دور الجامعات في في تحقيق الأمن السيبراني من خلال الكليات والاقسام والمناهج التي تحقق هذا الهدف

The role of universities in achieving cybersecurity through colleges, departments, and curricula that achieve this goal

أ. م . د . مسلم طاهر حسون م . د . كريم لفتة مشاري
كلية القانون / جامعة أهل البيت (ع)

المستخلص
أن مصطلح الأمن السيبراني يطلق على أمن المعلومات وأمن العمليات الالكترونية وأمن الشبكات وأمن التطبيقات ويمثل خطوات دفاعية عن البيانات والمعلومات على جميع الاجهزة الالكترونية المرتبطة بشبكة الانترنيت من التهديدات والهجمات الضارة وأعمال القرصنة وسرقة المعلومات للوصول للمعلومات الحساسة والشخصية لتغييرها وتدميرها وبالتالي التأثير على الامن الشخصي والامن الوطني، وتبرز أهمية دور الجامعات في تحقيق الثقافة السيبرانية والامن السيبراني والمسؤولية المجتمعية لادارة المخاطر من خلال دمج مبادئ الامن السيبراني في المناهج الدراسية فضلا عن تجهيز الطلبة بالمهارات والمعارف اللازمة التي تتماشى والمنظور الدولي للاتجاهات الناشئة في أطار الامن السيبراني مع ضرورة تعزيز الوعي لدى طلبة الجامعات والكليات بأهمية الامن السيبراني مما يؤهلهم لمواجهة مختلف التحديات الامنية السيبرانية المعاصرة ، وأن التعاون بين الجامعات والمؤسسات الحكومية وغير الحكومية يمكن أن يعزز من قدرات الامن الوطني والدفاع السيبراني ويسهم في حماية الاصول الوطنية من التهديدات والهجمات السيبرانية وهذا يسمح بتطور أستراتيجيات مشتركة وتبادل الخبرات ومن شأنه أن يحقق القدرات الامنية فضلا عن تطوير حلول مبتكرة لمواجهة التهديدات السيبرانية المتطورة، وعلى هذا الاساس تأتي أهمية تسليط الضوء ضمن بحثنا هذا على مفهوم الامن السيبراني وبيان دور الجامعات والكليات في تحقيق الامن السيبراني .

الكلمات المفتاحية : الامن السيبراني ، دور الجامعات والكليات ، تحقيق الامن السيبراني ، التحديات والتهديدات السيبرانية ،المؤسسات الاكاديمية

Abstract

The term cybersecurity refers to information security, electronic operations security, network security, and application security. It represents defensive steps for data and information on all electronic devices connected to the Internet from threats and malicious attacks, hacking, and information theft to access sensitive and personal information to change and destroy it, thus affecting personal and national security

The importance of the role of universities in achieving cyber culture cybersecurity, and social responsibility for risk management is highlighted by integrating cybersecurity principles into curricula, in addition to equipping students with the necessary skills and knowledge that are in line with the international perspective of emerging trends in the framework of cybersecurity, with the need to enhance awareness among university and college students of the importance of cybersecurity, which qualifies them to face various contemporary cybersecurity challenges

Cooperation between universities, governmental and non-governmental institutions can enhance national security and cyber defense capabilities and contribute to protecting national assets from cyber threats and attacks. This allows for the development of joint strategies and the exchange of expertise, which will achieve security capabilities as well as the development of innovative solutions to confront advanced cyber threats. On this basis, the importance of highlighting the concept of cyber security and explaining the role of universities and colleges in achieving cyber security comes

Keywords: Cyber security, the role of universities and colleges. achieving cyber security, cyber challenges and threats, academic institutions

المقدمة

أولاً :ـ موضوع البحث

الأمن السيبراني هو عبارة عن مجموعة من الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك

بهدف ضمان توافر واستمرارية عمل نظام المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني وبالتالي فالأمن السيبراني يمثل سلاح استراتيجي بيد الحكومات والأفراد ولاسيما ان الحرب السيبرانية باتت جزء لا يتجزأ من التكتيكات الحديثة للنزاعات المسلحة والهجمات بين الدول والأمن السيبراني في ظل المؤسسات الجامعية يعني تطبيق التقنيات والضوابط لحماية الانظمة الجامعية من الهجمات السيبرانية ويمثل مجموعة من الممارسات التي يتم استخدامها من قبل الجامعات للحماية من الوصول غير المصرح به الى مراكز البيانات والانظمة المختلفة فضلاً عن انه يعد استراتيجية امنة ضد الهجمات السيبرانية المصممة للوصول الى تعديل أو حذف أو تدمير او ابتزاز انظمة الجامعة الالكترونية

ثانياً :- اهمية البحث

تكمن اهمية البحث في ندرة الدراسات العلمية التي تناولت الأمن السيبراني في الجامعات والكليات العراقية فضلاً عن الأهمية التي تنطلق من تعدد الهجمات والتهديدات السيبرانية وممارسة المهام الادارية والفنية والالكترونية الجامعية الكترونياً مما يستوجب الاهتمام بممارسات الأمن السيبراني والأهمية الاساسية تكتسب من اهمية دور الجامعات والكليات في تحقيق الأمن السيبراني الوطني والجامعي

ثالثاً :- مشكلة البحث

ان البيئة الجامعية تضم اشكالات الكترونية رقمية مختلفة وانظمة معلوماتية متنوعة فضلاً عن انظمة تحتية متعددة الطلبات مع مستويات مختلفة من الشبكات والاتصالات وهذه البيئة الجامعية المفتوحة اصبحت مفتوحة للتهديدات والانتهاكات السيبرانية الالكترونية مما يستوجب ايجاد حلول كفوءة وفعالة لمواجهتها وعلى هذا الاساس فإن من الضروري وفي

اطار مشكلة البحث تسليط الضوء على بيان دور الجامعات والمؤسسات الاكاديمية في تحقيق الأمن السيبراني من خلال الكليات والاقسام الجامعية لتحقيق تلك الأهداف .

رابعاً :- منهجية البحث

استعدت طبيعة البحث الى استخدام المنهج الوصفي والتحليلي لملائمته لهذا البحث من خلال جمع المعلومات وتحليلها والمتعلقة بالاتجاهات الحديثة في الادارة الالكترونية الجامعية والآليات والأسس التي ترتكز عليها في فلسفة الأمن السيبراني في الجامعات.

خامساً :- هيكلية البحث

لغرض الاحاطة بموضوع بحثنا سنقوم بتقسيمه وفق خطة علمية تتضمن مطلبين يسبقهما مقدمة وتنتهي بخاتمة لاهم النتائج والمقترحات التي تم التوصل اليها

المطلب الأول : مفهوم الأمن السيبراني

الفرع الأول : تعريف الأمن السيبراني

الفرع الثاني : الامن السيبراني في ضوء التشريعات الوطنية المقارنة

المطلب الثاني: آليات الجامعات والكليات لتحقيق الأمن السيبراني

الفرع الأول : تدابير الأمن السيبراني في الجامعات والكليات

الفرع الثاني : الجامعات والكليات ودورها في تعزيز الأمن السيبراني

الخاتمة - النتائج - المقترحات

المطلب الأول: مفهوم الأمن السيبراني

أصبح الأمن السيبراني من أكثر الأمور أهمية بسبب التطور المتنامي لاستخدام الفضاء السيبراني من قبل الدول او المنظمات سواء كانت دولية ام محلية وهذا جعل الاستغناء عنه امراً مستحيلاً لاتصاله المباشر بالحياة المعاصرة فضلاً عن صلته الوثيقة بكافة مجالاتها العامة وخاصة فيما يتعلق بالسياسة والخصوصية والمعلومات التقنية .

والأمن السيبراني يعد الحجر الأساس الذي تعتمد عليه كافة الدول في جميع مؤسساتها الرسمية وغير الرسمية وان الاهتمام به يعد هدف من اهداف تحقيق الأمن الوطني لأي دولة وعلى هذا الاساس أصبح الأمن السيبراني حاجة رئيسة لكافة الدول كونه يتمكن من حمايتها وبناها التحتية الخاصة بها من الاعتداء والتدخل بصورة غير المشروعة لفرض السيطرة او التدمير أو السرقة،وسنتناول في هذا الإطار تعريف الأمن السيبراني في الفرع الأول بينما سيكون الثاني مخصصاً لبيان الأمن السيبراني في ضوء التشريعات الوطنية

الفرع الاول: تعريف الامن السيبراني

ان مهمة الامن السيبراني تكمن في حماية امن الدولة القومي والمعلوماتي من الهجمات السيبرانية الذكية بوصفه الركيزة الاساسية لاي مجتمع ومن غير الممكن تصور تقدم اي دولة وازدهارها بدون تحققه حيث تحول الامن السيبراني مع تزايد النشاطات في الفضاء السيبراني الى واحد من قطاع الخدمات التي تعد دعامة اساسية لأنشطة الدول والمنظمات على حد سواء ولعل ظهور الثورة التكنولوجية الرقمية الحديثة والتي كانت نتيجتها زيادة المعلومات الهائلة في وسائل الاتصالات والانظمة الحاسوبية وبناءً على ذلك برز المفهوم الخاص بالامن السيبراني ليكون محور الجانب الامني الذي يختص بحماية قاعدة البيانات والمعلومات فالامن السيبراني مصطلح يتكون من مقطعين الامن ويقصد به

السلامة والمعنى المناقض لكلمة الخوف ويقصد به الاطمئنان وهو يدل على الثقة والطمأنينة ([١]) ،اما السيبراني فان اصلها تعود الى اللغة اليونانية ويراد بها السيطرة او التحكم وهي كلمة مشتقة من كلمة (kybemetes) ويراد بها الشخص الذي يقوم بالتحكم بالدفة الخاصة بالسفينة وهذا المصطلح اطلق على الشخص المسيطر او المتحكم ([٢])، وبالتالي فان المقصود بالأمن السيبراني التحكم عن بعد وهذه الكلمة عندما ترد مع كلمه ثانية فانها تعني الادارة عن بعد مثل ما هو موجود حالياً في الامن السيبراني ([٣]).

ومن الناحية الاصطلاحية فان الامن السيبراني من المصطلحات الحديثة حيث عدته التعريفات بحسب الزاوية التي ينظر اليه من خلالها فقد عرف على انه يمثل وسائل دفاعية من شانها كشف واحباط المحاولات التي يقوم بها القراصنة وكذلك عرف على انه مجموعة وسائل من شانها الحد من خطر الهجوم الواقع على البرامجيات واجهزة الكمبيوتر او الشبكات وتشمل الوسائل والادوات المستخدمة في مواجهة القرصنة وكشف الفيروسات وايقافها ([٤]).

وقد عرف كذلك على انه مجموعة من الوسائل التقنية والتنظيمية والادارية المستخدمة لمنع الوصول غير المصرح به وسوء الاستغلال واستعادة كافة المعلومات الالكترونية ونظام الاتصالات والمعلومات التي تحتويها لتأمين استمرارية عمل النظم المتعلقة بالمعلومات والعمل على تحقيق حماية وسرية المعلومات واتخاذ كافة التدابير اللازمة لحماية المواطن والمستهلكين من المخاطر في الفضاء السيبراني ([٥]).

وقد عرفه فريق اخر على انه الدفاع الذي يستهدف حماية الفضاء الالكتروني من كل الهجمات السيبرانية الموجهة اليه سواء كانت من الداخل أو الخارج ([٦]) ومن الناحية القانونية فقد عرف الامن السيبراني من قبل الاعتماد الدولي للاتصالات (ITu) على انه جمع الادوات والسياسات والمفاهيم الامنية والمبادئ التوجيهية واساليب ادارة المخاطر والاجراءات والتدريب وافضل الممارسات والضمانات والتقنيات التي يمكن استعمالها لحماية البيئة السيبرانية واصول المنظمات والمستخدمين ([٧]).

وفي السياق نفسه فقد عرفته وكالة الامن الاوروبية التي تعد اول من اصدر قانون الاتحاد الاوروبي للامن السيبراني عام (٢٠١٨) على انه (قدرة النظام المعلوماتي على التصدي لمحاولات الاختراق والحوادث غير المتوقعة التي من شانها استهداف البيانات المتداولة او المخزونة وفق اطار توافقي ([٨]).

ويمكن القول ان الامن السيبراني يمثل النشاط الذي من شانه تأمين الحماية لكافة الموارد سواء كانت بشرية او مادية او غير مادية او تلك الموارد المرتبطة ارتباطاً وثيقاً بالتقنيات المتعلقة بالاتصالات والمعلومات فضلاً عن انه يضمن الحد

من الخسائر المتحققة في حال حصول التهديدات بما يؤمن امكانية اعادة الحال الى ما كان عليه بأسرع وقت ممكن .

الفرع الثاني: الامن السيبراني في ضوء التشريعات الوطنية المقارنة

لقد وردت العديد من التعريفات المتعلقة بالأمن السيبراني على صعيد التشريعات الوطنية فقد عرفته وزاره الدفاع الامريكية على انه (جميع الاجراءات التنظيمية الواجبة لضمان حماية المعلومات الالكترونية من مختلف الجرائم كالهجمات والتجسس والتخزين والحوادث وغيرها)([٩]).

اما في التشريع الفرنسي فقد عرفته الوكالة الوطنية الفرنسية لنظم المعلومات على انه (مجموعة كاملة من السياسات والانشطة التي تجري في الفضاء الالكتروني والمتعلقة بالحد من التهديدات والضعف والردع والمشاركة الدولية والاستجابة للحوادث والمرونة والتعافي بما في ذلك تشغيل شبكات الكمبيوتر وامن المعلومات ومهام انفاذ القانون والدبلوماسية والعسكرية والاستخباراتية فيما يتعلق بأمن واستقرار العالم) ([١٠]).

اما بالنسبة للتشريعات العربية فقد عرفه المشرع الاردني طبقاً لقانون الامن السيبراني رقم (١٦ لسنة ٢٠١٩) على انه (الاجراءات المتخذة لحماية الانظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الامن السيبراني والقدرة على استعادة عملها واستمراريتها سواء كان الوصول اليها بدون تصريح او سوء استخدام او نتيجة الاخفاق في اتباع الاجراءات الامنية او التعرض للخداع الذي يؤدي لذلك ([١١]).

وقد اورع المشرع الاماراتي وفقاً لقانون الامن السيبراني رقم (٣ لسنة ٢٠١٢) تعريفاً للامن السيبراني على انه (تامين وحماية الشبكة المعلوماتية وشبكة الاتصالات ونظم المعلومات وعمليات جمع المعلومات باستخدام اي من الوسائل الالكترونية) ([١٢]).

اما فيما يتعلق بتعريف الامن السيبراني طبقاً للتشريع العراقي فانه على الرغم من استخدام مصطلح الامن السيبراني على الصعيد التنفيذي لكنه لم يرد تعريفاً للأمن السيبراني لكون القاعدة التشريعية المتمثلة بقانون جرائم المعلوماتية العراقي غير كاملة وعلى هذا الاساس يمكن القول على انه من الضروري العمل على تأسيس استراتيجية وطنية تتعلق بالأمن السيبراني العراقي بصورة تتوافق مع المنهج المتبع من قبل التشريعات الوطنية والمنظمات الدولية المعنية كالاتحاد الدولي للاتصالات والاتفاقيات الدولية التي صادق عليها العراق ومنها الاتفاقية العربية لمكافحة جرائم تقنيه المعلومات الموقعة في القاهرة في (٢١ / ١٢ / ٢٠١٣) من اجل تحقيق التعاون بين الدول العربية في اطار مكافحة جرائم تقنية المعلومات.

ومما سبق فان الامن السيبراني يمثل كافة التدابير والاجراءات التنظيمية والقانونية

التي يستوجب ان تتخذ من قبل الاجهزة الامنية او الاجهزة الاخرى التابعة للدولة بهدف الحفاظ على سرية المعلومات الرقمية والحد من الاختراقات الواقعة مهما كان مصدرها سواء كانت بواسطة الفيروسات او الوسائل الاخرى لكن تم وصولها لجهات ذات العلاقة في الوقت المناسب وعدم وقوعها في ايدي الاشخاص غير المصرح لهم بالوصول.

المطلب الثاني: آليات الجامعات والكليات لتحقيق الأمن السيبراني

يعبر الامن السيبراني عن ممارسات دقيقة لحماية الشبكات الالكترونية والاجهزة والبيانات الجامعية من التلف او الضياع او السرقة او الوصول غير المصرح به حكماً يحمي الأمن الجامعي للمباني والاشخاص الموجودين في الجامعات والكليات من التهديدات الامنية المختلفة فان الامن السيبراني يحمي التقنيات الرقمية ومستخدمها من المخاطر الرقمية ويعد الامن السيبراني مصطلح حديث يعرف في بعض الجامعات باسم امن تكنولوجيا المعلومات وبالاحرى امن المعلومات الالكترونية (IT) ويمثل مجموعة من الوسائل التقنية والادارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستخدام واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وفي اطار الجامعات فان الامن السيبراني يعد مجالا يهتم بحماية المعلومات القيمة في الجامعات والكليات من الهجمات السيبرانية من قبل المتسللين والجهات تسعى الى تدمير وسرقة تلك المعلومات ([١٣]).

وفي اطار الامن السيبراني في الجامعات فانه يشكل مجموعة من الاجراءات والتدابير التي تم تصميمها وتطبيقها لحماية الانظمة الالكترونية الجامعية والمعلومات الحساسة من الهجمات والتهديدات الالكترونية سواء كانت تلك التهديدات تتم داخل الجامعات او خارجها)([١٤]).

وسوف نتناول في هذا المجال تدابير الامن السيبراني في الجامعات والكليات ومن ثم نتطرق الى دور الجامعات والكليات في تعزيز الامن السيبراني .

الفرع الاول: تدابير الامن السيبراني في الجامعات والكليات

سنحاول في هذا الاطار الاشارة الى اهم تدابير الامن السيبراني والاليات التي تحيط بها من خلال ايجاز ذلك حسب الفقرات الاتية :-

اولاً :- عناصر الامن السيبراني في الجامعات والكليات

يرتبط مفهوم الامن السيبراني في الجامعات والكليات بعدة عناصر لعل اهمها

١. الموارد البشرية : كالقيادات الاكاديمية واعضاء هيئات التدريس والطلاب والاداريين وبالتالي عليهم فهم مبادئ الأمن السيبراني وممارسته.
٢. العمليات : يستوجب ان يكون لدى الجامعات اطار عمل بكيفية التعامل مع الهجمات الالكترونية بحيث يوجه جميع المستخدمين ويرشدهم باليات

تحديد الهجمات السيبرانية وحماية الانظمة واكتشاف التهديدات والاستجابة لها ومعالجتها.

٣. التكنولوجيا الحديثة : التكنولوجيا الحديثة ضرورية لمنح الجامعات بكل ما تحتويه من ملاكات تدريسية وطلاب واداريين وادوات وبرامج امان الكترونية لحماية انفسهم من التهديدات والهجمات السيبرانية([١٥]).

ثانياً :- مجالات الامن السيبراني

تتضمن استراتيجية الامن السيبراني في الجامعات على مستويات من الحماية للدفاع ضد الجرائم الالكترونية ونود الاشارة الى ابرز مجالات الامن السيبراني في الجامعات

١. امان البيئة التحتية الحرجة وهذه الممارسات لحماية انظمة الكمبيوتر الجامعية والشبكات التي تعتمد عليها الجامعات
٢. امان الشبكة وتمثل تدابير امنية لحماية شبكة الكمبيوتر من المتطفلين.
٣. امان التطبيق وهي العمليات التي تساعد في حماية التطبيقات التي تمارسها الجامعات والكليات.
٤. امان المعلومات وتمثل تدابير لحماية المعلومات والبيانات الجامعية الاكثر حساسية من الوصول غير المصرح به.
٥. تعليم المستخدم النهائي وهذا يمثل بناء الوعي الامني للموارد البشرية بالجامعات لتحقيق امنها من التهديدات والهجمات السيبرانية من خلال البرامج التدريسية المتخصصة.
٦. التعافي من الكوارث وهذه اجراءات وتدابير للاستجابة للأحداث والمخاطر غير المتوقعة او المخطط لها او المفاجئة في الكوارث الطبيعية وحوادث الامن السيبراني
٧. تامين التخزين وهي تدابير ووسائل محددة لتخزين البيانات والمعلومات الجامعية ويتضمن التشفير ونسخ البيانات الغير القابلة للتغيير ([١٦]).

ويتضح مما سبق ان مجالات الامن السيبراني في الجامعات تتحدد بين وقائية وتدخل وحماية وتطوير موارد بشرية لتحسين اساليب الفضاء على التهديدات السيبرانية وهذا المجال لا شك يوضح حجم الخطر السيبراني الذي يحيط بالجامعات وبالتالي يتطلب وجود وعي من قبل القيادات الاكاديمية للموارد البشرية وهذه المخاطر وضرورة مواجهتها باليات فعالة.

ثالثاً :- تحديات الامن السيبراني في الجامعات

ان الامن السيبراني يواجه في الجامعات تحديات متواصلة من قبل المتسللين كانتهاك الخصوصية وفقدان البيانات وزيادة المخاطر ولعل من اهم هذه التحديات

١. التحدي الاول : ان احد اكثر التحديات خطورة هي الطبيعة المتطورة للمخاطر والتهديدات الأمنية السيبرانية حيث ان مع ظهور تقنيات حديثة يتم تطوير وسائل هجوم جديدة تتلائم مع حجم التطورات في ممارسة الامن السيبراني بالجامعات حيث قد تكون مواكبة هذه التغييرات المتكررة وتحديث ممارسات الحماية منها يعد امرا صعبا على الجامعات ([١٧]).
٢. ٢- التحدي الثاني : ضمان تحديث جميع عناصر الامن السيبراني بالجامعات باستمرار للحماية من نقاط الضعف المحتملة.
٣. التحدي الثالث :سهولة اختراق الملفات الجامعية والمواقع الجامعية لعدم تامينها بشكل كافي مما يؤدي لكثرة المخربين ([١٨]).
٤. التحدي الرابع : عدم التزام بعض القيادات الجامعية التي تتبلور في عدم اكتراثها بوجود استراتيجية لتطوير الممارسات السيبرانية في الحرم الجامعي فضلا عن عدم مشاركتها في وضع خطط ادارة الازمات السيبرانية وعدم توفيرها متطلبات الامن السيبراني البشرية او المادية.
٥. التحدي الخامس هذا التحدي يتمثل في نقص كفاءة الموارد البشرية المتعلقة بالتعامل مع الهجمات السيبرانية بسبب قلة البرامج التدريبية وعموميتها وعدم مسايرتها للاتجاهات الحديثة في اطار الأمن السيبراني فضلاً عن عدم اهتمام الموارد البشرية بمجال الامن السيبراني وحصر الاهتمام على ممارسة المهام المتعلقة بالمجالات الاكاديمية والبحثية والادارية والخدمية ([١٩]).

مما سبق يتضح تعدد التحديات التي تواجه الامن السيبراني في الجامعات وبالتالي يتطلب مواجهتها بأسلوب موضوعي من خلال توفير متطلبات الامن السيبراني من وعي وفهم الملاكات الجامعية بأهمية تطوير اليات الامن السيبراني وتوفير الموارد البشرية والمادية للتعامل مع التهديدات والهجمات السيبرانية فضلا عن تطوير وتحسين مستمر لأساليب وممارسات الامن السيبراني لتنسجم مع تعدد وتنوع وتطور المحاولات التي تخترق منظومة المعلومات الجامعية الالكترونية من قبل المتسللين.

رابعاً :- اساليب التهديدات والهجمات السيبرانية للجامعات

ان طرق واساليب التهديدات والهجمات السيبرانية في الجامعات تتعدد ونشير الى ابرزها

١. التصعيد الاحتيالي وهذا يتخذ شكل رسالة بريد الكتروني او رسالة فورية وهي مستخدمة لخداع المستخدم ليثق بالمصدر في محاولة احتياله للوصول الى بياناته ومعلوماته.

٢. البرامج الضارة (برامج الفدية) هذه البرامج تمنع المستخدمين من الوصول الى الشبكة او الملفات او البيانات الخاصة بهم وتسبب في حدوث اضطرابات ومشكلات في استرجاع تلك الملفات والمعلومات والبيانات وقد يكون الهدف الاساسي من تنفيذ هذه البرامج من قبل المهاجمين الحصول على فدية مالية لاستعادة الملفات المسروقة ([٢٠]).
٣. الاختراق : وهذا يتم من خلال معرفة كلمات السر او ارقام الامان للمستخدمين ويعتمد ذلك على مهارة المهاجمين لشبكات الجامعة الالكترونية فضلا عن ضعف برامج الحماية وهذا اسهم في تسهيل هؤلاء المهاجمين الى ملفات الجامعات في كافة الانشطة والتحكم فيها ([٢١]).

وخلاصة لما سبق فان الخطأ البشري يلعب دوراً هاماً في وقوع تلك التهديدات السيبرانية لكن مع تحسين التدريب على ممارسات الامن السيبراني والتوعية بدوافع ووسائل المهاجمين وتطبيق استراتيجية واضحة من قبل الجامعات والكليات في تحقيق الامن السيبراني يمكن للجامعات والكليات ان تحمي نفسها بشكل أفضل من الهجمات السيبرانية

الفرع الثاني: الجامعات والكليات ودورها في تعزيز الامن السيبراني

تبرز اهمية دور الجامعات والكليات في تعزيز الثقافة السيبرانية من خلال دمج مبادئ الامن السيبراني في المناهج الدراسية في المؤسسات التعليمية الجامعية فضلاً عن تجهيز الملاكات التدريسية والكليات بالمهارات المطلوبة والتي تتلائم والمنظور الدولي للاتجاهات

الناشئة في مجال الامن السيبراني مع ضرورة تعزيز الوعي لديهم بأهمية الامن الشخصي والقومي بما يجعله مؤهلين لمواجهة مختلف التحديات المتعلقة بالتهديدات والهجمات السيبرانية لنظام المعلومات والشبكات الالكترونية الجامعية مع تقديم الحلول والاستراتيجيات لمنع المخاطر والحوادث بصورة فعالة وكفاءة عالية([٢٢]).

وعلى هذا الاساس لابد ان يكون التعاون قائماً وبأعلى المستويات بين الجامعات والكليات والمؤسسات الحكومية وغير الحكومية لتعزيز قدرات الامن القومي والدفاع السيبراني ويسهل في حماية الموارد الوطنية من الهجمات السيبرانية .

وجدير بالإشارة ان منع الهجمات السيبرانية للبنية التحتية الحيوية لأي دولة يعتمد بشكل اساسي على توفر قوة عاملة ماهرة ومتعلمة في مجال الانترنت ويتم ذلك من خلال نظام تعليمي يمكن من بناء القدرة اللازمة لمواجهة التحديات السيبرانية عن طريق اشخاص يتمتعون بمهارات كفؤة لاكتشاف التهديدات والهجمات السيبرانية ومواجهتها وعلى هذا الاساس يستوجب على المؤسسات التعليمية تزويد الطلاب بالمعلومات المناسبة والمناهج الدراسية وتتضمن التحديات التي يواجهها

التعليم الجامعي في مجال الامن السيبراني الى مهارات الامن السيبراني وبالتكامل الاقتصادي والاجتماعي والقدرات الهيكلية والموارد الاقتصادية لوجود حاجة ضرورية لاستراتيجية وطنية لتعريف الامن السيبراني للهيئات التدريسية والطلبة بالبرامج الاكاديمية للامن السيبراني فضلاً الى دعم قدرات البحث والتطوير الامن السيبراني وعلى هذا الاساس ينبغي الدعوة الى تعزيز كفاءة الامن الاكاديمية والتركيز على الحاجه الى بناء قدرات الامن السيبراني لتحقيق قدر اكبر من الاستعداد السيبراني لكون هذا التهديد غالبا ما تواجهه حتى الدول التي لديها استعدادات متقدمة في ظل الامن السيبراني وفيما يتعلق بالكلية ينبغي اذكاء الوعي لهم بالامن السيبراني وعلاقته بالامن الوطني وبالأمن الشخصي وهذا يتحقق من خلال تثقيف الطلبة بالممارسات التي تعزز الامن السيبراني([٢٣]). ونود الاشارة الى اهم تدابير التي تحقق الامن السيبراني في اطار طلبة الجامعات :

١. يجب تضمين متطلبات الامن السيبراني في المقررات والمناهج الدراسية في الجامعات والكليات.
٢. العمل على التطبيق العملي من خلال مختبرات الحاسوب او عن طريق القيام بعقد دورات ليتسنى للطلبة المشاركة بها واعطائهم شهادات تخرج للتشجيع على اكتساب مهارة جديدة او عمل حوارات تفاعلية مع الطلاب حول استخدام كافة الوسائل التقنية بطرق امنة.
٣. انشاء مكتبة للامن السيبراني حيث من الضروري ان تحتوي الجامعات والكليات على مكتبة متخصصة بموضوع الامن السيبراني والعلوم العلمية بصورة عامة وان تهتم

بشكل واسع بامن المعلومات والجريمة الالكترونية من خلال تخصيص جزء من مكتبة الجامعة لتضمن للجامعة الاحتواء على الكتب والدوريات ورسائل الماجستير واطروحات الدكتوراه فضلا عن الوثائق المتعلقة بموضوعات الامن السيبراني ليتمكن الطلبة من الرجوع اليها بكل سهولة ([٢٤]).

٤. العمل على القيام بالمؤتمرات والندوات والادوات العلمية من قبل الكوادر التدريسية والعمل على دعوة الباحثين المختصين والمحليين والدوليين منهم للاستفادة من خبراتهم.
٥. العمل على اصدار دراسات بحثية علمية حول احتياجات الطلاب من المعلومات لزيادة الوعي لدى الطلاب بأهمية نشر ثقافه الامن السيبراني.
٦. تعميم المهارات والاستراتيجيات التي تتيح للطلبة تعزيز امنهم وامن مجتمعاتهم الالكترونية والقانونية([٢٥]).

٧. القيام بحملات توعوية مثل تعليق البوسترات حول المخاطر السيبرانية للطلبة واعضاء الهيئات التدريسية لمعرفة تداعيات هذه التهديدات والهجمات السيبرانية فضلا عن زيادة امنهم وسلامتهم.
٨. العمل على تفعيل أنشطة الطلاب في اتجاه تنمية ثقافة الامن السيبراني.
٩. القيام بالتواصل مع مؤسسات المجتمع المدني ووسائل الاعلام كمركز لاحياء ونشر الامن السيبراني([٢٦]).

مما تقدم يتضح لنا بان الجامعات والكليات بكافة اقسامها لها دور رئيسي في تعزيز وتحقيق الامن السيبراني من خلال الممارسات اليومية والمناهج الدراسية لتامين الحماية والحصانة لكافه البيانات والانظمة المعلوماتية للشبكة الالكترونية وعلى المستوى الامن الشخصي والوطني والدولي .

الخاتمة

تعرضنا وبشكل موجز وحسب متطلبات بحثنا الموسوم ب (دور الجامعات في تحقيق الامن السيبراني من خلال الكليات والاقسام والمناهج التي تحقق هذا الهدف) وقد توصلنا الى جملة من النتائج والتوصيات نذكر البعض وكالاتي :-

اولاً :- النتائج

١. عدم رغبة بعض القيادات الجامعية في تفعيل ادوارها لتطوير ممارسات الامن السيبراني بالجامعات والكليات على اعتبار ان تلك الممارسات فنية جمة.
٢. التخوف من التكلفة المالية المرتفعة والتي يتطلبها تطوير ممارسات الامن السيبراني.
٣. معارضة بعض الموارد البشرية بالجامعات لتنفيذ الرؤية وتطوير ممارسات الامن السيبراني.
٤. ان للجامعات والكليات دور اساسي في تنمية الامن السيبراني وحماية الشبكات الالكترونية من خلال وجود الملاكات التعليمية المتخصصة بمجال الامن السيبراني فضلا عن المناهج الدراسية التي تواكب التطورات الحاصلة في مجالات التكنولوجيا الحديثة ولا سيما في اطار التهديدات والهجمات السيبرانية.
٥. لوحظ عدم وجود تشريعات وطنية صريحة تتعلق بالأمن السيبراني وخاصة في المنظومة التشريعية العراقية.
٦. ان توفير الحصانة والحماية للمعلومات والبيانات الجامعية في مجال الامن السيبراني باتت من المتطلبات الضرورية الملحة التي يفرضها واقع المعلومات الامنية الحديثة.

٧. ان دور الجامعات والكليات والاقسام في مجال الفضاء السيبراني يقتضي البحث عن اهم الاليات في مجال ادارة نظم امن المعلومات للوقوف على متطلبات نجاحها ومعالجة المعوقات التي تواجهها فضلاً عن انشاء بنية تحتية معلوماتية قادرة على العمل بكفاءة عالية.
٨. ان تفعيل دور الجامعات والمؤسسات الاكاديمية كافة في مجال الامن السيبراني يتوقف على كفاءة التشريعات الوطنية والاتفاقيات الدولية لمواجهة التهديدات السيبرانية.
٩. يمكن استخدام تقنيات الذكاء الاصطناعي لمراقبة وتقييم الامتثال للقوانين الدولية المتعلقة بالأمن السيبراني من خلال مراقبة تداول البيانات وتحليل الانتهاكات والتهديدات المحتملة.
١٠. ان انتهاكات الامن السيبراني باستخدام الذكاء الاصطناعي مثل انتهاك حقوق الملكية الفكرية وسرقة البيانات والمعلومات الجامعية والتجسس السيبراني تشكل مصدراً للمسائلة القانونية.
١١. ان التعاون القانوني والمؤسسي بين الجامعات والكليات ومؤسسات الدولة الحكومية وغير الحكومية ومنظمات المجتمع المدني يحوز في القدرة على مواجهة التهديدات السيبرانية بفعالية وكفاءة عالية ويسهم في تحقيق الامن السيبراني.
١٢ـ ان تحقيق وتعزيز المسؤولية الجنائية والدولية من شانها الاسهام في الحد من الهجمات السيبرانية.

ثانياً :- المقترحات

١. اقامة اطار قانوني شامل لتفعيل دور الجامعات والكليات والمؤسسات الجامعية لاستخدام تقنيات الذكاء الاصطناعي في مجال الامن السيبراني.
٢. تعزيز الدور الفعال للتعاون الوطني والدولي والمنظمات المتخصصة في تبادل المعلومات والخبرات في مجال الامن السيبراني فضلا عن تطوير معايير دولية للسلامة والامن السيبراني.
٣. تعزيز التوعية في المؤسسات الحكومية وغير الحكومية والمؤسسات الجامعية الاكاديمية بالمسؤولية الدولية والجنائية وتحصين وحماية المعلومات الشخصية والوطنية في مجال الامن السيبراني من خلال التدريب والتثقيف.
٤. ضرورة العمل على استراتيجية وطنية تخص الامن السيبراني الوطني العراقي في المجالات كافة وخاصة في المجال الاكاديمي الجامعي بصورة تتوافق مع المناهج المتبعة من قبل الدول الاخرى والمنظمات الدولية.

٥. التزام القيادات الجامعية بتوفير المتطلبات البشرية والمالية والمادية لتطوير ممارسات الامن السيبراني بالجامعات والكليات لتحقيق اهداف الامن السيبراني.
٦. الاشراف على تصميم وتقييم البرامج التدريبية لأعضاء الهيئات التدريسية والاداريين والطلبة بالجامعات لتنمية قدراتهم ومهاراتهم في التعامل مع التهديدات السيبرانية.
٧. انشاء مراكز متخصصة للامن السيبراني بالجامعات لوقاية الجامعات والكليات من خطر التهديدات السيبرانية وتطوير تدابير الحماية وتطوير ممارسات الامن السيبراني.
٨. العمل على تحديث برامج الامن السيبراني وباستمرار لمواجهة كافة التهديدات الالكترونية التي تواجه الجامعات والكليات فضلا عن استخدام استراتيجيات متنوعة في مجال مكافحة الهجمات السيبرانية.
٩. تطوير وتنمية العلاقات بين المؤسسات الاكاديمية والجامعات والشركات والمؤسسات المتخصصة الوطنية في مجال الامن السيبراني وذلك لتبادل الخبرات وتطوير الممارسات وللأطراف كافة.
١٠. توعية الملاكات التدريسية والطلبة بمخاطر استخدام الاجهزة الشخصية مثل الهاتف المحمول او الحاسوب لتخزين او نقل معلومات سرية خاصة بالجامعات والكليات.
١١. العمل على تشجيع الموظفين التقنيين داخل الجامعات على التعاون فيما بينهم ومع الطلبة لتحقيق الامن السيبراني،
١٢. تطوير البنية التحتية السيبرانية داخل الجامعات للحد من الاختراق والتجسس والقرصنة الالكترونية.

الهوامش

(١)د. حسام حزام ناصر القريطي ، الأمن السيبراني وحماية امن المعلومات ، ط١ ، دار الفكر الجامعي ، الاسكندرية ٢٠٢٢ ، ص ١١ .

(٢) فارس محمد العمارات ، الامن السيبراني ، المفهوم وتحديات العصر، ط١ ، دار الخليج للنشر والتوزيع ، عمان ، ٢٠٢٢ ، ص ١٤.

(٣) اسراء شريف جيجان ، الامن السيبراني الصيني ، دراسة الدوافع والاهداف مجلة قضايا سياسية ، بغداد ، العدد /٦٥ ، ٢٠٢١ ، ص ٣٦.

(٤) فارس محمد العمارات ، مصدر سابق ، ص ١٥.

(٥) امنة علي البشير محمد ، الامن السيبراني بخصوص مقاعد مقاصد البشريه في ضوء مقاصد الشريعة ، مجلة كلية الدراسات الاسلامية ، الاسكندرية ، المجلد / ١ / العدد / ٣٧ ، ٢٠٢١ ، ص ٤٦٠ .

(٦) عبد الرحمن علي اللقاني ، دور الامن السيبراني في تعزيز امن المعلومات المالية الالكترونية ، ط١ ، دار اليازوري العلمية ، ٢٠٢٢ ، ص ١٢٦.

(٧) تقرير صادر عن الاتحاد الدولية للاتصالات التابع للامم المتحدة عام ٢٠٢٢ ، تقرير خالد طاهر عبد الله دور التشريعات الجزائية في حماية الامن السيبراني بدول مجلس التعاون الخليجي ، مجلة البحوث الفقهية والقانونية العدد / ٣٨ ، ٢٠٢٢ ، ص ٩٩٥.

(٨) زمورة جمال ، اهمية حوكمة الامن السيبراني لضمان تحول رقمي امن الخدمات الحكومية في الجزائر مجلة البحوث الاقتصادية المتقدمة ، الجزائر ، المجلد السابع ، العدد / الثاني ، ٢٠٢٢ ، ص ٤١٦.

(١) زمزرة جمال ، مصدر سابق ، ص ٤١٦.
(1) Hugo Loiseau Daniel venter cybersecurity in Humanities and sicial sciences , wILEY , VOlumel , p ٣٦
(١) ينظر المادة / ١ من قانون الامن السيبراني الاردني رقم (١٦ لسنة ٢٠١٩).
(١) ينظر المادة / ١ من قانون الامن السيبراني الاماراتي رقم (٣ لسنة ٢٠١٢).
(١) منال بن ابراهيم ، الوعي بجوانب الامن السيبراني في التعليم عن بعد ، المجلة العلمية لجامعة الملك فيصل ، العلوم الانسانية والادارية ، المجلد / ٢٢ ، العدد / ٢ / الرياض ، ٢٠٢١ ، ص ٢٩٩.
(١) شيماء سراج ، التحليل البعدي لدراسات الامن السيبراني في المجال التربوي ، المجلة العربية للعلوم التربوية والنفسية ، المؤسسة العربية للتربية والعلوم والاداب ، ٢٠٢٢ ، ص ١٩٩ المجلد / ٦ / العدد / ٢٦ ، الاسكندرية.
(1) Abdulrhman o. & omar .m The impact of Applying Electronic mangement system on the Rnglish level A case study st cinan and Engineeving , p . ٤dt
(1) catota frankie , cyberseurity edueation in developing of cyber scurity , 2019 , p10
(1) Fouad Noran shafik securing hjgher education agsinst cyberthrests from an institutional risk to national policy challengr journal of cyber policy p. 137
(1)Hujran , o. , Al . Debei , M .M., The imperative ofinfluencing , citizen attiude tosard government adiption and use computrrs in Humanbehavior l.189
(1) Peker Yesen , Ray , Lydia and stephanie cyberdcurity Awareness Modules for college and High school students National cyber summit Research Track . 24
(1) Naidin Denan and Zajnuddin . Ahmad cyber scurity threat Analysis in Higher Education Institutions during Covid - 19 pandenmic . Journal of scyberscurity . P 13
(١) خالد رواسكي ، دور الجامعة في تعزيز ثقافة الامن السيبراني ، الملتقى العلمي ، كلية علوم الاعلام والاتصالات ، الجزائر ، ٢٠٢٤
(١) سالي سعد محمد ، الامن السيبراني ودور الجامعات في تعزيزه لدى الطلبة ، مركز حمورابي للبحوث والدراسات الاستراتيجية ، بغداد ، ٢٠٢٢ ، ص ٤
(١) هاني رزاق عبد الجواد الالفي ، القيادات الاكاديمية وادوارها في تعزيز ممارسات الامن السيبراني ، جامعة المنصورة ، ٢٠٢٢ ، ص ٧٣٤.
(١) علياء عمر كامل فرج ، دواعي تعزيز الامن السيبراني في ظل التحول الرقمي ، جامعة سوهاج ، ٢٠٢١ ، ص ٥٢٩.
(١) سالي سعد محمد ، مصدر سابق ، ص ٥.

المصادر

اولاً :- المصادر العربية

١. دحام حزام ناصر القريطي ، الامن السيبراني وحماية امن المعلومات ، ط١ ، دار الفكر الجامعي ، الاسكندرية ، ، ٢٠٢١.
٢. فارس محمد العمارات ، الامن السيبراني المفهوم وتحديات العصر ، ط١ ، دار الخليج للنشر والتوزيع ، عمان ، ٢٠٢٢.
٣. عبد الرحمن علي اللقاني ، دور الامن السيبراني في تعزيز امن المعلومات المالية الالكترونية ، ط١ ، دار اليازوري العلمية ، ٢٠٠٢.
٤. سالي سعد محمد ، الامن السيبراني ودور الجامعات في تعزيزه لدى الطلبة ، مركز حمورابي للبحوث والدراسات الاستراتيجية ، بغداد ، ٢٠٢٢.
٥. خالد رواسكي ، دور الجامعة في تعزيز ثقافة الامن السيبراني ، كلية علوم الاعلام والاتصالات ، الجزائر ، ٢٠٢٤.
٦. هاني رزق عبد الجواد الالفي ، القيادات الاكاديمية وادوارها في تعزيز ممارسات الامن السيبراني ، جامعة المنصورة ، ٢٠٢٢.
٧. علياء عمر كامل فرج ، دواعي تعزيز الامن السيبراني في ظل التحول الرقمي ، جامعة سوهاج ، ٢٠٢١.

ثانياً :- المجلات العلمية

١. اسراء شريف جيحان ، الامن السيبراني الصيني ، دراسة بالدوافع والاهداف ، مجلة قضايا سياسية ، بغداد ، العدد / ٦٥ ، ٢٠٢١.
٢. امنة علي البشير ، الامن السيبراني في ضوء مقاصد الشريعة مجلة كليه الدراسات الاسلامية ، الاسكندرية ، المجلد / ١ / العدد / ٣٧ ، ٢٠٢١.
٣. خالد طاهر عبد الله ، دور التشريعات الجزائرية في حماية الامن السيبراني لدول مجلس التعاون الخليجي ، مجلة البحوث الفقهية والقانونية ، العدد / ٣٨ ، ٢٠٢٢.
٤. زمورة جمال ، اهمية حوكمة الامن السيبراني لضمان تحول رقمي امن الخدمات العمومية في الجزائر ، مجلة البحوث الاقتصادية المتقدمة ، الجزائر ، / ٧ ، العدد/ ٢ ، ٢٠٢٢.
٥. منال بن ابراهيم ، الوعي بجوانب الامن السيبراني في التعليم عن بعد المجلة العلمية لجامعة الملك فيصل للعلوم الانسانية والادارية ، المجلد / ٢٢ ، العدد / ٢ ، الرياض ، ٢٠٢١.
٦. شيماء سراج التحليل البعدي لدراسات الامن السيبراني في المجال التربوي ، المجلة العربية للعلوم التربوية والنفسية ، المؤسسة العربية للتربية والعلوم والاداب ، المجلد / ٦ / العدد / ٢٦ الاسكندرية ، ٢٠٢٢.

ثالثاً :- المصادر الاجنبية

1. Hugo Loiseau , Daniel ventre cyberscurity in Humsnities and social sciences , wilty
2. Abdul rahman , o & omar I.M The imlact of Aplying Electronic msnagment system on the English , Leel Acase study at ciham university international journal of Research and Engineering
3. catita , Frankie eyberscurity education in developing nation the Ecuadorian enviroment gournal of cybersurity ٢٠١٩
4. Fouad Noran shafik securing higher education against cyberthreats from an institution risk ti national policy challenge journal of cyber policy
5. Hujran o, Al Debel M,M , Ther imperative ofinfluen cing citizen attitude tiward government adoption and use cimputers in Human Behavior
6. Peker Yesen , Ray Lydia and stephanie cyberscurity Awareness Modules for college snd High school students National cyber summit Research
7. Naidu, Denan and Zainuddin Ahmed cyber scurity Threat Analysis in Higher Educatjon instituions during covid - ly pandemic journal of cyberscurity

رابعاً :- القوانين الوطنية والاتفاقات الدولية

١. تقرير الاتحاد الدولي للاتصالات التابع للامم المتحدة لعام ٢٠٢٢
٢. قانون الامن السيبراني الاردني رقم ١٦ لسنة ٢٠١٩
٣. قانون الامن السيبراني الاماراتي رقم ٣ لسنة ٢٠١٢