

## تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقويمية

د. الجوهرة بنت عثمان بن علي الركبان

أستاذ الإدارة والتخطيط التربوي المشارك - كلية التربية

جامعة الإمام محمد بن سعود الإسلامية

### الملخص:

هدفت الدراسة إلى التعرف على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، والكشف عن المعوقات التي تحدّ من تحقيقه، وتقديم مقترحات تُسهم في تحقيقه، وقد تكوّن أفراد الدراسة من (٦٣) موظفًا وموظفة من عمادة تقنية المعلومات وإدارة الأمن السيبراني، وتم تطبيق المنهج الوصفي المسحي، وكانت الاستبانة هي أداة جمع البيانات، وقد توصلت الدراسة إلى عدة نتائج منها: موافقة أفراد الدراسة بدرجة عالية وبمتوسط حسابي عام (٤, ١٤) على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، وموافقة أفراد الدراسة بدرجة متوسطة وبمتوسط حسابي عام (٢, ٦٣) على المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، وموافقة أفراد الدراسة بدرجة عالية وبمتوسط حسابي عام (٣, ٨١) على المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية. وعلى ضوء النتائج أوصت الدراسة بالتالي: تطوير البنية التحتية السيبرانية في الجامعة باستمرار للحدّ من الاختراقات والهجمات السيبرانية، وإيجاد آليات للتعامل الفوري مع مخاطر الأمن السيبراني، تتماشى مع الضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني.

**الكلمات المفتاحية:** الأمن السيبراني، أنظمة المعلومات الإدارية، إدارة الأمن السيبراني، عمادة تقنية المعلومات، الجامعة.

## Achieving cyber security for management information systems at Imam Muhammad bin Saud Islamic University: an evaluation study

### Abstract:

The study aimed to identify the reality of achieving cyber security for management information systems at Imam Muhammad bin Saud Islamic University, revealing the obstacles that limit its achievement, and presenting proposals that contribute to achieving it. The study members consisted of (63) male and female employees from the Deanship of Information Technology and Cyber Security Department, descriptive survey method was applied, and the questionnaire was the data collection tool. The study reached several results, including: the approval of the study members at a high degree with an average of (4.14) on the reality of achieving cyber security for management information systems, and the approval of the study members at a medium degree with an average of (2.63) on the obstacles that limit the achievement of cybersecurity for management information systems And the approval of the study members with a high degree with an average of (3.81) on the proposals that contribute to achieving cyber security for management information systems. In light of the results, the study recommended the following: Constantly developing the university's cyber infrastructure to limit cyber-intrusions and attacks and create mechanisms for immediate dealing with cyber security risks, in line with the basic controls issued by the National Cyber Security Authority.

**Keywords:** cyber security, management information systems, cyber security management, information technology deanship, university.

## المقدمة:

يمر العالم اليوم بتغيرات متسارعة في بيئة العمل، انعكست آثارها على تطوير إجراءات وأساليب العمل، وتوظيف الأنظمة التقنية الحديثة، وصولاً لتحقيق الميزة التنافسية، وكسب رضا المستفيدين.

فالأنظمة التقنية الحديثة تنظم العمليات الإدارية، وتسهّل من إجراءات العمل، مما يسهم في توفير الوقت والجهد، وينظم عملية اتخاذ القرارات، إلا أن تفعيل تلك الأنظمة كما يرى (البار والسميري، ٢٠١٩م: ١٠) يشوبه عددٌ من المشكلات والمخاطر؛ كالتعرض للاختراقات والتهديدات والهجمات الإلكترونية؛ الأمر الذي يشكل تحدياً أمام المؤسسات، خاصة التعليمية منها، والذي يتمثل في مدى قدرتها على إيجاد السبل الإدارية التي تساعد على تنظيم العمل، وتوفير الإجراءات الإدارية لضمان استمرارية عمل نظم المعلومات، وتعزيز حماية وخصوصية المعلومات الإدارية، وهو ما يعرف بالأمن السيبراني.

ولقد أكدت العديد من الدراسات والبحوث على أهمية الأمن السيبراني لأنظمة المعلومات الإدارية، حيث أشارت دراسة الصحفي وعسكول (٢٠١٩م) إلى أن الأمن السيبراني يعمل على حماية سير العمليات الإدارية، كما يحمي البيانات والمعلومات، ويمنع الدخول غير المرخص لها أو العبث بها.

كما أكدت دراسة البيشي (٢٠٢١م) على أن الأمن السيبراني يحافظ على المعلومات وتجانسها وسلامتها، ويكفّ العابثين عنها، ويجعلها أكثر جاهزية عند الحاجة لها، كما يحمي الأجهزة والشبكات من الاختراق، فمن خلال الأمن السيبراني يمكن معرفة الثغرات في الأنظمة ومعالجتها، وتوفير بيئة آمنة للمستخدمين.

واستشعاراً بأهمية البيانات والمعلومات والأنظمة التقنية، وأهمية حمايتها من أي تهديدات أو مخاطر، صدرت الموافقة على تأسيس الهيئة الوطنية للأمن السيبراني، وفق الأمر الملكي الكريم بتاريخ ١١/٢/١٤٣٩هـ؛ لتكون هي الجهة المختصة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه، حيث تهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة، وأمنها الوطني، والبنى التحتية الحساسة، والخدمات والأنشطة الحكومية، ولا يخفى ذلك أيّ جهة عامة أو خاصة أو غيرها من مسؤوليتها تجاه أمنها السيبراني بما لا يتعارض مع اختصاصات ومهام الهيئة (الهيئة الوطنية للأمن السيبراني، ٢٠٢٢م).

لذلك أصدرت الهيئة الوطنية للأمن السيبراني الإطار السعودي للتعليم العالي في الأمن السيبراني (ساير- التعليم)، الذي تم إعداده بالتعاون بين الهيئة، ووزارة التعليم، وهيئة تقويم التعليم والتدريب، حيث يسهم هذا الإطار في بناء وتطوير برامج أكاديمية عالية الجودة في مجال الأمن السيبراني، تكون متوائمة مع الاحتياج الوطني في سوق العمل، وتسهم في سد الفجوة في هذا المجال (الهيئة الوطنية للأمن السيبراني، ٢٠٢٢م).

ووقعت وزارة التعليم اتفاقية تعاون مع الهيئة الوطنية للأمن السيبراني، تهدف إلى تعزيز التعاون المشترك في مجالات التعليم، والبحث العلمي، والتدريب، والتوعية في مجال الأمن السيبراني، والتي تسهم في تأهيل الكوادر الوطنية في مجال الأمن السيبراني (وكالة الأنباء السعودية، ٢٠٢٢م).

وأنشئ برنامج التعاملات الإلكترونية الحكومية (يسر) لتطوير جودة وفاعلية الخدمات الرقمية في القطاع الحكومي؛ للاستجابة للأزمات، والمساهمة في استمرارية تقديم الخدمات، وتعزيز استقرار الأمن الوطني بالمملكة، حيث يقوم البرنامج بالتأكد من أن كل جهة حكومية تعمل على تطوير خدماتها، وتحويلها من تقليدية إلى إلكترونية، وقياس التحول الرقمي الحكومي لديها، ويشير البرنامج إلى ارتفاع مؤشر نضج الخدمات الحكومية الرقمية التي تقدمها الجهات الحكومية عام ٢٠١٩م ليصل إلى ٢٩، ٨١٪، فقد قيمت جامعة الإمام محمد بن سعود الإسلامية على سبيل المثال في الفئة الخضراء، والتي يتراوح أداؤها في مؤشر نضج الخدمات بين ٨٠٪- ٩٤٪ (جريدة المدينة، ٢٠٢٢م).

كما بادرت العديد من الجامعات السعودية بإنشاء إدارات للأمن السيبراني، وفقاً للأمر السامي الكريم بتاريخ ١٤ / ٨ / ١٤٣٨هـ، والذي ينص على أنه «يجب إنشاء إدارة معنية بالأمن السيبراني في الجهة، مستقلة عن إدارة تقنية المعلومات والاتصالات، ويفضل ارتباطها مباشرة برئيس الجهة أو من ينيبه» (الهيئة الوطنية للأمن السيبراني، ٢٠١٨م: ١٤).

ولكون جامعة الإمام محمد بن سعود الإسلامية من الجامعات العريقة في المملكة العربية السعودية، والتي تعيش التنافس مع نظيراتها من الجامعات السعودية للوصول للعالمية، ينبغي عليها الاهتمام بتحقيق الأمن السيبراني لأنظمة معلوماتها الإدارية؛ للحد من التهديدات والهجمات السيبرانية.

فقد صدر قرار رئيس جامعة الإمام محمد بن سعود الإسلامية بتاريخ ١٩/٦/١٤٤١هـ بإنشاء إدارة الأمن السيبراني في الجامعة، بحيث تتبنى تعزيز الأمن السيبراني، وحماية أصول الجامعة التقنية، وإدارة المخاطر المحتملة ضد المخاطر السيبرانية، لضمان استمرارية أعمال الجامعة التعليمية والبحثية والإدارية (جامعة الإمام محمد بن سعود الإسلامية، ١٤٤٣هـ).

فحجم البيانات والمعلومات الهائلة في الجامعة، واعتمادها على الأنظمة التقنية المتطورة، يدعم أهمية تعزيز الأمن السيبراني، ونشر ثقافة حماية المعلومات بين منسوبي الجامعة؛ لضمان الحماية لمعلوماتها الإدارية، والحد من الهجمات السيبرانية عليها.

### مشكلة الدراسة:

تعرض المؤسسات التعليمية للتهديدات والهجمات السيبرانية، وتستهدف تلك الهجمات أجهزة الحاسب الآلي، والشبكات الإلكترونية، والبنية التحتية المعلوماتية فيها؛ للإضرار بها، أو تعطيلها، أو تعديلها، أو استخدامها بشكل غير مشروع.

وقد أصبحت وسائل الأمان والحماية المحسوسة، وصناديق الحفظ والتخزين لا تكفي وحدها لتحقيق الأمان المنشود لحماية المعلومات (الشايح، ٢٠١٩م: ٤٥).

ويعد قطاع التعليم بمؤسساته المختلفة من أكثر القطاعات المستهدفة بالهجمات السيبرانية، حيث زادت الهجمات عليه في الربع الثالث من العام ٢٠٢٠م بنسبة ١٨٪، مقارنة بالربع الرابع من العام ٢٠١٩م، والتي كانت بنسبة ١٠,١٪ (الهيئة الوطنية للأمن السيبراني، ٢٠٢٢م).

ويشير المركز الوطني للأمن السيبراني في المملكة المتحدة إلى ارتفاع عدد محاولات التسلل إلى المؤسسات التعليمية في المملكة المتحدة، حيث تصدى المركز لعدد من هجمات الفيروسات الإلكترونية التي استهدفت تلك المؤسسات، وسببت اختلالاً على عدة مستويات، تراوحت بحسب مستويات الأمن الموجودة في كل مؤسسة (إندبننت عربية، ٢٠٢٢م).

كما يشير تقرير إدارة الأمن السيبراني في جامعة الإمام محمد بن سعود الإسلامية لعام ٢٠٢٢م إلى حجم الهجمات السيبرانية، فقد تم تصنيف (٧٨٠٠) حدثاً على أنه هجوم، ورصد (٧٩٤) رسالة تصيد، و(١٦٠) اتصالات مشبوهة (إدارة الأمن السيبراني، ٢٠٢٢م: ١٩-٢١).

وعلى الرغم من الجهود المبذولة لوزارة التعليم والمتمثلة في بناء وتطوير برامج أكاديمية في مجال الأمن السيبراني، وسعي الوزارة نحو إعداد وتدريب الكوادر الوطنية في مجال الأمن السيبراني، وجهود العديد من الجامعات السعودية في إنشاء إدارات للأمن السيبراني، تتولى مسؤولية وضع السبل المناسبة لحماية أنظمتها ومعلوماتها الإدارية، إلا أن نتائج بعض الدراسات السابقة أظهرت قصوراً في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، ووجود العديد من المعوقات التي تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في بعض المؤسسات التعليمية، ومنها الجامعات.

وقد أكدت دراسة الشيتي (٢٠١٩م) على وجود معوقات تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، وضعف سياسات حماية أنظمة المعلومات الإدارية بجامعة القصيم، والتي تتمثل في الافتقار لإدارة خاصة تتعلق بأمن المعلومات، إضافة إلى قلة الخبرة والوعي والتدريب للفنيين والموظفين بنظم المعلومات؛ مما أدى إلى حدوث مخاطر عديدة تتعلق بالاخترقات الأمنية، والتهديدات المستمرة لأنظمة الجامعة.

وتوصلت دراسة الخضري وآخرون (٢٠٢٠م) إلى عدم وضع برامج وسياسات محددة لأمن نظم المعلومات الإدارية، وعدم تطبيق معايير حوكمة نظم المعلومات الإدارية.

وتوصلت دراسة السمحان (٢٠٢٠م) إلى ضعف السياسات الأمنية لأنظمة المعلومات الإدارية بالجامعة، وقصور في تطبيق الإجراءات الإدارية اللازمة لتحقيق الأمن السيبراني داخل أنظمة المعلومات الإدارية بالجامعة، وعدم وجود خطة لإدارة مخاطر الأمن السيبراني لأنظمة المعلومات الإدارية بالجامعة، وعدم وجود أنظمة حماية للمعلومات السرية للمستخدم لأنظمة المعلومات الإدارية، وقصور توفير الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات الإدارية.

وأكدت دراسة الشبانان (٢٠٢٠م) وجود نقص في الكوادر البشرية المتخصصة في مجال الأمن السيبراني، وعدم وجود وحدة مختصة بالأمن السيبراني، وعدم وجود برامج للشراكة بين الجامعات من جهة، ومؤسسات المجتمع المدني والقطاع الخاص ذي الصلة من جهة أخرى، وذلك لدعم الجهود الاستباقية المحققة للأمن السيبراني. كما أكدت دراسة المنيع (٢٠٢٢م) على قصور الدعم الفني كأحد متطلبات تنفيذ الأمن السيبراني لأنظمة المعلومات الإدارية، وعدم تحديث برامج التطبيقات الحاسوبية لمنسوبي الجامعات باستمرار، وعدم وجود خطة لإدارة مخاطر الأمن السيبراني لنظم المعلومات الإدارية بالجامعة.

وبناءً على ما سبق من أهمية تحقيق الأمن السيبراني لحماية الأنظمة التقنية، والمعلومات الإدارية في الجامعة، واستناداً إلى نتائج الدراسات السابقة والتي أظهرت وجود معوقات تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في الجامعات، فقد جاءت هذه الدراسة لتقييم مدى تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية.

### أسئلة الدراسة:

- ١- ما واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية من وجهة نظر منسوبي عمادة تقنية المعلومات وإدارة الأمن السيبراني في الجامعة؟
- ٢- ما المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية من وجهة نظر منسوبي عمادة تقنية المعلومات وإدارة الأمن السيبراني في الجامعة؟

- ٣- ما المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية من وجهة نظر منسوبي عمادة تقنية المعلومات وإدارة الأمن السيبراني في الجامعة؟
- ٤- هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (٠,٠٥) فأقل بين آراء أفراد الدراسة حول محاور الدراسة تُعزى لاختلاف متغير (جهة العمل، الجنس، سنوات الخبرة)؟

#### أهداف الدراسة:

- ١- التعرف على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية.
- ٢- الكشف عن المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية.
- ٣- تقديم مقترحات تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية.
- ٤- تفسير الفروق ذات الدلالة الإحصائية عند مستوى الدلالة (٠,٠٥) فأقل بين آراء أفراد الدراسة حول محاور الدراسة تُعزى لاختلاف متغير (جهة العمل، الجنس، سنوات الخبرة).

#### أهمية الدراسة:

#### - الأهمية النظرية:

- أهمية موضوع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، وحمايتها من الهجمات السيبرانية.
- تعرض الجامعات للمخاطر والهجمات السيبرانية؛ مما يتطلب تأمين وحماية البيانات والمعلومات الإلكترونية.
- تقييم المخاطر التي قد تهدد أنظمة المعلومات الإدارية في الجامعات، ومحاولة إيجاد الوسائل والأساليب المناسبة للتغلب عليها.

- قلة الدراسات التي تناولت مجال الأمن السيبراني في التعليم العالي.
- إسهام الدراسة في الجانب البحثي والمعرفي في مجال الأمن السيبراني.



### - الأهمية التطبيقية:

- مساهمة نتائج الدراسة في إفادة صانعي القرار في الجامعات السعودية بالمعلومات اللازمة حول مدى تحقيق الأمن السيبراني؛ لاتخاذ قرارات من شأنها حماية البيانات والمعلومات الإلكترونية.
- مساهمة نتائج الدراسة في توجيه نظر منسوبي إدارة الأمن السيبراني إلى المعوقات التي تحد من تحقيق الأمن السيبراني في الجامعة؛ للعمل على تلافيتها.
- مساهمة نتائج الدراسة في توجيه منسوبي الجامعات السعودية إلى أهمية السعي نحو تحقيق الأمن السيبراني.

### حدود الدراسة:

الحدود الموضوعية: تناولت الدراسة التعرف على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، والكشف عن المعوقات التي تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، وتقديم مقترحات تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية.

الحدود المكانية: طبقت الدراسة على عمادة تقنية المعلومات وإدارة الأمن السيبراني في جامعة الإمام محمد بن سعود الإسلامية.

الحدود البشرية: منسوبي ومنسوبات عمادة تقنية المعلومات، وإدارة الأمن السيبراني في جامعة الإمام محمد بن سعود الإسلامية.

الحدود الزمانية: طبقت الدراسة في الفصل الدراسي الثاني من العام الجامعي ١٤٤٣ هـ.

### مصطلحات الدراسة:

#### الأمن السيبراني:

عرفته الهيئة الوطنية للأمن السيبراني بأنه «حماية الشبكات وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع» (الهيئة الوطنية للأمن السيبراني، ٢٠١٨م: ٣٢).

وتعرفه الباحثة إجرائياً في هذه الدراسة بأنه: مجموعة الإجراءات والعمليات الإدارية، والتقنية المستخدمة لحماية أنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية من أيّ هجمة، أو اختراق، أو تعطيل، أو سوء استخدام.

### أنظمة المعلومات الإدارية:

تُعرف بأنها «مجموعة من العناصر المتداخلة، أو المتفاعلة بعضها مع بعض، والتي تعمل على جمع مختلف أنواع البيانات والمعلومات، وتعمل على معالجتها، وتخزينها، وتجميعها وتوزيعها على المستخدمين بغرض دعم اتخاذ القرارات، وتأمين التنسيق على المنظمة، أو الجهة المستفيدة» (قنديلجي والجنابي، ٢٠٢١م: ٢٧).

وتعرفها الباحثة إجرائياً في هذه الدراسة بأنها: النظم التي تعمل على تهية المعلومات الإدارية، وجمعها، ومعالجتها، وتخزينها، وإنتاج تقارير؛ بهدف تدعيم عملية التخطيط، والتنسيق، وصنع القرار في جامعة الإمام محمد بن سعود الإسلامية.

### الإطار المفهومي:

#### مفهوم الأمن السيبراني:

تعددت تعريفات الأمن السيبراني تبعاً لاختلاف الزاوية التي ينظر إليها كل باحث أو جهة، حيث يُعرف بأنه: «حماية الشبكات وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات، من أي اختراق، أو تعطيل، أو تعديل، أو دخول، أو استخدام، أو استغلال غير مشروع» (الهيئة الوطنية للأمن السيبراني، ٢٠١٨م: ٣٢).

ويُعرف بأنه: مجموعة من الإجراءات التي اتخذت في الدفاع ضد هجمات قرصنة الكمبيوتر وعواقبها، وبما يضمن تنفيذ التدابير والإجراءات المضادة للحماية (بونيف، ٢٠١٩م: ١٢٣).

ويُعرف الأمن السيبراني في الجامعات بأنه: مجموعة الإجراءات والأنشطة الهادفة إلى حماية جميع الأصول الإلكترونية الخاصة بالجامعات، من بيانات، أو أجهزة، أو أنظمة إلكترونية، من استغلالها، أو الإضرار بها بأي شكل من الأشكال، ومعالجة الحاصل بأسرع وقت، وأقل تكلفة (الشبان، ٢٠٢١م: ١٧).

ومما سبق تستخلص الباحثة أهم مقومات الأمن السيبراني، وهي:

- أنه مجموعة من الإجراءات التي تهدف إلى حماية الشبكات، والأنظمة التقنية، والأجهزة، والبيانات.
- يمنع الهجمات الإلكترونية، أو الإضرار، أو سوء الاستخدام للبيانات والمعلومات الإدارية.
- محدد بالبيئة الإلكترونية.
- يضمن معالجة المشكلات التقنية بأسرع وقت، وأقل تكلفة.

#### أهداف الأمن السيبراني:

- يهدف الأمن السيبراني إلى توفير الحماية للشبكات، والأنظمة التقنية، والخدمات الإلكترونية التي تقدمها الجامعات، مما يضمن حماية بياناتها ومعلوماتها الإدارية من أي هجمة سيبرانية.
- ويشير (الجموسي، ٢٠١٦م: ١٢٠) إلى أن الأمن السيبراني يهدف إلى:
- تأمين البنية التحتية لأمن المعلومات والبيانات الخاصة بالطلاب، وأعضاء هيئة التدريس.
  - حماية شبكة المعلومات والاتصالات من أي اختراق محتمل؛ والتي لها دور مهم في تدفق المعلومات والبيانات من مقدم الخدمة إلى مستقبل الخدمة.
  - حماية شبكة المعلومات من أي هجوم محتمل؛ وذلك بمعرفة التقنيات المرتبطة بأمن المعلومات، ومن أهمها؛ كشف رسائل العدو، والعمل الجاد على التصدي لها.
  - تشفير جميع المعاملات الرقمية، بحيث يعجز أيُّ مخترق عن العبث بمحتوياتها.
  - توفير بيئة عمل آمنة، وذلك من خلال العمل الواعي عبر الشبكة العنكبوتية.

وتصنيف (صائع، ٢٠١٨م: ٣٥-٣٦) أهدافاً أخرى هي:

- توفير المتطلبات اللازمة للحد من المخاطر والجرائم السيبرانية.
- مقاومة البرمجيات الخبيثة، وما تستهدفه من إحداث أضرار بالغة بالمستخدمين وبأنظمة المعلومات.
- الحد من التجسس والتخريب الإلكتروني.
- التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها، وسد الثغرات في أنظمة المعلومات.

ولتحقيق تلك الأهداف قامت العديد من الجامعات السعودية بإنشاء إدارات للأمن السيبرانية، لحماية أنظمة معلوماتها الإدارية من المخاطر والهجمات السيبرانية.

وتهدف إدارة الأمن السيبراني في جامعة الإمام محمد بن سعود الإسلامية إلى:

- ضمان استمرارية الأعمال.
- رفع كفاءة الموظفين المعرفية في مجال الأمن السيبراني.
- تحديد الأصول وحمايتها، لضمان سرية ونزاهة وتوافر المعلومات.
- إدارة مخاطر الأمن السيبراني بشكل فعال للحد والتصدي للهجمات.
- الاستعداد والحد من تهديدات الأمن السيبراني.
- تقديم حلول أمن سيبرانية عالية الجودة.
- الالتزام بمعايير الأمن السيبراني العالمية، ومعايير الهيئة الوطنية للأمن السيبراني (إدارة الأمن السيبراني، ٢٠٢٢م: ٤).

وبناءً على ما سبق تجد الباحثة أن الأمن السيبراني - من خلال توفيره الحماية للأنظمة والخدمات الإلكترونية، والبيانات والمعلومات الإدارية في الجامعة، ومنعه للتهديدات والهجمات السيبرانية عليها - يعزز رضا المستفيدين من أعضاء هيئة التدريس والإداريين والطلاب، ويدعم ثقتهم بتلك الأنظمة والخدمات.

### عناصر الأمن السيبراني:

يعتمد الأمن السيبراني على عدة عناصر توفر الحماية للأنظمة التقنية والمعلومات الإدارية، وهي:

**أولاً: السرية والأمن:** وتعني التأكد من أن المعلومات لا تكشف، ولا يطلع عليها أشخاص غير مخولين لذلك. **ثانياً: التكاملية وسلامة المحتوى:** وهو التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله، وعلى نحو خاص لم يتم تدميره أو تغييره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي مع المعلومات أو عن طريق دخول غير مشروع.

**ثالثاً: استمرارية توفر المعلومات أو الخدمة:** إذ يجب التأكد من استمرار عمل النظام المعلوماتي، واستمرار القدرة على التفاعل مع المعلومات، وتقديم الخدمة لمواقع المعلوماتية، وأن المستخدم لن يتعرض إلى منع الاستخدام، أو الدخول إلى النظام.

**رابعاً: عدم إنكار التصرف المرتبط بالمعلومات ممن قام به:** ويقصد به ضمان عدم إنكار الشخص المتصل بالمعلومات أو مواقعها قيامه بتصرف ما، بحيث تتوافر قدرة إثبات هذا التصرف، وأن شخصاً ما في وقت معين قد قام به، وعدم قدرة مستلم رسالة معينة على إنكار استلامه لهذه الرسالة (الصحفي وعسكول، ٢٠١٩م: ٤٩٨-٤٩٩).

وتضيف الباحثة العناصر الآتية:

- **التقنية:** توفر التقنية الحماية اللازمة للأنظمة التقنية، والبيانات والمعلومات الإدارية.
- **الحلول الأمنية:** وذلك من خلال سنّ التشريعات واللوائح التي تكفل وجود فضاء سيبراني آمن، والاستفادة من الشبكات الآمنة، وأنظمة كشف التسلسل لحماية البيانات والمعلومات الإدارية.
- **الأشخاص المؤهلون:** فالأشخاص المؤهلون الذين يتولون مهمة إدارة الأمن السيبراني في المؤسسات المختلفة؛ ومنها الجامعات لهم دور في تحقيق الأمن السيبراني، والحد من الهجمات السيبرانية.

### مفهوم أنظمة المعلومات الإدارية:

تعددت تعريفات أنظمة المعلومات الإدارية من حيث الألفاظ المستخدمة، ولكنها تتفق من حيث المعنى، حيث تُعرف بأنها: نظام متكامل من مدخلات ومعالجة ومخرجات، وتُعدّ حلقة مهمة في الإدارة؛ حيث يُعتمد عليها وبشكل كلي في عمليات اتخاذ القرارات، للوصول إلى أعلى درجات الدقة والمصدقية والواقعية، وذلك لتحقيق أكبر قدر من الإنتاجية الفاعلة لأي منظمة (الشرع، ٢٠١٦م: ١٧).

وعُرفت بأنها: النظم التي تعتمد على الحاسوب في تهيئة البيانات والمعلومات المتعلقة بعمليات نشاطات المنظمة، والتي تقوم على وجود شبكة محلية تربط الحواسيب الموجودة في أماكن مختلفة في المنظمة بعضها مع بعض (الرواشدة، ٢٠١٧م: ١٧).

وعُرفت بأنها: النظم التي تتولى معالجة بيانات الأعمال، وتخزينها، وإنتاج تقارير ومعلومات تُمثل خلاصة لمعاملات المنظمة في مجالاتها الوظيفية (ياسين، ٢٠١٨م: ٢٨).

ومن التعريفات السابقة تستخلص الباحثة أهم ما يميز أنظمة المعلومات الإدارية، وهي كالتالي:

- اعتمادها على الحاسب الآلي في تهيئة البيانات والمعلومات الإدارية.

- أنظمة متكاملة تتألف من مدخلات، وعمليات، ومخرجات.

- تعمل على معالجة بيانات الأعمال، وتخزينها، وإنتاج تقارير.

- يُعتمد عليها في عملية اتخاذ القرارات الإدارية.

### خصائص أنظمة المعلومات الإدارية:

لأنظمة المعلومات الإدارية خصائص متعددة تميزها عن باقي الأنظمة، وهي:

- معالجة وإنتاج البيانات عن طريق عمليات الأعمال في المؤسسة، حيث يتم توفير المعلومات، وتقديم نظم

المعلومات الإدارية تقريراً يعرض الإجراءات والطرق المتبعة لمعالجة البيانات التي تم توليدها.

- تقوم نظم المعلومات بتصميم مواقع العمل عوضاً عن عملية تقسيم الموظفين، حيث يأخذ التصميم بعين الاعتبار مستويات العمل التي يقوم بها الشخص، مع ملاحظة أنها تكون معتمدة بشكل كبير على الهيكل الإداري للمؤسسة.
- تصميم المعلومات لتلبي احتياجات متخذي القرارات داخل المؤسسة في كافة المستويات الدنيا والوسطى والعليا.
- تصميم المعلومات لتناسب جميع المجالات المختلفة كالمالية، وشؤون الموظفين، وغير ذلك من المجالات المتعددة.
- تتميز نظم المعلومات الإدارية بأنها مترابطة ومتكاملة مع قواعد البيانات، ويجب أن يكون هذا التكامل خالياً من التكرار في تخزين البيانات ومعالجتها، بحيث يتم إيجاد نقطة واحدة لإدخال البيانات، ويتم أيضاً تحديث ملفات المعلومات لتتطابق البيانات مع أجهزة الحاسوب (بسيوني، ٢٠١٢م: ٢٣-٢٤).
- ويضيف (الشرع، ٢٠١٦م: ١٩) الخصائص الآتية:
- تعتبر نظم المعلومات الإدارية موجهة لخدمة الرقابة وتقديم التقارير، فهي مخصصة لتقديم التقارير عن العمليات الحالية القائمة، وبالتالي تساعد في الرقابة اليومية على الأنشطة.
- تعتمد نظم المعلومات الإدارية على المعلومات القائمة، وتدفع المعلومات الداخلة للمؤسسة أكثر من المعلومات الخارجة.
- ومما سبق تستنتج الباحثة أن أنظمة المعلومات الإدارية تعتمد بشكل مباشر على قواعد البيانات والمعلومات، وذلك لإنجاز وظائف الإدارة المختلفة من تخطيط وتنظيم، وتنسيق ورقابة، وتقويم واتخاذ للقرارات؛ مما يساهم في تحقيق الأهداف المنشودة بفعالية وكفاءة.

### أنواع أنظمة المعلومات الإدارية:

تتعدد أنواع أنظمة المعلومات الإدارية تبعاً لاختلاف المستوى الإداري الذي تطبق فيه، أو لاختلاف الوظائف الإدارية التي تعتمد فيها تلك الأنظمة، حيث تقسم أنظمة المعلومات الإدارية إلى: (محمد، ٢٠١٩م: ٤٨-٥٠)

### أولاً- حسب المستوى الإداري:

١. نظم معلومات دعم منفي الإدارة العليا: وهي أنظمة تسمح بتحويل البيانات الخاصة بالمؤسسة إلى تقارير ملخصة؛ ليستفيد منها مديرو القسم التنفيذي عن طريق الوصول السريع إلى جميع التقارير الواردة من كافة الإدارات والمستويات في المؤسسة.
٢. نظم دعم القرارات ونظم دعم القرارات الجماعية: وهي أنظمة حاسوبية تقوم بتحليل وعرض بيانات المؤسسة، بحيث تسمح للمستخدمين باتخاذ القرارات بشكل أسرع وأسهل.
٣. نظم قواعد المعرفة والنظم الخبيرة: وهي نظم حاسوبية تساعد على حل المشكلات، بأن تبنى على قاعدة من المعرفة والبيانات المتعلقة بالمؤسسة، حيث تقوم بترجمتها إلى حقائق للوصول إلى أجوبة وحلول.
٤. نظم التقارير الإدارية: وهي نظم حاسوبية تقوم بتحليل ودراسة بيانات المؤسسة بشكل دوري، لتقديم تقارير يومية، أو شهرية، أو سنوية عن بيانات المؤسسة، ويستفيد منها الإداريون.
٥. نظم معالجة المعاملات: وهي نظم حاسوبية تقوم بجمع وتخزين وتعديل معاملات البيانات الخاصة بالمؤسسة.
٦. نظم معلومات المكاتب: وهي نظم حاسوبية تهدف إلى زيادة إنتاجية المكاتب عن طريق جمع وتوزيع، ومعالجة وتخزين الرسائل الإلكترونية، والمستندات.



### ثانياً- حسب الوظائف الإدارية:

١. نظم معلومات التسويق والمبيعات: وهي نظم حاسوبية مصممة لدعم عملية اتخاذ القرارات التسويقية، عن طريق جمع بيانات التسويق الخاصة بالمؤسسة، وتخزينها، وتحليلها، وتوزيعها على المديرين، وفقاً للاحتياجات الإعلامية على أساس منتظم.

٢. نظم معلومات الموارد البشرية: وهي نظم حاسوبية مصممة للمؤسسات الصغيرة، ومتوسطة الحجم، للمساعدة في إدارة أنشطة الموارد البشرية.

٣. نظم معلومات المحاسبة والتمويل: وهي نظم حاسوبية تقوم بجمع وتخزين ومعالجة البيانات المالية، والمحاسبية المستخدمة من قبل صانع القرار، وهو الأسلوب القائم على الحاسوب لتتبع نشاط المحاسبة، بالتعاون مع موارد تكنولوجيا المعلومات؛ لدعم جميع وظائف المحاسبة، والأنشطة بها في ذلك التدقيق، والمحاسبة المالية، وإعداد التقارير، والمحاسبة الإدارية.

٤. نظم معلومات التصنيع والعمليات: وهي نظم حاسوبية تقوم بمساعدة الإدارة في المؤسسة في عمليات ونشاطات إنتاج السلع في كافة مراحلها.

وبناءً على ما سبق تجد الباحثة أن أنظمة المعلومات الإدارية متنوعة، لتخدم المستويات الإدارية المختلفة، ولتُسهم في تحقيق الوظائف الإدارية المتنوعة، حيث تُساعد أنظمة المعلومات الإدارية المؤسسات المختلفة؛ ومنها الجامعات في اتخاذ القرارات الإدارية المناسبة، وحل المشكلات المتنوعة؛ وذلك لاعتمادها على بيانات ومعلومات دقيقة توفرها تلك الأنظمة؛ مما يُسهم في زيادة إنتاجية الجامعة، وتحقيقها لأهدافها المنشودة.

### متطلبات تحقيق الأمن السيراني لأنظمة المعلومات الإدارية في الجامعات:

يعدّ موضوع تحقيق الأمن السيراني لأنظمة المعلومات الإدارية من الموضوعات المهمة التي تتطلب اهتماماً مؤسسياً في كافة المستويات الإدارية؛ ليتم تحقيقه بفعالية وكفاءة عالية، وحتى تضمن الجامعات فاعلية تحقيقه لا بد من مراعاة عددٍ من الضوابط والأسس التي تمثل متطلبات أساسية لتحقيق الأمن السيراني، ويحدد عدد من الباحثين (الخضري وآخرون، ٢٠٢٠م: ٢٣٢)، (البيشي، ٢٠٢١م: ٣٧٠)، (المنيع، ٢٠٢٢م: ١٧٩) أهم تلك المتطلبات بما يلي:

- تطوير البنية التحتية داخل الجامعات، للحد من الاختراق، والقرصنة الإلكترونية.
  - تطوير وتحديث البرامج والتطبيقات المعلوماتية والتقنية باستمرار.
  - امتلاك الجامعة لنظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الإلكترونية.
  - تحديث أنظمة الحماية بصورة منتظمة، لمواكبة التطورات التقنية الحديثة.
  - التوعية بتطبيق معايير أمن المعلومات، لمواجهة أي هجوم أو دخول غير مصرح به على أنظمة المعلومات الإدارية.
  - تحديد المسؤوليات وصلاحيات الوصول لكل فرد.
  - اعتماد آليات توثيق للوثائق العلمية والمراسلات الإدارية والأكاديمية بالجامعات آمنة ومحمية من الاختراق أو التهديدات الإلكترونية.
  - توفير المخصصات المالية لتحقيق الأمن السيبراني.
  - تشديد العقوبات على جرائم الفضاء السيبراني.
  - عقد الدورات التدريبية للموظفين التقنيين لتدريبهم على تطبيق الأمن السيبراني.
- وتضيف الباحثة المتطلبات الآتية:
- توفير موظفين متخصصين بالأمن السيبراني؛ لوضع وتطبيق السياسات والإجراءات اللازمة لتحقيق الأمن السيبراني، ومراقبة مدى التزام منسوبي الجامعة بالمحافظة على أمن الأجهزة، والشبكات، والأنظمة التقنية، والمعلومات الإدارية.
  - تزويد منسوبي الجامعة بصفة مستمرة بالتحديثات على السياسات والإجراءات المتعلقة بأمن المعلومات.
  - تشفير البيانات والمعلومات الإدارية بما يضمن حمايتها من الاختراقات والهجمات السيبرانية.

## الدراسات السابقة:

## - الدراسات العربية:

- أجرت خوجه (٢٠٢٠م) دراسة هدفت إلى تشخيص واقع التطوير التنظيمي في إدارات التعليم في المملكة العربية السعودية لتحقيق الأمن السيبراني، والتعرف على المتطلبات الإدارية الداعمة للأمن السيبراني، والتوصل إلى استراتيجية مقترحة، وقد استخدمت الدراسة المنهج الوصفي المسحي، وتم جمع المعلومات بواسطة الاستبانة والمقابلة، والتي طبقت على (١٠٠) فرد من الموظفين، ومن الخبراء، وأشارت النتائج إلى موافقة أفراد الدراسة بدرجة متوسطة على واقع التطوير التنظيمي في إدارة التعليم لتحقيق الأمن السيبراني، وموافقة أفراد الدراسة بدرجة عالية على المتطلبات الإدارية الداعمة للأمن السيبراني، ومنها: توافر سياسات كلمات المرور، وصلاحيات المستخدمين في نظم المعلومات، والإلزام باستخدام البرامج المرخصة والنسخ الأصلية، ودعم وتأييد الإدارة العليا لجهود تحقيق الأمن السيبراني، وحفظ نسخ احتياطية من الملفات، وتحديد معايير ومؤشرات تحقيق الأمن السيبراني في إدارة التعليم.
- أجرت المنتشري وحريري (٢٠٢٠م) دراسة هدفت إلى التعرف على درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة، وقد استخدمت الدراسة المنهج الوصفي التحليلي، وتم جمع المعلومات بواسطة الاستبانة، والتي طبقت على (٣٦٢) معلمة، وأشارت النتائج إلى أن المعلمات على درجة متوسطة من الوعي بمفاهيم الأمن السيبراني، والتي منها: أحتاج إلى دورات تدريبية في مجال الأمن السيبراني، وأُريد طلب المدرسة من منسوبيها تغيير كلمة المرور بشكل دوري، وأُريد توعية المعلمات في المدرسة بمفاهيم الأمن السيبراني، وبينت النتائج موافقة المعلمات بدرجة متوسطة على انتهاكات الأمن السيبراني، والتي منها: أُريد وضع المدرسة لنظام يمنع الوصول إلى مواقع إلكترونية من الممكن أن تضرّ بحاسبك، وأُريد وضع إجراءات وسياسات لحفظ الأمن السيبراني في المدرسة.

- أجرى الكردي (٢٠٢١م) دراسة هدفت إلى التعرف على واقع الأمن السيبراني والتعليم الإلكتروني في جامعات فلسطين، وقد استخدمت الدراسة المنهج الوصفي، وتم جمع المعلومات بواسطة الاستبانة، والتي طبقت على (٥٠) عضو هيئة تدريس، وأشارت النتائج إلى أن واقع الأمن السيبراني والتعليم الإلكتروني جاء بدرجة متوسطة، حيث تمثلت أبرز العبارات في: رفع شعور الطلبة وإحساسهم بالمساواة في توزيع الفرص في العملية التعليمية.
- أجرت الهندي (٢٠٢١م) دراسة هدفت إلى التعرف على دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، وقد استخدمت الدراسة المنهج الوصفي، وتم جمع المعلومات بواسطة الاستبانة، والتي طبقت على (٩٣) طالبًا من طلاب الدراسات العليا (ماجستير، دكتوراه)، بكلية الدراسات العليا للتربية بجامعة القاهرة، وتوصلت النتائج إلى تقديم تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول.
- أجرت المنيع (٢٠٢٢م) دراسة هدفت إلى التعرف على واقع تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية (٢٠٣٠)، ومعوقاته، ومتطلبات تحقيقه، وقد استخدمت الدراسة المنهج الوصفي التحليلي، وتم جمع المعلومات بواسطة الاستبانة، والتي طبقت على (٢١٠) موظفين تقنيين، وأشارت النتائج إلى موافقة أفراد الدراسة بدرجة متوسطة على واقع تحقيق الأمن السيبراني، كما بينت موافقة أفراد الدراسة بدرجة كبيرة جدًا على معوقات تحقيق الأمن السيبراني، ومنها: تدني مستوى الخبرة لدى الموظفين، واستخدام الأجهزة الشخصية لنقل أو تخزين معلومات سرية خاصة بالجامعة، وبينت النتائج موافقة أفراد الدراسة بدرجة كبيرة جدًا على متطلبات تحقيق الأمن السيبراني، ومنها: تحديث البرامج والتطبيقات المعلوماتية والتقنية باستمرار، وعقد الدورات التدريبية للموظفين التقنيين لتدريبهم على تطبيق الأمن السيبراني.

## - الدراسات الأجنبية:

- أجرى مالاft (Malavet, 2017) دراسة هدفت إلى التعرف على التهديدات السيبرانية الحالية، أو المحتملة التي تواجه مؤسسات التعليم العالي، وأبرز التحديات التي تواجهها، وطرح الحلول للتخفيف من حدوث التهديدات المستقبلية، وقد استخدمت الدراسة المنهج الوصفي بأسلوب دراسة الحالة، وتم جمع المعلومات بواسطة الاستبانة، والتي طبقت على جامعة تكساس، وتوصلت النتائج إلى أن الموارد المستخدمة لمنع انتهاك البيانات ليست دقيقة، والتي أدت إلى العديد من الانتهاكات السيبرانية، وأن أبرز التحديات التي تواجهها تمثلت في: قلة الموارد المالية لإضافة التدابير الوقائية، وضعف برامج توعية منسوبي الجامعة بأهمية الأمن السيبراني، وكيفية التعامل مع التهديدات المحتملة.
- أجرى ويجانتو وبراباو (Wijayanto, & Pranowo, 2020) دراسة هدفت إلى قياس سلوك ضعف الأمن السيبراني خلال جائحة كورونا، وقد استخدمت الدراسة المنهج الوصفي، وتم استخدام مقياس سلوك الأمن السيبراني للمخاطر، والذي طبق على إداريين ومديرين يعملون في جامعات وكليات بمنطقة جافا الوسطى في إندونيسيا، وبينت النتائج أن التنشئة الاجتماعية السوية هي السبيل لتحقيق الأمن السيبراني، وأن هناك حاجة ملحة للأمن السيبراني في ظل متطلبات التحول الرقمي بمختلف المؤسسات التعليمية.

## التعليق على الدراسات السابقة:

- اتفقت الدراسة الحالية مع غالبية الدراسات السابقة في استخدام المنهج الوصفي المسحي كمنهج للبحث والدراسة، فيما عدا دراستي: المنتشري وحريري (٢٠٢٠م)، والمنيع (٢٠٢٢م)، اللتين استخدمتا المنهج الوصفي التحليلي، ودراسة مالاft (Malavet, 2017) التي استخدمت أسلوب دراسة الحالة.
- اتفقت الدراسة الحالية مع الدراسات السابقة في استخدام الاستبانة كأداة للدراسة، فيما عدا دراسة خوجه (٢٠٢٠م) التي استخدمت الاستبانة والمقابلة، ودراسة ويجانتو وبراباو (Wijayanto, & Pranowo, 2020) التي استخدمت مقياس سلوك الأمن السيبراني للمخاطر.

- اتفقت الدراسة الحالية مع الدراسات السابقة في تطبيقها على مؤسسات التعليم العالي، فيما عدا دراستي: خوجه (٢٠٢٠م)، والمنثري وحريري (٢٠٢٠م)، فقد طبقتا على التعليم العام.
- اتفقت الدراسة الحالية مع بعض الدراسات السابقة في بعض أهدافها كدراسة مالافت (Malavet, 2017)، ودراسة الكردي (٢٠٢١م)، ودراسة المنيع (٢٠٢٢م).
- اختلفت الدراسة الحالية عن الدراسات السابقة في تناولها مجال أنظمة المعلومات الإدارية.
- استفادت الدراسة الحالية من الدراسات السابقة في إبراز مشكلة الدراسة، وتحديد منهج الدراسة وأداتها.
- تميزت الدراسة الحالية عن الدراسات السابقة في كونها تسعى إلى تقويم مدى تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية.

#### إجراءات الدراسة:

#### منهج الدراسة:

في ضوء طبيعة الدراسة، وأسئلتها، وأهدافها، تم استخدام المنهج الوصفي المسحي، والذي يُعرف بأنه: ذلك النوع من البحوث الذي يتم بواسطته استجواب جميع أفراد مجتمع البحث، أو عينة كبيرة منهم؛ وذلك بهدف وصف الظاهرة المدروسة، من حيث طبيعتها ودرجة وجودها (العساف، ٢٠١٦م: ١٩١).

#### مجتمع الدراسة:

تكون مجتمع الدراسة من:

- جميع منسوبي عمادة تقنية المعلومات في جامعة الإمام محمد بن سعود الإسلامية في الفصل الدراسي الثاني من العام الجامعي ١٤٤٣هـ، وعددهم (٩٢) موظفًا وموظفة، توزيعهم كالتالي: (٤٥) موظفًا، و(٤٧) موظفة (عمادة تقنية المعلومات، ١٤٤٣هـ، إحصائية غير منشورة).

- جميع منسوبي إدارة الأمن السيبراني في جامعة الإمام محمد بن سعود الإسلامية في الفصل الدراسي الثاني من العام الجامعي ١٤٤٣هـ، وعددهم (١١) موظفًا وموظفة، توزيعهم كالتالي: (٨) موظفين، و(٣) موظفات (إدارة الأمن السيبراني، ١٤٤٣هـ، إحصائية غير منشورة).

ونظرًا لصغر حجم مجتمع الدراسة فقد تم استخدام أسلوب الحصر الشامل لجميع أفراد المجتمع، حيث بلغت الاستجابات من جميع أفراد المجتمع (٦٣) موزعة كالتالي: بلغ عدد المستجيبين من منسوبي عمادة تقنية المعلومات (٥٢)، بنسبة (٥٦،٥٪)، من إجمالي مجتمع منسوبي عمادة تقنية المعلومات، وبلغ عدد المستجيبين من منسوبي إدارة الأمن السيبراني (١١)، بنسبة (١٠،٠٪) من إجمالي مجتمع منسوبي إدارة الأمن السيبراني.

### خصائص أفراد الدراسة وفقًا لمتغيرات الدراسة:

#### ١. توزيع أفراد الدراسة وفقًا لمتغير جهة العمل:

جدول (١): توزيع أفراد الدراسة حسب جهة العمل

التكرار	التكرار			جهة العمل
	المجموع	موظفة	موظف	
٨٢,٥	٥٢	٢٧	٢٥	عمادة تقنية المعلومات
١٧,٥	١١	٣	٨	إدارة الأمن السيبراني
١٠٠	٦٣	٣٠	٣٣	المجموع

يتضح من الجدول (١) أن ٨٢,٥٪ من أفراد الدراسة جهة عملهم عمادة تقنية المعلومات، وأن ١٧,٥٪ منهم جهة عملهم إدارة الأمن السيبراني، وتأتي هذه النتيجة متوافقة مع إحصائية عمادة تقنية المعلومات، وإحصائية إدارة الأمن السيبراني اللتين تشيران إلى أن عدد منسوبي عمادة تقنية المعلومات أكثر من عدد منسوبي إدارة الأمن السيبراني.

## ٢. توزيع أفراد الدراسة وفقاً لمتغير الجنس:

جدول (٢): توزيع أفراد الدراسة حسب الجنس

الجنس	التكرار	النسبة (%)
ذكر	٣٣	٥٢,٤
أنثى	٣٠	٤٧,٦
المجموع	٦٣	١٠٠

يتضح من الجدول (٢) أن ٥٢,٤٪ من أفراد الدراسة كانوا من الذكور، وأن ٤٧,٦٪ منهم كانوا من الإناث، وتأتي هذه النتيجة متوافقة مع إحصائية عمادة تقنية المعلومات، وإحصائية إدارة الأمن السيبراني اللتين تشيران إلى تقارب إجمالي عدد الذكور في عمادة تقنية المعلومات وإدارة الأمن السيبراني مع إجمالي عدد الإناث في عمادة تقنية المعلومات وإدارة الأمن السيبراني.

## ٣. توزيع أفراد الدراسة وفقاً لمتغير سنوات الخبرة:

جدول (٣): توزيع أفراد الدراسة حسب سنوات الخبرة

سنوات الخبرة	التكرار	النسبة (%)
أقل من ٥ سنوات	١٧	٢٧
٥-١٠ سنوات	٢٢	٣٤,٩
أكثر من ١٠ سنوات	٢٤	٣٨,١
المجموع	٦٣	١٠٠

يتضح من الجدول (٣) أن ٣٨,١٪ من أفراد الدراسة سنوات خبرتهم أكثر من ١٠ سنوات، وأن ٣٤,٩٪ منهم سنوات خبرتهم من ٥ - ١٠ سنوات، وأن ٢٧٪ منهم سنوات خبرتهم أقل من ٥ سنوات، وقد يرجع ذلك إلى أن غالبية أفراد الدراسة من موظفي وموظفات عمادة تقنية المعلومات والتي أنشئت قبل أكثر من ١٠ سنوات، في حين لم يمضِ على إنشاء إدارة الأمن السيبراني إلا أقل من ٣ سنوات.



### أداة الدراسة:

في ضوء الاطلاع على الأدبيات التربوية، والدراسات السابقة ذات العلاقة بموضوع الدراسة، قامت الباحثة بتصميم استبانة على الشكل المغلق الذي يحدد الاستجابات المحتملة لكل عبارة، حيث تم استخدام المقياس المتدرج الخماسي للحصول على استجابات أفراد الدراسة، وفق درجات الموافقة الآتية: موافقة بدرجة عالية جداً (٥)، عالية (٤)، متوسطة (٣)، منخفضة (٢)، منخفضة جداً (١).

ولتحديد طول فئات المقياس المتدرج الخماسي (الحدود الدنيا والعليا) المستخدم في محاور الدراسة، تم حساب المدى (٥-١=٤)، ثم تقسيمه على عدد فئات المقياس (٤/٥ = ٠,٨٠)، وتم إضافة هذه القيمة إلى أقل قيمة في المقياس وهي (١)؛ لتحديد الحد الأعلى لهذه الفئة، وهكذا أصبح طول الفئات كما هو موضح في الجدول (٤):

جدول (٤): تحديد فئات المقياس المتدرج الخماسي

منخفضة جداً	منخفضة	متوسطة	عالية	عالية جداً
١,٨٠-١	١,٨١- ٢,٦٠	٢,٦١-٣,٤٠	٣,٤١-٤,٢٠	٤,٢١-٥

### صدق أداة الدراسة:

قامت الباحثة بالتأكد من صدق الاستبانة من خلال:

أ. **الصدق الظاهري:** عرض الاستبانة في صورتها الأولية على ذوي الخبرة في تخصص الإدارة التربوية، والطلب منهم التفضل بإبداء ملاحظاتهم حول مدى وضوح ومناسبة عباراتها لأهداف الدراسة، وبناء على مقترحاتهم، تم تعديل بعض عباراتها، بحيث صيغت بصورتها النهائية على النحو التالي:

- الجزء الأول: ويشمل متغيرات الدراسة؛ (جهة العمل، الجنس، سنوات الخبرة).

- الجزء الثاني: ويتكون من:

١. واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، (١٦) عبارة.

٢. المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، (١٣) عبارة.

٣. المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، (١٣) عبارة.

ب. صدق الاتساق الداخلي: للتأكد من صدق الاتساق الداخلي تم حساب معامل الارتباط (بيرسون)؛ وذلك لقياس العلاقة بين درجة كل عبارة والدرجة الكلية للمحور الذي تنتمي إليه. كما يوضح ذلك الجدول (٥):

جدول (٥): معاملات الارتباط لكل عبارة من عبارات المحور بالدرجة الكلية للمحور الذي تنتمي إليه

معامل الارتباط			٢
المحور الثالث	المحور الثاني	المحور الأول	
**٠,٨٤٠	**٠,٦٠١	**٠,٧٨٤	١
**٠,٨١٦	**٠,٥٠٨	**٠,٧٢٠	٢
**٠,٨٢٦	**٠,٤٩٩	**٠,٦٨٤	٣
**٠,٦٢٢	**٠,٦٨٩	**٠,٥٦٣	٤
**٠,٧١٩	**٠,٧٣٢	**٠,٨٣٢	٥
**٠,٨٠٦	**٠,٧٩٣	**٠,٧٥٣	٦
**٠,٨١٤	**٠,٧٥٢	**٠,٧٢٦	٧
**٠,٨٠٢	**٠,٧٠١	**٠,٧٩٣	٨
**٠,٨٤٢	**٠,٥٩٨	**٠,٦٢٩	٩
**٠,٨٠٠	**٠,٧٦٨	**٠,٧٢٠	١٠

معامل الارتباط			م
المحور الثالث	المحور الثاني	المحور الأول	
**٠, ٨٨٠	**٠, ٧٢٧	**٠, ٧١٩	١١
**٠, ٦٤٦	**٠, ٦٩٦	**٠, ٦٣٩	١٢
**٠, ٨٠٧	**٠, ٥٢٥	**٠, ٨٦١	١٣
		**٠, ٤٥٨	١٤
		**٠, ٧٧٠	١٥
		**٠, ٥٧١	١٦

(\*\*) دالة عند ٠,٠١

يتضح من الجدول (٥) أن قيم معاملات ارتباط بيرسون لقياس العلاقة بين درجة كل عبارة والدرجة الكلية للمحور الذي تنتمي إليه دالة إحصائية عند مستوى الدلالة (٠,٠١)؛ مما يدل على صدق الاتساق الداخلي للاستبانة، ومناسبتها لقياس ما وضعت لقياسه.

#### ثبات أداة الدراسة:

للتأكد من ثبات الاستبانة تم استخدام معامل الثبات ألفا كرونباخ. كما يوضح ذلك الجدول (٥):

جدول (٦): معامل ألفا كرونباخ لقياس ثبات أداة الدراسة

معامل الثبات	المحور
٠,٩٢٩	واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية
٠,٨٩١	المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية
٠,٩٤٧	المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية
٠,٨٦٢	الثبات العام

يتضح من الجدول (٦) أن قيم معاملات الثبات مرتفعة، إذ بلغ معامل الثبات العام (٠,٨٦٢)، وهذا يدل على أن الاستبانة على درجة عالية من الثبات، ويمكن الاعتماد عليها في الحصول على المعلومات الخاصة بالدراسة.

### أساليب المعالجة الإحصائية:

١. التكرارات والنسبة المئوية: لوصف خصائص أفراد الدراسة.
٢. المتوسطات الحسابية: لمعرفة مدى ارتفاع أو انخفاض استجابات أفراد الدراسة عن محاور الدراسة.
٣. الانحرافات المعيارية: لمعرفة مدى تشتت استجابات أفراد الدراسة عن متوسطها الحسابي.
٤. معامل ارتباط بيرسون: للتحقق من صدق الاتساق الداخلي للاستبانة.
٥. معامل ألفا كرونباخ: لحساب ثبات الاستبانة.
٦. اختبار مان - ويتني (Mann-Whitney): لمعرفة الفروق الإحصائية.
٧. اختبارات (T): لمعرفة الفروق الإحصائية.
٨. اختبار كروسكال - والس (Kruskal - Wallis): لمعرفة الفروق الإحصائية.

### نتائج الدراسة ومناقشتها:

إجابة السؤال الأول: ما واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية من وجهة نظر منسوبي عمادة تقنية المعلومات وإدارة الأمن السيبراني في الجامعة؟  
للتعرف على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، تم تحليل استجابات أفراد الدراسة، وذلك على النحو التالي:

تحقيق الأمن السيرياني لأنظمة المعلومات الإدارية  
في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقويمية

العدد العشرون – يناير 2023م

د. الجوهرة بنت عثمان بن علي الركبان

جدول (٧): نتائج استجابات أفراد الدراسة حول واقع تحقيق الأمن السيرياني لأنظمة المعلومات الإدارية  
في جامعة الإمام محمد بن سعود الإسلامية

م	العبارة	درجة الموافقة					المتوسط	الانحراف المعياري	الترتيب	درجة الموافقة
		عالية جداً	عالية	متوسطة	منخفضة	منخفضة جداً				
١٤	تنبيه الجامعة منسوبها إلى عدم استخدام البريد الإلكتروني الرسمي في مواقع التواصل الاجتماعي	ك	٤١	١٧	٥	٠	٤,٥٧	٠,٦٤٠	١	عالية جداً
		%	٦٥,١	٢٧	٧,٩	٠				
١١	تنبيه الجامعة منسوبها من التعامل مع رسائل البريد الإلكتروني مجهولة المصدر	ك	٣٤	٢٤	٥	٠	٤,٤٦	٠,٦٤٣	٢	عالية جداً
		%	٥٤	٣٨,١	٧,٩	٠				
٤	تضع الجامعة نظاماً يمنع الوصول إلى المواقع الإلكترونية غير الآمنة	ك	٣٣	٢٥	٥	٠	٤,٤٤	٠,٦٤٢	٣	عالية جداً
		%	٥٢,٤	٣٩,٧	٧,٩	٠				
٩	توجه الجامعة منسوبها إلى اختيار كلمات مرور قوية تحتوي حروفاً وأرقاماً ورموزاً	ك	٣٣	٢٤	٤	٢	٤,٣٩	٠,٧٥٢	٤	عالية جداً
		%	٥٢,٤	٣٨,١	٦,٣	٣,٢				
١٥	توفر الجامعة الدعم الفني اللازم لمنسوبها لمعالجة المشكلات التقنية	ك	٢٩	٢٤	١٠	٠	٤,٣٠	٠,٧٣٢	٥	عالية جداً
		%	٤٦	٣٨,١	١٥,٩	٠				
١٣	توجه الجامعة منسوبها إلى استخدام البرامج المعتمدة والموثوقة	ك	٣٤	١٧	٩	٣	٤,٣٠	٠,٨٩١	٦	عالية جداً
		%	٥٤	٢٧	١٤,٣	٤,٨				
١٠	توجه الجامعة منسوبها إلى تحديث كلمات المرور باستمرار	ك	٢٧	٢٣	٨	٤	٤,١٢	٠,٩٧٥	٧	عالية جداً
		%	٤٢	٣٦,٥	١٢,٧	٦,٣				

عالية	٨	٠,٨٠٥	٤,١١	١	٢	٥	٣٦	١٩	ك	تعتمد الجامعة سياسة سبرانية تحد من التجسس والاختراق لأنظمتها الإدارية	١
				١,٦	٣,٢	٧,٩	٥٧,١	٣٠,٢	%		
عالية	٩	٠,٧٤٧	٤,٠٧	٠	٣	٦	٣٧	١٧	ك	توظف الجامعة نظامًا شبكيًا آمنًا لتبادل المعلومات بين منسوبيها	٢
				٠	٤,٨	٩,٥	٥٨,٧	٢٧	%		
عالية	١٠	٠,٩٤٨	٤,٠٦	١	٥	٥	٣٠	٢٢	ك	تهتم الجامعة بحماية المعلومات الشخصية لمنسوبيها	٥
				١,٦	٧,٩	٧,٩	٤٧,٦	٣٤,٩	%		
عالية	١١م	٠,٨١١	٤,٠٤	٠	٢	١٣	٢٨	٢٠	ك	تحديث الجامعة أنظمتها الإلكترونية باستمرار	٣
				٠	٣,٢	٢٠,٦	٤٤,٤	٣١,٧	%		
عالية	١١م	٠,٨١١	٤,٠٤	٠	٢	١٣	٢٨	٢٠	ك	تعتمد الجامعة آليات لاكتشاف نقاط الضعف التي تهدد الأمن السبراني	٦
				٠	٣,٢	٢٠,٦	٤٤,٤	٣١,٧	%		
عالية	١٣	١,٠٢	٤,٠٤	٢	٤	٧	٢٦	٢٤	ك	توجه الجامعة منسوبيها إلى استخدام برامج خاصة لحماية الحاسب من الاختراق	١٢
				٣,٢	٦,٣	١١,١	٤١,٣	٣٨,١	%		
عالية	١٤	٠,٩٨١	٣,٩٣	٢	١	١٧	٢٢	٢١	ك	تحتفظ الجامعة بنسخ احتياطية للملفات والمعلومات الإدارية	٧
				٣,٢	١,٦	٢٧	٣٤,٩	٣٣,٣	%		
عالية	١٥	٠,٩٣٨	٣,٩٢	١	٤	١٢	٢٨	١٨	ك	توفر الجامعة الصيانة الدورية لأجهزة الحاسب الآلي	٨
				١,٦	٦,٣	١٩	٤٤,٤	٢٨,٦	%		

متوسطة	١٦	١,١٢	٣,٣٩	٥	٦	٢٢	١٩	١١	ك	تنظم الجامعة دورات	١٦
				٧,٩	٩,٥	٣٤,٩	٣٠,٢	١٧,٥	%	تدريبية لمنسوبيها للتوعية بالأمن السيبراني	
عالية	المتوسط الحسابي العام = ١٤,٤، الانحراف المعياري العام = ٥,٥٩٣										

يتضح من الجدول (٧) موافقة أفراد الدراسة بدرجة عالية على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، وذلك بمتوسط حسابي عام (٤,١٤)، كما بلغ الانحراف المعياري العام (٥,٥٩٣)؛ مما يدل على تجانس استجابات أفراد الدراسة، حيث تراوحت متوسطات الاستجابات بين (٣,٣٩) و(٤,٥٧)، وهي متوسطات تتراوح ما بين موافق بدرجة متوسطة، وموافق بدرجة عالية جداً، حيث يتضح من النتائج موافقة أفراد الدراسة بدرجة عالية جداً على ست عبارات من أهمها:

جاءت العبارة (تنبه الجامعة منسوبيها إلى عدم استخدام البريد الإلكتروني الرسمي في مواقع التواصل الاجتماعي) في المرتبة الأولى بمتوسط حسابي (٤,٥٧)، حيث تفسر هذه النتيجة حرص الجامعة على توعية منسوبيها بعدم استخدام البريد الإلكتروني في مواقع التواصل الاجتماعي، وأن يقتصر استخدامه في التعاملات الأكاديمية والإدارية فقط.

جاءت العبارة (تنبه الجامعة منسوبيها من التعامل مع رسائل البريد الإلكتروني مجهولة المصدر) في المرتبة الثانية بمتوسط حسابي (٤,٤٦)، حيث تفسر هذه النتيجة حرص الجامعة على توعية منسوبيها بعدم التعامل مع رسائل البريد الإلكتروني مجهولة المصدر، حتى لا يحدث اختراق لأنظمة وشبكات الجامعة من خلال البريد الإلكتروني لمنسوبيها.

جاءت العبارة (تضع الجامعة نظاماً يمنع الوصول إلى المواقع الإلكترونية غير الآمنة) في المرتبة الثالثة بمتوسط حسابي (٤,٤٤)، حيث تفسر هذه النتيجة سعي الجامعة إلى الاستفادة من الأنظمة التقنية الحديثة، لمنع دخول منسوبيها إلى مواقع إلكترونية قد تضر بأجهزة وأنظمة الجامعة الإلكترونية.

ويتضح من النتائج موافقة أفراد الدراسة بدرجة متوسطة على عبارة واحدة، وهي (تنظم الجامعة دورات تدريبية لمسوييها للتوعية بالأمن السيبراني) التي جاءت في المرتبة السادسة عشرة بمتوسط حسابي (٣٩, ٣)، حيث تفسر هذه النتيجة قلة الدورات التدريبية لتوعية منسوبي الجامعة بضرورة تحقيق الأمن السيبراني، وأهمية أن تعمل الجامعة على تكثيف البرامج التدريبية لتوعية منسوبي الجامعة بالوسائل والأساليب اللازمة لتحقيق الأمن السيبراني، والحد من الهجمات السيبرانية.

يتضح من هذه النتيجة موافقة أفراد الدراسة بدرجة عالية على واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، وهذا يدل على سعي الجامعة نحو تحقيق الأمن السيبراني لأنظمة معلوماتها الإدارية، وذلك من خلال سن الأنظمة والقواعد المنظمة لاستخدام الخدمات الإلكترونية، وتطبيق الأساليب والاستراتيجيات المختلفة لحماية بياناتها وأنظمتها وبرامجها من المخاطر والهجمات السيبرانية، وتختلف هذه النتيجة عن نتيجة دراسة حوجه (٢٠٢٠م) التي بينت موافقة أفراد الدراسة بدرجة متوسطة على واقع التطوير التنظيمي في إدارة التعليم لتحقيق الأمن السيبراني، وتختلف مع نتيجة دراسة الكردي (٢٠٢١م) التي أشارت إلى أن واقع الأمن السيبراني في جامعات فلسطين جاء بدرجة متوسطة، كما تختلف مع نتيجة دراسة المنيع (٢٠٢٢م) التي أشارت إلى موافقة أفراد الدراسة بدرجة متوسطة على واقع تحقيق الأمن السيبراني.

إجابة السؤال الثاني: ما المعوقات التي تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية من وجهة نظر منسوبي عمادة تقنية المعلومات وإدارة الأمن السيبراني في الجامعة؟  
للكشف عن المعوقات التي تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، تم تحليل استجابات أفراد الدراسة، وذلك على النحو التالي:



تحقيق الأمن السيراني لأنظمة المعلومات الإدارية  
في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقويمية

العدد العشرون – يناير 2023م

د. الجوهرة بنت عثمان بن علي الركبان

جدول (٨): نتائج استجابات أفراد الدراسة حول المعوقات التي تحدّ من تحقيق الأمن السيراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية

م	العبارة	درجة الموافقة					المتوسط	الانحراف المعياري	الترتيب	درجة الموافقة
		عالية جداً	عالية	متوسطة	منخفضة	منخفضة جداً				
٤	قلة وعي منسوبي الجامعة بمخاطر الأمن السيراني	ك	٧	٢٤	٢٢	٦	٤	٣,٣٨	١	متوسطة
		%	١١,١	٣٨,١	٣٤,٩	٩,٥	٦,٣			
٩	استخدام منسوبي الجامعة كلمات مرور ضعيفة عند الدخول لحساباتهم الرسمية	ك	٧	١٧	١٨	١٥	٦	٣,٠٦	٢	متوسطة
		%	١١,١	٢٧	٢٨,٦	٢٣,٨	٩,٥			
١٣	ندرة الدورات التدريبية للتوعية بأهمية تحقيق الأمن السيراني	ك	٥	١٤	٢٦	١١	٧	٢,٩٨	٣	متوسطة
		%	٧,٩	٢٢,٢	٤١,٣	١٧,٥	١١,١			
١	قصور البنية التحتية في الجامعة عن تحقيق الأمن السيراني	ك	١	٨	٣٠	٢٠	٤	٢,٧١	٤	متوسطة
		%	١,٦	١٢,٧	٤٧,٦	٣١,٧	٦,٣			

متوسطة	٥	١,٢٧	٢,٦٥	١٥	١٦	١٢	١٦	٤	ك	استخدام منسوبي الجامعة البريد الإلكتروني الرسمي عند التسجيل في مواقع التواصل الاجتماعي	١١
				٢٣,٨	٢٥,٤	١٩	٢٥,٤	٦,٣	%		
منخفضة	٦	١,٠٤	٢,٦٠	٩	٢٢	١٩	١١	٢	ك	ضعف استخدام منسوبي الجامعة لبرامج حماية الحاسب من الاختراق	٧
				١٤,٣	٣٤,٩	٣٠,٢	١٧,٥	٣,٢	%		
منخفضة	٧	٠,٩٦٣	٢,٥٥	٧	٢٦	٢٠	٨	٢	ك	ضعف الأنظمة التقنية المستخدمة في الجامعة	٢
				١١,١	٤١,٣	٣١,٧	١٢,٧	٣,٢	%		
منخفضة	٨	١,٢٤	٢,٥٠	١٧	١٥	١٨	٨	٥	ك	استخدام منسوبي الجامعة برامج غير موثوقة	١٠
				٢٧	٢٣,٨	٢٨,٦	١٢,٧	٧,٩	%		
منخفضة	٩	١,٠١	٢,٤٩	١٠	٢٤	١٩	٨	٢	ك	ضعف الصيانة الدورية لأجهزة الحاسب الآلي	٨
				١٥,٩	٣٨,١	٣٠,٢	١٢,٧	٣,٢	%		

منخفضة	١٠	١,٢٩	٢,٤٧	١٨	١٨	١١	١١	٥	ك	الدخول إلى المواقع الإلكترونية غير الآمنة	١٢
				٢٨,٦	٢٨,٦	١٧,٥	١٧,٥	٧,٩	%		
منخفضة	١١	٠,٩٠٠	٢,٣٤	٩	٣١	١٦	٦	١	ك	ضعف البرامج المستخدمة لحماية الأنظمة التشغيلية في الجامعة	٣
				١٤,٣	٤٩,٢	٢٥,٤	٩,٥	١,٦	%		
منخفضة	١٢	٠,٨٨٣	٢,٢٧	١٣	٢٥	٢٠	٥	٠	ك	قصور الدعم الفني عن معالجة المشكلات التقنية	٦
				٢٠,٦	٣٩,٧	٣١,٧	٧,٩	٠	%		
منخفضة	١٣	١,٠١	٢,٢٠	١٨	٢٣	١٣	٩	٠	ك	قلة تحديث الأنظمة الإلكترونية في الجامعة	٥
				٢٨,٦	٣٦,٥	٢٠,٦	١٤,٣	٠	%		
متوسطة	المتوسط الحسابي العام = ٦٣, ٢، الانحراف المعياري العام = ٠,٧٠٢										

يتضح من الجدول (٨) موافقة أفراد الدراسة بدرجة متوسطة على المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، وذلك بمتوسط حسابي عام (٢, ٦٣)، كما بلغ الانحراف المعياري العام (٠,٧٠٢)؛ مما يدل على تجانس استجابات أفراد الدراسة، حيث تراوحت متوسطات الاستجابات بين (٢, ٢٠) و(٣, ٣٨)، وهي متوسطات تتراوح ما بين موافق بدرجة منخفضة، وموافق بدرجة متوسطة، حيث يتضح من النتائج موافقة أفراد الدراسة بدرجة متوسطة على خمس عبارات من أهمها:

جاءت العبارة (قلة وعي منسوبي الجامعة بمخاطر الأمن السيبراني) في المرتبة الأولى بمتوسط حسابي (٣, ٣٨)، حيث تفسّر هذه النتيجة أهمية أن تعمل الجامعة على توعية منسوبيها بمخاطر التهديدات والهجمات السيبرانية من خلال عقد الدورات التدريبية، وورش العمل المتخصصة. جاءت العبارة (استخدام منسوبي الجامعة كلمات مرور ضعيفة عند الدخول لحساباتهم الرسمية) في المرتبة الثانية بمتوسط حسابي (٣, ٠٦)، وقد تُعزى هذه النتيجة إلى عدم إدراك بعض منسوبي الجامعة أهمية اختيار كلمات مرور قوية لحساباتهم الرسمية، بحيث يصعب اختراقها والوصول إليها، على الرغم من توجيه الجامعة باستمرار منسوبيها إلى اختيار كلمات مرور قوية.

ويتضح من النتائج موافقة أفراد الدراسة بدرجة منخفضة على ثماني عبارات من أهمها:

جاءت العبارة (قصور الدعم الفني عن معالجة المشكلات التقنية) في المرتبة الثانية عشرة بمتوسط حسابي (٢, ٢٧)، حيث تفسّر هذه النتيجة توفر فريق الدعم الفني في الجامعة، لمعالجة المشكلات التقنية الطارئة طيلة أيام العمل، وبالتالي لا يعد هذا الأمر معوقاً.

جاءت العبارة (قلة تحديث الأنظمة الإلكترونية في الجامعة) في المرتبة الثالثة عشرة بمتوسط حسابي (٢, ٢٠)، حيث تفسّر هذه النتيجة سعي الجامعة إلى تحديث وتطوير أنظمتها وخدماتها الإلكترونية بشكل مستمر، وبالتالي لا يعد هذا الأمر معوقاً.

يتضح من هذه النتيجة موافقة أفراد الدراسة بدرجة متوسطة على المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، وهذا يدل على وجود بعض المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في الجامعة، الأمر الذي يتطلب السعي نحو إيجاد الحلول المناسبة لمواجهة تلك المعوقات، بما يضمن حماية معلومات وأنظمة وشبكات الجامعة من الاختراقات والتهديدات السيبرانية، وتتفق هذه النتيجة مع نتيجة دراسة المنتشري وحريري (٢٠٢٠م) التي بينت موافقة المعلمات بدرجة متوسطة على انتهاكات الأمن السيبراني، بينما تختلف هذه النتيجة مع نتيجة دراسة المنيع

تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية  
في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقييمية

العدد العشرون – يناير 2023م

د. الجوهرة بنت عثمان بن علي الركبان

(٢٠٢٢م) التي بينت موافقة أفراد الدراسة بدرجة كبيرة جداً على معوقات تحقيق الأمن السيبراني، ومنها؛ تدني مستوى الخبرة لدى الموظفين، واستخدام الأجهزة الشخصية لنقل أو تخزين معلومات سرية خاصة بالجامعة.

إجابة السؤال الثالث: ما المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية من وجهة نظر منسوبي عمادة تقنية المعلومات وإدارة الأمن السيبراني في الجامعة؟

للتعرف على المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام

محمد بن سعود الإسلامية، تم تحليل استجابات أفراد الدراسة، وذلك على النحو التالي:

جدول (٩): نتائج استجابات أفراد الدراسة حول المقترحات التي تُسهم في تحقيق الأمن السيبراني

لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية

م	العبارة	درجة الموافقة					الانحراف المعياري	الترتيب	درجة الموافقة
		عالية جداً	عالية	متوسطة	منخفضة	منخفضة جداً			
٤	تحديث برامج الحماية في أجهزة الحاسب بالجامعة بشكل تلقائي	ك	٢٦	٢٦	٦	٥	٠	١	عالية
		%	٤١,٣	٤١,٣	٩,٥	٧,٩	٠		
٥	إيجاد آليات للتعامل مع مخاطر الأمن السيبراني	ك	٢٢	٢٨	١٢	١	٠	٢	عالية
		%	٣٤,٩	٤٤,٤	١٩	١,٦	٠		
٣	تحديث الأنظمة التقنية في الجامعة بصفة مستمرة لسد الثغرات	ك	٢١	٢٧	١١	٤	٠	٣	عالية
		%	٣٣,٣	٤٢,٩	١٧,٥	٦,٣	٠		

عالية	٤	٠,٧٨٢	٤	٠	٢	١٣	٣١	١٧	ك	الاعتماد على برامج متطورة لحماية الأنظمة التشغيلية في الجامعة	٢
				٠	٣,٢	٢٠,٦	٤٩,٢	٢٧	%		
عالية	٥	١,٠٢	٣,٩٢	١	٤	١٧	١٨	٢٣	ك	الالتزام بأنظمة وتعليقات الجهات الوطنية المختصة بالأمن السيبراني	١٣
				١,٦	٦,٣	٢٧	٢٨,٦	٣٦,٥	%		
عالية	٦	٠,٩٣٦	٣,٨٤	١	٤	١٥	٢٧	١٦	ك	توعية منسوبي الجامعة بالمخاطر والتهديدات السيبرانية	١٠
				١,٦	٦,٣	٢٣,٨	٤٢,٩	٢٥,٤	%		
عالية	٧	٠,٩٥٣	٣,٨٤	١	٤	١٦	٢٥	١٧	ك	تطوير البنية التحتية في الجامعة باستمرار لتتلاءم مع تحقيق الأمن السيبراني	١
				١,٦	٦,٣	٢٥,٤	٣٩,٧	٢٧	%		
عالية	٨	١,٠١	٣,٨١	١	٥	١٨	٢٠	١٩	ك	توفير الدعم الفني الفوري لمعالجة المشكلات التقنية الطارئة	١١
				١,٦	٧,٩	٢٨,٦	٣١,٧	٣٠,٢	%		

عالية	٩	٠,٩٦٩	٣,٧٩	١	٦	١٣	٢٨	١٥	ك	توجيه الجامعة المستفيدين من أنظمتها إلى طرق حماية وأمن المعلومات	٨
				١,٦	٩,٥	٢٠,٦	٤٤,٤	٢٣,٨	%		
عالية	١٠	٠,٩٨٣	٣,٧٤	٢	٤	١٦	٢٧	١٤	ك	إيجاد آليات تخزين آمنة للملفات والوثائق الإدارية	٩
				٣,٢	٦,٣	٢٥,٤	٤٢,٩	٢٢,٢	%		
عالية	١١	١,١٢	٣,٧١	٤	٥	١٢	٢٦	١٦	ك	تخصيص ميزانية لدعم تحقيق الأمن السيبراني في الجامعة	٦
				٦,٣	٧,٩	١٩	٤١,٣	٢٥,٤	%		
متوسطة	١٢	١,٢٩	٣,٣٣	١٠	١	٢٤	١٤	١٤	ك	استقطاب كفاءات بشرية في مجال الأمن السيبراني	٧
				١٥,٩	١,٦	٣٨,١	٢٢,٢	٢٢,٢	%		
متوسطة	١٣	١,٠١	٣,٣٠	٣	٨	٢٧	١٧	٨	ك	عقد الدورات التدريبية للتعريف بطرق تحقيق الأمن السيبراني	١٢
				٤,٨	١٢,٧	٤٢,٩	٢٧	١٢,٧	%		
عالية	المتوسط الحسابي العام = ٣,٨١، الانحراف المعياري العام = ٠,٧٦٦										

يتضح من الجدول (٩) موافقة أفراد الدراسة بدرجة عالية على المقترحات التي تُسهم في تحقيق الأمن

السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، وذلك بمتوسط حسابي عام

(٨١, ٣)، كما بلغ الانحراف المعياري العام (٧٦٦, ٠)؛ مما يدل على تجانس استجابات أفراد الدراسة، حيث تراوحت متوسطات الاستجابات بين (٣, ٣٠) و(٤, ١٥)، وهي متوسطات تتراوح ما بين موافق بدرجة متوسطة، وموافق بدرجة عالية، حيث يتضح من النتائج موافقة أفراد الدراسة بدرجة عالية على إحدى عشرة عبارة من أهمها:

جاءت العبارة (تحديث برامج الحماية في أجهزة الحاسب بالجامعة بشكل تلقائي) في المرتبة الأولى بمتوسط حسابي (٤, ١٥)، حيث تفسر هذه النتيجة أهمية أن تستفيد الجامعة من الأنظمة التقنية المتطورة، والتي تعمل على تحديث برامج الحماية في أجهزة الحاسب الآلي في الجامعة بشكل تلقائي، ودون إشعار لمستخدمي تلك الأجهزة بضرورة تحديث البرامج.

جاءت العبارة (إيجاد آليات للتعامل مع مخاطر الأمن السيبراني) في المرتبة الثانية بمتوسط حسابي (٤, ١٢)، حيث تفسر هذه النتيجة أهمية أن تعمل الجامعة ممثلة بإدارة الأمن السيبراني على وضع سياسات واستراتيجيات للتعامل الفوري مع التهديدات والهجمات السيبرانية، وأن توعي منسوبيها باستمرار بمخاطر تلك الهجمات على أنظمة وبيانات وخدمات الجامعة الإلكترونية، كما يجب أن تعمل على تحديث وتطوير تلك الآليات بصفة مستمرة.

ويتضح من النتائج موافقة أفراد الدراسة بدرجة متوسطة على عبارتين، وهما:

جاءت العبارة (استقطاب كفاءات بشرية في مجال الأمن السيبراني) في المرتبة الثانية عشرة بمتوسط حسابي (٣, ٣٣)، حيث تفسر هذه النتيجة أهمية الاستفادة من الخبرات البشرية المتخصصة في مجال الأمن السيبراني، في تدعيم تحقيق الأمن السيبراني في الجامعة، والحد من التهديدات والهجمات السيبرانية.



جاءت العبارة (عقد الدورات التدريبية للتعريف بطرق تحقيق الأمن السيبراني) في المرتبة الثالثة عشرة بمتوسط حسابي (٣٠, ٣)، حيث تفسّر هذه النتيجة أهمية أن تعمل الجامعة على تكثيف البرامج التدريبية لتوعية منسوبي الجامعة بالوسائل والأساليب اللازمة لتحقيق الأمن السيبراني.

ويتضح من هذه النتيجة موافقة أفراد الدراسة بدرجة عالية على المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية؛ وهذا يدل على حرص الجامعة على تحقيق الأمن السيبراني بشكل كامل لأنظمة معلوماتها الإدارية، ورغبتها في تحسين وتطوير أساليب ووسائل وممارسات تحقيقه، وتتفق هذه النتيجة مع نتيجة دراسة مالافت (Malavet, 2017) حول أهمية تخصيص ميزانية لدعم تحقيق الأمن السيبراني، وأهمية توعية منسوبي الجامعة بالمخاطر والتهديدات السيبرانية، حيث بينت نتيجة دراسة مالافت (Malavet, 2017) أن أبرز التحديات التي تواجهها تمثلت في: قلة الموارد المالية لإضافة التدابير الوقائية، وضعف برامج توعية منسوبي الجامعة بأهمية الأمن السيبراني، وكيفية التعامل مع التهديدات المحتملة، واتفقت هذه النتيجة مع نتيجة دراسة خوجه (٢٠٢٠م) حول أهمية إيجاد آليات تخزين آمنة للملفات والوثائق الإدارية، والالتزام بأنظمة وتعليمات الجهات الوطنية المختصة بالأمن السيبراني، حيث بينت دراسة خوجه (٢٠٢٠م) موافقة أفراد الدراسة بدرجة عالية على أهمية حفظ نسخ احتياطية من الملفات، والالتزام بتعليمات اللجان والهيئات الوطنية في مجال الأمن السيبراني، كما اتفقت هذه النتيجة مع نتيجة دراسة المنتشري وحريري (٢٠٢٠م) حول أهمية توعية منسوبي الجامعة بالمخاطر والتهديدات السيبرانية، وإيجاد آليات تخزين آمنة للملفات والوثائق الإدارية، حيث بينت دراسة المنتشري وحريري (٢٠٢٠م) موافقة أفراد الدراسة حول أهمية التوعية بمفاهيم ومخاطر الأمن السيبراني، وأهمية نسخ الملفات احتياطياً في ذاكرة خارجية.

إجابة السؤال الرابع: هل توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0,05) فأقل بين آراء أفراد الدراسة حول محاور الدراسة تُعزى لاختلاف متغير (جهة العمل، الجنس، سنوات الخبرة)؟

أولاً- الفروق باختلاف متغير جهة العمل:

للتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية تُعزى لاختلاف متغير جهة العمل تم استخدام

اختبار مان - ويتني (Mann-Whitney)، كما يوضح ذلك الجدول التالي:

جدول (10): اختبار مان - ويتني (Mann-Whitney) لبيان الفروق بين استجابات أفراد الدراسة باختلاف متغير جهة العمل

المحور	جهة العمل	العدد	متوسط الرتب	مجموع الرتب	قيمة معامل مان-ويتني	الدلالة الإحصائية
واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	عمادة تقنية المعلومات	52	30,05	1562,50	184,50	0,066
	إدارة الأمن السيبراني	11	41,23	453,50		
المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	عمادة تقنية المعلومات	52	33,88	1761,50	188,50	0,077
	إدارة الأمن السيبراني	11	23,14	254,50		
المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	عمادة تقنية المعلومات	52	29,59	1538,50	160,50	*0,023
	إدارة الأمن السيبراني	11	43,41	477,50		

(\* دالة عند 0,05).

يتضح من الجدول (١٠) ما يلي:

- لا توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، حيث بلغ معامل مان ويتني (١٨٤, ٥٠) عند مستوى دلالة (٠, ٠٦٦) وهو أكبر من (٠, ٠٥).
  - لا توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، حيث بلغ معامل مان ويتني (١٨٨, ٥٠) عند مستوى دلالة (٠, ٠٧٧) وهو أكبر من (٠, ٠٥).
  - توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية لصالح (إدارة الأمن السيبراني)، حيث بلغ معامل مان ويتني (١٦٠, ٥٠) عند مستوى دلالة (٠, ٠٢٣) وهو أصغر من (٠, ٠٥).
- يتضح من الجدول السابق أن استجابات منسوبي (عمادة تقنية المعلومات، وإدارة الأمن السيبراني) متماثلة حول محوري (واقع تحقيق الأمن السيبراني، ومعوقات تحقيقه)، وقد يرجع ذلك إلى سعي جامعة الإمام محمد بن سعود الإسلامية نحو تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، ومحاولة تلافي المعوقات التي تحدّ من تحقيقه، لذلك فقد اتفقت استجابات منسوبي (عمادة تقنية المعلومات، وإدارة الأمن السيبراني) حول المحورين السابقين، في حين توجد فروق ذات دلالة إحصائية في استجاباتهم حول محور المقترحات التي تُسهم في تحقيق الأمن السيبراني، لصالح (إدارة الأمن السيبراني)، وقد يرجع ذلك إلى أن إدارة الأمن السيبراني هي المسؤول المباشر عن تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في الجامعة، وبالتالي فهي الأعلّم بالوسائل والأساليب التي يمكن أن تزيد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في الجامعة، وتتفق هذه النتيجة مع نتيجة دراسة المنيع (٢٠٢٢م) التي بينت أنه لا توجد فروق ذات دلالة إحصائية بين استجابات أفراد

الدراسة حول محوري واقع تحقيق الأمن السيبراني، ومعوقات تحقيقه تعزى إلى متغير الجامعة، بينما تختلف هذه النتيجة مع نتيجة دراسة الكردي (٢٠٢١م) التي بينت أنه توجد فروق ذات دلالة إحصائية بين استجابات أفراد الدراسة في جميع محاور الدراسة تعزى إلى متغير الجامعة.

### ثانياً- الفروق باختلاف متغير الجنس:

للتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية تُعزى لاختلاف متغير الجنس تم استخدام اختبار ت (T)، كما يوضح ذلك الجدول التالي:

جدول (١١): اختبار ت (T) لبيان الفروق بين استجابات أفراد الدراسة باختلاف الجنس

المحور	الجنس	المتوسط الحسابي	الانحراف المعياري	درجة الحرية	قيمة T	الدلالة الإحصائية
واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	ذكر	٤,١٧	٠,٦٠٥	٦١	٠,٥٤٤	٠,٥٨٨
	أنثى	٤,٠٩	٠,٥٨٨			
المعوقات التي تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	ذكر	٢,٦٧	٠,٦٣٢	٦١	٠,٤٢٩	٠,٦٧٠
	أنثى	٢,٥٩	٠,٧٨٠			
المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	ذكر	٣,٨٤	٠,٨٧٩	٦١	٠,٣٤١	٠,٧٣٤
	أنثى	٣,٧٨	٠,٦٣٣			

(\*) دالة عند ٠,٠٥.

يتضح من الجدول (١١) ما يلي:

- لا توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، حيث بلغ معامل T (٠,٥٤٤) عند درجة حرية (٦١) ومستوى دلالة (٠,٥٨٨) وهو أكبر من (٠,٠٥).

- لا توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول المعوقات التي تحدّ من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، حيث بلغ معامل T (٠,٤٢٩) عند درجة حرية (٦١) ومستوى دلالة (٠,٦٧٠) وهو أكبر من (٠,٠٥).

- لا توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، حيث بلغ معامل T (٠,٣٤١) عند درجة حرية (٦١) ومستوى دلالة (٠,٧٣٤) وهو أكبر من (٠,٠٥).

يتضح من الجدول السابق أن استجابات أفراد الدراسة (الذكور، والإناث) متماثلة حول محاور الدراسة، وقد يرجع ذلك إلى أنهم يعملون في بيئة عمل متشابهة، وتتوفر لديهم نفس الإمكانيات المادية والبشرية، وتواجههم نفس المعوقات، بصرف النظر عن جنسهم؛ مما ساهم في اتفاقهم حول مدى تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، وتتفق هذه النتيجة مع نتيجة دراسة الكردي (٢٠٢١م) التي بينت أنه لا توجد فروق ذات دلالة إحصائية بين استجابات أفراد الدراسة تعزى إلى متغير الجنس.

### ثالثاً- الفروق باختلاف متغير سنوات الخبرة:

للتعرف على ما إذا كانت هناك فروق ذات دلالة إحصائية تُعزى لاختلاف متغير سنوات الخبرة تم

استخدام اختبار كروسكال - والس (Kruskal - Wallis)، كما يوضح ذلك الجدول التالي:

جدول (١٢): اختبار كروسكال - والس (Kruskal - Wallis)، لبيان الفروق بين استجابات أفراد الدراسة باختلاف سنوات الخبرة

المحور	سنوات الخبرة	العدد	متوسط الرتب	مربع كاي	درجات الحرية	مستوى الدلالة
واقع تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	أقل من ٥ سنوات	١٧	٣٧	٢, ١٩	٢	٠, ٣٣٤
	٥ - ١٠ سنوات	٢٢	٢٨, ٢٥			
	أكثر من ١٠ سنوات	٢٤	٣١, ٩٠			
المعوقات التي تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	أقل من ٥ سنوات	١٧	٢٧, ٢١	١, ٦٩	٢	٠, ٤٢٩
	٥ - ١٠ سنوات	٢٢	٣٤, ٦٤			
	أكثر من ١٠ سنوات	٢٤	٣٢, ٩٨			
المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية	أقل من ٥ سنوات	١٧	٣٦, ٧٤	١, ٥٦	٢	٠, ٤٥٨
	٥ - ١٠ سنوات	٢٢	٣٠, ٠٩			
	أكثر من ١٠ سنوات	٢٤	٣٠, ٤٠			

يتبين من الجدول رقم (١٢) ما يلي:

- لا توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول واقع تحقيق الأمن السيبراني لأنظمة

المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، حيث بلغ معامل مربع كاي (٢, ١٩) عند

درجة حرية (٢) ومستوى دلالة (٠, ٣٣٤) وهو أكبر من (٠, ٠٥).

تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية  
في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقويمية

العدد العشرون - يناير 2023م

د. الجوهرة بنت عثمان بن علي الركبان

- لا توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول المعوقات التي تحد من تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، حيث بلغ معامل مربع كاي (١, ٦٩) عند درجة حرية (٢) ومستوى دلالة (٠, ٤٢٩) وهو أكبر من (٠, ٠٥).

- لا توجد فروق ذات دلالة إحصائية في استجابات أفراد الدراسة حول المقترحات التي تُسهم في تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، حيث بلغ معامل مربع كاي (١, ٥٦) عند درجة حرية (٢) ومستوى دلالة (٠, ٤٥٨) وهو أكبر من (٠, ٠٥).

يتضح من الجدول السابق أن استجابات أفراد الدراسة (أقل من ٥ سنوات، ٥ - ١٠ سنوات، أكثر من ١٠ سنوات) متماثلة حول محاور الدراسة، وقد يرجع ذلك إلى أن أفراد الدراسة بصرف النظر عن عدد سنوات خبرتهم يعملون في بيئة عمل متشابهة، وتتوفر لديهم نفس الإمكانيات المادية والتقنية؛ مما ساهم في اتفاقهم حول مدى تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في جامعة الإمام محمد بن سعود الإسلامية، وتتفق هذه النتيجة مع نتيجة دراسة المنتشري وحريري (٢٠٢٠م) التي بينت أنه لا توجد فروق ذات دلالة إحصائية بين استجابات أفراد الدراسة تعزى إلى متغير سنوات الخبرة.

### توصيات الدراسة:

- في ضوء نتائج الدراسة، تُقدم الباحثة التوصيات الآتية:
- تطوير البنية التحتية السيبرانية في الجامعة باستمرار؛ لتتواءم مع تحقيق الأمن السيبراني، ولتحدّ من الاختراقات والهجمات السيبرانية.
  - تخصيص ميزانية كافية تدعم تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية في الجامعة.
  - الاستفادة من الأنظمة التقنية المتطورة، التي تعمل على تحديث برامج الحماية في أجهزة الحاسب الآلي في الجامعة بشكل تلقائي، ودون إشعار لمستخدمي تلك الأجهزة بضرورة تحديث البرامج.
  - إيجاد آليات للتعامل الفوري مع مخاطر الأمن السيبراني، تتماشى مع الضوابط الأساسية الصادرة من الهيئة الوطنية للأمن السيبراني.
  - تحديث الأنظمة التقنية في الجامعة بصفة مستمرة، لسد الثغرات، وضمان تحقيق الأمن السيبراني في الجامعة.
  - الاعتماد على برامج متطورة لحماية الأنظمة التشغيلية في الجامعة من الهجمات السيبرانية.
  - توعية منسوبي الجامعة بمفاهيم ومخاطر الأمن السيبراني، وأهمية تحقيقه، وطرق وأساليب مواجهة التهديدات السيبرانية.
  - إيجاد آليات تخزين آمنة للملفات والوثائق الإدارية؛ لحمايتها من أي اختراق أو سوء استخدام.
  - إلزام جميع منسوبي الجامعة باختيار كلمات مرور قوية لحساباتهم الرسمية، تحتوي على حروف كبيرة وصغيرة، وأرقام ورموز، وتختلف عن كلمات مرور حساباتهم الشخصية، وأن يتم تغييرها كل ٣ أشهر.
  - توجيه المستفيدين من أنظمة الجامعة إلى طرق حماية وأمن المعلومات.



### مقترحات بحثية:

- تحقيق الأمن السيبراني لأنظمة المعلومات في إدارات التعليم: دراسة تقويمية.
- تصور مقترح لتطوير إدارات الأمن السيبراني في الجامعات السعودية.
- برنامج تدريبي مقترح لتعزيز الأمن السيبراني في الجامعات السعودية.
- دراسة مقارنة بين دور الجامعات السعودية، وجامعات أجنبية أخرى في تحقيق الأمن السيبراني.

## المراجع

### أولاً- المراجع العربية:

- إدارة الأمن السيبراني. (٢٠٢٢م). تقرير عام ٢٠٢٢م. الرياض، إدارة الأمن السيبراني.
- إندبننت عربية. (٢٠٢٢م). المدارس والجامعات البريطانية تتأهب بعد زيادة الهجمات السيبرانية. مسترجع من:  
<https://www.independentarabia.com>
- البار، عدنان والسميري، عيسى. (٢٠١٩). أساسيات الأمن السيبراني. الرياض، مكتبة الملك فهد الوطنية.
- بسيوني، عبد الحميد. (٢٠١٢م). نظم المعلومات الإدارية. القاهرة، دار الكتب للطباعة والنشر والتوزيع.
- بونيف، سامي. (٢٠١٩م). دور الاستراتيجيات الاستباقية في مواجهة الهجمات السيبرانية. المجلة الجزائرية للحقوق والعلوم السياسية. المجلد ٤، العدد ٧، ص ١٢١-١٣٥.
- البيشي، منير. (٢٠٢١م). الأمن السيبراني في الجامعات السعودية وأثره في تعزيز الثقة الرقمية من وجهة نظر أعضاء هيئة التدريس: دراسة على جامعة بيشة. مجلة الجامعة الإسلامية للدراسات التربوية والنفسية. المجلد ٦، العدد ٢٩، ص ٣٥٣-٣٧٢.
- جامعة الإمام محمد بن سعود الإسلامية. (١٤٤٣هـ). إدارة الأمن السيبراني. مسترجع من:  
[https://imamu.edu.sa/IS/Pages/default.aspx#/data\\_1](https://imamu.edu.sa/IS/Pages/default.aspx#/data_1)
- جريدة المدينة. (٢٠٢٢م). ٢٤ جامعة خارج النطاق الأخضر لتضج الخدمات الإلكترونية. مسترجع من:  
<https://www.al-madina.com/article/668055>
- الجموسي، جوهر. (٢٠١٦م). الافتراضي والثورة: مكانة الإنترنت في نشأة مجتمع مدني عربي. بيروت، المركز العربي للأبحاث ودراسة السياسات.
- الخضري، جيهان وسلامي، هدى وكليبي، نعمة. (٢٠٢٠م). الأمن السيبراني والذكاء الاصطناعي في الجامعات السعودية: دراسة مقارنة. مجلة تطوير الأداء الجامعي. المجلد ١٢، العدد ١، ص ٢١٧-٢٣٣.

تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية  
في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقويمية

العدد العشرون – يناير 2023م

د. الجوهرة بنت عثمان بن علي الركبان

خوجه، هيفاء. (٢٠٢٠م). التطوير التنظيمي في إدارات التعليم لتحقيق المتطلبات الإدارية الداعمة للأمن السيبراني استراتيجية مقترحة. رسالة دكتوراه غير منشورة، جامعة الملك سعود، الرياض.

الرواشدة، محمد. (٢٠١٧م). أثر نظم المعلومات الإدارية على تعزيز الشفافية لدى وزارة الشباب في الأردن. رسالة ماجستير غير منشورة، جامعة عمان العربية، البلقاء.

السمحان، منى. (٢٠٢٠م) متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. مجلة كلية التربية. العدد ١١١، ص ٣-٢٩.

الشايح، خالد. (٢٠١٩م). الأمن السيبراني مفهومه وخصائصه وسياساته. القاهرة، الدار العالمية.

الشبانات، فاطمة. (٢٠٢٠م). دور إدارة الجامعات السعودية الحكومية في تحقيق الأمن السيبراني: استراتيجية مقترحة. رسالة دكتوراه غير منشورة، جامعة الملك سعود، الرياض.

الشبانات، فاطمة. (٢٠٢١م). إدارة الأمن السيبراني في مؤسسات التعليم العالي. جدة، شركة تكوين للطباعة والنشر والتوزيع.

الشرع، مصطفى. (٢٠١٦م). أثر نظم المعلومات الإدارية في أداء العاملين في وزارة الصحة الأردنية. رسالة ماجستير غير منشورة، جامعة آل البيت، المفرق.

الشتي، ايناس. (٢٠١٩م). تقييم سياسات أمن وخصوصية المعلومات في المؤسسات التعليمية في المملكة العربية السعودية. مجلة الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات. المجلد ٢٢، العدد ١٤، ص ١١-٢٤.

صائع، وفاء. (٢٠١٨م). وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياجاتهم الأمنية من الجرائم الإلكترونية. المجلة العربية للعلوم الاجتماعية. المجلد ٣، العدد ١٤، ص ١٨-٧٠.

الصحفي، مصباح وعسكول، سناء. (٢٠١٩م). مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة. مجلة البحث العلمي في التربية. المجلد ١٠، العدد ٢٠، ص ٤٩٣-٥٣٤.

العساف، صالح. (٢٠١٦م). المدخل إلى البحث في العلوم السلوكية. الرياض، مكتبة العبيكان.

قنديلجي، عامر والجنابي، عبد القادر. (٢٠٢١م). نظم المعلومات الإدارية. عمان، دار المسيرة للنشر والتوزيع.

الكردي، كاظم. (٢٠٢١م). الأمن السيبراني والتعليم الإلكتروني في جامعات فلسطين من وجهة نظر أعضاء هيئة التدريس: جامعة النجاح الوطنية أنموذجاً. *المجلة العربية للمعلوماتية وأمن المعلومات*. العدد ٥، ص ١٠٣-١٢٣.

محمد، علياء. (٢٠١٩م). دور نظم المعلومات الإدارية في تحقيق التغيير التنظيمي. رسالة ماجستير غير منشورة، جامعة إفريقيا العالمية، الخرطوم.

المنتشري، فاطمة وحريري، رندة. (٢٠٢٠م). درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات. *المجلة العربية للتربية النوعية*. المجلد ٤، العدد ١٣، ص ٩٥-١٤٠.

المنيع، الجوهرة. (٢٠٢٢م). متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠. *المجلة العلمية*. المجلد ٣٨، العدد ١، ص ١٥٦-١٩٤.

الهيئة الوطنية للأمن السيبراني. (٢٠١٨م). الضوابط الأساسية للأمن السيبراني. الرياض، الهيئة الوطنية للأمن السيبراني.

الهيئة الوطنية للأمن السيبراني. (٢٠٢٢م). مسترجع من: <https://nca.gov.sa/pages/about.html>

الهندي، رشا. (٢٠٢١م). تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول. *مجلة جامعة الفيوم للعلوم التربوية والنفسية*. المجلد ١١، العدد ١٥، ص ٣٣٨-٣٨٣.

وكالة الأنباء السعودية. (٢٠٢٢م). مسترجع من:

<https://www.spa.gov.sa/viewfullstory.php?lang=ar & newsid=2205980>

ياسين، سعد. (٢٠١٨م). *نظم المعلومات الإدارية*. عمان، دار اليازوري العلمية للنشر والتوزيع.

تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية  
في جامعة الإمام محمد بن سعود الإسلامية: دراسة تقويمية

د. الجوهرة بنت عثمان بن علي الركبان

ثانياً- المراجع الأجنبية:

- Malavet, J. N. (2017). Cyber Security in Higher Education: Accuracy of Resources Utilized by Information Technology Departments to Prevent Data Breaches. Master's Requirement. Utica College, Ann Arbor.
- Wijayanto, H., & Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*. Volume 9, Issue 3, pp. 395-399.