المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الخامس - الإصدار التاسع والأربعون
تأريخ النشر: 20 نوفمبر 2023 م

الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول (دراسة نظرية تحليلية)

Cybersecurity in the Kingdom of Saudi Arabia between Reality and Hope (Analytical Theoretical Study)

إعداد: الدكتورة/ ندى بنت خالد المرداس

دكتوراه في إدارة الأعمال، كلية إدارة الأعمال، جامعة لينكولن، ماليزيا

Email: Nadak.M@icloud.com

ملخص الدراسة:

يهدف البحث إلى التعرف على الأمن السيبراني في المملكة العربية السعودية بهدف إلقاء الضوء على الوضع الواقعي الحالي والوضع المأمول مستقبلا. تكمن أهمية الدراسة في كونها تتناول مجالا مهماً، وهو الأمن السيبراني والمتمثل في الحفاظ على سرية وأمن المعلومات والذي قد يعرض العديد من القطاعات للأزمات، لاسيما في ظل الظروف الاقتصادية والسياسية المالية الصعبة. تلخصت مشكلة البحث في الإجابة على السؤال الرئيسي التالي: ما هو واقع الأمن السيبراني في المملكة العربية السعودية وما هو الوضع المأمول مستقبلا؟، اعتمدت الباحثة على استخدام المنهج الوصفي القائم على مراجعة عدد من الأدبيات السابقة، حيث تم شرح مفهوم أمن المعلومات والأمن السيبراني من حيث الأهمية والخصائص والأساليب، ومن ثم إلقاء الضوء على دور المملكة في مكافحة جرائم الأمن السيبراني.

توصلت الدراسة الى عدد من النتائج كان من أهمها: إن التحدي الحالي للدول هو مواجهة الجريمة الإلكترونية العابرة للقارات، لتفادي أي آثار قد تسببها، وبالتالي تحقيق الأمن السيبراني، من خلال مختلف الاتفاقيات الدولية أو الإقليمية في هذا المجال. كما تسعى جهود الدول إلى توحيد الرؤى لمواجهة هذه الجريمة أو الإرهاب السيبراني، وخلق آليات تساعد في التحقيق والمتابعة القانونية للمجرمين الإلكترونيين.

أوصت الدراسة بعدة توصيات أهمها: نشر ثقافة الأمن السيبراني بين العاملين داخل المنظمات وبين جميع أفراد المجتمع بشكل عام، وأهمية توفير البنية التحتية لمشروع الأمن السيبراني داخل الدولة، وتوفير الكوادر البشرية المؤهلة والمدربة من أجل تطبيق ناجح للأمن السيبراني، وتمكين المرأة بالمشاركة والعمل في مجالات الأمن السيبراني، وتطوير أفضل الممارسات والسياسات والبرامج لحماية الأطفال في العالم السيبراني لمواجهة التهديدات السيبرانية المتزايدة التي تستهدف الأطفال أثناء استخدامهم لشبكة الإنترنت وتعريضهم لجرائم سيبرانية متنوعة بعيداً عن أعين أسرهم.

الكلمات المفتاحية: الأمن السيبراني، أمن المعلومات، الإرهاب السيبراني، الجريمة الإلكترونية، المملكة العربية السعودية.

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الخامس - الإصدار التاسع والأربعون
تأريخ النشر: 20 نوفمبر 2023 م

Cybersecurity in the Kingdom of Saudi Arabia between Reality and Hope (Analytical Theoretical Study)

Abstract

The current research aims to identify cybersecurity in the Kingdom of Saudi Arabia with the aim of shedding light on the current realistic situation and the hoped-for future situation. The importance of this study lies in the fact that it addresses an important field, which is cybersecurity in the Kingdom, which is represented in maintaining the confidentiality and security of information, which may expose many sectors to crises, especially in light of the difficult economic, political, and financial conditions. The research problem was summarized by answering the following main question: What is the reality of cybersecurity in the Kingdom of Saudi Arabia and what is the desired situation in the future? The researcher relied on the use of a descriptive approach based on a review of a number of previous literatures, where the concept of information security and cybersecurity was explained. In terms of importance, characteristics, methods and objectives, clarifying the pros and cons, and then shedding light on the role of the Kingdom of Saudi Arabia in combating cybersecurity crimes.

The researcher reached a number of results, the most important of which were: The current challenge for countries is to confront transcontinental cybercrime, to avoid any effects it may cause, and thus achieve cybersecurity, through various international or regional agreements in this field. Countries' efforts also seek to unify visions to confront cybercrime and cyberterrorism, and create mechanisms that assist in the investigation and legal follow-up of cybercriminals.

The study recommended several recommendations, the most important of which are: spreading the culture of cybersecurity among workers within organizations and among all members of society in general, the importance of providing the infrastructure for a cybersecurity project within the country, and providing qualified and trained human cadres for a successful application of cybersecurity, in addition to providing regulations and legislation governing the application. Cyber security.

Keywords: Cyber Security, Information Security, Cyber Terrorism, Cybercrime, Kingdom of Saudi Arabia.

1. المقدمة:

واجهت منظمات الأعمال العديد من التحديات المرتبطة بازدياد المنافسة في جميع المجالات والتي كان من أهم أسباب ظهور هذه التحديات ما يسمى بالعولمة والتطور التكنولوجي اللذين ساهما بدورهما في إزالة الحواجز والحدود بين منظمات الأعمال من جهة والعملاء من جهة أخرى. إذ أصبحت الحدود بين الدول أخر ما يعيق المنظمة في تحقيق أهدافها في الانتشار حول العالم.

وبسبب الدور الكبير للتقدم التقني ودخوله في مختلف مجالات الحياة سواءً العلمية أو الإدارية أو المالية أو العسكرية، وانتشار رقعة عمل المنظومات الحاسوبية بحيث أصبحت لا تقتصر على منطقة جغرافية محددة بل تشمل الكرة الأرضية بأسرها، فقد أدى كل ذلك إلى نشوء مخاطر حقيقية ناجمة عن محاولة الدخول غير المشروع إلى البيانات المعالجة والمخزنة في الحواسيب والمنقولة فيما بينها، وذلك بغية الحصول على هذه المعلومات لأغراض مختلفة أو محاولة تغييرها أو تدميرها. وانطلاقاً من ذلك نشأت أفكار مختلفة في البداية تسعى إلى حماية هذه المعلومات، وقد تطورت هذه الأفكار بشكل متسارع نتيجة لتعاظم وتسارع المخاطر لتشكل علماً قائماً بحد ذاته هو علم حماية المعطيات، حيث يعتمد هذا العلم على أسس ومبادئ واضحة، كما أنه يملك أدوات مختلفة لتحقيقه، بحيث تعتبر التعمية إحدى أهم الأدوات المستخدمة (الناظر وسائد محمود، 2005).

ان عصر المعلومات الذي نعيشه الآن هو عصر أصبحت المعلومات فيه هي المقياس الذي نقيس به قوة المنظمة. فمن يمتلك المعلومات في هذا العصر يستطيع أن يسيطر، وهناك من يصنف المعلومات كسلاح جديد قد يفصل بين النصر والهزيمة، فمن يعلم سوف ينتصر حتى لو لم يكن الأقوى، ومن لا يعلم سوف ينهزم حتى لو كان هو الأقوى (داود، 2000).

وقد وجد استخدام اصطلاح أمن المعلومات في نطاق أنشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال، إذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات - وتحديدا الإنترنت - احتلت أبحاث ودراسات أمن المعلومات مساحة واسعة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات (الخالد وأمان، 2008).

ان الثورة التكنولوجية وصفت بأنها أعظم ظاهره، جعلت من التكنولوجيا ونظم المعلومات عنصرين من عناصر النجاح في عالم يتجه نحو العولمة والسرعة في تبادل المعلومات، حيث إننا اليوم في عالم يتحدث عن عنصر المعلومات وعن الجيل الرابع من تكنولوجيا المعلومات، لذلك فإن الاتجاه يسير نحو تطوير علاقة المنظمة بالسوق من أجل الحصول على فرص جديده تعتمد على الاستخدام الأمثل للمعلومات المتاحة عن الموردين والعملاء والمنافسين وكل ذوي العلاقة بالمنظمة ، الأمر الذي يضفي صفة الاستراتيجية على نظم المعلومات كأداة قادره على خلق وتعظيم القدرة التنافسية وتحقيق الأهداف (بحيصي وعصام، 2006).

لقد أدى الاستخدام السيئ لمختلف الوسائل التكنولوجية والتقنيات الحديثة من حواسيب وأجهزة هواتف ذكية، وكذا شبكة الانترنت إلى تنامي وتزايد الجريمة الإلكترونية، هذه الأخيرة والتي تتميز بمجموعة من الخصائص التي تميزها عن الجرائم التقليدية، من بينها أنها عابرة للحدود والقارات، تطلب ذلك ضرورة إيجاد آليات وحلول على المستوى المحلي والدولي، فالتعاون الدولي أصبح أكثر من ضرورة لمجابهة الجريمة الإلكترونية، وتفادي أو التقليل من آثارها.

وعندما بدأت أجهزة الحاسب بمختلف أنواعها والأجهزة المحمولة باحتواء معلومات مهمة، بدأ القلق على أمن هذه المعلومات والأجهزة التي تعالجها وتخزنها وتنقلها، فتم التفكير في حماية هذه الأجهزة وحماية المعلومات الموجودة بها. وعندما ارتبطت أجهزة الحاسب بشبكة الإنترنت واعتمد الناس على الإنترنت في أعمالهم، وتنمية تجارتهم، واستخدموها في التعليم، والتواصل الاجتماعي، وإنهاء إجراءاتهم الحكومية واستخدموا هذه الأجهزة في مهام عديدة ومختلفة، أصبحت معلوماتهم الحساسة والبالغة الأهمية معرضة للخطر والاختراق والاستيلاء فنشأ مجال أمن المعلومات Information Security وبات من أهم العلوم في عصر التكنولوجيا للحفاظ على هذه الثروة المعلوماتية المهمة لكل جهة، سواء أكانت حكومية أم أهلية، بعد اعتمادها بشكل متنامي على حلول تقنية المعلومات Technology Information في تسيير أعمالها وذلك لتحقيق أهداف المنظمة . وعندما نتحدث عن أمن المعلومات فلابد أن نشمل الحديث عن الأمن السيبراني Cyber Security فلقد أصبح الأمن مهما لصناع القرار في من أي سياسة أمنية وطنية، حيث بات معلوما أن الأمن السيبراني يشكل جزءا أساسيا من أمن الدول الكبرى، مثل الولايات المتحدة الأمريكية، الإتحاد الأوروبي، روسيا، الصين، الهند، وبعض الدول العربية، وفي مقدمتها المملكة العربية السعودية، مصر، ولبنان، وغيرها، فقد أصبح تصنيف الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية بالإضافة إلى ما تقدم. وقد أعلنت أكثر من 130 دولة حول العالم عن سيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني. وتم تخصيص أقسام وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني (البار والمرحبي، 2020).

ولا شك أن بناء مجتمع آمن معلوماتياً ينطوي على بناء أجهزة ووحدات متخصصة ومتسلحة بتقنيات نوعية لمكافحة كافة أشكال الجريمة الإلكترونية، وخلق بيئة تشريعية وقانونية ملائمة متطورة قادرة على ردع مرتكبي هذه الجرائم، والحد من إساءة استخدام تكنولوجيا المعلومات والاتصالات في أغراض إجرامية أو في أغراض غير مشروعة مستقبلية، إن مرتكبي الجرائم الإلكترونية مجرمون، قابعين أمام شاشات الحواسيب الإلكترونية، يختلفون في سلوكياتهم ودوافعهم عن المجرمين التقليديين (منصور، 2008).

1.1. مشكلة الدراسة:

أن هناك عدة تقارير واحصائيات تشير إلى أن 95% من الشركات الكبرى متعددة الجنسيات تعترف بتعرضها للقرصنة، حيث اتخذت أكثر من 135 حكومة في العالم إجراءات حازمة تخص العالم الافتراضي والأمن الإلكتروني، خاصة مع كثرة الاعتداءات الإلكترونية بين الدول، وأهمها تلك الهجمات المتبادلة بين الولايات المتحدة الأميركية من جهة، والصين وروسيا وإيران وكوريا الشمالية من جهة أخرى، ناهيك عن تزايد عمليات سرقة الملكية الفكرية وقرصنة المنشآت الاقتصادية والتجارية، والجامعات، والمعاهد البحثية، والمؤسسات الإعلامية، علاوة على انتشار شبكات الإرهاب السيبراني التي توفر نقاط التلاقي والتنسيق بين التنظيمات الإرهابية وتبادل المعلومات والخبرات (دحمانى، 2018).

ففي عالم الإنترنت اليوم، تسقط أنظمة، وتنهار مؤسسات، ويخلع رؤساء، كيف لا وهي حرب خارجة عن سيطرة الدول وأجهزتها، لا تعترف لاتفاقيات ولا معاهدات ولا مواثيق، وأبطالها افتراضيون. فقد ترك هذا التطور فراغا تشريعيا لدى العديد من الدول ووقفت أمامه النصوص القائمة عاجزه عن احتواء ما استجد على الساحة الجنائية من صور إجرامية مستحدثة (خلف، 2010).

ولهذا تبرز أهمية البحث الحالي في كونه سوف يوضح المتطلبات التي يجب أن نستعد من خلالها لتطبيق الأمن السيبراني داخل المنظمات السعودية حتى نستطيع أن نحافظ على معلوماتها الإلكترونية مستقبلاً وجعلها تشعر بالأمن والاستقرار وعدم الخوف من أي قرصنة على مواقعها الإلكترونية والحفاظ على سريتها وتحصينها من أي تخريب واختراق إلكتروني.

ومن خلال ما تقدم، يمكن بلورة مشكلة البحث بالسؤال الرئيس الآتي:

- **ما هو واقع الأمن السيبراني في المملكة العربية السعودية وما هو الوضع المأمول مستقبلا؟** وتنبثق منه الأسئلة الفرعية الآتية:
  - ما هي المتطلبات التشريعية لتطبيق الأمن السيبراني في المملكة العربية السعودية؟
  - ما هي المتطلبات البشرية لتطبيق الأمن السيبراني في المملكة العربية السعودية؟
  - ما هي المتطلبات التقنية لتطبيق الأمن السيبراني في المملكة العربية السعودية؟
  - ما هي المتطلبات المالية لتطبيق الأمن السيبراني في المملكة العربية السعودية؟

2.1. أهداف الدراسة:

يهدف البحث بشكل عام إلى التعرف على واقع الأمن السيبراني في المملكة العربية السعودية ومتطلبات تطبيق الأمن السيبراني في وذلك من خلال التعرف على:

- المتطلبات التشريعية لتطبيق الأمن السيبراني في المملكة العربية السعودية.
- المتطلبات البشرية لتطبيق الأمن السيبراني في المملكة العربية السعودية.
- المتطلبات التقنية لتطبيق الأمن السيبراني في المملكة العربية السعودية.
- المتطلبات المالية لتطبيق الأمن السيبراني في المملكة العربية السعودية.

3.1. أهمية الدراسة:

1.3.1. الأهمية النظرية:

- تكمن الأهمية النظرية للدراسة في توجيه أنظار الباحثين إلى أهمية الموضوع الذي تتناوله، وهو موضوع خصائص أمن المعلومات والأمن السيبراني والذي ظهر بمثابة استجابة لمتطلبات العصر فهو نمط قيادي يبين الالتزام، ويخلق الحماس والدافعية لدى العاملين ويزرع لديهم إحساساً بالأمل والطاقة للعمل ومواجهة التحديات بطريقة علمية منظمة.
- ومما يزيد هذه الدراسة أهمية من خلال إلقاء الضوء على الجوانب الإيجابية للسرية والتكاملية والإتاحة، حيث أن المنظمات في المملكة العربية السعودية تحتاج إلى أمن وحماية المعلومات لمواكبة التحولات والتغييرات من أجل الحفاظ على منظماتهم.
- تمثل هذه الدراسة من الناحية النظرية، إضافة جديدة للمكتبة السعودية وتمثل من الناحية التطبيقية أيضاً رؤية مستقبلية لتطوير جودة الأمن المعلوماتي في المنظمات داخل المملكة العربية السعودية.

2.3.1. الأهمية التطبيقية:

- تكمن أهمية هذه الدراسة من الناحية التطبيقية في كونها تتناول قطاعاً مهماً، وهو القطاع الأمني في المملكة والمتمثل في الحفاظ على سرية وأمن المعلومات والذي قد يعرض العديد من القطاعات للأزمات، لاسيما في ظل الظروف الاقتصادية والسياسية المالية الصعبة، إذ يأمل الباحث أن تزود الدراسة متخذي القرار للتكنولوجيا بنتائج علمية وميدانية يمكن الاستفادة منها بحيث تحقق الصورة المناسبة مع متطلبات العصر الحديث. كما تستمد هذه الدراسة أهميتها التطبيقية كونها:

- تبحث في موضوع مهم بالنسبة للإدارة أو المنظمات، حيث أن نجاح كثير من المنظمات يرتبط إلى حد كبير على قدرتها في المحافظة على أمن وسرية المعلومات، وتزداد هذه الأهمية في القطاعات الحكومية والخاصة وبعض الجهات الأخرى التي تتصف المعلومات فيها بالحساسية والأهمية البالغة.
- تكمن أهميتها في أنها ستخرج بتأصيل فكري فلسفي لطبيعة متغيرات الدراسة المبحوثة بناء على جهد تطبيقي لواقع خصائص أمن المعلومات في تحقيق الأمان المؤسسي عبر قدرات التعلم التنظيمية.
- تسهم في إضافة علمية ومعرفية في الأوساط المهتمة بمتغيرات الدراسة الحالية كون هذا الموضوع لم يطرق كثيرا في البيئة السعودية، والبيئة العربية.
- تنبع أهمية البحث في الآمل المعقود على التحول نحو تطبيق متطلبات الأمن السيبراني وما سيحققه من فوائد للأفراد والجماعات والمنظمات والمجتمع في تأمين للتهديدات والتحديات التي تواجه هذه المنظمات في المملكة العربية السعودية وسرعة تفادي أية أخطار قد تضر بها، وتقليل هامش هذا الخطر بأسرع وقت وأقل كلفة، وتحقيق الأمان التقني في العمل.
- كما تتجلى أهمية هذا البحث في بيان المنافع التي تواكب التحولات التي تسعى إليها كل الدول في هذا الجانب المهم في تحقيق الأمن السيبراني، وتحديد مدى الاستجابة لمتطلبات العصر وتحدياته، من خلال القدرة على توفير متطلبات تطبيق الأمن السيبراني، وتهيئة البنية التحتية اللازمة لتحقيق هذا الغرض.

2. الإطار النظري والدراسات السابقة:

1.2. الإطار النظري:

1.1.2. أمن المعلومات:

لقد أصبح العالم اليوم قرية عالمية بفضل استخدام الإنترنت على نطاق واسع، حيث يمكن لفكرة واحدة أن تصل إلى مليارات الأشخاص حول العالم بنقرة واحدة على كما أن فوائد المعلومات للمنظمات كبيرة بشكل لا يمكن إنكاره، والمعلومات حاليا هي القوة المحركة للمنظمات والاقتصاديات بسبب عولمة المنتجات والأسواق، حيث مكن الإنترنت من توافر المعلومات وبالتالي أصبح مصدر المعلومات الأكثر قيمة ووسيلة لنقل المعلومات، وأدى تزايد الاعتماد على المعلومات من قبل المنظمات إلى زيادة الاعتماد على سرية المعلومات ونزاهتها وتوافرها، وقد أدى التطور والنمو السريع لاقتصاد المعلومات إلى الحاجة الملحة لأمن المعلومات، بالإضافة إلى ذلك، تواجه المؤسسات مخاطر ونقاط ضعف عالمية متقدمة تسبب خسائر فادحة بسبب خروقات البيانات أو فقدان المعلومات، والحقيقة القاسية هي أن كل منظمة ستتعرض للهجوم، لكن السؤال هو متى وكيف؟، والهدف الرئيسي لأمن المعلومات اليوم هو حماية السرية والنزاهة وضمان توافر البيانات والبنية التحتية للمعلومات، وحمايتها

المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الخامس - الإصدار التاسع والأربعون
تأريخ النشر: 20 نوفمبر 2023 م

من سوء الاستخدام المتعمد أو اللاإرادي، ولا يمكن الوصول إلى حالة الأمن المطلوبة للمعلومات في أي منظمة إلا إذا كانت الإدارة العليا ملتزمة بالكامل بالإشراف على تطويرها، واتخاذها إجراءات صحيحة لضمان أمن المعلومات (Ndungu ,Kandel, 2015).

رسم توضيحي 1 - نموذج مكونات نظم المعلومات

إن الأمن المعلوماتي لم يعد مهمة يتولاها فنيون وتكنو قراط داخل المنظمات كل على حده بشكل مجزأ، بل أصبحت من القضايا التي يتولاها سياسيون واستراتيجيون وصناع قرار، يترجمونها في سياسات واستراتيجيات وطنية تعمل ضمن منظومة الأمن الوطني الشامل وتضبط العلاقة بين أمن المعلومات والأمن الوطني وتوجهها في مسارها الصحيح (غيطاس وجمال محمد، 2007).

كلما زاد الاعتماد المتزايد على التكنولوجيا في الأنشطة اليومية زاد من إمكانية إساءة استخدام هذه الأنظمة، حيث تركز معظم أبحاث أمن المعلومات على الحفاظ على السرية والتكاملية وتوافر المعلومات، حيث تضمن السرية أن الوصول إلى المعلومات يقتصر على الأفراد المخولين أو إلى مجموعة محددة داخل المنظمة، وتتضمن مقاربات أمن المعلومات كلا من الحلول التقنية وغير التقنية، وحث الباحثون في المجال الفني لأمن المعلومات على استخدام التكنولوجيا كوسيلة للقضاء على أي اختراق أمني للنظم يشمل هذا التشفير (Victoria, Mahabi, 2010).

1.1.1.2. مفهوم أمن المعلومات:

في دراسة للباحث (Victoria, Mahabi, 2010)، قام بتقسيم مفهوم أمن المعلومات إلى قسمين أساسيين: أحادي وثنائي. ويقصد بأمن المعلومات الأحادي: أن يكون النظام آمنا بحد ذاته، وموثوقا إن لم يتمكن أي متطفل خارجي من إحداث أي تغيير في النظام يخرجه عن سلوكه الطبيعي، أو أي تعديل أو تغيير في البيانات نفسها، أي يجب حمايته من أي اختراق خارجي، و مستخدم هذا النظام يعتمد عليه كليا ولا يشكل له هذا النظام أي هاجس أمني بشكل أو بأخر، وأما الأمن الثنائي: فيشير إلى أنظمة المعلومات التي تحتاج إلى الحماية من الطرفين أثناء التعامل معها مثل أنظمة التبادل التجاري الإلكتروني، والتي يفتقد فيها المشتري والبائع الثقة في بعضهما ويحتاجان ضمان سلوك أحدهما تجاه الآخر. وفي الواقع فان في مثل هذه الحالات يتم الافتراض بصدق وموثوقية أحد الأطراف للآخر لإتمام العملية التجارية.

أمن المعلومات، من زاوية أكاديمية: هو العلم الذي يبحث في نظريات وإستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها من أنشطة الاعتداء عليها. ومن زاوية تقنية: هو الوسائل والأدوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية. أما من الناحية القانونية: فإن أمن المعلومات هو محل دراسات وتدابير حماية سرية وسلامة محتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة، وهو هدف وغرض تشريعات حماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها (علوه ورأفت نبيل، 2006).

وتعرف لجنة أنظمة الأمن القومي الأمريكية أمن المعلومات بأنها حماية المعلومات وعناصرها الهامة بما في ذلك الأنظمة والأجهزة التي تستخدم وتخزن وترسل هذه المعلومات (الشهري وناصر، 2013). ووفقا لقانون الولايات المتحدة يعرف أمن المعلومات بأنه: "حماية المعلومات ونظم المعلومات من الوصول لغير المصرح لهم، والاستخدام، والتعديل وإحداث الخلل أو التدمير (U.S. Government, 2016).

أما) جواد والفتال، 2008)، فقد عرفا أمن المعلومات بأنه، مفهوم يتسع ليشمل الإجراءات والتدابير المستخدمة في المجالين الإداري والفني لحماية المصادر (من أجهزة وبرمجيات وبيانات وأفراد) من التجاوزات والتداخلات غير المشروعة التي تقع عن طريق الصدفة أو عمدا عن طريق التسلل أو كنتيجة لإجراءات خاطئة أو غير الوافية المستخدمة في إدارة هذه المصادر.

ويعرف (داود، 2000) أمن المعلومات بأنه، حماية وتأمين كافة الموارد المستخدمة في معالجة المعلومات، حيث يتم تأمين المنشأة نفسها والأفراد العاملين فيها وأجهزة الحاسبات المستخدمة فيها ووسائط المعلومات التي تحتوي على بيانات المنشأة ويتم ذلك عن طريق اتباع إجراءات ووسائل حماية عديدة تضمن في النهاية سلامة المعلومات، وهي الكنز الثمين الذي يجب على المنشأة الحفاظ عليه.

2.1.1.2. أهمية أمن المعلومات:

تتبع أهمية أمن المعلومات من أنها تستخدم من لدن الجميع بلا استثناء: الدول، والشركات، والأفراد، كما أنها هدف للاختراق من جانب الجميع وفي بعض الأحيان تكون المعلومات هي الفاصل بين المكسب والخسارة للشركات وقد تكلف الفرد ثروته وربما حياته، وفي هذا العصر بالذات لم تعد مشكلة الناس الحصول على المعلومات، وانما أصبحت مشكلتهم هي هذا الفيض الهائل من المعلومات كيف نحمي هذه المعلومات من الأخطار، ومن هنا اقتصر دور الكثير من مدراء ومشرفي أقسام وإدارات تقنية المعلومات على التعامل مع الشركات الأمنية لوضع البرامج المضادة للفيروسات وبرامج الاختراق والتسلل وغيرها ولكن جميعها تنصب في جزءٍ واحد هو وسائل الحماية (نهاد وخلود، 2013).

ويؤكد (داود، 2001)، بأن أهمية أمن المعلومات تنبع من أنها تستخدم من قبل الجميع بلا استثناء: الدول والشركات والأفراد، وكما أنها هدف للاختراق، وفي بعض الأحيان تكون المعلومات هي الفيصل بين النصر والهزيمة في الحروب، وأحيانا هي الفيصل بين المكسب والخسارة للشركات، وقد تكلف الفرد ثروته وربما حياته في بعض الأحيان.

إن أمن نظم المعلومات هي في الأساس وظيفة دفاعية، ويجب أن يكون المدافع الناجح ناجحا ضد جميع الهجمات، بغض النظر عن مكان حدوث الهجوم، وشكل الهجوم، أو وقت وقوع الهجوم، والتدابير المتخذة لزيادة أمن المعلومات، على الأغلب يجعل من النظام، صعب الاستخدام تقريبا أو مرهق، ونتائج الممارسة لذلك في الغالب (من وجهة نظر الأمن)، بأن المزايا الأمنية

ببساطة قد أهملت، أو ليست قيد التشغيل للحفاظ على الهدف من سهولة الاستخدام، والشبكات وأنظمة التشغيل المتوفرة بشكل تجاري هذه الأيام توفر آليات دفاعية ضعيفة فحسب، وبالتالي فإن المكونات التي تشكل النظام عرضة للخطر ويصعب حمايتها على حد سواء (T. Berson, et al., 1999).

3.1.1.2. الأركان الرئيسية لأمن المعلومات:

وأشار (السالمي والسليطي، 2008) إلى أن أهم مرتكزات الحماية التكاملية لخصوصية المعلومات، يتضمن البعد التقني من أجل توفير أدوات حماية تقنية تتيح للمستخدم التعامل مع البيئة الرقمية بقدر من الثقة والأمن، والبعد القانوني لتوفير التشريعات اللازمة لتنظيم مسائل الحماية، والبعد التوعوي لتثقيف وتوعية الأفراد بالمخاطر التي تتعرض لها البيانات والتعرف على أهم الوسائل اللازمة لضمان حمايتها.

ويرى (حسنين ورجب عبد الحميد، 2012)، أن أمن المعلومات هو عملية ليست بالبسيطة وانما هى عملية معقدة تتألف من مكونات ثلاث على نفس الدرجة من الأهمية والخطورة وهذه المكونات هى:

- **أولا: سرية المعلومات Data Confidentiality:**

وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة لمنع إطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا هو المقصود بأمن وسرية المعلومات، لذلك فان درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب حفظ سريتها: المعلومات الشخصية للأفراد، والميزانية المالية للشركات قبل إعلانها، والمعلومات والبيانات العسكرية الخاصة بالجيوش والمواقع العسكرية في البلاد.

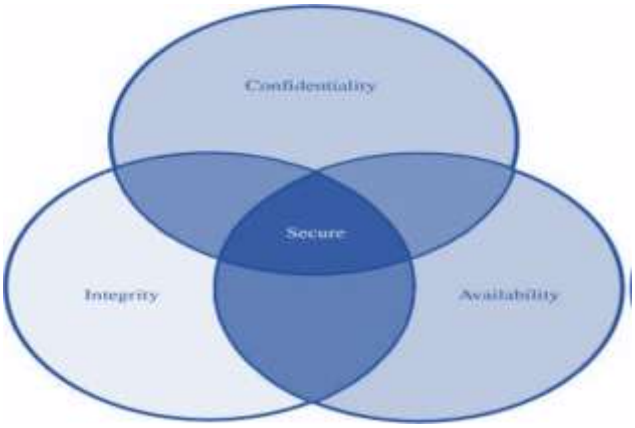
- **ثانيا: سلامة المعلومات Data Integrity:**

في هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، ومن أمثلة ذلك مثلاً: إعلان الوزارات أو الجامعات عن أسماء المقبولين للعمل بها، وتتمثل حماية هذه القوائم في أن تكون مؤمنة ضد التغيير والتزوير فيها بحذف أسماء ووضع غيرها مما يسبب الحرج والمشكلات القانونية للمؤسسات وخسائر فادحة في الأموال.

- **ثالثا: ضمان الوصول إلى المعلومات Availability:**

لعله من المنطقي أن نعرف ان كل إجراءات وصناعة المعلومات في الأساس تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمان سلامتها وعدم التغيير فيها لا يعني شيئاً إذا لم يستطع الأشخاص المخولون أو المصرح لهم الوصول إليها، وهنا تأتي أهمية الجانب الثالث من جوانب أو مكونات أمن المعلومات وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.

أما (Alan Calder, 2005)، فيرى أن أهم ما يميز هذا العصر هو توفر المعلومات وسهولة الحصول عليها من مصادر مختلفة ومتعددة. وتتفاوت نوعية هذه المعلومات وخصائصها باختلاف مصادرها ولكنها تتحد في إمكانية نسخها بأقل التكاليف وإمكانية تعديلها أو حذفها بدون ترك أية آثار تدل على ذلك مالم تتوفر الحماية اللازمة لمصادر هذه المعلومات من خلال الاعتماد على أنظمة أمن المعلومات. لذلك يرى أن تعبير أمن المعلومات بوجه عام يهدف إلى توفر ثلاث أمور رئيسية هي:



رسم توضيحي 2- العلاقة بين السرية والموثوقية والتوافر

- السرية: وتعني أن تتمتع المعلومات بسرية وخصوصية تامة والتأكد من عدم إمكانية الاطلاع عليها من أطراف غير مسئولة أو لأغراض غير شريفة.
- الموثوقية وسلامة المحتوى: وتشير إلى التأكد من عدم إمكانية تغيير المعلومات أو التعديل عليها وبالتالي سلامة محتوى تلك المعلومات واكتمالها.
- استمرارية التوفر أو الوجود: التأكد من توفير السبل التي تضمن توفر المعلومات والتصدي لأي مخاطر ممكنة من شأنها أن تؤثر على استمرار تواجدها ووضع الخطط والسياسات اللازمة لاسترجاع البيانات في حال تعرضها لأحد المخاطر المحتملة.

2.1.2. الأمن السيبراني:

يعرف الأمن السيبراني بأنه عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة (Richard, 2003).

يعرف الأمن السيبراني بأنه أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو على الأقل الحد من آثارها (جبور، 2017).

يعرف الأمن السيبراني بأنه "عملية تنظيم وتجميع الموارد والعمليات والهياكل التي تمكن الفضاء السيبراني من إيقاف عمليات الاختراق بصورها المختلفة، والتي تتم بصورة غير صحيحة وقانونية (Craigen & Daikun & Purse, 2014).

كما يعرف الأمن السيبراني بأنه، النشاط الذي يؤمن حماية الموارد البشرية، والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والاضرار، التي تترتب في حال تحقق المخاطر والتهديدات،

كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة (جبور، 2012).

1.2.1.2. أهداف الأمن السيبراني:

يعتبر أمن النظم من الركائز الضرورية والحاكمة في حماية الأفراد والمنظمات من الأضرار الناتجة من قصور الأمن، حيث يعتمد كل من الأفراد والمنظمات على أداء نظم معلوماتهم من خلال ضمان أمنها بطرق دقيقة، وملائمة وموثوق منها، ويتجه الأمن إلى حفظ فعالية وكفاءة نظم المعلومات، وتأكيد مستوى مناسب لتوافرها وسريتها وسلامتها، إلى جانب تسهيل تطويرها واستخدامها من قبل الأفراد المعنيين بأغراض جديدة غير تقليدية تختلف عن تلك التي تطبق بالفعل، كما تسهل استغلال تكنولوجيا المعلومات بأقصى طاقاتها وإمكانياتها. وبذلك يسهم مجال أمن المعلومات في حماية حقوق واهتمامات كل المعتمدين في التعامل معها بحمايتها وصيانتها من الضرر الناتج من فشل إجراءات توافرها وسريتها وسلامتها (الهادي ومحمد، 2006). ذكر (المنتشري، 2020)، مجموعة من الأهداف للأمن السيبراني نوردها كما يلي:

1. توفير بيئة آمنة تتمتع بقدر كبير من الموثوقية في مجتمع المعلومات.
2. تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات.
3. التصدي لهجمات وحوادث أمن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
4. توفير المتطلبات اللازمة للحد من الجرائم السيبرانية التي تستهدف المستخدمين.
5. مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث أضرار بالغة بالمستخدمين وأنظمة المعلومات.
6. الحد من التجسس والتخريب الإلكتروني على مستوى الحكومات والأفراد.
7. التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها وسد الثغرات في أنظمة المعلومات.

2.2.1.2. أبعاد الأمن السيبراني:

يطال الأمن السيبراني جميع المسائل العسكرية، الاقتصادية، والاجتماعية، والسياسية، والإنسانية، بهدف تحقيق منظومة أمن متكاملة تعمل على الحفاظ على الأمن القومي للدولة من كل التهديدات السيبرانية، وعليه لابد من توضيح أبعاد الأمن السيبراني، التي ذكرها (زريقة، 2019):

- **البعد العسكري:** يكمن في الحفاظ على قدرة الوحدات العسكرية على التواصل عبر الشبكات العسكرية، مما يسمح بتبادل المعلومات والأوامر وتدفقها (هي الفكرة التي خلقت وطورت من أجلها الشبكات ومن بعدها الإنترانت)، وإصابة الأهداف عن بعد، إلا أنها تمثل كذلك نقطة ضعف، خاصة إذا لم تكن مؤمنة جيدا من الاختراق، الذي قد يؤدي إلى تدمير قواعد البيانات العسكرية، أو قطع الاتصال بين القيادة والوحدات العسكرية، فضلا عن إمكانية التحكم في بعض الأسلحة وخروجها عن السيطرة (طائرات بدون طيار، صواريخ موجهة، أقمار صناعية ... الخ).
- **البعد الاقتصادي:** أصبح الإنترنت أساساً للمعاملات التجارية والمالية والاقتصادية، كما تستعمل الحواسيب في تسيير وتطوير الصناعات وتحريك الاقتصاد، وأصبح الكل مترابطا عبر شبكات الكمبيوتر، مما يستدعي الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.

- **البعد الاجتماعي:** مستخدمو الانترنت حول العالم يفوق مستخدمي الانترنت 4 مليارات شخص في العالم، منهم أكثر من 2.6 مليار يستخدمون مواقع التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب واسعا لتبادل الأفكار والخبرات الجيدة، لكن في المقابل يعرض أخلاقيات المجتمع للخطر، نظرا لصعوبة مراقبة محتوى الانترنت، كما يعرض الهويات لعمليات اختراق خارجي، قد تتسبب في تهديد السلم الاجتماعي للدولة، وعليه فلابد من العمل على توعية المواطن بهذه المخاطر لتحقيق الأمن السيبراني في بعده الاجتماعي.
- **البعد السياسي:** يعد التدخل الروسي السيبراني في الانتخابات الأمريكية أبرز دليل على ضرورة وأهمية الأمن السيبراني في بعده السياسي، إضافة إلى التسريبات للوثائق الحساسة والاختراقات التي غالبا ما تؤدي إلى أزمات دبلوماسية بين الدول، كما أن الفضاء السيبراني أصبح بيئة خصبة للحملات الانتخابية والدعاية لمختلف الفاعلين الدوليين.
- **البعد القانوني:** إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية في الفضاء السيبراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان الى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها.

3.2.1.2. تقنيات الأمن السيبراني الرئيسية وأفضل الممارسات:

من خلال تطبيق أفضل ممارسات الحماية التقنية، يمكن تقليل تعرُّض المنظمات والجهات المختلفة من الاختراقات الأمنية وحماية أنظمة المعلومات دون التأثير على خصوصية العميل وتجربة المستخدم ومنها:

- **إدارة الهوية والوصول (IAM):** تتضمن امتيازات الوصول لكل مستخدم، تسجيل الدخول الأحادي، المصادقة متعددة العوامل، وإدارة دورة حياة المستخدم، والتي تدير هوية كل مستخدم وامتيازاته، كما يمكن لأدوات إدارة الهوية والوصول أن تمنح متخصصي الأمن السيبراني رؤية أعمق للنشاط المشبوه على أجهزة المستخدم النهائي، مما يختصر من وقت التحقيق والاستجابة لعزل واحتواء الاختراقات وآثارها.
- **منصة أمن البيانات:** تعمل منصات أمن البيانات على حماية المعلومات الحساسة عبر بيئات متعددة، مثل البيئات المختلطة متعددة الأوساط السحابية، وتوفر رؤية مؤتمتة فورية لنقاط الضعف في البيانات ومراقبتها باستمرار لتفادي حدوث الاختراقات.
- **إدارة المعلومات والأحداث الأمنية (SIEM):** تتضمن تجميع البيانات من الأحداث الأمنية وتحليلها لاكتشاف أنشطة المستخدم المشبوهة تلقائيًا، وتفعيل الاستجابة الوقائية أو العلاجية. وتستخدم حلول إدارة المعلومات والأحداث الأمنية طرق كشف متقدمة، مثل: تحليل سلوك المستخدم والذكاء الاصطناعي.

4.2.1.2. أبرز التحديات التي تواجه المنظمات في مجال الأمن السيبراني:

- **المدة الزمنية لرصد الاختراق:** يُشكل الوقت العنصر الأهم في رصد الاختراقات، لذلك يُعَد توظيف الروبوتات والذكاء الاصطناعي من المجالات الواعدة والتي من شأنها تقديم الكثير في تطوير الأمن السيبراني، وذلك لتفوقها على البشر في معالجة عنصر التوقيت وأهميته في مكافحة الاختراقات كونها تعمل على مدار الساعة.

(55 يوم هو متوسط عدد الأيام بين حدوث الاختراق واكتشافه) (منشآت، 2023)

- **تهديدات إنترنت الأشياء:** كشفت إحدى الدراسات أن 70% من أجهزة إنترنت الأشياء بها ثغرات أمنية خطيرة، حيث تؤدي واجهات الويب غير الأمنة، وعمليات نقل البيانات، ونقص المعرفة للمستخدمين إلى تعريضهم للهجمات، ويتضاعف خطرها إثر حقيقة اتصال الأجهزة ببعضها، فالوصول إلى جهاز واحد يعني الوصول إلى جميع الأجهزة المتصلة به.
- **تأمين السحابة:** على الرغم من أن 64% من المتخصصين في تقنية المعلومات يعتقدون أن السحابة أكثر أمانا كبنية تحتية، إلا أن هناك الكثير من تحديات الأمان أمام جميع الأطراف من مزودي خدمة أو مستخدمين، حيث يجب أن تتكامل الحلول تكاملا ن ترك ثغرات يتسلَّل من خلالها المخترقون.
- **نقص الخبرات:** مازال هناك نقص كبير في عدد متخصصي الأمن السيبراني لتغطية الاحتياج المتزايد في أنحاء العالم، حيث أنّ أكثر من نصف المنشآت تعاني من نقص في مهارات الأمن السيبراني.

5.2.1.2. أمثلة على حالات الاستعمال المُمكنة للأمن السيبراني:

- **تأمين الأنظمة والعمليات (مصادقة الحسابات):** المصادقة هي عملية التحقق من الهوية، وتعمل من خلال مطابقة بيانات اعتماد المستخدم مع بيانات الاعتماد في قاعدة بيانات المستخدمين المصرح لهم للتحكم في الوصول إلى الأنظمة، ومنها: المصادقة أحادية العامل، مثل: طلب اسم المستخدم وكلمة المرور، والمصادقة الثنائية التي تتطلَّب عوامل إضافية، مثل: رمز التحقق المُرسل عى الهاتف المحمول، بصمة الإبهام، والتعرُّف على الوجه.
- **رصد التهديدات (آلية تتبع السياق):** تعمل بعض شركات الأمن السيبراني على تضمين الذكاء الاصطناعي وتعلم الآلة في مستشعراتها بما يسمح بتتبُّع الملفات أثناء نقلها عبر الشبكة وإرسالها لفحصها، وتكمن فائدة توظيف الذكاء الاصطناعي وتعلم الآلة في اكتشاف البرمجيات الضارّة وتتبُّع سياقها بما يتضمن اسم الملف وقيم التجزئة وبروتوكول النقل، مما يُمكن متخصصي الأمن السيبراني من معرفة كيفية وصول الملف ومعالجة المشكلة وتعزيز الحماية المستقبلية.
- **الاستجابة السريعة (توحيد البيانات):** يبذل المحللون جهدا في تتبع تنبيهات الشبكة والأجهزة المرتبطة بها لمعرفة أين تنتهي الهجمة السيبرانية، بينما يتيح توحيد البيانات للعمليات الأمنية مكانية ربط هذه المعلومات ورسم صورة شاملة تُمكّن المُحلل من فهم جلسة المستخدم، ومعرفة العمليات التي كانت تعمل عند تشغيل تنبيه البرامج الضارة، واكتشاف الإجراءات غير الروتينية، وكان ذلك يستغرق ساعة أو أكثر، بينما توحيد البيانات يدعم المُحلل بطريقة سهلة ويُمكن المنظمات من تقديم استجابة أسرع وأكثر تركيزا.

3.1.2. واقع الأمن السيبراني في المملكة العربية السعودية:

مع توسع استخدام الإنترنت وتواجده في كل مكان وفي يد جميع أفراد المجتمع، أصبح لدى قراصنة الإنترنت المزيد من الأجهزة ونقاط الضعف والثغرات التي يمكنهم استغلالها، بل وتجاوز ذلك إلى تهديد أمن الدول، وصاحب ذلك تضافر الجهود لصد الجرائم الإلكترونية.

كما فرض تداخل التقنيات والرقمنة تحديات جمة أمام المنشآت في سبيل تعزيز أمنها السيبراني، ويُظهر الارتفاع المطرد في عدد الاختراقات وخطورتها مدى حاجة هذه المنشآت إلى تركيز إنفاقها وأبحاثها في ممارسات الأمن السيبراني وتحسين موقفها السيبراني. حيث أظهرت دراسة استقصائية أجرتها (تينا بل Tenable) في عام 2020 أن 95% من المنشآت في المملكة

العربية السعودية تعرضت لهجوم سيبراني العام الماضي، فيما أفاد 85% من المشاركين السعوديين في الدراسة بأنهم شاهدوا زيادة كبيرة في عدد الهجمات خلال العامين الماضيين.

وفي هذا الإطار استهدفت رؤية المملكة العربية السعودية 2030 التطوير الشامل للوطن وأمنه واقتصاده ورفاهية مواطنيه وعيشهم الكريم، ولقد كان من الطبيعي أن يكون أحد مستهدفاتها التحول نحو العالم الرقمي وتنمية البنية التحتية الرقمية، بما يعبر عن مواكبة التقدم العالمي المتسارع في الخدمات الرقمية وفي الشبكات العالمية المتجددة، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ويتماشى مع تنامي قدرات المعالجة الحاسوبية وقدرات التخزين الهائلة للبيانات وتراسلها، وبما يهيئ للتعامل مع معطيات الذكاء الاصطناعي وتحولات الثورة الصناعية الرابعة.

إن هذا التحول يتطلب انسيابية المعلومات وأمانها وتكامل أنظمتها، ويستوجب المحافظة على الأمن السيبراني للمملكة العربية السعودية، وتعزيزه، حماية للمصالح الحيوية للدولة وأمنها الوطني والبنى التحتية الحساسة والقطاعات ذات الأولوية والخدمات والأنشطة الحكومية.

لذلك صدر أمر ملكي برقم (6801) بإنشاء هيئة باسم (الهيئة الوطنية للأمن السيبراني) في تاريخ (11 صفر 1439هـ) الموافق (31 أكتوبر 2017) ترتبط بمقام خادم الحرمين الشرفيين، وهي الجهة المختصة بشؤون الأمن السيبراني في المملكة، وتعد مرجع الدولة لحماية أمنها الوطني، ومصالحها الحيوية، والبنية التحتية الحساسة فيها، وتوفير خدمات تقنية أمنه وطرق دفاعية لحماية أنظمة المعلومات والاتصالات ضد الهجمات الإلكترونية، والحفاظ على سرية وسلامة المعلومات.

1.3.1.2. المنظومة البيئية للأمن السيبراني في المملكة العربية السعودية

1) **المنشآت التشريعية والتنظيمية (الهيئة الوطنية للأمن السيبراني):** صدرت الموافقة على تنظيم الهيئة الوطنية للأمن السيبراني في عام 1439هـ، من منطلق أهمية البيانات والأنظمة التقنية والبنى التحتية الحساسة، ولتكون الجهة المختصة بالأمن السيبراني والمرجع الوطني لشؤونه، ومن مهامها: وضع السياسات والمعايير، وضع أطر إدارة المخاطر والاستجابة للحوادث، بناء مراكز المعلومات الوطنية، مساندة الجهات المختصة. بناء القدرات المتخصصة، وتحفيز نمو قطاع الأمن السيبراني، وأهمها: إعداد الاستراتيجية الوطنية للأمن السيبراني، والتي تعكس الطموح الاستراتيجي للمملكة ورؤيتها (فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار)، وتُركز الاستراتيجية على تشجيع الأبحاث ودعم الابتكار والاستثمار في مجال الأمن السيبراني لتحويل مخرجات الأبحاث والتطوير إلى منتجات وخدمات، بالإضافة إلى تحفيز قطاع الأمن السيبراني والمنشآت العاملة فيه لضمان بناء قدرات وطنية.
2) **الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز:** هو مؤسسة وطنية تندرج تحت مظلة اللجنة الأولمبية السعودية، ويسعى الاتحاد إلى بناء قدرات محلية واحترافية في مجال الأمن السيبراني، وتطوير البرمجيات والدرونز بناء على أفضل الممارسات والمعايير العالمية، وذلك من خلال تنظيم المعسكرات والفعاليات التقنية، مثل: معسكر طويق للأمن السيبراني، ومعسكر طويق البرمجي، وعدد من المسابقات والهاكثونات.
3) **المبادرات والفعاليات التقنية:**

- تنظم الهيئة الوطنية للأمن السيبراني المنتدى الدولي للأمن السيبراني سنويًا منذ عام 2020م.، حيث يجمع صُناع القرار والخبراء وكبرى الشركات الرائدة من أنحاء العالم. كما شهدت المملكة العربية السعودية في أغسطس 2021م أكبر إطلاق

تقني للمبادرات والبرامج بقيمة تناهز أربعة مليارات ريال، بالتعاون مع عشرة من أهم عمالقة التقنية في العالم، بهدف تطوير المهارات والكفاءات التقنية وتمكين المملكة رقميًا لتصبح مركزا تقنيا رائدا منها: تنظيم فعالية Hack وهي من أكبر الفعاليات التقنية على مستوى العالم تجمع المخترقين الأخلاقيين لمناقشة المخاطر السيبرانية الدولية، يصاحبها منتدى للأعمال التقنية والدورات التدريبية وورش العمل، بالإضافة إلى إطلاق مؤتمر ليب Leap التقني الأكبر من نوعه، ليكون جزءًا من مبادرات تنفيذية تقنية تقام على مدار السنة.

- كما تم عقد مؤتمر الأمن السيبراني في نسخته الثالثة باسم (رسم الأولويات المشتركة في الفضاء السيبراني) الذي تم عقده في الرياض بتاريخ 1-2 نوفمبر/2023 وحضره عدة وزراء وممثلين من عدة دول ومتحدثين في عدة تخصصات. وتم خلال المؤتمر عقد عدة ورش عمل وجلسات حوارية وكان من أهم التوصيات التي انبثقت من هذا المؤتمر:

1. تعزيز قوة الصمود لمواجهة الهجمات السيبرانية
2. تمكين فضاء سيبراني آمن ومستدام وشامل
3. تثبيط الجرائم السيبرانية
4. حماية الفضاء الإلكتروني في عصر التقنيات الناشئة

اضافة الى انه تم التركيز على عدة مواضيع منها حماية الأطفال في الفضاء السيبراني وتمكين المرأة للمشاركة والعمل في مجالات الأمن السيبراني:

- **حماية الطفل في الفضاء السيبراني:**

وتمحور النقاش حول تطوير أفضل الممارسات والسياسات والبرامج لحماية الأطفال في العالم السيبراني لمواجهة التهديدات السيبرانية المتزايدة التي تستهدف الأطفال أثناء استخدامهم لشبكة الإنترنت وتعريضهم لجرائم سيبرانية متنوعة بعيداً عن أعين أسرهم، بما في ذلك استغلالهم وجعلهم ضحايا للانقياد وارتكاب الجرائم بحقهم، والتأثير الفكري على توجهاتهم ودفعهم لتبني ايديولوجيات متطرفة وإرهابية تشكل خطراً على الدول والمجتمعات. كما تشمل تلك الجرائم بحق الأطفال، التنمر السيبراني، وسرقة البيانات الشخصية، والاحتيال. كما أن التطورات المتسارعة التي تشهدها البيئة الرقمية وتقنية المعلومات والاتصالات اليوم يصاحبها تزايد في المخاطر المحدقة بأطفالنا وهم يمثلون مكونا مهم من مكونات العالم الرقمي وهم الأكثر التصاقا به، ومعرضون فيه لمختلف التجاوزات، والانتهاكات بحقهم في الحياة والنمو الأمر الذي يتطلب وقفة جادة وتعاونًا لحماية الأطفال وجعلهم في منأى عن المخاطر والتهديدات وصولاً إلى بيئة رقمية آمنة.

- **تمكين المرأة للمشاركة والعمل في مجالات الأمن السيبراني:**

ولتمكين المرأة وتفعيل دورها وإتاحة الفرص لها في جميع المجالات والتي من أهمها الأمن السيبراني والتي يظهر انها حصرا على الرجال في الوقت الحالي، طرقت النقاشات خلال المؤتمر حول الوضع الحالي في المملكة لمشاركة المرأة في مجالات الأمن السيبراني مقارنة بالرجال حيث انه حاليا يوجد امرأة واحدة عاملة لكل أربع رجال. وتمت الإشادة بمبادرة ولي العهد الأمير محمد بن سلمان - حفظه الله - لتمكين المرأة ودعم العاملات في مجالات الأمن السيبراني والتي تعتبر جزءاً استراتيجياً من رؤية المملكة 2030. لذلك أصبح هناك توجه في الآونة الأخيرة نحو زيادة عدد النساء في هذا المجال مما يعزز فرص العمل في المجتمع ويرفع مستوى الكفاءة في هذا القطاع، حيث إن النساء اللاتي يعملن حالياً في هذا القطاع أتوا بخبرات علمية

متنوعة خبرات علمية متراكمة على مدى سنوات متعددة وجاء الوقت لاستثمارها والاستفادة منها في رفع نضج الأمن السيبراني في الوطن وتشكيل مستقبله، الا أنه حتى الآن يوجد نقص في الكفاءات والخبرات وبرامج التدريب، وقد يحتاج هذا المجال وقتاً لكي ينمو وينضج ويستقر ويتزايد احتياج الجهات الحكومية والخاصة إلى أكفاء في الأمن السيبراني من الجنسين مع تزايد استخدام التقنية والتحول الرقمي.

4) **دعم رواد الأعمال:** أقيم تحدي الأمن السيبراني بالتعاون بين الهيئة الوطنية للأمن السيبراني ومنشآت وشركة سايت - إحدى شركات صندوق الاستثمارات العامة - ويهدف التحدي إلى إيجاد الحلول المبتكرة في مجال الأمن السيبراني، وتوطين هذه التقنيات من خلال عرض مشاريع الشركات الناشئة ورواد الأعمال، كما تضطلع الهيئة العامة للمنشآت الصغيرة والمتوسطة (منشآت) بتنظيم جائزة (ابتكر) الموجهة للمنشآت المتوسطة والصغيرة والمُتناهية الصغر، بهدف تشجيع الابتكار وتسليط الضوء على المنشآت الابتكارية في المملكة، كما تقام مسابقة منتدى (إم آي تي MIT) لريادة الأعمال في السعودية سنويًا منذ عام 2015م حيث تُروج المسابقة للابتكار والإبداع على مستوى العالم ودعم الشركات الناشئة بالسعودية، والتواصل مع رواد الأعمال المحليين لتحويل أفكارهم إلى واقع ملموس. وينشط في هذا المجال، مركز ذكاء لإنترنت الأشياء والأمن السيبراني التابع لهيئة منشآت، والذي يعمل على تقديم الخدمات التدريبية والاستشارية لرواد الأعمال والمنشآت الصغيرة والمتوسطة، وتنظيم اللقاءات والتحديات الجماعية، حيث نُظم تحدي ذكاء للأمن السيبراني لتصميم الحلول المبتكرة الداعمة لقطاع الأمن السيبراني، ومن أهدافه: زيادة عدد شركات الأمن السيبراني الناشئة في المملكة العربية السعودية، توطين تقنيات الأمن السيبراني، تمكين المواهب الوطنية، المساهمة الاقتصادية، وخلق الوظائف.

2.3.1.2. الفرص التقنية في المملكة العربية السعودية بين الواقع والمأمول:

يأتي الاهتمام بالأمن السيبراني مدفوعًا بتصاعد التهديدات الأمنية على مستوى العالم، وبالتحوّل الرقمي الذي تشهده المملكة العربية السعودية، والذي يدفع المنشآت إلى تبنّي الرقمنة في جميع عملياتها، وتبرز أهمية حلول الأمن السيبراني في محيط الأعمال لارتباطها ارتباطا مباشرا بالحفاظ على سمعة المنشأة بين موظفيها وعملائها، الحفاظ على ميزتها التنافسية، والحفاظ على استمرارية الإنتاجية من خلال تجنب الوقت الضائع الناتج عن التعرض لأي تهديد سيبراني.

تُعد حلول الأمن السيبراني مجالا جذابا لرواد الأعمال في المملكة العربية السعودية، حيث يُشير المنهج الحالي السائد في السوق السعودي فيما يتعلّق بالأمن السيبراني أن الشركات المالية هي الأقل استعدادا من ناحية البنية التحتية مقارنة بالاحتمالية العالية لتعرّضها للتهديد دونا عن الشركات الأخرى، حيث من المُحتمل أن تستهدف الهجمات السيبرانية الشركات المالية بواقع 300 مرة أكثر من الشركات الأخرى.

من العوامل الجاذبة الأخرى لحلول الأمن السيبراني عامة، هو نمو حجم سوق الأمن السيبراني السعودي بمُعدل نمو سنوي مُركب يبلغ 16.59% حتى نهاية عام 2023م إلى ما يُقدر بنحو 21 مليار ريال سعودي وفُقا لمجلس الأعمال السعودي الأمريكي، مصحوبًا بالتوجه نحو تعزيز القطاع، حيث حصدت المملكة ترتيب الأول عربيا والمرتبة 13 من بين 175 دولة في مؤشر الأمن السيبراني العالمي الصادر مؤخرا عن الاتحاد الدولي للاتصالات (ITU).

ومع ذلك ما تزال المملكة العربية السعودية تسجل أكبر عدد من الهجمات السيبرانية في الشرق الأوسط، ما يتبعه زيادة طلب المنشآت على حلول الأمن السيبراني، يُصاحبه وجود عجز بين الطلب والعرض في قطاع الأمن السيبراني السعودي، مما دفع 95% من شركات الأمن السيبراني المحلية إلى التركيز على تقديم الخدمات والعمليات السيبرانية، بينما تُركز 5% منها فقط على تطوير منتجات سيبرانية تواكب تغير التهديدات ومستواها.

من التحديات التي برزت مُؤخرا أيضا، نقص الكوادر الوطنية المُتخصصة اللازمة لتحقيق أهداف التوطين في قطاع الأمن السيبراني، مما دفع الهيئة الوطنية للأمن السيبراني إلى إنشاء الأكاديمية الوطنية للأمن السيبراني لتأهيل الكوادر الوطنية المُتخصصة وتقليل الفجوة بين العرض والطلب، ولقد دربت الأكاديمية في مبادرتها الأولي أكثر من 1000 متدرب من 113 جهة وطنية و23 جامعة سعودية.

من ناحية أخرى أنشأت شركة مُلكية للاستثمار أول صندوق استثماري في مجال الأمن السيبراني في المملكة العربية السعودية، باسم "صندوق مُلكية للأمن السيبراني" بالشراكة بين شركة مُلكية للاستثمار ومجموعة بالادين المالية الأمريكية، ويهدف الصندوق إلى إتاحة فرصة الاستثمار في شركات قطاع الأمن السيبراني وتقنياته على مستوى العالم، لتحقيق نمو رأس مالي على المدين المتوسط والطويل، كما تفتح الاستراتيجية الوطنية للأمن السيبراني عددا من الفرص المستقبلية من خلال تركيزها على تحقيق الحوكمة المتكاملة على المستوى الوطني، الإدارة الفعالة للمخاطر السيبرانية، حماية الفضاء السيبراني، تعزيز الشراكات والتعاون المحلي والدولي، وبناء القدرات الوطنية، وجميع هذه الأهداف تُعطي تصورا لتوفير منظومة بيئية داعمة لمشاريع ومنشآت الأمن السيبراني في المملكة العربية السعودية.

2.2. الدراسات السابقة:

دراسة (الدحياني، 2021)، بعنوان: متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر الخبراء.

هدفت الدراسة إلى التعرف على متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر المختصين، ولتحقيق هذا الهدف استخدم الباحث المنهج الوصفي المسحي، واستبانة تكونت من (7) فقرة موزعة على أربعة مجالات هي (المتطلبات التشريعية - المتطلبات البشرية - المتطلبات التقنية - المتطلبات المالية)، وذلك لغرض جمع البيانات. وبعد التأكد من صدقها وثباتها تم تطبيقها على عينة البحث، والتي بلغ عددها (70) موزعة بين المختصين في مجال الحاسوب والتقنيات والذكاء الاصطناعي، وقد خلصت الدراسة إلى أن درجة الموافقة على متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر المختصين كانت(عالية جداً)، على مستوى الأداة ككل وعلى مستوى كل مجال من مجالات البحث، كما كشفت نتائج البحث عن عدم وجود فروق ذات دلالة إحصائية في استجابات أفراد عينة البحث تعزى للمتغيرات الديموغرافية (الجنس، الدرجة العلمية، وسنوات الخبرة العملية في هذا التخصص)، وذلك على مستوى الدرجة الكلية للأداة وعلى مستوى كل مجال من مجالات البحث.

دراسة (العنزي، ماجد بن خلاف حمود،2020)، بعنوان: الإرهاب السيبراني وانعكاساته على الأمن الوطني، جامعة نايف العربية للعلوم الأمنية.

هدفت الدراسة إلى التعريف بالإرهاب السيبراني وانعكاساته على الأمن الوطني، حيث أجريت الدراسة على جميع العاملين في مراكز العمليات الأمنية من أعضاء الجمعية السعودية لأمن المعلومات في المملكة العربية السعودية. من أهم الاستنتاجات

المستخلصة من الدراسة أن الدافع الرئيسي للعمليات الإرهابية السيبرانية هو التوجهات السياسية لدى المنظمات الإرهابية، وأن من أهم عوامل تحقيق الأمن الوطني السيبراني هو استخدام أحدث أنظمة الحماية التقنية، وأوصت الدراسة برفع مستوى الوعي العام بأهمية الأمن السيبراني وبيان أنواع ووسائل تمديداته ومخاطره المحتملة.

دراسة (غيدان والربيعي، 2020)، بعنوان: الأمن السيبراني وسياسات المواجهة الدولية.

هدف البحث إلى بيان واقع الحروب السيبرانية، التي باتت تشكل خطرا عالميا لا تستثنى أية دولة منه، وما مدى التحديات التي تواجهها الدول للوقاية من هذه الحروب والهجمات، عن طريق توظيف الإمكانيات الاقتصادية والبشرية والتقنية لمواجهة هذه الهجمات، وقدم البحث معلومات نظرية حول الإستراتيجيات التي تسعى الدول الى وضعها لتأمين وتعزيز مكانتها من هذه الحروب والهجمات، وقد توصل البحث إلى أن مفهوم الأمن السيبراني اليوم من أهم المفاهيم التي تسعى الدول الى تحقيقها، لاسيما بعد التقدم التكنولوجي الهائل في مجالات الحياة، ومدى تأثير هذا التقدم على التفاعلات الدولية وتأثيره، حتى في تغيير شكل الحرب، وصولا الى الشكل الجديد للحرب ألا وهو "الحرب السيبرانية".

دراسة (بشرى الأمين، 2013)، بعنوان: واقع الجريمة الإلكترونية داخل المملكة العربية السعودية لاستقراء التحديات المستقبلية.

خلصت الدراسة الى عدم وجود انضباطية على ساحات الفضاء الإلكتروني السعودي تتيح نوعا من التسهيلات "اللوجستية " الرقمية للنشطاء والجناة لارتكاب جرائم وممارسات غير قانونية، جاءت في معظمها بسبب دوافع استعراضية وسياسية، ثم يليها دوافع جني الأرباح وتحقيق المكاسب المادية، كذلك رصدت الدراسة صعوبات أمنية في جمع الأدلة الرقمية والتتبع الإلكتروني لمصادر الجرائم الإلكترونية المتصلة بهجمات القرصنة والتسلل باستخدام أساليب DDOS وBOTNET من خارج الحدود الإلكترونية السعودية. كما أكدت الدراسة على خطورة جرائم المحتوى في المستقبل، خاصة الجرائم المتعلقة بالإرهاب واستقطاب الشباب، وترويج الفكر الجهادي والطائفي، وتنامي شبكة الجماعات التكفيرية، ضرورة تبني فلسفة التوعية وسياسة المحتوى المضاد على الإنترنت.

3. النتائج والتوصيات:

1.3. النتائج:

لقد آدى التطور التكنولوجي إلى مجموعة من النتائج الايجابية التي انعكست على تحسين الحياة العامة للأفراد، كما كان له الأثر الإيجابي على اقتصاديات الدول، ولكن الاستغلال السلبي للتكنولوجيا أفرز مجموعة من المفاهيم، من بينها ما يعرف بالجريمة الإلكترونية، حيث أدى استخدام الحاسوب وكذا شبكة الانترنت لأغراض تسبب أضرار للآخرين، تمس بخصوصياتهم، وتحد من حرياتهم في المجال المعلوماتي.

إن التحدي الحالي للدول هو مواجهة الجريمة العابرة للقارات، لتفادي الآثار الكارثية التي قد تسببها، وتحقيق الأمن السيبراني، الذي يحفظ السلامة الإلكترونية، ويحقق الأمن الإلكتروني، من خلال مختلف الاتفاقيات الدولية أو الإقليمية، أو إطار وإشراف مختلف البيئات والمنظمات الدولية الرسمية، فجهود الدول، تسعى إلى توحيد الرؤى لمواجهة الجريمة الإلكترونية والإرهاب السيبراني، وخلق آليات تساعد في التحقيق والمتابعة القانونية للمجرمين الإلكترونيين.

2.3. التوصيات:

➢ **التوصيات التشريعية:**

- وضع التشريعات التي تساهم في تطبيق الأمن السيبراني داخل المنظمات.
- إصدار اللوائح التي تضمن سرية تبادل المعلومات داخل المنظمات.
- وضع التشريعات التي تعمل على حماية أمن نظام المعلومات داخل المنظمات.
- إصدار التشريعات المنظمة للعمل الإلكتروني وإدارة نظم المعلومات داخل المنظمات.
- تغيير السياسات المؤسسية التقليدية المتعلقة بالعمل الإداري بما يتناسب مع إدارة الأعمال إلكترونيا.
- إيجاد تشريعات تضمن حق الملكية للمبتكرين في المجال الإلكتروني.

➢ **التوصيات البشرية:**

- تحرص المنظمات على تدريب القيادات والعاملين على مهارات تطبيق برامج الأمن السيبراني.
- ان توفر المنظمات قاعات تدريب للموظفين تحتوي على جميع الاحتياجات التدريبية التي ترفع من القدرات الإلكترونية لديهم.
- أن تستعين المنظمات بخبراء في تطبيق الأمن السيبراني.
- ان يمارس الموظفون العمل الجماعي لإنجاح عملية تطبيق الأمن السيبراني داخل المنظمة.
- عمل تغذية راجعة للقيادات والعاملين في ضوء التقييم.
- ضرورة اهتمام المنظمات بتأهيل وتطوير مهارات الموظفين من خلال الدورات التدريبية الدورية.

➢ **التوصيات التقنية:**

- عمل دراسة لاحتياجات المنظمات من الأجهزة والمعدات والبرامج والمستلزمات اللازمة لتطبيق الأمن السيبراني.
- توفير أجهزة حاسوبية حديثة كافية لجميع العاملين في نظم المعلومات داخل المنظمات.
- توفير الشبكة الإلكترونية الداخلية والبرامج والتطبيقات المتعلقة بعملية التطبيق.
- تحديث الموقع الإلكتروني للمنظمات باستمرار.
- توفير انظمة حماية آلية متطورة لحماية بيانات المنظمة
- توفير برامج الصيانة للشبكة الداخلية والبرامج والتطبيقات المستخدمة داخل المنظمة.

➢ **التوصيات المالية:**

- رصد موازنة لخطة تطبيق الأمن السيبراني داخل المنظمة..
- توفير الدعم المالي الكافي لشراء الاجهزة الحاسوبية والبرامج والتطبيقات الحديثة.
- تخصيص ميزانية لتطوير البرامج والتطبيقات المستخدمة.
- توفير المخصصات المالية اللازمة للربط الشبكي.
- تخصيص حوافز ومكافآت مناسبة للعاملين في البرنامج وإدارات نظم المعلومات.
- توفير المخصصات المالية اللازمة لبرامج تدريب وتأهيل الموظفين داخليا وخارجيا.

- توفير الدعم المالي المناسب للاستعانة بخبراء في مجال الأمن السيبراني.

➢ **التوصيات العامة:**

- نشر ثقافة الأمن السيبراني بين العاملين داخل المنظمات وبين جميع أفراد المجتمع بشكل عام.
- أهمية توفير البنية التحتية لمشروع الأمن السيبراني.
- توفير الكوادر البشرية المؤهلة والمدربة من أجل تطبيق ناجح للأمن السيبراني.
- توفير اللوائح والتشريعات المنظمة لتطبيق الأمن السيبراني.
- تمكين المرأة بالمشاركة والعمل في مجالات الأمن السبراني.
- تطوير أفضل الممارسات والسياسات والبرامج لحماية الأطفال في العالم السيبراني لمواجهة التهديدات السيبرانية المتزايدة التي تستهدف الأطفال أثناء استخدامهم لشبكة الإنترنت وتعريضهم لجرائم سيبرانية متنوعة بعيداً عن أعين أسرهم.
- إجراء المزيد من الدراسات حول متطلبات تطبيق الأمن السيبراني ومعوقات تطبيقه داخل المنظمات.

4. المراجع

1.4. المراجع باللغة العربية:

البار، عدنان مصطفى، والمرحبي، خالد علي. (2020). أمن المعلومات والأمن السيبراني، ورقة علمية، كلية الحاسبات وتقنية المعلومات، جامعة الملك عبد العزيز، السعودية.

بحيصي، عصام. (2006). تأثير تكنولوجيا المعلومات الحديثة وأثرها على القرارات الإدارية في منظمات لأعمال، مجلة الجامعة الإسلامية) سلسلة الدراسات الإنسانية) ، غزة، فلسطين، مجلد14، العدد الأول، ص155.

جبور، منى الأشقر. (2012). الأمن السيبراني :التحديات ومستلزمات المواجهة .اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني .جامعة الدول العربية: المركز العربي للبحوث القضائية والقانونية، بيروت، أغسطس، ص 27-28.

الجواد، دلال؛ الفتال، حمير. (2008). أمن المعلومات، دار اليازوري للنشر والتوزيع، عمان، الأردن، ص11.

حسنين، رجب عبد الحميد. (2012). أمن شبكات المعلومات الإلكترونية: المخاطر والحلول، - Cybrarians Journal – العدد 30، ص 1-12.

الخالد، أمان. (2008). بناء استراتيجية لأمن المعلومات وليس مجرد شراء أدوات الحماية، مؤسسة اليمامة الصحفية، العدد 14647.

خلف، سامية عبد الرزاق. (2010). التعدي على حرمة الحياة الخاصة باستخدام التكنولوجيا الحديثة، دراسة مقارنة، مجلة دراسات قانونية، بيت الحكمة - بغداد، ص112.

داود، حسن طاهر. (2000). الحاسب وأمن المعلومات، معهد الإدارة العامة، الرياض، ص30.

داود، حسن طاهر. (2000). جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، المملكة العربية السعودية، الرياض، ص23.

داود، حسن طاهر. (2001م). الحاسب وأمن المعلومات؛ معهد الإدارة العامة، المملكة العربية السعودية، الرياض، ص30.

دحماني، سليم. (2018). أثر التهديدات السيبرانية على الأمن القومي للولايات المتحدة الأمريكية، رسالة ماجستير غير منشورة، جامعة محمد بوضياف، المسيلة، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، الجزائر.

زريقة، إسماعيل. (2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع، بحث منشور في مجلة العلوم القانونية والسياسية، المجلد 10، العدد 1، جامعة محمد بومضيف المسيلة، الجزائر.

السالمي، علاء عبد الرزاق، السليطي، خالد إبراهيم. (2008). الإدارة الإلكترونية .دار وائل، عمان، ص305.

علوه، رأفت نبيل. (2006). تقنية في علم المكتبات، مكتبة المجتمع العربي للنشر والتوزيع، عمان، ص160.

غيطاس، جمال محمد. (2007). عصر المعلومات :القادم مذهل أكثر، مركز الخبرات المهنية، القاهرة

المنتشرى. (2020). دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات، جدة، المملكة العربية السعودية.

منصور، رامي وحيد (2016). الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، بحث مقدم إلى مسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية، صادر عن مجلس التعاون لدول الخليج العربية، الأمانة العامة، الرقم الموحد لمطبوعات المجلس 0531/091/ك/2016.

الناظر، سائد محمود. (2005). التعمية وأمن الشبكات، الجزء الأول، الطبعة 1، دار شعاع للنشر والعلوم.

نهاد، خلود. (2013). "أمن وسرية المعلومات وأثرها على الأداء التنافسي"، دراسة تطبيقية على شركتي التأمين العراقية العامة والحمراء للتأمين الأهلية، مجلة الدراسات المحاسبية والمالية، المجلد الثامن، العدد 23، المعهد العالي للدراسات المحاسبية والمالية، جامعة بغداد، العراق، ص 289-296.

الهادي، محمد. (2006). توجهات أمن وشفافية المعلومات في ظل الحكومة الإلكترونية، cybrarians journal، العدد 9، أكاديمية السادات للعلوم الإدارية، مصر، ص25.

2.4. المراجع باللغة الانجليزية:

Alan Calder, (2005). A Business Guide to Information Security, KOGAN PAGE.

Armstrong, Michael, (2006), "A Handbook of Human Resource Management Practice", Kogan Page, 10th ed, U.S.A.

C raigen, D, Diakun, N . & Purse, R. (2014). Defining Cyber Security. Technology Innovation Management Review. Carleton University, October, PP13-22.

Daft, Richard.L, (2001). Organization Theory and Design, 7th ed., South Western College Publishing, U.S.A.

Ndungu, Kandel, (2015) "Information Security Management in Organization, Thesis, Degree Program in Information Technology, Centria University of Applied Science, Finland.p8.

T. Berson, R. Kemmerer, and B. Lampson. (1999) "Draft of Chapter 3 of Realizing the Potential of C4I": Fundamental Challenges, National Academy Press.

U.S. Government, Legal Information Institute, Title 44, Chapter 35, Subchapter 111, §3542, Cornell University Law School. www.law.cornell.edu/uscode/44/3542.html, (accessed: 15 /8 /2016).

Victoria Mahabi, (2010)." Information Security Awareness: System Administrators and End-User Perspectives at Florida State University, degree doctor of philosophy, Florida State University, USA.p44.

Doi: https://doi.org/10.52133/ijrsp.v5.49.8