

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية مسح التعليم الجامعي: المملكة العربية السعودية إسم الطالبة: جنان حسين المحيسن

مشروع التخرج-2

كلية الإدارة-جامعة ميداوون

إشراف:

د. منى مصطفى العشري

عضو هيئة التدريس - كلية الإدارة - جامعة ميداوون

الفصل الدراسي الثاني- 2024



الشكر والتقدير

الحمد لله الذي وهبنا نعمة العقل والفكر، ومنّ علينا بنور العلم والمعرفة، والصلاة والسلام على أشرف المرسلين، سيدنا محمد وعلى آله وصحبه أجمعين.

أبدأ رسالتي بواجب الشكر لله تعالى، خالق الكون وخالق الإنسان، الذي علم الإنسان بالقلم ما لم يعلم، فهو سبحانه وتعالى المنان الذي لا ينقطع فضله، الملك القدوس السلام، مدبر الليالي والأيام، مصرف الشهور والأعوام، قدر الأمور فأجراها على أحسن نظام، ما شاء الله كان ومالم يشأ لم يكن، له الحمد والشكر على ما أنعم به على من فضله الخير الكثير والعلم الوفير، وأعانني على إنجاز هذا العمل الذي احتسبه عبادة من العبادات جعلها الله خالصة لوجهه الكريم.

أتقدم بخالص الشكر وعظيم الامتنان للدكتورة منى مصطفى العشري، أستاذة البحث، على ما قدمته لي من علم نافع وعطاء متميز وإرشاد مستمر، وعلى ما بذلته من جهد متواصل ونصح وتوجيه من بداية مرحلة البحث حتى إتمام هذه العمل.

مهما كتبت من عبارات وجمل فإن كلمات الشكر تظل عاجزة عن إيفاء حقها، فجزاها الله عني خير الجزاء وجعل ذلك في موازين حسناتها.

أرفع أسمى عبارات الشكر والتقدير إلى والديّ العزيزين اللذين غرسا فيّ حب العلم من الصغر، وقدا لي كل غالي ونفيس، وكان لهما الفضل بعد الله فيما وصلت إليه الآن. فلا أملك إلا الدعاء لهما بطول العمر وحسن العمل وبلوغ الجنان.

أشكر معالي مدير جامعة ميدا وشن وإلى جميع هيئة التدريس بجامعة ميدا وشن على ما قدموه لي من دعم وتشجيع خلال مسيرتي الدراسية.

أشكر كل من مد لي يد العون، أو أسدى لي معروفاً أو قدم لي نصيحة، أو كانت له إسهامه صغيرة أو كبيرة في إنجاز هذا العمل. فله مني خالص الشكر والتقدير.

أختم رسالتي بالحمد لله رب العالمين أولاً وآخراً، ظاهراً وباطناً، عدد خلقه ورضا نفسه وزنة عرشه ومداد كلماته، والصلاة والسلام على نبينا محمد وعلى آله وصحبه أجمعين.

اهداء

من قال "أنتى لها" نالها

لم تكن الرحلة قصيرة، بل ولم يكن من المفترض أن تكون كذلك. لم يكن الحلم قريباً، ولم يكن الطريق ممهداً بالورود، لكنني فعلتها

الحمد لله حباً وشكراً وامتناناً، بفضلها ها أنا اليوم أنظر إلى حلم طال انتظاره، وقد أصبح واقعاً أفخر به.

إلى ملاكي الطاهر، وقوتي بعد الله، داعمتي الأولى والأبدية (أمي)، أهديك هذا الإنجاز الذي لولا تضحياتك لما كان له وجود. ممتنة لأن الله اصطفاك لي من بين البشر، فأنت خير سندٍ وعوض.

إلى من دعمني بلا حدود وأعطاني بلا مقابل (أبي العزيز)، شكراً لك على إيمانك بي ودعمك لي في كل خطوة على طريق الحياة.

إلى من قال فيهم {سَنَشُدُّ عَضُدَكَ بِأَخِيكَ} إخواني، أدامكم الله ضلعاً ثباتاً لي، شكراً لكم على وجودكم في حياتي، وعلى كل ما تقدمونه لي من حبٍ ودعمٍ.

إلى (أخواتي العزيزات)، أنتم سندي في الشدائد، ورفيقاتي في كل لحظات الحياة. شكراً لكم على حبكم ودعمكم لي

إلى من آمنت بقدراتي (رفيقة دربي)، شكراً لك على إيمانك بي، ودعمك لي في كل وقتٍ وحينٍ.

أهديكم جميعاً هذا الإنجاز، ثمرة جهودي

والله ولي التوفيق.

شكر وتقدير

مستخلص

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية ضروري لضمان سلامة وحماية البيانات والأنظمة في البيئة الجامعية في المملكة العربية السعودية. تعتبر المؤسسات التعليمية هدفاً محتملاً للهجمات السيبرانية نظراً للكمية الكبيرة من المعلومات الحساسة المخزنة فيها وتأثير هذه الهجمات على العملية التعليمية.

تتضمن خطوات تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية تحديد الأصول الحاسوبية وتصنيفها وتقييم الثغرات والتهديدات المحتملة وتحديد مدى تأثيرها واحتمالية حدوثها. ينبغي للمؤسسات التعليمية تنفيذ سياسات وإجراءات أمنية قوية مثل إدارة هوية المستخدمين وحماية البيانات وتشفيرها وتحديث البرامج، والأنظمة بانتظام، وتوفير التدريب، والتوعية.

تحليل مخاطر الأمن السيبراني يساعد المؤسسات التعليمية في تعزيز أمان البيئة التعليمية وحماية البيانات الحساسة للطلاب وأعضاء هيئة التدريس. يساعد أيضاً في الحد من تأثير الاختراقات السيبرانية مثل تسريب البيانات الشخصية والتجسس الصناعي وتلاعب النتائج الأكاديمية.

باختصار، تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية في المملكة العربية السعودية يعتبر جزءاً هاماً من استراتيجية حماية المعلومات والأنظمة. من خلال تحليل المخاطر وتنفيذ التدابير الأمنية الملائمة، يمكن للمؤسسات التعليمية تعزيز أمان البيئة الجامعية وضمان الحفاظ على خصوصية وسلامة المعلومات في سياق التعليم الجامعي في المملكة العربية السعودية.

Summar

Cybersecurity risk analysis in educational institutions aims to identify and assess potential opportunities to penetrate cybersecurity systems and infrastructure in educational institutions and assess the potential impacts of such breaches on the educational process and the sensitive information stored therein. In this context, we will take a look at the state of university .education in Saudi Arabia

Educational institutions in Saudi Arabia are a . potential target of cyberattacks due to the vast amount of sensitive information stored in their systems, including students' personal information, faculty, research data and other information sources. Hacking this information can leak personal, financial, industrial espionage, manipulate academic results and disrupt .educational services

Educational institutions in Saudi Arabia must . implement cybersecurity risk analysis to identify potential security gaps and assess their potential impact. The analysis typically includes many steps such as identifying and classifying computer assets, assessing potential gaps, assessing threats, their likelihood of occurrence and impact, determining the current level of protection and identifying appropriate .risk mitigation actions

After risk analysis, educational institutions must . apply appropriate security measures to protect their systems, and the information stored therein. Strong user identity management policies and procedures should be implemented, data protection rules and policies developed and encrypted, software and systems regularly updated, training and awareness

provided to students and faculty members to identify .cyber threats and take appropriate prevention action

In short, cybersecurity risk analysis in educational . institutions plays an important role in protecting sensitive information and cybersecurity infrastructure in university education in Saudi Arabia through risk analysis and implementation of appropriate security procedures. Educational institutions can enhance the security of the digital education environment and maintain the privacy and integrity of information for .students and faculty.

المحتويات

2.....	الشكر والتقدير
3.....	الاهداء
4.....	مستخلص

الفصل الأول:

٧.....	المقدمة
٩.....	مشكلة البحث
١٠.....	أهمية البحث
١١.....	أسئلة البحث
١٢.....	اهداف البحث
1٣.....	فرضيات البحث
1٤.....	نموذج البحث
1٥.....	منهجية البحث
1٦.....	الدراسة الميدانية
1٨.....	هيكل المشروع

(الأول) الإطار النظري

- 1٩..... • الامن السيبراني
- ٢٠..... • تدابير الامن السيبراني
- ٢٣..... • أهمية الامن السيبراني في المؤسسات التعليمية

(الثاني) مسح التعليم الجامعي في المملكة العربية السعودية

- 2٤..... • نظرة عامة على التعليم الجامعي في المملكة العربية السعودية
- 2٥..... • التدابير الامن السيبراني الجامعات السعودية
- 2٦..... • التحديات التي تواجه الجامعات السعودية
- ٢٩..... • التفاصيل الإضافية حول امن السيبراني في الجامعات السعودية

(الثالث) تحليل البيانات

- ٣١..... • تحليل المقابلات مع خبراء الامن السيبراني
- ٣٢..... • تفسير نتائج التحليل
- ٣٣..... • أدوات تحليل المحتوى

- ٣٤..... • الخاتمة

الفصل الثاني:

الدراسات السابقة 3٥

الفصل الثالث: منهجية البحث

- ٣,١. المقدمة ٣٦
- ٣,٢. التعريف الإجرائي للامن السيبراني ٣٦
- ٣.٢.١. مخاطر الامن السيبراني (المتغير المستقل) ٣٦
- ٣.٢.٢. تدابير الوقاية للامن السيبراني (المتغير التابع) ٣٦
- مجتمع البحث وطرق أو تقنيات أخذ العينة
 - ٣.٤.١. مجتمع البحث ٣٧
 - ٣.٤.٣. عينة البحث ٣٧
 - ٣.٤.٣. طريقة وتقنيات أخذ العينة ٣٧
- طرق جمع البيانات
 - ٣.٥. المتغير المستقل (مخاطر الامن السيبراني) ٣٨
 - ٣.٥.٢. المتغير التابع (تدابير الامن السيبراني) ٣٨
- أنواع البيانات
 - تحليل البيانات الأولية ٣٩
 - تحليل البيانات الثانوية ٣٩
- طرق وإجراءات تحليل البيانات ٤٠
- الخاتمة ٤١

الفصل الرابع: التحليل الاحصائي ومناقشة النتائج

- ٤.١. المقدمة ٤٢
- ٤.٢. خصائص عينة الدراسة ٤٣
- ٤.٣.١. صدق والمقاييس المستخدمة في الدراسة ٤٨
- ٣.٢. ثبات أداة الدراسة ٥١
- التحليل الوصفي لمتغيرات الدراسة ٥٢
- معاملات الارتباط الخطي بين متغيرات الدراسة ٥٤
- نتائج اختبار فروض الدراسة ٥٥
- المناقشة ٥٦
- الخاتمة ٥٧

الفصل الخامس: المناقشة النتائج والاستنتاجات

- المقدمة ٥٨
- اهم النتائج التي توصل اليها البحث ٥٩
- توصيات لتحسين الامن السيبراني في الجامعات السعودية ٦٠
- حدود الدراسة ٦١
- الدراسات المستقبلية ٦٢
- الخاتمة ٦٣

٦٤	 الملخص
٦٧	 المراجع
٦٩	 الملاحق

قائمة الاشكال:

- الشكل 1 نموذج البحث من تصميم الباحثه.....1
- الشكل 2 بصلة البحث من تصميم الباحثه..... ١٠
- الشكل 3 هيكل البحث من اعداد الباحثه.....1٨
- ٢/١ جدول مجتمع العينة من إعداد الباحثه..... ٣٧
- ٢/٢ جدول عينة البحث من إعداد الباحثه..... ٣٧
- ٢/٣ جدول المتغير المستقل (مخاطر الامن السيبراني) من إعداد الباحثه..... ٣٨
- ٢/٤ جدول المتغير التابع (تدابير الامن السيبراني) من إعداد الباحثه..... ٣٨
- ٢/٥ جدول بيانات المستخلص للنتائج من أعداد الباحثه..... ٤٣
- ٢/٦ جدول صدق الاتساق الداخلي والتقاربي لمقاييس متغيرات الدراسة
من أعداد الباحثه..... ٤٨
- ٢/٧ جدول قياس الثبات لأداة الدراسة من أعداد الباحثه..... ٥١
- ٢/٨ جدول قياس استجابات أفراد العينة من أعداد الباحثه..... ٥٢
- ٢/٩ جدول دلالة المتوسطات الحسابية من إعداد الباحثه..... ٥٢
- ٢/١٠ المتوسطات الحسابية والانحرافات المعيارية لمتغيرات
الدراسة من إعداد الباحثه..... ٥٣
- ٢/١١ معاملات الارتباط بين متغيرات الدراسة من إعداد الباحثه..... ٥٤

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية

المقدمة:

العالم الرقمي:

يشهد العالم اليوم ثورة رقمية هائلة، حيث أصبحت تقنيات المعلومات والاتصالات جزءاً لا يتجزأ من جميع جوانب الحياة، بما في ذلك التعليم. ونتيجة لذلك، أصبحت المؤسسات التعليمية عرضة لمخاطر الأمن السيبراني بشكل متزايد.

مخاطر متزايدة:

تشمل مخاطر الأمن السيبراني التي تواجهها المؤسسات التعليمية ما يلي:

- **الاختراقات الإلكترونية:** يمكن للقراصنة اختراق أنظمة المؤسسات التعليمية وسرقة البيانات الحساسة، مثل معلومات الطلاب والموظفين.
- **البرامج الضارة:** يمكن لنشر البرامج الضارة على أجهزة الكمبيوتر التابعة للمؤسسات التعليمية أن يؤدي إلى تلف البيانات أو تعطيل الخدمات.
- **هجمات الحرمان من الخدمة:** يمكن استخدام هجمات الحرمان من الخدمة لتعطيل مواقع المؤسسات التعليمية على الإنترنت مما يمنع الطلاب والموظفين من الوصول إلى المعلومات والخدمات.
- **التنمر الإلكتروني:** يمكن استخدام الإنترنت لتنمر الطلاب على بعضهم البعض، مما قد يؤدي إلى مشاكل نفسية واجتماعية.

تأثيرات واسعة:

لا تقتصر مخاطر الأمن السيبراني على المؤسسات التعليمية فقط، بل يمكن أن تؤثر أيضاً على:

- **الطلاب:** قد تسرق بياناتهم الشخصية أو تُستخدم لارتكاب جرائم.
- **الموظفون:** قد تسرق بياناتهم الشخصية أو تستخدم لابتزازهم.
- **المؤسسات التعليمية:** قد تلحق الضرر بسمعتها أو تُجبر على دفع غرامات كبيرة.

حاجة ملحة للحلول:

في ظل هذه التحديات، هناك حاجة ملحة لتطوير حلول فعالة لضمان الأمن السيبراني في المؤسسات التعليمية تتضمن بعض الحلول:

- **رفع مستوى الوعي:** نشر الوعي بمخاطر الأمن السيبراني بين الطلاب والموظفين.
 - **تطوير البنية التحتية:** الاستثمار في تطوير البنية التحتية لتقنية المعلومات والاتصالات لجعلها أكثر أمانًا.
 - **تطبيق تدابير الأمن السيبراني:** تطبيق تدابير الأمن السيبراني الفعالة، مثل جدران الحماية وبرامج مكافحة الفيروسات.
 - **التعاون مع الجهات الخارجية:** التعاون مع الجهات الخارجية مثل الشركات الخاصة والحكومة، لتحسين الأمن السيبراني.
- المسؤولية المشتركة:**

يقع ضمان الأمن السيبراني في المؤسسات التعليمية على عاتق جميع الأطراف المعنية، بما في ذلك:

- **الطلاب:** يجب على الطلاب أن يكونوا على دراية بمخاطر الأمن السيبراني وأن يتخذوا خطوات لحماية أنفسهم.
- **الموظفون:** يجب على الموظفين اتباع ممارسات الأمن السيبراني الجيدة وحماية البيانات الحساسة.
- **المؤسسات التعليمية:** يجب على المؤسسات التعليمية الاستثمار في تطوير حلول الأمن السيبراني وتطبيقها بشكل فعال.

مستقبل التعليم:

يعتمد مستقبل التعليم على قدرة المؤسسات التعليمية على ضمان أمن أنظمتها وبياناتها من خلال العمل معاً، يمكن لجميع الأطراف المعنية خلق بيئة تعليمية آمنة وفعالة للجميع.

مشكلة البحث :

تعد مخاطر الأمن السيبراني من أهم التحديات التي تواجهها المؤسسات التعليمية في المملكة العربية السعودية تشمل هذه المخاطر:

- **الاختراقات الإلكترونية:**

يمكن للقراصنة اختراق أنظمة المؤسسات التعليمية وسرقة البيانات الحساسة، مثل معلومات الطلاب والموظفين.

- **البرامج الضارة:**

يمكن لنشر البرامج الضارة على أجهزة الكمبيوتر التابعة للمؤسسات التعليمية أن يؤدي إلى تلف البيانات أو تعطيل الخدمات.

- **هجمات الحرمان من الخدمة:**

يمكن استخدام هجمات الحرمان من الخدمة لتعطيل مواقع المؤسسات التعليمية على الإنترنت، مما يمنع الطلاب والموظفين من الوصول إلى المعلومات والخدمات.

- **التنمر الإلكتروني:**

يمكن استخدام الإنترنت لتنمر الطلاب على بعضهم البعض، مما قد يؤدي إلى مشاكل نفسية واجتماعية.

أهمية البحث:

- سيساعد هذا البحث في فهم مخاطر الأمن السيبراني التي تواجهها الجامعات السعودية بشكل أفضل.
- سيساعد هذا البحث في تحديد تدابير الأمن السيبراني التي يجب على الجامعات السعودية تطبيقها.
- سيساعد هذا البحث في التغلب على التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.
- سيساعد هذا البحث في تحسين الأمن السيبراني في الجامعات السعودية، مما سيحمي البيانات الحساسة للطلاب والموظفين.

أسئلة البحث:

- ما هي أهم مخاطر الأمن السيبراني التي تواجهها الجامعات السعودية؟
- ما هي تدابير الأمن السيبراني التي تتخذها الجامعات السعودية لحماية أنظمتها وبياناتها؟
- ما هي التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني؟
- ما هي أفضل الممارسات لتحسين الأمن السيبراني في الجامعات السعودية؟

اهداف البحث:

- لتحديد مخاطر الامن السيبراني التي يواجهها المؤسسات التعليمية بالمملكة العربية السعودية.
- لتحديد اهم التحديات التي يواجهها المؤسسات التعليمية في المملكة العربية السعودية.
- لاكتشاف الحلول التطويرية لضمان الامن السيبراني المؤسسات التعليمية في المملكة العربية السعودية.

فرضيات البحث:

1. . فرضيات رئيسية:

- الفرضية الأولى: تواجه الجامعات السعودية مخاطر عالية من الأمن السيبراني.
- الفرضية الثانية: لا تتخذ الجامعات السعودية تدابير كافية لحماية أنظمتها وبياناتها من مخاطر الأمن السيبراني.
- الفرضية الثالثة: هناك العديد من التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.

2. فرضيات فرعية:

- الفرضية الفرعية الأولى: أكثر مخاطر الأمن السيبراني شيوعاً التي تواجهها الجامعات السعودية هي الاختراقات الإلكترونية.
- الفرضية الفرعية الثانية: لا تمتلك الجامعات السعودية الموارد المالية أو البشرية الكافية لتطبيق تدابير الأمن السيبراني الفعالة.
- الفرضية الفرعية الثالثة: نقص الوعي بمخاطر الأمن السيبراني هو أحد أهم التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني.

نموذج البحث:

1. المتغيرات:

- المتغير المستقل: مخاطر الأمن السيبراني.
- المتغير التابع: تدابير الأمن السيبراني التي تتخذها الجامعات السعودية.
- المتغيرات المتداخلة الموارد المالية والبشرية الوعي بمخاطر الأمن السيبراني، البنية التحتية لتقنية المعلومات والاتصالات.

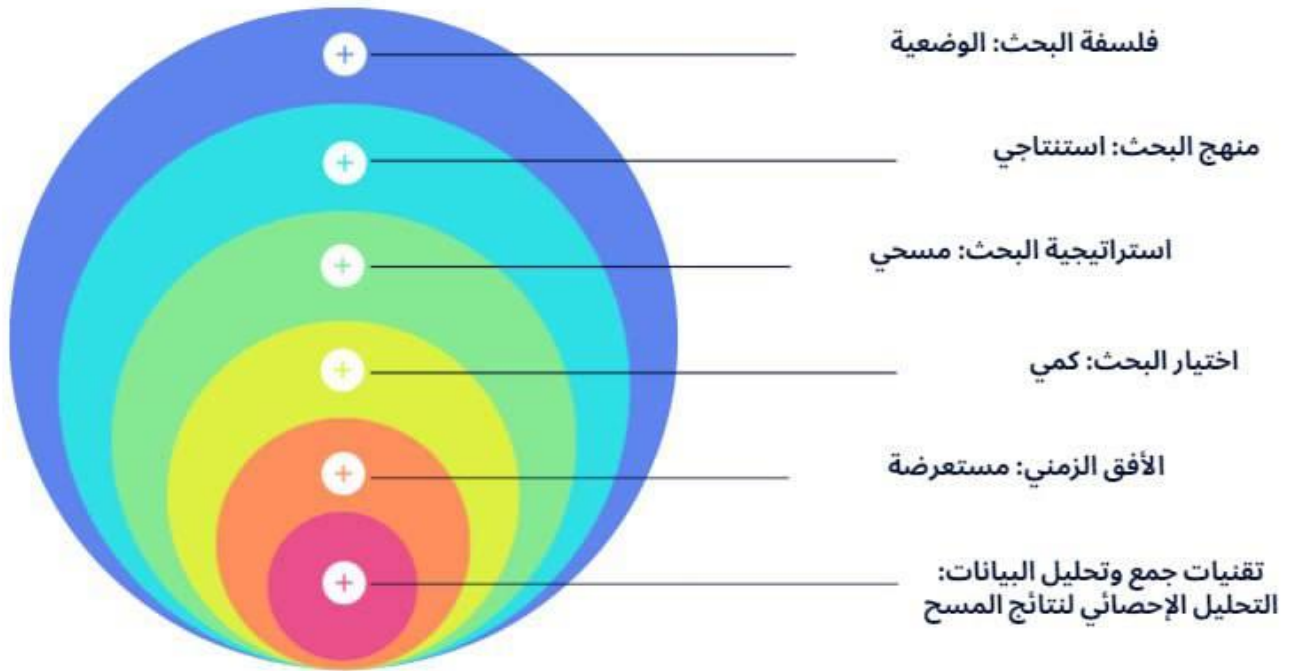
2. . العلاقات بين المتغيرات:

- العلاقة بين المتغير المستقل والمتغير التابع: تؤثر مخاطر الأمن السيبراني بشكل مباشر على تدابير الأمن السيبراني التي تتخذها الجامعات السعودية.
- العلاقة بين المتغيرات المتداخلة والمتغير التابع: تؤثر المتغيرات المتداخلة على قدرة الجامعات السعودية على تطبيق تدابير الأمن السيبراني.

منهجية البحث:

في هذي الدراسة، سيعتمد الباحث على منهجية البحث التحليلي الوصفي.

مخطط بصلة البحث



الدراسة الميدانية:

1. عنوان المشروع:

تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية دراسة حالة التعليم الجامعي في المملكة العربية السعودية

• مدة المشروع:

6 أشهر

2. خطوات المشروع:

أ. المرحلة التحضيرية:

- مراجعة الأدبيات ذات الصلة بمخاطر الأمن السيبراني في المؤسسات التعليمية.
- تحديد الجامعات السعودية التي سيتم دراستها.
- تصميم أدوات جمع البيانات.

ب. مرحلة جمع البيانات:

- إجراء مقابلات مع خبراء الأمن السيبراني في الجامعات السعودية.
- تحليل وثائق الجامعات السعودية المتعلقة بالأمن السيبراني.

ت. مرحلة تحليل البيانات:

- تحليل البيانات التي تم جمعها باستخدام التحليل الإحصائي.
- تفسير نتائج التحليل.

ث. مرحلة كتابة التقرير:

- كتابة تقرير نهائي يتضمن نتائج البحث وتوصياته.

3. المخاطر والتحديات:

- نقص التعاون من قبل الجامعات السعودية.
- صعوبة الحصول على البيانات.
- نقص الموارد المالية والبشرية.

4. خطة لإدارة المخاطر والتحديات:

- التواصل الفعال مع الجامعات السعودية.
- استخدام أدوات جمع البيانات المختلفة.
- البحث عن مصادر تمويل إضافية.

5. نتائج المشروع المتوقعة:

- فهم أفضل لمخاطر الأمن السيبراني التي تواجهها الجامعات السعودية.
- توصيات لتحسين الأمن السيبراني في الجامعات السعودية.

6. الفوائد المتوقعة من المشروع:

- تحسين الأمن السيبراني في الجامعات السعودية.
- حماية البيانات الحساسة للطلاب والموظفين.
- تعزيز الثقة في المؤسسات التعليمية.

7. خطة لنشر نتائج المشروع:

- نشر التقرير النهائي في مجلات علمية محكمة.
- تقديم نتائج البحث في مؤتمرات علمية.
- مشاركة نتائج البحث مع الجامعات السعودية والجهات الحكومية والقطاع الخاص.

هيكل المشروع:

الفصل الأول: الإطار العام للدراسة

الفصل الثاني: الإطار النظري

الفصل الثالث: منهجية البحث

الفصل الرابع: التحليل الإحصائي

الفصل الخامس: المناقشة والخاتمة

الأول

الأمن السيبراني:

الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية .
تهدف هذه الهجمات عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها.

أهدافه:

- حماية البيانات الحساسة.
- ضمان استمرارية الخدمات.
- حماية سمعة المؤسسة.

مخاطر الأمن السيبراني:

1. الهجمات الإلكترونية.

- الاختراقات الإلكترونية اختراق أنظمة المؤسسات وسرقة البيانات.
- البرامج الضارة: نشر برامج ضارة على أجهزة الحاسوب لإتلاف البيانات أو تعطيل الخدمات.
- هجمات الحرمان من الخدمة: تعطيل مواقع المؤسسات على الإنترنت.

2. الهجمات الاجتماعية:

- الاحتيال الإلكتروني: خداع الأشخاص للكشف عن معلوماتهم الشخصية أو المالية.
- التصيد الاحتيالي: إرسال رسائل بريد إلكتروني أو رسائل نصية تبدو وكأنها من مصدر موثوق به لخداع الأشخاص للكشف عن معلوماتهم الشخصية.
- الهندسة الاجتماعية: استخدام التلاعب النفسي لخداع الأشخاص للكشف عن معلوماتهم الشخصية أو اتخاذ إجراءات غير آمنة.

3. الداخلية:

- الأخطاء البشرية: الأخطاء التي قد يرتكبها الموظفون، مثل الكشف عن معلومات سرية عن طريق الخطأ أو استخدام كلمة مرور ضعيفة.
- السلوكيات الخبيثة: سلوكيات الموظفين الخبيثة، مثل سرقة البيانات أو تعطيل أنظمة المؤسسة.

تدابير الأمن السيبراني:

1. التدابير الوقائية:

- جدران الحماية: برامج تمنع الوصول غير المصرح به إلى أنظمة المؤسسة.
- برامج مكافحة الفيروسات: برامج تكتشف وتزيل البرامج الضارة.
- تحديثات البرامج: تحديث البرامج بانتظام لإصلاح الثغرات الأمنية.
- كلمات المرور القوية: استخدام كلمات مرور قوية يصعب تخمينها.
- التوعية بمخاطر الأمن السيبراني: توعية الموظفين بمخاطر الأمن السيبراني وكيفية حماية أنفسهم.

2. التدابير الرقابية:

- مراقبة الشبكة: مراقبة حركة الشبكة لاكتشاف الأنشطة المشبوهة.
- اختبار الاختراق: اختبار أنظمة المؤسسة بانتظام للعثور على الثغرات الأمنية.
- التحليل الجنائي الرقمي: التحقيق في الهجمات الإلكترونية لتحديد مصدرها وتأثيرها.

3. تدابير الاسترداد:

- النسخ الاحتياطي للبيانات: الاحتفاظ بنسخ احتياطية من البيانات المهمة في مكان آمن.
- خطط الاسترداد من الكوارث: خطط لإعادة تشغيل أنظمة المؤسسة في حالة وقوع هجوم إلكتروني.

- تحديد السياسات والإجراءات ينبغي للمؤسسات والمنظمات والأفراد وضع سياسات وإجراءات أمنية فعالة لحماية البيانات والأنظمة الإلكترونية. يشمل ذلك تحديد صلاحيات الوصول، وتنفيذ تحديثات الأمان، وإجراء نسخ احتياطية منتظمة، وتوفير التدريب والتوعية الأمنية للموظفين والمستخدمين.
- استخدام التشفير: ينبغي استخدام تقنيات التشفير لحماية البيانات الحساسة والاتصالات الإلكترونية. يمكن استخدام التشفير في الاتصالات عبر الإنترنت وتخزين البيانات وحماية الأجهزة المحمولة.
- تحديث وإدارة البرمجيات: يجب تحديث الأنظمة والبرمجيات بانتظام لتصحيح الثغرات الأمنية المعروفة وتحسين الأمان. ينبغي أيضًا إدارة البرمجيات بشكل فعال من خلال تثبيت التصحيحات وتقييد البرمجيات غير المصرح بها.
- رصد الأمان والاستجابة: يجب إنشاء نظام لرصد الأنشطة السيبرانية غير العادية واكتشاف التهديدات المحتملة. يتطلب ذلك استخدام أدوات رصد الأمان وتحليل السجلات وتطبيق إجراءات استجابة فورية لمواجهة الهجمات والتهديدات.
- التوعية والتدريب يجب توفير التدريب والتوعية الأمنية للموظفين والمستخدمين للتعرف على التهديدات السيبرانية وممارسات الأمان السليمة. يشمل ذلك التوعية حول البريد الإلكتروني المشبوه والرسائل الاحتيالية وتقنيات الهندسة الاجتماعية.
- الاحتفاظ بنسخ احتياطية: ينبغي إجراء نسخ احتياطية منتظمة للبيانات للحماية من فقدان البيانات أو تلفها نتيجة لهجمات أو أخطاء فنية.

- أمن الشبكات: يشير إلى حماية الشبكات المؤسسية والاتصالات بين الأجهزة. يشمل ذلك تأمين الجدران النارية والتأكد من أن الشبكات محمية بكلمات مرور قوية واستخدام تقنيات الكشف عن التسلل والتصدي للهجمات.
- أمن الأجهزة: يتعلق بحماية الأجهزة الإلكترونية مثل الحواسيب والهواتف المحمولة والأجهزة الذكية. يشمل ذلك تأمين الأجهزة بكلمات مرور وتشفير البيانات المخزنة عليها وتحديث البرامج والتطبيقات بانتظام.
- أمن البرمجيات: يتعلق بحماية البرمجيات من الثغرات الأمنية والبرامج الخبيثة. يشمل ذلك تحديث البرامج بصورة منتظمة لتصحيح الثغرات الأمنية المعروفة واستخدام برامج مكافحة الفيروسات والحماية من البرمجيات الخبيثة.
- أمن المعلومات: يتعلق بحماية البيانات والمعلومات الحساسة من الوصول غير المصرح به والاستخدام غير المشروع. يشمل ذلك تنفيذ سياسات الوصول والتحكم في الصلاحيات وتشفير البيانات واستخدام تقنيات الحماية المتقدمة مثل التوقيع الرقمي والتوثيق المزدوج.
- أمن السحابة يشمل حماية البيانات والتطبيقات والموارد المخزنة والمستضاف على السحابة. يتطلب تأمين السحابة استخدام تقنيات التشفير والتحقق من الهوية والتحكم في الوصول ومراقبة النشاطات غير العادية.
- الاستجابة للحوادث: يتعلق بالتصدي للحوادث الأمنية والتعامل معها بفعالية. يشمل ذلك إنشاء خطة استجابة للحوادث وتوفير فريق استجابة للتحقيق في الحوادث واستعادة النظام وتقييم الأضرار وتعزيز الأمان لتجنب تكرارها في المستقبل.
- التعاون والمشاركة: يعتبر التعاون بين الجهات المختلفة ومشاركة المعلومات الأمنية ذات أهمية كبيرة في مجال الأمن السيبراني. يشمل ذلك التعاون مع الحكومة والمؤسسات الأخرى والمشاركة في منصات ومبادرات.

أهمية الامن السيبراني في المؤسسات التعليمية

تحديث البرامج والتطبيقات بانتظام له أهمية كبيرة في مجال الأمان السيبراني وحماية الأنظمة والأجهزة الإلكترونية. إليك بعض الأسباب التي تبرز أهمية تحديث البرامج والتطبيقات بانتظام:

1. إغلاق الثغرات الأمنية: يتم اكتشاف ثغرات أمنية جديدة في البرامج والتطبيقات بشكل مستمر. عند تحديث البرامج بانتظام، يتم إصلاح وإغلاق هذه الثغرات، مما يعني أن النظام يكون أكثر صلابة وأماناً ضد الهجمات السيبرانية.
 2. التصدي للبرمجيات الخبيثة: يُستغل القرصنة الثغرات الأمنية في البرامج والتطبيقات لاختراق الأنظمة وتنفيذ برامج خبيثة. تحديث البرامج يساعد في منع دخول البرمجيات الخبيثة عن طريق تصحيح الثغرات وتحسين الأمان.
 3. تحسين الأداء والوظائف: يتم تحسين البرامج والتطبيقات من خلال التحديثات لتحسين الأداء وإضافة وظائف جديدة بالاستفادة من التحديثات، يمكنك الاستفادة من أحدث الميزات والتحسينات في البرنامج أو التطبيق، مما يعزز تجربتك وقدرتك على الاستخدام الفعال والأمن للأنظمة الرقمية.
 4. التوافق مع التغييرات الأخرى: قد يتطلب تحديث البرامج والتطبيقات توافقاً مع التغييرات الأخرى في النظام الأساسي أو المكونات الأخرى. من خلال التحديث المنتظم، يمكنك ضمان التوافق بين البرامج والتطبيقات والنظام العام، مما يقلل من مشاكل التوافق ويحافظ على استقرار النظام.
 5. الحصول على دعم فني وتحديثات الأمان: عندما تقوم بتحديث البرامج بانتظام، فإنك تستفيد من الدعم الفني المستمر من الشركة المطورة. يمكنك الحصول على دعم فني في حالة وجود أي مشاكل أو استفسارات، بالإضافة إلى تلقي تحديثات الأمان العاجلة التي تحمي النظام من التهديدات الجديدة.
- في النهاية، تحديث البرامج والتطبيقات بانتظام يعد إجراءً أساسياً للحفاظ على الأمان والحماية السيبرانية القوية. يوصى بتفعيل التحديثات التلقائية للبرامج والتطبيق يكون هناك تقطع في النص. كانت الجملة الأخيرة هي: "يوصى بتفعيل التحديثات التلقائية للبرامج والتطبيقات للحصول على أحدث التحديثات بشكل مستمر وبدون عناء يدوي."

الثاني

نظرة عامة على التعليم الجامعي في المملكة العربية السعودية:

- نظام التعليم الجامعي:

يتكون من 3 مراحل البكالوريوس والماجستير والدكتوراه.

يُشرف على التعليم الجامعي وزارة التعليم.

هناك جامعات حكومية وخاصة.

- عدد الجامعات:

34 جامعة حكومية.

11 جامعة خاصة.

- عدد الطلاب:

أكثر من 800 ألف طالب وطالبة.

- التخصصات:

تتوفر تخصصات متنوعة في مختلف المجالات، مثل العلوم والهندسة، والطب والإدارة والأعمال.

مخاطر الأمن السيبراني التي تواجه الجامعات السعودية:

- الهجمات الإلكترونية

اختراق أنظمة الجامعات وسرقة البيانات الحساسة، مثل معلومات الطلاب والموظفين.

نشر البرامج الضارة على أجهزة الحاسوب التابعة للجامعات.

تعطيل مواقع الجامعات على الإنترنت.

■ الهجمات الاجتماعية:

- الاحتيال الإلكتروني على الطلاب والموظفين.
- التصيد الاحتيالي لخداع الطلاب والموظفين للكشف عن معلوماتهم الشخصية.
- التلاعب بالطلاب والموظفين للحصول على معلومات سرية.

● المخاطر الداخلية:

- الأخطاء البشرية من قبل الطلاب والموظفين.
- السلوكيات الخبيثة من قبل بعض الطلاب والموظفين.

تدابير الأمن السيبراني التي تتخذها الجامعات السعودية:

● التدابير الوقائية:

- استخدام برامج مكافحة الفيروسات وجدران الحماية.
- تحديث البرامج بانتظام.
- توعية الطلاب والموظفين بمخاطر الأمن السيبراني.

● التدابير الرقابية:

- مراقبة حركة الشبكة.
- اختبار أنظمة الجامعة بانتظام.

● تدابير الاسترداد:

- الاحتفاظ بنسخ احتياطية من البيانات.
- خطط لإعادة تشغيل أنظمة الجامعة في حالة وقوع هجوم إلكتروني.

- **التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني:**

- **نقص الموارد المالية والبشرية:**

- لا تمتلك العديد من الجامعات الموارد المالية الكافية لتطبيق تدابير الأمن السيبراني الفعالة.
- لا يوجد لدى العديد من الجامعات عدد كاف من الموظفين المتخصصين في الأمن السيبراني.

- **نقص الوعي بمخاطر الأمن السيبراني:**

- لا يدرك العديد من الطلاب والموظفين مخاطر الأمن السيبراني وكيفية حماية أنفسهم.

- **التغيرات في التكنولوجيا:**

- تتطور التكنولوجيا بسرعة، مما يجعل من الصعب على الجامعات مواكبة التهديدات الجديدة.

نظرة عامة على التعليم الجامعي في المملكة العربية السعودية:

- يتمتع التعليم الجامعي في المملكة العربية السعودية بأهمية كبيرة ويعد من أولويات الحكومة السعودية. تسعى الحكومة إلى تعزيز جودة التعليم العالي وتطوير الجامعات والمؤسسات التعليمية، وذلك من خلال استثمارات كبيرة في البنية التحتية والبرامج الأكاديمية والبحث العلمي. تتوفر في المملكة العديد من الجامعات الحكومية والخاصة التي تقدم مجموعة واسعة من التخصصات والبرامج الأكاديمية.

- **مخاطر الأمن السيبراني التي تواجه الجامعات السعودية:**

- مثل العديد من الدول الأخرى، تواجه الجامعات السعودية تحديات في مجال الأمن السيبراني. بسبب الاعتماد المتزايد على التكنولوجيا والشبكات الإلكترونية في العمليات

الأكاديمية والإدارية، تكون الجامعات عرضة للتهديدات السيبرانية المحتملة. تشمل بعض المخاطر المحتملة التي تواجه الجامعات السعودية: اختراق الأنظمة الإلكترونية، سرقة المعلومات الحساسة، القرصنة، التجسس الإلكتروني، وتعطل الخدمات الإلكتروني.

تدابير الأمن السيبراني التي تتخذها الجامعات السعودية:

تتخذ الجامعات السعودية عدداً من التدابير لتعزيز الأمن السيبراني وحماية أنظمتها وبياناتها. تشمل هذه التدابير:

1. تطوير سياسات وإجراءات الأمن السيبراني: تقوم الجامعات بوضع سياسات وإجراءات واضحة لأمن السيبراني لتوجيه الموظفين والطلاب بشأن استخدام التكنولوجيا وتعاملهم مع المعلومات الحساسة.

2. التدريب والتوعية: تقدم الجامعات التدريب والتوعية المستمرة للموظفين والطلاب حول مخاطر الأمن السيبراني وكيفية التعامل معها، بما في ذلك تعلم كيفية التعرف على رسائل البريد الإلكتروني الاحتيالية والهجمات الإلكترونية الأخرى.

3. تحديث البرامج والأنظمة: يتم تحديث برامج الحماية وأنظمة الجامعات بشكل منتظم لمواجهة التهديدات السيبرانية الجديدة، وتثبيت التصحيحات التحديات التي تواجه الجامعات السعودية في تطبيق تدابير الأمن السيبراني: على الرغم من الجهود المبذولة، تواجه الجامعات السعودية تحديات في تنفيذ وتطبيق تدابير الأمن السيبراني.

التحديات التي تواجه الجامعات السعودية

1. **التكلفة:** تطبيق تدابير الأمن السيبراني يتطلب استثمارات مالية كبيرة في تكنولوجيا الحماية وتحديث الأنظمة وتدريب الموظفين. قد يكون من الصعب على الجامعات تخصيص الموارد المالية اللازمة لتلبية هذه التحديات.
2. **نقص المهارات:** قد يواجه الجامعات نقصاً في المهارات والخبرات المتخصصة في مجال الأمن السيبراني. قد يكون من الصعب توظيف وتدريب الكوادر اللازمة لتنفيذ وإدارة برامج الأمن السيبراني.
3. **التوافر المستمر:** تتطور تهديدات الأمن السيبراني باستمرار، وبالتالي يتطلب تطبيق تدابير الأمان السيبراني تحديثاً وتحسيناً مستمراً. يجب على الجامعات السعودية التكيف مع هذه التحديات وضمان توافر الإجراءات والتقنيات الحديثة لحماية الأنظمة والبيانات.
4. **التحديات القانونية والتنظيمية:** تواجه الجامعات تحديات في مجال الامتثال للقوانين واللوائح المتعلقة بالأمن السيبراني، بما في ذلك حماية البيانات الشخصية للطلاب والموظفين. يجب على الجامعات السعودية الالتزام بالتشريعات المحلية ذات الصلة وتوفير الإطار القانوني والتنظيمي اللازم لتعزيز الأمن السيبراني.

التفاصيل الإضافية حول الأمن السيبراني في الجامعات السعودية:

1. التعاون والشراكات: تعمل الجامعات السعودية على تعزيز التعاون والشراكات مع الجهات المعنية بالأمن السيبراني، بما في ذلك الجهات الحكومية والشركات الخاصة والمؤسسات الأكاديمية الأخرى. يتم تبادل المعلومات والخبرات والممارسات الجيدة لتعزيز قدرات الأمن السيبراني في القطاع التعليمي.

2. الفحص الأمني واختبار الاختراق: تقوم بعض الجامعات بإجراء فحوص أمنية دورية واختبارات اختراق لتحديد الثغرات والضعف في الأنظمة الإلكترونية. يتم استخدام هذه الاختبارات لتحسين أمان الأنظمة وإصلاح أي ثغرات مكتشفة.

3. الحوسبة السحابية الآمنة: تعتمد بعض الجامعات السعودية على الحوسبة السحابية لتخزين ومعالجة البيانات. يتم اتخاذ إجراءات أمان متقدمة لضمان حماية البيانات المخزنة في السحابة، مثل استخدام تقنيات التشفير وتطبيق سياسات الوصول المناسبة.

4. إدارة الهوية والوصول: يتم تنفيذ أنظمة إدارة الهوية والوصول في الجامعات للتحكم في الوصول إلى الأنظمة والموارد الحساسة. يتم تطبيق تقنيات مثل تحقق الهوية المتعددة العوامل وإعدادات الصالحيات المتقدمة للحفاظ على أمان البيانات والمعلومات.

5. رصد واستجابة الأمن: تقوم الجامعات بإنشاء فرق الاستجابة لأمن السبراني لرصد الأنشطة الاشتباه والتهديدات السبرانية والتعامل معها بشكل سريع وفعال. يتم استخدام أدوات رصد الأمن وتحليل السجلات والذكاء الاصطناعي لاكتشاف الأنشطة غير العادية والتهديدات الجديدة.

6. التوعية للمستخدمين: تعتبر التوعية الأمنية للموظفين والطالب عنصرًا مهمًا في الأمن السبراني. تقوم الجامعات بتوفير تدريب مستمر للمستخدمين حول ممارسات الأمان السبراني والوقاية من التهديدات، بما في ذلك التعرف على رسائل الاحتيال الإلكتروني ممكن أيضًا تقديم مزيد من المعلومات حول مواضيع أخرى إذا كنت ترغب في ذلك. فقط أخبرني بالموضوع الذي ترغب في معرفة المزيد عنه.

الثالث

• تحليل نتائج المقابلات مع خبراء الأمن السيبراني

1. جمع البيانات:

- ❖ إجراء مقابلات مع خبراء الأمن السيبراني من مختلف القطاعات (الحكومة، القطاع الخاص، الأكاديمية).
- ❖ تسجيل المقابلات وتحليلها.

• تحديد الموضوعات الرئيسية والنقاط الهامة التي تم طرحها من قبل الخبراء.

2. تحليل البيانات:

- ❖ تحليل محتوى المقابلات باستخدام تقنيات تحليل المحتوى مثل: تحليل التردد: تحديد عدد مرات تكرار الكلمات والعبارات.
- ❖ تحليل السياق: فهم معنى الكلمات والعبارات في سياق الجملة والفقرة.
- ❖ تحليل المشاعر: تحديد المشاعر والآراء التي تم التعبير عنها من قبل الخبراء.

3. تفسير النتائج:

- ❖ تفسير نتائج التحليل لتحديد الاتجاهات الرئيسية والتحديات والفرص في مجال الأمن السيبراني في المملكة العربية السعودية.
- ❖ صياغة النتائج في تقرير مكتوب أو عرض تقديمي.
- ❖ تفسير نتائج التحليل لتحديد نقاط القوة والضعف في برامج الأمن السيبراني في الجامعات السعودية.
- ❖ صياغة النتائج في تقرير مكتوب أو عرض تقديمي.

• تفسير نتائج التحليل:

1. دمج نتائج التحليلات:

- ❖ دمج نتائج تحليل المقابلات مع نتائج تحليل وثائق الجامعات.
- ❖ تحديد أوجه التشابه والاختلاف بين النتائج.

2. تفسير النتائج:

❖ تفسير النتائج لتحديد:

- الاتجاهات الرئيسية في مجال الأمن السيبراني في المملكة العربية السعودية.
- التحديات التي تواجه المملكة العربية السعودية في مجال الأمن السيبراني.
- الفرص المتاحة للمملكة العربية السعودية في مجال الأمن السيبراني.

3. صياغة النتائج:

- صياغة النتائج في تقرير مكتوب أو عرض تقديمي.
- تقديم توصيات لتحسين برامج الأمن السيبراني في المملكة العربية السعودية.

أدوات تحليل المحتوى:

- ❖ QDA MINER: أداة تحليل محتوى قوية تدعم العديد من تقنيات تحليل المحتوى مثل تحليل التردد وتحليل السياق وتحليل المشاعر.
- ❖ MAXQDA: أداة تحليل محتوى أخرى شائعة تدعم مجموعة واسعة من ميزات تحليل المحتوى، مثل تحليل النصوص والصور والصوت.
- ❖ NVIVO: أداة تحليل محتوى شائعة الاستخدام في العلوم الاجتماعية، وتدعم تحليل النصوص، والصور، والصوت والفيديو.
- ❖ ATLAS.TI: أداة تحليل محتوى قوية تدعم تحليل النصوص والصور والصوت والفيديو بالإضافة إلى تحليل الشبكات الاجتماعية.

خاتمة

في عصر التحول الرقمي الذي نعيشه، أصبح قطاع التعليم الجامعي أكثر عرضة من أي وقت مضى للتهديدات السيبرانية. فالاعتماد المتزايد على البنية التحتية التقنية والشبكات الإلكترونية في جميع الأنشطة التعليمية والبحثية والإدارية قد زاد من إمكانية تعرض الجامعات للاختراقات والهجمات الإلكترونية.

تتنوع مخاطر الأمن السيبراني في هذا القطاع وتشمل سرقة البيانات الشخصية والأكاديمية الحساسة الخاصة بالطلاب والموظفين، تعطيل أنظمة الجامعة وانقطاع الخدمات الإلكترونية، وحتى تسريب معلومات سرية ذات طبيعة بحثية أو إدارية. وقد أظهرت الدراسات وجود فجوة كبيرة في وعي وفهم القيادات التعليمية لهذه المخاطر وطرق التصدي لها.

لذلك، تبرز الحاجة الماسة لتعزيز ثقافة الأمن السيبراني في الجامعات من خلال جهود متكاملة على مستوى السياسات والإجراءات الأمنية، والتدريب المستمر للكوادر الأكاديمية والإدارية، وزيادة وعي جميع منسوبي الجامعات. فقط بهذا النهج الشامل يمكن للمؤسسات التعليمية التصدي بفعالية لمخاطر الأمن السيبراني وحماية أنشطتها وبياناتها الحيوية.

الفصل الثاني:

الدراسات السابقة

الفصل الثاني

الدراسات السابقة

- متطلبات تحقيق الأمن السيبراني في الجامعات السعودية في ضوء رؤية 2030" (2020) تحلل هذه الدراسة متطلبات تحقيق الأمن السيبراني في الجامعات السعودية من خلال تطبيق أداة بحث (الاستبانة على الموظفين التقنيين في ثلاث جامعات سعودية.
- درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة الرياض" (2020): تقيم هذه الدراسة مستوى وعي معلمات المرحلة المتوسطة بمخاطر الأمن السيبراني في المدارس العامة بمدينة الرياض.
- "استشارات إطار الامن السيبراني في التعليم العالي السعودي" (2019): تقدم هذه الدراسة إطاراً عاماً للأمن السيبراني في التعليم العالي السعودي، وتتناول مبادئ التصميم الأمني ومكونات أنظمة تقنية المعلومات والتهديدات السيبرانية، والسياسات، والتشريعات، والأخلاقيات.
- "الإجراءات المقترحة لإدارة المخاطر السيبرانية في المدارس الابتدائية بمصر" (2018) تناقش هذه الدراسة أهمية إدارة المخاطر السيبرانية في المدارس الابتدائية، وتقدم إجراءات مقترحة للتحكم في هذه المخاطر.

الفصل الثالث:

منهجية البحث

منهجية البحث

٣,١. المقدمة:

يوضح هذا الفصل منهجية البحث المستخدمة في التحقيق (تحليل مخاطر الأمن السيبراني بالتعليم الجامعي بالمملكة العربية السعودية).

التعريفات:

3,2. التعريف الاجرائي للأمن السيبراني: امن المعلومات على أجهزة وشبكات الحاسب الالى من أي تدخل غير مقصود او غير مصرح به او تغيير او اختلاف قد يحدث.

٣,٢,١. مخاطر الأمن السيبراني (المتغير المستقل تحديد مخاطر الأمن السيبراني للمنظمة وتقييمها واداراتها لحماية أصولها المعلوماتية والتقنية وفقا لسياسات وإجراءات المنظمة، وكذلك المتطلبات التنظيمية ذات العلاقة.

٣,٢,٢. تدابير الوقاية للأمن السيبراني (المتغير التابع): هي مجموعة الخطوات والإجراءات التي يتم اتخاذها لحماية الأنظمة والبيانات الرقمية من التهديدات السيبرانية تهدف هذي الاجرائيات إلى الكشف المكبر عن التهديدات السيبرانيو التصدي لها قبل الوقوع وتطبيق الضوابط الأمنية اللازمة.

مجتمع البحث وطرق أو تقنيات أخذ العينة

١,٤,٣. مجتمع البحث

جدول رقم (١) مجتمع البحث

القطاع	التصفيات	عدد الأشخاص
الجامعات السعودية	الطلاب والطالبات	٦٠

المصدر: الباحث (٢٠٢٤)

٣,٤,٢. عينة البحث

جدول رقم (٢) عينة البحث

عينة البحث	حجم العينة
استهداف الطلاب والطالبات بالجامعات السعودية	٤٠-٥٠ طالب وطالبة

المصدر: الباحث (٢٠٢٤)

٣,٤,٣. طريقة وتقنيات أخذ العينة:

عن طريق رابط استبيان (Google from) يتم توزيعه على مجموعة من الطلاب والطالبات.

طرق جمع البيانات

٣,٥. المتغير المستقل (مخاطر الأمن السيبراني)

جدول رقم (٣) المتغير المستقل

المتغير	الابعاد	الأبعاد البيانات
مخاطر الأمن السيبراني	مخاطر الأمن السيبراني	٦

بواسطة الباحث (٢٠٢٤)

٣,٥,٢. المتغير التابع (تدابير الوقاية للأمن السيبراني)

جدول رقم (٤) المتغير التابع

المتغير	الابعاد	عدد البيانات
تدابير الوقاية للأمن السيبراني	تدابير الوقاية التي تتخذها الجامعات السعودية للأمن السيبراني	٦

بواسطة الباحث: (٢٠٢٤)

أنواع البيانات

بناءً على البيانات الأولية والثانوية المقدمة، يمكنني تقديم التحليل والاستنتاجات التالية:

تحليل البيانات الأولية:

- تعد الاستبيان أداة مناسبة لجمع البيانات الأولية في هذه الدراسة، حيث يمكن من خلالها الحصول على معلومات شاملة عن موضوع البحث من المشاركين المستهدفين.
- معدل الاستجابة المرتفع يشير إلى اهتمام المشاركين بالموضوع وتعاونهم في تقديم البيانات المطلوبة للدراسة.
- التحليل الكمي المتقدم للبيانات الأولية باستخدام البرامج الإحصائية يُمكن من استخراج المؤشرات والمقاييس الإحصائية الهامة لاستنباط النتائج والاستنتاجات.

تحليل البيانات الثانوية:

- المراجعة الشاملة للدراسات السابقة ذات الصلة تساعد في بناء إطار نظري قوي يدعم الدراسة الميدانية وربط النتائج بالأدبيات السابقة.
- الاطلاع على المعلومات والبيانات المتاحة عبر المواقع الإلكترونية للأمن السيبراني في التعليم الجامعي يمكن من فهم السياق التنظيمي والتشغيلي للموضوع قيد البحث.
- التحليل والتفسير المنهجي للبيانات الثانوية يُساهم في تطوير رؤية شاملة وعميقة للموضوع والربط بين مختلف جوانبه.

طرق وإجراءات تحليل البيانات

بعد جمع البيانات من الضروري تحليل المعلومات التي تم جمعها لاستخلاص استنتاجات ذات معنى. كما تم استخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS) وتحديداً الإصدار ٢٨ لتحليل البيانات المجمعة.

تم إجراء اختبار توصيف العينة، من خلال التحليل الوصفي، للحصول على نظرة ثاقبة الخصائص مجتمع العينة. يساعد الباحثين على فهم التركيبة السكانية والتفضيلات والمعلومات الأخرى ذات الصلة بالأفراد المشاركين في الدراسة.

تعتبر اختبارات الصلاحية والموثوقية حاسمة في ضمان دقة البيانات المجمعة واتساقها.

اختبارات الصدق التحليلي العاملي (الاستكشافي) لتحديد ما إذا كانت أدوات البحث تقيس ما تهدف إلى قياسه، بينما تقوم اختبارات الثبات اختبار كرونباخ ألفا بتقييم ثبات النتائج مع مرور الوقت. تم إجراء اختبار توصيف العينة، من خلال التحليل الوصفي، للحصول على نظرة ثاقبة لخصائص مجتمع العينة.

يساعد الباحثين على فهم التركيبة السكانية والتفضيلات والمعلومات الأخرى ذات الصلة بالأفراد المشاركين في الدراسة.

الخاتمة

في هذا البحث، تم استكشاف منهجية شاملة لتحديد وتقييم مخاطر الأمن السيبراني في بيئة التعليم الجامعي من خلال اتباع نهج متعدد المراحل، تم تسليط الضوء على الجوانب الرئيسية المخاطر الأمن السيبراني المحتملة والتحديات التي تواجهها الجامعات في هذا السياق.

أولاً، تم إجراء مراجعة شاملة للأدبيات المتعلقة بأمن المعلومات في التعليم العالي لفهم الاتجاهات والممارسات الحالية. ثم تم استخدام إطار عمل تقييم المخاطر لتحديد المخاطر الرئيسية والتهديدات المحتملة التي تواجه البنية التحتية التقنية والموارد البشرية في الجامعات.

بالإضافة إلى ذلك، تم إجراء دراسة استقصائية لاستكشاف وجهات نظر أصحاب المصلحة الرئيسيين حول هذه المخاطر وأولوياتهم في إدارتها. وقد كشفت النتائج عن مجموعة متنوعة من التحديات والقضايا التي تواجهها الجامعات، بما في ذلك الوعي والتدريب غير الكافيين للموظفين، والاعتماد المتزايد على التقنيات الرقمية، وضعف الاستعداد للتصدي للهجمات السيبرانية.

في الختام، نتمنى ان يستفيد القارئون على التعليم الجامعي من نتائج هذا البحث المقدمة لتعزيز الأمن السيبراني في مؤسساتهم التعليمية.

الفصل الرابع:

التحليل الإحصائي

ومناقشة النتائج

الفصل الرابع

٤,١. المقدمة

يتناول هذا الفصل عرضاً لنتائج الدراسة الميدانية التي تم تحليلها إحصائياً باستخدام البرامج الإحصائية SPSS الإصدار ٢٨ الفصل الحالي للتحليل الإحصائي يتضمن الإحصاء الوصفي للعينة محل الدراسة باستخدام SPSS الإصدار ٢٨ اختبار صدق وثبات الاستبانة المستخدمة في جمع البيانات المطلوبة من عينة الدراسة الحالية، من أجل اختيار فرضيات البحث ومدى ملاءمة النموذج، إجراء تحليل الانحدار الخطي البسيط عبر SPSS ٢٨.

٤,٢. خصائص عينة الدراسة

- تم توزيع عينة الدراسة وفقاً للجنس- العمر- المستوى التعليمي -أسم الجامعة.
- تم حساب التكرار والنسب المئوية لأفراد عينة الدراسة وتتمثل في المعلومات الديموغرافية التي تشمل:
 - الجنس يشمل (ذكر-انثى)
 - الفئة العمرية تشمل (١٨ إلى ٢٥) (٢٥ إلى ٣٠) (٣٠ إلى ٤٠)
 - المستوى التعليمي يشمل (بكالوريوس-ماجستير-دكتوراه)
 - أسم الجامعة تشمل (جميع جامعات المملكة العربية السعودية)

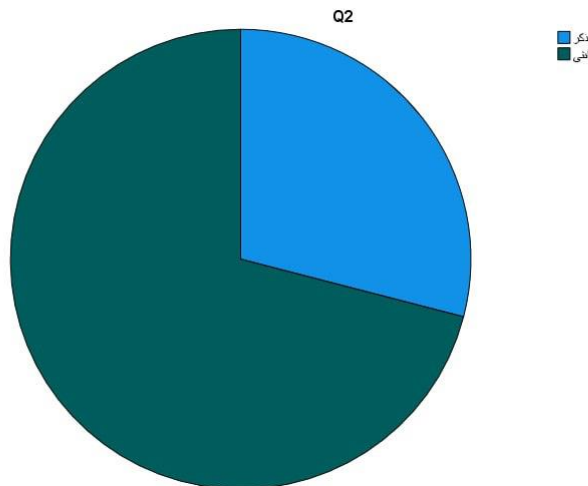
المتغير	فئات المتغير	العدد	نسبة العينة الإجمالية
الجنس	ذكر	10	77,8
	انثى	35	22,2
	الاجمالي	45	100
الفئة العمرية	١٨ إلى ٣٠	25	33,3
	٢٥ إلى ٣٠	11	24,4
	٣٠ إلى ٤٠	19	42,3
	الاجمالي	45	100
المستوى التعليمي	بكالوريوس	41	91,1
	ماجستير	4	8,9
	الاجمالي	45	100
أسم الجامعة	جامعة الإمام عبد الرحمن بن فيصل	10	22.2
	جامعة الملك فيصل	7	15.6
	جامعة نجران	3	6.7
	جامعة حائل	2	4.4
	جامعة بيشة	2	4.4
	جامعة أم القرى	2	4.4
	جامعة طيبة	1	2.2
	جامعة الملك عبد العزيز	3	6.7
	جامعة البترول	1	2.2

أسم الجامعة	جامعة الأميرة نوره	4	8.9
	جامعة شقراء	1	2.2
	جامعة سطات	2	4.4
	جامعة الإمام محمد بن سعود	1	2.2
	جامعة الملك سعود	3	6.7
	جامعة الملك خالد	1	2.2
	جامعة الالكترونية السعودية	2	4.4
	الاجمالي	45	100

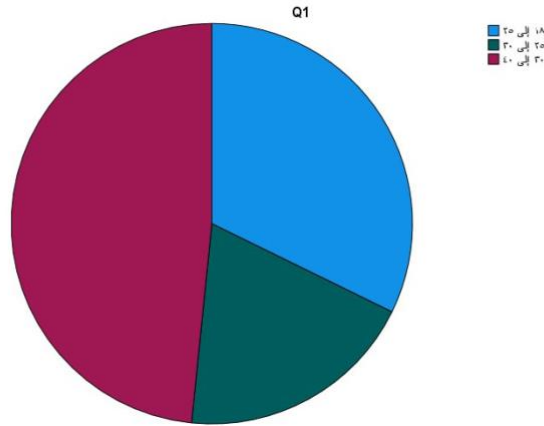
المصدر: من إعداد الباحث بالاعتماد على النتائج الإحصائية للدراسة الميدانية

من بيانات الجدول رقم (٥) تم استخلاص النتائج الآتية:

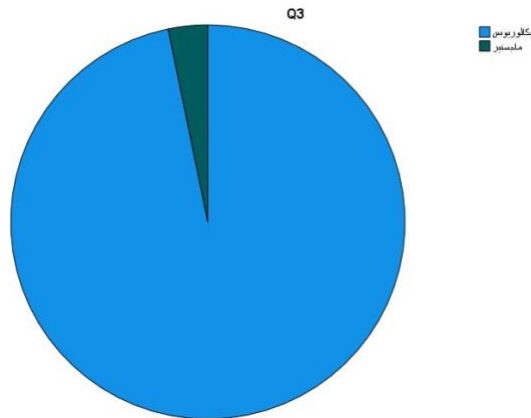
-بالنسبة للجنس: أظهرت النتائج الإحصائية ان عدد الذكور اقل من عدد الإناث, بينما عدد الإناث يشكل أكبر عدد من الذكور , حيث بلغت الذكور ١٠ مفردة بنسبة ٢٢,٢% من اجمالي العينة, بينما بلغت عدد الإناث ٣٥ مفردة بنسبة ٧٧,٨% من اجمالي العينة. كما موضح بالشكل التالي:



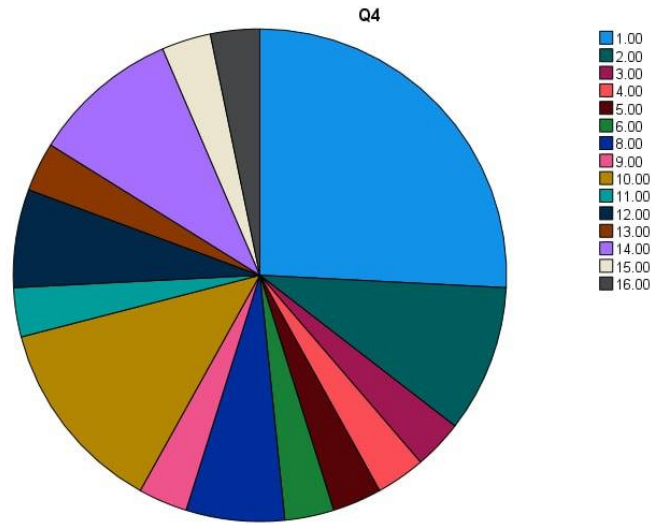
-أما فيما يتعلق بالعمر: فإن ١٥ مفردة ١٨ إلى ٢٥ سنة بنسبة ٣٣,٣% بينما الفئة العمرية من ٢٥ إلى ٣٠ سنة جاء بها ١١ مفردة بنسبة ٢٤,٤%. الفئة العمرية من ٣٠ إلى ٤٠ سنة جاء بها ١٩ مفردة بنسبة ٤٢,٣% الشكل يوضح ذلك.



-أما بالنسبة للمستوى التعليمي: بلغ عدد من يحملون مؤهل البكالوريوس ٤١ مفردة بنسبة ٩١,١% من إجمالي أفراد العينة. بينما بلغ عدد من يحملون مؤهل الماجستير ٤ مفردة بنسبة ٨,٩% من إجمالي عدد العينة. الشكل التالي يوضح ذلك.



-فيما يتعلق باسم الجامعة: فان عدد جامعة الإمام عبد الرحمن بن فيصل بلغ ١٠ مفردة بنسبة ٢٢,٢% بينما جامعة الملك فيصل جاء بها ٧ مفردة بنسبة ١٥,٦% بينما جامعة نجران جاء بها ٣ مفردة بنسبة ٦,٧% بينما جامعة حائل جاء بها ٢ مفردة بنسبة ٤,٤%. جاءت جامعة بيشة ٢ مفردة بنسبة ٤,٤% جاءت جامعة أم القرى ٢ مفردة بنسبة ٤,٤% بينما جاء بها جامعة طيبة ١ مفردة بنسبة ٢,٢%, بينما جامعة الملك عبد العزيز ٣ مفردة بنسبة ٦,٧%, جامعة البترول والمعادن ١ مفردة بنسبة ٢,٢% بينما جامعة الأميرة نورة جاء بها ٤ مفردة بنسبة ٨,٩%, جامعة شقراء جاء بها ١ مفردة بنسبة ٢,٢%, جامعة سطاتم جاء بها ٢ مفردة بنسبة ٤,٤%, جامعة الإمام محمد بن سعود جاء بها ١ مفردة بنسبة ٢,٢% بينما جامعة الملك سعود جاء بها ٣ مفردة بنسبة ٦,٧%, جامعة آلملك خالد جاء بها ١ مفردة بنسبة ٢,٢% واخيراً جامعة الإلكترونية السعودية جاء بها ٢ مفردة بنسبة ٤,٤% من اجمالي العينة. الشكل التالي يوضح ذلك.



٤.٣.١. صدق والمقاييس المستخدمة في الدراسة

من أجل التحقق من صدق وثبات المقاييس المستخدمة في الدراسة، تم اختبار صدق الاتساق الداخلي لأستبانات المستخدمة لقياس متغيرات الدراسة، بالإضافة إلى قياس الصدق التقاربي عن طريق قياس متوسط التباين المستخرج (Average Variance Extracted (AVE. بينما تم قياس الثبات للمقاييس المستخدمة في الدراسة عن طريق قياس كال من: قيمة ألفا كرونباخ Cronbach's alpha، قيمة الثبات المركب reliability Composite و قيمة معامل A-rho، من خلال نموذج المعادلة البنائية (Structural equation modelling (SEM، باستخدام برنامج التحليل الإحصائي SSPS بالإصدار ٢٨. الفقرات والجدول التالية توضح ذلك.

٤.٣.١. صدق المقاييس المستخدمة في الدراسة

صدق المقاييس المستخدمة في الدراسة
تم اختبار صدق الاتساق الداخلي للمقاييس المستخدمة في قياس متغيرات الدراسة، بالإضافة إلى قياس الصدق التقاربي عن طريق قياس متوسط التباين المستخرج Average Variance Expected (AVE) .

• صدق الاتساق الداخلي: يقصد به مدي اتساق كل عبارة من عبارات الاستبانة للمتغير الذي تنتمي إليه، لذا قامت الباحثة بقياس الاتساق الداخلي لأستبانات من خلال حساب معاملات الارتباط بين درجة كل عبارة والدرجة الكلية للمتغير التي تنتمي إليه، وفقا لدراسة (1974) Kaiser معامل الارتباط أقل من 0.5 يتم حذفه من الأستبانة.

• الصدق التقاربي Convergent Validity: يتم قياس متوسط التباين بين العبارات التي تقيس نفس المقياس، وذلك عن طريق احتساب متوسط التباين المستخرج AVE، التي يجب ان تكون قيمتها أكبر من 0.5 وقال (Hair et al. (٢٠٠٦)
الجدول التالية توضح النتائج الحصائية الخاصة بـ: (معاملات الارتباط، الانحراف المعياري، قيمة T المحسوبة، وقيمة P value - بين درجة كل عبارة والدرجة الكلية للمتغير لقياس صدق الاتساق الداخلي لأستبانات، كذلك احتساب قيمة متوسط التباين المستخرج AVE لقياس الصدق التقاربي لأستبانات، وذلك من خلال نموذج المعادلة البنائية SPSS بالإصدار 28، كما يلي:

الجدول رقم (٦) نتائج SPSS الخاصة باختبار صدق الاتساق الداخلي والتقاربي لمقاييس متغيرات الدراسة:

متوسط التباين المستخرج		العبارات	KMO	معامل الارتباط	الانحراف المعياري	P Values	المتغير	
0.670		A1	.614	.867	.45837		مخاطر الامن السيبراني	المتغير الأول
		A2		.727	.58861			
		A3		.682	.82572			
		A4		.640	.77329			
		A5		.435	.46818			
		A6		.913	.52223			
0.728	0.856	B1	.687	.844	.53936		تدابير الامن السيبراني	المتغير الثاني
		B2		.831	.77720			
		B3		.687	.69486			
		B4		.822	.86340			
		B5		.772	.77720			
		B6		.715	.70711			

المصدر: من أعداد الطالب باعتماد على النتائج الإحصائية للدراسة الميدانية برنامج SPSS

يتضح من الجدول بالأعلى:

- مقياس مخاطر الامن السيبراني: جميع معاملات الارتباط لكل العبارات ترتبط ارتباط قوي مع المتغير التابعة لها، عند قيم أكبر من 0.7. بالإضافة إلى أن قيم كل معاملات الارتباط للعبارات دالة احصائيا عند مستوى معنوية أقل من 0.001 وفقا لذلك فقد تحقق صدق الاتساق الداخلي للمقياس. كذلك، من النتائج بالأعلى المتعلقة بقيمة متوسط التباين المستخرج AVE ، يتضح ان قيمته لمتغير مخاطر الامن السيبراني هو $0.565 > 0.5$ ، وفقا لذلك، فقد تحقق الصدق التقاربي للاستبانة.

■ مقياس تدابير الامن السيبراني: جميع معاملات الارتباط للعبارات التي تقيس متغير تدابير الوقاية للامن السيبراني) للحماية من مخاطر الامن السيبراني وضع ارقام سرية قوية وتحقق بخطوتين (قيمتها أكبر من 0.7 بالإضافة إلى أن قيم كل معاملات الارتباط للعبارات دالة احصائيا عند مستوى معنوية أقل من 0.001 وفقا لذلك فقد تحقق صدق الاتساق الداخلي للمقياس بأبعاده. كذلك، من النتائج بالأعلى المتعلقة بقيمة متوسط التباين المستخرج، AVE لمتغير ككل الذي يساوي 0.736، كذلك قيم متوسط التباين المستخرج الأبعاد للحماية من مخاطر الامن السيبراني وضع ارقام سرية قوية وتحقق بخطوتين (هي: 0.758, 0.770, 0.68٠) على الترتيب. وفقا لذلك، فقد تحقق الصدق التقاربي للاستبانة.

٣.٢. ثبات أداة الدراسة

يشير ثبات الإستبيان إلى: الإستقرار في نتائج الإستبيان وعدم تغييرها بشكل كبير فيما لو تم إعادة توزيعها على أفراد العينة عدة مرات خلال فترات زمنية محددة لقياس ثبات الاستبانة المستخدمة لقياس متغيرات الدراسة، تم احتساب قيم ألفا كرونباخ بواسطة SPSS الإصدار 28، وقال Hair et al (2010) ، يجب ان تكون القيم الثالثة أكبر من 0.7 حتى يتحقق الثبات للمقياس.

قياس الثبات لأدات الدراسة

Cronbach's alpha		عدد العبارات	المتغير	
.670	.693	6	مخاطر الامن السيبراني	مخاطر الامن السيبراني
	.652			
	.577			
	.661			
	.595			
	.566			
.685	.688	6	تدابير الامن السيبراني	تدابير الامن السيبراني
	.640			
	.654			
	.698			
	.645			
	.627			

المصدر: من إعداد الباحث بناء على نتائج التحليل الإحصائي لبيانات الدراسة الميدانية.

يتضح من الجدول بالأعلى أن قيم معاملات الثبات لمقاييس الدراسة كما يلي:

- مقياس مخاطر الامن السيبراني: أظهرت النتائج الاحصائية ان قيم (ألفا كرونباخ، الثبات المركب Composite reliability، وقيمة rho-A) هم: ٠.٦٧٠، ٠.٦٨٩، ٠.٦٧٠ على الترتيب. مما يشير إلى جميع القيم أكبر من ٠.٥. وفقاً ل(Hair et al (٢٠١٠)، فقد تحقق ثبات المقياس.

■ مقياس تدابير الوقاية للامن السيبراني: أظهرت النتائج الإحصائية ان قيم (الفأ كرونباخ، الثبات المركب Composite reliability، وقيمة rhi-A) للمقياس ككل هم ٠.٦٨٥، ٠.٦٧٨، ٠.٦٨٥ على الترتيب. كذلك، قيم (الفأ كرونباخ، الثبات المركب Composite reliability، وقيمة tho-A) لابعاد ممارسات تدابير الوقاية للامن السيبراني، على الترتيب هم، الحماية من المخاطر السيبرانية: (٠.٦٣٦، ٠.٦٧٩، ٠.٦٣٦)، الحماية من المخاطر السيبرانية. مما يشير إلى أن جميع القيم أكبر من ٠.٥. وفقاً لـ (Hair et al (٢٠١٠)، فقد تحقق ثبات المقياس.

وفقاً للنتائج الإحصائية بالأعلى، التي اثبتت صدق وثبات المقاييس المستخدمة في الدراسة الحالية، مما يعني إمكانية الاعتماد على نتائجها وصالحية هذه الاستبانة للتطبيق والوثوق بها، واستخدامها في إجراء التحليلات الخاصة باختبار فروض الدراسة.

التحليل الوصفي لمتغيرات الدراسة

قد تم قياس استجابات أفراد العينة لفقرات المقياس، طبقاً لمقياس ليكرت الخماسي، وفقاً لما يلي:

موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
١	٢	٣	٤	٥

وقد تم حساب مستوى الأهمية وفقاً للمعادلة التالية:

تم حساب الوزن النسبي المقابل لكل فئة عن طريق ضرب المتوسط الحسابي في

$$[١٠٠ \div (\text{المقياس الخماسي}) = ٢٠\%]$$

يوضح الجدول التالي دلالة المتوسطات الحسابية، كما يلي:

دلالة المتوسطات الحسابية

قيمة المتوسط الحسابي	النتيجة (الاتجاه العام)	الوزن النسبي %	مستوى (درجة) الممارسة/الأهمية
من ١ إلى أقل من ١.٨٠	غير موافق بشدة	من ٢٠ إلى أقل من ٣٦ %	منخفض جداً

منخفض	من ٣٦ إلى أقل من ٥٢ %	غير موافق	من ١.٨٠ إلى أقل من ٢.٦٠ %
متوسط	من ٥٢ إلى أقل من ٦٨ %	محايد	من ٢.٦٠ إلى أقل من ٣.٤٠ %
مرتفع	من ٦٨ إلى أقل من ٨٤ %	موافق	من ٣.٤٠ إلى أقل من ٤.٢٠ %
مرتفع جدا	من ٨٤ إلى أقل من ١٠٠ %	موافق بشدة	من ٤.٢٠ إلى أقل من ٥ %

يوضح الجدول التالي التحليل الوصفي لمتغيرات الدراسة متمثلة في الأوساط الحسابية بالإعتماد على مقياس ليكرت الخماسي، والانحرافات المعيارية للمتغيرات طبقا للجدول المتعلق بدلالة المتوسط الحسابي. حيث يتم النظر إلى دلالة المتوسط الحسابي الموضح في الجدول بالأعلى لمعرفة مستوى مخاطر الامن السيبراني وكذلك مستوى تدابير الامن السيبراني وابعادها، وذلك وفقا لوجهة نظر عينة الدراسة. وذلك كما يلي:

المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة

المتغيرات	المتوسط الحسابي	الانحرافات المعيارية	الاتجاه العام	مستوى الأهمية / الممارسة
مخاطر الامن السيبراني	٣.٥٩٧	٠.٦٧٠	موافق	مرتفع
تدابير الامن السيبراني	٢.٦٥٨	٠.٥٧	موافق	مرتفع

يتضح من الجدول بالأعلى الخاص بالمتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة ما يلي:

- تظهر نتائج توصيف المتغير المستقل (مخاطر الامن السيبراني): إلى ان الاتجاه العام لمفردات عينة الدراسة هي الموافقة، مما يدل على تحقيق مستوى مرتفع من مخاطر الامن السيبراني، وذلك، حيث كان المتوسط الحسابي لاراء أفراد العينة هو (٣.٥٩٧) بنسبة موافقة عالية بلغت ٧٥.٣٦ %، عند انحراف معياري (٠.٦٧٠)

- بالنسبة لتوصيف المتغير التابع (تدابير الامن السيبراني): أوضحت النتائج ان الاتجاه العام لمفردات عينة الدراسة هي الموافقة، مما يدل على تحقيق مستوى مرتفع من تدابير الامن السيبراني، حيث بلغ المتوسط الحسابي للمتغير ككل (٢.٦٥٨) بنسبة موافقة بلغت (٦٤.٦٧%) عند انحراف معياري (٠.٥٧)، كذلك أوضحت النتائج الإحصائية الوصفية لابعاد ممارسات تدابير الامن السيبراني، أنّ الأبعاد الثلاثة لمتغير ممارسات تدابير الامن السيبراني (الحماية الطلاب والأرقام السرية) جاء الاتجاه العامه من قبل مفردات عينة الدراسة والموافقة عند مستوى مرتفع.

وفقا للنتائج الوصفية لمتغيرات الدراسة، اشارت النتائج الإحصائية الوصفية فيما يتعلق بالمتغير (مخاطر الامن السيبراني) الى الاتجاه العام لدى عينة الدراسة هو الموافقة وان تطبيقه في التعليم مرتفع، بينما كانت النتائج الإحصائية الوصفية للمتغير التابع (تدابير الامن السيبراني) وأبعاده ذات مستوى مرتفع في القطاع التعليم، وذلك من وجهة نظر عينة الدراسة.

معاملات الارتباط الخطى بين متغيرات الدراسة

يعرض الجدول التالي معاملات الارتباط الخطى (لبيرسون) بين متغيرات الدراسة، والتي تم قياسها باستخدام SPSS-28 V. وذلك على النحو التالي:

معاملات الارتباط بين متغيرات الدراسة

المتغيرات/المعنوية	مخاطر الامن السيبراني	تدابير الامن السيبراني
Pearson Correlation	.670	.746
Sig.(2-tailed)		<.001
N	204	204
Pearson Correlation	.703	.635
Sig.(2-tailed)	<.001	

313	313	N	
-----	-----	---	--

❖ الارتباط الخطي بين مخاطر الامن السيبراني (كمتغير مستقل) وتدابير الامن السيبراني وابعادها (كمتغير تابع):

- تبين وجود ارتباط معنوي قوي موجب (٠.٦٧٠) بين مخاطر الامن السيبراني كمتغير مستقل وتدابير الامن السيبراني (اجمالي) كمتغير تابع عند مستوى دلالة اقل من (٠.٠١).
- تبين وجود ارتباط معنوي قوي موجب بين مخاطر الامن السيبراني كمتغير مستقل وبين كل من أبعاد تدابير الامن السيبراني، عند معامل ارتباط: ٠.٦٧٠، ٠.٧٤٧ على الترتيب، كمتغير تابع عند مستوى دلالة اقل من (٠.٠١).
- يلاحظ مما سبق أن قيم معاملات الارتباط بين متغيرات الدراسة مرتفعة، ومما يدل على قوة هذا الارتباط.

❖ الارتباط الخطي بين أبعاد مخاطر الامن السيبراني وبين تدابير الامن السيبراني ككل، وبين بعضها البعض:

يتضح من نتائج الجدول السابق وجود ارتباط موجب معنوي بين تدابير الامن السيبراني وبين الأبعاد عند مستوى دلالة (٠.٠١).

نتائج اختبار فروض الدراسة

يتعلق هذا الجزء باختبار صحة الفرض الرئيسي للدراسة ومايتبعه من فروض فرعية، ويتم عرض النتائج الإحصائية التي تم التوصل اليها باستخدام كلا من الحزمة الإحصائية SPSS V.28، PLS-SEM على النحو التالي:

الفرض الرئيسي:

-توجد علاقة إيجابية ذات دلالة احصائية بين مخاطر الامن السيبراني وتدابير الامن السيبراني في التعليم الجامعي بالمملكة العربية السعودية
ويتفرغ من هذا الفرض الرئيسي فروضا فرعية كما يلي:

- ف ١: توجد علاقة ايجابية ذات دلالة بين مخاطر الامن السيبراني والاختراقات.
- ف ٢: توجد علاقة ايجابية ذات دلالة بين تدابير الامن السيبراني والحماية من الاختراقات والهجمات الالكترونية.

نتائج اختبار الفرض الرئيس للدراسة:

ينص هذا الفرض على أنه – توجد علاقة إيجابية ذات دلالة إحصائية بين مخاطر الامن السيبراني وتدابير الامن السيبراني بالتعليم الجامعي بالمملكة العربية السعودية.

ولاختيار هذا الفرض تم استخدام أسلوب تحليل الانحدار الخطي Simple Linear Regression Analysis بين مخاطر الامن السيبراني محل الدراسة كمتغير مستقل وتدابير الامن السيبراني (إجمالاً) كمتغير تابع.

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.177	1	.177	.841	.364 ^b
	Residual	9.067	43	.211		
	Total	9.244	44			

a. Dependent Variable: هل لديك خلفية عن مخاطر 21 من السيبراني

b. Predictors: (Constant), عدم تحديث البرامج والتطبيقات الجامعية بشكل دوري مما يسبب 21 اختراقات السيبرانية

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.139 ^a	.019	-.004-	.45920

a. Predictors: (Constant), عدم تحديث البرامج والتطبيقات الجامعية بشكل دوري مما يسبب 21 اختراقات السيبرانية

دوري مما يسبب 21 اختراقات السيبرانية



يتضح من الجداول بالأعلى ما يلي:

- يشير مستوى المعنوية لاختبار (F) هو (sig. F) اقل من (٠.٠١) مما يشير إلى معنوية نموذج الانحدار الخطي البسيط عند مستوى دلالة ٠.٠١
 - وتشير قيمة معامل الارتباط ($R=0.643$) الى وجود ارتباط موجب قوي بين مخاطر الامن السيبراني والاختراقات السيبرانية.
 - ويشير (معامل التحديد المعدل R^2) إلى أن (٥٥.٣%) من التباين الحاصل في تدابير الامن السيبراني والحماية من الاختراقات والهجمات.
- بناء على النتائج يتم السابقة يتم قبول الفرعي الثاني الذي ينص على وجود علاقة ارتباط إيجابية ذات دلالة بين مخاطر الامن السيبراني كمتغير مستقل وتدابير الامن السيبراني كمتغير تابع.

الخاتمة

بالختام التحليل الاحصائي لبيانات الدراسة الحالية، فقد تم باستخدام كلا من برنامجي SPSS SEM-PLS &V,28 ، فقد قامت الباحثة بالتحليل الوصفي لعينة الدراسة، كذلك قامت بالتحليل الوصفي لمتغيرات الدراسة. وفقا لنتائج التحليل الاحصائي لهذه الدراسة، فقد تحقق الصدق والثبات للمقاييس المستخدمة في قياس متغيرات الدراسة. كذلك، فقد تم إثبات الفرض الرئيسي للدراسة والفروض الثلاث الفرعية.

الفصل الخامس:

مناقشة النتائج

والاستنتاجات

المناقشة النتائج والاستنتاجات

المقدمة

تهدف هذه المرحلة إلى مناقشة النتائج التي تم التوصل إليها من خلال التحليل الإحصائي للبيانات المجمعة، وربطها بالإطار النظري للدراسة والدراسات السابقة ذات الصلة. كما تسعى إلى استخلاص الاستنتاجات والتوصيات المناسبة لتحسين وتعزيز الأمن السيبراني في التعليم الجامعي بالمملكة العربية السعودية.

النتائج والتوصيات

أهم النتائج التي توصل إليها البحث:

- الوعي بالأمن السيبراني:
 - ❖ قلة وعي الطلاب وأعضاء هيئة التدريس بمخاطر الأمن السيبراني.
 - ❖ نقص البرامج التعليمية والتدريبية حول الأمن السيبراني.
- البنية التحتية للأمن السيبراني:
 - ❖ عدم كفاية أنظمة الأمن السيبراني في الجامعات.
 - ❖ نقص الاستثمار في تقنيات الأمن السيبراني.
- الممارسات الأمنية:
 - ❖ عدم اتباع أفضل الممارسات للأمن السيبراني من قبل الطلاب وأعضاء هيئة التدريس.
 - ❖ نقص الوعي بأهمية استخدام كلمات مرور قوية.
- التهديدات السيبرانية:
 - ❖ التعرض لهجمات التصيد الاحتيالي والبرامج الضارة.
 - ❖ اختراق البيانات الشخصية للطلاب وأعضاء هيئة التدريس.

٥.٤. توصيات لتحسين الأمن السيبراني في الجامعات السعودية:

- رفع مستوى الوعي:
 - ❖ تنظيم حملات توعية حول مخاطر الأمن السيبراني.
 - ❖ تقديم برامج تعليمية وتدريبية حول الأمن السيبراني للطلاب وأعضاء هيئة التدريس.
- تحسين البنية التحتية للأمن السيبراني:
 - ❖ الاستثمار في تقنيات الأمن السيبراني الحديثة.
 - ❖ توظيف خبراء الأمن السيبراني لإدارة أنظمة الأمن السيبراني.
- تعزيز الممارسات الأمنية:
 - ❖ تطبيق أفضل الممارسات للأمن السيبراني في جميع أنحاء الجامعة.
 - ❖ إلزام الطلاب وأعضاء هيئة التدريس باستخدام كلمات مرور قوية.
- التعاون مع الجهات الخارجية:
 - ❖ التعاون مع الجهات الحكومية والخاصة لتحسين الأمن السيبراني في الجامعات.
- موضوع البحث:
 - ❖ تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية: مسح التعليم الجامعي في المملكة العربية السعودية.

٦.٤. حدود الدراسة

٦.٤.١. **لحدود الموضوعية:** تقتصر الدراسة على بيان واقع بمخاطر الامن السيبراني بابعادها (التحسين عمليات الامن السيبراني، تحقق بخطوتين، وضع ارقام سرية قوية) وواقع تدابير الامن السيبراني (عمل تدريب، تحديث تطبيقات والبرامج الجامعية) لدى الطلاب والطالبات والموظفين بالتعليم الجامعي.

٦.٤.٢. **الحدود البشرية:** تقتصر الدراسة على الموظفين والطلاب والطالبات بالتعليم الجامعي في المملكة العربية السعودية.

٦.٤.٣. **الحدود المكانية:** تحدد الدراسة في النطاق الجغرافي بالتعليم الجامعي بالمملكة العربية السعودية.

٦.٤.٤. **الحدود الزمانية:** سيتم اجراء الدراسة ضمن مجريات الفصل الثاني للعام الدراسي ١٤٤٦هـ الموافق ٢٠٢٤/٢٠٢٥ م.

الدراسة المستقبلية

- في ظل التحول الرقمي المتسارع والتوجه نحو التعليم الإلكتروني والخدمات الجامعية عن بُعد، من المتوقع أن تزداد أهمية وتعقيد تحديات الأمن السيبراني في المملكة. فالاعتماد المتزايد على البنية التحتية التقنية وأنظمة المعلومات في جميع أنشطة الجامعات سيزيد من إمكانية تعرضها للتهديدات الإلكترونية.
- ستتطلب هذه التطورات إجراء دراسات متعمقة لتقييم المخاطر السيبرانية المحتملة والتهديدات الناشئة في قطاع التعليم الجامعي السعودي. ومن المهم تحليل أبرز الممارسات الدولية في هذا المجال، وتحديد الثغرات والتحديات الخاصة بالسياق المحلي.
- كما ستكون هناك حاجة لإجراء مسوحات وبحوث ميدانية لقياس مستوى الوعي والاستعداد لدى القيادات الجامعية والكوادر التقنية والأكاديمية لمواجهة هجمات القرصنة والتجسس الإلكتروني. وستساعد هذه البيانات في تصميم برامج تدريبية وتوعوية فعالة.
- بالإضافة إلى ذلك، ستكون هناك حاجة لدراسة سياسات وإجراءات الأمن السيبراني المتبعة في الجامعات السعودية وتقييم مدى كفايتها. ومن المهم أيضًا تحليل التشريعات والأنظمة الوطنية ذات الصلة وسبل تطويرها لمواكبة المخاطر المتنامية.
- في المجمل، ستساهم هذه الدراسات المستقبلية في تعزيز قدرات المؤسسات التعليمية العالية في المملكة على مواجهة تحديات الأمن السيبراني وحماية بياناتها الحساسة وضمان استمرارية أنشطتها الأساسية.

الخاتمة

اختتم بحث الذي بحث فيه عن مختلف العوامل والأسباب المؤدية إلى (تحليل مخاطر الامن السببراني في المؤسسات التعليمية : مسح التعليم الجامعي المملكة العربية السعودية)، حيث استعرضت تفصيليا الدوافع والمحركات التي تقف خلف هذه الإشكالية وتطرق كذلك إلى ملخص بسيط للأفكار والنتائج والتوصيات التي تناولها البحث)، واواجه توصية للأفراد بضرورة الالتزام بأبرز القوانين والمعايير المرتبطة بموضوع دراستي، ونرفع أكف الضراعة إلى الله - عز وجل - أن يجعل هذا البحث مثقلا في ميزان أعماله وأعمالكم يوم الحساب، واسأل سبحانه وتعالى أن يوفقني لإنجاز المزيد من الأبحاث النافعة التي تسهم الفصل الراي في خدمة المسلمين والأمة الإسلامية ككل، والحمد لله الذي بنعمته تتم الصالحات.

الملخص

جاء تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية يهدف إلى تحديد وتقييم الفرص المحتملة لاختراق أنظمة المعلومات والبنية التحتية السيبرانية في المؤسسات التعليمية وتقييم التأثيرات المحتملة لهذه الاختراقات على العملية التعليمية والمعلومات الحساسة المخزنة فيها. في هذا السياق، سنلقي نظرة على دراسة حالة التعليم الجامعي في المملكة العربية السعودية.

تعد المؤسسات التعليمية في المملكة العربية السعودية هدفًا محتملاً للهجمات السيبرانية نظرًا للكمية الهائلة من المعلومات الحساسة المخزنة في أنظمتها، بما في ذلك المعلومات الشخصية للطلاب والأعضاء هيئة التدريس والبيانات البحثية والمصادر المعلوماتية الأخرى. يمكن أن يؤدي اختراق هذه المعلومات إلى تسرب البيانات الشخصية والمالية والتجسس الصناعي والتلاعب بالنتائج الأكاديمية وتعطيل الخدمات التعليمية.

يجب على المؤسسات التعليمية في المملكة العربية السعودية تنفيذ تحليل مخاطر الأمن السيبراني لتحديد الثغرات الأمنية المحتملة وتقييم مدى تأثيرها المحتمل. يشمل التحليل عادةً العديد من الخطوات مثل تحديد الأصول الحاسوبية وتصنيفها وتقييم الثغرات المحتملة وتقدير التهديدات واحتمالية حدوثها وتأثيرها، وتحديد مستوى الحماية الحالي وتحديد الإجراءات المناسبة للتخفيف من المخاطر.

بعد تحليل المخاطر، يجب على المؤسسات التعليمية تطبيق إجراءات أمنية مناسبة لحماية أنظمتها والمعلومات المخزنة فيها. يجب تنفيذ سياسات وإجراءات قوية لإدارة هوية المستخدمين ووضع قواعد وسياسات لحماية البيانات وتشفيرها وتحديث البرامج والأنظمة بانتظام وتوفير التدريب والتوعية اللازمة للطلاب وأعضاء هيئة التدريس للتعرف على التهديدات السيبرانية واتخاذ إجراءات الوقاية المناسبة.

باختصار، تحليل مخاطر الأمن السيبراني في المؤسسات التعليمية يلعب دور مهم في حماية المعلومات الحساسة والبنية التحتية السيبرانية في التعليم الجامعي في المملكة العربية السعودية من خلال تحليل المخاطر وتنفيذ إجراءات الأمن الملائمة، يمكن للمؤسسات التعليمية تعزيز أمان بيئة التعليم الرقمي والحفاظ على خصوصية وسلامة المعلومات للطلاب وأعضاء هيئة التدريس.

المراجع:

- ❖ إدارة الأمن السيبراني في مؤسسات التعليم العالي، فاطمة عبد الله الشبانان، 2021.
- ❖ الأمن السيبراني: مفاهيم وتطبيقات محمد بن عبد الرحمن آل عبد اللطيف، 2022.
- ❖ الأمن السيبراني وتحدياته في ظل التطورات التقنية، عبد الله بن محمد الحربي، 2023.
- ❖ المعهد العربي التخطيط (٢٠١٩) مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية.
- ❖ التحديات التي تواجه الأمن السيبراني في الجامعات السعودية، مجلة جامعة الملك عبد العزيز. 2023.
- ❖ أهمية الأمن السيبراني في التعليم الجامعي، مجلة جامعة الملك سعود، 2022.
- ❖ الوعي بالأمن السيبراني لدى الطلاب وأعضاء هيئة التدريس في الجامعات السعودية، مجلة جامعة الملك فهد للبترول والمعادن، 2021.
- ❖ محمود عزت، (٢٠١٨) الفضاء السيبراني وتحديات الامن المعلوماتي العربي، المجلة العربية ١، أبريل ٢٠١٨.
- ❖ التقرير الوطني للأمن السيبراني في المملكة العربية السعودية، الهيئة السعودية للبيانات والذكاء الاصطناعي، 2023.
- ❖ تقييم المخاطر السيبرانية في قطاع التعليم العالي، مركز الأمن السيبراني الوطني، 2022.
- ❖ الشيتي، ايناس إبراهيم (٢٠١٩) تقييم سياسات امن وخصوصية المعلومات التعليمية بالمملكة العربية السعودية دراسة تطبيقية على جامعة القصيم.
- ❖ العتيبي، عبد الرحمن بن بجاد (٢٠١٧) دور الامن السيبراني في تعزيز الامن الإنساني أطروحة ماجستير، جامعة نايف العربية للعلوم الأمنية.
- ❖ متطلبات تحقيق الامن السيبراني في الجامعات السعودية في ضوء رؤية ٢٠٣٠.
- ❖ السمحان، منى عبد الله. (٢٠٢٠) متطلبات الامن السيبراني لانظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية، جامعة المنصورة.
- ❖ جريدة سبق. (٢٠١٩) السعودية تحقق المركز ١٣ عالميا في مؤشر الأمم المتحدة للأمن السيبراني ٢٧/٣/٢٠١٩.

- ❖ الشوابكة، عدنان عواد. (٢٠١٩) دور إجراءات الامن المعلوماتي في الحد من مخاطر امن المعلومات في جامعة الطائف، مجلة دراسات وابحاث، مج (١١)، ع (٤) ١٦٤-١٨٧.
- ❖ الصاحب محمود، (٢٠١٣) سياسة امن المعلومات في الجامعات: حالة دراسية (جامعة بولنيكنيك فلسطين-الخليل) Cybrarians Journal، ع٣٣، ديسمبر.
- ❖ تحليل مخاطر الأمن السيبراني في جامعة سعودية، شركة XYZ للاستشارات 2021.
- ❖ (Rehman, H., Masood A. & Cheema A. (٢٠١٥). Information Security Management in Academic Institutes of Pakistan, nd. National Conference of Information Assurance (NCIA Protecting (٢٠١٩) John M. Broky, Thomas H. Bradley. (❖ Information with Cybersecurity, Berlin: Springer International Available at: ٣٥٠-٣٥١ .Pp ٢٠١٩ Publishing AG, https://link.springer.com. mplb ..١١٠٤.xn٠٨١٠٢٩٣http:// (٢٠١٩/٤/١٥) :ci.ekb.eg/content/pdf, Access Date

الملاحق

استبانة:

السلام عليكم ورحمة الله وبركاته

تحية طيبة،

يشرفني ان اضع بين ايديكم هذا الاستبيان المعد لأغراض البحث العلمي تهدف الاطروحة بعنوان "تحليل مخاطر الامن السيبراني بالتعليم الجامعي"، والذي اسعى من خلاله الى التعرف على آرائكم حول المحاور التي تتضمنها استمارة الاستبيان، علما بان جميع المعلومات التي سوف يتم جمعها سيتم التعامل معها بسرية تامة ولغرض البحث العلمي فقط.

من اجل هذا ارجوا منكم التفضل بالإجابة،

ولكم جزيل الشكر على تعاونكم.

الجنس	ذكر	انثى
المستوى التعليمي	بكالوريوس	ماجستير
العمر	18 الى 25	25 الى 30
اسم الجامعة		دكتورة

موافق بدرجة					العبارة	
موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة		
					المحور الأول: مخاطر الامن السيبراني	
					1 هل لديك خلفية عن مخاطر الامن السيبراني	
					2 عدم تحديث البرامج والتطبيقات الجامعية بشكل دوري مما يسبب الاختراقات السيبرانية	
					3 أكثر مخاطر الامن السيبراني شيوعا التي تواجهها الجامعات هي الاختراقات الالكترونية	
					4 هل تتعرض المؤسسات التعليمية الى مخاطر سيبرانية	
					5 عدم توفير حماية كافية ضد البرامج والتطبيقات الجامعية من العوامل التي تسبب الهجمات السيبرانية	
					6 مشاركة كلمة المرور الخاصة بين الموظفين والطلاب من العوامل التي تسبب الهجمات السيبرانية	

موافق بدرجة					العبارة	
موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة		
					المحور الثاني: تدابير الامن السيبراني التي تتخذها الجامعات السعودية	
					1	عقد دورات تدريبية للموظفين والطلاب بالمخاطر السيبرانية بالجامعات
					2	تقوم الجامعات بتحديث وتطوير التطبيقات الجامعية بشكل دوري
					3	وضع التحقق بخطوتين بالتطبيقات الجامعية للحماية من الهجمات السيبرانية
					4	تؤكد الجامعات على ضرورة استخدام كلمة مرور معقدة وقوية لا يمكن تخمينها للحماية من الاختراقات وتغيرها من وقت لآخر
					5	توفر الجامعات الدعم الفني والتقني لمعالجة لمشكلات والمشاكل السيبرانية
					6	وضع تطبيق لكشف الثغرات الجامعية للحماية من المخاطر السيبرانية

رابط الاستبيان:

<https://docs.google.com/forms/d/e/1FAIpQLSenfLF4ydfEIs0jwcNxnA65fB7UCnLH5ZRt6Kza0ZCW9KiQ/viewform>