دور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي

دراسة ميدانية – الجهاز المركزي للرقابة المالية – سورية

المسابقة الرابعة عشرة التي تنظمها المنظمة العربية للأجهزة العليا للرقابة المالية والمحاسبة للبحث العلمي في مجال الرقابة

إعداد الباحثة : عبير زرّاق

الجهاز المركزي للرقابة المالية–فرع حلب

الجمهوريّة العربيّة السوريّة

2024

ملخص البحث

دور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي

يتناول البحث التحديات التي فرضها التطور التكنولوجي على القطاع الحكومي، حيث تتعرض العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات لخطر الخروقات والهجمات السيبرانية.

وبما أنّ الرقابة على نظم المعلومات تعتبر جزءاً أساسياً من استراتيجيات الأمن السيبراني فأصبح هناك حاجة إلى الرقابة على نظم المعلومات من حيث مدى فعاليتها في أداء الأنشطة التشغيلية ومعالجة المعاملات المالية في القطاع الحكومي، فضلاً عن ضمان أمنها السيبراني.

يهدف البحث إلى معرفة دور الرقابة التي يمارسها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني، من خلال الممارسات الرقابية التي يقوم بها إضافةً لتقييمه لنظام الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات في القطاع الحكومي، وقد تناول البحث في الجانب النظري مكونات نظم المعلومات وعناصرها، مفهوم وأهمية أمن المعلومات، ومفهوم الأمن السيبراني ومتطلبات تحقيقه ومخاطره، وسلّط الضوء على أهمية الرقابة كأداة حيوية لتعزيز الأمن السيبراني في القطاع الحكومي.

ولتحقيق أهداف البحث تم إعداد استبيان صُمِّم بالاعتماد على الجانب النظري ذي العلاقة والدراسات السابقة، وقد تضمن الاستبيان الفرضية الأولى المتعلقة بدور المتغيرات الديموغرافية لأفراد عينة البحث (الجنس العمر، المسمى الوظيفي، المؤهل العلمي، سنوات الخبرة الوظيفية) والفرضية الثانية المتعلقة بالأسئلة عن الرقابة على نظم المعلومات والتي قسمت إلى محورين:

- دور نظم الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي.
- دور الرقابة التي يمارسها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي.

وتم تطبيق الاستبانة ميدانياً على مفتشي فرع الجهاز المركزي للرقابة المالية في محافظة حلب وتوصل البحث إلى عدم وجود فروق جوهرية ذات دلالة إحصائية في إجابات أفراد عينة البحث بما يخص المعلومات الشخصية، حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في

الحد من مخاطر الأمن السيبراني، وفي الفرضية الثانية ففي المحور الأول تبين ووجود دور دال إحصائياً لنظام الرقابة الداخلية والضبط الداخلي استناداً إلى مراجعة بنية وهيكلية الرقابة الداخلية وتقييم الضبط الداخلي من قبل مفتشي الجهاز المركزي للرقابة المالية، أما المحور الثاني فتبين عدم وجود دور دال إحصائياً للممارسات الرقابية التي يقوم بها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي.

وأوصى البحث بعدة توصيات نذكر منها:

تعزيز التدريب والتطوير المهني من خلال تنظيم دورات تدريبية متقدمة ومتخصصة في مجال الأمن السيبراني لجميع موظفي الجهاز المركزي للرقابة المالية، إعداد وتوزيع أدلة إرشادية مفصلة تشرح الأدوار والمسؤوليات والإجراءات المحددة التي يجب اتباعها في مجال الرقابة على نظم المعلومات والأمن السيبراني، توظيف خبراء متخصصين في مجال الأمن السيبراني في الجهاز المركزي للرقابة المالية لتنسيق الجهود وتقديم الدعم الفني لأفراد الجهاز في مهامهم.

قائمة المحتويات

الهيكل المنهجي للبحث

مقدمة:

من التحديات التي فرضها النظام العالمي الجديد في القرن الحالي؛ هو التطور العلمي والتكنولوجي الهائل وتطور دور التكنولوجيا في تسيير عمل المؤسسات حتى صار لا يقتصر على تسجيل البيانات وتحليل المعلومات والقيام بالعمليات الحسابية وإنما أصبح يدير المنشأة إدارة كاملة.[1]

وقضية أمن وسلامة المعلومات تعتبر من أهم قضايا العصر؛ حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير على ما تمتلكه من معلومات، لكن العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بأنواع شتى من الخروقات للمعلومات، كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاتها وتختلف هجمات الهاكرز من جهة لأخرى ومن مكان لآخر ومن زمن إلى زمن مستخدمة أدوات وآليات اختراق متجددة ومتطورة طول الوقت.[2]

ومع ظهور التقنيات الحديثة في نظم المعلومات والتكنولوجيا الرقمية، وتزايد عدد الشركات التي تتواجد على مواقع الإنترنت وتستخدمها في تعاملاتها الرقمية، وتستفيد منها في جوانبها العملياتية والإنتاجية والبيعية وحتى في تحصيل إيراداتها، فقد أصبحت أنظمتها وعملياتها وأنشطتها عرضة للكثير من المخاطر والتهديدات والتحديات ومنها تهديدات الأمن السيبراني؛ ويشمل ذلك فقدان المعلومات الخاصة والحساسة، والتلاعب وإتلاف البيانات والأنظمة والشبكات، وحتى الأصول المادية، وقد تسبب ذلك في تكبد الشركات تكاليف وخسائر كبيرة وتقويض الثقة، وبالتالي فقد برز موضوع الأمن السيبراني (Cyber security) والذي يشمل أمن المعلومات على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرَّح به أو تغيير أو

---

[1] الهلالي، الهلالي الشربيني،2020، مجلة تكنولوجيا التعليم والتعليم الرقمي–الجمعية المصرية للتنمية التكنولوجية، المجلد 1، العدد1 ص3

[2] السمحان، منى عبد الله،2020، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد111، ص1

تعطيل قد يحدث، وعليه فقد أصبح الأمن السيبراني ركيزة أساسية في كل المنظمات والمؤسسات بل وحتى الدول لمواجهة الحروب.[3]

لقد أثيرت التساؤلات عن كيفية الرقابة وأساليب تأكيد الثقة في النظم الإلكترونية والثقة في المواقع الإلكترونية وخاصة أمن المواقع الإلكترونية المخصصة لتبادل المعلومات ذات العلاقة بالحكومة الإلكترونية والأطراف المستفيدة، ولايزال محاطاً بالشكوك والخوف من عدم كفاية احتياطات الأمن المتخذة والمصممة لحماية البيانات المرسلة عبر الشبكة الإلكترونية، ويثار التساؤل عن كيفية حصول المراقب على أدلة الإثبات بشأن إنتاج السجلات التي تتضمن كافة العمليات التي حدثت فيما بين أطراف تعامل متباعدة عبر شبكة الإنترنت، ونتيجةً لنمو الحكومة الإلكترونية فإن الوحدات التي تتعامل معها تتجه إلى التشغيل الفوري للبيانات، فيما ينعكس على المحاسبة في صورة الإدخال الفوري غير الورقي للبيانات، والتشغيل الفوري غير المرئي للبيانات المحاسبية ويؤدي بالضرورة إلى تطوير أساليب الرقابة الحكومية حتى تتكيف مع النظم الفورية، ولكي يحقق المراقب هدف الرقابة بكفاءة وفاعلية، أصبح من الضروري أن يكون مدقق الحسابات على إلمامٍ كافٍ بنظم التشغيل الإلكترونية للبيانات والمشاكل المستحدثة في بيئة النظم وبأحدث المعايير والإجراءات والأساليب.[4]

وإنّ المتغيرات السريعة والمتتالية في بيئة الأعمال عظمت من دور نظم المعلومات والرقابة الداخلية، فنظم المعلومات الحديثة يجب أن تهتم بإدارة البيانات، وتوفير المعلومات اللازمة لتسيير الأعمال، وإنّ أي رقابة داخلية لا تخلو من نظم معلومات فعند قيام مدقق الحسابات الخارجي بمراجعة بنية وهيكلية الرقابة الداخلية سيدقق الدورة الرقابية الخاصة بنظم المعلومات مما سيدفعه إلى دراسة وتقييم نظم المعلومات المستخدمة وبالتالي هناك علاقة بين نظم المعلومات والرقابة الداخلية وإجراءات عمل المدقق (العمل الرقابي).[5]

---

3 علي، هبة جمال هاشم، 2023، منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل، المجلة العلمية للدراسات والبحوث المالية والتجارية، كلية التجارة، جامعة دمياط، م4، ع2، ص2

[4]الخصاونة ، ريم عقاب، 2010، تقييم إجراءات الرقابة الحكومية في ضوء تطبيق الحكومة الإلكترونية في المملكة الأردنية الهاشمية، مجلة جامعة النجاح للأبحاث، مجلد9/24، ص2692 .

[5]جاسم، عذراء ضياء،2020، دور نظم المعلومات والرقابة الداخلية في تعزيز استقلالية العمل الرقابي، مجلة الإدارة والاقتصاد، العدد126.ص186.

وحتى يتمكن المدققون من تحقيق أهداف الرقابة ينبغي عليهم فهم كيفية حفظ الأنظمة من التهديدات المختلفة وامتلاك فهم جيد لأنظمة المعلومات وقدراتها والمخاطر التي تواجهها.[6]

وتأسيساً على ما سبق فقد سعت الباحثة إلى:

معرفة دور الرقابة على نظم المعلومات التي يمارسها الجهاز المركزي للرقابة المالية في الحد من مخاطر الأمن السيبراني في القطاع الحكومي.

ومن أجل ذلك قامت الباحثة بتقسيم البحث إلى جزئيين:

أ- جزء مرتبط بالجانب النظري

ب- جزء مرتبط بالجانب العملي التحليلي للدراسة

تم تحديد الإطار العام للبحث ليعطي القارئ فكرة كاملة عن مشكلة البحث وأسئلته وفرضياته وأهداف البحث وأهميته وحدوده وصعوباته والدراسات السابقة، وقد تناولت الباحثة الجانب النظري ابتداءً من مقدمةٍ عن موضوع البحث مكون من فصلين كما يلي :

الفصل الأول: الرقابة على نظم المعلومات

الفصل الثاني: ماهية الأمن السيبراني

أما الجزء الثاني فخصص للدراسة الميدانية، حيث تناول الطريقة والإجراءات الخاصة بهذا البحث، وتم توضيح منهج البحث ومجتمعه وعينته وأدواته ومصادر الحصول على المعلومات ومن ثم عرض النتائج والتوصيات.

1- مشكلة البحث:

في ظل التطور التكنولوجي المتسارع وإدخال تقانة المعلومات وربط الشبكات في الجهات الحكومية والاتجاه نحو الحكومة الإلكترونية وأتمتة العمل الإداري والمالي؛ فإن هذا التطور التكنولوجي أدى إلى اعتماد أنظمة المعلومات في مختلف القطاعات لإدارة عملياتها اليومية، وبالتالي تزايدت المخاطر السيبرانية بشكل كبير، هذه المخاطر تشمل التهديدات السيبرانية مثل الهجمات الإلكترونية، واختراقات البيانات والبرمجيات الخبيثة، والتي يمكن أن تتسبب في خسائر مالية فادحة وفقدان الثقة بين العملاء، والإضرار بسمعة المؤسسات، ومع توسع استخدام خدمات

[6] ديبان، عبد اللطيف، 2004، نظم المعلومات المحاسبية وتكنولوجيا المعلومات، ص71

الإنترنت عالمياً بصورة عامة وانتشار استخدامه في سورية بصورة خاصة، وظهور التجارة الإلكترونية والحكومة الإلكترونية والاعتماد على خدمات الإنترنت في نواحي كثيرة، ظهر الجانب السلبي لاستخدام الإنترنت وذلك بظهور أنماط جديدة من الجرائم المستحدثة على هذه الخدمة وهو ما يطلق عليه اسم الجرائم المعلوماتية وما تشمله من أعمال القرصنة والتجسس وانتهاك خصوصيات الغير وجرائم سرقة المعلومات.

لذلك كان هناك حاجة ماسة إلى تعاون دولي للحد من تلك الجرائم الإلكترونية وحماية أمن المعلومات عن طريق تبادل الخبرات والتعاون على إيجاد وسائل قانونية وتقنية لمواجهة الأخطار التي تهدد أمن المعلومات.[7]

ويعتبر القطاع العام أكثر عرضةً للهجمات السيبرانية وذلك بسبب:[8]

1- مستودعات البيانات الغنية: غالباً ما تحتفظ مؤسسات القطاع العام بكميات هائلة من البيانات الحساسة بما في ذلك بيانات المواطنين، الأسرار الحكومية، السجلات المالية، وما إلى ذلك..، وتعتبر هذه البيانات ذات قيمة كبيرة لمجرمي الإنترنت لأغراض مختلفة مثل سرقة الهوية أو الاحتيال المالي أو التجسس.

2-البنية التحتية الحيوية: تدير العديد من مؤسسات القطاع العام البنية التحتية الحيوية مثل شبكات الكهرباء وإمدادات المياه وأنظمة النقل ومرافق الرعاية الصحية، ويمكن أن يؤدي تعطيل هذه الأنظمة أو إتلافها من خلال الهجمات السيبرانية إلى فوضى واسعة النطاق، وتعطيل الخدمات الأساسية، بل وحتى تهديد الأمن القومي.

3-الدوافع السياسية: تمثل مؤسسات القطاع العام مؤسسات حكومية، مما قد يجعلها أهدافاً للهجمات السيبرانية ذات الدوافع السياسية، فقد تستهدف مجموعات القرصنة أو الجهات الفاعلة التي ترعاها الدولة، الوكالات الحكومية لتعطيل العمليات أو نشر الدعاية أو سرقة معلومات حساسة لتحقيق النفوذ السياسي.

---

[7] الفوال، عصام، 2020، تقييم إمكانية الاستثمار في تطبيق نظام إدارة أمن المعلومات في قطاع الخدمات والاتصالات السورية، وزارة التعليم العالي، المعهد العالي لإدارة الأعمال، مشروع أعد لنيل درجة الماجستير في إدارة الأعمال، الإدارة التنفيذية، ص2

[8] https://www.skillcast.com مخاطر سيبرانية في القطاع العام، مايو، 2024، فيفيك دود،

4-قيود الميزانية: تعمل مؤسسات القطاع العام غالباً بميزانيات محدودة مخصصة لتدابير الأمن السيبراني مقارنة بنظيراتها في القطاع الخاص، وقد يؤدي ذلك إلى وجود بنية تحتية قديمة أو غير كافية للأمن السيبراني مما يجعلها أكثر عرضة للهجمات السيبرانية.

ويستمر الأمن السيبراني متصدراً قائمة أولويات خبراء الإنترنت وتكنولوجيا المعلومات، وتستمر جهود شركات الأمن السيبراني لمكافحة الجرائم المعلوماتية والهجمات السيبرانية، إلى جانب الجهود القانونية والتشريعات التي تحمي ضحايا هذه الجرائم، ولا تزال المخاوف والمخاطر الإلكترونية تؤرق العديد من الدول وأجهزة الأمن وبالطبع مستخدمي الإنترنت في العالم، ففي النصف الأول من عام 2022 وقع حوالي 2.8 مليار هجوم برمجيات خبيثة(Malware Attacks) في أنحاء العالم و236.1 مليون هجوم طلب فدية (Ransomware Attacks) بحلول عام 2023.[9]

مما يبرز الحاجة الملحة لتطبيق إجراءات فعّالة للحد من هذه المخاطر وبما أنّ الرقابة على نظم المعلومات تعتبر جزءاً أساسياً من استراتيجيات الأمن السيبراني؛ فأصبح هناك حاجة إلى الرقابة على نظم المعلومات من حيث مدى فعاليتها في أداء الأنشطة التشغيلية ومعالجة المعاملات المالية في القطاع الحكومي فضلاً عن ضمان أمنها السيبراني حيث أصبحت تهديدات الأمن السيبراني معقدة ومتكررة بشكل كبير وبالتالي أصبح لزاماً على المؤسسات الحكومية حماية الأنظمة والشبكات الإلكترونية من الهجمات والتهديدات الإلكترونية بشكل استباقي ومراقبة الشبكات والخوادم والتطبيقات بشكل دائم، بحثاً عن التهديدات الأمنية المحتملة والاستجابة لها في الوقت المناسب لضمان سلامة البيانات والعمليات والمعلومات الحساسة.

وبناءً على ذلك فإن مشكلة الدراسة تتلخص بعدم المعرفة الكافية لدور الرقابة على نظم المعلومات التي يمارسها الجهاز المركزي للرقابة المالية في الحد من مخاطر الأمن السيبراني في القطاع الحكومي.

واستناداً لما ذكر آنفاً يمكن إظهار مشكلة البحث من خلال السؤال التالي:

هل للرقابة على نظم المعلومات التي يمارسها الجهاز المركزي للرقابة المالية دور في الحد من مخاطر الأمن السيبراني في القطاع الحكومي ؟

[9]-Lebanon<https://al-akhbar.com

يتفرع عنه السؤالان التاليان:

1- هل يوجد دور لنظام الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي استناداً إلى مراجعة بنية وهيكلية الرقابة الداخلية وتقييمها من قبل الجهاز المركزي للرقابة المالية ؟

2- هل يوجد دور للرقابة التي يمارسها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي ؟

2-أهداف البحث:

يتمثل الهدف الرئيسي في السعي لمعرفة دور الرقابة التي يمارسها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي، ويمكن تقسيم هذا الهدف إلى الأهداف التالية:

1- بيان دور الرقابة التي يمارسها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني من خلال آليات الرقابة التي يستخدمها، إضافةً لتقييمه لنظام الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات في القطاع الحكومي.

2-دراسة مفهوم الأمن السيبراني والتعرف على مخاطره.

3-تحديد نقاط الضعف في عمليات الرقابة الحالية في ضوء نتائج الواقع الميداني قد تساعد في رفع مستوى الأداء، كما يمكن أن تكون دافعاً لتقديم المزيد من البرامج التدريبية المتخصصة.

4-تحديد الاحتياجات التدريبية، وتقديم مقترحات لبرامج تدريبية تساعد موظفي الجهاز المركزي للرقابة المالية في اكتساب المهارات والمعرفة اللازمة لمراقبة نظم المعلومات بفعالية.

5-تقديم توصيات لتحسين ممارسات الرقابة على نظم المعلومات بما يساهم في تعزيز الأمن السيبراني في القطاع الحكومي.

6-تلبية رغبة الباحثة بالتعمق في موضوع الرقابة على نظم المعلومات والأمن السيبراني والتعرف على أنواع التهديدات والمخاطر السيبرانية المختلفة التي تواجه نظم المعلومات، بهدف إثراء المعرفة الأكاديمية والمهنية للباحثة.

3 -أهمية البحث:

يكتسب هذا البحث أهمية خاصة، نظراً لزيادة التهديدات السيبرانية التي تستهدف القطاع الحكومي في ظل التطور التكنولوجي المتسارع وظهور ما يسمى بالحروب الإلكترونية والهجمات السيبرانية التي قد تؤدي إلى مخاطر جسيمة من الناحية القانونية والوضع المالي للمؤسسات المعتمدة على نظم المعلومات في عملها، ومع تزايد اعتماد القطاع الحكومي على التكنولوجيا الرقمية، يصبح تعزيز الأمن السيبراني ضرورة ملحة لحماية البيانات وضمان استمرارية العمل وبالتالي فإن المخاطر المتزايدة تفرض على الجهاز المركزي للرقابة المالية استراتيجيات لتطوير أدائه ليتلاءم مع البيئة الحديثة، وجاء هذا البحث ليعطي أهمية متزايدة لموضوع الرقابة على نظم المعلومات للحد من مخاطر الأمن السيبراني من خلال تعريف المدقق بمكونات نظم المعلومات وكيفية الرقابة عليها وحمايتها من التهديدات والاختراقات.

4- فرضيات البحث:

تنطلق فرضيات البحث من محاولة الإجابة على الأسئلة التي وردت في مشكلة الدراسة على النحو التالي:

الفرضية الأولى:

1-لاتوجد فروق ذات دلالة إحصائية للمتغيرات الديموغرافية (الجنس، العمر، المسمى الوظيفي المؤهل العلمي، سنوات الخبرة الوظيفية) حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي.

2-((لا يوجد دور دال إحصائياً للرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي)).

وتتفرع عنها الفرضيتان الفرعيتان التاليتان:

1-لا يوجد دور دال إحصائياً لنظام الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي استناداً إلى مراجعة بنية وهيكلية الرقابة الداخلية وتقييمها من قبل الجهاز المركزي للرقابة المالية.

2- لا يوجد دور دال إحصائياً للرقابة التي يمارسها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي.

5-حدود البحث:

الحدود المكانية: الجهاز المركزي للرقابة المالية فرع حلب.

الحدود الزمانية: المدة التي استغرقت لإنجاز البحث من تاريخ2024/2/01 و لغاية 2024/06/30

6-منهجية البحث:

فيما يخص الجانب النظري :

اعتمدت الباحثة على المنهج الوصفي التحليلي من خلال الاطلاع على المراجع والأبحاث والدوريات والدراسات السابقة ذات الصلة، إضافةً للمواقع الإلكترونية من أجل تحقيق أهداف البحث.

فيما يخص الجانب العملي : اعتمدت الباحثة على الاستبانة الإحصائية كأداة لإثبات صحة أو نفي فروض البحث، وتم تطبيق الاستبانة ميدانياً على فرع الجهاز المركزي للرقابة المالية في محافظة حلب، حيث تم استقصاء آراء أفراد عينة البحث باستخدام استبيان مصمم بالاعتماد على الجانب النظري ذي العلاقة، والدراسات السابقة لغرض جمع البيانات الأولية التي تخدم البحث، بغية معرفة دور الرقابة على نظم المعلومات للحد من مخاطر الأمن السيبراني في القطاع الحكومي.

وتم جمع البيانات وتحليلها واختبار الفرضيات باستخدام الأساليب الإحصائية والبرنامج الإحصائي ($SPSS_{18}$).

7-مجتمع وعينة البحث:

يتكون مجتمع البحث من مفتشي الجهاز المركزي للرقابة المالية في سورية والبالغ عددهم حوالي 950 مفتش وقد تم سحب عينة متمثلة بمفتشي الجهاز المركزي للرقابة المالية في محافظة حلب والبالغ عددهم 105 وتم استثناء مفتشي التأشير، كونهم لا يقومون بأعمال تدقيق متعلقة بنظم

المعلومات، تم توزيع 77 استبانة على عينة البحث واستعادة 69 استمارة منها 65 استمارة صالحة وتم تحليلها إحصائياً.

8-صعوبات البحث:

من أهم الصعوبات التي واجهت الباحثة خلال إعداد البحث؛ نقص المراجع التي تتحدث عن موضوع الرقابة التي تقوم بها الأجهزة العليا للرقابة المالية على نظم المعلومات والأمن السيبراني ونظراً لحداثة الموضوع فقد تم الاعتماد إلى حد ما على المواقع الإلكترونية.

9-الدراسات السابقة:

1-[10]دراسة ريم عقاب الخصاونة لعام 2009 بعنوان إطار لتقييم رقابة ديوان المحاسبة في المملكة الأردنيّة الهاشميّة في ضوء تطبيق الحكومة الإلكترونيّة:

هدفت الدراسة إلى إبراز أثر الحكومة الإلكترونية على الرقابة الحكومية وإيضاح التحديات الجديدة التي تواجه الرقابة الحكومية ولفت انتباه المدقق في ديوان المحاسبة نحو التحديات التي تستوجب إلمام مراقب الحسابات الكافي بتقنيات الحكومة الإلكترونية وبالمشاكل المتعلقة ببيئة تلك التقنية، والتعريف بأحدث الإجراءات والأساليب في مجال الرقابة الحكومية لعمليات الحكومة الإلكترونية، وتوصلت الدراسة إلى مجموعة من النتائج نذكر منها:

1- الإصدارات القانونية والمهنية في ديوان المحاسبة لا تفي بمتطلبات التدقيق الحكومي في ضوء تطبيق الحكومة الإلكترونية.

2- لا يوجد لدى ديوان المحاسبة أساليب تدقيق تتناسب مع بيئة التدقيق الحكومي في ضوء تطبيق الحكومة الإلكترونية.

3- لا تتوفر لدى العاملين في ديوان المحاسبة المهارات الفنيّة والمعرفيّة التي تفي بمتطلبات التدقيق الحكومي في ضوء تطبيق الحكومة الإلكترونيّة.

---

[10]الخصاونة ،ريم عقاب ،2009، اطار لتقييم رقابة ديوان المحاسبة في المملكة الأردنية الهاشمية في ضوء تطبيق الحكومة الالكترونية
رسالة دكتوراه ،جامعة عمان العربية للدراسات العليا ،الاردن .

2-دراسة ريم عقاب الخصاونة لعام 2010 بعنوان تقييم إجراءات الرقابة الحكومية في ضوء تطبيق الحكومة الإلكترونية في المملكة الأردنية الهاشمية:

هدفت الدراسة إلى التعرّف على إجراءات ديوان المحاسبة في المملكة الأردنية الهاشمية في ضوء تطبيق الحكومة الإلكترونية، وتطرق البحث إلى مجموعة من الإجراءات والخطوات المقترحة للرقابة الحكوميّة، وتوصّل البحث إلى أنه لا يتوفر لدى ديوان المحاسبة إجراءات رقابية ملائمة للعملية الرقابية الحكومية، ووجود قصور في معايير التدقيق الحكومي في المملكة الأردنيّة الهاشميّة، وعدم توفر إجراءات لتنفيذ عملية الرقابة الحكومية في مجال الأنظمة الحكوميّة وأوصى البحث بضرورة وضع إجراءات تدقيق ملائمة في ضوء الحكومة الإلكترونية.[11]

3-دراسة سليم مسلم الحكيم لعام 2010 بعنوان إمكانية الرقابة على نظم المعلومات المحاسبية المؤتمتة للمؤسسات العامة ذات الطابع الاقتصادي من قبل مفتشي الجهاز المركزي للرقابة المالية في سورية:

هدفت الدراسة إلى التعرف على إمكانية القيام بتقييم بنية الرقابة الداخلية المؤتمتة من قبل مفتّشي الجهاز عند قيامهم بعملية تدقيق المؤسسات الاقتصادية التي تستخدم نظم المعلومات المحاسبية المؤتمتة وفق معايير الرقابة على نظم المعلومات بما يتناسب والتطور الحاصل وأوصى البحث بتضمين قوانين الرقابة على المؤسسات العامة، قوانين تلزم مفتش الحسابات بإجراء رقابة على نظم المعلومات المحاسبية وذلك ليتناسب مع التطور الحاصل في المؤسسات العامة في سورية في مجال إدخال تقنية المعلومات، ونشر الوعي بين مفتشي الجهاز بضرورة إجراء الرقابة على نظم المعلومات واستخدام أحدث الأساليب الرقابية لتحقيق ذلك.[12]

4-دراسة آمنة محمد منصور لعام 2021 بعنوان تأثير الأمن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية:

دراسة استطلاعية لآراء عينة من المدققين والمحاسبين في وزارة التعليم العالي والبحث العلمي هدفت الدراسة إلى التعرّف على أهمية الأمن السيبراني من خلال تأثيره على الرقابة الداخلية وقيمة الوحدة الاقتصاديّة باعتماد إطار حوكمة تقنية المعلومات(COBIT5)، ومن أهم

---

[11] الخصاونة، ريم عقاب، 2010 تقييم إجراءات الرقابة الحكومية في ضوء تطبيق الحكومة الإلكترونية في المملكة الأردنية الهاشمية، مجلة جامعة النجاح للأبحاث، مجلد24(9).

[12] الحكيم، سليم مسلم، 2010، إمكانية الرقابة على نظم المعلومات المحاسبية المؤتمتة للمؤسسات العامة ذات الطابع الاقتصادي من قبل مفتشي الجهاز المركزي للرقابة المالية في سوريا، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول.

الاستنتاجات التي توصل إليها البحث؛ أن هناك تقبل واتفاق بشكل عام على وجود علاقة بين أبعاد ومتطلبات الأمن السيبراني على الأطر الحديثة للرقابة الداخلية وقيمة الوحدة الاقتصاديّة، وأوصت الباحثة بضرورة قيام الوحدة الاقتصادية بتبني وسائل فاعلة للتقويم المستمر للرقابة الداخلية للحفاظ على أمن المعلومات باعتماد الأطر الحديثة للرقابة الداخلية لتلافي وسائل اختراق النظم الإلكترونية ومحاولات التلاعب في معلوماتها[13].

5- دراسة حنان هارون فريد لعام 2022 بعنوان الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية:

هدفت الدراسة إلى إظهار دور المراجع في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره على دلالة القوائم المالية، حتى يستطيع المراجع مواكبة التغير السريع في بيئة الأعمال، وخلصت الدراسة إلى وجود تأثير معنوي لأهمية الإفصاح عن تقرير إدارة مخاطر الأمن السيبراني ووجود تأثير معنوي للدور المقترح لمراجع الحسابات وأثره على القوائم المالية.[14]

6-دراسة هبة جمال علي لعام 2023 بعنوان منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل:

هدفت الدراسة إلى التوصل لمنهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل بالبيئة المصرية، وتوصلت الدراسة إلى أن تقييم مخاطر الأمن السيبراني يعتمد على عمليات المراجعة التي تدرس وتقيم مجموعة من الضوابط المحددة مسبقا في مجموعة متنوعة من الموضوعات المتعلقة بالأمن السيبراني وأوضحت الدراسة وجود تأثير طردي معنوي لمخاطر هجمات الأمن السيبراني بمنشأة العميل على أعمال المراجع الخارجي، ووجود ارتباط طردي معنوي بين إدارة الإفصاح عن مخاطر الأمن السيبراني والمنهج الإجرائي المقترح لأعمال المراجع الخارجي، وتوصلت الدراسة إلى عدد من النتائج والتوصيات أهمها

[13] منصور، آمنة محمد، 2021، تأثير الأمن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية، دراسة استطلاعية، مجلة الإدارة والإقتصاد العدد 127، آذار

[14] فريد، حنان هارون، 2022، الدور المقترح لمراجع الحسابات في إضفاء الثقة على تقرير إدارة مخاطر الأمن السيبراني وأثره في دلالة القوائم المالية، معهد المستقبل العالي للدراسات التكنولوجية المتخصصة، المجلد13، العدد الرابع.

تضمين مخاطر الأمن السيبراني كجزء من تقييم المراجع لمخاطر تكنولوجيا المعلومات في منشأة العميل.[15]

7-دراسة جهان عادل أميرهم لعام 2022 بعنوان أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين:

هدفت الدراسة إلى اختبار ودراسة أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين، وتوصلت الدراسة إلى عدم إمكانية أصحاب المصالح متابعة عمليات المخاطر السيبرانية إلا بمساعدة المراجعة الداخلية، وأوصت الدراسة بأنه يتوجب على المراجع الداخلي أن يعيد تأهيل ذاته، وضرورة قيام إدارة المراجعة الداخلية بتقديم تقارير مستقلة إلى مجلس الإدارة ولجنة المراجعة تركز على مخاطر الأمن السيبراني.[16]

<u>ما يميز البحث الحالي عن الدراسات السابقة :</u>

على الرغم من توافر العديد من الدراسات التي تناولت الرقابة على نظم المعلومات والأمن السيبراني من منظور المراجع الخارجي، إلا أن الدراسات التي تناولت موضوع الرقابة على نظم المعلومات والأمن السيبراني من قبل الأجهزة العليا للرقابة المالية مازالت محدودة للغاية(على حد علم الباحثة)، يُظهر هذا النقص في الأبحاث فجوة في المعرفة التي تسعى هذه الدراسة لسدّها، فبينما تركّز الدراسات والأبحاث الحالية بشكل كبير على آليات وأساليب المراجعة الخارجية، تبرز الحاجة إلى فهم أعمق لدور الأجهزة العليا للرقابة المالية في الرقابة على نظم المعلومات وحمايتها من التهديدات السيبرانية في الجهات الخاضعة لرقابتها.

10-مخطط البحث:

يحتوي البحث على(الهيكل المنهجي للبحث) وثلاثة فصول كما يلي:

√الفصل الأول: الرقابة على نظم المعلومات

المبحث الأول: الرقابة

المبحث الثاني: التعريف بنظم المعلومات ومكوناتها

---

[15]علي، هبة جمال هاشم، 2023، منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل، المجلة العلمية للدراسات والبحوث المالية والتجارية، كلية التجارة، جامعة دمياط، م4، ع2.

[16]أميرهم، جيهان عادل، 2022، أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين، مجلة البحوث المالية والتجارية، المجلد23، العدد الثالث.

√الفصل الثاني: الأمن السيبراني

المبحث الأول: مفهوم أمن المعلومات

المبحث الثاني: ماهية الأمن السيبراني

√الفصل الثالث: الدراسة الميدانية وتضمن تصميم الدراسة الميدانية والاستنتاجات والتوصيات.

11-مصطلحات البحث:

1- **نظام المعلومات:** هو مجموعة من الموارد والمكونات المترابطة مع بعضها بشكل منتظم من أجل إنتاج معلومة مفيدة تسمح بالحصول على معالجة، تخزين، وإيصال المعلومات إلى المستخدمين بالشكل الملائم وفي الوقت المناسب من أجل مساعدتهم في أداء الوظائف الموكلة إليهم.

2-الأمن السيبراني: هو منع الضرر الذي يلحق بأجهزة الكمبيوتر وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية والاتصالات السلكية وحمايتها وترميمها، بما في ذلك المعلومات الواردة فيها لضمان توفرها وسلامتها والمصادقة والسرية وعدم الإنكار.

الفصل الأول: الرقابة على نظم المعلومات

المبحث الأول: الرقابة

- **الرقابة المالية:**

لقد أدى تطور الأعمال وتعددها وتشعب الوظائف الإدارية إلى تواجد ضرورة ملحة لعنصر الرقابة المالية سيما مع تطور تنظيم العمل الحكومي فزيادة الأعباء الحكومية وتعقيد التنظيم بالإضافة إلى التطور الهائل الذي لازم تنفيذ المهام المالية استدعى تطور الإجراءات الضابطة لضمان حسن سير الأعمال وتطلب ذلك المزيد من الأنظمة والإجراءات الفعالة للحفاظ على المال العام ومراقبة القائمين على تنفيذ اللوائح والقوانين مما يكفل الالتزام بالتعليمات والقواعد المالية المهنية المعمول بها.[17]

تعتبر الرقابة المالية البوصلة الموجهة للأداء المالي لدى الجهات الحكومية حيث تعتبر أداة مهمة لتحقيق الرقابة على القطاع العام من خلال الإجراءات العديدة التي تمارسها أدوات الرقابة المالية من أجل تعظيم الاستفادة من الموارد المالية للدولة والحفاظ عليها وفق أساليب رقابة فعالة ومعايير الحوكمة بشكل سليم، وتحقيق النتيجة المنشودة من توظيف الميزانيات الحكومية [18].
وبالتالي الرقابة المالية هي عملية الإشراف والفحص والمراجعة من جانب سلطة لها الحق قانوناً للتعرف على سير العمل داخل الجهة محل الرقابة للتأكد من حسن استخدام الأموال العامة للأغراض المخصصة لها، وأن التصرفات تحصل طبقاً للقوانين واللوائح والتعليمات المعمول بها، والكشف عن المخالفات ووسائل علاجها لتفادي تكرارها مستقبلاً من أجل ضمان صحة وسلامة عمليات التحصيل والإنفاق وفقاً للأصول والقواعد المهنية.

- **الجهاز المركزي للرقابة المالية :**

هو هيئة رقابية مستقلة ترتبط برئيس مجلس الوزراء وتهدف أساساً إلى تحقيق رقابة فعّالة على أموال الدولة ومتابعة أداء الأجهزة التنفيذية الإدارية والاقتصادية لمسؤولياتها من الناحية المالية

[17](السيد ،علاء ،2005،إطار مقترح لتطوير أداء الرقابة المالية ،الجامعة الإسلامية ،غزة ،فلسطين ،ص19)
[18](المطيري ، ،يوسف محمد، ،2020، أثر الرقابة المالية لديوان المحاسبة الكويتي على تفعيل معايير الحوكمة بالجهات)

ويختص بتدقيق حساباتها وتفتيشها ويمارس الجهاز رقابة مشروعية ورقابة محاسبية ورقابة كفاية إضافة إلى التحقيق والتفتيش.

يمارس الجهاز المركزي للرقابة المالية اختصاصاته على الجهات والوزارات والإدارات والهيئات العامة ذات الطابع الإداري والجهات التابعة لها، والجهات ذات الطابع الاقتصادي، ويمارس الجهاز أعماله بطريق التدقيق والمراجعة والتفتيش وفقاً للأحكام المنصوص عليها في المرسوم /64/ لعام 2003 ويقوم بأعمال التفتيش من تلقاء نفسه أو بناءً على طلب الجهات العامة أو بناءً على إخبار صريح مقدم من قبل المخبر.[19]

- **الرقابة الداخلية:**

تؤدي وظيفة الرقابة الداخلية في ظل نظام التشغيل الإلكتروني بشكل عام دوراً هاماً ودعماً رقابياً في كل دولة من دول العالم، التي تسعى إلى توفير أجهزة الرقابة المختلفة كعنصر جوهري بالنسبة للرقابة العامة والمساءلة باعتبار أن عملية الرقابة توفر المصداقية في المعلومات التي يتم التدقيق فيها،[20] وتعمل المؤسسات على وضع نظاماً داخلياً للرقابة وذلك لتحقيق أهدافها وحماية أصولها، وبما يكفل سير عملها بشكل صحيح، وهذا بدوره يعكس الالتزام بالسياسات والتعليمات الخاصة بالإدارة العليا، لذلك فقد سعت المؤسسات إلى اتباعها نظام الرقابة الداخلية لما له من أهمية كبيرة في مواكبة متطلبات تكنولوجيا المعلومات وفي تطوير العملية المهنية وذلك في ضوء وضع نظام رقابة داخلي في ظل نظام التشغيل الإلكتروني يعمل على حماية المؤسسات من كافة المخاطر التي تواجهها، ويعد نظام الرقابة الداخلية من أهم الأقسام التي تتطلب مواكبة التطورات وذلك لما لها من أهمية في تزويد الإدارة بالمعلومات التي تحتاجها في اتخاذ القرارات في الوقت المناسب، مما يتطلب تطوير الرقابة الداخلية كون الرقابة الداخليّة قاعدة معلومات للمنظمات وخاصة الإدارة.[21]

---

[19](المرسوم رقم 64 لعام 2003 المتضمن قانون الجهاز المركزي للرقابة المالية)

[20]لطفي، أمين السيد احمد،2007 ، التطورات الحديثة في المراجعة، الدار الجامعية، القاهرة مصر ، ص3

[21]الزيود، أيمن حسن علي،2022، مدى فاعلية الرقابة الداخلية وتطبيقها في ظل نظام التشغيل الإلكتروني من وجهة نظر موظفي بلدية سحاب، المجلة العربية للنشر العلمي،العدد42،ص726،

وتعرّف الرقابة الداخليّة بأنها جميع الإجراءات والوسائل المستعملة داخل الهيئات الإدارية العمومية والتأكد من دقة وصحة البيانات المحاسبية، ومختلف التقارير، ومدى احترام السياسة المرسومة وإن الهدف من هذه الرقابة هو المحافظة على المصلحة العامة، واحترام القوانين والحرص على إنفاق الاعتمادات المالية المفتوحة في الميزانية لغايتها التي رصدت من أجلها كما أن التسيير الجيد للأموال العامة يفترض ضرورة فرض رقابة داخلية على الإدارة ويجب أن تشمل هذه الرقابة مختلف مراحل تنفيذ عمليات النفقات وعمليات الإيرادات.[22]

وعرّف المعهد الأمريكي للمحاسبين الأمريكيين نظام الرقابة الداخلية بأنه: الخطة التنظيميّة ووسائل التنسيق والمقاييس المتبعة في المشروع، بهدف حماية أصوله، وضبط ومراجعة البيانات المحاسبية، والتأكد من دقتها ومدى الاعتماد عليها وزيادة الكفاية الإنتاجية، وتشجيع العاملين على التمسك بالسياسات الإداريّة الموضوعة.

وتعد الرقابة الداخلية من أهم الأدوات لضبط الأداء في القطاع العام، وهي من الآليات التي تعتمد عليها الأجهزة الرقابية العليا في الحكم على انضباط الأداء، وبالتالي فإن هذا يحقق الإصلاح في الوحدات الحكومية وذلك عن طريق الإصلاح المالي والإصلاح الإداري وإحداث التغير نحو الأفضل.[23]

وأشارت الدراسات أنه يتوجب على مراجع الحسابات تحديد مدى الاختبارات التي سيقوم بها باعتماده على نظام الرقابة الداخلية بسبب تحول المراجعة من تفصيلية إلى مراجعة اختبارية،[24]وأن يقوم بتقويم الرقابة الداخلية ونظام الضبط الداخلي وكذلك نظام المراجعة الإدارية ويأخذ نتائج التقويم عند إعداد الخطة التنظيمية لعملية المراجعة وتصميم برامجها واختيار أساليبها، كما يقوم مراجع الحسابات بتقويم التنظيم المحاسبي وسلامة المعلومات المستخرجة منه والاطلاع على تقارير مجلس الإدارة واللوائح وما في حكم ذلك، وللرقابة الداخلية دور هام في الحصول على قوائم مالية على درجة عالية من الشفافية والإفصاح والمصداقية من خلال

[22] Stephanie Damarey; Execution et controle des finans; Gualino Editeur,2007; p115

[23] محمد أمين، وليد ابراهيم،2018، دراسة تحليلية لدور أجهزة الرقابة العليا في تطوير نظم الرقابة الداخلية للحد من الفساد المالي بالوحدات الحكومية، ليبيا المجلة العلمية للدراسات التجارية والبيئية، جامعة قناة السويس، مجلد9، العدد2،ص8.

[24] الجابري، محمد، 2014، تقييم دور المدقق الداخلي في تحسين نظام الرقابة الداخلية لنظم المعلومات المحاسبية في شركات التأمين باليمن، مذكرة لنيل شهادة الماجستير، جامعة صنعاء، اليمن،ص29.

منظومة من أداء الإدارات واللجان والمجالس، وبالتالي هناك علاقة قوية بين الرقابة الداخلية والرقابة الخارجية، والمنظمات بحاجة إلى جهود كليهما معا".[25]

[25] عبد الحساني، وعد هادي، 2016، الرقابة الخارجية وأثرها في تقييم أداء الرقابة الداخلية, https://www.researchgate.net

المبحث الثاني: التعريف بنظم المعلومات ومكوناتها

تلعب نظم المعلومات دورا هاما في حياتنا بشكل عام وفي معظم أنواع الأنظمة بشكل خاص وتستخدم نظم المعلومات في المؤسسات المختلفة مثل (المصارف، أسواق الأوراق المالية الشركة العامة للكهرباء، الشركة العامة للمياه، الشركة العامة للاتصالات، التعليم العالي...)

وقد ازداد تأثير استخدام نظم المعلومات نتيجة توزع أماكن العمل وفروعه في مناطق جغرافية متباعدة والحاجة للتنسيق ما بين عمل هذه الفروع، وبالتالي نشأت الحاجة للقدرة على إدارة هذه النظم وتبادل المعلومات فيما بينها بسهولة ودقة وتكلفة أقل.[26]

وتعتبر هذه الأنظمة العمود الفقري للمؤسسة لإمدادها بالمعلومة المناسبة، ومع التطور التكنولوجي في جميع الميادين أصبحت أنظمة المعلومات مبنية أساساً على قواعد تكنولوجية انطلاقاً من عملية الإدخال ومروراً بعملية المعالجة وصولاً إلى المخرجات والتغذية العكسية.[27]

يشكل كل من الحاسب الآلي والبرمجيات والبيانات العناصر الأساسية لنظام المعلومات في البيئة الرقمية المرتبطة بالمنظمة، وقد يرتبط الحاسب الآلي بواسطة أجهزة وخدمات اتصال في شبكة بنهايات طرفية أو حسابات أخرى أو تسهيلات اتصال معينة، وقد تكون شبكة الحاسبات شبكة محلية LAN أو شبكة خاصة ممتدة على نطاق المصالح الإدارية للمؤسسة كشبكة الإنترنت، أو شبكة المجال العريض WAN كشبكة الإكسترانت أو شبكة معلومات دولية كالإنترنت، كما قد تكون وصلة اتصال خارجية مفتوحة لأي فرد مزود بالوسائل التكنولوجية التي تمكنه في الوصول إليها، وتشتمل كثير من شبكات المعلومات على تجميع من الشبكات الداخلية والخارجية، كما تتضمن شبكات الاتصال على بيانات اتصال، بالإضافة لتليفون وفاكس موديم، ومن الأجهزة الأخرى قد ترتبط الطابعات بأجهزة الحاسبات والاتصالات، وقد تتضمن برمجيات الحاسبات نظم تشغيل وبرمجيات التطبيقات التي تصمم خصيصا" لعميل معين أو منظمة حكومية معينة، وقد تركب البرمجيات في الحاسب الآلي أو تخزن على أقراص مدمجة CD–ROMs أو أي وسائل تخزين أخرى متاحة، وتساند الأدلة الورقية والتوثيقية أو المحمولة والمقروءة إلكترونيّاً تشغيل

---

[26] عداس، ضحى، ساكت، غسان،2020، نظام المعلومات المصرفية، منشورات جامعة حلب ،سوريا، كلية الاقتصاد، ص19–20

[27] مقراني، قدور، 2016، تقييم مدى مساهمة أمن نظم المعلومات الإلكتروني في الحد من مخاطر نظم المعلومات، دراسة حالة مؤسسة اتصالات الجزائر جامعة قاصدي مرباح، ورقلة، الجزائر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، مذكرة لنيل شهادة الماجستير، ص10.

الأجهزة والبرمجيّات واستخدامها وصيانتها، وينشأ الهيكل الكامل لنظم وتطبيقات المعلومات في البيئة الرقميّة بهدف تخزين البيانات والمعلومات ومعالجتها واسترجاعها وإرسالها أو نقلها للمستخدم المستهدف، وتجمع كل هذه العناصر المختلفة والعديدة معاً لتشكّل نظام المعلومات في البيئة الرقمّية.[28]

أولاً- تعريف نظم المعلومات:

تتعدد التعاريف الخاصة بالنظام من حيث الألفاظ المستخدمة، ولكنها تتفق من حيث المعنى ومن أهمها:

♦ نظام المعلومات: هو مجموعة من الموارد والمكونات المترابطة مع بعضها بشكل منتظم من أجل إنتاج معلومة مفيدة تسمح بالحصول على معالجة، تخزين، وإيصال المعلومات إلى المستخدمين بالشكل الملائم وفي الوقت المناسب من أجل مساعدتهم في أداء الوظائف الموكلة إليهم.[29]

♦ أنظمة المعلومات: هي مجموعة من الأجزاء (الأفراد، والتجهيزات، والإجراءات، والمعلومات) المترابطة والمتفاعلة معاً بشكل متناسق من خلال مجموعة من العمليات المنتظمة(تجميع وتخزين، ومعالجة، وتحليل). وعرض المخرجات والنتائج بالأشكال المختلفة للمعلومات (تقارير وأشكال، رسومات، مخططات) وتزود النتائج للمستفيدين من هذا النظام بطريقة تدعم وتخدم قراراتهم وتسهل أعمالهم وتمكنهم من التخطيط والرقابة على نشاطات المنظمة.[30]

♦ وترى الباحثة أن نظم المعلومات(Information Systems) تهتم بدراسة وتصميم وتطوير وإدارة نظم الحاسوب التي تساعد على جمع وتخزين واسترجاع المعلومات وتهدف إلى تحسين أداء المؤسسات عن طريق تسهيل العمليات الإدارية، وتوفير معلومات دقيقة في الوقت المناسب لدعم اتخاذ القرارات وتعزيز الكفاءة والفعالية.

---

[28] عبيرات، مقدم، هواري، معراج، 2022، إدارة مخاطر الأمن وشفافية المعلومات لنظم المعلومات في ظل البيئة الرقمية، جامعة الأغواط، الجزائر،ص1

[29] قاسم، عبد الرزاق محمد، 2008، نظم المعلومات المحاسبية الحاسوبية ، دار الثقافة للنشر والتوزيع، عمان، الأردن، ص19

[30] العبيدي، فاطمة ناجي، 2012 ، مخاطر استخدام نظم المعلومات المحاسبية المحوسبة وأثرها على فاعلية عملية التدقيق في الأردن، مذكرة منشورة للحصول على درجة الماجستير في المحاسبة، ص16

ثانياً– عناصر نظم المعلومات:

يتكون النظام من ثلاثة أجزاء رئيسة تتمثل في:

أ – **المدخلات:** هي كل شيء يأتي من خارج النظام ويدخل إليه، ومدخلات النظام هي موارد مختلفة يتم تحديدها بناء على الأهداف التي يسعى النظام إلى تحقيقها من هذه الموارد (الموارد البشرية، آلات، مواد أولية رؤوس أموال، معلومات إدارية،. الخ).

ب – **المعالجة:** وهي آلية التعامل مع المدخلات وتحويلها إلى مخرجات، حيث يجري على موارد النظام السابقة (المدخلات) عمليات معينة، وهي العمليات التحويلية المختلفة التي تؤدي إلى تحويل هذه المدخلات إلى الأهداف المراد تحقيقها من النظام أو ما يسمى المخرجات.

ج – **المخرجات:** وهي الأشياء الناتجة عن عملية المعالجة والتي تخرج من النظام، وتعبر عن كل ما ينتج عن هذا النظام في شكل سلع ملموسة أو غير ملموسة أو معلومات.

- يمكن تعريف المدخلات والمخرجات وتوضيحها بسهولة، أما آلية المعالجة فتختلف من نظام إلى آخر.
- يمكن أن تكون مدخلات نظام معين هي مخرجات نظام آخر وبالعكس.

ولكي يتم العمل داخل النظام بطريقة سليمة وفعالة لابد من إضافة عنصر رابع إلى مكونات النظام وهو الرقابة (مراقبة أداء النظام في مراحله كافة – التغذية المرتدة أو العكسية).

حيث أن المراقبة (التغذية العكسية) تمثل الإجراءات والتوجيهات التصحيحية المرافقة لمراحل عمل النظام وتأخذ بعين الاعتبار عند وضع الخطط، مع مراعاة طبيعة الظروف المتغيرة وتأثيرها على الخطط والعمليات وأهداف النظام، فهي عمليات وقائيّة وعلاجيّة.

وبالتالي فإنه في كافة نظم المعلومات[31]تسير المعلومة بدءاً من مستخدمي المعلومات، ثم تحويلها إلى مدخلة ثم معالجتها، ثم تحويلها إلى مخرجات، كل هذا من خلال تواجد رقابة عبر كل المراحل.

ويمكن القول أن عمل نظام المعلومات هو الحفاظ على قدرة دائمة للتفاعل مع البيانات، توفير المعلومات في الوقت المطلوب، وضمان الوصول الآمن إليها من خلال قنوات موثوقة، وتقديم الخدمة للمواقع المعلوماتية وضمان عدم تعرض المستخدم لأي قيود تمنعه من الوصول إليها.

[31] مقراني،2016، مرجع سبق ذكره، ص6

ثالثاً- مكونات نظم المعلومات:

1- الأجهزة والمعدات: وتتضمن جميع الأجهزة المادية والمواد المستخدمة في تشغيل المعلومات وتشتمل على:

-نظم الحاسب وتمثل وحدة التشغيل المركزية ووسائل التخزين الثانوية.

-الأجهزة المكملة: وتشتمل على الفأرة ولوحة المفاتيح والشاشات والطابعات.

-الوسائط: وهي جميع الأشياء الملموسة والتي يتم تسجيل البيانات عليها مثل الورق والأقراص الضوئيّة والممغنطة.

2- البرمجيّات: وتشمل جميع أنواع تعليمات تشغيل البيانات.

3-العنصر البشري ويقسم إلى:

-المستخدمين النهائيين ويمثلون الأفراد الذين يستخدمون النظام بطريقة مباشرة أو من يستخدمون مخرجاته المجهزة بواسطة أطراف آخرين.

-الأخصائيون في النظام الآلي ويمثلون الأفراد الذين يشغلون النظام ويطورونه.

4- قاعدة البيانات.

5-الشبكات.

رابعاً- أهمية نظم المعلومات:[32]

1-القيام بحسابات رقمية كبيرة الحجم وبالغة السرعة وتخزين المعلومات والبيانات بكميات كبيرة في مكان صغير يسهل الوصول إليه.

2-تحسين عملية اتخاذ القرارات وتوفير قنوات اتصال للمساعدة على زيادة تدقيق وتبادل المعلومات بشكل آمن.

3-تقليل حدوث الأزمات بما توفره تكنولوجيا المعلومات المستقبلية.

4-السرعة في الطباعة والتحرير للمعلومات والبيانات.

5-زيادة القيمة المضافة وتقاس قيمة المعلومات بمدى تغطية المنفعة الناتجة عنها لتكلفة إعدادها، إضافة إلى تقليل وقت الحصول على المعلومة.[33]

---

[32] المري، راشد محمد، 2022، أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية، مجلة البحوث الفقهية والقانونية، يناير، ص 1319-1320

[33] السديري، محمد بن أحمد، بن تركي، 2012، نظم المعلومات الإدارية، جامعة الملك سعود، ص23.

ويؤدي استخدام تكنولوجيا المعلومات إلى تحسين جودة العمل من خلال سهولة الاتصال والدقة العالية وخفض معدلات التكاليف واختصار الوقت والمجهود وتقليل المخاطر والمساهمة في إمكانية إيجاد منتجات أو خدمات جديدة مع وجود نظام أمني يستطيع حماية تلك المعلومات بالإضافة إلى تقديم الدعم في الموقف التنافسي للمؤسسات والهيئات.

فالتكنولوجيا تتيح الفرصة للمنظمة بأن تعيد النظر في الطريقة التي تدار بها، والتسيير من أجل التوصل إلى فكرة الإدارة المتكاملة، وفي ذات الوقت الحد من الانحرافات والأخطار البشرية وإلغاء الحواجز المكانية والزمانية، فهي تلعب دوراً كبيراً في تطوير جميع المجالات التي لا غنى عنها في حياة الشعوب والمؤسسات والدول.[34]

[34] نور الهدى، شابو،2021، دور تكنولوجيا الاتصال الحديثة في تحسين الخدمة العمومية، مذكرة لنيل شهادة الماجستير، الجزائر، جامعة العربي بن مهدي أم البواقي، ص31

الفصل الثاني الأمن السيبراني

عند دراسة مفهوم الأمن السيبراني لابد من التعرف على مفهوم أمن المعلومات والتمييز بين كل منهما، لأن دراسة مفهوم أمن المعلومات توفر معرفة متكاملة وشاملة حول كيفية حماية المعلومات والنظم التقنية من التهديدات المختلفة.

الفرق الأساسي بين الأمن السيبراني وأمن المعلومات؛ هو في نوع البيانات والمعلومات التي يحميها كل واحد منهم، فالأمن السيبراني يدرس كيفية توفير أمن للمعلومات الإلكترونية فقط، أما أمن المعلومات فهو يدرس كيفية تحقيق أمن المعلومات بمختلف أشكالها مثل الورقية أو الإلكترونية وغيرها من الأنواع.

واستناداً لذلك فإن أمن المعلومات هو التخصص الأشمل كونه يدرس حماية جميع أنواع البيانات، ومن ضمنه الأمن السيبراني.[35]

[35] https://horizons-edu.com

المبحث الأول: مفهوم أمن المعلومات

تعد المعلومات موردا رئيساً من موارد المؤسسة، ومصدراً مهما لنجاحها، وذلك لما لها دور في زيادة كفاءة وفعالية الأنشطة الإدارية المختلفة في المؤسسة، فالمعلومات الدقيقة والمتاحة بسرعة التدفق نحو إدارة المؤسسة سيساعدها في تأدية مهامها ووظائفها العديدة من تخطيط، تنظيم توجيه، اتخاذ القرارات، ورقابة وكذلك تسهل الاستغلال الجيد لها والتحكم في استخداماتها.

لذلك وعلى الرغم من ضرورة توافر المعلومات لأي منظمة، إلا أن ذلك غير كافياً لحل المشكلات التي تواجهها فالمعلومات يجب أن توضع في نظام يسهل عملية الحصول عليها في الوقت الملائم.

وقد جاءت نظم المعلومات للسيطرة على الكم الهائل من المعلومات، تخزينها، معالجتها، ونشرها بما يكفل توافر ما تحتاجه المؤسسة من بيانات ومعلومات ضرورية ودقيقة لمختلف المستويات الإدارية، ومختلف الأنظمة الفرعية، حتى تستطيع المؤسسة أن تحسن من أداءها وأن تزيد من كفاءاتها في اتخاذ القرارات.[36]

تعتبر المعلومات عنصرا أساسياً لأعمال أي منظمة، وبالتالي يجب حمايتها بشكل مستمر والعمل على إدارة مخاطرها بشكل فعال وفق أسس ومعايير حديثة.

-[37]يهتم أمن المعلومات **Information Security** بحماية المعلومات من المخاطر التي تهددها ومن الاعتداء عليها وذلك لتحقيق استمرارية الأعمال وتقليل الخسائر ورفع فرص النجاح والأرباح.

وعَرّفت المنظمة الدولية للقياس والهيئة الدولية للكهروتقنية أمن المعلومات من عدة نواحٍ وفق ما يلي:

-من الناحية الأكاديمية: هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها.

-من الناحية التقنية: هو الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية.

---

[36]حسين، سكفالي، مروة، مقلاتتي، 2020، نظم المعلومات الإدارية وأثرها على الأداء الوظيفي للعاملين، دراسة حالة بنك الفلاحة والتنمية الريفية وكالة قالما، مذكرة لنيل درجة الماجستير في علوم التيسير، إدارة أعمال، جامعة 8 ماي، قالما، ص2.

[37]المنظمة الدولية للقياس والهيئة الدولية للكهروتقنية، 2010، المركز القومي للمعلومات، الإدارة الفنية قسم الجودة والتطوير وحدة المعايير ، لجنة معايير نظم التشغيل والسرية والتأمين معيار قواعد الممارسة لإدارة أمن المعلومات، ISO 27002، ص6

-من الناحية القانونية: هو دراسة طرائق وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها أو استغلال نظمها في ارتكاب الجريمة.

- **المبادئ الأساسية لأمن المعلومات:**[38]

سعت المنظمات لتحقيق أمن نظم المعلومات، وذلك من خلال تحقيق الثالوث التالي:

1-**الموثوقية أو السريّة:** ويقصد بها التأكد من أن المعلومات لا تكشف ولا يطلع عليها، إلاّ من قبل الأشخاص المخوّل لهم بذلك، سواء كانت محفوظة على وسيط مادي أو يتم إرسالها عبر وسائل الاتصالات.

2-الإتاحة أو التوافر: ويقصد به التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل معه وضمان تقديم الخدمات وتوفير المعلومات إلى مستخدميها عند طلبها دون أي تأخير ودون أن يتعرضوا إلى منع استخدامها أو الدخول إليها.

3-التكاملية وسلامة المحتوى: ويقصد بها التأكد من أن محتوى المعلومات متكامل وصحيح ولم يتم تعديله أو تدميره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل بشكل غير شرعي ومقصود أو بشكل عرضي غير مقصود.

كما تم إضافة مبادئ أخرى مثل:

-**عدم الإنكار:** ويقصد به عدم إنكار الشخص الذي قام بتصرف ما متعلق بالمعلومات أو مواقعها (إرسال أو تعديل أو استلام) مسؤوليته أو قيامه بهذا التصرف.

-**التعرف أو التحقق من الهوية الشخصية:** ويقصد به التأكد من هوية الشخص الذي يحاول استخدام المعلومات الموجودة ومعرفة ما إذا كان هو المستخدم المخوّل للتعامل مع تلك المعلومات أم لا.

---

[38]- Janulevicius Justinas, 2016, op, cit, p12.

-Van der Meer Jeroen, 2012, Multi-criteria decision model inference and application in information security risk classification, Master Thesis of Computational Economics, Erasmus School of Economics, Eramus, University Rotterdam, p12 .

- **مكونات أمن المعلومات:** [39]

مع زيادة الاعتماد على البيئة الإلكترونيّة في تخزين ومعالجة ونقل المعلومات أصبح أمن الإنترنت (أمن الأجهزة الإلكترونية والشبكات والاتصالات التي يتم من خلالها تخزين ومعالجة ونقل المعلومات إلكترونياً) مكوناً رئيسياً من مكونات أمن المعلومات بالإضافة إلى مكونات أمن المعلومات التالية:

- الأمن المادي: وهو حماية المصادر والممتلكات والمباني ومنع الوصول غير المشروع إليها.
- أمن الأفراد: وهو حماية الأفراد الذين لهم حق الوصول للمعلومات.
- أمن العمليات: وهو حماية عمليات النظام التي يقوم بها الموظفون المخوّلون.
- خطط استمرارية العمل: ويقصد بها وضع خطط للتغلب على آثار الحوادث الأمنية واستئناف العمل الطبيعي بعد الحادثة.
- أمن البيانات: ويقصد به حماية سرية وسلامة وتوفر البيانات.

- **تهديدات أمن نظم المعلومات:**[40]

توجد كثير من التحديات التي تؤثر على الأداء السليم لوظائف نظم المعلومات منها:

1-التطورات التكنولوجية المتسارعة، المشكلات الفنية المتزايدة، الأحداث البيئيّة المتغيرة الضعف البشري وعدم ملائمة المؤسسات الاجتماعيّة والسياسيّة والاقتصاديّة الراهنة للمتغيرات المتلاحقة...، وتنبع التهديدات والمخاطر التي تواجه نظم المعلومات من الأفعال والتصرفات المقصودة وغير المقصودة على السواء التي قد ترد من مصادر داخلية أو خارجية.

2-العوامل الفنيّة التي تؤدي إلى لفشل نظم المعلومات عديدة ومتنوعة وفي بعض الأحيان قد تكون غير مفهومة.

3-أخطاء النظام من سوء استخدام الأجهزة والبرمجيّات والأخطاء الكامنة إضافة إلى التحميل الزائد أو المشكلات التشغيلية.

[39] Nationnal Institute of Standards and Technology,2016, Internal Report 7621,Revision 1,p2,Idem, p3.

[40] عبيرات، 2022، مرجع سبق ذكره، ص12

4–الفيروسات: غالباً تدخل الفيروسات في النظام من خلال البرمجيّات المصابة، المتطفلين الديدان، أو القنابل المنطقيّة، والتي تمثل بعض الوسائل الفنيّة المستخدمة لتعطيل النظام وتشويهه أو إتلاف أو تحريف بياناته ووظائفه المختلفة.

5–الأحداث البيئيّة الجسيمة: وتشمل على الحرائق، الزلازل، الفيضانات، العواصف الكهربائية الموجات الحرارية المرتفعة، أما أوضاع التجهيزات الطبيعية المعكوسة فقد تظهر من خلال اختراق مقاييس الأمن الطبيعية في حالات انقطاع التيار الكهربائي، سوء استخدام أجهزة التكييف، تسرب المياه، أو الإهمال المباشر في الأماكن المخصصة له، وقد يؤدي التنوع الكبير لمستخدمي نظام المعلومات والمتعاملين معه فيما يتعلق بتوعيتهم وتدريبهم واهتماماتهم المختلفة والمتفرقة في ظهور صعوبات خاصة بأمن المعلومات ونظمها.

إضافةً لاختيار المستخدمين لنظم المعلومات كلمات مرور واضحة يسهل تذكرها والتحقق منها أو الاشتراك بين المستخدمين في رموز التعريف وكلمات المرور، وترك منافذ الرقابة والوصول مفتوحة في مواقع الأمن مما يعرضها للاختراق.

وقد تحدث الأخطاء والاختراقات في تجميع البيانات والمعلومات ومعالجتها وتخزينها وإرسالها وحذفها، كما أن فشل عمل نسخ بديلة ومساندة للملفات والبرمجيات ذات الطبيعة الحرجة يضاعف من آثار الأخطاء والاختراقات ذات الطابع السلبي، وهذا قد يعرض المنظمة لنفقات وخسائر ترتبط بالوقت والجهد والمال الذي ينفق في إعادة إنشائها من جديد، كما أن سوء الاستخدام المقصود للنظام والوصول غير المصرح له وتعمد التخريب والتدمير والاحتيال أو السرقة تعتبر مخاطر وتهديدات خطيرة تؤثر على حياة النظام والمنظمة المالكة له، وهناك جزء أعظم من التهديدات التي تواجه نظم المعلومات من المصادر الخارجية، وعلى النقيض، فإن الأشخاص الذين منحو حق الوصول المعتمد للنظام قد يعرضون تهديدات أعظم تواجه نظم المعلومات أيضاً.

ولذلك فإنه من الضروري[41]إجراء تقييم منهجي لأمن نظام المعلومات بغية التمكن من وضع وتنفيذ ممارسات أمنية فعّالة، من خلال فحص أمن نظم المعلومات للوقوف على فعالية التدابير الأمنية المتخذة، والعمل على اعتماد حلول الحماية المناسبة والحد من المخاطر التي قد تؤثر

[41] https://www.dgssi.gov.ma

على سلامة نظم المعلومات، لذلك فمن الضروري أن تقوم الإدارات والمؤسسات العامة بتحديث نظم معلوماتها من خلال إجراء عمليات افتحاص أمن نظم المعلومات.

المبحث الثاني: ماهية الأمن السيبراني

لقد أصبحت دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي الذي نعيشه في العالم مؤخراً، حيث يشهد العالم المتقدم بكافة أرجائه تطور كبير لا يمكننا بأي حال أن نغفله، ولكن يوجد جانب آخر مظلم لذلك التطور الرقمي الذي نشهده، يمكن أن يجعل كبرى الدول والشركات والمؤسسات التجارية والاقتصادية مهددة بالاختراق، ولعل هذا من أسباب أهمية دراسة الأمن السيبراني، والذي يعمل على حماية البيانات والشبكات والأنظمة الإلكترونية من الهجمات والاختراقات التي قد تودي بها وباستقرارها. [42]

وقد أصبح الأمن السيبراني محور اهتمام متزايد للمنظمات، وسلطت جائحة COVID-19 الضوء على المخاطر السيبرانية لكل نوع من المؤسسات من خلال العمل عن بعد، وتوسيع بيئات العمل باستخدام برامج مؤتمرات الفيديو، وإضافة الأجهزة الشخصية وشبكات الواي فاي إلى أنظمة المؤسسة.

وفي دراسة أجراها مكتب المحاسبة الحكومية (GAO) بعنوان "هناك حاجة إلى إجراءات عاجلة لمعالجة تحديات الأمن السيبراني التي تواجه الأمة" تمت معالجة أربعة تحديات رئيسية للأمن السيبراني من خلال عشرة إجراءات مقترحة لحل المشكلات، وتشمل التحديات؛ وضع استراتيجية للأمن السيبراني، تعزيز الأنظمة الفيدرالية حماية البنية التحتية الحيوية، حماية البيانات الحساسة وضمان خصوصية البيانات.[43]

كذلك سعت بعض الدول النامية إلى اتخاذ إجراءات مماثلة لضمان الأمن السيبراني، وواجهت تلك الدول بعض المشكلات التي تتمثل في عدم وجود مبادرة شاملة للأمن السيبراني، ونقص الدعم الكافي، وعدم وجود مبادرات تعليمية قادرة على مواكبة التطورات الحاصلة في مجال الاتصالات وتكنولوجيا المعلومات، وانعكس هذا الأمر في تراجع مستوى الأمن السيبراني وأصبح مستخدمي الإنترنت لتلك الدول أكثر عرضة لهجمات وجرائم سيرانية.[44]

---

[42] السمحان ، 2020، مرجع سبق ذكره ، ص4

[43] https://governmenttechnolo gyinsider.com by Jackie Davis August 16.2018

[44] Kortjan & Solms,2013,*p.291*

في عام 2013 تعرضت شركة التجزئة الأمريكية العملاقة(Target) لاختراق بيانات، حيث سرقت تفاصيل بطاقات الائتمان والخصم والبيانات الشخصية ل 70 مليون عميل من قواعد بيانات الشركة، وقدرت الأضرار الإجمالية بأكثر من 18 مليار دولار.[45]

في عام 2022، تصدر الأمن السيبراني قائمة المخاطر الحرجة في تقرير الاتحاد الأوربي لمعاهد التدقيق الداخلي(ECIIA)،[46]كما أشار تقرير مشهد التهديدات السيبرانية الصادر عن شركة بوزيتف تكنولوجيز Positiv Technologies، إلى أن الجهات الحكومية في الشرق الأوسط تعتبر من الأهداف الرئيسية لمجرمي الإنترنت حيث إن 22% من إجمالي الهجمات السيبرانية قد استهدفت الدوائر الحكومية، وتشير تقديرات الخبراء إلى أن 78% من الهجمات السيبرانية على الشركات في منطقة الشرق الأوسط تستهدف أجهزة الحاسوب والخوادم ومعدات الشبكات، كما يعمد مجرمو الإنترنت إلى اختراق الأنظمة عن طريق نشر برامج ضارة، أو استغلال نقاط الضعف لسرقة المعلومات السرية أو لتعطيل تشغيل الأجهزة، وتشتهر الهجمات في الشرق الأوسط باستخدام المساحات التي تحذف الملفات الموجودة على الأجهزة المخترقة[47].

وفي أعقاب الاختراق الإلكتروني الذي استهدف مجلس مدينة ليستر، حيث تم الكشف عن وثائق سرية، بما في ذلك بيانات الإيجار بسبب هجوم برامج الفدية من قبل مجموعة INC Ransom أصبح من الواضح أن الهيئات الحكومية هي أهداف رئيسية لمجرمي الإنترنت، إضافةً لهجمات مماثلة على مؤسسات مثل NHS Dumfries و Galloway، مما يشير إلى اتجاه مثير للقلق ويتطلب اهتماماً فورياً[48].

ومن هنا تبرز الحاجة إلى فهم ماهية الأمن السيبراني والتعرف على مخاطره

كلمة السيبرانية مشتقة من الكلمة اللاتينية سايبر (Cyber) ومعناها تخيلي أو افتراضي والسايبر كلمة يجري استخدامها لوصف الفضاء الذي يضم الشبكات العنكبوتية المحوسبة ومنظومات الاتصال والمعلومات، وأنظمة التحكم عن بعد، وتعني: كل ما يتعلق أو يرتبط بالحواسيب

[45] www.imd.orgبقلم ديديبه كوسين وأبراهام هونغزي لو، مايو، 2021

[46] www.isaca.org /resources/isaca-journal/issues/2022/volume-3/

[47] www.ad-dawra.com

[48] www.mah6at.net مخاطر سيبرانية في القطاع العام، مايو، 2024، فيفيك دود،

وتكنولوجيا المعلومات والواقع الافتراضي، ومنها اشتقت صفة السيبرانية والسيبراني Cybernetics.[49]

كلمة سيبراني تعني : الإلكتروني وتطلق على كل ما يخص الشبكات الحاسوبية الإلكترونية وشبكات الإنترنت والتطبيقات الأخرى (فيس بوك–واتس أب) وغيرها من التطبيقات الأخرى وأيضاً الخدمات التي يتم من خلالها تحويل الأموال في الإنترنت وخدمات أون لاين وكثير من الخدمات الأخرى في كل تطبيقات الحياة حول العالم.[50]

تُعرّف السمحان الأمن السيبراني: بأنه اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية وذلك من خلال مجموعة من الوسائل المستخدمة تقنياً وتنظيمياً وإدارياً في منع الوصول غير المشروع للمعلومات الإلكترونيّة ومنع استغلالها بطريقة غير قانونيّة، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصيّة وسريّة من خلال اتباع التدابير والإجراءات اللازمة لحماية البيانات.[51]

وُيعرّف المعهد الوطني للمعايير والتكنولوجيا الأمن السيبراني بأنه: منع الضرر الذي يلحق بأجهزة الكمبيوتر وأنظمة الاتصالات الإلكترونية وخدمات الاتصالات الإلكترونية والاتصالات السلكية وحمايتها وترميمها، بما في ذلك المعلومات الواردة فيها لضمان توفرها وسلامتها والمصادقة والسرية وعدم الإنكار.[52]

ويُعرّف بأنه أمن تكنولوجيا المعلومات أو أمان الكمبيوتر أي حماية المعلومات والمعدات والأجهزة والكمبيوتر وموارد الكمبيوتر وأجهزة الاتصال والمعلومات المخزنة فيه من الوصول غير المصرح به أو الاستخدام أو التعطيل أو التعديل أو الكشف.[53]

وعُرّف بأنه عملية حماية المعلومات من خلال معالجة التهديدات التي تتعرض لها المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات.[54]

---

[49] العزازي، هاني محمد خليل إبراهيم، 2023، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مصر المعاصرة، عدد549، ص469،

[50] https;// www.mah6at.net

[51] السمحان، 2020، مرجع سبق ذكره، ص9

[52] www.imd.org بقلم ديديبه كوسين وأبراهام هونغزي لو، مايو، 2021،

[53] https:// www.sis.gov.eg

[54] أميرهم،2022، مرجع سيق ذكره ، ص337

وفي ضوء ما سبق فإن الأمن السيبراني هو مجموعة من الاستراتيجيات والتقنيات والممارسات التي تهدف إلى حماية الأنظمة الإلكترونية والشبكات وأجهزة الحاسوب والمعلومات من الهجمات السيبرانية، ويشمل ذلك حماية سرية المعلومات وسلامتها وتوافرها، ومنع الوصول غير المصرح به، واكتشاف الاستغلال غير القانوني للمعلومات أو الموارد الرقمية، وضمان استمرارية الأعمال من خلال توفير التدابير الوقائية والإجراءات اللازمة لمواجهة التهديدات السيبرانية المتزايدة.

1-المفاهيم المرتبطة بالأمن السيبراني :

- **الفضاء السيبراني** : يعرف الفضاء السيبراني **(Cyberspace)** أو الفضاء الإلكتروني بأنه عالم الحاسوب الافتراضي، أو الوسيلة الإلكترونية المستخدمة لتسهيل التواصل عبر شبكة الإنترنت، ويشمل الفضاء السيبراني شبكة حاسوب كبيرة مكونة من عدة شبكات حاسوب فرعية منتشرة في جميع أنحاء العالم.[55]

وعرّف الاتحاد الدولي للاتصالات الفضاء السيبراني : المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي أجهزة الكمبيوتر، الشبكات، البرمجيّات، حوسبة المعلومات، المحتوى الإلكتروني، معطيات النقل والتحكم الرقمي.[56]

- **الجريمة السيبرانيّة:** وهي استخدام الكمبيوتر كأداة لتحقيق أهداف غير قانونيّة، مثل ارتكاب الاحتيال، أو سرقة الهويّة أو الملكية الفكريّة، أو انتهاك الخصوصيّة.[57]
- **الهجوم السيبراني:** محاولة متعمدة يقوم بها فرد أو منظمة، بهدف اختراق نظام المعلومات الخاص بفرد أو مؤسَّسة، وغالباً ما يسعى من ينفذ تلك الهجمات إلى الحصول على فائدة جراء الهجوم على الطرف الآخر وتعطيل شبكته.

تحدث الهجمات السيبرانية يومياً ومنها ما يجري اكتشافه ومنها ما يزال غير مكتشف، وغالبا" ما يستهدف المهاجمون الأنظمة الإلكترونيّة الضعيفة، ويطالبون بفدية مقابل إعادتها أو عدم تعطيلها، ما يسفر عن خسارة الشركات والأفراد الضحايا أموالاً طائلة.[58]

---

[55] https:// mawdoo3.com

[56] The International Telecommunication Union , ITU Toolkit for Cybercrime Legislation , Geneva,2010,p12

[57] Michael Aaron Dennis,May, 2024,https://www.britannica.com

[58] قصي أبو شامة، 12 ديسمبر 2021 https:mawdoo3.com

في دراسة (Rolf H Weber:2016) التي هدفت إلى التعرف على التدابير التشريعيّة التي تقوم على حماية أمن المعلومات في بيئة الإنترنت من خلال إنترنت الأشياء، وخلصت الدراسة إلى أن سرعة التغيير والتطور التكنولوجي وتطور أساليب المهاجمين يتطلب ضرورة وجود أساليب جديدة لحماية المعلومات في بيئة الإنترنت إذ أن كل جهاز حاسب آلي متصل بالإنترنت يقع تحت تهديد هذه الجرائم مع وجود ثغرات عديدة تسهل هذه الهجمات، ويتطلب ذلك تعزيز الأمن المعلوماتي في بيئة الإنترنت بشكل عاجل وأيضاً المرونة المبتكرة بما يكفي للتصدي لهذه الهجمات.

2- أنماط الأمن السيبراني:[59]

√ أمن الشبكات: هو ممارسة تأمين شبكة الكمبيوتر من العناصر المتطفلة والانتهازية، سواء المهاجمين المستهدفين، أو البرامج الضارة.

√ أمان التطبيقات: يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات، إذ يمكن أن يوفر التطبيق المخترق الوصول إلى البيانات المصممة للحماية، وإنّ تطبيق مفهوم الأمان الناجح يبدأ في مرحلة التصميم الأولي قبل نشر البرنامج أو الجهاز.

√ أمن المعلومات: يحمي سلامة وخصوصية البيانات، سواء في مرحلة التخزين أو التناقل.

√ الأمن التشغيلي: يشمل العمليات والقرارات التي تتعامل مع أصول البيانات، وتكفل حمايتها.

3- المخاطر التي تهدد الأمن السيبراني :

يشير مفهوم مخاطر الأمن السيبراني إلى التهديدات والهجمات الإلكترونية المسببة لتعطيل أنظمة التكنولوجيا للمؤسسات وخدماتها الإلكترونية، ولا تضر هذه المخاطر بتقنيات وأجهزة المؤسسات فحسب بل أيضاً تكبدها خسائر وتلحق أضراراً بسمعتها.

وبحسب الرابطة الدولية لمشرفي التأمين IAIS فإن المخاطر السيبرانية تعني: أي مخاطر تنشأ عن استخدام البيانات الإلكترونيّة ونقلها بما في ذلك أدوات التكنولوجيا مثل شبكات الاتصالات كما أنها تشمل الأضرار الماديّة والاحتيال المرتكب عن طريق إساءة استخدام البيانات وأي مسؤوليّة تنشأ عن تخزين البيانات وتوفّر المعلومات الإلكترونيّة وسلامتها وسريتها.[60]

---

[59] السمحان، 2020، مرجع سبق ذكره، ص14

[60] IAIS. (2018), "Draft Application Paper on Supervision of Insurer Cybersecurity'",in IAIS (Ed.). IAIS,

ويمكن تقسيم مخاطر الأمن السيبراني لمجموعتين رئيسيتين وهما:[61]

أ – مجموعة مخاطر الأداء المرتبطة بتطبيق أدوات تكنولوجيا المعلومات الحديثة التي تعبر عن فشل تلك الأدوات في القيام بالمهام المخططة لها وتحقيق الاستفادة المرجوة منها.

ب– مجموعة المخاطر الأمنية التي تتضمن ثلاثة مخاطر أساسية وهى:

1– خطر خرقات الحماية المادية المتعلق باختراق المكونات المادية للبنية التحتيّة التي تعتمد عليها الشركة في خدمات تكنولوجيا المعلومات كالبحث في مخلفات البنية التحتيّة للشركة من أقراص مرنة أو أجهزة خاصة بالشبكات الإلكترونيّة والتي قد تتضمن أي معلومات أو كلمات سر يمكن الاعتماد عليها لإتمام عملية الاختراق والتجسس الموجي الذى يشير لاستخدام أجهزة متخصصة لالتقاط كافة المخرجات اللاسلكية من نظام تكنولوجيا المعلومات كالموجات الصوتية.

2–خطر خرق الحماية المتعلقة بالعاملين المرتبط بالمخاطر الداخلية والخارجية والمتعلقة بسلوك العاملين داخل الشركة، مثل قرصنة البرامج الجاهزة، انتهاك التصريح التي تنتج عن ضعف هيكل الرقابة الداخليّة، الهندسة الاجتماعيّة التي تشير لقيام العاملين بالشركة باستغلال علاقاتهم ووظيفتهم للوصول غير المصرح به للمعلومات واختلاس المعلومات.

3- خطر خرق الحماية المتعلقة بالمعلومات والاتصالات الذي يتضمن هجمات البيانات كالنسخ غير المصرح بها من البيانات، هجمات البرامج الجاهزة كالفيروسات والمصائد والأبواب الخلفية والقنوات السرية.

وتذهب دراسة جيهان عادل إبراهيم أن المخاطر السيبرانية تتمثل في ثلاثة محاور وهي : مخاطر سيبرانية تتعلق بالسرية، ومخاطر سيبرانية تتعلق بالنزاهة، ومخاطر سيبرانية تتعلق باستمرارية الأداء، وأن هذه **الأنواع الثلاثة من** المخاطر السيبرانية لها تأثيرات مباشرة ومختلفة على الأهداف حيث يؤدي تعطل الأعمال إلى المنع من العمل مما ينتج عنه خسارة في الإيرادات كما يؤدي الاحتيال إلى خسائر مالية مباشرة في الوقت الذي يستغرق التحقيق في تأثيرات اختراق البيانات وقتاً، الأمر الذي ينتج عنه أضرار معنوية تمس السمعة وفضلاً عن تكاليف التقاضي وبصفة عامة فإن خطر فقدان الثقة في أعقاب الهجمات الإلكترونية، قد يكون عالياً بالنسبة

[61] شحاته، السيد شحاته، 2022، نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية، المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد الثالث عشر، العدد الثاني، ص28

للقطاع المالي بالنظر إلى اعتماد المؤسسات المالية على ثقة عملائها مما يؤثر على قرارات المستثمرين.[62]

4- أنواع الجرائم السيبرانية:[63]

1-الإبتزاز الإلكتروني

2- سرقة الهوية أو انتحال الشخصية: هي نوع من أنواع الغش التي تحصل عندما يستخدم شخص ما معلومات تعريف شخصية تعود لشخص آخر، مثل الاسم، رقم جواز السفر، بطاقة الهوية، بطاقة الائتمان، تفاصيل الحسابات الإلكترونية أو صورته، دون إذنه، بغية ارتكاب أعمال احتيالية، سرقة المال وبطاقات الائتمان، أو مجرد الحاق الضرر والإساءة إلى السمعة كفتح حسابات مصرفية والحصول على قروض والقيام بأعمال غير مشروعة من خلال انتحال هوية الضحية بشكل كامل، أواستخدام حسابات بطاقات الائتمان العائدة للضحية بطرق غير مشروعة للقيام بعمليات شراء أو سحب مبالغ نقدية. ...الخ

3-التصيّد الاحتيالي عبر الإنترنت: هو نوع من تقنيات الخداع على شبكة الإنترنت التي غالباً ما تستخدم لسرقة بيانات المستخدمين الشخصية مثل تفاصيل تسجيل الدخول وكلمات المرور رقم الهاتف، بطاقات الائتمان وهي أن يقوم المجرمون السيبرانيون بإنشاء موقع إلكتروني مزيف يشبه الموقع الأصلي ومن ثم إرسال رابط الموقع المزيف إلى الضحية من خلال البريد إلكتروني على أساس أنها مرسلة من مصدر موثوق مثل الشركة أو البنك أو حتى الموقع الإلكتروني الذي تتعامل معه، ودفعه بأساليب مختلفة للضغط على الرابط المذكور، وفي هذه الحالة يتم توجيهه لإدخال معلومات شخصية هامة عنه، يمكن استخدامها من قبل المقرصن لاحقاً لغرض الاحتيال أو الدخول غير المشروع إلى حسابات الضحية، أو يؤدي ذلك إلى تثبيت برامج خبيثة على أجهزة الضحية، تساعد القراصنة في سرق المعلومات أو في عمليات التخريب.

4-قرصنة الأجهزة والبيانات: وتتضمن اختراق أو محاولة اختراق البيانات الإلكترونيّة الخاصة بالأفراد والمؤسَّسات الحكوميّة أو الخاصّة، بهدف سرقتها أو تخريبها، وقد تحتوي هذه البيانات

---

[62] أميرهم، 2022، مرجع سبق ذكره، ص339

[63] https://isf.gov.ib دليل التوعية حول المخاطر السيبرانية

على معلومات حساسة متعلقة بالمواطنين، العملاء، الموظفين أو بأمور أخرى لا تقل أهمية مثل الملكيّة الفكريّة.

5-برمجيات الفدية الخبيثة وتشفير البيانات: يتسبب هذا النوع من البرمجيات بتشفير البيانات الهامة أو تشفير الجهاز بأكمله بحيث لا يستطيع المستخدم الوصول إلى بياناته، ومن ثم يقوم المقرصن بالطلب من الضحية

مبلغاً مالياً (فدية) عبر العملات الرقمية مثل Bitcoin كونها صعبة التتبع، مقابل فك التشفير عن البيانات وإعادة الأمور لطبيعتها.

6-الاحتيال عبر البريد الإلكتروني الخاص بالعمل: هو نوع من عمليات الاحتيال التي تستهدف الشركات التي تجري عادة تحويلات مالية أو لديها موردين في الخارج، ويعتمد هذا النوع من الجرائم بشكل أساسي على الوصول إلى حسابات البريد الإلكتروني للمديرين التنفيذيين والمسؤولين عن التحويلات المالية في الشركة من خلال استحداث عناوين بريد إلكتروني مشابهة لها أو اختراق العناوين الأصلية بالاعتماد على تقنية التصيّد الاحتيالي أو على الهندسة الاجتماعيّة ومن ثم خداع الموظفين التابعين للشركة من خلال انتحال صفة الرئيس التنفيذي أو أي مسؤول تنفيذي مفوض بإعطاء الإذن لإجراء التحويلات المالية إلى الخارج، من أجل القيام بتحويلات احتيالية معجلة، بما يؤدي إلى خسائر مالية كبير.

5- إدارة مخاطر الأمن السيبراني:[64]

تعرّف إدارة مخاطر الأمن السيبراني بأنها عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونيّة ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسريّة وخصوصيّة البيانات.

وعرّفتها الاستراتيجية الوطنية للأمن السيبراني في العراق بأنها احتمال وجود تهديد وهشاشة الفضاء الإلكتروني للبلد مما يضر بأمن نظم المعلومات وهياكل البنى التحتية المعلوماتية الأساسية من خلال التهديدات السيبرانية والثغرات الموجودة في الفضاءات السحابيّة.

[64] يعقوب، ابتهاج إسماعيل وآخرون، 2022، مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 9، العدد1، ص1407-1408

وقام المعهد الوطني للمعايير والتكنولوجيا (NIST) بإصدار النسخة المحدثة رقم 2.0 من إطار العمل للأمن السيبراني وهو إطار عمل يوفر طريقة للمؤسسات لفهم مخاطر الأمن السيبراني وإدارتها والتخفيف منها بشكل أفضل، ويهدف هذا الإطار إلى مساعدة جميع المؤسسات على إدارة المخاطر، والتخفيف من حدتها ولم يعد يقتصر على المؤسسات العاملة في البنية التحتية الحيوية، والتي كان جمهورها المستهدف الأصلي، ويركز إطار الأمن السيبراني على مجموعة من الوظائف الأساسية: تحديد وحماية، الكشف، الاستجابة، الاسترداد، بالإضافة إلى إدارة الحوكمة التي تشمل صنع القرارات الاستراتيجية المتعلقة بالأمن السيبراني على مستوى المؤسسات.[65]

وتلعب المحاسبة والتدقيق دوراً مهما" في إدارة مخاطر الأمن السيبراني على اعتبار أنها من المخاطر الناشئة وهي الخطر الذي يؤدي إلى خسائر مالية فادحة فضلاً عن مخاطر السمعة والمخاطر التشغيليّة، من خلال بناء إدارة فاعلة لمخاطر الأمن السيبراني (مشابه لنظام الرقابة الداخلية) بإجراء الاختبارات اللازمة لفاعلية عناصر رقابة الأمن السيبراني باختيار نقط مرجعيّة معياريّة (ضوابط التكنولوجيا) داخل المنظمة.

وقد أعطى مجلس الرقابة على شركات المحاسبة العامة ACAOB أولويات مستقبلية لمخاطر الأمن السيبراني حيث تعمل على معالجة مخاطر الأمن السيبراني في عملية التدقيق وأصدر إرشادات لمساعدة المدققين على فهم هذه المخاطر وتخفيضها، حيث أوصى المجلس بأن يقوم المدققون بتقييم مخاطر أنظمة تكنولوجيا المعلومات الخاصة بهم وتنفيذ الضوابط للحماية من التهديدات الإلكترونيّة، وأن يقوم المراجع بإجراء اختبار دوري لأنظمة تكنولوجيا المعلومات الخاصة بهم لضمان فعاليتها.[66]

[65] https://www.barikat.com.tr
[66] https://fastercapital.com

6- متطلبات تحقيق الأمن السيبراني:[67]

1-تحديد إجراءات العمل في الشبكات المعلوماتية: يجب أن تكون واضحة ومحددة فيما هو مسموح أو غير مسموح فيما يتعلق بالأمن المعلوماتي على الشبكة.

2-توفير الآليات اللازمة لتنفيذ سياسات العمل: بحيث يتوفر الوضوح والدقة حول كيفية التنفيذ لهذه السياسات وتحديد العقوبات التي ستوقع في حالة حدوث اختراق.

3-المورد البشري: ضرورة الاهتمام بإسناد إدارة وتشغيل الشبكات المعلوماتية للعناصر البشرية الكفء، والمدربة والمؤهلة للتعامل مع التقنيات والتكنولوجيا الحديثة، وعدم إفساح أي مجال للهواة للعبث بمقدرات الهيئات الحكومية.

4-تحديث الأوضاع الأصلية لمعدات الشبكات: وفيه يتم كل فترة تغيير الأوضاع الأصلية للمعدات المرتبطة بشبكات المعلومات كإجراء احترازي، ما يساعد على منع الاختراق.

5- المراقبة: ضرورة الحرص على توفير المراقبة والمتابعة اللازمة والمستمرة للأنشطة المعلوماتية على الشبكة بالشكل الدقيق.

6-توفير نوع من المراقبة والمتابعة لأنشطة المعلومات على الشبكة بشكل دقيق ودائم، بهدف اكتشاف أي أنشطة مشبوهة أو حركات غير طبيعية ضمن نطاق الشبكة، والعمل على تفادي تفاقم الأوضاع.

7-حسن اختيار مواقع نقاط الشبكة: فلا بد من الدقة عند اختيار نقاط الاتصال بشبكات المعلومات، وأن تكون هذه النقاط في مواقع جيدة ومؤمنة ومحمية من الاختراق.

8- بروتوكولات التحقق والتشفير: ضرورة أن يتم تشفير بروتوكولات التحقق من الهوية وأنظمة تشفير البيانات بهدف تأمين المعلومات على الشبكة، وأن يتم اختيار البرامج المعروفة والمشهورة عالمياً.

9- [68]أمان نقطة النهاية: عادةً ما يمتلك الموظفون أجهزة كمبيوتر محمولة وأجهزة محمولة مملوكة للجهات العامة والتي تعد هدفاً شائعاً للهجمات الإلكترونيّة، يمكن أن تساعد حلول أمان

---

[67]القحطاني، سالم بن سعيد، العنزي، حمودبن محمد، 2011، تبادل المعلومات بين الأجهزة الأمنية في المملكة العربية السعودية: دراسة ميدانية، أطروحة دكتوراه، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، السعودية.

[68]https:// www.checkpoint.com الأمن الإلكتروني/ المحور السيبراني

نقاط النهاية المثبتة على الأجهزة في منع وعلاج إصابات البرامج الضارة والتهديدات السيبرانية الأخرى.

10- إنترنت الأشياء: يتم تشغيل البنية التحتية الحيوية والتحكم فيها عادةً بواسطة إنترنت الأشياء، مما قد يشكل خطراً كبيراً على الأمن السيبراني الحكومي بسبب نقاط الضعف غير المصححة وعوامل أخرى.

يجب إدارة أجهزة إنترنت الأشياء بعناية للتأكد من عدم إصابتها ببرمجيات الروبوتات الضارة أو استخدامها كنقاط وصول لشبكات المنظمات.

7- أهمية الرقابة في تعزيز تدابير الأمن السيبراني:

بيّن تقرير وحدة التفتيش المشتركة لدى دراسة الأمن السيبراني في مؤسسات منظومة الأمم المتحدة لعام 2021 في جنيف بأن هيئات الرقابة الداخلية والخارجية في مؤسسات منظومة الأمم المتحدة كانت مهتمة بمسائل الأمن السيبراني حتى في حال عدم وجود إشارات محددة في تفويضها إلى الموضوع بحد ذاته، وقد صادف المفتشون عدة أمثلة على التحسينات المؤسسيّة التي أُدخلت على إطار الأمن السيبراني في المنظمات المشاركة وهي تحسينات انبثقت عن توصيات الرقابة مثل إنشاء منصب رئيس موظفي أمن المعلومات، والتوصيات الخاصة بالتدريب، ووضع خارطة طريق يمكن تفعيلها، وما إلى ذلك.

وأشارت أن لجان المراجعة والرقابة تناولت مسائل الأمن السيبراني كجزء من تفويضها الذي يغطي الإدارة المركزية للمخاطر وليس في سياق الحوكمة المعنية بتكنولوجيا المعلومات والاتصالات.

وأن هذه اللجان تبنَّت موضوع الأمن السيبراني، ليس لمجرد دعم الإدارة ولكن لاطلاع الهيئات التشريعيّة والإداريّة على مخاطر الأمن السيبراني وتمكينها من المساهمة في التخفيف من المخاطر التي تواجه المنظمات ولتأكيد أنّ جميع هيئات الرقابة تُضيف قيمة قصوى من وجهة نظر الأمن السيبراني، وأشار التقرير أنه من الضرورة أن يسترشد عمل موظفي الرقابة بما لدى خبراء الأمن السيبراني داخل المنظمة من معرفة وخبرة، وأن تصب هذه المعرفة والخبرة في ذلك العمل[69] .

[69] https://www.unjiu.org

وهدفت دراسة أبو موسى بعام 2004(New challenges for Auditing E-Business, external auditors) إلى توضيح التحديات التي تواجه مدقق الحسابات الخارجي في بيئة الأعمال الإلكترونيّة وقدمت إرشاداً للمدققين لكيفية تدقيقها، وتم عرض أهم معايير التدقيق التي ستتأثر بالبيئة الإلكترونيَّة وهي:(معيار التخطيط لعملية التدقيق، معيار جمع وتقييم أدلة الإثبات استقلال المدقق، التدريب الكافي، فحص نظام الرقابة الداخلية) وتوصلت الدراسة إلى أنه يجب على مدقق الحسابات الخارجي أن يتفهم كيف ستؤثر التكنولوجيا الحديثة على عملية التدقيق، وأن على المدقق أن يحصل على المعرفة والمهارات الكافية التي تؤهله للتعامل مع البيئة الإلكترونيّة بالإضافة إلى أن التخطيط لعملية التدقيق أصبح من الأمور الخطيرة التي تتطلب اهتمام كبير من قبل مدققي الحسابات.

ولقد أصبحت مراجعة أنظمة وضوابط وعمليات مراقبة تقنية المعلومات أحد الموضوعات المركزية لعمليات المراجعة التي تجريها الأجهزة العليا للرقابة المالية والمحاسبية (**SAIS**) وهي نتيجة طبيعية للاعتماد على أنظمة تقنية المعلومات لدعم الحكومة ومؤسسات القطاع العام، وهذه الأنظمة المستخدمة يجب أن تحمي بيانات وأصول المنظمة بالإضافة إلى دعم المهام والأهداف المالية والأهداف المحددة الأخرى.

وأدى التقدم التكنولوجي إلى زيادة المخاطر ونقاط الضعف، ونمو أنظمة وشبكات تقنية المعلومات المستندة إلى الويب قد زاد من المخاطر الأمنية التي تواجه المنظمات الحكومية.

أيضا" نتج عن جائحة كوفيد -19 تحديات غير مسبوقة للمنظمات الحكومية التي كانت بحاجة الاستمرار في تنفيذ مهامها مع ضمان قدرة موظفيها على أداء عملهم بأمان وفعالية.

هذه الاتجاهات، جنباً إلى جنب مع التطور المتزايد للمتسللين وغيرهم من ذوي النوايا الخبيثة تزيد من خطر تعرض البيانات الحساسة للاختراق، ويمكن أن تؤدي الحماية غير الفاعلة لأنظمة وشبكات المنظمة إلى إعاقة تقديم الخدمات الحيوية، وعلى هذا النحو، يجب تحديد كل ثغرة جديدة، وتقييم المخاطر من حيث الاحتمالية والتأثير، والتخفيف من حدتها وفقاً لمدى استعداد المنظمة للمخاطر، والسيطرة عليها عند الاقتضاء.[70]

وأصدرت المنظمة الدولية للأجهزة العليا للرقابة (الإنتوساي) توجيهات إرشادية 5100 كإطار شامل لإجراء مراجعة نظم المعلومات ضمن إطار الإنتوساي، ويمكن تطبيق محتويات

[70](دليل مبادرة الانتوساي للتنمية بخصوص تدقيق تقنية المعلومات لمؤسسات التدقيق العليا،2022،ص1-3

التوجيهات الإرشادية المذكورة على مرحل التخطيط والتنفيذ وإعداد التقرير والمتابعة في عملية التدقيق.

وبالتالي يمكن القول بأن الرقابة التي تقوم بها الأجهزة العليا للرقابة المالية على نظم المعلومات يجب أن تلعب دوراً حيوياً في تعزيز الأمن السيبراني.

8- دور المدقق في الرقابة على نظم المعلومات لتعزيز الأمن السيبراني:

عند البدء بعملية التدقيق يجب على المدقق تقييم المخاطر، والذي يعد جزءاً مهماً من تخطيط المراجعة، تشير معايير المراجعة إلى أن المراجع مطالب بفهم مخاطر الأعمال التي قد تؤدي إلى مخاطر الأخطاء أو التحريفات الجوهرية في التقارير المالية، وبالتالي فإن مخاطر الأمن السيبراني هي مجال مخاطر لا يقل أهمية عن مخاطر الأعمال ولا يمكن تجاهلها. [71]

وعلى المدقق والمراجع القيام بفحص لنظام الرقابة الداخلي للمؤسسة من أجل التمكن من تكوين رأي واضح وصحيح حول المؤسسة.[72]

ويتوجب على المدقق ما يلي:[73]

1. تقييم مخاطر وضوابط الأمن السيبراني:

يجب على المدققين تقييم مخاطر وضوابط الأمن السيبراني للمؤسسة كجزء من عملية التدقيق الخاصة بهم؛ ويتضمن ذلك تقييم ممارسات إدارة المخاطر في الجهة الخاضعة للرقابة وسياسات أمن المعلومات، وضوابط تكنولوجيا المعلومات، لتحديد ما إذا كانت كافية للتخفيف من تهديدات الأمن السيبراني وحماية البيانات والأنظمة المالية للمؤسسة.

2. تقييم التأثير على التقارير المالية:

يمكن أن يكون لحوادث الأمن السيبراني تأثير كبير على التقارير المالية للمؤسسة، مما قد يؤدي إلى أخطاء أو عدم دقة في البيانات المالية، ويجب على المدققين النظر في الآثار المالية المحتملة لانتهاكات الأمن السيبراني مثل تكلفة جهود الإصلاح، والغرامات المحتملة، والأضرار

---

[71] (علي، 2023، مرجع سبق ذكره، ص4).

[72] لطفي، 2007، مرجع سبق ذكره، ص411

[73] https://gridlex.com/ the impact of cybersecurity risks on the audit process in accounting

التي تلحق بالسمعة، وتقييم ما إذا كانت هذه الأمور قد تم حسابها بدقة والإفصاح عنها في البيانات المالية للمؤسسة.

3. تحديد الاحتيال والتلاعب:

يمكن لتهديدات الأمن السيبراني أيضاً أن تخلق فرصاً للاحتيال والتلاعب بالبيانات المالية، يجب أن يكون المدققون يقظين عند اكتشاف الأنشطة الاحتيالية أو المخالفات المحتملة الناتجة عن حوادث الأمن السيبراني والتحقيق فيها، وقد يتضمن ذلك تحليل البيانات بحثاً عن أنماط غير عادية، وتعزيز المعلومات بمصادر خارجية، وإجراء مقابلات مع الإدارة والموظفين لجمع الأدلة والأفكار.

4. ضمان الامتثال للوائح:

أدى الانتشار المتزايد لمخاطر الأمن السيبراني إلى إدخال لوائح ومبادئ توجيهية مختلفة، تهدف إلى حماية البيانات الحساسة وضمان سلامة التقارير المالية، يجب على المدققين التأكد من امتثال المؤسسات لهذه اللوائح مثل اللائحة العامة لحماية البيانات،[74]تقييم السياسات والإجراءات المتخذة في الجهات الخاضعة للرقابة من خلال التحقق من وجود سياسات وإجراءات واضحة ومحدثة للأمن السيبراني، متابعة الالتزام بالمعايير والسياسات الأمنية الوطنية والدولية، التحقق من وجود إجراءات لاستعادة البيانات وأنظمة الاسترداد بعد الكوارث.

وتتضمن وظيفة التدقيق في ظل أنظمة المعلومات فحص كافة مكونات النظام والمتمثلة في العاملين الأجهزة، البرامج، قاعدة البيانات، هذه المكونات تتكامل فيما بينها لتحقيق الهدف من التدقيق كما يلي:[75]

أولا"– الرقابة على العاملين وتتناول بالأخص:

1–الإصرار على منح الموظف إجازته السنوية.

2–التحقق من وجود كلمات السّر وبرامج رقابة متخصصة لا تسمح لأي شخص الوصول لأي معلومة.

[74] Hunton, James , et al,2021, Business and Audit RISKS Associated with ERP SYSTEMS: knowledge Differences Between information systems audit specialists and financial auditors,p1-5

[75] عقبة، الرضا، 2008، تدقيق الحسابات في ظل نظم المعلومات المحاسبية، ورقة عمل ضمن الفعاليات العالمية لجمعية المحاسبين القانونيين السوريين ،سوريا، ص2–5

3-[76]تدقيق الضوابط اليدويّة مثل: فصل الواجبات بين مستخدمي النظام، ومنظمي جدولة الإنتاج والمبرمجين، ومشغّلي إدخال البيانات، ومديريّ الشبكات، وما شابه ذلك.

4-التأكد من تناوب المهام بين موظفي العمليات.

5-التحقق من وجود برامج للتدريب والتوعية بالأمن السيبراني للعاملين، وضمان فهم العاملين لأدوارهم ومسؤولياتهم في حماية المعلومات.

ثانيا"- الرقابة على الأجهزة وتضم ما يلي:

1-اختيار موقع آمن للأجهزة.

2-تحديد قائمة الموظفين المسموح لهم باستعمال الحاسوب.

3-الاحتفاظ بنسخ احتياطية للملفات والسجلات الهامة في مكان آمن.

4-التأمين على الأجهزة.

5-التركيز على الضوابط الموجودة لحماية الأصول وضمان سلامة البيانات، فعلى سبيل المثال من شأن الوقاية الكافية من الحرائق، واكتشاف المياه وضوابط الأمن المادي، أن تحمي أصول الحوسبة باهظة الثمن[77].

ثالثاً- الرقابة على البرمجيات من خلال:

1-التحقق من إجراءات اعتماد البرنامج.

2-إجراء مراجعة فجائية للبرنامج أثناء التشغيل وعدم الاعتماد على تقييم المخرجات فقط.

3-التأكد من أنّ مخرجات البرنامج تتماشى مع الهدف الذي صمم لأجله.

4-مراجعة التقارير المتضمنة مقاييس أداء النظام.

5-مراجعة البنية التحتية للجهة الخاضعة للرقابة للتأكد من تطبيق إجراءات الحماية اللازمة مثل(الجدران النارية، أنظمة كشف التسلّل، برامج مكافحة الفيروسات).[78]

6-تدقيق الضوابط التي تراقب تسجيل رسائل خطأ النظام وإعادة تشغيل البرامج الملغاة(المنتهية بشكل غير طبيعي) من شأنها أن تساهم في الحفاظ على سلامة البيانات.

رابعاً-الرقابة على قاعدة البيانات :

[76] Hunton, James , et al,2021,p1-5 مرجع سبق ذكره

[77] Hunton, James , et al,2021,p1-5 مرجع سبق ذكره

[78] Hunton, James , et al,2021,p1-5 مرجع سبق ذكره

على المدقق تدقيق قاعدة البيانات كونها تحتوي على البيانات الأساسية والسريّة للمؤسسة، لذلك يجب حمايتها من سوء الاستخدام خاصةً وأن تكلفة إعادة تصميم قاعدة بيانات أخرى مكلف جداً.

ويتوجب إجراء تحليل شامل للمخاطر لتحديد الثغرات ونقاط الضعف في نظم المعلومات، وتقييم تأثير المخاطر والتأكد من وضع خطط للاستجابة لها.

وعند انتهاء عملية التدقيق يتوجب إعداد تقرير يتضمن نتائج التدقيق وتقديم توصيات للتحسين ومتابعة تنفيذ التوصيات وتقييم تأثيرها على تقليل المخاطر، مما يسهم في بناء بنية تحتية قوية ومستدامة في القطاع الحكومي.

9- تكييف عملية التدقيق لمعالجة مخاطر الأمن السيبراني:[79]

1. تطوير خُبرات الأمن السيبراني:

يجب على المدققين تطوير الخبرة في إدارة مخاطر الأمن السيبراني وضوابطها، لتقييم مدى تعرض المؤسسة لتهديدات الأمن السيبراني بشكل فعّال، وقد يشمل ذلك الحصول على شهادات متخصصة، مثل مدقق نظم المعلومات المعتمد، وحضور الدورات التدريبية، والبقاء على إطلاع على الاتجاهات الناشئة وأفضل الممارسات في مجال الأمن السيبراني.

2. الاستفادة من التكنولوجيا وتحليلات البيانات:

يمكن للمدققين الاستفادة من أدوات التكنولوجيا وتحليل البيانات لتعزيز قدرتهم على تحديد وتقييم مخاطر الأمن السيبراني.

3. التعاون مع المتخصصين في تكنولوجيا المعلومات والأمن السيبراني:

نظراً لتعقيد مخاطر الأمن السيبراني، قد يحتاج المدققون إلى التعاون مع متخصصّي تكنولوجيا المعلومات والأمن السيبراني للحصول على الخبرة والرؤى اللازمة لتقييم ضوابط الأمن السيبراني وممارسات إدارة المخاطر في المؤسسة، قد يتضمن ذلك إشراك خبراء خارجيين لمواجهة التحديات التي تفرضها تهديدات الأمن السيبراني.

4. اعتماد منهج التدقيق المبني على المخاطر:

[79] https://gridlex.com/ the impact of cybersecurity risks on the audit process in accounting

يمكن أن يساعد نهج التدقيق القائم على المخاطر المدققين على تحديد أولويات جهودهم ومواردهم في المجالات الأكثر تعرضاً لمخاطر الأمن السيبراني، يتضمن ذلك تحديد وتقييم الأنظمة والعمليات الأكثر أهمية في المؤسسة وتحديد احتمالية وتأثير حوادث الأمن السيبراني المحتملة، وتصميم إجراءات التدقيق لمعالجة هذه المخاطر، والاستفادة من التكنولوجيا وتحليلات البيانات، والتعاون مع المتخصصين في سبيل ذلك.

الفصل الثالث الدراسة الميدانية

أولا": أساليب جمع البيانات :

لتحقيق أهداف البحث وإثبات فرضياته اعتمدت الباحثة على مصدرين أساسيين في جمع البيانات:

1- **المصادر الأولية:**

قامت الباحثة بجمع البيانات الأولية من خلال الاعتماد على الاستبانة كأداة أساسية للبحث وقد صممت خصيصاً لهذا الغرض من خلال دراسات سابقة، حيث تم دراسة المتغيرات محل البحث وذلك لمعالجة الجوانب التحليلية للبحث.

2- **المصادر الثانوية:** اتجهت الباحثة في معالجة الإطار النظري للبحث إلى مصادر البيانات الثانوية والتي تتمثل بالكتب والأبحاث والمجلات والرسائل والمنشورات في المواقع الإلكترونية ذات العلاقة بموضوع البحث.

ثانيا": مجتمع و عينة البحث :

1- مجتمع البحث:

يتكون مجتمع البحث من المفتشين في الجهاز المركزي للرقابة المالية في سورية، والبالغ عددهم حوالي(950) مفتشاً ومفتشة، وتم اختيار عينة من مجتمع البحث تم تمثيلها من مفتشي الجهاز المركزي للرقابة المالية – فرع حلب، وذلك لسرعة الإنجاز والحصول على المعلومات، ولسهولة التواصل.

2- عينة البحث:

تم أخذ فرع الجهاز المركزي للرقابة المالية في مدينة حلب وتم توزيع الاستبانة على مفتشي فرع حلب البالغ عددهم(77) مفتشاً ومفتشة، واعتمدت الباحثة على أسلوب العينة العشوائية الميسرة في اختيار عينة البحث، حيث تم استرداد(69) استبانة، والصالح منها للتحليل فقد بلغ(65) استبانة.

ثالثا" : أداة البحث :

تم تصميم استبانة لتحقيق الأهداف المرجوة من هذا البحث بالاعتماد على الدراسات السابقة والدراسات المماثلة والأساس النظري في هذا البحث، حيث وجهت لمفتشي فرع الجهاز المركزي في مدينة حلب، وقسمت الاستبانة إلى المحاور التالية:

- محور الخصائص الديموغرافية أو ما يعرف أيضاً بمحور البيانات الشخصية لعينة البحث، حيث تضمن هذا المحور على المتغيرات التالية: (الجنس، العمر، المسمى الوظيفي، المؤهل العلمي، سنوات الخبرة الوظيفية).
- محور تقييم نظام الرقابة الداخلية والضبط الداخلي، ويتكون من/15/ عبارة أو سؤال.
- محور الممارسات الرقابية للجهاز المركزي للرقابة المالية، ويتكون من /**13**/ عبارة أو سؤال.

وبذلك فإن العدد الإجمالي لعبارات الاستبانة /**28**/ عبارة أو سؤال، حيث كانت الإجابات تتبع مقياس ليكرت الخماسي كما هو موضح بالجدول التالي:

جدول رقم(1) مقياس ليكرت الخماسي

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

رابعاً: ثبات أداة البحث(الموثوقية):

تم إجراء اختبار الثبات(**Reliability**) على عينة البحث باستخدام معامل **Alpha Cronbach** ويقصد بثبات أداة القياس "الاتساق الداخلي بين عباراتها، ولثبات الأداة جانبان الأول هو استقرار المقياس كأن يتم الحصول على نفس النتائج إذا قيس المتغير عدة مرات متتالية، أما الجانب الآخر للثبات فهو الموضوعية أي أن يتم الحصول على نفس الدرجة بغض النظر عن الشخص الذي يعمل على تطبيق الاختبار أو الشخص الذي قام بتصميمه. إن قيمة معامل الارتباط **Alpha Cronbach** تتراوح بين (0−1) وحتى يتمتع المقياس بالثبات يجب ألا يقل الحد الأدنى لقيمة المعامل عن(0,70)"[80]، يوضح الجدول رقم(2) نتائج التحليل لمعامل**Alpha Cronbach** لكل محور(قسم) من محاور الاستمارة.

[80]- درة، عمر، **أثر إدارة العدالة التنظيمية على إدارة ضغوط العمل**(2007)، رسالة ماجستير في إدارة الأعمال، جامعة عين شمس، كلية التجارة، عين شمس، ص 91.

جدول (2) معامل Alpha Cronbach لمحاور الاستبانة

م	نص المحور	عدد الفقرات	قيمة معامل كرونباخ	تقييم الثبات	الترتيب
1	تقييم نظام الرقابة الداخلية والضبط الداخلي	15	0.702	متوسط	2
2	الممارسات الرقابية للجهاز المركزي للرقابة المالية	13	0.795	متوسط	1
--	جميع المحاور	28	0.812	عال	--

نلاحظ من الجدول رقم(2) أن قيمة معامل **Alpha Cronbach** لمحوري الاستبانة تتراوح بين**(0.702)** عند المحور المتعلق بتقييم نظام الرقابة الداخلية والضبط الداخلي، و**(0.795)** عند المحور المتعلق بالممارسات الرقابية للجهاز المركزي للرقابة المالية، أي أن قيم المعامل لمحوري الاستبانة أكبر من(0.70) مما يدل على أن أداة البحث تتسم بالاتساق الداخلي بين عباراتها، كما أن قيمة المعامل الكلي لعبارات الاستبانة قد بلغ**(0.812)** وهذه القيمة تعتبر عالية، والأمر الذي يدل على درجة ثبات جيدة تتمتع بها الاستبانة، وبالتالي فهي صالحة لقياس ما أُعدت له.

الإطار الميداني والمعالجة الإحصائية:

قامت الباحثة بتفريغ وتحليل الاستبانة من خلال البرنامج الإحصائي **SPSS18**، وتم إجراء الاختبارات الإحصائية المناسبة التي تخدم أهداف البحث وتثبت صحة فروضه أو تنفيها، حيث تم تطبيق الاستبانة كما أشرنا أعلاه على عينة مكونة من/65/ مفردة تمثل المجتمع المدروس والبالغ عددهم حوالي/950/ مفردة، أي أن حجم العينة يشكل ما نسبته /6.7%/ من حجم المجتمع.

إن الجدول التالي يوضح توزع أفراد العينة حسب البيانات الشخصية الخاصة بهم.

جدول رقم(3) توزع أفراد عينة البحث وفقاً لمتغيرات الجنس والمسمى الوظيفي والمؤهل العلمي

الجنس	العدد	النسبة %	المسمى الوظيفي	العدد	النسبة%	المؤهل العلمي	العدد	النسبة%
ذكور	44	67.7	مفتش معاون	6	9.2	إجازة	6	9.2
إناث	21	32.3	مفتش	26	40.0	دراسات	26	40.0
---	---	---	مفتش أول	33	50.8	ماجستير	33	50.8
المجموع	65	100	المجموع	65	100	المجموع	65	100

الجدول من إعداد الباحثة بالاعتماد على مخرجات البرنامج الاحصائي SPSS

جدول رقم(4) توزع أفراد عينة البحث وفقاً لمتغيري العمر وسنوات الخبرة

العمر	العدد	النسبة%	سنوات الخبرة	العدد	النسبة%
30-21	**0**	**0**	**أقل من سنة**	**2**	**3.1**
40-31	**25**	**38.5**	**من 1-5**	**5**	**7.7**
50-41	**22**	**33.8**	**من 6-10**	**18**	**27.7**
أكبر من 50	**18**	**27.7**	**من 11-15**	**9**	**13.8**
---	---	---	**أكثر من 15**	**31**	**47.7**
المجموع	**65**	**100**	المجموع	**65**	**100**

الجدول من إعداد الباحثة بالاعتماد على مخرجات البرنامج الإحصائي SPSS

- نتائج اختبار الفرضية الخاصة بالمتغيرات الديموغرافية التي تنص على أنه: لا توجد فروق ذات دلالة إحصائية بين إجابات عينة البحث حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي، وذلك تبعاً للخصائص الديموغرافية للعينة، حيث تم إجراء تحليل التباين الأحادي(**One Way ANOVA**) لمعرفة فيما إذا كان هناك فروق جوهرية ذات دلالة إحصائية بين إجابات عينة البحث حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي، وذلك تبعاً للخصائص التالية لعينة البحث:

1- حسب الجنس:

يبين الجدول رقم(**5**) التالي نتائج تحليل التباين الأحادي(**One Way ANOVA**) لإجابات أفراد عينة البحث حسب متغير الجنس لكل منهم.

الجدول رقم (5): نتائج تحليل التباين الأحادي (One Way ANOVA)

	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	المعنوية Sig.	الدلالة الإحصائية
بين المجموعات	**0.181**	**1**	**0.181**	**1.272**	**0.264**	**غير معنوي**
داخل المجموعات	**8.964**	**63**	**0.142**			
الإجمالي	**9.145**	**64**				

الجدول من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي للاستبيان.

من الجدول السابق نلاحظ أن قيمة المعنوية.**Sig** تساوي(**0.264**) وهي أكبر من مستوى المعنوية المفروض(**5%**)، الأمر الذي يشير إلى عدم وجود فروق جوهرية ذات دلالة إحصائية في إجابات أفراد عينة البحث حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي وفقاً لمتغير الجنس.

2- حسب المسمى الوظيفي:

يبين الجدول رقم(6) التالي نتائج تحليل التباين الأحادي(One Way ANOVA) لإجابات أفراد عينة البحث حسب المسمى الوظيفي لكل منهم.

الجدول رقم (6): نتائج تحليل التباين الأحادي (One Way ANOVA)

	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	المعنوية Sig.	الدلالة الإحصائية
بين المجموعات	0.61	2	0.31	2.23	0.12	غ/ معنوي
داخل المجموعات	8.53	62	0.14			
الإجمالي	9.15	64				

الجدول من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي للاستبيان.

من الجدول السابق نلاحظ أن قيمة المعنوية.**Sig** تساوي(**0.12**) وهي أكبر من مستوى المعنوية المفروض (**5%**)، الأمر الذي يشير إلى عدم وجود فروق جوهرية ذات دلالة إحصائية في إجابات أفراد عينة البحث حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي وفقاً لمتغير المسمى الوظيفي.

3- حسب العمر:

يبين الجدول رقم(7) التالي نتائج تحليل التباين الأحادي(One Way ANOVA) لإجابات أفراد عينة البحث حسب متغير العمر لكل منهم.

الجدول رقم (7): نتائج تحليل التباين الأحادي (One Way ANOVA)

	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	المعنوية Sig.	الدلالة الإحصائية
بين المجموعات	0.16	2	0.08	0.55	0.579	غ/ معنوي
داخل المجموعات	8.99	62	0.15			
الإجمالي	9.15	64				

الجدول من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي للاستبيان.

من الجدول السابق نلاحظ أن قيمة المعنوية.**Sig** تساوي(0.579) وهي أكبر من مستوى المعنوية المفروض(**5%**)، الأمر الذي يشير إلى عدم وجود فروق جوهرية ذات دلالة إحصائية في إجابات أفراد عينة البحث حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي وفقاً لمتغير العمر.

4- حسب المؤهل العلمي:

يبين الجدول رقم(8) التالي نتائج تحليل التباين الأحادي(One Way ANOVA) لإجابات أفراد عينة البحث حسب متغير المؤهل العلمي لكل منهم.

الجدول رقم (8): نتائج تحليل التباين الأحادي (One Way ANOVA)

	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	المعنوية Sig.	الدلالة الإحصائية
بين المجموعات	0.05	2	0.03	0.18	0.836	غ/ معنوي
داخل المجموعات	9.09	62	0.15			
الإجمالي	9.15	64				

الجدول من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي للاستبيان.

من الجدول السابق نلاحظ أن قيمة المعنوية.**Sig** تساوي**(0.836)** وهي أكبر من مستوى المعنوية المفروض**(5%)**، الأمر الذي يشير إلى عدم وجود فروق جوهرية ذات دلالة إحصائية في إجابات أفراد عينة البحث حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي وفقاً لمتغير المؤهل العلمي.

5- حسب سنوات الخبرة:

يبين الجدول رقم**(9)** التالي نتائج تحليل التباين الأحادي**(One Way ANOVA)** لإجابات أفراد عينة البحث حسب سنوات الخبرة لكل منهم.

الجدول رقم(9): نتائج تحليل التباين الأحادي (One Way ANOVA)

	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة F	المعنوية Sig.	الدلالة الإحصائية
بين المجموعات	0.48	4	0.12	0.83	0.514	غ/ معنوي
داخل المجموعات	8.67	60	0.14			
الإجمالي	9.15	64				

الجدول من إعداد الباحثة بالاعتماد على نتائج التحليل الإحصائي للاستبيان.

من الجدول السابق نلاحظ أن قيمة المعنوية.**Sig** تساوي**(0.514)** وهي أكبر من مستوى المعنوية المفروض**(5%)**، الأمر الذي يشير إلى عدم وجود فروق جوهرية ذات دلالة إحصائية في إجابات أفراد عينة البحث حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي وفقاً لمتغير سنوات الخبرة.

من خلال النتائج السابقة يتضح لنا عدم وجود فروق جوهرية ذات دلالة إحصائية بين إجابات عينة البحث فيما يتعلق بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي(تقييم نظام الرقابة الداخلية والضبط الداخلي، الممارسات الرقابية للجهاز المركزي للرقابة المالية)، وفقاً لخصائص العينة جميعها، وبناءً عليه فإننا نقبل فرضية العدم القائلة: بعدم وجود فروق جوهرية ذات دلالة إحصائية في إجابات أفراد عينة البحث حول الأسئلة المتعلقة بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع

الحكومي، مقابل رفض الفرضية البديلة القائلة بوجود فروق جوهرية ذات دلالة إحصائية بين إجابات عينة البحث فيما يتعلق بدور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي وفقاً لخصائص عينة البحث.

- نتائج اختبار الفرضية الخاصة بمتغيرات البحث الأصلية والتي تنص على أنه: لا يوجد دور دال إحصائياً للرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي، ويتفرع عن هذه الفرضية الفرضيتان الفرعيتان التاليتان:

1) لا يوجد دور دال إحصائياً لنظام الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي استناداً إلى مراجعة بنية وهيكلية الرقابة الداخلية وتقييم الضبط الداخلي من قبل الجهاز المركزي للرقابة المالية حيث جاءت النتائج كما هو موضح في الجدول التالي:

جدول رقم (10) استجابة أفراد عينة البحث حول تقييم نظام الرقابة الداخلية والضبط الداخلي

م	العبارة	درجة التحقق										المتوسط الحسابي	الأهمية النسبية	مستوى الموافقة
		موافق بشدة		موافق		محايد		غير موافق		غير موافق بشدة				
		ك	%	ك	%	ك	%	ك	%	ك	%			
1	توفر ضوابط الوصول للبيانات والمعلومات للحد من مخاطر الاختراق وسوء الاستخدام وإتلاف المعلومات الحساسة.	2	3.1	20	30.8	20	30.8	20	38.8	3	4.6	2.97	10	محايد
2	الاحتفاظ بنسخ احتياطية للملفات والسجلات الهامة في مكان آمن بشكل دوري	29	44.6	9	13.8	17	26.2	8	12.3	2	3.1	3.85	6	موافق
3	الضوابط الداخلية لتقنية المعلومات المتعلقة بسرية البيانات وسلامتها وصلاحيتها وتوافرها قد تم تبنيها من قبل	3	4.6	9	13.8	29	44.6	20	30.8	4	6.2	2.80	11	محايد
4	تطبيق إجراءات الأمان الأساسية مثل وجود كلمات سر قوية تتضمن أرقام وأحرف كبيرة وصغيرة ورموز غير قابلة للتنبؤ وتغييرها بانتظام	19	29.2	34	52.3	10	15.4	1	1.5	1	1.5	4.06	4	موافق
5	عدم مشاركة كلمات السر مع الآخرين.	54	83.1	6	9.2	5	7.7	--	--	--	--	4.75	1	موافق بشدة
6	الفصل بين الوظائف المتعارضة لمستخدمي النظام مثل فصل مهام المحاسبة عن مهام أمين الصندوق	3	4.6	5	7.7	7	10.8	5	7.7	--	--	4.60	2	موافق بشدة
7	وجود قائمة بأسماء الموظفين المخول لهم استعمال المنظومة	43	66.2	14	21.5	5	7.7	2	3.1	1	1.5	4.48	3	موافق بشدة

8	الإدارة المعنية بالأمن السيبراني في حال وجودها مستقلة عن الإدارة المعنية بتقنية المعلومات	1	1.5	7	10.8	9	13.8	39	60	9	13.8	14	2.26	غير موافق
9	تحديث الأجهزة القديمة وإصدارات البرامج غير المدعومة لما تسببه من مخاطر كبيرة على بيانات المؤسسة وعملياتها.	8	12.3	12	18.5	33	50.8	7	10.8	5	7.7	9	3.17	محايد
10	وجود كاميرات للمراقبة لكشف أي متسلل وصيانتها دورياً.	5	7.7	40	61.5	14	21.5	5	7.7	1	1.5	7	3.66	موافق
11	اختيار موقع آمن للأجهزة	12	18.5	9	13.8	38	58.5	4	6.2	2	3.1	8	3.38	محايد
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة للدخول على الشبكة مثل مقاوم الفيروسات.	11	16.9	43	66.2	8	12.3	--	--	3	4.6	5	3.91	موافق
13	تحديث برامج مكافحة الفيروسات بشكل دوري.	6	9.2	4	6.2	33	50.8	15	23.1	7	10.8	11	2.80	محايد
14	وضع ضوابط من أجل سرية البيانات وتشفيرها وعدم إمكانية الاطلاع عليها إلا من قبل الأشخاص المخول لهم ذلك.	3	4.6	8	12.3	29	44.6	19	29.2	6	9.2	12	2.74	محايد
15	نقل البيانات من موقع لآخر يتم عبر قنوات نقل آمنة غير قابلة للاختراق.	5	7.7	8	12.3	22	33.8	23	35.4	7	10.8	13	2.71	محايد
تقييم نظام الرقابة الداخلية والضبط الداخلي													3.476	موافق/ دال

يتضح من الجدول رقم(**10**) أعلاه إلى أن مستوى الموافقة جيد حيث بلغت قيمة المتوسط الحسابي الكلي ولجميع عبارات هذا المحور/3.48/ الأمر الذي يشير إلى إمكانية تحقيق الأمن السبيراني من خلال تقييم نظام الرقابة الداخلية والضبط الداخلي من قبل الجهاز المركزي للرقابة المالية، إذ أن معظم الإجابات تتجه نحو موافقة أفراد عينة البحث على عبارات المحور، والذي من شأنه المساعدة على تحقيق الأمن السيبراني في الجهات العامة الخاضعة للرقابة، وتشير بيانات الجدول السابق إلى أهم العبارات التي حازت على الترتيب الأعلى من بين عبارات المحور وهي على الترتيب:

1- عدم مشاركة كلمات السر مع الآخرين(العبارة رقم /5/)، بمتوسط موافقة قدره(**4.75**).

2- الفصل بين الوظائف المتعارضة لمستخدمي النظام مثل فصل مهام المحاسبة عن مهام أمين الصندوق(العبارة رقم /6/)، بمتوسط موافقة قدره(**4.60**).

3- وجود قائمة بأسماء الموظفين المخول لهم استعمال المنظومة، (العبارة رقم /7/)، بمتوسط موافقة قدره(**4.48**).

4- تطبيق إجراءات الأمان الأساسية مثل وجود كلمات سر قوية تتضمن أرقام وأحرف كبيرة وصغيرة ورموز غير قابلة للتنبؤ وتغييرها بانتظام(العبارة رقم /4/)، بمتوسط موافقة قدره(**4.06**)

5- استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة للدخول على الشبكة مثل مقاوم الفيروسات(العبارة رقم/12/)، بمتوسط موافقة قدره(**3.91**).

6- الاحتفاظ بنسخ احتياطية للملفات والسجلات الهامة في مكان آمن بشكل دوري (العبارة رقم/2/)، بمتوسط موافقة قدره(**3.85**).

7- وجود كاميرات للمراقبة لكشف أي متسلل، وصيانتها دورياً(العبارة رقم/10/)، بمتوسط موافقة قدره(**3.66**).

إن مستوى الموافقة للعبارات السابقة يتراوح بين موافق وموافق بشدة، الأمر الذي يشير إلى وجود دور دال إحصائياً للرقابة في بيئة نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي، ومنه فإننا نرفض فرضية العدم القائلة: بعدم وجود دور دال إحصائياً لنظام الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي استناداً إلى مراجعة بنية وهيكلية الرقابة الداخلية وتقييم الضبط الداخلي من قبل الجهاز المركزي للرقابة المالية، مقابل قبول الفرضية البديلة.

-تشير نتائج التحليل أن أفراد عينة البحث يرون أن الأنظمة الداخلية والضبط الداخلي في الجهات الخاضعة للرقابة كافية بحد ذاتها، إذا ما تم تفعيلها بالشكل المناسب لتحقيق مستوى مقبول من الأمن السيبراني، قد يعكس هذا الاعتقاد بأن المشكلة ليست في الأنظمة بحد ذاتها، وإنما في تطبيقها ومراقبتها.

2) - لا يوجد دور دال إحصائياً للرقابة التي يمارسها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي، حيث جاءت النتائج كما هو موضح في الجدول التالي:

جدول رقم(11) استجابة أفراد عينة البحث حول الممارسات الرقابية للجهاز المركزي للرقابة المالية

م	العبارة	درجة التحقق										المتوسط الحسابي	الأهمية النسبية	مستوى الموافقة
		موافق بشدة		موافق		محايد		غير موافق		غير موافق بشدة				
		ك	%	ك	%	ك	%	ك	%	ك	%			
1	التأكد من مقدرة الأنظمة المعلوماتية على توفير أدلة الإثبات الملائمة لعملية الرقابة	2	3.1	9	13.8	27	41.5	21	32.3	6	9.2	2.69	8	محايد
2	تقييم ومتابعة مدى التزام الهيئة الخاضعة للرقابة بتوفير إجراءات الملائمة والمتعلقة بأمن البيانات وحفظها من التلف أو التحريف والإجراءات المتبعة لسلامة نظام المعلومات.	6	9.2	14	21.5	21	32.3	22	33.8	2	3.1	3.00	5	محايد
3	التأكد من الاستعمال الفعال لبرامج الحماية (جدران النار) وبرامج الحماية من الفيروسات لحماية النظم من إدخال البرامج الضارة أو غير المخولة.	0	0	5	7.7	5	7.7	45	69.2	10	15.4	2.08	13	غير موافق
4	التأكد من الاستعمال الفعال للتشفير ويشمل ذلك الاحتفاظ بالسرية والأمن أثناء إرسال البيانات والمعلومات عبر الشبكة ومنع سوء الاستعمال من خلال تقنية التشفير.	2	3.1	3	4.6	21	32.3	17	26.2	22	33.8	2.17	12	غير موافق
5	الرقابة على التزام الجهات الخاضعة للرقابة في معالجة البيانات وفق القوانين والأنظمة المعمول بها والالتزام بالتشريعات الخاصة بالأمن السيبراني.	3	4.6	12	18.5	28	43.1	12	18.5	10	15.4	2.78	6	محايد
6	التأكد من القدرة على استعادة وثائق العمليات من ملفات الوثائق الإلكترونية مثل الوثائق المخزنة عبر الإنترنيت أو في الأنظمة الإلكترونية.	1	1.5	9	13.8	32	49.2	8	12.3	15	23.1	2.58	9	غير موافق
7	إعطاء المفتش صلاحية الاطلاع على جميع المعلومات في قاعدة البيانات والقيام بتدقيقها للتأكد من سلامة المخرجات وعدم الازدواج أو التكرار عن طريق أخذ عينة وحسابها يدويا للحصول على نتيجة واحدة.	0	0	3	4.6	50	76.9	6	9.2	6	9.2	2.77	7	محايد
8	التأكد من صلاحية أجهزة الحماية وتعبئتها بشكل دوري مثل أجهزة الحماية من الحريق.	7	10.8	47	72.3	8	12.3	3	4.6	0	0	3.89	1	موافق
9	التأكد من قيام الجهة الخاضعة للرقابة بإجراء جرد شامل لكافة معدات نظم المعلومات.	6	9.2	36	55.4	20	30.8	3	4.6	0	0	3.69	2	موافق

10	التأكد من وجود أنظمة وإجراءات لمعالجة الأخطاء والانحرافات المكتشفة.	13	20	4	6.2	14	21.5	29	44.6	5	7.7	3.14	4	محايد
11	التأكد من وجود خطط استمرارية الأعمال وإجراءات التعافي من الكوارث ومدى فعاليتها.	2	3.1	0	0	21	32.3	30	46.2	12	18.5	2.23	11	غير موافق
12	التأكد من وجود مصادقة للعمليات الهامة من قبل موظفين اثنين أو أكثر حسب الصلاحيات.	10	15.4	26	40	15	23.1	7	10.8	7	10.8	3.38	3	محايد
13	التأكد من أن مخرجات البرنامج تتماشى مع الهدف الذي صمم من أجله.	0	0	1	1.5	19	29.2	44	1.5	67.7	1.5	2.31	10	غير موافق
الممارسات الرقابية للجهاز المركزي للرقابة المالية												2.82	محايد/غير موافق	

يتضح من الجدول رقم(**11**) إلى أن مستوى الموافقة متدني جداً حيث بلغت قيمة المتوسط الحسابي الكلي ولجميع عبارات هذا المحور/**2.82**/ محايد وأقرب إلى عدم الموافقة، الأمر الذي يشير إلى عدم إمكانية تحقيق الأمن السيبراني في الجهات العامة من خلال الممارسات الرقابية التي يقوم بها الجهاز المركزي للرقابة المالية، إذ أن غالبية أفراد عينة البحث تتجه نحو الحياد وعدم الموافقة على الممارسات الرقابية التي يقوم بها الجهاز المركزي للرقابة المالية.

يمكن تفسير النتائج التي تشير إلى الحياد أو عدم الموافقة، قد يكون أفراد عينة البحث غير مطلعين بشكل كامل على السياسات والإجراءات المتعلقة بالأمن السيبراني، أو عدم وضوح السياسات والإجراءات الواجب اتباعها، أو عدم معرفة أفراد عينة البحث لمسؤوليتهم أو دورهم في تطبيق ومراقبة ممارسات الأمن السيبراني في الجهات الخاضعة للرقابة، أو عدم المعرفة الكافية أو الوعي بأهمية الأمن السيبراني والإجراءات المطلوبة لتحقيقه.

بالنظر إلى الجدول رقم(**11**) نجد أن عبارتين فقط من أصل ثلاث عشرة عبارة حازت على أعلى ترتيب موافق وهما /8-9/، أما بقية العبارات فقد كانت تتراوح كما أشرنا بين الحياد وعدم الموافقة الأمر الذي يشير إلى عدم وجود دور دال إحصائياً للممارسات الرقابية التي يقوم بها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي ومنه فإننا نقبل فرضية العدم القائلة: بعدم وجود دور دال إحصائياً للممارسات الرقابية التي يقوم بها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي، مقابل رفض الفرضية البديلة القائلة: بوجود دور دال

إحصائياً للممارسات الرقابية التي يقوم بها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي.

يمكن تفسير الأسباب المحتملة للنتائج :

1-وجود صعوبات في تنفيذ السياسات والإجراءات المتعلقة بالأمن السيبراني بسبب التعقيدات أو نقص الدعم.

2-نقص التدريب والتوجيه والمعرفة للتعامل مع مخاطر الأمن السيبراني بفعالية.

3-عدم كفاية المهارات التقنية المتعلقة بالأمن السيبراني بين أفراد عينة البحث.

4-نقص الموارد في الجهاز المركزي سواءً من حيث التكنولوجيا أو الخبرات البشرية، لتعزيز الأمن السيبراني في القطاع الحكومي.

5-عدم وضوح الدور المحدد للجهاز المركزي في مجال الأمن السيبراني، أو تضارب في الأدوار بين الجهاز المركزي والجهات الأخرى المعنية بالأمن السيبراني.

6-عدم وجود سياسات وإجراءات واضحة ومحددة لمهام أفراد عينة البحث فيما يتعلق بالأمن السيبراني.

التوصيات:

1-تطبيق إجراءات التحقق والتدقيق الدوري لنظم المعلومات في الجهات الخاضعة للرقابة لضمان الامتثال لمعايير الأمن السيبراني واتخاذ الإجراءات التصحيحية اللازمة.

2-تعزيز التدريب والتطوير المهني من خلال تنظيم دورات تدريبة متقدمة ومتخصصة في مجال الأمن السيبراني لجميع موظفي الجهاز المركزي للرقابة المالية، وتنظيم حملات توعية داخلية لتعزيز فهم الموظفين بأهمية الأمن السيبراني وكيفية المساهمة في تحقيقه، وتطوير المهارات والمعرفة بأحدث تقنيات وتحديات الأمن السيبراني.

3-عقد ورش عمل تفاعلية لزيادة الوعي وتبادل الخبرات بين أفراد الجهاز المركزي للرقابة المالية.

4-تشكيل فرق عمل مشتركة بين الجهاز المركزي للرقابة المالية والجهات الحكومية والجهات المعنية بالأمن السيبراني لتبادل المعرفة والخبرات حول أفضل الممارسات في الأمن السيبراني.

5- إعداد وتوزيع أدلة إرشادية مفصلة تشرح الأدوار والمسؤوليات والإجراءات المحددة التي يجب اتباعها في مجال الرقابة على نظم المعلومات والأمن السيبراني، وتشجيع موظفي الجهاز على المشاركة في وضع هذه الأدلة الإرشادية، مما يعزز الشعور لديهم بالمسؤولية والالتزام بالتنفيذ.

6-وضع مؤشرات أداء رئيسية لقياس فعالية الممارسات والإجراءات المتبعة من قبل موظفي الجهاز في مجال الأمن السيبراني.

7-إجراء تقييمات دورية لمراجعة الأداء وتحديد النقاط التي تحتاج إلى تحسين، وتنفيذ خطط تصحيحية عند الحاجة.

8-تحديث الأدلة الإرشادية والإجراءات المحددة لمهام موظفي الجهاز المركزي فيما يتعلق بالأمن السيبراني في الجهات الخاضعة للرقابة لضمان مواكبتها لأحدث التهديدات والتطورات.

9-تشجيع أفراد الجهاز المركزي للرقابة المالية على حضور المؤتمرات والندوات المتعلقة بالأمن السيبراني للاطلاع على أحدث التطورات والابتكارات.

10-توظيف خبراء متخصصين في مجال الأمن السيبراني في الجهاز المركزي للرقابة المالية لتنسيق الجهود وتقديم الدعم الفني لأفراد الجهاز في مهامهم.

11-تبادل أفضل الممارسات بين أعضاء الإنتوساي والأربوساي لتحسين الرقابة على نظم المعلومات والأمن السيبراني في القطاع الحكومي.

المراجع العربية:

1. الهلالي، الهلالي الشربيني،2020، مجلة تكنولوجيا التعليم والتعليم الرقمي–الجمعية المصرية للتنمية التكنولوجية، المجلد 1، العدد1.
2. علي، هبة جمال هاشم، 2023، منهج إجرائي مقترح لقياس مدى استجابة المراجع الخارجي للمخاطر السيبرانية في منشأة العميل، المجلة العلمية للدراسات والبحوث المالية والتجارية، كلية التجارة، جامعة دمياط، م4، ع2.
3. السمحان، منى عبد الله،2020، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، العدد111.
4. جاسم، عذراء ضياء، دور نظم المعلومات والرقابة الداخلية في تعزيز استقلالية العمل الرقابي، مجلة الإدارة والاقتصاد، العدد126.
5. الفوال، عصام، 2020، تقييم إمكانية الاستثمار في تطبيق نظام إدارة أمن المعلومات في قطاع الخدمات والاتصالات السورية، وزارة التعليم العالي، المعهد العالي لإدارة الأعمال، مشروع أعد لنيل درجة الماجستير في إدارة الأعمال، الإدارة التنفيذية.
6. الخصاونة، ريم عقاب،2009 ، إطار لتقييم رقابة ديوان المحاسبة في المملكة الأردنية الهاشمية في ضوء تطبيق الحكومة الإلكترونية رسالة دكتوراه، جامعة عمان العربية للدراسات العليا، الأردن.
7. الخصاونة، ريم عقاب، 2010 تقييم إجراءات الرقابة الحكومية في ضوء تطبيق الحكومة الإلكترونية في المملكة الأردنية الهاشمية، مجلة جامعة النجاح للأبحاث، مجلد9/24.
8. أحمد، مصطفى جبار، 2021، نظام الرقابة الداخلية في ظل التشغيل الإلكتروني وأثره على تقويم الأداء في المصارف، رسالة ماجستير، جامعة الشرق الأدنى، نيقوسيا.
9. الحكيم، سليم مسلم، 2010، إمكانية الرقابة على نظم المعلومات المحاسبية المؤتمتة للمؤسسات العامة ذات الطابع الاقتصادي من قبل مفتشي الجهاز المركزي للرقابة المالية في سوريا، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 26، العدد الأول.
10. المري، راشد محمد، يناير 2022، أثر تكنولوجيا المعلومات في النظام الأمني والرقابة الداخلية، مجلة البحوث الفقهية والقانونية.

11. منصور، آمنة محمد، 2021، تأثير الأمن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية، دراسة استطلاعية، مجلة الإدارة والاقتصاد العدد 127، آذار.
12. مقراني، قدور، 2016، تقييم مدى مساهمة أمن نظم المعلومات الإلكتروني في الحد من مخاطر نظم المعلومات، دراسة حالة مؤسسة اتصالات الجزائر جامعة قاصدي مرباح، ورقلة، الجزائر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، قسم علوم التسيير، مذكرة لنيل شهادة الماجستير.
13. السيد،علاء،2005 ، إطار مقترح لتطوير أداء الرقابة المالية، الجامعة الإسلامية، غزة، فلسطين.
14. المطيري، يوسف محمد،2020، أثر الرقابة المالية لديوان المحاسبة الكويتي على تفعيل معايير الحوكمة بالجهات الحكومية، مجلة كلية الاقتصاد والعلوم السياسية، المجلد21، العدد3.
15. المرسوم رقم 64 لعام 2003 المتضمن قانون الجهاز المركزي للرقابة المالية.
16. الزيود، أيمن حسن علي،2022، مدى فاعلية الرقابة الداخلية وتطبيقها في ظل نظام التشغيل الإلكتروني من وجهة نظر موظفي بلدية سحاب، المجلة العربية للنشر العلمي،العدد42.
17. محمد أمين، وليد ابراهيم،2018، دراسة تحليلية لدور أجهزة الرقابة العليا في تطوير نظم الرقابة الداخلية للحد من الفساد المالي بالوحدات الحكومية، ليبيا المجلة العلمية للدراسات التجارية والبيئية جامعة قناة السويس، مجلد9، العدد2.
18. الجابري، محمد، 2014، تقييم دور المدقق الداخلي في تحسين نظام الرقابة الداخلية لنظم المعلومات المحاسبية في شركات التأمين باليمن، مذكرة لنيل شهادة الماجستير، جامعة صنعاء، اليمن.
19. عداس، ضحى، ساكت، غسان،2020، نظام المعلومات المصرفية، منشورات جامعة حلب ،سورية كلية الاقتصاد.
20. عبيرات، مقدم، هواري، معراج، 2022، إدارة مخاطر الأمن وشفافية المعلومات لنظم المعلومات في ظل البيئة الرقمية، جامعة الأغواط، الجزائر.

21. قاسم، عبد الرزاق محمد، 2008، نظم المعلومات المحاسبية الحاسوبية، دار الثقافة للنشر والتوزيع عمان، الأردن.
22. العبيدي، فاطمة ناجي، 2012 ، مخاطر استخدام نظم المعلومات المحاسبية المحوسبة وأثرها على فاعلية عملية التدقيق في الأردن، مذكرة منشورة للحصول على درجة الماجستير في المحاسبة.
23. السديري، محمد بن أحمد، بن تركي، 2012، نظم المعلومات الإدارية، جامعة الملك سعود.
24. نور الهدى، شابو،2021، دور تكنولوجيا الاتصال الحديثة في تحسين الخدمة العمومية، مذكرة لنيل شهادة الماجستير، الجزائر، جامعة العربي بن مهدي أم البواقي.
25. حسين، سكفالي، مروة، مقلاتني، 2020، نظم المعلومات الإدارية وأثرها على الأداء الوظيفي للعاملين، دراسة حالة بنك الفلاحة والتنمية الريفية وكالة قالما، مذكرة لنيل درجة الماجستير في علوم التيسير، إدارة أعمال، جامعة 8 ماي، قالما.
26. المنظمة الدولية للقياس والهيئة الدولية للكهروتقنية، 2010، المركز القومي للمعلومات، الإدارة الفنية قسم الجودة والتطوير وحدة المعايير ، لجنة معايير نظم التشغيل والسرية والتأمين معيار قواعد الممارسة لإدارة أمن المعلومات، ISO 27002.
27. أميرهم، جيهان عادل، 2022، أثر جودة المراجعة الداخلية في الحد من مخاطر الأمن السيبراني وانعكاساته على ترشيد قرارات المستثمرين، مجلة البحوث المالية والتجارية، المجلد23، العدد الثالث.
28. العزازي، هاني محمد خليل إبراهيم، 2023، النظام القانوني الدولي لمكافحة المخاطر السيبرانية، مصر المعاصرة، عدد549.
29. شحاته، السيد شحاته، 2022، نحو دور فاعل للمراجع الداخلي في إدارة مخاطر الأمن السيبراني في الشركات المقيدة بالبورصة المصرية، المجلة العلمية للدراسات والبحوث المالية والإدارية، المجلد الثالث عشر، العدد الثاني.
30. يعقوب، ابتهاج إسماعيل وآخرون، 2022، مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية: دراسة اختبارية، مجلة الدراسات المالية والمحاسبية والإدارية، المجلد 9، العدد1.

31. القحطاني، سالم بن سعيد، العنزي، حمودين محمد، 2011، تبادل المعلومات بين الأجهزة الأمنية في المملكة العربية السعودية: دراسة ميدانية، أطروحة دكتوراه، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، السعودية.
32. دليل مبادرة الإنتوساي للتنمية بخصوص تدقيق تقنية المعلومات لمؤسسات التدقيق العليا،2022.
33. لطفي، أمين السيد أحمد، 2007 ، التطورات الحديثة في المراجعة، الدار الجامعية، الإسكندرية.
34. عقبة، الرضا، 2008، تدقيق الحسابات في ظل نظم المعلومات المحاسبية، ورقة عمل ضمن الفعاليات العالمية لجمعية المحاسبين القانونيين السوريين، سورية.
35. درة، عمر، أثر إدارة العدالة التنظيمية على إدارة ضغوط العمل(2007)، رسالة ماجستير في إدارة الأعمال، جامعة عين شمس، كلية التجارة، عين شمس.
36. ديبان، عبد اللطيف، 2004، نظم المعلومات المحاسبية وتكنولوجيا المعلومات.
37. السيد ،علاء ،2005،إطار مقترح لتطوير أداء الرقابة المالية ،الجامعة الإسلامية ،غزة ،فلسطين.

المراجع الأجنبية :

1. Stephanie Damarey; Execution et control des finans; Gualino Editeur,2007
2. Janulevicius Justinas, 2016, op, cit
3. Van der Meer Jeroen, 2012, Multi-criteria decision model inference and application in information security risk classification, Master Thesis of Computational Economics, Erasmus School of Economics, Erasmus, University Rotterdam
4. National Institute of Standards and Technology,2016, Internal Report 7621,Revision
5. Hunton, James , et al,2021, Business and Audit RISKS Associated with ERP SYSTEMS: knowledge Differences Between information systems audit specialists and financial auditors
6. IAIS. (2018), "Draft Application Paper on Supervision of Insurer Cybersecurity'", in IAIS (Ed.). IAIS,
7. The International Telecommunication Union , ITU Toolkit for Cybercrime Legislation , Geneva,2010
8. Kortjan, N. & Solms, R. (2013). Cyber security education in developing countries: a sout African perspective. Lecture notes of the institute for computer sciences, social informatics and telecommunications engineering

المواقع الإلكترونية:

- https://www.researchgate.net

عبد الحساني، وعد هادي، 2016، الرقابة الخارجية وأثرها في تقييم أداء الرقابة الداخلية

- https://www.skillcast.com

مخاطر سيبرانية في القطاع العام، مايو، 2024، فيفيك دود

- Lebanon<https://al-akhbar.com
- https://horizons-edu.com
- https://www.dgssi.gov.ma
- www.imd.org

بقلم ديديبه كوسين وأبراهام هونغزي لو، مايو، 2021

- www.isaca.org /resources/isaca journal/issues/2022/volume-3/
- www.ad-dawra.com
- www.mah6at.net

مخاطر سيبرانية في القطاع العام، مايو، 2024، فيفيك دود

- https;// www.mah6at.net
- www.imd.org

بقلم ديديبه كوسين وأبراهام هونغزي لو، مايو، 2021

- https:// www.sis.gov.eg
- https:// mawdoo3.com
- Michael Aaron Dennis,May, 2024,https://www.britannica.com
- 2021https:mawdoo3.com

قصي أبو شامة، 12 ديسمبر

- https://isf.gov.ib

دليل التوعية حول المخاطر السيبرانية

- https://www.barikat.com.tr
- https://fastercapital.com
- htts://gridlex.com/ the impact of cybersecurity risks on the audit process in accounting
- https:// www.checkpoint.com الأمن الإلكتروني/ المحور السيبراني
- https://www.unjiu.orghttps://governmenttechnolo gyinsider.com by Jackie Davis August 16.201

استبيان

عن بحث بعنوان:

دور الرقابة على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي

إعداد الباحثة: عبير زرّاق

تهدف الباحثة من خلال هذا الاستبيان إلى:

- **قياس دور الرقابة على نظم المعلومات التي يقوم بها مفتشي الجهاز المركزي للرقابة المالية بالإضافة إلى الإجراءات التي تقوم بها إدارات الجهات الخاضعة للرقابة (من خلال تقييم المفتش لنظام الرقابة الداخلية والضبط الداخلي) في الحد من مخاطر الأمن السيبراني في القطاع الحكومي، والذي يعتبر مفهوم حديث يعبر عن أمن الشبكات والأنظمة المعلوماتية وكافة البيانات والمعلومات والأجهزة المرتبطة بالإنترنت ومخاطره من فقدان المعلومات الخاصة والحساسة، والتلاعب واتلاف البيانات والأنظمة والشبكات.**

يرجى وضع علامة (√) في الخانة المناسبة لاختيارك:

(البيانات الشخصية)

1-الجنس :

ذكر □ انثى□

2-المسمى الوظيفي:

مفتش معاون □ 2-مفتش □ 3-مفتش أول□

3- العمر :

21 -30 سنة□ 31-40 سنة□ 41-50 سنة□ أكثر من 50 سنة□

4- المؤهل العلمي:

إجازة جامعية□ دراسات عليا (ماجستير – دكتوراه) □ ماجستير رقابة□

5-سنوات الخبرة

أقل من سنة□ 1-5سنوات□ 6-10سنة□ 11- 15سنة□ فوق 15 سنة□

المحور الأول: تقييم نظام الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي استناداً إلى مراجعة بنية وهيكلية الرقابة الداخلية وتقييمها من قبل الجهاز المركزي للرقابة المالية

الرقم	العبارة عند قيامك بمراجعة واختبار وتقييم نظام الرقابة الداخلية والضبط الداخلي في بيئة نظم المعلومات ماهي درجة موافقتك على العبارات التالية:	موافق بشدة	موافق	محايد	لا أوافق	لا أوافق بشدة
1	توفر ضوابط الوصول للبيانات والمعلومات للحد من مخاطر الاختراق وسوء الاستخدام واتلاف المعلومات الحساسة					
2	الاحتفاظ بنسخ احتياطية للملفات والسجلات الهامة في مكان آمن بشكل دوري					
3	الضوابط الداخلية لتقنية المعلومات المتعلقة بسرية البيانات وسلامتها وصلاحيتها وتوافرها قد تم تبنيها من قبل الجهة الخاضعة للرقابة					
4	تطبيق اجراءات الأمان الأساسية مثل وجود كلمات سر قوية تتضمن أرقام وأحرف كبيرة وصغيرة ورموز غير قابلة للتنبؤ وتغييرها بانتظام					
5	عدم مشاركة كلمات السر مع الآخرين					
6	الفصل بين الوظائف المتعارضة لمستخدمي النظام مثل فصل مهام المحاسبة عن مهام أمين الصندوق					
7	وجود قائمة بأسماء الموظفين المخول لهم استعمال المنظومة					
8	الإدارة المعنية بالأمن السيبراني في حال وجودها مستقلة عن الإدارة المعنية بتقنية المعلومات					
9	تحديث الأجهزة القديمة واصدارات البرامج غير المدعومة لما تسببه من مخاطر كبيرة على بيانات المؤسسة وعملياتها					

10	وجود كاميرات للمراقبة لكشف أي متسلل وصيانتها دوريا					
11	اختيار موقع آمن للأجهزة					
12	استخدام الأجهزة والبرمجيات التي تساعد على زيادة الرقابة للدخول على الشبكة مثل مقاوم الفيروسات					
13	تحديث برامج مكافحة الفيروسات بشكل دوري					
14	وضع ضوابط من أجل سرية البيانات وتشفيرها وعدم إمكانية الاطلاع عليها إلا من قبل الأشخاص المخول لهم ذلك					
15	نقل البيانات من موقع لآخر يتم عبر قنوات نقل آمنة غير قابلة للاختراق					

المحور الثاني: دور الرقابة التي يمارسها الجهاز المركزي للرقابة المالية على نظم المعلومات في الحد من مخاطر الأمن السيبراني في القطاع الحكومي:

الرقم	العبارة في الجهات الخاضعة للرقابة والتي تحتوي على نظم معلومات يقوم المفتش بعدة مهام ما درجة موافقتك على العبارات التالية :	موافق بشدة	موافق	محايد	لا أوافق	لا أوافق بشدة
1	التأكد من مقدرة الأنظمة المعلوماتية على توفير أدلة الاثبات الملائمة لعملية الرقابة					
2	تقييم ومتابعة مدى التزام الهيئة الخاضعة للرقابة بتوفير اجراءات الملائمة والمتعلقة بأمن البيانات وحفظها من التلف أو التحريف والاجراءات المتبعة لسلامة نظام المعلومات					
3	التأكد من الاستعمال الفعال لبرامج الحماية (جدران النار) وبرامج الحماية من الفيروسات لحماية النظم من إدخال البرامج الضارة أو غير المخولة					
4	التأكد من الاستعمال الفعال للتشفير ويشمل ذلك الاحتفاظ بالسرية والأمن أثناء ارسال البيانات والمعلومات عبر الشبكة ومنع سوء الاستعمال من خلال تقنية التشفير					
5	الرقابة على التزام الجهات الخاضعة للرقابة في معالجة البيانات وفق القوانين والأنظمة المعمول بها والالتزام بالتشريعات الخاصة بالأمن السيبراني					
6	التأكد من القدرة على استعادة وثائق العمليات من ملفات الوثائق الالكترونية مثل الوثائق المخزنة عبر الانترنيت أو في الأنظمة الإلكترونية					
7	اعطاء المفتش صلاحية الاطلاع على جميع المعلومات في قاعدة البيانات والقيام بتدقيق قاعدة البيانات للتأكد من سلامة المخرجات وعدم الازدواج أو التكرار عن طريق أخذ عينة وحسابها يدويا للحصول على نتيجة واحدة					
8	التأكد من صلاحية أجهزة الحماية وتعبئتها بشكل دوري مثل أجهزة الحماية من الحريق					
9	التأكد من قيام الجهة الخاضعة للرقابة بإجراء جرد شامل لكافة معدات نظم المعلومات					
10	التأكد من وجود أنظمة وإجراءات لمعالجة الأخطاء والانحرافات المكتشفة					
11	التأكد من وجود خطط استمرارية الأعمال واجراءات التعافي من الكوارث ومدى فعاليتها.					

12	التأكد من وجود مصادقة للعمليات الهامة من قبل موظفين اثنين أو أكثر حسب الصلاحيات					
13	التأكد من أن مخرجات البرنامج تتماشى مع الهدف الذي صمم من أجله					