الأمن السيبراني

وحمـــــاية أمن المعلومات

المشرف التربوي الاستاذ / فيصل محمد عسيري

(تقنية المعلومات)

.

الملخص

تعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيات الاتصالات والمعلومات المتصلة بالشبكة العالمية. غير أن هذا الاعتماد المطرد ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكة وأمن المعلومات والمجتمع المعلوماتي وأعضائه. إن سوء الاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية وأمن الأطفال .

لقد بات الأمن السيبراني يشكل جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات معلوماً أن صناع القرار في الولايات المتحدة الأمريكية، الاتحاد الأوروبي، روسيا، الصين، الهند وغيرها من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية. بالإضافة إلى ما تقدم، فقد أعلنت أكثر من ١٣٠ دولة حول العالم عن تخصيص أقساماً وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني. تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، الاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية .وتهتم الدراسة بمعرفة الامن السيبراني وتأثيرة في المملكة العربية السعودية

Summary

Modern societies are increasingly dependent on global communication and information technologies. However, this steady dependence is accompanied by a range of emerging and potential threats that are fundamentally threatening the network, information security and the information society and its members. The growing misuse of electronic networks for criminal purposes adversely affects the integrity of sensitive national information infrastructures, particularly on personal information and child security.

Cybersecurity has become an integral part of any national security policy. It has become known that policymakers in the United States of America, the European Union, Russia, China, India and other countries have categorized cybersecurity / cybersecurity issues as a priority in their national defense policies. In addition, more than ١٣٠ countries around the world have announced the allocation of cyber warfare divisions and scenarios within national security teams. All these efforts are added to traditional security efforts to combat cybercrime, e-fraud and other aspects of cybersecurity.

The study is concerned with the knowledge of cybersecurity in Saudi Arabia

المقدمة :

يعتبر الامن الركيزة الاساسية للمجتمع، بحيث لا يمكن تصور نمو اي نشاط بعيدا عن تحققه، سواء اكان ذلك، على المستوى التقني، ام على المستوى القانوني. وقد تحول الامن، مع بروز مجتمع المعلومات، والفضاء السيبراني، الى واحد من قطاع الخدمات، التي تشكل قيمة مضافة، ودعامة اساسية، لأنشطة الحكومات والأفراد، على السواء، كما هو الحال، مع التطبيقات الخاصة بالحكومة الالكترونية، والصحة الالكترونية، والتعليم عن بعد، والاستعلام، والتجارة الالكترونية، وغيرها الكثير. الا ان الوجوه المتعددة للامن السيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الإساءة إلى الأفراد، والمؤسسات، بل تتعداها الى تعريض سلامة الدول والحكومات، تزيد مهمة القيمين على الموضوع تعقيدا وصعوبة، وتستدعي مقاربة، شاملة، ومتكاملة، لجميع التحديات، التي يطرحها الفضاء السيبراني، بحيث تأتي الردود، والحلول المقترحة، ناجعة وفاعلة في تحقيق الامن، وبناء الثقة في الفضاء السيبيري، من أساسيات تسخير تقنيات المعلومات والاتصالات، في مجالات التنمية خدمة للمجتمعات الانسانية ([1]).

لذلك، لا بد من التوقف بداية، عند ماهية الامن السيبراني، والأخطار السيبرانية، لنستعرض بعدها أبعاد هذا الامن، وما يرتبط به من تحديات، مع التركيز على الاطارين التشريعي والتنظيمي في العالم العربي، والصعوبات الاكثر بروزا، لنصل الى أساسيات المواجهة، والمقترحات.

يعرف الأمن السيبراني بأنه مجموعة من الوسائل التقنية والإدارية التكنولوجية والعمليات والممارسات المصممة التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به. ويعرف أيضا بأنه أمن تكنولوجيا المعلومات، ويمكن أن تقلل تدابير الأمن السيبراني الفعالة من مخاطر الهجمات السيبرانية.

كذلك يمكن تعريف الامن السيبراني، انطلاقا من أهدافه، بانه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن امكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه، باسرع وقت ممكن، بحيث لا تتوقف عجلة الانتاج، وبحيث، لا تتحول الاضرار الى خسائر دائمة.

ويُعرّف الفضاء السّيبراني بأنّه المجال المجازيّ لأنظمة الحاسوب والشّبكات الإلكترونيّة حيث تُخزّن المعلومات الكترونيًّاً وتتمّ الاتصالات المباشرة على الشّبكة.

ويعتبر الأمن السيبراني مفهوم أوسع من أمن المعلومات حيث يتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية أو الخارجية والتي يتم تخزينها في خوادم داخل أو خارج المنظمات من الاختراقات ([٢]) .

تحديد المشكلة :

أصبحت تكنولوجيا المعلومات أكثر تعقيدًا من ذي قبل ، وارتبط بذلك احتمالات تعرض تلك التكنولوجيا لمخاطر من شأنها أن تؤثر على كفاءة وفعالية نظم المعلومات ، وبصفة خاصة نظام المعلومات المحاسبي ، ومن ثم على جودة المعلومات المحاسبية ، حيث يؤدي تعرض تلك النظم للمخاطر إلى التأثير على سرية ونزاهة وتوافر المعلومات ، وعلى الرغم من ذلك فإنه في مجال المال والأعمال لا يمكن الاستغناء عن تلك التكنولوجيا أو حتى الإقلال من الاعتماد عليها ، بل على العكس يزداد اهتمام المسئولين بالمنظمات المختلفة بتطوير تكنولوجيا المعلومات وتحقيق أقصى استفادة ممكنة من الإمكانات المتاح استخدامها .

وأصبح من الضروري على المنظمات والمؤسسات والشركات أن تهتم بوضع نظم وإجراءات تعمل على الحد من تلك المخاطر ، ووضع نظام جيد لإدارتها ، ووجد أن الحلول التكنولوجية ضرورية ولكنها غير كافية في مواجهة تحديات ومخاطر أمن المعلومات ، ومن ثم زاد الاهتمام بأمن المعلومات باعتبارها من المسئوليات التنفيذية المهتمة بالبنية التحتية التكنولوجية على مستوى المؤسسة وزيادة التركيز على استراتيجيات متطلبات العمل وإشراك الأشخاص المناسبين ، وتوظيف التكنولوجيا المناسبة ، وحماية أصول المعلومات الهامة .

ومن ثم تتمثل المشكلة في الإجابة عن التساؤلات التالية :

١ـ ما هي الوسائل التقنية والإدارية التكنولوجية والعمليات والممارسات المصممة التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به ؟

٢ـ ما هي طبيعة المخاطر التي تتعرض لها نظم المعلومات الالكترونية وما هي أنواعها ؟

٣ـ ما هي أسباب تعرض نظم المعلومات الالكترونية لتلك المخاطر ؟

٤ـ ما هي المعايير الدولية التي يتم استخدامها في إطار حوكمة أمن المعلومات ؟

٥ـ هل تساهم معايير حوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الالكترونية ؟

الأهداف :

١ـ التعرف على نوعية المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية .

٢ـ استكشاف أسباب تعرض نظم المعلومات المحاسبية الالكترونية إلى المخاطر.

٣ـ التعرف على ماهية الأمن السيبراني والتحقق من مدى استخدامه في بيئة الأعمال في المملكة العربية السعودية .

٤ـ تحديد المعايير المستخدمة في الأمن السيبراني ، وتحديد المعايير الأكثر تأثيرًا في الحد من مخاطر نظم المعلومات المحاسبية الالكترونية .

الأهمية:

تنبع أهمية البحث من خلال الاهتمام المتزايد بالمخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية في الهيئات والمؤسسات المختلفة ، وقيام الجهات المعنية بإصدار المعايير الدولية بمحاولة مواكبة التطورات السريعة والمتلاحقة في هذا المجال ويمكن إيضاح أهمية البحث من خلال ما يلي :

١ـ محاولة إلقاء الضوء على تنوع وتعدد المخاطر التي تتعرض لها نظام المعلومات المحاسبية الالكترونية .

٢ـ توضيح المحاولات التي تقوم بها المؤسسات والهيئات للحد من تلك المخاطر .

٣ـ إلقاء الضوء على منهج شامل يستخدم في مواجهة هذه المخاطر .

٤ـ معرفة المعايير التي يتم استخدامها عند تطبيق الأمن السيبراني (أمن المعلومات) داخل المؤسسات والهيئات المختلفة .

المنهج :

اعتمد الكاتب على المنهج العلمي بشقيه الاستنباطي والاستقرائي لتحليل وتقييم الدراسات والبحوث السابقة التي تناولت مخاطر نظم المعلومات المحاسبية الالكترونية والوسائل والإجراءات التي تتبعها الهيئات والمؤسسات في الحد من تلك المخاطر ودور أمن المعلومات (الأمن السيبراني) في ذلك .

كما قام الكاتب بإجراء دراسة ميدانية بهدف التعرف على نوعية المخاطر التي تتعرض لها نظم المعلومات المحاسبية في بيئة الأعمال السعودية ومدى استخدام أمن المعلومات والمعايير المتعلقة بها في الحد من تلك المخاطر .

حدود البحث :

استقصاء آراء عينة الدراسة وهم المديرون الماليون والمحاسبون وموظفو إدارة تكنولوجيا المعلومات والمراجع الخارجي لشركات الاتصالات ، وشركات تكنولوجيا المعلومات ، والبنوك العاملة في المملكة العربية السعودية .

أهداف الأمن السيبراني

أصبحت جميع أمورنا الحياتية الآن متعلّقة باستخدام الإنترنت والتكنولوجيا، وإن تنوّع وسائل المعلومات والاتصالات والتطبيقات وتفاوت خصائصها وطبيعتها زاد من حجم التعقيد بسبب تبادل المعلومات بين العالم وبين الأفراد والحكومات، فأصبحت من الأمور المهمة والحيوية للفرد وللمواطن، فجميع الوزارات والمؤسسات الحكومية والخدمات بالمملكة مرتبطة ارتباط وثيقاً وتقنياً بهذه التكنولوجيا التي توفر خدماتها للمواطنين وتوفر سبل الراحة كاختصار للوقت والتقليل من المادة. فيمكنك وأنت جالس الآن في منزلك وأمام شاشة كمبيوترك أو أمام شاشة جوالك أن تنهي جميع معاملات الحكومية من خلال هذه الخدمات والتطبيقات بالإنترنت ويمكنك إنهاء جميع معاملاتك خلال دقائق. ومع كل هذه الخدمات والراحة التي توفرها لنا هذه التكنولوجيا الجميلة، ظهرت مشكلة انبثقت مع هذه التكنولوجيا وهي الأمن السيبراني؛ وهو أنه لا بد أن نقوم بحماية سير هذه العمليات وحماية البيانات والتطبيقات وحفظ المعلومات الوطنية للأفراد والدولة، والمحافظة عليها؛ يعني منع أي دخول عليها غير مرخص أو العبث بها والتي لا بد أن يكون هناك نظام قوي يحمي هذه الخدمات والمعلومات التي توفرها وتزوّدنا بها هذه التكنولوجيا الجميلة عبر الفضاء الإلكتروني([٣])، لذلك ظهر مصطلح الأمن السيبراني في أواخر هذا العصر والذي جاء من لفظ السيبر المنقول عن كلمة (Cyber) اللاتينية ومعناها «الفضاء المعلوماتي»، وهو تعبير شامل يصف جميع الأمور المتعلّقة بحفظ هذه الخدمات والبيانات وتدفق سيرها والذي يحوي كل ما يتعلّق باستخدامات وآليات وتطبيقات وتجهيزات تقنية وتدفق البيانات والمعلومات، والبرامجيات، والترابط فيما بينها من خلال شبكات الحاسب والاتصالات والإنترنت.

لذلك جاء الأمر الملكي القاضي بإنشاء (الهيئة الوطنية للأمن السيبراني) وارتباطها بخادم الحرمين الشريفين الملك سلمان بن عبد العزيز خطوة رائدة قوية وجاءت في وقتها حقيقة لأني أنا بحكم تخصصي في هذا المجال من عشرات السنين إلا أن الوقت هذا زادت فيه الأمور تعقيداً وأصبحت الحماية ومعرفة ماذا يملك الطرف الآخر سواء من مهاجم الإلكتروني أو هكر يريد أن يدخل الأنظمة الداخلية، وللمحافظة على أمن المجتمع السعودي الإلكتروني واستقراره، وتأمين سلامة عمل

قطاعات الدولة الإلكترونية المختلفة من خلال تحقيق الأمن الإلكتروني لها من أي مشاكل قد يتم الاعتراض عليها أو أي اختراقات تهددها. يهدف الأمن السيبراني إلى تعزيز حماية جميع ما يتعلّق بالدولة إلكترونياً وأفراداً لحماية هذه الأنظمة الإلكترونية وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية وجميع مكوناتها المحيطة بالمجتمع من أجهزة وبرمجيات ومعدات وجميع ما يؤثّر على تقدّم هذه الخدمات([٤])، وما تحويه من بيانات، فأصبحت هذه أيضاً من أهم الأولويات المهمة والحيوية لجميع دول العالم لأنهم يريدون أن يحافظوا على بيانات مواطنيهم وحفظ ممتلكاتهم وبياناتهم الإلكترونية، وأخذ كثير من الدول على عاتقها وخاصة الدولة المتقدّمة في الكثير من الاهتمامات والاحتياطات والتعمق في هذا التخصص الذي يمس حياة مواطنيهم، فأنشئوا الكليات والمعاهد ومراكز البحوث حتى يتم معرفة كل شيء يقوم بتوفير الحماية لمواطنيهم ولمجتمعاتهم، ومن أهم ما يدور في هذه التخصص والذي يقدمه هو:

١- تأمين البنى التحتية لأمن المعلومات والبيانات الخاصة بالمواطنين، مثلاً عندنا في المملكة لا بد من حماية قوية لجميع ما يتعلّق ببيانات المواطنين وحفظها في مكان آمن، وكذلك جميع أجهزتها ومواردنا الحياتية سواء من ممتلكات إلكترونية من أي محاولة عبث أو اختراق أو تدمير وتوفير الحماية اللازمة.

٢- حماية شبكة المعلومات والاتصالات والتي تلعب دوراً كبيراً في تدفق خط سير تدفق البيانات بين المواطنين والدولة ومن طرف إلى طرف آخر، والتي إذا تعرضت إلى تخريب أو تدمير أو اختراق حتماً قد يؤثّر ويقطع هذه الاتصالات ويتوقف سير العمل وتتوقف الخدمات([٥]).

٣- حماية شبكة المعلومات من أي هجوم وذلك بمعرفة آخر التقنيات والتكنيكات الموجود في هذا المجال ومن أهمها كشف أهداف رسائل هذا العدو والتعرّف على طبيعة هذا المهاجم وذلك وماذا يريد من خلال معرفة تكنيكاته المستخدمة والأساليب المختلفة لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني مُحكم يمنع هذا الهجوم.

٤- تشفير التعاملات الإلكترونية بحيث لا يستطيع أي مخترق أو مهاجم أو عابث أن يدخل بسهوله لهذه البيانات والتطبيقات لأن التشفير أحد أساليب الحماية والتي يصعب فك رموزها. هذه أساسيات أرى أنه لا بد لكل مواطن سعودي أن يعرف هذه النقاط ويتعرَّف عليها جيداً ويعيد قراءتها أكثر من مرة لأنها تمس أمور حياتنا وتمس أمننا الإلكتروني، ماذا يجب على المجتمع العمل في حال تعرضت إلى هجمات من هذه النوعية في هذه الخدمات الإلكترونية وأدت إلى انقطاعها .

أبعاد الأمن السيبري

يرتبط الأمن السيبري بمجالات مختلفة سياسة وعسكرية واقتصادية وقانونية واجتماعية، بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من أي تهديدات سيبرية محتملة، ويمكن توضيح ذلك من خال الآتي([٦]):

١- البعد العسكري تكمن الميزة النسبية للقوة السيبرية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة إعطاء الأوامر العسكرية، والقدرة على إصابة الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي اختراق خارجي قد يتسبب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات، ومن ثم تدمير قواعد البيانات العسكرية، وتعطيل قدرة الدولة على النشر السريع لقدراتها وقواتها، أو قطع أنظمة الاتصال بين الوحدات العسكرية وتعطيل شبكات الكمبيوتر، كما يمكن أن يتم شل أنظمة الدفاع الجوي أو التوجيه الإلكتروني للخصم فضلا عن امكانية فقدان السيطرة على وحدات القيادة والتوجيه، بالإضافة إلى فقدان العدو قدرته على التحكم أو الاتصال بالأقمار الصناعية

٢- البعد الاقتصادي أصبح الفضاء الإلكتروني جاذبا لقطاعات المجتمع كافة، افرادا و جماعات وزاد الاعتماد بصورة أساسية على التكنولوجيا الرقمية في تخزين البيانات والمعلومات، بالإضافة لاستخدام الحاسب الآلي في تطوير الصناعات وتحريك الاقتصادات، وأصبحت المعاملات المالية والاقتصادية محوسبة، وباتت شبكات البنوك والبورصات وشركات الأسواق المالية مرتبطة ببعضها البعض بنظم و شبكات الكترونية، فأصبحت الإنترنت هي أساس المعاملات المالية والاقتصادية وباتت تشكل محورا رئيسيا للتطور الاقتصادي في القرن الحادي والعشرين، وهو ما أثار الحديث عن أهمية تحقيق الأمن السيبري في المجال الاقتصادي([٧]).

٣- البعد الاجتماعي يشير تقرير مؤسسة We Are Social إلى أن نحو ٢,٥ مليار نسمة؛ أي ما يعادل٣٥% من سكان العالم يستخدمون الإنترنت في عام٢٠١٤ وذلك بزيادة تقدر بـ١٣٥مليون مستخدم عن العام السابق ولا شك في ان هناك دورا للإنترنت في تعبير المواطن عن

تطلعاتــه فــي المجــالات المختلفــة ســواء سياســية أو علميــة أو اقتصاديــة أو ثقافيــة ..إلــخ، وبعــض مــن المــواد المنشــورة مفيــدة وتؤثــر بالإيجــاب علــى اخلاقيات المجتمع و البعض الاخر يمثل تهديدا له كالمــواد الإباحيــة، والإرهــاب، ونشــر الفكــر المتطــرف، ومحاولــة تجنيــد الشــباب، والترويــج للاتجــار بالممنوعــات..

٤- البعد السياسي: هنــاك أمثلــة كثيــرة تدفــع نحــو الاهتمــام بالبعــد السياســي للأمــن الســيبري كالتســريبات المختلفــة للوثائــق الحساســة، التــي ســببت مشكلات فــي عاقــات الــدول ببعضهــا البعــض، ممــا حتــم علــى الــدول إعــادة النظــر فــي سياســتها الخارجيــة فــي ظــل هــذه التســريبات. كمــا لا يجــب إغفــال الــدور البــارز لشــبكات التواصــل الاجتماعــي فــي تحقيــق أهــداف سياســية، كتنظيــم حمــلات انتخابيــة أو تظاهــرات افتراضيــة، وحــركات احتجاجيــة إلكترونيــة، هــذا ًفضــلا عــن قيــام بعــض الــدول، مثــل الولايــات المتحــدة ببــث رســائل سياســية علــى مواقــع التواصــل الاجتماعــي لتحقيــق أهدافهــا، كقيــام الجيــش الأمريكــي بتطويــر برنامــج إلكترونــي يعمــل علــى تدشــين حســابات شــخصية علــى مواقــع التواصــل الاجتماعــي بلغــات مختلفــة، بهــدف بــث رســائل مــن خلالهــا تدعــم الرؤيــة الأمريكيــة علــى مواقــع التواصــل الاجتماعــي ومــن ناحيــة أخــرى وجــدت كثيــر مــن الحــركات الإرهابيــة فــي هــذه المواقــع (٨) .

مجــالا لتجنيــد أفرادهــا وجمــع التمويــل لعملياتهــا، واســتخدامه كوســيط فــي الاتصــال بيــن هــذه الحــركات، ممــا اســتجوب علــى الــدول العمــل علــى حمايــة أمنهــا الداخلــي مــن التهديــدات والمخاطــر التــي قــد تتعــرض لهــا مــن خــال الإنترنــت مــن هــذا الجانــب.

٥- البعد القــانوني تعــد العلاقــة بيــن القانــون والتكنولوجيــا علاقــة تبادليــة، فالتطورات التكنولوجيــة المختلفــة تفتــرض مواكبــة التشــريعات القانونيــة لهــا مــن خــلال وضــع أطــر وتشــريعيات للأعمــال القانونيــة وغيــر القانونيــة منهــا، ولكــن بصــورة عامــة تفتقــد الجريمــة الســيبرية ًحاليــا للأطــر القانونيــة الصارمــة للتعامــل معهــا، ولعــل هــذا يعــود ًحاليــا لعوامــل، مثــل طبيعــة الجريمــة الإلكترونيــة ذاتهــا، وصعوبــة تحديــد هويــة مرتكبــي تلــك الجرائــم، ومرونــة التعريفــات المرتبطــة بتكنولوجيــا المعلومــات، إلــى جانــب كــون الجرائــم الســيبرية غيــر مقيــدة بحــدود الــدول الأمــر الــذي يقتضــي تفعيــل التعــاون الدولــي المشــترك لمكافحتهــا (٩).

خصائص الامن السيبراني

تعتبر هذه الجرائم، جرائم لها خصائص خاصة بها لا تتوافر في الجرائم التقليدية، فهي ذات بعد عالمي لا حدود جغرافية لها، كذلك هناك تبادل الخبرات الإجرامية فيما بين المجرمين لابتكار أساليب جديدة مواكبة، لا تتطلّب مجهوداً بل تنفذ بأقل جهد ممكن ولا تتطلب عنفًا

– صعوبة الاكتشاف لأنها لا تترك أثرًا يسهل تعقبه، بالإضافة إلى أنّ الضحية لا تلاحظها إلا بعد وقت من وقوعها ([١٠]) .

– السرعة وغياب الدليل وصعوبة إثباته بالإضافة إلى توفر وسائل تقنية تعرقل الوصول للدليل والبراهين

– التقنية العالية والخبرة الفائقة للمجرم في مجال الاتصالات، الشبكة العنكبوتية، استخدام الحاسوب والتكنولوجيا المعاصرة

– ضعف الأجهزة الأمنية والقضائية تجاهها نتيجة نقص الخبرة التقنية لديها نظرًا لما تَتطلبه هذه الجرائم من تقنية لاكتشافها والبحث عنها

الشّبكة العنكبوتيّة والأخطار المحدقة ([١١]) .

إنّ الشّبكة العنكبوتية هي مصدر مهم للمعلومات العامّة والبيانات ومنبر لتبادُلها واستثمارها، إلّا أنّ بعض الفئات تَستغلُّ هذه الإمكانيّة لإرسال مَعلومات ممنوعَة ومحظرة من أجل السَّيطرة والسُّلطة والرّبح الماديّ أو لتحقيق أهدافٍ شَخصيّة مشبوهة، ملتوية وإرهابية، في غياب نظم الحماية وقواعد الحيطة والضّوابط (المفروضة من قبل النظام الحاكم أو القائم) والرّقابة القانونية ([١٢]).

وحدة الأمن السيبراني ([١٣]) :

من أهداف الرؤية السعودية لعام ٢٠٣٠ هي تطوير البنية التحتية الرقمية حيث تم تسليط الضوء على الشراكات ما بين القطاعين العام والخاص كوسيلة لتطوير قطاع الاتصالات وتقنية المعلومات في المملكة، وتشمل الالتزامات تقوية حوكمة التحول الرقمي من خلال المجلس الوطني ودعم الاستثمارات المحلية في قطاع الاتصالات وتقنية المعلومات. ويعد الأمن السيبراني مكون أساسي من مكونات أي تحول رقمي حيث أن حماية البيانات والبنية التحتية سيكون مصدر قلق كبير للحكومة والعامة والقطاع الخاص بسبب نمو الهجمات السيبرانية في العقد السابق مما أصبح من الضروري التعامل مع مثل هذه الهجمات ومعالجتها بشكل مبتكر. بالإضافة الى أن إعداد وتثقيف الموظفين السعوديين يعد جزء أساسي من حركة التحول الرقمي([١٤]).

رؤية ومهمة وحدة الأمن السيبراني :

تتطلع وحدة الأمن السيبراني إلى المساهمة بشكل كبير في تحقيق رؤية ومهمة مركز الابتكار في جامعة الأمير سلطان والمبادرات السعودية لعام ٢٠٢٠.

الأهداف :

تهدف وحدة الأمن السيبراني الى تقديم الخدمات التعليمية والبحثية والتوعوية والتعاونية، والتي تشمل ولا تنحصر فقط على التالي:

١. اثراء التوعية بأهمية الأمن والاستعداد في الثقافة السعودية.

٢. مرفق جديد لمنهج متنامي ومتزايد من مقررات الأمن السيبراني الجامعية والعليا.

٣. الترويج للجامعة.

٤. خدمات استشارية (احتياجات الحكومة والصناعة).

٥. خدمات تدريبية.

٦. استضافة وتنظيم مؤتمرات ومنتديات وورش عمل ومسابقات.

٧. اقتراحات للبحث العلمي وبرنامج ماجستير الهندسة البرمجية.

٨. حلول لمنتجات أمن البرمجيات والتي تشمل: أدوات الاختبار ومجموعات البيانات والخدمات الأمنية.

٩. المشاريع (الممولة (محلياً أو عالمياً) أو المشتركة).

١٠. براءات الاختراع([١٥]).

١١. التعليم من أجل التوظيف: فرص عمل. ١٢. المنشورات.

واقع الدول العربية في مجال الفضاء السيبراني وضرورة إنشاء اجهزه\هيئات مختصة للأمن السيبراني في الوطن العربي:

إن المجتمع العربي ليس مجتمعًا منتجاً معلوماتياً على صعيد البرمجيات وعلى صعيد التجهيزات الإلكترونية الصلبة. وما زال يعاني من ضعف البيئة القانونية وقلة خبرة أهل المهن القانونية، ونقص التعليم الجامعي لهذه المادة، وهو يشهد واقعاً صعباً وغير متجانِس مع المعايير والمتطلبات الدولية والذي يعرض الكيانات العربية للإخطار والهجمات السيبرانية من قبل أفراد، مجموعات منظمة، مؤسسات خاصة، منظمات ارهابية (داعش)، دول متضررة او معادية (اسرائيل)، للنهوض

من هذا الواقع الجامد ومواكبة التحديات، يقتضي الإسراع في مقاربة مجال الفضاء السيبراني والجريمة السّيبرانية بالاستجابة الى:

١- استحداث استراتيجيات وطنية للحماية القومية أو لحماية معلومات الأفراد وبياناتها، والبنية التحتية للمؤسسات العامة والخاص([١٦])

٢- تطوير استراتيجيات وطنية لمكافحة جرائم المعلوماتية وذلك ناجم عن غياب تشريعات ملائمة لها، بالإضافة إلى عدم وجود تعاون إقليمي ودولي في هذا المجال

٣- تبني سياسة تعميم ثقافة وطنية تعنى بموضوع حماية الفضاء السيبراني، فقد شهد المجتمع العربي بطأ في بناء المعرفة والاستخدام المعلوماتي طوال ٣٠ سنة وعانى من صعوبة في الانخراط في عالم المعرفة مطلع الالفية الجديدة([١٧])

تقرير / الأمن السيبراني .. حماية وطنية لأمن الفرد والمجتمع في المملكة / إضافة أولى

أكد خبراء علوم الحاسب الآلي وأمن المعلومات في المملكة أن الأمر الملكي القاضي بإنشاء (الهيئة الوطنية للأمن السيبراني) وارتباطها بمقام خادم الحرمين الشريفين الملك سلمان بن عبدالعزيز آل سعود - أيده الله - خطوة رائدة للمحافظة على أمن المجتمع السعودي واستقراره وتأمين سلامة عمل قطاعات الدولة المختلفة من خلال تحقيق الأمن لها من أي اختراقات قد تحدث لا سمح الله في ظل التطور الهائل الذي نعيشه في هذا القرن في استخدامات الحاسب، وما صاحبه من تنوع في الوسائل الاتصالية، والبرامج الحاسوبية وتطبيقاتها، الأمر الذي زاد من حجم انتشار المعلومات، وتبادل البيانات بين مختلف قارات العالم.

وقالوا في تصريحات لوكالة الأنباء السعودية: إن تنوع وسائل الاتصالات وتفاوت خصائصها وطبيعتها زاد من حجم تبادل المعلومات بين العالم بشكل تسبب في زيادة العبء المالي على الدول التي تسعى إلى تحقيق الأمن المطلوب للفرد والمجتمع في ظل الاستخدام الواسع للحاسب الآلي وتطبيقاته، والأجهزة الذكية، وما يندرج تحتها من أعمال حفظ المستندات والمصادر الخاصة، مبينين أن قرار إنشاء الهيئة يأتي في إطار اهتمام خادم الحرمين الشريفين الملك سلمان بن عبدالعزيز آل سعود، وسمو ولي عهده الأمين - حفظهما الله - بالتحول للتعاملات الإلكترونية الحكومية في المملكة لما تقدمه من فوائد كبيرة للاقتصاد الوطني، وتأمين هذه التعاملات لينعم الجميع بخدماتها([١٨]).

وأوضح المتخصص في هندسة الحاسب العميد السابق لكلية الحاسب في جامعة الملك سعود البروفيسور سامي بن صالح الوكيل : إن مصطلح الأمن السيبراني أتى من لفظ السيبر المنقول عن كلمة (Cyber) اللاتينية ومعناها " الفضاء

المعلوماتي"، في حين يعني مصطلح الأمن السيبراني "أمن الفضاء المعلوماتي" من كل جوانبه، وهو عبارة عن تعبير شامل عن العالم الافتراضي الذي يحوي كل ما يتعلق باستخدامات وآليات وتطبيقات وتجهيزات تقنية المعلومات والحاسب الآلي، والترابط فيما بينها من خلال شبكات الحاسب والاتصالات والإنترنت. ([١٩])

وأشار إلى أن هذا المصطلح انتشر مع بروز ثورة المعلومات وبدء الاستخدام الواسع لشبكة الإنترنت، وتغلغل وسائل تقنية المعلومات في مناحي الحياة بعالمنا المعاصر، ويعد من أهم جوانب الأمن في الحياة المعاصرة نظرًا لازدياد انتشار استخدام الحاسب وتقنية المعلومات في جميع الأجهزة الحكومية والخاصة، والخدمات التجارية والبنكية، والتعليمية، والصحية، وفي مجال التحكم في نظم الاتصالات والأمن، والقطاعات العسكرية.

وشدّد على أن أمن الحاسب وتقنية المعلومات يعد مطلبًا حيويًا للمحافظة على خصوصية وسلامة تصرفات الأفراد والهيئات، مبينا أنه بدونه ستنهار الثقة في التعامل مع القطاعات التي تقدم خدماتها بالاعتماد على معالجة البيانات والمعلومات، إذ قد يؤدي ذلك لا سمح الله إلى توقف نشاط الفرد أو الهيئة أو إلى حدوث نتائج كارثية يصعب إزالة آثارها لاحقاً، وتكون مكلفة مالياً ومعنوياً([٢٠]).

وبين أن أمن الحاسب وتقنية المعلومات هو أيضاً من الأمور الضرورية في الحياة المعاصرة من منطلق أن ما تختزنه منظومة الحاسب من بيانات ومعلومات هي سلعة تعد ذات قيمة قد لا يقدر فقدها بثمن للفرد أو للهيئة أو المجتمع.

إن الأخطار المعلوماتية تضم أنواعًا متعددة التحديات التي يجب أخذها في الحسبان عند بناء وتطوير تجهيزات وأنظمة المعلوماتية التي تؤثر على خصوصية و سرّية المعلومات(Privacy) ، وتؤثر على وحدة و تجانس المعلومات (Integrity) أو على توفرها عند الطلب لصاحب الصلاحية ومنها : خطر منع الخدمة الذي يمنع استخدام الموارد والبرمجيات والتجهيزات المعلوماتية وتؤدي إلى انهيار النظام ومنع الاستفادة منه، و خطر التسلسل والاختراق Intrusion Attack : الذي ينجم عنه دخول غير المصرح له إلى الأنظمة والموارد المعلوماتية والتحكم بها أو استغلالها للهجوم على موارد وأنظمة أخرى، وخطر سرقة المعلومات الذي يمكن حدوثه بسبب ثغرات في الأنظمة أو التجهيزات أو باستخدام برامج خاصة مما يتيح لغير صاحب الشأن الاطلاع على البيانات المختزنة أو المرسلة وسرقتها أو العبث بها([٢١]).

ومن جهته، وصف أستاذ أمن المعلومات في كلية علوم الحاسب والمعلومات بجامعة الملك سعود البروفيسور خالد بن سليمان الغثبر، قرار إنشاء الهيئة الوطنية للأمن السيبراني تعنى بهذا الموضوع المهم والحساس بالخطوة المباركة التي تترجم عزم

المملكة العربية السعودية بقيادة خادم الحرمين الشريفين الملك سلمان بن عبدالعزيز آل سعود، وسمو ولي العهد - حفظهما الله - على إعطاء أمن المعلومات والخدمات الإلكترونية في المملكة أولوية عالية للتصدي للهجمات الإلكترونية المتكررة خاصةً مع تطور الخدمات الحكومية الإلكترونية وتحول المملكة إلى عصر جديد تقوده رؤية المملكة ٢٠٣٠ التي تمضي قدما في مواكبة التطور التقني والمعلوماتي([٢٢]).

وقال إن ارتباط الهيئة بمقام خادم الحرمين الشريفين الملك سلمان بن عبدالعزيز آل سعود له دلالة على مكانتها واستقلاليتها لتستطيع سن التنظيمات والإجراءات المتعلقة بالأمن السيبراني وتطبيقها على بقية الجهات الحكومية، ومن ثم متابعة تطبيقها للتأكد من تناغم عمل الجهات الحكومية في حماية معلومات وخدمات الوطن.

تقرير / الأمن السيبراني.. حماية وطنية لأمن الفرد والمجتمع في المملكة/ إضافة ثانية واخيرة

وبدوره قال المشرف العام على مركز القيادة والسيطرة للدراسات المتقدمة في جامعة الملك سعود البروفيسور الدكتور عبدالله بن شرف الغامدي، إن قرار إنشاء الهيئة الوطنية للأمن السيبراني أتى في الوقت المناسب للعمل على تحقيق التكامل بين أجهزة الدولة المعنية بذلك المجال مثل : الاتحاد السعودي للأمن الإلكتروني والبرمجيات التابع للهيئة العامة للرياضة، والمركز الوطني للأمن الإلكتروني في وزارة الداخلية، ومركز التميز في جامعة الملك سعود، ومركز الأمن السيبراني في مدينة الملك عبدالعزيز للعلوم والتقنية، بالإضافة إلى مراكز أخرى في وزارة الدفاع والشركات الوطنية الكبرى، وسوف تعمل الهيئة على سن الأنظمة والتشريعات وتوحيد الممارسات في سبيل ضمان تطبيق الأنظمة الحرجة للاتصالات وتقنية المعلومات والحفاظ على سرية وخصوصية وجاهزية وتكامل المعلومات في المملكة العربية السعودية، إلى جانب تأهيل الكوادر المختصة في مجال الأمن السيبراني والمجالات ذات العلاقة.

وأضاف أن الأمن السيبراني سيسهم في صد عمليات الاختراق التي صاحبة انتشار أنظمة المعلومات والاتصالات، مبينًا أن الاختراق وارسال البرمجيات الخبيثة وتعطيل الخدمة ظهر قبل الإنترنت من خلال إرسال الفيروسات التي كانت تحمل عن طريق وحدات التخزين(CD ، USB).
ولفت الغامدي النظر إلى أن التهديد بالاختراق موجود بكثرة منذ بداية الاعتماد الفعلي على أنظمة المعلومات والاتصالات، وليس مقتصرا فقط على البيانات بل يتدعى إلى أنظمة البنية التحتية الحرجة مثل أنظمة شبكات الطاقة، والمياه، ومحطات الكهرباء التي تدار عن بعد من خلال مراكز العمليات والتحكم، مؤكد أن

المملكة من الدول المتقدمة في استخدام الأنظمة الخدمية الإلكترونية ولديها امكانيات متقدمة في مجال حماية أمن المعلومات

واهتمت معظم الجامعات في المملكة بتدريس مواد أمن المعلومات في كليات الحاسب لديها والبعض منها اتجه إلى تخصيص برامج دراسات عليا في ذلك المجال كما في الجامعة السعودية الإلكترونية التي تعتمد على طريقة تعليم إلكترونية تختلف عن التعليم السائد في جميع جامعات المملكة وهو "التعليم الإلكتروني المدمج."

الدراسة الميدانية :

فروض الدراسة :

لتحقيق أهداف الدراسة يتم اختبار الفروض التالية :

١ـ تختلف الأهمية النسبية للمخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية .

٢ـ يؤدي عدم وجود سياسات وبرامج محددة لأمن المعلومات إلى زيادة المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية .

٣ـ تعمل الشركات والمؤسسات السعودية على تطبيق حوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الالكترونية .

٤ـ يوجد اختلاف معنوي في تأثير معايير حوكمة أمن المعلومات بشكل مستقل على الحد من مخاطر نظم المعلومات المحاسبية الالكترونية

مجتمع وعينة الدراسة :

يتكون مجتمع الدراسة من شركات الاتصالات ، وشركات تكنولوجيا المعلومات والبنوك العاملة في المملكة العربية السعودية ، وقد تم اختيار عينة عشوائية لمجتمع الدراسة من تلك الشركات والبنوك بلغ عددها خمس شركات لتكنولوجيا المعلومات بواقع ٨٠ استمارة ، وسبع شركات اتصالات بواقع ١٠٠ استمارة ، وأربعة بنوك بواقع ١٢٠ استمارة ، وقد تم توزيع استمارات الاستبيان داخل تلك الشركات والبنوك على الفئات الآتية :

١ـ المديرين الماليين والمحاسبين باعتبارهم القائمين على التعامل مع نظم المعلومات المحاسبية الالكترونية .

٢ـ الموظفين في إدارة تكنولوجيا المعلومات من متخصصين ومراجعي نظم المعلومات الالكترونية ومديري الإدارات .

٣ـ المراجعين الخارجين الذين يقومون بمراجعة أنظمة تلك الشركات والبنوك .

ويمكن توضيح التوزيع النسبي لمفردات العينة من خلال الجدول التالي :

جدول رقم (١)

التوزيع النسبي لاستمارات الاستقصاء على مفردات العينة

مفردات العينة	العدد	النسبة
شركات تكنولوجيا المعلومات	٨٠	%٢٧
شركات الاتصالات	١٠٠	%٣٣
البنوك	١٢٠	%٤٠
الإجمالي	٣٠٠	%١٠٠

<u>إدخال ومعالجة البيانات :</u>

قام الباحث بمراجعة استمارات الاستبيان للتأكد من اكتمالها وصلاحيتها لإدخال البيانات والتحليل الإحصائي ، وتم استبعاد الاستمارات التي لا تتوافر فيها الشروط اللازمة ، ويوضح الجدول التالي عينة الدراسة ومعدلات الإجابة الصحيحة القابلة للتحليل من بين مفردات العينة .

جدول رقم ٢

عدد الاستمارات المرسلة ، والواردة والمستبعدة والصحيحة

مفردات العينة	المرسل	الوارد		المستبعد		الصحيح	
		العدد	النسبة	العدد	النسبة	العدد	النسبة
شركات تكنولوجيا المعلومات	٨٠	٦٧	%٨٤	١٧	%٢١	٥٠	%٦٣
شركات الاتصالات	١٠٠	٧٨	%٧٨	٢٠	%٢٠	٥٨	%٥٨
البنوك	١٢٠	٩٨	%٨٢	٩	%٧,٥	٨٩	%٧٤
الإجمالي	٣٠٠	٢٤٣	%٨١	٤٦	%١٥	١٩٧	%٦٦

أساليب التحليل الإحصائي للبيانات :

قام الباحث بتفريغ الإجابات على الأسئلة بجداول البيانات ، وتم تحليلها بهدف تحديد مدى تحقق فروض الدراسة واستخلاص النتائج من خلال تطبيق بعض الأساليب الإحصائية الواردة بمجموعة البرامج الإحصائية للعلوم الاجتماعية (spss) وتحديد تم الاستعانة بالأساليب التالية :

أساليب الإحصاء الوصفي :

١ـ الوسط الحسابي .

٢ـ الانحراف المعياري .

٣ـ التكرار والنسبة .

أساليب الإحصاء الاستدلالي :

١ـ اختبار المصداقية والاعتمادية .

٢ـ اختبار " ت " .

٣ـ اختبار فريدمان .

٤ـ اختبار كروسكال والاس .

٥ـ اختبار " كا ٢ " .

نتائج الاختبارات الإحصائية لفروض الدراسة :

اختبار الثبات والصدق :

ويطلق عليه معامل ثبات ألفا ، وهو مقياس يوضح مدى الاعتماد على نتائج قائمة الاستقصاء ، ومدى إمكانية تعميم النتائج على مجتمع الدراسة ، وكذلك يوضح ثبات المحتوى لمتغيرات الدراسة .

وقد بلغت قيمة معامل الثبات للاستمارة ككل ٠,٩٨٥ ، ومعامل الصدق وهو الجذر التربيعي لمعامل الثبات ٠,٩٩١ مما يدل على ثبات أداة البحث ووجود درجة كبيرة من الاتساق الداخلي بين عبارات قائمة الاستقصاء ككل .

نتائج اختبار الفرض الأول :

ينص الفرض الأول على :

" تختلف الأهمية النسبية للمخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية " .

أولا : التحليل الوصفي :

تم استخدام تحليل التباين لتوصيف آراء العينة حول المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية من خلال المقاييس الإحصائية (الوسط الحسابي ، واختبار " ت " ، الانحراف المعياري) ، وذلك كما يوضحه الجدول رقم (٣) فيما يلي :

جدول (٣)

توصيف الآراء من خلال المقاييس الإحصائية حول المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية

السؤال	العدد	الوسط الحسابي	الانحراف المعياري	T.Test
١ـ إدخال غير متعمد لبيانات غير سليمة بواسطة الموظفين	١٩٧	٤,٢٩	١,٠٩	** ٠,٠٠
٢ـ إدخال متعمد لبيانات غير سليمة بواسطة الموظفين	١٩٧	٢,٨٨	٠,٩٣	** ٠,٠٠
٣ـ تدمير غير متعمد لبيانات بواسطة الموظفين	١٩٧	٤,٢١	١,١٦	** ٠,٠٠
٤ـ تدمير متعمد لبيانات بواسطة الموظفين	١٩٧	٢,٩٤	٠,٩٨	** ٠,٠٠
٥ـ دخول غير المصرح به للبيانات بواسطة الموظفين	١٦٩	٤,٢٠	١,١٦	** ٠,٠٠
٦ـ تبادل الموظفين لكلمات المرور	١٩٧	٤,٠٨	١,٢٢	** ٠,٠٠
٧ـ إدخال فيروسات الحاسب إلى النظام المحاسبي	١٩٧	٤,٢١	١,٢٤	** ٠,٠٠
٨ـ تدمير أو سرقة بعض المعلومات	١٩٧	٤,٠٨	١,٢٤	** ٠,٠٠

٩ـ عمل نسخ غير مصرح به من مخرجات النظام	١٩٧	٤,٢٨	١,١٦	** ٠,٠٠
١٠ـ عرض بيانات سرية على شاشات العرض	١٩٧	٤,١٦	١,١٠	** ٠,٠٠
١١ـ كوارث طبيعية مثل الحرائق أو انقطاع الطاقة	١٩٧	٤,١٦	١,١٩	** ٠,٠٠
١٢ـ مخاطر خارجية متمثلة في البرامج الخبيثة والاختراقات ... وغيرها	١٩٧	٤,٤٠	١,٠٤	** ٠,٠٠
الإجمالي	١٩٧	٤	١,١٣	

** دال إحصائيًا عند مستوى معنوية ٠,٠٥

ويتضح من الجدول السابق أن الوسط الحسابي العام يميل إلى الموافقة على أن العناصر التي تم ذكرها تمثل المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية ، وذلك بوسط حسابي عام قيمته (٤) ـ وانحراف معياري عام (١,١٣) .

ومن ثم يشير الانحراف المعياري إلى انخفاض التشتت أي يوجد تجانس في الآراء حول تلك المخاطر ، كما يشير اختبار " ت " إلى أن النتائج أقل من مستوى معنوية (٠,٠٥) بمعنى أن الفروق معنوية وجميع العناصر ـ بصفة عامة ـ تعتبر من المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية .

ثانيًا : اختبار فريدمان :

يوضح هذا الاختبار الأهمية النسبية للعبارات أي معرفة العنصر الأكثر أهمية من وجهة نظر مفردات العينة بشأن المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية ، وذلك من خلال متوسط الرتب حيث يأخذ العنصر الأكثر أهمية من وجهة نظر مفردات العينة أعلى متوسط للرتب ويتضح ذلك من خلال الجدول التالي :

جدول رقم (٤)

ترتيب الأهمية النسبية للمخاطر التي تتعرض لها

نظم المعلومات المحاسبية الالكترونية

السؤال	متوسط الرتب	مستوى العينة
١ــ مخاطر خارجية متمثلة في البرامج الخبيثة والاختراقات ... وغيرها	٨,٢٥	٠,٠٠**
٢ـ إدخال غير متعمد لبيانات غير سليمة بواسطة الموظفين	٧,٧٤	
٣ـ عمل نسخ غير مصرح بها من مخرجات النظام	٧,٥٧	
٤ـ إدخال فيروسات الحاسب إلى النظام المحاسبي	٧,٤٠	
٥ـ تدمير متعمد لبيانات بواسطة الموظفين	٧,٣٩	
٦ـ دخول غير المصرح به للبيانات بواسطة الموظفين	٧,٢٨	
٧ـ كوارث طبيعية مثل الحرائق أو انقطاع الطاقة	٧,١٠	
٨ـ عرض بيانات سرية على شاشات العرض	٧,٠٢	
٩ـ تدمير أو سرقة بعض المعلومات	٦,٦٩	
١٠ـ تبادل الموظفين لكلمات المرور	٦,٦٧	
١١ـ تدمير متعمد للبيانات بواسطة الموظفين	٢,٥٢	
١٢ــ إدخال متعمد لبيانات غير سليمة بواسطة الموظفين	٢,٣٥	

** دال إحصائيا عند مستوى معنوية ٠,٠٥

ويتضح من الجدول السابق ما يلي :

١ـ أن مستوى المعنوية أقل من (٠,٠٥) مما يدل على وجود اختلاف معنوي في الأهمية النسبية من وجهة نظر مفردات العينة حول مخاطر نظم المعلومات المحاسبية الالكترونية .

٢ـ أن أعلى متوسط للرتب يتمثل في أن المخاطر الخارجية المتمثلة في البرامج الخبيثة والاختراقات و.... غيرها تعد من أهم المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية ، بينما يتمثل كل من التدمير المتعمد للبيانات والإدخال المتعمد لبيانات غير سليمة من أقل المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية حيث أنها تأخذ أقل مستوى للرتب .

ثالثًا : اختبار كروسكال والاس :

ويتم إجراء هذا الاختبار لقياس التباين ـ الاتفاق والاختلاف ـ في آراء مفردات العينة حول المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية ، ويتضح ذلك من خلال الجدول التالي :

جدول رقم (٥)

قياس التباين في آراء مفردات العينة حول مخاطر

نظم المعلومات المحاسبية الالكترونية

البيان	مفردات العينة	العدد	متوسط الرتب	مستوى المعنوية
مخاطر أمن نظم المعلومات المحاسبية الالكترونية	شركات تكنولوجيا المعلومات	٥٠	٩٨,٠١	٠,٤٩١
	شركات الاتصالات	٥٨	٩١,٨٦	
	البنوك	٨٩	١٠٣,١٠	

ويتضح من الجدول السابق أن مستوى المعنوية للعناصر الممثلة لمخاطر نظم المعلومات المحاسبية الالكترونية مجتمعة أكبر من (٠,٠٥) مما يعني وجود اتفاق في آراء مفردات العينة حول اختلاف الأهمية النسبية للمخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية .

وبناءً على نتائج التحليل السابق فقد ثبت صحة الفرض الأول للدراسة والذي ينص على : **" تختلف الأهمية النسبية للمخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية "** .

نتائج اختبار الفرض الثاني :

ينص الفرض الثاني للدراسة على : " يؤدي عدم وجود سياسات وبرامج محددة لأمن المعلومات إلى زيادة المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية " .

أولا : التحليل الوصفي :

يوضح الجدول التالي توصيف آراء العينة بشأن أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية من خلال المقاييس الإحصائية الوسط الحسابي والانحراف المعياري واختبار " ت " :

جدول رقم (٦)

توصيف الآراء حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية

السؤال	العدد	الوسط الحسابي	الانحراف المعياري	T.Test
١ــ عدم توافر الخبرة اللازمة والتدريب الكافي للموظفين	١٩٧	١,٢٢	١,٢٢	٠,٠٠**
٢ـ عدم توافر الحماية الكافية ضد مخاطر الفيروسات	١٩٧	٤,٠٥	١,٢٢	٠,٠٠**
٣ــ عدم تحديد المسئوليات والصلاحيات لكل فرد داخل الهيكل التنظيمي	١٩٧	٤,٢٠	١,١٥	٠,٠٠**
٤ــ عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات	١٩٧	٤,٢٨	١,١٤	٠,٠٠**
٥ـ عدم تطبيق مبادئ ومعايير حوكمة أمن المعلومات	١٩٧	٤,٢٠	١,١٥	٠,٠٠**
الإجمالي	١٩٧	٤,١٩	١,١٩	

** دال إحصائيًا عند مستوى معنوية (٠,٠٥) .

ويلاحظ من الجدول السابق أن الوسط الحسابي العام يميل إلى الموافقة حول أسباب المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية ، وذلك بوسط حسابي عام (٤,١٩) ، وانحراف معياري (١,١٩) ، مما يشير إلى انخفاض التشتت أي يوجد تجانس في الآراء بشأن تلك الأسباب ، كما يشير اختبار " ت " إلى أن النتائج أقل من مستوى معنوية (٠,٠٥) بمعنى أن الفروق معنوية وجميع العناصر تعتبر من ضمن الأسباب التي تؤدي إلى زيادة مخاطر نظم المعلومات المحاسبية .

ثانيًا : اختبار فريدمان :

يوضح الجدول التالي قياس وترتيب الأهمية النسبية لأسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية :

جدول رقم (٧)

ترتيب الأهمية النسبية حول أسباب حدوث مخاطر

نظم المعلومات المحاسبية الالكترونية

السؤال	متوسط الرتب	مستوى العينة
١ـ عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات	٣,٢٠	٠,٠٠**
٢ـ عدم توافر الخبرة اللازمة والتدريب الكافي للموظفين	٣,٠٤	
٣ـ عدم تحديد المسئوليات والصلاحيات لكل فرد داخل الهيكل التنظيمي	٣,٠١	
٤ـ عدم تطبيق مبادئ ومعايير حوكمة أمن المعلومات .	٢,٩٨	
٥ـ عدم توافر الحماية الكافية ضد مخاطر الفيروسات	٢,٧٧	

** دال إحصائيًا عند مستوى معنوية (٠,٠٥) .

ويتضح من الجدول السابق ما يلي :

١ـ أن مستوى المعنوية أقل من (٠,٠٥) مما يدل على وجود اختلاف معنوي في الأهمية النسبية من وجهة نظر مفردات العينة بشأن أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية .

٢ـ أن أعلى متوسط للرتب يتمثل في أن عدم وجود سياسات وبرامج محددة لأمن نظم المعلومات يُعد من أهم أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية ، بينما يتمثل أقل متوسط للرتب في عدم توافر الحماية الكافية ضد مخاطر الفيروسات .

ثالثًا : اختبار كروسكال والاس :

يوضح الجدول التالي قياس التباين في آراء مفردات العينة حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية

جدول رقم (٥)

قياس التباين في آراء مفردات العينة حول أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية

البيان	مفردات العينة	العدد	متوسط الرتب	مستوى المعنوية
أسباب حدوث مخاطر أمن نظم المعلومات المحاسبية الالكترونية	شركات تكنولوجيا المعلومات	٥٠	١٠٨,١٦	٠,٤٩١
	شركات الاتصالات	٥٨	٩٨,٩٤	
	البنوك	٨٩	٩٣,٨٩	

ويتضح من الجدول السابق أن مستوى المعنوية لأسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية أكبر من (٠,٠٥) مما يعني وجود اتفاق في آراء مفردات العينة حول اختلاف أسباب حدوث مخاطر نظم المعلومات المحاسبية الالكترونية .

وبناء على نتائج التحليل السابق يتضح ثبوت صحة الفرض الثاني للدراسة والذي ينص على : **" يؤدي عدم وجود سياسات وبرامج محددة لأمن المعلومات إلى زيادة المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية "** .

نتائج اختبار الفرض الثالث :

ينص الفرض الثالث للدراسة على : " تعمل المؤسسات والهيئات السعودية على تطبيق حوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الالكترونية " .

جدول رقم (٩)

التوزيع التكرار والنسبي ، واختبار كا٢ ، واختبار كروسكال والاس حول مدى قيام العينة بتطبيق حوكمة أمن المعلومات

البيان	التكرار	النسبة	اختبار كا٢		اختبار كروسكال والاس		
			مستوى المعنوية	الدلالة الإحصائية	مفردات العينة	متوسط الرتب	مستوى المعنوية
لا	١٤٣	٧٢,٦			شركات تكنولوجيا المعلومات	١٠١,٦٩	
نعم	٥٤	٢٧,٤	٠,٠٠**	معنوي	شركات الاتصالات	٩٩,٢٥	٠,٤٦**
الإجمالي	١٩٧	١٠٠			البنوك	٩٥,٤٤	

** دال إحصائيًا عند مستوى معنوية (٠,٠٥) .

ويتضح من الجدول السابق أن أكثر مفردات العينة لا تقوم بتطبيق حوكمة أمن المعلومات ضمن إستراتيجيتها للحد من مخاطر نظم المعلومات المحاسبية الالكترونية وذلك بنسبة ٧٢,٦% من إجمالي حجم العينة ، عند مستوى معنوية أقل من (٠,٠٥) ، مما يدل على وجود فروق ذات دلالة إحصائية في آراء مفردات العينة ، كما تبين من اختبار " كروسكال والاس " أن مستوى المعنوية أكبر من (٠,٠٥) الأمر الذي يدل على وجود اتفاق بين آراء مفردات العينة بشأن عدم تطبيق الجهات التي يعملون بها لحوكمة المعلومات .

والجدول التالي يوضح التوزيع التكرار والنسبي ، واختبار كا٢ واختبار " كروسكال والاس " بشأن قيام عينة الدراسة بتطبيق معايير دولية خاصة بأمن المعلومات .

جدول رقم (١٠)

التوزيع التكرار والنسبي كا٢ واختبار " كروسكال والاس " حول مدى قيام عينة الدراسة بتطبيق معايير دولية خاصة بأمن المعلومات

البيان	التكرار	النسبة	اختبار كا٢		اختبار كروسكال والاس		
			مستوى المعنوية	الدلالة الإحصائية	مفردات العينة	متوسط الرتب	مستوى المعنوية
لا	٩٤	٤٧,٧			شركات تكنولوجيا المعلومات	٩٦,٧٥	
نعم	١٠٣	٥٢,٣	٠,٠٠**	معنوي	شركات الاتصالات	١٠٠,١٥	٠,٩٣**
الإجمالي	١٩٧	١٠٠			البنوك	٩٩,٥٢	

ويتضح من الجدول السابق أن نسبة ٥٢,٣% من إجمالي حجم العينة تقوم بتطبيق معايير دولية خاصة بأمن المعلومات (الأمن السيبراني) ، وذلك عند مستوى معنوية أقل من (٠,٠٥) ، مما يدل على وجود فروق ذات دلالة إحصائية في آراء مفردات العينة ، كما يتضح من نتائج اختبار " كروسكال والاس " أن مستوى المعنوية أكبر من (٠,٠٥) مما يدل على وجود اتفاق بين آراء مفردات العينة بشأن تطبيق معايير دولية خاصة لأمن المعلومات (الأمن السيبراني) .

ومن ثم يتضح للباحث ثبوت خطأ الفرد الثالث للدراسة والذي ينص على : **" تعمل المؤسسات والهيئات السعودية على تطبيق حوكمة أمن المعلومات في الحد من مخاطر نظم المعلومات المحاسبية الالكترونية "** .

النتائج والتوصيات :

نتائج الدراسة النظرية :

١ـ تتعدد صور المخاطر التي تتعرض لها نظم المعلومات المحاسبية الالكترونية ما بين مخاطر داخلية ومخاطر خارجية ، وتعتبر المخاطر الداخلية من أكثر المخاطر تهديدًا لنظم المعلومات المحاسبية .

٢ـ تتمثل أسباب حدوث تلك المخاطر في : نقص تدريب الموظفين على استخدام وحماية نظم المعلومات ، وسوء اختيارهم ، وعدم وجود ضوابط وإجراءات كافية تعمل على معالجة والوقاية من حدوث هذه المخطر .

٣ـ لا تكفي الحلول الالكترونية بمفردها في مواجهة المخاطر المختلفة التي تتعرض لها نظم المعلومات المحاسبية الالكترونية ، ومن ثم يجب على الشركات اتباع منهج متكامل لإدارة أمن المعلومات (الأمن السيبراني) بحيث يقوم على تقييم التكنولوجيا المستخدمة وتقييم سلوكيات الأفراد والاهتمام بالجوانب التنظيمية حتى يسهل التنبؤ بالمخاطر وإحباط أي محاولة للقيام بها .

نتائج الدراسة الميدانية:

في ضوء استخدام الأساليب الإحصائية (الوصفية والاستدلالية) تم التوصل إلى النتائج التالية:

١- يوجد اتفاق معنوى وتجانس في الآراء بين مفردات عينة الدراسة بشأن تعدد المخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية، وتعد المخاطر الخارجية متمثلة في البرامج الخبيثة والاختراقات و... غيرها من أكثر المخاطر أهمية (أكثرها تكرارا)، بينما يعد التدمير المتعمد للبيانات والإدخال المتعمد لبيانات غير صحيحة من أقل المخاطر أهمية (أقلها تكرارا).

٢- يود اتفاق في آراء مفردات العينة بشأن اختلاف الأهمية النسبة للمخاطر التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية.

٣- يوجد اتفاق في آراء مفردات العينة حول تعدد أسباب حدوث مخاطر نظم المعلومات المحاسبية الإلكترونية، ويعد عدم وجود سياسات وبرامج محددة لأمن المعلومات من أهم تلك الأسباب.

٤- يقوم عدد كبير من مفردات العينة بتطبيق المعايير الدولية لحوكمة أمن المعلومات بصورة منفردة، إلا أنها لا تعمل على تطبيق حوكمة أمن المعلومات - ضمن استراتيجية الشركة - للحد من مخاطر نظم المعلومات المحاسبية الإلكترونية، على الرغم من إدراك مفردات العينة لأهمية تطبيق حوكمة أمن المعلومات والفوائد المتحققة منها.

التوصيات:

في إطار ما جاء بالجزء النظري، وما أكدته الدراسة الميدانية فيمكن للباحثين تقديم التوصيات التالية:

١- زيادة الاهتمام بتوعية المنظمات المصرية بأهمية استخدام مبادئ ومعايير حوكمة أمن المعلومات حتى يتسنى لها مواجهة التحديات والمخاطر التي تواجه بيئة تكنولوجيا المعلومات.

٢- الاهتمام بإعداد دورات تدريبية خاصة بتكنولوجيا المعلومات للإلمام بالتطورات الحديثة في هذا المجال، والتعرف على الجرائم المحتملة المرتبطة بها وكيفية مواجهتها ولمتابعة التطورات المتلاحقة في مجال المعايير الدولية لأمن المعلومات.

٣- قيام الهيئة العامة للرقابة المالية بإلزام الشركات بتطبيق المعايير الدولية الخاصة بحوكمة أمن المعلومات داخل الشركات حتى تزيد درجة الثقة والمصداقية في المعلومات والبيانات التي تقوم تلك الشركات بالإفصاح عنها عبر الموقع الإلكتروني لها.

٤- قيام وزارة الاستثمار - مركز المديرين - بإعداد دليل قواعد ومعايير حوكمة أمن المعلومات" كمرفقات الدليل قواعد ومعايير حوكمة الشركات" حتى يتسنى للشركات المصرية معرفة أهمية حوكمة أمن المعلومات وخطورة عدم تنفيذها.

الخاتمة :

تعتمد المجتمعات الحديثة بشكل متنامي على تكنولوجيات الاتصالات والمعلومات المتصلة بالشبكة العالمية. غير أن هذا الاعتماد المطرد ترافقه مجموعة من المخاطر الناشئة والمحتملة التي تهدد وبشكل أساسي الشبكة وأمن المعلومات والمجتمع المعلوماتي وأعضائه. إن سوء الاستغلال المتنامي للشبكات الالكترونية لأهداف إجرامية يؤثر سلباً على سلامة البنى التحتية للمعلومات الوطنية الحساسة لا سيما على المعلومات الشخصية وأمن الأطفال .

فان الأمن السيبراني يشكل مجموع الأطر القانونية والتنظيمية، الهياكل التنظيمية، إجراءات سير العمل بالإضافة إلى الوسائل التقنية والتكنولوجية والتي تمثل الجهود المشتركة للقطاعين الخاص والعام، المحلية والدولية والتي تهدف إلى حماية الفضاء السيبراني الوطني، مع التركيز على ضمان توافر أنظمة المعلومات وتمتين الخصوصية وحماية سرية المعلومات الشخصية واتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني .

تبيّن توصيات الاتحاد الدولي للاتصالات وأفضل الممارسات الدولية أن الأمن السيبراني يعتمد على مزيج مركب من التحديات التقنية، السياسية، الاجتماعية والثقافية .

وبشكل أدق فإن صلاحية الأمن السيبراني الوطني تعتمد على **الركائز الخمسة** التالية:

١. تطوير إستراتجية وطنية للأمن السيبراني وحماية البنية التحتية للمعلومات الحساسة
٢. إنشاء تعاون وطني بين الحكومة ومجتمع صناعة الاتصالات والمعلومات
٣. ردع الجريمة السيبرانية
٤. خلق قدرات وطنية لإدارة حوادث الحاسب الآلي
٥. تحفيز ثقافة وطنية للأمن السيبراني

أن نقطة انطلاق الأمن السيبراني الوطني تبدأ بتطوير سياسة وطنية لرفع الوعي حول قضايا الامن السيبراني والحاجة لإجراءات وطنية والى التعاون الدولي. أما الخطوة الثانية فتتمثل بتطوير المخطط الوطني لتحفيز الأمن السيبراني بهدف تقليص مخاطر وأثار التهديدات السيبرانية وتتضمن المشاركة في الجهود الدولية والإقليمية لتحفيز الوقاية الوطنية من، و التحضير لـ، والاستجابة إلى و التعافي من الحوادث السيبرانية .

المراجع :

(١) سماح عبد الصبور ، الصراع السيبراني .. طبيعة المفهوم وملامح الفاعلين ، مجلة السياسة الدولة ، مؤسسة الأهرام ، ٢٠١٧ ، ص١٧ .

(٢) أنور ماجد عشقي ، الأمن السيبراني والقمة الخليجية الأمريكية ، الأمن والحياة ، جامعة نايف العربية للعلوم الأمنية ، ٢٠١٦ ، ص٢٦ .

(٣) مراد ماشوش ، الجهود الدولية لمكافحة الإجرام السيبراني ، جامعة الحسن الأول - كلية العلوم القانونية والاقتصادية والاجتماعية - مختبر البحث قانون الأعمال ، ٢٠١٨ ، ص٥٠ .

(٤) محمد بن أحمد بن علي المقصودي ، الجرائم المعلوماتية : خصائصها وكيفية مواجهتها قانونياً ، المجلة العربية للدراسات الأمنية ، مج٣٣، ع٧٠ ، جامعة نايف العربية للعلوم الأمنية ، ٢٠١٧ ، ص١٣ .

(٥)جوهر الجمّوسي ، الافتراضي والثورة: مكانة الإنترنت في نشأة مجتمع مدني عربي ، المركز العربي للأبحاث ودراسة السياسات ، بيروت ، ٢٠١٦ ، ص١٢٠ .

(٦) محمد الأمين البشري : التحقيق في جرائم الحاسب الآلي ، بحث مقدم إلى مؤتمر القانون والكمبيوتر و الانترنت المنعقد الفترة من ١-٣ مايو ، بكلية الشريعة والقانون بدولة الإمارات ٢٠٠٠ ، ص٣٩ .

(٧) المستشار عبد الفتاح بيومي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت ، مصر ، المحلة الكبرى ، دار الكتب القانونية ، ٢٠٠٧ ، ص١٩٨ .

(٨) هلالي عبد اللاه احمد : اتفاقية بودابست لمكافحة الجرائم المعلوماتية (معلقاً عليها) ، دار النهضة العربية ، الطبعة الأولى ، القاهرة ، ٢٠٠٧ ، ص١٢٩ .

(٩) هلالي عبد اللاه احمد مرجع سابق ، ص١٣٥ .

(١٠) المستشار عبد الفتاح بيومي ، مرجع سابق ، ص٩٨ .

(١١) حسن طاهر داوود : جرائم نظم المعلومات ، أكاديمية نايف العربية للعلوم الأمنية ، الطبعة الأولى ، الرياض ، ٢٠٠٠ ، ص١٨٠ .

)١٢(http://arabcb.org/initiative/٧٣٣

(١٣) حسن طاهر داود ، مرجع سابق ، ص١٩٢ .

(١٤) فؤاد الصلاحي ، الأمن السيراني ، مجلة الدوحة ، وزارة الإعلام ، ٢٠١٥ ، ص١٢٩ .

(١٥) محمد الأمين البشري ، مرجع سابق ، ص٩٠ .

(١٦) محمد الأمين البشري ، مرجع سابق ، ص٣٠٠ .

(١٧) محمد العريان ، مرجع سابق ، ص١٨٠ .

(١٨) محمد الأمين البشري ، مرجع سابق ، ص٢٠٧ .

(١٩) نفس المصدر .

(٢٠) محمد محمد الألفي ، مرجع سابق ، ص١٩ .

(٢١) مدحت رمضان ، مرجع سابق ، ص١٨٠ .

(٢٢) محمد محمد الألفي ، مرجع سابق ، ص١٩٢ .