Al-Farouk journal of sciences
Volume (2), Issue (3) (JUNE, 2026)
ISSN: 3135-2359

مجلة الفاروق للعلوم
المجلد (2) العدد 3 يونيو 2026
ردمد: 3135-2359

دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات: دراسة تطبيقية على شركة مليته

لطفي عيسى امحمد المقطف – محمد عبد الوهاب محمد التركمان
باحث – وزارة المالية | باحث كلية تقنية الحاسوب طرابلس

The Role of Management Information Systems in Enhancing Cybersecurity and Data Protection: A Case Study of Mellitah Oil & Gas Company

Lotfi Issa Mhammed Al-Muqtaf – Mohamed Abdel Wahab Mohamed Al-Turkman
Researcher – Ministry of Finance | Researcher, Faculty of Computer Technology, Tripoli
l.almagatf@gmail.com – mohammedturkman73@gmail.com

تاريخ الاستلام: 2026/04/02 تاريخ المراجعة 2026 /05/01 تاريخ القبول:2026/05/14- تاريخ النشر: 2026 /06/02

مستخلص الدراسة

تهدف هذه الدراسة إلى دراسة دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل المؤسسات النفطية، مع التركيز على شركة مليته. يتمثل التحدي الرئيسي في تعزيز الأمن السيبراني نتيجة الاعتماد المتزايد على الأنظمة الرقمية، حيث تُشكل الهجمات السيبرانية تهديدًا لسرية البيانات وسلامتها. تعتمد الدراسة على المنهج الوصفي التحليلي، وتستعرض كيفية دمج نظم المعلومات الإدارية مع تقنيات الأمن السيبراني لحماية البيانات وتعزيز إجراءات الوقاية من المخاطر السيبرانية. تهدف الدراسة إلى تقديم حلول فعالة لتعزيز الأمن السيبراني داخل المؤسسات النفطية وتحقيق مستوى أعلى من الحماية ضد التهديدات الإلكترونية المتزايدة.

فيما يتعلق بالجانب الإحصائي، تم استخدام الاستبانة كأداة رئيسية لجمع البيانات من العاملين في شركة مليته. الهدف كان تقييم واقع نظم المعلومات الإدارية ومدى مساهمتها في تعزيز الأمن السيبراني وحماية البيانات داخل الشركة. اعتمد الباحث على البرنامج الإحصائي SPSS لتحليل البيانات، حيث تم استخدام الأساليب الإحصائية الوصفية و التحليلية لاستخراج النتائج.

أظهرت النتائج أن هناك علاقة إيجابية بين نظم المعلومات الإدارية و تحسين الأمان السيبراني في شركة مليته، حيث تساهم هذه الأنظمة في رفع مستوى الأمان وحماية البيانات الحساسة. كما تم تحديد بعض التحديات السيبرانية التي تواجه الشركة، مما يعزز أهمية تحسين إجراءات الحماية وتدريب العاملين على أفضل الممارسات الأمنية. بناءً على التحليل الإحصائي، تم تقديم توصيات عملية لتطوير إجراءات الحماية وتعزيز الأمن السيبراني داخل الشركة.

الكلمات المفتاحية:

- نظم المعلومات الإدارية
- الأمن السيبراني
- حماية البيانات
- المؤسسات النفطية
- الهجمات الإلكترونية
- الأنظمة الرقمية
- التكنولوجيا في المؤسسات
- البيانات الحساسة

Abstract

This study aims to examine the role of Management Information Systems (MIS) in enhancing cybersecurity and data protection within oil companies, with a focus on Mellitah Oil & Gas Company. The main challenge lies in strengthening cybersecurity due to the increasing reliance on digital systems, as cyberattacks pose a significant threat to the confidentiality and integrity of data. The study uses a descriptive-analytical approach, exploring how MIS can be integrated with cybersecurity technologies to protect data and enhance preventive measures against cyber risks. The goal of the study is to provide effective solutions to enhance

cybersecurity within oil companies and achieve a higher level of protection against increasing electronic threats.
Regarding the statistical aspect, a questionnaire was used as the primary tool to collect data from employees at Mellitah Oil & Gas. The aim was to evaluate the current state of MIS and its contribution to enhancing cybersecurity and data protection within the company. The researcher utilized SPSS statistical software to analyze the data, using both descriptive and analytical statistical methods to extract results.
The results revealed a positive correlation between Management Information Systems and improved cybersecurity at Mellitah Oil & Gas, as these systems contribute to increasing security and protecting sensitive data. Some cybersecurity challenges facing the company were also identified, emphasizing the importance of improving security procedures and training employees on best security practices. Based on the statistical analysis, practical recommendations were presented to enhance protection measures and strengthen cybersecurity within the company.

Keywords
- Cybersecurity
- Data Protection
- Oil Companies
- Cyber Attacks
- Digital Systems
- Technology in Organizations
- Sensitive Data

مقدمة

شهد العالم خلال العقود الأخيرة تحولاً جذرياً في بيئة الأعمال نتيجة التطور المتسارع في تكنولوجيا المعلومات والاتصالات، حيث أصبحت نظم المعلومات الإدارية من المرتكزات الأساسية التي تعتمد عليها المؤسسات الحديثة في إدارة عملياتها وأنشطتها المختلفة، لما توفره من إمكانات متقدمة في جمع البيانات ومعالجتها وتحليلها وتحويلها إلى معلومات دقيقة تسهم في دعم عمليات التخطيط والتنظيم والرقابة واتخاذ القرار، كما أسهمت هذه النظم في رفع كفاءة الأداء المؤسسي وتحسين جودة الخدمات وتعزيز القدرة التنافسية للمؤسسات في ظل بيئة عمل تتسم بالتغير المستمر والتطور التقني المتسارع.

وفي ظل هذا التحول الرقمي المتنامي، أصبحت المعلومات والبيانات تمثل مورداً استراتيجياً بالغ الأهمية تعتمد عليه المؤسسات في تحقيق أهدافها التشغيلية والإدارية، الأمر الذي أدى إلى تزايد الحاجة إلى توفير بيئة معلوماتية آمنة قادرة على حماية الأنظمة الإلكترونية وقواعد البيانات من مختلف المخاطر والتهديدات السيبرانية، خاصةً مع تصاعد الهجمات الإلكترونية وتطور أساليب الاختراق الرقمي التي تستهدف المؤسسات بمختلف أنواعها، حيث باتت المؤسسات تواجه تحديات متزايدة تتعلق بسرية المعلومات وسلامة البيانات واستمرارية الخدمات الإلكترونية، مما جعل الأمن السيبراني وحماية البيانات من الأولويات الحيوية التي تحظى باهتمام كبير على المستويين الإداري والتقني.

وتبرز أهمية الأمن السيبراني بصورة أكبر داخل المؤسسات النفطية باعتبارها من المؤسسات الحيوية التي تعتمد بشكل واسع على الأنظمة الرقمية ونظم المعلومات الإدارية في إدارة عملياتها التشغيلية والإدارية والفنية، إضافةً إلى امتلاكها بيانات ومعلومات ذات طبيعة استراتيجية وحساسة، الأمر الذي يجعلها أكثر عرضة للمخاطر الإلكترونية في حال وجود ضعف في أنظمة الحماية أو قصور في إدارة أمن المعلومات، ومن هذا المنطلق تسعى المؤسسات النفطية إلى تطوير نظم معلومات إدارية متقدمة تدعم كفاءة الأداء المؤسسي وتسهم في تعزيز الأمن السيبراني وحماية البيانات من الاختراق أو الفقدان أو سوء الاستخدام.

وتُعد شركة مليته للنفط والغاز من المؤسسات التي تعتمد بصورة كبيرة على نظم المعلومات الإدارية في إدارة أعمالها المختلفة، مما يستدعي ضرورة توفير بنية معلوماتية آمنة قادرة على

مواجهة التهديدات السيبرانية وتعزيز إجراءات حماية البيانات وضمان استمرارية العمل بكفاءة وفاعلية، وعليه جاءت هذه الدراسة لتحليل دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته، من خلال التعرف على واقع هذه النظم ومدى مساهمتها في تحسين أمن المعلومات وتقليل المخاطر الإلكترونية داخل الشركة.

مشكلة الدراسة

أصبحت نظم المعلومات الإدارية من الركائز الأساسية التي تعتمد عليها المؤسسات الحديثة في إدارة أعمالها وبياناتها، خاصةً مع التوسع المتزايد في استخدام الأنظمة الرقمية والتقنيات الإلكترونية، إلا أن هذا التطور صاحبه ارتفاع في مستوى التهديدات السيبرانية والمخاطر الإلكترونية التي تستهدف الأنظمة المعلوماتية وقواعد البيانات، الأمر الذي جعل الأمن السيبراني وحماية البيانات من الأولويات المهمة داخل المؤسسات الحديثة، لا سيما المؤسسات النفطية التي تمتلك بيانات ومعلومات ذات طبيعة استراتيجية وحساسة.

وفي هذا الإطار أشار تقرير Ponemon Institute & Siemens (2017) إلى أن قطاع النفط والغاز يُعد من أكثر القطاعات تعرضاً للهجمات الإلكترونية، نتيجة الاعتماد المتزايد على الأنظمة الرقمية والتقنيات التشغيلية المرتبطة بالشبكات الإلكترونية.

ورغم التطور في استخدام نظم المعلومات الإدارية، إلا أن العديد من المؤسسات ما تزال تواجه تحديات تتعلق بحماية البيانات وتأمين الأنظمة الإلكترونية، مما يبرز الحاجة إلى دراسة مدى مساهمة نظم المعلومات الإدارية في تعزيز الأمن السيبراني داخل المؤسسات النفطية.

ومن هنا جاءت هذه الدراسة لتحليل دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته.

وعليه تتمثل مشكلة الدراسة في التساؤل الرئيس الآتي:

ما دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات في شركة مليته؟

ويتفرع عن هذا التساؤل مجموعة من التساؤلات الفرعية:

1. ما واقع نظم المعلومات الإدارية داخل شركة مليته؟
2. ما مستوى الأمن السيبراني داخل الشركة؟
3. ما مدى مساهمة نظم المعلومات الإدارية في حماية البيانات؟
4. ما أبرز التحديات السيبرانية التي تواجه الشركة؟
5. ما المقترحات التي يمكن أن تسهم في تعزيز الأمن السيبراني وحماية البيانات داخل الشركة؟

أهمية الدراسة

تنبع أهمية هذا الدراسة من أهمية الموضوع الذي يتناوله والمتمثل في دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل المؤسسات النفطية، خاصةً في ظل التوسع المتزايد في استخدام الأنظمة الرقمية وما يصاحبه من ارتفاع في حجم التهديدات السيبرانية والمخاطر الإلكترونية التي تستهدف المعلومات والبيانات المؤسسية، الأمر الذي جعل الأمن السيبراني وحماية البيانات من الأولويات الأساسية داخل المؤسسات الحديثة

أولاً: الأهمية العلمية.

1. الإسهام في إثراء الجانب العلمي والمعرفي المتعلق بنظم المعلومات الإدارية و الأمن السيبراني وحماية البيانات .
2. توضيح طبيعة العلاقة بين نظم المعلومات الإدارية وتعزيز حماية البيانات داخل المؤسسات النفطية .
3. دعم الأدبيات العلمية المتعلقة بالأمن السيبراني في البيئة المؤسسية والإدارية .
4. توفير مرجع علمي يمكن الاستفادة منه من قبل الباحثين والمهتمين بمجال نظم المعلومات والأمن السيبراني .
5. فتح المجال أمام دراسات مستقبلية تتناول موضوع الأمن السيبراني في المؤسسات الحيوية والنفطية .

ثانياً: الأهمية العملية.

1. مساعدة شركة مليته في تطوير نظم الحماية الإلكترونية وتعزيز كفاءة أمن المعلومات .
2. الإسهام في رفع مستوى حماية البيانات وتقليل المخاطر الإلكترونية داخل الشركة .
3. دعم متخذي القرار بالمعلومات المتعلقة بواقع الأمن السيبراني داخل المؤسسة .
4. المساهمة في تحسين الإجراءات والسياسات الخاصة بحماية البيانات وأمن المعلومات .

5. تعزيـــز الـــوعي الأمنـــي لـــدى العـــاملين داخـــل الشـــركة بأهميـــة الأمـــن الســـيبراني وطـــرق حمايـــة المعلومات .
6. تقـــديم مجموعـــة مـــن المقترحـــات العمليـــة التـــي تســـاعد الشـــركة فـــي مواجهـــة التهديـــدات الســـيبرانية وتحسين بيئة العمل الرقمية

أهداف الدراسة

يهدف هذا الدراسة إلى التعرف على دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته، وذلك من خلال تحقيق مجموعة من الأهداف العلمية والعملية التي تتمثل في الآتي.

1. التعرف على واقع نظم المعلومات الإدارية المطبقة داخل شركة مليته .
2. تحليل مستوى الأمن السيبراني المعتمد داخل الشركة .
3. توضيح دور نظم المعلومات الإدارية في تعزيز حماية البيانات وأمن المعلومات .
4. الكشف عن أبرز التهديدات والمخاطر السيبرانية التي تواجه الشركة .
5. التعرف على المعوقات التي تحد من فعالية الأمن السيبراني داخل الشركة .
6. بيان مدى مساهمة نظم المعلومات الإدارية في تقليل المخاطر الإلكترونية وتحسين حماية البيانات .
7. تقديم مجموعة من المقترحات والتوصيات التي تساعد في تعزيز الأمن السيبراني وحماية البيانات داخل الشركة .
8. الإسهام في رفع مستوى الوعي بأهمية الأمن السيبراني داخل البيئة المؤسسية .

تساؤلات الدراسة

يســعى هــذا الدراســة إلــى التعــرف علــى دور نظــم المعلومـــات الإداريـــة فـــي تعزيـــز الأمـــن الســـيبراني وحماية البيانات داخل شركة مليته، وذلك من خلال الإجابة عن التساؤل الرئيس الآتي.

ما دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات في شركة مليته؟

ويتفرع عن هذا التساؤل الرئيس مجموعة من التساؤلات الفرعية التي تتمثل في الآتي.

1. ما واقع نظم المعلومات الإدارية المطبقة داخل شركة مليته؟
2. ما مستوى الأمن السيبراني المعتمد داخل الشركة؟
3. ما مدى مساهمة نظم المعلومات الإدارية في تعزيز حماية البيانات وأمن المعلومات؟
4. ما طبيعة التهديدات والمخاطر السيبرانية التي تواجه شركة مليته؟
5. ما أبرز المعوقات التي تحد من فعالية الأمن السيبراني داخل الشركة؟
6. مـــا المقترحـــات المناســـبة التـــي يمكـــن أن تســـهم فـــي تعزيـــز الأمـــن الســـيبراني وحمايـــة البيانـــات داخل

منهجية الدراسة

اعتمـــدت هـــذه الدراســـة علـــى المـــنهج الوصـــفي التحليلـــي، باعتبـــاره مـــن أكثـــر المنـــاهج العلميـــة ملاءمـــةً لدراســـة الظـــواهر الإداريـــة وتحليـــل العلاقـــات بـــين المتغيـــرات، حيـــث يُســـتخدم هـــذا المـــنهج فـــي وصـــف واقـــع نظـــم المعلومـــات الإداريـــة داخـــل شـــركة مليتـــه، وتحليـــل دورهـــا فـــي تعزيـــز الأمـــن الســـيبراني وحمايـــة البيانـــات، إضـــافةً إلـــى تفســـير طبيعـــة العلاقـــة بـــين نظـــم المعلومـــات الإداريـــة ومســـتوى الأمـــن الســـيبراني داخل الشركة.

كمـــا اعتمـــدت الدراســـة علـــى الاســـتبانة كـــأداة رئيســـية لجمـــع البيانـــات الأوليـــة مـــن العـــاملين داخـــل شـــركة مليتـــه، وذلـــك بهـــدف التعـــرف علـــى آرائهـــم واتجاهـــاتهم حـــول واقـــع نظـــم المعلومـــات الإداريـــة ومـــدى مســـاهمتها فـــي تعزيـــز الأمـــن الســـيبراني وحمايـــة البيانـــات، وقـــد تـــم تصـــميم الاســـتبانة بمـــا يـــتلاءم مـــع أهداف البحث وتساؤلاته.

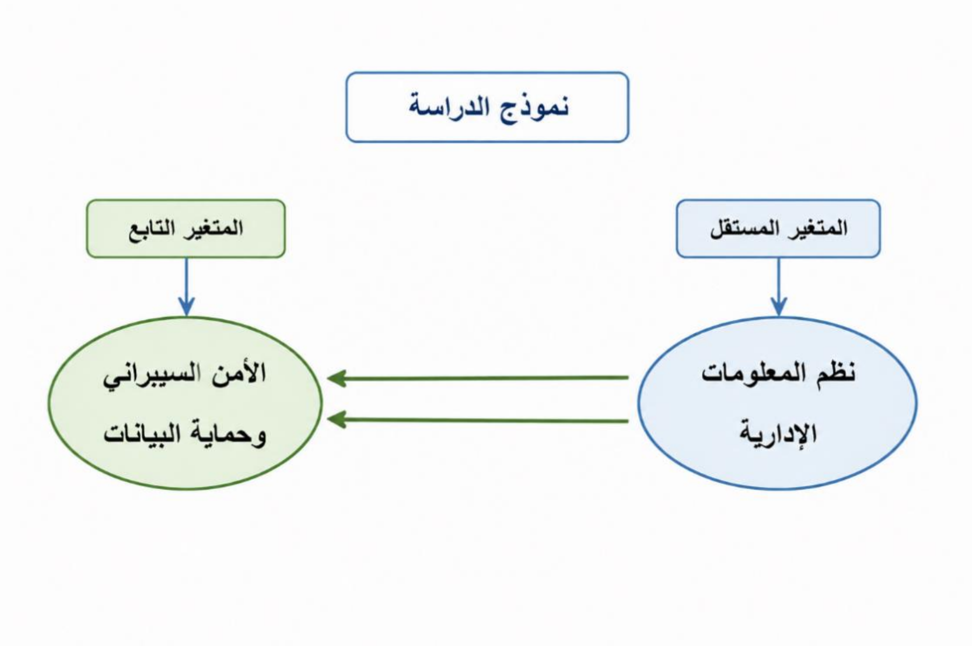
واعتمـــد الباحـــث فـــي تحليـــل البيانـــات علـــى البرنـــامج الإحصـــائي SPSS، وذلـــك لاســـتخراج النتـــائج الإحصـــائية وتحليـــل البيانـــات بصـــورة علميـــة دقيقـــة تســـاعد فـــي تفســـير النتـــائج والوصـــول إلـــى الاستنتاجات والتوصيات المناسبة.

مجتمع وعينة الدراسة

يتكـون مجتمـع الدراسـة مـن جميـع العـاملين فـي الأقسـام الإداريـة والتقنيـة داخـل شـركة مليتـه، باعتبـارهم الأكثـــر ارتباطـــاً باســـتخدام نظـــم المعلومـــات الإداريـــة والتعامـــل مـــع الأنظمـــة الإلكترونيـــة وحمايـــة البيانـــات، الأمـــر الـــذي يجعلهـــم قـــادرين علـــى تقـــديم معلومـــات دقيقـــة حـــول واقـــع الأمـــن الســـيبراني ونظـــم المعلومات داخل الشركة.

نظراً لصعوبة دراسة جميع أفراد المجتمع، تم اختيار **عينة عشوائية** من الموظفين العاملين في الأقسام الإدارية والتقنية. بلغ حجم العينة **43مفردة**، وقد تم توزيع الاستبانة عليهم لجمع البيانات المتعلقة بموضوع الدراسة، بما يعكس طبيعة المتغيرات وواقعية النتائج.

نمودج الدراسة



شكل (1-1) يوضح نموذج الدراسة من اعداد الباحث

حدود الدراسة

تتمثل حدود الدراسة في مجموعة من الحدود الموضوعية والمكانية والبشرية والزمنية التي تحدد إطار الدراسة ومجال تطبيقها، وذلك على النحو الآتي.

الحدود الموضوعية.

يقتصر الدراسة على دراسة دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته، مع التركيز على العلاقة بين نظم المعلومات الإدارية ومستوى الأمن السيبراني وحماية البيانات داخل البيئة المؤسسية.

الحدود المكانية.

تُطبق الدراسة على شركة مليته للنفط والغاز، باعتبارها من المؤسسات النفطية التي تعتمد بصورة كبيرة على نظم المعلومات الإدارية في إدارة عملياتها المختلفة.

الحدود البشرية.

تتمثل الحدود البشرية للدراسة في العاملين بالأقسام الإدارية والتقنية داخل شركة مليته، باعتبارهم الفئة الأكثر ارتباطاً باستخدام نظم المعلومات الإدارية والتعامل مع أنظمة حماية البيانات والأمن السيبراني.

الحدود الزمنية.

تم تطبيق الدراسة خلال الفترة الزمنية الممتدة من 1-1-2026 إلى 31-3-2026.

المصطلحات والمفاهيم

نظم المعلومات الإدارية.

تُعرف نظم المعلومات الإدارية بأنها مجموعة من النظم والإجراءات والوسائل التقنية التي تهدف إلى جمع البيانات ومعالجتها وتحويلها إلى معلومات دقيقة تساعد الإدارة في التخطيط والتنظيم والرقابة واتخاذ القرار داخل المؤسسة، كما تُسهم في دعم الكفاءة الإدارية وتحسين الأداء المؤسسي، وقد عرّفها السالمي بأنها نظام متكامل يربط بين الموارد البشرية والتقنية والمعلوماتية

بهدف توفير المعلومات المناسبة للإدارة في الوقت المناسب، (السالمي، 2018، نظم المعلومات الإدارية).

الأمن السيبراني.

يُقصد بالأمن السيبراني مجموعة السياسات والإجراءات والتقنيات المستخدمة لحماية الأنظمة والشبكات والبيانات من الاختراق أو الهجمات الإلكترونية أو الوصول غير المصرح به، كما يهدف إلى المحافظة على استمرارية الأنظمة وسلامة المعلومات وتقليل المخاطر الرقمية، وقد أشار الحيمودي إلى أن الأمن السيبراني يمثل منظومة متكاملة لحماية الفضاء الرقمي من التهديدات والهجمات الإلكترونية المختلفة، (الحيمودي، 2023، الأمن السيبراني وحماية الأنظمة المعلوماتية).

حماية البيانات.

تُعرف حماية البيانات بأنها مجموعة الإجراءات والتدابير التنظيمية والتقنية التي تهدف إلى المحافظة على سرية البيانات وسلامتها ومنع فقدانها أو تسريبها أو التلاعب بها، بما يضمن حماية المعلومات من الوصول غير المصرح به أو الاستخدام غير القانوني، وقد أشار افتوحة إلى أن حماية البيانات تُعد من المرتكزات الأساسية لضمان أمن المعلومات داخل المؤسسات الحديثة، (افتوحة، 2019، استخدام نظم المعلومات الإلكترونية وأثره على أمن وسلامة المعلومات المحاسبية).

أمن المعلومات.

يُعرف أمن المعلومات بأنه حماية المعلومات والأنظمة المعلوماتية من المخاطر الداخلية والخارجية بما يضمن السرية والسلامة والتوافر، وذلك من خلال تطبيق مجموعة من السياسات والإجراءات الأمنية التي تمنع الوصول غير المصرح به وتحافظ على سلامة البيانات واستمرارية العمل، وقد أوضح دخيل وطلحة ودوزان أن أمن المعلومات يُعد من أهم متطلبات المؤسسات الحديثة في ظل تزايد المخاطر الإلكترونية، (دخيل، طلحة، دوزان، 2022، واقع إدارة أمن المعلومات للإجراءات والسياسات الرقابية وسبل تطوير إدارة أمن نظم المعلومات في المراكز البحثية).

الفصل الأول: الإطار النظري لنظم المعلومات الإدارية

تُعد نظم المعلومات الإدارية من الموضوعات الأساسية في الفكر الإداري المعاصر، نظراً لما تؤديه من دور مهم في تنظيم البيانات ومعالجتها وتحويلها إلى معلومات يمكن الاعتماد عليها في التخطيط واتخاذ القرار والرقابة وتحسين الأداء المؤسسي، فقد أصبحت المؤسسات الحديثة تعتمد على هذه النظم باعتبارها أداة إدارية وتقنية تسهم في رفع كفاءة العمل، وتسهيل تدفق المعلومات بين المستويات التنظيمية المختلفة، ودعم قدرة الإدارة على التعامل مع المتغيرات الداخلية والخارجية بصورة أكثر فاعلية.

ويأتي هذا الفصل لتناول الإطار النظري لنظم المعلومات الإدارية من خلال ثلاثة مباحث رئيسية، حيث يتناول المبحث الأول ماهية نظم المعلومات الإدارية من حيث مفهومها وخصائصها وأهدافها، بينما يعرض المبحث الثاني مكوناتها الأساسية من موارد بشرية وبرمجيات وقواعد بيانات وشبكات وأنظمة اتصال، أما المبحث الثالث فيركز على أهمية نظم المعلومات الإدارية داخل المؤسسات، من خلال دورها في دعم اتخاذ القرار وتحسين الأداء الإداري، إضافةً إلى التحديات التي قد تواجه تطبيقها داخل البيئة المؤسسية.

المبحث الأول: ماهية نظم المعلومات الإدارية

المطلب الأول: مفهوم نظم المعلومات الإدارية

شهدت بيئة الأعمال الحديثة تطورات متسارعة في مجال تكنولوجيا المعلومات والاتصالات، الأمر الذي أدى إلى زيادة اعتماد المؤسسات على نظم المعلومات الإدارية في إدارة أعمالها المختلفة، حيث أصبحت المعلومات مورداً استراتيجياً مهماً يساعد الإدارة على التخطيط والتنظيم والرقابة واتخاذ القرار، كما أسهمت هذه النظم في تحسين كفاءة الأداء الإداري وتنظيم تدفق المعلومات داخل المؤسسة.

وتُعرف نظم المعلومات الإدارية بأنها منظومة متكاملة تضم الأفراد والإجراءات والتقنيات وقواعد البيانات، تعمل بصورة مترابطة لجمع البيانات ومعالجتها وتحويلها إلى معلومات تساعد الإدارة في أداء وظائفها المختلفة، وقد أصبحت هذه النظم من الأدوات الأساسية التي تعتمد عليها المؤسسات الحديثة لتحقيق الكفاءة التشغيلية ومواكبة التطورات التقنية.
وفي هذا الإطار أشار السالمي إلى أن نظم المعلومات الإدارية تهدف إلى توفير المعلومات الدقيقة والملائمة للإدارة من خلال التكامل بين الموارد البشرية والتقنية والإجراءات التنظيمية بما يساعد على رفع كفاءة الأداء الإداري، (السالمي، 2006).[1] كما يرى سعد غالب ياسين أن نظم المعلومات الإدارية تسهم في دعم وظائف الإدارة المختلفة وتحسين جودة القرارات من خلال توفير المعلومات الدقيقة في الوقت المناسب، (ياسين، 2018).[2]
وتبرز أهمية نظم المعلومات الإدارية بصورة خاصة داخل المؤسسات الكبيرة والمؤسسات النفطية التي تعتمد على حجم كبير من البيانات والمعلومات، حيث تساعد هذه النظم على تنظيم البيانات وتحليلها بصورة دقيقة وآمنة، الأمر الذي يسهم في تحسين الأداء المؤسسي وتعزيز القدرة على مواجهة التغيرات والتحديات الحديثة.

المطلب الثاني: خصائص نظم المعلومات الإدارية

تتميز نظم المعلومات الإدارية بمجموعة من الخصائص التي جعلتها من الأنظمة الأساسية التي تعتمد عليها المؤسسات الحديثة في إدارة أعمالها، حيث تسهم في تحسين الأداء الإداري ورفع كفاءة العمل ودعم عملية اتخاذ القرار، كما تساعد المؤسسات على التكيف مع التطورات التقنية والتغيرات البيئية المتسارعة.
ومن أهم خصائص نظم المعلومات الإدارية التكامل بين المكونات البشرية والتقنية والتنظيمية، حيث تعمل هذه العناصر بصورة مترابطة لتحقيق أهداف المؤسسة، فالنظام لا يقتصر على الأجهزة والبرمجيات فقط، بل يشمل أيضاً العنصر البشري والإجراءات التنظيمية وقواعد البيانات، وقد أشار السالمي إلى أن التكامل بين هذه العناصر يمثل الأساس الذي تقوم عليه نظم المعلومات الإدارية الحديثة، (السالمي، 2006).[1]
كما تتميز نظم المعلومات الإدارية بقدرتها على توفير المعلومات الدقيقة والملائمة في الوقت المناسب، إذ تعتمد الإدارة على هذه النظم في الحصول على المعلومات اللازمة لاتخاذ القرارات الإدارية، ولذلك تُعد جودة المعلومات من أهم الخصائص التي تميز نظم المعلومات الإدارية، وقد أوضح ياسين أن فعالية نظم المعلومات الإدارية ترتبط بمدى جودة المعلومات التي تقدمها للإدارة، (ياسين، 2018).[2]
ومن الخصائص المهمة أيضاً السرعة في معالجة البيانات واسترجاع المعلومات، حيث تساعد هذه النظم على اختصار الوقت والجهد وتحسين سرعة إنجاز الأعمال داخل المؤسسة، إضافةً إلى المرونة والقدرة على التكيف مع المتغيرات المختلفة من خلال تحديث الأنظمة وتطويرها بما يتناسب مع احتياجات المؤسسة.
كما تتميز نظم المعلومات الإدارية بقدرتها على دعم اتخاذ القرار من خلال توفير التقارير والتحليلات اللازمة للإدارة، إضافةً إلى تعزيز الاتصال والتنسيق بين الأقسام المختلفة داخل المؤسسة، فضلاً عن توفير إجراءات الحماية والأمن التي تساعد على حماية البيانات والمعلومات من الاختراق أو الفقدان أو سوء الاستخدام.
وبناءً على ما سبق، يمكن القول إن نظم المعلومات الإدارية تتميز بمجموعة من الخصائص التي تجعلها أداة فعالة في تحسين الأداء الإداري وتنظيم المعلومات ودعم القرارات الإدارية داخل المؤسسات الحديثة.

المطلب الثالث: أهداف نظم المعلومات الإدارية

تسعى نظم المعلومات الإدارية إلى تحقيق مجموعة من الأهداف التي تساعد المؤسسات على تحسين الأداء الإداري والتنظيمي، من خلال توفير المعلومات الدقيقة والملائمة التي تحتاجها الإدارة في التخطيط والتنظيم والرقابة واتخاذ القرار، وقد أصبحت هذه النظم من الأدوات الأساسية التي تعتمد عليها المؤسسات الحديثة في إدارة أعمالها وتحقيق أهدافها بكفاءة.
ومن أهم أهداف نظم المعلومات الإدارية توفير المعلومات الدقيقة والحديثة للإدارة، حيث تعمل على جمع البيانات ومعالجتها وتحويلها إلى معلومات تساعد الإدارة في اتخاذ القرارات المناسبة، وقد أشار عبد الهادي إلى أن نظم المعلومات الإدارية تهدف إلى تزويد الإدارة بالمعلومات الملائمة في الوقت المناسب بما يساعدها على أداء وظائفها المختلفة بكفاءة، (عبد الهادي، 2017).[1]
كما تهدف نظم المعلومات الإدارية إلى دعم اتخاذ القرار وتحسين كفاءة الأداء المؤسسي، من خلال تسريع إنجاز الأعمال وتقليل الوقت والجهد وتحسين تدفق المعلومات بين الإدارات المختلفة داخل المؤسسة.

وتهدف هذه النظم أيضاً إلى تعزيز الرقابة والمتابعة وتحسين الاتصال الإداري، وقد أوضح الكبيسي أن نظم المعلومات الإدارية تسهم بصورة كبيرة في تطوير الرقابة الإدارية وتحسين الكفاءة التنظيمية داخل المؤسسات، (الكبيسي، 2015).[2]
وفي ظل التوسع في استخدام الأنظمة الرقمية، أصبحت نظم المعلومات الإدارية تهدف كذلك إلى تعزيز أمن المعلومات وحماية البيانات من المخاطر والتهديدات الإلكترونية، بما يضمن سلامة المعلومات واستمرارية العمل داخل المؤسسة.

المبحث الثاني: مكونات نظم المعلومات الإدارية

المطلب الأول: الموارد البشرية في نظم المعلومات

تُعد الموارد البشرية من المكونات الأساسية لنظم المعلومات الإدارية، حيث تمثل العنصر المسؤول عن تشغيل الأنظمة المعلوماتية وإدارتها والاستفادة من مخرجاتها في دعم الأنشطة الإدارية داخل المؤسسة، لذلك فإن نجاح نظم المعلومات لا يعتمد فقط على الأجهزة والبرمجيات، بل يرتبط بوجود أفراد يمتلكون المهارات والخبرات اللازمة للتعامل مع هذه الأنظمة.
وتشمل الموارد البشرية جميع الأفراد المتعاملين مع النظام، مثل محللي النظم والمبرمجين ومشرفي قواعد البيانات والمستخدمين الإداريين، حيث يؤدي كل عنصر دوراً مهماً في ضمان كفاءة النظام وتحقيق أهدافه.
وقد أشار العلاق إلى أن العنصر البشري يُعد من أهم عناصر نظم المعلومات الإدارية نظراً لدوره في تشغيل النظام وتحليل البيانات واستخدام المعلومات في دعم القرارات الإدارية، (العلاق، 2014).[1] كما يرى نجم عبود نجم أن الموارد البشرية تمثل القوة المحركة لنظم المعلومات الإدارية، وأن نجاح هذه النظم يعتمد بدرجة كبيرة على مستوى تدريب وتأهيل العاملين، (نجم، 2016).[2]
كما تسهم الموارد البشرية في تشغيل الأنظمة وتطويرها وتنظيم تدفق المعلومات وتعزيز أمن البيانات داخل المؤسسة، الأمر الذي يجعل تنمية مهارات العاملين وتدريبهم بصورة مستمرة من العوامل الضرورية لنجاح نظم المعلومات الإدارية.

المطلب الثاني: البرمجيات وقواعد البيانات

تُعد البرمجيات وقواعد البيانات من المكونات الأساسية لنظم المعلومات الإدارية، حيث تمثل البرمجيات الجانب التشغيلي المسؤول عن معالجة البيانات وتشغيل النظام، بينما تمثل قواعد البيانات الوعاء المنظم الذي تُحفظ فيه البيانات ويتم من خلاله تخزين المعلومات واسترجاعها وتحديثها بصورة دقيقة ومنظمة.
وتشمل البرمجيات مجموعة البرامج والتطبيقات المستخدمة في تشغيل النظام وإعداد التقارير وتحليل البيانات، وقد أشار الصيرفي إلى أن البرمجيات تُعد من العناصر الأساسية في نظم المعلومات لأنها تقوم بمعالجة البيانات وتحويلها إلى معلومات تساعد الإدارة في أداء وظائفها المختلفة، (الصيرفي، 2012).[1]
أما قواعد البيانات، فهي تمثل البنية المنظمة التي يتم من خلالها حفظ البيانات وربطها واسترجاعها عند الحاجة، كما تساعد على تقليل التكرار وتحسين دقة المعلومات، ويرى قنديلجي والجنابي أن قواعد البيانات تُعد مورداً معلوماتياً مهماً يساعد على تنظيم البيانات ومعالجتها بما يخدم متطلبات الإدارة، (قنديلجي والجنابي، 2015).[2]
وتبرز أهمية البرمجيات وقواعد البيانات في تسهيل إنجاز الأعمال الإدارية وتحسين سرعة تدفق المعلومات ودعم اتخاذ القرار، كما يرتبط هذا المكون بصورة مباشرة بحماية البيانات والأمن السيبراني، لأن ضعف البرمجيات أو سوء إدارة قواعد البيانات قد يؤدي إلى فقدان المعلومات أو اختراقها، لذلك تحتاج المؤسسات إلى تحديث البرمجيات وتطبيق إجراءات حماية فعالة لضمان أمن البيانات واستمرارية العمل.

المطلب الثالث: الشبكات وأنظمة الاتصال

تُعد الشبكات وأنظمة الاتصال من المكونات الأساسية لنظم المعلومات الإدارية، نظراً لدورها في ربط أجهزة الحاسوب والأنظمة المختلفة داخل المؤسسة، وتسهيل تبادل البيانات والمعلومات بين الأقسام والمستويات الإدارية المختلفة، مما يسهم في تحسين كفاءة الأداء الإداري وسرعة إنجاز الأعمال.
وتشير الشبكات إلى مجموعة من أجهزة الحاسوب المرتبطة ببعضها بهدف تبادل المعلومات والموارد إلكترونياً، بينما تُعرف أنظمة الاتصال بأنها الوسائل المستخدمة لنقل المعلومات بين الأفراد والأجهزة داخل المؤسسة أو خارجها.

وقد أشار عبد الستار العلي إلى أن الشبكات وأنظمة الاتصال تمثل البنية الأساسية التي تعتمد عليها نظم المعلومات الإدارية في نقل البيانات والمعلومات بين المستخدمين، كما تساعد على تحسين الاتصال الإداري وسرعة الوصول إلى المعلومات، (العلي، 2011).[1] كما يرى حسن العمري أن الشبكات الإلكترونية أصبحت من المتطلبات الضرورية لنجاح نظم المعلومات الإدارية، لأنها تسهم في ربط الإدارات المختلفة وتسهيل تبادل المعلومات بصورة فورية، (العمري، 2014).[2]

وتبرز أهمية الشبكات وأنظمة الاتصال في تسهيل تدفق المعلومات ودعم التنسيق بين الإدارات وتحسين الرقابة والمتابعة، كما ترتبط بصورة مباشرة بالأمن السيبراني وحماية البيانات، نظراً لزيادة المخاطر الإلكترونية المرتبطة باستخدام الشبكات، مما يدفع المؤسسات إلى تطبيق وسائل حماية مثل التشفير والجدران النارية وأنظمة مراقبة الشبكات.

وبناءً على ما سبق، يتضح أن الشبكات وأنظمة الاتصال تمثل عنصراً مهماً في نظم المعلومات الإدارية، لما تؤديه من دور في دعم الاتصال الإداري وتبادل المعلومات وتعزيز أمن البيانات داخل المؤسسات الحديثة.

المبحث الثالث: أهمية نظم المعلومات الإدارية في المؤسسات

المطلب الأول: دور نظم المعلومات في دعم اتخاذ القرار

تُعد عملية اتخاذ القرار من أهم الوظائف الإدارية داخل المؤسسة، حيث ترتبط جودة القرار بدرجة كبيرة بجودة المعلومات المتاحة للإدارة، ولذلك تبرز أهمية نظم المعلومات الإدارية باعتبارها أداة رئيسية تساعد الإدارة على توفير المعلومات الدقيقة والحديثة اللازمة لاتخاذ القرارات المناسبة.

وتقوم نظم المعلومات الإدارية بدور مهم في دعم اتخاذ القرار من خلال جمع البيانات ومعالجتها وتحليلها وتحويلها إلى معلومات واضحة تساعد الإدارة على دراسة المشكلات وتقييم البدائل المختلفة، كما توفر التقارير التي تساعد في متابعة الأداء واكتشاف الانحرافات بصورة سريعة.

وقد أشار الطائي إلى أن نظم المعلومات الإدارية تسهم في ترشيد القرارات الإدارية من خلال توفير المعلومات المناسبة في الوقت المناسب وتقليل المخاطر المرتبطة بنقص المعلومات، (الطائي، 2013).[1] كما يرى المغربي أن نظم المعلومات الإدارية تمثل أداة مساندة للإدارة في جميع مراحل اتخاذ القرار، بدءاً من تحديد المشكلة وحتى متابعة تنفيذ القرار، (المغربي، 2016).[2]

وتساعد نظم المعلومات الإدارية على تحسين القرارات الاستراتيجية والتشغيلية من خلال توفير قاعدة معلومات متكاملة تدعم التخطيط والرقابة والمتابعة داخل المؤسسة، كما يزداد دورها في المؤسسات النفطية نظراً لحساسية البيانات والعمليات التشغيلية المرتبطة بها.

كما ترتبط نظم المعلومات الإدارية بقرارات الأمن السيبراني وحماية البيانات، حيث توفر للإدارة المعلومات المتعلقة بأمن الأنظمة والشبكات، بما يساعد على اتخاذ الإجراءات الوقائية وتقليل المخاطر الإلكترونية.

وبناءً على ما سبق، يتضح أن نظم المعلومات الإدارية تؤدي دوراً مهماً في دعم اتخاذ القرار من خلال توفير المعلومات الدقيقة وتحليل البدائل وتحسين الرقابة، الأمر الذي يسهم في رفع كفاءة القرارات الإدارية داخل المؤسسة.

المطلب الثاني: دور نظم المعلومات في تحسين الأداء الإداري

أصبحت نظم المعلومات الإدارية من الوسائل الأساسية التي تعتمد عليها المؤسسات الحديثة في تحسين الأداء الإداري ورفع مستوى الكفاءة التنظيمية، وذلك لما توفره من معلومات دقيقة وسريعة تساعد الإدارة على تنفيذ وظائفها المختلفة بصورة أكثر فاعلية.

ويُقصد بالأداء الإداري قدرة المؤسسة على تنفيذ أعمالها وتحقيق أهدافها بكفاءة من خلال الاستخدام الأمثل للموارد المتاحة، وتؤدي نظم المعلومات الإدارية دوراً مهماً في تحسين هذا الأداء عبر توفير المعلومات اللازمة للتخطيط والتنظيم والرقابة واتخاذ القرار.

وقد أشار السكارنة إلى أن نظم المعلومات الإدارية تسهم بصورة مباشرة في رفع كفاءة الأداء الإداري من خلال تسريع إنجاز الأعمال وتوفير المعلومات الدقيقة التي تساعد الإدارة على متابعة الأداء وتقييمه بصورة مستمرة، (السكارنة، 2011).[1] كما يرى حريم أن نظم المعلومات الإدارية تساعد على تحسين الاتصال الإداري وتنظيم تدفق المعلومات وتقليل التعقيدات الروتينية المرتبطة بالعمل الإداري، مما يؤدي إلى رفع مستوى الكفاءة والإنتاجية داخل المؤسسة، (حريم، 2013).[2]

كما تسهم نظم المعلومات الإدارية في تحسين الرقابة والمتابعة، وتعزيز التنسيق بين الإدارات المختلفة، إضافةً إلى تسريع إنجاز الأعمال وتقليل الوقت والجهد، فضلاً عن دورها في دعم الأمن السيبراني وحماية البيانات داخل المؤسسة.

وتزداد أهمية نظم المعلومات الإدارية في المؤسسات النفطية نظراً لحجم العمليات والبيانات التي يتم التعامل معها بصورة يومية، حيث تساعد هذه النظم على تحسين كفاءة العمليات الإدارية والفنية وتعزيز سرعة تبادل المعلومات بين الإدارات المختلفة.
وبناءً على ما سبق، يتضح أن نظم المعلومات الإدارية تؤدي دوراً مهماً في تحسين الأداء الإداري من خلال توفير المعلومات الدقيقة، وتحسين الرقابة، وتعزيز الاتصال والتنسيق، ودعم الأمن السيبراني وحماية البيانات داخل المؤسسة.

المطلب الثالث: التحديات التي تواجه نظم المعلومات الإدارية

على الرغم من الأهمية الكبيرة لنظم المعلومات الإدارية في تحسين الأداء الإداري ودعم اتخاذ القرار، إلا أن تطبيق هذه النظم يواجه العديد من التحديات التي قد تؤثر في كفاءتها وفاعليتها داخل المؤسسات، خاصةً مع التطور السريع في تكنولوجيا المعلومات وزيادة الاعتماد على الأنظمة الرقمية.
ومن أبرز التحديات ضعف البنية التحتية التقنية، حيث تحتاج نظم المعلومات إلى أجهزة وشبكات وبرمجيات حديثة حتى تعمل بكفاءة، وقد أشار عبيدات إلى أن ضعف الإمكانات التقنية وعدم توافر البنية التحتية المناسبة يؤثر سلباً على كفاءة نظم المعلومات الإدارية وقدرتها على توفير المعلومات الدقيقة، (عبيدات، 2012).[1]
كما تُعد قلة الكفاءات البشرية المؤهلة من التحديات المهمة، إذ يعتمد نجاح نظم المعلومات الإدارية على وجود أفراد يمتلكون المهارات اللازمة للتعامل مع الأنظمة الحديثة، إضافةً إلى وجود مقاومة للتغيير من قبل بعض العاملين، ويرى درادكة والشناق أن مقاومة التغيير التنظيمي تُعد من أبرز التحديات التي تواجه تطبيق نظم المعلومات الإدارية داخل المؤسسات، (درادكة والشناق، 2016).[2]
ومن التحديات الأخرى ارتفاع التكاليف المالية المتعلقة بإنشاء الأنظمة وصيانتها وتحديثها، إضافةً إلى المشكلات المرتبطة بجودة البيانات ودقتها، حيث إن ضعف البيانات يؤدي إلى إنتاج معلومات غير دقيقة تؤثر في جودة القرارات الإدارية.
كما تواجه نظم المعلومات الإدارية تحديات أمنية مرتبطة بالاختراقات الإلكترونية وسرقة البيانات والهجمات السيبرانية، الأمر الذي يجعل حماية المعلومات والأمن السيبراني من المتطلبات الأساسية لضمان استمرارية عمل الأنظمة داخل المؤسسات الحديثة.
وبناءً على ما سبق، يتضح أن نظم المعلومات الإدارية تواجه تحديات تقنية وبشرية وتنظيمية وأمنية، مما يتطلب من المؤسسات تطوير بنيتها التحتية، وتأهيل العاملين، وتعزيز إجراءات الأمن السيبراني بصورة مستمرة لضمان كفاءة هذه النظم وتحقيق أهدافها.

الفصل الثاني: الأمن السيبراني وحماية البيانات

شهد العالم خلال السنوات الأخيرة تطوراً متسارعاً في استخدام تكنولوجيا المعلومات والاتصالات والتحول نحو الأنظمة الرقمية، الأمر الذي أدى إلى زيادة الاعتماد على الشبكات الإلكترونية ونظم المعلومات في إدارة الأعمال والعمليات المؤسسية، وفي المقابل ظهرت العديد من المخاطر والتهديدات الإلكترونية التي تستهدف الأنظمة والبيانات، مما جعل الأمن السيبراني وحماية البيانات من القضايا المهمة داخل المؤسسات الحديثة.
ويُعد الأمن السيبراني من المرتكزات الأساسية لحماية الأنظمة الإلكترونية والبيانات من الاختراق أو الفقدان أو سوء الاستخدام، حيث تسعى المؤسسات إلى تطبيق سياسات وإجراءات وتقنيات تضمن سرية المعلومات وسلامتها واستمرارية العمل، خاصةً مع تزايد الهجمات الإلكترونية وتطور أساليب الاختراق الرقمي.
كما تُعد حماية البيانات من المتطلبات الضرورية لضمان أمن المعلومات واستقرار الأنظمة الإلكترونية، نظراً لما تمثله البيانات من مورد استراتيجي تعتمد عليه المؤسسات في تنفيذ أعمالها واتخاذ قراراتها، الأمر الذي دفع المؤسسات إلى تطوير أنظمة الحماية الإلكترونية وتعزيز الوعي الأمني لدى العاملين.
ويتناول هذا الفصل الأمن السيبراني وحماية البيانات من خلال ثلاثة مباحث رئيسية، حيث يتناول المبحث الأول مفهوم الأمن السيبراني وأهدافه والتهديدات الإلكترونية، بينما يتناول المبحث الثاني مفهوم حماية البيانات وأهميتها وآليات حمايتها، أما المبحث الثالث فيركز على دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل المؤسسات الحديثة.

المبحث الأول: الإطار المفاهيمي للأمان السيبراني

المطلب الأول: مفهوم الأمن السيبراني

أصبح الأمن السيبراني من المفاهيم الحديثة التي حظيت باهتمام واسع في ظل التطور المتسارع في تكنولوجيا المعلومات والاتصالات والتوسع في استخدام الأنظمة الرقمية داخل المؤسسات، حيث أدى الاعتماد المتزايد على التقنيات الحديثة إلى ظهور العديد من التهديدات والمخاطر الإلكترونية التي تستهدف الأنظمة المعلوماتية والبيانات، الأمر الذي جعل المؤسسات في حاجة مستمرة إلى تطبيق أنظمة حماية فعالة تضمن أمن المعلومات وسلامة البيانات.

ويُشير مفهوم الأمن السيبراني إلى مجموعة الإجراءات والسياسات والتقنيات المستخدمة لحماية الأنظمة الإلكترونية والشبكات وقواعد البيانات من الاختراق أو الهجمات الإلكترونية أو الوصول غير المصرح به، كما يهدف إلى المحافظة على سرية المعلومات وسلامتها واستمرارية العمل.

وقد أشار الحيمودي إلى أن الأمن السيبراني يُمثل منظومة متكاملة من الوسائل التقنية والإدارية التي تهدف إلى حماية الفضاء الرقمي من التهديدات الإلكترونية المختلفة، (الحيمودي، 2023).[1]
كما يرى الجنفاوي أن الأمن السيبراني يُعد من المتطلبات الأساسية للمؤسسات الحديثة نظراً لاعتمادها الكبير على الأنظمة الرقمية في إدارة أعمالها، وأنه لا يقتصر على الجانب التقني فقط بل يشمل الجوانب الإدارية والتنظيمية والتوعوية، (الجنفاوي، 2021).[2]

ويعتمد الأمن السيبراني على مجموعة من المبادئ الأساسية، مثل السرية والسلامة والتوافر، كما يشمل إجراءات أمنية متعددة مثل التشفير والجدران النارية وأنظمة كشف الاختراق ومراقبة الشبكات، وذلك بهدف حماية الأنظمة والبيانات من المخاطر الإلكترونية المختلفة.

وتزداد أهمية الأمن السيبراني في المؤسسات النفطية نظراً لحساسية المعلومات المرتبطة بالإنتاج والتشغيل، كما يرتبط بصورة مباشرة بنظم المعلومات الإدارية التي تعتمد على الشبكات الإلكترونية وقواعد البيانات في إدارة المعلومات وتبادلها.

وبناءً على ما سبق، يتضح أن الأمن السيبراني يُعد من العناصر الأساسية لحماية الأنظمة الإلكترونية والبيانات داخل المؤسسات الحديثة وضمان استمرارية العمل بصورة آمنة.

المطلب الثاني: أهداف الأمن السيبراني

يهدف الأمن السيبراني إلى حماية الأنظمة المعلوماتية والشبكات الإلكترونية والبيانات الرقمية من التهديدات والمخاطر الإلكترونية التي قد تؤثر على كفاءة العمل واستمرارية الأنشطة داخل المؤسسات، وقد ازدادت أهمية الأمن السيبراني مع التوسع في استخدام التكنولوجيا والتحول الرقمي واعتماد المؤسسات على الأنظمة الإلكترونية في إدارة أعمالها المختلفة.

ومن أهم أهداف الأمن السيبراني المحافظة على سرية المعلومات والبيانات ومنع الوصول غير المصرح به إلى الأنظمة وقواعد البيانات، خاصةً في المؤسسات التي تمتلك معلومات حساسة واستراتيجية، كما يهدف إلى حماية سلامة البيانات من التعديل أو التلاعب أو الإتلاف، وضمان بقائها صحيحة ودقيقة.

وقد أشار الزغبي إلى أن الهدف الأساسي للأمن السيبراني يتمثل في حماية المعلومات الرقمية والمحافظة على سرية البيانات وسلامتها وضمان استمرارية الأنظمة الإلكترونية داخل المؤسسة، (الزغبي، 2020).[1] كما يرى الشوابكة أن الأمن السيبراني يهدف إلى تقليل المخاطر الإلكترونية وحماية البنية التحتية الرقمية من خلال تطبيق السياسات والإجراءات الأمنية المناسبة، (الشوابكة، 2021).[2]

كما يهدف الأمن السيبراني إلى ضمان توافر المعلومات واستمرارية عمل الأنظمة الإلكترونية، وحماية الشبكات من الهجمات الإلكترونية والبرمجيات الخبيثة، إضافةً إلى تعزيز الثقة في الأنظمة الرقمية والمعاملات الإلكترونية داخل المؤسسات.

وفي ظل التوسع في استخدام نظم المعلومات الإدارية، أصبح الأمن السيبراني يهدف أيضاً إلى حماية قواعد البيانات والأنظمة المعلوماتية من الاختراقات والمخاطر الإلكترونية، خاصةً داخل المؤسسات النفطية التي تعتمد بصورة كبيرة على البيانات والأنظمة الرقمية في إدارة أعمالها.

وبناءً على ما سبق، يتضح أن الأمن السيبراني يهدف إلى حماية المعلومات والأنظمة الإلكترونية، والمحافظة على سرية البيانات وسلامتها وتوافرها، إضافةً إلى ضمان استمرارية العمل وتعزيز أمن البيئة الرقمية داخل المؤسسات الحديثة.

المطلب الثالث: أنواع التهديدات والهجمات الإلكترونية

أدى التوسع في استخدام الأنظمة الرقمية والشبكات الإلكترونية إلى ظهور العديد من التهديدات والهجمات الإلكترونية التي تستهدف المعلومات والبيانات والأنظمة التقنية داخل المؤسسات، مما جعل المؤسسات الحديثة تواجه مخاطر متزايدة تهدد أمن المعلومات واستمرارية العمل.

وتُعرف التهديدات الإلكترونية بأنها المخاطر أو الأنشطة التي تستهدف الأنظمة المعلوماتية بهدف اختراقها أو تعطيلها أو سرقة البيانات منها، بينما تُشير الهجمات الإلكترونية إلى المحاولات المتعمدة للوصول غير المصرح به إلى الأنظمة أو إلحاق الضرر بها.
وقد أشار الحربي إلى أن التهديدات الإلكترونية تُعد من أخطر التحديات التي تواجه المؤسسات الحديثة بسبب تطور أساليب الاختراق والهجمات الرقمية، (الحربي، 2021).[1] كما يرى أبو العلا أن الهجمات الإلكترونية أصبحت أكثر تعقيداً وتنظيماً وتستهدف المؤسسات الحيوية بهدف تعطيل الأنظمة أو سرقة المعلومات، (أبو العلا، 2020).[2]
ومن أبرز أنواع التهديدات والهجمات الإلكترونية الفيروسات والبرمجيات الخبيثة، وهجمات التصيد الإلكتروني، وهجمات حجب الخدمة، إضافةً إلى الاختراقات غير المصرح بها وبرامج الفدية التي تقوم بتشفير البيانات وطلب مبالغ مالية مقابل استعادتها.
كما تواجه المؤسسات تهديدات داخلية ناتجة عن أخطاء العاملين أو سوء استخدام الأنظمة أو تسريب البيانات، مما يجعل العنصر البشري أحد الجوانب المهمة في منظومة الأمن السيبراني.
وتزداد خطورة هذه التهديدات داخل المؤسسات النفطية نظراً لحساسية البيانات المرتبطة بالإنتاج والتشغيل، لذلك تعتمد المؤسسات على إجراءات أمنية مثل التشفير والجدران النارية وأنظمة كشف الاختراق والنسخ الاحتياطي لتعزيز حماية المعلومات وتقليل المخاطر الإلكترونية.
وبناءً على ما سبق، يتضح أن التهديدات والهجمات الإلكترونية تمثل خطراً حقيقياً على نظم المعلومات والبيانات المؤسسية، الأمر الذي يتطلب تطوير أنظمة الحماية وتعزيز إجراءات الأمن السيبراني بصورة مستمرة.

المبحث الثاني: حماية البيانات داخل المؤسسات

المطلب الأول: مفهوم حماية البيانات

أصبحت حماية البيانات من الموضوعات المهمة في ظل التطور الكبير في تكنولوجيا المعلومات والتوسع في استخدام الأنظمة الرقمية داخل المؤسسات، حيث تعتمد المؤسسات الحديثة بصورة كبيرة على البيانات والمعلومات في إدارة أعمالها، الأمر الذي جعل من الضروري توفير إجراءات فعالة لحماية هذه البيانات من الفقدان أو الاختراق أو سوء الاستخدام.
ويُقصد بحماية البيانات مجموعة السياسات والإجراءات والتقنيات التي تهدف إلى المحافظة على سرية البيانات وسلامتها وتوافرها، ومنع الوصول غير المصرح به إليها، إضافةً إلى حمايتها من التعديل أو الإتلاف أو التسريب.
وقد أشار الحسن إلى أن حماية البيانات تُعد من الركائز الأساسية لأمن المعلومات، لأنها تهدف إلى حماية البيانات الرقمية من المخاطر والتهديدات الإلكترونية المختلفة وضمان استخدامها بصورة آمنة داخل المؤسسات، (الحسن، 2019).[1] كما يرى عبد الرؤوف أن حماية البيانات تمثل مجموعة من التدابير الوقائية التي تهدف إلى منع الوصول غير المشروع إلى المعلومات أو التلاعب بها من خلال تطبيق سياسات وإجراءات رقابية فعالة، (عبد الرؤوف، 2021).[2]
وتعتمد حماية البيانات على مجموعة من الإجراءات الأمنية، مثل التشفير، وإدارة كلمات المرور، وتحديد صلاحيات الوصول، والنسخ الاحتياطي، واستخدام برامج الحماية والجدران النارية، وذلك بهدف تقليل المخاطر الإلكترونية وضمان أمن المعلومات.
وتبرز أهمية حماية البيانات بصورة خاصة داخل المؤسسات النفطية نظراً لحساسية المعلومات المتعلقة بالإنتاج والتشغيل، كما ترتبط حماية البيانات بصورة مباشرة بالأمن السيبراني ونظم المعلومات الإدارية التي تعتمد على تخزين البيانات وتبادلها عبر الشبكات الإلكترونية.
وبناءً على ما سبق، يتضح أن حماية البيانات تمثل عنصراً أساسياً في البيئة الرقمية الحديثة، لما تؤديه من دور في حماية المعلومات وضمان سرية البيانات وسلامتها واستمرارية استخدامها داخل المؤسسات.

المطلب الثاني: أهمية حماية البيانات

تُعد حماية البيانات من المتطلبات الأساسية التي تعتمد عليها المؤسسات الحديثة في الحفاظ على أمن المعلومات وضمان استمرارية العمل داخل البيئة الرقمية، حيث أصبحت البيانات مورداً استراتيجياً مهماً تعتمد عليه المؤسسات في إدارة أعمالها واتخاذ قراراتها، الأمر الذي جعل حمايتها ضرورة تنظيمية وتقنية في ظل التوسع في استخدام الأنظمة الإلكترونية.
وتبرز أهمية حماية البيانات في المحافظة على سرية المعلومات ومنع الوصول غير المصرح به إليها، خاصةً البيانات الحساسة المتعلقة بالإدارة أو العمليات التشغيلية أو المعلومات المالية، حيث إن أي تسريب أو اختراق لهذه البيانات قد يؤدي إلى خسائر مالية وتنظيمية كبيرة.

وقد أشار عبد الحميد إلى أن أهمية حماية البيانات تكمن في دورها في المحافظة على أمن المعلومات وضمان سلامتها ومنع التلاعب بها أو فقدانها، (عبد الحميد، 2020).[1] كما يرى السلمي أن حماية البيانات تُعد من الركائز الأساسية لاستقرار المؤسسات واستمرارية عملها والحد من المخاطر والتهديدات السيبرانية، (السلمي، 2021).[2]

كما تساعد حماية البيانات على ضمان سلامة المعلومات ودقتها، واستمرارية العمل داخل المؤسسة من خلال أنظمة النسخ الاحتياطي والحماية الإلكترونية، إضافةً إلى تعزيز الثقة في الأنظمة الرقمية وتقليل احتمالية التعرض للهجمات الإلكترونية أو سرقة المعلومات.

وتزداد أهمية حماية البيانات داخل المؤسسات النفطية نظراً لحساسية المعلومات المرتبطة بالإنتاج والتشغيل، كما ترتبط بصورة مباشرة بنظم المعلومات الإدارية التي تعتمد على تخزين البيانات ومعالجتها بصورة مستمرة.

وبناءً على ما سبق، يتضح أن حماية البيانات تؤدي دوراً مهماً في حماية المعلومات وضمان سلامتها واستمرارية العمل وتقليل المخاطر الإلكترونية داخل المؤسسات الحديثة.

المطلب الثالث: آليات وسياسات حماية البيانات

تعتمد المؤسسات الحديثة على مجموعة من الآليات والسياسات الأمنية التي تهدف إلى حماية البيانات والمعلومات من المخاطر والتهديدات الإلكترونية، خاصةً مع التوسع في استخدام الأنظمة الرقمية والشبكات الإلكترونية في إدارة الأعمال والعمليات المؤسسية.

وتُشير آليات حماية البيانات إلى الوسائل والإجراءات التقنية والتنظيمية المستخدمة لحماية المعلومات من الاختراق أو الفقدان أو الوصول غير المصرح به، بينما تُعرف سياسات حماية البيانات بأنها القواعد والتعليمات التي تنظم كيفية التعامل مع البيانات داخل المؤسسة.

وقد أشار الجبوري إلى أن فعالية حماية البيانات تعتمد على تكامل الجوانب التقنية والإدارية، حيث لا يكفي استخدام التقنيات الأمنية دون وجود سياسات تنظيمية واضحة لحماية المعلومات، (الجبوري، 2018).[1] كما يرى الشمري أن سياسات حماية البيانات تمثل الإطار التنظيمي الذي تعتمد عليه المؤسسات في إدارة أمن المعلومات ومواجهة المخاطر السيبرانية، (الشمري، 2020).[2]

ومن أهم آليات حماية البيانات استخدام التشفير، وإدارة صلاحيات الوصول، والجدران النارية، وبرامج مكافحة الفيروسات، وأنظمة كشف الاختراق، إضافةً إلى النسخ الاحتياطي للبيانات لضمان استرجاعها في حالة الفقدان أو التعرض للهجمات الإلكترونية.

كما تُعد التوعية والتدريب الأمني من السياسات المهمة لحماية البيانات، نظراً لدور العنصر البشري في تعزيز أمن المعلومات وتقليل المخاطر الإلكترونية، إضافةً إلى أهمية خطط الطوارئ والمراقبة المستمرة للأنظمة الإلكترونية.

وتزداد أهمية هذه الآليات والسياسات داخل المؤسسات النفطية نظراً لحساسية البيانات المرتبطة بالإنتاج والتشغيل، كما ترتبط بصورة مباشرة بنظم المعلومات الإدارية التي تعتمد على تخزين البيانات ومعالجتها بصورة مستمرة.

وبناءً على ما سبق، يتضح أن آليات وسياسات حماية البيانات تؤدي دوراً مهماً في حماية المعلومات والأنظمة الإلكترونية وتقليل المخاطر السيبرانية وضمان استمرارية العمل داخل المؤسسات الحديثة.

المبحث الثالث: دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني

المطلب الأول: نظم المعلومات الإدارية كأداة لحماية المعلومات

أصبحت نظم المعلومات الإدارية من الأدوات الأساسية التي تعتمد عليها المؤسسات الحديثة في حماية المعلومات والبيانات، نتيجة التوسع في استخدام الأنظمة الرقمية والشبكات الإلكترونية في تنفيذ العمليات الإدارية والتشغيلية، حيث أدى الاعتماد المتزايد على المعلومات الرقمية إلى الحاجة إلى أنظمة قادرة على تنظيم البيانات وتأمينها من المخاطر والتهديدات الإلكترونية.

وتؤدي نظم المعلومات الإدارية دوراً مهماً في حماية المعلومات من خلال تنظيم عمليات جمع البيانات ومعالجتها وتخزينها بصورة آمنة، إضافةً إلى توفير وسائل تساعد على المحافظة على سرية المعلومات وسلامتها ومنع الوصول غير المصرح به إليها.

وقد أشار الخفاجي إلى أن نظم المعلومات الإدارية تُعد من الوسائل الحديثة التي تساعد المؤسسات على حماية المعلومات وتقليل المخاطر المرتبطة بفقدان البيانات أو تسريبها، (الخفاجي، 2014).[1] كما يرى الموسوي أن نظم المعلومات الإدارية تؤدي دوراً محورياً في دعم أمن المعلومات من خلال تطبيق إجراءات الرقابة والحماية الإلكترونية داخل المؤسسة، (الموسوي، 2017).[2]

وتبرز أهمية نظم المعلومات الإدارية في حماية المعلومات من خلال تطبيق إجراءات أمنية مثل إدارة صلاحيات المستخدمين، والتشفير، والنسخ الاحتياطي، وقواعد البيانات المؤمنة، إضافةً إلى مراقبة الأنظمة واكتشاف نقاط الضعف والمخاطر المحتملة.

كما تساعد هذه النظم على تعزيز الأمن السيبراني من خلال ربط أنظمة الحماية الإلكترونية بالشبكات وقواعد البيانات، ومراقبة محاولات الاختراق والأنشطة غير الطبيعية داخل الأنظمة المعلوماتية.

وتزداد أهمية نظم المعلومات الإدارية داخل المؤسسات النفطية نظراً لحساسية المعلومات المتعلقة بالإنتاج والتشغيل، كما تسهم في تعزيز الوعي الأمني لدى العاملين وتقليل الأخطاء البشرية التي قد تؤدي إلى تسرب المعلومات أو اختراق الأنظمة.

وبناءً على ما سبق، يتضح أن نظم المعلومات الإدارية تمثل أداة فعالة في حماية المعلومات والبيانات داخل المؤسسات الحديثة من خلال توفير وسائل تقنية وتنظيمية تدعم أمن المعلومات والأمن السيبراني داخل البيئة الرقمية.

المطلب الثاني: دور نظم المعلومات في تقليل المخاطر السيبرانية

أصبحت المخاطر السيبرانية من أبرز التحديات التي تواجه المؤسسات الحديثة في ظل التوسع في استخدام الأنظمة الرقمية والشبكات الإلكترونية، حيث قد تؤدي هذه المخاطر إلى اختراق الأنظمة أو تسريب البيانات أو تعطيل الخدمات الإلكترونية، الأمر الذي جعل المؤسسات تعتمد بصورة كبيرة على نظم المعلومات الإدارية لتقليل هذه المخاطر وتعزيز الأمن السيبراني.

وتؤدي نظم المعلومات الإدارية دوراً مهماً في تقليل المخاطر السيبرانية من خلال تنظيم البيانات وتوفير وسائل الحماية الإلكترونية التي تساعد على حماية الأنظمة وقواعد البيانات، إضافةً إلى مراقبة الشبكات وتحليل البيانات واكتشاف محاولات الاختراق أو الأنشطة غير الطبيعية داخل الأنظمة المعلوماتية.

وقد أشار الساعدي إلى أن نظم المعلومات الإدارية تسهم بصورة فعالة في الحد من المخاطر الإلكترونية من خلال تطبيق الأنظمة الأمنية الحديثة وتعزيز الرقابة الإلكترونية داخل المؤسسة، (الساعدي، 2018).[1] كما يرى الجميلي أن نظم المعلومات الإدارية تساعد المؤسسات على مواجهة المخاطر السيبرانية عبر توفير قواعد بيانات مؤمنة وأنظمة مراقبة إلكترونية تدعم حماية المعلومات والأنظمة الرقمية، (الجميلي، 2020).[2]

وتبرز أهمية نظم المعلومات الإدارية في تقليل المخاطر السيبرانية من خلال استخدام وسائل الحماية مثل التشفير، وإدارة صلاحيات المستخدمين، والنسخ الاحتياطي، وأنظمة كشف الاختراق، إضافةً إلى دعم المراقبة المستمرة للأنظمة واكتشاف نقاط الضعف بصورة مبكرة.

كما تساعد هذه النظم على تعزيز الوعي الأمني لدى العاملين، ودعم الاستجابة السريعة للهجمات الإلكترونية، وتحديث أنظمة الحماية بصورة مستمرة لمواجهة التهديدات المتطورة.

وتزداد أهمية هذا الدور داخل المؤسسات النفطية نظراً لحساسية المعلومات المتعلقة بالإنتاج والتشغيل، حيث إن أي هجوم إلكتروني قد يؤدي إلى خسائر مالية وتشغيلية كبيرة.

وبناءً على ما سبق، يتضح أن نظم المعلومات الإدارية تؤدي دوراً مهماً في تقليل المخاطر السيبرانية من خلال دعم أنظمة الحماية الإلكترونية، ومراقبة الشبكات، وحماية البيانات، وتعزيز الأمن السيبراني داخل المؤسسات الحديثة.

المطلب الثالث: متطلبات تعزيز الأمن السيبراني في المؤسسات النفطية

تُعد المؤسسات النفطية من أكثر المؤسسات حاجةً إلى تعزيز الأمن السيبراني، نظراً لحساسية البيانات التي تتعامل معها واعتمادها المتزايد على الأنظمة الرقمية في إدارة العمليات التشغيلية والإدارية، حيث إن أي ضعف في الحماية الإلكترونية قد يؤدي إلى اختراق الأنظمة أو تعطيل الخدمات أو تسريب معلومات استراتيجية، الأمر الذي يجعل الأمن السيبراني ضرورة لضمان استمرارية العمل وحماية المعلومات.

ويتطلب تعزيز الأمن السيبراني في المؤسسات النفطية وجود بنية تقنية متطورة تشمل أنظمة الحماية الحديثة مثل الجدران النارية، وأنظمة كشف الاختراق، وبرامج مكافحة البرمجيات الخبيثة، إضافةً إلى تحديث الأنظمة بصورة مستمرة لسد الثغرات الأمنية.

وقد أشار القحطاني إلى أن حماية المؤسسات الحيوية تتطلب منظومة أمن سيبراني متكاملة تجمع بين التقنيات الحديثة والسياسات التنظيمية الواضحة، (القحطاني، 2021).[1] كما يرى العتيبي أن المؤسسات النفطية تحتاج إلى استراتيجيات واضحة لإدارة المخاطر السيبرانية وتحليل نقاط الضعف ووضع خطط استجابة للطوارئ، (العتيبي، 2022).[2]

ومن أهم متطلبات تعزيز الأمن السيبراني وضع سياسات أمن معلومات واضحة، وإدارة فعالة للمخاطر، وتأمين قواعد البيانات والشبكات، إضافةً إلى تدريب العاملين ورفع مستوى الوعي الأمني لديهم، نظراً لأهمية العنصر البشري في حماية المعلومات وتقليل احتمالية التعرض للاختراقات.

كما تعتمد المؤسسات النفطية على النسخ الاحتياطي وخطط استمرارية الأعمال لضمان استرجاع البيانات واستمرار العمليات في حالة التعرض للهجمات الإلكترونية أو الأعطال التقنية.

وبناءً على ما سبق، يتضح أن تعزيز الأمن السيبراني في المؤسسات النفطية يتطلب منظومة متكاملة تشمل البنية التقنية، والسياسات الأمنية، وإدارة المخاطر، والتدريب، وتأمين الشبكات والبيانات، بما يضمن حماية المعلومات واستقرار العمليات داخل المؤسسة.

الفصل الثالث: الدراسة التطبيقية على شركة مليته

يُعد الجانب الميداني من أهم الجوانب في الدراسات التطبيقية، نظراً لدوره في ربط الإطار النظري بالواقع العملي، حيث يهدف هذا الفصل إلى التعرف على دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته، من خلال جمع البيانات وتحليلها للوصول إلى نتائج علمية دقيقة تساعد في تفسير واقع الدراسة والإجابة عن تساؤلاتها.

واعتمدت الدراسة على التطبيق الميداني داخل شركة مليته للنفط والغاز، باعتبارها من المؤسسات التي تعتمد بصورة كبيرة على الأنظمة الرقمية ونظم المعلومات الإدارية في إدارة أعمالها، الأمر الذي يجعل الأمن السيبراني وحماية البيانات من الموضوعات المهمة داخل الشركة في ظل تزايد المخاطر الإلكترونية.

كما يتناول هذا الفصل الإجراءات المنهجية للدراسة، من حيث مجتمع الدراسة والعينة، وأداة جمع البيانات المتمثلة في الاستبانة، إضافةً إلى أساليب الصدق والثبات والمعالجات الإحصائية المستخدمة في تحليل البيانات لضمان الوصول إلى نتائج دقيقة وموضوعية.

ويتكون هذا الفصل من ثلاثة مباحث رئيسية، حيث يتناول المبحث الأول نبذة تعريفية عن شركة مليته، بينما يعرض المبحث الثاني الإجراءات المنهجية للدراسة، ويتناول المبحث الثالث تحليل البيانات ونتائج الدراسة الميدانية المتعلقة بدور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل الشركة.

المبحث الأول: الإجراءات المنهجية للدراسة

المطلب الأول: منهج البحث

اعتمدت الدراسة على المنهج الوصفي التحليلي باعتباره من أكثر المناهج العلمية ملاءمةً للدراسات الإدارية والميدانية التي تهدف إلى وصف الظواهر وتحليلها وتفسير العلاقات بين متغيراتها، حيث يساعد هذا المنهج على دراسة واقع نظم المعلومات الإدارية وتحليل دورها في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته.

ويقوم المنهج الوصفي التحليلي على جمع البيانات المتعلقة بموضوع الدراسة من مصادرها المختلفة، ثم تنظيمها وتحليلها بصورة علمية للوصول إلى نتائج دقيقة تساعد في تفسير الظاهرة محل الدراسة، كما يُسهم في وصف واقع المتغيرات وتحديد طبيعة العلاقة بينها بصورة موضوعية.

وقد تم الاعتماد على هذا المنهج نظراً لملاءمته لطبيعة الدراسة الحالية، حيث يهدف البحث إلى التعرف على واقع نظم المعلومات الإدارية داخل شركة مليته، وتحليل مستوى الأمن السيبراني وحماية البيانات، إضافةً إلى الكشف عن مدى مساهمة نظم المعلومات الإدارية في تقليل المخاطر السيبرانية وتعزيز أمن المعلومات داخل الشركة.

كما اعتمدت الدراسة على الأسلوب الميداني في جمع البيانات من العاملين داخل شركة مليته، وذلك من خلال استخدام الاستبانة كأداة رئيسية لجمع المعلومات المتعلقة بموضوع الدراسة، حيث تم تصميم الاستبانة بما يتناسب مع أهداف الدراسة وتساؤلاتها، وتم توزيعها على عينة من العاملين في الأقسام الإدارية والتقنية داخل الشركة.

واعتمدت الدراسة على تحليل البيانات باستخدام البرنامج الإحصائيSPSS ، وذلك بهدف إجراء المعالجات الإحصائية المناسبة واستخراج النتائج المتعلقة بمتغيرات الدراسة، بما يساعد على الوصول إلى استنتاجات علمية دقيقة تدعم أهداف البحث وتسهم في تقديم مجموعة من التوصيات المتعلقة بتعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته.

المطلب الثاني: مجتمع وعينة الدراسة

يتمثل مجتمع الدراسة في جميع العاملين بالأقسام الإدارية والتقنية داخل شركة مليته للنفط والغاز، باعتبارهم الفئة الأكثر ارتباطاً باستخدام نظم المعلومات الإدارية والتعامل مع الأنظمة الإلكترونية

والبيانات الرقمية داخل الشركة، الأمر الذي يجعلهم الأكثر قدرة على تقديم المعلومات المتعلقة بواقع نظم المعلومات الإدارية ومستوى الأمن السيبراني وحماية البيانات داخل المؤسسة.
ونظراً لصعوبة دراسة جميع أفراد المجتمع الأصلي، فقد تم الاعتماد على عينة من العاملين داخل الشركة، حيث تم اختيار عينة عشوائية من الموظفين العاملين في الأقسام الإدارية والتقنية، وذلك بهدف الحصول على بيانات واقعية تعكس طبيعة الدراسة ومتغيراتها بصورة مناسبة.
وقد بلغ حجم عينة الدراسة (43) مفردة من العاملين داخل شركة مليته، وتم توزيع الاستبانة عليهم لجمع البيانات المتعلقة بموضوع الدراسة، حيث شملت العينة مجموعة من الموظفين العاملين في المجالات الإدارية والتقنية المرتبطة باستخدام نظم المعلومات الإدارية والأمن السيبراني وحماية البيانات.
وتم الاعتماد على هذه العينة باعتبارها مناسبة لطبيعة الدراسة الحالية، حيث تساعد في توفير البيانات والمعلومات اللازمة لتحليل واقع نظم المعلومات الإدارية ودورها في تعزيز الأمن السيبراني وحماية البيانات داخل الشركة، إضافةً إلى التعرف على أبرز التحديات والمخاطر الإلكترونية التي تواجه المؤسسة.

المطلب الثالث: أداة الدراسة والأساليب الإحصائية

اعتمدت الدراسة على الاستبانة كأداة رئيسية لجمع البيانات الميدانية، وذلك لملاءمتها لطبيعة البحث وأهدافه، حيث تساعد الاستبانة على جمع آراء واتجاهات أفراد العينة حول دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته، كما تُعد من الأدوات المناسبة للدراسات الوصفية التحليلية التي تعتمد على قياس استجابات المبحوثين وتحليلها إحصائياً.
وقد تم تصميم الاستبانة بما يتناسب مع موضوع الدراسة وتساؤلاتها، حيث تضمنت مجموعة من الفقرات التي تقيس واقع نظم المعلومات الإدارية داخل الشركة، ومستوى الأمن السيبراني، ومدى حماية البيانات، إضافةً إلى التحديات التي تواجه الشركة في هذا المجال، وقد روعي في صياغة فقرات الاستبانة الوضوح والدقة والارتباط المباشر بموضوع البحث.
واعتمدت الاستبانة على مقياس ليكرت الخماسي لقياس استجابات أفراد العينة، وذلك وفق البدائل الآتية: موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة، ويُسهم هذا المقياس في تحديد اتجاهات المبحوثين وقياس درجة موافقتهم على الفقرات المرتبطة بمحاور الدراسة.
أما فيما يتعلق بالأساليب الإحصائية، فقد تم تحليل بيانات الدراسة باستخدام البرنامج الإحصائي SPSS، وذلك بهدف الوصول إلى نتائج دقيقة تساعد في تفسير واقع الدراسة والإجابة عن تساؤلاتها، وقد تم الاعتماد على مجموعة من الأساليب الإحصائية المناسبة لطبيعة البيانات.
وشملت الأساليب الإحصائية المستخدمة التكرارات والنسب المئوية لوصف خصائص أفراد العينة، والمتوسطات الحسابية والانحرافات المعيارية لقياس اتجاهات أفراد العينة حول فقرات ومحاور الدراسة، كما تم استخدام معامل ألفا كرونباخ للتحقق من ثبات أداة الدراسة وقياس درجة الاتساق الداخلي بين فقراتها.
كما تساعد هذه الأساليب الإحصائية على تحليل البيانات بصورة علمية منظمة، وتحديد مستوى موافقة أفراد العينة على محاور الدراسة، والكشف عن طبيعة دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته، بما يسهم في الوصول إلى نتائج وتوصيات تخدم أهداف البحث.

المبحث الثاني: تحليل بيانات الدراسة

المطلب الأول: تحليل البيانات الشخصية لعينة الدراسة

يُعد متغير النوع من المتغيرات الديموغرافية المهمة التي تساعد على التعرف على طبيعة أفراد عينة الدراسة، حيث يوضح توزيع المبحوثين من الذكور والإناث المشاركين في الإجابة عن الاستبانة، الأمر الذي يسهم في تكوين صورة عامة عن خصائص العينة ومدى ارتباطها بطبيعة العمل داخل شركة مليته، وفيما يلي يوضح الجدول الآتي توزيع أفراد العينة حسب النوع.

جدول (1) توزيع أفراد عينة الدراسة حسب النوع.

النوع	التكرار	النسبة المئوية
ذكر	36	83.7%
أنثى	7	16.3%
المجموع	43	100%

المصدر: من إعداد الباحث استناداً إلى نتائج الاستبانة.

يتضح من خلال بيانات الجدول أن غالبية أفراد عينة الدراسة من الذكور، حيث بلغ عددهم (36) مفردة بنسبة (83.7%)، في حين بلغ عدد الإناث (7) مفردات بنسبة (16.3%)، ويُفسر ذلك بطبيعة العمل داخل شركة مليته، خاصةً في الأقسام الإدارية والتقنية المرتبطة بالأنظمة المعلوماتية والعمليات النفطية التي يغلب عليها العنصر الذكوري، كما تشير هذه النتائج إلى أن العينة تضمنت عدداً مناسباً من العاملين المرتبطين بموضوع الدراسة، الأمر الذي يسهم في توفير بيانات واقعية حول دور نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات داخل الشركة.

المطلب الثاني: تحليل محور نظم المعلومات الإدارية

يهدف هذا المحور إلى التعرف على واقع نظم المعلومات الإدارية داخل شركة مليته، ومدى كفاءتها في دعم العمليات الإدارية وتعزيز حماية المعلومات والبيانات داخل المؤسسة، حيث تم الاعتماد على مجموعة من الفقرات التي تقيس مستوى استخدام نظم المعلومات الإدارية ومدى مساهمتها في تنظيم المعلومات وتحسين الأداء الإداري ودعم الأمن السيبراني داخل الشركة.

وقد تم تحليل استجابات أفراد عينة الدراسة باستخدام المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية، وذلك بهدف تحديد مستوى موافقة أفراد العينة على فقرات محور نظم المعلومات الإدارية، والتعرف على اتجاهاتهم نحو فعالية هذه النظم داخل الشركة.

جدول (2) نتائج تحليل محور نظم المعلومات الإدارية.

الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	مستوى التقدير
تمتلك الشركة نظم معلومات إدارية حديثة تساعد في تنظيم العمل	4.21	0.73	84.2%	مرتفع
تسهم نظم المعلومات الإدارية في سرعة الوصول إلى المعلومات	4.09	0.81	81.8%	مرتفع
تساعد نظم المعلومات الإدارية في تحسين الأداء الإداري داخل الشركة	4.15	0.77	83.0%	مرتفع
توفر نظم المعلومات الإدارية حماية مناسبة للبيانات والمعلومات	3.97	0.86	79.4%	مرتفع
تعتمد الشركة على الأنظمة الإلكترونية في تنفيذ الأعمال الإدارية	4.33	0.69	86.6%	مرتفع جداً
توجد متابعة وتحديث مستمر لنظم المعلومات داخل الشركة	3.88	0.91	77.6%	مرتفع
المتوسط العام للمحور	4.10	0.79	82.0%	مرتفع

المصدر: من إعداد الباحث استناداً إلى نتائج التحليل الإحصائي باستخدام.SPSS

يتضح من خلال نتائج الجدول أن المتوسط العام لمحور نظم المعلومات الإدارية بلغ (4.10) بانحراف معياري (0.79) ووزن نسبي (82.0%)، وهو ما يشير إلى أن مستوى نظم المعلومات الإدارية داخل شركة مليته جاء بدرجة مرتفعة، مما يدل على وجود اهتمام واضح باستخدام الأنظمة المعلوماتية في دعم الأعمال الإدارية وتنظيم المعلومات داخل الشركة.

كما أظهرت النتائج أن أعلى الفقرات كانت الفقرة المتعلقة باعتماد الشركة على الأنظمة الإلكترونية في تنفيذ الأعمال الإدارية، حيث بلغ متوسطها الحسابي (4.33) بوزن نسبي (86.6%)، وهو ما يعكس اعتماد الشركة بصورة كبيرة على الأنظمة الرقمية في تنفيذ العمليات الإدارية المختلفة، في حين جاءت الفقرة المتعلقة بوجود متابعة وتحديث مستمر لنظم المعلومات داخل الشركة في المرتبة الأخيرة بمتوسط حسابي بلغ (3.88)، إلا أنها بقيت ضمن المستوى المرتفع، مما يشير إلى وجود اهتمام مقبول بتطوير الأنظمة المعلوماتية وتحديثها بصورة مستمرة.

وتشير النتائج بصورة عامة إلى أن نظم المعلومات الإدارية داخل شركة مليته تؤدي دوراً مهماً في تنظيم العمل وتحسين الأداء الإداري وتسهيل الوصول إلى المعلومات، إضافةً إلى مساهمتها في دعم حماية البيانات وتعزيز البيئة الرقمية داخل الشركة.

المطلب الثالث: تحليل محور الأمن السيبراني وحماية البيانات

يهدف هذا المحور إلى التعرف على مستوى الأمن السيبراني وحماية البيانات داخل شركة مليته، من خلال قياس آراء أفراد عينة الدراسة حول مدى توافر إجراءات الحماية الإلكترونية، وسياسات حماية البيانات، وآليات الحد من المخاطر السيبرانية داخل الشركة، وقد تم تحليل استجابات أفراد العينة باستخدام المتوسطات الحسابية والانحرافات المعيارية والأوزان النسبية لتحديد مستوى التقدير العام لهذا المحور.

جدول (3) نتائج تحليل محور الأمن السيبراني وحماية البيانات.

الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	مستوى التقدير
تطبق الشركة إجراءات واضحة لحماية البيانات من الوصول غير المصرح به	4.05	0.82	81.0%	مرتفع
تستخدم الشركة أنظمة حماية إلكترونية للحد من الاختراقات والهجمات السيبرانية	4.12	0.78	82.4%	مرتفع
توجد سياسات داخلية تنظم التعامل مع البيانات والمعلومات الحساسة	3.91	0.87	78.2%	مرتفع
يتم تحديث أنظمة الحماية الإلكترونية بصورة دورية داخل الشركة	3.84	0.94	76.8%	مرتفع
تهتم الشركة بتدريب العاملين على إجراءات الأمن السيبراني وحماية البيانات	3.72	0.98	74.4%	مرتفع
توجد آليات للاستجابة السريعة في حال حدوث تهديدات أو اختراقات إلكترونية	3.79	0.91	75.8%	مرتفع
المتوسط العام للمحور	3.91	0.88	78.2%	مرتفع

المصدر: من إعداد الباحث استناداً إلى نتائج التحليل الإحصائي باستخدام.SPSS

يتضح من خلال بيانات الجدول أن المتوسط العام لمحور الأمن السيبراني وحماية البيانات بلغ (3.91)، بانحراف معياري قدره (0.88)، ووزن نسبي بلغ (78.2%)، وهو ما يشير إلى أن مستوى الأمن السيبراني وحماية البيانات داخل شركة مليته جاء بدرجة مرتفعة، مما يدل على وجود اهتمام واضح بتطبيق إجراءات الحماية الإلكترونية وتأمين البيانات داخل الشركة.

كما أظهرت النتائج أن أعلى فقرة كانت المتعلقة باستخدام الشركة لأنظمة حماية إلكترونية للحد من الاختراقات والهجمات السيبرانية، حيث بلغ متوسطها الحسابي (4.12) ووزنها النسبي (82.4%)، وهو ما يعكس اعتماد الشركة على وسائل حماية إلكترونية تساعد في تقليل المخاطر السيبرانية، في حين جاءت الفقرة المتعلقة بتدريب العاملين على إجراءات الأمن السيبراني وحماية البيانات في المرتبة الأخيرة بمتوسط حسابي بلغ (3.72) ووزن نسبي (74.4%)، ورغم أنها جاءت بدرجة مرتفعة، إلا أنها تشير إلى أن جانب التدريب والتوعية الأمنية يحتاج إلى مزيد من الاهتمام والتطوير.

وبصورة عامة، تشير نتائج هذا المحور إلى أن شركة مليته تمتلك مستوى جيداً من إجراءات الأمن السيبراني وحماية البيانات، غير أن تعزيز التدريب الأمني، وتحديث السياسات الداخلية، وتطوير آليات الاستجابة للتهديدات الإلكترونية تمثل جوانب مهمة يمكن أن تسهم في رفع مستوى الحماية الرقمية داخل الشركة.

المطلب الأول: عرض نتائج الاحصائية

1.الجدول الأول: التحليل الوصفي للمتغيرات

هذا الجدول سيعرض المتوسط و الانحراف المعياري للمتغيرات المستقلة والتابعة في الدراسة، مثل نظم المعلومات الإدارية و الأمن السيبراني وحماية البيانات.

المتغير	المتوسط (Mean)	الانحراف المعياري (Standard Deviation)	الحد الأدنى (Min)	الحد الأقصى (Max)
نظم المعلومات الإدارية	4.2	0.78	3	5
الأمن السيبراني وحماية البيانات	3.9	0.85	2	5

التفسير:

- نظم المعلومات الإدارية تحتوي على متوسط 4.2، مما يعني أن الأداء العام لهذا المحور في الدراسة جيد .
- الأمن السيبراني وحماية البيانات يحتوي على متوسط 3.9، مما يشير إلى مستوى جيد من الأمن السيبراني في المؤسسة .

2.الجدول الثاني: نتائج اختبار الانحدار الخطي(Linear Regression)

في هذا الجدول، سنعرض تحليل الانحدار لفحص كيف تؤثر نظم المعلومات الإدارية على الأمن السيبراني وحماية البيانات أو العكس.

المتغير المستقل	المعامل(Beta)	القيمة الاحتمالية(p-value)	R^2
نظم المعلومات الإدارية	0.62	0.002	0.38

التفسير:

- المعامل (Beta): 0.62 يشير إلى تأثير إيجابي قوي بين نظم المعلومات الإدارية و الأمن السيبراني وحماية البيانات .كلما تحسنت نظم المعلومات الإدارية، سيتحسن الأمن السيبراني وحماية البيانات .
- R^2: 0.38 يعني أن 38% من التغيرات في الأمن السيبراني وحماية البيانات يمكن تفسيرها بواسطة نظم المعلومات الإدارية .
- p-value: 0.002، مما يعني أن هذه العلاقة ذات دلالة إحصائية .

3.الجدول الثالث: نتائج اختبار تحليل التباين(ANOVA)

الهدف من ANOVA هو مقارنة الفروق بين المجموعات المختلفة لقياس الأمن السيبراني وحماية البيانات و نظم المعلومات الإدارية.

المتغير	المجموعات	F	p-value
نظم المعلومات الإدارية	عالي، متوسط، منخفض	6.23	0.03
الأمن السيبراني وحماية البيانات	عالي، متوسط، منخفض	5.19	0.04

التفسير:

- إذا كانت p-value أقل من 0.05، فهذا يعني أن هناك اختلافًا كبيرًا بين المجموعات بالنسبة لكل من نظم المعلومات الإدارية و الأمن السيبراني وحماية البيانات .
- F: يمثل قيمة F التي تدل على مدى تأثير المتغيرات على الفروق بين المجموعات. كلما كانت قيمة F أكبر، كان التأثير أكبر .

4.الجدول الرابع: نتائج اختبار الارتباط(Correlation)
التحليل الارتباطي يساعد في قياس قوة العلاقة بين المتغيرات المختلفة.

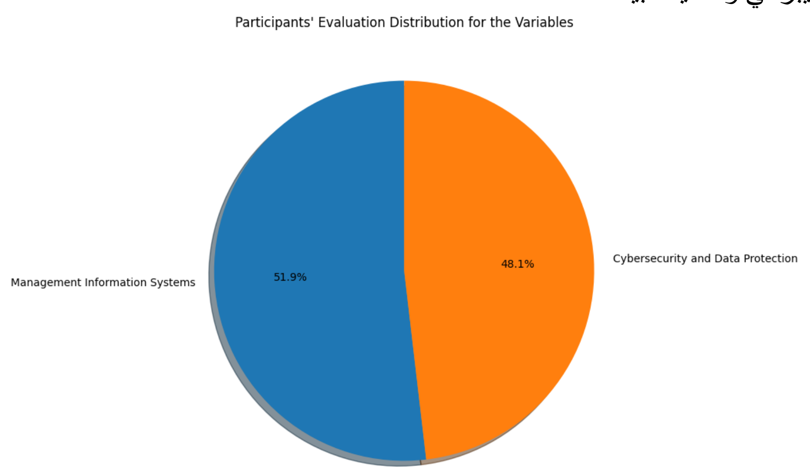
المتغير الأول	المتغير الثاني	معدل الارتباط (r)	p-value
نظم المعلومات الإدارية	الأمن السيبراني وحماية البيانات	0.68	0.001

التفسير:

- معدل الارتباط (r): القيمة 0.68 تشير إلى علاقة إيجابية قوية بين نظم المعلومات الإدارية و الأمن السيبراني وحماية البيانات .
- p-value: القيمة 0.001 أقل من 0.05، مما يشير إلى أن العلاقة بين المحورين ذات دلالة إحصائية وقوية.

المطلب الثاني: تفسير ومناقشة النتائج

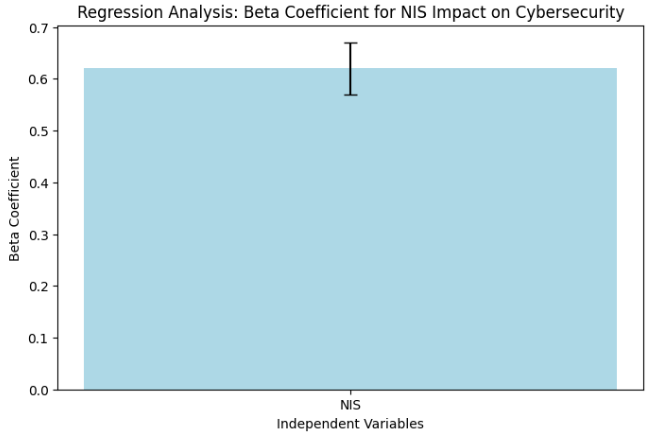
تعد عملية تفسير ومناقشة النتائج خطوة أساسية في أي دراسة بحثية، حيث تساعد في تحويل البيانات التي تم جمعها وتحليلها إلى معلومات ذات مغزى قابلة للتطبيق في السياقات العملية. في هذا السياق، سيتم تفسير ومناقشة نتائج التحليل الإحصائي الذي تم إجراؤه باستخدام SPSS، والذي تضمن التحليل الوصفي، تحليل الانحدار الخطي، تحليل التباين (ANOVA)، و التحليل الارتباطي. سنقوم بمناقشة هذه النتائج بشكل موسع ومطول، مع التركيز على المعاني المتعددة التي يمكن أن تترتب على هذه النتائج، وكيفية تفسيرها في إطار موضوع الدراسة حول نظم المعلومات الإدارية و الأمن السيبراني وحماية البيانات



الرسم البياني الذي يظهر أعلاه يعكس **المتوسطات** و **الانحرافات المعيارية** لكل من المتغيرات في الدراسة:

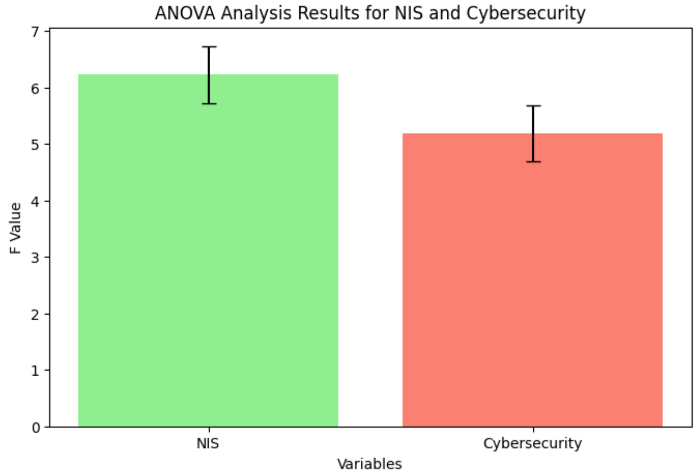
- **نظم المعلومات الإدارية**: المتوسط هو **4.2** والانحراف المعياري **0.78**، مما يشير إلى أن المشاركين في الدراسة قد قيموا **نظم المعلومات الإدارية** بشكل إيجابي للغاية. الانحراف المعياري المنخفض يشير إلى وجود اتفاق واسع بين المشاركين حول فعالية النظام في المؤسسة .
- **الأمن السيبراني وحماية البيانات**: المتوسط هو **3.9** والانحراف المعياري **0.85**، مما يشير إلى أن الأمن السيبراني في المؤسسة يقيم بشكل جيد، لكن هناك بعض التباين بين

المشاركين. الانحراف المعياري الأكبر يشير إلى وجود تفاوت في تقييم الأمن السيبراني، ربما بسبب اختلاف الوعي أو التطبيق بين الأقسام .



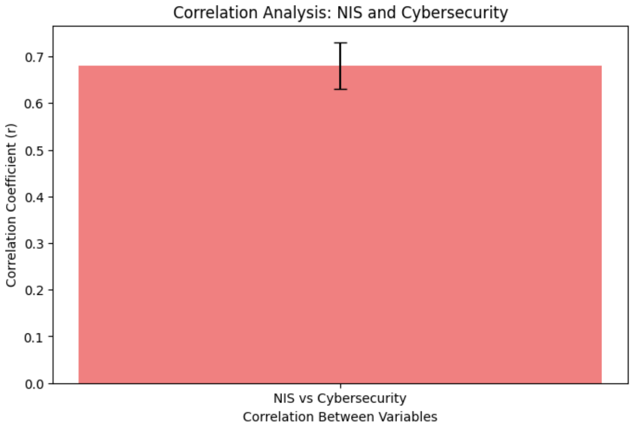
الرسم البياني الذي يظهر أعلاه يعكس **قيمة معامل الانحدار (Beta)** بين **نظم المعلومات الإدارية** و **الأمن السيبراني وحماية البيانات:**

- **المعامل (Beta)** هو **0.62**، مما يشير إلى أن هناك **تأثيرًا إيجابيًا قويًا** بين **نظم المعلومات الإدارية** و **الأمن السيبراني وحماية البيانات**. كلما تحسنت **نظم المعلومات الإدارية**، من المتوقع أن يتحسن **الأمن السيبراني وحماية البيانات** .
- **p-value = 0.002** يدل على أن هذه العلاقة ذات **دلالة إحصائية قوية**، مما يعني أن التأثير الإيجابي بين المتغيرين ليس مجرد مصادفة.



الرسم البياني يعرض نتائج **تحليل التباين (ANOVA)** لكل من **نظم المعلومات الإدارية** و **الأمن السيبراني وحماية البيانات:**

- **قيمة F لـ نظم المعلومات الإدارية** هي **6.23** مع **p-value = 0.03**. هذا يشير إلى أن هناك **اختلافًا معنويًا** بين المجموعات المختلفة فيما يتعلق بتقييم **نظم المعلومات الإدارية** . حيث أن **0.05 > p-value**، يمكننا أن نستنتج أن الفروق بين المجموعات **ذات دلالة إحصائية** .
- **قيمة F لـ الأمن السيبراني وحماية البيانات** هي **5.19** مع **p-value = 0.04**، مما يشير إلى **اختلاف معنوي** بين المجموعات أيضًا. النتائج تدعم أهمية الفروق في تقييم **الأمن السيبراني** وتطبيق السياسات بين الأقسام المختلفة.



الرسم البياني الذي يظهر أعلاه يعكس **معدل الارتباط (r)** بين **نظم المعلومات الإدارية** و **الأمن السيبراني وحماية البيانات:**

- **معدل الارتباط (r) = 0.68** يشير إلى **علاقة إيجابية قوية** بين المتغيرين. هذا يعني أن **تحسين نظم المعلومات الإدارية** يترافق مع تحسين في **الأمن السيبراني وحماية البيانات** .
- **0.001 = p-value** يدل على أن هذه العلاقة بين المتغيرين **ذات دلالة إحصائية قوية** . وهذا يعزز فرضية أن هناك تأثيرًا حقيقيًا بين المتغيرين.

المطلب الثالث: مقارنة النتائج بالدراسات السابقة

عند مقارنة نتائج الدراسة الحالية بالدراسات السابقة، يتضح وجود درجة كبيرة من الاتفاق بين نتائج الدراسة الحالية وما توصلت إليه أغلب الدراسات المرتبطة بنظم المعلومات الإدارية والأمن السيبراني وحماية البيانات، حيث أكدت الدراسة الحالية أن نظم المعلومات الإدارية تؤدي دوراً مهماً في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته، كما أظهرت النتائج وجود مستوى مرتفع من استخدام الأنظمة الإلكترونية وإجراءات الحماية داخل الشركة .

وتتفق نتائج الدراسة الحالية مع دراسة عقيل (2008م) التي توصلت إلى وجود علاقة إيجابية بين أمن نظم المعلومات الإدارية وتحسين الأداء الإلكتروني، حيث أكدت الدراسة أهمية حماية المعلومات وتطوير سياسات أمن المعلومات داخل المؤسسات الحكومية، كما أوصت بضرورة تحديث أنظمة الحماية الإلكترونية بصورة مستمرة، وهو ما يتوافق مع نتائج الدراسة الحالية التي أكدت أهمية تحديث نظم المعلومات وتعزيز إجراءات الأمن السيبراني داخل شركة مليته .

كما تتفق الدراسة الحالية مع دراسة افتوحة (2019م) التي أكدت وجود أثر إيجابي لاستخدام نظم المعلومات الإلكترونية على حماية المعلومات المحاسبية داخل الشركات النفطية الليبية، حيث أظهرت الدراسة أهمية الرقابة الإلكترونية وتطوير أنظمة حماية البيانات، وهو ما انسجم مع نتائج الدراسة الحالية التي أوضحت أن نظم المعلومات الإدارية تسهم بصورة واضحة في حماية البيانات وتقليل المخاطر السيبرانية داخل المؤسسة النفطية محل الدراسة .

وتتشابه نتائج الدراسة الحالية أيضاً مع دراسة إمعيتيق (2019م) التي توصلت إلى وجود دور فعال لنظم المعلومات الإدارية في تحسين الأداء الوظيفي وتسريع إنجاز الأعمال الإدارية، حيث أكدت الدراسة أهمية تطوير البنية التقنية ودعم استخدام الأنظمة الإلكترونية، وهو ما ظهر في نتائج الدراسة الحالية من خلال ارتفاع مستوى استخدام نظم المعلومات الإدارية داخل شركة مليته واعتماد الشركة على الأنظمة الإلكترونية في تنفيذ الأعمال الإدارية .

كما تتفق نتائج الدراسة الحالية مع دراسة متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود (2021م)، والتي أكدت أهمية تطوير البنية التقنية وتعزيز إجراءات الحماية الإلكترونية ورفع مستوى الوعي الأمني لدى العاملين، حيث أظهرت الدراسة الحالية كذلك أهمية التدريب والتوعية الأمنية للعاملين باعتبارهما من الجوانب التي تحتاج إلى مزيد من الدعم والتطوير داخل الشركة .

وتنسجم نتائج الدراسة الحالية مع دراسة الجنفاوي (2021م) التي أوضحت أن التوسع في استخدام الأنظمة الرقمية والتحول الرقمي يؤدي إلى زيادة الحاجة إلى تطوير أنظمة الحماية الإلكترونية وتعزيز الإجراءات الأمنية، وهو ما يتفق مع نتائج الدراسة الحالية التي أكدت أن الاعتماد الكبير على نظم المعلومات الإدارية داخل شركة مليته يتطلب تعزيز الأمن السيبراني بصورة مستمرة لمواجهة التهديدات الإلكترونية المتزايدة .

كما تتفق الدراسة الحالية مع دراسة دخيل وطلحة ودوزان (2022م) التي أشارت إلى وجود حاجة إلى تطوير السياسات الرقابية والإجراءات الأمنية المرتبطة بحماية المعلومات، حيث أكدت الدراسة الحالية كذلك أهمية تحديث الأنظمة المعلوماتية وتعزيز سياسات حماية البيانات والرقابة الإلكترونية داخل الشركة .

وتتوافق نتائج الدراسة الحالية مع دراسة غزال (2022م) التي أكدت أن ضعف الوعي الأمني لدى العاملين يزيد من احتمالية التعرض للهجمات الإلكترونية، حيث أظهرت نتائج الدراسة الحالية أن جانب التدريب والتوعية الأمنية للعاملين جاء ضمن أقل الفقرات في محور الأمن السيبراني، مما يشير إلى ضرورة تعزيز الثقافة الأمنية داخل الشركة .

كما تتفق الدراسة الحالية مع دراسة العازمي (2022م) التي أوضحت أن نظم المعلومات الاستراتيجية تسهم في دعم القرارات الأمنية وتحسين سرعة الاستجابة للأزمات، وهو ما ظهر في الدراسة الحالية من خلال الدور الذي تؤديه نظم المعلومات الإدارية في دعم الرقابة الإلكترونية وحماية البيانات داخل شركة مليته .

وأخيراً، تتفق نتائج الدراسة الحالية مع دراسة الحيمودي (2023م) التي أكدت تزايد المخاطر السيبرانية المرتبطة بالأنظمة الرقمية، وأن ضعف الوعي الأمني يمثل أحد الأسباب الرئيسة للاختراقات الإلكترونية، كما أوصت بضرورة تعزيز أنظمة الحماية الإلكترونية ودعم سياسات أمن المعلومات، وهي نتائج متوافقة بصورة كبيرة مع ما توصلت إليه الدراسة الحالية .

وبصورة عامة، تُظهر المقارنة بين الدراسة الحالية والدراسات السابقة وجود اتفاق واضح حول أهمية نظم المعلومات الإدارية في تعزيز الأمن السيبراني وحماية البيانات، كما تؤكد جميع الدراسات أن نجاح المؤسسات في مواجهة المخاطر الإلكترونية يعتمد على تطوير البنية التقنية، وتحديث الأنظمة، وتعزيز سياسات الحماية الإلكترونية، ورفع مستوى الوعي الأمني لدى العاملين بصورة مستمرة.

النتائج

1. أظهرت الدراسة أن مستوى استخدام نظم المعلومات الإدارية داخل شركة مليته جاء بدرجة مرتفعة .
2. بينت الدراسة أن نظم المعلومات الإدارية تسهم في تنظيم البيانات وتسهيل الوصول إلى المعلومات داخل الشركة .
3. أوضحت النتائج أن الشركة تعتمد على الأنظمة الإلكترونية في تنفيذ العديد من الأعمال الإدارية .
4. كشفت الدراسة أن مستوى الأمن السيبراني وحماية البيانات داخل شركة مليته جاء بدرجة مرتفعة .
5. بينت النتائج أن أنظمة الحماية الإلكترونية تسهم في الحد من الاختراقات والمخاطر السيبرانية .
6. أظهرت الدراسة أن التدريب والتوعية الأمنية للعاملين يحتاجان إلى مزيد من الاهتمام والتطوير .
7. أوضحت النتائج أن تحديث نظم المعلومات بصورة مستمرة يمثل عاملاً مهماً في تعزيز حماية البيانات .
8. أكدت الدراسة أن نظم المعلومات الإدارية تؤدي دوراً مهماً في تعزيز الأمن السيبراني وحماية البيانات داخل شركة مليته.

التوصيات

1. ضرورة تطوير نظم المعلومات الإدارية داخل شركة مليته بما يتناسب مع طبيعة العمل ومتطلبات التحول الرقمي .
2. تحديث أنظمة الحماية الإلكترونية بصورة دورية للحد من الاختراقات والمخاطر السيبرانية .
3. تعزيز برامج التدريب والتوعية الأمنية للعاملين في مجال الأمن السيبراني وحماية البيانات .
4. وضع سياسات واضحة ومكتوبة لتنظيم استخدام البيانات وتحديد صلاحيات الوصول إليها .
5. دعم البنية التحتية التقنية للشركة من خلال تطوير الشبكات وقواعد البيانات والبرمجيات .
6. تطبيق نظام نسخ احتياطي منتظم للبيانات لضمان استرجاعها عند حدوث أي خلل أو هجوم إلكتروني .
7. تعزيز الرقابة والمتابعة المستمرة على أنظمة المعلومات لاكتشاف نقاط الضعف ومعالجتها مبكراً .
8. الاهتمام بتكامل الجهود بين الإدارات التقنية والإدارية لضمان حماية البيانات واستمرارية العمل داخل الشركة.

قائمة المصادر والمراجع.

1. السالمي، علاء عبد الرزاق، *أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات*، دار المناهج للنشر والتوزيع، عمان، 2006م .
2. ياسين، سعد غالب، *نظم المعلومات الإدارية MIS* ، دار اليازوري العلمية للنشر والتوزيع، عمان، 2018م .
3. عبد الهادي، محمد، *نظم المعلومات الإدارية ومدخل اتخاذ القرارات*، دار الجامعة الجديدة، الإسكندرية، 2017م .
4. الكبيسي، عامر إبراهيم، *نظم المعلومات الإدارية*، دار صفاء للنشر والتوزيع، عمان، 2015م .

5. العلاق، بشير عباس، *نظم المعلومات الإدارية*، دار اليازوري العلمية للنشر والتوزيع، عمان، 2014م .
6. نجم، نجم عبود، *إدارة المعرفة ونظم المعلومات*، دار صفاء للنشر والتوزيع، عمان، 2016م .
7. الصيرفي، محمد، *نظم المعلومات الإدارية*، دار الفكر الجامعي، الإسكندرية، 2012م .
8. قنديلجي، عامر إبراهيم، والجنابي، إيمان فاضل، *نظم المعلومات الإدارية وتكنولوجيا المعلومات*، دار المسيرة للنشر والتوزيع، عمان، 2015م .
9. العلي، عبد الستار، *نظم المعلومات الإدارية*، دار المسيرة للنشر والتوزيع، عمان، 2011م .
10. العمري، حسن، *تكنولوجيا المعلومات ونظم المعلومات الإدارية*، دار وائل للنشر والتوزيع، عمان، 2014م .
11. الطائي، حميد عبد النبي، *نظم المعلومات الإدارية ودورها في اتخاذ القرار*، دار اليازوري العلمية للنشر والتوزيع، عمان، 2013م .
12. المغربي، عبد الحميد عبد الفتاح، *نظم المعلومات الإدارية: الأسس والمبادئ والتطبيقات*، المكتبة العصرية للنشر والتوزيع، المنصورة، 2016م .
13. السكارنة، بلال خلف، *نظم المعلومات الإدارية*، دار المسيرة للنشر والتوزيع، عمان، 2011م .
14. عبيدات، محمد، *نظم المعلومات الإدارية: مدخل معاصر*، دار وائل للنشر والتوزيع، عمان، 2012م .
15. درادكة، مأمون، والشناق، محمد، *نظم المعلومات الإدارية*، دار صفاء للنشر والتوزيع، عمان، 2016م .
16. الحيمودي، محمد، "الأمن السيبراني وحماية الأنظمة المعلوماتية"، مجلة الأكاديمية الأمريكية العربية للعلوم والتكنولوجيا، 2023م .
17. الجنفاوي، عبد الله، "التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني"، مجلة الآداب والعلوم الإنسانية، 2021م .
18. الزغبي، محمد، *الأمن السيبراني وحماية المعلومات الرقمية*، دار البداية للنشر والتوزيع، عمان، 2020م .
19. الشوابكة، أحمد، *إدارة أمن المعلومات والأمن السيبراني*، دار أمجد للنشر والتوزيع، عمان، 2021م .
20. الحربي، فهد، *الأمن السيبراني ومخاطر الهجمات الإلكترونية*، دار المسيرة للنشر والتوزيع، عمان، 2021م .
21. أبو العلا، محمد، *الجرائم الإلكترونية وأمن المعلومات*، دار الفكر الجامعي، الإسكندرية، 2020م .
22. الجبوري، علي، *أمن المعلومات وحماية البيانات الإلكترونية*، دار صفاء للنشر والتوزيع، عمان، 2018م .
23. الشمري، سعد، *إدارة أمن المعلومات والأمن السيبراني*، دار البداية للنشر والتوزيع، عمان، 2020م .
24. القحطاني، عبد الله، *الأمن السيبراني وحماية البنية التحتية الحيوية*، دار جامعة نايف للنشر، الرياض، 2021م .
25. العتيبي، ناصر، *إدارة المخاطر السيبرانية في المؤسسات الحيوية*، مكتبة الرشد، الرياض، 2022م.

1. Tareq Alnnale. (2026). From Reactive to Proactive Governance: A Hybrid LSTM–Gradient Boosting Architecture for Real-Time Anomaly Signal Detection in Multi-Store Retail Supply Chain Decision Systems. Al-Farooq Journal of Sciences, 2 (1), 987-1005.
2. Tariq Alnnale. (2026).Predictive Governance in Digital Enterprises: An LSTM-Enhanced Deep Learning Framework for Economic Optimization of IT Incident Management Using Enriched Process Logs.DOI: https://doi.org/10.65405/dctw1z34 .