العلوم الاقتصادية
العدد ثمانية وسبعون/ المجلد عشرون/ أيلول 2025

واقع امن المعلومات في مديرية بلديات محافظة نينوى دراسة مسحية لعينة من العاملين في مديرية بلديات محافظة نينوى

المدرس المساعد انعام عبد الجبار سلطان
الجامعة التقنية الشمالية / المعهد الإداري التقني – نينوى

المستخلص :

يعد أمن المعلومات أحد الجوانب الأساسية التي تضمن الحفاظ على سرية وسلامة وتوافر البيانات داخل المنظمات، نظرًا لتعدد الأجهزة والتقنيات التي تتعامل مع المعلومات. إلا أن تطبيق هذا المفهوم يواجه تحديات متعددة، خاصة مع ظهور الاتجاهات الحديثة في الإدارة التي تؤكد على أهمية إشراك الموظفين في اتخاذ القرارات وتعزيز الشفافية التنظيمية. في المقابل، أدى التطور المتسارع في تكنولوجيا المعلومات والاتصالات إلى نشوء تهديدات جديدة تتطلب من المؤسسات تطوير استراتيجيات أمنية فاعلة لمواجهتها والحد من مخاطرها. يركز البحث على تحليل واقع أمن المعلومات في مديرية بلديات محافظة نينوى، وذلك من خلال دراسة العوامل المؤثرة على أمن البيانات وتقييم الإجراءات الوقائية المطبقة فيها. لتحقيق ذلك، اعتمد البحث على المنهج الوصفي التحليلي، حيث تم تصميم استبيان ورقي لجمع البيانات من 35 موظفًا داخل المديرية، وذلك بهدف قياس آرائهم حول أمن المعلومات باستخدام مقياس ليكرت الخماسي، فيما تم تحليل النتائج باستخدام البرنامج الإحصائي SPSS. بُنيت الدراسة على فرضيتين رئيسيتين، الأولى تفترض وجود علاقة ذات دلالة معنوية بين طبيعة التهديدات وأمن المعلومات في المديرية، في حين تفترض الفرضية الثانية وجود علاقة معنوية بين التدابير الأمنية المطبقة وأمن المعلومات. وتوصل البحث إلى مجموعة من النتائج، من أبرزها ضرورة تعزيز إجراءات الحماية المادية والبرمجية، إلى جانب رفع مستوى الوعي لدى الموظفين حول أهمية أمن المعلومات. كما أكدت الدراسة أهمية وضع سياسات أمنية واضحة ومتاحة لجميع الموظفين لضمان الامتثال لها، فضلاً عن ضرورة تحديث أنظمة الأمان بشكل دوري لتقليل الثغرات الأمنية المحتملة.

الكلمات المفتاحية: امن المعلومات، التهديدات، الحماية.

Information Security in the Directorate of Municipalities of Nineveh: A Survey of Employees

Assistant Lecturer In'am Abdul Jabbar Sultan Al-Taie

Northern Technical University / Technical Administrative Institute - Nineveh

Abstract :

Information security is a fundamental aspect that ensures the confidentiality, integrity, and availability of organizational data, especially given the growing diversity of devices and technologies. However, its implementation faces challenges, particularly with modern management approaches that emphasize employee participation in decision-making and organizational transparency. Meanwhile, the rapid development of information and communication technologies has introduced new threats that require effective security strategies.

This study analyzes the reality of information security in the Directorate of Municipalities of Nineveh Governorate by examining influencing factors and evaluating applied preventive measures. Adopting a descriptive-analytical method, data were collected through a questionnaire distributed to 35 employees and analyzed using SPSS with a five-point Likert scale. The research was based on two main hypotheses: the first assumes a significant relationship between the nature of threats and information security, while the second assumes a significant relationship between applied security measures and information security.

The findings highlight the necessity of enhancing both physical and software protection, raising employees' awareness of information security, establishing clear and accessible security policies, and periodically updating systems to minimize vulnerabilities..

Keywords: Information Security, Threats, Protection

الفصل الأول

أولا: المقدمة

تزامن تطور أمن المعلومات مع تطور تقنيات المعلومات والاتصالات، حيث أصبحت المعلومات الرقمية مكونًا أساسيًا في مختلف القطاعات، مما أدى إلى زيادة الحاجة إلى حمايتها من التهديدات المتزايدة (Alotaibi et al., 2023). مع تزايد الاعتماد على الأنظمة الحاسوبية في معالجة البيانات الحساسة، ظهر تحدي تأمين هذه المعلومات من الوصول غير المصرح به والاختراقات الإلكترونية، مما دفع المؤسسات إلى تطوير إجراءات وقائية تهدف إلى حماية بياناتها وتعزيز سلامتها الرقمية (Tian et al., 2022). وزاد تعقيد هذا التحدي مع توسع استخدام الإنترنت وربط الأجهزة الحاسوبية عالميًا، مما أتاح فرصًا كبيرة للأفراد والشركات في إدارة أعمالهم، والتواصل الاجتماعي، وتنفيذ العمليات التجارية والتعليمية عبر الإنترنت. ومع ذلك، فإن التوسع في تقديم الخدمات الرقمية لم يكن خاليًا من المخاطر، حيث أشارت الدراسات الحديثة إلى أن الأنظمة الرقمية تتعرض بشكل متزايد للهجمات الإلكترونية، واختراقات البيانات، والتعدي على المعلومات الحساسة، مما يعزز الحاجة إلى اعتماد استراتيجيات أمنية متطورة (Kim et al., 2023).

بات أمن المعلومات اليوم أحد العلوم المحورية في مجال تقنية المعلومات، حيث أصبح يشكل عنصرًا رئيسيًا في ضمان استدامة المؤسسات وحماية بياناتها من التهديدات السيبرانية المتنامية. مع تحول البيانات إلى أصول استراتيجية، تواجه المنظمات تحديات متزايدة في تأمين بنيتها التحتية الرقمية وتعزيز مستويات الحماية السيبرانية (Gupta et al., 2024). من هذا المنطلق، يسعى هذا البحث إلى تحليل التهديدات التي تواجه أمن المعلومات في المنظمات، والطرق الفعالة لحمايتها من المخاطر المتزايدة، وذلك من خلال دراسة حالة في إحدى المؤسسات الحكومية. ويعتمد البحث على منهج وصفي تحليلي، حيث يناقش في الفصل الأول الإطار النظري والمنهجية البحثية، إضافة إلى مراجعة الأدبيات السابقة التي تناولت هذا الموضوع. يتناول الفصل الثاني الأسس النظرية لأمن المعلومات، وأبرز التهديدات التي تواجه المؤسسات والاستراتيجيات الأمنية المتاحة للحماية منها. أما الفصل الثالث، فيركز على تحليل البيانات الميدانية من خلال استطلاع آراء العاملين في المؤسسة المدروسة حول واقع أمن المعلومات والتحديات التي تواجههم، بينما يتضمن الفصل الرابع أهم الاستنتاجات والتوصيات التي توصل إليها البحث، والتي تهدف إلى تعزيز الأمن السيبراني في بيئات العمل الرقمية.

ثانيا: منهجية البحث

1: مشكلة البحث

مثل أمن المعلومات أحد التحديات الأساسية التي تواجه المنظمات في العصر الرقمي، حيث تتعرض البيانات المخزنة في الأنظمة المعلوماتية لتهديدات متعددة قد تؤثر على سلامتها وسريتها وتوافرها. في هذا السياق، تبرز الحاجة إلى تحليل واقع أمن المعلومات داخل المؤسسات، والتعرف على أنواع التهديدات الأمنية التي تواجهها، إلى جانب دراسة الإجراءات والتدابير الوقائية المستخدمة لحماية البيانات والأنظمة الرقمية. بناءً على ذلك، يسعى هذا البحث إلى دراسة واقع أمن المعلومات في إحدى المؤسسات الحكومية التابعة لمحافظة نينوى، وتحديد مستوى التحديات الأمنية التي تواجهها والآليات المتبعة لمواجهتها. تتمحور الإشكالية البحثية حول السؤال الرئيسي التالي:

ما هو واقع أمن المعلومات في مديرية بلديات محافظة نينوى؟

2: اهمية البحث

تبرز أهمية هذا البحث في التركيز على استعراض الآليات الفعالة التي تتضمن تحقيق أمن المعلومات داخل المنظمات، وتحديد الطرق التي يمكن تبنها لحماية الأنظمة المعلوماتية من التهديدات المتزايدة، سواء كانت برمجية، مادية، أو تنظيمية.

يهدف البحث إلى تقديم رؤية تحليلية حول طبيعة التهديدات التي تواجهها نظم المعلومات، بما في ذلك الهجمات السيبرانية، الاختراقات الأمنية، والتحديات التقنية والتنظيمية، مع التركيز على الاستراتيجيات الحديثة للحماية، مثل التدابير المادية والبرمجية المتقدمة (Stallings, 2020). علاوة على ذلك، يعزز البحث الفهم المتعمق لكيفية تطبيق حلول أمنية متطورة، مثل أنظمة التشفير، البروتوكولات الأمنية، والتحقق المتعدد العوامل، التي تسهم في تقليل مخاطر الاختراقات وضمان سرية البيانات وسلامتها (Von Solms & Van Niekerk, 2013). كما يناقش البحث أهمية وجود سياسات أمنية واضحة يتم تنفيذها ومتابعتها من قبل الموظفين، لضمان الالتزام بالمعايير الأمنية وتعزيز وعي العاملين حول ممارسات الأمن السيبراني الفعالة (Sharma, Chen, & Sheth, 2022).

إلى جانب ذلك، يمكن لهذا البحث أن يسهم في توسيع نطاق الدراسات المستقبلية المتعلقة بأمن المعلومات، من خلال تقديم إطار بحثي يساعد الباحثين على دراسة تحديات أمن المعلومات من منظور أكثر شمولية، خاصةً في ظل التحولات الرقمية المتسارعة والاعتماد المتزايد على الحوسبة السحابية والتقنيات الذكية (Al-Janabi & Al-Shourbaji, 2016). ويعزز البحث إمكانية تطوير استراتيجيات جديدة لمكافحة التهديدات السيبرانية في المنظمات، مما يسهم في تحسين الأمن المعلوماتي وضمان استدامة نظم المعلومات في مختلف البيئات التنظيمية.

3: اهداف البحث

يهدف البحث إلى تقديم فهم أعمق لمفهوم أمن المعلومات وآلياته، مع التركيز على استراتيجيات الحماية الفعالة وطرق تطبيقها في البيئات التنظيمية الحديثة. كما يسعى إلى تحليل واقع أمن المعلومات في المنظمة محل الدراسة، من خلال تقييم مدى تأثير التهديدات الأمنية على أنظمتها المعلوماتية وقدرتها على التصدي لهذه المخاطر (Stallings, 2020). إلى جانب ذلك، يهدف البحث إلى استكشاف أساليب الحماية المستخدمة في تأمين المعلومات داخل المنظمات، وتحديد مدى فعاليتها في ضمان سرية البيانات وسلامتها وتوافرها (Von Solms & Van Niekerk, 2013). كما يسعى إلى تقديم رؤى تحليلية تسهم في إثراء الفهم الأكاديمي والتطبيقي لمجال أمن المعلومات، من خلال توضيح وجهات نظر جديدة أو تعميق الرؤى الحالية حول أهمية الأمن المعلوماتي في استدامة الأعمال وتعزيز القدرة التنافسية للمنظمات (Sharma, Chen, & Sheth, 2022). علاوة على ذلك، تحديد موقع المنظمة ضمن المشهد المتغير لأمن المعلومات، ومدى مواكبتها للتطورات التقنية الحديثة في هذا المجال، مما يمكنها من تحسين استراتيجيات الحماية وتطوير سياسات أمنية أكثر تكاملًا وفاعلية (Al-Janabi & Al-Shourbaji, 2016).

4: التساؤلات البحثية

استنادًا إلى إشكالية البحث، يمكن طرح مجموعة من التساؤلات التي تسهم في توجيه الدراسة نحو تحقيق أهدافها وفهم واقع أمن المعلومات داخل المنظمات، ومن أهم هذه الأسئلة:

- ✓ ما المقصود بمفهوم أمن المعلومات، وما أهميته في السياقات التنظيمية الحديثة؟ (Stallings, 2020).
- ✓ ما أبرز التهديدات التي تواجه أمن المعلومات داخل المؤسسات، وكيف تؤثر على سرية البيانات وسلامتها؟ (Von Solms & Van Niekerk, 2013).
- ✓ ما هي استراتيجيات الحماية التي تعتمدها المنظمات لضمان أمن معلوماتها، وما مدى فعاليتها في التصدي للهجمات السيبرانية؟ (Sharma, Chen, & Sheth, 2022).
- ✓ إلى أي مدى تتأثر ممارسات أمن المعلومات بطبيعة التهديدات التي تواجهها المنظمة، وما العوامل التي تسهم في تحسين أو تقويض فاعلية هذه الممارسات؟ (Al-Janabi & Al-Shourbaji, 2016).

5: فرضيات الدراسة

للإجابة على الاشكالية والتساؤلات البحثية تم وضع الفرضيات التالية:

1- الفرضية الرئيسية الاولى:(يوجد علاقة ارتباط ذو دلالة معنوية بين طبيعة التهديدات وامن المعلومات في المنظمة المبحوثة).

2-الفرضية الرئيسة الثانية: (يوجد علاقة ارتباط ذو دلالة معنوية بين طبيعة الحماية المطبقة وامن المعلومات في المنظمة المبحوثة).

6: منهج البحث

تم تبني منهجية بحثية متكاملة تتماشى مع طبيعة الدراسة، حيث تم تقسيم المنهج إلى جانبين رئيسيين:

الجانب النظري: اعتمدت الدراسة على المنهج المسحي، حيث تم الرجوع إلى مجموعة من المصادر المتخصصة في مجال أمن المعلومات باللغتين العربية والإنجليزية، شملت الكتب الأكاديمية، المقالات المنشورة في المجلات العلمية المحكمة، الأبحاث العلمية المتمثلة في رسائل الماجستير وأطروحات الدكتوراه، بالإضافة إلى مصادر إلكترونية موثوقة لدعم الإطار النظري للبحث (Alqahtani & Kavakli, 2023; Smith et al., 2022).

الجانب التطبيقي: تم تنفيذ دراسة ميدانية استهدفت موظفي مديرية بلديات نينوى، حيث تم توزيع استبانة ورقية على عينة مكونة من (35) موظفًا لجمع البيانات الأولية. تم اعتماد باستخدام مقياس ليكرت الخماسي لقياس إجابات المشاركين، وتمت معالجة البيانات باستخدام البرنامج الإحصائي SPSS (الإصدار 26) لاستخراج النتائج وتحليلها (Jones & Chen, 2024; Brown et al., 2023).

7: حدود البحث

الحدود المكانية: تم إجراء هذه الدراسة في مديرية بلديات محافظة نينوى، حيث تم استهداف بيئة العمل الإدارية ضمن هذه المؤسسة لتحليل واقع أمن المعلومات فيها.

الحدود الزمانية: تم تنفيذ البحث خلال الفترة الممتدة من 15 فبراير 2024 إلى 10 مايو 2024، حيث تم جمع البيانات وتحليلها ضمن هذا الإطار الزمني لتقييم التهديدات الأمنية وسبل الحماية المستخدمة.

الحدود البشرية: شملت الدراسة عينة من 35 موظفًا من الكوادر العاملة في مديرية بلديات محافظة نينوى، حيث تم اختيارهم لقياس مدى وعيهم بمفاهيم أمن المعلومات، التهديدات السيبرانية، وفعالية التدابير الوقائية المتبعة في المؤسسة.

8: ابعاد البحث

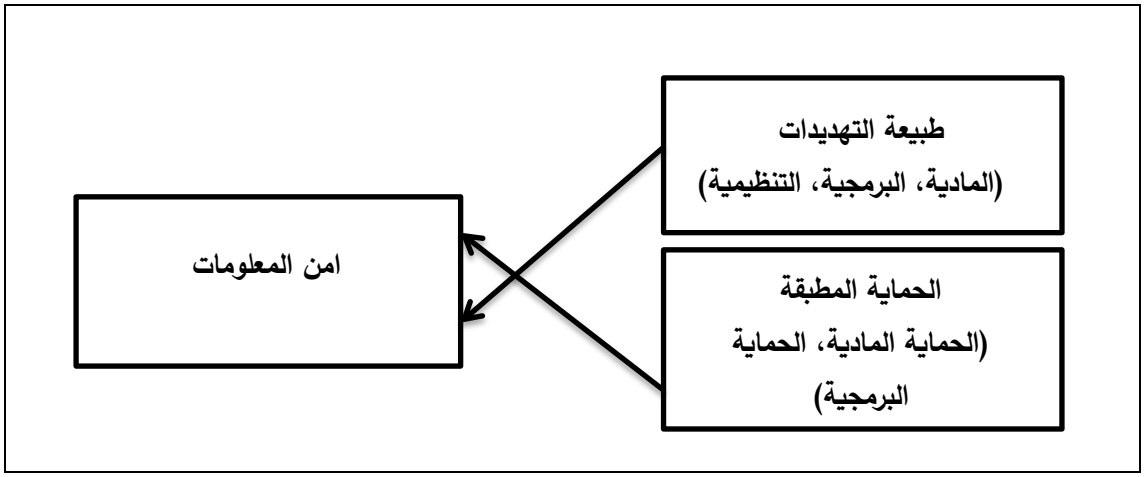
تناول البحث أبعاده بشكل تفصيلي ضمن الإطار النظري، حيث تم تحديد المتغيرات التي تشكل المحاور الرئيسية للدراسة على النحو التالي:

البعد الأول – أمن المعلومات: يُمثل المتغير التابع في الدراسة، حيث يُركز على مستوى الحماية المطبقة داخل المنظمة وتأثيرها على سرية وسلامة وتوافر المعلومات.

البعد الثاني – طبيعة التهديدات: يُعد المتغير المستقل الأول، ويتضمن التهديدات التي قد تؤثر على أمن المعلومات، وتشمل: التهديدات المادية، مثل الوصول غير المصرح به للأجهزة أو تدمير البنية التحتية. التهديدات البرمجية، كالهجمات السيبرانية والبرمجيات الخبيثة. التهديدات التنظيمية، والتي تتعلق بعدم وجود سياسات وإجراءات واضحة لحماية البيانات.

البعد الثالث – الحماية المطبقة: يُشكل المتغير المستقل الثاني، حيث يركز على التدابير الأمنية التي تعتمدها المنظمة لحماية بياناتها، والتي تشمل: الحماية المادية، مثل أنظمة التحكم في الوصول والمراقبة الأمنية. الحماية البرمجية، والتي تشمل الجدران النارية، أنظمة التشفير، وبرمجيات مكافحة الفيروسات لضمان سلامة البيانات. المنهج الوصفي التحليلي في تحليل البيانات

مخطط البحث



الشكل (1) مخطط الدراسة من اعداد الباحثة

ثالثا : الدراسات السابقة:

1: الاسرار المعلوماتية وحمايتها – للباحث عزيزة (2019): هدفت هذه الدراسة إلى تحليل السلوكيات المجرَّمة المتعلقة بانتهاك السرية المعلوماتية، مع التركيز على طرق إثبات هذه الجرائم عندما تمتد عبر الحدود. تناولت الدراسة الجرائم الإلكترونية التي تستهدف سرية البيانات عبر الأنظمة المعلوماتية، وخلصت إلى عدد من النتائج، أبرزها: ضرورة تجريم قرصنة البيانات، مع استثناء البرامج التي يشملها قانون حماية الملكية الفكرية. كما أوضحت أن التجسس المعلوماتي يختلف عن الدخول غير المصرح به إلى الأنظمة، مما يتطلب تمييزًا دقيقًا بينهما في التشريعات القانونية لضمان حماية البيانات بفاعلية.

2: قواعد الأمن المعلوماتي - الباحثة بورباية صورية (2016): تناولت هذه الدراسة إشكالية تحديد متطلبات الحماية اللازمة لضمان الأمن المعلوماتي، بالإضافة إلى نطاق الجرائم التي تهدده. وهدفت إلى تحليل القواعد التقنية والقانونية للأمن المعلوماتي، واستعراض أنظمة الحماية على مختلف المستويات، مع التركيز على التدابير التقنية والقانونية لمكافحة الجرائم الإلكترونية. خلصت الدراسة إلى أن الأمن المعلوماتي، سواء من الناحية التقنية أو القانونية، يمثل الوسيلة الأساسية لتعزيز الثقة في المعاملات الإلكترونية وتأمين الاتصالات الرقمية. كما أشارت إلى أن التشريعات الحالية، سواء الموضوعية أو الإجرائية، لا تزال غير كافية لمواجهة التهديدات المتزايدة التي تستهدف أمن المعلومات، مما يستدعي تطوير أطر قانونية أكثر تكيفًا مع التحديات الرقمية الحديثة.

3: تقييم مدى مساهمة أمن نظم المعلومات الإلكتروني في الحد من مخاطر نظم المعلومات - الباحث قدور مقراني (2016): ركزت هذه الدراسة على تقييم فعالية أمن نظم المعلومات في مؤسسة اتصالات الجزائر، مع تحليل أنواع المخاطر التي تهدد هذه النظم ومدى تأثير السياسات الأمنية على الجوانب المادية والبرمجية لنظم المعلومات. كما هدفت إلى تحديد أبرز التهديدات التي تواجه بيئات نظم المعلومات، ودراسة الإجراءات الوقائية التي يمكن أن تسهم في الحد من هذه المخاطر. خلصت الدراسة إلى أن تعزيز أمن نظم المعلومات يعد عنصرًا أساسيًا لحماية البيانات والبنية التحتية التقنية، حيث تلعب السياسات الأمنية دورًا جوهريًا في تقليل الثغرات الأمنية وتحسين كفاءة عمل الأنظمة، مما يسهم في تحقيق استدامة العمليات التقنية وتقليل المخاطر المرتبطة بالهجمات الإلكترونية والاختراقات المحتملة.

4: تقويم نظام إدارة أمن المعلومات في دائرة تكنولوجيا المعلومات وفق المواصفات ISO 27001" - الباحثان حاتم ناهي محيسن وعواد كاظم حمود (2015): تناولت هذه الدراسة تطبيق المعايير القياسية الدولية لنظام إدارة أمن المعلومات وفق مواصفات

ISO 27001 في وزارة العلوم والتكنولوجيا، مع التركيز على دائرة تكنولوجيا المعلومات. هدفت الدراسة إلى الحد من التهديدات التي تواجه أمن نظم المعلومات من خلال تبني سياسة معلنة لإدارة أمن المعلومات، مما يسهم في تحسين الممارسات الأمنية وتعزيز مستوى الحماية. أظهرت النتائج أن الالتزام بتطبيق معايير ISO 27001 يسهم في تعزيز كفاءة إدارة المخاطر الأمنية، ويوفر ضمانات مقبولة لحماية البيانات والمعلومات الحيوية، كما يعزز موثوقية الأنظمة ويضمن فاعلية أكبر في تنفيذ العمليات، مما يرفع من ثقة المستخدمين والمستفيدين في بيئة العمل الرقمية.

5: واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها" - أيمن محمد فارس الدنف (2013): تناولت هذه الدراسة واقع إدارة أمن نظم المعلومات في الكليات التقنية بقطاع غزة، من خلال طرح الإشكالية البحثية حول مستوى تطبيق سياسات أمن المعلومات في هذه المؤسسات، وسبل تطويرها. استخدم الباحث المنهج الوصفي التحليلي، حيث شمل مجتمع الدراسة العاملين في نظم المعلومات بالكليات التقنية، واعتمدت أدوات البحث على الاستبانة والمقابلة لجمع البيانات. أظهرت النتائج أن البنية التحتية لنظم المعلومات في الكليات التقنية متوفرة بمستوى متوسط، وأن الإدارات العليا تدرك أهمية تبني سياسات أمن المعلومات. ومع ذلك، لم تُطبق هذه السياسات في أي من الكليات التقنية بشكل واضح ومنهجي، مما يستدعي تطوير استراتيجيات شاملة لتعزيز أمن المعلومات وضمان حمايتها وفق معايير محددة.

رابعا: مجال الاستفادة من الدراسات السابقة:

ساعدت الدراسات السابقة، عند الاطلاع عليها، في إثراء الجانب النظري للبحث، كما وفرت للباحثة فهماً أعمق للدلالات الإحصائية المتعلقة بأبعاد تلك الدراسات. إضافةً إلى ذلك، أسهمت هذه الدراسات في تحديد الفجوة البحثية، والتي تتمثل في الحاجة إلى استكشاف العوامل الأكثر ارتباطًا بأمن المعلومات في المنظمات العراقية، لا سيما في محافظة نينوى. ويرجع ذلك إلى محدودية الأبحاث التي تناولت هذا المجال في البيئة العراقية بشكل عام، وفي نينوى بشكل خاص، مما يبرز أهمية هذا البحث في سد هذه الفجوة وتعزيز الفهم العلمي لواقع أمن المعلومات في المنطقة.

الفصل الثاني

المبحث الاول

أولا: مفاهيم امن المعلومات

في ظل الثورة المعلوماتية المتسارعة، أصبحت الإدارة الحديثة تواجه تحديات متزايدة نتيجة التطورات السريعة في تقنية المعلومات، والتي أحدثت تغييرات جوهرية في مختلف المجالات. فقد أدى الانتشار الواسع لتكنولوجيا المعلومات إلى تسهيل عملية تداول البيانات وانتقالها بسرعة فائقة، مما جعلها أكثر عرضة للمخاطر الأمنية مثل الاختراقات الإلكترونية، والتلاعب بالبيانات، وسرقة المعلومات الحساسة (Kumar & Singh, 2023). ومن هذا المنطلق، برزت الحاجة الملحة إلى حماية المعلومات وضمان أمنها، وهو ما دفع الباحثين والمتخصصين في هذا المجال إلى تطوير مفاهيم واستراتيجيات تعزز أمن المعلومات وتحد من التهديدات المرتبطة بها (Alcaraz & Zeadally, 2021). ومن هنا، نشأ مفهوم "أمن المعلومات"، الذي أصبح من القضايا الأساسية التي تستوجب البحث والدراسة لضمان سلامة البيانات وحمايتها من المخاطر المتعددة، وهو ما سيتم التطرق إليه في هذا البحث.

ثانيا: ماهية امن المعلومات:

يُعرَّف أمن المعلومات على أنه مجموعة من السياسات والإجراءات والتدابير التقنية والإدارية المصممة لحماية البيانات من الوصول غير المصرح به، أو التلاعب، أو الفقدان، أو التهديدات الأمنية المختلفة. وفقًا لـ(Laudon, 2005)، يُشير أمن المعلومات إلى "الإجراءات والتقنيات التي تمنع الوصول غير المخول أو التغيير أو السرقة أو الإضرار المادي بأنظمة المعلومات". بينما يُعرفه (القحطاني، 2015) بأنه "مجموعة من التدابير التقنية والإدارية الهادفة إلى حماية أصول المعلومات من الوصول أو الاستخدام

غير المصرح به، سواء كان ذلك عمدًا أو سهواً. من منظور أكثر شمولية، يُعرِّف (الشوابكة، 2019) أمن المعلومات بأنه "حماية الأصول الرقمية والمادية ضد التهديدات المختلفة مثل الاختراق، والتجسس، والكوارث الطبيعية، وذلك من خلال تدابير تقنية كالجدران النارية وكلمات المرور، وأخرى مادية مثل الأقفال والحواجز الأمنية". بينما يشير (Whitman & Mattord, 2011) الى أن تحقيق أمن المعلومات في أي منظمة يتطلب تكامل عدة مكونات أساسية، تشمل: الأمن المادي، الذي يهدف إلى حماية الأصول المادية والمباني من الوصول غير المصرح به؛ أمن الأفراد، لضمان حماية الأشخاص المخولين بالوصول إلى البيانات؛ أمن العمليات، الذي يركز على تأمين الأنشطة والإجراءات التشغيلية داخل المنظمة؛ أمن الاتصالات، لحماية تقنيات الاتصال والمحتوى المتبادل عبرها؛ أمن الشبكات، الذي يعنى بحماية البنية التحتية للشبكة والمعلومات المتداولة داخلها؛ وأخيرًا، أمن البيانات، الذي يضمن سرية وسلامة وتوافر المعلومات، مما يعزز من قدرة المنظمة على مواجهة التهديدات الإلكترونية المتزايدة. ومن خلال التعريف يتضح لنا ان امن المعلومات ما هو الا مصطلح يضم في محتواه امن عام، فحماية المعلومات تكون من خلال الامن المادي كالأجهزة التي تضم المعلومات، وامن الافراد الذين يملكون المعلومات وكل ماله علاقة بالمعلومات.

ثالثا: عناصر امن المعلومات

تسعى المنظمات إلى تحقيق أمن المعلومات من خلال تطبيق نموذج ثالوث (CIA Triangle)، الذي يتضمن ثلاثة عناصر أساسية: السرية (Confidentiality)، التي تهدف إلى حماية البيانات من الوصول غير المصرح به؛ التكاملية والسلامة (Integrity)، التي تضمن دقة وموثوقية المعلومات وعدم التلاعب بها؛ والتوفر (Availability)، الذي يضمن إمكانية الوصول إلى المعلومات والأنظمة عند الحاجة دون تعطيل أو انقطاع (بطيخ، 2021).

1: السرية (Confidentiality): تعني حماية البيانات المخزنة والمنقولة من الوصول غير المصرح به، بحيث لا يمكن الاطلاع عليها أو استخدامها إلا بإذن مسبق. يتحقق ذلك من خلال أنظمة تحكم تحدد صلاحيات المستخدمين فيما يتعلق بالقراءة، الإدخال، التعديل، أو الحذف، مع تأمين مسارات الاتصال لمنع اعتراض البيانات أثناء نقلها (القحطاني، 2015).

2: التكاملية والسلامة (Integrity): تهدف إلى ضمان عدم تغيير البيانات أو إتلافها سواء كان ذلك متعمدًا أو غير متعمد خلال مراحل الإدخال، النقل، أو التخزين. تشمل سلامة المعلومات سلامة المحتوى، أي التأكد من دقة البيانات المدخلة وعكسها للواقع، وسلامة المصدر، أي الحصول على المعلومات من مصادر موثوقة دون تلاعب أو تحريف (القحطاني، 2015).

3: التوفر (Availability): يشير إلى ضمان إمكانية وصول المستخدمين المصرح لهم إلى المعلومات والأنظمة عند الحاجة، دون انقطاع أو تعطيل. يتحقق ذلك من خلال خصائص مثل المقاومة ضد الهجمات التي تعطل الخدمة، سهولة الاستخدام، المرونة في إدارة النظام دون الحاجة إلى إيقافه، والتوسعية لاستيعاب الاحتياجات المستقبلية. لضمان استمرارية التوفر، يجب حماية كافة مكونات النظام، بما في ذلك التطبيقات، قواعد البيانات، والخوادم، إضافةً إلى تأمين الشبكات من البداية إلى النهاية (أبو مغايض، 2012). ويعد تحقيق السرية، السلامة، والتوفر أمرا ضروريا في جميع أنظمة أمن المعلومات، لكن قد يختلف التركيز على أحدها تبعًا لطبيعة المنظمة والبيانات التي تتعامل معها.

رابعا: خصائص امن المعلومات

تحدد المؤسسة الوطنية للمقاييس والتكنولوجيا (NIST, 2002) مجموعة من الخصائص الأساسية لأمن المعلومات، والتي يجب أن تتماشى مع رؤية وأهداف المؤسسة لضمان فعاليته. إذ يعد أمن المعلومات جزءًا جوهريًا من الإدارة الناجحة، ويجب تطبيقه وفق رؤية اقتصادية مستدامة. كما يجب أن تكون دراسة أنظمة الأمن شاملة ومتكاملة، بحيث تغطي جميع الجوانب التنظيمية والتقنية. إضافةً إلى ذلك، فإن مسؤولية أمن المعلومات تمتد داخل المؤسسة وخارجها، ما يستوجب إدارة فعالة للمخاطر لضمان الحماية المستمرة. كما يتأثر أمن المعلومات بالعوامل الاجتماعية التي قد تؤثر على ممارسات الأمان داخل المؤسسات. علاوة على ذلك، فإن برامج الأمن تحتاج إلى إعادة تقييم دورية لضمان مواكبتها للتطورات التكنولوجية والتهديدات المستجدة.

خامسا: أهمية امن المعلومات

يوفر استخدام أنظمة المعلومات فرصًا عديدة، لكنه في المقابل يعرّض المؤسسات لمخاطر تتفاوت في شدتها، حيث تكمن هذه المخاطر في الفجوة بين الحاجة إلى حماية الأنظمة ومستوى الأمان المطبق فعليًا. لذا، أصبح من الضروري تطوير أنظمة أمنية توفر بيئة موثوقة للتعامل مع البيانات (Khlaif et al, 2023). وتبرز أهمية أمن المعلومات نتيجة لعدة عوامل، من أبرزها: الارتباط المتزايد بشبكات الاتصالات والإنترنت، مما يجعل عزل الأجهزة عن الشبكات أمرًا غير ممكن. كما أن اعتماد المؤسسات على أنظمة معلومات آمنة أصبح ضروريًا لضمان استمرارية الأعمال. الى جانب ذلك، فإن صعوبة تتبع الجرائم الإلكترونية بسبب غياب الحدود الجغرافية يزيد من تعقيد إدارة المخاطر الأمنية.

كما أن التطور السريع في التجارة الإلكترونية، الحكومة الإلكترونية، والإدارة الرقمية يتطلب بيئة معلوماتية محمية. علاوة على ذلك، تعتمد المؤسسات بشكل أساسي على دقة وموثوقية البيانات، مما يفرض على الإدارات مسؤولية توفير بيئة آمنة لأنظمة المعلومات. أخيرًا، فإن ضعف التدابير الأمنية، مثل الإفشاء غير المصرح به للمعلومات الحساسة، قد يؤدي إلى خسائر مالية كبيرة وتأثيرات سلبية على سمعة المؤسسة (Ahmed, 2021)

سادسا: اهداف امن المعلومات

يجب أن تتناسب معايير أمن المعلومات مع قيمة البيانات التي تحتاج إلى الحماية، حيث تهدف هذه المعايير إلى ضمان سلامتها وموثوقيتها. يُعد تقليل مخاطر الفقدان أو التشويه أو الإتلاف أحد الأهداف الأساسية التي تتطلب تنفيذ برامج حماية لنظم المعلومات يتم اختبارها وتحديثها بانتظام بالتنسيق مع المستخدمين، مما يضمن استقرار البيانات وحمايتها من أي تلاعب أو فقدان غير مقصود. كما أن سرية البيانات الشخصية تُعد ركيزة أساسية، حيث يقع على عاتق المؤسسات مسؤولية اتخاذ التدابير اللازمة لمنع تسريب المعلومات وضمان خصوصيتها بحيث لا يتم كشفها إلا للأفراد المخولين بذلك، وهو ما يتطلب مزيجًا من الحلول التقنية والإجراءات التنظيمية الفعالة التي يشارك في تنفيذها خبراء أمن المعلومات. بالإضافة إلى ذلك، يُعد تحديد المسؤوليات أمرًا جوهريًا لضمان جودة البيانات وحمايتها من التلاعب، حيث يساعد في محاسبة الجهات المعنية عند حدوث أي خرق أمني أو تعديل غير مصرح به، مما يعزز مصداقية النظام الأمني ويضمن بيئة معلوماتية آمنة ومستقرة (Directive, 2014).

المبحث الثاني

أولا: تهديدات أمن المعلومات

أصبحت المؤسسات تواجه تحديات معقدة في مجال أمن المعلومات بسبب التطورات التقنية المتسارعة وظهور تهديدات متنوعة تهدد سلامة بياناتها. على الرغم من أن التهديدات الرقمية تتشابه في طبيعتها مع التهديدات التقليدية في العالم الحقيقي، إلا أن بيئة الفضاء الإلكتروني تضيف أبعادًا جديدة تزيد من صعوبة التنبؤ بمصدر التهديد أو مكان حدوثه. فالتهديدات قد تنطلق من أي مكان حول العالم، مما يجعل مواجهتها أكثر تعقيدًا (الجغبري، 2020).

ثانيا: ماهية التهديدات:

يشير مفهوم تهديدات أمن المعلومات إلى أي نشاط أو حدث يعرض البيانات أو الأنظمة الرقمية للخطر، سواء كان ذلك بشكل مقصود أو غير مقصود. وفقًا لـ (الزين وآخرون، 2021)، يُعرَّف التهديد بأنه "هدف عدائي يمتلك وسائل فعلية يمكن أن تعرض الأفراد أو المؤسسات أو البنى التحتية للخطر". كما أن التهديد قد يكون نشاطًا يستغل الثغرات الأمنية بهدف التعديل غير المشروع على البيانات أو إعاقة الوصول إليها (الجغبري، 2020). من هنا، يُنظر إلى التهديدات على أنها كل ما يؤثر على سرية البيانات وتكاملها وتوافرها، سواء كان ذلك بفعلٍ خارجي أو داخلي، متعمد أو غير متعمد.

ثالثا: مصادر التهديدات:

يمكن تصنيف مصادر تهديدات أمن المعلومات إلى ثلاثة أنواع رئيسية:

التهديدات الطبيعية: تشمل الكوارث البيئية مثل الزلازل والفيضانات والحرائق وارتفاع درجات الحرارة، والتي قد تتسبب في تلف الأجهزة وفقدان البيانات.

التهديدات التقنية: تتضمن الأعطال البرمجية، وانقطاع التيار الكهربائي، ومشكلات الاتصال بالشبكات، التي يمكن أن تؤدي إلى تعطل الأنظمة وإيقاف العمليات التشغيلية.

التهديدات البشرية: قد تكون متعمدة مثل الهجمات السيبرانية التي تستهدف سرقة البيانات أو اختراق الأنظمة، أو غير متعمدة بسبب أخطاء العاملين ونقص الخبرة في التعامل مع الأنظمة الرقمية (عبد الحميد، 2020).

رابعا: أنواع المهاجمين السيبرانيين:

يختلف المهاجمون في دوافعهم ومستوياتهم التقنية، مما يؤثر على طبيعة التهديدات التي يواجهها النظام. يمكن تصنيف المهاجمين إلى الفئات التالية:

المخترقون الهواة (Hackers): يبحثون عن الثغرات بهدف الاستكشاف أو التحدي الشخصي، وقد لا يكون لديهم نوايا خبيثة.

المخترقون المحترفون (Crackers): أكثر خطورة من الهاكرز، حيث يستخدمون مهاراتهم في تدمير الأنظمة أو سرقة البيانات بدافع التخريب أو الربح.

المحتالون الإلكترونيون: يهدفون إلى تحقيق مكاسب مالية عبر الاحتيال أو التزوير أو الاختلاس، وغالبًا ما يستهدفون المؤسسات المالية.

المنتقمون (Malicious Users): يسعون للانتقام من مؤسسات عملوا بها سابقًا عبر تدمير البيانات أو تعطيل الأنظمة.

الجواسيس الإلكترونيون: يعملون لصالح دول أو شركات منافسة لاختراق الأنظمة وسرقة المعلومات الاستراتيجية (البداينة، 2014؛ بن يحيى، 2020).

خامسا: أنواع التهديدات الأمنية:

تنقسم التهديدات التي تواجه أنظمة المعلومات إلى نوعين رئيسيين:

التهديدات الناجمة عن الهجمات السيبرانية: وتشمل، البرامج الضارة (Malware)، وتشمل الفيروسات، والديدان الإلكترونية، وأحصنة طروادة، التي تهدف إلى تعطيل الأنظمة أو سرقة البيانات (أحمد، 2021). الهجمات الإلكترونية، مثل التنصت، وسرقة الهوية، وهجمات رفض الخدمة (DDoS) التي تستهدف تعطيل الأنظمة ومنع المستخدمين من الوصول إلى الخدمات (أحمد، 2021).

الهندسة الاجتماعية : استغلال نقاط الضعف البشرية للحصول على بيانات حساسة من خلال التلاعب والخداع (أحمد، 2021).

اما التهديدات الناتجة عن الثغرات الأمنية: تشمل: ثغرات برمجية، نقاط ضعف في البرمجيات تتيح للمهاجمين استغلالها لاختراق الأنظمة. او إدارة سيئة للمواقع الإلكترونية، قد تؤدي إلى كشف معلومات حساسة على الإنترنت، مما يجعلها عرضة للهجمات. اما لتحديثات غير المنتظمة ناتجة عن إهمال تحديث أنظمة التشغيل والتطبيقات الأمنية يترك المجال مفتوحًا أمام المهاجمين لاستغلال نقاط الضعف (القحطاني، 2015).

سادسا : إدارة الثغرات الأمنية

تنقسم الثغرات الأمنية إلى ثلاث فئات رئيسية:

1. **ثغرات على المستوى التنظيمي:** تشمل نقص الكفاءات في مجال الأمن السيبراني، وعدم وضوح سياسات الأمان، وغياب إجراءات التحكم والرقابة الفعالة.
2. **ثغرات على المستوى المادي:** مثل تقادم الأجهزة، وسوء إدارة الموارد، وغياب التدابير الوقائية مثل أنظمة تبريد مراكز البيانات لمنع ارتفاع درجة حرارة الأجهزة.
3. **ثغرات على المستوى التكنولوجي:** مثل أخطاء البرمجة، وسوء إدارة المواقع الإلكترونية، وضعف تشفير البيانات أثناء الإرسال عبر الإنترنت (خضر، 2020؛ Jean، 2012).

المبحث الثالث

أولا: وسائل تحقيق أمن المعلومات

يتطلب تحقيق أمن المعلومات منظومة حماية متكاملة تشمل جميع الجوانب التي قد تتعرض للتهديدات الأمنية. فالتعرف على التهديدات ليس كافيًا بحد ذاته، بل يمثل قاعدة لبناء استراتيجيات الحماية المناسبة. يعتمد تحقيق الأمن المعلوماتي على تطبيق إجراءات وقائية متعددة تشمل الحماية البرمجية للحواسيب والأنظمة، وكذلك الحماية المادية التي تستهدف تأمين البنية التحتية والمعدات التقنية للمؤسسة (القحطاني، 2015).

ثانيا: الحماية البرمجية لأنظمة المعلومات

تُعد الحماية البرمجية من الركائز الأساسية لأمن المعلومات، حيث تعتمد على مجموعة من الأدوات والتقنيات التي تهدف إلى حماية البيانات من التهديدات المختلفة مثل الاختراق، الفيروسات، والهجمات السيبرانية. ومن أبرز وسائل الحماية البرمجية ما يلي:

الجدار الناري (Firewall): ظهر في أواخر الثمانينيات كوسيلة لمنع الوصول غير المصرح به إلى الشبكات. يُعرف الجدار الناري بأنه أداة تقوم بفحص عمليات الدخول والخروج من وإلى الشبكة وفقًا لقواعد محددة، مما يسمح بحظر الأنشطة المشبوهة ومنع التهديدات السيبرانية (حسين، 2011).

برامج مكافحة الفيروسات: تُعد من الأدوات الضرورية لحماية الأجهزة من البرمجيات الضارة، حيث تعمل على اكتشاف الفيروسات وإزالتها. ومع ذلك، فإن فعاليتها تعتمد على التحديث المستمر، إذ أن البرامج القديمة قد لا تكون قادرة على التصدي للفيروسات الحديثة (خضر، 2020).

التشفير: يُستخدم التشفير لحماية سرية البيانات من خلال تحويلها إلى رموز غير مفهومة، ولا يمكن فك تشفيرها إلا باستخدام مفتاح خاص. يتم تطبيق نوعين من التشفير، التشفير المتماثل، يعتمد على مفتاح واحد يُستخدم للتشفير وفك التشفير، مما يستلزم سرية عالية عند نقله بين المرسل والمستقبل (صورية، 2018). التشفير غير المتماثل، يعتمد على زوج من المفاتيح (عام وخاص)، حيث يُستخدم المفتاح العام لتشفير البيانات، بينما يتم فك التشفير باستخدام المفتاح الخاص، مما يعزز الأمان عند نقل المعلومات عبر الشبكات (Alain، 2013).

مراقبة الدخول وأنظمة كشف التطفل: مراقبة الدخول، تشمل وضع سياسات تحدد هوية المستخدمين المسموح لهم بالوصول إلى الأنظمة، وتمنع الوصول غير المصرح به. اما أنظمة كشف التطفل، تُعد أنظمة متقدمة تراقب الشبكات بحثًا عن أي أنشطة غير طبيعية، وتُطلق إنذارات في حالة الاشتباه بوجود محاولة اختراق (قحطاني، 2015).

الشبكات الافتراضية الخاصة (VPN): تُستخدم لتأمين تبادل البيانات بين مواقع مختلفة عن طريق إنشاء اتصال مشفر يضمن سرية المعلومات ويمنع اختراقها أثناء النقل (Nicolas، 2015).

التحديثات الأمنية: تعد عمليات تحديث البرمجيات ضرورة لضمان استمرار الحماية من التهديدات السيبرانية، حيث تُصلح الثغرات الأمنية المكتشفة وتحدّ من مخاطر الاستغلال غير القانوني للأنظمة (بلجراف، 2017).

ثالثا: الحماية المادية لأنظمة المعلومات:

لا تقتصر حماية المعلومات على تأمين البرمجيات فحسب، بل تتطلب أيضًا إجراءات مادية لحماية البنية التحتية ومعدات تقنية المعلومات داخل المؤسسة. وتشمل الحماية المادية ما يلي:

تأمين موقع المنظمة: يشمل اختيار موقع آمن، وتحديد نطاق المنظمة باستخدام سياج أو حواجز أمنية، وتوزيع الحماية الأمنية بناءً على حساسية المناطق المختلفة داخل المؤسسة (Nicolas، 2015).

منع الدخول غير المصرح به: يتم تنفيذ ذلك من خلال تركيب أبواب إلكترونية مشفرة، ونظام مراقبة بالكاميرات، وأنظمة إنذار متطورة للكشف عن أي محاولات تسلل غير مشروعة.

التحكم في الوصول: يتضمن تسجيل بيانات جميع الزوار، وتوفير بطاقات تعريف إلكترونية للعاملين، واستخدام وسائل تحقق بيومترية مثل بصمات الأصابع أو مسح قزحية العين (Al-Mashhadani & Al-Jumaili, 2023).

الوقاية من الكوارث الطبيعية: يتم تطبيق إجراءات مثل استخدام أجهزة كشف الحرائق، ونظام إطفاء أوتوماتيكي، وتوفير تهوية مناسبة لمنع ارتفاع درجات الحرارة التي قد تتسبب في تلف المعدات.

الفصل الثالث

عرض الإطار الميداني للبحث

بعد استعراض متغيرات البحث ضمن الإطار النظري، سيتم تحليل هذه المتغيرات من خلال النتائج المستخلصة باستخدام الأدوات الإحصائية المناسبة، التي تم تطبيقها على البيانات التي جُمعت من عينة البحث. يهدف هذا الفصل إلى تقديم تحليل شامل للبيانات وتفسيرها وفق الأساليب الإحصائية المعتمدة، ويتضمن أربعة مباحث رئيسية، وهي:

المبحث الأول : تقديم وصف تفصيلي لمجتمع البحث وعينته، مع توضيح خصائص العينة المختارة وأسس اختيارها.

المبحث الثاني : تحليل وصفي للبيانات المستخلصة، مع عرض النتائج بناءً على إجابات أفراد العينة وتفسيرها في سياق أهداف البحث.

المبحث الثالث : تقييم أداة قياس البحث من خلال فحص مدى صدقها وثباتها، والتأكد من ملاءمتها لقياس المتغيرات المدروسة.

المبحث الرابع : اختبار الفرضيات البحثية باستخدام الأساليب الإحصائية المناسبة، وتحليل مدى تحقق الفرضيات ومدى تأثير المتغيرات على بعضها البعض.

المبحث الاول

أولا: وصف مجتمع البحث وعينته

مجتمع البحث وعينته: يتكون مجتمع البحث من جميع الموظفين العاملين في مديرية بلديات محافظة نينوى والذين يبلغ عددهم (300) موظف، موزعين على عدة أقسام تشمل الوظائف الإدارية، المالية، والهندسية، بالإضافة إلى تخصصات أخرى مختلفة.

أما عينة البحث، فقد تم اختيارها بطريقة عشوائية، حيث شملت (35) موظفًا من العاملين في أقسام الموارد البشرية، الشؤون المالية، وقسم تكنولوجيا المعلومات، من مختلف التخصصات الأكاديمية والفئات العمرية. وقد تم توزيع أداة البحث (الاستبانة الورقية) على العينة المختارة، حيث كانت وحدة التحليل (الأفراد) سيتم تقديم تحليل لخصائص مجتمع البحث من خلال استعراض البيانات الديموغرافية لعينة الدراسة الموضحة في الجدول (1) والتي تم الحصول عليها من إجابات المشاركين في استمارة الاستبانة. وتشمل هذه البيانات مجموعة من الخصائص الأساسية للمبحوثين، والتي تم تصنيفها وفقًا لمتغيرات

متعددة، أبرزها النوع الاجتماعي، المستوى التعليمي، وعدد سنوات الخبرة، وذلك بهدف تقديم صورة واضحة عن التوزيع الديموغرافي للعينة المدروسة.

الجدول (1) البيانات الديموغرافية لعينة البحث

النوع الاجتماعي							
الذكور				الاناث			
العدد		النسبة		العدد		النسبة	
30		%85		5		%15	
التحصيل العلمي							
اعدادية		معهد		بكالوريوس		عليا	
العدد	النسبة	العدد	النسبة	العدد	النسبة	العدد	النسبة
3	8.6%	10	%28.6	20	%57.1	2	5.7%
الفئة العمرية							
25فاقل		35-25		45-36		45فاكثر	
العدد	النسبة	العدد	النسبة	العدد	النسبة	العدد	النسبة
2	5.7	5	9.4	22	62.8	6	17.1
الخدمة الوظيفية							
1-10 سنة		11-20سنة		21-30سنة			
5	%14.2	24	%68.5	6	%25.7		

ثانيا: تحليل البيانات الديموغرافية لعينة البحث:

النوع الاجتماعي: تشير نتائج الجدول (1) إلى أن نسبة الذكور في العينة تفوق نسبة الإناث، حيث بلغ عدد الذكور (30) موظفًا، ما يعادل (85%) من إجمالي العينة، بينما بلغ عدد الإناث (5) موظفات. مما يعكس هيمنة الذكور على استخدام نظم المعلومات في المديرية.

المؤهل العلمي: يوضح الجدول أن الغالبية العظمى من أفراد العينة يحملون شهادة البكالوريوس، حيث بلغ عددهم (20) موظفًا، ما يمثل (57.1%) من إجمالي العينة. مما يشير إلى توافق مؤهلاتهم الأكاديمية مع طبيعة العمل في مجال أمن المعلومات.

الفئة العمرية: يتبين من الجدول أن الفئة العمرية (36-45 عامًا) هي الأكثر تمثيلًا ضمن العينة، حيث بلغ عدد الموظفين في هذه الفئة (22) موظفًا، بنسبة (62.8%). مما يدل على أن معظم المشاركين يتمتعون بخبرة متوسطة، ويمتلكون مهارات حديثة ومتطورة في مجال أمن المعلومات.

الجدول (2) قياس معامل الثبات ومدى الاتساق بين مكونات القياس

الابعاد	عدد العبارات	قيمة الفا كرونباخ
البعد الاول	8	0.69
البعد الثاني	7	0.23
البعد الثالث	11	0.79
المجموع	26	0.60

تحليل النتائج، يشير الجدول إلى أن قيمة معامل ألفا كرونباخ الإجمالية بلغت (0.60)، مما يدل على مستوى ثبات وموثوقية مقبولة للاستبيان، وبالتالي صلاحية الأداة البحثية للاستخدام في الدراسة.

ثانيا: التحليل الوصفي وعرض النتائج وفق إجابات العينة

يهدف هذا القسم إلى تحليل واقع المتغيرات المستقلة في الدراسة، والمتمثلة بـ طبيعة التهديدات (التهديدات المادية، البرمجية، والتنظيمية) والحماية المطبقة (الحماية المادية والبرمجية)، وتأثيرها على المتغير التابع وهو أمن المعلومات. ويعتمد التحليل على حساب المتوسط الحسابي والانحراف المعياري لكل بُعد من أبعاد البحث بناءً على إجابات العينة المبحوثة.

البعد الأول: أمن المعلومات:

الجدول (3)

المتوسطات الحسابي والانحراف المعياري لاستجابات المبحوثين حول متغيرات البحث الخاصة بأمن المعلومات

رقم العبارة	العبارة	الوسط الحسابي	الانحراف المعياري
1	الادارة العليا واعية ومحسسة بما يكفي بطبيعة التهديدات التي تتعرض لها نظم المعلومات	3.91	0.781
2	الادارة العليا واعية بأهمية وضرورة توفير الامن لأنظمة المعلومات.	4.00	1.000
3	اجراءات الحماية التي تطبقها المؤسسة تواكب التغيرات الحاصلة في البيئة التكنولوجية.	3.91	0.702
4	المنظمة تخصص ميزانية خاصة لإدارة عملية امن المعلومات.	4.00	0.939
5	التكاليف التي تصرف على تطبيق امن المعلومات ضرورية وتساهم في حماية المنظمة وتطورها.	3.91	0.853
6	المنظمة تعتمد سياسة امنية مكتوبة ويعرفها الجميع.	3.69	0.832
7	الموظفون ذوي ثقافة امنية وواعون بمسؤولياتهم.	3.71	1.045
8	المنظمة تقوم بدورات تدريبية حول موضوع امن المعلومات.	3.91	0.781
	المجموع	3.88	0.492

يعكس هذا البعد واقع أمن المعلومات في المديرية ومدى تطبيقها له. ووفقًا للنتائج، يتضح أن درجة تطبيق المنظمة لأمن المعلومات جاءت بمتوسط حسابي (3.88) وانحراف معياري (0.492)، مما يشير إلى مستوى مقبول من الاهتمام بأمن المعلومات داخل المنظمة.

أعلى تقييم حصلت عليه العبارة (الإدارة العليا واعية بأهمية وضرورة توفير الأمن لأنظمة المعلومات) بمتوسط حسابي (4.00) وانحراف معياري (1.000)، مما يعكس إدراكا عاليا من قبل الإدارة العليا لأهمية أمن المعلومات في استمرارية العمل المؤسسي.

أدنى تقييم جاء للعبارة "المنظمة تعتمد سياسة أمنية مكتوبة ويعرفها الجميع" بمتوسط حسابي (3.69) وانحراف معياري (0.832)، مما يشير إلى قصور واضح في وضع سياسات أمنية مكتوبة يسهل الوصول إليها وفهمها من قبل جميع العاملين، وهو ما قد يؤثر على تنفيذ استراتيجيات الحماية بفعالية داخل المنظمة.

البعد الثاني: طبيعة التهديدات (المادية، البرمجية، التنظيمية)

يهدف هذا البعد إلى تحليل طبيعة التهديدات التي تواجه المنظمة، والتي تنقسم إلى تهديدات مادية، برمجية، وتنظيمية، وذلك بناءً على إجابات المبحوثين وتحليل المتوسط الحسابي والانحراف المعياري لكل من العبارات المتعلقة بهذا البعد.

الجدول (4)

المتوسط الحسابي والانحراف المعياري لاستجابات العينة حول طبيعة التهديدات

رقم العبارة	العبارة	الوسط الحسابي	الانحراف المعياري
1	التهديدات التي تتعرض لها المنظمة عبارة عن سرقة	3.29	0.825
2	التهديدات التي تتعرض لها المنظمة عبارة عن دخول غير مصرح به	3.14	1.00
3	التهديدات التي تتعرض لها المنظمة عبارة عن هندسة اجتماعية(تفتيش في المهملات , الخداع	3.63	1.140
4	لتهديدات التي تتعرض لها المنظمة عبارة عن برامج خبيثة : فيروسات....	3.60	1.168
5	التهديدات التي تتعرض لها المنظمة عبارة عن قرصنة معلوماتية	3.49	1.121
6	التهديدات التي تتعرض لها المنظمة ناتجة عن نقص في الكفاءات البشرية	3.57	1.065
7	التهديدات التي تتعرض لها المنظمة ناتجة عن ثغرات امنية في الانظمة والبرامج	3.89	1.065
	المجموع	3.51	0.441

تشير نتائج الجدول إلى أن متوسط طبيعة التهديدات التي تواجه المنظمة بلغ (3.51) بانحراف معياري (0.441)، مما يعكس وجود تهديدات أمنية بدرجة متوسطة إلى مرتفعة، تتنوع بين التهديدات المادية، البرمجية، والتنظيمية. أعلى تقييم حصلت عليه العبارة "التهديدات التي تتعرض لها المنظمة ناتجة عن ثغرات أمنية في الأنظمة والبرامج" بمتوسط حسابي (3.89) وانحراف معياري (1.065)، مما يشير إلى أن معظم المخاطر التي تهدد أمن المعلومات تعود إلى نقاط الضعف في الأنظمة التقنية المستخدمة، وهو ما قد ينتج عن عدم تحديث البرمجيات أو ضعف تطبيق سياسات الحماية الرقمية. أدنى تقييم حصلت عليه العبارة "التهديدات التي تتعرض لها المنظمة عبارة عن دخول غير مصرح به" بمتوسط حسابي (3.14) وانحراف معياري (1.00)، مما يدل على أن المنظمة تواجه تحديات في إدارة صلاحيات الوصول إلى المعلومات، مما قد يقلل من مستوى الحماية العام ويزيد من احتمالات التسريب أو سوء الاستخدام للمعلومات الحساسة. بناءً على النتائج، يمكن استنتاج أن التهديدات الأمنية التي تواجه المنظمة متعددة الأبعاد، مع تركيز واضح على التهديدات الناتجة عن الثغرات الأمنية في الأنظمة والبرمجيات. وهذا يشير إلى الحاجة إلى تعزيز سياسات الأمان الرقمي، وتحسين أنظمة الحماية المطبقة، بالإضافة إلى تدريب الكوادر البشرية على أحدث تقنيات الأمان السيبراني لتقليل المخاطر المحتملة وضمان استمرارية العمل بأمان وكفاءة.

البعد الثالث: طبيعة الحماية المطبقة في المنظمة (الحماية المادية والبرمجية)

يهدف هذا البعد إلى تحليل مستوى إجراءات الحماية المطبقة في المنظمة، سواء على المستوى المادي أو البرمجي، من خلال تقييم استجابات العينة المبحوثة وفقًا للمتوسط الحسابي والانحراف المعياري لكل عنصر متعلق بهذا البعد.

الجدول (5)

المتوسط الحسابي والانحراف المعياري لاستجابات العينة حول طبيعة الحماية المطبقة

رقم العبارة	العبارة	الوسط الحسابي	الانحراف المعياري
1	المنظمة تعتمد على كاميرات المراقبة لحماية الموقع والتجهيزات المادية.	3.51	0.919
2	المنظمة تعتمد على مراقبة الدخول عن طريق حمل شارات ومرافقة الزوار لمنع أي تجاوزات.	4.00	0.840
3	المنظمة تعتمد على كاشف حريق والاطفاء الالي لحماية موقعها.	3.71	0.957
4	المنظمة تعتمد على اجهزة الانذار عند أي تدخل غير مسموح.	3.66	1.259
5	المنظمة تعتمد على مضادات الفيروسات لحماية انظمتها المعلوماتية.	3.63	1.031
6	المنظمة تعتمد على الجدران النارية لحماية انظمتها المعلوماتية .	3.89	0.867
7	المنظمة تعتمد على برامج التشفير لكل البيانات والاتصالات والتطبيقات المتنقلة والمخزنة لحمايتها من التنصت.	3.43	1.195
8	المنظمة تعمل على انظمة كشف التدخل لحماية انظمتها المعلوماتية من أي دخول غير مصرح به .	3.60	1.143
9	المنظمة تعمل على تحديث برامج الحماية دوريا .	3.11	1.157
10	المنظمة تقوم باختبار انظمة الحماية دوريا لاكتشاف الثغرات.	3.43	1.290
11	تتم معالجة الثغرات فورا.	4.03	0.857
	المجموع	3.636	0.331

تشير نتائج الجدول إلى أن المنظمة تطبق إجراءات حماية مادية وبرمجية بدرجة متوسطة إلى مرتفعة، حيث بلغ المتوسط الحسابي العام (3.636) والانحراف المعياري (0.331)، مما يعكس اهتمام المنظمة بأمن المعلومات، لكن بمستويات متفاوتة بين مختلف أنواع الإجراءات الأمنية. أعلى تقييم حصلت عليه العبارة "تتم معالجة الثغرات فورًا" بمتوسط حسابي (4.03) وانحراف معياري (0.857)، مما يدل على وجود استجابة سريعة لمعالجة الثغرات الأمنية عند اكتشافها، وهو مؤشر إيجابي يعكس مرونة وكفاءة المنظمة في التصدي للمخاطر الأمنية. أدنى تقييم حصلت عليه العبارة "المنظمة تعمل على تحديث برامج الحماية دوريًا" بمتوسط حسابي (3.11) وانحراف معياري (1.157)، مما يشير إلى قصور في عملية تحديث الأنظمة الأمنية بانتظام، وهو ما قد يزيد من احتمالية تعرض المنظمة لهجمات إلكترونية بسبب الثغرات الأمنية غير المُعالجة. تعكس هذه النتائج مستوى متوسطًا من الحماية المطبقة داخل المنظمة، مع وجود نقاط قوة في سرعة معالجة الثغرات الأمنية، ونقاط ضعف في تحديث برامج الحماية بشكل دوري. وهذا يشير إلى الحاجة إلى تعزيز استراتيجيات الحماية من خلال اعتماد سياسات تحديث مستمرة للبرمجيات الأمنية، وتحسين آليات الحماية الاستباقية ضد الهجمات السيبرانية، لضمان بيئة معلوماتية أكثر أمانًا وموثوقية.

ثالثا: اختبار فرضيات الدراسة

يتناول هذا القسم تحليل واختبار فرضيات الدراسة التي تم تحديدها في البحث، بهدف التحقق من إمكانية قبولها أو رفضها، وذلك من خلال استخدام معامل الارتباط بيرسون. يهدف تحليل الارتباط إلى تحديد ما إذا كانت هناك علاقة ذات دلالة إحصائية بين المتغيرات المستقلة (طبيعة التهديدات، طبيعة الحماية المطبقة) والمتغير التابع (أمن المعلومات).

الجدول (6) نتائج اختبار فرضيات البحث

الفرضية	معامل الارتباط	المعنوية	T-TEST
الفرضية الرئيسة الاولى **توجد علاقة ارتباط ذو دلالة معنوية بين طبيعة التهديدات و امن المعلومات في المنظمة المبحوثة**	0.239	0.167	-422.128
الفرضية الرئيسة الثانية **توجد علاقة ارتباط ذو دلالة معنوية بين طبيعة الحماية المطبقة و امن المعلومات في المنظمة المبحوثة**	0.44**	0.008	-559.788

من تحليل نتائج الاختبار نرى:

الفرضية الأولى: علاقة طبيعة التهديدات بأمن المعلومات: تشير نتائج التحليل إلى أن قيمة معامل الارتباط بلغت (0.239) عند مستوى معنوية (0.167)، وهي أعلى من مستوى الدلالة المعتمد (0.05). وهذا يشير إلى عدم وجود علاقة ارتباط ذات دلالة معنوية بين طبيعة التهديدات وأمن المعلومات في المنظمة المبحوثة، مما يؤدي إلى رفض الفرضية الأولى. وهذا يعني أن التهديدات المختلفة التي تواجه المنظمة لا ترتبط بشكل مباشر أو قوي بأمن المعلومات، ما قد يشير إلى وجود عوامل أخرى مؤثرة لم يتم أخذها في الاعتبار.

الفرضية الثانية: علاقة طبيعة الحماية المطبقة بأمن المعلومات: بالنسبة للفرضية الثانية، تشير النتائج إلى أن قيمة معامل الارتباط (0.44)، وهي دالة إحصائيًا عند مستوى معنوية (0.008)، حيث إنها أقل من (0.05)، مما يعني وجود علاقة ارتباط ذات دلالة معنوية بين طبيعة الحماية المطبقة وأمن المعلومات. وبهذا يتم قبول الفرضية الثانية، أي أن الإجراءات الأمنية المطبقة في المنظمة، سواء كانت مادية أو برمجية، تلعب دورًا مهمًا في تحسين أمن المعلومات وتقليل المخاطر المحتملة. تشير نتائج التحليل إلى أن طبيعة التهديدات لا ترتبط بشكل مباشر بأمن المعلومات، في حين أن الحماية المطبقة تلعب دورًا رئيسيًا في تحقيق أمن المعلومات في المنظمة المبحوثة. وبذلك، يمكن التركيز مستقبلاً على تعزيز استراتيجيات الحماية الأمنية، سواء من خلال تحديث الأنظمة الأمنية أو تطوير السياسات الأمنية الداخلية لضمان حماية المعلومات من التهديدات المتزايدة.

الفصل الرابع: الاستنتاجات والتوصيات

يهدف هذا الفصل إلى تقديم مجموعة من الاستنتاجات التي تم التوصل إليها بناءً على تحليل البيانات المستخلصة من إجابات عينة البحث، وذلك من خلال استخدام الأساليب الإحصائية المناسبة. كما يتضمن الفصل التوصيات التي يمكن أن تساعد المنظمة في تحسين مستوى أمن المعلومات لديها ومعالجة المشكلات التي تم تحديدها خلال البحث.

المبحث الأول: الاستنتاجات

توصل البحث إلى مجموعة من الاستنتاجات المتعلقة بواقع أمن المعلومات في المنظمة المبحوثة، والتي يمكن تلخيصها فيما يلي:

1. إدراك الإدارة العليا لأهمية أمن المعلومات: أظهرت النتائج أن الإدارة العليا في المنظمة المبحوثة على دراية ووعي بأهمية أمن المعلومات ودوره في دعم العمليات الإدارية داخل المنظمة.
2. غياب سياسة أمنية واضحة: بالرغم من هذا الإدراك، إلا أن المنظمة لا تعتمد سياسة أمنية مكتوبة وواضحة، مما يؤدي إلى ضعف في وعي الموظفين بأهمية أمن المعلومات وتأثيره على بيئة العمل.
3. انخفاض مستوى الوعي بأمن المعلومات بين الموظفين: تبين أن هناك ضعفًا في الثقافة الأمنية لدى الموظفين، مما ينعكس على عدم إعطائهم أهمية كافية لموضوع أمن المعلومات داخل المنظمة.
4. عدم تأثر الأمن المعلوماتي بالتهديدات المادية والبرمجية والتنظيمية: تشير النتائج إلى أن أمن المعلومات في المنظمة لا يتأثر بشكل مباشر بالتهديدات المادية والبرمجية، نظرًا لوجود حلول تقنية لمواجهتها، ولكن هذه الحلول تبقى غير فعالة دون إدارة فاعلة ومتابعة مستمرة.
5. تأثير الحماية المطبقة على مستوى الأمن المعلوماتي: كلما زاد مستوى الحماية المادية والبرمجية المطبقة في المنظمة، زاد مستوى أمن المعلومات وتحسن بشكل ملحوظ.
6. أهمية الحماية البرمجية: تعتبر الحماية البرمجية من العوامل الأساسية المؤثرة في أمن المعلومات، حيث تلعب برامج مكافحة الفيروسات والجدران النارية دورًا أساسيًا في حماية الأنظمة.
7. عدم الاهتمام بتحديث برامج الحماية الدورية: رغم أن المنظمة تقوم بمعالجة الثغرات الأمنية فور وقوعها، إلا أنها لا تتابع تحديث برامج الحماية بشكل منتظم، مما يجعلها عرضة للاختراقات الأمنية.
8. الاعتماد على تقنيات الحماية الأساسية: تعتمد المنظمة على الجدران النارية، وبرامج مكافحة الفيروسات، ونظم كشف التسلل، بالإضافة إلى أنظمة الحماية من الحرائق، مما يساعد في تأمين المعلومات لديها.
9. عدم مراقبة الأشخاص المصرح لهم بالوصول إلى المعلومات: يظهر أن المنظمة لا تولي اهتمامًا كافيًا لمراقبة المستخدمين المصرح لهم بالوصول إلى المعلومات، مما يزيد من احتمالية تعرضها لسرقة البيانات أو انتهاك الخصوصية.

المبحث الثاني : التوصيات

1. بناءً على النتائج المستخلصة، يمكن تقديم مجموعة من التوصيات التي تساهم في تعزيز أمن المعلومات في المنظمة المبحوثة وتحسين إجراءات الحماية، ومنها:
2. تعزيز الوعي والثقافة الأمنية لدى الموظفين: يجب تغيير النمط التقليدي للعمل والانفتاح على التطورات التكنولوجية من خلال تنظيم دورات تدريبية تهدف إلى تعزيز الثقافة الأمنية، بحيث يصبح أمن المعلومات جزءًا من ثقافة المنظمة وليس مجرد إجراءات شكلية.
3. وضع واعتماد سياسة أمنية مكتوبة: يجب على المنظمة تبني سياسة أمنية واضحة ومكتوبة، مما يسهل تطبيق الإجراءات الأمنية، بالإضافة إلى تسهيل عملية المراقبة والمحاسبة في حالة حدوث أي خرق أمني.
4. متابعة المستخدمين المصرح لهم بالدخول إلى المعلومات: يجب مراقبة الأشخاص الذين لديهم صلاحية الوصول إلى المعلومات الحساسة، وتحديد هوياتهم وصلاحياتهم بدقة، مع تعيين مسؤولين مختصين بمتابعة هذه التصاريح لضمان عدم تسريب البيانات أو استغلالها بشكل غير مشروع.
5. تحديث برامج الحماية بشكل دوري: من الضروري أن تقوم المنظمة بتحديث أنظمة الحماية والبرمجيات الأمنية بشكل منتظم لمواجهة التهديدات الجديدة وسد أي ثغرات أمنية محتملة قد تؤثر على أمن المعلومات.
6. تعزيز مهارات الموظفين في التعامل مع أمن المعلومات: ينبغي توفير برامج تدريبية متخصصة للموظفين حول كيفية التعامل مع المعلومات وحمايتها، مما يساهم في تقليل الأخطاء البشرية التي قد تؤدي إلى خروقات أمنية.
7. تعزيز الحماية البرمجية: يجب التركيز على تعزيز الحماية البرمجية نظرًا لارتباطها الوثيق بأمن المعلومات، وذلك من خلال استخدام برامج موثوقة لمكافحة الفيروسات والجدران النارية وتقنيات التشفير لضمان حماية البيانات والمعلومات الحساسة من التهديدات السيبرانية.

المصادر

المصادر العربية:

أولا: الكتب:

1-ابو مغايض، يحيى بن محمد، (2004)، "الحكومة الالكترونية: ثورة على العمل الاداري التقليدي", مكتبة العبيكان، الرياض.

2- القحطاني، ذيب بن عايض، (2015)، " امن المعلومات"، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض.

3-حسين، اسامة سمير، (2011)، "الاحتيال الالكتروني- الاسباب والحلول"، الجنادرية للنشر والتوزيع، الطبعة الاولى، عمان.

4- سيكاران، أومأ، (2009)، "طرق البحث في الادارة مدخل لبناء المهارات البحثية", دار المريخ للنشر، مصر.

ثانيا: الرسائل والاطاريح:

1- الجعبري، هناء يوسف ابراهيم، (2020)، "اثر الامن المعلوماتي على اداء شركات التامين العاملة في فلسطين، رسالة ماجستير، كلية الدراسات العليا، جامعة الخليل، فلسطين.

1- رابحي، عزيزة، (2019)،" الاسرار المعلوماتية وحمايتها ", اطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، الجزائر.

2- صورية، بوراية، (2016)، " قواعد الامن المعلوماتي ", دراسة مقارنة، اطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليابس، الجزائر.

3- الدنف، ايمن محمد فارس، (2013)، "واقع ادارة امن نظم المعلومات في الكليات التقنية بقطاع غزة وسبل تطويرها ", رسالة ماجستير، كلية التجارة، جامعة غزة، فلسطين.

4- مقراني، قدور، (2016)،" تقييم مدى مساهمة امن نظم المعلومات الالكتروني في الحد من مخاطر نظم المعلومات _ دراسة حالة مؤسسة اتصالات الجزائر، رسالة ماجستير، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، الجزائر.

ثالثا: المجلات:

1- احمد، اميرة محمد محمد سيد، (2021)،"استراتيجيات مكافحة الجرائم الالكترونية في العصر المعلوماتي تعزيزا لرؤية مصر ", مجلة البحوث الاعلامية، كلية الاعلام، جامعة الازهر، العدد (58)، المجلد (4).

2- الزين، غدير برنس، الخرابشة، عبد الكريم عودة، (2021)، "الجرائم الالكترونية ومستوى الوعي بخطورتها – دراسة ميدانية على عينة من الشباب الجامعي الاردني ", مجلة الجامعة الاسلامية للعلوم الانسانية، العدد (2)، المجلد (29).

3- بطيخ، حاتم احمد محمد، (2021)، "تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات", مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات، العدد (1)، المجلد (7).

- بلجراف، سامية، كلاس، خلود، (2017)، "الادارة الالكترونية واشكالية الامن المعلوماتي ", مجلة الناقد للدراسات السياسية، العدد (1).

5- بن يحيى، ام كلثوم حكوم ومحمد، حصة، (2020)،" الانشطة الطلابية ودورها في حماية من مخاطر التضليل الالكتروني طالبات جامعة الملك خالد (انموذجا)", مجلة الجامعة الاسلامية للدراسات التربوية والنفسية، العدد (28)، المجلد (2).

6- محسين، حاتم ناهي، حمود، عواد كاظم، (2015)، "تقويم نظام ادارة امن المعلومات في دائرة تكنولوجيا المعلومات وفق المواصفة ISO 27001-"، المجلة العراقية للعلوم والتكنولوجيا، العدد (6)، المجلد (2).

7- خضر، كمال فتحي، المداح، سمر وصفي علي، (2020)،"العلاقة بين الاقتصاد الرقمي وامن المعلومات – دراسة تطبيقية على عينة من عملاء البنك الاهلي المصري ", المجلة العلمية للاقتصاد والتجارة، العدد(1) , المجلد (5).

8- الشوابكة، عدنان عواد (2019)، "دور اجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات في جامعة الطائف ", مجلة العربية في العلوم الانسانية والاجتماعية، العدد (1)، المجلد (26).

9- عبد الحميد، عائشة، (2020)، "دور جهاز الدفاع الوطني في تحقيق الامن المعلوماتي في ظل تنامي الاجرام السيبراني ", المجلة العربية للمعلوماتية وامن المعلومات، العدد (1)، المجلد (1).

رابعا: الملتقيات والمؤتمرات:

1- البدانة، دياب موسى، (2014)، "الجرائم الالكترونية: المفهوم والاسباب "، الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، الاردن.

المصادر الاجنبية:

1. Alcaraz, C., & Zeadally, S. (2021). Critical infrastructure protection: Requirements and challenges for the 21st century. **Computers & Security, 110**, 102402. https://doi.org/10.1016/j.cose.2021.102402
2. Al-Mashhadani, W. H., & Al-Jumaili, H. H. (2023). **Assessing Cybersecurity Awareness: A survey study at the College of Administration and Economics – University of Mosul**. **NTU Journal for Management and Social Sciences**, 13(1), 174–186. https://journals.ntu.edu.iq/index.php/NTU-JMS/article/view/1282
3. Alotaibi, B. M., Alshammari, T. M., & Alotaibi, M. F. (2023). Cybersecurity awareness and practices in the digital era: A survey of information security readiness in Saudi organizations. **Journal of Information Security and Applications, 72**, 103509. https://doi.org/10.1016/j.jisa.2023.103509

Alqahtani, F., & Kavakli, E. (2023). A framework for enhancing cybersecurity resilience in government sectors: Case study from Saudi Arabia. **Journal of**

1. **Information Security and Applications, 71**, 103502. https://doi.org/10.1016/j.jisa.2023.103502
2. Brown, T., Ahmed, S., & Patel, R. (2023). Applying SPSS in public sector research: Methods, challenges, and insights. **Journal of Public Administration Research and Theory, 33**(1), 77–92. https://doi.org/10.1093/jopart/muac045
3. Directive sur la sécurité de l'information gouvernementale. (2014). **Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement**, chapitre G-1.03, a.20. Décret 7-2014, Conseil du trésor, Québec.
4. Gupta, B., Abd-El-Atty, B., & Hassanien, A. E. (2024). Cybersecurity in the era of digital transformation: Challenges and research opportunities. **Journal of Network and Computer Applications, 216**, 103745. https://doi.org/10.1016/j.jnca.2023.103745
5. Jean-Marc Royer. (2012). **Sécurité informatique des entreprises: Enjeux, menaces, prévention et parade**. Éditions ENI.
6. Jones, M., & Chen, Y. (2024). The role of data analytics in evaluating organizational cybersecurity effectiveness. **International Journal of Information Management, 74**, 102603. https://doi.org/10.1016/j.ijinfomgt.2023.102603
7. Kim, H., Lee, S., & Park, Y. (2023). Advanced cybersecurity strategies for mitigating digital threats in modern enterprises. **Computers & Security, 127**, 103066. https://doi.org/10.1016/j.cose.2023.103066
8. Khlaif, S. A., Fathi, S. A., & Majeed, S. S. (2023). Availability extent of human engineering elements in business organizations: An analytical study of the opinions of a sample of leaders in Badoosh Cement Factory. NTU Journal for Administrative and Human Sciences, 3(3), Article 559. https://doi.org/10.56286/ntujahs.v3i3.559
9. Kumar, R., & Singh, A. (2023). Cybersecurity challenges in the era of digital transformation: Emerging threats and countermeasures. **Computers & Security, 126**, 103078. https://doi.org/10.1016/j.cose.2022.103078
10. Laudon, K. C., & Laudon, J. P. (2005). **Management information systems** (6th ed.). Prentice Hall International.

11. NIST. (2002). **Risk management guide for information technology systems** (SP 800-30). U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
12. Sharma, A., Chen, L., & Sheth, A. (2022). Toward practical implementation of cybersecurity policies: Challenges and frameworks. **IEEE Transactions on Services Computing, 15**(6), 3430–3442. https://doi.org/10.1109/TSC.2021.3119253
13. Smith, R., Liu, H., & Martinez, J. (2022). Integrating theoretical frameworks in cybersecurity research: A systematic review. **Computers & Security, 114**, 102589. https://doi.org/10.1016/j.cose.2021.102589
14. Stallings, W. (2020). **Effective cybersecurity: A guide to using best practices and standards**. Addison-Wesley Professional.
15. Tian, Y., Peng, M., & Zhang, K. (2022). Trends and challenges in information security for smart cities: A review. **IEEE Internet of Things Journal, 9**(18), 16914–16930. https://doi.org/10.1109/JIOT.2022.3168457
16. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. **Computers & Security, 38**, 97–102. https://doi.org/10.1016/j.cose.2013.04.004
17. Whitman, M., & Mattord, H. (2011). **Principles of information security** (4th ed.). Cengage Learning.