



دراسة مسحية لتطبيق إطار الأمن السيبراني وأثرها على الأنظمة التقنية في القطاع الصحي - المملكة العربية السعودية

**A survey study of the application cybersecurity framework
and their impact on the health sector - Kingdom of Saudi Arabia**

"قدمت هذه الرسالة استكمالاً لمتطلبات الحصول على درجة الماجستير كلية الإدارة –
إدارة المخاطر -جامعة الجميع الذكية"

إعداد البحث	الرقم الجامعي
سلطان عواض المطيري (قائد الفريق)	20223006323
عهد سعد الرويتع	20223006404
عبدالله فهد الخرجي	20223006376

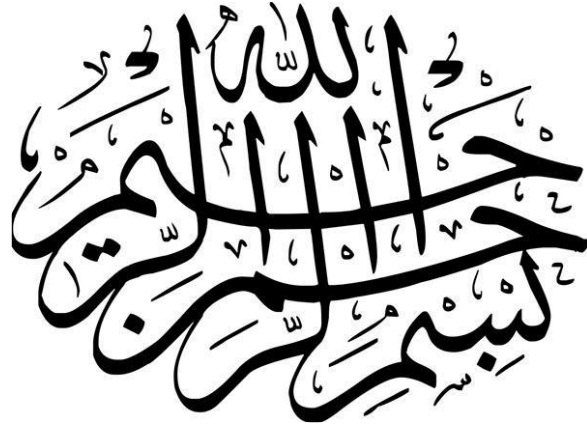
اشراف الدكتور

Waleed abdelgawwad

Midocean University

Imam Shafi'i College of Islamic and Arabic Sciences. s. Box: 6063
Moroni Comoros

2023 م - 1444هـ



(يَرْفَعُ اللَّهُ الَّذِينَ آمَنُوا مِنْكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ)

صدق الله العظيم

(المجادلة : 11)

شكر وتقدير

الحمد لله ، الحمد لله حمداً يملأ الميزان له الحمد عدد ما خطه القلم واحصاه الكتاب ووسعته الرحمة ،
والصلاة والسلام على خاتم الرسل ، ومن لا نبي بعده صلاة تقضي بها الحاجات وترفعنا لأعلى الدرجات وتبلغنا بها
أقصى الغايات من جميع الخيرات في الحياة وبعد الممات ولله الحمد والشكر أولاً وآخراً..
انطلاقاً من قول المصطفى صلى الله عليه وسلم (لا يشكر الله من لا يشكر الناس)...
إلى معنى الحب والحنان الى بسمه الحياة وسر الوجود إلى من كان دعاءهم سر نجاحنا بعد الله الى أمي وأبي.
إلى من وقفوا بجاني وشاركوني طعم الحياة ... إخواني وأخواتي الأعزاء..
إلى أستاذي الفاضل / وليد سليمان المشرف على هذه الدراسة وذلك نظير المجهود الذي بذله في متابعة هذه
الدراسة وما قدمه لنا من توجيهات دعم وتشجيع كان لها الأثر الواضح في إتمام هذه الدراسة.
والى كل من شددوا أزرونا وشاطرونا الأمر لإكمال الخطوات لولاهم بعد الله سبحانه وتعالى لاعتذر القلم عن رسم
الكلمات (زملائي) أطال الله أعماركم بالصحة والسعادة وسدد طريق الخير لخطاكم ..
كما نتوجه بالشكر لجميع العاملين في المستشفيات قيد البحث (مدينة الملك سعود الطبية، مستشفى الايمان
العام، مستشفى الملك سلمان ، مستشفى الامام الفيصل، مستشفى الامير محمد بن عبدالعزيز) لما قدموه
لنا من تسهيلات وتعاون كان له بالغ الأثر في إنجاح هذه الرسالة.

وكل الشكر والتقدير لكل شخص كان لنا عون بعد الله في إتمام هذا البحث ..

فهرس المحتويات

ب	شكر وتقدير
ت	فهرس المحتويات
ح	فهرس الجداول
ح	فهرس الأشكال
ح	فهرس الملاحق
1	الفصل الأول
1	الإطار العام للدراسة
2	مقدمة البحث
3	مشكلة البحث
4	ثالثاً: فرضيات البحث
4	أهداف البحث :
5	أهمية البحث :
5	الأهمية العلمية
5	الأهمية التطبيقية
6	حدود الدراسة
6	متغيرات البحث
7	مصطلحات البحث :
8	الفصل الثاني
8	الإطار النظري
9	المبحث الأول : مفهوم إطار الأمن السيبراني
9	مقدمة
9	أولاً : الأمن السيبراني... مفهومه وأهميته وأهدافه
9	مفهوم الأمن السيبراني :
9	الأمن السيبراني
10	مفاهيم المرتبطة بالأمن السيبراني
11	من أهم أهداف الأمن السيبراني : (جبور، 2016)

12	أهمية دراسة الأمن السيبراني :-
12	ثانياً : أنواع الجرائم السيبرانية
13	أسباب الجرائم السيبرانية
14	المبحث الثاني : فاعلية الأنظمة التقنية (التشغيلية)
14	مقدمة
15	أولاً : مفهوم النظام
15	ثانياً: مكونات النظام
16	ثالثاً : الفوائد التي تحققها الأعمال الإلكترونية للمنظمات
17	رابعاً :عناصر الأمن السيبراني
18	المبحث الثالث : الأنظمة التقنية في القطاع الصحي
19	تقنيات الأعمال الإلكترونية في المنظمات الصحية:
21	التحديات التي تواجه تبني تقنيات الأعمال الإلكترونية في المنظمات:
24	الفصل الثالث
24	الدراسات السابقة
25	مقدمة
25	1. الدراسات السابقة المحلية
27	2. الدراسات السابقة العربية
28	3- الدراسات السابقة الأجنبية
29	التعليق على الدراسات السابقة:
31	ملخص الفصل الثالث
32	الفصل الرابع
32	منهجية الدراسة
33	مقدمة
33	اولاً : منهج البحث:
34	ثانياً : مجتمع البحث
35	ثالثاً : عينة البحث
35	رابعاً : خطوات بناء أداة البحث (الاستبانة)

36	خامساً: مكونات أداة البحث (الاستبانة)-----
39	سادساً: صدق وثبات أداة البحث (الاستبانة)-----
46	سابعاً: التوزيع الطبيعي لمتغيرات البحث-----
46	ثامناً: الأساليب الإحصائية المستخدمة في البحث-----
47	ملخص الفصل الرابع-----
49	الفصل الخامس-----
49	تحليل البيانات واختبار فرضيات البحث-----
50	مقدمة-----
50	أولاً: تحليل خصائص عينة البحث-----
52	توزيع عينة البحث حسب مكان العمل-----
53	توزيع عينة البحث حسب الجنس-----
55	- توزيع عينة البحث حسب المسمى الوظيفي:-----
56	توزيع عينة البحث حسب عدد سنوات الخبرة في مجال العمل:-----
57	ثانياً: نتائج تحليل مجالات و أبعاد البحث-----
64	ثالثاً: اختبار ومناقشة فرضيات البحث-----
68	الفصل السادس-----
68	النتائج والتوصيات-----
69	مقدمة-----
69	أولاً: النتائج-----
71	ثانياً: التوصيات-----
72	الدراسات المستقبلية المقترحة-----
73	ملخص الفصل السادس-----
74	المراجع-----
81	قائمة المحكمين-----
85	ملخص الدراسة-----
86	ABSTRACT-----

فهرس الجداول

- جدول رقم (1) : مجتمع البحث، ونسبة التمثيل لكل مستشفى بالنسبة للمجتمع الكلي.....34
- جدول رقم (2) : يوضح توزيع فقرات الاستبانة على المجالات والأبعاد المكونة لها.....37
- جدول رقم (3) : تصحيح أداة البحث وفق مقياس ليكرت الخماسي.....37
- جدول رقم (4) : مستويات الموافقة على فقرات وأبعاد ومجالات البحث.....38
- جدول رقم (5) : معاملات الارتباط (الصدق) بين الدرجة الكلية للاستبانة والمجالات والأبعاد الفرعية.....39
- جدول رقم (6) : معاملات صدق الاتساق الداخل لفقرات البعد الأول.....40
- جدول رقم (7) : معاملات صدق الاتساق الداخل لفقرات البعد الثاني.....41
- جدول رقم (8) : معاملات صدق الاتساق الداخل لفقرات المجال فاعلية الأنظمة التقنية في القطاع الصحي.....42
- جدول رقم (9) : أدناه يوضح نتائج حساب معامل ألفا كرونباخ لقياس الثبات :.....44
- جدول رقم (19) : نتائج تحليل مجالات وأبعاد البحث.....58
- جدول رقم (20) : حساب الوسط الحسابي والانحراف المعياري والوزن النسبي.....60
- جدول رقم (21) : يوضح نتائج التحليل المتعلقة بفقرات المجال.....62
- جدول رقم (22) : يوضح ارتباط بيرسون بالمتغير التابع.....66
- جدول رقم (23) : علاقة المتغير التابع.....67

فهرس الأشكال

- شكل رقم (1) : توزيع عينة البحث حسب مكان العمل.....52
- شكل رقم (2) : توزيع عينة البحث حسب الجنس.....53
- شكل رقم (3) : التوزيع النسبي للعاملين السعوديين في المجالات الصحية (15 سنة فأكثر) حسب المهنة الرئيسية والجنس.....54
- شكل رقم (4) : توزيع عينة البحث حسب المسمى الوظيفي.....55
- شكل رقم (5) : توزيع عينة البحث حسب مجال العمل.....56

فهرس الملاحق

- الاستبانة النهائية78
- كتاب تسهيل مهمة باحث82
- الهيكل التنظيمي يوضح أقسام الأمن السيرياني في مستشفى الإمام فيصل84

الفصل الأول

الإطار العام للدراسة

أولا : مشكلة البحث

ثانيا: تساؤلات البحث

ثالثا: فرضيات البحث

رابعا: أهداف البحث

خامسا: أهمية البحث

سادسا : حدود الدراسة

سابعا: مصطلحات الدراسة

مقدمة البحث

تعرضت الأنظمة التقنية في القطاع الصحي في كثير من الدول لأزمات تتعلق بالأمن السيبراني خلال السنوات الأخيرة ؛ ومع انتشار الانترنت والتقنيات الحديثة كانت الأنظمة التقنية الصحية عرضة للاحتتمالات الخطيرة التي تشمل الاختراق والتهديدات الأخرى. هدف هذا البحث الى التعرف على إطار الأمن السيبراني الذي تطبقه الأنظمة الصحية في المملكة العربية السعودية، وتأثيره على نجاح الأنظمة التقنية في القطاع الصحي وللقيام بذلك سنقوم بدراسة إطار الأمن السيبراني السائد، وأثر تطبيق سياسات الأمن السيبراني على الأنظمة التقنية الصحية في المملكة العربية السعودية. إضافة إلى ذلك، سنقوم بتوضيح الإجراءات التي تطبقها الأنظمة الصحية السعودية لحماية أنظمتها التقنية والبيانات الخاصة بها . وبعد تقييم كفاءة سياسات الأمن السيبراني في مؤسسات القطاع الصحي أمراً بالغ الأهمية بسبب التطور في قطاع تكنولوجيا المعلومات والاتصالات . لذلك يجب على المستشفيات على وجه الخصوص أن تعكس ذلك في أدائها المؤسسي لتحقيق الأمان التقني لأنظمتها و التطبيقات المستخدمة لهذا الغرض . حيث أن أي خرق أو عيب يمكن أن يتسبب في أضرار جسيمة وخسائر فادحة لهذا القطاع الحيوي لذلك فإن ضمان أمن الأنظمة التقنية أمر بالغ الأهمية.

لقد أصبح إطار الأمن السيبراني قائماً بشكل دائم لحماية الأنظمة التقنية من السرقة أو التلاعب بها أو تدميرها ، بداية بتحديد أنظمة وبيانات القطاع الصحي التي تحتاج إلى تأمين، حيث أن هناك الكثير من النظم التي يحتاج قطاع الصحة لتأمينها، ومن الأمثلة على تلك النظم هو(إنترنت الأشياء)، حيث يتم استخدام إنترنت الأشياء كثيراً في كل مكان، وبشكا خاص في قطاع الصحة ، حيث أن هناك داخل المستشفيات الكثير من المعدات الطبية التي يتم ربطها بواسطة إنترنت الأشياء، على سبيل المثال أجهزة الاستشعار الطبية التي تغذي المستشفى بأنواع مختلفة من المعلومات المطلوبة وغير ذلك من الأدوات والأنظمة المتطورة ، وكلما ازدادت فاعلية هذه النظم، كلما ساهمت بشكل أكبر في تسهيل الحفاظ على النظم والتقنيات (الطائي، 2004، صفحة 177).

مشكلة البحث

تنبع أهمية فاعلية نظام الأمن السيبراني من الدور الكبير الذي يلعبه رسم الاطار في نجاح المؤسسات، فبالقدر الذي تتصاعد فيه فاعلية النظم التقنية ودرجة أمانها، تزداد قدرتها على إنجاز الوظائف التشغيلية بدقة وأمان ، وحيث تتم اليوم معالجة قضايا الأمن السيبراني في القطاع الصحي بالنظر إلى الزاوية المعلوماتية والبيانية فقط ، لكن من الناحية العملية فإن مشكلات الأمن السيبراني تحمل الكثير من التعقيدات من المشكلات الفنية والتنظيمية والتقنية، ولعل الحل يكمن بإدارة أفضل في مجال الأمن السيبراني عبر ممارسة عملية تقييم وإدارة المخاطر وإيجاد إطار لتحقيق الامن السيبراني للأنظمة التقنية ووضع الحلول الأمنية كإطار عام لسياسات الأمن السيبراني، ومراجعة أنظمة الرقابة والتحكم والحلول الاستراتيجية الأخرى الممكنة.

فقطاع الصحة قطاع حساس، وهو أحد القطاعات التي تحاول بكل قوتها جعل المخاطر منخفضة قدر الإمكان، لأنها ترتبط بعمليات إنقاذ الأرواح للمرضى .

ومن خلال هذه الدراسة يستطيع متخذي القرار في الادارات العليا في القطاع الصحي التعرف على واقع إطار الأمن السيبراني داخل المستشفيات والوقوف على جوانب الخلل ومعالجة أو إيجاد حلول لقضايا الأمن السيبراني المتعلقة في جانب القطاع الصحي ، حيث ان تضمين سياسات أمن المعلومات ضمن الخطة الإستراتيجية لنظم المعلومات يكفل الجودة للعمليات التشغيلية وكذلك للبيانات والمعلومات المختلفة (Doherty & Fulford, 2006).

وبناء على ما سبق يمكن صياغة مشكلة البحث من خلال السؤال الرئيسي التالي :

ما علاقة تطبيق إطار الأمن السيبراني بفاعلية الأنظمة التقنية في القطاع الصحي في المملكة العربية السعودية؟

ومن خلال ما سبق يمكن صياغة مشكلة الدراسة بالتساؤلات التالية:

1. ما هو مستوى تبني الإدارة العليا لإطار الأمن السيبراني في القطاع الصحي ؟
2. ما هو مستوى تقدير مخاطر الامن السيبراني وأثره على فاعلية الأنظمة التقنية في القطاع الصحي ؟
3. ما هو مستوى التدريب والتوعية بسياسة الأمن السيبراني وتأثيره على الأنظمة التقنية في القطاع الصحي ؟
4. ما علاقة مراجعة وتحديث سياسات الأمن السيبراني بفاعلية الأنظمة التقنية في القطاع الصحي ؟

ثالثاً: فرضيات البحث

يوجد علاقة ذات دلالة احصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين سياسات إطار الأمن السيبراني وفاعلية

الأنظمة التقنية في مستشفيات القطاع الصحي. ويتفرع منها الفرضيات الفرعية التالية:

أ. يوجد علاقة ذات دلالة احصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين تقدير الإدارة العليا لمخاطر أمن

المعلومات السيبراني وفاعلية النظم التقنية في مستشفيات القطاع الصحي في المملكة العربية السعودية.

ب. يوجد علاقة ذات دلالة احصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين التدريب والتوعية بتحديثات سياسات

أمن المعلومات السيبراني وفاعلية النظم التقنية في مستشفيات القطاع الصحي في المملكة العربية السعودية.

أهداف البحث

1. دراسة العلاقة بين سياسات الامن السيبراني بأبعادها الثلاثة (تقدير الإدارة العليا لمخاطر أمن المعلومات

السيبراني ، التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني ، وفاعلية النظم التقنية داخل

القطاع الصحي).

2 . معرفة مستوى سياسات أمن المعلومات السيبراني في القطاع الصحي .

3 . بيان مستوى فاعلية النظم التقنية في مستشفيات القطاع الصحي.

4. تقديم مجموعة من التوصيات التي تهدف لدعم سياسات أمن المعلومات السيبراني في القطاع الصحي ، وزيادة

فاعلية النظم التقنية.

5. تحديد الاستراتيجيات الحديثة التي يمكن تطبيقها في القطاع الصحي في المملكة العربية السعودية لتعزيز إطار

الأمن السيبراني.

أهمية البحث

الأهمية العلمية

يتوقع الباحثون أن يكون هذا البحث مرجعاً مهماً للباحثين والدارسين حيث أنه يلقي الضوء على قضية هامة وهي تحديد أثر تطبيق سياسة إطار الأمن السيبراني على الأنظمة التقنية في القطاع الصحي في المملكة العربية السعودية. كما يمكن لنا أن نستخدم نتائج هذه الدراسة لتحسين سياسات الأمن السيبراني وتأثيره على تجويد الأنظمة الموجودة داخل القطاع الصحي.

كما أنه بعد إطلاع الباحثين على الدراسات السابقة وجد أن تلك الدراسات ركزت بشكل أكبر على مفهوم إدارة أمن المعلومات بشكل عام، في حين عانت سياسات الأمن السيبراني من قلة الدراسات العربية.

الأهمية التطبيقية

تكمن أهمية البحث التطبيقية، في أنه سوف يساعد صناع القرار في القطاع الصحي داخل المملكة العربية السعودية على التعرف على واقع الأمن السيبراني وعلاقتها بفاعلية الأنظمة التقنية ، كما يمكنهم من الاعتماد على نتائج البحث لتطبيق سياسات الأمن السيبراني التي ستعكس بالإيجاب على رفع فاعلية الحماية للنظم التقنية والمعلوماتية وهو طريقة لحماية الأنظمة التقنية والبيانات من الاختراق أو الوصول غير المصرح به. حيث بات من الضروري أن يكون النظام التقني داخل القطاع الصحي الحالي في المملكة العربية السعودية محميًا من خلال إطار متكامل لتطبيق سياسات الأمن السيبراني، حتى يتمكن المستخدمون من الاعتماد على هذه الأنظمة لتوفير خدمات صحية آمنة. في هذه الدراسة، سيتم التركيز على تحديد مستوى الأمن السيبراني الذي يوجد في الأنظمة التقنية الصحية في المملكة العربية السعودية، وتحديد الفرص والتحديات المحتملة بشأن تطبيق إطار الأمن السيبراني في هذا القطاع.

كما سيتم التركيز على تحديد تأثير تطبيق إطار الأمن السيبراني على الأنظمة التقنية الصحية ، و بناءً على نتائج هذه الدراسة، يمكن للحكومة والجهات القطاعية في المملكة العربية السعودية من تطوير الإجراءات وسياسات الأمن السيبراني لحماية الأنظمة التقنية الصحية من الاختراق أو الوصول غير المصرح به.

حدود الدراسة

الحدود المكانية: تمت الدراسة في المملكة العربية السعودية.

الحدود الزمنية: طبقت الدراسة في الفترة من 1/2023 وحتى 4/2023

الحدود الموضوعية: ركزت الدراسة في التعرف على واقع إدارة الأمن السيبراني لنظم المعلومات في القطاع الصحي للمستشفيات الحكومية بالمملكة وسبل التطوير الممكنة لها من الواقع الذي تم دراسته.

الحدود المؤسسية: تناولت الدراسة خمس مستشفيات حكومية في المملكة:

1- مدينة الملك سعود الطبية

2- مستشفى الايمان العام

3- مستشفى الملك سلمان

4- مستشفى الامام الفيصل

5- مستشفى الامير محمد بن عبدالعزيز.

الحدود البشرية: تمت الدراسة على العاملين في مراكز ووحدات تكنولوجيا المعلومات إضافة إلى أعضاء أقسام / مراكز الحاسوب في المستشفيات الحكومية وكذلك العاملين بالأقسام المختلفة في المستشفيات والذين يستخدمون نظم المعلومات بشكل أساسي في أعمالهم اليومية.

الحدود الموضوعية: بحث علاقة سياسات تطبيق إطار الأمن السيبراني بفاعلية النظم التقنية في مستشفيات القطاع الصحي داخل المملكة العربية السعودية.

متغيرات البحث

1. المتغير المستقل: سياسات إطار الأمن السيبراني ويتفرع منه:

أ. تقدير الإدارة العليا لمخاطر أمن المعلومات السيبراني .

ب. التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني.

2. المتغير التابع: فاعلية الأنظمة التقنية داخل القطاع الصحي.

مصطلحات البحث :

عرف الباحثون مصطلحات البحث تعريفات إجرائية كما يلي :

1 . الأمن السيبراني : ويقصد به " جميع الاجراءات والتدابير والتقنيات والأدوات المستخدمة لحماية سلامة الشبكات والبرامج والبيانات من الهجوم أو التلف أو الوصول غير المصرح به ، ويشمل كذلك حماية الأجهزة والبيانات " .

2 . سياسات الأمن السيبراني: هي مجموعة من القواعد التي يتعين عليها الإتاحة والتطبيق والتحقق منها لضمان أمن المعلومات الخاصة بشركات ومؤسسات. تهدف إلى ضمان الخصوصية والنشاط السليم للمعلومات وأنظمة الحاسوب.

3 . الأنظمة التقنية : الانظمة التقنية هي الانظمة المصممة للتحكم في تشغيل الأجهزة، والبرامج، والتطبيقات، والشبكات المستخدمة في الشركات والمنظمات. يتضمن ذلك أنظمة الخدمات المحلية، والشبكات المتكاملة، وأنظمة وحدات التحكم المتقدمة، وأنظمة الحزم المتكاملة، وأنظمة الاتصالات، وأنظمة الحماية الأمنية، وأنظمة الإدارة المحلية والمتكاملة، وأنظمة الجداول الزمنية المتقدمة، وأنظمة الإدخال والإخراج المتقدمة، وأنظمة التخطيط المتكاملة، وأنظمة التشغيل المحلية والمتكاملة، وأنظمة التشغيل المحلية والمتقدمة.

4. التبني الفاعل لتقنيات ونظم الأمن السيبراني: وتعني في هذه الدراسة مدى قدرة المستشفيات على توظيف تقنيات ونظم الأمن السيبراني التي تمتلكها بشكل يحقق الغرض منها ويسهل الحفاظ على الأنظمة التقنية .

الفصل الثاني

الإطار النظري

المبحث الأول : مفهوم إطار الأمن السيبراني

المبحث الثاني : فاعلية الأنظمة التقنية (التشغيلية)

المبحث الثالث : الأنظمة التقنية في القطاع الصحي

المبحث الأول : مفهوم إطار الأمن السيبراني

مقدمة

يعتبر تزايد المعلومات وكثرة الاعتماد عليها من أهم السمات التي تميز العصر الحالي، ومع التطور التكنولوجي المتسارع، زاد الاهتمام بأمن المعلومات السيبراني، وأصبح من القضايا الهامة والرئيسية التي يهتم بها مصممي النظم ومستخدميها على السواء لضمان حماية معلوماتهم والحفاظ عليها. إن تطور تقنيات معالجة المعلومات وتداولها قد أدى إلى كثرة المعلومات وتشعبها، مما ألقى عبئاً كبيراً على المؤسسات للحفاظ على هذه المعلومات من خلال تنظيمها، حفظها، تحديثها، وسرعة استرجاعها، بالإضافة لتأمينها وحمايتها (القحطاني، 2008، صفحة 16).

أولاً: الأمن السيبراني... مفهومه وأهميته وأهدافه

مفهوم الأمن السيبراني:

معنى كلمة سيبراني (cyber): تطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الانترنت والفضاء السيبراني وهو يعني كل ما يتعلق ، بشبكات الحاسوب، والإنترنت، والتطبيقات المختلفة (كالواتساب، والفيس بوك، وغيرها من مئات التطبيقات)، وكل الخدمات التي تقوم بتنفيذها (كتحويل الأموال عبر النت، والشراء أون لاين، وغيرها من آلاف الخدمات في جميع مجالات الحياة على مستوى العالم) الموسوعة السياسية، (2018).

الأمن السيبراني

يقصد بالأمن السيبراني حماية الأشياء من خلال تكنولوجيا المعلومات مثل الأجهزة والبرمجيات. والقول بالأمن السيبراني يعني اتخاذ التدابير اللازمة لحماية الفضاء السيبراني من الهجمات السيبرانية، وذلك من خلال مجموعة من الوسائل المستخدمة تقنياً وتنظيماً وإدارياً في منع الوصول غير المشروع للمعلومات الإلكترونية ومنع استغلالها بطريقة غير قانونية ونظامية، وبذلك فإنه يهدف إلى الحفاظ على استمرارية الأنظمة والمعلومات المتوفرة بها، وحمايتها بكل خصوصية وسرية من خلال إتباع التدابير والإجراءات اللازمة لحماية البيانات (الغثرو والصبيح، 2012).

الأمن السيبراني لغوياً: الأمن السيبراني مكون من لفظتين: "الأمن"، و"السيبراني".

الأمن: هو نقيض الخوف، أي بمعنى السلامة والأمن مصدر الفعل أَمِناً.

وأمنه: أي اطمئنان النفس وسكون القلب وزوال الخوف، ويقال: أَمِنَ من الشر، أي سَلِمَ منه.

السيبراني: مصطلح السيبرانية الآن هو واحد من أكثر المصطلحات تردداً في معجم الأمن الدولي.

وكلمة cyber لفظة يونانية الأصل مشتقة من كلمة "kybernetes" بمعنى الشخص الذي يدير دفة السفينة

حيث تستخدم مجازاً للمتحكم.

الأمن السيبراني اصطلاحاً: هناك العديد من التعاريف التي قُدمت لمفهوم الأمن السيبراني، حيث يعرف بأنه

مجموعة من الإجراءات المتخذة في مجال الدفاع ضد الهجمات السيبرانية ونتائجها التي تشمل تنفيذ التدابير

المضادة المطلوبة " (ابوزيد، 2019).

وقدمت وزارة الدفاع الأمريكية تعريفاً دقيقاً لمصطلح الأمن السيبراني فاعتبرته " جميع الإجراءات التنظيمية

اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب،

التجسس والحوادث".

مفاهيم المرتبطة بالأمن السيبراني

هناك العديد من المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

الفضاء السيبراني: عرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI التواصل المشكل من خلال الربط

البيئي العالمي لمعدات المعالجة الآلية للمعطيات الرقمية. "فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير

مادية، مكونة من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو

مستعملين.

الردع السيبراني: يعرف الردع السيبراني بأنه " منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي

تدعم العمليات الفضائية " (بارة، 2017، صفحة 28).

الهجمات السيبرانية تعرف بأنها: " فعلاً يقوض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي،

من خلال استغلال نقطة ضعف معينة تمكن المهاجم من التلاعب بالنظام." (بوغرارة، 2018، صفحة 13).

الجريمة السيبرانية: مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها (جبور، 2016، صفحة 16).

وإجمالاً يمكن القول إن الأمن السيبراني هو مجموعة الآليات والإجراءات والوسائل والأطر التي تهدف إلى حماية البرمجيات وأجهزة الكمبيوتر (الفضاء السيبراني بصفة عامة) من مختلف الهجمات والاختراقات والتهديدات السيبرانية التي قد تهدد الأمن القومي للدول.

أمن المعلومات: وهو عبارة عن مجموع من الإجراءات التقنية والإدارية تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصود أو غير مصرح به بالتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات من أي تغيير أو تلف (القرشي، 2011، صفحة 29).

أهداف الأمن السيبراني

من أهم أهداف الأمن السيبراني : (جبور، 2016)

- ١- تعزيز حماية أنظمة التقنيات التشغيلية على كافة الأصعدة ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات وما تحويه من بيانات.
- ٢- التصدي لهجمات وحوادث امن المعلومات التي تستهدف الأجهزة الحكومية ومؤسسات القطاع العام والخاص.
- ٣- توفير بيئة آمنة موثوقة للتعاملات في مجتمع المعلومات.
- ٤- صمود البنى التحتية الحساسة للهجمات الإلكترونية.
- ٥- توفير المتطلبات اللازمة للحد من المخاطر والجرائم الإلكترونية التي تستهدف المستخدمين.
- ٦- التخلص من نقاط الضعف في أنظمة الحاسب الآلي والأجهزة المحمولة باختلاف أنواعها.
- ٧- سد الثغرات في أنظمة امن المعلومات.
- ٨- مقاومة البرمجيات الخبيثة، ما تستهدفه من أحداث أضرار بالغة للمستخدمين.
- ٩- حد من التجسس والتخريب الإلكتروني على مستوى الحكومة والأفراد.

أهمية الأمن السيبراني: (شلوش، 2018)

في عالم اليوم المترابط بواسطة الشبكات ، يستفيد الجميع من برامج الدفاع السيبراني.

وتتمثل أهمية الأمن السيبراني فيما يلي:

-الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيدي من العبث بها -تحقيق وفرة البيانات وجاهزيتها

عند الحاجة إليها.

-حماية الأجهزة والشبكات كـ كل من الاختراقات لتكون درعاً واقياً للبيانات والمعلومات.

-استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.

-استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.

-توفير بيئة عمل آمنة جداً خلال العمل عبر الشبكة العنكبوتية.

أهمية دراسة الأمن السيبراني :

هناك عدد من الأسباب التي تجعل دراسة الأمن السيبراني من أبرز المجالات التي تحتاج لوجود خبراء مؤهلين

لحماية أمن الشركات والمؤسسات والدول أيضاً، ومن أبرزها :

١. يشهد سوق العمل حاجة مستمرة لخبراء مجال الأمن السيبراني.

٢. بالعمل في مجال الأمن السيبراني يمكن جني الكثير من الأرباح المالية.

٣. الخبرة في مجال الأمن السيبراني ستكون غاية لكل مؤسسة مميزة.

٤. يشمل الأمن السيبراني كافة المجالات العملية بالرغم من اختلافها وتنوعها.

٥. تمكين الدارس من الحصول علي امتيازات فريدة في العمل.

ثانياً : أنواع الجرائم السيبرانية

تتعدد جرائم الأمن السيبراني ، من أهم هذه الجرائم: (<https://www.mah6at.net>)، (2018)

جرائم التعدي على البيانات المعلوماتية ، التعدي على الأنظمة المعلوماتية، إساءة استعمال الأجهزة أو البرامج

المعلوماتية، الجرائم الواقعة على الأموال، الاستغلال الجنسي للقاصرات، التعدي على الملكية الفكرية للأعمال

الرقمية، البطاقات المصرفية والنقود الإلكترونية، جرائم تمس المعلومات الشخصية، جرائم العنصرية والجرائم

ضد الإنسانية بوسائل معلوماتية، جرائم المقاومة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت، الجرائم المعلوماتية ضد الدولة والسلامة العامة، وجرائم تشفير المعلومات .

أسباب الجرائم السيبرانية

- الرغبة في جمع المعلومات وتعلمها.
- الاستيلاء على المعلومات والاتجار فيها.
- قهر النظام وإثبات التفوق على تطور وسائل التقنية.
- الحاق الأذى بأشخاص أو جهات.
- تحقيق أرباح ومكاسب مادية.
- تهديد الأمن القومي والعسكري.

أسباب تؤكد علي أهمية دراسة الأمن السيبراني:

أنماط الأمن السيبراني:

ينطبق هذا المصطلح على مجموعة متنوعة من السياقات، بدءاً من قطاع الأعمال، وصولاً إلى الحوسبة المتنقلة، وبالإمكان عموماً تقسيمها إلى عدة فئات شائعة كما يلي: (بوغرارة، 2018)

أمن الشبكات : هو ممارسة تأمين شبكة الكمبيوتر من العناصر المتطفلة والانتهازية، سواء المهاجمين المستهدفين، أو البرامج الضارة.

أمان التطبيقات : يركز على الحفاظ على البرامج والأجهزة خالية من التهديدات، إذ يمكن أن يوفر التطبيق المخترق الوصول إلى البيانات المصممة للحماية، وإن تطبيق مفهوم الأمان الناجح يبدأ في مرحلة التصميم الأولي قبل نشر البرنامج أو الجهاز.

المبحث الثاني : فاعلية الأنظمة التقنية (التشغيلية)

مقدمة

تتطور تكنولوجيا المعلومات بسرعة فائقة، وتستفيد منها المؤسسات بكافة أنواعها لتشكل لها سلاحا قويا للتميز عن منافسيها. وتعتبر نظم الأمن السيبراني أحد أهم الوسائل التكنولوجية التي تستخدمها المؤسسات لإدارة أنظمتها إدارة محكمة.

إن النظم التقنية هي عصب المؤسسات وعنصر أساسي لاستمرارها، لذا فإن المؤسسات بحاجة للتأكد من أن أنظمتها تناسب داخلها أو خارجها بشكل جيد وكفؤ، وللقيام بذلك فإن المؤسسات بحاجة لأنواع وتصنيفات مختلفة من وسائل الأمن السيبراني التي تساهم في المحافظة على النظم التقنية واجراء العمليات المختلفة عليها. ومن أهمها نظم الأمن السيبراني والتي تشكل أداة ذهبية للمؤسسات في عصرنا الحالي. (عبد ربه، 2013)

يناقش الباحثون في هذا المبحث عدة مفاهيم مرتبطة بنظم الأمن السيبراني وفاعليتها، مثل مفهوم النظام ومكوناته، مفهوم النظم التقنية وأنواعها وبعض المفاهيم المرتبطة بها مثل: عناصرها، مواردها، أهدافها، وظائفها، وخصائصها. بالإضافة لذلك، يشير الباحثون إلى الفرق بين الكفاءة والفاعلية، مفهوم فاعلية النظم التقنية، وكيفية قياس هذه الفاعلية.

أولاً : مفهوم النظام

يتكرر استخدام كلمة النظام (System) في حياتنا في مجالات مختلفة، وفيما يلي عرض الباحثون مفهوم النظام قبل الخوض في مفهوم نظم المعلومات الإدارية ليتضح المقصود بمصطلح النظام.

تستخدم كلمة النظام في العديد من المجالات وعلى نطاق واسع وذلك بحسب العلوم التي تستخدمها، مثل "النظام الاقتصادي"، "النظام السياسي"، "نظام المعلومات"، أو غيرها من المصطلحات، وفي كل المصطلحات السابقة فإن كلمة النظام تعني خواصاً مشتركة وأحد هذه الخواص يقصد بها مجموعة الترتيبات أو العناصر أو الأجزاء (الشorman، 2004).

التعريف الإجرائي (النظام) : هو مجموعة من العناصر المترابطة وذات العلاقة فيما بينها، تعمل مع بعضها البعض لتحقيق أهداف محددة.

ثانياً: مكونات النظام

بناء على التعريفات السابقة لمفهوم النظام، فقد اتضح للباحثين أن النظام هو عبارة عن مجموعة من العناصر، فإنه لا بد من الإشارة إلى هذه العناصر التي يتكون منها النظام.

يتكون النظام من عدة أجزاء رئيسية، صنفها (الشorman، 2004) إلى أربعة عناصر، وهي كالتالي:

1. المدخلات (Inputs) : تتكون من البيانات التي تخدم عملية المعالجة، وهي المادة الأولية (موارد مادية أو بشرية) التي تعمل على بدء خطوات عملية المعالجة.

2 . العمليات (Processes) : وهي النشاطات التي تحول المواد الأولية (المدخلات) لمعلومات مفيدة لتحقيق أهداف النظام.

3 . المخرجات (Outputs) : وهي نتائج تفاعل مكونات النظام الناتجة من عملية المعالجة.

4 . التغذية الراجعة (Feedback) : ويطلق عليها إعادة التغذية وهي مخرجات خاصة التصميم تستعمل للتحقق من النتائج، والتحكم في جودتها وتقويمها.

الأعمال الإلكترونية هي عبارة عن تكامل وترابط أعمال المنظمة بما في ذلك المنتجات والخدمات والإجراءات من خلال شبكة الانترنت بحيث تستطيع المنظمة إدارة أعمالها التجارية والإدارية.

كما أنها تحقق الربط بين عناصر البيئة الداخلية والخارجية للمنظمة بغض النظر عن التواجد الجغرافي، حيث إن جميع الموظفين والعملاء والمزودين والملاك وغيرهم يمكن ربطهم بإدارة المنظمة من خلال تقنيات الأعمال الإلكترونية بغض النظر عن اتساع حجم المنظمة.

الأعمال الإلكترونية تستند على تقنية شبكة الإنترنت فيما يخص توجيه وتنسيق الأعمال إلكترونياً داخل المنظمة، وعلى شبكة الإنترنت في مجالات رئيسية محددة أهمها إدارة سلسلة التوريد وخلق نوع من التنسيق بين المنظمة والمستفيدين في الخارج، وتخطيط موارد المنظمة، بحيث يتم إتاحة واستخدام الشبكة العنكبوتية لغرض تحسين أداء منظمات الأعمال القائمة أو إنشاء منظمات افتراضية جديدة.

مفهوم الأعمال الإلكترونية مفهوم واسع يتعدى حدود البيع والشراء عبر الإنترنت وكذلك يتعدى حدود أنشطة البيئة الداخلية للمنشأة من مخزون وإنتاج وموارد بشرية ومحاسبة ليشمل الأنشطة مع البيئة الخارجية مثل العلاقة مع الموردين والعلاقة مع العملاء بالإضافة إلى العلاقة مع المنافسين.

ثالثاً : الفوائد التي تحققها الأعمال الإلكترونية للمنظمات

تعد تقنيات الأعمال الإلكترونية واحدة من الفرص الهامة التي وفرتها تقنية الحوسبة للمنظمات في السنوات الأخيرة، حيث مكنت المنظمات لتصبح أكثر كفاءة وذلك من خلال توفير المزايا والفوائد الآتية: (ابوزيد، 2019)

1. تحسين العلاقة مع شركاء العمل : توافر تقنيات الأعمال الإلكترونية إمكانية الاتصال بالعملاء والمزودين والموظفين وشركاء العمل من خلال شبكة الإنترنت والانترنت والاكسترانت، حيث يساعد هذا الاتصال المباشر المنظمة في الاستجابة السريعة لحاجات العملاء وإقامة علاقة طيبة معهم، وكذلك مع الموردين مما يؤدي إلى تحفيز الموردين للوفاء بالتزاماتهم تجاه المنظمة وتوريد طلباتها في أسرع وقت، وهذا يقلل من كلفة المخزون .

2. تحقيق الميزة التنافسية : حيث تسمح تقنيات الأعمال الإلكترونية بالتشارك في المعلومات بين المنظمات وشركاء العمل من مزودين وبائعين، وتساعد هذه التقنيات في تخطيط وإدارة عمليات الطلب والعرض، كما أنها تسمح للمنظمات بإدارة أعمالها في أي وقت ومن أي مكان، حيث يمكن الاتصال بالبائعين عبر الويب بغض النظر عن موقعهم الجغرافي.

3. توفير أداة إدارية قوية لإدارة سلاسل التوريد : فهي تساعد في تقديم أفضل خدمة للعميل، كما أنها تساعد في خفض كلف الإنتاج والتوزيع للسلع والخدمات .

4. تحقيق التكاملية بين نظم المعلومات: من أهم الفوائد التي تحققها تقنيات الأعمال الإلكترونية الارتباطية والتفاعلية بين نظم المعلومات على مستوى المنظمة الواحدة أو مع المنظمات الأخرى وذلك من خلال تسهيل انسياب البيانات بين أنظمة المعلومات المرتبطة.

5. التغيير التنظيمي وتحسين الإجراءات: نتيجة لتوظيف حلول الأعمال الإلكترونية سوف تقوم إدارة تقنية المعلومات بقيادة التغيير التنظيمي في المنظمة وتغير ثقافتها، وذلك لأن ثقافة الأعمال الإلكترونية تختلف كلياً عن النموذج التقليدي للأعمال، سيتضمن التغيير التنظيمي الذي يرافق توظيف الأعمال الإلكترونية: تحسين عمليات المنظمة، الهيكل التنظيمي، وممارسات العمل، تمكين العاملين، إعادة هندسة إجراءات العمل للتوافق مع نظم المعلومات وغيره. يشمل العمليات والقرارات التي تتعامل مع أصول البيانات، وتكفل حمايتها.

رابعاً: عناصر الأمن السيبراني

حتى يتحقق الهدف من الأمن السيبراني، لا بد من توفر مجموعة من العناصر مع بعضها البعض لتكمل الدور في ذلك، ومن أهم أبعاد وعناصر الأمن السيبراني: (بوغرارة، 2018)

- التقنية: تشكل التكنولوجيا والتقنية دوراً في غاية الأهمية في حياة الأفراد والمنظمات، حيث توفر الحماية الفائقة لهم أمام الهجمات السيبرانية، وتشتمل حماية الأجهزة بمختلف أشكالها الذكية والحاسوبية والشبكات بالاعتماد على جدران الحماية واستخدام البرامج الضارة ومكافحة الفيروسات وغيرها.

- الأشخاص: يستوجب الأمر لزوماً على الأشخاص من مستخدمي البيانات والأنظمة في منشأة ما استخدام مبادئ حماية البيانات الرئيسية كتحديد كلمة مرور قوية، وتفادي فتح الروابط الخارجية والمرفقات عبر البريد الإلكتروني، إلى جانب القيام بعمل نسخ احتياطية للبيانات.

- الأنشطة والعمليات: يتم توظيف الأشخاص والتقنيات للقيام بالعديد من العمليات والأنشطة وتسييرها بما يتماشى مع تطبيق أسس الأمن السيبراني والتصدي لهجماته بكل كفاءة.

العاملون في نظم المعلومات:

إن نجاح نظم المعلومات الإدارية يعتمد بشكل كبير على مهارات العاملين القائمين على إدارة وتشغيل هذه النظم. ويجب توافر الأنواع التالية من العاملين عند اعتماد تطبيق نظم المعلومات الإدارية (تعليق، 2011، صفحة 33).

- مديري نظم المعلومات: يعتبر مسئولاً عن إدارة نظم المعلومات بالمؤسسة، وضمان صحة واكتمال هذه النظم.
2. مديري قواعد البيانات: يعتبر مسئولاً عن تصميم وضبط قاعدة البيانات الخاصة بالمؤسسة.
3. محلل النظم: يشكل حلقة الوصل بين المبرمجين وباقي أجزاء المنظمة، حيث يعمل على ترجمة المشكلات والمتطلبات الفنية والإدارية إلى متطلبات برمجية ونظم معلومات.
4. مصمم النظم: تعتبر وظيفته مكملة لوظيفة محلل النظم، حيث أنه يضع الوصف التفصيلي لمواصفات النظام، ويقوم بإدارة ومراقبة التنفيذ الفني للنظام.
5. المبرمج: وهو الشخص الذي تكون مهمته الأساسية كتابة البرمجيات.

المبحث الثالث : الأنظمة التقنية في القطاع الصحي

لا تختلف طبيعة الأعمال الإلكترونية في المنظمات الصحية، عن مثيلتها في منظمات الأعمال الأخرى، حيث إن الوظائف والعمليات الإدارية التي تقوم بها منظمات الأعمال نجدها في المنظمات الصحية، كما أن المنظمات الصحية تأثر كثيراً بالتطورات الحاصلة في الفكر الإداري الحديث مثل مبادرات تطبيق الجودة الشاملة وتحسين الخدمات المقدمة للعملاء، والتوجه نحو الزبون، والتسويق بالعلاقات وغيرها، فهي تسعى لتوظيف هذه المبادرات بالشكل الذي يحقق لها الكفاءة والفعالية في الأداء وبالتالي تحقيق أهدافها الإستراتيجية.

ومن ناحية أخرى، نجد أن المنظمات الصحية سواء كانت في القطاع العام أو في القطاع الخاص، تعمل في بيئة تنافسية قوية وسريعة التطور، تفرض عليها تحقيق التوافق بين إمكانياتها وقدراتها وبين ما تفرضه هذه البيئة من تغيرات خاصة في احتياجات الزبائن (المرضى) من الخدمات الصحية، مما يجعلها تواجه الكثير من التحديات من أجل تحقيق التميز التنافسي، ومن بين هذه التحديات الاستثمار في تقنية المعلومات كمدخل لتحسين الخدمات المقدمة وتحسين عمليات المنظمة ووظائفها المختلفة، وكذلك تسعى هذه المنظمات من خلال توظيف تطبيقات تقنية المعلومات والاتصالات إلى خفض تكاليف الإنتاج وزيادة الربحية بالنسبة لمنظمات القطاع الخاص (شلوش، 2018).

لذلك ينبغي على هذه المنظمات الاستفادة من حلول الأعمال الإلكترونية بالشكل الذي يخدم كل أنشطتها الفنية والإدارية، بما يضمن للمؤسسة الطبية الاستغلال الأمثل لمواردها، وتحسين عملياتها، ولا يعتمد نجاح هذه التقنيات على الاختيار الدقيق للمعدات والبرمجيات الخاصة بتخزين ومعالجة واستعادة المعلومات فحسب، وإنما يعتمد نجاحها بشكل أكبر على مدى ملائمتها لمختلف المستخدمين مقدمي خدمات الرعاية الصحية من أطباء وتمريض وفنيين وكذلك الإداريين، حيث تختلف رؤية وأولويات كل فئة من هذه الفئات وتختلف احتياجاتهم للمعلومات وكيفية الاستفادة كل منهم من هذه التقنيات.

ومن الفوائد التي تعود على المنظمات الصحية جراء توظيف حلول الأعمال الإلكترونية، إمكانية الوصول إلى المزودين بغض النظر عن أماكن تواجدهم، خفض تكاليف التوريد وتكاليف المخزون، تحسين العمليات وتوفير طرق جديدة لأداء العمل، وتحقيق المزايا التنافسية، بالإضافة إلى تقليل الأخطاء الطبية. كما أنها تواجه بعض التحديات مثل تلك المتعلقة بالمسائل الأمنية والقانونية، وعدم توفر مزودي خدمات تقنية المعلومات والاتصالات المناسبين، وكذلك عدم توافقية التقنيات المتوفرة مع احتياجات المستشفى، بالإضافة إلى ارتفاع تكلفة توظيف تقنيات الأعمال الإلكترونية.

تقنيات الأعمال الإلكترونية في المنظمات الصحية:

كشفت العديد من الدراسات عن تقنيات الأعمال الإلكترونية التي تتبناها المنظمات الصحية في الدول المتقدمة بغض النظر عن حجم تلك المنظمات، إجمالاً تتعلق هذه التقنيات بالتعاملات الإلكترونية التي تكون المنظمة طرفاً فيها سواء كانت بين المنظمة الصحية وبين منظمات أعمال أخرى. أو بين المنظمة الصحية والمنظمات الحكومية، أو بين المنظمة الصحية وموظفيها، وهذا يعني تنفيذ حجم كبير من الأنشطة المتعلقة بالسلع والخدمات إلكترونياً عبر الويب.

ومن أهم التقنيات والنظم التي تحتاجها المنظمات الصحية لتبني الأعمال الإلكترونية ما يأتي:

(النوايسة والعدوان، 2019)

1. البنية التحتية للاتصال: واحدة من تقنيات الأعمال الإلكترونية التي توفرها المنظمات الصحية لتمكين العاملين من تبادل المعلومات والاستفادة من خدمات أنظمة المعلومات الموزعة والمشاركة في الموارد المتاحة وذلك من خلال توفير الشبكات الحاسوبية المحلية الواسعة، كما تقوم المنظمة الصحية بتوفير خدمات الاتصال

بالإنترنت لجميع العاملين الإداريين والفنيين لتمكينهم من الاستفادة من هذه التقنية لخدمة أغراض العمل، بالإضافة إلى ذلك فإن امتلاك المنظمة الصحية لموقع الكتروني على الويب يعد من متطلبات تبني الأعمال الالكترونية فيها خاصة إذا كان هذا الموقع تفاعلي يمكن تنفيذ كثير من المهام الإدارية والفنية من خلاله مثل حجز المواعيد للعملاء (المرضى) وإرسال طلبات الشراء للموردين واستقبال العروض... الخ ، أخيراً تعدت تطبيقات البريد الإلكتروني من الخدمات الهامة التي يجب أن توفرها المنظمات الصحية لغايات توفير الاتصال وتبادل الرسائل بينها وبين المنظمات الأخرى وكذلك بينها وبين العاملين فيها.

2. التقنيات التي تحقق مشاركة البيانات إلكترونياً داخل المنظمة الصحية : حتى تكون المنظمة الصحية جاهزة لتوظيف نظم الأعمال الإلكترونية وتقنياتها المتعددة لابد من بناء وتصميم قواعد بيانات متكاملة حتى تمكن مستخدمي النظام (فنيين وإداريين) من الوصول للملفات والمشاركة في البيانات وتبادلها وذلك بشكل يغطي احتياجات كل منهم ويخدم أداء المهام المكلف بها، إضافة إلى أن هذه التقنيات تحقق للمنظمة الصحية إدارة فعالة للمعرفة من خلال تخزين المعرفة وتبادلها بين الأعضاء.

3. نظم إدارة سلاسل التوريد :على الحاسب وتطبيقاته الشبكية لغرض الربط بين أعضاء سلسلة التوريد من أجل تسهيل تدفق المواد والمعلومات بينهم، حيث تقوم المنظمات الصحية بتوظيف هذه النظم لغايات ضمان توريد الأدوية والمستلزمات الطبية بكفاءة عالية تضمن حسن الأداء وخفض تكاليف التوريد والتخزين، بالإضافة إلى المحافظة على سلامة المواد الطبية وبالاتي تقليل الأخطاء الطبية الناتجة عن سوء حفظ هذه المواد واستخدامها.

4. نظم تخطيط موارد المنشأة:

نظام متكامل لإدارة المنشآت يتكون من مجموعة منظومات مالية وإدارية وإنتاجية مترابطة تعمل على قاعدة بيانات موحدة، توفر أفضل حلول إدارة أعمال المنشآت لتقديم رؤية دقيقة للأعمال وتفعيل التطور والابتكار، حيث يتم توحيد جميع عمليات الأعمال في بيئة نظام موحد مبنية على قاعدة بيانات مركزية.

تشكل نظم تخطيط الموارد محورا رئيسيا لتطوير وحوسبة إجراءات العمل لأي منشأة، إذ أنها تمكن من الاستثمار الأمثل للموارد و بشكل فاعل، لذلك تشتمل تقنيات الأعمال الإلكترونية في المنظمات الصحية على النظم الفرعية لتخطيط الموارد والتي تركز على الموارد المالية والبشرية وإدارة المواد والمستلزمات الطبية. حيث تتكامل هذه النظم لتمكين المؤسسات الصحية من الاستثمار الأمثل لمواردها.

5. نظم إدارة العلاقة مع العملاء: يمكن النظر إلى إدارة على أنها إستراتيجية شاملة (CRM) العلاقة مع العملاء ونظام متكامل لتحديد العملاء الإيجابيين أكثر من غيرهم، لتحرص المنظمة على إدامة التواصل معهم لإقامة علاقة طيبة معهم، وانطلاقاً من هذا التصور يمكن تعريف نظم إدارة العلاقة مع العملاء بأنها واحداً من أهم حلول الأعمال الإلكترونية التي تتيح متابعة نشاطات البيع والتسويق والعلاقات العامة بحيث يعمل في الدرجة الأولى على جعل العميل محور الاهتمام الأساسي فيساعد على تكوين قاعدة بيانات متكاملة تستطيع عن طريقه المنظمة إنجاز كافة الأعمال المرتبطة بعملائها كالمتابعة وفتح الحسابات للعملاء وحفظ كافة الأحداث التي تتم بشكل يومي وإصدار التقارير وترتيب الأعمال ومعاينة كفاءة أداء الموظفين في التعامل مع العميل، وإدامة العلاقة الطيبة مع العميل.

تبني المنظمة الصحية لنظم (CRM) فعالة يجعلها قادرة على إدارة رضا العملاء (المرضى)، كما أن تمكّنها من جمع كافة المعلومات المتعلقة بالمرضى وإدارة هذه المعلومات بالشكل الذي يساعد في اكتشاف المعرفة من خلالها، حيث تحدد هذه المعرفة حاجات العملاء ورغباتهم، بالإضافة إلى توفير إمكانية التفاعل المباشر مع المرضى وتقديم الخدمات لهم والإجابة على استفساراتهم ومعالجة شكاوهم وتنظيم عملية تقديم الخدمات لهم.

6. نظم المعلومات الصحية: إضافة إلى ما سبق تهتم المنظمة الصحية بتوظيف نظم لإدارة ومتابعة الأنشطة الطبية فيها، وتعد هذه النظام من ضمن تقنيات الأعمال الإلكترونية التي تتبناها المنظمات الصحية، تعنى نظم المعلومات الصحية بتوفير مختلف الخدمات الإدارية والعلاجية للمرضى والأطباء والإدارات ذات العلاقة، وتوفر هذه النظم إدارة فعالة لبيانات ومعلومات المرضى خلال فترة علاجهم حيث تمكن الأطباء وباقي أقسام المستشفى من الوصول إلى المعلومات الطبية والبيانات الضرورية والتعامل معها بكفاءة عالية مع المحافظة على أمنها وسريتها، ومن أهم النظم الفرعية في النظام المتكامل لإدارة المعلومات الصحية، نظام معلومات المختبر ونظام معلومات الأشعة، نظام معلومات الصيدلية، و نظام إدارة السجلات الطبية وغيرها .

التحديات التي تواجه تبني تقنيات الأعمال الإلكترونية في المنظمات:

أشارت بعض الدراسات إلى بروز بعض المخاوف جراء توظيف تقنيات الأعمال الإلكترونية في المنظمات ومن أهمها : (جبور، 2016)

1. **المسائل الأمنية:** حيث تعد من محددات تبادل البيانات إلكترونياً، خاصة إذا كانت قيمة هذه البيانات مرتفعة مثل بيانات الزبائن المتعلقة ببطاقات الائتمان والحسابات البنكية وغيرها، وهذا يتطلب اتخاذ تدابير أمنية مناسبة تضمن المحافظة على سرية البيانات واحترام خصوصية المتعاملين والمحافظة على حقوقهم.

2. **كلفة تقنيات الأعمال الإلكترونية :**

تبقى مسألة الكلفة التي تتحملها المنظمات جراء توظيف حلول الأعمال الإلكترونية مصدر قلق لتلك المنظمات وملاكها، خاصة إذا كانت العوائد التي تترتب على توظيف هذه الحلول غير واضحة بالنسبة لهم، وهذا يتوقف على قدرة المنظمة في تحقيق التطبيق الناجح لتلك الحلول وتوفير عوامل النجاح والتقليل من العقبات وعوامل الفشل التي تواجه تطوير نظم الأعمال الإلكترونية، بحيث تتحول الكلف المترتبة على توظيف هذه النظم إلى استثمار طويل الأجل سوف يحقق الكثير من العوائد من خلال خفض كلف الإنتاج والتوزيع وزيادة الحصّة السوقية وزيادة الربحية.

3. **ضعف البنية التحتية للاتصالات والشبكات:**

أن تقنيات الأعمال الإلكترونية تحتاج لشبكة انترنت ذات موثوقية وكفاءة عالية وذلك لضخامة التعاملات الإلكترونية التي تتم في بيئة الأعمال الإلكترونية، لذلك فإن أي ضعف أو فشل في كفاءة شبكة الاتصال سواء المحلية أو شبكة

الانترنت سوف يؤدي إلى تعطيل الأعمال وبالتالي زيادة التكاليف بدلاً من خفضها، لذلك لابد من الانتباه إلى مسألة كفاءة شبكة الاتصال خاصة فيما يتعلق بالحدثة وعرض النطاق وأخذها بعين الاعتبار عند تبني تقنيات الأعمال الإلكترونية بشكل يضمن التوافق والموثوقية (الشيتي، 2019).

4. **الأعمال الإلكترونية في المنظمات الصحية:**

لا تختلف طبيعة الأعمال الإلكترونية في المنظمات الصحية، عن مثيلتها في منظمات الأعمال الأخرى، حيث إن الوظائف والعمليات الإدارية التي تقوم بها منظمات الأعمال نجدها في المنظمات الصحية، كما أن المنظمات الصحية تأثرت كثيراً بالتطورات الحاصلة في الفكر الإداري الحديث مثل مبادرات تطبيق الجودة الشاملة وتحسين الخدمات المقدمة للعملاء، والتوجه نحو الزبون، والتسويق بالعلاقات وغيرها، فهي تسعى لتوظيف هذه المبادرات بالشكل الذي يحقق لها الكفاءة والفعالية في الأداء وبالتالي تحقيق أهدافها الاستراتيجية.

ومن ناحية أخرى، نجد أن المنظمات الصحية سواء كانت في القطاع العام أو في القطاع الخاص، تعمل في بيئة تنافسية قوية وسريعة التطور، تفرض عليها تحقيق التوافق بين إمكانياتها وقدراتها وبين ما تفرضه هذه البيئة من تغيرات خاصة في احتياجات الزبائن (المرضى) من الخدمات الصحية، مما يجعلها تواجه الكثير من التحديات من أجل تحقيق التميز التنافسي، ومن بين هذه التحديات الاستثمار في تقنية المعلومات كمدخل لتحسين الخدمات المقدمة وتحسين عمليات المنظمة ووظائفها المختلفة، وكذلك تسعى هذه المنظمات من خلال توظيف تطبيقات تقنية المعلومات والاتصالات إلى خفض تكاليف الإنتاج وزيادة الربحية بالنسبة لمنظمات القطاع الخاص (النوايسة والعدوان، 2019).

لذلك ينبغي على هذه المنظمات الاستفادة من حلول الأعمال الإلكترونية بالشكل الذي يخدم كل أنشطتها الفنية والإدارية، بما يضمن للمؤسسة الطبية الاستغلال الأمثل لمواردها، وتحسين عملياتها، ولا يعتمد نجاح هذه التقنيات على الاختيار الدقيق للمعدات والبرمجيات الخاصة بتخزين ومعالجة واستعادة المعلومات فحسب، وإنما يعتمد نجاحها بشكل أكبر على مدى ملائمتها لمختلف المستخدمين مقدمي خدمات الرعاية الصحية من أطباء وتمريض وفنيين وكذلك الإداريين، حيث تختلف رؤية وأولويات كل فئة من هذه الفئات وتختلف احتياجاتهم للمعلومات وكيفية الاستفادة كل منهم من هذه التقنيات (الشيخي، 2019).

كما أنها تواجه بعض التحديات مثل تلك المتعلقة بالمسائل الأمنية والقانونية، وعدم توفر مزودي خدمات تقنية المعلومات والاتصالات المناسبين، وكذلك عدم توافقية التقنيات المتوفرة مع احتياجات المستشفى، بالإضافة إلى ارتفاع تكلفة توظيف تقنيات الأعمال الإلكترونية.

الفصل الثالث

الدراسات السابقة

أولاً: الدراسات التي تناولت الأمن السيبراني والأنظمة التقنية.

ثانياً: التعليق على الدراسات السابقة

ثالثاً: ملخص الفصل الثالث.

مقدمة

يوجد العديد من الدراسات التي تناولت موضوع الأمن السيبراني وسياساته، وكذلك النظم التقنية وفعاليتها. اختلفت هذه الدراسات في عدة جوانب منها: أبعاد الدراسة، مجتمع الدراسة، أدوات الدراسة، وغير ذلك من الاختلافات التي ميزت هذه الدراسات عن بعضها البعض. اطلع الباحثون على العديد من الدراسات السابقة باللغتين العربية والإنجليزية ذات الصلة بموضوع البحث، وذلك من خلال زيارتهم للمكتبات، وبحثهم في المواقع الإلكترونية وقواعد البيانات البحثية المختلفة، وقد انتقى الباحثون عددا من هذه الدراسات والتي رأوا أنها الأقرب لموضوع البحث، وذلك من خلال ارتباطها مع متغيرات البحث، سواء المتغير المستقل (سياسات إطار أمن المعلومات السيبراني) أو المتغير التابع (فاعلية الأنظمة التقنية الصحية) أو كلاهما.

1. الدراسات السابقة المحلية

أ. دراسة (الغثير و الصبيح، 2012)

حال أمن المعلومات السيبراني في المملكة العربية السعودية

هدفت هذه الدراسة إلى معرفة حال أمن المعلومات في المملكة العربية السعودية، استهدفت الدراسة مديري تقنية وأمن المعلومات في المنظمات السعودية خلال ورشة عمل خاصة في عام 2011. ركزت الدراسة على عدة مجالات وهي: الوصول إلى الشبكة، سياسات أمن المعلومات ومعاييرها، إدارة المخاطر، الوعي الأمني، ومخاوف ومشاكل أمن المعلومات والهجمات الفعلية. ومن أهم النتائج التي توصلت إليها الدراسة أن ثلاثة أرباع المنظمات المشاركة تمتلك سياسات لأمن المعلومات، وأن النسبة الأعلى لذلك كانت من نصيب القطاع العسكري، يليه القطاع الحكومي، وأخيراً القطاع الخاص. كما أشارت الدراسة إلى وجود اهتمام بمراجعة وتحديث السياسات الأمنية لديها، بينما أشارت لوجود ضعف في كل من عمليات تقييم المخاطر والثغرات الأمنية، عمليات التدريب والتوعية في أمن المعلومات، وعملية تطبيق معايير أمن المعلومات. كما وتوصلت النتائج إلى أن أعلى خمسة مخاوف في أمن المعلومات داخل المنظمات السعودية من الأعلى للأقل هي كالتالي:

عدم الالتزام بمعايير أمن المعلومات في المنظمة، قلة وجود العاملين المتخصصين في أمن المعلومات، نقص الممارسات العملية الكافية لحماية البيانات، غياب الممارسات الجيدة في اختيار كلمة السر، قلة الدعم المالي المخصص لأمن المعلومات.

ب. دراسة (نبي، عرفان، و مرزا، 2010)

دراسة عملية حول أمن المعلومات السيبراني في المنظمات السعودية

هدفت الدراسة إلى استكشاف حالة أمن المعلومات السيبراني والعمل على تحقيق فهم أفضل للحقائق السائدة في هذا المجال داخل المملكة العربية السعودية. تمت الدراسة على مجموعة من المنظمات في أربع قطاعات رئيسية (القطاع الخاص، قطاع البنوك والمصارف، قطاع الدفاع، القطاع الحكومي). وتوصلت الدراسة إلى أهمية سياسة أمن المعلومات في ضمان اتخاذ عوامل تحكم مناسبة، وبينت الدراسة أن أكثر من نصف المنظمات تمتلك سياسة أمن المعلومات وغالبيتها تميل إلى تطبيقها، ومنهم من تعتمد لمراجعة دورية لتلك السياسة. وحاز قطاع الدفاع على الأعلى في امتلاك سياسة أمن معلومات، بينما كان القطاع الحكومي الأقل امتلاكاً لها.

ج. دراسة (الشيتي، 2019)

حول تقييم سياسات أمن وخصوصية المعلومات في مؤسسات التعليم بالمملكة العربية السعودية، مع التطبيق علي جامعة القصيم .

توصلت الدراسة الي ضرورة وجود برامج توعية الموظفين وتشجيع البحوث في مجال الأمن السيبراني وأهمية تكامل وصحة البيانات في مؤسسات التعليم.

د. دراسة (العتيبي، 2017)

حول دور الأمن السيبراني في تعزيز الأمن الإنساني :

تمثلت مشكلة الدراسة في محاولة الاجابة عن سؤال رئيس : ما دورالأمن السيبراني في تعزيزالأمن الانساني ؟ تكون مجتمع الدراسة من العاملين في مجال الأمن السيبراني في شركة أرامكو السعودية فرع منطقة الرياض . عينة الدراسة (٤٠٠) فرد تم اختيارهم عشوائيا ، استخدمت الدراسة المنهج الوصفي التحليلي طبقت استبانة لجمع المعلومات من عينة الدراسة .

ومن أهم نتائج الدراسة :

- أن الإجراءات الفنية لحماية الفضاء السيبراني للشركة متوفرة بدرجة كبيرة، حيث يتم قفل النظام آلياً في حالة عدم استخدامه لفترة زمنية محددة.

- أن الإجراءات التقنية لحماية الفضاء السيبراني الخاص بالشركة متوفرة بدرجة كبيرة، استخدام القياسات الحيوية (بصمة العين - بصمة الإصبع - بصمة الصوت) لمرور المصرح لهم .

أوصي الباحث بضرورة العمل على اتباع الوسائل العلمية والعملية لحفظ الأمن السيبراني للمؤسسات والشركات الحكومية والخاصة ، كما أوصي بالمزيد من التعمق في دراسة الربط ما بين مجال الأمن السيبراني والأمن الإنساني.

2. الدراسات السابقة العربية

أ. دراسة (القرشي، 2011)

قياس كفاءة سياسات أمن المعلومات. دراسة حالة على شركة الإمارات العربية المتحدة

هدفت الدراسة إلى تحليل كيفية قياس كفاءة سياسات أمن المعلومات المطبقة في الشركة، والبحث عن اقتراح الطريقة المناسبة لقياس كفاءة هذه السياسات في الشركة. استخدم الباحث معيار ISO27004 لتوضيح كيفية قياس كفاءة سياسات أمن المعلومات. أوضحت نتائج الدراسة بأنه لا يوجد طريقة منهجية رسمية لقياس كفاءة سياسات أمن المعلومات في الشركة المجرى عليها الدراسة. وأشارت نتائج الدراسة بعدم وجود رضا تام من الموظفين تجاه تدريبهم على أمن المعلومات في الشركة. ومن المعايير التي استخدمها الباحث لقياس المخاطر التي تؤدي لقلّة كفاءة سياسات أمن المعلومات، قلّة الوعي بأمن المعلومات، ضعف برامج التدريب والتوعية، ووجود الاختراق والهجوم عن طريق الفيروسات بأنواعها المختلفة.

ب. (دراسة المعهد العربي للتخطيط "مخاطر الهجمات الالكترونية (السيبرانية) وآثارها الاقتصادية، 2019):

دراسة حالة دول مجلس التعاون الخليجي حاولت هذه الدراسة تسليط الضوء على أهمية المخاطر الالكترونية وآثارها الاقتصادية وكيفية إدارتها، وأعطت نماذج دولية لحوادث الإصا بة بها. ثم حللت وقيمت أوضاع دول مجلس التعاون الخليجي كنموذج أو دراسة حالة . وهدفت من ذلك الى زيادة الاهتمام بالاستثمار في الأمن

الإلكتروني واستدراك الثغرات في التخطيط الاقتصادي لمواجهة هذه المخاطر، وتتصدر دول مجلس التعاون الخليجي دول العالم الأخرى في بعض أنواع الهجمات السيبرانية على الأنشطة الاقتصادية مثل معدلات البرمجيات الخبيثة بالبريد الإلكتروني ونسب البريد الإلكتروني كما تفوق الخسائر الناجمة عن الهجمات الإلكترونية في دول المجلس المتوسط (Spam). المؤذي العالمي . وعلى الرغم من تحسن أداء دول المجلس في مجال مواجهة الهجمات الإلكترونية، إلا أن الدليل الع المي للأمن السيبراني الذي تصدره الأمم المتحدة يشير إلى وجود العديد من الثغرات القانونية والفنية والتنظيمية والتدريبية والتعاونية التي يجب سدها من خلال تحسين الأداء والإكمال والمراجعة للوضع الراهن في هذه الجوانب . ولا تكفي زيادة الإنفاق بمفردها في مواجهة التهديدات وتحقيق الأمن السيبراني في دول المجلس، بل لابد من تحسين الوعي والحوكمة والعمليات لأن هذه المنطقة هي إحدى أكثر مناطق العالم تقدماً في سرعة تبني واعتماد التكنولوجيا الحديثة .

3- الدراسات السابقة الأجنبية

أ. دراسة (Hadjor & Gadasu, 2014)

- The Influence of Organizational Culture on Information Security Policy Success. -

هدفت الدراسة إلى توضيح دور الثقافة التنظيمية في نجاح تطبيق سياسات أمن المعلومات. تكمن فكرة البحث في اكتشاف كيف يمكن أن تساعد خصائص الثقافة التنظيمية بالتأثير بشكل إيجابي على الأفراد، مما يؤثر بشكل إيجابي على نجاح سياسات أمن المعلومات. وتوصلت الدراسة إلى وجود دور ضروري للثقافة التنظيمية في نجاح سياسات أمن المعلومات، وأن تحقيق أمن المعلومات يتم من خلال التطبيق الناجح لسياسات أمن المعلومات، بوجود دور مباشر للثقافة التنظيمية.

دراسة (Knapp, 2012)

Policy Awareness, Enforcement and Maintenance: Critical to Information Security

Effectiveness in Organizations.

هدفت الدراسة لدراسة أثر الأبعاد الثلاثة لسياسات أمن المعلومات (التوعية، فرض التنفيذ، المراجعة والتحديث) على فاعلية برنامج أمن المعلومات. وتوصلت النتائج إلى أن الأبعاد الثلاثة السابقة لها تأثير على فاعلية

برنامج أمن المعلومات، مع أهمية اعتبار هذه الأبعاد هي الممثل لإدارة سياسات أمن المعلومات. وأشارت الدراسة إلى أن التوعية بسياسات أمن المعلومات لها التأثير الأكبر على فاعلية البرنامج، ويلمها فرض التنفيذ، بينما ذكرت نتائج الدراسة أن المراجعة والتحديث لها التأثير الأقل، ولكن لها أهمية إحصائية.

التعليق على الدراسات السابقة:

اتضح للباحثين من خلال عرضهم للدراسات السابقة وجود اهتمام كبير وتوجهات إيجابية نحو موضوعي سياسات أمن المعلومات السيبراني ونظم المعلومات التقنية. وفيما يلي أوجه الفائدة من الدراسات السابقة، وأوجه الاتفاق والاختلاف فيها، كما تشير إلى مدى تميز هذا البحث عن غيره من الدراسات السابقة.

1. أوجه الاستفادة من الدراسات السابقة

لقد تحقق للباحثين جملة من الفوائد من خلال اطلاعهم على الدراسات السابقة، حيث ساعدت الدراسات السابقة

السابقة

الباحثين فيما يلي:

أ. تحديد مشكلة البحث، وأسئلة البحث.

ب. تحديد متغيرات البحث.

ج. صياغة فرضيات البحث وأهدافه.

د. تحديد مجتمع البحث.

هـ. اختيار منهجية البحث، أدواته، والأساليب الإحصائية.

و. بناء الإطار النظري للبحث.

ز. صياغة فقرات الاستبانة.

2. أوجه الاختلاف والاتفاق بين الدراسات السابقة:

أ. الدراسات المتعلقة بأمن المعلومات وسياسات الأمن السيبراني :

- عدد من الدراسات المحلية والعربية أظهرت أهمية موضوع الأمن التقني ومخاطر الأمن السيبراني مثل دراسات (

(الغثبر و الصبيح، 2012) ودراسة (نبي، عرفان، و مرزا، 2010))، وكذلك بعض الدراسات الأجنبية مثل دراسة

(Hadjor & Gradasu, 2014).

- عدد من الدراسات المحلية والعربية والأجنبية أظهرت أهمية سياسات أمن المعلومات وتأثيرها الإيجابي على حماية المعلومات وأمن نظمها، مثل دراسة (الشيتي، 2019) ودراسة (العتيبي، 2017) (Knapp & Ferrante, 2012).

1. ما يميز هذا البحث عن الدراسات السابقة:

أ. وجد الباحثون أن كافة الدراسات المحلية قد تناولت دراسة أمن المعلومات بشكل عام، وبعضها تطرقت لدراسة سياسات أمن المعلومات كأحد الأبعاد الفرعية في الدراسة، أما في الدراسات الأخرى فإنه يوجد دراسة واحدة درست سياسات أمن المعلومات حيث أنها درست قياس كفاءة سياسات أمن المعلومات في الشركات في الإمارات العربية المتحدة، وباقي الدراسات درست أمن المعلومات ولكن من جوانب أخرى، وبعضها تطرق لسياسات أمن المعلومات كبعد فرعي. وبالرغم من ذلك، فقد اتضح للباحثين وجود اهتمام كبير بموضوع سياسات أمن المعلومات في الدراسات الأجنبية. وبذلك يعتبر الباحثون هذا البحث هو البحث الأول على حد علمهم الذي تناول سياسات الأمن السيبراني في مجال القطاع الصحي، وبالأخص في مستشفيات المملكة العربية السعودية.

ب. إن هذا البحث هو البحث الأول أيضاً على حد علم الباحثين الذي يبحث فاعلية الإطار السيبراني وتأثيره على الأنظمة التقنية في المستشفيات السعودية، ولم تتطرق أي دراسة لقياس فاعلية الأنظمة التقنية في المستشفيات السعودية داخل المملكة.

ج. يتميز هذا البحث أنه البحث الأول على حد علم الباحثون الذي يربط سياسات الأمن السيبراني بفاعلية الأنظمة التقنية في مستشفيات القطاع الصحي داخل المملكة، على الرغم من وجود بعض الدراسات التي ربطت بين موضوعي نظم المعلومات وأمن المعلومات ولكن من جوانب مختلفة.

أوجه الاختلاف والاتفاق بين الدراسات السابقة.

اشتمل مجتمع هذا البحث على العاملين في مراكز ووحدات تقنية المعلومات، بالإضافة للعاملين الذين يستخدمون نظم المعلومات أثناء عملهم اليومي في الأقسام والدوائر الإدارية في المستشفيات الخمسة محل البحث، بينما لاحظ الباحثون أن غالبية الدراسات التي تطرقت لمواضيع تخص أمن المعلومات أو نظم المعلومات يكون مجتمعها فقط العاملين في وحدات ومراكز تكنولوجيا المعلومات.

وقد آثر الباحثون تنوع طبيعة مجتمع البحث بين المستشفيات المختلفة؛ من منطلق التعرف إلى أي فروقات قد تظهر بينهما في نتائج البحث.

ملخص الفصل الثالث

تناول الباحثون في هذا الفصل مجموعة من الدراسات السابقة التي تناولت جوانب هذا البحث بمتغيريه المستقل (سياسات إطار الأمن السيبراني)، والتابع (فاعلية الأنظمة التقنية في القطاع الصحي) حيث استعرض الباحثون في الجزء الأول الدراسات التي تناولت الأمن السيبراني وسياسات أمن المعلومات، وفي الجزء الثاني الدراسات التي تناولت الأنظمة التقنية وفعاليتها، وفي الجزء الثالث قد تناول الباحثون الدراسات التي ربطت بين الأمن السيبراني وسياساته وفاعلية النظم التقنية. كما صنف الباحثون الدراسات في كل جزء من الأجزاء الدراسات لثلاثة تصنيفات (محلية، عربية، أجنبية)، حيث لقي الباحثون قصوراً في الدراسات العربية والمحلية التي تناولت سياسات الأمن السيبراني، كما لقت قصوراً في الدراسات المحلية التي تناولت موضوع فاعلية الأنظمة التقنية وخاصة في القطاع الصحي.

وفي ختام الفصل عقب الباحثون على الدراسات السابقة، حيث أوضحوا أوجه الاستفادة من هذه الدراسات ، وأوجه الاختلاف والاتفاق بينها، كما بينت مدى تميز هذا البحث عن هذه الدراسات . وأكد الباحثون أن هذه الدراسة هي الأولى – على حد علمهم – التي تربط سياسات الأمن السيبراني بفاعلية النظم التقنية في مستشفيات القطاع الصحي داخل المملكة.

الفصل الرابع

منهجية الدراسة

أولاً: منهج البحث

ثانياً : مجتمع البحث

ثالثاً : عينة البحث

رابعاً : خطوات بناء أداة البحث (الاستبانة)

خامساً: مكونات أداة البحث (الاستبانة)

سادساً: صدق وثبات أداة البحث (الاستبانة)

سابعاً: التوزيع الطبيعي لمتغيرات البحث

ثامناً: الأساليب الإحصائية المستخدمة في البحث

تاسعاً: الصعوبات التي واجهت الباحثون

عاشراً : ملخص الفصل الرابع

مقدمة

تعتبر منهجية البحث وإجراءاته محوراً رئيسياً في البحث، حيث أنه يتم من خلالها التركيز على الجانب التطبيقي والحصول على البيانات المطلوبة لإجراء التحليل الإحصائي للتوصل إلى النتائج، وتفسيرها في ضوء الأدبيات المتعلقة بموضوع البحث، وبالتالي تحقيق أهداف البحث.

يستعرض الباحثون في هذا الفصل الإجراءات المنهجية للبحث. وتتمثل هذه الإجراءات في تحديد منهج (أسلوب) البحث، اختيار مجتمع وعينة البحث، إعداد أداة البحث (الاستبانة) وتصحيحها. بالإضافة لدراسة صدق أداة البحث وثباتها، وتحديد أساليب التحليل الإحصائي التي تم الاعتماد عليها في تحليل بيانات البحث.

أولاً : منهج البحث:

اتبعت الدراسة الحالية منهج الوصف التحليلي ، بهدف التعرف على متطلبات تحقيق اطار الأمن السيبراني في القطاع الصحي داخل المملكة العربية السعودية في ضوء رؤية 2030 .

ويعرف (الحمداني، 2006) المنهج الوصفي التحليلي بأنه " المنهج الذي يسعى لوصف الظواهر أو الأحداث المعاصرة، أو الراهنة فهو أحد أشكال التحليل والتفسير المنظم لوصف ظاهرة أو مشكلة، ويقدم بيانات عن خصائص معينة في الواقع، ويتطلب معرفة المشاركين في الدراسة والظواهر التي ندرسها والأوقات التي نستعملها لجمع البيانات."

نظراً لطبيعة الدراسة والأهداف التي تسعى لتحقيقها والمتمثلة في معرفة مدى تبني المستشفيات العاملة في المملكة لسياسات الأمن السيبراني، وما هي التحديات التي تواجهها، وكذلك مقارنة مستويات تبني تلك التقنيات لدى المستشفيات ، لذلك سيتم استخدام الأسلوب الاستطلاعي الكشفي الذي يندرج تحت منهجية البحث الوصفي، حيث إنه مناسب لأجل بلورة بعض الفرضيات، ثم جمع البيانات بواسطة الاستبانة الإحصائية، و تحليلها باستخدام الطرق الإحصائية المناسبة وتفسير النتائج الإحصائية، وبناء عليه يتم اختبار صحة الفرضيات للوصول إلى استنتاجات تخدم أهداف الدراسة.

ثانياً : مجتمع البحث

يتكون مجتمع البحث عينة من العاملين في ادارات/ وحدات تكنولوجيا المعلومات، بالإضافة للعاملين الذين يستخدمون نظم الأمن السيبراني أثناء عملهم اليومي في اقسام تكنولوجيا المعلومات في المستشفيات الخمسة في المملكة (مدينة الملك سعود الطبية - مستشفى الايمان العام - مستشفى الملك سلمان - مستشفى الامام الفيصل - مستشفى الامير محمد بن عبدالعزيز).

جدول رقم (1) : مجتمع البحث، ونسبة التمثيل لكل مستشفى بالنسبة للمجتمع الكلي

المستشفى	مجتمع البحث	نسبة التمثيل /المجتمع الكلي
مستشفى الامام الفيصل	18	30%
مستشفى الامير محمد بن عبدالعزيز	14	23.3%
مستشفى الملك سلمان	13	21.7%
مدينة الملك سعود الطبية	9	15%
مستشفى الايمان العام	6	10%
المجموع	60	100%

لاحظ الباحثون أن مستشفى الامام الفيصل شكلت 30% من مجتمع البحث ، بينما شكلت مستشفى الأمير محمد بن عبد العزيز 23.3% من مجتمع البحث ، في حين أن مستشفى الملك سلمان شكلت 21.7% من عينة البحث ، وشكلت مدينة الملك سعود الطبية 15% من عينة البحث ، ومستشفى الايمان 10% من اجمالي العينة

ولقد أثر الباحثون اختيار المستشفيات الخمسة السابقة، حيث أنها من أهم المراكز الصحية وبها أكبر عدد من المراجعين بالإضافة إلى أنها تمتلك نظم معلومات إدارية متطورة على مستوى مستشفيات المملكة، كما تشمل هيكلتها على وحدة/ مركز تكنولوجيا التقنية أو أقسام الأمن السيبراني.

ثالثاً : عينة البحث

1- العينة (المجال البشري) :

تكون مجتمع الدراسة جميع الموظفين التقنيين في خمس مستشفيات سعودية في محافظة الرياض (مدينة الملك سعود الطبية - مستشفى الايمان العام - مستشفى الملك سلمان - مستشفى الامام الفيصل - مستشفى الامير محمد بن عبدالعزيز) ، أما عينة الدراسة التي اتبعها الباحثون هي العينة العشوائية ، والتي بلغ عددها (60) موظفاً مختصاً في مجال الدراسة .

2- شروط اختيار عينة البحث :

1. تحديد الأشخاص المستهدفين : سيكون الأشخاص المستهدفين في هذه الدراسة هم الأشخاص المعنيين بالمشاريع التقنية الصحية في المملكة العربية السعودية، وذلك من خلال التبادل المسبق للمعلومات مع الأطباء والإدارة والأمن السيبراني والمستخدمين النهائيين.
2. تحديد مجالات الدراسة: ستتضمن مجالات الدراسة مثل الأنظمة التقنية، والأمن السيبراني، والمشروع التقنية الصحية.
3. تحديد مصادر البيانات: سيتم الحصول على المعلومات من عدة مصادر مثل الملفات الإلكترونية، والمقابلات التي تستخدم لجمع البيانات الاستكشافية، والاستبيانات، والمقابلات المحلية.
4. تحديد طريقة جمع البيانات: سيتم استخدام طرق مختلفة لجمع البيانات، مثل المقابلات المباشرة، والمقابلات الإلكترونية ، والاستبيانات.

رابعاً : خطوات بناء أداة البحث (الاستبانة)

أعد الباحثون استبانة لدراسة سياسة أمن المعلومات وعلاقتها بفاعلية نظم المعلومات الإدارية في القطاع الصحي بالمملكة العربية السعودية. كانت استجابة العينة للتفكير دون ضغوط نفسية ، بالإضافة إلى إجراء المقابلة التي اتسمت بالموضوعية العلمية للنتائج.

اتبع الباحثون الخطوات التالية لإعداد الاستبيان بشكله النهائي:

1. الرجوع إلى الدراسات السابقة المتعلقة بموضوع البحث للاستفادة منها عند بناء الاستبيان وصياغة فقراته.
2. إعداد المسودة الأولى للاستبيان.
3. تقديم المسودة الأولى للاستبيان إلى المشرفين لتقويمها واستطلاع رأيهم في صدقها ، والمقاطع المرتبطة بها ، ومدى ملاءمتها لتحقيق أهداف البحث.
4. إعادة ترتيب مجالات الاستبيان وأبعاده وإجراء التعديلات التي اقترحها المشرف.
5. توزيع الاستبانة على عينة البحث لجمع البيانات اللازمة.

خامساً: مكونات أداة البحث (الاستبانة)

تكونت أداة البحث (الاستبانة) والتي صممت لبحث سياسات إطار أمن المعلومات السيبراني وعلاقتها بفاعلية النظم التقنية في القطاع الصحي في المملكة العربية السعودية، من قسمين رئيسيين كما يلي:

القسم الأول: تمثل بالمتغيرات الشخصية لأفراد عينة البحث، وهي (مكان العمل، الجنس، العمر، المسمى الوظيفي، سنوات الخبرة).

القسم الثاني: يعبر عن متغيرات البحث من خلال المجالات والأبعاد المكونة للاستبانة.

ويشمل هذا القسم على (20) فقرة منها (10) فقرات تقيس المتغير التابع (فاعلية الأنظمة التقنية في القطاع الصحي و(10) فقرات تقيس المتغير المستقل (سياسات إطار أمن المعلومات السيبراني) (بأبعاده الاثنين) (تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني ، التدريب والتوعية بتحديات سياسات أمن المعلومات السيبراني) والجدول أدناه يوضح ذلك.

جدول رقم (2) : يوضح توزيع فقرات الاستبانة على المجالات والأبعاد المكونة لها

المجال	البعد	عدد الفقرات
المجال الأول (المتغير المستقل) سياسات إطار أمن المعلومات السيبراني	تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني	5
	التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني	5
	أبعاد المجال الأول ككل "سياسات إطار أمن المعلومات السيبراني"	
المجال الثاني (المتغير التابع) فاعلية الأنظمة التقنية	فاعلية الأنظمة التقنية في القطاع الصحي	10
	مجموع الفقرات	
		20

3-صدق وثبات أداة البحث (الاستبانة)

استخدم الباحثون مقياس ليكرت (Likert Scale) الخماسي لتنقيح وسيلة البحث، بحيث تم إظهار فقرات الاستبانة على أفراد عينة البحث، ومقابل كل بند خمس حلول تحدد مستوى موافقتهم عليها. تم إعطاء إجابات أوزان رقمية لتمثل درجة الإجابة على الفقرة، مثلما هو موضح بالجدول أدناه :

جدول رقم (3) : تصحيح أداة البحث وفق مقياس ليكرت الخماسي

الإجابة	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
الدرجة	5	4	3	2	1

يتضح من الجدول أعلاه بأن الفقرة التي يتم "الموافقة عليها بشدة" تأخذ الدرجة (5) ، والفقرة التي يتم "الموافقة عليها" تأخذ الدرجة (4) ، أما الفقرة التي تكون نتيجة الإجابة عليها "محايد" تأخذ الدرجة (3) ، في حين أن الفقرة

التي تكون الإجابة عليها "غير موافق" تأخذ الدرجة (2)، وكذلك الفقرة التي يجاب عليها غير "موافق بشدة" تأخذ الدرجة (1).

ولتحديد مستوى الموافقة على كل فقرة من الفقرات، وكل بعد من الأبعاد، وكل مجال من مجالات ضمن أداة البحث، فقد تم الاعتماد على قيمة الوسط الحسابي وقيمة الوزن النسبي والجدول أدناه يوضح مستويات الموافقة استنادا لخمس مستويات (منخفض جداً، منخفض، متوسط، مرتفع، مرتفع جداً).

جدول رقم (4): مستويات الموافقة على فقرات وأبعاد ومجالات البحث

مستوى الموافقة	منخفض جداً	منخفض	متوسط	مرتفع	مرتفع جداً
الوسط (المتوسط) الحسابي	أقل من 1.80	1.80 إلى 2.59	2.60 إلى 3.39	3.40 إلى 4.19	أكبر من أو يساوي 4.20
الوزن النسبي	أقل من % 36	% 36 إلى % 51.9	% 52 إلى % 67.9	% 68 إلى % 83.9	أكبر من أو يساوي % 84

والجدول السابق يعطي دلالة واضحة على أن المتوسطات التي تقل عن (1.80) تدل على وجود درجة منخفضة جداً من الموافقة على الفقرة أو البعد أو المجال بمعنى وجود درجة مرتفعة جداً من عدم الموافقة، أما المتوسطات التي تتراوح بين (1.80 - 2.59) فهي تدل على وجود درجة منخفضة من الموافقة بمعنى درجة مرتفعة من عدم الموافقة على الفقرات أو الأبعاد والمجالات، بينما المتوسطات التي تتراوح بين (2.60 - 3.39) فهي تدل على وجود درجة متوسطة من الموافقة أو وجود درجة حيادية تجاه الفقرة أو البعد أو المجال المقصود، كما أن المتوسطات التي تتراوح بين (3.40 - 4.19) تدل على وجود درجة مرتفعة من الموافقة، في حين أن المتوسطات التي تساوي وتزيد عن (4.20) تدل على وجود درجة مرتفعة جداً من الموافقة، وهذا التقسيم تم تحديده وفق مقياس ليكرت الخماسي الذي تم اعتماده في تصحيح أداة البحث.

سادساً: صدق وثبات أداة البحث (الاستبانة)

تم التحقق من صدق أداة البحث وثباتها من خلال تطبيق الاستبانة على عينة مكونة من (60) مستجيب، وتم اتباع الطرق الموضحة فيما يلي للتأكد من صدق الاستبانة وثباتها، والتحقق من صلاحيتها لتطبيقها بعد ذلك على أفراد عينة البحث.

1. صدق أداة البحث:

صدق الاستبانة يعني أن تقيس الاستبانة ما وضعت لقياسه (الجرجاوي، 2010، صفحة 105). كما يقصد بالصدق "شمول الاستقصاء لكل العناصر التي يجب أن تدخل في التحليل من ناحية، ووضوح فقراتها ومفرداتها من ناحية ثانية، بحيث تكون مفهومة لكل من يستخدمها" (عبيدات، ذوقان، و عدس، 2001، صفحة 179) وعلى مستوى المجالات ككل فقد بلغ معامل ارتباط المجال الأول "سياسات الأمن السيبراني" بالدرجة الكلية للاستبانة (0.985)، بينما بلغ معامل ارتباط المجال الثاني "فاعلية النظم التقنية" بالدرجة الكلية للاستبانة (0.856)، وكانت جميع معاملات الارتباط (الصدق) ذات دلالة إحصائية عند مستوى 0.05. ويشير ذلك لوجود درجة مرتفعة من صدق الأبعاد الفرعية والمجالات الرئيسية للبيانات التي تم جمعها من أفراد العينة.

جدول قم (5) : (معاملات الارتباط (الصدق) بين الدرجة الكلية للاستبانة والمجالات والأبعاد الفرعية

المجال	البعد	عدد الفقرات	معامل الارتباط	مستوى الدلالة
المجال الأول (المتغير المستقل) سياسات الأمن السيبراني	تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني	5	0.809*	0.00
	التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني	5	0.796*	0.00
أبعاد المجال الأول		10	0.985*	0.00

0.00	0.856*	10	فاعلية الأنظمة التقنية في القطاع الصحي	المجال الثاني (المتغير التابع) فاعلية الأنظمة التقنية
------	--------	----	--	--

2- صدق الاتساق الداخلي:

يقصد بالاتساق الداخلي مدى اتساق كل فقرة من فقرات الاستبانة مع البعد أو المجال الذي تنتمي إليه هذه الفقرة، ويتم التحقق من وجود صدق الاتساق الداخلي من خلال حساب معاملات الارتباط بين درجة كل فقرة و الدرجة الكلية للبعد أو المجال الذي تنتمي إليه، وذلك بهدف التحقق من مدى صدق الاستبانة ككل. وفيما يلي عرض لنتائج التحقق من صدق الاتساق الداخلي لفقرات الاستبانة حسب الأبعاد والمجالات التي تتكون منها.

جدول رقم (6) : معاملات صدق الاتساق الداخلي لفقرات البعد الأول

م	دعم الإدارة العليا	معامل الارتباط	مستوى الدلالة
1	تدرك الإدارة العليا في المستشفى أهمية سياسات أمن المعلومات السيبراني.	0.895	0.000
2	تضع المستشفى التدابير الاحتياطية التي تحد من مستوى تعرض معلوماتها للخطر.	0.573	0.000
3	يوجد لدى المستشفى آليات مناسبة لمنع عمليات الوصول غير الشرعية (غير المرخص بها) للبيانات بواسطة العاملين.	0.658	0.000
4	تقوم المستشفى بتحديث طرق حماية معلوماتها تبعاً للتغيرات الحاصلة في بيئة التكنولوجيا.	0.821	0.000
5	يتوفر لدى المستشفى آليات مناسبة لمنع عمليات الإدخال المتعمدة للبيانات غير السليمة بواسطة العاملين.	0.642	0.000

يتضح من خلال الجدول السابق بأن معاملات صدق الاتساق الداخلي لفقرات البعد الأول "سياسات إطار أمن المعلومات السيبراني"، جميعها ذات دلالة إحصائية عند مستوى 0.05، حيث تراوحت قيم معاملات صدق الاتساق الداخلي لفقرات المجال بين (0.573) للفقرة الثانية والتي تنص على "تضع المستشفى التدابير الاحتياطية التي تحد من مستوى تعرض معلوماتها للخطر." و (0.895) للفقرة الأولى التي تنص على "تدرك الإدارة العليا في المستشفى أهمية سياسات أمن المعلومات السيبراني".

جدول رقم (7) : معاملات صدق الاتساق الداخلي لفقرات البعد الثاني

م	دعم الإدارة العليا	معامل الارتباط	مستوى الدلالة
1	تصدر المستشفى نشرات تثقيفية دورية عن أهمية أمن المعلومات السيبراني.	0.688	0.000
2	تنفذ المستشفى محاضرات تدريب وتوعية إلزامية للعاملين حول سياسات أمن المعلومات.	0.925	0.000
3	يتوافق مضمون ومحتوى البرامج التدريبية الخاصة بأمن المعلومات السيبراني مع بيئة ومتطلبات عمل المستشفى.	0.705	0.000
4	تقوم المستشفى بتحديث سياسات أمن المعلومات السيبراني تبعاً للتطورات والتغيرات التكنولوجية العالمية.	0.863	0.000
5	تطلعني المستشفى باستمرار على أي تحديث يطرأ على سياسات أمن المعلومات السيبراني.	0.623	0.000

يتضح من خلال الجدول السابق بأن معاملات صدق الاتساق الداخلي لفقرات البعد الثاني "التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني"، جميعها ذات دلالة إحصائية عند مستوى 0.05، حيث تراوحت قيم معاملات صدق الاتساق الداخلي لفقرات المجال بين (0.623) للفقرة الخامسة والتي تنص على "تطلعني المستشفى باستمرار على أي تحديث يطرأ على سياسات أمن المعلومات السيبراني." و (0.925) للفقرة

الثانية التي تنص على " تنفذ المستشفى محاضرات تدريب وتوعية إلزامية للعاملين حول سياسات أمن المعلومات".

جدول رقم (8) : معاملات صدق الاتساق الداخل لفقرات المجال فاعلية الأنظمة التقنية في القطاع الصحي

م	دعم الإدارة العليا	معامل الارتباط	مستوى الدلالة
1	تتوفر الوسائل الكافية لحماية الأنظمة التقنية في المستشفى من التلف أو التخريب	0.548	0.00
2	تحتوي الأنظمة التقنية في المستشفى على مميزات تعمل على حماية المعلومات وتقليل الأخطاء.	0.776	0.00
3	تتوفر القدرة لدى الأنظمة التقنية في المستشفى على اثبات التصرفات الخاصة بتهديد أو تسريب المعلومات	0.784	0.00
4	تقدم الأنظمة التقنية في المستشفى معلومات آمنة ودقيقة.	0.830	0.00
5	توفر الأنظمة التقنية في المستشفى معلومات ملائمة وتلي متطلبات العمل.	0.955	0.00
6	تحسن الأنظمة التقنية في المستشفى من إنتاجية العمل في المستشفى.	0.804	0.00
7	توفر الأنظمة التقنية في المستشفى المعلومات اللازمة في الزمن والوقت المناسبين.	0.725	0.00
8	تعطي المستشفى صلاحيات الدخول للأنظمة التقنية حسب المستوى الإداري.	0.757	0.00
9	تقوم المستشفى بتحديث الأنظمة التقنية و صيانتها بشكل مستمر.	0.509	0.00
10	توجد دائرة مستقلة للأنظمة التقنية في المستشفى.	0.784	0.00

يتضح من خلال الجدول السابق بأن معاملات صدق الاتساق الداخلي لفقرات المجال الثاني "فاعلية الأنظمة التقنية في القطاع الصحي"، جميعها ذات دلالة إحصائية عند مستوى 0.05، حيث تراوحت قيم معاملات صدق الاتساق الداخلي لفقرات المجال بين (0.509) للفقرة التاسعة والتي تنص على "تقوم المستشفى بتحديث الأنظمة التقنية وصيانتها بشكل مستمر." و (0.955) للفقرة الخامسة التي تنص على "توفر الأنظمة التقنية في المستشفى معلومات ملائمة وتلي متطلبات العمل."

وبناءً على الطرق السابقة، اتضح للباحث صدق أداة البحث (الاستبانة).

1. ثبات أداة البحث:

يقصد بثبات الاستبانة أن تعطي الاستبانة نفس النتائج إذا أعيد تطبيقها عدة مرات متتالية (الجرجاوي، 2010، صفحة 97). حيث أن الثبات يختص بمدى الوثوق في البيانات التي نحصل عليها من خلال تطبيق أداة البحث على العينة التجريبية، بمعنى أن النتائج التي يتم الحصول عليها من خلال تحليل بيانات أداة البحث يجب ألا تتأثر بالعوامل التي تعود إلى أخطاء الصدفة، فهو يعني دقة أداة البحث، وبصورة مختصرة يمكن وصف الثبات بأنه ضمان الحصول على نفس النتائج تقريباً إذا تم إعادة تطبيق الأداة على نفس المجموعة من الأفراد، وهذا يعني قلة تأثير عوامل الصدفة والعشوائية على نتائج الأداة (السيد، 2006، صفحة 2)

وتتضمن الحزمة الإحصائية للعلوم الاجتماعية (SPSS) العديد من أساليب حساب الثبات، وفي هذا البحث اعتمد الباحثون على طريقة ألفا كرونباخ، كما يلي:

تعتمد هذه الطريقة على الاتساق في إجابات الأفراد على فقرات المقياس، وعندما يكون المقياس متجانساً فإن كل فقرة فيه تقيس نفس العوامل العامة التي يقيسها المقياس، ويتم حساب معاملات الثبات بطريقة الاتساق الداخلي باستخدام طريقة ألفا كرونباخ (حسن ع.، 2011، صفحة 16).

جدول رقم (9) : أدناه يوضح نتائج حساب معامل ألفا كرونباخ لقياس الثبات :

المجال	البعد	معامل ثبات ألفا كرونباخ
تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني	تدرك الإدارة العليا في المستشفى أهمية سياسات أمن المعلومات السيبراني.	0.784
	تضع المستشفى التدابير الاحتياطية التي تحد من مستوى تعرض معلوماتها للخطر.	0.805
	يوجد لدى المستشفى آليات مناسبة لمنع عمليات الوصول غير الشرعية (غير المرخص بها) للبيانات بواسطة العاملين.	0.798
	تقوم المستشفى بتحديث طرق حماية معلوماتها تبعاً للتغيرات الحاصلة في بيئة التكنولوجيا.	0.791
	يتوفر لدى المستشفى آليات مناسبة لمنع عمليات الإيدخال المتعمدة للبيانات غير السليمة بواسطة العاملين.	0.798
التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني	تصدر المستشفى نشرات تثقيفية دورية عن أهمية أمن المعلومات السيبراني.	0.798
	تنفذ المستشفى محاضرات تدريب وتوعية إلزامية للعاملين حول سياسات أمن المعلومات.	0.783
	يتوافق مضمون ومحتوى البرامج التدريبية الخاصة بأمن المعلومات السيبراني مع بيئة ومتطلبات عمل المستشفى.	0.796
	تقوم المستشفى بتحديث سياسات أمن المعلومات السيبراني تبعاً للتطورات والتغيرات التكنولوجية العالمية.	0.786
	تطلعني المستشفى باستمرار على أي تحديث يطرأ على سياسات أمن المعلومات السيبراني.	0.799

0.801	تتوفر الوسائل الكافية لحماية الأنظمة التقنية في المستشفى من التلف أو التخريب	فاعلية الأنظمة التقنية في القطاع الصحي
0.792	تحتوي الأنظمة التقنية في المستشفى على مميزات تعمل على حماية المعلومات وتقليل الأخطاء.	
0.792	تتوفر القدرة لدى الأنظمة التقنية في المستشفى على اثبات التصرفات الخاصة بتهديد أو تسريب المعلومات	
0.791	تقدم الأنظمة التقنية في المستشفى معلومات آمنة ودقيقة.	
0.784	توفر الأنظمة التقنية في المستشفى معلومات ملائمة وتلبي متطلبات العمل.	
0.79	تحسن الأنظمة التقنية في المستشفى من انتاجية العمل في المستشفى.	
0.795	توفر الأنظمة التقنية في المستشفى المعلومات اللازمة في الزمن والوقت المناسبين.	
0.794	تعطي المستشفى صلاحيات الدخول للأنظمة التقنية حسب المستوى الإداري.	
0.803	تقوم المستشفى بتحديث الأنظمة التقنية و صيانتها بشكل مستمر.	
0.792	توجد دائرة مستقلة للأنظمة التقنية في المستشفى.	

يتضح من خلال الجدول السابق أن معاملات الثبات بطريقة ألفاكرونباخ كانت مرتفعة بشكل عام لجميع أبعاد ومجالات الاستبانة، حيث على مستوى أبعاد سياسات أمن المعلومات نجد أن معاملات الثبات بطريقة ألفاكرونباخ تراوحت بين (0.783) وذلك للبعد السابع "تنفذ المستشفى محاضرات تدريب وتوعية إلزاميه للعاملين حول سياسات أمن المعلومات" و(0.805) للبعد الثاني "تضع المستشفى التدابير الاحتياطية التي

تحد من مستوى تعرض معلوماتها للخطر"، وتشير جميع النتائج السابقة وجود درجة مرتفعة من الثبات في البيانات التي تم جمعها من أفراد العينة.

سابعاً: التوزيع الطبيعي لمتغيرات البحث

هناك نوعين من الاختبارات الإحصائية، النوع الأول يطلق عليه الاختبارات المعلمية (Parametric Tests)

والنوع الثاني يطلق عليه الاختبارات اللامعلمية (Non Parametric Tests).

ويشترط لاستخدام الاختبارات المعلمية التوزيع الطبيعي للبيانات المراد إجراء الاختبارات الإحصائية عليها، بينما تستخدم الاختبارات اللامعلمية كبديل للاختبارات المعلمية في حال عدم تحقق شرط التوزيع الطبيعي للبيانات ولكن ذلك يكون فقط في حال العينات الصغيرة التي يقل حجمها عن (30) مفردة، بينما العينات التي يزيد حجمها عن (30) مفردة يمكن التخلي عن شرط التوزيع الطبيعي وذلك وفقاً لما تقره نظرية النهاية المركزية (ربيع أ.،

2007، صفحة 111)

وبذلك تكون الاستبانة في صورتها النهائية كما هي في الملحق رقم (1)، وتكون الباحثون قد تأكدت من صدق وثبات استبانة البحث مما يجعلها على ثقة بصحة الاستبانة وصلاحيها لتحليل النتائج والإجابة على أسئلة البحث واختبار فرضياته.

ثامناً: الأساليب الإحصائية المستخدمة في البحث

اعتمد هذا البحث على استخدام الحزمة الإحصائية للعلوم الاجتماعية (SPSS V.22) لمعالجة وتحليل البيانات إحصائياً واختبار صحة فرضيات البحث. وفيما يلي مجموعة الأساليب الإحصائية الوصفية والاستدلالية التي تم استخدامها في البحث:

الأساليب الوصفية، وتمثلت فيما يلي:

أ. النسب المئوية والتكرارات: والتي تم استخدامها في وصف أفراد عينة البحث حسب المتغيرات الشخصية.

ب. الوسط (المتوسط) الحسابي: تم استخدامه بغرض توضيح مدى موافقة أفراد عينة البحث على أبعاد ومجالات البحث.

ج. الانحراف المعياري: والذي تم استخدامه لقياس مدى تشتت وانحرافات إجابات أفراد عينة البحث على الفقرات والأبعاد عن الوسط الحسابي لها، حيث أن انخفاض قيمة الانحراف واقتربها من الصفر تدل على مدى تركيز الإجابات وانخفاض تشتتها.

د. الوزن النسبي: وهو عبارة عن نسبة متوسط الإجابات على فقرة ما أو بعد ما إلى الدرجة العظمى للمقياس المستخدم، ويستخدم بغرض تحويل درجة الوسط الحسابي للإجابات إلى درجة مئوية.

الصعوبات التي واجهت الباحثون :

1. عدم تعاون بعض أفراد العينة من حيث قبول تعبئة الاستبانة.
2. ندرة الكتب والدراسات السابقة التي تناولت موضوع سياسات أمن المعلومات، وخاصة المراجع المحلية والعربية منها.
3. الصعوبة في ربط النتائج المتعلقة بعلاقة بعض أبعاد سياسات أمن المعلومات بفاعلية نظم المعلومات الإدارية مع دراسات أخرى نظراً لندرة الدراسات السابقة التي تناولت علاقة سياسات إطار الأمن السيبراني بالأنظمة التقنية في المنظمات.

ملخص الفصل الرابع

استعرض الباحثون في هذا الفصل منهجية البحث واجراءاته، حيث أشاروا إلى اعتمادهم "الأسلوب الوصفي التحليلي" حيث أنه أكثر المناهج استخداماً في دراسة الظواهر الاجتماعية والإنسانية، وأكثر الأساليب مناسبة لموضوع البحث. كما أوضح الباحثون المصادر التي تم استخدامها في البحث بنوعها الثانوية والأولية. واستعرضوا مجتمع البحث الذي تبين أنه يتكون من العاملين في مراكز ووحدات تكنولوجيا المعلومات في القطاع الصحي، بالإضافة للعاملين الذين يستخدمون الأنظمة التقنية في القطاع الصحي بالمستشفيات الخمسة محل البحث).

والذي بلغ 60 فرداً، وباستخدام المعادلات الإحصائية قد حدد الباحث حجم العينة المناسب. ولقد استخدم الباحث العينة العشوائية الطبقية لتطبيق أداة البحث "الاستبانة"، وأوضح الباحثون خلال هذا الفصل الخطوات التي تم اتباعها لإعداد الاستبانة بشكلها النهائي، بداية من مراجعة الأدبيات وصولاً لتوزيع الاستبانة على عينة البحث وجمعها، موضحين مكونات الاستبانة النهائية وأقسامها. كما استعرض الباحث المقياس المستخدم

في تصحيح أداة الاستبانة وهو مقياس ليكرت الخماسي، وأوضحوا الطرق التي تم استخدامها للتحقق من صدق وثبات الاستبانة من خلال تطبيق الاستبانة على عينة تجريبية مكونة من (60) فرداً، حيث أنه قدم تم استخدام طرق الصدق الظاهري، صدق الأبعاد الفرعية، وصدق الاتساق الداخلي للتأكد من صدق الاستبانة، بينما تم استخدام طريقة ألفا كرونباخ للتأكد من ثبات الاستبانة، وأشار الباحثون إلى النتائج لوجود درجة مرتفعة من الصدق، كما أشاروا لوجود درجة مرتفعة من الثبات.

كما أوضح الباحثون خلال هذا الفصل الأساليب الإحصائية التي تم استخدامها في هذا البحث (الأساليب الوصفية، والأساليب الإحصائية الاستدلالية)، واختتم الفصل بتوضيح الصعوبات التي واجهها الباحثون أثناء إعداد البحث.

الفصل الخامس

تحليل البيانات واختبار فرضيات البحث

أولاً: تحليل خصائص عينة البحث

ثانياً: نتائج تحليل مجالات و أبعاد البحث

ثالثاً: اختبار ومناقشة فرضيات البحث

يستعرض الباحثون في هذا الفصل تحليل بيانات البحث واختبار فرضياته. حيث أنها في البداية يستعرض الوصف الإحصائي لعينة البحث وذلك من خلال عرض توزيع أفراد عينة البحث حسب المتغيرات الشخصية (مكان العمل، الجنس، المسمى الوظيفي، سنوات الخبرة).

كما استعرض الباحثون نتائج تحليل مجالات وأبعاد البحث، وذلك من خلال تحليل النتائج المتعلقة بمجالي سياسات إطار الأمن السيبراني، وفاعلية الانظمة التقنية. بالإضافة لاختبار فرضيات البحث الثلاثة الرئيسة ومناقشتها. كما وضح الباحثون أبرز نتائج الاستبانة والتي تم التوصل إليها من خلال الاجراءات الإحصائية التحليلية، إذ تم استخدام برنامج الحزم الإحصائية للعلوم الاجتماعية (SPSS) للحصول على نتائج البحث.

أولاً: تحليل خصائص عينة البحث

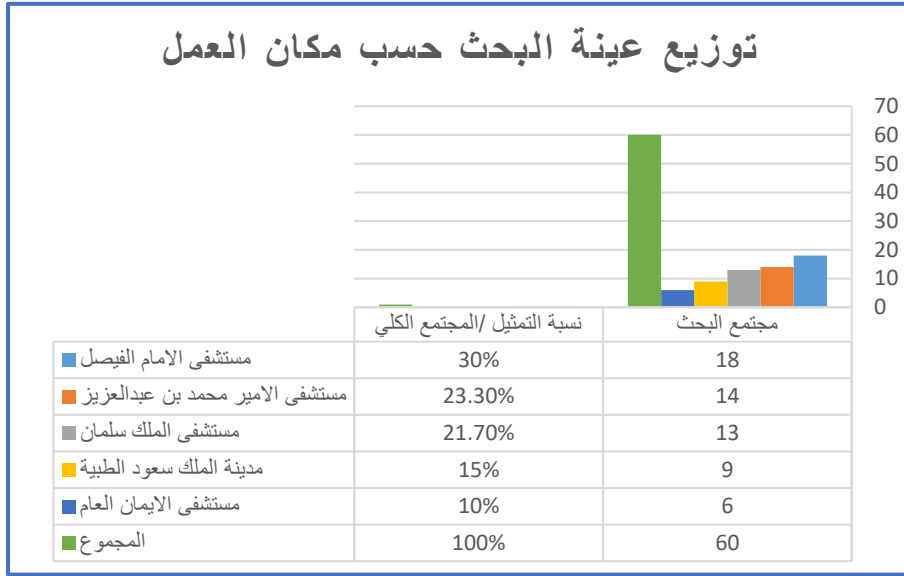
يتضمن تحليل خصائص عينة البحث الوصف الإحصائي للعينة وفق الخصائص والسمات الشخصية والتي تمثلت بكل من (مكان العمل، الجنس، العمر، المسمى الوظيفي، سنوات الخبرة) وفيما يلي عرض لنتائج عينة البحث وفق هذه الخصائص في الجدول الموضح أدناه :

جدول رقم (18): نتائج عينة البحث وفق الخصائص والسمات الشخصية

المتغير	الفئة	العدد	النسبة
مكان العمل	مدينة الملك سعود الطبية	9	15%
	مستشفى الايمان العام	6	10%
	مستشفى الملك سلمان	13	22%
	مستشفى الامام الفيصل	18	30%
	مستشفى الامير محمد بن عبدالعزيز	14	23%
	المجموع	60	100%
الجنس	ذكر	41	68%
	أنثى	19	32%
	المجموع	60	100%

18%	11	أقل من 5 سنوات	سنوات الخبرة
52%	31	أقل من 10 سنوات	
17%	10	أقل من 15 سنة	
13%	8	15 سنة فأكثر	
100%	60	المجموع	
8.3%	5	مدير	المسمى الوظيفي
8.3%	5	مساعد مدير	
5%	3	رئيس قسم	
61.7%	37	إداري	
16.7%	10	مبرمج / مصمم	
0%	0	أخرى	
100%	60	المجموع	

توزيع عينة البحث حسب مكان العمل

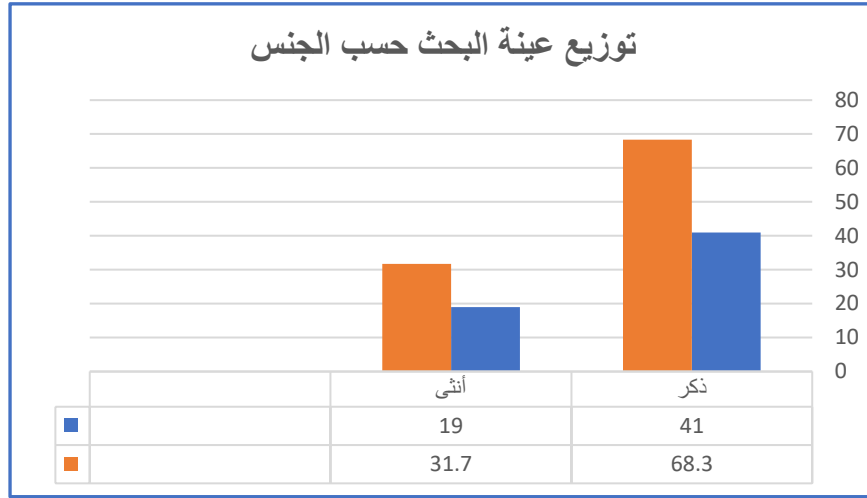


1 شكل رقم (1) : توزيع عينة البحث حسب مكان العمل

يتضح من البيانات الواردة في الجدول أعلاه والمتعلقة بتوزيع عينة البحث حسب مكان العمل، بأن نصيب مستشفى الامام فيصل كان الأكبر حيث بلغت نسبة الأفراد العاملين في مستشفى الامام فيصل من عينة البحث (30 %) بواقع (18) موظف.

ويعزو الباحثون ذلك إلى أن عدد العاملين الإجمالي في مستشفى الامام فيصل أكبر من باقي المستشفيات، وبالتالي فإن عدد أفراد العينة يتناسب مع عدد أفراد العاملين الإجمالي.

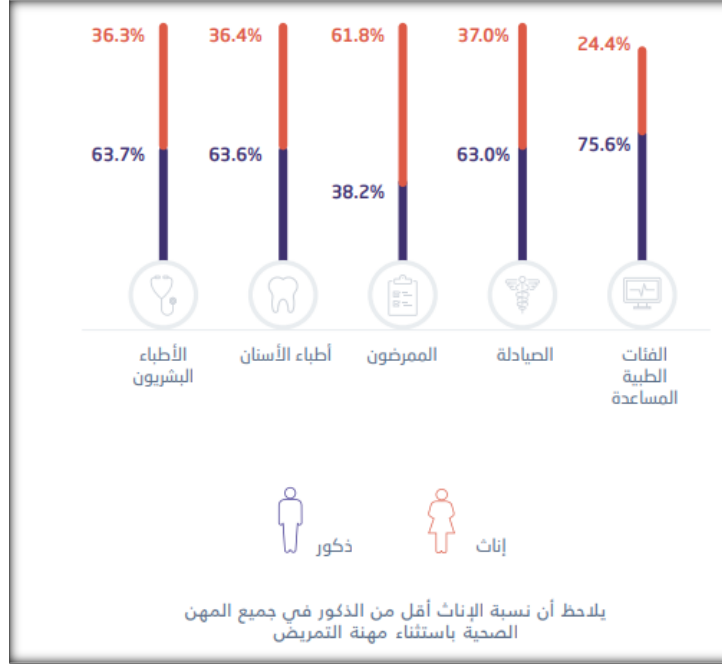
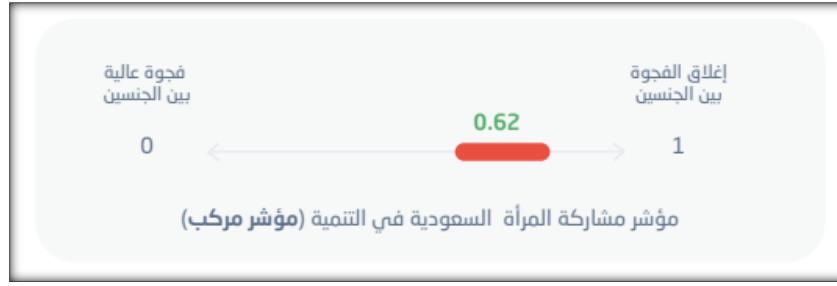
توزيع عينة البحث حسب الجنس



شكل رقم (2) : توزيع عينة البحث حسب الجنس

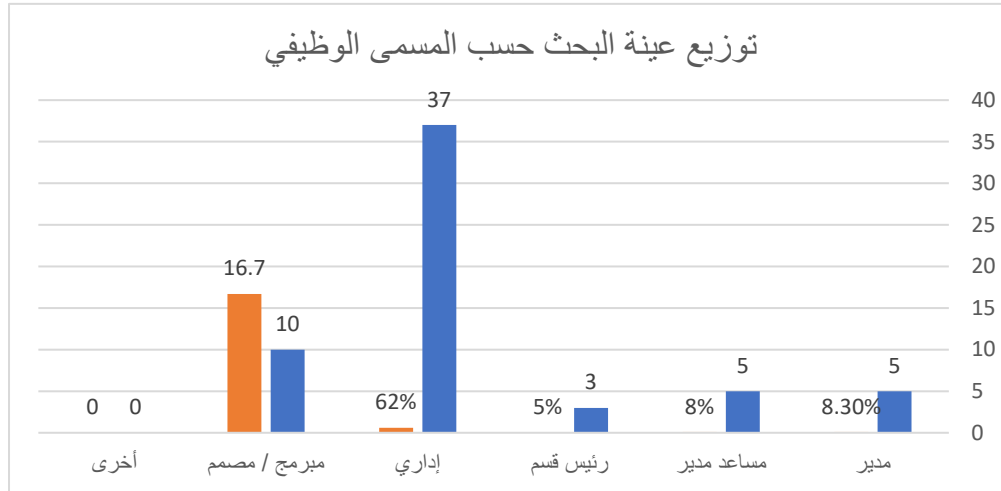
يتضح من الجدول أعلاه (والمتعلقة بتوزيع أفراد عينة البحث حسب متغير الجنس، أن غالبية أفراد عينة البحث كانوا من الذكور بنسبة (68.3 %) بواقع (41) موظف، في حين شكلت الإناث من عينة البحث نسبة تبلغ (31.7 %) بواقع (19) موظفة.

ويرى الباحثون أن ذلك يعود إلى العادات والتقاليد السائدة في المجتمع والتي تفضل الذكور على الإناث في العمل، حيث أن قدرات الذكور تتمثل بشكل أكبر في تحمل ضغوط وظروف العمل، وهذا يجعل عدد العاملات الإناث في المستشفيات الخمسة أقل من عدد العاملين الذكور. وتتوافق هذه البيانات مع التقارير الإحصائية الصادرة عن الهيئة العامة للإحصاء، حيث أصدرت الهيئة العامة تقرير خاص بعنوان "المرأة السعودية شريك النجاح" بمناسبة «اليوم العالمي للمرأة 2020» أشار فيه إلى تحقيق نجاحات بارزة في المحورين التعليمي والصحي من حيث نسبة المشاركة في القوى العاملة بين الأفراد والشكل التالي يوضح تلك النسب.



شكل رقم (3): التوزيع النسبي للعاملين السعوديين في المجالات الصحية (15 سنة فأكثر) حسب المهن الرئيسية والجنس

- توزيع عينة البحث حسب المسمى الوظيفي :

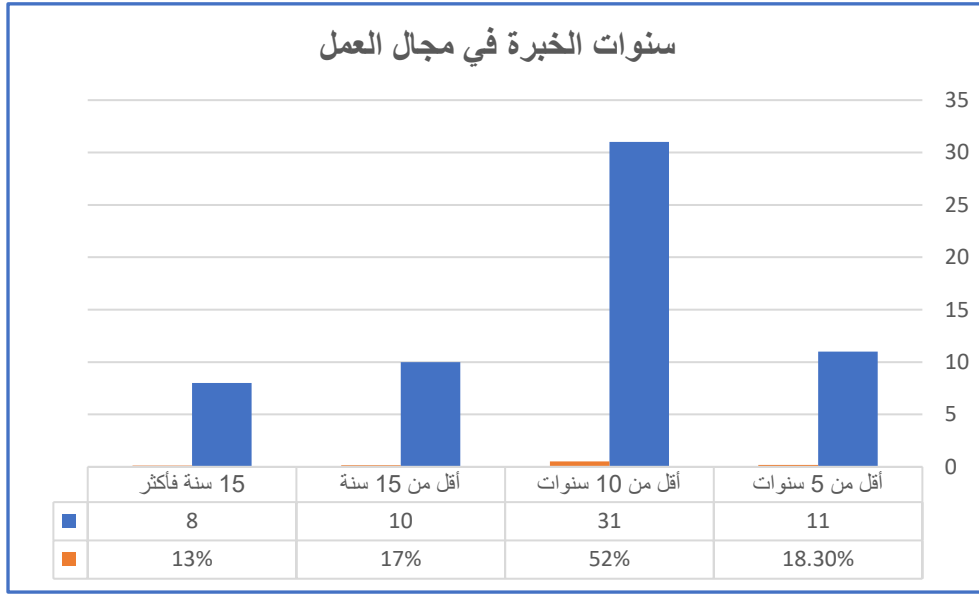


شكل رقم (4) : توزيع عينة البحث حسب المسمى الوظيفي

يتضح من الجدول أعلاه لتوزيع أفراد عينة البحث حسب المسمى الوظيفي، بأن معظم أفراد عينة البحث من فئة الإداريين وذلك بنسبة (62%) بواقع (37) إداري، أما في المرتبة الأخيرة جاء رؤساء الأقسام بنسبة (5%) وبواقع (3) رؤساء للأقسام.

ويعزو الباحثون ذلك إلى الاستخدام الكبير لنظم المعلومات في المستشفيات في مختلف الدوائر والأقسام، حيث أن المستشفيات تسير معظم عملياتها التي تخص المرضى والعاملين مستخدمة النظم التقنية والمعلوماتية المختلفة، مما يجعل فئة الإداريين هي الفئة الأكبر المتعاملة مع هذه النظم، ولا يقتصر التعامل مع النظم مع رؤساء الأقسام أو مديري الدوائر. ويرى الباحثون أن حصول نسبة فئة المبرمجين والمصممين على النسبة التالية يرجع إلى أعداد العاملين في وحدات ومراكز تكنولوجيا المعلومات مقارنة بأعداد العاملين الذين يستخدمون نظم المعلومات في الدوائر والأقسام الأخرى التي تنفذ أعمالها مستفيدة من نظم المعلومات بالمستشفى. كما ويفسر الباحثون انخفاض نسبة فئة المدراء ورؤساء الأقسام، بأن أعدادهم أقل مقارنة بأعداد الإداريين في الدوائر والأقسام، وهذا التوزيع الطبيعي للهيكل والدوائر الإدارية في المستشفيات.

توزيع عينة البحث حسب عدد سنوات الخبرة في مجال العمل :



شكل رقم (5) : توزيع عينة البحث حسب مجال العمل

يلاحظ الباحثون من الجدول التالي لتوزيع أفراد عينة البحث حسب عدد سنوات الخبرة في مجال العمل بأن

غالبية أفراد عينة البحث بنسبة (70 %) وبواقع (42) موظف، تقل سنوات خبرتهم عن 10 سنوات.

ويرى الباحثون أن ذلك يدل على أن الإداريين العاملين في المستشفى والمستخدمين لنظم المعلومات يتمتعون بخبرة

جيدة ومعلومات محدثة ولديهم معرفة كافية بعلوم الأمن السيبراني في المستشفى مما يساهم في زيادة إدراكهم

لأهمية إطار الأمن السيبراني وأهمية استخدام ذلك الاطار وتأثيره على الأنظمة التقنية داخل المستشفى.

ثانياً: نتائج تحليل مجالات وأبعاد البحث

يعرض الباحثون فيما يلي نتائج تحليل مجالات وأبعاد البحث، حيث يستعرض في البداية تحليل النتائج المتعلقة بالمجال الأول والذي يمثل المتغير المستقل (سياسات إطار أمن المعلومات السيبراني)، ثم نستعرض نتائج التحليل المتعلقة بالمجال الثاني والذي يمثل المتغير التابع (فاعلية الأنظمة التقنية في القطاع الصحي). ومن الجدير بالذكر أن الباحثين يقومون بالتعليق على أعلى فقرة، وأدنى فقرة في نتائج التحليل الإحصائي لتوضيح سبب حصولها على ذلك الترتيب من وجهة نظرهم.

1. تحليل النتائج المتعلقة بالمجال الأول "سياسات إطار أمن المعلومات السيبراني"

يستعرض الباحث فيما يلي النتائج المتعلقة بالمجال الأول "سياسات إطار أمن المعلومات السيبراني"، وبناءً على ذلك فإنه تم استعراض نتائج كل بعد من أبعاد المجال على حدى (تقدير الإدارة العليا لمخاطر أمن المعلومات السيبراني، التدريب والتوعية بتحديات سياسات أمن المعلومات السيبراني).

أ. النتائج المتعلقة بالبعد الأول "تقدير الإدارة العليا لمخاطر أمن المعلومات السيبراني".

فيما يلي عرض لأهم نتائج التحليل الإحصائي لفقرات البعد الأول "تقدير الإدارة العليا لمخاطر أمن المعلومات السيبراني" الذي يندرج تحت المجال الأول "سياسات إطار أمن المعلومات السيبراني"، حيث تم حساب الوسط الحسابي والانحراف المعياري والوزن النسبي لكل فقرة من فقرات البعد ومن ثم تم حساب الوسط الحسابي والانحراف المعياري والوزن النسبي للدرجة الكلية للبعد.

النتائج المتعلقة بفقرات البعد الأول "تقدير الإدارة العليا لمخاطر أمن المعلومات السيبراني":

فيما يلي عرض لأهم نتائج التحليل الإحصائي لفقرات البعد الأول "تقدير الإدارة العليا لمخاطر أمن المعلومات السيبراني" الذي يندرج تحت المجال الأول "سياسات إطار أمن المعلومات السيبراني"، حيث تم حساب الوسط الحسابي والانحراف المعياري والوزن النسبي لكل فقرة من فقرات البعد ومن ثم تم حساب الوسط الحسابي والانحراف المعياري والوزن النسبي للدرجة الكلية للبعد، كما تم التحقق من مساواة متوسطات الإجابة

على فقرات البعد للقيمة (3) التي تعبر عن الدرجة الحيادية باستخدام اختبار One Sample T-Test

جدول رقم (19) : نتائج تحليل مجالات و أبعاد البحث

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	قيمة اختبار t	القيمة الاحتمالية sig	الترتيب
1	تدرك الإدارة العليا في المستشفى أهمية سياسات أمن المعلومات السيبراني.	3.95	0.85	79%	8.635	0.00	2
2	تضع المستشفى التدابير الاحتياطية التي تحد من مستوى تعرض أنظمتها التقنية للخطر.	3.6	0.79	72%	5.917	0.00	5
3	يوجد لدى المستشفى آليات مناسبة لمنع عمليات الوصول غير الشرعية (غير المرخص بها) للبيانات بواسطة العاملين.	3.93	0.36	79%	19.969	0.00	3
4	تقوم المستشفى بتحديث طرق حماية معلوماتها تبعاً للتغيرات الحاصلة في بيئة التكنولوجيا.	4	0.49	80%	15.901	0.00	1
5	يتوفر لدى المستشفى آليات مناسبة لمنع عمليات الإدخال المتعمدة للبيانات غير السليمة بواسطة العاملين.	3.87	0.54	77%	12.531	0.00	4
	الدرجة الكلية للبعد	3.87	0.60	77%	12.6	0.00	

من الجدول أعلاه، يمكن استخلاص ما يلي:

أن الفقرة الرابعة التي تنص على " تقوم المستشفى بتحديث طرق حماية معلوماتها تبعاً للتغيرات الحاصلة في بيئة التكنولوجيا." جاءت في المرتبة الأولى من حيث قيمة الوسط الحسابي التي بلغت (4.0 من 5.0)، بوزن نسبي 80 % ويشير ذلك لوجود درجة مرتفعة جداً من الموافقة على هذه الفقرة من قبل أفراد عينة البحث، وذلك تبعاً للجدول السابق. والذي يوضح مستويات الموافقة على فقرات وأبعاد ومجالات البحث. ويرى الباحثون أن هذا يشير بدوره إلى الدور الذي تقوم به المستشفى بتحديث طرق حماية معلوماتها وانظمتها طبقاً لأحدث التكنولوجيا الحديثة من وجهة نظر أفراد عينة البحث.

أما الفقرة الثانية من فقرات البعد والت تنص على " تضع المستشفى التدابير الاحتياطية التي تحد من مستوى تعرض أنظمتها التقنية للخطر." جاءت في المرتبة الأخيرة من حيث قيمة الوسط الحسابي حيث بلغ الوسط الحسابي لهذه الفقرة (3.6 من 5.0) بوزن نسبي 72 %، وتشير هذه القيمة لوجود درجة مرتفعة من الموافقة على هذه الفقرة وذلك من وجهة نظر أفراد عينة البحث.

ويرى الباحثون أن ذلك يعود إلى أن المستشفيات بحاجة لإعطاء اهتمام أكبر في عملية اتخاذ التدابير الاحتياطية التي تحد من تعرض أنظمتها التقنية للخطر، حيث اتضح للباحثين أثناء الدراسة الاستطلاعية التي قاموا بها أن التدابير الاحتياطية بحاجة للمزيد من التدابير الاحترازية بالقدر الذي يمنع عمليات التخريب والاختراق المستقبلي.

وبلاحظ من خلال الجدول السابق أيضاً أن قيم اختبار (T) للتحقق من أن متوسط الإجابات يزيد عن القيمة (3) (التي تعبر عن الموقف الحيادي لأفراد العينة أم لا، كانت جميعها ذات دلالة إحصائية عند مستوى 0.05 حيث أن قيمة 0.000 (Sig)، وكانت جميع المتوسطات تزيد عن الدرجة الحيادية (3)، ويشير ذلك إلى أن متوسط الإجابة على كل فقرة من فقرات البعد تزيد عن القيمة (3) زيادة جوهرية وذات دلالة إحصائية عند مستوى 0.05، ويشير ذلك لأن موقف أفراد عينة البحث تجاه بعد " تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني " يتجه نحو الموقف الإيجابي.

النتائج المتعلقة بفقرات البعد الثاني " التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني ":

فيما يلي عرض لأهم نتائج التحليل الإحصائي لفقرات البعد الثاني " التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني " الذي يندرج تحت المجال الأول "سياسات إطار أمن المعلومات السيبراني"، حيث تم حساب الوسط الحسابي والانحراف المعياري والوزن النسبي لكل فقرة من فقرات البعد ومن ثم تم حساب الوسط الحسابي والانحراف المعياري والوزن النسبي للدرجة الكلية للبعد، كما تم التحقق من مساواة متوسطات الإجابة على فقرات البعد للقيمة (3) التي تعبر عن الدرجة الحيادية باستخدام اختبار (One Sample T-Test).

جدول رقم (20) حساب الوسط الحسابي والانحراف المعياري والوزن النسبي

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	قيمة اختبار t	القيمة الاحتمالية sig	الترتيب
1	تصدر المستشفى نشرات تثقيفية دورية عن أهمية أمن المعلومات السيبراني.	3.68	0.81	74%	6.5	0.00	5
2	تنفذ المستشفى محاضرات تدريب وتوعية إلزامية للعاملين حول سياسات أمن المعلومات.	3.93	0.69	79%	10.5	0.00	1
3	يتوافق مضمون ومحتوى البرامج التدريبية الخاصة بأمن المعلومات السيبراني مع بيئة ومتطلبات عمل المستشفى.	3.87	0.68	77%	9.9	0.00	2
4	تقوم المستشفى بتحديث سياسات أمن المعلومات السيبراني تبعاً للتطورات والتغيرات التكنولوجية العالمية.	3.85	0.82	77%	8.0	0.00	3
5	تطوعي المستشفى باستمرار على أي تحديث يطرأ على سياسات أمن المعلومات السيبراني.	3.82	0.43	76%	14.7	0.00	4
	الدرجة الكلية للبعد	3.83	0.69	77%	9.9	0.00	

ومن الجدول أعلاه، يمكن استخلاص ما يلي:

أن الفقرة الثانية التي تنص على "تنفذ المستشفى محاضرات تدريب وتوعية إلزامية للعاملين حول سياسات أمن المعلومات." جاءت في المرتبة الأولى من حيث قيمة الوسط الحسابي التي بلغت (3.93 من 5.0)، بوزن نسبي 79 % ويشير ذلك لوجود درجة مرتفعة جداً من الموافقة على هذه الفقرة من قبل أفراد عينة البحث، وذلك تبعاً للجدول السابق. والذي يوضح مستويات الموافقة على فقرات وأبعاد ومجالات البحث. ويرى الباحثون أن هذا يشير بدوره إلى الدور الذي تقوم به المستشفى من جهة المحاضرات والدورات التدريبية والبرامج التوعوية حول سياسات أمن المعلومات السيبراني من وجهة نظر أفراد عينة البحث.

أما الفقرة الأولى من فقرات البعد والتي تنص على "تصدر المستشفى نشرات تثقيفية دورية عن أهمية أمن المعلومات السيبراني." جاءت في المرتبة الأخيرة من حيث قيمة الوسط الحسابي حيث بلغ الوسط الحسابي لهذه الفقرة (3.68 من 5.0) بوزن نسبي 74 %، وتشير هذه القيمة لوجود درجة مرتفعة من الموافقة على هذه الفقرة وذلك من وجهة نظر أفراد عينة البحث.

ويرى الباحثون أن ذلك يعود إلى أن المستشفيات بحاجة لإعطاء اهتمام أكبر في الجانب التثقيفي من ناحية نشر النشرات الدورية والمعلومات المحدثّة عن آخر ما توصل إليه العلم في مجال الأمن السيبراني، حيث اتضح للباحثين أثناء الدراسة الاستطلاعية التي قاموا بها أن الجانب الإعلامي والتثقيفي المحدث بحاجة للمزيد من الاهتمام والتوعية والارشادات المستمرة في هذا الجانب كي يبقى العاملون على اطلاع دائم ومستمر في هذا المجال.

وبلاحظ من خلال الجدول السابق أيضاً أن قيم اختبار (T) للتحقق من أن متوسط الإجابات يزيد عن القيمة (3) (التي تعبر عن الموقف الحيادي لأفراد العينة أم لا، كانت جميعها ذات دلالة إحصائية عند مستوى 0.05 حيث أن قيمة 0.000 (Sig)، وكانت جميع المتوسطات تزيد عن الدرجة الحيدانية (3)، ويشير ذلك إلى أن متوسط الإجابة على كل فقرة من فقرات البعد تزيد عن القيمة (3) زيادة جوهرية وذات دلالة إحصائية عند مستوى 0.05، ويشير ذلك لأن موقف أفراد عينة البحث تجاه بعد "التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني" يتجه نحو الموقف الإيجابي.

1. تحليل النتائج المتعلقة بالمجال الثاني " فاعلية الأنظمة التقنية في القطاع الصحي "

فيما يلي عرض لأهم نتائج التحليل الإحصائي لفقرات المجال الثاني الذي يمثل المتغير التابع ضمن هذا البحث " فاعلية الأنظمة التقنية في القطاع الصحي "، حيث تم حساب الوسط الحسابي و الانحراف المعياري والوزن النسبي لكل فقرة من فقرات المجال ومن ثم حساب المتوسط الحسابي العام و الانحراف المعياري والوزن النسبي للدرجة الكلية للمجال، كما تم التحقق من مساواة متوسطات الإجابة على فقرات البعد للقيمة (3) التي تعبر عن الدرجة الحيادية باستخدام اختبار (One Sample T-Test).

جدول رقم (21) : يوضح نتائج التحليل المتعلقة بفقرات المجال

م	الفقرة	المتوسط الحسابي	الانحراف المعياري	الوزن النسبي	قيمة اختبار t	القيمة الاحتمالية sig	الترتيب
1	تتوفر الوسائل الكافية لحماية الأنظمة التقنية في المستشفى من التلف أو التخريب	3.87	0.39	77%	17.3	0.00	5
2	تحتوي الأنظمة التقنية في المستشفى على مميزات تعمل على حماية المعلومات وتقليل الأخطاء.	3.88	0.59	78%	11.7	0.00	4
3	تتوفر القدرة لدى الأنظمة التقنية في المستشفى على إثبات التصرفات الخاصة بتهديد أو تسريب المعلومات	3.58	0.74	72%	6.1	0.00	9
4	تقدم الأنظمة التقنية في المستشفى معلومات آمنة ودقيقة.	3.98	0.50	80%	15.1	0.00	1
5	توفر الأنظمة التقنية في المستشفى معلومات ملائمة وتلي متطلبات العمل.	3.90	0.57	78%	12.2	0.00	2

6	تحسين الأنظمة التقنية في المستشفى من انتاجية العمل في المستشفى.	3.68	0.70	74%	7.6	0.00	8
7	توفر الأنظمة التقنية في المستشفى المعلومات اللازمة في الزمن والوقت المناسبين.	3.75	0.68	75%	8.5	0.00	7
8	تعطي المستشفى صلاحيات الدخول للأنظمة التقنية حسب المستوى الإداري.	3.5	0.81	70%	5.6	0.00	10
9	تقوم المستشفى بتحديث الأنظمة التقنية و صيانتها بشكل مستمر.	3.89	0.44	78%	15.9	0.00	3
10	توجد دائرة مستقلة للأنظمة التقنية في المستشفى.	3.83	0.74	77%	8.7	0.00	6
الدرجة الكلية للبعد		3.786	0.62	76%	10.9	0.00	

يستعرض الباحثون فيما يلي النتائج المتعلقة بالمجال الثاني وهو "فاعلية الأنظمة التقنية في القطاع الصحي"، وبناء على ذلك فإنه تم استعراض نتائج كل أبعاد المجال الثاني وهو (فاعلية الأنظمة التقنية الصحية).

أ. النتائج المتعلقة بالبعد " فاعلية الأنظمة التقنية الصحية. "

أن الفقرة الرابعة التي تنص على " تقدم الأنظمة التقنية في المستشفى معلومات آمنة ودقيقة." جاءت في المرتبة الأولى من حيث قيمة الوسط الحسابي التي بلغت (3.98 من 5)، بوزن نسبي 80 % ويشير ذلك لوجود درجة مرتفعة جداً من الموافقة على هذه الفقرة من قبل أفراد عينة البحث، وذلك تبعاً للجدول السابق . والذي يوضح مستويات الموافقة على فقرات وأبعاد ومجالات البحث. ويرى الباحثون أن هذا يشير بدوره إلى طبيعة وفعالية الدور الذي تقوم به الأنظمة التقنية في المستشفى من جهة تقديم المعلومات والأمن والبيانات الدقيقة التي تخص العاملين وأصحاب المصلحة من وجهة نظر أفراد عينة البحث.

أما الفقرة الثامنة من فقرات البعد والتي تنص على " تعطي المستشفى صلاحيات الدخول للأنظمة التقنية حسب المستوى الإداري." جاءت في المرتبة الأخيرة من حيث قيمة الوسط الحسابي حيث بلغ الوسط الحسابي

لهذه الفقرة (3.5 من 5) بوزن نسبي 70 %، وتشير هذه القيمة لوجود درجة مرتفعة من الموافقة على هذه الفقرة وذلك من وجهة نظر أفراد عينة البحث.

ويرى الباحثون أن ذلك يعود إلى أن المستشفيات بحاجة لإعطاء صلاحيات الدخول للأنظمة التقنية حسب المستويات الإدارية، حيث اتضح للباحثين أثناء الدراسة الاستطلاعية التي قاموا بها أن جانب صلاحيات الدخول للأنظمة بحاجة للمزيد من القيود وضبط الصلاحيات كي يبقى نظام الضبط والسيطرة على النظام بشكل أقوى . ويلاحظ من خلال الجدول السابق أيضاً أن قيم اختبار (T) للتحقق من أن متوسط الإجابات يزيد عن القيمة (3) (التي تعبر عن الموقف الحيادي لأفراد العينة أم لا، كانت جميعها ذات دلالة إحصائية عند مستوى 0.05 حيث أن قيمة 0.000 (Sig) ، وكانت جميع المتوسطات تزيد عن الدرجة الحيادية (3) ، ويشير ذلك إلى أن متوسط الإجابة على كل فقرة من فقرات البعد تزيد عن القيمة (3) زيادة جوهرية وذات دلالة إحصائية عند مستوى 0.05 ، ويشير ذلك لأن موقف أفراد عينة البحث تجاه بعد " فاعلية الأنظمة التقنية الصحية " يتجه نحو الموقف الإيجابي .

ثالثاً: اختبار ومناقشة فرضيات البحث

يستعرض الباحثون فيما يلي نتائج اختبار الفرضيات الرئيسية للبحث، بالإضافة للفرضيات الفرعية. حيث أن الفرضية الأولى تختبر وجود علاقة ذات دلالة إحصائية بين المتغير المستقل (سياسات إطار الأمن السيبراني وفاعلية الأنظمة التقنية في مستشفيات القطاع الصحي) بأبعاده الاثنين، والمتغير التابع (فاعلية الأنظمة التقنية). أما الفرضية الثانية تختبر وجود فروق ذات دلالة إحصائية بين استجابات المبحوثين على مجالي سياسات الأمن السيبراني وفاعلية الأنظمة التقنية.

الفرضية الرئيسية الأولى:

تنص الفرضية الرئيسية الأولى على "يوجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين سياسات إطار الأمن السيبراني وفاعلية الأنظمة التقنية في مستشفيات القطاع الصحي في المملكة". ويتفرع من هذه الفرضية فرضيات فرعية، وقد تم التحقق من صحتها من خلال حساب معامل ارتباط بيرسون لقياس العلاقة بين أبعاد المجال الأول " سياسات إطار أمن المعلومات السيبراني.

من ناحية إحصائية، فإنه يتم اختبار الفرضية العدمية (H_0) التي تفترض عدم وجود علاقة ذات دلالة إحصائية، مقابل الفرضية البديلة (H_1) التي تفترض وجود علاقة ذات دلالة إحصائية، ويتم الحكم على نتيجة الاختبار بناءً على قيمة مستوى الدلالة المحسوبة للاختبار (Sig)، كما يلي:

- في حال كانت قيمة (Sig) أقل من مستوى 0.05، يتم رفض الفرضية العدمية والتوصل لصحة الفرضية البديلة، ويقال عندها أن الاختبار معنوي، ويعني ذلك وجود علاقة حقيقية وذات دلالة إحصائية.

- في حال كانت قيمة (Sig) أعلى من 0.05، يتم قبول الفرضية العدمية، ويعني ذلك عدم وجود علاقة ذات دلالة إحصائية.

وفيما يلي نتائج اختبار الفرضية الرئيسية الأولى والفرضيات الفرعية التابعة لها للتحقق من وجود علاقة بين المتغيرات المستقلة (تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني، التدريب والتوعية بتحديات سياسات أمن المعلومات السيبراني) والمتغير التابع المتمثل في "فاعلية الأنظمة التقنية في القطاع الصحي".
أ. بالنسبة للفرضية الفرعية الأولى:

"يوجد علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني و فاعلية الأنظمة التقنية في القطاع الصحي في المملكة".

بلغ معامل ارتباط بيرسون بين المتغير المستقل "تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني" والمتغير التابع "فاعلية الأنظمة التقنية في القطاع الصحي في المملكة"، ($r = 0.439$) وكان هذا الارتباط دال إحصائياً عند مستوى 0.05 حيث بلغت قيمة الدلالة المحسوبة ($\text{Sig} = 0.000$)، ويشير ذلك لوجود علاقة ذات دلالة إحصائية بين تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني و فاعلية الأنظمة التقنية في القطاع الصحي في المملكة. وبذلك يستنتج الباحثون رفض الفرضية العدمية وقبول الفرضية البديلة (H_1) التي تفترض "وجود علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني و فاعلية الأنظمة التقنية في القطاع الصحي في المملكة"، وهذه النتيجة تتفق مع فرضية الباحثين.

جدول رقم (22) : يوضح ارتباط بيرسون بالمتغير التابع.

المتغير التابع			المتغير المستقل
فاعلية الأنظمة التقنية في القطاع الصحي في المملكة			تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني
مستوى الدلالة (Sig.)	معامل ارتباط بيرسون (r)	عدد الاجابات	
0.000	*0.439	60	

يعزو الباحثون ذلك إلى ضرورة اهتمام الإدارة العليا ودعمها لسياسات الأمن السيبراني في المستشفيات من خلال دعم انشاء اطار لهذه السياسات، وتطبيقها وتطويرها باستمرار ، حيث أن ذلك يضمن اهتمام العاملين بها، وهذا ينعكس بشكل إيجابي على اهتمام إدارة المستشفيات بالأنظمة التقنية والسعي نحو زيادة فاعلية هذه النظم، من خلال تطوير قدرات هذه النظم وتوفير كافة سبل الحماية المناسبة لها.

أ. بالنسبة للفرضية الفرعية الثانية:

"يوجد علاقة ذات دلالة احصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني و فاعلية الأنظمة التقنية في القطاع الصحي في المملكة".

بلغ معامل ارتباط بيرسون بين المتغير المستقل " التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني" والمتغير التابع " فاعلية الأنظمة التقنية في القطاع الصحي في المملكة "، ($r = 0.580$) وكان هذا الارتباط دال إحصائياً عند مستوى 0.05 حيث بلغت قيمة الدلالة المحسوبة ($\text{Sig} = 0.000$)، ويشير ذلك لوجود علاقة ذات دلالة إحصائية بين التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني و فاعلية الأنظمة التقنية في القطاع الصحي في المملكة. وبذلك يستنتج الباحثون رفض الفرضية العدمية وقبول الفرضية البديلة (H1) التي تفترض "وجود علاقة ذات دلالة احصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني و فاعلية الأنظمة التقنية في القطاع الصحي في المملكة"، وهذه النتيجة تتفق مع فرضية الباحثين.

جدول رقم (23) علاقة المتغير التابع بمعمل ارتباط بيرون

المتغير التابع			المتغير المستقل
فاعلية الأنظمة التقنية في القطاع الصحي في المملكة			
مستوى الدلالة (Sig.)	معامل ارتباط بيرسون (r)	عدد الاجابات	التدريب والتوعية بتحديثات سياسات أمن المعلومات السبراني
0.000	*0.580	60	

يرى الباحثون أنه لكي تقوم الأنظمة التقنية بتحقيق أهدافها وتكون فعالة، يجب أن تتوفر لديها كافة الوسائل لحماية بياناتها وأنظمتها التقنية، ويجب أن توفر بوابات آمنة ودقيقة للمستخدمين وهذا يتطلب أن تكون المستشفيات على علم مسبق ودراسة واسعة لكافة المخاطر التي يمكن أن تتعرض لها هذه الأنظمة، وكيفية التعامل مع هذه المخاطر في حال حدوثها.

ومن خلال ما سبق يمكن التوصل إلى صحة الفرضية الأولى للبحث والتتفرض "وجود علاقة ذات دلالة احصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين سياسات إطار أمن المعلومات السبراني فاعلية الأنظمة التقنية في القطاع الصحي في مستشفيات المملكة"، وهذه النتيجة تتفق مع فرضية الباحثين.

يعزو الباحثون ذلك إلى أهمية سياسات الأمن السبراني بكافة أبعادها، ودورها الكبير في الحفاظ على أمن وسلامة النظم التقنية، وتقليل المخاطر الأمنية التي يمكن أن تتعرض لها هذه النظم، كما وتعمل سياسات الامن السبراني كمرشد للعاملين توجهم نحو الاستخدام الصحيح لنظم الامن السبرانية بما يضمن سلامة أنظمة المستشفى ويضمن توفير معلومات وبيانات آمنة ملائمة ودقيقة.

الفصل السادس

النتائج والتوصيات

أولاً: النتائج

ثانياً: التوصيات

ملخص الفصل السادس

المراجع

الملاحق.

مقدمة

بناءً على المفاهيم والجوانب المتعددة التي تناولها البحث في الإطار النظري وأدبيات البحث حول سياسات الأمن السيبراني وعلاقتها بفاعلية الأنظمة التقنية في القطاع الصحي – المملكة العربية السعودية، إضافة إلى ما جمعه من بيانات من خلال الاستبانة، وبعد نتائج التحليل الإحصائي لمجالات البحث وأبعاده، وتفسير هذه النتائج وربطها بالدراسات السابقة، خلص البحث إلى مجموعة من النتائج والتوصيات كما يظهر في هذا الفصل.

أولاً: النتائج

خلص البحث لمجموعة من النتائج، وهي كما يلي:

1. أظهرت نتائج البحث وجود علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين سياسات الأمن السيبراني وفاعلية الأنظمة التقنية في القطاع الصحي – المملكة العربية السعودية. حيث أشارت النتائج لوجود علاقة طردية بين سياسات الأمن السيبراني بأبعاده المختلفة (تقدير الإدارة العليا مخاطر الأمن السيبراني، التدريب والتوعية بتحديثات سياسات الأمن السيبراني)، و فاعلية الأنظمة التقنية في القطاع الصحي، أي أن الاهتمام بسياسات الأمن السيبراني بأبعاده يساهم في زيادة فاعلية النظم التقنية في مستشفيات المملكة بشكل إيجابي.

2. أظهرت نتائج البحث اهتمام المستشفيات في المملكة بسياسات الأمن السيبراني بأبعاده المختلفة، حيث اتضح ذلك من خلال حصول مجال (قيام المستشفى بتحديث طرق حماية معلوماتها تبعاً للتغيرات الحاصلة في بيئة التكنولوجيا) على وزن نسبي (80%) مما يدل على اتخاذ المستشفيات الإجراءات اللازمة بحماية أنظمتها ومعلوماتها التقنية.

3. أشارت النتائج اهتمام المستشفيات بوضع التدابير الاحتياطية المستقبلية التي تحد من مستوى تعرض أنظمتها التقنية للخطر، إلا أن هذه البرامج بحاجة لمزيد من الاهتمام والتطوير، حيث حصل هذا البعد على المرتبة الأخيرة بين أبعاد سياسات الأمن السيبراني بوزن نسبي (72%) مما يدل على أهمية توقع المخاطر المستقبلية وأخذ الإجراءات والتدابير المناسبة لمكافحتها.

4. بينت النتائج اهتمام المستشفيات بموضوع التدريب والتثقيف للعاملين في مجال الأمن السيبراني، حيث اتضح ذلك من خلال حصول مجال (تنفذ المستشفى محاضرات تدريب وتوعية إلزامية للعاملين حول سياسات أمن

المعلومات) على وزن نسبي (79%) مما يدل على اهتمام المستشفيات بالارتقاء بالكادر المختص في مجال الأمن السيبراني .

5. وأظهرت نتائج البحث باهتمام المستشفيات بإصدار نشرات تثقيفية دورية عن أهمية أمن المعلومات السيبراني ، إلا أن هذا البرنامج بحاجة إلى مواكبة مستمرة لنشر آخر الأخبار و التحديثات المتعلقة في هذا الجانب حيث حصل على المرتبة الأخيرة بين أبعاد البعد الثاني وهو " التدريب والتوعية بتحديثات سياسات أمن المعلومات السيبراني " بوزن نسبي 74% .

6 . بينت النتائج اهتمام المستشفيات بتقديم الأنظمة التقنية في المستشفى معلومات آمنة ، وذلك لضمان الحفاظ على النظم التقنية وتطبيقها وبياناتها ، حيث حصلت على وزن نسبي (80 %)، وهذا سيؤثر إيجابياً على فاعلية الأنظمة التقنية.

7. أشارت النتائج اهتمام المستشفيات في مجال احتواء الأنظمة التقنية في المستشفى على مميزات تعمل على حماية المعلومات وتقليل الأخطاء ، حيث حصلت على وزن نسبي قدرة (78 %)، ويدل ذلك على مواكبة المستشفيات للتطورات التكنولوجية المتسارعة، ومحاولتها الدائمة للتأكد من تكامل وجودة السياسات وتوافقها مع التغيرات المختلفة.

8 . توصلت النتائج لوجود اهتمام في مجال اعطاء المستشفى صلاحيات الدخول للأنظمة التقنية حسب المستوى الإداري ، حيث حصلت على وزن نسبي (70 %) وهذا يدل على الحاجة بإجراء المزيد من القيود على صلاحيات الدخول للأنظمة التقنية حسب المستوى الإداري وذلك تحسباً لمنع أي ثغرة لاختراق تلك النظم.

ثانياً: التوصيات

بناءً على النتائج التي توصل إليها البحث، يقترح الباحثون فيما يلي عدداً من التوصيات التي تتعلق بالتعامل مع سياسات الأمن السيبراني، بالإضافة إلى بعض الجوانب التي تساهم في رفع فاعلية الأنظمة التقنية في المستشفيات السعودية، وفقاً لرؤى سليمة:

1. زيادة دعم الإدارة العليا الدعم لإنشاء وتطبيق سياسات الأمن السيبراني، لما له من أثر إيجابي على رفع فاعلية الأنظمة التقنية.

2. وجود دائرة متخصصة بالأمن السيبراني في المستشفيات، وتعيين عاملين متخصصين في مجال الأمن السيبراني.

3. تعزيز العمل المستمر والدوري على تقدير المخاطر والتهديدات المحتملة التي يمكن أن تواجه معلومات المستشفيات وأنظمتها التقنية وبياناتها، لإمكانية وضع التدابير اللازمة لذلك.

4. الاهتمام بصياغة إطار لسياسات الأمن السيبراني بناءً على نتائج عملية تقدير مخاطر الأمن السيبراني، وقبل حصول أي مشاكل تخص الأنظمة التقنية في المستشفى.

5. العمل على توثيق سياسات الأمن السيبراني، وتوزيعها على كافة العاملين الذين يستخدمون نظم المعلومات الإدارية بالمستشفى، بالإضافة للعاملين في وحدات ومراكز تكنولوجيا المعلومات.

6. زيادة الاهتمام بدورات التدريب والتوعية للعاملين الذين يستخدمون الأنظمة التقنية بالمستشفى وللعاملين في وحدات ومراكز تكنولوجيا المعلومات حول سياسات الأمن السيبراني وأهميتها والعوامل المؤثرة على نجاح تطبيقها.

7. تعزيز الاهتمام بتوفير ميزانية مخصصة لتطبيق سياسات الأمن السيبراني بكافة مراحلها.

8. اتخاذ سياسات الأمن السيبراني المكتوبة والمعتمدة من الإدارة العليا كمرجع رئيسي عند حدوث أي مشاكل تخص الأمن السيبراني في المستشفى، وعدم الاكتفاء بالتعليمات والضوابط الإلكترونية.

9. فرض تنفيذ سياسات الأمن السيبراني على العاملين في وحدات ومراكز تكنولوجيا المعلومات، بالإضافة للعاملين الذين يستخدمون الأنظمة التقنية بالمستشفى، وتحديد العقوبات بحق من يخالفها.

10. العمل على تحديد جهة معروفة وواضحة لدى العاملين تكون مسئولة عن سياسات الأمن السيبراني في المستشفى.

11. القيام بعمليات مراجعة وتحديث لسياسات الأمن السيبراني بشكل دوري، وكذلك عند حدوث مشاكل تخص الأمن السيبراني في المستشفى.

- 12 . إعلام العاملين بأي تحديثات تطرأ على سياسات الأمن السيبراني .
- 13 . جعل الالتزام بتطبيق سياسات الأمن السيبراني أحد عوامل تقييم أداء العاملين في المستشفى.
- 14 . زيادة الاهتمام بقياس فاعلية الأنظمة التقنية في المستشفيات بشكل دوري، للعمل على تحسين هذه الفاعلية باستمرار.
- 15 . العمل على توفير مراكز للدعم الفني للرجوع إليها في حال حدوث أعطال في الأنظمة التقنية بالمستشفى.
- 16 . إعطاء المزيد من الاهتمام بالتطورات التكنولوجية الحديثة فيما يخص الأمن السيبراني والأنظمة التقنية ، ومحاولة دمج هذه التطورات في المستشفيات .
- 17 . لفت انتباه الباحثين لإجراء المزيد من الأبحاث حول سياسات الأمن السيبراني ومدى تأثيرها على النظم التقنية .

الدراسات المستقبلية المقترحة

بناءً على إطلاع الباحثين على الإطار النظري، والدراسات السابقة، وتحليلها ومناقشتها لنتائج هذا البحث وتحليل بياناته، فهي توصي ببعض الدراسات المستقبلية المقترحة التالية:

- 1 . الثقافة التنظيمية وعلاقتها بسياسات الأمن السيبراني في المستشفيات الحكومية داخل المملكة.
- 2 . سياسات الأمن السيبراني ودورها في تقليل المخاطر الإلكترونية في المستشفيات الحكومية في المملكة.
- 3 . فاعلية الأنظمة التقنية المحوسبة وأثرها على إدارة المخاطر الإلكترونية في المستشفيات الحكومية في المملكة العربية السعودية.
- 5 . أثر برامج التدريب والتوعية بالأمن السيبراني على فاعلية الأنظمة التقنية في المستشفيات الحكومية في قطاع الصحة داخل المملكة.
- 6 . أثر الأنظمة التقنية المحوسبة على أداء المستخدمين في المستشفيات الحكومية في قطاع الصحة داخل المملكة.

ملخص الفصل السادس

استعرض الباحثون في هذا الفصل النتائج التي توصلوا إليها بناء على نتائج التحليل الإحصائي، حيث أشارت النتائج لوجود درجة مرتفعة من الموافقة على كافة أبعاد سياسات الأمن السيبراني، إضافة لوجود درجة مرتفعة من الموافقة على مجال فاعلية الأنظمة التقنية. وبينت النتائج وجود علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين سياسات الأمن السيبراني وفاعلية الأنظمة التقنية في مستشفيات القطاع الصحي داخل المملكة

.واقترح الباحثون مجموعة من التوصيات المتعلقة بموضوع البحث.

وفي ختام الفصل اقترح الباحثون مجموعة من العناوين لدراسات مستقبلية مقترحة بخصوص سياسات الأمن

السيبراني والأنظمة التقنية لقطاع الصحة داخل المملكة.

المراجع

المراجع العربية :

- أسامة ، ربيع. (2007). التحليل الإحصائي باستخدام برنامج SPSS – الجزء الأول. ط 2 (المجلد ط2). مصر: كلية التجارة - جامعة المنوفية.
- ايناس ابراهيم الشيتي. (2019). تقييم سياسات أمن وخصوصية المعلومات في المؤسسات. القصيم: رسالة ماجستير - جامعة القصيم.
- خالد سليمان الغنير، و أمل ناصر الصبيح. (2012). ح ال أمن المعلومات السيبراني في المملكة العربية السعودية. مجلة دراسة المعلومات، الصفحات 189-205.
- دراسة المعهد العربي للتخطيط "مخاطر الهجمات الالكترونية (السيبرانية) وأثارها الاقتصادية. (2019). دراسة حالة دول مجلس التعاون الخليجي.
- رائد محمد عبد ربه. (2013). مبادئ نظم المعلومات الادارية (المجلد ط1). عمان - الاردن: الجنادرية للنشر والتوزيع.
- زياد الجرجاوي. (2010). القواعد المنهجية لبناء السبتيان (المجلد ط2). فلسطين: مطبعة أبناء الجراح.
- زياد محمد الشرمان. (2004). مقدمة في نظم المعلومات الادارية. عمان - الاردن: دار صفاء للنشر والتوزيع.
- سمير بارة. (2017). الأمن السيبراني في الجزائر السياسات والمؤسسات. الجزائر: المجلة الجزائرية للأمن السيبراني.
- سيد تعلق. (2011). نظم المعلومات الادارية (المجلد ط1). عمان - الاردن: دار الفكر.
- عبد الإله محمد النوايسة، و ممدوح حسن العدوان. (2019). جرائم التجسس الإلكتروني في التشريع الأردني. عمان - الأردن: الجامعة الأردنية.
- عبد الرحمن بن جاد العتيبي. (2017). دور الأمن السيبراني في تعزيز الأمن الإنساني ، أطروحة ماجستير. جامعة نايف العربية للعلوم الأمنية ، كلية العلوم الاستراتيجية.
- عبد الرحمن عبيدات، عبد الحق ذوقان، و كايد عدس. (2001). البحث العلمي- مفهومه وأدواته. عمان- الاردن: دار الفكر للنشر والتوزيع.
- عبد الرحمن نبي، الغنير عرفان، و خالد مرزا. (2010). دراسة عملية حول أمن المعلومات السيبراني في المنظمات السعودية. (مركز التميز لأمن المعلومات) السعودية: جامعة الملك سعود.

- عزت عبد الحميد حسن. (2011). الإحصاء النفسي والتربوي: تطبيقات باستخدام برنامج spss. مدينة نصر - القاهرة - مصر: دار الفكر العربي.
- محمد القرشي. (2011). قياس كفاءة سياسات أمن المعلومات - دراسة حالة على شركة في الامارات العربية المتحدة. ستوكهولم السويد: جامعة ستوكهولم.
- محمد حسن السيد. (2006). الخصائص السيكمومترية لأدوات القياس في البحوث النفسية والتربية باستخدام spss. السعودية: كلية التربية - جامعة الملك سعود.
- محمد عبد حسين الطائي. (2004). نظم المعلومات الادارية المتقدمة (المجلد ط1). عمان - الاردن: دار وائل للنشر والتوزيع.
- منصور سعيد القحطاني. (2008). مهددات الأمن المعلوماتي وسبل مواجهتها دراسة مسحية على منسوبي الحاسب الآلي بالقوات البحرية الملكية السعودية بالرياض. الرياض: كلية الدراسات العليا - جامعة نايف العربية للعلوم الأمنية - رسالة ماجستير غير منشورة.
- منى الأشقر جبور. (2016). السبرانية هاجس العصر. بيروت: جامعة الدول العربية - المركز العربي للبحوث القانونية والقضائية.
- موفق الحمداني. (2006). مناهج البحث العلمي. عمان - الأردن: مؤسسة الوراق للنشر.
- نورة شلوش. (2018). القرصنة الإلكترونية في الفضاء السيبراني التهديد المتصاعد لأمن الدول. بغداد - العراق: مجلة مركز بابل للدراسات الإنسانية.
- يوسف بوغراة. (2018). الأمن السيبراني: الاستراتيجية الجزائية للأمن والدفاع في الفضاء السيبراني. مجلة الدراسات الافريقية وحوض النيل.

— المراجع الأجنبية :

- Doherty, N. F., & Fulford, H. (2006). *Aligning the information security policy with the strategic information systems plan*. Computers & Security.
- Hadjor, G., & Gadasu, E. (2014). *The Influence of Organizational Culture on Information Security Policy Success*. Lulea. Sweden: Lulea University of Technology.
- Knapp, K. F. (2012). Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations. *Journal of Management & Policy Practic*, 5, pp. 66 – 80.

المواقع الإلكترونية :

- عبد الرحمن عاطف ابو زيد. (2019, 4 6). الأمن السيبراني في الوطن العربي. تم الاسترداد من المركز العربي للبحوث والدراسات: <http://www.acrseg.org/list.aspx?r=24734>
- <https://ab7as.net/>
- <https://www.mah6at.net>. (2018) .
- <https://www.mah6at.net> (2018) .
- <https://political-encyclopedia.org/dictionary/> (2018). تم الاسترداد من الموسوعة السياسية:

الملاحق



السادة الأفاضل/ العاملون في مجال الأمن السيبراني في القطاع الصحي حفظكم الله ورعاكم ،،،

السلام عليكم ورحمة الله وبركاته ،،،

الموضوع: المشاركة في تعبئة الاستبانة

نتشرف نحن الباحثين أننضع بين أيديكم استبانة لإجراء بحث بعنوان:

دراسة مسحية لتطبيق إطار الأمن السيبراني وتأثيرها على الأنظمة التقنية في القطاع الصحي -المملكة العربية السعودية

وذلك استكمالاً لمتطلبات الحصول على درجة الماجستير في كلية الإدارة من جامعة الجميع الذكية .

يشتمل مجتمع البحث جميع العاملين في وحدات ومراكز تكنولوجيا المعلومات، بالإضافة للعاملين الذين يستخدمون نظم المعلومات الإدارية أثناء عملهم اليومي في الأقسام والدوائر الإدارية في القطاع الصحي. لذا أرجو التكرم من سيادتكم بقراءة كل عبارة من عبارات الاستبانة، ثم وضع علامة (x) في الخانة التي تمثل وجهة نظركم نحو ما هو قائم بالفعل وفق تدرج خماسي (موافق بشدة، موافق، محايد، غير موافق، غير موافق بشدة). علماً بأن إجاباتكم سيتم معالجتها بسرية تامة ولأغراض البحث العلمي فقط. مع العلم بأن سياسات أمن المعلومات: هي مجموعة الإجراءات والقواعد التي تساهم في تعريف المستخدمين بمسؤولياتهم وواجباتهم لضمان أمن وحماية المعلومات في المؤسسات الصحية.

نشكر لكم تعاونكم، ونؤكد لكم أن إجاباتكم تأثيراً مهماً في دقة النتائج وتحقيق أهداف البحث.

وتفضلوا بقبول فائق الاحترام والتقدير،،،

يرجى التكرم باختيار البديل المناسب لكل عبارة من العبارات التالية وذلك بوضع إشارة (x)

القسم الأول: البيانات الشخصية

1. مكان العمل

- ☐ - مدينة الملك سعود الطبية
- ☐ - مستشفى الايمان العام
- ☐ - مستشفى الملك سلمان
- ☐ - مستشفى الامام الفيصل
- ☐ - مستشفى الامير محمد بن عبدالعزيز

2. الجنس

- ☐ ذكر ☐ أنثى

3. المسمى الوظيفي (اختر اجابة واحدة من فضلك)

- ☐ - مدير
- ☐ -مساعد مدير
- ☐ - رئيس قسم
- ☐ - إداري
- ☐ - مبرمج / مصمم
- أخرى (الرجاء التحديد): -----

4. عدد سنوات الخبرة في مجال العمل الحالي :

- ☐ • أقل من 5 سنوات
- ☐ • 5 سنوات - أقل من 10 سنوات
- ☐ • 10 سنوات - أقل من 15 سنة
- ☐ • 15 سنة فأكثر

القسم الثاني : مجالات البحث

م	سياسات إطار أمن المعلومات السيرياني	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تدرك الإدارة العليا مخاطر أمن المعلومات السيرياني					
2	تضع المستشفى التدابير الاحتياطية التي تحد من مستوى تعرض معلوماتها للخطر.					
3	يوجد لدى المستشفى آليات مناسبة لمنع عمليات الوصول غير الشرعية (غير المرخص بها) للبيانات بواسطة العاملين.					
4	تقوم المستشفى بتحديث طرق حماية معلوماتها تبعاً للتغيرات الحاصلة في بيئة التكنولوجيا.					
5	يتوفر لدى المستشفى آليات مناسبة لمنع عمليات الإدخال المتعمدة للبيانات غير السليمة بواسطة العاملين.					
	المجموع					
	التدريب والتوعية بتحديثات سياسات أمن المعلومات السيرياني					
1	تصدر المستشفى نشرات تثقيفية دورية عن أهمية أمن المعلومات السيرياني.					
2	تنفذ المستشفى محاضرات تدريب وتوعية إلزامية للعاملين حول سياسات أمن المعلومات.					
3	يتوافق مضمون ومحتوى البرامج التدريبية الخاصة بأمن المعلومات السيرياني مع بيئة ومتطلبات عمل المستشفى.					
4	تقوم المستشفى بتحديث سياسات أمن المعلومات السيرياني تبعاً للتطورات والتغيرات التكنولوجية العالمية.					
5	تطلعني المستشفى باستمرار على أي تحديث يطرأ على سياسات أمن المعلومات السيرياني.					

فاعلية الأنظمة التقنية في القطاع الصحي						
	فاعلية الأنظمة التقنية الصحية	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تتوفر الوسائل الكافية لحماية الأنظمة التقنية في المستشفى من التلف أو التخريب					
2	تحتوي الأنظمة التقنية في المستشفى على مميزات تعمل على حماية المعلومات وتقليل الأخطاء.					
3	تتوفر القدرة لدى الأنظمة التقنية في المستشفى على إثبات التصرفات الخاصة بتهديد أو تسريب المعلومات					
4	تقدم الأنظمة التقنية في المستشفى معلومات آمنة ودقيقة.					
5	توفر الأنظمة التقنية في المستشفى معلومات ملائمة وتلبي متطلبات العمل.					
6	تحسن الأنظمة التقنية في المستشفى من انتاجية العمل في المستشفى.					
7	توفر الأنظمة التقنية في المستشفى المعلومات اللازمة في الزمن والوقت المناسبين.					
8	تعطي المستشفى صلاحيات الدخول للأنظمة التقنية حسب المستوى الإداري.					
9	تقوم المستشفى بتحديث الأنظمة التقنية و صيانتها بشكل مستمر.					
10	توجد دائرة مستقلة للأنظمة التقنية في المستشفى.					

قائمة المحكمين

م	أسماء المحكمين	التخصص
1	د. ابراهيم عابدين	دكتوراة إدارة الأعمال
2	د. نضال المصري	دكتوراة إدارة الأعمال
3	د. حسن أبو ناصر	دكتوراة إدارة الأعمال
4	د. محمد صويص	دكتوراة إدارة الأعمال
5	د. يوسف الشنتف	دكتوراة إدارة الأعمال

إفادة مشروع تخرج

اسم الطالب: عهد سعيد الرويتع .
رقم الطالب الجامعي: 20223006404 .
حالة الطالب الأكاديمية: مستمر .
تاريخ القبول / فصل القبول: 2022-03-26 .
الجنسية: المملكة العربية السعودية .
رقم الهوية / الإقامة / جواز السفر: 1071699522 .
تفيد إدارة القبول والتسجيل في جامعة الجميع الذكية بالتعاون مع جامعة ميدأوشن بأن الطالب
الموضحة بياناته أعلاه هو أحد طلابها خريجي ماجستير إدارة المخاطر للعام الدراسي 2022/
2023، وأنه قدم مشروع التخرج بعنوان دراسة مسحية لتطبيق إطار الأمن السيبراني وتأثيرها على
الأنظمة التقنية في القطاع الصحي - المملكة العربية السعودية.
وقد أعطي له هذا التعريف بناءً على طلبه لتقديمه لمن يهمة الأمر دون أدنى مسؤولية على الجامعة.



التاريخ - Date
14-04-2023

مدير القبول والتسجيل
Admissions & Registration Manager

س.م.ع.

كتاب تسهيل مهمة باحث

إفادة مشروع تخرج

اسم الطالب: سلطان عواض المطيري .
رقم الطالب الجامعي: 20223006323 .
حالة الطالب الأكاديمية: مستمر .
تاريخ القبول / فصل القبول: 2022-03-13 .
الجنسية: المملكة العربية السعودية .
رقم الهوية / الإقامة / جواز السفر: 1048275877 .
تفيد إدارة القبول والتسجيل في جامعة الجميع الذكية بالتعاون مع جامعة ميدأوشن بأن الطالب
الموضحة بياناته أعلاه هو أحد طلابها خريجي ماجستير إدارة المخاطر للعام الدراسي 2022/
2023، وأنه قدم مشروع التخرج بعنوان دراسة مسحية لتطبيق إطار الأمن السيبراني وتأثيرها على
الأنظمة التقنية في القطاع الصحي- المملكة العربية السعودية.
وقد أعطي له هذا التعريف بناءً على طلبه لتقديمه لمن يهمل الأمر دون أدنى مسؤولية على الجامعة.



التاريخ - Date
20-04-2023

مدير القبول والتسجيل
Admissions & Registration Manager



ملخص الدراسة

لقد هدفت هذه الدراسة إلى تسليط الضوء على إطار سياسات الأمن السيبراني وتأثيرها على فاعلية الأنظمة التقنية في القطاع الصحي داخل مستشفيات المملكة العربية السعودية وفق رؤية المملكة 2030 نحو عمليات التحول الإلكتروني. حيث استخدم الباحثون المنهج "الوصفي التحليلي"، واعتمدت الاستبانة كأداة للبحث، مستخدمين "العينة العشوائية الطبقية" للاستطلاع آراء عينة البحث، والتي بلغت (60) موظفاً وموظفة من العاملين الذين يستخدمون الأنظمة التقنية أثناء عملهم اليومي في المستشفيات والدوائر الإدارية في (مدينة الملك سعود الطبية، مستشفى الايمان العام، مستشفى الملك سلمان، مستشفى الامام الفيصل، مستشفى الامير محمد بن عبد العزيز).

وخلص البحث إلى العديد من النتائج، والتي من أهمها:
- أبدى أفراد عينة البحث وجود درجة مرتفعة من الموافقة على أبعاد مجال "تقدير الإدارة العليا مخاطر أمن المعلومات السيبراني"، حيث حصلت أبعاد هذا المجال مجتمعة على وزن نسبي قدره (77) %.

- أبدى أفراد عينة البحث وجود درجة مرتفعة من الموافقة على مجال "فاعلية الأنظمة التقنية الصحية الموجودة في مستشفيات القطاع الصحي" بوزن نسبي قدره (76) %.

- وجود علاقة ذات دلالة إحصائية عند مستوى دلالة ($\alpha \leq 0.05$) بين إطار سياسات الأمن السيبراني وفاعلية النظم التقنية في مستشفيات القطاع الصحي في المملكة العربية السعودية.

قدم البحث مجموعة من التوصيات، والتي من أهمها:
- دعم المستشفيات لسياسات الأمن السيبراني، بداية من عملية تقدير المخاطر وإنشاء إطار شامل للسياسات وصولاً لمراجعة السياسات وتحديثها باستمرار.

- قياس المستشفيات لفاعلية نظم الأمن السيبراني لديها بشكل دوري.
- العمل على زيادة هذه الفاعلية وتحسينها باستمرار ومراقبة النظم التقنية أيضاً بشكل دائم لسد جميع الثغرات وتأمينها على الدوام.

ABSTRACT

This study aims to highlight the cybersecurity policy framework and its impact on the effectiveness of the technical systems in the health sector within the Kingdom of Saudi Arabia hospitals in accordance with the Kingdom's Vision 2030 towards e-transformation processes. The researchers used the "analytical descriptive" methodology, and adopted the identification as a research tool, using a "class random sample" to survey the sample of research, which amounted to 60 employees and employees who use technical systems during their daily work in hospitals and administrative services (**King Saud Medical City, General El - EMAN Hospital, King Salman Hospital, Imam Al Faisal Hospital, Prince Mohammed Abdulaziz Hospital**).

The research concluded many results, the most important of which are:

- The members of the research sample showed a high degree of approval of the dimensions of the area of "cybersecurity risk assessment of senior management", whereby the dimensions of this area combined gained a relative weight of.%(77)
- The members of the research sample showed a high degree of approval of the field of "effectiveness of health technical systems in health sector hospitals" at a relative weight of.%(76)
- A statistically significant relationship at an indicative level ($\alpha \leq 0.05$) between the cybersecurity policy framework and the effectiveness of technical systems in Saudi Arabia's health sector hospitals.

The research made a series of recommendations, the most important of which are:

- Hospital support for cybersecurity policies, starting from the risk assessment process and the establishment of a comprehensive policy framework to continuously review and update policies.
- Measuring hospitals' effectiveness of their cybersecurity systems periodically.
- Work to increase and continuously improve this effectiveness and also monitor technical systems permanently to fill and ensure all gaps. -Measuring hospitals' effectiveness of their cybersecurity systems periodically, to work to increase and continuously improve this effectiveness and also monitor technical systems permanently to fill and secure all gaps.



A survey study of the application cybersecurity framework and their impact on the health sector - Kingdom of Saudi Arabia

إعداد البحث	الرقم الجامعي
سلطان المطيري (قائد الفريق)	20223006323
عهد سعد الرويتع	20223006404
عبدالله فهد الخرجي	20223006376

اشراف الدكتور

Waleed abdelgawwad

Midocean University

**Imam Shafi'i College of Islamic and Arabic Sciences. s. Box: 6063
Moroni Comoros**

2023 م - 1444هـ