Kingdom of Saudi Arabia
Ministry of Higher Education
King Abdul-Aziz University
Faculty of Economics &
Administration

المملكـة العربيـة السعـوديـة
وزارة التـعليـم العالي
جـامـعـة الملك عبـد الـعـزيـز
شطر الطالبات
كـلـيـة الاقـتـصـاد والإدارة
قسـم الإدارة الـعـامـة

# دور الأمن السيبراني في تحقيق جودة الخدمات الإلكترونية بعمادة تقنية المعلومات بجامعة الملك عبد العزيز "دراسة ميدانية"

إعداد الطالبة

ساره بنت بندر نخيلان الإيداء

1802020

بحث تكميلي لنيل درجة الماجستير في الإدارة العامة

إشراف

د. خديجة بنت محمود زكي

كلية الاقتصاد والإدارة

جامعة الملك عبدالعزيز – جدة

العام الدراسي (1441هـ، 2020م)

**بسم الله الرحمن الرحيم**

**﴿يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ﴾**
**(سورة المجادلة:11)**

# الإهداء

الحمدالله التي تتم بنعمته الصالحات، الحمدالله حمدًا كثيراً طيباً مباركاً فيه.

أهدي بحثي هذا إلى روح أمي الحبيبة/ شيمة سلامة الشعلان محبة العلم فطالما كانت مصدر الإلهام والتحفيز لي دائمًا أسأل الله العظيم أن يجعل الفردوس الأعلى مكانك.

كما أهدي بحثي هذا إلى أمي الثانية الأميرة نوره بنت محمد الكبير على دعمها وتشجيعها لي خلال فترة دراستي فأشكرها من القلب وأسال الله أن يحفظها ويمد بعمرها.

## الشكر والتقدير

يقول الله - سبحانه وتعالى -: ﴿وَلَا تَنْسَوُا الْفَضْلَ بَيْنَكُمْ﴾ البقرة:[237]، وفي حديثٍ لرسول الله - صلى الله عليه وسلم - وإن ضعَّفه البعض - يقول فيه: ((يا عائشة، إذا حَشر الله الخلائقَ يوم القيامة، قال لعبدٍ من عباده اصطَنع إليه عبدٌ من عباده معروفًا: هل شكَرْته؟ فيقول: أي رب، علمتُ أنَّ ذلك منك فشكرتُك عليه، فيقول: لَم تَشْكرني إنْ لم تشكر مَن أجريتُ ذلك على يديه))، وفي رواية أخرى: ((مَن أجريت لك الخير على يديه))، وفي ثالثة: ((من أجريت لك النعمة على يديه)).

وعملاً بهاتين القاعدتين الإلهيتين العظيمتين: "الفضل والشكر"، يلزمني أن أردَّ الفضل والشكر إلى أهلهما؛ أرده أولاً إلى/ **د. خديجة بنت محمود زكي** التي أحاطتني بحبها واحترامها وتقديرها.

اللهم أجزها عني خير الجزاء، واهْدها لأحسن الأعمال؛ فلا يهدي لأحسنها إلا أنت، واصرف عنها سيِّئها، فلا يصرف عنها سيئها إلا أنت، اللهم وسِّع لها في دارها، وبارك لها في رزقها، وأعنها ولا تُعن عليها، وآثرها ولا تؤثر عليها؛ إنك سميعُ الدعاء.

**الباحثة،،،**

***ساره بندر الايداء***

# المستخلص

تهدف هذه الدراسة إلى التعرف على دور الأمن السيبراني في جودة الخدمات الإلكتروني بعمادة تقنية المعلومات بجامعة الملك عبد العزيز؛ ولتحقيق هذا الهدف اعتمدت الدراسة المنهج الوصفي التحليلي، وتكون مجتمع الدراسة من (221) من الموظفين والموظفات بعمادة تقنية المعلومات، واختيرت عينة عشوائية بسيطة مقدارها (150) موظف وموظفة، وتم استخدام الاستبانة كأداة للدراسة، وكانت أهم النتائج التي توصلت إليها الدراسة: يمارس العاملون في عمادة تقنية المعلومات بجامعة الملك عبدالعزيز بُعدي (السرية، الخصوصية) بدرجة مرتفعة، ويمارسون بعد التعزيز بدرجة مرتفعة جداً، أما بُعد جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز فتتميز بدرجة مرتفعة من وجهة نظر العاملين، تبين أن المتغيران المستقلان (الخصوصية، التعزيز) يؤثران في جودة الخدمات الإلكترونية، بينما المتغير المستقل (السرية) لا يؤثر بشكل واضح في جودة الخدمات الإلكترونية، لاتوجد فروق ذات دلالة إحصائية بين متوسطات تقديرات مجتمع الدراسة حول دور الأمن السيبراني في جودة الخدمات الإلكترونية تعزى إلى متغير (المؤهل العلمي، الخبرة العملية)؛ وفي ضوء النتائج التي توصلت إليها الدراسة توصي الباحثة بما يلي: أهمية قيام إدارة الجامعة بمراجعة صلاحيات المستخدمين على فترات منتظمة، وتحسين آليات ضبط الوصول للنظام، ووضع برامج وإجراءات خاصة بالمستويات الإدارية والصلاحيات ضمن النظام والتركيز على ضرورات الأمن السيبراني، كذلك وضع خطة استراتيجية لإدارة المخاطر الأمنية لنظم المعلومات في الجامعة؛ لضمان اكتشاف مبكر للمخاطر، وكيفية الوقاية من المخاطر والتصدي لها إذا وجدت، تقييم المخاطر التي يتعرض لها النظام بشكل مستمر، وتنمية الكوادر البشرية العاملة في مجالات الأمن السيبراني من خلال التوسع في عمليات البحث العلمي وإلحاق العاملين بدورات متخصصة في هذا المجال لرفع كفاءتهم، مع التركيز على العاملين الأقل خبرة حسب نتائج الدراسة، ضرورة تأسيس هيئات علمية لتأهيل وتدريب كوادر وطنية سعودية مختصة في القطاعات الحكومية والأهلية لدعم المجتمع ضد مخاطر الجريمة السيبرانية.

# ABSTRACT

This study aims to identify the role of cyber security in the quality of electronic services at the Deanship of Information Technology at King Abdelaziz University. 150) male and female employees, and the questionnaire was used as a tool for the study, and the most important findings of the study were: The employees of the Deanship of Information Technology at King Abdelaziz University practice after (confidentiality, privacy) to a high degree, and they practice after promotion to a very high degree, the quality of electronic services in the Deanship Information technology at King Abdelaziz University is characterized by a high degree from the point of view of employees, it was found that the two independent variables (privacy, reinforcement) affect the quality of electronic services, while the independent variable (confidentiality) does not clearly affect the quality of electronic services, there are no statistically significant differences Among the average estimates of the study community about the role of cybersecurity in the quality of electronic services, attributed to the variable (educational qualification, practical experience); In light of the findings of the study, the researcher recommends the following: the importance of the university administration reviewing users' powers at regular intervals, improving access control mechanisms to the system, developing programs and procedures for administrative levels and powers within the system, focusing on cybersecurity necessities, and developing a strategic plan for managing security risks The university's information systems, to ensure early detection of risks, how to prevent and respond to risks if any, assess the risks to which the system is exposed on an ongoing basis, and develop human cadres working in the areas of cybersecurity through the expansion of scientific research operations and enrolling workers in specialized courses in this field To raise their efficiency, with a focus on less experienced workers according to the results of the study, the necessity of establishing scientific bodies to qualify and train Saudi national cadres specialized in governmental and private sectors to support society against the dangers of cybercrime.

# قائمة المحتويات

# قائمة الأشكال

# قائمة الجداول

# الفصل الأول

# الإطار العام لدراسة

# الفصل الأول
# الإطار العـام لدراسة

## 1-4 مقدمة

تمكنت التطورات المطردة في التقنية الحديثة أن تكون من أبرز عناصر التطور في الدول المتقدمة، فهي تقوم بدور أساسي في منظمات الأعمال والمؤسسات الحكومية وغيرها من الميادين والمجالات العامة، وهي في الوقت ذاته عاملاً مهمًا لتسيير الأعمال لدى المنظمات الحكومية؛ مما يصعب معه الاستغناء عنها أو العمل بمعزل عنها؛ لما لها من دور في تسهيل الإجراءات وتبسيط التعاملات بين المنظمات، ويتضح تأثيرها على إنجاز متطلبات العمل بالدقة والسرعة والكفاءة العالية.

سادت التعاملات الإلكترونية عن نظيرتها التعاملات الورقية في جميع المجالات، وأضحى الاعتماد بشكل أساس على تقنية المعلومات والاتصالات والتي ترتبط بالشبكات لاسيما الشبكة العالمية (الإنترنت)، وفي خضم ذلك صاحبت هذه التعاملات الإلكترونية مجموعة من المخاطر الناشئة والمحتملة والتي تهدد الشبكات وأمن المعلومات والمجتمع المعلوماتي وأعضائه (توثيق)، مع تعرض الشبكات الإلكترونية إلى عمليات إجرامية تؤثر بشكل سلبًا على سلامة البنية التحتية للمعلومات الحساسة وبالتحديد المعلومات الشخصية وغيرها من البيانات المهمة الخاصة بالأفراد والمجتمعات والمنظمات؛ لذا كان من الأجدر أن يكون هناك نظامًا آمنًا يحمي هذه المعلومات بما يطلق عليه في العصر الحالي بالأمن السيبراني.

"لم يعد مفهوم الأمن بالنسبة للدول محدودًا على الأمن القومي بل أصبح الاهتمام بأمن المعلومات وحمايتها أمرًا ومطلبًا أمنيًا مهمًا للمحافظة على المجتمع والمنظمات والدولة ككل، فالتغيرات والتطورات التي حصلت في العالم أرغمت الدول على الاهتمام الفعلي بالفضاء الإلكتروني" (جلعود،2013،ص38-39)، كما أكد الخبراء في (الهيئة الوطنية للأمن السيبراني،1439هـ) " بأن الأمن السيبراني يعتبر مجالاً أساسيًا من مجالات أي تحول رقمي، فهو يحمي البيانات والبنية التحتية من أي هجمات سيبرانية وخاصة عندما حدث هجوم تقني في العقد السابق، وأصبح مصدر قلق للحكومة وعامة القطاعات الخاصة؛ لذا يجب التصدي لمثل هذه الهجمات ومعالجتها بشكل ذكي ومبتكر، إضافة إلى ذلك تجهيز الموظفين وإعدادهم وتأهيلهم وتثقيفهم بأهمية الأمن السيبراني وكيفية التعامل في حالة حدوث أي مخاطر إلكترونية محتملة وذلك يعد جزءًا أساسيا من حركة التحول الرقمي".

### 1-2 مشكلة الدراسة

"تعد مجالات الاختراق الأمني المعلوماتي من أكثر المواضيع أثارت للجدل والاهتمام من قبل المتخصصين في نظام المعلومات بسبب كونها الأساس في توفير الفرص التي تلائم لحدوث الاختراق" (الطائي والكيلاني، 2015م، ص135).

وقد أثبتت العديد من الدراسات أهمية الأمن السيبراني لحماية المعلومات للمنظمات والمؤسسات والحكومات ومن تلك الدراسات دراسة كاستنر (Kistner, 2006) ودراسة سترنجيني (Stringhini, 2014) ودراسة روجرز وآشفورد ( Rogers &Tina, 2015) والتي اعتبرت الجريمة الإلكترونية تهديداً بارزاً يتزايد في جميع جوانب المجتمع بما في ذلك الشركات والحكومة والبنوك والمواصلات والأفراد، ويعتمد أمن الشبكات على القدرة على التعرف على الهجمات السيبرانية الضارة والدفاع عنها.

### 1-3 أسئلة الدراسة

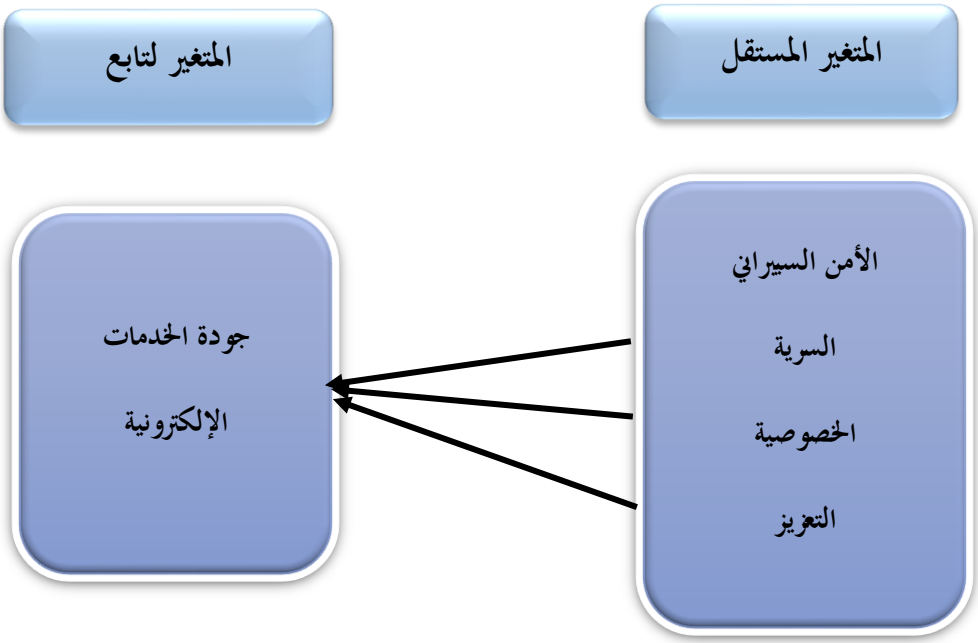
تتمثل مشكلة الدّراسة في محاولة الإجابة عن السؤال الرئيس التالي:

مادور الأمن السيبراني في جودة الخدمات الإلكترونية بعمادة تقنية المعلومات بجامعة الملك عبد العزيز؟

ويتفرع عن هذا السؤال عدة أسئلة فرعية هي:

1. مادور بُعد السرية في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟
2. مادور بُعد الخصوصية في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟
3. مادور بُعد التعزيز في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟
4. ما درجة جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟
5. ما دور الأمن السيبراني من خلال أبعاد (السرية، الخصوصية، التعزيز) في تجويد الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟
6. هل توجد فروق ذات دلالة إحصائية في استجابات عينة الدراسة حول دور الأمن السيبراني بأبعاده (السرية، الخصوصية، التعزيز) تعزى للمتغيرات الديمغرافية (المؤهل العلمي، الخبرة العملية)؟

### 1-4 نموذج الدراسة




**شكل (1) نموذج الدراسة من تصميم الباحثة**

### 1-5 أهمية الدارسة

تبرز أهمية هذه الدراسة في الكشف عن الدور الفعال للأمن السيبراني في جودة الخدمات الإلكترونية كونها تلقي الضوء على حماية الأنظمة الإلكترونية من الهجمات الإلكترونية الرقمية التي تهدف إلى تعطيل الأنظمة وتأخير مسيرتها العلمية، كما توضح أهمية التعزيز الأمني للخدمات الإلكترونية وجودتها، من خلال مستوى الخصوصية والسرية والتعزيز في جامعة الملك عبد العزيز بمحافظة جدة، وتتضح أهمية الدراسة فيما يأتي:

**الأهمية العلميّة:**

1. إطلاع العاملين في المنظمات الحكومية والخاصة على أهم الأبعاد في مجال الأمن السيبراني والتي تعزز الأمن المعلوماتي للمنظمة ولمواجهة الأخطار والجرائم الإلكترونية التي تهدد عملها بشكل متكرر.
2. قد تساعد المعلومات في هذه الدراسة الباحثين في الحصول على مادة علمية وإطارًا نظريًا حول الأمن السيبراني وأبعاده في حماية المنظمات.
3.

**الأهمية العمليّة:**

1. تحدد الدراسة الحالية الدور الذي يقوم به الأمن السيبراني في جودة الخدمات الإلكترونية وتوظيف نتائج الدراسة في مصلحة المنظمات الحكومية على وجه الخصوص.
2. قد تسهم توصيات هذه الدراسة تعزيز الأمن المعلوماتي ضد الجرائم والهجمات الإلكترونية التي تعترض عمل المنظمات.

## 1-6 أهداف للدراسة

تهدف هذه الدراسة إلى:

1. التعرف على دور السرية في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز.
2. التعرف على دور الخصوصية في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز.
3. التعرف على دور التعزيز دور في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز.
4. الكشف عن دور أساسيات الأمن السيبراني (السرية والخصوصية والتعزيز) في تجويد الخدمات الإلكترونية.
5. الكشف عن وجود فروق ذات دلالة إحصائية في استجابات عينة الدراسة حول دور الأمن السيبراني بأبعاده (السرية، الخصوصية، التعزيز) تعزى للمتغيرات الديمغرافية (المؤهل العلمي، الخبرة العملية).
6. التعرف على دور عمل الأمن السيبراني في التعزيز الأمني للخدمات الإلكترونية.

## 1-7 حدود الدراسة

**الحدود الموضوعية:** اقتصرت الدراسة على دراسة دور الأمن السيبراني في جودة الخدمات الإلكترونية.

**الحدود المكانية:** تم تطبيق الدراسة ميدانياً بعمادة تقنية المعلومات بجامعة الملك عبد العزيز.

**الحدود الزمانية:** تم إنجاز هذه الدراسة خلال الفصل الثاني للعام 1441-1442هـ

**الحدود البشرية:** تم تطبيق الدراسة على الموظفين بعمادة تقنية المعلومات بجامعة الملك عبد العزيز.

## 1-8 مصطلحات الدراسة

**الدور**: يُعرف الدور لغة بأنه " الطبقة من الشيء المدار بعضه فوق بعضه، وهو يعني: مهمة ووظيفة "قام بدور/لعب دورًا: أي شارك بنصيب كبير، وجمعها أدوار"(معجم المعاني،2019م)

أما الدور اصطلاحا فأنه يعني ‘‘هي مجموعة توقعات تخص مكانة نسقية بنائية يشغلها الفرد أو أنه سلوك يعكس متطلبات المكانة التي يشغلها الفرد. "(الغزاوي واخرون،1992م، ص258)، ويعرفه (عمر،1991م، ص226) بأنه ممارسات سلوكية تعكس مستلزمات وشروط خاصة به، مصاغة ومفروضة علية من قبل المجتمع "

**الأمن:**

يُعرف الأمن لغة ‘‘الطمأنينة وعدم الفزع، وهو أيضًا الأمان والأمانة بمعنى، قد أمنت فأنأ أمين، وأمنت غيري من الأمان والأمان، والأمن ضد الفزع، والأمانة ضد الخيانة" (معجم المعاني،2019م).

ويعرف الأمن اصطلاحًا بأنه: " السلام والطمأنينة واستمرار مظاهر الحياة ومقوماتها وشروطها، بعيدًا عن أي عامل تهديد ومصادر الخطر" (مراد،2017م، ص12).

ويراه هويدي (1991) "الإجراءات التي تعمل الدول جاهدة في حدود إمكانياتها للحفاظ على كيانها ومصالحها في الحاضر والمستقبل مع مراعاة المتغيرات الإقليمية والدولية"(ص 28).

أما أمين (1991) فيراه: "التخلص من جميع ما يمكن أن يهدد أمن الأفراد والدول، سواءً كان سياسيًا أو اقتصاديًا واجتماعيًا من خلال التركيز على الإصلاح المؤسسي وذلك بإصلاح المؤسسات الأمنية القائمة وإنشاء مؤسسات أمنية جديدة على المستويات المحلية والإقليمية والعالمية مع البحث عن سبل تنفيذ ما هو قائم من تعهدات دولية تهدف إلى تحقيق أمن الأفراد وهو لا يمكن تحقيقه بمعزل عن أمن الدول" (ص21).

في حين يراه عبد الكافي (2016): "حماية أساسيات البقاء بشكل يرتقي من حقوق وحريات البشر" (ص176).

**السيبراني/ السيبرانية:**

السيبرانية لغة: "مأخوذ من كلمة (سيبر) cyber، تعني صفة لأي شيء له علاقة في ثقافة الحواسيب أو التقنية المعلومات أو الواقع الافتراضي، وأن مفهوم السيبراني أو السيبرانية تعني فضاء الإنترنت" (الربيعة، هيئة الاتصالات وتقنية المعلومات،2017، ص 6).

أما في الاصطلاح فيراه إبراهيم، (2011)، "عالم الفضاء المصطنع أي المكان الخالي أو الافتراضي، أو الفضاء المصطنع الإلكتروني، حيث يتم تبادل المعلومات والبيانات في هذا الفضاء المصطنع بطريقة إلكترونية" (ص25)

ويراه الربيعة (2017): " المحافظة على أمن المعلومات والأجهزة وشبكات الحاسب الآلي، والعمليات والأليات التي يتم من خلالها حماية الأجهزة الحاسب الآلي والمعلومات والخدمات من أي تشابك مقصود أو غير مقصود أو غير مصرح به أو تغيير أو اختلاف قد يحدث، حيث يتم استخدام مجموعة من الحماية التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به، ومنع سوء الاستغلال واسترجاع المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها" (ص 6).

كما يراه الشايع (2019): " بأنه مجموعة من الوسائل التقنية والتنظيمية والإدارية المتخذة لتجنب الاستخدام غير المصرح به وسوء استغلال واستعادة المعلومات الإلكترونية وأنظمة الاتصال والمعلومات التي تحتويها وذلك بهدف استمرار وتيسير عمل نظم المعلومات وتعزيز الحماية والسرية والخصوصية البيانات الشخصية واتخاذ جميع التدابير المهمة لحماية الموطنين والمستهلكين من المخاطر في الفضاء السيبراني، وهو أفضل الممارسات والآليات لضمان التكنولوجيات والخدمات التي يمكن استخدامها في حماية البيئة السيبرانية وأصول المؤسسات والمستخدمين"، ويعرفه (الشايع،2019م، ص25) بأنه: "آلية حماية تضمن السرية، أي الملكية التي لم يتم الكشف عن معلومات عنها للأفراد أو الكيانات أو العمليات غير المصرح لهم، كما تتضمن النزاهة أي حماية دقة واكتمال المعلومات وطرق معالجتها، وتتضمن التوافر أي النفاذ وإمكانية الوصول الى المعلومات والأصول المرتبطة بالمستخدمين المرخص لهم حسب الحاجة، وتشمل أيضا الموثوقية أي الكيانات المشاركة في المعالجة، أو الاتصال، ولا ينبغي أن تكون قادرة على رفض تبادل البيانات".

**الجودة:**

الجودة لغة: **جَودة** (اسم)، الجمع (**جَوْدات** وجَوَدات)، مصدر(جَادَ)، عُرِفَ بِجَوْدَةِ صِنَاعَتِهِ بِإِتْقَانِهَا وَطَبِيعَتِهَا الجَيِّدَةِ (معجم المعاني،2019م).

أما اصطلاحا فيراها (حمود،2005م، ص75) "أنظمة تتضمن مجموعة من الفلسفات الفكرية المتكاملة ولأدوات الإحصائية والعملية الإدارية المستخدمة لتحقيق الأهداف ورفع كفاءة مستوى رضا العميل والموظف على حد سواء"، كما عرفها (عبد الفتاح، غنام، الافى،2010م، ص19) بأنها القيام في العمل الصحيح بالشكل السليم ومن أول وهلة مع الاعتماد على التقييم المستمر لعميل في معرفة مدى تحسن الأداء.

**الخدمات الإلكترونية:**

تُعرف الخدمات الإلكترونية لغة "خدمات تكنولوجيا المعلومات التي توصل النتائج الأساسية المرغوبة لدى العميل أو أكثر (معجم المعاني، 2019م).

أما اصطلاحا فتُعرف "تفعيل التطبيقات الإلكترونية الخاصة بمؤسسات القطاعين العام والخاص لتسهيل تناولها بين العملاء خارج تلك المؤسسة وذلك عبر شبكة تواصل إلكترونية"(لهزاني،2008م، ص48)، في حين يراها ابراهيم "تقديم الخدمات العامة التقنية المتكاملة على الخط للأفراد والمنظمات، وإضافة مميزات وقيمة حقيقية يشعر بها هؤلاء المنتفعون بالإضافة إلى تشكل علاقات تفاعلية مع المواطنين أفراد كانوا أو مؤسسات، من خلال تقديم لهم الخدمات غير تقليدية تتناسب مع خصوصية المواطن أو المنظمة الحكومية." (2012م، ص31).

**وسوف تتبنى الباحثة المصطلحات الإجرائية التالية:**

**الدور:**

المهمة أو الوظيفة التي يقوم بها الأمن الســـيبراني لرفع جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز.

**الأمن السيبراني:**

وسيلة تقنية حديثة تقوم بالعمل على حماية الأنظمة التشغيلية والشبكات العنكبوتية من أي هجوم تقني يكون الهدف منه، الوصول الى المعلومات والبيانات الحساسة، أو القيام بتغيرها أو إتلافها أو التجسس؛ وبشكل عام أن الأمن السيبراني هو رادع تقني في الفضاء الإلكتروني من أي تجاوزات غير مرخص بها ،ويقوم الأمن السيبراني بالمحافظة على السرية وخصوصية المعلومات بشكل دقيق وأيضا يعمل الأمن السيبراني على تعزيز أنظمة الحماية من أي هجمات خارجية مستهدفة.

**جودة الخدمات الإلكترونية**

تقديم الخدمات التكنولوجية المتطورة للمستفيدين سواءً من، أفراد، أم مؤسسات حكومية، وخاصة، في منتهى السرعة والدقة، وتقوم هذه الخدمات الإلكترونية على تسهيل إنجاز الخدمات بجودة تقنية عالية.

# الفصل الثاني

# أدبيات الدراسة

# الفصل الثاني
# أدبيات الدراسة

**مقدمة:**

يتناول هذا الفصل الأمن السيبراني ومفهومه والفرق بينه وبين أمن المعلومات وخصائصه واستراتيجياته وأبعاده و جودة الخدمات الإلكترونية، مفهومها ومبادئها الأساسية ومعوقات تطبيقها، كما توضح مقومات بناء تقنيات المعلومات الأمنية، ويمكن عرض هذه المعلومات كما يأتي:

## 2-1 المبحث الأول: الأمن السيبراني

أضحت التطورات المتلاحقة الحاصلة على مستوى المعاملات والخدمات الإلكترونية في ازدياد مستمر ويشهد العالم قفزات هائلة في نظام الاتصالات الرقمي مع استمرار انخفاض تكاليفه؛ مما يؤدي إلى تغيير جذري في طريقة أداء الأفراد والمؤسسات لأعمالهم، وكذلك نموًا كبيرًا في الخدمات الإلكترونية والمالية وجميع الأنظمة، ومع ازدياد التطور والتقدم التكنولوجي تبقى الأنترنت قناة مهمة للعديد من المجالات ومن ذلك مجال الأمن السيبراني الذي يعتمد على التطورات في شبكة الإنترنت.

### 2-1-1 مفهوم الأمن السيبراني

نظرًا للازدهار السريع للتقنية الحديثة؛ ومالها من دور فعال في تقدم الدول ونهضتها، فقد استندت الحكومات والمؤسسات والأفراد على التكنولوجيا المتطورة، وذلك عندما تحولت المنظمات من فكرة الثقافة الورقية إلى الثقافة الإلكترونية في كافة مجالات العمل، ومن خلال ذلك ظهر مجال الأمن السيبراني الذي يعد من أنظمة الحماية الوطنية للأغلب الدول المتقدمة، حيث يقوم بالحماية والمحافظة على المعلومات المهمة والحساسة للأجهزة والأنظمة الحكومية، وفي سياق هذا الموضوع فقد تعددت المفاهيم للأمن السيبراني ومن ذلك تعريف(الشايع، 2019م، ص23) " من الطرق الحديثة التي تستهدف إخفاق ومنع الهجمات على أي نظام حاسوبي و أي معلومات مهمه تكون متضمنة في الأجهزة ،ويستهدف الأمن السيبراني حماية البيانات أو أي شكل من الأصول الرقمية المخزنة في حاسوب لأي جهة أو في أي جهاز يحتوي على ذاكرة رقمية " ، كما عرفه باين Bain بأنه: "مجموعة من الأجهزة والبرامج المصممة لحماية شبكات الاتصال، وبرامج الحاسوب، والبيانات المخزنة من الهجوم، والإتلاف، والاستخدام غير المصرح به" (الشايع، 2019، ص25).

ويراه الخالد: "البيئة الافتراضية التي يتم فيها تبادل المعلومات الرقمية عبر شبكات حاسوبية، ويمكن تصور الفضاء السايبري كمجموعة ضخمة من شبكات الأنظمة الحاسوبية المتصلة مع بعضها، ومثلما تقع حروب تقليدية في عالم الواقع (كالتي تحدث في البر، والبحر والجو والفضاء) تقع حروب افتراضية في الفضاء السايبري تسبب أذى وخسائر قد تضاهي تلك الناتجة عن الحروب التقليدية "(2018، ص199)؛ وتعرف الباحثة الأمن السيبراني بأنه القدرة على حماية الأنظمة التشغيلية والشبكات من أي هجوم إلكتروني لعمل نظام إلكتروني في الفضاء الإلكتروني لصد ومنع التجاوزات غير المرخص بها.

### 2-1-2 أمـــن المعلومات

ذكر (الطائي، والكيلاني، 2015م، ص34) مجموعة من التعريفات لأمن المعلومات ومن ذلك:

- ❖ الحفاظ على المعلومات الحساسة وسلامتها وسريتها وملكيتها للأشخاص المنتفعين بها.
- ❖ هي الاحتفاظ بالمعلومات من أي تشابك عند استخدام أو تخزين معلومات مضللة أو تحريفها أو استبدالها أو سوء تفسيرها أو إلغاؤها أو سوء استخدامها.
- ❖ إصلاح جميع الاختراقات التقنية من قبل مالك المنظمة حتى يتم الحفاظ على المعاملات المهمة والمعلومات لدى المنظمة.
- ❖ حماية المعلومات والتي تشتمل على المنع والكشف والإعاقة والنقل والتحويل والاسترجاع والتصحيح، والإقرار.
- ❖ الإجراءات التي تحقق الحماية من خلال الالتزام بمعايير محددة بشكلٍ سليم وتحديد السلبيات والتهديدات الأمنية الخطيرة.
- ❖ الحماية الدقيقة والتي ما تكون من خلال صياغة ضوابط واضحة ومحددة بشكل سليم للمراقبة الأمنية وتطبيقها بفاعلية في إطار استخدام مجموعة من القواعد الرقابية كإرشادات توجه جهود الحماية.
- ❖ التركيز على حماية المعلومات المنظمة من سوء الاستخدام من قبل الأفراد غير المصرح لهم من خلال تحديد التهديدات التي قد تضر أمن المعلومات وتشخيص نقاط الضعف التي يعاني منها برنامج أمن المعلومات ومن ثم تحديد المخاطر المترتبة على تلك التهديدات واستغلال نقاط الضعف، ووضع سياسة أمن المعلومات وتنفيذ الضوابط والمعايير التي تسهم في تعزيز أمن المعلومات.

### 3-1-2 الفرق بين الأمن السيبراني والأمن المعلوماتي.

وذكر كلا من الشايع (2019، ص21)، والخالد (2018م، ص 20-22) الفرق بين الأمن السيبراني والأمن المعلومات يمكن عرضها في الجدول التالي:

**جدول ( 1) الفرق بين الأمن السيبراني والأمن المعلوماتي**

| م | الأمن السيبراني | أمن المعلومات |
|---|---|---|
| 1 | لا يعترف بالحدود، أي أن الفضاء السيبراني أو الفضاء الإلكتروني، بإمكانه التأثير في أكثر من منطقة جغرافية في وقت واحد. | هو الإطار الفيزيائي الذي يضم المعلومات، ويحفظها، ويعالجها. |
| 2 | الفضاء السيبراني شديد الاتساع وينمو بوتيرة سريعة. | يهتم أمن المعلومات بشكلين وهما محيط المعلومات الكتروني ومحيط غير إلكتروني (يدوي) بمعنى المحيط الإلكتروني يركز على المكان والتجهيزات التي تضم المعلومات الرقمية مثل (نظام حاسوبي)، أما المحيط اليدوي فهو مكان الذي يضم المعلومات الورقية ويحفظها فقط (مثل الخزنة الحديدة) |
| 3 | السرعة، حيث أن الأحداث في الفضاء السيبراني تتسم بسرعة الحدوث والاستجابات. | حدد أمن المعلومات ثلاث أطراف تتعامل معها وهي المالك، والقيم، والمستخدم. |

### 2-1-4 أهداف الأمن السيبراني

ذكر الشايع (2019)، الأهداف التي يحققها الأمن السيبراني والمتمثلة في:

1. حماية الأنظمة التقنية والمعلوماتية من الاختراقات والتهديدات والتجاوزات غير القانونية.
2. التعزيز الأمني لجميع الأصول المعلوماتية والتقنية في كافة الجهات الحكومية.
3. التوعية الأمنية لدى الأفراد والمجتمعات والمؤسسات في أهمية الأمن السيبراني.
4. إعداد جيل في المستقبل ويكون ذلك من خلال، تدريبهم وتطويرهم في مجال الأمن السيبراني.
5. إطلاق التخصصات السيبرانية العلمية والدورات التدريبة في جميع المنظمات التعليمة.
6. "ضمان سرية وسلامة، وتوافر الأنظمة التي تتم فيها معالجة المعلومات " (ص25)
7. تأمين وحماية وسرية البيانات والمعاملات الإلكترونية لكل من الأفراد والمنظمات الحكومية.
8. الردع الأمني من الهجمات التقنية التخريبية.
9. حماية التقنية لبنية التحتية.

### 2-1-5 خصائص الأمن السيبراني

وحددت البدانية خصائص الأمن السيبراني (الشايع،2019، ص 55-57) كما يأتي:

1. **الخصائص التقنية:** وهي البنية التحتية المعلوماتية الوطنية والاستخدام الواسع للأنترنت في كافة مؤسسات المجتمع".
2. **الخصائص الاجتماعية:** وهي التغير الاجتماعي والمشكلات الاجتماعية المعلوماتية.
3. **الخصائص الثقافية:** وهي الثقافة الكونية والعولمة ويعني بذلك "عولمة الأمن ولم يعد تهديد الأمن مشكلة وطنية أو إقليمية بل غدا مشكلة عالمية.
4. **الخصائص السياسية:** وتشمل اللاحدودية والحكومة الإلكترونية.
5. **الخصائص الاقتصادية:** وتشمل الاقتصاد الإلكتروني، والمهن الإلكترونية"

### 2-1-6 استراتيجيات الأمن السيبراني

يتبع الأمن السيبراني استراتيجيات لفعالية وتحقيق الأمن المعلوماتي للأنظمة الإلكتروني، كما أشار لها (الشايع، 2019، ص236-251-271) وهي:

**استراتيجية الردع /الدفاع السيبراني:** تركز هذه الاستراتيجية على الدفاع والردع الأمني من هجمات التقنية التي تستهدف البنية التحتية لتقنية المعلومات من الجرائم السيبرانية من اختراق أو تخريب أو تعطيل للأجهزة والبرمجيات الإلكترونية؛ وذكر الطيطي "أن استراتيجية الردع السيبراني "هي عملية الدفاع ضد الرمز التخريبي الفيروسي، وتأخذ بالاعتبار العديد من الخصائص التي تعمل على فحص الفيروس التخريبي المراد فحصه أو منعه من التنفيذ والانتشار والحد من تحقيق أهدافه" (الشايع، 2019).

**استراتيجيات الردع السيبراني:**

- **الاستراتيجية الوطنية للأمن السيبراني:** هذه المرحلة الثانية لاستراتيجيات الأمن السيبراني توضح الخطط الوطنية لحماية التقنيات المتطورة ؛ وتتسارع الدول بوضع خطط تتبعها للمحافظة على شبكات معلوماتها الوطنية "فقد أجبرت التطورات في مجال تقنية المعلومات ضغوطا وتحديات كبيرة على المنظمات مما تتطلب منها الاستجابة لمواجهة هذه الضغوطات، وأثرت عليها تحويل التحديات إلى فرص للنماء والتطوير في بيئة أعمال تكون أكثر انفتاحًا واندماجًا يومًا بعد يوم، وذلك عن طريق إعداد استراتيجية مدروسة لأمن المعلومات تكون حجر الزاوية لأمن المعلومات وتحول هذا النشاط إلى نشاط استباقي بدلاً من رد الفعل فكل منظمة قد تنتهج استراتيجية خاصة وفقًا للتهديدات الخاصة بها ومحركات الأعمال فيها ومتطلبات التوافق لبيئة الأعمال عندها؛ واستنادا إلى ما سبق، فقد أنشئت المملكة العربية السعودية ضمن رؤيتها المستقبلية للدولة الهيئة الوطنية

للأمن السيبراني، وذلك لمواكبة التطورات العالمية في مجال الفضاء السيبراني، وحماية منشئاتها المعلوماتية، من أي مخاطر أمنية تقنية " (الشايع،2019،ص 252).

- **استراتيجية إدارة المخاطر المعلوماتية:** أكد الدنف أن هذه الاستراتيجية "تعتبر إدارة المخاطر المعلوماتية عملية قياس وتقييم للمخاطر الأمنية وتطوير استراتيجيات لإدارتها، وتتضمن هذه الاستراتيجية نقل المخاطر إلى مكان آخر للتصدي لها وتقليل الأثار السلبية وقبول بعضها وكل تبعاتها، وتبدأ من هنا العمليات لإدارة المخاطر تبعث إلى الجهات المختصة تقريرها الذي يوضح توصياتها حول درجات المخاطر ويجري تحديد الإجراءات بتحليل المخاطر، حيث توضح العلاقة بين مدى قابلية المنظمة للتعرض للمخاطر والأثر الذي ينتج عن الخطر، وتعقيبًا على ما سبق في أن أهمية إدارة المخاطر تكمن في مسؤولية أفرادها في إدارة أي من المخاطر التقنية التي قد تحدث لشبكات المعلوماتية وأخذ الحيطة والحذر، وإعداد خطط فعالة للوقاية من الجرائم التقنية في حالة حدوث هجمات إجرامية تكنولوجية" (الشايع،2019، ص274).
- **استراتيجية حماية المحيط الخارجي:** ذكر الشايع أن هذه الاستراتيجية "تقوم بالبحث عن الثغرات الأمنية داخل أنظمة التشغيل، وأنظمة جدران الحماية، والمتصفحات، وخوادم الويب، حيث يمكن تحديد الشفرات الخبيثة المحتملة من خلال التعرف على التوقيعات والأنماط"(2019، ص276-277).

### 2-1-7 الجرائم والتهديدات السيبرانية

ذكر الطائي، والكيلاني، مجموعة من التعريفات للتهديدات والتي قد تكون:

"الشخص أو المنظمة أو الآلية أو الحدث الذي يمكن أن يلحق الضرر بالموارد المعلوماتية للمنظمة، أي ظرف أو حدث من المحتمل أن يؤثر سلبًا على العمليات التنظيمية (بما في ذلك مهمة، وظيفة، صورة، أو سمعة)، الأصول التنظيمية والأفراد والمنظمات الأخرى، أو للأمة من خلال تعديل المعلومات أو الحرمان من الخدمة. الخطر المتوقع الذي يمكن أن تتعرض له الأنظمة المعلوماتية وقد يكون شخصياً كالتجسس أو قراصنة من قبل مخترق أو يحدث تهديد الى الأجهزة والبرامج والمعطيات أو حوادث كالحريق وانقطاع التيار الكهربائي والكوارث البيئية"(2015م، ص113). ومن أهم أبعاد مفهوم التهديدات:

- توجد التهديدات متى ما وجدت نقاط الضعف ويمكن أن يكون هناك عدد من التهديدات لكل نقطة ضعف.
- تكون التهديدات المعلوماتية من فعل وتصرف مقصود وغير مقصود، والتي قد تأتي من جهات داخلية أو خارجية، كما أنها قد تتراوح من حدث مفاجئ أو حدث ثانوي تؤدي إلى عدم الكفاءة الدائمة المتوقعة، وقد تحدث أخطاء النظام من سوء استخدام الأجهزة والبرمجيات، أو التحميل الزائد أو المشاكل التشغيلية وغير ذلك.

- قد تتسبب الأخطاء الفنية بسبب الهجمات المختلفة التي يتعرض لها النظام، ويكون الغالب من الفيروسات في الأنظمة من خلال البرمجيات الضعيفة، أو المتطفلين، الديدان، أو القنابل المنطقية، إلخ. والتي تمثل بعض الوسائل الفنية المستخدمة لتعطيل النظام وتشويهه وعرقلة وظائفه المختلفة، إتلاف أو تحريف بياناته.
- يمكن تصنيف التهديدات في أنواع مختلفة بطرق مختلفة مثل التهديدات البشرية غير البشرية، التهديدات المتعمدة / غير المتعمدة، تهديدات المهرة / غير المهرة، التهديدات الداخلية / الخارجية، الفيروس، على سبيل المثال، هو تهديد غير بشري، لا متعمد، عمومًا في البداية على الأقل وخارجي، ويمكن أن يكون تهديد المهرة أو غير المهرة (اعتمادًا على مطور الفيروس) من ناحية أخرى، يوصف تهديد مدير النظم الساخط بأنه بشري، متعمد، ومهرة، وداخلي.
- التهديدات هي الأشياء التي يمكن أن تسبب الضرر، أو هي الأشياء السيئة المحتملة التي يمكن أن تحدث لأحد الأصول، ومن ثم يمثل خطراً ممكناً على النظام، وقد يكون هذا الخطر شخص يقوم بالتجسس أو التخريب، أو شي يحدث مشكلة في الحاسب وملحقاته، أو حدثاً مثل الحريق أو الفيضان، أو يستغل به نقطة ضعف النظام.

### 2-1-7-1 أنواع الجرائم السيبرانية

لقد ذكر (الشايع، 2019) بعض أنواع الجرائم السيبرانية وهي كالتالي:

1. الاختراقات التقنية للأنظمة والخدمات الإلكترونية.
2. تعديات أمنية لبنى التحتية لتقنية المعلومات.
3. وضع برامج التجسس وإرسال فيروسات تخريبة.
4. انتهاك الخصوصية للبيانات الشخصية للأفراد.
5. الاحتيال وسرقة الهوية مثل، استخدام بريد الإلكتروني يكون لشخص مجهول، ويكون أيضًا استخدام أرقام لشخص آخر وغيرها من الاحتيالات التكنولوجية.

### 2-1-7-2 أنواع التهديدات

تتجسد أهمية تحديد أنواع التهديدات في أنه يساعد إدارة المنظمة في رسم ما يصطلح عليها" خارطة التهديدات الأمن المعلوماتThreats Map Information Security والتي ذكرها (الطائي، والكيلاني، 2015م، ص115) ومن ذلك:

تقييم مصادر التهديد، حيث أن من المهم النظر في جميع مصادر التهديد المحتملة التي يمكن أن تسبب ضررًا لموارد المعلومات في المنظمة وفي كيفية التعامل معها، على النحو الذي يسهل معرفة وتحديد أي التهديدات الأكثر خطورة وبالتالي تركيز الرقابة على النشاط المرتبط

به ومن ثم السعي إلى تقليل الآثار السلبية المحتملة له، حيث يمكن استخدام أسس مختلفة في تصنيف التهديدات، وأهم هذه الأسس هي:

**نوع الهجوم المحتمل:** حدد الخبراء المختصين بالقضية الأمنية من خلال شبكات الإنترنت والتهديدات لأمن المعلومات إلى فرعين من أفرع الهجوم المحتملة وهما: هجوم تقني، وهجوم غير تقني.

**المصادر التي تنبع منها التهديدات:** يرى القحطاني والغثبر (2009) من الممكن تصنيف التهديدات حسب المصادر التي تتكون من نوعين وهما: مصادر تهديدات الداخلية ومصادر تهديدات الخارجية.

**نوع الحدث الحاصل:** يشير الطيطي إلى " أنه يتم تقسيم أنواع التهديدات على أساس ما الذي يعطل الأنظمة المعلومات إلى أربع أنواع ومن دون التطرق إلى مصادر التهديدات، وهي الفضح والكشف، والتعرض الغير المصرح به للمعلومات، الخداع، والتسلط الغير شرعي لأجزاء من النظام" (الطائي والكيلاني، 2015م، ص115).

### 2-1-8 الأمن السيبراني في المملكة العربية السعودية

"قامت المملكة العربية السعودية ضمن أهدافها لتطوير الوطني الذي يتوافق مع رؤية 2030، بالاهتمام الكلي لبنية التحتية التقنية والخدمات الإلكترونية وأي نشاط يعمل في مجال التقنية ولذلك فقد أنشئت المملكة، الهيئة الوطنية للأمن السيبراني، بموجب الأمر الملكي رقم (6810) بتاريخ 1439/2/11هـ، الذي يهدف إلى حماية وصيانة ومراقبة الثورة المعلوماتية للدولة من أي هجمات تقنية خبيثة، قد تصيب الخدمات والأنظمة والأجهزة الحكومية للدولة وأمنها الوطني ولذلك فقد عملت الهيئة الوطنية للأمن السيبراني بالمملكة، بوضع الخطط والبرامج والمعايير والضوابط الأساسية، والأهداف للأمن السيبراني داخل المملكة، ويكون قد تم تحقيق رفع مستوى الأمني لحماية الشبكات العنكبوتية والبنية التحتية للأنترنت، والتزام جميع المنظمات بتنفيذ الضوابط الأساسية لأمن السيبراني"

### 2-1-8-1 المكونات الهيكلية للضوابط الأساسية للأمن السيبراني:

ذكرت الهيئة الوطنية للأمن السيبراني بعض الهيكلية التي يعتمد عليها الأمن السيبراني ومن ذلك:

- ❖ الأمن السيبراني لأنظمة التحكم الصناعي.
- ❖ الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة.
- ❖ حوكمة الأمن السيبراني وصموده وتعزيزه.


**شكل (2) حكومة الأمن السيبراني**

**المصدر/ الهيئة الوطنية للأمن السيبراني**

### 2-8-1-2 القضايا الأساسية للأمن على الإنترنت

إن الأمن في نظام الحاسوب و الإنترنت لا يركز فقط منع على حالات الاختراق والهجوم من خلال الإنترنت والحد من العمليات القرصنة بل يهتم بالقضايا التي تكشف المعلومات في غاية السرية لأفراد أو شركات، حيث يقوم الكثير من الأفراد عند طلب خدمة من خلال الإنترنت لتعبئة نموذج خاص حيث يقوم المستخدم بتعبئة الاسم والعنوان وأرقام الهاتف وغيرها من المعلومات المطلوبة تعبئتها عند إجراء عمليات بيع أو شراء أو طلب خدمات مجانية من أحد المواقع الإلكترونية المنتشرة عبر الإنترنت حيث تطرأ الكثير من القضايا الأمنية والتي يجب على كل فرد أو شركة أن يأخذها بعين الاعتبار (الطيطي، 2010م، 392) مثل:

- كيف يتأكد المستخدم من أن هذا الموقع وما فيه من قواعد بيانات مخزنة ومحفوظة في خادمات ويب هي ملك المؤسسات ومنظمات شرعية وليست وهمية.
- كيف يتأكد الشخص أن هذا الموقع لا يحتوي على أي برامج تحتوي على شيفرات تقوم بعمليات قرصنة.

- ❖ كيف يتأكد الشخص بأن مالك هذا الموقع لن يزور ونشر هذه المعلومات الشخصية إلى أطراف أخرى.
- ❖ ومن ناحية المنظمات فكيف تتأكد في أن الموقع الإلكتروني الخاص بها، بأن أي مستخدم لن يقوم بعملية خرق أو قرصنة لخادماتها والتي تحتوي على المعلومات المخزنة في قواعد البيانات.
- ❖ كيف تتأكد من أن هذا المستخدم لن يقوم بتخريب الخادم حتى لا يتمكن المستخدمين الشرعيين من استخدام الموقع.
- ❖ كيف يتأكد الطرفان المستخدم والشركة من عدم وجود طرف ثالث يقوم بالاختراق أو التخريب.
- ❖ كيف يتأكد الطرفان الفرد والمنظمة من أن المعلومات التي يتم إرسالها بين الطرفين لم يحدث أن تم الاطلاع والتغيير في محتوياتها قبل وصولها إلى الطرف المستقبل.

إن هذه الأسئلة وغيرها توضح لنا القضايا الأمنية والتي تظهر عند تنفيذ التعاملات والتفاعل في التجارة الإلكترونية عبر الإنترنت والتي تحتوي عمليات ذات أهمية كبيرة مثل عملية دفع الأموال إلكترونيًا وعملية إرسال أرقام بطاقات اعتماد بنكية وعمليات إرسال معلومات قيمة وذات قيمة علمية وغيرها من المعلومات، ولذلك لا بد من توفير المزيد من التقنيات الحديثة لمواجهة كل هذا القضايا الأمنية والعمل على منعها أو الحد منها.

- ❖ التحقق **من الهوية**: إن العمل على التحقق في أنظمة الشبكات وخاصة الإنترنت يمكن تقسيمها إلى مرحلتين وهما:

**أ. العمل على التحقق من الكائن**: وهي عملية التأكد من هوية العميل أو المستخدم المدعي والتحقق من أنه هو ذاته وليس شخص آخر.

**ب. العمل على التحقق من الرسالة**: وهو العمل على التأكيد وتحقيق أن رسالة معينة هي رسالة حقيقية، قد جاءت من المصدر ولم يتم عليها أي تغيير أو تأثير.

- ❖ **الصلاحيات**: إن الصلاحيات المصرحة لأشخاص معينين تتكون من الضمانات التي تضمن أن العملاء المعنيين وتحت ظروف معينة مسموح بها لهم في استخدام خدمة معينة أو الحصول على معلومات معينة في وقت معين بصلاحية معينة (قراءة أو كتابة أو مسح أو تغيير أو صلاحيات كاملة أو أي خليط من هذه الصلاحيات) من قبل العاملين في تقديم لخدمة.
- ❖ **السرية**: إن السرية هي الأخذ بعين الاعتبار الخصوصية والسرية عند تبادل الرسائل، بحيث لا يتم الإفشاء عن محتويات هذه الرسالة إلى أي أطراف غير مصرح لهم. ومن الطرق العامة والمستخدمة لضمان السرية هي باستخدام نظام التشفير، ونظام التشفير يقوم بحفظ المعلومات المتبادلة بين الأطراف وعبر الشبكات السرية، ولضمان السرية للرسائل المتبادلة لا بد من أن تكون قناة التوزيع أمنة وأن الرسالة عند إرسالها في فضاء الافتراضي يجب أن تكون مشفرة بأحد أنظمة التشفير القوية والمعترفة عالمياً.

- **التكامل**: إن عملية التكامل هي تكامل الرسائل المرسلة بين الأطراف ومن خلال الشبكات كشبكة الإنترنت وشبكة الاتصالات اللاسلكية، حيث أنه لضمان التكامل للرسائل لا بد من استلام الرسائل نفسها بدون أن يتم اعتراضها أو تغيير محتوياتها ويتم ذلك بتقنيات بسيطة لمعرفة ما إذا تم تغيير محتوى الرسالة أم لا.
- **الخصوصية**: وهي عملية حفظ السرية وأمن المعلومات الخاصة في العملاء والتي تم حفظها في قواعد البيانات وضمن خادمات الويب بحيث لا يتم توزيعها إلى أي طرف آخر ولا يتم نشرها أو بثها بدون موافقة خطية من العميل نفسه.

## 2-2 المبحث الثاني: جودة الخدمات الإلكترونية

في العصر الحاضر أضحى الاهتمام الهائل بالجودة بما لها من أهمية كبيرة لدى المنظمات والمراكز الحكومية؛ وذلك لأنها تقوم بتجويد الخدمات المقدمة للمستفيد ين من أفراد المجتمع من قبل المؤسسة، كما أن للجودة دورٌ كبيرٌ في تقدم المنظمة بصورة مستمرة وفعالة لتحقق أعلى معايير الجودة في الخدمات والأعمال؛ وبالتحديد هذا المبحث في جودة الخدمات الإلكترونية التي تعمل على مدار الوقت في تقديم الخدمات المهمة للأفراد.

### 2-2-1 تعريف جودة الخدمة

يُعرف جمال الدين (2012) جودة الخدمة " فعل أو إجراء يقوم به أحد الأطراف بتقديمه لطرف آخر والتي تعتبر في الأساس غير ملموسة"، ومن خلال هذا التعريف اعرف جودة الخدمة هي تقديم الخدمة لمستفيدين وتلبية احتياجاتهم بكل كفاءة وأن تكون الخدمة تتلاءم مع توقعات العميل عندما تقدم له" (ص152)، ويعرفها (طواهير والهواري، 2014م) بأنها: "درجة تيسر موقع الويب لعملية الشراء، والتخزين، تسليم البضائع أو خدمة"، كما تعني أيضًا إلى أي مدى هذه الخدمة تلبي توجهات العملاء (الحلبي، 2017، ص 8).

### 2-2-2 مفهوم الخدمات الإلكترونية

هي: "إجراء الكثير من المعاملات كليًا أو جزئيًا عبر الإنترنت (الهزاني 2008، ص47)، ويعرفها أيضًا بأنها: "الخدمات التي تقدمها المؤسسات والأجهزة الحكومية كخدمة للمستفيدين ويكون ذلك بواسطة الوسائل التقنية الحديثة مثل البريد الإلكتروني، مواقع الشبكات وغيرها من الأدوات الإلكترونية وهي تحقق التفاعل بين مقدم الخدمة والمستفيد"، أما(كافي، 2009، ص 23) فيعرفها بأنها: "التوصيل الإلكتروني لمعلومات الحكومة وبرامجها وخدماتها عن طريق الإنترنت عادة"؛ ومن هذا المنطلق للمفهوم فإن الخدمات الإلكترونية هي خدمات التي تقدم فورًا للمستفيد بواسطة الشبكة العنكبوتية ويقوم بهذه الخدمة الموظف الذي يعمل على إجابة العميل وتنفيذ طلبه الإلكتروني دون الحاجة لحضوره في مقر الجهة المقصودة.

### 2-2-3 مميزات الخدمات الإلكترونية

ذكر (القدوة، 2010م، ص 175-177) بعض المميزات التي تميز الخدمات الإلكترونية وهي:

- ❖ تقديم الخدمات والمعلومات للأفراد المجتمع بكل سرعة وسهولة.
- ❖ المشاركة الفعالة في تبادل الأوراق الرسمية بين إدارات الجهات الحكومية.
- ❖ مكافحة الفساد بجميع أشكاله.
- ❖ توفير الوقت والجهد.
- ❖ تقليل التكاليف المادية.
- ❖ الخصوصية والحماية المعلوماتية.
- ❖ إدارة شؤون المواطنين من قبل الدولة في كافة الأجهزة الحكومية.

### 2-2-4 المبادئ الأساسية للخدمات الإلكترونية:

ذكر (الهزاني، 2008م) مجموعة من المبادئ للخدمات الإلكترونية منها:

- ❖ أن يكون هناك سهولة ووضوح وسرعة في الوصول إلى كافة الخدمات الإلكترونية لجميع المستفيدين وأيضًا أصحاب الهمم العالية في استخدام الخدمات التكنولوجية والاستفادة منها.
- ❖ أن تكون الخدمات متوفرة على مدار الوقت.
- ❖ تأمين معلومات الأفراد وحفظها من أي تعديات تخريبية تقنية.
- ❖ إمكانية الخدمات الإلكترونية من خلال القنوات التكنولوجية مثل الهاتف، شبكة الإنترنت وغيرها من الأدوات التقنية.
- ❖ أن تكون الخدمات الإلكترونية غير مكلفة وأن تحقق بنفس الوقت رضا المستفيد.
- ❖ موافقة المستفيدين في استخدام المعلومات الشخصية التابعة لهم عند تقديم الخدمة الإلكترونية.

### 2-2-5 معوقات تطبيق الخدمات الحكومية الإلكترونية

لقد ذكر (الهزاني،2008م، ص 45) المعوقات التي تحدث تأخير في تفاعل هذه الخدمات التقينه بسبب عدة عوائق وهي:

- ضعف البنية التحتية لتقنية الاتصالات، حيث تشكل البنية الأساس لتكوين الشبكات الإلكترونية.
- وجود تعارض بين خطوط سير الإجراء، كما هو واقع في المعاملات التقليدية، في حين تتطلب الخدمات الإلكترونية توحيد الإجراءات والقياسات، والمعايير حتى يتمكن المستخدم من الانتقال بين الصفحات الإلكترونية بانسجام دون تعارض أو تضارب.
- الخلط بين تقنية المعلومات، وأنظمة تبادل المعلومات.
- العائق النفسي المتمثل في مقاومة التغيير.

### 2-2-6 مقومات بناء تقنية المعلومات الأمنية

ذكر (السعيد، 2013م، ص33-37) بعض مقومات بناء تقنية المعلومات الأمنية وأهدافها وعلاقتها بصنع القرار الأمني ويرتبط ذلك بمؤسسات تقنية المعلومات وغيرها ومن ذلك:

- بناء الشبكة المعلوماتية المتطورة وبالتحديد لأحدث التقنية الحديثة في وسائل الاتصال والتطوير وأساليب العمل والتشغيل بمختلف أجهزة المنظمات
- بناء نظام معلومات لتحقق التكامل بين أجهزة المنظمات على المستوى (النوعي -الجغرافي)، وتكفل معالجة المشاكل والمواقف الأمنية وإدارة الأزمات.
- بناء قواعد بيانات لجميع مجالات العمل بالمنظمة الأمنية -الخدمية -التعليمية -التدريبية -الإدارية -المالية-الحربية).
- الاهتمام بإعداد كوادر مُدرّبة لرفع مستوى الأداء الشرطي وتدريس علوم نظم المعلومات بجميع الكليات والمعاهد الشرطية لجميع ضباط وأفراد الشرطة والعاملين المدنيين بالوزارة.

### 2-2-7 معايير جودة الخدمات الإلكترونية

تضمن معايير جودة الخدمات الإلكترونية الوصول إلى معاملات إلكترونية ذات جودة عالية تنال رضا وثقة جميع المستفيدين والعملاء وبما يحقق ويسهم في الوصول إلى الجودة الشاملة في تقديم الخدمات الإلكترونية، ومن تلك المعايير (وثيقة معايير جودة الخدمات الإلكترونية الحكومية،2015م):

- الاستخدامية Usability: وهي تقيس مدى سهولة استخدام الخدمة الإلكترونية ومدى قبولها لدى المستخدمين وذلك من خلال اتباعها لبعض الإجراءات والشروط.
- جودة المعلومات Information Quality: يجب أن تتحلى المعلومات الواردة عبر مختلف مراحل الخدمة بالدقة والموثوقية والسهولة وأن تكون واضحة المعنى.
- الأداء الموثوق(Realbility): تقيس مدى ثبات الخدمة وحصولها على ثقة المستخدمين من حيث الأداء والمتانة وهي تتطرق لقنوات الدفع الإلكتروني وتقديم معلومات موثوقة عن مواعيد الاستلام والتسليم وكيفية إيصال مخرجات الخدمة الإلكترونية.
- الاستجابة Responsiveness: يجب أن تتمتع الخدمة باستجابة عالية في خدمة عملاء المؤسسة وهذه الاستجابة يمكن تقييمها من خلال ثلاثة أبعاد يشمل سرعة إجراء الخدمة والتجاوب مع مخاوف الفئات المستهدفة (المستفيدين) والتوقع بالتغيرات التي تطرأ على حاجة المستفيدين.
- طمأنينة المتعامل Assurance: يقصد بطمأنينة التعامل توافر مجموعة من الضمانات التي من شأنها المحافظة على خصوصية المستفيدين وضمان أمن وسلامة بياناتهم.
- خدمة العملاء وأدوات التواصل الاجتماعي Customer & Web 2.0: يجب أن تكون خدمة العملاء متوفرة على مدار الساعة وعبر كل القنوات المتاحة.

## 2-3 المبحث الثالث: الدّراسات السّابقة

### 2-3-1 الدراسات الخاصة بالأمن السيبراني:

**دراسة الشهري، علي (2019) بعنوان: رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية.**

هدفت الدراسة إلى الكشف عن الجرائم الإلكترونية وأسبابها، وتحديد المهددات والمخاطر التي تواجه الأمن السيبراني في المملكة العربية السعودية لبلوغ استراتيجية تقلل من الجرائم الإلكترونية وتطور الأمن السيبراني. اعتمد الباحث في هذه الدراسة على المنهج الوصفي التحليلي، واستخدم أداة الدراسة وهي الاستبانة لجمع البيانات واعتمد أيضًا أداة S.W.O.T للتحليل الرباعي لوضع الخطة الاستراتيجية. وتوصل الباحث إلى: أن الجرائم الإلكترونية لا يمنعها أي حدود زمانية كانت أو مكانية وهذه الصفة تعتبر من أهم الصفات التي تميز طبيعة الجرائم الإلكترونية كما اتضح أن التقنيات الحديثة والإنترنت توفر فرصًا عديدة لزيادة الجرائم الإلكترونية. كما اتضح أيضًا أن انتهاك السياسة الأمنية الخاصة بالأمن السيبراني تعتبر أحد أهم التهديدات التي تواجه الأمن السيبراني في المملكة العربية السعودية.

**دراسة الشهري، أحمد (2019) بعنوان: مقترح للتدابير الوقائية من الجرائم السبرانية لتعزيز الاعتدال الفكري**

هدفت الدراسة إلى التعرف على الاحتياطيات الوقائية من الجرائم السيبرانية لمساعدة الانضباط الفكري في مجتمع المملكة العربية السعودية، تكون مجتمع الدراسة من الأعضاء في الهيئة التدريسية بكلية الحاسبات والمعلومات بجامعة الإمام محمد بن سعود الإسلامية بالرياض وجامعة الملك عبدالعزيز بجدة وجامعة الملك سعود بالرياض والبالغ عددهم (390) عضو هيئة تدريس، وبلغت عينة الدراسة (288) عضو استخدم الباحث المنهج المسحي الاجتماعي بالعينة العشوائية، والاستبانة كأداة من أدوات جمع البيانات وتوصل الباحث إلى: أن أفراد العينة يوافقون بشدة على محور "التدابير الوقائية، الموقفية والاجتماعية، المعتمدة في الوقاية من – الجرائم السيبرانية، أن العاملين موافقين بشدة على محور "التدابير التشريعية وإجراءات العدالة المفعلة للوقاية من الجرائم السيبرانية، أن أفراد العينة موافقين بشدة على محور "التدابير الخاصة ببناء القدرات الوطنية في المجالات ذات الصلة بالجرائم السيبرانية والوقاية منها، أن أفراد العينة موافقين على محور "التدابير والإجراءات المجتمعية، المؤسسية والشخصية، للوقاية من الجرائم السيبرانية، أظهرت نتائج الدراسة أن أفراد العينة موافقين على محور إسهام التدابير الوقائية، الموقفية والاجتماعية، من الجرائم السيبرانية في تعزيز الاعتدال الفكري داخل المجتمع السعودي.

**دراسة حميد، محمد (2019) بعنوان: رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة**

هدفت الدراسة إلى توضيح الرؤيا الاستراتيجية لمحاربة الجرائم السيبرانية، حيث تم تطبيقها على مدرسي هيئة التدريس بالشرطة اليمنية عددهم (121) مفردة، وتم استخدام المنهج الوصفي التحليلي، والاستبانة كأداة دراسة، ومن النتائج التي توصلت الدراسة إليها أن واقع الإرهاب السيبراني هو استغلال شبكة الإنترنت للتحريض على التطرف والعنف، وظهور طرق حديثة لتجنيد المتطرفين عبر الشبكات، ويتضح هدف مكافحة الجرائم السيبرانية في مساعدة الأمن الإنساني: لتنمية الوعي الفردي بالمخاطر التي تواجه ارتكاب الجرائم السيبرانية، وتشارك في تحقيق الأهداف والغايات من الأمن الإنساني بمحاوره المختلفة، والتي تعمل على تحقيق الوقاية المبكرة من الجرائم السيبرانية، وزيادة نسبة المكافحة الوطنية والوسائل الأمنية التي تستخدم في لحماية للبيئة الوطنية، تعزيز الحماية الفردية على المستوى الشخصي، ومن المعوقات التي تواجه مكافحة الجرائم السيبرانية: قلة الخبرات وضعف المؤهلين والتدريب لدى العناصر التي تكافح الجرائم السيبرانية، يوجد نوع من القصور في التشريع بشكل كبير في تجريم ارتكاب الجرائم السيبرانية، وأصبح من السهل الوصول للضحايا عن طريق الشبكة العنكبوتية، انخفاض نسبة الإبلاغ عن الجرائم السيبرانية للبعد عن إساءة السمعة أو ذبذبة ثقة العملاء.

**دراسة الشوابكة، عدنان عواد (2019) بعنوان: دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات**

هدفت الدراسة إلى التعرف على دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف. تم الاعتماد على المنهج الوصفي التحليلي؛ ولتحقيق ذلك تم تصميم استبانة مكونة من (52) فقرة، تم توزيعها على عينة الدراسية المكونة من (129) عاملاً، وقد توصلت الدراسة إلى أن الإجراءات الأمنية في الحد من مخاطر امن المعلومات في الجامعة عالية. والإجراءات الأمنية

لمنع الاختراق عن طريق الشبكة الحاسوبية Network Hacking جاءت بمستوى مرتفع، بينما الإجراءات الأمنية لمنع الاختراق عن طريق الهندسة الاجتماعية Social Engineering جاءت بمستوى متوسط، والإجراءات الأمنية لمنع الاختراق عن طريق البرمجيات الضارة Malware جاءت بمستوى متوسط، وساهمت إجراءات الأمن المعلوماتي في الحد من المخاطر الداخلية والخارجية والطبيعية التي يتعرض لها النظام.

**دراسة البسام، (2018): بعنوان: التحقيق في العوامل المتعلقة بالتوعية بالأمن السيبراني في القطاع المصرفي البحريني**

يركز البحث على دراسة العوامل المرتبطة بـ CSA في العمل المصرفي البحريني. تتمثل هذه العوامل في: دعم الإدارة العليا، الميزانية، إنفاذ سياسة الأمن السيبراني، والامتثال للأمن السيبراني وثقافة الأمن السيبراني، واعتمدت الدارسة المنهج الوصفي التحليلي، واستخدم الاستبيان كأداة للدراسة وتكون مجتمع الدراسة من (119) مفردة، وتوصلت الدراسة إلى: أهمية دعم الإدارة العليا من أجل الوعي بالأمن السيبراني في البنوك البحرينية ويظهر علاقة كبيرة بين التزام الإدارة العليا والدعم والوعي بالأمن السيبراني وجاء في المرتبة الثانية، أهمية الميزانية للأمن السيبراني الوعي في البنوك البحرينية تم الاتفاق بشدة من أفراد العينة مما يعكس وجود علاقة مهمة بين وضع ميزانية وتخصيص ميزانية لـ CSA وجاء في المرتبة الثالثة، أهمية إنفاذ السياسة للتوعية بأمن الفضاء الإلكتروني في البنوك البحرينية التي أشارت إلى أن المشاركين كانوا يعبّرون بقوة عن أهمية العلاقة بين تطبيق سياسة الأمن السيبراني ووكالة الفضاء الكندية وجاء بالمرتبة الخامسة، وجاء بالمرتبة الأولى أهمية الامتثال الأمني مما يعكس أن المشاركين كانوا توافق بشدة على أن الامتثال الأمني ضروري لـ CSA وأنه كان هناك علاقة مهمة بين الامتثال للأمن السيبراني وCSA، وجاء بالمرتبة الرابعة أهمية ثقافة الأمن السيبراني وأن المشاركين وافقوا بشدة على ذلك، ثقافة الأمن السيبراني المطلوبة لوكالة الفضاء الكندية وأن هناك علاقة مهمة بين ثقافة الأمن السيبراني ووكالة الفضاء الكندية، واستنتج الباحث: عدم وجود أدبيات كافية حول العوامل المرتبطة بـ CSA في القطاع المصرفي في البحرين.

**دراسة شلوش (2018): بعنوان: القرصنة الإلكترونية في الفضاء السيبراني "التهديد المتصاعد لأمن الدول**

هدفت هذه الدراسة إلى معرفة الاستراتيجيات والأليات المتبعة التي يمكن تفعيلها من قبل الأنظمة الدولية لتعزيز الأمن السيبراني الدولي وملامسة و علاقة القرصنة الإلكترونية التي تقوم بأحداث تغييرات في البيئة الأمنية السيبرانية الدولية وما هو تأثير هذه الهجمات السيبرانية، وبالتحديد القرصنة الإلكترونية؛ والتعرف على الأسلحة الإلكترونية الجديدة التي تقوم في الحماية؛ الأمنية التقنية ؛ و إضافة إلى التعرف على دور الأنظمة الدولية من الحد من الهجمات السيبرانية في عالم الفضاء السيبراني، أسفرت الدراسة عن النتائج التالية: العالم الرقمي يتحكم في جميع مجالات الحياة سواء العمل أو في الحياة الشخصية، أصبح الفضاء السيبراني أمرًا واقعًا لا فرار منه حيث نواجه فيه جميع مخاطر الحروب الإلكترونية، فالتحول الرقمي هو القوة السائدة في العصر الحالي الذي يتوجب على الدول والأفراد أخذ

الحذر والحيطة عند استعمال البيانات والمعلومات في المجال الافتراضي؛ لتجنب المخاطر المحتملة في التصيد الشبكي والهاكرز والجماعات الإرهابية.

**دراسة العتيبي، (2017) بعنوان: دور الأمن السيبراني في تعزيز الأمن الإنساني**

هدفت الدراسة الكشف عن دور الأمن السيبراني في تدعيم الأمن الإنساني، وقد تكون مجتمع الدراسة من العاملين في مجال الأمن السيبراني بشركة أرامكو السعودية بمنطقة الرياض في (12) محطة، والذين لديهم أجهزة حاسوب، وصل عددهم (820) موظف بناء على إدارة شؤون الموظفين بأرامكو. عينة الدراسة تكونت من (400) فرد من المجتمع وتم اختيارها عشوائياً. استخدم الباحث المنهج الوصفي التحليلي، واختار الاستبانة والمقابلة كأداتين لجمع المعلومات اللازمة للدراسة من الموظفين والقادة باعتبارهما انسب أدوات البحث العلمي التي تتفق مع معطيات الدراسة وأهدافها. وكانت أهم النتائج: إن الإجراءات الفنية لحماية الفضاء السيبراني للشركة متوفرة بدرجة كبيرة، حيث يتم قفل النظام آلياً في حالة عدم استخدامه لفترة زمنية محددة. إن الإجراءات التقنية لحماية الفضاء السيبراني الخاص بالشركة متوفرة بدرجة كبيرة، استخدام المقاييس الحيوية (بصمة العين – بصمة الإصبع – بصمة الصوت) لمرور المصرح لهم. أن السياسات للأمن السيبراني في الشركات المتوفرة بدرجات كبيرة في الشركة، حيث تتضمن الأنظمة الآلية الفعالة للإبلاغ عن أي من المحاولات للاختراق.

**دراسة هادي، سهيلة (2017): بعنوان: الحروب الإلكترونية في ظل عصر المعلومات**

هدفت هذه الدراسة إلى التعرف الأسلحة الأمنية الإلكترونية، وماالقطاعات المستهدفة في الحروب الإلكترونية، كما أشارت الدراسة عن رصد الاستراتيجيات الحروب الإلكترونية والإحاطة بأساليب عمل هذه الاستراتيجيات، وأيضا هدفت إلى ما هي أبرز الأليات التي يجب على الدولة اتباعها لمحاربة مخاطر الحروب الإلكترونية، أن كانت حروب سياسية، واقتصادية والاجتماعية، والثقافية، والأمنية، أسفرت الدراسة عن النتائج التالية: الحروب العسكرية يوجد فيها مجالا مناسبا لاستخدام الأسلحة الإلكترونية عبر التشويش على الاتصالات، يسبب التجسس بزرع فيروسات إلى تعطيل جميع القطاعات ويسبب خسائر مادية كبيرة، أحدثت الحرب الإلكترونية من ناحية البعد الثقافي حيث إنها كونت مناخا خصبا لتوظيف الأسلحة الإلكترونية، لحسم الحرب الإلكترونية من خلال نشر القيم الاستهلاكية والتفتيت الهوياتي، عبر برامج معلوماتية معروفة، وتقوم بالتأثير في الثقافة التعددية؛ معتمدة بذلك على الإعلام، تحت هدف رئيسي هو إفساد القدرة الإبداعية التي هي أساس النهضة والتطور المتمثل في المورد البشري، ينتج عن الحروب الإلكترونية مجموعة من المخاطر الجسيمة المهددة للأمن القومي؛ فتداعياتها العسكرية، والاقتصادية والاجتماعية، والثقافية، وحتى النفسية، تؤثر في استقرار الدولة والمجتمع، ولذلك يعمل المجتمع الدولي في مواجهة هذه التحديات والتصدي لها من خلال الاستعانة بالأفراد الذين

يملكون المهارات الإلكترونية، وأيضا إنشاء مراكز متخصصة تقوم بدراسة هذه الحروب التقنية للأجل تقنين مخاطر التهديدات الإلكترونية.

**دراسة روجرز وآشفورد (Rogers &Tina, 2015): بعنوان: تطبيقات الأمن السيبراني المجانية والبرامج الحاسوبية.**

من خلال التقارير والأخبار المعاصرة أصبح موضوع أمن الأجهزة في كل مكان من الحياة اليومية وصاحب ذلك أخبار حول الاختراقات لبيانات الشركات وسرقة الهوية عبر الإنترنت وهذا يحتم الحاجة نحو تأهيل القوى العاملة المخصصة في مجال الأمن بالمعرفة والمهارة من هنا هدفت الدراسة إلى غرس بعض الخبرة لدى طلاب المرحلة الجامعية في السنة الأولى من خلال المحاكاة وخاصة مسابقات الأمن السيبراني وضم فريق تنافسي في المستوى الثاني، أسفرت الدراسة عن النتائج التالية: تقديم برنامج عملي مقترح مع الشرح والروابط للبرامج المجانية للتجربة العملية التي طبقها الطلبة، تقديم ستة دورات تعليمية مقترحة على الأنترنت يمكن تطبيقها والاستفادة منها لتكرار التجربة.

**دراسة سترنجيني (Stringhini,2014): بعنوان: حماية الخدمات عبر الإنترنت من النشاط الضار.**

هدفت هذه الدراسة إلى تطوير تقنيات تمنع الأطراف الضارة التي تسيء استخدام خدمات الإنترنت عبر دراسة مشكلة البريد الإلكتروني العشوائي والتي يتم إساءة استخدامها لإرسال مئات الملايين من رسائل البريد الإلكتروني العشوائي إلى خوادم البريد في جميع أنحاء العالم، وأظهرت النتائج أن المهاجمين عادةً ما يقومون بتقسيم قائمة عناوين البريد الإلكتروني الضحية بين روبوتاتهم، وأنه من الممكن تحديد روبوتات تنتمي إلى نفس الروبوتات بواسطة تعداد خوادم البريد التي يتم الاتصال بها عن طريق عناوين IP مع مرور الوقت، لذا طورت هذه الدراسة نظامًا يسمى BOTMAGNIFIER، والذي يتعلم مجموعة من mailservers اتصلت بها الروبوتات التي تنتمي إلى الروبوتات معينة، ويجد المزيد من الروبوتات التي تنتمي إلى نفس الروبوتات ومن ثم يدرس مشكلة الحسابات التي أسيء استخدامها على الشبكات الاجتماعية عبر الإنترنت للكشف عن الحسابات المزيفة التي أنشأها مجرمو الإنترنت.

**دراسة كاستنر (Kistner, 2006): بعنوان: محاكاة الهجوم السيبراني والانصهار المعلومات نماذج تحسين عملية التحسين للأمان عبر الإنترنت.**

تعتبر الجريمة الإلكترونية تهديداً بارزاً يتزايد في جميع جوانب المجتمع بما في ذلك الشركات والحكومة والبنوك والمواصلات والأفراد، ويعتمد أمن الشبكات على القدرة على التعرف على الهجمات السيبرانية الضارة والدفاع عنها؛ لذلك هدفت هذه الدراسة إلى استخدام تقنيات بحث التشغيل لإنشاء أدوات من شأنها المساهمة بشكل كبير في الأمن السيبراني وتطوير إطار محاكاة وقالب لتمثيل فعال لشبكات الحاسب وأنظمة كشف التسلل للأمن السيبراني، أسفرت الدراسة عن النتيجة التالية: أن نموذج المحاكاة يمكن أن يكون أداة فعالة لتمكين اختبار أدوات الوعي المؤسسي ولتحديد الثغرات في الشبكة، بالإضافة إلى ذلك فإن هذه الدراسة حددت طرق دمج

المعلومات الخاصة بالوعي الظرفي وتقييم التهديد من خلال إدخال طريقة صقل عملية التكيف للأمن السيبراني من شأنها أن تساعد في تقدم مجال الأمن السيبراني.

**2-3-2 الدراسات الخاصة بجودة الخدمات الإلكترونية:**

**دراسة غانم، (2019) بعنوان: جودة الخدمات الإلكترونية في مكتبات الجامعة اللبنانية من وجهة نظر المستفيدين: معهد الفنون الجميلة –الفرع الرابع نموذجاً**

هدفت الدراسة قياس جودة الخدمات الإلكترونية التي تقدمها مكتبات الجامعة اللبنانية من وجهة نظر المستفيدين، وفقا لأبعاد جودة الخدمات الإلكترونية، واستخدمت الدراسة المنهج الوصفي التحليلي، وتكون مجتمع الدراسة من أعضاء هيئة التدريس بالجامعة، وتوصلت الدراسة إلى جودة الخدمات الإلكترونية التي تقدمها مكتبة معهد الفنون الجميلة الفرع الرابع احتلت درجة متوسطة، يواجه المستفيدين مشكلات ومعوقات أثناء استخدامهم للخدمات الإلكترونية بدرجة قليلة، كشفت الدراسة الميدانية لمكتبة عينة الدراسة على اهتمامها في توفير ودر الخدمات الإلكترونية، ورعايتها للمستفيدين، الخدمات الإلكترونية التي تقدمها المكتبة غير مواكبة التطورات التكنولوجية، والأجهزة التي تستخدمها المكتبة في تقديم الخدمات الإلكترونية غير متطورة.

**دراسة عبد الراضي، (2018) بعنوان: جودة الخدمات الإلكترونية وأثرها على رضا العملاء: دراسة تحليلية على مصر للطيران.**

هدفت هذه الدراسة تحليل وتحديد أثر جودة الخدمات الإلكترونية في تحقيق رضا عملاء مصر للطيران بغرض مساهمة مصر للطيران في تبني استراتيجيات مناسبة تمكنها من كسب رضا العميل والمحافظة على العملاء الحاليين وجذب عملاء جدد، ولتحقيق هدف الدراسة فقد تم توزيع عدد (٣٥٠) استمارة على عينة من عملاء مصر للطيران، قد أظهرت نتائج الدراسة أن هناك علاقة ذات دلالة إحصائية بين جودة الخدمات الإلكترونية (تصميم الموقع، سهولة الاستخدام، السرية، توفير الوقت، الموثوقية، الاستجابة، الاعتمادية، والاتصال) ورضا عملاء مصر للطيران بدرجة مرتفعة.

**دراسة العضايلة، (2017). أثر تطبيق معايير جودة الخدمات الإلكترونية وأثرها على رضا طالبات جامعة الأميرة نوره بالمملكة العربية السعودية: دراسة حالة**

هدفت هذه الدراسة الكشف عن أثر جودة الخدمات الإلكترونية على رضا طالبات جامعة الأميرة نورة والمقدمة لهن عن طريق حساب الجامعة على شبكة الإنترنت، ولتحقيق أهداف الدارسة استخدمت الاستبانة كأداة لجمع البيانات، وتكون مجتمع من (500) طالبة، والعينة من (306) طالبة، واعتمدت الباحثة على المنهج الوصفي التحليلي، وكانت أبرز النتائج ما يلي: أن درجة جودة الخدمات الإلكترونية المقدمة من جامعة الأميرة نورة من وجهة نظر الطالبات كانت بدرجة ضعيفة. وأكدت النتائج أيضا أن درجة

رضا الطالبات عن الخدمات الإلكترونية المقدمة بدرجة ضعيفة، كما أظهرت نتائج البحث أيضا إلى وجود أثر ذو دلالة إحصائية لتطبيق معايير جودة الخدمة الإلكترونية التي تقدمها جامعة الأميرة نورة على درجة رضا الطالبات عن هذه الخدمات.

**دراسة الصومالي (2015/1437) بعنوان: قياس أثر جودة الخدمات الإلكترونية في القطاع الحكومي نموذج مقترح**

هدفت الدراسة إلى تطوير نموذج مفاهيمي لجودة الخدمة الإلكترونية المقدمة عبر الموقع الإلكتروني للأجهزة الحكومية وأثرها في تحقيق رضا العملاء وزيادة القيمة المدركة، اعتمدت الدراسة المنهج الوصفي التحليلي وقد اختبر نموذج الدراسة والتوصل لنتائج الدراسة عن طريق تحليل البيانات الكمية عن طريق أداة الاستبانة التي وجهت للمستفيدين من الخدمات الإلكترونية لوزارة الداخلية وطبقت الدراسة على عينة اختيرت بطريقة عشوائية من منسوبي جامعة الملك عبدالعزيز بجدة فرع السليمانية من الشطرين _بنين وبنات) من إداريين وأكاديميين بواقع (350) مفردة من مستخدمي الخدمات الإلكترونية المتوفرة عبر موقع وزارة الداخلية، وتوصلت الدراسة إلى عدة نتائج من أهمها: وجود علاقة إيجابية بين الأبعاد الأربعة لجودة الخدمة الإلكترونية مع مستوى رضا المستفيدين عن الخدمات الإلكترونية التي تقدمها المديرية العامة للجوازات وبدرجة عالية، توصلت الدراسة إلى أن مقدمي الخدمات الإلكترونية في القطاع العام بصفة عامة يجب أن يركزوا على الاهتمام بالقيمة المدركة والتواصل مع العملاء وتوظيف الخدمات الإلكترونية بشكل فعال؛ لأن ذلك بالتالي سيزيد من رضا المستفيدين بالإضافة إلى ذلك يجب أن يركزوا على الحد من مخاوف المواطنين بشأن سوء الاستخدام أو سوء إدارة البيانات الشخصية.

**2-3-3 التعقيب على الدراسات السابقة:**

**أولاً:** تم تحديد الدراسات السابقة وفق موضوع الدراسة الحالية بهدف إثباتها وتعزيزها علميًا، حيث تم تقسيم الدراسات السابقة الى محورين، وتضمن المحور الأول الجرائم الإلكترونية كما جاء في دراسة (شلوش، 2018) بعنوان: "القرصنة الإلكترونية في الفضاء السيبراني، وأيضا في دراسة (سهيلة، 2017) بعنوان: "الحروب الإلكترونية في ظل عصر المعلومات"، دراسة (الردفاني 2014) بعنوان: "تحقيقات الشرطة في مواجهة تحديات الجرائم السيبرانية"، وأكدت هذه الدراسات على أهمية الاستراتيجيات، والآليات التي يجب تفعيلها في تعزيز الأمن السيبراني ومواجهة الجرائم الإلكترونية، التي تهدد استقرار المنظمات الحكومية وغير الحكومية، وأن يجب اتخاذ كافة التدابير الأمنية التقنية وتأمين البنية التحتية من الأخطار المحتملة من بعض فئات البشرية الذين يعملون على اختراقات تقنية إجرامية تضر بمصالح القطاعات العامة والخاصة وعلى مصالح الدولة ككل.

**ثانيا:** أما المحور الثاني في الدّراسات السابقة، فقد تناول في مجال الأمن السيبراني والخدمات الإلكترونية، من خلال دراسة بعنوان: "تطبيقات الأمن السيراني المجانية والبرامج الحاسوبية"، دراسة بعنوان: "حماية الخدمات عبر الإنترنت من النشاط الضار، (Rogers& tina, 2015)، اكدت هذه الدراسات على ضرورة التعزيز الأمني للإنترنت وأمن الشبكات والخدمات الإلكترونية بالتحديد، وحماية

الثورة المعلوماتية للأفراد والمؤسسات، واقتراح حلول للحماية الأنظمة الإلكترونية من أي تجاوزات غير شرعية وغير قانونية من سرقة معلومات أو الاستلال عليها بغير وجه حق، أو الاعتداء بضرب الأنظمة برامج تقنية ضارة.

**ثالثا: أوجه الاتفاق:** اتفقت هذه الدراسة الحالية مع أغلب الدراسات السابقة في الأهمية الكبرى لدور الأمن السيبراني في حماية الأنظمة الإلكترونية، من أي أضرار محتملة أو تهديدات تقنية تصيب الأجهزة، فقد اتفقت الدراسة الحالية مع الدراسات السابقة في التطرق للأضرار التي تأتي على شكل اختراقات أو سرقات أو تسريب معلومات أو ملفات ذات أهمية للمنظمات وخاصة المنظمات الحكومية، والعمل على تعزيز الأمن السيبراني في المنظمة وإيجاد حلول مقترحة لحفاظ على الثورة المعلوماتية.

**رابعًا: الفجوة البحثية**

**جدول (2) الفجوة البحثية**

| الدراسات السابقة | الفجوة البحثية | الدراسة الحالية |
|---|---|---|
| تناولت بعض الدراسات الجرائم الإلكترونية والحروب الإلكترونية وأثرها على مجالات عدة | تناولت الدراسات دور الأمن السيبراني للحد من الهجوم السيبراني ولكن لم تكن الدراسات تستهدف دور الأمن السيبراني في رفع جودة الخدمات الإلكترونية | تستهدف الدراسة الحالية تسليط الضوء على دور الأمن السيبراني في رفع جودة الخدمات الإلكترونية |
| تشترك بعض الدراسات مع الدراسة الحالية في المتغير التابع وهو جودة الخدمات الإلكترونية | ركزت الدراسات السابقة على جودة الخدمات الإلكترونية ولكن لم تربطها بدور الأمن السيبراني | تربط الدراسة الحالية للكشف عن دور الأمن السيبراني بجودة الخدمات الإلكترونية |
| تطرقت بعض الدراسات إلى الأمن السيبراني في مجال التعليم وبرامجه المجانية وغيرها | ركزت على زيادة وعي الطلبة والطالبات عن بالأمن السيبراني وبرامجه وتدريس مجال الأمن السيبراني | اتفقت الدراسة الحالية مع بعض الدراسات في أنها ركزت على الأمن السيبراني في المؤسسات التعليمية (جامعة الملك عبدالعزيز أنموذجًا) ولكنها تركز على دوره في جودة الخدمات الإلكترونية المقدمة للمستفيدين منها على مستوى المؤسسة التعليمية بكافة منسوبيها. |

**خامسا: أوجه الاختلاف:** اختلفت الدراسة الحالية مع الدراسات السابقة من حيث عينة الدراسة الحالية، ومنهج الدراسة الحالية، والأداة المستخدمة لقياس النتائج، كما عملت الدراسة الحالية بتوقيت زمني مختلف مع انطلاق رؤية 2030 بالمملكة العربية السعودية حيث تم إنشاء هيئة الأمن السيبراني لحماية الثورة المعلوماتية بالمملكة، واختلفت الدراسة أيضًا في التطبيق العلمي لها حيث يتم تطبيقها بجامعة الملك عبد العزيز، بعمادة بتقنية المعلومات، شطر الطالبات لعام 1441هـ 2020م.

**أوجه الاستفادة:**

أكدت الدراسات السابقة على أهمية الأمن السيبراني في وقتنا الحالي وما له من تأثير في حماية البينة التحتية المعلوماتية.

**ما يميز الدراسة الحالية عن الدراسات السابقة:**

تتميز الدراسة الحالية على قياس الفعلي في دور الأمن السيبراني في حماية الخدمات الإلكترونية في المنظمات وخاصة المنظمات الحكومية، وندرة الدراسات العلمية بمجال الأمن السيبراني بالعالم العربي وخاصة المملكة العربية السعودية واطلاع جميع الباحثين والمهتمين بالمجال الأمن السيبراني بالمملكة ما توصلت إليه هذه الدراسة الحالية من نتائج فعلية.

# الفصل الثالث

# إجراءات الدراسة

# الفصل الثالث

# إجراءات الدراسة

**تمهيد:**

يتضمن هذا الفصل منهج الدراسة الذي استخدمته الباحثة في دراستها، ويحدد مجتمع الدراسة وكيفية اختيار عينة الدراسة وخصائصها، كما يستعرض أداة الدراسة وطريقة بنائها والتحقق من صدقها وثباتها، ويتناول أخيراً تطبيق الدراسة الميدانية والأساليب الإحصائية التي استخدمتها الباحثة في معالجة البيانات وتحقيق أهداف الدراسة.

## 3-1 منهج الدراسة

تم الاعتماد من الناحية المنهجية لإجراء هذه الدراسة على الأساليب التالية:

- الأسلوب الوصفي القائم على المسح المكتبي لأهم الدراسات والجهود العلمية التي تبحث في موضوع دور الأمن السيبراني في جودة الخدمات الإلكترونية.
- الأسلوب الميداني الذي يعتمد على تطوير استبانة تشتمل على مجموعة من العبارات التي يمكن من خلالها جمع البيانات من عينة الدراسة، وتحليل هذه البيانات ومن ثم استخلاص النتائج.
- الأسلوب الإحصائي باستخدام برنامج الحزمة الإحصائية في العلوم الاجتماعية (**SPSS**) لمعالجة البيانات الأولية التي تم جمعها بهدف تحليلها واستخلاص النتائج منها.

## 3-2 مجتمع الدراسة

نظرا لتخصص هذه الدراسة الحالية بمجال الأمن السيبراني، يتكون مجتمع الدراسة من موظفين وموظفات عمادة تقنية المعلومات بجامعة الملك عبد العزيز، حيث بلغ عدد الموظفين والموظفات بعمادة تقنية المعلومات (221)، منهم (158) موظف، (63) موظفة.

## 3-3 عينة الدراسة

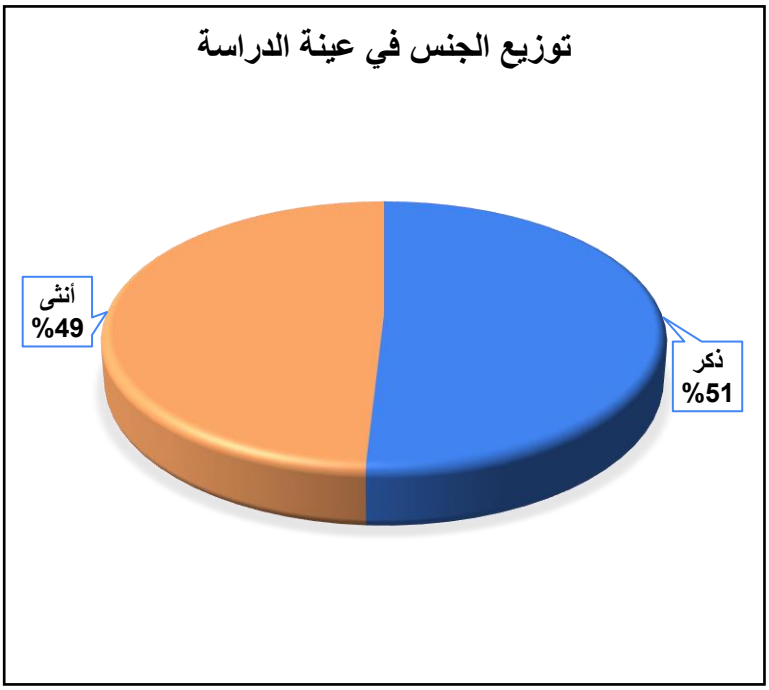
تم تطبيق الدارسة على عينة قصدية مقدراها (150) موظف وموظفة، تم توزيع الاستبيان عليهم، وبلغ عدد الاستبانات المستلمة المكتملة الإجابة (114) بنسبة (76 %) من مجتمع الدارسة.

**خصائص أفراد عينة الدراسة:**

**1- الجنس:**

**جدول (3) توزيع الجنس في عينة الدراسة**

| المتغير | المستويات | التكرار | النسبة (%) |
|---|---|---|---|
| الجنس | ذكر | 58 | **50.9** |
| | أنثى | 56 | **49.1** |
| | **المجموع** | **114** | **%100** |



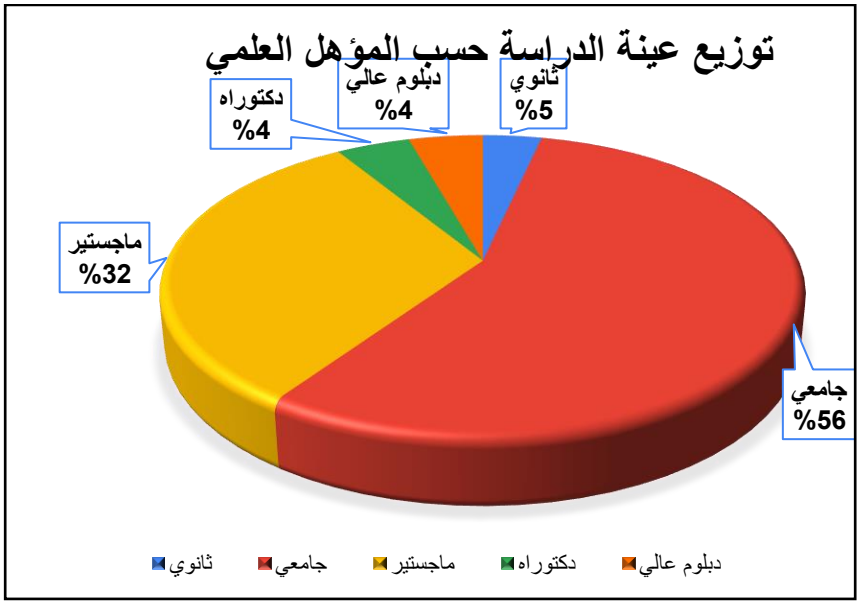

**شكل رقم (3) توزيع الجنس في عينة الدراسة**

يوضح الجدول السابق والرسم البياني أن ما نسبته (50.9 %) من أفراد عينة الدراسة من الذكور، وهي نسبة قليلة إذا ما قورنت بعدد الموظفين الذكور في مجتمع الدراسة، بينما بلغت نسبة الإناث في عينة الدراسة (49.1 %)، وتشير هذه النتيجة إلى أن نسبة الذكور والإناث في عينة الدراسة تكاد تكون متساوية.

2- المؤهل العلمي:

جدول (4) توزيع عينة الدراسة من حيث المؤهل العلمي

| المتغير | المستويات | التكرار | النسبة (%) |
|---|---|---|---|
| المستوى التعليمي | ثانوي | 4 | 3.5 |
| | جامعي | 64 | 56.1 |
| | ماجستير | 36 | 31.6 |
| | دكتوراه | 5 | 4.4 |
| | دبلوم عالي | 5 | 4.4 |
| | المجموع | 114 | %100 |



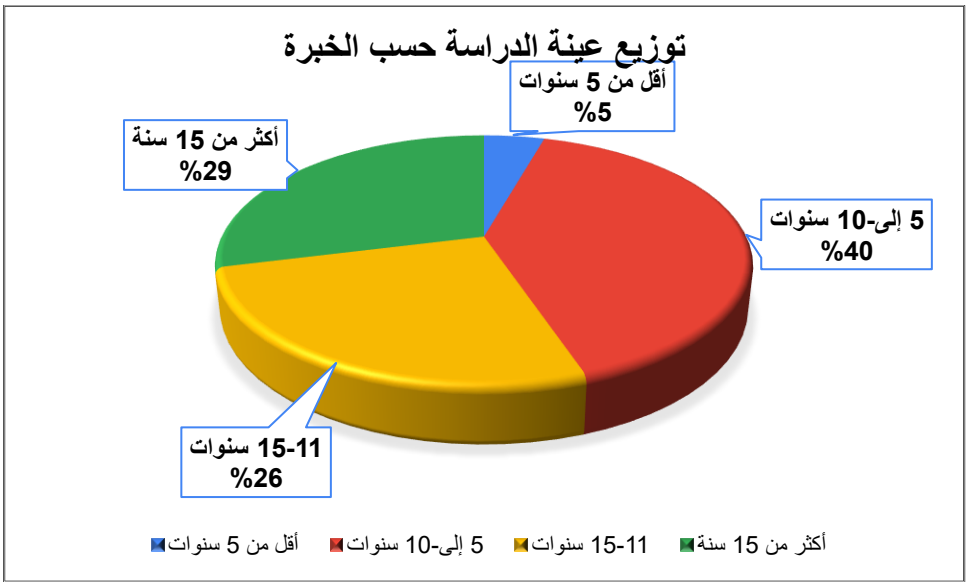

شكل ( 4) خصائص عينة الدراسة من حيث المستوى التعليمي

يوضح الجدول السابق: أن نسبة الحاصلين على مؤهل ثانوي (5 %)، بينما بلغت نسبة الحاصلين على مؤهل جامعي (56 %) وبلغت نسبة الحاصلين على الماجستير (32 %) وبلغت نسبة الحاصلين على الدكتوراه (4 %)، بينما بلغت نسبة الحاصلين على دبلوم (4 %)، وتشير نتائج تحليل العينة إلى تنوع المؤهل التعليمي لأفراد العينة، أي أن معظم عينة الدراسة تتوفر لديهم الكفاءة العلمية والقدرة على تفهم أسئلة الاستبانة والإجابة عليها وإعطاء البيانات الصحيحة.

### 3- الخبرة في مجال العمل:

جدول (5) توزيع عينة الدراسة من حيث الخبرة

| المتغير | المستويات | التكرار | النسبة (%) |
|---|---|---|---|
| الخبرة | أقل من 5 سنوات | 5 | **4.4** |
| | 5 إلى-10 سنوات | 46 | **40.4** |
| | 11-15 سنوات | 30 | **26.3** |
| | أكثر من 15 سنة | 33 | **28.9** |
| | المجموع | **114** | **%100** |




شكل (5) خصائص عينة الدراسة من حيث الخبرة

يوضح الجدول السابق تنوع خبرات أفراد عينة الدراسة من حيث الخبرة، إلا أن الأعلى تمثيلاً من كانت خبرتهم (من 5-10 سنوات) بنسبة (40 %)، يلي ذلك من تراوحت خبرتهم من (أكثر من 15 سنة) بنسبة (29 %)، يلي ذلك من انحصرت خبرتهم في الفئة (11 -15 سنة) بنسبة (26 %) وبلغت نسبة من كانت خبرتهم أقل من خمس سنوات بنسبة (5 %)، إن عامل التفاوت في سنوات الخبرة يشير إلى تمثيل العينة للواقع، وأن عينة الدراسة لديها خبرة جيدة.

## 3-4 أداة الدراسة

تم اختيار أداة الدراسة في جمع البيانات، فجمع البيانات لها أدوات محددة تختلف باختلاف مناهج البحث التي اعتمدتها الباحثة كذلك موضوع الدراسة، فضلاً عن مراعاة الصدق والثبات للأداة.

**خطوات تصميم أداة الدراسة وبنائها:**

اتبعت الباحثة الخطوات التالية لتصميم أداة الدراسة وبنائها المتمثلة في الاستبانة:

1. تحديد مصادر بناء الاستبانة:

اعتمدت الباحثة في بناء الاستبانة على ما يلي:

- ❖ الاطلاع على العديد من الدوريات والمجلات في التربية والأبحاث والدراسات السابقة ذات الصلة بمشكلة الدراسة الحالية.
- ❖ إجراء مقابلات مع المختصين في هذا المجال للتزود من خبراتهم.
- ❖ حضور دورات مخصصة للأمن السيبراني.

2. تحديد أهداف الاستبانة:

تم تصميم استبانة تهدف:

- ❖ معرفة دور الأمن السيبراني في جودة الخدمات الإلكترونية وما حققه من أثر فعال في الخدمات التقنية وحمايتها من الناحية المعلوماتية وهي السرية، والخصوصية، والتعزيز.
- ❖ الكشف عن الاختلافات بين متوسطات استجابات أفراد عينة الدراسة تبعا لمتغيري (المؤهل، الخبرة).

وقد كانت الإجابات على كل فقرة مكونة من (5) اختيارات حيث الدرجة (5) تعني موافق بشـــدة و(1) تعني غير موافق بشدة حسب مقياس ليكرت الخماسي (Scale Likert) الموضح في جدول رقم (3- 4).

**جدول (6) مقياس ليكرت الخماسي**

| التصنيف | موافق بشدة | ⟷ | | | غير موافق بشدة |
|---|---|---|---|---|---|
| **الدرجة** | **5** | **4** | **3** | **2** | **1** |
| **متوسط الدرجة** | 4.20 -5 | 3.40-4.19 | 2.60-3.39 | 1.80-2.59 | -1.78 1.00 |
| **التقدير** | مرتفعة جداً | مرتفعة | متوسطة | ضعيفة | ضعيفة جداً |

## 3-5 صدق أداة الدراسة

تم التأكد من صدق فقرات الاستبانة بطريقتين هما: الصدق الظاهري، وصدق الاتساق الداخلي.

### 1. الصدق الظاهري للأداة

تم التحقق من صدق الأداة بعرضها في صورتها الأولية على (3) محكمين من أعضاء هيئة التدريس المتخصصين في الإدارة، وقد أعدت الباحثة استمارة لاستطلاع آراء المحكمين حول:

- مدى قياس العبارة لمتغيرات محاور الدراسة.
- مدى وضوح العبارة.
- مدى أهمية العبارة.
- التعديل المناسب الذي يراه المحكم على العبارة.

وفي ضوء التعديلات التي أبداها المحكمين قامت الباحثة بتعديل صياغة بعض العبارات لتصبح أكثر وضوحاً وملاءمة لقياس ما وضعت من أجله.

## 2. صدق الاتساق الداخلي

"يقصد به مدى اتساق الفقرات في قياس ما وضعت من أجله، حيث يعد مؤشراً على صدق تلك الفقرات، للتأكد من صدق الفقرات، تم حساب معاملات الارتباط بين درجة كل فقرة بالدرجة الكلية للأداة والبُعد الذي تنتمي إليها باستعمال معامل ارتباط بيرسون، واستُعملت عينة التطبيق الأساسي لأداة الدراسة لهذا الغرض" (Koll, 1960: 426).

**جدول (7) معامل ارتباط بيرسون (Pearson Correlation) لصدق أداة الدراسة**

| المحور | معامل الارتباط بيرسون | الدلالة الإحصائية |
|---|---|---|
| **المحور الأول: الأمن السيبراني** | 0.876 | 0.00 |
| **البعد الأول: السرية** | 0.735 | 0.00 |
| **البعد الثاني: الخصوصية** | 0.797 | 0.00 |
| **البعد الثالث: التعزيز** | 0.792 | 0.00 |
| **المحور الثاني: جودة الخدمات الإلكترونية** | 0.934 | 0.00 |

*** الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$)**

يوضح الجدول السابق وجود علاقة ارتباطية طردية بين المحاور وذات دلالة إحصائية عالية (أقل من أو تساوي 0.05)، ويعتبر معامل ارتباط عالي مما يحقق صدق الاستبانة، وكذلك يؤكد مدى صلاحية الاستبانة للتطبيق أي أن الاستبانة تصلح للدراسة وتراوحت معاملات الارتباط ما بين (0.876: 0.934)، كما يوضح الجدول العلاقة بين متوسطي استجابات العينة لكل محور مع الدرجة الكلية للاستبانة؛ مما يشير إلى الاتساق والارتباط بين تلك المحاور في التعبير عن دور الأمن السيبراني في جودة الخدمات الإلكترونية.

## 3-6 ثبات أداة الدراسة

أجرت الباحثة خطوات الثبات على العينة بطريقة معامل ألفا كرونباخ.

**جدول (8) معامل الثبات ألفا كرونباخ (Cronbach's alpha) لأداة الدراسة ومحاورها**

| الثبات / المحور | عدد العبارات لكل محور | الثبات |
|---|---|---|
| **البعد الأول: السرية** | **6** | 0.931 |
| **البعد الثاني: الخصوصية** | **4** | 0.884 |
| **البعد الثالث: التعزيز** | **4** | 0.888 |
| **الثبات الكلي للمحور الأول: الأمن السيبراني** | | 0.863 |
| **المحور الثاني: جودة الخدمات الإلكترونية** | **7** | 0.891 |
| **الثبات الكلي لأداة الدراسة** | | **0.859** |

يوضح الجدول السابق ثبات أداة الدراسة بطريقة ألفا كرونباخ Cronbach's alpha، قد بلغ الثبات الكلي لأداة الدراسة (0.859)، وهو معامل ثبات مرتفع جداً ومناسب لأغراض الدراسة، كما تعد جميع معاملات الثبات لمحاور الدراسة مرتفعة، ومناسبة لأغراض هذه الدراسة، وهي نسبة ثبات عالية مما يشير إلى تمتع الاستبانة بالثبات، وبذلك تكون الباحثة قد تأكدت من صدق استبانة الدراسة وثباتها مما يؤكد صحة الاستبانة وجاهزيتها لتحليل النتائج لتجاوب عن أسئلة الدراسة، كما تشير إلى موثوقية استخدام الأداة في قياس ما أعدت لقياسه، وصلاحيتها للتطبيق الميداني.

## 3-7 الأساليب الإحصائية:

لتحقيق أهداف الدراسة وتحليل البيانات التي تم تجميعها، فقد تم استخدام العديد من الأساليب الإحصائية المناسبة باستخدام الحزم الإحصائية للعلوم الاجتماعية Package Statistical for Science Social (SPSS)

- التكرارات والنسب المئوية.
- المتوسط الحسابي Artithmetic Mean: لحساب الأوساط الحسابية العامة لمحاور أداة الدراسة، كما تم حساب الأوساط الحسابية الموزونة لكل عبارة من عبارات المحاور المختلفة لقياس دلالة الفروق باستخدام مربع كأي لاستجابات العينة.
- الانحراف المعياري Standard deviation: لمعرفة تشتت أو عدم تشتت استجابات العينة، كما يساعد في ترتيب العبارات أو المتغيرات مع الوسط الوزني، حيث إنه في حالة تساوى العبارات في مجموع الأوزان وبالتالي الوسط الوزني فإن العبارة أو المتغير الذي له انحراف المعياري أقل يأخذ الترتيب الأول.
- اختبار ألفا كرونباخ Cronbach's alpha للتأكد من اختبار درجة ثبات الاستبانة.
- معامل الارتباط بيرسون: Pearson Correlation Coefficient لقياس درجة دور الامن السيبراني في تجودة الخدمات الالكترونية .
- اختبار (One Way Anova): وقد استخدم في البحث لقياس دلالة الفروق بين التكرارات المحسوبة والتكرارات المتوقعة حسب استجابات مجتمع البحث في مختلف خصائصها الديموغرافية بهدف التعرف على الفروق بين متوسطات الاستجابات.

# الفصل الرابع

# عرض ومناقشة النتائج

# الفصل الرابع

# عرض ومناقشة النتائج

**مقدمة:**

يتناول هذا الفصل عرضاً للنتائج التي توصلت إليها الدراسة والمعالجة الإحصائية للنتائج، وذلك من خلال عرض نتائج أسئلة الدراسة ثم تفسير النتائج ومناقشتها في ضوء الأدبيات والدراسات السابقة.

## 4-1 عرض ومناقشة نتائج السؤال الأول:

**مادور بُعد السرية في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟**

تم استخدام بعض مقاييس الإحصاء الوصفي والتي تمثلت في المتوسط الحسابي والانحراف المعياري لكل عبارة من العبارات التي تقيس درجة السرية في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز من وجهة نظر العاملين بها.

**جدول (9) البعد الأول: السرية**

| م | العبـارة | مجموع الأوزان | الانحراف المعياري | المتوسط الحسابي | درجة الأهمية | التقدير |
|---|---|---|---|---|---|---|
| 1 | لدي كلمة مرور قوية تتكون من رموز وأحرف وأرقام صغيرة وكبيرة. | 530.0 | 0.6515 | 4.649 | 1 | مرتفعة جداً |
| 3 | يحدد النظام هوية الموظفين في حالة الدخول على البيانات أو القيام بتعديل عليها. | 499.0 | 0.8864 | 4.377 | 2 | مرتفعة جداً |
| 5 | توجد تعليمات إدارية صريحة حول حماية النظام من أي تلاعب أو غش. | 496.0 | 0.8306 | 4.351 | 3 | مرتفعة جداً |
| 6 | لدي معرفة بنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها. | 466.0 | 1.0181 | 4.088 | 4 | مرتفعة |
| 4 | يسمح النظام بإدخال نفس المسندات الإلكترونية أكثر من مرة. | 330.0 | 1.1080 | 2.895 | 5 | متوسطة |
| 2 | يتم تبادل أرقام المرور السرية بين الموظفين للأنظمة الإلكترونية. | 235.0 | 1.2214 | 2.061 | 6 | ضعيفة |
| | **المعدل العام للبعد الأول: السرية** | 426.0 | 0.5046 | 3.737 | **مرتفعة** | |

يوضح جدول (9) ما يلي:

- أن متوسطات عبارات البعد الأول: السرية تراوحت بين (2.061-4.649) وفق مقياس ليكرت الخماسي، حيث بلغ المتوسط العام لعبارات هذا البعد (3.737)، ووفقاً لمقياس ليكرت الخماسي، فإن درجة السرية من وجهة نظر عينة الدراسة كانت بدرجة مرتفعة، ويلاحظ أن أغلب استجابات عينة الدراسة على عبارات البعد الأول كانت تتراوح بين تقدير (ضعيفة: مرتفعة جداً)؛ مما يدل على أن اتجاهات أفراد العينة كانت إيجابية لهذا البعد، وهذه النتيجة تتفق مع نتيجة دراسة (الشهري، 2019) حيث أكدت أن أفراد العينة موافقون على محور "التدابير والإجراءات المجتمعية، المؤسسية والشخصية، للوقاية من الجرائم السيبرانية، وهو ما يؤكد على اتباعهم السرية كإحدى وسائل الأمن السيبراني، كما اتفقت مع نتيجة دراسة (الشوابكة، 2019) والتي أكدت أن الإجراءات الأمنية لمنع الاختراق عن طريق الشبكة الحاسوبية Network Hacking في الجامعة جاءت بمستوى مرتفع، مما يؤكد على استخدام السرية في المعلومات، واتفقت مع دراسة (البسام، 2018) والتي جاء بها أن المشاركين موافقين بشدة على أهمية دعم الإدارة العليا من أجل الوعي بالأمن السيبراني في البنوك البحرينية ويظهر علاقة كبيرة بين التزام الإدارة العليا والدعم والوعي بالأمن السيبراني وجاء في المرتبة الثانية مما يعكس أهمية السرية في المعلومات للأمن السيبراني، واتفقت أيضاً مع دراسة (العتيبي، 2017) التي توصلت إلى إن الإجراءات التقنية لحماية الفضاء السيبراني الخاص بالشركة متوفرة بدرجة كبيرة، واستخدام القياسات الحيوية (بصمة العين – بصمة الإصبع – بصمة الصوت) لمرور المصرح لهم، مما يعكس توفر السرية كأحد وسائل الأمن السيبراني؛ واختلفت النتيجة الحالية مع دراسة (حميد، 2019) حيث أنها أكدت على قلة الخبرة وضعف التأهيل والتدريب مما يعكس أن السرية غير متوفرة كأحد وسائل الأمن السيبراني.
- مما سبق يتضح أن العاملين في عمادة تقنية المعلومات بجامعة الملك عبد العزيز يمارسون بعد السرية بدرجة مرتفعة، وتعزو الباحثة ذلك إلى أن العاملين مدربين على الحفاظ على سرية المعلومات فأغلب عينة الدراسة من الحاصلين على مؤهل جامعي ودرجة الماجستير مما يؤهلهم للحفاظ على سرية المعلومات، ولإن عادة ما ينطوي الهجوم الإلكتروني على استخدام برمجيات ضارة لتغيير الرموز البرمجية الرقمية والمنطق الرياضي أو البيانات، مما يؤدي إلى عواقب تخريبية والتي يمكن أن تضر بسرية وسلامة وتوافر البيانات وبالتالي تؤدي إلى التلاعب في نظم المعلومات والبنية التحتية للشبكة.

## 2-4 عرض ومناقشة نتائج السؤال الثاني:

**مادور بُعد الخصوصية في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟**

تم استخدام بعض مقاييس الإحصاء الوصفي والتي تمثلت في المتوسط الحسابي والانحراف المعياري لكل عبارة من العبارات التي تقيس درجة الخصوصية في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز من وجهة نظر العاملين بها.

**جدول (10) البعد الثاني: الخصوصية**

| م | العبـارة | مجموع الأوزان | الانحراف المعياري | المتوسط الحسابي | درجة الأهمية | التقدير |
|---|---|---|---|---|---|---|
| **4** | يتم تشغيل وتحديث جدار الحماية باستمرار لمنع المتسللين من الوصول للبيانات الشخصية أو بيانات العمادة. | 516.0 | 0.7190 | 4.526 | 1 | مرتفعة جداً |
| **3** | تستخدم عمادة تقنية المعلومات عدة تقنيات مثل: المصادقة والترخيص والتشفير لحماية الأنظمة والبيانات الحساسة. | 483.0 | 0.7677 | 4.237 | 2 | مرتفعة جداً |
| **1** | تقوم عمادة تقنية المعلومات بمراجعة صلاحيات المستخدمين على فترات منتظمة. | 429.0 | 1.1075 | 3.763 | 3 | مرتفعة |
| **2** | أواجه اختراقات على بريدي الإلكتروني بشكل متكرر. | 217.0 | 0.9020 | 1.904 | 4 | ضعيفة |
| **المعدل العام للبعد الثاني: الخصوصية** | | **411.3** | **0.5505** | **3.607** | **مرتفعة** | |

يوضح جدول (10) ما يلي:

- أن متوسطات عبارات البعد الثاني: الخصوصية تراوحت بين (1.904-4.526) وفق مقياس ليكرت الخماسي، حيث بلغ المتوسط العام لعبارات هذا البعد (3.607)، ووفقاً لمقياس ليكرت الخماسي، فإن درجة الخصوصية من وجهة نظر عينة الدراسة كانت بدرجة مرتفعة، ويلاحظ أن أغلب استجابات عينة الدراسة على عبارات البعد الثاني كانت تتراوح بين تقدير (ضعيفة: مرتفعة جداً)، مما يدل على أن اتجاهات أفراد العينة كانت إيجابية لهذا البعد، وهذه النتيجة تتفق مع نتيجة دراسة (الشهري، 2019) حيث أكدت أن أفراد العينة موافقون بشدة على محور "التدابير الوقائية، الموقفية والاجتماعية، المعتمدة في الوقاية من – الجرائم السيبرانية، وهو ما يؤكد

- على توفر الخصوصية كإحدى وسائل الأمن السيبراني، كما اتفقت مع نتيجة (شلوش، 2018) بشكل ضمني حيث أكدت على الدول والأفراد اتخاذ الحذر والحيطة عند استعمال البيانات والمعلومات في المجال الافتراضي، لتجنب المخاطر المحتملة في التصيد الشبكي والهاكرز والجماعات الإرهابية، كما اتفقت مع دراسة (الشوابكة، 2019) والتي أكدت أن الإجراءات الأمنية لمنع الاختراق عن طريق الشبكة الحاسوبية Network Hacking في الجامعة جاءت بمستوى مرتفع، مما يؤكد على استخدام الخصوصية في المعلومات، واتفقت مع دراسة (البسام، 2018) والتي جاء بها أن المشاركين موافقين بشدة على أن الامتثال الأمني ضروري لـــ CSA وأنه كان هناك علاقة مهمة بين الامتثال للأمن السيبراني وCSA وجاء بالمرتبة الأولى أهمية الامتثال الأمني؛ مما يعكس أهمية الخصوصية في المعلومات للأمن السيبراني، واتفقت أيضاً مع دراسة (العتيبي، 2017) التي توصلت إلى إن الإجراءات الفنية لحماية الفضاء السيبراني للشركة متوفرة بدرجة كبيرة، حيث يتم قفل النظام آلياً في حالة عدم استخدامه لفترة زمنية محددة مما يعكس توفر الخصوصية كأحد وسائل الأمن السيبراني؛ واختلفت النتيجة الحالية مع دراسة (حميد، 2019) ضمنياً حيث أنها أكدت على قلة الخبرة وضعف التأهيل والتدريب مما يعكس أن الخصوصية غير متوفرة كأحد وسائل الأمن السيبراني.
- مما سبق يتضح أن العاملين في عمادة تقنية المعلومات بجامعة الملك عبد العزيز يمارسون بعد الخصوصية بدرجة مرتفعة، وتعزو الباحثة ذلك إلى أن العاملين مدركون باهتمام الجامعة بخصوصية الأمن السيبراني في الجامعة وهي لضمان سرية ومعلومات الطلبة وأعضاء هيئة التدريس والتي يتم حفظها في قواعد البيانات ولا يتم نشرها.

## 4-3 عرض ومناقشة نتائج السؤال الثالث:

**مادور بُعد التعزيز في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟**

تم استخدام بعض مقاييس الإحصاء الوصفي والتي تمثلت في المتوسط الحسابي والانحراف المعياري لكل عبارة من العبارات التي تقيس درجة التعزيز في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز من وجهة نظر العاملين بها.

**جدول (11) البعد الثالث: التعزيز**

| م | العبـارة | مجموع الأوزان | الانحراف المعياري | المتوسط الحسابي | درجة الأهمية | التقدير |
|---|---|---|---|---|---|---|
| 2 | تستخدم برامج مكافحة الفيروسات بشكل دوري في أجهزة عمادة تقنية المعلومات لحمايتها من البرامج الضارة. | 537.0 | 0.5601 | 4.711 | 1 | مرتفعة جداً |
| 4 | توجد نسخ احتياطية (Back up) بشكل دوري في أقراص صلبة أو سحابة خاصة بالعمادة. | 512.0 | 0.7785 | 4.491 | 2 | مرتفعة جداً |
| 3 | تستخدم برامج مكافحة التجسس بشكل دوري في أجهزة عمادة تقنية المعلومات لحمايتها من البرامج الضارة | 506.0 | 0.7986 | 4.439 | 3 | مرتفعة جداً |
| 1 | تتم مراقبة الموظفين للتأكد من تطبيق السياسات والإجراءات الوقائية لمنع تسريب المعلومات | 437.0 | 0.9678 | 3.833 | 4 | مرتفعة |
| **المعدل العام للبعد الثالث: التعزيز** | | 498.0 | 0.5905 | 4.368 | **مرتفعة جداً** | |

يوضح جدول (11) ما يلي:

- أن متوسطات عبارات البعد الثالث: التعزيز تراوحت بين (3.833-4.711) وفق مقياس ليكرت الخماسي، حيث بلغ المتوسط العام لعبارات هذا البعد (4.368)، ووفقاً لمقياس ليكرت الخماسي، فإن درجة التعزيز من وجهة نظر عينة الدراسة كانت بدرجة مرتفعة جداً، ويلاحظ أن أغلب استجابات عينة الدراسة على عبارات البعد الثالث كانت تتراوح بين تقدير (مرتفعة: مرتفعة جداً)، مما يدل على أن اتجاهات أفراد العينة كانت إيجابية بشكل كبير لهذا البعد، وهذه النتيجة تتفق مع نتيجة دراسة (الشهري، 2019) حيث أن أفراد العينة موافقون بشدة على محور "التدابير التشريعية وأنظمة العدالة الجنائية الفعالة للوقاية من الجرائم السيبرانية، ومحور "التدابير الخاصة ببناء القدرات الوطنية في المجالات ذات الصلة بالجرائم السيبرانية والوقاية منها، وهو ما يؤكد على توفر التعزيز اللازم لحماية المعلومات ويعزز الأمن السيبراني في الجامعة، كما توافقت مع دراسة (حميد، 2019) والتي تعمل على تحقيق الوقاية المبكرة من الجرائم السيبرانية، رفع نسبة الكفاءة الوطنية والوسائل الأمنية المستخدمة لحماية البنية التحتية الوطنية، مما يؤكد على استهداف تعزيز الأمن السيبراني ضد الانتهاكات، كما اتفقت النتيجة الحالية مع دراسة (البشام، 2018) والتي أكدت على أهمية الامتثال الأمني مما يعكس أن المشاركين موافقون بشدة على أن الامتثال الأمني ضروري لـ CSA وأنه كان هناك علاقة مهمة بين الامتثال للأمن السيبراني وCSA وجاء بالمرتبة الأولى،

كما اتفقت مع دراسة (العتيبي، 2017) التي أظهرت أن سياسات الأمن السيبراني متوفرة بدرجة كبيرة في الشركة، حيث تضمن الأنظمة آلية فعالة للإبلاغ عن أي محاولات للاختراق؛ وتباينت النتيجة الحالية مع دراسة (الشوابكة، 2019) والتي أظهرت أن الإجراءات الأمنية لمنع الاختراق عن طريق البرمجيات الضارة Malware جاءت بمستوى متوسط، وهو عكس ما أكدت عليه الدراسة الحالية وهو أن تعزيز الأمن السيبراني بمستوى مرتفع جداً.

- مما سبق يتضح أن العاملين في عمادة تقنية المعلومات بجامعة الملك عبد العزيز يمارسون بعد التعزيز بدرجة مرتفعة جداً، مما يعكس اهتمام الجامعة بالأمن السيبراني على أجهزة وشبكات الحاسب الآلي، بما في ذلك العمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث، حيث يساعد الأمن السيبراني في الحفاظ علي البيانات من الاختراقات، وذلك من بالاهتمام والحفاظ علي بنية المعلومات والخدمات التي تقدمها المؤسسات إلى المستفيدين وذلك عن طريق وضع جدار ناري يحمي بيئة العمل من الاختراقات، ولابد من وجود برامج مضادة للفيروسات"Antivirus"، وغلق مواقع الإنترنت الضارة.

## 4-4 عرض ومناقشة نتائج السؤال الرابع:

**ما درجة جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟**

تم استخدام بعض مقاييس الإحصاء الوصفي والتي تمثلت في المتوسط الحسابي والانحراف المعياري لكل عبارة من العبارات التي تقيس درجة جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز من وجهة نظر العاملين بها.

**جدول (12) جودة الخدمات الإلكترونية**

| م | العبارة | مجموع الأوزان | الانحراف المعياري | المتوسط الحسابي | درجة الأهمية | التقدير |
|---|---|---|---|---|---|---|
| 5 | تمتلك الجامعة فريق دعم فني متخصص يعمل على حل المشكلات التي تواجه المستخدمين عبر الموقع الإلكتروني. | 509.0 | 0.6542 | 4.465 | 1 | مرتفعة جداً |
| 4 | يضمن الموقع الإلكتروني للجامعة السرية للمعلومات الخاصة بالمستخدمين. | 496.0 | 0.6378 | 4.351 | 2 | مرتفعة جداً |
| 3 | يستطيع الموظف والطالب الوصول إلى الخدمات التي تقدمها الجامعة في موقعها الإلكتروني بسهولة. | 495.0 | 0.7623 | 4.342 | 3 | مرتفعة جداً |

| م | العبـارة | مجموع الأوزان | الانحراف المعياري | المتوسط الحسابي | درجة الأهمية | التقدير |
|---|---|---|---|---|---|---|
| 1 | توفر الصفحة الإلكترونية الخاصة بالجامعة معلومات وافية عن الجامعة واختصاصاتها | 484.0 | 0.6319 | 4.246 | 4 | مرتفعة جداً |
| 2 | يعرض الموقع الإلكتروني للجامعة المعلومات بكل دقة وموثوقية. | 446.0 | 0.8781 | 3.912 | 5 | مرتفعة |
| 7 | يوفر موقع الجامعة سهولة الحصول على الاستجابة السريعة للمستخدمين. | 416.0 | 0.9311 | 3.649 | 6 | مرتفعة |
| 6 | يوفر موقع الجامعة الرد الآلي عن أي استفسار من المستخدمين. | 400.0 | 1.0326 | 3.509 | 7 | مرتفعة |
| **المعدل العام: جودة الخدمات الإلكترونية** | | **463.7** | **0.5790** | **4.068** | **مرتفعة** | |

يوضح جدول (12) ما يلي:

- أن متوسطات عبارات جودة الخدمات الإلكترونية تراوحت بين (3.509-4.465) وفق مقياس ليكرت الخماسي، حيث بلغ المتوسط العام لعبارات هذا البعد (4.068)، ووفقاً لمقياس ليكرت الخماسي، فإن درجة جودة الخدمات الإلكترونية من وجهة نظر عينة الدراسة كانت بدرجة مرتفعة، ويلاحظ أن أغلب استجابات عينة الدراسة على عبارات جودة الخدمات الإلكترونية كانت تتراوح بين تقدير (مرتفعة: مرتفعة جداً)، مما يدل على أن اتجاهات أفراد العينة كانت إيجابية بشكل كبير لهذا البعد، وهذه النتيجة تتفق مع نتيجة دراسة (عبد الراضي، 2018) التي أظهرت نتائج الدراسة أن جودة الخدمات الإلكترونية (تصميم الموقع، سهولة الاستخدام، السرية، توفير الوقت، الموثوقية، الاستجابة، الاعتمادية، والاتصال) كانت بدرجة مرتفعة، واتفقت مع دراسة (الصومالي، 2015) والتي أظهرت وجود علاقة إيجابية بين الأبعاد الأربعة لجودة الخدمة الإلكترونية مع مستوى رضا المستفيدين عن الخدمات الإلكترونية التي تقدمها المديرية العامة للجوازات وبدرجة عالية؛ واختلفت النتيجة الحالية مع دراسة (غانم، 2019) وقد توصلت الدراسة إلى إن: جودة الخدمات الإلكترونية التي تقدمها مكتبة معهد الفنون الجميلة احتلت درجة متوسطة، كما اختلفت مع دراسة (العضايلة، 2017) حيث أظهرت أن مستوى جودة الخدمات الإلكترونية التي تقدمها جامعة الأميرة نورة من وجه نظر الطالبات كان بمستوى ضعيف.
- مما سبق يتضح أن جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز تتميز بدرجة مرتفعة من وجهة نظر العاملين، وتعزو الباحثة ذلك إلى أن الجامعة تهتم بكافة أنظمة الحماية والخصوصية وهذا أمر مهم للمستخدم لأن

الموقع يشمل بيانات ومعلومات خاصة ومهمة وذات قيمة بالإضافة إلى تمتع الموقع بواجهات تفاعلية حديثة وجذابة وسلسة وسهلة الاستخدام ويقوم الفريق الفني المسئول عن متابعة الموقع بدوره ليعمل بشكل متواصل وباستمرار والحد من أي انقطاع للخدمة وإن حدثت يتم حلها وتجاوزها بأقصى سرعة ممكنة دون التأثير على المستخدمين، كما يعرض الموقع الإلكتروني للجامعة المعلومات بكل دقة وموثوقية.

## 4-5 عرض ومناقشة نتائج السؤال الرابع:

**ما دور الأمن السيبراني من خلال أبعاد (السرية، الخصوصية، التعزيز) في تجويد الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز؟**

تم استخدام بعض مقاييس الإحصاء الوصفي والتي تمثلت في معامل الانحدار المتعدد لقياس أثر الأمن السيبراني بأبعاده على جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز.

**جدول (13) دور الأمن السيبراني في تجويد الخدمات الإلكترونية**

| المتغيرات المستقلة | معاملات الانحدار | قيمة اختبار T | القيمة الاحتمالية Sig |
|---|---|---|---|
| السرية | 0.066 | 0.919 | 0.360 |
| الخصوصية | 0.309 | 3.579 | 0.001 |
| التعزيز | 0.513 | 6.168 | 0.00 |
| معامل الارتباط = 0.722 | | معامل التحديد= 0.522 | |
| قيمة اختبار F = 39.985 | | القيمة الاحتمالية = 0.00 | |

يوضح جدول (13) ما يلي:

- معامل الارتباط = 0.722، ومعامل التحديد المعدل= 0.522 وهذا يعني أن 52.2% من التغير في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز من خلال العلاقة الخطية والنسبة المتبقية قد ترجع لعوامل أخرى تؤثر في جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز.
- فيمة الاختبار (F) بلغت (39.985) كما أن القيمة الاحتمالية تساوي (0.00) مما يعني وجود علاقة ذات دلالة إحصائية بين الأمن السيبراني وجودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز.

- تبين أن المتغيران المستقلان (الخصوصية، التعزيز) يؤثران في جودة الخدمات الإلكترونية، بينما المتغير المستقل (السرية) لا يؤثر بشكل واضح في جودة الخدمات الإلكترونية.

## 4-6 عرض ومناقشة نتائج السؤال الرابع:

**هل توجد فروق ذات دلالة إحصائية في استجابات عينة الدراسة حول دور الأمن السيبراني بأبعاده (السرية، الخصوصية، التعزيز) تعزى للمتغيرات الديمغرافية (المؤهل العلمي، الخبرة العملية)؟**

تم استخراج قيمة "ف" والدلالة المعنوية لجميع المحاور والدرجة الكلية للاستبانة، باستخدام تحليل التباين الأحادي One Way (ANOVA) طبقاً لاختلاف متغيرات الدراسة الشخصية والوظيفية.

**أولاً: المؤهل العلمي**

**جدول (14) نتائج تحليل التباين الأحادي (One Way ANOVA) طبقاً لاختلاف متغير المؤهل العلمي**

| المحاور | مصدر التباين | مجموع المربعات | درجات الحرية | متوسط المربعات | قيمة "ف" | الدلالة (Sig) |
|---|---|---|---|---|---|---|
| **السرية** | بين المجموعات | 1.882 | 4 | 0.471 | **1.908 | 0.114 |
| | داخل المجموعات | 26.890 | 109 | 0.247 | | |
| | المجموع | 28.772 | 113 | | | |
| **الخصوصية** | بين المجموعات | 2.202 | 4 | 0.550 | **1.872 | 0.120 |
| | داخل المجموعات | 32.044 | 109 | 0.294 | | |
| | المجموع | 34.246 | 113 | | | |
| **التعزيز** | بين المجموعات | 1.483 | 4 | 0.371 | **1.065 | 0.377 |
| | داخل المجموعات | 37.919 | 109 | 0.348 | | |
| | المجموع | 39.401 | 113 | | | |
| **الدرجة الكلية: الأمن السيبراني** | بين المجموعات | 1.356 | 4 | 0.339 | **1.882 | 0.119 |
| | داخل المجموعات | 19.634 | 109 | 0.180 | | |

| المحاور | مصدر التباين | مجموع المربعات | درجات الحرية | متوسط المربعات | قيمة "ف" | الدلالة (Sig) |
|---|---|---|---|---|---|---|
| | المجموع | 20.989 | 113 | | | |
| جودة الخدمات الإلكترونية | بين المجموعات | 1.015 | 4 | 0.254 | **0.750 | 0.560 |
| | داخل المجموعات | 36.872 | 109 | 0.338 | | |
| | المجموع | 37.886 | 113 | | | |
| **الدرجة الكلية للاستبانة** | **بين المجموعات** | **0.997** | **4** | **0.249** | **1.195** | **0.317** |
| | **داخل المجموعات** | **22.738** | **109** | **0.209** | | |
| | **المجموع** | **23.735** | **113** | | | |

*** الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$)**

**** الارتباط غير دال إحصائياً عند مستوى دلالة ($\alpha > 0.05$)**

- تبين أن القيمة الاحتمالية (Sig) المقابلة لاختبار تحليل التباين الأحادي أكبر من مستوى الدلالة ($\alpha > 0.05$)، في جميع محاور الاستبانة، الدرجة الكلية للاستبانة، وبذلك يمكن استنتاج عدم وجود فروق ذات دلالة إحصائية بين متوسطات تقديرات مجتمع الدراسة حول دور الأمن السيبراني في جودة الخدمات الإلكترونية تعزى إلى متغير المؤهل العلمي؛ وهذا يعني أن آراء أفراد مجتمع الدراسة لا يختلف باختلاف المؤهل العلمي، وتعزو الباحثة ذلك إلى أن مجتمع الدراسة على الرغم من اختلاف المستوى التعليمي إلا أن مستوى ممارسة الأمن السيبراني لديهم متقارب فأغلب عينة الدراسة على درجة كافية من التعليم ويحملون درجة البكالوريوس والماجستير.

**ثانياً: الخبرة العملية**

**جدول (15) نتائج تحليل التباين الأحادي (One Way ANOVA) طبقاً لاختلاف متغير الخبرة العملية**

| المحاور | مصدر التباين | مجموع المربعات | درجات الحرية | متوسط المربعات | قيمة "ف" | الدلالة (Sig) |
|---|---|---|---|---|---|---|
| السرية | بين المجموعات | 1.321 | 3 | 0.440 | **1.764 | 0.158 |
| | داخل المجموعات | 27.451 | 110 | 0.250 | | |
| | المجموع | 28.772 | 113 | | | |
| | بين المجموعات | 1.561 | 3 | 0.520 | **1.751 | 0.161 |

| المحاور | مصدر التباين | مجموع المربعات | درجات الحرية | متوسط المربعات | قيمة "ف" | الدلالة (Sig) |
|---|---|---|---|---|---|---|
| **الخصوصية** | داخل المجموعات | 32.685 | 110 | 0.297 | | |
| | المجموع | 34.246 | 113 | | | |
| **التعزيز** | بين المجموعات | 0.609 | 3 | 0.203 | | |
| | داخل المجموعات | 38.793 | 110 | 0.353 | 0.575** | 0.632 |
| | المجموع | 39.401 | 113 | | | |
| **الدرجة الكلية: الأمن السيبراني** | بين المجموعات | 0.592 | 3 | 0.197 | | |
| | داخل المجموعات | 20.397 | 110 | 0.185 | 1.065** | 0.367 |
| | المجموع | 20.989 | 113 | | | |
| **جودة الخدمات الإلكترونية** | بين المجموعات | 1.007 | 3 | 0.336 | | |
| | داخل المجموعات | 36.879 | 110 | 0.335 | 1.001** | 0.395 |
| | المجموع | 37.886 | 113 | | | |
| **الدرجة الكلية للاستبانة** | **بين المجموعات** | **0.698** | **3** | **0.233** | | |
| | **داخل المجموعات** | **23.037** | **110** | **0.209** | **1.112**** | **0.348** |
| | **المجموع** | **23.735** | **113** | | | |

*** الارتباط دال إحصائياً عند مستوى دلالة ($\alpha \leq 0.05$)**

**** الارتباط غير دال إحصائياً عند مستوى دلالة ($\alpha > 0.05$)**

- تبين أن القيمة الاحتمالية (Sig) المقابلة لاختبار تحليل التباين الأحادي أكبر من مستوى الدلالة ($\alpha > 0.05$)، في جميع محاور الاستبانة، الدرجة الكلية للاستبانة، وبذلك يمكن استنتاج عدم وجود فروق ذات دلالة إحصائية بين متوسطات تقديرات مجتمع الدراسة حول دور الأمن السيبراني في جودة الخدمات الإلكترونية تعزى إلى متغير الخبرة العملية؛ وهذا يعني أن آراء أفراد مجتمع الدراسة لا يختلف باختلاف الخبرة العملية، وتعزو الباحثة ذلك إلى أن مجتمع الدراسة على الرغم من اختلاف الخبرة العملية إلا أن مستوى ممارسة الأمن السيبراني لديهم متقارب فأغلب عينة الدراسة على خبرة بالعمل من (5-15) عام.

# الفصل الخامس

# الاستنتاجات والتوصيات

# الفصل الخامس

# الاستنتاجات والتوصيات

## تمهيد:

يتضمن هذا الفصل عرضاً موجزاً لأهم ما تناولته فصول الدراسة، كما يتضمن عرضاً لأهم نتائج الدراسة التي توصلت إليها الباحثة، وذلك من خلال الدراسة التطبيقية بالإضافة إلى مجموعة من التوصيات التي يمكن الاستفادة منها في عمادة تقنية المعلومات بجامعة الملك عبد العزيز.

ويشتمل هذا الفصل على:

- خلاصة الدراسة
- استنتاجات الدراسة
- التوصيات

## 5-1 الخلاصة

توصلت الباحثة في هذه الدراسة إلى التعرف على دور الأمن السيبراني في جودة الخدمات الإلكترونية بعمادة تقنية المعلومات بجامعة الملك عبد العزيز، ولقد تكونت الدراسة من خمسة فصول رئيسية، بالإضافة إلى المراجع والملاحق.

تناول **الفصل الأول**: الإطار العام للدراسة حيث تكون من مقدمة، مشكلة الدراسة، أسئلة الدراسة، نموذج الدراسة، أهداف الدراسة وأهميتها، مصطلحات الدراسة، حدود الدراسة.

كما تم تقسيم **الفصل الثاني** بعد التمهيد إلى ثلاثة مباحث: تناول المبحث الأول: الأمن السيبراني من جوانب مختلفة، وتناول المبحث الثاني: جودة الخدمات الإلكترونية، أما المبحث الثالث: فقد تناول مجموعة من الدراسات السابقة عن الأمن السيبراني من جهة وعن جودة الخدمات الإلكترونية من جهة أخرى، لمعرفة النتائج التي توصلت إليها هذه الدراسات، وذكر أوجه الشبه والفجوة البحثية والاختلاف بينها وبين الدراسة الحالية من حيث المنهج والمكان ومتغيرات الدراسة والأداة المستخدمة.

وتناول **الفصل الثالث**: الوصف المنهجي الذي تم استخدامه لإجراء هذه الدراسة وتضمن منهج الدراسة، المجتمع والعينة، كما شمل وصف للإجراءات التي قامت بها الباحثة في تصميم أداة الدراسة، وقياس ثباتها وصدقها، والأدوات التي استخدمت لجمع بيانات الدراسة.

**كما تناول الفصل الرابع**: التحليل الإحصائي للبيانات، ومناقشة نتائج الدراسة، حيث تم استخدام الحزمة الإحصائية للعلوم الاجتماعية (Statistical Package for Social Science) (SPSS: 25) لمعرفة نتائج تحليل الدراسة.

وتضمن **الفصل الخامس**: خلاصة لجميع فصول الدراسة، بالإضافة للاستنتاجات والتوصيات ثم تبعه المراجع والملاحق.

## 5-2 الاستنتاجات

أظهرت النتائج عند توزيع العينة:

- **يمارس العاملون في عمادة تقنية المعلومات بجامعة الملك عبدالعزيز بعد الســـرية بدرجة مرتفعة**، وتعزو الباحثة ذلك إلى أن العاملين مدربين على الحفاظ على سرية المعلومات فأغلب عينة الدراسة من الحاصلين على مؤهل جامعي ودرجة الماجستير مما يؤهلهم للحفاظ على ســرية المعلومات، ولأن عادة ما ينطوي الهجوم الإلكتروني على اســتخدام برمجيات ضــارة لتغيير الرموز البرمجية الرقمية والمنطق الرياضـي أو البيانات؛ مما يؤدي إلى عواقب تخريبية والتي يمكن أن تضـر بسـرية وسـلامة وتوافر البيانات وبالتالي تؤدي إلى التلاعب في نظم المعلومات والبنية التحتية للشبكة.
- **يمارس العاملون في عمادة تقنية المعلومات بجامعة الملك عبد العزيز بعد الخصوصية بدرجة مرتفعة**، وتعزو الباحثة ذلك إلى أن العاملين مدركون باهتمام الجامعة بخصـوصـية الأمن السـيبراني فيها لضـمان سـرية ومعلومات الطلبة وأعضـاء هيئة التدريس والتي يتم حفظها في قواعد البيانات ولا يتم نشرها.
- **يمارس العاملون في عمادة تقنية المعلومات بجامعة الملك عبد العزيز بعد التعزيز بدرجة مرتفعة جداً**، مما يعكس اهتمام الجامعة بالأمن السـيبراني على الأجهزة والحاسـب الآلي، وتتضـمن حماية المعدات وأجهزة الكمبيوتر والمعلومات والخدمات من أي تســجيل دخول غير مصــرح أو غير مقصــود أو تغيير قد يحدث، حيث يعاون الأمن الســيبراني في تأمين البيانات من الاختراق، وذلك بالاهتمام والحفاظ علي البيانات والمعلومات والخدمات التي تقدمها المؤسسات إلى العملاء وذلك عن طريق بناء جدار ناري لحماية بيئة العمل من الاختراق، ولابد من وجود برامج مضــادة للفيروســات"Antivirus"، وغلق مواقع الإنترنت الضارة.
- **جودة الخدمات الإلكترونية في عمادة تقنية المعلومات بجامعة الملك عبد العزيز تتميز بدرجة مرتفعة من وجهة نظر العاملين**، وتعزو الباحثة ذلك إلى أن الجامعة تهتم بكافة أنظمة الحماية والخصــوصــية وهذا أمر مهم للمســتخدم لأن الموقع

يشمل بيانات ومعلومات خاصة ومهمة وذات قيمة بالإضافة إلى تمتع الموقع بواجهات تفاعلية حديثة وجذابة وسلسة وسهلة الاستخدام ويقوم الفريق الفني المسؤول عن متابعة الموقع بدوره ليعمل بشكل متواصل وباستمرار والحد من أي انقطاع للخدمة وإن حدثت يتم حلها وتجاوزها بأقصى سرعة ممكنة دون التأثير على المستخدمين، كما يعرض الموقع الإلكتروني للجامعة المعلومات بكل دقة وموثوقية.

- تبين أن المتغيران المستقلان (الخصوصية، التعزيز) يؤثران في جودة الخدمات الإلكترونية، بينما المتغير المستقل (السرية) لا يؤثر بشكل واضح في جودة الخدمات الإلكترونية.
- عدم وجود فروق ذات دلالة إحصائية بين متوسطات تقديرات مجتمع الدراسة حول دور الأمن السيبراني في جودة الخدمات الإلكترونية تعزى إلى متغير (المؤهل العلمي، الخبرة العملية).

## 5-3 التوصيات

**في ضوء النتائج التي توصلت إليها الدراسة توصي الباحثة بما يلي:**

- أهمية قيام إدارة الجامعة بمراجعة صلاحيات المستخدمين على فترات منتظمة.
- تحسين آليات ضبط الوصول للنظام، ووضع برامج وإجراءات خاصة بالمستويات الإدارية والصلاحيات ضمن النظام والتركيز على ضرورات الأمن السيبراني.
- وضع خطة استراتيجية لإدارة المخاطر الأمنية لنظم المعلومات في الجامعة، لضمان اكتشاف مبكر للمخاطر، وكيفية الوقاية من المخاطر والتصدي لها إذا وجدت، تقييم المخاطر التي يتعرض لها النظام بشكل مستمر
- تنمية الكوادر البشرية العاملة في مجالات الأمن السيبراني عن طريق عمليات البحث العلمي والتحاق العاملين بدورات تدريبية في هذا المجال من أجل رفع كفاءتهم، مع التركيز على العاملين الأقل خبرة حسب نتائج الدراسة.
- ضرورة تأسيس هيئة علمية تؤهل وتدرب الكوادر الوطنية السعودية المختصة في المنظمات الحكومية والأهلية لدعم المجتمع ضد مخاطر الجريمة السيبرانية.
- تفعيل دور الوسائل العلمية والعملية للحفاظ على الأمن السيبراني للجامعات بشكل خاص والمؤسسات الحكومية بشكل عام.
- إجراء المزيد من الدراسات والربط ما بين مجالات الأمن السيبراني وتجويد الخدمات الإلكترونية.

# المراجع

أولاً: المراجع العربية


إدريس، جعفر عبد الله موسى (2015م). **إدارة الجودة الشاملة ومتطلبات الحصول على الأيزو**، خوارزم العلمية: المملكة العربية السعودية، جدة.

أمين، خديجة عرفة محمد (2009). **الأمن الإنساني: المفهوم والتطبيق في الواقع العربي والدولي**، جامعة نايف العربية للعلوم الأمنية، (ط1)، الرياض.

البسام، سارة عبد الرحمن (2018). **التحقيق في العوامل المتعلقة بالتوعية بالأمن السيبراني في القطاع المصرفي البحريني**، رسالة ماجستير غير منشورة، جامعة الخليج العربي، البحرين.

جمال الدين، شهاب أحمد (2012). **الأعمال والتجارة الإلكترونية**، مكتبة الملك فهد الوطنية، المملكة العربية السعودية، جدة.

جودة، محفوظ أحمد (2006م). **إدارة الجودة الشاملة مفاهيم وتطبيقات**، دار وائل للنشر والتوزيع: الأردن.

الحلبي، مؤمن عبدالسميع (2017م).**جودة الخدمات الإلكترونية وأثرها على رضا المستخدمين دراسة حالة على برنامج بلق بلس** غزة، رسالة ماجستير غير منشورة، الجامعة الإسلامية، غزة.

حميد، محمد مسعد (2019). **رؤية إستراتيجية لمكافحة الجرائم السيبرانية: اليمن دراسة حالة**، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية.

الخالد، ساري محمد (2018م). **اتجاهات في أمن المعلومات وأمانها**، العبيكان: الرياض.

الداردكة، مأمون سليمان (2006). **إدارة الجودة الشاملة وخدمة العملاء**، دار الصفا لنشر والتوزيع: الأردن.

الشايع، خالد بن سعد (2019م). **الأمن السيبراني مفهومه وخصائصه وسياساته**، الدار العالمية للنشر، الرياض.

الشهري، أحمد بن علي أحمد آل رزيق (2019). **مقترح للتدابير الوقائية من الجرائم السبرانية لتعزيز الاعتدال الفكري**، رسالة (دكتوراه) غير منشورة، –جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاجتماعية، قسم علم الاجتماع، تخصص علم اجتماع الجريمة.

الشهري، علي زايد محمد الجبيري (2019). **رؤية استراتيجية للحد من الجرائم الإلكترونية لتعزيز الأمن السيبراني في المملكة العربية السعودية**، رسالة (دكتوراه) غير منشورة، –جامعة نايف العربية للعلوم الأمنية، كلية العلوم الاستراتيجية، قسم الدراسات الاستراتيجية، تخصص دراسات استراتيجية.

الشوابكة، عدنان عواد (2019). دور إجراءات الأمن المعلوماتي في الحد من مخاطر أمن المعلومات في جامعة الطائف، **مجلة دراسات وأبحاث**، مج (11)، ع (4)، 164-187.

طواهير، عبدالجليل والهواري، جمال (2014). قياس أثر جودة الخدمات الإلكترونية على رضا الزبون: دراسة ميدانية مؤسسة بريد الجزائر، **المجلة السيبرانية**، العدد 35 سبتمبر.

عبد الراضي، حسين (2018). جودة الخدمات الإلكترونية وأثرها على رضا العملاء: دراسة تحليلية على مصر للطيران، **المجلة العلمية للدراسات التجارية والبيئية**، مج (9)، ع (4)، 825-852.

عبد الكافي، إسماعيل عبد الفتاح (2016). **شبكات التواصل والإنترنت: التأثير على الأمن القومي والاجتماعي**، المكتب العربي للمعارف، مصر.

العتيبي، عبد الرحمن بن بجاد (2017). **دور الأمن السيبراني في تعزيز الأمن الإنساني**، رسالة ماجستير غير منشورة، جامعة نايف العربية للعلوم الأمنية.

العضايلة، علي بن محمد (2017). أثر تطبيق معايير جودة الخدمات الإلكترونية وأثرها على رضا طالبات جامعة الأميرة نوره بالمملكة العربية السعودية: دراسة حالة، **المجلة الأردنية في إدارة الأعمال**، مج (13)، ع (3)، 307-329.

العلاق، بشير عباس (2004). **الخدمات الإلكترونية بين النظرية والتطبيق –مدخل تسويقي استراتيجي**، دار النشر المنظمة العربية للتنمية الإدارية.

غانم، رانية (2019). جودة الخدمات الإلكترونية في مكتبات الجامعة اللبنانية من وجهة نظر المستفيدين: معهد الفنون الجميلة– الفرع الرابع نموذجاً، **المركز العربي للبحوث والدراسات في علوم المكتبات والمعلومات**، مج (6)، ع (11)، 154-189.

قشطة، عصام صبحي (2017). فاعلية نظم الاتصالات الإدارية الحوسبة وأثرها في مصداقية امن المعلومات الإلكترونية لدى الجماعات الفلسطينية، دراسة دكتوراه غير منشورة، الجامعة الإسلامية غزة.

كاظم، حمود خضير (2005). **إدارة الجودة الشاملة**، دار المسيرة لنشر والتوزيع: الأردن.

كافي، مصطفى يوسف (2009). **الحكومة الإلكترونية في ظل الثورة العلمية التكنولوجية المعاصرة**، مؤسسة رسلان: سوريا.

مراد، عماد محمد (2016). **اثر جودة الخدمات الإلكترونية المقدمة من البنوك التجارية الأردنية على دراسة رضاء العملاء**، دراسة ماجستير غير منشورة، جامعة عمان.

الهزاني، نورة بنت ناصر (2008). **الخدمات الإلكترونية في الأجهزة الإلكترونية**، مكتبة الملك فهد الوطنية.

**ثانياً: المراجع الأجنبية**

Kistner, J.(2006). Cyber attack simulation and information fusion process refinement optimization models for cyber security(Master Science in Industrial Engineering Rochester Institute of Technology) Retrieved from https://scholarworks.rit.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=8951&context=theses.

Serapiglia,A.(2016). The Case for Inclusion of Competitive Teams in Security Education , Information Systems Education Journal (ISEDJ) 14 (5),ISSN: 1545-679X September 2016, Retrieved from https://files.eric.ed.gov/fulltext/EJ1135363.pdf.

Stringhini G.(2014). Stepping Up the Cybersecurity Game: Protecting Online Services from Malicious Activity(Doctoral dissertation Computer Science) Retrieved from https://pdfs.semanticscholar.org/d929/852b28071972a9ef3618aff9a45643c55407.pdf

**ثالثاً: المواقع الإلكترونية**

الربيعة، صالح بن علي بن عبد الرحمن موقع هيئة الاتصالات وتقنية المعلومات، تاريخ الدخول، 5 يناير، 2020، https://edu.moe.gov.sa/jeddah/DocumentCentre/Docs

موقع المعاني لغة العربية، تاريخ الدخول 12-ديسمبر، 2019، www.almaany.com.

الهيئة المنظمة للاتصالات للأمن السيبراني، تاريخ الدخول 10-ديسمبر، 2019، http://www.tra.gov.lb/Cybersecurity-AR.

# الملاحق

# ملحق (1)

## قائمة المحكمين

| م | الاسم | التخصص | كلية | المرتبة العلمية |
|---|---|---|---|---|
| 1 | هناء بنت عبد الله بن علي النعيم | علوم الحاسبات | الحاسبات وتقنية المعلومات | أستاذ |
| 2 | صباح عبد الله بن درر الصومالي | نظم المعلومات الإدارية | الاقتصاد والإدارة | أستاذ مشارك |
| 3 | فهد مزيد بن محمد العضياني | نظم المعلومات | الحاسبات وتقنية المعلومات بجدة | أستاذ مشارك |

## ملحق (2)

## الاستبانة في صورتها النهائية


Kingdom of Saudi Arabia
Ministry of Higher Education
King Abdul Aziz University
Faculty of Economics & Administration

المملكة العربية السعودية
عمادة الدراسات العليا
جامعة الملك عبد العزيز
كلية الاقتصاد والإدارة


أخي الموظف/ أختي الموظفة،،،

السلام عليكم ورحمة الله وبركاته،

تهدف هذه الدراسة التعرف على (دور الأمن السيبراني في جودة الخدمات الإلكترونية). ولرأيك أخي الموظف/ أختي الموظفة أكبر الأثر في إثراء هذه الدراسة وتحقيق هدفها.

لذا أرجو منكم التكرم بالإجابة عن عبارات الاستبانة بدقة وموضوعية وتأكدوا أن آرائكم الشخصية سوف تكون محل الاهتمام والتقدير ومحاطة بالسرية التامة ولن تستخدم إلا لغرض البحث العلمي فقط شاكرة ومقدرة كريم تعاونك وتقبلي تحياتي وتقديري.

الباحثة،،،

**تعليمات الإجابة: الرجاء وضع علامة (√) أمام الإجابة التي تراها مناسبة**

**أولا: المعلومات الشخصية**

**1.الجنس:**

- ❑ ذكر
- ❑ أنثى

**2. المؤهل العلمي**

- ❑ ثانوي.
- ❑ جامعي.
- ❑ ماجستير.
- ❑ دكتوراه
- ❑ أخرى تذكر.....

**3. الخبرة في مجال العمل:**

- ❑ أقل من 5 سنوات.
- ❑ من 5 – 10 سنوات.
- ❑ 11 – 15 سنة.
- ❑ أكثر من 15 سنة.

**ثانيا: البيانات الخاصة بموضوع الدراسة**

| المحور والبعد | م | العبارة | البدائل | | | | |
|---|---|---|---|---|---|---|---|
| | | | موافق بشدة | موافق | الى حد ما | غير موافق | غير موافق بشدة |
| المحور الأول: الأمن السيبراني | **السرية: من جانب حفظ وسرية المعلومات والبيانات والمعاملات والملفات التقنية من أي تجاوزات أمنية تقنية تلحق الضرر بها، والتأكد من عدم اطلاع على هذه المعلومات من الأفراد الغير مصرح لهم بذلك.** | | | | | | |
| | البعد الأول: السرية | 1 | لدي كلمة مرور قوية تتكون من رموز وأحرف وأرقام صغيرة وكبيرة | | | | | |
| | | 2 | يتم تبادل أرقام المرور السرية بين الموظفين للأنظمة الإلكترونية | | | | | |
| | | 3 | يحدد النظام هوية الموظفين في حالة الدخول على البيانات أو القيام بتعديل عليها | | | | | |
| | | 4 | يسمح النظام بإدخال نفس المستندات الإلكترونية أكثر من مرة. | | | | | |
| | | 5 | توجد تعليمات إدارية صريحة حول حماية النظام من أي تلاعب أو غش | | | | | |
| | | 6 | لدي معرفة بنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها. | | | | | |
| | **الخصوصية: من جانب حماية البيانات الشخصية للأفراد، من أي وسيلة اختراق أو التجسس على معلوماتهم الشخصية.** | | | | | | |
| | البعد الثاني: | 7 | تقوم عمادة تقنية المعلومات بمراجعة صلاحيات المستخدمين على فترات منتظمة. | | | | | |

| المحور والبعد | | م | العبارة | البدائل | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | موافق بشدة | موافق | الى حد ما | غير موافق | غير موافق بشدة |
| المحور الأول: الأمن السيبراني | | 8 | أواجه اختراقات على بريدي الإلكتروني بشكل متكرر. | | | | | |
| | | 9 | تستخدم عمادة تقنية المعلومات عدة تقنيات مثل: المصادقة والترخيص والتشفير لحماية الأنظمة والبيانات الحساسة. | | | | | |
| | | 10 | يتم تشغيل وتحديث جدار الحماية باستمرار لمنع المتسللين من لوصول للبيانات الشخصية أو بيانات العمادة. | | | | | |
| | **التعزيز: وذلك من جانب التعزيز الأمني والحماية، لكل الأنظمة التقنية، والخدمات الإلكترونية من أي تهديدات الإلكترونية محتملة، ويكون ذلك من خلال رفع جودة التعزيز الأمني التقني لبنية التحتية لتقنية المعلومات.** | | | | | | | |
| | البعد الثالث: التعزيز | 11 | تتم مراقبة الموظفين للتأكد من تطبيق السياسات والإجراءات الوقائية لمنع تسريب المعلومات | | | | | |
| | | 12 | تستخدم برامج مكافحة الفيروسات بشكل دوري في أجهزة عمادة تقنية المعلومات لحمايتها من البرامج الضارة. | | | | | |
| | | 13 | تستخدم برامج مكافحة التجسس بشكل دوري في أجهزة عمادة تقنية المعلومات لحمايتها من البرامج الضارة | | | | | |
| | | 14 | توجد نسخ احتياطية (Back up) بشكل دوري في أقراص صلبة أو سحابة خاصة بالعمادة. | | | | | |
| المحور الثاني: جودة الخدمات الإلكترونية | | 15 | توفر الصفحة الإلكترونية الخاصة بالجامعة معلومات وافية عن الجامعة واختصاصاتها | | | | | |
| | | 16 | يعرض الموقع الإلكتروني للجامعة المعلومات بكل دقة وموثوقية. | | | | | |

| المحور والبعد | م | العبـارة | البدائل | | | | |
|---|---|---|---|---|---|---|---|
| | | | موافق بشدة | موافق | الى حد ما | غير موافق | غير موافق بشدة |
| | 17 | يســـتطيع الموظف والطالب الوصـــول إلى الخدمات التي تقدمها الجامعة في موقعها الإلكتروني بسهولة. | | | | | |
| | 18 | يضـــمن الموقع الإلكتروني للجامعة الســـرية للمعلومات الخاصة بالمستخدمين. | | | | | |
| | 19 | تمتلك الجامعة فريق دعم فني متخصـــص يعمل على حل المشـــكلات التي تواجه المستخدمين عبر الموقع الإلكتروني | | | | | |
| | 20 | يوفر موقع الجـــامعـــة الرد الآلي عن أي استفسار من المستخدمين. | | | | | |
| | 21 | يوفر موقع الجامعة ســـهولة الحصـــول على الاستجابة السريعة للمستخدمين. | | | | | |