وزارة التعليم العالي والبحث العلمي

جامعة زيان عاشور بالجلفة

كلية العلوم الإنسانية والاجتماعية

قسم علم الاجتماع والديموغرافيا

دور الثقافة التنظيمية في تعزيز الأمن السيبراني داخل المؤسسات الجامعية

دراسة ميدانية بكلية العلوم الإجتماعية والإنسانية

جامعة زيان عاشور ـ الجلفة ـ

مذكرة مقدمة لنيل شهادة ماستر في علم الاجتماع
تخصص علم الاجتماع التنظيم والعمل.

إعداد الطالبة:
بلخير فاطمة

إشراف:
الدكتور: جلود رشيد

أمام لجنة المناقشة المكونة من :

د. حدادو فاطمة الزهراء	جامعة الجلفة	رئيسا
د. جلود رشيد	جامعة الجلفة	مشرفا ومقررا
د. بختي زهية	جامعة الجلفة	عضوا مناقشا

السنة الجامعية: 2025/ 2026


بسم الله الرحمن الرحيم

إهداء

إلى من أحمل إسمه بكل فخر، وصاحب السيرة العطرة واليد البيضاء التي لم تبخل علي يوماً بالدعم والتوجيه، **والدي العزيز**.

إلى نبع الحنان والراحة، من سهرت الليالي ودعت لي في جوف الليل بالتوفيق والنجاح، **أمي الغالية**.

إلى سند الحياة أمي الثانية أختي الكبرى **نورة**.

إلى شركاء العمر، الذين قاسموني اللحظات بحلوها ومرها، وكانوا لي دائماً مصدر قوة، إخوتي وأخواتي (**محمد، أحمد، حنان نسرين، سعيدة، زهرة، ايمان، نوال، ولميس**).

إلى من جمعتني بهم الأيام، فكانوا نعم العون في دروب العلم، وتشاركنا معاً لحظات الجد والمثابرة والذكريات الجميلة، صديقاتي (**لامية، إسراء، أسماء، بشرى**).

إلى كل من قدم لي يد العون.

إليكم جميعاً، أهدي هذا العمل المتواضع، ثمرة جهدي ونجاحي.

بالخير فاطمة

بسم الله الرحمن الرحيم

شكر وعرفان

الحمْدُ لِلّهِ العَلِيِّ القَديرِ الَّذي وفَّقَنا وأَنارَ لَنا دَرْبَ العِلْمِ، وأَعانَنا عَلَى إتْمَامِ هذَا العَمَلِ؛ تَطبيقاً لِقَوْلِهِ صلَّى اللهُ عَلَيْهِ وسَلَّمَ: "مَنْ لا يَشْكُرِ لا يَشْكُبِ النَّاسَ لا يَشْكُرِ اللهَ"، "مَنْ لا يَشْمُرِ النَّاسَ بالَّذِي هُشَكُرِ اللهَ"، نَتَقَدَّمُ بِجَزيلِ الشُّكْرِ وعظيمِ الامتِنانِ إلى الدُّكْتورِ المشْرِفِ الفَاضِلِ جُلُود رَشيد الَّذي لَمْ يَبْخَلْ عَلَيْنا بِتَوْجيهاتِه القَيِّمَةِ ونَصائِحِهِ السَّديدةِ طيلَةَ فَتْرةِ إنْجازِ المذَكَّرَةِ، وكَانَ لَنا سَنداً عِلْمِيَّاً مُتَمَيِّزاً.

كَما نَتَقَدَّمُ بِخالِص الشُّكْرِ والتَّقْديرِ إلى الأَساتِذَةِ الأَجلاءِ أَعْضاءِ لجْنَةِ المُناقَشَةِ المَوْقُورةِ لِتَفَضُّلِهِمْ بِقَبولِ تَقْييمِ هذا العَمَلِ وتَصويبِ مَسارِه.

ولا يَفُوتُنا أنْ نَتَوَجَّهَ بِبالِغِ الشُّكْرِ والامْتِنانِ إلى كَافَّةِ أَساتِذةِ قِسْم عِلْم الاجْتِماعِ بِجامِعَةِ الجِلْفَةِ، الَّذينَ غَمرونا بِعِلْمِهِمُ المعْرِفِيِّ طيلَةَ مِشْوارنا الدّراسِيِّ.

كَما نتَقَدَّمُ بِجَزِيلِ الشُّكْرِ إلى المسْؤولِينَ والمَوَظَّفينَ في كُلِّيَّةِ العُلُومِ الاجْتماعيَّةِ والإنْسانيَّةِ بِجامِعَةِ زِيان عاشـور على تَسْـهيلِهِمْ لِمهامّنا وتَهامّنا وتقديم التَّسْهيلاتِ اللازمةِ لإتْمامِ الدّراسةِ الميدانيَّةِ.

إلى كُلِّ هؤُلاءِ، وإلى كُلِّ مَنْ ساعَدَنا مِنْ قَريبٍ أو مِنْ بَعيدٍ، نَرْجُو مِنَ اللهِ العَلِيِّ القَديرِ أَنْ يَجْزِيهُمْ عَنَّا خَيْرَ الجَزاءِ.

ملخص الدراسة

تناولت هذه الدراسة موضوع "دور الثقافة التنظيمية في تعزيز الأمن السيبراني داخل المؤسسات الجامعية"، بالتطبيق على كلية العلوم الإنسانية والاجتماعية بجامعة زيان عاشور بالجلفة. هدفت الدراسة إلى الكشف عن مدى مساهمة القيم والمعايير التنظيمية السائدة في تدعيم جدار الحماية الرقمي للمؤسسة، خاصة في ظل التصاعد المستمر للتهديدات السيبرانية التي تستهدف القطاع الأكاديمي.

انطلقت الدراسة من إشكالية رئيسية مفادها: "إلى أي مدى تساهم الثقافة التنظيمية في تعزيز الأمن السيبراني داخل كلية العلوم الإنسانية والاجتماعية في ظل تزايد التهديدات الرقمية؟". وللإجابة عليها، تم الاعتماد على المنهج الوصفي ، واستخدام الاستبيان كأداة رئيسية لجمع البيانات من عينة الدراسة.

وقد تمحورت الدراسة حول فرضية:

- وجود علاقة ذات دلالة إحصائية بين نمط الثقافة التنظيمية السائد ومستوى تعزيز الأمن السيبراني.

الكلمات المفتاحية:

الثقافة التنظيمية، الأمن السيبراني، المؤسسات الجامعية، التهديدات الرقمية، الوعي الأمني.

.

Abstract

This study explores "The Role of Organizational Culture in Enhancing Cybersecurity within Higher Education Institutions," specifically focusing on the Faculty of **Humanities and Social Sciences at Ziane Achour University**, Djelfa. The study aims to uncover how prevailing organizational values and standards contribute to strengthening the institution's digital defense mechanisms, especially in light of the continuous escalation of cyber threats targeting the academic sector.

The research addresses a central problem: "To what extent does organizational culture contribute to enhancing cybersecurity within the Faculty of Humanities and Social Sciences amidst increasing digital threats?" To answer this, a descriptive approach was adopted, utilizing a questionnaire as the primary tool for data collection from the study sample.

The study was centered around the study hypothesis:

- There is a statistically significant relationship between the prevailing organizational culture pattern and the level of cybersecurity promotion.

Keywords:

Organizational Culture, Cybersecurity, University Institutions, Digital Threats, Security Awareness

فهرس المحتويات

فهرس الجداول

فهرس الأشكال

مقدمة:

يشهد العالم المعاصر تطورا متسارعًا في مختلف المجالات، ولا سيما في المجال التكنولوجي، حيث أصبحت التكنولوجيا الحديثة جزءًا أساسيًا في شتى القطاعات. فلم تعد المنظمات، سواء في مجالات التسيير أو الإنتاج أو تقديم الخدمات، تستغني عن الحلول التكنولوجية التي أسهمت بشكل كبير في تحسين جودة الخدمات المقدمة، من قبل المنظمات العامة أو الخاصة .وقد بات اعتماد التكنولوجيا من قبل المنظمات، لا سيما العمومية منها، تحديًا جوهريًا تسعى كل دولة إلى تحقيقه، كما أصبح تصنيف المنظمات من حيث جودة خدماتها قائمًا بشكل أساسي على سرعة الخدمة ودقتها، وهما عاملان يمكن تحقيقهما بكفاءة من خلال توظيف الرقمنة بشكل فعّال داخل المؤسسة .

أصبحت المنظمات تعتمد أكثر فاكثر على نظم المعلومات، فلا عجب أن يكون لأمن المعلومات أهمية واهتمام كبير من المنظمات والباحثين على حد سواء، اذ يمكن أن تؤدي خروقات المعلومات الحساسة للمنظمات لخسائر اقتصادية وكذلك أثار سلبية على سمعة المنظمة وثقة عملائها، فقد أجريت بحوث واسعة في تطوير أدوات تكنولوجية من الدرجة الأولى لضمان حماية أصول المعلومات بالمنظمة ومع ذلك فان تطور تقنيات الحماية قد لا يكون كافيا في الكثير من الأحيان، هنالك عدة أبحاث في أمن المعلومات ركزت تحديدا على فهم وتحسين استخدام الإجراءات والأنشطة الإدارية لحماية أصول المعلومات، ومع ذلك تواجه عدة منظمات اليوم معركة شرسة في محاولة تجديد الإجراءات والأنشطة الإدارية لكل خطر أمني محتمل، و هذا ما دفع الباحثين الى النظر في سلوك الموظفين المتعلق بأمن المعلومات والذي أطلق عليه اسم ثقافة امن المعلومات.

تمت دراسة ثقافة امن المعلومات منذ بداية القرن الواحد والعشرين هذا المصطلح لديه عدة تعريفات ومن جوانب مختلفة وتوجهات متنوعة ويجمع الباحثون على أن ثقافة امن المعلومات هي نمط مشترك من القيم والنماذج العقلية والأنشطة التي يتم تداولها ومشاركتها بين موظفي المنظمة مع مرور الوقت والتي تؤثر على أمن المعلومات، على الرغم من أهمية هذا الموضوع الا أنه موضوع لم يصل الى مرحلة النضج وذلك بسبب تشعبه لانتمائه للمواضيع الاجتماعية التكنولوجية إضافة الى أنه مصطلح مركب من مصطلحات كبيرة كالثقافة وأمن المعلومات اللذان يحملان في طياتهما الكثير من التشعبات والعلاقات المتداخلة مما شكل صعوبة للباحثين في معالجته.

الفصل الأول

الإطار المنهجي والنظري

- ❖ تمهيد
- ❖ الإشكالية
- ❖ الأسئلة الفرعية
- ❖ الفرضيات
- ❖ أسباب اختيار الموضوع
- ❖ تحديد مفاهيم الدراسة
- ❖ أهمية الدراسة
- ❖ أهداف الدراسة
- ❖ الدراسات السابقة
- ❖ التعقيب على الدراسات السابقة
- ❖ المقاربة النظرية
- ❖ إسقاط النظرية

تمهيد :

يعدُّ البحث العلمي عملية منظمة تبدأ برؤية واضحة للمشكلة وتنتهي بتقديم حلول أو فهم أعمق للظواهر المدروسة. وفي ظل الطفرة الرقمية التي مست مؤسسات التعليم العالي، برزت الحاجة الماسة لفهم التفاعل بين البعد التكنولوجي والبعد السوسيولوجي داخل الجامعات؛ إذ لم يعد التحدي يكمن في توفير الوسائل التقنية فحسب، بل في كيفية بناء وعي مؤسساتي يحمي هذه المكتسبات.

يأتي هذا الفصل ليمثل حجر الزاوية في دراستنا، حيث نسعى من خلاله إلى رسم المعالم المنهجية التي سنسير وفقها لاستقصاء العلاقة بين الثقافة التنظيمية كمتغير سيكولوجي واجتماعي، وبين الأمن السيبراني كمتغير تقني ووقائي داخل كلية العلوم الإنسانية والاجتماعية.

سنتناول في هذا الفصل العناصر الأساسية التالية:

الإطار التساؤلي من خلال صياغة إشكالية الدراسة التي تعكس الفجوة بين الواقع الرقمي والممارسة السلوكية، وتحديد الفرضيات التي تمثل إجابات مؤقتة ننتظر اختبارها ميدانياً. وأسباب اختيارنا للموضوع الذاتية والموضوعية، وسنتطرق لتحديد المفاهيم وذلك من اجل ضبط المصطلحات إجرائياً ومنع اللبس في التفسير مع رصدنا لأهمية وأهداف الدراسة لتوضيح الدوافع العلمية والعملية من وراء بحثنا هذا.

وفي نهاية الفصل سنستعرض التراكم المعرفي من خلال عرض الدراسات السابقة التي تقاطع معها بحثنا، وتحديد المقاربة النظرية التي ستشكل المنظار التحليلي المناسب والذي نطل من خلاله على الظاهرة المدروسة.

إن هذا الفصل هو الضابط المنهجي الذي يضمن وحدة الموضوع واتساقه، ويمهد الطريق للفصول اللاحقة، وهذا لضمان الوصول إلى نتائج علمية دقيقة تتسم بالموضوعية والمصداقية.

01. الإشكالية:

يشهد العالم المعاصر تحولاً جذرياً نحو الرقمنة الشاملة، حيث لم تعد التكنولوجيا مجرد أداة مساعدة، بل أصبحت العصب الحيوي الذي تقوم عليه كافة الوظائف المؤسساتية. وفي هذا السياق، انخرطت المؤسسات الجامعية باعتبارها قاطرة التجديد في هذا المسار، حيث اعتمدت كليات العلوم الإنسانية والاجتماعية بشكل كلي على النظم المعلوماتية في تسيير شؤونها البيداغوجية، وإدارة قواعد بيانات الطلبة، وتخزين النتاج البحثي للأكاديميين.

ومع هذا الانفتاح الرقمي الواسع، برزت تحديات أمنية بالغة التعقيد، كشفت عن قصور الرؤية التقنية الضيقة؛ إذ أثبتت الوقائع أن أقوى برمجيات التشفير وجدران الحماية تظل قاصرة ما لم يسندها وعي بشري يقظ. فالمؤسسة الجامعية، من منظور سوسيولوجي، ليست مجرد تراكم للأجهزة والوسائط التقنية، بل هي كيان اجتماعي وديناميكي تحكمه ثقافة تنظيمية عميقة الجذور، تتشكل من مزيج من القيم، والمعتقدات، والتمثلات التي توجّه سلوك الفاعلين (إداريين) تجاه التعامل مع المعلومة الرقمية.

إن معضلة الأمن السيبراني في بيئة أكاديمية ككلية العلوم الإنسانية والاجتماعية تكمن في كونها بيئة مفتوحة بطبعها، مما يضاعف من حجم التهديدات الرقمية التي تستغل الفجوة السلوكية للأفراد. ومن هنا، يبرز الدور المحوري للثقافة التنظيمية كمتغير حاسم؛ فهي التي تحدد مدى استجابة الأفراد لسياسات الحماية، ومدى تحول الأمن من مجرد تعليمات فوقية إلى ممارسة تلقائية وجزء من الهوية المهنية.

بناءً على هذا التصور الذي يضع العنصر البشري في قلب الاستراتيجية الدفاعية للمؤسسة، تتبلور ضرورة البحث في طبيعة العلاقة الارتباطية بين المناخ الثقافي السائد وبين فاعلية المنظومة الأمنية. ومن هذا المنطلق، تتحدد معالم دراستنا في محاولة الإجابة على التساؤل الجوهري التالي:

إلى أي مدى تساهم الثقافة التنظيمية في تعزيز الأمن السيبراني داخل كلية العلوم الإنسانية والاجتماعية في ظل تزايد التهديدات الرقمية؟

الاسئلة الفرعية

وللتفصيل في الإشكالية، يمكننا طرح الأسئلة التالية:

1/ما مستوى الثقافة التنظيمية السائدة داخل كلية العلوم الانسانية والاجتماعية؟

2/ما اثر التدريب والتوعية في مجال الأمن السيبراني على سلوك العاملين داخل الكلية؟

وعلى ضوء هذه التساؤلات تمت صياغة الفرضية العامة والفرضيات الجزئية بما يتناسب مع تساؤلات الإشكالية .

02. الفرضية العامة:

توجد علاقة ذات دلالة إحصائية بين نمط الثقافة التنظيمية السائد ومستوى تعزيز الأمن السيبراني في الكلية.

فرضيات فرعية

1/يؤثر مستوى ثقافة التنظيمية السائدة داخل الكلية في درجة الالتزام بممارسات الأمن السيبراني.

2/ يساهم التدريب والتوعية في مجال الأمن السيبراني في الحد من المخاطر الرقمية داخل الكلية.

03. أسباب اختيار الموضوع:

الأسباب الموضوعية:

- تزايد الهجمات السيبرانية التي تستهدف المؤسسات التعليمية والبحثية لسرقة البيانات أو الابتزاز.

- الإدراك المتزايد بأن الحلول التقنية (برامج الحماية) لا تكفي وحدها دون وجود وعي بشري داعم.

- ندرة الدراسات العربية التي تربط بين العلوم الإدارية (الثقافة التنظيمية) والعلوم التقنية (الأمن السيبراني).

الأسباب الذاتية:

- الرغبة في تسليط الضوء على دور العنصر البشري في منظومة الأمن الرقمي.

- الميل الشخصي للبحث في القضايا المعاصرة المرتبطة بالتحول الرقمي في الجامعة.

- الدافع المعرفي وحب الاطلاع خاصة وأن موضوعنا يتميز بالحداثة

04. تحديد المفاهيم:

1.4 المؤسسة الجامعية: هي البيئة التنظيمية (محل الدراسة) التي تضم تدفقات معلوماتية ضخمة (بحوث، بيانات شخصية، نتائج) وتتطلب حماية خاصة نظراً لانفتاحها الرقمي

الثقافة التنظيمية هي مجموعة القيم والمعتقدات والتقاليد التي تربط العاملين في المنظمة، حيث توجه سلوكهم وتتحكم في علاقاتهم وتفاعلاتهم مع بعضهم البعض وبالتالي يساعد هذا في تحقيق الكفاءة والفعالية داخل المنظمة [1]

2.4 الثقافة التنظيمية:

الثقافة:

لغة : كلمة ثقافة هي كلمة عربية الأصل ، وهي مشتقة من مصدر الفعل " ثقف " بمعنى فهم، وتشير كلمة ثقافة إلى عدد من المعاني منها : الحذق والفهم والفطنة والتهذيب .

أما في القران الكريم فتم استخدام الفعل ثقف بمعنى ظفر بالشيء وأخذه من باب الغلبة ، كما استعمل أيضا في الإدراك مصداقا لقوله تعالى: " **واقتلوهم حيث ثقفتموهم** "[2] أي : حيث تجدونهم وتدركونهم في حل أو حرم .

اصطلاحا:

تعريف تايلور: " الثقافة هي ذلك الكل المركب الذي يشمل على المعرفة و المعتقدات و الفن و الأخلاق و القانون و العادات أو أي قدرات أخرى وعادات يكتسبها الإنسان بصفته عضوا في

المجتمع " .

[1] محاضرات حول التطور التاريخي للثقافة التنظيمية ،جامعة أكلي محند أولحاج، البويرة ,27فيفري 2022
[2] سورة البقرة ، آية 191

يعرفها القريوتي : " بأنها الافتراضات و القيم الأساسية التي تطورها جماعة معينة ، من

اجل التكيف والتعامل مع المؤثرات الخارجية والداخلية ، و التي يتم الاتفاق عليها و على ضرورة تعليمها للعاملين الجدد ، ومن اجل إدراك الأشياء و التفكير بها بطريقة معينة تخدم الأهداف الرسمية .[1]

التعريف الإجرائي : هي منظومة القيم، المعتقدات، والتقاليد التي يشترك فيها أعضاء الجامعة، والتي تحدد كيفية تعاملهم مع الأصول المعلوماتية والالتزام بالضوابط الأمنية.

تعريف الأمن السيبراني: كلمة تتكون من شقين الأمن – السيبراني ومعناها:

3.4 الأمن:

لغة : هو نقيض الخوف أي بمعنى السلامة وسكون القلب وزوال الخوف ويقال: أمن الشر أي سلم منه

اصطلاحاً : هو عدم توقع مكروه في الزمن الآتي

وهو القدرة التي تتمكن بها الدولة من إطلاق مصادر قوتها الداخلية والخارجية والاقتصادية والعسكرية في شتى المناحي لمواجهة مصادر الخطر في الداخل والخارج في حالتي السلم والحرب، مع إستمرار الإنطلاق المؤمن لتلك القوى في الحاضر والمستقبل[2]

السيبراني:

هي ترجمة للفظة الاجنبية (cyber) ومعناها الافتراضي او المتخيل ، وقد اشتقت منها الفاظ شتى لها دلالات متنوعة من حيث فعالية المدلول و تأثيره في الفضاء السيبراني وهو ذلك الحيز الذي تتم فيه ومن خلاله مجمل الانشطة السيبرانية. [3]

الأمن السيبراني إصطلاحا :

هو أمن الشبكات والأنظمة المعلوماتية والبيانات والمعلومات والأجهزة المتصلة بالإنترنت، وهو المجال الذي يتعلق بإجراءات ومقاييس ومعايير الحماية المفروض

---

[1] القريوتي محمد قاسم, **السلوك التنظيمي دراسة السلوك الإنساني الفردي والجماعي** . ط 5,دار وائل , الاردن, 2009 ص 17

[2] عبد الرحمن بجاد، **دور الأمن السيبراني في تعزيز الأمن الانساني**، رسالة ماجستير في العلوم الإستراتيجية، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية قسم الامن الانساني، السعودية ، عام 2017 ، ص6

[3] محمود بري. **السيبرانية علم القدرة على التواصل والتحكم والسيطرة**. المركز الإسلامي للدراسات الاستراتيجية.ط1. بيروت. لبنان. 2019. ص10

اتخاذها، أو الالتزام بها لمواجهة التهديدات، ومنع التعديات، او للحد من اثارها في أقسى واسوأ الأحوال.[1]

من خلال التعريفات السابقة يمكن تعريف الأمن السيبراني بأنه : كل الاجراءات التي تتخذ لحماية الاتصالات والشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من برمجيات وأجهزة، وما تقدمه من خدمات، وما تحتويه من بيانات، سواء كانت حماية سابقة وقائية بواسطة وضع أنظمة حماية من المخاطر المحتملة أو حماية لاحقة من أي هجوم سيبراني أو اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع ويشمل أيضاً المحافظة على البنى التحتية الحساسة للدولة من هجمات الروبوتات وغيرها وسواء ارتكبت الجريمة السيبرانية عن طريق الجهات الحكومية أو غير الحكومية، وينظم الإجراءات الخاصة بالأمن السيبراني وفقاً للقوانين واللوائح الوطنية للدولة ، يمكن ان نستنتج ان الأمن السيبراني مصطلح يستخدم لوصف قدرات البلد او منظمة او شركة في الحماية من الهجمات الفيروسية.

التعريف الإجرائي:

هو ممارسة حماية الأنظمة والشبكات والبيانات الرقمية في الجامعة من الاختراق أو التلف، وضمان استمرارية الخدمات الأكاديمية والإدارية.

4.4 المخاطر الرقمية (Digital Risks)

التعريف الاصطلاحي:

هي احتمالية حدوث أضرار مادية أو معنوية (فقدان بيانات، اختراق خصوصية، تعطيل الأنظمة) نتيجة ثغرات في الأنظمة التقنية أو السلوكيات البشرية أثناء التعامل مع الوسائط الرقمية داخل المؤسسة الجامعية.

التعريف الإجرائي:

هي مجموعة التهديدات التي تواجه الأصول المعلوماتية لكلية العلوم الاجتماعية والإنسانية (مثل بيانات الطلبة، نتائج الامتحانات، البحوث الأكاديمية)، والتي تنجم عن ضعف الوعي الأمني لدى الموظفين أو غياب السياسات الرادعة.

5.4 التدريب(Training)

التعريف الاصطلاحي:

[1] عبدالله يحيي سعيد الزهراني ، **استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة** ، دراسة مقارنة ، رسالة قدمت لنيل درجة الماجستير في العلوم الإستراتيجية ، جامعة نايف العربية ، للعلوم الأمنية ، كلية العلوم الإستراتيجية قسم الدراسات الاستراتيجية ، السعودية ، عام 2020 ، ص 11

هو جهد تنظيمي مخطط يهدف إلى تعديل أو تطوير معارف ومهارات الموظفين، وتغيير اتجاهاتهم نحو تبني سلوكيات أمنية سليمة، بما يضمن تقليل الفجوة بين الأداء الحالي والأداء المنشود في مواجهة الهجمات السيبرانية.

التعريف الإجرائي:

هو البرامج والورشات التوعوية والتقنية التي تنظمها الجامعة الجلفة لفائدة موظفي وأساتذة كلية العلوم الاجتماعية والإنسانية، لتعريفهم بكيفية حماية حساباتهم، اكتشاف رسائل التصيد الاحتيالي، والتعامل الآمن مع قواعد البيانات الرقمية.

05. أهمية الدراسة:

تكمن أهمية هذه الدراسة في إمكانية الاستفادة من الإدارة الإلكترونية من ناحية الخدمة العمومية ، من طرف الموظفين لصالح تطوير العمل الإداري في المؤسسات العمومية ،و كذلك تكمن أهميتها في تسهيل العمل الإداري و تطوير المؤسسة من الناحية الإلكترونية ،عن طريق التخلي عن طرق العمل التقليدية و إستبدالها بطرق حديثة.

06.أهداف الدراسة:

- تحديد مستوى الوعي بالأمن السيبراني لدى الموظفين والطلبة داخل الجامعة.
- إبراز الدور الذي تلعبه القيم والمعايير التنظيمية في توجيه السلوك الأمني للأفراد.
- الكشف عن المعوقات الثقافية التي تحول دون تطبيق استراتيجية أمن سيبراني فعالة.
- تقديم نموذج مقترح لصناع القرار في الجامعة لبناء "ثقافة أمنية" مستدامة.

07. الدراسات السابقة

الدراسة المحلية:

لشيماء مرزوق وزين تركية إجلال إنعاكسات الأمن السيبراني على أمن المعلومات في البنوك، وهي عبارة عن مذكرة ماستر في العلوم الاقتصادية، تخصص اقتصاد نقدي

وبنكي (جامعة الشهيد الشيخ العربي التبسي، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم العلوم الاقتصادية ، 2023/2024، حيث هدفت هذه الدراسة إلى تبيان تأثير الأمن السيبراني على أمن المعلومات في البنوك، حيث تم إختيار المجتمع المجمع الجهوي لبنك بدر – تبسة ، وقد خلصت الدراسة أن الأمن السيبراني يساهم في حماية المعلومات البنكية من الهجمات السيبرانية، كما توصلت الباحثتين في ذات السياق إلى أن الأمن السيبراني يعد ضروري لنجاح النظام المصرفي الإلكتروني، إلا أن الباحثتين أغفلتا الحديث عن تقنيات الأمن السيبراني في تأمين معلومات العملاء المتواجدة على مستوى بنك بدر بتبسة.

الدراسة العربية:

القحطاني عادل محمد 2014. " تصور استراتيجي لتطوير أمن المعلومات تعزيزا للأمن الوطني في المملكة العربية السعودية، بالتطبيق على شركة سابك"، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية الرياض

هدفت الدراسة إلى تطوير أنظمة أمن المعلومات، والتعرف على ماهية أمن المعلومات، وأهمية تأمينه، وتحليل الأخطار التي تتعرض لها أنظمة المعلومات، ومعرفة مدى تأثير اختراق أنظمة المعلومات وصولا إلى تقديم رؤية استراتيجية، ومعرفة مدى اختراق أنظمة المعلومات وصولا إلى تقديم رؤية استراتيجية لتوفير وتطوير الأمن المعلوماتي بشركة سابك، وتكون مجتمع الدراسة وعينتها من شركة سابك في مدينة الرياض، واستخدمت الدراسة المنهج الوصفي التحليلي، مع الاستعانة بأداة الاستبانة لجمع المعلومات، بالإضافة إلى الأسلوب الاحصائي لتحليل البيانات التي تم الحصول جمعها.

وكان من أهم نتائجها: أن هناك أخطار يمكن أن تتعرض لها أنظمة المعلومات في شركة سابك، مثل: عملية اختراق لتعديل البيانات، أو إتلافها، أو تحميل برامج غير مصرح بها، مما يترتب على اختراق أنظمة المعلومات تأثير سلبي على الأداء الاقتصادي من خلال سرقة الأسرار، أو المعلومات التجارية، أو التسويقية، أو معرفة حسابات الشركة.

وكان من أهم توصيات الباحث: ضرورة دعم الإدارة لأنشطة الرقابة الداخلية على أمن المعلومات من خلال توفير الكوادر المؤهلة في قسم التحقيق الداخلي، بالإضافة لتوفير التدريب اللازم للموظفين، للتعرف على التحديات الجديدة التي تواجه أمن المعلومات، وأساليب مكافحتها، وضرورة توفير التدريب، والتوعية للموظفين مع التركيز على الموظفين الأقل خبرة.

الدراسة العالمية:

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

بحثت هذه الدراسة في أهمية النتائج التي توصلت اليها في مساعدة مدراء أمن المعلومات في وضع استراتيجيات أفضل لتنفيذ برامج توعية وتثقيف المستخدمين، وتحقيق التوازن بين النهج التقني وغير التقني والتركيز بشكل أكبر على سلوك المستخدم. ومساعدة المسؤولين التنفيذيين في المنظمة الذين يعتمدون بشكل أساسي على الأدوات والمنتجات التجارية مثل الجدران النارية والحماية من الفيروسات القائمة على الخادم للتفكير في الاستراتيجيات التي من شأنها مساعدتهم على استكشاف تأثيرات العوامل البشرية على منظماتهم، نظرًا لأن المستخدم النهائي يجب أن يشارك في أنظمة المعلومات الأمنية، وهذه الدراسة تساعده في تحقيق مساهمته في الحفاظ على أمن المعلومات للمنظم بشكل سليم، وتم جمع البيانات من خلال إجراء مسح ومقابلات مع مسؤولي النظام، وبيانات المستخدمين النهائيين باستخدام الاستبيان .

ومن أهم النتائج التي توصلت اليها الدراسة، الحاجة إلى تقييم الوعي بأمن المعلومات مع التركيز على وعي المستخدم من خلال النهوض بالتكنولوجيا والعمليات اليومية للجامعة، وأيضا من فهم المشاكل التي تعترض غير التقنيين في المجال الأمني للمعلومات، وعدم اهمال المستخدمين النهائيين لتكنلوجيا المعلومات والتركيز بشكل أكبر على سلوك المستخدم.

ومن أهم التوصيات التي خرجت بها الدراسة، التحقق من كيفية تعزيز المستخدمين والإداريين من الوحدات الأخرى، بخلاف الوحدات الأكاديمية، للتوعية الأمنية والتوافق مع السياسة الأمنية، خاصةً أنهم يتعاملون مع البيانات الحساسة مثل تلك التي يتم تغطيتها بموجب قانون الخصوصية والحقوق التعليمية، وأيضا توصي الدراسة بإجراء دراسات في جامعات أخرى من نفس الفئة لمقارنتها بنتائج هذه الدراسة.

التعقيب على الدراسات السابقة:

من خلال القراءة التحليلية المتقاطعة للدراسات (المحلية، العربية، والعالمية)، نخلص إلى أن إشكالية الأمن السيبراني لم تعد مجرد حزمة من الإجراءات التقنية، بل أضحت ظاهرة سوسيوتقنية متكاملة الأركان. ويمكننا رصد التدرج في الرؤية السوسيولوجية لهذه الدراسات وفق مايلي:

أولاً: الانتقال من "الوظيفية التقنية" إلى "الفعل الاجتماعي"

نلاحظ أن الدراسة المحلية انطلقت من منظور وظيفي كلاسيكي، حيث يُنظر للأمن السيبراني كأداة لحماية البناء الاقتصادي للمؤسسة (بنك بدر). السوسيولوجيا هنا ترى أن الأمن هو "وظيفة" تضمن استقرار النسق المصرفي. لكن بالانتقال إلى الدراسة العالمية (Victoria Mahabi)، نجد تحولاً نحو سوسيولوجيا الفعل؛ فالتركيز لم يعد على الأداة التقنية بل على الفاعل الاجتماعي (المستخدم النهائي)، مما يعني أن نجاح المنظومة الأمنية مرهون بمدى استيعاب الأفراد لأدوارهم داخل النسق، وليس بقوة البرمجيات فحسب

ثانياً: الأمن السيبراني كأداة للضبط والرقابة التنظيمية

تجلت في الدراسة العربية (القحطاني) ملامح سوسيولوجيا المنظمات من خلال التركيز على "الاستراتيجية" و"الرقابة". التعقيب السوسيولوجي هنا يشير إلى أن الأمن المعلوماتي يُستخدم كآلية لتعزيز الضبط الاجتماعي داخل المؤسسة. فالتوصية بتدريب الموظفين ودعم الرقابة الداخلية تعكس رغبة المؤسسة في قولبة سلوك الأفراد بما يتماشى مع أهدافها الأمنية، وهو ما يسمى في الأدبيات السوسيولوجية بعقلنة السلوك التنظيمي لمواجهة التهديدات الخارجية.

ثالثاً: سوسيولوجيا الوعي والتمثلات (العامل البشري)

أحدثت الدراسة العالمية خرقاً سوسيولوجياً مهماً بتسليط الضوء على التوازن بين النهج التقني وغير التقني. من منظور سوسيولوجي، هذا يعني الاعتراف بأن الثقافة الأمنية هي بناء اجتماعي يتشكل من خلال التفاعل اليومي. الفجوة التي أشارت إليها الدراسة بين مسؤولي النظام والمستخدمين العاديين تعبر عن تفاوت في الرأسمال المعرفي الرقمي، مما يخلق تراتبية داخل المؤسسة قد تؤدي إلى ثغرات أمنية ناتجة عن خلل في المعنى المشترك للأمن بين المهنيين والجمهور.

08. المقاربة النظرية:

09. أثر تكنولوجيا المعلومات والاتصالات عند أولريش بيك من منظور "مجتمع المخاطرة":

يتمحور اهتمام عالم الاجتماع والمنظر السوسيولوجي أولريش بيك صاحب مفهوم "مجتمع المخاطرة" كنتيجة حتمية لما يشهده عصر ما بعد الحدثة وما أفرزته العولمة من تحولات سريعة على عديد المجالات الاقتصادية والاجتماعية والسياسية والثقافية والبيئية

وعلى مستوى الأخلاق والقيم والهوية والمعارف هذا التغير و التحول الذي غير مفهوم الزمان والمكان، بحيث زادت معه مخاطره ولا يمكن التحكم فيها ولا حصرها أو التنبؤ بها في مكان أو زمان نتيجة للديناميكية السريعة التي يتميز بها هذا العصر؛ فبعدما كانت المخاطر أمرًا داخليا وإقليميا أو شَيْئًا خاص بمجتمع معين؛ تحول الأمر إلى أن تصبح هاته المخاطر أكثر خطورة وشمولية مما كانت عليه من قبل، خصوصا بدخول تكنولوجيا المعلومات والاتصالات، مما يستعدي بدوره مفهوم مجتمع المخاطرة" ليبرز أكثر إلى الواجهة لأنه السمة البارزة لمجتمع هذا العصر والحياة الراهنة.

هكذا تتعرض الحياة البشرية للخطر في صميمها وجوهرها، وقد تسلب الإنسان قوته في الحكم ويتحول إلى عدم القدرة على المعرفة؛ وإلى حالة لا يمكن انتشاله من المعاناة التي أوجد نفسه فيها، لأنه لا أحد يعرف هذه الإصابات لأنها جزء من الجهل وبالتالي يتعين على الناس الذين سرقت حواسهم وحكمهم الخاص استخدام المعرفة والجهل اللذين جمعوهما عند موقف المعناة بالنسبة لهم كعملة وعن طريهما يستطيع الناس التفاوض على بقائهم.

10. إسقاط نظرية مجتمع المخاطرة على موضوع الدراسة:

يُعد إسقاط نظرية **"مجتمع المخاطرة"** لأولريش بيك على دراستنا حول "الأمن السيبراني والثقافة التنظيمية" إسقاطاً عميقاً، لأنه ينقل الموضوع من مجرد جانب تقني جاف إلى أبعاد سوسيولوجية (اجتماعية) تفسر سلوك الأفراد داخل المؤسسة الجامعية.

حيث تتقاطع طروحات السوسيولوجي أولريش بيك حول "مجتمع المخاطرة" بشكل جوهري مع إشكالية الأمن السيبراني داخل كلية العلوم الإنسانية والاجتماعية؛ فتبني الكلية لتكنولوجيا المعلومات والاتصالات نقلها من حيز المخاطر التقليدية المنظورة إلى بيئة "المخاطر المصنعة" التي لا تدركها الحواس البشرية مباشرة، وهي السمة التي ميزت عصر ما بعد الحداثة. ومن هذا المنطلق، يصبح الأمن السيبراني في هذه الدراسة ليس مجرد إجراء تقني، بل هو محاولة تنظيمية لإدارة "حالة عدم اليقين" والجهل التقني التي قد تسلب الفرد (الموظف) قدرته على الحكم الصحيح وتجعله ثغرة أمنية. وبناءً عليه، فإن الثقافة التنظيمية داخل الكلية تمثل النسق القيمي والمعرفي الذي يحول "المعرفة بالمخاطر الرقمية" إلى سلوك أمني وقائي، مما يسمح للمؤسسة بالتفاوض على بقائها واستمراريتها الرقمية. فبدلاً من أن تظل المخاطر السيبرانية تهديدات مجهولة لا يمكن التنبؤ بها، تعمل التوعية والتدريب (كعناصر ثقافية) على تزويد الفاعلين داخل الكلية بالقدرة على إدراك هذه المخاطر والحد من شموليتها، محولةً بذلك الثقافة التنظيمية من مجرد إطار إداري إلى "درع سوسيولوجي" يواجه تداعيات العولمة الرقمية وتحديات مجتمع المخاطرة.

خلاصة الفصل :

في ختام هذا الفصل، نكون قد أرسينا القواعد المنهجية والمفاهيمية التي تنضبط بها دراستنا؛ فمن خلال صياغة الإشكالية وتحديد الفرضيات، رسمنا معالم الطريق للتحقق من الدور الذي تلعبه الثقافة التنظيمية في تحصين الأمن السيبراني. كما ساهم تحديد المفاهيم وضبط المقاربة النظرية في وضع إطار تفسيري يربط بين السلوك البشري والبيئة الرقمية داخل كلية العلوم الإنسانية والاجتماعية.

إن استعراض الدراسات السابقة وأهداف الدراسة أكد لنا أن معالجة الثغرات الرقمية لا تتم عبر الحلول التقنية الجاهزة فحسب، بل عبر فهم عميق للمناخ التنظيمي السائد. وبناءً على هذا التصور المنهجي، سننتقل في الفصل القادم إلى دراسة الإطار المفاهيمي للثقافة التنظيمية والامن السيبراني، وهذا بتفكيك مكوناتهما وأبعادهما، وفهم كيف تشكل هذه الثقافة المحرك الأساسي لسلوك الأفراد وتوجهاتهم داخل المؤسسة الجامعية.

الفصل الثاني

الإطار المفاهيمي للثقافة التنظيمية والأمن السيبراني

خطة الفصل:

- المبحث الأول: الثقافة التنظيمية
- المطلب الأول: مفهوم الثقافة التنظيمية
- المطلب الثاني: أهمية الثقافة التنظيمية في المؤسسات
- المبحث الثاني: الأمن السيبراني
- المطلب الأول: مفهوم الأمن السيبراني
- المطلب الثاني: تهديدات الأمن السيبراني في المؤسسات

تمهيد:

يُمثل هذا الفصل المرتكز النظري للدراسة، حيث يسعى إلى تسليط الضوء على متغيرين حيويين في بيئة العمل المعاصرة: الثقافة التنظيمية كبيئة حاضنة للسلوك الإنساني، والأمن السيبراني كدرع واقٍ للأصول الرقمية للمؤسسة.

في ظل التحول الرقمي المتسارع، لم يعد نجاح المؤسسات مرهوناً فقط بامتلاك تكنولوجيا متطورة، بل بمدى امتلاكها لثقافة تنظيمية واعية تدعم التوجهات الاستراتيجية وتحمي مكتسباتها المعلوماتية. ومن هذا المنطلق، يتم تناول هذا الفصل من خلال مبحثين أساسيين؛ يركز المبحث الأول على تفكيك مفهوم الثقافة التنظيمية، استعراض خصائصها، وعناصرها، وبيان دورها الجوهري في توجيه سلوك الأفراد وتحسين الأداء المؤسسي. أما المبحث الثاني، فينتقل إلى الجانب التقني والتنظيمي للأمن السيبراني، مستعرضاً ماهيته، أهدافه، والخصائص التي تميزه، وصولاً إلى تحليل التهديدات والمخاطر السيبرانية التي تواجهها المؤسسات، مع التركيز على التحديات الخاصة بالبيئة الجامعية.

المبحث الأول: الثقافة التنظيمية

المطلب الأول: مفهوم الثقافة التنظيمية

تُعد الثقافة التنظيمية من المفاهيم الأساسية في علوم الإدارة والسلوك التنظيمي، حيث تمثل مجموعة القيم والمعتقدات والاتجاهات المشتركة التي يتبناها أفراد المنظمة وتؤثر في طريقة تفكيرهم وسلوكهم داخل بيئة العمل. وتُشكل الثقافة التنظيمية الإطار الذي يحدد كيفية تفاعل الأفراد مع بعضهم البعض ومع بيئة العمل، كما تؤثر بشكل مباشر في الأداء التنظيمي ومستوى الالتزام والانتماء لدى العاملين.

وقد حظي مفهوم الثقافة التنظيمية باهتمام كبير من قبل الباحثين في مجالات الإدارة وعلم الاجتماع التنظيمي، وذلك لما لها من دور مهم في توجيه سلوك الأفراد داخل المنظمة وتحقيق أهدافها الاستراتيجية. فالثقافة التنظيمية لا تقتصر على القوانين والأنظمة الرسمية فقط، بل تشمل أيضًا القيم غير المكتوبة والعادات والتقاليد التنظيمية التي تتطور مع مرور الوقت نتيجة التفاعل بين أفراد المنظمة.

وتظهر أهمية الثقافة التنظيمية في كونها تشكل هوية المنظمة وتميزها عن غيرها من المنظمات، كما تساعد على تعزيز روح العمل الجماعي والتعاون بين العاملين، إضافة إلى دورها في دعم التغيير التنظيمي وتبني الابتكار والتطور التكنولوجي، وهو ما أصبح ضروريًا في ظل التحولات الرقمية المتسارعة التي تشهدها المؤسسات الحديثة.

ومن هذا المنطلق، أصبح الاهتمام بالثقافة التنظيمية أمرًا ضروريًا خاصة في المؤسسات التي تسعى إلى تعزيز الأمن السيبراني، حيث تلعب القيم التنظيمية والسلوكيات المهنية دورًا مهمًا في نشر الوعي الأمني لدى العاملين وتشجيعهم على الالتزام بإجراءات الحماية الرقمية.

الفرع الأول: تعريف الثقافة التنظيمية

تعددت تعريفات الثقافة التنظيمية تبعًا لاختلاف وجهات نظر الباحثين والدارسين في مجال الإدارة والسلوك التنظيمي. ومن أبرز هذه التعريفات تعريف إدغار شاين الذي يرى أن الثقافة التنظيمية هي:

"مجموعة من الافتراضات الأساسية التي يكتسبها أفراد المنظمة أثناء تعلمهم كيفية التكيف مع البيئة الخارجية والتكامل الداخلي، والتي يتم تعليمها للأعضاء الجدد باعتبارها الطريقة الصحيحة للإدراك والتفكير والشعور تجاه مشكلات العمل". [1]

[1] إدغار شاين، **الثقافة التنظيمية والقيادة**، ترجمة عبد الكريم أحمد، دار المريخ للنشر، الرياض، 2012، ص 35.

كما عرّفها بعض الباحثين بأنها منظومة من القيم والمعتقدات والرموز التي يشترك فيها العاملون داخل المنظمة، والتي تؤثر في سلوكهم وتحدد نمط العلاقات بينهم داخل بيئة العمل. [1]

ويرى باحثون آخرون أن الثقافة التنظيمية تمثل شخصية المنظمة، إذ تعكس الطريقة التي تُدار بها الأعمال داخل المؤسسة، والأساليب المتبعة في اتخاذ القرارات والتعامل مع العاملين والعملاء. [2]

وبناءً على هذه التعريفات يمكن القول إن الثقافة التنظيمية هي الإطار القيمي والسلوكي الذي يوجه تصرفات العاملين داخل المنظمة ويحدد طبيعة العلاقات التنظيمية، كما أنها تلعب دورًا مهمًا في تحقيق التماسك التنظيمي وتعزيز الأداء المؤسسي.

الفرع الثاني: خصائص الثقافة التنظيمية

تتميز الثقافة التنظيمية بعدد من الخصائص التي تجعلها عنصرًا أساسيًا في تشكيل السلوك التنظيمي داخل المؤسسات، ومن أهم هذه الخصائص ما يلي:

1- أنها ظاهرة مكتسبة:

تُكتسب الثقافة التنظيمية من خلال التفاعل المستمر بين العاملين داخل المنظمة، حيث يتعلم الأفراد القيم والمعتقدات السائدة من خلال الخبرة والتجربة والعمل الجماعي.

2- أنها مشتركة بين أفراد المنظمة:

تشترك غالبية أفراد المنظمة في تبني القيم والمبادئ الأساسية التي تشكل الثقافة التنظيمية، مما يؤدي إلى خلق نوع من الانسجام والتوافق بينهم.

3- أنها تتسم بالاستمرارية:

تتميز الثقافة التنظيمية بالاستقرار النسبي، حيث تستمر لفترات طويلة داخل المنظمة وتنتقل من جيل إلى آخر من العاملين.

4- قابليتها للتطور والتغيير:

رغم استقرارها النسبي، إلا أن الثقافة التنظيمية يمكن أن تتغير مع مرور الوقت نتيجة التغيرات في البيئة الداخلية والخارجية للمنظمة، مثل التحول الرقمي أو التغيرات التكنولوجية.

---

[1] أحمد ماهر، **السلوك التنظيمي: مدخل بناء المهارات**، الدار الجامعية، الإسكندرية، ص 112.
[2] محمد حسن عبد الفتاح، **إدارة الموارد البشرية** ، دار المسيرة للنشر والتوزيع، عمان، 2015، ص 112.

5- تأثيرها في السلوك التنظيمي:

تلعب الثقافة التنظيمية دورًا مهمًا في توجيه سلوك العاملين داخل المنظمة، حيث تؤثر في طريقة اتخاذ القرارات والتعامل مع المشكلات المهنية.

وتساهم هذه الخصائص في جعل الثقافة التنظيمية عنصرًا حيويًا في نجاح المؤسسات، خاصة في المؤسسات الحديثة التي تعتمد بشكل كبير على التكنولوجيا والأنظمة الرقمية.

الفرع الثالث: عناصر الثقافة التنظيمية

تتكون الثقافة التنظيمية من مجموعة من العناصر الأساسية التي تشكل في مجموعها الإطار الثقافي للمنظمة، ومن أبرز هذه العناصر ما يلي:

1- القيم التنظيمية:

تمثل القيم التنظيمية المبادئ الأساسية التي تؤمن بها المنظمة وتوجه سلوك العاملين فيها، مثل قيم التعاون، والالتزام، والشفافية، والابتكار.

2- المعتقدات التنظيمية:

تشير المعتقدات التنظيمية إلى الأفكار التي يؤمن بها العاملون داخل المنظمة حول طبيعة العمل والعلاقات المهنية، والتي تؤثر في طريقة تعاملهم مع المهام والمسؤوليات.

3- الأعراف التنظيمية:

تشمل الأعراف التنظيمية القواعد غير الرسمية التي تحكم سلوك الأفراد داخل المنظمة، مثل أساليب التواصل بين العاملين وطريقة التعامل مع المشكلات المهنية.

4- الرموز والشعارات التنظيمية:

تتمثل في الشعارات والرموز واللغة الخاصة التي تستخدمها المنظمة للتعبير عن هويتها وثقافتها، مثل الشعار المؤسسي أو اللباس المهني أو الطقوس التنظيمية.

5- القصص التنظيمية:

وهي القصص والحكايات التي تُروى داخل المنظمة حول إنجازات العاملين أو تاريخ المؤسسة، والتي تسهم في نقل القيم التنظيمية وتعزيز الانتماء المؤسسي.

وتتكامل هذه العناصر فيما بينها لتشكل الثقافة التنظيمية التي تميز كل منظمة عن غيرها، كما تلعب دورًا مهمًا في تعزيز الانضباط التنظيمي وتحقيق الأهداف الاستراتيجية للمؤسسة

المطلب الثاني: أهمية الثقافة التنظيمية في المؤسسات

تُعد الثقافة التنظيمية من العوامل الجوهرية التي تؤثر في نجاح المؤسسات واستمراريتها، إذ تمثل الإطار الفكري والقيمي الذي يوجه سلوك العاملين داخل المنظمة ويحدد طبيعة العلاقات بينهم. كما تسهم الثقافة التنظيمية في خلق بيئة عمل إيجابية قائمة على التعاون والالتزام وتحقيق الأهداف المشتركة. وقد أثبتت العديد من الدراسات في مجال الإدارة والسلوك التنظيمي أن المؤسسات التي تتمتع بثقافة تنظيمية قوية تكون أكثر قدرة على تحقيق الكفاءة والفعالية في الأداء، مقارنة بالمؤسسات التي تفتقر إلى ثقافة واضحة ومشتركة بين أفرادها. [1]

وتبرز أهمية الثقافة التنظيمية في قدرتها على تعزيز الانتماء المؤسسي لدى العاملين، وتحفيزهم على العمل بروح الفريق، إضافة إلى دورها في توجيه السلوك التنظيمي بما يتماشى مع أهداف المؤسسة وقيمها. كما تساعد الثقافة التنظيمية في مواجهة التحديات والتغيرات التي تفرضها البيئة الخارجية، مثل التطور التكنولوجي والتحول الرقمي، مما يجعلها عنصرًا أساسيًا في تطوير المؤسسات الحديثة وتحسين أدائها.

وعليه، فإن فهم أهمية الثقافة التنظيمية يعد أمرًا ضروريًا بالنسبة للقيادات الإدارية، حيث يساعدهم ذلك على بناء بيئة تنظيمية إيجابية تدعم الابتكار والتطور وتحقق الأهداف الاستراتيجية للمؤسسة.

الفرع الأول: دور الثقافة التنظيمية في تحسين الأداء

تلعب الثقافة التنظيمية دورًا محوريًا في تحسين أداء المؤسسات، حيث تسهم في توجيه جهود العاملين نحو تحقيق الأهداف التنظيمية بكفاءة وفعالية. فعندما تكون القيم التنظيمية واضحة ومشتركة بين العاملين، يصبح من السهل تحقيق التنسيق والتعاون بينهم، مما يؤدي إلى رفع مستوى الإنتاجية وتحسين جودة العمل.

كما تسهم الثقافة التنظيمية في تعزيز روح المبادرة والابتكار لدى العاملين، حيث تشجعهم على تقديم أفكار جديدة والمشاركة في تطوير العمل. فالمؤسسات التي تعتمد على ثقافة تنظيمية إيجابية تشجع على التعلم المستمر وتبادل المعرفة بين الموظفين، مما يؤدي إلى تحسين الأداء الفردي والجماعي داخل المنظمة.

ومن جهة أخرى، تساعد الثقافة التنظيمية في تقليل الصراعات التنظيمية وتعزيز روح التعاون بين العاملين، إذ تعمل القيم المشتركة على توحيد الجهود وتوجيهها نحو تحقيق أهداف

[1] تشارلز هاندي، **فهم المنظمات**، ترجمة محمد عبد الفتاح، دار المريخ للنشر، الرياض، 2011، ص 67.

المؤسسة. كما تسهم في دعم عملية اتخاذ القرار داخل المنظمة من خلال توفير إطار قيمي يساعد القادة الإداريين على اتخاذ قرارات تتماشى مع مبادئ المنظمة وثقافتها.[1]

كما أن الثقافة التنظيمية القوية تسهم في تحقيق الاستقرار التنظيمي، حيث يشعر العاملون بالانتماء للمؤسسة والالتزام بقيمها وأهدافها، الأمر الذي يؤدي إلى زيادة الرضا الوظيفي وتقليل معدل دوران العمالة.

الفرع الثاني: تأثير الثقافة التنظيمية على سلوك العاملين

تؤثر الثقافة التنظيمية بشكل كبير في سلوك العاملين داخل المؤسسة، إذ تشكل القيم والمعتقدات التنظيمية مرجعًا أساسيًا يحدد طريقة تصرف الأفراد في بيئة العمل. فعندما يتبنى العاملون ثقافة تنظيمية قائمة على التعاون والاحترام المتبادل، فإن ذلك ينعكس إيجابيًا على العلاقات المهنية بينهم ويعزز روح العمل الجماعي.

كما تسهم الثقافة التنظيمية في تشكيل اتجاهات العاملين نحو العمل، حيث تؤثر في مستوى التزامهم وانضباطهم الوظيفي. فالثقافة التنظيمية التي تشجع على المسؤولية والشفافية والالتزام بالقواعد المهنية تؤدي إلى تحسين سلوك العاملين وتعزيز أخلاقيات العمل داخل المؤسسة. [2]

ومن ناحية أخرى، تؤثر الثقافة التنظيمية في أسلوب تواصل العاملين داخل المنظمة، حيث تحدد طبيعة العلاقات التنظيمية وأساليب التفاعل بين الأفراد والإدارة. فالثقافة التنظيمية المنفتحة التي تشجع على الحوار وتبادل الآراء تسهم في تعزيز الثقة بين العاملين والإدارة، مما يؤدي إلى تحسين مناخ العمل وزيادة الإنتاجية.

كما تلعب الثقافة التنظيمية دورًا مهمًا في تعزيز الشعور بالانتماء لدى العاملين، إذ يشعر الموظفون بأنهم جزء من منظومة متكاملة تسعى لتحقيق أهداف مشتركة، مما يدفعهم إلى بذل المزيد من الجهد في أداء مهامهم الوظيفية.

الفرع الثالث: أنواع الثقافة التنظيمية

تتنوع الثقافة التنظيمية داخل المؤسسات تبعًا لطبيعة العمل والقيم التي تتبناها الإدارة، وقد قدم الباحثون عدة تصنيفات لأنواع الثقافة التنظيمية، من أبرزها ما يلي:

---

[1] علي السلمي، **السلوك التنظيمي في المنظمات المعاصرة**، دار غريب للنشر، القاهرة، 2008، ص 132.
[2] عبد الغني عبد الرحمن، **السلوك التنظيمي في المنظمات الحديثة**، دار الجامعة الجديدة، الإسكندرية، 2014، ص 98.

1- ثقافة القوة (Power Culture):

تتمركز هذه الثقافة حول القيادة المركزية، حيث تتركز السلطة في يد قائد أو مجموعة صغيرة من القادة الذين يتخذون القرارات الرئيسية داخل المنظمة. ويكثر هذا النوع من الثقافة في المؤسسات الصغيرة أو في المؤسسات التي تعتمد على القيادة الفردية.

2- ثقافة الدور (Role Culture):

تقوم هذه الثقافة على وضوح الأدوار والمسؤوليات داخل المنظمة، حيث يتم تحديد مهام كل فرد بدقة وفقًا للهيكل التنظيمي. ويظهر هذا النوع من الثقافة غالبًا في المؤسسات الحكومية أو المنظمات البيروقراطية.

3- ثقافة المهمة (Task Culture):

تركز هذه الثقافة على إنجاز المهام وتحقيق الأهداف التنظيمية، حيث يتم تشكيل فرق عمل تتعاون فيما بينها لحل المشكلات وتحقيق النتائج المطلوبة. وتتميز هذه الثقافة بالمرونة والاعتماد على العمل الجماعي. [1]

4- ثقافة الفرد (Person Culture):

يكون الفرد في هذا النوع من الثقافة محور الاهتمام داخل المنظمة، حيث تُمنح أهمية كبيرة لخبرات العاملين ومهاراتهم الفردية. ويظهر هذا النوع غالبًا في المؤسسات المهنية مثل مكاتب الاستشارات أو المؤسسات البحثية.

وتختلف المؤسسات في نوع الثقافة التنظيمية التي تتبناها، إلا أن الثقافة التنظيمية الفعالة هي التي تتوافق مع أهداف المؤسسة وطبيعة نشاطها، وتسهم في تعزيز الأداء التنظيمي وتحقيق النجاح المؤسسي.

[1] أحمد ماهر، **مرجع سابق**، ص 145.

المبحث الثاني: الأمن السيبراني

أصبح الأمن السيبراني من القضايا الأساسية التي تحظى باهتمام كبير في العصر الرقمي، خاصة مع التوسع الكبير في استخدام تكنولوجيا المعلومات والاتصالات داخل المؤسسات المختلفة. فقد أدى الاعتماد المتزايد على الأنظمة الرقمية والشبكات الإلكترونية إلى ظهور العديد من التهديدات والمخاطر التي تستهدف البيانات والمعلومات الحساسة، مما جعل حماية هذه الأنظمة ضرورة ملحة لضمان استمرارية العمل وسلامة المعلومات. [1]

ويشير مفهوم الأمن السيبراني إلى مجموعة الإجراءات والتقنيات والسياسات التي تهدف إلى حماية الأنظمة المعلوماتية والشبكات والبيانات من الهجمات الإلكترونية أو الاختراقات التي قد تؤدي إلى سرقة المعلومات أو إتلافها أو تعطيل الأنظمة. كما يسعى الأمن السيبراني إلى توفير بيئة رقمية آمنة تضمن سرية المعلومات وسلامتها وتوفرها للمستخدمين المصرح لهم فقط.

وتزداد أهمية الأمن السيبراني في المؤسسات الحديثة التي تعتمد بشكل كبير على التحول الرقمي، حيث أصبحت البيانات الرقمية أحد أهم الأصول الاستراتيجية للمؤسسات. ومن هذا المنطلق، فإن تعزيز الأمن السيبراني لا يقتصر فقط على استخدام التقنيات الحديثة للحماية، بل يشمل أيضًا نشر الوعي الأمني لدى العاملين داخل المؤسسة وتطوير ثقافة تنظيمية تدعم حماية المعلومات والأنظمة الرقمية

المطلب الأول: مفهوم الأمن السيبراني

يعد الأمن السيبراني أحد المفاهيم الحديثة التي ظهرت نتيجة التطور الكبير في مجال تكنولوجيا المعلومات والاتصالات، حيث أصبح من الضروري توفير آليات فعالة لحماية الأنظمة المعلوماتية من التهديدات الإلكترونية المختلفة. ويشمل الأمن السيبراني مجموعة من الإجراءات التقنية والتنظيمية التي تهدف إلى حماية المعلومات والبيانات الرقمية من الاختراق أو التلاعب أو الاستخدام غير المشروع.

ويعتمد الأمن السيبراني على مجموعة من الأدوات والبرمجيات والتقنيات التي تساعد على اكتشاف الهجمات الإلكترونية والتصدي لها، إضافة إلى وضع سياسات وإجراءات تنظيمية لضمان الاستخدام الآمن للأنظمة المعلوماتية داخل المؤسسات. كما يشمل أيضًا تدريب العاملين على كيفية التعامل مع المخاطر الإلكترونية وتجنب السلوكيات التي قد تؤدي إلى تعريض الأنظمة للاختراق.

ومن هنا، فإن الأمن السيبراني يمثل منظومة متكاملة تجمع بين الجوانب التقنية والتنظيمية والبشرية، بهدف توفير بيئة رقمية آمنة تحمي المعلومات والأنظمة من التهديدات المختلفة.

[1] عبد الرحمن توفيق، **إدارة أمن المعلومات**، مركز الخبرات المهنية للإدارة، القاهرة، 2016، ص 73.

الفرع الأول: تعريف الأمن السيبراني

تعددت تعريفات الأمن السيبراني نتيجة تنوع المجالات التي يرتبط بها، حيث عرفه بعض الباحثين بأنه مجموعة من الوسائل والإجراءات التقنية والإدارية التي تهدف إلى حماية الأنظمة المعلوماتية والشبكات والبيانات من الهجمات الإلكترونية أو الوصول غير المصرح به. [1]

كما يُعرف الأمن السيبراني بأنه مجموعة من السياسات والتقنيات التي تهدف إلى حماية المعلومات الرقمية من التهديدات الإلكترونية، وضمان سرية البيانات وسلامتها وتوفرها للمستخدمين المصرح لهم فقط. [2]

ويشير تعريف آخر إلى أن الأمن السيبراني هو عملية حماية الأنظمة المعلوماتية والأجهزة والشبكات من الهجمات الإلكترونية التي قد تستهدف سرقة البيانات أو تعطيل الخدمات الرقمية.[3] ومن خلال هذه التعريفات يمكن القول إن الأمن السيبراني هو منظومة متكاملة من الإجراءات والتقنيات والسياسات التي تهدف إلى حماية الفضاء الرقمي وضمان الاستخدام الآمن للأنظمة المعلوماتية داخل المؤسسات.

الفرع الثاني: أهداف الأمن السيبراني

يسعى الأمن السيبراني إلى تحقيق مجموعة من الأهداف الأساسية التي تهدف إلى حماية المعلومات والأنظمة الرقمية داخل المؤسسات، ومن أهم هذه الأهداف ما يلي:

1- حماية سرية المعلومات:

يهدف الأمن السيبراني إلى ضمان عدم وصول المعلومات الحساسة إلى الأشخاص غير المصرح لهم، وذلك من خلال استخدام تقنيات التشفير وأنظمة التحكم في الوصول إلى البيانات.

2- ضمان سلامة البيانات:

يقصد بسلامة البيانات الحفاظ على دقة المعلومات وعدم التلاعب بها أو تعديلها بطريقة غير مشروعة، وذلك من خلال استخدام أنظمة الحماية المختلفة التي تمنع الاختراق أو التغيير غير المصرح به.

[1] William Stallings, Cybersecurity and Network Security, Pearson Publishing, 2018, p. 12.
[2] يوسف أحمد العلي، **أساسيات الأمن السيبراني**، دار الفكر العربي، القاهرة، 2019، ص 101.

3- ضمان توفر المعلومات:

يسعى الأمن السيبراني إلى ضمان توفر المعلومات والأنظمة الرقمية للمستخدمين المصرح لهم في الوقت المناسب، مما يضمن استمرارية العمل داخل المؤسسات وعدم تعطل الخدمات الإلكترونية.

4- حماية البنية التحتية الرقمية:

يهدف الأمن السيبراني أيضًا إلى حماية الشبكات والأنظمة الإلكترونية التي تعتمد عليها المؤسسات في أداء أعمالها، وذلك من خلال اتخاذ إجراءات وقائية للحد من الهجمات الإلكترونية.

5- الحد من المخاطر الإلكترونية:

يسهم الأمن السيبراني في تقليل المخاطر التي قد تتعرض لها المؤسسات نتيجة الهجمات الإلكترونية مثل سرقة البيانات أو تعطيل الأنظمة أو الابتزاز الإلكتروني.

الفرع الثالث: خصائص الأمن السيبراني

يتميز الأمن السيبراني بعدد من الخصائص التي تجعله عنصرًا أساسيًا في حماية الأنظمة المعلوماتية داخل المؤسسات، ومن أبرز هذه الخصائص ما يلي:

1- الشمولية:

يشمل الأمن السيبراني جميع مكونات النظام المعلوماتي، بما في ذلك الأجهزة والبرمجيات والشبكات والبيانات، إضافة إلى العنصر البشري الذي يعد من أهم عناصر الأمن المعلوماتي.

2- الاستمرارية:

يتطلب الأمن السيبراني مراقبة مستمرة للأنظمة والشبكات من أجل اكتشاف التهديدات الإلكترونية والتصدي لها في الوقت المناسب.

3- التحديث المستمر:

نظرًا للتطور المستمر في أساليب الهجمات الإلكترونية، فإن أنظمة الأمن السيبراني تحتاج إلى تحديث دائم لمواكبة هذه التهديدات.

4- الوقاية والاستجابة:

لا يقتصر الأمن السيبراني على منع الهجمات فقط، بل يشمل أيضًا الاستجابة السريعة للحوادث الإلكترونية وتقليل آثارها على الأنظمة المعلوماتية.

5- الاعتماد على التكنولوجيا والوعي البشري:

يعتمد الأمن السيبراني على استخدام التقنيات الحديثة للحماية، إضافة إلى نشر الوعي الأمني بين العاملين داخل المؤسسات لتجنب السلوكيات التي قد تؤدي إلى اختراق الأنظمة.

وتبرز أهمية هذه الخصائص في تعزيز قدرة المؤسسات على مواجهة التهديدات الإلكترونية وضمان حماية المعلومات والأنظمة الرقمية، خاصة في ظل الاعتماد المتزايد على التكنولوجيا في مختلف مجالات العمل [1]

المطلب الثاني: تهديدات الأمن السيبراني في المؤسسات

في ظل التطور المتسارع لتكنولوجيا المعلومات والاتصالات، أصبحت المؤسسات تعتمد بشكل كبير على الأنظمة الرقمية في إدارة أعمالها وحفظ بياناتها، وهو ما أدى إلى زيادة تعرضها للتهديدات السيبرانية المختلفة. وتشمل هذه التهديدات مجموعة من الهجمات الإلكترونية التي تستهدف الأنظمة المعلوماتية والشبكات بهدف سرقة البيانات أو تعطيل الخدمات أو إحداث أضرار مادية ومعنوية بالمؤسسات.

وتعد المؤسسات الحديثة، وخاصة المؤسسات التعليمية والجامعية، من أكثر الجهات عرضة للهجمات السيبرانية بسبب اعتمادها الكبير على الأنظمة الرقمية في إدارة العملية التعليمية والبحث العلمي وتبادل المعلومات. كما أن وجود عدد كبير من المستخدمين داخل هذه المؤسسات، مثل الطلبة والأساتذة والموظفين، يزيد من احتمالية حدوث اختراقات أمنية نتيجة ضعف الوعي الأمني أو سوء استخدام الأنظمة المعلوماتية.

[1] محمد الهادي محمد، **أمن المعلومات وحماية الشبكات**، دار المسيرة للنشر والتوزيع، عمان، 2017، ص 55.

ومن هذا المنطلق، أصبح من الضروري على المؤسسات الاهتمام بتعزيز إجراءات الأمن السيبراني لمواجهة هذه التهديدات وحماية بياناتها وأنظمتها من الهجمات الإلكترونية المتزايدة.

الفرع الأول: أنواع الهجمات السيبرانية

تتنوع الهجمات السيبرانية التي تستهدف الأنظمة المعلوماتية للمؤسسات، وتختلف في أساليبها وأهدافها، ومن أبرز هذه الهجمات ما يلي:

1- هجمات البرمجيات الخبيثة (Malware):

تعد البرمجيات الخبيثة من أكثر أنواع الهجمات السيبرانية انتشارًا، وتشمل الفيروسات والديدان الإلكترونية وبرامج التجسس، حيث يتم تصميم هذه البرمجيات بهدف إلحاق الضرر بالأنظمة المعلوماتية أو سرقة البيانات الحساسة. [1]

2- هجمات التصيد الإلكتروني (Phishing):

تعتمد هذه الهجمات على خداع المستخدمين من خلال إرسال رسائل إلكترونية مزيفة تبدو وكأنها صادرة من جهات موثوقة، بهدف الحصول على معلومات حساسة مثل كلمات المرور أو البيانات البنكية. [2]

3- هجمات حجب الخدمة (Denial of Service – DoS):

تهدف هذه الهجمات إلى تعطيل الخدمات الإلكترونية من خلال إغراق الخوادم بطلبات كثيرة في وقت واحد، مما يؤدي إلى توقف النظام عن العمل وعدم قدرة المستخدمين على الوصول إلى الخدمات. [3]

4- هجمات الاختراق المباشر (Hacking):

يقوم المخترقون في هذا النوع من الهجمات بمحاولة الوصول غير المصرح به إلى الأنظمة المعلوماتية من خلال استغلال الثغرات الأمنية الموجودة في البرامج أو الشبكات.

---

[1] محمد الهادي محمد، **مرجع سابق** ، ص 121.
[2] عبد الرحمن توفيق، **مرجع سابق**، ص 154.
[3] يوسف أحمد العلي، **مرجع سابق** ، ص 143.

5- هجمات الفدية الإلكترونية (Ransomware):

في هذا النوع من الهجمات يقوم المهاجمون بتشفير بيانات المؤسسة ومنع الوصول إليها، ثم يطلبون دفع مبلغ مالي مقابل إعادة فتح البيانات أو فك التشفير عنها.

وتشكل هذه الهجمات تهديدًا حقيقيًا للمؤسسات التي تعتمد على الأنظمة الرقمية، مما يتطلب اتخاذ إجراءات وقائية فعالة لحماية البنية التحتية المعلوماتية.

الفرع الثاني: مخاطر الاختراقات المعلوماتية

تؤدي الاختراقات المعلوماتية إلى العديد من المخاطر التي قد تؤثر بشكل مباشر على أداء المؤسسات واستقرارها، ومن أبرز هذه المخاطر ما يلي:

1- سرقة البيانات الحساسة:

تعد سرقة المعلومات من أخطر نتائج الاختراقات السيبرانية، حيث قد يتمكن المخترقون من الوصول إلى بيانات مهمة مثل المعلومات الشخصية أو البيانات المالية أو الأسرار المهنية للمؤسسة.

2- تعطيل الأنظمة الإلكترونية:

قد تؤدي الهجمات السيبرانية إلى تعطيل الأنظمة المعلوماتية لفترات طويلة، مما يؤثر سلبًا على سير العمل داخل المؤسسة ويؤدي إلى خسائر مادية كبيرة.

3- الإضرار بسمعة المؤسسة:

عند تعرض المؤسسة لاختراق أمني، قد يؤدي ذلك إلى فقدان ثقة المستخدمين والعملاء فيها، مما يؤثر على سمعتها ومكانتها في المجتمع.

4- الخسائر المالية:

تتحمل المؤسسات التي تتعرض لهجمات سيبرانية تكاليف كبيرة لإصلاح الأنظمة المتضررة واستعادة البيانات المسروقة أو المفقودة.

5- انتهاك الخصوصية:

قد تؤدي الاختراقات المعلوماتية إلى الكشف عن معلومات شخصية أو سرية، مما يشكل انتهاكًا لخصوصية الأفراد ويعرض المؤسسة للمساءلة القانونية.

الفرع الثالث: تحديات الأمن السيبراني في المؤسسات الجامعية

تواجه المؤسسات الجامعية مجموعة من التحديات المتعلقة بتطبيق الأمن السيبراني، وذلك بسبب طبيعة البيئة الأكاديمية التي تعتمد على الانفتاح وتبادل المعلومات بين عدد كبير من المستخدمين. ومن أهم هذه التحديات ما يلي:

1- ضعف الوعي الأمني لدى المستخدمين:

يعد نقص المعرفة بمخاطر الأمن السيبراني من أبرز التحديات التي تواجه الجامعات، حيث قد يقوم بعض الطلبة أو الموظفين باستخدام الأنظمة بطريقة غير آمنة مما يعرضها للاختراق.

2- تنوع الأجهزة والشبكات:

تستخدم الجامعات عددًا كبيرًا من الأجهزة والشبكات المختلفة، مثل الحواسيب الشخصية والهواتف الذكية والأجهزة اللوحية، مما يزيد من صعوبة تأمينها بشكل كامل.

3- محدودية الموارد المالية والتقنية:

تعاني بعض المؤسسات الجامعية من نقص الموارد اللازمة لتطوير أنظمة أمن سيبراني متقدمة، مما يجعلها أكثر عرضة للهجمات الإلكترونية.

4- كثرة المستخدمين داخل النظام المعلوماتي:

تضم الجامعات عددًا كبيرًا من الطلبة والأساتذة والموظفين الذين يستخدمون الشبكات الجامعية بشكل يومي، وهو ما يزيد من احتمالية حدوث ثغرات أمنية.

5- التطور المستمر للهجمات الإلكترونية:

تتطور أساليب الهجمات السيبرانية بشكل مستمر، مما يتطلب من المؤسسات الجامعية تحديث أنظمة الحماية بشكل دائم لمواجهة هذه التهديدات. [1]

وعليه، فإن تعزيز الأمن السيبراني في المؤسسات الجامعية يتطلب تبني استراتيجيات متكاملة تشمل استخدام التقنيات الحديثة للحماية، إضافة إلى نشر ثقافة الوعي الأمني بين جميع المستخدمين داخل المؤسسة.

[1] .William Stallings, Network Security Essentials, Pearson Education, 2017, p. 85

خلاصة الفصل:

نستخلص مما سبق في هذا الفصل أن العلاقة بين الثقافة التنظيمية والأمن السيبراني هي علاقة تكاملية بامتياز؛ فالمؤسسة ليست مجرد أجهزة وأنظمة، بل هي كيان اجتماعي تحركه قيم ومعتقدات مشتركة. ويمكن إيجاز أهم النتائج التي توصلنا إليها في النقاط التالية:

الثقافة كمرجع سلوكي: الثقافة التنظيمية هي البوصلة التي تحدد هوية المؤسسة وتوجه سلوك العاملين فيها؛ فهي لا تقتصر على القواعد الرسمية بل تمتد لتشمل الأعراف والافتراضات غير المكتوبة التي تضمن انسجام الأفراد وتفانيهم في تحقيق الأهداف.

تنوع النماذج الثقافية: تختلف المؤسسات في أنماطها الثقافية (سواء كانت ثقافة قوة، دور، مهمة، أو فرد)، إلا أن الثقافة الناجحة هي التي تتسم بالمرونة والقدرة على مواكبة التغيرات التكنولوجية الحديثة.

الأمن السيبراني كمنظومة شاملة: لم يعد الأمن السيبراني مجرد جدران حماية تقنية، بل هو منظومة متكاملة تشمل (التقنيات، السياسات، والعنصر البشري)، ويهدف بالأساس إلى ضمان الثالوث الأمني: السرية، السلامة، والتوافر.

محورية العنصر البشري: أثبتت الدراسة أن التهديدات السيبرانية (كالاحتيال) غالباً ما تستهدف الحلقة الأضعف وهم الأفراد؛ لذا فإن الوعي الأمني المنبثق من ثقافة تنظيمية قوية هو خط الدفاع الأول والأهم.

خصوصية التحديات الجامعية: تواجه المؤسسات الجامعية تحديات مزدوجة بسبب طبيعتها المنفتحة وكثرة مستخدميها، مما يجعل من تبني ثقافة أمنية داخل إطار الثقافة التنظيمية العامة ضرورة حتمية لحماية البحث العلمي والبيانات الأكاديمية.

في الختام، يتضح أن تعزيز الأمن السيبراني يبدأ من غرس قيم الانضباط والمسؤولية الرقمية في صلب الثقافة التنظيمية، بحيث يصبح السلوك الأمني الآمن جزءاً من الهوية اليومية للموظف والباحث على حد سواء.

الفصل الثالث

دور الثقافة التنظيمية في تعزيز الأمن السيبراني داخل المؤسسات الجامعية

خطة الفصل:

- ❖ المبحث الأول: العلاقة بين الثقافة التنظيمية والأمن السيبراني
- ❖ المطلب الأول: تأثير الثقافة التنظيمية على سلوك الأفراد في الأمن السيبراني
- ❖ المطلب الثاني: بناء ثقافة تنظيمية داعمة للأمن السيبراني
- ❖ المبحث الثاني: آليات تعزيز الأمن السيبراني في الجامعات
- ❖ المطلب الأول: استراتيجيات تطبيق الأمن السيبراني في المؤسسات الجامعية
- ❖ المطلب الثاني: نماذج وتجارب في تعزيز الأمن السيبراني

تمهيد:

ينتقل البحث في هذا الفصل من الإطار المفاهيمي العام إلى المستوى الإجرائي والتحليلي، حيث يتم استكشاف الدور المحوري الذي تلعبه الثقافة التنظيمية كمتغير وسيط ومؤثر في فاعلية الأمن السيبراني داخل المؤسسات الجامعية. ففي ظل التزايد المطرد للهجمات التي تستهدف الأصول المعرفية والبحثية، لم يعد كافياً الاستثمار في التكنولوجيا وحدها، بل أضحى لزاماً صياغة عقلية تنظيمية واعية تدرك أن الأمن الرقمي هو مسؤولية تشاركية.

ومن هذا المنطلق، يسعى هذا الفصل إلى تبيان طبيعة العلاقة التفاعلية بين الثقافة والأمن عبر مبحثين متكاملين؛ يخصص المبحث الأول لدراسة انعكاسات الثقافة التنظيمية على سلوك الأفراد، ومدى مساهمة الوعي الأمني والالتزام بالسياسات في تحصين المؤسسة، مع التركيز على دور القيادة في غرس هذه القيم. أما المبحث الثاني، فيستعرض الآليات العملية والخطط الاستراتيجية لتعزيز الأمن السيبراني في الجامعات، مستعرضاً نماذج وتجارب عالمية وعربية، وصولاً إلى تقديم مقترحات عملية تهدف إلى بناء بيئة جامعية رقمية آمنة ومستدامة.

المبحث الأول: العلاقة بين الثقافة التنظيمية والأمن السيبراني

أصبحت العلاقة بين الثقافة التنظيمية والأمن السيبراني من الموضوعات المهمة في الدراسات الحديثة، خاصة في ظل التحول الرقمي الذي تشهده المؤسسات الجامعية واعتمادها المتزايد على الأنظمة المعلوماتية في إدارة العملية التعليمية والبحثية. فالأمن السيبراني لا يعتمد فقط على الوسائل التقنية والبرمجيات المتطورة، بل يتأثر بشكل كبير بسلوك الأفراد داخل المؤسسة ومدى التزامهم بإجراءات الحماية.

وتلعب الثقافة التنظيمية دورًا أساسيًا في تشكيل هذا السلوك، حيث تسهم القيم التنظيمية والمعتقدات المشتركة في توجيه تصرفات العاملين داخل المؤسسة نحو الاستخدام الآمن للتكنولوجيا. كما تساعد الثقافة التنظيمية الإيجابية في تعزيز الوعي الأمني لدى الأفراد وتشجيعهم على الالتزام بسياسات الحماية، مما يقلل من احتمالية وقوع الاختراقات الأمنية أو تسرب البيانات.

وفي هذا السياق، تُعد المؤسسات الجامعية بيئة حساسة من حيث الأمن السيبراني، نظرًا لاحتوائها على كميات كبيرة من البيانات الأكاديمية والبحثية، إضافة إلى كثرة المستخدمين داخل شبكاتها. ولذلك فإن بناء ثقافة تنظيمية داعمة للأمن السيبراني يعد من أهم العوامل التي تساعد الجامعات على حماية أنظمتها المعلوماتية وضمان سلامة بياناتها.

المطلب الأول: تأثير الثقافة التنظيمية على سلوك الأفراد في الأمن السيبراني

يُعد سلوك الأفراد أحد أهم العوامل المؤثرة في مستوى الأمن السيبراني داخل المؤسسات، حيث تشير العديد من الدراسات إلى أن نسبة كبيرة من الحوادث الأمنية تحدث نتيجة أخطاء بشرية أو عدم الالتزام بإجراءات الحماية. ومن هنا تأتي أهمية الثقافة التنظيمية التي تسهم في توجيه سلوك العاملين نحو الاستخدام الآمن للأنظمة المعلوماتية.

فالثقافة التنظيمية التي تشجع على الالتزام بالقواعد المهنية والمسؤولية الجماعية تساعد على نشر الوعي الأمني بين العاملين، كما تدفعهم إلى اتباع الممارسات الصحيحة في التعامل مع البيانات والأنظمة الرقمية. كما أن وجود ثقافة تنظيمية قوية يعزز الشعور بالمسؤولية لدى الأفراد تجاه حماية المعلومات والأنظمة داخل المؤسسة. [1]

وعليه، فإن تعزيز الثقافة التنظيمية الداعمة للأمن السيبراني يعد خطوة أساسية في تقليل المخاطر الإلكترونية داخل المؤسسات الجامعية، حيث يسهم ذلك في بناء بيئة عمل واعية بأهمية حماية المعلومات والالتزام بالإجراءات الأمنية.

[1] أحمد ماهر، **مرجع سابق**، ص 178.

الفرع الأول: الوعي الأمني

يعد الوعي الأمني من أهم العوامل التي تسهم في حماية الأنظمة المعلوماتية داخل المؤسسات، حيث يشير إلى مستوى إدراك الأفراد للمخاطر السيبرانية ومعرفتهم بكيفية التعامل معها. ويعتمد نجاح أنظمة الأمن السيبراني بدرجة كبيرة على مدى وعي المستخدمين بالتهديدات الإلكترونية وأساليب الوقاية منها.

وتسهم الثقافة التنظيمية في تعزيز هذا الوعي من خلال نشر قيم المسؤولية والالتزام داخل المؤسسة، إضافة إلى تنظيم برامج تدريبية وورش عمل تهدف إلى تعريف العاملين بمخاطر الهجمات السيبرانية وطرق التعامل معها. كما تساعد الثقافة التنظيمية الإيجابية في تشجيع العاملين على الإبلاغ عن أي تهديدات أو سلوكيات مشبوهة قد تعرض الأنظمة المعلوماتية للخطر. [1]

ومن خلال تعزيز الوعي الأمني لدى الأفراد، يمكن للمؤسسات الجامعية تقليل نسبة الحوادث الأمنية الناتجة عن الأخطاء البشرية، مثل فتح الروابط المشبوهة أو استخدام كلمات مرور ضعيفة.

الفرع الثاني: الالتزام بسياسات الحماية

تعد سياسات الحماية من أهم الأدوات التي تعتمد عليها المؤسسات لضمان الاستخدام الآمن للأنظمة المعلوماتية، حيث تتضمن مجموعة من القواعد والإجراءات التي يجب على العاملين اتباعها لحماية البيانات والأنظمة الرقمية.

غير أن فعالية هذه السياسات تعتمد بدرجة كبيرة على مدى التزام الأفراد بها، وهو ما يتأثر بشكل مباشر بالثقافة التنظيمية السائدة داخل المؤسسة. فالثقافة التنظيمية التي تشجع على الانضباط والمسؤولية المهنية تسهم في تعزيز التزام العاملين بتطبيق سياسات الأمن السيبراني. [2]

كما أن المؤسسات التي تسعى إلى ترسيخ ثقافة أمنية قوية تعمل على توعية العاملين بأهمية هذه السياسات وضرورة الالتزام بها، إضافة إلى توفير التدريب المستمر حول كيفية تطبيقها في بيئة العمل. ويسهم ذلك في تقليل المخاطر المرتبطة بالاستخدام غير الآمن للأنظمة المعلوماتية.

---

[1] عبد الرحمن توفيق، **مرجع سابق**، 2016، ص 203.
[2] محمد الهادي محمد، **مرجع سابق** ، 2017، ص 189.

الفرع الثالث: دور القيادة في نشر ثقافة الأمن

تلعب القيادة الإدارية دورًا مهمًا في تعزيز الثقافة التنظيمية الداعمة للأمن السيبراني داخل المؤسسات، حيث تقع على عاتق القادة مسؤولية وضع السياسات والإجراءات التي تهدف إلى حماية الأنظمة المعلوماتية. كما يسهم القادة في نشر الوعي الأمني بين العاملين من خلال تشجيعهم على الالتزام بالممارسات الآمنة في استخدام التكنولوجيا.

وتعمل القيادة الفعالة على توفير بيئة تنظيمية تشجع على التعلم المستمر وتبادل المعرفة حول قضايا الأمن السيبراني، إضافة إلى دعم البرامج التدريبية التي تهدف إلى تطوير مهارات العاملين في مجال حماية المعلومات. كما تسهم القيادة في تعزيز ثقافة المسؤولية المشتركة تجاه الأمن السيبراني، بحيث يدرك جميع أفراد المؤسسة أن حماية المعلومات مسؤولية جماعية وليست مقتصرة على قسم تقنية المعلومات فقط.

ومن خلال هذا الدور القيادي، يمكن للمؤسسات الجامعية بناء ثقافة تنظيمية قوية تسهم في تعزيز الأمن السيبراني وحماية البيانات والأنظمة الرقمية من التهديدات المختلفة.

المطلب الثاني: بناء ثقافة تنظيمية داعمة للأمن السيبراني

في ظل التطور المتسارع في مجال التكنولوجيا والاعتماد المتزايد على الأنظمة الرقمية داخل المؤسسات الجامعية، أصبح بناء ثقافة تنظيمية داعمة للأمن السيبراني أمرًا ضروريًا لضمان حماية المعلومات والبيانات الحساسة. فالأمن السيبراني لا يعتمد فقط على استخدام التقنيات والبرمجيات الحديثة، بل يتطلب أيضًا وجود وعي تنظيمي وسلوك مسؤول من قبل جميع الأفراد داخل المؤسسة.

وتسهم الثقافة التنظيمية الداعمة للأمن السيبراني في تعزيز التزام العاملين بالممارسات الآمنة في استخدام الأنظمة المعلوماتية، كما تساعد على نشر الوعي بالمخاطر الإلكترونية وطرق الوقاية منها. وتتحقق هذه الثقافة من خلال مجموعة من الإجراءات التنظيمية والتوعوية التي تهدف إلى ترسيخ مفهوم الأمن السيبراني كجزء أساسي من ثقافة العمل داخل المؤسسة.

كما أن المؤسسات الجامعية التي تسعى إلى تعزيز أمنها السيبراني تعمل على تطوير استراتيجيات متكاملة تشمل تدريب العاملين، ووضع سياسات واضحة لحماية المعلومات، وتعزيز روح المسؤولية الجماعية تجاه حماية البيانات والأنظمة الرقمية. ومن خلال هذه الإجراءات يمكن للمؤسسات بناء بيئة تنظيمية آمنة تدعم الاستخدام المسؤول للتكنولوجيا وتحمي المعلومات من التهديدات السيبرانية المختلفة.

الفرع الأول: التدريب والتوعية الأمنية

يُعد التدريب والتوعية الأمنية من أهم الوسائل التي تعتمد عليها المؤسسات لتعزيز الثقافة التنظيمية الداعمة للأمن السيبراني. فالكثير من الهجمات الإلكترونية تحدث نتيجة نقص المعرفة لدى المستخدمين بكيفية التعامل مع التهديدات السيبرانية، مثل رسائل التصيد الإلكتروني أو الروابط المشبوهة.

لذلك تحرص المؤسسات على تنظيم برامج تدريبية وورش عمل توعوية تهدف إلى تعريف العاملين بمخاطر الأمن السيبراني وطرق الوقاية منها. وتشمل هذه البرامج تدريب الموظفين على استخدام كلمات مرور قوية، وتجنب فتح الرسائل الإلكترونية المشبوهة، والتعامل الآمن مع البيانات الحساسة.[1]

كما تسهم هذه البرامج في تعزيز قدرة العاملين على اكتشاف التهديدات الإلكترونية والإبلاغ عنها في الوقت المناسب، مما يساعد على تقليل المخاطر السيبرانية داخل المؤسسة. بالإضافة إلى ذلك، تساعد برامج التوعية الأمنية في ترسيخ مفهوم المسؤولية الفردية تجاه حماية المعلومات والأنظمة الرقمية.

ومن هنا، فإن الاستثمار في التدريب والتوعية الأمنية يعد خطوة أساسية في بناء ثقافة تنظيمية قوية تدعم الأمن السيبراني داخل المؤسسات الجامعية.

الفرع الثاني: السياسات التنظيمية للأمن المعلوماتي

تعد السياسات التنظيمية للأمن المعلوماتي من الركائز الأساسية التي تعتمد عليها المؤسسات لضمان حماية بياناتها وأنظمتها الرقمية. وتشمل هذه السياسات مجموعة من القواعد والإجراءات التي تنظم استخدام الأنظمة المعلوماتية داخل المؤسسة، وتحدد مسؤوليات الأفراد في الحفاظ على أمن المعلومات.

وتسهم هذه السياسات في توجيه سلوك العاملين داخل المؤسسة نحو الالتزام بالممارسات الآمنة في استخدام التكنولوجيا، كما تساعد على الحد من المخاطر المرتبطة بالاستخدام غير السليم للأنظمة الرقمية.[2]

---

[1] عبد الرحمن توفيق، **مرجع سابق**، ص 221.
[2] عبد الرحمن توفيق، **المرجع نفسه**، ص 245.

ومن أبرز السياسات التنظيمية التي تعتمدها المؤسسات في مجال الأمن المعلوماتي: سياسات إدارة كلمات المرور، وسياسات حماية البيانات، وسياسات استخدام البريد الإلكتروني، إضافة إلى سياسات التحكم في الوصول إلى الأنظمة المعلوماتية.

كما تعمل المؤسسات على مراجعة هذه السياسات بشكل دوري وتحديثها بما يتناسب مع التغيرات التكنولوجية والتحديات الأمنية الجديدة، وذلك لضمان فعاليتها في مواجهة التهديدات السيبرانية المختلفة.

الفرع الثالث: تعزيز المسؤولية الجماعية

يُعد تعزيز المسؤولية الجماعية من العوامل المهمة في بناء ثقافة تنظيمية داعمة للأمن السيبراني، حيث لا يمكن تحقيق مستوى عالٍ من الحماية المعلوماتية دون مشاركة جميع أفراد المؤسسة في تطبيق إجراءات الأمن السيبراني.

فالأمن السيبراني لا يقتصر فقط على دور قسم تكنولوجيا المعلومات، بل هو مسؤولية مشتركة بين جميع العاملين داخل المؤسسة. لذلك تسعى المؤسسات إلى نشر ثقافة تنظيمية تقوم على التعاون والتكامل بين مختلف الأقسام في مجال حماية المعلومات والأنظمة الرقمية.[3]

كما تعمل المؤسسات على تشجيع العاملين على الالتزام بالممارسات الآمنة في استخدام التكنولوجيا، والإبلاغ عن أي سلوكيات أو أنشطة قد تشكل تهديدًا للأمن السيبراني. ويسهم هذا التعاون في تعزيز قدرة المؤسسة على اكتشاف المخاطر الإلكترونية والتعامل معها بشكل فعال.

إضافة إلى ذلك، فإن تعزيز المسؤولية الجماعية يساعد على ترسيخ ثقافة أمنية داخل المؤسسة تقوم على الوعي والالتزام والانضباط، مما يؤدي في النهاية إلى تحسين مستوى الأمن السيبراني وحماية المعلومات من التهديدات المختلفة.

المبحث الثاني: آليات تعزيز الأمن السيبراني في الجامعات

في ظل التحول الرقمي المتسارع الذي تشهده المؤسسات الجامعية، أصبح الأمن السيبراني من أهم الأولويات التي يجب الاهتمام بها لضمان حماية الأنظمة المعلوماتية والبيانات الأكاديمية والبحثية. فالجامعات تعتمد بشكل كبير على الشبكات الإلكترونية في إدارة العملية التعليمية والبحث العلمي، إضافة إلى تخزين كميات كبيرة من المعلومات الحساسة المتعلقة بالطلبة والأساتذة والموظفين.

ومع تزايد التهديدات السيبرانية التي تستهدف المؤسسات التعليمية، أصبح من الضروري تبني مجموعة من الآليات والاستراتيجيات التي تساعد على تعزيز الأمن السيبراني داخل الجامعات. وتشمل هذه الآليات وضع سياسات واضحة لأمن المعلومات، واستخدام التقنيات الحديثة للحماية، إضافة إلى إدارة المخاطر السيبرانية بشكل فعال. كما أن الاستفادة من التجارب الدولية في هذا المجال يمكن أن تساعد المؤسسات الجامعية على تطوير استراتيجيات فعالة لحماية أنظمتها الرقمية.

المطلب الأول: استراتيجيات تطبيق الأمن السيبراني في المؤسسات الجامعية

تسعى المؤسسات الجامعية إلى تبني استراتيجيات فعالة لتطبيق الأمن السيبراني بهدف حماية أنظمتها المعلوماتية من التهديدات الإلكترونية المختلفة. وتعتمد هذه الاستراتيجيات على مجموعة من الإجراءات التنظيمية والتقنية التي تهدف إلى تعزيز مستوى الحماية المعلوماتية داخل المؤسسة.

كما تتطلب هذه الاستراتيجيات التعاون بين مختلف الأقسام داخل الجامعة، إضافة إلى توفير الموارد البشرية والتقنية اللازمة لتطبيق أنظمة الحماية بشكل فعال. وتشمل استراتيجيات الأمن السيبراني عدة عناصر أساسية من بينها وضع سياسات أمن المعلومات، واستخدام التقنيات الحديثة للحماية، إضافة إلى إدارة المخاطر السيبرانية.

الفرع الأول: وضع سياسات أمن المعلومات

تعد سياسات أمن المعلومات من أهم الأدوات التي تعتمد عليها المؤسسات الجامعية لضمان حماية بياناتها وأنظمتها الرقمية. وتشمل هذه السياسات مجموعة من القواعد والإجراءات التي تنظم كيفية استخدام الأنظمة المعلوماتية داخل الجامعة، وتحدد مسؤوليات الأفراد في الحفاظ على أمن المعلومات.

وتسهم هذه السياسات في توجيه سلوك المستخدمين داخل المؤسسة نحو الاستخدام الآمن للتكنولوجيا، كما تساعد على الحد من المخاطر المرتبطة بالاستخدام غير السليم للأنظمة المعلوماتية. وتشمل سياسات أمن المعلومات عادةً عدة جوانب مثل سياسات إدارة كلمات المرور، وسياسات حماية البيانات، وسياسات استخدام البريد الإلكتروني والشبكات.[1]

كما تعمل الجامعات على مراجعة هذه السياسات بشكل دوري وتحديثها بما يتناسب مع التغيرات التكنولوجية والتحديات الأمنية الجديدة، وذلك لضمان فعاليتها في مواجهة التهديدات السيبرانية.

[1] عبد الرحمن توفيق، **مرجع سابق**، 2016، ص 246.

الفرع الثاني: استخدام التقنيات الحديثة للحماية

تعتمد المؤسسات الجامعية على مجموعة من التقنيات الحديثة لتعزيز مستوى الأمن السيبراني وحماية الأنظمة المعلوماتية من الهجمات الإلكترونية. وتشمل هذه التقنيات أنظمة الحماية مثل الجدران النارية، وبرمجيات مكافحة الفيروسات، وأنظمة كشف التسلل التي تساعد على مراقبة الشبكات واكتشاف الأنشطة المشبوهة.[1]

كما يتم استخدام تقنيات التشفير لحماية البيانات الحساسة ومنع الوصول غير المصرح به إليها، إضافة إلى استخدام أنظمة المصادقة المتعددة التي تعتمد على أكثر من وسيلة للتحقق من هوية المستخدم.

وتساعد هذه التقنيات في تقليل احتمالية تعرض الأنظمة المعلوماتية للاختراق، كما تسهم في تعزيز قدرة المؤسسات الجامعية على اكتشاف الهجمات السيبرانية والاستجابة لها بشكل سريع وفعال.

الفرع الثالث: إدارة المخاطر السيبرانية

تعد إدارة المخاطر السيبرانية من العناصر الأساسية في استراتيجيات الأمن السيبراني داخل المؤسسات الجامعية. ويقصد بإدارة المخاطر عملية تحديد التهديدات المحتملة التي قد تواجه الأنظمة المعلوماتية، وتحليل آثارها المحتملة، ثم وضع الإجراءات المناسبة للحد من هذه المخاطر.[2]

وتشمل إدارة المخاطر السيبرانية عدة مراحل، منها تحديد الأصول المعلوماتية المهمة داخل المؤسسة، وتقييم نقاط الضعف في الأنظمة المعلوماتية، إضافة إلى وضع خطط للاستجابة للحوادث الأمنية.

كما تسهم إدارة المخاطر في مساعدة المؤسسات الجامعية على اتخاذ قرارات استراتيجية بشأن استثماراتها في مجال الأمن السيبراني، وذلك من خلال تحديد الأولويات وتخصيص الموارد اللازمة لتعزيز الحماية المعلوماتية.

المطلب الثاني: نماذج وتجارب في تعزيز الأمن السيبراني

تسعى العديد من الجامعات حول العالم إلى تطوير استراتيجيات فعالة لتعزيز الأمن السيبراني داخل مؤسساتها، وذلك من خلال تبني أحدث التقنيات وتطبيق أفضل الممارسات في مجال

[1] محمد الهادي محمد، **مرجع سابق** ، 2017، ص 216.
[2] محمد الهادي محمد، **المرجع نفسه**، 2017، ص 217.

حماية المعلومات. كما أن دراسة هذه التجارب يمكن أن تساعد المؤسسات الجامعية الأخرى على الاستفادة من الخبرات الدولية في هذا المجال وتطوير سياساتها الأمنية.

وفي المقابل، تسعى الجامعات العربية أيضًا إلى تعزيز مستوى الأمن السيبراني لديها من خلال تطوير البنية التحتية المعلوماتية وتبني استراتيجيات حديثة للحماية، رغم التحديات التي تواجهها في هذا المجال.

الفرع الأول: تجارب جامعات عالمية

تعد الجامعات العالمية من المؤسسات الرائدة في مجال تطبيق استراتيجيات الأمن السيبراني، حيث تعتمد العديد منها على أنظمة متقدمة لحماية شبكاتها وبياناتها الرقمية.

فعلى سبيل المثال، تعتمد بعض الجامعات الأمريكية على مراكز متخصصة في الأمن السيبراني تعمل على مراقبة الشبكات بشكل مستمر واكتشاف التهديدات الإلكترونية في وقت مبكر. كما تقوم هذه الجامعات بتنظيم برامج تدريبية دورية للطلبة والموظفين لتعزيز الوعي الأمني لديهم.

كما تعمل بعض الجامعات الأوروبية على تطوير برامج تعليمية متخصصة في مجال الأمن السيبراني، بهدف إعداد كوادر بشرية مؤهلة قادرة على مواجهة التحديات الأمنية في العصر الرقمي.

الفرع الثاني: واقع الأمن السيبراني في الجامعات العربية

شهدت الجامعات العربية خلال السنوات الأخيرة اهتمامًا متزايدًا بقضايا الأمن السيبراني، وذلك نتيجة تزايد التهديدات الإلكترونية التي تستهدف المؤسسات التعليمية.

وتعمل العديد من الجامعات العربية على تطوير بنيتها التحتية المعلوماتية وتعزيز أنظمة الحماية الرقمية لديها، من خلال استخدام تقنيات حديثة للحماية وتدريب العاملين على أساليب الاستخدام الآمن للتكنولوجيا.

ومع ذلك، لا تزال بعض الجامعات العربية تواجه تحديات في مجال الأمن السيبراني، مثل نقص الكوادر المتخصصة، وضعف الوعي الأمني لدى المستخدمين، إضافة إلى محدودية الموارد المالية والتقنية اللازمة لتطوير أنظمة الحماية.

الفرع الثالث: مقترحات لتعزيز الأمن السيبراني

من أجل تعزيز الأمن السيبراني داخل المؤسسات الجامعية، يمكن اقتراح مجموعة من الإجراءات التي تسهم في تحسين مستوى الحماية المعلوماتية، ومن أبرز هذه المقترحات ما يلي:

-تطوير سياسات واضحة وشاملة لأمن المعلومات داخل الجامعات.

-تنظيم برامج تدريبية مستمرة لتعزيز الوعي الأمني لدى الطلبة والأساتذة والموظفين.

-الاستثمار في التقنيات الحديثة للحماية مثل أنظمة كشف التسلل والتشفير.

-إنشاء وحدات أو مراكز متخصصة في الأمن السيبراني داخل الجامعات.

-تعزيز التعاون بين الجامعات والمؤسسات المتخصصة في مجال الأمن السيبراني.

وتسهم هذه الإجراءات في تعزيز قدرة الجامعات على مواجهة التهديدات السيبرانية وضمان حماية أنظمتها المعلوماتية وبياناتها الأكاديمية والبحثية.

خلاصة الفصل:

يُمكن استخلاص جملة من النتائج والحقائق الجوهرية التي انتهى إليها هذا الفصل، والتي تؤكد في مجملها أن الأمن السيبراني في الوسط الجامعي هو "ثقافة" قبل أن يكون "تقنية"، وذلك وفق النقاط الآتية:

السلوك البشري كخط دفاع أول: تأكد لنا أن الثقافة التنظيمية هي المحرك الأساسي لسلوك الأفراد؛ فبقدر ما تنجح الجامعة في نشر الوعي الأمني وترسيخ قيم المسؤولية، بقدر ما تتقلص الفجوات الأمنية الناتجة عن الأخطاء البشرية (مثل التصيد الإلكتروني)

القيادة هي القدوة الأمنية: لا يمكن بناء ثقافة أمنية دون دعم مباشر من الإدارة العليا؛ فالقادة هم المسؤولون عن توفير الموارد، ووضع السياسات، وتحويل الأمن السيبراني من مجرد وظيفة تقنية إلى قيمة تنظيمية عليا.

تكامل الاستراتيجية والتقنية: إن تعزيز الأمن في الجامعات يتطلب التوازي بين استخدام التقنيات الحديثة (كالتشفير وجدران الحماية) وبين وضع سياسات تنظيمية واضحة ومحدثة تنظم الحقوق والواجبات الرقمية لجميع المنتسبين.

المسؤولية الجماعية: خلص الفصل إلى أن الأمن السيبراني الناجح في الجامعات هو نتاج عمل تعاوني (تشاركي) لا يستثني أحداً، من الطالب إلى الأستاذ وصولاً إلى الإداري، مما يستدعي برامج تدريبية مستمرة لا تتوقف عند مرحلة معينة.

الاستفادة من النماذج العالمية: أظهرت التجارب أن الجامعات الناجحة أمنياً هي تلك التي أنشأت مراكز متخصصة وربطت بين البحث الأكاديمي والتطبيق الميداني للأمن السيبراني، وهو ما تفتقر إليه بعض الجامعات العربية التي لا تزال تواجه تحديات في نقص الكوادر والموارد.

في الختام يُعد هذا الفصل تأكيداً على أن الحماية الحقيقية للمؤسسات الجامعية تكمن في أنسنة الأمن السيبراني، أي بجعله جزءاً لا يتجزأ من السلوك اليومي والوعي الجماعي داخل الحرم الجامعي، لضمان حماية المكتسبات العلمية في فضاء رقمي دائم التغير.

الفصل الرابع

الإجراءات المنهجية للدراسة

تمهيد:

سنتطرق في هذا الفصل إلى أهم مجالات الدراسة التي تمثلت في المجال المكاني والزماني والبشري.

ثم المنهج المستخدم في الدراسة الذي تمثل في المنهج الوصفي وأدوات الدراسة التي تمثلت في الاستبيان وأخيرا عينة الدراسة المتمثلة في موظفين الكلية.

أولا / مجالات الدراسة:

1. المجال المكاني : أجريت هذه الدراسة بكلية العلوم الإجتماعية والإنسانية بجامعة زيان عاشور الجلفة.

2. المجال الزماني

أُنجزت هذه الدراسة خلال الموسم الجامعي **2025–2026**، حيث شملت مرحلة استطلاعية لجمع المعلومات، تلتها مرحلة ميدانية تم فيها توزيع الاستبيان على عينة من موظفي الكلية واسترجاعه وتحليله.

3. المجال البشري (مجتمع الدراسة)

يتمثل مجتمع الدراسة في جميع الموظفين العاملين بكلية العلوم الاجتماعية والانسانية جامعة زيان عاشور - الجلفة، والبالغ عددهم الإجمالي **72** موظفاً. يتوزعون على عدة مناصب وظيفية بالكلية

عينة الدراسة:

العينة العرَضية، وتُسمى عينة الصدفة / العينة المتاحة: وتعني اختيار أفراد المجتمع الذين يسهل الالتقاء بهم والوصول إليهم في زمان ومكان محددين حتى يكتمل العدد المطلوب.

ونظراً لطبيعة مجتمع الدراسة المكون من **72** موظفاً إدارياً، ولإعتبارات ميدانية تتعلق بتواجد الموظفين في مكاتبهم وتفرغهم للاستجابة لأداة البحث، اعتمدنا على العينة العَرَضية (عينة الصدفة) كأحد أنواع العينات غير الاحتمالية، حيث بلغ حجم العينة **24** موظفاً تم اختيارهم بناءً على إمكانية الالتقاء بهم وتجاوبهم أثناء الزيارات الميدانية لمقر الدراسة، وهو ما يمثل نسبة 33.3% من المجتمع الأصلي.

ثانيا / المنهج المستخدم في الدراسة:

نظرا لطبيعة الدراسة والأهداف المراد الوصول إليها يجب إتباع منهج معين على حسب دراسة العينة ويعرف منهج البحث العلمي بأنه: مجموعة من الأدوات والطرق والتقنيات الخاصة، والتي يتم استخدامها في فحص المعارف والظواهر المكتشفة، أو هو استكمال لبعض النظريات والمعلومات، ويعتمد ذلك على تجميع بعض التأكيدات، ويجب أن تكون قابلة للقياس والاستنتاج[1]

ولقد إعتمدنا في دراستنا المتمثلة في دور الثقافة التنظيمية في تعزيز الأمن السيبراني داخل المؤسسات الجامعية على المنهج الوصفي الذي يعرف على أنه: طريقة لدراسة الظواهر أو المشكلات العلمية من خلال القيام بوصف بطريقة علمية، ومن ثم الوصول إلى تفسيرات منطقية لها دلائل وبراهن تمنح الباحث القدرة على وضع أطر محددة للمشكلة ويتم إستخدام ذلك في تحديد نتائج البحث.

ثالثا / أدوات الدراسة:

إعتمدنا في هذه الدراسة على أداة الإستبيان.

الإستبيان: هو عبارة عن مجموعة من الأسئلة توجه للمبحوثين بهدف الحصول على معلومات معينة، وهي من أكثر الأدوات المستعملة.[2]

وقد تم تقسيم عبارات الإستبيان إلى خمسة محاور كالتالي :

1. **المحور الأول:** وهو محور البيانات الشخصية يضم 04 أسئلة المتعلقة بالمفردة من حيث: الجنس، السن، الخبرة المهنية، المنصب الوظيفي.
2. **المحور الثاني:** فقد اشتمل على 07 أسئلة كلها تتعلق باستبيان الثقافة التنظيمية ودعم الإدارة.
3. **المحور الثالث:** اشتمل على 05 أسئلة كلها تتعلق استبيان التدريب والتوعية.
4. **المحور الرابع:** اشتمل على 07 أسئلة كلها تتعلق استبيان السلوك والممارسات.
5. **المحور الخامس:** اشتمل على 05 أسئلة كلها تتعلق استبيان التهديدات الرقمية والالتزام.

[1] السعدي محمد وعايشة شريف ، **منهج البحث العلمي**. الإسكندرية، مصر: دار الهلال العربي 2017 ص 24
[2] عمار بوحوش ، **مناهج البحث العلمي وطرق إعداد البحوث**، ديوان المطبوعات الجامعية ، بن عكنون الجزائر ، ط4، 2007 ص 64

الفصل الخامس

عرض و تحليل و مناقشة النتائج

النتائج:

الجدول رقم (01): يوضح توزيع العينة حسب الجنس:

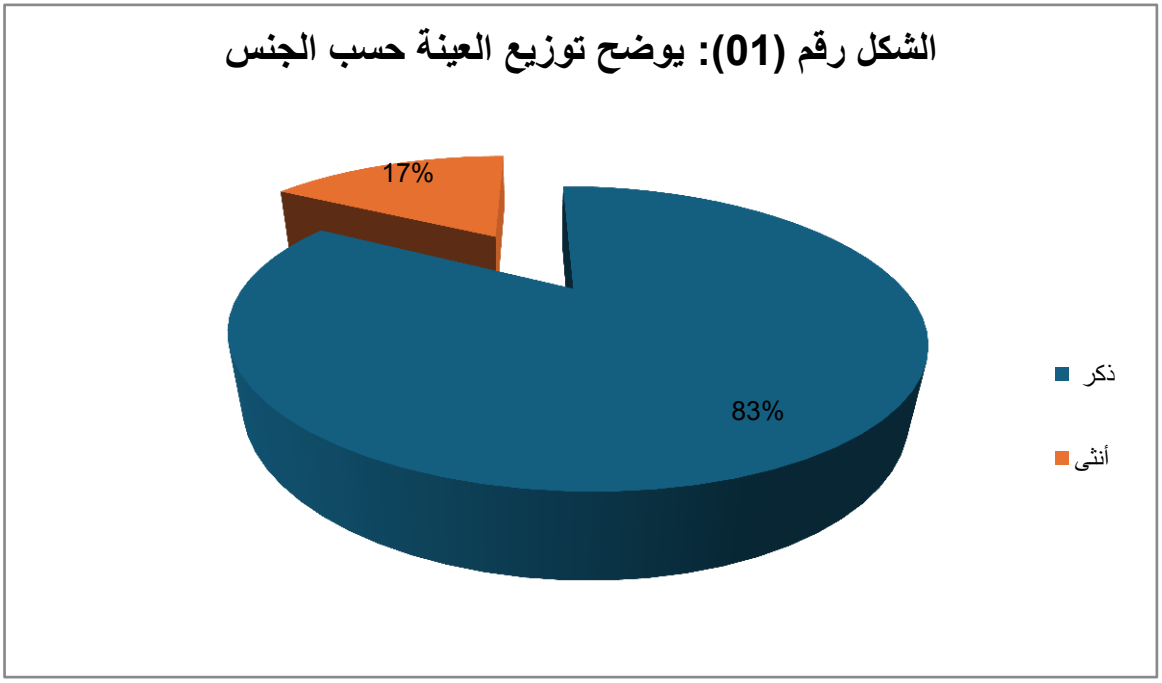
الجنس	التكرار	النسبة المئوية (%)
ذكر	20	83.30
أنثى	04	16.70
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

عند ملاحظتنا للجدول الذي يوضح توزيع العينة حسب الجنس نجد أن الذكور يمثلون الأغلبية الساحقة بنسبة 83.30%، بينما تمثل الإناث نسبة 16.70%.

يعكس هذا التباين هيمنة ذكورية واضحة في البيئة الإدارية والتقنية للكلية محل الدراسة، وقد يرتبط هذا بطبيعة التوظيف أو التخصصات التقنية السائدة التي لا تزال تجذب الذكور بشكل أكبر في هذا السياق التنظيمي.

الشكل رقم (01): يوضح توزيع العينة حسب الجنس



المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

الجدول رقم (02): يوضح توزيع العينة حسب السن:

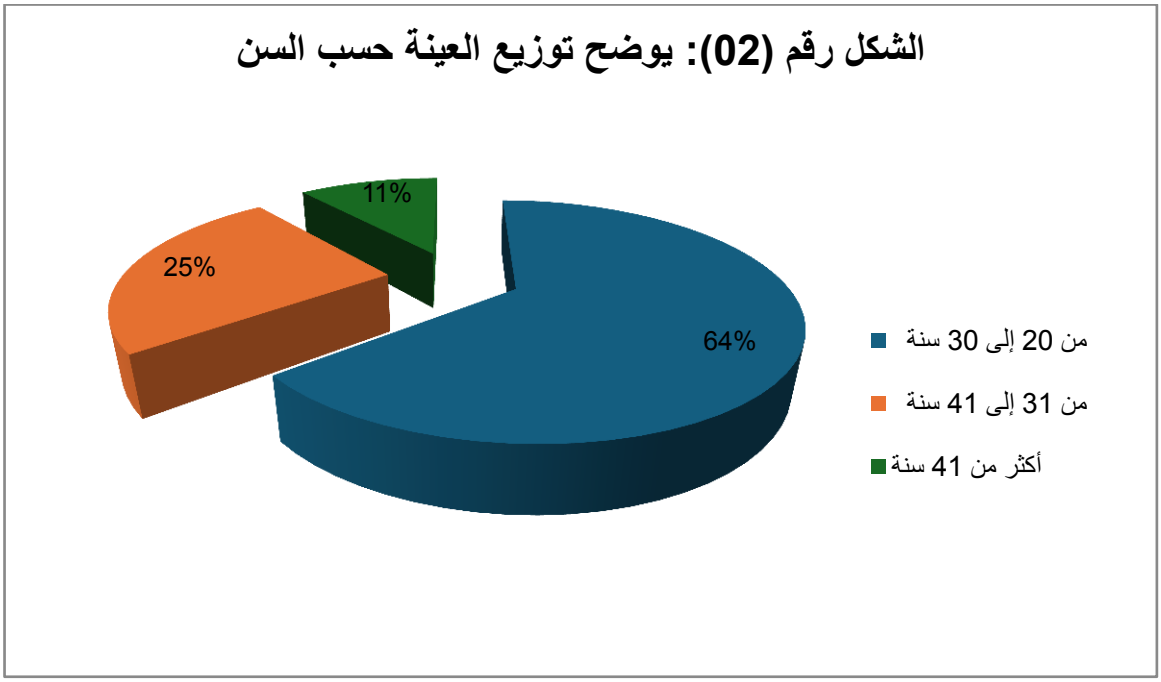
السن	التكرار	النسبة المئوية (%)
من 20 إلى 30 سنة	02	8.30
من 31 إلى 41 سنة	07	29.20
أكثر من 41 سنة	15	62.50
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

عند قراءة الجدول توزيع العينة حسب السن نلاحظ ان الفئة الغالبة هي "أكثر من 41 سنة" بنسبة 62.50%، تليها الفئة من "31 إلى 41 سنة" بنسبة 29.20%، في حين أن الفئة الشابة (20-30 سنة) تمثل 8.30% فقط.

يتسم المجتمع المبحوث بالنضج العمري اجتماعياً، هذا يعني أننا نتعامل مع "مهاجرين رقميين " وليس "أصليين رقميين"، مما قد يفسر حاجتهم الماسة للتدريب لمواكبة التهديدات السيبرانية المتطورة.

الشكل رقم (02): يوضح توزيع العينة حسب السن



المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

الجدول رقم (03): يوضح توزيع العينة حسب الخبرة المهنية:

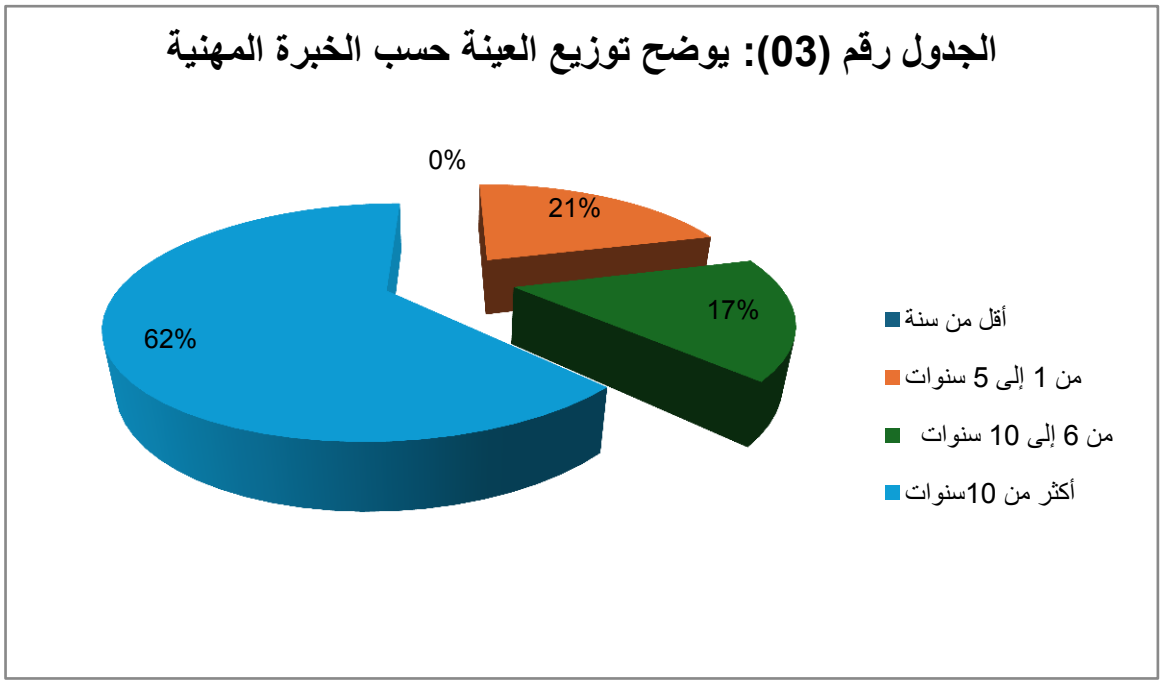
الخبرة المهنية	التكرار	النسبة المئوية (%)
أقل من سنة	00	00
من 1 إلى 5 سنوات	05	20.80
من 6 إلى 10 سنوات	04	16.70
أكثر من 10سنوات	15	62.50
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

عند قراءة جدول توزيع العينة حسب الخبرة المهنية نجد أنه يمتلك 62.50% من العينة خبرة تزيد عن 10 سنوات، في حين أن الفئة التي خبرتها (من 06-10 سنة) تمثل 16.70% بينما لم يسجل أي موظف خبرة أقل من سنة.

هاته النتائج تشير إلى استقرار وظيفي عالٍ وتراكم في الخبرات الإدارية التقليدية. مهنياً، الخبرة الطويلة قد تكون "سلاحاً ذو حدين"؛ فهي توفر دراية بالأنظمة، لكنها قد تولد مقاومة لتغيير العادات التقنية القديمة.

الجدول رقم (03): يوضح توزيع العينة حسب الخبرة المهنية



المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

الجدول رقم (04): يوضح توزيع العينة حسب المناصب الوظيفية:

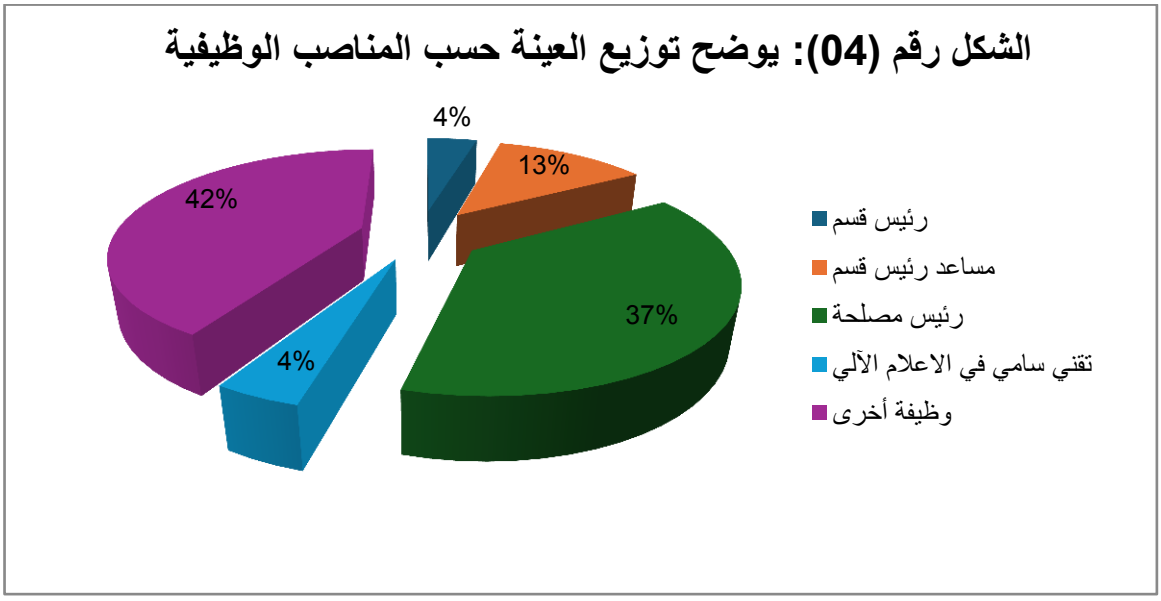
الخبرة المهنية	التكرار	النسبة المئوية (%)
عميد	00	00
نائب عميد	00	00
رئيس قسم	01	4.20
مساعد رئيس قسم	03	12.50
رئيس مصلحة	09	37.50
تقني سامي في الإعلام الآلي	01	4.20
وظيفة أخرى	10	41.7
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

نلاحظ انه تتركز الكتلة الأكبر في "وظيفة أخرى" بنسبة 41.7% و "رئيس مصلحة" بنسبة 37.50% بينما تمثل كل من "رئيس قسم" و"فئة تقني سامي في الإعلام الآلي" نسبة 4.20% من العينة المبحوثة.

نلاحظ ان تنوع المناصب الإدارية الوسطى والتنفيذية يشير إلى توزيع المسؤوليات الرقمية على مستويات مختلفة، مما يجعل أمن المعلومات مسؤولية مشتتة تتطلب تنسيقاً مركزياً.

الشكل رقم (04): يوضح توزيع العينة حسب المناصب الوظيفية



المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

الجدول رقم (05): يوضح توزيع العينة حسب رأيهم ما إذا كانت تحرص إدارة الكلية على توعية الموظفين بمخاطر استخدام الإنترنت بشكل دوري؟:

هل تحرص إدارة الكلية على توعية الموظفين بمخاطر استخدام الإنترنت بشكل دوري؟:	التكرار	النسبة المئوية (%)
نعم	08	33.30
لا	16	66.70
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

عند قراءة الجدول نجد أنه أفاد 66.70% من المبحوثين بأن الإدارة لا تحرص على توعيتهم دورياً، بينما يرى 33.30% عكس ذلك.

يظهر هنا "قصور اتصالي" من جانب الإدارة. سوسيولوجياً غياب التوعية الدورية يضعف الثقافة الوقائية ويترك الموظف معتمداً على اجتهاده الشخصي في مواجهة المخاطر.

الجدول رقم (06): يوضح توزيع العينة حسب رأيهم ما إذا كانت توجد تعليمات واضحة ومعلنة داخل الكلية تحظر مشاركة كلمات المرور الخاصة بالحسابات المهنية؟

هل توجد تعليمات واضحة ومعلنة داخل الكلية تحظر مشاركة كلمات المرور الخاصة بالحسابات المهنية؟	التكرار	النسبة المئوية (%)
نعم	15	62.50
لا	09	37.50
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

أكد 62.50% وجود تعليمات واضحة ومعلنة تحظر مشاركة كلمات المرور. بينما يرى 37.50% من المبحوثين عكس ذلك

يعكس هذا وجود "وعي إجرائي" رسمي. فالإدارة تعتمد على "الأوامر المكتوبة" كأداة ضبط اجتماعي داخل الكلية، وهي وسيلة تقليدية لكنها فعالة في تحديد المسؤوليات الفردية.

الجدول رقم (07): يوضح توزيع العينة حسب رأيهم ما إذا كانوا هل تشعر أن إدارة الكلية تضع الأمن السيبراني ضمن أولوياتها الإدارية؟

هل تشعر أن إدارة الكلية تضع الأمن السيبراني ضمن أولوياتها الإدارية؟	التكرار	النسبة المئوية (%)
نعم	08	33.30
لا	16	66.70
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

يرى 66.70% أن الإدارة لا تضع الأمن السيبراني ضمن أولوياتها، مقابل 33.30% يروون ذلك.

يوجد "فقدان ثقة" أو عدم إدراك الموظفين لجهود الإدارة. سوسيولوجياً عندما لا يشعر الموظف بأن الإدارة تهتم بالأمن، قد يقل التزامه الشخصي بالمعايير الأمنية.

الجدول رقم (08): يوضح توزيع العينة حسب رأيهم ما إذا كانت الكلية توفر نسخاً احتياطية للملفات الإدارية والبيداغوجية الهامة؟

هل توفر الكلية نسخاً احتياطية للملفات الإدارية والبيداغوجية الهامة؟	التكرار	النسبة المئوية (%)
نعم	18	75
لا	06	25
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

نلاحظ انه صرح 75% من المبحوثين بأن الكلية توفر نسخاً احتياطية للملفات. بينما ربع المبحوثين والممثلين بنسبة 25% صرحوا بلا.

تشير هذه النسبة المرتفعة إلى اهتمام الإدارة بالجانب "التقني المادي" للحماية (حفظ البيانات من الضياع) أكثر من اهتمامها بالجانب "البشري السلوكي" (التوعية).

الجدول رقم (09): يوضح توزيع العينة حسب رأيهم ما إذا كان يتم إبلاغ الموظفين فوراً في حال اكتشاف أي محاولة اختراق لأنظمة الجامعة؟

هل يتم إبلاغ الموظفين فوراً في حال اكتشاف أي محاولة اختراق لأنظمة الجامعة؟	التكرار	النسبة المئوية (%)
نعم	11	45.80
لا	13	54.20
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

عند السؤال عن الإبلاغ الفوري عن محاولات الاختراق يرى 54.20% أن الإدارة لا تبلغ الموظفين فور اكتشاف محاولات اختراق، بينما يؤكد 45.80% الإبلاغ.

تعكس هذه النسبة المتقاربة "غموضاً في الشفافية المؤسسية". سوسيولوجياً عدم الإبلاغ الفوري يضعف روح التعاون واليقظة الجماعية لدى الموظفين.

الجدول رقم (10): يوضح توزيع العينة حسب رأيهم ما إذا كان يوجد ميثاق أو وثيقة مكتوبة تحدد مسؤوليات الموظف تجاه حماية البيانات الرقمية؟

هل يوجد ميثاق أو وثيقة مكتوبة تحدد مسؤوليات الموظف تجاه حماية البيانات الرقمية؟	التكرار	النسبة المئوية (%)
نعم	10	41.70
لا	14	58.30
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

أشار 58.30% إلى غياب ميثاق أو وثيقة مكتوبة تحدد مسؤولياتهم تجاه حماية البيانات. بينما يرى 41.70% عكس ذلك.

غياب الميثاق يعني غياب "العقد الرقمي" بين الموظف والمؤسسة. اجتماعياً هذا يؤدي إلى تميع المسؤولية القانونية والأخلاقية عند وقوع حوادث أمنية.

الجدول رقم (11): يوضح توزيع العينة حسب رأيهم ما إذا كانت الكلية تشجع الموظفين على تقديم مقترحات لتحسين الأداء الرقمي والأمني؟

هل تشجع الكلية الموظفين على تقديم مقترحات لتحسين الأداء الرقمي والأمني؟	التكرار	النسبة المئوية (%)
نعم	05	20.80
لا	19	79.20
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

نلاحظ ان الأغلبية الساحقة 79.20% صرحت أن الكلية لا تشجعهم على تقديم مقترحات. بينما من يرون انها تشجعهم يمثلون نسبة 79.20% من المبحوثين.

يشير هذا إلى نمط "إدارة بيروقراطية عمودية" تفتقر للتشارك. وسوسيولوجياً تهميش دور الموظف في تقديم المقترحات يجعله "متلقياً سلبياً" للتعليمات وليس "شريكاً" في المنظومة الأمنية.

الجدول رقم (12): يوضح توزيع العينة حسب رأيهم ما إذا كان سبق لك المشاركة في دورة تدريبية حول كيفية حماية البيانات الرقمية داخل الجامعة؟

هل سبق لك المشاركة في دورة تدريبية حول كيفية حماية البيانات الرقمية داخل الجامعة؟	التكرار	النسبة المئوية (%)
نعم	6	25
لا	18	75
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

بالنسبة للمشاركة في دورات تدريبية نجد 75% من العينة لم يسبق لهم المشاركة في أي دورة تدريبية حول حماية البيانات داخل الجامعة. بينما تبقى نسبة 25% تمت مشاركتهم.

تعكس هذه النسبة "فجوة مهارية" حادة. وفي السوسيولوجية غياب التدريب الرسمي يجعل الموظف هو "الحلقة الأضعف" في سلسلة الأمن السيبراني بالكلية.

الجدول رقم (13): يوضح توزيع العينة حسب رأيهم ما إذا كان تتوفر في أروقة الكلية أو مكاتبها ملصقات إرشادية حول الأمن السيبراني؟

هل تتوفر في أروقة الكلية أو مكاتبها ملصقات إرشادية حول الأمن السيبراني؟	التكرار	النسبة المئوية (%)
نعم	5	20.80
لا	19	79.20
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

عند قراءة الجدول نرى أنه أكد 79.20% عدم وجود ملصقات إرشادية في الأروقة أو المكاتب. بينما يرى 20.80% عكس ذلك.

غياب الوسائل البصرية الإرشادية يعني غياب "البيئة المنبهة"، الملصقات تساهم في خلق وعي جمعي مستمر، وغيابها يعكس ضعف الاستراتيجية التوعوية الميدانية.

الجدول رقم (14): يوضح توزيع العينة حسب رأيهم ما إذا كان هل تصلك رسائل توعوية عبر البريد الإلكتروني المهني حول كيفية تجنب الروابط المشبوهة؟

هل تصلك رسائل توعوية عبر البريد الإلكتروني المهني حول كيفية تجنب الروابط المشبوهة؟	التكرار	النسبة المئوية (%)
نعم	8	33.30
لا	16	66.70
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

نرى ان نسبة 66.70% من العينة المبحوثة اجابتهم كانت لا تصلهم رسائل توعوية حول تجنب الروابط المشبوهة. وفي المقابل من تصلهم رسائل توعوية يمثلون نسبة 33.30%

يشير ذلك إلى ضعف استغلال "القنوات الرقمية الرسمية" في نشر الثقافة الأمنية. البريد المهني هو أداة العمل الأساسية، وعدم استخدامه للتوعية يعد هدراً لفرص وقائية هامة.

الجدول رقم (15): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يعتقدون أن التدريب الذي تلقيته إن وجد كافٍ للتعامل مع التهديدات الرقمية الحالية؟

هل تعتقد أن التدريب الذي تلقيته إن وجد كافٍ للتعامل مع التهديدات الرقمية الحالية؟	التكرار	النسبة المئوية (%)
نعم	8	33.30
لا	16	66.70
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

يرى 66.70% أن التدريب الذي تلقوه (إن وجد) غير كافٍ للتعامل مع التهديدات الحالية. وفي المقابل نسبة 33.30% يرون عكس ذلك.

تعكس هذه النتيجة شعوراً بالعجز الرقمي أو عدم الثقة في المؤهلات المكتسبة. سوسيولوجياً هذا الشعور يزيد من القلق الوظيفي تجاه التعامل مع التكنولوجيا.

الجدول رقم (16): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يعرفون من هو الشخص أو القسم المسؤول عن الدعم الفني والأمني في الكلية عند وقوع مشكلة؟

هل تعرف من هو الشخص أو القسم المسؤول عن الدعم الفني والأمني في الكلية عند وقوع مشكلة؟	التكرار	النسبة المئوية (%)
نعم	13	54.20
لا	11	45.80
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

نلاحظ ان نسبة 54.20% من المبحوثين يعرفون الجهة المسؤولة عن الدعم الفني، مقابل 45.80% لا يعرفون.

توضح النتائج وجود "خارطة تواصل مهنية" غير مكتملة. نصف الموظفين تقريباً سيواجهون ارتباكاً عند وقوع حادث أمني لعدم معرفة "المرجعية الفنية" التي يجب اللجوء إليها.

الجدول رقم (17): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يقومون بتغيير كلمة المرور الخاصة بحسابك الأكاديمي بشكل منتظم؟

هل تقوم بتغيير كلمة المرور الخاصة بحسابك الأكاديمي بشكل منتظم؟	التكرار	النسبة المئوية (%)
نعم	09	37.50
لا	15	62.50
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

من خلال الجدول نلاحظ ان 62.50% من العينة لا يقومون بتغيير كلمات مرورهم بشكل منتظم. بينما نسبة 25% يقومون بتغييرها.

يعكس هذا السلوك "الرتابة والتهاون التقني". سوسيولوجياً يميل الموظفون لتبسيط الإجراءات لتفادي النسيان، مما يجعل الحسابات الأكاديمية عرضة للاختراق بسهولة.

الجدول رقم (18): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يتجنبون استخدام وسائط التخزين غير معروفة على أجهزة الكلية usb

هل تتجنب استخدام وسائط التخزين غير معروفة على أجهزة الكلية usb	التكرار	النسبة المئوية (%)
نعم	17	70.80
لا	07	29.20
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

نلاحظ انه يلتزم 70.80% بتجنب وسائط التخزين غير المعروفة. اما من لا يتجنبون يمثلون نسبة 29.20% من العينة.

يظهر هنا وعي وقائي "مادي" مرتفع. سوسيولوجياً ارتبطت مخاطر الفيروسات بالـ USB في الذاكرة الجمعية للموظفين لسنوات، مما خلق سلوكاً وقائياً تلقائياً.

الجدول رقم (19): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يقومون بإغلاق جهاز الكمبيوتر الخاص بك أو تسجيل الخروج عند مغادرة المكتب؟

هل تقوم بإغلاق جهاز الكمبيوتر الخاص بك أو تسجيل الخروج عند مغادرة المكتب؟	التكرار	النسبة المئوية (%)
نعم	23	95.80
لا	01	04.20
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

التزام شبه تام بنسبة 95.80% بإغلاق الأجهزة أو تسجيل الخروج عند مغادرة المكاتب. وتبقى نسبة 04.20% لا يقومون بذلك.

يعكس هذا السلوك ارتباط الأمن بالحيز المكاني. الموظف يرى أن حماية الجهاز تبدأ من غلقه فيزيائياً، وهو ما ينم عن انضباط مهني عالٍ في التعامل مع الأجهزة كعهدة مادية.

الجدول رقم (20): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يتأكدون من هوية المرسل قبل فتح أي مرفقات في البريد الإلكتروني؟

هل تتأكد من هوية المرسل قبل فتح أي مرفقات في البريد الإلكتروني؟	التكرار	النسبة المئوية (%)
نعم	18	75
لا	06	25
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

نلاحظ ان ثلاثة أرباع العينة أي 75% يتأكدون من هوية المرسل قبل فتح المرفقات. بينما 25% منهم لا يتأكدون.

يشير هذا إلى وجود "حذر رقمي" جيد لدى الموظفين. سوسيولوجياً يعكس ذلك تنامي الوعي بمخاطر الاختراقات عبر الهندسة الاجتماعية والبريد الاحتيالي.

الجدول رقم (21): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يستخدمون برامج حماية مفعلة على جهازك المكتبي؟

هل تستخدم برامج حماية مفعلة على جهازك المكتبي؟	التكرار	النسبة المئوية (%)
نعم	16	66.70
لا	08	33.30
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

عند قراءة الجدول نلاحظ ان 66.70% من العينة يستخدمون برامج حماية مفعلة على أجهزتهم. بينما 25% منهم لا يستخدمونها.

تعكس النسبة ثقة الموظفين في "الحماية البرمجية". اجتماعياً قد يعتمد الموظفون على هذه البرامج كدرع تقني يعوض نقص خبراتهم الأمنية الذاتية.

الجدول رقم (22): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يتجنبون الدخول إلى المواقع غير الموثوقة أثناء استخدام شبكة الجامعة

هل تتجنب الدخول إلى المواقع غير الموثوقة أثناء استخدام شبكة الجامعة	التكرار	النسبة المئوية (%)
نعم	19	79.20
لا	05	20.80
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

اجاب عن سؤال تجنب المواقع غير الموثوقة أثناء استخدام شبكة الجامعة 79.20% بنعم بينما اجاب 20.80% لا.

يعكس هذا السلوك "احترام الملكية العامة" والالتزام بأخلاقيات العمل. الموظف يدرك أن استخدام شبكة الجامعة يتطلب رقابة ذاتية على سلوكه التصفحي.

الجدول رقم (23): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يفرقون بين البيانات العامة والبيانات السرية (مثل نتائج الطلبة) عند التعامل معها رقمياً؟

هل تفرق بين البيانات العامة والبيانات السرية (مثل نتائج الطلبة) عند التعامل معها رقمياً؟	التكرار	النسبة المئوية (%)
نعم	21	87.50
لا	03	12.50
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

أغلبية ساحقة بنسبة 87.50% من العينة تفرق بين أنواع البيانات (مثل نتائج الطلبة) وتبقى نسبة 12.50% لا تفرق بين أنواع البيانات.

يعكس هذا التصرف الوعي المهني والأخلاقي. اجتماعياً تُصنف نتائج الطلبة كأمانة في العرف الأكاديمي، وهذا الوازع الأخلاقي انتقل بنجاح إلى التعامل الرقمي.

الجدول رقم (24): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يعتقدون أن ثقافة الحفاظ على السرية داخل الكلية تساهم في تقليل الاختراقات؟

هل تعتقد أن ثقافة الحفاظ على السرية داخل الكلية تساهم في تقليل الاختراقات؟	التكرار	النسبة المئوية (%)
نعم	21	87.50
لا	03	12.50
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

عند ملاحظتنا للجدول نجد انه يؤمن 87.50% أن ثقافة السرية تساهم في تقليل الاختراقات. بينما 12.50% من العينة يرون عكس ذلك.

يظهر هنا إيمان جمعي بدور الثقافة التنظيمية في الحماية. سوسيولوجياً هذا الوعي موجود كقيمة، لكنه يحتاج إلى تفعيل إداري وتقني.

الجدول رقم (25): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يشعرون بالقلق من تزايد التهديدات الرقمية التي قد تستهدف بيانات الكلية؟

هل تشعر بالقلق من تزايد التهديدات الرقمية التي قد تستهدف بيانات الكلية؟	التكرار	النسبة المئوية (%)
نعم	14	58.30
لا	10	41.70
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

يشعر 58.30% من عينة الدراسة بالقلق من التهديدات التي تستهدف بيانات الكلية. و41.70% لا يشعرون بالقلق.

القلق هو انعكاس الشعور بالمخاطرة في المجتمع الرقمي، هذا القلق سوسيولوجياً هو إيجابي لأنه قد يكون محفزاً للتعلم والالتزام بالإجراءات الأمنية.

الجدول رقم (26): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يلتزمون بالتعليمات الأمنية الصادرة عن الجامعة حتى لو كانت تبطئ من سرعة إنجاز عملك؟

هل تلتزم بالتعليمات الأمنية الصادرة عن الجامعة حتى لو كانت تبطئ من سرعة إنجاز عملك؟	التكرار	النسبة المئوية (%)
نعم	21	78.50
لا	03	21.50
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

يؤكد 78.50% من العينة التزامهم بالتعليمات الأمنية حتى لو أدت لبطء إنجاز العمل. بينما من اجابوا بعدم الالتزام نسبتهم 21.50%

تعكس هذه النسبة تقديم "قيمة الأمن" على "قيمة السرعة". سوسيولوجياً هذا يدل على ولاء وظيفي وإدراك بأن التبعات الأمنية أسوأ من التأخر الإداري.

الجدول رقم (27): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يؤمنون بأن الأمن السيبراني هو مسؤولية كل موظف وليس تقنيي الإعلام الآلي فقط؟

هل تؤمن بأن الأمن السيبراني هو مسؤولية كل موظف وليس تقنيي الإعلام الآلي فقط؟	التكرار	النسبة المئوية (%)
نعم	20	83.30
لا	04	16.70
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

يؤمن 83.30% أن الأمن مسؤولية الجميع وليس التقنيين فقط. في حين تبقى ما لا يرونه مسؤولية الجميع ممثلين في نسبة 16.70%

تشير هذه النتيجة إلى نضج في "المواطنة التنظيمية الرقمية". وتحطم هذه القيمة النظرة التقليدية التي تضع العبء على أهل الاختصاص فقط، وتوزع المسؤولية اجتماعياً على الكل.

الجدول رقم (28): يوضح توزيع العينة حسب رأيهم ما إذا كانوا يروون أن الثقافة السائدة في الكلية تشجع على التحول الرقمي الآمن؟

هل ترى أن الثقافة السائدة في الكلية تشجع على التحول الرقمي الآمن؟	التكرار	النسبة المئوية (%)
نعم	13	54.20
لا	11	45.80
المجموع	24	100

المصدر: من اعداد الطالبة بالإستعانة ببرنامج Excel و Spss

يرى 54.20% من أفراد العينة أن الثقافة السائدة تشجع على التحول الرقمي الآمن، مقابل 45.80% لا يروون ذلك.

تعكس هذه النسبة "انقساماً في الرؤية التنظيمية". نصف الموظفين تقريباً يرى البيئة محفزة، والنصف الآخر يراها محبطة أو غير مهيأة، مما يتطلب عملاً سوسيولوجياً لتجانس الرؤى داخل الكلية.

بناءً على المعطيات الإحصائية المفرغة من الاستبيان (عينة مكونة من 24 موظفاً)، وفي إطار الإشكالية المطروحة حول دور الثقافة التنظيمية في تعزيز الأمن السيبراني داخل كلية العلوم الإنسانية والاجتماعية جامعة زيان عاشور، نقدم لكم عرضاً وتحليلاً ومناقشة شاملة للفرضيات، وصولاً إلى التوصيات:

أولاً: الخصائص السوسيوديموغرافية والمهنية لعينة الدراسة:

قبل الدخول في اختبار الفرضيات، من الضروري فهم طبيعة العينة التي تم استجوابها:

الجنس: يطغى على العينة العنصر الذكوري بنسبة 83.30% (20 موظفاً) مقابل 16.70% للإناث.

السن والخبرة المهنية: تمتاز العينة بنضج عمري ومهني كبير؛ حيث إن 62.50% تتجاوز أعمارهم 41 سنة، وبنفس النسبة (62.50%) يملكون خبرة مهنية تفوق 10 سنوات. هذا يعني أننا نتعامل مع فئة مستقرة وظيفياً وتواكب الإدارة التقليدية والحديثة.

المنصب الوظيفي: تتوزع العينة على مناصب إدارية مختلفة، أبرزها رؤساء المصالح بنسبة 37.50%، ووظائف إدارية أخرى بنسبة 41.7%، مع ندرة المتخصصين التقنيين (تقني سامي في الإعلام الآلي بنسبة 4.20% فقط.

ثانياً: عرض وتحليل الفرضيات الجزئية ومناقشتها

1.عرض وتحليل الفرضية الجزئية الأولى

***نص الفرضية:** "يؤثر مستوى الثقافة التنظيمية السائدة داخل الكلية في درجة الالتزام بممارسات الأمن السيبراني."

لتحليل هذه الفرضية، نربط بين المؤشرات الثقافية التنظيمية (اللوائح، الأولويات، والوعي الجماعي) وبين السلوكيات التطبيقية للموظفين:

- الجانب التنظيمي الرسمي (البيئة الثقافية): تظهر النتائج تبايناً حاداً؛ فرغم وجود تعليمات واضحة تحظر مشاركة كلمات المرور بنسبة 62.50% (الجدول 17)، إلا أن 58.30% يؤكدون غياب ميثاق أو وثيقة مكتوبة تحدد مسؤولياتهم الرقمية (الجدول 10). والأخطر من ذلك، أن 66.70% من الموظفين يشعرون بأن إدارة الكلية لا تضع الأمن السيبراني ضمن أولوياتها الإدارية (الجدول 07).

- **الالتـزام بممارسـات الأمـن السـلوكي:** علـى النقـيض مـن ضـعف الاهتمـام الإداري، أظهـر الموظفون سلوكيات حمائية ذاتية عالية جداً:

95.80% يقومون بإغلاق حواسيبهم أو تسجيل الخروج عند مغادرة المكتب (الجدول 19).

87.50% يفرقون تماماً بين البيانات العامة والسرية (مثل نتائج الطلبة) (الجدول 23).

79.20% يتجنبون المواقع غير الموثوقة عبر شبكة الجامعة (الجدول 22).

75% يتأكدون من هوية المرسل قبل فتح المرفقات(الجدول 20).

70.80% يتجنبون وسائط التخزين (USB) غير المعروفة (الجدول 18)

78.50% يلتزمون بالتعليمات الأمنية حتى لو أبطأت عملهم (الجدول 26).

مناقشة الفرضية الأولى:

النتائج تقودنا إلى ملمح سوسيولوجي مثير للاهتمام: مستوى الالتزام بممارسات الأمن السيبراني مرتفع جداً لدى الأفراد، لكنه لا يعود إلى ثقافة تنظيمية مؤسساتية موجهة من الإدارة، بل ينبع من "ثقافة مهنية ذاتية" وحرص شخصي من الموظفين. فالموظف يدرك قيمة "السرية" (حيث يرى 87.50% أن ثقافة السرية تقلل الاختراقات) (الجدول 24)، ويمارس الحماية بشكل تلقائي (الخروج من النظام، فحص المرسل)، بالرغم من أن الإدارة مقصرة في مأسسة هذه الثقافة (غياب الميثاق المكتوب، وضعف الشعور بأولوية الأمن لدى القيادة).

وبالتالي، تتحقق الفرضية جزئياً؛ فالثقافة السائدة كقيم "أخلاقية مهنية" تؤثر إيجاباً، بينما الثقافة التنظيمية "الإدارية" لا تزال بحاجة إلى تفعيل وضبط.

2.عرض وتحليل الفرضية الجزئية الثانية:

نـص الفرضية: "يساهم التدريب والتوعية في مجال الأمن السيبراني في الحد من المخاطر الرقمية داخل الكلية."

نبحث هنا في حجم التدريب والتوعية المقدمين، ومدى انعكاسهما على وعي الموظفين بالمخاطر:

واقـع التـدريب والتوعيـة الرقميـة: تشير الأرقام إلى عجز واضح في المنظومة الاتصالية والتأهيلية للكلية:

75% من الموظفين لم يسبق لهم المشاركة في أي دورة تدريبية حول حماية البيانات داخل الجامعة (الجدول 12).

66.70 يرون أن إدارة الكلية لا تحرص على توعيتهم بشكل دوري بمخاطر الإنترنت (الجدول 05).

66.70% لا تصلهم رسائل توعوية عبر البريد الإلكتروني المهني (الجدول 14).

79.20% يؤكدون غياب الملصقات الإرشادية في أروقة الكلية (الجدول 13).

79.20% يشيرون إلى أن الكلية لا تشجعهم على تقديم مقترحات لتحسين الأداء الأمني (الجدول 11).

انعكاس ذلك على التهديدات والمخاطر: نتيجة لهذا النقص المعرفي والتوعوي، يظهر الخلل في نقطتين حساسين:

62.50% من الموظفين لا يقومون بتغيير كلمات المرور الخاصة بحساباتهم الأكاديمية بشكل منتظم (الجدول 17). وهو سلوك تقني يحتاج لتوعية مستمرة.

66.70% يقرون بأن التدريب الذي تلقوه (إن وُجد) غير كافٍ للتعامل مع التهديدات الحالية (الجدول 15). كما أن 58.30% يعيشون حالة قلق مستمر من تزايد التهديدات الرقمية (الجدول 25).

مناقشة الفرضية الثانية:

تثبت المعطيات صحة هذه الفرضية بطريقة عكسية؛ فغياب التدريب (75%) وضعف التوعية الدورية (66.70%)، أدى مباشرة إلى إضعاف بعض السلوكيات الحمائية الحيوية مثل إهمال تغيير كلمات المرور بانتظام بنسبة 62.50%، وتوليد شعور عام بعدم الكفاءة الرقمية والقلق من الاختراقات. لو كان هناك تدريب وتوعية ممنهجة، لساهم ذلك مباشرة في ردم الفجوة الأمنية (الحد من المخاطر)، وتجاوز العشوائية في التعامل مع الحسابات المهنية.

ثالثاً: عرض وتحليل ومناقشة الفرضية العامة

نص الفرضية العامة: توجد علاقة ذات دلالة إحصائية بين نمط الثقافة التنظيمية السائد ومستوى تعزيز الأمن السيبراني في الكلية.

من خلال دمج نتائج الفرضيتين الجزئيتين، يمكننا صياغة القراءة الشاملة التالية:

يتضح أن نمط الثقافة التنظيمية السائد حالياً في الكلية هو نمط بيروقراطي تقليدي/ دفاعي وليس نمطاً رقمياً استباقياً.

المؤشر الإيجابي في العلاقة: هناك وعي قيمي جماعي قوي جداً؛ فـ 83.30% من الموظفين يؤمنون بأن الأمن السيبراني هو مسؤولية كل موظف وليس تقنيي الإعلام الآلي فقط. هذا الأساس الثقافي البشري هو الذي يحمي الكلية حالياً، ويتجلى في حرصهم على النسخ الاحتياطي (حيث يؤكد 75% توفره)، والحفاظ على السرية.

المؤشر السلبي في العلاقة: هذا النمط الثقافي التقليدي للإدارة يمارس التعتيم والمركزية؛ حيث إن 54.20% من الموظفين يذكرون أنه لا يتم إبلاغهم فوراً في حال اكتشاف محاولة اختراق. كما أن الإدارة لا تستثمر في هذا الاستعداد البشري عبر التدريب أو التشجيع على المقترحات.

الاستنتاج العام:

الفرضية العامة محققة وثابتة. فالنمط الثقافي التنظيمي يؤثر بشكل مباشر على مستوى تعزيز الأمن. الثقافة الذاتية الإيجابية للموظفين عززت الأمن السلوكي (إغلاق الأجهزة، فرز البيانات)، بينما الثقافة الإدارية السلبية (ضعف الاتصال، غياب التدريب والتوعية) أضعفت الأمن التقني والهيكلي للكلية (ثبات كلمات المرور، القلق الرقمي، غياب المواثيق). الأمن السيبراني منظومة متكاملة (بشر، تكنولوجيا، سياسات)، والخلل الثقافي التنظيمي يعطل تلاحم هذه المنظومة.

رابعاً: مناقشة عامة للنتائج

تؤكد هذه الدراسة في كليات العلوم الإنسانية والاجتماعية حقيقة سوسيولوجية هامة:
*التكنولوجيا لا تحمي نفسها، والإنسان هو الحلقة الأقوى أو الأضعف في سلسلة الأمن الرقمي.
تمتلك الكلية رأسمال بشرياً واعياً ومسؤولاً (أغلبهم ذو خبرة تفوق 10 سنوات)، يقدس سرية العمل الإداري والبيداغوجي. ولكن تقع المنظومة تحت تهديد الفجوة التنظيمية الرقمية؛ فالإدارة

لا تزال تتعامل مع الأمن السيبراني كأمر ثانوي أو تقني بحت يخص مهندس الإعلام الآلي وحده عند حدوث مشكلة.

*إن غياب أدوات الاتصال الأمني الداخلي (الملصقات، بريد التوعية، ورش التدريب) يجعل الموظف يواجه التهديدات المعقدة والمتطورة بناءً على اجتهاده الشخصي فقط، وهو ما يفسر شعور الغالبية 66.70% بأن التدريب غير كافٍ.

خامساً: توصيات واقتراحات

بناءً على التشخيص الإحصائي السابق، نقترح حزمة من الإجراءات العملية لتعزيز الثقافة التنظيمية الرقمية داخل الكلية:

1. **مأسسة الأمن السيبراني:** صياغة ميثاق استخدام رقمي مكتوب وملزم يوزع على كافة الموظفين ويحدد بوضوح مسؤولياتهم، حقوقهم، والخطوات الواجب اتباعها عند رصد أي خطر.

2. **أنسنة التدريب والتعليم المستمر:** تنظيم دورات تدريبية دورية ومكثفة (مستهدفة نسبة الـ 75% غير المدربة)، تركز على المهارات السلوكية التقنية مثل: الإدارة الآمنة لكلمات المرور وتحديثها، والتعرف على هجمات الهندسة الاجتماعية والروابط الخبيثة.

3. **تفعيل الاتصال التوعوي الداخلي:** إطلاق حملات توعية دورية عبر البريد الإلكتروني المهني (إرسال نصائح أسبوعية قصيرة ونشر ملصقات إرشادية في أروقة الكلية ومكاتب الإدارة لتذكير الموظفين بالقواعد الأساسية.

4. **تعزيز الشفافية وبناء الثقة:** اعتماد سياسة الإبلاغ الفوري والشفاف للموظفين في حال وجود أي ثغرات أو محاولات اختراق لأنظمة الجامعة، لرفع درجة اليقظة الجماعية.

5. **التحول نحو الإدارة التشاركية:** فتح قنوات لاستقبال مقترحات الموظفين لتحسين الأداء الرقمي، وتثمين مبادراتهم، مما يشعرهم بأنهم شركاء حقيقيون في حماية أصول الكلية.

6. **تفعيل آليات الإلزام البرمجي:** لتعويض النقص في التغيير الطوعي لكلمات المرور، يُقترح فرض تحديث دوري إجباري (كل 3 أشهر مثلاً) لجميع الحسابات الأكاديمية للموظفين.

خاتمة الدراسة

في ختام هاته الدراسة، يمكن القول إن التحول الرقمي الشامل الذي تشهده المؤسسات الجامعية، قد نقل معركة الحفاظ على أمن المعلومات من أروقة المختبرات التقنية ومكاتب مهندسي البرمجيات إلى عمق البنية السوسيولوجية والثقافية للمؤسسة. لقد أثبتت هذه الدراسة أن الأمن السيبراني لم يعد مجرد مسألة أجهزة وبرمجيات (Hardware and Software) ، بل هو في مقامه الأول مسألة عنصر بشري وثقافة تنظيمية (Human Element and Organizational Culture). فمهما بلغت جدران الحماية الرقمية من التعقيد، فإنها تظل عاجزة عن صد التهديدات ما لم تكن مسنودة بوعي سليم وسلوك أمني مسؤول يتبناه الفاعلون الإداريون والأكاديميون كجزء لا يتجزأ من هويتهم المهنية اليومية.

لقد كشفت المعالجة السوسيولوجية لثقافة أمن المعلومات في البيئة الأكاديمية أن التحدي الأكبر لا يكمن في غياب التشريعات أو نقص الوسائل التقنية، بل في الفجوة السلوكية والمعرفية التي تجعل من الفرد الحلقة الأضعف وأحياناً المخترق غير المتعمد لأنظمة المعلومات.

إن البيئة الجامعية بطبيعتها المفتوحة والتشاركية تتطلب نموذجاً أمنياً فريداً؛ نموذجاً لا يقوم على القيود الفوقية الصارمة التي قد تعيق العمل البيداغوجي، بل يقوم على التنظيم الذاتي النابع من قيم ومعتقدات مشتركة تشكل في مجموعها ثقافة أمن المعلومات. هذه الثقافة هي التي تحول إجراءات السلامة الرقمية من مجرد تعليمات جافة ومفروضة إلى ممارسات تلقائية واعية تحمي النتاج العلمي، وبيانات الطلبة، والخصوصية المؤسساتية.

وعلى الرغم من أن مفهوم ثقافة أمن المعلومات ما زال يواجه تحديات مفاهيمية لكونه يقع في نقطة التقاطع بين الأنظمة الاجتماعية والأنظمة التكنولوجية (Socio-Technical Systems)، إلا أن هذه الدراسة تؤصل لضرورة تبني هذا المفهوم كأداة استراتيجية لإدارة المخاطر. إن تجديد الأنشطة الإدارية ومواكبة التهديدات الرقمية المتسارعة لن يكتب له النجاح إلا من خلال الاستثمار في العقلية التنظيمية، وبناء مناخ يدمج الحس الأمني ضمن القيم المحورية للمؤسسة الجامعية.

إن الأمن السيبراني في الجامعة هو مسؤولية جماعية تبدأ من قناعة الفرد وتنتهي بحصانة المؤسسة، وتظل الثقافة التنظيمية هي الحاضنة الأساسية والضمانة الأكيدة لاستدامة هذا الأمن في عصر لا يتوقف فيه التطور الرقمي ولا تنام فيه التهديدات.

قائمة المصادر والمراجع:

القرآن الكريم:

سورة البقرة ، آية 191

الكتب العربية:

1. أحمد ماهر، ***السلوك التنظيمي مدخل بناء المهارات***، الدار الجامعية، الإسكندرية.
2. إدغار شاين، ***الثقافة التنظيمية والقيادة***، ترجمة عبد الكريم أحمد، دار المريخ للنشر، الرياض، 2012.
3. السعدي محمد وعايشة شريف ، ***منهج البحث العلمي***. الإسكندرية، مصر: دار الهلال العربي 2017
4. القريوتي محمد قاسم, ***السلوك التنظيمي دراسة السلوك الإنساني الفردي والجماعي*** . ط 5,دار وائل , الاردن, 2009
5. تشارلز هاندي، ***فهم المنظمات***، ترجمة محمد عبد الفتاح، دار المريخ للنشر، الرياض، 2011.
6. عبد الرحمن توفيق، ***إدارة أمن المعلومات***، مركز الخبرات المهنية للإدارة، القاهرة، 2016
7. عبد الغني عبد الرحمن، ***السلوك التنظيمي في المنظمات الحديثة***، دار الجامعة الجديدة، الإسكندرية، 2014
8. علي السلمي، ***السلوك التنظيمي في المنظمات المعاصرة***، دار غريب للنشر، القاهرة، 2008.
9. عمار بوحوش ، ***مناهج البحث العلمي وطرق إعداد البحوث***، ديوان المطبوعات الجامعية ، بن عكنون الجزائر ، ط4، 2007
10. محمد حسن عبد الفتاح، ***إدارة الموارد البشرية***، دار المسيرة للنشر والتوزيع، عمان، 2015
11. محمود بري. ***السيبرانية علم القدرة على التواصل والتحكم والسيطرة***. المركز الإسلامي للدراسات الاستراتيجية. ط1. بيروت. لبنان. 2019.
12. يوسف أحمد العلي، ***أساسيات الأمن السيبراني***، دار الفكر العربي، القاهرة، 2019.

المحاضرات:

1. محاضرات حول ***التطور التاريخي للثقافة التنظيمية*** ،جامعة أكلي محند أولحاج، البويرة ,27فيفري 2022

الدراسات والرسائل:

1. عبدالله يحيي سعيد الزهراني ، ***استراتيجيات الأمن السيبراني في ضوء التقنيات والتحديات الحديثة*** ، دراسة مقارنة ، رسالة قدمت لنيل درجة الماجستير في العلوم الإستراتيجية ، جامعة نايف العربية ، للعلوم الأمنية ، كلية العلوم الإستراتيجية قسم الدراسات الاستراتيجية ، السعودية ، عام 2020
2. عبد الرحمن بجاد، ***دور الأمن السيبراني في تعزيز الأمن الانساني***، رسالة ماجستير في العلوم الإستراتيجية، جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية قسم الامن الانساني، السعودية ، عام 2017

المراجع الاجنبية:

1. William Stallings, Cybersecurity and Network Security, Pearson Publishing, 2018.

الملاحق

وزارة التعليم العالي
جامعة زيان عاشور- الجلفة
كلية العلوم الإجتماعية والإنسانية
قسم علم الإجتماع والديموغرافيا

إستمارة إستبيان

عزيزي الموظف / عزيزتي الموظفة بكلية العلوم الانسانية والاجتماعية بجامعة زيان عاشور الجلفة، تحية طيبة وبعد. وفي إطار إعداد دراسة علمية لنيل شهادة الماستر في تخصص علم الاجتماع التنظيم والعمل، نضع بين أيديكم هذا الاستبيان الموسوم بـ:

دور الثقافة التنظيمية في تعزيز الأمن السيبراني داخل المؤسسات الجامعية
دراسة ميدانية في كلية العلوم الانسانية والاجتماعية بجامعة زيان عاشور الجلفة

تعد هذه الدراسة من المواضيع الحيوية والمعاصرة. خاصة مع التحول الرقمي المتسارع الذي تشهده الجامعات الجزائرية. وان اختيارنا لجامعة زيان عاشور وتحديدا كلية العلوم الانسانية والاجتماعية يضيف بعدا هاما للدراسة كون التخصصات الإنسانية غالبا ما تركز على العنصر البشري وهو حلقة مهمة في الأمن السيبراني.

نرجو منكم التكرم بالإجابة على أسئلة الاستبيان بكل موضوعية وصراحة، مع العلم أن:

- المعلومات ستبقى سرية تماماً ولن تُستخدم إلا لأغراض البحث العلمي.
- لا توجد إجابة صحيحة وأخرى خاطئة؛ رأيكم الشخصي هو ما يهمنا.
- لا يتطلب الاستبيان ذكر الاسم واللقب أو أي بيانات تدل على هويتكم.

شاكرين لكم سلفاً سعة صدركم ووقتكم الثمين ومساهمتكم الفعالة في إنجاح هذا العمل العلمي.

ملاحظة: الإجابة تكون بوضع علامة (**X**) أمام الإجابة التي تراها مناسبة.

من اعدد الطالبة: **فاطمة بلخير** تحت إشراف الأستاذ: **جلود رشيد**

الجزء الأول: البيانات العامة

1 -الجنس: ذكر ☐ انثى ☐

2 - العمر: من 20 الى 30 سنة ☐ من 31 الى 40 سنة ☐ من 41 فما فوق ☐

3 -الخبرة المهنية: أقل من سنة ☐ من 1 الى 5 سنوات ☐ من 6 الى 10 سنوات ☐ أكثر من 10 سنوات ☐

4 -المنصب الوظيفي: عميد ☐ نائب عميد ☐ رئيس قسم ☐ مساعد رئيس قسم ☐ رئيس مصلحة ☐ تقني سامي في الإعلام الآلي ☐ وظيفة أخرى ☐

الإجابة تكون بوضع علامة (X) أمام الإجابة التي تراها مناسبة. في حالة الإجابة بـ (نعم) يرجى التوضيح:

الجزء الثاني: الثقافة التنظيمية ودعم الإدارة

1هل تحرص إدارة الكلية على توعية الموظفين بمخاطر استخدام الإنترنت بشكل دوري؟

نعم ☐ لا ☐

التوضيح :

.....

2هل توجد تعليمات واضحة ومعلنة داخل الكلية تحظر مشاركة كلمات المرور الخاصة بالحسابات المهنية؟

نعم ☐ لا ☐

التوضيح:

.....

3هل تشعر أن إدارة الكلية تضع الأمن السيبراني ضمن أولوياتها الإدارية؟

نعم ☐ لا ☐

التوضيح

.....

4هل توفر الكلية نسخاً احتياطية للملفات الإدارية والبيداغوجية الهامة؟

نعم ☐ لا ☐

التوضيح :

.....

5هل يتم إبلاغ الموظفين فوراً في حال اكتشاف أي محاولة اختراق لأنظمة الجامعة؟

نعم ☐ لا ☐

التوضيح :

.....

6هل يوجد ميثاق أو وثيقة مكتوبة تحدد مسؤوليات الموظف تجاه حماية البيانات الرقمية؟

نعم ☐ لا ☐

التوضيح :

.....

7هل تشجع الكلية الموظفين على تقديم مقترحات لتحسين الأداء الرقمي والأمني؟

نعم ☐ لا ☐

التوضيح :

.....

الجزء الثالث: التدريب والتوعية

8هل سبق لك المشاركة في دورة تدريبية حول كيفية حماية البيانات الرقمية داخل الجامعة؟

نعم ☐ لا ☐

التوضيح :

.....

9هل تتوفر في أروقة الكلية أو مكاتبها ملصقات إرشادية حول الأمن السيبراني؟

نعم ☐ لا ☐

التوضيح :

.....

10هل تصلك رسائل توعوية عبر البريد الإلكتروني المهني حول كيفية تجنب الروابط المشبوهة؟

نعم ☐ لا ☐

التوضيح :

.....

11هل تعتقد أن التدريب الذي تلقيته (إن وجد) كافٍ للتعامل مع التهديدات الرقمية الحالية؟

نعم ☐ لا ☐

التوضيح :

.....

12هل تعرف من هو الشخص أو القسم المسؤول عن الدعم الفني والأمني في الكلية عند وقوع مشكلة؟

نعم ☐ لا ☐

التوضيح :

.....

الجزء الرابع: السلوك والممارسات (الأمن السيبراني)

13هل تقوم بتغيير كلمة المرور الخاصة بحسابك الأكاديمي بشكل منتظم؟

نعم ☐ لا ☐

التوضيح :

.....

14هل تتجنب استخدام وسائط التخزين (USB) غير المعروفة على أجهزة الكلية؟

نعم ☐ لا ☐

التوضيح :

.....

15هل تقوم بإغلاق جهاز الكمبيوتر الخاص بك أو تسجيل الخروج عند مغادرة المكتب؟

نعم ☐ لا ☐

التوضيح :

.....

16هل تتأكد من هوية المرسل قبل فتح أي مرفقات في البريد الإلكتروني؟

نعم ☐ لا ☐

التوضيح :

.....

17هل تستخدم برامج حماية (Antivirus) مفعلة على جهازك المكتبي؟

نعم ☐ لا ☐

التوضيح :

.....

18هل تتجنب الدخول إلى المواقع غير الموثوقة أثناء استخدام شبكة الجامعة (Wi-Fi)؟

نعم ☐ لا ☐

التوضيح :

.....

19هل تفرق بين البيانات العامة والبيانات السرية (مثل نتائج الطلبة) عند التعامل معها رقمياً؟

نعم ☐ لا ☐

التوضيح :

.....

الجزء الخامس: التهديدات الرقمية والالتزام

20هل تعتقد أن ثقافة الحفاظ على السرية داخل الكلية تساهم في تقليل الاختراقات؟

نعم ☐ لا ☐

التوضيح :

.....

21هل تشعر بالقلق من تزايد التهديدات الرقمية التي قد تستهدف بيانات الكلية؟

نعم ☐ لا ☐

التوضيح :

.....

22هل تلتزم بالتعليمات الأمنية الصادرة عن الجامعة حتى لو كانت تبطئ من سرعة إنجاز عملك؟

نعم ☐ لا ☐

التوضيح :

.....

23هل تؤمن بأن الأمن السيبراني هو مسؤولية كل موظف وليس تقنيي الإعلام الآلي فقط؟

نعم ☐ لا ☐

التوضيح :

.....

24هل ترى أن الثقافة السائدة في الكلية تشجع على التحول الرقمي الآمن؟

نعم ☐ لا ☐

التوضيح :

.....

الهيكل التنظيمي لكلية العلوم الإجتماعية والإنسانية بجامعة زيان عاشور الجلفة