جامعة قاصدي مرباح، ورقلة – الجزائر
كلية العلوم الاقتصادية و التجارية و علوم التسيير
قسم العلوم المالية والمحاسبية

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي، الطور الثاني
في ميدان : علوم اقتصادية، علوم التسيير وعلوم تجارية
فرع : علوم مالية ومحاسبية، التخصص : تدقيق ومراقبة التسيير

بعنوان :

أثر نظام الحماية الالكتروني في الحد من مخاطر نظم المعلومات
دراسة حالة مؤسسة ENAGEO

من إعداد الطالبتين: قابل نور الهدى – هيمة هاجر

نوقشت وأجيزت علنا بتاريخ :19جوان 2019
أمام اللجنة المكونة من السادة :

الدكتور/ محمد الطيب دويس (أستاذ– جامعة قاصدي مرباح ورقلة) رئيسا
الدكتور/ خالد رجم (أستاذ محاضر أ – جامعة قاصدي مرباح ورقلة) مشرفا ومقررا
الاستاذ/ كاوجة بشير (أستاذ مساعد أ– جامعة قاصدي مرباح ورقلة) مناقشا

السنة الجامعية : 2018 – 2019

جامعة قاصدي مرباح، ورقلة – الجزائر
كلية العلوم الاقتصادية و التجارية و علوم التسيير
قسم العلوم المالية والمحاسبية

مذكرة مقدمة لاستكمال متطلبات شهادة ماستر أكاديمي، الطور الثاني
في ميدان : علوم اقتصادية، علوم التسيير وعلوم تجارية
فرع : علوم مالية ومحاسبية، التخصص : تدقيق ومراقبة التسيير

بعنوان :

أثر نظام الحماية الالكتروني في الحد من مخاطر نظم المعلومات
دراسة حالة مؤسسة ENAGEO

من إعداد الطالبتين: قابل نور الهدى – هيمة هاجر

نوقشت وأجيزت علنا بتاريخ :19 جوان 2019
أمام اللجنة المكونة من السادة :

الدكتور/ محمد الطيب دويس (أستاذ– جامعة قاصدي مرباح ورقلة) رئيسا
الدكتور/ خالد رجم (أستاذ محاضر أ – جامعة قاصدي مرباح ورقلة) مشرفا ومقررا
الاستاذ/ كاوجة بشير (أستاذ مساعد أ– جامعة قاصدي مرباح ورقلة) مناقشا

السنة الجامعية : 2018 – 2019

الشكر

اعترافا بالود وحفظا للجميل وتقديرا للامتنان نتقدم بجزيل الشكر وبأسمى

عبارات التقدير والاحترام الى الأستاذ المشرف: **خالد رجم**

الذي لم يبخل علينا بالتوجيه والنصح؛

و نتقدم بالشكر إلى إطارات المؤسسة الوطنية للجيوفيزياء على حسن

الاستقبال ومساعدتهم لنا، وعلى رأسهم السيد: **قابل عنتر**.

كما نشكر كل من ساعدنا من قريب أو من بعيد ولو بكلمة أو دعوة صادقة.

قابل نور الهدى

هيمة هاجر

الملخص:

تهدف هذه الدراسة الى تحليل واقع نظام الحماية الالكتروني في المؤسسة الوطنية للجيوفيزياء بحاسي مسعود، وكذا مدى تأثيره في الحد و التقليل من احتمالية حدوث مخاطر نظام المعلومات ، وقد تم الاعتماد على المنهج الوصفي وذلك باستخدام كل من أداتي المقابلة مع إطارات ومسيري نظام المعلومات في المؤسسة، والاستبانة التي تم توزيعها على عينة قصدية وهي مستخدمي النظام في المؤسسة، وقدرها 59 فردا، كما اعتمدنا أيضا على دراسة الحالة من أجل تشخيص ووصف واقع نظام المعلومات وكذا نظام الحماية الالكتروني في المؤسسة، وقد توصلنا إلى جملة من النتائج أهمها : تعرض المؤسسات إلى عدة مخاطر تهدد أمن نظم المعلومات أشدها مخطر الموظفين عند إدخالهم معلومات خاطئة بشكل غير متعمد، وأيضا مخطر فقدان البيانات نظرا لعدم توفر نسخ احتياطية خارج المؤسسة، كما لاحظنا اختلالات على مستوى نظام الأمن منها عدم الصرامة في معاقبة الموظفين بشأن عدم الالتزام بالسياسات الأمنية كإلزامية تغيير كلمة المرور، وكذا عدم استعمال الفلاش ديسك في نقل البيانات، بالإضافة إلى نقص الأيام التدريبية من أجل رفع الوعي بمخاطر نظام المعلومات و كذا الأمن الإلكتروني.

الكلمات المفتاحية: نظام المعلومات، نظام الحماية الالكتروني ،سياسات الأمنية ، مخاطر نظم المعلومات، الأمن الالكتروني، الجدار الناري، الفيروسات، مضادات الفيروسات.

Abstract :

The objective of this study was to analyze the reality of the electronic protection system in the National Geophysics Institution in Hassi Masoud, as well as its effect on reducing and reducing the probability of the risks of the information system. We also used the questionnaire as it was distributed to a target sample of 59 users of the system in the organization. We also relied on the case study to diagnose and describe the reality of the information system and the electronic protection system in the organization. The most important results were: There are several risks to the security of information systems as the most dangerous is the risk of employees, as the data because of the lack of backup copies outside the institution, and we noted imbalances at the level of the security system, including the lack of strict punishment of employees for non-compliance with security policies such as mandatory change password and not use Flash Disk in data transfer, in addition to the lack of training days in order to raise awareness of the risks of the information system and such electronic security.

Keywords: information system, electronic protection system, security policies, information systems risks.

قائمة المحتويات:

العنوان	الصفحة
الإهداء	III
الشكر	IV
الملخص	V
قائمة المحتويات	VI
قائمة الجداول	VII
قائمة الأشكال	VIII
قائمة الاختصارات والرموز	X
قائمة الملاحق	IX
المقدمة	ب
الفصل الأول: الأدبيات النظرية والتطبيقية لمساهمة نظام الحامية الالكتروني في الحد من مخاطر نظام المعلومات	01
تمهيد الفصل الأول	02
المبحث الأول: الإطار النظري لأثر نظام الأمن الالكتروني في الحد من مخاطر نظم المعلومات	02
المبحث الثاني: الدراسات السابقة	18
خلاصة الفصل الأول	23
الفصل الثاني: الدراسة الميدانية لتقييم أثر نظام الحماية الالكتروني في الحد من مخاطر النظم المعلومات	25
تمهيد الفصل الثاني	26
المبحث الأول: عينة وأدوات الدراسة	26
المبحث الثاني: تحليل ومناقشة نتائج الدراسة الميدانية	29
خلاصة الفصل الثاني	49
الخاتمة	51
المراجع	55
الملاحق	59
الفهرس	70

قائمة الأشكال :

الرقم	عنوان الشكل	الصفحة
1-1	تطور نظام المعلومات	4
1-2	العناصر الأساسية لنظام المعلومات	5
1-3	طبيعة جنس العاملين المستجوبين	35
1-4	متغير العمر	36
1-5	متغير المستوى	37
1-6	متغير الخبرة	37

قائمة الجداول :

الرقم	عنوان الجداول	الصفحة
1-1	النظرة الحديثة لنظم المعلومات	7
1-2	مقارنة بين الدراسات السابقة و الدراسات الحالية	22
1-3	جدول ليكرت الثلاثي للمحور الاول	28
2-3	مقياس المحور الثاني	29
3-3	المتوسطات المرجحة و الاتجاه الموافق لها	29
1-4	واقع نظام المعلومات الالكتروني	30
2-4	محتويات قاعة الاجهزة و المعدات (DINTIC) بالمؤسسة الوطنية enageo	31
3-4	الاجهزة الالكترونية الجديدة الخاصة بالشبكة الواسعة بالمؤسسة الوطنية enageo	33
4-4	التطبيقات المنجزة بالمؤسسة الوطنية enageo	33
1-5	معاملات ثبات الأداة حسب المعامل (ألفا كرونباخ) حجم العينة(N=59)	38
2-5	نتائج اجابات المستجوبين الخاصة بالبعد الاول	39
3-5	نتائج اجابات المستجوبين الخاصة بالبعد الثاني	40
4-5	نتائج اجابات المستجوبين الخاصة بالبعد الثالث	41
1-6	معامل الارتباط بين نظام الأمن الالكتروني ومخاطر نظام المعلومات	43
1-7	السياسات الأمنية	45
1-8	سلبيات وايجابيات نظام المعلومات	46
1-9	المقارنة مدى امكانية حدوث مخاطر نظام المعلومات	46

قائمة الملاحق:

الرقم	عنوان الملحق
01	أسئلة المقابلة
02	استمارة الاستبيان
03	الهيكل التنظيمي لقسم نظام المعلومات بالمؤسسة الوطنية Enageo
04	مخطط الشبكة المحلية (LAN) بالمؤسسة الوطنية Enageo
05	مخطط الشبكة الواسعة WAN بالمؤسسة الوطنية Enageo
06	صورة لغرفة الخوادم الموجودة بالمؤسسة
07	اللوائح القانونية المعلنة في المؤسسة
08	واجهة مضاد الفيروسات
09	واجهات البرامج المنجزة بالمؤسسة
10	تطبيقات برنامج أوراكل

قائمة الاختصارات والرموز:

الاختصار	الدلالة باللغة الأجنبية	الدلالة باللغة العربية
SPSS	Statistical Package Social Sciences	الحزمة الإحصائية للعلوم الاجتماعية
ISACA	Society of the Review and Control of Information Systems	جمعية ومراجعة ومراقبة نظم المعلومات
VSAT	Very Small Aperture Terminal	المحطات الأرضية ذات الحجم الصغير
IP	Internet Protocol	بروتوكول انترنيت
LAN	Local Area Networks	الشبكة المحلية للاتصالات
WAN	Wide Area Networks	الشبكة الواسعة للاتصالات
SGBD	Système de Gestion de base des données	نظام تسيير قاعدة البيانات
ERP	Resource Planning System	نظام تخطيط الموارد
VPN	Vitual Private Networks	الشبكة المحلية الافتراضية

توطئة:

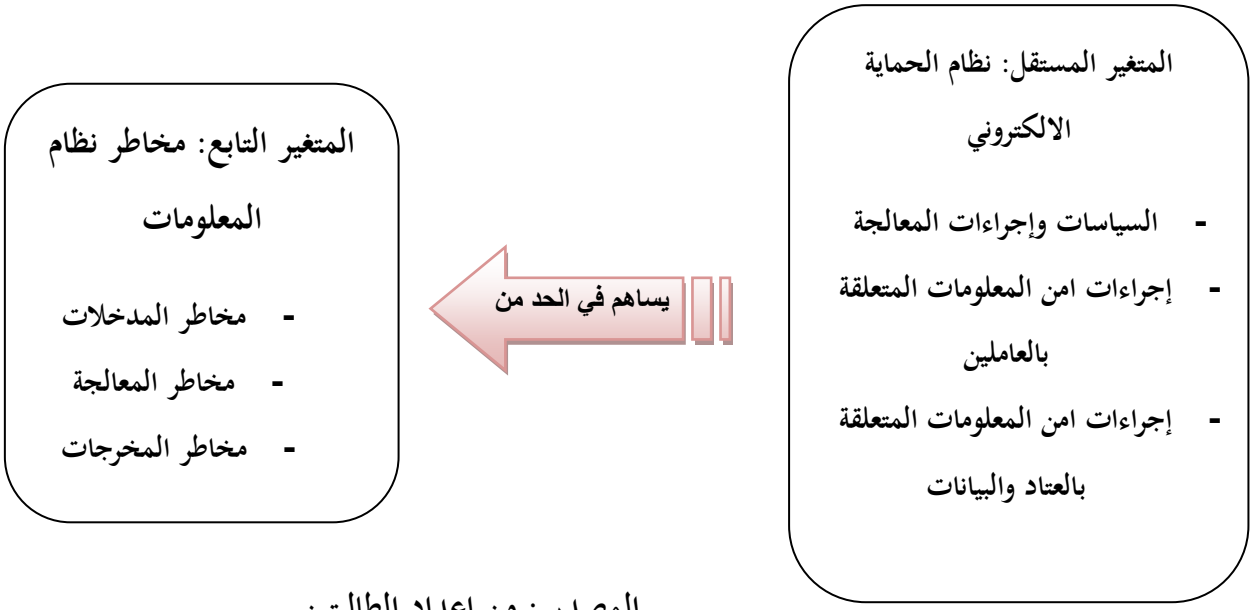
أصبحت المؤسسات على اختلاف أنماطها تعتمد على أنظمة المعلومات المختلفة إن كانت معقدة أو بسيطة ،وتعتبر هذه الأنظمة العمود الفقري للمؤسسة لإمدادها بالمعلومة المناسبة ،ومع التطور التكنولوجي في جميع الميادين .

ولقد وفرت التكنولوجيا الوقت والجهد ولكن بالمقابل أدى الى ازدياد المخاطر المحيطة بأنظمة المعلومات في ظل الانفتاح على الاقتصاد العالمي ، من هنا كان على المؤسسات أن تشدد من إجراءاتها الأمنية لحماية أنظمتها المعلوماتية ،و من هذا المنطلق سعت العديد من الشركات الوطنية، إلى تصميم وبناء نظام معلومات إلكتروني، مستهدفة من خلاله توفير نظام أمن الكتروني لما يميز هذا النظام من بنية تحتية، تتمثل في الحواسيب وأجهزة شبكات الاتصالات الإلكترونية وقواعد البيانات، التي تتميز بالسرعة الفائقة في المعالجة والاسترجاع المعلومات والقدرة الهائلة على تخزينها, مما يحقق السيطرة على الكم الهائل من المعلومات الضرورية , وضمان وصولها بالشكل الصحيح والملائم وفي الوقت المناسب الى كافة المستويات الادارية .

- **الإشكالية :**

ما مدى نجاعة نظام الحماية الالكتروني في الحد من مخاطر نظم المعلومات في المؤسسة الوطنية للجيوفيزياء ؟

- **نموذج الدراسة**



المصدر : من اعداد الطالبتين

● الأسئلة الفرعية :

1. ما مدى كفاءة مكونات نظام المعلومات الإلكتروني في المؤسسة محل الدراسة؟
2. ما مدى كفاءة مكونات نظام الأمن الالكتروني في المؤسسة محل الدراسة ؟
3. ما مدى فعالية نظام الأمن الالكتروني في الحد من مخاط نظام المعلومات فيالمؤسسة محل الدراسة؟

●فرضيات الدراسة :

في ضوء العرض السابق لمشكلة البحث و الأسئلة الفرعية المتعلقة بأثر نظام الأمن الالكتروني على ادارة مخاطر نظم المعلومات في مؤسسة جيوفيزياء ، يمكن صياغة الفرضيات التالية بهدف اختبار صحتها :

1. يتوفر نظام المعلومات الالكتروني في المؤسسة محل الدراسة على جميع العناصر المهمة من عتاد و كذا برامج حديثة، وأيضا قواعد بيانات و شبكات بالإضافة الى افراد مؤهلين.
2. لدى المؤسسة محل الدراسة نظام امن الكتروني يشمل كل عناصر الأمن الالكتروني لحماية أنظمتها من كل أنواع الاختراق
3. يساهم نظام الامن الالكتروني في المؤسسة في الحد من مخاطر نظام المعلومات.

● **مبررات اختيار موضوع الدراسة :** هناك سببين اساسيين في اختيار هذا الموضوع :

✓ **مبررات موضوعية :**

_ الموضوع يدخل ضمن التخصص،

_ أهمية موضوع الأمن الالكتروني.

✓ **مبررات ذاتية :**

_ الاهتمام الشخصي بمواضيع الأمن الالكتروني و نظم المعلومات.

● أهداف الدراسة :

يسعى هذا البحث إلى إبراز مجموعة من الأهداف، والتي يمكن توضيحها كما يلي:

1- التعرف على المخاطر المحيطة بنظام المعلومات الالكتروني.

2- العمل على تطبيق سياسة الأمن الالكتروني من اجل الحد من مخاطر نظم المعلومات ويجب أن تكون ناجحة .

3-الخروج بنتائج واقتراحات حول فعالية نظام الأمن الالكتروني في إدارة مخاطر نظم المعلومات ، وكيفية الاستفادة من تطبيقاته من أجل تعظيم مكاسبه سواء بالنسبة للمؤسسة أو العاملين.

• حدود الدراسة:

الحدود المكانية :فيما يخص الإطار المكاني للدراسة الميدانية فكان بمؤسسة ENAGEO بحاسي مسعود

الحدود الزمانية :أما ما يخص الإطار الزماني للدراسة فقد كانت خلال فترة أفريل 2019 الى ماي 2019

• صعوبات الدراسة:

_ صعوبة برمجة المقابلة مع الاطارات نظرا لالتزاماتهم العديدة.

_ صعوبة في استعادة كل الاستبيانات الموزعة بالإضافة لتأخر استلامها.

• منهجية الدراسة والأدوات المستخدمة:

قصد الوصول الى معرفة دقيقة لعناصر اشكاليتنا وقصد فهم أدق وأفضل للموضوع اعتمدنا في دراسة على :

1- المنهج الوصفي؛

2- اجراء مقابلة مع عمال مديرية تكنولوجيا المعلومات (مسيري النظام)؛

3- توزيع استبيان على عينة قصدية من عمال المؤسسة الوطنية للجيوفيزياء لمعرفة مدى فعالية نظام الأمن الالكتروني في إدارة مخاطر نظم المعلومات ؛

4- استخدام برنامج SPSSلمعالجة البيانات التي تم جمعها ؛

• هيكل الدراسة :

من أجل معالجة هذا الموضوع قمنا بتقسيم البحث كما يلي:

الفصل الأول : الأدبيات النظرية والتطبيقية لنظام الأمن الالكتروني

المبحث الأول : الإطار النظري لمخاطر نظم المعلومات الالكترونية

المبحث الثاني : الدراسات السابقة

الفصل الثاني : دراسة حالة في المؤسسة الوطنية للجيوفيزياء

المبحث الأول : العينة والأدوات المستخدمة في الدراسة

المبحث الثاني : تحليل ومناقشة نتائج الدراسة الميدانية.

تمهيد:

تعد المعلومات اليوم موردا مهما ورئيسيا من موارد المنظمة؛ ذلك أنها تشكل عاملا هاما لنجاح المنظمة في تحقيق رسالتها وأهدافها، خاصة في ظل عالم يتميز بدرجة عالية من التعقيد والتغيير، نتيجة انتشار مفاهيم الخوصصة والعولمة، فأصبحت المعلومة سلاحا تنافسيا، وموردا استراتيجيا يتوقف عليه نجاح المنظمة أو فشلها.

ومن خلال ما سبق سيتم تقسيم الفصل الأول إلى مبحثين، تناولنا في المبحث الأول: الإطار النظري لأثر نظام الأمن الالكتروني في الحد من مخاطر نظم المعلومات ، ثم قسمنا هذا المبحث إلى أربعة مطالب: أولا تناولنا عموميات حول نظم المعلومات وخصصنا المطلب الثاني لنظام الأمن الالكتروني، وبالنسبة للمطلب الثالث تحدثنا عن تقييم نظام الأمن الالكتروني، وفي المطلب الأخير تناولنا مخاطر نظام المعلومات، أما المبحث الثاني : الدراسات السابقة، فقسمناه الي مطلبين الأول خصصناه لدراسات السابقة باللغة العربية، أما المطلب الثاني تناولنا به الدراسات السابقة باللغة الأجنبية.

المبحث الأول: الإطار النظري لأثر نظام الأمن الالكتروني في الحد من مخاطر نظم المعلومات:

المطلب الأول: الاطار النظري لنظام المعلومات:

إن نظام المعلومات يلعب دورا هاما وحساسا داخل المؤسسة بصفته منتجا للمعلومات, فهو يعتبر عنصرا حيويا, إذ على أساس المعلومات التي ينتجها يتم اتخاذ القرارات الفورية والاستراتيجية للمؤسسة .

الفرع الأول: ماهية نظام المعلومات:

أولا :التعريف الأول:

يرى أحمد فتحي الحيت أن نظام المعلومات "هو مجموعة من الإجراءات، التي تتفاعل مع بعضها البعض بهدف معالجة البيانات وتحويلها، بهدف استخدامها في عملية صنع القرار. إن المعلومات هي بيانات تمت معالجتها بشكل يسمح باستخدامها والاستفادة منها حيث أصبحت ذات معنى وفائدة، فالمعلومات هي البيانات التي خضعت للمعالجة، والتحليل، والتفسير، بهدف استخراج المقارنات والمؤشرات والعلاقات، التي تربط الحقائق والأفكار والظواهر مع بعضها البعض[1] "

ثانيا :التعريف الثاني:

"An information system can be defined technic 63 ally as a set of interrelated components that collect (or retrieve), process, store, and distribute information to support decision making and control in an organization. In addition to supporting decision making, coordination, and control, information systems may also help managers and workers analyze problems, visualize complex subjects"[2]

يمكن تعريف نظام معلومات فنيا، كمجموعة من المكونات المترابطة تهدف إلى جمع ومعالجة وتخزين وتوزيع المعلومات، لدعم القرار والتحكم في المؤسسة ،وبالإضافة إلى دعم عملية صنع القرار، والتنسيق، والسيطرة، فإن نظم المعلومات تساعد أيضا الإدارة العليا على تحليل المشاكل، و الموضوعات المعقدة، بتوفير المعلومات المناسبة في الوقت المناسب للمساعدة في اتخاذ القرار.[3]

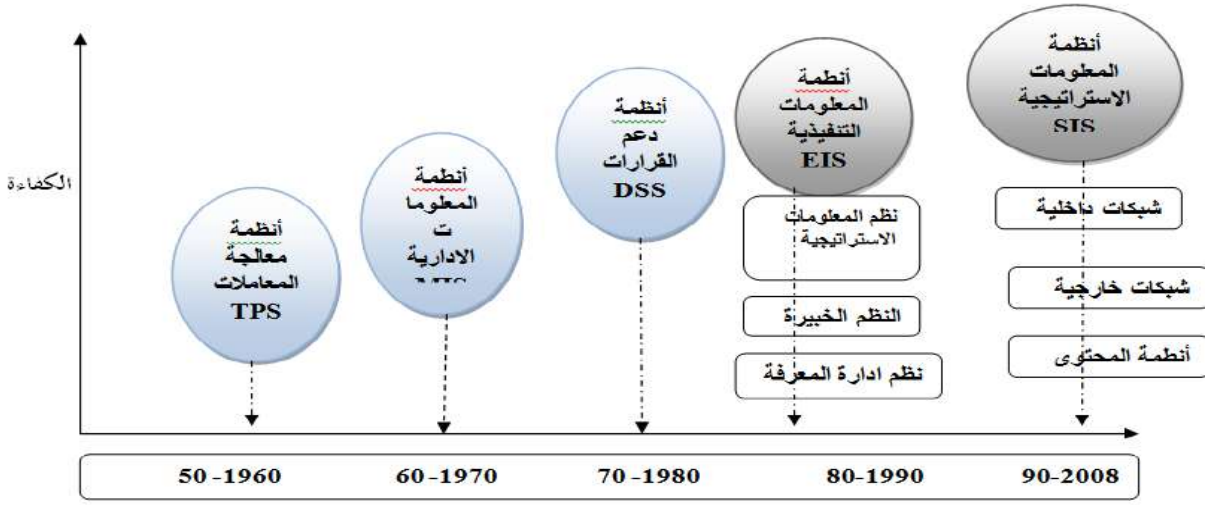
---

[1] أحمد فتحي الحيت, مبادئ الادارة الالكترونية, دار الحامد للنشر والتوزيع, عمان,2015,ص:114

[2] laudon & laudon-management information system-the digital firm , idition9, Pearson Education, USA,2006, page:50

[3] رجم خالد ، تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية ، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير ورقلة (الجزائر)، 2017ص49

الشكل رقم(1-1) تطور نظام المعلومات



المصدر: خالد رجم ، تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية ، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير ورقلة، 2017 ص49.

من الشكل أعلاه، تتضح فكرة جوهرية في نظام المعلومات، وهي أن ظهوره كان بهدف تقديم الدعم، والمساندة لإدارة المنظمات في مختلف المستويات، لكن التطور التكنولوجي في ميدان الحاسوب، والبرمجيات خلال الفترة الممتدة من 1970 إلى 1990فتحت مجالا واسعا لاستخدامات متطورة له TIC .فتحت مجالا واسعا لاستخدامات متطورة له.

كما نجد أن نظم معالجة المعاملات، هي أول نظم المعلومات التي ظهرت في المؤسسة، لدعم المستوى التشغيلي، ثم ظهرت نظم المعلومات الإدارية التي تدعم وظائف المؤسسة، بعدها ظهرت نظم دعم القرار التي تساعد على اتخاذ القرارات، في ظل عدم التأكد، بالإضافة إلى النظم التنفيذية، وآخرها نظم المعلومات الاستراتيجية، كما لا ننسى أخر تطبيقات أنظمة المعلومات في المؤسسة، وهي نظام تخطيط موارد المؤسسة ERP

الفرع الثاني :عناصر نظام المعلومات:

يتكون أي نظام للمعلومات في أي مؤسسة، من مجموعة من العناصر، وهذه العناصر لا تعدو أن تكون المدخلات بأشكالها المتنوعة، المعالجة أو التشغيل، ثم المخرجات على الصورة المخطط لها، ثم التغذية المرتدة والرقابة عليها، والبيئة الخارجية المحيطة والمؤثرة في المؤسسة، وتتمثل في التالي:

أولا: المدخلات : تتمثل في سلسلة البيانات التي تنساب من قنوات الاتصال المختلفة من المصادر الداخلية، والمصادر الخارجية أو من النظام ذاته، عندما يعتمد جزء امن مخرجاته كمدخلات جديدة لتغذية النظام[4].

.**ثانيا: المعالجة** :تتم معالجة البيانات المدخلة، بإجراء عدد من العمليات لإنتاج المخرجات المعينة المحتاج إليها [5]

[4]محمد ال فرج الطائي، الموسوعة الكاملة في نظم المعلومات الادارية الحاسوبية ,دار زهران, الأردن, 2002, ص:44

[5]أبو بكر محمود الهوش، **نظم وشبكات المعلومات**، **مؤسسة الثقافة الجامعية**، مصر،2007,ص95

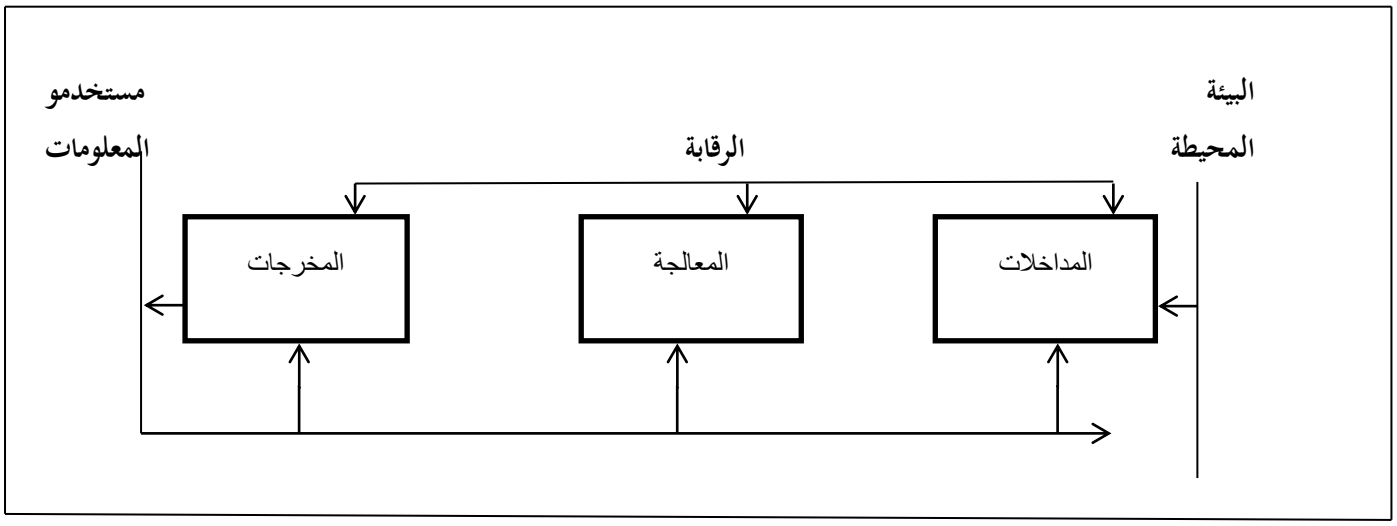
ثالثا: المخرجات :تتحول المدخلات بفعل عمليات المعالجة ،إلى المخرجات التي تطرح في البيئة المحيطة، أو تستخدم كمدخلات جديدة للنظام نفسه، والتي تكون على نوعين حصرا في جميع أنواع الأنظمة، وهما المادة فقط، أو المعلومات فقط، أو كليهما معا.

رابعا: التغذية العكسية :هي سريان وتدفق المعلومات من وإلى النظام، بعد تقييم العمليات المنفذة، وأخذها بعين الاعتبار في ضوء القرارات، والعمليات المستقبلية، وهي في الواقع دليل للأداء المستقبلي، وتقوم بتصحيح النظام من خلال ضوابط، وتعديلات لازمة للتخلص من الأخطاء ورفع كفاءة الأداء للنظام، لتحقيق الأهداف التي يرمي النظام إلى تحقيقها خدمة للشركة ككل

خامسا: الرقابة :هي مقياس الأداء وضبط العمليات المؤدية إلى الهدف المرجو، وهي محصلة معرفة سبق تحديدها عن آلية عمل النظام، وتشمل الرقابة قياس وتقييم مسار المدخلات، العمليات والمخرجات، للتأكد بأن النظام يؤدي وظائفه بصورة متماشية مع الأهداف والخطط الموضوعة، فإذا كانت هناك أي انحرافات، فإنه يجري القيام بالتعديلات اللازمة على المدخلات والعمليات والمعالجة وصولا لتصحيح المسار نحو الأهداف الموضوعة.

سادسا: البيئة :تتأثر المؤسسة بالبيئة المحيطة بها، وتصدر مخرجاتها أيضا إلى هذه البيئة بعد تشغيلها، مما يعني وجود علاقة تبادلية وثيقة بين المؤسسة والبيئة المحيطة، يؤثر كل منهما في الآخر سلبا أو إيجابا، ويزداد هذا التأثير إذا كانت البيئة محكومة ومقيدة، مثل النظم الاقتصادية، والسياسية الموجهة أو المغلقة وفق الشكل الآتي:

الشكل رقم(1-2) لعناصر الأساسية لنظام المعلومات



المصدر: عبد الرزاق محمد قاسم، تحليل وتصميم نظم المعلومات المحاسبية، دار الثقافة، دمشق، 2009ص 16

من خلال الشكل السابق، يتبن سير المعلومة بدءا من مستخدمي المعلومات، تم تحولها إلى مدخلة، ثم معالجتها، تم تحولها إلى مخرجات، كل هذا من خلال تواجد رقابة عبر كلال مراحل.

الفرع الثالث :مستويات نظام معلومات:

إن نظم المعلومات تتوزع حسب المستويات التنظيمية بالمؤسسة، حيث يمكن تصنيفها ابتداء من المستوى الأدنى وصعودا إلى المستوى الأعلى كالآتي[6] :

أولا: المستوى الاستراتيجي (Strategic Level Systems) :

Information Systems that support the long-range planning activities of senior management.

نظم المستوى الاستراتيجي، التي تمكن المسيرين في الإدارة العليا من القيام بالنشاطات ذات البعد الاستراتيجي، وتسمح لهم بتحديد الأهداف طويلة الأجل، واختيار الوسائل الضرورية لتحقيقها، فالهدف من هذه النظم هو إحداث التوافق بين التغيرات التي تحدث في البيئة الخارجية للمؤسسة، مقارنة بقدرتها الحالية والمستقبلية، وتساعد هذه النظم في الإجابة على عدة تساؤلات منها:

كيف ستكون مستويات العمالة في الخمس سنوات المقبلة؟ ما هو اتجاه تكاليف الصناعة مستقبلا؟ ما هي المنتجات التي يجب تقديمها خلال الخمس سنوات المقبلة؟، بالإضافة إلى دراسة (الوضع الاستراتيجي، تخطيط الأرباح، التنبؤ بالمبيعات لخمس سنوات، التخطيط الاستراتيجي...)؛

ثانيا :المستوى الإداري (Management level Systems) :

أما نظم المستوى الإداري، فهي تعمل على مساندة مسؤولي الأنشطة في اتخاذ القرارات شبه الهيكلية وتسيير الأنشطة في الإدارة الوسطى، كما تخدم تخطيط الوظائف عن طريق تقديم ملخص روتيني يهدف إلى تحقيق السرعة في انجاز التقارير المطلوبة، والتساؤل الرئيسي الذي تحاول هذه النظم الإجابة عليه هو:

ما هو وضع المؤسسة مقارنة بالتوقعات؟ وما هي أهدافها التشغيلية؟ كما يشتمل على (إدارة المبيعات، تحليل مبيعات السوق، تخطيط الإنتاج، تسيير المخزون، تسيير الموازنة السنوية...) حيث يتم في هذا المستوى استعمال المعلومات لاتخاذ القرارات القصيرة الأجل

ثالثا :المستوى التشغيلي (Operational level systems)

فنظم المستوى التشغيلي تعمل على دعم النشاطات الروتينية المتكرّرة ومتابعة سير المعاملات داخل المؤسسة والمرتبطة بالوظائف الأساسية من تسويق ومبيعات، إنتاج وتصنيع، مالية ومحاسبة، موارد بشرية وهي تجيب على الأسئلة المختلفة المتعلقة بهذه الوظائف

الجدول رقم(1-1) النظرة الحديثة لنظم المعلومات

النظرة التقليدية	النظرة الاستراتيجية
وظيفة ادارة نظام المعلومات هي مركز تكاليف.	نظام المعلومات عنصر من عناصر سلسلة القيمة
تكنولوجيا المعلومات والاتصال هي وسيلة.	نظام المعلومات هو اصل من اصول المؤسسة

[6] رجم خالد، تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية ، مرجع سابق، ص52

تكنولوجيا المعلومات والاتصال لها اثر ودور وظيفي و تشغيلي.	نظام المعلومات له وظيفة الدعم الاستراتيجي
تستغل تكنولوجيا المعلومات والاتصال في كل وظيفة على حدا.	نظام المعلومات عبارة عن نظام مدمج ومتكامل ويشارك في تسييره جميع الاطراف
تكنولوجيا المعلومات والاتصال ميدان محتكر من طرف مهندسي الاعلام الالي فقط.	نظام المعلومات ميدان متعدد وليس مخصص لفئة معينة حيث يستخدم ويسير من طرف المسيرين+ مهندسي الاعلام الالي

المصدر: رجم خالد، تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية ، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير ورقلة،2017 ص53

ما نستنتجه من الشكل أعلاه أن النظرة لنظم المعلومات قد تطورة بشكل كبير من نظرة تقليدية وظيفية روتينية إلى نظرة استراتيجية حيث أصبحت نظم المعلومات كوسيلة لتحقيق الميزة التنافسية و تحقيق الأداء المطلوب لكن هذا يتوقف دائما على مدى الاستغلال الأمثل للنظام و مدى توافق النظام مع استراتيجية المؤسسة.

الفرع الرابع :أهداف وأهمية نظام معلومات :

أولا :أهداف نظام المعلومات : تتلخص هذه أهداف في الآتي[7] :

_ **تزويد الإدارة العليا بالمعلومات** :تحتاج الإدارة في جميع أعمالها إلى المزيد من المعلومات بحيث يعمل النظام على مد الإدارة العليا بمعلومات عن الفرص والتهديدات النابعة من البيئة الخارجية، وكذلك عن مؤشرات الأداء داخل المؤسسة وهو ما يمكن الإدارة من زيادة القيمة المضافة.

_ **تحديد المسؤولية** : تساعد نظم المعلومات في تحديد أدوار الأفراد والأقسام بالمؤسسة وبالتالي تحديد مسؤولية هؤلاء، وبتحديد المسؤولية فإنه يمكن محاسبة المقصرين والتعرف على المهملين.

_ **تخفيض عدد المشاكل** :لعل الهدف الحقيقي من التفكير في نظام جديد هو التخلص من المشاكل الموجودة في ظل النظام الحالي، بيد أنه عملي ا من غير الممكن التخلص من كل المشاكل ولكن فقط تخفيض عددها وتخفيض حجمها كلما أمكن ذلك.

_ تنظيم الإجراءات :وهذه الوظيفة للنظام مستمدة من الاسم "نظام" أي شيء مخطط ومحدد ومرتب وفي غيبة النظام فإن الغلبة تكون للفوضى والعشوائية، والمؤسسة تتوقع من النظام الجيد تقنين الإجراءات وسد الثغرات في سير خطط العمل الحالية.

_ **السيطرة على الموارد المتاحة** : الموارد المتاحة قد تكون مادية كأجهزة ومعدات، أو بشرية كالعاملين والعملاء أو معنوية كبيانات موجودة أو يمكن الحصول عليها، إلا أن هذه الموارد التي قد تكون السيطرة عليها عملا في منتهى الأهمية، للاستفادة منها استفادة قصوى.

فعلى سبيل المثال يمكن لمؤسسة أن تحصر عدد وتخصصات العاملين، لتعيد توزيع أدوارهم ووظائفهم ما يكفل الاستفادة منهم في زيادة الإنتاج دونما الحاجة لتعيين أي عامل إضافي.

[7] محمد الصيرفي، **نظم المعلومات الإدارية** ، طبعة الأولى، مؤسسة حورس الدولية، الإسكندرية،،2005ص ص 186-188

ـ **ضمان انسياب العمل** :من وظائف النظام أن يؤدي إلى التنسيق والانسجام بين النظم الفرعية بما يكفل انسياب العمل والتخلص من الاختناقات الموجودة، ففي مؤسسة يتم العمل على مراحل يجب أن يعمل النظام على توزيع الأدوار والطاقات، بما لا يخلق تكدس ا في مرحلة ما فتتعطل السلسلة .

ثانيا : أهمية نظام المعلومات :

ـ المساعدة في اتخاذ القرار: حيث يوفر نظام المعلومات لمتخذي القرارات بالمعلومات اللازمة لتوضيح المشكلة المراد دراستها او اتخاذ قرارا بشأنها كما تساعد المعلومات المتوفرة على دراسة النتائج المحتملة عن القرار المتخذ، مثال اذا اردنا اتخاذ قرارات تجارية يجب توفير معلومات عن المبيعات الحالية بالاضافة الى التنبؤ بالمبيعات على ستة أشهر؛

ـ تطوير أنظمة المؤسسة و رفع أدائها: من خلال الرقابة المستمرة وكشف الانحرافات ثم اتخاذ الاجراءات التصحيحية؛

ـ التنسيق بين مختلف اجزاء المنظمة من خلال توفير مختلف المعلومات المتعلقة بكافة المستويات التنظيمية و مختلف الوظائف وهذا لإعطاء صورة واضحة ومتكاملة عن المؤسسة.[8]

المطلب الثاني: نظام الأمن الالكتروني:

ان استخدام تكنولوجيا المعلومات والاتصال وفر الكثير من الوقت والجهد للعاملين ، إلى أنه أدى إلى زيادة مخاطر أنظمة المعلومات، من هنا كان على المؤسسات أن تشدد من إجراءاتها الأمنية لحماية

أنظمتها المعلوماتية ،و من هذا المنطلق سعت المؤسسات إلى تصميم وبناء نظام حماية إلكتروني للحد من مختلف المخاطر المحيطة بنظام المعلومات المتمثلة في مخاطر تتعلق بالأفراد.

الفرع الأول: نظام الحماية الالكتروني (الأمن الالكتروني):

أمن نظام المعلومات هو جميع الطرق والتقنيات ووسائل الأمن والحماية لموارد نظام المعلومات، ويمثل الهدف من أي برنامج امن يعد لنظام المعلومات حماية المنظمة وذلك بتقليل المخاطر التي تؤثر على توافر المعلومات وسريتها وسلامتها بمستوى مقبول ومحدد وعليه يجب على المؤسسة وضع قواعد السلامة وإتباع السياسات الأمنية وفق المعايير المتعارف عليها لضمان السير السليم للنظام وينبغي ان يتضمن التخطيط والرقابة الإدارية على امن النظام ما يلي :

-تحديد الأهداف والتي تعتبر بمثابة معايير لتقييم امن النظام فيما بعد، وتتمثل هذه الأهداف في حماية مكونات النظام؛

-تقدير الاحتمالات والتكاليف المرتبطة بمخاطر امن تشغيل البيانات؛

-إعداد خطة تضمن مستوى مقبولا من الأمن وبتكلفة معقولة، وتصف هذه الخطة كافة الإجراءات الرقابية التي سيتم تطبيقها وأهداف هذه الإجراءات، هذا وينبغي إن يتم فحص الخطة والتصديق عليها قبل وضعها موضع التنفيذ؛

-تحديد المسؤوليات عن امن النظام؛

-اختبار إجراءات الرقابة على امن النظام، وذلك للتحقق من مدى فعاليتها في تحقيق أهدافها المرجوة[9]؛

[8] رجم خالد, مطبوعة نظام المعلومات جامعة ورقلة، 2018، ص15

[9] الطاهر بن عمارة، خالد رجم، أثر نظام الحماية الالكترونية في الحد من مخاطر تكنولوجيا المعلومات والاتصال, مجلة رؤى اقتصادية، جامعة الوادي، 2018 ص 3

الفرع الثاني: عناصر الأمن الالكتروني:

من أجل حماية المعلومات من المخاطر التي تتعرض لها لا بد من توفر مجموعة من العناصر التي يجب أخذها بعين الاعتبار لتوفير الحماية الكافية للمعلومات، ولقد صنفت تلك العناصر إلى خمسة عناصر وهي:

التحقق من المستعمل: التأكد من هوية الشخص الذي يستخدم المعلومات، عن طريق فحص الصلاحيات الالكترونية لكل مستخدم.

سلامة المحتوى: أي التأكد من أن محتوى المعلومات صحيح ولم يحرف، ولتفادي ذلك يجب على المؤسسة تأمين سلامة المحتوى من خلال إتباع وسائل حماية مناسبة مثل البرمجيات والتجهيزات المضادة للاختراقات والفيروسات.

استمرارية توفر المعلومات أو الخدمة: سلامة وامن التخزين والاسترجاع تعني التأكد من استمرارية عمل نظام المعلومات بكل مكوناته واستمرار القدرة على التفاعل وتقديم الخدمات لمستخدمين المرخص لهم بها، ومنع استخدامها أو الوصول إليها بطرق غير مشروعة.

المسؤولية: إمكانية تتبع الأثر في حالات التغيير والتحريف والحذف. ويقصد به ضمان توفر طريقة أو وسيلة لإثبات أي تصرف يقوم به أي شخص في وقت معين.

السرية أو الموثوقية: أي التأكد من أن المعلومات لا يمكن الاطلاع عليها من قبل أشخاص غير مصرح لهم.[10]

الفرع الثالث: متطلبات أمن نظم المعلومات:

تعتبر مسألة حماية أمن نظم المعلومات من المسائل الهامة والضرورية والتي ينبغي على المؤسسة أخذها بعين الاعتبار ووضع خطة حماية شاملة في حدود إمكانياتها التنظيمية والمادية ويجب أن تكون تلك الحماية قوية وليست ضعيفة ولذلك فإنه توجد عدة متطلبات لحماية أمن نظم المعلومات:[11]

-وضع سياسة حماية عامة لأمن نظم المعلومات تتحدد حسب طبيعة عمل وتطبيقات المنشأة؛

-يجب على الإدارة العليا في المنشأة دعم أمن نظم المعلومات لديها؛

-يجب أن توكل مسؤولية أمن نظم المعلومات في المؤسسة لأشخاص محددين؛

-تحديد الحماية اللازمة لنظم التشغيل والتطبيقات المختلفة؛

-تحديد آليات المراقبة والتفتيش لنظم المعلومات والشبكات الحاسوبية؛

-الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن ؛

-تشفير المعلومات التي يتم حفظها و تخزينها ونقلها على مختلف الوسائط؛

-تأمين استمرارية عمل وجاهزية نظم المعلومات خاصة في حالة الأزمات ومواجهة المخاطر المتعلقة بنظم المعلومات.

المطلب الثالث : مخاطر وتهديدات نظم المعلومات:

تواجه نظم المعلومات العديد من المخاطر التي قد تؤثر على تحقيق أهداف الشركات وذلك لاعتمادهم على الحاسوب،حيث تزامن تطور أنظمة المعلومات مع التطور في تكنولوجيا المعلومات وسرعة انتشار المعلومات واستخدامها الكترونيا ، ولقد صاحب هذا

[10] الطاهر بن عمارة ,رجم خالد, مرجع سابق, ص 4

[11] المرجع السابق، ص 4

التطور في استخدام المعلومات الالكترونية العديد من المخاطر والمشاكل التي تؤثر على أمن المعلومات سواء كانت تلك المخاطر مقصودة أو غير مقصودة .

الفرع الأول: ماهية مخاطر نظام المعلومات:

تتجه العديد من الشركات إلى الاعتماد على التكنولوجيا المعلومات من خلال نظم معلومات متكاملة، والتي تؤدي إلى دقة وسرعة تشغيل العمليات، وبالتالي تحقيق العديد من المزايا التنافسية للشركات، ومع ذلك فإنه تطبيق تكنولوجيا المعلومات يصاحبه العديد من المخاطر.

وتعرف المخاطر بصفة عامة بأنها احتمال وقوع حدث ما أو تصرف ما من شأنه أن يؤدي إلى فشل المنظمة في تحقيق أهدافها وهناك العديد من المخاطر التي تواجه الشركات، تتمثل في الآتي: [12]

- المخاطر الاستراتيجية Strategic Risk
- المخاطر البيئية Environmental Risk
- مخاطر السوق Market Risk
- مخاطر التشغيل Operational Risk
- مخاطر الائتمان Credit Risk
- مخاطر الالتزام Compliance Risk

وتعد مخاطر تكنولوجيا المعلومات أحد أنواع المخاطر التي تواجه الشركات، والتي قد تكون جزء من أحد المخاطر السابقة.

وتعرف مخاطر تكنولوجيا المعلومات بصفة خاصة على أنها " كل ما ينتج عنه وجود خطأ أو خلل في تكنولوجيا المعلومات تؤدي إلى تأثير سلبي على أعمال المنظمة، ولقد جاء تعريف جمعية ومراجعة ومراقبة نظم المعلومات ISACA لمخاطر نظم المعلومات متسقا مع ما سبق، وعرفتها على أنها:

"احتمال حدوث تصرف ما أو حدث ما له تأثير سلبي على المنظمة وعلى نظم المعلومات الخاصة بها ،أي احتمال أن يحدث استغلال لنقاط الضعف في الأصل أو مجموعة من الأصول فيسبب خسائر أو أضرار للأصول"

ويتطلب الكشف عن الأبعاد المختلفة لمخاطر نظم المعلومات تناول المقومات الأساسية لأي نظام معلومات وهي:[13]

1- **الأفراد:** وهم الدين يقومون بتشغيل النظام، وأداء الوظائف المختلفة.

2- **الإجراءات:** تتضمن تلك الإجراءات سواء في النظام اليدوي أو النظام الآلي تجميع وتشغيل وتخزين البيانات عن أنشطة المنظمة.

3- **البيانات:** وهي تتعلق بالعمليات التي تقوم بها المنظمة.

4- **البرامج:** وهي التي تستخدم في تشغيل بيانات النظام.

5- **البنية التحتية لتكنولوجيا المعلومات:** وهي تشمل أجهزة الكمبيوتر، وملحقاتها، ووسائل اتصالات الشبكات.

وتتسم أسباب مخاطر تكنولوجيا المعلومات والآثار الناتجة عنها بالتعقيد، وبصفة خاصة في المنظمات كبيرة الحجم، ويمكن تقسيم أسباب مخاطر تكنولوجيا المعلومات إلى أسباب خارجية، وأسباب داخلية مصدرها البيئة الداخلية.

---

[12] علاء محمد شوقي ابراهيم عيسى، **تأثير تطبيق حوكمة الشركات على مخاطر نظم المعلومات**، دار الجزائرية للنشر والتوزيع،2015 ص 63

[13] مصطفلى فتحي، **أمن المعلومات**، دورة علمية، المنظمة العربية للتنمية الإدارية، 2010 ص 10

الفرع الثاني: مخاطر نظم المعلومات:

أولا: من حيث مصدرها: توجد عدة مخاطر لنظم المعلومات تختلف من حيث المصدر:[14]

1-مخاطر داخلية: حيث يعتبر موظفي المنشآت هم المصدر الرئيسي للمخاطر الداخلية التي تتعرض لها نظم المعلومات المحاسبية الإلكترونية ودلك لأن موظفي المنشآت على علم ومعرفة بمعلومات النظام وأكثر دراية من غيرهم بالنظام الرقابي المطبق لدى المنشأة، ومعرفة نقاط القوة والضعف ونقاط القصور لهدا النظام ويكون لديهم القدرة على التعامل مع المعلومات والوصول إليها من خلال صلاحيات الدخول الممنوحة لهم، ولدلك فإن موظفي الشركة غير الأمناء يستطيعون الوصول للبيانات وإمكانية تدميرها أو تحريفها أو تغييرها.

2-مخاطرخارجية: وتتمثل في أشخاص خارج المنشأة ليس لهم علاقة مباشرة بالمنشأة مثل قراصنة المعلومات والمنافسين الدين يحاولون اختراق الضوابط الرقابية والأمنية للنظام بهدف الحصول على معلومات سرية عن المنشأة أو قد تتمثل في كوارث طبيعية مثل الزلزال والبراكين والفيضانات والتي قد تحدث تدمير جزئي أو كلي للنظام في المنشأة.

ثانيا: من حيث المتسبب لها:

1-مخاطر ناتجة عن العنصر البشري: وتلك الأخطاء قد تحدث من قبل أشخاص بشكل مقصود وبهدف الغش والتلاعب أو بشكل غير مقصود نتيجة الجهل أو السهو أو الخطأ.

2-مخاطر ناتجة عن العنصر غير البشري: وهي تلك الأخطاء قد تحدث بسبب كوارث طبيعية ليس للإنسان علاقة بها مثل حدوث الزلزال والبراكين والفيضانات والتي قد تؤدي إلى تلف النظام ككل أو جزء منه.

ثالثا: من حيث العمدية (القصد):

1-مخاطر ناتجة عن تصرفات معتمدة (مقصودة): وتتمثل في تصرفات يقوم بها الشخص متعمدا مثل إدخال بيانات خاطئة وهو يعلم دلك، أو قيامه بتدمير بعض البيانات متعمدا دلك بهدف الغش والتلاعب والسرقة، وتعتبر هده المخاطر من المخاطر المؤثرة جدا على النظام.

2-مخاطر ناتجة عن تصرفات غير معتمدة (غير مقصودة): 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 هده المخاطر أقل ضررا من المخاطر المقصودة ودلك لإمكانية إصلاحها.[15]

رابعا: من حيث الآثار الناتجة عنها: تتعدد وتتفرق المخاطر من حيث الآثار الناتجة عنها:[16]

1-مخاطر تنتج عنها أضرار مادية: وهي المخاطر التي تؤدي إلى حدوث أضرار للنظام وأجهزة الكمبيوتر أو تدمير لوسائل تخزين البيانات والتي قد يكون سببها كوارث طبيعية لا علاقة للإنسان بها أو قد تكون بسبب البشر بطريقة معتمدة أو عفوية.

---

[14] حرية شعبان محمد الشريف، **مخاطر نظم المعلومات المحاسبية الإلكترونية "دراسة تطبيقية على المصارف العاملة في قطاع غزة "، مدكرة** ماجستير منشورة، كلية التجارة بالجامعة الإسلامية بغزة، 2006 ص84

[15] حورية شعبان محمد الشريف, مرجع سبق ذكره ص85

[16] رجم خالد، **تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية** مرجع سبق ذكره ، ص 71

2-مخاطر فنية ومنطقية: وهي المخاطر الناتجة عن أحداث قد تؤثر على البيانات وإمكانية الحصول عليها للأشخاص المخول لهم بذلك عند الحاجة لها أو إفشاء بيانات سرية لأشخاص غير مصرح لهم بمعرفتها وذلك من خلال تعطيل في ذاكرة الكمبيوتر أو إدخال فيروسات للكمبيوتر قد تفسد البيانات أو جزء منها وتلك المخاطر قد تؤثر على الموقف التنافسي للمنشأة وقد تحدث المخاطر السابقة من خلال قيام المهاجم بالبحث في مخلفات التقنية الخاصة بالمؤسسة من قمامة وأوراق متروكة بهدف الحصول على أي معلومات قد تساعد على اختراق النظام للحصول على كلمات السر المدونة على الأوراق الملقاة أو الأقراص الصلبة التي يتم استبدالها ، أو أي معلومة أخرى تساهم في اختراق النظام والتي تعرف بتقنية القمامة ، ونستطيع أن ندرك درجة خطورة تقنية القمامة من خلال معرفة ما حصل مع وزارة العدل الأمريكية.

حيث قامت وزارة العدل الأمريكية ببيع مخلفات أجهزة تقنية بعد أن تقرر إتلافها وكان من ضمن تلك المخلفات جهاز كمبيوتر يحتوي قرصه الصلب على كافة العناوين الخاصة ببرنامج حماية الشهود وخوفا من نشر تلك المعلومات أو استثمارها ضد الوزارة فقد قامت وزارة العدل بنقل كافة الشهود وتغيير مكان إقامتهم وهوياتهم وهدا تطلب تكلفة مالية ضخمة ودلك بسبب الإخفاق في إتلاف الأقراص بطريقة صحيحة.

خامسا: المخاطر من حيث علاقتها بمراحل النظام: لمخاطر علاقة من حيث مراحل نظم المعلومات ندكر منها:[17]

1-مخاطر المدخلات: 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:

أ-خلق بيانات غير سليمة:

ويتم دلك من خلال خلق بيانات غير حقيقية ولكن بواسطة مستندات صحيحة يتم وضعها داخل مجموعة من العمليات دون أن يتم اكتشافها، ومثال دلك استخدام أسماء وهمية لموظفين لا يعملون بالشركة وإدراج تلك الأسماء ضمن كشوف الرواتب وصرف رواتب شهرية لهم أو إدخال فواتير وهمية باسم أحد الموردين.

ب-تعديل أو تحريف بيانات المدخلات:

ويتم ذلك من خلال التلاعب في المدخلات والمستندات الأصلية بعد اعتمادها من قبل المسؤول وقبل إدخالها إلى النظام، ودلك عن طريق تغيير في أرقام مبالغ بعض العمليات لصالح المحرف، أو تغير أسماء بعض العملاء أو معدلات الفائدة.

ج-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، ومثال ذلك قيام الموظف المسؤول عن المرتبات في المنشأة بتدمير مذكرات وتعديلات تفصيلات حساب البنك لحساب آخر خاص بالموظف الحرف.

د-إدخال البيانات أكثر من مرة:

---

[17] صام محمد البحيصي و أ. حرية شعبان الشريف **مخاطر نظم المعلومات المحاسبية الإلكترونية: دراسة تطبيقية على المصارف العاملة في قطاع غزة** "مجلة الجامعة" الجامعة الاسلامية (سلسلة الدراسات الإنسانية) المجلد السادس عشر، العدد الثاني، 2008الجامعة الإسلامية – غزة – فلسطين ص 904- 905

والمقصود بذلك قيام الموظف بتكرار إدخال البيانات إلى الحاسب إما بطريقة مقصودة أو غير مقصودة، ويتم ذلك من خلال إدخال بيانات بعض المستندات أكثر من مرة إلى النظام قبل أوامر الدفع وذلك إما بعمل نسخ إضافية من المستندات الأصلية وتقدم كل من الصورة والأصل أو إعادة لإدخال البيانات مرة أخرى إلى النظام.

2-مخاطر تشغيل البيانات: ويقصد بها المخاطر المتعلقة بالبيانات المخزنة في ذاكرة الحاسب والبرامج التي تقوم بتشغيل تلك البيانات وتتمثل مخاطر تشغيل البيانات في الاستخدام غير المصرح به لنظام وبرامج التشغيل وتحريف وتعديل البرامج بطريقة غير قانونية أو عمل نسخ غير قانونية أو سرقة البيانات الموجودة على الحاسب الآلي، ومثال على ذلك قيام الموظف 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.

3-مخاطر مخرجات الحاسب: 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 أو عمل نسخ غير مصرح بها من المخرجات أو الكشف الغير مسموح به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق أو طبع و توزيع المعلومات بواسطة أشخاص غير مسموح لهم بذلك، كذلك توجيه تلك المطبوعات والمعلومات خطأ إلى أشخاص ليس لهم الحق في الاطلاع على تلك المعلومات أو تسليم المستندات الحساسة إلى أشخاص تتوافر فيهم الناحية الامنية بغرض تمزيقها أو التخلص منها مما يؤدي إلى استخدام تلك المعلومات في أمور تسيء إلى المؤسسة وتضر بمصالحها.

سادسا: مخاطر نظم المعلومات حسب الغرض منها:

تتعرض نظم المعلومات الحاسوبية إلى العديد من الأخطار والتهديدات التي قد تهدد أمن نظم معلوماتها، وقد تتنوع مصادر تلك التهديدات بحسب الأغراض التي تقوم بها تلك النظم ويمكن تصنيف أنواع التهديدات والأخطار بحسب مصادرها إلى أربعة أنواع رئيسية:[18]

- خرق النظم الحاسوبية بهدف الاطلاع على المعلومات المخزنة فيها والوصول إلى معلومات شخصية أو أمنية عن شخص ما أو التجسس الصناعي، أو التجسس المعادي للوصول إلى معلومات عسكرية سرية.
- خرق النظم الحاسوبية بهدف التزوير أو الاحتيال التلاعب بالحسابات في البنوك، التلاعب بفاتورة الهاتف، التلاعب بالضرائب، تغيير بيانات شخصية من السجل المدني أو السدل العام للموظفين، إلخ.
- خرق النظم الحاسوبية بهدف تعطيل هذه النظم عن العمل لأغراض تخريبية باستخدام ما يسمى بالبرامج الخبيثة مثل الفيروسات، الدودة، حصان طروادة، أو القنابل الإلكترونية (إما من قبل الافراد أو العصابات أو الجهات الاجنبية بغرض شل هذه النظم الحاسوبية) أو المواقع على الانترنيت (عن العمل وخاصة في ظروف خاصة أو في أوقات الحرب.
- أخطار ناتجة عن فشل التجهيزات في العمل، أعطال كهربائية، حريق ، كوارث طبيعية(فيضانات، زلزال).

[18] يزيد ذكار، **"تقييم كفاءة نظام المعلومات الإلكتروني"**، مذكرة ماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ورقلة،2016 ص 12

ومن خلال ما سبق تصنيف المخاطر التي تواجه نظم المعلومات الإلكترونية بشكل عام إلى أربعة أصناف رئيسية:

1: **مخاطر المدخلات**: وهي المخاطر التي تتعلق بأول مرحلة من مراحل النظام وهي مرحلة إدخال البيانات إلى النظام الآلي وتتمثل تلك المخاطر في البنود التالية:

- ✓ الإدخال غير المتعمد (غير المقصود) لبيانات غير سليمة بواسطة الموظفين.
- ✓ الإدخال المتعمد (المقصود) لبيانات غير سليمة بواسطة الموظفين.
- ✓ التدمير غير المتعمد للبيانات بواسطة الموظفين.
- ✓ التدمير المتعمد (المقصود) للبيانات بواسطة الموظفين.

2: **مخاطر تشغيل البيانات**: وهي المخاطر التي تتعلق بالمرحلة الثانية من مراحل النظام وهي مرحلة تشغيل ومعالجة البيانات المخزنة في ذاكرة الحاسب وتتمثل تلك المخاطر في البنود التالية:[19]

- المرور (الوصول غير الشرعي وغير المرخص به) للبيانات والنظام بواسطة الموظفين.
- المرور غير الشرعي (غير المرخص به) للبيانات والنظام بواسطة أشخاص من خارج المنشأة.
- اشتراك العديد من الموظفين في نفس كلمة السر.
- إدخال فيروسات الكمبيوتر للنظام المحاسبي والتأثير على عملية تشغيل بيانات النظام.
- اعتراض وصوول البيانات من أجهزة الخوادم إلى أجهزة المستخدمين.

3: **مخاطر مخرجات الحاسب**: وتلك المخاطر تتعلق بمرحلة مخرجات عمليات معالجة وتشغيل البيانات وما يصدر عن هذه المرحلة من قوائم للحسابات أو أشرطة ملفات ممغنطة وكيفية استلام تلك المخرجات، وتتمثل تلك المخاطر في البنود التالية:

- ❖ طمس أو تدمر بنود معينة من المخرجات.
- ❖ خلق مخرجات زائفة / غير صحيحة.
- ❖ سرقة البيانات / المعلومات.
- ❖ عمل نسخ غير مصرح(مرخص) بها من المخرجات.
- ❖ الكشف غير المرخص به للبيانات عن طريق عرضها على شاشت العرض أو طبعها على الورق.
- ❖ طبع وتوزيع المعلومات بواسطة أشخاص غير مصرح لهم بذلك.
- ❖ المطبوعات والمعلومات الموزعة يتم توجيهها خطأ إلى أشخاص غير مخول لهم/ ليس لهم الحق في استلام نسخة منها.
- ❖ تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الامنية بغرض تمزيقها أو التخلص منها.

[19] رجم خالد، **محاضرات امن المعلومات**، مقياس نظام المعلومات سنة أولى ماستر تدقيق ومراقبة التسيير، جامعة ورقلة، 2015-2016

4: مخاطر بيئية: وهي المخاطر التي تحدث بسبب عوامل بيئية، مثل الزلزال والعواصف والفيضانات والاعاصير المتعلقة بأعطال التيار الكهربائي والحرائق، سواء كانت تلك الكوارث طبيعية أو غير طبيعية فإنها قد تؤثر على عمل النظام وقد تؤدي إلى تعطل عمل التجهيزات وتوقفها لفترات طويلة مم يؤثر على أمن وسلامة نظم المعلومات الإلكترونية.

الفرع الثالث: أسباب حدوث مخاطر نظم المعلومات:

تتعرض نظم المعلومات للعديد من المخاطر التي تهدد أمنها وقد قمنا بتقسيم تلك المخاطر إلى أربعة أقسام رئيسية تتعلق بمراحل النظام الأساسية من إدخال وتشغيل ومخرجات والقسم الرابع يتعلق بالمخاطر البيئية وقد ترجع أسباب حدوث تلك المخاطر إلى أسباب تتعلق بالمدخلات والمخرجات وأسباب تتعلق بالتشغيل أو قد نعتبرها أسباب إدارية رقابية وأسباب لها علاقة بالموظفين، **وتتلخص تلك الاسباب في البنود التالية:**[20]

- ✓ عدم كفاية وفعالية الأدوات الرقابية المطبقة لدلى إدارة المنشأة.
- ✓ ضعف نظام الرقابة الداخلية لدى المنسأة وعدم فعاليتها.
- ✓ اشتراك بعض الموظفين في استخدام نفس كلمات السر من أجل الدخول إلى النظام والعبث بمحتوياته.
- ✓ عدم الفصل بين المهام والوظائف المتعلقة بنظم المعلومات في المنشأة.
- ✓ عدم وجود سياسات واضحة وبرامج محددة ومكتوبة فيما يختص بأمن نظم المعلومات المحاسبية لدى المنشأة.
- ✓ عدم توفر الحماية الكافية ضد مخاطر فيروسات الكمبيوتر.
- ✓ ضعف وعدم كفاءة النظم الرقابية المطبقة على مخرجات الحاسب.
- ✓ عدم وجود سياسات وبرامج محددة ومكتوبة لأمن نظام المعلومات.
- ✓ عدم التوصيف الدقيق للهيكل الوظيفي والإداري الذي يحدد المسؤوليات والصلاحيات لكل شخص داخل الهيكل التنظيمي لدى المنشأة.
- ✓ عدم توافر الخبرة اللازمة والتدريب الكافي والخلفية العلمية والمهارات المطلوبة لتنفيذ الاعمال من قبل موظفي المنشأة.
- ✓ عدم إلزام الموظفين بأخذ إجازاتهم الدورية.
- ✓ عدم الاهتمام الكافي بفحص التاريخ الوظيفي المهني للموظفين الجدد قد يؤثر على قاعدة وضع الرجل المناسب في المكان المناسب.
- ✓ عدم الاهتمام بدراسة المشاكل الاقتصادية والاجتماعية والنفسية لموظفي المنشأة.

---

[20] حرية شعبان محمد الشريف، **مخاطر نظم المعلومات المحاسبية الإلكترونية "دراسة تطبيقية على المصارف العاملة في قطاع غزة "، مذكرة** ماجستير منشورة، كلية التجارة بالجامعة الإسلامية بغزة، 2006 ص84

الفرع الرابع: تهديدات نظم المعلومات:

تتعدد الوسائل وأساليب القرصنة في الاختراق الامن المعلوماتي،إلا أنها في مجملها تهدف إلى مهاجمة هذه الأهداف وتحقيق نفع معين للمهاجم من وراء ذلك، وفي بعض الأحيان لا يكون الهدف من الاختراق نفع معين للمهاجم سوى تعريض المستهدف الخطر والضرر، تحدث المشكلة الأمنية عندما يتم اختراق النظام لديك من خلال أحد المهاجمين أو المتسللين (الهاكر) أو الفيروسات أو نوع آخر من البرامج الخبيثة ومن أهم الاساليب والطرق ما يلي:

أولا: البرامج الخبيثة:

وهي عبارة عن برامج تم إعدادها من قبل مبرمجين وذلك لغرض إلحاق الضرر بالبيانات المستهدفة كتخريبها وإزالتها أو السيطرة عليها وإلحاق الضرر بها. وتتميز هذه البرامج بقدرتها على التناسخ والانتشار والانتقال من مكان إلى آخر. ويمكن تقسيم هذه البرامج إلى عدة أنواع وذلك بحسب سلوكها.[21]

ثانيا: أنواع الهجوم Attacks:

توجد مجموعة من الهجومات التي يستعملها المتجسسون على المستهدفون من أجل إلحاق الضرر وتجسس على نظام المعلومات ونذكر منها:[22]

1-هجوم التصنت على الرسائل: Attacks Interception

وفكرة عمل هذا الهجوم: أن المهاجم يراقب الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهو ما يسمى بالتصنت على الاتصال Eavesdropping

2-هجوم توقيف: Interruption Attacks

وهذا النوع يعتمد على قطع قناة الاتصال إيقاف الرسالة أو البيانات من الوصول إلى المستقبل وهو ما يسمى أيضا برفض الجدمة.[23]

3-هجوم يعدل على محتوى الرسالة: Modification Attacks

فإنه هنا يتدخل المهاجم بين المرسل والمستقبل يعتبر وسيط بين المرسل والمستقبل وعندما تصل إلى Attacker يقوم بتغيير محتوى الرسالة ومن ثم إرسالها إلى المستقبل، والمستقبل طبعا يعلم بتعديل الرسالة من قبل Attacker.

4-الهجوم المزور أو المفبرك:Fabrication Attacks

وهنا يرسل المهاجم رسالة مفادها أنه صديقه ويطلب منه معلومات أو كلمات سرية خاصة بالشركة.[24]

---

[21] مصطفى فتحي، **أمن المعلومات**، دورة علمية، المنظمة العربية للتنمية الإدارية، 2010 ص 13

[22] مصطفى فتحي، نفس المرجع ص 13

[23] رجم خالد، **محاضرات امن المعلومات**، مرجع سبق ذكره 2015- 2016

[24] رجم خالد، محاضرات امن المعلومات , مرجع سبق ذكره

المبحث الثاني: الدراسات السابقة:

المطلب الأول: الدراسات السابقة باللغة العربية :

الفرع الأول: دراسة (أبو موسى سنة 2004) **بعنوان "المخاطر الهامة التي تهدد أمن نظام المعلومات المحاسبية الإلكترونية في المنشآت السعودية – دراسة تطبيقية "** وهدفت الدراسة إلى التركيز حول أهمية المخاطر التي تواجه أمن نظام المعلومات المحاسبية الإلكترونية في المنشآت السعودية وأنواع تلك المخاطر ودلك من أجل دراستها و التعرف على الإجراءات اللازمة من أجل مواجهتها، وأستخدم الباحث المنهج البحثي الوصفي التحليلي، وتكون مجتمع الدراسة من العاملين على نظم المعلومات في المنشأة وجمعت أدوات الدراسة بين الاستبانة والمقابلة ، حيث توصلت الدراسة إلى مجموعة من النتائج أهمها، اكتشاف نسبة كبيرة من التلاعبات و الاختلاسات والتعديات على أمن نظام المعلومات المحاسبية لعدم كفاية وفعالية الأدوات و

الضوابط الرقابية المطبقة في المنشأة وأن معظم هده التلاعبات و الاختلاسات التي تم اكتشافها قد تم تسويتها داخليا ولم يتم الإفصاح أو التقرير عنها للجمهور حفاظا على سمعة الشركة و تحسين صورتها في السوق .

الفرع الثاني: دراسة (بشرى علي زينل سنة 2012) **بعنوان "فعالية التدريب في تحقيق نجاح أمن نظام المعلومات – دراسة استطلاعية لآراء عينة من العاملين في نظم المعلومات –جامعة الموصل"** وهدفت الدراسة إلى بيان مدى فعالية التدريب ومساهمته في تحقيق النجاح للعاملين في نظم المعلومات و حمايتها وتهدف إلى تحديد مدى توافر البنية التحتية و الإمكانيات المادية و البرمجية ، وأستخدم الباحث في جانبه العلمي المنهج الوصفي التحليلي، إد تم توزيع 55 استمارة استبانة على مجموعة من العاملين في مجال نظم المعلومات من منتسبي جامعة الموصل ، حيث توصلت الدراسة إلى مجموعة من النتائج أهمها، وجود تباين على مستوى الجنس و الخبرة العملية المباشرة في إجابات أفراد العينة حول موضوع أمن نظام المعلومات ، في حين لم تظهر النتائج أي تباين فب إجابات العينة من المتدربين وغير المتدربين حول هدا الموضوع .

الفرع الثالث: دراسة (رجم خالد سنة2018) **بعنوان "أثر نظام الحماية الإلكتروني في الحد من مخاطر تكنولوجيا المعلومات و الاتصال–دراسة مقارنة لعينة من المؤسسات "** و تهدف هده الدراسة إلى تقييم مدى مساهمة نظام الحماية الإلكتروني في الحد من مخاطر تكنولوجيا المعلومات و الاتصال دراسة مقارنة لعينة من المؤسسات في ولاية ورقلة ، حيث تم الاعتماد على المنهج الوصفي التحليلي باستخدام كل من أداة المقابلة و الاستبيان حيث تمثلت عينة الدراسة في ثلاثة مؤسسات اتصالات الجزائر سونلغاز ، ليند غاز ، بمجمل 222 استبيان موجه إلى مسيري و مستخدمي تكنولوجيا المعلومات و الاتصال في المؤسسة كانت نسبة الاستجابة 79% ، كما تم الاعتماد في تحليل بيانات الاستبانة على برنامج الحزمة الإحصائية للعلوم الاجتماعيةSpss ، حيث توصلت الدراسة إلى مجموعة من النتائج أهمها ،تعرض المؤسسات إلى عدة مخاطر تهدد أمن نظم المعلومات الإلكترونية و فعالية السياسات الأمنية و ضوابط للموظفين داخل
المؤسسة من شأنه ضمان الحد من مخاطر استخدام تكنولوجيا المعلومات و الاتصال بالإضافة إلى أن عملية التكوين في مجال الأمن الإلكتروني في المؤسسات به عدة اختلالات و نقائص انطلاقا من تحديد احتياجات التكوين حد داته .

الفرع الرابع: دراسة (حرية شعبان محمد الشريف 2006) **بعنوان "مخاطر نظم المعلومات المحاسبية الإلكترونية دراسة تطبيقية على المصارف العاملة في قطاع غزة"** تهدف هذه الدراسة إلى التعرف على المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، والتعرف على أهم الأسباب التي تؤدي إلى حدوث تلك المخاطر والإجراءات التي تحول دون وقوع تلك المخاطر حيث استعانت الباحثة بما تناولته الدراسات السابقة والأبحاث التي اهتمت في هذا المجال، كذلك تم التعرف على الإجراءات والوسائل الرقابية المتبعة من قبل المصارف العاملة في قطاع غزة لمواجهة تلك المخاطر التي قد تواجه نظم معلوماتها المحاسبية الالكترونية وبناء على ذلك تم استخلاص بعض النتائج التي تسهم في التعرف على أهم المخاطر التي تواجه نظم المعلومات المحاسبية الالكترونية في المصارف العاملة في قطاع غزة، وتقديم التوصيات في هذا المجال كما استخدمت الدراسة المنهج الوصفي التحليلي في الوصول لنتائج الدراسة، حيث تم توزيع استبانه على المصارف العاملة في قطاع غزة وفروعها وقد تم استخدام برنامج التحليل الإحصائي(SPSS) للعلوم الإنسانية والاجتماعية لمعالجة البيانات باستخدام التكرارات والنسب المئوية،

والمتوسطات الحسابية، واختبار الإشارة إلي معلمي (Sign Test)وقد تم التوصل إلى مجموعة من النتائج أهمها ،أوضحت الدراسة قلة عدد موظفي تكنولوجيا المعلومات في المصارف العاملة في قطاع غزة حيث يعتمد الفروع على موظف واحد مهمته تشغيل أنظمة الحاسوب بينما الموظفين المختصين يكون مكانهم في المراكز الرئيسية للفروع وغالبا ما توجد في الضفة الغربية ، وأن الإدارة الجيدة تستطيع أن تقلل أو تحد من حدوث المخاطر التي تواجه نظم المعلومات المحاسبية لدى المصارف ، وأن تطبيق إجراءات أمن النظم المعلوماتية يقلل من إمكانية حدوث مخاطر نظم المعلومات المحاسبية.

الفرع الخامس : دراسة (مقراني قدور 2015) **بعنوان "تقييم مدى مساهمة أمن نظم المعلومات الكترونية في الحد من مخاطر نظم المعلومات دراسة حالة مؤسسة اتصالات الجزائر** " هدفت هذه الدراسة إلى تقييم أمن نظام المعلومات في مؤسسة اتصالات الجزائر،حيث إلى تطرقت إلى المخاطر المحدقة بنظام المعلومات والإجراءات التي من شانها الحد من هذه المخاطر،ومن محاولة إسقاط هذه المعطيات على نظام المعلومات داخل المؤسسة المعينة بالدراسة،وقد اعتمد الباحث على المنهج الوصفي في الجانب النظري من أجل تسليط الضوء على نظم المعلومات ومخاطرها والعناصر الأمنية، وأثناء إعداد هذه الدراسة تم توزيع الاستبيان الذي تمثل في 100استمارة أهم النتائج المتوصل إليها هي أن السياسات الأمنية داخل نظام المعلومات من شانها ضمان ديمومة عمل هذا النظام في ظروف مثلى مع إشراك العامل البشري في هذه السياسات.

المطلب الثاني: الدراسات السابقة باللغة الأجنبية :

الفرع الأول:دراسة (الباحثان **RYAN** and **BORDOLOI** سنة 1997) **بعنوان "تقييم مخاطر أمن نظام المعلومات في النظم المحاسبية الإلكترونية في المنشآت التي تحولت من نظام أجهزة الكمبيوتر الكبيرة الى نظام خدمة العملاء –دراسة تطبيقية"** وهدفت الدراسة إلى قيام البحثان بتطوير قائمة شملت خمسة عشر من المخاطر المحتملة التي قد تهدد أمن نظام المعلومات الإلكترونية بناءا على الدراسات السابقة و أبحاث تمت في هدا الشأن، وأستخدم الباحث في جانبه العلمي المنهج الوصفي التحليلي، إد تم توزيع عدد من الاستبيانات من أجل القيام بترتيب مدى خطورة و أهمية المخاطر المحتملة لأمن نظم المعلومات المحاسبية الإلكترونية في بيئة أجهزة الحاسب الألي الكبيرة و كدلك في نظام خدمة العملاء ، حيث توصلت الدراسة إلى مجموعة من النتائج أهمها، وجود فروق جوهرية بين المنشآت التي لديها نظام أجهزة الكمبيوتر و تلك التي تطبق نظام خدمة العملاء فيما يختص بمخاطر أمن نظم المعلومات المحاسبية

الفرع الثاني:دراسة (الباحث **MICHAEL E.WHITMAN** سنة 2003) **بعنوان "درجة خطورة التهديدات التي تواجه أمن نظام المعلومات وعدد مرات حدوثها"** وهدفت الدراسة إلى تركيز الباحث للإجابة على ثلاثة أسئلة كالآتي : السؤال الأول يتعلق بحصر التهديدات التي تواجه أمن المعلومات و السؤال الثاني يتعلق بدرجة خطورة هده التهديدات والسؤال الثالث يتعلق بعدد مرات حدوثها ، ثم قام الباحث بعمل دراسة مسحية 1000 موظف أغلبهم من مدراء نظم المعلومات و المدراء المشرفين ، حيث توصلت الدراسة إلى مجموعة من النتائج أهمها، أن الهجوم المعتمد للبرمجيات و حالات فشل أو أخطاء البرامج التقنية و الخطأ أو الفشل البشري قد تم تصنيفهما ضمن الثلاث مخاطر الهامة في جميع بيئات تكنولوجيا المعلومات .

الفرع الثالث:دراسة (الباحث **LOCH و آخرون** سنة 1992) **بعنوان "المخاطر الأمنية التي تواجه أمن النظم المحاسبية الإلكترونية في بيئة الحاسبات الشخصية و الحاسبات الكبيرة و الحاسبات الإلكترونية– الولايات المتحدة "** وهدفت الدراسة إلى تطوير قائمة تضمنت اثني عشر من المخاطر المحتملة التي قد تواجه أمن نظم المعلومات المحاسبية الإلكترونية بناءا على الأبحاث النظرية المتاحة وكذلك محاولة إختبار مدى وجود و أهمية تلك الخاطر عمليا من خلال البحث الميداني، ثم قام الباحثون بعمل دراسة مسحية 257 أغلبهم من مديري نظم المعلومات الإدارية ، حيث توصلت الدراسة إلى مجموعة من النتائج أهمها، أن الوارث الطبيعية و الأحداث غير المقصودة لموظفي المنشأة قد تم تصنيفها ضمن الثلاث مخاطر الهامة في جميع بيئات تكنولوجيا المعلومات، كما أعطى المشاركون في الدراسة أهمية أكبر للمخاطر الداخلية مقارنة بالمخاطر الخارجية لأمن نظم المعلومات المحاسبية الإلكترونية.

الفرع الرابع:(دراسة (**Kreicberga 2010**) **بعنوان" التهديدات الداخلية لأمن المعلومات–التدابير المضادة والعنصر البشري"** تحدد الغرض العام من الدراسة لاستيضاح المعرفة حول دور العامل البشري في حقل أمن نظم المعلومات وتساءلت الدراسة حول العوامل التي تؤثر على السلوك الأمني للموظفين ؟ ،
وكيف ينظروا تجاه التدابير الأمنية المضادة للتهديدات الداخلية ؟ واستخدم المنهج الكيفي النوعي) وكانت أداة المقابلة التي أجريت مع مسؤولي أمن المعلومات والمستخدمين بالإضافة لم لمراجعة وتحليل الوثائق والمستندات ، والملاحظة المباشرة لسلوك المستخدمين وتوصلت الدراسة إلى ، رضا وقبول الموظفين والتدابير الأمنية عناصر مهمة في تحقيق سلوك أمن تجاه أمن نظم المعلومات، وأن يواجه الموظفون صعوبة ومقدار من التعقيد في فهم الوثائق المتعلقة بأمن المعلومات، تطبيق المتطلبات البشرية لأمن المعلومات يحتاج إلى حالة وعي بأهمية أمن نظم المعلومات.

الفرع الخامس: دراسة (**Lan 2007**) **بعنوان": إدارة أمن نظم المعلومات في الجامعات الاسترالية"** هدفت الدراسة إلى معرفة واقع إدارة أمن نظم المعلومات في الجامعات الأسترالية، وما هي العوامل الأساسية التي تؤثر في فعاليتها، وكيف يمكن تحسينها، وأجريت الدراسة على38 جامعة أسترالية، وطرحت الأسئلة على رئاسات الجامعات ومديري أقسام تكنولوجيا المعلومات ومسئولي أمن المعلومات، عبر مقابلة استخدم فيها أسلوبي الأسئلة المفتوحة والمغلقة، وتوصلت الدراسة للنتائج التالية: يختلف واقع إدارة أمن المعلومات من جامعة لأخرى ويعود ذلك لعدة عوامل منها،منهجية الإدارة الأمنية، واهتمام الإدارة العليا وانخراطها، وحجم الإنفاق على أمن المعلومات، والجهد المبذول على مواجهة التهديدات الأمنية، ومستوى أهمية تكنولوجيا المعلومات، والثقافة العامة للمؤسسة ، أهم العوامل المؤثرة في فاعلية دور إدارة أمن المعلومات تعود لأسباب :

نقص الخبرات وضعف هيكلية إدارة أمن المعلومات، و وجود فجوة بين ما هو مأمول وما هو معمول به من وعي بأمن المعلومات وسبب ذلك هو قلة الاكتراث بالمخاطر والتهديدات، وتطوير السياسات الأمنية بشكل واضح وقابل للعمل ويتم الامتثال له ضمن القواعد الأمنية والقانونية, وأن للتغلب على ضعف إدارة أمن نظم المعلومات فأنه من الضروري تطوير فاعلية العناصر والكوادر البشرية كأحد أهم مرتكزات إدارة أمن نظم المعلومات.

الفرع السادس: دراسة (**2015 Mwita Simion Maroa**) **بعنوان" العوامل المؤثرة في فعالية أمن نظم المعلومات في جامعة نيروبي"** عالجت هذه الدراسة العوامل المؤثرة في أمن المعلومات أخذت كدراسة حالة جامعة نيروبي،بمحاولة قياس أثر السياسات الأمنية على الفعالية الأمنية المتبعة في الجامعة نيروبي،وقد تمثل مجتمع الدراسة المستهدف جميع مستعملي نظام المعلومات في جميع الكليات والإدارات الملحقة بجامعة نيروبي لسنة 2015, واستعملت الدراسة المنهج الوصفي ,كما استعمل الباحث أسلوب الاستبيان حيث تم توزيع استبيان 130, وتمكن استرجاع 120 وقد توصل الباحث إلى أهم النتائج وتمثلت في أن دعم الإدارة العليا والسياسات الأمنية لنظم المعلومات وتدريب المستخدمين وزيادة الوعي يؤثرون على فعالية أمن نظم المعلومات في الجامعة نيروبي لكن بدرجات مختلفة ,حيث يزداد تأثير العوامل الثلاثة الأخيرة بقوة مقارنة بعامل دعم الإدارة العليا

المطلب الثالث: مقارنة الدراسات الحالية بالدراسات السابقة :

حاولنا تلخيص أوجه المقارنة بين الدراسة الحالية والدراسات السابقة سواء العربية أو الأجنبية حيث سنوضح نقاط التشابه ونقاط الاختلاف :

جدول رقم (1 –3) : مقارنة بين الدراسات السابقة والدراسات الحالية

	الحالية	السابقة
من حيث الزمان و المكان	أنجزت دراستنا في فترة زمنية 2019 أما بالنسبة للحدود المكانية فكانت بمؤسسة ENAGO	تمت في بيئة عربية وأجنبية وكانت من 1992 الى 2015 حيث شملت الدراسات الأماكن التالية: أستراليا ,الولايات المتحدة ,الجزائر ,غزة،ورقلة،السعودية
من حيث العينة	شملت دراستنا على عينة قدرها 40عامل	استخدمت الدراسات أغلبها العينة

	حيث قمنا باجراء مقابلات مع اطارات موارد البشرية تكنلوجيا الاعلام الألي	عشوائية
من حيث منهج و ادوات الدراسة	لقد حاولنا في دراستنا اسقاط النظري على الواقع حيث استخدمنا الاستبيان و المقابلة اضافة الى دراسة حالة.	استخدمت معظم الدراسات اداتي المقابلة و الاستبيان و من ناحية منهج الدراسة وقد اعتمدت الدراسات على نفس منهج دراستنا الوصفي والتحليلي
من حيث نوع القطاع	استهدفت الدراسة مؤسسة اقتصادية عمومية.	تنوعت الدراسات السابقة بين القطاع الخاص و العام(خدماتية – صناعية- تجارية).
من حيث المتغيرات	اعتمدنا على متغيرين : المتغير المستقل : نظام الامن المعلوماتي المتغير المتبع: مخاطر نظام المعلومات	اعتمدت الدراسات السابقة على كل من المتنغيرات: – واقع ادارة امن المعلومات – العوامل المؤثرة في نظام الامن – فعالية التدريب في تحقيق نجاح أمن نظام المعلومات – مخاطر أمن نظام المعلومات في نظم محاسبية الالكترونية

المصدر : من اعداد الطالبتين

خلاصة الفصل :

ان نظم المعلومات المصدر الرئيسي للإدارة لتزويدها بالمعلومات اللازمة لاتخاذ القرارات المناسبة التي تساعدها على أداء وظائفها بالطريقة الصحيحة والمثلى والوصول إلى الأهداف المطلوبة بأفضل الطرق وأمثلها .

وبعد تقديمنا للجانب النظري للموضوع في الفصل الأول الذي تطرقنا من خلاله الى عموميات حول نظام المعلومات، ومن باب اخر تناولنا نظام الأمن الالكتروني وتطرقنا ايضا للمخاطر التي تتهدد نظام المعلومات عبر عدة تصنيفات كان أهمها المخاطر وتهديدات متعلقة بمراحل النظام من مدخلات ومعالجة ومخرجات، ثم التهديدات التي يتعرض لها النظام ,

سنحاول في الفصل التالي الوقوف على الدراسة الميدانية التي عالجت لأثر نظام الأمن الالكتروني على ادارة مخاطر نظم المعلومات في مؤسسات محل الدراسة.

تمهيد:

حاولنا في الفصل الأول التطرق الى مكونات نظام المعلومات الإلكتروني و كذا إجراءات الحماية من اجل الحد من مخاطر نظم المعلومات ،أما في هذا الفصل سنحاول إسقاط الدراسة النظرية على أرض الواقع، وقدتم اختيار المؤسسة محل الدراسة لملاءمتها للموضوع من حيث توفر نظام معلومات الكرتوني اذ سنحاول تشخيص واقع نظامها المعلوماتي ، والسياسات الأمنية المتبعة ، ومن أجل الوصول إلى ذلك سنتطرق في المبحث الأول لطريقة الدراسة والأدوات المستعملة فيها، و نستعرض أهم النتائج التي توصلنا لها من خلال استعمال أداة المقابلة في تشخيص نظام المعلومات والسياسات الأمنية لمؤسسات محل الدراسة ، وفي المبحث الثاني نقوم بعرض نتائج أداة الاستبيان لمعرفة مدى مساهمة الأمن الكتروني في الحد من المخاطر نظم المعلومات في المؤسسة محل الدراسة .

المبحث الأول : عينة وأدوات الدراسة:

نتطرق في هذا المبحث للعينة والأدوات المستخدمة في هذه الدراسة، حيث يتضمن التعريف بمجتمع وعينة الدراسة، كما يوضح الأدوات الإحصائية والبرامج المستخدمة في الدراسة.

المطلب الأول: عينة ومجتمع الدراسة:

الفرع الأول: مجتمع الدراسة

يتمثل مجتمع الدراسة في جميع مستخدمي نظام المعلومات في مؤسسة ENGEOحاسي مسعود ولاية ورقلة.

الفرع الثاني : عينة الدراسة

قمنا بسحب عينة قصدية (مستخدمي النظام)قدرها(59) ، حيث تم توزيع (70) استبانة ، وقد تم استرجاع (65) حيث تم استبعاد 6.

أولا: التعريف بالمؤسسة الوطنية للجيوفيزياء (ENAGEO)

المؤسسة الوطنية للجيوفيزياء (Enageo): مؤسسة ذات اسهم، راس مالها 7.000.000.000 دج، مؤسسة خدمات في المجال البترولي منبثقة من مجموعة سوناطراك، يقع مقرها الرئيسي في حاسي مسعود ولها فرعين (مقر بومرداس، مقر بولاد فايت)، أنشأت في عام 1981م بموجب المرسوم التنفيذي (المرسوم 172/81 بتاريخ 01-08-1981)، تحت اشراف وزارة والمناجم؛
نشاطها الرئيسي انجاز الدراسات الجيوفيزيائية لطبقات الأرض، ونشاطات ثانوية تتمثل في: الحفر الهيدروليكي، الأشغال الطوبوغرافية، الأشغال الجيوتقنية والجيوفيزياء العامة.

تمت الدراسة بمديرية المعلوماتية والتكنولوجيات الجديدة للمعلومات والاتصالات (DINTIC) من مهامها:
Diretion de l'**I**nfrmatique & **N**ouvelles **T**echnologies de l'**I**nformation et de la **C**ommunication

أ- الإشراف على تصميم وإرسال الشبكات المعلوماتية داخل المؤسسة؛
ب- المساهمة في تحقيق وتنفيذ مختلف المشاريع المتعلقة بالمعلوماتية؛
ج- ضمان السير الحسن لمختلف التطبيقات المعلوماتية وصيانتها، وضمان استمرار عمل نظم المعلومات؛

د- المساهمة في عملية تكوين وتوعية الافراد بمختلف التطبيقات، والصيانة الدورية للاجهزة.

الفرع الثالث : أدوات الدراسة

أولا: الاستبيان

تم الاعتماد على الاستبيان كأداة مكملة للمقابلة، وقد تم تصميمه من خلال اعتمادنا على بعض الاستبيانات المتعلقة بالدراسات السابقة، استخدمنا مقياس ليكرت الثلاثي، وحكم الاستبيان من طرف مجموعة من الأساتذة في كلية العلوم الاقتصادية والعلوم التجارية، وذلك قصد الحصول على تقييم الاستبيان من قبلهم وبغية الاستفادة من آرائهم، وبعد أن تمت عملية التحكيم، والقيام بإجراء التعديلات اللازمة على فقرات الاستبيان ظهر في شكله النهائي (الملحق رقم 1) وقد تم تقسيمه إلى جزئين كما يلي:

الجزء الأول : يشتمل على فقرات الاستبيان، ويتضمن محورين:

- **المحور لأول** : لخاص بمحور نظام الأمن الالكتروني ويتألف من 25 عبارة موزعة من 01 إلى 25، ويتكون من أربعة أبعاد؛
- **المحور الثاني** : يتعلق هذا محتوى مخاطر نظم المعلومات ، وهو يتكون من 11 عبارة موزعة من 26 إلى 36.

الجزء الثاني: الخاص بالخصائص الديمغرافية لكل عامل من الجنس، السن، المستوى التعليمي، المنصب، سنوات الخبرة.

ثانيا : المقابلة

وتعتبر المقابلة من الأدوات المهمة لجمع المعلومات. ولقد تم تصميم اسألة المقابلة أنظر الملحق رقم (02) ممايخدم متغيرات الدراسة ولقد تم اجراء المقابلة مع مسيري نظام المعلومات في المؤسسة (مديرية تكنولوجيا المعلومات وال اتصال)

ثالثا : دراسة الحالة

تم الاعتماد على **دراسة الحالة** من اجل تشخيص واقع مكونات نظام الأمن الالكتروني والتي لها علاقة مباشرة بموضوع الدراسة، والتي تعتبر مصدرا أساسيا ولا يمكن الاستغناء عنه في دراستنا هذه.

الفرع الرابع : البرامج والأدوات الإحصائية

أولا : البرامج الإحصائية

بعد استرداد الاستبيانات من العينة المستجوبة، قمنا بترميزها ثم تفريغها في برنامج EXCEL 2010 ، *ثم تم نسخها في* بحزمة البرامج التطبيقية الإحصائية في مجال العلوم الاجتماعية والإنسانية نسخة 23 (SPSS V23) بغرض المعالجة الإحصائية للبيانات.

ثانيا : الأدوات الإحصائية

من أجل معالجة بيانات الدراسة وبغرض الحصول على نتائج تساعدنا في فهم موضوع الدراسة قمنا بالاستعانة بحزمة البرامج التطبيقية الإحصائية في مجال العلوم الاجتماعية والإنسانية (SPSS V23)، وتشمل هذه الأساليب على ما يلي:

1. معامل الثبات ألفا كرونباخ للتأكد من ثبات أداة الدراسة؛
2. استخدام المتوسط الحسابي المرجح لمعرفة اتجاهات أفراد الدراسة نحو كل فقرة أو بعد من فقرات وأبعاد الدراسة، حيث يقدم لنا ترتيب الفقرات حسب أعلى متوسط مرجح لمعرفة الفقرات أو الأبعاد المهمة؛
3. استخدام الانحراف المعياري لمعرفة مدى انحراف استجابة أفراد الدراسة نحو كل فقرة، وهو أيضا يوضح التشتت الحاصل في إجابات أفراد الدراسة، حيث أنه كلما اقتربت قيمته من الصفر، كلما دل ذلك على تركز الإجابات وعدم تشتتها، أما إذا كانت قيمته تساوي أو تفوق الواحد الصحيح فإن ذلك يعني عدم تركز الإجابات وتشتتها؛
4. مصفوفة الارتباط بيرسون لغرض اختبار العلاقة بين فعالية نظام الامن و المخاطر.

الفرع الخامس : الطريقة المستخدمة في القياس

لتحليل البيانات والمعطيات المجمعة بالاعتماد على مقياس ليكرت الثلاثي اعتمدنا على حساب التكرارات النسبية والنسب المئوية والمتوسطات الحسابية المرجحة والانحرافات المعيارية.

وقد تم الاعتماد على مقياس ليكرت الثلاثي الذي يعبر عن الخيارات (موافق، محايد، غير موافق) وهو مقياس ترتيبي، والجدول التالي يوضح درجات الموافقة حسب جدول ليكرت:

جدول رقم (3-1): جدول ليكرت الثلاثي للمحور الاول

العبارات	غير موفق	محايد	موفق
الأوزان	01	02	03

المصدر: من إعداد الطالبتين اعتمادا على الدراسات السابقة

درجات مقياس ليكرت التي قد تم إدخالها في برنامج SPSS على الجدول أعلاه، حيث أعطينا كل إجابة درجة.

ومن أجل تحديد الاتجاه أعطينا لاحتمالات الإجابات الثلاثة السابقة أوزان محددة كالتالي: موافق درجة 3؛ محايد درجة 2؛ غير موافق درجة. 1، كما يبينه الجدول أعلاه، وبعد ذلك يتم حساب المتوسط الحسابي المرجح لتحديد الاتجاه العام للإجابات، اما بالنسبة للمحور الثاني فقد اعتمدنا على المقياس:

جدول رقم (3-2): مقياس المحور الثاني

لم يحدث ابدا	احيانا	يحدث دائما
01	02	03

المصدر: من إعداد الطالبتين اعتمادا على الدراسات السابقة

الجدول رقم (3-3): المتوسطات المرجحة والاتجاه الموافق لها

المتوسط المرجح	(01.66-01.00)	(02.33-01.67)	(03.00-02.34)
الاتجاه	غير موافق	محايد	موافق
	لم يحدث ابدا	احيانا	يحدث دائما

المصدر: من إعداد الطالبتين اعتمادا على الدراسات السابقة

المبحث الثاني: تحليل ومناقشة النتائج الدراسة الميدانية

المطلب الأول : عرض نتائج الدراسة :

الفرع الأول :عملية تدقيق نظام المعلومات في المؤسسة:

انه من المهم دراسة عملية تدقيق نظام المعلومات بالمؤسسة، لانه ينتج عنه في الاخير تقرير يبدي فيه المدقق الداخلي رايه حول مدى كفاءة وفاعلية نظام المعلومات ككل، وعليه سنعتمد على خطوات واساليب هاته العملية في تقييم نظام المعلومات، موضحة كما يلي:

1- المرحلة الاولى: الاعلام والتحضير:

يتم بالمؤسسة الوطنية إعلام رئيس المديرية كتابيا برسالة ادارية عقد اجتماع لتحديد المخاطر المحيطة بنظام المعلومات، دراسة عامة، وضع خطة شاملة ، بها تحديد فريق العمل، والمدة الزمنية الازمة.

2- المرحلة الثانية: الدراسة في ارض الواقع: وشملت ما يلي:

أولا : دراسة شاملة حول واقع نظام المعلومات الالكتروني بالمؤسسة:

الجدول رقم (4-1) : واقع نظام المعلومات الإلكتروني

	التعيين	مؤسسة ENAGEO
الموارد البشرية People Ressources	الكفآت (مستعمل، ومتخصص)	جزائرية منها ذوي شهادات جامعية، تقنيين من مراكز التكوين ومنها ذوي خبرة ومهارات مكتسبة حسب المهام المسندة.
	التكوينات والتدريب	التدريب الاولي عند استلام المنصب، وجود قاعة دائمة للتكوينات، وجود تكوينات في قطاع اختصاص المؤسسة.
	التوظيف والانتقاء	تعتمد على الشهادة وعوامل اخرى
	الاستجابة وقابلية التغيير	صعوبة الاستجابة ورفض التغيير، ارشف كبير في كل مكتب وبتنظيم فردي.
	الحماية	كلمة مرور لكل شخص، وتقوم الادارة بتغييرها بانتظام
	العقوبات والمحفزات	موجود وغير مطبق وغير صارم
الجانب المادي Hardware Networks	المعدات والتجهيزات	عدد كافي من الخوادم كل حسب وضيفته، حواسب شخصية من نوع (HP, Dell, Condor, Fujitsu ,Alfatron)، طابعات مرتبطة بالشبكة من نوع HP، 200 جهاز كمبيوتر محمول، 40 ماسح ضوئي، 300 طابعة مكتبية، وأجهزة تخزين الكهرباء Onduleurs، اجهزة حماية فيزيائية ضد القرصنة والفيروسات، Firewall UTM Modèle XB360،
	الشبكات الموصولة بالخادم	شبكات الداخلية LAN، وVSAT.
	الحماية	انضمة الحماية ضد الحرائق، وحدة تخزين كهرباء لكل خادم
	الصيانة ومراقبة	وجود دائرة صيانة بها (Helpdesk Group، Hard Maintenance Service)،
البرمجيات والقواعد Software	البرامج	ويندوز (XP-07) Windows حسب معرفة مستخدم الجهاز. برامج مكتبية، وبرامج وظيفية منفصلة منجزة محليا، اغلب مخرجاتها ورقية، برامج مكافحة البريد المزعج ANTI-Spam، الجدار الناري: 2و Firewall UTM Modèle XB360 1، وكذلك استخدام برنامج التشفير Cryptage، للحماية من الاختراقات، والبريد المحلي للمؤسسة (Messagerie).
	الحداثة والتحديث	برامج مكتبية منفصلة منجزة من قبل Dintic يبدا العمل بها منذ تاريخ برمجتها ويجري تحديثها كلما استدعت الضرورة لذلك.
	الحماية	مضادات فيروسات مكتبية مختلفة، مع ترك امكانية التوقيف للمستعمل. مضاد الفيروسات / Kaspersky، برامج مضادة للقرصنة ANTI-SPYWARE
	المعلومة	تعتمد على المعلومات الالكترونية مع وجود عدد كبير من المعلومات الورقية وبعض المعلومات الشفوية
	عقود الصيانة	توفر الجانب البشري المتخصص في الصيانة

	الصيانة	فجائية عند التوقف
	التراخيص	اغلب البرامج منجزة بالمؤسسة، بعض البرامج مقتناه عن طرق النسخ
	الارشفة الإلكترونية	تحفظ المعلومات على مستوى المديرات كل شهر. نسخ لجميع مخرجات الوثائق على حوامل ورقية، تخزن في مقر الارشيف المكون من 6 غرف و16 مكتب وخزائن حجم كبير.
	الطباعة	كل عملية تطبع من اجل المصادقة عليها والارشفة.

المصدر:من اعداد الطالبتين اعتمادا على وثائق مقدمة من مديرية

من خلال جدول واقع نظام تتبين النقاط التالية:

1- المورد البشري: يعتبر العمود الفقري فهو من أهم الموارد الواجب توفرها لتشغيل النظام، وعليه فان المديرية Dintic، توفر على أفراد ذو الخبرة والكفاءة العالية لتشغيل النظام وضمان إنجاحه موزعين على أقسامها بالمديرية قسم مطوري البرمجة، قسم الشبكة، قسم صيانة الأجهزة، وتقوم المؤسسة بتدريب العمال في مختلف الاختصاصات؛ لتدعيم الجانب البشري بالمديرية.

2-الموارد المادية (Hardware): بما أن الموارد المادية تعتبر من أهم مكونات نظام المعلومات الالكتروني، ومن خلال الملاحظة والوثائق المقدمة فان المؤسسة تحتوي المؤسسة Enageo على اجهزة إعلام آلي متطورة تتماشى مع البرنامج المستعمل Oracle، حيث تم اقتناءها من نفس المؤسسة التي تم اقتناء منها برنامج Oracle مع ظمان معقول، وتوفر المؤسسة لكل مستعمل جهاز على مستوى كل المكاتب (Hp, Dell, Condor, Fujitsu)، طابعات رقمية متصلة بالشبكة نوع (Hp)، والات نسخ، والات طبع لكشوف الاجور، أجهزة تامين الكهرباء (Onduleur).

تتوزع هذه الأجهزة على مستوى مكاتب المستخدمين، وكذلك تحتوي مديرية (DINTIC) على قاعة الأجهزة والمعدات مبينة في الجدول التالي:

الجدول رقم (4-2) : محتويات قاعة الاجهزة والمعدات(DINTIC) بالمؤسسة الوطنية Enageo

EQUIPEMENT	***Quantité***
Serveurs VSAT iDirecti DX.	4
Un HUB VSAT iDirect 12100 4IF.	1
Une Baie de Stockage HP EVA 4400.	1
Une Baie de Stockage EMC CX-2.	1
Un châssis HP Bla de System Matrix 7000 de 06 serveurs Bla de sous VMware vSphere.	1
serveurs de Gestion (Oracle) sous Linux Redhat 5.	2
Serveurs de Gestion (Oracle) sous MS Windows Server 2003.	2
Serveur de Fichiers sous MS Windows Server 2003.	1
Serveur BlackBerry sous MS Windows Server 2003	1

Serveurs Proxy MS ISA 2006.	2
Serveurs de messagerie MS Exchange 2007.	2
Contrôleurs de domaine MS Windows Server 2008.	2
Serveur Cisco Unity.	1
Serveurs Cisco CUCM	2
Serveurs d'administration des réseaux.	2

المصدر: وثيقة مقدمة من مديرية (DINTIC).

كما قامت المؤسسة بمنح أجهزة الحاسب محمولة لكل المسؤولين، وأيظا المهندسين في مديرية (DINTIC)، بوصل استلام وتعهد بتحمل المسؤولية التامة لحماية الجهاز ومحتواه، ويسمح لهم باخراجه من المؤسسة حتى في اوقات العطل، وذلك للتواصل مع باقي العمال في حال حدوث اي مشاكل اثناء العمل والتي تتعلق بالبرنامج، فيمكن ذلك المسؤولين بتوجيه العمال عن كيفية تصليح المشكل، وهذا من اجل ضمان السير السليم للعمل.

كما يوجد على مستوى المديرية قسم صيانة الاجهزة (Département Maintenace)، وهو خاص بصيانة الاجهزة والمعدات والشبكات، وأي عطل مادي او فيزيائي (Hard, Soft) في الجهاز من ناحية التشغيل يقوم القسم بالاهتمام به وتصليحه وصيانته وكذلك حمايته من الفيروسات بتثبيت برامج مضادات الفيروسات.

3- الشبكة المعلوماتية : تسعى مديرية DINTIC لمؤسسة Enageo، لرفع مستوى البنية التحتية لنظام المعلومات العام بهدف تلبية المتطلبات الجديدة لانجاز الانشطة والأعمال التي تتغير باستمرار. وعليه فان المؤسسة تحتوي على شبكات معلوماتية مختلفة وذلك من اجل ضمان وصول وتوفر البيانات والمعلومات المتعلقة بمختلف أنشطة المؤسسة لجميع مستخدمي البرامج والتطبيقات وهي:

- **الشبكة الداخلية (Intranet)**: وهي متاحة لجميع الموظفين للاطلاع على القواعد والقوانين المتعلقة بالسير الحسن لمختلف الانشطة والوظائف بالمؤسسة،
- **الشبكة العالمية (Internet)**: وذلك قصد استفادة العمال منها، مع حجب المواقع الغير مسموح بها.
- **والبريد المحلي: (Messagerie)**: وذلك لضمان التواصل المستمر بين الموظفين ومستخدمي النظام، خاصتا بعد اعتماد البريد الالكتروني كدليل اثبات حتى في النزاعات.
- **شبكة الاتصال المحلية (LAN) Local Area Network**: وهي شبكة حاسوبية محلية تربط اجهزة الحاسوب الخاصة بالمؤسسة مع بعضها البعض ومع موزع قاعدة البيانات، لتوفير البيانات والمعلومات للمستخدمين من اجل انجاز الوظائف المختلفة.
- **الشبكة الواسعة (Wan)**: تستخدمها كلى المؤسستين للتواصل مع جميع فروعها ومختلف الموردين والعملاء حيث قامت مؤخرا مؤسسة Enageo باستبدال الأجهزة المتعلقة بها لقدمها، وعجزها عن تلبية المتطلبات والأمن، وتم استبدالها بموجهات وجدران نارية تسمح بالدخول لمواقع مختلفة للتواصل مع مختلف المستخدمين ومواقع الانترنت بامان وموثوقية، حيث قامت المؤسسة بتدريب الموظفين بقسم الشبكة للاستخدام الجيد لهذه الأجهزة. والجدول الموالي يمثل الأجهزة التي تم استبدالها.

الجدول رقم (4-3) : الاجهزة الالكترونية الجديدة الخاصة بالشبكة الواسعة بالمؤسسة الوطنية **Enageo**.

EQUIPMENT	*Quantité*
Routeur Modèle 1	3
Carte WAN E1 G703 à 1 port	4
Firewall UTM Modèle XB360	20
Switch Access 2950	15
Plateforme de Supervision Modèle 1	1

المصدر : قسم الشبكات بمديرية (**DINTIC**) بالمؤسسة الوطنية **Enageo** .

4-قاعدة البيانات في المؤسسة:

- تتمثل قاعدة بيانات المؤسسة في كل المعلومات و البيانات التي تتعلق بالنشاط سواء كان مصدرها من داخل المؤسسة او خارجها، فالمؤسسة تحتوي على نظام SGBD حيث يتم تخزين فيه البيانات و المعلومات في شكل ملفات بطريقة منهجية و نظامية في ذاكرة الخادم Serveur وذلك لحماية النظام.
- يتيح وجود برمجيات نظام SGBD امكانية التسيير السهل لبيانات و معلومات من ناحية انشاء المعالجة و التخزين .. ويتم الدخول بصفة عامة لهذا النظام عن طريق استخدام كلمة السر.
- ويتيح ايضا للمستخدم استغلال المعلومات و البيانات و اخرى للإطلاع عليها فقط دون استخدامها
- وأخرى سرية متاحة فقط للأشخاص المعينين من طرف الادارة العليا.

4-البرنامج المستعمل:

اشترت المؤسسة Enageo سنة 2006 ببرنامج (Oracle) SGBD "نظام تسيير قاعدة البيانات" من المؤسسة الجزائرية ORSIMA بمبلغ 3.342.440,00 دج، ويقوم فرع نظام المعلومات بالمؤسسة بعمليات تطوير البرامج المستعملة للنظام (Oracle) على مستوى المؤسسة، أي برمجة عدة تطبيقات مختلفة وذلك بما يتناسب مع احتياجات كل فرع، وكذلك القيام بمعالجة مختلف المشاكل والصعوبات التي تواجه العمال في تطبيق واستعمال البرنامج (عمليات المعالجة). والجدول الموالي يتضمن هذه التطبيقات وأهم أعمالها و تاريخ بداية تشغيلها:

الجدول رقم (4-4): التطبيقات المنجزة بالمؤسسة الوطنية Enageo

إسم التطبيق وتاريخه	الانجازات المحققة
Gestion des Payes	حساب أجور العمال، السماح بتحويل عمليات الاجور، متابعة حالات العمال.
Gestion de la Facturation	متابعة أوامر الفواتير، تتبع الفواتير، مراقبة العقود، رصد العملاء. متابعة التحويلات، متابعة شهادات الضمان ، متابعة مبيعات الشركة. رصد المشاريع، الفوترة و المحاسبة.
GDPS : Gestion De Production Sismique	إدارة مهام إنتاج، توحيد التقارير.
gStock	متابعة طلبات الشراء، متابعة العقود مع الموردين، متابعة أوامر الشراء، متابعة اجراءات التسليم، ارجاع الطلبات للموردين، متابعة طلبات العملاء، متابعة المخرجات والتحويلات المالية، عمليات التجديد، عمليات الجرد.
Gestion des Prestataires	متابعة مقدمي الخدمات، مراقبة العقود، متابعة القوانين والاجراءات، مراقبة الأجهزة، أوامر الدفع، متابعة التحويلات، متابعة بطاقات الدفع.
Gestion des Achats	السماح للهياكل بمتابعة طلبات الشراء، السماح للاشخاص التابعين لادارة تسيير المشتريات ادارة وتسيير المشتريات بشكل افضل، استخراج تقارير مباشرة من التطبيق.

المصدر: من إعداد الطالبتين استنادا على معلومات مقدمة من قسم نظام المعلومات

6- وصف وتقييم نظام الامن الالكتروني:

للمؤسسة سياسات امنية لحماية نظام المعلومات الالكتروني وذلك كمايلي:

أ_ حماية الاجهزة و العتاد:

- امضاء تعهد من طرف مسؤولي عمال مديرية DINTIC بتحمل المسؤولية التامة لحماية الجهاز(الحاسوب) و محتواه بالسماح لهم بإخراجه من المؤسسة في اوقات العطل في حالة حدوث اي مشاكل اثناء العمل التي تتعلق بالعمل.
- يوجد على مستوى المديرية قسم صيانة الاجهزة Département Helpdesk et maintenance.
- غرفة الاجهزة الالكترونية غرفة يتواجد فيها الخوادم تحتوي على اجهزة تبريد وأجهزة انذار ضد الحرائق وغير مسموح الدخول اليها إلا للمخولين فقط.

ب_حماية البرامج و الشبكات:

رسائل البريد الالكتروني المرسلة من مديرية Enageo الى مديرية Enageo عن طريق شبكات المؤسسة او الانترنت مما يمكن اختراقها في اي وقت وبالتالي تلجأ المؤسسة لاستخدام برامج للحماية منها:

- الجدران النارية Firewall UTM modèle 1et 2
- استخدام برامج التشفير cryptage
- تستخدم المؤسسة مضادات الفيروسات Kaspersky وهو مضاد للقرصنة و التجسس و anti-spyware برامج مكافحة البريد المزعج ، و anti-spam ، وغيرها من برامج الحماية .
- تمتلك المؤسسة اجهزة تأمين الكهرباء و إنذارات الحرائق لحماية الاجهزة و الاوراق من التلف و الضياع على مستوى المكاتب.

ج- حماية الأفراد:

- كل موظف لديه كلمة سر خاصة به وتقوم الادارة بتغيرها بالانتظام.
- تنضم المؤسسة دورات تدريبية لكل مستخدم وذلك لتطبيق قواعد ومتطلبات الامن المنصوص عليها في المؤسسة كاللوائح و الاعلانات القانونية.

د- حماية قواعد البيانات:

- تحتوي المؤسسة على مقر خاص بالأرشيف، تخزن فيه كل الملفات المهمة الخاصة بالمؤسسة ، ويتم التخزين عن طريق جهاز الحاسب باستخدام برنامج SGDB .
- او عن طريق النسخ الاحتياطي الآني و الدوري.
- وهذا المقر يتمتع بحماية كبيرة وممنوع الدخول اليه إلا للمخولين لهم فقط.

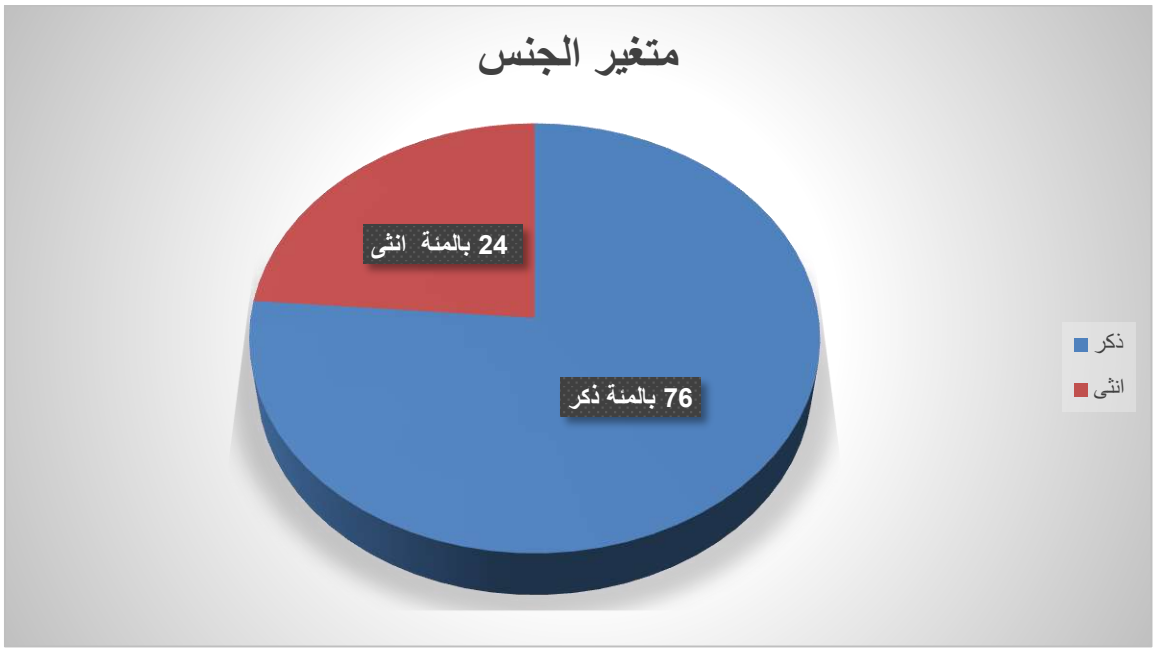
المطلب الثاني : نتائج الاستبيان

الفرع الأول :تحليل نتائج المتغيرات الشخصية

سنعرض خصائص العينة المستجوبة وذلك من خلال متغيرات: الجنس،السن، المستوى الدراسي، سنوات الخبرة .

- **الجنس**: سنوضح في التمثيل البياني الآتي طبيعة جنس العاملين المستجوبين:

الشكل رقم:(3-1) طبيعة جنس العاملين المستجوبين

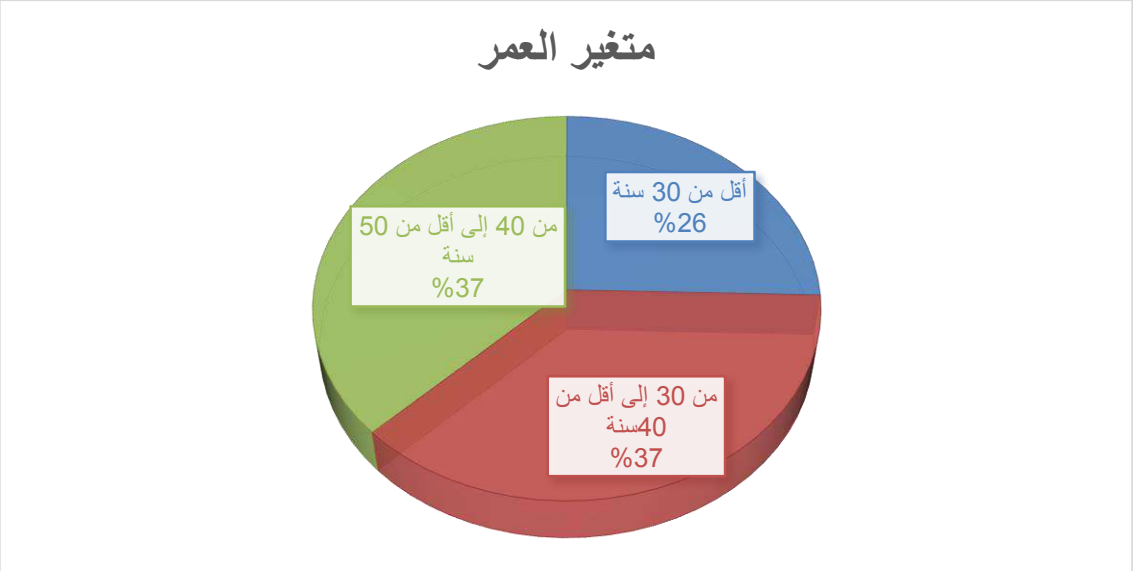


المصدر: من اعادا الطالبتين بناءا على مخرجات SPSS

من خلال الشكل أعلاه تبين النتائج أن العينة متباينة من حيث الجنس اذ أن الذكور بنسبة 76 بالمئة في حين الاناث بنسبة 24 بالمئة و هذا راجع لطبيعة نشاط المؤسسة و نظام الدوام.

- **العمر:**

الشكل رقم:(4-1) متغير العمر



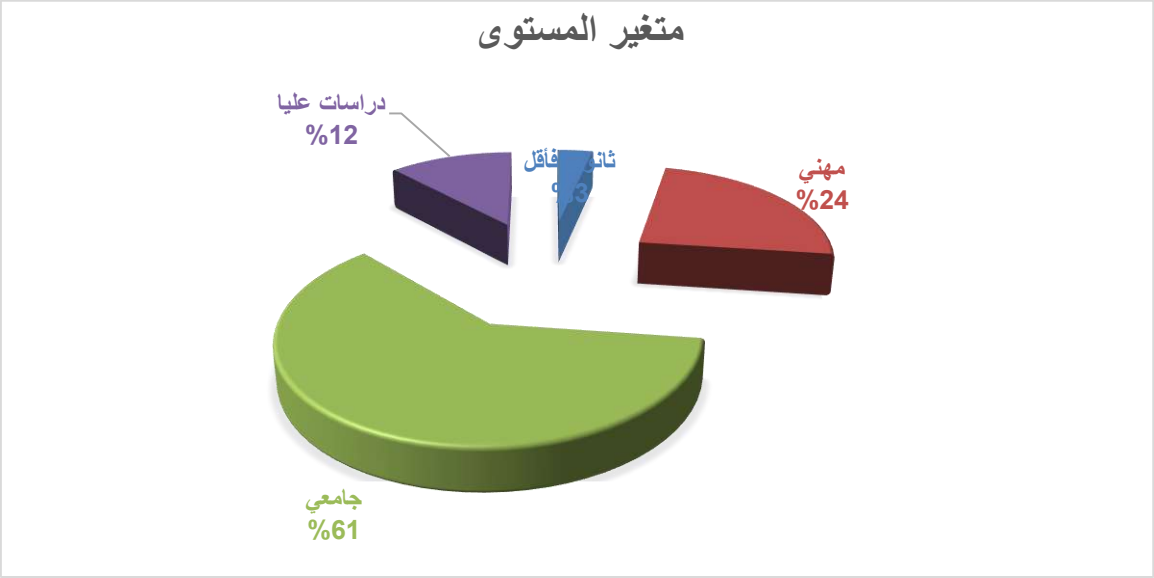
المصدر: من اعادا الطالبتين بناءا على مخرجات SPSS

إن الملاحظ للشكل والجدول أعلاه يجد أن ما يعادل 37 في المائة من أفراد العينة تمتد أعمارهم من 30 إلى 40 سنة، تليها الفئة العمرية التي أعمارهم من 40 الى 50 بنسبة 37 بالمئة وتأتي في الأخير الفئة اقل من 30 سنة وهي بنسبة 26 في المائة، بمعنى أن غالبية أفراد العينة تقل أعمارهم عن 40 سنة وهو السن الذي يكون فيه الفرد في أعلى نشاطه ودافعيته، والذي يعود بالنفع على المؤسسة. و كذا الفئة الثالثة تعبر عن الخبرة.

أما بالنسبة للعمال الذين أعمارهم من 41 فأكثر فنلاحظ أن نسبتهم قليلة نوعا ما مقارنة بالفئات العمرية الأخرى

- **متغير المستوى التعليمي:**

الشكل رقم:(5-1) متغير المستوى

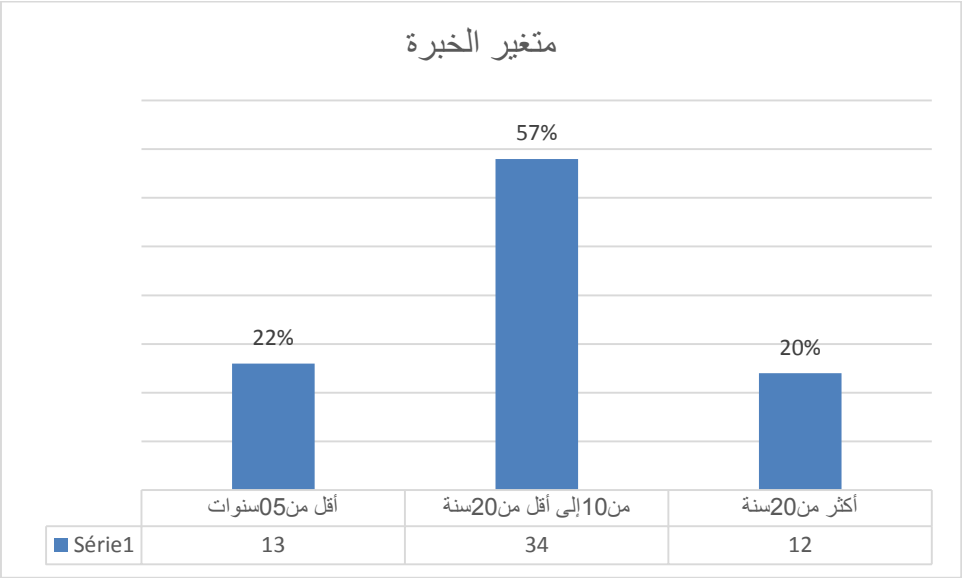


المصدر: من اعداد الطالبتين بناءا على مخرجات SPSS

يتضح من خلال مما سبق أن ما نسبته 61 في المائة من عينة الدراسة، هم حاصلين عل شهادة جامعية ليسانس ، ونسبة لا تقل 12في المائة حاصلين على دراسات عليا ، مما يعني أن حوالي 83 في المائة من أفراد عينة الدراسة هم حاصلين على شهادات جامعية، إذ يعد هذا مؤشرا هاما على أن أفراد العينة في مجملهم لديهم القدرة على الإجابة على أسئلة الاستبيان وهذا من شأنه أن يعزز الثقة في الإجابات ويرفع من درجة الاعتماد عليه في التحليل .

- **الخبرة:**

الشكل رقم:(6 –1) متغير الخبرة



المصدر: من اعداد الطالبتين بناءا على مخرجات SPSS

يتضح لنا من خلال إشكال أعلاه أن نسبة أفراد العينة الذين لديهم الخبرة في مجال العمل ، الممتد من10 سنوات إلى اقل من 20 سنة بلغت تقريبا أكثر 57% ، إذ ما يعد هذا مؤشرا ايجابيا على أن أفراد العينة من ذوي الخبرات العالية نسبيا، وهي خبرة كافية لتقييم نظام الأمن الكتروني ومساهمته في الحد من المخاطر نظم المعلومات.

الفرع الثاني: تحليل نتائج المحاور

سيتم حساب كل من المتوسطات الحسابية والانحرافات المعيارية، وتحديد الدرجة التي تتوافق مع المتوسط الحسابي في ضوء طريقة القياس التي تم الإشارة إليها سابقا.

- **ثبات أداة الدراسة**

نقيس الثبات مدى استقرار أداة الدراسة وعدم تناقضها، حيث يوضح ما إذا كانت قائمة الاستقصاء ستعطي نفس النتائج باحتمال مساوي لقيمة المعامل المحسوب في حالة ما إذا تم إعادة توزيعها على نفس أفراد العينة، وتم الاعتماد في هذه الدراسة على معامل الثبات ألفا كرونباخ والذي يعتبر أحد أهم طرق قياس الثبات الداخلي، والجدول أدناه يوضح معامل الثبات لأبعاد ومتغيرات الدراسة.

- **الجدول رقم (5–1): معاملات ثبات الأداة حسب المعامل (ألفا كرونباخ) حجم العينة (N=59)**

عدد العبارات	ألفا كرونباخ
42	0.791

- **المصدر**: من إعداد الطالبتين بناءً على مخرجات برنامج SPSS

- يتبين لنا من خلال نتائج الجدول أعلاه أن قيمة معامل الثبات لمجموع أبعاد الاستبيان ككل هو 0.791 وهو مقبول إحصائيا، مما يعني ثبات أداة الدراسة وصلاحيتها للإجابة على الأسئلة واختبار الفرضيات.

أولا : النتائج الخاصة بالمحور الأول : نظام الامن الالكتروني

البعد الأول : السياسات والإجراءات

الجدول رقم (5-2): نتائج إجابات المستجوبين الخاصة بالبعد الأول

العبارات	الترتيب	المتوسط المرجح	الانحراف المعياري	الاتجاه
1. توجد في المؤسسة سياسات وإجراءات مكتوبة لأمن المعلومات.	3	2,475	,8170	موافق
2. تدرك الإدارة أهمية سياسات أمن المعلومات.	5	2,451	,6248	موافق
3. يتم مراجعة وتطوير سياسات أمن المعلومات بشكل دوري	1	2,610	,5877	موافق
4. يتم إدخال المعلومات بعد مصادقة الرئيس المصلحة المباشر.	6	2,153	,8054	محايد
5. لا يسمح لغير المختصين بالوصول إلى الأجهزة والعتاد المحوسب.	7	2,390	,7660	موافق
6. يمنع الدخول لمواقع الانترانت بأجهزة الموصولة بالخادم المركزي.	4	2,458	,6248	موافق
7. لا يسمح بتثبيت البرامج غير الأصلية (الغير المرخصة) و المقرصنة.	2	2,508	,7040	موافق
8. يتم تجديد العتاد دوريا.	9	2,085	,7721	محايد
9. يفرض على الموظفين تغيير كلمة المرور دوريا	10	1,864	,8191	محايد
10. يتم التصريح بعناوين الحواسيب IP حتى يتم الدخول النظام	8	2,380	,7660	موافق
11. تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها	2	2,508	,7057	موافق
البعد الأول :		2.35	0,7346	موافق

المصدر: من إعداد الطالبتين بناءً على مخرجات البرنامج الإحصائي SPSS

البعد الثاني : إجراءات أمن المعلومات المتعلقة بالعاملين

الجدول رقم (5–3): نتائج إجابات المستجوبين الخاصة بالبعد الثاني

العبارات	الترتيب	المتوسط المرجح	الانحراف المعياري	الاتجاه
1. يتوافر تدريب للعاملين على النظم المحوسبة بشكل دوري لتطوير مهارتهم المتعلقة بالمستجدات الأمنية.	7	2,288	,7668	محايد
2. تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المؤسسة	3	2,441	,7257	موافق
3. يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص المؤسسة كجزء من شروط التوظيف.	1	2,492	,7281	موافق
4. يطلب من الموظفين والمتعاقدين الإبلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.	3	2,291	,6173	محايد
5. هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.	5	2,407	,6726	موافق
6. يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة.	2	2,490	,6791	موافق
7. لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا.	4	2,407	,7220	موافق
البعد الثاني : إجراءات أمن المعلومات المتعلقة بالعاملين		2,402	0.701	موافق

المصدر: من إعداد الطالبتين بناءً على مخرجات البرنامج الإحصائي SPSS

البعد الثالث : إجراءات أمن المعلومات المتعلقة بالعتاد والبيانات

الجدول رقم (5–4): نتائج إجابات المستجوبين الخاصة بالبعد الثالث

العبارات	الترتيب	المتوسط المرجح	الانحراف المعياري	الاتجاه
1. تستخدم المؤسسة شتئ الوسائل (أبواب –أقفال – بطاقات دخول –كاميرات)لحماية مكونات نظم المعلومات	10	2,203	,7830	محايد
2. يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها.	5	2,340	,8598	موافق
3. يمنع الموظف الغير المختص من أجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات.	2	2,390	,8098	موافق

4. كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم الخدمات نظم المعلومات محمية من العبث بها أو إتلافها.	8	2,281	,7204	محايد
5. تستخدم طرق تشفير لحماية البيانات.	4	2,356	,8044	موافق
6. توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات و في مكان امن.	6	2,305	,7934	محايد
7. توجد برامج حماية لتتبع ومنع الاختراق والتسلل.	7	2,288	,8105	محايد
8. تحتوي الشبكة على جدار ناري يحمي الشبكة من الاختراق.	9	2,271	,8269	محايد
9. يتم تثبيت مضادات الفيروسات والتحديثات الدورية .	1	2,424	,6998	موافق
10. يتم صيانة الشبكة والعتاد دوريا	3	2,373	,6669	موافق
البعد الثالث : أمن المعلومات المتعلقة بالعتاد والبيانات		2,342	0,777	موافق

المصدر: من إعداد الطالبتين بناءً على مخرجات البرنامج الإحصائي SPSS

المحور الثاني : إدارة مخاطر نظام المعلومات

الجدول رقم(5-4) نتائج المحور الثاني

العبارات	الترتيب	المتوسط المرجح	الانحراف المعياري	الاتجاه
1. الإدخال غير المتعمد(غير المقصود)للبيانات غير سليمة بواسطة الموظفين.	1	2,520	,6821	يحدث دائما
2. الإدخال المتعمد (المقصود)للبيانات غير سليمة بواسطة الموظفين.	5	1,983	,7309	احيانا
3. التدمير غير المتعمد(الحذف) للبيانات بواسطة الموظفين.	10	1,814	,7982	احيانا
4. التدمير المتعمد (الحذف) للبيانات بواسطة الموظفين.	7	1,912	,7526	احيانا
5. المرور (الوصول)غير الشرعي للبيانات او للنظام بواسطة الموظفين	11	1,797	,7139	احيانا
6. المرور غير الشرعي(غير المرخص به)للبيانات او للنظام بواسطة أشخاص من خارج المؤسسة.	13	1.24	,5946	لم يحدث ابدا

7. تعرضت اجهوة الحاسوب في المؤسسات الى الفيروسات.	3	2,174	,7463	**احيانا**
8. تم تعديل بعض خصائص أو تدمير بنود معينة من المخرجات.	12	1,62	,7675	**لم يحدث ابدا**
9. خلق مخرجات زائفة / غير صحيحة.	6	1,966	,8087	**احيانا**
10.سرقة البيانات / المعلومات.	9	1,847	,8266	**احيانا**
11.عمل نسخ غير مصرح (مرخص)بها من المخرجات.	2	2,220	,7208	**احيانا**
12.الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.(أي اطلاع موظفين او اشخاص اخرين على مخرجات تم طبعها وهم غير مرخصين لذلك).	4	2,161	,7912	**احيانا**
13.تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.	8	1,881	,7212	**لم يحدث ابدا**
14.تم سرقة كلمة مرور موظف معين واستخدامها بطريقة غير شرعية.	14	1,223	,7766	**لم يحدث ابدا**
المحور الثاني : إدارة مخاطر نظام المعلومات		**2,001**	**0.745**	**احيانا**

المصدر: من إعداد الطالبتين بناءً على مخرجات البرنامج الإحصائي SPSS

كانت الفقرة التي تنص " المرور غير الشرعي(غير المرخص به)للبيانات أو للنظام بواسطة أشخاص من خارج المؤسسة." أكثر العبارات " لم يحدث أبدا " من طرف المستجوبين بمتوسط حسابي قدؤه 1,24 أي يتفقون انه لم يسبق حدوثه.

و كانت نتيجة الفقرة" تعرضت أجهزة الحاسوب في المؤسسات إلى الفيروسات."احيانا " .

كانت العبارة الأولى التي تنص " الإدخال غير المتعمد (غير المقصود)للبيانات غير سليمة بواسطة الموظفين." أكثر العبارات "يحدث دائما " من طرف العينة، بمتوسط حسابي 2.52 1,88 اذ يتفقون على ان المؤسسة تعاني من الإدخال غير المتعمد (غير المقصود)للبيانات غير سليمة بواسطة الموظفين هذا الأمر صعب اكتشاف والقضاء عليه.

كانت نتيجة الفقرة الرابعة " التدمير المتعمد (الحذف) للبيانات بواسطة الموظفين "أحيانا " ، إذا سجل المتوسط الحسابي 1.912 أي ان العملية حدثت في مرات قليلة.

في حين كانت نتيجة الفقرات 6 ،8، 13، 14 على نتجية لم يحدث أبدا وهذه نتيجة جيدة بالنظر الى الأهمية النسبية لهاته المخاطر خاصة بما يتعلق بالمرور الغير الشرعي لأشخاص من خارج المؤسسة و كذا تسليم معلومات حساسة لأشخاص غير مرخص لهم.

الفرع الثالث: تحليل معامل الارتباط بين نظام الأمن الالكتروني و إدارة مخاطر نظام المعلومات

يبين الجدول التالي مصفوفة الارتباط ما بين نظام التقييم وأداء العاملين في مؤسسة سونلغاز ورقلة:

الجدول رقم (6-1): معامل الارتباط بين نظام الامن الالكتروني و مخاطر نظام المعلومات

		إدارة مخاطر نظام المعلومات	نظام الامن الالكتروني
نظام الامن الالكتروني	Pearson Correlation	1	-,266*
	Sig. (2-tailed)		,002
	N	59	59
إدارة مخاطر نظام المعلومات	Pearson Correlation	-,266*	1
	Sig. (2-tailed)	,002	
	N	59	59

المصدر: من إعداد الطالبتين بناءً على مخرجات البرنامج الإحصائي SPSS

هناك ارتباط عند القيمة sig تساوي0,01 *** Correlation is significant at the 0.01 level (2-tailed)**

من خلال القيمة الاحتمالية sig تساوي 0.02 أقل من مستوى المعنوية 0.05، يتبين وجود دلالة إحصائية لتأثير نظام الأمن الإلكتروني على مخاطر نظام المعلومات ، حيث كان **r** معامل ارتباط=**r** -0.266 ، أي أنه يوجد ارتباط خطي سالب بنسبة 26.6 بالمائة، بمعنى أنه توجد علاقة عكسية ضعيفة بين نظام الامن الالكتروني و مخاطر نظام المعلومات، أي أنه كلما كان نظام الامن الالكتروني فعال كلما ساهم في تقليل من حدوث مخاطر نظام المعلومات.

المطلب الثاني : مناقشة نتائج الدراسة

1- بالنسبة لعتاد نظام المعلومات:

من خلال تشخيص واقع نظام المعلومات بالمؤسسة اتضح لنا أن المؤسسة تتوفر على أهم عناصر النظام من حيث العتاد اذ قامت المؤسسة على مر الخمس سنوات الماضية بتجديد البنية بما يتعلق بالعتاد سواء حواسيب او خوادم ..الخ.

2- بالنسبة للبرامج:

تتوفر المؤسسة على مجموعة من المهندسين الممتازين في الاعلام الآلي وهذا ما مكنها من اكتساب مجموعة من البرامج المتكاملة مع بعضها البعض و المبرمجة و المطورة محليا، وهذه ميزة تمكنها من تطويرها الى ERP مستقبلا، كما نعلم انه كلما كان البرنامج مطور من طرف مهندسي المؤسسة كلما انخفض مخطر الاختراق الخارجي، وكذا سهولة التصحيح.

3- بالنسبة للشبكات:

تتوفر المؤسسة على اهم شبكة وهي الانترانت بين مصالح المؤسسة و كذا مجمع سونطراك، كما تسمح الإدارة بالاستخدام المحدود للانترنت.

4- بالنسبة لقواعد البيانات:

لدى المؤسسة قاعدة بيانات داخل المؤسسة تم توفيرها بخصائص ممتازة جدا من حيث سرعة و كمبة التخزين، لكن يبق مخطر عدم توفر نسخة احتياطية خارج المؤسسة قائما، اذ ان النسخة الاحتياطية موجودة بنفس المكان.

5- البعد الأول: سياسات الأمنية

من خلال تشخيصنا لواقع نظام الأمن الالكتروني في المؤسسة توصلنا الى أن إدارة نظام المعلومات تسعى للتطبيق الصارم لجميع السياسات والإجراءات المتعلقة بالامن الالكتروني، ولكن كانت إجابات الافراد محايد بما يتعلق بتغيير كلمة المرور وهذا راجع الى ان العديد من الموظفين لا يقومون باحترام هذه التعليمة و نقترح هنا هو برمجت تغيير كلمة المرور آليا كل شهر او ثلاث اشهر حتى يلزم المستخدم بذلك.كما لم يتفق افراد العينة بشان عبارة يتم تجديد العتاد دوريا ولاحظنا ذلك من خلال تفاوت نوع العتاد من مصلحة الى أخرى.

6- البعد الثاني: إجراءات أمن المعلومات المتعلقة بالعاملين

من خلال الدراسة الميدانية ان إدارة نظام المعلومات تسعى الى تدريب المستخدمين وتوعيتهم بمخاطر النظام و كذا تحديد صلاحيات المستخدمين و أيضا كلمة المرور، لكن الافراد اجابو بمحايد بما يتعلق بالتدريب أي ان هناك تفاوت في توفير فرصة للتدريب حول مستجدات نظام المعلومات و كذا نظم الحماية. كما اختلف الأفراد في هل الإدارة تطلب منهم تقديم الاقتراحات بشأن نقاط الضعف. كما لاحظنا توفر كل الإجراءات الأخرى.

7- البعد الثالث:أمن المعلومات المتعلقة بالعتاد والبيانات

من خلال تشخيص النظام توصلنا الى توفر مختلف سياسات حماية العتاد من حيث توفير معدلات الكهرباء للحواسيب و كذا وجود الخوادم في غرفة ذات خصائص و كذا محمية من أي دخول غير مسموح به، لكن النقاط السلبية و التي لم يتفق عليها المستخدمين من حيث التوفر بشكل فعل هي كل من مدى توفر الكابلات الكهربائية في ظروف محمية، و كذا عدم توفر برامج للحماية من الاختراق الخارجي، و أيضا بالنسبة لقواعد البيانات لا توجد نسخ احتياطية خارج المؤسسة. كما لم نجد وسائل حماية الغرف كالأقفال الخاصة او الأبواب الخاصة وكذا غياب الكميرات عدا غرفة الخادم.

8- السياسات الامنية لحماية النظام:

من خلال نتائج المقابلة و الاستبيان يمكن تلخيص مدى تطبيق المؤسسة للسيايات الأمنية من خلال الجدول التالي:

الجدول رقم (7-1): السياسات الأمنية

السياسات الأمنية	مستوى التطبيق
مضادات الفيروسات	موجودة غير شاملة كل الأجهزة
عدم استعمال فلاش ديسك	غير مطبقة
كاميرات مراقبة	غير موجودة
تحديد الصلاحيات بدقة	مطبقة
كلمة السر شخصية لكل فرد	مطبقة
تغيير كلمة السر دوريا	غير مطبقة
الجدار الناري (العتاد)	موجود
مضادات الحرائق	موجودة
إنذارات السرقة	موجودة فقط في غرفة الخادم
إجراءات وسياسات أمنية مكتوبة	موجودة
الصيانة الدورية	متوسطة
صيانة داخلية	داخليا
دورات تحسيسية دورية في امن المعلومات	قليلة
برامج حماية الشبكة	موجودة
نسخ احتياطية	موجودة
نسخ احتياطية خارج المؤسسة	غير موجودة
تشفير البيانات المهمة	مطبقة
مولد الكهرباء	موجود
مخزن ومعدل الكهرباء	موجود

المصدر: من إعداد الطالبتين

9- سلبيات و ايجابيات نظام المعلومات في المؤسسة:

الجدول (8-1): سلبيات وايجابيات نظام المعلومات

الإيجابيات	السلبيات
– قيام المؤسسة بدورات تدريبية للموظفين من اجل استخدام الجيد للأجهزة الالكترونية. – قسم صيانة الأجهزة داخل المؤسسة. – طريقة الاتصال بين المديريات و الموظفين عن طريق Outlook مما يساعد على حماية سرية المعلومات من الاختراق. – ممنوع إحضار الحواسيب الشخصية للمؤسسة. – وضع قارورات مضاد الحرائق قرب كل مكتب. – غرفة الخوادم تحتوي على اجهزة تبريد و اجهزة انذار ضد الحرائق و الكاميرات. – نظافة مكاتب المؤسسة.	– السماح بإدخال FlashDisk الغير في حواسيب المؤسسة. – القبول بالدخول الى La Salle Serveur. – غرفة الخادم تقع بين مكاتب المؤسسة. – التركيب غير السليم للأجهزة الالكترونية. – غياب وجود اجراءات و اللوائح القانونية و الامنية عند كل مكتب. – امكانية استخدام كلمة السر الشخصية بين الموظفين. – ترك الموظف مكانه دون غلق الحاسوب او نافذة التشغيل.

المصدر: من إعداد الطالبتين

10- مدى إمكانية حدوث مخاطر نظام المعلومات:

من خلال نتائج المقابلة و الاستبيان يمكن تلخيص مصفوفة مخاطر نظام المعلومات وفق الجدول الاتي:

الجدول (9-1): المقارنة مدى إمكانية حدوث مخاطر نظام المعلومات

المخاطر المؤسسة	درجة المخطر
المتعلقة بالمدخلات	متوسط
سرقة بيانات	منخفض
انتحال شخصية	منخفض
الفيروسات	متوسط

استعمال فلاش ديسك	مرتفع
المخرجات زائفة	منخفض
مخطر اختراق الشبكة	متوسط
مخطر الانترانت في المؤسسة	منخفض
مخطر انقطاع الكهرباء	متوسط
عدم وجود أهداف ورؤية الاستراتيجية أمن نظام المعلومات	مرتفع
عدم وجود الإجراءات الأمنية	منخفض
عدم وجود تدقيق في المجال الأمن نظام المعلومات	منخفض
غياب البنية الشبكة	منخفض
عدم توفير لوازم الأمنية لحفاظ على الخوادم ماديا	منخفض
مخاطر الأفراد الغير المتعمدة	مرتفع
مخاطر الأفراد المتعمدة	منخفض
انتحال الشخصية بسرقة كلمة المرور	منخفض

المصدر: من اعداد الطالبتين بناءا على تحليل نتائج دراسة الحالة

15.نقاط الضعف الموجودة على مستوى السياسات الأمنية لنظام المعلومات في المؤسسة:

رقم1: عدم وضع الملفات الرئيسة في الأرشيف على مستوى بعض المديريات؛

رقم2: إلغاء تثبيت مضادات الفيروسات من قبل المستخدمين؛

رقم3: مخاطر الشبكة الكهربائية على الأجهزة الالكترونية؛

رقم4: الخطر المادي على غرفة الأجهزة الالكترونية؛

رقم5: عدم التمكن من السيطرة على عملية سرقة البيانات من قبل الموظفين؛

رقم6: تأخير في تنفيذ عقد الصيانة لنظام مكافحة الحرائق في غرفة الأجهزة الالكترونية؛

رقم7: ميثاق أمن نظام المعلومات غير معلن عنه اي غير متاح لجميع الموظفين الذين يستخدمون النظام.

خلاصة الفصل:

حاولنا في دراستنا الميدانية التطرق بشكل أساسي لأثر نظام الأمن الالكتروني على ادارة مخاطر نظم المعلومات من الناحية التطبيقية وهذا من خلال معرفة واقع نظامها المعلوماتي الالكتروني والسياسات الامنية المتبعة وتحديد أثرها في الحد من المخاطر نظم المعلومات فلقد استعملنا الاستبيان والمقابلة لمعرفة مدى مساهمة الأمن الالكتروني في الحد من المخاطر .

الخاتمة:

حاولنا من خلال هذه الدراسة التعرف على أثر نظام الامن الالكتروني في إدارة مخاطر نظم المعلومات في المؤسسة الوطنية للجيوفيزياء حاسي مسعود من حيث الحد والتقليل منها، حيث قسمنا دراستنا إلى فصلين، الفصل الأول الأدبيات النظرية لنظام الأمن الإلكتروني تناول الإطار المفاهيمي للدراسة، والدراسات السابقة للموضوع، أما الفصل الثاني فقد تضمن الجانب التطبيقي (دراسة ميدانية).

من خلال الدراسة النظرية والميدانية التي قمنا بها وذلك من أجل معالجة الإشكالية التالية: **ما مدى نجاعة نظام الأمن الالكتروني في إدارة مخاطر نظم المعلومات في المؤسسة الوطنية للجيوفيزياء ؟**

أولا: نتائج البحث:

بعد العرض المقدم سابقا وكذا التحليل والتفسير لمختلف النتائج المتوصل إليها، سنحاول تلخيصها في النقاط الآتية:

- تتوفر المؤسسة على مجموعة من المهندسين الممتازين في الاعلام الآلي وهذا ما مكنها من اكتساب مجموعة من البرامج المتكاملة مع بعضها البعض والمبرمجة والمطورة محليا.
- يتميز نظام المعلومات في المؤسسة محل الدراسة من كفاءة في المكونات المادية والبرمجية.
- تطوير البرامج من طرف مهندسي المؤسسة، وهذا ما يخفض من مخطر الاختراق.
- لدى المؤسسة محل الدراسة نظام الكتروني فعال ويحميها ويحد من مخاطر نظم المعلومات عدا بعض المخاطر مثل مخاطر الافراد الغير المتعمدة وكذا الفيروسات، وكذا مخطر فقدان البينات وهذا بسبب وجود النسخة الاحتياطية في نفس مكان النسخة الأصلية.
- توفر مختلف سياسات حماية العتاد من حيث توفير معدلات الكهرباء للحواسيب وكذا وجود الخوادم في غرفة ذات خصائص وكذا محمية من أي دخول غير مسموح به.
- تسعى إدارة نظام المعلومات الى تدريب المستخدمين وتوعيتهم بمخاطر النظام وكذا تحديد صلاحيات المستخدمين.
- تتوفر المؤسسة على اهم شبكة وهي الانترانت بين مصالح المؤسسة وكذا مجمع سوناطراك.

- لدى المؤسسة قاعدة بيانات داخل المؤسسة تم توفيرها بخصائص ممتازة جدا من حيث سرعة وكمية التخزين.
- أن المؤسسة تتوفر على أهم عناصر النظام من حيث العتاد.
- وجود إجراءات وسياسات أمنية مكتوبة ومعلنة من طرف إدارة DINTIC.
- تأخير في تنفيذ عقد الصيانة لنظام مكافحة الحرائق في غرفة الأجهزة الالكترونية.

ثانيا: اختبار الفرضيات:

بعد عرض مختلف النتائج المتوصل إليها ومناقشتها سنقوم فيما يلي باختبار مدى صحة الفرضيات المتعلقة بموضوع الدراسة والمتمثلة في:

- **الفرضية الأولى: يتميز نظام المعلومات الإلكتروني بتوفر جميع العناصر الاساسية، العتاد، البرامج، قواعد البيانات، الافراد، الشبكات.**

من خلال الدراسة الميدانية توصلنا الى ان نظام المعلومات الالكتروني في المؤسسة محل الدراسة يتوفر على جميع العناصر الاساسية **ومنه نثبت صحة الفرضية.**

- **الفرضية الثانية: يتميز نظام الأمن الإلكتروني بالكفاءة من حيث مكونات (العتاد، البرامج، السياسات الأمنية).**

من خلال الدراسة الميدانية توصلنا الى ان نظام الأمن الالكتروني يتوفر على جميع المقومات، من حيث العتاد اذ تسعى المؤسسة الى توفير الاجهزة وفق المعايير وكذا بالنسبة للبرامج اذ توفر المؤسسة كل البرامج لحماية البيانات، اما بالنسبة للسياسات الامنية فتوجد في المؤسسة كل السياسات المتعلقة بالأفراد والبرامج والاجهزة، والبيانات، **ومنه نثبت صحة الفرضية.**

- **الفرضية الثالثة: يحيط بنظام المعلومات في المؤسسة محل الدراسة العديد من المخاطر منها داخلية وخارجية.**

من خلال الدراسة الميدانية توصلنا الى ان نظام الأمن الالكتروني في المؤسسة تحيط به مخاطر تتعلق بإدخال البيانات، مخاطر تتعلق بالتشغيل، مخاطر تتعلق بالمخرجات، ومخاطر تتعلق بالبيئة. **ومنه نثبت صحة الفرضية.**

- **الفرضية الرابعة: يتميز نظام الأمن الإلكتروني بالفعالية من حيث الحد من مخاطر نظام المعلومات**

من خلال الدراسة الميدانية توصلنا الى ان نظام المعلومات الإلكتروني في المؤسسة يتعرض الى العديد من المخاطر وعليه تم وضع نظام امن الكتروني للحد منها لكن هناك بعض المخاطر التي لم يتم الحد منها

مثلا المخاطر المتعلقة الافراد ، وكذا مخاطر الفيروسات، وهذا راجع الى النقائص الموجودة على مستوى نظام الأمن .**ومنه نثبت الصحة الفرضية جزئيا**.

ثالثا: التوصيات:

بعد استعراض نتائج الدراسة فإنه يمكننا الخروج بمجموعة من التوصيات وهي كالتالي:

- اتخاد التدابير اللازمة للحد من خطر الفيرسة و كذا اخذ البيانات من طرف اشخاص غير مرخص لهم وهذا بمنع استخدام USB، CD، إلا بترخيص من DINTIC.
- الزامية احترام وتنفيذ عقود صيانة نظام الوقاية من الحرائق، واسناد المسؤولية لجهة محددة للمتابعة.
- ادراج إدارة أمن نظام المعلومات صمن مستوى عالي في الإدارة لإعطائها قوة أكبر لتدعيم تطوير النظام الإلكتروني.
- وضع اجراءات واللوائح القانونية والأمنية عند كل مكتب.
- تغيير مقر غرفة الخادم التي تقع بين مكاتب المؤسسة، نظرا لأهميتها الكبيرة وذلك لتجنب عدم دخول غير المرخصين لهم.
- ضرورة مراقبة عملية الصيانة للأجهزة والبرامج، يجب أن تكون هذه العملية دورية ومنتظمة.
- يجب على المؤسسة تطبيق اجراءات عقابية صارمة على الموظفين الذين ينتهكون اجراءات وسياسات أمن المعلومات.

رابعا: أفاق البحث:

برزت لنا أثناء القيام بهذه الدراسة عدة اشكاليات جديرة بالطرح لمواصلة البحث العلمي، هذا ما يدفعنا إلى طرح عدة أسئلة نتركها آفاقا لهذا البحث منها:

- واقع إدارة أمن نظم المعلومات في الجامعات الجزائرية.
- المخاطر المحتملة التي قد تواجه أمن نظم المعلومات المحاسبية الإلكترونية.
- مخاطر المستهلك الالكتروني دراسة حالة مواقع البيع عند طريق الانترنت.

الملحق رقم (1): أسئلة المقابلة

❖ **هل توجد جهة مختصة بأمن المعلومات؟**

06. شخص موكل له القيام بقضايا أمن المعلومات ومتابعتها؟ وما هي المعوقات لفعل ذلك ؟

07. هل يعتبر أمن المعلومات أولوية بالنسبة لكم ؟ وكيف ترون متطلبات الأمن(السرية – التوفر السلامة)بالنسبة لأنشطة المعلومات

هل لديكم سياسة أمن معلومات؟

08.ما هي البنية التحتية لتكنولوجيا المعلومات، بمعنى ما هو طبيعة نظم المعلومات ككل؟

09.هل تلبي البنية التحتية الحالية لنظم المعلومات احتياجات الأقسام (المؤسسة)بمعنى هل الشبكة فعالة، هل البرمجيات ذات كفاءة ،

❖ **هل الخوادم تعمل بشكل مناسب، هل يتم مراجعة دورية وفحص و إجراء تقييم للبنية التحتية؟**

10. ماذا عن خطط الاستبدال لمكونات نظام المعلومات ؟ تكلم عن كل جزء بشكل منفرد:

- **المادي.**
- **البرمجي**
- **نظم تشغيل**
- **برامج التطبيقات**
- **الشبكي (وسائط النقل – الشبكة اللاسلكية – الموجهات والمبدلات–تحسين سرعة النقل –الربط بالانترنت)**

11.هل يتم إجمال التهديدات التي من الممكن التعرض لها وبدوره السؤال أشمل هل تقومون بإدارة وتحليل للمخاطر ؟ ما هي الأنواع ونسب التهديدات من وجهة نظرك]

- **الثغرات الأمنية**
- **التهديدات بأنواعها:**
- **التهديدات الغير متعمدة**
- **التهديدات المتعمدة**
- **التهديدات الطبيعية**
- **الأخطاء التقنية**
- **الأخطاء الإدارية**

الملحق رقم(2):الاستبيان

جامعة قاصدي مرباح – ورقلة
كلية العلوم التجارية والعلوم الاقتصادية وعلوم التسيير
قسم علوم التسيير

استبيان

السادة والسيدات إطارات، موظفو المؤسسة: يشرفني أن أتقدم إلى سيادتكم المحترمة بهذه الاستمارة التي تدخل ضمن متطلبات انجاز مذكرة ماستر تحت عنوان **أثر نظام الأمن الالكتروني على ادارة مخاطر نظم المعلومات** "، وأعلمكم أن الإجابات المقدمة من طرفكم سوف تحضي بالأهمية البالغة لدينا ولن تستخدم إلا لأغراض البحث العلمي. نشكركم شكرا جزيلا على مساهمتكم الجادة بالإجابة على العبارات المرفقة وبصراحة تامة.

اعداد: قابل نور الهدى، هيمة هاجر **اشراف: رجم خالد** **ولكم منا كل الشكر والتقدير.**

ملاحظة: يرجى وضع علامة (X) في الخانة التي ترى أنها مناسبة.

المحور الأول : نظام الأمن الكتروني

الرقم	البعد الأول : السياسات والإجراءات	غير موافق	محايد	موافق
01	توجد في المؤسسة سياسات وإجراءات مكتوبة لأمن المعلومات.			
02	تدرك الإدارة أهمية سياسات أمن المعلومات.			
03	يتم مراجعة وتطوير سياسات أمن المعلومات بشكل دوري.			
04	يتم إدخال المعلومات بعد مصادقة الرئيس المصلحة المباشر.			
05	لا يسمح لغير المختصين بالوصول إلى الأجهزة والعتاد المحوسب.			
06	يمنع الدخول لمواقع الانترانت بأجهزة الموصولة بالخادم المركزي.			
07	لا يسمح بتثبيت البرامج غير الأصلية (الغير المرخصة) و المقرصنة.			
08	يتم تجديد العتاد دوريا.			
09	يفرض على الموظفين تغيير كلمة المرور دوريا			
10	يتم التصريح بعناوين الحواسيب IP حتى يتم الدخول النظام			
11	تسجل أي عملية أثناء المعالجة باسم الموظف الذي قام بها			
	البعد الثاني إجراءات امن المعلومات المتعلقة بالعاملين	**غير موافق**	**محايد**	**موافق**
12	يتوافر تدريب للعاملين على النظم المحوسبة بشكل دوري لتطوير مهارتهم المتعلقة بالمستجدات الأمنية.			
13	تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في المؤسسة			
14	يطلب من الموظف التوقيع على تعهد بعدم الإفصاح عن معلومات حساسة تخص المؤسسة كجزء من شروط التوظيف.			
15	يطلب من الموظفين والمتعاقدين الإبلاغ عن أي نقاط ضعف يلاحظونها في الأنظمة.			

16	هناك سجل رقابي يتضمن أنشطة المستخدم وحوادث أمن المعلومات.			
17	يتم تطبيق إجراءات عقابية على الموظف الذي ينتهك إجراءات وسياسات أمن المعلومات في المؤسسة.			
18	لكل موظف كلمة السر الخاصة به ويطلب منه تغييرها دوريا.			
	البعد الثالث : إجراءات امن المعلومات المتعلقة بالعتاد والبيانات	**غير موافق**	**محايد**	**موافق**
19	تستخدم المؤسسة شتئ الوسائل (أبواب –أقفال – بطاقات دخول –كاميرات)لحماية مكونات نظم المعلومات			
20	يوجد في المؤسسة مصدر بديل للكهرباء في حالة انقطاعها.			
21	يمنع الموظف الغير المختص من أجراء تعديلات مادية على الأجهزة العاملة ضمن نظم المعلومات.			
22	كوابل الكهرباء والاتصالات التي تنقل البيانات أو التي تدعم الخدمات نظم المعلومات محمية من العبث بها أو إتلافها.			
23	تستخدم طرق تشفير لحماية البيانات.			
24	توفر الأنظمة المستخدمة خدمة النسخ الاحتياطي للبيانات و في مكان امن.			
25	توجد برامج حماية لتتبع ومنع الاختراق والتسلل.			
26	تحتوي الشبكة على جدار ناري يحمي الشبكة من الاختراق.			
27	يتم تثبيت مضادات الفيروسات والتحديثات الدورية .			
28	يتم صيانة الشبكة والعتاد دوريا			

المحور الثاني : مخاطر نظم المعلومات

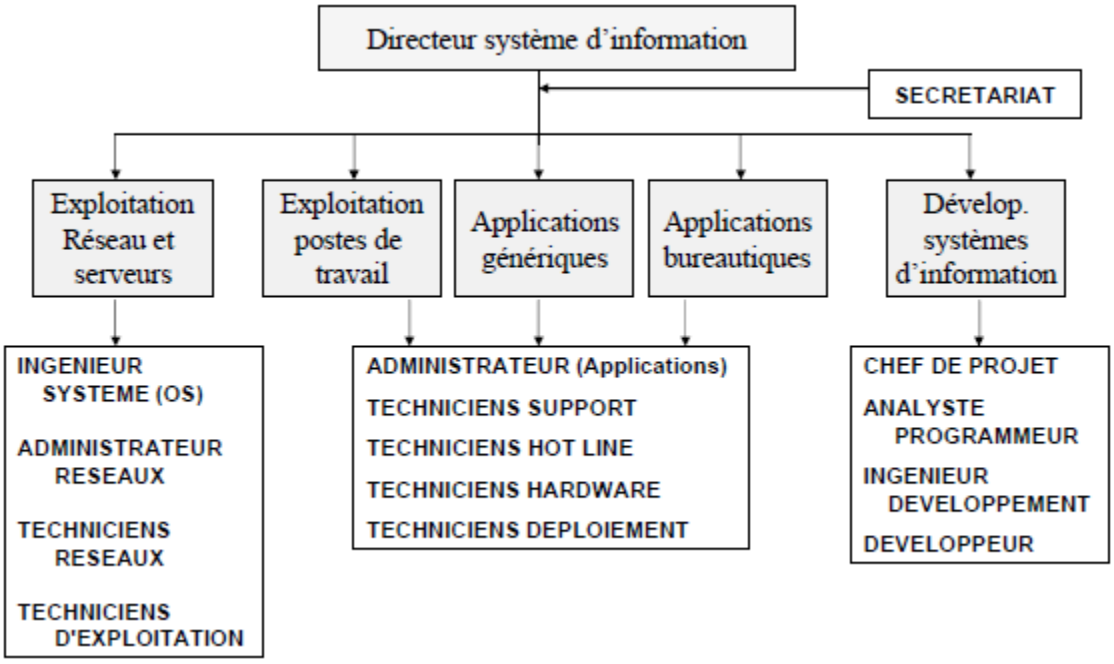
الرقم		لم يحدث ابدا	احيانا	يحدث دائما
01	الإدخال غير المتعمد(غير المقصود)للبيانات غير سليمة بواسطة الموظفين.			
02	الإدخال المتعمد (المقصود)للبيانات غير سليمة بواسطة الموظفين.			
03	التدمير غير المتعمد(الحذف) للبيانات بواسطة الموظفين.			
04	التدمير المتعمد (الحذف) للبيانات بواسطة الموظفين.			
05	المرور (الوصول)غير الشرعي للبيانات او للنظام بواسطة الموظفين			
06	المرور غير الشرعي(غير المرخص به)للبيانات او للنظام بواسطة أشخاص من خارج المؤسسة.			
07	تعرضت اجهوة الحاسوب في المؤسسات الى الفيروسات.			
08	تم تعديل بعض خصائص أو تدمير بنود معينة من المخرجات.			
09	خلق مخرجات زائفة / غير صحيحة.			
10	سرقة البيانات / المعلومات.			
11	عمل نسخ غير مصرح (مرخص)بها من المخرجات.			

12	الكشف غير المرخص به للبيانات عن طريق عرضها على شاشات العرض أو طبعها على الورق.(أي اطلاع موظفين او اشخاص اخرين على مخرجات تم طبعها وهم غير مرخصين لذلك).			
13	تسليم المستندات الحساسة إلى أشخاص لا تتوافر فيهم الناحية الأمنية بغرض تمزيقها أو التخلص منها.			
14	تم سرقة كلمة مرور موظف معين واستخدامها بطريقة غير شرعية.			

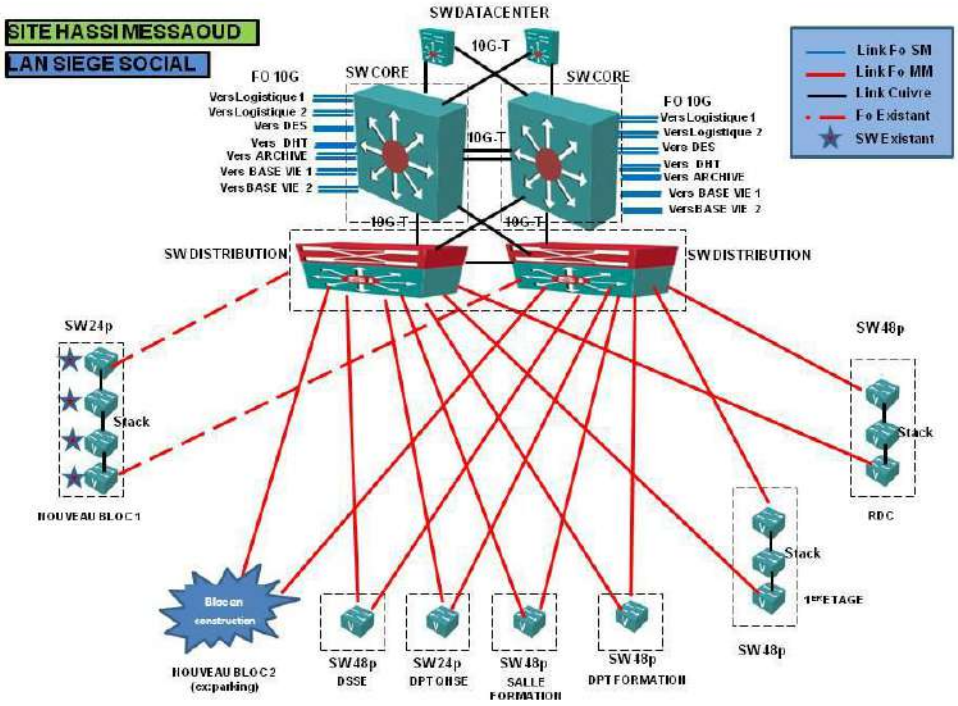
معلومات متعلقة بالموظف:

الجنس	**ذكر**	**أنثى**		
العمر	أقل من 30 سنة	من 30 إلى أقل من 40سنة	من 40 إلى أقل من 50 سنة	50 سنة فأكثر
مستوى التعليم	ثانوي فأقل	مهني	جامعي	دراسات عليا
الخبرة	أقل من05سنوات	من05 إلى أقل من10سنوات	من10إلى أقل من20سنة	أكثر من20سنة
المسمى الوظيفي				

الملحق رقم (3): الهيكل التنظيمي لقسم نظام المعلومات بالمؤسسة الوطنية Enageo



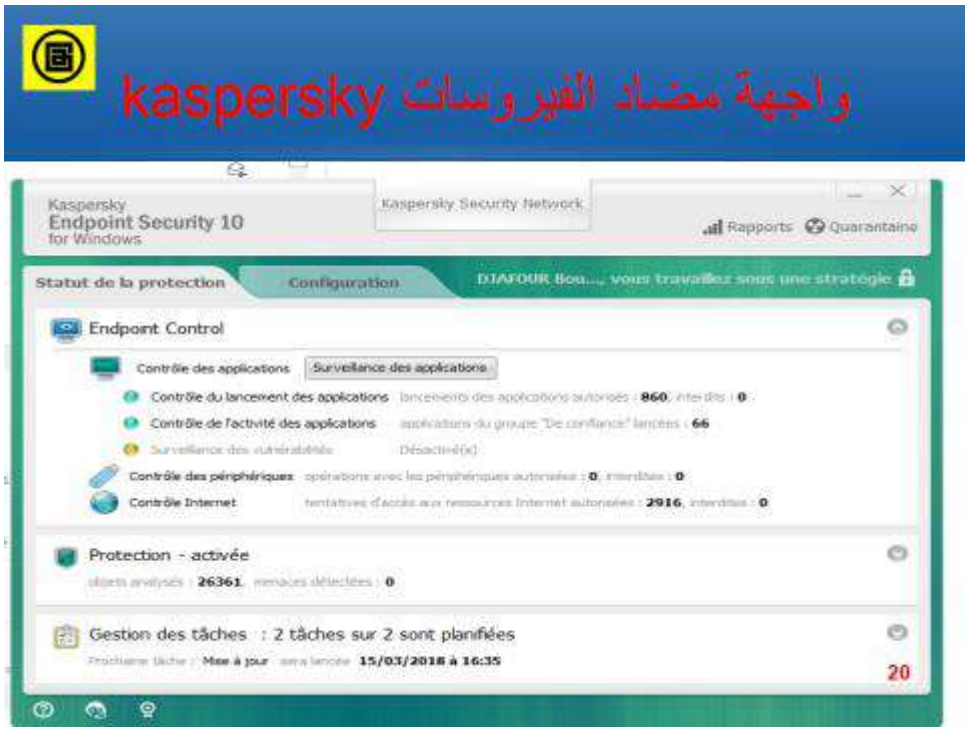
الملحق رقم (4): مخطط الشبكة المحلية (LAN) بالمؤسسة الوطنية Enageo



الملحق رقم (5): صورة لغرفة الخوادم الموجودة بالمؤسسة

الملحق رقم (6): اللوائح القانونية المعلنة في المؤسسة

الملحق رقم (7): واجهة مضاد الفيروسات



الملحق رقم (8): واجهات البرامج المنجزة بالمؤسسة

الملحق رقم (9): تطبيقات برنامج أوراكل

تطبيقات برنامج ORACLE

Le Nom D'application	La date D'application
Application gestion des achats	01\01\2015
Application gestion des stocks	01\07\2014
Application gestion de la facturation	01\01\2014
Application gestion des prestataires	01\08\2014
Application gestion des payes	2010 jusqua 5 ans
Application gestion de la production sismique	01\02\2014

9

fppt.com

أولا : المراجع باللغة العربية

الكتب:

1. أبو بكر محمود الهوش، "**نظم وشبكات المعلومات، مؤسسة الثقافة الجامعية**"، مصر، 2007.
2. أحمد فتحي الحيت، **مبادئ الادارة الالكترونية**، دار الحامد للنشر والتوزيع، عمان,2015، ص:114.
3. حمد ال فرج الطائي، **الموسوعة الكاملة في نظم المعلومات الادارية الحاسوبية**، دار زهران، الأردن, 2002، ص:44.
4. عبد الرزاق محمد قاسم، **تحليل وتصميم نظم المعلومات المحاسبية**، دار الثقافة، دمشق، 2009،ص 16.
5. محمد الصيرفي، نظم المعلومات الإدارية، طبعة الأولى، مؤسسة حورس الدولية، الإسكندرية،2005ص ص 186-188.
6. علاء محمد شوقي ابراهيم عيسى، **تأثير تطبيق حوكمة الشركات على مخاطر نظم المعلومات**، دار الجزائرية للنشر والتوزيع،2015 ص 63.

المجلات العلمية:

1. الطاهر بن عمارة، خالد رجم، "**أثر نظام الحماية الالكترونية في الحد من مخاطر تكنولوجيا المعلومات والاتصال**"، مجلة رؤى اقتصادية، جامعة الوادي، 2018 ص 3.
2. مصطفى فتحي، **أمن المعلومات**، دورة علمية، المنظمة العربية للتنمية الإدارية، 2010 ص 13.

المذكرات والأطروحات:

1-أمل ابراهيم أبو رحمة، **نظام معلومات الموارد البشرية وأ رها على فاعلية ادارة شؤون الموظفين في فلسطين**، مذكرة ماجستير، ادارة الأعمال، غزة2005 .

3. رجم خالد، **تقييم أثر نظام معلومات الموارد البشرية على استراتيجيات إدارة الموارد البشرية**، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير ورقلة، 2017ص49.

4. حرية شعبان محمد الشريف، **مخاطر نظم المعلومات المحاسبية الإلكترونية "دراسة تطبيقية على المصارف العاملة في قطاع غزة "**، مذكرة ماجستير منشورة، كلية التجارة. بالجامعة الإسلامية بغزة، 2006 ص84.

5. يزيد ذكار، "**تقييم كفاءة نظام المعلومات الإلكتروني**"، مذكرة ماستر، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، ورقلة،2016 ص 12.

المطبوعات والمحاضرات البيداغوجية:

1. خالد رجم، "**محاضرات أمن نظم المعلومات**"، مقياس مراجعة نظام المعلومات، أولى ماستر، جامعة ورقلة، 2015-2016.

2. رجم خالد، "**مطبوعة نظام المعلومات** "، ثانية جذع مشترك علوم التسيير ،جامعة ورقلة، 2018، ص15.

ثانيا: المراجع باللغة الأجنبية:

1-الكتب:

1- Laudon & laudon-management information systems-the digital firm, idition9, Pearson Education, USA, 2006.

2- Oihab Allal-Chérif et Olivier Dupouet, « Optimisez votre Système d'Information « vers la PME numérique en réseau » », Afnor, Saint-Denis, France, 2014.

2-البحوث العلمية:

1- MWITA SIMION MAROA, « Factors affecting information systems security effectiveness in university of Nairobi », Thesis of Master of science degree in information systems, Kenya, 2015.

2- Robert Reix, système d'information et management desorganisation, édition 5 Vuibert –gestion, paris, France.

3- Robert Reix, Bernard Fallery, Michel Kalika et Frantz Rowe, » Système d'information et gestion des organisations », 6 Edition, Vuibert, paris, 2011.

3–مواقع الانترانت:

- ✓ http://asca.sy/download/PDF/murajaa-pdf.pdf
- ✓ http://www.accdiscussion.com/t12332
- ✓ https://sqarra.wordpress.com/inaudit/

العنوان	الصفحة
الإهداء	III
الشكر	IV
الملخص	V
قائمة المحتويات	VI
قائمة الجداول	VII
قائمة الأشكال	VIII
قائمة الاختصارات والرموز	X
قائمة الملاحق	IX
المقدمة	ب
الفصل الأول: الأدبيات النظرية والتطبيقية لأثر نظام الحماية الالكتروني في الحد من مخاطر نظم المعلومات	01
المبحث الأول: الإطار النظري لأثر نظام الحماية الالكتروني في الحد من مخاطر نظم المعلومات	02
المطلب الأول: الإطار النظري لنظام المعلومات	02
الفرع الأول: ماهية نظام معلومات	03
الفرع الثاني: عناصر نظام معلومات	04
الفرع الثالث: مستويات نظام معلومات	06
الفرع الرابع: أهداف وأهمية نظام المعلومات	07
المطلب الثاني: نظام الأمن الالكتروني	08
الفرع الأول: نظام الحماية الالكتروني (الأمن الالكتروني)	08
الفرع الثاني: عناصر الأمن الالكتروني	09
الفرع الثالث: متطلبات أمن نظم المعلومات	09
المطلب الثالث: مخاطر نظام المعلومات	10
الفرع الأول: ماهية مخاطر نظم المعلومات	10
الفرع الثاني: مخاطر نظم المعلومات	11
الفرع الثالث: أسباب حدوث مخاطر نظم المعلومات	13
الفرع الرابع: تهديدات نظم المعلومات	16

المبحث الثاني: الدراسات السابقة	18
المطلب الأول: الدراسات السابقة باللغة العربية	18
المطلب الثاني: الدراسات السابقة باللغة الأجنبية	19
المطلب الثالث: مقارنة الدراسة الحالية بالدراسات السابقة	20
الفرع الأول: أوجه التشابه	23
الفرع الثاني: أوجه الاختلاف	23
الفصل الثاني: الدراسة الميدانية لأثر نظام الحماية الالكتروني في الحد من مخاطر نظم المعلومات	25
المبحث الأول: عينة وأدوات الدراسة	25
المطلب الأول: عينة ومجتمع الدراسة	25
الفرع الأول: مجتمع الدراسة	25
الفرع الثاني: عينة الدراسة	26
الفرع الثالث: أدوات الدراسة	26
الفرع الرابع: البرامج والأدوات الإحصائية	27
الفرع الخامس: الطريقة المستخدمة في القياس	28
المبحث الثاني: تحليل ومناقشة نتائج الدراسة الميدانية	29
المطلب الاول: عرض نتائج الدراسة	29
الفرع الأول: عملية تدقيق نظام المعلومات في المؤسسة	29
المطلب الثاني: نتائج الاستبيان	35
الفرع الأول: تحليل نتائج المتغيرات الشخصية	35
الفرع الثاني: تحليل نتائج المحاور	38
الفرع الثالث: تحليل معامل الارتباط بين نظام الحماية الإلكتروني ومخاطر نظم المعلومات	43
المطلب الثالث: مناقشة نتائج الدراسة	44
الخاتمة	51
المراجع	55
الملاحق	59
الفهرس	70