الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي
جامعة أكلي محند أولحاج
-البويرة-
كلية العلوم الإجتماعية والإنسانية

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira -
Tasdawit Akli Muḥend Ulḥağ - Tubirett -
Faculté des Sciences Sociales et Humaines

قسم: علوم الاعلام والاتصال

الموضوع:

متطلبات تحقيق الأمن السيبراني في أنظمة المعلومات الادارية

"دراسة حالة جامعة اكلي محند أولحاج – البويرة- "

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في علوم الاعلام و الاتصال

تخصص: اتصال و علاقات عامة

من إعداد الطلبة:

- **بغدالي آسيا**
- **لعقاب أسامة**
- **مشنان سيليا**

إشراف الأستاذة:

- **د/ جميلة اوشن**

السنة الجامعية: 2023/2022

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي
جامعة أكلي محند أولحاج - البويرة

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj, Bouira
Tasdawit Akli Muhend Ulhaj Tubirett

التصريح الشرفي الخاص بالالتزام بقواعد النزاهة العلمية

انا الممضي اسفله،

السيد(ة) حشنان يسيليا الصفة: طالب (ماستر / دكتوراه)

الحامل(ة) لبطاقة التعريف الوطنية: 1054...0 والصادرة بتاريخ 05/04/2016

المسجل(ة) بكلية / معهد العلوم الانسانية والاجتماعية قسم علوم الاعلام والاتصال

تخصص: اتصال وعلاقات عامة

والمكلف(ة) بإنجاز اعمال بحث(مذكرة. التخرج، مذكرة ماستر. مذكرة ماجستير. اطروحة دكتوراه).

عنوانها: متطلبات تحقيق الامن السيبراني في نظم المعلومات الجامعية

دراسة بجامعة البويرة

أصرح بشرفي اني ألتزم بمراعاة المعايير العلمية والمنهجية الاخلاقيات المهنية والنزاهة الاكاديمية المطلوبة في انجاز البحث المذكور أعلاه.

التاريخ: 13/06/2023

توقيع المعني (ة)

هيئة مراقبة السرقة العلمية:

النسبة: % 04

البويرة في: 26 JUIN 2023

الامضاء

الجمهورية الجزائرية الديمقراطية الشعبية
جامعة البويرة
مديرية الدراسات و المسائل المرتبطة بالطلبة
العلوم الاجتماعية

د. خالدي مصطفى
مصطفى بوهام نائب العميد
للدراسات و المسائل المرتبطة بالطلبة

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي
جامعة أكلي محند أولحاج - البويرة

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj, Bouira
Tandami Akli Mohand (Hind) Tinzirt

التصريح الشرفي الخاص بالالتزام بقواعد النزاهة العلمية

02

انا الممضي اسفله،

السيد(ة) ..... الصفة: طالب (ماستر / دكتوراه)

الحامل(ة) لبطاقة التعريف الوطنية: ..... والصادرة بتاريخ .....

المسجل(ة) بكلية / معهد ..... قسم .....

تخصص: .....

والمكلف(ة) بإنجاز اعمال بحث(مذكرة. التخرج، مذكرة ماستر. مذكرة ماجستير. أطروحة دكتوراه).

عنوانها: .....

.....

أصرح بشرفي اني ألتزم بمراعاة المعايير العلمية والمنهجية الاخلاقيات المهنية والنزاهة الاكاديمية المطلوبة في انجاز البحث المذكور أعلاه.

التاريخ ..... توقيع المعني (ة)

هيئة مراقبة السرقة العلمية:

النسبة: % 04

البويرة في ..... الامضاء

نائب العميد للدراسات والعلاقات الخارجية والتعاون والتظاهرات العلمية
للدراسات والوسائل المرتبطة بالطلبة

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire

وزارة التعليم العالي و البحث العلمي
جامعة أكلي محند أولحاج - البويرة

Ministère de l'Enseignement Supérieur
et de la Recherche Scientifique
Université Akli Mohand Oulhadj - Bouira
Tasdawit Akli Muḥend Ulḥağ - Tubirett

التصريح الشرفي الخاص بالالتزام بقواعد النزاهة العلمية

انا الممضي اسفله،

السيد(ة) لحقاب اسماعيل الصفة: طالب (ماستر / دكتوراه)

الحامل(ة) لبطاقة التعريف الوطنية: 109236085 والصادرة بتاريخ 2017/04/05

المسجل(ة) بكلية / معهد العلوم الإنسانية والعلوم الإسلامية قسم علوم الإعلام والاتصال

تخصص: اتصال وعلاقات عامة

والمكلف(ة) بإنجاز اعمال بحث(مذكرة. التخرج، مذكرة ماستر. مذكرة ماجستير. اطروحة دكتوراه).

عنوانها: صناعة الإشاعة وتحقيق الأمن السيبراني في الأوساط الجامعية

الجزائرية جامعة آكلي محند أولحاج - البويرة -

أصرح بشرفي اني ألتزم بمراعاة المعايير العلمية والمنهجية الاخلاقيات المهنية والنزاهة الاكاديمية المطلوبة في انجاز البحث المذكور أعلاه.

التاريخ: 13/06/2023

توقيع المعني(ة)

هيئة مراقبة السرقة العلمية:

النسبة: 04 %

البويرة في: 26 JUIN 2023

الامضاء

جامعة البويرة
نيابة العمادة للدراسات و المسائل المرتبطة بالتكوين
كلية العلوم الإجتماعية

د. خالدي مصطفى
مكلف بمهام نائب العميد
للدراسات و المسائل المرتبطة بالتكوين

الشكر والعرفان:

قال رسول الله صل الله عليه وسلم :"من لم يشكر الناس لم يشكر الله ومن اهدى إليكم معروفا فكافئوه فإن لم تستطيعوا فادعوا له:" .

عملا بهذا الحديث واعترافا بالجميل، نحمد الله عز وجل ونشكره على أن وفقنا لإتمام هاذا العمل المتواضع .

ونتقدم بالشكر الجزيل الى الاستاذة المشرفة " الدكتورة جميلة اوشن" التي رافقتنا طيلة هذا البحث وامدتنا بالمعلومات والنصائح القيمة راجين من الله عز وجل أن يسدد خطاها ويحقق مناها فجزاها الله عنا كل خير .

كما نتقدم بخالص الشكر والتقدير الى الأساتذة الكرام أعضاء لجنة المناقشة على قبولهم مناقشة مذكرتنا .

كما لا ننسى ان نشكر مهندسي ادارة جامعة البويرة وعلى رأسهم المهندس "حمبلي سفيان" على مساعدتنا في إثراء هذا العمل .

ولا يفوتنا كذلك ان نتوجه بالشكر الجزيل الى كل اساتذة كلية العلوم الإنسانية والاجتماعية بجامعة البويرة خاصة اساتذة قسم علوم الاعلام والاتصال كل باسمه ومقامه .

وفي الاخير لا يفوتنا أن نعبر عن بالغ تحياتنا الى كل من ساهم في إنجاز هذا العمل من قريب أو من بعيد .

الاهداء

ما أجمل أن يجود المرء بأغلى ما لديه والأجمل أن يهدي الغالي للأغلى

هي ثمرة جهدي أجنيها اليوم هي هدية أهديها:

الى من تتسابق الكلمات لتخرج معبرة عن مكنون ذاتها الى الشمس التي انارت دربي ودفأتني بحنانها

الى صاحبة القلب الحنون مالكة الصدر الرحيم ..... أمي الحبيبة.

الى من أحمل اسمه بكل فخر، الى من سهر الليالي الطوال وعارك الأيام الشداد، الى من علمتني تجاربه

أن النجاح لا يكون الا بالتصميم والكفاح والعمل الجاد ..... أبي الغالي .

الى تلك المجموعة القزحية التي لونت حياتي واعطتها لونا وطعما جميلين، الى القلوب الطاهرة والنفوس البريئة

الى من تقاسمت معهم هموم الحياة وحلوها ..... اخوتي وأخواتي.

الى من حبهم يجري في عروقي الى رياحين حياتي ..... كتاكيت العائلة "ميسم، عبد الباسط،

رمزي، عبد النور

الى من بصحبتهم تعلمت أن الدنيا مهما قست علينا لها وجهها المشرق، الى من علموني أن الوفاء لا يكون

الا في الصديق، الى من يسكنون بجوار قلبي ..... أصدقائي الأعزاء .

الى استاذتي الفاضلة "الدكتورة جميلة أوشن" لكي خالص الشكر والتقدير.

الى من علمونا حرفا من ذهب وكلمات من درر وعبارات من أسمى وأجلى العبارات في العلم

الى من صاغوا لنا من علمهم حروفا ومن فكرهم منارة تنير لنا سيرة العلم والنجاح

الى اساتذتي الكرام في جميع الأطوار.

الى زميلي في هذا العمل ..... مشنان سيليا ولعقاب أسامة .

الى كل زملائي طيلة المشوار الدراسي، الى كل طلبة علوم الاعلام والاتصال.

الى كل الأرواح الغالية التي فارقتنا يوما واحزننا رحيلهم، الى من مزقوا قلوبنا بفراقهم، الى من تركوا

في حياتنا ثغرة لا يملؤها سواهم ..... رحمكم الله واسكنهم فسيح جناته.

الى كل من وسعتهم ذاكرتي ولم تسعهم مذكرتي .

آسيا

الاهداء

الحمد لله رب العالمين والصلاة والسلام على أشرف المرسلين سيدنا محمد و

على آله وصحبه ومن اتبعهم الى يوم الدين

اهدي ثمرة جهدي المتواضع

الى من بلغ الرسالة وأدى الأمانة النبي محمد صلى الله عليه وسلم .

الى من لا يمكن للكلمات أن توفي حقها ، كانت ولا زالت وستظل في قلوبنا

في كل مسافة لك ذكرى، ومع كل حبة رمل لك ذكرى،

وبكل قطرة مطر لك في قلوبنا أجمل ذكرى..... جدتي رحمها الله.

الى التي حملتني في بطنها وغمرتني بحبها وسهرت الليالي لراحتي..... أمي الحنونة .

إلى أمي الثانية التي لم تنجبني ... حبيبة قلبي .... خالتي نادية

الى الذي ربانى على الإيمان وانار لي درب العلم والإحسان، الى الذي زرع في نفسي أجمل المبادئ

الى الذي وضع كل ثقته في..... أبي الغالي.

إلى أبي الثاني.. وسند ظهري.. وعمود قلبي.. خالي جلول

الى من حبهم يجري في عروقي ويلهج بذكرهم فؤادي..... أختاي "كهينة وأمينة" حفظهم الله ورعاهم .

الى من عروقهم متصلة بقلبي لا يحلو النبض الا بهم ..خالتي "دنيا وسعاد"

الى زوجي وسندي في الحياة..... مشنان حسين .

الى من عرفني بهم القدر وتقاسمنا حلو الحياة ومرها ..... أصدقائي الأعزاء .

الى الاستاذة الفاضلة" الدكتورة جميلة اوشن" لكي كل الشكر والامتنان .

الى كل الزملاء والزميلات الذين تقاسمنا معهم لذة الفرح والنجاح وأخص بالذكر بغدالي آسيا ولعقاب أسامة .

الى كل من يحبونني .

الى كل من نسيهم قلمنا ولم ينساهم قلبنا .

سيليا

إهداء

خريج 2023

الحمد لله الذي بنعمته تتم الصالحات

"وَآخِرُ دَعْوَاهُمْ أَنِ الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ" سورة يونس، الآية 10 -

اللّهم كمّا أنعمّت فَزِدْ وكما زدتّ فَبارك وكما باركتَ فَتمّمْ وكما اتممت فثبّت

اللهم ليس بجهدي واجتهادي وإنما بتوفيقك وبركتك علي فالحمد لله عند البدء وعند الختام

لقد كانَ الحُلمَ يوسُفيَّ الطُموح يعقوبيَّ المَشقة

...نحنُ لها وان أبت رُغماً عَنها اتينا بها

ابي الغالي إلى من رفعت وأرفع به رأسي عالياً افتخاراً به.. الذي لم يكن يوماً رجلاً عادياً، شكرا لانك كنت حليما ..

رحيما حنونا واثقا

إلى امي حبيبتي التي حملتني على أكفِ الراحة فلازمتني دعواتها منذ بدأت وإلى الآن وبعد الآن وإلى الأبد، إلى التي أغمضت عيناي عن

التي رأتني بقلبها قبل عينيها ... إلى شجرتي التي لا كل المحبطات والفشل، وأحتضنتني بقوة حتى لا تنفذ طاقتي، إلى جنتي أمي

إلى جدتي العزيزة ?تذبل.. إلى الظل الذي آوي إليه في كل حين إليك

الى من لم اشبع من انفاسه وورا ثيناه الثرى .... روح أخي الغالي وقرة عيني خالد رحمه الله

لإخواني الأعزاء نصر الدين، رضا، شريف سندي في هذه الحياة في حلوها ومرها

أخواتي الغاليات سعاد، نوال، رتيبة، عفاف كما لا أنسى حلاوة البيت براعم واطفال العائلة

.ما زال للطريق بقية فلا الرحلة ابتدات ولا الدّرب انتهى

شكراً لكل روح عانقتني بالحب والدعوات، لكل من كان سبباً لفرحتي

شكرا إلى من كانت لنا سندا دائم دكتورة اوشن جميلة

لزميلتي مشنان سيليا، بغدالي أسيا ... أهدي هذا النجاح إلى عائلة لعقاب الذين نساهم قلمنا لن ينساهم

قلبنا

الحمد لله حتى يبلغ الحمد منتهاه

لعقاب_أسامة

ملخص

نهدف من خلال هذه الدراسة الى التعرف على متطلبات تحقيق الأمن السبيراني في نظم المعلومات الادارية (جامعة اكلي محمد اولحاج البويرة)، وقد ركزنا على الأمن السبيراني نظرا لأهميته في حماية وتأمين المعلومات والبيانات السرية، اعتمدنا في دراستنا على منهج دراسة حالة مطبقا على عينة قصدية من خلال اداة المقابلة المعمقة، توصلنا من خلال هذه الدراسة الى مجموعة من النتائج اهمها:

1-عدم تحقيق المتطلبات الامن السيبراني بسبب نقص الإمكانيات والخبرة اللازمة لتفعيل هذا النظام الذي لا بد من العمل به لحماية بيانات الجامعة والمعلومات الخاصة بها .

2-لم تراقي بعد الى المستوى المطلوب لتحقيق متطلبات التقنية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الادارية، نظرا الى الصعوبات والعراقيل التي تواجه الموظفين والاداريين، وضرورة تفعل اشتراكات دورية لبعض البرامج الخاصة بالحماية ضد الفيروسات والانشطة المشبوهة، وهناك لميزانية البحث العلمي دورا كبيرا في توفير هذه البرامج، التي يجب توفرها وتزويد الجامعة بأنظمة حماية عالية المستوى لأنظمة المعلومات الادارية.

3-تنفتح مختلف الآراء والأفكار المطروحة حول تعزيز الثقة الرقمية من خلال تواجدها في مختلف الدورات والمؤتمرات الخاصة بهذا المجال .

4- يحقق الأمن السيبراني سرية المعلومات الادارية من خلال إنشاء حسابات آمنة ووضع سياسة امن سيبراني فعالة، وكذلك من خلال ضمان سرية وسلامة وتوافر المعلومات بالإضافة إلى استخدام نظام التشفير وجدار الحماية لتحقيق الحماية الكاملة .

5- يعتلي الامن السبيراني مجموعة من المعوقين التنظيمية والتقنية، وهو ما يحول دون تحقيقه في نظم المعلومات الادارية بجامعة البويرة.

Abstract:

Through this study, we aim to identify the requirements for achieving cybersecurity in administrative information systems (University of Aïn Témouchent - Mohamed Bouguerra) with a focus on cybersecurity due to its importance in protecting and securing confidential information and data. In our study, we adopted a case study approach applied to a purposive sample using the deep interview tool. Through this study, we have reached a set of results, the most important of which are:

1. Failure to achieve cybersecurity requirements due to a lack of resources and necessary expertise to activate this system, which is necessary to protect the university's data and information.
2. The necessary technological requirements for achieving cybersecurity in administrative information systems have not yet been met, due to the difficulties and obstacles faced by employees and administrators. There is a need for regular subscriptions to specific protection programs against viruses and suspicious activities. The research budget plays a significant role in providing these programs, which must be available and equipped with high-level security systems for administrative information systems.
3. Various opinions and ideas have emerged regarding enhancing digital trust through their presence in various courses and conferences related to this field.
4. Cybersecurity ensures the confidentiality of administrative information through the establishment of secure accounts, the implementation of an effective cybersecurity policy, as well as ensuring the confidentiality, integrity, and availability of information. This is achieved through the use of encryption systems and firewalls to achieve comprehensive protection.
5. Cybersecurity faces various organizational and technical obstacles, which prevent its achievement in the administrative information systems at the University of Aïn Témouchent.

مقدمة

منذ ظهور التكنولوجيا الرقمية والثورة المعلوماتية، أصبحت تكنولوجيا المعلومات ضرورة من ضرورات عصرنا الحالي، وباتت أداة إستراتيجية تسهل الوصول إلى الميزة التنافسية الدائمة، ونتيجة لهذه الطفرة الكبيرة التي حدثت في وسائل الاتصالات وشبكات المعلومات والدخول في عصر العولمة والانترنت، برز جانب من جوانب العولمة الذي يتطلب إهتماما كبيرا وهو الأمن السيبراني الذي يشمل جميع الإجراءات والتقنيات التي تهدف إلى حماية البيانات والمعلومات الحساسة من الوصول غير المصرح به والاختراق والتلاعب والتدميز والتهديدات الأمنية المتعلقة بالتكنولوجيا، حيث تعد العولمة وتطور التكنولوجيا مسببين رئيسيين لتزايد التهديدات السيبرانية.

يتعامل الأمن السيبراني مع مجموعة واسعة من المخاطر التي تشمل الاختراقات الإلكترونية والبرمجيات الخبيثة وسرقة الهوية الرقمية وغيرها من الهجمات السيبرانية.

وفي ظل اتصال عالمنا بالأنترنت واندماجها بالبنى التحتية للمؤسسات أصبح الأمن السيبراني ذو أهمية قصوى، وجزء أساسيا من استراتيجية حماية نظم المعلومات الإدارية خاصة في ظل تزايد المعلومات وكثرة الاعتماد عليها، و في ضوء التوسع الكبير في تبادل هذه المعلومات وانتقالها من مكان إلى أخر برز الاهتمام بأمن وسلامة هذه المعلومات والمحافظة على تكاملها وعلى وصولها سليمة للشخص المعني وحده دون غيره [1].

تعد نظم المعلومات الإدارية من بين النظم التي تعتمد على تقنية المعلومات وتكنولوجيا المعلومات لجمع البيانات وتحويلها إلى معلومات قيمة للمدريين وأعضاء الفريق. وتنبع أهميتها وفعالية نظم المعلومات الإدارية من الدور الكبير الذي تلعبه في نجاح المؤسسات بالقدر الذي تتصاعد فيه فاعلية نظم المعلومات الإدارية، تزيد القدرة على إنجاز الوظائف الإدارية بدقة وانتظام، حيث تشكل أداة لتحقيق الميزة التنافسية وحاضنا للمعلومات والبيانات المهمة التي تدعم عمليات اتخاذ القرارات في المؤسسات وتحسين أدائها.[2]

يهدف الأمن السيبراني إلى توفير الحماية اللازمة لشبكات الأنظمة والتطبيقات والبيانات الموجودة في نظم المعلومات الإدارية، ويعد أمرا حيويا في الجامعات نظرا لكمية البيانات الحساسة والمعلومات الشخصية التي يتم تخزينها ومعالجتها هناك، حيث تتعرض الجامعات لتهديدات سيبرانية متنوعة، تشمل الإختراقات

[1]–داود حسن، **أمن شبكات المعلومات**، معهد الإدارة العامة، مركز البحوث، الرياض، 2004، ص37.

[2]–الطائي محمد عبد حسين أل فرج: **نظم المعلومات الإدارية المتقدمة**، دار وائل للنشر والتوزيع، عمان، الأردن، 2004، ص117.

الإلكترونية والبرمجيات الخبيثة وسرقة الهوية والاحتيال الإلكتروني وغيرها من أشكال الهجمات السيبرانية، بهدف الوصول إلى المعلومات الحساسة كالبحوث السرية ومعلومات الطلاب والأعضاء الأكاديميين أو لتعطيل الأنظمة الحاسوبية والشبكات .

وانطلاقا من الأهمية التي احتلها الأمن السيبراني وعلاقته بتوفير الحماية اللازمة لأنظمة المعلومات، تبذل الجامعات جهود معتبرة لحماية نظم معلوماتها الإدارية والرقمية في بيئة التعليم العالي من خلال إجراءات ومتطلبات تسعى لتحقيقها، وهذا ما سنناقشه من خلال هذه الدراسة من حيث التعرف على متطلبات تحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج البويرة، واشتملت الدراسة على قسمين نظري وميداني بالإضافة إلى خاتمة، وتكونت من أربعة فصول عنون الأول بالإطار العام للدراسة وتم فيه تحديد الإشكالية وطرح التساؤلات وأهداف وأهمية الدراسة وأهم أسباب إختيار الموضوع .

كما عرضنا المنهجية المتبعة في هذه الدراسة من حيث المنهج المستخدم وأدوات جمع البيانات والعينة المختارة، إلى جانب عرض مفاهيم الدراسة ومجالاتها، وعرض الدراسات السابقة .

جاء الفصل الأول تحت عنوان تأصيل مفاهيمي لأنظمة المعلومات الإدارية في المؤسسة وتضمن (03) مباحث رئيسية، عنون المبحث الأول: أساسيات عن نظم المعلومات وطبيعة نظم المعلومات، وتناول مفهوم نظم المعلومات وخصائص وموارد وأنواع المعلومات .

عنون المبحث الثاني: مقاربة معرفية حول المعلومات الإدارية وتناول مفهوم نظم المعلومات الإدارية وتطورها وأبعادها وخصائصها ومكوناتها وجاء المبحث الثالث تحت عنوان نظم المعلومات الإدارية وضائفها وأهميتها وتحديات تطبيقها، تناول وظائف وأهمية وتحديات نظم المعلومات الإدارية وأهم المداخل المعاصرة لدراستها.

أما الفصل الثاني تطرقنا فيه إلى الإطار النظري والمفاهيمي للأمن السيبراني، وقسم هو الأخر إلى (03) مباحث رئيسية، عنون المبحث الأول مقاربة معرفية لمفهوم الأمن السيبراني تناول مفهوم الأمن السيبراني ونشأته وخصائصه وأهدافه، وجاء في المبحث الثاني مبادئ الأمن السيبراني وأبعاده وأهميته وتحدياته. وجاء المبحث الثالث عنون بالثقة الرقمية والأمن السيبراني وتناول مفهوم ثقة الرقمية ومتطلبات بناءها ودور الثقة الرقمية في تعزيز الأمن السيبراني .

وأخيرا الجانب التطبيقي الذي خصص للدراسة الميدانية حول متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة البويرة من خلال توزيع دليل المقابلة على بعض الموظفين الإداريين بالجامعة والتي تضمن 5 محاور كالآتي:

*المحور الأول: المتطلبات الإدارية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج البويرة.

*المحور الثاني: المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج البويرة.

*المحور الثالث: أثر الأمن السيبراني في تعزيز الثقة الرقمية بجامعة أكلي محند أولحاج البويرة .

*المحور الرابع: دور الأمن السيبراني في مواجهة نظم المعلومات الإدارية أكلي محند أولحاج البويرة.

*المحور الخامس: معوقات تحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج بالبويرة .

ثم قمنا بتحليل نتائج المقابلة وبتقديم نتائج الدراسة وفي الأخير قدمن خاتمة شملت التوصيات بخصوص موضوع البحث.

العنوان: متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة أكلي محند أولحاج–دراسة حالة جامعة أكلي محند أولحاج البويرة.

الفصل الأول: الإطار العام للدراسة

1–تحديد الإشكالية.

2–تساؤلات الدراسة.

3–أسباب إختيار الموضوع.

4–أهداف الدراسة.

5–أهمية الدراسة.

6–منهج الدراسة وأدواته

7–مجتمع البحث وعينة الدراسة .

8–مجالات الدراسة.

9–تحديد مفاهيم الدراسة.

10–الدراسات السابقة.

1-تحديد الإشكالـــــــــية:

إن الحفاظ على متطلبات الأمن من القضايا والهواجس الكبرى التي اهتمت بها المجتمعات الإنسانية على مر الأزمنة وصولا إلى العصر الحالي الذي اتفق الكثير من المفكرين على تسميته بعصر العولمة .

فلقد أدت الثورة الرقمية المعاصرة إلى إيجاد أفاق غير مسبوقة للتواصل وتبادل المعلومات والأفكار والآراء على كافة مجالات النشاط الإنساني، خاصة مع انتشار الهواتف الذكية والأجهزة الكفية المحمولة أصبحت الشبكة العنكبوتية أمرا متاحا لجميع أفراد المجتمع.

تعد تكنولوجيا المعلومات والاتصالات من أبرز إفرازات الثورة الرقمية التي تطرح نفسها وبقوة في مجال إدارة المؤسسات، أين تتجه هذه الأخيرة اليوم إلى استعمال هذه التكنولوجيات للاستفادة من المزايا التي توفرها فيما يتعلق بتحسين أدائها وربح الوقت في إدارة معلوماتها خصوصا فيما يتعلق بنظم المعلومات الإدارية التي أصبحت تتعامل مع كم هائل من المعلومات في بيئة داخلية متزايدة النمو، وفي وسط خارجي معقد بالكثير من الأبعاد والمتغيرات .

غير أن هذا الاستخدام يحمل الكثير من المخاطر التي قد تؤثر على السير العادي للعمل، وتصاحبه جملة من التهديدات والاعتداءات الإلكترونية التي تلحق أضرارا بالغة بالمؤسسة قد تصل إلى حد التلاعب بمعلوماتها والتخريب الكلي لها، وفي ظل تزايد هذه التهديدات الأمنية في مجال التكنولوجيا الرقمية برز مفهوم الأمن السيبراني كأحد الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية.

يعد الأمن السيبراني من أهم متطلبات استقرار المؤسسات كونه يقوم في الأساس على ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف عادة إلى الوصول للمعلومات الحساسة أو تغييرها أو اتلافها من أي اختراق سيبراني والوصول غير مصرح به للبيانات باعتباره مصدر أمان لجميع الوسائل التكنولوجية .

باتت دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي ذلك تزامنا مع التركيز على مختلف التنظيمات على المعلومات كمصدر للميزة التنافسية، برزت الحاجة إلى الاعتماد على الأمن السيبراني كأحد التطبيقات الأمنية في حماية كل مايتعلق بنظم معلوماتها.

ويتميز قطاع التعليم العالي والبحث العلمي عن القطاعات الأخرى بأنه وزيادة عن سعيه لرقمنته إدارته، فإنه مكلف بالتعليم والتكوين العاليين في مجال الرقمنة والبحث التطوير في هذا المجال .

وتعتبر المؤسسة الجامعية كأحد مؤسسات التعليم العالي في واجهة القاطرة، بل أن الجامعات اليوم هي أكثر المؤسسات التي تتقدم وتتنافس فيما بينها في جميع الوظائف وتسعى إلى إيجاد الحلول لجميع المشاكل التي تعترضها وتوفير الأمن والحماية لنظم معلوماتها الإدارية وجامعة أكلي محند أولحاج بالبويرة من بين هذه الجامعات التي إعتمدت على رقمنة إدراتها قصد تحقيق والعمل بنظم المعلومات الإدارية .

وانطلاقا مما سبق أمككنا طرح الإشكال التالي: **ماهي متطلبات تحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج –البويرة–؟**

2–تساؤلات الدراسة:

2–1ماهي المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج ؟

2–2ماهي المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج –البويرة–؟

2–3كيف يؤثر الأمن السيبراني في تعزيز الثقة الرقمية بجامعة أكلي محند الحاج بالبويرة؟

2–4ماهو دور الأمن السيبراني في مواجهة النظم الإدارية بالجامعة ؟

2–5 ما هي معوقات تحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج البويرة؟

3–أسباب اختيار موضوع الدراسة:

إن اختيار الباحث لموضوع دراسته قد يكون لأسباب واعتبارات كثيرة، ومن أهم الأسباب التي دفعت الباحث لاختيار هذا الموضوع:

-الارتباط المباشر لموضوع الدراسة بتخصصنا باعتبار الأمن السيبراني من إفرازات تكنولوجيا الاعلام والاتصال.

-الرغبة في دراسة الأمن السيبراني والتحديات التي يمثلها ومدى فاعليتها في مواجهة التهديدات السيبرانية .

-دراسة الأمن السيبراني واحدة من مستحدثات التطور التكنولوجي والرقمي الذي نعايشه في العالم مؤخرا .

-دور نظم المعلومات الإدارية في التسيير داخل الجامعة كأحد أليات التعامل مع مختلف المشكلات والتعقيدات .

-التطلع إلى إثراء جانب البحث العلمي.

4-أهداف الدراسة:

لا يستطيع أي باحث أن يقوم بدراسة ظاهرة معينة دون أن يقوم بتحديد جملة من الأهداف التي يسعى للوصول إليها ودراستنا الحالية تهدف إلى:

-محاولة التعرف على المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج البويرة.

-محاولة التعرف على المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج –البويرة–.

– محاولة التعرف على أثر الأمن السيبراني في تعزيز الثقة الرقمية بجامعة أكلي محند أولحاج –البويرة–.

-محاولة التعرف على على دور الأمن السيبراني في مواجهة النظم الإدارية لجامعة أكلي محند أولحاج البويرة.

-محاولة التعرف على معوقات تحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج–البويرة–.

5-أهمية الدراسة:

إن مسايرة التغيرات لابد من ان يتم وفق أليات وإجراءات تحمي الأنظمة والمعلومات، فالأمن في الفضاء السيبراني يعتبر أمرا مهما، لذا بدأت الكثير من المؤسسات الخاصة الأكاديمية منها بتبني وتطبيق أمن المعلومات وممارسة الأمن السيبراني وتوفير متطلباته .

حيث باعتبار الجامعة صانع وناقل للمعرفة فإنها تعتمد على المعلومات والشبكات بشكل متزايد، خاصة في بيئة التعليم الإلكتروني التي فرضتها جائحة كورونا، وهذا الاندفاع المتزايد نحو توظيف الانترنت والأجهزة والشبكات في العمل الإداري والأكاديمي يجعل الجامعة عرضة للمخاطر الالكترونية والجرائم الافتراضية.

حيث يعد الأمن السيبراني الحل الأمثل لمتابعة الاستخدام الواسع للانترنت وتطبيقاته وأنظمته المختلفة، للتقليل من المخاطر التي تنشأ من سوء الاستخدام، فالأمن السيبراني طريقة مثلى لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف إلى الولوج للمعلومات المهمة ومحاولة إتلافها أو ابتزاز المستخدمين من خلالها .

حيث أن تصعيد الهجمات الإحتيالية يعد مشكلة كبيرة، والأمن السيبراني بمثابة أليات للتصدي لهذه الهجمات والحد من مخاطرها، كما أن أهمية الأمن السيبراني تعود إلى الحاجة الضرورية لتطوير استراتيجية وطنية وحماية البنية التحتية للدولة ومؤسساتها للحفاظ على المعلومات الحساسة، إضافة إلى ردع الجريمة الإلكترونية، كما أن الأمن السيبراني له أبعاده تتعلق بالحماية الفكرية والممتلكات والأسرار والمحافظة على المعلومات وتجانسها وسلامتها، ويكشف العابثين بها ويجعلها أكثر جهوزية عند الحاجة لها، ويساهم الأمن السيبراني في حماية الأجهزة والشبكات من الاختراق، ويعد درعا واقيا لما تحويه، ويمكن من خلال الأمن السيبراني معرفة الثغرات في الأنظمة ومعالجتها، وتوفير بيئة أمنة للمستخدمين.

كما أن اعتماد الجامعة على الأنظمة التقنية يجعلها من أكثر المؤسسات حاجة إلى بناء ثقة رقمية لحماية المعلومات والأنظمة وزيادة ثقة المستخدمين لهذه الأنظمة والشبكات، والثقة الرقمية هي واحدة من متطلبات إرساء مجتمع المعرفة، وإدارة المعرفة، كما أنها أصبحت جزء من الميزة التنافسية لكثير من المؤسسات خاصة الأكاديمية منها، وفي ظل بيئة التعلم الإلكترونية فإن هناك حاجة لإرساء قواعد ومبادئ الثقة الرقمية، والتي تتحقق بإرساء قواعد وأنماط الثقافة السيبرانية التي تعزز قدرة المستخدم على حماية بياناته من التلف أو من الهجمات الرقمية.

بشكل عام فإن أهمية ثقافة الأمن السيبراني تتمثل في أنها جدار حماية للأفراد والمؤسسات، وتساهم في الوصول لأمن البيانات، والقدرة على استردادها والاستفادة منها بالوقت المناسب، وكلما ضعفت قدرات المجرم على الوصول لبيانات الجامعة فإن ذلك يعزز استعداد المستخدم لمواصلة ومتابعة بياناته بثقة وأمن.

6- منهج الدراسة وأدواتها:

تندرج الدراسة الحالية ضمن الدراسات الوصفية "وهي من البحوث التي تهدف إلى اكتشاف الواقع ووصف الظواهر وصفا دقيقا وتحديد خصائصها تحديدا كيفيا أو كميا تقوم بالكشف عن الحالة المسابقة للظواهر وكيف وصلت إلى صورتها الحالية وتحاول التنبؤ بما ستكون عليه في المستقبل.[1]

أ-منهج الدراسة:

يعتبر المنهج ضروريا في أي بحث علمي، لأنه الطريق الذي يستعين به الباحث ويتبعه في كل مراحل دراسته بغية الوصول إلى نتائج علمية موضوعية، كما أن إختيار المنهج المناسب للدراسة يرتبط بطبيعة المشكلة المبحوث فيها، والمجال الذي تنتمي إليه، وكذا الإمكانات المتاحة لدى الباحث.[2]

ويعرف **المنهج** على أنه "مجموعة من القواعد والقوانين التي تبين لنا أوجه الخطأ والصواب في خطوات البحث وطرق البحث عن الحقيقة والعلم الذي يبحث في المناهج وينتقدها" .[3]

إن **دراسة الحالة** هو المنهج الذي نراه ملائما لدراستنا، ويعرف أحمد بن مرسلي منهج دراسة حالة على أنه "منهج قائم بذاته يتضمن خطوات بحثية محددة ترسم بدقة، الطريق الموصل إلى الغرض العلمي المطلوب، في إطار توظيف العديد من الأدوات البحثية مثل الاستبيان، الملاحظة، والمقابلة وتحليل مضمون..الخ، في جمع المعلومات، وهو يستخدم منفردا في دراسة ظاهرة معينة أو إلى جانب مناهج أخرى"[4]

---

[1]-مروان عبد المجيد ابراهيم: **أسس االبحث العلمي لإعداد الرسائل الجامعية**، مؤسسة الوراق للنشر والتوزيع، ط1، الأردن، 2000، ص40.

[2]-أحمد بن مرسلي: **مناهج البحث في علوم الاعلام والاتصال**، ديوان المطبوعات الجامعية، الجزائر، 2007م، ص285.

[3]-لحسن عبد باشيوة وأخرون: **البحث العلمي مفاهيم وأساليب تطبيقات**، الوارق للنشر والتوزيع، الأردن، 2009م، ص 253.

[4]-أحمد بن مرسلي: **مناهج البحث العلمي في علوم الإعلام والاتصال**، مرجع سابق، ص305.

ب-أدوات الدراسة:

يعتمد أي باحث على مجموعة من الأدوات لجمع البيانات والمعلومات حول الظاهرة أو المشكلة محل الدراسة، ويمكن تعريف أدوات جمع البيانات بأنها الوسيلة أو الأسلوب أو الألية التي يستعملها الباحث لجمع المعلومات والأدلة وطرق تحليلها.[1]

اعتمدنا في هذه الدراسة على المقابلة وتعرف عل أنها محادثة بين طرفين (شخصين أو أكثر)، حول موضوع معين وفقا لمعايير وأنماط محددة، فهي طريقة بحث علمية تستخدم فيها عملية اتصال شفوية لجمع المعلومات تخدم هدفا محددا.[2]

7-مجتمع البحث وعينة الدراسة.

أ-مجتمع البحث:

تعتبر مرحلة تحديد مجتمع البحث من أهم الخطوات المنهجية في البحوث وهي تتطلب من الباحث دقة بالغة، حيث يتوقف عليها إجراء البحث وتصميمه وكفاءة نتائجه .[3]

ويعرف مجتمع البحث بأنه "جميع الأفراد أو الأشياء أو العناصر الذين لهم خصائص واحدة يمكن ملاحظتها".[4]

، وتعرف العينة "على أنها جزء من المجتمع الكلي المراد تحديد سماته، ممثلة بنسبة مئوية يتم حسابها طبقا للمعايير الاحصائية وطبيعة مشكلة البحث، ومصادر بيانته.[5]

وتعرف العينة القصدية بأنها "العينة التي يعتمد الباحث أن تكون من حالات معينة أو وحدات معينة لأنها تمثل المجتمع الأصلي، تعرف تحت أسماء متعددة مثل: الغرضية، العمدية، أو النمطية، يقوم فيها الباحث

---

[1]-محمد شيا: **مناهج التفكير وقواعد البحث في العلوم الإنسانية والإجتماعية**، مجد المؤسسة الجامعية للنشر والتوزيع، ط1، بيروت، 2007م، ص17.

[2]- فضيل دليو: **مدخل إلى منهجية البحث في العلوم الإنسانية والاجتماعية**، دار هومة للنشر والتوزيع، الجزائر، 2014، ص201

[3]-محمد شفيق: ال**خطوات المنهجية لإعداد البحوث الاجتماعية**، المكتب الجامعي الحديث، الإسكندرية، 1999م، ص112.

[4]-مصطفى عليان ربحي، عثمان محمدغنيم: **مناهج وأساليب البحث العلمي**، دار صفاء للنشر والتوزيع، عمان، 2009م، ص.137

3-محمد عبد الحميد: **تحليل المحتوى في بحوث الاعلام**، ديوان المطبوعات الجامعية، الجزائر، 1979م، ص91.

من اختيار المفردات بطريقة تحكمية لا مجال للصدفة فيها، وفق إدراك مسبق ومعرفة جيدة لمجتمع البحث ولعناصره وبالتالي لا يجد صعوبة سحب مفرداتها بطريقة مباشرة.[1]

وقد اعتمدنا في دراستنا هذه على العينة القصدية وذلك لتلائمها والموضوع محل الدراسة، حيث تستخدم العينة القصدية في الدراسات الاستطلاعية التي تتطلب القياس، وقمنا باستخدامها لمعرفة متطلبات الأمن السيبراني في نظم المعلومات الادارية لجامعة البويرة، حيث اخترنا عينة تتكون من 06 مفردات من بين كل الاداريين التقنيين بجامعة آكلي محند أولحاج، وقمنا بتوزيع دليل المقابلة عليهم من أجل الحصول على المعلومات.

8-تحديد مفاهيم الدراسة:

يساعد تحديد المفاهيم الباحث على توضيح المعاني والمفاهيم التي يتناولها في البحث وذلك بهدف إزالة الغموض والالتباس حول المعنى المتبنى في الدراسة، لأن غموض المفهوم يفقد الموضوع قيمتع العلمية، ونشير إلى أننا سنقتصر على تحديد مفهوم الأمن السيبراني، المعلومات الإدارية، الجامعة .

-1 الأمن السيبراني:

أ-الأمن لغة: إن الأمن من المفاهيم ذات الدلالة الواسعة والثرية في اللغة العربية وأصل الكلمة الألف والميم والنون، وهي إسم شتق من الفعل الثلاثي "أمن" فيقال "أمن، أمنا، أمانا، وأمنة والذي يعني اطمأن إلى الشيء ووثق به وأركن إليه "[2]

ب-الأمن اصطلاحا: يعتبر تعريف باري بوزان barry buzan لمفهوم الامن من أكثر التعاريف تداولا حيث يعرف الأمن بأنه العمل على التحرر من التهديد، فإن حالة الأمن تتحقق عندما تنتهي فيها كل أشكال التهديد.[3]

ج-السيبراني لغة: السيبرانية أو cyber هي كلمة إنجليزية، ولقد عرف قاموس أكسفورد كلمة سيبراني بأنها صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي.[4]

---

[1]-أحمد زكي بدوي: **معجم المصطلحات الاجتماعية**، مكتبة لبنان، ط1، بيروت، 1978م، ص364.

[2]-**منجد الطلاب**، دار المشرق، بيروت، 1999، ص82.

[3]- سليمان عبد الله الحربي: **مفهوم الأمن ومستوياته وصيغه وتهديداته -دراسة نظرية في المفاهيم والأطر-**، المجلة العربية للعلوم السياسية، العدد19، 2008، ص17.

[4]-وليد احمد الروضان: **مالفرق بين أمن المعلومات والأمن السيبراني**، صحيفة الجزيرة الالكترونية، مؤسسة الجزيرة للصحافة والطباعة والنشر، قطر، 2010، ص25.

د-الأمن السيبراني إصطلاحا:

يعرف بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة، بتقنيات الاتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن بحيث لا تتوقف عجلة الانتاج، وبحيث لا تتحول الأضرار إلى خسائر مادية [1]

هـ-الأمن السيبراني إجرائيا: هو مجوع الإجراءات والبرامج والتطبيقات التي توفرها جامعة أكلي محند أولحاج البويرة لحماية أنظمتها وشبكاتها والمعلومات والبيانات المتوفرة لديها من الجرائم الإلكترونية بشتى أنواعها، ومنع الوصول غير المصرح به لهذه الشبكات والأنظمة.

2- نظم المعلومات الإدارية:

أ-المعلومات لغة: تعد المعلومات كمصطلح أحد المشتقات العربية من مصدر (علم)، وهي بهذا الإشتقاق تكون وثيقة الصلة بالعلم والمعرفة والتعليم والتعلم والدراية والإحاطة والإدراك والمعرفة والوعي والإعلام والشهرة والتمييز والتسيير وتحديد المعالم **information** هي المقابل الإنجليزي لكلمة المعلومات والإعلام في العربية.[2]

ب-المعلومات اصطلاحا: البيانات المنظمة والمعروضة بشكل يجعلها ذات معنى للشخص الذي يستلمها لذلك فإن المعلومات قيمة حقيقية للمستخدم، وتقدم إضافة للمعرفة الموجودة لديه حول ظاهرة أو حدث أو مجال معين، فالمعلومات تخبر المستخدم بشيء مالا يعرفه أو لا يمكن توقعه.[3]

ج-نظم المعلومات الإدارية: هي عبارة عن نوع خاص من أنظمة العمل التي تستخدم تكنولوجيا المعلومات من أجل التقاط ونقل وتحويل واسترجاع ومعالجة وعرض المعلومات التي تدعم واحدا أو أكثر من أنظمة

---

[1]-حسن سعيد عبد اللطيف: **اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت**، دار النهضة العربية، القاهرة، 2013م، ص214.

[2]-عمر أحمد همشري: **المكتبة ومهارات استخدامها**، دار صفاء للنشر والتوزيع، عمان، 2009م، ص21.

[3]-محمد نور بورهان، غازي ابراهيم رحو: **نظم المعلومات المحوسبة**، دار المناهج للنشر والتوزيع، عمان، 1998م، ص24.

العمل وتتكون من مجموعة الموارد المترابطة التي تعمل معا بشكل متفاعل وتشمل على الأجهزة والبرمجيات والموارد البشرية والبيانات والشبكات والاتصالات.[1]

د-نظم المعلومات الإدارية إجرائيا: مجموعة منظمة من الوسائل التي توفر معلومات عن الماضي والحاضر والتنبؤ بالمستقبل فيما يتعلق بأنشطة وعمليات الجامعة (اكلي محند أولحاج البويرة)، وأيضا بما يحدث في بيئتهما الخارجية والتي تؤدي إلى تدعيم وضائف التخطيط والرقابة والعمليات في المنظمة من خلال ما توفره من معلومات في التوقيت المناسب لصنع القرار.

3- الجامعـــــــــة:

أ-الجامعة لغة: تعني التجميع والتجمع، أما كلمة كلية فمصدرها الكلمة اللاتينية cologie، وتشير إلى التجمع والقراءة معا، وقد استخدمت في القرن 13 بمعنى كلية، وفي أكسفورد تدل على مكان التجمع المحلي للطلاب، متضمنا مكان الإقامة المعينة والتعليم.[2]

ب-الجامعة اصطلاحا: هي مؤسسة للتعليم العالي تهتم بتدريس وتعليم الطلاب الذين ينهون دراستهم الثانوية، وتظهر عددا من المعاهد والكليات التي تتولى تدريب العلوم الإنسانية وما يتفرع عنها ويتحصل الطالب الذي يستخرج من الجامعة على شهادة في اختصاص معين، تعنى الجامعة بتثقيف المجتمع من خلال توعية الطلاب وحث روح التعاون والالفة بينهم وتزويدهم بالمعرفة الضرورية ضمن اختصاص كل فرد منهم، وتعنى بالحفاظ على التروة الوطنية وصوصا التراث الوطني، بتكريم رجالات الفكر وتدعيم البنيان الثقافي الوطني وتزويد المجتمع برجال وخبراء واختصاصيين يعملون على نهضته وتطويره نحو الأفضل. [3]

ج-إجرائيا: الجامعة مؤسسة تمثل قمة الهرم التعليمي، تحتوي على معاهد وكليات وتدرس فيها مختلف العلوم، يدرس فيها طلبة مختلف التخصصات على يد أساتذة متخصصين في مجالات عدة، ويتحصل من خلالها الطلاب على شهادة في تخصص معين، كما تعنى الجامعة بتثقيف الطلاب وتنمية روح التعاون وتعزيز معارفهم.

---

[1]-غسان عيسى العمري، سلوى أمين السمرائي، "**نظم المعلومات الاستراتيجية مدخل استراتيجي معاصر**"، دار المسيرة للنشر والتوزيع، ط1، الأردن، 2008، ص106.

[2]-محمد منير مرسي: **التعليم الجامعي المعاصر وقضاياه واتجاهاته**، دار النهضة العربية للطباعة والنشر، مصر، 2002م، ص17..

[3]-جرجيس ميشال جرجس: **معجم مصطلحات التربية والتعليم**، دار النهضة العربية، لبنان، 2005م، ص251.

9-الدراسات السابقة:

تشكل الدراسات السابقة جزءا أساسيا من البحث العلمي، ويعد وجوده شرط أساسي في كل بحث، وفي إطار حدود البحث والإمكانيات المتوفرة لدينا تمكنا من الحصول على بعض الدراسات السابقة التي تعتبر لبنة لموضوع بحثنا ومن أهم هذه الدراسات:

- الدراسة الأولى[1]:

هدفت هذه الدراسة إلى التعرف على نوعية قضايا الأمن السيبراني، والكشف عن نوع الجرائم السيبرانية التي تناولتها الصحافة الإلكترونية السعودية من خلال الإشكالية التالية: كيف عالجت الصحف الإلكترونية السعودية الجرائم السيبرانية؟، قصد الإجابة على الإشكالية المطروحة اعتمد الباحث على المنهج التحليلي الوصفي باستخدام أداة تحليل المضمون، وتمثل مجتمع البحث في الصحف الإلكترونية السعودية، وبلغت جملة المادة التي تم تحليلها نحو(2548 مادة) تضمن موضوع الدراسة، بالتطبيق على صحف (سبق، عاجل، المواطن).

-توصلت الدراسة إلى مجموعة من النتائج أبرزها تصدر صحيفة "عاجل" في نشر الجرائم السيبرانية يليها صحيفة "سبق"، ثم صحيفة "المواطن" .

-كشفت نتائج الدراسة تصدر القضايا الأمنية ترتيب القضايا التي صاحبت الجرائم السيبرانية، يليها يليها القضايا الاجتماعية والصحية.

-بينت النتائج تعدد الجرائم السيبرانية حيث تصدرت قضايا الأداب العامة، يليها تسجيل المكالمات والتصوير بدون إذن.

أفادت هذه الدراسة في الجانب المنهجي فقد ساعدتنا في توسيع القاعدة المعرفية الخاصة بمشكلة البحث، كما ساهمت في إثراء الخلفية النظرية.

[1]-العتيبي، محمد بن معيض مشاري النفيعي، **معالجة الصحافة الالكترونية لجرائم الأمن السيبراني في المملكة العربية السعودية** –دراسة تحليل المضمون، رسالة ماجستير، كلية العلوم الاجتماعية، قسم الإعلام، جامعة نايف للعلوم الأمنية، 2020.

-الدراسة الثانية[1]:

هدفت هذه الدراسة التعرف على مفهوم الأمن السيبراني وأهم جرائم التي يتعامل معها الأمن السيبراني لدى طلاب الجامعات السعودية، والتعرف على واقع تطبيق الذكاء الإصطناعي في الجامعات السعودية من خلال الإشكالية التالية: ماهو واقع تطبيق الذكاء الاصطناعي كمدخل لتطوير صناعة القرار في المملكة العربية السعودية ؟

قصد الإجابة على الإشكالية المطروحة اعتمد الباحثون على المنهج التحليلي الوصفي، وذلك لوصف الأمن والذكاء الإصطناعي من خلال الاطلاع على الأدبيات المرتبطة بموضوع البحث، تكونت عينة البحث الخاصة بتطبيق الأمن السيبراني إلى مجموعة من طلاب الجامعات السعودية، وأعضاء هيئة التدريس والإداريين، وتم توزيع 321 استمارة استبيان على مجموعة من طلاب الجامعة .

توصلت الدراسة إلى مجموعة من النتائج أهمها وجود اتفاق وتجانس في الأراء بين أفراد عينة البحث بشأن تعدد المخاطر التي تتعرض لها الجامعات السعودية متمثلة في البرامج الخبيثة والاختراقات، مما يعد تدمير للبيانات.

-يوجد اتفاق بين أفراد العينة حول الأهمية النسبية التي تتعرض لها أنظمة الجامعة الإلكترونية.

-ندرة التدريب على برامج الذكاء الاصطناعي وضعف التكنولوجيا المستخدمة في الوضع الراهن .

-قلة خبرة القيادات التربوية في التعامل مع الذكاء الاصطناعي .

أفادت هذه الدراسة في إثراء الجانب المعرفي حيث تم التعرف على مصطلح الأمن السيبراني ومجالات استخدامه، كما ساهمت في رفد الدراسة بما تحتاج إليه لرسم اتجاهاتها الفكرية والتطبيقية .

[1]-جيهان محمد سعد الخضري، هدى جبريل علي سلامي، نعمة ناصر: **الأمن السيبراني والذكاء الاصطناعي في الجامعة السعودية دراسة مقارنة**، مجلة تطوير الأداء الجامعي، مجلد12، العدد1، جامعة جازان السعودية، 2020.

-الدراسة الثالثة [1]:

هدفت هذه الدراسة إلى معرفة الدور الذي يلعبه الإعلام الجزائري في التصدي للجريمة السيبرانية من خلال أحد القنوات الخاصة الجزائرية، وهي قناة النهار من خلال البرنامج الأسبوعي "تحريات" تمحورت إشكالية الدراسة كالتالي: ماهو دور الإعلام الجزائري في التصدي للجريمة السيبرانية من خلال قناة النهار؟

وقصد الإجابة على الإشكالية المطروحة تم الاعتماد على المنهج المسحي القائم على الوصف والتحليل، وتم الاعتماد على أدوات الملاحظة والتحليل لرصد هذا الدور، تكونت عينة الدراسة في ثلاثة أعداد من برنامج تحريات تم بثها خلال سنة 2020، تم اختيارها بناء على طبيعة هذه الدراسة التي تعنى بالاعلام والجريمة السيبرانية .

توصلت الدراسة إلى مجموعة من النتائج أبرزها:

-أن أغلب هذه الجرائم المرتكبة تمت عن طريق موقع التواصل الاجتماعي الفايسبوك تعرض من خلالها عدد الأشخاص إلى عمليات إبتزاز وتهديد بنشر الصور أغلبها مقابل المال .

-أن الاعلام يشجع الضحايا على إبلاغ الأمن بالجرائم السيبرانية التي يتعرضون لها من أجل القضاء عليها بدل السكوت عنها وتفاقمها.

-أن الاعلام يلعب دورا مهما في كشف كل خفايا الجريمة الإلكترونية، وذلك باستظافة الجانب القانوني والأمني والنفسي والاجتماعي .

-أن الإعلام يقوم بدعم الأمن في مرافقته في عمله لأجل التصدي للجريمة السيبرانية.

استفادت دراستنا الحالية من هذه الدراسة في تحليل واقع الأمن السيبراني في المجتمع الجزائري وما يتطلبه من مقترحات كما أفادت في توظيف الاعلام الجديد في التوعية بمخاطر الجرائم السيبرانية.

تسير الدراسة الحالية في نفس الاتجاه بهدف تعزيز فكرة وثقافة الأمن السيبراني والتوصل إلى المتطلبات اللازمة لتحقيقه في مختلف أبعاده وتوفير إطار حوكمة له خصوصا في الجامعات الجزائرية.

[1]-زينب ياقوت: **دور الاعلام الجزائري في التصدي للجريمة السيبرانية -قناة النهارانموذجا**-، مقال علمي، مجلة طلبنة للدراسات العلمية الأكاديمية، العدد1، المجلد 05، الجزائر، 2021.

10-حدود الدراسة:

اخذت الدراسة أبعاد حدودية بين الزمانية والمكانية والبشرية والمتمثلة كالآتي:

الحدود الزمانية: أجريت هذه الدراسة خلال السداسي الثاني من الموسم الجامعي 2022\2023 خلال الفترة الممتدة من شهر فيفري الى شهر جوان .

الحدود المكانية: وهي الاطار المكاني الذي أجريت فيه هذه الدراسة والذي تتوزع عليه عينة البحث وتطبق فيه أدوات جمع البيانات، وتمثل الاطار المكاني لدراستنا في جامعة آكلي محند اولحاج بالبويرة .

الحدود البشرية: يرتبط المجال البشري بالجمهور الذي شملته الدراسة، والتي تمثلت في عدد من الاداريين التقنيين بجامعة آكلي محند أولحاج، الذين أجريت معهم مقابلة من أجل الحصول على المعلومات

الفصل الأول: تأصيل مفاهيمي لأنظمة المعلومات الإدارية في المؤسسة.

تمهيد

المبحث الأول: أساسيات عن نظم المعلومات وطبيعة نظم المعلومات.

1. مفهوم نظم المعلومات .
2. خصائص نظم المعلومات .
3. موارد نظم المعلومات .
4. أنواع نظم المعلومات .

المبحث الثاني: مقاربة معرفية حول المعلومات الإدارية.

1. مفهوم نظم المعلومات الإدارية وتطورها.
2. مكونات نظم المعلومات الإدارية .
3. أبعاد نظم المعلومات الإدارية .
4. خصائص نظم المعلومات الإدارية .

المبحث الثالث: نظم المعلومات الإدارية وضائفها وأهميتها وتحديات تطبيقها.

1. وظائف نظم المعلومات الإدارية .
2. أهمية نظم المعلومات الإدارية .
3. تحديات نظم المعلومات الإدارية .
4. المداخل المعاصرة لدراسة نظم المعلومات الإدارية .

خلاصة الفصل

تمهيد:

تمثل المعلومات موردا من الموارد المهمة للمنظمة، والتي نستطيع من خلالها تحقيق مزايا تنافسية وأداء متميز وصولا إلى نجاح المنظمة، وأن هذه المعلومات تحتاج إلى إدارة وتخطيط وتنظيم ورقابة للاستفادة منها، ولتحقيق ذلك ينبغي أن تتم عملية إدارة المعلومات في إطار منظم ويمثل هذا الإطار بنظام المعلومات الإدارية الذي بات اليوم من الضروريات الحتمية لكل المنظمات لدورها البارز في الفكر الإداري والمعلوماتي.

ولهذا سنحاول في هذا الفصل عرض تأصيل مفاهيمي لأنظمة المعلومات الإدارية من خلال ثلاثة مباحث رئيسية، جاء الأول منهما بعنوان أساسيات عن نظم المعلومات وطبيعتها نتطرق من خلاله إلى مفهوم نظم المعلومات ومن ثم خصائصها وبعدها موارد نظم المعلومات وأنواع نظم المعلومات، وجاء المبحث الثاني تحت عنوان مقاربة معرفية حول المعلومات الإدارية سنتطرق من خلال عناصره الأربعة إلى مفهوم نظم المعلومات الإدارية ومراحل تطورها وكذا مكونات نظم المعلومات الإدارية وأهم أبعادها وخصائصها.

في حين خصص المبحث الثالث لعرض وظائف نظم المعلومات الإدارية، وأهميتها وتحديات نظم المعلومات الإدارية، وأهم المداخل المعاصرة لدراسة نظم المعلومات الإدارية .

-المبحث الأول: أساسيات عن نظم المعلومات وطبيعة نظم المعلومات.

1-مفاهيم حول نظم المعلومات:

يشير مصطلح نظم المعلومات إلى أنه مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها، والتي تعمل على جمع البيانات والمعلومات ومعالجتها وتخزينها وتوزيعها بغرض دعم صنع القرار، والتنسيق وتأمين السيطرة على المنظمة، إضافة إلى تحليل المشكلات، وتشمل نظم المعلومات بيانات الأشخاص الأساسيين والأماكن والنشاطات والأمور الأخرى التي تخص المنظمة والبيئة المحيطة بها[1].

يعرف نظام المعلومات بأنه نظام من الأنظمة الأخرى الموجودة بالمشروع يقوم بمهمة تجميع البيانات وتحويلها إلى معلومات حسب إجراءات وقواعد محددة تساعدها الإدارة وفئات أخرى في اتخاذ القرارات التي تتعلق بالتخطيط والرقابة، والعناصر الرئيسية لنظم المعلومات هي تجميع البيانات وتشغيلها وتخزينها واسترجاعها وتحويلها .[2]

وبالتالي نظم المعلومات مجموعة من الإجراءات التي يتم من خلالها تجميع

واسترجاع تشغيل وتخزين، ونشر المعلومات بغرض دعم عمليات صنع القرار

وتحقيق الرقابة في المنظمة .[3]

وعرفت نظم المعلومات الإدارية على أنها مجموعة من العناصر المتداخلة والمتفاعلة مع بعضها البعض التي تعمل على جمع مختلف البيانات والمعلومات وتعمل على معالجتها وتخزينها وتوزيعها على المستفدين بغرض دعم القرار والرجوع إليها حين الحاجة إليها.[4]

---

[1]-منعم زمير، **محمد الفيومي: إدارة أنظمة تكنولوجيا المعلومات**، دار الشركة العربية المتحدة للتسويق والتوريدات، القاهرة، 2013م، ص29.

[2]-صلاح عبد المنعم مبارك: **اقتصاديات نظم المعلومات المحاسبية الإدارية**، دار المطبوعات الجامعية، الإسكندرية، 2008م، ص51.

[3]-عبد الهادي مسلم: **مذكرات في نظم المعلومات الإدارية، مبادئ وتطبيقات**، الناشرمركز التنميةالإدارية، الإسكندرية، 1994م، ص16.

[4]-علاء الدين عبد القادر: **نظم المعلومات الإدارية**، دار المسيرة للنشر والتوزيع، الأردن، 2008م، ص27.

2-خصائص نظم المعلومات:

يقوم نظام المعلومات على توفير العديد من الصفات الأساسية التي تبرز صحة أداء النظام لوظائفه ومدى كفائته وهي كالتالي:

*التوافق: لتقييم نظام المعلومات لا بد من مراعاة الظروف البيئية التي يعمل فيها سواء بتحديد نوعية المدخلات والمخرجات أو بتلبية احتياجات المستخدم، فعلى نظام المعلومات أن يكون منسجما ومتوافقا مع البيئة المحيطة به. [1]

*شبكات الاتصال: تمثل هذه الشبكات إحدى القنوات التي تضمن تدفق المدخلات والمخرجات بين الأنظمة، فنتائج نظام معين قد تكون من مدخلات نظام أخر، مما يوضح أن عامل الاتصال متوافر بين الأنظمة الفرعية وبأن النظام يتميز بالفاعلية في إنجاز وظائفه.

*التغذية العكسية: هي أسلوب التعامل مابين النظام وبيئته الخارجية واستيعابه لمختلف النتائج والظروف الناجمة عن هذه العلاقة فالوقت يمثل العامل الأساسي الذي يحدد قيمة عمل النظام .

*التكلفة: تسعى هذه الخاصية إلى تحقيق التوازن بين قيمة المعلومات وتكلفتها أي أن المعلومات التي يوفرها النظام تتناسب مع قيمتها أثناء الاستخدام .

*استخراج المعلومات: لإعداد المعلومات لا بد من التقيد بالفترة الزمنية المحددة لأن أي تأخر يؤدي إلى نقص في قيمة المعلومات بحيث يصبح معناها بلا فائدة .

*التوجيه: تخضع عملية التوجيه إلى قواعد وقوانين تضمن لها الصحة والدقة في معانيها حيث يجب مراعاة تقديم المعلومات بكمية معتبرة وأن تكون مناسبة وذات نوعية ومصدر سليم.[2]

3-موارد نظم المعلومات:

يحتوي نظم المعلومات على أربعة موارد أساسية: الماديات والبرمجيات والأفراد والبيانات وهي كالتالي:

---

[1]-حمودي كاهنة: **نظام أمن المعلومات في الجزائر -دراسة حالة بلدية سوق الإثنين-**، مذكرة ماستر، تخصص سياسات عامة وإدارة محلية، جامعة مولود معمري، تيزي وزو، 2017/2016، ص24.

[2]-حمودي كاهنة: **نظام أمن المعلومات في الجزائر**، مرجع سابق، ص25.

أ–موارد الماديات: ويشمل جميع المعدات المادية والمواد المستخدمة في معالجة البيانات، وهي بالأخص المكائن مثل الحاسوبات والألات الحاسبة، كما تشمل أوساط البيانات مثل الأوراق والأقراص المغناطيسية، ومن أمثلة الماديات في نظام المعلومات الحاسوبي: [1]

*الحاسوبات الكبيرة والصغيرة والدقيقة.

*محطات الحاسوب وتستخدم لوحة المفاتيح لإدخال البيانات أو الطابعات لإخراج المنتجات أو المعلومات والأقراص الضوئية أو المغناطيسية للخزن.

*شبكات الاتصال وتتكون من الحاسوبات والمحطات ومعالجة الاتصالات ومعدات أخرى مربوطة بوسائط الاتصال المختلفة لتوفير قوة حاسبتية داخل المنظمة .

ب–موارد البرمجيات: يعني مصطلح برمجيات مجموعة الإيعازات الخاصة بمعالجة البيانات، ولكن هذا المصطلح لايشمل فقط البرامج التي توجه وتدير المكونات المادية للحاسوب ولكنه يشمل مجموعة الإيعازات التي يحتاجها الأفراد لمعالجة البيانات والتي تسمى إجراءات ومن البرمجيات:

*برمجيات المنظومة، مثل نظام التشغيل التي يدير ويدعم عمليات منظومة الحاسوب .

*البرمجيات التطبيقية وهي برامج توجه المعالجة لاستخدام معين للحاسوب من قبل المستخدم النهائي، ومن أمثلتها نظام السيطرة على التخزين، ونظام الرواتب ونظام معالجة النصوص.

*الإجراءات وهي توجيهات تشغيلية للأفراد الذين يستخدمون نظام المعلومات ومن أمثلتها التوجيهات الخاصة بملأ الاستمارات أو استخدام حزمة برمجيات معينة.

ج–موارد الأفراد: هناك حاجة للأفراد لتشغيل جميع أنظمة المعلومات وهذا المورد يتكون من الإختصاصيين والمستخدمين النهائيين: [2]

*الإختصاصيين: وهم الأفراد الذين يحللون ويصممون ويشغلون نظام المعلومات، ويتكونون من محللي الأنظمة والمبرمجين، ومشغلي الحاسوب والملاك الإداري والتقني والكتابي وطبيعيا، يقوم محللو النظام بتصميم النظام بالاستناد إلى الاحتياجات المعلوماتية للمستفدين النهائيين، ويقوم المبرمجون بإعداد برامج

[1]–عماد الصباغ: **نظم المعلومات ماهيتها ومكوناتها**، دار الثقافة للنشر والتوزيع، عمان، 2000م، ص 24.

[2]- عماد الصباغ: **نظم المعلومات ماهيتها ومكوناتها**، مرجع سابق، ص26.

الحاسوب بناءا على المواصفات التي يقدمها محلل النظم.ويقوم مشغلو الحاسوب بتشغيل الحاسوبات الكبيرة والصغيرة

*المستخدمون النهائيون: هم الأفراد الذين يستخدمون نظام المعلومات ويمكن أن يكون المدراء أو المحاسبين أو المهندسين أو البائعين أو العملاء أو الكتبة أو أكثرها مستخدمين نهائيين لأنظمة المعلومات.

ج–موارد البيانات: البيانات هي من أكثر المواد الخام لنظم المعلومات، إن مفهوم موارد البيانات قد تم توسيعه من قبل المدراء وإختصاصي أنظمة المعلومات، فقد وجدو أن البيانات والمعلومات تشكل موارد ثمينة للمنظمة، لذلك فالبيانات والمعلومات التي تخزن في قواعد بيانات وقواعد نماذج وقواعد معرفة تعتبر اليوم جزءا من موارد البيانات أو موارد المعلومات للمنظمة .

والبيانات تسجل وتخزن عادة باستخدام أوساط بيانات مختلفة تشمل الأوراق والأوساط الضوئية أو المغناطيسية أو الوسائل الإلكترونية، ومن أمثلتها الوثائق الورقية، والأشرطة المغناطيسية والأقراص البصرية، المصغرات الفيلمية وشرائح والدوائر الإلكترونية .[1]

4–أنواع نظم المعلومات:

يعتمد كل نوع من هذه الأنظمة على نوع العمل الذي يؤديه النظام وتتمثل في مايلي:

*نظم معالجة المعاملة: تقع هذه الأنظمة ضمن المستوى التشغيلي للمؤسسة، وهي أنظمة معلومات مبرمجة تعالج كم هائل من المعلومات وتستخدم لإنجاز الأعمال التجارية الروتينية واليومية، وتؤهل المؤسسة للمحافظة على علاقتها بالبيئة الخارجية.

*أنظمة المكتب الأوتوماتيكية وأنظمة العمل المصرفي: تقع هذه الأنظمة ضمن المستوى الأعلى للمؤسسة، وهي أنظمة معلومات مبرمجة تعمل على تحقيق التفاعل بين الأفراد والحواسيب، وتتطلب هذه الأنظمة أفراد مختصين وحواسيب مبرمجة تعمل بشكل صحيح وتعطي هذه الأنظمة مجالا واسعا من مهام المؤسسة.

*نظم دعم القرارات: تقع هذه الأنظمة ضمن مستوى الأعلى للمؤسسة وهي أنظمة معلومات مبرمجة تشبه أنظمة إتخاذ القرارات التقليدية .

[1]- عماد الصباغ: **نظم المعلومات ماهيتها ومكوناتها**، مرجع سابق، ص26.

*الأنظمة الجيدة وأنظمة الذكاء الإصطناعي: الأنظمة الخبيرة تستخدم الذكاء الاصطناعي لإيجاد الحلول ووضعها في متناول المستخدمين للنظام بالاعتماد على الإمكانيات المعرفية المتاحة لها في المنظمة.

*نظم دعم التنفذيين: هي تلك النظم التي تدعم توجه التنفذيين على طلرق المساعدة بقصد صناعة واتخاذ القرارات على المستوى الاستراتيجي وربط متغيرات الأعمال وربطها بما يحدث في البيئة الخارجية من خلال تجهيز المخططات وإعداد مخططات الإتصالات التي تساعده على تحقيق غايات أعمال التنفذيين. [1]

رأينا من حلال هذا المبحث أن نظام المعلومات يمثل الإصدار المتكامل لتدفق المعلومات من مصادرها المختلفة إلى مراكز استخدامها لاتخاذ القرارات وعليه فهي تمثل نظام متكامل من العنصر البشري والألات يهدف إلى تقديم معلومات بالشكل المطلوب وتماز هذه النظم بالشمولية لما لها من عناصر مهمة تساهم في تحديد الإجراءات اللازمة إتخاذها أثناء استخدام هذا النظام في المؤسسات الإدارية والإقتصادية وأنها تعتمد على مجموعة من الموردات المادية والتقنية والبشرية التي من شأنها تسهيل عملية النظام وتوفير البيانات والمعلومات في الوقت المناسب وبالجودة المناسبة وبالدقة المناسبة.

المبحث الثاني: مقاربة معرفية حول نظم المعلومات الإدارية

1-مفهوم نظم المعلومات الإدارية وتطورها:

أ-مفهوم نظم المعلومات الإدارية:

تعد نظم المعلومات الإدارية إحدى الحقول الهامة للنظرية الإدارية وتطبيقاتها الحديثة في مختلف الأنظمة، إلا أنه مازال هناك خلاف قائم على المفهوم العلمي لنظم المعلومات الإدارية والدور الذي تؤديه في إنجاز وظائف وأنشطة الإدارية، ويعد نظام المعلومات الإداري من النظم الفرعية لأي نظام وهو نظام حيوي وهام له مكانته واعتباره لما له من دور فاعل في تطوير عمل النظم، حيث تعمل هذه النظم على توفير معلومات دقيقة وشاملة واضحة يتم الاستنارة والاسترشاد بها أثناء قيام المؤسسات بأعمالها، ولايقتصر ذلك المستويات

[1]-بسود مبارك، يوخني أمينة: **دور نظم المعلومات في إدارة الموارد البشرية -دراسة حالة جامعة أدرار-**، مذكرة ماستر، تخصص إدارة أعمال، جامعة أحمد دراية، أدرار، 2020/2019، ص11.

الإدارية العليا، بل تعمل هذه الأنظمة على توفير المعلومات لكافة المستويات الإدارية بالقدر المناسب والتوقيت المناسب [1]

لقد تعددت تعاريف نظم المعلومات الإدارية وهذا ناتج عن إختلاف طريقة تناول هذا الموضوع من قبل الباحثين والمختصين، وهناك من يشار إلى نظم المعلومات

الإدارية (mis) بشكل عام على الاستخدام في مساعدة الإدارة على إنجاز أهدافها من خلال نظم وبرمجيات مصممة لتتم من تشغيل العمليات الإدارية بأسلوب وتقنية تكنولوجية سهلة وميسرة وبشكل أفضل من الطرق التقليدية، ويحقق وفرات في موارد ومصادر المنظمة وزيادة في كفاءة وإنتاجية هذه العمليات.[2]

وهناك من يجدها على أنها نوع خاص من أنظمة العمل تستخدم تكنولوجيا المعلومات من أجل إلتقاط ونقل وتحويل واسترجاع ومعالجة وعرض المعلومات التي تدعم واحدا من أكثر من أنظمة العمل وتتكون من مجموعة الموارد المترابطة التي تعمل معا بشكل متفاعل وتشمل على الأجهزة والبرمجيات والموارد البشرية والبيانات والشبكات والاتصالات.[3]

يعرفها الصباغ على أنها بيئة تحتوي على عدد من العناصر التي تتفاعل فيما بينها ومع محيطها بهدف جمع البيانات ومعالجتها حاسوبيا وإنتاج وبث المعلومات لمن يحتاجها لصناعة القرارات.[4]

هي تلك النظم الرسمية وغير الرسمية التي تمد الإدارات بمعلومات سابقة حالية وتنبؤية في صورة شفوية أو مرئية للعمليات الداخلية للمؤسسة ولعناصر البيئة المحيطة بها، بهدف دعم الإداريين وخاصة المدراء والعناصر البيئية الأساسية وإتاحة المعلومات الدقيقة الواضحة، وفي إطار الوقت المناسب لمساعدتهم على إنجاز العمل والإدارة واتخاذ القرارات.[5]

---

[1]--الأعرجي، عاصم وعلاونة، علي أحمد: **واقع وأثار استخدام أنظمة المعلومات المحوسبة:** دراسة ميدانية في مركز وزارة التربية والتعليم الأردنية، المجلة العربية للإدارة، عدد1، مجلد22، 2002م، ص57.

[2]–ربحي مصطفى العليان: **إدارة المعرفة،** دار صفاء للنشر والتوزيع، عمان، 2008، ص269.

[3]–غسان عيسى العمري، سلوى أمين السمرائي: **نظم المعلومات الاستراتيجية مدخل استراتيجي معاصر**، دار المسيرة للنشر والتوزيع، عمان، 2008ص106.

[4]–عماد الصباغ: **نظم المعلومات، ماهيتها ومكوناتها**، دار الثقافة للنشر والتوزيع، 2000، ص11.

[5]–سليم الحسنية: **نظم المعلومات الإدارية، إدارة المعلومات في عصر المنظمة الرقمية،** مؤسسة التوراق للنشر والتوزيع، 2006، ص53.

نظم المعلومات الإدارية هي الية تسمح بجمع وتصنيف واسترجاع معلومات مخزنة في ملفات بصورة يدوية أو ميكانيكية سابقا، وإلكترونية حاليا، إضافة إلى بناء مهم وإنتاج معلومات جديدة من المعلومات السابقة والموجودة أصلا في النظام بعد معالجتها.[1]

ب- مراحل تطور نظم المعلومات الإدارية:

مرت نظم المعلومات الإدارية في تطورها بثلاث مراحل أساسية، حيث رافق كل مرحلة تغير واضح في الدور الذي أصبحت تؤديه تلك النظم داخل المؤسسات، وفيما يلي نذكر هذه المراحل:

***المرحلة الأولى:** والتي شهت أول ظهور للإعلام الألي، إمتدت من 1955م إلى نهاية الخمسينات، وقد لوحظ أول استعمالات الاعلام الألي خاصة في المهام المرتبطة بخزينة المؤسسة كحساب الأخر مثلا، أو إدخال تعديلات فيما يتعلق بالمزايا الاجتماعية للعمال، وكذا أنظمة المعاشات.

***المرحلة الثانية:** شملت هذه المرحلة سنوات السيتنيات والسبعينات، وفيها بدأت المؤسسات في استعمال الإعلام الألي كنظام معلومات لأغراض الرقابة والتسيير .

***المرحلة الثالثة:** والتي شملت سنوات الثمانينيات والتسعينات، حيث شمل نظام المعلومات كل النشاطات الأساسية للمؤسسة. [2]

2-مكونات نظم المعلومات الإدارية:

لكل نظام مكونات أساسية يقوم عليها ونظم المعلومات الإدارية تتكون من:

***الأجهزة (Hardware):** أي نظام معلومات يجب أن يحتوي على مجموعة من المعدات والحواسيب الألية خاصة وأن أجهزة الحواسيب أصبحت متوفرة وبأسعار في متناول معظم المنظمات، ونظام الحاسوب يمكن أن يكون حاسوبا شخصيا أو متوسط الحجم أو كبير أو حتى شبكة واسعة ومتنوعة.[3]

***البرمجيات(software):** وهي الأنظمة التي تشتغل بواسطتها الحواسيب وتنقسم إلى قسمين: تتمثل في برمجيات النظم وتعني تلك البرامج التي تساعد على تنفيذ العمليات، مثل ترتيب البيانات واسترجاعها من

---

[1]-عامر إبراهيم قنديلجي وعلاء الدين عبد القادر الجنابي: **نظم المعلومات الإدارية**، دار المسيرة، عمان، 2007م، ص38.

[2]-مرمي مراد: **أهمية نظم المعلومات الإدارية كأداة للتحليل البيئي في المؤسسات الصغيرة والمتوسطة** الجزائرية، مذكرة ماجستير، تخصص إقتصاد وتسيير المؤسسات الصغيرة والمتوسطة، جامعة فرحات عباس، سطيف، 2010/2009، ص24.

[3]-سليم الحسنية: **نظم المعلومات الإدارية**، مرجع سابق، ص56.

الذاكرة وبرمجيات التطبيقات وهي التي تقوم بتشغيل بيانات المنظمة مثل برامج الأجور والمحاسبة وبرامج التصنيع، هذه البرامج يتم إعدادها من طرف مختصين في البرمجة بالمنظمة نفسها أو الحصول عليها جاهزة أما برامج النظم فيتم الحصول عليها من طرف موردي الأجهزة .

***قواعد البيانات (data base):** وهي عبارة عن المخزن الذي يحوي على البيانات التي نصف كل الأحداث والعمليات الجارية في المنظمة، وتكون مخزنة في شكل ملفات يدوية أو إلكترونية بواسطتها يعمل نظام المعلومات على تحويلها إلى معلومات لذلك تعتبر جد مهمة لأي نظام معلوماتي.[1]

***العمليات (Operation):** هي عمليات تقوم بوصف وترتيب جميع الخطوات والتعليمات المحددة لإنجاز العمليات الحاسوبية، وتسمى بخريطة مسار النظام وتقوم بشرح ماالذي يجب عمله.

***الأفراد(Staff):** يعتبر النصر الأساسي لنظام المعلومات الذي يتولى تحليل المعلومات ووضع البرامج وإدارة المعلومات. [2]

3- أبعاد نظم المعلومات الإدارية:

تشمل المعلومات الإدارية ثلاثة أبعاد رئيسية وهي كالتالي:

***البعد التنظيمي:** ومن أهم عناصره:

_الأفراد العاملون .

-الهياكل التنظيمية وهو إطار يركز على تخصيص الوضائف وتقسيمها على العاملين ووضع الأنظمة والإجراءات وتحديد السلطة .

-العمليات الإدارية وهي مجموعة من الأنشطة المترابطة التي تهدف للقيام بإنجاز نشاط معين.

-الثقافة وهي القيم والأعراف التي تتبناها وتؤمن بها المنظمات.

-السياسات وهي عبارة عن خطة توفر إطارا عاما لمساعدة المسؤولين في المنظمة في عملية صنع القرارات بما يسهم في تنفيذ استراتيجية المنظمةوتحقيق أهدافها بنجاح. [3]

---

[1]-سليم الحسنية: **نظم المعلومات الإدارية**، مرجع سابق، ص57.

[2]-بشير يزيد الوليد: **نظم المعلومات الإدارية**، دار الراية للنشر والتوزيع، عمان، د.س، ص119.

[3]-الطاهر اسمهان، ماجد الخفاف، مها مهدي: **نظم المعلومات الإدارية**، دار وائل للنشر والتوزيع، 20111م، ص70.

***البعد الإداري: من أهم عناصره:**

-متخذ القرار .

-المخططون.

-الإبداع في العمليات والمبدعون لعمليات جديدة .

-القادة القادرون على وضع خطط وأجندة جديدة للعمل.

*البعد التكنولوجي: من أهم عناصره:

-المعدات وهي المعدات المادية.

-البرمجيات وهي التعليمات والبرامج التفصيلية .

-المخازن وهي أدوات مادية لتخزين البيانات والبرمجيات .

-تكنولوجيا الاتصالات وتقوم بنقل البيانات من موقع مادي لأخر.

-شبكات الأعمال تقوم بالربط الحاسوبي وتمكن من مشاركة البيانات والموارد.[1]

4-خصائص نظم المعلومات الإدارية:

تمتاز نظم المعلومات الإدارية بجملة من الخصائص وهي كالتالي:

*تدعم نظم المعلومات الإدارية القرارات الهيكلية وشبه الهيكلية ومستوى الرقابة الإداري والتشغيل كما تفيد لأغراض التخطيط لمستوى الإدارة العليا .

*تعتبر نظم المعلومات الإدارية مفيدة لاتخاذ القرارات باعتماد على البيانات الحالية والماضية .

*تعتبر نظم المعلومات موجه لخدمة الرقابة وتقديم التقارير وهي مخصصة لتقديم تقارير عن العمليات الحالية القائمة وبالتالي تساعد في الرقابة اليومية على الأنشطة.

*تعتبر نظم المعلومات الإدارية قليلة المرونة نسبيا .

*تعتمد نظم المعلومات الإدارية على احتياجات معروفة ومستقرة للمعلومات .

[1]-الطاهر اسمهان، ماجد الخفاف، مها مهدي: **نظم المعلومات الإدارية**، مرجع سابق، ص71.

*تعتمد على المعلومات القائمة وتدفق للمعلومات الداخلة للمنظمة أكثر من المعلومات الخارجة .

*تطلب نظم المعلومات الإدارية عملية طويلة نسبيا من التعميم والتحليل. [1]

-رأينا من خلال هذا المبحث كيف أصبحت المعلومات في الوقت الحالي تشكل أحد الموردات الهامة للمؤسسات، وكيف تطورت نظم المعلومات بدءا من ظهور الاعلام الالي إلى غاية استعماله وتعميمه على كل نشاطات المؤسسة ما شكل بذلك نظم المعلومات الإدارية التي تمثل نظام يعمل على جمع وتحليل ونقل المعلومات على مستوى الإداري من خلال مكوناتها البشرية والمادية والتقنية المترابطة فيما بينها وبأبعادها التنظيمية وإدارية وتكنولوجية التي جعلت منها أهم النظم التي تساهم في توفير المعلومات المفيدة لمساعدة الإدارة على إنجاز أهدافها.

المبحث الثالث: نظم المعلومات الإدارية وضائفها وأهميتها وتحديات تطبيقها.

1-وظائف نظم المعلومات الإدارية:

يمكن تحديد وظائف نظم المعلومات الإدارية بالنقاط الأتية:

*الحصول على البيانات (المدخلات): تتضمن وظيفة الحصول على البيانات اختيار كل البيانات اللازمة وتحديدها سواء من داخل المنظمة أو خارجها في ضوء احتياجات المستويات الإدارية في المنظمة.

*تعليمات تشغيل البيانات (الإجراءات) يتم تحديد هذه التعليمات الأتية:

أ-**الاستخدام:** إذ يحدد طبيعة استخدام المعلومات مواصفات المعلومات المطلوبة ومن ثم طريقة معالجة البيانات.

ب-**الخبرات المتخصصة:** إذ يشترك المتخصصون في وضع تعليمات وبرامج التشغيل اللازمة لإعداد التقارير المطلوبة .

ج-**تكنولوجيا المعلومات:** إذ تحدد التكنولوجيا المستخدمة الإجراءات الفنية للتشغيل.

[1]-محمد بكري وسونيا سلطان: **نظم المعلومات الإدارية**، الدار الجامعية الإبراهيمية، 20011، ص55.

*معالجة البيانات: تتضمن هذه الوظيفة تقويم البيانات للتأكد من صحتها ومناسبتها وتحديد درجة أهميتها للمنشأة، وتتم معالجة البيانات بهدف إعداد المعلومات التي تطلبها الإدارة وتجري عمليات المعالجة وفقا لإجراءات أو برامج معدة سابقا.

*تخزين المعلومات: تحفظ جميع المعلومات التي يتم الحصول عليها سواء استخدمت في غرض معين أو لم تستخدم ويتم حفظ المعلومات وتخزينها بطريقة يسهل الرجوع إليها عند الحاجة. [1]

*المخرجات: بعد معالجة البيانات يتم استخراج المعلومات التي تحقق الهدف من عملية المعالجة، وبعد حفظ نسخة من كل البيانات والمعلومات، تعد نسخة من المعلومات ترسل إلى الجهة أو الأشخاص الذين يستخدمونها، ونأخذ هذه المخرجات أشكالا تختلف باختلاف التكنولوجيا المتاحة .

*الاتصال: ليس للمعلومات أي قيمة إذا لم تستخدم لذلك لابد من توصيلها بالشكل المطلوب وفي الوقت المناسب إلى مستخدميها.

ولا تقتصر وظيفة الاتصال في نظم المعلومات الإدارية على مجرد توصيل المعلومات إلى مستخدميها بل لابد أن يكون الاتصال مزدوجا في الاتجاهين بين النظم والمستفدين للتأكد من فهمهم للمعلومات المطلوبة، ويتم استرجاع نتائج ذلك الاتصال إلى النظم بالمقارنة بين النتائج والمعايير الموضوعة لتقييم الأداء. [2]

2-أهمية نظم المعلومات الإدارية:

حتى عهد قريب لم تكن هناك نظرة إلى نظم المعلومات على أنها تمثل أحد الأصول الهامة في المنظمة أو المنشأة وكانت عبارة عن فن شخصي ولا تخرج عن حدود المنظمة ولكن اليوم أصبح الوضع مختلف حيث أصبح هناك إدراك ووعي متزايد بأهمية أنظمة المعلومات الإدارية وذلك لزيادة التخصص في العمل وظهور أساليب جديدة في اتخاذ القرارات والاتجاه نحو المركزية في اتخاذ القرار فتظهر أهمية نظم المعلومات الإدارية فيما يلي:

*تقديم المعلومات إلى المستويات الإدارية المختلفة .

---

[1]-الحميدي، نجم عبد الله والعبيد، عبد الرحمان الأحمد والسامرائي، سلوى أمين: **نظم المعلومات الإدارية مدخل معاصر**، 2004م، ص23.

[2]- الحميدي، نجم عبد الله والعبيد، عبد الرحمان الأحمد والسامرائي، سلوى أمين: **نظم المعلومات الإدارية مدخل معاصر**، مرجع سابق، ص24.

*تقديم المعلومات إلى الأقسام المختلفة بغية إصدار تقارير سواء كانت تجميعية أو تفصيلية أو عن أنشطة المنظمة.

*مساعدة الإدارة في إتخاذ قرارات ناجحة وفعالة وصائبة، من خلال تهيئة المعلومات في الوقت المناسب.

*تقديم تقارير تفصيلية شهرية أو فصلية أو سنوية عن نشاطات المنظمة.

*المساعدة في تقديم نشاطات المنظمة وتقييم النتائج بغية تصحيح الانحرافات.[1]

*توفير المعلومات للإدارة وتهيئتها في الوقت المناسب لمساعدتها وتحفيزها على اتخاذ القرار الفعال والصحيح واستغلال مصادر المعلومات ومواردها داخل المؤسسة وإحكام السيطرة على المعلومات الواردة جميعها.

*القدرة على تبادل وتشارك المعلومات والتحاور عبر الشبكات والاتصالات داخل المنظمة وخارجها.

*القدرة على حفظ وتخزين جميع المعلومات التي تتعامل بها المنظمة ومعالجتها وإمكانية استرجاعها بالشكل والوقت والحجم الذي يخدم المستفيد النهائي .

*القدرة على التخطيط والتنبؤ للمستقبل ضمن احتمالات مدروسة واقتراح بدائل في حالة وجود خلل في تنفيذ الخطط وتوقع احتياجات المنظمة المستقبلية الكفيلة بتحقيق الأهداف. [2]

مما سبق يتضح أن نظم المعلومات الإدارية تزايدت أهميتها بعد الحرب العالمية وذلك بعد ظهور الكمبيوتر، وتكمن أهميتها من خلال توفير الوقت الكبير للمدراء من إنجاز المهام الاستراتيجية المهمة وذلك بتقليص الوقت الذي يضيع على الأعمال الروتينية كإدخال البيانات والإجراءات في صغائر الأمور وكذا ربط جميع فروع وأقسام المؤسسة من خلال الأنظمة المحوسبية، حيث أصبح من السهل تبادل المعلومات والبيانات بين الموظفين وكل هذا الامر تم بدراسة النظام وتحليله من قبل متخصصي نظم المعلومات الإدارية .

3-تحديات نظم المعلومات الإدارية:

[1]-فايز جمعة صالح النجار، نظم المعلومات الإدارية، دار حامد للنشر والتوزيع، 2009م، ص63.

[2]-جاد سيد محمد: **نظم المعلومات الإدارية، الأساسيات والتطبيقات الإدارية**، 2011، كلية التجارة جامعة السويس، السويس، 20011م، ص181.

هناك مجموعة من التحديات التي تواجه المؤسسات في محاولتها للتطبيق الواسع لنظم المعلومات الإدارية وعلى مستوى عالمي من أجل التحول من المؤسسات التقليدية إلى المؤسسات الرقمية ويمكن إجمالها فيمايلي:

*التحدي الاستراتيجي: وهو أن ندرك هذه المؤسسات بوجود المؤسسات الرقمية والتأكد من أفضليتها على المؤسسات التقليدية، ومعرفة كيف تتمكن من استخدام تكنولوجيا المعلومات وضمن إستراتيجية طويلة المدى لتحقيق فعالية أفضل لنشاطاتها ومنافسة أكبر من خلال التطبيق المتزايد للنشاطات بشكل تكنولوجي ورقمي.

*تحدي العولمة: وهو أن تعي المؤسسات تماما متطلبات تطبيق تكنولوجيا المعلومات ونظم المعلومات عالميا وقدرتها على توفير الإحتياجات اللازمة لممارسة العمليات والنشاطات الرقمية وعلى المستوى العالمي.

*تحدي هيكلة البيانات والبنية التحتية لها: ويمثل قدرة المؤسسات على إعادة بناء الهيكل التنظيمي وتطوير هيكل بيانات منسجم مع هيكل المؤسسات وتوفير بنية تحتية من تكنولوجيا المعلومات تخدم وتدعم أهداف التنظيم .

*تحدي الاستثمار في نظم المعلومات: وهو أن يبين كيف تستطيع المؤسسات القيمة المتوقعة لنظم المعلومات ويجب أن تكون عملية الإحلال التكنولوجي للوسائل التقليدية مبررة التكاليف أي يجب أن تغطي العوائد المرتقبة جراء تطبيق نظام المعلومات للتكاليف المطلوبة ضمن مدة الإستثمار.

*تحدي المسؤولية والسيطرة: وهنا يتوجب على المؤسسات أن تتأكد من الكيفية التي يستطيع التنظيم من خلالها استخدام وتطبيق نظم المعلومات ضمن الأخلاقيات العامة وفي حدود المسؤولية الإجتماعية المناسبة.[1]

–وهناك تحديات أخرى يمكن إجمالها كالتالي:

*تناقص قيمة المعلومات إذا لم تستخدم في وقتها المناسب.

*صعوبة إدخال بعض البيانات وذلك لعدم القدرة على التعبير عنها مثل تحويل بعض البيانات إلى قيم كمية مثل الأفكار الحديثة لإنتاج وتطوير منتج ما .

[1]-العتيبي، صبحي جبر: **تطور الفكر في الأساليب والإدارة**، دار الحامد للنشر والتوزيع،، عمان، 2004م، ص18.

*تغييرات البيئية حيث تؤدي إلى تغيير الإحتياجات التي على أساسها بني نظام المعلومات، وبالذات تأثير البيئة الخارجية ولذلك فإن المعلومات لا يمكن أن تنتهي يكتمل بناؤها لأنها في حالة بناء مستمر وبالتالي يصبح تحديث نظام المعلومات أمرا ضروريا بالرغم من التكلفة .

*تسارع تغير تكنولوجيا الحاسب الألي .[1]

4-المداخل المعاصرة لدراسة نظم المعلومات الإدارية:

هناك العديد من العلوم ومجالات المعرفة التي تستخدم فيها دراسة نظم المعلومات الإدارية ومن هنا كان لابد من التعرف على إسهامات هذه العلوم والمجالات والربط بينها بغرض التوصل إلى إطار عام يسهل من خلاله فهم عناصر ومكونات وأساليب تشغيل هذه النظم، وبصفة عامة يمكن التمييز بين ثلاثة مداخل لدراسة نظم المعلومات الإدارية وهي:

***المدخل التقني(Approche Technique):**

طبقا لهذا المدخل فلقد تمت دراسة نظم المعلومات الإدارية كمجال جديد للدراسة، من خلال التركيز على تنمية نماذج معيارية والمستمدة أساسا من علوم ذات طبيعة كمية، كالإعلام الآلي، علوم التسيير وبحوث العمليات وبالنسبة للإعلام الالي فقد كان له الدور من خلال وضع النظريات وطرق الحساب، وكذا أساليب تخزين واسترجاع البيانات، وركزت علوم التسيير على البحث عن نماذج لاتخاذ القرارات ونماذج للتطبيقات الإدارية، أما بالنسبة لبحوث العمليات بالأساليب الكمية في إتخاذ القرارات وحل المشكلات .

***المدخل السلوكي (Approche comportementale):**

شغلت الدراسات في نظم المعلومات والتي انصبت حول المسائل السلوكية جزءا كبيرا، فالمدخل التقني وحده غير كاف لمعرفة بعض الجوانب كالتكامل الإستراتيجي للمؤسسة، تصميم وتطبيق استخدام نظم المعلومات، فلقد شاركت العديد من العلوم السلوكية من خلال المفاهيم والطرق التي جاءت بها في إثراء الدراسات التي تنتمي إلى هذا المجال.[2]

---

[1] الشوابكة عدنان: **دور نظم وتكنولوجيا المعلومات في إتخاذ القرارات الإدارية**، دار اليازوري العلمية للنشر والتوزيع، عمان، 2001، ص55.

[2] – مرمي مراد: **أهمية نظم المعلومات الإدارية كأداة للتحليل البيئي في المؤسسات الصغيرة والمتوسطة** الجزائرية، مرجع سابق، ص29.

***المدخل التقني –الاجتماعي (Approche Sociotechnique):**

لايوجد مدخلا واحدا نستطيع من خلاله الكشف عن حقيقة تعقد نظم المعلومات، لذلك يكون من الضروري لفهم هذا التعقد أن يستخدم منظور متعدد الأبعاد يشمل على الجوانب الاجتماعية والتكنولوجية، كما أن أخذ هذه الجوانب مجتمعة في دراسة النظم سوف يحقق الفعالية في أداء النظام، وبالتالي تحقيق أحسن عائد تنظيمي للمؤسسة وهذا يعني أن التكنولوجيا يجب أن تطور بحيث تلبي احتياجات المؤسسات والأفراد، ومن ناحية أخرى تجنب تغير هيكل المؤسسات ومواقف الأفراد عن طريق التكوين والتعليم، حتى يتم استعاب التطورات التكنولوجية وبذلك تصل كل من التكنولوجيا والأفراد إلى تحقيق فاعلية أداء النظام ككل داخل المؤسسة.[1]

–رأينا من خلال هذا المبحث أن ما تقوم به المعلومات الإدارية من وظائف داخل المؤسسة، جعلها تكتسي أهمية بالغة في حياة الأشخاص الطبعيين والاعتباريين باعتبارها أحد الموارد التي لا يمكن أن تستغني فيها المؤسسات في القيام بأعمالها ونشاطاتها في ظل مايشهد العصر من تطورات متسارعة متلاحقة وفي ضوء التحديات التي تواجهه هذه النظم.

[1] – مرمي مراد: **أهمية نظم المعلومات الإدارية كأداة للتحليل البيئي في المؤسسات الصغيرة والمتوسطة** الجزائرية، مرجع سابق، ص30.

خلاصة الفصل:

إن التطور الكبير لتكنولوجيا المعلومات والاتصالات كان له الأثر الكبير في تحسين وتطوير مايعرف بنظم المعلومات الإدارية والمطبقة في معظم المؤسسات باعتبارها موردا حيويا بالنسبة لجميع أنواع المؤسسات، خاصة في ظل التحولات السريعة التي تشهدها بيئة أعمال المؤسسات، وحاجة القائمين عليها إلى إتخاذ قرارات سريعة وحاسمة، فإن تصميم وبناء نظم معلومات إدارية فعالة يصبح ضرورة ملحة، حيث تمكن هؤلاء المسيرين من الإحاطة بما يحدث من تغيرات في البيئة الخارجية وما تفرضه من فرص أو تهديدات وكذلك معرفة مايجري في جميع وضائف المؤسسة من خلال اعتماد المؤسسات على رقمنة إداراتها وحماية شبكاتها وبرامجها ونظم معلوماتها الإدارية ضد الهجمات الرقمية.

الفصل الثاني: الإطار النظري والمفاهيمي للأمن السيبراني.

تمهيد

المبحث الأول: مقاربة معرفية لمفهوم الأمن السيبراني .

1-مفهوم الأمن السيبراني وأهم المفاهيم المرتبطة به.

2-نشأة الأمن السيبراني .

3-الفرق بين الأمن السيبراني وأمن المعلومات .

4-خصائص الأمن السيبراني وأهدافه .

المبحث الثاني: الأمن السيبراني، مبادئه وأبعاده وأهميته وتحدياته.

1-مبادئ الأمن السيبراني .

2-أبعاد الأمن السيبراني .

3-أهمية الأمن السيبراني .

4-تحديات الأمن السيبراني .

المبحث الثالث: الثقة الرقمية والأمن السيبراني .

1. مفهوم الثقة الرقمية .
2. متطلبات بناء الثقة الرقمية .
3. دور الثقة الرقمية في تعزيز الأمن السيبراني .

خلاصة الفصل

تمهيد:

أصبح الانترنت الجهاز العصبي المركزي في المجتمع وبين فئات الشباب والأجيال الواعدة بل أصبحت كافة القطاعات وبشكل أساسي تعتمد على البنية التحتية الحيوية لتكنولوجيا المعلومات والاتصال، و في ظل تزايد إقبال المجتمعات الحديثة على تقنيات الاتصال والمعلومات المرتبطة بهذه الشبكة العالمية، رافق هذا الاعتماد المستمر تشكل مجموعة من المخاطر الناشئة والمحتملة التي تهدد بشكل رئيسي تلك الشبكات وأمن المعلومات ومجتمع المعلومات وأفراده، وعليه فإن الأمن السيبراني الفعال أصبح ضرورة وسيلة فعالة للحماية.

وسنحاول في هذا الفصل الإطار النظري والمفاهيمي للأمن السيبراني، من خلال ثلاث مباحث رئيسية جاء الأول تحت عنوان مقاربة معرفية حول الأمن السيبراني وضم في طياته أربعة عناصر جاءت بالترتيب التالي مفهوم الأمن السيبراني وأهم المفاهيم المرتبطة به، ثم نشأة الأمن السيبراني ومن ثم عرض الفرق بين الأمن السيبراني وأمن المعلومات وخصائص الأمن السيبراني وأهدافه .وخصص المبحث الثاني لعرض مبادئ الأمن السيبراني وأبعاده وأهميته وتحدياته. وجاء المبحث الثالث تحت عنوان الأمن السيبراني والثقة الرقمية وضم في طياته مفهوم الثقة الرقمية ومتطلبات بناءها ودور الأمن السيبراني في تعزيز الثقة الرقمية.

-المبحث الأول مقاربة معرفية حول الأمن السيبراني .

1-مفهوم الأمن السيبراني وأهم المفاهيم المرتبطة به .

أ-مفهومه:

تعددت التعريفات المقدمة حول مفهوم الأمن السيبراني باعتباره من المفاهيم المثيرة للاهتمام والدراسة ومن بين هذه التعريفات نذكر مايلي:

يعرف الأمن السيبراني على أنه مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.[1]

هو النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويتضمن إمكانية الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ماكان عليه، بأسرع وقت ممكن، بحيث لا يتوقف عجلة الانتاج وبحيث لا تتحول الأضرار إلى خسائر دائمة. ويعرف أيضا بأنه العملية أو النشاط والقدرة أو نظم المعلومات واتصالات الدولة، حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف والاستخدام غير المصرح به أو التعديل والاستغلال.[2]

الأمن السيبراني مجموعة وسائل من شأنها الحد من خطر الهجوم على البرمجيات وأجهزة الحاسوب أو الشبكات، وتشمل تلك الوسائل والأدوات المستخدمة في مواجهة القرصنة وكشف الفيروسات ووقفها وتوفير الاتصالات المشفرة.[3]

---

[1]-منى الأشقر جبور: **الأمن السيبراني، التحديات ومستلزمات المواجهة**، المركز العربي للبحوث القانونية والقضائية، 2012، ص16.

[2]- بارة سمير: **الأمن السيبراني في الجزائر السياسات والمؤسسات**، المجلة الجزائرية للأمن السيبراني، العدد4، ص257.

[3]- طمطامي سالم: **الصحافة الإلكترونية والأمن السيبراني-دراسة حالة الجزائر**، مذكرة ماستر، تخصص صحافة مطبوعة وإلكترونية، جامعة أحمد درارية، أدرار، ص16.

وكتعريف اخر نجد أنه مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية، والمبادئ التوجيهية، من المخاطر المحدقة بالمعلومات ومعالجتها والإجراءات والتدريب وأفضل الممارسات وضمان التقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المستخدم.

وعرف أيضا على أنه فن ضمان وجود واستمرارية مجتمع المعلومات للأمة، وضمان وحماية فضاء الانترنت والمعلومات الخاصة به، والأصول البنية التحتية الحيوية.[1]

الأمن السيبراني حزمة العمليات والإجراءات التي يتم اتخاذها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجوم أو السرقة أو الإختراق أو التلف، ويشمل الأمن السيبراني مجموع الوسائل التقنية والتنظيمية والإدارية، لمنع سوء استغلال وضمان عمل منظم للمعلومات وحماية للسرية والخصوصية ومواجهة مخاطر الفضاء السيبراني.[2]

ب-أهم المفاهيم المرتبطة بالأمن السيبراني:

***الفضاء السيبراني:**

الفضاء السيبراني بيئة تفاعلية جديدة تشمل عناصر مادية وغير مادية، مكون من مجموعة من الأجهزة الرقمية وأنظمة الشبكات والبرمجيات والمستخدمين سواء مشغلين أو مستعملين.[3]

الفضاء السيبراني هو مجال افتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنت وكم هائل من المعلومات والأجهزة، كما أن هناك من عرف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة.[4]

عرفته الوكالة الفرنسة لأمن أنظمة الإعلام Anssi على أنه فضاء التواصل المشكل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية، وعرفه الاتحاد الدولي للاتصالات الذي يصف الفضاء

[1]-بارة سمير: **الأمن السيبراني في الجزائر السياسات والمؤسسات**، مرجع سابق، ص258.

[2]-بلعسل بنت نبي ياسمين، عمروش الحسين: **التهديدات الإلكترونية والأمن السيبراني في الوطن العربي**، مجلة نوميروس الأكاديمية، المجلد2، العدد2، 2021، ص22.

[3]-إسماعيل زروقة: **الفضاء السيبراني والتحول في مفاهيم القوة والصراع**، مجلة العلوم القانونية والسياسية، العدد1، المجلد10، 2019، ص1017.

[4]-عباس بدران: الحروب **الإلكترونية الاشتباك في عالم متغير**، مركز دراسات الحكومة الإلكترونية، بيروت، 2010، ص4.

السيبراني بأنه المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي أجهزة الكمبيوتر، الشبكات البرمجيات حوسبة المعلومات، المحتوى، معطيات النقل والتحكم ومستخدمو كل هذه

العناصر. [1]

***الجريمة السيبرانية:**

هي نشاط إجرامي تستخدم فيه تقنية الحاسب الألي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود، فهي السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية، فهي جرائم العصر الرقمي، وهي كلها تنفذ عن طريق التقنية.[2]

إن الجرائم السيبرانية تعد من الجرائم التي تباينت تسميتها عبر المراحل الزمنية لتطورها، فكانت بداية من مصطلح إساءة استخدام الكمبيوتر، مرورا باصطلاح احتيال الكمبيوتر والجريمة المعلوماتية، فاصطلاحات جرائم الكمبيوتر والجريمة المرتبطة بالكمبيوتر، وجرائم التقنية العالية إلى جرائم الهاكرز فجرائم الانترنت، إلى أخر المصطلحات للجرائم السيبرانية.[3]

***الهجمات السيبرانية:**

معظم التعاريف الواردة بشأن الهجمات السيبرانية تشترك في معنى متقارب وهو استهداف مواقع إلكترونية من خلال وسائل اتصالية إلكترونية أخرى.[4]

وإن كان المختصون في القانون الدولي العام يقرون بأن المصطلح يكتنفه الغموض والالتباس بسبب عدم الاتفاق على تعريف محدد له، فمنهم من تبنى مصطلح الفضاء السيبراني بالاستناد إلى المحيط الذي تجرى فيه الاعتداءات السيبرانية[5].

---

[1]–إسماعيل زروقة: **الفضاء السيبراني والتحول في مفاهيم القوة والصراع**: مرجع سابق، ص5.

[2]–زينب ياقوت:: **دور الإعلام الجزائري في التصدي للجريمة السيبرانية قناة النهار أنموذجا**، مرجع سابق، ص1368.

[3]–عبد العزيز بن غرام الله: **جرائم الانترنت وعقوبتها وفق نظام مكافحة الجرائم المعلوماتية**، دار الكتاب الجامعي، الرياض، 2017، ص20.

[4]–أحمد عيسى نعمة الفتلاوي: **الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عن ضوء التنظيم الدولي المعاصر**، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد4، جامعة بابل، 2016، ص611.

[5]–بن صابر بلقاسم: **الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر**، مجلة حقوق الإنسان والحريات العامة، العدد 4، جامعة عبد الحميد مستغانم، 2017، ص188.

ولقد عرفها بعض الباحثين بأنها فعل يفوض من قدرات وضائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ما يمكن للمهاجم من التلاعب بالنظام. [1]

وتعرف الهجمات السيبرانية على أنها هجوم عبر الفضاء الالكتروني يهاسبات دف إلى السيطرة على مواقع إلكترونية لتعطيلها أوتدميرها أو الإضرار بها.[2]

***القوة السيبرانية:**

عرفها جوزيف ناي على أنها مجموعة من الموراد المتعلقة بالتحكم والسيطرة على أجهزة الحاسبات والمعلومات والشبكات الإلكترونية والبنية التحتية والمعلوماتية والمهارات البشرية المدربة للتعامل مع هذه الوسائل وتجدر الإشارة إلى أن القوة السيبرانية أخذت دفعا مهما في اتجاهين الأول، تدعيم القوة الناعمة للدول من خلال التأثير في توجهات الرأي العام والثاني يندرج في زيادة النفقات من طرف الدول لسياسات الدفاع السيبراني. [3]

2-نشأة الأمن السيبراني:

إذا نظرنا إلى الماضي في التاريخ، نجد أن النواة الأولى للفضاء السيبراني يمكن إرجاعها إلى إندلاع الحرب الأهلية الأمريكية في عام 1861م، في ذلك الوقت تم استخدام التلغراف لأول لإدارة الحرب، حيث أصبح التلغراف جزءا مهما من نظام الحرب، وفي عام 1988م أظهر علماء ألمان أن الطاقة الكهربائية تولد ترددات في الفضاء كإشارات يمكن تنبيها ومراقبتها، وهو اكتشاف أثار الاهتمام حيث أصبح يعرف بترددات هيرتز التي طورها البريطانيون إلى نظام الراديو، كان أول تطبيق عملي لهذه التقنية في عام 1904م، أثناء الحرب الروسية اليابانية، عندما قصفت سفينتين حربيتين يابانيتين (كاسوجا) و(تسين) القاعدة البحرية الروسية في ميناء أرثر، وكان لديهم سفينة صغيرة تقوم بمعايرة النيران باستعمال راديو (اللاسيلكي)[4].

---

[1]-بن صابر بلقاسم: **الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر**، مرجع سابق، ص188.

[2]-أحمد عيسى نعمة الفتلاوي: **الهجمات السيبرانية**، مرجع سابق ص614.

[3]-يوسف يوغرارة: **الأمن السيبراني الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني**، المركز الديمقراطي العربي، مجلة الدراسات الإفريقية وحوض النيل، المجلد1، العدد3، 2018، ص108.

[4]-قطاف سليمان: **الأمن السيبراني والمضامين المرتبطة به**، مجلة طبنة للدراسات العلمية الأكاديمية، العدد02، المجلد05، جامعة الأغواط، 2022، ص44.

إن الحربان العالميتان اللتان شهدهما العالم في النصف الأول من القرن العشرين كانت نقطة الانطلاق للتفكير في دور التكنولوجيا في إدارة الصراع وتحقيق النصر، لذلك سعت الدول المتحاربة إلى تطوير القدرات التكنولوجية المتمثلة في الاتصالات اللاسيلكية (الرادار). وفي أوائل التسعينات أصبح التركيز على المعلومات مصدرا

للميزة التنافسية، لذلك بدأت التطبيقات الأمنية في حماية كل مايتعلق بجمع المعلومات وتخزينها ومعالجتها وتسليمها داخل المؤسسة من المنافسين الذين يحاولون الحصول عليها، إنه غير قانوني ويسمى(أمن المعلومات أو من نظام المعلومات) بالإضافة إلى الحماية المادية، ومع انتشار استخدام تكنولوجيا المعلومات والاتصالات، وتم توسيع مفهوم أمن الشبكات ليشمل حماية التجارة الالكترونية بين الأطراف داخل الوكالة التجارية والإدارة، وكذلك الرهانات المختلفة على مستوى التهديدات السيبرانية وعلى المستوى الاستراتيجي، مثل الحرب السيبرانية والدفاع السيبراني، على المستوى القانوني، مثل المراقبة الالكترونية وحماية الحياة الخاصة، وعلى المستوى الاقتصادي مثل المنافسة والحاجة للإبداع، وللأمن السيبراني أبعاد متعددة ومختلفة.[1]

3-الفرق بين الأمن السيبراني وأمن المعلومات:

يعرف أمن المعلومات من الناحية القانونية على أنه مجموعة الإجراءات والقوانين التي يتم فرضها بهدف تأمين كل المعلومات والوسائط والأجهزة المستخدمة في حفظ ومعالجة وتبادل المعلومات عبر الشبكة.[2]

أما من الناحية التقنية يعرف على أنه مجموعة الإجراءات والتدابير القانونية التي تستخدم سواء في المجال الفني أو الوقائي لصيانة المعلومات مثل الأجهزة والبرمجيات والبيانات المتعلقة بالتطبيقات وكذلك الأفراد العاملين في مجال ويشير كذلك أمن المعلومات إلى الدخول إلى كل موارد المنشأة من قبل أطراف غير محولة باستخدام النظام.[3]

إن العلاقة بين أمن المعلومات وأمن السيبراني هي علاقة جزئية، حيث يتضمن أمن المعلومات حماية المعلومات من الوصول غير المصرح به، وقد تكون المعلومات في شكل مستندات ورقية أو مخزنة على وسائط إلكترونية، ولكن لا يمكننا أن نقول أبدا أن أمن المعلومات يشمل أمان الشبكة تماما، كما لايمكننا

[1]-قطاف سليمان: **المرجع نفسه**، ص45.

[2]-الطائي: **التجارة الإلكترونية**، دار المستقبل الواعد للأجيال القادمة، دار ثقافة للنشر والتوزيع، ، عمان، 2010، ص149.

[3]-السالمي عمر: **تكنواوجيا المعلومات**، دار المنهج، عمان، 2000، ص391.

القول أن أن أمان الشبكة يتضمن أمن المعلومات، ويشمل الأمن السيبراني أمن المعلومات المنقولة أو المخزنة أو المعالجة في أنظمة تكنولوجيا الاتصالات والمعلومات، وهذا صحيح، لكنه يشمل أيضا الحفاظ على توافر أمن الخدمات المقدمة عبر الفضاء السيبراني مثل الطاقة الكهربائية ووسائل الاتصال، لذلك لا يصح القول أن أمن المعلومات يشمل الأمن السيبراني أمن المعلومات لأنه لا علاقة له بأمن المعلومات المكتوبة على المستندات الورقية، وذلك لأنه لا ينتمي إلى نطاق الفضاء السيبراني هي التقاطع من حيث الاهتمام بأمن المعلومات الموجودة بالسايبر، ويختلفان فيما تبقى من الاهتمامات وفي نفس الوقت لا نستطيع استخدام أمن المعلومات والأمن السيبراني كمصطلحين مرادفين تماما.[1]

4-خصائص الأمن السيبراني وأهدافه:

أ-خصائص الأمن السيبراني:

بما أن الجريمة الإلكترونية تتميز بمنهجية وأساليب جديدة ذات بعد تكنولوجي أعلى من الجرائم التقليدية كان لابد أن يأتي الأمن السيبراني للتغلب على هذه المشكلة مواكب التطور التكنولوجي ولذا تميز الأمن السيبراني بعدد من الخصائص منها:

*الاكتشاف والتعقب: حيث يهدف الأمن السيبراني إلى اكتشاف الجريمة الالكترونية وتعقب أثرها وبالتالي التغلب عليها.

*السرعة وغياب الدليل: فصعوبات إثبات الجرائم الإلكترونية نظرا لاستخدام المخترقين وسائل تقنية حديثة عالية تفوق خبرة المجرم .

*ضعف الأجهزة الأمنية والقضائية اتجاه التعامل مع الجرائم الإلكترونية نتيجة نقص الخبرة الرقمية لدى الأجهزة الأمنية مما يعزز دور الأمن السيبراني في تحقيق الأمن الرقمي للمؤسسات والجامعات السعودية في حماية البيانات والبنى التحتية لتلك المؤسسات.[2]

ب-أهداف الأمن السيبراني:

[1]-قطاف سليمان: **الأمن السيبراني والمفاهيم المرتبطة به،** مرجع سابق، ص50.

[2]-عبد الفتاح البيومي: **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، دار الكتب القانونية، مصر، 2007، ص197.

إن أهم هدف للأمن السيبراني هو حماية وتأمين المعطيات والبيانات وحماية الشبكات وأجهزة الكمبيوتر والبرمجيات من أي إختراق سيبراني للوصول غير المصرح به إلى البيانات، وأصبح الغرض من الأمن السيبراني له مهمة الدفاع والقدرة في صد أي هجوم سيبراني في الحرب السيبرانية، وذلك لحماية البنية التحتية من أجل سلامة المواطنين وممتلكاتهم الإلكترونية، نلخص ذلك فيما يلي:

*تأمين البنى التحتية لأمن المعطيات والبيانات الخاصة بالأفراد، لابد من حماية فعالة لجميع مايتعلق بمعلومات الأشخاص وحفظها حفظا أمنا، والأجهزة ومواردها وغيرها من الممتلكات الإلكترونية من أي محاولة أو إختراق أو تعديل لتحقيق الحماية اللازمة .

*حماية شبكة المعلومات والاتصالات اتي تلعب دورا مهما في تدفق البيانات بين المواطنين والدولة من جهة إلى أخرى، والتي إذا تعرضت للخطر أو تم إختراقها يمكن أن تؤثر حتما على هذه الاتصالات وتعطلها، وتوقف تدفق البيانات، العمل وإيقاف الخدمة.[1]

*ضمان استمرارية عمل تطبيقات نظم المعلومات .

*العمل على حماية خصوصية وسرية المعلومات الشخصية سواء للأفراد والمنظمات العامة أو الخاصة .

*استخدام التدابير اللازمة لأجل حماية المواطنين من المخاطر المترتبة على دخول شبكة الانترنت .

*حماية الأجهزة التقنية وكذلك التشغيلية .

*المحافظة على شبكات المعرفة والمعلومات.[2]

وبهذا فالأمن السيبراني يشكل حماية لأنظمة التكنولوجيا من خلال تفعيل أنظمة الحماية للأفراد والمؤسسات.

-رأينا من خلال هذا المبحث أن الأمن السيبراني مفهوم متعدد الأبعاد فهو ذلك النشاط الذي يؤمن حماية الموارد البشرية المالية المرتبطة بتقنيات الاتصال والمعلومات يضمن الحد من الخسائر والأضرار من الهجمات الإلكترونية ويتقاطع مفهوم الأمن السيبراني مع عدة مفاهيم أبرزها الأمن السيبراني حيث يعد مفهومه أوسع يتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكات الداخلية والخارجية في حين

[1]-جوهر الجموسي: **الإفتراضي والثورة مكانة الانترنت في نشأة مجتمع مدني عربي**، المركز العربي للأبحاث ودراسة السياسات، بيروت، 2019م، ص12.

[2]-خالد مخلف الجنفاوي: **التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديمية بالكويت**، المجلة العربية للأداب والدراسات الإنسانية، المجلد5، العدد19، 2021، الكويت، ص11

يشكل أمن المعلومات حماية أنظمة المعلومات من النفاذ غير المصرح أو السرقة أو التعديل أو التشهير الغير المصرح به.

-المبحث الثاني: الأمن السيبراني، مبادئه وأبعاده وأهميته وتحدياته

1-مبادئ الأمن السيبراني

استنادا إلى توجيهات الخبراء الإقلميين والأطر الدولية والإقليمية بشأن الأمن السيبراني، فقد حددت جمعية الانترنت المبادئ الأساسية التالية لتأمين شبكة الانترنت المبادئ التالية:

*الوعي: بتعيين على جميع الجهات المعنية في كل من القطاعين العام والخاص فهم المخاطر التي تهدد أمنها، ومدى تأثير تلك المخاطر عليها وعلى الأخرين في النظام البيئي الخاص بالبنية التحتية لشبكة الانترنت .

*المسؤولية: يجب على جميع الجهات المعنية تحمل مسؤولية مواجهة المخاطر الأمنية في إطار أدوارها ومؤسساتها، مع الأخذ في عين الاعتبار للأثار المترتبة على اتخاذ إجراء ما أو التقاعس عن تنفيذه .

*التعاون: يجب إشراك جميع الجهات المعنية بما في ذلك الأطراف المعنية خارج الحدود، في حوار مستمر حول الأمن السيبراني لمواجهة التهديدات الجديدة والمستمرة ومواجهة فعالة .[1]

-وهناك ثلاثة معايير أخرى أساسية اتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار إليها بمثلث أو ثلاثي وهي السرية والأمانة والتوافر .

*السرية: ويقصد بها عدم كشف المعلومات لغير أطرافها بما يوفر الخصوصية والسرية للمعلومات المتداولة على الفضاء الرقمي .

*الأمانة: وتعني عدم التلاعب بالمعلومات أو حذفها أو تعديلها بحيث يضمن المستخدم دقة نقل مايريد من معلومات دون تدخل في أثناء النقل أو التخزين أو المعالجة .

*التوافر: أما فيما يخص فهو استمرار توفر المعلومة للشخص أو الجهة التي يسمح لها المستخدم بالاطلاع عليها عند الحاجة. [1]

[1]- مجتمع الانترنت: **المبادئ التوجيهية المتعلقة بأمن البنية التحتية للانترنت في الدول العربية**، مجتمع الانترنت، 2020، ص2.

2-أهمية الأمن السيبراني:

للأمن السيبراني أهمية بالغة في الفضاء السيبراني، خاصة ما تعلق بالجانب الوقائي للبيانات، والمعلومات والاتصالات المختلفة وتكمن هذه الأهمية في النقاط التالية:

*إستكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها .

*توفير بيئة عمل أمنة جدا خلال العمل عبر الشبكة العنكبوتية .

*الحفاظ على المعلومات وتجانسها وسلامتها وذلك بكف الأيادي من العبث بها، وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها .

*يحمي الأمن السيبراني مختلف أنواع البيانات الحساسة والمهمة من تعرضها للسرقة أو الإتلاف.

*يحمي الأمن السيبراني مختلف أنواع البيانات الحساسة والمهمة من تعرضها للسرقة أو الإتلاف.

*تعرض الأمن السيبراني للإختراق من شأنه أن يحدث الكثير من الأضرار التي تلحق بسمعة الشركة أو المؤسسة وبالتالي تؤثر على مستوى التعاملات التي تقوم بها في الأسولق التجارية. [2]

3-أبعاد الأمن السيبراني:

***البعد العسكري:**

تكمن الميزة النسبية للقوة السيبرانية في قدرتها على ربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الإلكتروني، بما يسمح بسهولة تبادل المعلومات وتدفقها، وسرعة إعطاء الأوامر العسكرية، والقدرة على إصابة الأهداف عن بعد وتدميرها، وقد تتحول هذه الميزة إلى نقطة ضعف إن لم تكن الشبكة الإلكترونية المستخدمة في ذلك مؤمنة جيدا من أي إختراق خارجي قد يتسبب في شن هجمات إلكترونية مضادة على شبكات القوات المسلحة وأجهزة الاستخبارات.[3]

---

[1]-مركز هيدور: **الأمن الرقمي وحماية المعلومات الحق في استخدام شبكة أمنة،** مصر، مركز هيدور، ص70.

[2]-طمطامي سالم: **الصحافة الإلكترونية والأمن السيبراني-دراسة حالة الجزائر**، مذكرة ماستر، مرجع سابق، ص39.

[3]-محمد الأمين البشري: **التحقيق في جرائم الحاسب الألي،** بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات، 200، ص39.

***البعد الإقتصادي:**

أصبح الفضاء الإلكتروني جانبا لقطاعات المجتمع كافة، إفرادا وجماعات وزاد الاعتماد بصورة أساسية على التكنولوجيا الرقمية في تخزين البيانات والمعلومات، بالإضافة إلى إستخدام الحاسب الألي في تطوير الصناعات وتحريك الإقتصادات، وأصبحت المعاملات المالية والإقتصادية محوسبة، وباتت شبكات البنوك والبورصات وشركات الأسواق المالية مرتبطة ببعضها البعض بنظم وشبكات إلكترونية، فأصبحت الانترنت هي أساس المعاملات المالية والاقتصادية وباتت تشكل محورا رئيسيا للتطور الاقتصادي في القرن الحادي والعشرين ن وهو ما أثار الحديث عن أهمية تحقيق الأمن السيبراني في المجال الإقتصادي.[1]

***البعد القانوني:**

تعد العلاقة بين القانون بين القانون والتكنولوجيا علاقة تبادلية، فالتطورات التكنولوجية المختلفة تفترض مواكبة التشريعات القانونية لها من خلال وضع أطر وتشريعات للأعمال القانونية وغير القانونية منها. [2]

***البعد الاجتماعي:** تعتبر الشبكة الدولية للمعلومات مجالا مفتوحا لجميع لجميع الأفراد حيث يمكن لجميع المتعاملين السيبرانيين أن يستفيدو من البنية التحتية والخدمات المتاح لهم دون تحمل المخاطر الأمنية وهنا يجب التمويه إلى ضرورة التحسيس بأخلاقيات الأمن السيبراني .[3]

***البعد السياسي:** لقد اصبح بإمكان المواطن أن يتحول إلى لاعب أساسي وأصبح بإمكانه الاطلاع على الخلفيات القرارات السياسية عبر الكم الهائل من المعلومات التي سهل عليه الوصول لها عن طريق الانترنت وهنا نشير إلى التسريبات للوثائق الحساسة مثلا والتي تثير مشكلات عويصة وأيضا دور شبكات التواصل الاجتماعي في تنظيم الدعايات السياسية والانتخابية وتنظيم التظاهرات الإفتراضية ....إلخ، وأصبح الفضاء السيبراني ملاذا للتجنيد من طرف التنظيمات الإرهابية والعديد من الإيديولوجيات والدعايات الدينية. [4]

4-تحديات الأمن السيبراني:

*الإنسان: إن أكبر وأخطر تحديات الأمن السيبراني هي العنصر البشري والمتمثل فيمايلي:

---

[1]- عبد الفتاح البيومي: **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، مرجع سابق، ص197.

[2]-هلالي عبد الله أحمد: **إتفاقية بودابست لمكافحة الجرائم المعلوماتية**، دار النهضة العربية، ط1، القاهرة، 2007م، ص129.

[3]-طمطامي سالم: **الصحافة الإلكترونية والأمن السيبراني**، مرجع سابق، ص25.

[4]- هلالي عبد الله أحمد: **إتفاقية بودابست لمكافحة الجرائم المعلوماتية**، مرجع سابق، ص135.

-التمكن من التحكم في ردود الفعل العاطفية .

-السياسة الأمنية معقدة وتستند إلى أحكام بشرية .

-أنظمة الأمن هي من تصميم الإنسان والإنسان هو الذي يسيرها ويثبت معاييرها ويستعملها.

-إساءة استخدام الحقوق: حتى نظام أو تطبيق جيد وموثوق به يمكن أن يتعرض للهجوم من قبل الأشخاص الذين ينتهكون حقوقهم .

-الموارد البشرية: يعد نقص المتخصصين في مجال أمن منظومات الأمن تحديا حقيقيا للشركات.

*المنظومات تخاطر عند استعمالها للأمن السيبراني .

*الإبتكار في خدمة الهجمات السيبرانية ولهذا فإن المراقبات التقليدية للمخاطر يجب أن تتكيف مع التهديدات الحالية والمستقبلية.

*ظهور تقنيات جديدة وبالتالي نقاط ضعف جديدة وباستمرار وحتى للشركات التي لديها موارد لابأس بها.

*توسع وتطور رقعة الهجومات السيبرانية وذلك راجع إلى الإرتفاع المذهل لعدد الأشياء المتصلة بالانترنت، وكذا مستعملي الإنترنت من جهة وتهديدات الدول فيما بينها والذي أدى إلى تصاعد عدد ب الحروب السيبرانية والتجسس السيبراني من جهة أخرى.

*التشفير له نقاط ضعف وكلمات المرور يمكن كسرها.[1]

اتضح من خلال هذا المبحث أن الأمن السيبراني بمبادئه وأبعاده السياسية والاقتصادية والاجتماعية والقانونية مرتبط بالتحول الرقمي الناجح الذي يعتمد على أطر وأليات وبيئة تشريعية متقدمة داعمة للرقمنة والبنية التحتية التي من خلالها يتم حماية جميع أنواع الأجهزة الخاصة المحمولة والمعدات التقنية من خطر الهجمات والاختراقات السيبرانية، مما يخوله أهمية كبرى على مستوى الصعيد الدولي والمحلي واللجوء إلى الاعتماد على سياسات مرنة وتطويرها لتحقيق الأمن السيبراني وتجاوز تحدياته.

[1]-ساعد بوقرص: **الامن السيبراني مخاطر وتهديدات تتطلب ممارسات وتوصيات واستراتيجيات خاصة**، مجلة الأبحاث في الحماية الإجتماعية، العدد3، جامعة العلوم والتكنولوجيا، هواري بومدين، وهران، 20022، ص74.

المبحث الثالث: الثقة الرقمية والأمن السيبراني .

1-مفهوم الثقة الرقمية:

تعرف الثقة بشكل عام بأنها احتمال ذاتي بأن يتوقع أحد الفاعلين أن يقوم فاعل أخر بعمل معين تعتمد عليه فائدته، بعبارة أخرى هي رغبة شخص في الاعتماد على شخص أخر في سياق معين يشعر فيه بالأمان حتى لو صاحب ذلك حدوث عواقب سلبية.[1]

تعرف الثقة الرقمية بأنها استخدام البيانات والمعلومات والأنظمة والشبكات في إطار من الطمأنينة محفوظة ومحمية من هجمات المجرمين الرقميين، وأنه يمكن استرداد البيانات والمعلومات اللازمة بالوقت المناسب.

والثقة الرقمية هي واحدة من عوامل نجاح الجامعات وقدرتها على تأدية رسالتها ورؤيتها .[2]

حيث أشارت كليمان أن الثقة الرقمية أن تقوم المؤسسة على توفير المتطلبات العصرية والرقمية والاتصالية، وتضمن الاستخدام الأمن لها، وأن المستخدم يمكنه الإعتماد على البيانات والمعلومات، وأن مايحصل عليه هو أمن وصادق، فالثقة الرقمية من متطلبات إرساء مجتمع المعرفة وإدارة المعرفة

وأنها أصبحت جزء من الميزة التنافسية لكثير من المؤسسات خاصة الأكاديمية وفي ظل بيئة تعلم إلكترونية فإن هناك حاجة لإرساء قواعد ومبادئ الثقة الرقمية، وان يكون هناك نماذج وبرامج حماية تساهم تسهم في

تعزيز ثقة المستخدم بالتقنيات والبرامج وأن يدرك المستخدم أنه في مكان

رقمي أمن.[3]

---

[1]-خادم نبيل، مقدم أحلام: **دور بناء الثقة في تطوير المعاملات الرقمية (فرنسا أنموذجا)**، مجلة الفكر القانوني والسياسي، العدد01، المجلد 05، 2021م، ص143.

[2]-منير عبد الله مفلح البيشي: **الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس –دراسة على جامعة بيشة–**، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، العدد06، مجلد، 29، 2021، ص356

[3]- منير عبد الله مفلح البيشي: **الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس**، مرجع سابق، ص356.

2-متطلبات بناء الثقة الرقمية:

يتطلب بناء الثقة الرقمية تحديد مواصفات خاصة للخدمات الإلكترونية، تحظى بثقة المستخدم وتشعره بالأمان، إضافة إلى توفير بيئة قانونية وفيما يأتي أهم متطلبات بناء الثقة الرقمية .

*ثقة المستخدم بالبيئة الرقمية:

يشكل انعدام ثقة المستخدمين بالعالم الرقمي أحد أهم الأسباب التي تحول دون استثمار الإمكانيات الكامنة للانترنت وتطوير تطبيقات وخدمات إلكترونية جديدة، حيث يعد عنصر الثقة والأمان أبرز العناصر اللازمة لتوفير بيئة مواتية لبناء مجتمع المعلومات، إذ يرتبط إستخدام الأفراد للخدمات الإلكترونية على شعورهم بالراحة والطمأنينة والأمان عند استخدامها.

*البنية الأساسية والنظم المعلوماتية:

في ظل اتساع نطاق شبكة الانترنت، أصبح المجرمون قادرين على إيجاد فرص جديدة في البيئة الرقمية القابلة للخرق، وذلك القيام بأعمال إجرامية ضدها أو ضد البنية الأساسية الوطنية، وأصبحت البرمجيات الخبيثة والاعتداءات على الشبكات والنظم عن بعد معروفة بالنسبة لمستخدمي شبكة الانترنت ولا ينجو منها إلا المستخدمون المحصنون.[1]

*الإطار القانوني للتحول الرقمي:

يستغل المجرمون غياب نظام المساءلة، والثغرات في بنى تكنولوجيا المعلومات والاتصالات وأنظمتها وأنظمتها في التشريعات الوطنية لارتكاب الجرائم المعلوماتية وخاصة في البلاد التي لم تسن قوانين تجرم الاعتداءات المعلوماتية أو التي لا تطبق هذه القوانين، وقد وضعت بعض البلدان قوانين لمكافحة الجرائم المعلوماتية وسوء استخدام تكنولوجيا المعلومات والاتصالات، ولكن تطبيقها مازال يواجه عددا من الصعوبات، لاسيما في المنطقة العربية في غياب أليات للتطبيق ومحاماة وقضاة مدربين على تطبيقها.

*ضعف البنية الأساسية:

يشكل غياب البنية التنظيمية إحدى الإشكاليات التي تعيق حماية الفضاء السيبراني، فالمؤسسات والشركات التي تستخدم تكنولوجيا المعلومات والاتصالات لا تعتبر عنصري الحماية والأمان أساسيين في حالات عديدة، ولا تستحدث في هيكلها المؤسسي أية إدارة أو حدة تختص بمراقبة أمن

[1]-رضا حسين قنديل: **أثر مشاريع التحول الرقمي في تحسين بطاقة أداء الثقة الرقمية بالتطبيق على وزارة التربية والتعليم**، المجلة العربية للإدارة، العدد01، مجلد 45، مصر، ص8.

تكنولوجيا المعلومات والاتصالات وتطبيقاتها وبحمايته وضمانه، كما أنها لا تخضع أية سياسات أو خطط عمل لمواجهة التهديدات المعلوماتية الخارجية.[1]

3-دور الثقة الرقمية في تعزيز الأمن السيبراني

مع اتساع انتشار البرمجيات الخبيثة كالفيروسات والديدان المتطفلة والبرمجيات التجسسية التي أصبح المستخدمون بحاجة إلى التدرب على أليات الحماية الشخصية من التهديدات الخارجية، والتوعية بضرورة التعامل بحذر مع الخدمات المقدمة عبر الفضاء السيبراني لحماية معلوماتهم وممتلكاتهم الشخصية الحاسوبية .

حيث أن موضوع الثقة بالخدمات الإلكترونية موضوع متشعب وذو أبعاد مختلفة وهو يتطلب تظافر جهود جهات وطنية مختلفة في القطاعين العام والخاص لبناء الثقة بالعالم الرقمي وتعزيز أمنه، ويعتبر عامل الثقة لتكنلوجيا المعلومات والاتصالات موضوعا شأنه في مجتمع المعلومات .

فالثقة تحتاج إلى الحماية والأمن على المستوى التكنولوجي ووضع التشريعات السيبرانية وتطبيقها إلى جهود كبيرة وإلى توفر كوادر بشرية تملك الكفاءة اللازمة لتشغيل النظم المعلوماتية واستثمارها.

ومن أجل الإحاطة بمختلف الاحتياجات، لا بد بكل بلد أن يضع إطارا وطنيا عاما لتوضيح احتياجاته من حيث تطوير الخدمات الإلكترونية واستخدامها وطنيا لما لتلك الخدمات من أثر إيجابي على تطوير مجتمع المعلومات ونمو الهياكل الاقتصادية والاجتماعية .

من المؤكد أن بناء الثقة بالخدمات الإلكترونية وتعزيز أمنها لايقتصر على حماية أمن النظم المعلوماتية والشبكية فحسب، بل يتطلب كذلك تحديد مواصفات خاصة للخدمات الإلكترونية تحظى بثقة المستخدم وتشعره بالأمان، وتوفير بيئة قانونية ملائمة للفضاء السيبراني تحمي مستعملي هذه الخدمات ومستثمريها من الإعتداءات والاستخدامات غير اللائقة.[2]

رأينا من خلال هذا المبحث ان تحقيق الثقة الرقمية يعتمد على إرساء قواعد وأنماط من الثقافة السيبرانية التي تعزز قدرة المستخدم على حماية بياناته من التلف والهجمات الرقمية وعليه يتكفل الأمن السيبراني بكافة الإجراءات التي يمكن أن تعزز ثقة المستخدم الرقمية .

---

[1]- رضا حسين قنديل: **أثر مشاريع التحول الرقمي في تحسين بطاقة أداء الثقة الرقمية بالتطبيق على وزارة التربية والتعليم**، مرجع سابق، ص08.

[2]-لعربي أسيا: **بناء الثقة بالخدمات الإلكترونية بمنطقة إسكوا**، اللجنة الاقتصادية والاجتماعية، ص ص1-4

.

-خلاصة الفصل:

لقد ظهر مفهوم الأمن السيبراني عالميا بشكل مزامن لبروز ثورة الانترنت والمعلومات ونمو القطاع الرقمي، وفي ظل التطور الرهيب في مجال الإعلام الالي وتكنولوجيا الاتصالات والمعلومات والإيجابيات التي حملتها الشبكة العالمية من جهة، إلا أنها من جهة أخرى حملت العديد من التهديدات والمخاطر التي ترجمت في شكل جرائم إلكترونية أوجب على المنظمات توفير حماية شبكات الكمبيوتر والمعلومات من هذه الهجومات الخبيثة، عن طريق تفعيل برامج وأليات تقنية، وقدرات بشرية لمواجهة تلك التعديات على المعلومات الإلكترونية .

الاطار التطبيقي

متطلبات تحقيق الامن السيبراني لأنظمة المعلومات الادارية لمؤسسات الجامعة

تمهيد:

تحتل الدراسة الميدانية مكانة هامة في البحث العلمي بحيث تسمح للباحث باختيار مختلف ادوات البحثية والوصول الى نتائج علمية ذات مصداقية من خلال تطبيق مجموعة من التقنيات و الطرق المنهجية التي تصور الرؤية الواضحة لموضوع الدراسة.

المبحث الأول: تحليل البيانات الشخصية للمبحوثين

الجنس	التكرار	النسبة
ذكر	5	100%
انثى	0	0%
المجموع	5	100%

جدول يبين طبيعة الوظيفة

الوظيفة	التكرار	النسبة
مهندس	4	80%
استاذ	1	20%
مساعد مهندس	0	0%
تقني سامي	0	0%
المجموع	5	100%

جدول يبين الأقدمية في العمل

الأقدمية	التكرار	النسبة
من سنة الى 3 سنوات	1	20%
من 6 سنوات الى تسعة سنوات	1	20%
من عشرة سنوات فما فوق	3	60%
المجموع	5	100%

جدول يبين البيانات الشخصية للمبحوثين

الرقم	الجنس	الوظيفة	الأقدمية في العمل
01	ذكر	رئيس خلية الاعلام الآلي لرئاسة الجامعة	من عشر سنوات فما فوق
02	ذكر	أستاذ	من سنة الى ثلاث سنوات
03	ذكر	مساعد مهندس اعلام آلي	من ستة سنوات الى تسعة سنوات
04	ذكر	تقني سامي بالمكتبة المركزية	من عشر سنوات فما فوق
05	ذكر	مهندس اعلام آلي (كلية ع إ)	من عشر سنوات فما فوق

المبحث الثاني: مفهوم الامن السيبراني لدى المبحوثين

1- أجمع أغلب المبحوثين على مفهوم الأمن السيبراني في حماية أجهزة الكمبيوتر والشبكات والتطبيقات لغرض الأمن لنظامها المعلوماتية منها الإدارية بعد قراءتنا إلى الإجابات المقدمة لنا تبين لنا أن أغلبية الإجابات كانت متقاربة وتتمحور في محور واحد هو حماية المعلومات من خطر جهات الخارجية لكن بعد بحثنا في هذا الموضوع لاحظنا أن هذا تعريف هو سطحي ولم يكن بالشكل المطلوب.

تعددت التعريفات المقدمة حول مفهوم الأمن السيبراني باعتباره من المفاهيم المثيرة للاهتمام والدراسة، ومن بين هذه التعريفات نذكر الأهم منها: يعرف الأمن السيبراني على أنه مجموعة من الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات وتعزيز الحماية وسرية وخصوصية البيانات الشخصية و اتخاذ جميع التدابير

اللازمة لحماية المواطنين والمستهلكين من مخاطر الفضاء السيبراني وهذا من بين المفاهيم المشابهة للأمن السيبراني.

2- توفر إدارة خاصة بالأمن السيبراني لدى الجامعة إن طبيعة الإدارة المتوفرة هي خلية مصغرة تسهر على وضع نظام الحماية وتطبيقه في الجامعة ومن هنا يتضح لنا أن الجامعة لم تصل بعد إلى تكوين إدارة وفريق مسير لها كما يجب، وإن هذه الخلية غير مفعلة بشكل رسمي حسب بعض الإجابات المقدمة لنا بعدم توفر أي إدارة خاصة بالأمن السيبراني ولا توجد هناك أي حماية للمعلومات بشكل فعلي لعدم امتلاك الجامعة لإمكانيات مادية وبشرية للتقدم إلى الأمام و نحو الأفضل، المكلف بهذه الإدارة هو مسؤول الخلية وطاقمه العامل معه الذي يسهر لتوفير الحماية والأمن للمعلومات من أي هجمات خارجية تهدد المعلومات في الجامعة وهي على شكل محاولات فردية يقوم بها مسؤول هذه الخلية المتواجدة على مستوى رئاسة الجامعة.

3- التزام الوحدات الإدارية و المكلفين بها بالجامعة و بالمتطلبات التنظيمية لتحقيق الأمن السيبراني معظم الإجابات كانت بلا هنا يعني أن الجامعة ليس لها التزام للوحدات الإدارية والمكلفين بها بالجامعة لأن هناك نقص في الإمكانيات وانعدام الخبرة والتجربة تجعل لا تعرف العالم الذي تدور بالدخل لهذا على الخلية المكلفة بهذه المهام الالتزام بالعمل على تطبيق الوحدات الإدارية وإعطاء لها الضوء الأخضر للعمل وكذلك تحديد وسائل الحماية مع وضع الخطط الدورية لأن من أهم أهداف الأمن السيبراني هو حماية وتأمين المعطيات والبيانات وحماية الشبكات وأجهزة الكومبيوتر والبرمجيات من أي اختراق سيبراني للوصول غير المصرح به إلى البيانات والغرض الأساسي من الأمن السيبراني هو مهمة الدفاع والقدرة في صد أي هجوم سيبراني في الحرب السيبراني وكذلك ضمان استمرارية عمل تطبيقات نظام المعلومات.

4- الإجراءات اللازمة لإدارة الأصول المعلوماتية التي صرح بها المبحوثين كانت كالتالي: وضع قاعدة معطيات أمينة تحتوي على جميع الأصول المعلوماتية للموظف مزودة ببرامج حماية البيانات الشخصية اما الإجراء الآخر المقدم تطوير الشبكة المحلية للجامعة ووضع نظام حماية (poscface) متطور للإدارة لأصول الموظفين عن بعد وتسهيل تخزينها والمحافظة عليها، جامعة لا يتوفر لديها إدارة خاصة بالأمن السيبراني كيف لها أن تنجح في وضع إجراءات لإدارة الأصول المعلوماتية.

5- تطبيق نظم إدارة هويات الدخول والصلاحيات، تسهيل الإجراءات الإدارية اللازمة لتحقيق الأمن المعلومات داخل أنظمة المعلومات الإدارية بالجامعة، وجود خطة لإدارة مخاطر الأمن المعلوماتي لأنظمة المعلومات الإدارية للجامعة، تطبيق متطلبات الأمن المعلوماتي في إدارة الأصول المعلوماتية والتقنية بالجامعة، التزام الجامعة بسياسات إدارة أمن الشبكات، توعية العاملين والإداريين والأكاديميين بأهمية تطبيق الأمن المعلوماتي.

حماية الموظفين من أي هجوم سيبراني يجب توفر الإدارة أولا مع تطوير الشبكات بعد نصل إلى مرحلة حماية أصول المعلوماتية وأيضا العمل على حماية خصوصية وسرية المعلومات الشخصية الخاصة بالموظفين سواء للأفراد والمنظمات الخاصة والعامة.

6- طبيعة تدريب الموظفين والإداريين الجامعة على متطلبات تحقيق الأمن السيبراني أجمع على عدم تلقيهم، نستنتج أن الجامعة ليس لها أي مسار نحو تحقيق متطلبات الأمن السيبراني لعدم وضع أي دورات تدريبية أو إعطاء توجيهات إلى الموظفين والإداريين بالجامعة يحثهم للعمل على تحقيق هذا الأمن الذي بمثابة القوة الضاربة للجامعة مما يزيد من قوتها وحماية معلوماتها المهددة من أي خطر في أي لحظة أما جامعات أخرى تولي اهتمام كبير وواسع إلى تحقيق الأمن السيبراني ومتطلباته مثال عن ذلك الجامعة السعودية التي تبرمج للموظفين دورات تكوينية تدربهم على كيفية تحقيق هذه

المتطلبات وأهمية العمل بها لزيادة قوة الرقمنة الخاصة بها، وكذلك جامعة المسيلة بالجزائر التي شهدت قفزة نوعية في مجال الرقمنة وتحقيق متطلبات الأمن السيبراني لحماية معلومات الجامعة ونذكر أيضا جامعة البحرين تنفق المليارات لحماية أنظمتها وشبكاتها كما يذكر أن دولة قطر هي من أكبر الدول المنفقة للأمن السيبراني لحماية معلوماتها الحساسة عكس بعض الدول التي لم تعطي أي اهتمام في ظل التطورات التكنولوجية التي أصبح من الضروري مواكبة هذا العصر الجديد.

7- خضوع الأجهزة الشخصية والمحمولة للموظفين والإداريين متطلبات تحقيق الأمن السيبراني حسب المبحوثين كانت معظم الإيجابيات بلا والآخر منها كانت بنعم لتطبيق فحص الأجهزة الخاصة بالموظفين تثبيت تطبيق الحماية من الفيروسات وتفعيل الجدار الناري كما يسمى بجدار الحماية وهو جهاز أمان للشبكة يراقب ويتحكم في حركة مرور الشبكة الواردة والصادرة بناء على مجموعة من قواعد الأمان والغرض الأساسي منها سماح بضرورة حركة المرور مصرح بها وعادة ما يتم وضعها بين الشبكة الداخلية والإنترنت لحماية الشبكة من التهديدات الخارجية كما يمكن استخدامها أيضا لتقسيم الشبكة إلى مناطق أمان مختلفة لهذا يجب على مسؤول الخلية وطاقمه تفعيل هذا الجدار الناري لحماية الأجهزة الشخصية والمحمولة للموظفين لأنها تعطي حماية كبيرة لهذه الأجهزة وتبعدهم عن الهجمات السيبراني.

8- تطبيق الجامعة لمتطلبات الأمن السيبراني لحماية بيانات والمعلومات الجامعة هناك تناقض في الإجابات للمبحوثين البعض يقول نعم والآخر يلتزم الصمت ويحتفظ بالجواب عن هذا السؤال الذي في نظره حساسة وتهدد معلومات الجامعة، نكرر القول الجامعة التي لا يتوفر لديها إدارة خاصة بالأمن السيبراني وتخصص لموظفيها دورات تكوينية وتدرب على كيفية تحقيق متطلبات الأمن

السيبراني وكذلك عدم توفر الإمكانيات المادية في ميزانية البحث العلمي دفع الاشتراك لبعض البرامج بشكل دوري.

بعد الانتشار الكبير للإنترنت والأجهزة الذكية والأجهزة المحمولة أصبح من الضروري في وقتنا الحالي الانتباه للأمن السيبراني وكيفية حماية أنفسنا في الفضاء الرقمي الذي بات يشكل خطرا كبيرا على المعلومات كما يعد الأمن السيبراني من أكثر المواضيع انتشارا في أيامنا هذه وتعلمه أصبح ضرورة لابد منها أن تفعل في الجامعة.

أما لضمان حماية معلومات الجامعة من أي خطر أو للعمليات السيبرانية تؤدي بالجامعة إلى خطر مجهول لهذا يجب على الجامعة أن تعطي أهمية واسعة للعمل بالأمن السيبراني كما يجب أن تكون هناك لمحة عامة في مشهد الأمن السيبراني ووضع دورات تكوينية من قبل أهل الاختصاص لتزداد الخبرة ويتم تطويرها مع مواكبة رقمنة القطاع.

9- تطبيق الجامعة لمتطلبات الأمن السيبراني لحماية البريد الإلكتروني ذلك بتعاقد الشركة رقم مع واحد عالميا GOOGLE لتحسين الخدمة والاستفادة من الحماية القصوى إرسال إشعارات إنذار للإدارة، تطبيق نظام خاص على مستوى مصلحة الإعلام الآلي لرئاسة الجامعة، أيضا استخدام البريد الإلكتروني الاحترافي هو أن يحتوي على اسم نشاطك التجاري فيه يسهل التواصل ويؤمن المعلومات عكس البريد الإلكتروني العادي، لكن حسب الإجابات التي بحوزتنا الجامعة لا تمنح أي حماية فعلية إلى البريد الإلكتروني الخاص للأسرة الجامعية مجرد محاولات فردية من قبل مستخدمين الأجهزة لهذا يجب على الجامعة تطبيق هذه الحماية، ففي عالمنا الرقمي الحالي باتت التهديدات الأمنية من أهم المخاطر التي تسعى الجامعة الكبرى للتصدي لها للحفاظ على ما لديها من بيانات ومعلومات والتي تعد ثروتها ويتم إرسالها عبر البريد الإلكتروني غالبا.

المبحث الثالث: المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة آكلي محند الحاج

1- برامج الحماية ضد الفيروسات والأنشطة المشبوهة والبرمجيات الضارة للأنظمة المعلومات الإدارية:

أهم شيء هو الجدار الناري الذي يقوم به حماية كاملة لشبكة الإنترنت من خلال تفحص التطبيقات المستعملة وكذلك تصفية المواقع الإلكترونية ومراقبتها وهناك مشكل وحيد يواجه الجامعة ويعرقل هذه العملية هو إجبارية دفع ثمن الاشتراك السنوي الباهظ الذي مفروض على جامعة البويرة دفعه أو حرمان من تلقى هذه الخدمات استعمال تطبيقات الحماية ضد الفيروسات مثل Kasparsky antivirus وأحيانا يكون مجاني استعمال التطبيقات مفتوحة المصدر penservice ذات حماية عالية، كاسبرسكي لاب هي شركة متخصصة في أمن الحواسيب تقدم حلول وتطبيقات لبرامج مضادة للفيروسات مقرها الرئيسي في العاصمة الروسية موسكو ولها مكاتب إقليمية في الصين، واليابان، الولايات المتحدة، فرنسا، ألمانيا، المملكة المتحدة، كوريا، بولندا، وبالنسبة إلى جامعة البويرة هناك مشكل آخر وهو ضعف في ميزانية البحث العلمي التي تمول هذه البرامج وتساهم في كسبها.

2- توفر الجامعة لأنظمة حماية أمنية للأجهزة التقنية للحاسوب:

ومعظم الإجابات كانت بلا إلا إجابة واحدة كان تبرير إجابتها من خلال تطبيق الحماية ضد الفيروسات واقتناء أنظمة المعلومات لتسهيل تحسينها دوريا mise a jour أمن الحاسوب هو فرع من فروع التكنولوجيا المعروفة باسم أمن المعلومات كما هي مطبقة على الحاسوب والشبكات والهدف من أمن الحاسوب يتضمن حماية المعلومات والممتلكات من السرقة والفساد، بينما يسمح للمعلومات والممتلكات ان تبقى منتجة وفي متناول مستخدميها المستهدفين لهذا على الجامعة أن يتوفر فيها تطبيقات الحماية وتفعيل جدار الحماية الرقمي سابق وتعريفه الذي يتحكم في إشارات المرور لشبكات الحاسوب لكي تحافظ على حماية معلوماتها

الهامة من الوصول غير المصرح به أو سوء الاستخدام الذي يؤثر سلبا على الجامعة والموظفين ويهدد معلوماتهم.

3- الإجراءات التقنية المتبعة لحماية البريد الإلكتروني لدى موظفين والمستخدمين:

البريد الإلكتروني للجامعة يعمل تحت رعاية Google (Gmail) الذي يوفر الحماية اللازمة والمثالية بالإضافة إلى طاقم مسير محليا يعمل على مراجعة كل الإنذارات الأمنية الخاصة بحسابات المستخدمين والموظفين بالجامعة وهذا حسب إجابة رئيس مصلحة الإعلام الآلي برئاسة الجامعة عكس ما تم الإجابة عليه من طرف مهندسي بعض الكليات والتزام الصمت، وجب على الجامعة أن تكون لها إجراءات تقنية متبعة لحماية البريد الإلكتروني من أي خطر سيبراني، حماية البريد الإلكتروني هي مصطلح واسع النطاق يصف مختلف الإجراءات والتقنيات المستخدمة في حماية الاتصالات الرقمية داخل المنظمات أو الجامعات يتضمن ذلك إجراءات الأمان التقليدية مثل الكشف عن برامج التجسس، وأمان تسجيل الدخول وتشفير البريد الإلكتروني، بالإضافة إلى أنظمة أرشفة البريد الإلكتروني السحابية أو المحلية والتخلص من الكوارث والنسخ الاحتياطي، من أهم إجراءات التي وجب إتباعها وضع سياسات أمان البريد الإلكتروني استخدام حلول تأمين البريد الإلكتروني، إجراء تدريب لتوعية الموظفين بالمخاطر الأمنية، منع تسرب البيانات وضع الهاتف المحمول في الحسابات، التعاقد مع مقدم خدمات وحلول حماية البريد الإلكتروني موثق.

4- إخضاع إدارة أمن الشبكات لمتطلبات التحقيق الأمن السيبراني:

إن إدارة الأمن المعلوماتي تحتاج إلى قدرات خاصة ومتطورة التي تكون بالتكوين المستمر والعالي في هذا المجال بالإضافة إلى اقتناء أجهزة متطورة أحيانا تكون باهظة الثمن للحصول عليها، وذلك من أجل حماية المصادر الإلكترونية للجامعة، يعرف نظام الشبكات أنه نظام يعني برابط أجهزة الحاسوب مع بعضها البعض باستخدام إحدى تقنيات الاتصالات المخصصة لذلك حيث تهدف هذه العملية إلى تبادل البيانات

والمعلومات، أو بهدف استخدام ومشاركة الأجهزة و شبكتها مع أكثر من جهاز، ويوفر أمن الشبكات الحماية القصوى للبيانات والمعلومات في الشبكات بهدف تجنب المخاطر التي قد تلحق بها مثل الاختراق، ومن الجدير بالذكر أن هذه المخاطر قد تكون داخلية أم خارجية ولهذا يوجد وسائل وأدوات اللازمة لحمايتها.

5- إمكانية استرداد الملفات المحذوفة من جهاز الكمبيوتر:

هناك إمكانية استرداد الملفات المحذوفة حيث يمكن استعادة الملفات المحذوفة من خلال سلة المحذوفات حيث توجد سلة المحذوفات على سطح المكتب، عند حذف ملف أو مجلد ما من حاسوبك لا يتم حذفه بشكل نهائي بل يتم نقله إلى سلة المحذوفات التي تتيح المستخدم استعادته عند حذفه عن طريق الخطأ، لكن لفترة محددة بعدها يتم حذفه نهائيا، وهناك ميزة تسمى بالنسخ الاحتياطي والاستعادة هذه الميزة فريدة من نوعها لأنها تتيح للمستخدمين إنشاء نسخ احتياطية للملفات لاستعادتها لاحقا لاسترداد الملفات المحذوفة نهائيا.

6- تزويد الجامعة بأنظمة عالية الحماية لمستوى أنظمة المعلومات الإدارية:

معظم إجابات كان بلا لأن الجامعة لا تملك أنظمة حماية عالية المستوى لأنظمة المعلومات، لم تصل إلى المستوى المطلوب، وجب تطبيق نظام الجدار الناري Fortgat، يعمل الجدار الناري أو ما يسمى بجدار الحماية عن طريق فحص حركة المرور الشبكة الواردة والصادرة وتطبيق مجموعة من القواعد لتحديد ما إذا كان يجب السماح بحركة المرور أو حظرها، يمكن أن تستند هذه القواعد إلى عوامل مختلفة مثل عناوين IP للمصدر والوجهة ونوع حركة المرور مثل تصفح الويب والبريد الإلكتروني والمنافذ المستخدمة كما يمكن تكوين جداران الحماية لحظر جميع حركات المرور الواردة باستثناء حركة المرور المسموح بها صراحة، أو يمكن تهيئتها للسماح لجميع حركات المرور الواردة باستثناء حركة المرور المحظورة صراحة، يمكن أيضا تسجيلها لكي تمر عبر جدار الحماية مما يوفر للمسؤولين سجلا مفصلا لنشاط الشبكة، كما أنها توفر جدران الحماية ميزات جيدة لأمان مثل اكتشاف التسلل والوقاية منه، ومسح برامج مكافحة الفيروسات والبرامج

الضارة وتصفية المحتوى يمكن أن تساعد هذه الميزات في حماية الشبكة من أنواع مختلفة من التهديدات السيبرانية.

7- إمكانية تأمين نظام أمن شبكي لتبادل المعلومات الإدارية:

حسب آراء البعض أنه لا يوجد هناك نظام تأمين شبكي لتبادل المعلومات الإدارية وكان رأي أحدهم كالتالي: وضع ميثاق الأمن المعلوماتي الخاص بالجامعة وتحسين الأنظمة المعلوماتية لتصحيح الثغرات وتجديد عتاد الحماية لمواكبة التطورات في المجال، كذلك السهر واليقظة الدائمة بالإضافة إلى التكوين المستمر في هذا المجال ما يجعلنا نتأكد أن الجامعة بعيدة كل البعد عن تفعيل أنظمة الحماية أو التأمين لنظام شبكي، كذلك نقص الخبرة وعدم العمل في الميدان مما يصعب تجسيد هذا النظام على أرض الواقع، يجب على المسؤول الأول بالجامعة أن يعطي اهتمام كبير لتفعيل مثل هذه الأنظمة لأنها توفر الحماية القصوى للمعلومات والبيانات كما يجب تدريب الموظفين على كيفية العمل بهذه الأنظمة مع وضع سيناريو أسوأ الذي يحدث في الجامعة أو تعرضها إلى هجمات من جهات خارجية غير مصرحة المصدر كذلك وضع دراسة معمقة للحاجيات و متطلبات تحقيق تطبيق نظام شبكي مزدوج يوفر الأمان والأمن، يعرف الدكتور "عائض الماري" هو: العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها، ومن زاوية تقنية هو: وسائل وأدوات وإجراءات اللازمة توفيرها لضمان حماية المعلومات من أخطار داخلية وخارجية.

8- السماح للموظفين بنقل معلومات خاصة بالعمل للمنزل مع استخدام جهاز الكومبيوتر الخاص للعمل عليها:

هنا كانت أغلبية الإجابات بنعم وتوافق على إجابة موحدة لأن هناك بعض الحالات ذات الآجال المحددة التي تستلزم العمل لساعات إضافية وكذلك على ضيق الوقت في فترة الدوام والعمل الخاص بالموظفين لكن

هناك تعقيب على هذا الإجراء، الموظف عندما يسمح له بنقل معلومات خاصة واستخدام جهاز كمبيوتر الخاص به أن يوفر الحماية اللازمة للمعلومات المسموح له بنقلها أم ليس هناك أي نظام للحماية من فيروسات التي تؤدي بالخطر إلى هذه المعلومات، يجب أن تكون هناك رقابة ولا للإجراءات العشوائية التي تخدم المصلحة العامة قبل التفكير في المصلحة الخاصة.

9- توفر خلية طوارئ في حالة حدوث جريمة واعتداء سيبراني على نظم المعلومات الإدارية:

أغلب الإجابات المقدمة لنا كانت بلا هذا ما يعني أن الجامعة ليس لديها أي مخطط مفعل لحماية معظم معلوماتها الإدارية من أي جريمة سيبرانية، وهذا ما يشكل خطر كبير على نظم معلوماتها وخاصة إن كانت معلومات حساسة تؤدي بالجامعة إلى الهاوية، حيث تعد نظم المعلومات الإدارية إحدى الحقول الهامة للنظرية الإدارية وتطبيقاتها الحديثة في مختلف الأنظمة، ومن مكونات نظم المعلومات الإدارية نجد ما يلي: الأجهزة، البرمجيات، قواعد البيانات، العمليات، الأفراد، ومن أبعادها: البعد التنظيمي من أهم عناصره: الأفراد العاملون، الهياكل التنظيمية، العمليات الإدارية: وهي مجموعة من الأنشطة المترابطة التي تهدف للقيام بإنجاز نشاط معين، الثقافة: وهي القيم والأعراف التي تتبناها وتؤمن بها المنظمات، السياسات: وهي عبارة عن خطة توفر إطار ما لمساعدة المسؤولين في المنظمة في عمليات صنع القرارات بما ساهم في تنفيذ استراتيجية المنظمة وتحقيق أهدافها.

اثر الأمن السيبراني في تعزيز الثقة الرقمية بجامعة آكلي محند اولحاج-البويرة:

سد الثغرات في أنظمة المعلومات الادارية من خلال الأمن السيبراني:

أجمع المبحوثين على أن الأمن السيبراني يعمل على سد الثغرات في أنظمة المعلومات الادارية من خلال تحقيق الحماية اللازمة لها.

فالأمن السيبراني يعمل على توفير بيئة عمل آمنة من خلال العمل عبر الشبكة العنكبوتية وفي استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها والحفاظ على المعلومات وتجانسها وسلامتها وتحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.

مساهمة الأمن السيبراني في تعزيز الثقة الرقمية:

أكد كل المبحوثين على أن لتطبيق الأمن السيبراني دور مهم في تعزيز الثقة الرقمية بالجامعة وذلك من خلال اعتباره جزء من استراتيجية الرقمنة التي تتطلب استعمال الوسائل الرقمية دون اللجوء إلى الأنظمة القديمة التي تأخذ الجهد والوقت، وعلى أنه اهم نقطة لتحقيق أهداف الرقمنة عن طريق تحقيق الحماية للمعلومات الرقمية من كل الهجمات التي قد تشكك في قدرات الجامعة الرقمية.

يتطلب بناء الثقة الرقمية وتعزيزها تزويد المستخدم بالخدمات الالكترونية القائمة على الشفافية في التعامل والتفاعل، بحيث يكون على بينة من السياسات والاجراءات التي تطبقها الجامعة والتي تؤمن الخدمات في مجال حماية المعلومات وضمان أمنها وسريتها.

تطبيق متطلبات الأمن السيبراني لتعزيز الثقة الرقمية:

أجمع المبحوثين على أن تطبيق متطلبات الأمن السيبراني غير كافية لوحدها على الرغم من أنها اساس محوري، بل يجب تضافر الجهود والالتزام بالمتطلبات والواجبات.

يعتبر عامل الثقة بتكنولوجيا المعلومات والاتصالات موضوعا شائكا في مجتمع المعلومات، فالثقة الرقمية تحتاج إلى الحماية والأمن على المستوى التكنولوجي، ووضع التشريعات السيبرانية وتطبيقها والى توفر كوادر بشرية تملك الكفاءة اللازمة لتشغيل النظم المعلوماتية واستثمارها.

كيفية بناء الجامعة لسياستها السيبرانية للحد من حالات التجسس التخريب الرقمي:

حسب إجابات المبحوثين تكون عن طريق إنشاء ميثاق الأمن المعلوماتي الذي يوجه الى رواد الجامعة من اساتذة وطلبة وموظفين وبتخصيص ميزانية لتجهيز الجامعة بكل ما يلزم من عتاد الحماية وتكوين المتخصصين في هذا المجال بالإضافة إلى تحسين كل الأنظمة المستعملة.

فأهمية وضرورة استخدام سياسات الأمن السيبراني في الجامعة تتزايد للتغلب على مشكلات عوائق الاختراقات الشبكية مما يعرض الجامعة لخطر الجهود المتكررة وضياع وقتها بالاستمرار في محاولة القدرة

على مواكبة التطور السريع في تكنولوجيا المعلومات من أجهزة وبرامج، الأمر الذي تصدت له العديد من الجامعات العالمية بإدراج سياسات الأمن السيبراني من خلال استراتيجيات متنوعة واضحة المعالم بحيث تستخدمها بالطريقة التي تضمن تطوير أدائها وترقية الحياة الرقمية .

سياسات وخطط الجامعة لتعزيز ثقة المستخدم بأنظمتها وبرامجها:

حسب إجابات المبحوثين تكون عن طريق وضع مخطط رقمنة الجامعة وخلية الأمن المعلوماتي التي بدورها تقوم بوضع سياسة الأمن المعلوماتي.

تساهم الجامعة بشكل فعال في استقرار المجتمع وأمنه وحماية شباب المجتمع من المخاطر والتهديدات المعاصرة التي تواجههم، وبشكل خاص من المخاطر المرتبطة بالجانب الثقافي والمعلوماتي الرقمي والتي تؤثر على الأفراد أثناء التعاملات مع التطبيقات الرقمية المختلفة، ويمكن لإدارة الجامعة العمل على وضع خطط مقترحة للتوعية وتوفير وحدة للأمن السيبراني للإشراف على تقديم التوعية والحماية واصدار نشرات دورية خاصة بمفاهيم الأمن السيبراني و بالتعامل مع المعلومات والبيانات من خلال متخصصين، وكذلك بدعوة الكفاءات البشرية في مجال الأمن السيبراني للاشتراك في هذه الندوات والمؤتمرات، وادراج مقررات دراسية خاصة بمفاهيم الأمن السيبراني ضمن البرامج التعليمية بالجامعة.

السياسات والأنظمة المرنة التي تعتمد عليها الجامعة لتعزيز الثقة الرقمية:

حسب إجابات المبحوثين تكون في سياسة الاقتراح والتشاور لمكونات الأسرة الجامعية قبل التطبيق والاستغلال، ووضع الكثير من المنصات الرقمية.

إن تعزيز الثقة الرقمية بالجامعة يتطلب عددا من السياسات والأنظمة المرنة التي يمكن لجميع المستويات تنفيذها وتطويرها حسب موقعها في مواجهة مختلف المشكلات التي تسببها المخاطر السيبرانية المعاصرة، وتتمثل في وضع ادارة رقمية مرنة قادرة على مسايرة التطور والتنمية، وفي تأمين الخدمات الرقمية الادارية بالجامعات والتي يمكن اجمالها في الوظائف التالية: الجدولة/ تقديم المحتوى الرقمي/ التواصل الرقمي/ المحاضرات/ سجل درجات الطالب/ الامتحانات/ الأنشطة والواجبات والقدرة على ادارة هذه الوظائف بمنتهى

السرية والأمن، وكذلك في التوعية بأهمية تكوين كوادر وطنية مؤهلة للتصدي للهجمات السيبرانية وفي توفير الامكانيات اللازمة و المشاركة الفعالة بين جميع القيادات الادارية في تطبيق هذه السياسات والأنظمة.

الآراء والأفكار المطروحة التي تأخذها الجامعة حول تعزيز الثقة الرقمية:

من خلال إجابات المبحوثين تبين ان الجامعة دائما تأخذ بالآراء والأفكار المطروحة حول تعزيز الثقة الرقمية لتحقيق الثقة الرقمية وتعزيزها ينبغي على الجامعة التواجد في مختلف الدورات والمؤتمرات المتعلقة بموضوع الرقمنة من أجل تبادل الآراء و الحصول على الأفكار، و اكتساب المهارات والاحاطة بمختلف المستجدات الحاصلة .

الأمن السيبراني كمتحكم للأمان في استخدام شبكات الجامعة:

أجمع المبحوثين على أن الأمن السيبراني كاف كمتحكم للأمان استخدام برامج الجامعة ومختلف شبكاتها.

أصبح تأمين شبكات المعلومات والاتصالات وبناء ثقافة الأمن السيبراني أمرا اساسيا في عالم اليوم، فالأمن السيبراني يعد ممارسة لحماية الأنظمة والشبكات والبيانات والأجهزة والبرامج من اي هجمات رقمية ضارة، ويتناول الجوانب المتعلقة بضمان التشغيل الآمن و الموثوق به على جميع مستويات أنظمة الحوسبة والشبكات المترابطة كما ان هذا لا يعني بلوغه للنسبة الكاملة لمستوى الحماية.

إمكانية استعانة الجامعة بخبراء متخصصين من أجل تطبيق الأمن السيبراني لتعزيز ثقة المستخدم:

تبين حسب إجابات المبحوثين أن الجامعة لا تلجأ الى الاستعانة بخبراء متخصصين في مجال الأمن السيبراني.

مع الاستخدامات المتقدمة للتكنولوجيا ظهرت فرص جديدة تتطلب إعادة اكتساب مهارات رقمية جديدة، بالإضافة إلى تهديدات الفيروسات والقرصنة والاختراقات المنتشرة على أجهزة الحاسوب، وضعف الدراية بوسائل الأمن وحماية المعلومات على الحاسوب، وهو ما يستدعي ويزيد من الحاجة إلى وجود خبراء متخصصين في مجال الأمن السيبراني من أجل تعزيز الثقة الرقمية داخل الجامعة.

دور الأمن السيبراني في مواجهة نظم المعلومات الادارية:

كيفية تحقيق الأمن السيبراني لسرية نظم المعلومات الإدارية وعدم الكشف والاطلاع عليها من قبل أشخاص غير مخولين بذلك:

حسب المبحوثين يكون ذلك عن طريق إنشاء حسابات آمنة تتوفر على صلاحيات محدودة ووضع سياسة أمن سيبراني فعالة من خلال التطبيقات الخاصة بالصارمة وتحليل كل المعلومات الداخلة والخارجة من الجامعة وغلق المنافذ الهشة التي يمكن أن تعتبر كثغرات أمنية وتصحيحها غالبا عن طريق التحديث الدائم للتطبيقات، وكذلك عن طريق جدار الحماية الذي يرفع مستوى حماية بيانات ومعلومات المنظمة أو المؤسسة من التهديدات والمخاطر بالإضافة إلى نظام الكشف الذي يسمح بتجنب الأضرار التنظيمية والقانونية نتيجة عدم الالتزام بالضوابط.

الحماية الأساسية التي يوفرها الأمن السيبراني لنظم المعلومات الادارية من خلال عملية إدخالها أو معالجتها أو نقلها:

حسب المبحوثين يكون من خلال الاعتماد على نظام التشفير واتخاذ مجموعة من إجراءات الأمن السيبراني التي تساعد على ضبط وتحقيق الثقة في تبادل المعلومات.

إن الهدف الرئيسي لحماية المعلومات هو ضمان سرية وسلامة(نزاهة) وتوافر المعلومات(CIA) وأي مشكلة تهدد المثلث الأمني(CIA) يعتبر تهديد أمني يجب التعامل معه وحله بوضع آليات تقنية وإجراءات مشددة لتفاديه أو التقليل من آثاره.

الطريقة التي يوفر بها الأمن السيبراني بيئة أمنية موثوقة لنظم المعلومات الادارية وبنى تحتية لديها حساسية للهجمات الالكترونية:

حسب المبحوثين يكون عن طريق حماية مستعملي نظم المعلومات من الهجمات الالكترونية والمساعدة في استرجاع المعلومات بوضع نسخ في خوادم مركزية باستعمال شبكة الإنترنت وكذلك بالاعتماد على برامج وتطبيقات آمنة .

يكون ذلك عن طريق حماية شبكة المعلومات والاتصالات التي تلعب دورا كبيرا في تدفق خط سير تدفق البيانات بين الأفراد والدولة ومن طرف إلى طرف آخر، والتي اذا تعرضت إلى التخريب أو التدمير أو الاختراق حتما قد يؤثر ويقطع هذه الاتصالات ويتوقف سير العمل وتتوقف الخدمات، وتكون حماية هذه

الشبكات بمعرفة آخر التقنيات والتكنيكات الموجودة في هذا المجال ومن أهمها كشف أهداف العدو والتعرف على طبيعة هذا المهاجم وماذا يريد من خلال معرفة تكنيكاته المستخدمة والاساليب المختلفة لكي يتم العمل على إيقاف هذا الهجوم بأسلوب علمي وتقني محكم يمنع هذا الهجوم.

وكذلك عن طريق تشفير التعاملات الالكترونية بحيث لا يستطيع أي مخترق أو مهاجم أو عابث أن يدخل بسهولة لهذه البيانات والتطبيقات لأن التشفير أحد أساليب الحماية والتي يصعب فك رموزها.

حماية الأمن السيبراني لنقاط الضعف في أنظمة الحاسب الآلي التي يعتمد عليها في نقل وتخزين واسترجاع المعلومات الادارية:

حسب المبحوثين يكون عن طريق تفعيل الجدار الناري وتطبيقات الحماية ووضع المعلومات في خادم مركزي ذو تخزين مزدوج لتسهيل مراقبة واسترجاع المعلومات حال ضيعها.

تنوع وسائل الاتصالات وتفاوت خصائصها وطبيعتها زاد من حجم تبادل المعلومات بين العالم بشكل تسبب في زيادة العبء المالي على الدول التي تسعى إلى تحقيق الأمن المطلوب للفرد والمجتمع في ظل الاستخدام الواسع للحاسب الآلي وتطبيقاته، وما يندرج تحتها من أعمال حفظ البيانات والمستندات والمصادر الخاصة، الأمر الذي يستدعي وجود هيئة وطنية للأمن السيبراني تعنى بهذا الموضوع الحساس تعمل على توفير بيئة آمنة و سن التنظيمات والقوانين المتعلقة بالأمن السيبراني وتطبيقها على مختلف الجهات ومن ثم متابعة تطبيقها للتأكد من تناغم عمل مختلف هذه الجهات في حماية المعلومات والخدمات وسد الثغرات.

عرض نتائج الدراسة

في ضوء التساؤلات من خلال الدراسة المنجزة حول متطلبات تحقيق الأمن السيبراني لنظم المعلومات الإدارية بجامعة البويرة وبناء على ما تم استفادة من مجريات المقابلات مع المبحوثين وانطلاقا من تساؤلات الدراسة تم توصل إلى:

- أجمع المبحوثين على مفهوم الأمن السيبراني أنه هو نظام صارم من أجل حماية المعلومات الشخصية والشبكات والأجهزة من أي هجمات سيبرانية.

- عدم توفر إدارة لدى الجامعة خاصة بالأمن السيبراني وإنما هناك خلية مصغرة تسعى إلى وضع نظام الحماية وتطبيقه في الجامعة مكلف بهذه الإدارة هو مسؤول الخلية وطاقمه العامل معه.
- عدم التزام الوحدات الإدارية والمكلفين بها بالجامعة بالمتطلبات التنظيمية لتحقيق الأمن السيبراني.
- الجامعة لا تعطي اهتمام كبير لمتطلبات تحقيق الأمن السيبراني ليس هناك أي تدريب خاص بموظفين الجامعة والإداريين وهذه الإجابة أجمع عليها جميع المبحوثين بعد تواصلنا معه وهذه نقطة أساسية ولابد من تفعيلها لتوعية الموظفين والإداريين بضرورة توفير الأمن السيبراني.
- لم تطبق الجامعة متطلبات الأمن السيبراني لحماية بيانات والبريد الإلكتروني.
- لم ترتقي بعد جامعة البويرة إلى المستوى المطلوب لتحقيق متطلبات التقنية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكل محند أولحاج نظرا إلى الصعوبات والعراقيل التي تواجه الموظفين والإداريين وضرورة تفعل اشتراكات دورية لبعض البرامج الخاصة بالحماية ضد الفيروسات والأنشطة المشبوهة وهناك لميزانية البحث العلمي دورا كبيرا في توفير هذه البرامج التي يجب توفرها وتزويد الجامعة بأنظمة حماية عالية المستوى لأنظمة المعلومات الإدارية.
- بعض المبحوثين اعتبره الاستبيان تدخلا في عملهم ولم يتم تزويدنا بأي معلومات مفيدة في دراستنا.
- من خلال الدراسة المنجزة حول متطلبات تحقيق الأمن السيبراني لنظم المعلومات الادارية بالبويرة وبناء على ما تم استقاؤه من المقابلات مع المبحوثين وانطلاقا من تساؤلات الدراسة تم التوصل الى جملة من النتائج نخلص إلى أهمها:
- يعمل الأمن السيبراني على سد الثغرات في أنظمة المعلومات الادارية من خلال تطبيقه باستخدام مجموعة من البرمجيات والتقنيات الرقمية الحديثة .
- يلعب الأمن السيبراني دورا مهما في تعزيز الثقة الرقمية بجامعة البويرة من خلال توفير بيئة عمل قانونية آمنة وبنى تحتية متينة تحظى بثقة المستخدم.
- تعتمد الجامعة في بناء سياستها السيبرانية للحد من حالات التجسس على انشاء ميثاق الأمن المعلوماتي وتكوين المتخصصين في هذا المجال بالإضافة إلى تخصيص ميزانية وتحسين كل الأنظمة المستعملة.
- تتوفر جامعة البويرة على سياسات وخطط تعزز ثقة المستخدم بها وببرامجها منها وضع مخطط رقمنة الجامعة بالإضافة إلى خلية الأمن المعلوماتي التي بدورها تقوم بوضع سياسة الأمن المعلوماتي.

- تعتمد جامعة البويرة في تعزيز ثقتها الرقمية على سياسة الاقتراح والتشاور ووضع الكثير من المنصات الرقمية.
- تنفتح جامعة البويرة على مختلف الآراء والأفكار المطروحة حول تعزيز الثقة الرقمية من خلال تواجدها في مختلف الدورات والمؤتمرات الخاصة بهذا المجال.
- يتطلب تحقيق الأمن السيبراني للأمان في استخدام شبكات الجامعة وبرامجها توفير أنظمة الأمن السيبراني وإنشاء الطرق الدفاعية التي تحقق الميزة التنافسية للجامعات.
- تبين أن الجامعة لا تلجأ الى الاستعانة بخبراء متخصصين في تطبيق الأمن السيبراني لتعزيز ثقة المستخدم بها.
- يحقق الأمن السيبراني سرية المعلومات الادارية من خلال أنشاء حسابات آمنة ووضع سياسة أمن سيبراني فعالة، وكذلك من خلال ضمان سرية وسلامة وتوافر المعلومات بالإضافة إلى استخدام نظام التشفير وجدار الحماية لتحقيق الحماية الكاملة.
- يقوم موظفي الجامعة بتفعيل جدار الحماية ووضع المعلومات في خادم مركزي ذو تخزين مزدوج لحماية نقاط الضعف في أنظمة الحاسب الآلي.
- تعاني جامعة البويرة من نقص الخبرة في مجال الأمن السيبراني وهو ما يشكل عائق أمام تطبيقه.
- استخدام الأجهزة الشخصية يؤثر على نقل المعلومات السرية بالجامعة وهو مايعتبر تهديد كبير لسرية معلوماتها.
- تحديد المسؤوليات والمهام شيئ مهم وهو ما يمكن من تطبيق الأمن السيبراني في الجامعة.
- يعد ضعف تأطير موظفي التقنيات ونقص الحماية الكاملة لبرامج الاختراق الحديثة من معوقات تحقيق الأمن السيبراني والتي تستدعي اتخاذ الإجراءات اللازمة.
- ضعف آليات حماية البنية التحتية السيبرانية والأجهزة المعلوماتية بالجامعة الجزائرية وهو ما يتطلب وجود هيئة وطنية للأمن السيبراني تعنى بهذا الموضوع.
- نقص تطبيق التشريعات في مجال الجرائم الإلكترونية لنقص الوعي والقدرة على تطبيقها.

التوصيات والمقترحات:

- وضع الاطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية بالإضافة لحماية الخصوصية والهوية الرقمية.

- تدريب الطاقم الاداري للجامعة على كيفية استخدام قواعد الحماية عبر الشبكات الرقمية.
- ضرورة توفير برامج تعليمية لتنمية مفهوم الأمن السيبراني من خلال التعليم الرقمي بالجامعات.
- وضع استراتيجية رقمية تتضمن مجالات الأمن السيبراني .
- نشر ثقافة ومفاهيم الأمن السيبراني داخل بيئة الجامعة .
- التوعية بأساليب الحماية الادارية والفنية لجميع من يتعامل مع البيئة الرقمية للجامعات.
- تأمين الخدمات الرقمية الادارية بالجامعات.
- إتاحة مواقع رقمية للإبلاغ عن الجرائم السيبرانية ضد أي بيانات داخل الجامعة.
- عقد دورات تدريبية وورش عمل توضح كيفية حدوث الاختراقات السيبرانية، وكيفية مواجهتها والتصدي لها.
- تشجيع وحث جميع أفراد الجامعة لتأهيل قدراتهم الرقمية بشكل صحيح.
- اعداد برامج تعاونية مشتركة بين جامعة البويرة ومختلف الجامعات الجزائرية ذات الخبرة في مجال الأمن السيبراني.
- إطلاق مبادرات تستهدف مفاهيم الأمن السيبراني.
- توفير الامكانيات اللازمة لتطبيق متطلبات الأمن السيبراني.
- الاعتماد على سياسة مرنة يمكن تغييرها وتطويرها لتحقيق الأمن وحماية الأجهزة والتقنيات والشبكات والبرامج مما يسهم في تحقيق الثقة.
- الاهتمام بآراء وأفكار العاملين حول سبل الحماية والأمن السيبراني.
- وضع استراتيجية وسياسة أمنية واضحة وملزمة لكل المعنيين بصياغة المعلومات والبنى التحتية.
- وضع استراتيجية لنشر الوعي وبنائه لدى مختلف شرائح الجامعة.

خاتمة

خاتمة:

أدت التطورات الهائلة والمتلاحقة في التكنولوجيا الاتصال والمعلومات إلى إمكانية تحويل معطيات فروع المعرفة المختلفة إلى معلومات رقمية يسهل الحصول عليها وتخزينها، واسترجاعها ونقلها من جهاز لأخر بغير عناء، واستخدامها بتكاليف قليلة في وقت قصير للغاية وهاذا نتاجا للتحول الرقمي الذي شهده العالم مؤخرا، أين أصبحت سلامة وأمن المعلومات أبرز القضايا التي أصبح نجاح المؤسسات التعليمية يعتمد على ماتملكه من معلومات، لكن في المقابل العديد من المعلومات والأنظمة والبنى التحتية لمؤسسات التعليم العالي المتصلة بالشبكات عرضة للخطر بين حين وأخر للهجمات والتهديدات السيبرانية .

ويعد الأمن السيبراني بأبعاده ومستوياته المختلفة مكونا أساسيا من مكونات ومتطلبات أي تحول رقمي والحل الأمثل لمتابعة الاستخدام الواسع للانترنت وتطبيقاته وأنظمته المختلفة للتقليل من المخاطر التي تنشأ من سوء الإستخدام.

ونحن من خلال دراستنا هذه بشقيها النظري والتطبيقي إرتأينا إلى أن نبين متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة أكلي محند أولحاج البويرة من خلال جملة الإجراءات والأساليب المطبقة على عينة الدراسة، ومن خلال النتائج العامة للدراسة واتضح لنا أن جامعة أكلي محند أولحاج تعاني من نقص الخبرة في مجال الأمن السيبراني وهو مايشكل عائق أمام تطبيقه وضعف البنية التحتية السيبرانية والأجهزة المعلوماتية بالجامعة.

وختاما يجب أن نسلط الضوء على أهمية تحقيق الأمن السيبراني في أنظمة المعلومات الإدارية في الجامعات، فمع التطور التكنولوجي السريع وزيادة الإعتماد على التكنولوجيا الرقمية في إدارة الجامعات، أصبح حماية المعلومات والبيانات الحساسة ضرورة حتمية .

كما نشير في الأخير إلى أن نتائج الدراسة التي قمنا بها خاصة فقط بجامعة أكلي محند أولحاج –البويرة-، لذا لايمكن تعميمها على كافة الجامعات الجزائرية.

ومن خلال تحليلنا المقابلات ونتائج الدراسة لخصنا إلى مجموعة من الاقتراحات والتوصيات نوجزها فيما يلي:

*وضع الإطار التشريعي الملائم لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية بالإضافة لحماية الخصوصية والهوية الرقمية.

*تدريب الطاقم الإداري للجامعة عن كيفية استخدام قواعد الحماية عبر الشبكات الرقمية .

*ضرورة توفير برامج تعليمية لتنمية مفهوم الأمن السيبراني من خلال التعليم الرقمي بالجامعات .

*وضع استراتيجية رقمية تتضمن مجالات الأمن السيبراني .

*نشر ثقافة ومفاهيم الأمن السيبراني داخل بيئة الجامعة.

*التوعية بأساليب الحماية الإدارية والتقنية لجميع من يتعامل مع البيئة الرقمية للجامعة .

*تأمين الخدمات الرقمية بالجامعة .

*إتاحة مواقع رقمية للإبلاغ عن الجرائم السيبرانية ضد أي بيانات داخل الجامعة.

*عقد دورات تدريبية وورش عمل توضح كيفية حدوث الاختراقات السيبرانية، وكيفية مواجهتها والتصدي لها.

*تشجيع وحث جميع أفراد الجامعة لتأهيل قدراتهم الرقمية بشكل صحيح .

*إعداد برامج تعاونية مشتركة بين جامعة البويرة ومختلف الجامعات الجزائرية ذات الخبرة في المجال السيبراني.

*إطلاق مبادرات تستهدف الأمن السيبراني .

*توفير الإمكانيات اللازمة لتطبيق متطلبات الأمن السيبراني.

*الاعتماد على سياسة مرنة يمكن تغييرها وتطويرها لتحقيق الأمن وحماية الأجهزة والتقنيات والشبكات والبرامج مما يسهم في تحقيق الثقة .

*الإهتمام بأراء وأفكار العاملين حول سبل الحماية والأمن السيبراني.

*وضع إستراتيجية وسياسة أمنية واضحة وملزمة لكل المعنيين بصياغة المعلومات والبنى التحتية.

*وضع إستراتيجية لنشر الوعي وبنائه لدى مختلف شرائح الجامعة.

قائمة المراجع

قائمة المراجع:

***القواميس والمعاجم:**

1. بدوي أحمد زكي: **معجم المصطلحات الاجتماعية،** مكتبة لبنان، ط1، بيروت، 1978 .
2. **منجد الطلاب،** دار المشرق، بيروت، 1999.

***الكتب:**

1. بن مرسلي أحمد: **مناهج البحث في علوم الاعلام والاتصال،** ديوان المطبوعات الجامعية، الجزائر، 2007م، ص285.
2. يزيد الوليد بشير: **نظم المعلومات الإدارية،** دار الراية للنشر والتوزيع، عمان، د.س، ص119.
3. جاد سيد محمد: **نظم المعلومات الإدارية، الأساسيات والتطبيقات الإدارية،** كلية التجارة جامعة السويس، السويس، 2011م.
4. الجموسي جوهر: **الإفتراضي والثورة مكانة الانترنت في نشأة مجتمع مدني عربي،** المركز العربي للأبحاث ودراسة السياسات، بيروت، 2019م.
5. العليان ربحي مصطفى: **إدارة المعرفة،** دار صفاء للنشر والتوزيع، عمان، 2008.
6. السالمي عمر: **تكنواوجيا المعلومات،** دار المنهج، عمان، 2000.
7. سليم الحسنية: **نظم المعلومات الإدارية، إدارة المعلومات في عصر المنظمة الرقمية،** مؤسسة التوراق للنشر والتوزيع، 2006.
8. الشوابكة عدنان: **دور نظم وتكنولوجيا المعلومات في إتخاذ القرارات الإدارية،** دار اليازوري العلمية للنشر والتوزيع، عمان، 2001.
9. مبارك صلاح عبد المنعم: **اقتصاديات نظم المعلومات المحاسبية الإدارية،** دار المطبوعات الجامعية، الإسكندرية، 2008م.
10. الطاهر اسمهان، ماجد الخفاف، مها مهدي: **نظم المعلومات الإدارية،** دار وائل للنشر والتوزيع 2011م.

11. الطائي: **التجارة الإلكترونية**، دار المستقبل الواعد للأجيال القادمة، دار ثقافة للنشر والتوزيع، ، عمان، 2010.
12. عامر إبراهيم قنديلجي وعلاء الدين عبد القادر الجنابي: **نظم المعلومات الإدارية**، دار المسيرة، عمان، 2007م.
13. بدران عباس: الحروب **الإلكترونية الاشتباك في عالم متغير**، مركز دراسات الحكومة الإلكترونية، بيروت، 2010.
14. بن غرام الله عبد العزيز: **جرائم الانترنت وعقوبتها وفق نظام مكافحة الجرائم المعلوماتية**، دار الكتاب الجامعي، الرياض، 2017.
15. البيومي عبد الفتاح: **مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت**، دار الكتب القانونية، مصر، 2007.
16. مسلم عبد الهادي: **مذكرات في نظم المعلومات الإدارية، مبادئ وتطبيقات**، الناشرمركز التنميةالإدارية، الإسكندرية، 1994م.
17. العتيبي، صبحي جبر: **تطور الفكر في الأساليب والإدارة**، دار الحامد للنشر والتوزيع،، عمان، 2004م.
18. علاء الدين عبد القادر: **نظم المعلومات الإدارية**، دار المسيرة للنشر والتوزيع، الأردن، 2008 م.
19. الصباغ عماد: **نظم المعلومات، ماهيتها ومكوناتها**، دار الثقافة للنشر والتوزيع، 2000.
20. غسان عيسى العمري، سلوى أمين السمرائي، "**نظم المعلومات الاستراتيجية مدخل استراتيجي معاصر**"، دار المسيرة للنشر والتوزيع، ط1، الأردن، 2008.
21. فايز جمعة صالح النجار، نظم المعلومات الإدارية، دار حامد للنشر والتوزيع، 2009م.
22. دليو فضيل: **مدخل إلى منهجية البحث في العلوم الإنسانية والاجتماعية**، دار هومة للنشر والتوزيع، الجزائر، 2014.
23. لحسن عبد باشيوة وأخرون: **البحث العلمي مفاهيم وأساليب تطبيقات**، الوارق للنشر والتوزيع، الأردن، 2009م.
24. لحميدي، نجم عبد الله والعبيد، عبد الرحمان الأحمد والسامرائي، سلوى أمين: **نظم المعلومات الإدارية مدخل معاصر**، 2004م.

25. لعربي أسيا: **بناء الثقة بالخدمات الإلكترونية بمنطقة إسكوا**، اللجنة الاقتصادية والاجتماعية.
26. مجتمع الانترنت: **المبادئ التوجيهية المتعلقة بأمن البنية التحتية للانترنت في الدول العربية**، مجتمع الانترنت، 2020.
27. محمد بكري وسونيا سلطان: **نظم المعلومات الإدارية**، الدار الجامعية الإبراهيمية، 20011، ص55.
28. محمد شفيق: الخطوات **المنهجية لإعداد البحوث الاجتماعية**، المكتب الجامعي الحديث، الإسكندرية، 1999م.
29. شيا محمد: **مناهج التفكير وقواعد البحث في العلوم الإنسانية والإجتماعية**، مجد المؤسسة الجامعية للنشر والتوزيع، ط1، بيروت، 2007م.
30. محمد عبد الحميد: **تحليل المحتوى في بحوث الاعلام**، ديوان المطبوعات الجامعية، الجزائر، 1979م
31. مرسي محمد منير: **التعليم الجامعي المعاصر وقضاياه واتجاهاته**، دار النهضة العربية للطباعة والنشر، مصر، 2002م.
32. هيدور مركز: **الأمن الرقمي وحماية المعلومات الحق في استخدام شبكة أمنة**، مصر، مركز هيدور، ص70.
33. مروان عبد المجيد ابراهيم: **أسس االبحث العلمي لإعداد الرسائل الجامعية**، مؤسسة الوراق للنشر والتوزيع، ط1، الأردن، 2000.
34. عليان ربحي مصطفى ، عثمان محمدغنيم: **مناهج وأساليب البحث العلمي**، دار صفاء للنشر والتوزيع، عمان، 2009م.
35. منعم زمير، **محمد الفيومي: إدارة أنظمة تكنولوجيا المعلومات**، دار الشركة العربية المتحدة للتسويق والتوريدات، القاهرة، 2013م.
36. جبور منى الأشقر: **الأمن السيبراني، التحديات ومستلزمات المواجهة**، المركز العربي للبحوث القانونية والقضائية، 2012.
37. هلالي عبد الله أحمد: **إتفاقية بودابست لمكافحة الجرائم المعلوماتية**، دار النهضة العربية، ط1، القاهرة، 2007م.

38. وليد أحمد الروضان: **مالفرق بين أمن المعلومات والأمن السيبراني**، صحيفة الجزيرة الالكترونية، مؤسسة الجزيرة للصحافة والطباعة والنشر، قطر، 2010.

***المذكرات والأطروحات:**

1. بسود مبارك، يوخني أمينة: **دور نظم المعلومات في إدارة الموارد البشرية –دراسة حالة جامعة أدرار -**، مذكرة ماستر، تخصص إدارة أعمال، جامعة أحمد درارية، أدرار، 2020/2019.
2. حمودي كاهنة: **نظام أمن المعلومات في الجزائر -دراسة حالة بلدية سوق الإثنينن -**، مذكرة ماستر، تخصص سياسات عامة وإدارة محلية، جامعة ملود معمري، تيزي وزو، 2017/2016.
3. طمطامي سالم: **الصحافة الإلكترونية والأمن السيبراني-دراسة حالة الجزائر**، مذكرة ماستر، تخصص صحافة مطبوعة وإلكترونية، جامعة أحمد درارية، أدرار.
4. مرمي مراد: **أهمية نظم المعلومات الإدارية كأداة للتحليل البيئي في المؤسسات الصغيرة والمتوسطة** الجزائرية، مذكرة ماجستير، تخصص إقتصاد وتسيير المؤسسات الصغيرة والمتوسطة، جامعة فرحات عباس، سطيف، 2010/2009.

***المجلات والدوريات:**

1. الفتلاوي أحمد عيسى نعمة: **الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عن ضوء التنظيم الدولي المعاصر**، مجلة المحقق المحلي للعلوم القانونية والسياسية، العدد4، جامعة بابل، 2016.
2. زروقة إسماعيل: **الفضاء السيبراني والتحول في مفاهيم القوة والصراع**، مجلة العلوم القانونية والسياسية، العدد1، المجلد10، 2019.
3. الأعرجي، عاصم وعلاونة، علي أحمد: **واقع وأثار استخدام أنظمة المعلومات المحوسبة:** دراسة ميدانية في مركز وزارة التربية والتعليم الأردنية، المجلة العربية للإدارة، عدد1، 2022.
4. بلعسل بنت نبي ياسمين، عمروش الحسين: **التهديدات الإلكترونية والأمن السيبراني في الوطن العربي**، مجلة نوميروس الأكاديمية، المجلد2، العدد، 2021.
5. بن صابر بلقاسم: **الهجمات السيبرانية ومواجهتها في ضوء القانون الدولي المعاصر**، مجلة حقوق الإنسان والحريات العامة، العدد 4، جامعة عبد الحميد مستغانم، 2017.

6. جيهان محمد سعد الخضري، هدى جبريل علي سلامي، نعمة ناصر: **الأمن السيبراني والذكاء الاصطناعي في الجامعة السعودية دراسة مقارنة**، مجلة تطوير الأداء الجامعي، مجلد12، العدد1، جامعة جازان السعودية، 2020.

7. خادم نبيل، مقدم أحلام: **دور بناء الثقة في تطوير المعاملات الرقمية (فرنسا أنموذجا)**، مجلة الفكر القانوني والسياسي، العدد01، 2022.

8. رضا حسين قنديل: **أثر مشاريع التحول الرقمي في تحسين بطاقة أداء الثقة الرقمية بالتطبيق على وزارة التربية والتعليم**، المجلة العربية للإدارة، العدد01، مجلد 45، مصر، .2020.

9. ياقوت زينب: **دور الاعلام الجزائري في التصدي للجريمة السيبرانية –قناة النهارانموذجا-**، مقال علمي، مجلة طلبنة للدراسات العلمية الأكاديمية، العدد1، المجلد 05، الجزائر، 2021.

10. بوقرص ساعد: **الامن السيبراني مخاطر وتهديدات تتطلب ممارسات وتوصيات واستراتيجيات خاصة**، مجلة الأبحاث في الحماية الإجتماعية، العدد3، جامعة العلوم والتكنولوجيا، هواري بومدين، وهران، 2002.

11. الحربي سليمان عبد الله: **مفهوم الأمن ومستوياته وصيغه وتهديداته –دراسة نظرية في المفاهيم والأطر-**، المجلة العربية للعلوم السياسية، العدد19، 2008.

12. قطاف سليمان: **الأمن السيبراني والمضامين المرتبطة به**، مجلة طبنة للدراسات العلمية الأكاديمية، العدد02، المجلد05، جامعة الأغواط، 2022.

13. البشري محمد الأمين: **التحقيق في جرائم الحاسب الألي**، بحث مقدم إلى مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، الإمارات، 2000.

14. الجنفاوي مخلف: **التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديمية بالكويت**، المجلة العربية للأداب والدراسات الإنسانية، المجلد5، الكويت، 2021.

15. مفلح البيشي منير عبد الله: **الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس –دراسة على جامعة بيشة-**، مجلة الجامعة الإسلامية للدراسات التربوية والنفسية، العدد06، 2021.

16. يوغرارة يوسف: **الأمن السيبراني الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني**، المركز الديمقراطي العربي، مجلة الدراسات الإفريقية وحوض النيل، المجلد1، 2018.

الملاحق

المقابلة

تحية أما بعد:

تشكل هذه المقابلة جزءا من دراسة الماستر تخصص اتصال وعلاقات عامة بهدف التعرف على متطلبات تحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج "البويرة "و نرجو منكم الإجابة على أسئلة المقابلة دون تسجيل أي معلومات شخصية علما أن المعلومات ستعامل بالسرية التامة ولا تستخدم إلا لدراسات علمية .

***المتطلبات الإدارية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج البويرة .**

1. ماهو تصورك لمفهوم الأمن السيبراني؟

.....

2. هل تتوفر لدى الجامعة إدارة خاصة بالأمن السيبراني ؟

نعم ⊡ لا⊡

اذا كانت الاجابة نعم حدد طبيعة الادارة المتوفرة ؟ .....

3. من هو المكلف بهذه الإدارة؟

.....

4. هل تلتزم الوحدات الإدارية والمكلفين بها بالجامعة بالمتطلبات التنظيمية لتحقيق الأمن السيبراني ؟

نعم ⊡ لا ⊡

اذا كانت الاجابة نعم كيف ذلك؟ .....

5. ماهي الإجراءات اللازمة لإدارة الأصول المعلوماتية التي بحوزة الموظفين ؟

.....

6. هل تدرب الجامعة الموظفين والإداريين على متطلبات تحقيق الأمن السيبراني ؟

نعم ⊡ لا ⊡

اذا كانت الاجابة نعم ماهو طبيعة التدريب؟ .....

7. هل أجهزة الموظفين والإداريين الشخصية والمحمولة خاضعة لمتطلبات تحقيق الأمن السيبراني من قبل الجامعة؟

نعم ⊡ لا ⊡

اذا كانت اجابتك نعم كيف يكون ذلك؟ .....

8. هل تطبق الجامعة متطلبات الأمن السيبراني لحماية بيانات ومعلومات الجامعة ؟

نعم ⊡ لا ⊡

اذا كانت الاجابة نعم كيف يكون ذلك؟.....

9. هل تطبق الجامعة متطلبات الأمن السيبراني لحماية البريد الإلكتروني؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم كيف يكون ذلك؟.....

***المتطلبات التقنية اللازمة لتحقيق الامن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج .**

1. هل هناك برامج حماية ضد الفيروسات والأنشطة المشبوهة والبرمجيات الضارة لأنظمة المعلومات الإدارية؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم ماهي هذه البرامج ؟.....

2. هل توفر الجامعة أنظمة حماية أمنية للأجهزة التقنية الحاسوبية ؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم كيف ذلك؟ .....

3. ماهي الإجراءات التقنية المتبعة لحماية البريد الإلكتروني لدى موظفين ومستخدمين الجامعة؟

.....

4. كيف تخضع إدارة أمن الشبكات لمتطلبات تحقيق الأمن السيبراني ؟

.....

5. هل يمكن استرداد الملفات المحذوفة من جهاز الكمبيوتر؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم كيف ذلك؟.....

6. هل الجامعة مزودة بأنظمة حماية عالية المستوى لأنظمة المعلومات الإدارية ؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم ماطبيعة هذه الأنظمة؟.....

7. حسب رأيك، كيف يمكن تأمين نظام شبكي أمن لتبادل المعلومات الإدارية؟

.....

8. هل يسمح للموظفين نقل معلومات خاصة بالعمل للمنزل واستخدام جهاز الكمبيوتر الخاص للعمل عليها؟

نعم ⊡ لا ⊡

اذا كانت الإجابة لا لماذا ؟ .....

9. هل تتوفر لديكم خلية طوارئ في حالة حدوث جريمة واعتداء سيبيراني على نظم المعلومات الإدارية؟

نعم ⊡ لا ⊡

اذا كانت الاجابة نعم ماطبيعة وظائفها؟.....

***أثر الأمن السيبراني في تعزيز الثقة الرقمية بجامعة أكلي محند أولحاج –البويرة–.**

1. هل تطبيق الأمن السيبراني يعمل على سد الثغرات في أنظمة المعلومات الإدارية ؟

نعم ⊡ لا ⊡

اذا كانت الاجابة نعم كيف ذلك ؟.....

2. حسب رأيك هل تطبيق الأمن السيبراني يساهم في تعزيز الثقة الرقمية بالجامعة؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم كيف ذلك؟.....

3. هل يكفي تطبيق متطلبات الأمن السيبراني لتعزيز الثقة الرقمية؟

نعم ⊡ لا ⊡

اذا كانت الإجابة لا لماذا؟ .....

4. كيف تبني الجامعة سياساتها السيبرانية للحد من حالات التجسس والتخريب الرقمي ؟

.....

5. هل لدى الجامعة سياسات وخطط لتعزيز ثقة المستخدم بأنظمة الجامعة وبرامجها؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم ماهي هذه السياسات والخطط؟.....

6. حسب رأيك، هل تعتمد الجامعة على سياسات وأنظمة مرنة يمكن تغييرها لتعزيز الثقة الرقمية؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم ماهي هذه السياسات والأنظمة ؟.....

7. هل تأخذ الجامعة بعين الاعتبار الأراء والأفكار المطروحة حول تعزيز الثقة الرقمية ؟

دائما ⊡ احيانا ⊡ نادرا ⊡

8. هل ترون أن الأمن السيبراني كاف كمتحكم للأمان في استخدام شبكات الجامعة وبرامجها؟

نعم ⊡ لا ⊡

اذا كانت الإجابة لا ماهو ماهو البديل ؟ .....

9. هل تلجأ الجامعة إلى الإستعانة بخبراء متخصصين من أجل تطبيق الأمن السيبراني لتعزيز ثقة المستخدمين؟

نعم ⊡ لا ⊡

إذا كانت الإجابة نعم لماذا؟.....

***دور الأمن السيبراني في مواجهة نظم المعلومات الإدارية:**

1. كيف يحقق الأمن السيبراني سرية نظم المعلومات الإدارية وعدم الكشف والاطلاع عليها من قبل أشخاص غير مخولين بذلك ؟

.....

2. هل يوفر الأمن السيبراني الحماية الأساسية لنظم المعلومات الإدارية خلال عملية إدخالها وإخراجها أو معالجتها أو نقلها؟.

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم كيف ذلك؟.....

3. كيف يوفر الأمن السيبراني بيئة أمنية موثوقة لنظم المعلومات الإدارية وبنى تحتية لديها حساسية للهجمات الإلكترونية؟

.....

4. كيف يوفر الأمن السيبراني حماية لنقاط الضعف في أنظمة الحاسب الالي التي يعتمد عليها في نقل وتخزين واسترجاع المعلومات الإدارية؟

.....

***معوقات تحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة أكلي محند أولحاج البويرة**

1. حسب رأيك، هل توجد علاقة بين تدني مستوى الخبرة المهنية لدى الموظفين وتحقيق الأمن السيبراني في نظم المعلومات الإدارية بالجامعة؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم كيف ذلك؟ .....

2. هل يؤثر استخدام الأجهزة الشخصية مثل الهاتف المحمول لتخزين أو نقل معلومات سرية خاصة بالجامعة ؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم كيف ذلك؟.....

3. هل يشكل عدم تحديد المسؤوليات والصلاحيات الوصل بكل فرد عائق أمام تحقيق متطلبات الأمن السيبراني لنظم المعلومات الإدارية؟

نعم ⊡ لا ⊡

إذا كانت الإجابة نعم كيف ذلك؟.....

4. هل ترون أن عدم تعاون موظفي التقنيات في الجامعة سبب لعدم تحقيق الأمن السيبراني ؟

دائما ⊡ احيانا ⊡ نادرا⊡

5. هل قلة ضعف التأطير موظفي التقنيات تؤدي إلى تشكيل عائق أمام تطبيق الأمن السيبراني؟

نعم ⊡ لا ⊡

اذا كانت الإجابة نعم كيف ذلك؟.....

6. حسب رأيك، هل عدم توفير حماية كاملة ضد برامج الاختراق الحديثة يمثل عائقا لتحقيق متطلبات الأمن السيبراني ؟

نعم ⊡ لا ⊡

إذا كانت الإجابة نعم كيف ذلك؟.....

7. هل تعتقدون أن أليات حماية البنية التحتية السيبرانية والأجهزة المعلوماتية بالجامعة الجزائرية ضعيفة؟

نعم ⊡ لا ⊡

إذا كانت الإجابة لا لماذا؟.....

8. هل التشريعات في مجال الجرائم الإلكترونية

كافية ⊡ غير كافية ⊡

برر اجابتك في كلتا الحالتين .....

بيانات المستجوبين:

الجنس:

- ذكر ⊡ - انثى ⊡

***الوظيفة:**

- مهندس ⊡

- أستاذ ⊡

- مساعد مهندس ⊡

- تقني سامي ⊡

اخرى اذكرها.....

***الأقدمية:**

- من سنة إلى ثلاثة سنوات ⊡

- من ستة سنوات إلى تسعة سنوات ⊡

- من عشرة سنوات فما فوق ⊡

فهرس المحتويات

فهرس المحتويات:

الفصل الأول: الإطار العام للدراسة..... 5
1-تحديد الإشكالـــــية: 6
2-تساؤلات الدراسة: 7
3-أسباب اختيار موضوع الدراسة: 7
4-أهداف الدراسة: 8
5-أهمية الدراسة: 9
6- منهج الدراسة وأدواتها: 10
7-مجتمع البحث وعينة الدراسة. 11
8-تحديد مفاهيم الدراسة: 12
9-الدراسات السابقة: 15
10-حدود الدراسة: 18
الفصل الأول: تأصيل مفاهيمي لأنظمة المعلومات الإدارية في المؤسسة. 19
تمهيد:..... 20
-المبحث الأول: أساسيات عن نظم المعلومات وطبيعة نظم المعلومات. 21
1-مفاهيم حول نظم المعلومات: 21
2-خصائص نظم المعلومات:..... 22
3-موارد نظم المعلومات: 22
4-أنواع نظم المعلومات: 24
المبحث الثاني: مقاربة معرفية حول نظم المعلومات الإدارية 25
1-مفهوم نظم المعلومات الإدارية وتطورها:..... 25
2-مكونات نظم المعلومات الإدارية: 27
4-خصائص نظم المعلومات الإدارية: 29

المبحث الثالث: نظم المعلومات الإدارية وضائفها وأهميتها وتحديات تطبيقها. 30
1-وظائف نظم المعلومات الإدارية: 30
2-أهمية نظم المعلومات الإدارية: 31
3-تحديات نظم المعلومات الإدارية: 32
4-المداخل المعاصرة لدراسة نظم المعلومات الإدارية: 34
خلاصة الفصل: 36
الفصل الثاني: الإطار النظري والمفاهيمي للأمن السيبراني. 37
تمهيد: 38
-المبحث الأول مقاربة معرفية حول الأمن السيبراني 39
1-مفهوم الأمن السيبراني وأهم المفاهيم المرتبطة به 39
2-نشأة الأمن السيبراني: 42
3-الفرق بين الأمن السيبراني وأمن المعلومات: 43
4-خصائص الأمن السيبراني وأهدافه: 44
-المبحث الثاني: الأمن السيبراني، مبادئه وأبعاده وأهميته وتحدياته 46
1-مبادئ الأمن السيبراني 46
2-أهمية الأمن السيبراني: 47
3-أبعاد الأمن السيراني: 47
4-تحديات الأمن السيبراني: 48
المبحث الثالث: الثقة الرقمية والأمن السيبراني 50
1-مفهوم الثقة الرقمية: 50
2-متطلبات بناء الثقة الرقمية: 51
3-دور الثقة الرقمية في تعزيز الأمن السيبراني 52
-خلاصة الفصل: 53

الاطار التطبيقي 54
المبحث الأول: تحليل البيانات الشخصية للمبحوثين 56
المبحث الثاني: مفهوم الامن السيبراني لدى المبحوثين..... 57
المبحث الثالث: المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني في نظم المعلومات الإدارية بجامعة آكلي محند الحاج 62
عرض نتائج الدراسة 71
التوصيات والمقترحات: 73
خاتمة: 76
قائمة المراجع:..... 80
المقابلة 87
فهرس المحتويات: 95