AL KUT JOURNAL OF ECONOMIC AND ADMINISTRATIVE SCIENCES
Publisher: College of Economics and Management - Wasit University

أثر تقنيات الأمن السيبراني في تعزيز أمن المعلومات الفندقية دراسة تطبيقية

لفنادق الدرجة الأولى في العاصمة العراقية- بغداد

The Impact of Cybersecurity Technologies on Enhancing Hotel Information Security: An Applied Study of First-Class Hotels in the Capital of Iraq – Baghdad

أ.م.د. حسن عودة غضاب

الجامعة التقنية الوسطى- الكلية التقنية الادارية- بغداد

Assoc. Prof. Hassan Odah Ghdaab

Middle Technical University – Technical College of Management - Baghdad

hassan85@mtu.edu.iq

المستخلص:

هدفت الدراسة الحالية إلى التعرف على تقنيات الأمن السيبراني والمتمثلة بـــــــــــ(أمن الشبكات ، أمن البيانات، أمن الاجهزة الطرفية، أمن التطبيقات، أمن البريد الالكتروني) في تعزيز أمن المعلومات الفندقية في المنظمات الفندقية، وقد هدفت الدراسة التعرف على مدى إدراك المنظمات المبحوثة لمفهوم تقنيات الأمن السيبراني ، وقد استعمل المنهج الوصفي التحليأتي، إذ اختير عينة مكونه من (70) من الموظفين الذين يعملون في المنظمات الفندقية المبحوثة في العاصمة العراقية- بغداد والمتمثلة بـــــــــــ**(فندق فلسطين ميرديان- فندق عشتار شيراتون- فندق بابل روتانا).** و**توصلت الدراسة إلى عدد من الاستنتاجات أبرزها:** الاختلافات بين الأبعاد: على الرغم من أن جميع الأبعاد كانت مؤثرة، فإن هناك تبايناً في قوة التأثير، على سبيل المثال، أمن الشبكات وأمن البريد الإلكتروني هما الأبعاد الأكثر تأثيراً، في حين كان لأمن البيانات وأمن الأجهزة الطرفية تأثير أقل نسبياً.

الكلمات المفتاحية: الأمن السيبراني ، تقنيات الأمن السيبراني، أمن المعلومات الفندقية.

Abstract:

The aim of the current study was to identify cybersecurity technologies, which include (network security, data security, endpoint security, application security, and email security), and their role in enhancing hotel information security in hospitality organizations. The study also aimed to assess the level of awareness of the surveyed organizations regarding the concept of cybersecurity technologies. The descriptive analytical approach was used, and a sample of 70 employees working in the surveyed hospitality organizations in Baghdad, Iraq, was selected. These organizations included (Palestine Meridien Hotel, Ishtar Sheraton Hotel, and Babylon Rotana Hotel). The study reached several conclusions, the most prominent of which were: Differences between the dimensions: Although all dimensions had an impact, there were variations in the strength of the effect. For example, network security and email security were the most influential dimensions, while data security and endpoint security had a relatively lower impact.

Keywords: Cybersecurity, Cybersecurity Technologies, Hotel Information Security.

المقدمة:

في ظلّ التطور التكنولوجي المتسارع وانتشار استعمال الإنترنت في جميع مجالات الحياة اليومية، أصبحت المنظمات الفندقية تعتمد بشكل متزايد على نظم المعلومات الإلكترونية لتقديم خدماتها المتنوعة مثل الحجز الإلكتروني، والدفع الرقمي، وإدارة البيانات الخاصة بالزبائن. ومع هذه الاعتمادية العالية على تكنولوجيا المعلومات، تزايدت التهديدات الإلكترونية التي قد تؤثر سلباً في سرية البيانات وأمان المعلومات الحساسة. من هنا تبرز أهمية تقنيات الأمن السيبراني بوصفها أداة رئيسة لحماية هذه الأنظمة من الهجمات الإلكترونية التي قد تؤدي إلى اختراق البيانات أو تعطيل الخدمات المقدمة للزبائن.

وفي العصر الرقمي الحديث، أصبح الأمن السيبراني أحد الركائز الأساسية في المنظمات الفندقية للحفاظ على سلامة الأنظمة المعلوماتية وحماية البيانات الحساسة من الاختراقات والهجمات الإلكترونية. وقد شهد القرن الحادي والعشرون ثورة جديدة أعقبت ثورة تكنولوجيا المعلومات والاتصالات التي اتسم بها القرن العشرون، وتُعرف هذه الثورة بالثورة السيبرانية، التي تُعدّ الميدان الخامس للصراع البشري بعد الأرض والبحر والجو والفضاء.

وأدّت ثورة المعلومات وتطور شبكاتها العالمية إلى عولمة القطاع السياحي والفندقي من خلال التوسّع في تطبيق نظم السياحة الإلكترونية، التي تعتمد بصورة مكثفة على توافر البيانات والمعلومات، التي أصبحت تشكّل البنية التحتية التي تمكّن المنظمات الفندقية من أداء مهامها. إذ تمّ هيكلة البحث في أربعة محاور؛ تضمن المحور الأول منهجية الدراسة، بينما جاء المحور الثاني لبيان الجانب النظري، أما المحور الثالث فقد تناول الجانب العملي، وأخيراً جاء المحور الرابع ليسلّط الضوء على الاستنتاجات والتوصيات.

المحور الأول / منهجية الدراسة

أولاً: مشكلة الدراسة

في ظلّ الاعتماد المتزايد على تكنولوجيا المعلومات في صناعة السياحة والفنادق، أصبح أمن المعلومات أحد أبرز التحديات التي تواجه الفنادق على مستوى العالم، ولا سيما في الدول التي تمرّ بمرحلة تطور في قطاعها الرقمي مثل العراق؛ إذ يتزايد تهديد الهجمات السيبرانية التي تستهدف المنظمات الفندقية، بما في ذلك فنادق الدرجة الأولى في العاصمة بغداد، مما يعرّض بيانات الزبائن والمعلومات الحساسة لخطر كبير.

وتتنوّع التهديدات السيبرانية بين هجمات اختراق أنظمة المعلومات، وبرمجيات الفدية، والهجمات الموجّهة لسرقة البيانات المالية، أو حتى تعطيل الأنظمة الإلكترونية. ومن هنا برزت مشكلة الدراسة، التي يمكن تمثيلها بالآتي:

ما مدى تأثير تقنيات الأمن السيبراني في تعزيز أمن المعلومات الفندقية؟

ثانياً: أهمية الدراسة:

تتجلى أهمية هذه الدراسة في مناقشة موضوع مهم قد يؤدي التغاضي عنه إلى حدوث مشكلات عديدة وأضرار بالغة، ألا وهو حماية أنظمة المعلومات الخاصة بالمنظمات المبحوثة من جرائم الإنترنت والأنشطة الإجرامية السيبرانية؛ وذلك من خلال استثمار ما يُعرف بالأمن السيبراني لمواجهة هذه الهجمات غير المشروعة التي تستهدف الاستيلاء على المعلومات والبيانات التي تشملها هذه الأنظمة.

إذ أصبح مفهوم الأمن السيبراني مؤخراً تحدياً كبيراً في نمو السياحة العالمية، خاصة مع انتشار السياحة الرقمية والسياحة الذكية، والتوسع الهائل في تطبيق أنظمة الحجز الإلكتروني وفي جميع جوانب صناعة السياحة والفنادق، فضلاً عن أنّه المفتاح في عملية تطوير وتسويق وترويج وإدارة المواقع السياحية والفنادق في الوقت الحالي.

كما استمدت الدراسة أهميتها من الدور الذي يلعبه الأمن السيبراني وأثره في تحقيق الميزة التنافسية، بوصفه أحد المرتكزات المهمة في زيادة القدرة التنافسية للمنظمات الفندقية. وعليه يمكن تحديد أهمية الدراسة من خلال ما يأتي:

توضيح مدى إدراك الإدارات الفندقية لأهمية الأمن السيبراني في المنظمات المبحوثة.

المساهمة في تكوين نظام معرفي حول مدى تطبيق الإدارات الفندقية لأنظمة الأمن السيبراني.

توضيح مدى قدرة الإدارات الفندقية على التعامل مع الأمن السيبراني بفاعلية وكفاءة عالية في إدارة المنظمات المبحوثة.

تُعدّ الدراسة من الدراسات الحديثة في مجال البحوث العلمية المتعلقة بالأمن السيبراني الفندقي.

ثالثاً: أهداف الدراسة:

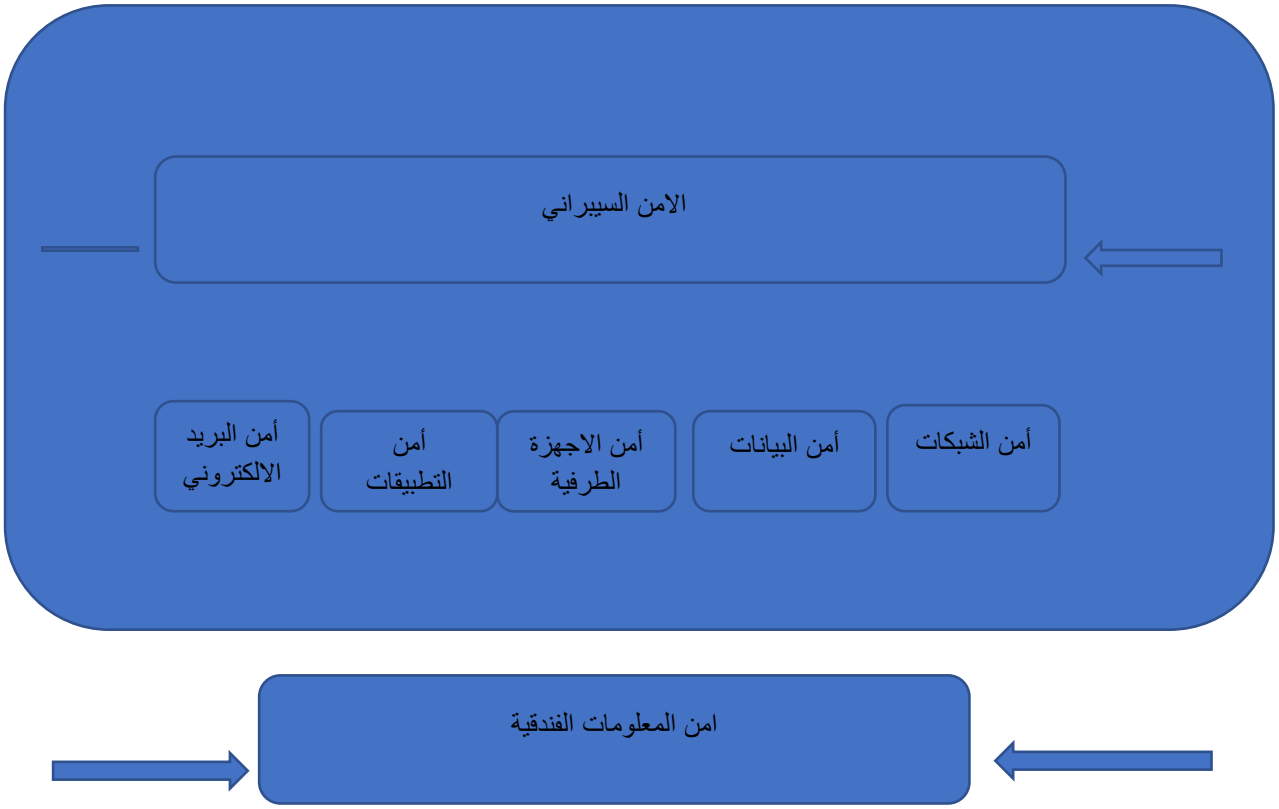
تهدف الدراسة إلى تحقيق جملة من الأهداف، أهمها:

التعرّف على مدى إدراك المنظمات المبحوثة لمفهوم الأمن السيبراني.

التعرّف على تقنيات الأمن السيبراني وأهميتها في المنظمات المبحوثة.

رابعاً: أنموذج الدراسة المقترح:

يتضمن أنموذج الدراسة الآتي:



شكل (1) أنموذج الدراسة المقترح

خامساً: فروض الدراسة:

لتحقيق أهداف الدراسة تم صياغة الفرضية الآتية:

الفرضية الرئيسة الأولى: توجد علاقة تأثير موجبة ذات دلالة معنوية بين تقنيات الأمن السيبراني وأمن المعلومات الفندقية. وتنبثق عنها الفرضيات الاتية:

1. هناك علاقة احصائية بين أمن الشبكات وأمن المعلومات الفندقية.
2. هناك علاقة احصائية بين أمن البيانات وأمن المعلومات الفندقية .
3. هناك علاقة احصائية بين أمن الاجهزة الطرفية وأمن المعلومات الفندقية .
4. هناك علاقة احصائية بين أمن التطبيقات وأمن المعلومات الفندقية .
5. هناك علاقة احصائية بين أمن البريد الالكتروني وأمن المعلومات الفندقية .

سادساً: منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليأتي لغرض اختبار نموذجها وفرضياتها؛ وذلك بدراسة وتحديد العلاقة والاثر بين متغيراتها من خلال جمع البيانات ذات العلاقة بالمنظمات المبحوثة ميدان الدراسة، وعليه فيما يأتي أهم الخطوات التي اعتمدت في ذلك:

- **أساليب جمع البيانات:** جُمعت المعلومات الخاصة بالدراسة من خلال:

1. **المصادر العربية والأجنبية، فضلاً عن الدوريات والرسائل والأطاريح الجامعية التي لها علاقة بموضوع الدراسة.**
2. **استمارة الاستبيان:** أعدت الاستبانة في ضوء الرؤية العلمية المتحققة من خلال استطلاع المصادر العلمية والمتمثلة بالجدول الاتي:

وصف متغيرات الدراسة في الاستبانة (1)

ت	المتغيرات الرئيسية	المتغيرات الفرعية	تسلسل الفقرات في الاستمارة	عدد الفقرات	مصادر القياس
الاول	تقنيات الأمن السيبراني	أمن الشبكات	X1-X4	4	الرفيعي، 2025 علي، 2024 أمير، 2023
		أمن البيانات	X5-X8	4	
		أمن الاجهزة الطرفية	X9-X12	4	
		أمن التطبيقات	X13-X16	4	
		أمن البريد الالكتروني	X17-X20	4	
الثاني	أمن المعلومات الفندقية		Y21-Y30	10	بن قيدة، 2025 رشيدة ورحاب، 2024 مرزوق وإجلال، 2023

المصدر: اعداد الباحث في ضوء استمارة الاستبانة

استعمل مقياس ليكرت (Likert) الخماسي في تحديد درجة لكل فقرة وتندرج من (اتفق بشدة، اتفق، محايد، لا اتفق، لا اتفق بشدة)، ويعد من المقاييس الذي يتميز بالدقة والمرونة لتحديد مستوى الاتفاق مع فقرات الاستبانة ، وما كان بين ذلك (محايد) فأنه يعبر عن الاعتدال والوسطية لمتغيرات الدراسة.

والجدول الاتي يوضح اوزان الفقرات:

جدول (2) أوزان مقياس ليكرت (Likert) الخماسي

الإجابة	اتفق بشدة	اتفق	محايد	لا اتفق	لا اتفق بشدة
الوزن	5	4	3	2	1

المصدر: اعداد الباحث

سابعاً: حدود الدراسة: وتتحدد الدراسة الحالية بحدود وكالاتي:

1- **الحدود المكانية:** تتمثل الحدود المكانية للدراسة بالمنظمات الفندقية في العاصمة العراقية – بغداد والمتمثلة بـ **(فندق فلسطين ميرديان- فندق عشتار شيراتون- فندق بابل روتانا).**

2- **الحدود الزمانية للدراسة:** لقد أنجزت عملية جمع البيانات وانجاز الإطار النظري للدراسة ما بين 2025/8/2 م ولغاية 2025/11/24 م.

3- **الحدود البشرية للدراسة:** تتمثل الحدود البشرية للدراسة بالقيادات الادارية والموظفين في المنظمات المبحوثة.

المحور الثاني: الجانب النظري للدراسة:

أولاً: الأمن السيبراني

مفهوم الأمن السيبراني

هو مجموعة من الإجراءات والممارسات المصممة لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تهدف عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها أو ابتزاز المال من المستخدمين (منصور، 2022: 45). ويرى (أميرن، 2023: 173) أنه الحدّ من خطر الهجمات الضارة على برامج وأجهزة الحاسوب والشبكات من خلال استعمال أدوات كشف الاختراقات، ووقف أنشطة الفيروسات، ومنع الدخول غير المصرح به، وتأكيد الهويات، وتمكين الاتصالات المشفرة. وأضاف (علي، 2024: 173) أنه ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. ويرى (الرفيعي، 2025: 260–261) أنه مجموعة من الوسائل التقنية والتنظيمية والإدارية التي تستعمل لمنع الاستعمال غير المصرح به وسوء الاستغلال، بالإضافة إلى استعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات المرتبطة بها، بهدف ضمان استمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية، مع اتخاذ جميع الإجراءات اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

وفي ضوء المفاهيم السابقة يمكن تحديد المفهوم الإجرائي للأمن السيبراني في المنظمات الفندقية بأنه مجموعة الإجراءات التقنية والإدارية التي تتضمن القواعد والعمليات والآليات التي يتم اتخاذها لمنع أي تدخل مقصود أو غير مقصود أو سوء استغلال فيما يتعلق بنظم المعلومات والاتصالات في المنظمة الفندقية، وضمان تأمين وحماية وسرية وخصوصية البيانات الشخصية للزبائن.

2 .أهمية الأمن السيبراني: أصبح الأمن السيبراني إحدى أهم الأولويات التي تعتني بها مختلف أطياف المجتمع، في الوقت الذي أصبح فيه الإنترنت أحد الضروريات الحيوية لكل من الأفراد والحكومات والمؤسسات والمنظمات. ومن ثمّ برزت أهمية توفير الحماية من عمليات الاحتيال عبر الإنترنت أو سرقة الهوية، إلى جانب حماية المعلومات المالية التي

قد يؤثر اختراقها في الوضع المالي للأفراد والمؤسسات، في ظل ما تعانيه تلك الجهات من تحديات عديدة، منها محدودية الموارد وضعف مهارات الأمن السيبراني (كريمة، 2024: 156).

وتتمثل أهمية الأمن السيبراني في (فهمي وخضير وآخرون، 2025: 22)، و(منصور، 2021: 226)، و(الهزاني، 2023: 80)، و(سراج، 2022: 204) فيما يأتي:

أ- قدرته على مكافحة الهجمات والمخاطر السيبرانية، سواء كانت مقصودة أم غير مقصودة، والسعي للتصدي لأضرارها وآثارها السلبية ومحاولة معالجتها.

ب- التغلب على التهديدات التي قد تنتج عن إيقاف تكنولوجيا المعلومات والاتصالات.

ت- مقاومة المخاطر الناتجة عن استعمال تكنولوجيا المعلومات والاتصالات بطريقة غير سليمة.

ث- تأمين قواعد البيانات والحفاظ على النظم المعلوماتية والشبكات، وحماية الأجهزة ضد الأنشطة الإلكترونية غير المشروعة ومنع دخول غير المخولين إلى أنظمة المعلومات.

3 .تقنيات الأمن السيبراني في المنظمات الفندقية:

تتضمن مجموعة متنوعة من العمليات التي تستهدف تحقيق الأمن السيبراني في المنظمات الفندقية، وتشمل الأنواع الآتية:

أ- أمن الشبكات:

يُعد أمن الشبكات أحد أهم جوانب الأمن السيبراني، خصوصاً في قطاع الضيافة، حيث تعتمد الفنادق بشكل كبير على الأنظمة المتصلة بالإنترنت لإدارة العمليات اليومية مثل الحجوزات والدفع الإلكتروني وخدمة الإنترنت للنزلاء (Jain & Pal, 2017, p.791).

ب- أمن البيانات:

يُعنى بحماية المعلومات الحساسة من السرقة أو التلف أو الوصول غير المصرح به. وفي بيئة الفنادق يُعد تأمين بيانات الضيوف، مثل الأسماء وأرقام جوازات السفر وبطاقات الائتمان وسجل الإقامة، أمراً بالغ الأهمية لما له من تأثير مباشر في سمعة الفندق وثقة العملاء (الطويسي وزهري، 2023: 274).

ت- أمن الأجهزة الطرفية:

يمثل خط الدفاع الأول ضد التهديدات السيبرانية التي قد تستهدف أجهزة الحاسوب والهواتف المحمولة وأجهزة نقاط البيع والأجهزة الذكية الأخرى المستخدمة في الفندق.

ث- أمن التطبيقات:

هو حماية البرمجيات، سواء كانت تطبيقات ويب أو تطبيقات هاتف محمول أو أنظمة داخلية، من التهديدات الإلكترونية عبر تصميمها واختبارها وتشغيلها بطريقة أمن ة تحمي البيانات والوظائف من الاستغلال أو الاختراق، وهو جانب حاسم في الأمن السيبراني، خاصة في الفنادق التي تعتمد على تطبيقات متعددة لإدارة الحجوزات والدفع الإلكتروني وعلاقات الضيوف وخدمات الغرف عبر تطبيقات الهاتف المحمول أو المواقع الإلكترونية (السمحان، 2020: 14).

ج- أمن البريد الإلكتروني:

هو مجموعة من السياسات والتقنيات التي تهدف إلى حماية أنظمة البريد الإلكتروني في الفندق، ويُعد أحد أهم مكونات الأمن السيبراني، خصوصاً في بيئة الفنادق التي تستعمل البريد الإلكتروني للتواصل مع الضيوف والموردين وشركاء الأعمال، ومع ذلك يُعد البريد الإلكتروني من أكثر القنوات المستخدمة في الهجمات الإلكترونية مثل التصيّد الاحتيالي والبرمجيات الخبيثة (الجنفاوي، 2021: 85).

ثانياً: أمن المعلومات الفندقية

1. مفهوم أمن المعلومات

يُعرَّف أمن المعلومات بأنه مجموعة من السياسات والإجراءات والتدابير التقنية والإدارية المصممة لحماية البيانات من الوصول غير المصرح به أو التلاعب أو الفقدان أو التهديدات الأمن ية المختلفة (سلطان، 2025: 242).

ويرى (رشيد ورحاب، 2024: 24) أنه حماية المعلومات وعناصرها الحساسة، بما فيها الأنظمة والأجهزة التي تستعمل لتخزين المعلومات ومعالجتها ونقلها. وأضاف (مرزوق وإجلال، 2024: 25) أنه توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها من خلال توفير الأدوات والوسائل اللازمة لحمايتها وفق معايير وإجراءات تمنع وصولها إلى أشخاص غير مخولين. ويرى (مورد، 2023: 66) أنه استعمال إجراءات وتدابير مختلفة لضمان الحماية اللازمة لجميع البرامج والأنظمة المستخدمة لمعالجة المعلومات، بوصفها من الموارد والمزايا الرئيسة التي ينبغي على المنظمات الفندقية والبنوك الحفاظ عليها. وفي ضوء المفاهيم السابقة يمكن تحديد المفهوم الإجرائي لأمن المعلومات الفندقية بأنه يشير إلى الجهود والتدابير التي تتخذها المنظمات الفندقية لحماية المعلومات الشخصية وبيانات الزبائن من التهديدات الإلكترونية والاختراقات، بما يضمن سلامة المعلومات وسرية البيانات واستمرارية العمليات الفندقية.

2 .أهمية أمن المعلومات في المنظمات الفندقية:

أ- حماية البيانات الحساسة للزبائن:

تهدف إلى حماية المعلومات الشخصية والمالية مثل الأسماء وأرقام جوازات السفر وبيانات الاتصال ومعلومات بطاقات الائتمان؛ إذ تُعد هذه البيانات من الأصول الحيوية التي يجب تأمينها ضد الاختراق أو التسريب؛ لأن أي خرق للبيانات قد يؤدي إلى فقدان ثقة الزبائن وتعريض الفندق لمسؤوليات قانونية وأضرار مادية ومعنوية. لذلك تعتمد الفنادق على تقنيات تشفير قوية وإجراءات مصادقة متعددة وأنظمة مراقبة متقدمة لضمان سرية المعلومات وخصوصيتها.

ب- ضمان استمرارية الأعمال الفندقية:

يُعد الحفاظ على استمرارية العمليات التشغيأتية هدفاً جوهرياً لأمن المعلومات في القطاع الفندقي؛ إذ قد تتسبب الهجمات الإلكترونية، مثل الفيروسات، في تعطيل أنظمة الحجز والدفع الإلكتروني، مما يؤدي إلى توقف الخدمة وخسائر مالية كبيرة. ومن خلال تطبيق حلول أمن ية فعالة مثل أنظمة النسخ الاحتياطي وخطط الاستجابة للطوارئ واختبارات الجاهزية السيبرانية، تضمن الفنادق استمرار تقديم خدماتها للنزلاء دون انقطاع (الجنفاوي، 2021: 87).

ت- منع الوصول غير المصرح به:

يهدف إلى منع أي محاولات دخول غير قانونية إلى الأنظمة أو البيانات المحمية، ويشمل ذلك حماية الشبكات الداخلية وأنظمة الحجز والبيانات المالية والمعلومات الشخصية للنزلاء. ويتم ذلك عبر استعمال الجدران النارية(Firewalls) ، وأنظمة كشف التسلل(IDS/IPS) ، وآليات المصادقة متعددة العوامل(Multi-Factor Authentication) ، مع تحديد صلاحيات المستخدمين بوضوح لضمان وصول المصرح لهم فقط.

ث- الامتثال للوائح القانونية والتنظيمية:

يُعدّ الامتثال للأنظمة والقوانين المحلية والدولية من الركائز الأساسية لأمن المعلومات في المنظمة الفندقية؛ إذ تفرض هذه اللوائح على الفنادق اتخاذ تدابير محددة لحماية خصوصية البيانات وضمان سلامتها، ولا سيما عند التعامل مع معلومات النزلاء المالية والشخصية. ومن أبرز هذه التشريعات: اللائحة العامة لحماية البيانات (GDPR) في الاتحاد الأوروبي، ومعايير أمن بيانات بطاقات الدفع (PCI-DSS) التي تُلزم الفنادق بحماية بيانات بطاقات الائتمان. ويسهم الالتزام بهذه المعايير في تجنب الغرأمات والعقوبات القانونية؛ فضلاً عن تعزيز ثقة العملاء والشركاء (الخضيري وآخرون، 2020: 222).

ج- الحفاظ على السمعة:

تُعدّ السمعة من أهم الأصول غير الملموسة في القطاع الفندقي؛ إذ يعتمد نجاح الفندق بدرجة كبيرة على ثقة الزبائن. وقد يؤدي أي خرق أمن ي أو تسريب للمعلومات إلى فقدان هذه الثقة وترك أثر سلبي طويل الأمد في الصورة العامة للفندق. لذلك يُعدّ الأمن السيبراني أداة استراتيجية لحماية السمعة الفندقية من خلال الوقاية من الحوادث الرقمية، والاستجابة السريعة والفعّالة لها عند حدوثها، فضلاً عن الشفافية في إدارة الأزمات، الأمر الذي يعزز القدرة التنافسية ويسهم في جذب العملاء الجدد.

ح- كشف التهديدات والاستجابة لها بفاعلية:

يُعدّ الكشف المبكر عن التهديدات والاستجابة الفعّالة لها من العناصر الأساسية في حماية الأنظمة الفندقية؛ إذ قد تتطور الهجمات الإلكترونية بسرعة وتُحدث أضراراً كبيرة خلال وقت قصير إذا لم يتم التعامل معها فوراً. ولهذا تعتمد المنظمات الفندقية على أنظمة مراقبة ذكية وتحليلات سلوكية لرصد الأنشطة غير الطبيعية، فضلاً عن أنظمة إنذار فورية تُمكّن فرق الأمن من اتخاذ إجراءات سريعة. كما أعدت خطط استجابة للحوادث تتضمن خطوات واضحة للتعامل مع

التهديدات وتقليل الأضرار واستعادة الأنظمة في أسرع وقت ممكن، الأمر الذي يعزز استقرار العمليات ويحمي سمعة الفندق.

خ- تأمين شبكات الإنترنت العامة والخاصة داخل الفندق:

تُعدّ شبكات الإنترنت في الفنادق، سواء المخصصة للضيوف أم للاستعمال الداخلي، أهدافاً محتملة للهجمات الإلكترونية، مما يجعل تأمينها أمراً بالغ الأهمية. إذ يمكن للمخترقين استغلال الثغرات في الشبكات العامة — مثل شبكات الواي فاي الخاصة بالزبائن — للوصول إلى بيانات المستخدمين أو اختراق الأنظمة الداخلية. ولتفادي ذلك تعمل الفنادق على فصل الشبكات العامة عن الشبكات الخاصة، واستخدام تقنيات تشفير قوية، وجدران حماية، وأنظمة كشف التسلل. كما يتم تقييد الوصول إلى الشبكات الداخلية وتحديد مستويات الصلاحيات للمستخدمين، بما يضمن بيئة رقمية أمن ة لكل من الموظفين والنزلاء.

د- تدريب الموظفين على الممارسات الأمن ية:

يُعدّ الموظفون خط الدفاع الأول ضد التهديدات في المنظمات الفندقية؛ إذ تمثل الأخطاء البشرية أحد الأسباب الرئيسة للاختراقات الأمن ية. لذلك تركّز برامج أمن المعلومات على توعية العاملين وتدريبهم على أفضل الممارسات الأمن ية، مثل التعرف على رسائل التصيّد الاحتيالي، والتعامل الأمن مع كلمات المرور، وعدم فتح الروابط أو المرفقات المشبوهة. كما يتم تدريبهم على كيفية التعامل الصحيح مع البيانات الحساسة والالتزام بسياسات الأمن المعتمدة داخل الفندق. ويسهم هذا التدريب المستمر في تعزيز الثقافة الأمن ية وتقليل احتمالات وقوع الحوادث السيبرانية الناتجة عن الخطأ البشري (السمحان، 2020: 12)

3. خصائص أمن المعلومات في المنظمات الفندقية:

فقد ذكر كل من (السمحان،12:2020) ، (ربيعى وسمر،182;2022) . أن أمن المعلومات لا بد أن تتسم ببعض الخصائص:

أ- **النزاهة:** وتعنى عدم السماح بالعبث بالبيانات أو التعديل عليها إلا من قِبل الأشخاص المصرح لهم بذلك، لأن تبادل المعلومات باستعمال الفضاء الإلكتروني يجعلها أكثر عرضة للتلاعب بها والتغيير فيها بواسطة الأشخاص والهيئات الأخرى.

ب- **توافر المعلومات وإتاحتها:** وتعنى امكانية وصول وحصول المستخدمين (المصرح لهم فقط) على المعلومات التي يحتاجونها فى أي وقت وبصورة أمن ة.

ت- **الأصالة:** ويقصد بها التحقق من حقيقة الأفراد الذين يتعاملون مع المعلومات أو يتبادلونها لضمان عدم التعرض لأي تهديدات سيبرانية من قِبل قراصنة يدعون إنهم جهات فعلية وموثوقة.

ث- **عدم التنصل (عدم الإنكار):** وتعنى إسناد وتسجيل المعاملات والانشطة التي تتم عبر الفضاء الرقمي للأطراف والجهات التي قامت بها بشكل فعلي، حتى يتم إثبات هذه المعاملات في حالة إنكار الجهة لأنشطتها، وتعد هذه الخاصية من الخصائص التي لا يتم الاهتمام بها بصورة فعالة عند تحديث الأمن السيبرانى وتصميمه.

ج- **تكامل وسلامة المعلومات:** وذلك يعنى أن أمن المعلومات يساعد في الحفاظ على وحماية ما تحتويه الشبكات المعلوماتية من معلومات وبيانات من أي تغيير قد يطرأ عليها ومن التعديل أو الحذف أو إضافة أي معلومات أخرى على

هذا المحتوى الخاص بهذه الشبكات فهو لا يقبل بأي مما سبق ذكره إلا إنه يسمح بذلك من لدن المؤهلين والمتخصصين القائمين على الإشراف على هذه الشبكات ومحتواها.

ح- **السرية والموثوقية:** أي أن أمن المعلومات يقوم على تأمين المعلومات وحمايتها من السرقة عن طريق عدم إعطاء الأذن ومنع كافة الأشخاص الغير متخصصين أو الغير مخول لهم من الوصول إلى المعلومات أو الاطلاع على الشبكات المعلوماتية، وإنما يسمح للمتخصصين والمشرفين على هذه الشبكات المعلوماتية والأشخاص المخول لهم فقط بالدخول والحصول على المعلومات بعد التأكيد عليهم بضرورة عدم مشاركتها مع الاشخاص غير المتخصصين أو غير المخول لهم وضرورة عدم تسريبها لهم بأي شكل.

خ- **الاستمرارية:** ويقصد بها توفير وإتاحة الخدمات بشكل مستمر ومنتظم دون توقف.

المحور الثالث: الجانب العملي

أولا: عرض النتائج وتحليلها:

أ. **وصف افراد عينة الدراسة:**

بهدف التعرف على خصائص وسمات افراد عينة الدراسة فقد شمل وصف عينة الدراسة الفقرات المبنية في الجدول (2) وكما يأتي:

جدول (2) وصف افراد عينة الدراسة

المتغير	الفئة	التكرار	النسبة
النوع الاجتماعي	ذكر	45	% 64.28
	انثى	25	%35.71
	المجموع	70	%100
العمر	اقل من 30 سنة	21	30
	30-اقل 40 سنة	35	50
	40- اقل 50 سنة	14	20
	50 سنة فأكثر	-	-
	المجموع	70	%100
المؤهل العلمي	أعدادي	8	%11.42
	دبلوم	4	%5.71

	بكالوريوس	45	%64.28
	دبلوم عالي	6	%8.57
	ماجستير	4	%5.71
	دكتوراه	3	%4.28
	المجموع	70	%100
حسب المنصب	بدون مصب (الموظفين)	58	%82.85
	منصب	4	%5.71
	مدير	12	%17.14
	المجموع	70	%100

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

من الجدول (2) نلاحظ ما يأتي:

- فيما يخص غالبية النوع الاجتماعي العينة كانت من الذكور اذ بلغت النسبة المئوية لهم64.28 %، ، بينما بلغت نسبة الاناث 35.71%.
- فيما يخص العمر كانت اقل من 30 سنة اذ بلغت النسبة المئوية لهم30، بينما 30-اقل 40 سنة بلغت النسبة المئوية لهم50، في حين 40- اقل 50 سنة بلغت النسبة لهم20، أما 50 سنة فأكثر فكانت النسبة هي- .
- أما المؤهل العلمي كانت اعدادي النسبة المئوية لهم11.42% ، في حين بلغت النسبة المئوية لـــــــــــ الدبلوم5.71%، في حين كانت النسبة المئوية للبكلوريوس64.28%، أما الدبلوم العالي فكانت النسبة المئوية لهم8.57%، أما الماجستير فكانت النسبة المئوية لهم5.71% ، في حين الدكتوراه بلغت النسبة المئوية لهم 4.28%.
- فيما يخص المنصب بلغت النسبة المئوية للموظفين الذين لا يمتلكون منصب82.85% ، أما النسبة المئوية للذين يمتلكون منصب5.71% ، في حين بلغت النسبة المئوية للذين في موقع مدير17.14%.

ب. وصف وتشخيص متغيرات الدراسة على مستوى المنظمات المبحوثة: يركز هذا الجزء من الجانب الميداني على وصف وتشخيص متغيري الدراسة وكما موضح أدناه:

1. **وصف وتشخيص تقنيات الأمن السيبراني:** اعتمدت الدراسة لقياس تقنيات الأمن السيبراني في المنظمات المبحوثة على خمسة مكونات تمثلت بـ (أمن الشبكات، أمن البيانات ، أمن الاجهزة الطرفية، أمن التطبيقات، أمن البريد الالكتروني) ، وكما موضحة في الجدول (3)

الجدول (3) يبين إجابات المبحوثين والوسط الحسابي والانحراف المعياري ومعامل الاختلاف في العينة المبحوثة

السؤال	لا اتفق بشدة	لا اتفق	محايد	اتفق	اتفق تمأما	المتوسط	الانحراف المعياري	معامل الاختلاف
1	22	2	0	38	8	3.11	1.518	48.81
2	0	24	6	12	28	3.63	1.321	36.39
3	22	2	18	5	23	3.07	1.645	53.58
4	0	25	20	2	23	3.33	1.271	38.16
أمن الشبكات x1						3.2857	1.32990	40.47
5	22	2	15	2	29	3.20	1.725	53.91
6	0	25	15	4	26	3.44	1.315	38.23
7	22	7	13	2	26	3.04	1.706	56.12
8	0	30	14	2	24	3.29	1.331	40.45
أمن البيانات x2						3.2429	1.40970	43.47
9	22	9	13	2	24	2.96	1.681	56.79
10	1	31	9	3	26	3.31	1.399	42.26
11	23	6	8	3	30	3.16	1.783	56.42
12	1	28	8	4	29	3.46	1.411	40.78
أمن الاجهزة الطرفية x3						3.2214	1.49488	46.40
13	23	3	12	4	28	3.16	1.742	55.12
14	0	23	10	6	31	3.64	1.341	36.84
15	24	3	9	8	26	3.13	1.744	55.71
16	0	23	5	28	14	3.47	1.151	33.17

أمن التطبيقات x4							**3.3500**	**1.38404**	**41.31**
17	**22**	**0**	**9**	**17**	**22**	**9**	**3.24**	**1.654**	**51.05**
18	**0**	**22**	**17**	**9**	**22**	**9**	**3.44**	**1.235**	**35.90**
19	**22**	**3**	**15**	**8**	**22**	**8**	**3.07**	**1.645**	**53.58**
20	**2**	**23**	**15**	**4**	**26**	**4**	**3.41**	**1.357**	**39.79**
أمن البريد الالكتروني x5							**3.2929**	**1.35866**	**41.26**
الأمن السيبراني x							**3.2786**	**1.29516**	**39.50**

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

من خلال النتائج أعلاه تبين بان متوسط إجابة محور **الأمن السيبراني** x بلغ 3.2786 وبانحراف معياري 1.29516 ومعامل اختلاف مستوى بلغ 39.50 أما على المحاور الفرعية التابعة للمحور **الأمن السيبراني** فكان متوسط إجابة محور **أمن الشبكات** 3.2857 وانحراف معياري 1.32990 ومعامل الاختلاف 40.47 وقد حصلت الفقرة الثانية على اقل معامل الاختلاف بلغ 36.39 بمتوسط 3.63 وبانحراف معياري بلغ 1.321 أما متوسط إجابة **أمن البيانات** فكان 3.2429 وانحراف معياري 1.40970 ومعامل الاختلاف43.47 وقد حصلت الفقرة السادسة على اقل معامل الاختلاف بلغ 38.23 بمتوسط 3.44 وبانحراف معياري بلغ 1.315 أما متوسط إجابة **أمن الاجهزة الطرفية** فكان 3.2214 وانحراف معياري 1.49488 ومعامل الاختلاف 46.40 وقد حصلت الفقرة الثانية عشر على اقل معامل الاختلاف بلغ 40.78 بمتوسط 3.46 وبانحراف معياري بلغ 1.411 أما متوسط إجابة **أمن التطبيقات** فكان 3.3500 وانحراف معياري 1.38404 ومعامل الاختلاف 41.31 وقد حصلت الفقرة السادسة عشر على اقل معامل الاختلاف بلغ 33.17 بمتوسط 3.47 وبانحراف معياري بلغ 1.151 أما متوسط إجابة **أمن البريد الالكتروني** فكان 3.2929 وانحراف معياري 1.35866 ومعامل الاختلاف 41.26 وقد حصلت الفقرة الثأمن ة عشر على اقل معامل الاختلاف بلغ 35.90 بمتوسط 3.44 وبانحراف معياري بلغ 1.235 أما اعلى معامل اختلاف فقد حصلت عليه الفقرة التاسعة والتابعة الى **محور أمن الاجهزة الطرفية** اذ بلغ 56.79 بمتوسط 2.96 وبانحراف معياري 1.681.

2. وصف وتشخيص أمن المعلومات الفندقية:

الجدول (4) يبين إجابات المبحوثين والوسط الحسابي والانحراف المعياري ومعامل الاختلاف في العينة المبحوثة

السؤال	**لا اتفق بشدة**	**لا اتفق**	**محايد**	**اتفق**	**اتفق تمأما**	**المتوسط**	**الانحراف المعياري**	**معامل الاختلاف**
1	**0**	**22**	**0**	**36**	**12**	**3.54**	**1.112**	**31.41**

2	**0**	**22**	**5**	**12**	**31**	**3.74**	**1.315**	**35.16**
3	**22**	**5**	**19**	**11**	**13**	**2.83**	**1.494**	**52.79**
4	**1**	**25**	**22**	**5**	**17**	**3.17**	**1.204**	**37.98**
5	**22**	**2**	**24**	**4**	**18**	**2.91**	**1.549**	**53.23**
6	**0**	**29**	**20**	**1**	**20**	**3.17**	**1.251**	**39.46**
7	**22**	**7**	**21**	**3**	**17**	**2.80**	**1.538**	**54.92**
8	**1**	**32**	**18**	**6**	**13**	**2.97**	**1.167**	**39.29**
9	**26**	**10**	**14**	**7**	**13**	**2.59**	**1.527**	**58.95**
10	**0**	**28**	**21**	**7**	**14**	**3.10**	**1.144**	**36.90**
أمن المعلومات الفندقية y						**3.0829**	**1.15645**	**37.51**

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

من خلال الجدول أعلاه نلاحظ محور أمن المعلومات الفندقية، فقد حصل على متوسط بلغ 3.0829 بانحراف معياري 1.15645 وبمعامل اختلاف 37.51 وقد حصلت الفقرة الأولى على اقل معامل اختلاف بلغ 31.41 بمتوسط 3.54 وبانحراف معياري بلغ 1.112 أما اعلى معامل اختلاف، فقد حصلت علية الفقرة التاسعة، فقد بلغ 58.95 بمتوسط 2.59 وبانحراف معياري 1.527.

ثانيا: اختبار فرضيات الدراسة:

أ. علاقات الارتباط:

جدول رقم 5 يبين معاملات الارتباط بين متغيرات البحث

الأمن السيبراني x	أمن البريد الالكتروني x5	أمن التطبيقات x4	أمن الاجهزة الطرفية x3	أمن البيانات x2	أمن الشبكات x1	اسم المتغير
0.688**	0.772**	0.687**	0.633**	0.634**	0.712**	أمن المعلومات الفندقية y

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

نلاحظ من الجدول أعلاه

- بلغ معامل الارتباط 0.712** الذي يعني أن هناك علاقة معنوية بدرجة عالية وبثقة 99% بين أمن الشبكات x1 وبعد أمن المعلومات الفندقية y
- بلغ معامل الارتباط **0.634 الذي يعني ان هناك علاقة معنوية بدرجة عالية وبثقة 99% بين أمن البيانات x2 وبعد أمن المعلومات الفندقية y .
- بلغ معامل الارتباط **0.633 الذي يعني ان هناك علاقة معنوية بدرجة عالية وبثقة 99% بين أمن الاجهزة الطرفية x3 وبعد أمن المعلومات الفندقية y .
- بلغ معامل الارتباط **0.687 الذي يعني ان هناك علاقة معنوية بدرجة عالية وبثقة 99% بين أمن التطبيقات x4 وبعد أمن المعلومات الفندقية y .
- بلغ معامل الارتباط **0.772 الذي يعني ان هناك علاقة معنوية بدرجة عالية وبثقة 99% بين أمن البريد الالكتروني x5 وبعد أمن المعلومات الفندقية y .
- بلغ معامل الارتباط **0.688 الذي يعني ان هناك علاقة معنوية بدرجة عالية وبثقة 99% بين الأمن السيبراني x وبعد أمن المعلومات الفندقية y .

ب. تحليل الانحدار :

اولا: تحليل الانحدار المحور الرئيسي للأمن السيبراني x وفروعه على محور أمن المعلومات الفندقية y :

جدول رقم 6 يبين اثر أمن الشبكات x1 على أمن المعلومات الفندقية y

المتغير المعتمد	معامل التحديد R^2	معامل الانحدار β	قيمة t المحسوبة	قيمة F المحسوبة	مستوى الدلالة P	طبيعة العلاقة
أمن المعلومات الفندقية y	0.685	0.720	12.166	148.014	0.000	العلاقة معنوية

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

من خلال الجدول أعلاه بلغ معامل التوضيح 0.685 مما يعني ان أمن المعلومات x1 تؤثر على بعد أمن المعلومات الفندقية y بنسبة 68.5% أما اختبار t فهو معنوي الاثر مما يعني ان معلمات النموذج هي ذات دلالة معنوية أما اختبار F فبلغت قيمة F المحسوبة 148.014 ويملك مستوى دلالة P التي هي 0.000 وهي أصفر من 0.05 مما يعني ان النموذج ذات دلالة معنوية.

جدول رقم 7 يبين اثر أمن البيانات x2 على أمن المعلومات الفندقية y

المتغير المعتمد	معامل التحديد R^2	معامل الانحدار β	قيمة t المحسوبة	قيمة F المحسوبة	مستوى الدلالة P	طبيعة العلاقة

أمن المعلومات الفندقية y	0.516	0.589	8.512	72.451	0.000	العلاقة معنوية

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

من خلال الجدول أعلاه بلغ معامل التوضيح 0.516 مما يعني أن أمن البيانات x2 تؤثر على بعد أمن المعلومات الفندقية y بنسبة 51.6% أما اختبار t فهو غير معنوي الاثر مما يعني ان معلمات النموذج هي ذات دلالة غير معنوية أما اختبار F، فبلغت قيمة F المحسوبة 72.451، ويملك مستوى دلالة P التي هي 0.000، وهي أصفر من 0.05 مما يعني ان النموذج ذات دلالة غير معنوية.

جدول رقم 8 يبين اثر أمن الاجهزة الطرفية x3 على أمن المعلومات الفندقية y

المتغير المعتمد	معامل التحديد R^2	معامل الانحدار β	قيمة t المحسوبة	قيمة F المحسوبة	مستوى الدلالة P	طبيعة العلاقة
أمن المعلومات الفندقية y	0.460	0.525	7.613	57.960	0.000	العلاقة معنوية

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

الجدول أعلاه بلغ معامل التوضيح 0.460 مما يعني ان أمن الاجهزة الطرفية x3 تؤثر على بعد أمن المعلومات الفندقية y بنسبة 46.0% أما اختبار t فهو معنوي الاثر مما يعني ان معلمات النموذج هي ذات دلالة معنوية أما اختبار F فبلغت قيمة F المحسوبة 57.960 ويملك مستوى دلالة P التي هي 0.000 وهي أصفر من 0.05 مما يعني ان النموذج ذات دلالة معنوية.

جدول رقم 9 يبين أمن التطبيقات x4 على أمن المعلومات الفندقية y

المتغير المعتمد	معامل التحديد R^2	معامل الانحدار β	قيمة t المحسوبة	قيمة F المحسوبة	مستوى الدلالة P	طبيعة العلاقة
أمن المعلومات الفندقية y	0.666	0.682	11.651	135.738	0.000	العلاقة معنوية

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

من خلال الجدول أعلاه بلغ معامل التوضيح 0.666 مما يعني ان أمن التطبيقات x4 تؤثر على بعد أمن المعلومات الفندقية y بنسبة 66.6% أما اختبار t فهو معنوي الاثر مما يعني ان معلمات النموذج هي ذات دلالة معنوية أما اختبار F فبلغت قيمة F المحسوبة 135.738 ويملك مستوى دلالة P التي هي 0.000 وهي أصفر من 0.05 مما يعني ان النموذج ذات دلالة معنوية.

جدول رقم 10 يبين اثر أمن البريد الالكتروني x5 على أمن المعلومات الفندقية y

المتغير المعتمد	معامل التحديد R^2	معامل الانحدار β	قيمة t المحسوبة	قيمة F المحسوبة	مستوى الدلالة P	طبيعة العلاقة
أمن المعلومات الفندقية y	0.719	0.722	13.202	174.294	0.000	العلاقة معنوية

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

من خلال الجدول أعلاه بلغ معامل التوضيح 0.719 مما يعني ان أمن البريد الالكتروني x5 تؤثر على بعد أمن المعلومات الفندقية y بنسبة 71.9% أما اختبار t فهو معنوي الاثر مما يعني ان معلمات النموذج هي ذات دلالة معنوية أما اختبار F فبلغت قيمة F المحسوبة 174.294 ويملك مستوى دلالة P التي هي 0.000 وهي أصفر من 0.05 مما يعني ان النموذج ذات دلالة معنوية.

جدول رقم 11 يبين اثر الأمن السيبراني x على أمن المعلومات الفندقية y

المتغير المعتمد	معامل التحديد R^2	معامل الانحدار β	قيمة t المحسوبة	قيمة F المحسوبة	مستوى الدلالة P	طبيعة العلاقة
أمن المعلومات الفندقية y	0.698	0.746	12.530	157.000	0.000	العلاقة معنوية

المصدر: من أعداد الباحث بالاعتماد على نتائج الحاسبة.

من خلال الجدول أعلاه بلغ معامل التوضيح 0.698 مما يعني ان الأمن السيبراني x يؤثر على بعد أمن المعلومات الفندقية y بنسبة 69.8% أما اختبار t فهو معنوي الاثر مما يعني ان معلمات النموذج هي ذات دلالة معنوية أما اختبار F فبلغت قيمة F المحسوبة 157.000 ويملك مستوى دلالة P التي هي 0.000 وهي أصفر من 0.05 مما يعني ان النموذج ذات دلالة معنوية.

المحور الرابع: - الاستنتاجات والتوصيات

اولا: الاستنتاجات:

1. الارتباط القوي بين الأبعاد المختلفة للأمن السيبراني وأمن المعلومات الفندقية: جميع الأبعاد الخمسة للأمن السيبراني (أمن الشبكات، أمن البيانات، أمن الأجهزة الطرفية، أمن التطبيقات، وأمن البريد الإلكتروني) أظهرت ارتباطاً إيجابياً مع أمن المعلومات الفندقية، حيث تراوحت معاملات الارتباط بين 0.633 و0.772، مما يدل على أن كل من هذه الأبعاد تؤثر بشكل معنوي في تعزيز أمن المعلومات الفندقية.

2. تفاوت في تأثير الأبعاد المختلفة للأمن السيبراني: من بين الأبعاد الخمسة، كان لأمن البريد الإلكتروني أكبر تأثير على أمن المعلومات الفندقية بنسبة 71.9%، يأتيه أمن الشبكات بنسبة 68.5%، مما يشير إلى أهمية توفير حماية قوية للبريد الإلكتروني والشبكات في البيئة الفندقية.
3. مستوى الأداء الحالي للأمن السيبراني:أظهرت نتائج الدراسة أن متوسط درجة تقييم الأمن السيبراني في المنظمات المبحوثة بلغ 3.2786، مع انحراف معياري يبلغ 1.29516، مما يعني أن هناك تبايناً ملحوظاً بين مستويات تطبيق تقنيات الأمن السيبراني في المؤسسات المختلفة، كما أن معامل الاختلاف المرتفع في بعض الأبعاد (مثل أمن الأجهزة الطرفية) يشير إلى تفاوت في الجهود المبذولة لتحسين أمن هذه الأبعاد.
4. علاقات معنوية بين المتغيرات: كانت جميع القيم المتعلقة بمستوى الدلالة (P) أقل من 0.05، مما يدل على أن جميع النماذج التي اختبرت (الارتباط والانحدار) هي ذات دلالة معنوية، مما يعني أن الأبعاد المختلفة للأمن السيبراني تؤثر فعلاً في أمن المعلومات الفندقية.
5. الاختلافات بين الأبعاد: رغم أن جميع الأبعاد كانت مؤثرة، إلا أن هناك تبايناً في قوة التأثير. على سبيل المثال، أمن الشبكات وأمن البريد الإلكتروني هما الأبعاد الأكثر تأثيراً، في حين كان لأمن البيانات وأمن الأجهزة الطرفية تأثير أقل نسبياً.
6. تشير النتائج الإحصائية إلى وجود علاقة ارتباط قوية وإيجابية وذات دلالة معنوية عالية بين الأبعاد الخمسة للأمن السيبراني (أمن الشبكات، أمن البيانات، أمن الأجهزة الطرفية، أمن التطبيقات، وأمن البريد الإلكتروني) وبين أمن المعلومات الفندقية، وكذلك بين الأمن السيبراني ككل وأمن المعلومات الفندقية، وكما يأتي:

أ. نتائج الارتباط والتأثير (الانحدار):

- أمن البريد الإلكتروني (x5): يمتلك أقوى معامل ارتباط وتأثير على أمن المعلومات الفندقية (0.772 ارتباط، 0.719 معامل تحديد R2)، مما يشير إلى أنه البعد الأكثر أهمية في التأثير على أمن المعلومات الفندقية.
- أمن الشبكات (x1): يظهر ارتباطاً قوياً وتأثيراً كبيراً (0.712 ارتباط، 0.685 معامل تحديد R2).
- الأمن السيبراني الكلي (x): يؤثر على أمن المعلومات الفندقية بنسبة% 69.8 (**0.688 ارتباط، 0.698 معامل تحديد R2)، وهذا يدل على أهمية تطبيق التقنيات الأمن ية بشكل شمولي.
- أمن التطبيقات (x4): يمتلك أيضاً تأثيراً قوياً (0.687 ارتباط، 0.666 معامل تحديد R2).
- أمن البيانات (x2): يمتلك ارتباطاً قوياً (0.634{**}) ويؤثر بنسبة % 51.6.
- أمن الأجهزة الطرفية (x3): يمتلك ارتباطاً قوياً 0.633 ويؤثر بنسبة % 46.0.

ب. **نتائج الوصف والتشخيص:**

- **محور الأمن السيبراني (x)**: بلغ متوسط الاستجابة الكلي 3.2786، وهو ما يميل إلى حد ما نحو "اتفق" (باعتبار مقياس ليكرت الخماسي).
- **محور أمن المعلومات الفندقية (y)**: بلغ متوسطه 3.0829، وهو يميل بشكل طفيف نحو "محايد".

- **أقل تشتتاً في الأمن السيبراني**: حصلت الفقرة المتعلقة بـ **أمن التطبيقات (الفقرة 16)** على أقل معامل اختلاف (33.17)، مما يشير إلى وجود أعلى مستوى من الاتفاق والتقارب في استجابات المبحوثين حول هذه النقطة.

- **أكثر تشتتاً في الأمن السيبراني**: حصلت الفقرة المتعلقة بـ **أمن الأجهزة الطرفية (الفقرة 9)** على أعلى معامل اختلاف (56.79)، مما يدل على تباين كبير في آراء المبحوثين حول هذه النقطة بالذات، وبمتوسط منخفض (2.96) يميل نحو "لا أتفق" أو "محايد".

- **أقل تشتتاً في أمن المعلومات الفندقية**: حصلت **الفقرة الأولى** على أقل معامل اختلاف (31.41) وأعلى متوسط (3.54)، مما يشير إلى اتفاق عالٍ حول هذه العبارة.

- **أكثر تشتتاً في أمن المعلومات الفندقية**: حصلت **الفقرة التاسعة** على أعلى معامل اختلاف (58.95) وأقل متوسط (2.59)، مما يدل على تباين كبير وعدم اتفاق حول هذه العبارة.

ثانيا: التوصيات:

1. تعزيز أمن البريد الإلكتروني والشبكات: نظراً لأن أمن البريد الإلكتروني وأمن الشبكات لهما أكبر تأثير على أمن المعلومات الفندقية، يجب أن تركز المؤسسات الفندقية على تعزيز أمان البريد الإلكتروني من خلال تقنيات مثل فحص الرسائل المزعجة، والتشفير، واستعمال المصادقة متعددة العوامل. كما ينبغي تعزيز حماية الشبكات من خلال استعمال جدران نارية قوية، وكشف التسلل، والرقابة على حركة مرور البيانات.
2. مراجعة وتطوير استراتيجيات أمن الأجهزة الطرفية: بما أن أمن الأجهزة الطرفية أظهر معامل اختلاف مرتفع، فمن المهم أن تقوم المنظمات الفندقية بتحديث وتحسين تقنيات الأمان الخاصة بالأجهزة الطرفية، مثل أجهزة الحاسوب المحمولة، الهواتف الذكية، والطابعات، التي قد تشكل نقطة ضعف في النظام الأمن ي، يجب التأكد من تثبيت تحديثات الأمان بانتظام واستعمال برامج مكافحة الفيروسات.
3. زيادة التدريب والتوعية: يجب أن تكون هناك برامج تدريبية دورية للعاملين في القطاع الفندقي لتعزيز فهمهم للمخاطر السيبرانية، تدريب الموظفين على أسس الأمن السيبراني، مثل التعامل مع البريد الإلكتروني المشبوه، واستعمال كلمات مرور قوية، وحماية البيانات الحساسة، يمكن أن يقلل من المخاطر الأمن ية بشكل كبير.
4. تحليل الأداء وتحسين التقنيات الحالية: يوصى بأن تقوم المنظمات الفندقية بتحليل أوجه القصور في تقنيات الأمان الحالية وتحديثها وفقاً للتطورات التكنولوجية والتهديدات المتزايدة، يتعين أن يتم تقييم فعالية أدوات الأمان بشكل دوري وتحديثها أو استبدالها إن لزم الأمر.
5. التفاعل مع الشركات المتخصصة في الأمن السيبراني: من أجل التأكد من تطبيق أفضل الممارسات في مجال الأمن السيبراني، يفضل التعاون مع شركات أمن ية متخصصة، يمكن لهذه الشركات تقديم استشارات ومراجعات دورية لأمان الأنظمة وتقديم حلول تقنية متطورة لحماية البيانات والمعلومات الفندقية.
6. **تعزيز وتأمين البريد الإلكتروني بشكل خاص (أولوية قصوى):** نظراً لأعلى معامل تأثير لـ "أمن البريد الإلكتروني"، يجب على المنشآت الفندقية الاستثمار بشكل مكثف في حلول متقدمة لتصفية البريد المزعج، وأنظمة الكشف عن التصيد الاحتيالي، وتطبيق سياسات صارمة لكلمات المرور وتدريب الموظفين على التعرف على رسائل البريد الإلكتروني المشبوهة.

7. **الاستثمار في أمن الشبكات والتطبيقات:** يجب مواصلة تعزيز أمن الشبكات وأمن التطبيقات، فهما من الأبعاد ذات التأثير العالي، يتضمن ذلك تحديث جدران الحماية، وأنظمة كشف ومنع الاختراقات، وإجراء اختبار اختراق منتظم للتطبيقات الفندقية (مثل أنظمة إدارة الممتلكات PMS وأنظمة الحجز).
8. **مراجعة سياسات أمن المعلومات الفندقية:** نظراً لأن متوسط أمن المعلومات الفندقية يميل للمحايدة، يجب على الإدارة العليا مراجعة وتحديث سياسات أمن المعلومات لتكون أكثر فاعلية وصرامة، وضمان التزام الموظفين بها، خاصة في الفقرات التي حظيت بأعلى تباين أو أقل اتفاق.

المصادر:

1. عبد الحميد منصور، 2022, "الأمن السيبراني: حماية الأنظمة الرقمية في العصر الحديث، ط 1، دار الفكر العربي، القاهرة، مصر.
2. أمير، نهى، 2023، الأمن السيبراني في استراتيجية الأمن القومي الروسي، بحث منشور في مجلة آفاق آسيوية، العدد 7، الجزء 11.
3. محمد، علي صباح، 2024، تحديات الأمن السيبراني على الاستقرار الأمن ي في العراق، بحث منشور في مجلة كلية دجلة الجامعة، المجلد 7، العدد 2.
4. الرفيعي، على محمد أمن يف،2025، الأمن السيبراني وتأثيره في مستقبل الهيمنة الامريكية، بحث منشور في مجلة تكريت للعلوم السياسية، المجلد 1، العدد 38.
5. كريمة، أحمد المختار السيد، 2024، دور الأمن السيبراني في مكافحة الفساد، بحث منشور في مجلة القرطاس، العدد الخامس والعشرين، المجلد الثاني.
6. السمحان، مني عبدالله، 2020، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، بحث منشور في مجلة كلية التربية، جامعة المنصورة، العدد 111.
7. ربيعي، حسين وسمر، محمود، 2022، الحروب السيبرانية: المخاطر واستراتيجيات تحقيق الأمن السيبراني الدولي والداخلي ،المجلة الجزائرية للأمن الإنساني ،المجلد 7, العدد 2.
8. الجنفاوي، خالد مخلف، 2021، التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الاكاديمية بالكويت، المجلة العربية للآداب والدراسات الانسانية، المجلد الخامس، العدد 19.
9. الخضري، جيهان سعد محمد وسلامي، هديل جبريل علي وكليبي، نعمة ناصر مدبش، 2020، الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية دراسة مقارنة، مجلة تطوير الاداء الجامعي، المجلد 12، العدد 1 .
10. مشوش، مراد، 2019، الجهود الدولية لمكافحة الأمن السيبراني، مجلة الواحات للبحوث والدراسات، المجلد 12، العدد 2.
11. الطويسي، محمد أحمد وزهري، محمد عبد الفتاح، 2023، دور الأمن السيبراني في تحقيق الميزة التنافسية لفنادق الخمس نجوم بمنطقة المثلث الذهبي بالأردن، مجلة كلية السياحة والفندقة، عدد 14.
12. Jain, J. & Pal, P. (2017): A Recent Study over Cyber Security and its Elements, International Journal of Advanced Research in Computer Science (India: Rajasthan, Janardan Rai Nagar Rajasthan Vidyapeeth, Vol.8, No. 3.

13. منصور، أمن ة محمد، 2021، تأثير الأمن السيبراني على الرقابة الداخلية وانعكاسها على الوحدة الاقتصادية، دراسة استطلاعية لأراء عينة من المدققين والمحاسبيين في وزارة التعليم العالي والبحث العلمي، Journal of Administration and Economics 127.

14. الهزاني، نورة بنت ناصر بن عبد الله، 2023، ضوابط ومتطلبات تطبيق الأمن السيبراني لحماية البيانات في جامعة الاميرة نورة، مجلة مكتبة فهد الوطنية، العدد الثأمن والعشرون.

15. سراج، شيماء أحمد محمد أحمد، 2022، التحليل البعدي لدراسات الأمن السيبراني في المجال التربوي، المجلة العربية للعلوم التربوية والنفسية، المؤسسة العربية للتربية والعلوم والآداب، المجلد 6، العدد 26.

16. بن قيدة، عبد الرؤوف، 2025، بناء نموذج تأثير العوامل التنظيمية على ثقافة أمن المعلومات في المنظمة الجزائرية، دراسة حالة منظمة أوريدو الجزائر، أطروحة مقدمة ضمن متطلبات نيل شهادة دكتوراه الطور الثالث في علوم التسيير، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، الجزائر .

17. رشيدة، عبدو رحاب، بلخضر، 2024، حفظ أمن المعلومات في ظل الذكاء الإصطناعي، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في الحقوق، جامعة محمد البشير الإبراهيمي – برج بوعريريج – الجزائر .

18. مرزوق، شيماء وإجلال، زين تركية، 2023، إنعكاسات الأمن السيبراني على أمن المعلومات في البنوك، مذكرة مقدمة لاستكمال متطلبات نيل شهادة ماستر أكاديمي، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، الجزائر.

19. سلطان، انعام عبد الجبار، 2025، واقع أمن المعلومات في مديرية بلديات محافظة نينوى دراسة مسحية لعينة من العاملين في مديرية بلدية محافظة نينوى، مجلة العلوم الاقتصادية، العدد ثمانية وسبعون، المجلد عشرون .

20. موارد، شايب محمد حمادي، 2023، تحديات المن السيبراني لأنظمة المعلومات في البنوك والمؤسسات المالية، مجلة إنارة للدراسات الإقتصادية، الإدارية والمحاسبية، المجلد الرابع، العدد الأول.

الاستبانة

المحور الأوّل: المعلومات التعريفية:-

ملاحظة : وضع علامة (✓) داخل المستطيل

1. النوع الاجتماعي : ذكر ☐ أنثى ☐
2. العمر : أقل من 35 سنة ☐ 36-45 سنة ☐ 46-55 سنة ☐ 56 فأكثر ☐
3. المؤهل العلمي : دبلوم ☐ بكالوريوس ☐ ماجستير ☐ دكتوراه ☐
4. حسب المنصب : بدون منصب ☐ منصب ☐

مدير

أولاً: المتغير المستقل تقنيات الأمن السيبراني:

ت	العبارات	لا اتفق تمأما	لا اتفق	محايد	اتفق	اتفق تمأما
أمن الشبكات:						
1	يعاني الفندق بشكل متزايد من هجمات الاختراق والاختر اقات السيبرانية التي تهدد سرية وسلامة المعلومات الفندقية					
2	تظل الفنادق عرضة للتهديدات السيبرانية نتيجة للثغرات المنية والهجمات المتطورة					
3	يطبق الفندق سياسات واجراءات لتحقيق المن الشامل للبيانات					
4	يواجه الفندق تحديات فريدة في مجال أمن المعلومات نتيجة لضرورة التوازن بين سهولة الوصول للزبئن وحماية البيانات					
أمن البيانات:						
5	الافتقار لاستعمال تقنيات الكشف المبكر والاستجابة الفعالة للحتفاظ على سلامة البيانات وثقة الزبئن					
6	توفير اجراءات للتعامل مع حوادث الأمان مثل اختراقات البيانات والاحتيال بما في ذلك خطط الطوارئ وإجراءات الاستجابة السريعة					
7	تبني آليات لتقييم وتحسين المان بناء على التهديدات الجديدة وتطورات التكنولوجيا					
8	توفير إطار قوي لمان المعلومات يسهم في تعزيز الثقافة المنية داخل الفندق مما يزيد من					

	وعي الموظفين ويقلل من مخاطر الاختراقات					
أمن الاجهزة الطرفية:						
9	الادارة العليا واعية بأهمية وضرورة توفير الأمن لأنظمة المعلومات.					
10	اجراءات الحماية التي تطبقها المؤسسة تواكب التغيرات الحاصلة في البيئة التكنولوجية.					
11	الفندق يخصص ميزانية خاصة لإدارة عملية أمن المعلومات					
12	الموظفون ذوي ثقافة أمن ية وواعون بمسؤولياتهم.					
أمن التطبيقات:						
13	التهديدات التي يتعرض لها الفندق عبارة عن دخول غير مصرح به					
14	التهديدات التي يتعرض لها الفندق عبارة عن برامج خبيثة					
15	توفير خدمات النسخ الاحتياطي واستعادة البيانات يضمن استمرارية العمليات الفندقية في حالة حدوث اختراقات أو فقدان للبيانات					
16	استعمال التقنيات البيو مترية مثل بصمات الأصابع والتعرف على الوجه يعزز الحتمية ويقلل من فرص الاختراقات بشكل فعال					
أمن البريد الالكتروني:						
17	هل هناك سياسة أو إجراء محدد للإبلاغ عن البريد الإلكتروني المريب أو المشتبه فيه					
18	هل يوجد لدى الفندق سياسة واضحة تتعلق					

	باستعمال البريد الإلكتروني في الأعمال اليومية					
19	هل يتم فحص رسائل البريد الإلكتروني الواردة باستعمال أدوات مكافحة الفيروسات والتصيد					
20	هل يستخدم الفندق تقنية تشفير للبريد الإلكتروني لحماية البيانات الحساسة					

ثانياً: المتغير التابع: - أمن المعلومات الفندقية

ت	العبارات	لا اتفق تمأما	لا اتفق	محايد	اتفق	اتفق تمأما
1	هل يتم يكون هناك تدريب منتظم للموظفين حول مفاهيم أمن المعلومات وحمايتها في الفندق					
2	يحرص الفندق على الوقاية من أخطار قرصنة معلوماتها.					
3	يستعين الفندق بمختصين تقنيين لضمان التسيير الجيد لنظام معلوماته.					
4	يقدم الفندق للموظفين برامج توعية عن حماية المعلومات.					
5	يقوم الفندق بإقامة دورات تثقيفية للعاملين حول أمن المعلومات.					
6	تحفيز الموظفين على تبني أفضل الممارسات في إدارة كلمات المرور والوصول الأمن إلى البيانات يعزز أمن النظام الفندقي					
7	هل يعرف جميع الموظفين كيفية التعامل مع الهجمات الإلكترونية مثل التصيد الاحتيالي والبرمجيات الخبيثة					

8	هل توجد سياسة رسمية مكتوبة لإدارة أمن المعلومات في الفندق					
9	هل هناك إجراءات واضحة للإبلاغ عن الحوادث الأمنية المتعلقة بأمن المعلومات في الفندق					
10	هل يتم تغيير كلمات المرور بشكل دوري وتطبيق سياسة كلمات مرور قوية داخل الفندق					