جامعة المنصورة
كلية التربية

متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود

إعداد

د. مني عبد الله السمحان

أستاذ مشارك كلية الدراسات التطبيقية وخدمة المجتمع
جامعة الملك سعود- المملكة العربية السعودية

مجلة كلية التربية – جامعة المنصورة
العدد ١١١ – يوليو ٢٠٢٠

متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود

د. / مني عبد الله السمحان

أستاذ مشارك كلية الدراسات التطبيقية وخدمة المجتمع

جامعة الملك سعود- المملكة العربية السعودية

مقدمة :

إن قضية أمن وحماية المعلومات تعتبر من أهم قضايا العصر-عصر الثورة الصناعية الرابعة- حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير علي ما تمتلكه من معلومات ، لكن العديد من المعلومات والأنظمة والبني التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بأنواع شتى من الخروقات للمعلومات، كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاتها ، وتختلف هجمات الهاكرز من جهة لأخرى ومن مكان لآخر ومن زمن الي زمن مستخدمة أدوات وآليات اختراق متجددة ومتطورة طول الوقت .

وهذا يؤكد علي أهمية الأمن السيبراني وذلك للحفاظ علي أمن وسلامة الوطن والمواطنين.

وقد أدت نهاية الحرب الباردة إلى بروز العديد من التحديات والتهديدات التي لم يشهدها المجتمع الدولي من قبل، والتي تُعرف بالتهديدات العابرة للحدود التي لا تعترف لا بالحدود أو السيادة الوطنية أو فكرة الدولة القومية، الأمر الذي أدى إلى حدوث تحولات في حقل الدراسات الأمنية والاستراتيجية وكذلك على مستوى الممارسة السياسية .

وفي هذا الاطار استهدفت رؤية المملكة العربية السعودية 2030التطوير 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 الولوية والخدمات والنشطة الحكومية؛ لذلك صدر امر ملكي برقم (٦٨٠١) بإنشاء هيئة باسم (الهيئة الوطنية للأمن السيبراني) في تاريخ (١١ صفر ١٤٣٩ه) الموافق (٣١ أكتوبر ٢٠١٧م) ترتبط بمقام خادم الحرمين الشرفيين، وهي الجهة المختصة بشؤون الأمن السيبراني في المملكة، وتعد مرجع الدولة لحماية امنها الوطني، ومصالحها الحيوية، والبنية التحتية الحساسة فيها، وتوفير خدمات تقنية امنه وطرق دفاعية لحماية أنظمة المعلومات والاتصالات ضد الهجمات الإلكترونية، والحفاظ على سرية وسلامة المعلومات.

(الهيئة الوطنية للأمن السيبراني) :

https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

ومع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصة في القرن الحادي والعشرون وما نتج عنه من تداعيات عديدة بسبب ظهور تهديدات وجرائم سيبرانية أصبحت تشكّل تحدياً كبيراً للأمن القومي وكذلك الدولي، لدرجة أن العديد من الباحثين اعتبر الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية، تبلورت بشكل أساسي في ظهور الأمن السيبراني cyber security كبُعد جديد ضمن أجندة حقل الدراسات الأمنية، وقد اكتسب اهتمامات العديد من الباحثين في هذا المجال.

لقد أصبحت دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي الذي نعايشه في العالم مؤخرًا، حيث يشهد العالم المتقدم بكافة أرجائه تطور كبير لا يمكننا بأي حال أن نغفله، لذا أصبحت تلك الدراسات التكنولوجية في مجال الحوسبة الرقمية مقصد الكثيرين من الدارسين المتميزين حول العالم، ولكن يوجد جانب آخر مظلم لذلك التطور الرقمي الذي نشهده، يمكن أن يجعل كبرى الدول والشركات والمؤسسات التجارية والاقتصادية مهددة بالاختراق، ولعل هذا من أسباب أهمية دراسة الأمن السيبراني، والذي يعمل على حماية البيانات والشبكات والأنظمة الالكترونية من الهجمات والاختراقات التي قد تودي بها وباستقرارها.

ومن هنا تبرز الحاجة إلى ضرورة فهم ماهية الأمن السيبراني ودراسته دراسة علمية مستفيضة من مختلف جوانبه بعمق كمتغير جديد في العلاقات الدولية.

مشكلة البحث :

على الرغم من الإيجابيات الهائلة التي تحققت بفضل تقنية المعلومات، فإن تلك الثورة المعلوماتية المتصاعدة قد صاحبتها في المقابل جملة من الانعكاسات السلبية الخطيرة نتيجة سوء الاستخدام، ومن بين تلك الانعكاسات المستحدثة، ظاهرة الجريمة الرقمية، والتي تصاعدت أخطارها بدورها مما افرز نوعًا جديدًا من الجرائم العابرة للقارات، التي لم تعد أخطارها وأثارها محصورة في نطاق دولة بعينها مما أثار بعض التحديات القانونية أمام الأجهزة المعنية بمكافحة الجريمة.

وقد انتشرت في الآونة الأخيرة كلمة الأمن السيبراني، ومع سماع هذه الكلمة كثيرا من خبراء مجال أمن المعلومات ظهرت علي السطح أسئلة كثيرة منها، ما هو الأمن السيبراني وهل أمن المعلومات جزء من الأمن السيبراني وما الفرق بينهما ؟ وعلى من ينطبق هذا المصطلح وما هي التهديدات التي يحمي منها الأمن السيبراني ؟ وهل تقع على المؤسسات فقط أم على المؤسسات والأفراد وكيفية الحماية من حروب الجيل الرابع .؟

وقد لاحت في الأفق عدة أبعاد فيما يخص الفضاء السيبراني، البعد الأول هو الاقتصادي، فينقسم اقتصاد الإنترنت إلي مجالين رئيسيين، المجال الأول يتعلق بصناعة تكنولوجيا المعلومات والاتصالات (ICT) ، ويشمل تطوير أجهزة وبرمجيات وانتاجها وخدمات أخري، أما المجال الثاني فهو مجال التجارة الإلكترونية من خلال فتح سوق حر علي شبكة الإنترنت. أما البعد الثاني فهو يتعلق بأمن المعلومات فنجد أن العديد من الدول تقوم بتخصيص قيمة كبيرة من ميزانيتها لأجل مجابهة الهجمات السيبراني وتحديث وتطوير أنظمة الأمان لديها. أما البعد الثالث فهو البعد الأمني، وخير مثال علي ذلك هو مركز تكامل استخبارات التهديد السيبراني (CTIIC) بالولايات المتحدة الأمريكية الذي يعمل علي التنسيق بين مختلف أجهزة الأمن الأمريكية الأخري، مثل : مكتب التحقيقات الفيدرالي، وكالة الاستخبارات المركزية، ووكالة الأمن القومي. وكذلك المثال العربي علي ذلك وهو الهيئة الوطنية للأمن السيبراني في المملكة العربية السعودية (أبو زيد،٢٠١٩)

أثر الهجمات السيبرانية على السعودية :

تسبب الهجمات الإلكترونية ضررًا كبيرًا على البنية التحتية ، وفي السعودية تضمنت أبرز الحوادث الرئيسية في هجمات استهدفت في البداية شركة أرامكو السعودية المملوكة للدولة في عام ٢٠١٢ وعطلت نشاط الشركة لمدة شهر في ما يشار إليه بأكبر اختراق في التاريخ .٣٧ وقد تسببت هذه البرمجيات الخبيثة في حدوث خلل مرة أخرى في نوفمبر٢٠١٦ ويناير ٢٠١٧.

كذلك أوضح تقرير Over Security Advisory Council والصادر في ٢٠١٦، أن الهجوم علي شركة أرامكو السعودية قد كلفها تغيير ٥٠٠٠٠ قرص صلب لأجهزتها الحاسوبية، ولم تستطع استخدام الأنترنت لمدة خمسة أشهر تقريبًا، وهذا يعتبر زمناً قياسيًا في الإصلاح، خاصة إذا مأخذنا في الإعتبار إمكانات أرامكو المالية والتقنية؛ وفي عام ٢٠١٣، عانت بنوك الإمارات العربية المتحدة وسلطنة عمان من خسارة بلغت أكثر من ٤٥ مليون دولار أمريكي بسبب واحدة من أكبر عمليات سرقة أجهزة الصراف الآلي الإلكترونية في المنطقة.

هاجم Mamba Ransomware المملكة العربية السعودية في يوليو٢٠١٧ ، وتم استهداف شبكات الشركات داخل المملكة العربية السعودية. ظهرت Mamba Ransomware في عام ٢٠١٦ في الولايات المتحدة الأمريكية وكانت واحدة من الفيروسات الأولى التي لا تشفر الملفات ، ولكن الأقراص الصلبة بأكملها. ويستخدم أداة شرعية Disk Cryptor لتشفير القرص بأكمله .(أبو زيد،٢٠١٩)

وبناء علي هذا يمكن القول أن التحول الرقمي في المملكة العربية السعودية أدي إلى نمو استخدام الإنترنت والتكنولوجيا والمعاملات الإلكترونية لذلك، زادت الهجمات السيبرانية منذ ذلك الحين، مما دفع السعودية لتخصيص جهد أكبر في هذا المجال، ومازال الميدان يحتاج المزيد من الجهود في هذا الاتجاه حفاظا علي أمن المعلومات بالمملكة.

وفي ضوء ماسبق تتحدد مشكلة البحث في محاولة الاجابة عن السؤال التالي :

ما متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود ؟

هدف البحث :

يهدف البحث الي :

معرفة متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود.

أهمية البحث :

تتمثل أهمية البحث في موضوع البحث نفسه ، حيث أن الدراسات التربوية في مجال الأمن السيبراني للمعلومات مازالت محدودة ، كما أن الهجمات الارهابية مازالت مستمرة وقد تتزايد مع التطور التكنولوجي والثورة المعرفية . كما تبدو أهمية البحث في محاولة التوصل الي توصيات ومقترحات تدعم الأمن السيبراني لأنظمة المعلومات الادارية بجامعة الملك سعود.

أداة البحث :

يعتمد البحث علي الاستبانة كأداة لجمع المعلومات من عينة من العاملين بجامعة الملك سعود بالرياض لتعرف وجهة نظرهم حول كيفية تحقيق الأمن السيبراني بالجامعة من خلال المتطلبات الادارية ، والتقنية ، والشرية ، والمادية .

مصطلح البحث :

الأمن السيبراني : ويقصد به :

" جميع الاجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به ، ويشمل كذلك حماية الأجهزة والبيانات "

الاطار النظري والدراسات السابقة :

الدراسات السابقة :

دراسة المعهد العربي للتخطيط (٢٠١٩) مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي

حاولت هذه الدراسة تسليط الضوء على أهمية المخاطر الالكترونية وآثارها الاقتصادية وكيفية إدارتها، وأعطت نماذج دولية لحوادث الإصابة بها. ثم حلّلت وقيّمت أوضاع دول مجلس التعاون الخليجي كنموذج أو دراسة حالة. وهدفت من ذلك الى زيادة الاهتمام بالاستثمار في الأمن الإلكتروني واستدراك الثغرات في التخطيط الاقتصادي لمجابهة هذه المخاطر، وتتصدر دول مجلس التعاون الخليجي دول العالم الأخرى في بعض أنواع الهجمات السيبرانية على الأنشطة الاقتصادية مثل معدلات البرمجيات الخبيثة بالبريد الالكتروني ونسب البريد الالكتروني المؤذي .(Spam) كما تفوق الخسائر الناجمة عن الهجمات الالكترونية في دول المجلس المتوسط العالمي . وعلى الرغم من تحسن أداء دول المجلس في مجال مواجهة الهجمات الالكترونية، إلا أن الدليل العالمي للأمن السيبراني الذي تصدره الأمم المتحدة يشير إلى وجود العديد من الثغرات القانونية والفنية والتنظيمية والتدريبية والتعاونية التي يجب سدها من خلال تحسين الأداء والإكمال والمراجعة للوضع الراهن في هذه الجوانب. ولا تكفي زيادة الإنفاق بمفردها في مواجهة التهديدات وتحقيق الأمن السيبراني في دول المجلس، بل لابد من تحسين الوعي والحوكمة والعمليات لأن هذه المنطقة هي إحدى أكثر مناطق العالم تقدماً في سرعة تبني واعتماد التكنولوجيا الحديثة .

دراسة الشيتى(٢٠١٩) حول تقييم سياسات أمن وخصوصية المعلومات في مؤسسات التعليم بالمملكة العربية السعودية، مع التطبيق علي جامعة القصيم . توصلت الدراسة الي ضرورة وجود برامج توعية الموظفين وتشجيع البحوث في مجال الأمن السيبراني وأهمية تكامل وصحة البيانات في مؤسسات التعليم.

دراسة (El Hissi وآخر ، ٢٠١٨) حاولت الدراسة اقتراح اطار لحوكمة الأمن السيبراني في الجامعات الحكومية بالمغرب ، خلصت الدراسة الي استخدام نظام الأمن السيبراني في المؤسسات الأكاديمية سئؤدى الي فوائد عديدة ادارية ومادية وأكاديمية.

دراسة العتيبى (٢٠١٧) حول دور الأمن السيبراني في تعزيز الأمن الإنساني :

تمثلت مشكلة الدراسة في محاولة الاجابة عن سؤال رئيس : مادور الأمن السيبراني في تعزيز الأمن الانساني ؟

تكون مجتمع الدراسة من العاملين في مجال الأمن السيبراني في شركة أرامكو السعودية فرع منطقة الرياض. عينة الدراسة (٤٠٠) فرد تم اختيارهم عشوائيا ، استخدمت الدراسة المنهج الوصفي التحليلي طبقت استبانة لجمع المعلومات من عينة الدراسة ، كما استخدمت المقابلة

من أهم نتائج الدراسة :

- أن الإجراءات الفنية لحماية الفضاء السيبراني للشركة متوفرة بدرجة كبيرة، حيث يتم قفل ال نظام آلياً في حالة عدم استخدامه لفترة زمنية محددة
- أن الإجراءات التقنية لحماية الفضاء السيبراني الخاص بالشركة متوفرة بدرجة كبيرة، استخدام القياسات الحيوية (بصمة العين – بصمة الإصبع – بصمة الصوت) لمرور المصرح لهم .

أوصي الباحث بضرورة العمل على اتباع الوسائل العلمية والعملية لحفظ الأمن السيبراني للمؤسسات والشركات الحكومية والخاصة ، كما أوصي بالمزيد من التعمق في دراسة الربط ما بين مجال الأمن السيبراني والأمن الإنساني.

دراسة البكري(٢٠١٧) حول أمن المعلومات بالمكتبات الجامعية السودانية، هدفت التعرف علي مخاطر عدم تأمين المعلومات وكيفية تأمينها بالنسبة للمكتبات الجامعية، استخدم البحث المنهج التاريخي ن خلال الاطلاع علي الأدبيات المنشورة وأداة الملاحظة للمكتبات الجامعية بالسودان.

دراسة (Rehman وآخرون ،٢٠١٥) حول واقع أنظمة ادارة الأمن السيبراني في معاهد التعليم العالي بجامعات باكستان ، أوصت بضرورة وجود ادارة للمخاطر الموجودة، ووضع سياسات أمنية لمعالجة هذه المخاطر .

ويبدو أن الدراسات السابقة في مجال الأمن السيبراني مازالت محدودة (علي حد علم الباحثة) الا أن ماتم من أبحاث علمية أو أدبيات نظرية أكد علي أهمية دراسة الأمن السيبراني

من مختلف أبعاده، والدراسة الحالية تسير في نفس الاتجاه لتعزيز فكرة وثقافة الأمن السيبراني خاصة في المجال الجامعي حيث أنها تكاد تكون محدودة جدا .

الأمن السيبراني...مفهومه وأهميته وأهدافه :

مفهوم الأمن السيبراني :

معنى كلمة سيبراني (cyber)

تطلق كلمة" سيبراني "على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والفضاء السيبراني يعني الفضاء الإلكتروني(Cyberspace) ، وهويعني كل ما يتعلق بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالوتسآب، والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها (كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم (https://www.mah6at.net)/

الأمن السيبراني :

- يقصد بالأمن السيبراني " Cyber Security " حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات ويشار إليها " ICT " وذلك اختصار Information and Communication Technologies

والقول بالأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنيًا وتنظيميًا وإداريًا في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع إستغلالها بطريقة غير قانونية ونظامية، وبذلك فإنه يهدف إلى الحفاظ على إستمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال إتباع التدابير والإجراءات اللازمة لحماية البيانات .

الأمن السيبرانى لغويا : الأمن السيبراني مكوّن من لفظتين" :الأمن"، و"السيبراني"

الأمن :هو نقيض الخوف، أي بمعنى السلامة .والأمن مصدر الفعل أَمِنَ أَمْناً وأَمَاناً وأَمَنَةً :أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه .

السيبراني :مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وكلمة "cyber" لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة، حيث تستخدم مجازاً للمتحكم ."governor" وأشار بعض المؤرخين الي أن أصلها يرجع إلى عالم الرياضيات الأمريكي (Norbert Wieners 1894-1964) وذلك للتعبير عن التحكم الآلي

الأمن السيبراني اصطلاحاً :هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يُعرّف بأنه" مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير المضادة المطلوبة."

وهذا ما ذهب إليه الكاتبان Neittaanmäki Pekka, Lehto Martti في كتابهما Cyber Security: Analytics, Technology and Automation، حيث عرفا الأمن السيبراني أنه : "عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة."

بينما عرّفه (إدوارد أمورسو Amoroso Edward) بأنه" :وسائل من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل الأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها، وتوفير الاتصالات المشفرة."...

وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010-2011 عُرّف الأمن السيبراني بأنه" :مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين."

وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني فاعتبرته " جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث." في حين اعتبر الإعلانُ الأوروبي الأمنَ السيبراني أنه" قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات."

وتجدر الإشارة إلى أن الأمن السيبراني مفهوم أوسع من أمن المعلومات، فالأمن السيبراني يهتم بأمن كل ما هو موجود على السايبر من غير أمن المعلومات، بينما أمن المعلومات لا يهتم بذلك، كما أن أمن المعلومات يهتم بأمن المعلومات الفيزيائية" الورقية"، بينما لا يهتم الأمن السيبراني بذلك. (الموسوعة السياسية https://political-encyclopedia.org/dictionary/)

مفاهيم المرتبطة بالأمن السيبراني

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

الفضاء السيبراني :عرفته الوكالة الفرنسية لأمن أنظمة الإعلامANSSI ، بأنه" :فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية ."فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين .

الردع السيبراني : يُعرف الردع السيبراني بأنه" منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية "

الهجمات السيبرانية تعرف بأنها " :فعلاً يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام."

الجريمة السيبرانية :مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها

(الموسوعة السياسية https://political-encyclopedia.org/dictionary/)

وإجمالا يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر (الفضاء السيبراني بصفة عامة) من مختلف الهجمات والاختراقات والتهديدات السيبرانية التي قد تهدد الأمن القومي للدول.

أمن المعلومات " Information Security "

هو حماية بيانات المؤسسة ويعتمد ذلك علي ثلاث محاور رئيسية ويرمز لها " CIA " وهي السرية" Confidentiality " سلامة المعلومة " Integrity " إتاحة المعلومة في أي وقت " Availability " (أحمد عيسى ،٢٠١٩)

وهو عبارة عن مجموع من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تامين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف.

أهداف الأمن السيبراني

من أهم أهداف الأمن السيبراني : (https://ab7as.net)

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

٢- التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.

٣- توفير بيئة أمنة موثوقة للتعاملات في مجتمع المعلومات.

٤- صمود البني التحتية الحساسة للهجمات الإلكترونية.

٥- توفير المتطلبات الأزمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.

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

٧- سد الثغرات في أنظمة امن المعلومات.

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

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

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

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

أهمية الأمن السيبراني :

في عالم اليوم المترابط بواسطة الشبكات ، يستفيد الجميع من برامج الدفاع السيبراني. وتتمثل أهمية الأمن السيبراني فيما يلى :

- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها-تحقيق وفرة البيانات وجاهزيتها عند الحاجةِ إليها
- حماية الأجهزة والشبكات ككّل من الاختراقات لتكون درعٌ واقٍ للبيانات والمعلومات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيقِ مبادئ الأمن السيبراني.
- توفير بيئة عمل آمنة جدًا خلال العمل عبر الشبكة العنكبوتية.

أهمية دراسة الأمن السيبراني :

هناك عدد من الأسباب التي تجعل دراسة الأمن السبراني من أبرز المجالات التي تحتاج لوجود خبراء مؤهلين لحماية أمن الشركات والمؤسسات والدول أيضًا، ومن أبرزها :

١. يشهد سوق العمل حاجة مستمرة لخبراء مجال الأمن السيبراني
٢. بالعمل في مجال الأمن السيبراني يمكن جني الكثير من الأرباح المالية
٣. الخبرة في مجال الأمن السيبراني ستكون غاية لكل مؤسسة مميزة
٤. يشمل الأمن السيبراني كافة المجالات العملية بالرغم من اختلافها وتنوعها
٥. تمكين الدارس من الحصول علي امتيازات فريدة في العمل

أهم المسارات الوظيفية المتاحة بعد دراسة الأمن السيبراني

يشهد هذا المجال اقبال وطلب كبير في شتى المجالات، ولذلك تشير التقارير والإحصاءات العالمية إلى زيادة كبيرة في طلب محترفي الأمن السبراني، حيث أن سوق الأمن السبراني قد نما وتطور في كافة دول العالم بشكل ملحوظ، ففي عام ٢٠٠٤ كان يقدر بـ ٣,٥ مليار دولار، بينما كان في عام ٢٠١٥ يُكلف ٧٥ مليار دولار، ويُتوقع أن يحقق ما يقارب ١٧٠ مليار دولار في عام ٢٠٢٠. . (https://ab7as.net)

ومن المتوقع عقب دراسة الأمن السبراني والحصول على درجة البكالوريوس سيجد الخريج العديد من الفرص الوظيفية المميزة في عدد من المجالات، وتتنوع المسارات الوظيفية التابعة لتلك الدراسة، حيث تشمل: مهندس الدعم السحابي، متخصص دعم تكنولوجيا المعلومات، مهندس الدعم الفني، مطور برامج وتطبيقات.-مسؤول الشبكات.-مسؤول الطب الشرعي الرقمي.

أنواع الجرائم السيبرانية :

تتعدد جرائم الأمن السيبراني ، من أهم هذه الجرائم :

جرائم التعدي على البيانات المعلوماتية ، التعدي على الأنظمة المعلوماتية، إساءة استعمال الأجهزة أو البرامج المعلوماتية، الجرائم الواقعة على الأموال ،الاستغلال الجنسي للقاصرات، التعدي على الملكية الفكرية للأعمال الرقمية، البطاقات المصرفية والنقود الإلكترونية، جرائم تمس المعلومات الشخصية، جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية، جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت، الجرائم المعلوماتية ضد الدولة والسلامة العامة، وجرائم تشفير المعلومات . (https://ab7as.net)

أسباب الجرائم السيبرانية

- الرغبة في جمع المعلومات وتعلمها.
- الاستيلاء على المعلومات والاتجار فيها.
- قهر النظام وإثبات التفوق على تطور وسائل التقنية.
- الحاق الأذى بأشخاص أو جهات.
- تحقيق أرباح ومكاسب مادية.
- تهديد الأمن القومي والعسكري

أسباب تؤكد علي أهمية دراسة الأمن السيبراني :

أنماط الأمن السيبراني :

ينطبق هذا المصطلح على مجموعة متنوعة من السياقات، بدءًا من قطاع الأعمال، وصولًا إلى الحوسبة المتنقلة، وبالإمكان عمومًا تقسيمها إلى عدّة فئات شائعة كما يلي :

(https://www.arageek.com/**)**

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

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

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

الأمن التشغيلي

يشمل العمليات والقرارات التي تتعامل مع أصول البيانات، وتكفل حمايتها.

عناصر الأمن السيبراني: (https://www.mah6at.net/)

حتى يتحقق الهدف من الأمن السيبراني، لا بد من توفر مجموعة من العناصر مع بعضها البعض لتكمل الدور في ذلك، ومن أهم أبعاد وعناصر الأمن السيبراني:

- التقنية :(technology) تشكل التكنولوجيا والتقنية دورًا في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة

بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

- الأشخاص :(People) يستوجب الأمر لزومًا على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانبِ القيام بعمل نسخ احتياطية للبيانات.
- الأنشطة والعمليات :(Process) يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

أبعاد الأمن السيبراني : (https://ab7as.net)

أولا: الأبعاد العسكرية:

تنشا أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشاة النووية، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي إلى كوارث.

ثانيا: الأبعاد السياسية:

تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار امن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها.

ثالثا: الأبعاد الاقتصادية:

يرتبط الأمن السيبراني ارتباطا وثيقا بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة فاغلب الدول تعتمد في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة والمعلومات على المستويات، مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية.

رابعا: الأبعاد القانونية:

ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومن ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا

المجتمع وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد ويقوم الأمن السيبراني في هذا البعد علـــى حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات

آليات (متطلبات) تحقيق الأمن السيبراني (https://www.arageek.com/)

قد تساعدك الخطوات البسيطة أدناه في الحفاظ على مستوى جيّد من الأمان والسلامة السيبرانية:

- **الموثوقيّة :** وتعني استخدام المواقع الموثوق بها عند تقديم معلومـــات شخـــصية، والقاعـــدة الأساسية هي التحقق من عنوان.URL ، وإذا كان الموقع يتضمن https في بدايتـــه، فهـــذا يعني أنه موقع آمن، أمّا إذا كان عنوان URL يحتوي على http بدونs ؛ فيجنّب الحذر من إدخال أيّ معلومات حساسة مثل بيانات بطاقة الائتمان، أو رقم التأمين الاجتماعي.....الخ
- **البريد الاحتيالي:** ويعني عدم مرفقات البريد الإلكتروني أو النقر فوق روابط الرســـائل مـــن المصادر غير المعروفة، إذ إنّ إحدى الطرق الأكثر شيوعًا التي يتعرض فيهـــا الأشـــخاص للسرقة أو الاختراق هي عبر رسائل البريد الإلكتروني المتخفية على أنها مرسلة من شخص موثوق به.
- التحديثات(Always up-to-date) وتعني الحرص دائمًا على تحديث الأجهزة ، فغالبًـــا مـــا تحتوي تحديثات البرامج على تصحيحات مهمة لإصلاح مـــشكلات الأمـــان، وإنّ هجمـــات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحـــدث بـــرامج الأمان.
- **النسخ الاحتياطي:** ويتطلب هذا عمل نسخ احتياطية من الملفات بانتظام لمنع هجمات الأمـــان على الإنترنت

الاطار الميداني :

لتحقيق هدف البحث تم تطبيق الاستبانة علي عينة قوامها (٤٧٨) تمثل نـــسبة حـــوالي (٥%) من المجتمع الأصلي من جميع العاملين بالجامعة وعـــددهم (٩٣٢٧) والجـــدول التـــالي يوضح توزيع أفراد العينة.

جدول (١)

توزيع أفراد عينة البحث وفقا لمتغيري الجنس والمسمي الوظيفي

الجنس	عدد	%	المسمي الوظيفي	عدد	%
ذكور	٢٢٦	٤٧	أكاديمي	١٨٠	٣٨
إناث	٢٥٢	٥٣	اداري	٢٩٨	٦٢
مجموع	٤٧٨	١٠٠	مجموع	٤٧٨	١٠٠

جدول (٢)

توزيع عينة البحث وفقا لمتغيري المؤهل العلمي وسنوات الخدمة

المؤهل العلمي	عدد	%	سنوات الخدمة	عدد	%
ثانوية عامة أو أقل	٢	٠و٤	١-٥	٧٤	١٥و٥
بكالوريوس	١٩١	٤٠	٦-١٠	١١٢	٢٣و٤
ماجستير	١٧٤	٣٦و٤	١١-١٥	١٨٣	٣٨و٣
دكتوراه	١١١	٢٣و٢	١٦-٢٠	١٠٩	٢٢و٨
مجموع	٤٧٨	١٠٠	مجموع	٤٧٨	١٠٠

المعالجة الاحصائية :

- تمت إجراءات المعالجة الإحصائية للبيانات الواردة فى الاستبانة باستخدام برنامج الحزم الاحصائية للعلوم الاجتماعية (Statistical Package for Social Sciences (SPSS)
- تم حساب قيمة كا ٢ لحسن المطابقة لكل مفردة، وذلك للكشف عن الفروق في اختيارات أفراد العينة لبدائل الاستجابة الثلاثة (موافق –غير متأكد –غير موافق) وذلك بتطبيق المعادلة الآتية:

كا ٢= مج (ت – ت م) ٢/ ت م

حيث أ ن ت = التكرار الملاحظ أو التجريبي.

ت م = التكرار المتوقع.

- حساب التكرا رات ونسبتها لكل مفردة.
- حساب التقدير الرقمي لكل مفردة من خلال المعادلة الآتية:

التقدير الرقمي =٣ *تكرار موافق + ٢ *تكرار غير متأكد + ١ *تكرارغير موافق

- حساب الوزن النسبي لكل مفردة، من خلال المعادلة الآتية:

الوزن النسبي = التقدير الرقمي x ١٠٠ / ن

ن = عدد العينة

- ترتب العبارات حسب الوزن النسبي أو الأهمية النسبية لكل منها؛ حيث إن: الأهمية النسبية أو التقدير المئوي= الوزن النسبي / عدد البدائل

نتائج الدراسة :

نتائج المحور الأول: المتطلبات الادارية

جدول (٣) استجابات عينة البحث حول المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني بجامعة الملك سعود (ن=٤٧٨)

م	العبارات	درجة التحقق						الوزن النسبي	الترتيب	قيمة كا٢ ●
		موافق		غير متأكد		غير موافق				
		ك	%	ك	%	ك	%			
١	توجد إدارة خاصة بالأمن السيبراني في الجامعة	٢٤٦	٥١,٥	١٣٤	٢٨	٩٨	٢٠,٥	٢٣١	١٣	٧٤,٧٨
٢	توجد سياسات أمنية لأنظمة المعلومات الإدارية بالجامعة	٣٣١	٦٩,٢	١٤٧	٣٠,٨	٠	٠	٢٦٩	١	٧٠,٨٣
٣	تطبيق الإجراءات الإدارية اللازمة لتحقيق الأمن السيبراني داخل أنظمة المعلومات الإدارية بالجامعة	٣٤١	٧١,٣	١٢٥	٢٦,٢	١٢	٢,٥	٢٦٩	١م	٣٥٠,٧٧
٤	توجد خطة لإدارة مخاطر الأمن السيبراني لأنظمة المعلومات الإدارية في الجامعة	٣٢٨	٦٨,٦	١٣٨	٢٨,٩	١٢	٢,٥	٢٦٦	٣	٣١٧,٦٤
٥	يتم تقييم مخاطر الأمن السيبراني على أنظمة المعلومات الإدارية بشكل دوري	٢٧٧	٥٧,٩	١٨٨	٣٩,٣	١٣	٢,٧	٢٥٥	٨	٢٢٦,٤٥
٦	تلتزم الوحدات الإدارية بالجامعة بالمتطلبات التنظيمية لتحقيق الأمن السيبراني	٢٤٣	٥٠,٨	٢١٤	٤٤,٨	٢١	٤,٤	٢٤٦	١١	١٨٢,٧٩
٧	تطبق متطلبات الأمن السيبراني إدارة الأصول المعلوماتية والتقنية بالجامعة	٢٩٨	٦٢,٣	١٦٤	٣٤,٣	١٦	٣,٣	٢٥٩	٦	٢٤٩,٧٦
٨	تطبق الجامعة متطلبات الأمن السيبراني لحماية البريد الالكتروني	٢٨١	٥٨,٨	١٨٩	٣٩,٥	٨	١,٧	٢٥٧	٧	٢٤٢,١٦
٩	تطبق الجامعة متطلبات الامن السيبراني لإدارة أمن الشبكات	٣٢٣	٦٧,٦	١٤٨	٣١	٧	١,٥	٢٦٦	٣م	٣١٤,٥٧
١٠	تطبق الجامعة متطلبات الامن السيبراني الخاصة بالأجهزة المحمولة والأجهزة الشخصية للموظفين	٢٤٦	٥١,٥	٢١٧	٤٥,٤	١٥	٣,١	٢٤٨	١٠	١٩٨,٧٦
١١	تطبق الجامعة متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجامعة	٣٠٣	٦٣,٤	١٦٤	٣٤,٣	١١	٢,٣	٢٦١	٥	٢٦٧,٧٧
١٢	تطبق الجامعة متطلبات الأمن السيبراني للتشفير لأنظمة المعلومات الإدارية	٢٠١	٤٢,١	٢٦٨	٥٦,١	٩	١,٩	٢٤٠	١٢	٢٢٦,٨٥
١٣	تطبق الجامعة متطلبات الامن السيبراني لإدارة النسخ الاحتياطية للبيانات والمعلومات الإدارية	٢٤٠	٥٠,٢	٢٣٢	٤٨,٥	٦	١,٣	٢٤٩	٩	٢٢١,٥٤

● قيمة كا٢ دالة عند مستوى ٠١و٠

تشير بيانات جدول(٣) الي الدلالة الاحصائية لقيم كا٢ لجميع عبـــارات المحـــور الأول٠ المتطلبات الادارية) كما بينتها استجابات عينة البحث حول امكانية تحقيق الأمن السيبراني مـــن خلال المتطلبات الادارية حيث تتجه الاستجابات الي الاختيار (موافق) وهذا يعني موافقة عينـــة البحث علي المتطلبات الادارية لتحقيق الأمن السيبراني بالجامعة .

كما تشير بيانات الجدول الي عبارات خمس حازت الترتيب الأعلى بين عبارات المحـــور علي التوالي وهي :

- توجد سياسات أمنية لأنظمة المعلومات الإدارية بالجامعة
- تطبيق الإجراءات الإدارية اللازمة لتحقيق الأمن السيبراني داخل أنظمة المعلومات الإداريـــة بالجامعة
- تطبق الجامعة متطلبات الامن السيبراني لإدارة أمن الشبكات
- توجد خطة لإدارة مخاطر الأمن السيبراني لأنظمة المعلومات الإدارية في الجامعة
- تطبق الجامعة متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجامعة

نتائج المحور الثاني: المتطلبات التقنية

جدول (٤)

استجابات عينة البحث حول المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني بجامعة الملك سعود (ن=٤٧٨)

م	العبارات	درجة التحقق						الوزن النسبي	الترتيب	قيمة كا٢●
		موافق		غير متأكد		غير موافق				
		ك	%	ك	%	ك	%			
١	توجد بالجامعة أنظمة حماية أمنية للأجهزة التقنية والحاسوبية	٤٠٩	٨٥,٦	٦٤	١٣,٤	٥	١	٢٨٥	٤	٥٩٧,٧٥
٢	تحدث أنظمـــة وبـــرامج الحاســـب الآلـــي بالجامعة بشكل دوري	٢٦٩	٥٦,٣	٢٠١	٤٢,١	٨	١,٧	٢٥٥	١٣	٢٣٠,١١
٣	تحدث برامج الحماية لأجهزة الحاسب الآلي بالجامعة	٤٦٠	٩٦,٢	١٢	٢,٥	٦	١,٣	٢٩٥	١	٨٥١,١٦
٤	توجد أنظمة حمايـــة للمعلومـــات الـــسرية للمستخدم لأنظمـــة المعلومـــات الإداريـــة بالجامعة	٤٣١	٩٠,٢	٤٧	٩,٨	٠	٠	٢٩٠	٣	٣٠٨,٥
٥	تطبق متطلبات الامـــن الـــسيبراني لإدارة هويات الدخول والصلاحيات	٤٤٠	٩٢,١	٣١	٦,٥	٧	١,٥	٢٩١	٢	٧٤٣,٤
٦	تطبق متطلبات الامن الـــسيبراني لحمايـــة أنظمة المعلومات الإدارية ومعالجة أجهـــزة المعلومات بالجامعة	٢٥٢	٥٢,٧	٢٢١	٤٦,٢	٥	١	٢٥٢	١٦	٢٢٧,٢٥

م	العبارات	درجة التحقق						الوزن النسبي	الترتيب	قيمة كا٢●
		موافق		غير متأكد		غير موافق				
		ك	%	ك	%	ك	%			
٧	توفر الجامعة برامج حماية ضد الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة لأنظمة المعلومات الإدارية على أجهزة الجامعة	٢٨٣	٥٩,٢	١٨٤	٣٨,٥	١١	٢,٣	٢٥٧	١٢	٢٣٧,٩
٨	تطبق متطلبات الأمن السيبراني إدارة الأصول المعلوماتية والتقنية بالجامعة	٢٥٨	٥٤	٢١٣	٤٤,٦	٧	١,٥	٢٥٣	١٤	٢٢٤,٨٢
٩	تطبق الجامعة متطلبات الأمن السيبراني لحماية البريد الالكتروني	٢٩٨	٦٢,٣	١٧٤	٣٦,٤	٦	١,٣	٢٦١	٨	٢٦٩,٥٩
١٠	تطبق الجامعة متطلبات الأمن السيبراني لإدارة أمن الشبكات	٢٩٦	٦١,٩	١٧٧	٣٧,١	٥	١	٢٦١	٨م	٢٦٨,٦٧
١١	تطبق الجامعة متطلبات الامن السيبراني الخاصة بالأجهزة المحمولة والأجهزة الشخصية للموظفين	٢٢٥	٤٧,١	٢٣٠	٤٨,١	٢٣	٤,٨	٢٤٢	١٩م	١٧٥,٠٦
١٢	تطبق الجامعة متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجامعة	٢٩٩	٦٢,٦	١٧٥	٣٦,٦	٤	٠,٨	٢٦٢	٧	٢٧٥,٤
١٣	تطبع الوثائق السرية على طابعة عامة في جهة العمل	١٦٨	٣٥,١	٢١٨	٤٥,٦	٩٢	١٩,٢	٢١٦	٢٦	٥٠,٥٣
١٤	تنقل معلومات خاصة بالعمل للمنزل وتستخدم جهاز الكمبيوتر الخاص بك في المنزل للعمل عليها	٢٦٠	٥٤,٤	١٨٦	٣٨,٩	٣٢	٦,٧	٢٤٨	١٧	١٦٩,٨٢
١٥	عند القيام بحذف ملف من جهاز الكمبيوتر هل يمكن استرداد هذه المعلومات	٢٤٧	٥١,٧	٢٠٨	٤٣,٥	٢٣	٤,٨	٢٤٧	١٨	١٧٩,٧٥
١٦	قمت بتسجيل الدخول إلى حساب العمل باستخدام الكمبيوتر في أماكن عامة مثل ٢٣٥المكتبة، مقهى انترنت أو لوبي فندق	١٦١	٣٣,٧	١٥٨	٣٣,١	١٥٩	٣٣,٣	٢٠٠	٣٠	β٠,٠٣
١٧	تستخدم نفس كلمة المرور لحسابات العمل التي تستخدمها لحساباتك الشخصية في المنزل مثل الفيس بوك ، وتويتر، أو كلمة المرور الشخصية للبريد الألكتروني	٢٣٥	٤٩,٢	١٧٠	٣٥,٦	٧٣	١٥,٣	٢٣٤	٢٣	٨٣,٤٣
١٨	سبق وإن طلب منك رئيسك بالعمل أو أي شخص آخر في عملك كلمة المرور الخاصة بك	١٩٣	٤٠,٤	١٥٣	٣٢	١٣٢	٢٧,٦	٢١٣	٢٧	١٢,٠٥٤
١٩	درجة الأمان الذي تشعر به لجهازك	٢٤٨	٥١,٩	١٨٤	٣٨,٥	٤٦	٩,٦	٢٤٢	١٩	١٣٣,٧٧
٢٠	تعرف ما هو هجوم الاصطياد الإلكتروني وتحديده	٢٣٢	٤٨,٥	٢٠٠	٤١,٨	٤٦	٩,٦	٢٣٩	٢١	١٢٤,١٣
٢١	تعرف كيفية الاحتيال عبر البريد الالكتروني	٢٨٢	٥٩	١٦٩	٣٥,٤	٢٧	٥,٦	٢٥٣	١٤م	٢٠٤,٩٣٣
٢٢	يسمح بالرسائل الفورية (الدردشة) عبر أجهزة وشبكات الجامعة	١٥٣	٣٢	١٤٩	٣١,٢	١٧٦	٣٦,٨	١٩٥	٣١	β٢,٦٧
٢٣	سبق وأن أعطيت كلمة المرور الخاصة بك شخص آخر	١٩٣	٤٠,٤	١١٠	٢٣	١٧٥	٣٦,٦	٢٠٤	٢٩	٢٣,٩٣
٢٤	يسمح بتنزيل البرامج وتثبيتها على جهاز الكمبيوتر الخاص بك في العمل	٢٠١	٤٢,١	١٦٢	٣٣,٩	١١٥	٢٤,١	٢١٨	٢٥	٢٣,٢٨

م	العبارات	درجة التحقق						الوزن النسبي	الترتيب	قيمة كا٢●
		موافق		غير متأكد		غير موافق				
		ك	%	ك	%	ك	%			
٢٥	يمكن استخدام أجهزتك الشخصية مثل هاتفك المحمول لتخزين أو نقل معلومات سرية خاصة بالجامعة	١٩٨	٤١,٤	١٠٤	٢١,٨	١٧٦	٣٦,٨	٢٠٥	٢٨	٣٠,٣٤
٢٦	جهاز الكمبيوتر الخاص بك له قيمة لدى المخترقين حتى يستهدف	١٩٨	٤١,٤	١٩٨	٤١,٤	٨٢	١٧,٢	٢٢٤	٢٤	٥٦,٣
٢٧	درجة الحذر عند فتح مرفق في البريد الإلكتروني	٣٣١	٦٩,٢	١١٥	٢٤,١	٣٢	٦,٧	٢٦٣	٦	٢٩٩,٠٥
٢٨	التحديث تلقائيا في جهاز الكمبيوتر الخاص بك	٣٢٠	٦٦,٩	١٢١	٢٥,٣	٣٧	٧,٧	٢٥٩	١١	٢٦٥,١٦
٢٩	عند تهيئة قرص صلب أو محو ملفات داخل القرص الصلب هل المعلومات المحفوظة وبشكل دائم تفقد	٢٢٢	٤٦,٤	٢٢٢	٤٦,٤	٣٤	٧,٢	٢٣٩	٢١م	١٤٧,٨٨
٣٠	تعرف كيف تخبر إذا تعرض جهازك لجهوم أو تصيد	٣٠٨	٦٤,٤	١٤٧	٣٠,٨	٢٣	٤,٨	٢٦٠	١٠	٢٥٦,٣٢
٣١	تعرف بمن تتصل في حالة حدوث اختراق أو اعتداء	٣٣٢	٦٩,٥	١٢٩	٢٧	١٧	٣,٦	٢٦٦	٥	٣٢٠,٠٤

● قيمة كا٢ دالة عند مستوى ٠١و٠ β قيم كا٢ غير دالة

تشير بيانات جدول (٤) الي الدلالة الاحصائية لقيم كا٢ لجميع عبارات المحور الثاني (المتطلبات التقنية) كما بينتها استجابات عينة البحث حول امكانية تحقيق الأمن السيبراني من خلال المتطلبات التقنية ،حيث تتجه الاستجابات الي الاختيار موافق، ماعدا العبارتين (١٦، ٢٢) حيث أن قيم كا٢ غير دالة احصائيا ، وتتجه استجابات عينة البحث الي عدم الموافقة

- عبارة (١٦) قمت بتسجيل الدخول إلى حساب العمل باستخدام الكمبيوتر في أماكن عامة مثل المكتبة، مقهى انترنت أو لوبي فندق
- عبارة (٢٢) يسمح بالرسائل الفورية (الدردشة) عبر أجهزة وشبكات الجامعة

كما تشير بيانات الجدول الي عبارات خمس حازت الترتيب الأعلي بين عبارات المحور علي التوالي وهي :

- تحدث برامج الحماية لأجهزة الحاسب الآلي بالجامعة
- تطبق متطلبات الأمن السيبراني لدارة هويات الدخول والصلاحيات
- توجد أنظمة حماية للمعلومات السرية للمستخدم لأنظمة المعلومات الادارية بالجامعة
- توجد بالجامعة أنظمة حماية أمنية للأجهزة التقنية والحاسوبية
- تعرف بمن تتصل في حالة حدوث اختراق أو اعتداء

نتائج المحور الثالث: المتطلبات البشرية

جدول (٥)

استجابات عينة البحث حول المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني بجامعة الملك سعود (ن=٤٧٨)

م	العبارات	درجة التحقق						الوزن النسبي	الترتيب	قيمة كا٢●
		موافق		غير متأكد		غير موافق				
		ك	%	ك	%	ك	%			
١	تقوم الجامعة بتوعية الموظفين والإداريين والأكاديميين بأهمية تطبيق الأمن السيبراني	٣٢٩	٦٨,٨	١٢٨	٢٦,٨	٢١	٤,٤	٢٦٤	٢	٣٠٦,٩٣
٢	تدرب الجامعة الموظفين والإداريين والأكاديميين على متطلبات تحقيق الأمن السيبراني	٣١٨	٦٦,٥	١٤٢	٢٩,٧	١٨	٣,٨	٢٦٣	٣	٢٨٥,٢٦
٣	تؤهل الجامعة الموارد البشرية القائمة على تقنية المعلومات في مجال تطبيق الامن السيبراني	٢٦٦	٥٥,٦	١٩٦	٤١	١٦	٣,٣	٢٥٢	٤	٢٠٨,٧٩
٤	توفر الجامعة الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات الإدارية	٣٣٥	٧٠,١	١٣١	٢٧,٤	١٢	٢,٥	٢٦٨	١	٣٣٤,٩٥
٥	تقيم الجامعة لقاءات دورية للمختصين بتطبيق الامن السيبراني لتعريفهم بالمستجدات في المجال	٢٤٢	٥٠,٦	٢١٩	٤٥,٨	١٧	٣,٦	٢٤٧	٥	١٩٢,٣٨
٦	تم توقيعك على بند (المحافظة على سرية المعلومات) قبل البدء في العمل بالجامعة	٢١٦	٤٥,٢	٢١٦	٤٥,٢	٤٦	٩,٦	٢٣٦	٨	١٢٠,٩٢
٧	يتلقى الموظف قبل البدء في عمله توضيح بالمهام والمسؤوليات ذات العلاقة لأمن أنظمة المعلومات الإدارية	١٩٦	٤١	١٠٩	٢٢,٨	١٧٣	٣٦,٢	٢٠٥	٩	٢٥,٥١
٨	يتم تذكير الموظف أثناء عمله ومن وقت لآخر بهذه المهام والمسؤوليات مع تبليغه بكل جديد	٢٤٠	٥٠,٢	١٩٦	٤١	٤٢	٨,٨	٢٤١	٧	١٣٥,٦٨
٩	توجد إجراءات واضحة لإدارة الأصول المعلوماتية التي بعهدة الموظف كالأجهزة المحمولة	٢٢٦	٤٧,٣	٢٢٥	٤٧,١	٢٧	٥,٦	٢٤٢	٦	١٦٤,٨٧

● قيمة كا٢ دالة عند مستوى ٠,٠١

تشير بيانات جدول(٥) الي الدلالة الاحصائية لقيم كا٢ لجميع عبارات المحور الثالث (المتطلبات البشرية) كما بينتها استجابات عينة البحث حول امكانية تحقيق الأمن السيبراني من خلال المتطلبات البشرية حيث تتجه الاستجابات الي الاختيار (موافق) وهذا يعني موافقة عينة البحث علي المتطلبات البشرية لتحقيق الأمن السيبراني بالجامعة .

كما تشير بيانات الجدول الي عبارات خمس حازت الترتيب الأعلي بين عبارات المحور علي التوالي وهي :

- توفر الجامعة الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات الإدارية.
- تقوم الجامعة بتوعية الموظفين والإداريين والأكاديميين بأهمية تطبيق الأمن السيبراني.
- تدرب الجامعة الموظفين والإداريين والأكاديميين على متطلبات تحقيق الأمن السيبراني.
- تؤهل الجامعة الموارد البشرية القائمة على تقنية المعلومات في مجال تطبيق الامن السيبراني.
- تقيم الجامعة لقاءات دورية للمختصين بتطبيق الامن السيبراني لتعريفهم بالمستجدات في المجال.

وهذا يعني أن هذه العبارات كفيلة بتحقيق الأمن السيبراني لأنظمة المعلومات الادارية بالجامعة من حيث كونها متطلبات بشرية لا غني عنها ، وهذا لا يعني اهمال المتطلبات الأخرى التي أفاد بها عينة البحث كما وردت استجاباتها في الجدول (٥)

نتائج المحور الرابع: المتطلبات المادية

جدول (٦)

استجابات عينة البحث حول المتطلبات المادية اللازمة لتحقيق الأمن السيبراني بجامعة الملك سعود (ن=٤٧٨)

م	العبارات	درجة التحقق						الوزن النسبي	الترتيب	قيمة كا٢●
		موافق		غير متأكد		غير موافق				
		ك	%	ك	%	ك	%			
١	تمتلك الجامعة نظام حماية عالي المستوى للأمن السيبراني	٣١٧	٦٦,٣	١٥٢	٣١,٨	٩	١,٩	٢٦٤	٢	٢٩٨,٢
٢	توفر الجامعة المتطلبات المادية اللازمة لتحقيق الامن السيبراني	٢٣٠	٤٨,١	٢٢٦	٤٧,٣	٢٢	٤,٦	٢٤٤	٩	١٧٧,٦١
٣	توفر الجامعة نظام حماية عالي المستوى لأنظمة المعلومات الإدارية	٢٨٥	٥٩,٦	١٨٠	٣٧,٧	١٣	٢,٧	٢٥٧	٧	٢٣٦,١٩
٤	تزود الجامعة منسوبيها بأجهزة حديثة ومتطورة لإدارة نظام المعلومات الإدارية بها	٢٤٤	٥١	٢١٧	٤٥,٤	١٧	٣,٦	٢٤٧	٨	١٩٣
٥	توفر الجامعة لأجهزة تقنية المعلومات الصيانة الدورية والمستمرة الضرورية لتحقيق الأمن السيبراني	٣٢٤	٦٧,٨	١٢٦	٢٦,٤	٢٨	٥,٩	٢٦٢	٣	٢٨٥,٤١
٦	تحدث الجامعة برامج التطبيقات الحاسوبية لمنسوبيها باستمرار	٤٣٤	٩٠,٨	٢٧	٥,٦	١٧	٣,٦	٢٨٧	١	٧١٠,٥٤
٧	تعمل الجامعة على تجديد أجهزة الحاسب الآلي لمنسوبيها	٢٢٨	٤٧,٧	١٢٥	٢٦,٢	١٢٥	٢٦,٢	٢٢٢	١١	٤٤,٤
٨	توفر الجامعة الدعم التقني اللازم لمنسوبيها لمعالجة المشكلات الطارئة	٣٢٤	٦٧,٨	١٠٨	٢٢,٦	٤٦	٩,٦	٢٥٨	٦	٢٦٧,٣٣
٩	تمتلك الجامعة برامج حديثة لتوفير الحماية والأمن السيبراني لأنظمة المعلومات الإدارية	٣٠١	٦٣	١٦٤	٣٤,٣	١٣	٢,٧	٢٦٠	٥	٢٦٠,٤٩
١٠	تمتلك الجامعة نظام حوكمة تقني لتوفير الامن السيبراني للتعاملات الإلكترونية	٢١٥	٤٥	٢٥٤	٥٣,١	٩	١,٩	٢٤٣	١٠	٢١٧,٥٤
١١	تمتلك الجامعة نظام شبكي آمن لتبادل المعلومات الإدارية	٣٠٦	٦٤	١٦٤	٣٤,٣	٨	١,٧	٢٦٢	م٣	٢٧٨,٨٨

● قيمة كا٢ دالة عند مستوى ٠,٠١

تشير بيانات جدول(٦) الي الدلالة الاحصائية لقيم كا٢ لجميع عبارات المحور الرابع (المتطلبات المادية) كما بينتها استجابات عينة البحث حول امكانية تحقيق الأمن السيبراني من خلال المتطلبات المالية حيث تتجه الاستجابات الي الاختيار (موافق) وهذا يعنى موافقة عينة البحث علي المتطلبات المادية لتحقيق الأمن السيبراني بالجامعة .

كما تشير بيانات الجدول الي عبارات خمس حازت الترتيب الأعلى بين عبارات المحور علي التوالي وهي :

- تحدث الجامعة برامج التطبيقات الحاسوبية لمنسوبيها باستمرار
- تمتلك الجامعة نظام حماية عالي المستوى للأمن السيبراني
- توفر الجامعة لأجهزة تقنية المعلومات الصيانة الدورية والمستمرة لتحقيق الأمن السيبراني
- تمتلك الجامعة نظام شبكي آمن لتبادل المعلومات الإدارية
- تمتلك الجامعة برامج حديثة لتوفير الحماية والأمن السيبراني لأنظمة المعلومات الإدارية

وهذا يعني أن هذه المتطلبات ضرورية بدرجة أكبر لحماية أنظمة المعلومات الادارية بالجامعة تحت مظلة المتطلبات المالية كما أشار اليها أفراد عينة البحث ، هذا اضافة الي المتطلبات المالية الأخرى التي تم ذكرها في الجدول (٦)

جدول (٧)

العبارات التي حازت الترتيب الأول ضمن الخمس الأوائل فى محاور الاستبانة الأربعة وفقا للوزن النسبي والتقدير المئوي

م	العبارة	الوزن النسبي	التقدير المئوي %	الترتيب
١	تحدث برامج الحماية لأجهزة الحاسب الآلي بالجامعة	٢٩٥	٣و٩٨	١
٢	تطبق متطلبات الأمن السيبراني لإدارة هويات الدخول والصلاحيات	٢٩١	٩٧	٢
٣	توجد أنظمة حماية للمعلومات السرية للمستخدم لأنظمة المعلومات الإدارية بالجامعة	٢٩٠	٦و٩٦	٣
٤	تحدث الجامعة برامج التطبيقات الحاسوبية لمنسوبيها باستمرار	٢٨٧	٧و٩٥	٤
٥	توجد بالجامعة أنظمة حماية أمنية للأجهزة التقنية والحاسوبية	٢٨٥	٩٥	٥
٦	توجد سياسات أمنية لأنظمة المعلومات الإدارية بالجامعة	٢٦٩	٦و٨٩	٦
٧	تطبيق الإجراءات الإدارية اللازمة لتحقيق الأمن السيبراني داخل أنظمة المعلومات الإدارية بالجامعة	٢٦٩	٦و٨٩	٦ مكرر
٨	توفر الجامعة الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات الإدارية	٢٦٨	٣و٨٩	٨
٩	توجد خطة لإدارة مخاطر الأمن السيبراني لأنظمة المعلومات الإدارية في الجامعة	٢٦٦	٦و٨٨	٩
١٠	تعرف بمن تتصل في حالة حدوث اختراق أو اعتداء	٢٦٦	٦و٨٨	٩مكرر
١١	تطبق الجامعة متطلبات الامن السيبراني لإدارة أمن الشبكات	٢٦٦	٦و٨٨	٩مكرر
١٢	تقوم الجامعة بتوعية الموظفين والإداريين والأكاديميين بأهمية تطبيق الأمن السيبراني	٢٦٤	٨٨	١٢
١٣	تمتلك الجامعة نظام حماية عالى المستوى للأمن السيبراني	٢٦٤	٨٨	١٢مكرر
١٤	تدرب الجامعة الموظفين والإداريين والأكاديميين على متطلبات تحقيق الأمن السيبراني	٢٦٣	٦ز٨٧	١٤
١٥	توفر الجامعة لأجهزة تقنية المعلومات الصيانة الدورية والمستمرة الضرورية لتحقيق الأمن السيبراني	٢٦٢	٣و٨٧	١٥
١٦	تمتلك الجامعة نظام شبكي آمن لتبادل المعلومات الإدارية	٢٦٢	٣و٨٧	١٥مكرر
١٧	تمتلك الجامعة برامج حديثة لتوفير الحماية والأمن السيبراني لأنظمة المعلومات الإدارية	٢٦٠	٦و٨٦	١٧
١٨	تطبق الجامعة متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجامعة	٢٥٥	٨٥	١٨
١٩	تؤهل الجامعة الموارد البشرية القائمة على تقنية المعلومات في مجال تطبيق الامن السيبراني	٢٥٢	٨٤	١٩
٢٠	تقيم الجامعة لقاءات دورية للمختصين بتطبيق الامن السيبراني لتعريفهم بالمستجدات في المجال	٢٤٧	٣و٨٢	٢٠

توضح بيانات الجدول (٧) أن نسب التقدير المئوي للوزن النسبي للعبارات العشرين تراوحت بين (٣و٨٢% – ٣و٩٨ %) وهي نسب مرتفعة تعكس أهمية هذه العبارات كواقع

يتحقق في الجامعة (كما أقرت بذلك عينة البحث) بالإضافة الي كونها متطلبات ضرورية لحمايـــة أنظمة المعلومات الادارية بالجامعة

كما تشير قيم الوزن النسبي والتقدير المئوي لعبارات الجدول أن جامعة الملك سعود تمتلك أدوات هامة تضمن حماية أنظمة المعلومات الادارية بالجامعة ، ومن ثم يؤكد البحث علي أهمية الأخذ الاستمرار في حماية أنظمة المعلومات من خلال هذه المتطلبات التي أقر بوجودهـــا أفـــراد **عينة البحث.**

من آليات (متطلبات) تحقيق الأمن السيبراني

كيفية تحقيق الأمن السيبراني :

تعليمات ضرورية الي المسئولين والعاملين في مجال أنظمة المعلومات الادارية :

قد تساعد التعليمات التالية في الحفاظ على مستوى جيّد من الأمان والسلامة السيبرانية:

- عمل نسخ احتياطية لملفات المعلومات بانتظام لمنع هجمات الأمان على الإنترنت .
- استخدام المواقع الموثوق بها عند تقديم معلومات شخصية
- عدم فتح مرفقات البريد الإلكتروني أو النقر فوق روابط الرسائل من المصادر غير المعروفة
- الحرص دائمًا على تحديث الأجهزة فغالبًا ما تحتوي تحديثات البرامج على تصحيحات مهمـــة لإصلاح مشكلات الأمان، وإنّ هجمات المخترقين الناجحة تتركز على الأجهزة القديمة بنسبة كبرى، والتي لا تملك أحدث برامج الأمان.

توصيات البحث:

- التأكيد علي ضرورة اهتمام جامعة الملك سعود بمتطلبات حماية أنظمة المعلومات الاداريـــة بالجامعة كما اشار البحث اليها في جدول (٧) حيث أقر بأهميتها أفراد عينة البحث
- إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في بالمملكة
- تشجيع بحوث ودراسات الأمن السيبراني في أطروحات الماجستير والدكتوراه
- تشجيع مجالات البحث العلمي والابتكارفي مجال الأمن السيبراني
- توعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية الاحترافيـــة لـــديهم وإرســـاء بنية تحتية للدخول إلي مجال صناعة البرمجيات العالمية والقـــدرة علـــي منافـــسة المنـــتج المستورد

- تشجيع مؤسسات المجتمع المدني والتأكيد علي دورها الفعّال في التعامل مع الاستخدام غير الآمن لتكنولوجيا المعلومات، وذلك من خلال الأنشطة العلمية ونشر ثقافة الاستخدام الآمن لشبكة الانترنت والتطبيقات الرقمية الحديثة.
- تشجيع الاستثمار في مجال الأمن السيبراني وينقسم الاستثمار لجانبين، الأول توطين التكنولوجيا والبني التحتية السيبرانية، الثاني تطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة علي بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها.
- اجراء مزيد من الدراسات العلمية حول قضية أمن المعلومات بمختلف مؤسسات المملكة عامة ، ومجال التعليم بشكل خاص
- عقد دورات تدريبية مستمرة للعاملين في مجال المعلومات

مصادر البحث

١. أبو زيد ، عبد الرحمن عاطف (٢٠١٩) الأمن السيبراني في الوطن العربي .. دراسة حالة المملكة العربية السعودية المركز العربي للبحوث والدراسات علي الموقع بتاريخ ٢٠٢٠/٤/٦: http://www.acrseg.org/list.aspx?r=24734

٢. البكري ، يوسف الشيخ (٢٠١٧) أمن المعلومات بالمكتبات الجامعية السودانية بالإشارة الي مكتبتي جامعة النيلين وجامعة وادى النيل، في المؤتمر الثالث والعشرون لجمعية المكتبات الخاصة، قطر

٣. أحمد عيسى : بوابة أخبار اليوم العدد الأسبوعي الأربعاء، ١٨ سبتمبر ٢٠١٩ – ٠٢:٠٤ م https://akhbarelyom.com/news/newdetails

٤. الشيتي، إيناس ابراهيم(٢٠١٩) تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية بالمملكة العربي السعودية دراسة تطبيقية علي جامعة القصيم ، ماجستير غير منشورة، جامعة القصيم

٥. العتيبي،، عبد الرحمن بن بجاد (٢٠١٧) دور الأمن السيبراني في تعزيز الأمن الإنساني أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية

٦. –الهيئة الوطنية للأمن السيبراني : المملكة علي الموقع https://ega.ee/wp-content/uploads/2019/03/Essential-Cybersecurity-Controls.pdf

٧. الموسوعة السياسية بتاريخ ٢٠٢٠/٤/٦ علي الموقع https://political-encyclopedia.org/dictionary/

٨. المعهد العربي للتخطيط (٢٠١٩) مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي علي الموقع :
https://www.researchgate.net/institution/Arab_Planning_Institute2

9. El Hissi, Y.& Arezki, S.(2018).Conceptualization of an Information System Governance Model Dedicated to the Governance of Scientific Research in Moroccan University,2018 4th International Conference on Computer and Technology Applications.
10. Rehman, H.,Masood ,A.& Cheema ,A.(2013). Information Security Management in Academic Institutes of Pakistan,2nd .National Conference of Information Assurance(NCIA)

مواقع نت :

- https://ab7as.net
- https://www.arageek.com/
- What is Cyber-Security? ، من موقع: usa.kaspersky.com ، اطّلع عليه بتاريخ ٤-٢-٢٠١٩
- What is cyber security? What you need to know ، من موقع: us.norton.com ، اطّلع عليه بتاريخ ٤-٢-٢٠١٩

مصادر اضافية :

- محمود عزت،(٢٠١٨) الفضاء السيبراني وتحديات الأمن المعلوماتي العربي، المجلة العربية العدد ٤٩٨، أبريل ٢٠١٨
- Ivanov Anton, Orkhan Mamedov. The Return of Mamba Ransomware Secure list - Information about Viruses, Hackers and Spam. N.p., 09 Aug. 2017. Web. 13 Sept. 2017
- https://securelist.com/thereturn-ofmamba-ransomware/79403
- (https://www.easyunime.com/advice/) 2019