الأمن السيبراني ودوره في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين

د. منار عبدالله محمد حسن

أستاذ مساعد في الإدارة الرياضية – قسم التربية الرياضية

كلية العلوم الصحية والرياضية – جامعة البحرين

Doi: 10.21608/jsbsh.2023.210542.2445

المقدمة:

إن استضافة وتنظيم الفعاليات الرياضية الكبرى قد تحول إلى صناعة ضخمة يتم تمويلها بمليارات الدولارات وتشرف عليها كافة مؤسسات الدول وتسخر لها كافة الإمكانيات لضمان نجاحها وتميزها، وتسعى الدول إلى الحصول على حق تنظيم هذه الفعاليات بكافة السبل، وتضعها كأولوية لها وهدف من أهدافها التي يمكن من خلال تحقيقها دعم النواحي التنموية لهذه الدول، ولقد أصبح التنافس على تنظيم وانجاح الفعاليات الرياضية الكبرى على أشده خاصة خلال العقدين الأول والثاني من القرن الحادي والعشرين، وليس أدل على ذلك مما يحدث في سبيل الحصول على تنظيم بطولات ككاس العالم لكرة القدم للرجال والدورات الأولومبية، حيث يتم حشد الإمكانات الاقتصادية لهذا الغرض، وتقف القيادات السياسية خلف مساعي نيل حق تنظيم هذه الفعاليات، حيث يعتبر الفوز بتنظيم هذه الفعاليات بمثابة بوابة للعبور إلى العالمية، وفرصة لكي تعكس وجهها الحضاري أمام العالم ككل، كما أن تنظيم هذه الفعاليات عادة ما يكون له مردود اقتصادي وتنموي على الدول، كما أنه عادة ما يلعب دور كبير في تعزيز قدرات القوى البشرية في العمل على تنظيم وإدارة هذه الفعاليات (درويش، الصغير، ومغاوري، ٢٠١٣).

ويرى (جمال الدين، ٢٠٢٣) إن تنظيم الفعاليات بمختلف أنواعها يحتاج إلى مستوى مرتفع من الحماية لتجنب ما يمكن أن تتعرض له هذه الفعاليات من تهديدات قد تقود إلى إلغائها أو تهديد صحة وسلامة المشاركين، وعادة ما يتم تصنيف هذه التهديدات إلى تهديدات تقليدية، منها الهجمات الإرهابية التي يمكن أن يتم تنفيذها على مواقع هذه الفعاليات أو ضد الشخصيات القائمة على تنفيذ هذه الفعاليات أو من الحضور، والنوع الثاني من التهديدات هو التهديدات السيبرانية أو تلك المتعلقة بالأمن السيبراني، وهو نوع من التهديدات التي ترتبط جملة وتفصيلاً بأمن المعلومات، ولعل الفعاليات الرياضية هي أحد أنواع الفعاليات التي يمكن أن تواجه تحديات أمنية من كلا النوعين المشار لهما، يعتبر أمن المعلومات المتعلقة بتنظيم الفعاليات، والبيانات الخاصة بالمشاركين، وبيانات التنظيم والترتيبات جميعها عرضة للخطر حيث يمكن أن تتعرض لهجمات سيبرانية تنظمها جماعات أو منظمات هدفها إفساد هذه الفعاليات وخاصة الفعاليات الرياضية الكبرى والتي تشمل البطولات الرياضية المحلية والإقليمية والدولية وبعض المؤتمرات الرياضية.

تعتبر المخاطر السيبرانية هي أبرز أنواع المخاطر التي تهدد نجاح الفعاليات الرياضية الكبرى، ذلك لأن الكثير من الهجمات السيبرانية يمكنها أن تنال من البنية التحتية التقنية لهذه الفعاليات، واصبح من الهام وجود شراكات بين الجهات القائمة على تنظيم هذه الفعاليات والجهات الأمنية التي يمكنها أن تتابع مستوى تأمين الفعاليات وتأمين كافة البيانات والمعلومات والمؤسسات التي يتم من خلالها تنظيم الفعاليات، وهو ما يشمل حماية عمليات بيع التذاكر، والأمور التنظيمية والإقامة والمواصلات للفرق أو المنتخبات والجهات المشاركة في الفعاليات (بن زرارة وأعراب،٢٠٢٢).

ولقد برزت أهمية الأمن السيبراني وتطورت وسائله وأدواته خلال السنوات القليلة المنصرمة كاستجابة للتطورات التقنية التي يشهدها العالم، وكرد فعل لما ظهر من تهديدات تنال من أمن الأشخاص والمشروعات الخاصة بالبنية التحية والمعلومات الخاصة بالأفراد والمؤسسات، وأصبحت هذه التهديدات مرتفعة الخطورة لما يمكنها أن تسببه من خسائر، وأصبحت مواجهتها مرتفعة التكلفة وتتطلب جهداً كبيراً وإمكانات كبيرة، إلا أن تكلفة مواجهتها تسهم في تجنب المخاطر الجسيمة التي تترتب عليها، حيث أن هذه التهديدات تمس الأمن القومي للدول وعناصره، وتضرب الاستقرار المجتمعي وتؤثر على سمعة الدولة ككل وقدرتها على استضافة الفعاليات الكبرى، من ثم فإن تعزيز ممارسات الأمن السيبراني خلال تنفيذ الفعاليات الرياضية لا يقل أهمية عن الفعاليات السياسية والاقتصادية وغيرها.

مشكلة الدراسة:

إن تنظيم وإدارة الفعاليات الرياضية قد تحولت بشكل عام إلى مجال مهني واحترافي ولم يعد يدار بشكل عشوائي، بل توجد العديد من الأسس والقواعد التي التي يتم تطبيقها في غالبية دول العالم (سامر، ٢٠١٠)، ولقد شهد هذا المجال العديد من التطورات والتغيرات خلال السنوات القليلة الماضية، وذلك بعد أن أصبح هذا المجال مرتبطاً ومتداخلاً مع العديد من المجالات الهامة في الحياة الاقتصادية مثل (السياحة، الأعمال التجارية، وقت الفراغ)، كما أن الفعاليات الرياضية الكبرى عادة ما تترك آثار وانعكاسات على مختلف عناصر النظم الاجتماعية في الدولة المنظمة، وهي عملية تتطور مع تطور الرياضة والعناصر ذات الصلة بها، ولتحقيق نجاحات رياضية واقتصادية واجتماعية من خلال تنظيم الفعاليات الرياضية الكبرى أصبح من الهام تأمين هذه الفعاليات بشكل متقن.

كنتيجة للأهمية المتزايدة للفعاليات الرياضية ودورها في تحقيق التنمية الاقتصادية، وتحسين صورة الدولة أصبحت هذه الفعاليات مستهدفة من قبل بعض الجماعات والمنظمات الداخلية والخارجية، وأصبحت الآلية المفضلة لتهديد هذه الفعاليات هي استخدام الوسائل والأدوات السيبرانية التي يمكنها أن تصيب عمليات وآليات تنظيم هذه الفعاليات بالأضرار الجسيمة، حيث يمكن للهجمات السيبرانية أن تحقق أهدافًا لا يمكن للهجمات التقليدية أن تحققها ، ومن ثم أصبح توافر الأمن السيبراني وإدارة مخاطره ضرورة للحماية من الاستخدام السيء لتكنولوجيا الاتصال والمعلومات، خاصة مع تصاعد دور الفاعلين

من غير الدول في الكثير من الفعاليات الدولية ومنها الرياضية ودخول هؤلاء الفواعل مجال تهديد الأمن السيبراني (إليوت وجينكنسون، ٢٠٢٠)، ومن ثم أصبحت هناك اتجاهات عديدة لتحقيق ذلك الأمن خلال الفعاليات الرياضية الكبرى عبر التنسيق بين الحكومات، والمجتمع المدني، والشركات التكنولوجية، والإعلام، وغيرها ولزيادة القدرة على إدارة المخاطر السيبرانية التي يمكن أن تضرب الفعاليات الرياضية الكبرى هناك سلسلة من الإجراءات التقنية لتحقيق الأمن السيبراني، أبرزها: تطوير المخطط الوطني لتحفيز الأمن السيبراني بهدف تعزيز المشاركة في الجهود الدولية والإقليمية (الغبيوي، ٢٠٢٠).

وبشكل عام توجه مملكة البحرين اهتماماً كبيراً بآليات تحقيق الأمن السيبراني كأحد الركائز الرئيسية خلال تنظيم الفعاليات الكبرى، ويعتبر تنظيم الفعاليات الرياضية الكبرى في مملكة البحرين محل اهتمام القيادة، ولعل أبرز هذه الفعاليات هو سباق الفورمولا (١) الذي يعقد سنوياً، ومن ثم تبرز مشكلة البحث الحالي والتي يمكن صياغتها في السؤال البحثي التالي "هل توجد علاقة ذات دلالة إحصائية بين ممارسات الأمن السيبراني وتأمين الفعاليات الرياضية الكبرى في مملكة البحرين؟"

أهداف الدراسة

تسعى الباحثة من خلال هذه الدراسة إلى تحقيق الأهداف التالية:

١- التعرف على واقع استخدام أنظمة الأمن السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين.

٢- تقييم دور أنظمة الأمن السيبراني في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين.

أسئلة الدراسة:

تسعى الباحثة من خلال هذه الدراسة الإجابة على الأسئلة التالية:

١- ما هو واقع استخدام أنظمة الأمن السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين؟

٢- إلى أي مدى تسهم أنظمة الأمن السيبراني في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين؟

أهمية الدراسة:

تبرز أهمية هذه الدراسة من خلال أنها:

١- تتناول موضوع ذو أهمية خاصة في العصر الحديث وهو الأمن السيبراني وما يرتبط به من تهديدات للفعاليات التي تنفذ في الدول.

٢- تلقي هذه الدراسة الضوء على آليات حماية الفعاليات الرياضية الكبرى وما يرتبط بها من تحديات أمنية خاصة تلك المتعلقة بالأمن السيبراني، وهي متطلب هام تحتاجه العديد من المؤسسات والشركات التي تنظم الفعاليات الرياضية الكبرى.

٣- يمكن أن تكون نتائج الدراسة ذات أهمية للمؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين، حيث توضح مدى استعدادات المتاحة لتبني الفعاليات الرياضية الكبرى.

٤- تعتبر نتائج الدراسة ذات أهمية للمؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين حيث تبرز مدى قدرتها على توظيف أنظمة الأمن السيبراني في حماية تلك الفعاليات.

٥- تعتبر نتائج الدراسة ذات أهمية للباحثين الذين يتناولون بالدراسة موضوعات ذات صلة بمتغيرات الدراسة.

حدود الدراسة:

- **الحدود الزمنية:** تم تطبيق الدراسة الحالية خلال الفترة من ٢٠ مارس ٢٠٢٣ وحتى ٢٠ ابريل ٢٠٢٣.
- **الحدود المكانية:** تم تطبيق الدراسة في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين.
- **الحدود البشرية:** تم تطبيق الدراسة على الإداريين في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين.

مصطلحات الدراسة:

١- الأمن السيبراني:

مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني (شفيق، ٢٠١٨).

٢- الفعاليات الرياضية:

"سلسلة من المنافسات التي تقام بين مجموعة من الوحدات أفراد كانوا أو جماعات بقصد تحديد الفائزين منهم أو ترتيبهم حسب نتائجهم" (حنتوش وعبد العظيم، ٢٠١٦).

٣- تهديدات الامن السيبراني:

مجموعة المخاطر التي تعترض تحقيق الأمن السيبراني، وعادة ما تكون هذه المهددات موجهة نحو أجهزة الحاسوب أو أمن الشبكات والبيانات(زروقة، ٢٠١٩).

الدراسات السابقة:

من الدراسات التي ألقت الضوء تهديدات الأمن السيبراني:

(١) **دراسة** (Andree, 2022) بعنوان " تأمين الأحداث الرياضية الكبرى خاصة كرة القدم خلال أزمة كوفيد -١٩"، هدفت هذه الدراسة إلى تحديد مستوى فاعلية تأمين أحداث بطولة اليورو ٢٠٢٠ والتي أقيمت في عام ٢٠٢١ في إنجلترا نظرا لظروف جائحة كورونا، وظفت هذه الدراسة المنهج الوصفي المسحي، استخدمت الدراسة الاستبانة التي تم توزيعها على عينة شملت (٣٥٥) من العاملين في الشركات القائمة على حماية وتأمين فاعليات البطولة، كما تم إجراء مجموعة من المقابلات، وتوصلت الدراسة إلى أن هناك فهم عام للعمليات المتعلقة بالحوكمة الأمنية والعمليات المتعلقة بالأمن بشكل أفضل في التجمعات الرياضية الحالية ، والتي تتعلق بشكل متزايد بمفاهيم "الأمن" و"السلامة" و"المخاطر"، كان من أهم الإجراءات الخاصة بحماية فاعليات البطولة هو تقييم عمليات نقل البيانات داخلياً وخارجيا أثناء البطولات في جو غير آمن ومليء بالتهديدات، حيث مثلت التهديدات السيبرانية تهديداً أمنياً له تأثيرات شديدة على عالم كرة القدم، كما يعتبر التوجه الحالي في تنظيم الأحداث الرياضية الكبرى هو تأمين عمليات نقل المعلومات.

(٢) **دراسة (الخاطر، ٢٠٢١)** وهي بعنوان " الأمن السيبراني "، هدفت الدراسة إلى مناقشة أهمية الأمن السيبراني وبيان أهم جهود الدول لتحقيق الأمن السيبراني خلال تنفيذ الفعاليات المختلفة، وظفت الدراسة المنهج الوصفي المسحي، واستخدمت الاستبانة التي وزعت على عينة شملت (٥٥) من العاملين في مجال الأمن المعلوماتي في قوة دفاع البحرين، وتوصلت الدراسة إلى نتائج أهمها أنه يمكن تعريف الأمن السيبراني على أنه هو "مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع الوصول غير المصرح به، وسوء الاستغلال، وسرقة المعلومات الإلكترونية، وتشويه الاتصالات والمعلومات التي تحتويها، وذلك بهدف حماية وحفظ وضمان توافر واستمرارية عمل نظُم المعلومات"، كما أن تحقيق الأمن السيبراني خلال الفعاليات الكبرى يتطلب تكاتف وتشارك الجهود بين المؤسسات السياسة والعسكرية والاقتصادية والإعلامية، وتسهم مواجهات تهديدات الأمن السيبراني في تنفيذ فعاليات آمنة للمشاركين ولمعلوماتهم الشخصية، كما تسهم في الحفاظ على المنشآت التي يتم تنفيذ الفعاليات فيها.

(٣) **دراسة تامر الداوودي (٢٠١٩)** بعنوان " متطلبات الأمن والحماية في تنظيم البطولات الرياضية "، هدفت الدراسة إلى تحديد أهم المعايير التي يجب اتباعها في تنظيم البطولات الرياضية خاصة تلك التي تتعلق بتحقيق أمن وسلامة المشاركين، وتحديد أهم الإجراءات الواجب الالتزام بها لتجنب المخاطر السيبرانية في إدارة البطولات الرياضية الكبرى، وظفت الدراسة المنهج الوصفي المسحي، واستخدمت الاستبانة لجمع البيانات من عينة بلغت (٧٧) مشارك من القائمين على إدارة البطولات الرياضية في جمهورية مصر العربية، توصلت الدراسة إلى نتائج أهمها أن تأمين فاعليات

البطولات الكبرى يتطلب جهد مشترك بين مختلف المؤسسات، يلعب قطاع أمن المعلومات دوراً كبيراً في تأكيد حماية البطولات الرياضية من خلال قدرته على مواجهة التهديدات السيبرانية للمعلومات المتعلقة بالبطولات والمشاركين.

(4) دراسة (Ohata, 2018) بعنوان " حلول الأمن السيبراني لتأمين الفاعليات الدولية الكبرى"، هدفت هذه الدراسة إلى مناقشة الأدوار التي يمكن أن يقوم بها الأمن السيبراني في تأمين مختلف أنواع الفعاليات الدولية الكبرى، تم توظيف المنهج الوصفي، وشملت عينة الدراسة التي وزع عليها الاستبيان (١٤٧) مختص في مجال الأمن السيبراني ممن يوكل لهم تأمين الفعاليات الكبرى بمختلف أنواعها في الولايات المتحدة الأمريكية، من أهم نتائج الدراسة التي تم الوصول لها أن تطبيق ممارسات الأمن السيبراني تسهم بشكل كبير في تحقيق أمن الفعاليات الكبرى سواء السياسية أو الاقتصادية والرياضية وغيرها.

(٥) دراسة (Windholz, 2016) بعنوان " تأمين السلامة في الأحداث الرياضية الكبرى" هدفت هذه الدراسة إلى تقييم أدوار المسؤولين عن حماية وسلامة الرياضيين والكوادر المشاركة في الأحداث الرياضية الكبرى بناء على قوانين الصحة والسلامة الأسترالية، حتى يمكن تحقيق هدف الدراسة تم توظيف المنهج الوصفي المسحي، تم توزيع أداة الاستبانة على (٢٢٥) من العاملين في الجهات المسؤولة عن تأمين المشاركين في الأحداث الرياضية الكبرى، وتوصلت الدراسة على نتائج أهمها أن الشركات والمؤسسات المسؤولة عن تأمين الأحداث الرياضية الكبرى تتبنى إجراءات صارمة لحماية وتأمين الأحداث والفعاليات لضمان سلامة العمل والمشاركين، تتطلب إدارة المخاطر في الأحداث الرياضية الكبرى الإعتماد على التقنيات الحديثة، وتعتبر عمليات تأمين الأحداث الرياضية الكبرى جزءًا من مخطط قومي يتم تخصيص ميزانيات خاصة به لما له من تأثيرات على وضع الدولة.

التعليق على الدراسات السابقة:

أ. **من حيث الأهداف:** يوجد تشابه كبير بين أهداف الدراسة الحالية مع الدراسات السابقة في التعرف على واقع استخدام ممارسات الأمن السيبراني في تأمين الفعاليات الكبرى وخاصة الرياضية.

ب. **من حيث المنهج المستخدم:** اعتمدت جميع الدراسات السابقة على المنهج الوصفي، وهو ما مثل الدافع الرئيسي لتوظيف الدراسة الحالية لنفس المنهج إضافة إلى ملائمة هذا المنهج لموضوع الدراسة.

ت. **من حيث العينة:** تنوعت العينات التي تم تطبيق أداة الدراسات السابقة عليها، فمن هذه الدراسات من استخدم القائمين على إدارة البطولات الرياضية، ومنهم من وظف المختصين في مجال الأمن السيبراني، ودراسات أخرى استخدمت العاملين في مجال الأمن المعلوماتي، بينما ركزت الدراسة الحالية فقط على الإداريين في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى

في مملكة البحرين.

ث. **من حيث وسائل جمع البيانات: اعتمدت** جميع الدراسات السابقة على الاستبانة كأداة يمكن من خلالها جمع البيانات من العينة البحثية، وهي الأداة نفسها التي اعتمدت عليها الدراسة الحالية.

ج. **من حيث النتائج:** جميع الدراسات السابقة قد توصلت إلى نفس النتائج التي توصلت لها الدراسة الحالية، وهي أن هناك دور فعال لاستخدام أنظمة الأمن السيبراني في تأمين الفعاليات الرياضية.

ح. **تميزت الدراسة الحالية عن سابقاتها** بتناولها عينة الإداريين في المؤسسات والشركات المنظمة للفعاليات الرياضية الكبرى، وهذا مالم تجده الباحثة في الدراسات السابقة التي ركزت عيناتها في مستخدمي ومتخصصين أنظمة الأمن السيبراني، ومنظمي الفعاليات الرياضية.

إجراءات الدراسة:

حتى يتم الإجابة على تساؤلات الدراسة اتبعت الباحثة مجموعة من الإجراءات المنهجية.

منهجية الدراسة

وظفت هذه الدراسة المنهج الوصفي المسحي، وذلك لملائمته للهدف الذي تسعى الدراسة لتحقيقه منها، وكذلك لتوافقه مع طبيعة الدراسة التي تهدف إلى تحديد دور الأمن السيبراني في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين.

مجتمع الدارسة

تكون مجتمع الدراسة من الإداريين العاملين في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية في مملكة البحرين وعددهم (٣٥٠).

عينة الدارسة

تكونت عينة الدراسة من (١٨٥) موظف من العاملين في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين، وهو ما يمثل (٥٢.٨%) من مجتمع الدراسة.

قسمت عينة الدراسة على النحو التالي:

الجدول (١) توزيع عينة الدراسة

نوع العينة	العدد	النسبة المئوية
العينة الاستطلاعية	٣٠	%١٦.٢
العينة الأساسية	١٥٥	%٨٣.٨
الإجمالي	٣٥	%١٠٠

يتضح من خلال الجدول (١) أن الباحثة قامت بتقسيم عينة الدراسة العاملين في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين إلى قسمين، الأول هو العينة الاستطلاعية، وبلغت (٣٠) مشارك بنسبة (١٦.٢%) من إجمالي عينة الدراسة، والثاني عينة أساسية للدراسة بلغت (١٥٥) مشارك بنسبة (٨٣.٨%).

أداة الدراسة:

للقيام بعملية جمع البيانات الأولية للدراسة، والتي تسهم في التوصل إلى إجابات لأسئلة الدراسة، صُمِمَ استبيان بعنوان " **الأمن السيبراني ودوره في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين**"، تم صياغة الاستبيان بالرجوع إلى عدد من الدراسات السابقة منها: (Andree, 2022؛ الخاطر، ٢٠٢١؛ الداوودي، ٢٠١٩) ، وقد تم التحقق من الصدق الظاهري لها من خلال عرضها على محكمين من حملة الدكتوراه والمختصين في الإدراة الرياضية أو الأمن السيبراني (ملحق ٢) والذين قدموا مجموعة من الملاحظات على بعض جوانب الاستبيان، والتي قامت الباحثة بأخذها بعين الاعتبار لتظهر الأداة في صورتها النهائية (ملحق ٣).

تحتوي الاستبانة في صورتها النهائية على (٦٤) فقرة، وتوزعت على محورين أساسيين:

(١) **المحور الأول:** محور واقع أنظمة الأمن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية، ويشتمل على (٥٤) فقرة، وتنقسم إلى أربعة أبعاد: المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني (١٣) فقرة، المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني (٢٢) فقرة، المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني (٨) فقرات، المتطلبات المادية اللازمة لتحقيق الأمن السيبراني (١١) فقرة.

(٢) **المحور الثاني:** محور دور أنظمة الأمن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية، واشتمل على (٩) فقرات.

المعاملات العلمية لأداة الدراسة

أولاً: الصدق

حتى يمكن التحقق من صدق محتوى استمارة الاستقصاء تم عرضها على (١٠) محكمين من حملة الدكتوراه في تخصص الغدراة الرياضية أو الأمن السيبراني (ملحق رقم ٢)، حيث طلب منهم إبداء الرأي في أداة الدراسة فيما يخص مناسبة العبارات ومن حيث التعديل أو الحذف أو الإضافة، حيث توضح الجداول التالية نتائج صدق المحتوى:

جدول (٢) صدق محتوى محور" واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية "(ن = ١٠)

البعد	العبارة	مناسب		غير مناسب		التعديل المقترح
		ت	%	ت	%	
المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني	١	١٠	%١٠٠	٠	%٠	لا يوجد
	٢	١٠	%١٠٠	٠	%٠	لا يوجد
	٣	١٠	%١٠٠	٠	%٠	لا يوجد
	٤	١٠	%١٠٠	٠	%٠	لا يوجد
	٥	١٠	%١٠٠	٠	%٠	لا يوجد
	٦	١٠	%١٠٠	٠	%٠	لا يوجد

	٧	١٠	%١٠٠	٠	%٠	لا يوجد
	٨	١٠	%١٠٠	٠	%٠	لا يوجد
	٩	١٠	%١٠٠	٠	%٠	لا يوجد
	١٠	١٠	%١٠٠	٠	%٠	لا يوجد
	١١	٩	%٩٠	١	%٢٠	تعديل
	١٢	١٠	%١٠٠	٠	%٠	لا يوجد
	١٣	١٠	%١٠٠	٠	%٠	لا يوجد
المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني	١	١٠	%١٠٠	٠	%٠	لا يوجد
	٢	١٠	%١٠٠	٠	%٠	لا يوجد
	٣	١٠	%١٠٠	٠	%٠	لا يوجد
	٤	١٠	%١٠٠	٠	%٠	لا يوجد
	٥	١٠	%١٠٠	٠	%٠	لا يوجد
	٦	١٠	%١٠٠	٠	%٠	لا يوجد
	٧	١٠	%١٠٠	٠	%٠	لا يوجد
	٨	١٠	%١٠٠	٠	%٠	لا يوجد
	٩	١٠	%١٠٠	٠	%٠	لا يوجد
	١٠	١٠	%١٠٠	٠	%٠	لا يوجد
	١١	١٠	%١٠٠	٠	%٠	لا يوجد
	١٢	١٠	%١٠٠	٠	%٠	لا يوجد
	١٣	١٠	%١٠٠	٠	%٠	لا يوجد
	١٤	١٠	%١٠٠	٠	%٠	لا يوجد
	١٥	١٠	%١٠٠	٠	%٠	لا يوجد
	١٦	٩	%٩٠	١	%١٠	تعديل
	١٧	١٠	%١٠٠	٠	%٠	لا يوجد
	١٨	١٠	%١٠٠	٠	%٠	لا يوجد
	١٩	١٠	%١٠٠	٠	%٠	لا يوجد
	٢٠	١٠	%١٠٠	٠	%٠	لا يوجد
	٢١	١٠	%١٠٠	٠	%٠	لا يوجد
المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني	١	١٠	%١٠٠	٠	%٠	لا يوجد
	٢	٩	%٩٠	١	%١٠	تعديل
	٣	١٠	%١٠٠	٠	%٠	لا يوجد
	٤	١٠	%١٠٠	٠	%٠	لا يوجد
	٥	١٠	%١٠٠	٠	%٠	لا يوجد
	٦	١٠	%١٠٠	٠	%٠	لا يوجد
	٧	١٠	%١٠٠	٠	%٠	لا يوجد
	٨	١٠	%١٠٠	٠	%٠	لا يوجد

المتطلبات المادية اللازمة لتحقيق الأمن السيبراني	١	١٠	%١٠٠	٠	%٠	لا يوجد
	٢	١٠	%١٠٠	٠	%٠	لا يوجد
	٣	٧	%٧٠	٣	%٣٠	تعديل
	٤	١٠	%١٠٠	٠	%٠	لا يوجد
	٥	٩	%٩٠	١	%١٠	تعديل
	٦	١٠	%١٠٠	٠	%٠	لا يوجد
	٧	١٠	%١٠٠	٠	%٠	لا يوجد
	٨	١٠	%١٠٠	٠	%٠	لا يوجد
	٩	١٠	%١٠٠	٠	%٠	لا يوجد
	١٠	١٠	%١٠٠	٠	%٠	لا يوجد
	١١	١٠	%١٠٠	٠	%٠	لا يوجد

يبين الجدول (٢) آراء الخبراء حول " محور واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية "، يتضح أنه تم تعديل أربع فقرات من اجمالي (٥٤) فقرة في هذا المحور، وتمت الموافقة على جميع الفقرات الـ (٥٠) ، وراعت الباحثة ملاحظات الخبراء وتم تعديل الفقرات الأربع حتى ظهر المحور بصورته النهائية المتكاملة بناء على آرائهم.

جدول (٣) صدق محتوى محور" دور أنظمة الامن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية "(ن = ١٠)

العبارة	مناسب		غير مناسب		التعديل المقترح
	ت	%	ت	%	
١	١٠	%١٠٠	٠	%٠	لا يوجد
٢	١٠	%١٠٠	٠	%٠	لا يوجد
٣	٩	%٩٠	١٠	%١٠	تعديل
٤	١٠	%١٠٠	٠	%٠	لا يوجد
٥	١٠	%١٠٠	٠	%٠	لا يوجد
٦	٧	%٧٠	٠٣	%٣٠	حذف
٧	١٠	%١٠٠	٠	%٠	لا يوجد
٨	١٠	%١٠٠	٠	%٠	لا يوجد
٩	١٠	%١٠٠	٠	%٠	لا يوجد

يبين الجدول (٣) الذي يتناول آراء الخبراء حول " محور دور أنظمة الامن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية "، يتضح أنه تمت الموافقة على جميع الفقرات المحور وهي (٩) فقرات، ولقد ظهر المحور بصورته النهائية المتكاملة بناء على آرائهم.

ثانياً: الثبات

للتأكد من ثبات الاستبانة، تم تنفيذ الدراسة الاستطلاعية على العينة استطلاعية التي تم اختيارها

من إجمالي عينة البحث والتي بلغت (٣٠) مشارك، بنسبة (١٦.٢%) من الإداريين في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين، حيث تم الاعتماد على قيم (كرونباخ–ألفا) من خلال تحليل نتائج العينة الاستطلاعية، كما هو مبين في الجدول (٤):

الجدول (٤) قيم معاملات ألفا كرونباخ لأبعاد الاستبيان (ن= ٣٠)

المحاور	عدد أفراد العينة الاستطلاعية	عدد العبارات	معامل ثبات ألفا كرونباخ
واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية	٣٠	٥٤	٠.٨٧٩
دور أنظمة الامن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية	٣٠	٩	٠.٨٥٢
إجمالي فقرات الاستبيان	٣٠	٦٣	٠.٨٦٥

يتضح من الجدول (٤) الذي يعرض قيم معامل (كرونباخ–ألفا) الخاص بمحاور استمارة الاستقصاء أن قيم (كرونباخ–ألفا) لمحور " واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية " والذي تضمن (٥٤) فقرة (٨٧.٩%) وهي قيمة مرتفعة، وبالنسبة إلى قيم (كرونباخ–ألفا) الخاصة بمحور " دور أنظمة الامن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية " والذي اشتمل على (٩) فقرات فلقد جاءت (٨٥.٢%) وهي قيمة مرتفعة ايضاً، أما قيمة قيم (كرونباخ–ألفا) لإجمالي فقرات استنارة الاستقصاء التي تضمنت (٦٣) فقرة فكانت (٨٦.٥%) وهي أيضاً قيمة مرتفعة، الأمر الذي يعني أن استبانة الدراسة الحالية تتمتع بمستوى ثبات مرتفع.

ثالثا-صدق الاتساق الداخلي

لقياس مستوى صدق الاتساق الداخلي بين فقرات الاستبانة والدرجة الكلية للأبعاد، والمحاور والاستبانة ككل قامت الباحثة بحساب معامل ارتباط بين كل فقرة من فقرات الاستبانة مع الدرجة الكلية للمحور والدرجة الكلية للاستبانة، ومن خلال معامل الارتباط ببين مجموع كل بعد ومحور مع الدرجة الكلية لاستمارة الاستقصاء، كما هو وارد من خلال الجداول الآتية:

(١) صدق الاتساق الداخلي للمحور الأول (واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية)

جدول (٥) قيمة معامل الارتباط بين درجة كل عبارة ومجموع المحور المنتمية إليه والمجموع الكلي للستبانة للمحور الأول (بعد المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني) (ن= ٣٠)

م	العبارات	معامل الارتباط	
		العبارة والمحور	العبارة والمجموع الكلي
١	توجد إدارة خاصة بالأمن السيبراني في المؤسسة	.852**	.730**
٢	توجد سياسات أمنية لأنظمة المعلومات الإدارية بالمؤسسة	.841**	.795**
٣	تطبق الإجراءات الإدارية اللازمة لتحقيق الأمن السيبراني داخل أنظمة المعلومات الإدارية بالمؤسسة	.875**	.792**
٤	توجد خطة لإدارة مخاطر الأمن السيبراني لأنظمة المعلومات الإدارية في المؤسسة	.718**	.782**
٥	يتم تقييم مخاطر الأمن السيبراني على أنظمة المعلومات الإدارية بشكل دوري في المؤسسة	.875**	.697**
٦	تلتزم الوحدات الإدارية بالمؤسسة بالمتطلبات التنظيمية لتحقيق الأمن السيبراني	.816**	.766**
٧	تطبق متطلبات الأمن السيبراني إدارة الأصول المعلوماتية والتقنية بالمؤسسة	.663**	.668**
٨	تطبق المؤسسة متطلبات الأمن السيبراني لحماية البريد الالكتروني	.882**	.792**
٩	تطبق المؤسسة متطلبات الأمن السيبراني لإدارة أمن الشبكات	.870**	.709**
١٠	تطبق المؤسسة متطلبات الامن السيبراني الخاصة بالأجهزة المحمولة والأجهزة الشخصية للموظفين	.772**	.662**
١١	تطبق المؤسسة متطلبات ا لأمن السيبراني لحماية بيانات ومعلومات الجامعة	.774**	.712**
١٢	تطبق المؤسسة متطلبات الأمن السيبراني للتشفير لأنظمة المعلومات الإدارية	.715**	.792**
١٣	تطبق المؤسسة متطلبات الامن السيبراني لإدارة النسخ الاحتياطية للبيانات والمعلومات الإدارية	.896**	.844**

جدول (٦) قيمة معامل الارتباط بين درجة كل عبارة ومجموع المحور المنتمية إليه والمجموع الكلي للاستبانة للمحور الأول (بعد المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني) (ن= ٣٠)

م	العبارات	معامل الارتباط	
		العبارة والمحور	العبارة والمجموع الكلي
١	توجد بالمؤسسة أنظمة حماية أمنية للأجهزة التقنية والحاسوبية.	.755**	.728**
٢	تحدث أنظمة وبرامج الحاسب الآلي بالمؤسسة بشكل دوري.	.811**	.802**
٣	تحدث برامج الحماية لأجهزة الحاسب الآلي بالمؤسسة.	.752**	.699**
٤	توجد أنظمة حماية للمعلومات السرية للمستخدم لأنظمة المعلومات الإدارية بالمؤسسة.	.813**	.827**
٥	تطبق متطلبات الامن السيبراني لإدارة هويات الدخول والصلاحيات للموظفين في المؤسسة.	.813**	.800**
٦	تطبق متطلبات الامن السيبراني لحماية أنظمة المعلومات الإدارية ومعالجة أجهزة المعلومات بالمؤسسة.	.667**	.711**
٧	توفر المؤسسة برامج حماية ضد الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة لأنظمة المعلومات الإدارية على أجهزة المؤسسة.	.816**	.699**
٨	تطبق متطلبات الأمن السيبراني الأصول المعلوماتية والتقنية بالمؤسسة.	.752**	.700**

٩	تطبق المؤسسة متطلبات الأمن السيبراني لحماية البريد الإلكتروني.	.663**	.580**
١٠	تطبق المؤسسة متطلبات الأمن السيبراني لإدارة أمن الشبكات.	.598**	.532**
١١	تطبق المؤسسة متطلبات الامن السيبراني الخاصة بالأجهزة المحمولة والأجهزة الشخصية للموظفين.	.733**	.809**
١٢	تطبق المؤسسة متطلبات الأمن السيبراني لحماية بيانات ومعلومات المؤسسة.	.700**	.732**
١٣	تطبع الوثائق السرية على طابعة خاصة في المؤسسة.	.899**	.852**
١٤	تمنع الإدارة نقل المعلومات الخاصة بالعمل للمنزل واستخدام جهاز الكمبيوتر الخاص بك للعمل عليها في المنزل.	.820**	.780**
١٥	لا يمكن استرداد المعلومات على جهاز الكمبيوتر الخاص بالعمل عند القيام بحذف ملف منها.	.829**	.697**
١٦	هناك نظام في المؤسسة يمنع تسجيل الدخول إلى حساب العمل باستخدام الكمبيوتر في أماكن عامة مثل المكتبة، مقهى انترنت أو لوبي فندق.	.902**	.876**
١٧	لا تستخدم نفس كلمة المرور لحسابات العمل التي تستخدمها لحساباتك الشخصية في المنزل مثل الفيس بوك، وتويتر، أو كلمة المرور الشخصية للبريد الالكتروني.	.698**	.630**
١٨	تمنع المؤسسة عن افصاحك عن كلمة المرور الخاصة بك لأي شخص داخل وخارج المؤسسة.	.761**	.880**
١٩	تمنع المؤسسة الرسائل الفورية (الدردشة) عبر الأجهزة والشبكات التابعة لها.	.942**	.861**
٢٠	لا يسمح بتنزيل البرامج وتثبيتها على جهاز الكمبيوتر الخاص بك في المؤسسة.	.739**	.899**
٢١	لا يمكن استخدام أجهزتك الشخصية مثل هاتفك المحمول لتخزين أو نقل معلومات سرية خاصة بالجامعة.	.741**	.708**
٢٢	تعرف بمن تتصل في حالة حدوث اختراق أو اعتداء على جهازك في العمل.	.825**	.802**

جدول (٧) قيمة معامل الارتباط بين درجة كل عبارة ومجموع المحور المنتمية إليه والمجموع الكلي للاستبانة للمحور الأول (بعد المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني) (ن= ٣٠)

م	العبارات	معامل الارتباط	
		العبارة والمحور	العبارة والمجموع الكلي
١	تقوم المؤسسة بتوعية الموظفين بأهمية تطبيق الأمن السيبراني	.775**	.712**
٢	تدرب المؤسسة الموظفين على متطلبات تحقيق الأمن السيبراني	.839**	.819**
٣	تؤهل المؤسسة الموارد البشرية القائمة على تقنية المعلومات في مجال تطبيق الامن السيبراني	.811**	.752**
٤	توفر المؤسسة الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات الإدارية	.716**	.702**
٥	تقيم المؤسسة لقاءات دورية للمختصين بتطبيق الامن السيبراني لتعريفهم بالمستجدات في المجال	.893**	.851**
6	تم توقيعك على بند (المحافظة على سرية المعلومات) قبل البدء في العمل بالمؤسسة	.699**	.653**

7	يتلقى الموظف قبل البدء في عمله توضيح بالمهام والمسؤوليات ذات العلاقة لأمن أنظمة المعلومات الإدارية في المؤسسة	.830**	.811**
8	توجد إجراءات واضحة لإدارة الأصول المعلوماتية التي تقع في عهدة الموظف كالأجهزة المحمولة	.858**	.891**

جدول (٨) قيمة معامل الارتباط بين درجة كل عبارة ومجموع المحور المنتمية إليه والمجموع الكلي للاستبانة للمحور الأول (بعد المتطلبات المادية اللازمة لتحقيق الأمن السيبراني) (ن= ٣٠)

م	العبارات	معامل الارتباط	
		العبارة والمحور	العبارة والمجموع الكلي
١	تمتلك المؤسسة نظام حماية عالي المستوى للأمن السيبراني	.879**	.861**
٢	توفر المؤسسة المتطلبات المادية اللازمة لتحقيق الامن السيبراني	.832**	.843**
٣	توفر المؤسسة نظام حماية عالي المستوى لأنظمة المعلومات الإدارية	.848**	.842**
٤	تزود المؤسسة منسوبيها بأجهزة حديثة ومتطورة لإدارة نظام المعلومات الإدارية بها	.905**	.894**
٥	توفر المؤسسة لأجهزة تقنية المعلومات الصيانة الدورية والمستمرة الضرورية لتحقيق الأمن السيبراني	.855**	.793**
6	تحدث المؤسسة برامج التطبيقات الحاسوبية لمنسوبيها باستمرار	.829**	.733**
7	تعمل المؤسسة على تجديد أجهزة الحاسب الآلي لمنسوبيها	.725**	.710**
8	توفر المؤسسة الدعم التقني اللازم لمنسوبيها لمعالجة المشكلات الطارئة	.809**	.811**
9	تمتلك المؤسسة برامج حديثة لتوفير الحماية والأمن السيبراني لأنظمة المعلومات الإدارية	.805**	.715**
10	تمتلك المؤسسة نظام حوكمة تقني لتوفير الامن السيبراني للتعاملات الإلكترونية	.781**	.723**
11	تمتلك المؤسسة نظام شبكي آمن لتبادل المعلومات الإدارية	.879**	.777**

يتضح من خلال الجداول (٥)، (٦)، (٧)، (٨) الخاصة بقيم معامل الارتباط بين درجة كل عبارة ومجموع المحور المنتمية إليه والمجموع الكلي للاستبانة للمحور الأول (واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية) والأبعاد الأربعة (المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني، المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني، المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني ، المتطلبات المادية اللازمة لتحقيق الأمن السيبراني) يتضح للباحثة أن قيمة (ر) المحسوبة أعلى من قيمتها المجدولة عند مستوى معنوية (٠.٠٥) وهو ما يظهر صدق الاتساق الداخلي لفقرات المحور الأول التي يبلغ عددها (٥٤ فقرة).

(٢) صدق الاتساق الداخلي للمحور الثاني (دور أنظمة الامن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية)

جدول (٩) قيمة معامل الارتباط بين درجة كل عبارة ومجموع المحور المنتمية إليه والمجموع الكلي للاستبانة للمحور الثاني (دور أنظمة الامن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية) (ن= ٣٠)

	العبارات	معامل الارتباط	
		العبارة والمحور	العبارة والمجموع الكلي
١	يتم تأمين أنظمة الأمن السيبراني ضد اختراق الشبكة والاطلاع على المعلومات الخاصة بالمؤسسة من خلال سرقة كلمة السر الخاصة بالمعنيين أثناء الفعاليات الرياضية الكبرى.	.718**	.665**
٢	يتم تأمين أنظمة الأمن السيبراني ضد التعرض للاختراق أثناء محاولة معالجة اختراق سابق للمواقع الإلكترونية الخاصة بالفعاليات الرياضية الكبرى.	.889**	.802**
٣	يتم تأمين أنظمة الأمن السيبراني ضد هجمات حقن قواعد البيانات من خلال إدخال برمجية ضارة مكان كلمة السر أو اسم المستخدم بحيث تمكن المحتال من الوصول إلى قواعد البيانات الخاصة بالفعاليات الرياضية الكبرى بهدف سرقتها أو التعديل فيها أو تدميرها.	.696**	.791**
٤	يتم تأمين أنظمة الأمن السيبراني ضد ادعاء جهة معينة بأنها جهة موثوق بها من قبل مستخدم تابع للفعاليات الرياضية الكبرى تطلب منه إستخدام ملف مرفق يكون ضارا به.	.817**	.765**
٥	يتم تأمين أنظمة الأمن السيبراني ضد ادعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم التابع للفعاليات الرياضية الكبرى، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر.	.908**	.836**
٦	يتم تأمين أنظمة الأمن السيبراني ضد وصول رسالة مزيفة على شكل رابط من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها.	.852**	.715**
٧	يتم تأمين أنظمة الأمن السيبراني ضد البرامج التي تظهر بأنها تعمل بشكل معين ومفيد للمستخدم بينما هي في الواقع تقوم بعمل ضار وخفي عن المستخدم مثل الاضرار بالحاسوب أو إرسال معلومات إلى المحتال عن الفعاليات الرياضية الكبرى.	.849**	.671**
٨	يتم تأمين أنظمة الأمن السيبراني المواقع الإلكترونية للفعاليات الرياضية الكبرى ضد الفيروسات وهي برامج تدخل إلى الحاسوب وتتصل بالملفات المخزنة به ثم تكرر نفسها بحيث يتم تدمير هذه الملفات.	.828**	.768**
٩	يتم تأمين أنظمة الأمن السيبراني الفعاليات الرياضية الكبرى ضد البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. والتي يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الانترنت	.833**	.719**

يتضح من خلال الجدول (٩) الذي يتناول قيمة معامل الارتباط بين درجة كل عبارة ومجموع المحور المنتمية إليه والمجموع الكلي للاستبانة للمحور الثاني (دور أنظمة الأمن السيبراني في تأمين

الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية) يتضح للباحثة أن قيمة (ر) المحسوبة أعلى من قيمتها المجدولة عند مستوى معنوية (٠.٠٥) وهو ما يظهر صدق الاتساق الداخلي لفقرات المحور الثاني التي يبلغ عددها (٩ فقرات).

نتائج الدراسة ومناقشتها

عرض نتائج التحليل الاحصائي للمتغيرات الديموغرافية للمشاركين بالاستجابة على استمارة الاستقصاء

جدول (٩) نتائج التحليل الاحصائي للمتغيرات الديموغرافية للمشاركين بالاستجابة على استمارة الاستقصاء

(ن= ١٥٥)

المتغير		التكرار	النسبة
النوع	ذكر	٩٧	%٦٢.٦
	أنثى	٥٨	%٣٧.٤
العمر	٣٥ سنة أو أقل	٦٨	%٣٤.٩
	٣٦ – ٥٩ سنة	٧٨	%٥٠.٣
	أكبر من ٦٠ سنة	٩	%٥.٨
نوع المؤسسة المنتظمة للفعاليات الرياضية التي تعمل بها	نادي	٣٤	%٢١.٩
	اتحاد	١٧	%١١
	شركة	٩٩	%٦٣.٩
	أخرى	٥	%٣.٢
هل سمعت عن أنظمة الأمن السيبراني؟ (فقط إذا كانت إجابتك نعم يمكنك إكمال تعبئة الاستبيان)	نعم	١٥٥	%١٠٠
	لا	٠	%٠
هل تستخدم مؤسستك بعض أنظمة الأمن السيبراني خلال التنظيم للفعاليات الرياضية؟	نعم	١٥٥	%١٠٠
	لا	٠	%٠
الإجمالي		١٥٥	%١٠٠

من خلال الجدول رقم (١٠) الذي يتناول نتائج التحليل الاحصائي للمتغيرات الديموغرافية للمشاركين بالاستجابة على استمارة الاستقصاء يتضح للباحثة أن المشاركين الذكور يمثلون (٦٢.٦%) بينما الإناث (٣٧.٤%)، وفيما يتعلق بالفئات العمرية للمشاركين يتضح ان من هم(٣٦) حتى(٥٩) سنة يمثلون (٥٠.٤%)، ومن هم (٣٥) سنة فأقل يمثلون (٣٤.٨%)، أما الفئة العمرية أكبر من(٦٠) سنة فيمثلون (٥.٨%)، وفيما يتعلق بنوع المؤسسة المنتظمة للفعاليات الرياضية يتضح ان (٦٣.٩%) من المشاركين يعملون في شركات، ويعمل (٢١.٩%) في الأندية، ويعمل(١١%) في الاتحادات الرياضية، بينما يعمل (٣.٢%) في مؤسسات أخرى، ويظهر التحليل أن (١٠٠%) من المشاركين قد سمعوا عن أنظمة الأمن السيبراني، وفيما يتعلق باستخدام المؤسسة لبعض أنظمة الأمن السيبراني خلال التنظيم للفعاليات الرياضية يتضح للباحثة أن (١٠٠%) من المشاركين يعملون في مؤسسات تستخدم بعض أنظمة الأمن السيبراني خلال التنظيم للفعاليات الرياضية.

عرض نتائج السؤال الأول ومناقشتها:

نص السؤال الأول على " ما هو واقع استخدام أنظمة الأمن السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين؟"

حتى يمكن الإجابة على هذا السؤال تم حساب المتوسطات الحسابية والأهمية النسبية لاستجابات عينة الدراسة على عبارات محور " واقع استخدام أنظمة الأمن السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين"، وذلك من خلال أربعة أبعاد هي واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية) والأبعاد الأربعة (المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني، المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني، المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني ، المتطلبات المادية اللازمة لتحقيق الأمن السيبراني) ، حيث اشتمل هذا المحور على (٥٤) فقرة، وجاءت النتائج كما هو موضح في الجداول (١١-١٢-١٣-١٤)

الجدول رقم (١١) بعد استجابات العينة لبعد المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني (ن = ١٥٥)

	أوافق بشدة	أوافق	محايد	لا اوافق	لا أوافق بشدة	المتوسط الحسابي	الأهمية النسبية	اتجاه العبارة
	%	%	%	%	%			
١. توجد إدارة خاصة بالأمن السيبراني في المؤسسة	43.20%	36.70%	15.00%	4.00%	1.10%	3.65	%73	مرتفع
٢. توجد سياسات أمنية لأنظمة المعلومات الإدارية بالمؤسسة	35.90%	33.80%	22%	7.30%	1%	3.62	%72.4	مرتفع
٣. تطبق الإجراءات الإدارية اللازمة لتحقيق الأمن السيبراني داخل أنظمة المعلومات الإدارية بالمؤسسة	31.70%	40.30%	18.80%	8%	1.20%	3.67	%73.4	مرتفع
٤. توجد خطة لإدارة مخاطر الأمن السيبراني لأنظمة المعلومات الإدارية في المؤسسة	49.00%	30.50%	17.90%	2.20%	0.40%	3.78	%75.6	مرتفع
٥. يتم تقييم مخاطر الأمن السيبراني على أنظمة المعلومات الإدارية بشكل دوري في المؤسسة	49.00%	28.00%	16.00%	2.90%	4.10%	3.84	%76.8	مرتفع

٦. تلتزم الوحدات الإدارية بالمؤسسة بالمتطلبات التنظيمية لتحقيق الأمن السيبراني	62.80%	22.70%	3.90%	6.40%	4.20%	4.00	%80	مرتفع
٧. تطبق متطلبات الأمن السيبراني إدارة الأصول المعلوماتية والتقنية بالمؤسسة	38.50%	29.70%	24.40%	6.00%	1.40%	3.94	%78.8	مرتفع
٨. تطبق المؤسسة متطلبات الأمن السيبراني لحماية البريد الالكتروني	36.40%	44.20%	9.80%	4.70%	4.90%	4.03	%80.6	مرتفع
٩. تطبق المؤسسة متطلبات الأمن السيبراني لإدارة أمن الشبكات	25.40%	48.20%	17.50%	6.60%	2.30%	٣.٨٣	%77	مرتفع
١٠. تطبق المؤسسة متطلبات الامن السيبراني الخاصة بالأجهزة المحمولة والأجهزة الشخصية للموظفين	46.10%	30.00%	18.50%	4.00%	1.40%	3.89	%77.8	مرتفع
١١. تطبق المؤسسة متطلبات ا لأمن السيبراني لحماية بيانات ومعلومات الجامعة	37.10%	40.20%	19.60%	3.00%	0.10%	3.85	%77	مرتفع
١٢. تطبق المؤسسة متطلبات الأمن السيبراني للتشفير لأنظمة المعلومات الإدارية	39.00%	37.40%	20.80%	2.70%	0.10%	3.86	%77.2	مرتفع
١٣. تطبق المؤسسة متطلبات الامن السيبراني لإدارة النسخ الاحتياطية للبيانات والمعلومات الإدارية	41.00%	27.60%	16.40%	10.20 %	4.80%	3.76	%75.2	مرتفع
المجموع	42.37%	34.37%	16.12%	4.98%	2.16%	٣.٨٢	%٧٦.٤	مرتفع

يتبين من الجدول (١١) أنه يوجد مستوى مرتفع من المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني، وهو ما يعزى المتوسط الحسابي الإجمالي وهو (٣.٨٢) من (٥.٠٠) لجميع فقرات هذا البعد، وهو متوسط مرتفع، ولقد حصلت الفقرة الثامنة على أعلى درجة بمتوسط حسابي (٤.٠٣) وأهمية نسبية (٧٣.٨%)، وهو ما يدل على موافقة المشاركين على محتوى الفقرة الذي ينص على " تطبق المؤسسة متطلبات الأمن السيبراني لحماية البريد الالكتروني"، حيث تجد الباحثة أن أخطر التهديدات الواقعة على النواحي الإدارية هي الموجهة نحو البريد الإلكتروني الذي يحتوي على معلومات إدارية عديدة يمكن من

خلالها تهديد إقامة الفعاليات الرياضية، وهذا ما أكده الجنابي والحسيناوي (٢٠١٤)، كما يتضح من خلال الجدول (١١) كذلك أن الفقرة الثانية قد حصلت على أدنى درجة بمتوسط حسابي (٣.٦٢)، وأهمية نسبية (٧٢.٤%)، وهو ما يدل على وجود مستوى متوسط من الموافقة من المشاركين على محتوى الفقرة الذي ينص على " توجد سياسات أمنية لأنظمة المعلومات الإدارية بالمؤسسة ". وترى الباحثة ان الترتيبات الإدارية يمكنها تحقيق الأمن السيبراني ومجابهة تهديداته على الفعاليات الرياضية الكبرى في مملكة البحرين ولعل حصول الفقرة الثانية على أدنى درجة مع وجود مستوى مرتفع من التطبيق وموافقة أفراد العينة على وجود سياسات أمنية لأنظمة المعلومات الإدارية بالمؤسسة كل كذلك يعتبر مؤشر لضرورة إيلاء مزيد من الاهتمام بالسياسات الأمنية مستقبلاً خشية تعرض الفعاليات لتهديدات سيبرانية قد تعطل تنفيذها وهو ما يعود بالخسارة الكبيرة على مملكة البحرين، وقد تشابهت هذه النتيجة مع نتيجة دراسة إليوت وجينكنسون (٢٠٢٠).

الجدول رقم (١٥) استجابات العينة لبعد المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني (ن = ١٥٥)

	أوافق بشدة	أوافق	محايد	لا اوافق	لا أوافق بشدة	المتوسط الحسابي	الأهمية النسبية	اتجاه العبارة
	%	%	%	%	%			
١.توجد بالمؤسسة أنظمة حماية أمنية للأجهزة التقنية والحاسوبية	%٤٠.٨٠	%٢٥.٣٠	%١٣.٢٠	%١٥.٩٠	%٤.٨٠	٣.٩٧	%79.4	مرتفع
٢.تحدث أنظمة وبرامج الحاسب الآلي بالمؤسسة بشكل دوري	%٢٧.٣٠	%٤٤.١٠	%١٠.٠٠	%١٠.٠٠	%٨.٦٠	٣.١٢	%62.4	متوسط
٣.تحدث برامج الحماية لأجهزة الحاسب الآلي بالمؤسسة	%٤٦.٠٠	%٢٨.٠٠	%٩.٠٠	%١٤.٠٠	%٣.٠٠	٣.٤٧	%69.4	مرتفع
٤.توجد أنظمة حماية للمعلومات السرية للمستخدم لأنظمة المعلومات الإدارية بالمؤسسة	%٤٧.٧٠	%٢٧.٣٠	%١٩.٣٠	%٤.٥٠	%١.٢٠	٣.٣٢	%66.4	متوسط
٥.تطبق متطلبات الامن السيبراني لإدارة هويات الدخول والصلاحيات للموظفين في المؤسسة	%٥٦.٧٠	%٣٣.٥٠	%٦.٢٠	%٢.٦٠	%١.٠٠	3.99	%79.8	مرتفع
٦.تطبق متطلبات الامن السيبراني لحماية أنظمة المعلومات الإدارية ومعالجة أجهزة المعلومات بالمؤسسة	%٢٣.٠٠	%٢٨	%٣٣.٠٠	%٢.٤٠	%١٣.٦٠	3.35	%67	متوسط

٧. توفر المؤسسة برامج حماية ضد الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة لأنظمة المعلومات الإدارية على أجهزة المؤسسة	%٥٩.٥٠	%٣٤.٠٠	%٣.١٠	%١.١٠	%٢.٣٠	3.91	%78.2	مرتفع
٨. تطبق متطلبات الأمن السيبراني الأصول المعلوماتية والتقنية بالمؤسسة	%٥٦.٢٠	%٢٥.٤٠	%١٢.٠٠	%٥.٤٠	%١.٠٠	4.1	%82	مرتفع
٩. تطبق المؤسسة متطلبات الأمن السيبراني لحماية البريد الإلكتروني	%٥٤.٠٠	%٣٣.٢٠	%٧.٢٠	%٤.٠٠	%١.٦٠	4.22	%84.4	مرتفع
١٠. تطبق المؤسسة متطلبات الأمن السيبراني لإدارة أمن الشبكات	%٤٠.٣٠	%٣٧.٩٠	%١٠.٥٠	%٧.٩٠	%٣.٤٠	3.82	%76.4	مرتفع
١١. تطبق المؤسسة متطلبات الامن السيبراني الخاصة بالأجهزة المحمولة والأجهزة الشخصية للموظفين	%٣٩.٠٠	%٣٧.٤٠	%٢٠.٨٠	%٢.٧٠	%٠.١٠	4.32	%86.4	مرتفع
١٢. تطبق المؤسسة متطلبات الأمن السيبراني لحماية بيانات ومعلومات المؤسسة	%٤٨.١٠	%٣٠.٥٠	%١٢.٣٠	%٤.١٠	%٥.٠٠	4.33	%86.6	مرتفع
١٣. تطبع الوثائق السرية على طابعة خاصة في المؤسسة	%٢٩.٠٠	%٣٠.٠٠	%٣٠.٨٠	%٩.٢٠	%١.٠٠	3.26	%65.2	متوسط
١٤. تمنع الإدارة نقل المعلومات الخاصة بالعمل للمنزل واستخدام جهاز الكمبيوتر الخاص بك للعمل عليها في المنزل	%٥٥.٠٠	%٢٩.٦٠	%١٢.٠٠	%٢.٤٠	%١.٠٠	4.45	%89	مرتفع
١٥. لا يمكن استرداد المعلومات على جهاز الكمبيوتر الخاص بالعمل عند القيام بحذف ملف منها	%٣٤.٠٠	%٢٢.٠٠	%٥.٠٠	%٣٤.٠٠	%٥.٠٠	2.55	%51	مرتفع
١٦. هناك نظام في المؤسسة يمنع تسجيل الدخول إلى حساب العمل باستخدام الكمبيوتر في أماكن عامة مثل المكتبة، مقهى انترنت أو لوبي فندق	%٥١.٩٠	%٣٠.٤٠	%٣.١٠	%٧.٠٠	%٧.٦٠	4.19	%83.8	مرتفع

١٧. لا تستخدم نفس كلمة المرور لحسابات العمل التي تستخدمها لحساباتك الشخصية في المنزل مثل الفيس بوك ، وتويتر، أو كلمة المرور الشخصية للبريد الالكتروني	%٤٤.٠٠	%٤١.٠٠	%٦.٠٠	%٤.٠٠	%٥.٠٠	3.76	%75.2	مرتفع
١٨. تمنع المؤسسة عن افصاحك عن كلمة المرور الخاصة بك لأي شخص داخل وخارج المؤسسة	%٣٩.٨٠	%٣٦.٤٠	%١٨.٠٠	%٤.٦٠	%١.٢٠	3.68	%73.6	مرتفع
١٩. تمنع المؤسسة الرسائل الفورية (الدردشة) عبر الأجهزة والشبكات التابعة لها	%٤٩.١٠	%٣٠.٦٠	%١٥.٧٠	%٢.٨٠	%١.٨٠	3.97	%79.4	مرتفع
٢٠. لا يسمح بتنزيل البرامج وتثبيتها على جهاز الكمبيوتر الخاص بك في المؤسسة	%٤٥.٥٠	%٣١	%١٣.٢٠	%٢.٤٠	%٨.٣٠	4.0	%80	مرتفع
٢١. لا يمكن استخدام أجهزتك الشخصية مثل هاتفك المحمول لتخزين أو نقل معلومات سرية خاصة بالجامعة	%٦٤.٠٠	%٣١.٠٠	%٢.٠٠	%١.٥٠	%١.٥٠	4.18	%83.6	مرتفع
٢٢. تعرف بمن تتصل في حالة حدوث اختراق أو اعتداء على جهازك في العمل	%٤٠.٦٠	%٣٩.٧٠	%١٠.٠٠	%٥.٠٠	%٤.٧٠	3.80	%76	مرتفع
المجموع	45.07%	32.09%	12.38%	6.70%	3.76%	3.80	%76.1	مرتفع

يتبين من الجدول (١٢) أنه يوجد مستوى مرتفع من المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني ، وهو ما يعزى المتوسط الحسابي الإجمالي وهو (٣.٨٠) من (٥.٠٠) لجميع فقرات هذا البعد، وهو متوسط مرتفع، ولقد حصلت الفقرة الرابعة عشر على أعلى درجة بمتوسط حسابي (٤.٤٥) وأهمية نسبية (٧٣.٨%)، وهو ما يدل على موافقة المشاركين بشدة على محتوى الفقرة الذي ينص على " تمنع الإدارة نقل المعلومات الخاصة بالعمل للمنزل واستخدام جهاز الكمبيوتر الخاص بك للعمل عليها في المنزل "، ويعتبر هذا الإجراء من أهم الإجراءات التي يمكنها أن تحول دون وقوع تهديد سيبراني على المعلومات الخاصة بالفعاليات الرياضية الكبرى في مملكة البحرين، حيث أن الاحتفاظ بالبيانات داخل الإطار المؤسسي وعلى أجهزة هذه المؤسسة فقط يقلل من فرص سرقة هذه البيانات (جمال الدين، ٢٠٢٣)، كما يتضح من خلال الجدول (١٢) كذلك أن الفقرة الخامسة عشر قد حصلت على أدنى درجة بمتوسط حسابي (٢.٥٥)، وأهمية نسبية (٥١.٤%)، وهو ما يدل على وجود مستوى منخفض من

الموافقة للمشاركين على محتوى الفقرة الذي ينص على " لا يمكن استرداد المعلومات على جهاز الكمبيوتر الخاص بالعمل عند القيام بحذف ملف منها" ، وتعزو الباحثة هذه النتيجة إلى أن تأمين البيانات الخاصة بالفعاليات الرياضية الكبرى يرتكز أساساً على تأمين الأجهزة التي تحتوي على هذه البيانات، حيث أن قابلية استرداد البينات المحذوفة بالخطأ أو عن عمد يعطي الإداريين فرصاً أكبر للحفاظ على هذه البيانات من الضياع، ،وتجد الباحثة كذلك بأن رغم أهمية هذه الخاصية على حماية المعلومات من الضياع، إلا أنها سلاح ذو حدين، يمكن من خلالها أن تتحول إلى تهديد على نجاح أي فعالية لذلك فإن هذا الجانب يتطلب تأمين الدخول على الأجهزة الخاصة بالعمل، وحماية المستخدمين بكلمات سر.

الجدول رقم (١٣) استجابات العينة لبعد المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني(ن = ١٥٥)

	أوافق بشدة	أوافق	محايد	لا اوافق	لا أوافق بشدة	المتوسط الحسابي	الأهمية النسبية	اتجاه العبارة
	%	%	%	%	%			
١.تقوم المؤسسة بتوعية الموظفين بأهمية تطبيق الأمن السيبراني	%٥٣.٠٠	%٣٦.٨٠	%٦.٧٠	%٢.٥٠	%١.٠٠	4.25	%85	مرتفع
٢.تدرب المؤسسة الموظفين على متطلبات تحقيق الأمن السيبراني	%٦١.٠٠	%٢٦	%٥	4.00%	4%	4.27	%85.4	مرتفع
٣.تؤهل المؤسسة الموارد البشرية القائمة على تقنية المعلومات في مجال تطبيق الامن السيبراني	%٤٩.٠٠	%٢٧.٥٠	%١٢.٤٠	%٥.١٠	6.00%	4.33	%86.6	مرتفع
٤.توفر المؤسسة الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات الإدارية	53.90%	%٢٦.٠٠	%١.٠٠	%٦.٨٠	%١٢.٣٠	4.39	%87.8	مرتفع
٥.تقيم المؤسسة لقاءات دورية للمختصين بتطبيق الامن السيبراني لتعريفهم بالمستجدات في المجال	%٤١.٥٠	32.60%	%١٨.٠٠	%٤.٩٠	%٣.٠٠	3.71	%74.2	مرتفع
٦.تم توقيعك على بند (المحافظة على سرية المعلومات) قبل البدء في العمل بالمؤسسة	%٢٢.٣٠	%٤١.٢٠	%٢٥.٠٠	%٥.١٠	6.40%	3.15	%63	متوسط

٧.يتلقى الموظف قبل البدء في عمله توضيح بالمهام والمسؤوليات ذات العلاقة لأمن أنظمة المعلومات الإدارية في المؤسسة	44.50%	%٣٣.٥٠	%٣.٥٠	%٧.٠٠	%١١.٥٠	٣.٩١	%78.2	مرتفع
٨.توجد إجراءات واضحة لإدارة الأصول المعلوماتية التي تقع في عهدة الموظف كالأجهزة المحمولة	%٤٢.٠٠	28.10%	%١٦.٤٠	%٤.٥٠	%٩.٠٠	٣.٨٨	%77.6	مرتفع
المجموع	45.90%	31.46%	11.00%	4.99%	6.65%	٣.٩٨	%٧٩.٧	مرتفع

يتبين من الجدول (١٣) أنه يوجد مستوى مرتفع من المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني، وهو ما يعزى المتوسط الحسابي الإجمالي وهو (٣.٩٨) من (٥.٠٠) لجميع فقرات هذا البعد، وهو متوسط مرتفع، ولقد حصلت الفقرة الرابعة على أعلى درجة بمتوسط حسابي (٤.٣٩) وأهمية نسبية (٨٧.٨%)، وهو ما يدل على موافقة المشاركين بشدة على محتوى الفقرة الذي ينص على " توفر المؤسسة الدعم الفني اللازم لتطبيق الأمن السيبراني لأنظمة المعلومات الإدارية "، وتعزو الباحثة هذه النتيجة إلى أن هذا الإجراء يعتبر من أهم الإجراءات التي يمكنها أن تحول دون وقوع تهديد سيبراني على المعلومات الخاصة بالفعاليات الرياضية الكبرى، حيث أن الدعم الفني المستمر للعاملين يمنع وقوع تهديدات سيبرانية يكون مصدرها الفيروسات أو الهجمات الإلكترونية التي ترتكز على ضعف صيانة الأجهزة أو تحديث البرامج والتطبيقات المستخدمة (بن زرارة وأعراب، ٢٠٢٣)، كما يتضح من خلال الجدول (١٣) كذلك أن الفقرة السادسة قد حصلت على أدنى درجة بمتوسط حسابي (٣.١٥)، وأهمية نسبية (٥١.٤%)، وهو ما يدل على وجود مستوى منخفض من الموافقة للمشاركين على محتوى الفقرة الذي ينص على " تم توقيعك على بند (المحافظة على سرية المعلومات) قبل البدء في العمل بالمؤسسة "، وتعزو الباحثة هذه النتيجة وجود ثغرات في التعليمات الخاصة بقرارات واتفاقيات وعقود العمل في بعض المؤسسات في هذ الجانب الهام، حيث يؤكة شفيق (٢٠١٨) إلى أن إلزام العاملين بالحفاظ على سرية البيانات في موقع العمل أمر محوري، فمن خلال توقيع العاملين على تعليمات وتوجيهات الحفاظ على السرية للمستخدمين من العاملين يعتبر جزء لا يتجزأ من مخططات الحفاظ على سرية البيانات.

الجدول رقم (١٤) استجابات العينة لبعد المتطلبات المادية اللازمة لتحقيق الأمن السيبراني (ن = ١٥٥)

	أوافق بشدة	أوافق	محايد	لا اوافق	لا أوافق بشدة	المتوسط الحسابي	الأهمية النسبية	اتجاه العبارة
	%	%	%	%	%			
١. تمتلك المؤسسة نظام حماية عالي المستوى للأمن السيبراني	43.10%	36.40%	6.00%	11.00%	3.50%	3.85	%77	مرتفع
٢.توفر المؤسسة المتطلبات المادية اللازمة لتحقيق الامن السيبراني	37.00%	35.90%	12.00%	8.00%	7.10%	3.89	%77.8	مرتفع
٣.توفر المؤسسة نظام حماية عالي المستوى لأنظمة المعلومات الإدارية	%٤٩.٠٠	31.00%	8.60%	7.50%	3.90%	4.12	%82.4	مرتفع
٤.تزود المؤسسة منسوبيها بأجهزة حديثة ومتطورة لإدارة نظام المعلومات الإدارية بها	36.00%	29.00%	15.20%	12.90%	6.90%	3.66	%73.2	مرتفع
٥.توفر المؤسسة لأجهزة تقنية المعلومات الصيانة الدورية والمستمرة الضرورية لتحقيق الأمن السيبراني	33.00%	41.50%	5.20%	11.70%	8.60%	3.70	%74	مرتفع
٦.تحدث المؤسسة برامج التطبيقات الحاسوبية لمنسوبيها باستمرار	46.50%	25.40%	13.00%	7.50%	7.60%	4.01	%80.2	مرتفع
٧.تعمل المؤسسة على تجديد أجهزة الحاسب الآلي لمنسوبيها	%٤٧.٧٠	33.40%	10.80%	6.40%	1.70%	4.15	%83	مرتفع
٨.توفر المؤسسة الدعم التقني اللازم لمنسوبيها لمعالجة المشكلات الطارئة	44.90%	30.00%	16.40%	2.00%	6.70%	4.20	%84	مرتفع
٩.تمتلك المؤسسة برامج حديثة لتوفير الحماية والأمن السيبراني لأنظمة المعلومات الإدارية	56.00%	33.00%	4.50%	3.60%	2.90%	4.26	%85.2	مرتفع

١٠. تمتلك المؤسسة نظام حوكمة تقني لتوفير الامن السيبراني للتعاملات الإلكترونية	37.50%	24.80%	17.70%	8.30%	11.70%	3.75	%75	مرتفع
١١. تمتلك المؤسسة نظام شبكي آمن لتبادل المعلومات الإدارية	%٣٨.٠٠	34.00%	10.80%	9.00%	8.20%	3.81	%76.2	مرتفع
١٢. تمتلك المؤسسة نظام حماية عالي المستوى للأمن السيبراني	62.00%	31.00%	2.10%	3.00%	1.90%	4.38	%87.6	مرتفع
المجموع	%٤٤.٢٣	%٣٢.١٢	%١٠.١٩	%٧.٥٨	%٥.٨٩	3.77	%٧٥.٤	مرتفع

يتبين من الجدول (14) أنه يوجد مستوى مرتفع من المتطلبات المادية اللازمة لتحقيق الأمن السيبراني ، وهو ما يعزى المتوسط الحسابي الإجمالي وهو (٣.٧٧) من (٥.٠٠) لجميع فقرات هذا البعد، وهو متوسط مرتفع، ولقد حصلت الفقرة التاسعة على أعلى درجة بمتوسط حسابي (٤.٢٦) وأهمية نسبية (٨٥.٢%)، وهو ما يدل على موافقة المشاركين بشدة على محتوى الفقرة الذي ينص على " تمتلك المؤسسة برامج حديثة لتوفير الحماية والأمن السيبراني لأنظمة المعلومات الإدارية "، ويعتبر هذا الإجراء من أهم الإجراءات التي يمكنها أن تحول دون وقوع تهديد سيبراني على المعلومات الخاصة بالفعاليات الرياضية الكبرى في مملكة البحرين– كما تجده الباحثة – ويؤكد على ذلك إليوت وجينكنسون (٢٠٢٠)، الذين أيدوا بأن استخدام البرامج الحديثة في توفير الحماية لأنظمة المعلومات هو وسيلة فاعلة للتصدي لأية هجمات معلوماتية، كما ويتضح من خلال الجدول (١٤) كذلك أن الفقرة الرابعة قد حصلت على أدنى درجة بمتوسط حسابي (٣.٦٦)، وأهمية نسبية (٥١.٤%)، حيث نصت الفقرة على " تزود المؤسسة منسوبيها بأجهزة حديثة ومتطورة لإدارة نظام المعلومات الإدارية " ورغم أن الدرجة تعتبر مرتفعة إلا أن الباحثة ترى أن الأجهزة الحديثة ليست بحجم أهمية البرامج المستخدمة فيها، فقد يكون الجهاز ليس جديد أو متطور، لكن البرامج التي تمت برمجتها في هذا الجهاز ذات كفاءة وفاعلية عالية في تقديم الحماية.

جدول رقم (15) إستجابات عينة الدراسة على عبارات محور واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية (ن = 155)

م	البعد	عدد الفقرات	الأهمية النسبية	الترتيب
١	**المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني**	13	%٧٦.٤	2
٢	**المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني**	22	%76.1	3
٣	**المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني**	8	%٧٩.٧	1
	المتطلبات المادية اللازمة لتحقيق الأمن السيبراني	11	%75.4	4

الأهمية النسبية الإجمالية لجميع فقرات وأبعاد محور الأمن السيبراني ودوره في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين	54	76.9%	

يتبين من الجدول (15) التحليل الإجمالي النتائج محور " واقع أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية " ، والذي تضمن (٥٤) أن أنظمة الامن السيبراني في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية في مملكة البحرين ذات مستوى مرتفع من الفاعلية، وهو ما يفسر في ضوء الأهمية النسبية للفقرات الـ (٥٤) التي شملها هذا المحور، حيث بلغت الأهمية النسبية الإجمالية (٧٦.٩%) وهي أهمية مرتفعة، وتعتبر المتطلبات البشرية اللازمة لتحقيق الأمن السيبراني هي ذات الأهمية النسبية الأعلى (٧٩.٧%)، ثم جاءت المتطلبات الادارية اللازمة لتحقيق الأمن السيبراني في الترتيب الثاني من حيث الأهمية النسبية التي بلغت(٧٦.٤%)، ثم المتطلبات التقنية اللازمة لتحقيق الأمن السيبراني بأهمية نسبية (٧٦.١%)، وأخيراً المتطلبات المادية اللازمة لتحقيق الأمن السيبراني بأهمية نسبية (٧٥.٤%) وتعزو الباحثة هذه النتيجة إلى أن العنصر البشري هو الأهم في العملية الإدارية، فمهما تم تأمير توفر المتطلبات المادية والإدارية، ولم يتوفر العنصر البشري المؤهل ذو الكفاءة، فلا فائدة من جميع المتطلبات الأخرى (الخاطر، ٢٠٢١)، وأن المتطلبات الإدارية يأتي بعدها من خلال الدور الذي تلعبه في تحقيق الضبط والالتزام في تطبيق التقنيات التي تعزز قدرة المؤسسات على التصدي لتهديدات الأمن السيبراني، وقد تشابهت هذه النتيجة من نتائج دراسة (الغيبوي، ٢٠٢٠).

عرض نتائج السؤال الثاني ومناقشتها:

نص السؤال الثاني على " إلى أي مدى تسهم أنظمة الأمن السيبراني في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين؟"، وللإجابة على هذا التساؤل قامت الباحثة بحساب المتوسطات الحسابية والأهمية النسبية لاستجابات عينة الدراسة على عبارات محور "دور أنظمة الامن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية"، ولقد اشتمل هذا المحور على (٩) فقرات، وجاءت النتائج كما هو موضح في الجدول (١٦)

الجدول رقم (١٦) استجابات العينة لمحور دور أنظمة الامن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية (ن = ١٥٥)

	أوافق بشدة	أوافق	محايد	لا اوافق	لا أوافق بشدة	المتوسط الحسابي	الأهمية النسبية	اتجاه العبارة
	%	%	%	%	%			
١. يتم تأمين أنظمة الامن السيبراني ضد اختراق الشبكة والاطلاع على المعلومات الخاصة بالمؤسسة من خلال سرقة كلمة السر الخاصة بالمعنيين أثناء الفعاليات الرياضية الكبرى	41.00%	26.00%	15.00%	15.00%	3.00%	3.84	%77	مرتفع
٢. يتم تأمين أنظمة الامن السيبراني ضد التعرض للاختراق أثناء محاولة معالجة اختراق سابق للمواقع الإلكترونية الخاصة بالفعاليات الرياضية الكبرى	36.00%	36.00%	13.00%	10.00%	5.00%	3.92	%79.8	مرتفع
٣. يتم تأمين أنظمة الامن السيبراني ضد هجمات حقن قواعد البيانات من خلال إدخال برمجية ضارة مكان كلمة السر أو اسم المستخدم بحيث تمكن المحتال من الوصول إلى قواعد البيانات الخاصة بالفعاليات الرياضية الكبرى بهدف سرقتها أو التعديل فيها أو تدميرها	42.50%	33.50%	8.70%	10.30%	5.00%	3.77	%81.6	مرتفع
٤. يتم تأمين أنظمة الامن السيبراني ضد ادعاء جهة معينة بأنها جهة موثوق بها من قبل مستخدم تابع للفعاليات الرياضية الكبرى تطلب منه إستخدام ملف مرفق يكون ضارا به	39.40%	35.20%	13.70%	9.20%	2.50%	3.65	%75.8	مرتفع
٥. يتم تأمين أنظمة الامن السيبراني ضد ادعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم التابع للفعاليات الرياضية الكبرى، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر	38.40%	41.90%	5.90%	10.00%	3.80%	3.97	%76	مرتفع
٦. يتم تأمين أنظمة الامن السيبراني ضد وصول رسالة مزيفة على شكل رابط من جهة (غالبا مالية ومعروفة) لطلب معلومات أو التحقق منها	51.00%	29.00%	11.00%	9.00%	%٠.٠٠	3.70	%75	مرتفع

٧. يتم تأمين أنظمة الامن السيبراني ضد البرامج التي تظهر بأنها تعمل بشكل معين ومفيد للمستخدم بينما هي في الواقع تقوم بعمل ضار وخفي عن المستخدم مثل الاضرار بالحاسوب أو إرسال معلومات إلى المحتال عن الفعاليات الرياضية الكبرى	41.00%	39.00%	10.00%	9.00%	1.00%	4.11	80%	مرتفع
٨. يتم تأمين أنظمة الامن السيبراني المواقع الإلكترونية للفعاليات الرياضية الكبرى ضد الفيروسات وهي برامج تدخل إلى الحاسوب وتتصل بالملفات المخزنة به ثم تكرر نفسها بحيث يتم تدمير هذه الملفات	46.90%	31.70%	5.00%	3.00%	13.40%	4.00	%80.6	مرتفع
٩. يتم تأمين أنظمة الامن السيبراني الفعاليات الرياضية الكبرى ضد البرمجيات التي تؤدي إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب. والتي يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الانترنت	43.00%	39.00%	4.00%	10.00%	4.00%	4.02	%82.2	مرتفع
المجموع	42.13%	34.59%	9.59%	9.50%	4.19%	٣.٩٣	%٧٨.٦	مرتفع

يتبين الجدول (١٦) أنه يوجد ارتفاع في مستوى فاعلية الدور الذي تلعبه أنظمة الأمن السيبراني في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية، وهو ما يعزى إلى المتوسط الحسابي الإجمالي وهو (٣.٩٣) من (٥.٠٠) لجميع فقرات هذا المحور، وهو متوسط مرتفع، ولقد حصلت الفقرة السابعة على أعلى درجة بمتوسط حسابي (٤.١١) وأهمية نسبية (٨٠%)، وهو ما يدل على موافقة المشاركين على محتوى الفقرة الذي ينص على " يتم تأمين أنظمة الأمن السيبراني ضد البرامج التي تظهر بأنها تعمل بشكل معين ومفيد للمستخدم بينما هي في الواقع تقوم بعمل ضار وخفي عن المستخدم مثل الاضرار بالحاسوب أو إرسال معلومات إلى المحتال عن الفعاليات الرياضية الكبرى"، حيث إن القيام بتأمين أنظمة الأمن السيبراني في مواجهة البرامج الضارة يسهم في التصدي للعمليات الاحتيالية التي تتعرض لها الفعاليات الرياضية الكبرى (Libber, 2021)، كما يتضح من خلال الجدول (15) كذلك أن الفقرة الرابعة قد حصلت على أدنى درجة بمتوسط حسابي (.653)، وأهمية نسبية (٥١.٤%)،حيث نصت الفقرة على " يتم تأمين أنظمة الأمن السيبراني ضد إدعاء جهة معينة بأنها جهة موثوق بها من قبل مستخدم تابع للفعاليات الرياضية الكبرى تطلب منه إستخدام ملف مرفق يكون ضاراً به " ورغم أن هذه الدرجة ما تزال مرتفعة أيضاً إلا أن الباحثة تعزو هذه النتيجة إلى

أن المؤسسات الرياضية في الواقع لن تتعامل إلا مع جهات تجد أنها موثوق بها، وتم التعامل معها مسبقاً في فعاليات أخرى قد لا تكون كبيرة، ولكن تعاملها السابق معها قد وفر لها ثقة في التعامل معها مرة أخرى في فعاليات كبرى. وفي هذا الجانب أيضاً يؤكد جمال الدين (٢٠٢٣) على ضرورة عدم الركض وراء أية إدعاءات بموثوقية التعاملات خصوصاً مع قرب موعد تنفيذ الفعاليات، حيث أن الكثير منها قد يكون ضار بأمن وسلامة المعلومات ذات الصلة بالفاعليات الرياضية الكبرى.

الاستنتاجات:

بعد عرض النتائج ومناقشتها في ضوء مجموعة من الأسئلة التي تحقق أهداف الدراسة يمكن استنتاج ما يلي:

١. يتم استخدام أنظمة الأمن السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين بمستوى مرتفع من الفعالية.
٢. لتحقيق استخدام أكثر فاعلية لأنظمة السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى توجد مجموعة متنوعة من المتطلبات منها متطلبات بشرية ومتطلبات إدارية ومتطلبات تقنية ومتطلبات مادية.
٣. تعتمد الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية على العنصر البشري في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين بشكل كبير، كنتيجة للثقة الكبيرة في هذا العنصر البشري، وفي قدرته على إدارة المخاطر السيبرانية التي تواجه الفعاليات الرياضية الكبرى في مملكة البحرين.
٤. توجد مجموعة من المتطلبات الإدارية التي يتم تحقيقها بشكل فعال في سبيل الحصول على أعلى مستوى من تأمين الفعاليات الرياضية.
٥. تعتبر المكونات التقنية هي الركن الرئيسي في تحقيق فاعلية المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى على مجابهة مخاطر الأمن السيبراني.
٦. تلعب أنظمة السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى دوراً ايجابياً وفاعلاً في تأمين الفعاليات الرياضية الكبرى في الأندية والاتحادات والشركات المنظمة للفعاليات الرياضية.

التوصيات:

بناءاً على النتائج التي أظهرتها الدراسة، توصي الباحثة بالتالي:

١. العمل على تحديث أنظمة وبرامج الحاسب الآلي بالمؤسسة بشكل دوري لتجنب المخاطر التي تتصل البرامج الخبيثة التي يمكنها أن تهاجم الفعاليات الرياضية الكبرى في مملكة البحرين.

٢. ضرورة توفير أنظمة حماية للمعلومات السرية للمستخدم لأنظمة المعلومات الإدارية بالمؤسسات المنظمة والمشرفة على الفعاليات الرياضية الكبرى في مملكة البحرين.
٣. العمل على تطبيق متطلبات الأمن السيبراني لحماية أنظمة المعلومات الإدارية ومعالجة أجهزة المعلومات بالمؤسسة.
٤. التأكيد على ضرورة طباعة الوثائق ذات الصلة بالفاعليات الدولية على طابعات خاصة بالمؤسسة لضمان عدم تسرب هذه المعلومات.
٥. تنفيذ دراسات مستقبلية تعزز المتاحة حالياً حول تأثير تأمين الفعاليات الرياضية الكبرى من خلال الأمن السيبراني.

قائمة المراجع

المراجع العربية

١. اسماعيل زروقة. (٢٠١٩). الفضاء السيبراني والتحول في مفاهيم القوة والصراع، مجلة العلوم القانونية والسياسية.

٢. أمينة بن زرارة؛ و فطيمة أعراب. (٢٠٢٣). الحلول الرقمية الابتكارية في مجال حماية الهوية والخصوصية والأمن السيبراني خلال جائحة كوفيد-١٩. مجلة رقمنة للدراسات الإعلامية والاتصالية، (١) ٣.

٣. جنيفر إليوت ونايجل جنكينسون. (٢٠٢٠). المخاطر السيبرانية: التهديد الجديد للاستقرار المالي، منشورات صندوق النقد الدولي، ٢٠٢٠.

٤. حسام سامر عبده .(٢٠١٠). الإدارة الرياضية الحديثة ، ط١ ، عمان ، دار اسامة للتوزيع والنشر.

٥. خليفة الخاطر. (٢٠٢١). الأمن السيبراني، دراسة ماجستير، الكلية الملكية للقيادة والأركان والدفاع الوطني، الدورة ١٣، مملكة البحرين.

٦. سلام حنتوش وعلي عبد العظيم الإدارة الرياضية بين النظرية والتطبيق لطلبة التربية الرياضية، ط١ ، عمان ، دار دجلة للنشر والتوزيع، ٢٠١٦ .

٧. سلمان عكاب الجنابي و علي حسين الحسيناوي .(٢٠١٤). الادارة والتنظيم في التربية الرياضية ، ط١، عمان ، مكتبة المجتمع العربي للنشر والتوزيع.

٨. كمال درويش؛ وليد الصغير؛ أحمد حمد؛ ومحمد مغاوري .(٢٠١٣). اقتصاديات الرياضة، مصر: مكتبة الأنجلو المصرية.

٩. مالك الغبيوي. (٢٠٢٠). الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية.

١٠. نوران شفيق. (٢٠١٨). أثر التهديدات الإلكترونية على العلاقات الدولية دراسة في أبعاد الأمن الإلكتروني، سلسلة السياسة الدولية والاستراتيجية.

١١. هبه جمال الدين. (٢٠٢٣) الأمن السيبراني والتحول في النظام الدولي. مجلة كلية الاقتصاد والعلوم السياسية، (١) ٢٤.

المراجع الأجنبية

1. Andree, J. (2022). Sport Mega-Events, Security and COVID-19: Securing the Football World. Critical research in Gootball, 1-66.
2. Ohata, T. (2018). Cyber Security Solutions for Major International Events. Fujisti Scientific & technical journals , 57-65.
3. Libber. M. (2021) Safety and Security of Sporting Events in the Modern Era. Sports Desitination management Journal (6) 5.pp86-94

ملخص البحث

الأمن السيبراني ودوره في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين

د. منار عبدالله محمد حسن

ناقشت الباحثة من خلال هذه الدراسة واقع ممارسات الأمن السيبراني ودوره في تأمين الفعاليات الرياضية الكبرى في مملكة البحرين، حيث طبقت المنهج المسحي، وتم إعداد الاستبانة كأداة لجمع البيانات الأولية من مجتمع العاملين الذي شمل الإداريين في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين ، شملت العينة (١٨٥) من المشاركين، منها (٣٠) مشارك كعينة استطلاعية و (١٥٥) مشارك كعينة أساسية، من خلال التحليل الاحصائي لبيانات الدراسة عبر استخدام برنامج (SPSS)، توصلت الباحثة إلى أنه يتم استخدام أنظمة الأمن السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى في مملكة البحرين بمستوى مرتفع، ذلك من خلال مجموعة متنوعة من الإمكانات بشرية والإدارية والتقنية، وتلعب أنظمة السيبراني في المؤسسات الرياضية والشركات المنظمة للفعاليات الرياضية الكبرى دوراً ايجابياً وفاعلاً في تأمين الفعاليات الرياضية الكبرى في تلك المؤسسات، وأوصت الباحثة بالعمل على تحديث أنظمة وبرامج الحاسب الآلي بالمؤسسات بشكل دوري لتجنب المخاطر التي تتصل بالبرامج الخبيثة التي يمكنها أن تهاجم الفعاليات الرياضية الكبرى خلال تنفيذها، واوصت بضرورة توفير أنظمة حماية للمعلومات السرية للمستخدم لأنظمة المعلومات الإدارية بالمؤسسات المنظمة والمشرفة على الفعاليات الرياضية الكبرى في مملكة البحرين.

الكلمات المفتاحية: الأمن السيبراني– الفعاليات الرياضية الكبرى– حماية المعلومات

Abstract

Cybersecurity and its Role in securing Major Sporting Events in the Kingdom of Bahrain

Dr. Manar Abdulla Mohamed

Through this study, the researcher discussed the status of cybersecurity practices and its role in securing major sporting events in the Kingdom of Bahrain. The study applied the descriptive and quantitative approach. A questionnaire was designed as a tool for collecting primary data from the study sample that included administrators in sports institutions and companies organizing sporting events in the Kingdom of Bahrain. The research sample was made up of (185) of the participants, including (30) participants as an pilot sample and (155) participants as a basic sample. Through the data analysis, the study concluded that cybersecurity systems are used in sports institutions and companies organizing major sporting events in the Kingdom of Bahrain with a high level of effectiveness. Cybersecurity contributes to achieve a highly effective role in organizing major sporting events. Also, there are various portential, including human portential, administrative portential, technical portential. Cybersecurity systems play a positive role in sports institutions and companies organizing major sporting events played a to secure major sporting events in clubs. The study recommended that the institution's computer systems and programs have to be updated periodically to avoid the risks related to malicious programs that could attack major sporting events during implementation. It also, recommended the need to provide protection systems for the user's confidential information for the administrative information systems of the institutions organizing and supervising the events. Major sports in the Kingdom of Bahrain.

key words: Cybersecurity - Major sporting events - Information protection