NTU Journal for Administrative and Human Sciences (2024) 4 (4) : 157 - 180
DOI: https://doi.org/10.56286/ntujahs.v4i4

IRAQI Academic Scientific Journals

JAHS NTU

P-ISSN: 2789-1240 E-ISSN:2789-1259
NTU Journal for Administrative and Human Sciences
Available online at: https://journals.ntu.edu.iq/index.php/NTU-JMS/index

Assessing Cybersecurity Awareness: A survey study at the College of Administration and Economics – University of Mosul

Hani Ramadhan Allaw Alkhaled
University of Mosul
College of Administration and Economics

Article Information

Received: 01.04, 2024
Accepted: 28, 04, 2024
Published online: 01, 12, 2024

Corresponding author:
Hani Ramadhan Allaw Alkhaled
University of Mosul
College of Administration and Economics
Department of Management Information Systems
Hani_alnaimi@uomosul.edu.iq

Key Words:
cybersecurity, cyber-attacks.

A B S T R A C T

Cybersecurity awareness plays a vital role in protecting individuals and organizations from cyber-attacks. The research aims to evaluate the level of awareness of cybersecurity and the readiness of the study-community at the College of Administration and Economics/ University of Mosul to take actions that would prevent or reduce electronic risks and cyber-attacks. The study adopted the descriptive analytical method. A questionnaire survey was used to collect data for this study. The sample size was 100 respondents distributed between teachers and employees with different academic qualifications and years of service. Several statistical methods were used to analyze the data, such as arithmetic means and standard deviations to determine the level of awareness of cybersecurity among the answers of the sample studied, and to conduct One-Way ANOVA tests between the variables of the study and determine the differences in the level of awareness of cybersecurity between groups of one variable. The study concluded that there is a good level of awareness of cybersecurity and electronic safety among the members of the College of Administration and Economics at the University of Mosul. The results of the variance analysis showed that there are no statistically significant differences in the level of awareness of cybersecurity among the college's members due to the variables of gender, class, academic qualification and years of service.

THIS IS AN OPEN ACCESS ARTICLE UNDER THE CC BY LICENSE:
https://creativecommons.org/licenses/by/4.0/

تقييم الوعي بالأمن السيبراني: دراسة مسحية في كلية الإدارة والاقتصاد–جامعة الموصل

م.م هاني رمضان علو الخالد
جامعة الموصل
كلية الإدارة والاقتصاد
Hani_alnaimi@uomosul.edu.iq

المستخلص:

يلعب الوعي بالأمن السيبراني دورًا حيويًا في حماية الأفراد والمؤسسات من الهجمات السيبرانية. يهدف البحث الى تقييم مستوى الوعي بالأمن السيبراني ومدى استعداد مجتمع الدراسة في كلية الإدارة والاقتصاد/ جامعة الموصل لاتخاذ الإجراءات التي من شأنها منع او الحد من المخاطر الالكترونية والهجمات السيبرانية. اعتمدت الدراسة الأسلوب الوصفي التحليلي، تم استخدام استمارة استبيان لجمع البيانات والمعلومات الخاصة بالدراسة، وكان حجم العينة 100 مستجيب موزعين بين تدريسين وموظفين بمؤهل علمي وسنوات خدمة مختلفة. واستخدمت عدة اساليب احصائية لتحليل البيانات، كالأوساط الحسابية والانحرافات المعيارية لمعرفة مستوى الوعي بالأمن السيبراني بين إجابات العينة المبحوثة، وأجراء اختبارات تحليل التباين الأحادي One Way ANOVA بين متغيرات الدراسة وتشخيص مستوى الفروقات بمستوى الوعي بالأمن السيبراني بين مجموعات المتغير الواحد. خلصت الدراسة الى انه يوجد وعي بمستوى جيد بالأمن السيبراني وإجراءات السلامة الالكترونية بين منتسبي كلية الإدارة والاقتصاد في جامعة الموصل، كذلك كانت نتائج تحليل التباين الأحادي بانه لا توجد فروقات معنوية ذو دلالة إحصائية بمستوى الوعي بالأمن السيبراني بين منتسبي الكلية تعزى الى متغيرات الجنس والصفة والمؤهل العلمي وسنوات الخدمة.

الكلمات المفتاحية: الامن السيبراني، الهجمات السيبرانية.

المقدمة : ي عصر التكنولوجيا الرقمية المتقدمة والربط الشبكي، أصبحت شبكة الانترنت فضاءً مفتوحاً للأعمال والتفاعلات الاجتماعية، حيث تتجاوز حدود الزمان والمكان لتربط العالم بشكل لم يسبق له مثيل. ومع تزايد هذا الاستخدام والاعتماد على الإنترنت، أصبح الوعي بالأمن السيبراني أمرًا ضروريًا لضمان سلامة المعلومات والأجهزة المستخدمة في تخزين المعلومات. إن مستخدمي الإنترنت الذين يتصرفون بإهمال أو بشكل سيئ يزيدون من احتمالية وقوع هجوم أمني على أنظمة المعلومات التي يستخدمونها (Huraj et al., 2023). أصبحت طبيعة التهديدات السيبرانية اليوم أكثر تعقيدًا وغير مسبوقة من حيث النطاق والمهارة والتكرار والقدرة على مهاجمة الأهداف، ويمكن أن تؤدي أيضًا إلى خسائر مالية فادحة (Albrechtsen, 2007). لقد دعى العديد من الباحثين إلى اتخاذ بعض الإجراءات العاجلة للتوعية بالأمن السيبراني لأنه أحد أهم متطلبات مجتمع الإنترنت اليوم (Furnell, 2008; Rezgui and Marks, 2008; Shaw et al., 2009). لا تهدف دراسة "الوعي بالأمن السيبراني" الى إثارة المخاوف بين مستخدمي الإنترنت، بل لإكسابهم معرفة بطبيعة الهجمات السيبرانية ومهارة بطرق التعامل معها (Choo, 2011).

ازداد الاهتمام بمفهوم الأمن السيبراني مع زيادة توجه العالم والعاملين نحو الكمبيوتر والأنظمة الحاسوبية والشبكة العنكبوتية وتعتبره جامعة هارفرد "الذراع الرابعة للجيوش الحديثة". نظراً لتكرار هجمات القرصنة على أطر البيانات في المدارس والكليات، فمن الضروري أن يكون المنتسبين ذوي العلاقة على دراية بعواقب وتحديات الأمن السيبراني والجرائم السيبرانية (Alharbi & Tassaddiq, 2021). ويأتي الاهتمام بالأمن السيبراني مع زيادة الخسائر الناتجة عن الهجمات الإلكترونية، وما يعنيه ذلك من تهديدات على امن الدول، وعلى السلم والأمن الدوليين. فمن المتوقع أن تصل الأضرار الناجمة عن جرائم الإنترنت إلى ما يقدر بنحو ١٠.٥ ترليون دولار بحلول العام ٢٠٢٥ (Borrett and Corbineau,2021).

تعتبر المشكلة الأساسية في البحث هي نقص المعلومات حول وعي المنتسبين بالأمن السيبراني وما هي الاستعدادات والإجراءات التي يستطيع المنتسبين اتخاذها حال وقوع تهديد سيبراني. يهدف البحث الى تقييم الوعي بالأمن السيبراني بين منتسبي كلية الإدارة والاقتصاد كجزء من مؤسسة أكبر وهي جامعة الموصل كذلك معرفة الفروقات الفردية بين افراد العينة من ناحية الوعي بالأمن السيبراني تبعاً للجنس والصفة والمؤهل العلمي وسنوات الخدمة. حيث تمثل الجامعات مركزًا للبحث والتطوير وتخزين المعلومات الحساسة الخاصة بالمنتسبين وهي بالتالي عرضة للاختراقات والتهديدات السيبرانية، ان تقييم مدى استعدادهم للتعامل مع التحديات السيبرانية او تجنبها يمكن أن يلعب دورًا مهماً في منع وقوع الهجمات. ينقسم البحث لأربعة محاور أساسية، المحور الأول منهجية البحث، أما المحور الثاني فيشمل على إطار نظري لمفهوم الأمن السيبراني وأهمية دراسته وماهم معاييره، في حين تضمن المحور الثالث على الجانب

العملي الميداني من تحليل بيانات العينة موضوع الدراسة والاجابة على فرضيات الدراسة، وجاء المحور الرابع بالاستنتاجات والمقترحات.

المحور الأول: منهجية البحث

أولا: مشكلة البحث: تكمن المشكلة الرئيسية في الازدياد الكبير بمستوى الهجمات السيبرانية حول العالم والذي يستهدف اغلب المؤسسات المرتبطة بالأنترنت سواءاً الحكومية منا وغير الحكومية حيث بلغت خسائر الهجمات السيبرانية في العالم في العام 2023 وبحسب صحيفة الكارديان البريطانية (2024) عن مقالها "عودة عصابات برامج الفدية في العام الماضي" مايقارب 1.1 مليار دولار يدفعها الضحايا على شكل فدية للمهاجمين. بالإضافة الى قلة المعلومات لدى الكلية عن مستوى وعي اغلب منتسبي الكلية بمفهوم الأمن السيبراني والتهديدات الالكترونية ومستوى الجهوزية للتعامل مع تلك التهديدات. كما تعد نتائج البحث ضرورية من اجل تطوير استراتيجيات فعالة لتحسين وتوعية المنتسبين بأهمية الأمن السيبراني وتنفيذ ممارسات وقائية للوصول الى أفضل أداء الكتروني عبر الفضاء الرقمي.

ثانياً: أهمية البحث: إن تقييم الوعي بالأمن السيبراني في كلية الإدارة والاقتصاد في جامعة الموصل يمكن أن يساهم في الكشف عن الثغرات الأمنية ونقاط الخلل والضعف وتشخيص اهم الاحتياجات لتجاوز تلك الثغرات. كما يمكن لنتائج البحث أن تساعد في تحسين الوعي بالأمن السيبراني بين منتسبي الكلية وتزويدهم بالمعرفة الأساسية والمهارات اللازمة للتعامل مع التهديدات السيبرانية قبل وقوعها. وبالتالي، سيكون للبحث تأثير إيجابي على حماية البيانات والمعلومات الحساسة وضمان استدامة بيئة التعلم والعمل الالكتروني.

ثالثاً: اهداف البحث: تنقسم اهداف البحث في جانبية النظري والعملي من حيث تلخيص مفهوم الأمن السيبراني والتعرف على اهم ابعاده وعناصره والإجابة على فروض الدراسة قيد البحث. وتمثلت اهم اهداف البحث بالآتي:

1. تقييم مستوى الوعي بالأمن السيبراني ومستوى الاعداد والتهيئة لدى المنتسبين في كلية الادارة والاقتصاد في جامعة الموصل لمواجهة أي تهديدات الكترونية محتملة.
2. نشر مفهوم الأمن السيبراني والتعريف على اهم الابعاد التي تؤثر فيه عن طريق توفير تعريف شامل بمصطلح الأمن السيبراني، بالإضافة الى توضيح اهم المفاهيم ذات العلاقة بالعمل الالكتروني ومخاطر الهجمات السيبرانية واهم التهديدات التي قد يتعرض لها مجال التعليم والعمل الإداري.
3. تقديم المقترحات لتحسين وتعزيز إجراءات الأمن السيبراني في المجتمع قيد الدراسة بالإضافة الى المجتمعات التي تشترك مع مجتمع الدراسة بنفس الظروف والخصائص وسبل تنفيذ تلك المقترحات.

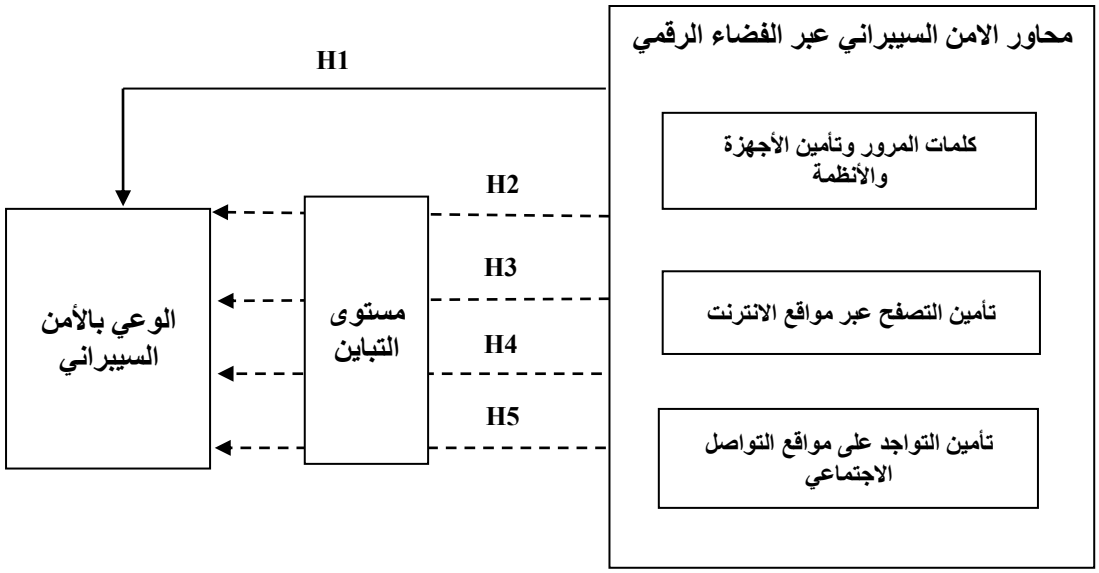
رابعاً: حدود الدراسة الزمانية والمكانية والبشرية: امتدت الحدود الزمانية للدراسة من 1-09-2023 الى 31-03-2024. بينما كانت حدود الدراسة المكانية ضمن كلية الإدارة والاقتصاد في جامعة الموصل شاملة على كل المنتسبين الذين يتعاملون مع الحاسوب والانترنت من تدريسيين وموظفين.

خامساً: أدوات جمع البيانات: تم اعتماد الأسلوب المسحي القائم على استخدام استمارة استبيان ورقية تضمنت مجموعة من الأسئلة ذات العلاقة بقياس مدى الوعي بالأمن السيبراني.

سادساً: مجتمع وعينة الدراسة: يتمثل مجتمع الدراسة بكلية الإدارة والاقتصاد/ جامعة الموصل والتي تعد من الكليات الكبيرة في الجامعة من حيث المساحة وعدد المنتسبين والبالغ عدد منتسبيها 260 تدريسي و158 موظف. وتمثلت عينة الدراسة بمجموعة من المنتسبين في الكلية تدريسيين وموظفين من كلا الجنسين بحجم 100 فرد ممن يتطلب نمط عملهم اليومي التعامل مع الحاسوب المرتبط بالأنترنت سواءاً ضمن نشاطات التدريسي المتمثلة بالتعليم المدمج وتصفح الانترنت والتواصل مع الطلبة عبر بعض مواقع التواصل او الاعمال الإدارية المكلف بها التدريسي او الموظف الإداري المسؤول عن تشغيل أجهزة الحاسوب والأنظمة المحوسبة واستخدام شبكة الانترنت لإنجاز الاعمال المكلف بها.

سابعاً: مخطط الدراسة الفرضي: يتمثل مخطط الدراسة بالمحاور الثلاثة انفة الذكر والتي تشكل اجمالاً وعي شامل بالأمن السيبراني.

الشكل (1): مخطط الدراسة الفرضي



ثامناً: فرضيات البحث:

1. **الفرضية الرئيسية الاولى:** لا يوجد لدى منتسبي كلية الإدارة والاقتصاد/ جامعة الموصل وعي بالأمن السيبراني.
2. **الفرضية الرئيسية الثانية:** لا توجد فروقات معنوية ذو دلالة إحصائية بمستوى الوعي بالأمن السيبراني تعزى لمتغير الجنس.
3. **الفرضية الرئيسية الثالثة:** لا توجد فروقات معنوية ذو دلالة إحصائية بمستوى الوعي بالأمن السيبراني تعزى لمتغير الصفة.
4. **الفرضية الرئيسية الرابعة:** لا توجد فروقات معنوية ذو دلالة إحصائية بمستوى الوعي بالأمن السيبراني تعزى لمتغير المؤهل العلمي.
5. **الفرضية الرئيسية الخامسة:** لا توجد فروقات معنوية ذو دلالة إحصائية بمستوى الوعي بالأمن السيبراني تعزى لمتغير سنوات الخدمة.

تاسعاً: الدراسات السابقة: نُشرت مؤخراً الكثير من الدراسات والأبحاث التي تناولت موضوعة الأمن السيبراني وأثره على الامن المجتمعي او أثره على الاقتصاد القومي، من ناحية أخرى هدفت بعض الدراسات الحديثة أثر الوعي بالأمن السيبراني على المؤسسات التعليمية من مدارس وجامعات. في الجدول ادناه بعض اهم الدراسات التي هدفت الى دراسة الوعي بالأمن السيبراني او العوامل المؤثرة في الوعي بالأمن السيبراني.

جدول (1): الدراسات السابقة ذات العلاقة

تسلسل	الباحث/ الباحثين والسنة	عنوان الدراسة	ملخص الدراسة	اهم النتائج
1	نوره عمر الصائغ واخرون، 2020	وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم.	"يهدف البحث الحالي إلى معرفة درجة وعي المعلمين بالأمن السيبراني وعلاقته بتطبيق أساليب حديثة لحماية الطلبة من مخاطر الإنترنت، وأساليب تعزيز القيم والهوية الوطنية لديهم، وتكونت العينة من (104) معلماً ومعلمة في مدارس مدينة الطائف الحكومية والأهلية. أظهرت نتائج الدراسة ارتفاع وعي المعلمين بالأمن السيبراني في مجال حماية الأجهزة الخاصة والمحمولة من مخاطر الاختراق الإلكتروني	"وجدت الدراسة علاقة ارتباط موجبة ومتوسطة بين وعي المعلمين بالأمن السيبراني واستخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت، فيما لم توجد فروق ذات دلالة إحصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت تبعاً لنوع المدرسة. ولم توجد فروق ذات دلالة احصائية بين استجابات المعلمين حول الوعي بالأمن السيبراني واساليب حماية الطلبة من مخاطر الانترنت تبعا للجنس والتخصص

			والهجمات السيبرانية، وفي درجة استخدامهم لأساليب حماية الطلبة من مخاطر الإنترنت".	والمؤهل العلمي وسنوات الخبرة في التدريسي.".
2	Talal Alharbi, and Asifa Tassaddiq. 2021.	تقييم الوعي بالأمن السيبراني بين طلاب جامعة المجمعة.	هدفت هذه الدراسة إلى تقصي وتقييم مستوى الوعي بالأمن السيبراني وامتثال المستخدم لدى طلاب المرحلة الجامعية في جامعة المجمعة باستخدام استبيان علمي يعتمد على عدة عوامل أمان لاستخدام الإنترنت .وتم اجراء تقييم كمي للمعرفة بالجرائم الإلكترونية والحماية بين الطلاب لإظهار الحاجة إلى تعليم المستخدم والتدريب والوعي. تم في هذه الدراسة دراسة المخاوف المتعلقة بالسلامة المتعلقة برسائل البريد الإلكتروني وفيروسات الكمبيوتر والتصيد الاحتيالي والإعلانات المزورة والنوافذ المنبثقة والفاشيات التكميلية على الإنترنت.	ينبغي تضمين برنامج للتوعية والتدريب في مجال الأمن السيبراني للطلاب. تحتاج المؤسسات الأكاديمية إلى عقد دورات تدريبية وتوعية أمنية شاملة بانتظام للتأكد من أن جميع المستخدمين على اطلاع كافي بأكثر التهديدات السيبرانية شيوعاً واهم نقاط الضعف.
3	Eilts, D. 2020	تقييم جاهزية ومرونة الأمن السيبراني في الشركات الصغيرة.	الهدف الرئيسي من هذه الدراسة البحثية هو التحقق من الاستعداد لمخاطر للأمن السيبراني في الشركات الصغيرة (CyPRisT) لتقييم مواقف الأمن السيبراني لتلك الشركات الصغيرة (الاستعداد والمرونة)، ومن ثم تطوير برنامج استراتيجي لإدارة مخاطر الأمن السيبراني الخاصة بهم.	استكشفت هذه الدراسة البحثية العلاقة بين مبنيين مرتبطين باستعداد الأمن السيبراني ومرونة الشركات الصغيرة. كما أن الشركات الصغيرة معرضة لخطر كبير فيما يتعلق بتسوية الأنظمة لأن أصحابها لا يعرفون ما يجب حمايته. ولمعالجة هذه المشكلة، يجري تطوير موارد الأمن السيبراني والمواد والأدوات التعليمية لتقليل نقاط الضعف لدى الشركات الصغيرة.
4	أ. م. د. ماجد صدام سالم. 2022	الامن السيبراني العراقي وأثره في امن الدولة	يهدف البحث الى ابراز وتوضيح المفاهيم المتعلقة بالفضاء السيبراني للعراق وتوضيح العلاقة ما بين قوة الامن السيبراني والامن	الامن السيبراني جزء لا يتجزء عن امن الدولة واهتمامها الإنساني والاجتماعي ولا يقل أهمية عن الامن الصحي والامن الغذائي والامن

			القومي العراقي من مختلف الجوانب عبر تشخيصها للواقع ورصد الابعاد والمؤشرات لتساعد في تكوين رؤية واضحة وبالتالي اتخاذ القرار المناسب.	المائي. كما أصبحت الدول او الجماعات السيبرانية قوة مساندة لقوة الدولة التقليدية (السياسية والاقتصادية والحربية) وبالتالي امتلاك فرصة أكبر للوصول الى أهدافها المرجوة.
5	Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. 2023	الوعي الأمني وتقييم الكفاءة في قطاع الطاقة	تهدف هذه الورقة إلى تقييم الوعي الأمني والكفاءة لدى القوى العاملة في مؤسسات الطاقة الكهربائية وأنظمة الطاقة الأوروبية(EPES) خلال جائحة كوفيد-19 والحرب الأوكرانية. شارك في الحملة 132 مشاركًا من أصل 266 موظفًا مدعوًا .وقد تم الكشف عن نتائج مهمة فيما يتعلق باستعداد أمن المعلومات ومرونة الأفراد.	تكشف النتائج عن اختلافات كبيرة بين القوى العاملة المشاركة، مما يوضح أنه لا تزال هناك إجراءات يتعين اتخاذها لتأمين البنى التحتية الحيوية لقطاع الطاقة من التهديدات الداخلية غير المقصودة.

تناولت الدراسات السابقة دراسة مستوى الوعي بالأمن السيبراني من وجهات نظر مختلفة في مؤسسات رسمية حكومية وغير حكومية. الدراسات التي تناولت قطاع التعليم تعتبر محدودة نسبياً وركزت على الطلبة دون الكادر التدريسي والإداري والذي يلعب دور أساس في حماية الأجهزة والأنظمة من أي اختراقات او هجمات سيبرانية باستثناء الدراسة الأولى (نوره واخرون، 2020) والثانية (Alharbi and Tassaddig, 2021) التي قيمت مستوى تأثير المعلمين على الطلبة في مجال الامن السيبراني في المدارس لكنها لم تقيم مستوى الوعي بالأمن السيبراني لدى الكادر التدريسي نفسه. ولما لقطاع التعليم من أهمية كبيرة وكونها هدف ثمين للمخترقين والعصابات الالكترونية، توجب اجراء بعض الدراسات التي تقيم مستوى الوعي بالأمن السيبراني لدى المنتسبين في قطاع التعليم العالي من تدريسيين وموظفين وسد هذه الفجوة المعرفية.

تم الاعتماد على بعض فقرات الدراسات السابقة لصياغة منهجية هذه الدراسة وتنظيم الاستبانة الخاصة بالجانب الميداني. حيث تم اعتماد انموذج NIST 2018 في (Eilts, D. 2020) لتحديد إطار الامن السيبراني. تناولت الدراسة (أ.م.د. ماجد صدام سالم. 2022) أثر الامن السيبراني على الامن القومي والتي كانت انعطافة في فهم اثار الامن السيبراني على المجتمع والدولة، تم الاستفادة من الدراسة أعلاه ادراج بعض الفقرات التي توضح أهمية فهم إجراءات الامن السيبراني للحفاظ على بيئة عمل امنة ومستقرة في مؤسسات الدولة ومنها الجامعات والكليات الحومية.

تم تصميم فقرات استمارة الاستبيان ومحاور الأسئلة بالاعتماد على (Alharbi and Tassaddig, 2021) حيث جاءت بثلاث محاور: كلمات المرور والأجهزة ، تصفح الانترنت ، مواقع التواصل الاجتماعي.

المحور الثاني: الإطار النظري

أولاً: مفهوم وتعريف الأمن السيبراني:

أتى مصطلح الامن السيبراني من الكلمتين (Cyber security) واصل كلمة سايبر هي لاتينية وتعني الفضاء الرقمي فأصبحت ترجمة كلمة الأمن السيبراني الى العربية هي امان الفضاء الرقمي، وبالنتيجة هو مصطلح اوسل واشمل من مصطلح امن المعلومات والبيانات ليشمل شبكة الانترنت والشبكات الداخلية وكل ما يدور فيها من نشاطات بالإضافة الى امن المعلومات المخزنة على الحواسيب وأجهزة التخزين الدائمية. فيمكن القول بان الامن السيبراني يشمل جميع الإجراءات والخطوات التي من شانها حماية المعدات المادية والمعلومات المخزنة عليها من أي محاولات للسرقة او التخريب او الاستخدام غير المشروع بالإضافة الى تامين الفعاليات الالكترونية عبر الفضاء الرقمي (سالم، 2022، 2-3)

كما يذهب البعض الى إعطاء مفهوم أوسع لمصطلح الامن السيبراني ليشمل جميع النشاطات والإجراءات الرقمية الحكومية التي من شانها ضمان استمرارية الاعمال الإدارية الالكترونية للدولة وبالشكل الامن والموثوق (خليفة، 2019، 5).

ظهر مصطلح الأمن السيبراني بعد ظهور الحاسوب بعدة سنوات وبالتحديد في العام 1972 حيث كان مجرد فكرة استمرت حتى نهاية السبعينيات من القرن العشرين مع ظهور اول تطبيق مكافحة الفايروسات وتعقب مساره من قبل الباحث بوبتوماس أطلق عليه إسم (كريبر) وقد تمكن هذا البرنامج من التحرك عبر الشبكة.

يمكن تلخيص تعريف لمصطلح الامن السيبراني كما عرفه سالم (2022) بانه "عملية الحد من خطر الهجمات الضارة على برامج وأجهزة الكومبيوتر والشبكات من خلال استخدام أدوات كشف الاختراقات ووقف نشاطات الفيروسات ومنع الدخول غير المسموح به، وتأكيد الهويات وتمكين الاتصالات المشفرة، وهو كذلك مجموعة من التقنيات والعمليات والممارسات لحماية الشبكات والحواسيب والبرامج والبيانات من الهجوم او الضرر او الوصول غير المسموح به من اجل ضمان السرية والنزاهة".

ويذكر الرنتيسي وعقل (2011) انه على الجامعات ان تكون رائدة في مجال قيادة التطور التكنولوجي في جميع المجالات وتوظيفه خدما للعملية التعليمة والإدارية، ولكن يبدوا ان معظم أعضاء الهيئة التدريسية تكون استجابتهم بطيئة للتحديات التكنولوجية التي تواجههم في مجال عملهم.

كما تم تعريفه بحسب (Craigen, D., et al, 2014) على انه تنظيم وجمع الموارد والعمليات والهياكل المستخدمة لحماية الفضاء الإلكتروني والأنظمة التي تدعم الفضاء الإلكتروني من الأحداث التي تتناقض وحقوق الملكية الفكرية.

مما تقدم يمكن تلخيص تعريف لمصطلح الامن السيبراني عل انه جميع العمليات والإجراءات المادية والبرمجية المتخذة من قبل الافراد او أصحاب القرار لمنع تعرضهم لاي هجمات رقمية، كذلك يشمل مصطلح الامن السيبراني على الإجراءات المتبعة للتقليل من الاثار السلبية الناتجة عن الهجمات الرقمية في حال وقوعها.

ثانياً: عناصر الامن السيبراني: يتكون مفهوم الأمن السيبراني من مجموعة من العناصر الرئيسية هي:

1- **القوة السيبرانية:** وتعد القدرة على الوصول الى النتائج المطلوبة من خلال الوصول المشروع وغير المشروع الى المعلومات والبيانات المتوفرة على الفضاء الالكتروني، وذلك باستخدام الأدوات المتاحة ومهارات المختصين بالأمن السيبراني لاستخدام الانترنت والوصول الى النقاط المستهدفة. وما يعزز القوة السيبرانية هو التحول الهائل نحو الرقمنة في اغلب نشاطات الافراد والمؤسسات المدنية والحكومية وتوفر كثير من المعلومات ذات الطابع السري على الفضاء الرقمي ما يشجع المخترقين على العمل على تنفيذ هجماتهم وبشكل متكرر. (مهدي وصفاء، 2020، 154).
من جانب اخر، تعتبر القوة السيبرانية وجود قوة الكترونية ونظام متماسك لإدارة وحماية موارد الدولة المعلوماتية وأجهزتها من التهديدات السيبرانية وضمان سلامة الإجراءات الحكومية من أي تهديد. (شلوش، 2018، 199).

2- **الفضاء السيبراني:** وهو البيئة التي تشمل على كل من الموارد المادية والبرمجية والبشرية التي تعمل في الفضاء الرقمي. تشمل الموارد المادية على أجهزة الحاسوب وجميع الأجهزة والقطع المادية المرتبطة بالشبكة، وتشمل الموارد البرمجية على التطبيقات المسؤولة عن تشغيل وإدارة الأجهزة، والموارد البشرية تشمل على المشغلين للأجهزة المادية وإدارة البرامجيات المرتبطة بالشبكة. (رزوقة، 2019، 71).

3- **الدفاع السيبراني:** ويقصد به الدفاع الالكتروني وهو مجموعة من القدرات والإمكانات التي تمتلكها الدولة عموماً او القوات الأمنية خصوصاً وذلك لمنع او الحد والتخفيف من الهجمات السيبرانية وتسريع التعافي من الاثار التي تتركها تلك الهجمات. يعرف البرلمان الأوربي على انه عملية تطبيق لجميع الإجراءات والممارسات الالكترونية وغير الالكترونية الأمنية التي من شأنها حماية الدولة من الهجمات السيبرانية او الحد من اثارها لتامين البنية التحتية للدولة وضمان استمرار نظم الاتصالات والسيطرة على العمليات. (Nye, 2010,6)

4- **الردع السيبراني:** نتيجة لتطور الفضاء الالكتروني بشكل متسارع ومستمر والذي يشمل البرمجيات والمعدات فان من الصعب منع الهجمات السيبرانية بشكل نهائي نتيجة للثغرات التي يتم اكتشافها باستمرار في أنظمة التشغيل او التطبيقات المضادة للفايروسات فضلاً عن صعوبة تعقب مصدر الهجمات وبالتالي يكون من الصعب استخدام وسائل الردع الالكترونية التقليدية كالهجمات

السيبرانية المضادة، لذا تم تبني استراتيجية الردع السيبراني تشمل على التخفيف من حدة تأثير الهجمات السيبرانية حال حدوثها او الوصول الى (صفر اثر) على الأجهزة والمعلومات الحرجة ذات الأهمية القصوى. فالردع الالكتروني بحسب (Singer, 2014, 55) هو القدرة على تغيير تصرفات العدو من خلال ايهامهم بارتفاع التكلفة وانخفاض العائد من الهجمات السيبرانية وما سينتج عنه من ردة فعل قوية من الجهة المقابلة.

5- **الهجوم السيبراني:** وهو فعل عدائي يستهدف الأجهزة او البرمجيات او المعلومات المتاحة على الفضاء الالكتروني لتحقيق هدف شخصي او سياسي من خلال استغلال الثغرات الموجودة في أنظمة التشغيل لدى الطرف المستهدف او ضعف في أنظمة الدفاع ضد الفايروسات والتطبيقات الضارة. تتمكن بعض الهجمات السيبرانية من اغلاق أجهزة الحواسيب وتعطيلها بشكل دائم ومهاجمة أجهزة السيطرة على الطاقة الكهربائية او أنظمة متابعة الملاحة في المطارات وتعطيلها ما يسبب ارباك كبير في العمل ناهيك عن سرقة المعلومات المتوفرة على قواعد البيانات المرتبطة بالشبكة العنكبوتية، ما يسبب ضرر كبير للمؤسسة صاحبة العلاقة سواءاً عسكرية او صحية او تعليمية فمستوى الضرر يختلف من مؤسسة الى أخرى. (سليمان، 2020، 249).

ويمكن تقسيم الهجمات السيبرانية الى أربع فئات وهي الحرب السيبرانية وهي التي تنشأ بين بلدين والإرهاب السيبراني وهو الذي تنفذه جماعة ضد جماعة او دولة ضد دولة او جماعة ضد دولة والتجسس السيبراني وهو الذي ينفذ بدافع التجسس وسرقة المعلومات وأخيرا الجريمة السيبرانية التي يكون الدافع ورائها الجريمة فقط، يلاحظ ان الإرهاب والحرب السيبرانية نادرة في يومنا هذا والأكثر انتشارا هما التجسس السيبراني والجريمة السيبرانية. (ياسين، 2014، 62).

ثالثاً: اهمية تقييم الوعي بالأمن السيبراني:

تأتي أهمية الوعي بالأمن السيبراني من ازدياد مخاطر الهجمات السيبرانية لمؤسسات التعليم العالي في السنوات الأخيرة كما اشارت العديد من الدراسات والاستطلاعات (Przyborski, Kristen, et al., 2019) (Rezgui, Y., & Marks, A. 2008). واعتباراً من العام 2017 تضاعفت الخروقات والهجمات على مراكز البيانات في مؤسسات التعليم العالي حول العالم ولاتزال عناوين ومواقع الانترنت ذات الامتداد edu. هدفاً شائعا لأغلب الهجمات السيبرانية حول العالم حتى ازدادت نسبة تلك الهجمات بنسبة 72% في الأعوام 2018-2019 (Przyborski, Kristen, et al., 2019). وان من اهم الهجمات التي استهدف مؤسسات التعليم العالي هي من نوع phishing و ransomware والتي تعني الاصطياد والفدية على التوالي (John Chapman, 2020). تعود الزيادة الكبيرة على مستوى العالم من حوادث الأمن السيبراني بشكل أساسي إلى أن معظم العاملين في المؤسسات او الافراد في بيوتهم لا يتبعون تعليمات وقواعد الامن السيبراني الدقيقة بالإضافة على عدم مواكبة التعليمات وقواعد الانت السيبراني للتطور الحاصل بتقنيات الاختراق والهجمات السيبرانية او ضعف بأنظمة الحماية.(Whitman, M. E., & Mattord, H. J., 2021)

يمكن أن يصبح الهجوم السيبراني مكلفًا إذا لم تكن المؤسسة على وعي تام بالأمن السيبراني ومستعدة لمواجهة أي تهديد قد يحصل، أو انها تفتقر إلى القدرة على التعافي من حادث الأمن السيبراني بعد وقوعه. فقد تتعرض المؤسسات الربحية وغير الربحية غير المستعدة لمواجهة التهديد السيبراني لخطر الإفلاس او الانهيار الكامل، عندها قد لا يكون لدى صانعي

القرار أو المديرين في تلك المؤسسات أي خيار سوى الاستجابة لطلبات المهاجمين في حال كان نوع الهجوم، هجوم الفدية ransomware. (Darrell Eilts, 2020).

رابعاً: مؤشر الامن السيبراني:

يصدر مؤشر الامن السيبراني عن الاتحاد الدولي للاتصالات التابع للجميع العامة للأمم المتحدة، يهتم هذا مؤشر في رصد مستوى التحسن في مستويات الوعي العالمي بأهمية الأمن السيبراني وما هي التدابير المتخذة لتطويره في 194 دولة من دول العالم وذلك بالاستناد على خمسة مؤشرات اساسية هي: 1- التدابير التنظيمية 2- التدابير القانونية 3- التدابير التقنية 4- التدابير الهادفة الى تعزيز قدرات الأمن السيبراني 5- تدابير تعزيز التعاون. يتم جمع البيانات عن طريق استبيان الكتروني يرسل من قبل الاتحاد الى المنظمات الرسمية في كل بلد للإجابة عليه. يزن كل مؤشر 20 نقطة فيكون المجموع 100 نقطة تتنافس على أساسها الدول لتسلق سلم التصنيف العالمي لتقرير الاتحاد العالمي للاتصالات. (UN, 2020, 29)

صدر التقرير الأخير عن الاتحاد العالمي للاتصالات في العام 2021 وهو مؤشر بيانات العام 2020 حيث تم تصنيف الدول حسب المناطق او القارات، ما يهمنا هو المنطقة العربية والعراق بالتحديد، حيث جاء العراق بالتسلسل 17 عربياً و 129 عالمياً. تصدرت الولايات المتحدة الامريكية قائمة دول العالم والمملكة العربية السعودية قائمة الدول العربية متقدمة 11 مرتبة عن تصنيف العام 2018. الجدول (2) يمثل ترتيب الدول العربية حسب مؤشر الاتحاد العالمي للاتصالات وفق مؤشر الامن السيبراني للعام 2020.

جدول (2): ترتيب الدول العربية وفق مؤشر الامن السيبراني للعام 2020

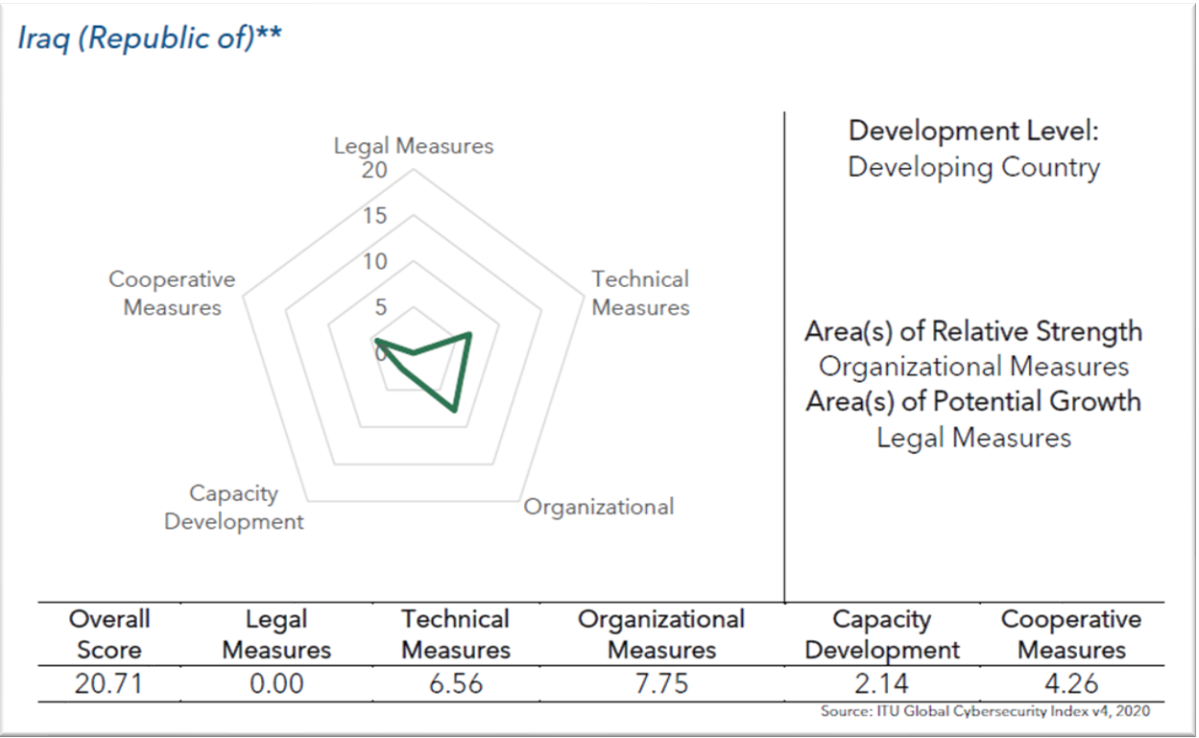
الدولة	الترتيب العربي	الترتيب الدولي	النقاط
المملكة العربية السعودية	1	2	99,54
الامارات العربية المتحدة	2	5	98,06
سلطنة عمان	3	21	96,04
مصر	4	23	95,48
قطر	5	27	94,50
تونس	6	45	86,23
المغرب	7	50	82,41
البحرين	8	60	77,86
الكويت	9	65	75,05
الاردن	10	71	70,96
السودان	11	102	35,03
الجزائر	12	104	33,95
لبنان	13	109	30,44
ليبيا	14	113	28,78
الاراضي الفلسطينية	15	112	25,18
سوريا	16	126	22,14
العراق	17	129	20,71
موريتانيا	18	133	18,94
الصومال	19	137	17,25
جزر القمر	20	174	3,72
جيبوتي	21	179	1,73
اليمن	22	182	0

.Global Cybersecurity Index 2020. Measuring commitment to cybersecurity.ITU.UN.2021.p29

يشير التقرير أعلاه الى ان العراق لم يقدم الإجابة على كثير من بيانات الاستبيان الالكتروني (الشكل 2 ادناه) ما أثر سلباً على مجموعة النقاط الحاصل عليها، وهو الامر الواجب معرفة ان كان سببه نقص البيانات لدى المؤسسات الرسمية ام تهاون الجهات الرسمية مع هذا الملف في العراق وانعدام وجود متخصصين بالأمن السيبراني في العراق.

توجد في العراق اقسام تعنى في موضوعة الامن السيبراني وهي تفتقر الى التنسيق او التعاون المحترف وكل جهة من هذه الجهات المنتمية الى مؤسسات حكومية تعمل لمفردها. يجب على العراق السعي لإنشاء هيئة تهتم بقضايا الامن السيبراني. (سالم، 2022، 8)

الشكل (2): المؤشرات الخمس للأمن السيبراني في العراقي وفق تقرير عام 2020



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
20.71	0.00	6.56	7.75	2.14	4.26

Source: ITU Global Cybersecurity Index v4, 2020

خامساً: المخاطر او الخسائر المتوقعة من الهجمات السيبرانية:

حساب التكلفة الحقيقية او مستوى الخطورة الناتجة عن الهجمة السيبرانية تختلف من مؤسسة الى أخرى حسب حجم الضرر الذي احدثته الهجمة وكمية المعلومات التي تم فقدانها او الأجهزة التي تم تعطيلها ومدى حساسية المعلومات التي تم فقدانها. فمنها ما يكون هجمات مدمرة تتسبب بانهيار تلك المؤسسة ومنها ما يسبب خسائر مادية يمكن معالجتها وتلافيها خلال أيام من تاريخ الهجمة. بالإضافة الى الأثر الذي قد تحدثه الهجمة على العاملين في تلك المؤسسة من فقدانهم الثقة في المؤسسة التي يعملون فيها وجدوى النظام الالكتروني الأمني المعتمد. (Chapman et al, 2018, 117) يتوجب على إدارة المؤسسات تخصيص المبالغ المالية الازمة لدعم الامن السيبراني والتحوط لاي طارئ قد يحدث، وتشمل تلك التخصيصات على إقامة الدورات التوعوية للعاملين، بناء منظومات امنية للحد او منع أي هجوم سيبراني محتمل وتهيئة الظروف اللازمة للتعافي من أي حادث سيبراني قد يحدث، ويشمل على شراء مستلزمات وأجهزة إضافية وخزن المعلومات الحساسة بأكثر من نسخة والحفاظ عليها بعيداً عن الأجهزة المتصلة بالأنترنت.

سادساً: أفضل ممارسات الامن السيبراني:

يعد تنفيذ أفضل الممارسات الآمنة للأمن السيبراني أمرًا مهمًا وحيوياً للأفراد والمؤسسات على حد سواء لضمان استمرارها والحفاظ على مواردها الداخلية والخارجية. يصعب تأمين الفضاء السيبراني لعدة عوامل منها: قدرة الجهات المهاجمة على العمل من أي مكان في العالم، والترابط بين الفضاء السيبراني والاجهزة المادية، وصعوبة تجاوز جميع من نقاط الضعف او الخلل في شبكات الفضاء الرقمي. تذكر وكالة الامن السيبراني والبنية التحتية الامريكية CISA عل موقعها الرسمي على الانترنت مجموعة من أفضل الممارسات التي يتحتم على الافراد والمؤسسات اتباعها لتحقيق اعلى نسبة امان ممكنة في الفضاء الالكتروني قبل وقوع الهجمات السيبرانية، ما يعني ان الإجراءات التالية هي لمنع او الحد من وقوع الهجمات السيبرانية: (*4 Things You Can Do to Keep Yourself Cyber Safe | CISA*, 2022)

1- **استخدام كلمة مرور قوية:** تعني كلمة مرور قوية استخدام كلمة مرور طويلة نوعاً ما (لا تقل عن 15 ارقام وحروف ورموز)، بالإضافة الى انها فريدة وغير مكررة في مواقع أخرى. وتعد من اهم الممارسات الجيدة لحماية الأنظمة والحسابات والأجهزة من اختراقات الهاكرز وسرقة البيانات، ويجب عدم خزن كلمات المرور في المتصفحات ما يجعل احتمالية سرقتها أكبر. كما ينصح بتجنب كتابة كلمات المرور على أوراق وخزنها قريبة من جهاز الحاسوب تجنباً لسرقتها وتسريبها للمخترقين.
2- **تفعيل خاصية المصادقة متعددة المراحل:** وتنص على طلب أكثر من دليل اثبات شخصية من المستخدم للسماح له بالدخول الى النظام الالكتروني او الحسابات على الانترنت، كأن يطلب منا كلمة مرور بالإضافة الى رقم هاتف يتم استخدامه لإرسال كود الدخول كخطوة ثانية إضافية لطلب كلمة المرور او طلب بصمة الابهام.
3- **تحديث برامج الحاسوب ومتصفحات الانترنت:** عملية تحديث البرامج على الحاسوب بشكل دوري ومنتظم بحسب توصيات الشركة المصنعة للبرامج يساهم بشكل كبير على معالجة الثغرات الأمنية في هذه البرامج، حيث تقوم الشركات المصنعة لهذه البرامج باكتشاف تلك الثغرات بشكل مستمر وتعمل على إصلاحها بتحديثات تطلق بشكل دوري. تنصح وكالة الامن السيبراني والبنية التحتية الامريكية على اختيار خيار Auto Update من داخل اعدادات البرامج او نظام التشغيل لضمان التحديث الدوري في حال نسيان المستخدم القيام بهذه المهمة بالإضافة الى ضمان تحديث البرامج فور توفرها على الانترنت وعدم انتظار المستخدم للقيام بالتحديث والذي قد يأتي متأخراً وبعد فوات الأوان.
4- **التفكير قبل الضغط على أي رابط:** تنص وكالة الامن السيبراني الامريكية على ان 90% من الهجمات السيبرانية الناجحة تبدأ بضغط مستخدمي الحواسيب على روابط مرسلة إليهم عبر الايميل او تطبيقات التواصل الأخرى. لذا من الجيد ان لا يضغط المستخدم على أي رابط الكتروني الا اذا كان الرابط مرسل من جهة رسمية بالإضافة الى ضرورة قراءة المستخدم للرابط والتحقق من الامتدادات الامنة والتي هي على سبيل المثال لا الحصر .com و .net و .gov و .edu الخ.

كما تضيف المجموعة الأمريكية للخدمات التكنولوجية (Team, 2023)، مجموعة من أفضل الممارسات الإضافية التي تحقق نسبة امان في الفضاء الرقمي:

1- **تفعيل جدار الحماية Firewall:** والذي يعد عنصراً حاسماً في أي استراتيجية لأمن الشبكات. فهو يساعد على منع الوصول غير المصرح به إلى الشبكة والانظمة ويمكن تهيئته لمنع أنواع معينة حركة المرور عبر الشبكة. فضلاً عن تنصيب أحد برامج مضادات الفايروسات والتي تعمل على فحص وتامين الاتصال بالإنترنت.

2- **وضع خطة التعافي من الهجمات:** يمكن أن تساعد خطة التعافي من الهجمات في تخفيف تأثير الهجوم السيبراني حال وقوعه. يتضمن ذلك الحصول على نسخة احتياطية لجميع البيانات والأنظمة المهمة، وخطة لاستعادتها في حالة فقدان النسخة الاصلية.

3- **استخدام الشبكات الخاصة الافتراضية (VPN):** توفير الشبكات الخاصة الافتراضية طبقة إضافية من الأمن عن طريق تشفير جميع البيانات المنقولة بين جهاز الشركة والاجهزة البعيدة وهذا يجعل من الصعب على مجرمي الإنترنت اعتراض المعلومات الحساسة وسرقتها.

4- **توفير تدريب للعاملين مع تجربة اختراق تجريبي:** اقحام المنتسبين في دورات تطويرية وتثقيفية في مجال الأمن السيبراني واهم الخطوات الواجب اتباعها قبل وبعد وقوع الهجمة السيبرانية، بالإضافة الى اجراء محاكاة لهجمة سيبرانية على خوادم وأنظمة المؤسسة ودراسة نتائجها.

سابعاً: إطار الامن السيبراني:

تم تطوير إطار عمل لمفهوم الامن السيبراني ليكون شاملاً لجميع المؤسسات والشركات الصغيرة منها والكبيرة الربحية منها وغير الربحية: (NIST, 2018, 7-9)

1- **التحديد:** ويشمل على تطوير فهم تنظيمي لإدارة مخاطر الامن السيبراني على الأنظمة الالكترونية والأشخاص والبيانات. يمكن هذا البعد المنظمة من تركيز جهودها وتحديد أولوياتها وادراج خططها ضمن استراتيجية إدارة المخاطر وتحديد الاحتياجات في المنظمة.

2- **الحماية:** وتشمل على تطوير وتنفيذ انظمة وتعليمات الحماية المهمة والتي تدعم عملية منع او الحد من التهديدات السيبرانية في حال حدوثها.

3- **الاكتشاف:** تشمل على تنفيذ الأنشطة اللازمة لاكتشاف وقوع أي حدث متعلق بالأمن السيبراني في الوقت المناسب.

4- **الاستجابة:** تشميل على تطوير وتنفيذ الأنشطة المناسبة لاتخاذ الإجراءات اللازمة فيما يتعلق بتهديدات الامن السيبراني التي تم اكتشافها في مرحلة الاكتشاف، تدعم هذه الخطوة احتواء تأثير الهجمة السيبرانية حال وقوعها.

5- **التعافي:** ويشمل تطوير وتنفيذ الأنشطة المناسبة للحفاظ على خطط المؤسسة والمرونة في تنفيذها واستعادة أي من الخدمات التي تعطلت أثر الهجمة السيبرانية، ويجب ان تكون خطوة التعافي في الوقت المناسب لتقليل اثر الهجمات السيبرانية.

الشكل (2): الوظائف الخمس في إطار الامن السيبراني NIST الإصدار 1.1

Source: NIST, 2018

المحور الثالث: الجانب الميداني:

أولا: وصف مجتمع الدراسة: تأسست كلية الإدارة والاقتصاد في العام 1968 وكانت كلية أهلية تابعة لجمعية الاقتصاديين العراقيين/ فرع الموصل وكان اسمها "كلية المحاسبة وإدارة الاعمال" وكانت تقتصر الدراسة فيها على الدراسة المسائية وعدد طلابها 240 طالباً في العام 1968–1969 ومدة الدراسة فيها خمس سنوات وتقتصر على قسم واحد "المحاسبة وإدارة الاعمال". ثم تم الحاقها بالجامعة المستنصرية ذات العام الدراسي. تم افتتاح قسم الاقتصاد في السنة الثانية لافتتاح الكلية. ثم في العام 1974 التحق الكلية بجامعة الموصل. تلبي الكلية حاجات السوق من القوة العاملة من سبع تخصصات وهي الإدارة والمحاسبة والاقتصاد والمالية والمصرفية والإدارة الصناعية ونظم المعلومات الإدارية والتسويق. كما توفر الكلية دراسات عليا في بعض تخصصاتها، وللكلية دور فاعل في دوائر المحافظة وغرفة التجارة وهيأة الاستثمار.

تضم الكلية ما يقرب من 260 تدريسي و 158 موظف و 6450 طالب دراسات أولية (5000 طالب صباحي و 1450 طالب مسائي) و 450 طالب دراسات عليا، ما يجعلها من اكبر الكليات في جامعة الموصل وتتوفر خدمة الانترنت فيها طيلة فترة الدوام الرسمي لكل الكادر من موظفين وتدريسيين على حد سواء، واعتماد جميع وحداتها وشعبها على العمل المؤتمت باستخدام الحاسبات ما يجعلها عينة بحث ممتازة لدراسة موضوعة الامن السيبراني ومدى تطبيق معايير الامن الرقمي. https://uomosul.edu.iq/administrationeconomic/

ثانياً: وسائل القياس: تم استخدام البرنامج الاحصائي SPSS v26 في التحليل الوصفي لإجابات العينة المبحوثة واستخراج الأوساط الحسابية والانحرافات المعيارية والنسب المئوية بالإضافة الى تحليل التباين الأحادي One Way ANOVA لتحديد مستوى الفروقات في إجابات العينة على أسئلة متغير الوعي بالأمن السيبراني تبعاً لمتغير الجنس والصفة والمؤهل العلمي وسنوات الخدمة ثم الاجابة على فروض الدراسة.

ثالثاً: وصف العينة: تمثلت عينة البحث بالأفراد المنتسبين في كلية الإدارة والاقتصاد/ جامعة الموصل من تدريسيين وموظفين من حملة شهادة البكالوريوس والدبلوم العالي والماجستير والدكتوراه وبحجم 100 فرد. تم توزيع استمارات الاستبيان بشكل عشوائي بين افراد المجتمع المبحوث لتحقيق صفة العشوائية والتجانس في الإجابات. الجدول (3) يصف عينة البحث:

جدول رقم (3): وصف عينة البحث

الجنس		
	العدد	**النسبة المئوية**
ذكر	57	%57
انثى	43	%43
الصفة		
	العدد	**النسبة المئوية**
تدريسي	59	%59
موظف	41	%41
المؤهل العلمي		
	العدد	**النسبة المئوية**
بكالوريوس	34	%34

دبلوم عالي	5	%5
ماجستير	33	%33
دكتوره	28	%28
سنوات الخدمة		
	العدد	**النسبة المئوية**
1-10 سنة	11	%11
11-15 سنة	39	%39
16-20 سنة	32	%32
أكثر من 20 سنة	18	%18

رابعاً: التكرارات والنسب المئوية والاوساط الحسابية والانحرافات المعيارية للإجابات: يشير الجدول (4) ادناه الى التكرارات والنسب المئوية والاوساط والانحرافات المعيارية لإجابات العينة المبحوثة متمحورة حول مقياس ليكرت الخماسي حيث كان المقياس كالاتي (اتفق بشدة=1، اتفق=2 ، محايد=3 ، لا اتفق=4 ، لا اتفق بشدة=5).

جدول (4): الاوساط الحسابية والنسب المئوية والانحرافات المعيارية لإجابات العينة

الاجابة / الفقرة		اتفق بشدة		اتفق		محايد		لا اتفق		لا اتفق بشدة		الوسط الحسابي	الانحراف المعياري
		التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة	التكرار	النسبة		
كلمة المرور وحماية الاجهزة	X1	60	%60	36	%36	2	%2	2	%2	0	%0	1.46	0.642
	X2	23	%23	44	%44	13	%13	16	%16	4	%4	2.34	1.121
	X3	32	%32	38	%38	17	%17	13	%13	0	%0	2.11	1.004
	X4	32	%32	36	%36	12	%12	17	%17	3	%3	2.23	1.162
	X5	19	%19	32	%32	16	%16	21	%21	12	%12	2.75	1.313
	X6	26	%26	49	%49	15	%15	9	%9	1	%1	2.10	0.927
المؤشر العام			%32		%39		%13		%13		%3	2.17	1.028
تامين التصفح عبر الانترنت	X7	29	%29	42	%42	15	%15	13	%13	1	%1	2.15	1.019
	X8	32	%32	52	%52	13	%13	3	%3	0	%0	1.87	0.747
	X9	24	%24	39	%39	23	%23	13	%13	1	%1	2.28	1.006
	X10	18	%18	37	%37	22	%22	21	%21	2	%2	2.52	1.078
	X11	57	%57	34	%34	4	%4	5	%5	0	%0	1.57	0.795
	X12	13	%13	50	%50	21	%21	15	%15	1	%1	2.41	0.933
المؤشر العام			%29		%42		%16		%12		%1	2.13	0.930
المواقع التي توجد على	X13	50	%50	26	%26	16	%16	8	%8	0	%0	1.82	0.978
	X14	58	%58	31	%31	8	%8	3	%3	0	%0	1.56	0.770
	X15	55	%55	32	%32	4	%4	8	%8	1	%1	1.68	0.952

1.025	2.00	%1	1	%9	9	%19	19	%31	31	%40	40	X16	
1.006	2.33	%2	2	%10	10	%30	30	%35	35	%23	23	X17	
0.929	1.84	%1	1	%8	8	%6	6	%44	44	%41	41	X18	
0.943	1.87	%1		%8		%13		%33		%45		**المؤشر العام**	
0.970	**2.06**	**%2**		**%11**		**%14**		**%38**		**%35**		**المؤشر الاجمالي**	

المصدر: من اعداد الباحث بالاعتماد على نتائج تحليل البيانات باستخدام SPSS

تشير بيانات الجدول (4) أعلاه الى توزيع الفقرات وإجابات العينة المبحوثة على المحاور الثلاثة (كلمة المرور وحماية الأجهزة، تامين التصفح عبر الانترنت، تامين التواجد على مواقع التواصل الاجتماعي) وكانت الاوساط الحسابية والانحرافات المعيارية والسب المئوية لكل محور كالاتي:

1- **كلمة المرور وحماية الأجهزة:** فيما يخص هذا المحور، تشير الأوساط الحسابية الى وجود وعي عالي بالأمن السيبراني لدى العينة المبحوثة حيث تمحور المؤشر العام لمتوسط الإجابات حول الاتفاق بشدة والاتفاق بنسبة 71% وهي (32% و 39%) على التوالي. مقابل نسبة عدم اتفاق وعدم اتفاق بشدة بنسبة 16% فقط وهي (13% و 3%) على التوالي ونسبة حياد بلغت 13% ، وبوسط حسابي (2.13) وانحراف معياري (1.028). وقد حصل السؤال الاول على اعلى نسبة اتفاق بوسط حسابي (1.46) وانحراف معياري (0.642) والذي ينص على (أقوم باستخدام كلمة مرور بطول 8 مراتب على الأقل وتتكون من ارقام وحروف ورموز). بينما حصل السؤال الخامس على اقل نسبة اتفاق بوسط حسابي (2.75) وانحراف معياري (1.313) والذي ينص على (لا أرى بإمكانية مشاركة كلمة مرور جهاز الحاسبة الخاص بيه في العمل مع الزملاء للقيام بالأعمال بدلا عني).

2- **تامين التصفح عبر الانترنت:** فيما يخص هذا المحور، تشير الأوساط الحسابية الى وجود وعي عالي بالأمن السيبراني لدى العينة المبحوثة حيث تمحور المؤشر العام لمتوسط الإجابات حول الاتفاق بشدة والاتفاق بنسبة 71% وهي (29% و 42%) على التوالي. مقابل نسبة عدم اتفاق وعدم اتفاق بشدة بنسبة 13% فقط وهي (12% و 1%) على التوالي ونسبة حياد بلغت 16% ، وبوسط حسابي (2.13) وانحراف معياري (0.930). وقد حصل السؤال الحادي عشر على اعلى نسبة اتفاق بوسط حسابي (1.57) وانحراف معياري (0.795) والذي ينص على (اتجنب الضغط على الروابط المجهولة المصدر عن حاجتي لتحميل الملفات من الانترنت). بينما حصل السؤال العاشر على اقل نسبة اتفاق بوسط حسابي (2.52) وانحراف معياري (1.078) والذي ينص على (أقوم بفحص التاريخ history الخاص بالمتصفح للتأكد من عدم وجود أي نشاطات مشبوهة).

3- **تامين التواجد على مواقع التواصل الاجتماعي:** فيما يخص هذا المحور، تشير الأوساط الحسابية الى وجود وعي عالي بالأمن السيبراني لدى العينة المبحوثة حيث تمحور المؤشر العام لمتوسط الإجابات حول الاتفاق بشدة والاتفاق بنسبة 78% وهي (45% و 33%) على التوالي. مقابل نسبة عدم اتفاق وعدم اتفاق بشدة بنسبة 9% فقط وهي (8% و 1%) على التوالي ونسبة حياد بلغت 13% ، وبوسط حسابي (1.87) وانحراف معياري (0.943). وقد حصل السؤال الرابع عشر على اعلى نسبة اتفاق بوسط حسابي (1.56) وانحراف معياري (0.770) والذي ينص على (اتجنب قبول طلبات الصداقة والتواصل مع الغرباء على مواقع التواصل الاجتماعي). بينما حصل السؤال السابع عشر على اقل نسبة اتفاق بوسط حسابي (2.33) وانحراف معياري (1.006) والذي ينص على (أقوم بعمل إبلاغ عن النشاطات المشبوهة من بعض الحسابات على مواقع التواصل الاجتماعي).

وجاء المؤشر الإجمالي للمحاور الثلاثة ولجميع الأسئلة كالاتي: نسبة الاتفاق بشدة والاتفاق هي 73% (35% و 38%) على التوالي ونسبة عدم الاتفاق وعدم الاتفاق بشدة هي 13% (11% و 2%) على التوالي وبوسط حسابي (2.06) وانحراف معياري (0.970). **بناءاً على ما تقدم نرفض الفرضية الرئيسية الأولى القائلة بعدم وجود وعي بالأمن السيبراني بين منتسبي كلية الإدارة والاقتصاد في جامعة الموصل ونقبل الفرضية البديلة القائلة بوجود وعي بالأمن السيبراني بين منتسبي الكلية.**

خامساً: تحليل انوفا الأحادي (One Way ANOVA) لإيجاد الفروقات بين افراد العينة بمستوى الوعي بالأمن السيبراني: تم باستخدام برنامج SPSS v26 اجراء اختبار Normality وتبين ان جميع العينات تتبع التوزيع الطبيعي وبالتالي تحقق شرط اختبار الأنوفا الذي يتطلب ان تتبع بيانات الاختبار التوزيع الطبيعي. وتم اجراء اختبار Homogeneity وتبين بانه هناك تجانس بين عينات المتغيرات قيد الدراسة وقد تحقق شرط التجانس أيضاً والذي يشترط تحققه قبل اجراء اختبار الأنوفا. ولغرض الإجابة على فروض الدراسة الخاصة بوجود فروقات بين مجموعات المتغيرات المستقلة على متغير الوعي بالأمن السيبراني من عدمه، سيتم اجراء اختبار الأنوفا الأحادي كالاتي:

1- متغير الجنس المستقل مع متغير الوعي بالأمن السيبراني المعتمد.
2- متغير الصفة المستقل مع متغير الوعي بالأمن السيبراني المعتمد.
3- متغير المؤهل العلمي المستقل مع متغير الوعي بالأمن السيبراني المعتمد.
4- متغير سنوات الخدمة المستقل مع متغير الوعي بالأمن السيبراني المعتمد.

1-اختبار متغير الجنس المستقل مع متغير الوعي بالأمن السيبراني المعتمد: الجدول (5) ادناه يوضح بيانات اختبار الأنوفا لمتغير الجنس مع متغير الوعي بالأمن السيبراني.

جدول (5): جدول تحليل انوفا بين متغير الجنس ومتغير الوعي بالأمن السيبراني

الجنس	الوسط الحسابي	الانحراف المعياري	F المحسوبة	F الجدولية	Sig.	الدلالة الإحصائية
ذكر	2.021	0.474	0.542	3.940	0.463	غير دال احصائياً
انثى	2.094	0.467				

المصدر: من اعداد الباحث بالاعتماد على نتائج تحليل البيانات باستخدام SPSS

يتضح من بيانات الجدول (5) أعلاه بان قيمة F المحسوبة اصغر من قيمة F الجدولية وان قيمة .Sig أكبر من مستوى المعنوية 0.05، ما يعني بانه لا توجد فروقات ذات دلالة إحصائية عند مستوى معنوية 0.05 بمستوى الوعي بالأمن السيبراني تبعاً لمجموعات متغير الجنس (ذكر ، انثى). مما تقدم نقبل الفرضية **الرئيسية** الثانية القائلة بعدم وجود فروقات معنوية ذات دلالة إحصائية بمستوى الوعي بالأمن السيبراني تبعاً لمتغير الجنس ونرفض الفرضية البديلة القائلة بوجود فروقات معنوية ذات دلالة إحصائية بمستوى الوعي بالأمن السيبراني تبعاً لمتغير الجنس.

2-اختبار متغير الصفة المستقل مع متغير الوعي بالأمن السيبراني المعتمد. الجدول (6) ادناه يوضح بيانات اختبار الأنوفا لمتغير الصفة مع متغير الوعي بالأمن السيبراني.

جدول (6): جدول تحليل انوفا بين متغير الصفة ومتغير الوعي بالأمن السيبراني

الصفة	الوسط الحسابي	الانحراف المعياري	F المحسوبة	F الجدولية	Sig.	الدلالة الإحصائية
تدريسي	2.043	0.512	0.113	3.940	0.737	غير دال احصائياً
موظف	2.076	0.409				

المصدر: من اعداد الباحث بالاعتماد على نتائج تحليل البيانات باستخدام SPSS

يتضح من بيانات الجدول (6) أعلاه بان قيمة F المحسوبة أصغر من قيمة F الجدولية وان قيمة .Sig أكبر من مستوى المعنوية 0.05، ما يعني بانه لا توجد فروقات ذات دلالة إحصائية عند مستوى معنوية 0.05 بمستوى الوعي بالأمن السيبراني تبعاً لمجموعات متغير الوصف (تدريسي، موظف). مما تقدم نقبل الفرضية **الرئيسية** الثالثة القائلة بعدم وجود فروقات معنوية ذات دلالة إحصائية بمستوى الوعي بالأمن السيبراني تبعاً لمتغير الصفة ونرفض الفرضية البديلة القائلة بوجود فروقات معنوية ذات دلالة إحصائية بمستوى الوعي بالأمن السيبراني تبعاً لمتغير الصفة.

3-اختبار متغير المؤهل العلمي المستقل مع متغير الوعي بالأمن السيبراني المعتمد. الجدول (7) ادناه يوضح بيانات اختبار الأنوفا لمتغير الصفة مع متغير الوعي بالأمن السيبراني.

جدول (7): جدول تحليل انوفا بين متغير المؤهل العلمي ومتغير الوعي بالأمن السيبراني

المؤهل العلمي	الوسط الحسابي	الانحراف المعياري	F المحسوبة	F الجدولية	Sig.	الدلالة الإحصائية
بكالوريوس	2.075	0.413	0.073	2.70	0.974	غير دال احصائياً
دبلوم عالٍ	2.100	0.512				
ماجستير	2.027	0.476				
دكتوراه	2.061	0.541				

المصدر: من اعداد الباحث بالاعتماد على نتائج تحليل البيانات باستخدام SPSS

يتضح من بيانات الجدول (7) أعلاه بان قيمة F المحسوبة أصغر من قيمة F الجدولية وان قيمة .Sig أكبر من مستوى المعنوية 0.05، ما يعني بانه لا توجد فروقات ذات دلالة إحصائية عند مستوى معنوية 0.05 بمستوى الوعي بالأمن السيبراني تبعاً لمجموعات متغير المؤهل العلمي (بكالوريوس، دبلوم عال، ماجستير، دكتوراه). مما تقدم نقبل الفرضية **الرئيسية** الرابعة القائلة بعدم وجود فروقات معنوية ذات دلالة إحصائية بمستوى الوعي بالأمن السيبراني تبعاً لمتغير المؤهل العلمي ونرفض الفرضية البديلة القائلة بوجود فروقات معنوية ذات دلالة إحصائية بمستوى الوعي بالأمن السيبراني تبعاً لمتغير المؤهل العلمي.

4-اختبار متغير سنوات الخدمة المستقل مع متغير الوعي بالأمن السيبراني المعتمد. الجدول (8) ادناه يوضح بيانات اختبار الأنوفا لمتغير الصفة مع متغير الوعي بالأمن السيبراني.

جدول (8): جدول تحليل انوفا بين متغير سنوات الخدمة ومتغير الوعي بالأمن السيبراني

سنوات الخدمة	الوسط الحسابي	الانحراف المعياري	F المحسوبة	F الجدولية	Sig.	الدلالة الإحصائية
1–10 سنة	2.075	0.394	0.148	2.70	0.931	غير دال احصائياً
11–15 سنة	2.018	0.525				
16–20 سنة	2.075	0.431				
أكثر من 20 سنة	2.096	0.485				

المصدر: من اعداد الباحث بالاعتماد على نتائج تحليل البيانات باستخدام SPSS

يتضح من بيانات الجدول (8) أعلاه بان قيمة F المحسوبة أصغر من قيمة F الجدولية وان قيمة .Sig أكبر من مستوى المعنوية 0.05، ما يعني بانه لا توجد فروقات ذات دلالة إحصائية عند مستوى معنوية 0.05 بمستوى الوعي بالأمن السيبراني تبعاً لمجموعات متغير سنوات الخدمة (1–10 سنة، 11–15 سنة، 16–20 سنة، أكثر من 20 سنة). مما تقدم نقبل الفرضية **الرئيسية** الخامسة القائلة بعدم وجود فروقات معنوية ذات دلالة إحصائية بمستوى الوعي بالأمن السيبراني تبعاً لمتغير سنوات الخدمة ونرفض الفرضية البديلة القائلة بوجود فروقات معنوية ذات دلالة إحصائية بمستوى الوعي بالأمن السيبراني تبعاً لمتغير سنوات الخدمة.

المحور الرابع: الاستنتاج والمقترحات:

الاستنتاجات:

1- يوجد مستوى وعي بالأمن السيبراني بين السادة التدريسيين والموظفين في كلية الإدارة والاقتصاد/ جامعة الموصل.
2- وجود مستوى وعي منخفض نسبياً في بعض فقرات محاور الامن السيبراني لكنها لم تؤثر على مستوى الوعي العام.
3- لا يوجد دور لعامل الشهادة او سنوات الخدمة في تحديد مستوى الوعي بالأمن السيبراني لدى المنتسبين حيث لم تسجل أي فروقات ذات دلالة إحصائية في مستوى الوعي بالأمن السيبراني بين افراد العينة المبحوثة تبعاً لجنسهم او صفتهم او تحصيلهم الدراسي او سنوات الخدمة لديهم.
4- هناك حاجة الى تعزيز مستوى الوعي بالأمن السيبراني في بعض فقرات الامن السيبراني والتي أظهرت مستوى اتفاق منخفض من قبل المستجيبين.

المقترحات:

1- الاستعانة بمختصين في الامن الرقمي لإقامة دورات تطويرية على مستوى الكلية تركز في مضمونها على الفقرات التي حازت على اقل نسبة اتفاق في إجاباتها. بالإضافة الى دورات متقدمة للكادر ذو اختصاص الحاسبات في الكلية ليكونوا مرجع لبقية المنتسبين في الكلية.
2- العمل على تطوير شبكة انترنت داخلية تتمتع بخصائص حماية إضافية لأغراض العمل الإداري لا يمكن من خلالها الولوج الى مواقع التواصل الاجتماعي او مواقع الانترنت غير الموثوقة والتي تمثل مصدر خطر كبير للاختراقات والهجمات السيبرانية.

3- شمول الإداريين الذين يعملون على إدارة أنظمة المعلومات في الكلية بدورات دورية منتظمة تطلعهم على اهم الادوات والطرق الحديثة للتعامل مع مخاطر الهجمات السيبرانية وطرق التعامل مع الهجمة السيبرانية حال وقوعها والتعافي منها بأقل الخسائر الممكنة.

4- بالتعاون مع مركز الحاسبة الالكترونية في الجامعة، يتم جعل تراخيص الدخول الى الأنظمة الإلكترونية من داخل شبكة انترنت الجامعة حصراً حيث لا يمكن الولوج لتلك الأنظمة من خارج شبكة الجامعة، وذلك من اجل توفير مستوى حماية إضافية لأنظمة المعلومات ومنع دخول أي شخص من خارج محيط الجامعة.

المصادر:

أولا: العربية

1- الصائغ، عمر والسواط، حمود، واخرون. (2020). وعي المعلمين بالأمن السيبراني وأساليب حماية الطلبة من مخاطر الإنترنت وتعزيز القيم والهوية الوطنية لديهم. *مجلة كلية التربية (أسيوط)*, *36*(6), 41-90.

2- أ. م. د. سالم، ماجد صدام. (2022). الامن السيبراني العراقي وأثره في قوة الدولة. *مجلة العلوم التربوية والإنسانية*، (18), 69-84.

3- خليفة، ايهاب. (2019). الامن السيبراني الماهية والاشكاليات. القاهرة: أوراق مصرية

4- الرنتيسي، محمود وعقل، مجدي. (2011). تكنولوجيا التعليم بين النظرية والتطبيق، غزة، فلسطين.

5- شلوش، نورة. (2018). القرصنة الالكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدولة. مجلة بابل للدراسات الإنسانية. العدد 2 المجلد 8، 199

6- مهدي، لبنى خميس وصفاء، تغريد. (2020). أثر السيبرانية في تطور القوة. حمورابي، 145-161.

7- رزوقة، اسماعيل. (2019). الفضاء السيبراني والتحول في مفاهيم القوة والصراع. الجزائر: مجلة العلوم القانونية والسياسية، العدد 1، المجلة 10.

8- سليمان، علي فاضل. (2020). حق الدفاع الشرعي عن الهجمات السيبرانية. تكريت: مجلة جامعة تكريت للحقوق، العدد 4، المجلد4.

9- ياسين، احمد. (2014). الحروب المستقبلية في القرن الحادي والعشرين. أبو ظبي: مركز الامارات للبحوث الاستراتيجية.

ثانياً: الاجنبية

1- Albrechtsen, E. (2007), "A qualitative study of users' view on information security", Computers & Security, Vol. 26 No. 4, pp. 276-289.

2- Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2). https://doi.org/10.3390/bdcc5020023

3- Huraj, L., Lengyelfalusy, T., Hurajová, A., & Lajčin, D. (2023). Measuring Cyber Security Awareness: A Comparison between Computer Science and Media Science Students. *TEM Journal*, *12*(2), 623–633. https://doi.org/10.18421/TEM122-05

4- Furnell, S. (2008), "End-user security culture: a lesson that will never be learnt?", Computer Fraud & Security, Vol. 2008 No. 40, pp. 6-9.

5- Rezgui, Y. and Marks, A. (2008), "Information security awareness in higher education: an exploratory study", Computers & Security, Vol. 27 Nos 7-8, pp. 241-253.

10- Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.-J. (2009), "The impact of information richness on information security awareness training effectiveness", Computers & Education, Vol. 52 No. 1, pp. 92-100.
11- Choo, K.-K.R. (2011), "The cyber threat landscape: challenges and future research directions", Computers & Security, Vol. 30 No. 8, pp. 719-731.
12- Amy Borrett and Georges Corbineau, **Cybersecurity rankings reveal leading global cyber powers,** TECHMOINITOR, Nov. 27, 2020, https://translate.google.com/translate?sl=auto&tl=ar&u=https://techmonitor.ai/cybersecurity/cybersecurity-rankings-reveal-leading-global-cyber-powers, ACCESSED ON 09/11/2021
13- Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23.
14- Eilts, D. (2020). An empirical assessment of cybersecurity readiness and resilience in small businesses.
15- Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2023). A security awareness and competency evaluation in the energy sector. *Computers & Security*, *129*, 103199.
16- 3-Joseph S. Nye, J. (2010). *Cyber Power.* Harvard College: Belfer Center for Science and International Affairs.
17- Przyborski, K., Breitinger, F., Beck, L., & Harichandran, R. S. (2019)." CyberWorld" as a Theme for a University-wide First-year Common Course.
18- Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & security*, *27*(7-8), 241-253.
19- John Chapman. 2020. Cyber security in universities and colleges is improving, but there's no room for complacency. https://www.jisc.ac.uk/blog/cybersecurity-in-universities-and-colleges-is-improving-but-theres-no-room-forcomplacency- 20-oct-2020.
20- Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, *4*(10).
21- Darrell Eilts. 2020. An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Computing and Engineering. (1106) https://nsuworks.nova.edu/gscis_etd/1106.
22- Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.
23- Chapman, J., Chinnaswamy, A., & Garcia-Perez, A. (2018, January). The severity of cyber attacks on education and research institutions: a function of their security posture. In *Proceedings of ICCWS 2018 13th international conference on cyber warfare and security. Academic Conferences and Publishing Limited* (pp. 111-9).

ثالثاً: مواقع الانترنت:

1- *4 things you can do to keep yourself Cyber safe | CISA*. (2022, December 18). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe

2- Team, A. (2023, December 11). *The Top 10 cybersecurity Best practices for 2023*. American Technology Services. https://networkats.com/best-cyber-security-practice-2023/
3- Milmo, D. (2024, February 7). *Ransomware gangs staged a "major comeback" last year.* The Guardian. https://amp.theguardian.com/technology/2024/feb/07/ransomware-gangs-staged-comeback-last-year-says-crypto-research-firm.
4- الموقع الرسمي لكلية الإدارة والاقتصاد. https://uomosul.edu.iq/administrationeconomic