جامـعة غـرداية

كلية العلوم الاقتصادية و التجارية و علوم التسيير

الميدان العلوم الاقتصادية و التجارية و علوم التسيير

قسم العلوم المالية والمحاسبة

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر أكاديمي

التخصص: محاسبة

بعنـــوان:

متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية

دراسة حالة مؤسسة نفطال فرع غرداية (2018 -2023)

من إعـــداد الطالبين :

* طاهر محمد السعيد

* سليماني خالد

تحـت اشـــراف :

* د. روانـــي بوحفـــص

نوقشت وأجيزت علنا بتاريخ :2023/06/15

أمام لجنـة المناقشـة المكونة من :

أ.د. دوار إبراهيم.....رئيـسا

د. رواني بوحفص.....مشـرفا ومقـررا

د. شرع مريم.....مناقـشا

السنة الجامعية 2023/2022

جامـعة غـرداية

كلية العلوم الاقتصادية و التجارية و علوم التسيير

الميدان العلوم الاقتصادية و التجارية و علوم التسيير

قسم العلوم المالية والمحاسبة

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر أكاديمي

التخصص: محاسبة

بعنـــوان:

متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية

دراسة حالة مؤسسة نفطال فرع غرداية (2018-2023)

من إعـــداد الطالبين :

* طاهر محمد السعيد

* سليماني خالد

تحـت اشـــراف :

* د. روانـــي بوحفـــص

نوقشت وأجيزت علنا بتاريخ :2023/06/15

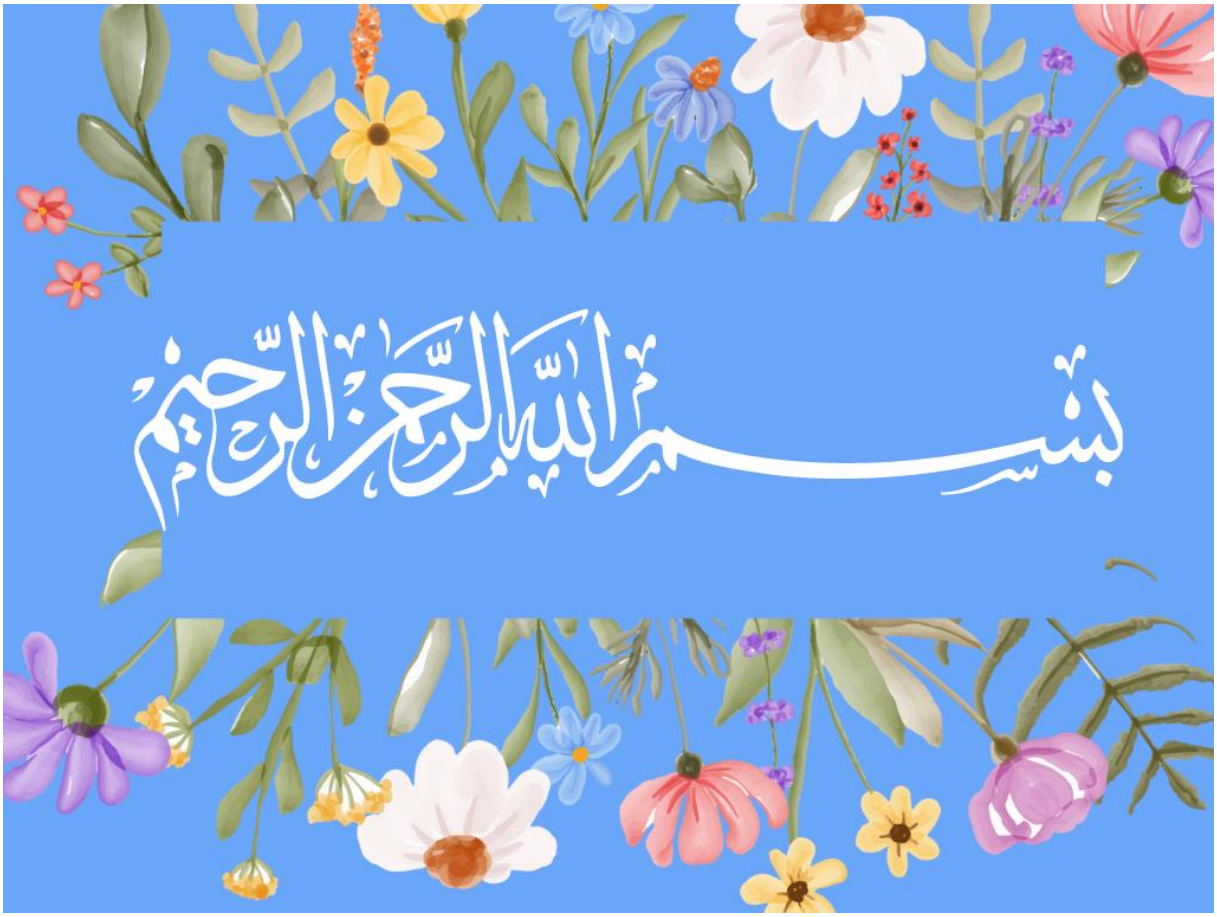
أمام لجنـة المناقشـة المكونة من:

أ.د. دوار إبراهيم.....رئيـسا

د. رواني بوحفص.....مشـرفاومقـررا

د. شرع مريم.....مناقـشا

السنة الجامعية 2023/2022


بسم الله الرحمن الرحيم

الاهداء

بسم الله الرحمن الرحيم

والصلاة والسلام على أشرف المرسلين والمبعوث رحمة للعالمين نحمد الله تعالى على توفيقه ونعمته علينا لإتمام هذا العمل والمتمثل في مذكرة التخرج لنيل شهادة الماستر في محاسبة

أهدي هذا العمل إلى الوالدين الكريمين على ما بذلوه , وضحوا بالنفس والنفيس في تعليمنا وأسال الله عز وجل أن يبارك في أعمارهم وكل أسرتي كبيرهم وصغيرهم إلى إخوتي (إسحاق - شيماء - وئام) وكذلك زملائي في الدراسة وكل الأصدقاء الأعزاء .

الى كل من اعانني في هذا العمل والى كل من علموني ان اشق طريق النجاح اساتذتي الكرام

وأخص بالذكر أساتذة جامعة غرداية

إلى كل أساتذة الذين مروا في مشواري الدراسي

طاهر محمد السعيد

الإهداء:

إلى القوي الحاني ...الباحث عن الحق دائما ولا يخاف فيه لومة لائم:
والدي العزيز رحمه الله

إلى من علمت أجيالاً...وعلمتني، وهذبت أجيالاً...وهذبتني :
أمي حفظها الله

إلى مهندس حياتي ...زوجي الغالية و أم أبنائي (أحمد ياسر ، بيسان رغد، سندس)
إلى ثمار حياتي اليانعة: أمي الثانية "فضيلة " رحمها الله ، أمال ، أسماء ، إبراهيم ، الهام ، مختار ، محمد ضياء الدين

الشكر

قال رسول الله صلى الله عليه و سلم:
" من لم يشكر الناس لم يشكر الله "
صدق رسول الله صلى الله عليه و سلم

الحمد لله على إحسانه و الشكر له على توفيقه و إمتنانه و نشهد أن لا إله إلا الله وحده لاشريك له تعظيما لشأنه و نشهد أن سيدنا و نبينا محمد عبده و رسوله الداعي إلى رضوانه ;صلى الله عليه و على آله و أصحابه و أتباعه و سلم

بعد شكر الله سبحانه و تعالى على توفيقه لنا لإتمام هذا العمل أتقدم بجزيل الشكر إلى الوالدين العزيزين الذين أعانوني و شجعوني على الإستمرار في مسيرة العلم و النجاح، و إكمال الدراسة في هذا المشروع، كما أتوجه بالشكر الجزيل إلى من شرفني بإشرافه على عملي بحثي الدكتور "رواني بوحفص " الذي لن تكفي حروف هذا العمل لإيفائه حقه بصبره الكبير علينا، وتوجيهاتها العلمية التي لا تقدر بثمن ؛ و التي ساهمت بشكل كبير في إتمام و إستكمال هذا العمل؛ أيضا أشكر مدير مؤسسة نفطال" حروز نوردين " الذي كان أكثر من متعاون مع هذا العمل ;كما أشكر جميع أساتذة جامعة غرداية الذين ساهموا بتوجيهاتهم في هذا العمل كل باسمه ومقامه .

كما أتوجه بخالص شكري و تقديري إلى كل من ساعدني من قريب أو من بعيد على إنجاز و إتمام هذا العمل.

" رب أوزعني أن أشكر نعمتك التي أنعمت علي و على والدي و أن أعمل صالحا ترضاه و أدخلني برحمتك في عبادك الصالحين "

الملخص :

هدفنا من خلال هذه الدراسة إلى معرفة أهم متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية من خلال الدراسة حالة لمؤسسة نفطال فرع غرداية خلال الفترة الممتدة من سنة 2018 إلى 2023 باستخدام المنهج الوصفي وأداتي المقابلة والملاحظة كأداتي جمع البيانات ،وخلصت الدراسة إلى ما يلي:

تولي شركة نفطال فرع غرداية أهمية كبرى للأمن السيبراني لأنظمة المعلومات المحاسبية ،وهذا من خلال الجهود المتخذة من قبل المؤسسة في مجال الأمان والحماية السيبرانية ،لكن هناك بعض نقاط الضعف وجب على المؤسسة تلافيها والتي من أبرزها نقص الثقافة السيبرانية للعاملين ،أيضا تعرفنا على الأمن السيبراني في الجزائر والذي رأيناه جد متأخر مقارنة بدول الأخرى.

الكلمات المفتاحية: الأمن السيبراني ، نظام المعلومات المحاسبي ،الذكاء الاصطناعي ، الذكاء السيبراني.

Abstract:

The aim of this study is to identify the key requirements for implementing cyber security in accounting information systems through a case study of the Naftal Branch in Ghardaia, spanning from 2018 to 2023. The study utilizes a descriptive approach and employs interviews and observations as data collection tools. The study findings are as follows:

Naftal Ghardaia Branch attaches great importance to cyber security in accounting information systems, as evidenced by the efforts made by the institution in the field of security and cyber protection. However, there are some weaknesses that need to be addressed, most notably the lack of cyber awareness among employees. Additionally, we gained insights into Algerian cyber security, which we found to be significantly lagging behind other countries.

Keywords: cyber security, accounting information system, artificial intelligence, cyber intelligence.

Résumé :

L'objectif de cette étude est d'identifier les principales exigences pour la mise en œuvre de la cyber sécurité dans les systèmes d'information comptable à travers une étude de cas de la succursale Naftal à Ghardaia, couvrant la période de 2018 à 2023. L'étude utilise une approche descriptive et utilise des entretiens et des observations comme outils de collecte de données. Les résultats de l'étude sont les suivants :

La succursale Naftal de Ghardaia accorde une grande importance à la cyber sécurité des systèmes d'information comptable, comme en témoignent les efforts déployés par l'institution dans le domaine de la sécurité et de la protection cybernétique. Cependant, il existe quelques faiblesses qui doivent être traitées, notamment le manque de sensibilisation à la cybernétique chez les employés. De plus, nous avons acquis des connaissances sur la cyber sécurité en Algérie, que nous avons constaté être considérablement en retard par rapport à d'autres pays.

Mots-clés : cyber sécurité, système d'information comptable, intelligence artificielle, intelligence cybernétique.

“


الفهرس

”

قائمة المحتويات

قائمـــة الجـــداول

قائمـة الأشــكال البيانيــة

قائمة الملاحق

قائمة الاختصارات والرموز

إختصار/الرمز	الدلالة باللغة الأجنبية	الدلالة باللغة العربية
IT	Information Technology	تكنولوجيا المعلومات
AIS	Accounting Information System	نظام المعلومات المحاسبي
RMS	Risk Managment System	إدارة مخاطر المؤسسة
SQL	Structured query language	لغة الاستعلامات الهيكلية
DDOS	Distributed denial of service	رفض خدمة الموزع
SAC	Systems Auditability and Control	رقابة وتدقيق الأنظمة
COBIT	Control Objectives for Information Technology	أهداف الرقابة وتكنولوجيا المعلومات
NIST	National Institute of Standards and Technology	المعهد الوطني للمعايير والتكنولوجيا
SOX	Sarbanes-Oxley Act	قانون ساربنز أوكسلي
COSO	The Committee of Sponsoring Organizations of the treadway Commission's Internal Control	لجنة المنظمات الراعية لإطار الرقابة الداخلية المتكامل التابع للجنة تريدوي
ISACA	Information Systems Audit and Control Association	الجمعية الدولية لتدقيق والرقابة على أنظمة المعلومات
ISO	Organisation internationale de normalisation	منظمة التقيس الدولية
AI	Artificial Intelligence	الذكاء الأصطناعي
SAI	Super Artificial Intelligence	الذكاء الاصطناعي الخارق
SSO	Single Sign-On	تسجيل الدخول الأحادي
IOT	Internet Of Thing	انترنت الأشياء

الواقع الإفتراضي	Viertul Reality	**VR**
نظام اللامركزي لتسويق	System decentralize et Commercialisation	**SD COM**

“

مقدمة عامة

”

أ- توطئة:

أدى التطور الكبير الذي حصل في مجالات عدة والتي من أهمها مجال تكنولوجيا المعلومات وأجهزة الحاسوب تأثر في علوم شتى وذلك من خلال الاستفادة من الميزات التي توفرها هذه التكنولوجيا ،حيث يعتبر عصرنا الحالي فترة ثورية في مجال المعلومات والاتصالات وكذا أتمتة العمليات والتغيرات والتطورات الحاصلة بسبب الذكاء الاصطناعي، إذ أصبحت المعلومات تمثل السمة الأساسية في العقود أخيرة من القرن الواحد والعشرين ،وتعود هذه الظاهرة إلى تطور تكنولوجيا المعلومات وارتفاع حجم المعلومات التي يتعين معالجتها وتخزينها وتقديمها للنظام بشكل كبير، مما جعل من الصعب السيطرة عليها والتحكم بها ،ومن هنا انتشر استخدام تطبيقات وأدوات تكنولوجيا المعلومات والاتصال في جميع المجالات وعلى جميع المستويات وأصبح استخدام الحاسوب في معالجة المعلومات المحاسبية ضرورة لا يمكن الاستغناء عنها واهمية بالغة لمعظم المؤسسات ،حيث يتيح ذلك إنتاج واستهلاك المعلومات بطريقة أكثر كفاءة وفعالية من أجل تحقيق أهداف المرجوة التي تطمح لها المؤسسات وهذا نتيجة لتقنيات الحديثة المتوفرة لنظم المعلومات المحوسبة.

ومن الجهة الأخرى يحمل التقدم التكنولوجي الهائل العديد من المخاطر المتعلقة بأمن وكفاءة نظام المعلومات المحاسبي، وذلك نظرًا لعدم مواكبة التطور التكنولوجي بتطور مماثل في الممارسات والضوابط الرقابة و الحماية ،فنظرا لتنوع المخاطر التي يوجهها نظام المعلومات المحاسبي فقد حرصت المؤسسات على اتباع ضوابط رقابية مستمدة من تكنولوجيا المعلومات، وهذا ما يتطلب فهم كيفية حفاظ على الأنظمة من التهديدات والتجاوزات المختلفة لضمان سرية والسلامة المعلومات المحاسبية التي ينتجها نظام المعلومات ،وهنا يتجلى دور الأمن السيبراني في حماية المعلومات الحساسة للمؤسسات وما يضمنه من مجابهة كل أشكال الاختراقات والجرائم السيبرانية وهذا ما يحافظ على استمرارية ونجاح المؤسسات في أداء أعمالها وحماية البنية التحتية الحيوية الحساسة للدول.

ب- طرح الإشكالية الرئيسية :

تكمن مشكلة البحث في التعرف على متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية باعتبار ان هذا الأخير يعتبر وسيلة أساسية لحماية والرقابة على نظم المعلومات والحفاظ على أمانها ،وعليه وبناءًا على ما سبق يمكننا طرح التساؤل التالي:

فيما تتمثل أهم متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في مؤسسة نفطال فرع – غرداية – ؟

ج– الاسئلة الفرعية : وبغرض دراسة الإشكالية الرئيسية يمكننا تقسيمها إلى إشكاليات فرعية:

- ما دور نظام المعلومات المحاسبي في المؤسسات الاقتصادية ؟
- فيما تتمثل أهم أساسيات الأمن السيبراني لأنظمة المعلومات المحاسبية ؟
- ماهي أهم المخاطر التي تواجه نظم المعلومات المحاسبية ،وما حلول مجابهتها؟
- كيف تتعامل مؤسسة نفطال – غرداية– مع مخاطر السيبرانية على نظام المعلومات المحاسبية التي تمتلكه ؟

د– فرضيات الدراسة : بغية إجابة على الأسئلة الفرعية السابقة قمنا بصياغة الفرضيات التالية :

- تتمثل أهم متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية في توفر أدوات وأنظمة الأمان والحماية وممثلة في نظم التشغيل والشبكات الحاسوبية المتطورة والتطبيقات المختلفة التابعة لها.
- يعتبر نظام المعلومات المحاسبي من أهم الأنظمة الفرعية الموجودة داخل المؤسسة ،بحيث يتمثل دوره في إنتاج المعلومات التي تعكس الواقع الاقتصادي من أجل توفيرها للأطراف ذوي العلاقة والتي على ضوئها يتخذ قرارات.
- تتمثل هذه الأساسيات في مجموعة من الإجراءات التي تهدف لمحافظة على سرية المعلومات الإلكترونية.
- يواجه نظام المعلومات المحاسبي العديد من المخاطر نتيجة استخدامه وسائل تكنولوجيا المعلومات والاتصال والتي يتم مواجهتها بواسطة أدوات الحماية والرقابة المتعلقة بأمن السيبراني.
- تتعامل مؤسسة نفطال – غرداية – مع المخاطر السيبرانية بمجموعة من سياسات الأمان والحماية لأنظمة المعلومات المطبقة على مستوى المؤسسة.

هـ– أهداف الدراسة : ومن بين الأهداف التي تنوي الدراسة التعرف عليها:

- تحديد طبيعة المخاطر التي تواجه نظام المعلومات المحاسبي أثناء إستخدامه.
- التعرف على أسباب حدوث المخاطر التي تهدد أمان نظم المعلومات المحاسبية.
- معرفة أهم الطرق وأساليب واستراتيجيات المستخدمة من طرف منفذي الجرائم السيبرانية.

- تحديد أهم إجراءات الحماية والضوابط الرقابية المتعلقة بأمن السيبراني للحد من المخاطر التي تهدد نظم المعلومات المحاسبية.
- تشخيص وضع المؤسسات الجزائرية في كيفية حفاظها على سرية وسلامة بياناتها ومدى جاهزيتها لتطبيق الأمن السيبراني.

و- أهمية الدراسة :

تناولت هذه الدراسة موضوعا يحظى بأهمية بالغة وممثل في " **الأمن السيبراني لأنظمة المعلومات المحاسبية**" والذي يمكن اعتباره موضوعا هاما وجب الوقوف عليه ،وتتلخص هذه الأهمية في النقاط الرئيسية التي تطرقت لها هذه الدراسة ،بحيث قدمت هذه الدراسة مجموعة من المخاطر المتعلقة بنظم المعلومات التي تواجه المؤسسات أثناء أداء مهامها ،كما قدمت أيضا بعض الطرق والاستراتيجيات المتبعة من قبل مجرمي الانترنت ،وأيضا قدمت مجموعة من المقترحات والحلول لها ، أيضا سلطت هذه الدراسة الضوء على واقع أمان نظم المعلومات في الجزائر وبعض الاجتهادات المبذولة من طرف القائمين على أمان تكنولوجيا المعلومات والاتصال ،كما تطرقت هذه الدراسة إلى مستجدات الحديثة فيما يخص ثورة الذكاء الاصطناعي وما سيقدمه هذا الأخير في مجال الأمن السيبراني ،وفتحت الدراسة الحالية أفاق مستقبلية جديدة لدراسات أخرى لتعمق أكثر في موضوع أمن نظم المعلومات ولما لا التطرق لأكثر لجوانب التعلم العميق Deep learning وعلم ألة Machine Science.

ز- مبررات اختيار موضوع الدراسة: تختلف أسباب اختيار الموضوع بين ما هو ذاتي متعلق بالطلبة وما هو موضوعي وهي كما يلي:

1- مبررات ذاتية :

- الميول والاهتمام الشخصي بكل ما يخص مواضيع متعلقة بجوانب التكنولوجية.
- محاولة التعرف أكثر على جوانب أمن السيبراني وأنظمة الحماية من قبل الطلبة للأجل الاستفادة.
- تماشي الموضوع مع طبيعة التخصص المنتمون له (محاسبة).

أ- مبررات موضوعية :

- حداثة الموضوع باعتباره موضوع الساعة في كل العالم مما يمكننا في تقديم إضافة وهذا ما يسمح بإثراء المكتبة الجزائرية بمرجع جديد.
- امكانية تقديم حلول لمخاطر والمشاكل التي يتم مواجهتها اما من قبل المؤسسات الجزائرية أو حتى المجتمع وهذا بسبب امتلاك الخلفية في المواضيع التكنولوجية والجوانب الحماية التي تسمح بتقديم هذه المقترحات.
- تداعيات ثورة الذكاء الاصطناعي والتغير الذي يشهده العالم حاليا أو مستقبليا في جميع المجالات ومن بينها الموضوع الذي نحن بصدد دراسته.
- تأثيرات الموضوع على المؤسسات الاقتصادية على مستوى الجزئي وعلى الدول على مستوى الكلي ،وكذا على المجتمع بمحاولة نشر ثقافة السيبرانية من خلال موضوعنا.

ح- حدود الدراسة :

1- حدود مكانية : تمت الدراسة بشكل عام على مستوى البيئة المحاسبية الجزائرية وعلى مستوى مؤسسة "نفطال- غرداية -" بشكل خاص.

2- حدود زمانية : تمت الدراسة خلال الفترة الزمنية الممتدة من سنة 2018 إلى غاية سنة 2023.

3- حدود بشرية : ركزت الدراسة على المسؤولين القائمين على نظام المعلومات المحاسبي وأنظمة الأخرى ذات العلاقة به.

ط- منهجية الدراسة وأدوات المستخدمة :

بغية تحقيق أهداف الدراسة واختبار فرضياتها قمنا باستخدام المنهج الوصفي في الدراسة النظرية حيث تم إجراء مسح نظري في الأدبيات المتعلقة بالأمن السيبراني وأنظمة المعلومات المحاسبية ،وتم عرض أهم الدراسات السابقة الخاصة بموضوع محل الدراسة ومن أجل تحقيق نوع من الربط بين التراكم المعرفي (النظري) والعملي (التطبيقي)، وفي الدراسة التطبيقية تم اعتماد المنهج الوصفي التحليلي من خلال تم استعمال أسلوب دراسة الحالة باستخدام أداتي المقابلة والملاحظة كأداتي لجمع البيانات.

ي- تقسيمات البحث :

من أجل معالجة هذا الموضوع تم تقسيم الدراسة إلى فصلين فصل نظري وفصل تطبيقي تم سبقهم بمقدمة وختمهم بخاتمة بحيث كل فصل يحتوي على مبحثين وثلاثة مطالب إلا المبحث الأول في الفصل الأول الذي يحتوي على مطلبين.

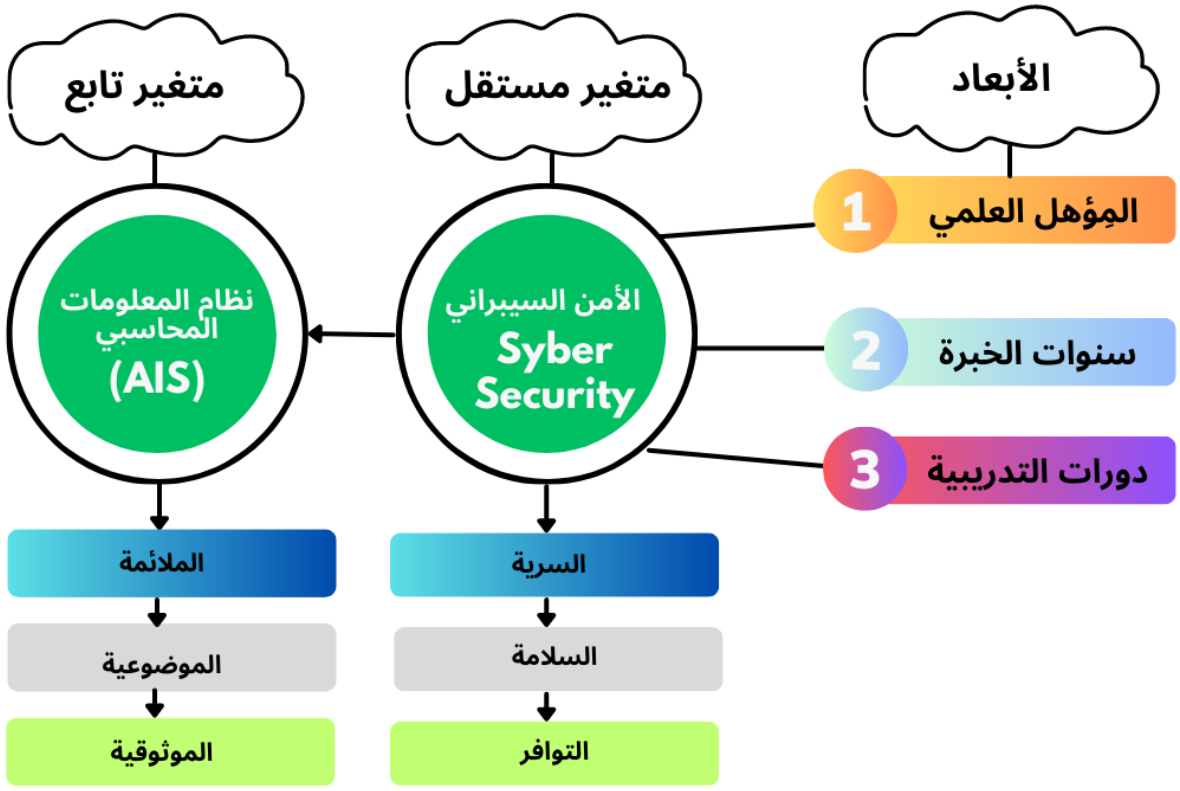
فالفصل الأول جاء تحت عنوان " **الإطار النظري للأمن السيبراني وأنظمة المعلومات المحاسبية**" تم فيه معالجة مجموعة من المعارف النظرية للأنظمة المعلومات المحاسبية ومخاطر المعرضة لها ،بإضافة إلى تقديم بعض المفاهيم حول الأمن السيبراني ودوره في حماية أنظمة المعلومات ،كما تخلل هذا الفصل من خلال المبحث الثاني عرض بعض الدراسات السابقة العربية والأجنبية التي عالجت الموضوع وما يميز دراستنا الحالية عن نظيرها من دراسات السابقة.

أما في الفصل الثاني الذي حمل عنوان " **دراسة أهم متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية "دراسة ميدانية لمؤسسة نفطال – غرداية –** قمنا من خلال هذا الفصل باختبار فرضيات الدراسة من خلال دراسة حالة مؤسسة محل الدراسة.

وفي الأخير نختتم موضوعنا هذا بتلخيص واختبار للفرضيات التي طرحت في مقدمة البحث، ثم عرض للنتائج المتوصل إليها، وأخيرا قمنا بتقديم اقتراحات بناء على النتائج المتوصل إليها، إضافة إلى أفاق المستقبلية البحث.

ك- نموذج الدراسة : يوضح الشكل التالي نموذج الدراسة والذي يتكون من المتغير المستقل والمتمثل في الأمن السيبراني والمتغير التابع المتمثل في نظام المعلومات المحاسبي ،ومجموعة من أبعاد والممثلة في: المؤهل العلمي ،سنوات الخبرة ،دورات التدريبية ،وكذا بعض من أبعاد الفرعية المتعلقة بكل متغير.

شكل رقم(01): أنموذج الدراسة



المصدر: من إعداد الطالبان اعتمادا على الدراسات السابقة

ل– صعوبات الدراسة : خلال انجازنا لهذا البحث الاكاديمي اعترضتنا بعض الصعوبات من أهمها ما يلي:

- رفض عدة المؤسسات في قبول إجراء تربص وخاصة المؤسسات التي تطبق نظامي Oracle و SAP.
- عدم تصريح بكافة المعلومات وإجابة على الاسئلة المطروحة من قبل المؤسسة محل الدراسة ،ربما لحساسية بعض الأسئلة
- عدم وجود منصة أو قاعدة بيانات التي تسمح باطلاع على أهم إحصائيات المتعلقة بجرائم الالكترونية في الجزائر.

الفصل الأول الإطار النظري للأمن السيبراني وأنظمة المعلومات المحاسبية

تمهيد :

يشهد عصرنا الحالي تطورات وتغيرات في مجال الإعلام والاتصال، حيث أصبحت المعلومات المنتجة من طرف وسائل الإعلام واتصال تلعب دوراً مهماً في تسيير الأعمال وبناء المنظمات والحفاظ على الموارد المتاحة ،وهذا ما يتطلب توفيرا لمعلومات ذات جودة وموثوقية، ولا يقتصر هذا الاهتمام على الموارد المالية والبشرية فحسب بل أصبح الاعتماد على المعلومات وسيلة حيوية في مختلف مجالات الحياة وتأتي المحاسبة على رأس هذه المجالات ،حيث تعتبر مجالاً مهماً في إدارة المال والأعمال واتخاذ القرارات المالية الحاسمة ،ولذلك أصبحت أنظمة المعلومات المحاسبية ذات أهمية بالغة في توفير المعلومات المالية الموثوقة والدقيقة التي تساعد على إدارة الأعمال بكفاءة وفعالية.

فمثلما تطورت العديد من العلوم، تطورت المحاسبة أيضًا مع تطور التقنيات الحديثة، حتى أصبحت اليوم تعتمد على نظام للمعلومات تستند إلى إجراءات وتقنيات تكنولوجيا المعلومات.

وبالنظر إلى التطورات السريعة التي يشهدها عالمنا المعاصر في مجال تقنيات المعلومات واتصالات ،فإنه من المهم أن يستخدم المحاسبون والمدراء النظم الحديثة للمعلومات المحاسبية ،وأن يحرصوا على تأمينها وحمايتها من خطر الاختراق السيبراني والاحتيال المالي ،فمع تزايد استخدام أنظمة المعلومات المحاسبية أصبح الأمر يشكل تحدياً أمنياً حقيقياً مما يتطلب الأمر اتخاذ إجراءات أمنية متعددة للحد من هذه المخاطر ،فالبيانات المالية الحساسة تشكل هدفاً للهجمات السيبرانية لذلك يجب حمايتها بشكل فعال وجدي.

وانطلاقا مما سبق نهدف من خلال هذا الفصل تقديم مساهمة معرفية تتناول نظم المعلومات المحاسبية والمخاطر التي تواجهها وكذا دور أمن السيبراني في حماية هذه أنظمة ،أيضا سوف نقدم مجموعة من الدراسات السابقة حول هذا الموضوع لإبراز وتأكيد ما تم استعراضه ، بحيث تم تقسيم الفصل إلى مبحثين وفقا لما يلي :

المبحث الأول : أمن السيبراني وأنظمة المعلومات المحاسبية.

المبحث الثاني : الدراسات السابقة.

المبحث الأول: الأمن السيبراني وأنظمة المعلومات المحاسبية

يلعب نظام المعلومات المحاسبي دورا بارزا وحيويا داخل المؤسسة وذلك باعتباره منتجا للمعلومات والتي على أساسها يتم اتخاذ قرارات ورسم استراتيجيات مستقبلية للمؤسسة ،لهذا تسعى المؤسسات والقائمين على نظم المعلومات على حماية هذه النظم من كل أشكال الاختراقات والتجاوزات ،ومن خلال هذا المبحث سوف نستعرض بعض مفاهيم حول نظام المعلومات المحاسبي ومخاطر التي يتم مواجهتها عند تطبيقه وأيضا من خلال المطلب الثالث قدمنا بعض المفاهيم والمتعلقة بالأمن السيبراني ودوره في حماية أنظمة المعلومات المحاسبية .

المطلب الأول: مفاهيم أساسية لنظام المعلومات المحاسبي

بغية التعرف على نظام المعلومات المحاسبي وجب علينا أولا التطرق لبعض المفاهيم المهمة والتي لها علاقة بنظم المعلومات المحاسبية ومن بينها : البيانات ،المعلومات ،النظام ، نظرية النظم ، المعلومات المحاسبية.... ،بعد هذا سوف نقدم مفاهيم خاصة بنظام المعلومات المحاسبي وما يحتويه هذا النظام .

1- تعريف البيانات "DATA" :

تعرف البيانات: على أنها عبارة عن مجموعة من الحقائق أو الارقام أو الاعداد للأحداث معينة وغير جاهزة للاستعمال بشكلها الحالي[1] ،والتي يتم حصول عليها من مصادر متعددة لتحويلها الى معلومات جاهزة الاستخدام.

تعرف أيضا: بانها المادة الأساسية الأولية اللازمة للإنتاج المعلومات[2] ،ومن خلال ما سبق يمكننا القول أن البيانات هي عبارة عن مدخلات نظام المعلومات أي هي مجموعة من الأحداث وأرقام وأعداد مبهمة والتي لم يتم معالجتها من قبل النظام والتي لا يمكن من خلالها اتخاذ القرار.

[1] زين عبد المالك ،**أثر تطبيق حوكمة الشركات على مخاطر نظام المعلومات المحاسبي دراسة ميدانية** ، أطروحة دكتوراه ،كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة علي لونيسي ،البليدة ،الجزائر ،2020/2019 ،ص:28.

[2] زعابطة عبد اللطيف ، **أثر تكنولوجيا المعلومات على نظام المعلومات المحاسبي دراسة حالة شركات الاتصالات الجزائر – الأغواط –** ،أطروحة دكتوراه ، **كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة غرداية ، الجزائر ، 2021 /2022 ،ص:** 10

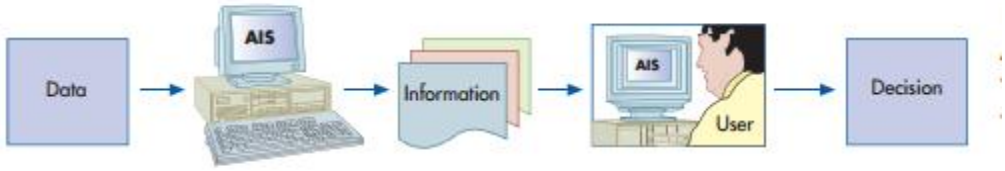
2- تعريف المعلومات "INFORMATION" : تتشكل المعلومات من مجموعة من المفاهيم والآراء والاستنتاجات والبيانات المنظمة والمتعلقة بموضوع معين.[1]

وتعرف أيضا بانها: عبارة عن قيم لها معنى والمستخدمة في اتخاذ القرارات والناتجة عن معالجة وتشغيل بيانات معينة.[2]

ومما سبق يمكننا القول أن المعلومات هي عبارة عن مخرجات نظام المعلومات أي هي مجموعة من أرقام وأعداد الجاهزة للاستخدام والتي تمت معالجتها من قبل النظام والتي يمكن على ضوئها اتخاذ قرارات .

ويمكن تلخيص ما سبق وفقا لشكل الاتي :

الشكل رقم (02) : يوضح ألية ظهور المعلومات



Source: Romney, Marshall B., Steinbart, Paul John. ***Accounting information systems***. 14th Ed Harlow, England : Pearson, 2018,P:11.

2-1- خصائص المعلومات : لكي تكون المعلومات ذات فائدة بالنسبة لمستخدميها وجب توفر فيها بعض خصائص أساسية: الملائمة "Relevance " - الموضوعية "Objectivity" - الموثوقية "Reliability" - قابلة للفهم "Understandabiliy"

- **الملائمة** : ويقصد بها أن تغطي وتراعي المعلومات احتياجات متخذي القرار مما يضمن تقليل من حالة عدم التأكد التي تحيط بعملية اتخاذ القرار .

[1] نوح سماح ،**دور نظام المعلومات المحاسبي في تقييم الأداء المالي للمؤسسة الاقتصادية دراسة حالة مؤسسة مطاحن الزيبان القنطرة – بسكرة –** ، أطروحة دكتوراه ، كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة محمد الخيضر ،بسكرة ،الجزائر ، 2019/2018 ،ص:11.

[2] عبد العزيز سيد مصطفى وأخرون ، **أساسيات تكنولوجيا المعلومات تطبيقات محاسبية** ، كلية التجارة ،جامعة القاهرة ،مصر ، 2019 ،ص:20.

- **الموضوعية** : والمقصود بها أن تحوز مخرجات نظام المعلومات بقابلية التحقق وأن تكون بعيدة عن أي تحيز وعاكسة لمصداقية وطبيعة الأحداث المستقبلية .[1]
- **الموثوقية** : هي أن تكون المعلومات خالية من الأخطاء وبعيدة عن التحيز بدرجة معقولة ومقبولة ،وأن تعبر عن مصداقية ما تمثله.
- **قابلة للفهم**: وهي أن تتسم المعلومات بالوضوح والدقة والسهولة التامة ، أي أن تكون بلغة بسيطة يستطيع جميع مستخدمي هذه المعلومة فهمها.

3– تعريف نظام المعلومات :

قبل التطرق إلى تعريف نظام المعلومات وجب علينا تقديم بعض مفاهيم حول مصطلح النظام " System" ونظرية المتعلقة بهذا الأخير والمتمثلة في نظرية النظم "System Theory" والمعلومات المحاسبية "Accounting Information".

أ– نظرية النظم : برزت فكرة النظم على يد العالم الألماني **لودينغ فون بارتالانفي** " **Ludwing Von Betralanffy**" تحت مسمى " **النظرية العامة للنظم**" وتعرف هذه النظرية بإنها : تفكير منهجي نظامي متعلق بظواهر و أشياء المحيطة بحيث

تتجاوز النظرة التقليدية التي ترى الأشياء والحقائق كمجموعة من المعطيات المستقلة وغير مرتبطة بعلاقات.[2]

ب– النظام : يعتبر أصل كلمة نظام من الكلمة اللاتينية "Systema" والتي هي مشتقة من الكلمة اليونانية القديمة "Systema " وهذه الأخيرة مشتقة من "Sym" والتي تعني "Together" "معا". ويعرف أيضا : بانه عبارة عن مجموعة من العناصر والموارد المترابطة والمتفاعلة مع بعضها البعض والتي تسعى إلى تحقيق أهداف مشتركة .[3]

[1] عبد العزيز سيد مصطفى وأخرون ،**نظم المعلومات المحاسبية مدخل تطبيقي عملي** ،كلية التجارة ،جامعة القاهرة ، مصر ،2019،ص:22.

[2] عطاالله أحمد الحسبان ،**نظم المعلومات المحاسبية** ،دار اليازوري العلمية لنشر والتوزيع ،الأردن ،2013 ،ص:27– 29.

[3] بوعزيز رضا ،**مساهمة نظام المعلومات المحاسبي الجيد في تسهيل مهمة محافظ الحسابات دراسة مجموعة من الشركات الجزائرية** ، أطروحة دكتوراه ،كلية العلوم الاقتصادية والتجارية وع التسيير ، جامعة الجزائر 3 ،الجزائر ، 2022/2021 ، ص:11– 13.

ج– معلومات المحاسبية : تعرف على أنها : عبارة عن مجموعة من المعلومات الكمية أو الكيفية والمتعلقة بالأحداث الاقتصادية الناتجة عن العمليات التشغيلية والتي تمت معالجتها من خلال نظم المعلومات المحاسبية والمقدمة للجهات التي لها علاقة بالوحدة إما داخليًا أو خارجيًا.[1]

د– تكنولوجيا المعلومات IT: هي عبارة عن مجموعة من الأجهزة والبرامج المستخدمة للأداء مهام الأساسية كتخزين البيانات واستعادتها وإدارة ومعالجة المعلومات و تجهيزها وإرسالها للأطراف المعنية.[2]

هـ – حوسبة السحابية " Cloud Computing ": هي تلك المصادر والأنظمة الحاسوبية المتوافرة تحت الطلب عبر الشبكة والتي تستطيع تقديم عدد معين من الخدمات الحاسوبية المتكاملة كتخزين البيانات والنسخ الاحتياطي والمزامنة الذاتية والطباعة عن بعد.[3] أو هي عملية مشاركة موارد الحاسب المادية أو البرمجية المتوفرة تحت الطلب عبر الشبكة عن طريق مزود الخدمة لأداء مجموعة من الخدمات المتكاملة.[4]

3–1– نظام المعلومات : يتألف النظام المعلومات من مجموعة متكاملة من الموارد ،بما في ذلك الأجهزة والبرمجيات والموظفين والإجراءات، والتي تمكن المؤسسة من الحصول على المعلومات ومعالجتها وتخزينها ونشرها بأشكال مختلفة مثل : النصوص والصور وأصوات وغيرها.[5]

يعرف أيضا : على أنه مجموعة من المكونات المترابطة، بما في ذلك معدات تكنولوجيا المعلومات IT مثل أجهزة الكمبيوتر والخوادم، بالإضافة إلى المعدات المحمولة والمتنقلة، والتي تحتوي على برامج متكاملة تقوم بجمع ومعالجة وتخزين ونشر المعلومات بهدف مساعدة إدارة العمليات اليومية واتخاذ القرارات، وتوفير قدرات التنسيق والرقابة والتحليل والتمثيل للمواقف داخل المؤسسة.[6]

3–2– مكونات نظام المعلومات : يمكن اعتبار أن أي نظام يتشكل من العناصر الأساسية التالية :

---

[1] زياد هاشم السقا ،**نظام المعلومات المحاسبي** ،الطبعة الثانية ،دار الطارق للنشر والتوزيع ،العراق ، 2011 ،ص:30.

[2] هدى يوسف محمد السليمان، **أثار استخدام تكنولوجيا المعلومات على نظم المعلومات المحاسبية** ،المجلة العربية لنشر العلمي ،الأردن،،المجلد: 05 ،العدد:50 ،2022،ص:359.

[3] سامية خرخاش وأخرون ،**أهمية استخدام الحوسبة السحابية في المؤسسات** ،ملتقى دولي حول التحول الرقمي للمؤسسات والنماذج التنبؤية على المعطيات الكبيرة، جامعة مسيلة ،12و13, 2017

[4] ظبية أحمد أبو عنين ،**إدارة الموارد في الحوسبة السحابية** ،ملتقى افتراضي السحابي الأول ،السعودية،2020/04/08.

[5] Yvon Pesqueux. ***Système d'information et organisation***. Master. France. 2020.P :02.

[6] Laudon, Kenneth, et al. ***Management des systèmes d'information : corrigés des exercices***. 11e édition. Paris: Pearson Education, 2010.P:07.

أ- المدخلات Input: وهي البيانات التي تمثل المادة الأولية الخام للنظام والتي تنشأ نتيجة الأحداث الاقتصادية الحاصلة والجارية داخل وخارج المؤسسة [1] ، فمن الممكن أن تستخدم مدخلات نظام معين كمخرجات لنظام أخر وذلك عن طري التغذية العكسية للنظام" Feedback" باستخدامها كمدخلات جديدة في التشغيل ،أو من خلال العلاقات الترابط والتكامل الموجودة بين هذه النظم .[2]

ب- المعالجة Process: تعني عملية المعالجة مجموعة من الإجراءات أو الخطوات التي يتم اتباعها لتحويل البيانات الخام إلى معلومات قيمة ومفيدة. وتشمل هذه العملية العديد من الخطوات مثل تحليل وجمع البيانات وتحديثها، وتحويلها إلى صيغة ملائمة للتخزين والاستخدام، وتحليلها بواسطة الأدوات والتقنيات المختلفة ،والتحكم والسيطرة في البيانات الداخلة لنظام وإنتاج تقارير ورسوم بيانية وغيرها من الإخراجات المفيدة لاتخاذ القرارات. بالإضافة إلى ذلك يمكن أن تتضمن عملية المعالجة أيضًا إجراءات الحفظ والتحميل والنشر والتوزيع والحفاظ على البيانات بطريقة آمنة ومرنة. وباختصار فإن عملية المعالجة تعني تحويل البيانات الخام إلى معلومات قيمة وقابلة للاستخدام والتحليل.[3]

ج- المخرجات Output: يمكن تحديد المخرجات على أنها المعلومات أو المنتجات أو الخدمات التي تنتج عن عملية معالجة النظام ،يمكن أن تكون المخرجات خارجية ويعني ذلك أنها يتم إنتاجها وتقديمها مباشرة للبيئة الخارجية للنظام، أو يمكن أن تكون داخلية ويعني ذلك أنها تشكل المنتج أو المدخل لنظام فرعي آخر داخل بيئة النظام.[4]

د- التغذية العكسية Feedback : هي عملية التقييم تتضمن الحصول على البيانات والمعلومات اللازمة لتحليل عناصر النظام السابقة (المدخلات، العمليات التشغيلية، المخرجات)، والتأكد من دقتها وإمكانيتها في تحقيق أهداف النظام[5].

---

[1] فوضيل لحسن ،**دور نظام المعلومات المحاسبي في إدارة مخاطر البنوك –دراسة حالة البنوك التجارية–** ،أطروحة دكتوراه ، كلية العلوم الاقتصادية والتجارية وع التسيير ، جامعة حسيبة بن بوعلي ،الشلف ،2018 ،ص:7.

[2] ربيع أحمد بن يحي ، **فعالية نظم المعلومات المحاسبية في ظل استخدام تكنولوجيا المعلومات** ،مجلة المحاسبة ،التدقيق والمالية ، عين الدفلى ، الجزائر ،المجلد:01 ،العدد:01 ، 2019 ،ص:23 – 24.

[3] فوضيل لحسن، مرجع سبق ذكره ، ص:08 .

[4] Tony boczko, ***corporate accounting information systems***, pearson education limited, england, 2007, p: 57.

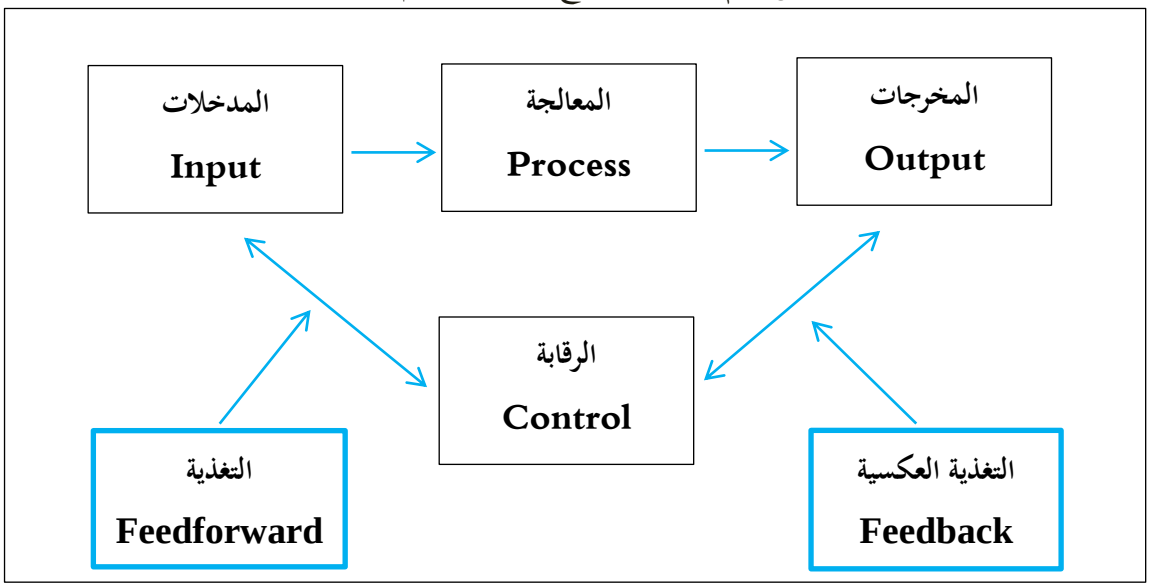
[5] زياد هاشم السقا ،**مرجع سبق ذكره** ،ص :19.

أي هي أحد العوائد الهامة للنظام حيث تركز على توجيه ومتابعة تنفيذ المخرجات التي تم إنتاجها من قبل النظام وتقوم برقابتها لضمان تحقيق أهداف النظام بشكل صحيح وسليم .[1]

هـ- الرقابة Control: وتشمل هذه المرحلة على عملية الرقابة المتعلقة بالنظام مراقبة المدخلات وعمليات المعالجة، وتهدف هذه الأدوات إلى التأكد من مطابقة النتائج النهائية للخطط المحددة مسبقًا.[2]

يمكن تمثيل هذه العناصر الأساسية لنظام المعلومات وفق الشكل التالي :

الشكل رقم (03): يوضح مكونات نظام المعلومات



المصدر: من إعداد الطالبان بناءا على شكل "**Tony boczko**"، مرجع سابق ،ص:56 .

4- تعريف نظام المعلومات المحاسبي ، أهدافه ،أهميته : يُعَدُّ نظام المعلومات المحاسبي داخل المؤسسة من أهم مصادر المعلومات التي يعتمد عليها مُتَخِذُ القرار في الحصول على المعلومات الضرورية للتعامل مع المواقف التي يتعرض لها، لذلك ينبغي تصميم هذا النظام بشكل يتوافق مع طبيعة نشاط المؤسسة والتحديات التي تواجهها.

يوجد عدة تعريفات لنظام المعلومات المحاسبي "**AIS**" لهذا سوف نستعرض بعضها كالاتي:

نظام المعلومات المحاسبي : يعد بانه الجزء الأساسي والأهم من نظام المعلومات الإدارية للمؤسسة في مجال المال و الأعمال، والذي يقوم بجمع وحصر البيانات المالية من مصادر داخلية وخارجية للمؤسسة، وبعد ذلك

[1] نهاد محمد وهيب وأخرون ،**تقويم نظام المعلومات المحاسبي لشركة التمور العراقية** ،مجلة كلية مدينة العلم ،العراق ،المجلد:14 ،العدد: 02، 2022،ص: 20.

[2] زين عبد المالك **مرجع سبق ذكره** ،ص:46.

تشغيلها وتحويلها إلى معلومات مالية قيمة ومفيدة لمستخدمي هذه المعلومات لمساعدتهم على اتخاذ قرارات مناسبة وملائمة .[1]

ويعرف أيضا : أنه مجموعة من المكونات التي تشكل وسائل ألية و وثائق ومستندات وسجلات وتقارير وإجراءات وأشخاص ومعدات وأدوات تكنولوجيا المعلومات والاتصال، والتي تتكامل وتتفاعل مع بعضها البعض لتحقيق هدف معالجة البيانات المحاسبية. يتم ذلك من خلال تسجيل وتجميع وتبويب وتلخيص البيانات المحاسبية، ثم تحويلها إلى معلومات محاسبية يتم تمثيلها في شكل قوائم مالية.[2]

كما يعرف : على أنه عبارة عن مجموعة من المعدات" **hardware** "والبرمجيات " **software** " القادرة على تحويل المدخلات إلى المخرجات ،أي تحويل البيانات المحاسبية " **data Accounting**" إلى معلومات محاسبية " **Information Accounting** " من خلال تلخيص واسترجاع واختبار وتلبية محتاجي المعلومات .[3]

كما يعرف أيضا: أنه عملية جمع وتسجيل البيانات المحاسبية ومعالجتها وتلخيصها وتجميعها وتقديمها للمستخدمين الداخلين والخارجين.[4]

و على ضوء ما سبق يمكننا تقديم تعريف يلخص كل تعاريف مذكورة سابقا: نظام المعلومات المحاسبية هو مجموعة من العمليات والإجراءات والأدوات التكنولوجية التي تهدف إلى جمع وتسجيل ومعالجة البيانات المحاسبية من مصادر متعددة، ثم تحويلها إلى معلومات محاسبية مفيدة للمستخدمين الداخلين والخارجين، وذلك من خلال استخدام مجموعة من المكونات والأدوات المختلفة، بما في ذلك الأجهزة الحاسوبية، والبرمجيات، والوثائق والسجلات، والتقارير، والإجراءات، والأشخاص، والمعدات، والأدوات التكنولوجية الأخرى، ويتم عرض هذه المعلومات في شكل قوائم مالية.

---

[1] علي عبد الفاتح الشاهر وأخرون ،**تصميم نظام المعلومات المحاسبي بإستخدام برمجية (Excel /Ms)** ،مجلة تنمية الرافدين ،العراق ،المجلد :41 ،العدد:133 ،2022، ص:15.

[2] زعابطة عبد اللطيف ،**مرجع سبق ذكره** ،ص:50.

[3] Turner, Leslie, et al. ***Accounting Information Systems: The Processes and Controls***. John Wiley and Sons, USA , 2016.P : 04.

[4] Mancini, Daniela, et al. ***Accounting Information Systems for Decision Making***. Springer Science and Business Media, Germany ,2013,P: 07.

4-1-أهداف نظام المعلومات المحاسبي : إن هدف أي نظام معلومات محاسبي هو تزويد كافة المستخدمين بالمعلومات الضرورية التي يحتاجونها ،بحيث تتجلى هذه أهداف فيما يلي:

- تزويد المتلقي بالمعلومات المناسبة لاتخاذ القرارات الصائبة المتعلقة بتخصيص الموارد النادرة والاستفادة الأمثل منها.
- تزويد بالمعلومات اللازمة لتوجيه الموارد البشرية والمادية بشكل فعال، والمساهمة في زيادة كفاءتها في مجالات متعددة، بالإضافة إلى مراقبة الأداء والتحكم في الجودة.
- تزويد بالمعلومات التي تساعد الإدارة في أداء دورها كوكيل لملاك الموارد المتاحة وتقديم التقارير اللازمة للأطراف المعنية، وذلك لتمكينهم من اتخاذ القرارات المناسبة بشأن الاستمرار أو عدم الاستمرار في النشاط بشكل مستمر.[1]
- يهدف نظام المعلومات المحاسبي إلى تحقيق الحماية الكافية لأموال المؤسسة ومراقبتها وذلك من خلال من خلال اتباع الإجراءات والتعليمات المتعلقة بتسجيل ومعالجة بيانات وفقا للقواعد محاسبية. وبفضل المعلومات التي يوفرها النظام، تتمكن الإدارة من متابعة ومراقبة نشاط العاملين، بينما يستطيع أصحاب المؤسسة متابعة ومراقبة نشاط الإدارة وتقييم كفاءتها والتأكد من سير كافة أوجه النشاط في المؤسسة بشكل جيد وسليم.[2]

4-2-أهمية نظام المعلومات المحاسبي: تعد أنظمة المعلومات المحاسبية عنصرا هاما لدي أ مؤسسة لما تقدمه من معلومات والتي استنادا لها تتخذ مجموعة من قرارات ،لهذا تتحدد هذه الأهمية في ما يلي:

- يُمكن من توفير معلومات محاسبية مفصلة ودقيقة تعكس الصورة الحقيقية للوضع المالي للمؤسسة.
- إن توفير المعلومات الأكثر دقة وتفصيلاً المتعلقة بالأعمال المؤسسة يساعد في تحسين أدائها عن طريق فهم أفضل للمعلومات التي تشكل أساسًا لاتخاذ القرارات وتعزيز اتصالها مع الأطراف المختلفة.[3]
- توفر المعلومات ذات موثوقية والتي على أساسها توضع الاستراتيجيات وترسم السياسات وتعد الخطط.
- تساهم في تعزيز مردودية المؤسسة وزيادة أداءها المالي مما يسمح بتحقيق أهدافها على الآجال القصيرة أو الطويلة.

---

[1] زين عبد المالك ،**مرجع سبق ذكره** ،ص:57- 58.

[2] ربيع بن يحي وأخرون ،**مرجع سبق ذكره** ،ص:23.

[3] علي عبد الفاتح الشاهر وأخرون ،**مرجع سابق** ،ص:17.

- تقدم المعلومات الضرورية لتقييم الأداء وتحليله بشكل دقيق ومناسب، وذلك لاتخاذ القرارات الملائمة وتحسين وضعها الحالي.[1]

المطلب الثاني : مخاطر تطبيق أنظمة المعلومات المحاسبية :

تعد أنظمة المعلومات المحاسبي أداة أساسية لدى المؤسسات في أداء مهامها باختلاف أشكالها وأنواعها وهذا مع التطورات والتغيرات التكنولوجية المتواصلة واتساع استخدامها في جل المجالات تقريبا ،ومع ذلك فهي تتعرض هذه الأنظمة إلى العديد من الأخطار والتهديدات التي توجهها عند أنجاز أعمالها مما تؤثر على كفاءة وفعالية أدائها وكذا دقة وسلامة بياناتها . ومن خلال هذا المطلب سوف نقدم بعض العموميات حول مخاطر أنظمة المعلومات المحاسبية وأسباب التي تؤدي إلى حدوثها.

1- المخاطر المتعلقة ببيئة أنظمة المعلومات المحاسبية

1-1- تعريف المخطر " The Risk": وفقا لمعيار **ISO 31000 "RMS"** يعرف بانه : هو التأثير عدم اليقين أو عدم التأكد على الأهداف ،وهذا التأثير هو الانحراف إيجابي أو سلبي عن المتوقع.[2] بمعنى أخر هو: هو حادث احتمالي غير مؤكد الوقوع ينتج عن وقوعه نتائج غير مرغوب فيها.

يعرف أيضا بانه : تقدير مدى احتمال حصول الحدث وما ينجم عنه من عواقب ،ويمكن اختصار تعريف الخطر عن طريق "معادلة المخاطرة" : الخطر= التهديدات * الثغرات * الأثر ،وتعتبر هذه المعادلة أكثر استعمالا وشيوعا في مجال إدارة وتسيير المخاطر وكذا تحديد وتقييم المخاطر.[3]

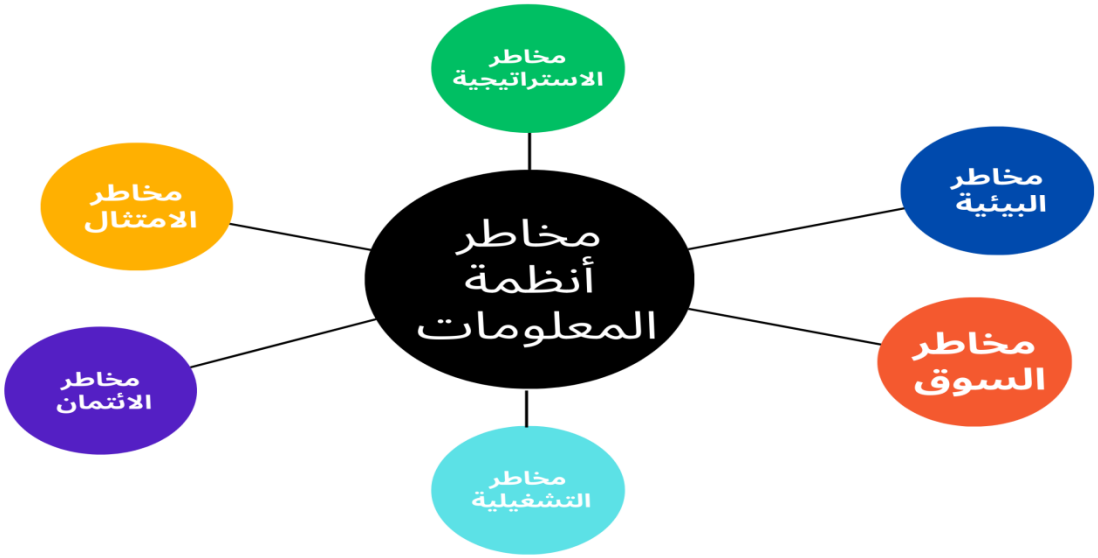
ويتضح من خلال الشكل التالي بان هناك العديد من المخاطر التي تصطدم في وجه المؤسسة:

[1] بوعزيز رضا ،**مرجع سابق** ،ص:43.

[2] International Organization for Standardization ,https://www.iso.org/obp/ui#iso:std:iso:guide:73:ed-1:v1:en , 18/03/2023,23 :21.

[3] Nicolas Mayer, Jean philippe Humbert, ***« la gestion des risques pour les systèmes d'information*** » , centrede recherche public Henri Tudor, Article paru dans le magasin MISC n24 , 2006 ,p3.

الشكل رقم (04) : يوضح مخاطر أنظمة المعلومات



المصدر : من إعداد الطالبان بناءا ISACA, **“ *The Risk IT Framework Excerpt*”**, United States of America, The Information Systems Audit and Control Association, 2009 ,P:11.

1-2- مفهوم مخاطر أنظمة المعلومات المحاسبية : هي عبارة عن مجموعة متنوعة من التهديدات والمخاطر ابتداء من المدخلات الخاطئة للمعاملات ووصولا إلى أشخاص الذين يمتلكون أمكانيات الوصول الى شريط النسخ الاحتياطي الذي يحتوي على جميع البيانات المالية والهامة للمؤسسة.[1]

2- أسباب ظهور المخاطر التي تواجه نظام المعلومات المحاسبي :

تواجه نظم المعلومات المحاسبية الكثير من المخاطر التي تهدد أمنها واستقرارها ،وتعود هذه المخاطر إلى عدة أسباب والتي لها علاقة إما بالنظام بحد ذاته (مدخلات ، معالجة ،مخرجات) أو بالقائمين عن النظام (الموظفين) ،وكذلك لا يجب أن ننسى أسباب

المتعلقة بالمخاطر البيئية لنظام ،وتتلخص هذه الأسباب في العناصر التالية :[2]

- عدم كفاية وفعالية الأساليب والأدوات الرقابية المطبقة من إدارة المؤسسة.

[1] تك مقدم من موضوع, https://cutt.us/8RN4b ,18/03/2022, 00:10.

[2] حرية شعبان محمد الشريف ،**مخاطر نظم المعلومات المحاسبية الإلكترونية** ،رسالة ماجستير في المحاسبة والتمويل ،كلية التجارة ،جامعة الإسلامية ،غزة، 2006 ،ص:84 - 85.

- ضعف أنظمة الرقابة الداخلية لدى المؤسسة وعدم فعاليتها.
- تشارك بعض الموظفين في استخدام نفس كلمة السر من أجل الدخول إلى النظام والعبث في محتوياته.
- عدم الفصل بين المهام والوظائف المحاسبية المتعلقة بنظام المعلومات المحاسبية في المؤسسة .
- عدم وجود سياسات واضحة ومحددة مسبقا ومكتوبة فيما يتعلق بأمن نظم المعلومات المحاسبي في المؤسسة .
- عدم توفر الحماية الازمة لمخاطر الفيروسات الحواسيب.
- ضعف نظام الرقابة المطبقة على مخرجات نظام المعلومات المحاسبي.
- عدم توفر الخبرة اللازمة والمؤهلات العلمية والعملية والمهارات المطلوبة لتنفيذ الأعمال من قبل موظفي المؤسسة.
- عدم وجود الوعي الكافي لدى موظفين بضرورة فحص أي برامج أو روبط خارجية أو أقراص ممغنطة جديدة قبل إدخالها إلى جهاز الحاسوب.

3- تصنيفات مخاطر نظم المعلومات المحاسبي :

إن استخدام تطبيقات وبرامج نظم المعلومات المحاسبية من طرف مؤسسات المال والأعمال يوفر لها العديد من المزايا والمنافع ،لكن في الوقت نفسه يعرضها للكثير من المخاطر والتهديدات التي تستهدف بياناتها ومعلوماتها المحاسبية ،ويمكن تصنيف هذه المخاطر إلى أنواع مختلفة من وجهات نظرة متعددة:

- من حيث مصدرها : مخاطر داخلية ، مخاطر خارجية
- من حيث المتسبب :مخاطر بشرية ،جرائم الحوسبة ، مخاطر بيئية
- من حيث أساس العمدية : مخاطر متعمدة ومخاطر غير متعمدة
- من حيث الأثار الناجمة عنها : مخاطر تنتج عنها أضرار مادية ،مخاطر فنية ومنطقية
- من حيث علاقتها بالنظام: مخاطر مدخلات ،مخاطر المعالجة ،مخاطر مخرجات

وفيما يلي توضيح لهذه المخاطر:

أولا: من حيث المصدر: وتنقسم إلى نوعين :[1]

[1] زين عبد المالك، **مرجع سبق ذكره** ،ص: 74 - 75.

أ– مخاطر داخلية : إن استخدام برامج تكنولوجيا المعلومات IT في النظم المحاسبية أدى إلى تخفيض مخاطر الداخلية ،فالنظم الألية قللت من التهديدات الناشئة عن الأخطاء العشوائية وتعتبر مخاطر الداخلية مرتبطة بصفة مباشر بالموظفين باعتبارهم هم مصدر الرئيسي لهذه المخاطر ، ومع هذا فإن عملية زيادة استخدام النظم الألية أدى بصورة مباشرة إلى زيادة احتمالية الوقوع في جرائم الحاسوب مثل :السرقة ،الاختلاس ،التزوير .وفيما يلي بعض مخاطر الداخلية :

- ❖ دخول غير مصرح للبيانات والبرامج المحاسبية
- ❖ استخدام الحاسوب للارتكاب أعمال غير نظامية
- ❖ فقدان البيانات وتحريفها أثناء تحويلها من المستخدم إلى مركز معالجة بيانات.
- ❖ مراجعة وتصحيح غير مناسب للبيانات بعد ترميزها
- ❖ ضياع أو تحريف قاعدة البيانات المحاسبية

ب– مخاطر خارجية : وتكون هذه المخاطر صادرة من أشخاص الذين ليس لهم علاقة مباشرة بالمؤسسة مثل : قراصنة خارجيون ، منافسين الذين يحاولون اختراق الضوابط الرقابية بهدف حصول على معلومات سرية عن المؤسسة أو تتمثل في كوارث طبيعية مثل: فيضانات ، براكين ، زلازل قد تدمر أنظمة المؤسسة.

ثانيا: من حيث المتسبب : يمكن تصنيف الأخطار التي يمكن أن يتعرض لها نظام المعلومات المحاسبي من حيث المتسبب فيها بشكل عام إلى ثلاث فئات :[1]

أ– مخاطر بشرية : ويمكن تعريفها بأنها تلك الأخطار التي يمكن أن تحدث في أثناء إعداد وتصميم التجهيزات وقنوات الاتصال وأجهزة الحاسوب التي ستعمل على تنفيذ نظم المعلومات، وكذلك من خلال عمليات البرمجة أو الاختيار أو تجميع البيانات أو إدخالها إلى النظام، وتشكل الأخطار البشرية أغلب المشكلات التي تواجهه أمن وسلامة نظم المعلومات المحاسبية في المنظمات.

ب– جرائم الحوسبة : يترتب على استخدام تطبيقات نظم المعلومات المحاسبية المعقدة ظهور ما يطلق عليه "بجرائم الحاسبات" ،حيث يقصد بها استخدام برامج نظام المعلومات بصورة مباشرة أو غير مباشرة في القيام

[1] زعابطة عبد اللطيف ، **مرجع سبق ذكره** ،ص : 125 – 126.

بتصرفات غير قانونية مثل : السرقة ،الاختلاس ،تحريف البيانات.... ،مما يؤدي إلى إضرار بمصالح الأطراف التي لها علاقة بالمؤسسة والممثلين في مستخدمي المعلومات المحاسبية.

ج– مخاطر بيئية : وهي المخاطر التي تكون نتيجة العوامل الطبيعية والبيئية والتي تهدد أنظمة و أجهزة معلومات المؤسسة مثل : الزلازل ، العواصف ، الفيضانات ، الأعاصير ، والأخطار المتعلقة بالحرائق والتيار الكهربائي.

ثالثا : من حيث أساس العمدية : يمكن تقسيمها إلى نوعين :[1]

أ – مخاطر متعمدة : و تتمثل في تصرفات يقوم بها الشخص متعمدا مثل ادخال بيانات خاطئة وهو يعلم ذلك، أو قيامه بتدمير بعض البيانات متعمدا ذلك بهدف الغش والتلاعب والسرقة، وتعتبر هذه المخاطر من المخاطر المؤثرة جدا على النظام.

ب– مخاطر غير متعمدة : وتتمثل في تصرفات يقوم بها الأشخاص نتيجة الجهل وعدم الخبرة الكافية كإدخالهم لبيانات بطريقة خاطئة بسبب عدم معرفتهم بطرق ادخالها أو السهو في عملية التسجيل وتعتبر هذه المخاطر أقل ضررا من المخاطر المقصودة وذلك لإمكانية إصلاحها.

رابعا : من حيث الأثار الناجمة عنها : وتصنف إلى نوعين:

أ– مخاطر تنتج عنها أضرار مادية: و هي المخاطر التي تسبب أضرارًا للنظام أو للأجهزة الحاسوبية، أو تؤدي إلى تدمير وسائل التخزين، ويمكن أن تنجم عن كوارث طبيعية لا يمكن التحكم بها، أو قد تنشأ بسبب تدخلات بشرية سواء كانت مقصودة أو غير مقصودة.

ب – مخاطر فنية ومنطقية: وهي المخاطر التي تؤثر على سلامة وسرية البيانات و التي قد تعرضها للخطر، إما بتعطل ذاكرة الحاسوب أو بإدخال فيروسات تؤدي إلى تلف أو فقدان جزء من البيانات، وقد تؤدي هذه المخاطر إلى الكشف عن بيانات سرية من طرف أشخاص غير مخولين برؤيتها، مما يعرض المؤسسة لخسائر قد تؤثر على مكانتها التنافسية في السوق.[2]

[1] حرية شعبان محمد الشريف ، مرجع سبق ذكره ،ص : 76.

[2] عبد المالك زين وأخرون ، **أثر مخاطر نظام المعلومات المحاسبي على جودة المعلومات المحاسبية** ،مجلة رؤئ اقتصادية ، الوادي ،الجزائر ، المجلد : 09 ، العدد :02 ، 2019 ،ص : 414 .

خامسا : من حيث علاقتها بالنظام:

أ– مخاطر مدخلات : وهي المخاطر الناتجة عن عدم تسجيل البيانات في الوقت المناسب, وبشكلها الصحيح أو عدم نقل البيانات بدقة خلال خطوط الاتصال. وتتمثل المخاطر المتعلقة بأمن المدخلات إلى أربعة أقسام أساسية وهي:

1– خلق بيانات غير سليمة: ويتم ذلك من خلال خلق بيانات غير حقيقية, ولكن بواسطة مستندات صحيحة يتم وضعها

داخل مجموعة من العمليات دون أن يتم اكتشافها.

2– تعديل أو تحريف بيانات المدخلات: ويتم ذلك من خلال التلاعب في المدخلات والمستندات الأصلية بعد اعتمادها من قبل المسؤول وقبل إدخالها إلى النظام.

3– حذف بعض المدخلات: ويحدث ذلك من خلال حذف أو استبعاد بعض البيانات قبل إدخالها إلى الحاسب الآلي,

وذلك إما بشكل متعمد ومقصود, أو بشكل غير متعمد وغير مقصود.

4– إدخال البيانات أكثر من مرة: والمقصود بذلك قيام الموظف بتكرار إدخال البيانات إلى الحاسب إما بطريقة مقصودة أو غير مقصودة.[1]

ب – مخاطر المعالجة : ويقصد بها المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسوب والبرامج التي تقوم بمعالجة تلك البيانات، وتتمثل مخاطر المعالجة في الاستخدام غير المصرح به لنظام وبرامج المعالجة وتحريف وتعديل البرامج بطريقة غير قانونية أو عمل نسخ غير قانونية أو سرقة البيانات الموجودة على الحاسوب، ومثال ذلك قيام موظف بإعطاء أوامر للبرنامج بأن لا يسجل أي قيود في السجلات المالية تتعلق بعمليات البيع الخاصة بعميل معين من أجل الاستفادة من مبلغ العملية لصالح المحرف نفسه.[2]

[1] ماهر فؤاد زهيري ، **مخاطر أمن نظم المعلومات المحاسبية الإلكترونية و استراتيجيات مواجهتها** ، رسالة ماجستير في المحاسبة ، كلية الاقتصاد ، جامعة تشرين ، سوريا ، 2015 ، ص :46.

[2] زين عبد المالك ، **مرجع سبق ذكره** ،ص : 79.

ج- مخاطر المخرجات : ويقصد بها المخاطر المتعلقة بالمعلومات والتقارير التي يتم الحصول عليها بعد عملية تشغيل ومعالجة البيانات, وقد تحدث تلك المخاطر من خلال طمس أو تدمير بنود معينة من المخرجات, أو خلق مخرجات زائفة وغير صحيحة, أو سرقة مخرجات الحاسب, أو إساءة استخدامها.[1]

3- أنواع المخاطر التي تتعرض لها أنظمة المعلومات المحاسبية :

تعتبر نظم المعلومات المحاسبية نافذة من النوافذ التي يحاول مجرمي الأنترنت الدخول منها وذلك بإتباع العديد من الطرق والاستراتيجيات ، ومن خلال ما سبق يمكننا تقسيم هذه المخاطر كالاتي:

3-1- مخاطر خرق الحماية المتعلقة بالأشخاص وشؤون الموظفين: تعد هذه المخاطر متصلة بصفة مباشر مع الموظفين ،أي أن مصدر هذه المخاطر يكون من داخل المؤسسة ،وعموما تتنوع هذه المخاطر ،نذكر منها:

أ- التخفي بانتحال صلاحيات المفوض "Masquerading ": يقصد به بانه نوع من إجراءات التهديد حيث يكتسب كيان غير مصرح له إمكانية الوصول إلى نظام أو يقوم بعمل ضار من خلال التظاهر بشكل غير قانوني بأنه كيان مرخص له.[2]

ب- الهندسة الاجتماعية "Social Engieneering" : هي هجمات إلكترونية تنشأ عن تفاعل بشري، حيث يكتسب المهاجم ثقة الضحية من خلال الاصطياد أو التخويف أو التصيد الاحتيالي، ويجمع المعلومات الشخصية ويستخدمها لتنفيذ هجوم.[3]

ج- الإزعاج أو التحرش"Harassment": وهي تهديدات يجمعها توجيه رسائل الازعاج والتحرش وربما التهديد والابتزاز أو في أحيان كثيرة رسائل المزاح على نحو يحدث مضايقة.

د- قرصنة البرمجيات " Software Piracy " : وهي عملية قرصنة البرامج وتتحقق عن طريق نسخها دون تصريح أو استغلالها على نحو مادي دون تخويل بهذا الاستخدام ، أو تقليدها ومحاكاتها والانتفاع المادي بها على نحو يخل بحقوق المؤلف.

3-2- مخاطر خرق الحماية المتعلقة بالاتصالات والمعطيات: يقصد بهذه المخاطر العمليات والأنشطة والهجمات التي تستهدف المعطيات والبرامج من قبل مجرمي الأنترنت ،وتنقسم إلى نوعين:

---

[1] مرجع سابق .

[2] NIST,https://csrc.nist.gov/glossary/term/masquerading#:~:text=Definition(s)%3A,posing%20as%20an%20aut horized%20entity,22/03/2023,15:43.

[3] Microsoft, https://cutt.us/mOdkU ,22/03/2023,16:03.

أ- هجمات المعطيات " Data Attacks": وتتضمن مايلي:

- **النسخ غير مصرح به للمعطيات "Unauthorized Copying of Data"**: هي عملية استيلاء على كافة أنواع المعطيات عن طريق النسخ ، وهنا تشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها.
- **تحليل الاتصالات Traffic analysis**: الهجوم هنا ينصب على دراسة أداء النظام في مرحلة التعامل ومتابعة ما يتم فيه من اتصالات وارتباطات بحيث يستفاد منها في تحديد سلوكيات المستخدمين وتحديد نقاط ضعفهم ووقت الهجوم المناسب أي الرقابة على حركة النظام.
- **القنوات المخفية Covert chanels**: وهي عملياً صورة من صور اعتداءات التخزين ، حيث يخفي المقتحم معطيات أو برمجيات او معلومات مستولى عليها كأرقام بطاقات ائتمان في موضع معين من النظام وتتعدد أغراض الاخفاء ، فقد تكون تمهيدا لهجوم لاحق أو تغطية اقتحام سابق.[1]
- **شخص في الوسط "Man in the Middle"**: هو هجوم يعترف فيه المهاجم اتصالا بين طرفين يتطلب هجوم رجل في الوسط أن يضع المهاجم نفسه بين طرفين متصلين وينقل الرسائل لهما ، بينما يعتقد الطرفان أنهما يتواصلان مع بعضهما البعض بشكل مباشر بهدف مراقبة محتويات الرسائل وربما تغييرها.[2]
- **هجوم التصيد "Plishing attack "**: يحدث التصيد الاحتيالي عندما يحاول المهاجمون خداع المستخدمين للقيام "بشيء خاطئ" ، مثل النقر فوق ارتباط سيئ يؤدي إلى تنزيل برامج ضارة أو توجيههم إلى موقع ويب مخادع. لكن مصطلح "التصيد الاحتيالي" يستخدم بشكل أساسي لوصف الهجمات التي تصل عبر البريد الإلكتروني ، أي هو هجوم يحاول فيه المهاجم خداع المستخدم للكشف عن معلومات حساسة.[3]

[1] امجد يوسف إسماعيل ،**مخاطر نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الأردنية** ،رسالة ماجستير في محاسبة والتمويل ،الأردن ،2011، ص : 28– 29.

[2] ENISA , https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle ,22/03/2023,20:10.

[3] National Cyber Security Centre, https://www.ncsc.gov.uk/guidance/phishing ,22/03/2023 ,20:15.

✧ **SQL injection attack**: هو هجوم يستغل فيه المهاجم ثغرة أمنية في قاعدة البيانات "Database" لأجل تعديل هذه البيانات أو حذفها مما يتسبب في تغييرات مستمرة في محتوى التطبيق أو سلوكه ، في بعض الحالات يمكن للمهاجم تصعيد هجوم حقن SQL لخرق الخادم الأساسي أو البنية التحتية الخلفية الأخرى ، أو تنفيذ هجوم رفض الخدمة DDOS.[1]

✧ **رفض خدمة الموزع "Distributed denial of service (DDOS)"**: هو محاولة خبيثة لتعطيل حركة المرور العادية للخادم أو الخدمة أو الشبكة المستهدفة من خلال إغراق الهدف أو البنية التحتية المحيطة به بهجوم فيضان SYN من الألاف البرامج الموزعة المرتبطة بالشبكة.[2]

ب- هجمات البرمجيات : وتحتوي على ما يلي:

✧ **الأبواب الخلفية "Trap door"** يسمى أيضًا(باب المصيدة) هو برنامج يسمح بالوصول غير المصرح به إلى النظام دون المرور بإجراء تسجيل الدخول العادي قد تكون أهدافه هو توفير وصول سهل لأداء البرنامج الصيانة ، أو قد تكون لارتكاب عملية احتيال أو إدخال فيروس في النظام.[3]

✧ **إختطاف الجلسة " Session Higacking"**: بكل بساطة هي أن يجلس مهاجم مكان مستخدم النظام فيطلع على المعلومات أو يجري أية عملية في النظام أي يستولي فيها المهاجم على الجلسة بين المستخدم والخادم.[4]

✧ **هجمات عبر التلاعب بنقل المعطيات عبر أنفاق النقل "Tunneling"**: هي تلك الأنفاق التي تستخدم لنقل البيانات عبر الشبكة باستخدام بروتوكولات لا تدعمها تلك الشبكة مثل الشبكات الخاصة الافتراضية VPN, [5] وهنا تصبح طريقة للاعتداء عندما يتم نقل معطيات غير مشروعة عبر هذه الأنفاق.

---

[1] Port swigger Centre , https://portswigger.net/web-security/sql-injection ,22/03/2023,21:00.

[2] Cloud Flare , https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ ,22/03/2023,21:10.

* **فيضان SYN flood**: هو نوع من هجوم رفض الخدمة (DDoS) الذي يهدف إلى جعل الخادم غير متاح لحركة المرور المشروعة من خلال استهلاك جميع موارد الخادم المتاحة.

[3] Hall, James A. *Accounting Information Systems*. Seventh Edition, Cengage Learning, USA , 2010.P:727.

[4] امجد يوسف إسماعيل ،**مرجع سبق ذكره** ،ص :32.

[5] Cloud Flare ,**Idem , https://www.cloudflare.com/learning/network-layer/what-is-tunneling/ .**

- **هجمات الوقتية "Timing attacks"**: وهي هجمات تتم بطرق تقنية معقدة للوصول غير المصرح به الى البرامج أو المعطيات ، وتقوم جميعها على فكرة استغلال وقت تنفيذ الهجمة متزامنا مع فواصل الوقت التي تفصل العمليات المرتبة في النظام.[1]
- **تهكير كلمات المرور"Password Cracking"**: هو مجموعة من التدابير المختلفة المستخدمة لاكتشاف كلمات مرور الكمبيوتر .أي عملية تخمين كلمات المرور للوصول إلى النظام وتكون هذه لعدة أغراض ولكن الغرض الأكثر ضررًا هو الحصول على وصول غير مصرح به إلى جهاز كمبيوتر دون علم مالك الكمبيوتر. ينتج عن هذا الجرائم الإلكترونية مثل سرقة كلمات المرور بغرض الوصول إلى المعلومات المصرفية.[2]
- **روبوتات "Botunet"**: هي عبارة عن أجهزة الكمبيوتر المختطفة المستخدمة لتنفيذ العديد من عمليات الاحتيال والهجمات الإلكترونية ، بمعنى أخر هي شبكة حواسيب يسيطر عليها مهاجم لتنفيذ الهجمات بحيث يستخدمها المهاجم كأداة لأتمتة الهجمات الجماعية ، مثل سرقة البيانات وتعطل الخادم وتوزيع البرامج الضارة.[3]
- **هجوم القوة الغاشمة"Brute force attack"**: يستخدم هجوم القوة الغاشمة التجربة والخطأ لتخمين معلومات تسجيل الدخول أو مفاتيح التشفير أو البحث عن صفحة ويب مخفية. يعمل المتسللون من خلال جميع المجموعات الممكنة على أمل التخمين بشكل صحيح. هذه طريقة هجوم قديمة ، لكنها لا تزال فعالة ، بمعنى أخر هو هجوم يحصل فيه مهاجم على وصول إلى النظام الكمبيوتر عن طريق تخمين كلمات المرور.[4]
- **البرمجيات الخبيثة" malware"** : نذكر منها : الديدان Worms, القنابل المنطقية Logic, حصان الطروادة Trojan horse, الجذور الخفية rootkit, سلامي Salamis, Bomb, فيروسات Viruses , زومبي Zombie , إدواري Adware .....

[1] امجد يوسف إسماعيل ، **مرجع سبق ذكره** ،ص:33.
[2] Techopedia , https://www.techopedia.com/ , 23 /03/2023,09:00.
[3] Kaspersky , https://usa.kaspersky.com/resource-center/threats/botnet-attacks ,23/03/2023,09:30.
[4] Ibid, https://www.kaspersky.com/resource-center/definitions/brute-force-attack .

جميع هذه البرمجيات تمتلك صفة مشتركة وهي أنها تعتبر برمجيات ضارة، تهدف إلى التسبب في الضرر والتدمير سواء كان ذلك بتدمير النظام أو البرمجيات أو المعطيات أو الملفات أو الوظائف، أو استغلالها للقيام بمهام غير مشروعة مثل الاحتيال أو الغش في النظام.[1]

تشكل الفيروسات والهجمات الإلكترونية وسيلة شائعة وفعالة لنشر البرمجيات الضارة عبر الإنترنت ، وقد أصبحت هذه الهجمات منظمة وتسبب خسائر كبيرة تصل إلى الملايين. وبالتالي، فإنه يجب على المستخدمين اتخاذ إجراءات الوقاية والحماية لمنع هذه البرمجيات الضارة من التسبب في الاضرار وإتلاف أنظمة المؤسسات .

المطلب الثالث : الأمن السيبراني لحماية أنظمة المعلومات المحاسبية

يعتبر الأمن السيبراني للأنظمة المعلومات المحاسبية من الأمور الحيوية والحاسمة التي يجب على أي مؤسسة مهتمة بالحفاظ على بياناتها المالية وتأمين سريتها وحمايتها من الاختراقات الإلكترونية الضارة أن توليه اهتماماً كبيراً. فالأنظمة المعلوماتية المحاسبية هي أحد أهم الأدوات التي تستخدمها المؤسسات لإدارة أعمالها ومراقبة نشاطاتها المالية، وبالتالي فإن أي خلل أو اختراق يمكن أن يؤدي إلى تعرض هذه المعلومات للخطر وتعريض المؤسسة للأضرار المالية والقانونية. لهذا ومن خلال هذا المطلب سوف نقدم بعض المفاهيم العامة حول الأمن السيبراني وكذا علاقته بنظام المعلومات المحاسبي والمعايير المتعلقة به.

1- عموميات حول الأمن السيبراني Cyber security :

1-1- تعريف الأمن السيبراني : لغوياً: الأمن السيبراني مكوّن من لفظتين: "الأمن"، و"السيبراني"

الأمن: هو نقيض الخوف، أي بمعنى السلامة. والأمن مصدر الفعل أَمِنَ أَمْناً وأَمَاناً وأَمَنَةً: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه. وقد عرّفه قاموس بنغوين للعلاقات الدولية بأنه مصطلح يشير إلى غياب ما يُهدد القيم النادرة .

السيبراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي، وتشير المقاربة الإيتيمولوجية لكلمة "cyber" إلى أنها لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة.[2]

[1] امجد يوسف إسماعيل ، **مرجع سبق ذكره** ،ص:33.

[2] الموسوعة السياسية، https://cutt.us/rshaZ، 2023،22:20/03/24.

يشير مصطلح "الأمن السيبراني" أو ما يطلق عليه ب " أمن نظم المعلومات " إلى أنه : عبارة عن مجموعة من الإجراءات والسياسات والأدوات والمفاهيم الأمنية والمبادئ التوجيهية التي تستخدم لتحديد وتقييم وتقليل المخاطر التي تهدد البيئة الإلكترونية، والتي تتضمن معالجة المعلومات وحماية الموارد الرقمية وتنظيم أصول المستخدمين. وتتضمن هذه الإجراءات أيضًا التدريب على أفضل الممارسات وضمان الاستخدام الآمن للتقنية المختلفة التي تساعد على حماية الأنظمة والشبكات الإلكترونية.[1]

وعرفه "**Martti Lehto** " وأخرون على أنه : " :عبارة عن مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قراصنة الكمبيوتر وعواقبها، ويتضمن تنفيذ التدابير المضادة المطلوبة.[2]

وعرف أيضا بإنه : خارطة الطريق للإكتشاف الهجمات الإلكترونية وتحديدها من خلال تطوير أساليب متقدمة لكشف عن التهديدات وصدها ومحافظة على أمن وسلامة المعلومات .[3]

وعلى ضوء ماسبق يمكن القول بإن "الأمن السيبراني" : هو عبارة على مجموعة من الاساليب والأدوات والسياسات الأمنية المستخدمة لمواجهة تحديات الفضاء السيبراني الممثلة في الانشطة والهجمات السيبرانية للمحافظة على أمان المعلومات وسرية البيانات وسيرورة وتوافر الأنظمة والشبكات الإلكترونية ومجابهة كافة أنواع التهديدات والاختراقات التي تسعى لتدمير البنية التحتية الحيوية.

1-2- أهمية الأمن السيبراني : تتمثل أهميته فيما يلي:[4]

- يهدف الحفاظ على البيانات إلى ضمان سلامتها وتكاملها ومنع التلاعب بها.
- تحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها.
- حماية الأجهزة والشبكات والحفاظ عليها من الاختراقات والتجاوزات.
- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

---

[1] وفاء مطروح وأخرون ،**تداعيات جائحة كوفيد – 19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر** ،المجلة الدولية للإتصال الاجتماعي ، المجلد:09 ،العدد:02 ،مستغانم ،2022،ص:222.

[2] Lehto, Martti, and Others . *Cyber Security: Analytics, Technology and Automation*. Springer, Switzerland, 2015.P :25.

[3] Parker, Sandra, et al. “Cybersecurity in Process Control, Operations, and Supply Chain.” *Computers & Chemical Engineering*, vol. 171, Elsevier BV, _Netherlands ,Feb . 2023,. https://doi.org/10.1016/j.compchemeng.2023.1081

* **البنية التحتية الحيوية** : يقصد بها المراكز الحساسة كقطاعات الاتصالات ومحطات الطاقة وقواعد البيانات الحكومية والبنوك والمؤسسات المالية.

[4] وفاء مطروح وأخرون ،**مرجع سبق ذكره**،ص:224.

- توفير بيئة عمل آمنة جداً خلال العمل عبر الشبكة العنكبوتية.
- حماية الشبكات من الولوج غير المصرح به.
- تحسين مستوى حماية المعلومات وضمان استمرارية الأعمال.
- في حالة حدوث خرق للنظام الأمني السيبراني، يتم استيراد البيانات المسربة في أسرع وقت ممكن.

1- 3- عناصره: وهي ثلاثة عناصر أساسية إتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار إليها بثلاثي CIA وهي:[1] السرية confidentiality ، السلامة Integrity ، التوافر Availability .

- **السرية** : هي عبارة على حماية خصوصية المعلومات المتداولة عبر الإنترنت وضمان عدم كشفها لأي طرف غير مخول بها، مما يعزز السرية والأمان لهذه المعلومات.
- **السلامة:** هي عملية عدم التلاعب بالمعلومات، وعدم حذفها أو تعديلها خلال عملية النقل أو التخزين أو المعالجة، مما يضمن دقة وصحة المعلومات ويسمح للمستخدم بالحصول على المعلومات التي يرغب فيها دون تدخل أو تعديل غير مصرح به.
- **التوافر:** يقصد بها استمرار توفير المعلومة للشخص أو الجهة التي يسمح لها المستخدم بالاطلاع عليها عند الحاجة، وبشكل مستمر ومنتظم، وذلك لضمان توافر المعلومة للأطراف المعنية في الوقت المناسب وبشكل دقيق، مما يساعد على اتخاذ القرارات الصحيحة والمناسبة.

2- إجراءات ووسائل الأمن السيبراني في ظل أنظمة المعلومات المحاسبية:

الأمن السيبراني هو مجموعة من الاجراءات والوسائل التي تسمح بالحد من الجرائم والتهديدات السيبرانية المستهدفة للنظام البيئي السيبراني المتمثل في البنية التحتية الحيوية ، وتتضح هذه الوسائل خلال ما يلي :

أ- إدارة كلمة السر"Password Management": تُستخدم كوسيلة للتحقق من هوية المستخدم وتعريفه، وذلك بهدف السماح له بالوصول إلى النظام وتحديد البرامج والملفات التي يُسمح له بالوصول إليها والقيام بالعمل من خلالها.[2]

[1] بن علية بن جدو ،**تحديات اللأمن السيبراني لمواجهة الجريمة الإلكترونية** ، المجلة الجزائرية للأمن الانساني ، المجلد :07 ،العدد:02 ،2022، ص:304,

[2] امجد يوسف إسماعيل ، **مرجع سبق ذكره** ،ص:34.

ب- تشفير البيانات "Data ptography" : تقنية التشفير تُعد واحدة من أهم تقنيات الحماية التي تحظى اهتماماً كبيرا في مجال سرية وموثوقية وسلامة البيانات المتبادلة. تعتمد هذه التقنية على تعديل محتوى الرسالة باستخدام مفتاح التشفير قبل إرسالها، ويكون بإمكان المستقبل استعادة المحتوى الأصلي للرسالة باستخدام مفتاح فك الشفرة. وينقسم إلى قسمين هما :

- **التشفير المتماثل** : يتم استخدام فيه نفس المفتاح لتشفير وفك شفرة الرسالة، وبالتالي يعرف المرسل والمستقبل نفس المفتاح ولا يتم إرساله مع الرسالة، بل يتم إرساله بطريقة أخرى.
- **التشفير غير المتماثل** : يتم استخدام مفتاحين، واحد للمرسل وآخر للمستقبل. يستخدم المفتاح العام لتشفير الرسالة، ويعرفه الجميع، بينما يستخدم المفتاح الخاص لفك الشفرة، ويعرفه فقط المستقبل. يترابط المفتاحان بشكل متبادل ولكن لا يدل أي منهما على الآخر تمامًا، وبالتالي لا يمكن فك الشفرة باستخدام المفتاح العام.

ج- البرمجيات المضادة للاعتداءات الإلكترونية: تعتبر برامج الحماية أكثر البرامج شهرة وانتشارًا بين مستخدمي الحواسيب والشبكات، حيث تقوم بالكشف عن البرامج الخبيثة الموجودة في ذاكرة الحواسيب وتحطيمها ومنع الهجمات الأخرى. ويمكن أن تكون هذه البرامج مخصصة لتحديد تهديد واحد، مثل برنامج " Spybot Search and Destroy" الذي يهدف إلى القضاء على برامج التجسس، أو برنامج "Coffre Fort" الذي يساعد على إنشاء مساحة آمنة للبيانات الحساسة على الحاسوب. كما يمكن أن تكون هذه البرامج متكاملة، حيث تقوم بمجموعة من المهام التي تهدف إلى حماية الحاسوب والمعلومات المخزنة به من التهديدات المختلفة، مثل: برنامج "Kaspersky Internet Security" الروسي ، برنامج Webroot SecureAnywhere ، برنامج Comodo Windows Antivirus.....[1]

ت- النسخ الاحتياطي "Backup": تلجأ إدارة نظم المعلومات لعمل الملفات الاحتياطية (Backup) لحفظ الملفات حيث يتم إعداد نسخ احتياطية من البيانات والبرامج لمواجهة احتمال فقدان أو تخريب البيانات أو البرامج نتيجة أخطاء التشغيل أو نتيجة اختراق نظام المعلومات.[2]

د- الجدران النارية " Firewalls": هي برامج خاصة تعمل على حماية الشبكات التي تكون مرتبطة بشبكة الأنترنت، حيث توضع مع خادم الشبكة، وبالتالي فهي تؤمن الحماية لكل الحاسبات المرتبطة بالشبكة وليس

[1] زعابطة عبد اللطيف ، **مرجع سبق ذكره** ،ص : 140 – 141.
[2] زين عبد المالك ، **مرجع سبق ذكره** ،ص : 83.

الحاسب واحد فقط، تعمل بمدأ ترشيح البيانات وعدم السماح للأشخاص غير المخول لهم بالدخول إلى الشبكة ويمكن لها حتى التحكم في مستخدمي هذه الشبكة بمنعهم من الدخول إلى بعض الملفات دون غيرها. ويوجد نوعين من الجدران النارية كما يلي:

- **الجدران النارية البرمجية:** يمكن استعمال هذا النوع من الجدران على الحاسبات المستقلة أو الحايبات المرتبطة بالشبكة أو على الخوادم ، ومن أشهر هذه البرمجيات نذكر: eSafe Desktop Comoodo ,Zone Alarm Pro.
- **الجدران النارية المادية** : وتسمى كذلك بالعلب السوداء، وهي تستعمل عادة على الخوادم، وهي أكثر قوة من الجدران البرمجية لكونها غير معنية بنقاط ضعف نظام تشغيل الحاسب ومختلف ثغراته. ومن أشهر الجدران المادية نذكر: WatchGuard, WatchGuard Firebox,SOHO .....[1]

هـ- فحص الاختراقات Penetration : يتم استئجار خدمات شركات متخصصة في الأمن السيبراني لتمثيل دور المهاجمين والاختراق إلى النظام، بهدف تحديد نقاط الضعف التي يمكن اختراقها في نظام الأمن، ثم يتم إخطار إدارة الشركة بتلك النقاط لإصلاحها. وهذا يساعد الشركة في تقييم قدراتها على منع وكشف الوصول غير المصرح به إلى النظام، وتحسين دفاعات الشبكة.

و- تقنيات الاشعار بالاستلام الرسالة (إختبار الصدى Echo check): هي عبارة عن تقنيات برمجية تستخدم للتحقق من استلام البيانات بشكل كامل من قبل الوحدة المتلقية، وذلك من خلال عملية المصادقة التلقائية.

ز- الإجراءات التنظيمية Organizational Procedures: وهي تعني أن يتم تنظيم ومراقبة الوصول إلى البرامج والبيانات المخزنة في نظم المعلومات بعناية "السيطرة على الوصول" (Access Control) . ويتم ذلك من خلال تحديد سياسات وإجراءات الأمان وتطبيقها، وتحديد مستويات الصلاحية للمستخدمين والمسؤولين في النظام، وتطبيق تقنيات الحماية المناسبة للموارد المختلفة. ويتم ذلك عن طريق الهيكل التنظيمي لدائرة نظم المعلومات والفصل بين الوظائف المختلفة المسؤولة عن تطبيق سياسات الأمان والسيطرة على الوصول.

[1] زعابطة عبد اللطيف ،مرجع سابق .

ر- السياسات والإجراءات Policies & Procedures: وهي عبارة على تطوير وتنفيذ سياسات وإجراءات للتعامل مع أخطاء النظام في مجال البرامج والبيانات وأنظمة التشغيل وتوضيحها للعاملين بحيث يمكن معالجتها من خلال أنظمة الأمان لاستعادة النظام وإتاحته للمستخدمين.

ي- مصفوفة الرقابة Access Matrix : وتتم عبر برمجة مصفوفة الرقابة على الوصول آلياً في النظام حيث تتضمن تحديداً للصلاحيات الممنوحة لكل مستخدم ومجموعات المستخدمين في النظام. تتضمن هذه الصلاحيات تحديد البرامج والملفات التي يمكن للمستخدم الوصول إليها، وذلك من خلال تحديد رقم المستخدم وكلمة السر المرتبطة به. [1]

3- متطلبات تحقيق الأمن السيبراني لدى المؤسسات :

تعد مسألة حماية أمن نظم المعلومات المحاسبية من أهم القضايا التي يجب أن تولي المؤسسات اهتماماً كبيراً بها وتطبيق خطط حماية شاملة تتماشى مع إمكانياتها التنظيمية والمادية. يجب أن تكون هذه الحماية قوية وفعالة ولذلك يتطلب الأمر توفر عدة متطلبات لحماية أمن نظم المعلومات المحاسبية، وتشمل: [2]

- ✯ ينبغي وضع سياسة حماية شاملة لأمن نظم المعلومات المحاسبية تتناسب مع طبيعة عمل وتطبيقات المؤسسة.
- ✯ يتعين على الإدارة العليا في المؤسسات دعم جهود حماية نظم المعلومات والاهتمام بها لضمان سلامتها وعدم تعرضها للتهديدات الأمنية.
- ✯ يجب تعيين أشخاص مختصين مسؤولين عن أمن نظم المعلومات في المؤسسات.
- ✯ يجب تحديد متطلبات الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة.
- ✯ يجب تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية.
- ✯ يجب إنشاء نسخ احتياطية لنظم المعلومات بشكل آمن.
- ✯ يجب تشفير المعلومات التي يتم حفظها وتخزينها ونقلها عبر مختلف الوسائط.
- ✯ يجب تأمين استمرارية عمل وجاهزية نظم المعلومات، خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات.

[1] امجد يوسف إسماعيل ، **مرجع سبق ذكره** ،ص:35- 36.

[2] حرية شعبان محمد الشريف ، مرجع سبق ذكره ،ص : 85– 86.

4- المعايير و النماذج العالمية لأمن نظم المعلومات :

تولي العديد من المنظمات الدولية اهتماما كبيرا بموضوع الرقابة في ظل أنظمة المعلومات ، وذلك من خلال إصدار معايير ونماذج وقوانين تحتوي على الأساليب والإجراءات اللازمة لكيفية لإنشاء وتقييم أنظمة رقابة داخلية فعالة تتناسب مع بيئة نظم المعلومات وما ينتجها. مما يسمح بتحقيق الحد الأدنى لأمن المعلومات ومن بين هذه المعايير ونماذج نذكر:

- **SAC**
- **COBIT**
- **NIST**
- **ISO**

وكذا بعض القوانين المرتبطة بأمن المعلومات :

- **SOX**
- **COSO**

4-1- معايير تدقيق أنظمة المعلومات :

هي معايير تقوم بإصدارها الجمعية الدولية لتدقيق والرقابة على أنظمة المعلومات ISACA,وهي هيئة مستقلة تم تأسيسها سنة 1967 وهذا من أجل وضع معايير دولية خاصة بأنظمة المعلومات وكيفية تدقيقها ،وتوضح هذه المعايير في الجدول التالي :

الجدول رقم (01): يوضح معايير تدقيق أنظمة المعلومات

البيان	التبويب
دستور مهنة تدقيق نظم المعلومات	**ISACA 01**
الإستقلالية	**ISACA 02**
الأخلاقيات المهنية	**ISACA 03**
الكفاية المهنية	**ISACA 04**
التخطيط	**ISACA 05**
أداء عملية التدقيق	**ISACA 06**
التقرير	**ISACA 07**
أنشطة المتابعة	**ISACA 08**
المخالفات والتصرفات غير القانونية	**ISACA 09**
حوكمة تكنولوجيا المعلومات	**ISACA 10**
إستخدام تقييم المخاطر في عملية تخطيط التدقيق	**ISACA 11**
الأهمية النسبية في التدقيق	**ISACA 12**
إستخدام عمل الخبراء الأخرين	**ISACA 13**
أدلة إثبات في التدقيق	**ISACA 14**
الضوابط الرقابية لتكنولوجيا المعلومات	**ISACA 15**
التجارة الإلكترونية	**ISACA 16**

المصدر : رواني بوحفص ، **التدقيق المالي والمحاسبي دروس نظرية** ، كلية العلوم الاقتصادية والتجارية وعلوم التسيير ،جامعة غرداية ، 2017 – 2018 ،ص:34.

4-2-1- نموذج SAC (SAC Model) :

أصدر مجمع المراجعين الداخليين الأمريكي نموذج (SAC) عام 1977 والمعدل عام 1994 بعنوان" الرقابة والنظم القابلة للمراجعة "، وقد عرف النموذج نظام الرقابة الداخلية بأنه: "مجموعة العمليات والوظائف والأنشطة والنظم الفرعية، والإجراءات، والموارد البشرية للمنشأة التي تقدم تأكيداً بأن أهداف المنشأة يتم تحقيقها والتأكيد على أن المخاطر يتم تخفيضها إلى المستوى المقبول.

وقد ركز هذا النموذج على وجهة نظر المنشأة المتعلقة بتكنولوجيا المعلومات، والمخاطر المرتبطة بتخطيط وتنفيذ واستخدام النظم الآلية كما أكد على مسئولية الإدارة تحديد وفهم وتقييم المخاطر المرتبطة دمج التكنولوجيا في المنشأة، ورقابة ومتابعة استخدام المنشأة للتكنولوجيا، ويتكون نموذج (SAC) مما يلي: ملخص تنفيذي، بيئة الرقابة والمراجعة ،استخدام تكنولوجيا المعلومات في المراجعة، إدارة موارد الحاسب، إدارة المعلومات وتطوير النظم نظم الأعمال ، العمليات الحسابية حسب هدف المستخدم النهائي ،ظهور الأساليب التكنولوجية.، الاتصالات الأمن ، خطط مواجهة الأحداث الطارئة.

وقد أشار نموذج (SAC) إلى أن معايير تقييم نظام الرقابة الداخلية تتضمن ما يلي: بيئة الرقابة الداخلية النظم اليدوية والآلية، إجراءات الرقابة.

4-2-2- نموذج NIST (NIST Model):

أصدر المعهد القومي للمعايير والتكنولوجيا الأمريكي (NIST) في عام 2001 إرشاداً بعنوان "التقييم الذاتي لنظم تكنولوجيا المعلومات"، ويتضمن هذا النموذج العناصر الجوهرية التي تدعم أهداف وأساليب تأمين ضوابط الرقابة على النظام وتنقسم إلى سبعة عشر عنصراً تم تبويبها في ثلاث مجموعات على النحو التالي:

- ضوابط الرقابة الإدارية تتضمن(5 عناصر).
- ضوابط الرقابة التشغيلية تتضمن(9 عناصر).
- ضوابط الرقابة الفنية تتضمن(3 عناصر).[1]

4-2-3- نموذج COBIT (COBIT Model) :

اسم المعيار هو اختصار ل أهداف الرقابة على المعلومات والتكنولوجيا المرتبطة بها" . يصدر عن مؤسسة مراجعة ورقابة أنظمة المعلومات ISACA منذ عام 1994، على أن يعدل ويطور كل سنة تحت إشراف 90 خبيرا دوليا في مجال تكنولوجيا المعلومات، ويتمثل الغرض الأساسي من هذا المعيار في وضع الأساليب والإجراءات المناسبة لبناء أنظمة المعلومات الإلكترونية بصفة عامة، إدارتها وكيفية استغلالها، الرقابة عليها ومراجعتها، بالإضافة إلى السبل الكفيلة بالتحكم في المخاطر المرتبطة بها. يتكون COBIT من أربعة مجالات أساسية متعلقة بأنظمة المعلومات الإلكترونية، وهي:[2]

- التخطيط والتنظيم
- حيازة والتنفيذ

[1] جيهان عبد المعز الجمال، **المراجعة في البيئة الالكترونية** ، الطبعة الأولى ، دار الكتاب الجامعي ،الإمارات العربية المتحدة ،2014، ص:150 – 153.

[2] زعابطة عبد اللطيف ، **مرجع سبق ذكره** ،ص : 143.

- التوصيل والتدعيم
- الرقابة والتقييم

4-3- معايير ISO :وهي منظمة التقييس دولية أنشئت عام 1947 تقوم بوضع وإعداد معايير خاصة بالتقييس وكذا معايير خاصة بأمن المعلومات وحماية نظم المعلومات، ومن أهم المعايير التي أصدرتها هذه المنظمة نذكر:

أ- **معيار ISO 27001**: تم إصدار هذا المعيار عام 2005 وهو خاص بوضع الأسس والقواعد الهامة، وإرسائها فيما يخص نظام إدارة وحماية وأمن المعلومات، وهذه الأسس تهتم بكيفية تصميم وتطبيق ورقابة وصيانة واجراء التطوير المستمر لأداء هذه الإدارة، وكذلك تقييم المخاطر الالكترونية، ويقدم هذا المعيار نموذجاً يسمى PDCA وهذا النموذج يطبق في كافة الوحدات خاصةً الحكومية، ويعد هذا النموذج اختصاراً لأربعة مراحل:

- الخطة Plan : تأسيس نظام لإدارة أمن المعلومات.
- التنفيذ Do: البدء في تنفيذ الخطط وتشغيلها
- التحقق Check: مراجعة النظام بعد تنفيذه.
- العمل Act : صيانة وتحسين النظام.

ب – معيار ISO 27002 : أصدر هذا المعيار عام 2005، وأهتم هذا المعيار بالتطبيق العملي للأسس والقواعد التي تم إعدادها بواسطة المعيار السابق أي أن هذا المعيار بمثابة الخطوط التي يجب المضي نحوها بعد مرحلة التطبيق، وذلك بهدف حماية الأصول التكنولوجية، وتوفير الأمان لها، وكذلك محاولة تجنب الوقوع في مخاطر التشغيل الالكتروني، وذلك من خلال اتباع السياسات الخاصة لكل من : الإدارة التنظيمية إدارة الموارد، إدارة أمن المعلومات، إدارة تطوير نظم المعلومات إدارة الأعمال المستمرة والتطوير، إدارة الشكاوي.

ج – معيار ISO 38500 : وهو المعيار الدولي لحوكمة تكنولوجيا المعلومات وهذا المعيار يقوم على الآتي: [1]

- تحديد المهام والمسؤوليات بوضوح ودقة بالنسبة لإدارة تكنولوجيا المعلومات.
- استراتيجية التخطيط بما يتوائم مع أهداف الشركة ومتطلباتها.
- اقتناء تكنولوجيا المعلومات لأسباب منطقية ومقبولة محددة مسبقاً.
- الثقة بأن الأداء التكنولوجي يسير على ما يرام.
- توافق تكنولوجيا المعلومات مع القوانين واللوائح الأخرى.

[1] ماهر فؤاد زهيري ، **مرجع سبق ذكره** ، ص: 53- 54.

- الأخذ في الاعتبار الموارد البشرية.

4-4 – قانون SOX :

تعد تداعيات الفضائح التجارية لشركات Worldcom ,Enron , Merck,Tyco ...، سبب في بزوغ قانون ساربنز أوكسلي Sarbanes-Oxley Act والذي صدر سنة 2002 من قبل الحكومة الفدرالية الأمريكية[1]، بهدف حماية المستثمرين عن طريق تحسين موثوقية المعلومات المالية وضمان الافصاح عنها وهذا بالنسبة لشركات المدرجة في الاسواق المالية في السوق الأمريكي ،ومن متطلبات هذا القانون :[2]

- وجوب إحتواء كل تقرير سنوي على تقرير خاص بأنظمة رقابة الداخلية .
- تلعب تكنولوجيا المعلومات IT دورا أساسيا في عملية إعداد تقرير.

4- 5- نموذج COSO ("COSO ERM Model"2017):

هو إطار صادر من قبل لجنة تريدواي "treadway Commission's" للرقابة الداخلية لتقييم وتفعيل نظم الرقابة الداخلية ،وهذا الإطار ملائم لإنجاز أهداف الوحدة الاقتصادية (التشغيلية، التقارير المالية، الإلتزام)[3] ،يبدأ من عملية الضوابط الداخلية ، كما أنه يساعد على تحسين وسائل السيطرة على الشركات من خلال تقييم فاعلية نظام الرقابة الداخلية، ويحتوي على خمسة مكونات رئيسة هي: بيئة الرقابة ،تقييم المخاطر، مراقبة ،الأنشطة المعلومات والاتصالات، متابعة .[4]

5- علاقة الأمن السيبراني مع أنظمة المعلومات المحاسبية :

يرتبط الأمن السيبراني إرتباطا وطيدا بأنظمة المعلومات ،فمهمة حماية الأنظمة والبيانات المخزنة والمعلومات الحساسة في الفضاء السيبراني من أي شكل من أشكال التهديدات والجرائم السيبرانية المختلفة " syber crimes " ، فأنظمة المعلومات المحاسبية تشكل جزء رئيسيا في الحياة اليومية للمؤسسات والهيئات الحكومية وهي مستخدمة جل الأعمال التجارية والمالية الحقيقية على الواقع أو الأعمال الإفتراضية كتجارة الإلكترونية "E-Commerce ، الإدارة الإلكترونية Electonic management ،والخدمات المصرفية "Banking services" ، وغيرها من أعمال ....،لذلك فإن أي اختراق أو تجاوز لأمن نظم المعلومات سوف يسبب بخسائر كبيرة مما يعطل الأنشطة ويفقد البيانات ويخرب البنية التحتية الحيوية الحساسة ،وحسب محمد حمد الكويتي

[1] ريتشارد دول وأخرون ،**نظم المعلومات المحاسبية** ، ترجمة :نضال محمود الرمحي ، الطبعة الأولى ،دار الفكر ، الأردن ،2014 ،ص:324.

[2] ماهر فؤاد زهيري ، **مرجع سابق**.

[3] سلماني عادل ،**مطبوعة في مقياس تدقيق ومراقبة أنظمة المعلومات** ،كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة غرداية ،2018-2019 ،ص: 87.

[4] ماهر فؤاد زهيري ، **مرجع سابق، ص:55**.

رئيس الأمن السيبراني لدولة الإمارات إلى أنه تشير بعض الدراسات المتخصصة إلى أن العالم يتكبد مليارات الدولارات سنويا جراء الهجمات السيبرانية بل أن بعض قدر هذه الخسائر ب 6 تريليونات دولار ,وإن تكلفة هذه الهجمات تصل إلى نحو 13 مليون دولار بالنسبة لشركة الواحدة سنويا[1]، أيضا يمكن ذكر بعض الأحداث التي شغلت الرأي العام في هذا المجال، مثل هجوم WannaCry عام 2017، والذي أصاب أكثر من 200 ألف جهاز حاسوب في 150 دولة حول العالم، وأدى إلى خسائر مالية كبيرة.[2]

ومن هذا يمكننا القول أنه توجد علاقة ذات صلة وتكامل بين الأمن السيبراني وأنظمة المعلومات المحاسبية ،بحيث يعتبر أمن نظم المعلومات عنصرا أساسيا لضمان سيرورة وسرية وسلامة أنظمة المعلومات المحاسبية وكذا حماية الشبكات وحواسيب والبرامج المتصلة بها .

6- الذكاء الاصطناعي وعلاقته مع أنظمة المعلومات المحاسبية :

يتزايد استخدام الذكاء الاصطناعي (AI) في الأمن السيبراني لتحسين سرعة ودقة اكتشاف التهديدات والاستجابة لها. بحيث أن كبرى الشركات والمؤسسات في العالم اتجهت للبحث في دمج وإدخال الذكاء الاصطناعي للإنشاء جدار أمني عالي الكفاءة والفعالية،. وفيما يلي سوف نقدم تعريفا لذكاء الأصطناعي والعلاقة التي تجمعه معا لأمن السيبراني :

يعرف الذكاء الاصطناعي "Artificial Intelligence" على أنه : علم يبحث في مفهوم الذكاء البشري وخصائصه وتحديد جوانبه ومن ثم محاكاة سلوكياته ، كما يشمل مجالات متنوعة حيث أن الجانب المشترك بين مجالات الذكاء الاصطناعي هو القدرة على اختراع الآلات حاسوبية تحاكي خصائص الذكاء البشري.[3]

ويعرف أيضا بإنه: عملية حاسوبية تستند إلى الإبداع والاستيعاب لكافة الأمور والسلوكيات، وتهدف إلى معالجة المواقف والمشكلات وإيجاد حلول ذكية وفعالة باستخدام تقنيات الحوسبة والتعلم الألي.[4]

---

[1] **الخليج** ، **6تريليونات دولار خسائر الهجمات السيبرانية عالمياً | صحيفة الخليج(alkhaleej.ae)** ، 2023/03/27، 11:25.

[2] Chack Point , https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/wannacry-ransomware/ ,27/03/2023 , 12 :00.

* **WannaCry**: برنامج من البرامج الفدية الخبيثة Ransomware

[3] يبان فراس النعانعة وأخرون ، **الصعوبات التي تواجه مديري المكتبات الجامعة الأردنية نحو استخدام تطبيقات الذكاء الاصطناعي** ،مؤتمر بعنوان التقنيات الناشئة وتطبيقاتها في المكتبات ومؤسسات المعلومات ،الكويت ،9/7 مارس 2023 ،ص:685.

[4] روان بنت مفلح جهني ، **استخدام تقنية الذكاء الاصطناعي روبوت المحادثة chatbot لتقديم الخدمات المعلومات في المكتبات الجامعية في المملكة العربية السعودية** ، مؤتمر بعنوان التقنيات الناشئة وتطبيقاتها في المكتبات ومؤسسات المعلومات ،الكويت ،9/7 مارس 2023 ،ص:39.

وبسبب ثورة الحاصلة في مجال الذكاء الاصطناعي الحالية والمستقبلية سوف يؤدي هذا إلى تغير في العديد من الأعمال والوظائف وهذا نتيجة أتمتة العديد من المهام ، وعلى سبيل الذكر نذكر بعض تطبيقات الرائجة حاليا في مجال AI :

- ChatGPT, copilot, Midjourney من شركة Opan AI.
- Bard من شركة google.
- Bing AI من شركة Microsoft.
- برامج أخرى : برنامج الكتابة Notion AI, برنامج لينسا Lensa AI, برنامج الرسم Blockadelabs,برنامج فليكي Fliki AI .

ويمكن لخوارزميات الذكاء الاصطناعي تحليل كميات كبيرة من البيانات في الوقت الفعلي ، وتحديد الأنماط وإجراء تنبؤات بناءً على تلك البيانات. وهذا بسبب ثورة في طريقة تصميم أنظمة المعلومات المحاسبية المؤتمتة (AIS) والمتوافقة مع الذكاء الاصطناعي (AI)، أيضا يمكن اكتشاف التهديدات وتحليل حركة مرور الشبكة وكشف الاحتيال.

أيضا ومن خلال الذكاء السيبراني "Syber intelligence" يمكن حصول على معلومات لتتبع وتحليل ومقاومة التهديدات السيبرانية أو الرقمية وترتيب أولويات الخطر وتقييمها وذلك نتيجة لوفرة المعلومات والقدرة على جمعها ،أيضا يمكن التنبؤ بالأساليب والأدوات المستخدمة من مجرمي الأنترنت ،والتوقع الأوقات الفعلية للهجوم.[1]

[1] Alsmadi, Izzat. *The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics*. Springer, Switzerland , 2019,P :75/76.

* **أتمتة** : يقصد بها التحكم في الآلات والعمليات المستخدمة في الصناعات المختلفة بواسطة أنظمة مستقلة تعتمد على التقنيات التكنولوجيا الحديثة، مثل الروبوتات وبرامج الحاسوب ، وذلك لأداء المهام التي كانت تتم يدويًا في الماضي.

وعلى ضوء ما سبق يتضح لنا أن عملية دمج الذكاء الاصطناعي كنظام حماية استباقي للاستجابة الآلية قبل بدء الهجوم والتنبؤ به سوف يحمي المؤسسات والحكومات من كافة أشكال الخروقات والتهديدات السيبرانية وهذا بتغطيته لثغرات أنظمة المعلومات المحاسبة وتصحيحه للأخطاء واستنتاجه وتوقعاته لسلوكيات وأساليب وأدوت التي يستخدمها المخترقون. حيث أن هدف الأساسي لذكاء الاصطناعي هو تطوير أنظمة الحاسوبية والآلات التي يمكن أن تفكر وتتصرف مثل الذكاء البشري وتنافسه .

ومع ذلك ، فإن استخدام الذكاء الاصطناعي في الأمن السيبراني يثير أيضًا مخاوف بشأن إمكانية استخدام الذكاء الاصطناعي من قبل مجرمي الإنترنت لأتمتة الهجمات وتجنب الاكتشاف ،ومن المهم للمؤسسات تنفيذ الضمانات المناسبة والمراقبة المستمرة وتقييم أنظمة الأمان القائمة على الذكاء الاصطناعي للتأكد من أنها فعالة وآمنة.

المبحث الثاني: الدراسات السابقة

سنتطرق من خلال هذا المبحث إلى عرض أهم الدراسات السابقة و التي لها علاقة بموضوع البحث من خلال دراسة المتغيرات ذات العلاقة بالموضوع الحالي ،بحيث اختلفت وتباينت الدراسات في معالجة مواضيعها بغية التوصل إلى النتائج المرجوة ،ومنه فتعتبر هذه الدراسة كمحاولة إضافة أو تكملة إلى بعض الجوانب التي لم يتم توصل إليها من خلال الدراسات السابقة .

المطلب الأول : الدراسات باللغة العربية

يركز هذا المطلب على أهم الدراسات باللغة العربية والتي لها علاقة بإحدى متغيرات الدراسة ،وفي إطار معالجتنا لموضوع "**متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية**" ،وقع بين أيدينا بعض الدراسات السابقة والتي أشارت لأحد أو بعض مكونات هذا الموضوع والتي سوف نوردها تباعا كالاتي :

الفرع الأول: دراسة زعابطة عبد اللطيف (2022)

الجدول رقم (02): دراسة زعابطة عبد اللطيف

الدراسة / السنة	دراسة زعابطة عبد اللطيف (2022)
عنوان الدراسة	أثر مخاطر تكنولوجيا المعلومات على نظام المعلومات المحاسبي دراسة حالة "شركة اتصالات الجزائر – الأغواط– "
نوع والمكان	الدراسة عبارة عن أطروحة دكتوراه ،الجزائر.
إشكالية الدراسة	ماهي المخاطر التي تواجهها المؤسسات الاقتصادية عند استخدامها لتكنولوجيا المعلومات في نظام المعلومات المحاسبي وما الحلول الممكنة لمواجهة هذه المخاطر؟
أهداف الدراسة	هدفت الدراسة إلى معرفة أهم أنواع المخاطر التي تواجه عملية استخدام تكنولوجيا المعلومات ،ثم تم التطرق إلى مختلف الإجراءات والممارسات التي من شأنها الحد من ذلك الأثر سعيا نحو الاستخدام الأمثل لتكنولوجيا المعلومات في نظام المعلومات المحاسبي.
منهج الدراسة	تم اعتماد على أسلوب المسح المكتبي وذلك من ناحية الجانب النظري ، أما من حيث الجانب التطبيقي فتم الاعتماد على المنهج الوصفي التحليلي من خلال اسلوب دراسة الحالة اعتمادا على الملاحظة والمقابلة الشخصية.

نتائج الدراسة	خلصت الدراسة إلى أن شركة اتصالات الجزائر تولي اهتماما واضحا بخصوص الحد من مخاطر التكنولوجيا المعلومات ،وهذا عبر الوسائل البشرية والتقنية وكذا الضوابط الرقابية والأمنية المرتبطة بنظم المعلومات ،إلا أنه الا يزال هنالك بعض الثغرات التي ينبغي تداركها.

المصدر: من إعداد الطالبان بناءا على معطيات دراسة زعابطة عبد اللطيف

الفرع الثاني : دراسة جوهر بنت عبد الرحمن إبراهيم المنيع (2022)

الجدول رقم (03) : دراسة جوهر بنت عبد الرحمن إبراهيم المنيع

الدراسة / السنة	دراسة جوهر بنت عبد الرحمن إبراهيم المنيع (2022)
عنوان الدراسة	متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030
نوع والمكان	الدراسة عبارة عن مقال علمي ،السعودية
إشكالية الدراسة	ما متطلبات تحقيق الأمن السيبراني في الجامعات السعودية وفق لرؤية 2030؟
أهداف الدراسة	هدفت الدراسة إلى التعرف على واقع تحقيق الأمن السيبراني في الجامعات السعودية على ضوء رؤية 2030 ،وكذا معرفة أهم المعوقات التي تحول دون تحقيق ذلك.
منهج الدراسة	تم اغتماد على المنهج الوصفي التحليلي ، وقد تم استخدام أداة الاستبيان كأداة لجمع البيانات.
نتائج الدراسة	وتوصلت الدراسة إلى أن أفراد العينة موافقون بدرجة متوسطة على واقع تحقيق الأمن السيبراني في الجامعات السعودية على ضوء رؤية 2030 ، وأيضا توصلت الدراسة إلى أنها هناك بعض المعيقات التي تحول دون تحقيق الأمن السيبراني في الجامعات السعودية ومن أهم هذه المعيقات : ● تدني مستوى الخبرة لدى الموظفين ● ضعف في التعاون بين موظفي التقنيات في الجامعات السعودية لتحقيق الأمن السيبراني

المصدر: من إعداد الطالبان بناءا على معطيات دراسة جوهر بنت عبد الرحمن إبراهيم المنيع

الفرع الثالث : دراسة حنين جميل أبو حسين (2021)

الجدول رقم (04) : دراسة حنين جميل أبو حسين

الدراسة / السنة	دراسة حنين جميل أبو حسين (2021)
عنوان الدراسة	الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة).
نوع والمكان	دراسة عبارة رسالة ماجستير ،الأردن .
إشكالية الدراسة	تتمثل إشكالية الدراسة في معرفة إطار القانوني لخدمات الأمن السيبراني
أهداف الدراسة	هدفت الدراسة إلى التعرف على الإطار القانوني لخدمات الأمن السيبراني ،ومعرفة مفهوم الفضاء السيبراني وتأثيره على دول العالم.
منهج الدراسة	اعتمدت الدراسة على المنهج الوصفي.
نتائج الدراسة	وقد توصلت الدراسة إلى مجموعة من النتائج نذكر منها: ان الأمن السيبراني يقوم على حماية المؤسسات والموظفين والأفراد ،لهذا وجب على المؤسسات تنفيذ أدوات الأمن السيبراني وأساليب إدارة المخاطر وتحسين باستمرار وذلك مع تغير تقنيات الحالية وتحديثاتها المتواصلة ،ايضا توصلت الدراسة إلا أن المشرع الأردني لم يعالج في قانون الأمن السيبراني المسائل التقنية والفنية من حيث الطبيعة والأثر والتصنيف.

المصدر: من إعداد الطالبان بناءا على معطيات دراسة حنين جميل أبو حسين

المطلب الثاني : دراسات باللغة الأجنبية

يحتوي هذا المطلب على بعض الدراسات الأجنبية ذات صلة بالموضوع الذي نحن بصدد معالجته والموسوم ب **"متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية"**

،والتي سوف يتم عرضها في الجداول التالية:

الفرع الأول: دراسة " Morteza Safaei Pour and others "(2023)

الجدول رقم (05) : دراسة "Morteza Safaei Pour and others"

الدراسة / السنة	دراسة " Morteza Safaei Pour and others "(2023)
عنوان الدراسة	"A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security" "**مراجعة شاملة لتقنيات القياس الحديثة على الإنترنت للأمن السيبراني**"
نوع والمكان	الدراسة عبارة عن مقال علمي ، هولندا.
إشكالية الدراسة	تعالج الدراسة إشكالية كيفية قياس تقنيات والدفاعات المقابلة للاختراقات والهجمات الإلكترونية وكذا قياس المناهج الإنترنت المطورة للأمن السيبراني.
أهداف الدراسة	هدفت هذه الدراسة إلى معرفة أهم هجمات السيبرانية وذلك من حيث الكثافة والتنوع والتأثير ، وكذا تحقيق في تهديدات الأمن السيبراني الحالية وتقييم مدى كفاءة وفعالية الدفاعات المقابلة لها
منهج الدراسة	تم اعتماد على المنهج الوصفي التحليلي خلال هذه الدراسة.
نتائج الدراسة	توصل الباحثون من خلال هذه الدراسة إن عملية ترك انتقال البنية التحتية الحيوية للمجتمع أدى إلى تعرض للعديد من التهديدات الأمنية ،وذلك بالرغم من الجهود الكبيرة المبذولة من الأطراف ذات صلة بهذا الأمر (الحكومات ، المؤسسات ، الأكاديميين) والتي تهدف إلى تخفيف من هذه القضايا المنتشرة والمتعلقة بجرائم السيبرانية . وأوصى الباحثون إلى وجوب قياس نجاح هذه المبادرات والمتعلقة بتقليل المخاطر الأمنية وكذا الأساليب والدفاعات المنتشرة لضمان الأمن الإلكتروني .

المصدر : من إعداد الطالبان بناءا على معطيات دراسة Morteza Safaei Pour and others

الفرع الثاني : دراسة " Deepak Sharma and others "(2023)

جدول رقم (06) : دراسة " Deepak Sharma and others "

الدراسة / السنة	دراسة Deepak Sharma and others (2023)
عنوان الدراسة	"A bibliometric analysis of cyber security and cyber forensics research" " تحليل ببليومتري لأبحاث الأمن السيبراني والجرائم الإلكترونية "
نوع والمكان	الدراسة عبارة عن مقال علمي ، هولندا.
إشكالية الدراسة	تمثلت إشكالية هذه الدراسة في الاحصائيات الأوراق والبحوث المنشورة خلال الفترة الممتدة (2011-2021) والمتعلقة بالأمن السيبراني والجرائم الإلكترونية ،وكذا مصادر النشر والمؤسسات وأهم الكلمات الرئيسية المستخدمة وماهي أهم النتائج ذات الأهمية الكبرى التي نتجت عند تحليل هذه البحوث.
أهداف الدراسة	هدفت الدراسة إلى تحليل المنشورات السنوية والاتجاهات والأنماط في الأبحاث المتعلقة بالأمن السيبراني والجرائم الإلكترونية والمنشورة على " Wep Of Science " ما بين الفترة الزمنية (2011-2021) بما في ذلك إحصائيات المتعلقة بالنشر والباحثين والبلدان والكلمات الرئيسية ،أيضا سعت الدراسة إلى تحديد أهم النتائج التي نتجت على ضوء تحليل البحوث المنشورة لتوفير نظرة شاملة على الحالة الحالية والاتجاهات المستقبلية للبحث في مجال الأمن السيبراني.
منهج الدراسة	اعتمدت هذه الدراسة على المنهج الوصفي التحليلي.
نتائج الدراسة	خلصت الدراسة أنه على الرغم من أن معظم الأبحاث التي تم نشرها في مجال الأمن السيبراني والجرائم الإلكترونية خلال العقد الماضي تركزت على مجال العلوم الحاسوبية، إلا أنه يمكن توجيه المزيد من الجهود في المستقبل نحو استكشاف تقنيات التعلم العميق ونقل المعرفة لتحسين الكشف عن التهديدات والقضاء عليها بدقة أكبر. كما يحتاج مجال مراقبة حالة النظام ونمذجة البيانات السيبرانية إلى مزيد من الأبحاث. كما يمكن إجراء مزيد من الأبحاث في مجالات التطبيقية الأقل استكشافاً للأمن السيبراني والجرائم الإلكترونية ،أيضا يمكن للباحثين إجراء تحليلات ببليومترية شاملة لمجالات محددة في الأمن السيبراني مثل اكتشاف البرامج الضارة.

المصدر : من إعداد الطالبان بناءا على معطيات دراسة Deepak Sharma and others

الفرع الثالث : دراسة "Olfa Ismail"(2021)

جدول رقم (07): دراسة Olfa Ismail

الدراسة / السنة	دراسة Olfa Ismail (2021)
عنوان الدراسة	" Conception et mise en oeuvre d'une culture sécurité des systèmes d'information : le cas des PME " **"تصميم وتنفيذ ثقافة أمن نظم المعلومات: حالة المؤسسات الصغيرة والمتوسطة"**
نوع والمكان	الدراسة عبارة عن أطروحة دكتوراه ،فرنسا.
إشكالية الدراسة	عالجت هذه الدراسة إشكالية كيفية فهم وتصور ثقافة أمن نظم المعلومات من طرف مستخدمي المؤسسات الصغيرة والمتوسطة
أهداف الدراسة	هدفت هذه الدراسة إلى معرفة كيفية تصميم وفهم الثقافة الأمنية لمستخدمي أنظمة المعلومات في المؤسسات الصغيرة والمتوسطة ، وكذلك كيفية تحسين مدى فهم مستخدمين للإجراءات الأمنية وماهي العوامل المؤثرة فيها.
منهج الدراسة	خلال هذه الدراسة تم إعتماد على المنهج الوصفي ، باستخدام أداة المقابلة كأداة لجمع البيانات.
نتائج الدراسة	توصلت هذه الدراسة إلى مجموعة من النتائج نذكر منها : ● توصلت من خلال هذه الدراسة إلى أن الموظفين يعتبرون أنهم هم الحلقة الأضعف في نظام المعلومات ● اتضح لصاحبة البحث أن تحسين الثقافة أو الإجراءات الأمنية لا يقتصر فقط على رفع الوعي أو التدريب وإنما على مجموعة من العوامل الأخرى ● ومن خلال دراسة حالة ثمانية مؤسسات الصغيرة والمتوسطة البحث وذلك عن طريق إجراء 32 مقابلة ،تم التوصل إلى أن هناك مجموعة عوامل خارجية (السياق القانوني ،قطاع النشاط ....)وعوامل داخلية (إدارة مخاطر ،التدريب والوعي ،مديري مؤسسات الصغيرة والمتوسطة الحجم) تؤثر بشكل ايجابي على رفع ثقافة الأمنية لمستخدمي نظم المعلومات ،ونتيجة لهذا فإن الثقافة الأمنية الإيجابية مفيدة في خلق سلوك مرتبط بالأمن ● من العوامل الأخرى المؤثرة في الثقافة الأمنية هي: خبرة المستخدم .

المصدر : من إعداد الطالبان بناءا على معطيات دراسة Olfa Ismail

المطلب الثالث : مقارنة الدراسة الحالية مع الدراسة السابقة

يركز هذا المطلب على المقارنة بين الدراسة الحالية مع الدراسات السابقة من خلال ذكر أهم أوجه التشابه وأوجه الاختلاف بين دراستنا والدراسات السابقة والتي تم التطرق لها سلفا ،فمن خلال استعراض وبالرجوع إلى الدراسات السابقة فإننا نرى ما يميز دراستنا الحالية عن مثيلاتها من دراسات السابقة والمتمثلة في دراسة أهم متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية وكذا التوقيت الزمني الحالي وما يميزه من أحداث جارية متعلقة بتطورات في تكنولوجيا المعلوماتIT والثورة الذكاء اصطناعي IA،الشي الذي يميز الدراسة الحالية عن نظيرتها من دراسات السابقة من جهة ويكمل هذه الدراسات من جهة أخرى ،ومن خلال الجداول التالية سوف نستعرض أهم أوجه الاختلاف وأوجه التشابه لدراستنا الحالية مقارنة بدراسات السابقة :

الفرع الأول : الدراسات باللغة العربية

جدول رقم(08): مقارنة الدراسة الحالية مع الدراسة باللغة العربية

المقارنة	أوجه التشابه	أوجه الاختلاف
دراسة زعابطة عبد اللطيف	تحتوي هذه الدراسة على نفس متغير التابع والمتعلق بأنظمة المعلومات المحاسبية ،أيضا تم استخدام نفس المنهج المتبع خلال هذه الدراسة والمتمثل في المنهج الوصفي التحليلي ،كذلك نفس أداتي جمع البيانات وهما الملاحظة والمقابلة.	تختلف دراستنا مع هذه الدراسة من حيث حدود الدراسة والمؤسسة محل الدراسة والممثلة في درستنا مؤسسة نفطال فرع "غرداية" ،فدراسة زعابطة عبد اللطيف تم في أغواط سنة 2022 ،أما بالنسبة لدراستنا فقد تمت في غرداية سنة 2023. كذلك تختلف هذه الدراسة من حيث المتغير المستقل فالمتغير الخاص بهذه الدراسة متعلق "بالأمن السيبراني" أما بالنسبة لدراسة زعابطة عبداللطيف متعلق "بتكنولوجيا المعلومات". أيضا تختلف دراستنا من حيث بعض أهداف الدراسة فدراستنا تهتم بمعرفة أهم متطلبات

		تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية.
دراسة جوهر بنت عبدالرحمن إبراهيم المنيع	تتشابه هذه الدراسة مع إحدى متغيرات دراستنا الحالية والمتمثل في الأمن السيبراني ، أيضا تتشابه من حيث المنهج المتبع خلال دراستنا وهو المنهج الوصفي التحليلي.	أولا تختلف هذه الدراسة مع دراستنا في حدود الدراسة فقد تمت هذه الدراسة في السعودية سنة 2022 ،أما دراستنا في الجزائر – غرداية – سنة 2023. أيضا تختلف في العينة الدراسة بحيث تمثلت العينة الخاص بهذه الدراسة في الجامعات السعودية عكس دراستنا التي كانت متعلقة بمؤسسات الاقتصادية الجزائرية ،وكذلك أداة جمع البيانات حيث تم استخدام خلال هذه الدراسة أداة الاستبيان أما بالنسبة لدراستنا سوف نستخدم أداتي الملاحظة والمقابلة.
دراسة حنين جميل أبو حسين	تتشابه هذه الدراسة مع دراستنا من حيث المنهج الدراسة المتبع ،ومع إحدى متغيرات دراسة الحالية والمتمثل في الأمن السيبراني.	هذه الدراسة عبارة عن دراسة نظرية ،أما بالنسبة لدراستنا سوف تتكون من جانب النظري وجانب التطبيقي والمتمثل في دراسة الميدانية التي تم إجراءها ،أيضا تختلف هذه الدراسة من حيث أهداف الدراسة وكذلك في حدود الدراسة فقد تمت هذه الدراسة في الأردن سنة 2021.

المصدر: من إعداد الطالبان بناءا على معطيات دراسة باللغة العربية

الفرع الثاني : الدراسات باللغة الأجنبية

جدول رقم(09) :مقارنة الدراسة الحالية مع الدراسة باللغة الأجنبية

المقارنة	أوجه التشابه	أوجه الاختلاف
دراسة **Morteza Safaei Pour and others**	تطرقت الدراسة لنفس المتغير والمتمثل في الأمن السيبراني ، أيضا اعتمدت هذه الدراسة على نفس منهج دراستنا والمتمثل في المنهج الوصفي التحليلي.	اختلفت هذه الدراسة في أهداف الدراسة بحيث اهتمت هذه الدراسة في كيفية قياس تقنيات الحديثة والموجودة على الأنترنت للأمن السيبراني وذلك لكيفية الحد من التهديدات والمخاطر الأمنية ، أيضا اختلفت في حدود المكانية الدراسة.
دراسة **Deepak Sharma and others**	تطرقت أيضا هذه الدراسة للإحدى متغيرات الدراسة الخاص بنا والمتمثل في الأمن السيبراني ،أيضا اعتمدت على نفس المنهج البحث وهو المنهج الوصفي.	تختلف هذه الدراسة في هدف الدراسة فدراسة تهدف إلى تحليل الأوراق البحثية المنشورة والمتعلقة بموضوع الامن السيبراني وهذا يختلف عن دراستنا التي سوف تدرس الأمن السيبراني بالنسبة للأنظمة المعلومات المحاسبي ، وأيضا تختلف من حيث حدود المكانية لدراسة.
دراسة **Olfa Ismail**	عالجت هذه الدراسة نفس متغير الذي قمنا بدراسته والمتعلق بأمن نظم المعلومات ، أيضا تتشابه مع الدراسة الحالية من حيث منهج المتبع خلال الدراسة والمتمثل في المنهج الوصفي ، أيضا تتشابه مع بعض أهداف هذه الدراسة ،واستخدمت هذه الدراسة نفس أداة جمع البيانات والمتمثلة في أداة الملاحظة والمقابلة.	تختلف هذه الدراسة في حدود الدراسة بحيث تمت الدراسة في فرنسا سنة 2021 ،أما بالنسبة لدراستنا تمت في الجزائر – غرداية – سنة 2023 ، أيضا اختلفت الدراسة الحالية مع هذه الدراسة من حيث العينة الدراسة والتي تمت بالنسبة لهذه الدراسة على مستوى مؤسسات الصغيرة والمتوسطة أما دراستنا كانت على مستوى مؤسسات الاقتصادية الجزائرية.

المصدر: من إعداد الطالبان بناءا على معطيات دراسة باللغة الأجنبية

خلاصة الفصل:

وخلال دراستنا لهذا الفصل يمكننا القول بأن نظام المعلومات المحاسبي من أهم الأنظمة الفرعية الموجودة داخل الوحدة الاقتصادية حيث يختص بتوليد البيانات والمعلومات التي تعكس الواقع الاقتصادي، وتوفيرها لأصحاب المصالح قصد اتخاذ القرارات، وتعتبر أنظمة المعلومات وأمن السيبراني موضوعان حيويان في عالم المال والأعمال حيث تلعب الأنظمة الإلكترونية الحديثة دوراً مهماً في تسيير الأعمال واتخاذ القرارات الإدارية والتخطيطية والمالية ومع ذلك فإن الأنظمة الحديثة تواجه تحديات عديدة في مجال أمن السيبراني، من حيث تهديدات الاختراق السيبراني والاحتيال المالي وأمن المعلومات وسلامتها، لذلك يجب على الشركات والمؤسسات اتخاذ إجراءات أمنية وقائية لحماية أنظمتها المعلوماتية والمالية وتتضمن هذه الإجراءات تأمين البيانات والمعلومات والتحقق من صحة الهوية والوصول للبيانات وتقييم المخاطر المحتملة والتعامل معها بطريقة فعالة وسريعة. وعلاوة على ذلك يجب على الموظفين الالتزام بسياسات الأمن والاستخدام الآمن للأنظمة المعلوماتية ومتابعة مستجدات ثورة الذكاء اصطناعي بمحاولة دمجه وإدخاله كنظام دفاعي استباقي قبل حدوث الهجوم أو تنبأه بمخاطر محتملة وتصحيحه للأخطاء وتغطيته للثغرات.

وبشكل عام يمكن القول إن أنظمة المعلومات وأمن السيبراني هما جزء لا يتجزأ من الأعمال الحديثة ،وأن التحديات التي يتم مجابهتها تتطلب تحديث وتطوير لاستراتيجيات الأمن والحماية ،وذلك لتحقيق الأهداف والحفاظ على سلامة وأمان المعلومات والموارد المالية.

الفصل الثاني دراسة الميدانية في مؤسسة نفطال –غرداية–

تمهيد :

تحاول مؤسسات الاقتصادية الجزائرية ان تحافظ على معلوماتها من أي شكل من أشكال تسريب المعلومات ولا تسمح الا بما تعتقد انه لن يؤثر على قوتها ولن يزيد من قوة منافسيها وبالتالي فهي تحمي نفسها من خلال وجود كيفية معينة للتعامل مع البيانات من حيث امكانية الحصول عليها من مصادرها المختلفة و حفظها و نقلها و استرجاعها بهدف اجراء العمليات اللازمة ،تظهر الأهمية البارزة لنظم المعلومات بالنسبة لمؤسسات من حيث وجود نظام معلومات داخل المؤسسة يوفر مخرجات يتم على أساسها بناء و اتخاذ كافة القرارات التي تحدد المكانة الاستراتيجية الحالية والمستقبلية للكيانات.

ومن خلال هذا الفصل سوف نتطرق الى دراسة حالة لمؤسسة نفطال لولاية غرداية ،بهدف معرفة اذا كانت لأنظمة المعلومات دور هام في المجال العملي ،وكذلك التطرق الى أهم البرامج المستعملة في المؤسسة و العوائق التي تواجهها.

حيث يتناول هذا الفصل وصفاً لطريقة عمل برنامج SD COM التي تستعمله المؤسسة الوطنية نفطال ،وسوف نقوم بإجراء مقابلة مع القائمين على مؤسسة نفطال لمعرفة واقع أمن نظم المعلومات في مؤسسة محل الدراسة ،كما أيضا سوف نقدم نموذج مقترح لأمن نظم المعلومات ، لهذا تم تقسيم الفصل إلى مبحثين وفقا لما يلي :

المبحث الأول : تشخيص نظام SD COM في مؤسسة نفطال.

المبحث الثاني : تقييم نظام معلومات لمؤسسة نفطال

المبحث الأول: تشخيص نظام SD COM في مؤسسة نفطال

تحتل مؤسسة نفطال مكانة أساسية في الاقتصاد الوطني بحكم عملها في قطاع استراتيجي مهم في البلاد و هذا ما يتطلب على القائمين عليها ،جودة و فعالية في التسيير من خلال العمل الإداري المحكم الذي يضمن تحقيق ميزة تنافسية ممتازة ، و من هذا تحتاج المؤسسة الى أنظمة معلومات تتماشي مع المتطلبات المذكورة سلفا و من بين هذه الأنظمة نجد نظام SD COM و الأنظمة الفرعية التابعة له ،من خلال هذا المبحث سوف نقدم لمحة على مؤسسة نفطال ومن ثم التطرق الى النظام المطبق على مستوى المؤسسة " SD COM ".

المطلب الأول : لمحة على مؤسسة نفطال و نظام SD COM المطبق لديها

01- تعريف مؤسسة نفطال " فرع الزفت بغرداية":

تأست شركة سوناطراك وفقا لمرسوم 63-491 المؤرخ في 1963/12/31 بمهمة نقل وتسويق المحروقات وتم بعد ذلك توسيع نطاق صلاحياتها و ذلك في مجال البحث وتحويل المحروقات بمقتضى المرسوم رقم 66-296 المؤرخ في 1966/09/22 و في سنة 1980.

و يرجع أصل كلمة نفطال إلى:

- NAFT:مصطلح عالمي يعني " النفط ".
- AL: حرفان يشيران إلى كلمة " الجزائر ".

تعتبر شركة نفطال هي الشركة الوحيدة التي تضمن تسويق و توزيع الموارد البترولية و مشتقات البترول عبر كافة التراب الوطني فمنذ تاريخ إنشائها إلى يومنا الحالي طرأت عليها تغييرات نذكر الأهم منها:

سنة 1998 نشأت خلية الأمن الصناعي ومديرية مراقبة ومراجعة الحسابات وتنظيمها ومديرية الوقود و زيوت التشحيم و المطاط الزفت (LPC).

02- مديرية الزفت لولاية غرداية

تعتبر مديرية الزفت أحد الفروع التي تشكل الفرع التجاري للمؤسسة ومن أكثرها مردودية ومساهمة في الارباح التي تحققها المؤسسة ،وتختص بتسويق مختلف أنواع الزفت في السوق الوطنية و الموجهة أساسا لقطاع الأشغال العمومية

يحتل فرع الزفت لمؤسسة نفطال الريادة في السوق الوطنية في مادة الزفت حيث يسيطر على 56 % من إجمالي المبيعات في سوق مفتوح يشهد منافسة شرسة من مؤسسات وطنية و أجنبية وهذا ما يعطي له الأهمية الكبيرة في استراتيجية المجمع ككل.

إضافة لذلك فإن اسعار الزفت حرة و غير محددة مثل مختلف أنواع الوقود المحددة من طرف الدولة في إطار سياسة الدعم التي تنتهجها .

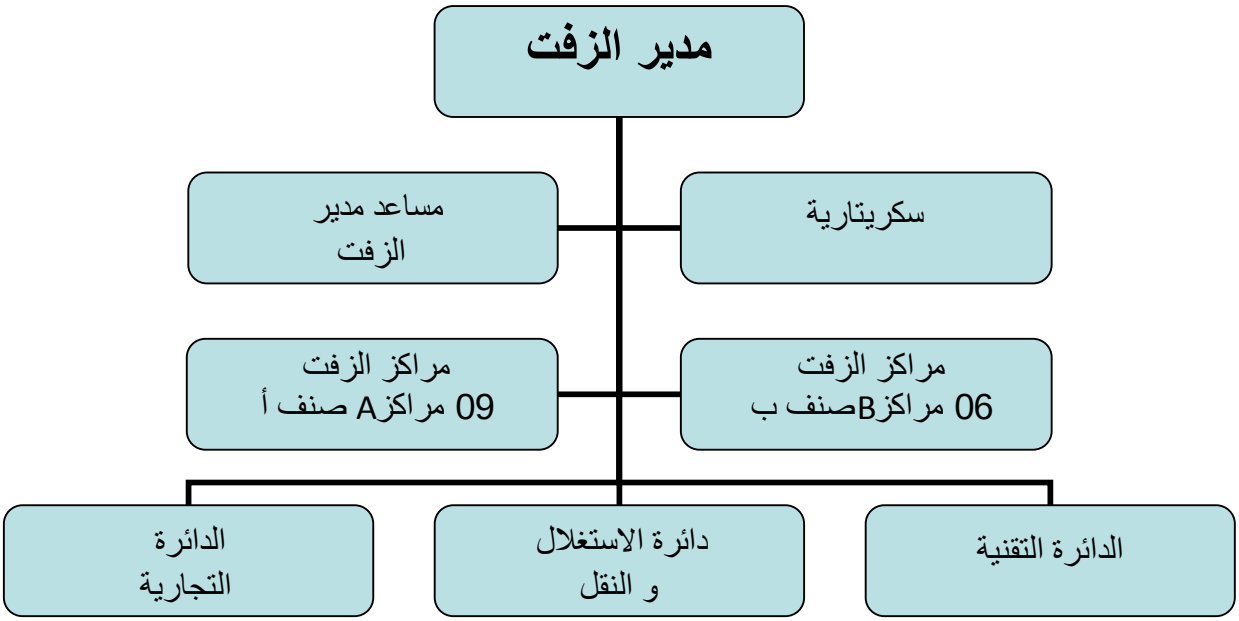
يسوق فرع الزفت لنفطال العديد من أنواع الزفت المستعملة في السوق الوطنية نذكر منها على سبيل المثال :

- الزفت الخام BITUME PUR
- الزفت المخفف 600/400 CUT-BUK400/600
- الزفت المخفف 0/1 CUT-BUK0/1
- المستحلب الحامضي ÉMULSION

تقوم المؤسسة بالتموين مباشرة من المؤسسة الأم سوناطراك بهذه المادة وذلك من مصفاتي أرزيو بوهران وسكيكدة ،ونظرا لعدم كفاية هذه الكمية لتغطية احتياجات المؤسسة تقوم باستيراد مادة الزفت الخام من الأسواق الدولية و بالخصوص من إسبانيا و إيطاليا حيث تمثل الكمية المستوردة ثلاثة أرباع الكمية المنتجة محليا وهذا راجع لمحدودية قدرات التكرير لدى المؤسسة الأم سوناطراك وكذلك نوعية البترول الجزائري الممتازة القليل من الشوائب والتي لا تنتج كميات كبيرة من الزفت إذ أن الزفت يمثل الشوائب التي يحتويها البترول الخام .

تنقسم هذه المراكز إلى صنفين أ و ب بحسب القدرة التخزينية ورقم الأعمال وعدد العمال حيث يحتوي كل مركز على مصلحة تجارية ومصلحة الاستغلال ومصلحة المحاسبة والإدارة :

الشكل رقم (05) : الهيكل التنظيمي لمديرية الزفت



المصدر : من إعداد الطالبين بناء على بيانات من مديرية الزفت لولاية (غرداية) 2023.

- **مراكز الزفت صنف أ:** الجزائر –غرداية – وهران–مستغانم– بجاية– العلمة– سكيكدة–عنابة– تقرت

- **مراكز الزفت صنف ب:** أم البواقي – عين الدفلة– عين الصفراء– تمنراست – عين صالح –باتنة

يبلغ عدد العمال في مديرية الزفت 1080 عامل

03- تعريف نظام " SD COM "

تستعمل مؤسسة نفطال برنامجا خاصا بإدارة أعمال المؤسسة و مواردها تم تطويره من طرف إطاراتها و مهندسي الإعلام الآلي ،يسمى هذا البرنامج بـ:SD COM ،حيث يتيح هذا البرنامج القيام بعمليات "المبيعات، الفوترة الزبائن ،المخزونات .....الخ ، حيث يتم تجميع المعطيات بشكل يومي ومن ثم بشكل شهري الى المديرية المركزية .

مميزات نظام المعلومات الالكتروني SD COM : من خلال تطبيق نظام SD COM كنظام للمعلومات استفادة مؤسسة نفطال فرع غرداية من عدة مميزات منذ تطبيق هذا النظام ، لهذا سوف نلخصها في النقاط التالية:[1]

- سهولة ربطه مع برامج المحاسبية والغير محاسبية الأخرى.
- يسهل عمل المحاسبين وهذا من خلال مجموعة من ميزات التي يقدمها البرنامج.
- متصل بالشبكة الرئيسية وقابل للتحديث.
- تسهيل أداء المهام اليومية من خلال سهولة البحث والتخزين في النظام.
- ضمان حماية المعلومات.
- يقدم معلومات دقيقة وموثوقة وفي الوقت المناسب.

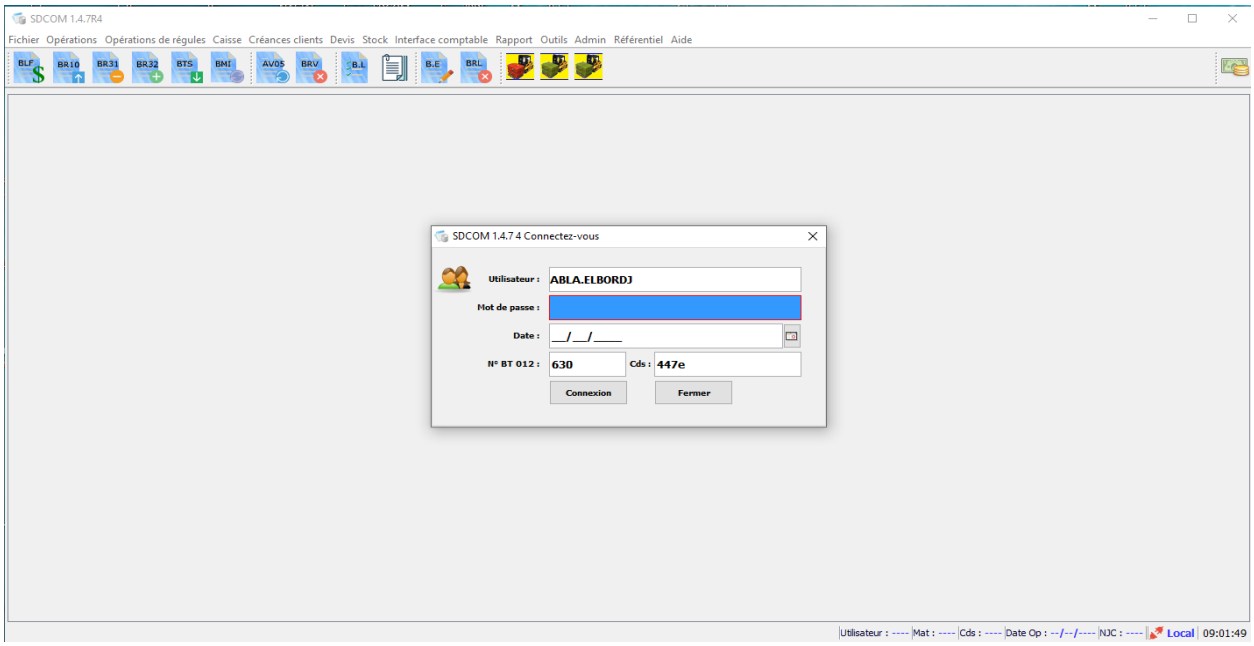
تم العمل ببرنامج SD COM بداية من سنة 2018 بالتوازي مع برنامج NAFT COM بحيث من المميزات التي تم اكتسابها نظير تطبيق هذا البرنامج ،التي أصبح من خلالها المسير يستطيع النظر الى كل العمليات و الأعمال التي تقوم بها المؤسسة خلال مدة زمنية قصيرة ،ايضا يعتبر هذا البرنامج من اختراع محلي أي وطني و هذا من أجل ضمان سرية المعلومات الخاصة بالمؤسسة .

ومن خلال هذا البرنامج يمكن للمديرية المركزية تتبع جميع العمليات التي تحدث على مستوى المديريات الفرعية عبر كامل القطر الوطني.

تتضح واجهة البرنامج من خلال الشكل التالي :

[1] مقابلة مع مدير مؤسسة نفطال ، 2023/05/18، 10:00

الشكل رقم 06-01: يوضح واجهة برنامج SD COM



المصدر:من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

المطلب الثاني : سيرورة عمل نظام SD COM

01- المدخلات نظام SD COM

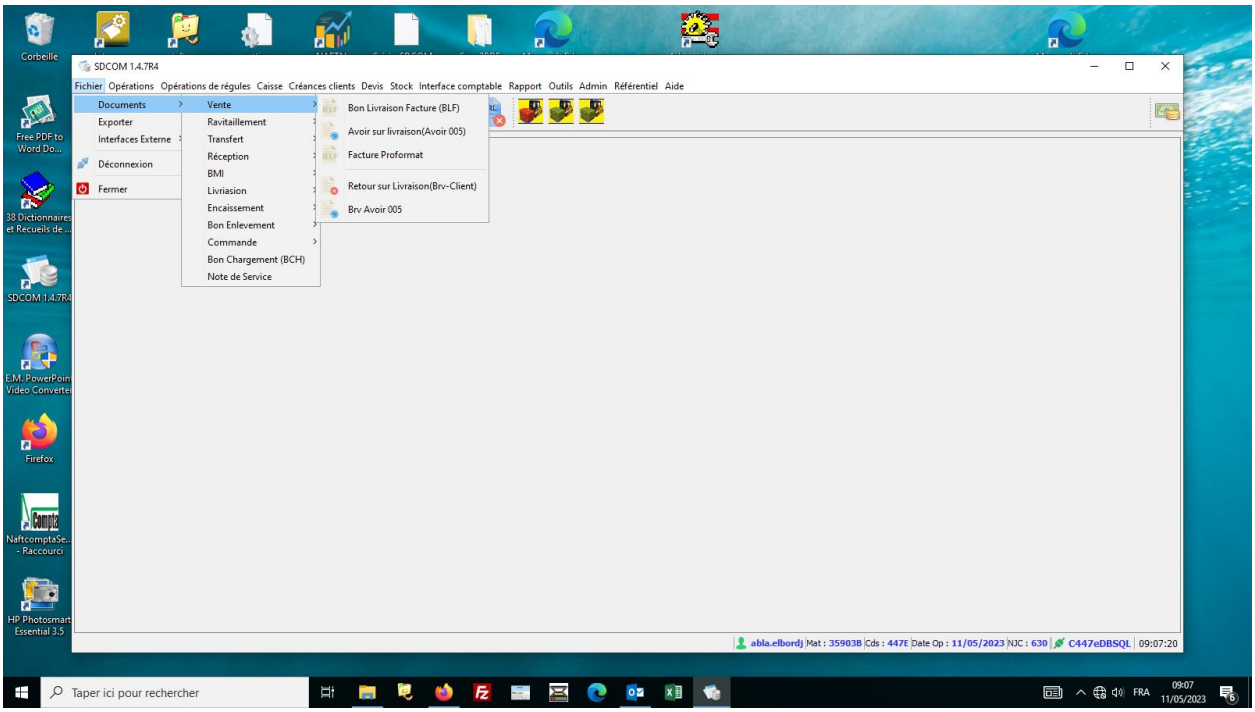
- نظام SD COM هو نظام خاص بمؤسسة نفطال حيث تم إنشاؤه من طرف أخصائيين في مجال الإعلام الألي تابعين للشركة الأم، بهدف تسهيل عمل المؤسسة وهو نظام محمي ،يتم الدخول اليه من خلال حسابات شخصية لبعض المسيرين في المؤسسة ،حيث الصورة أدناه تبين طريقة الولوج لهذا البرنامج :

- بعد فتح البرنامج تظهر لنا نافذة تحتوي على مختلف المعالجات التي يقوم بها هذا الأخير حيث نجد من بينها ما يلي :

- المبيعات
- دخول و خروج السلع .
- التحويلات إلى مؤسسات أخرى.
- الاستقبال.
- تحويلات المنتوجات الخام إلى منتوجات تامة الصنع بهدف تسويقها.

- الشيكات أو التسديدات الخاصة بالزبائن

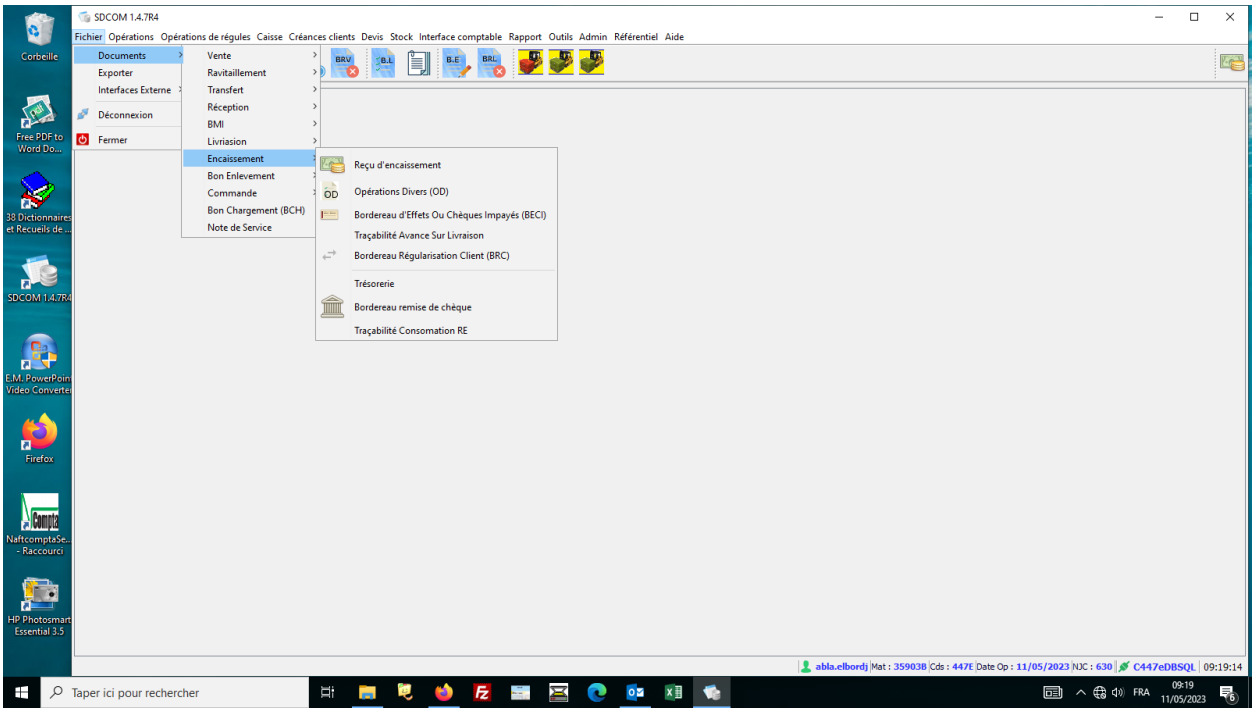
الشكل رقم 06-02: يبين جميع المعالجات



المصدر:من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

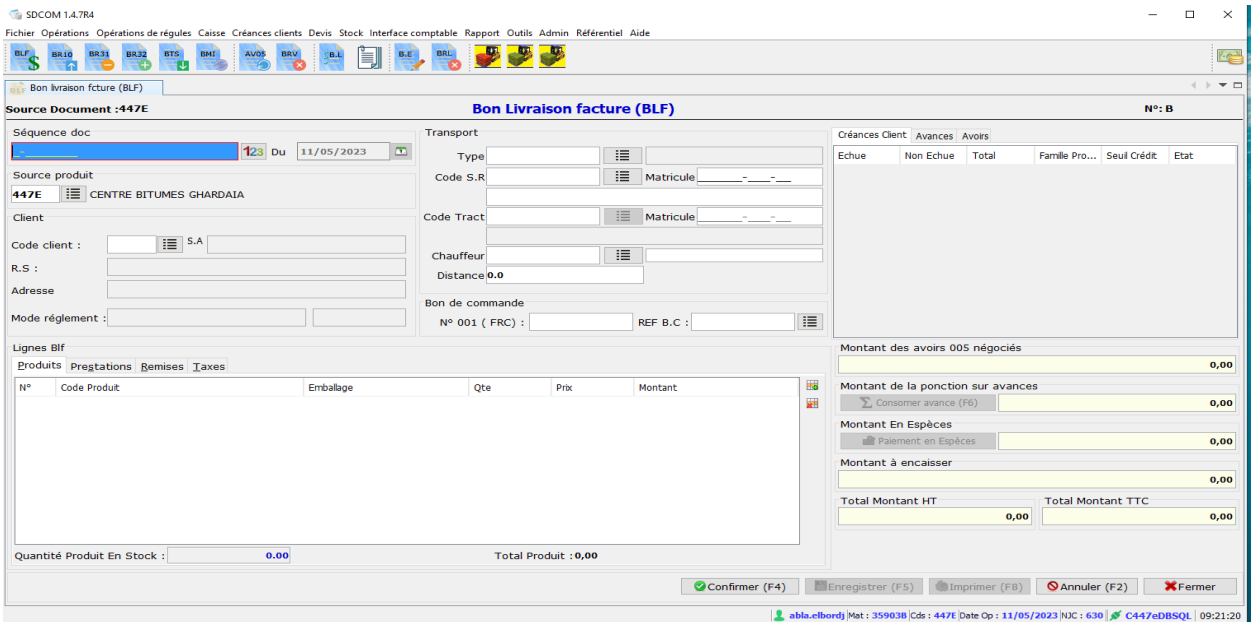
- يوضح الشكل أدناه طريقة استخدام الشركة للبرنامج من خلال الشيكات أو التسديدات الخاصة بالزبائن الذين تكون لديهم معاملات مع هذه الأخيرة ، الأشكال من رقم (**06 – 03** إلى**06 - 06**) توضح هذا:

الكل رقم 06–03: يبين الشيكات أو التسديدات الخاصة بالزبائن



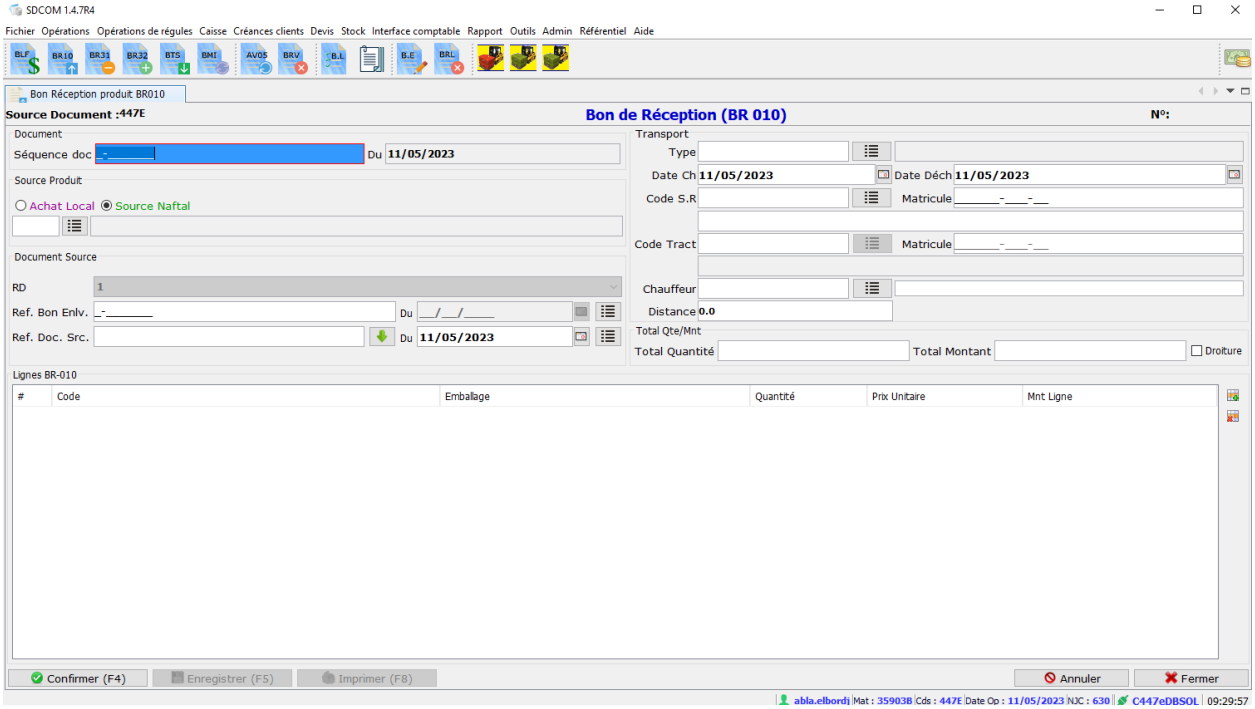
المصدر: من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

الشكل رقم 06– 04 : يوضح فاتورة المبيعات



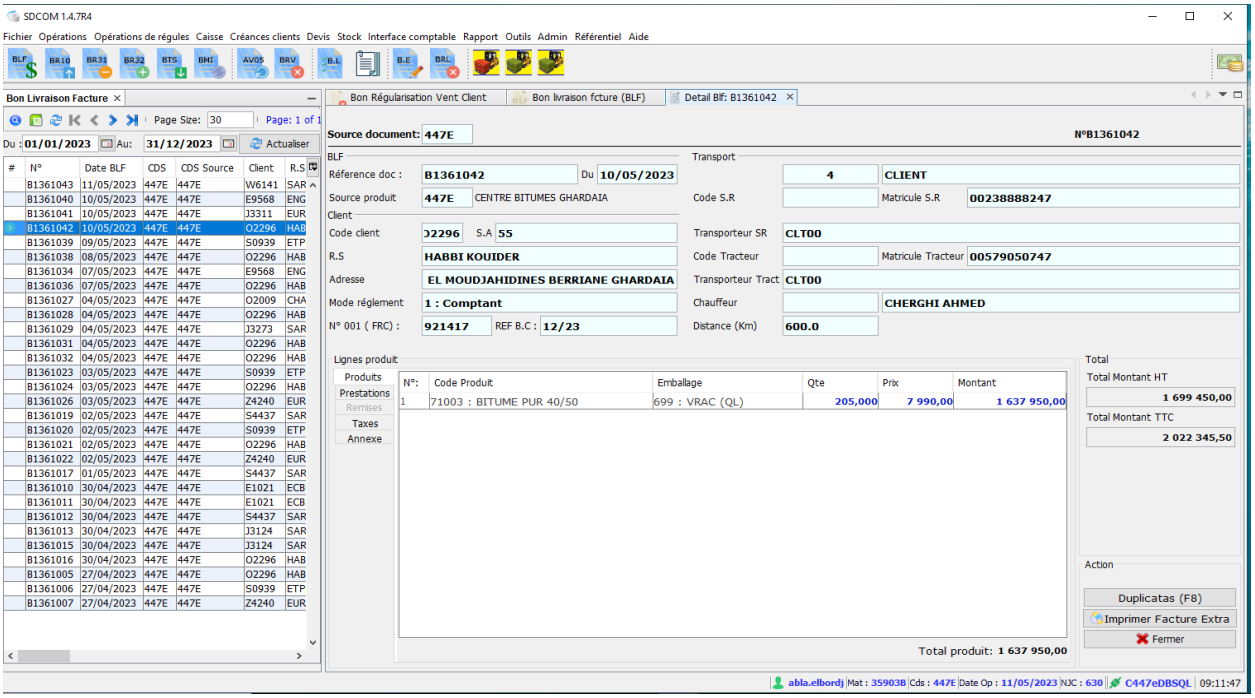
المصدر: من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

الشكل رقم 06-05: يوضح وصل استقبال الشحنات



المصدر:من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

الشكل رقم 06- 06: يوضح معالجة فاتورة بعد إدخال كافة المعلومات

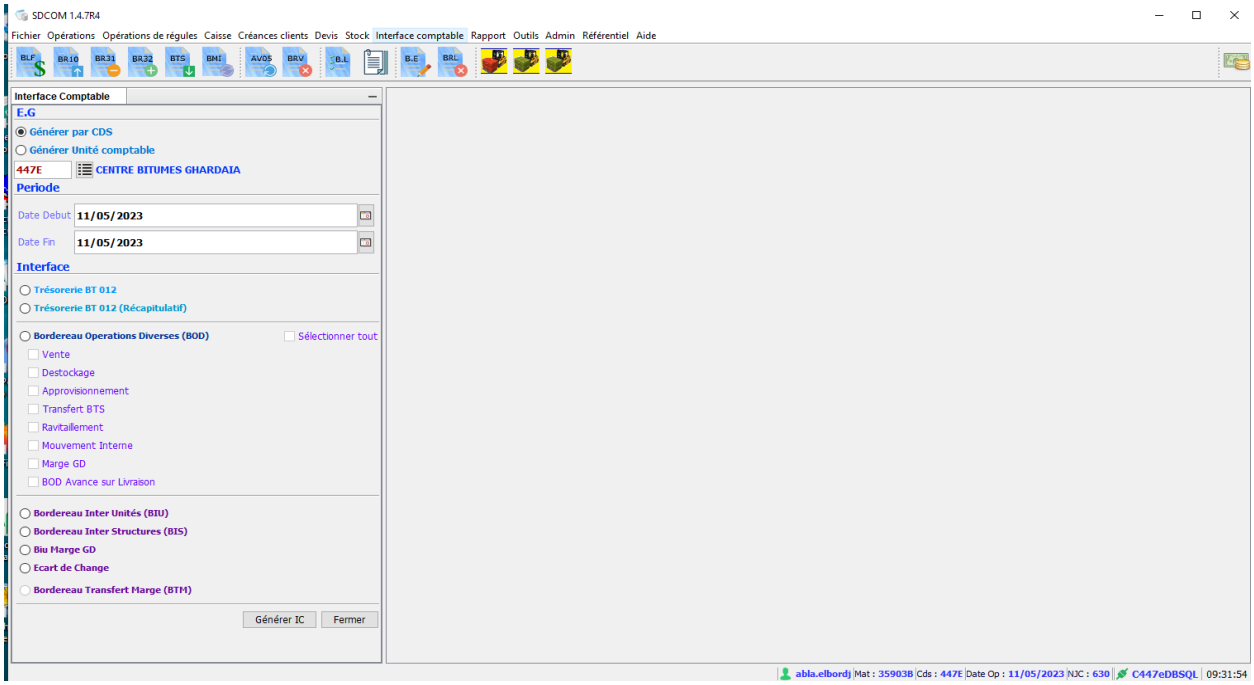


المصدر:من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

02- الية المعالجة لنظام SD COM

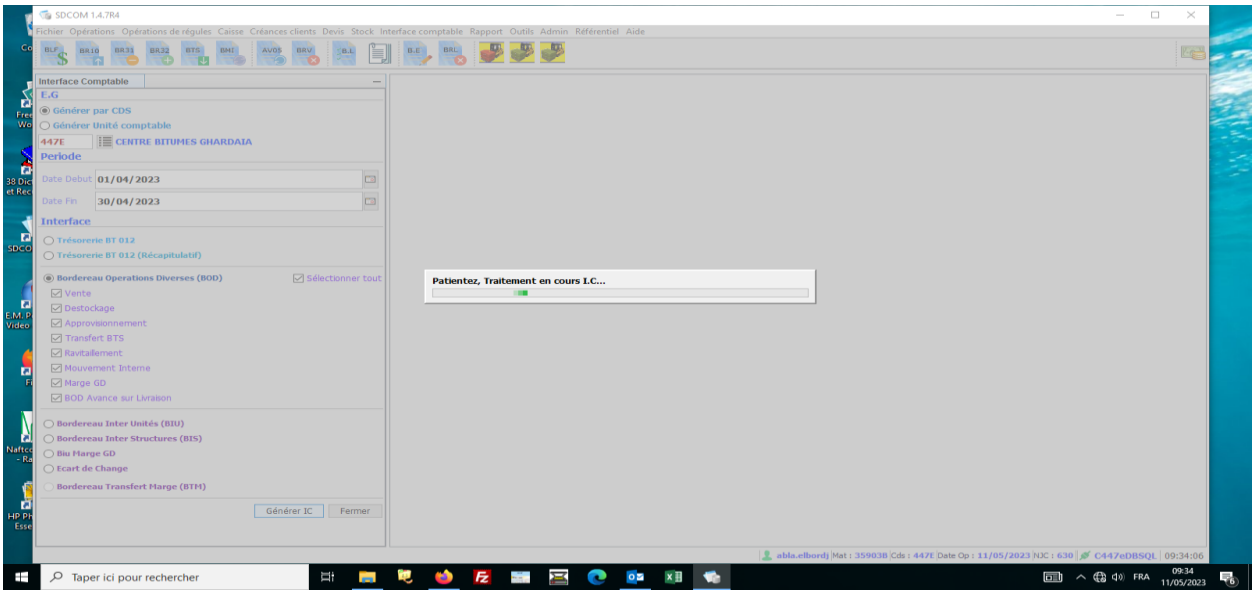
- في هذه المرحلة تتم عملية المعالجة من قبل النظام حيث أن الشكلين أدنا يبين لنا هذه العملية :

الشكل رقم 06 – 07: يبين كيفية معالجة البيانات



المصدر:من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

الشكل رقم 06 – 08 : يوضح عملية إرسال البيانات إلى مصلحة المحاسبة

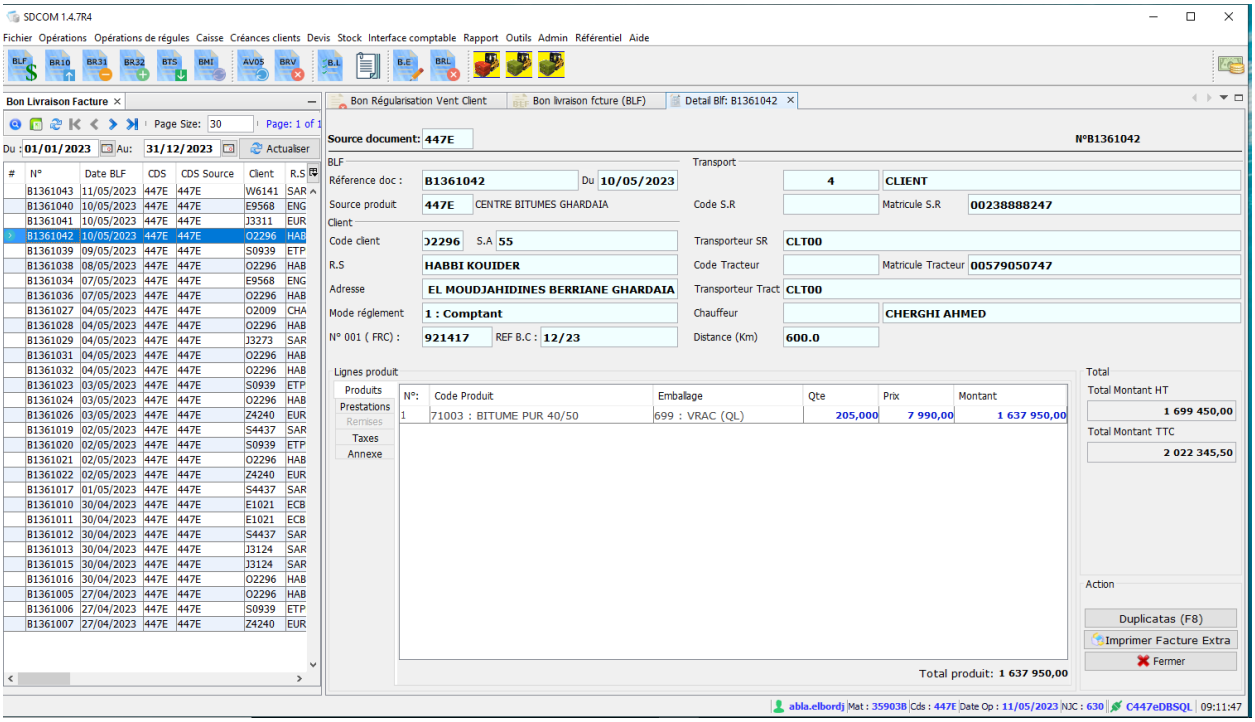


المصدر:من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

- بعد القيام بعملة المعالجة من قبل النظام يتم ارسال الملف المتحصل عليه الى مصلحة المحاسبة و المالية بالمؤسسة NAFT COMPTA .

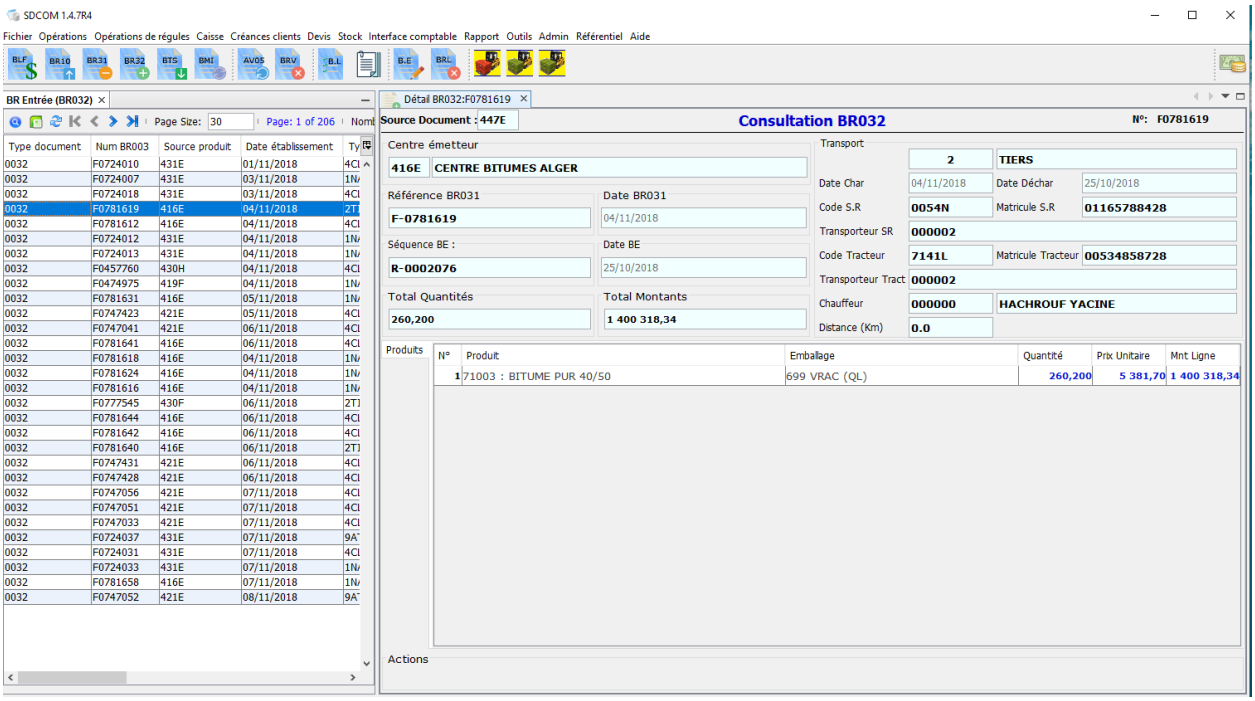
الأشكال الثلاثة أدناه تبين المراحل التي تمر بها عملية المعالجة

الشكل رقم 06 – 09: يوضح كيفية معالجة الفاتورة من قبل المصلحة



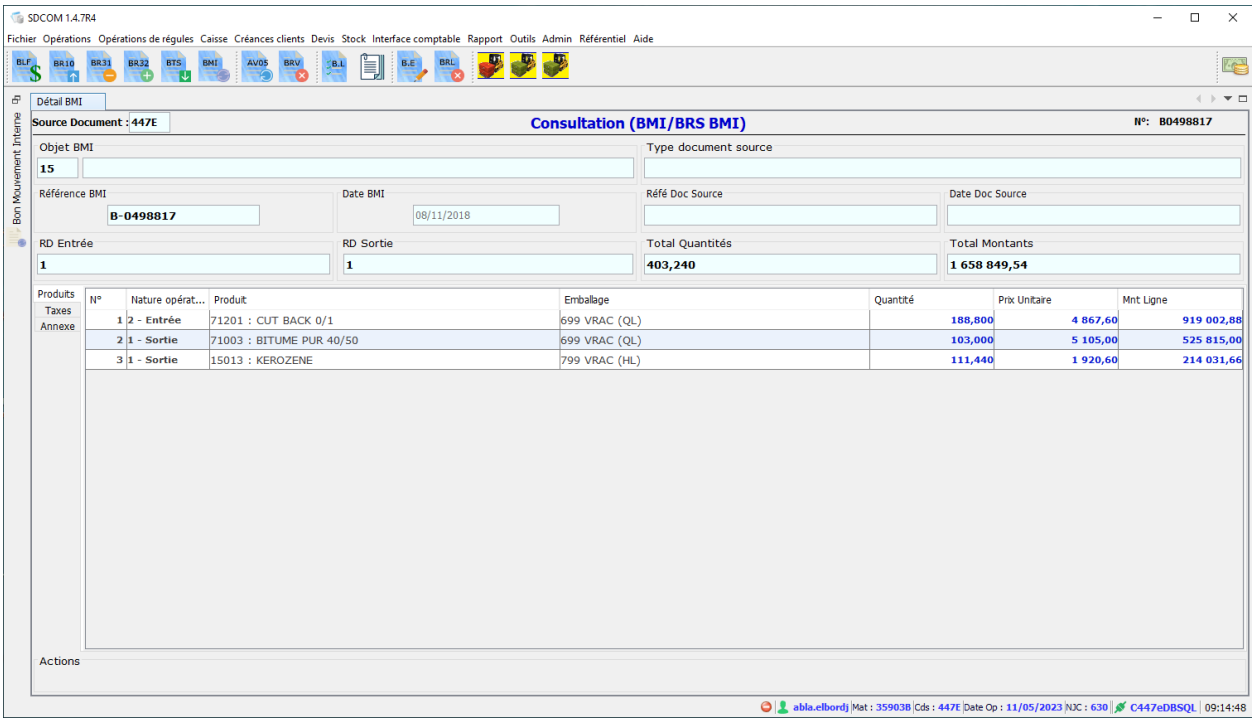
المصدر: من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

الشكل رقم 06 – 10: يبين عملية خروج السلع BR 32



المصدر: من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

الشكل رقم 06 – 11: التحويلات الخاصة بالمواد الخام دخولها و تحويلها الى مواد قابلة للاستعمال

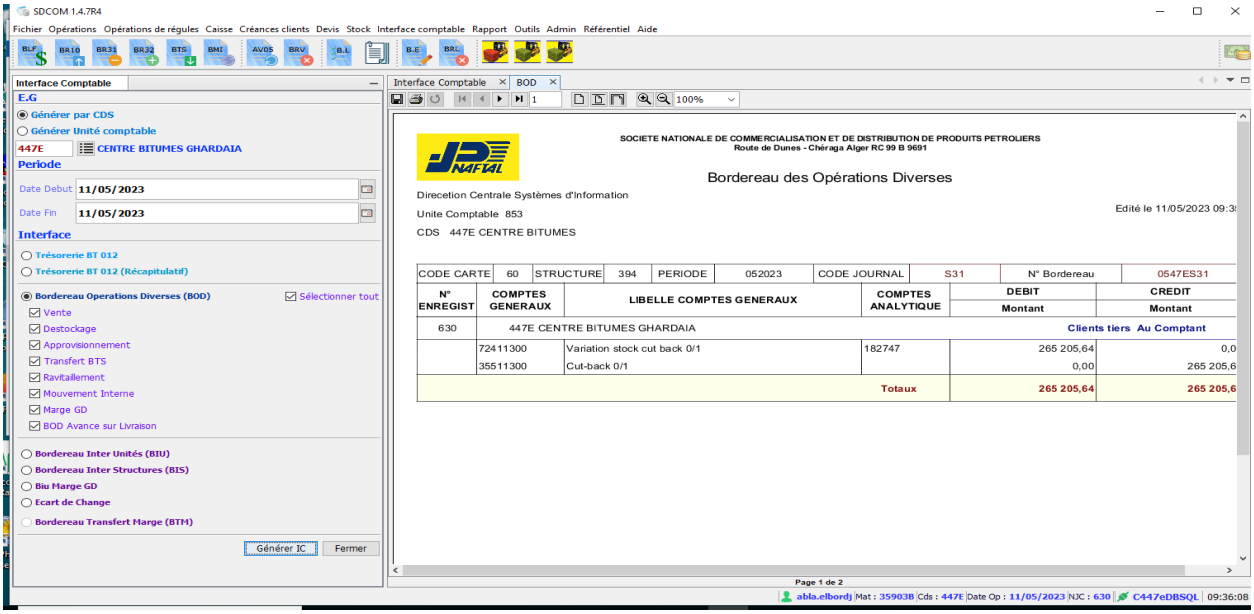


المصدر: من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

03- مخرجات نظام SD COM

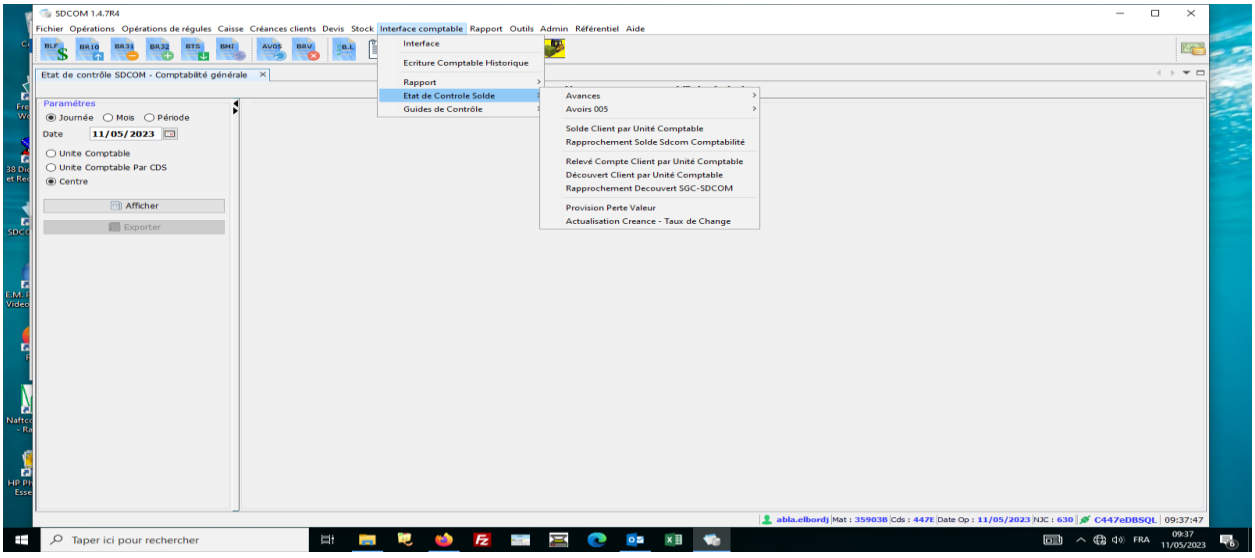
- بعد عملية المعالجة الألية التي يقوم بها النظام تظهر لنا النتائج و التي هي مبينة في الشكلين 06 – 12،06 – 13 أدناه:

الشكل رقم 06 – 12: يبين مخرجات برنامج SD COM



المصدر: من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

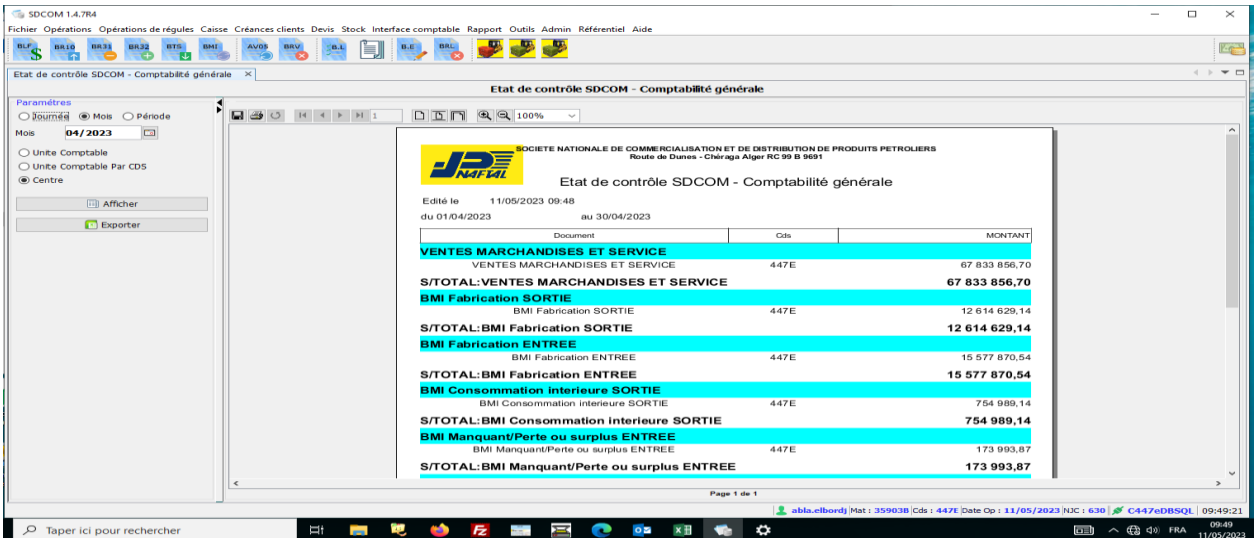
الشكل رقم 06 – 13: يوضح العلاقة بين SD COM ومحاسبة العامة



المصدر: من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

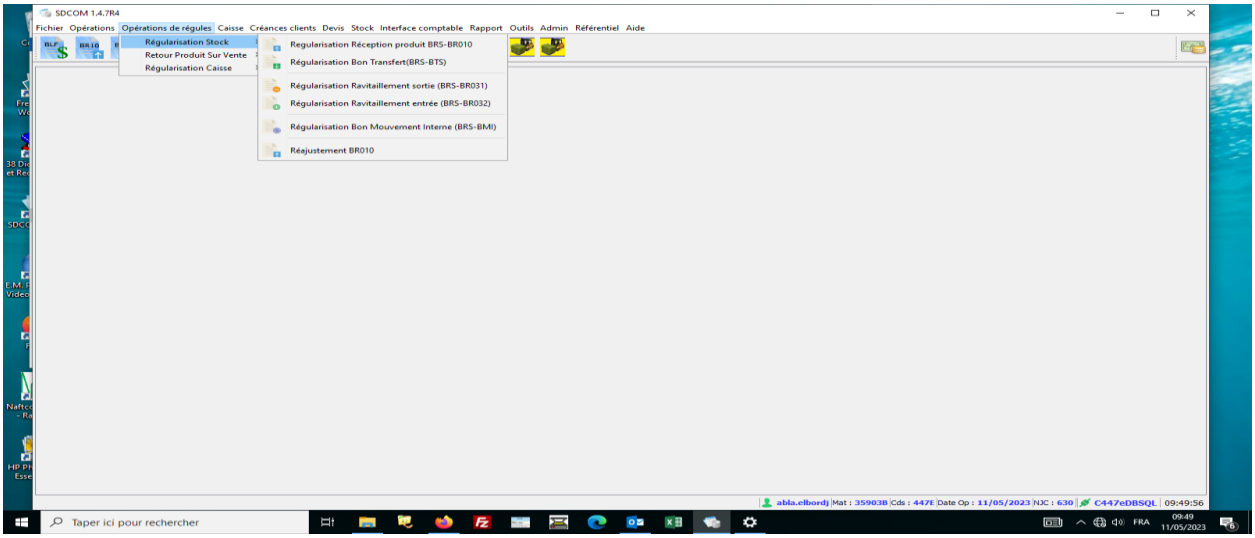
- تمثل الصورتين أدناه (الشكل **06 – 14**، **06 – 15**) المخرجات التي تم التوصل اليها داخل المؤسسة ،يحث الدول أدناه بين لنا جميع العمليات التي ظهرت فيها أخطاء ،ليقوم من خلالها المراجع العمل على تصحيح واعادة النظر في العمليات بهدف الوصول الى نتائج صحيحة ، و هي العلاقة بين نظام SD COM المحاسبة العامة .

الشكل رقم 06 – 14: يوضح الأخطاء التي تم اكتشافها من طرف برنامج SD COM



المصدر:من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

الشكل رقم 06 – 15: يبين عملية تصحيح الأخطاء التي تم استخرجها



المصدر:من إعداد الطالبين بالاعتماد على نظام المعلومات الالكتروني SD COM بمؤسسة نفطال فرع غرداية

المبحث الثاني : تقييم نظام المعلومات المطبق في مؤسسة نفطال

سعينا من خلال هذا المبحث إلى فهم الواقع الحالي لأنظمة المعلومات في المؤسسة محل الدراسة، ومدى فعالية الإجراءات المتخذة لحماية هذه الأنظمة من التجاوزات التي تشكل تهديدًا لها. حيث تعد أنظمة المعلومات الحديثة أساسا لعمل المؤسسات ونجاحها ،حيث يتيح لها إدارة بياناتها ومعلوماتها بشكل فعال وتحسين العمليات واتخاذ القرارات الاستراتيجية.

و تشهد أنظمة المعلومات اليوم تعقيدًا متزايدًا نظرًا للتقدم التكنولوجي السريع والتحديات الأمنية المتزايدة. بحيث تواجه العديد من المنظمات تهديدات أمنية متنوعة مثل الاختراقات الإلكترونية، والبرامج الضارة، وسرقة البيانات والهجمات السيبرانية ،وتعتبر هذه التهديدات خطيرة ويمكن أن تتسبب في تأثيرات سلبية كبيرة على المؤسسة، بما في ذلك فقدان البيانات الحساسة، وتعطيل الخدمات.

فمن خلال هذا المبحث سنقوم بدراسة واقع أنظمة المعلومات في المؤسسة نفطال" فرع غرداية" ودراسة درجة حماية المتوفرة لديها من التجاوزات والتهديدات الأمنية ،لهذا سنقوم بإجراء مقابلات مع المسؤولين والموظفين ذات الصلة بأمور أنظمة المعلومات وحمايتها.

المطلب الأول : عرض وتحليل بيانات المقابلة

أولا : إعداد المقابلة :

للإلمام بمتغيرات الدراسة، وبغية تحقيق الأهداف المرجوة وصولا إلى النتائج المتوقعة ،تم إعداد وصياغة مضمون المقابلة التي تضمنت 20 أسئلة، من خلال إسقاط أهم جوانب الدراسة النظرية لموضوع البحث على الجانب التطبيقي، في محاولة منا لاستطلاع آراء القائمين على أنظمة الحماية بمؤسسة نفطال فرع غرداية بخصوص متطلبات تطبيق الامن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية وماهي أهم الإجراءات المطبقة لحماية أنظمة الموجودة على المستوى المؤسسة.

ومن أجل تسهيل عملية التحليل والمناقشة قمنا في صلب هذه الدراسة بإستعراض أسئلة المقابلة وكذلك الأجوبة المتحصل عليها .

ثانياً:أعضاء المقابلة :

ولمعرفة متطلبات تطبيق الامن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية ارتأينا أن نقوم بإجراء مقابلة مع القائمين على أنظمة الحماية بمؤسسة نفطال فرع غرداية ، كما يوضحه الشكل الموالي:

الجدول رقم (10): أعضاء المقابلة

الترميز	الصفة	الخبرة
E1	مدير ومحاسب مؤسسة نفطال – فرع غرداية –	أكثر من 15سنوات
E2	مهندسة اعلام الي مؤسسة نفطال – فرع غرداية –	–

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

ثالثا: مضمون المقابلة:

تضمنت المقابلة 20 سؤال موجهة الى مدراء ومهندس الاعلام الالي مؤسسة نفطال – فرع غرداية –، كانت المقابلة بمثابة فضاء لإبداء آرائهم في مجال أنظمة المعلومات وإجراءات الحماية ،فيما يلي الاسئلة التي تضمنتها المقابلة:

1– السؤال الأول: ماهو واقع الرقمنة في مؤسسة نفطال ؟

الهدف من هذا السؤال هو الحصول على معلومات حول واقع الرقمنة في مؤسسة نفطال. يتعلق ذلك بفهم مدى تبني المؤسسة للتقنيات الرقمية واستخدامها في عملياتها وأنظمتها المختلفة ،من خلال الإجابة على هذا السؤال يمكن توضيح ما إذا كانت مؤسسة نفطال تعتمد على التقنيات الرقمية في عملياتها المختلفة ،مثل التسويق والمبيعات وإدارة المخزون والمحاسبة وغيرها.

2– السؤال الثاني: هل فكرت مؤسسة نفطال في مخطط للرقمنة ؟

استهدفنا من خلال هذا السؤال معرفة ما إذا كانت المؤسسة نفطال قد اتخذت خطوات لتحويل عملياتها وعملياتها التقنية إلى نظام رقمي. يهدف الرقمنة إلى استخدام التكنولوجيا الحديثة والتحول الرقمي لتحسين الكفاءة والإنتاجية وتقديم خدمات أفضل للعملاء.

3– السؤال الثالث: ماهي البرمجيات المستخدمة في شركة نفطال؟

طرحنا هذا السؤال لمعرفة البرمجيات المستخدمة في شركة نفطال ،ومن المهم معرفة هذه المعلومة لأن البرمجيات تلعب دورًا حاسمًا في عمليات الرقمنة وتحسين الكفاءة في المؤسسة.

4- السؤال الرابع: البرامج المستخدم في مجال المحاسبي و المالي ؟ هل انتاج محلي أو أجنبي ؟

الهدف من هذا السؤال هو تحديد البرامج التي تستخدم في مجال المحاسبة والمالية، وتحديد ما إذا كانت تلك البرامج محلية الإنتاج أم أجنبية والتعرف على سياسة واختيارات شركة نفطال ،ومن خلال هذا يمكننا الاستنتاج أن برامج محاسبية ومالية محلية الإنتاج هل هي متاحة ؟و هل تلبي احتياجات ؟

5- السؤال الخامس: ماهي مدخلات و المخرجات هذا النظام ؟

عندما نتحدث عن مدخلات النظام، نقصد بها المعلومات والبيانات أما بالنسبة للمخرجات، فهي النتائج أو البيانات التي يتم إنتاجها من النظام بعد معالجة المدخلات وهدف من هذا سؤال هو معرفة مدخلات ومخرجات النظام الذي تستخدمه شركة نفطال. هذه المعلومة تساعدنا في فهم كيفية تنظيم وتدفق المعلومات والبيانات في المؤسسة.

6- السؤال السادس: هل يرقى هذا البرنامج الى نظام معلومات محاسبي متكامل؟

الهدف من هذا السؤال هو تحديد ما إذا كان البرنامج الذي تستخدمه شركة نفطال يرقى إلى مستوى نظام معلومات محاسبي متكامل. ويهدف هذا السؤال أيضا إلى فهم مدى تكامل البرامج في تلبية احتياجات المعلومات المحاسبية في المؤسسة.

7- السؤال السابع: في رأيكم ماهي المرتكزات التي يقوم عليها هذا النظام اذا كان موجودا ؟ في حالة بـ:

لا – ماهي جهود المؤسسة في بناء نظام المعلومات؟

كنا نهدف من هذا السؤال إلى تحديد أهم المرتكزات التي يقوم عليها النظام إذا كان موجودًا، وإذا لم يكن موجودًا، فأردنا أن نأخذ فكرة عن جهود المؤسسة المبذولة في بناء نظام المعلومات.

8- السؤال الثامن: هل يتم تخزين البيانات و معلومات المؤسسة في الأدوات السحابية أو الخوادم الالكترونية ؟اذا كان بالخوادم فهل ملكية الخوادم للمؤسسة أو لهيئة اخرى؟

لقد كان الهدف من هذا السؤال هو تحديد ما إذا كانت بيانات ومعلومات مؤسسة نفطال يتم تخزينها في الأدوات السحابية أو الخوادم الإلكترونية، وفي حالة ما إذا كان في الخوادم، فأردنا من خلال السؤال إلى تحديد ملكية تلك الخوادم.

9- السؤال التاسع: هل هناك جدار ناري لحماية مختلف الأنظمة و البيانات الموجود في المؤسسة؟

الهدف من هذا السؤال هو تحديد ما إذا كان هناك جدار ناري (Firewall) لحماية مختلف الأنظمة والبيانات في مؤسسة نفطال. أيا المغزى من هذا السؤال التأكد من وجود تدابير أمنية فعالة للحماية والتصدي للتهديدات الخارجية التي قد تستهدف الأنظمة والبيانات.

10- السؤال العاشر: في العمليات المالية العادية هل يتم استخدام تطبيقات اخرى؟

أردنا من وراء طرح هذا السؤال إلى تحديد ما إذا كانت هناك تطبيقات أخرى تستخدم في العمليات المالية العادية. أيضا هدفنا من هذا السؤال إلى استكشاف استخدام تطبيقات إضافية في إدارة العمليات المالية وتعزيز كفاءتها ودقتها.

11- السؤال الحادية عشر في المعاملات الخارجية كعمليات الجباية و التحصيلات *هل يتم استخدام تطبيقات مثل: مساهمتك ، جبايتك.....الخ.

الهدف من هذا السؤال هو التحقق من ما إذا كانت المؤسسة تستخدم تطبيقات خاصة لإدارة المعاملات الخارجية مثل عمليات الجباية والتحصيلات كمساهمتك و جبايتك.....،ويهدف السؤال إلى استكشاف استخدام تطبيقات محددة لتسهيل وتحسين هذه العمليات وتنظيمها.

12- السؤال الثانية عشر: في تسيير محطات الوقود *هل يتم استخدام اجهزة TPE في عمليات التعبئة؟

يهدف هذا السؤال هو التحقق من ما إذا كانت محطات الوقود تستخدم أجهزة TPE (نقاط البيع الإلكترونية) في عمليات التعبئة. يهدف السؤال إلى استكشاف استخدام هذه الأجهزة الإلكترونية لتسهيل عمليات التعبئة وتحسين تجربة العملاء.

13- السؤال الثالث عشر : هل هذه الاجهزة مرتبطة بنظام الكتروني مركزي ؟

الهدف من السؤال هو التأكد من ما إذا كانت أجهزة TPE في محطات الوقود متصلة بنظام إلكتروني مركزي وذلك لتحسين الاتصال وتدفق المعلومات بين الأجهزة والنظام الرئيسي وتعزيز إدارة المحطة بشكل عام.

14- السؤال الرابع عشر : بطاقات الدفع الالكترونية المستخدمة عندكم *هل هي معتمدة من طرف شركة "SATIM"

الهدف من السؤال هو التأكد من مدى اعتماد المؤسسة على بطاقات الدفع الإلكترونية التي تم توفيرها من قبل شركة "SATIM"، وهذا يساعد في تقييم مستوى الأمان والجودة في العمليات المالية التي يتم تنفيذها باستخدام هذه البطاقات.

15- السؤال الخامس عشر : هل تقوم المؤسسة بتكوين مستمر للمهندسين و التقنيين في مجال البرمجيات و تحديثاتها ؟

يهدف هذا السؤال إلى التحقق من ما إذا كانت المؤسسة تقوم بتكوين مستمر للمهندسين والتقنيين في مجال البرمجيات و تحديثاتها ،يساعد هذا السؤال إلى استكشاف مدى التزام المؤسسة بتطوير وتحسين مهارات فريقها الفني وتأهيلهم بشكل دوري لمواكبة التطورات في مجال البرمجيات واستخدام التقنيات الحديثة.

16- السؤال السابع عشر : في ظل اتجاه الدولة نحو استخدام الذكاء الاصطناعي و الروبوتيك في الانتاج و التخزين ،هل هناك اتجاه المؤسسة نحو اعادة تجديد اصولها الثابتة ؟

ارتأينا من خلال طرح هذا سؤال لتحقق مما إذا كانت المؤسسة تأخذ في الاعتبار هذه التكنولوجيات المتقدمة وتعمل على تحديث وتجديد أصولها لتكون قادرة على الاستفادة من فوائد الذكاء الاصطناعي والروبوتيك في عملياتها ،إذا كانت المؤسسة تتبنى هذا الاتجاه، فإنها تعبر عن رغبتها في الابتكار والتطور لتكون على مستوى المنافسة في سوق العمل الحالي وتحقيق تحسينات مستدامة في أدائها ونموها.

17-السؤال السابع عشر هل تم اختراق الأنظمة التي تستخدمها مؤسسة نفطال من قبل ؟

لقد هدفنا من خلال هذا سؤال هو التأكد من توافر إجراءات الأمان اللازمة في مؤسسة نفطال ومعرفة ما إذا كانت قد تعرضت لاختراق سابقًا ،هذا يمكن أن يساعد في تقييم فعالية إجراءات الأمان الحالية وتحديد أي نقاط ضعف قد تحتاج إلى تعزيزها. كما يساعد في إدراك أهمية تطوير استراتيجيات أمان متقدمة لحماية الأنظمة والبيانات في المستقبل.

18- السؤال الثامن عشر اذا كانت نعم ماهي الاجراءات التي تم اتخاذها؟ و هل أثرت على سيرورة عمل المؤسسة؟

كان هدف من هذا السؤال هو التحقق من الإجراءات التي اتخذتها مؤسسة نفطال في حالة تعرض أنظمتها للاختراق ،يهدف السؤال إلى معرفة كيفية استجابة المؤسسة للهجمات السيبرانية وإدارة الأزمات الأمنية.

19- السؤال التاسع عشر هل هذا الاختراق كان نتيجة أخطاء داخلية او قصور في انظمة المعلومات ؟

الهدف من هذا السؤال هو التحقق من ما إذا كانت الاختراقات السابقة التي تعرضت لها مؤسسة نفطال ناجمة عن أخطاء داخلية أو قصور في أنظمة المعلومات. يهدف السؤال إلى استكشاف الأسباب المحتملة للاختراقات وتحديد المسؤولية عن وقوعها.

20- السؤال العشرين : في حالة الاخطاء الداخلية *هل يتم الاستعانة بجهات أمنية سيبرانية ؟

استهدفنا من هذا السؤال معرفة ما إذا كانت مؤسسة نفطال تستعين بجهات أمنية سيبرانية خبراء في مجال حماية أنظمة في حالة وجود أخطاء داخلية ،يهدف السؤال إلى استكشاف مدى تعاون المؤسسة مع الخبراء والاستشاريين في مجال الأمن السيبراني لتقديم الدعم والتوجيه في معالجة الثغرات والاختراقات .

21 – السؤال الواحد والعشرين : في رأيكم ماهي معوقات تطبيق التكنولوجيا لدى المؤسسة ؟

طرحنا هذا السؤال لتعرف على أهم المعوقات التي تواجه مؤسسة نفطال في تطبيق التكنولوجيا ،الغرض من السؤال هو تحديد العوامل التي قد تعيق اعتماد التكنولوجيا واستفادة المؤسسة الكاملة من فوائدها.

22- السؤال الثاني و العشرين في رأيكم ماهي معوقات التي تواجه المؤسسة في هذا المجال ؟

لقد كان هدف من هذا السؤال هو التعرف على معيقات التي تواجه مؤسسة نفطال بشكل عام في مجال حماية أنظمة المعلومات.

23- السؤال الثالث والعشرين : جهود المؤسسة و استراتيجيتها في مجال الأمن السيبراني لقطاع مهم في مجال الطاقة ؟

نهدف من هذا السؤال إلى الحصول على معلومات حول جهود المؤسسة نفطال واستراتيجيتها في مجال الأمن السيبراني لقطاع الطاقة ،الغرض من هذا التعرف على الإجراءات والتدابير التي تتخذها المؤسسة لحماية أنظمتها ومعلوماتها من التهديدات السيبرانية والاحتياطات التي تتبعها للتعامل مع الهجمات والاختراقات المحتملة.

المطلب الثاني : تحليل الأجوبة واستخلاص نتائج المقابلة

فيما يلي سنقوم بعرض أجوبة القائمين على أنظمة الحماية بمؤسسة نفطال فرع غرداية ،وكذا قمنا بترميز المستجوبين على النحو التالي: (E1، E2)

أولا : عرض إجابات المقابلة تحليلها وتقيمها

1- عرض وتحليل أجوبة السؤال الأول: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (11)**: أجوبة وتحليل على السؤال الأول

السؤال الأول	
ما هو واقع الرقمنة في مؤسسة نفطال ؟	
الترميز	**الجواب**
E1	تولي مؤسسة أهمية كبيرة جدا للرقمنة العمليات والأعمال وهذا من خلال التوجه نحو إلغاء استعمال الورق والاعتماد على الحلول الرقمية والمعلوماتية
E2	تُعطي مؤسسة نفطال أهمية كبيرة للرقمنة والتحول الرقمي في أعمالها. فهي تدرك أن العصر الحالي يتطلب التكيف مع التكنولوجيا الحديثة واستغلال فوائدها في تحسين الكفاءة والإنتاجية. وتهدف المؤسسة إلى إلغاء استخدام الورق تدريجيًا والاعتماد على الحلول الرقمية والمعلوماتية.
تحليل الإجابتين:	
توضّح هذه المقابلة أن مؤسسة نفطال قد استثمرت بشكل كبير في وسائل الرقمنة لمواكبة تحولات الرقمية الحالية في بيئة المال والأعمال، وبتالي تعتبر الرقمنة والتحول الرقمي أمرًا هاما لمؤسسة نفطال، وهذا ما يتطلبه العصر الرقمي الحالي ، لهذا وجب تكييف الأعمال والعمليات مع التكنولوجيا الحديثة واستغلال الفوائد الكبيرة التي تقدمها بهدف تحسين الكفاءة والإنتاجية، وتحقيق التكامل والتنسيق بين العمليات المختلفة، وتوفير بيئة عمل مرنة ومستدامة. ويعكس واقع الرقمنة في مؤسسة نفطال الحاجة الملحة لاستخدام التكنولوجيا وتحديث مختلف الأنظمة لتحسين تجربة الزبائن وتوفير الخدمات بطريقة تتسم بالسهولة والسرعة وأمان. علاوة على ذلك تشير هذه المقابلة إلى أن الرقمنة والحلول التابعة لها أصبحت جزءًا أساسيًا من استراتيجية مؤسسة محل الدراسة في تلبية احتياجات زبائنها وترحيبًا بمتطلبات التحول الرقمي في القطاع الطاقة بشكل عام.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

2- عرض وتحليل أجوبة السؤال الثاني: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي:

الجدول رقم (12): أجوبة وتحليل على السؤال الثاني

السؤال الثاني	
هل فكرت مؤسسة نفطال في مخطط للرقمنة ؟	
الترميز	**الجواب**
E1	نعم هذا الفكر الذي تريد مؤسسة نفطال توجه إليه حيث أن هناك إرادة لدى الإدارة العليا للمؤسسة ممثلة في شخص المدير العام صرح مرارا وتكرارا على ضرورة التوجه لهذا المجال. تعتبر المؤسسة على دراية بأن الرقمنة ستسهم في تحسين إنتاجية العمل وتقليل التكاليف وزيادة التنافسية في سوق الطاقة. تهدف أيضًا إلى توسيع قدرتها على الابتكار وتطوير حلول تقنية جديدة تلبي احتياجات العملاء والمستهلكين في قطاع الطاقة. باعتبارها مؤسسة رائدة في قطاع الطاقة، تسعى نفطال لأن تكون في طليعة المؤسسات التي تعتمد على التكنولوجيا والابتكار، وأن تضع استراتيجية قوية لتطوير وتحسين الأنظمة الرقمية والبنية التحتية التكنولوجية التي تعتمد عليها.
E2	تحاول مؤسسة نفطال وضع مخططًا للرقمنة كجزء من استراتيجيتها المستقبلية. بحيث هدفها محاولة تعزيز الرقمنة وتحسين الأعمال من خلال اعتماد التكنولوجيا الحديثة وتطوير البنية التحتية الرقمية
نقد الإجابتين	
اتضح من خلال هذه المقابلة إلى أن مؤسسة نفطال فرع غرداية مهتمة بشكل كبير بتطبيق الرقمنة ،بحيث تتميز بوجود مخططات مستقبلية محددة لتطبيق تقنيات الرقمنة الحديثة، تهدف المؤسسة أيضا لتحسين أدائها وتحسين جودة خدماتها وتعظيم أرباحها وهذا عبر استخدام التكنولوجيا الحديثة، ونظرًا لأنه يعد جزءًا أساسيًا من استراتيجية المؤسسة، يمكن أن يتوقع المرء أن يكون للمؤسسة نفطال خططًا مفصلة لتطوير الرقمنة على المدى الطويل والقصير، هذه الخطط قد تتضمن تحديث الأنظمة المعلومات وأنظمة حماية خاصة بها وتكثيف استخدام التقنيات الحديثة ،حيث تشير هذه المقابلة إلى أن مؤسسة نفطال تولي اهتمامًا كبيرًا للرقمنة ،ولا يتمحور تطوير مؤسسة نفطال رقميا على تثبيت نظام معلوماتي جديد فحسب ،بربل انه يشمل أيضًا تحسين البنية التحتية الرقمية، ويعني هذا أن المؤسسة تريد تعزيز الرقمنة على جميع المستويات، مما يمكنها في تعزيز تنافسيتها وجذب وإرضاء زبائن الحاليين والجدد.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

3- عرض وتحليل أجوبة السؤال الثالث: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (13):** أجوبة وتحليل على السؤال الثالث

السؤال الثالث	
ماهي البرمجيات المستخدمة في شركة نفطال؟	
الترميز	**الجواب**
E1	هناك الكثير من البرمجيات المستخدمة على مستوى مؤسسة نفطال فرع غرداية والتي مهمتها أداء المهام واعمال الوظيفية ومختلف أنشطة ،لهذا سوف نذكر على سبيل المثال بعض هذه البرامج : SD COM –NAF G1 –NAF-COMPTA –NAF IMMO-NAF IP
E2	نعم توجد لدى مؤسسة مجموعة من البرامج والتي مهمتها مساعدة في تنظيم وتخزين البيانات بشكل مركزي ومنهجي، مما يسهل الوصول إليها وإدارتها بكفاءة ،وكذا تحسين أداء وربح وقت وتكاليف والتي على رأسها نظام المعلومات : SD COM .
تحليل الإجابتين:	
يمكن القول بأن المؤسسة لها العديد من البرمجيات يتم استخدمها من قبل مجمل المصالح المختلفة لدى المؤسسة ،وهذا لأجل أداء مجموعة من الأعمال التواجه مختلف الوظائف ،ومن بين هذه الوظائف نذكر: مصلحة الشراء – مصلحة المحاسبة والمالية – مصلحة الموارد البشرية والأجور– مصلحة الجودة.... ، والغرض من هذه البرمجيات تنظيم وتتبع العمليات والموارد المالية للمؤسسات بشكل فعال ،ومن خلال هذه البرمجيات يتم حصول على تقارير دقيقة وشاملة تغطي جميع مستويات المؤسسة ،أيضا ترفع هذه البرامج كفاءة العمل وتقلل الجهد المبذول وكذا توفير تخزين وحفظ البيانات المالية الحساسة بشكل أمن ومنظم.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

4- عرض وتحليل أجوبة السؤال الرابع: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (14):** أجوبة وتحليل على السؤال الرابع

السؤال الرابع	
هل البرامج المستخدم في مجال المحاسبي والمالي ؟ هل انتاج محلي أو أجنبي ؟:	
الترميز	**الجواب**
E1	**- هل انتاج البرامج :** محلي: ■ أجنبي : ☐

	نعم تعتبر البرامج الموجودة على مستوى مؤسستنا من إنتاج محلي بحيث تم تطويرها من قبل مهندسي المؤسسة بالتعاون مع مديري المالية والمحاسبة.
E2	– **هل انتاج البرامج :** محلي: ■ أجنبي : □ البرامج المستخدمة لدينا هي من إنتاج مهندسين تابعين للمديرية العامة.
تحليل الإجابتين:	
يمكن القول بأن مؤسسة نفطال دائما تحاول إنتاج أنظمة وبرامج معلوماتية من خلال مهندسين والتقنين التابعين لها وهذا محاولة منها لضمان سرية معلوماتها بالدرجة الأولى وثقتها في مهندسين التابعين لها.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

5– عرض وتحليل أجوبة السؤال الخامس: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (15)**: أجوبة وتحليل على السؤال الخامس

السؤال الخامس	
ماهي مدخلات والمخرجات هذا النظام ؟	
الترميز	**الجواب**
E1	تعتبر مدخلات بأنها عبارة عن مجموعة من بيانات كحركة المبيعات ،المخزونات ، الخزينة ،الفواتير ، الأجور. أما بالنسبة للمخرجات فهي عبارة عن مختلف القوائم المالية.
E2	قد تشمل المدخلات في شركة نفطال على سبيل المثال: بيانات الإنتاج النفطي والغازي، معلومات المخزون، بيانات العملاء والعقود، معلومات الموظفين، وغيرها من المعلومات ذات الصلة. فأما بالنسبة للمخرجات قد تشمل في شركة نفطال مثلاً: تقارير الإنتاج والأداء، تحليلات البيانات، الفواتير والفواتير المالية، تحديثات المخزون، وغيرها من البيانات المهمة لعمليات الشركة واتخاذ القرارات..
تحليل الإجابتين:	
تبين من المقابلة أن مدخلات النظام هي عبارة عن مجموعة من البيانات وممثلة فيما يلي : حركة المبيعات ،الفواتير ،المخزونات ... التي يتم معالجتها من قبل النظام لكي تصبح معلومات جاهزة الاستخدام والتي على ضوئها يتم اتخاذ قرارات ومن بين هذه المخرجات نجد: مختلف القوائم المالية.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

6- عرض وتحليل أجوبة السؤال السادس: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي:

الجدول رقم (16): أجوبة وتحليل على السؤال السادس

السؤال السادس	
هل يرقى هذا البرنامج الى نظام معلومات محاسبي متكامل؟ **- في كلتا الاجابتين لماذا؟** نعم: ☐ لا: ☐	
الجواب	**الترميز**
نعم: ▬ لا: ☐ حسب ما توضح لنا ومنذ تطبيق هذا البرنامج في سنة 2018. بشكل عام، يمكن أنه برنامج متكامل .	**E1**
نعم: ▬ لا: ☐ نعم يمكنك القول أنه برنامج متكامل.	**E2**
تحليل الإجابتين:	
من خلال إجابتين المقدمة من طرف المعنين بالمقابلة ، يتوضح أن النظام المعلومات المحاسبي الموجود على مستوى مؤسسة نفطال يمكن القول أنه يرقى إلى نظام المعلومات متكامل ،وهذا نظرا لتوفيره جميع متطلبات التي تحتاجها مختلف المصالح التابعين للمؤسسة ،كما تميزه بالنظام حماية قوي للحفاظ على معلومات حساسة والمهمة الخاصة بالمؤسسة ،أيضا من خلال هذه المقابلة يمكننا أن نرى أن فكرة هذا النظام هي قائمة على أخطاء وثغرات نظام السابق.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

7- عرض وتحليل أجوبة السؤال السابع: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي:

الجدول رقم (17): أجوبة وتحليل على السؤال السابع

السؤال السابع	
السؤال السابع: في رأيكم ماهي المرتكزات التي يقوم عليها هذا النظام اذا كان موجودا ؟ **في حالة إجابة ب لا: ماهي جهود المؤسسة في بناء نظام المعلومات؟**	
الجواب	**الترميز**
يرتكز النظام الموجود لدينا على جودة المعلومات المالية وهذا ما يضمن دقة وسلامة البيانات التي ينتجها	**E1**

	النظام.
E2	بما أن النظام لم تصدر منه أية أخطاء أو أعطاب إلى وقتنا الحالي ، يمكن القول أنه يرتكز على دقة وثبات وتحقيق استمرارية في أداء أعمال ومهام.
تحليل الإجابتين:	
يؤكد أصحاب الإجابات (**E1**، **E2**) أن النظام الموجود لدى المؤسسة من أهم مرتكزاته هي جودة ودقة المعلومات المحاسبية ،فهذه الأخيرة تلعب دورا حيويا في نجاح واستمرارية المؤسسات ،وتساهم في تحسين مصداقية وشفافية لدى المؤسسات مما يدعم نموها وكبر حجمها.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

8- عرض وتحليل أجوبة السؤال الثامن: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي:

الجدول رقم (18): أجوبة وتحليل على السؤال الثامن

السؤال الثامن	
هل يتم تخزين البيانات ومعلومات المؤسسة في الأدوات السحابية أو الخوادم الالكترونية ؟اذا كان بالخوادم فهل ملكية الخوادم للمؤسسة أو لهيئة اخرى ؟	
الترميز	**الجواب**
E1	- **تخزين السحابي:** ☐ **الخوادم:** ▬ يتم تخزين بيانات ومختلف معلومات الخاصة بالمؤسسة على مستوى خوادم إلكترونية خاصة بالمؤسسة ، بحيث تعود ملكية هذه الخوادم إلى مؤسسة.
E2	- **تخزين السحابي:** ☐ **الخوادم:** ▬ نعم يتم تخزين كل معلومات على مستوى خوادم إلكترونية.
تحليل الإجابتين:	
يؤكد المدير ومهندسة الإعلام ألي التابعين لمؤسسة نفطال فرع غرداية أن عملية تخزين البيانات الخاصة بالمؤسسة تكون خوادم إلكترونية موجودة على مستوى المؤسسة ،من ملكية مؤسسة أيضا ، ويرجع اختيار المؤسسة تخزين في الخوادم إلى محاولة سيطرة على بياناتها بشكل كامل ،أيضا تمتاز الخوادم بدرجة عالية من الأمان والحماية وتكلفة أقل للتخزين ، أيضا تعتبر الخوادم قابلة للتخصيص وفقا للاحتياجات المؤسسة ،وتقليل من المخاطر المتعلقة بالاعتماد على خوادم الغرباء.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

9- عرض وتحليل أجوبة السؤال التاسع: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (19):** أجوبة وتحليل على السؤال التاسع

السؤال التاسع	
هل هناك جدار ناري لحماية مختلف الأنظمة والبيانات الموجود في المؤسسة ؟	
الترميز	**الجواب**
E1	نعم هناك جدار ناري (Firewall) لحماية مختلف الأنظمة والبيانات في مؤسسة نفطال. الذي هو عبارة عن نظام أمني يستخدم لفصل شبكة الكمبيوتر الداخلية عن الشبكة الخارجية (مثل الإنترنت) ولمنع وفحص التدفقات غير المصرح بها من وإلى الشبكة الداخلية.
E2	يوجد لدينا جدار ناري لحماية النظام من مختلف التجاوزات والاختراقات.
تحليل الإجابتين:	
يشرح المدير ومهندسة الإعلام ألي بأن مؤسسة نفطال فرع غرداية تمتلك جدار الناري لحماية أنظمتها من كل أشكال الاختراقات والتسللات الغير مصرح بها وتوفير بيئة موثوقة وأمنة للعمل وضمان التبادل الإلكتروني للبيانات.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

10- عرض وتحليل أجوبة السؤال العاشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (20):** أجوبة وتحليل على السؤال العاشر

السؤال العاشر	
في العمليات المالية العادية هل يتم استخدام تطبيقات اخرى ؟	
الترميز	**الجواب**
E1	**نعم:** ▬ **لا:** ☐ نعم في العمليات والمعاملات المالية، يتم استخدام بعض تطبيقات المساعدة تيسير وتسريع هذ العمليات المالية ومن بين هذه التطبيقات أنظمة الدفع الإلكتروني.
E2	**نعم:** ▬ **لا:** ☐ نعم هذا ممكن.

تحليل الإجابتين:
يشرح المدير بأنه في بعض المعاملات المالية العادية ، تلجأ المؤسسة إلى بعض تطبيقات أخرى للأداء مهامها ومن بين هذه تطبيقات نذكر : أنظمة الدفع الإلكتروني كأجهزة **TPE** القارئة للبطاقات ، وبطاقات الوقود خاصة بمؤسسات نفطال مهمتها أداء مختلف الخدمات.

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

11- عرض وتحليل أجوبة السؤال الحادية عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (21)**: أجوبة وتحليل على السؤال الحادية عشر

السؤال الحادية عشر	
السؤال الحادية عشر في المعاملات الخارجية كعمليات الجباية والتحصيلات *هل يتم استخدام تطبيقات مثل: مساهمتك ، جبايتك.....الخ.	
الترميز	**الجواب**
E1	**نعم:** ▬ **لا:** ▭ نعم في معاملات الخارجية كما تم ذكرهم في سؤالكم مثل العمليات الجبائية والتحصيلات تستخدم بعض التطبيقات المساعدة ومن بينها منصتي : جبايتك ، ومساهمتك ،وهذا من قبل المديرية العامة للمالية والمحاسبة.
E2	**نعم:** ▬ **لا:** ▭ ربما هذا أيضا ممكن.
تحليل الإجابتين:	
تكشف هذه المقابلة واقع المعاملات الخارجية في مؤسسة نفطال فرع غرداية كالعمليات الجبائية والتحصيلات ،حيث يتم استخدام منصتي جبايتك ومساهمتك وهذا من قبل مديرية العامة للمالية المحاسبة ،وهذا بسبب أنها معتمدة من قبل مديرية الضرائب ،أيضا تقدم مجموعة من حلول جبائية تساعد المؤسسة في كيفية تصريح بالواجبات التي اتجاه مصالح الضرائب.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

12- عرض وتحليل أجوبة السؤال الثاني عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (22):** أجوبة وتحليل على السؤال الثاني عشر

السؤال الثاني عشر	
في تسيير محطات الوقود * هل يتم استخدام أجهزة TPE في عمليات التعبئة؟ وادا كانت الإجابة نعم، هل هذه الأجهزة مرتبطة بنظام الكتروني مركزي؟	
الترميز	**الجواب**
E1	نعم ،تمتلك مؤسسة أجهزة قارئة للبطاقات **TPE**، بحيث هي موجودة على مستوى بعض المحطات. وهي مرتبطة بنظام إلكتروني مركزي بحيث يمكن المؤسسة من استفادة من تبسيط وتنظيم عمليات البيع ،وتوفير الوقت والجهد في إدارة المعاملات المالية.
E2	نعم متوفر وكذلك هي مرتبطة بالنظام المركزي
تحليل الإجابتين:	
من خلال إجابات المقدمة نلاحظ انا قارئ البطاقات **TPE** متوفرة لدى المؤسسة وهي كذلك مرتبطة بأنظمة إلكترونية مركزية يمكننا أن نقول أن هذا ما يساعدها على تحسين كفاءتها ودقتها في إدارة بياناتها.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

13- عرض وتحليل أجوبة السؤال الثالث عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (23):** أجوبة وتحليل على السؤال الثالث عشر

السؤال الثالث عشر	
بطاقات الدفع الالكترونية المستخدمة عندكم *هل هي معتمدة من طرف شركة "SATIM" ؟	
الترميز	**الجواب**
E1	**نعم:** ☐ **لا:** ▬ لا هذه الأجهزة خاصة بمؤسسة نفطال وفقط.
E2	لا،بطاقات الإلكترونية هي من إنتاج للمديرية العامة لمؤسسة نفطال.
تحليل الإجابتين:	
يُأكد المدير أن بطاقات الدفع الإلكتروني المستخدمة لدى المؤسسة ليست معتمدة لدى شركة SATIM ،بل معتمدة من طرف مؤسسة أي خاصة بمؤسسة نفطال.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

14- عرض وتحليل أجوبة السؤال الرابع عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (24):** أجوبة وتحليل على السؤال الرابع عشر

السؤال الرابع عشر	
هل تقوم المؤسسة بتكوين مستمر للمهندسين والتقنيين في مجال البرمجيات وتحديثاتها ؟	
الترميز	**الجواب**
E1	**نعم:** ▬ **لا:** ☐ نعم هناك دائما برامج تكوينية على مدار السنة.
E2	**نعم:** ▬ **لا:** ☐ نعم تكوينات دائما موجودة ومتواصلة وخاصة بعد ظهور أنظمة وبرمجيات حديثة وجب علينا مواكبتها وتتبع تطورات الحديثة.
تحليل الإجابتين:	
تسعى المؤسسة دائما لرفع من كفاءة عاملين وهذا بإقامة تكوينات في مجال البرمجيات وكيفية استعمالها ،أيضا تختص هذه التكوينات في أمور الخاصة بالحماية وهذا من خلال نشر سياسات وإجراءات أمنية وجب إتباعها ، أما بالنسبة للمديرية العامة فتكون التكوينات عن طريق إرسال العاملين خاصة المهندسين والقائمين على جوانب الحماية إلى خارج وهذا من اجل رفع كفاءتهم.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

15- عرض وتحليل أجوبة السؤال الخامس عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (25):** أجوبة وتحليل على السؤال الخامس عشر

السؤال الخامس عشر	
في ظل اتجاه الدولة نحو استخدام الذكاء الاصطناعي والروبوتيك في الانتاج والتخزين ،هل هناك اتجاه المؤسسة نحو اعادة تجديد اصولها الثابتة ؟	
الترميز	**الجواب**
E1	نعم: ▬ لا: ☐ نعم هناك جهود وتوجهات في ذلك من خلال تجديد أصول المؤسسة في ظل الموارد المالية المتوفرة لدى المؤسسة.

E2	نعم: ▬ لا: ☐ نعم هناك رغبة بخصوص ذلك ، لكن حاليا ليست ذات أولية بالنسبة للاحتياجات.
تحليل الإجابتين:	
ومن خلال أجوبة اتضح لنا أن هناك توجه لمؤسسة نفطال لاستخدام الذكاء الاصطناعي والروبوتيك في الانتاج والتخزين ،لكن في وقت الحالي ليس من مخططات المؤسسة.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

16- عرض وتحليل أجوبة السؤال السادس عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (26)**: أجوبة وتحليل على السؤال السادس عشر

السؤال السادس عشر	
هل تم اختراق الأنظمة التي تستخدمها مؤسسة نفطال من قبل ؟ **اذا كانت نعم ماهي الاجراءات التي تم اتخاذها؟ وهل أثرت على سيرورة عمل المؤسسة؟**	
الترميز	**الجواب**
E1	**نعم**: ▬ **لا**: ☐ نعم تم اختراق المؤسسة مرة واحدة وهذا سنة 2020 (بداية أزمة كورونا) ،أدى ها إلى تعامل بطرق التقليدية (أوراق ، عدم استعمال الشبكة)
E2	**نعم**: ▬ **لا**: ☐ نعم تم اختراق المؤسسة من قبل. مما أدى ذلك إلى تعطيل كامل في المعاملات الإلكترونية لمدة شهر ونصف تقريبا وهذا ما أثر على سيرورة العمل .
تحليل الإجابتين:	
من خلال إجابات المقدمة نلاحظ أنه وفي سنة 2020 تحولت المؤسسة إلى معاملات التقليدية وهذا بسبب تعرض إلى اختراق أدى إلى تعطل المعاملات الإلكترونية ومن بين الإجراءات المتخذة بهذا صدد فصل الشبكة عن البرامج المحاسبية وتم تحول إلى الشبكة الداخلية.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

17- عرض وتحليل أجوبة السؤال السابع عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (27)**: أجوبة وتحليل على السؤال السابع عشر

السؤال السابع عشر	
هل هذا الاختراق كان نتيجة أخطاء داخلية او قصور في انظمة المعلومات ؟	
الجواب	**الترميز**
أخطاء داخلية: ☐ **قصور في انظمة المعلومات :** ▬	**E1**
أخطاء داخلية: ☐ **قصور في انظمة المعلومات:** ▬	**E2**
تحليل الإجابتين:	
نستخلص من هدا الأجوبة المقدمة أن في سنة 2020 كان هناك تقصير من ناحية نظم المعلومات وأن أنظمة حمايتها سيئة، وهذا ما تم استغلاله لشن هجوم على مؤسسة	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

18- عرض وتحليل أجوبة السؤال الثامن عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (28)**: أجوبة وتحليل على السؤال الثامن عشر

السؤال الثامن عشر	
في حالة الاخطاء الداخلية *هل يتم الاستعانة بجهات أمنية سيبرانية ؟	
الجواب	**الترميز**
نعم: ▬ **لا:** ☐ نعم يمكن هذا من قبل المديرية العامة تستقدم خبراء أمنين وسيبرانيين لوضع خطط واستراتيجيات أمنية للحماية.	**E1**
نعم: ▬ **لا:** ☐ نعم ،إذا كان الأمر يتطلب ذلك.	**E2**
تحليل الإجابتين:	
نرى من خلال إجابات المستجوبين أن إدا كان الخطأ داخلي يتم استعانة بخبراء في مجال الحماية وهذا من قبل المديرية العامة بكون أن مؤسسة نفطال بولاية غرداية تعتبر فرع تحت سلطة مديرية العامة.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

19- عرض وتحليل أجوبة السؤال التاسع عشر: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (29):** أجوبة وتحليل على السؤال التاسع عشر

السؤال التاسع عشر	
في رأيكم ماهي معوقات التي تواجه المؤسسة في مجال الأمن السيبراني ؟	
الترميز	**الجواب**
E1	تكمن معوقات في تكاليف العالية للأنظمة.
E2	من بين المعيقات نقص الموارد اللازمة لضمان الحماية وكدلك نقص ثقافة لدى العمال.
تحليل الإجابتين:	
من خلال أجوبة نستنتج أن من بين أهم المعوقات التي تواجه مؤسسة نفطال في مجال الأمن السيبراني نجد: نقص الثقافة الأمنية لدي العاملين بدرجة الأولى ، قصور من المؤسسة في تجهيز الفروع بالأجهزة اللازمة لضمان حماية أنظمتها ومعلوماتها المالية والتهديدات الخارجية.	

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

20- عرض وتحليل أجوبة السؤال العشرين: جاءت أجوبة مدير ومهندسة الاعلام الالي على هذا السؤال على النحو التالي: **الجدول رقم (30):** أجوبة وتحليل على السؤال العشرين

السؤال العشرين	
جهود المؤسسة واستراتيجيتها في مجال الأمن السيبراني لقطاع مهم في مجال الطاقة ؟	
الترميز	**الجواب**
E1	شراء أنظمة حماية متطورة Kaspersky ، تكوين عالي المستوى في الخارج للمهندسين في الإعلام ألي ، شراء تجهيزات متطورة.
E2	تشمل جهود المؤسسة نفطال في مجال الأمن السيبراني في : وضع استراتيجية الأمن السيبراني ،تنفيذ إجراءات الوقاية ،التدريب والتوعية.
تحليل الإجابتين:	
على ضوء إجابة من طرف مدير مؤسسة نفطال ومهندسة الإعلام ألي ،استخلصنا أن المؤسسة تستثمر المؤسسة في أنظمة حماية متطورة مثل Kaspersky وتقديم تدريب متقدم للمهندسين الإعلام الألي وشراء أجهزة متطورة بهدف تعزيز الأمن السيبراني وتحسين البنية التحتية التكنولوجية ،تلك الجهود تعكس التزام المؤسسة بتعزيز الأمان	

السيبراني وحماية البيانات والأصول الحيوية من خلال استراتيجية محكمة وتنفيد إجراءات الوقاية الفعالة وتوفير التدريب المستمر والتوعية ، نلاحظ أن المؤسسة تسعى إلى ضمان استمرارية العمليات دون تعرضها للهجمات السيبرانية مرة أخرى.

المصدر: من إعداد الطالبين بناءا على مخرجات المقابلة مؤسسة نفطال غرداية 2023.

ثانيا: استخلاص النتائج :

من خلال هذا العنصر سوف نستعرض أهم نتائج المقابلة التي تم استخلاصها ،والتي تم إجراءها مع إطاري مؤسسة نفطال (مدير ، مهندسة إعلام آلي) ،التي كان هدفها التعرف على واقع أنظمة المعلومات الموجودة لدى المؤسسة ودرجة حمايتها وهذا ما يتم سرده تباعا كالاتي:

1. يتضح من خلال الأجوبة التي لها علاقة بالرقمنة والتحول الرقمي أن المؤسسة تولي أهمية كبرى لرقمنة العمليات والأعمال لمواكبة تكنولوجيا الحديثة ،هذا من خلال وضع مخططات مستقبلية لتطبيق تقنيات الرقمنة بهدف تحسين الأداء وجودة خدمات المؤسسة.
2. تسعى مؤسسة نفطال للوصول إلى نظام معلومات متكامل وهذا من خلال الأنظمة المطبقة على مستوى المؤسسة حاليا ، والتي من بينها نظام SD COM الذي يعتبر نظاما للمعلومات ، وحسب إجابات المستجوبين أن هذا نظام يفي بالغرض إلى حد الساعة منذ تطبيقه ،بحيث من مرتكزات الرئيسية لهذا النظام جودة ودقة المعلومات المحاسبية التي يوفرها.
3. يتبين من خلال الإجابات المقدمة من مدير ومهندسة الإعلام آلي أن هناك مجموعة من البرمجيات التي يتم استخدامها على مستوى مختلف المصالح والوظائف ،ومن بين هذه البرمجيات نجد: NAF G1 – NAF IMMO-NAF IP –NAF-COMPTA ، إضافة لنظام SD COM وهذه البرمجيات هي برامج مطورة من قبل مهندسين وتقنين تابعين للمديرية العامة لمؤسسة نفطال ،وعلى ضوء هذا استخلصنا أن هذه البرامج من إنتاج محلي والغرض من هذا هي محاولة المؤسسة ضمان لسرية معلوماتها وكذا ثقتها في مؤهلات مهندسيها.
4. تمتلك مؤسسة نفطال خوادم إلكترونية يتم من خلالها تخزين جميع معلوماتها وبياناتها ،وتفضل المؤسسة التخزين في الخوادم عكس التخزين في السحابات الإلكترونية لمحاولة منها السيطرة على كافة بياناتها

لتجنب أية تحريف أو تعديل فيها من خلال متسللين الغير مصرح بهم وضمان الأمان والحماية لها ،وهذا مالا يضمنه التخزين السحابي.

كما تمتلك المؤسسة أيضا جدران نارية (Firewall) لحماية مختلف الأنظمة والعمليات الموجودة في بنيتها التحتية الرقمية. توفر هذه الجدران النارية طبقة إضافية من الحماية وتعزز أمان الشبكة والمعلومات المهمة ، كما تساعدها في منع الوصول غير المصرح به من خلال رصد محاولات الاختراق وتحليلها ومنعها قبل أن تتسبب في أي ضرر والوقوف أمام كل التهديدات السيبرانية المحتملة.

5. يتوضح من خلال الإجابات المقدمة أنه وفي العمليات المالية العادية يتم استخدام تطبيقات مختلفة بهدف تسريع هذه المعاملات المالية ،ومن بين هذه التطبيقات استخدام أنظمة الدفع الإلكتروني ممثلة في أجهزة القارئة للبطاقات TPE ،والتي تمتلكها المؤسسة ومربوطة بنظام إلكتروني مركزي يتم تسييرها من خلاله ،كما تستخدم المؤسسة مجموعة من بطاقات إلكترونية (بطاقات الوقود) وهي خاصة بمؤسسة.

أما في المعاملات الخارجية الجبائية ، تستخدم المؤسسة بعض التطبيقات المساعدة المختصة بجوانب الضريبية والجبائية ومعتمدة من قبل مديرية العامة للضرائب والممثلة في منصتي : جبايتك ، مساهمتك.

6. يتجلى لنا أن حسب أجوبة المدير ومهندسة إعلام ألي أن هناك توجه لمؤسسة نفطال في استخدام بعض من تكنولوجيات الحديثة مثل : الذكاء الاصطناعي والروبوتيك في أداء أعمالها كإنتاج والتخزين ...،وهذا من خلال محاولتها لتجديد أصولها في ظل الموارد المالية المتوفرة لديها.

7. تواجه مؤسسة نفطال مجموعة من مخاطر أثناء أداء مهامها مثل أي مؤسسة تشتغل في طل تغيرات تكنولوجيا المعلومات والاتصال ومن بين هذه المخاطر : المخاطر السيبرانية ،التي وفي سنة 2020 تم اختراق المؤسسة ومن تأثيرات هذه الاختراق تم تعطيل كامل للمعاملات الإلكترونية المعتادة المؤسسة أن تقوم بها وهذا لمدة شهر ونصف تقريبا ،وسبب هذا الاختراق لم يكن في أخطاء الداخلية المرتكبة من قبل العاملين بل كان قصور في أنظمة المعلومات الموجودة أنداك لدى المؤسسة ،والتي كانت تتصف بدرجة حمايتها السيئة وهذا ما تم استغلاله من قبل مجرمين السيبرانين.

لكن ومنذ ذلك الاختراق سعت المؤسسة إلى رفع من كفاءتها في مجال الأمان والحماية السيبرانية ،وهذا من خلال تطبيق أنظمة تمتاز بحماية العالية ومنها نظام SD COM ،وكذا تطبيق مجموعة من

إجراءات الوقائية وخاصة مع مديرين والمسؤولين وأصحاب المراكز الحساسة في المؤسسة كتشفير البيانات واستخدام VPN في الهواتف الخلوية الخاصة بهم ،ولا تمانع مؤسسة نفطال في استعانة بخبراء خارجين في مجال الحماية وأمن السيبراني إذا ما تطلب ذلك لتصميم انظمة حماية متطورة قادرة على مجابهة جرائم السيبرانية واكتشاف أهم الثغرات الموجودة لدى المؤسسة.

8. تبرز أهم المعيقات التي تواجه مؤسسة نفطال حسب إجابات مدير ومهندسة إعلام ألي في مجموعة من الأمور التي لها علاقة مباشر بمؤسسة أو عكس ذلك ومنها: التكلفة العالية للبرمجيات الأمان وأنظمة الحماية لذا وجب تخصيص لها موارد مالية بشكل خاص ،أيضا تواجه مؤسسة مشكل نقص ثقافة السيبرانية لدى العاملين في مؤسسة ، تقصير في تجهيز الفروع التابعين للمؤسسة بالأجهزة اللازمة.
9. لهذا تسعى مؤسسة نفطال جاهدة في إتباع استراتيجية واضحة ومتكاملة في مجال الأمن السيبراني تتميز بكفاءة وفعالية وخاصة بالنسبة لقطاع حساس مثل الذي تعمل فيه المؤسسة وهو قطاع الطاقة ،ومن جهود الحالية التي أقدمت المؤسسة حاليا: شراء أنظمة حماية متطورة ك Kaspersky ، تكوين عالي المستوى لمهندسي الإعلام ألي وهذا بإرسالهم إلى خارج البلاد ،شراء مجموعة مختلفة من أجهزة متطورة.

المطلب الثالث : مقترح أنموذج لأمن نظم المعلومات

لبناءا أنموذج لأمن نظام المعلومات سنعرج على مؤشر GCI العالمي للأمن الإلكتروني وتجارب الدول في هذا المجال بالإضافة إلى الأدوات الممكن استخدامها للحد من مخاطر السيبرانية مع التعرف على أهم أنظمة المعلومات المحاسبية (ERP) الحديثة والكيفيات المستخدمة في الاختراق وهذا للوصول إلى التحديات الراهنة للأمن السبراني مع الذكاء الاصطناعي وأفاقهما المستقبلية.

أولا: مؤشر GCI العالمي للأمن الإلكتروني:

يعتبر مؤشر GCI (Global Cybersecurity Index) مؤشر دولي يقيس مدى استعداد الدول لمكافحة التهديدات السيبرانية وتعزيز الأمان الإلكتروني ،يتم تطوير هذا المؤشر بواسطة الاتحاد الدولي للاتصالات (ITU) وهو وكالة تابعة للأمم المتحدة ،يهدف هذا مؤشر GCI إلى تقييم قدرة الدول على التصدي للتهديدات السيبرانية من خلال تحليل عدة عوامل مختلفة، مثل السياسات والتشريعات المتعلقة بالأمن السيبراني

والقدرات الفنية والتقنية للحماية، والتعاون والتنسيق بين الأطراف المعنية، والتوعية والتدريب في مجال الأمن السيبراني.

يستند مؤشر GCI إلى البيانات المقدمة من الدول المشاركة والتقارير المقدمة للاتحاد الدولي للاتصالات ،يتم تحليل هذه البيانات وتقييمها لتحديد مستوى استعداد الدول في مجال الأمن السيبراني ،تصدر النتائج في تقرير سنوي يعكس ترتيب الدول وتطورها في مجال الأمان الإلكتروني.

يعد مؤشر GCI أداة مهمة لقياس التقدم في مجال الأمن السيبراني وتحفيز الدول على تعزيز قدراتها واستراتيجياتها في هذا الصدد ،كما يساهم في تعزيز التعاون الدولي في مجال الأمن السيبراني وتبادل الخبرات والممارسات الجيدة بين الدول.

ومن خلال الشكل التالي سوف نرى ترتيب الدول عالميا التي تتمتع بأكثر أمان إلكتروني الصادر سنة 2020:

الشكل رقم (07): يوضح ترتيب الدول من حيث مؤشر GCI العالمي للأمن الإلكتروني

Table 3: GCI results: Global score and

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14
Latvia	97.28	15

المصدر: ITU , **Global Cybersecurity Index 2020** ,P :25.

ومن خلال الشكل التالي سوف نرى ترتيب الدول العربية أكثر أمان إلكترونيا:

الشكل رقم(08) : يوضح ترتيب الدول العربية من حيث مؤشر GCI العالمي للأمن الإلكتروني

Country Name	Overall Score	Regional Rank
Saudi Arabia	99.54	1
United Arab Emirates	98.06	2
Oman	96.04	3
Egypt	95.48	4
Qatar	94.5	5
Tunisia	86.23	6
Morocco	82.41	7
Bahrain	77.86	8
Kuwait	75.05	9
Jordan	70.96	10

المصدر: ITU , **Global Cybersecurity Index 2020** ,P :29.

ومن خلال الشكلين الماضين فنرى و.م.أ هي صاحبة المركز الأول عالميا وهذا شيء طبيعي نظرا لسيطرت الشركات الأمريكية على تكنولوجيا المعلومات واتصال في العالم ، لكن الشي غير عادي هو احتلال المملكة العربية السعودية المرتبة الثانية عالميا وهذا يعتبر إنجاز وجب الوقوف عنده وإشادة به.

أ- تجربة السعودية في الأمان الإلكتروني:

إن تطور الرهيب الذي شهدته المملكة العربية السعودية في مجال أمن السيبراني لم يكن وليد الصدفة ،بل كان وراءه عمل كبير قام بها القائمين على أمن الإلكتروني في هذه البلاد ،فلو نرى ترتيب أخر سنوات من حيث مؤشر GCI فيمكننا أن نرى قفز كبيرة التي قامت بها في هذا الترتيب ، ويمكن توضيح هذا عبر الشكل التالي:

الجدول رقم (31): يوضح ترتيب السعودية في مؤشر GCI

2020	2018	2017
المركز 2	**المركز 13**	**المركز 46**

المصدر : من إعداد الطالبان باعتماد على برنامج سين2.

ومن أسباب هذه قفز كبيرة نذكر ما يلي :[1]

- الاستفادة من تجارب الدول الأخرى.
- عدم الوقوف فقط على تجارب الدول الأخرى بتفعيل مراكز البحث والتطوير.
- مراكز خاصة بمراقبة الأمن السيبراني.
- رفع الوعي والتعليم والتدريب.

ب- ترتيب الجزائر في مؤشر GCI العالمي :

أما بالنسبة للجزائر فنرى أنها متأخرة جدا في ترتيب مؤشر GCI إما عالميا أو عربيا ،والممثلة كلاتي:

الشكل رقم (09): الشكلين التالين يوضحان تريب الجزائر عالميا وعربيا في مؤشر GCI

عالميا

Algeria	33.95	104

عربيا

Algeria	33.95	12

المصدر : ITU,**IBID**,P:26/29

ج- الأمن السيبراني في التشريع الجزائري :

وكنظيرتها من الدول الأخرى أيضا سعت الجزائر لمجابهة الجرائم السيبرانية ومحاولة صدها ،وهذا ببزوغ القانون رقم 09- 04 سنة 2009 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ،حيث تضمن هذا القانون 6فصول و19 مادة توضيحية في مجال تطبيقه وعلى ضوء هذا القانون تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا والإعلام والاتصال ومكافحته . لكن هذا غير كاف فوجب من القائمين على الجوانب الأمنية وضع خطط واستراتيجيات تتماشى مع ما تشهده التغيرات الحديثة لتكنولوجيا الإعلام واتصال.

ثانيا: بعض الأدوات ممكن استخدامها للحد من مخاطر السيبرانية:

1- الدليل النشط Active Directory: هو خدمة دليل تم تطويرها بواسطة Microsoft ظهرت لأول مرة في2000 ،وتستخدم لإدارة وتنظيم الموارد داخل بيئة الشبكة. ويوفر هذا أخير قاعدة بيانات مركزية

[1] برنامج سين2, https://www.youtube.com/watch?v=82ETlrSTHBE, 2023 /05/18, 20:00.

لتخزين وإدارة المعلومات حول موارد الشبكة مثل المستخدمين وأجهزة الكمبيوتر والمجموعات والكائنات الأخرى ،ويقدم الدليل النشط مجموعة كبيرة للغاية من المميزات الأساسية، ومن بينها إمكانية الفهرسة والاستعلام التي تمكن المسؤولين المستخدمين والبرامج من الوصول إلى المعلومات المتعلقة بالدليل بفعالية كبيرة بالإضافة إلى أنه يعمل على تحديد فئات السمات والكائنات التي يتضمن عليها الدليل، وهو يعمل بمثابة "Catalogue" كتالوج شامل يتضمن على المعلومات التفصيلية حول جميع الكائنات داخل الدليل بالإضافة إلى إمكانية النسخ التي تعمل على نشر البيانات من خلال الشبكة.

يسمح Active Directory للمسؤولين بتحديد سياسات الأمان وكيفية تنفيذها ،وإدارة وصول المستخدم إلى موارد الشبكة ،وتبسيط مهام إدارة الشبكة ، يستخدم بنية هرمية تسمى المجال لتنظيم وتمثيل موارد الشبكة مع كل مجال يحتوي على كائنات ونطاقات فرعية .تتضمن بعض الميزات الرئيسية لActive Directory ما يلي:[1]

- **إدارة المستخدم والمجموعة:** يتيح Active Directory للمسؤولين إنشاء وإدارة حسابات ومجموعات المستخدمين ، وتعيين الأذونات وحقوق الوصول ، وتحديد سياسات المجموعة.
- **المصادقة والترخيص:** يوفر إطارًا لمصادقة المستخدمين وتفويضهم للوصول إلى موارد الشبكة بناءً على بيانات اعتمادهم والأذونات المعينة.
- **تسجيل الدخول الأحادي:** يدعم Active Directory تسجيل الدخول الأحادي (SSO) ، مما يسمح للمستخدمين بتسجيل الدخول مرة واحدة والوصول إلى موارد متعددة داخل الشبكة دون إعادة إدخال بيانات الاعتماد الخاصة بهم.
- **خدمات المجال:** تقدم خدمات المجال مثل وحدات التحكم بالمجال ، وهي خوادم مسؤولة عن مصادقة المستخدمين والحفاظ على قاعدة بيانات الدليل.
- **إدارة نهج المجموعة:** تسمح للمسؤولين بتحديد السياسات وكيفية تنفيذها عبر الشبكة ، والتحكم في الجوانب المختلفة لتجربة المستخدم وسلوك النظام.

[1] محمد عمر ، https://www.momar.tech/2021/05/active-directory.html ، 2023/05/15، 20:00.

يتم استخدام Active Directory بشكل شائع في بيئات الشبكات المستندة إلى Windows ويتكامل مع منتجات وخدمات Microsoft الأخرى ، مثل Windows Server و Exchange Server و SharePoint. إنها تلعب دورًا مهمًا في إدارة وتأمين موارد الشبكة ، وتسهيل إدارة المستخدمين ، وتبسيط المهام الإدارية في بيئات المؤسسة ،وبمناسبة فإن مؤسسة نفطال قامت بإدراج خدمة البريد الإلكتروني ضمن كائنات البريد النشط ،عبر اعتماد على منصة Outlook بديلا للبريد الإلكتروني gmail ،ومن أهم الميزات التي اكتسبتها نظير تطبيقها Outlook:

- ♣ سهولة نقل المعلومات والاتصال.
- ♣ يمنع نقل الفيروسات.
- ♣ يمنع تثبيت البرامج الضارة.[1]

1. **جدار الحماية الناري Firewall** : جدار الحماية هو جهاز أو برنامج أمان شبكة يعمل كحاجز بين شبكة داخلية وشبكات خارجية مثل الإنترنت لحماية الشبكة الداخلية من الوصول غير المصرح به والأنشطة الضارة ،بحيث يقوم بإنشاء محيطًا أمنيًا ويراقب ويتحكم في حركة مرور الشبكة الواردة والصادرة بناءً على قواعد أمان محددة مسبقًا ،ويتمثل الغرض الأساسي من جدار الحماية هو فرض سياسات الأمان ومنع الوصول غير المصرح به إلى الشبكة. ومن أهم جدران الحماية المعروفة والموصى بها نذكر: Bitdefender BOX، Cisco Firepower ، Sophos XG ،Check Point Next Generation Firewall.[2]

وهناك عدة جوانب أساسية وجب تركيز عليها من قبل مصالح دعم نظم المعلومات وكذا المؤسسات على توفير أنظمة الحماية الخاص بها واتباع سياسات أمنية فعالة لاجتناب تعرضها للاختراق منها: الشبكات ، الويب التطبيقات ، البريد الالكتروني ،الخوادم .....،بحيث تعد هذه الأدوات المذكورة الأن إضافة إلى ما تم ذكره سلفا في جانب النظري وسائل يمكن من خلالها الحد من المخاطر السيبرانية.

[1] مقابلة مع رئيسة مصلحة إعلام آلي بمؤسسة نفطال ،2023/05/11, 09:00.

[2] Spice works, https://www.spiceworks.com/it-security/network-security/articles/top-10-firewall-hardware-devices/ ,15/05/2023,19:00.

ثالثا: أنظمة المعلومات المحاسبية (ERP) :

تعد أنظمة إدارة الموارد المؤسسة ERP عبارة عن مجموعة من التطبيقات أو الوحدات المتكاملة لإدارة عمليات الأعمال الأساسية لمؤسسات بما في ذلك عمليات المالية والمحاسبية وادارة الموارد البشرية الإعداد أوامر الشراء والمبيعات وإدارة المخازن وغير ذلك الكثير، لهذا من خلال هذا سوف نستعرض أهم البرامج المعروفة عالميا والمستخدمة في مجال المال والأعمال والممثلة في الشكل التالي:

الشكل رقم(10) :أنظمة المعلومات المحاسبية

المصدر: من إعداد الطالبان باعتماد على مواقع هذه البرامج

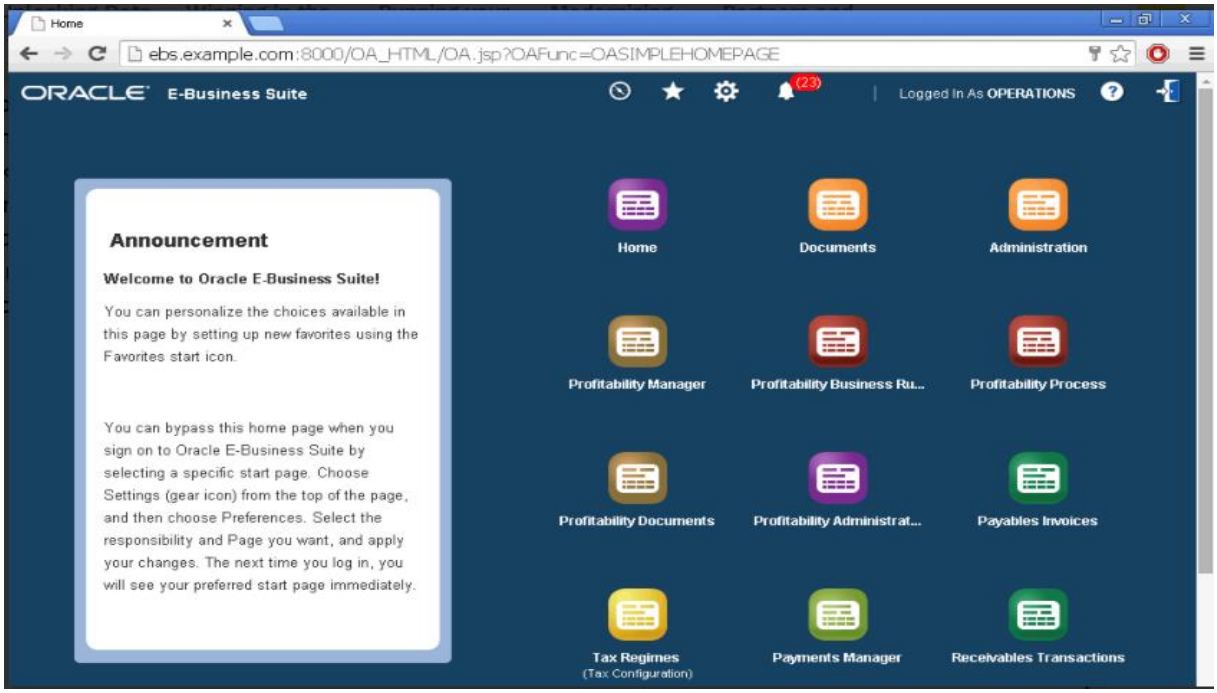
1- Oracle للأعمال الإلكترونية (Oracle E-Business) :

تأسست Oracle في 1977 من قبل Larry Ellison ، وكانت Oracle هي أول نظام لإدارة قواعد البيانات يدمج لغة SQL. تعد Oracle أيضًا أول شركة برمجيات تقوم بتطوير ونشر الإنترنت بنسبة 100 بالمائة وتمكين برامج المؤسسة عبر خط إنتاجها بالكامل :قاعدة البيانات وتطبيقات الأعمال والتطبيقات أدوات التطوير ودعم القرار ،أيضا تعتبر Oracle هي المالك الحصري للغة جافا Java، Oracle هي واحدة من الموردين الرائدين في العالم للبرامج في إدارة التكوين بحيث كبرى الشركات في العالم تستخدم هذه الحزمة على غرار :شركة أرامكو المحتلة المركز الثاني عالميا من حيث القيمة السوقية ، شركة الاتصالات السعودية STC ، وفي الجزائر فشركتي سونطراك و إتصالات الجزائر يستخدمان هذا البرنامج من خلال وجود أكثر من 55 تطبيق تغطي شؤون المالية والمحاسبية ،حيث يعد برنامج Oracle E-Business الأمريكي عبارة عن مجموعة كاملة ومتكاملة من تطبيقات الذي يسمح بإدارة كافة الأعمال الأساسية للمؤسسات.

1-1- التعريف ببرنامج (Oracle E-Business):

سوف يتم استعراض الواجهة الرئيسية للبرنامج أولا ،ثم يتم عرض الواجهة التي من خلالها يتم ذهاب إلى تطبيقات الفرعية :

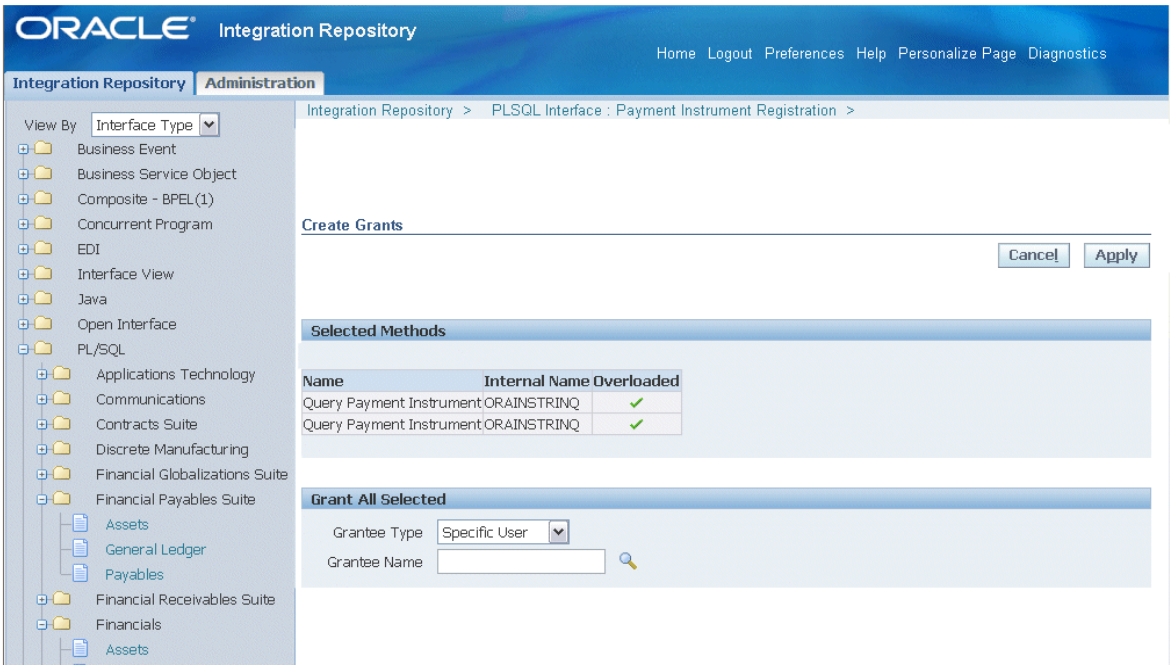
الشكل رقم (11) :واجهة الإستخدام الرئيسية لبرنامج **Oracle E-Business**



المصدر : **https://blog.pythian.com/oracle-e-business-suite-updates-from-openworld-2014/**

نلاحظ في الشكل أعلاه واجهة الاستخدام الرئيسية لبرنامج Oracle E-Business ،التي تحتوي على مجموعة متنوعة من أدوات وتطبيقات التي تغطي كل أعمال وأنشطة المؤسسات المتعلقة بجوانب المالية والمحاسبية وإدارة موارد البشرية وإنتاج.....

الشكل رقم(12) : الواجهة ذهاب إلى تطبيقات الفرعية



المصدر : **https://docs.oracle.com/cd/E18727-01/doc.121/e12064/T291171T466519.htm**

نلاحظ في الشكل أعلاه واجهة ذهاب إلى تطبيقات الفرعية لبرنامج Oracle E-Business ،و من بين هذه تطبيقات نذكر:

- Oracle Financials
- Oracle Order Management
- Oracle Enterprise Asset Management
- Oracle Warehouse Management System
- Oracle Inventory
- أو الذهاب لقاعدة البيانات Oracle Data bases

2- برنامج SAP:

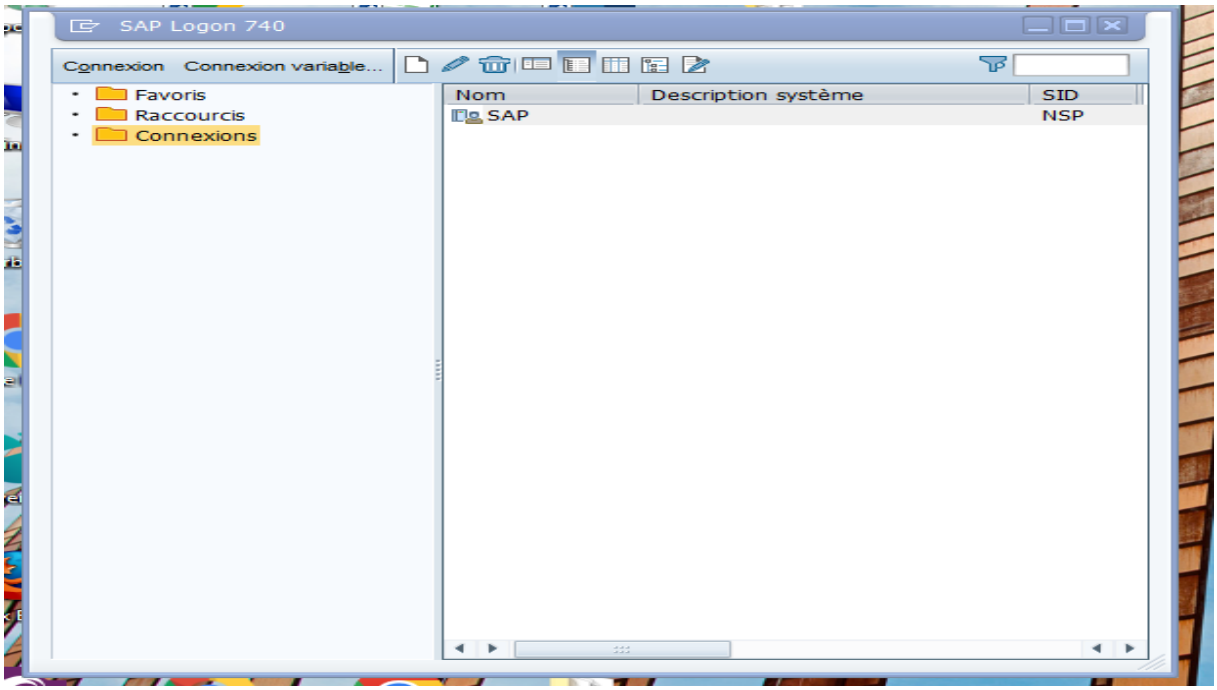
تأسست SAP في عام 1972 ، وهي رائدة في تقديم حلول الأعمال التعاونية. بحلول أبريل 2005كان قد حدث ما يقدر بـ 12 مليون مستخدم في جميع أنحاء العالم مع أكثر من 88,700 تثبيت . تتكون قائمة العملاء من الشركات من جميع الأحجام في 26 صناعة مختلفة ، بما في ذلك صناعة الطيران والسيارات ، والبنوك ، والمواد الكيميائية ، والسلع الاستهلاكية ، والتعليم العالي ، ومكتب البريد ، والمرافق.

ويعد برنامج SAP الألماني أحد أنظمة ERP التي تساعد على المؤسسات على دمج كافة أنظمة المعلومات الفرعية في نظام واحد والتي تهدف إلى أدارة مهامها وأعمالها اليومية ، بحيث يستخدم هذا البرنامج من عدة شركات عالمية نذكر: الخطوط الجوية السعودية (Saudia Airlines) ، شركة كوكاكولا (Coca-Cola)،شركة فولكس فاجن (Volkswagen) ،شركة إل جي (LG) ،وفي الجزائر شركة سونطراك أيضا تستخدم هذا البرنامج ومن خلال تطبيق فرعي mySAP ERP Financials لمالية والمحاسبة و المحاسبة الإدارية ،الذي يساعد وظائف المحاسبة المالية المستخدمين على الامتثال للمعايير الدولية مثل GAAP ومعايير التقارير المالية الدولية (IFRS).

2-1- التعريف ببرنامج SAP :

سوف يتم استعراض الواجهة الرئيسية للبرنامج أولا ،وكذا واجهة إدخال المعلومات الشخصية للمهني ،ثم يتم عرض الواجهة التي من خلالها يتم ذهاب إلى تطبيقات الفرعية :

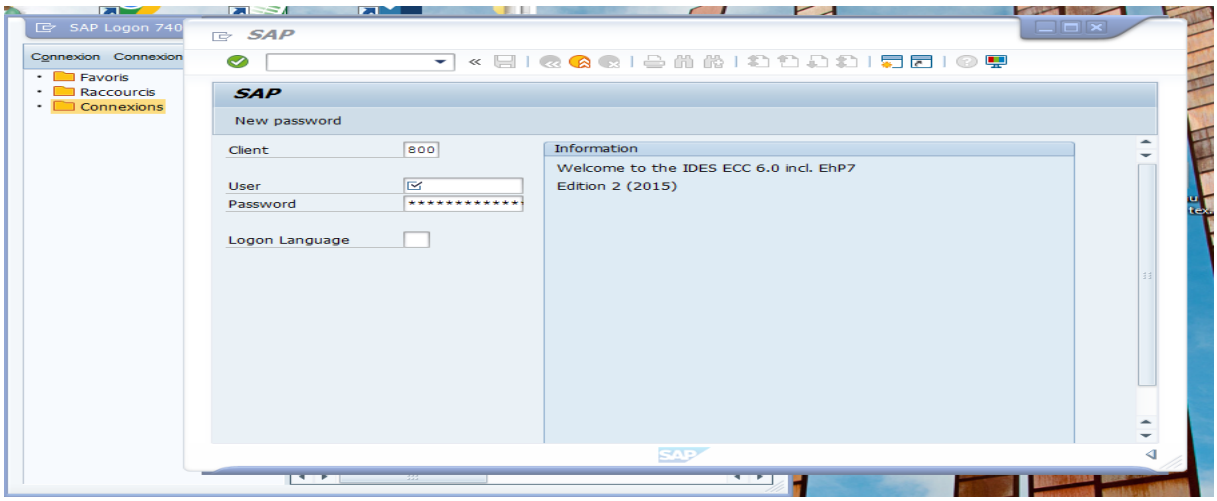
الشكل رقم(13): يوضح واجهة دخول برنامج SAP



المصدر: من إعداد الطالبان بإعتماد على برنامج SAP (2014)

نلاحظ من خلال الشكل أعلاه واجهة الدخول المستخدم إلى برنامج SAP ،والتي يتم من خلالها المستخدم الدخول إلى حسابه الخاص.

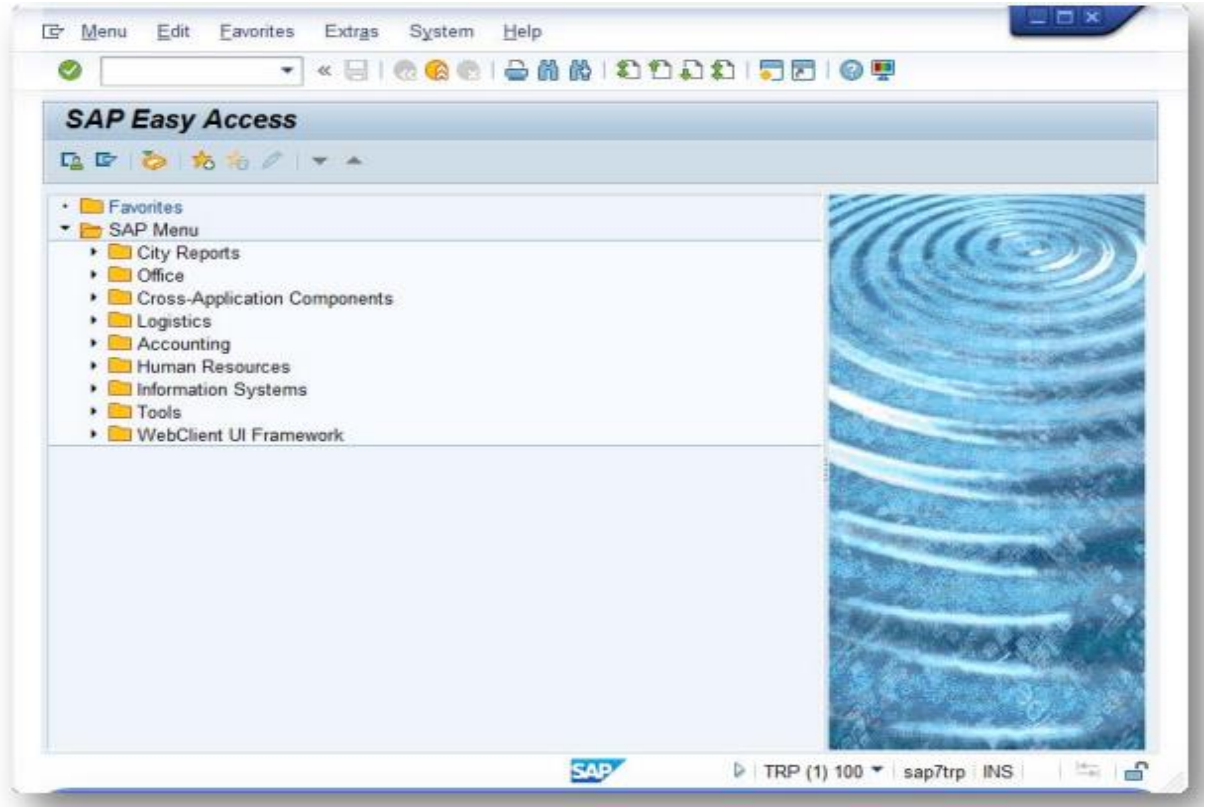
الشكل رقم(14) : يوضح واجهة إدخال الرقم السري الخاص بالمهني



المصدر: من إعداد الطالبان باعتماد على برنامج SAP (2014)

يتضح من خلال الشكل السابق واجهة إدخال اسم المستخدم والرقم السري الخاص بالمهني والذي من خلالهم يتم الدخول إلى برنامج الرئيسي.

الشكل رقم (15) : يوضح واجهة استخدام الرئيسية للبرنامج وتطبيقات الفرعية



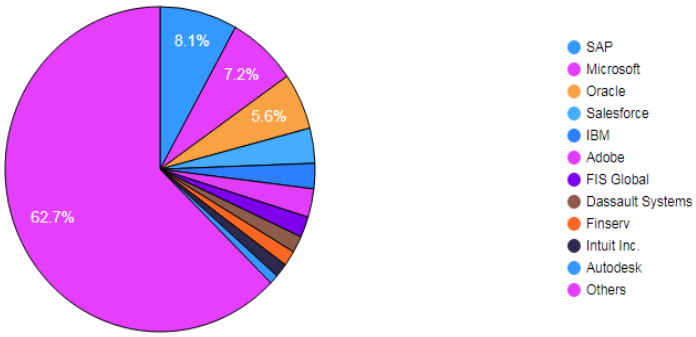
المصدر: من إعداد الطالبان باعتماد على برنامج SAP (2014)

نلاحظ في الشكل أعلاه واجهة ذهاب إلى تطبيقات الفرعية لبرنامج SAP ، كبرامج الخاصة بجانب المالي والمحاسبي أو الخاصة بموارد البشرية والزبائن .....

2-2- مكانة السوقية لبرنامجي Oracle E-Busines وSAP في العالم:

تشكل البرامج الحاسوبية جزءًا أساسيًا من حياتنا اليومية وعالم المال والأعمال ،وتتنوع هذه البرامج في مجالات مختلفة مثل أنظمة التشغيل وحزم البرامج والتطبيقات الخاصة بإدارة الموارد والتصميم وإدارة قواعد البيانات ،بحيث يوضح الشكل التالي أهم هذه البرامج التي تحظى بشعبية هائلة وتسيطر على حصة كبيرة من السوق على مستوى العالم:

الشكل رقم(16) :يوضح حصة السوقية لبرامج المؤسسات



المصدر: /https://www.infoclutch.com/installed-base/enterprise-application/oracle-e-business

ومن خلال الشكل أعلاه نلاحظ سيطرت برنامج SAP على قائمة البرامج أكثر حصة سوقية في العالم ،حيث يحظى هذا البرنامج بتواجد قوي في الشركات والمؤسسات الكبيرة حول العالم مثل ما تم ذكره سابقا ،وهذا راجع لقدرتها على تكامل العمليات المختلفة داخل المؤسسات وتوفير نظرة شاملة وموحدة للبيانات والعمليات التجارية.

كما يعزز نظام SAP ERP الكفاءة والفعالية في إدارة الموارد المالية وإدارة سلسلة التوريد وإدارة المخزون وإدارة المبيعات والتسويق والموارد البشرية والعديد من المجالات الأخرى....

ويوفر نظام SAP ERP مجموعة شاملة من التقارير والأدوات التحليلية التي تساعد المديرين التنفيذيين على اتخاذ قرارات استراتيجية مستنيرة والتحكم في أداء الشركة بشكل فعال.

أيضا بالنسبة لبرنامج Oracle E-Busines فهو يحتل مرتبة الثالثة وهذا نظير مميزات التي يقدمها التي تساعد في إدارة الموارد المؤسسات على تحسين كفاءتها وفاعليتها في العمليات وتحقيق التكامل بين مختلف وحدات العمل والأقسام المختلفة.

3- برنامج Odoo :

يمثل نظام أودو odoo واحدًا من نظم تخطيط الموارد الهامة للمؤسسات ، فهو يتيح مجموعة أدوات متكاملة للمساعدة في أداء أعمال شركات، كما يوفّر البرنامج حلولًا رقمية لأصحاب الأعمال من أجل تسهيل عملية التوسع ،ويتميز برنامج أودو بكونه مفتوح المصدر الأمر الذي ساهم في تطويره، إذ تمكنت الشركة من الاستفادة من خبرات أصحاب الأعمال، إضافةً إلى آلاف المطورين للوصول لنسخة متكاملة من النظام.

3-1- التعريف ببرنامج Odoo:

سوف يتم إستعراض الواجهة الرئيسية للبرنامج odoo:

الشكل رقم (17) : يمثل الواجهة الرئيسية لبرنامج **Odoo**

المصدر: https://www.cybrosys.com/odoo/odoo-books/odoo-15-studio/user-interface/

من خلال الشكل أعلاه تتضح الواجهة الرئيسية لبرنامج Odoo وتطبيقات الفرعية التابعة له كبرامج الخاصة بجانب المالي أو المبيعات أو الزبائن والجودة.....

رابعا: كيفيات ومنهجيات الاختراق المستخدمة:

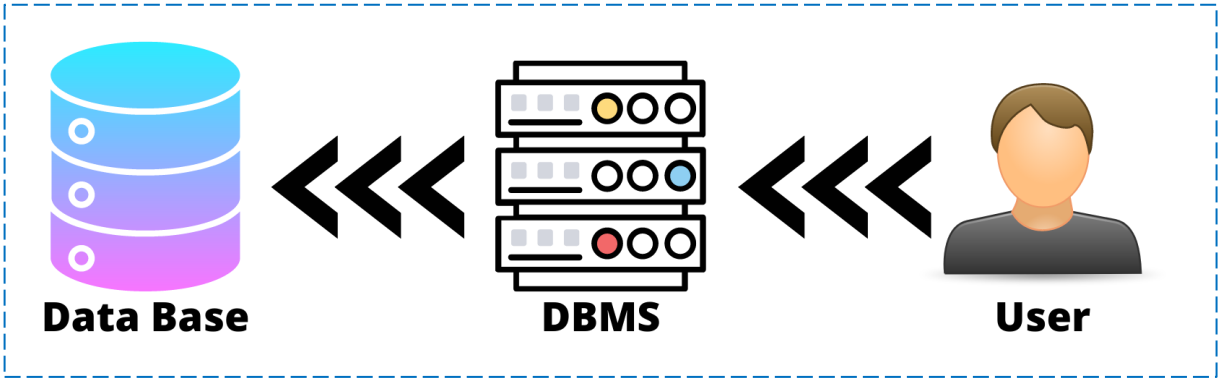
في عصر الاتصالات الرقمية والتكنولوجيا الحديثة، أصبحت الاختراقات والتجاوزات الإلكترونية ظاهرة شائعة ومستمرة ،وأصبحت تشكل تهديدًا خطيرًا على الأمان السيبراني والخصوصية الشخصية، حيث يمكن أن تؤدي إلى تسريب المعلومات السرية والحساسة، والتلاعب بالبيانات، وتعطيل الأنظمة، وسرقة الهوية، والقرصنة المالية، والتشويش الإلكتروني.

تعتمد هذه الاختراقات والتجاوزات على الثغرات في أنظمة الأمان والبرمجيات والشبكات، وقد تتم بواسطة قراصنة الإنترنت، والمجرمين السيبرانيين ،والمتسللين ،والمستخدمين غير قانونين.

لهذا من خلال هذا العنصر سوف نتطرق إلى أهم منهجيات وأساليب الشائعة والمستخدمة من طرف مجرمي الإنترنت:

- **SQL injection attack**: كما تم ذكره سابقا هو هجوم يستخدمه الهاكر يستهدف من خلاله ثغرة أمنية في قاعدة البيانات لتعديل البيانات داخل هذه أخيرة مما يسمح بوجود تغيرات واضطرابات مستمرة داخل النظام أي يصبح هذا الهاكر يتعامل مباشرة مع DBMS ،الشكل التالي يوضح هذه العملية:

الشكل رقم (18) : يوضح ألية سير نقل البيانات بين User وData Base



المصدر: من إعداد الطالبان بناءا على مكتسبات القبلية لطالبين.

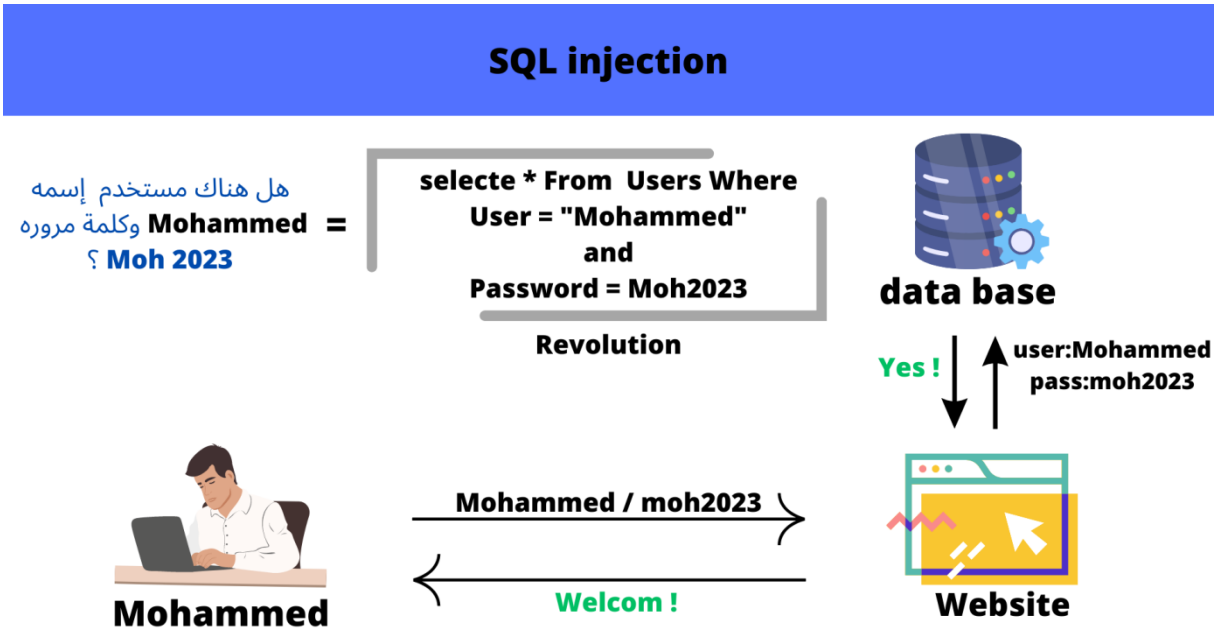
من خلال هذا الشكل يمكننا القول أن شرط أساسي لحماية قاعدة البيانات أن لا يتعامل User مع DBMS لأنه في حالة تعامله مع DBMS سوف يمكنه من استخدام صلاحيات Data Base ،وتكون هذه العملية من خلال عمل filter لمنع User من تعامل بصفة مباشرة DBMS.

هذه الثغرة يقوم المخترق باستغراق ضعف بتدقيق البيانات التي تأخذ من زوار الصفحة ويحاول التواصل بشكل مباشر مع Data base.

لهذا سوف نقوم بمثال توضيحي من أجل شرح بشكل أكثر وضوح وتفصيل:

نفترض أن هناك User اسمه Mohammed وكلمة سره Moh2023 ،هذا المستخدم يحاول الدخول إلى الموقع والذي قام بإدخال بياناته الشخصية ،فالموقع سوف يتحقق من بيانات المدخلة من قبل User ، الموقع سوف يسأل هل هناك مستخدم بهذا إسم وهل هذه كلمة مروره ؟ ،وهذا سؤالين سوف يتم طرحهم عبر لغة SQL من خلال الجدول الموضح في الشكل ، وسوف ترد Data base على سؤالين المطروحين بشكل إيجابي وتسمح ل User بدخول ،ويمكن تلخيص ما سبق في الشكل التالي:

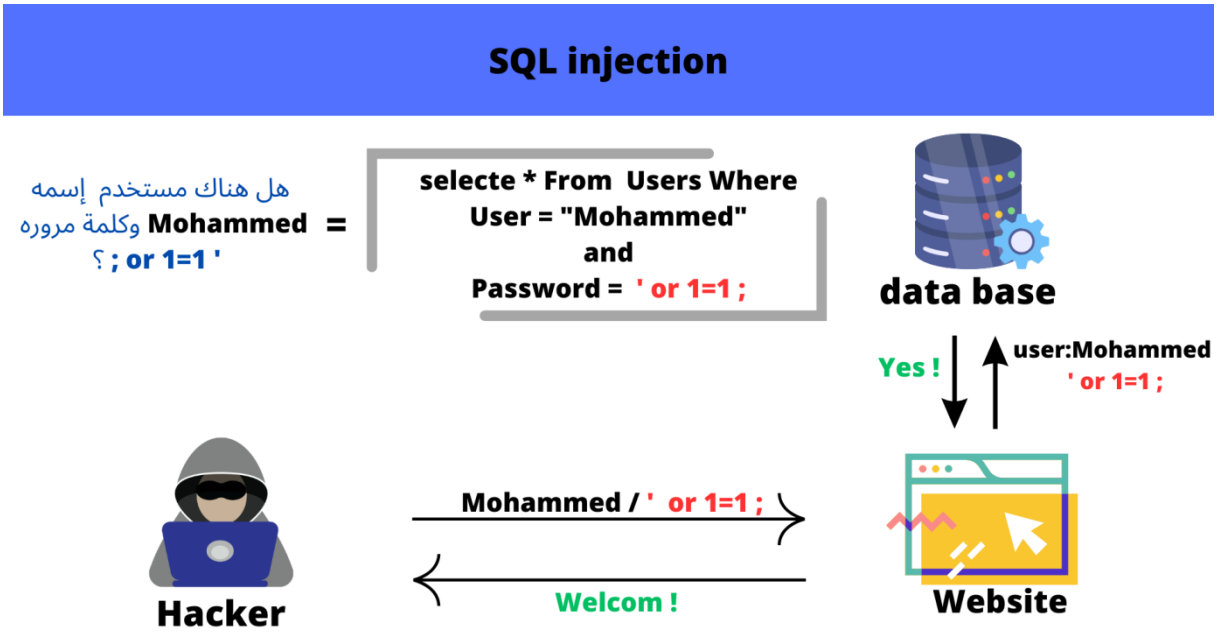
الشكل رقم(19) : يوضح عملية دخول مستخدم للموقع



المصدر: من إعداد الطالبان بناءا على مكتسبات القبلية لطالبين.

لكن هذه في حالة دخول User عادي ،أما بالنسبة لمحاولة Hacker الدخول إلى الموقع فسوف يقوم بإدخال User Nameبشكل عادي والممثل في مثالنا في Mohammed لكن بالنسبة لكلمة المرور لن يدخل كلمة مرور لأنه لا يعرفها سوف يدخل SQL Statement والممثلة في أمر التالي ; ' Or 1=1 في هذا الحالة الموقع سوف يسأل Data baseمن خلال لغة SQL من خلال الجدول الموضح في الشكل سوف ترد Data base على سؤالين المطروحين بشكل إيجابي وتسمح ل Hacker بدخول ،ويمكن تلخيص ما سبق في الشكل التالي:

الشكل رقم(20) : يوضح عملية دخول هاكر للموقع



المصدر: من إعداد الطالبان بناءا على مكتسبات القبلية لطالبين.

✧ **رفض خدمة الموزع "Distributed denial of service (DDOS)":**

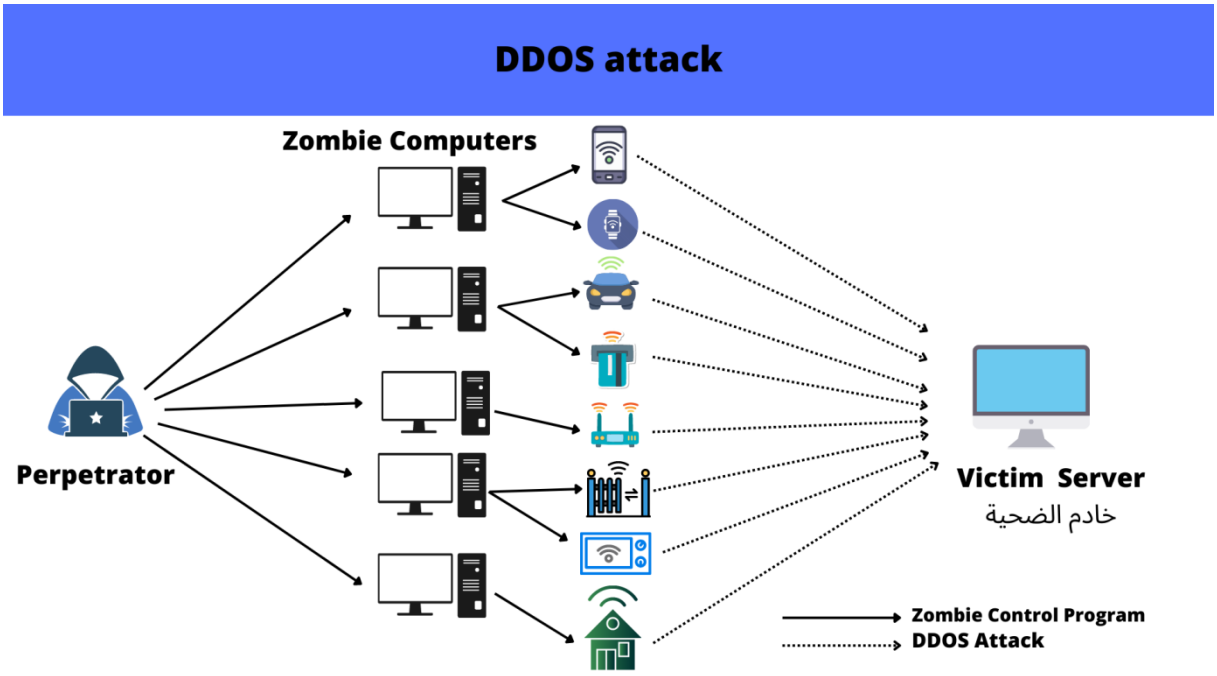
هجمات DDoS (توزيع الخدمة المرفوضة) هي نوع من هجمات الإنترنت التي تستهدف تعطيل خدمة تعمل هذه الهجمات على إغراق مصادر الموارد لدي الخادم أو الشبكة المستهدفة، مما يتسبب في تعطيلها وجعلها غير قادرة على تقديم الخدمة للمستخدمين .

تتم هجمات DDoS عن طريق التحكم في شبكة كبيرة من الأجهزة المخترقة المعروفة بـ "(botnet)"، هذه الأجهزة المخترقة تُصاب ببرامج ضارة خاصة تجعلها تنضم إلى الشبكة وتتبع أوامر المهاجم. عند تنفيذ الهجوم، يتم توجيه حركة المرور المفرطة من هذه الأجهزة المخترقة نحو الهدف المستهدف، مما يسبب ضغطًا هائلاً على موارد الخادم ويتسبب في تعطيله.

تستخدم هجمات DDoS كوسيلة لتعطيل الخدمات عبر الإنترنت والمواقع الشخصية وخوادم الألعاب والشبكات الكبيرة. يهدف المهاجمون إلى إلحاق الضرر الاقتصادي بالمؤسسات أو إثارة الفوضى عبر الإنترنت أو تنفيذ عمليات احتيالية ،كما يمكن استخدام هجمات DDoS كوسيلة لتحويل الانتباه عن الهجمات الأخرى التي يتم تنفيذها في الخلفية.

وكل ما سبق يمكن تلخيصه في الشكل التالي :

الشكل رقم(21) : يوضح هجمات DDOS



المصدر: من إعداد الطالبان باعتماد على **James Hall** ، مرجع سبق ذكره ،ص:538.

هذا الشكل يراعي تطورة الحديثة الذي وصلت له تكنولوجيا المعلومات IT ، لان الهجمات أيضا في تطور مماثل لم وصلت إليه التكنولوجيا ،فهجمات الحالية أصبح المخترقين يستطيعون ضم كل أشياء المرتبطة بالإنترنت وهو نظير ثورة "IOT" Internet of Thing .

خامسا: الأمن السيبراني "تحديات وحلول ":

يواجه الأمن السيبراني تحديات مستمرة نتيجة للتطورات التكنولوجية والتهديدات المتطورة التي تستهدف الأنظمة والبيانات الحساسة. من خلال الجدول التالي نلخص أهم التحديات وحلول الممكنة لها:

الجدول رقم(32) : يوضح أهم "تحديات وحلول" أمن السيبراني

التحديات / المشاكل	الحلول الممكنة
تطور الهجمات السيبرانية	حماية والوعي من أهم الهجمات التي يمكن أن نتعرض لها
اتساع نطاق وصعوبة	تخطيط حسب موارد متاحة وترتيب الأولويات
نقص المواهب والمهارات	التدريب والتعليم
تكلفة والاستثمار	تحسين الأنظمة وابتكار
الثقافة	نشر الوعي

المصدر : من إعداد الطالبان باعتماد على سيف حطاب و مراد بوعاش.

سادسا: الأمن السيبراني والذكاء الاصطناعي " أفاق مستقبلية" :

أدت الثورة الحالية في مجال تكنولوجيا المعلومات **IT** إلى بناء توقعات مستقبلية في مجال الذكاء الاصطناعي والأمن السيبراني وما سوف يحمله مستقبليهما ،والتي سوف تؤدي إلى تغير العالم وهذا من خلال ظهور تكنولوجيات جديدة لم يتصور العقل البشري الوصول إليها ،لهذا من خلال هذا العنصر سوف يتم تقديم أهم التوقعات المستقبلية المتداولة في مجالي **AI** و **Syber Security**.

◄ **تطور الذكاء الاصطناعي الخارق "Super Artificial Intelligence"** : سيشهد الذكاء الاصطناعي تطورًا كبيرًا في القدرة على فهم وتفسير البيانات والمعلومات. ستصبح الأنظمة الذكية قادرة على التعلم والتكيف بشكل أفضل مع تغيرات البيئة والظروف المتغيرة ،سوف يكون لدينا ذكاء اصطناعي قوي بشكل لا يصدق سيكون قادرا على فعل كل ما يستطيع العقل البشري القيام به وربما سوف يتفوق عليه.[1]

◄ **التطور في مجال التعلم العميق "Deep learning"**: سيؤدي التركيز المستمر على التعلم العميق إلى تطور قدرات الذكاء الاصطناعي في مجالات مثل التعرف على الصوت والصورة واللغة الطبيعية. ستزداد دقة وفعالية النظم الذكية في التعامل مع البيانات المعقدة وفهمها.

[1] بيل غيتس ، **لقد بدأ عصر الذكاء الإصطناعي** ، ترجمة، طاهر أبو العيد ،ص:10.

* **سيف حطاب** : خبير في الأمن السيبراني.

* **مراد بوعاش** : خبير في الذكاء الإصطناعي. https://www.facebook.com/moubachirsv/videos/3144572159166220/ ، تم إطلاع عليه في 2023/02/23، 18:00.

- **التطور في مجال الروبوتات الذكية**: ستشهد الروبوتات الذكية تقدمًا كبيرًا في القدرة على التفاعل والتعاون مع البشر. ستصبح الروبوتات قادرة على تنفيذ مهام متعددة والتفاعل مع البيئة المحيطة بشكل أكثر ذكاءً.
- **إتساع في نطاق الأتمتة** : تعتبر التقنيات الحديثة مثل الذكاء الاصطناعي AI والتعلم الآلي Machine learning والروبوتات robotics وإنترنت الأشياء IOT من العوامل التي ستدفع إلى مزيد من الأتمتة في مختلف الصناعات والقطاعات.

من المتوقع أن يؤدي التطور التكنولوجي إلى تحسين كفاءة العمليات وتقليل الأخطاء البشرية ،مما يؤدي إلى زيادة الإنتاجية وتحسين جودة المنتجات والخدمات ،قد تشهد الشركات والمؤسسات تبني نظم أتمتة شاملة تغطي مختلف جوانب العمل ،بدءًا من إدارة الموارد البشرية وحتى إدارة سلسلة التوريد والتسويق والمالية.

قد يتم استخدام الذكاء الاصطناعي والتعلم الآلي لتحليل البيانات الضخمة "BIG DATA" واستخلاص الأنماط والتوجيهات، مما يساعد في اتخاذ قرارات استراتيجية أكثر ذكاءً وتنبؤًا ،قد تشهد الروبوتات والأتمتة الذكية استخدامًا أكبر في مجالات مثل التصنيع والخدمات اللوجستية والصحة والزراعة وغيرها ،حيث يمكن للآلات تنفيذ المهام بدقة وكفاءة عالية.

على الرغم من الفوائد المتوقعة لأتمتة العمليات ،فقد ينشأ أيضًا تحديات جديدة مثل مشاكل الأمان والخصوصية والقضايا الأخلاقية المرتبطة بتطبيقات الذكاء الاصطناعي واستخدام البيانات الضخمة ،ستكون هناك حاجة إلى إطار قانوني وتنظيمي يضمن حماية المستهلكين والموظفين والبيانات المستخدمة في عمليات الأتمتة.

بشكل عام، من المتوقع أن تستمر أتمتة العمليات في التطور والتوسع في المستقبل ،مع تحسين الأداء وتوفير فرص جديدة للابتكار والنمو في الأعمال والصناعات المختلفة.

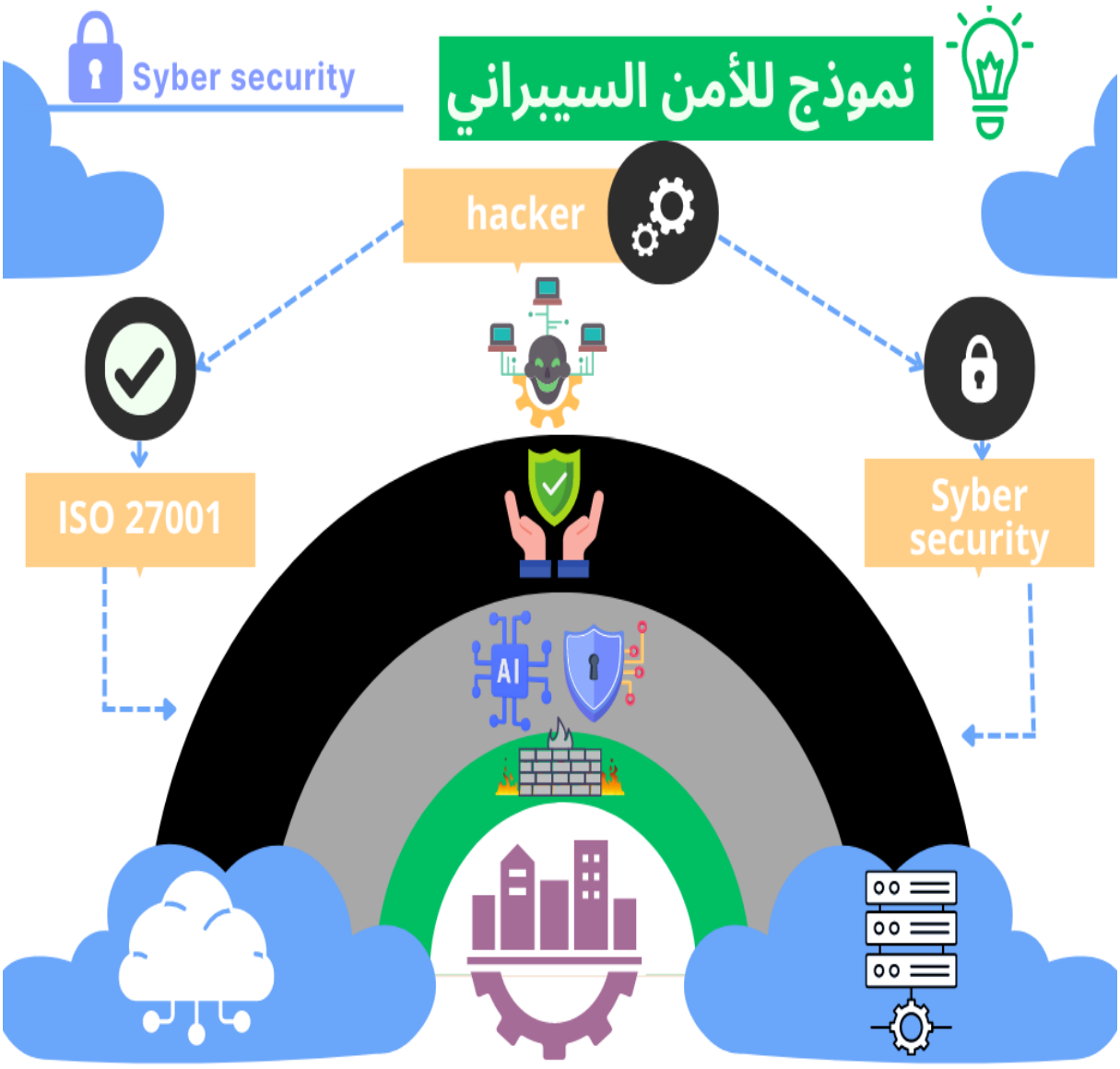
- **التحسينات في الأمن السيبراني"Syber security"**: سيصبح الأمن السيبراني أكثر أهمية مع تزايد تبادل البيانات والمعلومات عبر الإنترنت للتعرف على السلوك الاختراقي ومكافحته من خلال إمكانية ظهور ذكاء السيبراني وتفعيل دور الهاكر الأخلاقي Ethical hacke ،ستزداد أهمية الحماية السيبرانية في مجالات حيوية مثل الرعاية الصحية والنقل والطاقة والصناعة.

بشكل عام، فإن التوجهات المستقبلية للذكاء الاصطناعي والأمن السيبراني تهدف إلى تعزيز القدرة على التعامل مع التحديات الرقمية المعقدة وحماية الأنظمة والشبكات الحيوية من الهجمات السيبرانية ،سيكون للتكنولوجيا الذكية والابتكار دور كبير في تحقيق هذه الأفاق المستقبلية وتعزيز الأمان والحماية الرقمية.

أنموذج للأمن السيبراني:

من خلال درستنا لموضوع أردنا تقديم نموذج للأمن السيبراني الذي يمكن من خلاله ضمان الأمان والحماية ، وهو كالتالي :

الشكل رقم22: أنموذج للأمن السيبراني



المصدر : من إعداد الطالبين بناءا على ما سبق ذكره

الشكل رقم 23: يوضح رموز نموذج الأمن السيبراني

المصدر : من إعداد الطالبين بناءا على ما سبق ذكره

خلاصة الفصل :

وعلى ضوء ما سبق اتضح لنا أن مؤسسة نفطال فرع غرداية تحاول أن تتماشى مع متطلبات تكنولوجيا المعلومات والاتصال الحديثة وهذا من خلال إتباع إجراءات وتطبيق سياسات بهذا الصدد ومن بينها اعتماد نظام SD COM نظاما للمعلومات وتخلي عن نظام Naftal Com الذي من خلال تم معالجة نقاط ضعف نظام السابق من خلال ميزات مكتسبة نظام الجديد المطبق ،بإضافة إلى إتباع بعض الإجراءات التي هدف منها محاولة تحقيق أقصى قدر من الحماية لمعلوماتها.

ومن خلال هذا الفصل تم التعرف على واقع نظام المعلومات في مؤسسة نفطال وهذا من خلال المقابلة التي أجريت مع القائمين على المؤسسة ،وكذا معرفة مدى قدرت أنظمة الحماية الموجودة على مستوى مؤسسة محل الدراسة على مجابهة كل أنواع اختراقات والتجاوزات إلكترونية ،أيضا تم تسليط الضوء على وضع أمن السيبراني على مستوى العالم والجزائر ،وتم تقديم نموذج مقترح لأمن نظم معلومات يمكن من خلاله وقاية من الجرائم إلكترونية.

“

خاتمة عامة

”

خاتمة:

حاولنا من خلال تناولنا لهذا الموضوع والموسوم ب" متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في مؤسسات الاقتصادية الجزائرية ،معالجة إشكالية البحث التي تتمحور حول أهم متطلبات الأمن السيبراني الواجب توفرها لحماية أنظمة المعلومات المحاسبية من مخاطر التي تواجهها في ظل تكنولوجيا المعلومات والاتصال وقد تدعم هذا البحث بدراسة تطبيقية على مؤسسة نفطال فرع غرداية ،الذي سعينا من خلاله إلى إسقاط أهم الجوانب نظرية المذكورة على جانب تطبيقي.

تطرقنا في الفصل الأول إلى ماهية أنظمة المعلومات المحاسبية والتعرف على معلومات والخصائص الوجب توفرها في عصر السرعة ،وبعد هذا ركزنا على أهم المخاطر التي تواجهها نظم المعلومات المحاسبية ،وصولا إلى التركيز على الأمن السيبراني لحماية هذه الأخيرة مع تقديم بعض الدراسات السابقة التي تناولت الموضوع من أجل تدعيم وتأكيد ما تم ذكه سابقا.

وقد تناولنا خلال الفصل الثاني دراسة حالة لمؤسسة نفطال من خلال إلقاء نظرة على واقع نظم المعلومات المحاسبية في هذه المؤسسة ابتداء بإلقاء لمحة على تاريخ المؤسسة وهيكلها التنظيمي وصولا إلى نظام المعلومات المطبق لديها والمتمثل في برنامج SD COM ،حيث تم شرح جميع المراحل التي يمر بها النظام (المدخلات – المعالجة – المخرجات) ، كما تم إجراء مقابلة مع القائمين على نظم المعلومات لمعرفة مدى كفاءة ودرجة حماية هذه الأخيرة ،وسلطنا الضوء على واقع أمن السيبراني على مستوى الدولي والمحلي كما تم تقديم مقترح لأمن نظم المعلومات بتركيز على ثورة الذكاء الصناعي وما هو قادم.

أولا : نتائج اختبار الفرضيات الدراسة:

انطلاقا من طريقة المعالجة التي تم اعتمادها ،والتي جمعت بين الدراسة النظرية من جهة ،والدراسة التطبيقية من جهة أخرى ،تم التوصل أثناء اختبارنا للفرضيات إلى النتائج التالية :

ف1: بخصوص الفرضية الأولى والتي مضمونها يُعرب بأن أهم متطلبات تطبيق الأمن السيبراني لأنظمة المعلومات المحاسبية في المؤسسات الاقتصادية الجزائرية هي توفر أدوات وأنظمة الأمان والحماية وممثلة في نظم التشغيل والشبكات الحاسوبية المتطورة والتطبيقات المختلفة التابعة لها ،اتضح لنا من خلال دراسة النظرية والتطبيقية وخاصة من خلال دراسة حالة لمؤسسة نفطال أن الأمن السيبراني يتطلب مجموعة الموارد والتي من بينها أنظمة التشغيل والشبكات الحاسوبية المتطورة من أجل ضمان أمان والحماية السيبرانية.

ف2: فيما يخص الفرضية الثانية ولتي مفادها أن "نظام المعلومات يعتبر أحد أهم الأنظمة الفرعية الموجودة داخل المؤسسة ،بحيث يتمثل دوره في إنتاج المعلومات التي تعكس الواقع الاقتصادي من أجل توفيرها للأطراف ذوي العلاقة والتي على ضوئها يتخذ قرارات ،فقد اتضح أن هذه الفرضية صحيحة حيث أن هذا نظام المعلومات يقوم بتسجيل مدخلات النظام كالبيانات المحاسبية والمعبرة عن أحداث الاقتصادية ويقوم بمعالجتها عن طريق تبويبها وتلخيصها وتحليلها وعرض نتائجها كمخرجات لنظام ممثلة في مختلف التقارير والقوائم المالية.

ف3: اما بالنسبة للفرضية الثالثة والمتعلقة بأساسيات الأمن السيبراني لأمن نظم المعلومات ممثلة في مجموعة من الإجراءات التي تهدف لمحافظة على سرية المعلومات الإلكترونية ، تبين أن هذه الفرضية صحيحة ،فقد تعرفنا من خلال جانب النظري على أهم هذه الإجراءات والتي هدفها حماية المعلومات الإلكترونية.

ف4: فيما يتعلق بالفرضية الرابعة التي تنص على أن نظام المعلومات المحاسبي يواجه العديد من المخاطر نتيجة استخدامه وسائل تكنولوجيا المعلومات والاتصال والتي يتم مواجهتها بواسطة أدوات الحماية والرقابة المتعلقة بأمن السيبراني ،وهذه الفرضية صحيحة حيث تم شرح أهم المخاطر التي تواجه المؤسسات ،وكذا الحلول الممكنة لمجابهتها وهذا من خلال الجانب النظري والتطبيقي معا.

ف5: أما بشأن الفرضية الأخيرة والتي افترضت أن مؤسسة نفطال – غرداية – تتعامل مع المخاطر السيبرانية بمجموعة من سياسات الأمان والحماية لأنظمة المعلومات المطبقة على مستوى المؤسسة ،ونستخلص من خلال

دراسة التطبيقية أن هذه الفرضية صحيحة بحيث ،ومنذ سنة 2020 التي تعرضت فيها مؤسسة لاختراق اتخذت المؤسسة مجموعة من إجراءات الحازمة بهذا الشأن والموضحة سابقا في جانب التطبيقي.

ثانيا : النتائج العامة للدراسة :

من خلال الدراسة التطبيقية توصلنا إلى النتائج التالية :

- ✯ يمتاز نظام SD COM والتي كانت بداية تطبيقه سنة 2018 بعدة ميزات استفادة منها المؤسسة والتي من أهمها : ضمان الحماية للمعلومات ،بحيث يرى القائمين على هذا النظام من خلال المقابلة الذي تم إجراءها أن نظام يتميز بدرجة حماية عالية وأنه يرقى إلى أن يكون نظام معلومات متكامل حسب ما تم رؤيته منذ تطبيقه.
- ✯ تهدف مؤسسة محل الدراسة إلى وضع مخططات مستقبلية لمواكبة تكنولوجيا الحديثة كاستخدام الروبوتات والذكاء الاصطناعي ومتطلبات التحولات الرقمية بهدف تحسين أداء المهام ورفع من جودة الخدمات المقدمة.
- ✯ تمتلك مؤسسة نفطال خوادم إلكترونية تخزن فيها معلوماتها وبياناتها وهذا ما يسمح لها بالتحكم الكامل في معلوماتها.
- ✯ المؤسسة معرضة للمخاطر السيبرانية لوجود بعض نقاط الضعف وخاصة بالنسبة لفروع التابعين للمؤسسة التي تسعى لمعالجتها ،والتي منها: نقص الثقافة السيبرانية لدى العاملين بالمؤسسة ،عدم وجود أجهزة وأنظمة حماية متطورة بسب عدم تخصيص موارد مالية لاقتنائها أو لتكلفتها العالية.
- ✯ اتضح لنا أن هناك جهود حالية اتخذتها المؤسسة محل الدراسة في مجال الأمان والحماية السيبرانية وخاصة بالنسبة للقطاع الاستراتيجي الذي تشتغل فيه لحماية معلوماتها و أصولها ومن بينها: شراء أنظمة حماية Kaspersky ،أيضا التركيز على تكوينات تمتاز بمستويات عالية في مجال الأمن والحماية ،وإرسال مهندسي أو تقنين الإعلام ألي إلى خارج البلاد ، شراء بعض الأجهزة متطورة بخصوص هذا الأمر ،لكن هذا غير كافي بالنسبة لمؤسسة مثل مؤسسة نفطال.
- ✯ من خلال استعرضنا لوضع الجزائر في مؤشر GCI العالمي للأمن الإلكتروني ،نرى أن الأمن السيبراني في الجزائر متأخر كثيرا.

- استخلصنا ان الجزائر تحاول تماشي مع تغيرات تكنولوجيا المعلومات ولاتصال الحديثة وهذا من خلال قانون رقم 04/09 الصادر سنة 2009 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ،لكن هذا لم يلبي التغيرات والتطورات الذكاء الاصطناعي الخارق S AI ، أنترنت الأشياء IOT ،والواقع الافتراضي VR.
- بمثل ما رأيناه في الجانب التطبيقي للاتجاهات المستقبلية للأمن السيبراني والذكاء الاصطناعي ،فقد استخلصنا أن هناك عدة تغيرات سوف تحدث وخاصة في حالة وصول Super Artificial Intelligence الذي سوف يمكن المؤسسات من توقع حدوث المشكل أو الخطر قبل حدوثه أو إيجاد حل له وهذا من خلال الذكاء السيبراني الذي سوف يصل إلى مراحل لم يكن توقع الوصول إليها.

ثالثا: اقتراحات الدراسة :

من خلال النتائج المتوصل إليها يمكننا صياغة الاقتراحات التالية والتي موجهة للمؤسسة محل الدراسة من جهة وموجه للدولة ومؤسسات الاقتصادية أخرى من جهة أخرى :

- ينبغي على مؤسسات الاقتصادية الجزائرية مواكبة التطورات الحديثة لتكنولوجيات المبتكرة والتحولات الرقمية وخاصة المتعلقة بالذكاء الاصطناعي ،الأمن السيبراني ،الانترنت الأشياء ،الواقع الافتراضي ....،وهذا من خلال المؤتمرات والأبحاث والندوات الدولية أو المحلية ،ومتابعة مستجدات الجديدة للمخاطر تكنولوجيا المعلومات والاتصال بغرض اتخاذ الإجراءات المناسبة له.
- يجب على المؤسسات الاقتصادية الجزائرية فهم الجيد لبيئة تكنولوجيا المعلومات وكل شيء مربوط بها ،وأن تضع خطط رقابية تتميز بتحديث مباشر لتغيرات الداخلية والخارجية لتفادي المخاطر المرتبطة بها في ضوء إصدارات ومعايير المنظمات الدولية.
- من مستحسن على مؤسسة نفطال تعجيل في خطط المستقبلية الموضوعة لمواكبة تكنولوجيات الحديثة وهذا بتخصيص الموارد المالية اللازمة لها.
- يتوجب على مؤسسة نفطال تلافي نفاط الضعف الموجودة على مستوى المؤسسة من خلال شراء أنظمة أمان وحماية متطورة ،ونشر الثقافة السيبرانية للعاملين على مستوى المؤسسة والفروع التابعة لها من خلال استثمار في التدريب والتعليم.

- نقترح على مؤسسة نفطال الاستعانة بخبراء سيبرانين خارجين لأجل تقييم النظام المطبق وتقديم اقتراحات أمنية ووقائية.
- وجب على مؤسسة نفطال تفعيل أدوات وإجراءات التي من ممكن استخدامها للحد من مخاطر السيبرانية ،ونذكر منها: الجدران النارية ،تشفير البيانات ،النسخ الاحتياطي ،البرمجيات المضادة للاعتداء إلكتروني .
- يجدر بأصحاب القرار أما على مستوى مؤسسات الاقتصادية أو على مستوى الدولة جعل الأمن والحماية أولويًا وليس اختياريا من خلال تطوير استراتيجيات شاملة أمنية ،وكذا جعله في بداية العمل وليس في نهاية العمل مع تشجيع التفكير الإبداعي والابتكار للكفاءات الموجودة في المؤسسات الاقتصادية الجزائرية.
- من الضروري التركيز على البحث والتطوير في تقنيات وأساليب حماية الأمنية من خلال تفعيل مراكز البحث والتطوير ،وكذا تنظيم أحداث وملتقيات مع أكاديميين ومختصين أصحاب الحلول لحل المشاكل التي تواجهها المؤسسات.
- نقترح أيضا توفير مكاتب وأشخاص مؤهلين يقدمون استشارات لمؤسسات في مجال الأمن السيبراني ،وكذا وجب جلب مختصين من دول أخرى لتبادل الآراء وأفكار.
- يتوجب تفعيل دور **The White hacker** لاكتشاف أهم الثغرات والعيوب الموجودة في أنظمة المؤسسات من أجل وضع أنظمة دفاع استباقية تقدم إنذار مبكرا قبل تعمق ووجود اختراق في نظام.
- من الواجب على المشرع الجزائري مراعاة تطورات وتغيرات تكنولوجية بإصدار قوانين ووضع خطط واستراتيجيات تراعي تكنولوجيات الحديثة.

رابعا : أفاق الدراسة :

حاولنا من خلال هذه الدراسة الإلمام بجوانب الموضوع النظرية والميدانية قدر الامكان، ومن أجل مواصلة البحث في هذا الموضوع نقترح بعض المواضيع كأفاق مستقبلية للدراسة ومن أهمها:

- دور **ISO 27001** في تعزيز أمن السيبراني في المؤسسات الاقتصادية الجزائرية.
- مدى استخدام أنظمة الإنذار المبكر في المؤسسات الاقتصادية الجزائرية من أجل تحقيق الأمن السيبراني.
- الأمن المالي السيبراني ودوره في الحد من الجرائم الإلكترونية.
- الأمن السيبراني كأداة لتطوير المؤسسات الاقتصادية الجزائرية.
- متطلبات تطبيق الذكاء السيبراني في مؤسسات الاقتصادية الجزائرية.

خاتمة عامة

- دور التوعية الاجتماعية في نشر الثقافة المالية السيبرانية.
- الذكاء المالي السيبراني ودوره في محاربة الاحتيالات المالية والمحاسبية.

“


المراجع

”

المراجع

أولا : المراجع بلغة العربية:

أ- الكتب :

1. جيهان عبد المعز الجمال، **المراجعة في البيئة الالكترونية** ، الطبعة الأولى ، دار الكتاب الجامعي ،الإمارات العربية المتحدة ،2014.
2. ريتشارد دول وأخرون ،**نظم المعلومات المحاسبية** ، ترجمة :نضال محمود الرمحي ، الطبعة الأولى ،دار الفكر ، الأردن ،2014.
3. زياد هاشم السقا ،**نظام المعلومات المحاسبي** ،الطبعة الثانية ،دار الطارق للنشر والتوزيع ،العراق ،2011.
4. عبد العزيز سيد مصطفى و ايناس مصطفي سليمان و ايمان عباس حلمي واخرون ، **أساسيات تكنولوجيا المعلومات تطبيقات محاسبية** ، كلية التجارة ،جامعة القاهرة ،مصر ، 2019.
5. عبد العزيز سيد مصطفى وأحمد السباعي قطب وعبد الحميد عبد المنعم منطاش وأخرون ،**نظم المعلومات المحاسبية مدخل تطبيقي عملي** ،كلية التجارة ،جامعة القاهرة ، مصر ،2019.
6. عطاالله أحمد الحسبان ،**نظم المعلومات المحاسبية** ،دار اليازوري العلمية لنشر والتوزيع ،الأردن ،2013.

ب – المقالات العلمية :

1. بن علية بن جدو ،**تحديات اللأمن السيبراني لمواجهة الجريمة الإلكترونية** ، المجلة الجزائرية للأمن الانساني ، المجلد :07 ،العدد:02، 2022.
2. بيل غيتس ، **لقد بدأ عصر الذكاء الإصطناعي** ، ترجمة، طاهر أبو العيد ،ص:10.
3. جوهر بنت عبد الرحمن إبراهيم المنيع ، **متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030** ،إدارة البحوث والنشر العلمي ،المجلد:38 ،العدد الأول ،مصر ،2022.
4. ربيع أحمد بن يحي ، **فعالية نظم المعلومات المحاسبية في ظل استخدام تكنولوجيا المعلومات** ،مجلة المحاسبة ،التدقيق والمالية ، عين الدفلى ، الجزائر ،المجلد:01 ،العدد:01 ، 2019,
5. عبد المالك زين وأخرون ، **أثر مخاطر نظام المعلومات المحاسبي على جودة المعلومات المحاسبية** ،مجلة روئ اقتصادية ، الوادي ،الجزائر ، المجلد : 09 ، العدد :02 ، 2019.
6. علي عبد الفاتح الشاهر وأخرون ،**تصميم نظام المعلومات المحاسبي بإستخدام برمجية (Excel /Ms)** ،مجلة تنمية الرافدين ،العراق ،المجلد :41 ،العدد:133، 2022.
7. نهاد محمد وهيب وأخرون ،**تقويم نظام المعلومات المحاسبي لشركة التمور العراقية** ،مجلة كلية مدينة العلم ،العراق ،المجلد:14 ،العدد: 02، 2022.
8. هدى يوسف محمد السليمان، **أثار استخدام تكنولوجيا المعلومات على نظم المعلومات المحاسبية** ،المجلة العربية لنشر العلمي ،الأردن،،المجلد: 05 ،العدد:50، 2022.
9. وفاء مطروح وأخرون ،**تداعيات جائحة كوفيد – 19 وتأثيرها على تحقيق الأمن السيبراني في الجزائر** ،المجلة الدولية للاتصال الاجتماعي ، المجلد:09 ،العدد:02 ،مستغانم ،2022.

ج – رسائل الماجستير وأطروحات الدكتوراه:

1. امجد يوسف إسماعيل ،**مخاطر نظم المعلومات المحاسبية الإلكترونية في الشركات المالية الأردنية** ،رسالة ماجستير في محاسبة والتمويل ،الأردن ،2011.
2. بوعزيز رضا ،**مساهمة نظام المعلومات المحاسبي الجيد في تسهيل مهمة محافظ الحسابات دراسة مجموعة من الشركات الجزائرية** ، أطروحة دكتوراه ،كلية العلوم الاقتصادية والتجارية وع التسيير ، جامعة الجزائر 3 ،الجزائر ، 2022/2021.
3. حرية شعبان محمد الشريف ،**مخاطر نظم المعلومات المحاسبية الإلكترونية** ،رسالة ماجستير في المحاسبة والتمويل ،كلية التجارة ،جامعة الإسلامية ،غزة ،2006.
4. حنين جميل أبو حسين ، **الإطار القانوني لخدمات الأمن السيبراني (دراسة مقارنة)**، ماجستير في قانون عام ، جامعة شرق الأوسط ، كلية الحقوق ،الأردن ، 2021.
5. زعابطة عبد اللطيف ، **أثر تكنولوجيا المعلومات على نظام المعلومات المحاسبي دراسة حالة شركات الاتصالات الجزائر – الأغواط –** ،أطروحة دكتوراه ، كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة غرداية ، الجزائر ، 2022/ 2021 .
6. زين عبد المالك ،**أثر تطبيق حوكمة الشركات على مخاطر نظام المعلومات المحاسبي دراسة ميدانية** ، أطروحة دكتوراه ،كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة علي لونيسي ،البليدة ،الجزائر ،2020/2019
7. فوضيل لحسن ،**دور نظام المعلومات المحاسبي في إدارة مخاطر البنوك –دراسة حالة البنوك التجارية–** ،أطروحة دكتوراه ، كلية العلوم الاقتصادية والتجارية وع التسيير ، جامعة حسيبة بن بوعلي ،الشلف ،2018.
8. ماهر فؤاد زهيري ، **مخاطر أمن نظم المعلومات المحاسبية الإلكترونية و استراتيجيات مواجهتها** ، رسالة ماجستير في المحاسبة ، كلية الاقتصاد ، جامعة تشرين ، سوريا ، 2015.
9. نوح سماح ،**دور نظام المعلومات المحاسبي في تقييم الأداء المالي للمؤسسة الاقتصادية دراسة حالة مؤسسة مطاحن الزيبان القنطرة – بسكرة –** ، أطروحة دكتوراه ، كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة محمد الخيضر ،بسكرة ،الجزائر ، 2019/2018.

د – الملتقيات العلمية :

1. روان بنت مفلح جهني ، **استخدام تقنية الذكاء الاصطناعي روبوت المحادثة chatbot لتقديم الخدمات المعلومات في المكتبات الجامعية في المملكة العربية السعودية** ، مؤتمر بعنوان التقنيات الناشئة وتطبيقاتها في المكتبات ومؤسسات المعلومات ،الكويت ،9/7 مارس 2023.
2. سامية خرخاش وأخرون ،**أهمية استخدام الحوسبة السحابية في المؤسسات** ،ملتقى دولي حول التحول الرقمي للمؤسسات والنماذج التنبؤية على المعطيات الكبيرة، جامعة مسيلة ،12و13, 2017
3. ظبية أحمد أبو عنين ،**إدارة الموارد في الحوسبة السحابية** ،ملتقى افتراضي السحابي الأول ،السعودية،2020/04/08.

4. بيان فراس النعانعة وأخرون ، **الصعوبات التي تواجه مديري المكتبات الجامعة الأردنية نحو استخدام تطبيقات الذكاء الاصطناعي** ،مؤتمر بعنوان التقنيات الناشئة وتطبيقاتها في المكتبات ومؤسسات المعلومات ،الكويت ،9/7 مارس 2023.

هـ – المطبوعات الجامعية :

1. رواني بوحفص ، **التدقيق المالي والمحاسبي دروس نظرية** ، كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة غرداية ،2017 – 2018.
2. سلماني عادل ،**مطبوعة في مقياس تدقيق ومراقبة أنظمة المعلومات** ،كلية العلوم الاقتصادية والتجارية وع التسيير ،جامعة غرداية ،2018– 2019.

ثانيا :المراجع بلغة الأجنبية :

A. Books :

1. Alsmadi, Izzat. ***The NICE Cyber Security Framework: Cyber Security Intelligence and Analytics***. Springer, Switzerland , 2019 .
2. Hall, James A. ***Accounting Information Systems***. Seventh Edition, Cengage Learning, USA , 2010
3. Laudon, Kenneth, et al. ***Management des systèmes d'information : corrigés des exercices***. 11e édition. Paris: Pearson Education, 2010.
4. Lehto, Martti, and Others . ***Cyber Security: Analytics, Technology and Automation***. Springer, Switzerland, 2015.
5. Romney, Marshall B., Steinbart, Paul John. ***Accounting information systems***. 14th Ed Harlow, England : Pearson, 2018.
6. Tony boczko, ***corporate accounting information systems***, pearson education limited, england, 2007.
7. Turner, Leslie, et al. ***Accounting Information Systems: The Processes and Controls***. John Wiley and Sons, USA , 2016.

B. THE Articles :

1. Deepak Sharma and Ruchi Mittal, Ravi Sekhar, Pritesh Shah, , Matthias Renz , "**A bibliometric analysis of cyber security and cyber forensics research**", Results in Control and Optimization , ELSEVIER , Netherlands,2023.
2. Mancini, Daniela, et al. ***Accounting Information Systems for Decision Making***. Springer Science and Business Media, Germany ,2013,

3. Morteza Safaei Pour and Christelle Nader, Kurt Friday, Elias Bou-Harb ,**A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security**, Computers & Security,ELSEVIER , Netherlands,2023.

4. Nicolas Mayer, Jean philippe Humbert, ***« la gestion des risques pour les systèmes d'information*** » , centrede recherche public Henri Tudor, Article paru dans le magasin MISC n24 , 2006.
5. Parker, Sandra, et al. “**Cybersecurity in Process Control, Operations, and Supply Chain**.” *Computers & Chemical Engineering*, vol. 171, Elsevier BV, Netherlands ,Feb. 2023,. https://doi.org/10.1016/j.compchemeng.2023.1081.

C. University papers :

1. Olfa Ismail**. Conception et mise en oeuvre d'une culture sécurité des systèmes d'information : le cas des PME**. Gestion et management. Université de Bretagne occidentale - Brest, 2021.
2. Yvon Pesqueux. ***Système d'information et organisation***. Master. France. 2020.

D. Other references

1. ISACA, **“ *The Risk IT Framework Excerpt*”**, United States of America, The Information Systems Audit and Control Association, 2009.

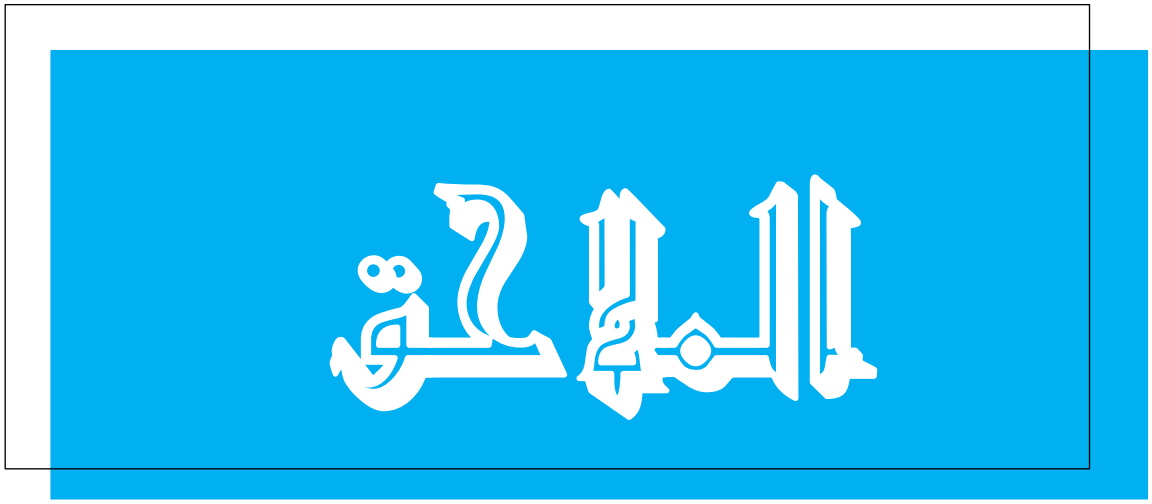
ي- المواقع الإلكترونية :

1. **الخليج** ، **6تريليونات دولار خسائر الهجمات السيبرانية عالمياً | صحيفة الخليج(alkhaleej.ae)** ، 2023/03/27، 11:25.
2. **سيف حطاب * مراد بوعاش** ، https://www.facebook.com/moubachirsv/videos/3144572159166220/، تم إطلاع عليه في 2023/02/23، 18:00.
3. برنامج سين2,https://www.youtube.com/watch?v=82ETlrSTHBE, 2023 /05/18, 20:00,
4. محمد عمر ، https://www.momar.tech/2021/05/active-directory.html ، 2023/05/15، 20:00.
5. تك مقدم من موضوع, https://cutt.us/8RN4b, 18/03/2022, 00:10.
6. الموسوعة السياسية، https://cutt.us/rshaZ، 2023/03/24، 22:20.

E. Web site :

1. National Cyber Security Centre, https://www.ncsc.gov.uk/guidance/phishing ,22/03/2023 ,20:15.
2. Chack Point , https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/wannacry-ransomware/ ,27/03/2023 , 12 :00.
3. Cloud Flare , https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ ,22/03/2023,21:10.
4. Cloud Flare , https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ ,22/03/2023,21:10.
5. Cloud Flare ,**Idem , https://www.cloudflare.com/learning/network-layer/what-is-tunneling/ .**
6. ENISA , https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle ,22/03/2023,20:10.
7. International Organization for Standardization ,https://www.iso.org/obp/ui#iso:std:iso:guide:73:ed-1:v1:en , 18/03/2023,23 :21.
8. Microsoft, https://cutt.us/mOdkU ,22/03/2023,16:03
9. NIST,https://csrc.nist.gov/glossary/term/masquerading#:~:text=Definition(s)%3A,posing%20as%20an%20aut horized%20entity,22/03/2023,15:43.
10. Port swigger Centre **, https://portswigger.net/web-security/sql-injection** ,22/03/2023,21:00
11. Techopedia , https://www.techopedia.com/ , 23 /03/2023,09:00.

“


الحق

”

الملاحق :

ملحق رقم **01** : عرض مقابلة

المقـابلـة

✓ **الجزء الأول: معلومات شخصية**

1. الاسم واللقب :

2. الهاتف :

3. الإيميل :

4. الصفة:

مدير: ☐ محاسب: ☐ مهندس إعلام آلي: ☐ تقني: ☐

5.عدد سنوات الخبرة:

5 سنوات فاقل: ☐ 6 /10 سنوات: ☐ من 15/11 سنة: ☐ أكثر من 15 سنة: ☐

✓ **الجزء الثاني: أسئلة المقابلة:**

1-ماهو واقع الرقمنة في مؤسسة نفطال؟ .....

.....

2-هل فكرت مؤسسة نفطال في مخطط للرقمنة؟.....

.....

3- ماهي البرمجيات المستخدمة في شركة نفطال؟ .....

.....

4- البرامج المستخدم في مجال المحاسبي و المالي ؟ هل انتاج محلي أو أجنبي؟.....

.....

5- ماهي مدخلات و المخرجات هذا النظام؟.....

.....

6- هل يرقى هذا البرنامج الى نظام معلومات محاسبي متكامل؟.....

.....

7- في رأيكم ماهي المرتكزات التي يقوم عليها هذا النظام اذا كان موجودا ؟ في حالة بـ:
لا – ماهي جهود المؤسسة في بناء نظام المعلومات؟.....

.....

8- هل يتم تخزين البيانات و معلومات المؤسسة في الأدوات السحابية أو الخوادم الالكترونية ؟اذا كان بالخوادم فهل ملكية الخوادم للمؤسسة أو لهيئة اخرى؟.....

.....

9- هل هناك جدار ناري لحماية مختلف الأنظمة و البيانات الموجود في المؤسسة؟.....

.....

10 – في العمليات المالية العادية هل يتم استخدام تطبيقات اخرى؟.....

.....

11 في المعاملات الخارجية كعمليات الجباية و التحصيلات *هل يتم استخدام تطبيقات مثل: مساهمتك ،جبايتك.....الخ؟.....

.....

12 – في تسيير محطات الوقود *هل يتم استخدام اجهزة TPE في عمليات التعبئة؟.....

.....

13 – هل هذه الاجهزة مرتبطة بنظام الكتروني مركزي؟.....

.....

14- بطاقات الدفع الالكترونية المستخدمة عندكم *هل هي معتمدة من طرف شركة "SATIM" ؟ .....

.....

16- هل تقوم المؤسسة بتكوين مستمر للمهندسين و التقنيين في مجال البرمجيات و تحديثاتها ؟.....

.....

17- في ظل اتجاه الدولة نحو استخدام الذكاء الاصطناعي و الروبوتيك في الانتاج و التخزين ،هل هناك اتجاه المؤسسة نحو اعادة تجديد اصولها الثابتة؟.....

.....

18- هل تم اختراق الأنظمة التى تستخدمها مؤسسة نفطال من قبل ؟ اذا كانت نعم ماهي الاجراءات التي تم اتخاذها؟ و هل أثرت على سيرورة عمل المؤسسة؟.....

.....

19- هل هذا الاختراق كان نتيجة أخطاء داخلية او قصور في انظمة المعلومات ؟.....

.....

20- في حالة الاخطاء الداخلية *هل يتم الاستعانة بجهات أمنية سيبرانية ؟.....

.....

21- في رأيكم ماهي معوقات تطبيق التكنولوجيا لدى المؤسسة ؟.....

.....

22- في رأيكم ماهي معوقات التى تواجه المؤسسة في هذا المجال ؟ .....

.....

23- جهود المؤسسة و استراتجيتها في مجال الأمن السيبراني لقطاع مهم في مجال الطاقة ؟ .....

.....

.....