تهديدات الامن السيبراني للقطاع الفندقي العراقي وآلية مواجهاتها دراسة تحليلية للمنظمات الفندقية العراقية

أ . م . د. حسن عودة غضاب[1]
hassan85@mtu.edu.iq

المستخلص: تهدف الدراسة إلى عرض أهم التهديدات التي تواجه القطاع الفندقي العراقي من أجل تحقيق الامن السيبراني والذي يلعب دورا محوريا في معالجة التحديات المستقبلية، نظرا لاستخدمه كتكنولوجيا لإدارة شبكات المنظمات الفندقية، وذلك لمحاولة وضع اليات للحد من هذه التهديدات واتخاذ كافة الاجراءات الاحترازية التي يمكن ان تزعزع استقرار المنظمات الفندقية، وبقدر ما كانت التكنولوجيا سببا في تطوير القطاع الفندقي وتسهيل الولوج إلى خدماته والاستفادة منها، كانت هناك آثار سلبية تمثلت في تهديد هذا القطاع باختراق منظوماته المعلوماتية والاستيلاء على المعطيات التي تحتويها مما يشكل تهديدا خطيرا على المنظمات الفندقية من جهة، ومساسا بمعلوماتهم ومعلومات الزبائن من جهة أخرى، لهذا حاولنا أن نبحث في هذه الدراسة عن مفهوم الأمن السيبيراني وأهم التهديدات التي يمكن أن تواجه القطاع الفندقي العراقي، وتوصلت الدراسة إلى أن هناك أثر سلبي على الأداء والسمعة الفندقية: أي اختراق أو تسرب بيانات أو هجوم يُمكن أن يؤدي إلى خسائر مالية، خسارة ثقة الزبائن، وكذلك أمور قانونية، مما يُضعف التنافسية ويضر بالأعمال خصوصًا في قطاع يعتمد على خدمة الزبائن والثقة. وأوصت الدراسة تأسيس سياسات أمنية واضحة وثابتة: اعتماد سياسة أمن المعلومات تتضمن سرية البيانات، خصوصية الزبائن، التحديثات الأمنية، التحكم في وصول المستخدمين.

الكلمات المفتاحية: مفهوم الامن السيبراني، أهمية الامن السيبراني، مجالات الامن السيبراني، مفهوم المخاطر السيبرانية، أهمية ادارة المخاطر السيبرانية، أنواع المخاطر السيبرانية.

1. المقدمة

في ظل التحول الرقمي المتسارع وتزايد الاعتماد على تقنيات المعلومات والاتصالات في مختلف القطاعات، بات الأمن السيبراني يشكل أحد أبرز التحديات التي تواجه المنظمات، لاسيما في القطاع الفندقي، تُعد المنظمات الفندقية من بين الأهداف الرئيسية للهجمات السيبرانية نظراً لما تمتلكه من قواعد بيانات حساسة تتعلق بالنزلاء، أنظمة الحجز، والمعاملات المالية، وفي السياق العراقي، حيث تسعى الفنادق إلى تحديث بنيتها التحتية الرقمية

[1] استاذ مساعد دكتور : قسم تقنيات الادارة السياحية – الجامعة التقنية الوسطى- الكلية التقنية الادارية بغداد – بغداد – العراق

وتحسين خدماتها التكنولوجية، تتفاقم التهديدات السيبرانية نتيجة لضعف الوعي الأمني، ونقص الكوادر المتخصصة، وغياب الاستراتيجيات الشاملة لحماية الأنظمة والمعلومات.

ورغم التوسع النسبي في استخدام التكنولوجيا داخل المنظمات الفندقية، إلا أن البيئة الأمنية الرقمية لا تزال تعاني من العديد من الثغرات، كضعف البنية التحتية السيبرانية، وقلة الوعي الأمني لدى الكوادر، ونقص السياسات والإجراءات الوقائية، الأمر الذي يعزز من احتمالية تعرض هذه المنظمات إلى تهديدات سيبرانية متزايدة، سواء كانت موجهة من جهات إجرامية أو ناجمة عن سوء استخدام داخلي أو تقني.

المحور الاول

منهجية الدراسة

اولاً: مشكلة الدراسة

مع التوسع المتسارع في استخدام التقنيات الرقمية والأنظمة الإلكترونية في إدارة العمليات الفندقية، أصبحت الفنادق أكثر اعتمادًا على البنى التحتية الرقمية لتقديم خدماتها، مثل أنظمة الحجز الإلكتروني، قواعد بيانات النزلاء، أنظمة الدفع الإلكتروني، وشبكات الإنترنت المفتوحة للنزلاء. ورغم الفوائد التي تحققها هذه الأنظمة، إلا أنها باتت عرضة بشكل متزايد لمجموعة متنوعة من التهديدات السيبرانية، مثل الهجمات الإلكترونية، تسريب البيانات، البرمجيات الخبيثة، وهجمات الفدية.

وفي السياق العراقي، تواجه المنظمات الفندقية تحديات مضاعفة ناتجة عن ضعف البنية التحتية لتقنية المعلومات، وغياب التشريعات الصارمة الخاصة بأمن المعلومات، إضافة إلى انخفاض الوعي الأمني السيبراني لدى العديد من العاملين في هذا القطاع، الأمر الذي يعرّضها لمخاطر عالية تتعلق باختراق الأنظمة، فقدان البيانات الحساسة، وتأثر ثقة الزبائن وسمعة المنشآت.

تتمثل مشكلة الدارسة في التعرض المتزايد للمنظمات الفندقية العراقية لتهديدات الأمن السيبراني، في ظل ضعف الاستعدادات التقنية والإدارية لمواجهتها، وغياب سياسات أمنية واضحة، مما يتطلب تحليل هذه التهديدات واقتراح آليات مناسبة لتعزيز الأمن السيبراني في هذا القطاع الحيوي.

وهناك تساؤل فرعي مفاده كيف يمكن للقطاع الفندقي العراقي أن يعمل على تفادي التهديدات؟ وما هي أسباب تخلف القطاع الفندقي العراقي في هذا المجال.

ثانياً: أهمية الدراسة:

تنبع أهمية الدراسة من التزايد المطّرد في الاعتماد على الأنظمة الرقمية والتقنيات الحديثة في إدارة وتشغيل المنظمات الفندقية، ولا سيما في ظل التحول الرقمي الذي يشهده القطاع الفندقي العراقي،ومع هذا التحول، تبرز تهديدات الأمن السيبراني كأحد أبرز التحديات التي تواجه استمرارية العمل، وحماية البيانات الحساسة، وضمان ثقة الزبائن.

وتتجلى أهمية الدراسة من عدة جوانب، أبرزها:

1. **أهمية عملية وتطبيقية:** تسهم الدراسة في تزويد أصحاب القرار والإدارات الفندقية في العراق برؤية واضحة حول طبيعة التهديدات السيبرانية المحتملة، مما يمكّنهم من اتخاذ التدابير المناسبة لحماية نظمهم ومعلوماتهم.
2. **أهمية بحثية وعلمية:** تعد هذه الدراسة من الدراسات القليلة إن لم تكن النادرة التي تتناول موضوع الأمن السيبراني ضمن السياق الفندقي العراقي تحديدًا، ما يُشكّل إضافة علمية إلى أدبيات هذا المجال، ويفتح آفاقًا لدراسات لاحقة أكثر تعمقًا.
3. **أهمية اقتصادية وإدارية:** تساعد الدراسة في تقليل الأضرار المالية والخسائر المحتملة الناتجة عن الهجمات السيبرانية، من خلال تعزيز الوعي بالأمن الرقمي وتطوير استراتيجيات استجابة فعّالة، مما ينعكس إيجابًا على الأداء المالي والإداري للقطاع الفندقي.
4. **أهمية مجتمعية:** تسهم في تعزيز ثقة الزبائن المحليين والدوليين بالمنظمات الفندقية العراقية، من خلال التأكيد على وجود سياسات وإجراءات فاعلة لحماية بياناتهم الشخصية والمالية، الأمر الذي يُعزز من تنافسية القطاع الفندقي ويدعم الاقتصاد السياحي في العراق.
5. **أهمية قانونية وتشريعية:** يمكن أن تساهم الدراسة في تسليط الضوء على فجوات السياسات والتشريعات ذات الصلة بالأمن السيبراني، مما يوفر أرضية علمية يمكن الاستناد إليها في تطوير إطار قانوني داعم لأمن المعلومات في القطاع السياحي والفندقي.

ثالثاً: اهداف الدراسة:

يمكن ايجاز الأهداف الجوهرية لهذه الدراسة فيما يلي:

1. عرض أهم التهديدات التي تواجه القطاع الفندقي العراقي من أجل تحقيق الامن السيبراني والذي يلعب دورا محوريا في معالجة التحديات المستقبلية.
2. تحديد أنواع التهديدات السيبرانية التي تواجه المنظمات الفندقية في العراق.
3. تقييم مدى وعي هذه المنظمات بالأمن السيبراني ومستوى الجاهزية لديها لمواجهة هذه التهديدات.
4. اقتراح آليات فعالة للتصدي لتلك التهديدات، تناسب خصوصية السياق العراقي الفندقي.
5. تحليل البنية التحتية التقنية لدى الفنادق العراقية من حيث نقاط الضعف السيبرانية (مثل الشبكات، الأجهزة، أنظمة الحجز والدفع، التخزين السحابي).
6. دراسة ممارسات الأمان المعلوماتي المتبعة حالياً في المنظمات الفندقية (سياسات، تدريب الموظفين، النسخ الاحتياطي، التشفير، مراقبة الدخول، الاستجابة للحوادث).

رابعاً: فروض الدراسة:

تنطلق فرضية الدراسة الحالية من أن التحديات المتعددة التي تواجه الأمن السيبراني في القطاع الفندقي العراقي، مثل نقص التكنولوجيا الحديثة، ضعف البنية التحتية التقنية، قلة الوعي والتدريب، والتحديات القانونية والتنظيمية والاقتصادية، تؤثر بشكل كبير على المنظمات الفندقية العراقية، وتعتمد الدراسة على الفرضية أن تحسين هذه الجوانب من خلال استثمارات في التكنولوجيا والتدريب، تطوير تشريعات قوية، وتعزيز التعاون

الدولي، وتحسين مستوى التحضر والتوعية السيبراني في القطاع الفندقي العراقي يمكن أن يكون له تأثير ايجابي على تعزيز الامن السيبراني والتصدي للتهديدات المتزايدة في ظل التقدم التكنولوجي السريع.

خامساً: منهجية الدراسة:

ستعتمد منهجية الدراسة على المنهج الوصفي التحليلي لوصف وتحليل الوضع الحالي للأمن السيبراني في القطاع الفندقي العراقي، من خلال جمع البيانات الأولية عبر مقابلات مع خبراء الأمن السيبراني ومسؤولين حكوميين، واستخدام الاستبيانات لجمع آراء المتخصصين، بالأضافه إلى ذلك، سيتم دراسة حالات سيبرانية سابقة في القطاعات المختلفة وحالات من دول أخرى لاستخلاص الدروس المستفادة، وفي النهاية، سيتم وضع توصيات وحلول عمليه لتعزيز الأمن السيبراني في القطاع الفندقي العراقي بناءً على نتائج التحليل.

سادساً: تقسيمات الدراسة:

وبناءا على ما سبق يمكن استعراض تقسيمات الدراسة من خلال المحاور الاتية:

المحور الاول: منهجية الدراسة

المحور الثاني: مفهوم الامن السيبراني، أهمية الامن السيبراني، 3. مجالات الامن السيبراني.

المحور الثالث: مفهوم المخاطر السيبرانية، أهمية أدارة المخاطر السيبرانية، أنواع المخاطر السيبرانية.

المحور الرابع: آليات موجهة التهديدات السيبراني في المنظمات الفندقية العراقية.

المحور الخامس: الاستنتاجات والتوصيات وآفاق الدراسة.

المحور الثاني:- الجانب النظري للدراسة

أولا: الامن السيبراني:-

مفهوم الامن السيبراني : هو مجموعة من السياسات والإجراءات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات الإلكترونية،(فضل الله،1346:2025). ويرى (علي لبن،550:2024) أنه مجموعة من الإجراءات التي تتخذ في الدفاع ضد الهجمات السيبرانية، وعواقبها، وتنفيذ التدابير المضادة المطلوبة. وأضاف (الرحامنة،79:2023) هي مجموعة الأنشطة والعمليات التي تهدف إلى حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ، ويضمن الحد من حدوث الأضرار والخسائر المترتبة في حال تحقق المخاطر والتهديدات، كما يتيح اعادة الوضع الى ما كان عليه بوقت أسرع، بحيث لا تتوقف عجلة الانتاج، ولا تتحول الأضرار إلى خسائر دائمة. ويرى (سالم،71:2022) بأنه عملي الحد من خطر الهجمات الضارة على برامج وأجهزة الكمبيوتر والشبكات من خلال استخدام أدوات كشف الاختراقات ووقف نشاط الفايروسات، ومنع الدخول غير المسموح به، وتأكيد الهويات وتمكين الاتصالات المشرة. وبموجب ما ذكر من مفاهيم للأمن السيبراني حيث يعرفه الباحث بأنه جميع الإجراءات التنظيمية واللازمة لضمان حماية المعلومات الفندقية بجميع أشكالها المادية والالكترونية من مختلف الجرائم ، الهجمات ،التخريب ، التجسس و الحوادث.

1. أهمية الامن السيبراني للمنظمات الفندقية العراقية: يعد الأمن السيبراني عنصرا اساسيا في مكافحة الجرائم الإلكترونية التي تنشأ في الفضاء الرقمي أو الافتراضي، هذه الجرائم التي ينفذها أفراد أو جماعات

ذو مهارات عالية في مجال التقنية، تسبب أضرارا جسيمة للمنظمات الفندقية العراقية، الذي أصبحت مترابطة من خلال الإنترنت، وتتمثل الاهمية في : (فهمي واخرون،22:2025)، (أبو الفضل،1865:2024)، (التونى،626:2023).

أ. قدرته على مكافحة الهجمات والمخاطر السيبرانية سواء كانت مقصودة أو غير مقصودة، والسعي في التصدي لأضرارها وآثارها السلبية ومحاولة علاجها.

ب. حماية الأجهزة والشبكات :تُعتبر حماية الأجهزة والشبكات كدرع واقٍ للبيانات والمعلومات الفندقية من الاختراقات أمرًا أساسيًا للحفاظ على سلامة المعلومات وضمان استمرارية العمل.

ت. استكشاف نقاط الضعف ومعالجتها :تتمثل إحدى خطوات الأمن السيبراني في الكشف المبكر عن الثغرات ونقاط الضعف في الأنظمة، ثم معالجتها بشكل فوري للحد من المخاطر المحتملة.

ث. حماية المواقع الإلكترونية :تعتمد المنظمات الفندقية العراقية بشكل كبير على مواقعها الإلكترونية في التسويق والتواصل مع العملاء. وبالتالي، فإن تعطل هذه المواقع قد يؤدي إلى خسائر مالية كبيرة، وفقدان المعاملات، وتراجع ثقة العملاء. لذلك، يشمل الأمن السيبراني حماية المواقع الإلكترونية من الأضرار غير المتوقعة لضمان استمرارية العمل وتعزيز الثقة.

ج. حماية سمعة المنظمات الفندقية :تسعى المنظمات الفندقية العراقية إلى كسب ثقة العملاء وتعزيز سمعتها وعلامتها التجارية في السوق. ويتحقق ذلك من خلال تطبيق استراتيجيات الأمن السيبراني التي تضمن حماية كاملة للبيانات الفندقية وتفادي أي انتكاسات أمنية مفاجئة. وبناء تاريخ قوي في حماية البيانات يعزز قاعدة العملاء ويزيد من ولائهم.

ح. تعزيز الوضع السيبراني :يوفر الأمن السيبراني للمنظمات الفندقية العراقية حماية رقمية شاملة، مما يمنح الموظفين مرونة وأمانًا في الوصول إلى الإنترنت. كما تتيح هذه الاستراتيجية للمنظمات القدرة على التصرف بسرعة وفعالية أثناء وبعد الهجمات الإلكترونية، مما يعزز من جاهزيتها واستمراريتها.

2. مجالات الامن السيبراني في المنظمات الفندقية العراقية: أصبح من الضروري أن تتطور وسائل الأمن السيبراني، لتواجه تطور طرق الاختراق والهجمات السيبرانية، ولذلك أصبح الأمن السيبراني يشمل العديد من المجالات كما يلي:

أ. **أمن الشبكات:** وهو عملية اتخاذ الإجراءات الوقائية لغرض حماية البنى التحتية للشبكات ومنع الوصول غير المصرح به كمحاولات التدمير او التعطيل، مما يوفر بيئة امنة للمستخدمين لغرض أداء الوظائف الحيوية المسموح بها كما وأن الأمن السيبراني للشبكات يتضمن مجموعة واسعة من التقنيات والأجهزة والإجراءات المستخدمة لحمايتها، كما يتضمن مجموعة من القواعد والتكوينات المصممة لضمان سرية البيانات وسلامتها وإمكانية الوصول إليها ويهدف إلى تأمين الشبكات الداخلية من التهديدات المختلفة من خلال عدة وسائل(الحسيني والدعمي،423:2025).

ب. **أمن التطبيقات:** يرتبط هذا النوع بتأمين التطبيقات الموجودة على الشبكة بهدف الحفاظ عليها من أي تهديدات من شأنها التركيز على تدمير تلك التطبيقات التي تمثل العمود الفقري للشبكة وخاصة المنظمات

التي تعمل على تطوير وبيع التطبيقات والخدمات السحابية الحديثة، ولكن بعض الأحيان التهيئة الخاطئة أثناء الإعدادات الأولية للأمان تكون سببًا أساسيا لحدوث اختراقات للبيانات والحسابات السحابية، في حين يتم استخدام خدمة سحابية كبيرة مثل Microsoft 365 كنوع من أنواع التأمين للتطبيقات الموجودة على الشبكة لكنها تحتاج لتخصيص إعدادات الأمان من خلال الإعدادات الافتراضية (البحيري،67:2023).

ت. **الامن التطبيقي:** إذا تعرضت البيانات الفندقية إلى الاختراق يساعد هذا النوع على الوصول إلى العديد من الخطط البديلة، لذلك يتم الاعتماد علية في المنظمات الفندقية العراقية (أبو الفضل،1865:2024).

ث. **أمن المعلومات:** يختص بأمن وحماية بيانات الخاصة بالمنظمات الفندقية العراقية فضلا عن بيانات الزبائن وذلك من منطلق الحفاظ على خصوصية وسرية البيانات والامتثال للوائح والقوانين المنظمة للخصوصية، إذ أن المنظمات لا بد لها من الالتزام وتطبيق معايير أمن المعلومات، في حين إن المنظمات التي تخل عن هذه المعايير تتعرض لعقوبات خاصة إذا كان الإهمال يؤدي إلى اختراق المعلومات التعريفية للأشخاص، لذا فأن المنظمات الفندقية العراقية وضمن مجال الأمن السيبراني تعمل على تأمين جمع البيانات ونقلها، وتطبيق وسائل الحماية الكافية من التعرض للانتهاك (خليفة،7:2025).

ج. **الامن السحابي:** هو مجموعة من السياسات والتقنيات والممارسات المصممة لحماية البيانات والتطبيقات والبنية التحتية المخزنة على الحوسبة السحابية، ويهدف إلى تأمين الأنظمة السحابية ضد التهديدات السيبرانية مثل الاختراقات، وسرقة البيانات، والهجمات الإلكترونية، أصبحت الحاجة إلى أمن سحابي قوي ضرورة لضمان حماية البيانات الحساسة من الوصول غير المصرح به، ومكافحة الهجمات الإلكترونية مثل البرمجيات الخبيثة والتصيد الاحتيالي، والامتثال للقوانين وضمان استمرارية الأعمال من خلال أنظمة النسخ الاحتياطي واستعادة البيانات، يعد الأمن السحابي عنصرا أساسيا لحماية البيانات والتطبيقات المخزنة على السحابة، وأصح من الضروري تطبيق استراتيجيات أمان قوية لضمان سرية وسلامة المعلومات (الحسيني والدعمي،424:2025).

المحور الثالث

أولا: المخاطر السيبرانية

1. **مفهوم: المخاطر السيبرانية:** بأنها حدوث خسائر محتملة تتحقق عندما يؤثر التهديد السيبراني، على أحد الاصول ذات القيمة ويؤدي إلى تأثير جوهري على المنظمة الفندقية ،(موسى،255:2025). ويرى (أبو عيشة،373:2024) أنها تشير إلى المخاطر التي تنطوي عليها حدث إلكتروني خبيث يؤدي إلى الخسارة المالية وتعطيل الاعمال الفندقية، وتشمل جميع المخاطر المتعلقة بالأنترنت، مثل تخزين البيانات الشخصية للزبائن، أو أجراء الحجز الالكتروني عبر الانترنت التي قد تؤدي إلى الاضطراب او الإضرار بسمعة المنظمة الفندقية، نتيجة فشل أنظمة تكنولوجيا المعلومات الخاصة بها. وأضاف (جبر،59:2023) هو كل تصرف غير شرعي موجه بالوسائل الإلكترونية نحو أمن أنظمة المعلومات والبيانات التي تحويها. ويرى (إبراهيم واخرون،401:2022) بأنها هجوم عبر الإنترنت يقوم على التسلل إلى مواقع إلكترونية غير مرخص بالدخول إليها، بهدف تعطيل أو إتلاف البيانات المتوفرة فيها أو الاستحواذ عليها.

2. **أهمية ادارة المخاطر السيبرانية للمنظمات الفندقية:** تُعد المخاطر السيبرانية من القضايا الحيوية التي تواجهها المنظمات الفندقي في العصر الرقمي، نظراً لاعتمادها الكبير على الأنظمة التكنولوجية في تشغيل عملياتها اليومية، مثل الحجز الإلكتروني، إدارة بيانات النزلاء، أنظمة الدفع، والاتصالات الداخلية والخارجية، وتتمثل الاهمية في (موسى,256:2025) و (أبو عيشة,374:2024).

أ. **حماية بيانات النزلاء الحساسة:** المنظمات الفندقية تجمع كميات كبيرة من البيانات الشخصية والمالية للنزلاء، مثل:أسماء كاملة، أرقام بطاقات ائتمان، معلومات جوازات السفر، عادات الإقامة والطلبات الخاصة، أي اختراق لتلك البيانات قد يؤدي إلى خسائر قانونية ومالية جسيمة وفقدان الثقة.

ب. **حماية العمليات التشغيلية الفندقية:** حيث تعتمد المنظمات الفندقية على أنظمة إلكترونية لإدارة: الحجوزات، الغرف الذكية، أنظمة الدخول الآلي، أوي هجوم إلكتروني (مثل هجوم فدية) قد يعطّل العمليات كليًا ويؤدي إلى إغلاق مؤقت.

ت. **الحفاظ على سمعة المنظمات الفندقية:** الهجمات السيبرانية قد تُنشر في الإعلام وتُشوّه صورتها، واستعادة الثقة بعد حادثة اختراق قد تكون عملية طويلة ومكلفة.

ث. **التهديدات المتزايدة مع التحول الرقمي**: اعتماد المنظمات الفندقية على تقنيات مثل إنترنت الأشياء، والذكاء الاصطناعي، والتطبيقات الذكية زاد من سطح الهجمات، وهذا يجعل من الضروري استباق التهديدات وتحديث الأنظمة بشكل دوري.

ج. **مخاطر الابتزاز المالي الفندقي:** هجمات الفدية تستهدف المنظمات الفندقية للحصول على المال مقابل استرجاع البيانات، المنظمات الفندقية قد تكون هدفًا مغريًا بسبب حساسية البيانات وضغط الوقت في العمل.

3. **أنواع الهجمات السيبرانية التي تستهدف المنظمات الفندقية:** تختلف الهجمات السيبرانية التي تستهدف المنظمات الفندقية حسب الهدف والطريقة والمصدر والتأثير والحجم والتعقيد والتكرار والشدة والخطورة،(آل محيا ومكين,9:2025) و(التائب والسائح,200:2025) و (أبو عيشة,375:2024). ومن أنواع الهجمات السيبرانية التي تستهدف البنوك ما يلي:

أ. **الهجمات النشطة:** هي الهجمات التي تهدف إلى التأثير على البيانات أو الأنظمة أو الشبكات أو الخدمات بشكل ملحوظ أو مزعج أو مدمر، مثل التعديل أو الحذف أو الإضافة أو العرقلة أو القرصنة أو الاستيلاء أو الاستخدام غير المصرح به، تتضمن أمثلة الهجمات النشطة الفيروسات، والديدان، وأحصنة طروادة، وبرامج الفدية، وشبكات الروبوت.

ب. **هجمات التصيد الاحتيالي:** تتضمن هجمات التصيد الاحتيالي إرسال رسائل بريد إلكتروني أو رسائل نصية مزيفة تبدو وكأنها تأتي من مصدر موثوق به، وتحاول هذه الرسائل إقناع الضحايا بالكشف عن معلومات حساسة، مثل كلمات المرور أو بيانات الفندقية.

ت. **هجمات انتحال الهوية:** تتضمن هجمات انتحال الهوية استخدام معلومات شخصية مسروقة، مثل اسم المستخدم وكلمة المرور، للوصول إلى حساب شخص آخر، يمكن للمهاجمين استخدام هذه المعلومات للوصول إلى الحسابات الفندقية أو إجراء عمليات شراء.

ث. **هجمات برامج الفدية:** تتضمن هجمات برامج الفدية سرقة بيانات حساسة وتعطيل الوصول إليها حتى يدفع الضحية فدية، يمكن للمهاجمين استخدام هذه البيانات للابتزاز أو لطلب فدية.

ج. **الهجمات السلبية:** هي الهجمات التي تهدف إلى الحصول على البيانات أو الأنظمة أو الشبكات أو الخدمات بطريقة مخفية أو مقنعة، مثل الاستطلاع أو الاستنساخ أو الاستخبارات أو الاسترجاع أو التنصت أو التجسس أو القرصنة أو الاختطاف أو الاستخدام غير المصرح به، تتضمن أمثلة الهجمات السلبية: صيد الأسماك، وصيد الأسماك بالرمح، والصيد، والزراعة، والانتحال، والاستنشاق، والمسح الضوئي، والتمرير السريع، والكشط، والغزل عبر الإنترنت، والخداع عبر الإنترنت.

ح. **هجمات اختراق البيانات:** تتضمن هجمات اختراق البيانات الوصول غير المصرح به إلى أنظمة الكمبيوتر أو الشبكات الفندقية، يمكن للمهاجمين استخدام هذه المعلومات لسرقة البيانات الحساسة أو لتعطيل العمليات الفندقية.

خ. **الهجمات الداخلية:** هي الهجمات التي يتم إطلاقها من داخل المنظمات الفندقية أو من قبل أشخاص لديهم صلة أو علاقة أو إمكانية الوصول إلى المنظمات الفندقية، مثل الموظفين أو العملاء أو الشركاء أو الموردين أو المقاولين أو المنظمين أو المنافسين أو الوكالات الحكومية أو الأطراف الخاصة، وتكون هذه الهجمات ناجمة عن الإهمال أو الجهل أو الخطأ أو الفشل أو المخالفة أو التلاعب أو الخيانة أو الانتقام أو الجشع أو الفضول أو الرغبة أو الخوف أو الضغط أو الابتزاز أو الإغراء أو الإكراه أو الإقناع أو الاستغلال.

د. **الهجمات الخارجية:** هي الهجمات التي يتم إطلاقها من خارج البنك أو من قبل أشخاص ليس لديهم أي اتصال أو علاقة أو وصول إلى المنظمات الفندقية، مثل المتسللين والقراصنة والفيروسات والمبرمجين ومرسلي البريد العشوائي والصيادين والمحتالين ومجرمي الإنترنت والناشطين عبر الإنترنت أو الناشطين السيبرانيين أو المرتزقة السيبرانيين أو الميليشيا السيبرانية أو المافيا السيبرانية أو الإرهابيين السيبرانيين أو المحاربين السيبرانيين أو الجنود السيبرانيين أو وكلاء السيبرانية أو الجواسيس السيبرانيين أو الدول المارقة السيبرانية أو الدول القومية السيبرانية.

المحور الرابع

آليات موجهة التهديدات السيبراني في المنظمات الفندقية

لضمان أمن المعلومات الفندقية الحساسة، يجب على المنظمات الفندقية تبني استراتيجية شاملة لمواجهة التهديدات السيبيرانية تتضمن مجموعة من الإجراءات الوقائية والاستباقية، هذه الإجراءات ضرورية لحماية البيانات من التهديدات المتزايدة في العصر الرقمي،(التائب والسائح,201:2025) و(جبر,64:2023) تتمثل بـــــــــــ الاتي:

أ. تقييم المخاطر المنتظمة:

الأهمية: يساعد تقييم المخاطر في تحديد نقاط الضعف المحتملة في النظام الفندقي ، مما يسمح باتخاذ إجراءات استباقية لتقليل احتمالية حدو ث اختراقات.

الإجراءات: إجراء تقييمات دورية وشامل ة للمخاطر لتقييم الثغرات الأمنية تحليل التهديدات المحتملة وتحديد أولويات الإجراءات التصحيحية .

ب. توعية الموظفين وتدريبهم:

الأهمية: يعتبر الموظفون خط الدفاع الأول ضد الهجمات السيبرانية ، لذا يجب تزويدهم بالمعرفة اللازمة للتعرف على التهديدات مثل التصيد الاحتيالي والبرمجيات الخبيثة.

الإجراءات: إجراء برامج تدريبية منتظمة وشاملة لرفع مستوى الوعي الأمني لدى الموظفين وتدريبهم على أفضل الممارسات الأمنية .

ت. تشفير البيانات الفندقية:

الأهمية: يضمن التشفير حماية البيانات من الوصول غير المصرح به حتى في حالة اختراق النظام.

الإجراءات: استخدام تقنيات تشفير قوية لحماية البيانات أثناء التخزين والنقل ، والتأكد من أن جميع الأجهزة التي تحتوي على بيانات حساسة مشفرة .

ث. تحديث البرامج باتنظام :

الأهمية: التحديثات الأمنية تسد الثغرات التي يمكن أن يستغلها المهاجمون للوص ل إلى النظام .

الإجراءات: تثبيت التحديثات الأمنية والتصحيحات فور صدورها، وكذلك التأكد من أن جميع البرامج وأنظمة التشغيل محدثة إلى آخر إصدار .

ج. مراقبة الأنظمة والكشف عن التهديدات :

الأهمية: المراقبة المستمرة تسمح بالكشف المبكر عن أي نشاط مشبوه ، مما يتيح اتخاذ إجراءات سريعة لمنع الهجمات أو تقليل تأثيرها .

الإجراءات: المراقبة المستمرة تسمح بالكشف المبكر عن أي نشاط مشبوه، مما يتيح اتخاذ إجراءات سريعة لمنع الهجمات أو تقليل تأثيرها، وتحليل لأنماط السلوكية لتحديد الأنشطة غير المعتادة التي قد تشير إلى هجوم محتمل.

المحور الخامس:- الاستنتاجات والتوصيات وآفاق الدراسة

اولا: الاستنتاجات:

1. نقص الوعي والتدريب: غالبية العاملين في المنظمات الفندقية لا يمتلكون فهمًا كافيًا لمفهوم الأمن السيبراني، خصوصًا فيما يتعلق بالتهديدات الحديثة مثل الهندسة الاجتماعية، التصيد الاحتيالي، واختراق الأنظمة الداخلية.

2. ضعف البُنى التحتية التقنية والأمنية: الفُتحات الأمنية في البنية التحتية لتكنولوجيا المعلومات، مثل الشبكات اللاسلكية غير الآمنة، استخدام برمجيات قديمة، ضعف التحديثات الأمنية، أو عدم وجود سياسات أمنية واضحة تُعتبر نقطة ضعف كبيرة.
3. غياب الأطر التشريعية والتنظيمية المناسبة: القوانين العراقية المتعلقة بالأمن السيبراني أو حماية البيانات قد تكون غير مكتملة، أو تفتقر إلى التطبيق الفعّال أو الجزاءات الرادعة، هذا يترك المنظمات، بما في ذلك القطاع الفندقيفي مأزق من الناحية القانونية عند التعرض لهجمات سيبرانية.
4. محدودية القدرة على الرد والتعافي: المنظمات الفندقية ربما تفتقر إلى خطط استجابة للحوادث السيبرانية أو فرق مختصة للتعامل مع الاختراقات، مما يزيد من الأضرار الاقتصادية والسمعة حين تقع الحوادث.
5. الاعتماد المتزايد على الأنظمة الرقمية دون أمن متناسب: مع الرقمنة المؤسسية (الحجوزات الإلكترونية، إدارة الزوار، أنظمة الدفع عبر الإنترنت) زادت النقاط التي يُمكن أن تُستهدفها الهجمات، لكن بدون التزام كافٍ بإجراءات الحماية.
6. أثر سلبي على الأداء والسمعة الفندقية: أي اختراق أو تسرب بيانات أو هجوم يُمكن أن يؤدي إلى خسائر مالية، خسارة ثقة الزبائن، وكذلك أمور قانونية، مما يُضعف التنافسية ويضر بالأعمال خصوصًا في قطاع يعتمد على خدمة الزبائن والثقة.

ثانيا: التوصيات:

1. رفع مستوى الوعي والتدريب المستمر: دورات تدريبية دورية لجميع العاملين – من الإدارة العليا إلى الموظفين التقنيين والعاملين في استقبال الزوار حول المخاطر السيبرانية، وكيفية التعرف على الهجمات (مثل البريد الاحتيالي، الروابط الخبيثة، إلخ).
2. تأسيس سياسات أمنية واضحة وثابتة: اعتماد سياسة أمن المعلومات تتضمن سرية البيانات، خصوصية الزبائن، التحديثات الأمنية، التحكم في وصول المستخدمين.
3. تحديد مسؤولية أمنية واضحة (من هو المسؤول في المنظمات الفندقية عن الأمن السيبراني؟) وإنشاء وحدة أمنية أو وظيفة أمن المعلومات.
4. تحديث البُنى التحتية التقنية: متمثة بـــــــــــــــــــ

أ. استخدام أنظمة تشفير للبيانات أثناء النقل وعند التخزين.

ب. الحفاظ على تحديث البرامج والأنظمة التشغيلية وتطبيق التصحيحات الأمنية فور صدورها.

ت. استخدام جدران نارية، أنظمة كشف التطفل(IDS/IPS) ، والمراقبة المستمرة للشبكة.

5. تحسين إدارة المخاطر: من خلال إجراء تقييم دوري لمخاطر الأمن السيبراني وتحديد التهديدات المحتملة، الثغرات، تقدير الأثر والاحتمالية.
6. استخدام التكنولوجيا المتقدمة: مثل أنظمة مراقبة تلقائية وتحليل السجلات، أدوات تحليل التهديدات، البرمجيات المضادة للبرمجيات الخبيثة، الحماية ضد برامج الفدية.

ثالثا: آفاق الدراسة: بعد دراستنا لهذا الموضوع تم اقتراح بعض العناوين التي تستحق الدراسة والتحليل، أهمها:

1. دور التدريب والتوعيةفي بناء ثقافة الأمن السيبراني في الفنادق الممتازة والتصدي للهجمات السيبرانية.
2. دور الذكاء الإصطناعي في اكتشاف ومكافحة الإحتيال المالي في فنادق الدرجة الاولى في العاصمة العراقية- بغداد.
3. تأثير الإبتكار التكنولوجي على استراتيجيات أمن المعلومات الفندقية ومواجهة التهديدات السيبرانية.

تقييم الثغرات الأمنية الجديدة والتهديدات المستقبلية للفنادق: رؤية مستقبلية لتطورات أمن المعلومات.

المصادر العربية

1. أبراهيم، فاطمة علي ويوسف، رحاب والسيد، وليد محمود، 2022، الأمن السيبراني والنظافة الرقمية، المجلة المصرية لعلوم المعلومات، المجلد 9، العدد 2.
2. أبو الفضل، عبدالعال مصطفى، 2024، أثر الإنفاق في الأمن السيبراني على الأداء في البنوك التجارية المصرية مع دراسة ميدانية، مجلة الدراسات التجارية المعاصرة، كلية التجارة جامعة كفر الشيخ، المجلد العاشر، العدد السابع عشر، الجزء الثالث.
3. أبو عيشة، علاء محمد محمود، 2024، دور الإفصاح الخارجي عن جودة أنشطة المراجعة الداخلية في تحسين إدارة المخاطر السيبرانية دراسة تطبيقية، المجلة العلمية للدراسات والبحوث المالية والادارية – المجلد السابع عشر- العدد الاول.
4. آل محيا، عبد الإله سعيد ومكين، أروى أحمد،2025، أثر الهندسة الاجتماعية على مخاطر الامن السيبراني في البنوك في مدينة الرياض في المملكة العربية السعودية، مجلة العلوم الاقتصادية والإدارية والقانونية، المجلد9، العدد 1.
5. البحيري، شيرين، 2022، دور الإعلام الرقمي في تعزيز الامن السيبراني ومكافحة التهديدات والجرائم السيبرانية، المجلة العلمية لبحوث العلاقات العامة والإعلان، العدد الخامس والعشرون، يناير/ يونيو.
6. التائب، علي مفتاح والسائح، جبريل عمر، 2025، أهمية تطبيق الأمن السيبراني المحاسبي في المصارف التجارية الليبية: دراسة تطبيقية على المصارف التجارية العاملة في مدينة سرت، مجلة جلة الدراسات الاقتصادية - كلية الاقتصاد - جامعة سرت المجلد 8، العدد 1.
7. التونى، شريهان مصطفى، 2023، اثر وعي العملاء بالقرصنة الالكترونية كأداة لتحقيق الامن السيبراني دراسة ميدانية على البنوك الحكومية بمحافظة بور سعيد، المجلة العلمية التجارة والتمويل كلية التجارة جامعة طنطا، العدد الرابع، ديسمبر.
8. جبر، غريب جبر، 2023، تهديدات الأمن السيبراني للمصارف الإلكترونية وآلية مواجهاتها، المجلة الاكاديمية للعلوم الاجتماعية، المجلد 1، العدد 1.

9. الحسيني، سرور حافظ والدعمي، وليد عباس، 2025، أثر الأمن السيبراني في الحد من القصور الذاتي للمصارف، مجلة الغري للعلوم الاقتصادية والادارية، المجلد 21، العدد 2.
10. خليفة، سندس علي، 2025، استراتيجيات تعزيز الأمن السيبراني وتأثيرها على ثقة العملاء وأداء المصارف العراقية، مجلة تكريت للعلوم الإدارية والاقتصادية، المجلد 21، العدد 69، الجزء الاول.
11. الرحامنة، عبد المجيد أحمد، 2023، متطلبات تحقيق الأمن السيبراني في البنوك الإسلامية الأردنية، مجلة العلوم الاسلامية والدينية، المجلد 8، العدد 1.
12. سالم، ماجد صدام، 2022، الامن السيبراني العراقي واثرة في قوة الدولة، مجلة العلوم التربوية والانسانية، المجلد 18، العدد 18.
13. علي لبن، خالد أنور، 2024، الأمن السيبراني للعاملين بالقطاع الحكومي بريف محافظة الشرقية، مجلة الاقتصاد الزراعي والعلوم لاجتماعية، المجلد 15، العدد 11.
14. فضل الله، هيثم رزق، 2025، دور الذكاء الاصطناعي في تعزيز فعالية الأمن السيبراني دراسة تحليلية للتحديات والحلول المستقبلية، المجلة المصرية للدراسات المتخصصة، المجلد 13، العدد 46، الجزء الخامس.
15. فهمي, تقى محروس و خضير, أحمد محروس وبسيوني, محمد شعبان ورمضان, هدير مسعود, 2025, تأثير الامن السيبراني على الولاء للعلامة التجارية في شركات الطيران: دراسة من منظور العلاء, بحث منشور في مجلة كلية السياحة والفنادق جامعة مدينة السادات, المجلد 9, العدد (2-1).
16. موسى، عمرو عادل عبد الفتاح، 2025، مؤشر مقترح للإفصاح عن المخاط السيبرانية في سياق بيئة المعلوماتية المصرية الرقمية، مجلة الابداع المحاسبي، المجلد الثاني، العدد الثاني.

Cybersecurity Threats to the Iraqi Hospitality Sector and Mechanisms for Countering Them: An Analytical Study of Iraqi Hotel Organizations

[1] **Associate Professor Hassan Odah Ghdaab**

hassan85@mtu.edu.iq

Abstract:

The study aims to present the most significant threats facing the Iraqi hotel sector in order to achieve cybersecurity, which plays a pivotal role in addressing future challenges, given its use as a technology for managing hotel organizations' networks. The objective is to develop mechanisms to mitigate these threats and take all necessary precautionary measures to prevent any potential destabilization of hotel organizations. While technology has contributed significantly to the development of the hotel sector and facilitated access to and utilization of its services, it has also had negative consequences — namely, the threat of cyberattacks, data breaches, and unauthorized access to the organizations' information systems. This poses a serious risk not only to hotel organizations themselves but also to the privacy and safety of their customers' information. Therefore, this study seeks to explore the concept of cybersecurity and identify the main threats that may face the Iraqi hotel sector. The study concludes that there is a negative impact on hotel performance and reputation: any breach, data leak, or cyberattack can result in financial losses, loss of customer trust, and legal consequences — all of which weaken competitiveness and harm business operations, especially in a sector that relies heavily on customer service and trust. The study recommends the establishment of clear and consistent security policies: adopting an information security policy that ensures data confidentiality, customer privacy, security updates, and controlled user access.

Keywords: Concept of Cybersecurity, Importance of Cybersecurity, Cybersecurity Fields, Concept of Cyber Risks, Importance of Cyber Risk Management, Types of Cyber Risks.

[1]Assistant Professor, PhD Department of Tourism Management Techniques – Middle Technical University – Technical Institute of Administration, Baghdad – Iraq.