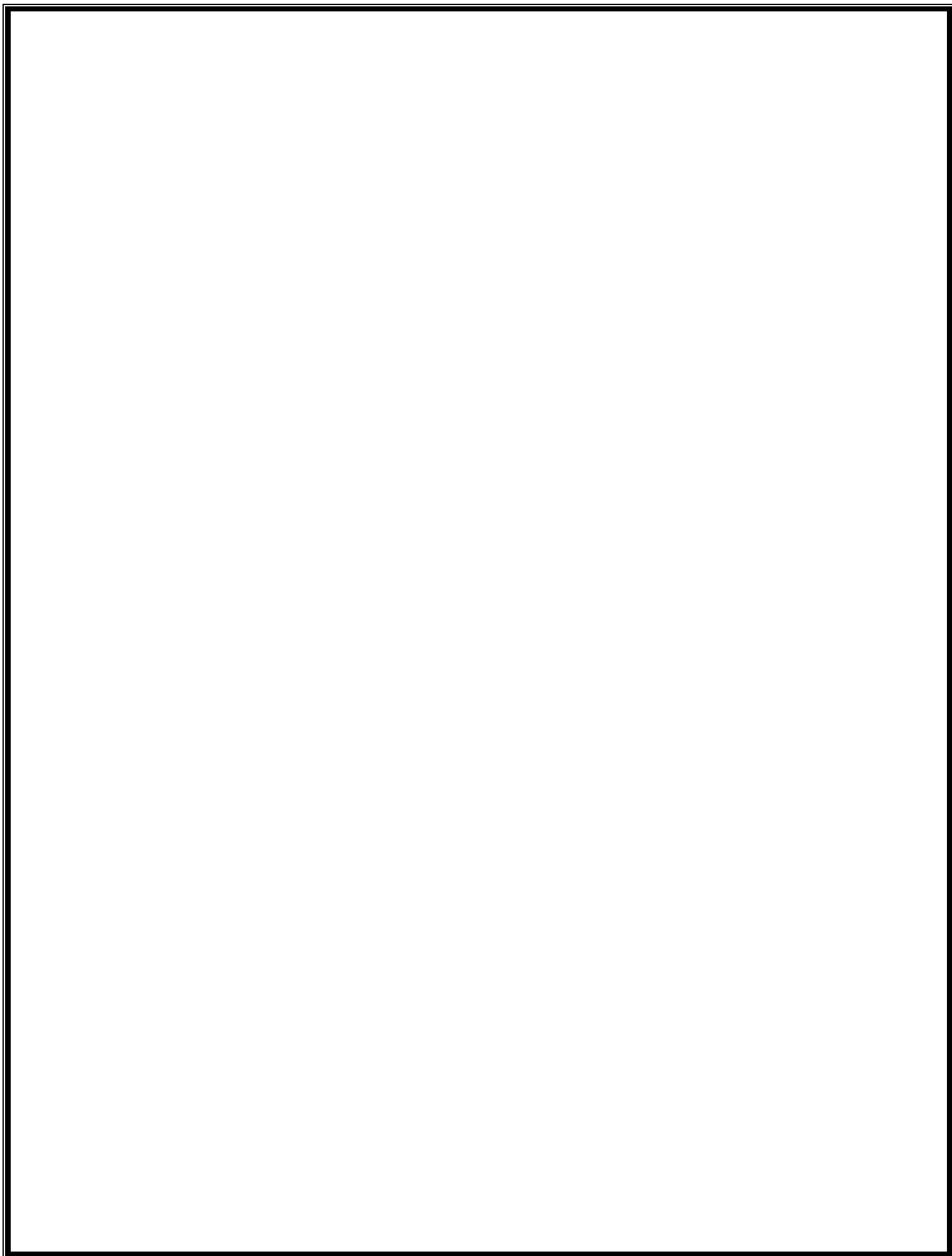
242000156

إشراف/

د. أسماء ابوعنزة

العام الدراسي:

2024



4	المقدمة:
5	مشكلة الدراسة:
6	أهداف الدراسة:
6	أهمية الدراسة:
7	تساؤلات البحث :
8	فروض الدراسة :
9	دراسات سابقة :
17	الفجوة البحثية:
18	المنطلقات النظرية للدراسة:
19	المنهجية وطرق البحث :
20	المراجع :

المقدمة:

مع التطورات السريعة في التكنولوجيا والتحول الرقمي أصبحت المعلومات والبيانات من الأصول الأكثر قيمة للمؤسسات المالية ويشكل الأمن السيبراني جزءًا حيويًا من حماية هذه الأصول خاصة في المؤسسات المالية الكبرى مثل البنك المركزي السعودي والتي تحتوي على قواعد بيانات ضخمة تحتوي على معلومات حساسة. (جونز ، 2019)

وفي هذا السياق تصبح حماية المعلومات السرية من محاولات الاختراق والهجمات الإلكترونية مسؤولية ذات أهمية قصوى للحفاظ على استقرار النظام المالي وثقة الجمهور تواجه المؤسسات المالية اليوم تهديدات متزايدة ومعقدة من حيث التنوع والتكنولوجيا المستخدمة في الهجمات الإلكترونية مما يدفعها إلى تبني أنظمة أمنية متقدمة تعتمد على أحدث الأساليب والتقنيات لضمان حماية البيانات وتشمل هذه الأنظمة الحديثة تقنيات الذكاء الاصطناعي والتعلم الآلي وتحليل البيانات الضخمة وأنظمة التشفير القوية بالإضافة إلى أنظمة المراقبة والاستجابة الفورية. (العتيبي، 2020)

تعتبر الحماية الرقمية أحد أهم القضايا في العصر الحديث، حيث تشهد التكنولوجيا تطورًا سريعًا مما يفتح أبوابًا جديدة للتهديدات والمخاطر على الأفراد والمؤسسات، ومع تزايد الاعتماد على الأنظمة الرقمية في كافة جوانب الحياة، من إدارة الأعمال إلى حفظ المعلومات الشخصية والحكومية، أصبح تأمين البيانات وحمايتها من الاختراقات أمرًا بالغ الأهمية. (سليمان ، 2019)

تختلف طرق الحماية وتتنوع التقنيات المستخدمة في الحفاظ على سرية المعلومات، وتبرز أهمية دور الأنظمة الحديثة التي تم تطويرها لمكافحة هذه التهديدات هذه الأنظمة تشمل أدوات وتقنيات متقدمة تهدف إلى

تعزيز الأمان الرقمي وتوفير بيئة آمنة لانتقال البيانات وحفظها إذ إن حماية المعلومات السرية أصبحت تحديًا معقدًا يتطلب استخدام أنظمة متكاملة تساهم في الوقاية والكشف عن المخاطر والتعامل معها بسرعة وفعالية. من بين هذه الأنظمة، تأتي تقنيات مثل التشفير، وأنظمة الكشف عن التسلل، وأدوات المصادقة متعددة العوامل كأمثلة بارزة على الجهود المبذولة لحماية المعلومات من المخاطر المتزايدة، وعليه تمثل الأنظمة الحديثة حجر الزاوية في استراتيجيات الأمان السيبراني التي تهدف إلى مواجهة مخاطر الاختراقات والحفاظ على سرية المعلومات في ظل التهديدات المتطورة.

مشكلة الدراسة:

في ظل التقدم التكنولوجي المتسارع يشهد القطاع المالي زيادة كبيرة في الهجمات السيبرانية التي تستهدف المعلومات السرية والبيانات الحساسة، وتعتبر البنوك المركزية، بما في ذلك البنك المركزي السعودي، من أهم المؤسسات التي تحتاج إلى حماية بياناتها بدقة وفاعلية لضمان استقرار النظام المالي وحماية بيانات الأفراد والشركات لكن مع تطور تقنيات الهجمات وأساليب الاختراق، تبرز تحديات عديدة أمام الأنظمة الأمنية التقليدية.

يتمثل جوهر المشكلة في معرفة مدى قدرة الأنظمة الأمنية الحديثة التي يعتمد عليها البنك المركزي السعودي على حماية المعلومات السرية والتصدي لمخاطر الاختراق المتزايدة، ومدى كفاءة هذه الأنظمة في مواجهة تهديدات سيبرانية تتسم بالتطور المستمر، ما يثير التساؤل حول فعالية هذه التقنيات وقدرتها على تأمين البيانات في مواجهة التهديدات المتنامية.

تسعى هذه الدراسة إلى استكشاف دور الأنظمة الحديثة التي يتبناها البنك المركزي السعودي في حماية المعلومات السرية من مخاطر الاختراق والهجمات الإلكترونية ومن خلال تحليل السياسات الأمنية والتقنيات

المستخدمة تهدف الدراسة إلى فهم مدى فعالية هذه الأنظمة في حماية المعلومات الحساسة وتحديد التحديات التي تواجه البنك في تحسين وتطوير أنظمة الحماية.

أهداف الدراسة:

1. تحليل السياسات الأمنية التي يتبعها البنك المركزي السعودي ودورها في حماية المعلومات

السرية

2. تقييم فعالية الأنظمة الحديثة المستخدمة لحماية المعلومات من التهديدات الإلكترونية

3. تحديد التحديات والعقبات التي تواجه البنك المركزي السعودي في تطوير أنظمة الحماية

4. اقتراح تحسينات على أنظمة الأمن لتعزيز حماية المعلومات السرية

أهمية الدراسة:

تعتبر حماية المعلومات السرية في القطاع المصرفي من أهم التحديات التي تواجه المؤسسات المالية في عصر التحول الرقمي حيث أدى التطور التكنولوجي وانتشار البيانات إلى زيادة احتمالية التعرض للهجمات السيبرانية التي تستهدف البيانات الحساسة، مما يجعل من الضروري تطبيق أنظمة أمنية متقدمة وفعالة وفي المملكة العربية السعودية، يلعب البنك المركزي السعودي دورًا حيويًا في ضمان أمن واستقرار النظام المالي، مما يعزز أهمية دراسة فعالية الأنظمة الأمنية المستخدمة في حماية المعلومات السرية وتقييم قدرتها على مواجهة التهديدات المتزايدة.

• الأهمية العلمية:

تقدم هذه الدراسة مساهمة علمية في مجال أمن المعلومات السيبراني، خصوصًا في القطاع المالي، من خلال تحليل الأنظمة الأمنية الحديثة المستخدمة في حماية البيانات ستضيف الدراسة إلى الأدبيات العلمية عبر توضيح تقنيات الحماية المتطورة وتقييم فعاليتها ضمن بيئة مصرفية مهمة كالبنك المركزي السعودي، بما يسهم في إغناء المعرفة حول كيفية التصدي للتهديدات السيبرانية المعقدة.

• الأهمية العملية:

تساعد هذه الدراسة صناع القرار والمختصين في البنك المركزي السعودي في اتخاذ خطوات محسوبة لتعزيز أنظمة الحماية المعتمدة حاليًا ومن خلال تحليل فعالية الأنظمة الحالية، يمكن اقتراح تحسينات وإجراءات محددة تساهم في تعزيز الحماية وتقليل فرص الاختراق، مما ينعكس إيجابًا على ثقة العملاء ويعزز استقرار النظام المالي السعودي.

تبرز أهمية هذه الدراسة في توفير فهم عميق للإجراءات الأمنية المتبعة في مؤسسة مالية مرموقة مثل مؤسسة النقد العربي السعودي (البنك المركزي السعودي) والتي تعتبر قلب النظام المالي في المملكة و يساهم هذا البحث في توضيح كفاءة أنظمة الأمن المتبعة بالإضافة إلى تقديم توصيات لأفضل الممارسات في مجال الحماية السيبرانية

تساؤلات البحث :

- ما هي السياسات الأمنية المتبعة لدى البنك المركزي السعودي؟
- ما هي الأنظمة الحديثة التي يعتمد عليها البنك المركزي السعودي لحماية المعلومات؟

- ما مدى فعالية هذه الأنظمة في حماية المعلومات السرية؟
- ما هي التحديات والعقبات التي تواجه البنك المركزي السعودي في حماية المعلومات؟
- ما هي التوصيات الممكنة لتحسين أنظمة حماية المعلومات السرية لدى البنك المركزي السعودي؟
- كيف يمكننا رفع مستوى الوعي لدى الموظفين والمستخدمين بأهمية الأمن السيبراني وأفضل ممارساته؟

فروض الدراسة :

وقد تم صياغة مجموعة من الفرضيات التي ستساعد في اختبار الفرضيات وتوجيه التحليل على النحو

التالي:

1- أن تطبيق سياسات الأمن الحديثة في البنك المركزي السعودي يساهم بشكل فعال في حماية

المعلومات السرية من مخاطر الاختراق

2- أن الأنظمة الحديثة مثل الذكاء الاصطناعي والتعلم الآلي تلعب دوراً حيوياً في الكشف

المبكر والاستجابة للهجمات السيبرانية

3- أن أنظمة الحماية في البنك المركزي السعودي فعالة للغاية في حماية المعلومات مقارنة

بالمؤسسات المالية الأخرى

4- إن البنك المركزي السعودي يواجه تحديات فنية وتنظيمية تحد من قدرته على تعزيز مستوى

الحماية الأمنية

5- يمكن تحسين أنظمة حماية المعلومات السرية في البنك المركزي السعودي من خلال زيادة

الاستثمار في التكنولوجيا وتدريب الموظفين

دراسات سابقة :

1- دراسة (كريستوفر، 2019) ، بعنوان " تحليل استراتيجيات الأمن السيبراني في البنوك

المركزية: دراسة حالة على البنك المركزي الأمريكي "

تناولت هذه الدراسة الاستراتيجيات التي يستخدمها بنك الاحتياطي الفيدرالي الأمريكي لحماية المعلومات المالية الحساسة وشملت مراجعة تقنيات تحليل التنبؤ المتقدمة وتقييم فعالية أنظمة الذكاء الاصطناعي في التنبؤ بالتهديدات قبل وقوعها وأظهرت الدراسة أن الاعتماد على الذكاء الاصطناعي يساهم بشكل كبير في خفض معدلات الهجمات الناجحة

واعتمد جونز على منهج دراسة الحالة من خلال تحليل معمق لأنظمة الأمن في بنك الاحتياطي الفيدرالي الأمريكي بما في ذلك مراجعة الأدبيات المتخصصة ودراسة التقارير والبيانات الصادرة عن البنك والمقابلات مع المتخصصين في الأمن السيبراني.

من أهم النتائج التي توصلت إليها الدراسة (الحاجة إلى التحديث المستمر أشارت الدراسة إلى الحاجة إلى تطوير وتحديث أنظمة الأمن لمواكبة التهديدات المتزايدة، التدريب والتوعية أكدت الدراسة على أهمية رفع الوعي وتدريب الموظفين لمواجهة التهديدات السيبرانية بشكل فعال، التعاون بين المؤسسات أوصت الدراسة بتعزيز التعاون بين البنوك المركزية والمؤسسات الأخرى لتبادل المعلومات حول التهديدات المحتملة.

2- دراسة (العتيبي، 2020) ، بعنوان " الأمن السيبراني في القطاع المالي السعودي: التحديات

والحلول "

ركزت هذه الدراسة على تحديات الأمن السيبراني في البنوك السعودية بما في ذلك البنك المركزي السعودي واستعرضت الدراسة التقنيات الحديثة المستخدمة مثل التشفير المتقدم وأنظمة المصادقة البيومترية كما قدمت توصيات لمعالجة التهديدات المتزايدة بما في ذلك تعزيز وعي الموظفين وتحسين كفاءة نظام الأمن اعتمد الدكتور العتيبي على التحليل الوصفي من خلال جمع البيانات من مصادر متعددة منها التقارير الحكومية والتقارير الصادرة عن مؤسسة النقد العربي السعودي (ساما) بالإضافة إلى إجراء مقابلات مع متخصصين في الأمن السيبراني في المملكة العربية السعودية كما تم تحليل الأنظمة والسياسات المعمول بها حالياً في البنوك السعودية توصلت الدراسة إلى عدة نتائج مهمة منها (أظهرت الدراسة أن هناك حاجة ملحة لتعزيز الوعي الأمني بين الموظفين والعملاء على حد سواء حيث يساهم نقص الوعي في زيادة خطر التعرض للاختراقات، نقص الكوادر المتخصصة: أكدت الدراسة وجود نقص في الكفاءات المحلية المتخصصة في مجال الأمن السيبراني، مما يزيد من صعوبة معالجة التحديات بشكل فعال، كما أظهرت تطور الأساليب الهجومية: أشار العتيبي إلى أن الأساليب المستخدمة في الهجمات السيبرانية أصبحت أكثر تعقيداً وتنوعاً مما يتطلب استخدام تقنيات متقدمة ومرنة لمواجهتها.

أوصت الدراسة بعدة توصيات لتعزيز الأمن السيبراني في القطاع المالي السعودي منها الاستثمار في التدريب والتطوير تدريب الموظفين على أفضل ممارسات الأمن وتوفير برامج توعوية لزيادة وعي العملاء بالأمن الإلكتروني

كما أوصت بتعزيز البنية التحتية التكنولوجية الاستثمار في التقنيات الحديثة مثل الذكاء الاصطناعي وتحليل البيانات لتحسين أنظمة الكشف عن التهديدات و التعاون الإقليمي والدولي: تعزيز التعاون بين

المؤسسات المالية السعودية والمؤسسات الأخرى في المنطقة لتبادل المعلومات والخبرات في مجال الأمن السيبراني

3-دراسة (بريان، 2018) ، بعنوان " أثر تطبيق أنظمة حماية المعلومات على أمن البيانات

في البنوك التجارية"

تناولت هذه الدراسة تأثير أنظمة أمن المعلومات على أمن البيانات في البنوك التجارية وتم تحليل العديد من التقنيات الحديثة مثل إدارة الهوية والمصادقة المتعددة وأثرها في الحد من الاختراقات وأشارت النتائج إلى أن البنوك التي تعتمد على أنظمة أمنية متقدمة تتمتع بمستوى أمان أعلى مقارنة بالبنوك التي تعتمد على هذه الأنظمة

اعتمد الباحثون على المنهج الكمي والنوعي في جمع وتحليل البيانات وتضمنت الدراسة استبانات وزعت على عدد من العاملين في البنوك التجارية بالإضافة إلى مقابلات مع مديري الأمن السيبراني في هذه المؤسسات كما استخدم الباحثون تحليل البيانات من تقارير أمن البنوك لدراسة تأثير تطبيق أنظمة الحماية على فعالية الأمن السيبراني ، توصلت الدراسة إلى عدة نتائج أبرزها (تحسين الأمن ولكن ببطء: أظهرت النتائج أن تطبيق أنظمة حماية المعلومات له تأثير إيجابي على أمن البيانات ولكن التقدم يكون بطيئاً في بعض الأحيان بسبب التعقيدات التقنية، تكاليف التنفيذ المرتفعة: أشارت الدراسة إلى أن تطبيق أنظمة الحماية يتطلب استثمارات مالية كبيرة مما قد يشكل عائقاً للبنوك الصغيرة أو المتوسطة الحجم، الحاجة إلى التحديث المستمر: أكدت الدراسة أن فعالية أنظمة حماية المعلومات تعتمد على التحديث المستمر لمواكبة التغيرات في أساليب الهجوم السيبراني مما يتطلب مراقبة وتطويراً دورياً

أوصت الدراسة بعدة نقاط مهمة لتحسين أمن البيانات في البنوك التجارية أبرزها: ضرورة توفير تدريب دوري للموظفين لتعزيز الوعي بأهمية أمن المعلومات وكيفية التصرف في حالات التهديد و الاعتماد على التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي، للكشف عن التهديدات والسيطرة عليها بشكل أسرع، وأوصت التعاون مع شركات الأمن السيبراني: توسيع الشراكات مع المؤسسات المتخصصة في الأمن السيبراني لتحديث الأنظمة والحصول على الدعم الفني المتقدم

4-دراسة (هوا، 2021)، بعنوان " دور الذكاء الاصطناعي في حماية المعلومات السرية في

القطاع المالي"

ناقشت الدراسة كيفية استخدام تقنيات الذكاء الاصطناعي مثل التعلم الآلي وتحليل البيانات الضخمة للكشف عن محاولات الاختراق وتحليل الأنشطة المشبوهة وأظهرت الدراسة أن الذكاء الاصطناعي يساهم بشكل كبير في تحسين سرعة اكتشاف التهديدات ويساعد في تحسين دقة التنبؤ بالأنشطة الضارة المحتملة اعتمدت تشانغ على المنهج التجريبي والتحليلي حيث تم تحليل عدة حالات لدور الذكاء الاصطناعي في حماية البيانات داخل المؤسسات المالية المختلفة كما تم تحليل بيانات ونتائج أنظمة الذكاء الاصطناعي المعتمدة في مجال الأمن السيبراني من خلال تحليل النتائج التي تم جمعها من مؤسسات متعددة والاعتماد على البيانات الصادرة عن شركات الأمن الرقمي ، توصلت الدراسة إلى نتائج مهمة و أبرزها (تحسين كفاءة الكشف عن التهديدات: تبين أن الذكاء الاصطناعي يمكنه اكتشاف التهديدات بشكل أسرع بكثير من الأنظمة التقليدية وذلك لقدرته على التعلم والتكيف مع أساليب الهجوم الجديدة، تحليل الأنماط والسلوك: يمكن للذكاء الاصطناعي تحليل سلوك المستخدم وتحديد الأنماط غير الطبيعية مما يساهم في مواجهة محاولات الاختراق

التي تعتمد على الوصول غير المصرح به، تقليل الأخطاء البشرية: أكدت الدراسة أن الاعتماد على الذكاء الاصطناعي يقلل من الاعتماد على العامل البشري في الكشف عن التهديدات مما يقلل من الأخطاء المحتملة). أوصت الدراسة بعدة نقاط لتعزيز دور الذكاء الاصطناعي في حماية المعلومات السرية منها الاستثمار في أنظمة الذكاء الاصطناعي التنبؤية لتعزيز القدرات التنبؤية لأنظمة الذكاء الاصطناعي للكشف عن التهديدات قبل حدوثها مما يعزز حماية المعلومات الحساسة و تحديث قواعد البيانات والتعلم المستمر يجب تحديث قواعد البيانات التي تعتمد عليها أنظمة الذكاء الاصطناعي لتشمل التهديدات الجديدة دمج الذكاء الاصطناعي مع الأدوات التقليدية الجمع بين أدوات الحماية التقليدية والذكاء الاصطناعي لتحقيق مستويات شاملة وفعالة من الأمن.

5-دراسة(ريتشارد ،2017) ، بعنوان " فعالية التشفير في حماية المعلومات الحساسة: دراسة

مقارنة بين تقنيات التشفير التقليدية والحديثة "

ركزت الدراسة على مقارنة فعالية تقنيات التشفير التقليدية مثل DES و AES وتقنيات التشفير الحديثة وأثرها في حماية المعلومات السرية وأظهرت النتائج أن تقنيات التشفير الحديثة توفر حماية أفضل وأوصت بضرورة الاعتماد عليها في المؤسسات المالية بسبب التطور المستمر لتهديدات الأمن السيبراني

اعتمد الباحثون على التحليل التجريبي حيث قاموا بتطبيق مجموعة من تقنيات التشفير على عينات من البيانات الحساسة في بيئة تجريبية وتم اختبار الأداء من حيث السرعة وقوة التشفير وقدرتها على تحمل الهجمات كما تم جمع البيانات من الدراسات السابقة وتقارير الأمن لتحليل نقاط القوة والضعف لكل تقنية أظهرت الدراسة عدة نتائج رئيسية منها (قوة التشفير الحديث: وجد أن التشفير القائم على التكنولوجيا الحديثة وخاصة التشفير الكمومي يوفر مستويات أعلى بكثير من الأمان مقارنة بالطرق التقليدية حيث يعتمد التشفير

الكمومي على مبادئ ميكانيكا الكم التي تعيق فك التشفير باستخدام الطرق التقليدية، الكفاءة والسرعة: لوحظ أن التقنيات التقليدية مثل RSA و AES لا تزال فعالة وسريعة للعديد من التطبيقات ولكن التشفير الحديث يتميز بقدرته على توفير حماية أكبر وخاصة في مواجهة التهديدات المتقدمة، تكاليف التحديث: أشارت الدراسة إلى أن اعتماد التشفير الحديث قد يكون مكلفاً ويتطلب بنية تحتية متقدمة، مما قد يشكل تحدياً لبعض المنظمات. أوصت الدراسة بعدة توصيات مهمة لتحسين حماية البيانات الحساسة باستخدام التشفير منها التحول التدريجي نحو التشفير الحديث توجيه المنظمات للبدء بالتحول التدريجي نحو التشفير الحديث مثل التشفير الكمي حيث توفر هذه التقنيات حماية أكبر على المدى الطويل و التحديث المستمر للتشفير التقليدي الحفاظ على تقنيات التشفير التقليدية وتعزيزها خاصة في التطبيقات التي لا تتطلب أماناً عالياً و التدريب والتوعية رفع الوعي بين المتخصصين بتقنيات التشفير الحديثة وأهمية مواكبة التطورات المستمرة في هذا المجال.

6-دراسة (سليمان، خالد، 2019) بعنوان " تأثير التوعية الأمنية على مستوى حماية

المعلومات في المؤسسات المالية"

هدفت هذه الدراسة إلى معرفة تأثير برامج التوعية الأمنية للموظفين على حماية المعلومات وأظهرت الدراسة أن المؤسسات المالية التي تقوم بتدريب موظفيها بشكل منتظم لديها معدلات اختراق أقل بسبب انخفاض الأخطاء البشرية مما يعزز أمن المعلومات الحساسة

اعتمد الباحثون على المنهج الوصفي التحليلي، حيث قاموا بمراجعة الأدبيات السابقة المتعلقة بالأمن السيبراني بالإضافة إلى استخدام الاستبيانات والمقابلات مع الموظفين في المؤسسات المالية المختلفة وتم تحليل بيانات الاستبيان لقياس مستوى الوعي الأمني وتأثيره على سلوك الأفراد في مواجهة التهديدات الأمنية توصلت الدراسة إلى عدة نتائج مهمة أبرزها (زيادة الوعي يعزز الأمن: تبين أن الوعي الأمني يلعب دورًا حيويًا في الحد من المخاطر المتعلقة بسرقة البيانات والاحتيال الإلكتروني حيث يساهم الموظفون المدربون بشكل أفضل في تحسين مستوى الأمن داخل المؤسسات المالية، تحسين سلوك الموظفين: أظهرت الدراسة أن الموظفين الذين يتلقون تدريبًا مستمرًا في مجال الأمن السيبراني يتخذون قرارات أكثر أمانًا مثل تجنب فتح رسائل البريد الإلكتروني المشبوهة أو استخدام كلمات مرور قوية، التحديات في تنفيذ التوعية: أشار الباحثون إلى وجود تحديات تتعلق بتنفيذ برامج التوعية مثل عدم كفاية الموارد أو عدم تفاعل بعض الموظفين مع هذه البرامج).

أوصت الدراسة بعدة استراتيجيات لتحسين الوعي الأمني في المؤسسات المالية منها تعزيز برامج التدريب المستمر فمن الضروري توفير برامج تدريبية دورية للموظفين بما في ذلك محاكاة لهجمات إلكترونية فعلية لتعليمهم كيفية التعامل مع التهديدات و دمج الوعي مع ثقافة المؤسسة فيجب أن يكون الوعي الأمني جزءًا من ثقافة المؤسسة حيث يتم تعزيز السلوكيات الأمنية في جميع جوانب العمل اليومي.

استهداف العملاء أيضًا من المهم للمؤسسات المالية تدريب عملائها على كيفية حماية معلوماتهم الشخصية من خلال الرسائل التعليمية والمواد التوعوية عبر قنوات مختلفة و استخدام التقنيات الحديثة في التوعية مثل تقنيات الواقع الافتراضي أو الذكاء الاصطناعي، والتي يمكن أن تساعد في تقديم برامج تدريبية أكثر تفاعلية وجاذبية

7-دراسة (جون، 2021) بعنوان " التحديات المستقبلية للأمن السيبراني في البنوك المركزية:

الاتجاهات الحديثة والحلول المتاحة "

تستكشف هذه الدراسة التحديات المستقبلية التي تواجه البنوك المركزية في حماية معلوماتها السرية في ظل التطور التكنولوجي السريع وتتناول بعض الحلول المبتكرة مثل الحوسبة الكمومية والتشفير الكمومي وتناقش أهمية تطوير استراتيجيات مرنة تواكب التغيرات السريعة في تكنولوجيات الهجمات السيبرانية.

الدراسات الأجنبية :

8- **Smith, A., & Johnson, L. (2020).** "Cybersecurity Strategies in Central Banks: A Case Study of the Federal Reserve."

تستعرض هذه الدراسة استراتيجيات الأمن السيبراني التي تبناها بنك الاحتياطي الفيدرالي الأمريكي لحماية معلوماته الحساسة في مواجهة التهديدات السيبرانية المتزايدة وتركز الدراسة على توظيف التكنولوجيا المتقدمة مثل الذكاء الاصطناعي والتعلم الآلي لتحليل الأنماط والكشف عن الأنشطة المشبوهة في وقت مبكر ووجدت الدراسة أن استخدام أنظمة الذكاء الاصطناعي والتعلم الآلي ساهم بشكل فعال في تحسين كفاءة اكتشاف التهديدات وسرعة الاستجابة مما ساهم في تعزيز مستوى الأمان وأوصت الدراسة بزيادة الاعتماد على الحلول التقنية المتقدمة وأنظمة التحليل التنبؤي بالإضافة إلى تعزيز تدريب الموظفين على إدارة المخاطر السيبرانية لضمان الأمن الشامل

9- **Brown, T. & Miller, C. (2019).** "The Impact of Encryption Technology on Data Security in Commercial Banks."

ملخص: تستكشف هذه الدراسة دور تقنيات التشفير في تعزيز أمن البيانات داخل البنوك التجارية مع التركيز على الفروق بين تقنيات التشفير التقليدية (مثل DES) والتقنيات الحديثة (مثل AES وRSA) وتهدف الدراسة إلى قياس فعالية هذه التقنيات في حماية البيانات وتقليل احتمالية حدوث الخروقات وتوصلت الدراسة إلى أن تقنيات التشفير الحديثة توفر مستوى أعلى بكثير من الأمان مقارنة بالتقنيات التقليدية وذلك بفضل قدرتها على التشفير بكفاءة وسرعة مع صعوبة فك تشفير الأكواد غير المصرح بها وأوصت الدراسة البنوك التجارية بالاعتماد بشكل أكبر على أحدث تقنيات التشفير لضمان حماية قوية لبيانات العملاء وأشارت إلى أهمية الاستثمار المستمر في تحديث أنظمة التشفير لمواكبة التهديدات السيبرانية المتطورة.

الفجوة البحثية:

على الرغم من الجهود الكبيرة التي بذلتها الدراسات السابقة في مجال الأمن السيبراني لحماية المعلومات في القطاع المالي، تظل هناك فجوات بحثية تحتاج إلى الاستكشاف ركزت الدراسات السابقة بشكل رئيسي على عدة جوانب مثل دور الذكاء الاصطناعي في التنبؤ بالتهديدات وتحليل الأنماط (جونز، 2019؛ سميث وجونسون، 2020)، والتشفير كأداة لحماية البيانات في البنوك التجارية (براون وويليامز، 2018؛ براون وميلر، 2019)، ومع ذلك لم تتناول الدراسات السابقة بشكل كافٍ تأثير الأنظمة الأمنية الحديثة على حماية المعلومات السرية في البنوك المركزية، وخاصة ضمن السياق السعودي، حيث تختلف التحديات والبيئة القانونية والسياسات الأمنية عن باقي البنوك المركزية الأخرى.

بالإضافة إلى ذلك، لم تركز الدراسات السابقة على استخدام تحليل شامل يجمع بين الأنظمة التقليدية والذكاء الاصطناعي والتشفير بشكل متكامل، بما يتيح فهمًا أعمق لمدى تكامل هذه الأنظمة في التصدي للتهديدات السيبرانية المستمرة، كما أن معظم الدراسات تركز على الجانب التقني للأمن السيبراني، بينما تغتقر

إلى التطرق إلى العوامل البشرية مثل وعي الموظفين والبرامج التدريبية، والتي تثبت أهميتها في تعزيز الأمن السيبراني (سليمان وعلي، 2019).

بناءً على ما سبق، تسعى هذه الدراسة إلى سد الفجوة من خلال دراسة تطبيقية على البنك المركزي السعودي، مع التركيز على تقييم تكامل الأنظمة الأمنية الحديثة وتحديد فعالية كل من الجوانب التقنية والبشرية في حماية المعلومات السرية في البنوك المركزية ضمن السياق السعودي.

المنطلقات النظرية للدراسة:

تستند هذه الدراسة إلى مجموعة من المنطلقات النظرية التي تدعم الفهم العميق لدور الأنظمة الحديثة في حماية المعلومات السرية من مخاطر الاختراق. وتتضمن هذه المنطلقات ما يلي:

1- نظرية الأمن السيبراني : تعنى هذه النظرية بتحليل أساليب وتقنيات حماية المعلومات والأنظمة الإلكترونية من التهديدات السيبرانية و تركز على فهم المخاطر المحتملة وكيفية إدارتها من خلال تطبيق استراتيجيات أمنية متكاملة و سيتم استخدام هذه النظرية لفهم التحديات التي تواجه البنوك المركزية بما في ذلك البنك المركزي السعودي وكيفية تصميم الأنظمة الأمنية لمواجهة تلك التحديات

2- نظرية إدارة المخاطر : تركز هذه النظرية على عملية تحديد وتقييم المخاطر المرتبطة بالعمليات والأنظمة و تشمل استراتيجيات للتقليل من المخاطر من خلال التقييم المستمر والتحديث سيتم توظيف هذه النظرية في دراسة كيفية تقييم البنك المركزي السعودي للمخاطر المتعلقة بالاختراقات وكيفية تطوير استراتيجيات للتقليل من هذه المخاطر

3- نظرية تكنولوجيا المعلومات : تستند هذه النظرية إلى دراسة تأثير تكنولوجيا المعلومات على الأعمال والعمليات و تشمل تأثيرها على العمليات الداخلية والخارجية للمؤسسات و ستساعد هذه النظرية

في فهم كيفية استخدام البنك المركزي السعودي للتقنيات الحديثة مثل الذكاء الاصطناعي والتشفير لتحسين أمن المعلومات

4- نظرية سلوك المستخدم : تتعلق هذه النظرية بدراسة كيفية تفاعل الأفراد مع الأنظمة والتكنولوجيا بما في ذلك مدى التزامهم بالإجراءات الأمنية المعمول بها و سيتم استخدام هذه النظرية لتحليل سلوك موظفي البنك المركزي السعودي في ما يتعلق بعمليات الأمان السيبراني ومدى وعيهم بالتقنيات والتدابير الأمنية

المنهجية وطرق البحث :

تتطلب دراسة دور الأنظمة الحديثة في حماية المعلومات السرية من مخاطر الاختراق منهجية متكاملة تعتمد على عدة طرق بحثية لتحقيق الأهداف المرجوة وفيما يلي وصف للمنهجية المستخدمة وطرق البحث التي يمكن اعتمادها:

المنهج الوصفي التحليلي : يعتمد هذا المنهج على وصف الظواهر والأنظمة الأمنية المعتمدة في البنك المركزي السعودي، بالإضافة إلى تحليل البيانات والمعلومات المتعلقة بالأمن السيبراني و سيتم استخدامه لجمع المعلومات حول السياسات الأمنية وتقييم فعالية الأنظمة المستخدمة وتحليل التحديات التي تواجهها هذه الأنظمة

المراجع :

- براون، ريتشارد، وتومسون، ديفيد (2017) فعالية التشفير في حماية المعلومات الحساسة: دراسة مقارنة بين تقنيات التشفير التقليدية والحديثة. مجلة الأمن المعلوماتي
- تشانغ، هوا (2021) دور الذكاء الاصطناعي في حماية المعلومات السرية في القطاع المالي، مجلة التكنولوجيا المالية والابتكار
- جونز، بريان، وويليامز، أليكس (2018)، أثر تطبيق أنظمة حماية المعلومات على أمن البيانات في البنوك التجارية. مجلة إدارة وأمن المعلومات
- جونز، كريستوفر (2019) تحليل استراتيجيات الأمن السيبراني في البنوك المركزية: دراسة حالة على البنك المركزي الأمريكي ، مجلة الأمن السيبراني والدراسات المالية
- العتيبي، سعود محمد (2020) الأمن السيبراني في القطاع المالي السعودي: التحديات والحلول ، مجلة الدراسات المالية والأمنية
- علي، نادر سليمان، ومحمد، خالد حسن (2019) تأثير التوعية الأمنية على مستوى حماية المعلومات في المؤسسات المالية. مجلة الأبحاث المالية والتوعية الأمنية
- Smith, Andrew, & Johnson, Linda (2020) *Cybersecurity Strategies in Central Banks: A Case Study of the Federal Reserve*
- Brown, Thomas, & Miller, Charles (2019). *The Impact of Encryption Technology on Data Security in Commercial Banks*

MidOcean University

Faculty of Humanities

Digital Law Specialisation



**The role of modern systems in protecting confidential
information from the risks of hacking A case study on the Saudi
Central Bank**

Preparation:

saleh saad alshahrani

242000156

Supervision:

Dr. Asma Abuanzeh

1446-2024