المجلة الإلكترونية الشاملة متعددة التخصصات
العدد السابع والستون شهر (1) 2024

حماية المعلومات من الهجمات السيبرانية في عمادة القبول والتسجيل في جامعة الملك عبد العزيز: دراسة حالة

Repel Cyberattacks at the Deanship of Admission and Registration at King Abdulaziz University: A Case Study

د. هند بادي البادي[1]، غدي مسعد الردادي[2]

[1]halbadi@kau.edu.sa

[2] galraddadi0005@stu.kau.edu.sa

[1] أستاذ مساعد، قسم علم المعلومات، جامعة الملك عبد العزيز، جده، المملكة العربية السعودية

[2] ماجستير إدارة المعلومات، قسم علم المعلومات، جامعة الملك عبد العزيز، جده، المملكة العربية السعودية

الملخص

هدفت الدراسة الى التعرف على أهم الأسباب التي دفعت عمادة القبول والتسجيل بجامعة الملك عبد العزيز لتطبيق الأمن السيبراني. كما ركزت الدراسة على أهمية تطبيق الأمن السيبراني في عمادة القبول والتسجيل بجامعة الملك عبد العزيز من أجل الحفاظ على سرية البيانات وسلامتها من خلال الوقوف على السياسات والضوابط المتبعة في العمادة لتحقيق أمن البيانات. تكمن أهمية الدراسة في الإفادة من المعلومات المتعلقة حول الأمن السيبراني، بالإضافة إلى تحسين ضوابط ومعايير الأمن السيبراني للوقاية من الهجمات السيبرانية على الجامعة. تم جمع البيانات من خلال المقابلة الشخصية مع مسؤولة وحدة الحوكمة والمخاطر والالتزام بمركز الأمن السيبراني بجامعة الملك عبد العزيز. وكان من أهم النتائج أن عمادة القبول والتسجيل طبقت الأمن السيبراني لحماية بيانات الطلاب والطالبات وفقاً لضوابط الهيئة العامة للأمن السيبراني في حماية البيانات والحد من المخاطر السيبرانية. كما قد بينت النتائج الاهتمام الكبير من قبل مركز الأمن السيبراني تجاه موظفي العمادة في توعيتهم لتطبيق سياسات الأمن السيبراني للحفاظ على سلامة البيانات. وعليه توصي الدراسة بأهمية استمرار عمادة القبول والتسجيل في تحقيق ضوابط الهيئة العامة للأمن السيبراني لحماية البيانات، والاطلاع على رأي الموظفين المسؤولين عن الأمن السيبراني في العمادة حول سبل تعزيز وتقوية الأمن السيبراني بفاعلية لحماية البيانات.

الكلمات المفتاحية

الأمن السيبراني، الهجمات السيبرانية، الوعي السيبراني، عمادة القبول والتسجيل، جامعة الملك عبد العزيز، امن البيانات

Abstract

This study aimed to determine the primary reasons for implementing cybersecurity by the Deanship of Admissions and Registration at King Abdulaziz University in Jeddah, Saudi Arabia. The study examined the significance of cybersecurity measures to safeguard data confidentiality and integrity within the Deanship. The study sought to accomplish this by analyzing the policies and controls implemented by the Deanship to ensure data security. The importance of this study lies in gaining knowledge related to cybersecurity and enhancing cybersecurity protocols and standards to prevent cyberattacks on university data. The study gathered data through an interview with the head of the Governance, Risk, and Compliance Department at the Cybersecurity Center of King Abdulaziz University. One of the key findings indicated that the implementation of cybersecurity by the Deanship aimed to protect the data of both male and female students and comply with the controls set by the General Authority for Cybersecurity in safeguarding data. To ensure data security and confidentiality, King Abdulaziz University adheres to the policies and controls set by the National Cybersecurity Authority laid out to protect data and minimize cyber risks. Additionally, the results revealed a strong commitment from The Center for Cyber Security in raising awareness among the deanship employees about the importance of implementing cybersecurity policies to preserve data integrity. Consequently, the study suggests the continued implementation of the controls set by the General Authority for Cybersecurity to protect data, as well as obtaining input from the cybersecurity personnel in the Deanship to enhance further and fortify cybersecurity measures effectively.

Keywords:

Cyber security, Cyber-attacks, Cyber awareness, Deanship of Admission & Registration, King Abdulaziz University, Data Security

المقدمة

شهدت تكنولوجيا المعلومات والاتصالات في الآونة الأخيرة تغييرات جذرية، حيث أصبح العالم بأسره على ترابط وتواصل، وباتت تكنولوجيا المعلومات هي المسيطرة؛ بل إنها أصبحت الدافع الرئيسي الذي يقود قضية الازدهار والتطور، وباتت حياتنا تعتمد بشكل كبير على التكنولوجيا. وعلى الرغم من الإيجابيات التي صاحبت التكنولوجيا والإنترنت إلا أنه أوجد انعكاسات سلبية بسبب سوء الاستخدام، ومن أبرز تلك الانعكاسات: الجرائم السيبرانية، التي تفاقمت مخاطرها سواء على الدولة أو الأفراد. (ابن إبراهيم، ٢٠٢١). كما ظهرت أنواع خطرة من الجرائم السيبرانية التي تعتمد على التقنيات المتطورة كالذكاء الاصطناعي، والبرامج الخبيثة لاختراق أنظمة المنظمة، للقيام بالتهديد والابتزاز. (أحمد، ٢٠٢٢). تزايدت الهجمات الإلكترونية في العقود القليلة الماضية نظراً للتحول الالكتروني لمعظم او جميع القطاعات والجهات (الصحية، التعليمية، المصرفية، الثقافية،...الخ). ويعد قطاع التعليم العالي أحد الجهات التي تأثرت بهذه الهجمات، حيث يعد قطاع التعليم العالي هدفًا رئيسيًا لمجرمي الإنترنت بسبب الكميات الهائلة من البيانات الحساسة المخزنة في أنظمة الجامعات ومعاهد التدريب ونحوه، مما يجعل قطاع التعليم العالي يواجه تحديات كبيره في ضمان امن المعلومات والشبكات من بيانات الطلبة والموظفين والمنسوبين. تحوي الجامعات اعداد هائلة من الطلبة والطالبات والموظفين والمنسوبين، وعليه فإن حجم المعلومات لتي يتطلب حمايتها هائل جدا، مما يشكل تحديات أمام أقسام تكنولوجيا المعلومات لإدارة شبكتها الواسعة من الأجهزة وحماية معلوماتها كذلك. لذلك أصبح الأمن السيبراني عنصرًا لا غنى عنه في حماية بيانات ومعلومات الجامعات حتى تستطيع الجامعات مواجهة الهجمات السيبرانية (Haque, et al., 2023, Argaw, et al., 2020).

سعت المملكة العربية السعودية الى التحول الالكتروني لتسهيل حياة المواطنين، واخذت بالحسبان أهمية الحفاظ على امن المعلومات لكل من المواطنين والمقيمين والهيئات، الجهات الحكومية والخاصة، الوزارات وغيره. وعليه حققت المملكة العربية السعودية إنجازاً عالمياً في الحفاظ على امن المعلومات وحصولها على المرتبة الثانية عالمياً في مؤشر الأمن السيبراني؛ وذلك حسب تقرير الكتاب السنوي للتنافسية العالمية لعام ٢٠٢٢، الذي نشره مركز التنافسية العالمي التابع للمعهد الدولي للتنمية الإدارية في سويسرا IMD، إذ يعد التقرير من أكثر التقارير شمولية في العالم، ويسعى التقرير لتصنيف وتنظيم مقدرة الدول لإيجاد البيئة الداعمة لتطويرها والحفاظ عليها (صحيفة سبق الإلكترونية، ٢٠٢٢).

وإدراكاً من المملكة العربية السعودية لأهمية الأمن السيبراني، ومن باب تحقيق الأمن والمحافظة عليه، أنشئت المملكة العربية السعودية هيئة الأمن السيبراني، والاتحاد السعودي للأمن السيبراني والبرمجة والدرونز، للحفاظ على الأمن ومواكبة التطورات في مجال المعلومات والتكنولوجيا. (شلوش، ٢٠١٨). إضافة إلى ذلك، فإن المؤسسات الاكاديمية كالجامعات تعد من أبرز البيئات التي يتم مهاجمتها وسرقة بياناتها، كالسرقة العلمية والقرصنة على موقع الجامعة والتهديدات السيبرانية. كما تحتوي بعض الجامعات على عدد من الطلاب البعض منهم بمستويات ضعيفة، والبعض الأخر بمستويات مرتفعة فيقوم بالبحث عن الثغرات الموجودة في أنظمة الجامعة وشبكاتها ويقوم بإتلافها، على عكس الفئة الأولى

من الطلاب التي قد يُتلف الأنظمة بدون قصد، ونتيجة لذلك فقد تكون تلك الاختراقات فقط لإبراز قدراتهم أمام زملائهم. (الصاحب، ٢٠١٣). وعليه يجب على المؤسسات الأكاديمية الحفاظ على سرية البيانات والمعلومات من خلال تطبيق الجدران النارية، وكلمات التشفير التي تحافظ على أصل المعلومة في المؤسسة. (الشوابكة، ٢٠١٩).

وعليه جاءت هذه الدراسة للتعرف على أهم الاسباب التي دفعت عمادة القبول والتسجيل بجامعة الملك عبد العزيز بمدينة جدة في المملكة العربية السعودية لتطبيق الأمن السيبراني والتعرف على أهم الضوابط والسياسات المتبعة لتطبيق الأمن السيبراني في عمادة القبول والتسجيل بجامعة الملك عبد العزيز.

أهمية الدراسة

- الأهمية النظرية

يُسهم هذا البحث في الإفادة من المعلومات المتعلقة حول الأمن السيبراني وأهمية تطبيقه في مؤسسات التعليم من أجل الحفاظ على البيانات والمعلومات الإلكترونية.

- الأهمية التطبيقية

١. يُسهم هذا البحث في تحسين ضوابط ومعايير الأمن السيبراني المستخدمة لحماية البيانات من مخاطر التهديدات والهجمات السيبرانية على الجامعات، من خلال النتائج والتوصيات التي توصلت إليها الدراسة.
٢. تُفيد هذه الدراسة بالارتقاء بالجامعة لجعلها مؤسسة تعليمية تمتاز بوجود أنظمة سيبرانية وضوابط وسياسات تحقق لها ميزة تنافسية بين الجامعات الأخرى.
٣. تُفيد هذه الدراسة الحالية الباحثين؛ لعمل دراسات مستقبلية متعلقة بتقنية الأمن السيبراني التي تطبق في الجامعات.

مشكلة الدراسة

ما هي قواعد وسياسات الأمن السيبراني المطبقة في عمادة القبول والتسجيل في جامعة الملك عبد العزيز لضمان سرية المعلومات والبيانات لمنسوبي الجامعة في ظل تفاقم في الجرائم الالكترونية؟

تساؤلات الدراسة

١. ماهي الاسباب التي دفعت عمادة القبول والتسجيل في جامعة الملك عبد العزيز لتطبيق الامن السيبراني؟
٢. ماهي السياسات والضوابط المتبعة لتحقيق الأمن السيبراني في عمادة القبول والتسجيل في جامعة الملك عبد العزيز؟
٣. ما أبرز البرامج والأدوات المستخدمة لتحقيق الأمن السيبراني في عمادة القبول والتسجيل بجامعة الملك عبد العزيز؟
٤. ما مدى تمكن الموظفين والموظفات في عمادة القبول والتسجيل بجامعة الملك عبد العزيز من تطبيق الامن السيبراني لحماية المعلومات؟

أهداف الدراسة

تسعى الدراسة إلى تحقيق الأهداف التالية:

١- تحديد الأسباب التي دفعت عمادة القبول والتسجيل بجامعة الملك عبد العزيز لتطبيق الأمن السيبراني.
٢- الكشف عن السياسات والضوابط المتبعة لتحقيق الأمن السيبراني في عمادة القبول والتسجيل بجامعة الملك عبد العزيز.
٣- التعرف على البرامج والأدوات المستخدمة لتحقيق الأمن السيبراني في عمادة القبول والتسجيل بجامعة الملك عبد العزيز.
٤- قياس درجة الوعي بأهمية استخدام تقنية الأمن السيبراني وأهمية تطبيقه لدى موظفي عمادة القبول والتسجيل بجامعة الملك عبد العزيز.

حدود الدراسة

اقتصرت الدراسة على الحدود التالية:

- الحدود الموضوعية: التعرف على سبل الوقاية من الهجمات السيبرانية لحماية المعلومات المتبعة بعمادة القبول والتسجيل شطر الطالبات بجامعة الملك عبد العزيز بمدينة جدة في المملكة العربية السعودية.
- الحدود الزمانية: 2023م / 1444هـ.
- الحدود المكانية: عمادة القبول والتسجيل شطر الطالبات بجامعة الملك عبد العزيز بمدينة جدة في المملكة العربية السعودية.
- الحدود البشرية: المسؤولين عن الأمن السيبراني بعمادة القبول والتسجيل بجامعة الملك عبد العزيز.

مصطلحات الدراسة

١. الأمن السيبراني Cyber security

عرفت (المنتشري، ٢٠٢٠) الأمن السيبراني بأنه الإجراءات التي يتم إتباعها لحماية شبكات المعلومات من محاولة التلاعب بالمعلومات، والتسبب بالأضرار للمستخدمين، بما في ذلك حماية المستخدمين من الاختراق والفيروسات الضارة، والوصول غير المشروع للأشخاص وغيرها من الأساليب الضارة التي تهدف لتعديل أو تعطيل تلك البيانات والمعلومات المخزنة على شبكة المعلومات.

كما عرفته الهيئة الوطنية للأمن السيبراني على انه: حماية لأنظمة تقنية المعلومات والشبكات ومكوناتها من الأجهزة والبرمجيات، من الاختراقات أو التعديلات غير المشروعة، بالإضافة إلى شمول مفهوم الأمن السيبراني لأمن المعلومات والأمن الإلكتروني والأمن الرقمي. (الهيئة الوطنية للأمن السيبراني، 2018، ص٣٢)

وتعرفه الدراسة إجرائياً بأنه: الإجراءات والعمليات التي تقوم بها المؤسسات للحد من الاختراقات والهجمات غير المشروعة للأنظمة، بهدف حماية البيانات والشبكات من أي تلاعب أو تعديل عليها، أو الوصول غير المصرح به لتلك البيانات.

٢. مركز الأمن السيبراني Cyber Security Center

ويقصد بمركز الأمن السيبراني في هذه الدراسة بأنه مركز مبني بمواصفات عالمية يهدف إلى التصدي للهجمات السيبرانية بجامعة الملك عبد العزيز بمنهجية سليمة، كما يعمل على ارسال تحذيرات وبرامج توعية على البريد الالكتروني لجميع منسوبي الجامعة.

٣. الهجمات السيبرانية Cyber attacks

فعل يضعف من قدرات وظائف الموارد التقنية المتمثلة في أجهزة الحاسب الآلي وأنظمتها، وبياناتها، والشبكات المتصلة بها، عن طريق استغلال ثغرة أو نقطة ضعف ما، تُمكن المهاجم من استغلال الموارد التقنية بطريقة غير مسموح بها (شلوش، ٢٠١٨).

اي عمل سيبراني الاستخدام ضد نظام المعلومات بطريقة تسبب حادثًا سيبرانيًا يهدف إلى انتهاك السياسة الأمنية والتسبب في تلف الخدمات او المعلومات (Li & Liu, 2021).

تعرف الدراسة الهجمات السيبرانية اجرائياً على أنها: هجوم غير مشروع يتسبب بأضرار مادية ويهدف الى انتهاك معلومات وبيانات الأشخاص والجهات بغرض التخريب أو السرقة.

٤. الأمن السيبراني في المؤسسات الأكاديمية Cyber Security in Academic institutions

أداة أمنة تحقق الحماية الكاملة للبيانات (ماشوش، ٢٠١٨).

عُرف الأمن السيبراني بأنه جميع التدابير التي يتم اتخاذها لحماية شبكات المعلومات وأجهزة الحاسب الآلي بهدف الحفاظ على سلامة تلك المعلومات من أي تعديل أو حذف أو اخترق أو دخول غير مشروع لتلك الأجهزة والشبكات، كما يشمل الأمن السيبراني تلك التدخلات الفنية التي تعمل على حماية البيانات من أي تعديل أو دخول غير مشروع بما في ذلك أمن الفضاء الإلكتروني (Richardson, et al., 2020)

وتعرفه الدراسة إجرائياً بأنه: عمليات الحماية والاحتياطات والوسائل التقنية التي تقوم بها المؤسسات الأكاديمية، بهدف حماية المصادر المختلفة من (البيانات الرقمية الشخصية، البرمجيات، البيانات الخاصة بالمؤسسة) من الاختراقات غير المشروعة، واتخاذ الإجراءات الأمنية المناسبة لحماية منسوبي المؤسسة من مخاطر الاختراقات السيبرانية.

٥. الأمن السيبراني في المملكة العربية السعودية

إدراكاً من المملكة العربية السعودية لأهمية الأمن السيبراني في تصدي الهجمات جميع قطاعات الدولة توافقاً مع رؤية المملكة العربية السعودية ٢٠٣٠م، جاء الأمر الملكي بأنشاء الهيئة الوطنية للأمن السيبراني ١٤٣٩/٢/١١هـ - ٢٠١٧/١٠/٣١م، لحماية البيانات والأنظمة التقنية من أخطار الهجمات الإلكترونية. ومن اختصاصات الهيئة وضع ضوابط ومعايير الأمن السيبراني وإرسالها للمؤسسات الحكومية، لتطبيقها والتقييد بها تفادياً للمخاطر السيبرانية المحتملة. وفي تاريخ ١٤٣٩/١١/١٠هـ - ٢٠١٨/٧/٢٣م، صدر الأمر السامي بأن "على جميع الجهات الحكومية رفع مستوى أمنها السيبراني لحماية شبكاتها وأنظمتها وبياناتها الإلكترونية، والالتزام بما تصدره الهيئة الوطنية للأمن السيبراني من سياسات وأطر ومعايير، وضوابط وإرشادات بهذا الشأن"(الضوابط الأساسية للأمن السيبراني،٢٠١٨). واكمالاً لما بدأته الهيئة، تم إنشاء ضوابط الأمن السيبراني للبيانات (DCC – 1: 2022) لتمكن المؤسسات الحكومية من الحفاظ على البيانات وسريتها وإتاحتها في الوقت المناسب لمن هو مخول بذلك.

الدراسات السابقة:

ركزت دراسة (المنيع، ٢٠٢٢) على واقع تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠. واعتمدت الدراسة على المنهج الوصفي التحليلي، كما تكون المجتمع البحثي من موظفين تقنين للجامعات السعودية التالية: (جامعة أم القرى، جامعة الإمام عبد الرحمن بن فيصل، جامعة الإمام محمد بن سعود الإسلامية)، وطبقت الاستبانة على عينة عشوائية عددهم (٢١٠) موظف. وتوصلت الدراسة إلى مجموعة من النتائج أهمها اتفاق عينة الدراسة بنسبة عالية فيما يخص متطلبات تحقيق الأمن السيبراني في الجامعات السعودية، كذلك اتفاقهم على المعوقات التي تحيل من تحقيق الأمن السيبراني. وقد خرجت الدراسة بالعديد من التوصيات من أبرزها: نشر التوعية بين الموظفين بمخاطر استخدام الأجهزة الشخصية لنقل المعلومات المهمة والسرية في الجامعات، وتقديم الحوافز لتشجيع الموظفين في مجال الأمن السيبراني.

تهدف دراسة (الشهري، ٢٠٢١) إلى توضيح الدور الذي تؤديه إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لدى طلبة كلية التربية بجامعة الإمام محمد بن سعود الإسلامية، ومعرفة مدى الوعي بماهية الأمن السيبراني لدى الطلبة. واعتمدت الدراسة على المنهج الوصفي المسحي، وتم توزيع استبانة على عينة مكونة من (١٨٨) طالب وطالبة، وتوصلت الدراسة لعدد من النتائج من أبرزها أن طلاب كلية التربية بجامعة الإمام محمد بن سعود الإسلامية لديهم معرفة متوسطة بالأمن السيبراني، وأن ممارسة إدارة الجامعة لدورها في تعزيز الوعي بالأمن السيبراني لدى هؤلاء الطلبة جاءت بدرجة متوسطة. وقدمت الدراسة بعض التوصيات منها: مساندة إدارة الجامعة لطلابها بالتوعية بمخاطر الأمن السيبراني من خلال إقامة البرامج والحملات التوعوية، واستقطاب الجامعة لمختصين بالتقنية للتعريف بالأمن السيبراني وأفضل الاستخدامات الصحيحة للتقنية.

تناولت دراسة (البيشي، ٢٠٢١) واقع الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقافة الرقمية من وجهة نظر أعضاء هيئة التدريس، وتم استخدام المنهج الوصفي التحليلي، واعتمدت الدراسة على أداة الاستبانة وتم تطبيقها على عينة عشوائية مكونه من (٢١٠) عضو هيئة تدريس، وتوصلت الدراسة الى انه من وجهة نظر عينة الدراسة أن نسبة واقع الأمن السيبراني المطبق في الجامعات السعودية مرتفعة (٧٣,١٨%)، و نسبة مستوى الثقة الرقمية لدى الجامعات السعودية كذلك مرتفعة (٧٤,٥٨%)، كما يؤثر الأمن السيبراني في تعزيز الثقة الرقمية بنسبة (٤٦,٧٠%)، وأوصت الباحثة بوضع ميزانية لمتطلبات الأمن السيبراني، و إلقاء الضوء على برامج أمن المعلومات وتوفيرها لتحقيق الثقة من قبل المستفيد. هدفت الدراسة التي أجرتها (القحطاني، ٢٠١٩) إلى التعرف على مدى توفر الوعي بالأمن السيبراني لدى طلبة الجامعات السعودية من منظور اجتماعي، واستخدمت الدراسة منهج المسح الاجتماعي بأسلوب العينة، وتم توزيع استبانة على عينة عشوائية مكونة من (٤٨٦) طالبا وطالبة. وتوصلت الدراسة إلى مجموعة من النتائج أبرزها أن المفهوم الأقرب من وجهة نظر العينة للأمن السيبراني هو "تطبيق عدد من الأساليب التقنية والإدارية التي تعمل على منع الاختراقات غير المشروعة والتلاعب بالبيانات من حذف وتعديل، بالإضافة لمنع استعادة نظم المعلومات والمعاملات الإلكترونية من قبل المخترقين للقيام بإعمال الإتلاف للبيانات والأجهزة"، ويعد النصب الإلكتروني من أكثر الجرائم السيبرانية التي يتعامل معها الأمن السيبراني في العصر الحالي. كما وضحت الدراسة بعض المعوقات الاجتماعية التي تعيق وقايتهم من الجرائم السيبرانية، وأوصت الدراسة بأهمية التوعية ووضع العقوبات على مرتكبي الجرائم السيبرانية.
هدفت دراسة (Chizanga et al., 2022) إلى تقييم العوامل الرئيسية المؤثرة على الوعي بالأمن السيبراني في مكافحة الجرائم السيبرانية والتحقق من وعي أعضاء هيئة التدريس بالأمن السيبراني في الجامعات الكينية العامة من خلال التحليل الوصفي. اعتمدت الدراسة على توزيع أداة الاستبيان على أعضاء هيئة التدريس من ٣١ جامعة ٧٥(٥٢,٦%) رجلاً، و٦٨(٤٧,٦%) امرأة. وخلصت الدراسة إلى أن عدد كبير من المشتركين ليس لديهم التدريب الكافي في مجال الأمن السيبراني، وأن معظم الجامعات ليس لديها سياسية إلزامية للأمن السيبراني. كما توصلت الدراسة إلى أن غالبية المشتركين لا يدركون ماهية كلمة المرور القوية، وكيفية الحفاظ على معلوماتهم الشخصية. ومن المتوقع من الجامعات الكينية العامة أن تحقق الأمان الكامل للمعلومات، وبذلك تكون قادرة على صد الهجمات السيبرانية من خلال تطبيقها لضوابط أمن المعلومات والأمن السيبراني.
هدفت دراسة (Alharbi & Tassaddiq, 2021) إلى فحص وتقييم الوعي بالأمن السيبراني لدى طلاب جامعة المجمعة عن طريق توزيع استبيان على عينة من الطلاب والطالبات. ومن أهم النتائج التي توصلت إليها الدراسة أن ٢١% من الطلاب لم يكونوا على دراية بمخاطر تثبيت البرامج المجانية من مصادر غير موثوقة، وأن ٤٢,٧% من الطلاب يستخدمون كلمات مرور قوية. وتوصي الدراسة بأنه يجب على جامعة المجمعة تقوية وتعزيز المعرفة حول عوامل الأمن السيبراني، وأن أساليب التثقيف السلبية مثل البريد الإلكتروني غير كافية لتوعية الطلاب، بل يجب أن تقوم بإدراج الدورات التدريبية في مجال الأمن السيبراني بانتظام، للتأكد من أن جميع الطلاب على دراية كافية بكيفية التصدي للهجمات

السيبرانية. تهدف دراسة (Ulven, & Wangen, 2021) إلى مراجعة الأدبيات الحالية المتعلقة بمخاطر الأمن السيبراني في مؤسسات التعليم العالي، تتبنى الدراسة الأسلوب المكتبي، حيث وجد أن البحث التجريبي في نطاق مخاطر الأمن السيبراني في التعليم العالي نادر، كما أتضح وجود فجوة كبيرة في النتائج التي قامت بها الدراسات والأبحاث على مدار فترة زمنية تتجاوز ١٢ عاماً. ولكن أتضح وجود اتفاق على ضرورة توافر متطلبات و مصادر الأمن السيبراني وأهميته في الحفاظ على أمن وسلامة المعلومات من التهديدات الإلكترونية، بالإضافة إلى اكتشاف تسعة مخاطر إلكترونية تتطلب وجود الأمن السيبراني.

تهدف دراسة (Von Solms & Van Niekerk, 2013) لمعرفة الفرق بين مصطلحي الأمن السيبراني وأمن المعلومات، فالكثير يستخدم مصطلح الأمن السيبراني بالتبادل مع مصطلح أمن المعلومات بالرغم من وجود تداخل كبير بين الأمن السيبراني وأمن المعلومات، إلا أن المصطلحين غير متماثلين تماماً. إضافة إلى ذلك، تفترض الدراسة أن الأمن السيبراني يفوق نطاق أمن المعلومات التقليدي التي لا تشمل حماية موارد المعلومات فقط، بل تشمل حماية الأصول الأخرى، بما في ذلك الشخص نفسه. في أمن المعلومات، الإشارة إلى العامل البشري غالباً ما تتعلق بدور (أدوار) البشر في العملية الأمنية. أما في جانب الأمن السيبراني هذا العامل يوجد له بُعد إضافي، وهو اعتبار البشر أهداف للهجمات السيبرانية أو حتى المشاركة بدون قصد في هجوم إلكتروني. هذا البعد الإضافي له آثار أخلاقية على المجتمع عموماً، فيجب حماية بعض الفئات الضعيفة، كالأطفال، حيث يمكن اعتبارها مسؤولية مشتركة.

التعقيب على الدراسات السابقة

اتفقت الدراسات السابقة على أهمية تطبيق تقنية الأمن السيبراني في الجامعات لحماية البيانات والمعلومات، خاصةً مع التحول الرقمي حيث ارتفعت معدلات الهجمات السيبرانية واختراق البيانات مما دعى الجامعات إلى الحرص على توفير بيئة أمنة للبيانات والعمليات الرقمية من خلال اتباع السياسات والضوابط الخاصة بالأمن السيبراني. واتفقت الدراسة الحالية مع دراسة (المنيع، ٢٠٢٢) في أهمية نشر التوعية بين الموظفين بمخاطر استخدام الأجهزة الشخصية لنقل المعلومات المهمة والسرية في الجامعات. وتتفق كذلك الدراسة الحالية مع دراسة (الشهري،٢٠٢١) ودراسة (القحطاني، ٢٠١٩) ودراسة (Alharbi, & Tassaddiq, 2021) في جانب الحاجة لمساندة إدارة الجامعة لطلابها بالتوعية بالأمن السيبراني من خلال إدراج الدورات التدريبية في مجال الأمن السيبراني، للتأكد من أن جميع الطلاب على دراية كافية بكيفية التصدي للهجمات السيبرانية. واتفقت دراسة (البيشي، ٢٠٢١) مع الدارسة الحالية في أنه يجب إلقاء الضوء على أهم برامج أمن المعلومات وتوفيرها في الجامعة لتحقيق الثقة من قبل المستفيد. وتتفق دراسة (Ulven, & Wangen, 2021) مع الدراسة الحالية على ضرورة توافر متطلبات ومصادر الأمن السيبراني وأهميته في الحفاظ على أمن وسلامة المعلومات من التهديدات الإلكترونية. كما تتفق الدراسة التي أجرها (Chizanga et al.,2022) مع الدراسة الحالية في أهمية تطبيق الجامعة لضوابط أمن المعلومات والأمن السيبراني لتكون قادرة على صد الهجمات السيبرانية وتحقيق الأمان الكامل للمعلومات. واتفقت الدراسة الحالية مع دراسة (Von Solms & Van Niekerk, 2013) في توضيح الفرق بين

مصطلحي الأمن السيبراني وأمن المعلومات، حيث أن الأمن السيبراني يفوق نطاق أمن المعلومات التقليدي التي لا تشمل حماية موارد المعلومات فقط، بل تشمل حماية الشخص نفسه. وتميزت الدراسة الحالية عن بقية الدراسات في مجال الأمن السيبراني في طرحها لأهم السياسات والضوابط المتبعة في مجال الأمن السيبراني في جامعة الملك عبد العزيز.

منهج الدراسة وادواته

منهج الدراسة

اعتمدت الدراسة على منهج دراسة الحالة؛ الذي يخدم موضوع البحث ويساعد على الإجابة على التساؤلات المطروحة من خلال إجراء المقابلة، كذلك الاطلاع على الإنتاج الفكري المتعلق بموضوع الأمن السيبراني.

مجتمع وعينة الدراسة

تكون مجتمع الدراسة من المسؤولين عن الأمن السيبراني بعمادة القبول والتسجيل شطر الطالبات، وتم إجراء المقابلة مع مسؤولة وحدة الحوكمة والمخاطر والالتزام بمركز الأمن السيبراني بجامعة الملك عبد العزيز، بمدينة جدة، في المملكة العربية السعودية.

تم إجراء مقابلة شخصية مع مسؤولة وحدة الحوكمة والمخاطر والالتزام بمركز الأمن السيبراني بجامعة الملك عبد العزيز.

أداة الدراسة

اعتمدت الدراسة على المقابلة الشخصية، كأداة رئيسية في جمع البيانات حول موضوع الدراسة لمعرفة مدى التزام عمادة القبول والتسجيل في تطبيق الضوابط التي وضعت من قبل الهيئة الوطنية للأمن السيبراني لحماية امن معلوماتها. وعليه تم إجراء المقابلة مع مسؤولة وحدة الحوكمة والمخاطر والالتزام بمركز الأمن السيبراني بجامعة الملك عبد العزيز للحصول على إجابات تساعد في إتمام الدراسة. (الجدول 1)

النتائج والمناقشة

تحليل البيانات

اصدرت الهيئة الوطنية للأمن السيبراني سبعة ضوابط للأمن السيبراني وعملت على تعميمها على الجهات ومتابعة آلية الالتزام والتطبيق لضمان امن المعلومات في المملكة العربية السعودية. وعليه اعتمدت الدراسة الحالية على نوعين من الضوابط للأمن السيبراني (الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للبيانات) وذلك لتحليل نتائج الدراسة والوقوف على الضوابط والتشريعات التي اعتمدتها عمادة القبول والتسجيل لضمان حماية امن وسرية المعلومات.

يوضح الشكل رقم (1,2,3,4) الضوابط الأساسية للأمن السيبراني وضوابط الأمن السيبراني للبيانات والتي اعتمدتها عمادة القبول والتسجيل في جامعة الملك عبد العزيز.

1 حوكمة الأمن السيبراني (Cybersecurity Governance)

١-١-١	برنامج التوعية والتدريب بالأمن السيبراني
الهدف	ضمان التأكد من أن العاملين بالجهة لديهم التوعية الأمنية اللازمة وعلى دراية بمسؤولياتهم في مجال الأمن السيبراني. والتأكد من تزويد العاملين بالجهة بالمهارات والمؤهلات والدورات التدريبية المطلوبة في مجال الأمن السيبراني لحماية الأصول المعلوماتية والتقنية للجهة والقيام بمسؤولياتهم تجاه الأمن السيبراني.
الضوابط	
١-١-١	يجب تطوير واعتماد برنامج للتوعية بالأمن السيبراني في الجهة من خلال قنوات متعددة دورياً، وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره، وبناء ثقافة إيجابية للأمن السيبراني.
١-١-٢	يجب تطبيق البرنامج المعتمد للتوعية بالأمن السيبراني في الجهة.
١-١-٣	يجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها، بما في ذلك: ١-١-٣-١ التعامل الآمن مع خدمات البريد الإلكتروني خصوصاً مع رسائل التصيد الإلكتروني. ١-١-٣-٢ التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين. ١-١-٣-٣ التعامل الآمن مع خدمات تصفح الإنترنت. ١-١-٣-٤ التعامل الآمن مع وسائل التواصل الاجتماعي.
١-١-٤	يجب توفير المهارات المتخصصة والتدريب اللازم للعاملين في المجالات الوظيفية ذات العلاقة المباشرة بالأمن السيبراني في الجهة، وتصنيفها بما يتماشى مع مسؤولياتهم الوظيفية فيما يتعلق بالأمن السيبراني، بما في ذلك: ١-١-٤-١ موظفو الإدارة المعنية بالأمن السيبراني. ١-١-٤-٢ الموظفون العاملون في تطوير البرامج والتطبيقات والموظفون المشغلون للأصول المعلوماتية والتقنية للجهة. ١-١-٤-٣ الوظائف الإشرافية والتنفيذية.
١-١-٥	يجب مراجعة تطبيق برنامج التوعية بالأمن السيبراني في الجهة دورياً.

شكل (1) برنامج التوعية والتدريب بالأمن السيبراني (الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، 2018)

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-٧	حماية البيانات والمعلومات (Data and Information Protection)
الهدف	ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
الضوابط	
١-٧-٢	يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة، والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة.
٢-٧-٢	يجب تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة.
٣-٧-٢	يجب أن تغطي متطلبات الأمن السيبراني لحماية البيانات والمعلومات بحد أدنى ما يلي: ١-٣-٧-٢ ملكية البيانات والمعلومات. ٢-٣-٧-٢ تصنيف البيانات والمعلومات وآلية ترميزها (Classification and Labeling Mechanisms). ٣-٣-٧-٢ خصوصية البيانات والمعلومات.
٤-٧-٢	يجب مراجعة تطبيق متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة دورياً.

شكل (2) حماية البيانات والمعلومات (الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، 2018)

٢-١٣	إدارة حوادث وتهديدات الأمن السيبراني (Cybersecurity Incident and Threat Management)
الهدف	ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعّال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة، مع مراعاة ما ورد في الأمر السامي الكريم رقم ٣٧١٤٠ وتاريخ ١٤ / ٨ / ١٤٣٨هـ.
الضوابط	
١-١٣-٢	يجب تحديد وتوثيق واعتماد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.
٢-١٣-٢	يجب تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة.
٣-١٣-٢	يجب أن تغطي متطلبات إدارة حوادث وتهديدات الأمن السيبراني بحد أدنى ما يلي: ١-٣-١٣-٢ وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد. ٢-٣-١٣-٢ تصنيف حوادث الأمن السيبراني. ٣-٣-١٣-٢ تبليغ الهيئة عند حدوث حادثة أمن سيبراني. ٤-٣-١٣-٢ مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة. ٥-٣-١٣-٢ الحصول على المعلومات الاستباقية (Threat Intelligence) والتعامل معها.
٤-١٣-٢	يجب مراجعة تطبيق متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة دورياً.

شكل (3) إدارة حوادث وتهديدات الأمن السيبراني (الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، 2018)

٢ تعزيز الأمن السيبراني (Cybersecurity Defense)

٢-١	إدارة هويات الدخول والصلاحيات (Identity and Access Management)					
الهدف	ضمان حماية الأمن السيبراني للوصول المنطقي (Logical Access) إلى الأصول المعلوماتية والتقنية للجهة؛ من أجل منع الوصول غير المصرح به، وتقييد الوصول إلى ما هو مطلوب؛ لإنجاز الأعمال المتعلقة بالجهة.					
الضوابط		مستوى تصنيف البيانات				
١-١-٢	بالإضافة للضوابط الفرعية ضمن الضابط ٢-٢-١ في الضوابط الأساسية للأمن السيبراني، يجب أن تغطي متطلبات الأمن السيبراني المتعلقة بإدارة هويات الدخول والصلاحيات، بحد أدنى، ما يلي:	عام	مقيد	سري	سري للغاية
	١-١-١-٢ التقييد الحازم بالسماح للحد الأدنى من العاملين للوصول والاطلاع ومشاركة البيانات بناء على قوائم صلاحيات مقتصرة على موظفين سعوديين إلا بموجب استثناء من قبل صاحب الصلاحية (رئيس الجهة أو من يفوضه) وعلى أن يتم إعتمادهذه القوائم من قبل صاحب الصلاحية.			✓	✓
	٢-١-١-٢ منع مشاركة قوائم الصلاحيات المعتمدة مع الأشخاص غير المصرح لهم.		✓	✓	✓
٢-١-٢	إدارة هويات الدخول وصلاحيات الاطلاع على البيانات باستخدام أنظمة إدارة الصلاحيات الهامة والحساسة (Privileged Access Management).		✓	✓	✓
٣-١-٢	بالإضافة للضابط الفرعي ٢-٢-٥ في الضوابط الأساسية للأمن السيبراني، يجب مراجعة قوائم الصلاحيات المعتمدة والصلاحيات المستخدمة للتعامل مع البيانات حسب المدة المحددة لكل مستوى.	كل سنة على الأقل		كل ٣ أشهرعلى الأقل	

شكل (4) إدارة هويات الدخول والصلاحيات (الهيئة الوطنية للأمن السيبراني، ضوابط الأمن السيبراني للبيانات، ٢٠٢٢)

يوضح الجدول رقم (1) أهم سبل الوقاية من الهجمات السيبرانية لدى عمادة القبول والتسجيل في جامعة الملك عبد العزيز، من خلال تحليل اسئلة المقابلة الشخصية والوقوف على الأسباب التي دفعت الجامعة لتطبيق الامن السيبراني، والسياسات والضوابط المتبعة لتحقيق الأمن السيبراني. إضافة الى معرفة أبرز البرامج والأدوات المستخدمة لتحقيق الأمن السيبراني، ومعرفة مدى تمكن الموظفين والموظفات في عمادة القبول والتسجيل في جامعة الملك عبد العزيز من تطبيق الامن السيبراني لحماية المعلومات. ولتحليل البيانات، اعتمدت الدراسة برنامج SWOT لمعرفة مواطن القوة والضعف والتي تتمثل في أهمية تطبيق الامن السيبراني على ملفات عمادة القبول والتسجيل (الشكل 5).

جدول رقم (١) الأسئلة والإجابات المطروحة في المقابلة الشخصية

السؤال	الإجابة
1 - ماهي الأسباب التي دفعت عمادة القبول والتسجيل في جامعة الملك عبد العزيز لتطبيق الامن السيبراني؟	بناء على الإجابة أتضح أن عمادة القبول والتسجيل قامت بتطبيق الأمن السيبراني لحماية البيانات والمعلومات الشخصية والدرجات الخاصة بالطلاب والطالبات من الاختراقات والتهديدات في الفضاء السيبراني، بالإضافة إلى تحقيقها لضوابط الهيئة الوطنية للأمن السيبراني في حماية البيانات، من خلال تطبيقها لوثيقة ضوابط الأمن السيبراني الخاصة بالبيانات. وبناء على تلك المعطيات ترى الدراسة الاهتمام الكبير من قبل مركز الأمن السيبراني في وضع واعتماد السياسات والضوابط المتعلقة بالأمن السيبراني ومتابعة الالتزام بها، لتحافظ من خلالها على أمن وسلامة البيانات والشبكات داخل الحرم الجامعي.
2 - ماهي السياسات والضوابط المتبعة لتحقيق الأمن السيبراني في عمادة القبول والتسجيل في جامعة الملك عبد العزيز؟	بناء على المعطيات التي حصلت عليها الدراسة خلال المقابلة الشخصية أتضح أن جامعة الملك عبد العزيز تتبع سياسات وضوابط وآليات الحوكمة التي أصدرتها الهيئة الوطنية للأمن السيبراني، فمن خلال مركز الأمن السيبراني في الجامعة يتم إرسال تلك السياسات والضوابط لكل قطاعات الجامعة ليتم الالتزام بها تفادياً للهجمات السيبرانية.
3 - ما أبرز البرامج والأدوات المستخدمة لتحقيق الأمن السيبراني في عمادة القبول والتسجيل بجامعة الملك عبد العزيز؟	يتبين من خلال الإجابة أنه يوجد برامج وأدوات مستخدمة تُرسل من وزارة التعليم، إضافة إلى برامج تُرسل من الهيئة الوطنية للأمن السيبراني لتمكن العمادة من حماية بياناتها، ولم يتم الإفصاح عن أسماء البرامج والأدوات المستخدمة بسبب سرية وحساسية الموضوع.

4- ما مدى تمكن الموظفين والموظفات في عمادة القبول والتسجيل في جامعة الملك عبد العزيز من تطبيق الامن السيبراني لحماية المعلومات؟	كشفت الإجابة عن هذا السؤال الاهتمام الكبير الذي يقدمه مركز الأمن السيبراني بتقديم التوعية لجميع منسوبي الجامعة بعمل كروت توعوية لموظفين القطاعات في الجامعة وتشمل موظفين عمادة القبول والتسجيل، كذلك تقديم التوعية للطلاب عبر العديد من القنوات مثل البريد الإلكتروني، والورش التدريبية، ووسائل التواصل الاجتماعي، وكذلك عمل ورشات عمل لتوعية الموظفين لتطبيق سياسات الأمن السيبراني لحماية البيانات.

يوضح الشكل رقم (5) تحليل مواطن القوة والضعف لتطبيق الامن السيبراني في عمادة القبول والتسجيل. حيث ان اهم الأسباب التي دعت الجامعة لتطبيق الأمن السيبراني فيما يخص بيانات الطلبة والطالبات وأعضاء هيئة التدريس ومن في حكمهم هي؛ تزايد نسبة الاختراقات السيبرانية حول العالم وقلة وعي المستخدمين بالتهديدات والمخاطر السيبرانية. كما تكمن اهم نقاط الضعف في عدم إدراك بعض المنسوبين والطلاب لمخاطر الاختراقات السيبرانية.

شكل رقم (5) تحليل مواطن القوة والضعف لتطبيق الامن السيبراني في عمادة القبول والتسجيل

نتائج الدراسة

أظهرت الدراسة أن:

١- عمادة القبول والتسجيل في جامعة الملك عبد العزيز طبقت أمن المعلومات لحماية (بيانات الطلاب والطالبات ومنسوبي الجامعة، والدرجات، والمعلومات الشخصية)، بالإضافة لتحقيق ضوابط الهيئة العامة للأمن السيبراني في حماية البيانات.

٢- تتبع جامعة الملك عبد العزيز السياسات والضوابط وآليات الحوكمة التي أصدرتها الهيئة الوطنية للأمن السيبراني لتقليل المخاطر السيبرانية، وتعتبر الضوابط الأساسية للأمن السيبراني ضوابط إلزامية، ومن أمثلة تلك الضوابط (الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، ٢٠١٨):

أ- يجب تطوير واعتماد برنامج للتوعية بالأمن السيبراني في الجهة من خلال قنوات متعددة دورياً، وذلك لتعزيز الوعي بالأمن السيبراني وتهديداته ومخاطره، وبناء ثقافة إيجابية للأمن السيبراني، ضمن المكون الفرعي برنامج التوعية والتدريب بالأمن السيبراني رقم (١-١-١٠) (الشكل 1).

ب- يجب أن يغطي برنامج التوعية بالأمن السيبراني كيفية حماية الجهة من أهم المخاطر والتهديدات السيبرانية وما يستجد منها، ضمن المكون الفرعي برنامج التوعية والتدريب بالأمن السيبراني رقم (1-10-3) (الشكل1).

ت- يجيب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجهة، والتعامل معها وفقاً للمتطلبات التشريعية والتنظيمية ذات العلاقة، ضمن المكون الفرعي حماية البيانات والمعلومات رقم (2-7-1) (الشكل 2).

ث- يجيب تحديد وتوثيق واعتماد متطلبات إدارة حوادث وتهديدات الأمن السيبراني في الجهة، ضمن المكون الفرعي إدارة حوادث وتهديدات الأمن السيبراني رقم (2-13-1) (الشكل 3).

ج- التقييد الحازم بالسماح للحد الأدنى من العاملين للوصول والاطلاع ومشاركة البيانات بناء على قوائم صلاحيات مقتصرة على موظفين سعوديين إلا بموجب استثناء من قبل صاحب الصلاحية وعلى أن يتم اعتماد هذه القوائم من قبل صاحب الصلاحية، ضمن المكون الفرعي إدارة هويات الدخول والصلاحيات رقم (2-1-1-1) (الشكل 4).

ح- إدارة هويات الدخول وصلاحيات الاطلاع على البيانات باستخدام أنظمة إدارة الصلاحيات الهامة والحساسة، ضمن المكون الفرعي إدارة هويات الدخول والصلاحيات رقم (2-1-2) (الشكل 4).

٣- اعتماد البرامج والأدوات التي تُرسل من وزارة التعليم، إضافة إلى برامج من الهيئة العامة للأمن السيبراني لتمكن العمادة من حماية بياناتها.

٤- بينت نتائج الدراسة الاهتمام الكبير الذي يقدمه مركز الأمن السيبراني بعمل كروت توعوية لموظفين القطاعات في الجامعة وتشمل موظفين عمادة القبول والتسجيل، وكذلك عمل ورشات عمل لتوعوية الموظفين لتطبيق سياسات الأمن السيبراني لحماية البيانات.

التوصيات والمقترحات

بناءً على النتائج توصي الدراسة بـ:

١- أهمية استمرار عمادة القبول والتسجيل في تحقيق ضوابط الهيئة العامة للأمن السيبراني لحماية البيانات.

٢- الاطلاع على رأي الموظفين المسؤولين عن الأمن السيبراني بالعمادة حول سبل تعزيز وتقوية الأمن السيبراني بشكل أكثر فاعلية لحماية البيانات.

٣- إجراء المزيد من الدراسات حول سبل الوقاية من الهجمات السيبرانية في الجامعات.

الخاتمة

الأمن السيبراني أمر في غاية الأهمية لحماية سرية وسلامة البيانات من الهجمات السيبرانية. لذلك على الجامعات رفع مستوى أمنها السيبراني، وأتابع السياسات والضوابط التي من شأنها الحفاظ على البيانات من الاختراقات. فالبيئة الجامعية تعد من أبرز البيئات التي يتم اختراقها وسرقة بياناتها لما تحتويه من بيانات سرية وذات أهمية بالغة. فبدأت عمادة القبول والتسجيل في تطبيق تقنية الأمن السيبراني لكي تحافظ على سلامة البيانات التي تمتلكها من الاختراقات، ووضع الضوابط الخاصة بالأمن السيبراني بعمادة القبول والتسجيل. كما اشارت نتائج الدراسة الحالية إلى اهتمام مركز الأمن السيبراني في تقديم التوعية اللازمة لموظفي العمادة لتوعيتهم بأهمية الأمن السيبراني وأهمية تطبيقه، كما تتبع جامعة الملك عبد العزيز سياسات وضوابط الهيئة الوطنية للأمن السيبراني للوقاية من الهجمات السيبرانية.

المراجع

ابن إبراهيم، منال حسن محمد. (٢٠٢٠). الوعي بجوانب الأمن السيبراني في التعليم عن بعد. المجلة العلمية لجامعة الملك فيصل – العلوم الإنسانية والإدارية، مج٢٢، ع٢، ٢٩٩-٣٠٧.

احمد، فاطمة علي إبراهيم، يوسف، رحاب فايز أحمد، والسيد، وليد محمود. (٢٠٢٢) الأمن السيبراني والنظافة الرقمية. المجلة المصرية لعلوم المعلومات، مج٩، ع٢، ٣٩٠-٤٢٢.

البيشي، منير عبد الله مفلح. (٢٠٢١). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة. مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، مج ٢٩, ع٦، ٣٥٣-٣٧٢.

شلوش، نورة. (٢٠١٨). القرصنة الإلكترونية في الفضاء السيبراني، التهديد المتصاعد لأمن الدول، مجلة مركز بابل للدارسات الإنسانية، جامعة بابل، العراق، مج٨، ع٢.

الشهري، مريم بنت محمد فضل. (٢٠٢١). دور إدارة الجامعة في تعزيز الوعي بالأمن السيبراني لدى طلبة كلية التربية بجامعة الإمام محمد بن سعود الإسلامية. مجلة العلوم الإنسانية والإدارية، ع٢٥. ٨٣-١٠٤.

الشوابكة، عدنان عواد، (٢٠١٩). دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف. مجلة دراسات وأبحاث، مج١١، ع٤، ١٦٤-١٨٧.

الصاحب، محمود حسن. (٢٠١٣). سياسة أمن المعلومات في الجامعات: حالة دراسية. *[سيبريان جورنال]*، مج. ٢٠١٣، ع. ٣٣.

القحطاني، نورة بنت ناصر. (٢٠١٩) مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية. شؤون اجتماعية، مج٣٦, ع١٤٤، ٨٥-١٢٠.

ماشوش، مراد. (٢٠١٨). الجهود الدولية لمكافحة الإجرام السيبراني .*مجلة القانون والأعمال، ع٣٧، ١٦٧-١٩٩ .*

المملكة تحقق المرتبة الثانية عالمياً في مؤشر الأمن السيبراني. (٢٠٢٢). في *صحيفة سبق*.
https://2u.pw/RbLBb75

المنتشرى، فاطمة يوسف، وحريري، رندة. (٢٠٢٠). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات .*المجلة العربية للتربية النوعية، ع ١٤، ٩٥-١٤٠ .*

المنيع، الجوهرة بنت عبد الرحمن إبراهيم (٢٠٢٢). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠. مجلة كلية التربية، مج ٣٨, ع١ – ١٥٥-١٩٤.

الهيئة الوطنية للأمن السيبراني. (2018). *الضوابط الأساسية للأمن السيبراني*. https://nca.gov.sa/ecc-ar.pdf

الهيئة الوطنية للأمن السيبراني. (٢٠٢٢). *ضوابط الأمن السيبراني للبيانات*. https://2u.pw/WjQzX5j

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2), 23.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*, 1-10.

Chizanga, M. K., Agola, J., & Rodrigues, A. (2022). Factors Affecting Cyber Security Awareness in Combating Cyber Crime in Kenyan Public Universities. *International Research Journal of Innovations in Engineering and Technology*, *6*(1), 54.

Haque, M. A., Ahmad, S., John, A., Mishra, K., Mishra, B. K., Kumar, K., & Nazeer, J. (2023). Cybersecurity in Universities: An Evaluation Model. *SN Computer Science*, *4*(5), 569.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176-8186.

Richardson, M., Lemoine, P., Stephens, W. and W. and Waller, R. (2020). Planning for cyber security in schools: The human factor, *Educational Planning*, 2(2), 23-39

Ulven, J. B., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet 2021, 13, 39.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.